Information Security (CP3404)

Chapter 15 – Vulnerability Assessment

Based on the Fifth Edition of:

M. Ciampa:. *CompTIA® Security + Guide to Network Security Fundamentals*

Department of Information Technology, College of Business, Law & Governance

Learning Objectives

- Define vulnerability assessment and explain why it is important
- Explain the differences between vulnerability scanning and penetration testing
- Describe the security implications of integration with third parties
- List techniques for mitigating and deterring attacks

Outline

1. Assessing Vulnerabilities
2. Vulnerability Scanning vs. Penetration Testing
3. Third-Party Integration
4. Mitigating and Deterring Attacks

Preface

- Exactly how vulnerable are we?
- it is a fact that *all* computer systems, and the information contained on those systems, are vulnerable to attack
- Successful attacks are inevitable, organizations must protect themselves by:
  - Realistically evaluating their vulnerabilities
  - Assessing how an attacker could penetrate their defenses
  - Taking proactive steps to defend against those attacks

Assessing Vulnerabilities

Assessing Vulnerabilities — What is Vulnerability assessment

- First step any security protection plan begins with assessment of vulnerabilities
- Vulnerability assessment – Systematic and methodical evaluation of exposure of assets to attackers, forces of nature, and any other entity that could cause potential harm
- Variety of techniques and tools can be used in evaluating the levels of vulnerability

Assessing Vulnerabilities

Assessing Vulnerabilities — What is Vulnerability Assessment

- Vulnerability assessment involves:
  - Identify what needs to be protected (asset identification)
  - What pressures are against those assets (threat evaluation)
  - How susceptible current protection is (vulnerability appraisal)
  - What damages could result from the threats (risk assessment)
  - Analysis of what to do about it (risk mitigation)

Assessing Vulnerabilities

Vulnerability Assessment — Asset Identification

- Asset identification – Process of inventorying items with economic value
- Common assets:
  - People (e.g., employees, customers, contractors, vendors)
  - Physical assets (e.g., buildings, automobiles)
  - Data (e.g., employee databases, inventory records)
  - Hardware (e.g., computers, servers, networking equipment)
  - Software (e.g., application programs, operating systems)

Assessing Vulnerabilities

Vulnerability Assessment — Asset Identification

- After an inventory of the assets has been taken important to determine each item's relative value.
- Value based on:
  - Asset's criticality to organization's goals
  - How much revenue asset generates
  - How difficult to replace asset
  - Impact of asset unavailability to the organization
  - Can rank using a number scale

Assessing Vulnerabilities

Vulnerability Assessment — Threat Evaluation

- After asset identification, the next step is to determine the potential threats against the assets
- Threat evaluation – List potential threats from threat agent (an entity with the power to carry out a threat against an asset)
- Threat agents are not limited to attackers, but also include natural disasters, such as fire or severe weather (see Table 15-1)

Assessing Vulnerabilities

Category of threat	Example
Natural disasters	Fire, flood, or earthquake destroys data
Compromise of intellectual property	Software is pirated or copyright infringed
Espionage	Spy steals production schedule
Extortion	Mail clerk is blackmailed into intercepting letters
Hardware failure or errors	Firewall blocks all network traffic
Human error	Employee drops laptop computer in parking lot
Sabotage or vandalism	Attacker implants worm that erases files
Software attacks	Virus, worm, or denial of service compromises hardware or software
Software failure or errors	Bug prevents program from properly loading
Technical obsolescence	Program does not function under new version of operating system
Theft	Desktop system is stolen from unlocked room
Utility interruption	Electrical power is cut off

Table 15-1 Common threat agents

Assessing Vulnerabilities

Vulnerability Assessment — Threat Evaluation

- Threat modeling – Goal of understanding attackers and their methods
- Attack tree – Provides visual representation of potential attacks as inverted tree structure
- Attack tree displays
  - Goal of attack
  - Types of attacks that could occur
  - Techniques used in attacks

