CTF Writeups

TRYHACKME

Basic Pentesting Lab

Step 1:

Connect your Kali Linux with OpenVpn Configration File.

Step 2:

Start the Machine in the Basic Pentesting lab and copy the Target Machine IP Address.

Perform ping command to the Target Machine to check the network connectivity.

Step 3:

Here Comes the Pentesting Part, The First and foremost Step in Pentesting is Information Gathering is performing nmap scan to the target to Discover about the Open ports in the target Machine.

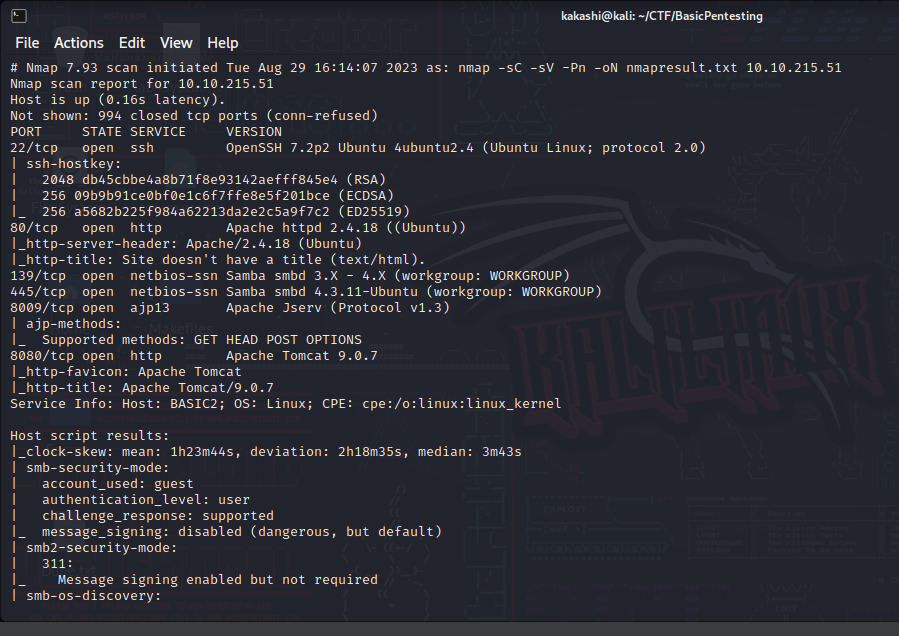
> nmap -sV -sC -Pn -oN nmapresult.txt 10.10.215.51

-sV means Version Scan which will give version of the service running on the open ports.

-sC means Script Scan which will use the default nmap script.

-Pn means don’t ping scan which will skip the ping icmp packet and think that host will be active and perform the nmap scan.

-oN saves the output file



Step 4:

After Performing nmap scan we found that port 22(ssh), 80(http), 139,445(samba smb).

Since Port 80 is open we can enter the IP Address of the Target Machine in our Local Browser to gather information about the target.

Since there is not sufficient information in the webpage and the page source, while surfing internet about the Apache httpd 2.4.18 version in which port 80 is running some of the possible vulnerabilities is Directory Traversal, PE, DOS, etc. so we can try to enumerate the directories in the target website using 2 methods:

1. Using Nmap script http-enum
2. Using Directory Traversal tools like gobuster and dirbuster.

Method 1: Using nmap script -

> sudo nmap –script http-enum `TARGET-IP`

Method 2: Using gobuster -

>gobuster -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u 10.10.215.51

-w means wordlist

-u means url

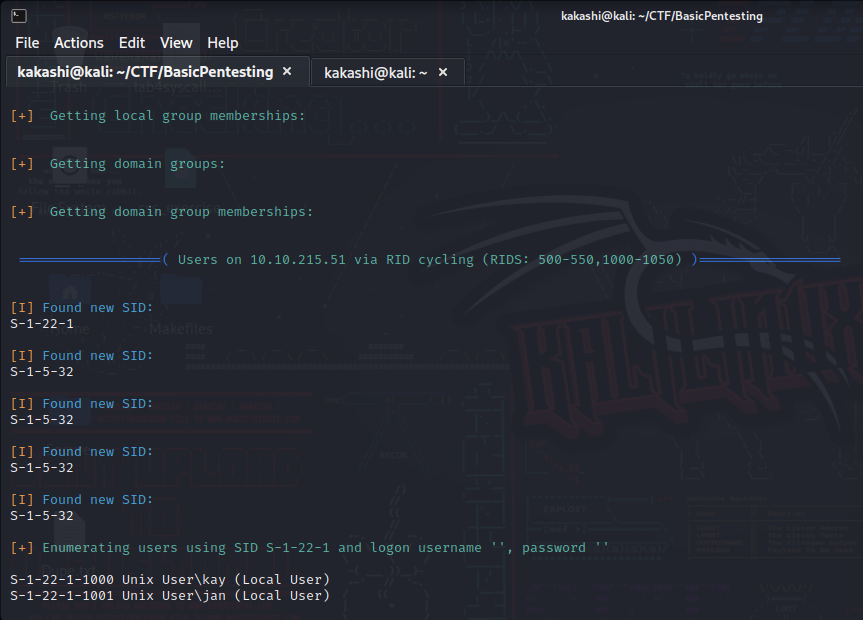
After Performing the Directory Enumeration we found that /development can be accessible.

Search 10.10.215.51/development in your browser, you can see that there is 2 files in it, it is the conversation between 2 people J and K. In their Conversation they stated that their SMB need to Configured and there is a Weak Password.

Step 5:

To Gather More information about the SMB and Windows we can **enum4linux** tool which will information about users,groups,policies and broken ACL and it will figure out weak credentials.

> enum4linux -a 10.10.215.51 | tee enum4linux.log



We found the Users in the Target System. We need to crack the password of the user.

Step 6:

For cracking Password, we can **Hydra** Bruteforcer tool

> hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.215.51

This will give the password of the username jan

Step 7:

Try Login with the Gathered Credential in ssh

jan : armando

> ssh jan@10.10.215.51

After Login surf through the files in the machine there we found a rsa private key of the another user kay copy the content in the private key file and break the cipher

Step 8:

Breaking the rsa\_file with **john the ripper** tool.

The id\_rsa is stored in a file called kay\_id\_rsa

>python /path/ssh2john.py kay\_id\_rsa > forjohn.txt

This will break the rsa private key now we need to extract the password from it.

> john forjohn.txt –wordlist=/usr/share/wordlists/rockyou.txt

This will give the password of the kay user.

Try to login with kay:beesaw credential in ssh in the same jan terminal

> ssh -i /kay/.ssh/id\_rsa kay@10.10.215.51

After login open the pass.bak which contains the flag for the CTF and submit it.

Since jan is a non root user we need to escalate to root user

To do that we use **linpeas** tool.