Week 9: Auditing, Testing and monitoring

Ayman El Hajjar

6COSC002W - Security and Forensics

Email: a.elhajjar@westminster.ac.uk
Twitter: @azelhajjar

15 March 2021

University of Westminster

Session Overview

Auditing, Testing, and Monitoring

- A security audit is a crucial type of evaluation to avoid a data breach
- Auditing a computer system involves checking to see how its operation has met security goals
- Audit tests may be manual or automated
- Before you can determine whether something has worked, you must first define how it's supposed to work
  - Known as assessing a system

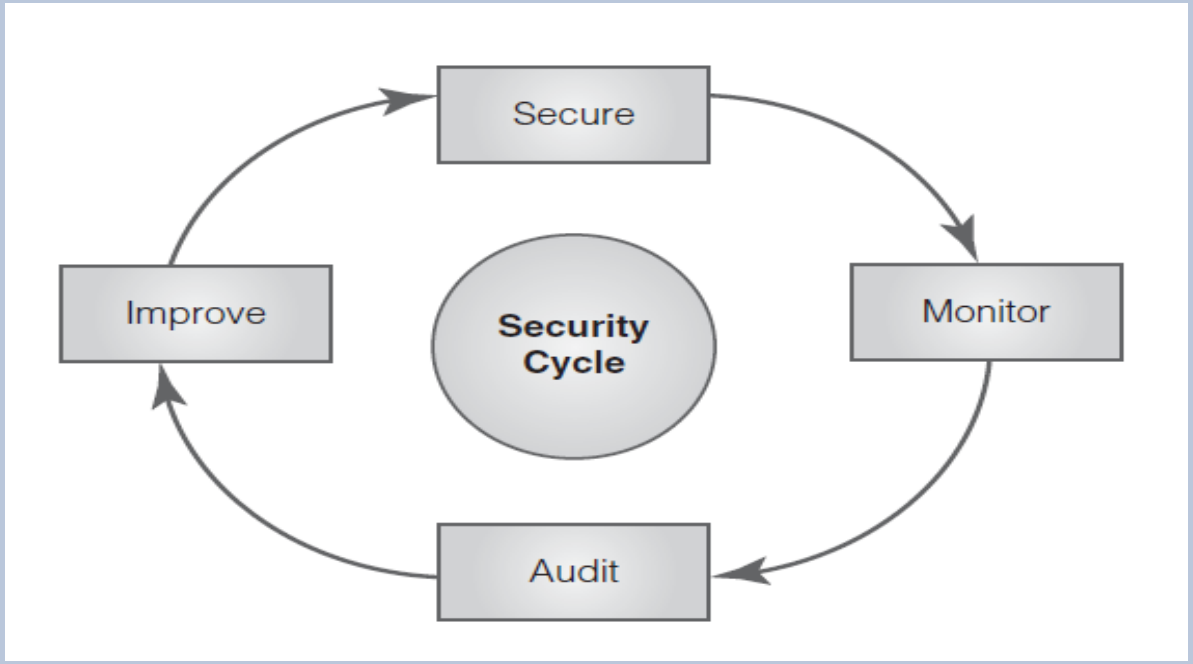
Security Auditing and Analysis

Are security policies sound and appropriate for the business or activity?

Are there controls supporting your policies?

Is there effective implementation and upkeep of controls?

Security Controls Address Risk



Determining What Is Acceptable

- Define acceptable and unacceptable actions
- Create standards based on those developed or endorsed by standards bodies
- Communications and other actions permitted by a policy document are acceptable
- Communications and other actions specifically banned in your security policy are unacceptable

Areas of Security Audits

Large in scope and cover entire departments or business functions

Narrow and address only one specific system or control

Purpose of Audits

Appropriateness of controls

- Is the level of security control suitable for the risk it addresses?

Correct installation of controls

- Is the security control in the right place and working well?

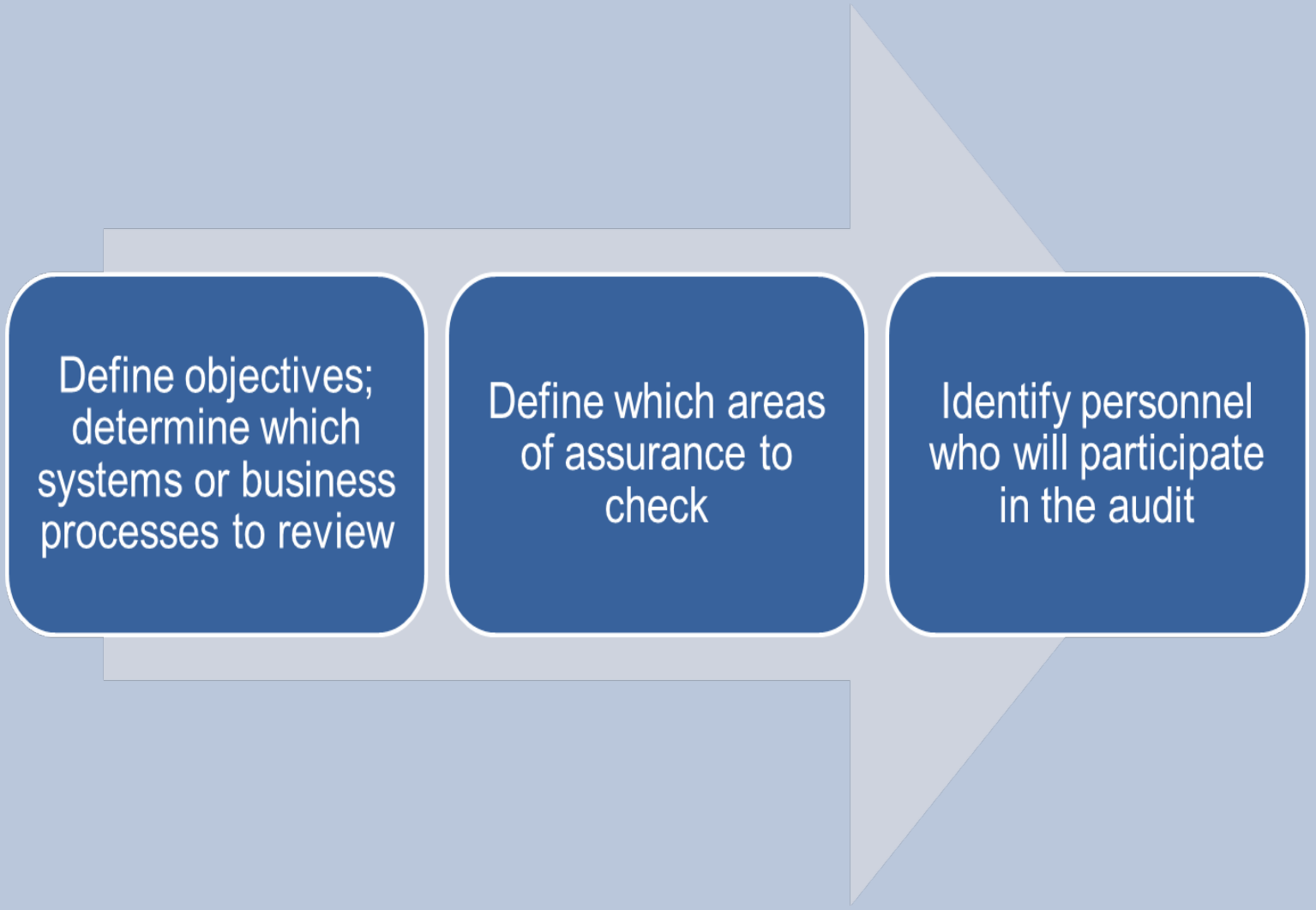
Address purpose of controls

- Is the security control effective in addressing the risk it was designed to address?