See partial attack trees of Figures 15-1 and 15-2

Assessing Vulnerabilities

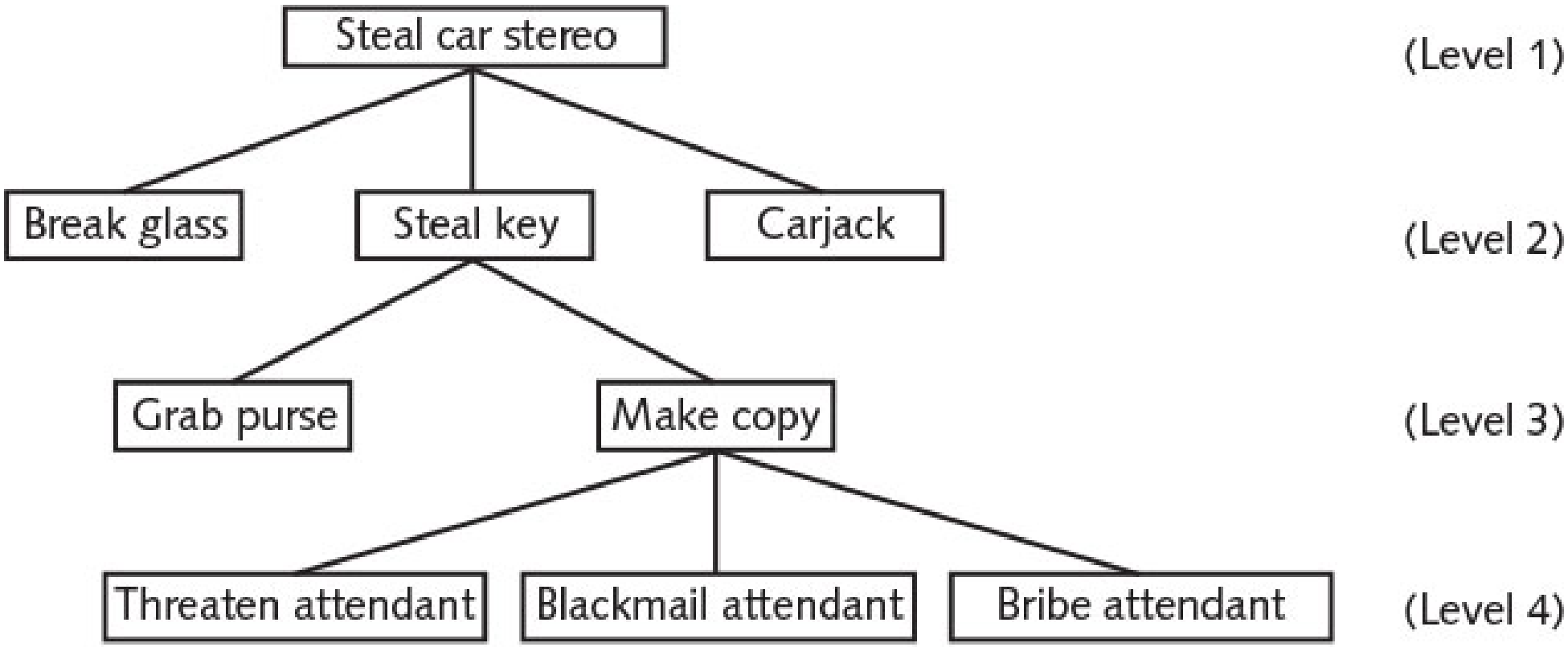

Figure 15-1 Attack tree for stealing a car stereo

Assessing Vulnerabilities

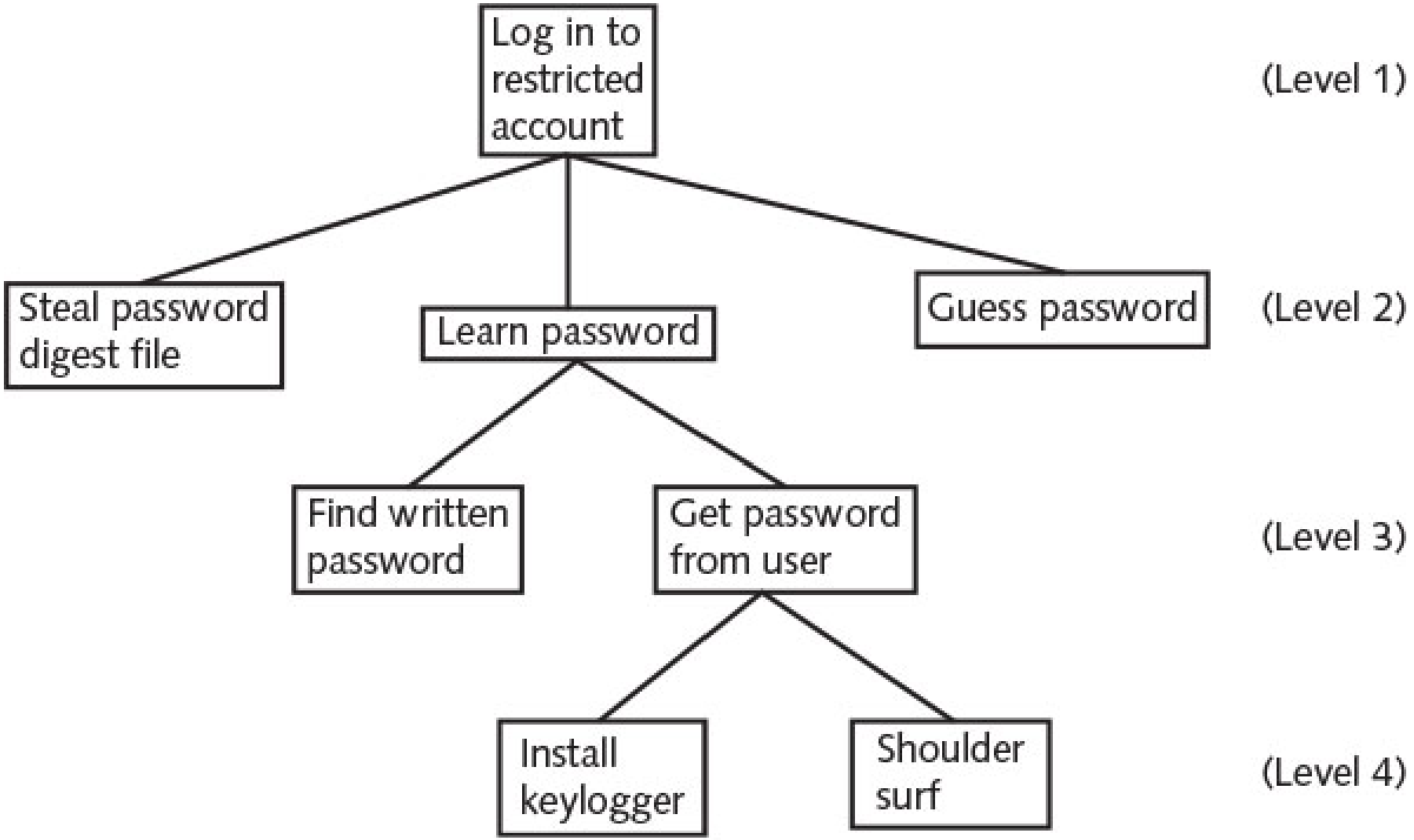

Figure 15-2 Attack tree for logging into restricted account

Assessing Vulnerabilities

Vulnerability Assessment — Vulnerability Appraisal

- Vulnerability appraisal – Determine current weaknesses as snapshot of current organization security
- Every asset should be viewed in light of each threat
- Catalog each vulnerability

Assessing Vulnerabilities

Vulnerability Assessment — Risk Assessment

- Risk Assessment – Determine damage resulting from attack and assess likelihood that vulnerability is risk to organization
- Requires realistic look at several different types of attacks that might occur
- Based upon vulnerabilities recognized in vulnerability appraisal, a risk assessment of impact can then be undertaken
- Not all vulnerabilities pose the same risk (see Table 15-2)

Assessing Vulnerabilities

Impact	Description	Example
No impact	This vulnerability would not affect the organization.	The theft of a mouse attached to a desktop computer would not affect the operations of the organization.
Small impact	Small impact vulnerabilities would produce limited periods of inconvenience and possibly result in changes to a procedure.	A specific brand and type of hard disk drive that fails might require that spare drives be made available and that devices with those drives be periodically tested.
Significant	A vulnerability that results in a loss of employee productivity due to downtime or causes a capital outlay to alleviate it could be considered significant.	Malware that is injected into the network could be classified as a significant vulnerability.
Major	Major vulnerabilities are those that have a considerable negative impact on revenue.	The theft of the latest product research and development data through a backdoor could be considered a major vulnerability.
Catastrophic	Vulnerabilities that are ranked as catastrophic are events that would cause the organization to cease functioning or be seriously crippled in its capacity to perform.	A tornado that destroys an office building and all of the company's data could be a catastrophic vulnerability.

