Experiment 1

Title: To learn about different hacking tools and Nmap (Network Mapper), Metasploit, Wireshark.

Aim: The aim of this experiment is to study and provide comprehensive understanding of key hacking tools, specifically focusing on Nmap (Network Mapper), Metasploit and Wireshark.

Objective:

1. Explore the core features and capabilities of Nmap, Metasploit and Wireshark.
2. Investigate real world applications and use cases of each hacking tools in network security and penetration testing.
3. Provide insights into the ethical consideration and responsible usage guidelines for employing hacking tools.

Requirement:

Hardware Requirement:

Computer System

Software Requirement:

Nmap (Network Mapper)

Metasploit

Wireshark

Theory:

Ethical Hacking Tools-

Automation has left its imprint on every industry out there and the real of ethical hacking is no different. With the onset of various tools in the ethical hacking industry it has been transformed. Ethical Hacking tools help in information gathering, creating backdoors and payloads, cracking passwords and array of the other activities.

Nmap (Network Mapper)-

Nmap short for network mapper is a reconnaissance tool that is widely used by ethical hackers to gather information about a target system. This information is a key to deciding the proceeding step to attack the target system. Nmap is a cross platform and works on Mac, Linux and Windows. It has gained immense popularity in the hacking community due to its ease of the use and powerful searching and scanning abilities.

Using Nmap you can-

1. Audit device Security
2. Detect open ports on remote hosts.
3. Network Mapping and enumeration
4. Find vulnerabilities inside any network.

Metasploit-

Metasploit is an open-source pen-testing framework written by ruby. It acts as a public resource for researching security vulnerabilities and developing code.

This allow a network administrator to break into his own network to identify security risks and Metasploit logo- ethical hacking tools edureka document which vulnerabilities need to be addressed first. It is also one of the few hacking tools used by beginner hackers to practise their skills. It also used to allow you to replicate websites for phishing and other social engineering purposes.

The framework includes a set of security tools that can be used to-

1. Evade detections Systems.

2. Run security vulnerability scans.
3. Execute remote attacks.
4. Enumerate networks and hosts.

Supported platform include:

1. Mac OS X
2. Linux
3. Windows

Wireshark-

Wireshark is an open source tool for profiling network traffic and analyzing packets. Such a tool is often referred to as a network analyzer, network protocol analyzer or sniffer.

Wireshark, formerly known as Ethereal, can be used to examine the details of traffic at a variety of levels ranging from connection-level information to the bits that make up a single packet. Packet capture can provide a network administrator with information about individual packets such as transmit time, source, destination, protocol type and header data. This information can be useful for evaluating security events and troubleshooting network security device issues.

Features:

1. Deep Inspection: Dissecting Network Protocols Layer by Layer
2. Live Capture: Witnessing Network Traffic in Real-Time
3. Offline Analysis: Reviewing Network Traffic at Your Convenience
4. Filtering: Zeroing in on Relevant Network Data
5. Color Coding: Visualizing Packet Types and Status
6. Graphical and Statistical Analysis: Visualizing Network Activity

Conclusion: Hence we had been successfully studied about the different hacking tools and also studied tools like Nmap(Network Mapper), Metaspoit and Wireshark also studied their different kinds of Functionalities.

Experiment 2

Title: Installation of Kali Linux and learn tools like sqlmap, autopsy, social engineering toolkit.

Aim: The aim of this experiment is to study and provide comprehensive understanding of key tools as well as installation of kali linux and learn tools like sqlmap, autopsy, social engineering toolkit.

Objective:

1. Explore the core features and capabilities of sqlmap, autopsy and social engineering toolkit.
2. To get deep knowledge about the kali linux and studied its properties.
3. Investigate this tools with real life applications and collaborate with them.