Service Organization Control (SOC) Reports

Report	Contents	Audience
SOC 1	Internal controls over financial reporting	Users and auditors Organizations that must comply with the law
SOC 2	Security (confidentiality, integrity, availability) and privacy controls	Management, regulators, stakeholders Service providers, hosted data centres, managed cloud computing providers
SOC 3	Security (confidentiality, integrity, availability) and privacy controls	Public Customers of SOC 2 service providers

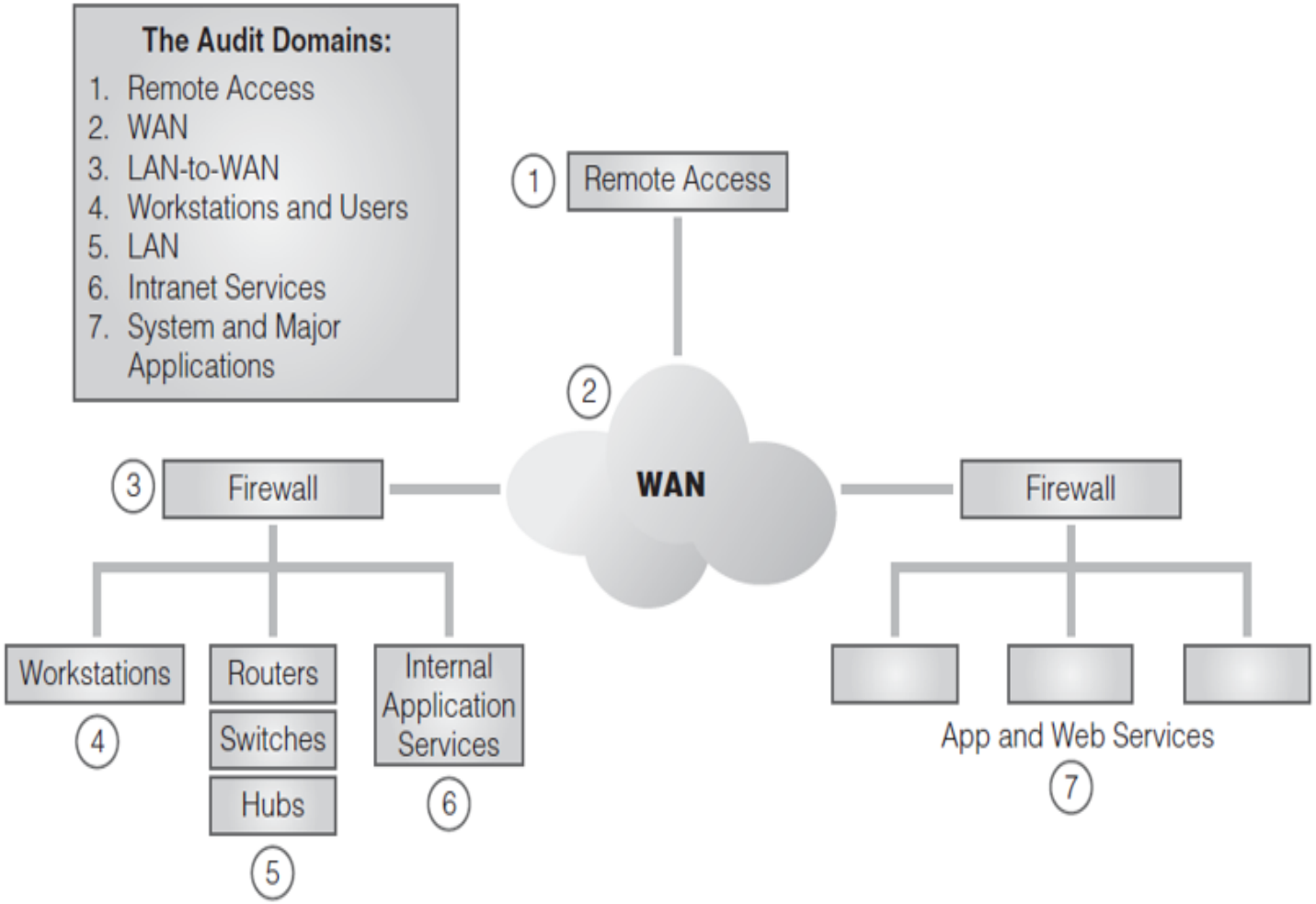
Defining Your Audit Plan



Defining the Scope of the Plan

- Survey the site(s)
- Review documentation
- Review risk analysis output
- Review server and application logs
- Review incident logs
- Review results of penetration tests

Audit Scope and the Seven Domains of the IT Infrastructure



Auditing Benchmarks

Benchmark—The standard to which your system is compared to determine whether it is securely configured

- ISO 27002—ISO 27002
- NIST Cybersecurity Framework (CSF)
- ITIL (Information Technology Infrastructure Library)
  - Control Objectives for Information and related Technology (COBIT)
  - Committee of Sponsoring Organizations (COSO)

Audit Data Collection Methods

- Questionnaires
- Interviews
- Observation
- Checklists
- Reviewing documentation
- Reviewing configurations
- Reviewing policy
- Performing security testing

Areas Included in Audit Plan

Area	Audit Goal
Antivirus software	Up-to-date, universal application
System access policies	Current with technology
Intrusion detection and event monitoring systems	Log reviews
System-hardening policies	Ports, services
Cryptographic controls	Key management, usage (network encryption of sensitive data)
Contingency planning	Business continuity plan (BCP), disaster recovery plan (DRP), and continuity of operations plan (COOP)

Areas Included in Audit Plan (cont.)

Area	Audit Goal
Hardware and software maintenance	Maintenance agreements, servicing, forecasting of future needs
Physical security	Doors locked, power supplies monitored
Access control	Need to know, least privilege
Change control processes for configuration management	Documented, no unauthorized changes
Media protection	Age of media, labeling, storage, transportation

Audit questions: Control Checks and Identity Management

- Approval process: Who grants approval for access requests?
- Authentication mechanisms: What mechanisms are used for specific security requirements?
- Password policy and enforcement: Does the organization have an effective password policy and is it uniformly enforced?
- Monitoring: Does the organization have sufficient monitoring systems to detect unauthorized access?
- Remote access systems: Are all systems properly secured with strong authentication?

Post-Audit Activities

- Exit interview
- Data analysis
- Generation of audit report
  - Findings
  - Recommendations
  - Timeline for implementation
  - Level of risk
  - Management response
  - Follow-up

Monitoring and Testing Security Systems

- Common risks are:
  - Attackers who come in from outside, with unauthorized access, malicious code, Trojans, and malware
  - Sensitive information leaking from inside the organization to unauthorized people who can damage your organization

Monitoring

Monitor traffic with an IDS, which identifies abnormal traffic for further investigation

Use an IPS to actively block malicious traffic

Security Monitoring

- Baselines
- Alarms, alerts, and trends
- Closed-circuit TV
- Systems that spot irregular behavior

Security Monitoring for Computer Systems

Real-time monitoring

- Host IDS
- System integrity monitoring
- Data loss prevention (DLP)

