



NETWORK **SECURITY**

02 SYSTEM VULNERABILITIES

Contents



2.1 Vulnerabilities, A Closer Look

2.1.1 Definitions

2.1.2 Sources of Vulnerabilities

2.2 Vulnerabilities Assessment

2.2.1 Assessment Services

2.2.2 Assessment Advantages

2.1 A Closer Looks



2.1.1 (*new*) Definitions

- System vulnerabilities are weaknesses in the software or hardware on a server or a client that can be exploited by a determined intruder to gain access to a network.
- A system vulnerability is a condition, a weakness of or an absence of security procedure, or technical, physical, or other controls that could be exploited by a threat.

2.1 A Closer Looks



2.1.2 Sources of Vulnerabilities

- The most frequently mentioned sources of security vulnerability are:
 - design flaws,
 - poor security management,
 - incorrect implementation,
 - Internet technology vulnerability,
 - the nature of intruder activity,
 - the difficulty of fixing vulnerable systems,
 - the limits of effectiveness of reactive solutions,
 - social engineering.

2.1 A Closer Looks



2.1.2.1 Design Flaws

- Hardware and software, quite often have design flaws.
- Hardware systems are less susceptible to design flaws than software.
- But the biggest problems in system security vulnerability are due to software design flaws.

2.1 A Closer Looks



- Three major factors contribute a great deal to software design flaws:
 - human factors,
 - software complexity,
 - trustworthy software sources.

2.1 A Closer Looks



Human Factors

- *Memory lapses and attentional failures*
- *Rush to finish*
- *Overconfidence and use of nonstandard or untested algorithms*
- *Malice: Bugs, viruses, worms and Trojan*
- *Complacency*

2.1 A Closer Looks



Software Complexity

- *Complexity*: A program may present billions of possible outcomes.
- *Difficult testing*: There will never be a complete set of test programs.
- *Ease of programming*: easy to learn, hard to be good, and difficult to check errors.
- *Misunderstanding of basic design specifications*: Affects the design phases and improper specification.

2.1 A Closer Looks



Trustworthy Software Sources

- We tend to do not care about the quality of a software as long as it does what we want it to do.
- Shareware and freeware have a high potential of bringing hostile code into trusted systems.

2.1 A Closer Looks



Re-Use, Re-Engineering & Outlived Design

- Software re-use is the integration and use of software assets from a previously developed system.
- Both software re-engineering and re-use are hailed for cutting down on the escalating development and testing costs.

2.1 A Closer Look



2.1.2.2 Poor Security Management

- Security management is both a technical and an administrative security process to provide protection.
- The most effective way is to implement security risk assessment.
- But, security management by itself is a complex process.
- Poor security management is a result of little control.

2.1 A Closer Looks



- Good security management is made up of a number of implementable security components that include:
 - risk management,
 - information security policies and procedures,
 - standards, guidelines,
 - information classification,
 - security monitoring,
 - security education.

2.1 A Closer Look



2.1.2.3 *Incorrect Implementation*

- Very often is a result of incompatible interfaces.
- An incompatible interface means that existing references to the interface can fail or behave incorrectly.

2.1 A Closer Looks



- Incompatibility in system interfaces may be caused by a variety of conditions usually created by things such as:
 - Too much detail,
 - Not enough understanding of the underlying parameters,
 - Poor communication during design,
 - Selecting the software or hardware modules before understanding the receiving software,
 - Ignoring integration issues,
 - Error in manual entry.

2.1 A Closer Looks



2.1.2.4 Internet Vulnerability

- Internet technology has been and continues to be vulnerable.
- No one knows how many hardware and software vulnerabilities are there, but a few are always discovered every day by hackers.
- And the problem is more prevalent with software.

2.1 A Closer Looks



- Software vulnerabilities can be put into four categories:
 - Operating system vulnerabilities,
 - Port-based vulnerabilities,
 - Application software based errors,
 - System protocol software.

2.1 A Closer Looks



2.1.2.5 Nature of Intruder Activities

- It is ironic that as “useful” technology develops so does the “bad” technology.
- One thing is clear, though: hacker technology is flourishing.

2.1 A Closer Look



2.1.2.6 Difficulties of Fixing Vulnerable Systems

- It is difficult to fix known system vulnerabilities.
- There are also logistic problems.
- There are several factors affecting the quick fixing of patches.

2.1 A Closer Looks



2.1.2.7 Limits of Effectiveness of Reactive Solutions

- Serious growing system security problem.
- One of the new security problems is to find a “good” solution.
- Are we reaching the limits of our efforts ??

2.1 A Closer Looks



- Richard D. Pethia said yes with the following reasons:
 - Software are kept up with the vulnerabilities fixes.
 - Thousands of connected computers that are vulnerable to one form of attack or another.
 - Attack technology has now advanced.

2.1 A Closer Looks



2.1.2.8 Social Engineering

- Social engineering is an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to gain the information (usernames and passwords) one needs to gain access to the system.
- It utilizes two human weaknesses:
 - no one wants to be considered ignorant
 - human trust

2.2 Vulnerability Assessment

- Vulnerability assessment is a process that works on a system to identify, track, and manage the repair of vulnerabilities on the system.
- Items that are checked by this process in a system under review are varies.

2.2 Vulnerability Assessment

- Most vulnerability assessment services will provide system administrators with:
 - network mapping and system finger printing,
 - a complete vulnerability analysis,
 - prioritized list of misconfigurations.

2.2 Vulnerability Assessment

- Assessment produces a final report
- This report consists of:
 - prioritized recommendations for mitigating or eliminating weaknesses,
 - it also contains recommendations of further reassessments.

2.2 Vulnerability Assessment



2.2.1 Vulnerability Assessment Services

- there is a growing number of system vulnerability services.
- Among the services are:
 - Vulnerability Scanning,
 - Penetration Testing, and
 - Application Assessment

2.2 Vulnerability Assessment

2.2.1.1 *Vulnerability Scanning*

- To provide a comprehensive security review of the system.
- To spot critical vulnerabilities and gaps in the system's security practices.
- Produce final report for strategic advice and recommendations.

2.2 Vulnerability Assessment

2.2.1.2 *Penetration Testing*

- All known hacking techniques and tools are tested.
 - finds new and sometimes obscure vulnerabilities.
 - identifies processes and procedures of attack.
 - categorizes sources and severity of vulnerabilities.

2.2 Vulnerability Assessment

- 2.2.1.3 Application Assessment
 - Web applications become more widespread and use as main interface between user and network.
 - It has opened a new security paradigm in system administration.

2.2 Vulnerability Assessment



2.2.2 Assessment Advantages

- Provide and develop signatures and updates for new vulnerabilities.
- Automated and regularly scheduled scan of all network resources.

Exercise 01



1. Why port scanning is classified as a type of attacks?

- What is port scanning
- How port scanning works
- What are the dangerous of port scanning

Exercise 01



2. Names and describes tools (software) that can be used to detect and respond to an attack.

Exercise 01



3. In your opinion, what type of attacks is the most dangerous attack ? Defense your answer.