Requirement:

Hardware Requirement:

Computer System

Software Requirement:

1. Kali Linux
2. Sqlmap
3. Autopsy
4. Social engineering toolkit

Theory:

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

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

The following are the features of Kali Linux:

1. Over 600 Penetration Testing Tools Pre-installed
2. Full Customization of Kali ISOs
3. Developed in a Secure Environment
4. Adherence to the Filesystem Hierarchy Standard (FHS)
5. Live USB Boot
6. Kali Linux Full Disk Encryption
7. Kali Linux Amazon EC2 AWS Images
8. Kali Linux Metapackages
9. Automating Kali Linux Deployment
10. Kali Linux NetHunter

Steps to install kali linux:

1. Downloaded the iso file
2. Created a bootable drive
3. Accessed the Kali Installer Menu

4. Began the installation
5. Set up the Storage
6. Installed the GRUB bootloader

sqlmap

sqlmap goal is to detect and take advantage of SQL injection vulnerabilities in web applications. Once it detects one or more SQL injections on the target host, the user can choose among a variety of options to perform an extensive back-end database management system fingerprint, retrieve DBMS session user and database, enumerate users, password hashes, privileges, databases, dump entire or user’s specific DBMS tables/columns, run his own SQL statement, read specific files on the file system and more.

autopsy

The Autopsy Forensic Browser is a graphical interface to the command line digital forensic analysis tools in The Sleuth Kit. Together, The Sleuth Kit and Autopsy provide many of the same features as commercial digital forensics tools for the analysis of Windows and UNIX file systems (NTFS, FAT, FFS, EXT2FS, and EXT3FS).

Social Engineering Toolkit Usage

The Social-Engineer Toolkit (SET) is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of time. These kind of tools use human behaviors to trick them to the attack vectors.

Conclusion: Hence we had been successfully studied about the installation of the kali linux operating system and also learn the different kinds of tools like sqlmap, autopsy and social engineering toolkit.

Experiment 3

Title: To scan e-mail attachments for malware.

Aim: The aim of this experiment is to provide comprehensive understanding and key points of the scanning e-mail attachments for malware.

Objective:

1. Explore the core features and capabilities of the scanning e-mail attachments for malware.
2. Study brief about the malware.
3. Learned deeply about the malware and its functions.

Requirement:

Hardware Requirement:

Computer System

Software Requirement:

Theory:

Email attachment scanning is the process of checking the files that are attached to an email message for any signs of malware. Email attachment scanning can be done by using a software tool that scans the files before you download or open them, or by using an online service that analyzes the files for you. Email attachment scanning can help you detect and remove malware before it infects your computer or network.

Why is email attachment scanning important?

Email attachment scanning is a crucial part of computer maintenance and security, as malware can cause serious damage to your computer and data. Malware can delete, encrypt, or corrupt your files and folders, monitor your keystrokes, passwords, and online activity, send spam or phishing emails from your account, install other malware or viruses on your system, take control of your webcam or microphone, access your contacts, documents, or financial information, and slow down or crash your computer. Additionally, malware can spread from your computer to other devices or networks, putting your colleagues and clients at risk.

How do you scan your email attachments for malware?

There are various ways to scan your email attachments for malware, depending on the type of email service and software you use. For instance, you can use an antivirus or anti-malware program that scans your attachments automatically or on demand. You should make sure to update the program regularly and run a full scan periodically. Alternatively, you can use a web-based email service that scans your attachments before you download or open them. Gmail, Outlook, and Yahoo Mail have built-in security features that can detect suspicious attachments. Additionally, you can upload your attachments to VirusTotal, which scans them with multiple antivirus engines and gives a report of the results. Lastly, sandboxing tools such as Sandboxie can be used to isolate your email attachments from your system and run them in a virtual environment, allowing you to open them safely and observe their behavior.
Add your perspective

How do you educate your colleagues and clients about email attachment scanning?

Educating your colleagues and clients about email attachment scanning is essential to prevent malware infections and data breaches. It's important to explain the risks and consequences of malware, as well as how email attachments can be a source of infection. Show them how to scan their email attachments for malware using the methods mentioned above, or recommend tools or services

that you use. Additionally, teach them how to identify and avoid suspicious or unsolicited email attachments, such as those with unusual file names, extensions, or sizes, or that come from unknown or spoofed senders. Remind them to backup their data regularly and report any suspicious activity on their computers or networks. Finally, encourage them to ask questions and seek help if they need assistance with scanning email attachments.
Add your perspective

How do you test your email attachment scanning skills?

One way to test your email attachment scanning skills is to use a test file that simulates malware but does not actually harm your computer. For example, you can use the EICAR test file, which is a standard file that antivirus programs recognize as malware and react accordingly. You can download the EICAR test file from its official website and attach it to an email message. Then, you can scan the email attachment with your antivirus or anti-malware program, or with an online file scanner, and see if they detect and block the test file. If they do, it means that your email attachment scanning skills are working well. If they do not, it means that you need to update or change your program or service, or check your settings and preferences.

