GETTING STARTED WITH

HACKTHEBOX

ME

Cristina Solana

Assembled in Miami

@nightshiftc

▸ Full Stack Software Engineer

▸ Bug Bounty Program / VDP Manager

▸ MiamiJS meetup Founder and Co-organizer

▸ Write at ethicalhacking.sh

CONNECTING TO HACKTHEBOX

You   Internet   VPN Server   HTB Network

```
$ sudo openvpn htb.ovpn
```

HACKER METHODOLOGY

▸ Recon
searching for vulnerabilities that can be used to gain access

▸ Exploitation
Using vulnerabilities identified during by recon to gain access

▸ Privilege Escalation
Gain elevated access to resources that are usually protected

▸ Post Exploitation (not applicable to HTB)
Persistence, Data Extraction, Removing evidence of breach

RECON

▸ Passive

Don't interact with the target directly: OSINT, viewing a webpage and its source, googling, looking at social media, Github repos.

▸ Active

Interact directly with the systems in order to gather system level information. Can be illegal. Get permission.

PORT SCANNING WITH NMAP

```
$ nmap -sV -sC -T4 10.10.10.75
```

▸ **-sV**
version detection

▸ **-T4**
paranoid (0) | sneaky | polite |
normal (3 - default) | aggressive |
insane (5)

▸ **-sC**
Performs a script scan using the
default set of scripts

▸ **-p-**
Scan ports from 1 through 65535

DIRECTORY & FILE DISCOVERY

Brute forcing with a wordlist to search for unlinked directories and files

▸ Word Lists
  - in Kali: /usr/share/wordlists
  - Daniel Miessler's SecLists

```
$ feroxbuster -u http://10.10.10.75/nibbleblog -x html php
-w ~/labs/tools/SecLists/Discovery/Web-Content/raft-
medium-directories.txt -s 200 204 301 -d 1 —silent
```

FINDING PUBLIC EXPLOITS

▸ Metasploit
penetration testing framework that helps you find and exploit vulnerabilities

▸ Common Vulnerabilities and Exposures (CVE) repositories
e.g. Exploit-DB, Mitre

METASPLOIT FRAMEWORK

It is many things, but among them it is a collection of exploits that can be used to exploit known vulnerabilities from within the MSF Console

▸ **use**
   changes context to the indicated exploit

▸ **show options**
   displays options for current exploit and if they are required

▸ **set**
   set option values for current payload

▸ **exploit**
   attempts to run exploit with designated options

NETCAT REVERSE SHELL

A reverse shell is a shell session established using Remote Command Execution (RCE) from the remote victim machine instead of the attacker's.

```
$ nc -nvlp 1234
```

▶ **-l**
Listen mode

▶ **-v**
Verbose mode

▶ **-n**
Disable DNS resolution for faster connection

▶ **-p**
Listener port

TTY SHELL

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
— CTRL+Z
$ echo $TERM
  xterm-256color
$ stty size
  67 318
$ stty raw -echo; fg
— ENTER, ENTER
$ export TERM=xterm-256color
$ export stty rows 67 columns 318
```
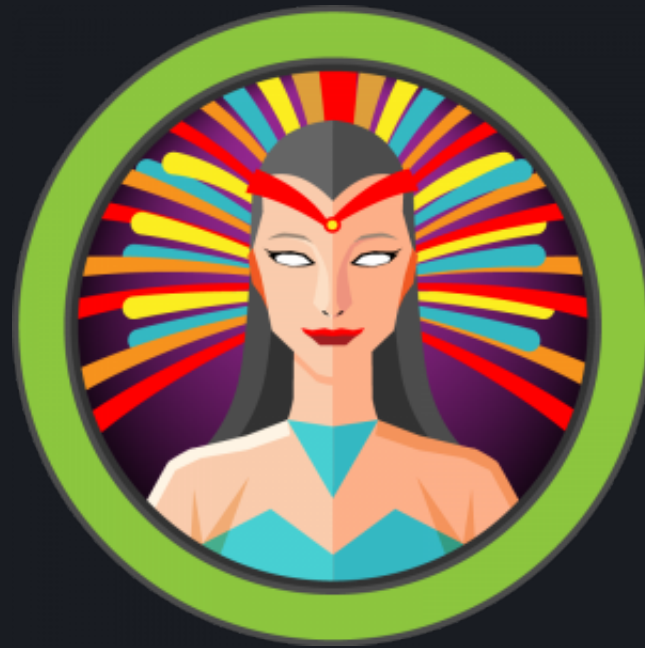
WHY ROOT USER?

▸ Remove any or all files

▸ Change the permissions of any or all files

▸ Create, update and remove user accounts

▸ Remove or install software

LINUX ENUMERATION SCRIPTS

‣ linPEAS

‣ Linux Smart Enumeration

‣ LinEnum

‣ g0tmi1k's Linux Priv Esc cheat sheet

CONTINUED LEARNING

| Lame | Bashed | Shocker | Valentine |

▸ Courses:

   ▸ [Tib3rius' Linux Privilege Escalation](#)

   ▸ [Tib3rius' Window Privilege Escalation](#)