T.C.
İNÖNÜ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SİBER GÜVENLİK ALANINDA DÜZENLENEN UYGULAMALI ÖĞRETİCİ CTF YARIŞMALARINDA KULLANILAN PROGRAMLARA GENEL BİR BAKIŞ

YÜKSEK LİSANS TEZİ

GÖKHAN ALGAÇ

FİZİK ANABİLİM DALI

Tez Danışmanı: Doç. Dr. Serkan Alagöz

AĞUSTOS – 2020

T.C.
İNÖNÜ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SİBER GÜVENLİK ALANINDA DÜZENLENEN UYGULAMALI ÖĞRETİCİ CTF YARIŞMALARINDA KULLANILAN PROGRAMLARA GENEL BİR BAKIŞ

YÜKSEK LİSANS TEZİ

GÖKHAN ALGAÇ
(36183612018)

FİZİK ANABİLİM DALI

Tez Danışmanı: Doç. Dr. Serkan Alagöz

AĞUSTOS – 2020

TEŞEKKÜR VE ÖNSÖZ

Tez çalışmam boyunca bana rehberlik eden; bilgi, deneyim ve tecrübelerini esirgemeyen danışmanım **Doç. Dr. Serkan ALAGÖZ**'e teşekkür ederim.

Tüm eğitim hayatım boyunca benden maddi ve manevi desteklerini esirgemeyen her zaman yanımda olan sevgili aileme teşekkürlerimi bir borç bilirim.

ONUR SÖZÜ

Yüksek Lisans Tezi olarak sunduğum **"Siber Güvenlik Alanında Düzenlenen Uygulamalı Öğretici Ctf Yarışmalarında Kullanılan Programlara Genel Bir Bakış"** başlıklı bu çalışmanın bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın tarafımdan yazıldığını ve yararlandığım bütün kaynakların, hem metin içinde hem de kaynakçada yöntemine uygun biçimde gösterilenlerden oluştuğunu belirtir, bunu onurumla doğrularım.

Gökhan ALGAÇ

İÇİNDEKİLER

ÇİZELGELER DİZİNİ

ŞEKİLLER DİZİNİ

SEMBOLLER VE KISALTMALAR

APACHE : Web sunucu programı
ARPANET : Paket Dağıtımı Ağı
ASP : Dinamik Servis Sayfaları
BLUETOOTH : Kısa Mesafe Radyo Frekansı Teknolojisi
CERN : Avrupa Nükleer Araştırma Merkezi
CIA : Merkezi İstihbarat Teşkilatı
DARPA : Savunma İleri Düzey Araştırma Projeleri Kurumu
DOS : Hizmet Engelleme
EXPLOİT : Sömürme
FTP : Dosya İletim Protokolü
FBI : ABD Federal Soruşturma Bürosu
HTTP : Hiper Metin Transferi Protokolü
MAC : Medya Erişim Denetimi
ISO : Uluslararası Standardizasyon Örgütü
ISS : İnternet Yayımlama Servisi
IP : İnternet Protokolü
KEYGEN : Şifreleme Kırıcısı
LAN : Yerel Alan Ağı
LİNUX : UNIX işletim sistemi türevi
LTE : Uzun Süreli Gelişim
NSA : ABD Ulusal Güvenlik Dairesi
OWASP : Açık web uygulama güvenliği projesi
ORACLE : İlişkisel Veritabanı Yönetim Sistemi
PHP : Üstün yazı Ön işlemcisi
RAM : Rastgele erişimli hafıza
SQL : Yapısal Sorgulama Dili

TCP **:** İletim Kontrol Katmanı

VPN **:** Özel Sanal Ağ

XSS **:** Siteler Arası Komut Dosyası

WEP **:** Kablolu Erişime Eşdeğer Gizlilik

WAN **:** Geniş Alan Ağı

WİFİ **:** Kablosuz Bağlantı Alanı

WWW **:** Geniş Dünya Ağı

ÖZET

Yüksek Lisans Tezi

SİBER GÜVENLİK ALANINDA DÜZENLENEN UYGULAMALI ÖĞRETİCİ CTF YARIŞMALARINDA KULLANILAN PROGRAMLARA GENEL BİR BAKIŞ

Gökhan ALGAÇ

İnönü Üniversitesi

Fen Bilimleri Enstitüsü

Fizik Ana Bilim Dalı

47 + x sayfa

2020

Danışman: Doç. Dr. Serkan ALAGÖZ

Bu tezde, siber güvenlik tatbikatı ve simülasyonlarında kullanılan programlar incelenmiştir. Bir siber güvenlik tatbikatı bu bilgilere sahip kişilerin bilgilerini uygulamaya dökerek kendilerini test etmelerini sağlar. İki farklı türü mevcuttur. Jeopardy ve savunma-saldırı. Genel olarak web, mobil, kriptografi, adli, ağ, sömürme, tersine mühendislik, bilgi gizleme ve ikili analiz kategorilerinden oluşur.

Bu tezde, siber güvenlik tatbikatı ve simülasyonlarında kullanılan programlar analiz edilerek konu bilimsel açıdan ele alındı. Diğer taraftan programların yapısı, ilişkileri, farklılık ve benzerlikleri ortaya çıkarıldı. Çalışmadaki bir diğer sonuç ise bu süreçte her ne kadar yapılması planlanan tatbikatın hedef kitlesine göre farklılıklar arz etse de, türüne bakılmaksızın genel bir siber güvenlik tatbikatındaki gerekli süreçleri de ortaya koydu.

Anahtar Kelimeler: Siber Güvenlik, Ctf, Program

ABSTRACT

M. Sc. Thesis

AN OVERVİEW OF THE PROGRAMS USED İN THE PRACTİCAL TUTORİAL CTF COMPETİTİONS HELD İN THE FİELD OF CYBER SECURİTY

Gökhan ALGAÇ

Inonu University, Graduate School of Natural and Applied Science Department of Physics

47 + x pages

2020

Advisor: Assoc. Prof. Dr. Serkan ALAGÖZ

In this thesis, the programs used in cyber security exercises and simulations are examined. A cyber security drill allows people with this information to put their knowledge into practice and test themselves. There are two different types. Jeopardy and defense-attack. It generally consists of web, mobile, cryptography, forensic, network, exploitation, reverse engineering, information hiding and binary analysis categories.

In this thesis, the topics used in cyber security exercises and simulations were analyzed and the subject was handled scientifically. On the other hand, the structure, relationships, differences and similarities of the programs were revealed. Another conclusion in the study, although it varies according to the target audience of the exercise planned to be carried out in this process, also revealed the necessary processes in a general cyber security exercise regardless of its type.

Keywords: Cyber Security, Ctf, Program

1. GİRİŞ

Bilişim sistemlerinin ve yazılımların güvenliğinin sağlanmasında önemli yöntemlerden biri de uygulamaların ve sistemlerin gerçeğe oldukça yakın bir şekilde sanal ortama taşınması ve gerçek sistemler üstünde yapılabilecek her türlü savunma ve saldırı senaryolarının test edilmesine olanak sağlanmasıdır. CTF kurumsal servisleri, istemcileri, ağ bileşenlerini, sunucuları ve bütün bu bileşenlerde oluşabilecek zafiyetleri içeren senaryolar barındırmaktadır [1]. Siber güvenlik tatbikatları, bu alandaki bilinirliliği arttırmak, siber dünyada meydana gelebilecek olası farklı senaryolarda ne yapılması gerektiği konusunda gerekli ortam ve materyalin oluşturulması ve bu alanla ilgili uzmanların uygulamalı eğitimleri açısından bakıldığında oldukça önemli bir araçtır. Siber güvenlik tatbikatlarında gerçeğe oldukça yakın şekilde oluşturulan senaryolarla özellikle siber saldırılar ile karşı karşıya iken stres altında doğru kararları verebilme ve takım halinde koordineli hareket edebilmenin zorunluluğunu taşıyarak oldukça önemli katkılar sağlanmaktadır [2].

İngiliz bir bilim insanı olan Tim Berners-Lee, 1989’ da CERN' de çalışırken (www) icat etti. Web aslında dünyanın her yerindeki üniversiteleri ve üniversitelerdeki bilim insanları arasında otomatik bilgi paylaşımı talebini karşılamak üzere tasarlanmış ve geliştirilmiştir [3].

İnternet'in ortaya çıkması Amerikan Federal Hükümeti Savunma Bakanlığı'nın araştırma ve geliştirme birimi olan Darpa’ ya uzanır. Savunma Bakanlığı 1969' da çeşitli askeri araştırma ve bilgisayar projelerini desteklemek için arpanet isminde paket anahtarlamalı bir ağ geliştirmeye başladı. Bu ağ, ABD' deki araştırma kuruluşları ve üniversitelerin değişik türdeki bilgisayarlarını da kapsayarak büyüdü. Stanford Üniversitesi' nde 1973 yılında ağ için bir protokol seti geliştirmek hedefiyle internet working projesi başlatıldı. TCP (İletim Kontrol Protokolü’nün) 1978’e kadar dört türü geliştirildi ve denendi.

1980'de bu grup sabitleşti ve arpanet'e bağlı bilgisayarlar arasındaki iletişimi basitleştirdi. Tüm arpanet kullanıcıları 1983' te (TCP/IP) olarak bilinen Internet Protokolü/ İletim Kontrol Protokolü' ne geçiş yaptılar. O sene TCP/IP, arpaneti de kapsayan Savunma Bakanlığı internetinde kullanılmak için standartlaştırıldı. 1990'da arpanet kullanımdan kaldırıldı. Yerini Japonya, ABD, Pasifik ülkeleri ve Avrupa'daki hükümet ve ticari işletimindeki omurgalar aldı.

Şekil 1.1. İlk Web Sitesinin Yeniden Oluşturulmuş Sayfasının Ekran Görüntüsü [4].

Siber dünya kara, deniz, hava ve uzaydan sonra yeni bir savaş alanı olarak kabul gördüğünden beri özellikle ulusal güvenlik bakımından son derece önemli olmaya başlamıştır. Siber saldırıların gizli ve anonim olarak yapılabilmesi, reddedilebilirliği ve başka alanlara göre, gerçekleştirilen faaliyetlerin oldukça düşük maliyetlerde olması, bu saldırıları oldukça popüler hale getirmiştir. Öyle ki ülkeler, basit düzeyde gerçekleştirilen siber saldırılar bir kenara, oldukça ileri düzeyde teknoloji ve sofistike seviyede siber silahlar geliştirmeye başlamışlardır.

Siber savunma alanında ülke, kurum yada kuruluşların teknik yeterliliklerini test etme, gerekli eğitimleri ve bilinçlendirmeyi sağlaması bakımından siber savunma tatbikatları tüm dünya genelinde yaygınlık kazanmaya ve oldukça önemli rol oynamaya başlamıştır [2].

Bu bölümde bilişim güvenliği sisteminde yaygın olarak kullanılan güvenlik yazılımları genel özellikleri ile tanıtılacaktır. Çizelge 1 ve 2‘ deki güvenlik yazılımları işlevlerine göre kategoriler halinde sunulmuştur.

1. Kötücül yazılım temizleyici
2. Uygulamaya özel tarayıcılar
3. Web tarayıcı araçları
4. Şifre kırıcılar
5. Şifreleme araçları
6. Hata ayıklayıcılar
7. Güvenlik duvarları
8. Adli bilişim araçları
9. Otomatik böcek bulma programları
10. Genel amaçlı araçlar
11. Saldırı tespit sistemleri
12. Paket işçiliği araçları
13. Port tarayıcılar
14. Rootkit dedektörleri
15. Güvenlik odaklı işletim sistemleri
16. Paket koklayıcıları
17. Güvenlik açığı sömürü araçları
18. Ağ trafiği izleme araçları
19. Güvenlik açığı tarayıcıları
20. Web proxy araçları
21. Web güvenlik açığı tarayıcıları
22. Kablosuz ağ araçları [5].

Çizelge 1.1. Bilgisayar Sistemlerinde Sık Kullanılan Bazı Güvenlik Araçları 1

Genel Amaçlı Araçlar	Kötücül Yazılım Temizleyici	Rootkit Tarayıcıları	Böcek Bulma Araçları	Uygulamaya Özel Tarayıcılar	Web Tarayıcı Araçları	Web Proxy Araçları	Web Güvenlik Açığı Tarayıcıları	Şifre Kırıcılar	Şifreleme Araçları	Hata Ayıklayıcılar
Netcat	CleanAV	Sysintenius	n3af	İke-scan	Firedon	Pares Proxy	Burp Suite	Aircrack	OpenSS HPuTTY SSH	IDA Pro
Pingtebetnetstat	Virus Total	Tripwire	Wfuzz	NBTScan	Firybug	Sel wtrip	W3af	Cain andAbel	True Crypt	Intranity Debugger
Perl/PyhtonRuby	Malwarebytes Anti-Malware	DurpSec	Wapiti	THC Amap	Tamper Daya	Fiddler	Nikto	John the Ripper	Gen PQPQP	WinDbg
VMware		HijackThis	Skipfish		No Script	Ratprox y	Web Scan	THC Hydra	Open VPN	OllyDbg
Google		AIDE					SQL map	ophcrack	Keepass	GDP
Firefox							Skipfish	Medusa	Stusnet	
tURL							AppScan	fgtdump	OpenSSL	
Socat							Fire Bug	Lopht Crack	Tbe	
							Samurai WTF	Solar Wendr		
							Net Sparker	Rairbow Crack		
								Wfuzz		
								Brutus		

Çizelge 1.2. Bilgisayar Sistemlerinde Sık Kullanılan Bazı Güvenlik Araçları 2

Adli Bilişim Araçları	Paket İşçiliği Araçları	Paket Koklayıcıları	Port Tarayıcılar	Saldırı Tespit Sistemleri	Güvenlik Odaklı İşletim Sistemleri	Güvenlik Duvarları	Güvenlik Açığı Sömürü Araçları	Güvenlik Açığı Tarayıcıları	Ağ Trafiği İzleme Araçları	Kablosuz Ağ Araçları
Maltego	Netcat	WireShark	Angry IP Scanner	Snort	Keoppix	Netfilter	Metasploit	Nesson	Ettercap	Aircrack
TheSleuth Kit	Hping	Ettercap	SuperScan	OSSEC HIDS	SELinux	Norton	W3af	CoreImpact	Npep	Kısmet
Encase	Scapy	Cain&Abel	NetScan Tools	OSSIM	Helix	Zone Alarm	CoreImpact	Open Vas	Ntop	Net scanbler
Helix	Yersinia	TCP dump	UticornScan	squil	Backtrack	Open BSDPF	sqlmap	Nespoie	Ettercap	SSH DER
	Nestnesis	Kısmet		Arclight SIEM platform			Catvan	GFİ LanGuard	Solar Winds	Kis MAC
	Socat	Network Miser		Honeyd			Web Goat	Retina	Sphınk	
		Dsniff					Dradin	MBBA	Napos	
		Nrap					BtEY	QualiyGuard	Argun	
		Ngrep					Sqlninja	Nipper	Pöf	
		Etherape						SAINT		
		Pöf						Secturia		
		inSSIDer						PSİ		

