Hands-On Ethical Hacking and Network Defense, Edition 4

Chapter 13: Network Protection Systems

Module Objectives

- By the end of this module, you should 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

Using Network Protection Systems

- **Network protection system**
  - Any device or system designed to protect a network
- **Unified Threat Management (UTM)** device
  - Term used to describe a single device that combines many network protection functions
    - Such as those performed by routers, firewalls, intrusion detection and prevention systems, VPNs, web-filtering systems, and malware detection and filtering systems
- **Security appliance**
  - Can describe both UTMs and network protection systems

Using Routers to Reduce Network Attacks

- Routers are hardware devices
  - Used to send packets to different network segments
  - Main purposes
    - Reduce broadcast traffic passing over a network
    - Choose the best path for moving packets
- Routing protocols
  - **Link-state routing protocol**
    - Sends link-state advertisements to other routers
  - **Distance-vector routing protocol**
    - Router passes its routing table to neighboring routers on the network
  - **Path-vector routing protocol**
    - Uses dynamically updated paths or routing tables to transmit packets from one autonomous network to another

Cisco Router Components (1 of 2)

- Random access memory (RAM)
  - Holds the router's running configuration, routing tables, and buffers
    - If turned off, contents stored in RAM are erased
- Nonvolatile RAM (NVRAM)
  - Holds router's configuration file
    - Information is not lost if the router is turned off
- Flash memory
  - Holds the Internetwork Operating System (IOS) the router is using
  - Rewritable memory, so IOS can be upgraded

Cisco Router Components (2 of 2)

- Read-only memory (ROM)
  - Contains a minimal version of Cisco IOS
    - Used to boot router if flash memory gets corrupted
- Interfaces
  - These components are the hardware connectivity points to the router
    - The components you're most concerned with
- Basic Cisco commands
  - A security professional should be aware of the basic Cisco commands
    - To view information in the Cisco router components
  - Example: `RouterB# **show running-config**`
    - To see what information is stored in RAM, a Cisco administrator uses the command above

Cisco Router Configuration (1 of 2)

- Configuration modes:
  - **User mode**
    - Administrator can perform basic troubleshooting tests and list information stored on the router
    - Indicated by the router name followed by a > symbol
    - When first logging on to a Cisco router, you're in user mode by default
  - **Privileged mode**
    - Administrator can perform full router configuration tasks
    - Indicated by a router name followed by a # sign

Cisco Router Configuration (2 of 2)

- Modes to configure the router in privileged mode
  - Global configuration mode
    - Administrator can configure router settings that affect overall router operation
  - Interface configuration mode
    - Administrator can configure an interface on the router, such as a serial port

Cisco Commands (1 of 3)

Mode	Command	Prompt	Description
Privileged or user	`show version`	`Router#` or `Router>`	Displays the router's version information, including the IOS version number
Privileged or user	`show ip route`	`Router#` or `Router>`	Displays the router's routing table
Privileged or user	`show interfaces`	`Router#` or `Router>`	Lists configuration information and statistics for all interfaces on the router
Privileged or user	`show flash`	`Router#` or `Router>`	Shows the contents of flash memory and the amount of memory used and available
Privileged	`show running-config`	`Router#`	Displays the currently running router configuration file

Cisco Commands (2 of 3)

Mode	Command	Prompt	Description
Privileged	`show running-config`	`Router#`	Displays the currently running router configuration file
Privileged	`show startup-config`	`Router#`	Displays the contents of NVRAM
Privileged	`copy running-config startup-config`	`Router#`	Copies the running configuration to NVRAM so that changes made are carried out the next time the router is started
Privileged	`copy startup-config running-config`	`Router#`	Copies the startup configuration from NVRAM to memory (RAM)
Global configuration (privileged)	`configure terminal`	`Router (config)#`	Enables you to change configuration settings that affect overall router operation

Cisco Commands (3 of 3)