Table 15-2 Vulnerability impact scale

Assessing Vulnerabilities

Vulnerability Assessment — Risk Mitigation

- Risk mitigation – Determine what to do about risks
- Risk can never be entirely eliminated; would cost too much or take too long
- Some risks must be accepted by default and degree of risk must always be assumed
- Question is not, *How can we eliminate all risk?* but *How much acceptable risk can we tolerate?*
- Once toleration level is known, steps can be taken to mitigate risk

Table 15-3 summarizes vulnerability assessments steps

Assessing Vulnerabilities

Vulnerability assessment action	Steps
1. Asset identification	a. Inventory the assets b. Determine the assets' relative value
2. Threat identification	a. Classify threats by category b. Design attack tree
3. Vulnerability appraisal	a. Determine current weaknesses in protecting assets b. Use vulnerability assessment tools
4. Risk assessment	a. Estimate impact of vulnerability on organization b. Calculate risk likelihood and impact of the risk
5. Risk mitigation	a. Decide what to do with the risk

Table 15-3 Vulnerability assessment actions and steps

Assessing Vulnerabilities

Assessment Techniques

- Several techniques can be used in vulnerability assessment
- Two (2) common techniques are:
  1. Baseline Reporting
  2. Software Program development

Assessing Vulnerabilities

Assessment Techniques — Baseline Reporting

- Baseline – Imaginary line by which an element is measured or compared; can be seen as standard
- IT baseline is checklist against which systems can be evaluated and audited for security posture
- Outlines major security considerations for system and becomes the starting point for solid security
- Baseline reporting – Comparison of present state of system to its baseline
- Deviations include not only technical issues but also management and operational issues

Assessing Vulnerabilities

Assessment Techniques — Software Program Development

- Important for software vulnerabilities be minimized while software being developed instead of after released
- Software improvement to minimize vulnerabilities is difficult:
  - Size and complexity – Millions of lines of code
  - Lack of formal specifications – The work on one programmer may unintentionally open a security vulnerability that was closed by another programmer
  - Ever-changing attacks – A code written today could be vulnerable tomorrow

Assessing Vulnerabilities

Assessment Techniques — Software Program Development

- Different assessment techniques to minimize vulnerabilities:
  - Requirements – List of features needed along with guidelines for maintaining quality
  - Design – Analysis of design of software program conducted by personnel from different levels of project
  - Implementation – Presenting code to multiple reviewers to reach agreement about its security
  - Verification – Errors identified and corrected
  - Release – Software shipped
  - Support – As vulnerabilities uncovered necessary security updates are created and distributed (See Figure 15-3)

Assessing Vulnerabilities

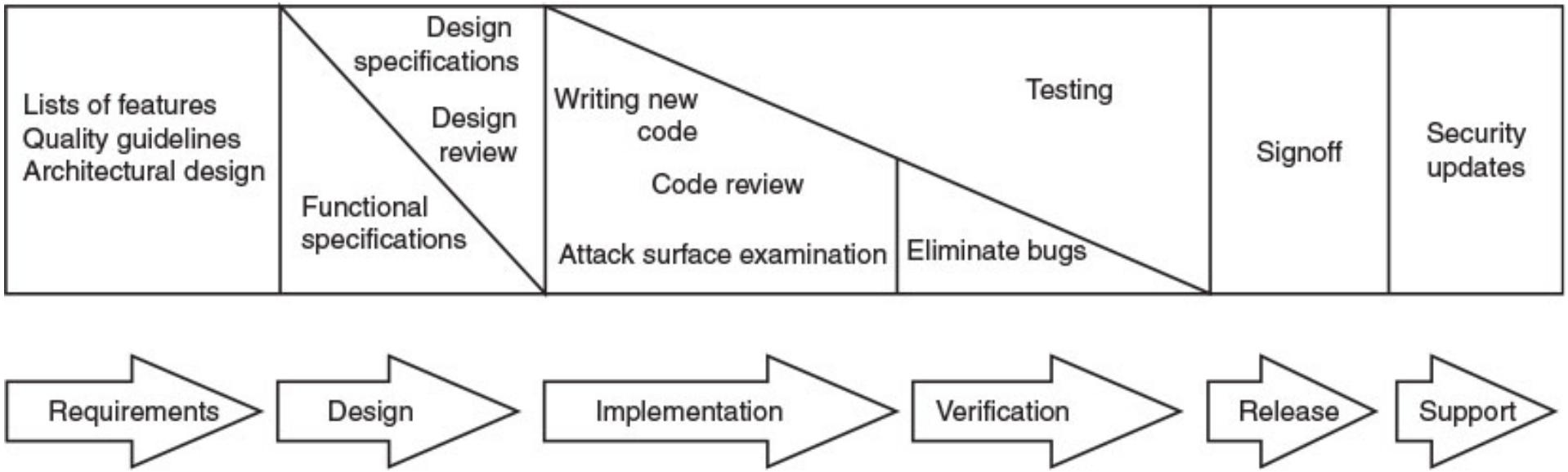

Figure 15-3 Software development process

Assessing Vulnerabilities

Assessment Tools

- Many tools available to perform vulnerability assessments:
  - Port Scanners
  - Banner Grabbing Tools
  - Protocol Analyzers
  - Vulnerability Scanners
  - Honeypots and Honeynets
- These tools can likewise used by attackers to uncover vulnerabilities to be exploited

Assessing Vulnerabilities

Assessment Tools — Port Scanners

- TCP/IP networks exchange information between program running on one system (process) and same/corresponding process running on remote system
- Port number – TCP/IP numeric value as identifier to applications and services on systems
- Each packet/datagram contains source port and destination port
- Identifies both originating application/service on local system and corresponding application/service on remote system

Assessing Vulnerabilities

Assessment Tools — Port Scanners (Cont.)

