Washkewicz College of Engineering

Name: Aditya Sairam Pullabhatla

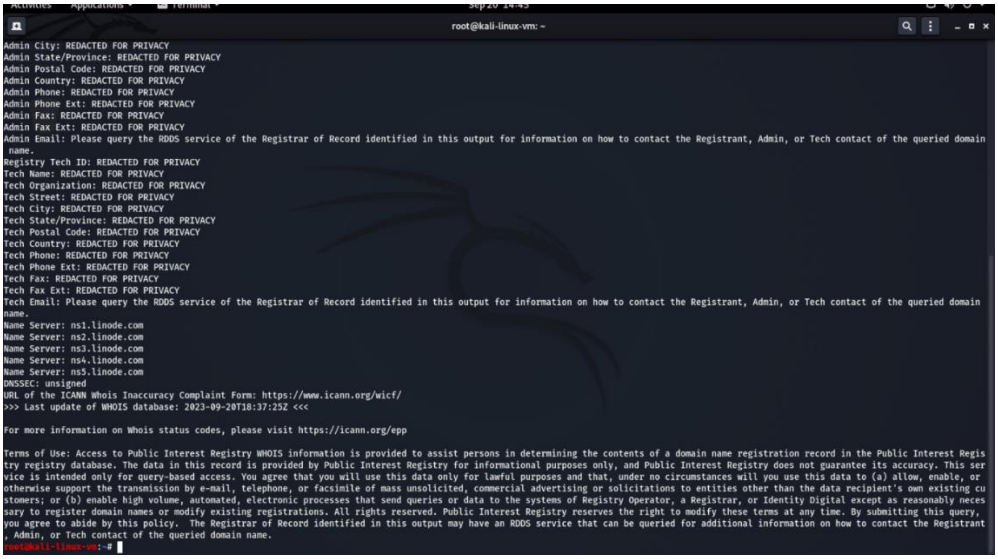
CSU ID: 2863159

Assignment 1

Passive recon: Run a whois command on nmap.org.

1. **Paste a screen shot of all the information that you received.**

Ans:



2. **What specific information from this command could be useful to a penetration tester and should be documented?**

Ans: A penetration tester is a legitimate simulated attack carried out on a computer system to assess its security. To identity and illustrate the financial effects of system flaws, penetration testers employ the same tools, strategies and procedures as attackers. A penetration tester may find specific commands that can be used for documentation:

- **Registery Domain ID:** When a domain name is registered, a specific identification known as the Registry Domain ID is connected to it. It acts as a guide or a key that aids in specifically identifying a certain domain inside the domain registry's database. When a domain is registered, either the domain registry or the domain registrar normally assigns this identification.
- **Registrar WHOIS server:** The domain registrar's dedicated WHOIS service enables users to request and obtain comprehensive information about a domain name. This server enables penetration testers and investigators to have access to extra information about a domain, such as ownership information and registration history, which can be useful for evaluating the target's internet presence and doing security assessments.
- **Registrar URL:** The domain registrar's website's URL is known as the registrar URL. It acts as a portal to the registrar's services, which include domain registration, maintenance, and support. Penetration testers can use this URL to learn about the registrar's policies, services, and even uncover contact information or security-related resources.
- **Domain Status:** A domain's current state inside the domain registry is shown by its domain status. Frequently used status values include "active," "clientTransferProhibited," and "inactive." It is essential to comprehend the domain's state in order to evaluate its availability and any constraints or limits that could effect its usage or transfer. This data may be used by penetration testers to find out whether the domain is being used right now or if there are any legal limitations.
- **Registrant Information:** Information about the person or business that owns and operates the domain is included in the Registrant Information. This information normally consists of the registrant's name, organization (if relevant), contact address, contact phone numbers, and email addresses. When determining possible security threats or launching targeted attacks, penetration testers may utilize this information to identify and characterize the domain owner.
- **Admin Information:** Contact information is provided for the administrative contact who is in charge of overseeing the domain. The admin's name, organization (if relevant), contact information (including phone and email addresses), and address are all listed here. These details might be used by penetration testers to open lines of communication with the domain's administrators and learn more about the domain's management procedures, perhaps assisting with security analyses or vulnerability disclosures.

3. **What other tools/services could you use to find similar information?**

Ans: **WHOIS DOMAIN:** For domain name professionals, cybersecurity specialists, and others interested in learning more about internet domains, Whois.DomainTools.com is a comprehensive web platform that offers crucial domain-related information and tools. The service provides a robust WHOIS lookup tool that enables users to acquire comprehensive information about domain registrations, ownership, and history records. It offers facts on domain availability, contact information for the registrant, DNS records, and more.

Additional sophisticated services provided by DomainTools include threat analysis and domain monitoring. Users are able to keep track of domain ownership changes, keep track of brand references, and spot possible cybersecurity risks. The protection of a company's online brand reputation and the investigation of dangerous online activity by cybersecurity experts may both greatly benefit from this service.

EDGAR: The U.S. Securities and Exchange Commission (SEC) manages the Electronic Data Gathering, Analysis, and Retrieval system, often known as EDGAR. It acts as a thorough archive for financial filings, disclosures, and reports made by publicly traded firms and other entities obliged to file with the SEC.

ROBTEX: Numerous networking and cybersecurity-related services are offered through the website and online tool known as Robtex. It is well recognized for its lookup services for DNS and IP addresses, as well as for its capacity to compile and present data on internet resources including domain names, IP addresses, and network-related information.

4. **Linux Review question: How can you find out more information about a command line tool, such as options, syntax and examples?**

Ans: To find out more information about a command line tool, including its options, syntax, and examples have various methods:

- **Man command:** Most Linux distributions make command-line tool documentation pages (man pages) available. The man command, followed by the name of the tool, will provide you access to them. Running '*man ls*', for instance, would allow you to access the ls command's documentation page. Man pages include comprehensive details on how to use a command, including with examples of usage and a list of possible options.