Mode	Command	Prompt	Description
Interface configuration (privileged)	`interface serial`	`Router (config-if)#`	Enables you to configure the serial interface you identify, such as serial 0
Interface configuration (privileged)	`interface fastethernet`	`Router (config-if)#`	Enables you to configure the Fast Ethernet interface you specify

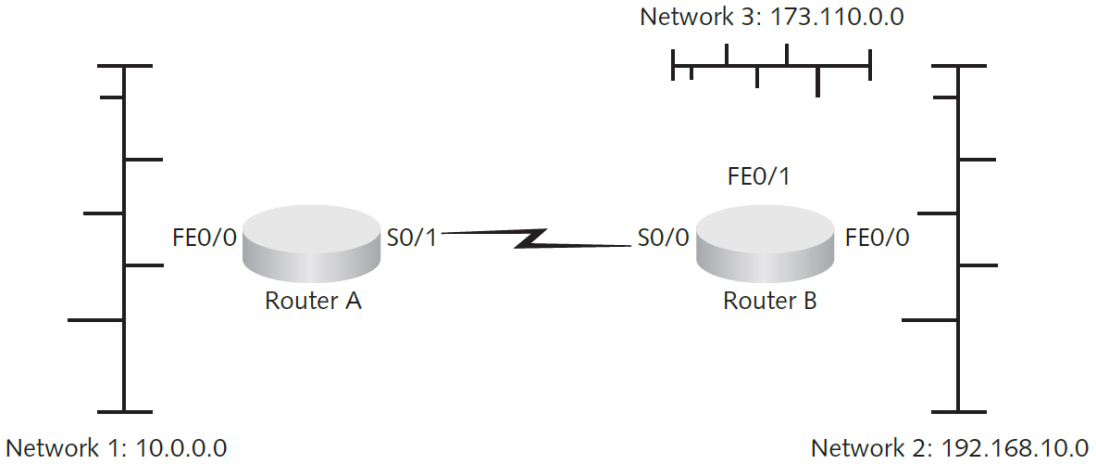
Using Access Control Lists

- Several types of access control lists
  - This section focuses on **IP access lists**
  - IP access lists: Lists of IP addresses, subnets, or networks that are allowed or denied access through a router's interface
- An administrator can create two types of access lists on a Cisco router
  - Standard IP access lists
  - Extended IP access lists

Standard IP Access Lists

- Can restrict IP traffic entering or leaving a router's interface based on source IP address
  - To restrict all traffic from Network 3 from entering Network 1, an administrator can create a standard IP access list that looks like:

```
access-list 1 deny 173.110.0.0 0.0.255.255
access-list permit any
```



Extended IP Access Lists

- Restrict IP traffic entering or leaving based on the following criteria:
  - Source IP address
  - Destination IP address
  - Protocol type
  - Application port number
- Configuration
  - Same as configuring a standard IP access list
    - A network administrator can decide which interface to apply an access list to, based on several variables

Knowledge Check Activity 13-1

Which type of routing protocol advertises only new paths to other routers on the network?

a. Link-state routing protocol
b. Routing table protocol
c. Path-vector routing protocol
d. Distance-vector routing protocol

Knowledge Check Activity 13-1: Answer

Which type of routing protocol advertises only new paths to other routers on the network?

Answer: a. Link-state routing protocol

A link-state routing protocol sends link-state advertisements to other routers; these advertisements identify the network topology and any changes or paths discovered recently on the network. This method is efficient because only new information is sent over the network

Polling Activity 13-1

Which of the following Cisco components stores a router's running configuration, routing tables, and buffers?

a. NVRAM

b. RAM

c. ROM

d. Flash memory

Polling Activity 13-1: Answer

Which of the following Cisco components stores a router's running configuration, routing tables, and buffers?

Answer: b. RAM

The RAM holds the router's running configuration, routing tables, and buffers.

