USN | | | | | | | | | | |

Internal Assessment Test 3 – May 2024

Sub:	Network Security					Sub Code:	18EC821	Branch:	ECE	
Date:	11-05-2024	Duration:	90 min's	Max Marks:	50	Sem / Sec:	8 – A, B, C, D		OBE	

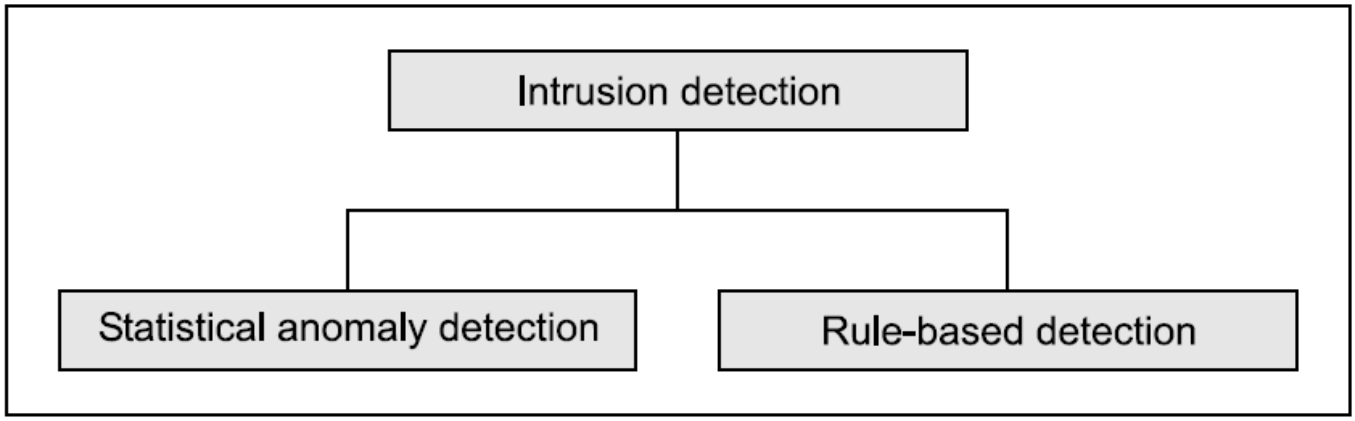
	Answer any FIVE FULL Questions	MARKS	CO	RBT
1.	Explain three classes of intruders with examples, discuss intruder patterns of behavior.	[10]	CO4	L2
2.	With neat diagram, illustrate the profiles of intruder and authorized users. Also discuss approaches to intrusion detection.	[10]	CO4	L2
3.	Describe the overall taxonomy of software threats (Terminology of Malicious program).	[10]	CO4	L2
4.	Explain the anti-virus approaches and also in detail the generations of antivirus software.	[10]	CO4	L2
5.	Explain the different purposes for which internal firewall can be used.	[10]	CO5	L2
6.	Explain four general techniques that the firewall use to control access.	[10]	CO5	L2
7.	Discuss the characteristic of Bastion Host.	[10]	CO5	L3
8.	Discuss the capabilities which one within the scope of a firewall.	[10]	CO5	L3

Solution

Q1. Intruders are said to be of three types, as explained below:

(a) Masquerader A user who does not have the authority to use a computer, but penetrates into a system to access a legitimate user's account is called as a masquerader. It is generally an external user.
(b) Misfeasor There are two possible cases for an internal user to be called a misfeasor:
● A legitimate user, who does not have access to some applications, data or resources accesses them.
● A legitimate user, who has access to some applications, data or resources misuses these privileges.
(c) Clandestine User An internal or external user who tries to work using the privileges of a supervisor user to avoid auditing information being captured and recorded is called as a clandestine user.
How do intruders try to attack? A simple example may be considered, where the attackers try to obtain the passwords of legitimate users, so as to impersonate them. Some of the popularly known methods of password guessing are as follows:
1. Try all possible short password combinations (2-3 characters).
2. Collect information about users, such as their full name, names of family members, their hobbies, etc.
3. Try default passwords that are provided by the supplier of a software product (e.g. Oracle comes with scott as the user name and tiger as the password).
4. Try words that people choose as passwords most often. Hacker bulletin boards maintain these lists. Also, try words from dictionary.
5. Try using phone numbers, dates of birth, social security numbers, bank account numbers, etc.
6. Tap the communication line between a user and the host network.

