UNIT - 1

Date ____/____/____
Page ____

① **Introduction to Network Security, Computer Security and Cyber Security -**

Network Security is protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system. Eg - Antivirus System.

Computer Security measures and controls that ensure confidentiality, integrity and availability of information system assets including hardware, software, firmware, and information being processed, stored and communicated.

Cybersecurity is the body of technologies, process and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term security implies cybersecurity.

② **Security Principles -**

(1) Confidentiality - This term covers two related concepts -

(i) Data confidentiality assures that private or confidential information is not made available or disclosed to unauthorized individuals.

(ii) Privacy assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

(2) Integrity - This term covers two related concepts -

(i) Data Integrity assures that information and programs are changed only in a specified and authorized manner.

(ii) System Integrity assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

(3) Availability assures that systems work promptly and service is not denied to authorized users.

③ **Security terminology -**

(1) Vulnerability - A defect or weakness in the feasibility, design, implementation, operation or maintenance of a system.

(2) Threat - An adversary who is capable and motivated to exploit a vulnerability.

(3) Attack - The use or exploitation of a vulnerability. This term is neither malicious nor benevolent. A bad guy may attack a system, and a good guy may attack a problem.

(4) Attacker - The person or process that initiates an attack. This can be synonymous with threat

(5) Exploit - The instantiation of a vulnerability, something that can be used for an attack. A single vulnerability may lead to multiple exploits, but not every vulnerability may have an exploit (Eg - Theoretical vulnerabilities)

(6) Target - The person, company, or system that is directly vulnerable and impacted by the ~~exploit~~ exploit. Some exploits may have multiple impacts, with both primary (main) targets and secondary (incidental) targets.

(7) Attack Vector - The path from an attacker to a target. This includes tools & techniques

(8) Defender - The person or process that mitigates or prevents an attack.

(9) Compromise - The successful exploitation of a target by an attacker.

(10) Risk - A qualitative assessment describing the likelihood of an attacker / threat using an exploit to successfully bypass a defender, attack a vulnerability, and compromise a system.

(1) Security Threats -

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Sources of security threats are -

(1) Open architecture, work in progress design philosophy.
(2) Weaknesses in Network Infrastructure and Communication Protocols
(3) Rapid growth of Cyberspace
(4) The Growth of the Hacker Community
(5) Vulnerability in Operating System Protocol
(6) The Invisible Security Threat - The Insider Effect
(7) Social Engineering
(8) Physical Theft

⑤ Type of attacks -

(1) Active attacks - It attempts to alter system resources or affect their operations. Four types -

(i) Masquerade - takes place when one entity pretends to be a different entity

(ii) Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

(iii) Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

(iv) Denial of service prevents or inhibits the normal use or management of communication facilities.

(2) Passive attacks - attempts to learn or make use of information from the system but does not affect system resources. Two types -

(i) Release of message contents → Read contents of messages

(ii) Traffic analysis → Observe pattern of messages.

⑥ Types of Hacker attacks -

(1) Operating system attacks - Today's operating systems contain many features, making them increasingly complex. These features use additional processes and services, which means more vulnerabilities for hackers to exploit.

(2) Application level attacks - Newer software applications that come with a multitude of features and functionalities, making them increasingly complex that leads to more vulnerabilities for hackers to exploit. Eg - Buffer overflow attacks.

(3) Shrink-Wrap code attacks - Software developers will often use free libraries and code licensed from other sources in their programs. If vulnerabilities in that code are discovered, many pieces of software are at risk.

(4) Misconfiguration attacks - Even systems that are otherwise very secure can be hacked if they are not configured correctly.

(7) Introduction to Intrusion -

An intrusion is a deliberate unauthorized attempt, successful or not, to break into, access, manipulate, or misuse some valuable property and where the misuse may result into or render the property unreliable or unusable. The person who intrudes is an intruder. Six types of intrusion are -

(1) Attempted break-ins
(2) Masquerade attacks
(3) Penetrations of the security control system
(4) Leakage
(5) Denial of service
(6) Malicious use

(8) Terminologies -

(1) Firewall - It is a program or hardware device that protects the resources of a private network from users of other networks.

(2) Honeypot - It is a device intended to be compromised. The goal of a honeypot is to have the system probed, attacked, and potentially exploited.

(3) Burglar Alarm - A signal suggesting that a system has been or is being attacked

(4) Detection Rate - It is defined as the number of intrusion instances detected by the system divided by the total no. of intrusion instances present in the test set.

(5) False Alarm Rate - defined as the no. of 'normal' patterns classified as attacks divided by the total no. of 'normal' patterns.

(9) Intrusion Detection System (~~IDS~~) - (IDS) -

It can be defined as the the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion Detection System is typically one part of an overall protection system that is installed as a system or device. Three ways to detect an intrusion -

(1) Signature Recognition (Misuse Detection) - It tries to identify events that misuse a system.

