COURSE TECHNOLOGY
CENGAGE Learning™

Guide to Network Security
1st Edition

Chapter Nine
Network Vulnerability Assessment

Objectives

- Name the common categories of vulnerabilities
- Discuss common system and network vulnerabilities
- Find network vulnerabilities using scanning tools and in-depth penetration testing
- Access sources of information about vulnerabilities and determine how best to remediate those vulnerabilities

Introduction

- To maintain secure networks:
  - Must identify network vulnerabilities
- Self-assessment methods
  - Scanning and penetration tools
- Network security vulnerability definition
  - Defect in a device, configuration, or implementation
    - May lead to loss of revenue, information, or value

Common Vulnerabilities

- Major categories of network vulnerabilities
  - Software or firmware defects
  - Configuration or implementation errors
  - Process or procedure weaknesses

Defects in Software or Firmware

- Buffer overruns
  - Programmer does not ensure quantity of input data fits size of available data buffer
- Format string problems
  - User input passed to a formatting function without validation
- Integer overflows
  - Programmer does not restrict data to data type size boundaries

Defects in Software or Firmware (cont'd.)

- C++ catastrophes
  - Vulnerability specific to C++ and other object-oriented languages
  - Attacker can modify contents of a class
    - Takes advantage of uninitialized function pointers
    - Attacker can take control of program execution
- Catching exceptions
  - Incorrect error-handling
  - Attacker intercepts error-handling call to run malicious code

Defects in Software or Firmware (cont'd.)

- Command injection
  - Program does not properly validate user input
    - Input passed to a database
- Failure to handle errors correctly
  - Failing to catch an error and recover the program
    - Leads to denial-of-service or program crash
    - Opportunity to exploit the program execution flow
- Information leakage
  - Release of sensitive data outside intended organization

Defects in Software or Firmware (cont'd.)

- Race conditions
  - Two threads, processes, or applications are able to modify a resource
    - Programmer has not taken precautions to ensure desired order of events
- Poor usability
  - User finds application difficult to work with
    - Finds way to bypass security features

Defects in Software or Firmware (cont'd.)

- Not updating easily
  - If update method is difficult to use, it won't be used
- Executing code with too much privilege
  - Many applications require administrative privileges to install or run
    - Application failure can be exploited by an attacker
- Failure to protect stored data
  - Protect data during transit and while at rest

Defects in Software or Firmware (cont'd.)

- Weaknesses introduced with mobile code
  - ActiveX control, Flash application, Java applet
  - Attackers can exploit program vulnerabilities
- Use of weak password-based systems
  - Best practices: strong passwords using encryption; enforcing periodic password changes
- Weak random numbers
  - Libraries that provide pseudo-random numbers often inadequate
  - Use seed values and cryptographic libraries

Defects in Software or Firmware (cont'd.)

- Using cryptography incorrectly
  - Developers may incorrectly implement cryptographic function
    - Fail to follow proper steps to encrypt data properly
- Failing to protect network traffic
  - Vulnerable to eavesdropping
  - Wired networks as vulnerable as wireless
- Improper use of PKI, especially SSL
  - Application developer must implement correctly

Defects in Software or Firmware (cont'd.)

- Trusting network name resolution
  - DNS information can be manipulated by attackers
  - Application should verify true communication destination during execution

Errors in Configuration or Implementation

- Apache HTTP Server example
  - MaxClients configuration directive specifies number of concurrent requests that can be processed
    - Default value is 256
  - Must have memory capacity to process those requests
  - System administrator must set MaxClients value to match the hardware:
    - Or denial of service situation will result

Weaknesses in Processes and Procedures

- Soft vulnerabilities that result from human error
  - More difficult to detect and fix
- Examples of process or procedure vulnerabilities
  - Policy is violated
  - Processes that implement policy are inadequate or fail
- Solutions
  - Awareness and training sessions for employees
  - Regular review of policies and implementation

Finding Vulnerabilities on the Network

- Topics discussed in this section
  - Various automated tools available
  - Wide variety of network reconnaissance and vulnerability mapping capabilities
  - Manual process of penetration testing

Scanning and Analysis Tools

- Used to collect information an attacker would need to launch a successful attack
- Attack methodology
  - Series of steps or processes used by an attacker
- Security analysis tools
  - Simple to complex
  - Some are developed by the security research community
    - Available free on the Web

