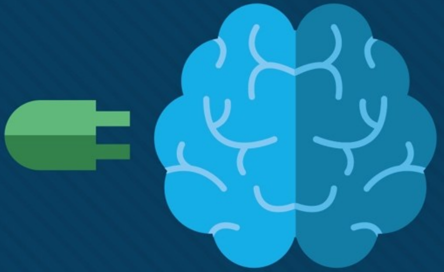


Chapter 13: Security

Instructor Materials

IT Essentials v7.0

Chapter 13: Security

IT Essentials 7.0 Planning Guide

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter 13: Security

IT Essentials v7.0

Chapter 13 - Sections & Objectives

- 13.1 Security Threats
  - Explain security threats.
  - Describe different types of malware.
  - Describe measures that protect against malicious software.
  - Describe different types of network attacks.
  - Describe different social engineering attacks.

- 13.2 Security Procedures
  - Explain security procedures.
  - Explain what a security policy is.
  - Explain physical security measures.
  - Describe measures that protect data.
  - Describe how to destroy data.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter 13 - Sections & Objectives (Cont.)

- 13.3 Securing Windows Workstations
  - Configure basic security settings and policies for end devices.
    - Explain how to secure a workstation.
    - Configure security using the Windows Local Security Policy tool.
    - Manage Windows users and groups.
    - Configure security using the Windows firewall tool.
    - Configure a browser for secure access.
    - Configure security maintenance in Windows.
- 13.4 Wireless Security
  - Configure wireless security.
    - Configure wireless devices for secure communication.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

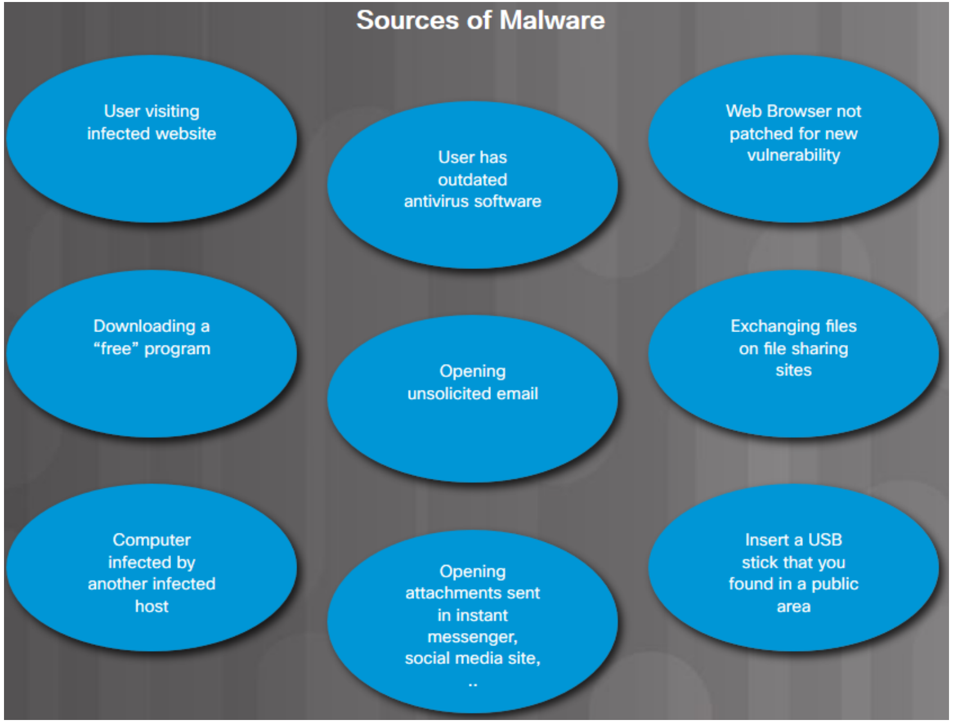
Chapter 13 - Sections & Objectives (Cont.)

- 13.5 Basic Troubleshooting Process for Security
  - Explain how to troubleshoot basic security problems
    - Explain the six steps of the troubleshooting process for security.
    - Describe advanced problems and solutions for security.

13.1 Security Threats

Malware

- There are many types of threats created to disrupt computers and networks.
  - The greatest and most common threat for computers and the data contained on them is malware.
- Malware is typically installed on a computer without user knowledge. Once a host is infected, the malware could:
  - Change the computer configuration.
  - Delete files or corrupt hard drives.
  - Collect information stored on the computer without the user's consent.
  - Open extra windows on the computer or redirect the browser.



Sources of Malware

User visiting infected website

User has outdated antivirus software

Web Browser not patched for new vulnerability

Downloading a "free" program

Opening unsolicited email

Exchanging files on file sharing sites

Computer infected by another infected host

Opening attachments sent in instant messenger, social media site, ..

Insert a USB stick that you found in a public area

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Malware

Viruses and Trojan Horses

- The first and most common type of computer malware is a **virus**.
  - Viruses require human action to propagate and infect other computers.
  - A virus hides by attaching itself to computer code, software, or documents on the computer. When opened, the virus executes and infects the computer.
- Cybercriminals also use **Trojan horses** to compromise hosts.
  - A Trojan horse is a program that looks useful but also carries malicious code.
  - Trojan horses are often provided with free online programs such as computer games.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Malware

Types of Malware

- **Adware** can display unsolicited advertising using pop-up web browser windows, new toolbars, or unexpectedly redirect a webpage to a different website.

- **Ransomware** typically denies a user access to their files by encrypting the files and then displaying a message demanding a ransom for the decryption key.

- **Rootkits** are difficult to detect and are used by cybercriminals to gain admin level access to a computer.

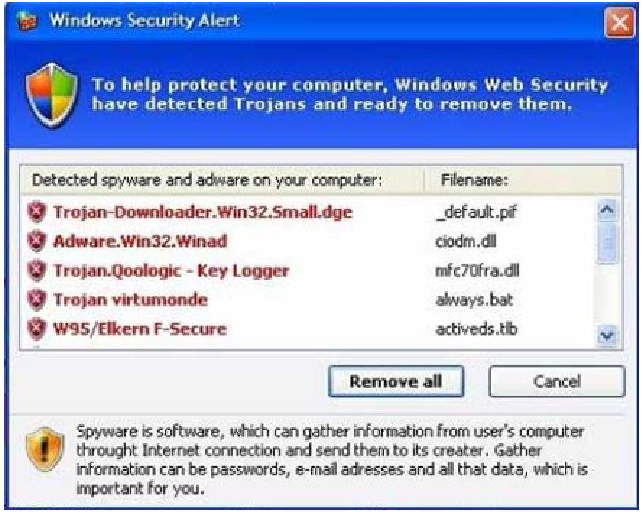
- **Spyware** is similar to adware but is used to gather information about the user and send it back to cybercriminals.

- **Worms** are self-replicating programs that propagate automatically without user action by exploiting vulnerabilities in software.

Preventing Malware

Anti-Malware Programs

- It is important that you protect computers and mobile devices using reputable antivirus software.
- Today, antivirus programs are commonly referred to as anti-malware programs
  - Anti-malware programs can detect and block Trojans, rootkits, ransomware, spyware, keyloggers, and adware programs.
  - Anti-malware programs continuously look for known patterns against a database of known malware signatures.
  - They can also use heuristic malware identification techniques which can detect specific behavior associated with some types of malware.



Windows Security Alert

To help protect your computer, Windows Web Security have detected Trojans and ready to remove them.

Detected spyware and adware on your computer:	Filename:
Trojan-Downloader.Win32.Small.dge	_default.pif
Adware.Win32.Winad	ciodm.dll
Trojan.Qoologic - Key Logger	mfc70fra.dll
Trojan virtumonde	always.bat
W95/Elkern F-Secure	activeds.tlb

Spyware is software, which can gather information from user's computer throught Internet connection and send them to its creater. Gather information can be passwords, e-mail adresses and all that data, which is important for you.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

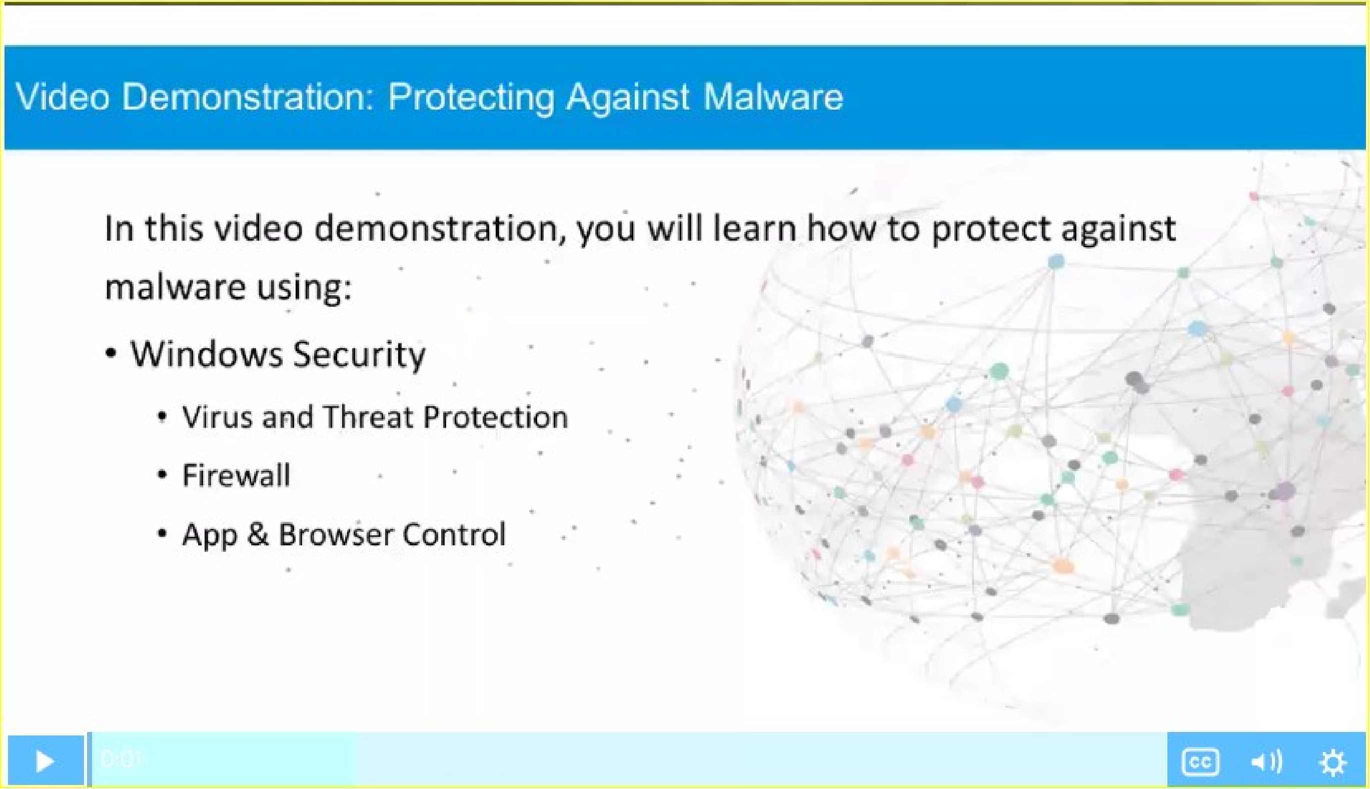
Preventing Malware

Signature File Updates

- New malware is always being developed; therefore, anti-malware software must be updated regularly. This process is often enabled by default.
- Always download the signature files from the manufacturer’s website to make sure the update is authentic and not corrupted by malware.
  - To avoid creating too much traffic at a single website, some manufacturers distribute their signature files for download to multiple download sites. These download sites are called mirrors.
- **CAUTION**: When downloading signature files from a mirror, ensure that the mirror site is a legitimate site. Always link to the mirror site from the manufacturer’s website.

Preventing Malware

Video Explanation – Anti-Malware Programs



Video Demonstration: Protecting Against Malware

In this video demonstration, you will learn how to protect against malware using:

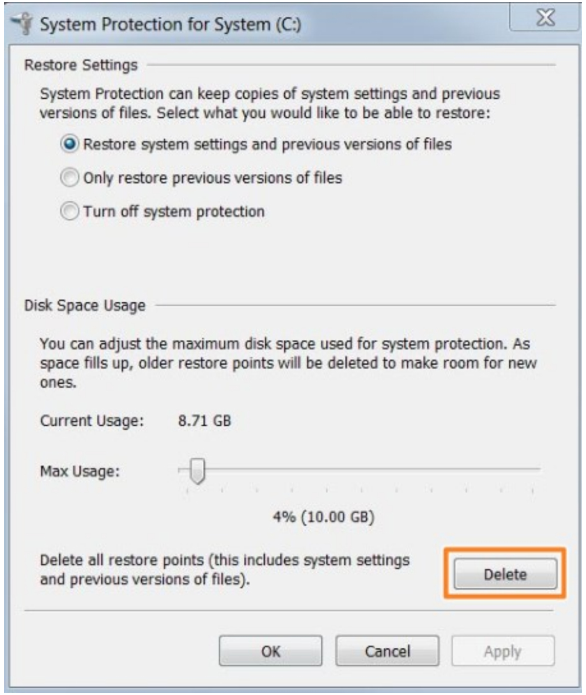
- Windows Security
  - Virus and Threat Protection
  - Firewall
  - App & Browser Control

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Preventing Malware

Remediating Infected Systems

- When a malware protection program detects that a computer is infected, it removes or quarantines the threat. However, the computer is most likely still at risk.
- Many antimalware programs can be set to run on system start before loading Windows.
- Removing malware may require that the computer be rebooted into Safe Mode.
- It may be necessary to contact a specialist to ensure that the computer has been completely cleaned. Otherwise, the computer may need to be reformatted, the operating system reinstalled, and your data recovered from the most recent backups.
- The OS system restore service may include infected files in a restore point. Therefore, after a computer has been cleaned of any malware, the system restore files should be deleted.



System Protection for System (C:)

Restore Settings

System Protection can keep copies of system settings and previous versions of files. Select what you would like to be able to restore:

● Restore system settings and previous versions of files

○ Only restore previous versions of files

○ Turn off system protection

Disk Space Usage

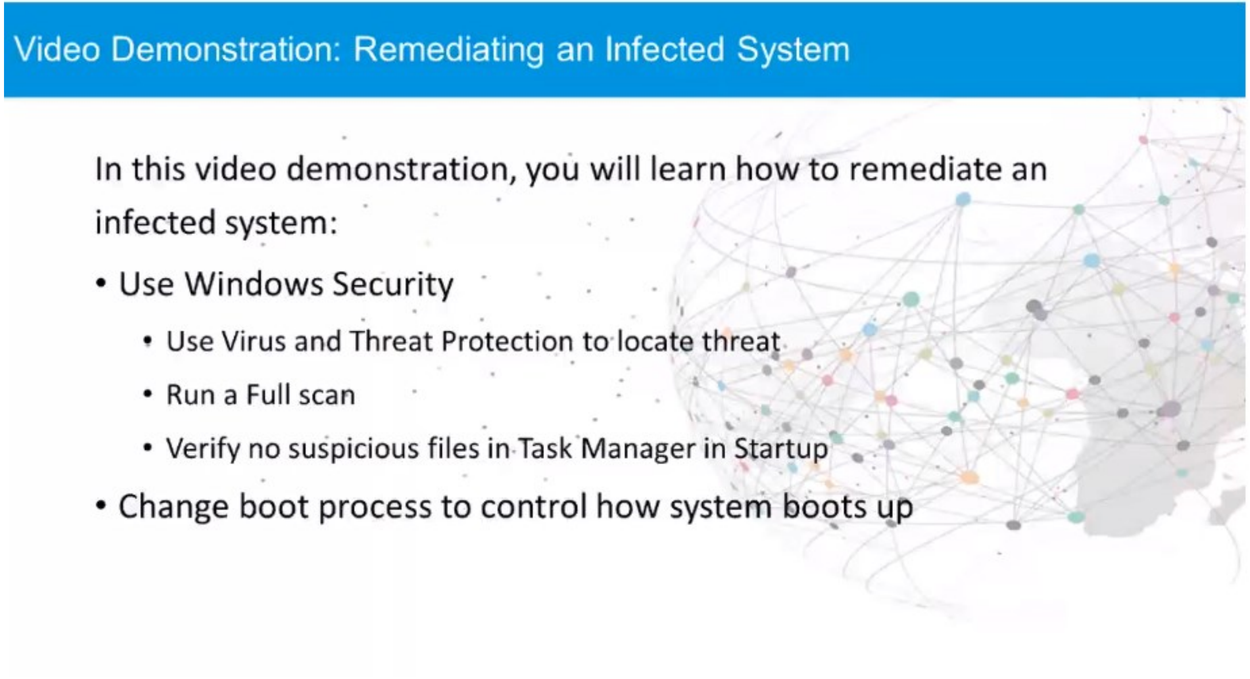
You can adjust the maximum disk space used for system protection. As space fills up, older restore points will be deleted to make room for new ones.