- Port numbers are 16 bit length so have decimal value 0-65,535
- TCP/IP divides port numbers into three (3) categories:
  1. Well-known port numbers (0 - 1023) – Reserved for most universal applications
  2. Registered port numbers (1024 - 49151) – Other applications that not as widely used
  3. Dynamic and private port numbers (49152 - 65535) – Available for use by any application
- A lsit of common protocols, communication protocols, and the service port numbers is provided in Table 15-4

Assessing Vulnerabilities

Protocol name	Communication protocol	Port number
File Transfer Protocol (FTP)—Data	TCP, UDP	20
File Transfer Protocol (FTP)—Commands	TCP	21
Secure Shell (SSH), Secure Shell File Transfer Protocol (SFTP), Secure Copy (SCP)	TCP, UDP	22
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name System (DNS)	TCP, UDP	53
Hypertext Transfer Protocol (HTTP)	TCP	80
Post Office Protocol v3 (POP3)	TCP	110
NetBIOS	TCP, UDP	139
Internet Message Access Protocol (IMAP)	TCP	143
Hypertext Transfer Protocol Secure (HTTPS)	TCP	443
Microsoft Terminal Server	TCP, UDP	3389

Table 15-4 Common protocols, communication protocols, and ports

Assessing Vulnerabilities

Assessment Tools — Port Scanners (Cont.)

- Because port numbers are associated with applications and services, if attacker knows specific port is accessible could indicate what services are being used
- Port security – Implement by disabling unused application/service ports to reduce number of threat vectors

Assessing Vulnerabilities

Assessment Tools — Port Scanners (Cont.)

- Port scanner – Software can be used to search system for port vulnerabilities (see Figure 15-4, and Table 15-5)
- Port scanners typically used determine state of port to know what applications/services are running
- There are three (3) port states:
  1. Open – Application/service assigned to port is listening for any instructions
  2. Closed – No process is listening at this port (host system will send back a reply that this service is unavailable)
  3. Blocked – Host system does not reply to any inquiries to this port number

Assessing Vulnerabilities

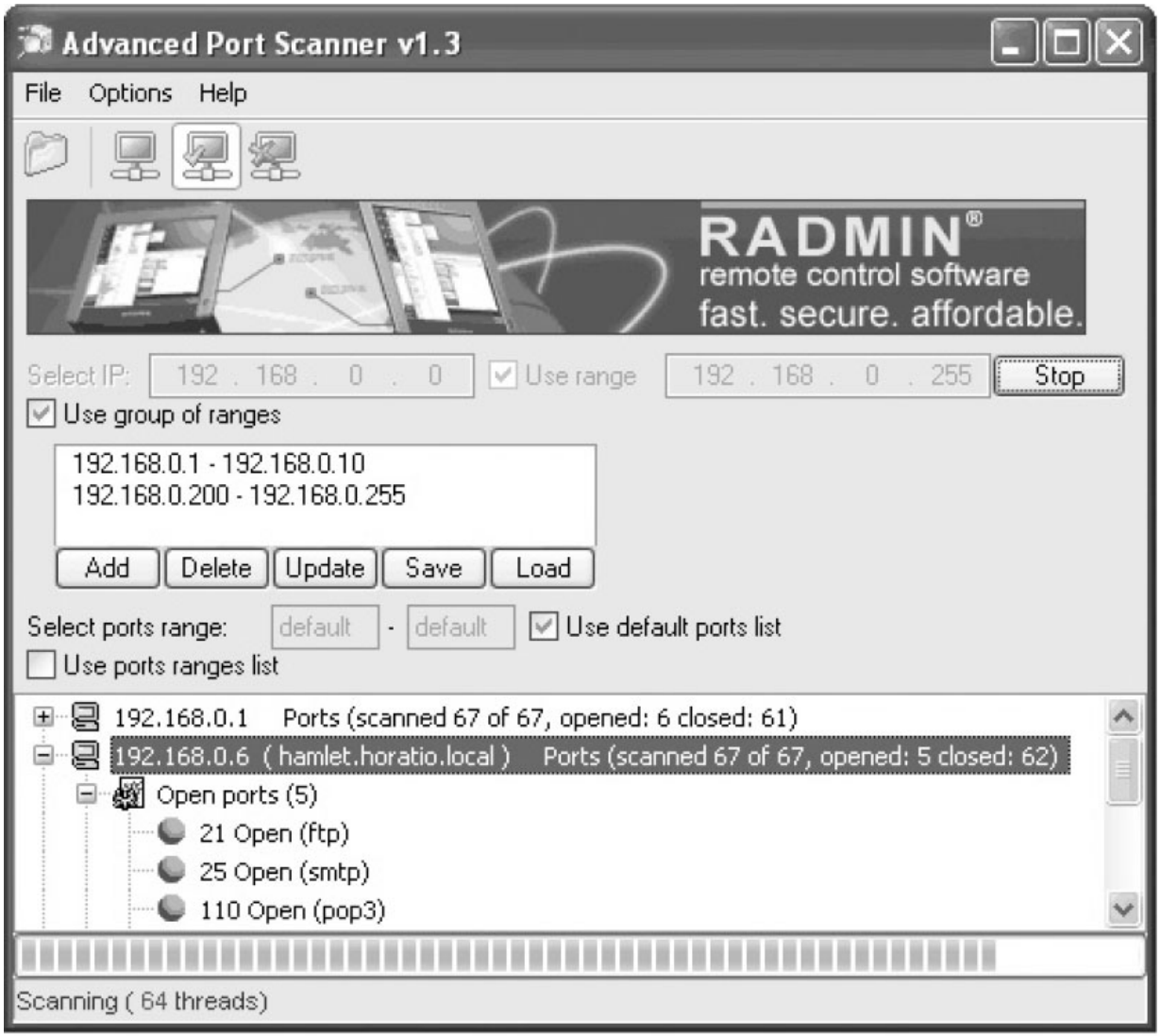

Figure 15-4 Port scanner

Source: RADMIN Advanced Port Scanner. Copyright © 1999–2014 Famatech. All rights reserved