  Example: man -ls

- **--help command:** A --help or -h option is available for many command-line utilities. The tool's usage, available options, and occasionally examples are briefly described when the command is run with this option.

  Example: ls --help

5. **List 3 additional ways, which penetration test can enumerate and find additional IP/network space given a single domain?**

Ans: There are various ways where a penetration test can enumerate and find additional IP/network space given a single domain, some of the methods are:

- **DNS enumeration**: The procedure of obtaining or requesting domain name system (DNS) data from a target network or domain is known as DNS enumeration. It is a frequent tactic that is employed in both proper system management and security evaluations like ethical hacking and penetration testing. The domain structure, network architecture, and perhaps sensitive hostnames or IP addresses can all be learned by DNS enumeration.
- **Reverse IP lookup**: An IP address is mapped to a corresponding domain name through a method called reverse IP lookup, also known as reverse DNS lookup or PTR (Pointer) Record Lookup. Reverse IP lookup serves the opposite purpose of typical DNS (Domain Name

System), which resolves domain names to IP addresses by giving a domain name for a given IP address.

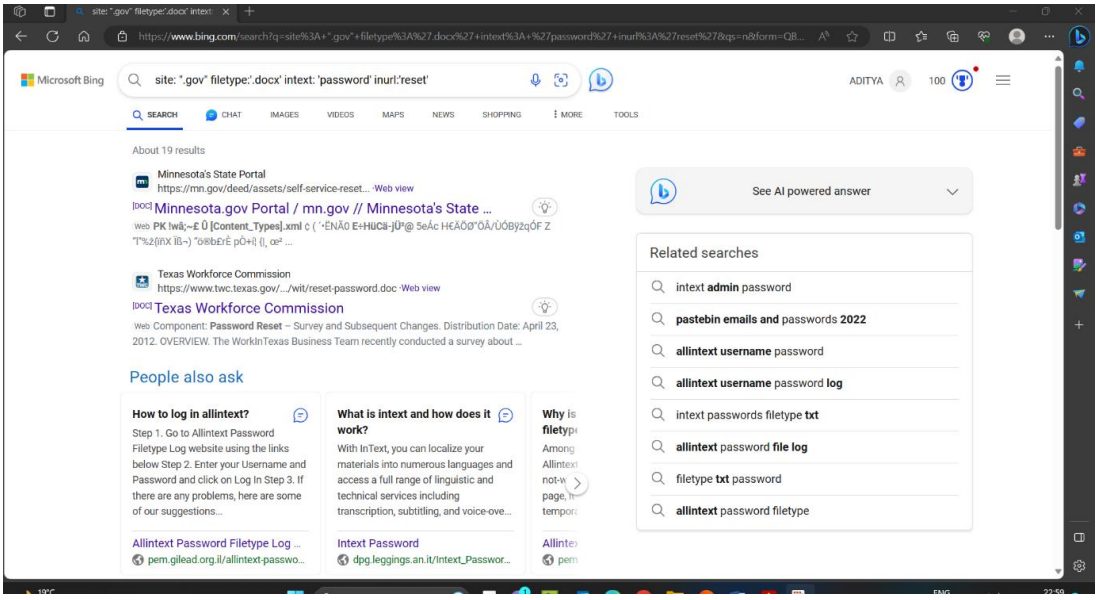
- **Port Scanning**: A network reconnaissance method called port scanning is used to find open ports and services on a target machine or network. It is an essential stage in both normal network management and security testing as well as potentially harmful actions. Main purpose of port scanning involves network Mapping, Security assessment.
- **OSINT**: The OSINT approach may be used to learn details about a company, such as its IP addresses and network architecture. To learn more about the target's internet presence, testers can look for information from publicly accessible sources including social media accounts, job listings, and open papers.

Using Google Dorks, run a search and narrow the results to only include: all .gov TLDs, the term "password" inside the body of the page, the term "reset" in the URL, and only return .docx files.

6. **What was the search query that you used?**
   Ans: site:".gov" filetype:"docx" intext:"password" inurl:"reset"

7. **Paste a screen shot of the result of the google dorks search results.**

Ans:



8. **Example two ways a penetration testing could gather e-mail addresses of key employees.**

Ans: Google Dorking is a technique for discovering content on the web that makes advantage of Google's powerful search operators and filters. When used maliciously, it can provide security problems even if it can be a beneficial tool for information retrieval and study. Google Dorking is a popular tool used by ethical hackers and penetration testers for information gathering and reconnaissance. Google Dorking might be used to compile email addresses of important individuals inside a business, which is one of the major hazards that comes with it.

Social Engineering Security experts can determine if an organization is vulnerable to social engineering threats by conducting social engineering penetration testing. Instead than looking for

technological flaws, these tests are designed to find weaknesses in human behavior, rules, and processes. Such testing may lead, among other things, to the collecting of email addresses or other sensitive information about important personnel.

9. **Why would a list of e-mail addresses be useful to a penetration tester?**

Ans: To perform phishing attacks, A list of email addresses may be a useful resource for doing ethical hacking and penetration testing for a number of reasons, but it's crucial to stress that any usage of such a list must always be done in a legal, ethical, and authorized manner.

An email address list might be used in the following ways by a penetration tester:

A collection of email addresses can be used by a penetration tester to find possible targets inside a company. By selecting certain people or departments to evaluate for vulnerabilities, the test's scope may be better understood.

Phishing campaigns: To determine a company's vulnerability to phishing assaults, ethical penetration testers frequently run phishing simulations. With a collection of email addresses, they may replicate phishing attacks and send them to staff members to gauge how well-aware they are of the risks and how they will react.

Spear phishing: A penetration tester may occasionally engage in spear phishing, which is creating phishing emails that are specifically targeted and tailored to the user. The selection of specific employees or organizational functions as targets for these simulations is aided by a list of email addresses.

Training for User Awareness: A penetration tester can provide user awareness training using the email address list. Employees may learn how to spot phishing efforts and how to react to them by seeing samples of actual phishing attacks.