Protecting with Firewalls (1 of 2)

- **Firewalls**
  - Hardware devices with embedded OSs
  - Software installed on general-purpose computer systems
- Firewalls serve two main purposes
  - Control access to traffic entering an internal network
  - Control traffic leaving an internal network
- Advantages of hardware firewall
  - Usually faster than software firewalls
  - Can handle a larger throughput than software firewalls
- Disadvantage of hardware firewall
  - Locked into the firewall's hardware

Protecting with Firewalls (2 of 2)

- Advantage of software firewall
  - Can add network interface cards (NICs) easily to the server running the software
- Disadvantages of software firewall
  - Configuration problems can be a concern
  - Rely on the OS on which they're running

Examining Firewall Technology

- Technologies used by firewalls in reducing attacks
  - **Network Address Translation (N A T)**
  - Access lists
  - Packet filtering
  - Stateful packet inspection (SPI)
  - Application layer inspection

Network Address Translation

- The most basic security feature of a firewall
- Internal private IP addresses are mapped to public external IP addresses
  - Hides the internal infrastructure from unauthorized personnel
- Port Address Translation (PAT)
  - Derived from N A T
  - Allows thousands of internal IP addresses to be mapped to one external IP address

Access Lists

- Used to filter traffic based on:
  - Source IP address
  - Destination IP address
  - Ports or services
- Firewalls also use this technology
- Creating access lists on a firewall
  - Similar to creating them on a router

Packet Filtering

- Packet filters
  - Screen packets based on information contained in the packet header, such as the following:
    - Protocol type
    - IP address
    - TCP/UDP port

Stateful Packet Inspection

- Stateful packet filters
  - Record session-specific information about a network connection, including a **state table**
    - State table is a way for the firewall to track the state of connections
      - Based on what kind of traffic is expected in a two-way session
    - Port scans relying on spoofing or sending packets after a three-way handshake are made ineffective if the firewall uses a state table
    - Recognize types of anomalies that most routers ignore
- **Stateless packet filters**
  - Handle each packet on an individual basis
    - Hence, not resistant to spoofing or DoS attacks

State Table Example

Source IP	Source port	Destination IP	Destination port	Connection state
10.1.1.100	1022	193.145.85.201	80	Established
10.1.1.102	1040	193.145.85.1	80	Established
10.1.1.110	1035	193.145.85.117	23	Established
192.145.85.20	1080	10.1.1.210	25	Closed

Application Layer Inspection

- **Application-aware firewall**
  - Inspects network traffic at a higher level in the OSI model than a traditional SPI firewall does
    - SPI ensures that a packet's source, destination, and port are inspected before forwarding the packet
    - A firewall performing application layer inspection ensures that the network traffic's application protocol is the type allowed by a rule
  - Some application-aware firewalls act as a proxy for all connections
    - Act as a safety net for servers or clients (or both)
      - Depending on what the firewall is protecting
    - **Web application firewall (WAF)**
      - An application-aware firewall that is protecting a web application

Implementing a Firewall

- Using a single firewall between a company's internal network and the Internet can be dangerous
  - Provides hackers complete access to the internal network if the firewall is compromised
- Use a demilitarized zone (DMZ) instead
  - Adds a layer of defense

Demilitarized Zone (1 of 3)

- Small network containing resources that a company wants to make available to Internet users
  - Helps maintain security on the company's internal network
- Sits between the Internet and the internal network
  - Sometimes referred to as a "perimeter network"

Demilitarized Zone (2 of 3)

