CS 4177 Software Vulnerabilities

**Software Reverse Engineering**

**Analyzing Exploits Through Powershell-Empire**

Developed by Gilbert G., Fernando R., Jose S., Hector D.

Tool: Empire PowerShell

Virtual Machine: Kali Linux & Windows 7 Professional

-----------------

***FALLEN EMPIRE: “Using Tools on A Post Exploited Machine”​***

This exercise can be completed with many other tools; however, this exercise is meant to familiarize yourself with the open-source tool called Empire. Empire was released in 2015 with the sole purpose to create an environment similar to what hackers use, this is referred to an attack framework. This ranges from using a PowerShell to escalate privileges, create/modify system processes, and exfiltrate data via the network. The ultimate objective is to learn how a particular virus or can take over a network and communicate across a network.

Mission Briefing – You’re in IT in tasked to save medical records from threat

A computer on your network has been exploited! You received an email from an anonymous party detailing some private information regarding patients at the hospital you work for. After analyzing the information and concluded that the network has been breached, you have been assigned to a task force to simulate a “worst case scenario” in terms of what information may have been taken from these hackers that hasn’t been revealed to you already. Using the Empire PowerShell Tool, you will begin exploiting a simulated version of the system.

A diagram of a computer

Description automatically generated

Step 0: First Time Setup – (Kali Linux with Empire)

1. Start by downloading Virtual Box, choose the one best for your system.

* <https://www.virtualbox.org/wiki/Downloads>
* NOTE: Make sure you select the 32 or 64-bit version, depending on your CPU.

