Network and Server Attacks and Penetration

Chapter 12

Lecturer: Pei-yih Ting

Overview

- Goal of Security Control
- Phases of Control
- Methods of Taking Control
- Common Points of Attack
- Multifront Attacks
- Auditing to Recognize Attacks
  - Malicious Code
  - System Bugs and Vulnerabilities
  - DOS
  - Illicit Nodes, War Driving
- Unwanted Control

Security Control

- Security control is the basic responsibility of information security practitioners
  - Their security mechanisms must enforce the CIA Triad
- The CIA Triad has three components
  - Confidentiality
  - Integrity
  - Availability
- Attackers have the DAD Triad
  - Disclosure
  - Alteration
  - Destruction (Denial)

Phases of Control

- Attackers progress through five phases to gain control of a system or network
- Phase 1: No Access
  - External users have no access to a network
  - Implemented through strict perimeter controls (firewall, router,…)
- Phase 2: External Application Access
  - External users have limited access to certain applications such as Web service
  - Main abuse is DoS attacks
  - Could exploit vulnerabilities on the web server

Phases of Control (cont'd)

- Phase 3: User Access
  - Authorized users have basic privileges to log on and use applications, e-mail, and the Internet
  - Typically granted to all non-administrative users
  - Attackers attempt to masquerade as legitimate users and have access to all normal uses
- Phase 4: Superuser Access
  - Attackers attempt to get access to superuser privileges
  - Superusers have access to sensitive and critical applications and data

Phases of Control (cont'd)

- Phase 4 (cont'd)
  - Superuser accounts are sometimes called root accounts on UNIX systems and Administrator accounts on Windows
  - Each person with superuser privileges should have a separate account for accountability reasons
- Phase 5: total Control
  - Superuser privileges that extend over an entire network (domain superuser) are even more damaging
  - Network superusers can change attributes of the network itself

Methods of Taking Control

- Attackers often start with Phase 1 or 2 access to a system
  - And try to escalate
  - The goal may or may not be to gain Phase 5 access
- A network security scenario
  - A web server located in the DMZ of a simple firewall installation
  - Cracker begins with Phase 2 access to the Web server
- Reaching Phase 3
  - Can use a tool like nmap to probe applications and exploit a known vulnerability

Network Security Scenario

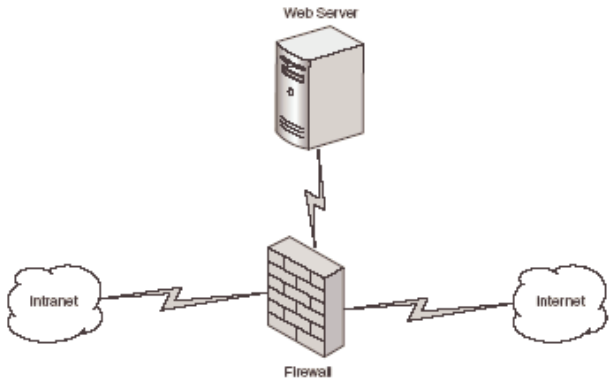

Figure 12.1
Network security scenario

Methods of Taking Control (cont'd)

- Reaching Phase 3 (cont'd)
  - Run a password-cracking algorithm: cracker, john
  - Locate a public domain script and find a vulnerability
  - Locate a custom-written script and try common techniques like buffer overflow
- Reaching Phase 4
  - Use a password-cracking algorithm on an administrative account
  - Use a rootkit program
    - A suite of cracking tools for superuser access

Methods of Taking Control (cont'd)

- Reaching Phase 5
  - See if the same passwords work for local and firewall administrative accounts
  - Launch a set of series of attacks on the firewall
- Best defense is a layered perimeter protection
  - Vary and layer security devices
  - Use intrusion-detection techniques
  - Be proactive about finding and repairing potential security vulnerabilities

Recognizing Attacks

- It can be difficult to recognize that you are or have been attacked
  - Attacks range from very obvious to very subtle
- Symptoms can mimic other problems
  - For example, a general slowdown in Web performance could be due to legitimate traffic or to a low-level Denial of Service attack
- To maximize the functionalities of your resources, use extra security at common points of attack

