SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY
LAB MANUAL

VI SEMESTER

1923607 - NETWORK THREATS AND ATTACKS LABORATORY

Regulation – 2019

ACADEMIC YEAR 2024 – 2025 (EVEN SEMESTER)

PREPARED BY

Ms. C. Jesifica Cinthamani, A.P (O.G) / CYS

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs):

PEO1: To mould students to exhibit top performance in the higher education and research and to become the State–of–the–art technocrat.

PEO2: To impart the necessary background in Cyber Security by providing solid foundation in Mathematical Science and Engineering with security fundamentals.

PEO3: To equip the students with the breadth of Cyber Security threats innovate novel security solutions for the benefit of common man.

PEO4: To groom the students to be multifaceted entrepreneurs with professional ethical attitudein broader social perspective.

PEO5: To provide an ambience learning environment that is conducive for the growth of successful professional career of students.

PROGRAMME OUTCOMES (POs):

After going through the four years of study, our Computer Science and Engineering Graduates will exhibit ability to:

PO#	Graduate Attribute	Programme Outcome
1	Engineering knowledge	Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialisation for the solution of complex engineering problems.
2	Problem analysis	Identify, formulate, research literature, and analyse Complex engineering problems reaching substantiatedconclusions using first principles of mathematics, natural sciences, and engineering sciences.
3	Design/development of solutions	Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for public health and safety, and cultural, societal, and environmental considerations.
4	Conduct investigations of complex problems	Use research–based knowledge and researchMethods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions
5	Modern tool usage	Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools, including prediction and modelling to complex engineering activities, with an understanding of the Limitations.
6	The engineer and society	Apply reasoning informed by the contextual knowledge toassess societal, health, safety, legal, And cultural issues and the consequent responsibilities relevant to the professionalengineering practice
7	Environment and sustainability	Understand the impact of the professionalengineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and Need for sustainable development.
8	Ethics	Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice
9	Individual and team work	Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings
10	Communication	Communicate effectively on complex engineering activities with the engineering community and with the society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receiveclear instructions
11	Project management and finance	Demonstrate knowledge and understanding of the engineering and management principles and apply these toone's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments
12	Life–long learning	Recognize the need for, and have the preparation and ability to engage in independent and life–long learning in the broadest context of technological change

PROGRAM SPECIFIC OUTCOMES (PSOs):

PSO1: Exhibit proficiency in planning, implementing and evaluating team oriented–software Programmingsolutions to specific cyber threat problems and society needs.

PSO2: Demonstrate professional skills in applying programming skills, competency and decision making capability through secure tools with hands–on experiences.

PSO3: Apply logical thinking in analyzing complex real world problems, and use professional and ethicalbehaviors to provide proper solutions to those cyber problems.

PSO4: Demonstrate the ability to work effectively as part of a team in applying security technology to businessand personal situations.

1923607 NETWORK THREATS AND ATTACKS LABORATORY

L T P C

0 0 4 2

OBJECTIVES:

- To learn various network threats.
- To implement the Trojan horses and spyware.
- To implement Denial of service attacks.
- To implement simulate data interception and theft.
- To Implement a code to simulate data modification and

Fabrication

LIST OF EXPERIMENTS

1. Study about various network threats and network attacks
2. Demonstrate Trojan horses and spyware.
3. Detect Denial of service attacks
4. Implement a code to simulate data interception and theft
5. Implement a code to simulate data modification and fabrication
6. Demonstrate Phising attack
7. Study about various protection models.

COURSE OUTCOMES:

- Learn various network threats.
- Implement the Trojan horses and spyware.
- Implement Denial of service attacks.
- Implement simulate data interception and theft.
- Implement a code to simulate data modification and fabrication

Course Outcomes	Programme Outcomes (PO)												PSO			
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4
CO 1	1	2		3									3		1	
CO 2		2		3									2	2		
CO 3	1		2										3		1	
CO 4	2	1		3									3			
CO 5	2		3	3									1		3	

INDEX

1. STUDY ABOUT VARIOUS NETWORK THREATS AND NETWORK ATTACKS

AIM:

To Study about various network threats and network attacks

DESCRIPTION:

Network threats refer to any malicious or potentially harmful activity that targets a computer network, its infrastructure, or its users. These threats can come from a variety of sources, such as cybercriminals, hackers, insiders, or even natural disasters. A network attack is a type of cyberattack that targets computer networks, systems, and devices to gain unauthorized access, steal sensitive information, or disrupt normal operations. Network attacks can be carried out through various methods, including malware, social engineering, and exploiting vulnerabilities in software or hardware. Network threats and attacks are potential risks to the security and integrity of computer networks and their data. Here are some of the most common network threats and attacks:

MALWARE:

Malware refers to malicious software designed to harm computers or networks. Malware are malicious software programs used to gather information about victims through compromised devices. After successful deployments, hackers can mine devices for classified information and use them to commit identity theft, blackmail, or other business-damaging actions. Examples include viruses, worms, Trojan horses, and ransomware. Malware is a type of software that is designed to harm or exploit computer systems, networks, or devices. The term "malware" is a combination of the words "malicious" and "software." Malware can take many forms, including viruses, worms, Trojans, ransomware, spyware, and adware.

Here are some examples of malware:

Virus:
A virus is a type of malware that can replicate itself and spread to other systems or devices. It often attaches itself to a legitimate program or file, and can cause damage by deleting files or stealing data. Examples of viruses include the Melissa virus and the ILOVEYOU virus.

Worm:
A worm is a self-replicating malware program that can spread across networks or the internet. Worms do not need to attach themselves to a host program, and can spread by exploiting vulnerabilities in network software or systems. Examples of worms include the Conficker worm and the Code Red worm.

Trojan:
A Trojan, or Trojan horse, is a type of malware that masquerades as a legitimate program, but actually contains hidden malicious code. Trojans can be used to steal data, spy on users, or give

attackers remote control over a system. Examples of Trojans include the Zeus Trojan and the Backdoor Rustock.A Trojan.

Ransomware:
Ransomware is a type of malware that encrypts a user's files or locks them out of their system, and demands a ransom payment in exchange for the decryption key or access. Examples of ransomware include WannaCry and Petya.

Spyware:
Spyware is a type of malware that is designed to spy on a user's activities or steal their personal information. Spyware can monitor keystrokes, track web browsing, and capture login credentials. Examples of spyware include the Zango spyware and the CoolWebSearch spyware.

Adware:
Adware is a type of malware that displays unwanted advertisements or pop-ups on a user's device or browser. Adware can slow down a system and make it more vulnerable to other types of malware. Examples of adware include the Superfish adware and the Conduit adware.

Malware can be spread through various means, such as email attachments, malicious websites, infected software downloads, and social engineering attacks. To protect against malware, users should keep their software up-to-date, use anti-virus and anti-malware software, and exercise caution when downloading or opening files from unknown sources.

PHISHING:

Phishing is a type of social engineering attack that tricks users into revealing sensitive information, such as passwords and credit card numbers. Phishing attacks can be carried out through email, text messages, or social media. Phishing attacks are scams where hackers disguise themselves as a trusted entity and attempt to gain access to networks and steal personal information, such as credit card details. Phishing scams take the form of emails, text messages, or phone calls. Similar to rogue security software, phishing attacks are designed to appear legitimate. This encourages victims to click on malicious links or download malware-laden attachments.
Types of Phishing attacks are Spear Phishing, Whaling, Vishing, Email Phishing.
Phishing is a type of social engineering attack where an attacker impersonates a trustworthy entity or person to trick a victim into revealing sensitive information or performing an action that they shouldn't. The goal of phishing is to steal personal or financial information, install malware, or gain unauthorized access to systems or networks.

Here are some examples of phishing attacks:

Email phishing:
An attacker sends an email that appears to be from a legitimate source, such as a bank, social media platform, or online retailer, and asks the victim to click on a link or download an attachment. The link or attachment is designed to install malware or direct the victim to a fake website where they are asked to enter their login credentials or personal information.

Spear phishing:
Spear phishing is a more targeted type of phishing attack where the attacker gathers information about the victim, such as their name, job title, or employer, and uses this information to create a

more convincing phishing email or message. For example, an attacker may impersonate a CEO or other high-ranking executive and request sensitive information from an employee.

Smishing:

Smishing, or SMS phishing, is a type of phishing attack that uses text messages to trick victims into revealing sensitive information or clicking on a link. Smishing messages often appear to be from a legitimate source, such as a bank or government agency, and may ask the victim to verify their account or click on a link to claim a prize.

Vishing:

Vishing, or voice phishing, is a type of phishing attack that uses phone calls to trick victims into revealing sensitive information. Vishing attacks often involve the attacker posing as a representative of a bank or other financial institution and asking the victim to verify their account information or enter their PIN.

Clone phishing:

Clone phishing is a type of phishing attack where the attacker creates a nearly identical copy of a legitimate email or message, but replaces a legitimate link or attachment with a malicious one. Clone phishing messages often appear to be from a trusted sender, such as a coworker or vendor, and may contain urgent or sensitive information.

To protect against phishing attacks, users should be cautious of unexpected emails, messages, or phone calls, and should never click on links or download attachments from unknown sources. Users should also verify the legitimacy of emails or messages by checking the sender's email address or phone number, and by contacting the sender directly to confirm the request.

DENIAL OF SERVICE (DOS) AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS:

DoS and DDoS attacks are designed to overwhelm a network or system with excessive traffic, making it unavailable to legitimate users. In a DoS attack, the traffic comes from a single source, while in a DDoS attack, the traffic comes from multiple sources. A DDoS attack causes websites to crash, malfunction, or experience slow loading times. cybercriminals infect internet-connected devices and convert them into bots. Hackers send the bots to a victim's IP address. This results in a high volume of internet traffic bombarding the website with requests and causing it to go offline. Some examples are: AWS Attack in 2020, Mirai Krebs Attacks in 2016, Mirai Dyn Attack in 2016, GitHub Attack in 2018, Cloud Flare Attack in 2014. A Denial of Service (DoS) attack is a type of cyberattack that attempts to disrupt or disable access to a website, server, or network by overwhelming it with traffic or requests. The goal of a DoS attack is to render the targeted system or network unavailable to users, causing disruption or financial losses for the organization.

Here are some examples of DoS attacks:

Ping flood:

A ping flood attack sends a large number of ping requests to a server or network, overwhelming it with traffic and causing it to crash or become unresponsive.

Distributed Denial of Service (DDoS):

A DDoS attack uses a network of compromised devices, called a botnet, to send a large number of requests or traffic to a targeted server or network. The combined traffic from the botnet can overwhelm the system, causing it to crash or become unavailable. The Mirai botnet is one example of a DDoS attack.

SYN flood:
A SYN flood attack exploits a vulnerability in the TCP/IP protocol by sending a large number of SYN requests to a server, but never completing the three-way handshake required to establish a connection. This leaves the server in a state of waiting, using up resources and potentially causing it to crash or become unresponsive.

HTTP flood:
An HTTP flood attack sends a large number of HTTP requests to a server, causing it to become overwhelmed and potentially crash or become unresponsive.

Slowloris:
A Slowloris attack sends a large number of HTTP requests to a server, but keeps the connections open and sends data slowly over a long period of time. This keeps the server's resources tied up, causing it to become unresponsive or crash.

DoS attacks can be difficult to prevent or mitigate, as they often involve a large amount of traffic that is difficult to distinguish from legitimate traffic. To protect against DoS attacks, organizations can use anti-DDoS services or technologies, implement rate limiting and traffic filtering, and have a robust incident response plan in place.

MAN-IN-THE-MIDDLE (MITM) ATTACKS:

MitM attacks occur when an attacker intercepts communication between two parties and can eavesdrop, manipulate or impersonate one or both parties. This is typically achieved by compromising the network infrastructure, such as a router or switch. Man-in-the-middle (MITM) network attacks occur when malicious parties intercept traffic conveyed between networks and external data sources or within a network. In most cases, hackers achieve man-in-the-middle attacks via weak security protocols. These enable hackers to convey themselves as a relay or proxy account and manipulate data in real-time transactions. A Man-in-the-Middle (MitM) attack is a type of cyberattack where an attacker intercepts communications between two parties to steal information or alter the contents of the communication. The attacker can insert themselves between the two parties and monitor or manipulate the information being exchanged, without the knowledge or consent of either party.

Here are some examples of MitM attacks:

Wi-Fi eavesdropping:
An attacker can intercept and monitor traffic between a device and a Wi-Fi network by setting up a rogue access point or by using a Wi-Fi sniffer. This allows the attacker to steal sensitive information, such as login credentials or financial data.

DNS spoofing:
DNS spoofing involves redirecting a victim's traffic to a fake website or server by altering the DNS resolution process. This allows the attacker to steal login credentials, financial data, or other sensitive information.

Email hijacking:
An attacker can intercept and alter emails by compromising the email server or by using malware to gain access to a victim's email account. This allows the attacker to read, modify, or delete emails, and to impersonate the victim in further communications.

IP spoofing: IP spoofing involves forging the source IP address of a communication to impersonate a legitimate sender or to hide the attacker's identity. This can be used to launch other types of attacks, such as DoS attacks or port scanning.

HTTPS spoofing:
HTTPS spoofing involves creating a fake SSL certificate to impersonate a legitimate website, and then intercepting and altering traffic between the victim's device and the fake website. This allows the attacker to steal login credentials, financial data, or other sensitive information.

MitM attacks can be difficult to detect and prevent, as they often involve sophisticated techniques and exploit vulnerabilities in the communication protocols or software. To protect against MitM attacks, organizations can use secure communication protocols, such as HTTPS and VPN, and implement strong authentication and encryption mechanisms. Users should also be cautious of unexpected or suspicious communications, and should verify the identity and authenticity of the sender before sharing sensitive information.

PASSWORD ATTACKS:

Password attacks involve attempting to gain unauthorized access to a system by cracking or guessing passwords. This includes brute-force attacks, where an attacker tries a large number of passwords until the correct one is found. Unauthorized access refers to network attacks where malicious parties gain access to enterprise assets without seeking permission. Such incidences may occur due to weak account password protection, unencrypted networks, insider threats that abuse role privileges, and the exploitation of inactive roles with administrator rights. Password attacks are a type of cyberattack that attempt to gain unauthorized access to a system or account by guessing or cracking the password. Password attacks can be carried out using various techniques and tools, and can be highly effective if the password is weak or easily guessable.

Here are some examples of password attacks:

Brute force attack:
A brute force attack involves attempting to guess the password by trying every possible combination of characters until the correct password is found. This type of attack can be time-consuming and resource-intensive, but can be successful if the password is short or simple.

Dictionary attack:
A dictionary attack involves using a pre-computed list of commonly used passwords or words from a dictionary to guess the password. This type of attack is faster than a brute force attack and can be highly effective if the password is a common word or phrase.

Social engineering:
Social engineering attacks involve tricking the user into revealing their password through persuasion or deception. This can include phishing emails or phone calls, where the attacker impersonates a trusted source and asks the user to reveal their password.

Password spraying:
Password spraying involves using a small list of commonly used passwords to attempt to gain access to multiple accounts. This type of attack is more targeted than a brute force attack and can be highly effective if the password is a commonly used one.

Keylogging:
Keylogging involves using malware to record every keystroke entered by the user, including passwords. This type of attack can be highly effective if the malware is installed on the victim's device.

To protect against password attacks, users and organizations can implement strong password policies, such as requiring longer and more complex passwords, and enforcing regular password changes. Two-factor authentication can also be used to add an extra layer of security, requiring a second factor, such as a code or biometric verification, to access the account. Users should also be cautious of suspicious emails or requests, and should never reveal their passwords to anyone.

SQL INJECTION:

SQL injection attacks involve injecting malicious code into a database query, which can allow an attacker to access or manipulate sensitive data. Unmoderated user data inputs could place organizational networks at risk of SQL injection attacks. Under the network attack method, external parties manipulate forms by submitting malicious codes in place of expected data values. They compromise the network and access sensitive data such as user passwords. SQL injection is a type of cyberattack that targets the database of a web application by inserting malicious SQL code into the input fields of a web form. SQL injection attacks can result in unauthorized access to sensitive data or the modification or deletion of data in the database.

Here are some examples of SQL injection attacks:

Login bypass:
An attacker can insert a malicious SQL query into the login form of a web application to bypass the authentication mechanism and gain access to the system without a valid username and password.

Data extraction:
An attacker can use SQL injection to extract sensitive data from the database, such as login credentials, credit card numbers, or personal information.

Database modification:
An attacker can use SQL injection to modify or delete data in the database, such as changing the password of a user or deleting an entire table.

Command injection:
An attacker can use SQL injection to execute system commands on the server hosting the web application, potentially gaining complete control over the system.

CROSS-SITE SCRIPTING (XSS):

XSS attacks occur when an attacker injects malicious code into a website, which can be executed by unsuspecting users who visit the site. This can allow the attacker to steal sensitive information, such as login credentials. Cross-site scripting (XSS) is a type of cyberattack that targets web applications by injecting malicious code into web pages viewed by other users. XSS attacks can be used to steal sensitive information, such as login credentials or personal data, or to hijack user sessions and carry out unauthorized actions on behalf of the victim.