2. WEB

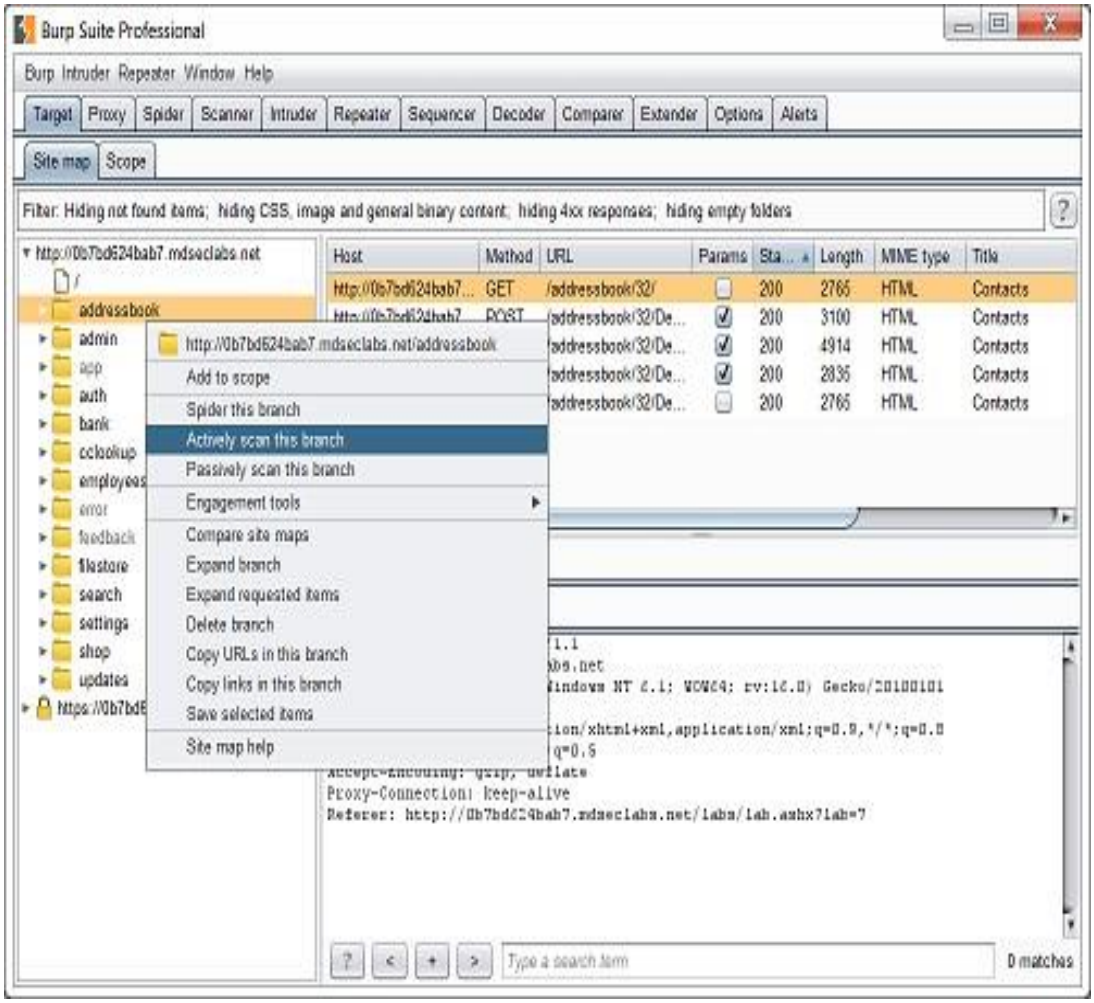
Sistemler güvenlik bakımından ne kadar dikkatli olsalar da bilgisayarlarda çalışan yazılımlardan veya insanlardan kaynaklanan farklı sebeplerle güvenlik zafiyetlerinin oluşması her zaman muhtemeldir. Bu nedenle yazılımların ve ağların sürekli kontrol edilmesi sistemlerin ve yazılımların güvenliğinin sağlanması için çok önemlidir. Bu bilginin ve uygulamanın güvenliğinin sağlanması bakımından gerekli olan bir durumdur. Uygulamayı yazılım açıkları bakımından güvenli bir hale getirmek için zafiyetleri bilmek gerekmektedir. Bu yazılım zafiyetleri sürekli değişmektedir.

Örneğin; 2010' da dünyada bulunan ilk 10 Web Uygulama Güvenlik Riskleri aşağıdaki gibidir.

A1: Kontrol Edilmeyen Yönlendirme
A2: Güvensiz Doğrudan Nesne Referansı
A3: Güvensiz Depolama ile Şifreleme
A4: Enjeksiyon Açıklıkları
A5: Yeterli Olmayan Transport Layer Koruma
A6: URL Erişim Kısıtlamalarına Uyulmaması
A7: İhlal Edilen Oturum Yönetimi ve Kimlik Doğrulama
A8: Siteler Ötesi İstek Sahteciliği
A9: Güvenlik Yapılandırılmasının Yanlış Olması
A10: Siteler Arası Betik Yazma

2.1. Burp Suite

Web ataklarında kullanılan oldukça güçlü tümleşik bir araçtır. Web sistemi saldırılarını hızlandırmak ve kolaylaştırmak için çok çeşitli araçlar ve arabirimler içerir.



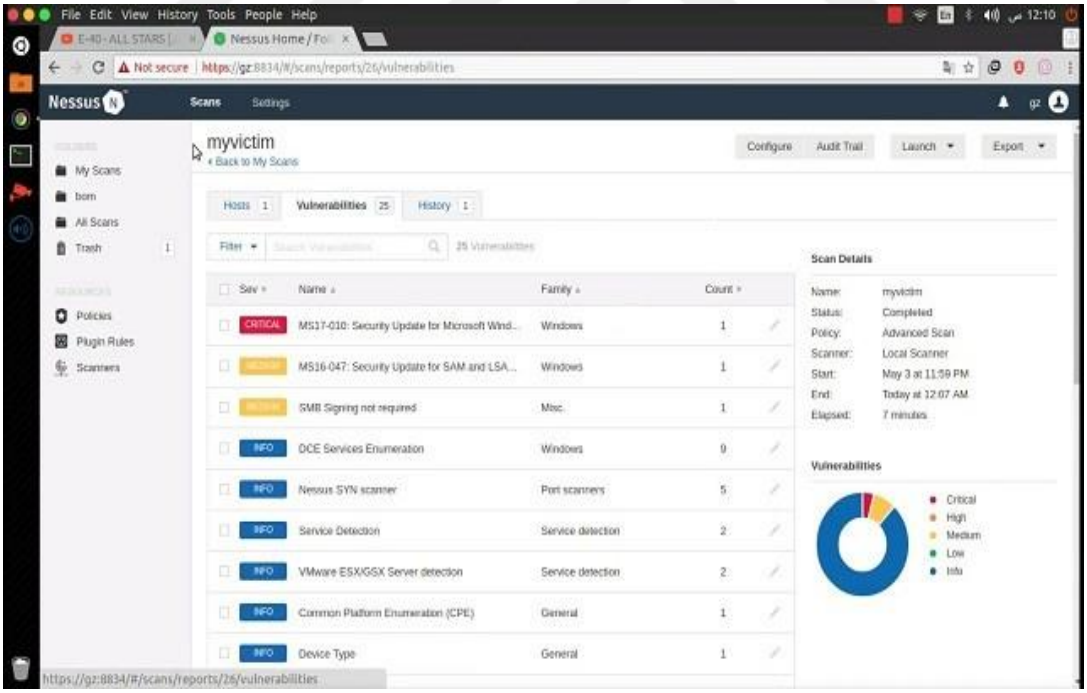
Şekil 2.1. Burp Suite Programının Ekran Görüntüsü

2.2 W3af

Web açıklarını bulmak, saldırıları tespit etmek için oldukça güçlü, esnek ve popüler bir programdır. Kullanılması oldukça kolaydır. Korunmasızlık sömürücü ve web değerlendirme eklentileri mevcuttur. Web penetrasyon yazılımları arasında en güçlülerden biridir.

2.3. Nessus

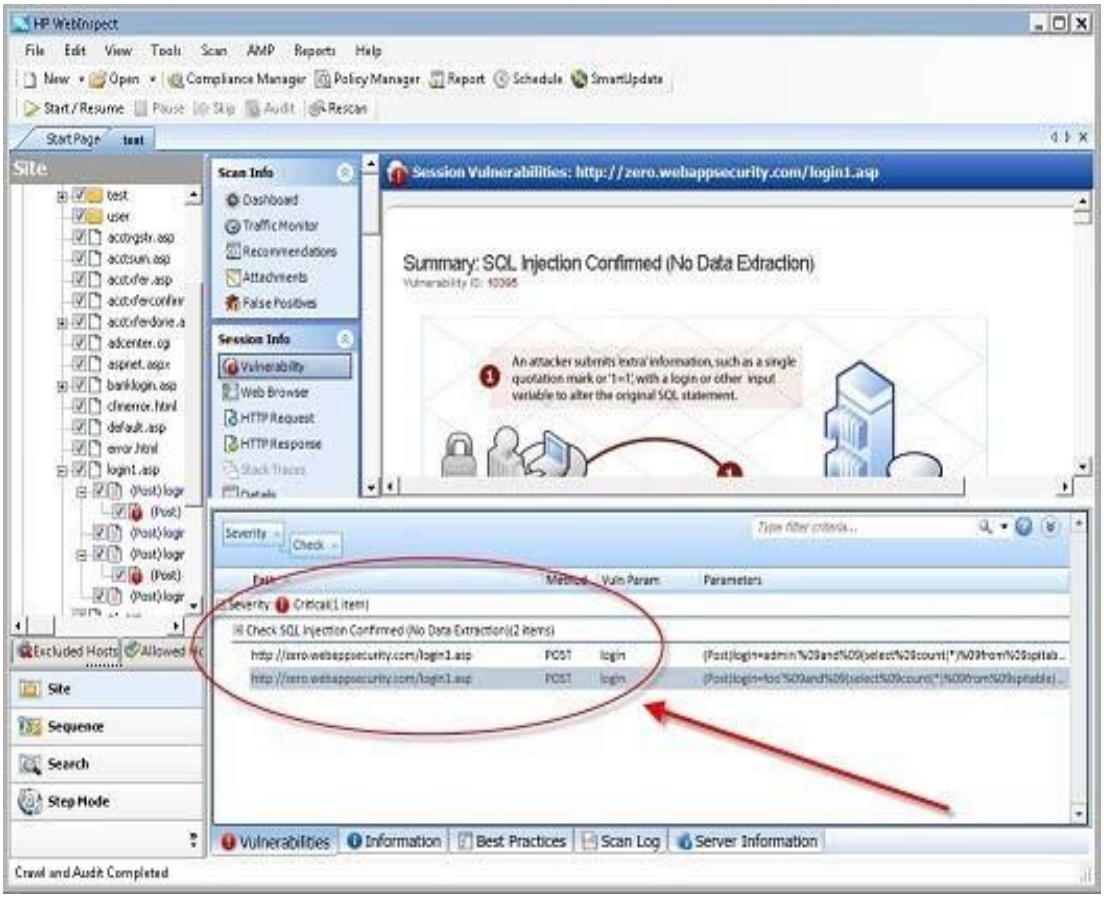
Güncel ve güçlü uzaktan tarama yazılımıdır. Windows' ta ve UNIX' in birçok türevi üzerinde çalışabilir. Arayüzü ve ek yazılımları ile oldukça kullanışlı güvenlik yazılımıdır. 1200'ün üstünde güvenlik açığını bulabilir ve bunlarla ilgili farklı biçimlerde raporlar hazırlayabilir (LaTeX, HTML, ASCII, vs.). En önemli özelliği kurallara takılmadan tarama yapmasıdır [6].



Şekil 2.2. Nessus Programının Ekran Görüntüsü

2.4. WebInspect

Web uygulamaları üzerinde bilgi güvenliğinin sağlanmasına açıklık taramada kullanılır. Aynı zamanda uygulamaların çalıştığı sunucularda potansiyel güvenlik risklerine karşı incelenerek değerlendirilmiş olur. Microsoft Visual Studio .NET, Oracle Application Server, Lotus Domino, Macromedia vb. araçlarla geliştirilen uygulamalar üzerinde kodlama hataları, web servisleri, script ve makrolar güvenlik taramasından geçirilir. WebInspect Enterprise Edition içerisinde hazır kompleks tarama yapabilen yardımcı test araçları ile gelişmiş kolay kullanılabilir bir web ara yüzüne sahiptir.

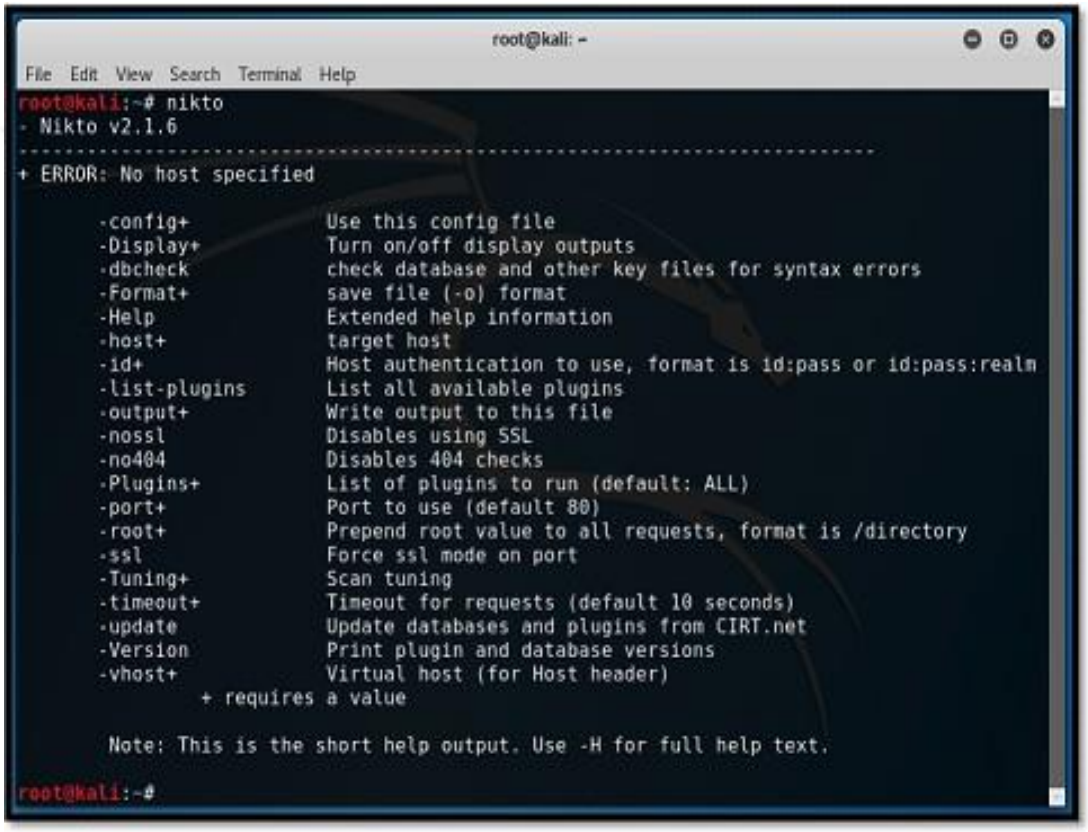


Şekil 2.3. Weblnspect Sql İnjectionTesti

2.5. Nikto

Web sunucuları üzerinde kapsamlı güvenlik test hizmeti yapan açık kaynak kodlu popüler bir yazılımdır. Güncel bir nikto test aracı sistem üzerinde 6000 civarında bilinen güvenlik açıklıklarını sınar. Uygulamayı gerçek portal ortamına almadan birçok güvenlik uzmanı ve yazılım geliştiriciler nikto ile testten geçirirler.