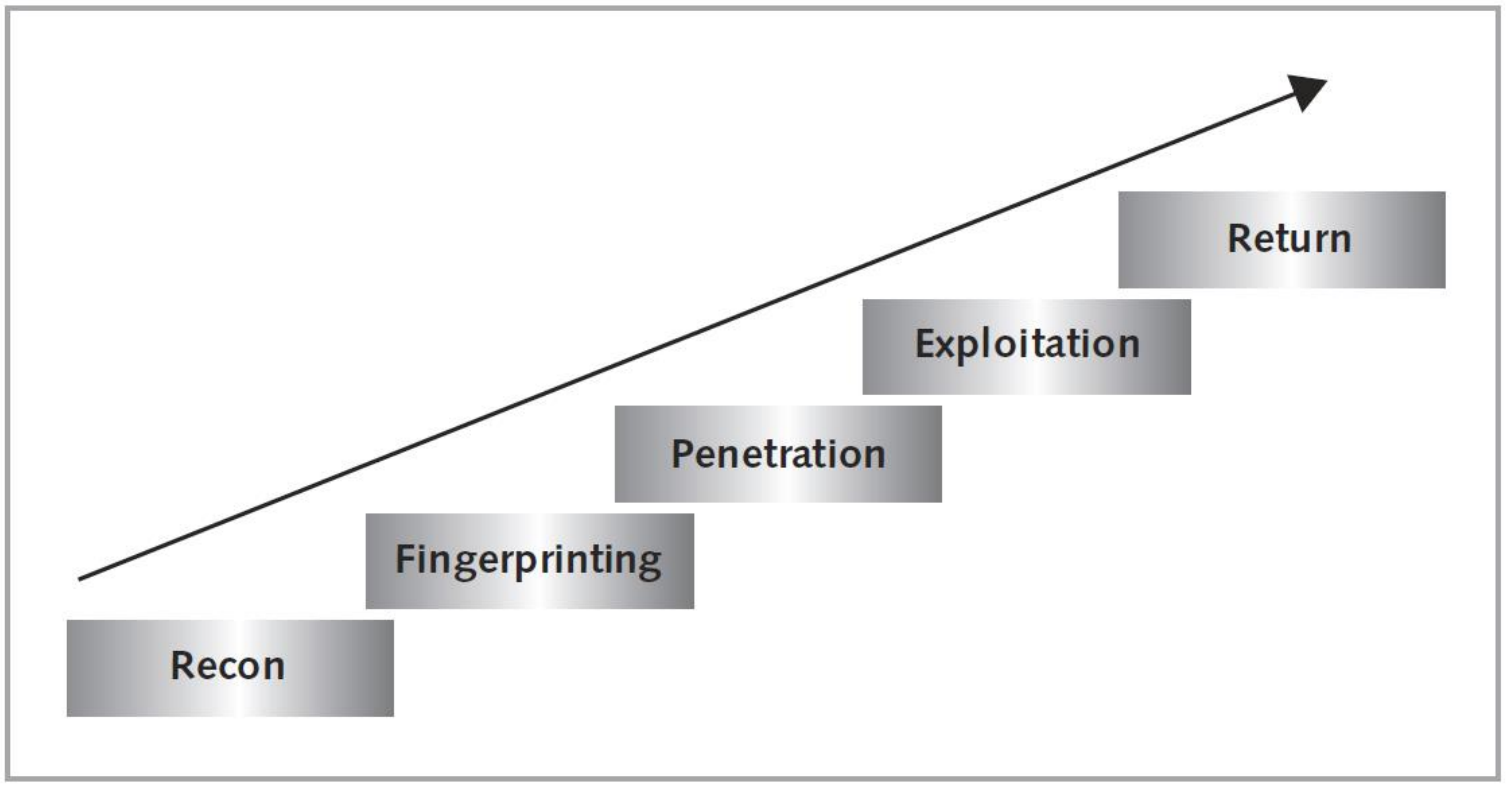

Figure 9-1 Standard attack methodology
© Cengage Learning 2013

Scanning and Analysis Tools (cont'd.)

- Reconnaissance
  - Exploring the Internet presence of a target
  - Also called footprinting
- Target IP addresses
  - Identify Web site's assigned address range
  - Easily done using `nslookup` command
  - Can also collect name, phone number, and e-mail address of technical contact

Scanning and Analysis Tools (cont'd.)

