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.

A computer screen with white text

Description automatically generated

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.

A screen shot of a computer program

Description automatically generated

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.

A screen shot of a computer

Description automatically generated

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.

A screenshot of a computer

Description automatically generated

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.

A screenshot of a computer

Description automatically generated

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.

1. **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.

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

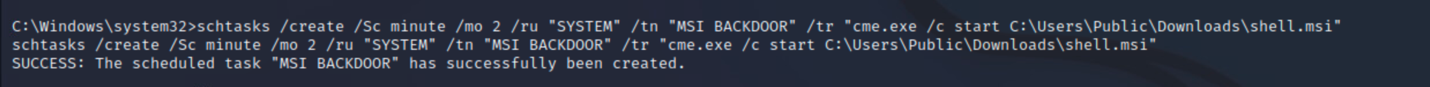
(10 points)

A computer screen shot of a computer code

Description automatically generated

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

(10 points)



1. **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.

1. **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.   
A screenshot of a computer

Description automatically generated

1. **Use Hashcat to crack NTLM password hashes. Submit a screenshot of the output**

(10 points)

A screen shot of a computer

Description automatically generated

1. **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)

A computer screen shot of a computer

Description automatically generated

1. **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

1. **Submit a screenshot of the following command in your shell:**

**whoami && dir “C:\Program Files”**

(10 points)

A screenshot of a computer

Description automatically generated