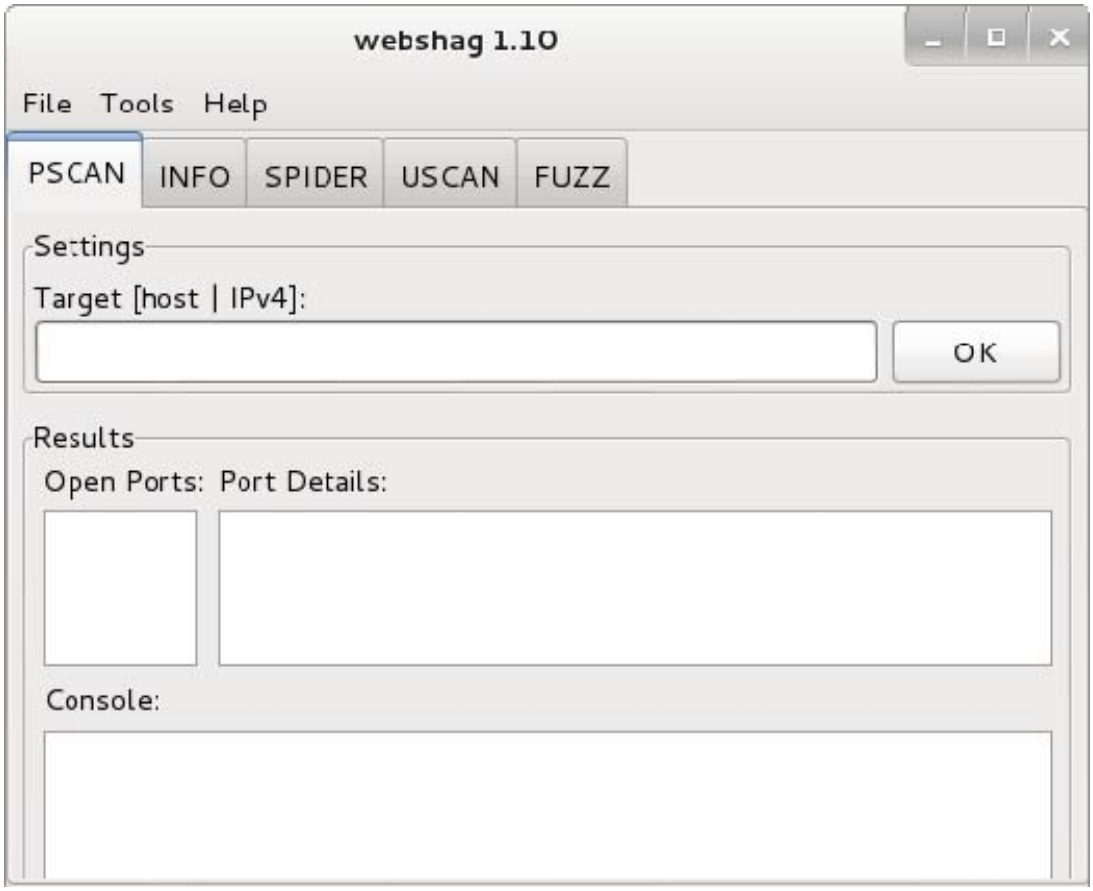
Potansiyel tehlike oluşturacak uygulama açıklıkları, unutulmuş scriptler ve yanlış yapılandırmalara karşı statik web açıklıklarını tarar. Sanal makine üzerinde kurulum yapıp uygulamaların test edilmesi daha sağlıklı sonuçlar verir.



Şekil 2.4. Nikto Kali Linux Üzerindeki Ön Sayfası

2.6. Webshag-Gui

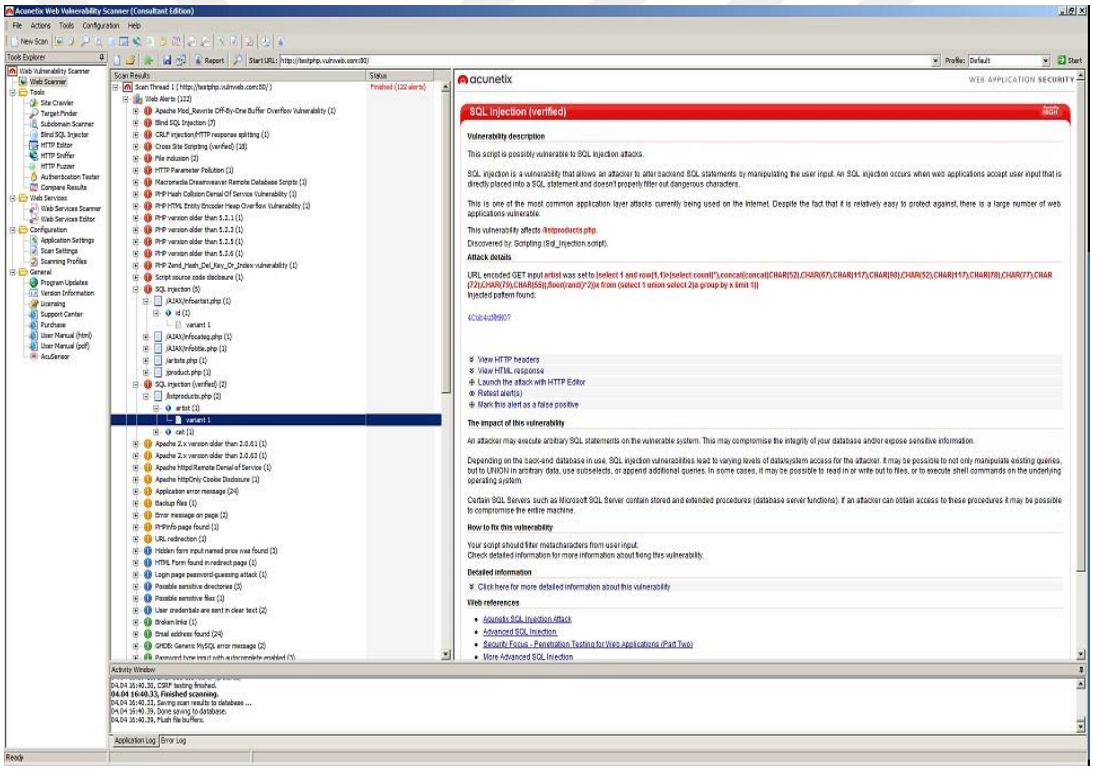
Linux ve Windows platformlarda çalışan web sunucu güvenlik denetim aracıdır. HTTP, HTTPS web yayını yapan sunucular üzerinde kimlik doğrulama testi, URL ve web sitelerini hata ve açıklıklara karşı tarar. Özellikle USCAN komutu ile web sitesi güvenlik işlemi yapılır. FUZZ ile web sunucusundaki gizli dosyalar taranır. Grafiksel ekran üzerinden kolay kullanıma sahiptir.



Şekil 2.5. Webshag-Gui Programı

2.7. Acunetix

Web uygulama projelerinin sunumunun yapıldığı 80 portu siber saldırıların gerçekleştiği en önemli kanaldır. Online portal işlem sayfaları, formlar, üyelikler, parasal işlemler gibi dinamik içerikli yazılımlar üzerinde SQL injection, XSS ve diğer güvenlik açıklarını test eden gelişmiş bir yazılımdır. PCI DSS, OWASP önemli 10 açıklığı ve HIPAA uyum raporlarına uygun taramalar gerçekleştirir. İşlem sonuçları kabul edilebilir, düşük, yüksek ve kritik seviyelerde risk ölçeklemesi gerçekleştirir. Yeni güvenlik açıklıklarının tanınabilmesi için online update işlemi gerçekleştirilir. Sunucularda kullanılan PHP, ASP, ASP.NET, IIS, Apache gibi yazılım araçları üzerindeki olabilecek açıklıkları da tanır ve raporlar [7].



Şekil 2.6. Acunetix Programı Üzerinde Sql İnjection

3. MOBİL

Mobilleşme bilişim teknolojilerinin ilerlemesiyle birlikte sürekli yaygınlaşmış, kurumsal ve bireysel hizmetleri kolaylaştırması ile de tüm alanlarda hızlıca yayılmaya başlamıştır.

Mobil fırsatlardan yararlanabilmek için gün geçtikçe ortaya birçok inovasyon çıkmıştır. İşletim sistemlerinde Google'nin Android yazılımı, donanım alanında Apple'ın ipad cihazları, Skype gibi programlar ve LTE, 4G gibi ağ teknolojileri örnek olarak gösterilebilir.

Kurumlar ve kişiler değişen ve gelişen mobil teknolojilere uyum sağlayıp mobil aygıtların kullanımını artırırken, bu cihazlardaki güvenlik zafiyetleri, kurumların ve kişilerin en büyük kaygıları arasında bulunmaktadır.

Mobil aygıtlardaki kızılötesi, bluetooth, wi-fi ve benzeri erişilebilirliği sağlayan çok sayıdaki özellik, saldırganlar için dizüstü ve masaüstü bilgisayarlara göre mobil cihazları cazip bir duruma getirmiştir. Mobil aygıtlara ait aşağıdaki özelliklerde açık olması halinde aygıtlar saldırıya açık hale gelebilir:

- Bluetooth
- Sms
- Wi-Fi
- USB –Ağ tarayıcı –Email sunucusu
- Fiziksel Erişim
- Kızılötesi
- İşletim Sistemi açıkları
- Üçüncü taraf uygulamaları [8]

3.1. Termux

Termux Android cihazlarda kullanılabilen bir konsoldur. Android cihazların çekirdeği Linux çekirdeğidir. Bu sebeple Termux bildiğimiz Linux terminalinin mobil versiyonudur. Herhangi bir linux dağıtımında yapabildiğimiz her şeyi (neredeyse) Termux üzerinden yapabiliriz.

Şekil 3.1. Termux

Termux'u açtığımız zaman karşımıza siyah bir konsol geliyor. Nerede olduğumuzu belirten bir $ işareti var. Soldan sağa doğru parmağımızla çektiğimiz zaman bir menü geliyor. Bu menüde keyboard yazısı klavyeyi gösterip gizlemeye yarıyor. New session ise yeni bir terminal açmaya yarıyor. Yeni terminali kapatmak için konsola exit yazıp entera basmamız gerekiyor. Termux ile aklınıza gelen herşeyi yapabilirsiniz. Sqlmap kullanabilirsiniz, bruteforca yapabilirsiniz, metasploit framework ile ağdaki cihazlara sızabilirsiniz. Kısacası kali Linux toollarını yükleyerek istediğiniz herşeyi yapabilirsiniz. Termux kullanmak root izni gerektirmez [9].

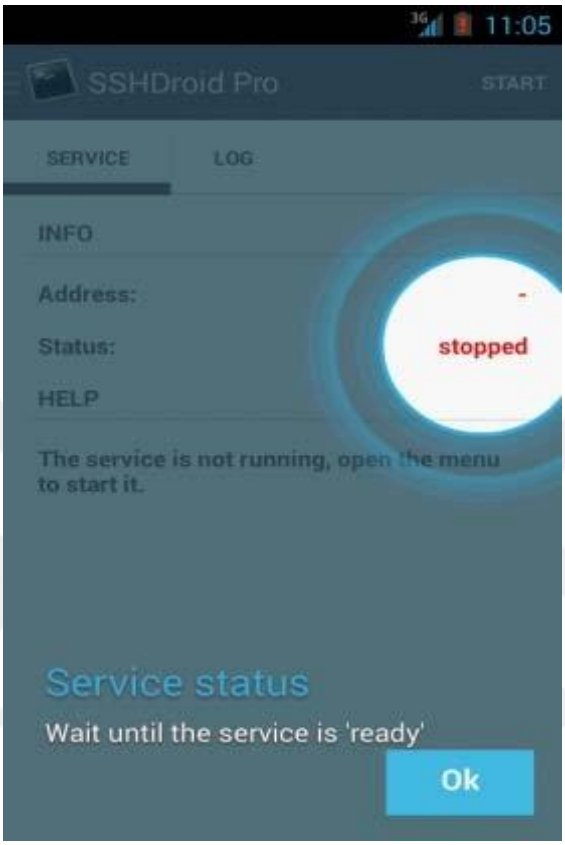
3.2. Hackode

Ravi Kumar tarafından geliştirilen siber güvenlik profesyonellerinin, etik hackerların penetrasyon testi yapmasını hedefleyen bir uygulamadır. Exploit, keşif içeren modüller ve birçok tarama yapma imkanı sunmaktadır. Google dorklarını kullanarak açık olan siteleri bulur [10].

Şekil 3.2. Hackode

3.3. SSHDroid

Android için ssh sunucu uygulamasıdır. Bu uygulama bir bilgisayardan telefonunuza bağlanmak, dosyaları düzenlemek ve çalıştırmak için izin verir [11].



Şekil 3.3. SSHDroid

3.4. Fing - Network Tools

Fing uygulaması milyonlarca kişi tarafından kullanılan en başarılı ücretsiz bir ağ bulma aracıdır. Fing'in ağ tarayıcısı her ağı tarar ve tüm bağlı cihazları hızlı ve doğru bir şekilde tespit eder. İnternet hız testleri, wifi hız testleri, indirme hızı ile yükleme hızı analizi ve gecikme süresi testleri yapabilirsiniz [12].

Şekil 3.4. Fing- Network Tools

4. KRİPTOGRAFİ

Kriptografi, bilgi güvenliğini analiz eden ve anlaşılanı anlaşılamaz hale getiren çalışma alanıdır. Başka bir deyişle belli matematiksel yöntemleri içeren şifre çözme ve şifreleme bilimidir [13].

Temel olarak aşağıdaki konularla ilgilenir:

Gizlilik: İzinsiz kullanıcılar tarafından veri anlaşılamamalı.

Bütünlük: İletilmek istenen yada saklanan bilgi farkına varılmadan değiştirilememeli.

Reddedilemezlik: Bilgi gönderen şahıs, sonradan bilgiyi gönderdiğini inkar edememeli.

Kimlik belirleme: Gönderen ve alıcı, karşılıklı kimliklerini doğrulayabilmeli. Farklı kimliğe bürünme fırsatına davetsiz bir misafir erişmemelidir [14].

Kuantum Kriptografi

Kuantum kriptografi'de ana ilke bir kere kullanılan anahtarlı kriptografi yönteminin kullanılmasıdır. Veri iletimi elektriksel izler yerine fotonlar aracılığıyla yapılmaktadır. Haliyle iletişim kanalı fiber optik ağa gereksinim duyar [15].

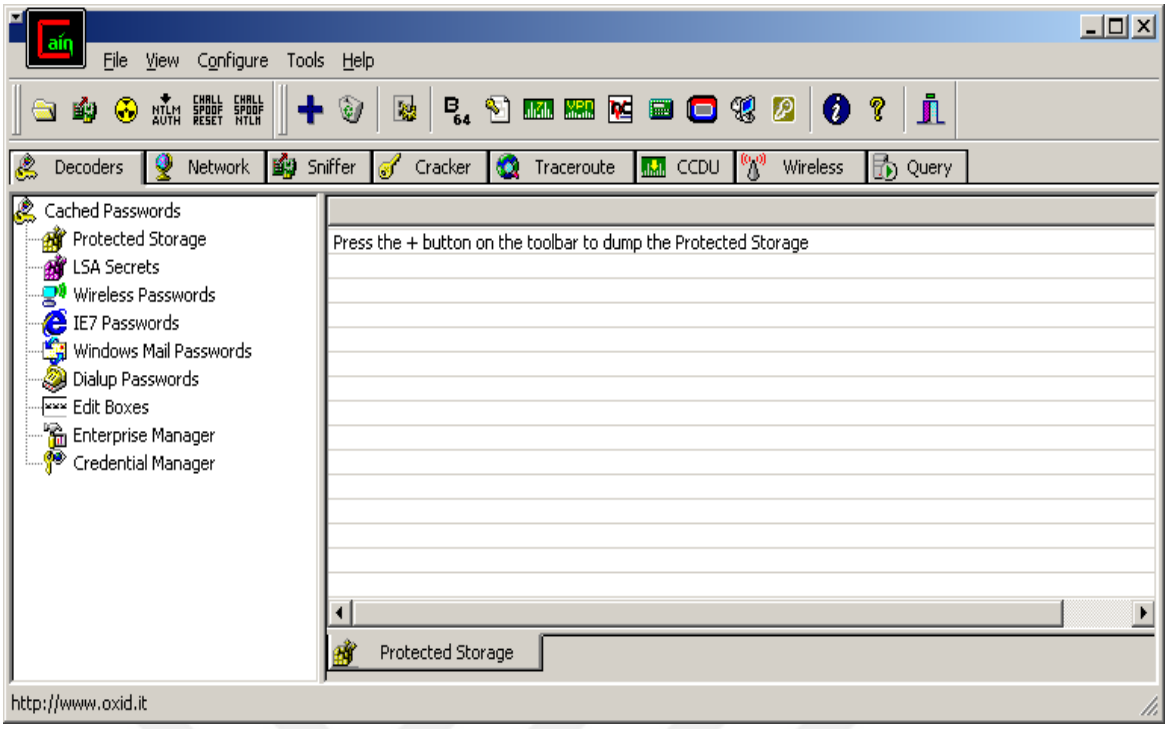
4.1. John The Ripper

John the Ripper oldukça güçlü bir şifre kırma uygulamasıdır. Çevrimdışı şifre kırma test ve denetim aracıdır. DES/MD5/AES/LM vb. değişik algoritmalarla karmaşık okunamaz halde şifrelenmiş parola dosyalarını çözümleme testi için kullanılır. Linux, Windows, Unix sistemlerinde sorunsuz çalışır. John The Ripper aracı ile birlikte gelen "password.lst" sözlük dosyası içerisinde alternatif şifre sözlük saldırıları dener [5-7].