Assessing Vulnerabilities

Name	Scanning process	Comments
TCP connect scanning	This scan attempts to connect to every available port. If a port is open, the operating system completes the TCP three-way "handshake" and the port scanner then closes the connection; otherwise an error code is returned.	There are no special privileges needed to run this scan. However, it is slow and the scanner can be identified.
TCP SYN scanning	Instead of using the operating system's network functions, the port scanner generates IP packets itself and monitors for responses. The port scanner generates a SYN packet, and if the target port is open, that port will respond with a SYN+ACK packet. The scanner host then closes the connection before the "handshake" is completed.	SYN scanning is the most popular form of TCP scanning because most sites do not log these attempts. This scan type is also known as "half-open scanning," because it never actually opens a full TCP connection.
TCP FIN scanning	The port scanner sends a finish (FIN) message without first sending a SYN packet. A closed port will reply but an open port will ignore the packet.	FIN messages as part of the normal negotiation process can pass through firewalls and avoid detection.
Xmas Tree port scan	An Xmas Tree packet is a packet with every option set to *on* for whatever protocol is in use. When used for scanning, the TCP header of an Xmas Tree packet has the flags finish (FIN), urgent (URG), and push (PSH) all set to *on*. By observing how a host responds to this "odd" packet, assumptions can be made about its operating system.	The term comes from the image of each option bit in a header packet being represented by a different-colored "light bulb." When all are turned on, it can be said that the packet "was lit up like a Christmas tree."

Table 15-5 Port scanning

Assessing Vulnerabilities

Assessment Tools — Banner Grabbing Tools

- Banner – Message that service transmits when another program connects to it
- Banner grabbing – When program used to intentionally gather this information
- Banner grabbing can be used as assessment tool to perform inventory on services and systems operating on server
- Can be done by using Telnet to create connection with host and then querying each port
- Attackers can also make use of banner grabbing when performing reconnaissance on a system

Assessing Vulnerabilities

Assessment Tools — Protocol Analyzers

- Protocol analyzers – Hardware or software that captures packets to decode and analyze contents (see Figure 15-5)
- Common uses for protocol analyzers (see Table 15-6):
  - Used by network administrators for troubleshooting
  - Characterizing network traffic
  - Security analysis