Common Points of Attack

- Common attack points should be particularly monitored for key indicators of an attack
- Web server attacks
  - Web servers are crucial for many businesses but are probably the most vulnerable to attack
  - Unexplained server load can be a sign of attack and should be investigated
    - Other causes can be server misconfiguration, operating system flaws, programming errors, etc.
  - Integrity preservation tools will be effective

Common Points of Attack (cont'd)

- DNS Server Attacks
  - DNS servers have numerous vulnerabilities, BIND
  - The most important security technique is to stay up-to-date with patches
- Mail Server Attacks
  - SMTP servers can be in a DMZ, but it still has some exposure to the Internet
  - Monitor inbound traffic for attacks such as DoS attacks
  - Monitor outbound traffic for unusual activity that might indicate spammers are using your relay

Common Points of Attack (cont'd)

- Firewall Attacks
  - The firewall is the most critical perimeter protection device
  - Single firewalls can easily be flooded in a DoS or DDoS attack
  - If you see increasing or unusual traffic, investigate it
- Test/Development System Attacks
  - It does not take long for an unprotected system to be compromised
  - Don't ever attach an unprotected system to the Internet

Multifront Attacks

- Crackers will sometimes try to launch multiple simultaneous attacks
  - Chances are some will work
- If you suspect a particular location is launching multiple attacks
  - Block access at the router level until it can be resolved
- The better protected your system is, the more likely crackers will give up and go after easier prey

Auditing to Recognize Attacks

- Intrusion detection systems can sometimes detect attacks as they occur
- Audit trails can provide diagnostic assistance after the fact
  - Useful for understanding what happened and how to stop it from happening again
  - Sometimes auditing can detect attacks that would go unnoticed otherwise

Malicious Code

- Antivirus software scans instantaneously
  - Inbound and outbound e-mail
  - Web content
  - Other network traffic
- You should analyze audit trails from antivirus software
- Traffic patterns may give you clues
  - about attacks
  - about whether there is infected data on your system

System Bugs and Vulnerabilities

- All operating systems and major applications have vulnerabilities
- You must stay up-to-date on patches
- You must analyze audit trails for attempts to exploit the vulnerabilities
- Symptoms of a system that has unpatched vulnerabilities include
  - Unexplained crashes/reboots
  - Unusual traffic that does n0t meet protocol specifications
  - Repeated ping traffic between systems

Denial of Service (DoS) Attacks

- DoS attacks deny resources to legitimate users
- They can be easy to detect
  - A resource becomes unavailable and you hear immediate complaints
- They can be more subtle
  - Gradual slowing of response times
  - Intermittent unavailability of resources
- Subtle symptoms can have several different causes but should be investigated
- Pay attention to changing patterns in network activity

Illicit Nodes

- Network jacks are becoming very common
  - Often found in public places
- Wireless networks are becoming prevalent
- Crackers can often find paths to penetrate a network internally through jacks or wireless devices
- The network should be configured to reject internal traffic from unrecognized systems
  - Monitor the MAC addresses of network nodes
  - Investigate any new addresses

War Driving

- War driving is named after war dialing
- Crackers drive around searching for wireless network access points
  - Once accessed, they can work as network insiders to crack the entire network
- It can be a good idea to separate wireless users and segment them with a firewall
- Be careful implementing a wireless network until you understand the unique security requirements
  - Implement necessary identification / authentication

Unwanted Control

- Damage caused by a cracker with full control of your system can be irreversible
- Be aware of techniques used by crackers to gain control
  - Rootkits, malicious code, exploitation of well known vulnerabilities
- Use audit trails to examine administrative activity
  - Always investigate unusual or suspicious activity

Summary

- Information security practitioners are responsible for security control
  - They must enforce the basic requirements of the CIA Triad (confidentiality, integrity, availability)
- There are 5 phases of control that a cracker might aspire to:
  - Phase 1: No access
  - Phase 2: External application access
  - Phase 3: User access
  - Phase 4: Superuser access
  - Phase 5: Total control

Summary (cont'd)

- Methods used by a cracker to take control include:
  - Exploiting known vulnerabilities in systems, scripts, and applications, cracking passwords, and using rootkit suites and other tools
- Recognizing attacks start with monitoring common points of attack that include
  - Web servers, DNS servers, mail servers, firewalls, and test/development systems
- Use auditing to recognize and/or diagnose attacks

Assignments

- Reading: Chapter 12
- Practice 12.6 Challenge Questions

- Turn in Challenge Exercise 12.1 next week