Şekil 4.1. John The Ripper

4.2. Caın & Abel

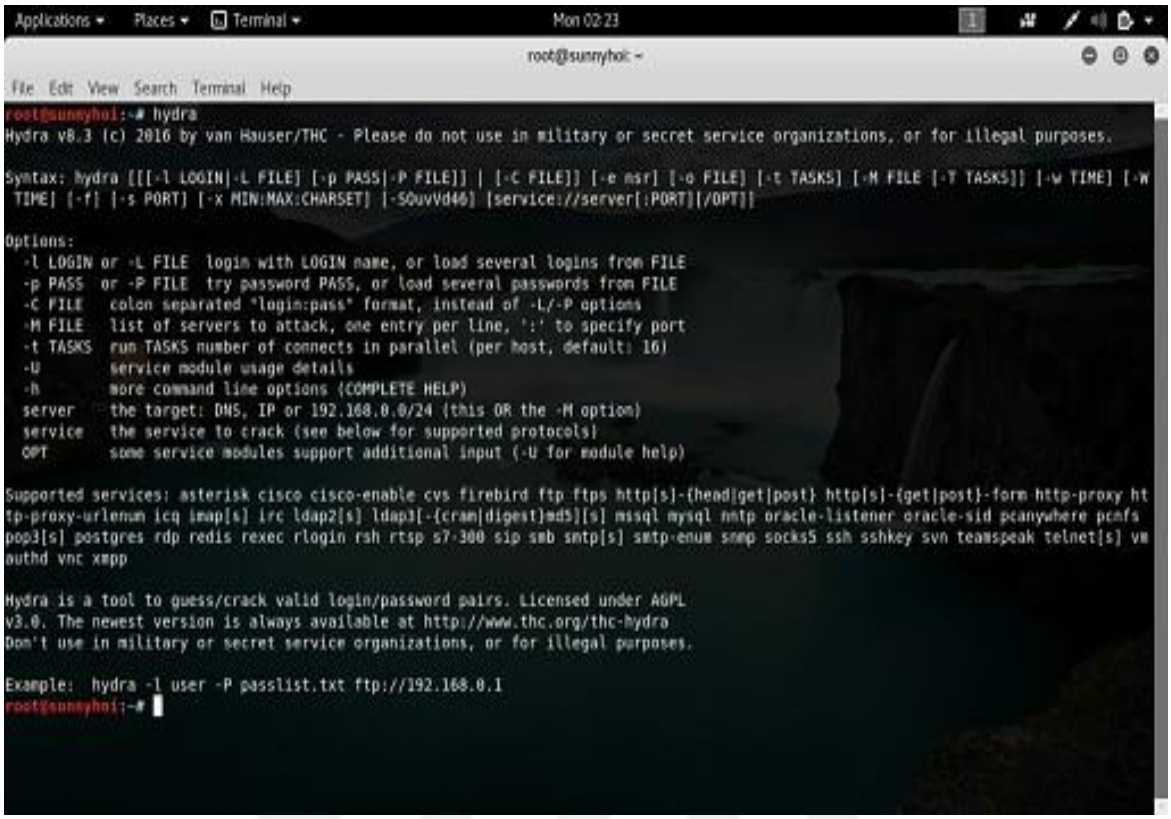
ARP Poison dalında oldukça iyi sayılabilecek programlardan biridir. Pek çok protokolde şifre kırma ve yakalama test işlemi yapabilir. MSSQL, ORACLE, MYSQL, WEP, LM, NTLM, NTLMv2, Cisco-IOS MD5, Cisco Type-7, IKE-PSK gibi geniş kapsamlı uygulama ve protokol üzerinde şifre çözümleme denemesi gerçekleştirebilir. Ayrıca SSH-1, HTTPS, VoIP trafiklerini de şifre yakalama atakları gerçekleştirebilmekledir. Bu test aracını güvenlik denetleyicileri, sistem yöneticileri ve yazılım geliştiriciler tarafından penetrasyon testlerinde sıklıkla kullanır.



Şekil 4.2. Cain- Abel [5-7].

4.3. Hydra

Pek çok protokolde şifre kırma ve yakalama test işlemi yapabilir. MSSQL, ORACLE, MYSQL, WEP, LM, NTLM, NTLMv2, Cisco-IOS MD5, Cisco Type-7, IKE-PSK gibi geniş kapsamlı uygulama ve protokol üzerinde şifre çözümleme denemesi gerçekleştirebilir.

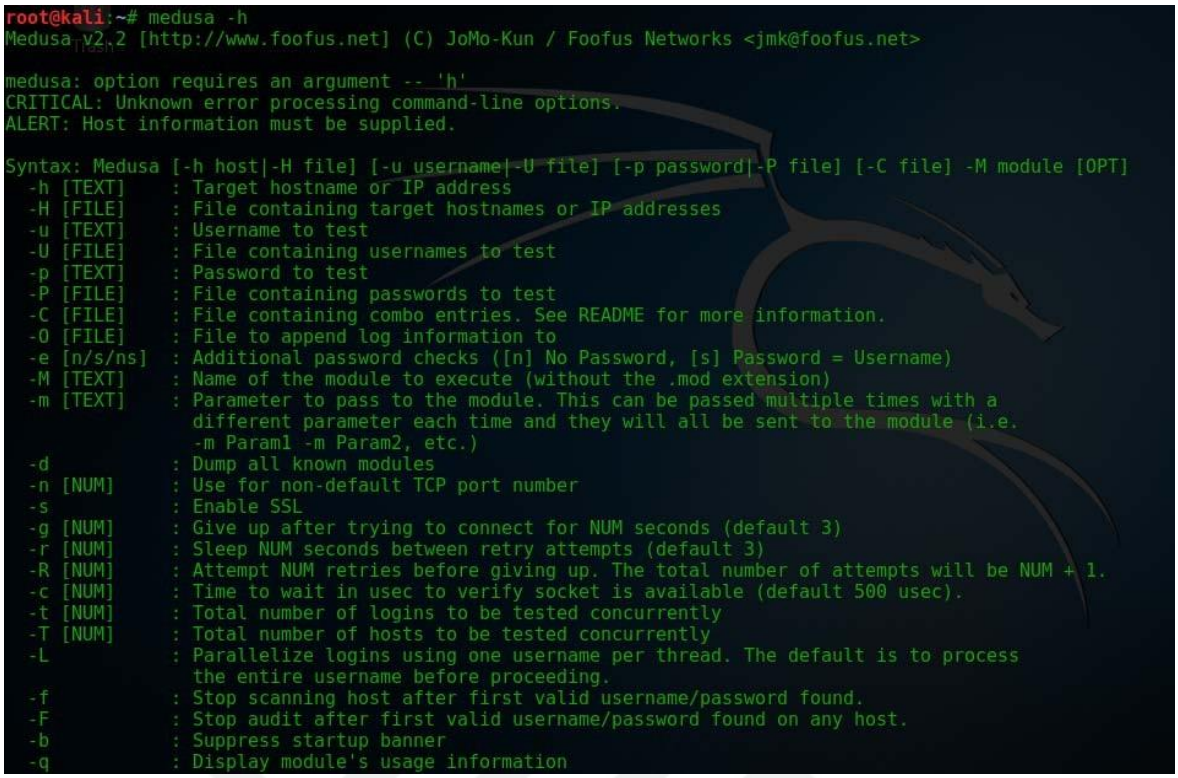


Şekil 4.3. Hydra Kali Linuxta Temel Parametreleri

4.4. Medusa

Güvenlik yöneticilerinin kötü ve zayıf şifrelerin bir siber tehdit haline dönüşmemesi için açık kaynak kodlu bir parola denetim aracıdır. Kolayca tahmin edilebilen, anlamlı günlük kelimelerden oluşan, takım, nesne, sayı, canlı isimleri gibi değişkenlerden oluşan 3,5 milyon kelime hugewordlist.txt dosya mevcuttur.

Örnek; #medusa-h Hedef IP Numarası -u "admin"-P hugewordlist.txt-M http şeklinde bir dizilimde uzaktaki bir sistemde online erişimle http uygulaması üzerinde kullanıcı adı “admin” olan bir sisteme 3,5 milyon farklı şifre denemesi gerçekleştirir. Bu şekilde bir testle sistemdeki zayıf şifreler tespit edilir ve güçlü şifre kullanımı sağlanmış olur.



Şekil 4.4. Medusa [7].

5. ADLİ

Adli bilişim, bilgisayar verisinin elde edilmesi, tanımlanması, muhafazası, dökümantasyonu ve yorumlanmasıdır [16].

Bu dalda en çok SIFT, Forensic Toolkit ve Encase Forensic gibi yazılımlar bilinir.

5.1. Encase Forensic

Dünyada kullanılan adli bilişim yazılımlarının ön sıralarında yer alır. İşletim sistemi olarak windows üzerinden çalışmaktadır.

Bu yazılım ile:

Veriyi kurtarabilmekte,

Dosyalar üstünde hash analizi ve imza analizi yapılabilmektedir.

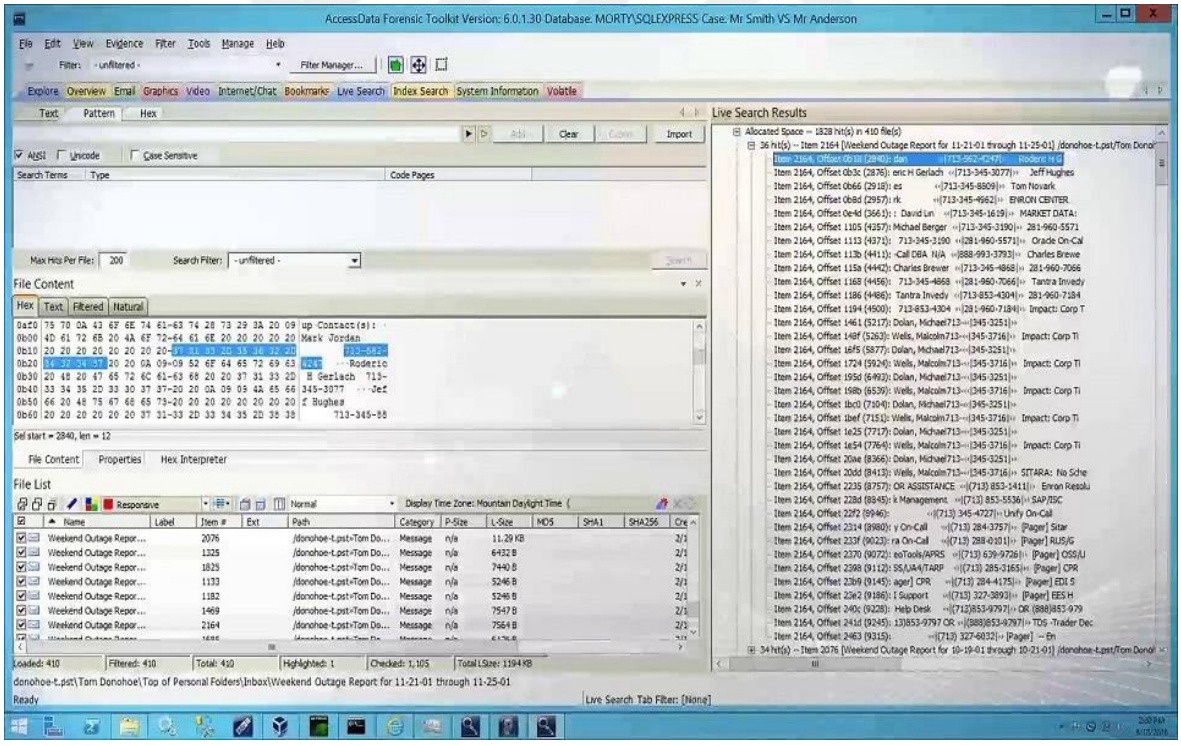
5.2. Forensic Toolkit (Ftk)

AccessData Software firması tarafından kullanıma sunulan ücretli bir programdır. FTK programı ile yapılan adli bilişim analizleri mahkemelerde onay görmüş bir güvenirliğe sahiptir.

Bu yazılım ile:

Adli kopya ve E-delil üzerinden hash incelemesi yapılabilmektedir,

100'den fazla yazılımın şifresi geri getirilip bulunabilmektedir.



Şekil 5.1. Forensic Toolkit

5.3. The Sleuth Kit ve Autopsy

Windows ve Unix sistemlerinde çalışabilmektedir. Komut satırı üstünden kullanılabilen analiz ve inceleme yazılımıdır.

Bu yazılım ile:

Veriyi kurtarabilir,

Steganography denetlemesi yapılabilir [17].

6. AĞ

Birden çok sayıda bilgisayarın karşılıklı iletişim halinde bulunmasıdır. Bu iletişim internetten aynı lokasyonda olan iki bilgisayar arasında da olabilir, farklı kıtalardaki iki bilgisayar arasındada [18].

Bilgisayar ağları birçok açıdan sınıflandırılabilir. Bunlar, point-to-point (noktadan noktaya) veya multi-point (çok uçlu); bounded (sınırlı) veya brodcast (çoklu) yayın kullananlar; devre, mesaj veya paket anahtarlamalıdır. Bunlar aynı zamanda ağ topolojilerine göre de sınıflandırılabilir. Ayrıca coğrafi konumuna göre iletişim sistemleri Lan ve Wan olmak üzere ikiye ayrılır [19].

Belirli bir ağdaki yazılım güvenlik açıklarının tespit edilmesi için, birden fazla ağ elemanı arasındaki etkileşimler dikkate alınmalıdır. Bir güvenlik açığı analiz aracının pratikte faydalı olması için iki özellik çok önemlidir. İlk olarak, analizde kullanılan modelin hata bildirme topluluğundaki resmi güvenlik açığı özelliklerini otomatik olarak bütünleştirebilmesi gerekir. İkincisi, analiz, binlerce makineye sahip ağlara ölçeklenebilmelidir [20].

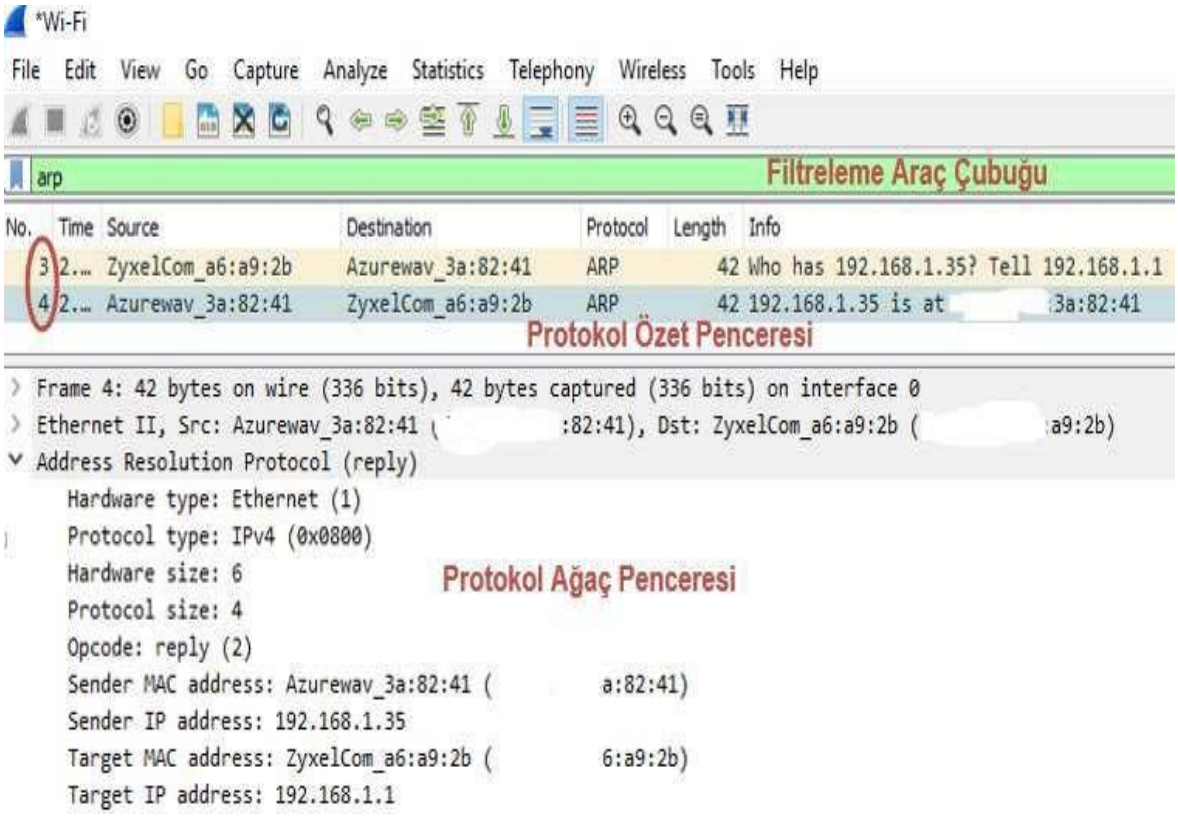
6.1. Wireshark

Wireshark, temelinde protokol analiz ve bir ağ paket (sniffer) programıdır.

