Cyber Security

Subject Code:-102045607

Unit-3 Fundamentals of Ethical hacking and social engineering

Ethical Hacking Concepts and Scopes

Ethical Hacking

- Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities so as to ensure system security.
- It focuses on simulating techniques used by attackers to verify the existence of exploitable vulnerabilities in the system security.
- Ethical hackers performs security assessment of their organization with the permission of concerned authorities.
- Ethical Hacking sometimes called as **Penetration Testing** is an act of intruding/penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages.

Ethical Hacking Concepts and Scopes

Why Ethical Hacking is Necessary

- To beat a hacker, you need to think like one!
- The company employs an Ethical hacker to protect and secure their data. The Ethical hacker's tests do not always mean a system is attacked by malicious attackers. Sometimes, it means the hacker is preparing and protecting their data in precaution.

Some of the advanced attacks caused by hackers include:-

- Piracy
- Vandalism
- Credit card theft
- Theft of service
- Identity theft
- Manipulation of data
- Denial-of-service Attacks

Ethical Hacking Concepts and Scopes

Skills of an Ethical Hacker

1. **Technical Skills**
    - The Ethical Hackers must have strong knowledge in all Operating Systems like Windows, Linux, and Mac.
    - The Ethical Hackers should be skilled with Networking and have a strong knowledge of basic and detailed concepts in technologies, software, and hardware applications.
    - Ethical Hackers must know all kinds of attacks.

Ethical Hacking Concepts and Scopes

Skills of an Ethical Hacker

2. Non-Technical Skills

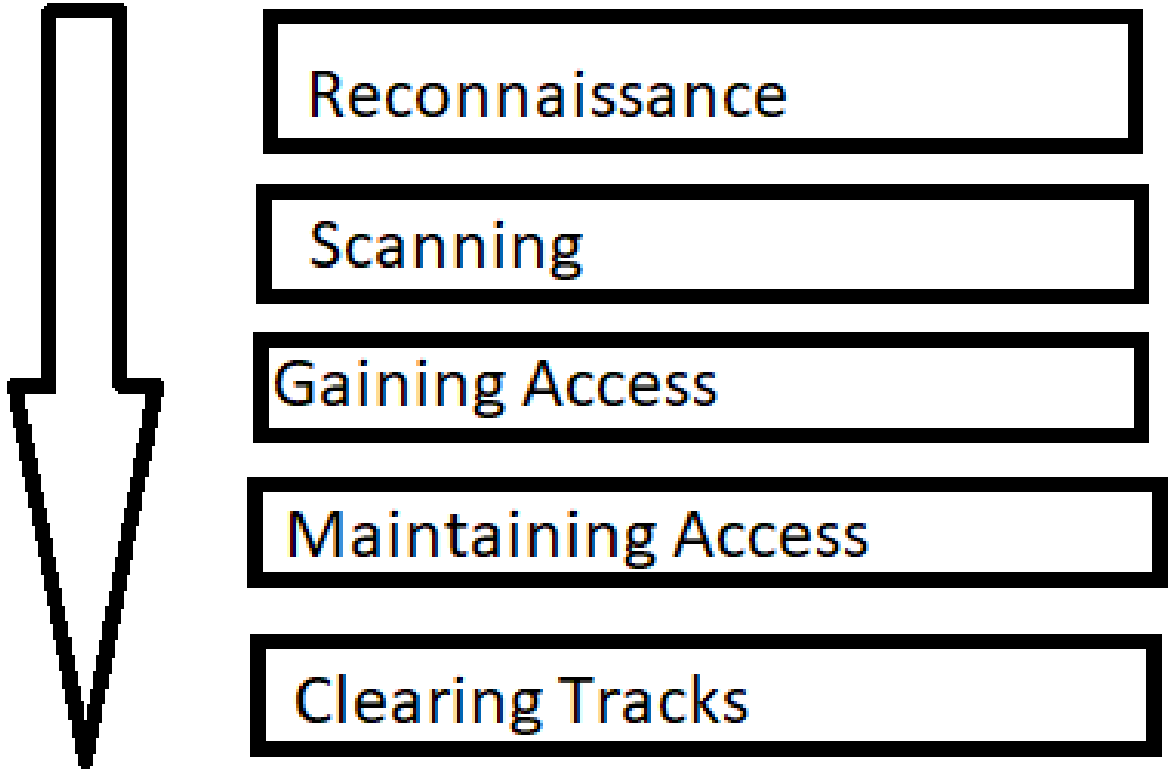
- Communication Skills
- Learning Ability
- Problem-solving skills
- Proficient in the security policies
- Awareness of laws, standards, and regulations.