Assessing Vulnerabilities

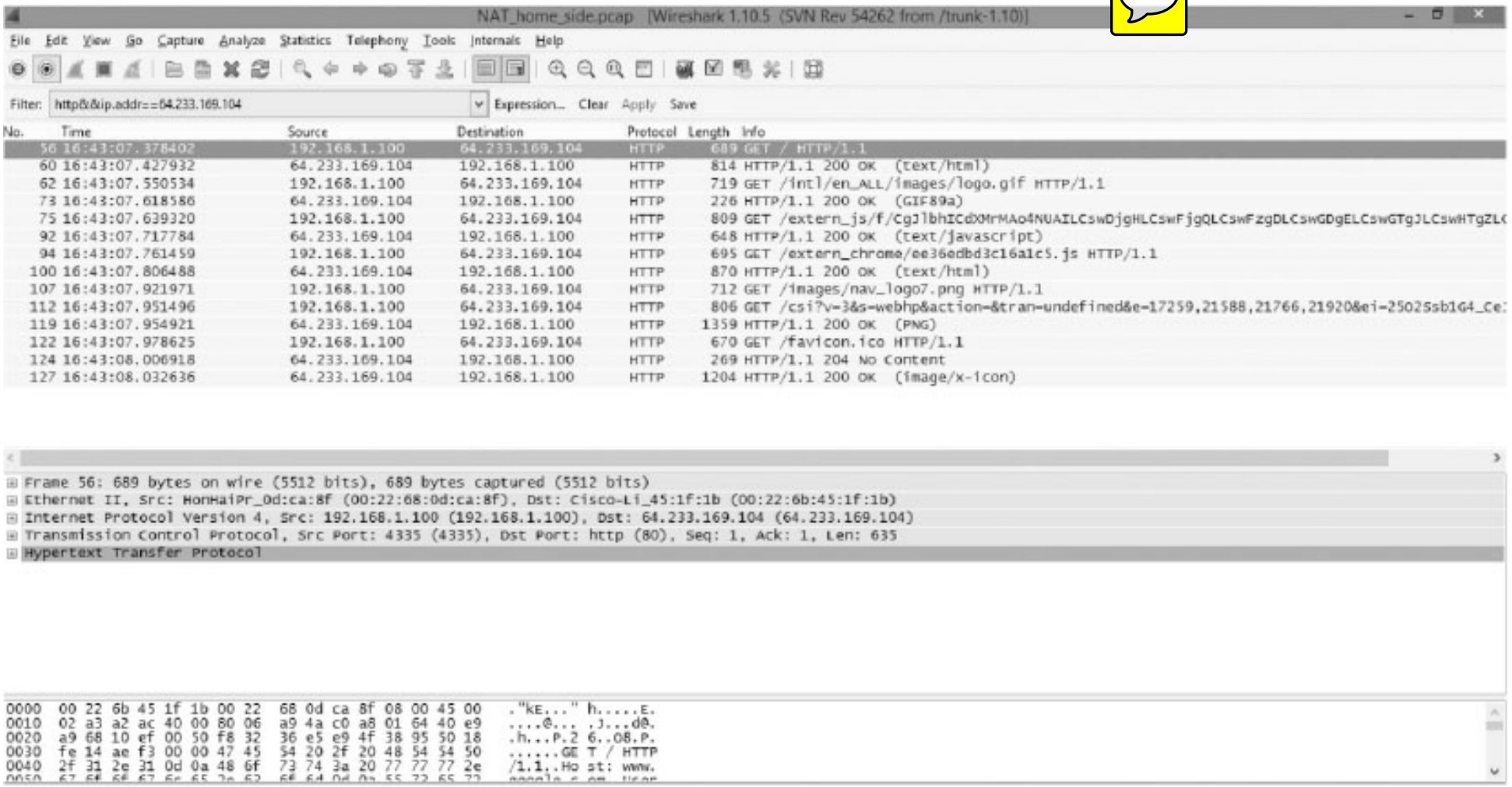

Figure 15-5 Protocol analyzer

Source: Wireshark Software

Assessing Vulnerabilities

Security information	Explanation
Unanticipated network traffic	Most network managers know the types of applications that they expect to see utilizing the network. Protocol analyzers can help reveal unexpected traffic and even pinpoint the computers that are involved.
Unnecessary network traffic	Network devices may by default run network protocols that are not required and may pose a security risk. As a precaution, a protocol analyzer can be set to filter traffic so it can help identify unnecessary network traffic and the source of it.
Unauthorized applications/services	Servers can be monitored to determine if they have open port numbers to support unauthorized applications/services. Many protocol analyzers allow filtering on specified port numbers, so it is possible to constantly monitor for specific port number requests.
Virus detection and control	A filter in the protocol analyzer can be set to watch for a known text pattern contained in a virus. The source and destination of the packets can then be used to identify the location of the virus.
Firewall monitoring	A misconfigured firewall can be detected by a protocol analyzer watching for specific inbound and outbound traffic.

Table 15-6 Protocol analyzer security information

Assessing Vulnerabilities

Assessment Tools — Vulnerability Scanners

- Vulnerability scanner – Generic term for range of products that look for vulnerabilities in networks or systems.
- Intended to identify vulnerabilities and alert network administrators to these problems (see Figure 15-6)
- Most vulnerability scanners maintain database that categorizes and describes vulnerabilities that it can detect

Assessing Vulnerabilities

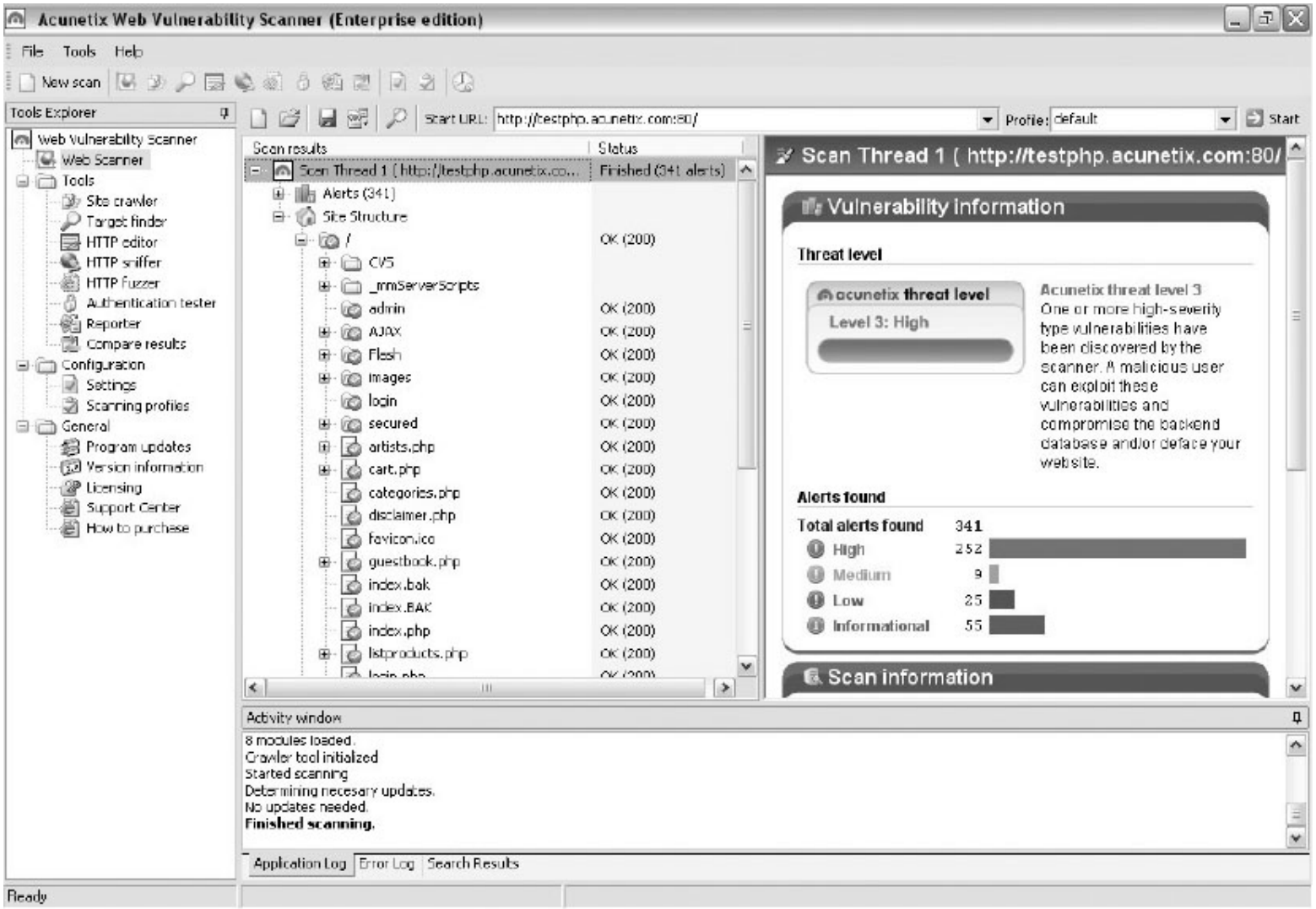

Figure 15-6 Vulnerability scanner

Source: Acunetix Software

Assessing Vulnerabilities

Assessment Tools — Vulnerability Scanners (Capabilities)

- Alert when new systems are added to network
- Detect when an application is compromised or subverted
- Detect when an internal system begins to port scan other systems
- Detect which ports are served and which ports are browsed for each individual system
- Identify which applications and servers host or transmit sensitive data
- Maintain log of all interactive network sessions

Assessing Vulnerabilities

Assessment Tools — Vulnerability Scanners

- Problem with assessment tools is no standard for collecting, analyzing, reporting vulnerabilities
- Open Vulnerability and Assessment Language (OVAL) – Designed to promote open and publicly available security content (see Figure 15-7)
- Standardizes information transfer across different security tools and services

Assessing Vulnerabilities

OVAL Results Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.10.1	jOVAL	5.10.1.1_Dev	2012-09-01	18:09:08