- Target Web site
  - Collect information that can be used in social engineering attacks
  - `View Source` command can be used to see code behind the page
- Business research
  - Source of attack intelligence: business-oriented Web sites
- Google hacking
  - Attacker can discover additional Internet locations not commonly associated with the company

Scanning and Analysis Tools (cont'd.)

- Fingerprinting
  - Attacker communicates with systems on the target network
    - Reveals information about internal structure and operational nature of target network
- Sam Spade
  - Enhanced Web scanner
  - Scans entire Web site for valuable information

Scanning and Analysis Tools (cont'd.)

- Wget
  - Tool that allows remote individual to mirror entire Web sites
  - Used on UNIX or Linux systems
  - Used to collect all the source code
- Port scanners
  - Used to identify computers active on the network
  - Most popular is Nmap
    - Runs on UNIX and Windows systems

TCP Port Numbers	TCP Service
20 and 21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
67 and 68	DHCP or bootstrap
80	HTTP
110	POP3
161	SNMP
194	IRC
443	HTTPS
8080	Used for HTTP proxy services

Table 9-1 Commonly used port numbers

Scanning and Analysis Tools (cont'd.)

- Firewall analysis tools
  - Used to discover firewall rules
- Nmap option called "Idle scanning" can be used
- Firewalk: tool that reveals where routers and firewalls are filtering traffic to the target host
- hping: modified ping client
  - Supports multiple protocols and many parameters

Scanning and Analysis Tools (cont'd.)

- Operating system detection tools
  - Used to determine remote computer's operating system
  - XProbe2: sends ICMP queries against the target host
  - Nmap: includes a version detection engine
- Wireless security tools' recommended capabilities
  - Sniff wireless traffic
  - Scan wireless hosts
  - Assess network's privacy or confidentiality level

Scanning and Analysis Tools (cont'd.)

- Wireless security tools examples
  - NetStumbler
  - AirSnare
  - Vistumbler
  - Aircrack-ng
- Vulnerability scanner types
  - Active
    - Produces network traffic to actively probe systems
    - Product examples: GFI LanGuard and Nessus

