UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Network Security Administration and Management

BITS 3353

Lecture 6: Vulnerability Assessment and Mitigating Attacks

Objectives

- Define vulnerability assessment and explain why it is important
- List vulnerability assessment techniques and tools
- Explain the differences between vulnerability scanning and penetration testing
- List techniques for mitigating and deterring attacks

Vulnerability Assessment

A vulnerability assessment is a systematic and methodical evaluation of exposure of assets to attackers, forces of nature and any other entity that could cause potential harm.

It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

Elements of Vulnerability Assessment

ASSET IDENTIFICATION

Process of inventorying items with economic value

- Identify what needs to be protected
- After an inventory of the assets has been identify, its important to determine each item's relative value.

THREAT EVALUATION

List potential threats from threat agent

- What pressures are against those assets
- Threat agents are not limited to attackers

THREAT MODELING

Goal of understanding attackers and their methods

VULNERABILITY APPRAISAL

Determine current weaknesses as snapshot of current organization security

- How susceptible current protection is
- Every asset should be viewed in light of each threat

RISK ASSESSMENT

Determine damage resulting from attack and assess likelihood that vulnerability is risk to organization

- What damages could result from the threats
- Not all vulnerabilities pose the same risk

RISK MITIGATION

- Determine what to do about risks
- Determine how much risk can be tolerated

Common Threat Agents

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

Vulnerability Assessment Actions and Steps

Asset identification

- Inventory the assets
- Determine the assets' relative value

Threat identification

- Threat evaluation and threat modelling
- Classify threats by category
- Design attack tree

Vulnerability Appraisal

- Determine current weaknesses in protection assets
- Use vulnerability assessment tools

Risk assessment

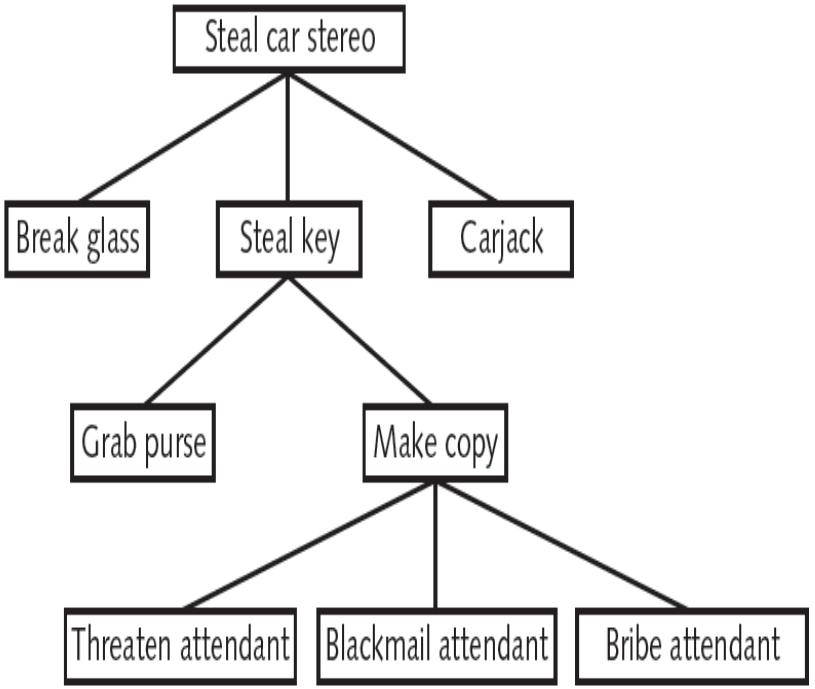
- Estimate impact of vulnerability on organization
- Calculate risk likelihood and impact of the risk