Assessment and Reporting: The list of email addresses may be used to keep tabs on whether employees have received phishing emails, as well as if they clicked on any links or gave sensitive information. For determining the organization's security posture and producing thorough reports for enhancement, this information is essential.

Password cracking In order to unlock user accounts, systems, or files, a procedure known as password cracking is utilized. Password cracking techniques can be used by penetration testers or ethical hackers to evaluate the security of an organization's systems and to find weak or simple passwords that might be used by bad actors.

For the following reasons, a list of email addresses might be helpful to a penetration tester for password-cracking:

User enumeration: The collection of email addresses aids in finding legitimate user accounts in a target system. For targeted password cracking operations, knowing which accounts are present is essential. Attackers frequently go for individual user accounts, and having a list of email addresses gives them a place to start.

Targeted Attacks: In some circumstances, penetration testers may need to perform targeted password cracking against particular user accounts to evaluate the security of their credentials. Testers can rank these accounts using the list of email addresses in order of importance or probable effect.

Organization hierarchy exploration: Top tier employee details.

Exploring an organization's hierarchy entails learning about its internal workings, including information on its top managers or workers. It's critical to understand the moral and legal ramifications of such behaviors, even though a list of email addresses may be valuable in this situation.

How a list of email addresses relates to investigating organizational hierarchies and if it may be helpful to a penetration tester are as follows:

Locating critical people: A collection of emails may be used by a penetration tester to locate critical people, including senior executives, within a company. This list is a good place to start when figuring out the organizational structure and locating high-value targets for security audits.

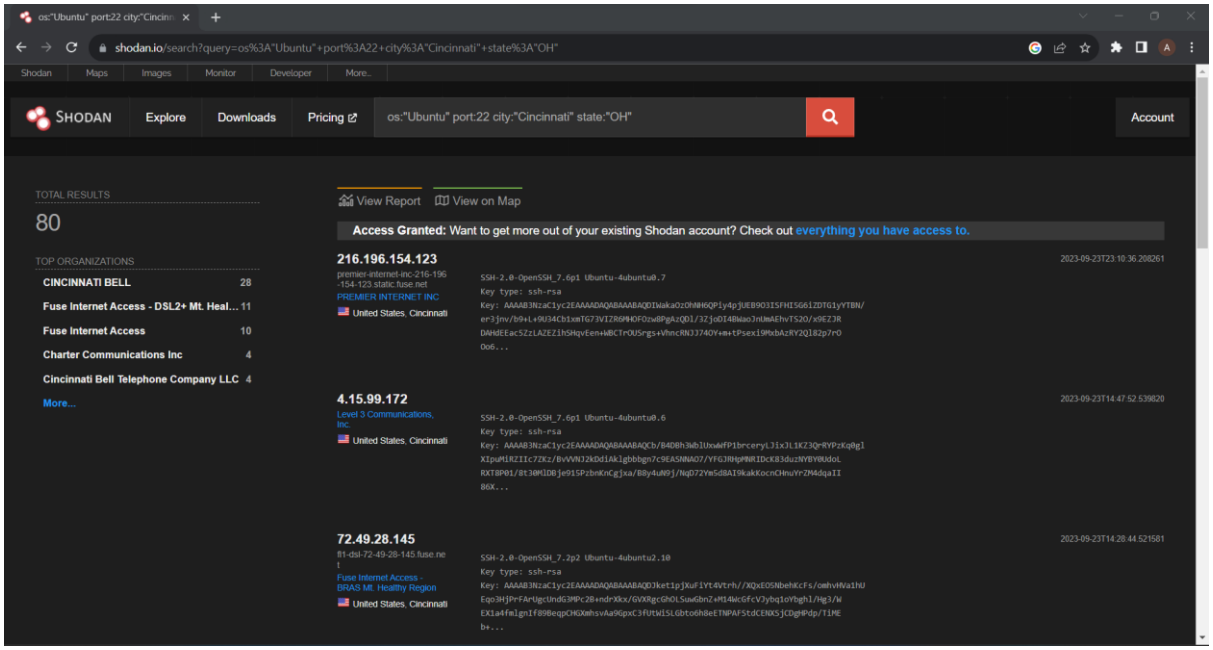
Targeted assaults: In the event that the penetration test involves targeted assaults like spear phishing, having access to the email accounts of senior staff members might be useful. To obtain private data, attackers may create highly customized phishing emails addressed to certain executives. In this instance, the receivers of these fictitious assaults are represented by the email addresses.

Penetration testers frequently utilize the email accounts of important workers to conduct security awareness testing. To determine if top-tier personnel are aware of and can react to security risks correctly, this entails sending simulated phishing emails or social engineering tries.

Run a search on Shodan to return results that have an Ubuntu server running with port 22 open
and based in Cincinnati, OH.

os:"Ubuntu" port:22 city:"Cincinnati" state:"OH"

