Chapter 13 – Network Protection Systems

Lecture Notes

Overview

This chapter describes several network protection systems that security professionals and network administrators can use to better protect their networks. You will learn about firewall technologies and how they can contribute to make a network safer. You will also learn about intrusion detection systems and intrusion prevention systems and their role in network defense. Finally, the chapter introduces the concept of honeypots and how they can be used to better understand the techniques of hackers.

Chapter Objectives

After reading this chapter and completing the exercises, you will be able to:

- Explain how routers are used as network protection systems
- Describe firewall technology and tools for configuring firewalls and routers
- Describe intrusion detection and prevention systems and Web-filtering technology
- Explain the purpose of honeypots

Tips

Understanding Network Protection Systems

1. A network protection system is simply any device or system designed to protect a network.

2. A Unified Threat Management (UTM) device is a single device that combines many network protection functions, such as those performed by:
    a. Routers
    b. Firewalls
    c. Intrusion detection and prevention systems
    d. VPNs
    e. Web-filtering systems
    f. Malware detection and filtering systems

3. The term security appliance can be used to describe both UTMs and network protection systems.

Understanding Routers

1. Routers are hardware devices used on a network to send packets to different network segments.

2. The routing protocols used by routers in a best-path decision-making process.
    a. Link-state routing protocol
    b. Distance-vector routing protocol
    c. Path-vector routing protocol

Understanding Basic Hardware Routers

1. Vulnerability information released by Cisco about its products is an example of the issues security professionals work with.

Tip	Articles from SecurityFocus about exploiting Cisco routers available at http://www.securityfocus.com/infocus/1734 and http://www.securityfocus.com/infocus/1749.

Cisco Router Components

1. The components used by a Cisco router.
    a. Random access memory (RAM)
    b. Nonvolatile RAM (NVRAM)
    c. Flash memory
    d. Read-only memory (ROM)
    e. Interfaces

Cisco Router Configuration

1. Understand configuration mode.

2. Understand what kind of configuration tasks administrators can do once they are in privileged mode.

3. Understand global configuration mode.

4. Understand the interface configuration mode.

5. See Table 13-1 for some of the commands available on Cisco routers and their functions.

Understanding Access Control Lists

1. IP access lists are lists of IP addresses, subnets, or networks that are allowed or denied access through a router's interface.

2. Understand both types of access lists.
    a. Standard IP access lists
    b. Extended IP access lists

Tip	See http://www.certiology.com/cisco-certifications/ccna/ccna-routing-and-switching/free-cisco-ccna-study-guide/access-lists.html for more on standard IP and extended IP access lists.

Standard IP Access Lists

1. Standard IP access lists can restrict IP traffic entering or leaving a router's interface based on source IP address.

Extended IP Access Lists

1. Extended IP access lists can restrict IP traffic entering or leaving a router's interface based on:
    a. Source IP address
    b. Destination IP address
    c. Protocol type
    d. Application port number

Understanding Firewalls

1. Firewalls are hardware devices or software installed on a system having two purposes:
    a. Controlling access to all traffic that enters an internal network.
    b. Controlling all traffic that leaves an internal network.

2. Understand the advantages and disadvantages of hardware-based and software-based firewalls.

Understanding Firewall Technology

1. Firewall technologies described in this section.
    a. Network address translation (NAT)
    b. Access lists
    c. Packet filtering
    d. Stateful packet inspection (SPI)
    e. Application layer inspection

Network Address Translation

1. NAT can help a security professional hide the corporate internal network from outsiders.

2. PAT is used to map thousands of internal IP addresses to one external IP address.

Tip	For more information about NAT and PAT: http://www.enterprisenetworkingplanet.com/netsp/article.php/3632496/Networking-101-Understanding-NAT-and-PAT.htm.

Access Lists

1. Access lists are also used to filter traffic based on source IP address, destination IP address, and ports or services.

Packet Filtering

1. Packet filters screen packets based on information contained in the packet header, such as:
    a. Protocol type
    b. IP address
    c. TCP/UDP port

Stateful Packet Inspection

1. Stateful packet filters record session-specific information about a network connection.

2. See Table 13-2 for a state table, which is a file that stateful packet filters use to record session-specific information about a network connection.

2. Stateful packet filters can recognize types of anomalies that most routers ignore.

Tip	More about stateful packet inspection at http://www.webopedia.com/TERM/S/stateful_inspection.html.

