3. How Scanning and Analysis tools are useful in enforcing Information Security?

Explain different types of the Scanning and Analysis tools available. (Nov /Dec 2011)

- Scanners, sniffers, and other analysis tools are useful to security administrators in enabling them to see what the attacker sees
- Scanner and analysis tools can find vulnerabilities in systems
- One of the preparatory parts of an attack is known as foot printing – collecting IP addresses and other useful data
- The next phase of pre-attack data gathering process is called fingerprinting – scanning all known addresses to make a network map of the target

The attack protocol is a series of steps or processes used by an attacker, in a logical sequence to launch an attack against a target system or networks. One of the preparatory part of the attack protocol is the collection of publicly available information about a potential target, a process known **as** foot printing.

information about a potential target, a process known as foot printing.

Foot printing

- Foot printing is the organized research of the Internet addresses owned or controlled by the target organization. The attacker uses public Internet data sources to perform keyword searches to identify the network addresses of the organization. This research is augmented by browsing the organization's web pages.
- The next phase of the attack protocol is a second intelligence or data-gathering process called **fingerprinting.** This is systematic survey of all of the target organization's **Internet addresses (**which are collected during the foot printing phase); the survey is conducted to ascertain the network services offered by the hosts in that range.
- Fingerprinting reveals useful information about the internal structure and operational nature of the target system or network for the anticipated attack.

Port Scanners

- Port scanners fingerprint networks to find ports and services and other useful information
- Why secure open ports?
    - An open port can be used to send commands to a computer, gain access to a server, and exert control over a networking device
    - The general rule of thumb is to remove from service or secure any port not absolutely necessary for the conduct of business

Vulnerability Scanners

- Vulnerability scanners are capable of scanning networks for very detailed information

- As a class, they identify exposed usernames and groups, show open network shares, expose configuration problems, and other vulnerabilities in servers

Packet Sniffers

- A network tool that collects copies of packets from the network and analyzes them
- Can be used to eavesdrop on the network traffic
- To use a packet sniffer legally, you must be:
  - on a network that the organization owns
  - under direct authorization of the owners of the network
  - have knowledge and consent of the content creators (users)

Content Filters

- Although technically not a firewall, a content filter is a software filter that allows administrators to restrict accessible content from within a network
- The content filtering restricts Web sites with inappropriate content

Trap and Trace

- Trace: determine the identity of someone using unauthorized access
- Better known as honey pots, they distract the attacker while notifying the administrator

Wireless Security Tools

- Organization that spends its time securing wired network and leaves wireless networks to operate in any manner is opening itself up for security breach.
- A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess level of privacy or confidentiality afforded on the wireless network

Firewall Analysis Tools

- Several tools automate remote discovery of firewall rules and assist the administrator in analyzing the rules
- Administrators who feel wary of using same tools that attackers use should remember:
  - It is intent of user that will dictate how information gathered will be used

- A tool that can help close up an open or poorly configured firewall will help network defender minimize risk from attack