Name:THEJAS

REG NO : 145CS20022

Date:02-03-2023

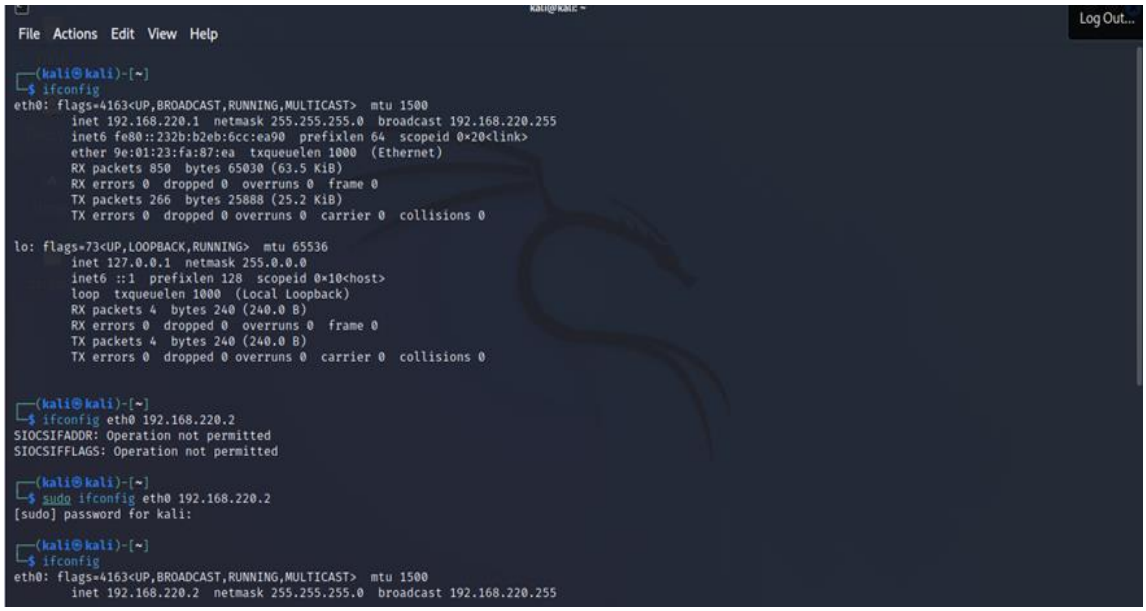
Task:2

1.Perform IP address spoofing:

In IP spoofing, a hacker uses tools to modify the source address in the packet header to make the receiving computer system think the packet is from a trusted source, such as another computer on a legitimate network, and accept it. This occurs at the network level, so there are no external signs of tampering.

$ ifconfig eth0 192.168.209.15

$ ifconfig



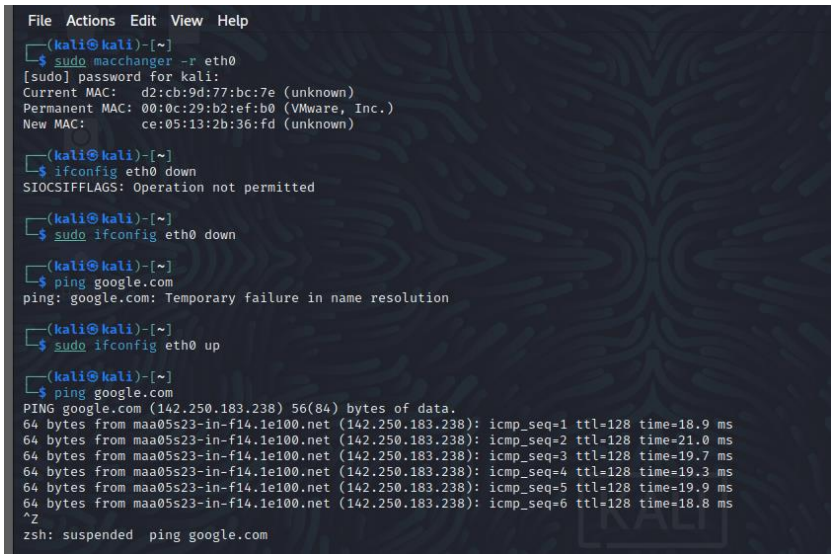
2.Perform MAC address spoofing:

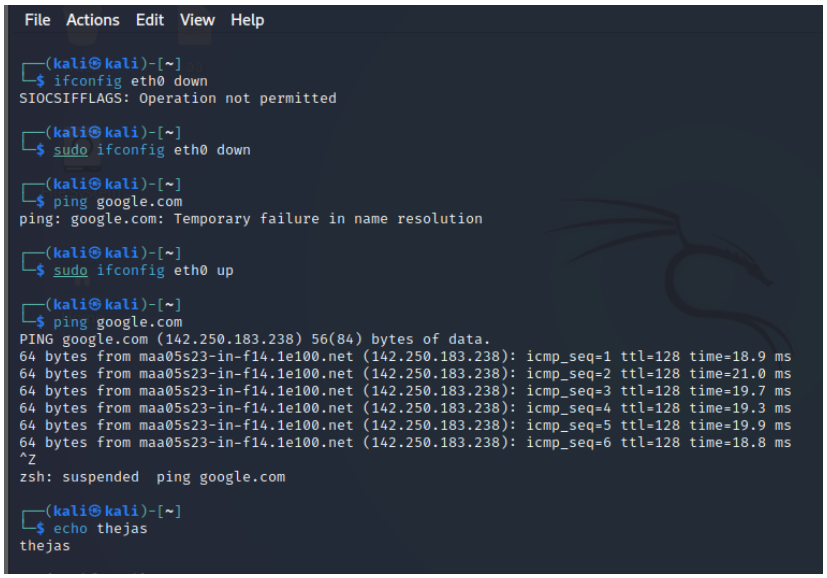
An attacker can mimic your MAC address and redirect data sent to your device to another and access your data. A MAC spoofing attack is when a hacker changes the MAC address of their device to match the MAC address of another on a network in order to gain unauthorized access or launch a Man- in-the-Middle attack.

$ macchanger –s eth0

$ ifconfig

$ macchanger –r eth0



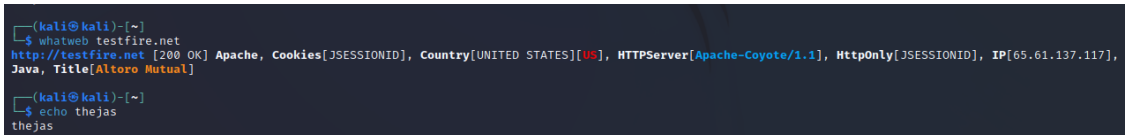


3.Any 5 whatweb commands:

Basic scanning:

The most basic command to scan a website with WhatWeb is:

$ whatwebtestfire.net

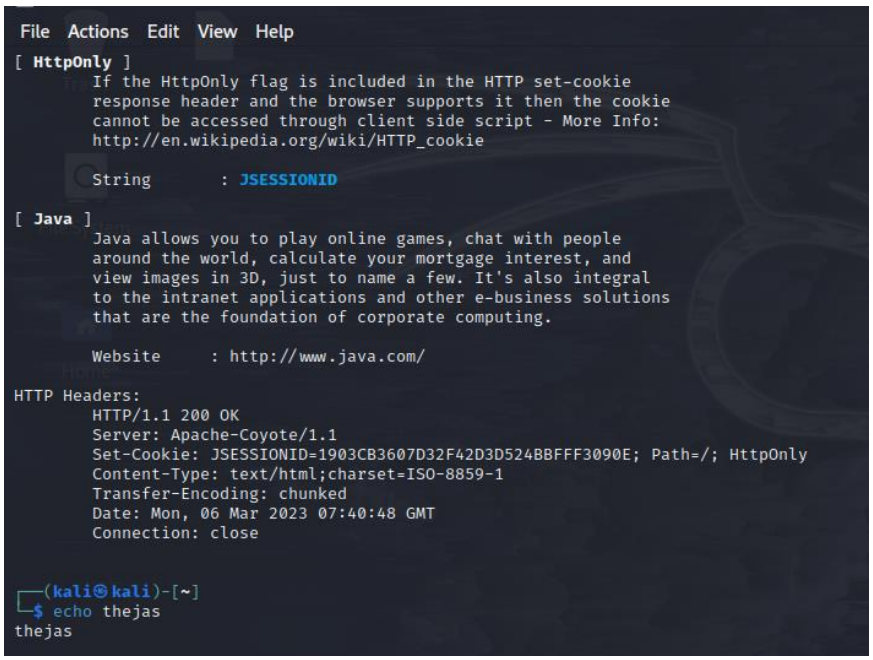


This will perform a default scan of the website and display the identified technologies.