OVAL Definition Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.10	PSIRT OVAL Definition Generator	0.1	2012-09-01	20:26:10

System Information	
Host Name	R1
Operating System	Cisco IOS
Operating System Version	15.1(3)T
Architecture	unknown
Interfaces	Interface Name: FastEthernet0/0 IP Address: 172.18.122.246/26 MAC Address: 001d.a105.9cc8 Interface Name: FastEthernet0/1 IP Address: 14.4.1.126/24 MAC Address: 001d.a105.9cc9

OVAL System Characteristics Generator Information				
Schema Version	Product Name	Product Version	Date	Time
5.10.1	jOVAL	5.10.1.1_Dev	2012-09-01	18:09:08

OVAL Definition Results

☐ True ☐ False ☐ Error ☐ Unknown ☐ Not Applicable ☐ Not Evaluated

ID	Result	Class	Reference ID	Title
oval:cisco.oval:def:13	true	vulnerability	CVE-2012-0381cisco-sa-20120328-ike	cisco-sa-20120328-ike-CVE-2012-0381

Figure 15-7 OVAL output

Source: jOVAL Open Source Software

Assessing Vulnerabilities

Assessment Tools — Honeypots and Honeynets

- Honeypot – Computer protected by minimal security and intentionally configured with vulnerabilities and contains bogus data files
- Goal is trick attackers into revealing their techniques
- Honeynet – Network set up with intentional vulnerabilities and honeypots

Quick Quiz

1. The goal of _____ is to better understand who attackers are, why they attack, and what types of attacks might occur.
   Answer:

Quick Quiz

1. The goal of _____ is to better understand who attackers are, why they attack, and what types of attacks might occur.
   Answer: threat modeling

Quick Quiz

1. The goal of _____ is to better understand who attackers are, why they attack, and what types of attacks might occur.
   Answer: threat modeling

2. A _____ involves determining the damage that would result from an attack and the likelihood that the vulnerability is a risk to the organization.
   Answer:

Quick Quiz

1. The goal of _____ is to better understand who attackers are, why they attack, and what types of attacks might occur.
   Answer: threat modeling

2. A _____ involves determining the damage that would result from an attack and the likelihood that the vulnerability is a risk to the organization.
   Answer: risk assessment

Quick Quiz

1. The goal of _____ is to better understand who attackers are, why they attack, and what types of attacks might occur.
   Answer: threat modeling

2. A _____ involves determining the damage that would result from an attack and the likelihood that the vulnerability is a risk to the organization.
   Answer: risk assessment

3. A(n) _____ is a computer typically located in an area with limited security and loaded with software and data files that appear to be authentic, yet they are actually imitations of real data files.
   Answer:

Quick Quiz

1. The goal of _____ is to better understand who attackers are, why they attack, and what types of attacks might occur.
   Answer: threat modeling

2. A _____ involves determining the damage that would result from an attack and the likelihood that the vulnerability is a risk to the organization.
   Answer: risk assessment

3. A(n) _____ is a computer typically located in an area with limited security and loaded with software and data files that appear to be authentic, yet they are actually imitations of real data files.
   Answer: honeypot

Vulnerability Scanning vs. Penetration Testing

Vulnerability Scanning vs. Penetration Testing

- (2) Two important vulnerability assessment procedures are:
  1. Vulnerability Scanning
  2. Penetration Testing
- Similar and therefore often confused
- Both play an important role in uncovering vulnerabilities

Vulnerability Scanning vs. Penetration Testing

Vulnerability Scanning

- Vulnerability scan – Automated software searches a system for known security weaknesses
- Creates report of potential exposures
- Should be conducted on existing systems and as new technology is deployed
- Usually performed from inside security perimeter
- Does not interfere with normal network operations

Vulnerability Scanning vs. Penetration Testing

Vulnerability Scanning — Methods

- Intrusive vulnerability scan – Attempts to actually penetrate system in order to perform simulated attack (see Table 15-7)
- Non-intrusive vulnerability scan – Uses only available information to hypothesize status of the vulnerability
- Credentialed vulnerability scan – Scanners that permit username and password of active account to be stored and used
- Non-credentialed vulnerability scans – Scanners that do not use credentials

Vulnerability Scanning vs. Penetration Testing

Type of scan	Description	Advantages	Disadvantages
Intrusive vulnerability scanning	Vulnerability assessment tools use intrusive scripts to penetrate and attack.	By attacking a system in the same manner as an attacker would, more accurate results are achieved.	The system may be unavailable for normal use while the scan is being conducted. Also, it may disable security services for the duration of the attack.
Non-intrusive vulnerability scanning	Through social engineering and general reconnaissance efforts, information is gathered regarding the known vulnerabilities and weaknesses of the system.	Organizations can avoid any disruption of service or setting off alerts from IPS, IDS, and firewalls. These scans also mimic the same reconnaissance efforts used by attackers.	Time is needed for all the information to be analyzed so that the security status of the system based on the data can be determined.

Table 15-7 Intrusive and non-intrusive vulnerability scans

Vulnerability Scanning vs. Penetration Testing

Penetration Testing

- Penetration testing – Designed to exploit system weaknesses
- Relies on tester's skill, knowledge, cunning
- Usually conducted by independent contractor, i.e., white hat hackers or ethical attackers
- Tests usually conducted outside the security perimeter and may even disrupt network operations
- End result is penetration test report

Vulnerability Scanning vs. Penetration Testing

Penetration Testing — Techniques

- Black box test – Tester has no prior knowledge of network infrastructure
- White box test – Tester has in-depth knowledge of network and systems being tested
- Gray box test – Some limited information has been provided to the tester

Table 15-8 compares Vulnerability scanning and penetration testing features

Vulnerability Scanning vs. Penetration Testing

Feature	Vulnerability scan	Penetration test
Frequency	When new equipment is installed and at least once per month thereafter	Once per year
Goals	Reveal known vulnerabilities that have not yet been addressed	Discover unknown exposures to the normal business processes
Tester	In-house technician	Independent external consultant
Location	Performed from inside	Performed from outside
Disruption	Passive evaluation with no disruption	Active attack with potential disruption
Tools	Automated software	Knowledge and skills of tester
Cost	Low (approximately $1500 plus staff time)	High (approximately $12,500)
Report	Comprehensive comparison of current vulnerabilities compared to baseline	Short analysis of how the attack was successful and the damage to data
Value	Detects weaknesses in hardware or software	Preventive; reduces the organization's exposure

