Chapter Objectives

• What is in a security policy
• Mobile device security methods and devices
• To perform operating system and data protection
• How to optimize security for Windows
• To configure wireless security options
• Common techniques used when dealing with irate customers
CompTIA A+ Exam Objectives Covered in This Chapter

801-1.1: Configure and apply BIOS settings.
801-2.5: Compare and contrast wireless networking standards and encryption types.
801-2.6: Install, configure, and deploy a SOHO wireless/wired router using appropriate settings.
801-2.9: Compare and contrast network devices, their functions, and features.
801-3.3: Compare and contrast laptop features.
801-5.3: Given a scenario, demonstrate proper communication and professionalism.
801-5.4: Explain the fundamentals of dealing with prohibited content/activity.
802-1.1: Compare and contrast the features and requirements of various Microsoft operating systems.
802-1.4: Given a scenario, use appropriate operating system features and tools.
CompTIA A+ Exam Objectives Covered in This Chapter

802-1.5: Given a scenario, use Control Panel utilities.
802-1.6: Set up and configure Windows networking on a client/desktop.
802-1.8: Explain the differences among basic OS security settings.
802-1.9: Explain the basics of client-side virtualization.
802-2.1: Apply and use common prevention methods.
802-2.2: Compare and contrast common security threats.
802-2.3: Implement security best practices to secure a workstation.
802-2.4: Given a scenario, use the appropriate data destruction/disposal method.
802-2.5: Given a scenario, secure a SOHO wireless network.
802-2.6: Given a scenario, secure a SOHO wired network.
802-3.3: Compare and contrast methods for securing mobile devices.
802-4.7: Given a scenario, troubleshoot common security issues with appropriate tools and best practices.
Security Policy

- Physical Access
- Antivirus
- Acceptable Use
- Password
- Email Usage
- Remote Access
- Emergency Procedures
Physical Security Devices

- Smart Card
- Key Fob
- RFID (Radio Frequency ID)
- RSA (Rivest Shamir Adleman) Security Token
- TPM (Trusted Platform Module)
- Computer Cage
- Tracking Module
- Privacy Filter
- Mantrap
Protecting the Operating System and Data

- File Systems and Security
- Patches, Updates, and Service Packs
- Antivirus
- Encryption
- BitLocker
- DEP (Data Execution Prevention)
- Passwords
- Auditing
- Permissions

© 2014 Pearson IT Certification
www.pearsonITcertification.com
Internet Security

- Encryption
- Rootkit
- Hijacking
- Spam
- Cookie
- Proxy Server
- Firewall
- Antivirus and Antispyware
- Social Engineering
- Phishing

© 2014 Pearson IT Certification
www.pearsonITcertification.com
# Types of Network Attacks

<table>
<thead>
<tr>
<th>Attack Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
</tr>
<tr>
<td>ARP (Address Resolution Protocol)</td>
</tr>
<tr>
<td>Spoofing</td>
</tr>
<tr>
<td>Backdoor</td>
</tr>
<tr>
<td>Brute Force</td>
</tr>
<tr>
<td>DoS (Denial of Service)</td>
</tr>
<tr>
<td>DDoS (Distributed Denial of Service)</td>
</tr>
<tr>
<td>Reconnaissance</td>
</tr>
<tr>
<td>Replay</td>
</tr>
<tr>
<td>Smurf</td>
</tr>
<tr>
<td>TCP/IP Hijacking</td>
</tr>
<tr>
<td>Vulnerability Scanner</td>
</tr>
</tbody>
</table>

© 2014 Pearson IT Certification
www.pearsonITcertification.com
Security Incidents

- Virus
- Spyware or Grayware
- Phishing
- Child Exploitation
- Software Piracy
Wireless Authentication and Encryption

- Open Authentication
- Shared Key Authentication
- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2
Trust begins with professionalism in your attire, attitude, written communication, and oral communication.

Be honest with the customer.

Do not use or discuss any material you see while in a customer area.

Do not touch or move things or papers in a customer area.

Do what you say you will do.

Every time you step into a customer area or talk to a customer, it might lead to a professional reference, a job recommendation, a job lead, or a promotion. Be professional in all that you do.
A+ Certification Exam Tips

This chapter has information relating to both the 801 and 802 exams and is the most complex chapter because so many security issues need to be experienced in order to know exactly what things to try. As a starting point, be very familiar with the Internet Explorer Internet Options tabs. Review them right before the 802 exam.

Be very familiar with wireless security techniques: default usernames, SSID, encryption, SSID broadcasting, MAC filtering, radio power levels, and static IP addressing.

Know what to do if you happen across prohibited content/data.

Review what to do with security problems such as computer slowdowns, lockups, pop-ups, viruses, malware, and spam.

Know the symptoms of a virus and malware.

For mobile devices, be able to compare and contrast passcode locks, remote wipes, remote backup applications, failed login attempts restrictions, locator apps, antivirus, and patching/OS updates.
A security policy guides a company in security matters. The policy defines such things as physical access, antivirus, acceptable usage of devices and data, password policies, email usage guidelines, remote access strategies, and emergency procedures.

Physical security can include door access, key control, authentication methods including the use of smart cards, key fobs, RFID, biometric devices, physical protection of network devices such as servers, APs, switches, and routers, as well as privacy filters.

BIOS security options include configuring a supervisor/user password, disabling unused ports, disabling USB ports, and disabling device options.

To protect the operating system, use NTFS, and have a plan for updating the operating system, web browser, antivirus, antimalware, and antispyware. Encrypt files and folders as necessary. Use BitLocker and TPM technologies, implement a firewall, and disable AutoRun.

If a computer with sensitive data on the hard drive is to be donated, moved, or sold, perform the following: (1) secure erasing, (2) degaussing, and (3) drilling through drive platters and then destroying the pieces with a hammer.
Chapter Summary

- If virtualization is used, ensure that each virtual machine has adequate protection (firewall, antivirus, antimalware, and antispyware).
- Some virus or malware files are quarantined and must be manually deleted.
- The Windows guest account should be disabled; the administrator account should be renamed and have a strong password. User accounts provide the amount of administration dictated by what the person needs (principle of least privilege).
- Permissions should be assigned appropriately to remotely accessed files and folders. Use either share permissions or NTFS permissions (for more control), but not both on the same network share. If a file is placed in a folder that has permissions, the file inherits the folder permissions. Effective permissions are the bottom-line permissions someone has when group permissions and individual permissions have been granted.
- A hijacked browser can cause a different home page to appear, a particular web page to be displayed, a rootkit or other malware to be installed, different DNS settings to be applied, or a new or updated HOSTS file applied.
- Email applications now protect against spam, but you can also create rules to block messages from a particular source or subject line.
• Cookies store typed information including sign-ons, sites visited, passwords, and data entered through the web browser.

• Internet Explorer can be customized to various levels of alerts and protection.

• When a security incident occurs, identify the issue, report it through the proper channels and to the appropriate authorities, and preserve the data by using a chain-of-custody form.

• On a wireless network, implement encryption and authentication. Change default SSIDs and passwords.

• Secure a mobile device with a PIN, facial recognition, a password, or a passcode/pattern. Secure important data using remote backups to the cloud. Remote data wiping can be configured if the device is compromised or stolen.

• When dealing with a customer, a co-worker, or your boss, maintain your professionalism and do everything you can to build trust.