Here are some examples of XSS attacks:

Reflected XSS:
In a reflected XSS attack, an attacker injects malicious code into a web page that is immediately returned to the user by the web application. This can happen when the web application doesn't properly sanitize user input, such as search queries or form data. When the user views the infected web page, the malicious code is executed in their browser, allowing the attacker to steal their data or hijack their session.

Stored XSS:
In a stored XSS attack, an attacker injects malicious code into a web page that is permanently stored on the server and served to all users who view the page. This can happen when the web application allows users to post comments or other content that is not properly sanitized. When other users view the infected web page, the malicious code is executed in their browser, allowing the attacker to steal their data or hijack their session.

DOM-based XSS:
In a DOM-based XSS attack, an attacker injects malicious code that is executed in the victim's browser, but is not sent to the server. This can happen when the web application uses JavaScript to dynamically update the content of the web page based on user input. If the JavaScript code doesn't properly sanitize user input, an attacker can inject malicious code that is executed in the browser.

EAVESDROPPING:

Eavesdropping is the act of intercepting and monitoring network traffic to obtain sensitive information. This can be accomplished using a network sniffer or by compromising a network device. Eavesdropping is a type of cyberattack that involves intercepting and monitoring communications between two parties without their knowledge or consent. This can allow attackers to steal sensitive information, such as login credentials, financial data, or personal information.

Here are some examples of eavesdropping attacks:

Packet sniffing:
In a packet sniffing attack, an attacker intercepts and monitors network traffic to capture data packets that contain sensitive information, such as usernames and passwords. This can be done using specialized software or hardware that can capture and analyze network traffic.

Wireless eavesdropping:
In a wireless eavesdropping attack, an attacker intercepts and monitors wireless communications between devices, such as Wi-Fi or Bluetooth signals. This can be done using specialized antennas or software that can capture and decode wireless signals.

SHOULDER SURFING:

In a shoulder surfing attack, an attacker physically observes a user entering sensitive information, such as a password or PIN, by looking over their shoulder or from a distance. This can be done in public places, such as coffee shops or airports, where users are more likely to use their devices in public. Here's an example of a packet sniffing attack: Suppose there's a user who logs into their bank account using a web browser over an unsecured Wi-Fi network, such as a public Wi-Fi hotspot. An attacker who is also connected to the same network can use packet sniffing software to intercept and capture the user's network traffic. When the user enters their login credentials, such as their username and password, the data packets containing this information are sent over the network in plaintext, which means that anyone who intercepts them can read the data. The attacker can capture and analyze these packets using packet sniffing software, and extract the user's login credentials from the captured data. To protect against eavesdropping attacks, users should avoid using unsecured public Wi-Fi networks and use encrypted connections, such as HTTPS or VPNs, to protect their communications. Organizations should also implement network security measures, such as encryption and firewalls, to protect against eavesdropping attacks.

INSIDER THREATS:

These are threats posed by individuals within an organization who have access to sensitive information or systems, and may intentionally or unintentionally cause harm. Insider threats refer to security risks posed by individuals who have authorized access to an organization's systems, data, or facilities. These individuals can be employees, contractors, or even business partners. Insider threats can be intentional, such as when an employee steals sensitive data for personal gain, or unintentional, such as when an employee inadvertently exposes confidential information.

Here are some examples of insider threats:

Data theft:
An employee may intentionally steal sensitive data, such as customer information, trade secrets, or financial data, for personal gain. For example, a financial analyst may steal confidential financial information to profit from insider trading.

Misuse of access privileges:
An employee with elevated access privileges may use their permissions to carry out unauthorized activities, such as changing system configurations or deleting critical files. For example, a system administrator may use their access privileges to delete sensitive data or modify system settings.

Accidental exposure:
An employee may accidentally expose sensitive data, such as through an email attachment or a misconfigured cloud storage account. For example, an employee may send an email with sensitive information to the wrong recipient or accidentally share confidential files on a public file-sharing platform.

Sabotage:
An employee may intentionally sabotage an organization's systems or data, such as by deleting critical files or introducing malware. For example, a disgruntled employee may delete important data on their last day of work to cause damage to the company.

Social engineering:
An employee may unknowingly fall victim to a social engineering attack, such as a phishing email or a phone scam. For example, an attacker may impersonate a company executive and request sensitive information from an employee.

Malicious insiders:
A malicious insider is an employee who intentionally causes harm to their organization. This can include stealing data, sabotaging systems, or even physically damaging equipment. For example, an IT employee may plant a logic bomb in a critical system to cause it to fail at a specific time.

Insider threats can be difficult to detect and prevent, as the individuals involved may have legitimate access to the organization's systems and data. To mitigate the risk of insider threats, organizations should implement strong access controls, monitor employee activity, conduct regular security training, and establish clear policies and procedures for data handling and incident response.These are just a few examples of the many network threats and attacks that exist. It is important to have appropriate security measures in place, such as firewalls, intrusion detection systems, and encryption, to protect against these threats.

Network threats can be difficult to detect and mitigate, and can have serious consequences, such as data breaches, financial loss, and reputational damage. As such, it's important for organizations to take proactive steps to protect their networks from these threats, including implementing strong security policies, using firewalls and antivirus software, conducting regular security audits, and providing employee training on cybersecurity best practices.

2 . DEMONSTRATION OF TROJAN HORSES AND SPYWARE

AIM:

To demonstrate Trojan Horses and Spyware

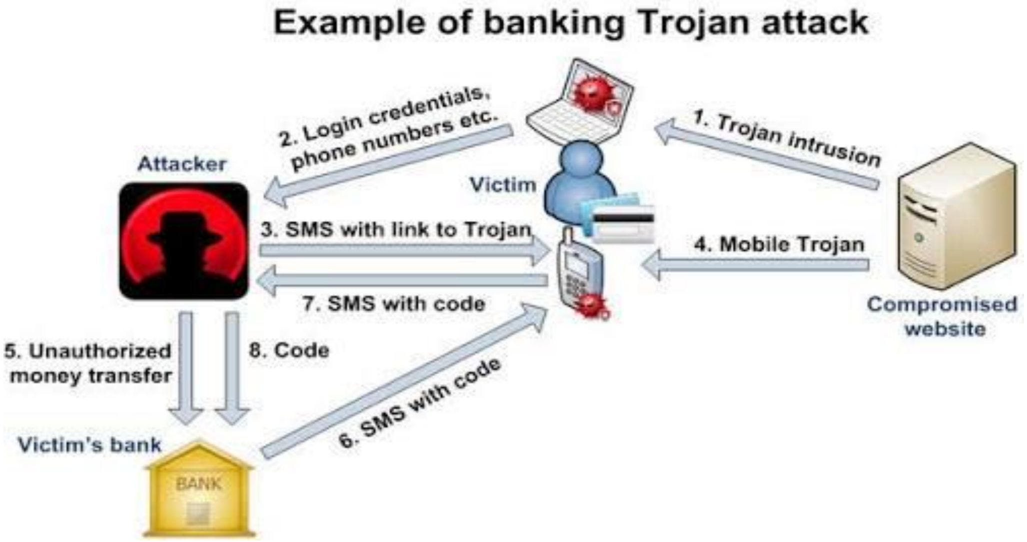
DESCRIPTION:

Trojan horses and spyware are two types of malware that can infect computers and networks, often with the goal of stealing sensitive information or giving an attacker control over the system.

TROJAN HORSES:

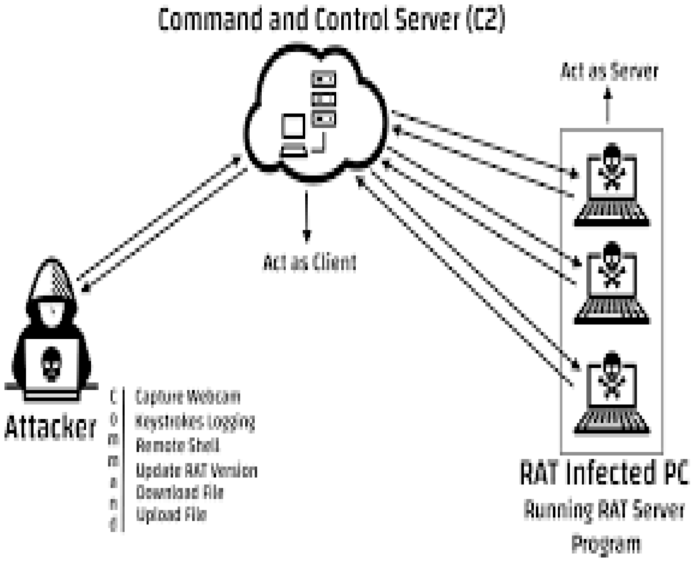
A Trojan horse is a type of malware that disguises itself as a harmless or desirable program, such as a game or utility, but in reality, it contains malicious code that can harm a system. Once the Trojan horse is downloaded and executed, it can perform a variety of actions, such as stealing data, installing additional malware, or giving an attacker remote access to the system. For example, a Trojan horse could be disguised as a popular game download. Once a user downloads and installs the game, the Trojan horse could be executed and start stealing data from the user's system, such as login credentials, financial information, or personal documents.

Example:
QakBot is an eCrime banking trojan that can spread laterally throughout a network utilizing a worm-like functionality through brute-forcing network shares and Active Directory user group accounts, or via server message block (SMB) exploitation. Despite QakBot's anti-analysis and evasive capabilities, the CrowdStrike Falcon platform prevents this malware from completing its execution chain when it detects the VBScript execution.


Example of banking Trojan attack
Attacker
2. Login credentials, phone numbers etc.
Victim
1. Trojan intrusion
3. SMS with link to Trojan
4. Mobile Trojan
7. SMS with code
Compromised website
5. Unauthorized money transfer
8. Code
6. SMS with code
Victim's bank
BANK

How Do Trojans Work:

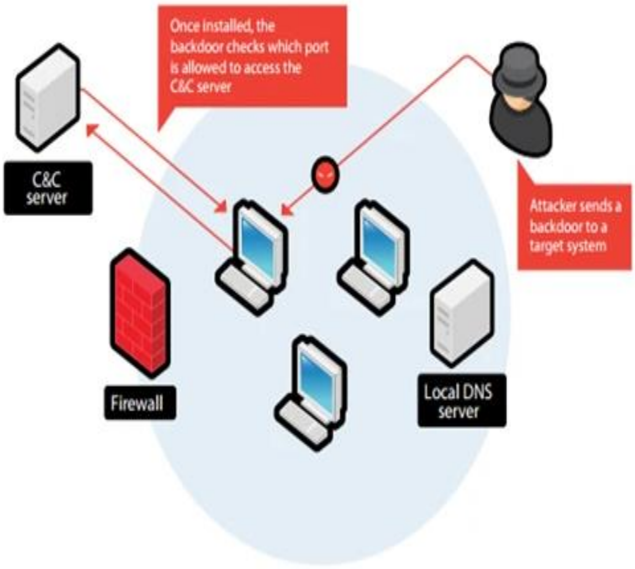
Unlike computer viruses, a Trojan horse cannot manifest by itself, so it needs a user to download the server side of the application for it to work. This means the executable (.exe) file should be implemented and the program installed for the Trojan to attack a device’s system. A Trojan virus spreads through legitimate-looking emails and files attached to emails, which are spammed to reach the inboxes of as many people as possible. When the email is opened and the malicious attachment is downloaded, the Trojan server will install and automatically run every time the infected device is turned on. Devices can also be infected by a Trojan through social engineering tactics, which cyber criminals use to coerce users into downloading a malicious application. The malicious file could be hidden in banner advertisements, pop-up advertisements, or links on websites. A computer infected by Trojan malware can also spread it to other computers. A cybercriminal turns the device into a zombie computer, which means they have remote control of it without the user knowing. Hackers can then use the zombie computer to continue sharing malware across a network of devices, known as a botnet.



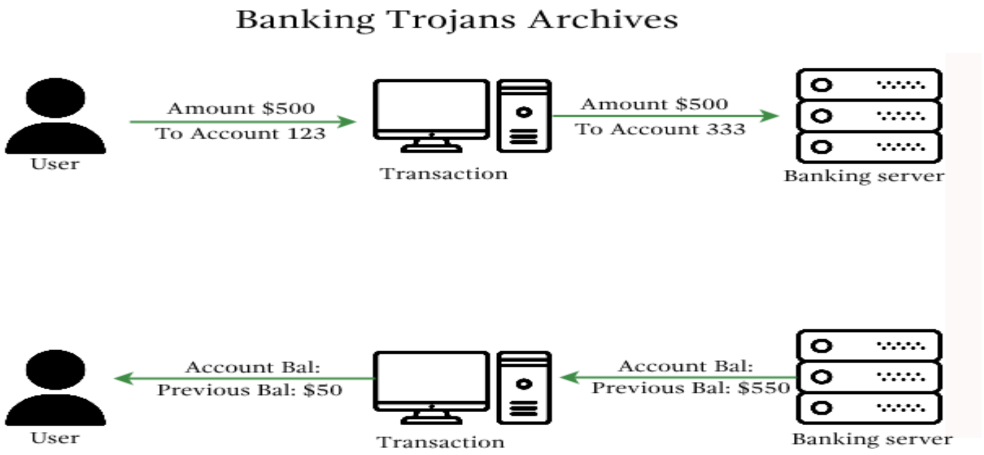
Most Common Types of Trojan Malware:

Backdoor Trojan:

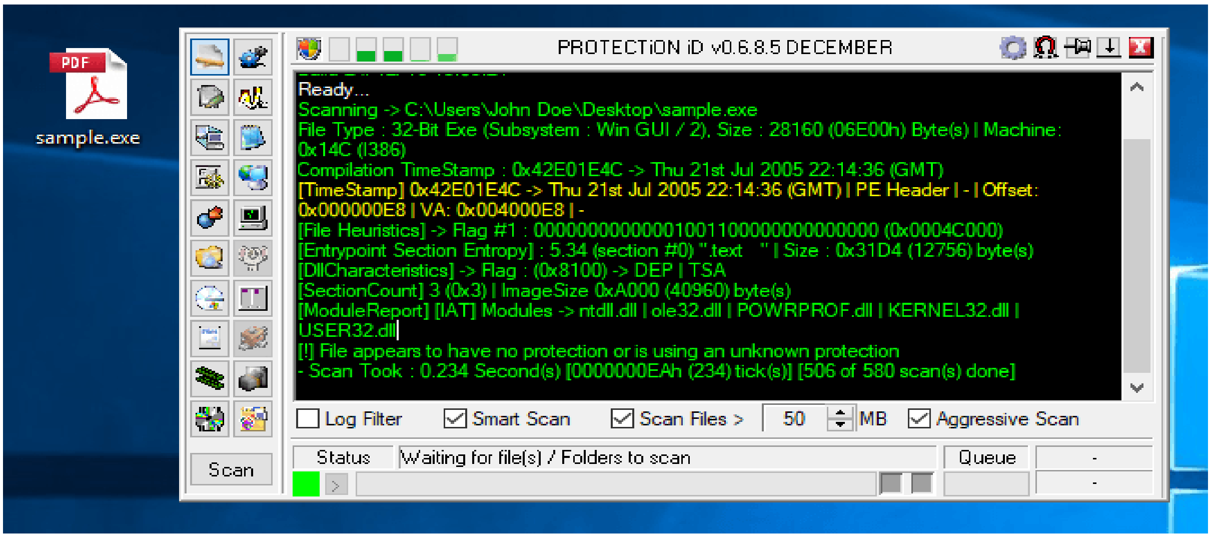
A backdoor Trojan enables an attacker to gain remote access to a computer and take control of it using a backdoor. This enables the malicious actor to do whatever they want on the device, such as deleting files, rebooting the computer, stealing data, or uploading malware. A backdoor Trojan is frequently used to create a botnet through a network of zombie computers.


Once installed, the backdoor checks which port is allowed to access the C&C server
C&C server
Attacker sends a backdoor to a target system
Firewall
Local DNS server

Banker Trojan:
A banker Trojan is designed to target users' banking accounts and financial information. It attempts to steal account data for credit and debit cards, e-payment systems, and online banking systems.



Downloader Trojan:
A downloader Trojan targets a computer that has already been infected by malware, then downloads and installs more malicious programs to it. This could be additional Trojans or other types of malware like adware.