Current Usage: 8.71 GB

Max Usage: 4% (10.00 GB)

Delete all restore points (this includes system settings and previous versions of files).

Video Explanation – Remediating an Infected System



Video Demonstration: Remediating an Infected System

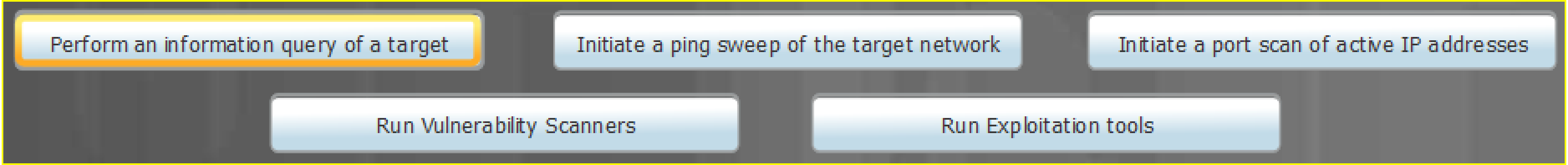
In this video demonstration, you will learn how to remediate an infected system:

- Use Windows Security
  - Use Virus and Threat Protection to locate threat
  - Run a Full scan
  - Verify no suspicious files in Task Manager in Startup
- Change boot process to control how system boots up

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Attacks

Networks Are Targets

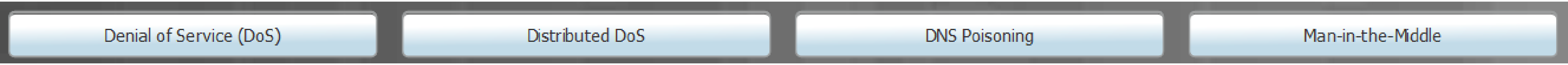

Perform an information query of a target
Initiate a ping sweep of the target network
Initiate a port scan of active IP addresses
Run Vulnerability Scanners
Run Exploitation tools

- Attacker is looking for network information about a target using Google search, whois and other tools.
- Attacker initiates a ping sweep of the discovered target’s public network address to determine which IP addresses are active.
- Attacker determines which services are available on the active port using Nmap, SuperScan and other tools.
- Attacker runs vulnerability scanner to discover the type of applications and OSs running on target host using Nipper, Secuna PSI and other tools.
- Attacker attempts to discover vulnerable services to exploit using Metasploit, Core Impact and other tools.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Attacks

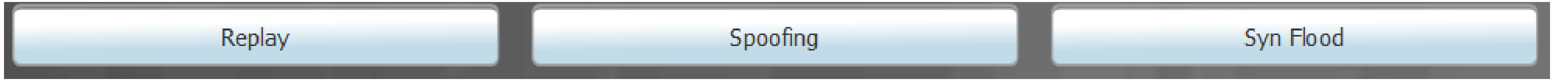
Types of TCP/IP Attacks



- **Denial of Service (DoS)** is an attack where the attacker completely overwhelms a target device with false requests to create a denial of service for legitimate users.
- **Distributed DoS** is an amplified DoS attack using many infected hosts called zombies to overwhelm a target.
- **DNS Poisoning** is an attack where the attacker has successfully infected a host to accept false DNS records pointing to malicious servers.
- **Man-in-the-Middle** is an attack where an attacker intercepts communication between two hosts.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Types of TCP/IP Attacks (Cont.)

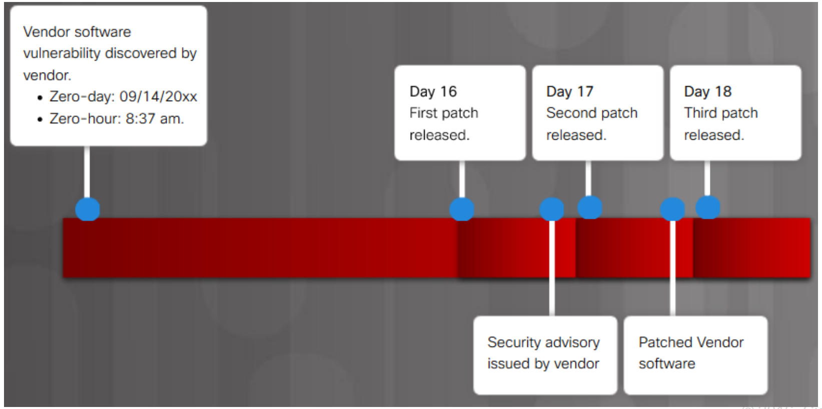


- **Replay** is a type of spoofing attack where the attacker capturs an authenticated packet, alters it, and sends it to the original destination.
- **Spoofing** is an attack where the attacker forges an IP address to gain access to resources.
- **Syn Flood** is a type of DoS attack that exploits the TCP three-way handshake.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Zero-Day

- The following two terms are commonly used to describe when a threat is detected:
  - **Zero-day** – Sometimes also referred to as zero-day attacks, zero-day threat, or zero-day exploit. This is the day that an unknown vulnerability has been discovered by the vendor. The term is a reference to the amount of time that a vendor has had to address the vulnerability.
  - **Zero-hour** – This is the moment when the exploit is discovered.
- The software can be exploited until a patch that addresses the vulnerability is made available.



Vendor software vulnerability discovered by vendor.

- Zero-day: 09/14/20xx
- Zero-hour: 8:37 am.

Day 16 First patch released.

Day 17 Second patch released.

Day 18 Third patch released.

Security advisory issued by vendor

Patched Vendor software

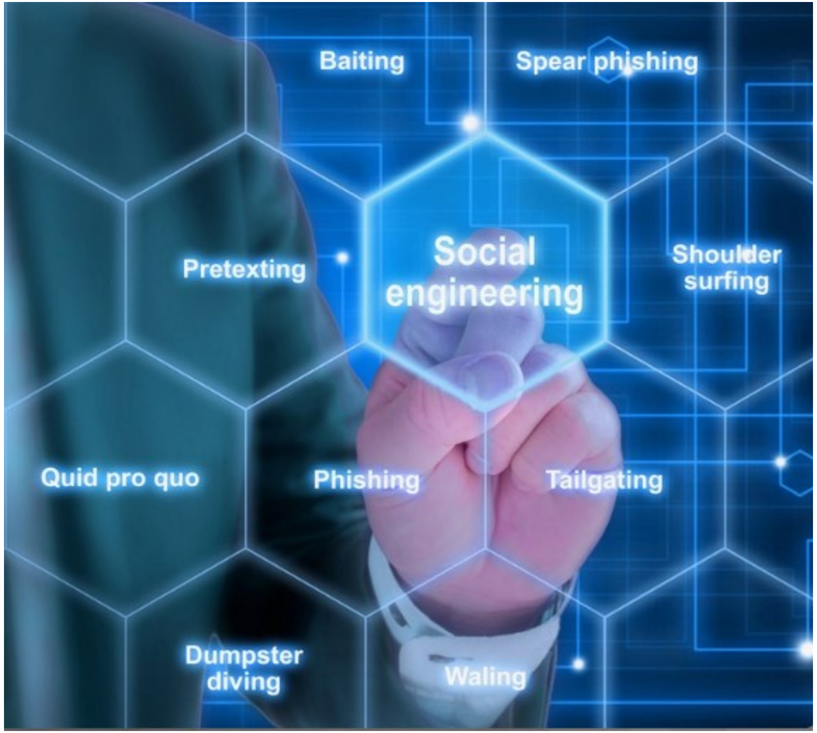
Protecting Against Network Attacks

- There is no single solution to protect against all TCP/IP or zero-day attacks.
- One solution is to use a defense-in-depth approach, also known as a layered approach, to security.
  - This requires a combination of networking devices and services working together in tandem.
- All network devices including the router and switches must be secured to prevent attackers from tampering with the devices.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Social Engineering

- Cybercriminals use social engineering techniques to deceive unsuspecting targets into revealing confidential information.
- Social engineering is an access attack that attempts to manipulate individuals into performing actions or divulging confidential information.
- Social engineers often rely on human nature and people’s willingness to be helpful.
- **Note**: Social engineering is often used in conjunction with other network attacks.



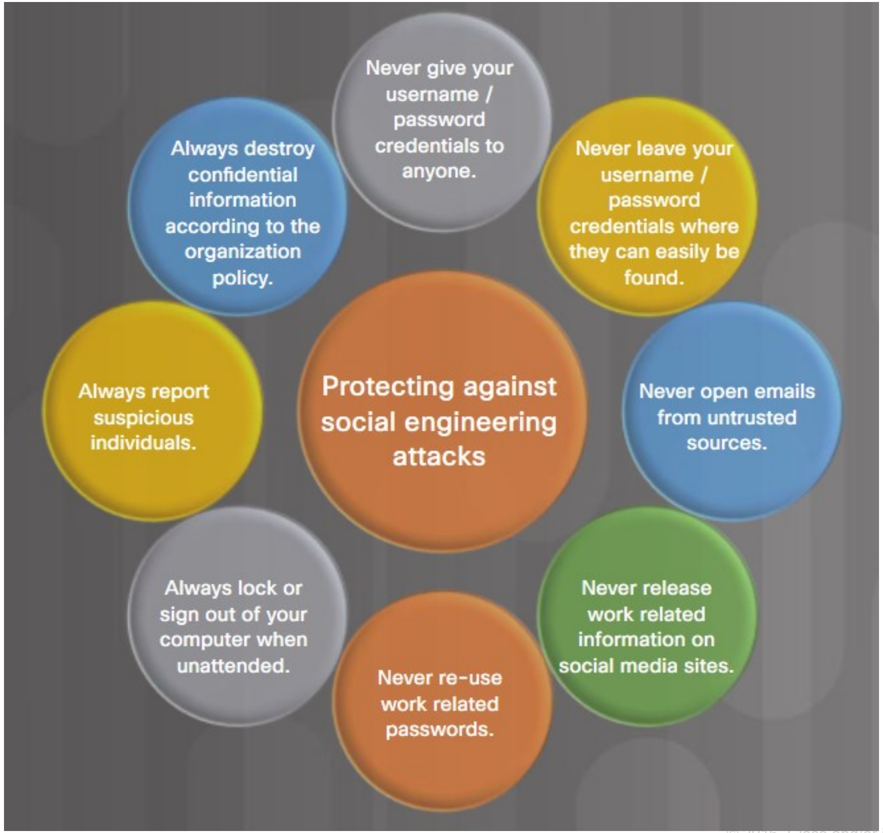
Social Engineering Techniques

- **Pretexting** - An attacker pretends to need personal data in order to confirm the identity of the recipient.
- **Phishing** - An attacker sends fraudulent email disguised as being from a trusted source.
- **Spear Phishing** - An attacker creates a targeted phishing attack for a specific individual or organization.
- **Spam** – Unsolicited email which often contains harmful links, malware, or deceptive content.
- **Something for Something** – When an attacker requests personal information in exchange for something.
- **Baiting** - An attacker leaves a malware infected flash drive in a public location.
- **Impersonation** – An attacker pretends to be someone they are not.
- **Tailgating** – An attacker follows an authorized person into a secure area.
- **Shoulder surfing** - An attacker looks over someone’s shoulder to steal information.
- **Dumpster Diving** - An attacker searches through trash for confidential information.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Social Engineering Attacks

Protecting Against Social Engineering



Protecting against social engineering attacks

Never give your username / password credentials to anyone.

Never leave your username / password credentials where they can easily be found.

Never open emails from untrusted sources.

Never release work related information on social media sites.

Never re-use work related passwords.

Always lock or sign out of your computer when unattended.

Always report suspicious individuals.

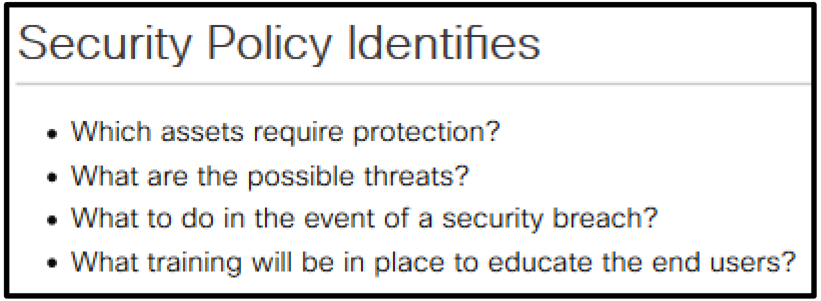
Always destroy confidential information according to the organization policy.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.2 Security Procedures

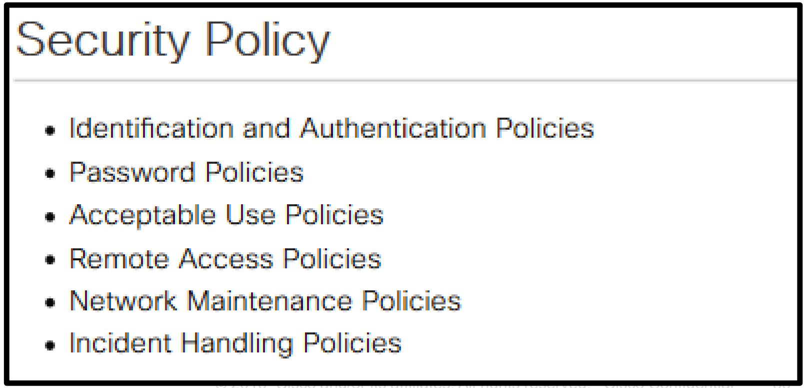
What is a Security Policy

- A security policy is:
  - a set of security objectives that ensure the security of a network, the data, and the computers in an organization.
  - a constantly evolving document based on changes in technology, business, and employee requirements.
  - usually created by a committee with members consisting of management and IT staff.
- It is up to the IT staff to implement security policy specifications in the network.



Security Policy Identifies

- Which assets require protection?
- What are the possible threats?
- What to do in the event of a security breach?
- What training will be in place to educate the end users?