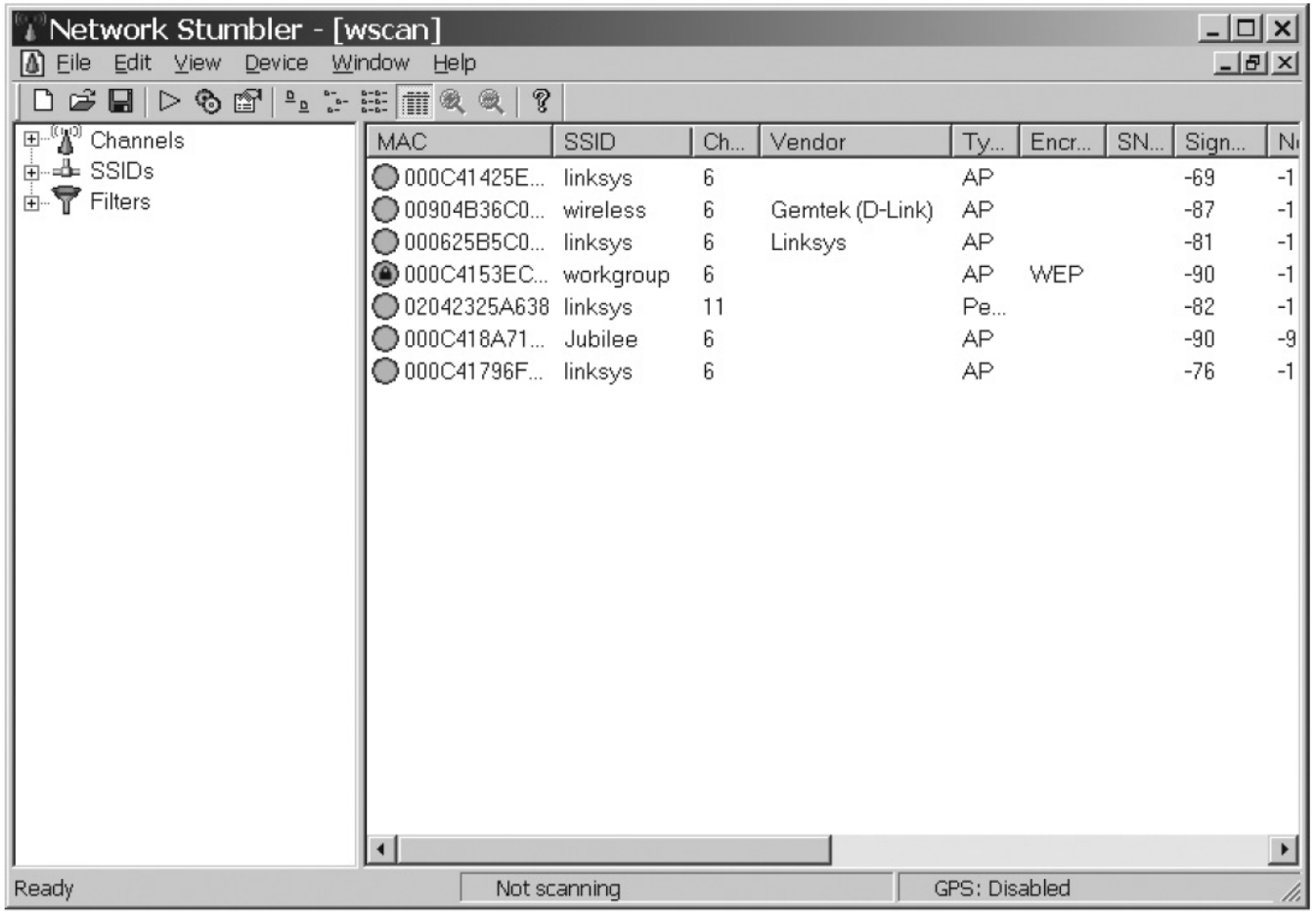

Figure 9-4 Wireless scanning with NetStumbler

Ranking	Product	Web Page
1	Nessus	*www.nessus.org* and *www.tenablesecurity.com*
2	OpenVAS	*www.openvas.org/*
3	Core Impact	*www.coresecurity.com/content/core-impact-overview*
4	Nexpose	*www.rapid7.com/products/vulnerability-management.jsp*
5	GFI LanGuard	*www.gfi.com/network-security-vulnerability-scanner*
6	QualsyGuard	*www.qualys.com/*
7	MBSA (Microsoft Baseline Security Analyzer)	*technet.microsoft.com/en-us/security/cc184923*
8	Retina	*www.eeye.com/Products/Retina.aspx*
9	Secunia PSI	*secunia.com/vulnerability_scanning/personal/*
10	Nipper	*nipper.titania.co.uk/*