Verbose scanning:

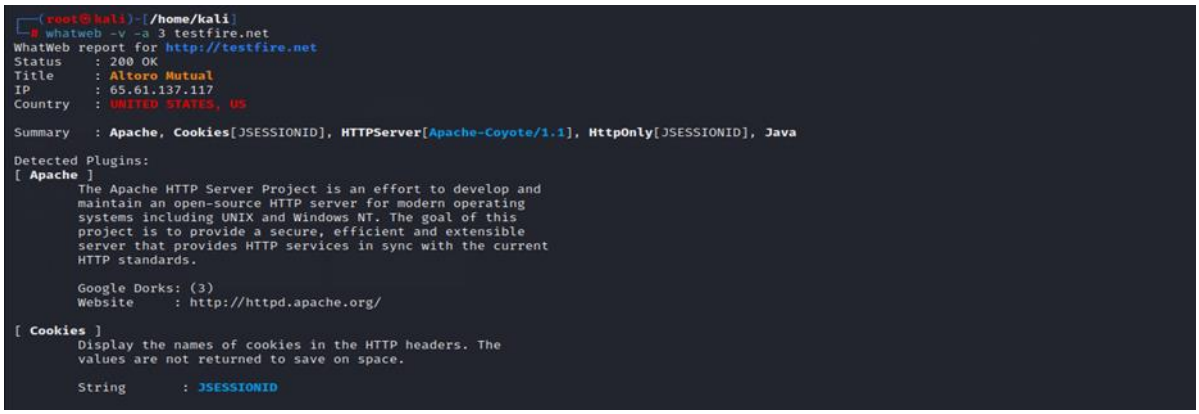
If you want more detailed information about the website, you can use the verbose flag (-v):

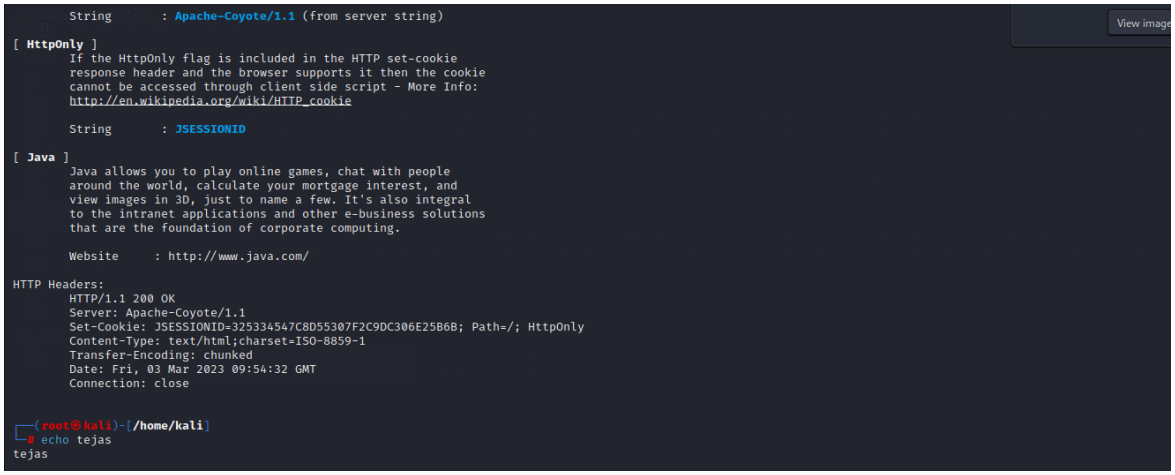
$ whatweb -v [website URL]



This will perform a more thorough scan and provide additional details, such as HTTP headers and server information.

