Updated: Sep 19, 2022

Class Activity - Exploiting Cupcake

💡This is a class activity to be collaboratively worked on with a partner. Once you figure out the answer or technique with your partner, execute it on your own system. The submission will be individual.

The purpose of this activity is to give you a sense of some of the steps taken to recon, assess, exploit, achieve a foothold and elevate privileges on a system.

Passive Recon

Through passive recon, we have discovered that the target organization (SHIRE) is running a webserver that purportedly runs a status application.

Part 1 - Active Recon (20 minutes)

The target is cupcake.shire.org at 10.0.5.23
What can you find out about the target?
Make sure to check the top 100 tcp ports to see what ports are listening
For those ports that are open, run another scan that attempts to run version detection against the service port.

```
Deliverable 1.  Provide a screenshot of  your team's version
detection scan(s).

Deliverable 2.  Examine any applications that are publicly
accessible.  What did you find?

Deliverable 3.  You should have the versions of at least two
applications.  Go ahead and hit the internet and see if your group
can find:
   1. The operating system (this is easy) and the
   2. release (a bit harder).
   3. What did you find and how did you find it?  Be prepared to
      share your findings with the rest of the class.
```

Part 1 - Recap

💡Your instructor or peers will fill in the gaps. Make sure to take notes and revisit the Deliverables if you need to. Please do not progress further in the activity until told to do so.

Updated: Sep 19, 2022

Part 2 - Dealing with Targets and Scans (10 minutes)

Prerequisites

- Install `nmaptocsv` using the following commands:

```
sudo apt update
sudo apt install python3-pip
sudo pip install nmaptocsv
```

- Watch the instructor demo video on a way to organize the results of your scans. The demo goes after a Windows DNS server (that no longer exists), you will be using 10.0.5.23

`Deliverable 4. Provide a screenshot similar to the one below that shows your exported googlesheet of nmap scan data against cupcake. Note, the scan in the demo did not show version detection. See if you can figure out how to do that. You will have at least two ports.`

IP	FQDN	PORT	PROTOCOL	SERVICE	VERSION
10.0.5.22		53	tcp	domain	Simple DNS Plus
10.0.5.22		88	tcp	kerberos-sec	Microsoft Windows Kerberos (server time: 2021-09-20 19:50:47Z)
10.0.5.22		135	tcp	msrpc	Microsoft Windows RPC
10.0.5.22		139	tcp	netbios-ssn	Microsoft Windows netbios-ssn
10.0.5.22		389	tcp	ldap	Microsoft Windows Active Directory LDAP (Domain: shire.local0.
10.0.5.22		445	tcp	microsoft-ds?	
10.0.5.22		3389	tcp	ms-wbt-server	Microsoft Terminal Services

Part 3 - Vulnerability Detection (10 Minutes)

Based upon what you have learned about the operating system and the nature of the web service, leverage google and exploit db to find potential vulnerabilities. Take about 10 minutes to see what you can find and be prepared to present your findings. Focus on remote vulnerabilities that might give us a foothold on the target.

`Deliverable 5. What potential remote vulnerabilities did your team find?`

Part 3 - Recap

💡Your instructor or peers will fill in the gaps. Make sure to take notes and revisit the Deliverables if you need to. Please do not progress further in the activity until told to do so.