Table 9-2 Top 10 vulnerability scanner products

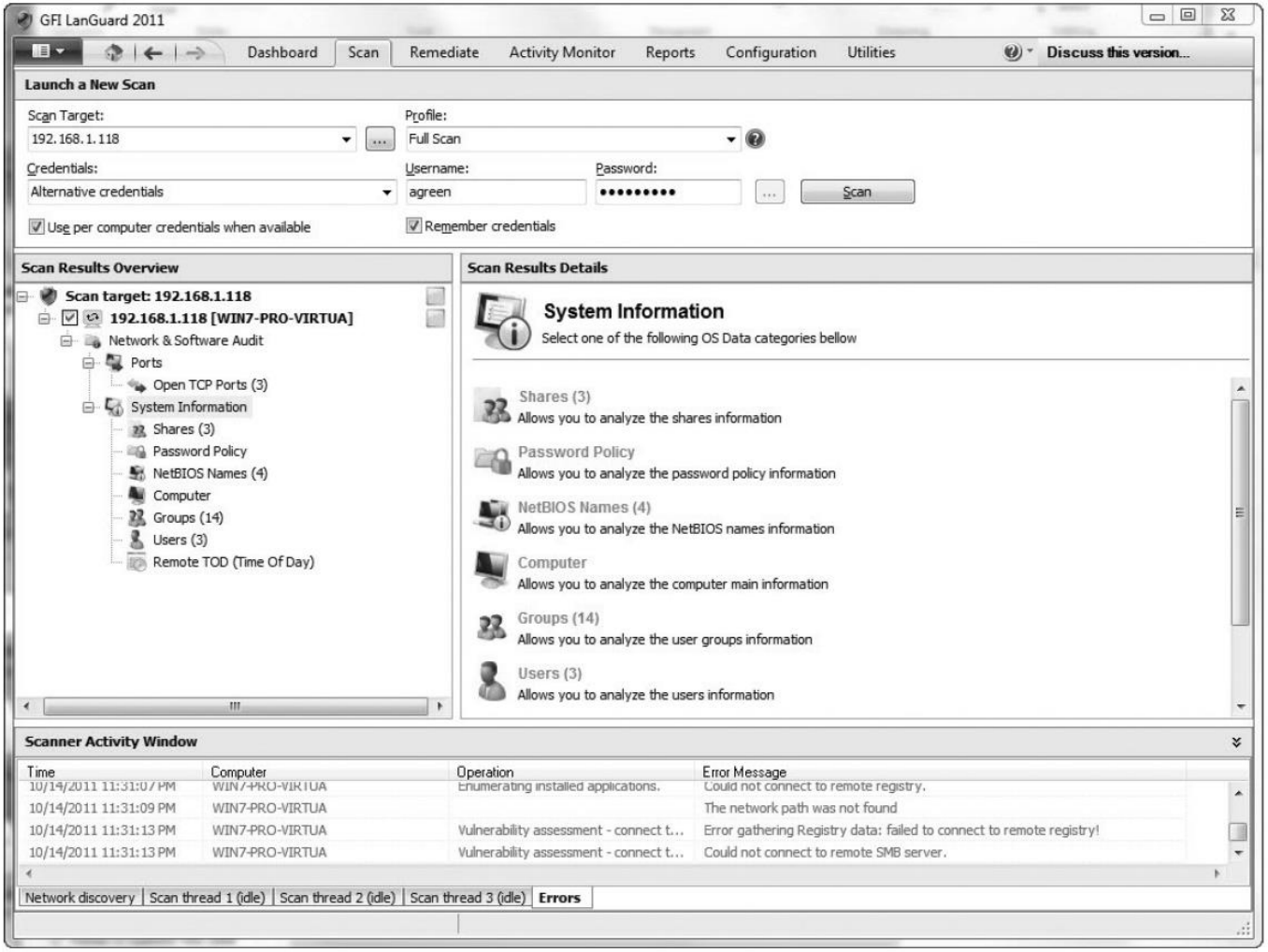

Figure 9-6 Vulnerability scanning with LanGuard
© Cengage Learning 2013

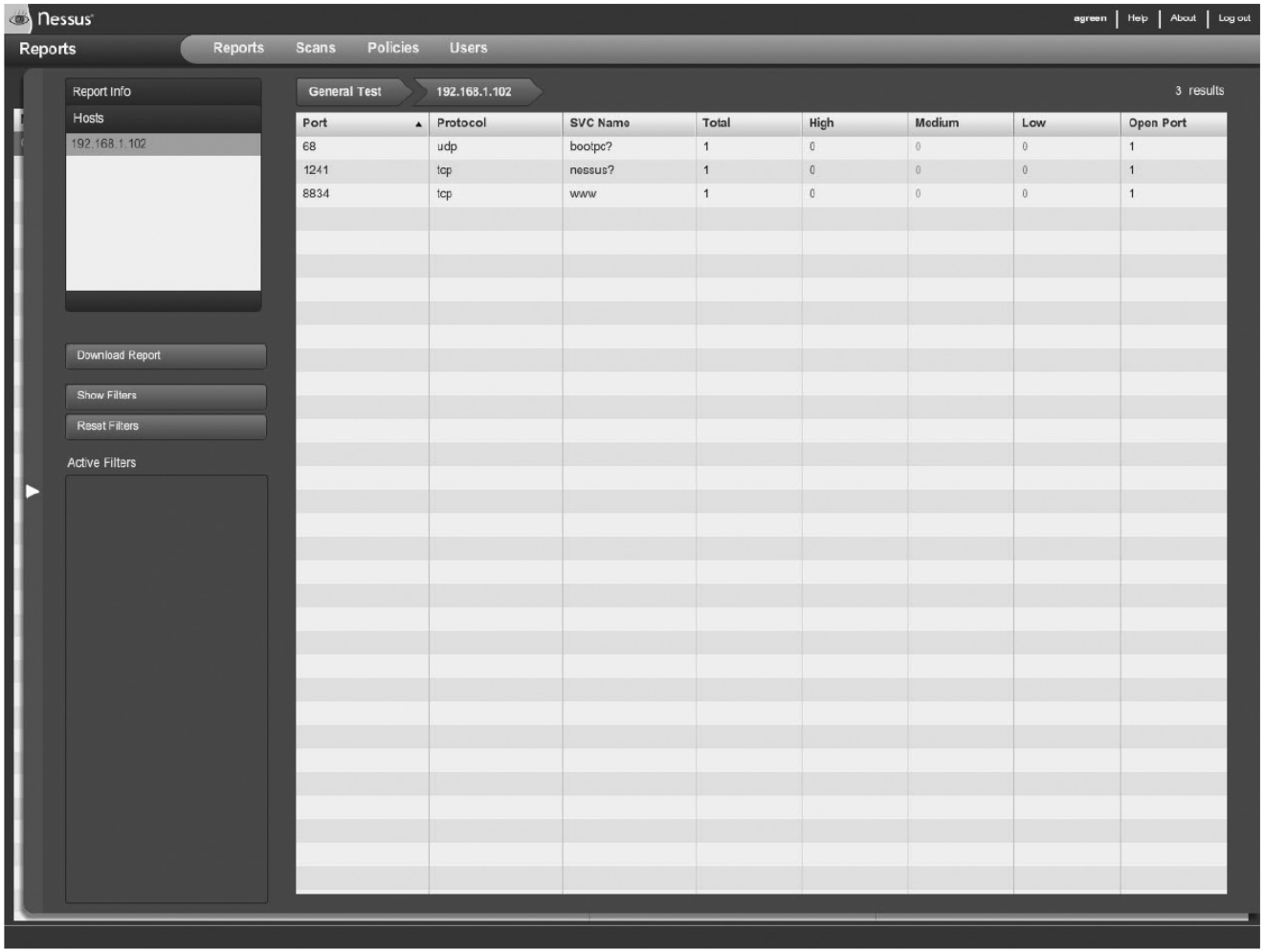

Figure 9-7 Vulnerability scanning with Nessus
© Cengage Learning 2013

Scanning and Analysis Tools (cont'd.)

- Vulnerability scanner types (cont'd.)
  - Passive
    - Listens to network traffic
    - Identifies vulnerable versions of server and client software
    - Product examples: Passive Vulnerability Scanner by Tenable Network Security and RNA by Sourcefire

Scanning and Analysis Tools (cont'd.)

- Vulnerability scanner types (cont'd.)
  - Fuzzers
    - Produce a variety of user inputs
    - Monitor programs for unexpected crashes
    - See Table 9-3 for fuzzing tool product examples
- Penetration
  - Once necessary intelligence gained:
    - Attacker can begin penetrating the network
  - Automated tools used to exploit system vulnerabilities

Fuzzer APIs and Frameworks	
Product	**Web Page**
SPIKE	*http://immunityinc.com/resources-freesoftware.shtml*
Scratch	*http://packetstormsecurity.org/UNIX/misc/scratch.rar*
LXAPI	*http://lxapi.sourceforge.net/*
PEACH	*http://peachfuzzer.com/*
antiparser	*http://antiparser.sourceforge.net/*
Autodafe	*http://autodafe.sourceforge.net/*
Web Application Fuzzing Tools	
Product	**Web Page**
