KCA

UNIVERSITY

~1989~

CAT 1

GROUP H MEMBERS.

20/03491	WACHIRA VICTOR ALVIN.
20/03059	NZUKI BRIAN MUUO.
20/04744	NGUGI FRANCIS.
20/03488	MURIUKI CAXTON MUNENE.
20/03763	KANGANGA MARGARET NYOKABI.
20/04915	JUMA BASIL WASONGA.
20/04218	ZAMZAM MOHAMMED DIBA.
20/03697	BUNDI JOY WANJIKU.
20/03963	WAMBUI HOPESUSAN WANJERI.
20/03433	MUTAVE JOHN.
19/03231	NIGEL MUAKA

1. **Discuss firewalls and their various uses in security.**

A mechanism to filter out malicious traffic before it crosses the network perimeter,

Uses of Firewalls.

1) ***Prevents the Passage of Unwanted Content***

Without a secure firewall, unwanted content can penetrate the system with ease. Most operating systems come with a firewall that can efficiently block malicious and unwanted internet information. Every time a new system is put to use, the user must verify whether a firewall already exists or not; if not, a third-party firewall can be installed.

2) ***Prevents Unauthorized Remote Access***

A rigorous firewall eliminates any chance that a potential hacker may get remote access to a system. Such remote access is wholly prohibited and may also be meant to be damaging. To safeguard your data, transactions, and other sensitive information, you need a robust firewall. For businesses, the loss of sensitive information and data can spell disaster.

3) ***Prevents Indecent Content***

Young minds can be harmed by exposure to indecent content, leading to odd habits and immoral actions. By blocking the entry of immoral and indecent content, a robust firewall safeguards the computer systems, enabling parents to keep their kids secure.

4) ***Guarantees Security Based on Protocol and IP Address***

The use of hardware firewalls for protocol-based traffic analysis is advantageous. Every time a connection is made, a record of the activities is kept from the start to the finish, helping to protect the system.

5) ***Protects Conversations and Coordination Contents***

No company can simply afford the cost of such vital content being leaked because the majority of the content from these coordinating operations must be confidential and must be safeguarded effectively. A firewall successfully protects the systems and permits a secure and safe flow of information, giving the stakeholders a sense of security.

2. **Discuss the emerging IoT technologies and Address IoT Security Issues**

- ***Blockchain***

  Blockchain technology is a fantastic fit for IoT applications since they are dispersed by nature, enable thriving interaction between diverse network nodes, and ensure safe record keeping.

- ***Smart Cities***

Over the past five years, a number of governmental organizations have started IoT technology projects that will completely transform cities. Using vast volumes of data, the government will be able to adopt many intelligent solutions for a variety of problems, including citizen safety, energy use, transportation congestion, sustainable development, and more.

- ***IoT Powered with 5G Technology***

  Not only is 5G technology a new era in wireless technology, but The importance of 5G technology also lies in the fact that reliable connectivity will lead to IoT devices that perform more reliably.

  The benefits of 5G include lower latency, network slicing, real-time data processing, wide coverage, and real-time data processing.

- ***Traffic Management***

  Many organizations these days are giving arrangements and solutions that utilize IoT-installed technology in traffic systems and vehicles to sketch more smart traffic networks, presumed to reduce unnecessary traffic and congestion.

- ***Digital Twin***

  A "digital twin" is a virtual representation that serves as the real-time digital equivalent of a physical object or process. It can be exercised for varied things such as diagnosing, optimizing, monitoring, and controlling asset utilization and performance.

- ***Voice Activated IoT Devices***

  Artificial intelligence-powered virtual assistants like Google Assistant, Amazon Echo, and Siri, as well as voice-based user interfaces built by Apple, have raised the bar for voice-based user interfaces.

  Voice biometry is another fascinating advancement in voice recognition technology. Speech biometry enables businesses to create a digital profile of a person's voice by examining a range of distinct traits like pitch, intensity, tone, dominating frequencies, dynamics, etc.