Non-real-time monitoring

- Application logging
- System logging

Log activities

- Host-based activity
- Network and network devices

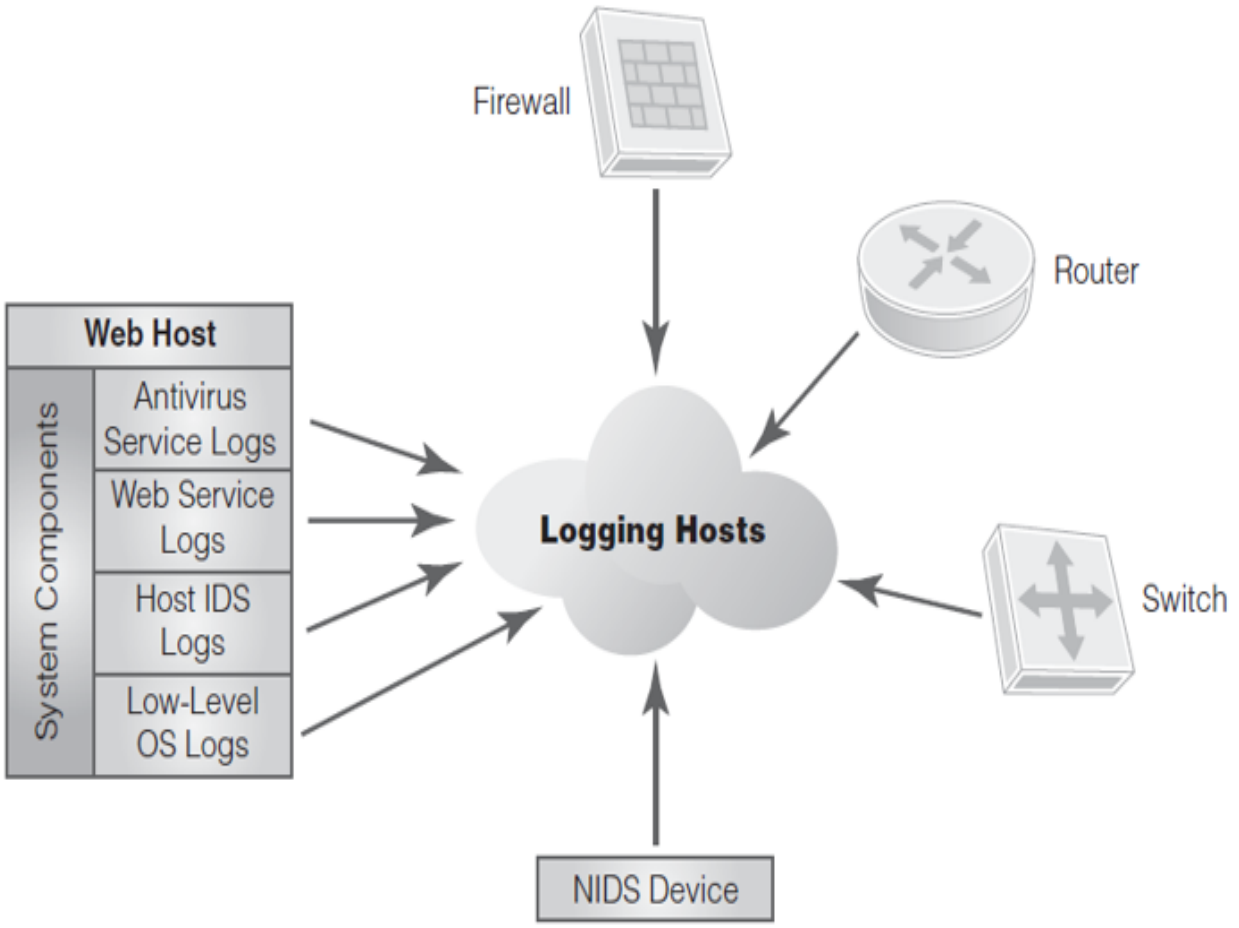
HIDS

- Software processes or services designed to run on server computers
- Intercept and examine system calls or specific processes for patterns or behaviors that should not normally be allowed
- HIDS daemons can take a predefined action such as stopping or reporting the infraction
- Detect inappropriate traffic that originates inside the network
- Recognize an anomaly that is specific to a particular machine or user

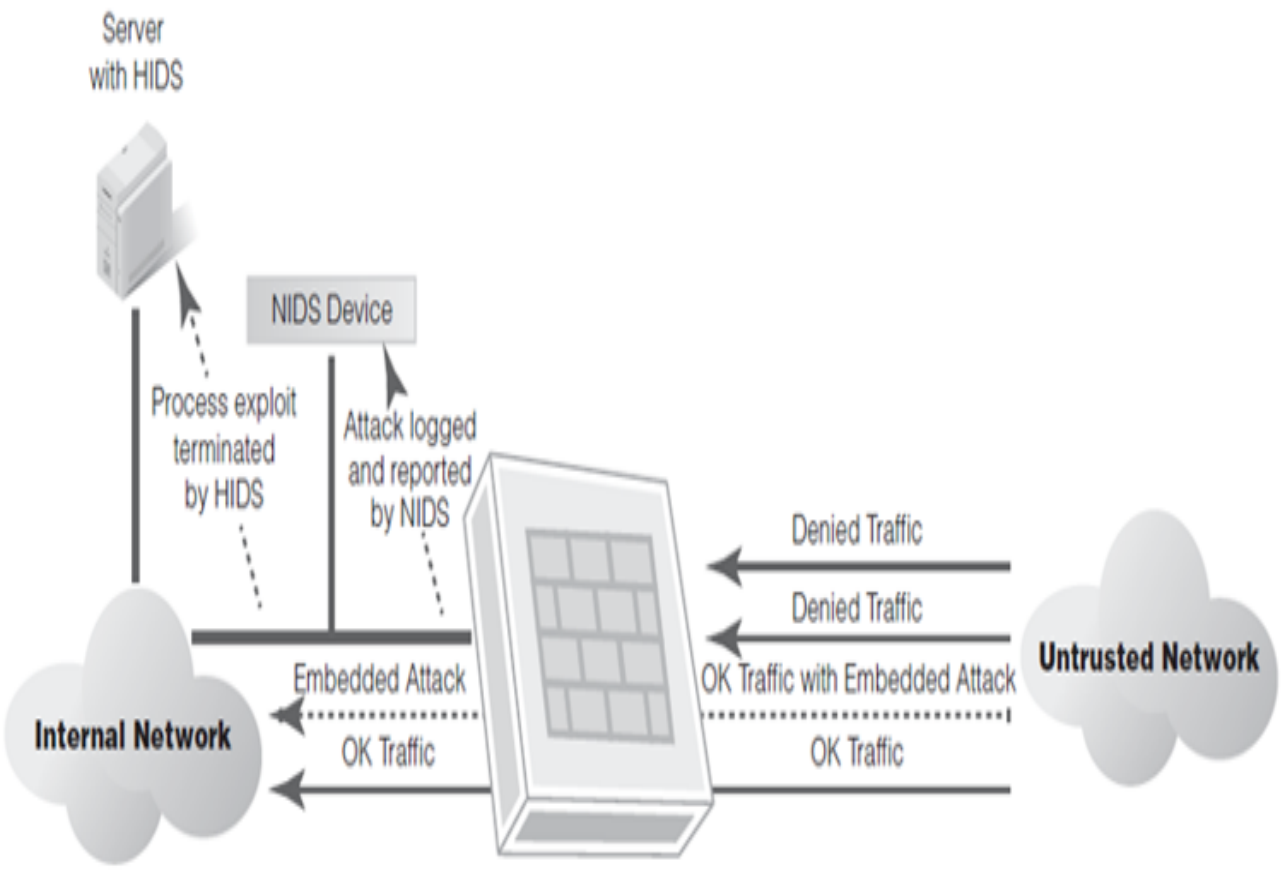
Types of Log Information to Capture

Event logs	• General operating system and application software events
Access logs	• Access requests to resources
Security logs	• Security-related events
Audit logs	• Defined events that provide additional input to audit activities