Ethical Hacking Concepts and Scopes

Scope of Ethical Hacking:-

- Ethical hacking is generally used as penetration testing to detect vulnerabilities, risk and identify the loopholes in a security system and to take corrective measures against those attacks.
- Ethical hacking is a key component of risk evaluation, auditing, and counter-frauds.
- The scope for the Ethical Hackers is high and it is one of the rapidly growing careers at present as many malicious attackers cause a threat to the business and its networks.
- Industries like Information Technology and Banking Sectors hire several Ethical hackers to protect their data and infrastructure. Also, in the upcoming days, the demand for this profile is going to be high compared to other profiles due to an increased threat of vulnerabilities.

Phases of ethical hacking



Phases of ethical hacking

1. Reconnaissance:

This is the first step of Hacking. It is also called as **Footprinting** and **information gathering** Phase. This is the preparatory phase where we collect as much information as possible about the target. We usually collect information about three groups,

- Network
- Host
- People involved

There are two **types of Footprinting**:

Active: Directly interacting with the target to gather information about the target. Eg Using Nmap tool to scan the target

Passive: Trying to collect the information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

Phases of ethical hacking

2. Scanning:

Three types of scanning are involved:

- **Port scanning:** This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.
- **Vulnerability Scanning:** Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools
- **Network Mapping:** Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the haking process.