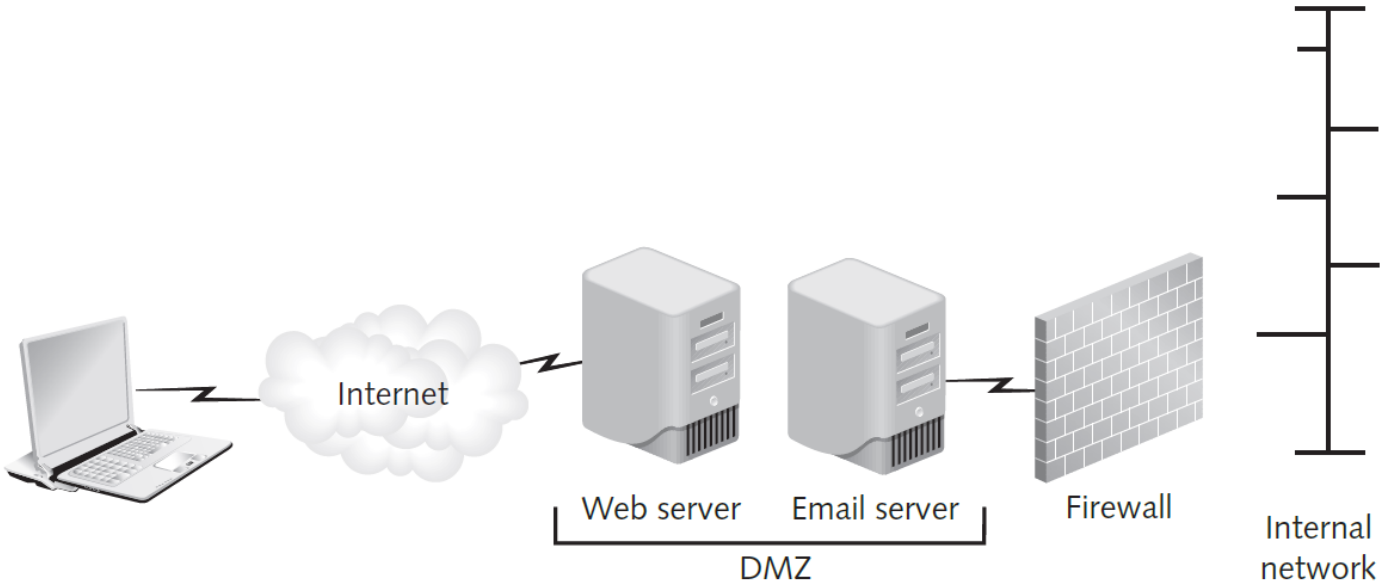


Figure 13-2 A DMZ protecting an internal network

Demilitarized Zone (3 of 3)