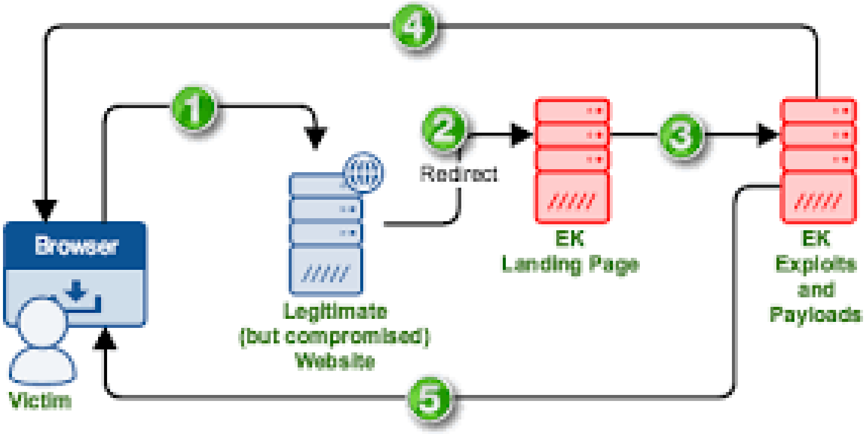


```
Ready...
Scanning -> C:\Users\John Doe\Desktop\sample.exe
File Type : 32-Bit Exe (Subsystem : Win GUI / 2), Size : 28160 (06E00h) Byte(s) | Machine:
0x14C (I386)
Compilation TimeStamp : 0x42E01E4C -> Thu 21st Jul 2005 22:14:36 (GMT)
[TimeStamp] 0x42E01E4C -> Thu 21st Jul 2005 22:14:36 (GMT) | PE Header | - | Offset:
0x000000E8 | VA: 0x004000E8 | -
[File Heuristics] -> Flag #1 : 00000000000001001100000000000000 (0x0004C000)
[Entrypoint Section Entropy] : 5.34 (section #0) ".text   " | Size : 0x31D4 (12756) byte(s)
[DllCharacteristics] -> Flag : (0x8100) -> DEP | TSA
[SectionCount] 3 (0x3) | ImageSize 0xA000 (40960) byte(s)
[ModuleReport] [IAT] Modules -> ntdll.dll | ole32.dll | POWRPROF.dll | KERNEL32.dll |
USER32.dll
[!] File appears to have no protection or is using an unknown protection
- Scan Took : 0.234 Second(s) [0000000EAh (234) tick(s)] [506 of 580 scan(s) done]
```

☐ Log Filter ☑ Smart Scan ☑ Scan Files > 50 MB ☑ Aggressive Scan

Status: Waiting for file(s) / Folders to scan | Queue: -

Exploit Trojan:
An exploit malware program contains code or data that takes advantage of specific vulnerabilities within an application or computer system. The cybercriminal will target users through a method like a phishing attack, then use the code in the program to exploit a known vulnerability.



Spy Trojan:
Spy Trojans are designed to sit on a user’s computer and spy on their activity. This includes logging their keyboard actions, taking screenshots, accessing the applications they use, and tracking login data.

How to Recognize a Trojan Virus:
A Trojan horse virus can often remain on a device for months without the user knowing their computer has been infected. However, telltale signs of the presence of a Trojan include computer settings suddenly changing, a loss in computer performance, or unusual activity taking place. The best way to recognize a Trojan is to search a device using a Trojan scanner or malware-removal software.

How to Protect Yourself from Trojan Viruses:
A Trojan horse virus can often remain on a device for months without the user knowing their computer has been infected. However, telltale signs of the presence of a Trojan include computer settings suddenly changing, a loss in computer performance, or unusual activity taking place. The best way to recognize a Trojan is to search a device using a Trojan scanner or malware-removal software.

Examples of Trojan Horse Virus Attacks:
Trojan attacks have been responsible for causing major damage by infecting computers and stealing user data. Well-known examples of Trojans include:

Rakhni Trojan:
The Rakhni Trojan delivers ransomware or a cryptojacker tool—which enables an attacker to use a device to mine cryptocurrency—to infect devices.

Tiny Banker:
Tiny Banker enables hackers to steal users' financial details. It was discovered when it infected at least 20 U.S. banks.

Zeus or Zbot:
Zeus is a toolkit that targets financial services and enables hackers to build their own Trojan malware. The source code uses techniques like form grabbing and keystroke logging to steal user credentials and financial details.

SPYWARE:

Spyware is a type of malware that is specifically designed to monitor a user's activity and collect sensitive information, such as keystrokes, browsing history, and login credentials. Spyware can be installed on a system through a variety of methods, including email attachments, software downloads, and malicious websites. Once spyware is installed, it can monitor a user's activity and send the collected data back to a remote server controlled by an attacker. The attacker can then use this information for nefarious purposes, such as stealing personal information, blackmail, or identity theft. For example, a user may inadvertently download spyware when they click on a link in an email that appears to be from a trusted source. The spyware could then monitor the user's keystrokes and capture login credentials, which could be used by an attacker to gain access to the user's financial accounts. Spyware is a type of malware that is designed to collect information about a user's computer activity without their knowledge or consent. This can include browsing habits, login credentials, and personal information. The collected information is then sent to the attacker's server, where it can be used for malicious purposes, such as identity theft or targeted advertising.

Here are some examples of spyware:

Keyloggers:
Keyloggers are a type of spyware that records every keystroke made on a user's computer, including passwords, login credentials, and credit card numbers. This information can be used by attackers to gain unauthorized access to the victim's accounts or steal their sensitive information.

Adware:
Adware is a type of spyware that displays unwanted advertisements on a user's computer. Adware can be installed along with other software or downloaded from malicious websites. Adware can also collect information about a user's browsing habits to display targeted advertisements.

Remote Access Trojans (RATs):
RATs are a type of spyware that allows attackers to gain remote access to a victim's computer. This can allow attackers to monitor the victim's activity, steal sensitive information, or install additional malware.

Browser hijackers:
Browser hijackers are a type of spyware that modifies a user's web browser settings without their consent. This can include changing the default homepage, search engine, or installing unwanted browser extensions. Browser hijackers can also collect information about a user's browsing habits to display targeted advertisements.

Mobile spyware:
Mobile spyware is a type of spyware that is designed to collect information from a victim's mobile device, such as call logs, text messages, and GPS location. Mobile spyware can be installed through malicious apps or downloaded from untrusted sources.

To protect against spyware, users should be cautious when downloading software or opening attachments from untrusted sources. Users should also regularly update their software and use antivirus software to detect and remove spyware. Additionally, users can use browser extensions or ad blockers to prevent unwanted advertisements and browser hijackers from affecting their web browsing experience.In both cases, Trojan horses and spyware can have serious consequences for the security and privacy of a system and its users. It is important to have appropriate security measures in place, such as anti-malware software and user education, to prevent and mitigate the impact of these threats.

3. DETECTING DENIAL OF SERVICE ATTACKS

AIM:

To Detect Denial Of Service attacks

DESCRIPTION:

Detecting Denial of Service (DoS) attacks can be challenging, as they often involve overwhelming a network or system with excessive traffic, making it unavailable to legitimate users. However, there are some methods that can be used to detect and mitigate DoS attacks.

Monitor network traffic:
By monitoring network traffic, administrators can detect an increase in traffic volume that may be indicative of a DoS attack. Network monitoring tools can be used to identify unusual spikes in traffic and isolate the source of the traffic.

Implement intrusion detection and prevention systems (IDPS):
IDPS can help detect DoS attacks by analyzing network traffic and identifying patterns that are indicative of an attack. IDPS can also block traffic from known malicious sources, which can help mitigate the impact of an attack.

Check system logs:
System logs can provide valuable information about the health and performance of a system, including indications of a DoS attack. Logs can be used to identify unusual traffic patterns, failed login attempts, or other indicators of an attack.

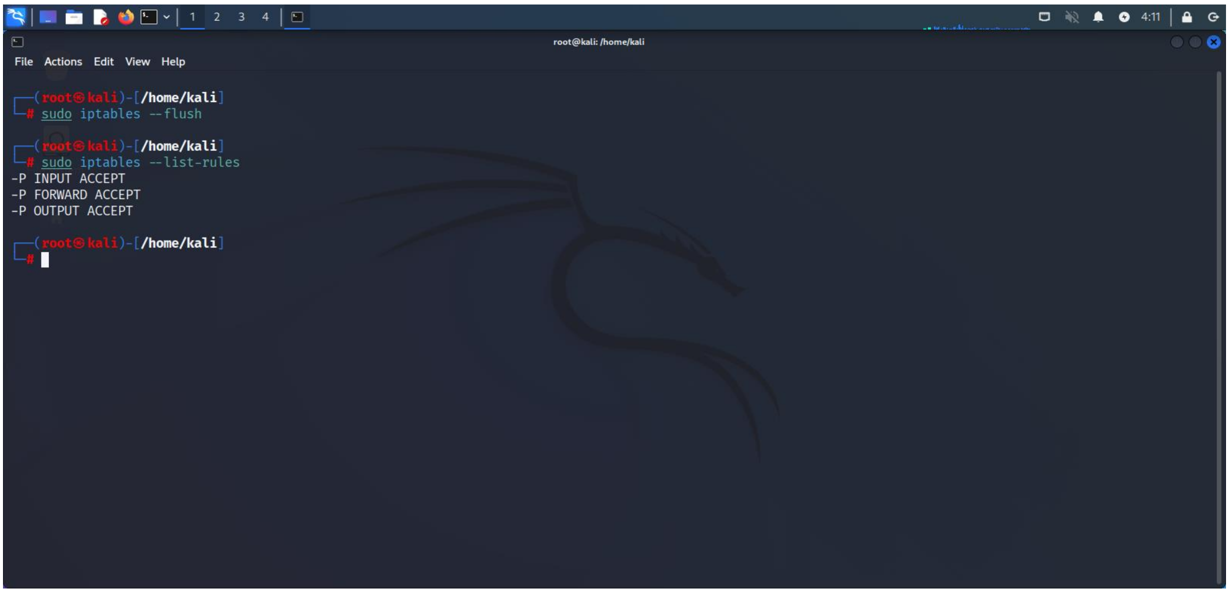
Use traffic filtering:
Traffic filtering can be used to block traffic from known malicious sources, such as IP addresses associated with previous attacks or botnets. This can help mitigate the impact of an attack by limiting the amount of traffic that reaches the system.

Perform stress tests:
Regular stress testing can help identify vulnerabilities in a system that may be exploited in a DoS attack. By simulating a DoS attack, administrators can identify weaknesses in their defenses and take steps to address them before an actual attack occurs.

PROCEDURE:

Step 1: Use the command sudo iptables –flush to remove all the existing rules in the iptables

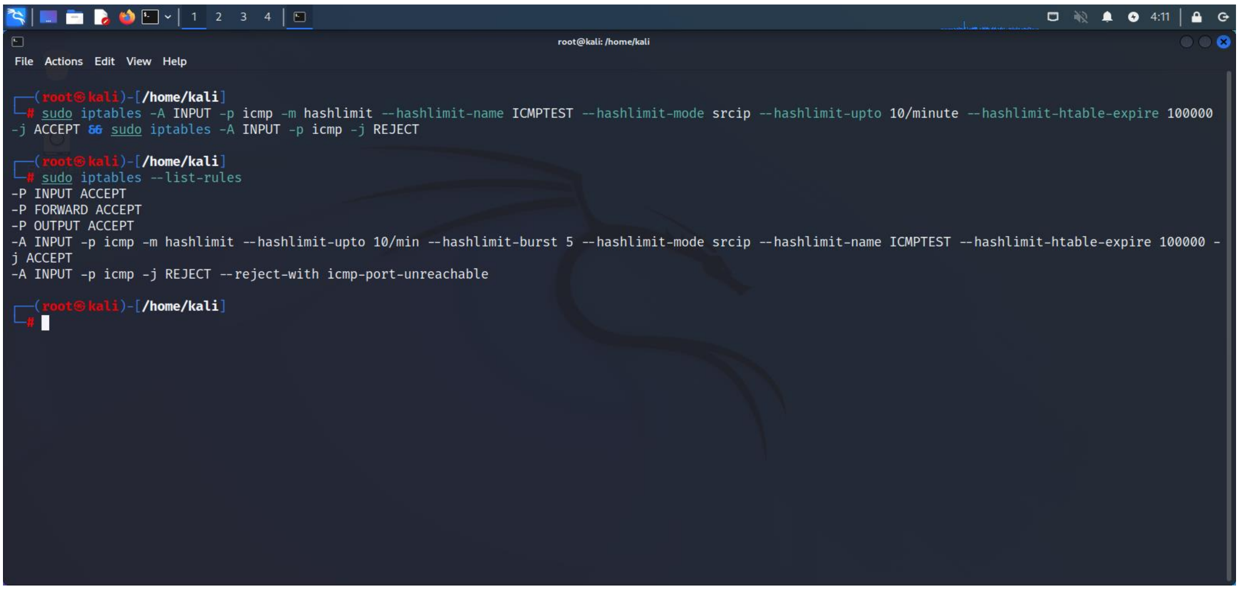
Step 2: To list the available rules give sudo iptables –list-rules.



```
┌──(root㉿kali)-[/home/kali]
└─# sudo iptables --flush

┌──(root㉿kali)-[/home/kali]
└─# sudo iptables --list-rules
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT

┌──(root㉿kali)-[/home/kali]
└─# 
```

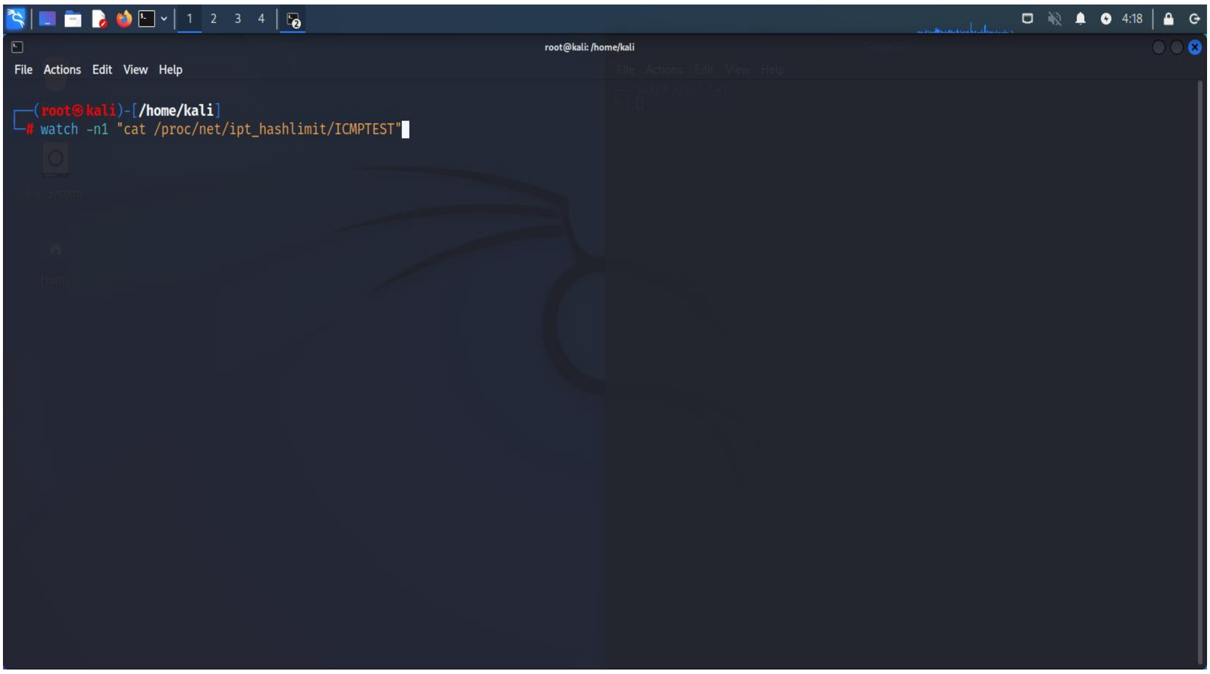
Step 3: Configure the iptables by using the following command sudo iptables -A INPUT -p icmp -m hashlimit --hashlimit-name ICMPTEST --h-j ACCEPT && sudo iptables -A INPUT -p icmp -j REJECT