MielieTool	*https://www.ee.oulu.fi/research/ouspg/MielieTools*
Wapiti	*http://wapiti.sourceforge.net/*
WebFuzzer	*http://gunzip.altervista.org/g.php?f=projects#webfuzzer*
HP WebInspect	*https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-201-200^9570_4000_100__&jumpid=reg_R1002_USEN*
Browser Fuzzing Tools	
Product	**Web Page**
MangleMe	*http://lcamtuf.coredump.cx/soft/mangleme.tgz*
AxMan	*http://metasploit.com/users/hdm/tools/axman/*
COMRaider	*http://labs.idefense.com/software/fuzzing.php#more_comraider*
TagBruteForcer	*http://research.eeye.com/html/tools/*
Hamachi	*http://metasploit.com/users/hdm/tools/hamachi/hamachi.html*

Table 9-3 Fuzzing tools

Scanning and Analysis Tools (cont'd.)

- Penetration (cont'd.)
  - Examples of testing tools
    - Core Impact
    - Immunity's CANVAS
    - Metasploit Framework
  - See Figure 9-10 for screenshot of the Metasploit Framework

Figure 9-10 Vulnerability exploitation with the Metasploit Framework
© Cengage Learning 2013

Scanning and Analysis Tools (cont'd.)

- Exploitation
  - Tools and techniques for breaking into more systems
    - Gaining further network access or gaining access to more resources
- Netcat
  - Utility to assist with file transfer
  - Can be used as a remote shell utility
    - Allows control of a remote system
  - Can act as a port scanner

Scanning and Analysis Tools (cont'd.)