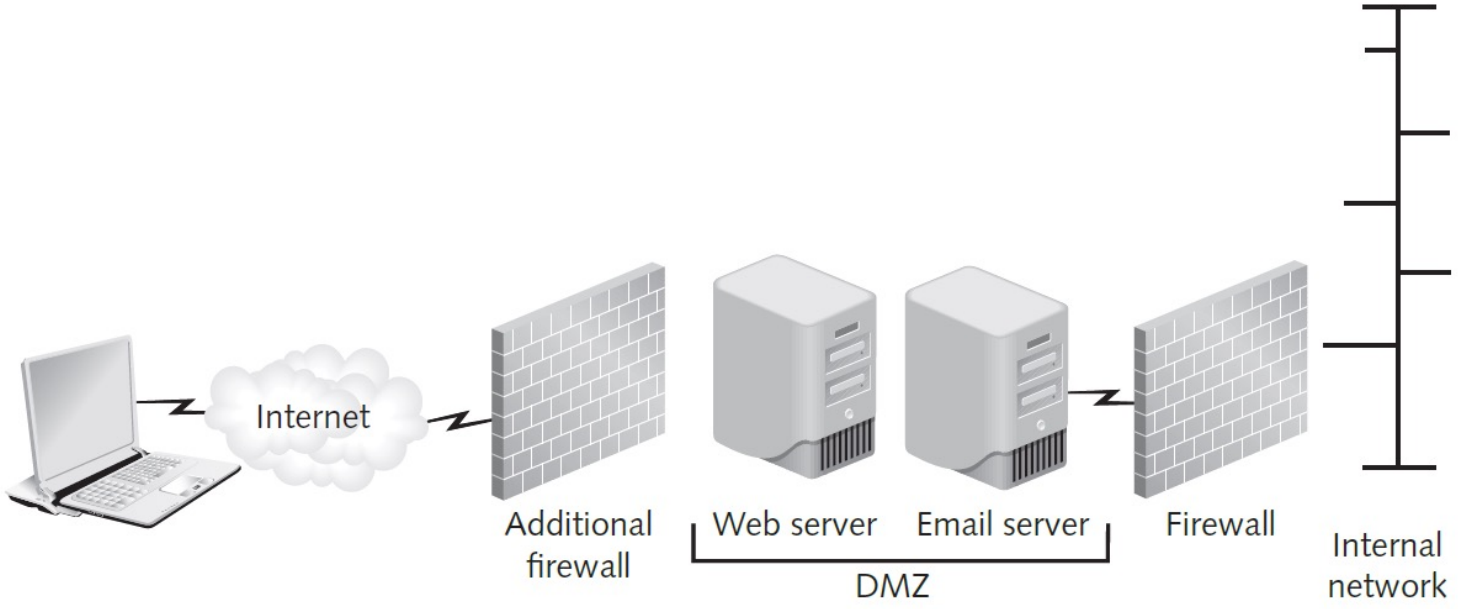


Figure 13-3 An additional firewall used to protect the DMZ

Examining the Cisco Adaptive Security Appliance Firewall

- Cisco Adaptive Security Appliance (A S A) firewall
  - One of the most widely used firewalls
  - Replaced the Cisco PIX firewall
  - Added advanced modular features
    - Intrusion detection and prevention
    - More sophisticated application layer inspection

Configuring the A S A Firewall (1 of 2)

- Similar logon prompt as a Cisco router
  - Prompt

```
If you are not authorized to be in this XYZ Hawaii network
device, log out immediately!
Username: admin
Password: ********
```

    - The banner warning serves a legal purpose
  - Prompt after successful log on

```
Type help or '?' for a list of available commands.
ciscoasa>
```

Configuring the A S A Firewall (2 of 2)

- After entering the correct password, you are placed in a privileged mode
- To enter configuration mode in A S A:
  - Use the same command as on a Cisco router
    `configure terminal` or `configure t`
- Look at how the firewall uses access lists to filter traffic
  - To view access list type, use the following command:
    `# show run access-list`
- Next, look at the object group listing in the A S A configuration

  `show run object-group`

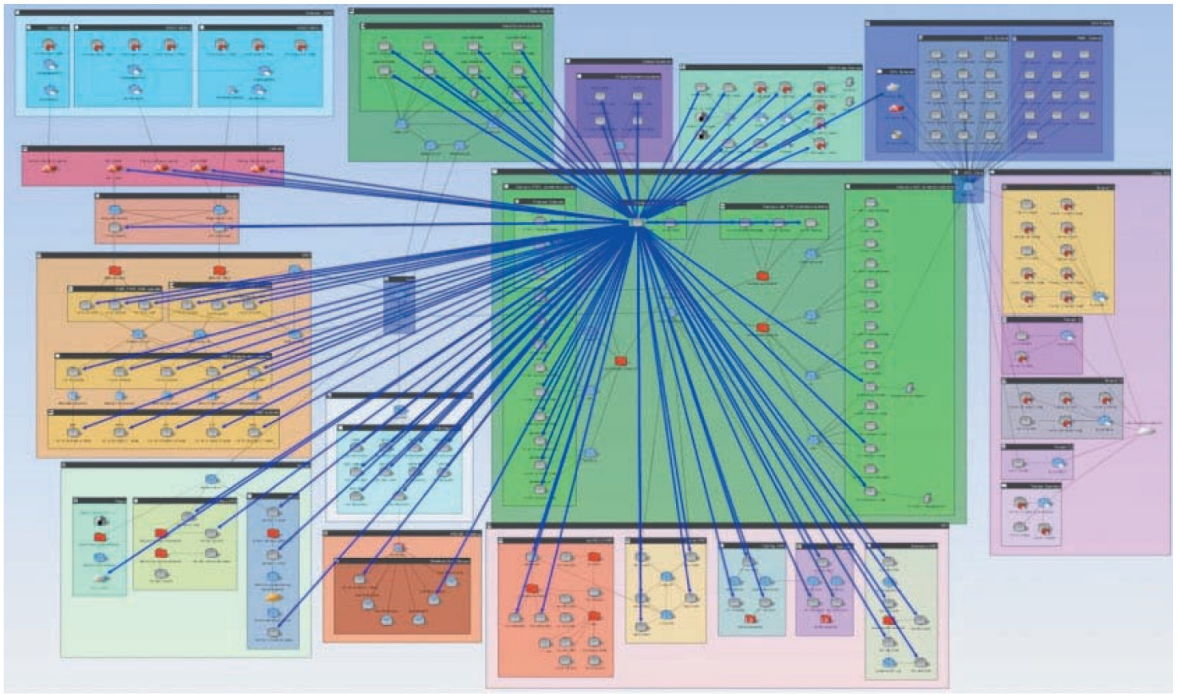
Using Configuration and Risk Analysis Tools for Firewalls and Routers (1 of 3)