Özellikleri:

Çok kıstasta filtreleme ve arama, gerçek zamanlı inceleme yapmaya imkan sağlar.

Paketleri ve protokol bilgilerini detaylı bir şekilde gösterebilir [21].

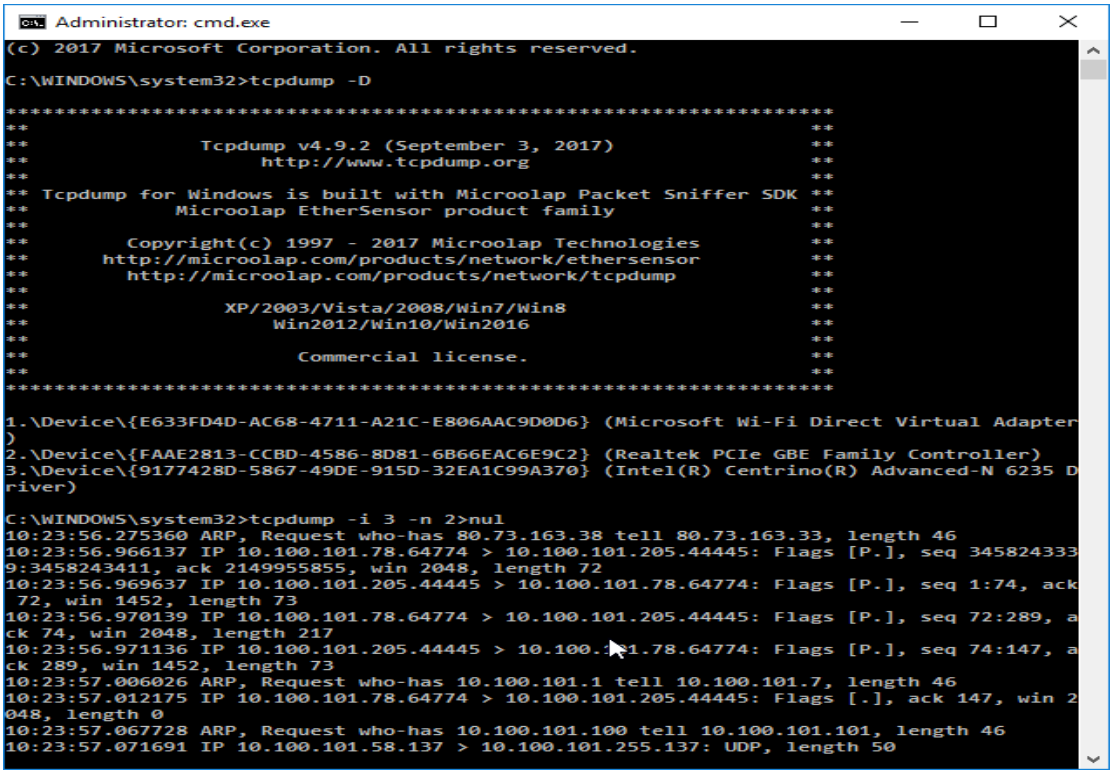


Şekil 6.1. Yakalanan Örnek Bir Paket Çifti

6.2. Tcpdump

Linux barındıran cihazlarda komut satırında çalışan paket analiz eden bir yazılımdır. Kullanan kişiye bulunduğu ağ üzerinden gelen veya giden paketleri yakalama ve izleme imkanı sunar [22].

Kernel'e giriş-çıkış olmadan paketleri yakalar bu nedenle Linux için kullandığınız kurallar tcpdump'ı etkilemez [23].



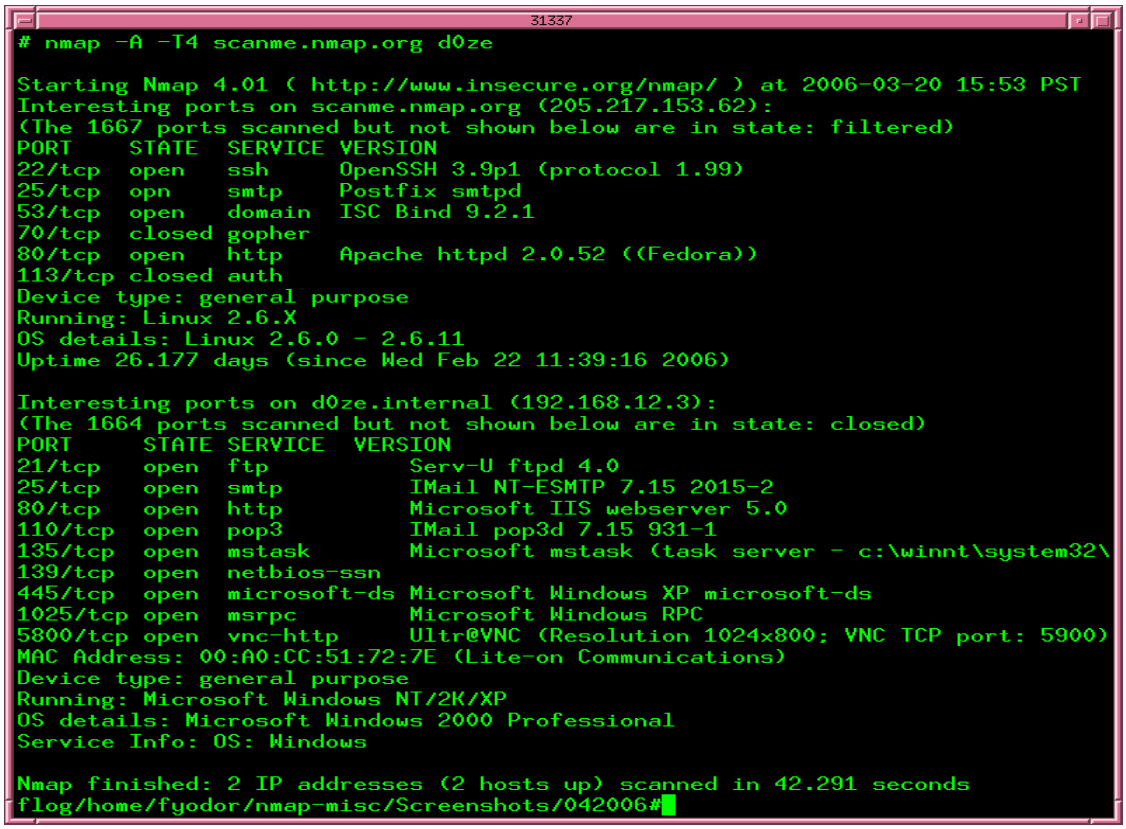
Şekil 6.2. Tcpdump

6.3. Nmap

Güvenlik denetimlerinde kullanılan gelişmiş bir ağ tarayıcıdır. Çok kapsamlı parametrik bir kullanımı vardır. Ağdaki servisler, portlar, cihazların model ve ayrıntıları bu modülle elde edilebilir. IP paket gönderimi ve ping metodu ile testler gerçekleşir.

Örneğin; “#nmap –sP 10.1.1.0/24” komutu verildiğinde 10.1.1 bloğunda bulunan 255 adet IP taranır açık olan bilgisayarlar üzerindeki portların açık ve kapalı durumu hakkında rapor oluşturacaktır. Tarama sonuçları istenilen dosyaya aktarılabilir [7].

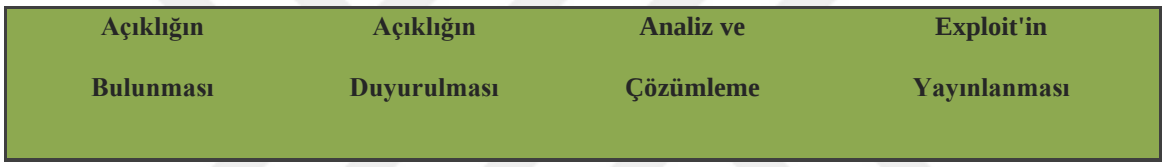
Nmap bir port tarayıcıdır. Her bilgisayar herhangi bir zamanda açık veya kapalı olan 65535 bağlantı noktasına sahiptir. Http veya Ftp gibi bazı servisler varsayılan olarak kendileriyle ilişkilendirilmiş bağlantı noktalarına sahiptir. Http 80 numaralı bağlantı noktasında çalışır. Ftp 21 numaralı bağlantı noktasında çalışır ve böyle devam eder [24].



Şekil 6.3. Nmap

7. SÖMÜRME

Tespit edilen bir açıklığın kullanımını ifade eden yöntem ve araçlara exploit işlemi denir [25]. Amaç güvenlik açıklığının barındırdığı riski pratik olarak göstermek ve çalışan sistemler üzerinde gerçekliğinin doğrulanmasıdır. Exploit'ler tespit edilen bir açıklık üzerinde açık kaynak kodlu yazılımlar kullanılarak küçük programlardan ve yöntemlerden oluşur. Açık kaynak kodlu olmasının avantajı test işleminde art niyetli kişiler tarafından oluşturulmuş zararlı kodların sisteme bulaşma durumu kontrol edilebilir. İlgili açıklıkla ilişkili exploit kodlar analiz edilerek arka tarafta nasıl bir senaryo ile sistemi ele geçiriliyor tespit edilebilir. Farklı sistemlere de uyarlanabilir. Piyasadaki hazır ticari yazılımlar genelde yayınlanmış exploit'ler kendi sistemlerine entegre edilmesi ile tarama kütüphanelerini genişletmektedirler.



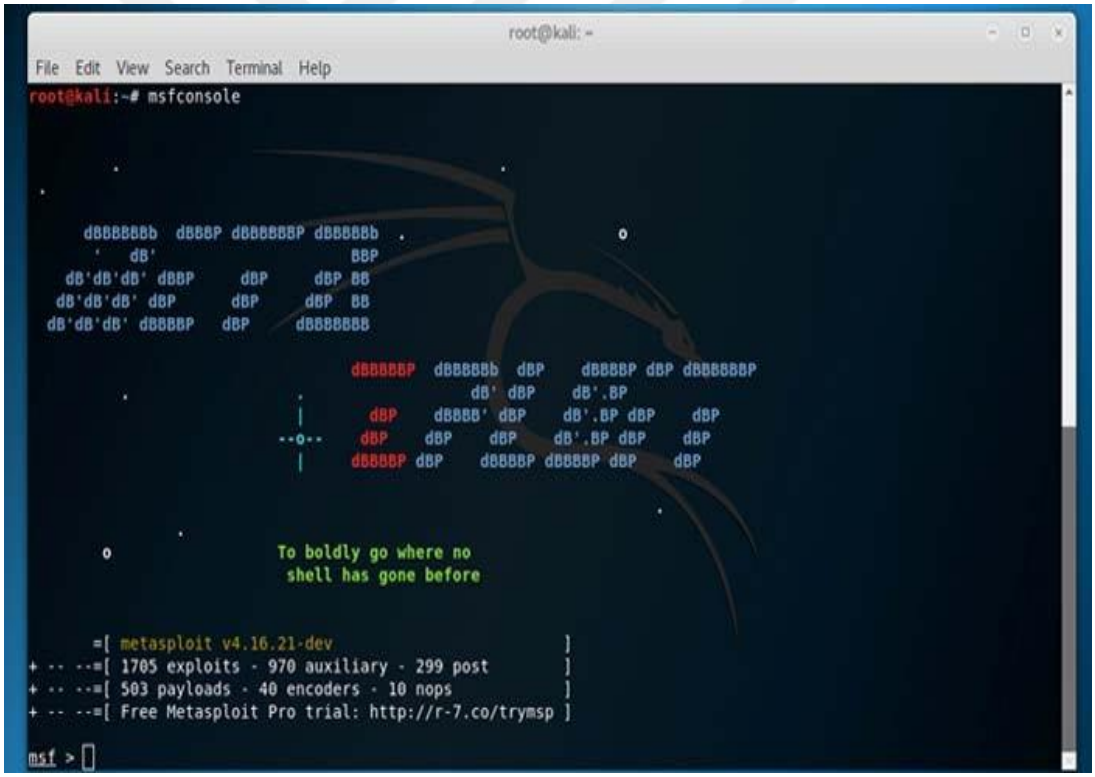
Şekil 7.1. Exploit Oluşturma Evresi

Şekil 7.1'deki süreçte görüleceği üzere bir sistemde açıklık tespit edildiğinde genellikle hemen duyurulur. Bazen açıklığı bulan kişi açıklık tespit edilen ilgili yazılım firması ile doğrudan iletişime geçip açıklığı kapattırabilir. Eğer açıklık duyurulmuşsa derhal kapatma yönünde iyileştirmeler yapılarak yayınlanır. Kullanıcıları bu açıklığı güncelleme veya yayınlanan açıklığa özgü bir yama kurulumu ile kapatmış olur. Exploit'ler işletim sistemi ve uygulama türü gibi pek çok özelliklerine göre ayırt edilir [26].

7.1. Metasploit

Script tabanlı web saldırısı çerçevelerinin çok iyi bilinen bir örneği Metasploit'tir. Farklı işletim sistemlerinde çalışan çeşitli savunmasız sunucuları, hizmetleri ve uygulamaları hedef alan 800 saldırı komut dosyası ve sayımı vardır. Ayrıca, yeni saldırı komut dosyaları oluşturmak için yerleşik modüller sağlar. Açık kaynak olması nedeniyle, metasploit, hackerlar tarafından penetrasyon testi dışındaki amaçlarla, özellikle yasa dışı hackleme yoluyla kolayca elde edilir ve kullanılır [27].

2003 yılında başlatılan Metasploit, Perl'de yazılmış bir ağ güvenlik oyunu olarak başladı, ancak daha sonra Ruby on Rails çerçevesi kullanılarak yeniden yazıldı. Yalnızca ağ taraması ve güvenlik açığı analizi için değil, aynı zamanda ağ istismarlarının geliştirilmesi için de kullanılabilecek bir açık kaynak araçları paketi olarak geliştirilmiştir [28].