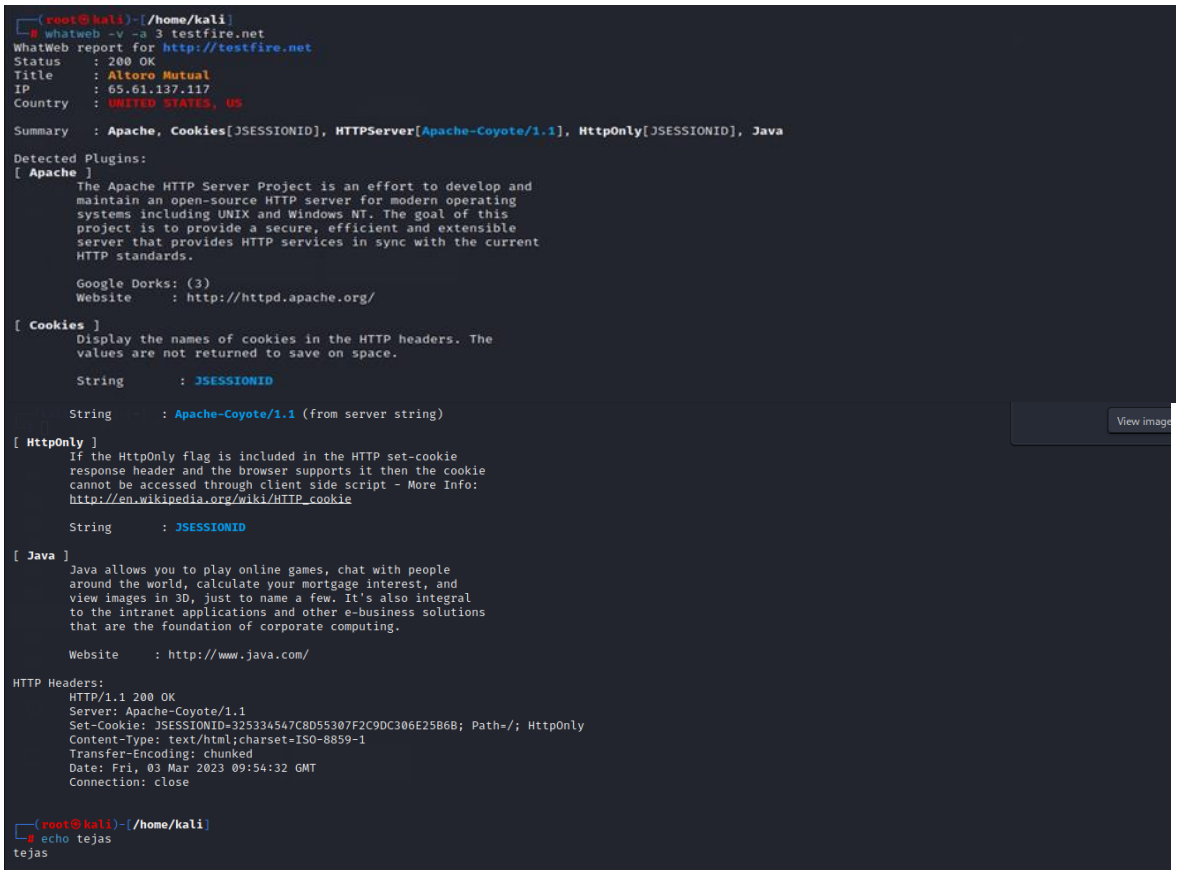
$ whatweb –a 3 testfire.net





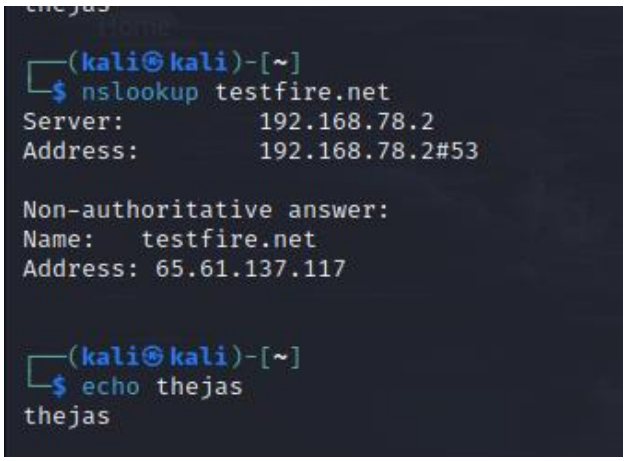
$ whatweb --max –redirect 2 testfire.net

$ whatweb –v –a 3 testfire.net



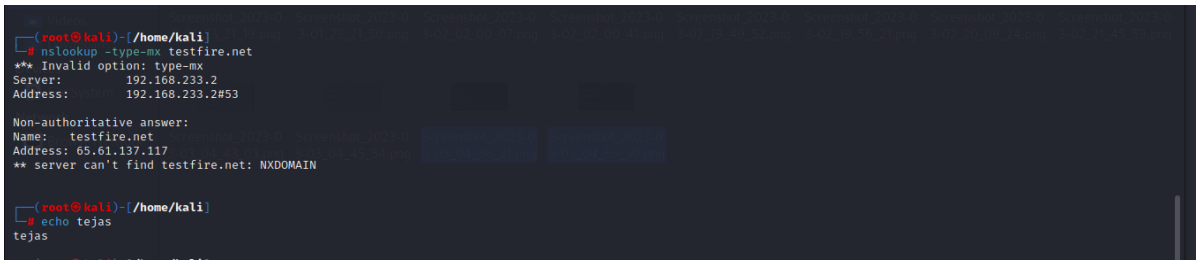
4.Any 5 nslookup commands:

$ nslookuptesfire.net



$ nslookup -type=mx testfire.net

This command will perform a DNS lookup for the mail exchange (MX) records associated with the domain name “testfire.net”.