10. **Paste screenshot of your result**



11. **What version of SSH is running on the first returned result?**

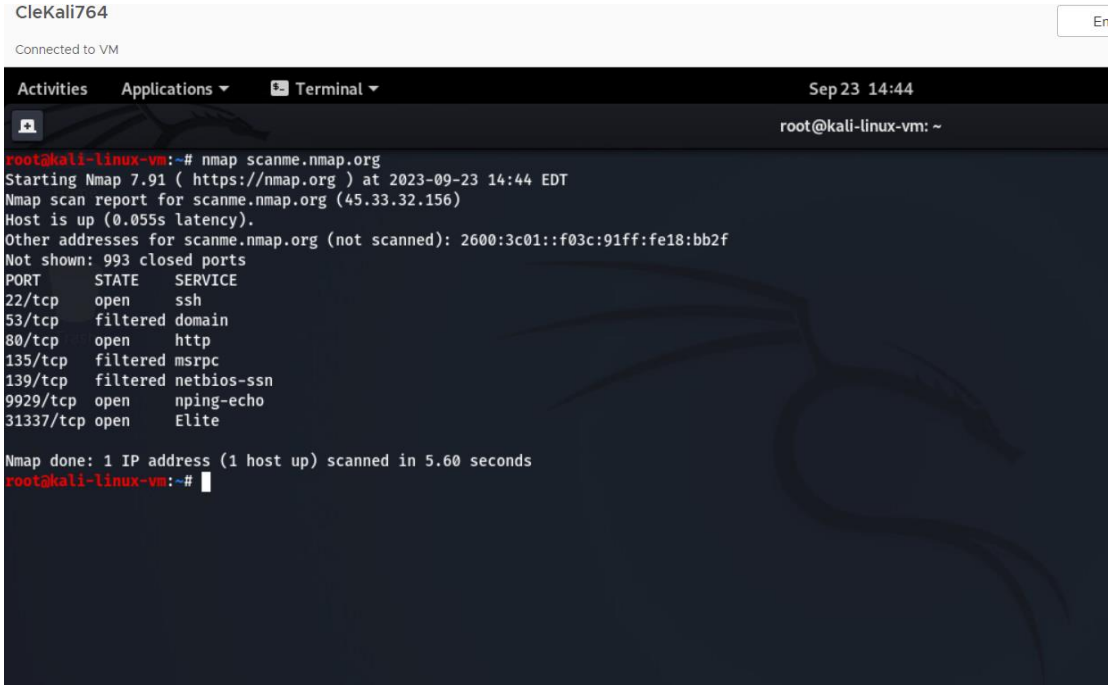
Ans: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7

Module Activity Description:

Part two: Active recon

Run an nmap scan against scanme.nmap.org

1. **Paste the screenshot of the result.**



2. **Explain what information from this scan may be useful to a penetration tester.**

- **Ip 45.33.32.156:** An American hosting company named "Linode" has a server with the IP address 45.33.32.156. Virtual private servers (VPS) and other hosting services are provided by Linode, a well-known provider of cloud hosting.
- **Latency:** A key component of network performance, latency affects how quickly data moves along a network from one point to another. It reflects the lag or delay in data transmission and is commonly measured in milliseconds (ms). In many apps, latency may significantly affect how users feel. Low latency is essential for an immersive and smooth gaming experience while playing games online since it allows player actions to be reflected in real-time. Similar to voice over IP (VoIP) calls, video conferencing, and low latency make guarantee that talks flow naturally and without annoying pauses. Physical distances should be kept to a minimum, routing methods should be effective, and network infrastructure should be optimized. The quality of network-dependent apps as a whole and user happiness may both be improved by resolving latency concerns, which allow enterprises to offer services more quickly and effectively.
- **Filtered domain:** A domain that has had its content screened or had access denied is referred to as a filtered domain. The primary purpose of these measures is to restrict the kinds of content that users may view or to prevent access to particular websites. Filtered domains, for example, support the maintenance of a focused atmosphere in workplaces and educational institutions by preventing access to unsuitable or distracting websites. However, parental control filters protect kids from viewing inappropriate web information. In order to regulate material or uphold social standards, some governments also utilize content filtering to block or prohibit access to particular websites. The continued difficulty of striking a balance between access and control in the digital era is highlighted by the fact that users may utilize a variety of strategies, such as VPNs, to get around filtered domains despite these limitations.

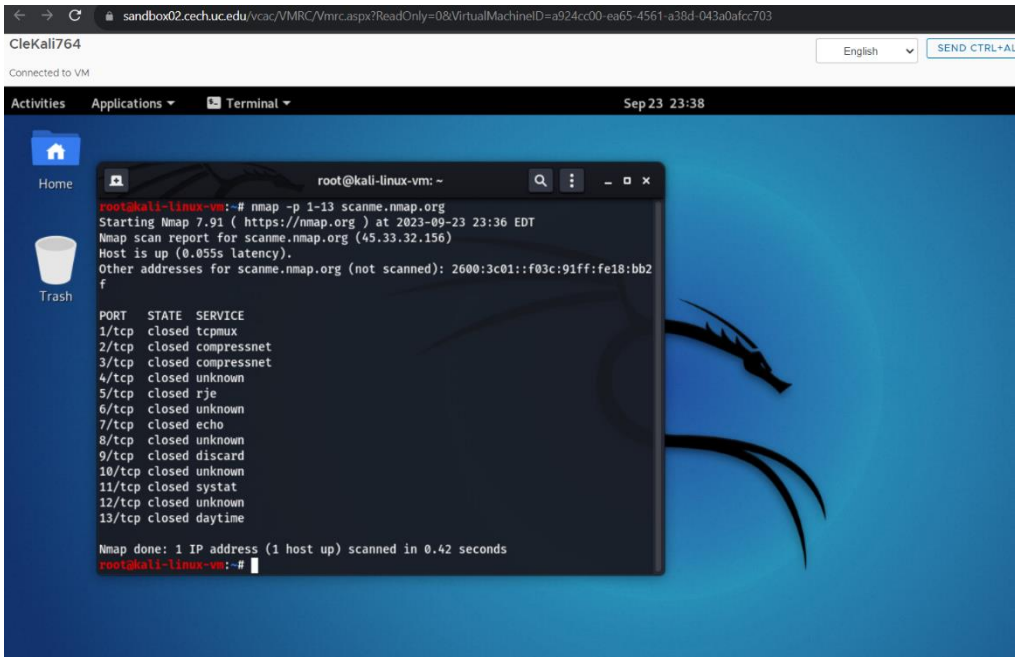
- **Open ssh:** The open-source software package for secure network communication known as OpenSSH, or short for "Open Secure Shell," is quite popular and well-regarded. OpenSSH provides a reliable and encrypted method of connecting to distant servers and devices. It was primarily created for remote login and secure file transfer across unprotected network connections.Using encryption to safeguard sensitive data while it is in transit is one of OpenSSH's most prominent features. Secure key exchange mechanisms and powerful cryptographic algorithms are used to accomplish this. For system administrators, programmers, and security-conscious users, OpenSSH is a reliable option since it preserves the confidentiality and integrity of data. Secure remote access to servers and other devices across the internet is made possible via OpenSSH, which is essential for remote server management. It is crucial for managing and maintaining systems in a secure and effective manner, and has evolved into a necessary component of many operating systems. OpenSSH is a pillar of secure network communication in the digital age, whether it is being used for secure file transfers or secure shell access.
- **Filtered netbois-ssn:** Filtered NetBIOS-SSN, sometimes referred to as NetBIOS Session Service, is a network communication protocol that is used to share files, printers, and other resources on a local network. If NetBIOS-SSN traffic is filtered, it usually signifies that firewall rules or security measures have been implemented to limit or regulate the transmission of NetBIOS communication.

