Skills Assessment

To keep you sharp, your SOC manager has assigned you the task of analyzing older attack logs and providing answers to specific questions.

Navigate to the bottom of this section and click on `Click here to spawn the target system!`

RDP to `[Target IP]` using the provided credentials, examine the logs located in the `C:\Logs\*` directories, and answer the questions below.

Skills Assessment

```
MisaelMacias@htb[/htb]$ xfreerdp /u:Administrator /p:'HTB_@cad3my_lab_W1n10_r00t!@0' /v:[Targ
```

VPN Servers

Warning: Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK — 161ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

? Go to Questions

Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection File

Target(s): Click here to spawn the target system!

RDP to with user "Administrator" and password "HTB_@cad3my_lab_W1n10_r00t!@0"

+3 By examining the logs located in the "C:\Logs\DLLHijack" directory, determine the process responsible for executing a DLL hijacking attack. Enter the process name as your answer. Answer format: _.exe

Dism.exe

Submit

RDP to with user "Administrator" and password "HTB_@cad3my_lab_W1n10_r00t!@0"

+2 By examining the logs located in the "C:\Logs\PowershellExec" directory, determine the process that executed unmanaged PowerShell code. Enter the process name as your answer. Answer format: _.exe

Calculator.exe

Submit

RDP to with user "Administrator" and password "HTB_@cad3my_lab_W1n10_r00t!@0"

+3 By examining the logs located in the "C:\Logs\PowershellExec" directory, determine the process that injected into the process that executed unmanaged PowerShell code. Enter the process name as your answer. Answer format: _.exe

rundll32.exe

Submit

RDP to with user "Administrator" and password "HTB_@cad3my_lab_W1n10_r00t!@0"

+2 By examining the logs located in the "C:\Logs\Dump" directory, determine the process that performed an LSASS dump. Enter the process name as your answer. Answer format: _.exe

Processhacker.exe

Submit

RDP to with user "Administrator" and password "HTB_@cad3my_lab_W1n10_r00t!@0"

+1 By examining the logs located in the "C:\Logs\Dump" directory, determine if an ill-intended login took place after the LSASS dump. Answer format: Yes or No

No

Submit

RDP to with user "Administrator" and password "HTB_@cad3my_lab_W1n10_r00t!@0"

+2 By examining the logs located in the "C:\Logs\StrangePPID" directory, determine a process that was used to temporarily execute code based on a strange parent-child relationship. Enter the process name as your answer. Answer format: _.exe

werfault.exe

Submit

Previous

Finish