Lecture NS10 2018

Chapter 21: Malicious Software

Describe main types of the malicious software Answer: maybe https://en.wikipedia.org/wiki/Malware ?

Ch22: Intruders

Q1 : Briefly describe three classes of intruders

One of the two most publicized threats to security is the intruder (the other is viruses), often referred to as a hacker or cracker.
3 classes of intruders:

- **Masquerader:** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account

- **Misfeasor:** A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges
- **Clandestine user:** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection

Q2: Give examples of Intrusions

- Performing a remote root compromise of an e-mail server
- Defacing a Web server
- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information, without authorization
- Running a packet sniffer on a workstation to capture usernames and passwords
- Using a permission error on an anonymous FTP server to distribute pirated software and music files
- Dialing into an unsecured modem and gaining internal network access
- Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password
- Using an unattended, logged-in workstation without permission

Q3: Describe basic approaches to Intrusion detections

Chapter 23

1. Describe major characteristics of firewalls: There

are four major characteristics of firewalls:

- Service control: Determines the types of Internet services that can be accessed, inbound or outbound.
- Direction control: Determines the direction in which particular service request may be initiated and allowed to flow through the firewall.
- User control: Controls access to a service according to which user is attempting to access it. This feature is typically applied to users inside the firewall.
- Behaviour control: Controls how particular service are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on server

2. Briefly describe four types of firewalls.

There are four types of firewalls:

- Packet Filtering Firewall
- Stateful Inspection Firewall
- Application Level Gateway
- Circuit Level Gateway

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

2. SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter ruleset allowing inbound and outbound SMTP traffic. You generate the following ruleset:

a. Describe the effect of each rule.

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	?
2	Out	172.16.1.1	192.168.3.4	TCP	1234	?
3	Out	172.16.1.1	192.168.3.4	TCP	25	?
4	In	192.168.3.4	172.16.1.1	TCP	1357	?

b. Your host in this example has IP address 172.16.1.1. Someone tries to send e-mail from a remote host with IP address 192.168.3.4. If successful, this generates an SMTP dialogue between the remote user and the SMTP server on your host consisting of SMTP commands and mail. Additionally, assume that a user on your host tries to send e-mail to the SMTP server on the remote system. Four typical packets for this scenario are as shown:

Indicate which packets are permitted or denied and which rule is used in each case.