  Filtering NetBIOS-SSN can be a crucial security precaution, particularly in bigger networks and via the internet, as the NetBIOS protocol was not created with security in mind and can present security problems if not adequately regulated. Filtering reduces possible vulnerabilities and unauthorized access by, for example, blocking specific NetBIOS ports or restricting access to NetBIOS services.

  Filtered NetBIOS-SSN can be used by enterprises to improve the security of their network infrastructure and lessen the risk of sensitive data being exposed to danger. This procedure is crucial for contemporary network security because it guards against unwanted access and preserves the integrity and confidentiality of network resources.

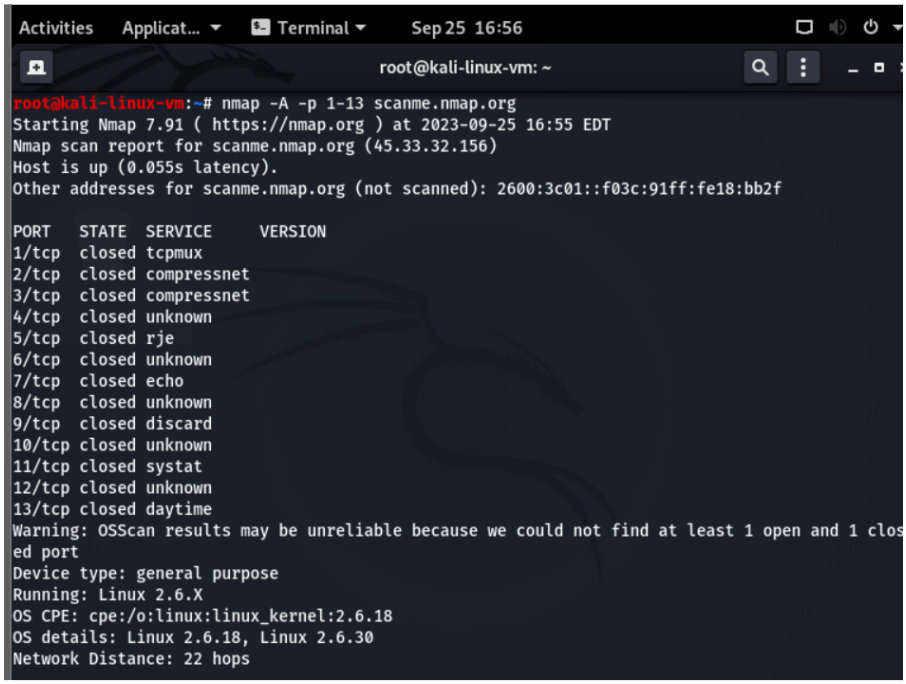
Run another nmap scan against scanme.nmap.org. This time include the options to include version detection, the top 13 ports, and operating system detection.

3. **Paste the screen shot of the result.**



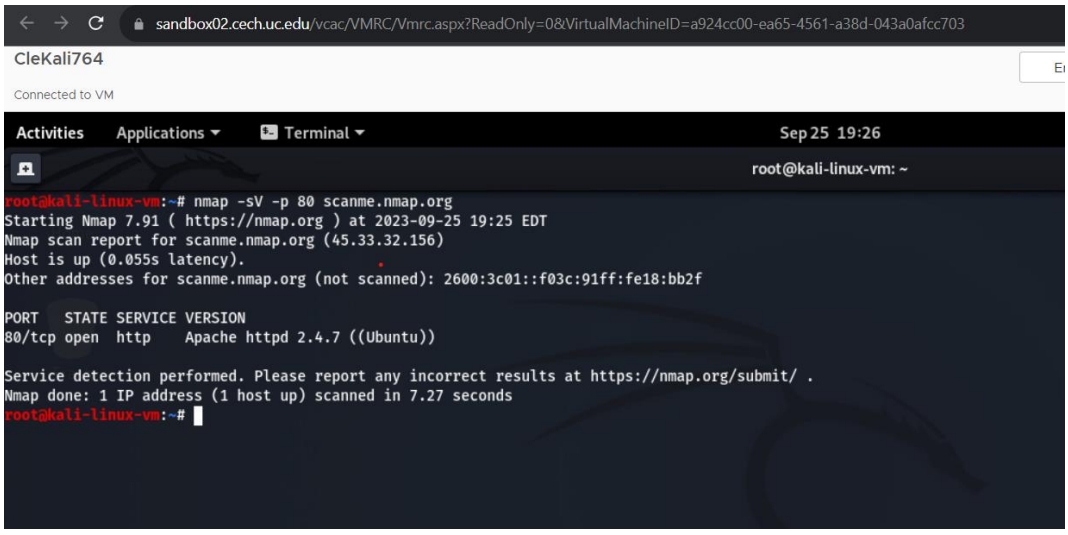
4. What OS is the system running (Best guess)?

Ans: Linux 2.6.18, Linux 2.6.30



5. What version of Apache is this system running?

Ans: Apache httpd 2.4.7((Ubuntu))



6. What happens if nmap itself cannot determine if a host is alive or not?

Ans: Instances where Nmap is unable to establish a clear connection with or response from the target host are indicated by the tool's inability to identify whether a host is alive or not. Several things, such as network setups, firewalls, or host-specific settings, may be to blame for this.