Phases of ethical hacking

3. Gaining Access:

- This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

4. Maintaining Access:

- Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

Phases of ethical hacking

5. Clearing Track:

- No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

Enterprise Information Security Architecture

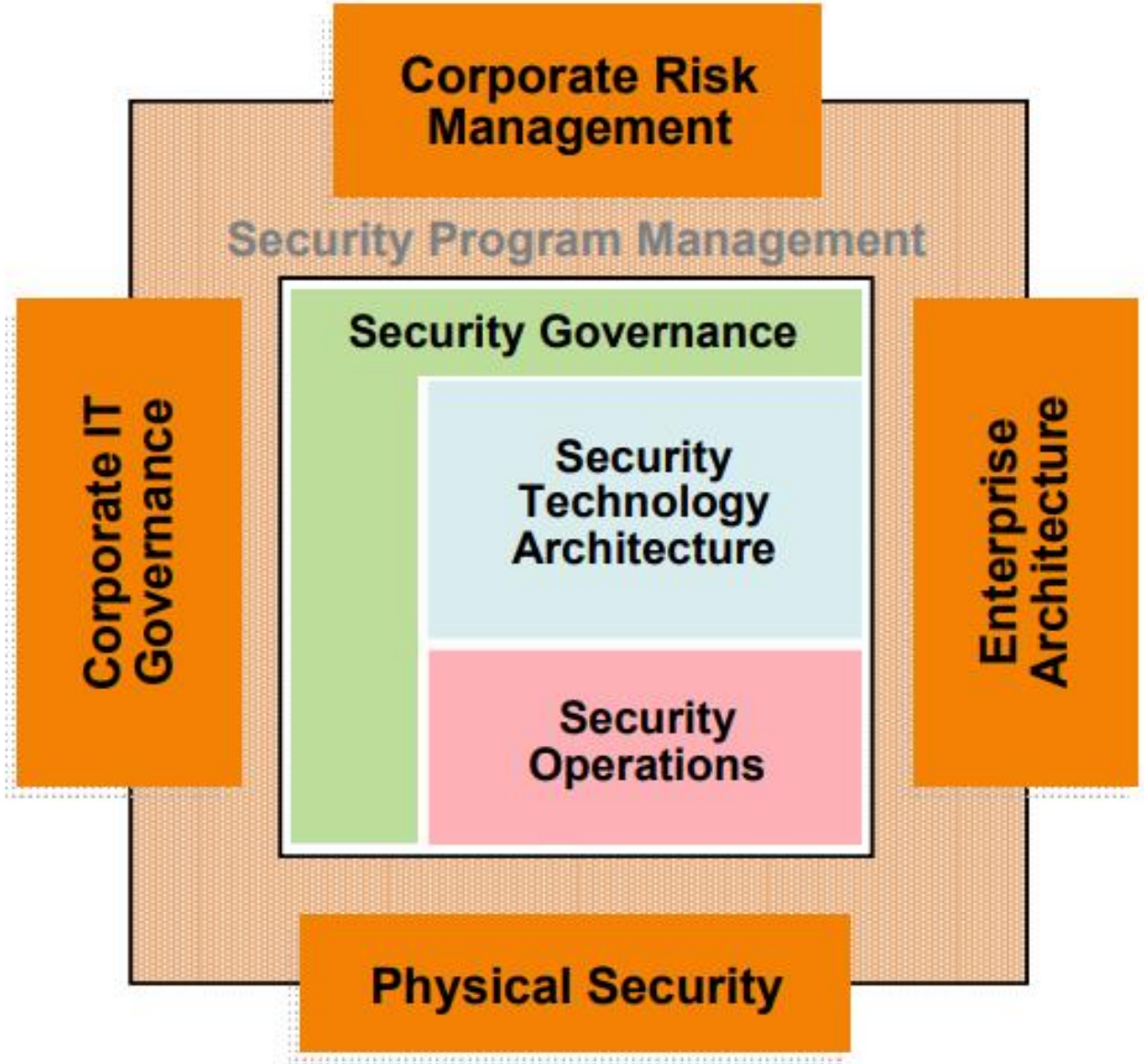
- Enterprise information security architecture (EISA) is the practice of applying a comprehensive and rigorous method for describing a current and/or future structure and behaviour for an organization's security processes, information security systems, personnel, and organizational sub-units so that they align with the organization's core goals and strategic direction.
- The primary purpose of creating an enterprise information security architecture is to ensure that **business strategy and IT security** are aligned.

Enterprise Information Security Architecture

Security of enterprise is done in a generic manner by applying three ways

- **Prevention** – This involves preventing the networks from intruders by avoiding security Breaches. This is normally done by the implementation of firewalls.
- **Detection** – This process focuses on the detection of the attacks and the breaches that are done over the network.
- **Recovery** – Once an attack occurs, recovery is essential for preventing the information asset of the enterprise that may damage due to the attack. For this, some recovery mechanisms are being employed by the enterprises. Till date, most of the researches and works have been done in the area of prevention and detection of the attack.