Step 4: To check the configured rules give sudo iptables –list-rules



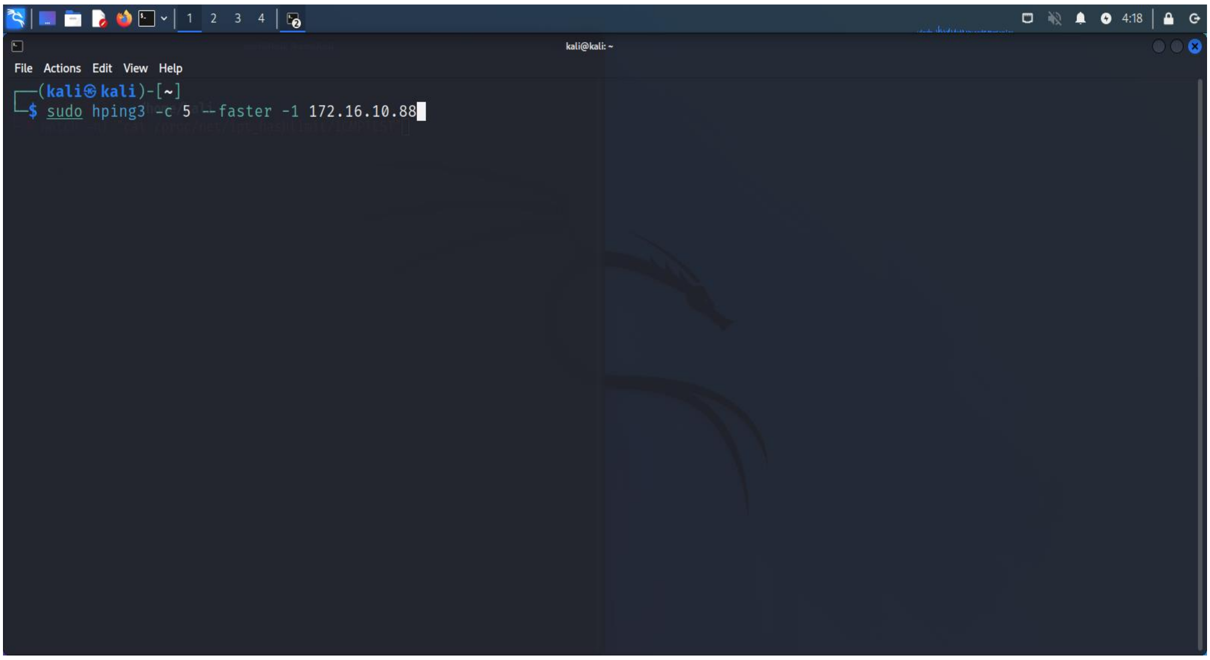
```
┌──(root㉿kali)-[/home/kali]
└─# sudo iptables -A INPUT -p icmp -m hashlimit --hashlimit-name ICMPTEST --hashlimit-mode srcip --hashlimit-upto 10/minute --hashlimit-htable-expire 100000
-j ACCEPT && sudo iptables -A INPUT -p icmp -j REJECT

┌──(root㉿kali)-[/home/kali]
└─# sudo iptables --list-rules
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -p icmp -m hashlimit --hashlimit-upto 10/min --hashlimit-burst 5 --hashlimit-mode srcip --hashlimit-name ICMPTEST --hashlimit-htable-expire 100000 -
j ACCEPT
-A INPUT -p icmp -j REJECT --reject-with icmp-port-unreachable

┌──(root㉿kali)-[/home/kali]
└─# 
```

Step 5: Using the watch command give the input as watch -n1 "cat /proc/net/ipt_hashlimit/ICMPTEST"

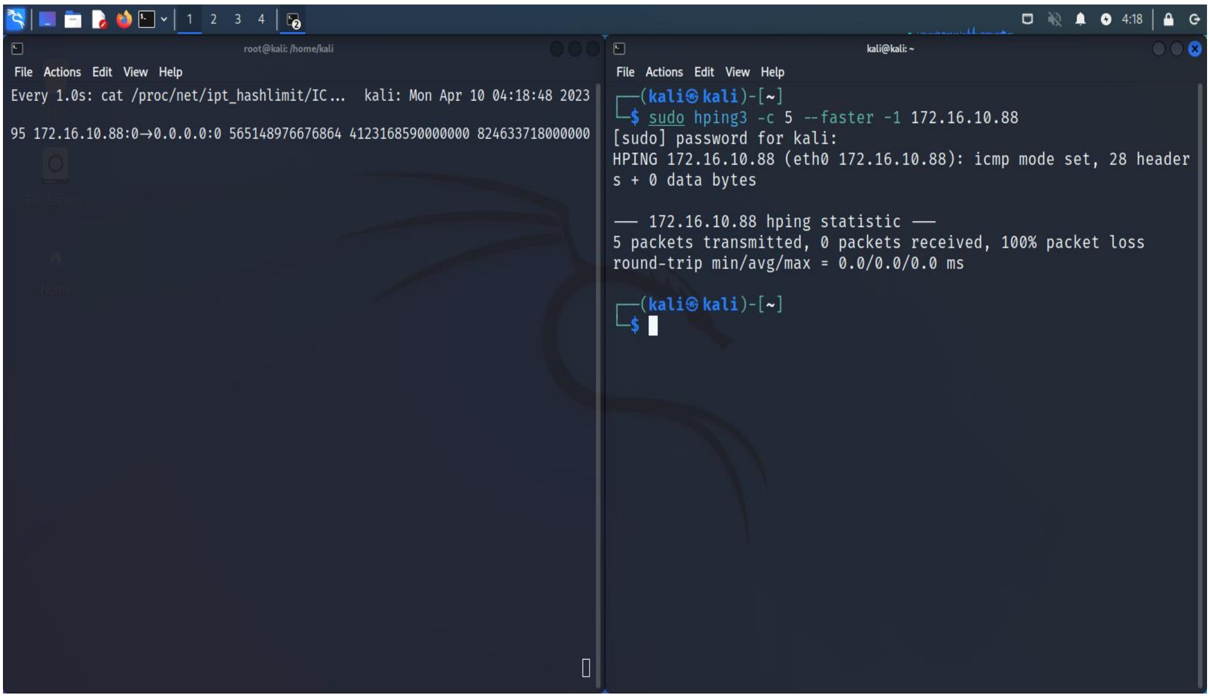


```
┌──(root㉿kali)-[/home/kali]
└─# watch -n1 "cat /proc/net/ipt_hashlimit/ICMPTEST"
```

Step 6: Give the following command sudo hping3 -c 5 --faster -1 172.16.10.88



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -c 5 --faster -1 172.16.10.88
```



```
Every 1.0s: cat /proc/net/ipt_hashlimit/IC...   kali: Mon Apr 10 04:18:48 2023

95 172.16.10.88:0→0.0.0.0:0 565148976676864 4123168590000000 8246337180000000
```

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -c 5 --faster -1 172.16.10.88
[sudo] password for kali:
HPING 172.16.10.88 (eth0 172.16.10.88): icmp mode set, 28 header
s + 0 data bytes

--- 172.16.10.88 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(kali㉿kali)-[~]
└─$ 
```

3. IMPLEMENT A CODE TO SIMULATE DARA INTERCEPTION AND THEFT

AIM:

To implement a code to simulate data interception and theft

WIRESHARK:

Wireshark is very similar to tcpdump, but has a graphical front-end and integrated sorting and filtering options. Wireshark lets the user put network interface controllers into promiscuous mode (if supported by the network interface controller), so they can see all the traffic visible on that interface including unicast traffic not sent to that network interface controller & MAC address. However, when capturing with a packet analyser in promiscuous mode on a port on a network switch, not all traffic through the switch is necessarily sent to the port where the capture is done, so capturing in promiscuous mode is not necessarily sufficient to see all network traffic. Port mirroring or various network taps extend capture to any point on the network. Simple passive taps are extremely resistant to tampering.

FUNTIONALITY OF WIRESHARK:

Wireshark is a network protocol analyzer tool that allows users to capture, inspect, and analyze network traffic in real-time. It is an open-source software that runs on various platforms, including Windows, Linux, and macOS. The primary functionality of Wireshark includes:

- Wireshark can capture packets of data that are sent and received over a network interface, such as Ethernet or Wi-Fi. It can capture traffic in real-time or from a saved file.

- Wireshark can analyze and dissect packets of data to determine the underlying network protocols being used, such as TCP, UDP, HTTP, DNS, and more. It can also decode the data within each packet and display it in a human-readable format.

- Wireshark allows users to filter and search network traffic based on specific criteria, such as protocol, IP address, port number, and more. This can help to isolate specific network issues or identify suspicious activity.

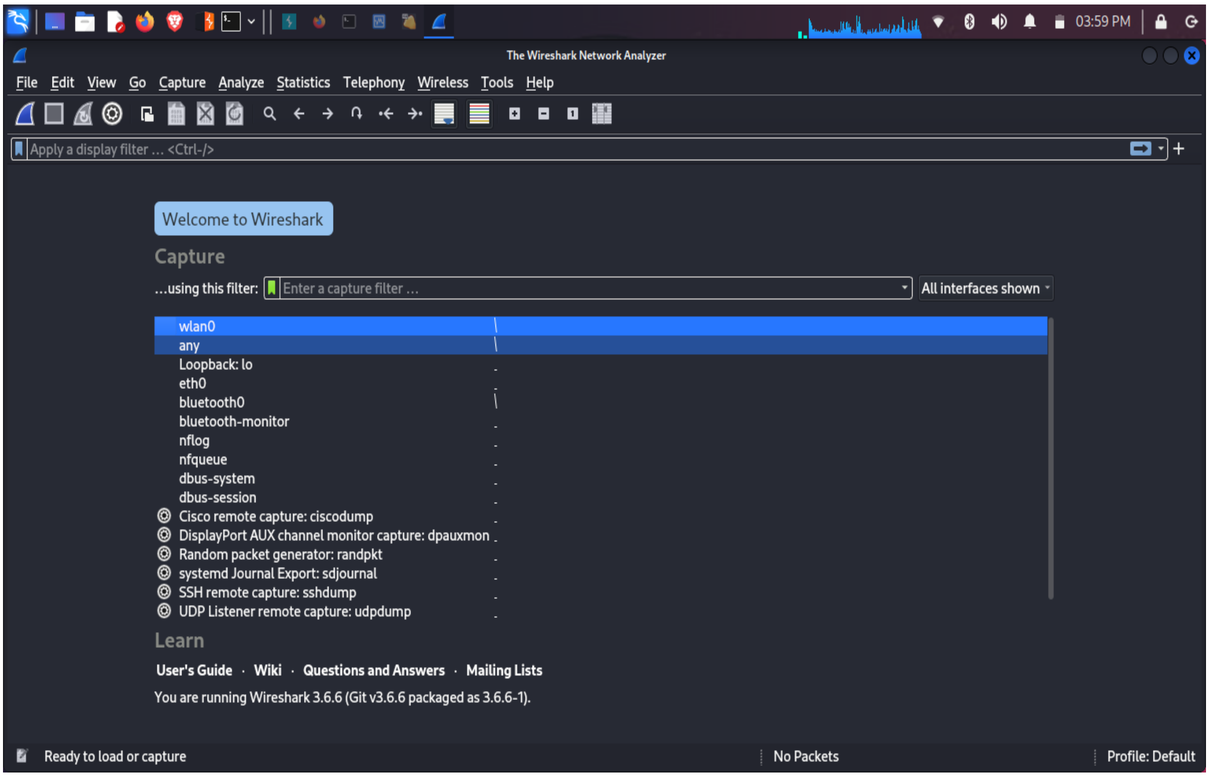
- Wireshark can provide statistical information on network traffic, such as the amount of data sent and received, the network latency, and the number of packets dropped.

- Wireshark is highly customizable, allowing users to create custom protocol dissectors, filters, and display options.

PRPOCEDURE:

Step 1: Download and install Wireshark Tool from www.wireshark.orgin.

Step 2: Open the Wireshark Tool in application menu OR run the command “wireshark” in the terminal.


03:59 PM
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

```
wlan0
any
Loopback: lo
eth0
bluetooth0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
```

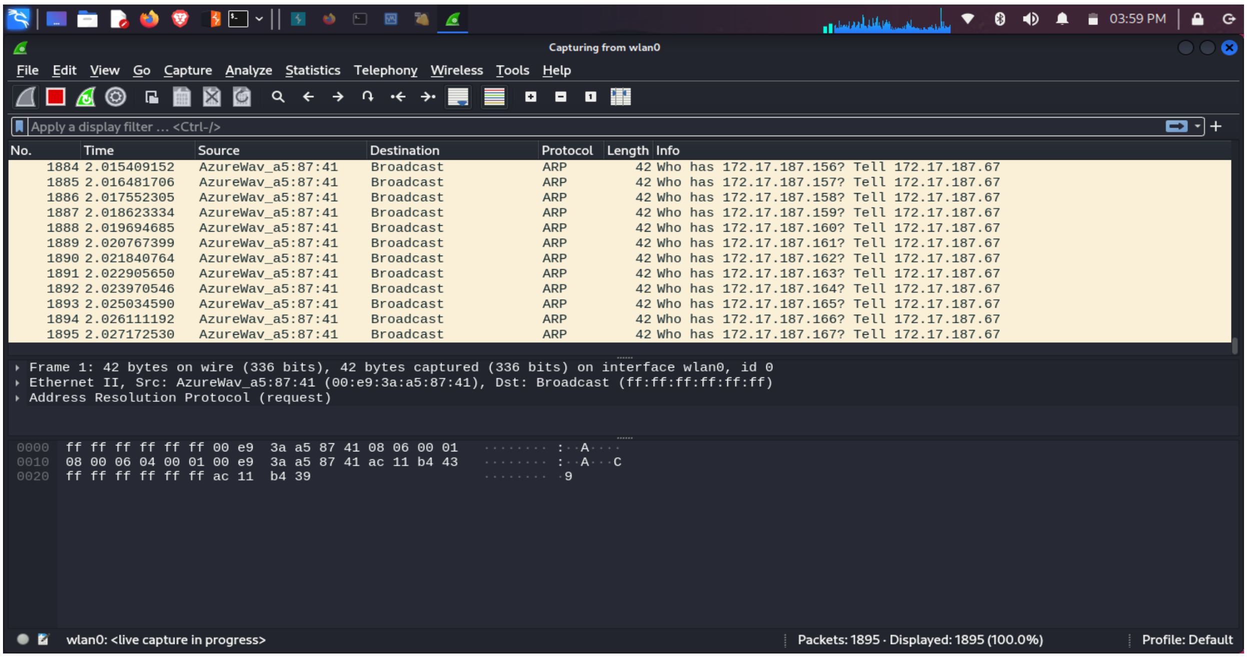
You are running Wireshark 3.6.6 (Git v3.6.6 packaged as 3.6.6-1).

Ready to load or capture

No Packets

Profile: Default

Step 3: Select an interface to capture traffic.


03:59 PM
Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

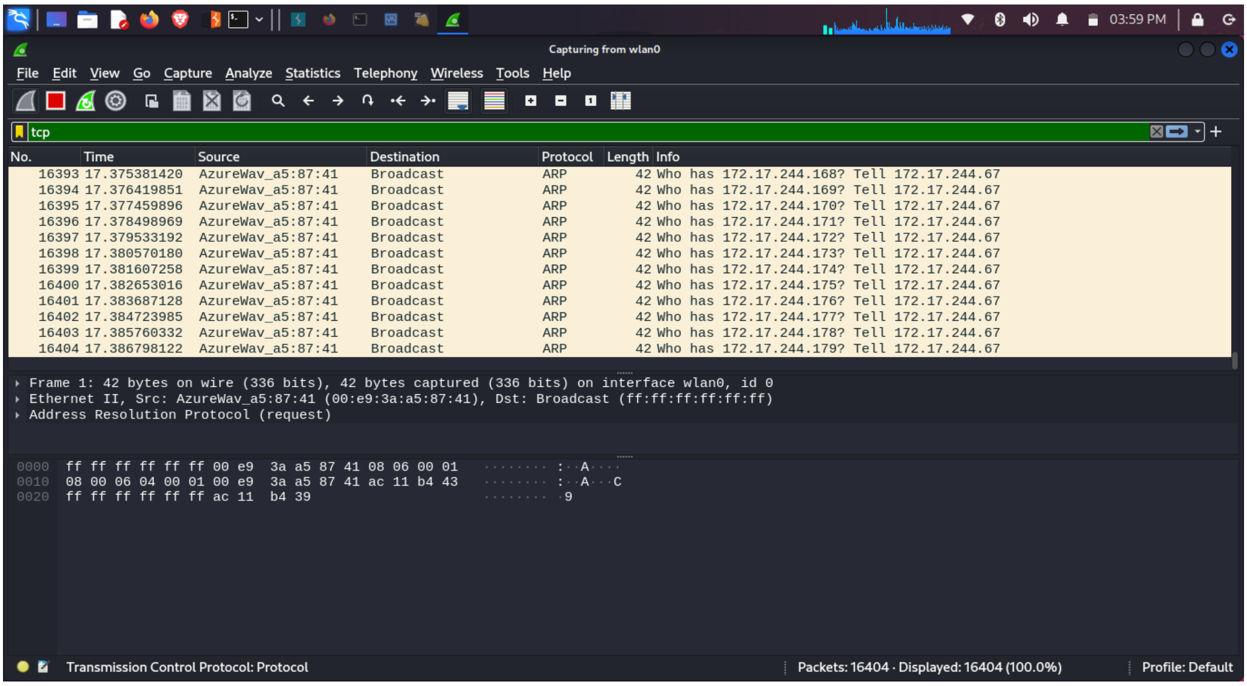
```
No.     Time          Source              Destination       Protocol Length Info
   1884 2.015409152   AzureWav_a5:87:41   Broadcast         ARP        42 Who has 172.17.187.156? Tell 172.17.187.67
   1885 2.016481706   AzureWav_a5:87:41   Broadcast         ARP        42 Who has 172.17.187.157? Tell 172.17.187.67
   1886 2.017552305   AzureWav_a5:87:41   Broadcast         ARP        42 Who has 172.17.187.158? Tell 172.17.187.67
   1887 2.018623334   AzureWav_a5:87:41   Broadcast         ARP        42 Who has 172.17.187.159? Tell 172.17.187.67
   1888 2.019694685   AzureWav_a5:87:41   Broadcast         ARP        42 Who has 172.17.187.160? Tell 172.17.187.67
   1889 2.020767399   AzureWav_a5:87:41   Broadcast         ARP        42 Who has 172.17.187.161? Tell 172.17.187.67
   1890 2.021840764   AzureWav_a5:87:41   Broadcast         ARP        42 Who has 172.17.187.162? Tell 172.17.187.67
   1891 2.022905650   AzureWav_a5:87:41   Broadcast         ARP        42 Who has 172.17.187.163? Tell 172.17.187.67
   1892 2.023970546   AzureWav_a5:87:41   Broadcast         ARP        42 Who has 172.17.187.164? Tell 172.17.187.67
   1893 2.025034590   AzureWav_a5:87:41   Broadcast         ARP        42 Who has 172.17.187.165? Tell 172.17.187.67
   1894 2.026111192   AzureWav_a5:87:41   Broadcast         ARP        42 Who has 172.17.187.166? Tell 172.17.187.67
   1895 2.027172530   AzureWav_a5:87:41   Broadcast         ARP        42 Who has 172.17.187.167? Tell 172.17.187.67

› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlan0, id 0
› Ethernet II, Src: AzureWav_a5:87:41 (00:e9:3a:a5:87:41), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 e9  3a a5 87 41 08 06 00 01   ········ :··A····
0010  08 00 06 04 00 01 00 e9  3a a5 87 41 ac 11 b4 43   ········ :··A···C
0020  ff ff ff ff ff ff ac 11  b4 39                     ········ ·9
```

wlan0: <live capture in progress>

Packets: 1895 · Displayed: 1895 (100.0%)

Profile: Default

Step 4: Apply a filter in the filter panel.