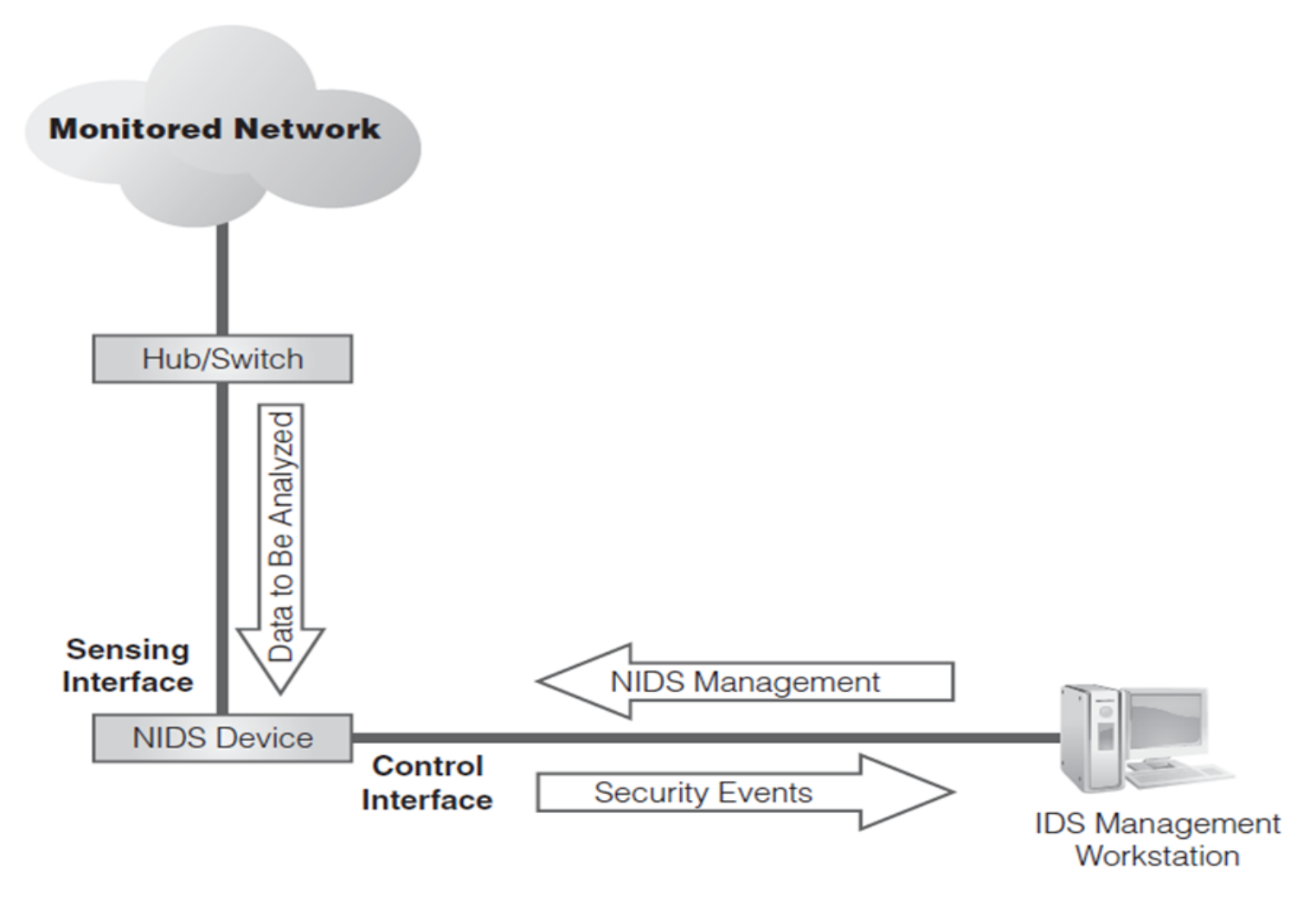
Types of Log Information



IDS as a Firewall Complement



Basic NIDS as a Firewall Complement



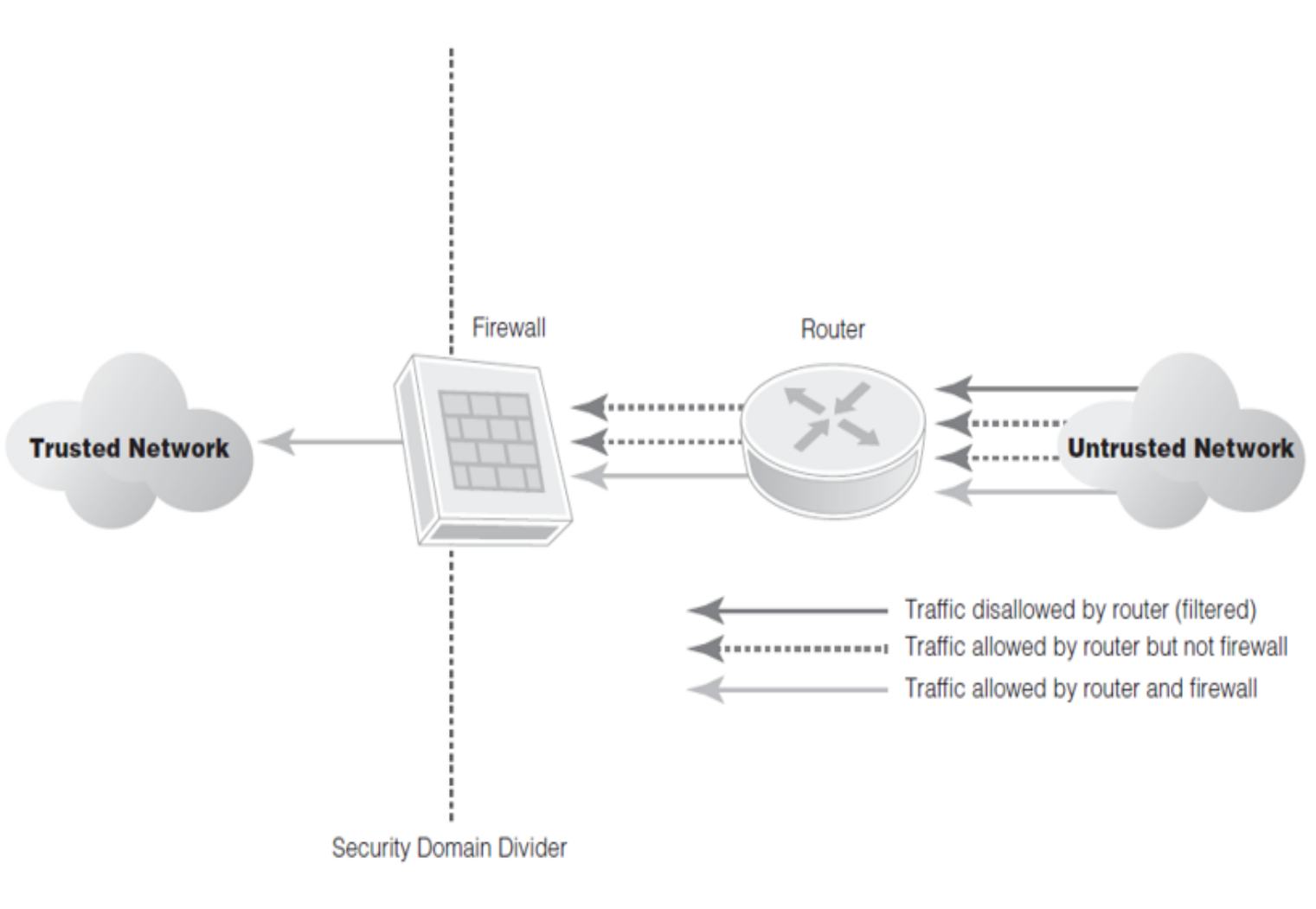
Analysis Methods

Pattern- or signature-based IDSs
- Rule-based detection
- Rely on pattern matching and stateful matching

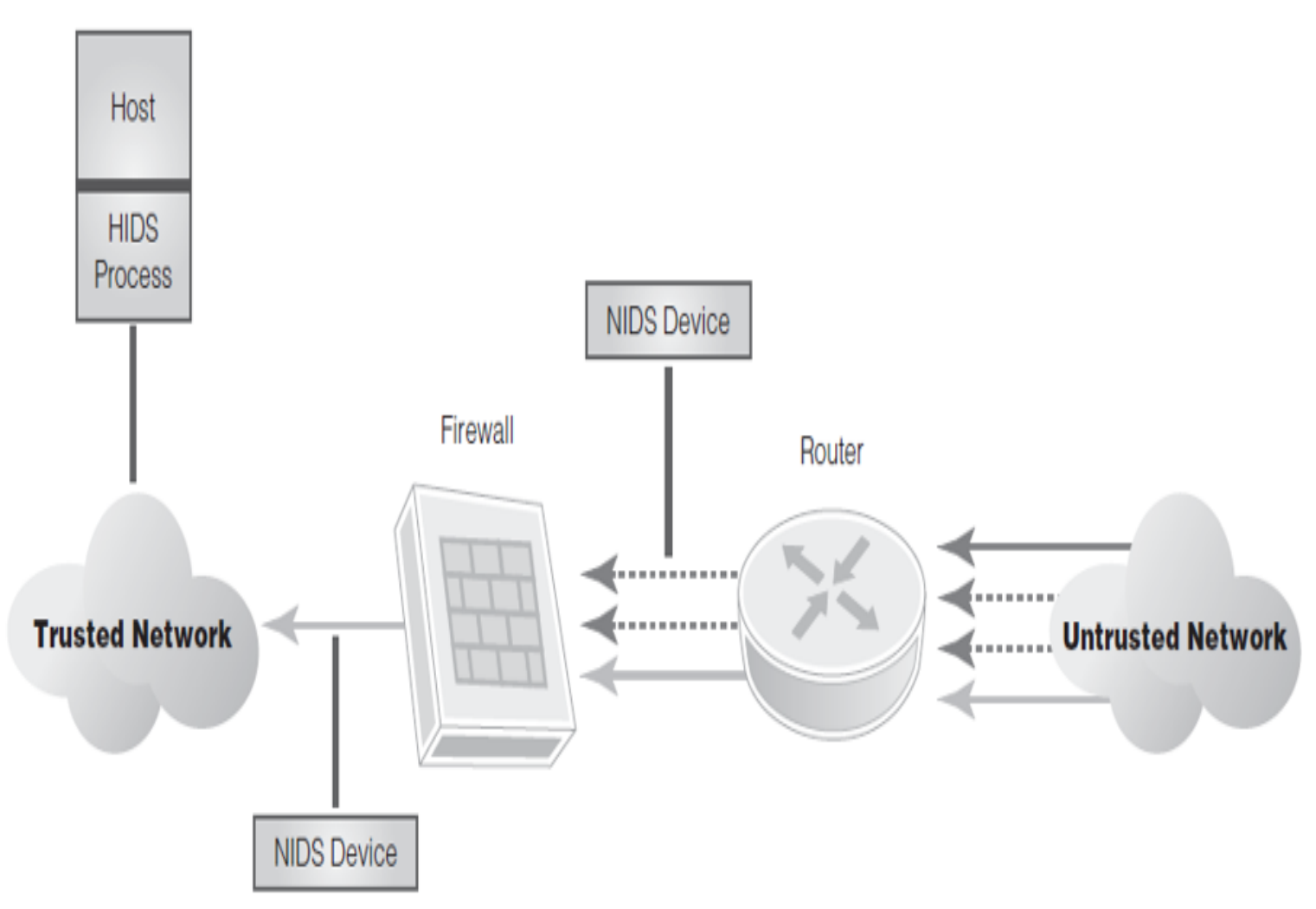
Anomaly-based IDSs
- Profile-based systems