Enterprise Information Security Architecture



Vulnerability Assessment and Penetration Testing

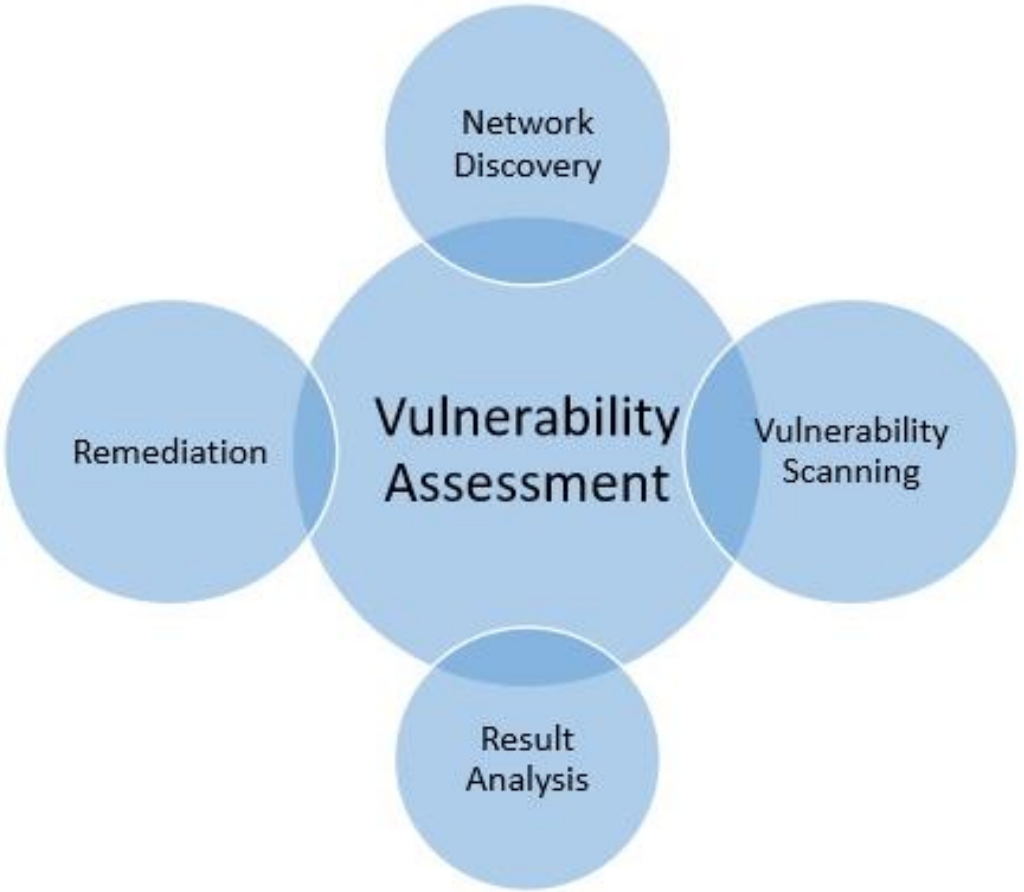
Vulnerability Assessment

- Vulnerability assessment is the technique of identifying (discovery) and measuring security vulnerabilities (scanning) in a given environment. It is a comprehensive assessment of the information security position (result analysis). Further, it identifies the potential weaknesses and provides the proper mitigation measures (remediation) to either remove those weaknesses or reduce below the risk level.

Vulnerability Assessment and Penetration Testing

Vulnerability Assessment

The following diagram summarizes the vulnerability assessment –



Vulnerability Assessment and Penetration Testing

Penetration Testing

- Penetration testing replicates the actions of an external or/and internal cyber attacker/s that is intended to break the information security and hack the valuable data or disrupt the normal functioning of the organization. So, with the help of advanced tools and techniques, a penetration tester (also known as ethical hacker) makes an effort to control critical systems and acquire access to sensitive data.

Vulnerability Assessment and Penetration Testing

Penetration Testing	Vulnerability Assessments
Determines the scope of an attack.	Makes a directory of assets and resources in a given system.
Tests sensitive data collection.	Discovers the potential threats to each resource.
Gathers targeted information and/or inspect the system.	Allocates quantifiable value and significance to the available resources.
Cleans up the system and gives final report.	Attempts to mitigate or eliminate the potential vulnerabilities of valuable resources.
It is non-intrusive, documentation and environmental review and analysis.	Comprehensive analysis and through review of the target system and its environment.
It is ideal for physical environments and network architecture.	It is ideal for lab environments.
It is meant for critical real-time systems.	It is meant for non-critical systems.