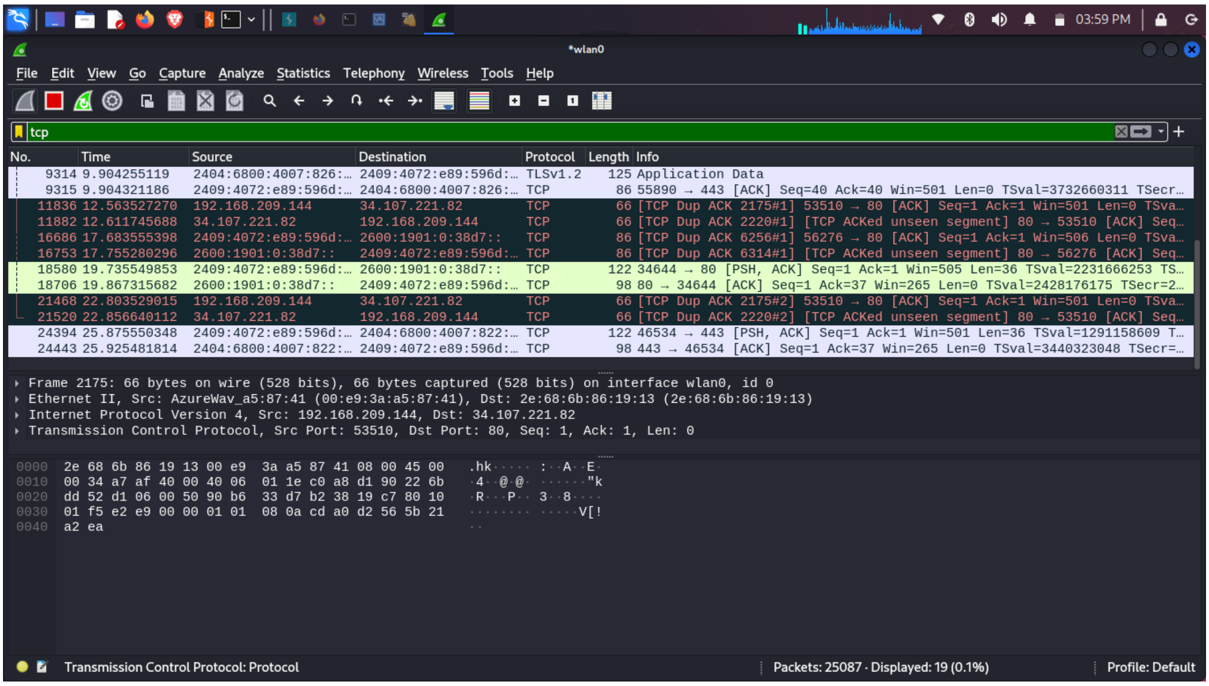

Capturing from wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
03:59 PM

tcp

```
No.   Time            Source              Destination   Protocol Length Info
16393 17.375381420 AzureWav_a5:87:41  Broadcast     ARP      42 Who has 172.17.244.168? Tell 172.17.244.67
16394 17.376419851 AzureWav_a5:87:41  Broadcast     ARP      42 Who has 172.17.244.169? Tell 172.17.244.67
16395 17.377459896 AzureWav_a5:87:41  Broadcast     ARP      42 Who has 172.17.244.170? Tell 172.17.244.67
16396 17.378498969 AzureWav_a5:87:41  Broadcast     ARP      42 Who has 172.17.244.171? Tell 172.17.244.67
16397 17.379533192 AzureWav_a5:87:41  Broadcast     ARP      42 Who has 172.17.244.172? Tell 172.17.244.67
16398 17.380570180 AzureWav_a5:87:41  Broadcast     ARP      42 Who has 172.17.244.173? Tell 172.17.244.67
16399 17.381607258 AzureWav_a5:87:41  Broadcast     ARP      42 Who has 172.17.244.174? Tell 172.17.244.67
16400 17.382653016 AzureWav_a5:87:41  Broadcast     ARP      42 Who has 172.17.244.175? Tell 172.17.244.67
16401 17.383687128 AzureWav_a5:87:41  Broadcast     ARP      42 Who has 172.17.244.176? Tell 172.17.244.67
16402 17.384723985 AzureWav_a5:87:41  Broadcast     ARP      42 Who has 172.17.244.177? Tell 172.17.244.67
16403 17.385760332 AzureWav_a5:87:41  Broadcast     ARP      42 Who has 172.17.244.178? Tell 172.17.244.67
16404 17.386798122 AzureWav_a5:87:41  Broadcast     ARP      42 Who has 172.17.244.179? Tell 172.17.244.67

› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlan0, id 0
› Ethernet II, Src: AzureWav_a5:87:41 (00:e9:3a:a5:87:41), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 e9  3a a5 87 41 08 06 00 01   ········ :··A····
0010  08 00 06 04 00 01 00 e9  3a a5 87 41 ac 11 b4 43   ········ :··A···C
0020  ff ff ff ff ff ff ac 11  b4 39                     ········ ·9
```

Transmission Control Protocol: Protocol | Packets: 16404 · Displayed: 16404 (100.0%) | Profile: Default

Step 5: Inspect the specified packet using wireshark.


*wlan0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
03:59 PM

tcp

```
No.   Time            Source                Destination           Protocol Length Info
 9314 9.904255119  2404:6800:4007:826:… 2409:4072:e89:596d:… TLSv1.2  125 Application Data
 9315 9.904321186  2409:4072:e89:596d:… 2404:6800:4007:826:… TCP       86 55890 → 443 [ACK] Seq=40 Ack=40 Win=501 Len=0 TSval=3732660311 TSecr…
11836 12.563527270 192.168.209.144      34.107.221.82        TCP       66 [TCP Dup ACK 2175#1] 53510 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSva…
11882 12.611745688 34.107.221.82        192.168.209.144      TCP       66 [TCP Dup ACK 2220#1] [TCP ACKed unseen segment] 80 → 53510 [ACK] Seq…
16686 17.683555398 2409:4072:e89:596d:… 2600:1901:0:38d7::   TCP       86 [TCP Dup ACK 6256#1] 56276 → 80 [ACK] Seq=1 Ack=1 Win=506 Len=0 TSva…
16753 17.755280296 2600:1901:0:38d7::   2409:4072:e89:596d:… TCP       86 [TCP Dup ACK 6314#1] [TCP ACKed unseen segment] 80 → 56276 [ACK] Seq…
18580 19.735549853 2409:4072:e89:596d:… 2600:1901:0:38d7::   TCP      122 34644 → 80 [PSH, ACK] Seq=1 Ack=1 Win=505 Len=36 TSval=2231666253 TS…
18706 19.867315682 2600:1901:0:38d7::   2409:4072:e89:596d:… TCP       98 80 → 34644 [ACK] Seq=1 Ack=37 Win=265 Len=0 TSval=2428176175 TSecr=2…
21468 22.803529015 192.168.209.144      34.107.221.82        TCP       66 [TCP Dup ACK 2175#2] 53510 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSva…
21520 22.856640112 34.107.221.82        192.168.209.144      TCP       66 [TCP Dup ACK 2220#2] [TCP ACKed unseen segment] 80 → 53510 [ACK] Seq…
24394 25.875550348 2409:4072:e89:596d:… 2404:6800:4007:822:… TCP      122 46534 → 443 [PSH, ACK] Seq=1 Ack=1 Win=501 Len=36 TSval=1291158609 T…
24443 25.925481814 2404:6800:4007:822:… 2409:4072:e89:596d:… TCP       98 443 → 46534 [ACK] Seq=1 Ack=37 Win=265 Len=0 TSval=3440323048 TSecr=…

› Frame 2175: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlan0, id 0
› Ethernet II, Src: AzureWav_a5:87:41 (00:e9:3a:a5:87:41), Dst: 2e:68:6b:86:19:13 (2e:68:6b:86:19:13)
› Internet Protocol Version 4, Src: 192.168.209.144, Dst: 34.107.221.82
› Transmission Control Protocol, Src Port: 53510, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

0000  2e 68 6b 86 19 13 00 e9  3a a5 87 41 08 00 45 00   .hk····· :··A··E·
0010  00 34 a7 af 40 00 40 06  01 1e c0 a8 d1 90 22 6b   ·4··@·@· ······"k
0020  dd 52 d1 06 00 50 90 b6  33 d7 b2 38 19 c7 80 10   ·R···P·· 3··8····
0030  01 f5 e2 e9 00 00 01 01  08 0a cd a0 d2 56 5b 21   ········ ·····V[!
0040  a2 ea                                              ··
```

Transmission Control Protocol: Protocol | Packets: 25087 · Displayed: 19 (0.1%) | Profile: Default

5. IMPLEMENT A CODE TO SIMULATE DATA MODIFICATION AND FABRICATION

AIM:

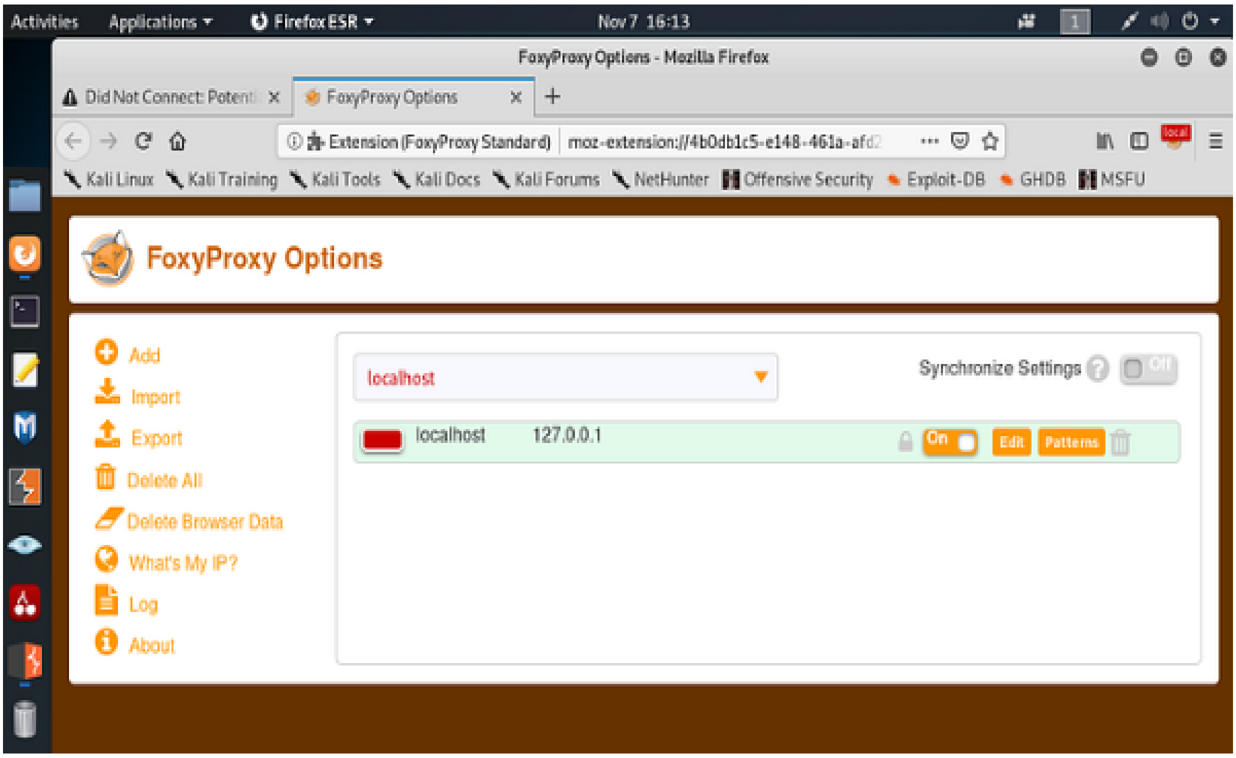
To implement a code to simulate data modification and fabrication

PROCEDURE:

Step 1: Download and install “Burpsuite” tool from https://portswigger.net/burp

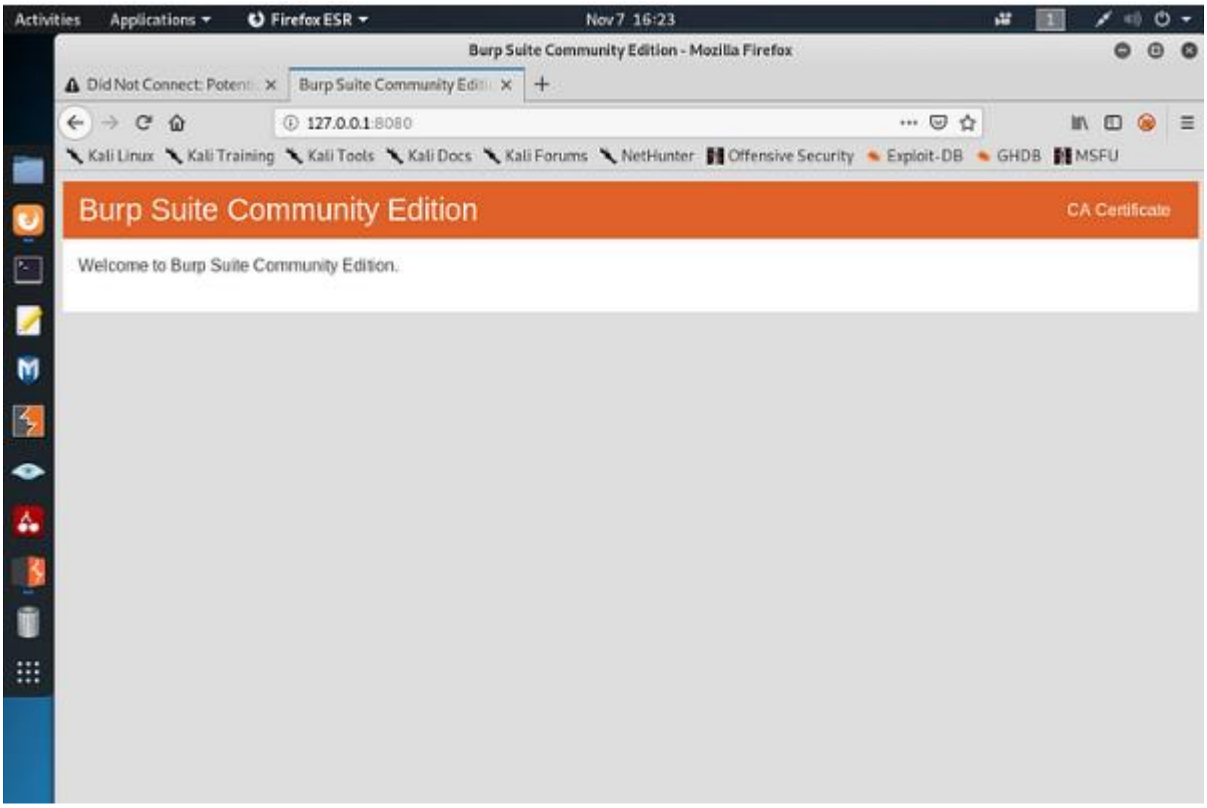
Step 2: Open Burpsuite from application menu OR run the command “burpsuite” in terminal.