Security Policy

- Identification and Authentication Policies
- Password Policies
- Acceptable Use Policies
- Remote Access Policies
- Network Maintenance Policies
- Incident Handling Policies

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Policy

Security Policy Category

Identification and Authentication Policies
Password Policies
Acceptable Use Policies
Remote Access Policies
Network Maintenance Policies
Incident Handling Policies

- **Identification and Authentication Policies** – Outlines verification procedures and specifies authorized persons that can have access to network resources.
- **Password Policies** – Ensures passwords meet minimum requirements and are changed regularly.
- **Acceptable Use Policies** – Identifies network resources and usages that are acceptable to the organization and may include ramifications for policy violation.
- **Remote Access Policies** – Identifies how remote users access a network and what is accessible?
- **Network Maintenance Policies** – Specifies network device operating systems and end-user application update procedures.
- **Incident Handling Policies** – Describes how security incidents are handled.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Securing Devices and Data

- The goal of the security policy is to ensure a safe network environment and to protect assets.
- An organization’s assets include their data, employees, and physical devices such as computers and network equipment.
- The security policy should identify hardware and equipment that can be used to prevent theft, vandalism, and data loss.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

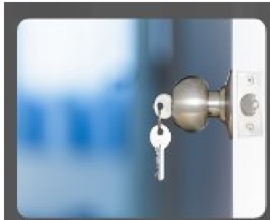
Physical Security

- Physical security is as important as data security.
  - For example, if a computer is taken from an organization, the data is also stolen or worse, lost.
- Physical security involves securing:
  - Access to an organization’s premise
  - Access to restricted areas
  - The computing and network infrastructure

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Policy

Security Policy Category


Conventional lock

Deadbolt lock

Electronic lock

Token-based lock

Biometric lock

Multifactor lock

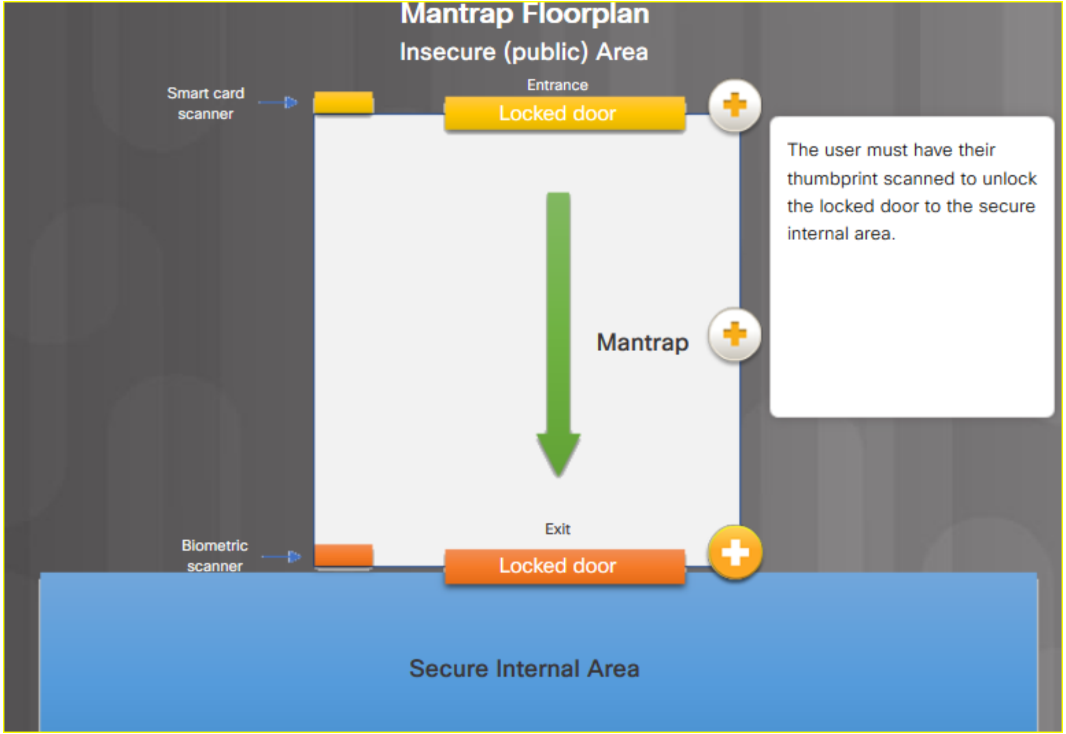
- **Conventional lock** – Unlocked by entering the required key into the door handle mechanism.
- **Deadbolt lock** – Unlocked by entering the required key into a lock separate from the door handle mechanism.
- **Electronic lock** – Unlocked by entering a secret combination code or PIN into the keypad.
- **Token-based lock** – Unlocked by swiping a secure card or by using a near proximity reader to detect a smart card or wireless key fob.
- **Biometric lock** – Unlocked by using a biometric scanner such as a thumbprint reader.
- **Multifactor lock** – A lock that uses a combination of the above mechanisms.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Protecting Physical Equipment

Mantraps

- In high-security environments, mantraps are often used to limit access to restricted areas and to prevent tailgating.
  - A mantrap is a small room with two doors, one of which must be closed before the other can be opened.
  - Typically, a person enters the mantrap by unlocking one door. Once inside the mantrap, the first door closes and then the user must unlock the second door to enter the restricted area.



The user must have their thumbprint scanned to unlock the locked door to the secure internal area.

Securing Computers and Network Hardware

- Organizations must protect their computing and network infrastructure.
  - This includes cabling, telecommunication equipment, and network devices.
- There are several methods of physically protecting computer and networking equipment.
- Network equipment should only be installed in secured areas. As well, all cabling should be enclosed within conduits or routed inside walls to prevent unauthorized access or tampering.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

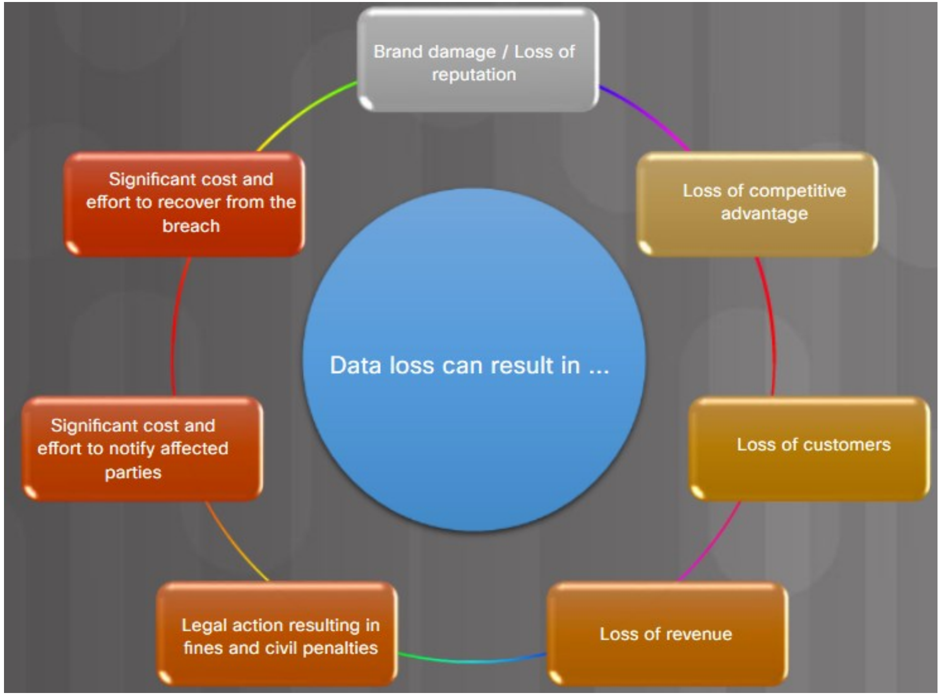
Securing Computers and Network Hardware (Cont.)

- Factors that determine the most effective equipment to use to secure equipment and data include:
  - How the equipment is used
  - Where the computer equipment is located
  - What type of user access to data is required
- For example:
  - A computer in a busy public place requires additional protection from theft and vandalism.
  - In a busy call center, a server may need to be secured in a locked equipment room.
  - While using a laptop in a public place, a security dongle and key fob ensure that the computer locks if the user and laptop are separated.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Data – Your Greatest Asset

- Data is likely to be an organization's most valuable assets. Organizational data may include research and development, sales, financial, human resource, employee, and customer data.
- Data can be lost or damaged in circumstances such as theft, equipment failure, or a disaster.
- Data loss or exfiltration are terms used to describe when data is lost, stolen, or leaked to the public.
- Data can be protected from data loss using data backups, file/folder encryption and permissions.



Data loss can result in ...

- Brand damage / Loss of reputation
- Loss of competitive advantage
- Loss of customers
- Loss of revenue
- Legal action resulting in fines and civil penalties
- Significant cost and effort to notify affected parties
- Significant cost and effort to recover from the breach

Data Backups

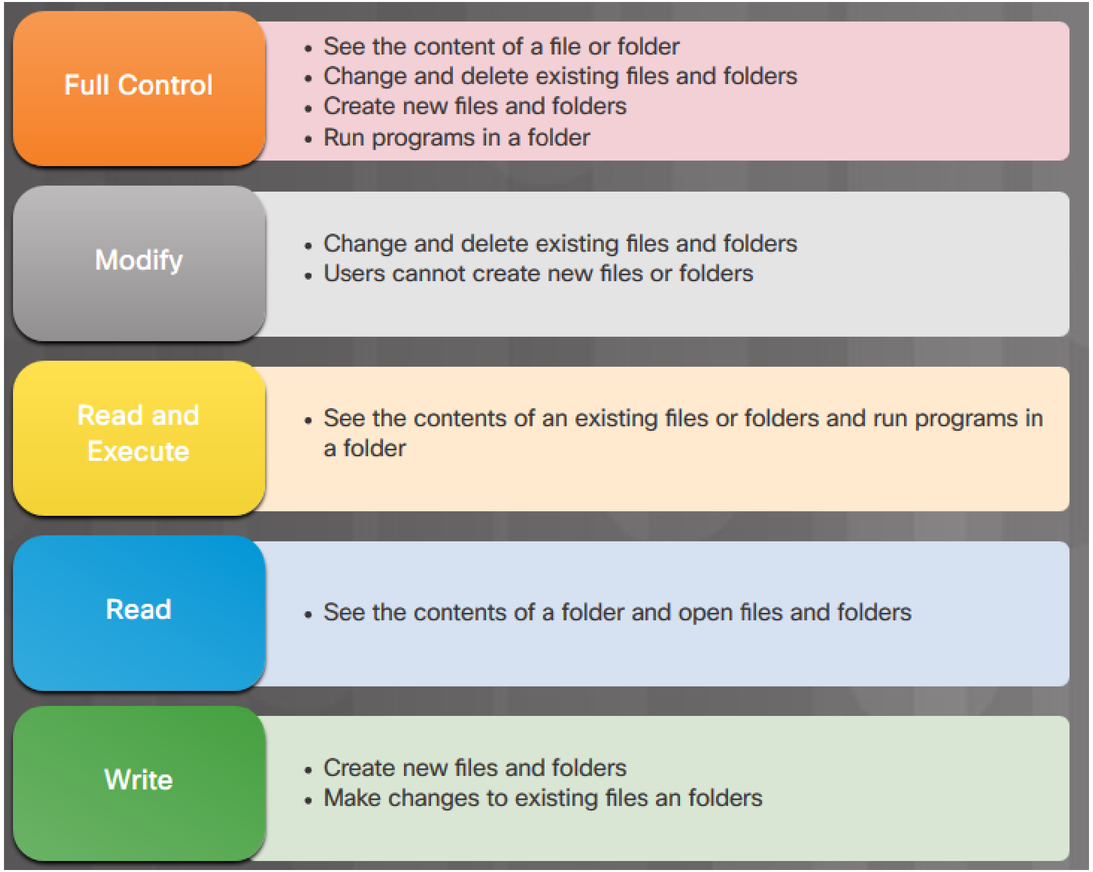
- Backing up data is one of the most effective ways of protecting against data loss.
  - A data backup stores a copy of the information on a computer to removable backup media
  - Data backups should be performed on a regular basis as identified in the security policy.
  - Data backups are usually stored offsite to protect the backup media if anything happens to the main facility.
- Windows hosts have a backup and restore utility.
- macOS hosts have a **Time Machine** utility to perform backup and restore functions.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Protecting Data

File and Folder Permissions

- Permissions are rules you configure to limit folder or file access for an individual or for a group of users.
- Users should be limited to only the resources they need in a computer or on a network.
  - This is known as the principle of least privilege.

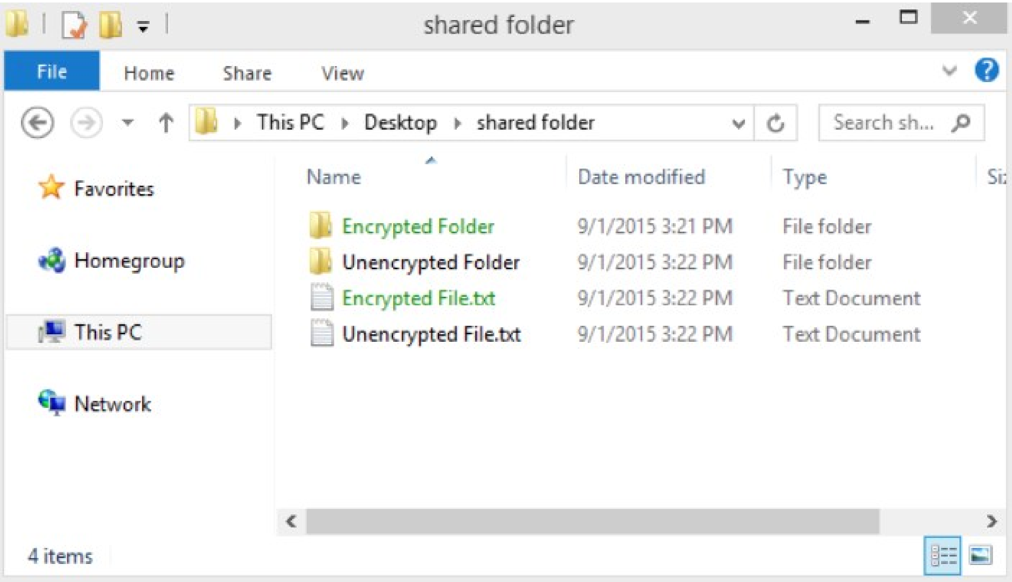


Full Control	• See the content of a file or folder • Change and delete existing files and folders • Create new files and folders • Run programs in a folder
Modify	• Change and delete existing files and folders • Users cannot create new files or folders
Read and Execute	• See the contents of an existing files or folders and run programs in a folder
Read	• See the contents of a folder and open files and folders
Write	• Create new files and folders • Make changes to existing files an folders

Protecting Data

File and Folder Encryption

- Encryption is often used to protect data.
  - Encryption is where data is transformed using a complicated algorithm to make it unreadable.
  - A special key must be used to return the unreadable information back into readable data.
- Encrypting File System (EFS) is a Windows feature that can encrypt data.
  - EFS is directly linked to a specific user account.
    - Only the user that encrypted the data will be able to access it after it has been encrypted.