Vulnerability Assessment and Penetration Testing

- Vulnerability assessment identifies the weaknesses and gives solution to fix them. On the other hand, penetration testing only answers the question that "can anyone break-in the system security and if so, then what harm he can do?“

- A vulnerability assessment attempts to improve security system and develops a more mature, integrated security program. On the other hand, a penetration testing only gives a picture of your security program’s effectiveness.

- the vulnerability assessment is more beneficial and gives better result in comparison to penetration testing. But, experts suggest that, as a part of security management system, both techniques should be performed routinely to ensure a perfect secured environment.

Vulnerability Assessment and Penetration Testing

Vulnerability Scanning Tools

Category	Tool	Description
Host Based	STAT	Scan the network for numerous systems.
	TARA	Research Assistant for Tiger Analytical.
	Cain & Abel	By sniffing the network and cracking HTTP passwords, you may recover your password.
	Metasploit	Open-source code development, testing, and exploitation platform.
Network-Based	Cisco Secure Scanner	Security Issues Diagnosis and Repair
	Wireshark	For Linux and Windows, an open-source network protocol analyzer.
	Nmap	Security auditing tool that is open-source and free.
	Nessus	Auditing without agents, reporting, and patch management integration
Database-Based	SQL diet	SQL server door with the Dictionary Attack tool.
	Secure Auditor	Enable enumeration, scanning, auditing, penetration testing, and forensics on the operating system.
	DB-scan	Database Trojan detection, including hidden Trojan detection via baseline scanning.

Social Engineering

- Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

- A perpetrator first investigates the intended victim to **gather necessary background information, such as potential points of entry and weak security protocols**, needed to proceed with the attack. Then, the attacker moves to **gain the victim's trust and provide stimuli for subsequent actions that break security practices**, such as **revealing sensitive information or granting access to critical resources.**

Social Engineering

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction, ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

Social Engineering Types

1. Phishing Attacks

Phishing attackers pretend to be a trusted institution or individual in an attempt to encourage you to expose personal data and other valuables.

Attacks using phishing are targeted in one of two ways:

- **Spam phishing,** or mass phishing, is a widespread attack aimed at many users. These attacks are non-personalized and try to catch any unsuspecting person.
- **Spear phishing** and by extension, **whaling** , use personalized info to target particular users. Whaling attacks specifically aim at high-value targets like celebrities, upper management, and high government officials.

Social Engineering Types

2. Baiting Attacks

- **Baiting** abuses your natural curiosity to coax you into exposing yourself to an attacker. Typically, potential for something free or exclusive is the manipulation used to exploit you. The attack usually involves infecting you with malware.

Popular methods of baiting can include:

- USB drives left in public spaces, like libraries and parking lots.
- Email attachments including details on a free offer, or fraudulent free software.

3. Physical Breach Attacks

Physical breaches involve attackers appearing in-person, posing as someone legitimate to gain access to otherwise unauthorized areas or information.

Social Engineering Types

4. Scareware

- Scareware involves victims being bombarded with false alarms and made-up threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.

5. **Pretexting**

- Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.

- The attacker usually starts by establishing trust with their victim by copying co-workers, police, bank and tax officials, or other persons who have right-to-know authority.

Scanning and enumeration

What is Scanning?

- Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network. Network scanning is used to create a profile of the target organization.
- Scanning refers to collecting more information using complex and aggressive reconnaissance techniques.

Network Scanning:

- **Port Scanning** – detecting open ports and services running on the target.
- **Network Scanning** – IP addresses, Operating system details, Topology details, trusted routers information etc
- **Vulnerability scanning** – scanning for known vulnerabilities or weakness in a system

Scanning and enumeration

Enumeration and its Types

- Enumeration is defined as the process of extracting user names, machine names, network resources, shares and services from a system. In this phase, the attacker creates an active connection to the system and performs directed queries to gain more information about the target. The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase.