Step 3: Install FoxyProxy extension In Firefox and add a localhost proxy:



Step 4: Install Burp Suite Certificate. Go to the local address and download the certificate

In firefox install the certificate.

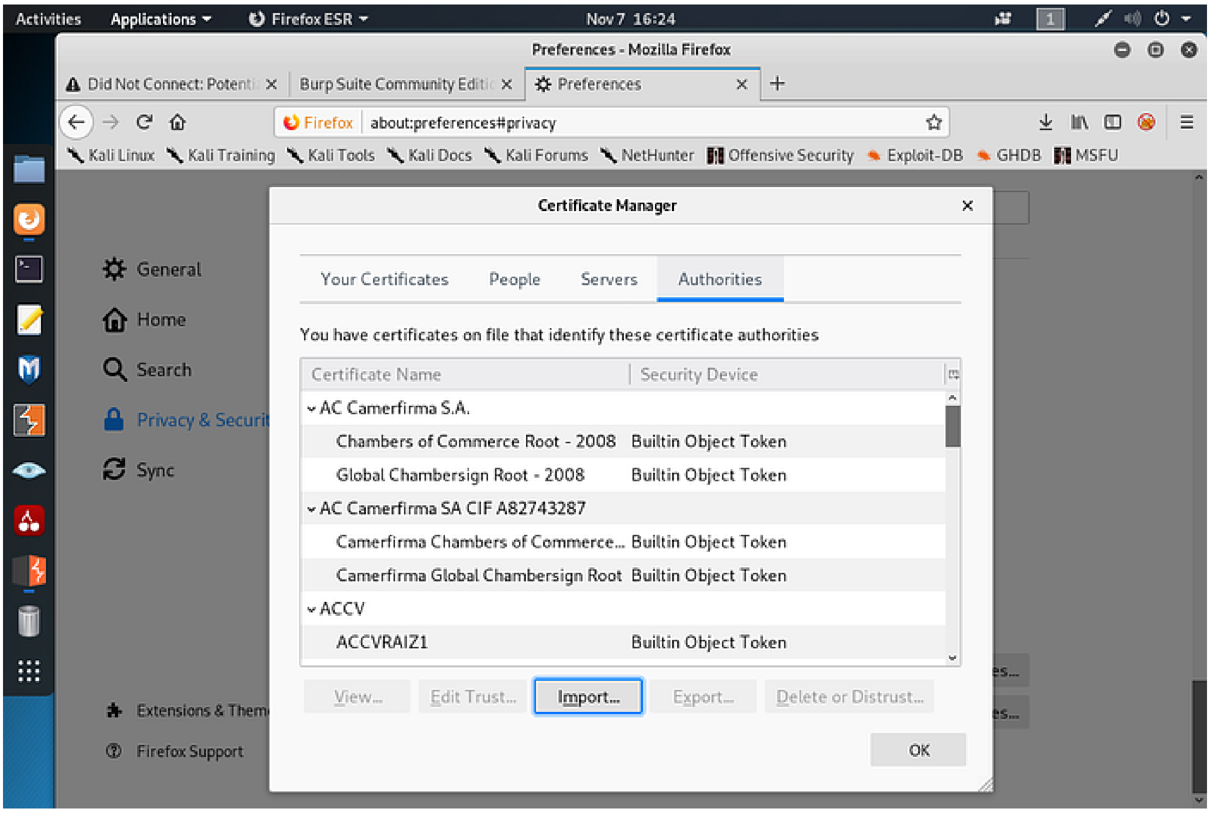


127.0.0.1:8080

Burp Suite Community Edition

Welcome to Burp Suite Community Edition.

Step 5: Import the Downloaded certificate into firefox.

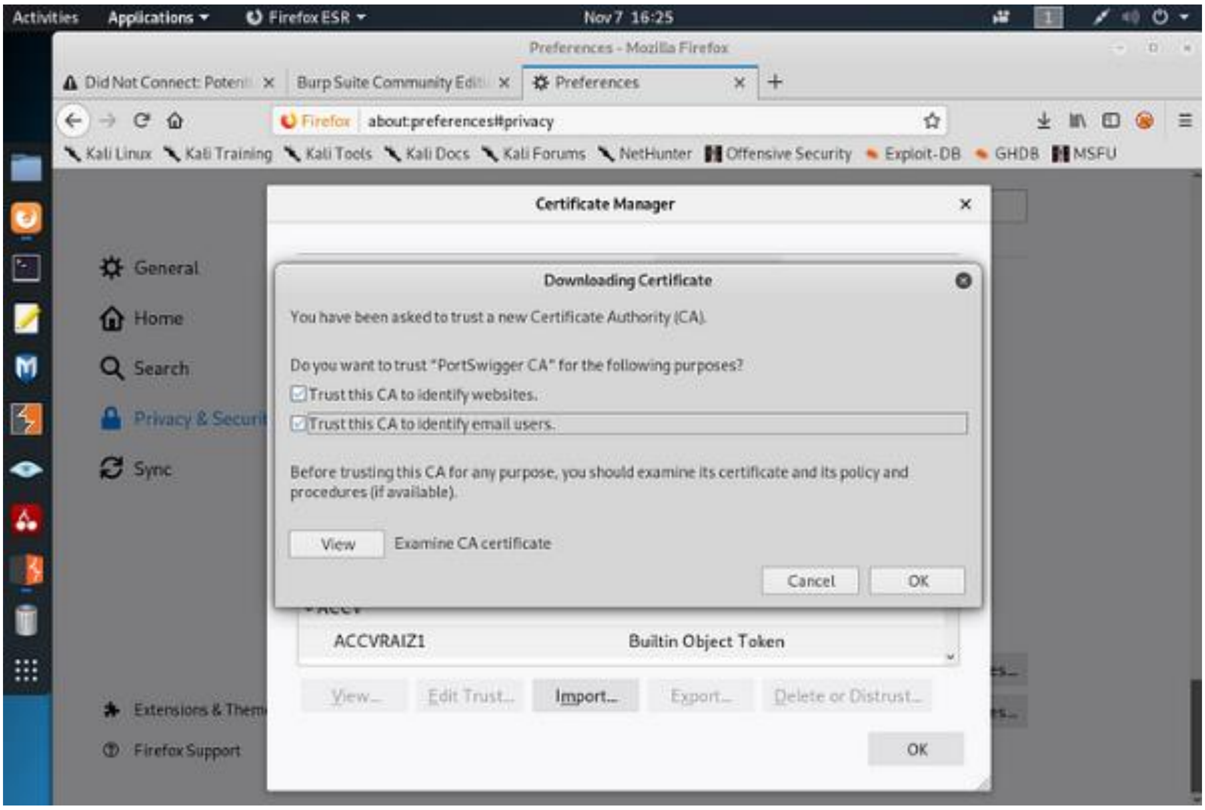


about:preferences#privacy

Certificate Manager

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
⌄ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
⌄ AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce...	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
⌄ ACCV	
ACCVRAIZ1	Builtin Object Token



Certificate Manager

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "PortSwigger CA" for the following purposes?

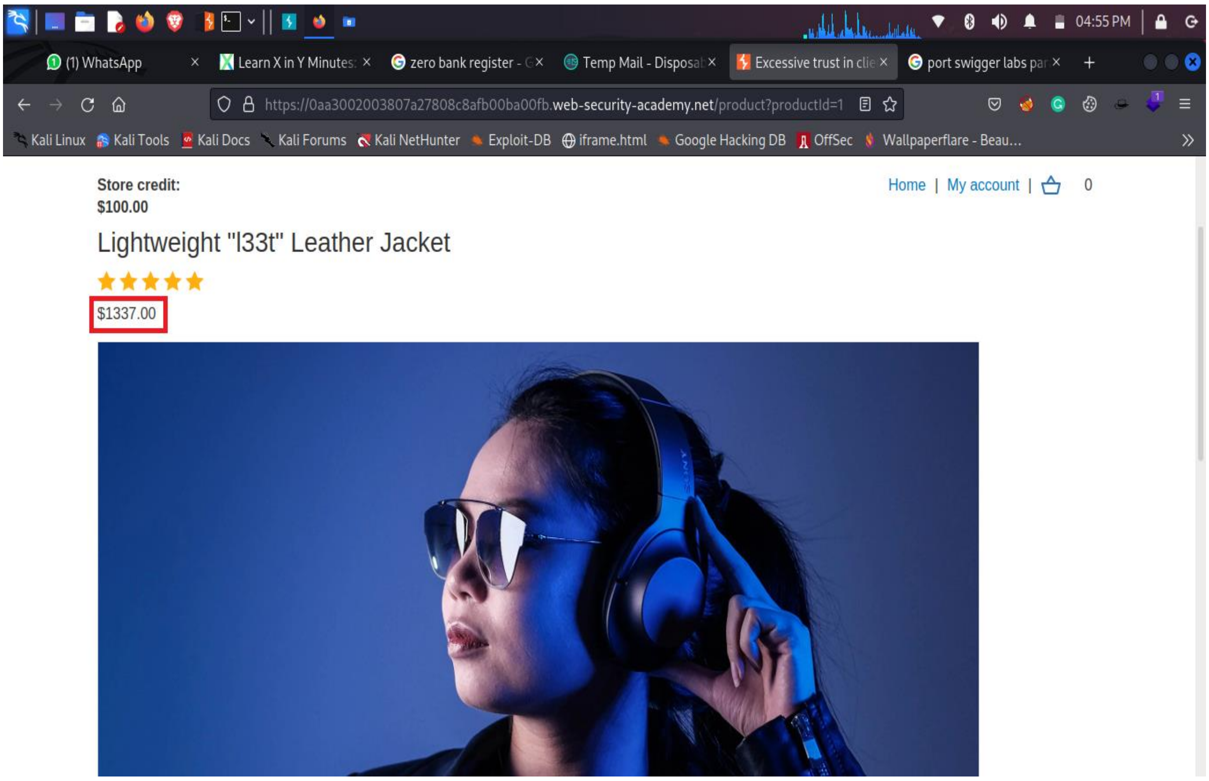
☑ Trust this CA to identify websites.

☑ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

ACCVRAIZ1 Builtin Object Token



https://0aa3002003807a27808c8afb00ba00fb.web-security-academy.net/product?productId=1

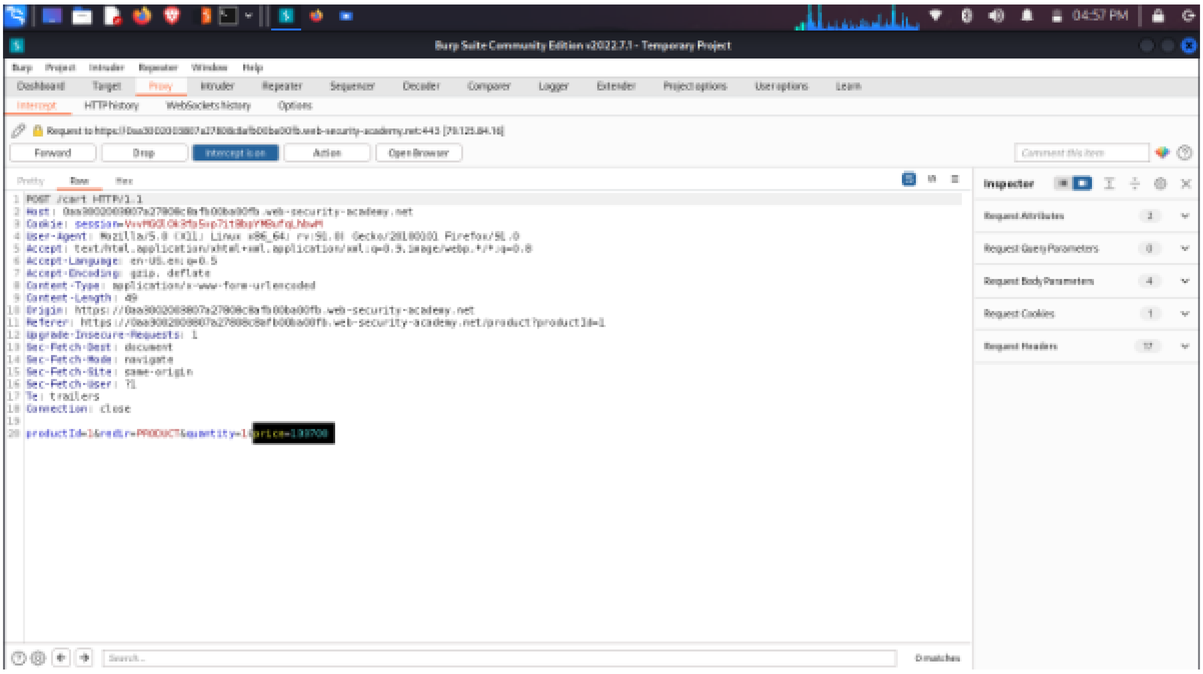
Store credit:
$100.00

Lightweight "l33t" Leather Jacket

★★★★★

$1337.00

Step 6: Capture the Packet using Burpsuite.

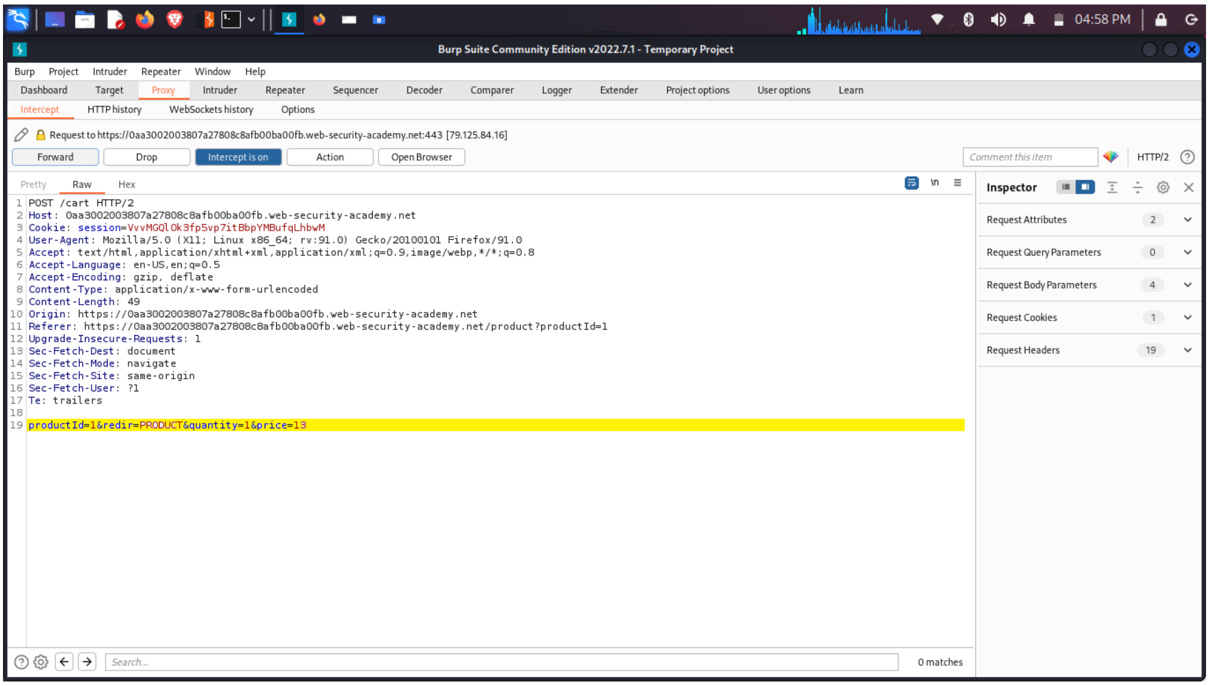


Burp Suite Community Edition v2022.7.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 4
Request Cookies 1
Request Headers 17
Search...
0 matches

Request to https://0aa3002003807a27808c8afb00ba00fb.web-security-academy.net:443 [79.125.84.16]

```
POST /cart HTTP/1.1
Host: 0aa3002003807a27808c8afb00ba00fb.web-security-academy.net
Cookie: session=VvvMGQlOk3fp5vp7itBbpYMBufqLhbwM
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: https://0aa3002003807a27808c8afb00ba00fb.web-security-academy.net
Referer: https://0aa3002003807a27808c8afb00ba00fb.web-security-academy.net/product?productId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

productId=1&redir=PRODUCT&quantity=1&price=133700
```

Step 7: Change the value of price in packet using Burpsuite Tool.