Updated: Sep 19, 2022

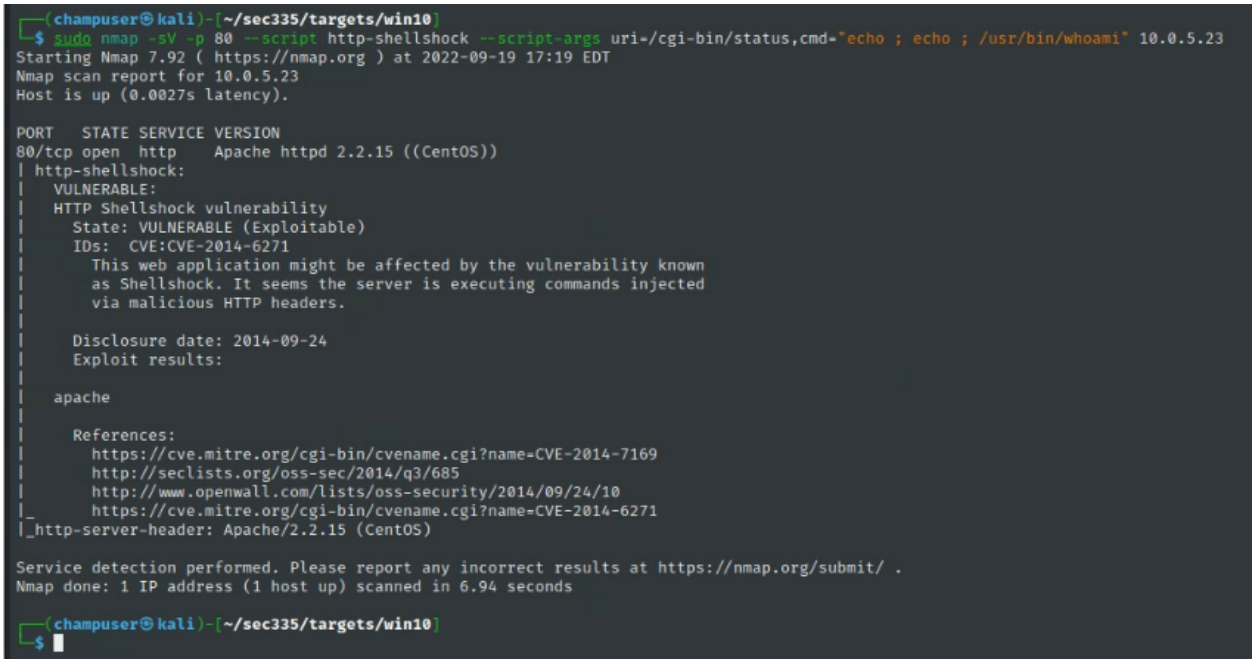
Part 4 - Remote Code Execution Vulnerability

> 💡 Your instructor will demo a remote code execution vulnerability that you will leverage to both gain information on your target.

Testing the Vulnerability

Just because your research indicated the potential of a vulnerability, let's see if we can confirm it both by hand and by use of an nmap script

`Deliverable 6. Using the following screenshot as a point of departure. Determine what the target's running kernel version (you would use the uname command for this). Provide a screenshot that shows the major and minor release of the kernel.`



`Deliverable 7. The following technique exposes the OS release. Show similar screenshots that show:`

- the contents of /etc/passwd
- the code behind the status cgi
- the results of running ifconfig

Updated: Sep 19, 2022

Part 5 - The foothold

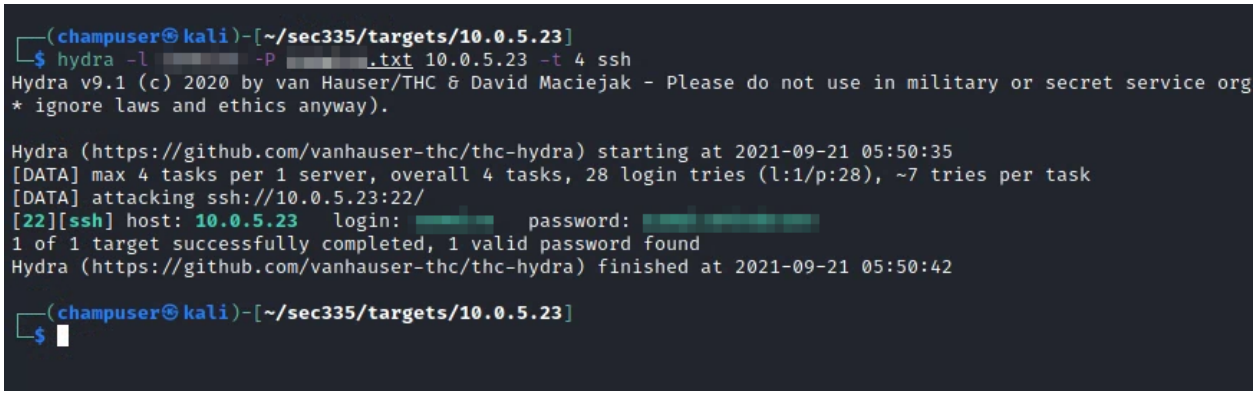
Building a password list

Do a case insensitive search of your search term on the contents of /usr/share/wordlists/rockyou.txt.gz. You may wish to extract the gzip or use zcat.

