SteelMountain

Enumeration

Nmap

```
PORT      STATE SERVICE           REASON          VERSION
80/tcp    open  http              syn-ack ttl 125 Microsoft IIS httpd 8.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/8.5
|_http-title: Site doesn't have a title (text/html).
135/tcp   open  msrpc             syn-ack ttl 125 Microsoft Windows RPC
139/tcp   open  netbios-ssn       syn-ack ttl 125 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds      syn-ack ttl 125 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server? syn-ack ttl 125
| ssl-cert: Subject: commonName=steelmountain
| Issuer: commonName=steelmountain
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2021-07-30T09:59:04
| Not valid after:  2022-01-29T09:59:04
| MD5:   2723 f795 ab28 b2ab e460 ab47 5f5a 27a5
| SHA-1: 83a2 028a e1ae 33f2 209f 68cf b196 a669 0a39 105b
| -----BEGIN CERTIFICATE-----
| MIIC3jCCAcagAwIBAgIQITwoVs9AfINOMqQSPY5d6DANBgkqhkiG9w0BAQUFADAY
| MRYwFAYDVQQDEw1zdGVlbG1vdW50YWluMB4XDTIxMDczMDA5NTkwNFoXDTIyMDEy
| OTA5NTkwNFowGDEWMBQGA1UEAxMNc3RlZWxtb3VudGFpbjCCASIwDQYJKoZIhvcN
| AQEBBQADggEPADCCAQoCggEBAJQrylUfu++wEcXo7FWTrTSaBVuRizndTLbU+Nlj
| h1XeYZ77RPODlpxvTFsTUoa0PzUHVBYPEXZUyH9TOUcmHAmVP3u1cnUsm6uQ8pCp
| /LsW50IVSiNVlKGDBNAOlQTXMUCMXu+pZ4O06mysbgai2ouVBxAp+07Agw3QcC15
| va1iVNe/oiVSUzfgi29GcVuhAMSmF4/tkWQ7zumN8PZc7+eUaQVwWUiKsf9/Z488
| kIBGGktPBW7xZuA5/f83L+4Dyw+nxJcG16PSQglhdbScf/v/rpiyySqzuMyZxlDh
| 8BXZFjYqnDAa+89yWMFJWDU919dOyBwBCfNdXXHVc/Wc6e0CAwEAAaMkMCIwEwYD
| VR0lBAwwCgYIKwYBBQUHAwEwCwYDVR0PBAQDAgQwMA0GCSqGSIb3DQEBBQUAA4IB
| AQBhOd7Cn+9SjZ6dXQHdpgvKahVRwh2R1dwzkF3uG3upQVRxMOrcmYY5QOKWa/xb
| uvGddHuUCa16CmMuOPpoNvZVHuacWzQV3R58VYcE77WSl8+xh6JE/263UXBtqiwC
| 6YOlO/3Lx4bS5qZzca5owh+m6f0RhFon+xy/I90+utmPasW5be+ZG+ddWNtYN2mb
| jJ8T2PHkEiMicUKs9/CxeKLGrTfZ0Fypv4C++YxPxftc2Bg9jHQATqNcis6dAwDM
| zV0SSpLltz5gDQ/wQNxbds9hk3/Y5t4SFp1Fnyj+GoRPA26gSSMFhxreHfRiMqv3
| eKKZ+4PxexnZ+EgM7bkj24lM
|_-----END CERTIFICATE-----
|_ssl-date: 2021-07-31T10:02:19+00:00; +36s from scanner time.
5985/tcp  open  http              syn-ack ttl 125 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
8080/tcp  open  http              syn-ack ttl 125 HttpFileServer httpd 2.3
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: HFS 2.3
|_http-title: HFS /
47001/tcp open  http              syn-ack ttl 125 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc             syn-ack ttl 125 Microsoft Windows RPC
```

```