(2) Anomaly Detection - It detects Any behaviours that fall outside the predefined or accepted model of behaviour.

(3) Protocol Anomaly Detection - Modules are built on TCP/IP protocols using the specifications to check for the expected behaviour.

(10) Types of Intrusion Detection Systems -

(1) Network-based Intrusion Detection - These mechanisms typically consist of a black box that is placed on the network in promiscuous promiscuous mode, listening for patterns indicative of a intrusion.

(2) Host-based Intrusion Detection - These mechanisms usually include auditing for events that occur on a specific host. These are not as common, due to the overhead they incur by having to monitor each system event.

(3) Hybrid IDS - Combination of Network-based Intrusion Detection and Host-based Intrusion Detection.

(4) Log file monitoring - These mechanisms are typically programs that parse log files after an event has already occurred, such as failed log in attempts

(5) File Integrity Checking - These mechanisms check for Trojan horses, or files that have otherwise been modified, indicating an intruder has already been there. Eg - Tripwire.

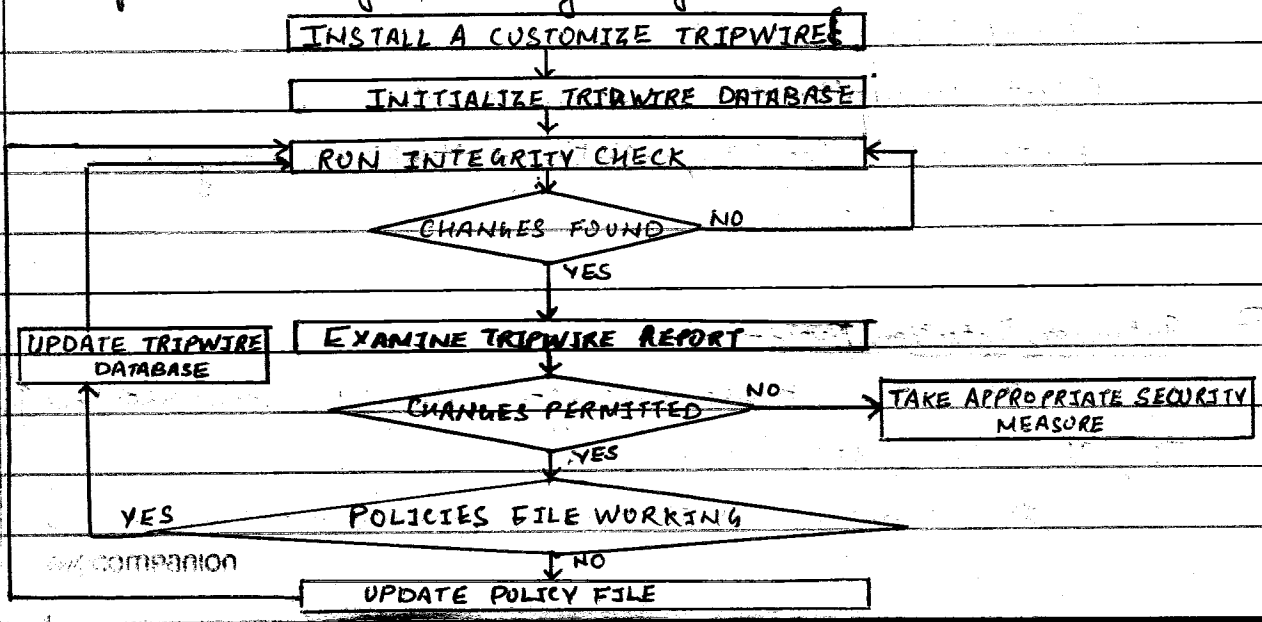
Same

(11) System Integrity Verifiers (SIVS) -

It is a type of Intrusion Detection Systems that monitors system files and detects changes by an Intruder. SIVs may watch other components, such as the Windows registry, as well as chron configuration, to find known signatures.

Tripwire is one of the popular SIVs

Tripwire - It is an SIV monitor. It works with a database that maintains information about the byte count of files. If the byte count has changed, it will be identified with the system security manager.



(12) Indication of Intrusion -

(1) System Indications -

(i) Modification to system software and configuration files.
(ii) Gaps in the system accounting.
(iii) Unusually slow system performance.
(iv) System crashes or reboots
(v) Short or incomplete logs
(vi) logs containing strange timestamps.
(vii) logs with incorrect permissions or ownership
(viii) Missing logs
(ix) Abnormal system performance
(x) Unfamiliar processes
(xi) Unusual Graphic displays or text messages

(2) File System Indications -

(i) The presence of new, unfamiliar files, or programs.
(ii) Changes in file permissions
(iii) Unexplained changes in file size
(iv) Rogue files on the system that do not correspond to your master list of signed files.
(v) Unfamiliar file names in directories
(vi) Missing files.