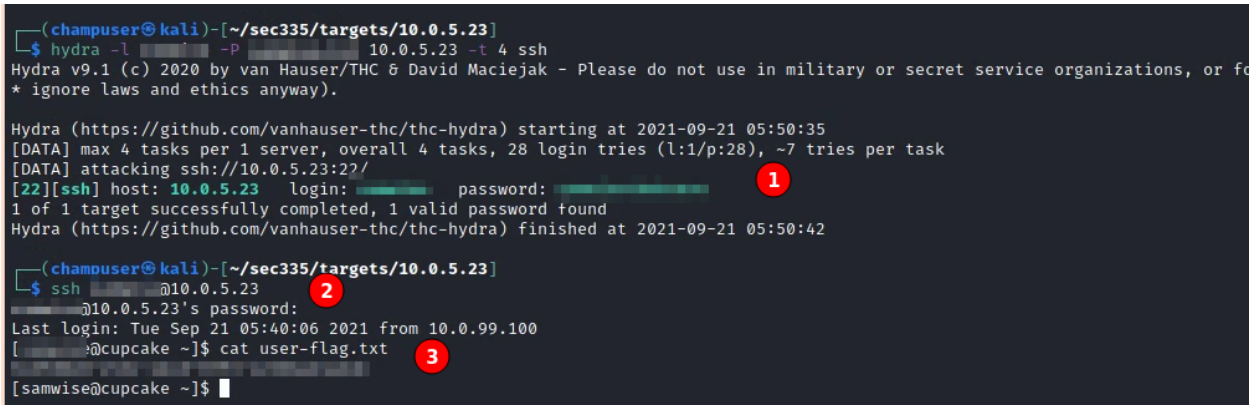
`Deliverable 8. Armed with the contents of /etc/passwd, let's see if we can build a list of likely passwords for the target account. You should end up with 28 passwords in your list. Provide a screenshot that shows how you generated the list as well as the list contents.`

Brute Force

Hydra is a versatile tool for testing a variety of passwords against a service like ssh. Adjust the syntax here to run your own attack against cupcake using the following screenshot as a guide.



`Deliverable 9. Show a screenshot of your hydra session as well as a ssh login session using the targeted account. Also dump the contents of user-flag.txt using cat or more.`



Note, if SSH complains that you are using old protocols, add this to ~/.ssh/config

Updated: Sep 19, 2022

```
┌──(champuser㉿kali)-[~]
└─$ cat .ssh/config
HostkeyAlgorithms +ssh-rsa
PubkeyAcceptedAlgorithms +ssh-rsa
```

💡There are other exploit paths to get to an interactive shell. Feel free to explore them.

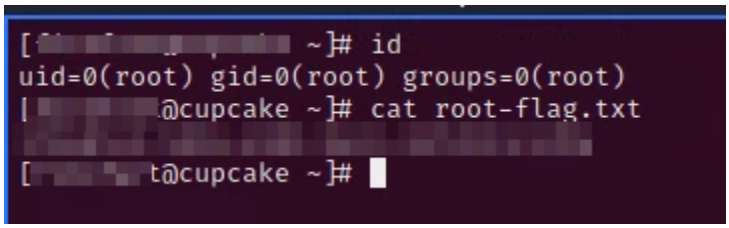
💣This is a shared target that other students will be going after. Do not hide or change any flags or alter passwords unless explicitly needed for the exploit. If you have any questions about this, ask your instructor. Also, clean up after yourself. Delete any files you have dropped on the system to the extent possible. Make a directory in which to create your files so that they are easily distinguished from another student's work. There is a way to determine what other remote users are logged in. Use that to get a sense of how busy the target is. If you suspect the system has been trashed by someone else, just revert it to "ExploitReady" and start the VM.

Part 6. Root Compromise 🐄

💡Now that we have a foothold as a valid user, we can attempt to escalate to root.

The following spoiler video shows a method for achieving root compromise. Feel free to try others. There is the potential here to break the system. If you've done so, this is ok. You have the power to access this target in vcenter only to revert the snapshot and power it back on again. When using any technique the alters accounts on the system, make sure you use your own unique username so that you don't wipe out someone else's work.

`Deliverable 10.  Provide a screenshot that shows the results of the id command as well as the contents of root-flag.txt similar to the one below.`



Updated: Sep 19, 2022

Deliverable 11. Tech Journal - Technical You likely have a lot of journaling to do! Provide link(s) to content that covers:

- How you determined the versions of the two services exposed by cupcake
- How you dealt with parsing nmap result with nmaptocsv
- The techniques you used to invoke remote code execution
- The generation of a list of passwords and subsequent ssh bruteforce
- Transfer of files using python and wget or any other mechanism you chose
- Compiling and running a privilege escalation exploit (It can be different than the demo!)

Deliverable 12. Tech Journal Reflection - Reflect on the exercise with emphasis on those techniques that you didn't quite understand or questions you would like to research. This is not uncommon, this exercise demonstrates an end-to-end attack it is not expected you will know how all the techniques used work in detail.