Common methods of detecting anomalies
- Statistical-based methods
- Traffic-based methods
- Protocol patterns

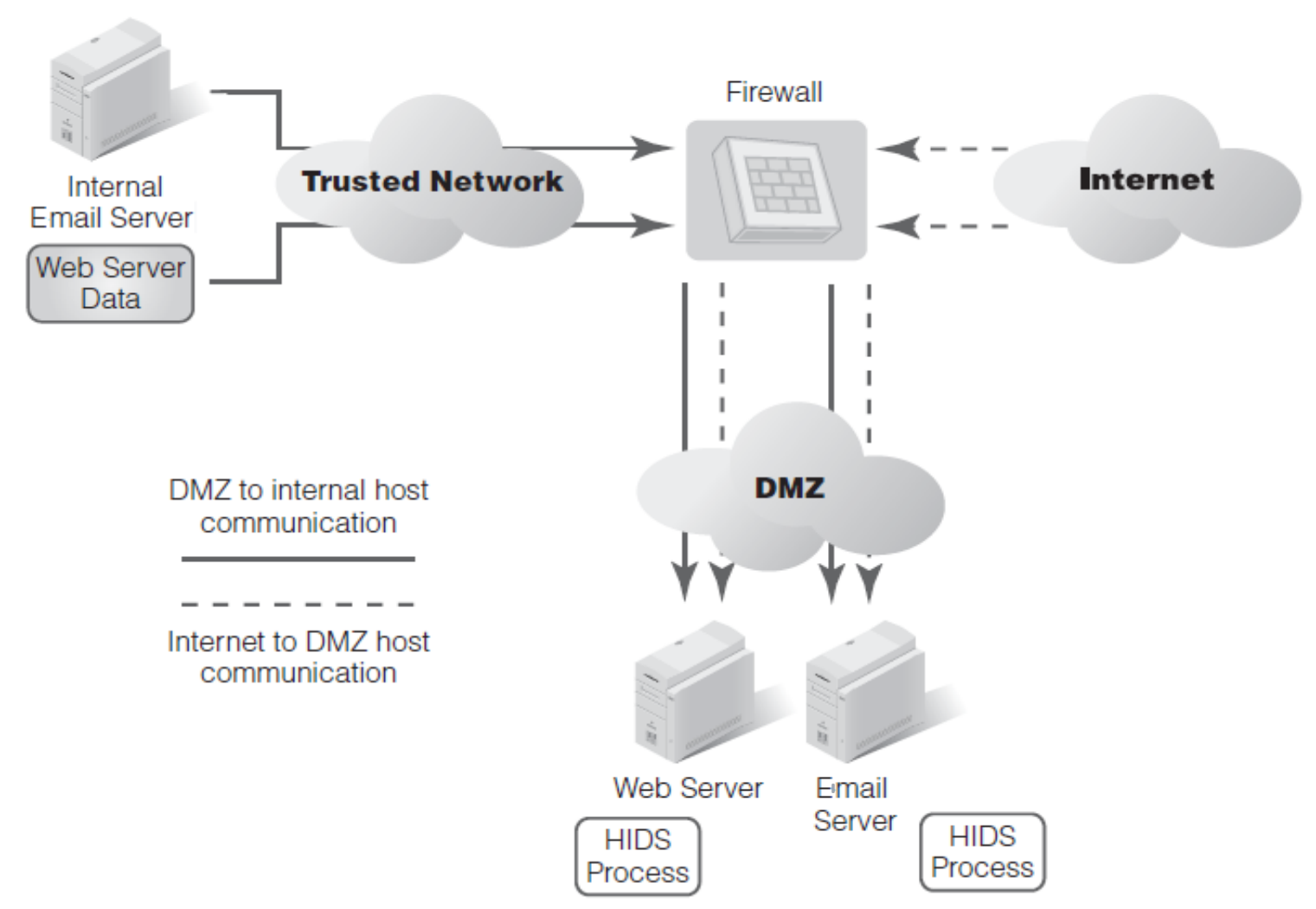
Layered Defense: Network Access Control



Using NIDS Devices to Monitor Outside Attacks



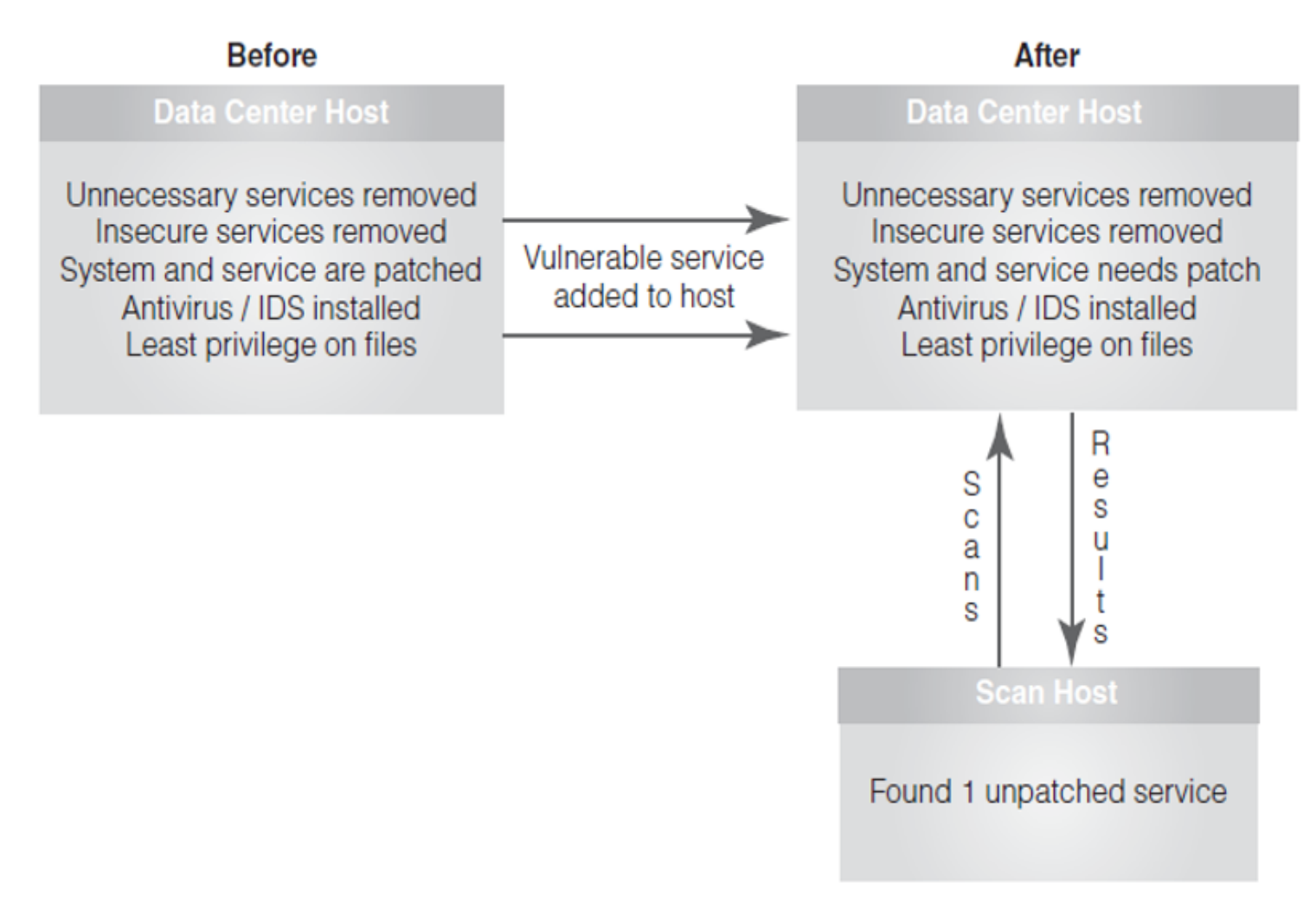
Host Isolation and the DMZ



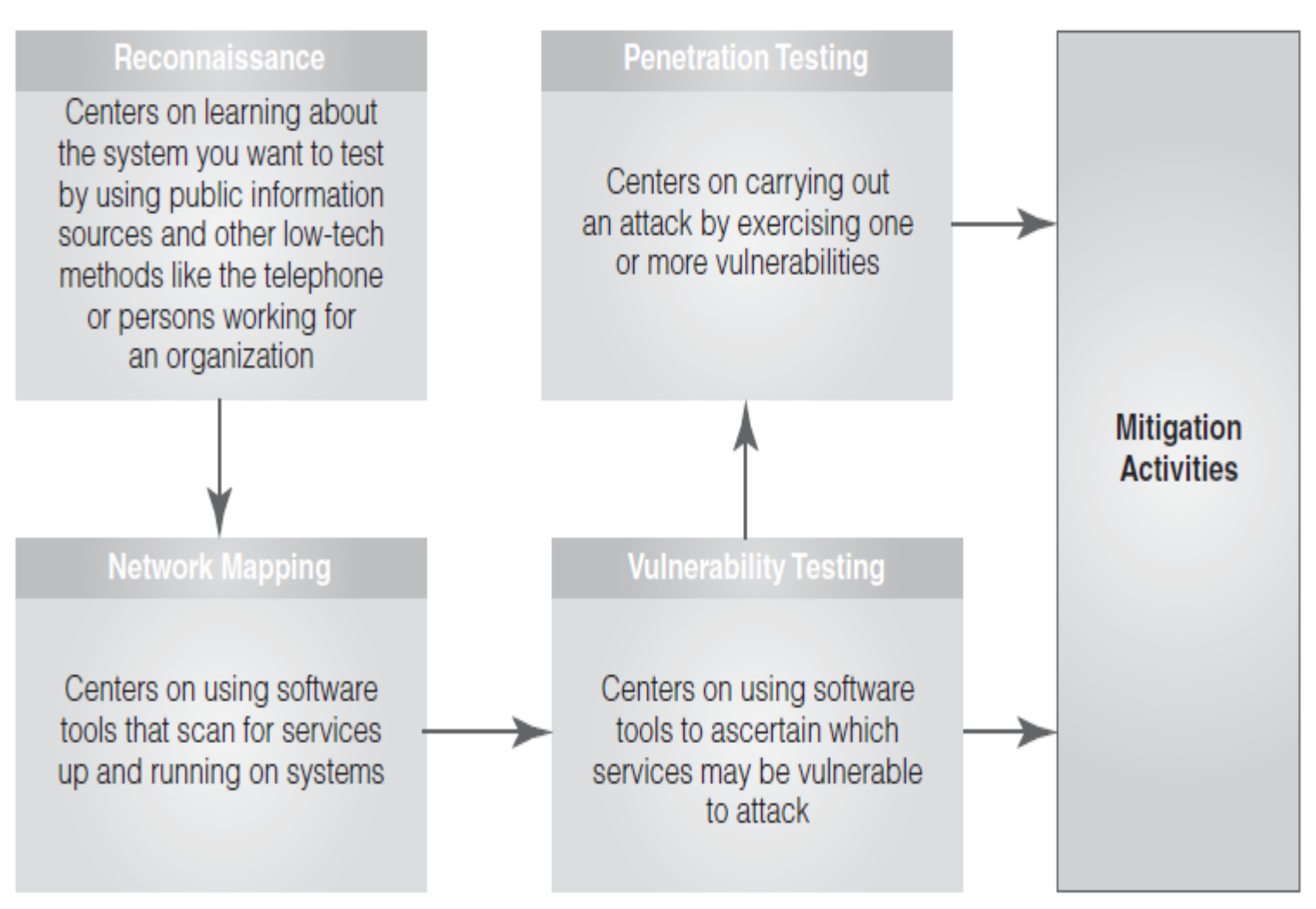
System Hardening

- Turn off or disable unnecessary services; protect ones that are still running
- Secure management interfaces and applications
- Protect passwords through aggressive password policies
- Disable unnecessary user accounts
- Apply the latest software patches available
- Secure all computers/devices from unauthorized changes
- Disable unused network interfaces
- Disable unused application service ports
- Use MAC filtering to limit device access
- Implement 802.1x, PNAC

Testing


Before
Data Center Host
Unnecessary services removed
Insecure services removed
System and service are patched
Antivirus / IDS installed
Least privilege on files
Vulnerable service added to host
After
Data Center Host
Unnecessary services removed
Insecure services removed
System and service needs patch
Antivirus / IDS installed
Least privilege on files
Scans
Results
Scan Host
Found 1 unpatched service

