RANKA
DATE / /
PAGE

Q1 Define IDS? Discuss its classification? Describe its significance in Network Security?

Ans Intrusion detection systems are important tools for security computer network & systems. They are designed to monitor network traffic & system activity in real time to identify security threats. There are two main types of IDS:

1) Network based IDS (NIDS):

This type of IDS is placed on a network segment such as a switch or router, to monitor all Network traffic that passes through it. NB: NIDS system can monitor all network protocol including those used by operating system, application & other type of network.

devices. The can detect security threats such as unauthorised access, unauthorised use of system resources & malicious network traffic. such as malware or misuses.

2) Host - based IDS (HIDS):

This type is installed on individual hosts such as server workstation, or laptops to monitor system activity. HIDS system can monitor events such as login attempts, file access & changes to system setting. They can also detect threat such as unauth software installation changes to system files, and malicious processes.

Both type of IDS use a variety of technique to detect potential security threat. These technique include :-

RANKA
DATE / /
PAGE

1) Signature-based detection:-

This technique uses a databases of known attack signature to identify known threats. The IDS compare network traffic or system activities against the signature database, & if a match, an alert is generated.

2) Anamaly based detection:

This techniques uses machine learning algorithm to identifies abnormal or suspicious behaviour. The IDS monitor network traffic or systems activity & build a model of normal behaviour. Any deviation from the normal behaviour are considered potential security threats. & generate an alert -

3) Rule based detection :-

This technique used set of predefined rules to identify potential security threats ; the rule can be based on network traffic patterns, system activities or other types of events. If a rule is triggered an alert is generated.

IDS system are critical components of a comprehensive security strategy & play an important role is protecting computer network & system from potential security threats. However, it is important to note that no IDS system can provide 100% protection & it is essential to implement other security measure, such as firewall ; encryption & user education, to reduce the risk of security breaches.

The significance of IDS in network security lies in their ability to provide an early warning of potential security threats & to help organisation respond to these threats in a ~~final~~ timely & effective manner:-

1) Early Detection: IDS system monitor network traffic & system activity in real time, allowing them to detect potential security threats as soon as they occur.

2) Improved visibility: IDS system provide detailed information about network traffic & system activity / allowing organisation to gain a better understanding of the security posture of their network & system.

3) Compliance: Many regulation:

such as HIPAA, PCI-DSS & SOX, requires organisation to implement security measure to protect information. IDS system can help organization meet these requirement by providing evidence of their security posture & by detecting security incident that may lead to regulatory action.

4) Cost Saving: IDS system can help organization reduce the cost of security breaches by detecting potential threats early, reducing the amount of damage caused, & allowing organization, to respond quickly to mitigate the risk.

5) Integration with other security technology:- IDS system can be integrated with other security technologies such as firewall,

antivirus software & intrusion prevention system to provide a more comprehensive security solution.

RANKA
DATE / /
PAGE

Q2 What is meant by Cyber Security Metric & what assistance it provide to the organization? Discuss some important cybersecurity metrics that portray the current threat scenario really well.

Ans Cybersecurity metrics are quantative measure that help organisation evaluate the effectivenes of their cyber security measures & the overall security posture of their network & systems these metrics provide organisation with valuable information about the security of these assests allow them to make informed decision about how to allocate resources to improve the security responde.

1) Risk assesment :- By measuring the effectivenes of instence security measure organization can identify

areas where their security posture is weak & prioritize efforts to reduce risks. This can help organisation make informed decision about where to allocate resources.

2) Resource allocation: By measuring the effectiveness of security measure, organisation can determine which means that are measure providing them value & dedicate resources more effectively.

3) Improved Decision Making: By providing data & insights into the security posture of their network & systems.

4) Trend Analysis: By tracking cyber security metrics over time, organisation can identify trends in their security posture & make

informed decision about how to respond to change in the threat landscape.

Metrics that organisation can use to evaluate the effectiveness of their security measure & to understand threat landscape.

1) Threat Intelligence: This metric measure or number & type of threats that organisation are facing, as well as the frequency & security of these threats.