Conclusion: Hence we had been successfully completed the study of the scanning e-mail attachments for malware.

Experiment 4

Title: To study and implement the use of network reconnaissance tools like WHOIS, dig, traceroute, ns lookup to gather information about networks and domain registers.

Aim: The aim of this experiment is to study and implement the use of the network reconnaissance tools like WHOIS, dig, tracerout, nslookup to gather information about networks and domain registers.

Objective: 1. Learned different network tools that are widely used.

2. To gain knowledge about the how the working of the network devices.

3. Investigate this tools and their applications in real life.

Requirement:

Hardware Requirement:

Computer System

Software Requirement:

1. WHOIS
2. Dig
3. Traceroute
4. nslookup

Theory:

Traceroute-

The traceroute, tracer tot tracepath command is similar to ping but provides information about the path a packet takes. Traceroute sends packet to a destination, asking each internet router along the way to reply when it passes it on the packet. This will show you the path packets takes when you send them between your location and a destination.

WHOIS-

This whois command is looks up the registration record associated with a domain name. This can show you more information about who registered and owns a domain name, including their contact information.

Installation: sudo apt-get install whois

Commands: whois google.com

The whois protocol had its origin in the Arpanet Nicname protocol and was based on the NAME/FINGER protocol.

The whois was originally implemented on the network control program.

Dig-

Dig is a networking tool that can query DNS servers for information. It can be very helpful for diagnosing problems with domain pointing and is a way to verify that your configuration is working.

Installation:sudo apt-get install dig

Commands: dig google.com

The dig command output has the following sections:

1. Header
2. Question Section

3. Answer Section
4. Authority Section
5. Additional Section

Nslookup

Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS-related problems.

Installation:sudo apt-get install nslookup

Commands: nslookup google.com

Conclusion: In this experiment we had study and implement the use of the network reconnaissance tools like WHOIS, dig, traceroute, ns lookup for the purpose of the gathering information about the networks and domain registars.

Experiment 5

Title: To study and implement about Foot-printing and Reconnaissance.

Aim: The aim of this experiment is to study and implement about the footprinting and reconnassiance.

Objective:

1. Learned about the Footprinting.
2. To gain knowledge about the reconnaissance.

Requirement:

Hardware Requirement:

Computer System

Software Requirement:

Theory:

Footprinting means gathering information about a target system that can be used to execute a successful cyber attack. To get this information, a hacker might use various methods with variant tools. This information is the first road for the hacker to crack a system. There are two types of footprinting as following below.

- **Active Footprinting:** Active footprinting means performing footprinting by getting in direct touch with the target machine.
- **Passive Footprinting:** Passive footprinting means collecting information about a system located at a remote distance from the attacker.

Different kinds of information that can be gathered from Footprinting are as follows:

- The operating system of the target machine
- Firewall
- IP address
- Network map
- Security configurations of the target machine
- Email id, password
- Server configurations
- URLs
- VPN

Sources are as follows:

- **Social Media:** Most people have the tendency to release most of their information online. Hackers use this sensitive information as a big deal. They may create a fake account for looking real to be added as friends or to follow someone's account for grabbing their information.

- **JOB websites:** Organizations share some confidential data on many JOB websites like monsterindia.com. For example, a company posted on a website: "Job Opening for Lighttpd 2.0 Server Administrator". From this, information can be gathered that an organization uses the Lighttpd web server of version 2.0.

- **Google:** Search engines such as Google have the ability to perform more powerful searches than one can think and one had gone through. It can be used by hackers and attackers to do something that has been termed Google hacking. Basic search techniques combined with advanced operators can do great damage.

- **Social Engineering:** There are various techniques that fall in this category. A few of them are:

- **Eavesdropping:** The attacker tries to record the personal conversation of the target victim with someone that's being held over communication mediums like the Telephone.
- **Shoulder Surfing:** In this technique, Attacker tries to catch the personal information like email id, password, etc; of the victim by looking over the victim's shoulder while the same is entering(typing/writing) his/her personal details for some work.

