Module-2

Q-1 What are the types of hacker ?

A-1

There are different types of hackers, and they are classified based on their intentions and motives. Here are some common types of hackers:

1. White hat hacker: White hat hackers, also known as ethical hackers, are individuals who use their hacking skills to find vulnerabilities in computer systems and networks for the purpose of improving security. White hat hackers work with organizations to identify and fix security issues and vulnerabilities to prevent malicious attacks.
2. Black hat hacker: Black hat hackers are individuals who use their hacking skills to gain unauthorized access to computer systems and networks for personal gain or malicious purposes. Black hat hackers are often involved in criminal activities such as stealing sensitive data, distributing malware, or conducting financial fraud.
3. Grey hat hacker: Grey hat hackers are individuals who operate in a morally ambiguous area between black and white hat hacking. They may find vulnerabilities in systems without permission but do not intend to cause harm. Grey hat hackers often report their findings to the affected organizations for a reward or recognition.
4. Script kiddie: Script kiddies are individuals who use pre-existing tools and scripts to launch attacks on computer systems and networks without any technical expertise or knowledge of coding. They are often motivated by the desire for recognition among peers or to cause chaos.

5. Hacktivist: Hacktivists are individuals who use their hacking skills for political or social activism. They may use their skills to gain unauthorized access to computer systems and networks to protest against political or social issues, and to promote their message.
6. State-sponsored hacker: State-sponsored hackers are individuals who are hired by government agencies or organizations to launch cyber-attacks on other governments or organizations for espionage, sabotage, or disruption. They are often highly skilled and have access to advanced tools and techniques.

Q-2 Explain in brief – ethical hacking and cyber security .

A-2

Cybersecurity is the practice of protecting computer systems, networks, and sensitive information from unauthorized access, theft, and damage. Cybersecurity involves the use of various technologies, processes, and policies to secure digital assets and prevent cyber-attacks. Cybersecurity aims to provide confidentiality, integrity, and availability of information systems and networks.

Ethical hacking, also known as "penetration testing" or "pen testing," is a form of cybersecurity testing that involves simulating attacks on computer systems and networks to identify vulnerabilities and weaknesses. Ethical hackers use the same techniques as malicious hackers to identify security flaws and report them to the organization to fix them before malicious actors can exploit them. Ethical hacking is an important part of cybersecurity as it helps organizations to identify and mitigate security risks before they can cause harm.

Q-3 Explain Foot printing Methodology.

A-3

Footprinting is a process of gathering information about a target organization or system that can be used to identify vulnerabilities and plan further attacks. It is an essential part of the reconnaissance phase of a cyber attack and involves several steps. Here is a brief explanation of the footprinting methodology:

1. Passive footprinting: This involves gathering information about the target organization or system from publicly available sources, such as websites, social media platforms, and search engines. The goal is to gather as much information as possible without raising any red flags.
2. Active footprinting: This involves using more intrusive techniques to gather information about the target organization or system. This can include scanning the target's network to identify open ports, running vulnerability scans, and using social engineering techniques to gather information from employees.
3. Network mapping: This involves creating a map of the target's network and identifying all the devices, servers, and applications that are in use. This helps the attacker to identify potential entry points and weaknesses in the network**.**
4. Enumeration: This involves using various techniques to gather information about the target's network services, such as operating system information, user account information, and network configuration details. This information can be used to identify vulnerabilities that can be exploited in further attacks.
5. Vulnerability identification: This involves using the information gathered during the footprinting process to identify potential vulnerabilities that can be exploited in further attacks. This can

include software vulnerabilities, misconfigurations, and weak passwords.