Scanning and enumeration

Techniques for Enumeration

- Extracting user names using email ID's
- Extract information using the default password
- Brute Force Active Directory
- Extract user names using SNMP
- Extract user groups from Windows
- Extract information using DNS Zone transfer

Scanning and enumeration

Services and Port to Enumerate

- TCP 53: DNS Zone transfer
- TCP 135: Microsoft RPC Endpoint Mapper
- TCP 137: NetBIOS Name Service
- TCP 139: NetBIOS session Service (SMB over NetBIOS)
- UDP 161: SNMP
- TCP/UDP 3368: Global Catalog Service
- TCP 25: Simple Mail Transfer Protocol (SMTP)

Insider Attack

An insider threat is a security risk that originates from within the targeted organization. It typically involves a current or former employee or business associate who has access to sensitive information or privileged accounts within the network of an organization, and who misuses this access.

Traditional security measures tend to focus on external threats and are not always capable of identifying an internal threat originating from inside the organization.

Insider Attack

Types of insider threats include:

- **Malicious insider—**also known as a Turncloak, someone who maliciously and intentionally abuses legitimate credentials, typically to steal information for financial or personal incentives. For example, an individual who holds a grudge against a former employer, or an opportunistic employee who sells secret information to a competitor. Turncloaks have an advantage over other attackers because they are familiar with the security policies and procedures of an organization, as well as its vulnerabilities.

Insider Attack

Types of insider threats include:

- **Careless insider**—an innocent person who unknowingly exposes the system to outside threats. This is the most common type of insider threat, resulting from mistakes, such as leaving a device exposed or falling victim to a scam. For example, an employee who intends no harm may click on an insecure link, infecting the system with malware.
- **A mole**—an imposter who is technically an outsider but has managed to gain insider access to a privileged network. This is someone from outside the organization who poses as an employee or partner.

Preventing Insider Threats

- **Protect critical assets—**these can be physical or logical, including systems, technology, facilities, and people. Intellectual property, including customer data for vendors, proprietary software, schematics, and internal manufacturing processes, are also critical assets.
- **Enforce policies**—clearly document organizational policies so you can enforce them and prevent misunderstandings. Everyone in the organization should be familiar with security procedures and should understand their rights in relation to intellectual property (IP) so they don't share privileged content that they have created.
- **Increase visibility**—deploy solutions to keep track of employee actions and correlate information from multiple data sources. For example, you can use deception technology to lure a malicious insider or imposter and gain visibility into their actions.

Preventing Insider Threats

- **Increase Visibility**

In a 2019 SANS survey on advanced threats, more than a third of respondents admitted to lacking visibility over insider misuse. Therefore, it's important to deploy tools that continuously monitor user activity as well as aggregate and correlate activity information from multiple sources.

- **Promote Culture Changes**

Ensuring security is not only about know-how but also about attitudes and beliefs. To combat negligence and address the drivers of malicious behavior, you should educate your employees regarding security issues and work to improve employee satisfaction.

Preventing Insider Threats

Other ways to prevent

- #1 Security Policy
- #2 Physical Security
- #3 Screen New Hires
- #4 Use Multifactor Authentication
- #5 Secure Desktops
- #6 Segment LANs
- #7 Seal Information Leaks
- #8 Investigate Unusual Activities
- #9 Implement Perimeter Tools & Strategies
- #10 Monitor Misuse