A screenshot of a computer

Description automatically generated

1. Then Download the Kali-Linux Distro for Virtual Box.

* <https://www.kali.org/get-kali/#kali-virtual-machines>

1. Extract the Downloaded VM.

A yellow folders with a zipper

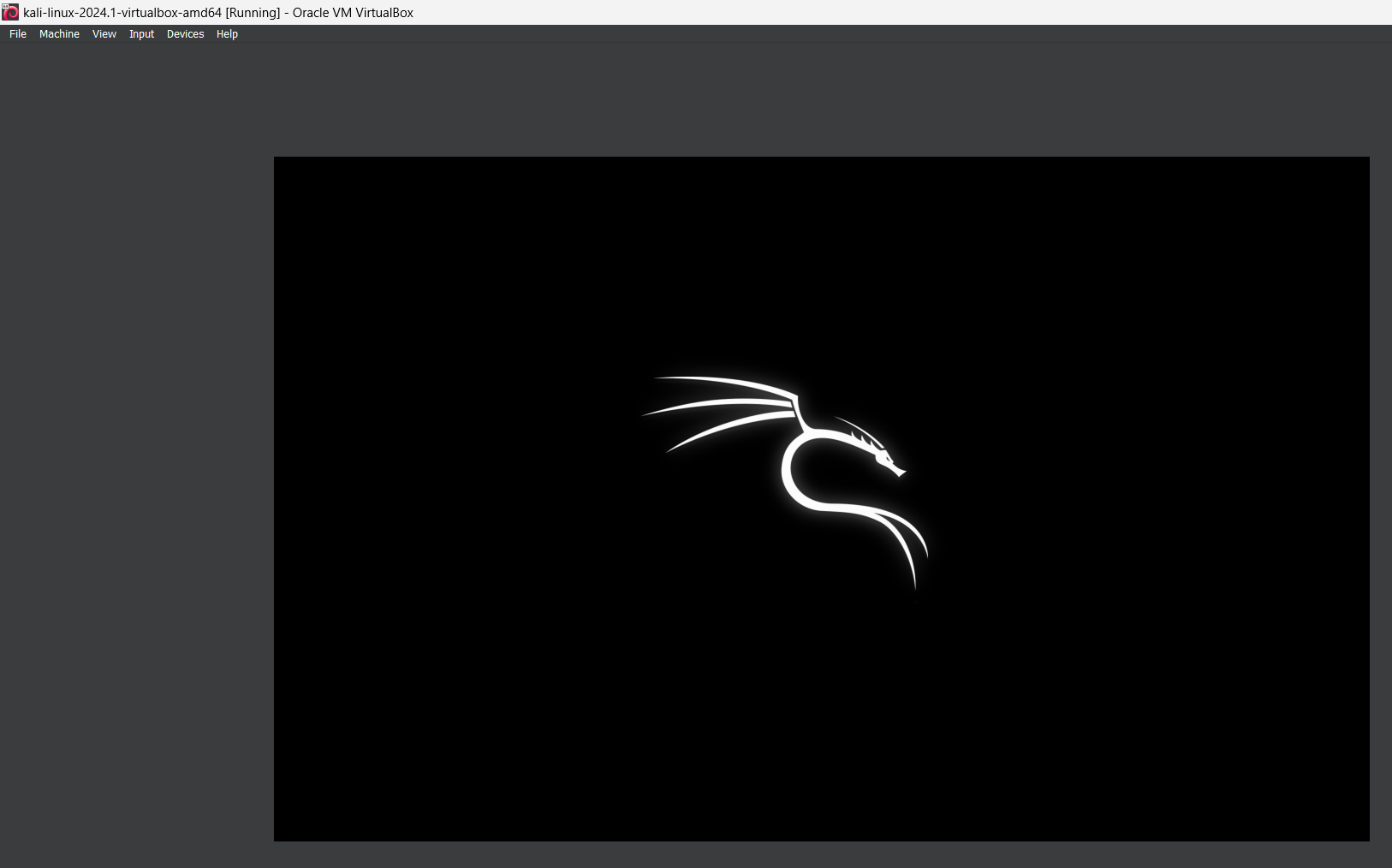
Description automatically generated

1. Install the virtual box. (It will count up to 100%)

A screenshot of a computer

Description automatically generated

1. Now, Start the virtual box, if you see this it is correct!



1. You may now Log in to the system.
   1. Username: kali
   2. Password: kali
2. After logging in, you will now be in the desktop of Kali-Linux! We can finally begin to work through the project, after a few more installs of our tools.  
   A computer screen shot of a logo

   Description automatically generated
3. Open a terminal, then type the following command so we can update kali.

sudo apt update && sudo apt upgrade -y

* + Note: This may take a while. (About 15 minutes)

A screen shot of a computer program

Description automatically generated

1. Now that kali is updated, we can download Empire.

git clone https://github.com/BC-SECURITY/EMPIRE.git



1. Now we have Empire ready to go! Now we can setup the windows Machine we will be exploiting!

Step 0: First Time Setup – (Windows 7 Professional)

1. Download This Windows 7 Professional .ISO file from this link.

<https://archive.org/details/20230422_20230422_1429>

1. Set it up through virtual box, allocating 4 gigs of ram and 32 gigs of storage.

A screenshot of a computer

Description automatically generated

1. Allow windows to fully install! (It will restart, just don’t click any keys and let it do its thing)
2. Set up username and password.
   1. On Setup machine, it is:
   2. Usename: Nurse-Judee
   3. Password: abc123

A screenshot of a computer screen

Description automatically generated

1. You will now have a VM with the targeted machine. Drag the files we gave for setup into “Judee’s” documents folder, so we can steal them later.

A screenshot of a computer

Description automatically generated

1. The Windows machine will now be ready. We modified the simulation to feel more “real,” as seen below.
   1. We set a new wallpaper and added sticky notes.

A screenshot of a computer

Description automatically generated

The windows machine now just needs to be exploited, which we will do via the Kali Linux Machine. Let’s go back to it!