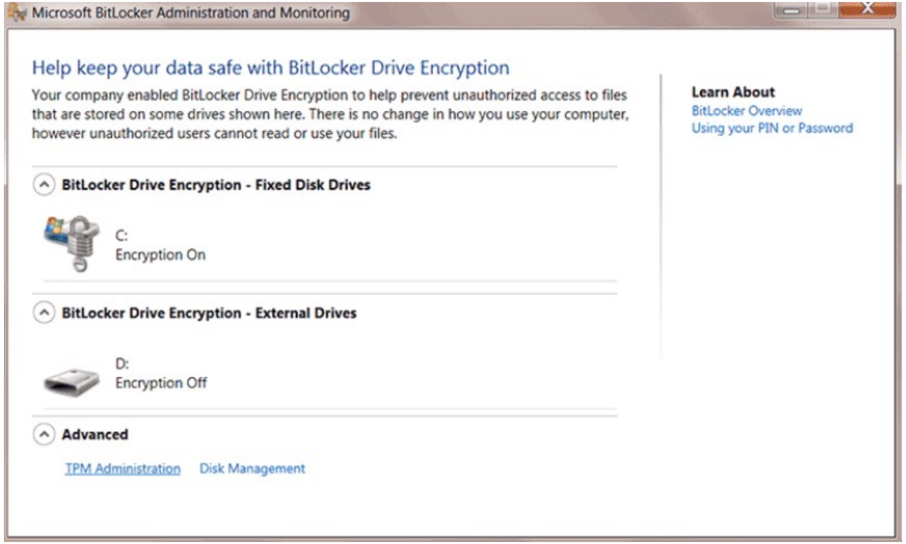
Name	Date modified	Type	Si
Encrypted Folder	9/1/2015 3:21 PM	File folder	
Unencrypted Folder	9/1/2015 3:22 PM	File folder	
Encrypted File.txt	9/1/2015 3:22 PM	Text Document	
Unencrypted File.txt	9/1/2015 3:22 PM	Text Document	

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Protecting Data

Windows BitLocker and BitLocker to Go

- You can encrypt an entire hard drive using a feature called BitLocker.
- To use BitLocker:
  - At least two volumes must be present on a hard disk.
  - The Trusted Platform Module (TPM) must be enabled in BIOS.
    - The TPM is a specialized chip installed on the motherboard that stores encryption keys, digital certificates, and passwords.
- BitLocker encryption can also be used with removable drives by using BitLocker To Go.
  - BitLocker To Go does not use a TPM chip, but still provides encryption and requires a password.



Microsoft BitLocker Administration and Monitoring

Help keep your data safe with BitLocker Drive Encryption

Your company enabled BitLocker Drive Encryption to help prevent unauthorized access to files that are stored on some drives shown here. There is no change in how you use your computer, however unauthorized users cannot read or use your files.

BitLocker Drive Encryption - Fixed Disk Drives

C:
Encryption On

BitLocker Drive Encryption - External Drives

D:
Encryption Off

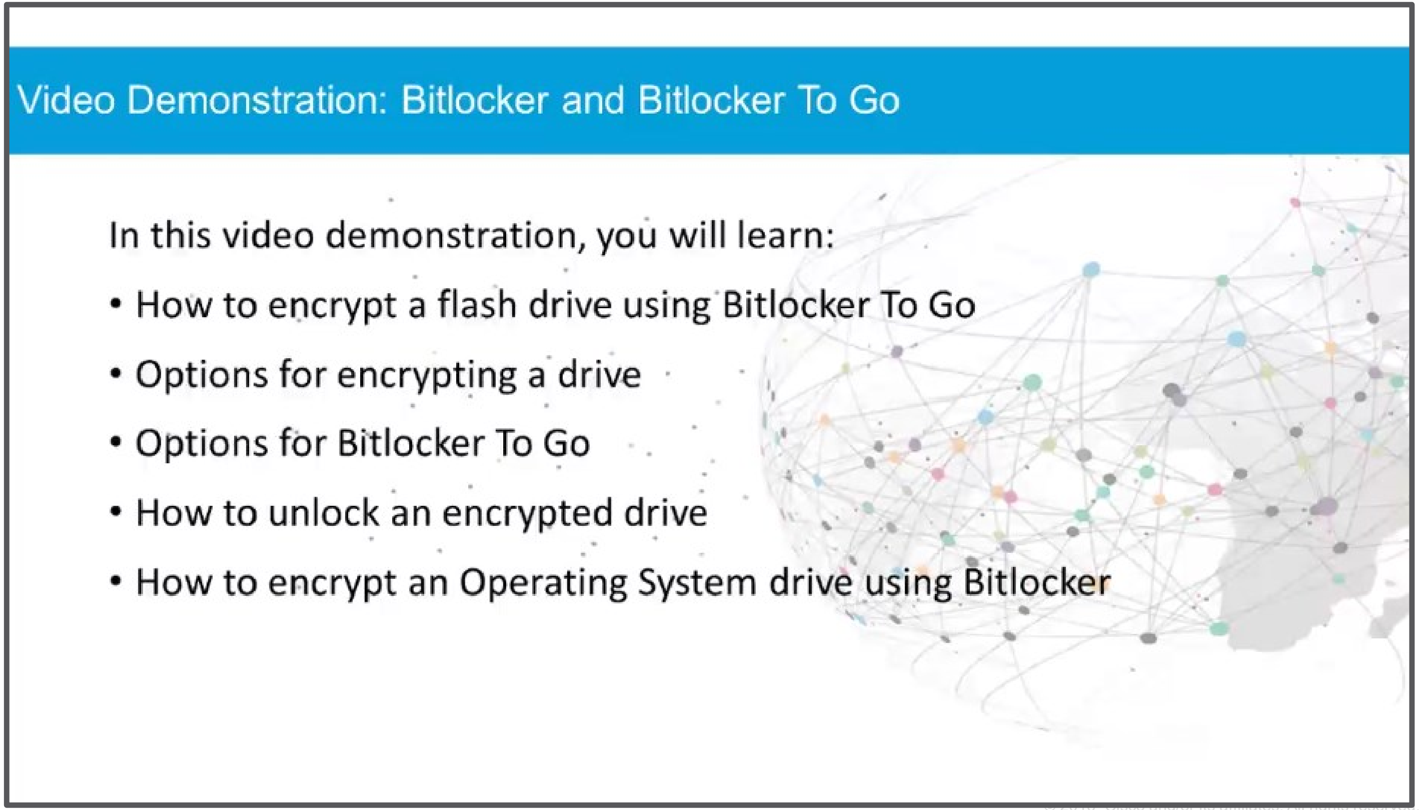
Advanced

TPM Administration   Disk Management

Learn About
BitLocker Overview
Using your PIN or Password

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Video Demonstration – BitLocker and BitLocker To Go



Video Demonstration: Bitlocker and Bitlocker To Go

In this video demonstration, you will learn:

- How to encrypt a flash drive using Bitlocker To Go
- Options for encrypting a drive
- Options for Bitlocker To Go
- How to unlock an encrypted drive
- How to encrypt an Operating System drive using Bitlocker

© 2016 Cisco and/or its affiliates. All rights reserved.

Lab – Bitlocker and Bitlocker To Go

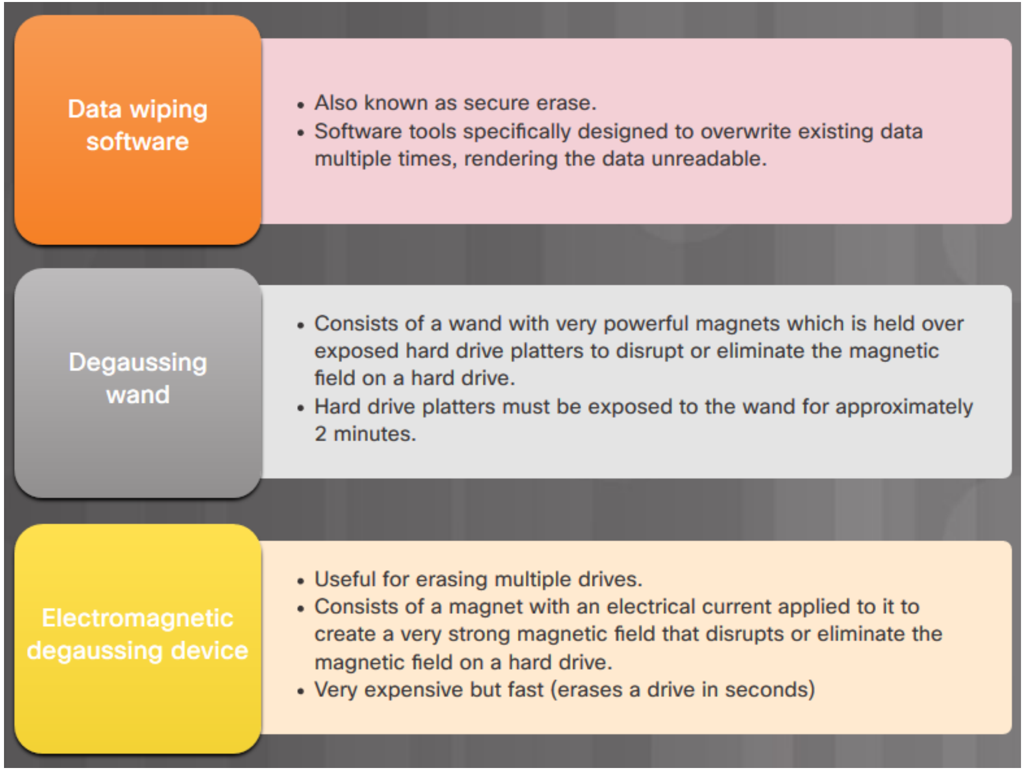
In this lab, you will enable BitLocker encryption on a removable data drive and on the computer system drive.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Data Destruction

Data Wiping Magnetic Media

- Protecting data also includes removing files from storage devices when they are no longer needed.
- Simply deleting files or reformatting the drive may not be enough to ensure your privacy.
- Software tools can be used to recover folders, files, and even entire partitions.
  - For this reason, storage media should be fully erased using one or more of the methods listed in the figure.



Data wiping software

- Also known as secure erase.
- Software tools specifically designed to overwrite existing data multiple times, rendering the data unreadable.

Degaussing wand

- Consists of a wand with very powerful magnets which is held over exposed hard drive platters to disrupt or eliminate the magnetic field on a hard drive.
- Hard drive platters must be exposed to the wand for approximately 2 minutes.

Electromagnetic degaussing device

- Useful for erasing multiple drives.
- Consists of a magnet with an electrical current applied to it to create a very strong magnetic field that disrupts or eliminate the magnetic field on a hard drive.
- Very expensive but fast (erases a drive in seconds)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

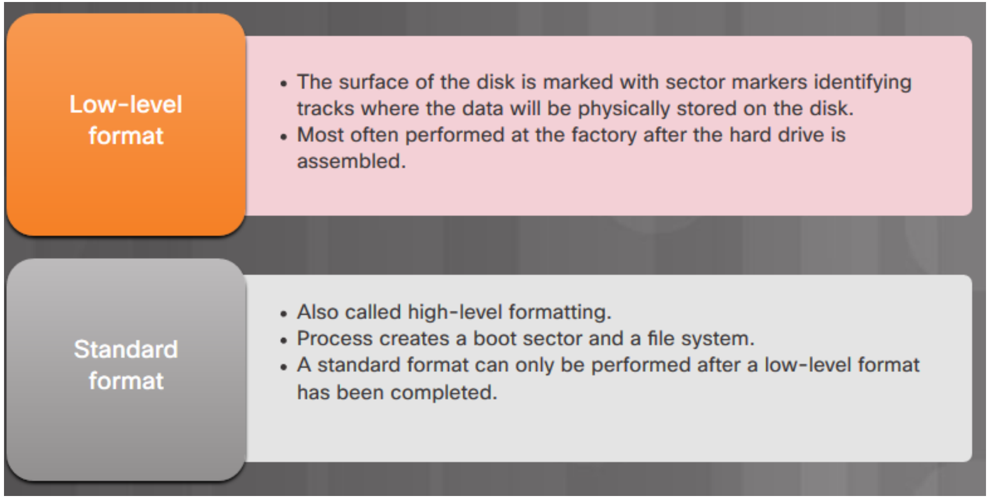
Data Wiping Other Media

- SSDs are comprised of flash memory instead of magnetic platters.
  - Common techniques used for erasing data such as degaussing are not effective with flash memory.
  - Perform a secure erase to fully ensure that data cannot be recovered from an SSD and hybrid SSD.
- Other storage media and documents (e.g., optical disks, eMMC, USB sticks) must also be destroyed.
  - Use a shredding machine or incinerator that is designed to destroy documents and each type of media.
- When thinking about what devices must be wiped or destroyed, remember that devices besides computers and mobile devices store data.
  - Printers and multifunction devices may also contain a hard drive that caches printed or scanned documents. This caching feature can be turned off in some instances, or the device needs to be wiped on a regular basis.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hard Drive Recycling and Destruction

- When a storage media is no longer needed, the media can either be:
  - **Destroyed** - Destroying the hard drive fully ensures that data cannot be recovered from a hard drive.
  - **Recycled** - Hard drives that have been wiped can be reused in other computers. The drive can be reformatted, and a new operating system installed.



Low-level format

- The surface of the disk is marked with sector markers identifying tracks where the data will be physically stored on the disk.
- Most often performed at the factory after the hard drive is assembled.

Standard format

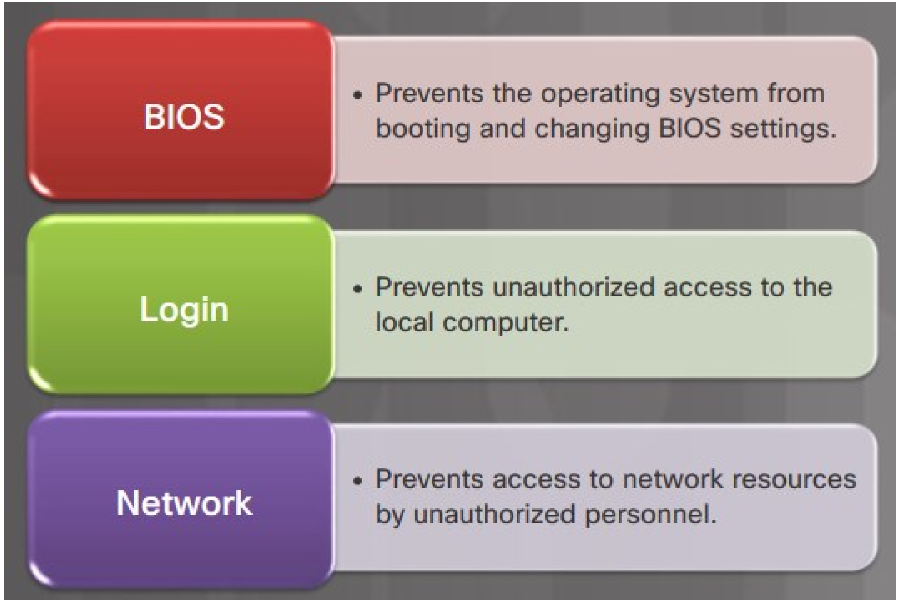
- Also called high-level formatting.
- Process creates a boot sector and a file system.
- A standard format can only be performed after a low-level format has been completed.

13.3 Securing Windows Workstations

Securing a Workstation

Securing a Computer

- Computers and workstations should be secured from theft.
  - Lock your workstation when you are not present to prevent unauthorized users from stealing or accessing local computer and network resources.
  - If you must leave a computer in an open public area, cable locks should be used to deter theft.
  - Use a privacy screen to protect the information displayed on your screen from prying eyes
- Access to your computer must also be protected.
  - There are three levels of password protection that can be used on a computer.



BIOS

- Prevents the operating system from booting and changing BIOS settings.

Login

- Prevents unauthorized access to the local computer.