- Packet sniffer
  - Network tool that collects copies of packets
- Legal requirements for using a packet sniffer
  - Must be connected to a network the organization owns
  - Must be directly authorized by the network owners
  - Must have knowledge and consent of the content creators
- Wireshark
  - Free, client-based network protocol analyzer

Ranking	Product	Web Page
1	Wireshark	*www.wireshark.org*
2	Cain & Abel	*www.oxid.it/cain.html*
3	Tcpdump	*www.tcpdump.org/*
4	Kismet	*www.kismetwireless.net/*
5	Ettercap	*ettercap.sourceforge.net/*
6	NetStumbler	*www.stumbler.net/*
7	Dsniff	*www.monkey.org/~dugsong/dsniff/*
8	Ntop	*www.ntop.org/*
9	Ngrep	*ngrep.sourceforge.net/*
10	EtherApe	*etherape.sourceforge.net/*

Table 9-4 Top 10 packet sniffers

Scanning and Analysis Tools (cont'd.)

- Return
  - Attacker's action to ensure ability to return to the target unobstructed
    - Examples: installing backdoors, installing bots, or creating user accounts

Penetration Testing

- Specialized service to assess security posture
  - Many organizations use regularly
- Uses all techniques and tools available to an attacker
- Attempts to penetrate organization's defenses
- Scope
  - May be limited
  - Depends on goal of the test
    - Identifying vulnerability or carrying out exploit

Penetration Testing (cont'd.)

- Can be conducted by internal teams or outsourced
- Categories of testing
  - Black box
    - Team is given no information
  - Gray box
    - Team is given some general information
  - White box
    - Team is given full information about organization's network structure and defenses

Recommended Vulnerability Assessment Methodology

- Stages in evaluating and validating vulnerabilities
  - Stage 1: identify technical weaknesses while minimizing organizational impact
    - Review documentation
    - Review rule sets and security configurations
    - Perform wireless scanning
    - Identify active hosts and known vulnerabilities
  - Stage 2: validate technical weaknesses
    - Review rule sets and security configurations
    - Identify active hosts and known vulnerabilities
    - Perform a penetration test using social engineering

Recommended Vulnerability Assessment Methodology (cont'd.)

- Stages in evaluating and validating vulnerabilities (cont'd.)
  - Stage 3: identify and validate technical weaknesses from the attacker's viewpoint
    - Conduct external penetration test
    - Review audit logs

Addressing Vulnerabilities

- Options for addressing a vulnerability
  - Fix it
  - Mitigate it
  - Ignore it
  - Remove the system, service, or process

Vulnerability Disclosure

- Approaches to handling the disclosure of vulnerabilities
  - Full disclosure
  - Delayed disclosure
    - Disclose only after a fix is available
  - Responsible disclosure
    - Report vulnerability to the vendor first
    - Allow vendor time to fix

Vulnerability Disclosure (cont'd.)

- Public disclosure lists
  - Vendor announcements
  - Full-disclosure mailing lists
  - The Common Vulnerabilities and Exposures database (CVE List)
    - Maintained by Mitre Corporation
  - The National Vulnerability Database (NVD)
    - Sponsored by the Department of Homeland Security
- Internet Storm Center
  - Mission: provide network threat detection and analysis

Vulnerability Disclosure (cont'd.)

- Forum of Incident Response and Security Teams (FIRST)
  - Organization that facilitates information sharing on latest cyber threats and attacks
- United States Computer Emergency Response Team (US-CERT)
  - Centralized collection and reporting facility
  - Tracks and disseminates information about current computer security threats

Vulnerability Disclosure (cont'd.)

- Information Sharing and Analysis Center (IT-ISAC)
  - Specialized forum for managing risks to IT infrastructure
  - Group is made up of members in the IT sector

Vulnerability Risk Assessment

- Organization must assess risk posed by each vulnerability
- Remediation efforts should be proportional to assessed risk
- Vendors may assign priorities to fixes
  - Problem: inconsistent terminology between vendors
- Common Vulnerability Scoring System (CVSS)
  - Standardized method for rating IT vulnerabilities
  - Consists of three metric groups
    - Base, temporal, environmental