Step 1: Set Up EMPIRE to Hack Judee’s PC– (Kali Linux)

1. Open up the Kali\_Linux Virutal Box.
2. Open 2 terminals, one will be the client, and one will be our server.
3. Let’s start with the server first:

sudo powershell-empire server

A screenshot of a computer screen

Description automatically generated

1. Now start client in new terminal tab:

sudo powershell-empire client

A computer screen shot of a map

Description automatically generated

Check to make sure we have a listener already.  
A screenshot of a computer

Description automatically generated

Now that we have it setup, just specify the port.

A screenshot of a computer

Description automatically generated

Now setup the stager so we can get the command to control Judee’s Machine.

A screenshot of a computer

Description automatically generated

Now use the listener on http with port 8805, then execution gives us what we need to run on Judee's machine to take control!  
A screenshot of a computer screen

Description automatically generated

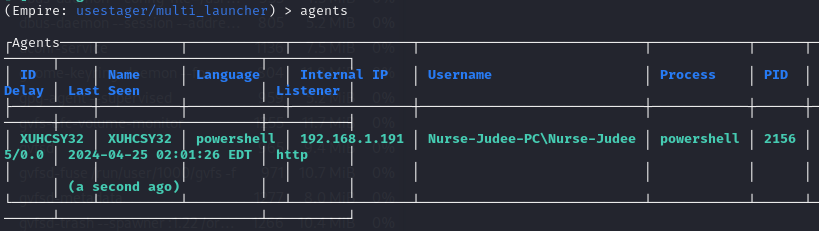
Now back to the Windows 7 Machine, Run it via powershell to take control! A screenshot of a computer screen

Description automatically generated

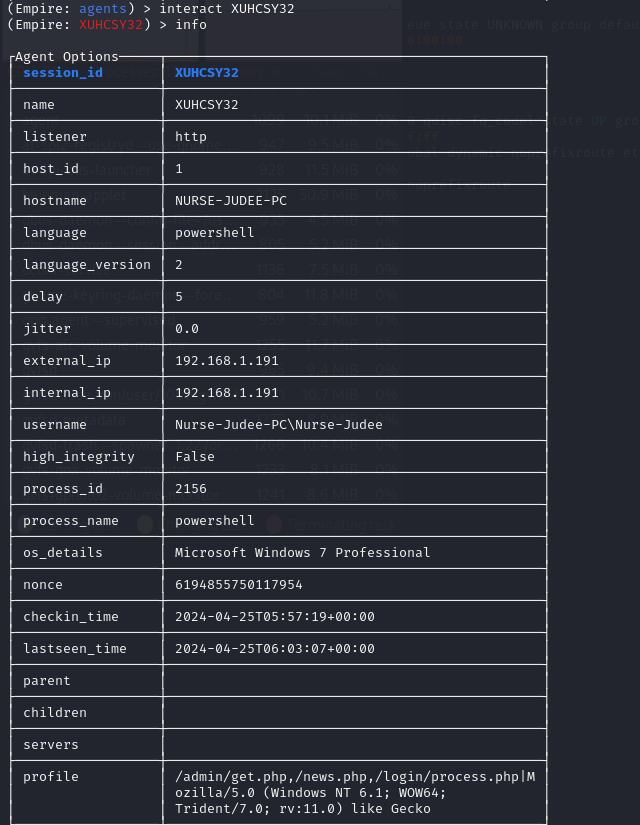
Now on Kali, see popup that it found Judees machine. We have exploited Judee!



Type agents so we can see Judee’s Pc’s information.