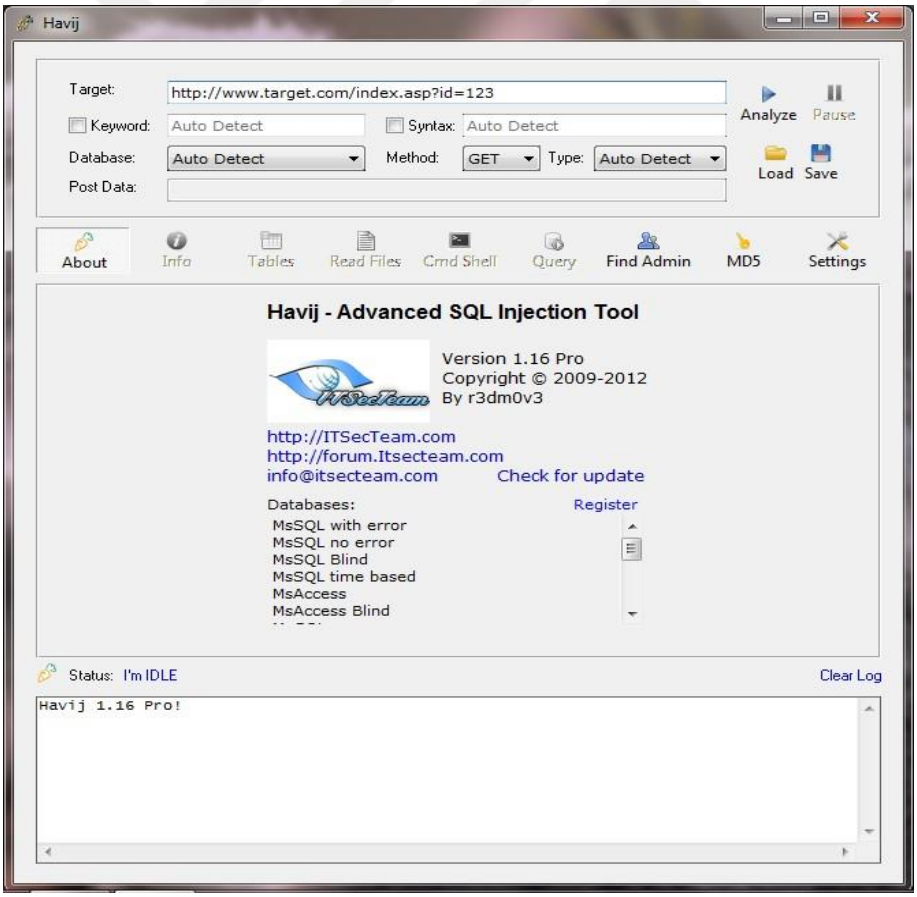


Şekil 7.2. İçindeki Modülleri Listeleyen Ekran İle Metasploit

7.2. Havij

Sql injection, sql ifadelerinin bir giriş bölümüne eklendiği veri temelli uygulamalara saldırı için yapılan kod enjeksiyon yöntemidir. Sql injection, bir uygulamanın yazılımındaki güvenlik açığından yararlanır. Sql injection genellikle web siteleri için saldırı vektörü olarak bilinir, ancak her çeşit sql veritabanına saldırmak için kullanılabilir. Temel fikir, web uygulamasındaki sunucu seviyesini arka uçlara erişim sağlamak için atlamaktır.

Sql injection gerçekleştirmek için kullanılan araç havij'dir. Havij, penetrasyon testi uzmanlarının bir web sitesi sayfasındaki sql injection açıklarını bulup kullanmaları için yardımcı olan otomatik bir sql injection aracıdır. Bu yazılımı kullanarak, bir saldırgan arka uç veritabanı parmak izini gerçekleştirebilir, dbms oturum açma adlarını ve hatta şifre karmalarını alabilir, tablo ve sütunları silebilir, veritabanından veri alabilir, sunucuda sql ifadeleri çalıştırabilir [29].



Şekil 7.3. Havij

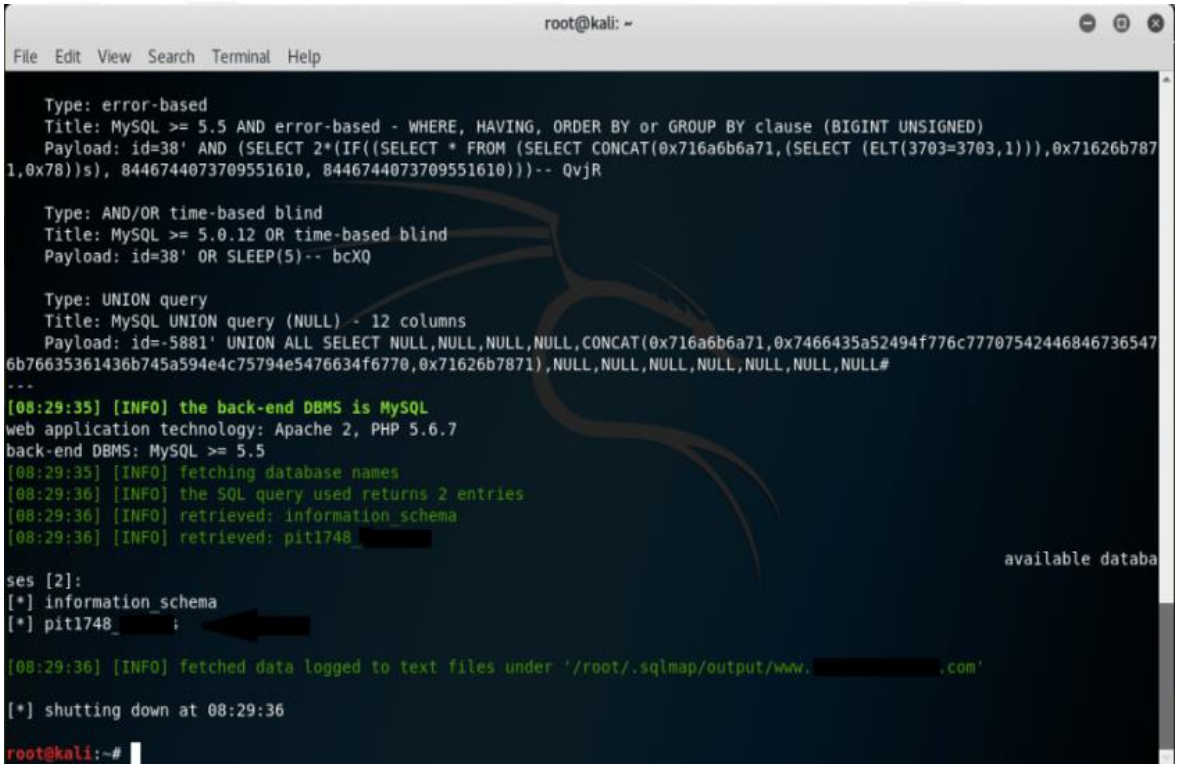
7.3. Sqlmap

Web uygulama ve sunucularında Sql injection tespitini ve ortaya çıkan zafiyetlerin exploit edilmesini otomatik bir şekilde yapan açık kaynak kodlu bir yazılımdır [30].

Bir siteye ait veritabanlarını bulmaya çalışıyorsak:

sqlmap -u http://www.hedef.com/index.php?id=2 –dbs

Buradaki kod şekil 7.4 ‘deki gibi veritabanlarını listeler.



Şekil 7.4. Sqlmap Üzerinde Veritabanı İsimlerini Listeleme

Gelen listede gösterilenler siteye ait veritabanlarıdır [31].

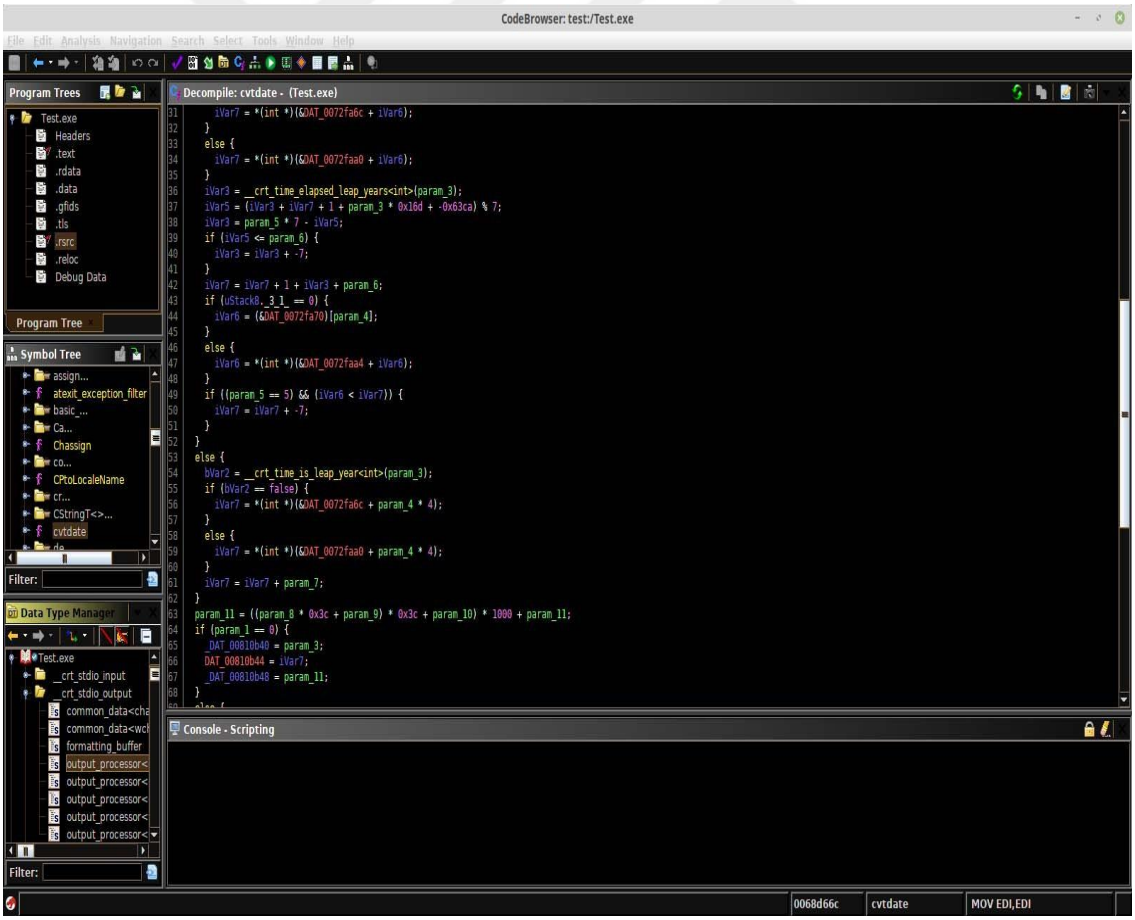
8. TERSİNE MÜHENDİSLİK

Tersine Mühendislik, bir sistemin, cihazın veya yazılımın yapısının, çalışma sisteminin veya işlevinin çıkarımcı bir fikir yürütme analizi ve incelemesi ile keşfedilmesi işlemidir [32].

Başarılı bir tersine mühendislik uygulamasında yazılımın çalışma prensibi çözülerek, kaynak kodu yeniden oluşturulur. Böylece yazılım aynı işlevleri yerine getirir şekilde yapılandırılabilir [33].

8.1. Ghıdra

Grafiksel kullanıcı arayüzüne sahip, java ile oluşturulmuş bir programdır. Linux, iOS, Windows, Android ve Mac gibi tüm işletim sistemleri için hazırlanmış ikili dosyaları inceleme yeteneğine sahiptir [34].

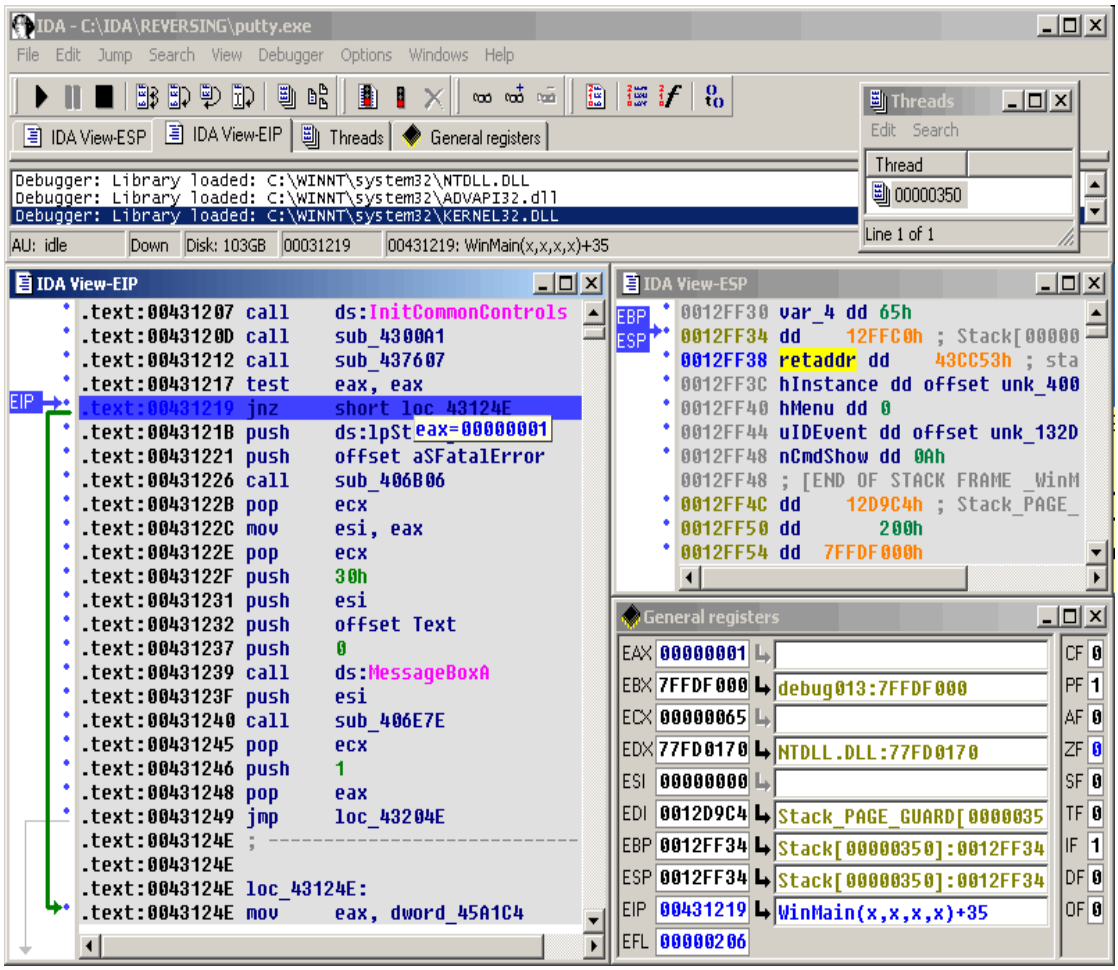


Şekil 8.1. Ghıdra

8.2. Ida Pro

Ida, Windows, Linux veya Mac OS X'te barındırılan ve çok fazla özellik sunan çok işlemcili bir hata ayıklayıcıdır [35].

Bir sökme aracı olarak, IDA pro, kaynak kodun her zaman kullanılamadığı ikili programları araştırır. Ida pro yerel ve uzak hata ayıklayıcı olarak kullanılabilir [36].