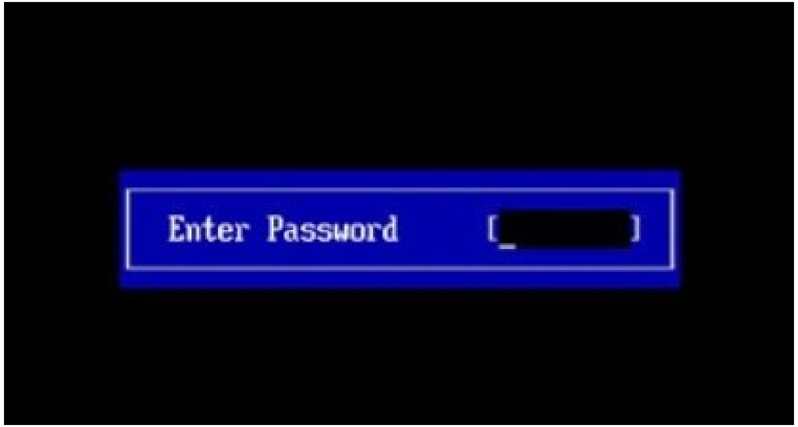
Network

- Prevents access to network resources by unauthorized personnel.

Securing a Workstation

Securing BIOS

- A Windows, Linux, or Mac login password can be bypassed.
- Setting a BIOS or UEFI password prevents someone from altering the configured setting and may also prevent someone from booting the computer.
- All users, regardless of user account, share BIOS passwords.
- UEFI passwords can be set on a per-user basis, however, an authentication server is required.



Enter Password [_]

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Securing a Workstation

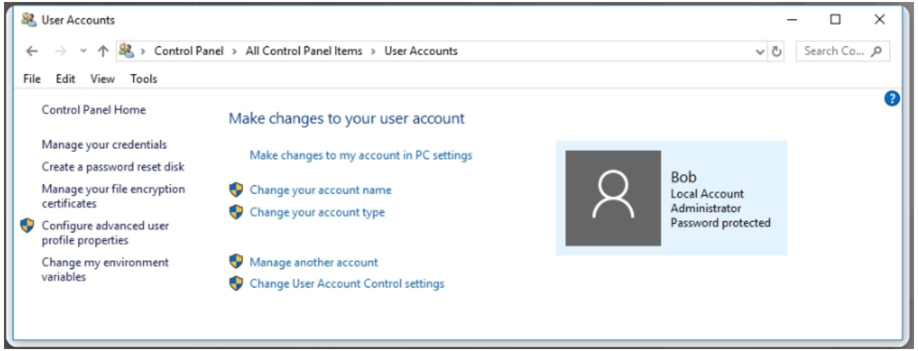
Securing Windows Login

- The most common type of password protection is the computer login.
- Depending on your computer system, Windows 10 may also support other sign-in options. Specifically, Windows 10 supports the following sign-in options:
  - **Windows Hello** – Feature that enables Windows to use facial recognition or use your fingerprint to access Windows.
  - **PIN** – Enter a pre-configured PIN number to access Windows.
  - **Picture password** - You choose a picture and gestures to use with the picture to create a unique password.
  - **Dynamic lock** – Feature makes Windows lock when a pre-paired device such as a cell phone goes out of range of the PC.

Securing a Workstation

Local Password Management

- Password management for stand-alone Windows computers can be set locally using the Windows **User Accounts** tool.
  - To create, remove, or modify a password in Windows, use **Control Panel > User Accounts**
- It is also important to make sure that computers are secure when users are away.
  - A security policy should contain a rule about requiring a computer to lock when the screensaver starts.
  - In all versions of Windows, use **Control Panel > Personalization > Screen Saver**
    - Choose a screen saver and a wait time, and then select the **On resume, display logon screen** option.


User Accounts

Control Panel › All Control Panel Items › User Accounts

Search Co...

File Edit View Tools

Control Panel Home

Manage your credentials

Create a password reset disk

Manage your file encryption certificates

Configure advanced user profile properties

Change my environment variables

Make changes to your user account

Make changes to my account in PC settings

Change your account name

Change your account type

Manage another account

Change User Account Control settings

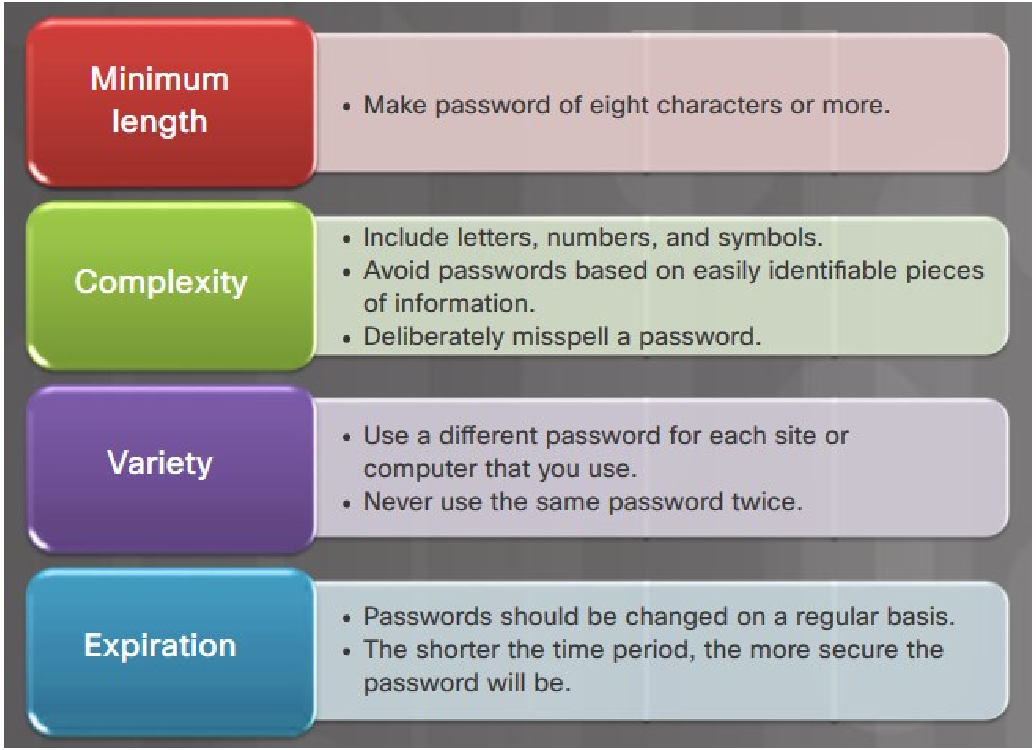
Bob
Local Account
Administrator
Password protected

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Securing a Workstation

Usernames and Passwords

- Usernames, like passwords, are an important piece of information and should not be revealed.
- Password guidelines are an important component of a security policy.
- Any user that must log on to a computer or connect to a network resource should be required to have a password.
- Passwords help prevent theft of data and malicious acts.
- Passwords also help to confirm that the logging of events is valid by ensuring that the user is the correct person.



Minimum length	• Make password of eight characters or more.
Complexity	• Include letters, numbers, and symbols. • Avoid passwords based on easily identifiable pieces of information. • Deliberately misspell a password.
Variety	• Use a different password for each site or computer that you use. • Never use the same password twice.
Expiration	• Passwords should be changed on a regular basis. • The shorter the time period, the more secure the password will be.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Windows Local Security Policy

- In most networks that use Windows computers, Active Directory is configured with Domains on a Windows Server.
  - Windows computers are members of a domain.
  - The administrator configures a Domain Security Policy that applies to all computers that join.
  - Account policies are automatically set when a user logs in to Windows.
- For stand-alone computers that are not part of an Active Directory domain, the Windows Local Security Policy can be used to enforce security settings.
  - To access Local Security Policy in Windows 7 and Vista, use **Start > Control Panel > Administrative Tools > Local Security Policy**.
  - In Windows 8, 8.1, and Windows 10, use **Search > secpol.msc** and then click **secpol**.
- **Note**: In all versions of Windows, you can use the **Run** command **secpol.msc** to open the Local Security Policy tool.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Windows Local Security Policy

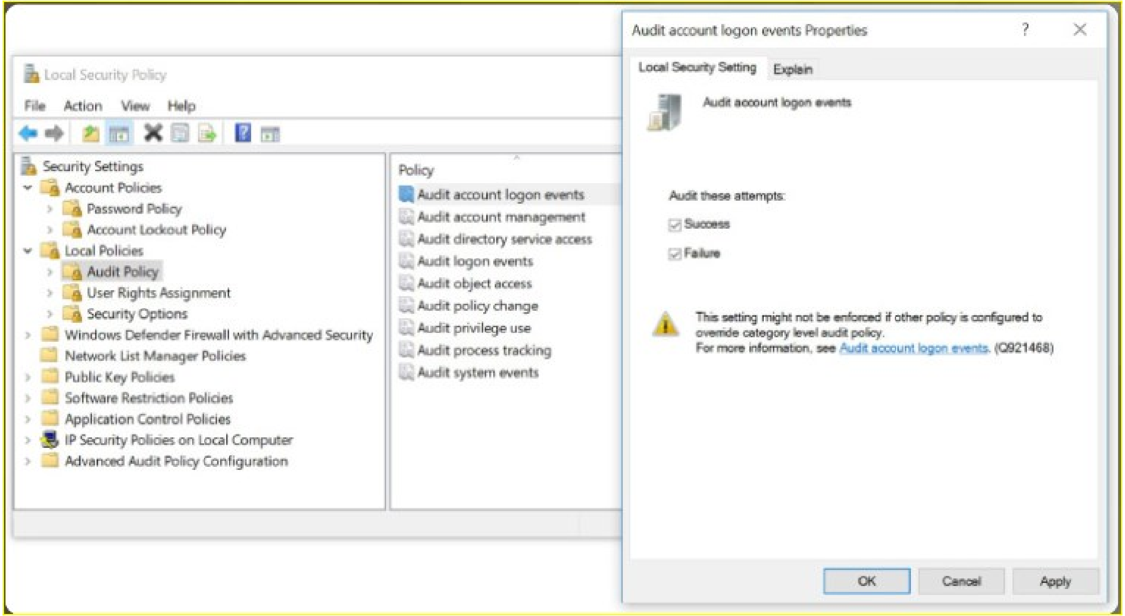
Account Policies Security Settings

- The security policy will identify the password policies required.
- The Windows local security policy can be used to implement the password policies.
  - Use **Account Policies > Password Policy** to enforce password requirements
  - Use **Account Policies > Account Lockout Policy** to prevent brute-force attacks
    - This Account Lockout Policy would also protect against a dictionary attack. This is a type of brute-force attack that attempts every word in a dictionary hoping to gain access.

Windows Local Security Policy

Local Policies Security Settings

- The Local Policy in the Local Security Policy is used to configure audit policies, user rights policies, and security policies.
  - It can also be used to log successful and unsuccessful login attempts.
- Use the **Local Policies > Audit Policy** to enable auditing.



Audit account logon events

Audit these attempts:

☑ Success

☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account logon events. (Q921468)

Exporting the Local Security Policy

- An administrator may need to implement an extensive local policy for user rights and security options. This policy most likely would need to be replicated on each system.
- To help simplify this process, the **Local Security Policy** can be exported and copied to other Windows hosts.
- The steps to replicate a Local Security Policy on other computers are:
    1. Use the **Action > Export List…** feature to export the policy of a secure host.
    2. Save the policy with a name, such as **workstation.inf**. to external media.
    3. Then import the Local Security Policy file to other stand-alone computers.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Configure Windows Local Security Policy

In this lab, you will configure Windows Local Security Policy. You will modify password requirements, enable auditing, configure some user rights, and set some security options. You will then use Event Manager to view logged information.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

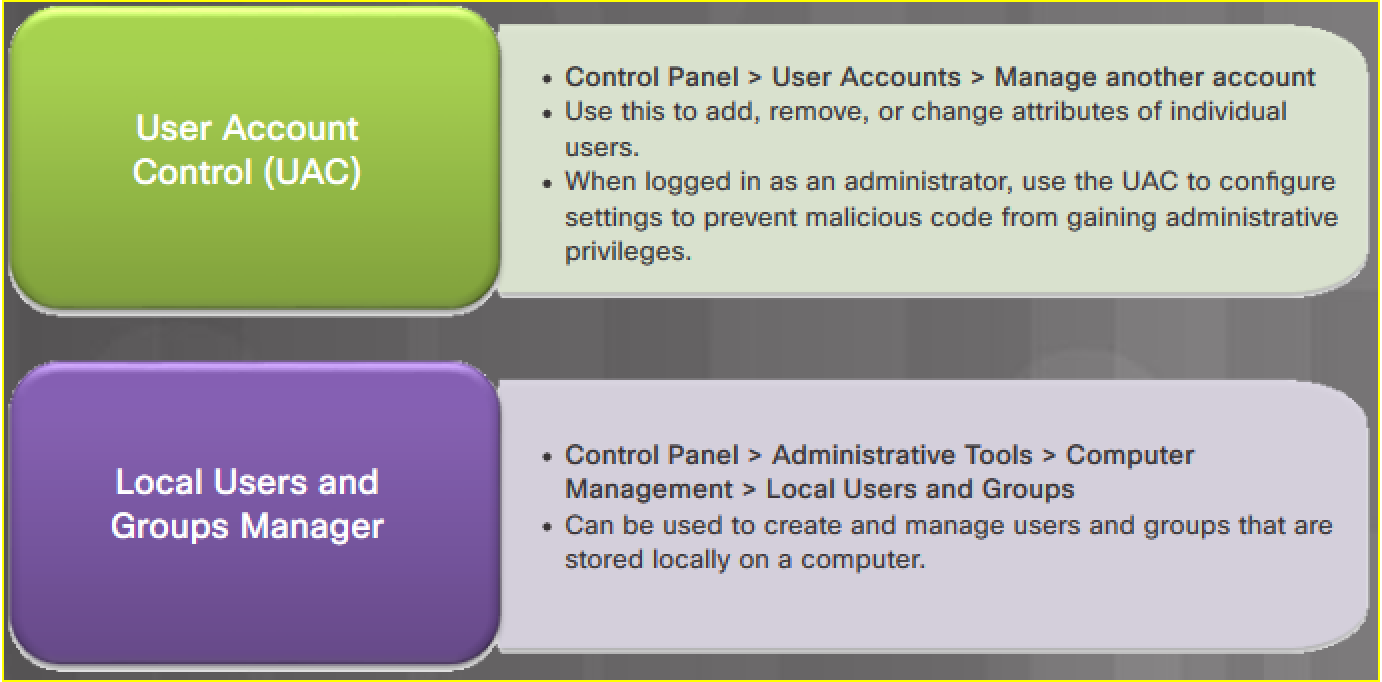
Managing Users and Groups

Maintaining Accounts

- **Terminating Employee Access** – When an employee leaves an organization, Immediately disable the account, or change login credentials.
- **Guest Access** – Special guest account for temps and guests with additional privileges can be created and disabled as required.
- **Track Login Times** – Allow employee login only during specified hours of the day, and block logins the rest of the day.
- **Log Failed Login Attempts** – Configure a specified number of times a user can attempt to login.
- **Idle Timeout and Screen Lock** – Configure an idle timer to automatically log the user out. User must log back in to unlock the screen.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Managing Users Account Tools and User Account Tasks



User Account Control (UAC)

- Control Panel > User Accounts > Manage another account
- Use this to add, remove, or change attributes of individual users.
- When logged in as an administrator, use the UAC to configure settings to prevent malicious code from gaining administrative privileges.