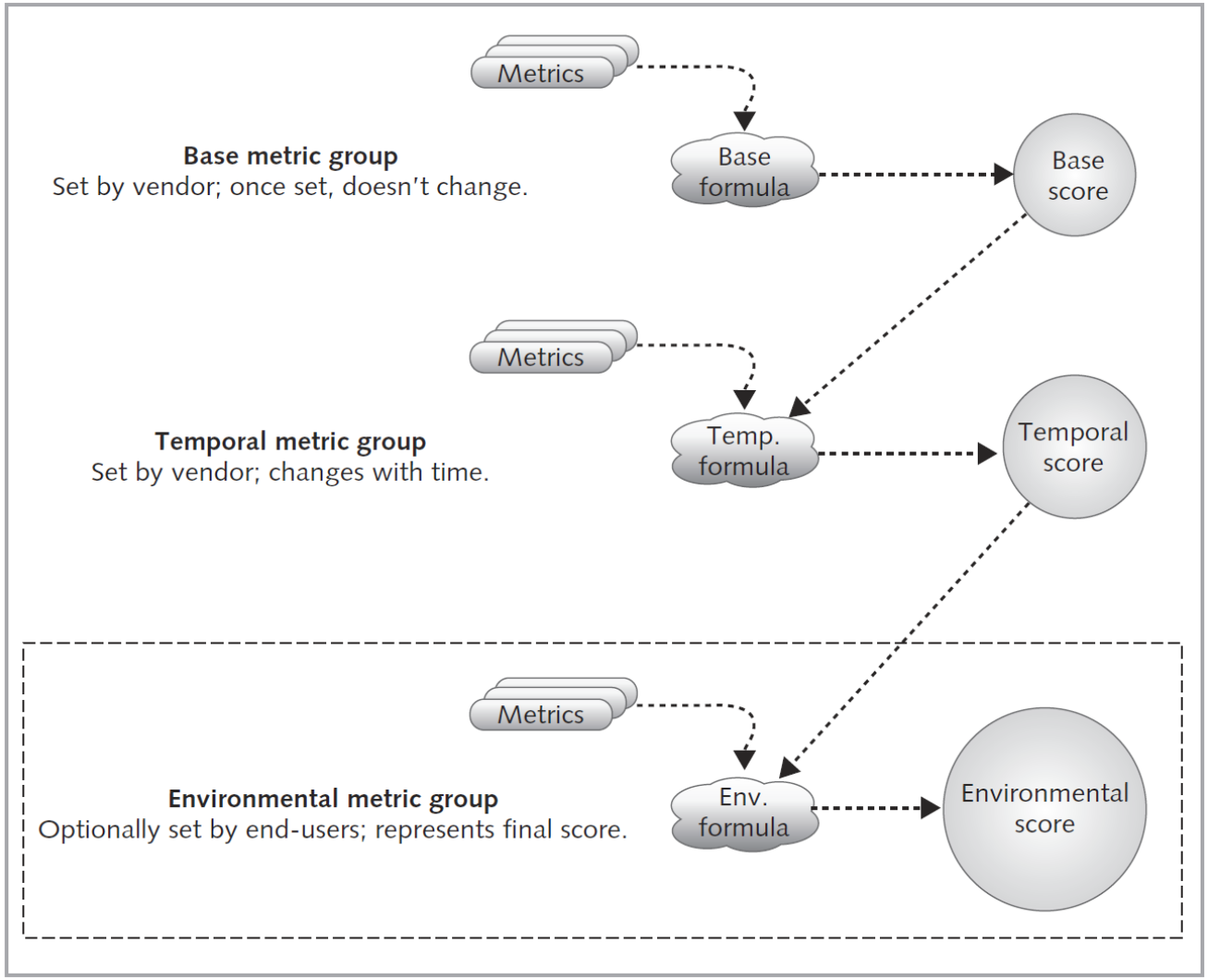

Figure 9-20 CVSS metric groups and how they interact

© *Cengage Learning 2013*

Vulnerability Risk Assessment (cont'd.)

- Other factors
  - Exposure
  - Criticality of the affected assets
  - Compensating factors
  - Downtime requirements

Summary

- Information security professionals must systematically identify system vulnerabilities
  - Methods: scanning and penetration testing
- Categories of network vulnerabilities
  - Software or firmware defects
  - Configuration or implementation errors
  - Process or procedure weaknesses
- Various sources are available for tracking current threats
  - Vendor announcements, full-disclosure mailing lists, and CVE

Summary (cont'd.)

- Tools to assess network vulnerabilities
  - Intrusion detection/prevention systems
  - Active and passive vulnerability scanners
  - Automated log analyzers
  - Protocol analyzers (sniffers)
- Penetration testing assesses an organization's security posture on a regular basis