- **Archive.org:** The Archived version refers to the older version of the website which existed a time before and many features of the website have been changed. archive.org is a website that collects snapshots of all the websites at a regular interval of time. This site can be used to get some information that does not exist now but existed before on the site.

- **An Organization's Website:** It's the best place to begin for an attacker. If an attacker wants to look for open-source information, which is information freely provided to clients, customers, or the general public then simply the best option is: "ORGANISATION's WEBSITE".

- **Using Neo Trace:** NeoTrace is a powerful tool for getting path information. The graphical display displays the route between you and the remote site, including all intermediate nodes and their information. NeoTrace is a well-known GUI route tracer program. Along with a graphical route, it also displays information on each node such as IP address, contact information, and location.

- **Who is:** This is a website that serves a good purpose for Hackers. Through this website information about the domain name, email-id, domain owner, etc; a website can be traced. Basically, this serves as a way for Website Footprinting.

Advantages:

- Footprinting allows Hackers to gather the basic security configurations of a target machine along with network route and data flow.
- Once the attacker finds the vulnerabilities he/she focuses on a specific area of the target machine.
- It allows the hacker to identify as to which attack is handier to hack the target system.

Counter Measures:

- Avoid posting confidential data on social media websites.
- Avoid accepting unwanted friend requests on social media platforms.
- Promotion of education on various hacking tricks.
- Usage of footprinting techniques for identifying and removing sensitive information from social media platforms.
- Proper configuration of web servers to avoid loss of information about system configuration.

Reconnaissance

Information Gathering and getting to know the target systems is the first process in ethical hacking. Reconnaissance is a set of processes and techniques (Footprinting, Scanning & Enumeration) used to covertly discover and collect information about a target system.

During reconnaissance, an ethical hacker attempts to gather as much information about a target system as possible, following the seven steps listed below −

- Gather initial information
- Determine the network range
- Identify active machines
- Discover open ports and access points
- Fingerprint the operating system
- Uncover services on ports
- Map the network

We will discuss in detail all these steps in the subsequent chapters of this tutorial. Reconnaissance takes place in two parts − **Active Reconnaissance** and **Passive Reconnaissance**.

Active Reconnaissance

In this process, you will directly interact with the computer system to gain information. This information can be relevant and accurate. But there is a risk of getting detected if you are planning active reconnaissance without permission. If you are detected, then system admin can take severe action against you and trail your subsequent activities.

Passive Reconnaissance

In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

Conclusion: Hence we had been successfully studied and implement about Foot-printing and Reconnaissance.

Experiment 6

Title: To study and implement about fingerprinting and packet tracing tools.

Aim: The aim of this experiment is to study and implement about the footprinting and reconnaissance.

Objective:

1. Learned about fingerprinting in the deep.
2. Learned about the different kinds of packet tracing tools.

Requirement:

Hardware Requirement:

Computer System

Software Requirement:

1. Wireshark
2. Snoop
3. Tcptrace

Theory:

Fingerprinting

The term OS fingerprinting in Ethical Hacking refers to any method used to determine what operating system is running on a remote computer. This could be –

- **Active Fingerprinting** − Active fingerprinting is accomplished by sending specially crafted packets to a target machine and then noting down its response and analyzing the gathered information to determine the target

OS. In the following section, we have given an example to explain how you can use NMAP tool to detect the OS of a target domain.

- **Passive Fingerprinting** − Passive fingerprinting is based on sniffer traces from the remote system. Based on the sniffer traces (such as Wireshark) of the packets, you can determine the operating system of the remote host.

We have the following four important elements that we will look at to determine the operating system −

- **TTL** − What the operating system sets the **Time-To-Live** on the outbound packet.
- **Window Size** − What the operating system sets the Window Size at.
- **DF** − Does the operating system set the **Don't Fragment** bit.
- **TOS** − Does the operating system set the **Type of Service**, and if so, at what.

By analyzing these factors of a packet, you may be able to determine the remote operating system. This system is not 100% accurate, and works better for some operating systems than others.

Packet Tracing Tools-

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

Packet Tracing Tools-

1. Wireshark

2. Tcpdump

3. Kismet

4. Fiddler

5. Capsa

6. Scapy

7. Paessler PRTG

8. OmniPeek

9. NetFlow Analyzer

10. Ettercap

11. EtherApe

12. Snort

13. Justniffer

14. Microsoft Network Monitor

15. NetFlow

16. Tcptrace

17. Snoop
18. SmartSniff

Conclusion: Hence we had been successfully studied and implement about fingerprinting and packet tracing tools about their functionality.