The host's status will often be marked as "unknown" or "unreliable" in these circumstances by Nmap in the scan findings. This indicates that Nmap's attempt to determine the host's state during the scanning procedure was unsuccessful.

Troubleshooting network problems, confirming the host's accessibility, and looking for any security measures, such as firewalls or stealthy setups, that could be impeding Nmap's ability to establish host status are common steps in dealing with this circumstance.

The complexity and difficulties that might occur during network scanning and reconnaissance are ultimately shown when Nmap is unable to ascertain host status. Gaining a deeper grasp of the host's condition and network accessibility may require more research and changes.

7. How could you bypass the above behavior?

Ans: It might be difficult to get beyond Nmap's inability to tell if a host is alive, and it could be necessary to use extra techniques and tools to learn more about the target host

Ping Scanning: Nmap frequently employs ICMP (Internet Control Message Protocol) Echo Requests (ping) to ascertain host availability. If the target host is set up to block ICMP, you can attempt getting around this restriction by using Nmap's -Pn option to forgo host discovery through ping and continue scanning.

Using the -p option in Nmap, you may immediately scan ports against the target without the need for host discovery probes. By doing so, you might be able to determine the host's open ports and active services, which can reveal information about the host's condition.

An illustration is nmap -p 1-65535.

Active Reconnaissance: Even if ICMP or conventional ping techniques are banned, take into account employing active reconnaissance techniques, such as sending certain application-level requests or probes to the target server. In order to communicate with the target services directly, this may include utilizing tools like hping or unique scripts.

Firewall Testing: If you believe a firewall or network filtering device is preventing you from conducting scans, you may evaluate the filtering rules and perhaps find open ports using firewall testing tools like firewalk.

8. Explain the difference between a –sS and –sT scan? Which is faster and why?

Ans: When using Nmap to scan open ports on a target machine, the -sS (TCP SYN) and -sT (TCP Connect) searches are two common options. Their methods and the depth of the bonds they build with each other vary.

the TCP SYN Scan (-sS):
A TCP SYN packet is sent to each target port during a SYN scan by Nmap. A SYN-ACK packet is returned by the target if the port is open. Nmap attempts to establish a connection but fails, instead sending a RST (reset) message to break the connection.
Because they don't perform the entire three-way handshake of a typical TCP connection, SYN scans are inconspicuous. As a result, they are less likely to set off firewall or intrusion detection system restrictions.
Due to the fact that they only establish a partial connection, SYN scans are typically quicker than TCP Connect scans. They swiftly decide whether a port is open or closed before moving on to the next port without making a full connection.

Using TCP Connect Scan (-sT),
The three-way handshake is completed by Nmap in a TCP Connect scan to create a full TCP connection with each target port. To finish the connection establishment, it sends a SYN packet, waits for a SYN-ACK response, and then sends an ACK.

Accuracy: Because TCP Connect scans successfully establish a complete connection, they are more accurate because they verify if the port is open. They deliver trustworthy outcomes.
Speed: Due to the time-consuming process of establishing a complete connection for each tested port, TCP Connect scans are often slower than SYN scans.

Which is quicker, and why?
Compared to TCP Connect scans (-sT), SYN scans (-sS) are quicker. SYN scans have a speed advantage due to their incomplete connection establishment. They are effective for speedy port scanning because they can rapidly determine the state of a port and go on to the next port without fully connecting.
However, TCP Connect scans are more trustworthy since they create full connections and offer clear information on open ports. They are useful when precision is crucial and stealth is not a top priority, albeit being slower owing to the complete connection setup.

Your aims will determine whatever scan type you choose. SYN scans are preferred if speed is important and you don't mind a little ambiguity. TCP Connect scans, despite their slower speed, are the best option if precision and a verified open port status are necessary.

Qn. 2 Use the link https://tryhackme.com/room/introtonetworking and complete the Task - Networking Tools Ping, which is Task #5 in that page by reading the tutorial on Networking Tools – Ping and answer all the five questions. **In addition, provide screenshot of the answers**. Note: You need to register in the website using the link -https://tryhackme.com/login to answer the questions**.**