Application Layer Inspection

1. An application-aware firewall inspects network traffic at a higher level in the OSI model than a traditional stateful packet inspection.

Implementing a Firewall

1. Understand why demilitarized zones (DMZs) are used.

Demilitarized Zone

1. A DMZ is a small network containing resources available to Internet users.

2. Understand how to configure a good DMZ. See Figure 13-2 and Figure 13-3.

Tip See http://compnetworking.about.com/cs/networksecurity/g/bldef_dmz.htm for more on DMZs.

Understanding the Cisco Adaptive Security Appliance Firewall

1. Cisco ASA has replaced the Cisco PIX firewall and added advanced modular features, such as intrusion detection and prevention and more sophisticated application layer inspection.

Configuring the ASA Firewall

1. Understand the process of logging into an ASA firewall.

2. Understand how to change to a different configuration mode once inside the ASA firewall.

3. See the examples in the book of configuration rules and files.

Using Configuration and Risk Analysis Tools for Firewalls and Routers

1. One of the best Web sites for finding configuration benchmarks and configuration assessment tools for Cisco routers and firewalls is the Center for Internet Security.

2. See Figure 13-4 for the use of RedSeal, a unique network risk analysis and mapping tool.

Tip Visit the RedSeal Web site at http://www.redseal.net/.

Understanding Intrusion Detection and Prevention Systems

1. Understand the difference between an intrusion detection system (IDS) and an intrusion prevention system (IPS).

Network-Based and Host-Based IDSs and ISPs

1. Understand the differences between network-based and host-based IDSs/ISPs.

2. Describe the differences between passive systems and active systems.

3. Understand how anomaly detectors function.

Web Filtering

1. Methods hackers use once they get into a network – try to get users to visit bogus Web sites and install malicious Trojan codes, which can then be controlled remotely.
2. Blocking access to uncategorized sites is a very effective security practice but could cause inconvenience for users.
3. Understand drive-by downloads.

Security Operations Center (SOC)

1. In large organizations that have sensitive or critical data, normal administrative expertise isn't enough to follow up on and do damage assessment, risk remediation, and legal consultation. These organizations might need a Security Operations Center (SOC).
2. A SOC is a permanent team whose members are responsible solely for security-response functions. A SOC would also monitor for artifacts left behind by attackers (called indicators of compromise).
3. Security Information and Event Management (SIEM) tools can help the teams identify attacks and indicators of compromise by collecting, aggregating, and correlating log and alert data from routers, firewalls, IDS/IPS, endpoint logs, Web-filtering devices, honeypots, and other security tools.

Understanding Honeypots

1. A honeypot is a computer placed on the perimeter of a network that contains information intended to lure and then trap hackers.
2. Honeypot computers are configured to have vulnerabilities and that one goal of a honeypot is to keep hackers connected long enough to be traced back.

How Honeypots Work

1. Administrators can configure honeypots to divert hackers' attention from the real company's network to these vulnerable, but controlled, machines.
2. See Table 13-4 and Table 13-5 for commercial and open-source honeypots.
3. Understand how virtual honeypots are created.

Tip	Visit http://www.opencanary.org/en/latest/ for an overview of OpenCanary.

<u>Additional Resources</u>

1. How Network Address Translation Works: http://computer.howstuffworks.com/nat.htm
2. How Firewalls Work: http://computer.howstuffworks.com/firewall4.htm
3. Personal Firewall Reviews: http://www.firewallguide.com/software.htm
4. Snort: http://www.snort.org/
5. Linux Iptables HOWTO: http://www.linuxguruz.com/iptables/howto/iptables-HOWTO.html
6. A Virtual Honeypot Framework: http://www.citi.umich.edu/techreports/reports/citi-tr-03-1.pdf

Key Terms

- active systems
- anomaly-based IDS
- application-aware firewall
- demilitarized zone (DMZ)
- distance-vector routing protocol
- drive-by downloads
- firewalls
- honeypot
- host-based IDSs/IPSs
- indicators of compromise
- intrusion detection systems (IDSs)
- intrusion prevention systems (IPSs)
- IP access lists
- link-state routing protocol
- Network Address Translation (NAT)
- network-based IDSs/IPSs
- network protection system
- passive systems
- path-vector routing protocol
- privileged mode
- security appliance
- Security Information and Event Management (SIEM)
- Security Operations Center (SOC)
- stateful packet filters
- stateless packet filters
- state table
- user mode
- Unified Threat Management (UTM)