Local Users and Groups Manager

- Control Panel > Administrative Tools > Computer Management > Local Users and Groups
- Can be used to create and manage users and groups that are stored locally on a computer.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Local Users and Groups Manager

- The Local Users and Groups tool can limit the ability of users and groups to perform certain actions by assigning rights and permissions
- To configure all of the users and groups on a computer using the **Local Users and Groups Manager** tools, type **lusrmgr.msc** in the Search box, or Run Line utility.
  - The **Local Users and Groups > Users** window displays current user accounts on the computer.
- Double-clicking a user or right-clicking and choosing **Properties** opens the user properties window:
  - change the user options defined when the user was created
  - lock an account
  - assign a user to a group
  - control which folders the user has access to.
  - To add a user, click the **Action** menu and select **New User**.
  - Here you can assign a username, full name, description, and account options.

Managing Groups

- Users can be assigned to groups for easier management.
- The Local Users and Groups Manager tool is used to manage local groups on a Windows computer.
  - Use **Control Panel > Administrative Tools > Computer Management > Local Users and Groups** to open the Local Users and Groups Manager.
  - From the Local Users and Groups window, double-click **Groups** to list all of the local groups on the computer.
- Double click a group to view its properties.
- To create a new group, click the **Action > New Group** to open the **New Group** window
  - Here you can create new groups and assign users to them.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Managing Users and Groups

Active Directory Users and Computers

- While local accounts are stored in the in the Local Security Accounts database of a local machine, domain accounts are stored in the Active Directory on a Windows Server Domain Controller (DC).
- Only domain administrators are allowed to create domain accounts on the Domain Controller.
  - Domain accounts are accessible from any computer joined to the domain.
- The Active Directory is a database of all computers, users, and services in an Active Directory domain.
  - The Active Directory Users and Computers console on Windows server is used to manage Active Directory users, groups, and Organizational Units (OUs).
    - Organizational units provide a way to subdivide a domain into smaller administrative units.
- Creating a new group account in active directory is similar to creating a new user.
  - Open Active directory Users and Computers and select the container that will house the group, click **Action**, click **New** and then click **Group** and fill in the group details and click **OK**.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Managing Users and Groups

Lab – Configure Users and Groups in Windows

In this lab, you will create users and groups and delete users using the Local Users and Groups Manager. You will also assign group and user permission to the folders.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Firewalls

- A firewall protects computers and networks by preventing undesirable traffic from entering internal networks.
- A firewall can allow outside users controlled access to specific services.
- Firewall services can be provided as follows:
  - **Host-based firewall** – Using software such as Windows Defender Firewall.
  - **Small office home office (SOHO)** – Network-based solution using a home or small office wireless router.
  - **Small to medium-sized organization** - Network-based solution using a dedicated device such as a Cisco Adaptive Security Appliance (ASA) or enabled on a Cisco Integrated Services Router (ISR).
  - The focus of this section is on the host-based firewall solution using Windows Firewall.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Software Firewalls

- A software firewall is a program that provides firewall services on a computer to allow or deny traffic to the computer.
  - A software firewall applies a set of rules to data transmissions through inspection and filtering of data packets.
- Windows Firewall is an example of a software firewall that helps prevent cybercriminals and malware from gaining access to your computer.
  - It is installed by default when the Windows OS is installed.
    - **Note**: In Windows 10 the Windows Firewall was renamed to Windows Defender Firewall. In this section, Windows Firewall includes Windows Defender Firewall.
- Windows Firewall settings are configured using the Windows Firewall window.
  - To change Windows Firewall settings, you must have administrator privileges to open the Windows Firewall window.
  - To open the Windows Firewall window, use **Control Panel > Windows Firewall**.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Windows Firewall

- Windows Firewall has a standard set of inbound and outbound rules that are enabled depending on the location of the connected network.
  - Firewall rules can be enabled for a private network, a guest or public network, or a corporate domain network.
- From the Windows Firewall window, you can enable or disable Windows Firewall, change notification settings, allow apps through the firewall, configure advanced settings, or restore firewall defaults.
- If you wish to use a different software firewall, you will need to disable Windows Firewall.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Windows Firewall

Configuring Exceptions in Windows Firewall

- You can allow or deny access to specific programs or ports from the Windows Firewall window.
- To configure exceptions and allow or block applications or ports, click on **Allow an app or feature through the Windows Firewall** to open the allowed apps window and be able to:
  - Add an allowed program or port
  - Change an allowed program or port
  - Remove an allowed program or port

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Windows Firewall with Advanced Security

- Another Windows tool that is available to provide even greater access control with Windows Firewall policies is the Windows Firewall with Advanced Security.
  - It is called Windows Defender Firewall with Advanced Security in Windows 10.
- To open it, from the Windows Firewall window, click on **Advanced settings** to open it.
  - **Note**: Alternatively, enter **wf.msc** in the search box and press enter.
- Windows Defender Firewall with Advanced Security provides these features:
  - **Inbound and Outbound Rules** – Configure inbound rules that are applied to incoming internet traffic and outbound rules which are applied to traffic leaving your computer.
  - **Connection Security Rules** – Secures traffic between two computers and requires that both computers have the same rules defined and enabled.
  - **Monitoring** –Displays the firewall inbound or outbound active rules or any active connection security rules.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Configure Windows Firewall

In this lab, you will explore the Windows Firewall and configure some advanced settings.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Web Security

- Web browsers are not only used for web browsing, they are also now used to run other applications including Microsoft 365, Google docs, interface for remote access SSL users, and more.
- To help support these additional features, browsers use plug-ins to support other content.
  - However, some of these plug-ins may also introduce security problems.
- Browsers are targets and should be secured.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Web Security

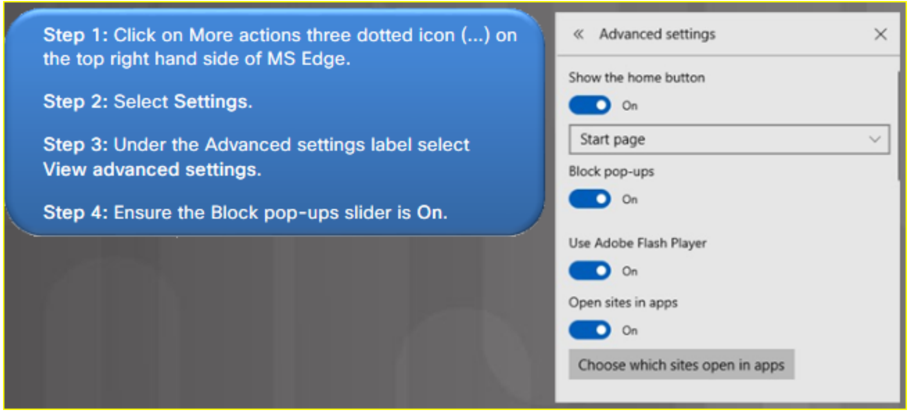
InPrivate Browsing

- Web browsers retain information about the web pages that you visit, the searches that you perform, and other identifiable information including usernames, passwords, and more.
- The information retained by web browsers can be recovered and exploited to steal your identity, your money, or change your passwords on important accounts.
- To improve security when using a public computer, always:
  - **Clear your browsing history** – All web browser have a way to clear their browsing history, cookies, files, and more.
  - **Use the InPrivate mode** – Using an InPrivate browser temporarily stores files and cookies and deletes them when the InPrivate session has ended.
- For Internet Explorer 11, use **Tools > InPrivate Browsing**
  - **Note**: As an alternative press **Ctrl+Shift+P** to open an InPrivate window.

Web Security

Pop-up Blocker

- Pop-ups are initiated while browsing, such as a link on a page that opens a pop-up to deliver additional information or a close-up of a picture.
- Some pop-ups are initiated by a website or advertiser and are often unwanted or annoying.
- Most web browsers offer the ability to block pop-up windows.
  - This enables a user to limit or block most of the pop-ups that occur while browsing the web.
  - To enable the Internet Explorer 11 Pop-up Blocker feature, use **Tools > Pop-up Blocker > Turn on Pop-up Blocker**.



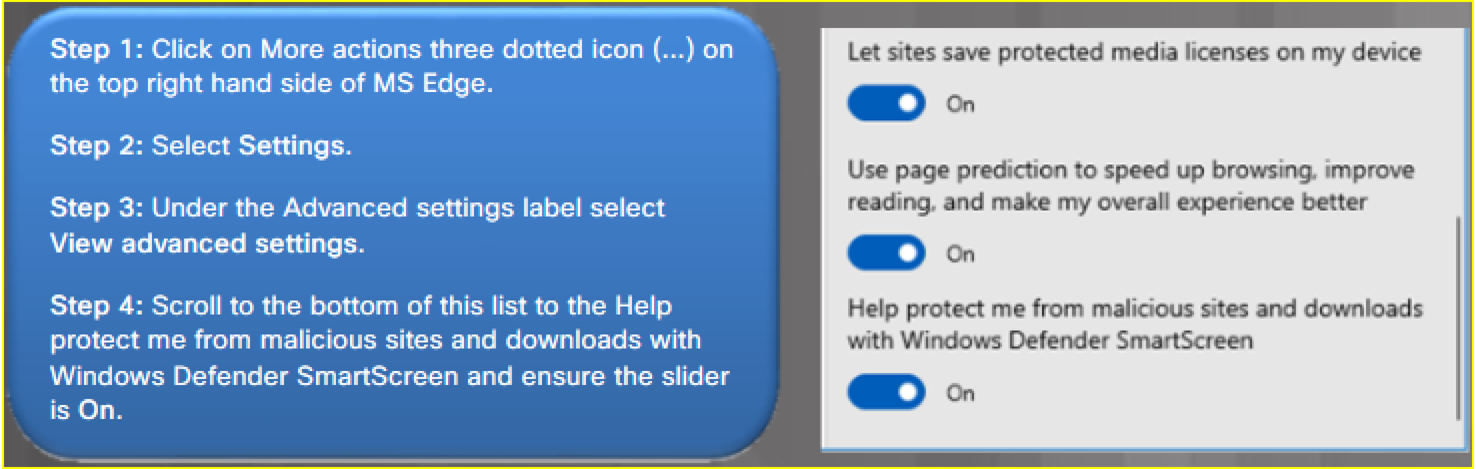
Step 1: Click on More actions three dotted icon (...) on the top right hand side of MS Edge.

Step 2: Select Settings.

Step 3: Under the Advanced settings label select View advanced settings.

Step 4: Ensure the Block pop-ups slider is On.

SmartScreen Filter



Step 1: Click on More actions three dotted icon (...) on the top right hand side of MS Edge.

Step 2: Select Settings.

Step 3: Under the Advanced settings label select View advanced settings.

Step 4: Scroll to the bottom of this list to the Help protect me from malicious sites and downloads with Windows Defender SmartScreen and ensure the slider is On.

Let sites save protected media licenses on my device

On

Use page prediction to speed up browsing, improve reading, and make my overall experience better

On

Help protect me from malicious sites and downloads with Windows Defender SmartScreen

On

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

ActiveX Filtering

- Some web browsers may require you to install an ActiveX control.
  - ActiveX controls can be used for malicious reasons.
- When ActiveX filtering is enabled, you can choose which websites are allowed to run ActiveX controls.
  - Sites that are not approved cannot run these controls, and the browser does not show notifications for you to install or enable them.
- To enable ActiveX filtering in Internet Explorer 11, use **Tools > ActiveX Filtering**.
- To view a website that contains ActiveX content when ActiveX filtering is enabled, click the blue **ActiveX Filtering** icon in the address bar, and click **Turn off ActiveX Filtering**.
  - After viewing the content, you can turn ActiveX filtering for the website back on by following the same steps.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Maintenance

Restrictive Settings

- Devices often come with security features that are not enabled or the security features use default settings.
  - Default permissive settings may leave devices exposed to attackers.
- Many devices now ship with restrictive settings and must be configured to enable access.
- It is your responsibility to secure devices and configure restrictive settings whenever possible.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Disable Auto-Play

- Older Windows hosts used AutoRun to simplify the user experience.
  - When new media (e.g., flash drive, CD, or DVD drive) is inserted into the computer, AutoRun would automatically look for a file named **autorun.inf** and execute it.
  - Malicious users used this feature to infect hosts.
- Newer Windows hosts now use AutoPlay.
- AutoPlay provides additional controls and can prompt the user to choose an action based on the content of the new media.
  - Use the **Control Panel > AutoPlay** window, to open the AutoPlay window and configure the actions associated with specific media.
- The most secure solution is to turn off AutoPlay.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Operating System Service Packs and Security Patches

- Patches are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack.
  - Manufacturers can combine patches and upgrades into a comprehensive update application called a service pack.
- It is critical to apply security patches and OS updates whenever possible.
- Windows routinely checks the Windows Update website for high-priority updates that can help protect a computer from the latest security threats.
  - Depending on the setting you choose, Windows automatically downloads and installs any high-priority updates that your computer needs or notifies you as these updates become available.

13.4 Configure Wireless Security

Common Communication Encryption Types

- Communication between two computers may require secure communication.
- There are two major requirements:
  - The first requirement is that received information has not been altered by someone who has intercepted the message.
  - The second is that anyone who can intercept the message is unable to read it.
- The following technologies accomplish these requirements:
  - Hash encoding
  - Symmetric encryption
  - Asymmetric encryption

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Common Communication Encryption Types (Cont.)

- Hash encoding, or hashing, ensures the integrity of the message.
  - This means that the message is not corrupt nor has it been tampered with during transmission.
  - Hashing uses a mathematical function to create a numeric value, called a message digest that is unique to the data
  - The most popular hashing algorithm is Secure Hash Algorithm (SHA), which is replacing the older Message Digest 5 (MD5) algorithm.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Common Communication Encryption Types (Cont.)

- Symmetric encryption ensures the confidentiality of the message.
  - If an encrypted message is intercepted, it cannot be understood. It can only be decrypted (i.e., read) using the password (i.e., key) that it was encrypted with.
  - Symmetric encryption requires both sides of an encrypted conversation to use an identical encryption key to encode and decode the data.
  - Advanced Encryption Standard (AES) and the older Triple Data Encryption Algorithm (3DES) are examples of symmetric encryption.
- Asymmetric encryption also ensures confidentiality of the message.
  - It requires two keys, a private key and a public key.
  - The public key can be widely distributed, including emailing in plain text or posting on the web.
  - The private key is kept by an individual and must not be disclosed to any other party.
  - RSA is the most popular example of asymmetric encryption.