Social Engineering Targets and Defence Strategies

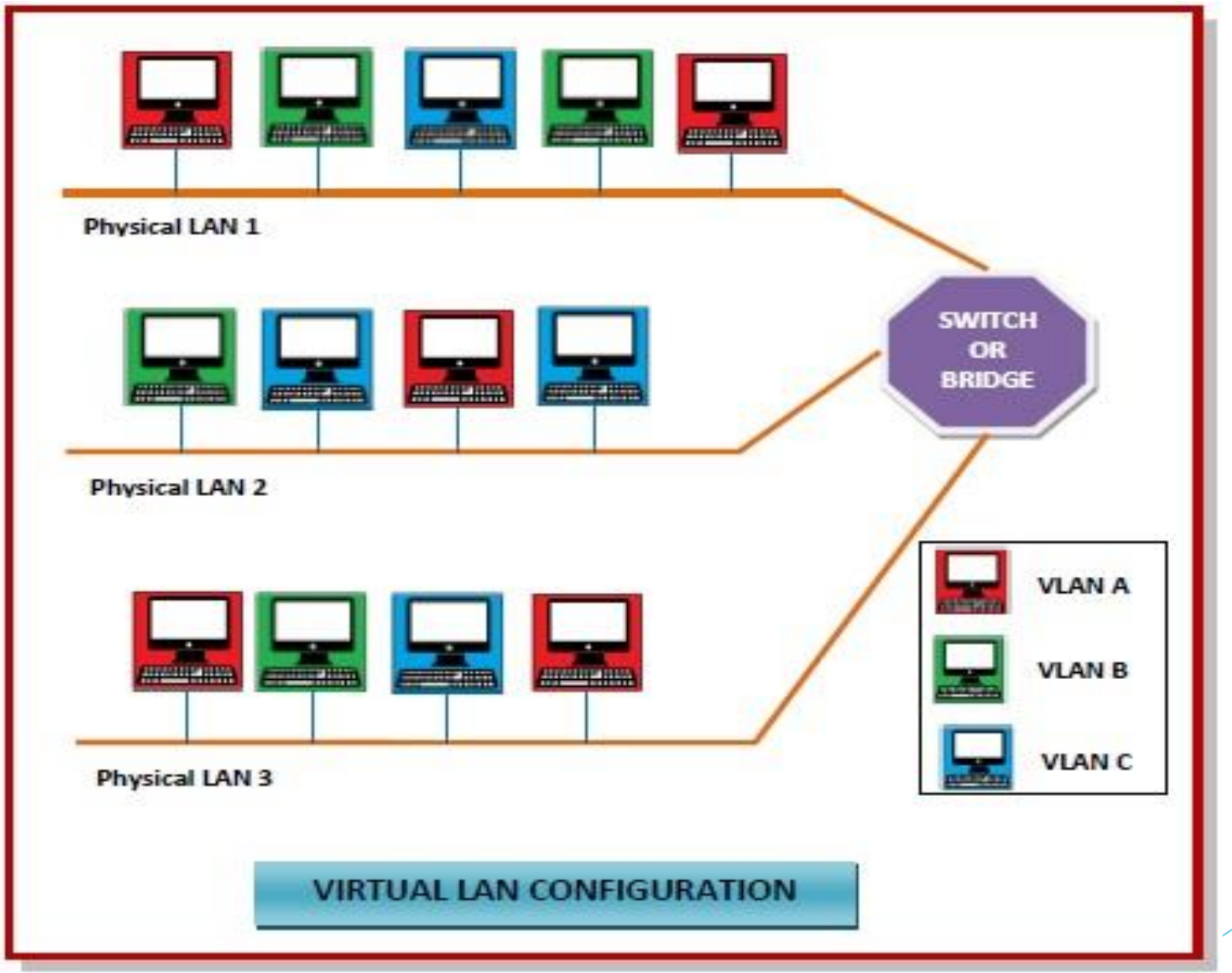
- Don’t open emails and attachments from suspicious sources
- Use multifactor authentication
- Be cautious of tempting offers
- Keep your antivirus/antimalware software updated
- Lock your laptop
- Read your company’s privacy policy
- Build a positive security culture
- Train your staff to learn the psychological triggers and other giveaways
- Test the effectiveness of the training
- Implement technological cyber security measures

Virtual LAN

Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network.

Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprise of a subset of ports on a single or multiple switches or bridges. This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.