3. Discuss Cryptography; encryption, signatures, hashing, and PKI, etc.

Encryption: This process converts ordinary text—such as a text message or email—into "ciphertext," an unintelligible format. This contributes to maintaining the privacy of digital data that is either stored on computer systems or sent over a network like the Internet.

Signature: This refers to the typical pattern or footprint of a malicious assault on a computer network or system.

Hashing is the process of transforming any given string of characters into another value. **Public key infrastructure (PKI):** In order to create, administer, distribute, utilize, store, and revoke digital certificates, as well as manage public-key encryption, a public key infrastructure, or PKI, must be in place. PKI is a collection of roles, policies, hardware, software, and procedures.

4. **Discuss scanning in ethical hacking, including major types, scanning techniques, and common scanning tools.**

Scanning is a logical extension (and overlap) of active reconnaissance that helps attackers identify specific vulnerabilities.
Network scanning can be classified into two main categories:

(i) Port scanning: Scanning is a process used to identify active ports on the network. A port scanner sends client requests to the range of ports on the target network and then saves the details about the ports that send a response back.
There are different types of port scanning. Below is a list of some of the most commonly used ones:

1) TCP scanning
2) SYN scanning
3) UDP scanning
4) ACK scanning
5) Window scanning
6) FIN scanning

(i) Vulnerability scanning is a type of network scanning used for ethical hacking to find out weaknesses in the network. This type of scanning identifies vulnerabilities that occur due to poor programming or misconfiguration of the network.

Scanning Tools

1. Nmap for network scanning

Nmap is a free and open-source network scanner. You can scan a network with Nmap either by using the IP address of the target:

2. Nikto for network scanning.

Nikto is a web server scanner that tests for dangerous files and outdated service software. And these details can be exploited and used to hack the network. Nikto is designed to scan the web server in the quickest possible time.

3. Nessus for Network Scanning

5. **Discuss in detail the methodology you would follow in conducting a vulnerability assessment in an organization.**

The assessment would be conducted in the following order:

Phase 1 — Reconnaissance

This is a set of techniques like footprinting, scanning, and enumeration, along with processes used to discover and find information about the target system.

1. Information gathering: The goal here is to gather as much intriguing, novel, and vital information as you can on the target. And to accomplish this, a variety of tools are accessible, which hackers employ to thwart any actually planned attacks.
2. Finding the network range — After learning the target IP address, the network range needs to be found. The maximum number of networks that will provide a clear plan and hacking matrix must be determined.
3. Finding the active machines on the target network range is the first step in identifying the active machines. Pinging the target network is a straightforward method. We must follow the correct procedure in order to finish the process without getting caught by the host or refused.

4. Finding open ports and access points — An ethical hacker starts the port scanning procedure to find the open TCP and UDP access port points after detecting the network range and active computer.
5. OS fingerprinting is the method of discovering the operating system that is installed on the target device. So, OS The method by which we compute and identify the operating system of a remote computer is called fingerprinting.
6. Fingerprinting Services — These include delivering carefully constructed packets to a target system and then recording their response. It is examined by compiling the data to identify the target OS.
7. Network mapping is the examination of a network's physical connectedness. In-network mapping, which is distinct from network discovery or network enumerating that results in the identification of the features of the devices, allows an ethical hacker to identify the devices on the network and their connectivity.

Phase 2- Scanning

Vulnerability To identify network flaws, scanning will be utilized. It will be used to find network vulnerabilities brought on by subpar programming or incorrect configuration.

Scanning Tools to be used

1. Nmap for network scanning

Nmap is a free and open-source network scanner. You can scan a network with Nmap either by using the IP address of the target:

2. Nikto for network scanning

Nikto is a web server scanner that tests for dangerous files and outdated service software. And these details can be exploited and used to hack the network. Nikto is designed to scan the web server in the quickest possible time.

3. Nessus for Network Scanning

Phase 3: Access the system.

System hacking involves first accessing the passwords.

A dictionary attack is cracking an application that runs against user accounts that have files loaded. A brute force attack tries every character combination and tests it by the computer until the password is compromised. Rule-Based Offense When the attacker learns something about the password, they launch the attack.