Q-4 Find Basic Information using google advance search operator and pipl search

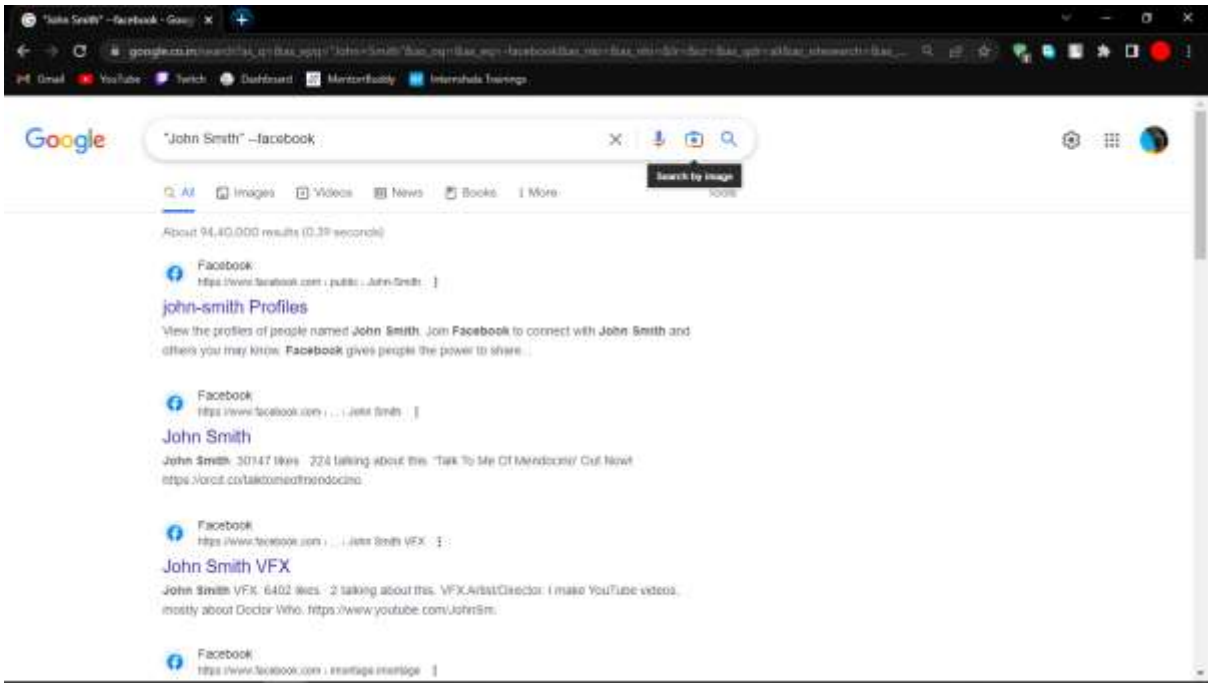
A-4

1. Google Advanced Search Operators:

a. Use quotation marks ("") to search for an exact phrase. For example, "John Smith" will only return results that include the exact phrase "John Smith".

b. Use the minus sign (-) to exclude specific terms from your search. For example, "John Smith" -Facebook will exclude any results that include the term "Facebook".

c. Use the site: operator to search for information on a specific website. For example, site:linkedin.com "John Smith" will only return results from LinkedIn that include the exact phrase "John Smith".



2. Pipl Search:

Pipl is a search engine that specializes in finding information about people. It searches across a variety of sources, including social media profiles, public records, and online directories. Here's how to use Pipl:

a. Go to pipl.com and enter the person's name, email, username, or phone number in the search bar.

b. Pipl will then search its database for any matches and provide you with basic information such as the person's name, age, location, and social media profiles.

c. You can also use the advanced search options to narrow down your search results by location, age, or profession.

It's important to note that both Google advanced search operators and Pipl search can provide basic information about a person, but they should not be used for malicious purposes or to violate someone's privacy. Always use these tools responsibly and with respect for others' privacy.

Q-5 Find Vulnerability tool and check port and service.