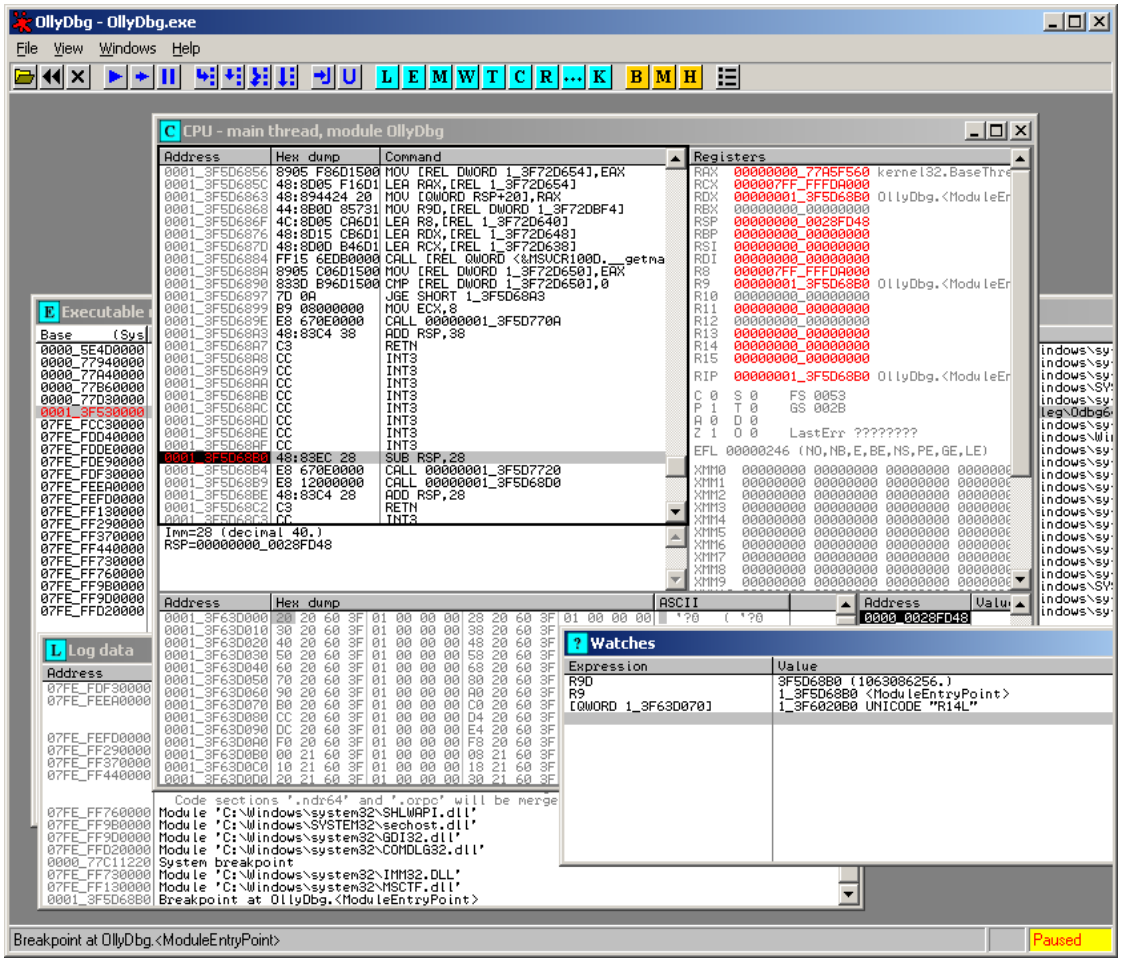


Şekil 8.2. Ida Pro

8.3. Ollydbg

Bir programın nasıl çalıştığını, nerede hangi dosyayı kullandığını, oluşturduğunu, sildiğini anlamanıza yardımcı olur. Bir programın keygenini yazmanıza yardımcı olur [37].

OllyDbg, Microsoft ® Windows ® için 32-bit montajcı düzeyinde analiz hata ayıklayıcısıdır. Kaynağın kullanılamadığı durumlarda özellikle yararlıdır. Ascii ve unıcode karakter dizilerini dinamik olarak tanır [38].



Şekil 8.3. Ollydbg

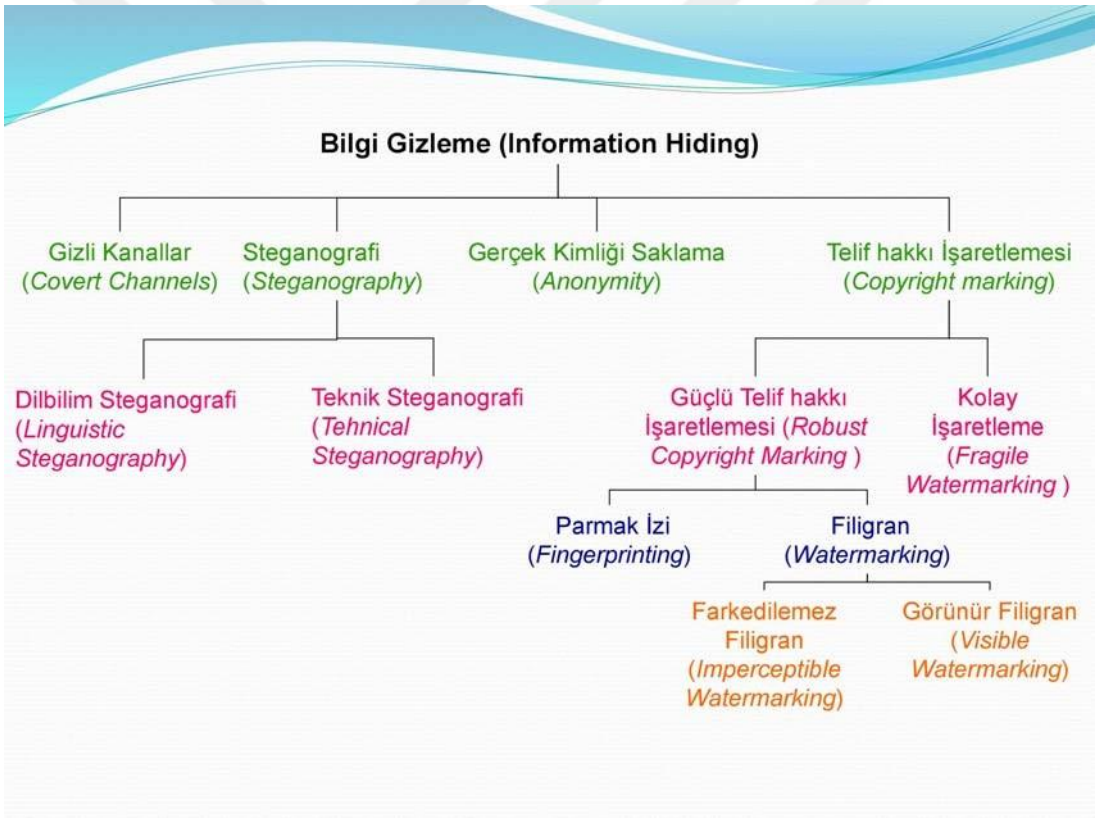
9. BİLGİ GİZLEME

Bir bilginin veya mesajın, masum görünüşlü bir ortam içerisine gizlenerek başka bir yere iletilmesidir.

Encapsulation işlemiyle benzerlik taşır.

Encapsulation ;

Bir modülün gerçekleştirdiği işlemlerin bazılarını, nasıl gerçekleştirdiği bilgisini başkalarından bilinçli olarak gizlemektir. Amaç, içeriği gizlemekten ziyade kontrolsüz erişimi engellemektir.



Şekil 9.1. Bilgi Gizleme [39].

Steganografi, gizlenmiş mesajların tespit edilmesini önleyen şekillerde bilgiyi gizleme sanatıdır. Mesajın varlığını gizleyen çok çeşitli gizli iletişim yöntemlerini içerir. Bu yöntemler görünmez mürekkepleri, mikro noktaları, karakter dizilimlerini, dijital imzaları, gizli kanalları ve yayılı spektrum iletişimini içerir [40].

Bu yöntemle video görüntüleri, ses, sayısal resim üzerinde veri saklanabilir [41].

Çizelge 9.1. Steganograpy ve Kriptografi Arasındaki Farklar [42].

Teknikler	Steganography	Kriptografi
Tanım	Steganograpy Kapak Yazmak Demektir	Kriptografi Gizli Yazı Demektir
Amaç	Bir Mesajın varlığını Gizli Tutmaya Odaklanır	Bir Mesajın İçeriğini Gizli Tutmaya Odaklanır
Anahtar	İsteğe Bağlı	Gerekli
Taşıyıcı	Herhangi Bir Dijital Ortam	Genellikle Metin Tabanlı
Görünürlük	Asla	Her Zaman
Sunulan Güvenlik Hizmetleri	Gizlilik Doğrulama	Gizlilik Kullanılabilirliği, Veri Bütünlüğü
Saldırılar	Saldırgan Steganograpy'nin Steganaliz Olduğunu Tespit Ettiğinde Kırılır	Saldırgan Kriptoanaliz Olarak Bilinen Gizli Mesajı Okuyabilirken Kırılır
Sonuç	Stegho Dosyası	Şifre Metni

9.1. Stegdetect

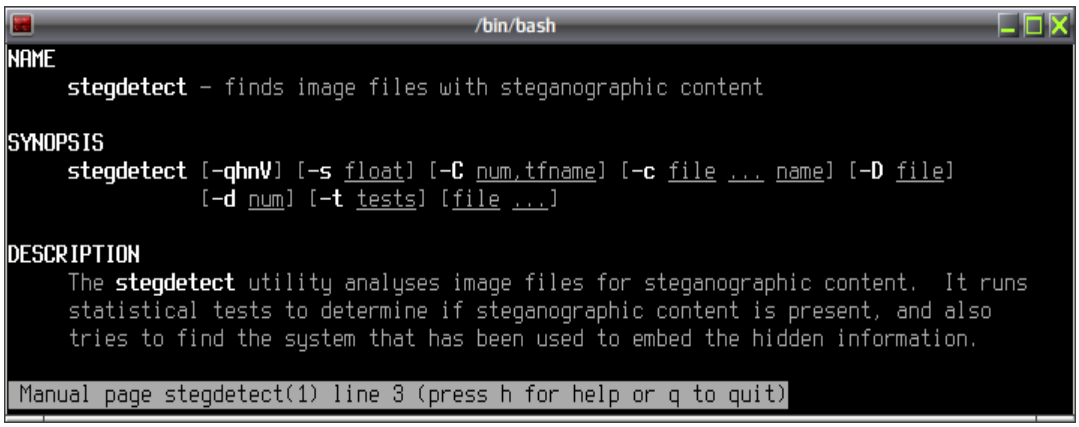
Stegdetect, görüntülerdeki steganografik içeriği tespit etmek için kullanılan otomatik bir araçtır. Stegdetect ve Stegbreak Niels Provos tarafından geliştirilmiştir [43].

Görüntü dosyalarındaki steganographic içeriği analiz eder. Steganografik içeriğin var olup olmadığını belirlemek için istatistiksel testler uygular ve ayrıca gizli bilgileri yerleştirmek için kullanılan sistemi bulmaya çalışır.

-q 'Sadece steganographic olması muhtemel görüntüleri bildirir.

-h 'Sadece DCT histogramını hesaplar. Değerleri görüntülemek için -d seçeneğini kullanın.
.
-n 'Yanlış pozitifleri bastırmak için JPEG başlık bilgilerinin kontrol edilmesini sağlar. Etkinleştirildiğinde, yorum alanları içeren tüm JPEG görüntüler negatif olarak değerlendirilir. JFIF marker 1.1 sürümüyle eşleşmezse, OutGuess kontrolü devre dışı bırakılır.

-V 'Yazılımın sürüm numarasını görüntüler [44].



Şekil 9.2. Stegdetect

9.2. Steghide

Steghide, çeşitli görüntü ve ses dosyalarındaki verileri gizleyebilen bir steganografi programıdır.

Renk açısından, örneklem frekansları değişmez, bu nedenle gömme işlemlerini birinci dereceden istatistiksel testlere karşı dirençli kılar.

Steghide kullanmak için aşağıdaki kütüphanelerin kurulu olması gerekir.

Libmhash ;

Çeşitli karma algoritmalar ve şifreleme anahtarı oluşturma algoritmaları sağlayan bir kütüphane. Steghide, bu kütüphaneye, bir şifreyi kriptografik ve steganografik algoritmalar için girdi olarak kullanılabilecek bir forma dönüştürmesi için ihtiyaç duyar.

Libmcrypt ;

Çok fazla simetrik şifreleme algoritması sağlayan bir kütüphane. Steghide komutunu libmcrypt olmadan derlerseniz, gömmeden önce verileri şifrelemek veya şifreli verileri çıkarmak için (doğru şifreyi bilseniz bile) steghide kullanamazsınız.

Libjpeg ;

JPEG görüntü sıkıştırma uygulayan bir kütüphane. Bu kütüphane olmadan, verileri jpeg dosyalarına gömemez ve jpeg dosyalarından veri çıkaramazsınız.

Zlib ;

Kayıpsız veri sıkıştırma kütüphanesi. Bu kütüphaneyi kurmadan steghide derlerseniz, gömmeden önce verileri sıkıştırmak veya bir stego dosyasından sıkıştırılmış verileri çıkarmak için steghide kullanamazsınız [45].

10. İKİLİ ANALİZ

İkili Kod

İkili kod, doğrudan bir bilgisayar tarafından yorumlanan bir programlama verisinin temel şeklidir. Bir donanım parçası tarafından okunup daha büyük bir bilgisayar programının parçası olarak yürütülebilmesi için sipariş edilen ve yapılandırılmış bir 0 ve 1 dizisinden oluşur. C veya Java gibi yüksek seviyeli dillerde yazılmış kaynak kodunu, bilgisayar programının yürütüldüğü işlemci mimarisine özgü makine koduna çeviren çok aşamalı bir derleme işleminin bir ürünüdür. Bir anlamda, insan tarafından okunabilen kaynak koddan çevrilmiş bilgisayarın doğrudan dilidir.

İkili Analiz

İkili analiz (kod incelemesi), bir uygulamanın kaynak kodunda görünürlük olmadan yalnızca ikili çalıştırılabilir koduyla ilgilenen statik bir analiz şeklidir. Genellikle, veri araçlarını, akışları ve kontrol yollarını çeşitli yollarla modellemeye çalışarak ikiliyi tersine çevirmek için çok adımlı bir yaklaşımdan oluşur. Ardından, tanınan güvenlik açığı kalıplarını tespit etmek ve sonuçları düzeltilebilir düzeltmelerle ayrıntılı güvenlik açığı raporlarında sentezlemek amacıyla türetilmiş modeli analiz etmeye çalışılır.

İkili kod incelemeleri tipik olarak, ikili kodun ayrıştırılması ve sökülmesi ve bilinen güvenlik açığı kalıplarının tanınması yoluyla güvenlik açıklarını keşfederler. Bu, tampon taşması, işlenmemiş hata koşulları, siteler arası komut dosyası çalıştırma (XSS) ve çeşitli enjeksiyon saldırısı vektörleri gibi bazı genel zayıflık türlerini kapsayabilir. Özellikle kötü niyetli kod tespiti ve arka kapılar ve rootkitler gibi düşük seviyeli konular için uygundur. Bu, makine seviyesi talimat setlerinin kendiliğinden ultra düşük seviye analizinin bir sonucudur [46].

Çizelge 10.1. Ascii karakter tablosu [47].

	Binary Code						
A	100 0001	H	100 1000	O	100 1111	V	101 0110
B	100 0010	I	100 1001	P	101 0000	W	101 0111
C	100 0011	J	100 1010	Q	101 0001	X	101 1000
D	100 0100	K	100 1011	R	101 1010	Y	101 1001
E	100 0101	L	100 1100	S	101 0011	Z	101 1010
F	100 0110	M	100 1101	T	101 0100	a	110 0001
G	100 0111	N	100 1110	U	101 0101	b	110 0010

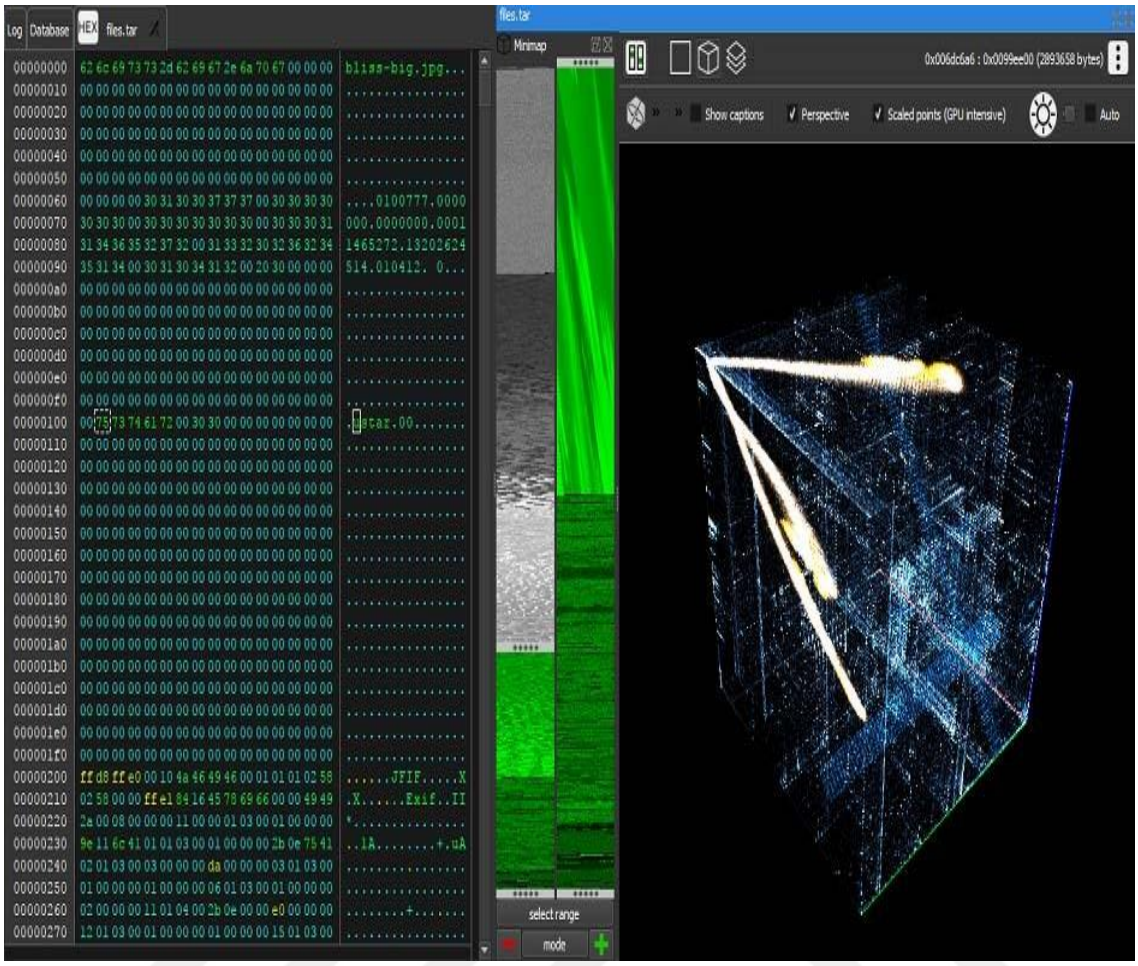
10.1. Veles

Kapsamlı ve oldukça gelişmiş bir veri analizi ve veri görselleştirme aracıdır.