Q2. Intrusion Detection
Intrusion prevention is almost impossible to achieve at all times. Hence, more focus is on intrusion detection.
Following factors motivate efforts on intrusion detection:
(a) The sooner we are able to detect an intrusion, the quicker we can act. The hope of recovering from attacks and losses is directly proportional to how quickly we are able to detect an intrusion.
(b) Intrusion detection can help collect more information about intrusions, strengthening the intrusion prevention methods.
(b) Intrusion detection systems can act as good deterrents to intruders.
Intrusion detection mechanisms, also known as Intrusion Detection Systems (IDS) are classified into two categories: Statistical anomaly detection and Rule-based detection.



(a) Statistical Anomaly Detection In this type, behavior of users over time is captured as statistical data and processed. Rules are applied to test whether the user behavior was legitimate or not.
This can be done in two ways:
(i) Threshold Detection In this type, thresholds are defined for all the users as a group and frequency of various events is measured against these thresholds.
(ii) Profile-based Detection In this type, profiles for individual users are created and they are matched against the collected statistics to see if any irregular patterns emerge.
(b) Rule-based Detection A set of rules is applied to see if a given behavior is suspicious enough to be classified as an attempt to intrude. This is also classified into two sub-types: (i) Anomaly Detection Usage patterns are collected to analyze deviation from these usage patterns,
with the help of certain rules.
(ii) Penetration Identification This is an expert system that looks for illegitimate behavior.
9.6.4 Distributed Intrusion Detection
Focus has started moving from intrusion detection on single systems to distributed systems, e.g. a LAN or a WAN. Following factors are important in this scheme of distributed intrusion detection:
● Different systems in the distributed system may record audit information in different formats. This needs to be uniformly processed.
● Typically one or a few nodes on the distributed system would be used to gather and analyze audit information. Hence, there should be provisions to securely send audit information from all other hosts to these hosts.
9.6.5 Honeypots
Modern intrusion detection systems make use of a novel idea, called as honeypots. A honeypot is a trap that attracts potential attackers. A honeypot is designed so as to do the following:
● Divert the attention of a potential intruder from critical systems
● Collect information about the intruder's actions
● Provide encouragement to the intruder so as to stay on for some time, allowing the administrators to detect this and swiftly act on it
Honeypots are designed with two important goals in mind:
(a) Make them look like real-life systems. Put as much of real-looking (but fabricated) information into them as possible.
(b) Do not allow legitimate users to know about or access them.
Naturally, anyone trying to access a honeypot is a potential intruder. Honeypots are armed with sensors and loggers, which alarm the administrators of any user actions.

Q3. Boot Sector Virus
A Personal Computer is infected with a boot sector virus if it is booted normally or by accidentally from an infected hard disk in hard disk drive. Boot sector virus could not usually spread across a network.
File Virus
When the infected file is opened or used the virus may overwrite the file and grounds everlasting smash up to the content of the overwritten file. These viruses target a large series of operating systems, like Macintosh, UNIX, DOS, and Windows. file virus could spread across a network
Multipartite virus
A multipartite virus infects both boot sectors and file sector. An infected file is often used to infect the boot sector; and could spread across a network. Macro Virus

Macro viruses are macros which call it-self again and again. If a user works on a document that contains a macro virus and unsuspectingly executes this macro virus, then, it can copy itself into that application's set up files. If the infected PC is on a network, the infection is very much possible to extend quickly to other computers on the network.
E-Mail Worm
Viruses attached to email messages can infect a complete project in affair of minutes; estimate companies millions of dollars annually in lost efficiency and clean-up cost.

Q4. One can launch an application-level attack or a network level attack using a virus. In simple terms, a virus is a piece of program code that attaches itself to legitimate program code, and runs when the legitimate program runs. It can then infect other programs in that computer, or programs that are in other computers but on the same network.
\