Risk mitigation

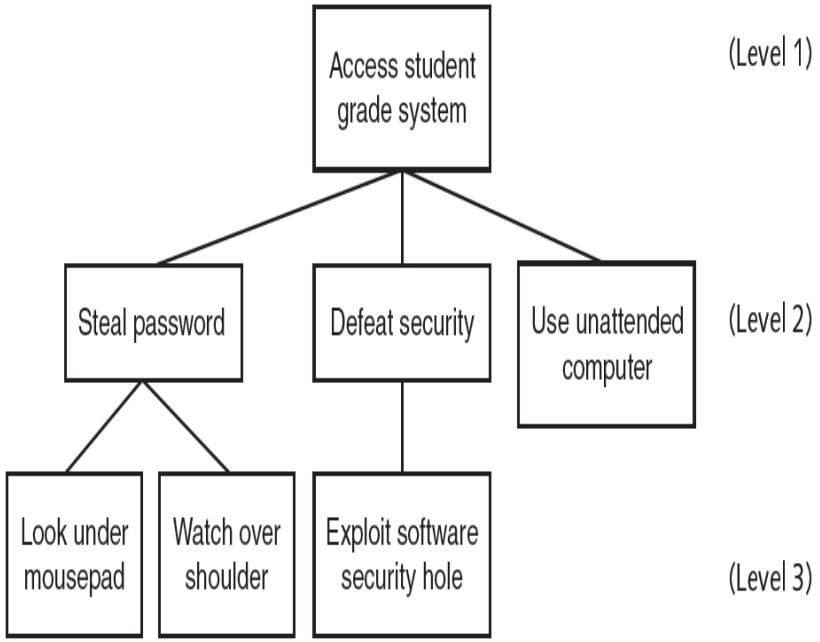
- Decide what to do with the risk

Attack Tree

Attack Tree: Provides visual representation of potential attacks



Attack tree for stealing a car stereo



Attack tree for breaking into grading system

Vulnerability Impact Scale

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

Vulnerability Assessment Technique

BASELINE REPORTING

Comparison of present state of system to its baseline

- 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

Vulnerability Assessment Technique

APPLICATION DEVELOPMENT TECHNIQUES

Minimize vulnerabilities during software development

- Challenges to approach
  - Software application size and complexity
  - Lack of security specifications
  - Future attack techniques unknown

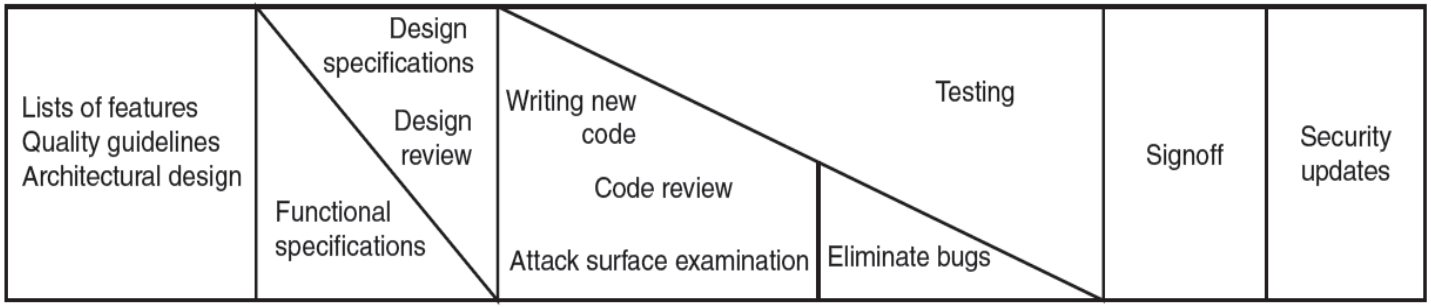
Vulnerability Assessment Technique

SOFTWARE DEVELOPMENT ASSESSMENT TECHNIQUES

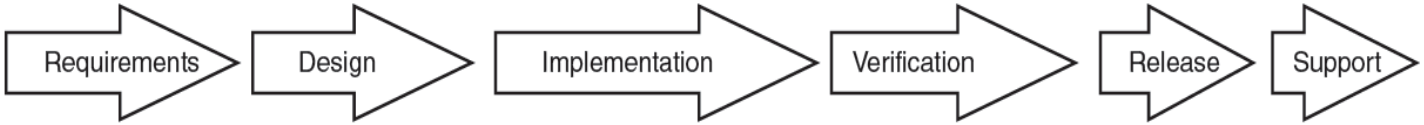
Review architectural design in requirements phase

- Important for software vulnerabilities be minimized while software being developed instead of after released

- Conduct design reviews
  - ✓ Consider including a security consultant
- Conduct code review during implementation phase
  - ✓ Examine attack surface (code executed by users)
- Correct bugs during verification phase
- Create and distribute security updates as necessary



Software development process



Assessment Tools

PORT SCANNER
Software can be used to search system for port vulnerabilities

PROTOCOL ANALYZER
Hardware or software that captures packets to decode and analyze content

VULNERABILITY SCANNER
Automated software searches a network or system for known security vulnerabilities or weaknesses

BANNER GRABBING TOOLS
Software used to intentionally gather message that service transmits when another program connects to it

HONEYPOTS AND HONEYNETS
Goal is to trick attackers into revealing their techniques

Port Scanning

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
Stealth scans	A stealth scan uses various techniques to avoid detection. Because a port scan is an incoming connection with no data, it is usually logged as an error; a stealth scan tries to "fool" the logging services	One technique is to scan slowly over several days to avoid detection; another technique is to flood the target with spoofed scans and embed one scan from the real source address
Xmas Tree port scan	An Xmas tree packet is a packet with every option set 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 lightbulb and all are turned on, so that it can be said "The packet was lit up like a Christmas tree"

