CIT 270: SYSTEMS SECURITY I

CHAPTER 13: VULNERABILITY ASSESSMENT & DATA SECURITY

BYU IDAHO

INTRODUCTION

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

Note

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to yellow words. These highlighted words denote a topic that will almost always be on your chapter quiz.

ASSESSING THE SECURITY POSTURE

A vulnerability assessment is comprised of five steps:

1. Asset identification; most important step
2. Threat evaluation
3. Vulnerability appraisal
4. Risk assessment
5. Risk mitigation

Reminder: Risk management is not identical to vulnerability assessment. Risk management looks at dangers that an asset faces. Vulnerability assessments examine the consequences for the assest if it is successfully compromised.

ASSESSING THE SECURITY POSTURE: THREAT EVALUATION

Category of Threat	Example
Natural disasters	Fire, flood, or earthquake destroys an area
Espionage	Spy steals production schedule
Extortion	Mail clerk is blackmailed into intercepting letters
Hardware failure / errors	Firewall blocks all network traffic
Human error	Employee drops laptop computer in the parking lot
Sabotage or vandalism	Attacker implants worm that erases files
Software attacks	Virus, worm, or DoS compromises hardware or software
Technical obsolescence	Program does not function under new version of operating system
Utility interruption	Electrical power is cut off

ASSESSING THE SECURITY POSTURE: THREAT EVALUATION

Examples on page 570.

ASSESSING THE SECURITY POSTURE: RISK ASSESSMENT

Impact	Description	Example
No impact	Does not really not affect the organization	The theft of a mouse attached to a desktop
Small impact	Produce limited periods of inconvenience and possibly result in changes to procedures	A specific brand/ type of hard drive that fails might require that spare drives be made available and devices with those drives are periodically tested
Significant	A vulnerability that results in a loss of productivity due to downtime or causes a capital outlay to alleviate it	Malware that is injected into the network could be classified as a significant vulnerability
Major	A vulnerability that causes a considerable negative impact on revenue.	The theft of the latest production research and development data through a backdoor
Catastrophic	A vulnerability that would cause the organization to cease functioning or be seriously crippled in its operations	A tornado destroys an office building and all of the companies data

ASSESSING THE SECURITY POSTURE: RISK MITIGATION

Vulnerability Assessment Action	**Steps**
1. Asset identification	Inventory the assets and their relative value
2. Threat identification	Classify threats by category and design attack tree
3. Vulnerability Appraisal	Determine current weaknesses in protecting assets and use vulnerability assessment tools
4. Risk Management	Estimate impact of vulnerability and calculate risk likelihood and impact of the risk
5. Risk Mitigation	Decide what to do with the risk

VULNERABILITY ASSESSMENT TOOLS: PORT SCANNERS

Protocol Analyzer: hardware or software that captures packets to decode and analyze their contents; Wireshark.

Vulnerability Scanner: generic term for a range of products that look for vulnerabilities in networks or systems.

Active Scanner: sends *probes* to a network device and examines the responses received back to evaluate whether a specific device needs remediation.

Passive Scanner: identifies the current software OS and applications being used on the network, and indicates which ones might have a vulnerability.

VULNERABILITY ASSESSMENT TOOLS: TYPES OF PORT SCANNERS

Type	Description	Uses
Network Mapping Scanner	Combines network device discovery tools and network scanners to find open ports or discover shared folders.	Can be used to create visual maps of the network that also identify vulnerabilities that need correction.
Wireless Scanner	Can discover malicious wireless network activity such as failed login attempts, record these to an event log, and alert an administrator.	Detects security weaknesses inside the local wireless network with internal vulnerability scanning.
Configuration Compliance Scanner	Used to evaluate and report any compliance issues related to specific industry guidelines.	A compliance audit is a comprehensive review of how an enterprise follows regulatory guidelines.

VULNERABILITY ASSESSMENT TOOLS

Honeypot: a computer located in an area with limited security and loaded with software and data files that appear to be authentic.

Honeynet: a network setup with intentional vulnerabilities connecting multiple honeypots.

Honeynet and DMZ

VULNERABILITY ASSESSMENT TOOLS: CRACKERS

Banner Grabbing: using a program that intentionally gathers banner messages; OS type, software type, software version, last modified, and so on.

Wireless Cracker: designed to test the security of a wireless LAN by attempting to break its protections of WPA or WPA2.

Password Cracker: designed to break the digest of a password to determine its strength.

VULNERABILITY ASSESSMENT TOOLS: COMMAND-LINE TOOLS

Name	Description	How its used
Ping	Tests the connection between two devices	Can flood the network to determine how it responds to a DoS attack
Netstat	Displays detailed information about how a device is communicating with other network devices	Determines the source of malware that is sending out stolen information or communicating with a C&C server.
Tracert	Shows the path that a packet takes	Can detect faulty or malicious routing paths
Nslookup (Win) or Dig (Linux)	Queries the DNS to obtain a specific domain name or IP address mapping	Used to verify correct DNS configurations
Ipconfig (Win), IP, and Ifconfig (Linux)	Displays all current TCP/IP network configuration values and refreshes DHCP and DNS settings	Used to alter current settings such as IP address, subnet mask, and default gateway to test if configurations are secure
Tcpdump	Linux command-line protocol analyzer	Can monitor network traffic for unauthorized traffic

VULNERABILITY ASSESSMENT TOOLS: OTHER TOOLS

Nmap: a third-party network mapper that provides security vulnerability scanning to determine what type of devices are connected to the network and what software or services they are running.

Netcat: command-line alternative to the Nmap with additional features added to its ability to scan for vulnerabilities.

Depending on your organization you might benefit from exploitation frameworks that replicate attacks (done during your vulnerability assessment) and steganography assessment tools that determine how well data has been hidden in images.

ASSESSING THE SECURITY POSTURE: THREAT EVALUATION

Vulnerability Scanning pages 584 – 585.

Penetration Testing pages 586 – 588.

Practicing Data Privacy and Security pages 588 – 595.