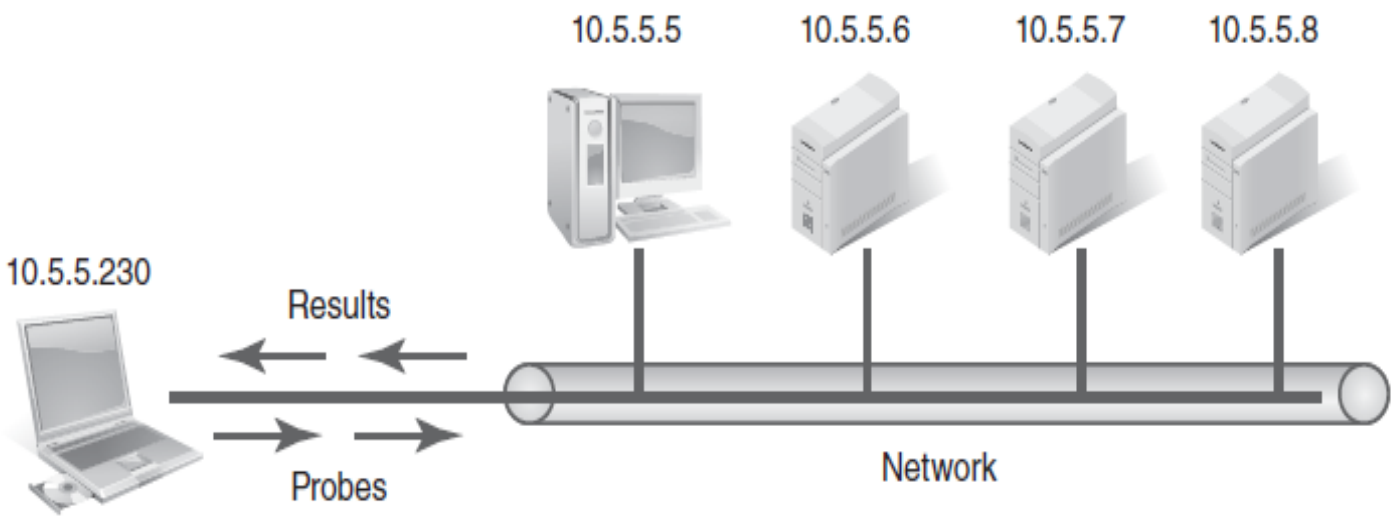
Security Testing Road Map



Establishing Testing Goals and Reconnaissance Methods

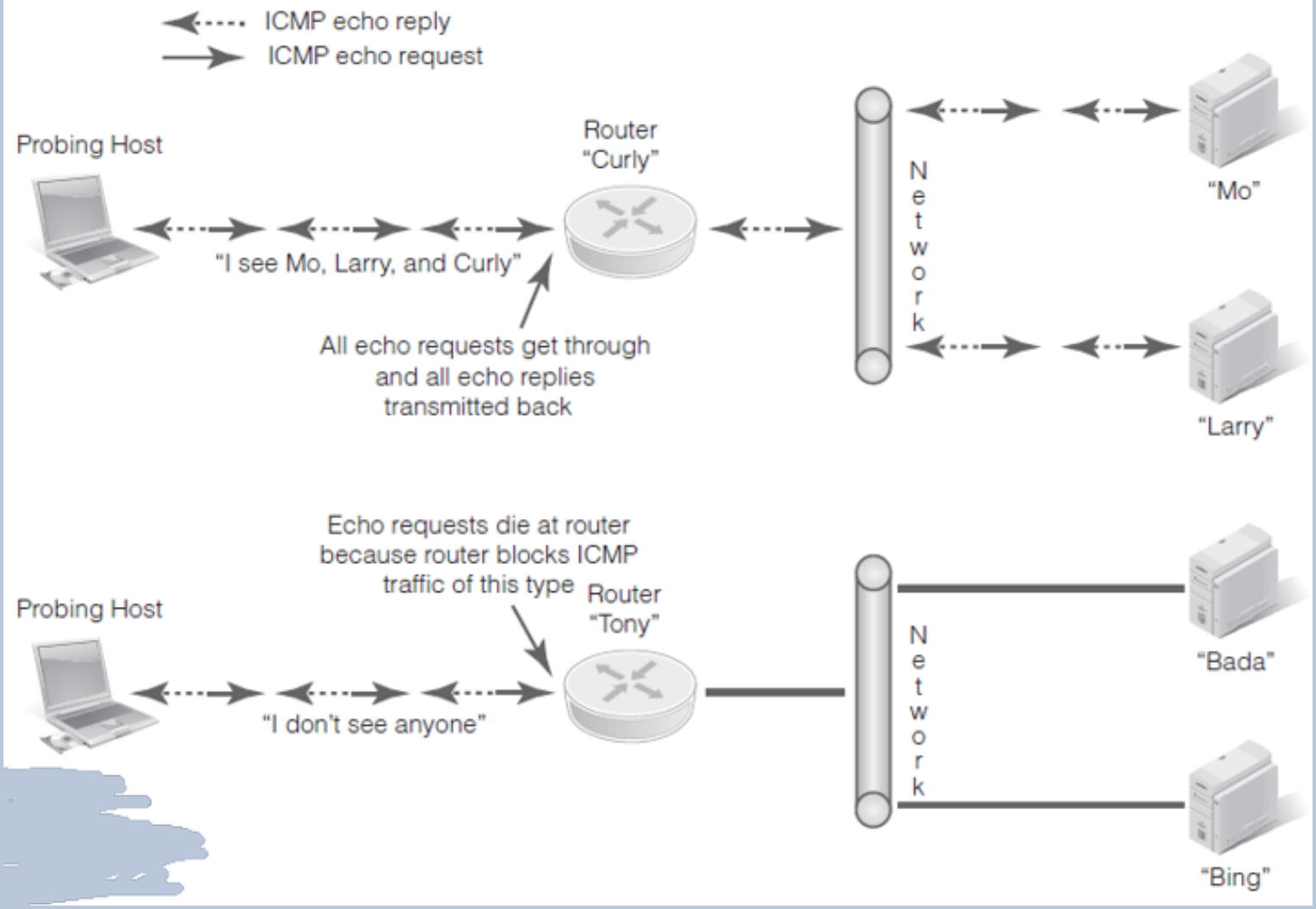
- Establish testing goals
  - Identify vulnerabilities and rank them according to how critical they are to your systems
  - Document a point-in-time (snapshot) test for comparison to other time periods
  - Prepare for auditor review
  - Find the gaps in your security