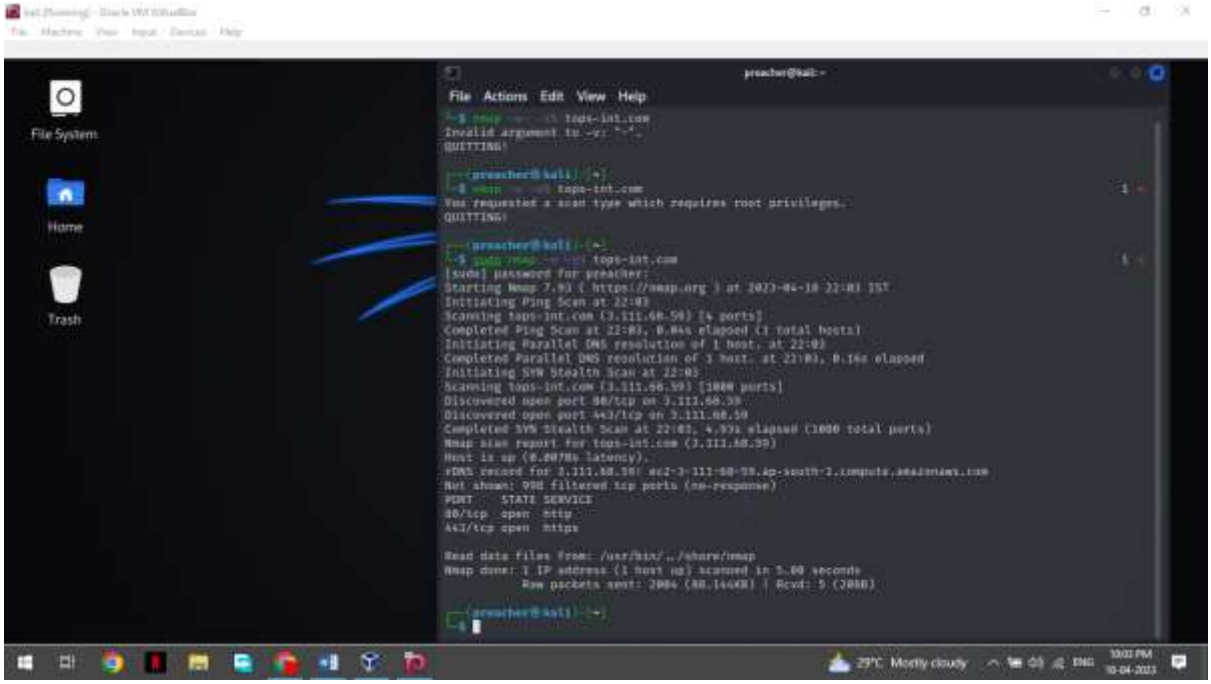
A-5

Nmap is a powerful open-source tool that can be used for port scanning, OS detection, and vulnerability assessment. It can be run from the command line and has a variety of scanning options and scripts available.

To check for open ports and services on a network using Nmap, for example, you can use the following command:

Nmap –v- -sS <target ip addresses>

This is use as stealth scan for Finding open ports and services on a target Ip.


File System
Home
Trash
preacher@kali: ~
File Actions Edit View Help
Invalid argument to -v: '-'.
QUITTING!
You requested a scan type which requires root privileges.
QUITTING!
[sudo] password for preacher:
Starting Nmap 7.93 (https://nmap.org) at 2023-04-10 22:03 IST
Initiating Ping Scan at 22:03
Scanning tops-int.com (3.111.60.59) [4 ports]
Completed Ping Scan at 22:03, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:03
Completed Parallel DNS resolution of 1 host. at 22:03, 0.16s elapsed
Initiating SYN Stealth Scan at 22:03
Scanning tops-int.com (3.111.60.59) [1000 ports]
Discovered open port 80/tcp on 3.111.60.59
Discovered open port 443/tcp on 3.111.60.59
Completed SYN Stealth Scan at 22:03, 4.93s elapsed (1000 total ports)
Nmap scan report for tops-int.com (3.111.60.59)
Host is up (0.0078s latency).
rDNS record for 3.111.60.59: ec2-3-111-60-59.ap-south-1.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
443/tcp open https
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.08 seconds
Raw packets sent: 2004 (88.144KB) | Rcvd: 5 (200B)
29°C Mostly cloudy
ENG
10:03 PM
10-04-2023