Experiment 7

Title: To study and implement about system hacking using session cookies.

Aim: The aim of this experiment is to study and implement about the different kinds of system hacking using session cookies.

Objective:

1. Too deeply gain knowledge about the different kinds of system hacking in ethical hacking.
2. To study about the session cookies and their working.
3. To study and also implement the different kinds of the system hacking.

Requirement:

Hardware Requirement:

Computer System

Software Requirement:

Theory:

It's a dangerous kind of cyberattack that you could unknowingly be vulnerable to. In fact, a recent Stake study found that 31% of ecommerce applications are vulnerable to session hijacking. Also known as cookie hijacking, session hijacking is a type of attack that could result in a hacker gaining full access to one of your online accounts.

Session hijacking is such a scary concept because of just how many sites we login to each and every day. Take a second and think about how many sites you access daily that require you to login in with a set of credentials. For the vast majority of us, it's a number that's much higher than just one or two. It's also a number that has most likely been steadily growing over time, as more and more online services become a part of our increasingly “connected” lifestyles. And since we store extremely sensitive information all over the place online these days, such as credit card or social security numbers, the effects can be devastating.

What Is a Session?

Before we get into session hijacking, let’s first review what exactly we mean by a “session.” HTTP is inherently stateless, which means that each request is carried out independently and without any knowledge of the requests that were executed previously. In practical terms, this means that you’d have to enter your username and password again for every page you viewed. As a result, the developers needed to create a way to track the state between multiple connections from the same user, rather than asking them to re-authenticate between each click in a web application.

Sessions are the solution. They act as a series of interactions between two devices, for example your PC and a web server. When you login to an application, a session is created on the server. This maintains the state and is referenced during any future requests you make.

These sessions are used by applications to keep track of user-specific parameters, and they remain active while the user remains logged in to the system. The session is destroyed when you log out, or after a set period of inactivity on your end. At that point, the user’s data is deleted from the allocated memory space.

Remote server remember that you’re logged in and authenticated. Because this kind of attack requires the attacker to have knowledge of your session cookie, it’s also sometimes referred to as cookie hijacking. It’s one of the most popular methods for attacking client authentication on the web.

What is Session Hijacking?

Session hijacking occurs when a user session is taken over by an attacker. As we discussed, when you login to a web application the server sets a temporary session cookie in your browser. This lets the remote server remember that you're logged in and authenticated. Because this kind of attack requires the attacker to have knowledge of your session cookie, it's also sometimes referred to as cookie hijacking. It's one of the most popular methods for attacking client authentication on the web.

Common Methods of Session Hijacking

1. Session Fixation
2. Session Sniffing
3. Cross-Site Scripting
4. Malware
5. Brute Force

How to Prevent Session Hijacking

While there are many different ways for hackers to carry out session hijacking attacks, the good news is that there are relatively simple security measures and best practices you can employ to protect yourself. Different ones protect against different session hijacking methods, so you'll want to enact as many of them as you can. Here are some of the most common prevention measures that you'll want to start with:

1. Use HTTPS On Your Entire Site

As we've seen, using HTTPS only on login pages won't keep you fully safe from session hijacking. Use SSL/TLS on your entire site, to encrypt all traffic passed between parties. This includes the session key. HTTPS-everywhere is widely used by major banks and ecommerce systems because it completely prevents sniffing attacks.

Conclusion: Hence we had been studied the system hacking using the session cookies and implement it.

Experiment 8

Title: To find vulnerabilities for any website using Nikto.

Aim: The aim of this experiment is to find out the different kinds of vulnerabilities of any given website by using Nikto tool.

Objective:

Requirement:

Hardware Requirement:

Computer System

Software Requirement:

Nikto

Theory:

Before attacking any website, a hacker or penetration tester will first compile a list of target surfaces. After they've used some good recon and found the right places to point their scope at, they'll use a web server scanning tool such as Nikto for hunting down vulnerabilities that could be potential attack vectors.

Nikto is a simple, open-source web server scanner that examines a website and reports back vulnerabilities that it found which could be used to exploit or hack the site. Also, it's one of the most widely used website vulnerabilities tools in the industry, and in many circles, considered the industry standard.