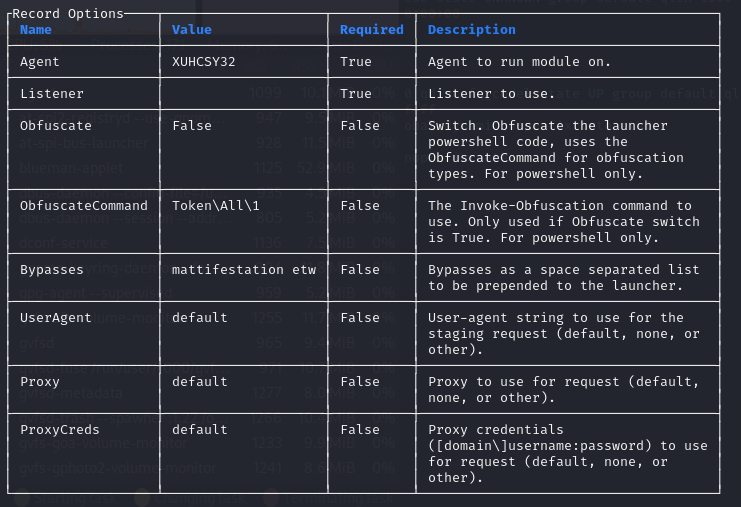


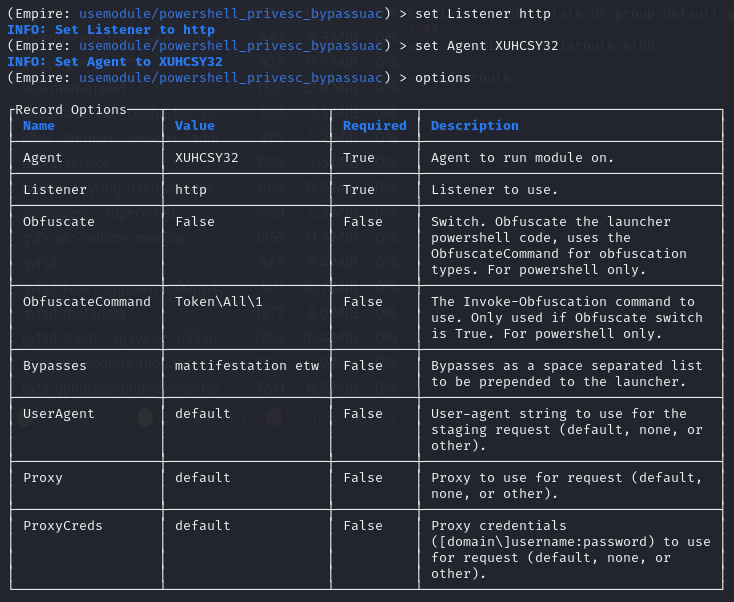
Type ‘interact XUHCSY32’, and then info so we can see more information about Judee’s PC.



***Notice how we don't have “high\_integrity” on Judee’s PC? Let's escalate privileges for ourselves ;3***

Type usemodule powershell\_privesc\_bypassuac on the kali machine.

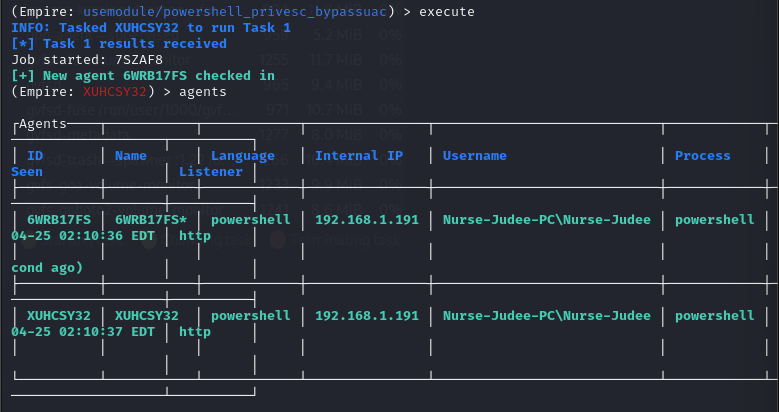
Set the listener to the http one we already set up, then set the agent to the name of Judee’s PC, then type options.



Now type execute.