- Reconnaissance methods
  - Social engineering
  - Whois service
  - Zone transfer

Network Mapping

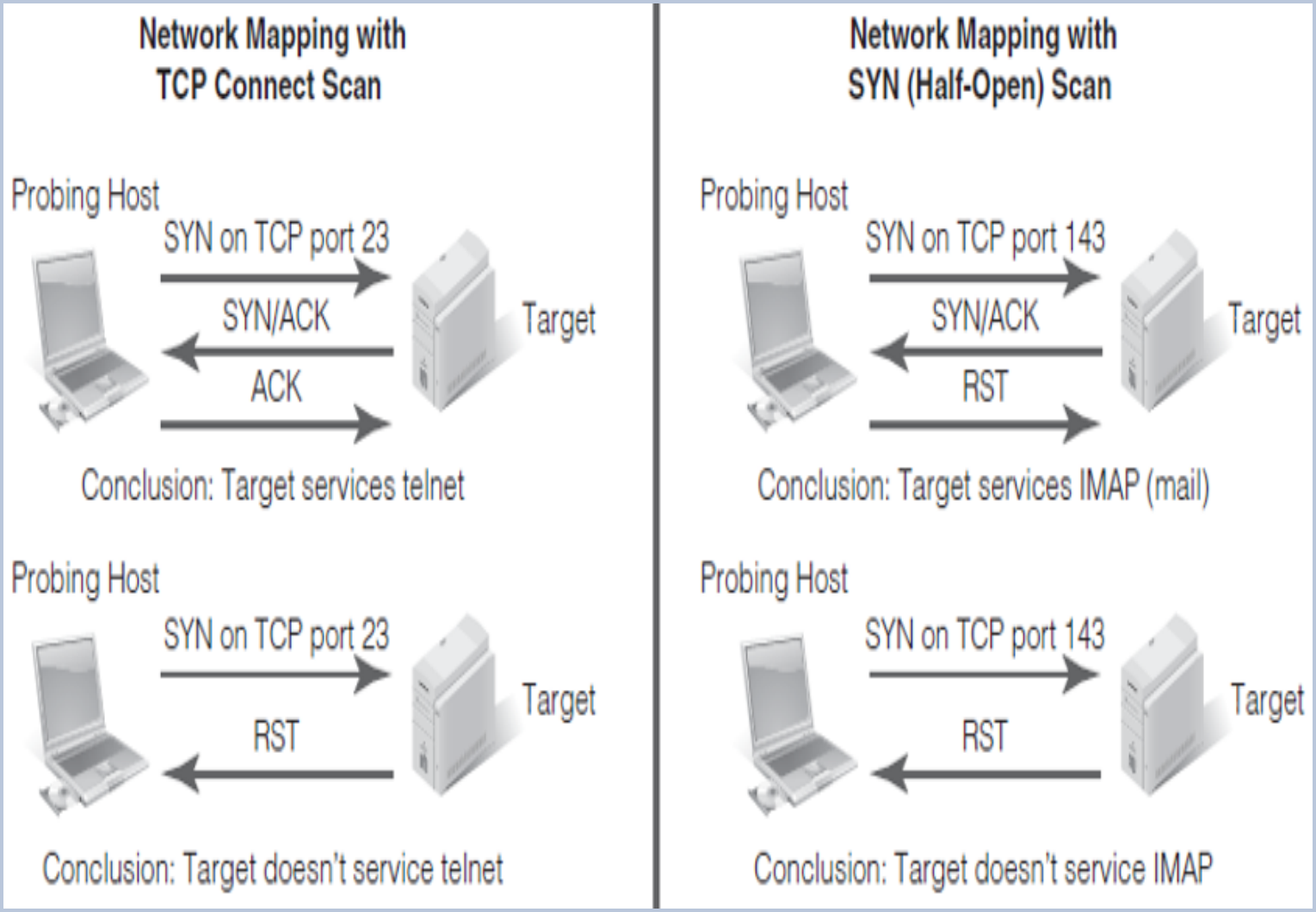


Host Name	IP	Services	OS
user-5	10.5.5.5	http, netbios,ftp	Windows Server 2008
server-6	10.5.5.6	http, netbios	Windows Server 2012
server-7	10.5.5.7	telnet, smtp	Linux
server-8	10.5.5.8	dns, finger, telnet	Solaris

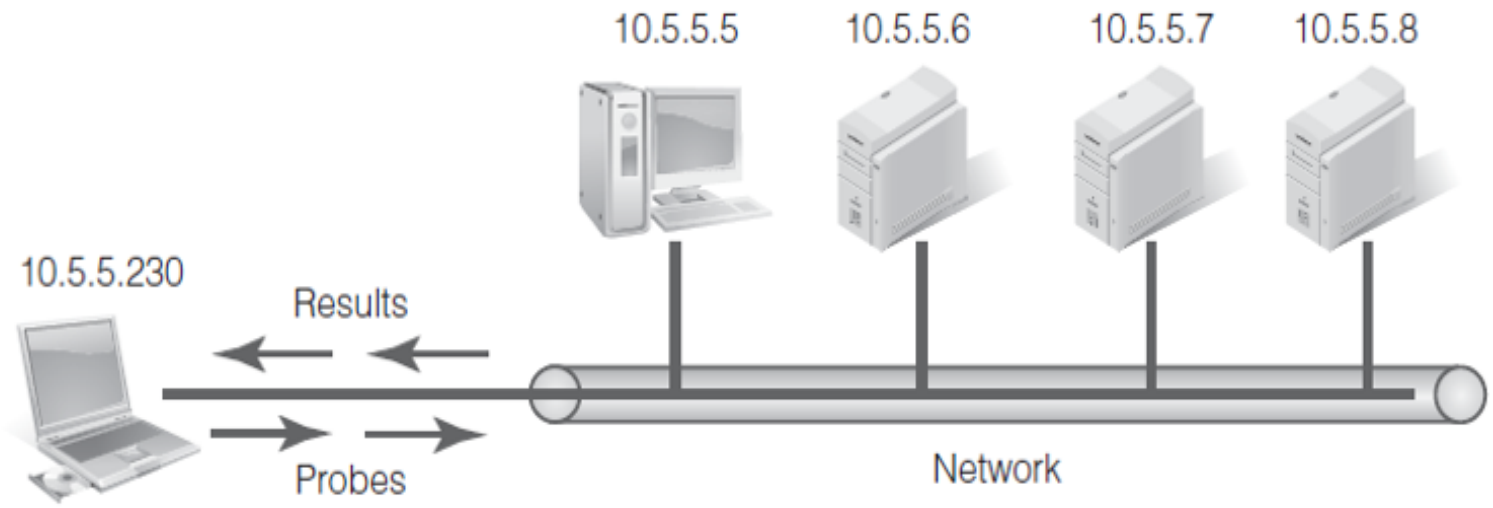
Network Mapping with ICMP (Ping)