49153/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49154/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49155/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49157/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49162/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
49164/tcp open  msrpc         syn-ack ttl 125 Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Microsoft Windows Server 2012 (96%), Microsoft Windows Server 2012 R2 (96%), Microsoft
Windows Server 2012 R2 Update 1 (96%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1
(96%), Microsoft Windows Vista SP1 (96%), Microsoft Windows Server 2012 or Server 2012 R2 (95%), Microsoft
Windows 7 or Windows Server 2008 R2 (94%), Microsoft Windows Server 2008 SP2 Datacenter Version (93%),
Microsoft Windows Server 2008 R2 (93%), Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (93%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.91%E=4%D=7/31%OT=80%CT=%CU=44611%PV=Y%DS=4%DC=T%G=N%TM=61051F88%P=x86_64-pc-
linux-gnu)
SEQ(SP=103%GCD=1%ISR=10E%CI=I%II=I%TS=7)
OPS(O1=M505NW8ST11%O2=M505NW8ST11%O3=M505NW8NNT11%O4=M505NW8ST11%O5=M505NW8ST11%O6=M505
WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)
ECN(R=Y%DF=Y%T=80%W=2000%O=M505NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)
T3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)
T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=80%CD=Z)

Uptime guess: 0.003 days (since Sat Jul 31 05:57:58 2021)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 35s, deviation: 0s, median: 35s
| nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user: <unknown>, NetBIOS MAC: 02:b7:2b:68:64:95 (unknown)
| Names:
|   STEELMOUNTAIN<00>    Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   STEELMOUNTAIN<20>    Flags: <unique><active>
| Statistics:
|   02 b7 2b 68 64 95 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 47918/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 50505/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 29382/udp): CLEAN (Failed to receive data)
|   Check 4 (port 49419/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-07-31T10:02:08
|_  start_date: 2021-07-31T09:58:55
```

```
TRACEROUTE (using port 445/tcp)
HOP RTT       ADDRESS
1   193.03 ms 10.4.0.1
2   ... 3
4   457.21 ms 10.10.70.250

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
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 90.65 seconds
           Raw packets sent: 66 (4.308KB) | Rcvd: 389 (167.358KB)
```