- Center for Internet Security (C I S)
  - One of the best websites for finding configuration benchmarks and configuration assessment tools
- Benchmark
  - Industry consensus of best configuration practices on how and why to secure a Cisco router or firewall
    - For Cisco devices, use the C I S Cisco IOS Benchmark
    - The most recent version is 16.0
- C I S offers a useful tool called Configuration Assessment Tool (C A T)
  - Faster and easier to use
  - Available for both *nix and Windows systems

Using Configuration and Risk Analysis Tools for Firewalls and Routers (2 of 3)

- RedSeal
  - A unique network risk analysis and mapping tool
  - Can identify configuration vulnerabilities in routers or firewalls
  - Generates professional-looking reports that can be customized
  - Analyzes IPSs and OS vulnerability scans of a network
    - To produce detailed analysis and mapping
  - Shows a graphical representation of vulnerabilities discovered in the context of the network on which they are found

Using Configuration and Risk Analysis Tools for Firewalls and Routers (3 of 3)



Source: RedSeal

Figure 13-4 The RedSeal network risk map

Polling Activity 13-2

Firewalls use which of the following to hide the internal network topology from outside users?

a. Packet filtering
b. SPI
c. ACL
d. N A T

Polling Activity 13-2: Answer

Firewalls use which of the following to hide the internal network topology from outside users?

Answer: d. N A T

The most basic security feature of a firewall is Network Address Translation (N A T). With N A T, internal private IP addresses are mapped to public external IP addresses, hiding the internal infrastructure from unauthorized personnel.

Protecting with Intrusion Detection and Prevention Systems

- **Intrusion detection systems (IDSs)**
  - Monitor network devices
    - Security administrators can identify attacks in progress and stop them
  - Examine the traffic traversing a connection and compares it with known exploits
    - Similar to virus software using a signature file to identify viruses
- **Intrusion prevention systems (IPSs)**
  - Similar to IDSs
  - Also perform some sort of action to prevent the intrusion

Network-Based and Host-Based IDSs and IPSs (1 of 4)

- **Network-based IDSs/IPSs**
  - Monitor activity on network segments
  - Sniff traffic as it flows over the network
    - Alerts security administrator when something suspicious occurs
  - Some of these systems can block traffic
- **Host-based IDSs/IPSs**
  - Used to protect a critical network server or database server
  - The IDS or IPS software is installed on the system you're attempting to protect

Network-Based and Host-Based IDSs and IPSs (2 of 4)

- IDSs can also be categorized by how they react when they detect suspicious behavior
  - **Passive systems**
    - Don’t take preventative action
    - Send out an alert and log the activity
  - **Active systems**
    - Log events and send out alerts
    - Can also interoperate with routers and firewalls to stop an attack

Network-Based and Host-Based IDSs and IPSs (3 of 4)

- Vendors have started focusing their marketing efforts on IPSs
  - A true network-based IPS is installed inline to network infrastructure
    - Traffic has to pass through IPS before going into or out of the network
  - More capable of stopping malicious traffic because it is inline
  - Host-based IPSs operate at the OS (or kernel) level
    - Intercept traffic that is not allowed by the host policy