Table 15-8 Vulnerability scan and penetration test features

Third-Party Integration

Third-Party Integration

- Increasing number of organizations use third-party vendors to create partnerships
- Third-party integration – Risk of combining systems and data with outside entities, continues to grow
- On-boarding – Start-up relationship between partners
- Off-boarding – Termination of agreements

Third-Party Integration

Third-Party Integration —Risks

- On-boarding and off-boarding – How will entities combine their services without compromising their existing security defenses?
- Application and social media network sharing – How will different applications be shared between partners?
- Privacy and risk awareness – What happens if privacy policy of one of the partners is less restrictive than that of the other partner?
- Data considerations – Who owns data generated through the partnership and how data protected?

Third-Party Integration

Third-Party Integration —Interoperability Agreements

- Service Level Agreement (SLA) – Service contract between a vendor and a client
- Blanket Purchase Agreement (BPA) – Prearranged purchase or sale agreement between a government agency and a business
- Memorandum of Understanding (MOU) – Describes agreement between two or more parties
- Interconnection Security Agreement (ISA) – Agreement intended to minimize security risks for data transmitted across a network

Mitigating and Deterring Attacks

Mitigating and Deterring Attacks

- Standard techniques for mitigating and deterring attacks:
  - Creating a Security Posture
  - Selecting Appropriate Conntrols
  - Configuring Controls
  - Hardening
  - Reporting

Mitigating and Deterring Attacks

Mitigating and Deterring Attacks — Creating a Security Posture

- Security posture describes strategy regarding security
- Elements of security posture:
  - Initial baseline configuration – Standard security checklist against which systems are evaluated for a security posture
  - Continuous security monitoring – Continual observation of systems and networks through vulnerability scanning and penetration testing
  - Remediation – Address the vulnerabilities they are exploited by attackers

Mitigating and Deterring Attacks

Mitigating and Deterring Attacks — Selecting Appropriate Controls

- Selecting appropriate controls to use is key to mitigating and deterring attacks
- Many different controls can be used
- Common controls that are important to meet specific security goals (see Table 15-9)

Mitigating and Deterring Attacks

Security goal	Common controls
Confidentiality	Encryption, steganography, access controls
Integrity	Hashing, digital signatures, certificates, nonrepudiation tools
Availability	Redundancy, fault tolerance, patching
Safety	Fencing and lighting, locks, CCTV, escape plans and routes, safety drills

Table 15-9 Appropriate controls for different security goals

Mitigating and Deterring Attacks

Mitigating and Deterring Attacks — Configuring Controls

- Key to mitigating and deterring attacks is proper configuration and testing of the controls
- One category of controls is those either detect or prevent attacks
- Another example of configuring controls regards what occurs when a normal function is interrupted by failure: does safety take priority or does security?

Mitigating and Deterring Attacks

Mitigating and Deterring Attacks — Hardening

- Hardening – Eliminate as many security risks as possible
- Techniques to harden systems:
  - Protecting accounts with passwords
  - Disabling unnecessary accounts
  - Disabling unnecessary services
  - Protecting management interfaces and applications

Mitigating and Deterring Attacks

Mitigating and Deterring Attacks — Reporting

- Providing information regarding events that occur
- Alarms or alerts – Sound warning if specific situation is occurring (e.g., alert if too many failed password attempts)
- Reporting can provide information on trends
- Can indicate a serious impending situation (e.g., multiple user accounts experiencing multiple password attempts)

Quick Quiz

1. **True or False:** In a white box test, the tester has no prior knowledge of the network infrastructure that is being tested.
   Answer:

Quick Quiz

1. **True or False:** In a white box test, the tester has no prior knowledge of the network infrastructure that is being tested.
   Answer: False

Quick Quiz

1. **True or False:** In a white box test, the tester has no prior knowledge of the network infrastructure that is being tested.
   Answer: False

2. An agreement through which parties in a relationship can reach an understanding of their relationships and responsibilities is known as a(n) _____.
   Answer:

Quick Quiz

1. **True or False:** In a white box test, the tester has no prior knowledge of the network infrastructure that is being tested.
   Answer: False

2. An agreement through which parties in a relationship can reach an understanding of their relationships and responsibilities is known as a(n) _____.
   Answer: interoperability agreement

Quick Quiz

1. **True or False:** In a white box test, the tester has no prior knowledge of the network infrastructure that is being tested.
   Answer: False

2. An agreement through which parties in a relationship can reach an understanding of their relationships and responsibilities is known as a(n) _____.
   Answer: interoperability agreement

3. A(n) _____ is an approach, philosophy, or strategy regarding security.
   Answer:

Quick Quiz

1. **True or False:** In a white box test, the tester has no prior knowledge of the network infrastructure that is being tested.
   Answer: False

2. An agreement through which parties in a relationship can reach an understanding of their relationships and responsibilities is known as a(n) _____.
   Answer: interoperability agreement

3. A(n) _____ is an approach, philosophy, or strategy regarding security.
   Answer: security posture

Quick Quiz

1. **True or False:** In a white box test, the tester has no prior knowledge of the network infrastructure that is being tested.
   Answer: False

2. An agreement through which parties in a relationship can reach an understanding of their relationships and responsibilities is known as a(n) _____.
   Answer: interoperability agreement

3. A(n) _____ is an approach, philosophy, or strategy regarding security.
   Answer: security posture

4. The purpose of _____ is to eliminate as many security risks as possible and make the system more secure.
   Answer:

Quick Quiz

1. **True or False:** In a white box test, the tester has no prior knowledge of the network infrastructure that is being tested.
   Answer: False

2. An agreement through which parties in a relationship can reach an understanding of their relationships and responsibilities is known as a(n) _____.
   Answer: interoperability agreement

3. A(n) _____ is an approach, philosophy, or strategy regarding security.
   Answer: security posture

4. The purpose of _____ is to eliminate as many security risks as possible and make the system more secure.
   Answer: hardening