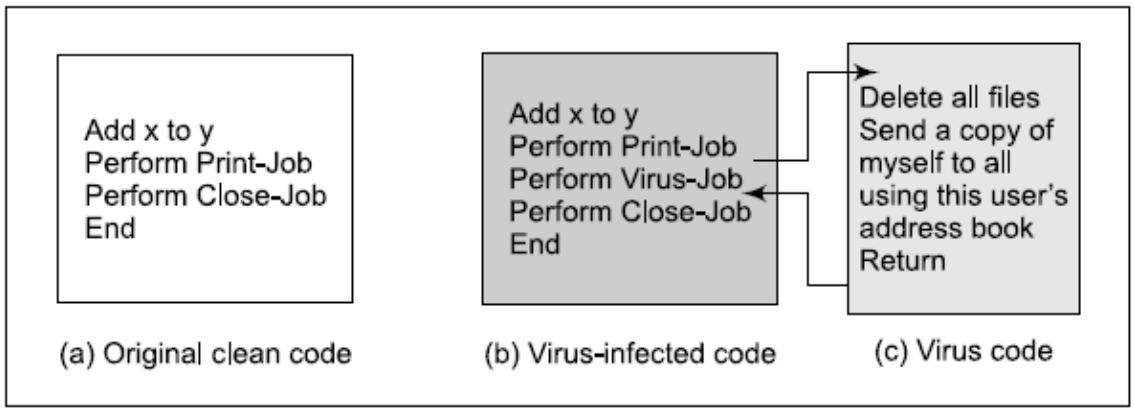


Fig. 1.14 Virus

Viruses can also be triggered by specific events (e.g. a virus could automatically execute at 12 p.m. every day). Usually viruses cause damage to computer and network systems to the extent that they can be repaired, assuming that the organization deploys good backup and recovery procedures.
A virus is a computer program that attaches itself to another legitimate program, and causes damage to the computer system or to the network.
During its lifetime, a virus goes through four phases:
(a) Dormant Phase Here, the virus is idle. It gets activated based on a certain action or event (e.g. the user typing a certain key or a certain date or time is reached, etc). This is an optional phase.
(b) Propagation Phase In this phase, a virus copies itself, and each copy starts creating more copies of itself, thus propagating the virus.
(c) Triggering Phase A dormant virus moves into this phase when the action/event for which it was waiting is initiated.
(d) Execution Phase This is the actual work of the virus, which could be harmless (display some message on the screen) or destructive (delete a file on the disk).
Viruses can be classified into the following categories:
(a) Parasitic Virus This is the most common form of virus. Such a virus attaches itself to executable files and keeps replicating. Whenever the infected file is executed, the virus looks for other executable files to attach itself and spread.
(b) Memory-resident Virus This type of virus first attaches itself to an area of the main memory and then infects every executable program that is executed.
(c) Boot sector Virus This type of virus infects the master boot record of the disk and spreads on the disk when the operating system starts booting the computer.
(d) Stealth Virus This virus has intelligence built in, which prevents anti-virus software programs from detecting it.
(e) Polymorphic Virus A virus that keeps changing its signature (i.e. identity) on every execution, making it very difficult to detect.
(f) Metamorphic Virus In addition to changing its signature like a polymorphic virus, this type of virus keeps rewriting itself every time, making its detection even harder.

Q5. A firewall acts like a sentry. If implemented, it guards a corporate network by standing between the network and the outside world. All traffic between the network and the Internet in either direction must pass through the firewall. The firewall decides if the traffic can be allowed to flow or whether it must be stopped from proceeding further. Packet Filters
As the name suggests, a packet filter applies a set of rules to each packet and based on the outcome, decides to either forward or discard the packet. It is also called as screening router or screening filter. Such a firewall implementation involves a router, which is configured to filter packets going in either direction (from the local network to the outside world and vice versa). The filtering rules are based on a number of fields in the IP and TCP/UDP headers, such as source and destination IP addresses, IP protocol field (which identifies if the protocol in the upper transport layer is TCP or UDP), TCP/UDP port numbers (which identify the application which is using this packet, such as email, file transfer or World Wide Web). A packet filter performs the following functions.
(a) Receive each packet as it arrives.
(b) Pass the packet through a set of rules, based on the contents of the IP and transport header fields of the packet. If there is a match with one of the set rules, decide whether to accept or discard the packet based on that rule. For example, a rule could specify: disallow all incoming traffic from an IP address 157.29.19.10 (this IP address is taken just as an example) or disallow all traffic that uses UDP as the higher (transport) layer protocol.
(c) If there is no match with any rule, take the default action. The default can be discard all packets or accept all packets. The former policy is more conservative, whereas the latter is more open. Usually, the implementation of a firewall begins with the default discard all packets option and then rules are applied one-by-one to enforce packet filtering.
Q6.
IP Address Spoofing An intruder outside the corporate network can attempt to send a packet towards the internal corporate network, with the source IP address set equal to one of the IP addresses of the internal users. Source Routing Attacks An attacker can specify the route that a packet should take as it moves along the Internet. The attacker hopes that by specifying this option, the packet filter can be fooled to bypass its normal checks. Discarding all packets that use this option can thwart such an attack. Tiny Fragment Attacks IP packets pass through a variety of physical networks, such as Ethernet, Token Ring, X.25, Frame Relay, ATM, etc. All these networks have a pre-defined maximum frame size (called as the Maximum Transmission Unit or MTU). Many times, the size of the IP packet is greater than this maximum size allowed by the underlying network. In such cases, the IP packet needs to be fragmented, so that it can be accommodated inside the physical frame and carried further. An attacker might attempt to use this characteristic of the TCP/IP protocol suite by intentionally creating fragments of the original IP packet and sending them. The attacker feels that the packet filter can be fooled, so that after fragmentation, it checks only the first fragment and does not check the remaining fragments.
Q7. A Bastion Host is a special-purpose computer on a network specifically designed and configured to withstand attacks. Here are the key characteristics of a Bastion Host:

1. Isolated Functionality:
- Single Function: Typically, a bastion host is set up to perform a specific, limited set of tasks, such as handling incoming requests from the internet to the internal network. This reduces its attack surface.
- Minimal Services: Only the essential services needed for its function are running, reducing potential vulnerabilities.