1. What command would you use to ping the bbc.co.uk website?

Ans: ping bbc.co.uk

2. Ping *muirlandoracle.co.uk*
   What is the IPv4 address?

Ans: 217.160.0.152

3. What switch lets you change the interval of sent ping requests?

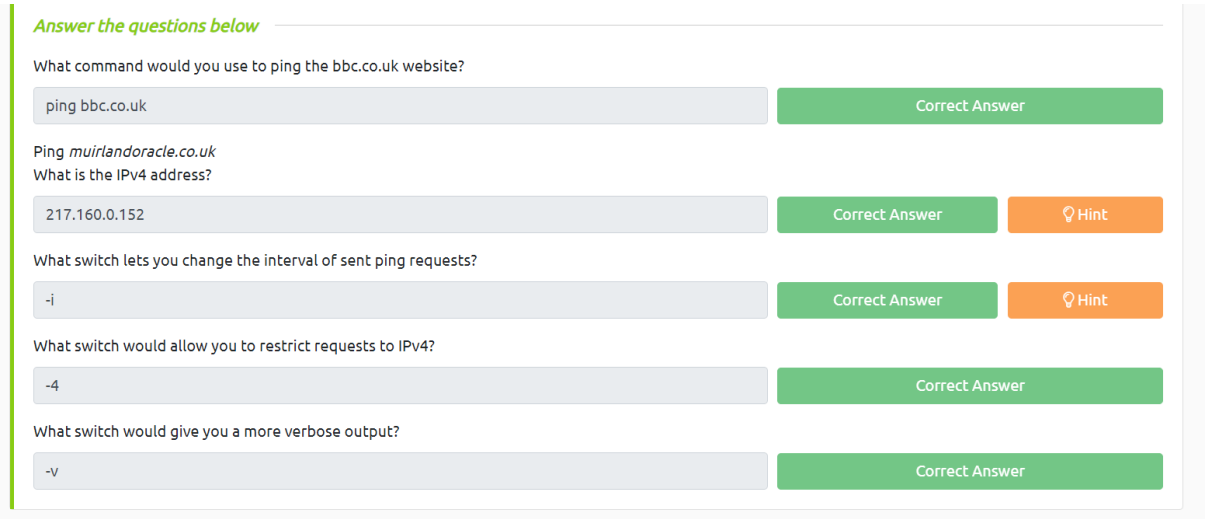
Ans: -i

4. What switch would allow you to restrict requests to IPv4?

Ans: -4

5. What switch would give you a more verbose output?

Ans: -v

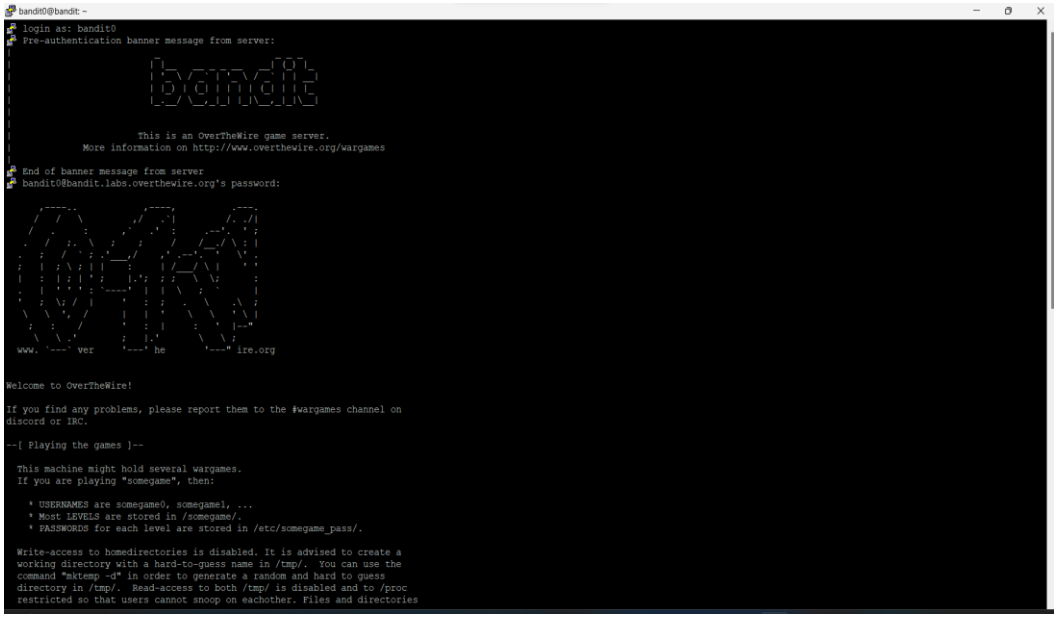


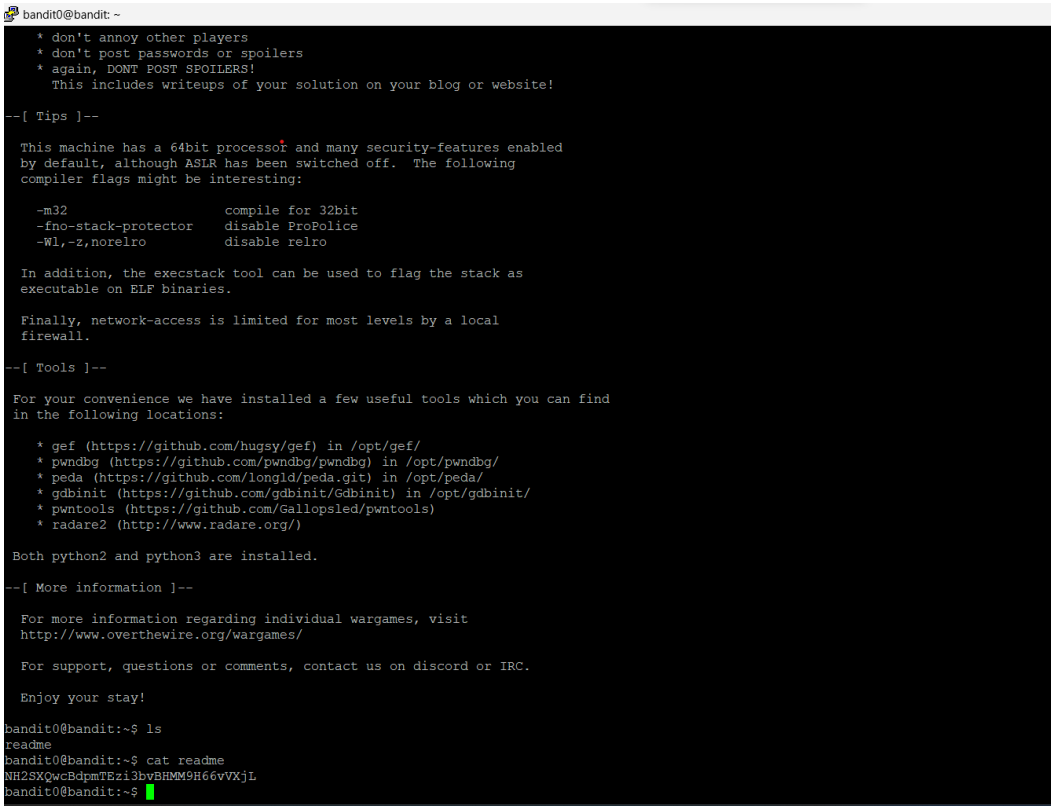
Bandit Level 0

The goal of this level is for you to log into the game using SSH. The host to which you need to connect is bandit.labs.overthewire.org, on port 2220. The username is bandit0 and the password is bandit0. Once logged in, go to the Level 1 page to find out how to beat Level 1.