Although this tool is extremely effective, it's *not* stealthy at all. Any site with an intrusion-detection system or other security measures in place will detect that it's being scanned. Initially designed for security testing, stealth was never a concern.

The Right Way to Use Nikto

If you just run Nikto by itself on a targeted website, you may not know what to do with the information from the scan. Nikto is actually more like a laser pointer to call in a much larger strike, and you'll see how that plays out in a little bit.

First, let's talk about the target surface. This is pretty much anywhere a hacker will attempt to attack and could include things such as network-exposed printers and a web server. When we get to using Nikto later, we'll need to provide it with one of three different types of information: an IP address for a local service, a web domain to attack, or an SSL/HTTPS website.

Before diving right into a scan with Nikto, it's better to do some additional reconnaissance using an open-source intelligence tool such as Maltego. Tools like this can help build a profile and a more focused list of available targets that should be concentrated on. Once that's done, Nikto can be used to hone in on potential vulnerabilities for targets on the list.

Steps:

- Install Nikto
- Get to Know Nikto
- Use the Basic Syntax
- Scan an SSL-Enabled Website
- Scan an IP Address
- Scan an HTTP Website
- Pair Scans with Metasploit

Conclusion: In this experiment we had been able to find out the different kinds of the vulnerabilities in the website using the Nikto.

Experiment 9

Title: To study and implement about sniffing and their tools.

Aim: The aim of this experiment is to study and implement about the sniffing, how it work and also learn their different kinds of tools.

Objective:

Requirement:

Hardware Requirement:

Computer System

Software Requirement:

Auvik.

SolarWinds Network Packet Sniffer.

Wireshark.

Theory:

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is also called wiretapping applied to the computer networks.

There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

What can be sniffed?

One can sniff the following sensitive information from a network −

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

Types of Sniffing

Sniffing can be either Active or Passive in nature.

Passive Sniffing

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

Active Sniffing

In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting **address resolution packets** (ARP) into a target network to flood on the switch **content addressable**

memory (CAM) table. CAM keeps track of which host is connected to which port.

Protocols which are affected

Protocols such as the tried and true TCP/IP were never designed with security in mind and therefore do not offer much resistance to potential intruders. Several rules lend themselves to easy sniffing −

- **HTTP** − It is used to send information in the clear text without any encryption and thus a real target.
- **SMTP** (Simple Mail Transfer Protocol) − SMTP is basically utilized in the transfer of emails. This protocol is efficient, but it does not include any protection against sniffing.
- **NNTP** (Network News Transfer Protocol)− It is used for all types of communications, but its main drawback is that data and even passwords are sent over the network as clear text.
- **POP** (Post Office Protocol) − POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.
- **FTP** (File Transfer Protocol) − FTP is used to send and receive files, but it does not offer any security features. All the data is sent as clear text that can be easily sniffed.
- **IMAP** (Internet Message Access Protocol) − IMAP is same as SMTP in its functions, but it is highly vulnerable to sniffing.
- **Telnet** − Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and hence, it can be easily sniffed.

Sniffing Tools

1. **BetterCAP:** The BetterCAP tool is a very powerful, flexible, and portable best software tool created to perform various types of MITM

attacks against networks and manipulate its HTTP, HTTPS, and TCP traffic in real-time, sniffing it for as well as credentials, and much more through it.

2. **Ettercap:** Ettercap tool is a software comprehensively sharp tool suited for man-in-the-middle attacks for networks. It has features as well as sniffing of live connections, content filtering.

3. **Wireshark:** The Wireshark tool is one of the most widely common software as known and uses packet sniffers. It offers an unlimited number of features designed to implement and assist in the dissection and analysis of traffic for it. The Wireshark packet sniffing tool is known for both its data capture and analysis capabilities.

4. **Tcpdump:** The tcpdump tool is a well-known command-line packeting analyzer. It provides the ability to intercept and ability to observing TCP/IP and other packets during transmission over the network.

5. **WinDump:** A Windows port of the popular to Linux as well as packet sniffers at tcpdump, which is a command-line tool that is perfect for displaying header information through it. Due to the success of tcpdump on Unix-like operating systems os, it was “ported over” to the windows platforms to it.