Network Mapping with TCP/SYN Scans



Operating System Fingerprinting



What port mappers "think":

- 10.5.5.5 looks like Windows Server 2003 based on the way its TCP/IP communications are structured....
- 10.5.5.6 looks like Windows Server 2008 because it did not respond with an RST when I sent a FIN and it runs IIS 5 according to the http banner....
- 10.5.5.7 looks like Linux because it did send back an RST in response to my FIN and its TCP/IP communications behave like Linux....

Testing Methods

Black-box testing

- Uses test methods that aren't based directly on knowledge of a program's architecture or design

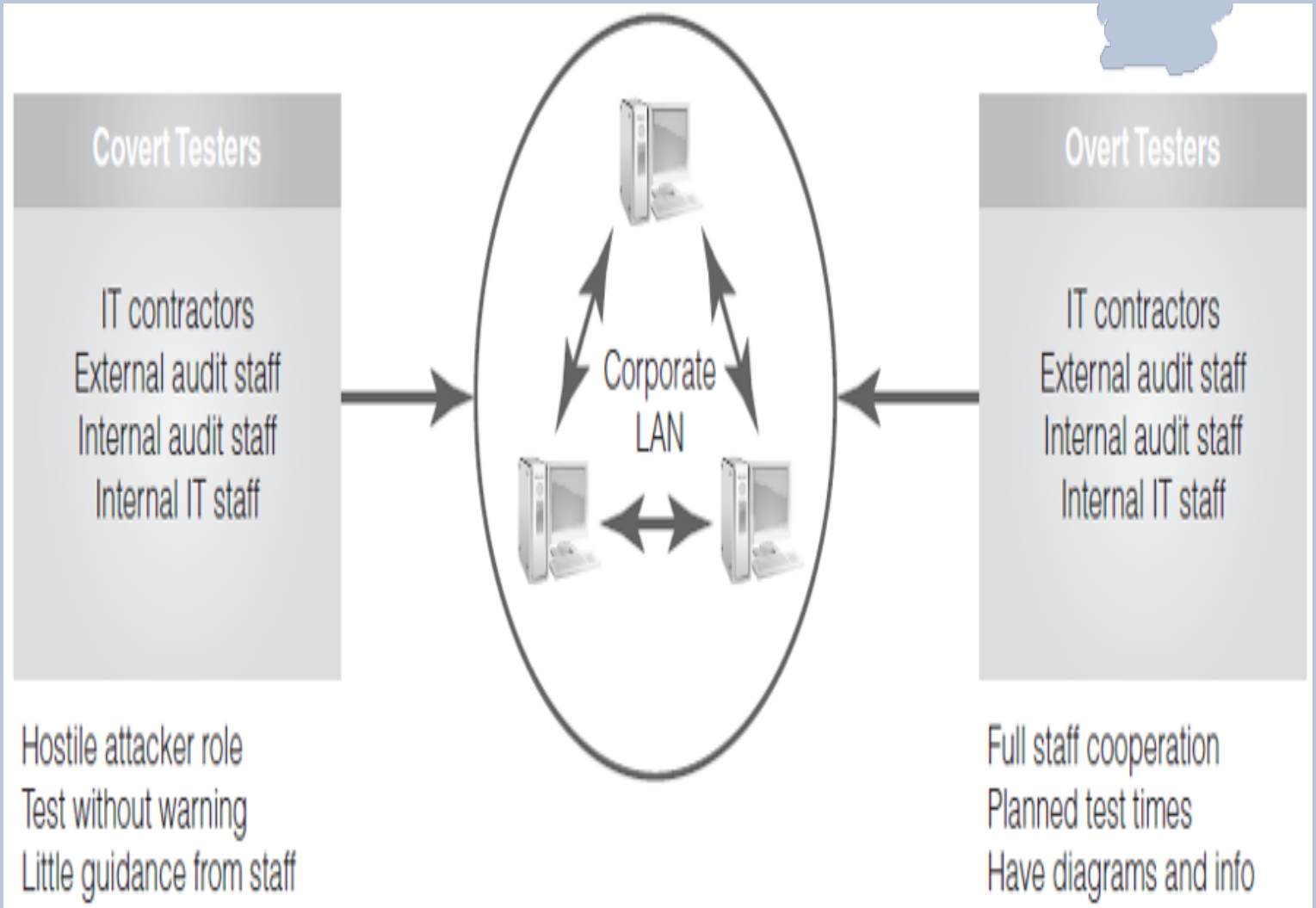
White-box testing

- Is based on knowledge of the application's design and source code

Gray-box testing

- Lies somewhere between black-box testing and white-box testing

Covert versus Overt Testers



Security Testing Tips and Techniques

- Choose the right tool
- Tools make mistakes
- Protect your systems
- Tests should be as “real” as possible

Honeypots

- Decoy systems designed to:
  - Lure a potential attacker away from critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to respond
  - Systems are filled with fabricated information that a legitimate user of the system wouldn't access
  - Resources that have no production value
  - Therefore incoming communication is most likely a probe, scan, or attack
  - Initiated outbound communication suggests that the system has probably been compromised

Honeypot Classifications

- Low interaction honeypot
- Consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems
- Provides a less realistic target
- Often sufficient for use as a component of a distributed IDS to warn of imminent attack
- High interaction honeypot
- A real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers
- Is a more realistic target that may occupy an attacker for an extended period

Honeypot example

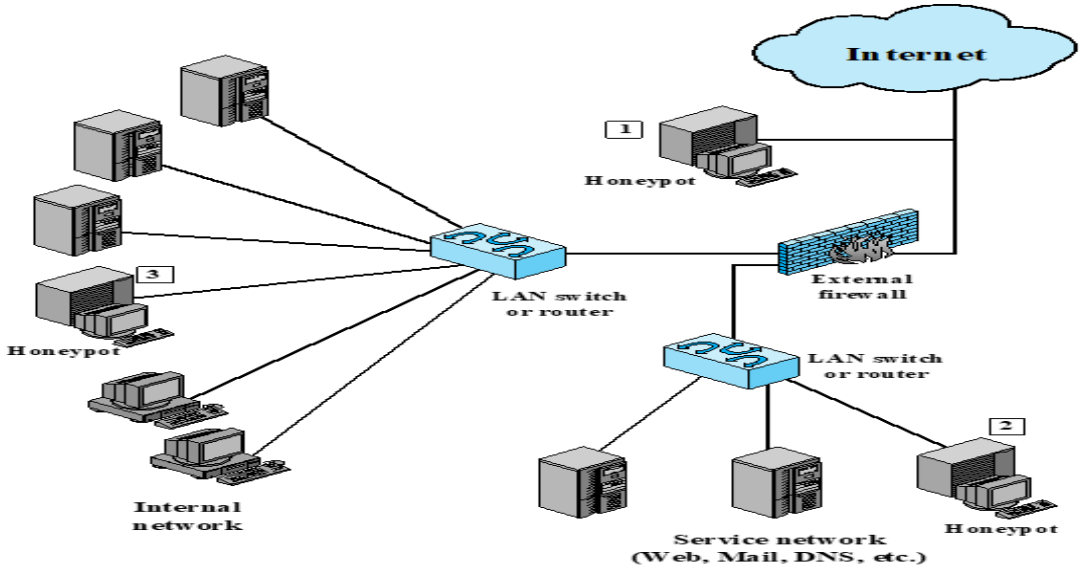


Figure 8.8 Example of Honeypot Deployment

Summary

- Practices and principles of security audits
- Ways to monitor systems
- Capturing and analyzing log data
- Assessing an organization's security compliance
- Monitoring and testing security systems