Soham Khochare
9615
TE Comps B

FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING

Cybersecurity Assignment-1

1) The TCP/IP protocol stack consists of several layers which have their responsibilities. They are as follows

i] Application layer :- This layer is where user application interact with the network
- protocol like http, ftp, smtp & dns operate here
- Way for application to communicate over the network

ii] Transport layer :- Manages end-to-end communication
- Controls data flow
- Ensures reliable, ordered and error checked delivery of data

iii] Internet Layer :- Also known as network layer, this layer handles the addressing and routing of data packets across interconnected networks.

iv] Link layer :- This layer deals with the physical connection between devices on the same network

2] IP addrssing and routing are crucial processes in computer networking that enables data to travel from a source to destination across interconnected networks

- IP addressing : In this unique numerical label is assigned to devices on network
- Routing : Determining best path for data packets to travel from source to destination
  - When a packet is sent from source and device it contains source and destination IP addresses
  - When a packet travels through routers, each router examines destination IP address and forwards it
  - This continues until packet reaches the destination network
  - Routing protocols help in efficient transmission in several ways like Dynamic Adaptation, Load Balancing, Redundancy & Reliability, Scalibility and fast convergence

3] Steps of Ethical hacking are as follows

1]. Reconnaissance : In this initial phase, ethical hacker gathers as much information as possible about the target system. This includes identifying IP. addresses, domain names network topology, potential entry points and other publicly available information

2] Scanning : In this step ethical hackers use various tools and techniques to scan the target system for open ports, services and vulnerabilities

3] Enumeration : During this phase the ethical hackers further probes the target system to obtain detailed information about users, shares and services

4] Vulnerability Assessment : In this step the ethical hacker analyses the information collected during scanning and enumeration to identify potential vulnerabilities & weakness in the target system

5] Gaining Access : Once potential vulnerabilities are identified, ethical hackers attempt to exploit them to gain unauthorized access to the target system.

6] Maintaining Access : After gaining intial access ethical hackers work to maintaining a foothold in the target system

7] Covering Tracks : In the ethical hacking process, the goal is to leave no traces behind to avoid detection by the target organization

8] Reporting : After completing the assesment ethical hackers compile a comprehensive report detailing their findings, including identified vulnerabilities, potential risks and recommended remediation steps

9] Post-Mortem Analysis: This step involves conducting a debriefing session with the organization to discuss the result of the ethical hacking engagement

4]

OSI Model	TCP/IP Model
i] Consists of seven layers providing a detailed breakdown of network functionality	i] Comprises four layers offering a more streamlined approach to network communication
ii] Has 3 distinct layers that correspondence to TCP/IP Application layers	ii] Combine functionalities of these 3 OSI layers into its application layer
iii] Developed by the ISO as a universal reference mode with a more theoretical approach	iii] Originated from the architecture of ARPANET and is the foundation of the internet's structure
iv] Less commonly used a practical framework for networking, mainly used for conceptual teaching	iv] Widely used in network implementation and closely align with how the internet function

5 Information gathering and reconnaissance also known as the initial phase of a cyber attacks, involve the collection of data about a target network or system to identify vulnerabilities and potential entry points

- This phase aids attackers in crafting a well-informed strategy for subsequent attacks

The process typically entails

1. Passive Data Collection : Attackers gather publicly available information such as domain names, IP and organization details

2. Network Mapping : Attackers identify active devices, open ports and services using tools Nmap, aiding in understanding the network's layout and potential weakness

3. DNS Enumeration : Attackers extract domain related information through DNS queries, revealing potential subdomains and mail server details

4. WHOIS Lookup : Attackers use WHOIS database to aquire ownership and contact information for domains, which might help in social engineering attacks

6] Vulnerability Assessment and Penetration testing are key elements in cybersecurity

- Vulnerability Assessment

- The purpose of this process is to identify vulnerabilities and weakness in system networks or applications.

- It provides a report highlighting the severities

- This process is conducted regularly to maintain security readiness

- Eg. of Tools : Nessus, OpenVAS, Qualys, Nexpose

PENETRATION TESTING

- This process simulates real-world attacks to evaluate system resistance
- It exploits vulnerabilities to assess impact and extent of compromise
- It produces a detailed report with exploited vulnerability and outcomes
- This process is conducted peridically or after significant changes
- Eg of tools: Metasploit, Nmap, Bumpsuite.

- In a vulnerability assesment, outdated software on a web server might be found, while in penetration testing, the tester would exploit it to showcase potential consequences highlighting the differing scope of these practices
- Both processes are crucial for robust security

7] Social Engineering attacks are manipulative tactics used by malicious actors to deceive individuals into divulging confidential information on granting access.

- Key characteristics include exploiting human psychology, leveraging trust and relying on manipulation rather than technical exploits.

- To prevent such attacks organization can implement effective employee education strategies.

1. Awareness Program: Regularly conduct training session to raise awareness about common social engineering tactics such as phishing and pretexting

2. Simulated Attacks. Run mock social engineering campaigns to expose employees to real life scenarios without actual risks, helping them recognize suspicious behaviours

3. Phishing Training: Teach employees to Identify phishing emails by scrutinizing sender details, URLs and attachments

4. Multi-Factor Authentication : Promote the use of MFA for accessing sensitive systems, reducing the effectiveness of stolen credentials.

5. Clear Policies : Develop and communicate clear security policies, emphasizing the importance of not sharing sensitive information

8] • Viruses are malicious program that ~~attacks~~ attach themselves to legitimate files on software

• They spread when infected files are executed

• Worms are self-replicating malware that spread over networks, exploiting vulnerabilities to infect other systems

• Unlike viruses, they don't need a host file to propogate

• Trojans are disguised as legitimate software but contain malicious code

• Trojans often rely on social engineering to trick users into installing them

• These impact network security in the following way

1. Data can be breached as malware can steal sensitive data which can lead to privacy violation

2. Malware can distrupt network services and operations, causing downtime and loss

3. Worms can rapidly spread across network overwhelming systems and clogging network traffic

4. Malware can lead to financial theft, fraud, etc impacting both individual & organizations

5. Some malware can corrupt/delete data causing permanent loss and impacting productivity