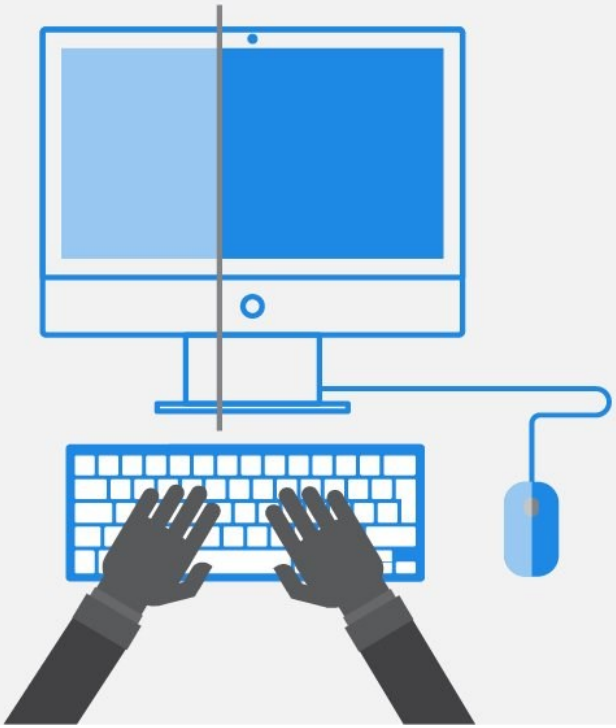
Port scanning

Port Scanning

Protocol	Port number
File Transfer Protocol (FTP)	20 (data) and 21 (control)
Secure Shell (SSH), Secure Shell File Transfer Protocol (SFTP), Secure Copy (SCP)	22
Telnet	23
Trivial File Transfer Protocol (TFTP)	69
Hypertext Transfer Protocol (HTTP)	80
NetBIOS	139
Hypertext Transfer Protocol Secure (HTTPS)	443
FTP Secure (FTPS)	989 (data) and 990 (control)

Commonly used default network ports

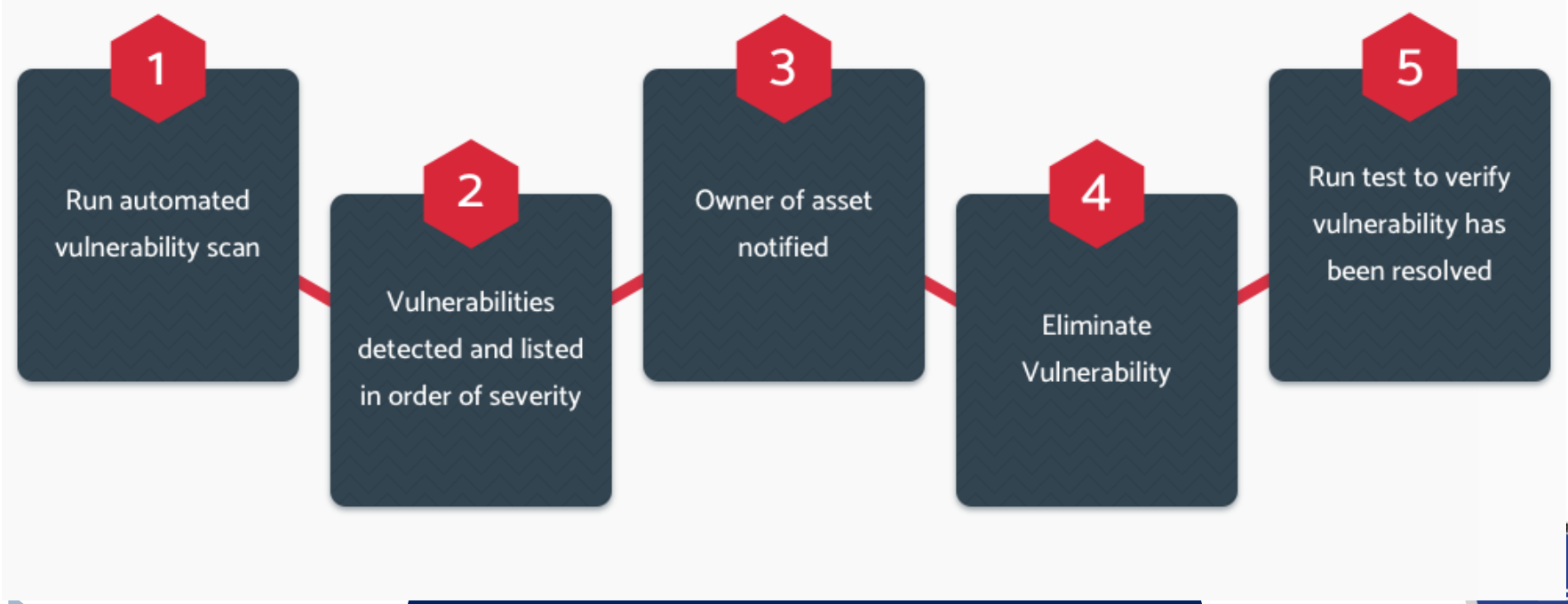
PENETRATION TESTING VS. VULNERABILITY SCANNING