2) Vulnerability Assessment :-

This metric measure number & security of vulnerabilities in an organization system & application.

3) Incident response: This metric measure the time it takes for an organization to detect & respond to a security incident

4) Data Loss Prevention: This metric measure the extent to which an organisation is able to prevent sensitive data from being lost or stolen. This information can be used to prioritize efforts improved DLP measure & to reduce risk of data loss.

5) User Awareness: This metric measures intent to which employees & other user are aware of security threats & best practice for protecting sensitive information.

6) Network Security: This metric measure the effectiveness of network

security measure such as firewall & intrusion detection system in prevention of unauthorized access to an organisation networks & system.

In conclusion there are some of the most important cyber security measure and to understand current threat landscape. By using these metrics; organisation can make informed decision about their security position & allocate resources more effectively to probe.

RANKA
DATE / /
PAGE

Q3. Define Network Security tools? Explain the technical Description of any five such tools for Network Scanning, penetration Testing & vulnerabilities Analysis?

Ans Security Network tools are: software & hardware solution designed to protect computer network from various threats such as cyber attack, data breaches, & unauthorized access; these tools can be classified into several categories:

1) firewall: A firewall is a network security system that monitors & control incoming & outgoing network traffic based on pre-determined security rules. It helps to prevent unauthorized access to a network & protect against cyber attacks.

2) Intrusion Detection & prevention System:

These system are designed to detect & prevent unauthorized access to a network by monitoring network traffic for signs of malicious activity. They can also block malicious traffic in time to prevent an attack from happening.

3) VPN (Virtual Private Network):

VPN are used to securely connect to a remote Network over the internet. They encrypted all the data transmitted between users devices & the VPN server, making it difficult for anyone to intercept or steal the data.

4) Anti-virus: These are designed to detect & remove malicious software from a network. They protect against viruses, worms, Trojans & others

types of malacious malware that can harm & it user.

5) Network Access control (NAC): It is a security solution that controls who has access to a network & what they can do on the network. It helps to prevent unauth access & ensure that only ~~otho~~ authorized users have access to sensitive information.

6) Security Information & Event Management (SIEM): It is a ~~security~~ security solution that aggregate log data from multiple sources within a network to provide a centralized view of network security. It can detect threat & provide real time notification of security incident.

RANKA
DATE / /
PAGE

Network Scaning tool:-

(1) Nmap :- It operates by sending packets to the target Network & analyzing the process.

(a) Port scan : Sends packets to target host and to determine which port are open, closed or filtered.

(b) Version Scan: It can identify the version number of services running on a target host.

(c) OS Scan: Nmap can identify the operating system of a target host by analyzing the response to its packets.

(d) Script Scan : Nmap support a large number of script that can run against target host.

RANKA
DATE / /
PAGE

(2) Metasploit allows security professional to perform various penetration tests, key features are:-

a) Exploit Database: Metasploit maintain a large database of exploit for a wide range of system & application.

b) Payload generation: It allows the user to generate payload that can be delivered to target system via an exploit. These payload can be used remotely too.

c) Automated testing: Metasploit provide a variety of reporting option including the ability to generate report & various formats such as HTML, PDF & CSV.

RANKA
DATE / /
PAGE

Vulnerability Analysis:

Nessus is commercially used vulnerabilities tool that provides detailed reporting & remediation guidance.

1) Asset Discovering: Nessus perform scan of the Network to identify all connected hosts & devices as well as the services they offer.

2) Vulnerability Scanning: Nessus perform a scan of each host & device on the Network to identify potential vulnerabilities.

3) Threat Intelligence: Nessus integrates with various threat intelligence feeds to provide up-to-date information on the latest threats & vulnerabilities.

4) Reporting: Detailed report that summarizes the result of the vulnerability Analysis.

5) Remediation Support: Nessus provide support for remediation efforts, including the ~~abil~~ ability to automate the process of applying patches & updates as well as the ability to enforce security policies & configuration.

6) Custom policies: Nessus allows users to create custom policies that can be used to target specific assests & vulnerabilities.