6. **OmniPeek:** This tool is manufactured by WildPackets, OmniPeek is a commercial (working) product that is the evolution rise of the as well as product EtherPeek tool, Omnipeek by Savvius is innovated for to larger the networks with a vast amount of data running through them every

second and At its core, its performances, analytics, and forensics tool providing the best functional as well as in-depth closely analysis.

7. **Dsniff:** It is a pair of tools designed to perform sniffing packets with differentiating protocols with the intention of intercepting and revealing passwords as well the Dsniff tool is designed for the Unix and Linux platforms and does not have a full equivalent on the Windows platforms for support.

8. **MSN Sniffer:** This MSN Sniffer is a sniffing utility system that is specifically designed for sniffing traffic generated by the MSN Messenger GUI application.

9. **EtherApe:** This tool is a Linux/Unix GUI tool designed to display graphically a system's internal as incoming and outgoing connections.

10. **NetWitness NextGen:** It includes a hardware-based sniffer, along with other features designed to monitor and analyze all traffic on a network. This tool is used by the FBI and other law enforcement agencies for verification.

Conclusion: Here we had been studied about the sniffing and their working and their tools and also implement it.

Experiment 10

Title: To perform Denial of Service(DoS) attack using hping3.

Aim: The aim of this experiment is to perform practical on the Denial of Service(DoS) attack b using the hping3.

Objective:

1. The main purpose of this experiment is to gain knowledge about the Denial of Service(DoS).
2. The goal of this practical is to perform practical on Denial of Service(DoS) and also to implement it.
3. Here we all are also able to perform this attack by using the hping3.

Requirement:

Hardware Requirement:

Computer System

Software Requirement:

hping3

Theory:

A denial-of-service (DoS) attack is a cyberattack on devices, information systems, or other network resources that prevents legitimate users from accessing expected services and resources.

This is usually accomplished by flooding the targeted host or network with traffic until the target can't respond or crashes. DoS attacks can last from a few hours to many months, costing companies and consumers time and money while their resources and services are unavailable.

KEY TAKEAWAYS

- A denial-of-service (DoS) is a form of cyberattack that prevents legitimate users from accessing a computer or network.
- In a DoS attack, rapid and continuous online requests are sent to a target server to overload the server's bandwidth.
- Distributed denial-of-service (DDoS) attacks leverage a wide web of computers or devices infected with malware to launch a coordinated barrage of meaningless online requests, blocking legitimate access.

How Denial-of-Service (DoS) Attacks Work

DoS attacks are on the rise as businesses and consumers use more digital platforms to communicate and transact with each other.

Cyberattacks are often launched to steal personally identifiable information (PII), causing considerable damage to companies' financial pockets and reputations. Data breaches can target a specific company or a host of companies at the same time. For example, a company with high-security protocols in place may be attacked through a member of its supply chain that has inadequate security measures. When multiple companies have been selected for an attack, the perpetrators can use a DoS approach.

This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games, such as popular Minecraft servers. Increasingly, DoS attacks have also been used as a form of resistance. Richard Stallman has stated that DoS is a form of 'Internet Street Protests'. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

What’s hping3?

hping3 is a free packet generator and analyzer for the TCP/IP protocol. Hping is one of the de-facto tools for security auditing and testing of firewalls and networks, and was used to exploit the Idle Scan scanning technique now implemented in the Nmap port scanner. The new version of hping, hping3, is scriptable using the Tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet manipulation and analysis in a very short time.

Like most tools used in computer security, hping3 is useful to security experts, but there are a lot of applications related to network testing and system administration.

hping3 should be used to…

- Traceroute/ping/probe hosts behind a firewall that blocks attempts using the standard utilities.
- Perform the idle scan (now implemented in nmap with an easy user interface).
- Test firewalling rules.
- Test IDSes.
- Exploit known vulnerabilties of TCP/IP stacks.
- Networking research.
- Learn TCP/IP (hping was used in networking courses AFAIK).
- Write real applications related to TCP/IP testing and security.
- Automated firewalling tests.
- Proof of concept exploits.
- Networking and security research when there is the need to emulate complex TCP/IP behaviour.

- Prototype IDS systems.
- Simple to use networking utilities with Tk interface.

Conclusion: In this experiment we had perform the Denial of Service (DoS) attack using hping3 and learn deeply about it.