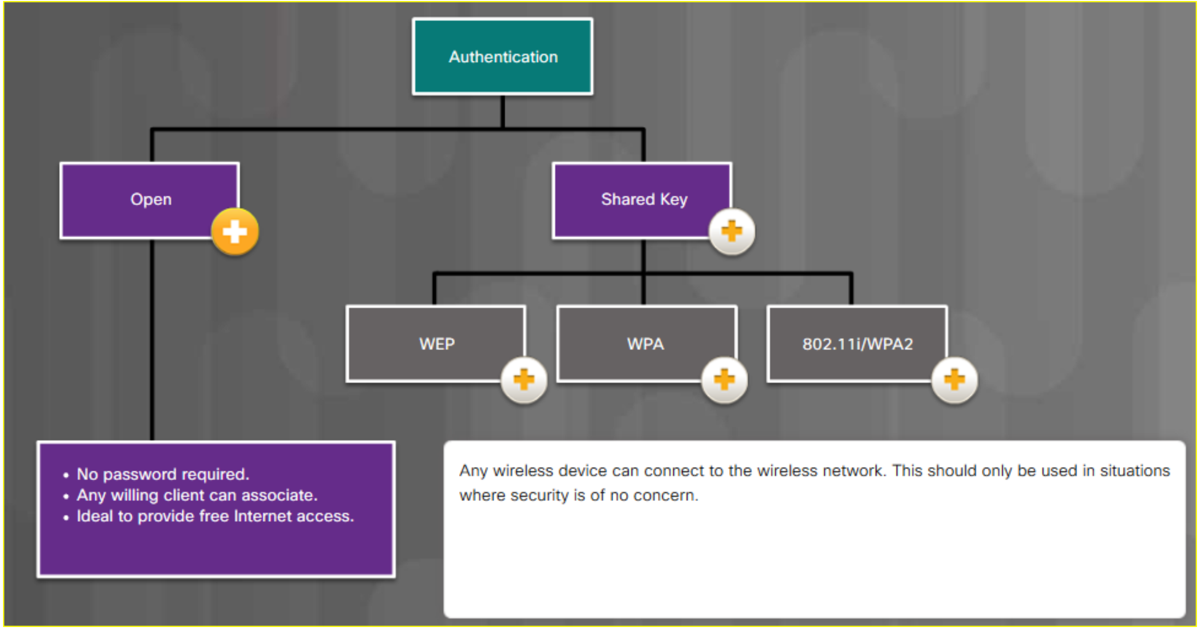
Service Set Identifiers

- The Service Set Identifier (SSID) is the name of the wireless network.
  - A wireless router or access point broadcasts the SSID by default so that devices can detect the wireless network.
- If the SSID broadcast setting has been disabled on a wireless router or access point, users must manually enter the SSID on wireless clients to connect to the wireless network.
  - Disabling the SSID broadcast provides very little security:
    - Someone who knows the SSID of the wireless network can manually enter it.
    - A wireless network will also broadcast the SSID during a computer scan.
    - A SSID can also be intercepted in transit.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authentication Methods

- A Shared Key provides mechanisms to authenticate and decrypt data between a wireless client and AP of wireless router.
- WEP stands for Wired Equivalent Privacy.
- WPA stands for Wi-Fi Protected Access.
- IEEE 802.11i/WPA2 is the current industry standard for securing WLANs. Both use the Advanced Encryption Standard (AES).



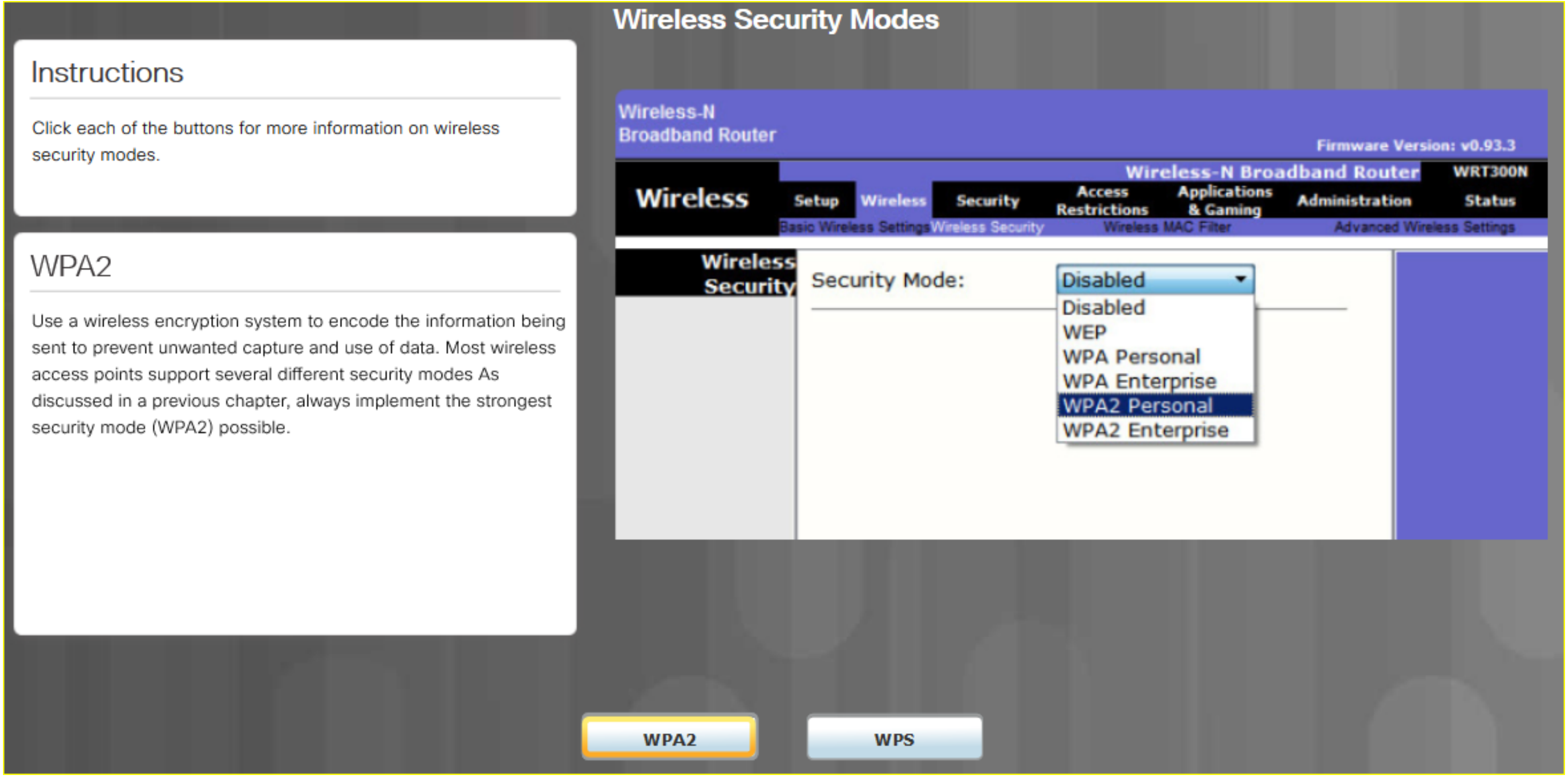
- No password required.
- Any willing client can associate.
- Ideal to provide free Internet access.

Any wireless device can connect to the wireless network. This should only be used in situations where security is of no concern.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configure Wireless Security

Wireless Security Modes



Wireless Security Modes

Instructions

Click each of the buttons for more information on wireless security modes.

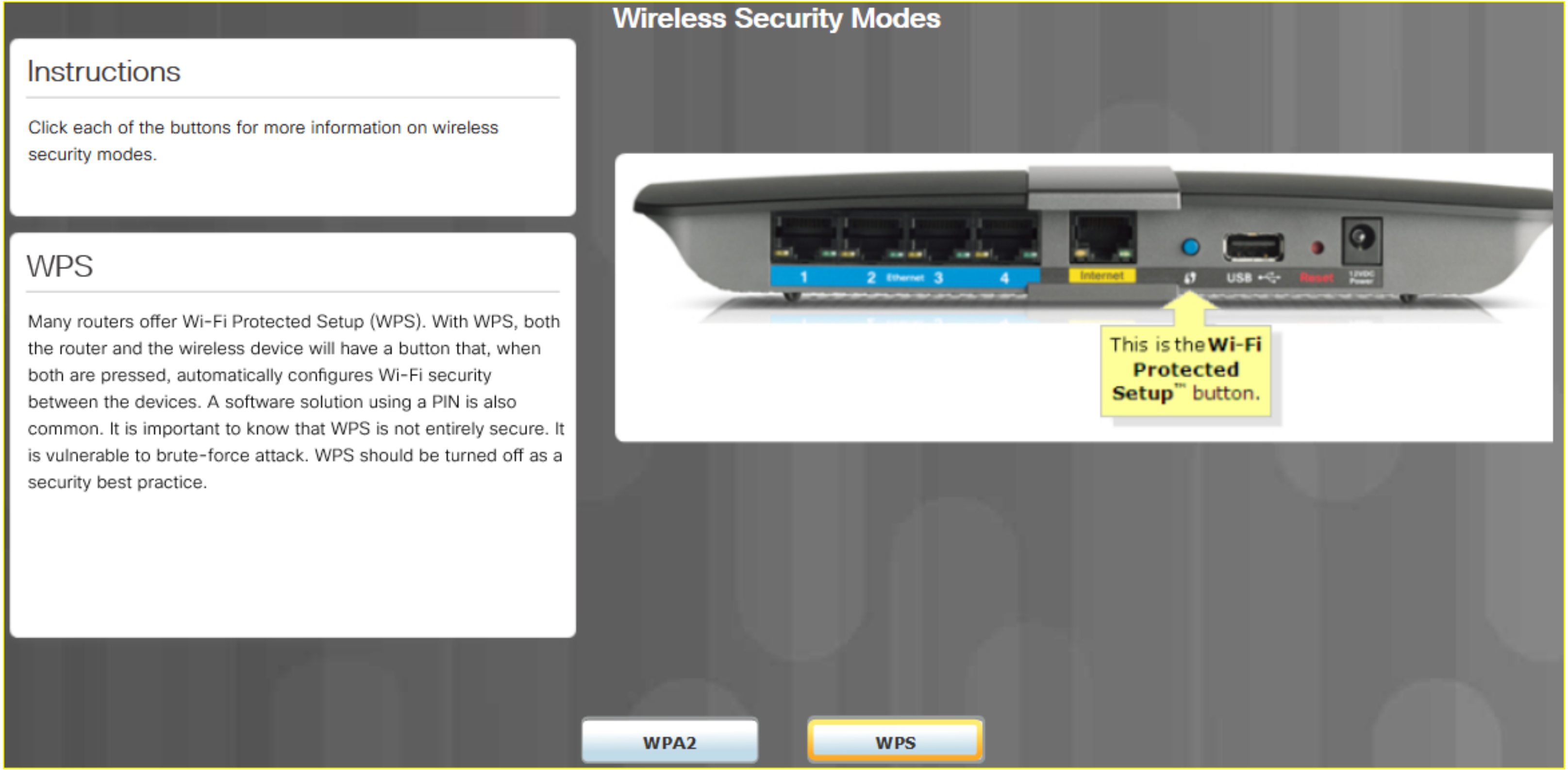
WPA2

Use a wireless encryption system to encode the information being sent to prevent unwanted capture and use of data. Most wireless access points support several different security modes As discussed in a previous chapter, always implement the strongest security mode (WPA2) possible.

Security Mode: Disabled

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Wireless Security Modes (Cont.)



Wireless Security Modes

Instructions

Click each of the buttons for more information on wireless security modes.

WPS

Many routers offer Wi-Fi Protected Setup (WPS). With WPS, both the router and the wireless device will have a button that, when both are pressed, automatically configures Wi-Fi security between the devices. A software solution using a PIN is also common. It is important to know that WPS is not entirely secure. It is vulnerable to brute-force attack. WPS should be turned off as a security best practice.

This is the **Wi-Fi Protected Setup™** button.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Firmware Updates

- Most wireless routers offer upgradable firmware.
  - Firmware releases may contain fixes for common problems reported by customers as well as security vulnerabilities.
- It is important to periodically check the manufacturer’s website for updated firmware.
- It is common to use a GUI to upload the firmware to the wireless router.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Firewalls

- A hardware firewall inspects data packets from the network before they reach devices on the inside network.
  - The firewall can be configured to block individual ports, a range of ports, or specific application traffic.
- Most wireless routers also include an integrated hardware firewall.
- They can be configured to allow two different types of traffic into your network:
  - Responses to traffic that originates from inside your network
  - Traffic destined for a port that you have intentionally left open

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Port Forwarding and Port Triggering

- Hardware firewalls can be used to block ports to prevent unauthorized access in and out of a LAN.
- However, there are situations when specific ports must be opened so that certain programs and applications can communicate with devices on different networks.
- Port forwarding is a rule-based method of directing traffic between devices on separate networks.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Configure Wireless Security

Universal Plug and Play

- Universal Plug and Play (UPnP) is a protocol that enables devices to dynamically forward traffic through network ports without the need for user intervention or configuration.
- Port forwarding is often used for:
  - Streaming media
  - Hosting games
  - Providing services from home and small business computers to the internet.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer – Configure Wireless Security

In this activity, you will configure the wireless router to:

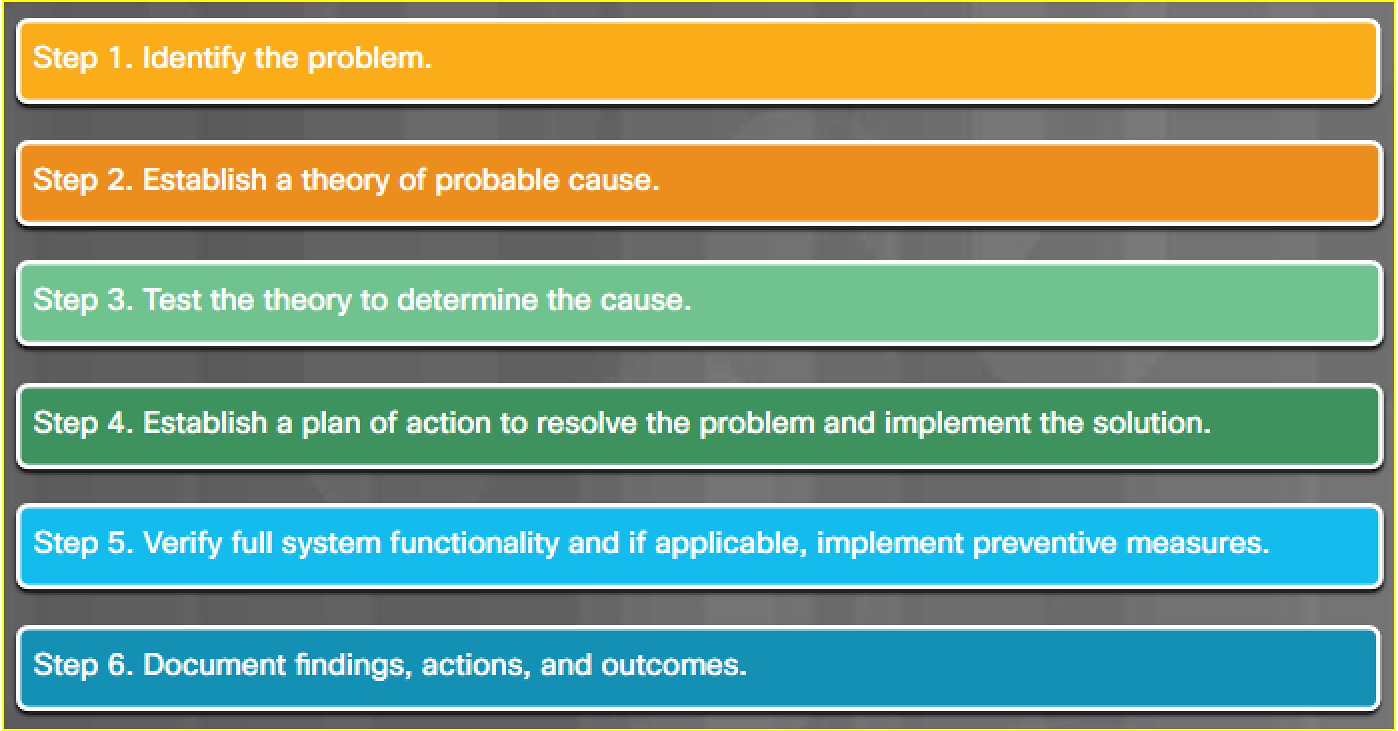
- Use WPA2 Personal as the security method
- Rely on MAC filtering to increase security
- Support Single Port Forwarding

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.5 Basic Troubleshooting Process for Security

Applying the Troubleshooting Process to Security

The Troubleshooting Process



Step 1. Identify the problem.