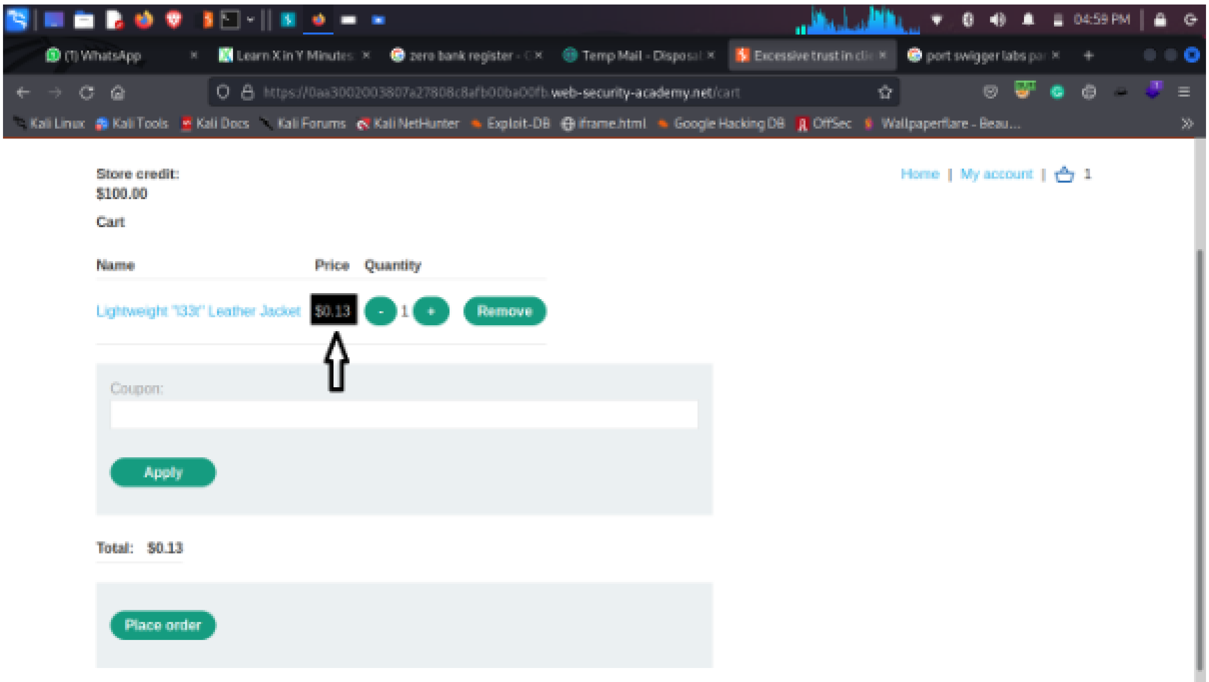


04:58 PM
Burp Suite Community Edition v2022.7.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/2
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 4
Request Cookies 1
Request Headers 19
Search...
0 matches

Request to https://0aa3002003807a27808c8afb00ba00fb.web-security-academy.net:443 [79.125.84.16]

```
POST /cart HTTP/2
Host: 0aa3002003807a27808c8afb00ba00fb.web-security-academy.net
Cookie: session=VvvMGQlOk3fp5vp7itBbpYMBufqLhbwM
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: https://0aa3002003807a27808c8afb00ba00fb.web-security-academy.net
Referer: https://0aa3002003807a27808c8afb00ba00fb.web-security-academy.net/product?productId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

productId=1&redir=PRODUCT&quantity=1&price=13
```

Step 8: The price value is changed in the cart.



Store credit:
$100.00

Cart

Name	Price	Quantity	
Lightweight "l33t" Leather Jacket	$0.13	- 1 +	Remove

Coupon:

Apply

Total: $0.13

Place order

6. DEMONSTRATE PHISHING ATTACK

AIM:

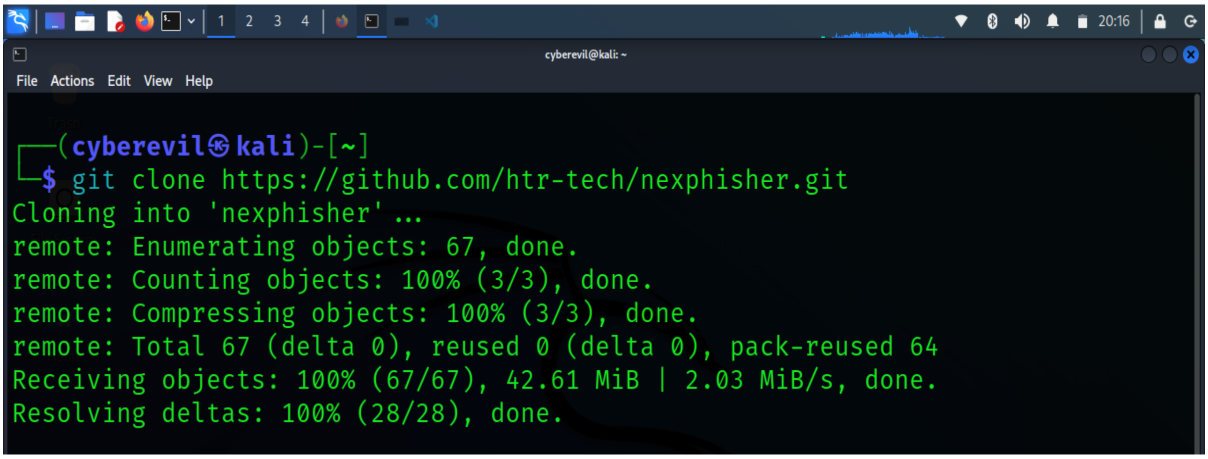
To demonstrate phishing attack

DESCRIPTION:

Phishing is a type of cyber attack in which an attacker uses social engineering tactics to trick a user into revealing sensitive information, such as login credentials, credit card numbers, or other personal information. Phishing attacks often involve the use of emails, text messages, or phone calls that appear to be from a legitimate source, such as a bank, social media platform, or online retailer. The goal of a phishing attack is to convince the user to click on a malicious link or download a file that contains malware, or to provide sensitive information directly to the attacker. Phishing attacks can be highly effective because they often appear to be legitimate and exploit human psychology and trust. To demonstrate a phishing attack for educational purposes, you could create a simulated phishing email or website that resembles a legitimate source, such as a bank or online retailer. The email or website could contain a message that urges the user to take action, such as clicking on a link or providing sensitive information, and provide instructions on how to do so. However, it is important to remember that any demonstration of a phishing attack should be conducted with the utmost care and caution, and should never be used to harm or deceive others. It is always important to prioritize the security and privacy of individuals and organizations, and to adhere to ethical standards when conducting any demonstrations or experiments.

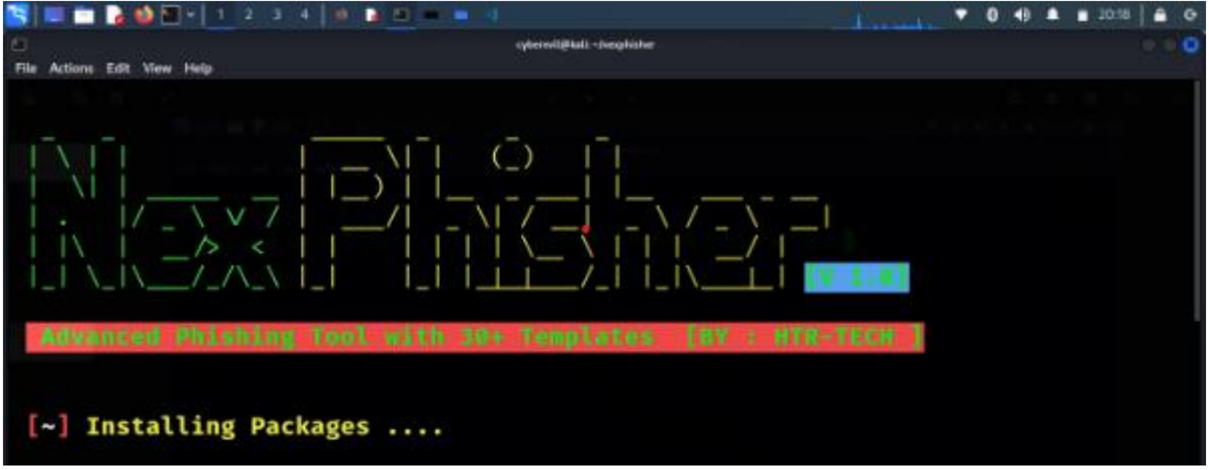
PROCEDURES:

Step 1: Download Nexphisher from Github



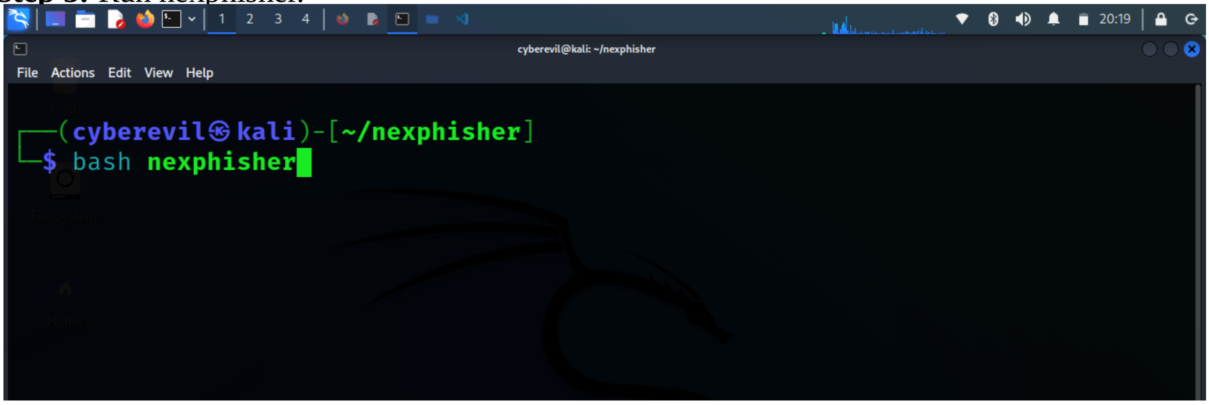
```
┌──(cyberevil㉿kali)-[~]
└─$ git clone https://github.com/htr-tech/nexphisher.git
Cloning into 'nexphisher' ...
remote: Enumerating objects: 67, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 67 (delta 0), reused 0 (delta 0), pack-reused 64
Receiving objects: 100% (67/67), 42.61 MiB | 2.03 MiB/s, done.
Resolving deltas: 100% (28/28), done.
```

Step 2: Install required Package for nexphisher.



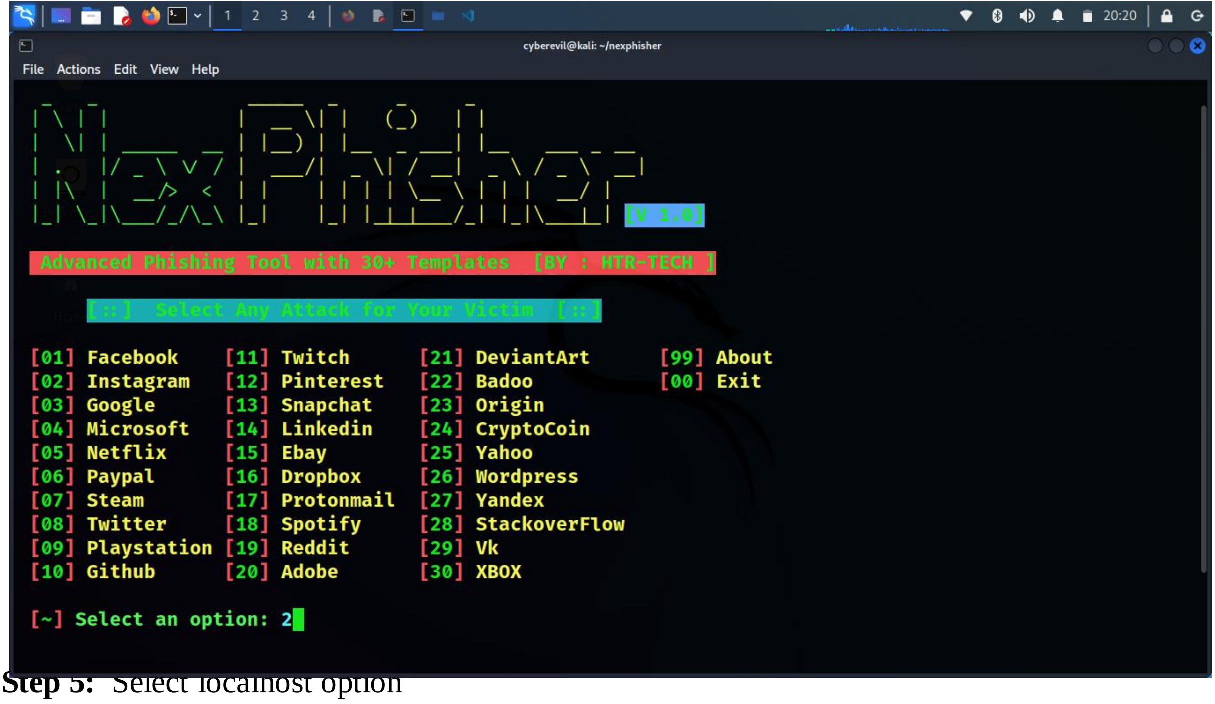
```
[V 1.0]
Advanced Phishing Tool with 30+ Templates   [BY : HTR-TECH ]

[~] Installing Packages ....
```

Step 3: Run nexphisher.



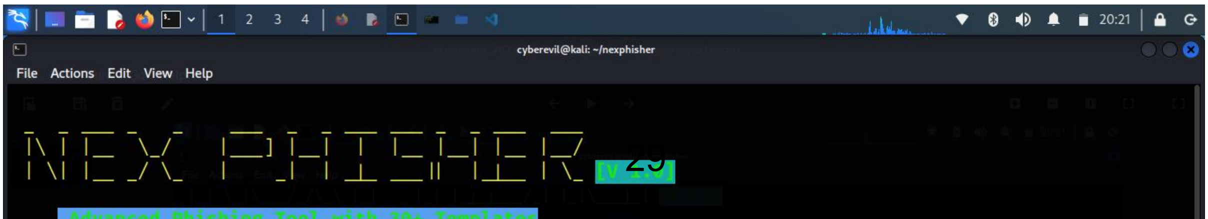
```
┌──(cyberevil㉿kali)-[~/nexphisher]
└─$ bash nexphisher
```

Step 4: Select an option.



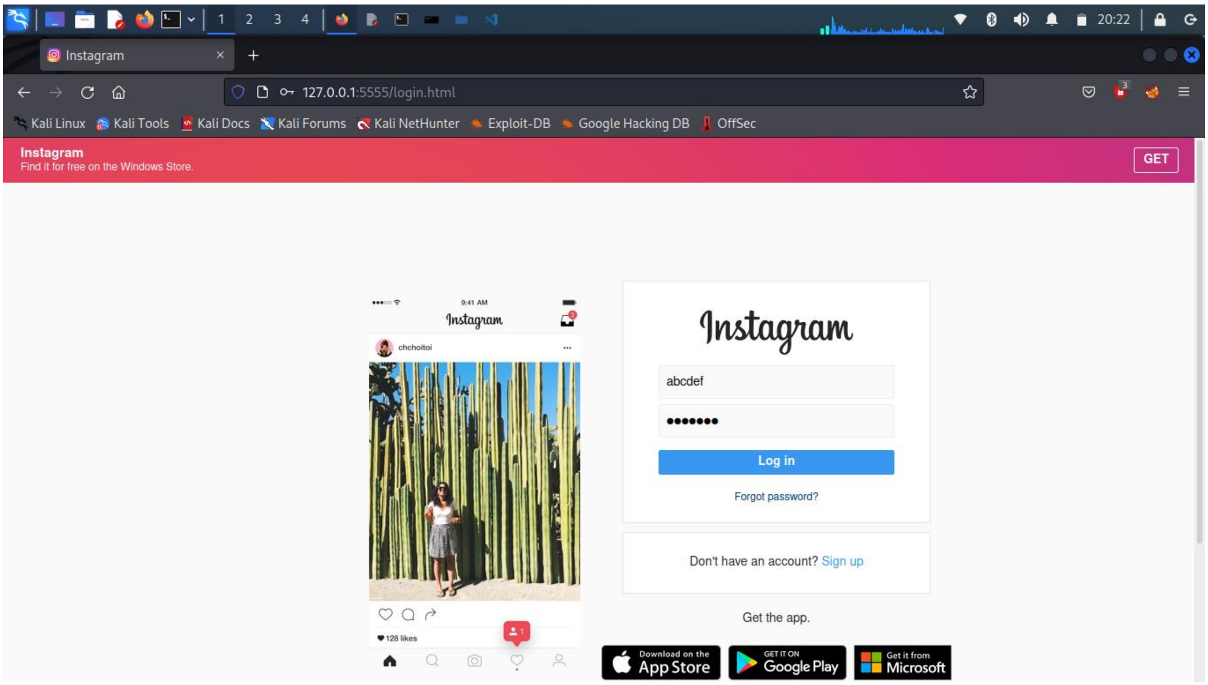
```
[V 1.0]
Advanced Phishing Tool with 30+ Templates   [BY : HTR-TECH ]

[ :: ]  Select Any Attack for Your Victim  [ :: ]

[01] Facebook      [11] Twitch        [21] DeviantArt      [99] About
[02] Instagram     [12] Pinterest     [22] Badoo           [00] Exit
[03] Google        [13] Snapchat      [23] Origin
[04] Microsoft     [14] Linkedin      [24] CryptoCoin
[05] Netflix       [15] Ebay          [25] Yahoo
[06] Paypal        [16] Dropbox       [26] Wordpress
[07] Steam         [17] Protonmail    [27] Yandex
[08] Twitter       [18] Spotify       [28] StackoverFlow
[09] Playstation   [19] Reddit        [29] Vk
[10] Github        [20] Adobe         [30] XBOX

[~] Select an option: 2
```