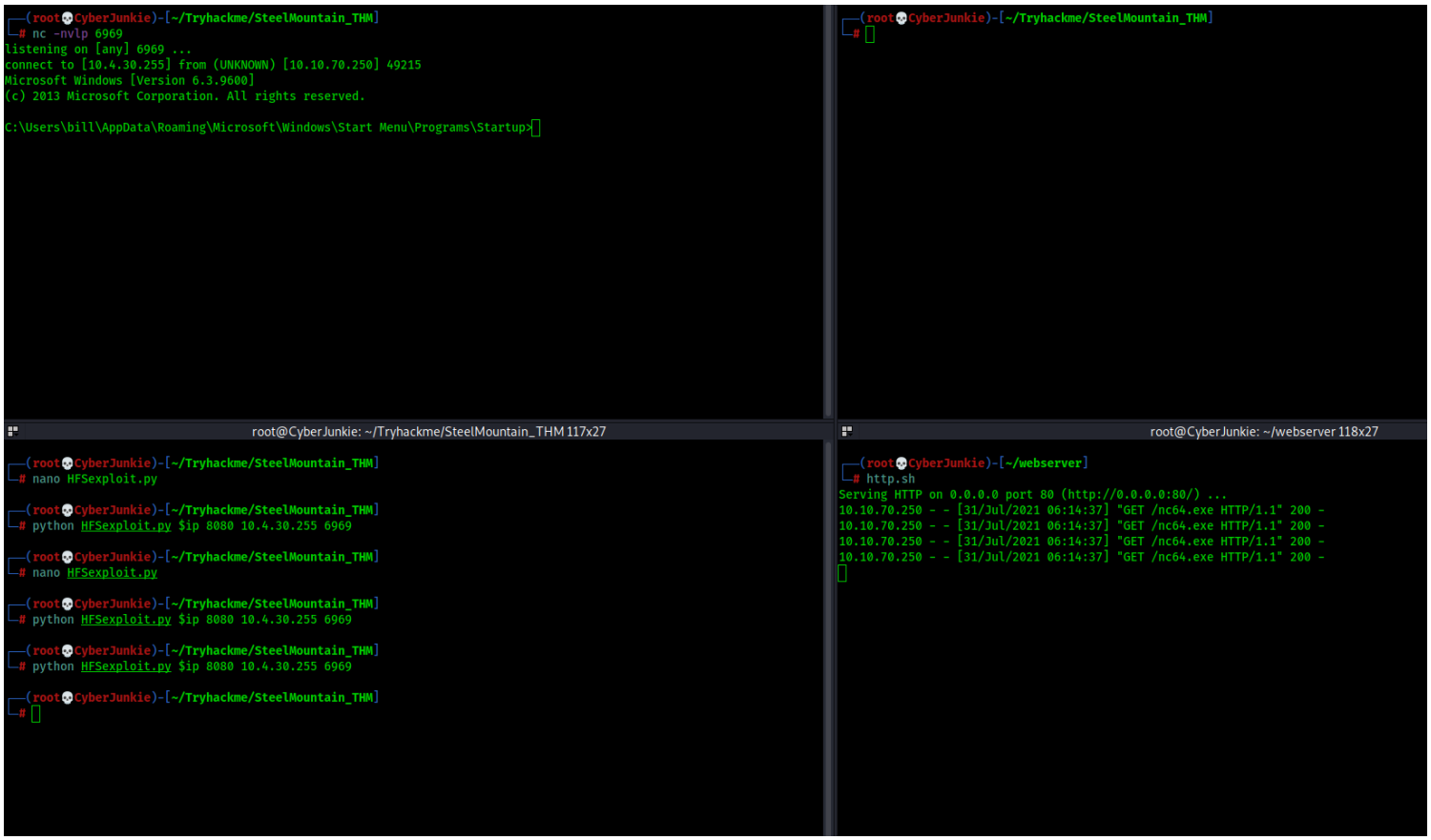
POC

Port 8080 has http file server running which is vulnerable to a rce (CVE-2014-6278)

Exploitation

we use the exploit now to gain a shell

i used a exploit from github and followed the instructions and got a shell back



#

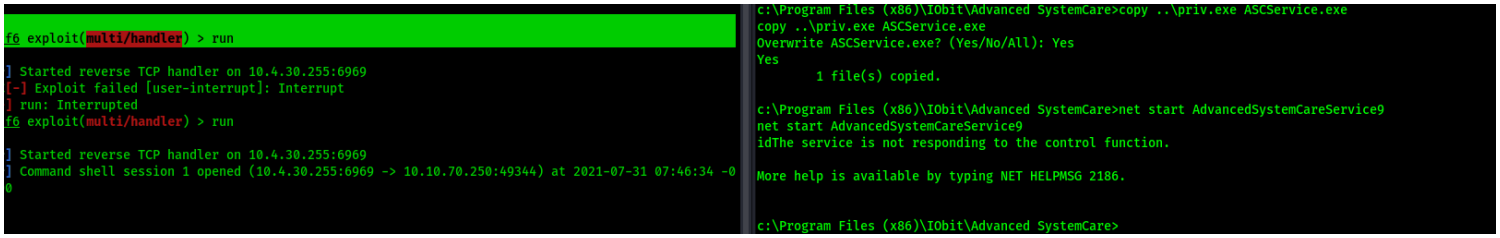
PostExploitation

Got the user flag in bill user desktop

We run powerup and now we see that we have certain kind of red flags here. One is unquoted service escalations and that too of a not so common executable

so we will try to hijack this

we gwt admin shell by creating a malicious payload from msfvenom



we get root flag

Loot

C

Credentials

Flags

User Flag

b04763b6fcf51fcd7c13abc7db4fd365

Root Flag

9af5f314f57607c00fd09803a587db80