(3) Network Indications -

(i) Repeated probes of the available services on your machines
(ii) Connection from unusual locations
(iii) Repeated log in attempts from the remote host
(iv) Arbitrary data in log files, indicating an attempt at creating either a Denial of Service, or a Crash service.

(13) Intrusion Detection Tools -

It works best when used after vulnerability scans have been performed. They then stand watch.

All network-based ID tools can provide scan probes in addition to

Date ___/___/___
Page ___

port and host scans. As monitoring tools, they give information on -

(i) Hundred of thousands of network connections.

(ii) External break in attempts

(iii) Internal scans.

(iv) Misuse pattern of confidential data

(v) Unencrypted remote logins or a web session.

(vi) unusual or potentially troublesome observed network traffic.

All this information is gathered by these tools monitoring network components and services that include - Servers for Mail, FTP and Web activities, DNS, RADIUS, TCP/IP Ports, Routers, Bridges, Drive Space, Event log entries, file modes & existence and file contents.

Current ID tools are -

NAME	SOURCE
Snort 2.x	www.snort.org
BlackICE Defender	NetworkICE
Check Point RealSecure	Check Point Software Technologies
Cisco Secure IDS	Cisco Systems
Dragon Sensor	Network Security Wizards
eTrust Intrusion Defense	Computer Associates
HP Openview Node Sentry	Hewlett - Packard
Iucent RealSecure	Iucent Technologies
Network Flight Recorder	Network Flight Recorder
RealSecure	ISS (Internet Security System)
Silent Runner	Silent Runner
Vanguard Enforcer	Vanguard Integrity Professionals

(14) Post Attack IDS measures - Steps are -

(1) Configure a firewall to filter out the IP address of the intruder

(2) Alert the user/administrator (sound/email/page)

(3) Write an entry in the event log. Send an SNMP Trap msg datagram to a management console like Tivoli.

(4) Save a trace file of the raw packets for later analysis
(5) Launch a separate program to handle the event.
(6) Terminate the TCP session - Forge a TCP FIN (finish) or RST (Reset) packet to forcibly terminate the connection.

(15) Evading IDS Systems -

Many simple network intrusion detection systems rely on "pattern matching" Attack scripts have well-known patterns, so compiling a database of the output of known attack scripts provides good detection, but can be easily evaded by simply changing the script.

IDS evasion focuses on the fooling signature matching by altering on the attacker's appearance.

Eg - Some POP3 servers are vulnerable to a buffer overflow when a long password is entered.

→ Ways to Evade IDS are Insertion, Evasion, Denial-of-Service, Complex attacks, Obfuscation, Desynchronization - Post Connection SYN, Desynchronization - Pre Connection SYN, Fragmentation and Session Splicing.

→ Tools to evade IDS are SideStep, ADMutate, Mtudam v 0.7.1, Stick, Fragroute and Anzen NIDSbench.

(16) Penetration Testing -

In the context of penetration testing, the tester is limited by resources - Example time, skilled resources and access to equipment - as outlined in the penetration Testing agreement.

A pentest (Penetration Testing) simulates methods that intruders use to gain unauthorized access to an organization's networked systems and then compromise them

(17) Categories of Security Assessment -

Every organization uses different types of security assessments to validate the level of security on its network resources.

Security assessments categories are security audits, vulnerability assessment

and penetration testing.

Each type of security assessment requires that the people conducting the assessment have different skills.

(18) **Vulnerability Assessment -**

It scans a network for known security weaknesses. Vulnerability scanning tools search network segments for IP-enabled devices and enumerate systems, operating systems, and applications.

Vulnerability scanners can test systems and network devices for exposure to common attacks and it also can identify common security configuration mistakes.

Limitations -

(1) Vulnerability scanning software must be updated when new vulnerabilities are discovered or improvements are made to the software being used.

(2) The methodology used as well as the diverse vulnerability scanning software packages assess security differently. This can influence the result of the assessment.

(19) **Types of Penetration Testing -**

(1) External Testing - It involves analysis of publicly available information, a network enumeration phase, and the behaviour of security devices analyzed.

(2) Internal Testing - It will performed from a number of network access points, representing each logical and physical segment. Three types -

(i) Black-hat testing - Zero Knowledge Testing

(ii) Gray-hat testing - Partial knowledge Testing

(iii) White-hat testing - Complete knowledge Testing.

(20) **Risk Management -**

An unannounced test is usually associated with higher risk and a greater potential of encountering unexpected problems.

Risk = Threat X Vulnerability

A planned risk is any event that has the potential to adversely affect the penetration test.

The pentest team is advised to plan for significant risks to enable contingency plans in order to effectively utilize time and resources.

Metrics for Risk Management -

For developing effective metrics for risk management, activities are -

(1) Determination of the organization's risk tolerance
(2) Comprehensive resource valuation.
(3) Complete Risk assessment
(4) Business impact assessment of important systems
(5) Tests of control effectiveness and reliability
(6) Known level of metric accuracy.