Vulnerability Scanning

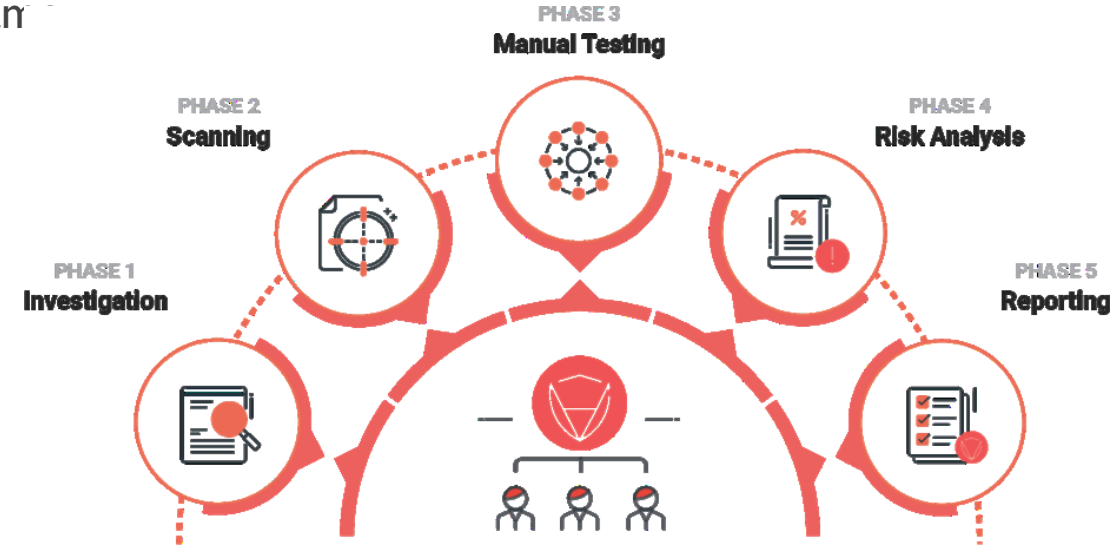
A vulnerability scan makes use of an automated tool to scan your systems and networks for publicly known vulnerabilities. This will provide you with a list of detected security flaws, allowing you to take remediation steps and install the latest versions and patches.

New vulnerabilities are always coming to light. So, vulnerability scan should be conducted at regular intervals



Penetration Testing

Penetration test is where a **security professional takes on the role of a hacker and attempts to exploit your systems** in the same way a malicious party would. They will then provide a report based on their findings detailing how they managed to compromise your network and systems (should they manage to do so) and how you can go about preventing others from doing the sam



- 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

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 $1,500 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 to reduce exposure to business

Vulnerability scan and penetration testing features

Mitigating and Deterring Attacks

1 Creating a security posture

- Security posture describes strategy regarding security
- Initial baseline configuration
  - –Standard security checklist
  - –Systems evaluated against baseline
  - –Starting point for security
- Continuous security monitoring
  - –Regularly observe systems and networks
- Remediation
  - –As vulnerabilities are exposed, put plan in place to address them

Mitigating and Deterring Attacks

2 Configuring Controls

- Properly configuring controls is key to mitigating and deterring attacks
- Some controls are for detection
  - –Security camera
- Some controls are for prevention
  - –Properly positioned security guard
- Information security controls
  - –Can be configured to detect attacks and sound alarms, or prevent attacks

Mitigating and Deterring Attacks

3 Hardening

- Purpose of 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

4 Reporting

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

Summary

- Vulnerability assessment
  - –Methodical evaluation of exposure of assets to risk
  - –Five steps in an assessment
- Risk describes likelihood that threat agent will exploit a vulnerability
- Several techniques can be used in a vulnerability assessment
- Port scanners, protocol analyzers, honeypots are used as assessment tools
- Vulnerability scan searches system for known security weakness and reports findings
- Penetration testing designed to exploit any discovered system weaknesses
  - –Tester may have various levels of system knowledge
- Standard techniques used to mitigate and deter attacks
  - –Healthy security posture
  - –Proper configuration of controls
  - –Hardening and reporting