Bandit Level 0 > Level 1: The password for the next level is stored in a file called readme located in the home directory. Use this password to log into bandit1 using SSH. Whenever you find a password for a level, use SSH (on port 2220) to log into that level and continue the game.

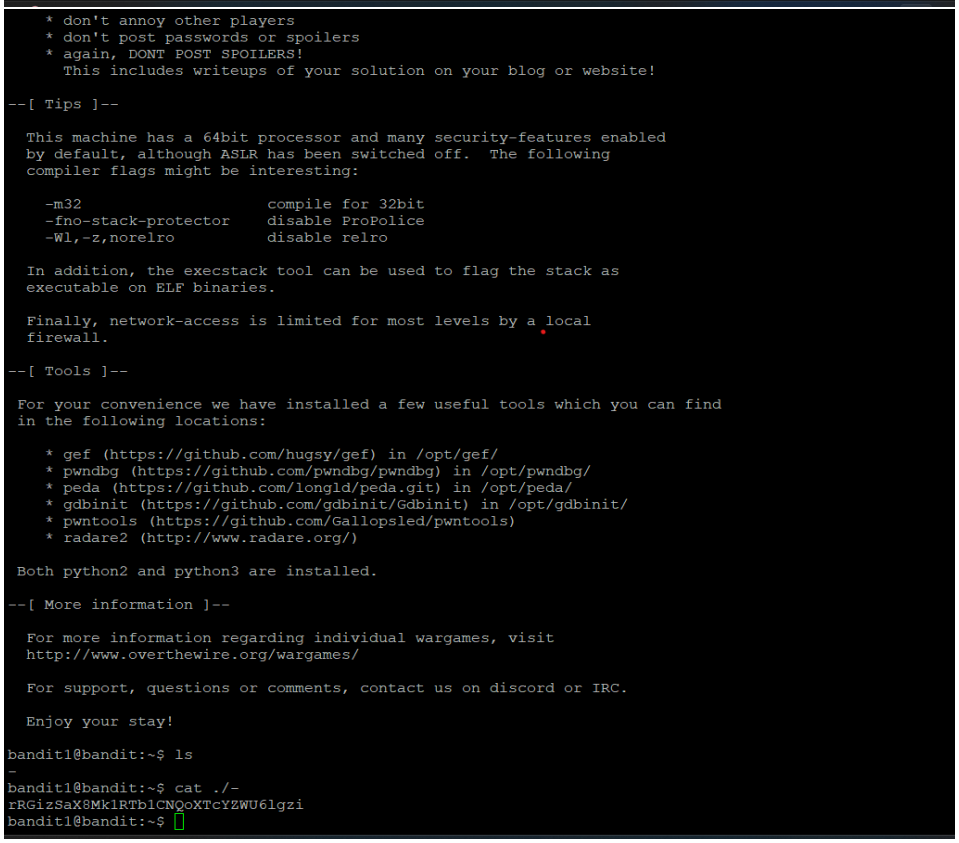
- After login to the bandit0 the command "*cat readme*" the password achieved is:
- Password: NH2SXQwcBdpmTEzi3bvBHMM9H66vVXjL





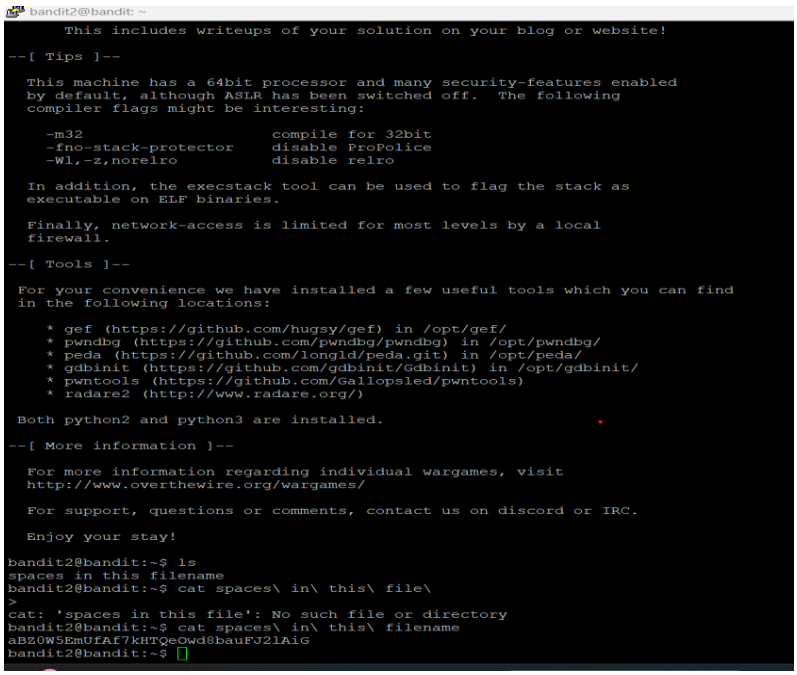
Bandit Level 1 > level 2: The password for the next level is stored in a file called - located in the home Directory

- From using the password achieved from bandit 0 login to bandit level 1
- To open the file name "-"
- Type command "*cat ./-*" to open the file
- Password achieved is: rRGizSaX8Mk1RTb1CNQoXTcYZWU6lgzi



Bandit Level 2 > Level 3: The password for the next level is stored in a file called spaces in this filename located in the home directory

- From using the password achieved from bandit 1 login to bandit level 2
- To open the file name “spaces in this file name”
- Type command “cat spaces\ in\ this\ filename” to open the file
- Password achieved is: aBZ0W5EmUfAf7kHTQeOwd8bauFJ2lAiG



Bandit level 3 > level 4: The password for the next level is stored in a hidden file in the inhere directory.

- From using the password achieved from bandit 2 login to bandit level 3
- To file directory using command “cd inhere”
- For search for list of files in directory type command “ls -a” will get a file name .hidden
- Type command “cat .hidden” to open the file
- Password achieved is: 2EW7BBsr6aMMoJ2HjW067dm8EgX26xNe