BASIC PENTESTING

Exploiting Network and Web app vulnerabilitis

1. Task

The aim of this exercise is to target and pentest a virtual machine hosted by *TryHackMe,* a cyber security learning platform. I'll discover and exploit vulnerabilities and exposures and, at the end of the task, making use of some basic pentesting tool, I'll be able to:

- ***Enumerate*** the machine (informations gathering)
- Find ***exposed services***/ports
- Performing ***Web scanning***
- ***Brute-forcing*** usernames and passwords
- Hash ***cracking***
- Find vectors for ***privilege escalation***

2. Execution

For this task we have used a Vmware Workstation virtual machine hosting Kali Linux, which provides us with all the basic tools already installed.

PING

At first, we simply *Ping(ICMP protocol)* the target machine to confirm to be able to communicate with it.

NMAP – Footprinting

We start our enumeration process using ***Nmap*** *(Network Mapper)*. With Nmap we'll be able to discover open port and running services*. The syntax for this is:

```
user@kali$    nmap    10.10.143.244
```

**Note: This is a beginner level exercise, and by so we only run the most basic nmap scan, but we could have actually passed arguments specifiyng Target destination, Host discovery, Scan Techniques, Port Specificationnand so on.*

This first scan will reveal us a ***SSH service on port 22***. A ssh service is a program that allow a user to run a command prompt on a remove machine/server. We want to gain access this service in order to be able to retrieve important data. As result of the scan we can also see that an ***HTTP service is running on port 80***. In fact, if we search for the Ip address on the browser we can actually find a website on maintenance.

DIRB – Web Scanning *(Exploiting Http, Open port 80)*
Inspecting the webpage we can see the *HTML* code and we find out a comment left on the *Body* of the program: “*check our dev note section to find to work on..”*. We can now exploit this information and search for directories on the website and see if we can find some other useful informations.
To do so we use ***DIRB***: *dirb* is a contents web scanner. It looks for existing web objects, such as directories, launching a dictionary based attack. We simply pass:

```
user@kali$    dirb    http://10.10.143.244
```

As result of this we discover a listable directory called /d*evelopment.* In this directory we eventually find the Dev.txt note file stated on the comment left by the developers on the body of the website’s HTML. We open the file to retrieve useful informations :

- Version that is been used
- *SMB service active. Client-server protocol*
- Apache web server set up

The same */development* directory also includes another text file from which is possible to gather even further informations:

- Users name’s first letter are J and K
- K’s Hash is easy to crack and it’s inside the directory: */etc/shadow*
- System in use is Linux

Enum4linux – Enumeration Tool *(Exploiting SSH, Open port 22)*
We now run an enumaration tool called **enum4linux.** We simply pass:

```
user@kali$    enum4linux     10.10.143.244
```

We can now see a long list of informations like the usernames: Jan and Key. We now recall that on port 22 is running an ssh service and it’s time to use a bruteforce tool to crack jan ssh’s password.

HYDRA – Passwords bruteforcing
Hydra is a list-based password cracker that we’ll be use to gain access the ssh service. We pass:

```
user@kali$  hydra    -l    jan    -P    /usr/share/wordlists/rockyou.txt
10.10.143.244    ssh
```

With this syntax we specify: username, password list path, target Ip and service(*ssh*). The result will eventually show the password: **armando**.
We can now connect to the server with the ssh command:

```
user@kali$:    ssh    jan@10.10.143.244
```

And here we go! We are now connected to the ssh server with Jan credentials. This allow us to run commands on terminal, search for files and informations. The user Jan has limited privileges, this is why it's now time to perform a **privilage escalation.**

Privilege escalation

When we start to look around we soon understant that Jan has very limited privilege, and any access attempt to a file or directory is denied. To find out this we can simply run basci terminal commands: **cd** , **ls**, **ls -la**, **cat** etc..
One particular command - *user@kali$* ***ls -la*** - will make us notice that we can access an *hidden folder* called **.ssh**. Inside the folder we eventually discover the file **id_rsa.**

John the Ripper – Hash cracker

id_rsa and *id_rsa.pub* are respectively a private key and a public key. Our attention goes *on the id_rsa file* which can give us access to *ssh* as *Kay*. All we need to do is copy and paste the content of the file on our machine passing:

```
user@kali$    nano    key
```

Before being able to use the private key we need to decrypt it using our hash cracker: **John the Ripper.** John doesn't accept ssh format key and so we firstly need to run a python, part of the John the Ripper repository, called **ssh2john.py.** To do so we run the command:

```
user@kali$:  /usr/share/john/ssh2john.py     key  >  hash
```

With this syntax we specify the script location, the file to input and the name of the new output file. Now our hash key is on a readable format for **John**. We run:

```
user@kali$:     john     hash
```

And by so the terminal will show us the passphrase: **beeswax**. It's now the moment to finally access ssh for the user kay using:

```
user@kali$:     ssh      -i      Key      kay@10.10.143.244
```

And using our brand new decrypted passphrase we can now log in to the server as Kay! As we notice the user Kay had administrative privilege and we can now access the file *pass.bak* which contains his password.

BOOT2ROOT

Our last step is to access the root, and as the user Kay has all the priviliges to do so we can simply type:

```
kay@basic2:-#      sudo   -i
```

and we are in! We finally search into the file system, find the root folder and output the content of the flag to complete the task.

3. Conclusions

At the beginning of the exercise we have only been given an Ip address. Thanks to Nmap, Dirb, Enum4linux, Hydra and John The Ripper we have been able to gather information, to crack passwords, to gain access to a ssh service and log in as a root user.
Despite being a beginner-level exercise, this task gave us the chance to try out some of the fundamental tools used in CyberSecurity.
When running these tools we rarely used options to extend their potential or to activate particular features. In a real world scenario, to obtain a similar result, we'll surely need a deeper knowledge of these tools, along with a strong networking, protocols and web knowledge.

Resources

1. Cyber security learning platform
TryHackMe, Basic Pentesting Room
2. Nmap
https://nmap.org/
3. John the Ripper
https://github.com/openwall/john
4. Dirb
http://dirb.sourceforge.net/
5. Hydra
https://github.com/vanhauser-thc/thc-hydra
6. Enum4linux
https://github.com/CiscoCXSecurity/enum4linux

Credit: Alessio Ragazzi, London