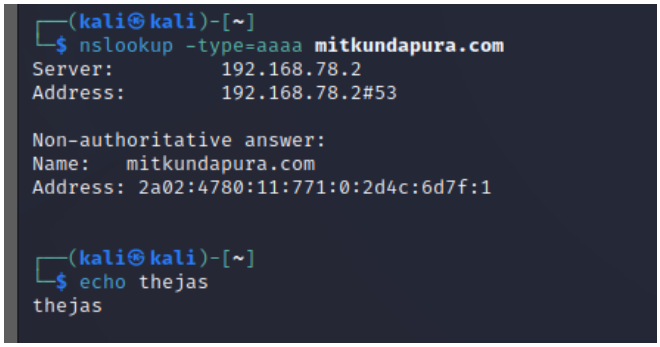
$ nslookup -type=ns testfire.net

This command will perform a DNS lookup for the name server (NS) records associated with the domain name “testfire.net”.

$ nslookup -type=a www.testfire.net

This command will perform a DNS lookup for the IPv6 address associated with the subdomain www.testfire.net

$ Nslookup –type=aaaamitkundapura

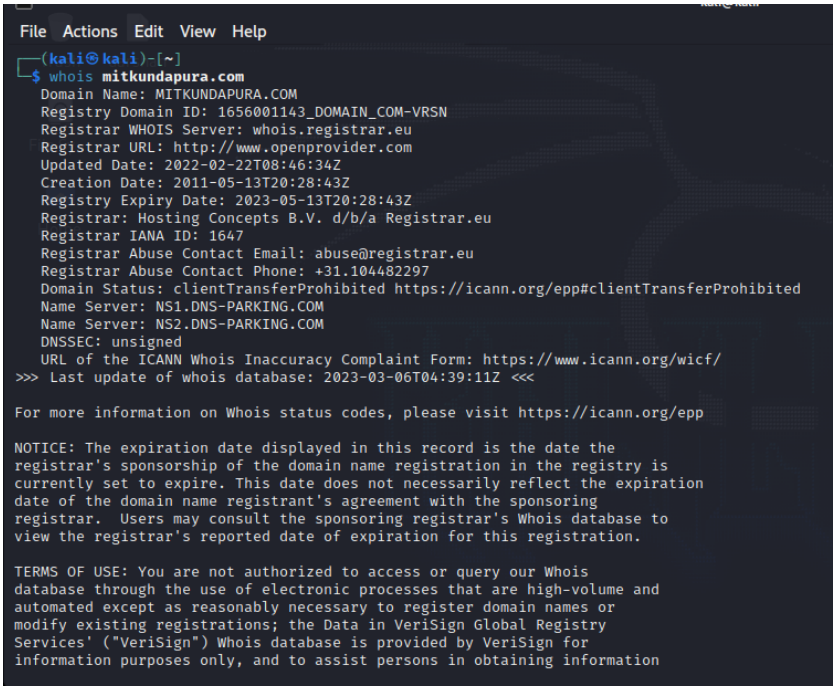


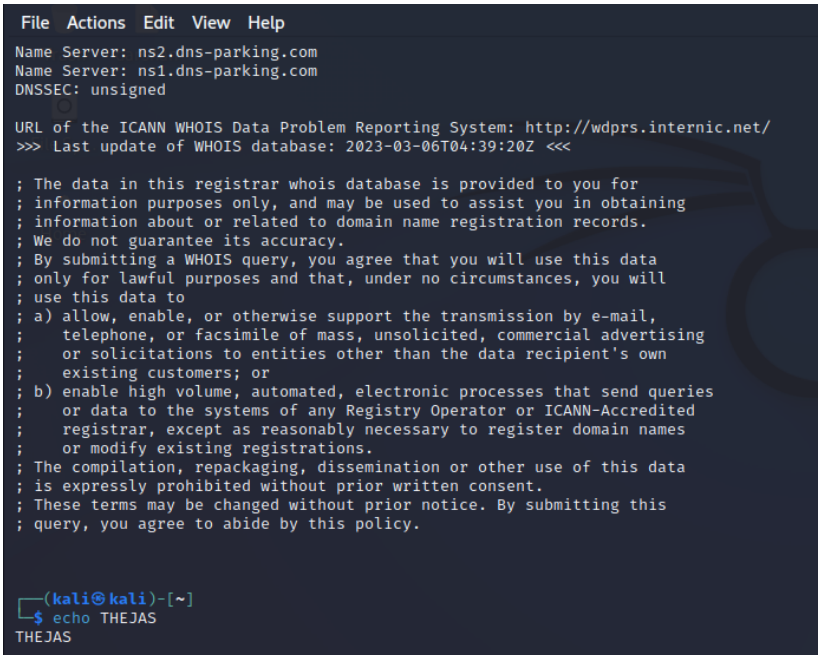
5.whois Commands:

The whois command is a protocol used to look up information about domain names, IP addresses, and other network-related information. Here are some common WHOIS commands:

$ whois mitkundapura.com

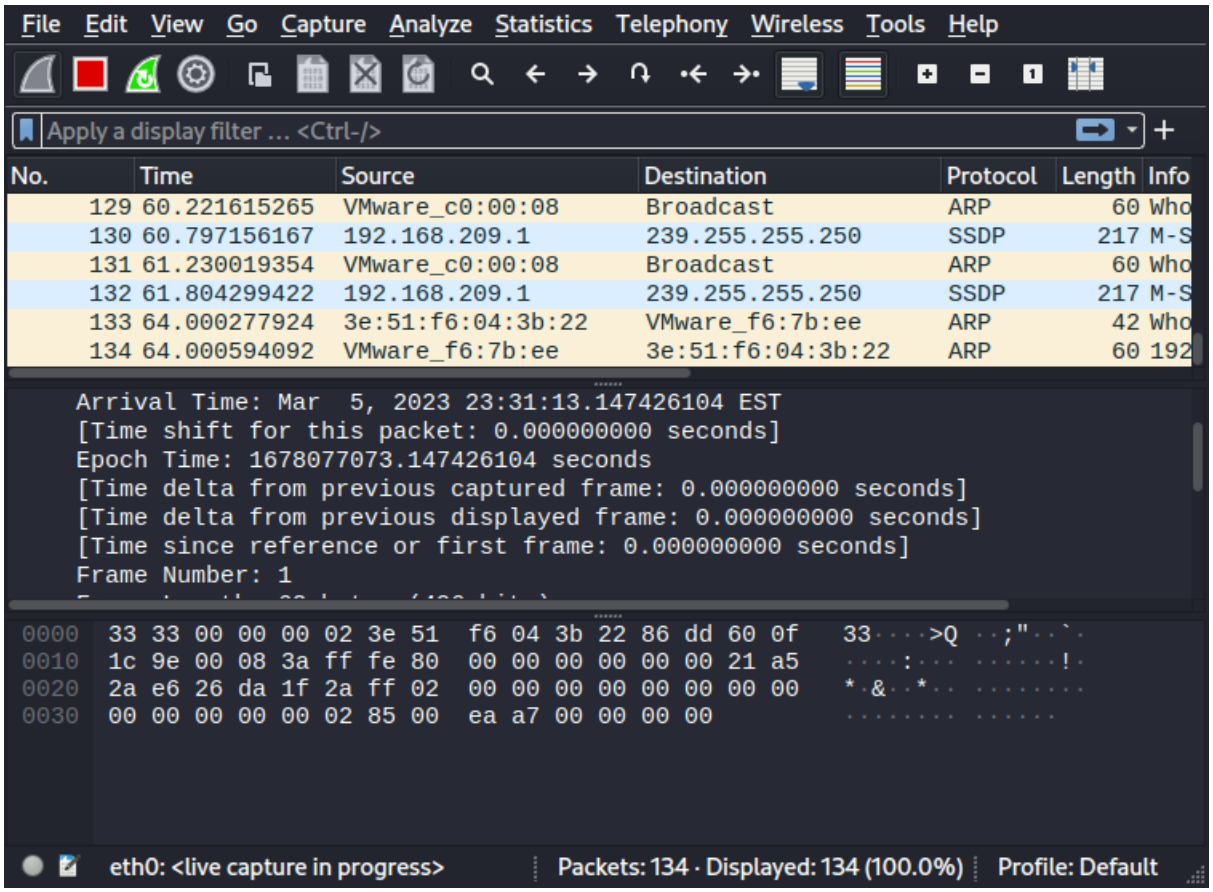
This command will display information about the domain name, such as the name of the registrant, the name servers, and the date of registration





6.Find data packets using wireshark:

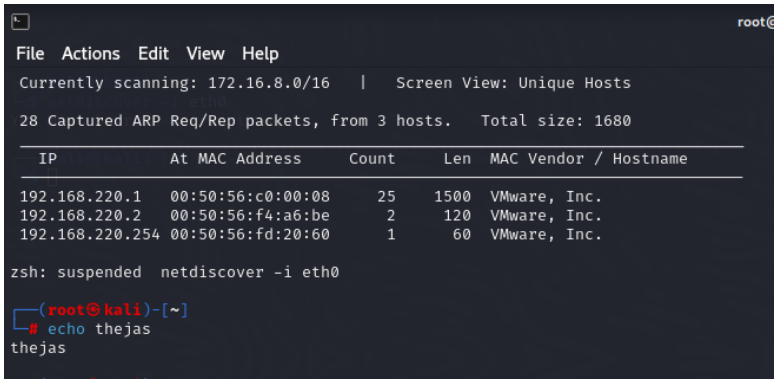
You can easily find packets once you have captured some packets or have read in a previously saved capture file. Simply select Edit Find Packet... in the main menu. Wireshark will open a toolbar between the main toolbar and the packet list, "The "Find Packet" toolbar".



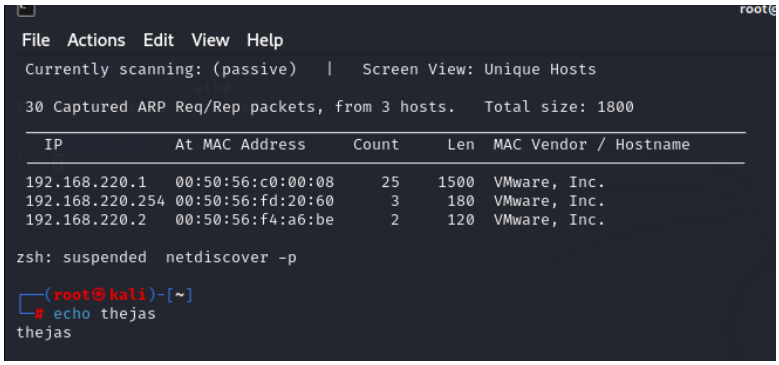
7.Any 5 netdiscover command:

Netdiscover is a network scanning tool used for discovering hosts and gathering information about them on a local network. Here are some of the basic commands:

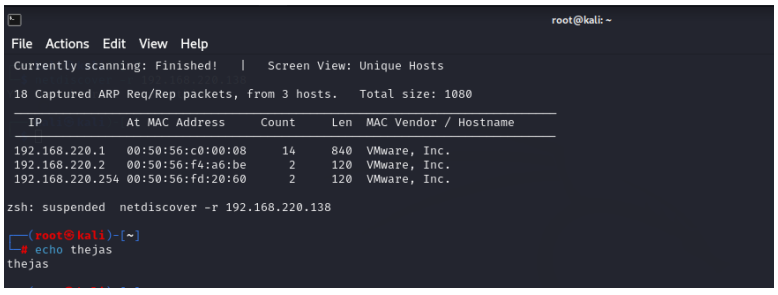
$ netdiscover -i eth0



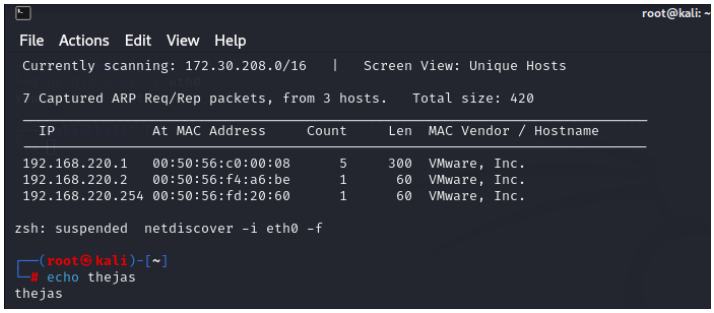
$ netdiscover -p



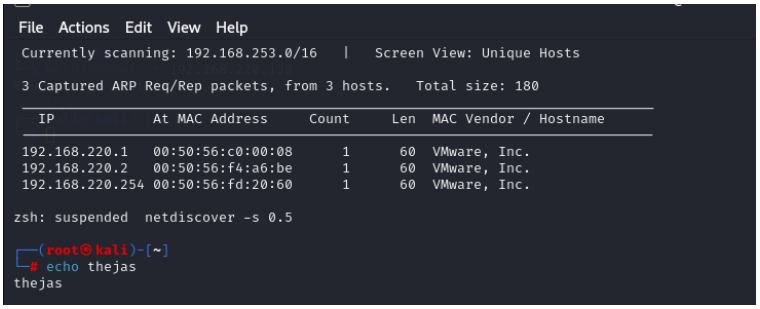
$ netdiscover -r 192.168.0.15



$ netdiscover -i eth0 -f

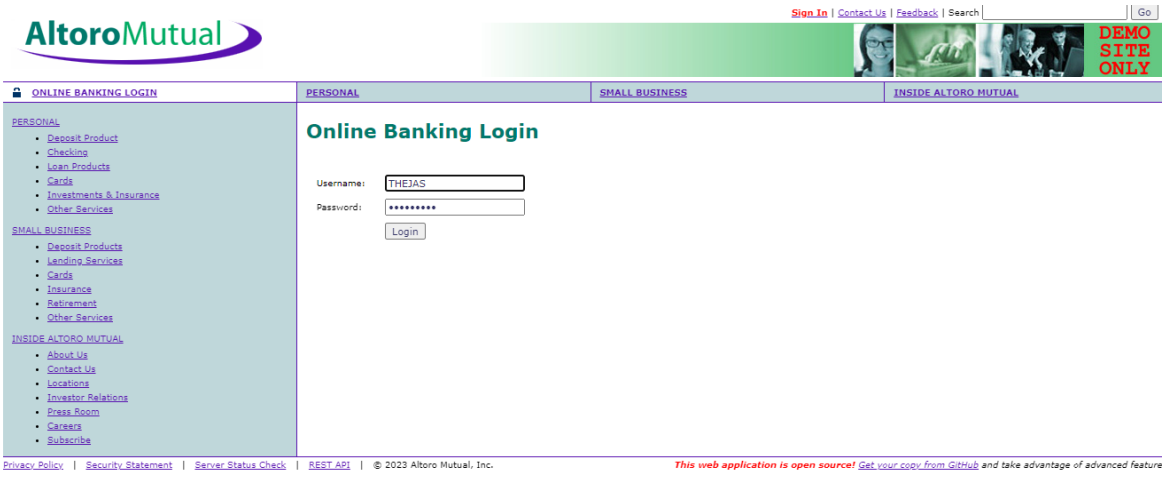


$ netdiscover –s 0.5



8.CryptoConfiguration Flaw:

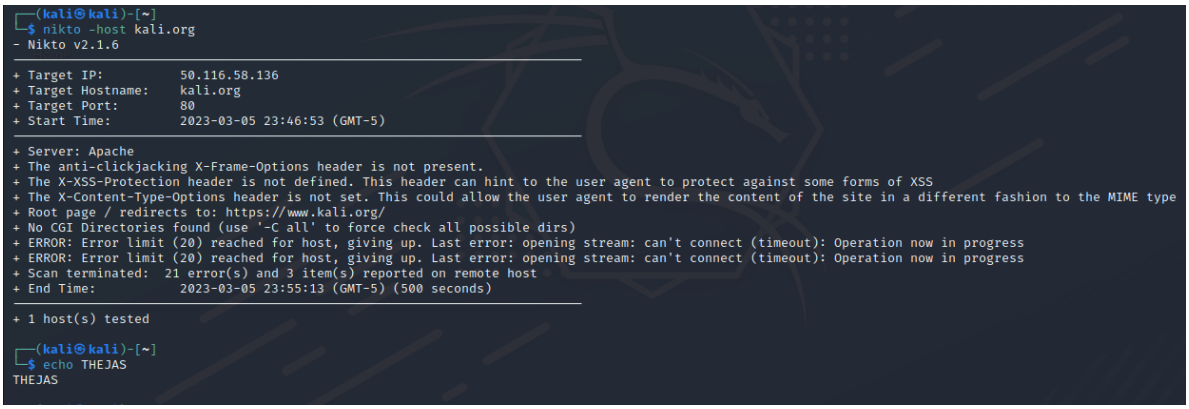
CryptoConfiguration typically refers to the configuration of cryptographic protocols and algorithms used to protect sensitive data and communications.A flaw is context could refers to a weakness or vulnarabilty in the configuration that could that could potentially be exploited by the attackers.



9.Nikto commands:

Nikto is a popular web server scanner that can help you identify potential vulnerabilities on a web server. Here are some common Nikto commands:

$ nikto -host kali.org



10.Find Xml pages in website using dirbuster:

DirBuster is a multi threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within. DirBuster attempts to find these. DirBuster searches for hidden pages and directories on a web server. Sometimes developers will leave a page accessible, but unlinked. DirBuster is meant to find these potential vulnerabilities. This is a Java application developed by OWASP.