Step 5: Select localhost option



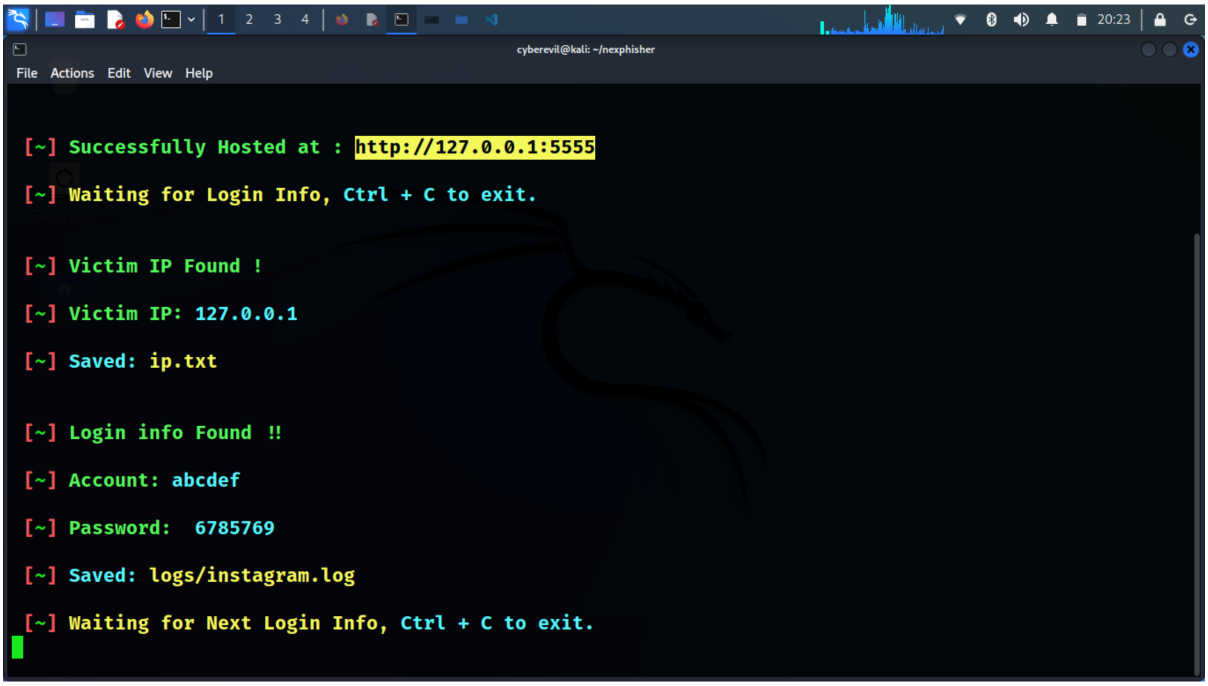
```
NEX PHISHER [V 1.0]
Advanced Phishing Tool with 30+ Templates
```

Step 6: Victim tries to enter Username & Password in the Phishing website.



abcdef

•••••••



```
[~] Successfully Hosted at : http://127.0.0.1:5555

[~] Waiting for Login Info, Ctrl + C to exit.

[~] Victim IP Found !

[~] Victim IP: 127.0.0.1

[~] Saved: ip.txt

[~] Login info Found !!

[~] Account: abcdef

[~] Password:  6785769

[~] Saved: logs/instagram.log

[~] Waiting for Next Login Info, Ctrl + C to exit.
```

7. PROTECTION MODELS

AIM:

To study about protection models

DISCRIPTION:

There are several different protection models that exist, each with its own unique approach to safeguarding people, organizations, and systems from harm or damage. here are some of the most common models:

ACCESS CONTROL MODEL:

This model is used to regulate access to resources, systems, and data by controlling who is allowed to access what and under what circumstances. This model grants access privileges to users based on the work that they do within an organization. The model allows an administrator to assign a user to single or multiple roles according to their work assignments in which each role enables access to specific resources. Access control is a data security process that enables organizations to manage who is authorized to access corporate data and resources. Secure access control uses policies that verify users are who they claim to be and ensures appropriate control access levels are granted to users.

Access control is managed through several components:

1. Authentication
Authentication is the initial process of establishing the identity of a user. For example, when a user signs in to their email service or online banking account with a username and password combination, their identity has been authenticated. However, authentication alone is not sufficient to protect organizations' data.

2. Authorization
Authorization adds an extra layer of security to the authentication process. It specifies access rights and privileges to resources to determine whether the user should be granted access to data or make a specific transaction.

3. Access
Once a user has completed the authentication and authorization steps, their identity will be verified. This grants them access to the resource they are attempting to log in to.

4. Manage
Organizations can manage their access control system by adding and removing the authentication and authorization of their users and systems. Managing these systems can become complex in modern IT environments that comprise cloud services and on-premises systems.

5. Audit
Organizations can enforce the principle of least privilege through the access control audit process. This enables them to gather data around user activity and analyse that information to discover potential access violations.

1.A.) MANDATORY ACCESS CONTROL MODEL:

This model is used to enforce strict security policies by giving administrators the ability to set rules and permissions that cannot be overridden by users. Mandatory access control (MAC) is a security strategy that restricts the ability individual resource owners have to grant or deny access to resource objects in a file system. MAC criteria are defined by the system administrator, strictly enforced by the operating system (OS) or security kernel, and are unable to be altered by end users.
Often employed in government and military facilities, mandatory access control works by assigning a classification label to each file system object. Classifications include confidential, secret and top secret. Each user and device on the system is assigned a similar classification and clearance level. When a person or device tries to access a specific resource, the OS or security kernel will check the entity's credentials to determine whether access will be granted. While it is the most secure access control setting available, MAC requires careful planning and continuous monitoring to keep all resource objects' and users' classifications up to date. As the highest level of access control, MAC can be contrasted with lower-level discretionary access control (DAC), which allows individual resource owners to make their own policies and assign security controls.

1.B.) ROLE-BASED ACCESS CONTROL MODEL:

This model is used to grant access to resources based on an individual's role or job function within an organization. Role-based access control (RBAC) restricts network access based on a person's role within an organization and has become one of the main methods for advanced access control. The roles in RBAC refer to the levels of access that employees have to the network. Employees are only allowed to access the information necessary to effectively perform their job duties. Access can be based on several factors, such as authority, responsibility, and job competency. In addition, access to computer resources can be limited to specific tasks such as the ability to view, create, or modify a file. As a result, lower-level employees usually do not have access to sensitive data if they do not need it to fulfill their responsibilities. This is especially helpful if you have many employees and use third-parties and contractors that make it difficult to closely monitor network access. Using RBAC will help in securing your company’s sensitive data and important applications.

1. C.) DISCRETIONARY ACCESS CONTROL MODEL:

This model is used to give users more control over access to resources and data, allowing them to grant or deny access to others. Discretionary access control (DAC) is a type of security access control that grants or restricts object access via an access policy determined by an object's owner group and/or subjects. DAC mechanism controls are defined by user identification with supplied credentials during authentication, such as username and password. DACs are discretionary because the subject (owner) can transfer authenticated objects or information access to other users. In other words, the owner determines object access privileges.

1.D) ATTRIBUTE-BASED ACCESS CONTROL:

The Attribute-Based Access Control (ABAC) model is a type of access control model used to determine whether an entity (such as a user or a process) is allowed to access a particular resource (such as a file or a database). In an ABAC model, access decisions are made based on the attributes of the entity requesting access, the attributes of the resource being accessed, and the environmental attributes that may be relevant to the access request. Attributes can include things like user roles, job titles, departmental affiliations, security clearance levels, location, time of day, and many other factors that may be relevant to the access decision. The ABAC model provides a flexible and dynamic approach to access control, as it allows access decisions to be made based on a wide variety of attributes and conditions. It is commonly used in large organizations with complex access control requirements, as it can accommodate a wide variety of policies and rules.

BELL-LAPADULA

This Model was invented by Scientists David Elliot Bell and Leonard.J. LaPadula.Thus this model is called the Bell-LaPadula Model. This is used to maintain the Confidentiality of Security. Here, the classification of Subjects(Users) and Objects(Files) are organized in a non-discretionary fashion, with respect to different layers of secrecy.

It has mainly 3 Rules:

SIMPLE CONFIDENTIALITY RULE:

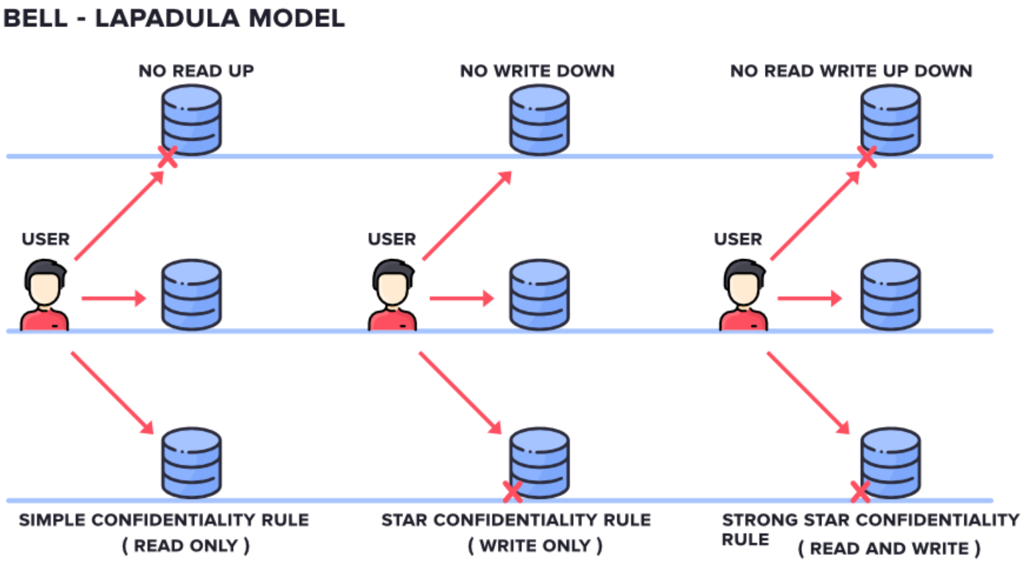
Simple Confidentiality Rule states that the Subject_can only Read the files on the Same Layer of Secrecy and the Lower Layer of Secrecy but not the Upper Layer of Secrecy, due to which we call this rule as NO READ-UP

STAR CONFIDENTIALITY RULE:

Star Confidentiality Rule states that the Subject_can only Write the files on the Same Layer of Secrecy and the Upper Layer of Secrecy but not the Lower Layer of Secrecy, due to which we call this rule as NO WRITE-DOWN

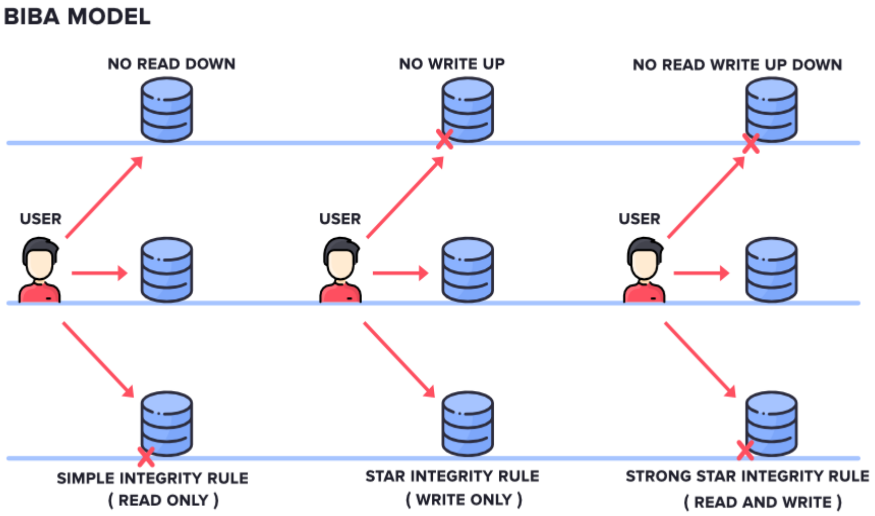
STRONG STAR CONFIDENTIALITY RULE:

Strong Star Confidentiality Rule is highly secured and strongest which states that the Subject_Can Read and Write the files on the Same Layer of Secrecy only and not the Upper Layer of Secrecy or the Lower Layer of Secrecy, due to which we call this rule as NO READ WRITE UP DOWN



BIBA:

This Model was invented by Scientist Kenneth .J. Bib**a**. Thus this model is called Biba Model. This is used to maintain the Integrity of Security. Here, the classification of Subjects(Users) and Objects(Files) are organized in a non-discretionary fashion, with respect to different layers of secrecy. This works the exact reverse of the Bell-LaPadula Model.

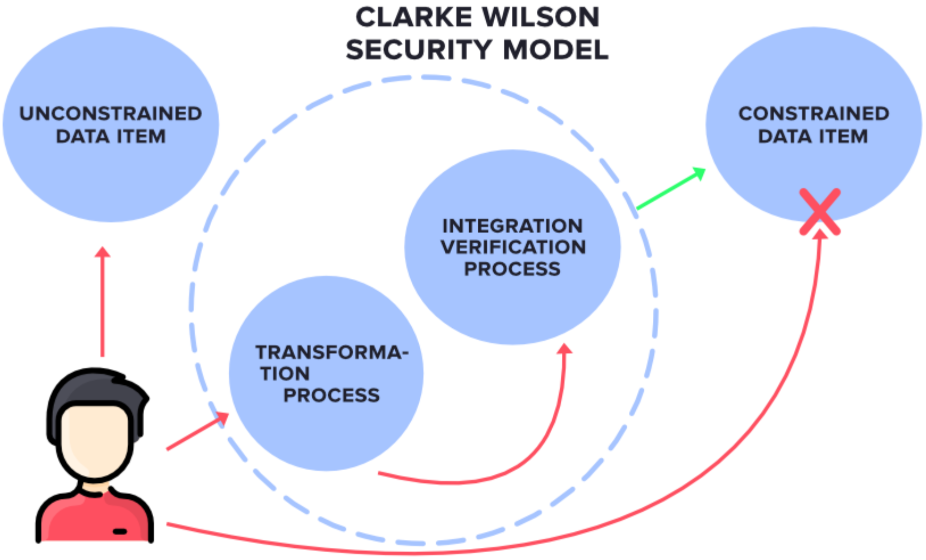


It has mainly 3 Rules:

SIMPLE INTEGRITY RULE:
Simple Integrity Rule states that the Subject can only Read the files on the Same Layer of Secrecy and the Upper Layer of Secrecy but not the Lower Layer of Secrecy, due to which we call this rule as NO READ DOWN.

STAR INTEGRITY RULE:
Star Integrity Rule states that the Subject can only Write the files on the Same Layer of Secrecy and the Lower Layer of Secrecy but not the Upper Layer of Secrecy, due to which we call this rule as NO WRITE-UP

STRONG STAR INTEGRITY RULE:
Clarke Wilson Security Model
This Model is a highly secured model. It has the following entities.



Subject: It is any user who is requesting for Data Items.

Constrained Data Items: It cannot be accessed directly by the Subject. These need to be accessed via Clarke Wilson Security Model.

Unconstrained Data Items: It can be accessed directly by the Subject.
The Components of Clarke Wilson Security Model.

Transformation Process: Here, the Subject's request to access the Constrained Data Items is handled by the Transformation process which then converts it into permissions and then forwards it to Integration Verification Process.

Integration Verification Process: The Integration Verification Process will perform Authentication and Authorization. If that is successful, then the Subject is given access to Constrained Data Items.

NON-INTERFERENCE MODEL:

The non-interference model in networking refers to a security model that aims to prevent unauthorized access and modification of data by ensuring that users or processes only have access to the resources they need to perform their tasks, and nothing more. In this model, each user or process is granted the minimum level of privilege necessary to carry out its function. This helps to limit the potential damage that can be caused by a compromised user or process. The non-interference model is often used in high-security environments, such as military and government organizations. In this model, the system is divided into several security levels or compartments, with each level having its own set of resources, users, and processes. Users at a higher security level cannot access resources at a lower level, and vice versa. This ensures that information cannot be leaked or modified between levels. Additionally, the non-interference model also includes auditing and monitoring features that track user activity and detect any suspicious or unauthorized behaviour. This helps to ensure that the system remains secure and that any potential threats are identified and addressed promptly. Overall, the non-interference model provides a robust and effective way to secure sensitive information and resources in a networked environment.