2. Hardened Security:
- Security Patches: Regularly updated with the latest security patches to protect against known vulnerabilities.
- Access Control: Strict access control measures are in place. Only authorized personnel have access to the system.
- Firewall Rules: Configured with strict firewall rules to limit the types of traffic that can interact with the host.

3. Monitoring and Logging:

- Activity Logging: Comprehensive logging of all activities, including user logins and system changes, is maintained to detect any unauthorized access attempts.
- Intrusion Detection: Often integrated with intrusion detection systems (IDS) to monitor for and alert on suspicious activities.

4. Strong Authentication:
- Multi-Factor Authentication (MFA): Often requires multi-factor authentication for access, providing an extra layer of security.
- Secure Access Methods: Utilizes secure access methods such as SSH for remote login, ensuring that communications are encrypted.

5. Network Segmentation:
- DMZ Placement: Usually placed in a demilitarized zone (DMZ) to act as a buffer between the external network and the internal network.
- Controlled Connectivity: Limited and controlled connectivity to the internal network, reducing the risk of an attack spreading.

6. Simplified Configuration:
- Minimal Software: Contains only the necessary software to perform its functions, minimizing potential vulnerabilities.
- Configured for Security: Configurations are optimized for security, with default settings often disabled or altered to reduce risk.

By incorporating these characteristics, a bastion host serves as a fortified gateway, protecting the internal network from external threats.

Q8. A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Within the scope of a firewall, the following capabilities are essential:

1. Packet Filtering:
- Basic Filtering: Inspects each packet passing through the firewall and accepts or rejects it based on user-defined rules.
- Stateless vs. Stateful Filtering: Stateless firewalls filter packets independently of the state of the connection, while stateful firewalls keep track of active connections and make filtering decisions based on the state of the connection.

2. Network Address Translation (NAT):
- IP Address Modification: Translates private internal IP addresses to a public IP address and vice versa, allowing multiple devices on a local network to share a single public IP address.
- Port Address Translation (PAT): Maps multiple private IP addresses to a single public IP address but with different port numbers, enhancing the security and efficiency of the network.

3. Virtual Private Network (VPN) Support:
- Secure Tunneling: Supports VPN functionalities to establish secure, encrypted connections over the internet, allowing remote users to securely access the internal network.
- VPN Termination: Acts as an endpoint for VPN connections, providing secure remote access to the network.

4. Application Layer Filtering:
- Deep Packet Inspection (DPI): Analyzes the content of packets up to the application layer, allowing for more granular control and detection of malicious payloads or applications.
- Content Filtering: Blocks or permits traffic based on specific content criteria, such as URLs, file types, or keywords.

5. Intrusion Detection and Prevention Systems (IDPS):

- Threat Detection: Monitors network traffic for suspicious activities and known attack patterns, generating alerts for potential threats.
- Threat Prevention: Automatically takes action to block or mitigate identified threats, enhancing the security posture of the network.

6. Logging and Monitoring:
- Traffic Logs: Maintains detailed logs of all network traffic, providing insights into network usage and potential security incidents.
- Real-Time Monitoring: Offers real-time monitoring capabilities to detect and respond to security events as they occur.

7. Policy Management:
- Rule-Based Policies: Allows administrators to define and enforce security policies based on IP addresses, ports, protocols, and user identities.
- Granular Controls: Provides granular controls over network access, enabling tailored security measures for different segments of the network.

8. High Availability and Load Balancing:
- Failover Capabilities: Supports high availability configurations to ensure continuous network protection in case of hardware or software failures.
- Load Balancing: Distributes network traffic across multiple servers or firewalls to optimize performance and prevent overloads.

9. User Authentication and Access Control:
- Identity-Based Access: Integrates with authentication systems to enforce user-based access controls, ensuring that only authorized users can access certain network resources.
- Multi-Factor Authentication (MFA): Supports MFA to enhance the security of user authentication processes.

10. Advanced Threat Protection (ATP):
- Malware Detection: Identifies and blocks malware using signature-based detection, heuristics, and sandboxing.
- Zero-Day Protection: Provides defenses against unknown or zero-day threats by analyzing behavior and employing machine learning techniques.

11. Quality of Service (QoS):
- Traffic Shaping: Manages bandwidth allocation and prioritizes critical applications or services to ensure optimal network performance.