Temel amacı, kullanıcılara gerekli en az çaba ile büyük miktarlarda ikili veride çeşitli ince görselleştirme kalıplarını belirlemelerine yardımcı olmaktır.

Diyagram, Katmanlı Diyagram ve Trigram olmak üzere üç tür görselleştirme modu vardır [48].

Görselleştirmeler tamamen ikili verilerin istatiksel gösterimleridir [49].



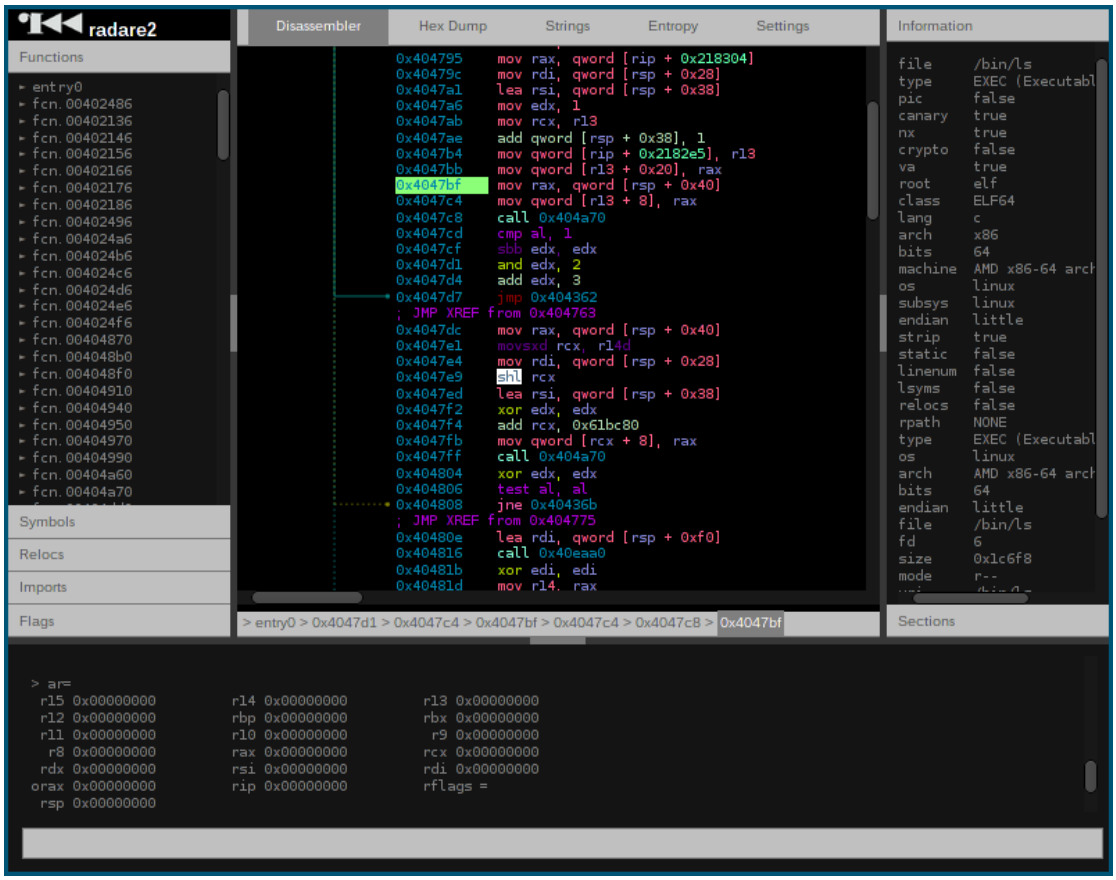
Şekil 10.1. Veles

10.2. Radare2

Kötü amaçlı yazılım, veya başka türdeki ikili dosyaları analiz etmek için kullanılabilir. Birçok farklı dosya türünde tersine mühendislik uygulamak için popüler bir çerçevedir. Dosya sistemlerinde adli bilişimde de kullanılabilir ve veri oymacılığı yapabilir [50].

Git sürümünü değilde başka bir makine için ikili dosyaları kurmak istiyorsanız (Windows, OS X, iOS, vb.)

https://www.radare.org/r/down.html [51].



Şekil 10.2. Radare2

11. TARTIŞMA VE SONUÇ

Her geçen gün değişen ve ilerleyen bilişim teknolojileri inanılmaz bir hızda toplumu, yaşam kültürünü ve alışkanlıklarımızı değiştirmektedir. Bu değişim siber güvenlik açısından daha da önemli hale gelmektedir. Siber zafiyetler her geçen gün daha da değişip ilerledikçe bu sistemleri korumak gittikçe önem kazanmaktadır. Bu önlemler çoğu zaman saldırıdan sonra sistemi veya kurumu korumaya çalışsa da ancak belli bir hasar aldıktan sonra düzeltilebilmektedir. Oysa saldırıdan önce sisteme yapılacak bir tatbikat sistemin zafiyetlerini, güvenlik açıklıklarını ve olası davranışlarını inceleyebilecektir. Bu çalışma, toplumda siber güvenlik hakkında daha fazla bilgi ve yeteneğe sahip olmaya gereksinim duyan herkese katkı sağlamayı amaçlamıştır. Çalışmanın en önemli çıktısı, siber güvenlik ile ilgili özellikle teknik konulardaki Türkçe kaynak sıkıntısına ithafen referans niteliğinde kaynak sağlamaktır. Bu amaç kapsamında, Windows ve Linux tabanlı sistemlerde savunma, saldırı, bilgi toplama ve analiz çalışmalarında yardımcı olması açısından bilişim uzmanlarının ilgili bilgilere hızlı erişebilmesi adına bir referans modeli tasarlanmıştır. Özgün bir çalışma olarak bu bilgiler zihin haritalama yöntemi ile hiyerarşik olarak sınıflandırılarak birbirleriyle ilişkili olarak sunulmuştur.

Siber güvenlik alanındaki farkındalığın artması genel bir bakış açısı kazandırması için yapılan bu çalışmada, siber güvenlik tatbikatı ve simülasyonlarında kullanılan programlar incelenmiştir. Ayrıca, konu uzmanlarına farklı bir bakış açısı kazandırması ve gerekli ortam ve materyallerin ne olduğu hakkında fikir veren bu çalışmada siber güvenlik tatbikatlarının ne olduğu, hangi aşamalardan geçtiği, alt parametrelerinin benzerlik ve farklılıklarının neler olduğu ortaya çıkarıldı. Her aşamanın birbirleriyle ilişkili olduğu kompleks bir senaryo dahilinde yada gerçek bir savaş ortamında olması gerekli süreçleri de ortaya koydu.

KAYNAKLAR

[1] Erişim: 24 Mayıs 2019, bilgem.tubitak.gov.tr/tr/urunler/sibermeydan-ctf-siber-guvenlik-simulasyon-ve-yarisma-ortami.

[2] **Şeker, E.** (2017) " Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:3, No:2, S:33-41.

[3] Erişim: 24 Mayıs 2019, https://home.cern/sciense/computing/birth-web.

[4] Erişim: 27 Mayıs 2019, http://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/ internet'in-tarihçesi.

[5] **Baykara, M., Daş, R., Karadoğan, İ.** (2013) Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. 1st International Symposium on Digital Forensics and Security (ISDFS'13), Elazığ, Turkey.

[6] **Eken, H.** Mobil ve Web Uygulamalarının Yazılım Güvenliği. E-Devlet ve Bilgi Toplumu Direktörlüğü, TÜRKSAT AŞ, Ankara.

[7] **Şahinaslan, H.** (2013) " Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma' (Doktora Tezi), Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı.

[8] **Weinberg, H., Gökce, K. G. Şahinaslan, E., Dincel, S.** (2014) "Mobil Yaşamda Siber Güvenlik Yaklaşımı' 7th International Conference on Information Security And Cryptology-İstanbul.

[9] **Termux** (t.y.). Erişim: 20 Mayıs 2019, https://skbilisim.com/post/termux- nedir-ne-ise-yarar.

[10] Erişim: 21 Mayıs 2019, https://www.webtekno.com/mobil/android-icin-en-iyi hack-uygulamalari-h15085.html.

[11] Erişim: 20 Mayıs 2019, https://play.google.com/store/apps/details?id=berserker.android.apps.sshdroid&hl=tr.

[12] Erişim: 20 Mayıs 2019, https://play.google.com/store/apps/details?id= com.overlook.android.fing

[13] **Bilgi güvenliği** (t.y.). Erişim: 23 Mayıs 2019, http://www.pki.iam.metu.edu.tr/yazi-makale/atillaB_01.pdf

[14] **Fındık, Oğuz**. (2004) " Şifrelemede Kaotik Sistemin Kullanılması' (Yüksek Lisans Tezi), Selçuk Üniversitesi.

[15] Erişim: 23 Mayıs 2019, http://www.temizkod.com/kriptoloji-nedir/

[16] **Oğuz, R.** (2018) "Adli Bilişimde İnceleme Süreçleri ' (Yüksek Lisans Tezi), Ankara Üniversitesi Sağlık Bilimleri Enstitüsü.

[17] **Özbek, M.** (2013) " Adli Bilişimde Delillerin Toplanması ve İncelenmesi ' (Yüksek Lisans Tezi), İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü.

[18] Erişim: 07 Şubat 2020, https://www.turkhackteam.org/network/1344-network-nedir-nasil-kurulur.html

[19] **Erdem, O. Ayhan.** (2014) "Bilgisayar Ağları ve Açık Sistem Mimarisi '.

[20] **Ou, X., Govindavajhala, S, AW Appel** (2005) – USENIX güvenlik sempozyumu.

[21] Erişim: 07 Mayıs 2019, http://www.ktu.edu.tr/dosyalar/bilgisayar_4ccd2.pdf

[22] Erişim: 09 Mayıs 2019, http://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/06/tcp dump-kullanımı.

[23] **Önal, H.** (2010)" Tcpdump İle Trafik Analizi (Sniffing) '.

[24] **Shaw, D.** (2015) " Nmap Essentials '.

[25] **Özavcı, F.** (2013) "Metasploit Framework Giriş Seviyesi Denetmen Rehberi', GamaSEC Bilgi Güvenliği Denetim ve Danışmanlık, S.1-251, Ankara.

[26] **Offensive Security,** (2013) " The Exploit Database ', A Great Resource For Penetration Testers, Vulnerability Researchers, and Security Addicts Alike, CVE and Archive, http://www.exploit- db.com/, and http:// 1337day.com/.

[27] **Gupta, H., Kumar, R.** (2015) "Protection Against Penetration Attacks Using Metasploit' 2015 4th International Conference on Reliability Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions).

[28] **Bradbury, D.** (2019) "Hands-on with Metasploit Express' https://www.scie ncedirect.com/science/article/pii/S1353485810700921

[29] **Nagpal, B., Singh, N., Chauhan, N., Panesar, A**." Tool Based İmplementati on Of Sql İnjection For Penetration Testing' International Conference On Computing, Communication & Automation.

[30] Erişim: 05 Mayıs 2019, https://www.netsparker.com.tr/blog/web-guvenligi/ileri-seviye-sglmap-kullanimi/

[31] Erişim: 07 Mayıs 2019, https://aridoshika.com/kali-linux-sqlmap-kullanimi/

[32] Erişim: 07 Mayıs 2019, https:// www.tech-worm.com / tersine-muhendislik- nedir-tersine-muhendislik-turleri-uygulamalari/

[33] Erişim: 27 Mayıs 2019, https://wmaraci.com/nedir/tersine-muhendislik

[34] Erişim: 13 Mayıs 2019, http://ozdenercin.com/2019/03/15/nsain-tersine-muhendislik-yazilimi-ghidra/

[35] Erişim: 15 Mayıs 2019, https://www.hex-rays.com/products/ida/index.shtml

[36] Erişim: 07 Nisan 2019, https://www.hex-rays.com/products/ida/ida- executive.pdf

[37] **Turkhackteam Tersine Mühendislik Kulubü,** Ollybdg Kullanımı https://www.turkhackteam.org/tersine-muhendislik/1669053-ollydbg kullanimi-tersine-muhendislik-kulubu.html

[38] Erişim: 11 Nisan 2019, http://www.ollydbg.de/

[39] Erişim: 27 Nisan 2019, https://slideplayer.biz.tr/slide/2866574/ "İnformation Hiding Technigues' Anonymous.

[40] **Johnson, Neil F., Jajodia, S.** (1988) "Exploring steganography: Seeing the unseen' Computer (Volume: 31 , Issue: 2 , Feb. 1998).

[41] **Şahin, A., Buluş, E., Sakallı, M.Tolga** (2006) " 24- Bit Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme' Trakya Üniversitesi.

[42] **Rahmani, M., Arora, KC., Pal, N.** (2014) "A Crypto-Steganography: A Survey' (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014.

[43] Erişim: 27 Nisan 2019, https://github.com/abeluck/stegdetect

[44] Erişim: 15 Mayıs 2019, https://linux.die.net/man/1/stegdetect

[45] Erişim: 22 Mayıs 2019, http://steghide.sourceforge.net/

[46] Erişim: 22 Mayıs 2019, https://www.synopsys.com/software-integrity/resources/knowledge-database/binary-code.html

[47] Vikipedi Erişim: 26 Mayıs 2019, http://e-wiki.org/tr/images/Ascii_karakter_tablosu

[48] Erişim: 12 Mayıs 2019, https://www.softpedia.com/get/Programming/Other-Programming-Files/Veles.shtml

[49] Erişim: 16 Mayıs 2019, https://codisec.com/binary-visualization-explained/

[50] Erişim: 14 Mayıs 2019, https://linuxsecurity.expert/tools/radare2/

[51] Erişim: 19 Mayıs 2019, https://www.megabeets.net/reversing-a-self-modifying-binary-with-radare2/

ÖZGEÇMİŞ

Ad Soyad : GÖKHAN ALGAÇ

Doğum Yeri ve Tarihi : Malatya 02/07/1988

E-posta : gkhnalgac@gmail.com

Lisans : İnönü Üniversitesi Fen Bilgisi Öğr. Bölümü (2011-2015)