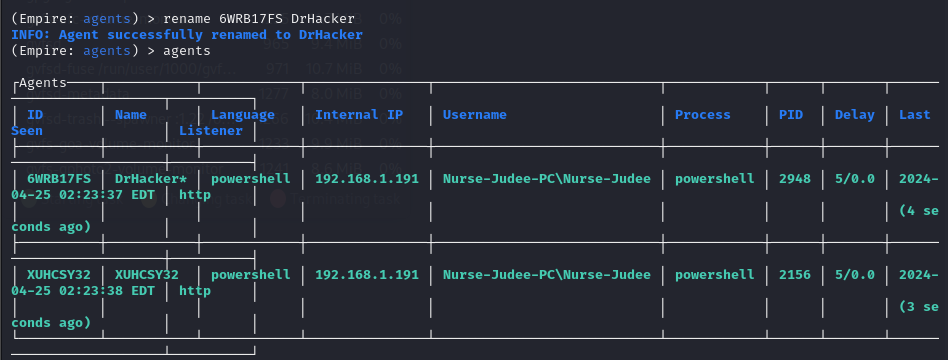
You will hear the windows VM give you a happy windows 7 noise, meaning it did what we assigned it to!

We have created a new agent on Judee’s PC, which is a hacked user that has full admin access to her whole computer. Let's check that it's there by typing agents again!

The one with the asterisk (\*) is our hacked account! We have successfully excalated priveleges via powershell-empire on Judee’s PC.

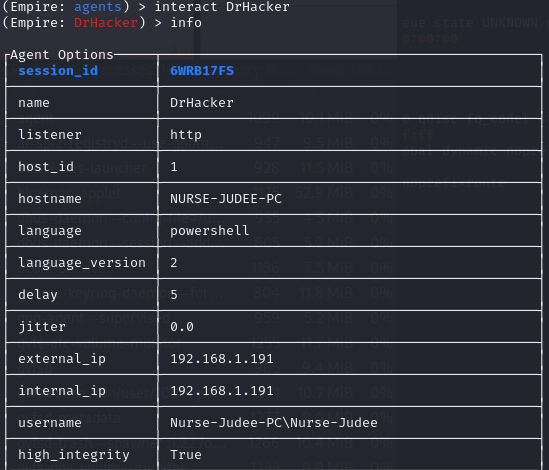
Lets rename it so its easier to follow now.

Type rename 6WRB17FS <yourname> (We’re using DrHacker)



The vector of attack is confirmed to be very bad at this point. 🙁 But since were here, let’s steal some files from Judee.

Type interact DrHacker, then type info to confirm we have escalated privleges.



Now lets navigate through Judee’s machine to find good things!

On kali, type shell explorer.exe



This opens the file explorer on Judee’s computer.

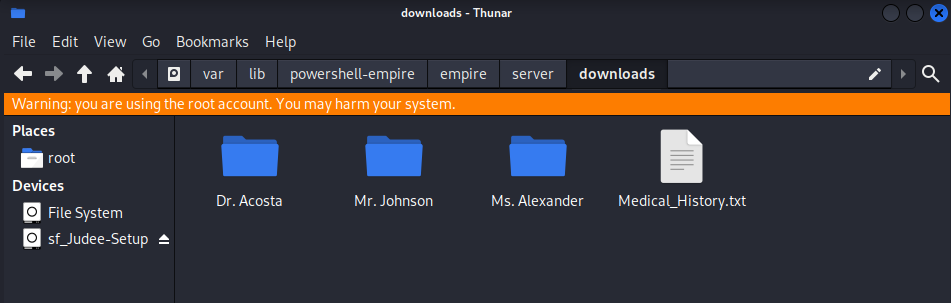
We can clearly see Judee has documents on her documents folder.

Use Powershell-empire to download it using the download command.



After downloading, it will be in the directory where all the powershell-empire files are stored.

/var/lib/powershell-empire/server/downloads/



***You have now stolen items from Judee! You proved how bad this exploit was!***