Network-Based and Host-Based IDSs and IPSs (4 of 4)

- **Anomaly-based IDS**
  - Uses a baseline of normal activity
    - Sends an alert if the activity deviates significantly from this baseline
  - Most IDS/IPS solutions have anomaly-detection capabilities built in

Product	Description
McAfee Network Protection System	A network-based IDS/IPS with anomaly-detection capabilities
Snort	A popular open-source network-based IDS
Cisco Sourcefire	Enterprise Snort-based IDSs and IPSs
FireEye Intrusion Prevention System	A network-based IDS/IPS which can be deployed as a physical appliance or a cloud-based virtual appliance.

Web Filtering (1 of 2)

- Attackers commonly target the user workstations that are usually allowed access to the Internet
  - If they get an internal user to visit a bogus website or install malicious code from an email attachment, they don't need to break through a firewall
  - After Trojan code is installed on a user's workstation, the attackers can control the Trojan remotely with commands that might seem to be normal traffic
    - Can run network scans from the compromised workstation

Web Filtering (2 of 2)

- Web filtering is used to detect users' attempts to access known malicious websites and block them
  - Some web-filtering systems can actually block malicious code:
    - Before it gets to a user's workstation
    - Before it has a chance to connect to an attacker's control system outside the network
- Mass compromises are used to initiate **drive-by downloads**
  - Website visitors download malicious code without their knowledge
  - Exploit a security flaw in the browser or a third-party application

Security Operations Center (SOC)

- **SOC**
  - Permanent team whose members are responsible solely for security-response functions
- **Indicators of compromise**
  - Artifacts left behind by attackers, which indicate that a system or network has been compromised
- **Security Information and Event Management (SIEM**) tools
  - Help SOC teams identify attacks and indicators of compromise by collecting, aggregating, and correlating log and alert data from various tools
    - Routers, firewalls, IDS/IPS, end point logs, web-filtering devices, honeypots, and other security tools

Knowledge Check Activity 13-2

Which of the following describes a tool that collects logs and alerts from multiple devices for security analysis?

a. Log Management System (LMS)
b. Security Information and Event Management (SIEM)
c. Network-based IPS
d. Honeypot

Knowledge Check Activity 13-2: Answer

Which of the following describes a tool that collects logs and alerts from multiple devices for security analysis?

Answer: b. Security Information and Event Management (SIEM)

SIEM is a tool that can help security-response teams identify attacks and indicators of compromise by collecting, aggregating, and correlating log and alert data from routers, firewalls, IDS/IPS, end point logs, web-filtering devices, honeypots, and other security tools.

Discussion Activity 13-1

Discuss which type of malicious activity can be prevented by web filters.

Discussion Activity 13-1: Answer

Discuss which type of malicious activity can be prevented by web filters.

Answer: Drive-by download

Explanation: In 1988, the National Security Agency (NSA) thought the Data Encryption Standard (DES) was at risk of being broken because of its longevity and the increasing power of computers. NSA proved to be correct in its assumption. The increased processing power of computers soon made it possible to break DES encryption.

Using Honeypots

- **Honeypot**
  - Computer placed on the network perimeter
    - Contains information to lure and then trap hackers
  - Main goal is to distract hackers from attacking legitimate network resources
  - A security professional configures the computer to have vulnerabilities
    - So, hackers spend time trying to exploit these vulnerabilities
  - Another goal is to have hackers connected to the “phony” computer long enough to be detected
  - Serves as an excellent data collector and early warning system

How Honeypots Work

- Honeypot appears to have important data or sensitive information stored on it
  - Could store fake financial data that tempts hackers into attempting to browse through the data
- Basic belief is that hackers will spend time exploiting vulnerabilities
  - Stop looking for other areas to exploit and access a company's resources
- Enables security professionals to collect data on attackers
- Virtual honeypots
  - Created using a programming language rather than configuring a physical device

Self-Assessment

What is the main goal of using honeypots?

Describe the different routing protocols used in the best-path decision making process.

Summary

- Now that the lesson has ended, you should 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