Virtual LAN


Physical LAN 1
Physical LAN 2
Physical LAN 3
SWITCH OR BRIDGE
VLAN A
VLAN B
VLAN C
VIRTUAL LAN CONFIGURATION

Virtual LAN

Features of VLANs

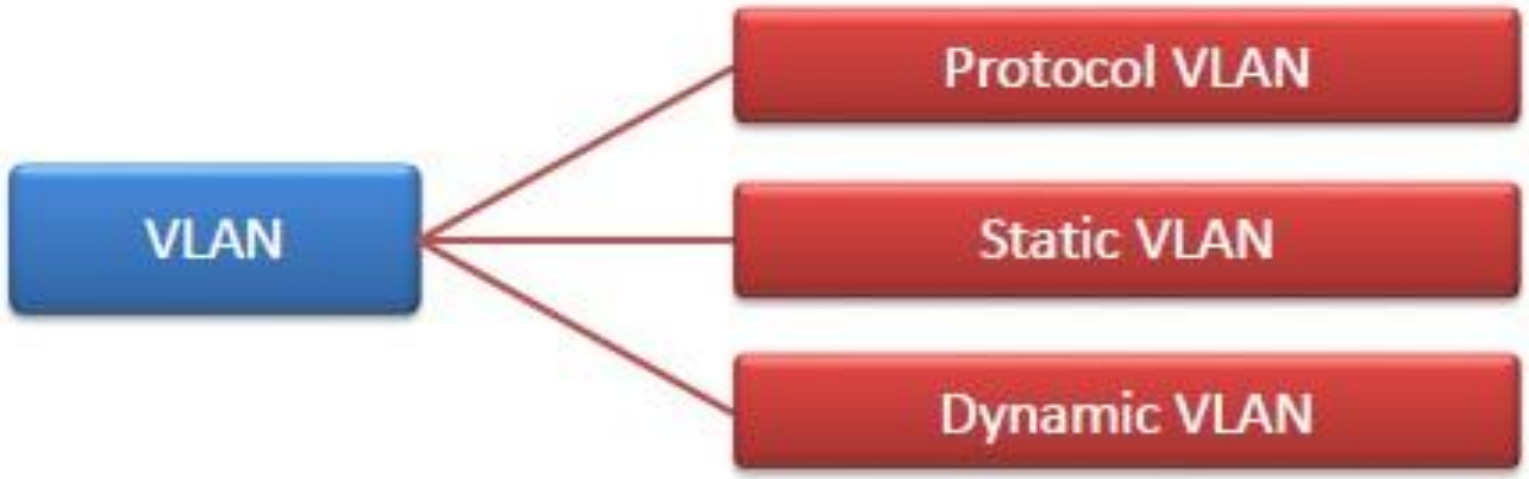
- A VLAN forms sub-network grouping together devices on separate physical LANs.
- VLAN's help the network manager to segment LANs logically into different broadcast domains.
- VLANs function at layer 2, i.e. Data Link Layer of the OSI model.
- There may be one or more network bridges or switches to form multiple, independent VLANs.
- Using VLANs, network administrators can easily partition a single switched network into multiple networks depending upon the functional and security requirements of their systems.
- VLANs eliminate the requirement to run new cables or reconfiguring physical connections in the present network infrastructure.

Virtual LAN

Features of VLANs

- VLANs help large organizations to re-partition devices aiming improved traffic management.
- VLANs also provide better security management allowing partitioning of devices according to their security criteria and also by ensuring a higher degree of control connected devices.
- VLANs are more flexible than physical LANs since they are formed by logical connections. This aids is quicker and cheaper reconfiguration of devices when the logical partitioning needs to be changed.

Types of VLANs



Protocol VLAN – Here, the traffic is handled based on the protocol used. A switch or bridge segregates, forwards or discards frames the come to it based upon the traffics protocol.

Port-based VLAN – This is also called static VLAN. Here, the network administrator assigns the ports on the switch / bridge to form a virtual network.

Dynamic VLAN – Here, the network administrator simply defines network membership according to device characteristics.

Thank you!