Step 2. Establish a theory of probable cause.

Step 3. Test the theory to determine the cause.

Step 4. Establish a plan of action to resolve the problem and implement the solution.

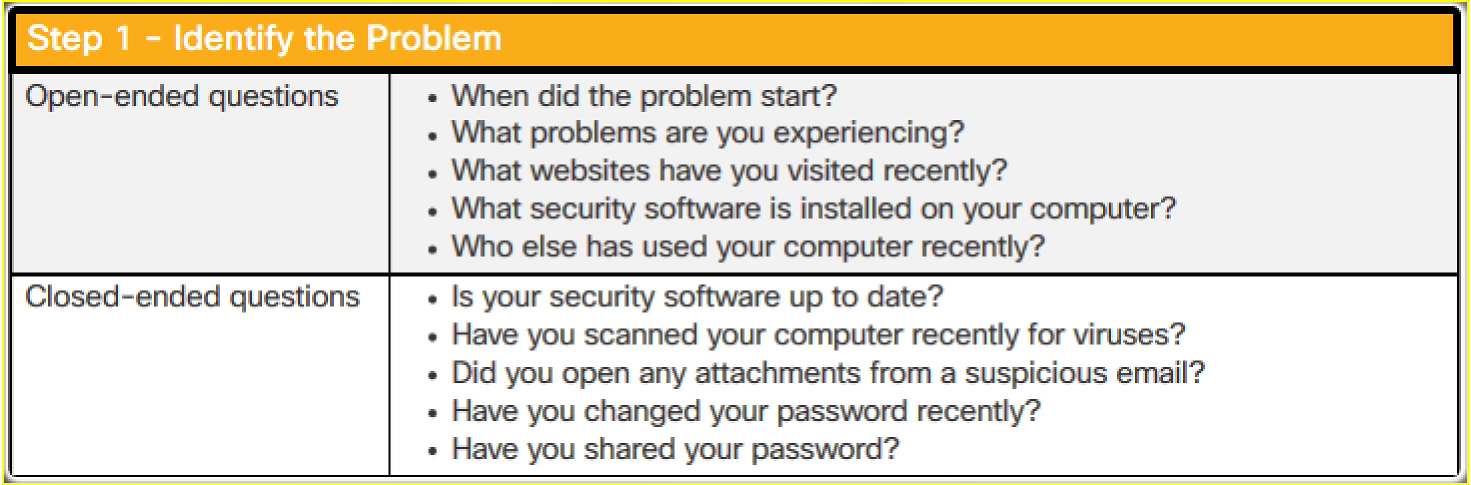
Step 5. Verify full system functionality and if applicable, implement preventive measures.

Step 6. Document findings, actions, and outcomes.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Applying the Troubleshooting Process to Security

Identify the Problem

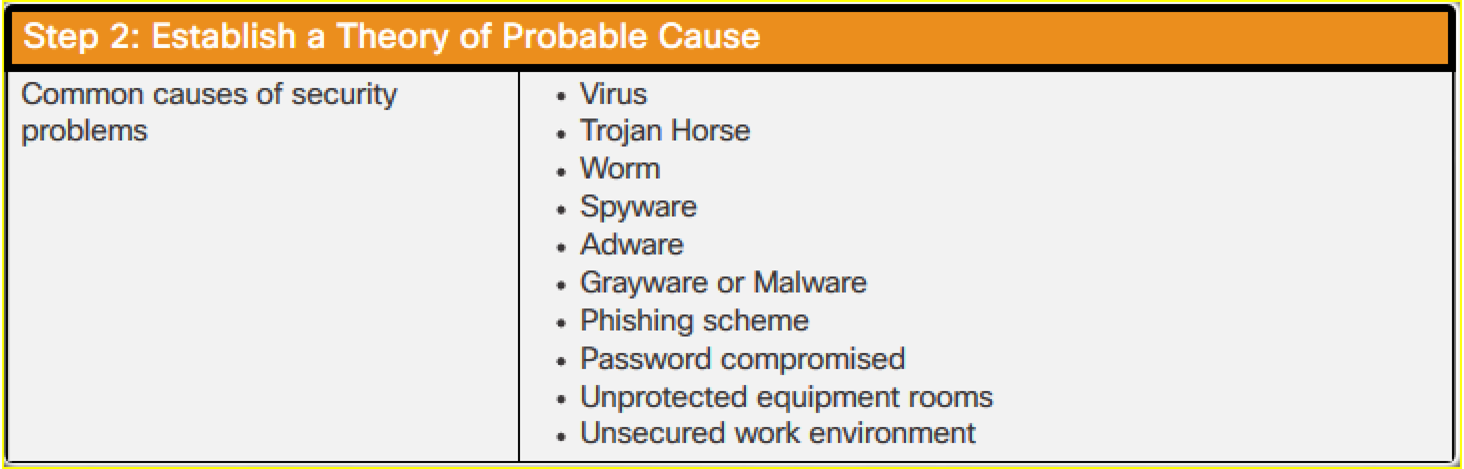


Step 1 - Identify the Problem	
Open-ended questions	- When did the problem start? - What problems are you experiencing? - What websites have you visited recently? - What security software is installed on your computer? - Who else has used your computer recently?
Closed-ended questions	- Is your security software up to date? - Have you scanned your computer recently for viruses? - Did you open any attachments from a suspicious email? - Have you changed your password recently? - Have you shared your password?

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Applying the Troubleshooting Process to Security

Establish a Theory of Probable Cause

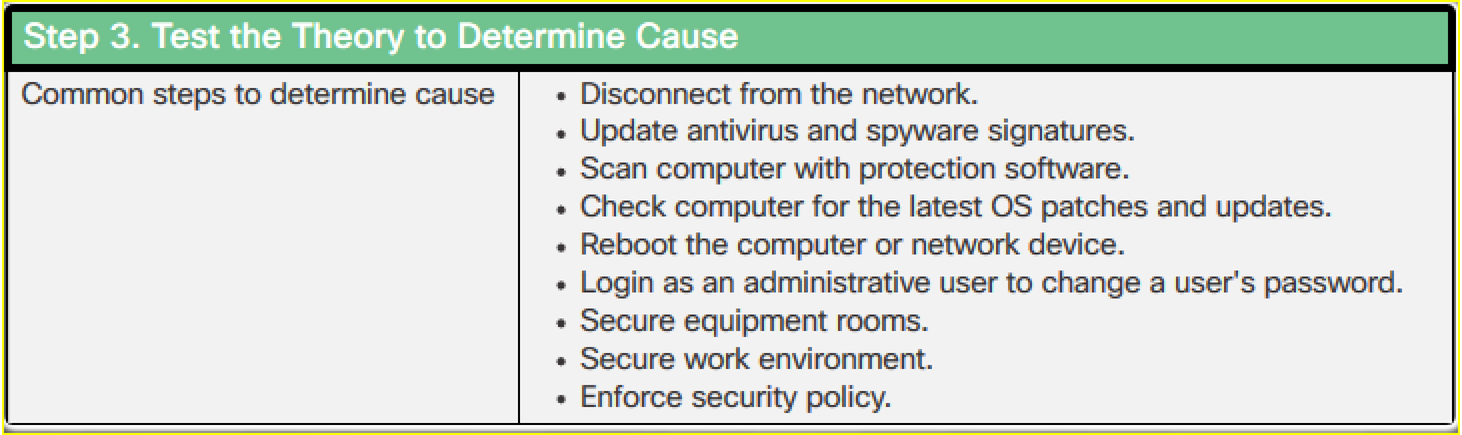


Step 2: Establish a Theory of Probable Cause	
Common causes of security problems	• Virus • Trojan Horse • Worm • Spyware • Adware • Grayware or Malware • Phishing scheme • Password compromised • Unprotected equipment rooms • Unsecured work environment

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Applying the Troubleshooting Process to Security

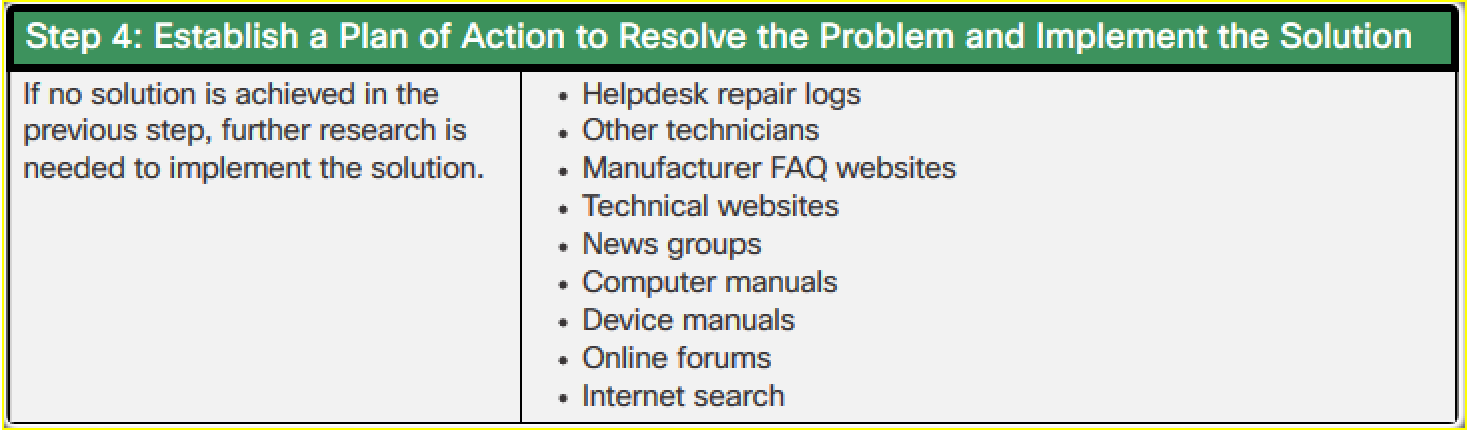
Test the Theory to Determine Cause



Step 3. Test the Theory to Determine Cause	
Common steps to determine cause	• Disconnect from the network. • Update antivirus and spyware signatures. • Scan computer with protection software. • Check computer for the latest OS patches and updates. • Reboot the computer or network device. • Login as an administrative user to change a user's password. • Secure equipment rooms. • Secure work environment. • Enforce security policy.

Applying the Troubleshooting Process to Security

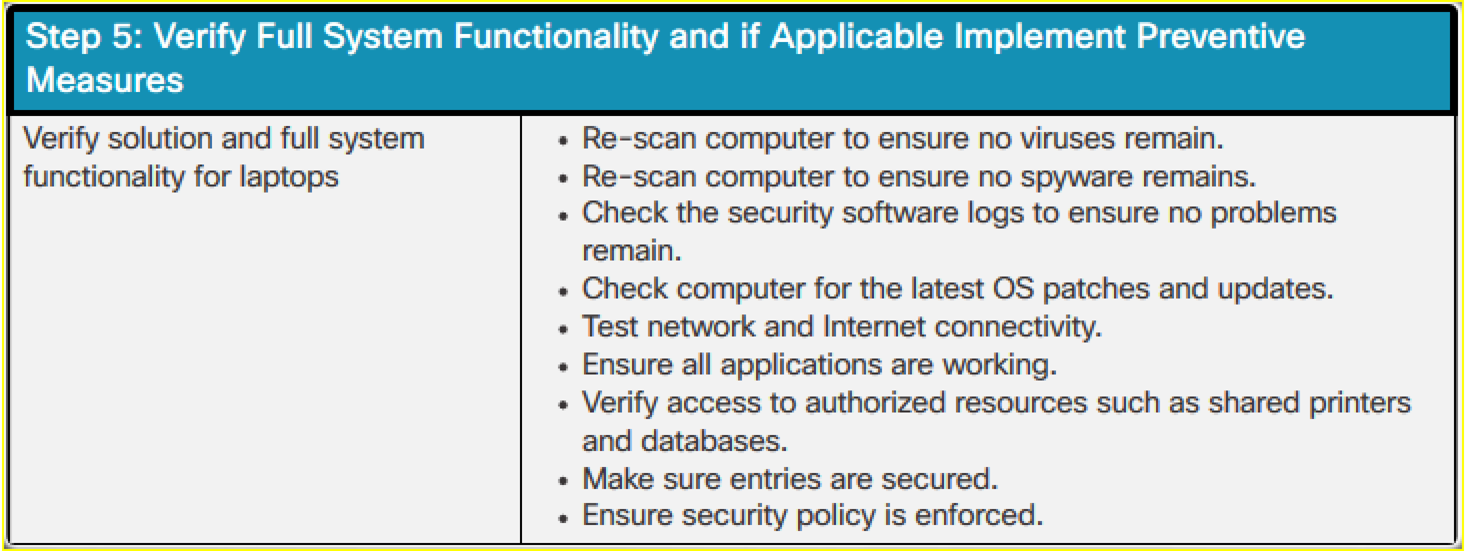
Establish a Plan of Action to Resolve the Problem and Implement the Solution



Step 4: Establish a Plan of Action to Resolve the Problem and Implement the Solution	
If no solution is achieved in the previous step, further research is needed to implement the solution.	• Helpdesk repair logs • Other technicians • Manufacturer FAQ websites • Technical websites • News groups • Computer manuals • Device manuals • Online forums • Internet search

Applying the Troubleshooting Process to Security

Verify Full System Functionality and if Applicable Implement Preventative Measures

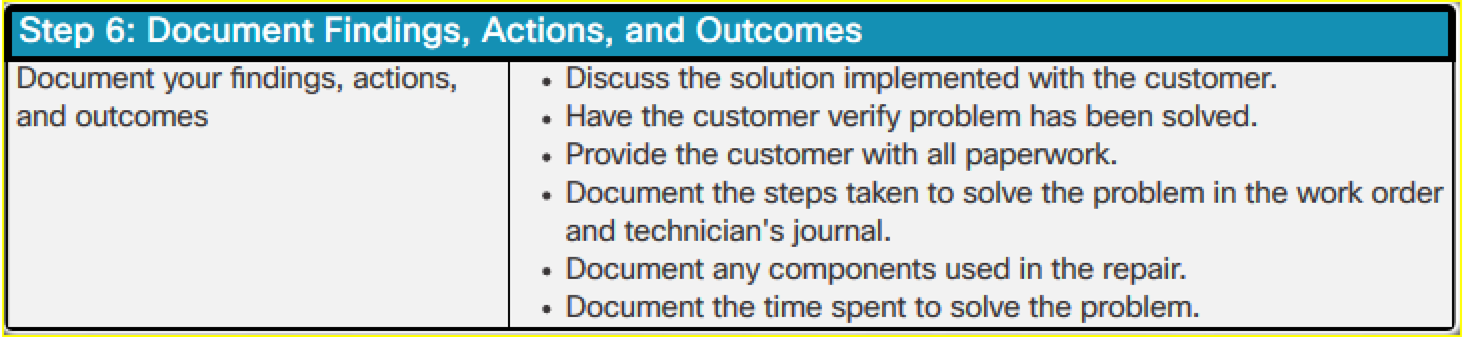


Step 5: Verify Full System Functionality and if Applicable Implement Preventive Measures	
Verify solution and full system functionality for laptops	• Re-scan computer to ensure no viruses remain. • Re-scan computer to ensure no spyware remains. • Check the security software logs to ensure no problems remain. • Check computer for the latest OS patches and updates. • Test network and Internet connectivity. • Ensure all applications are working. • Verify access to authorized resources such as shared printers and databases. • Make sure entries are secured. • Ensure security policy is enforced.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Applying the Troubleshooting Process to Security

Document Findings, Actions, and Outcomes

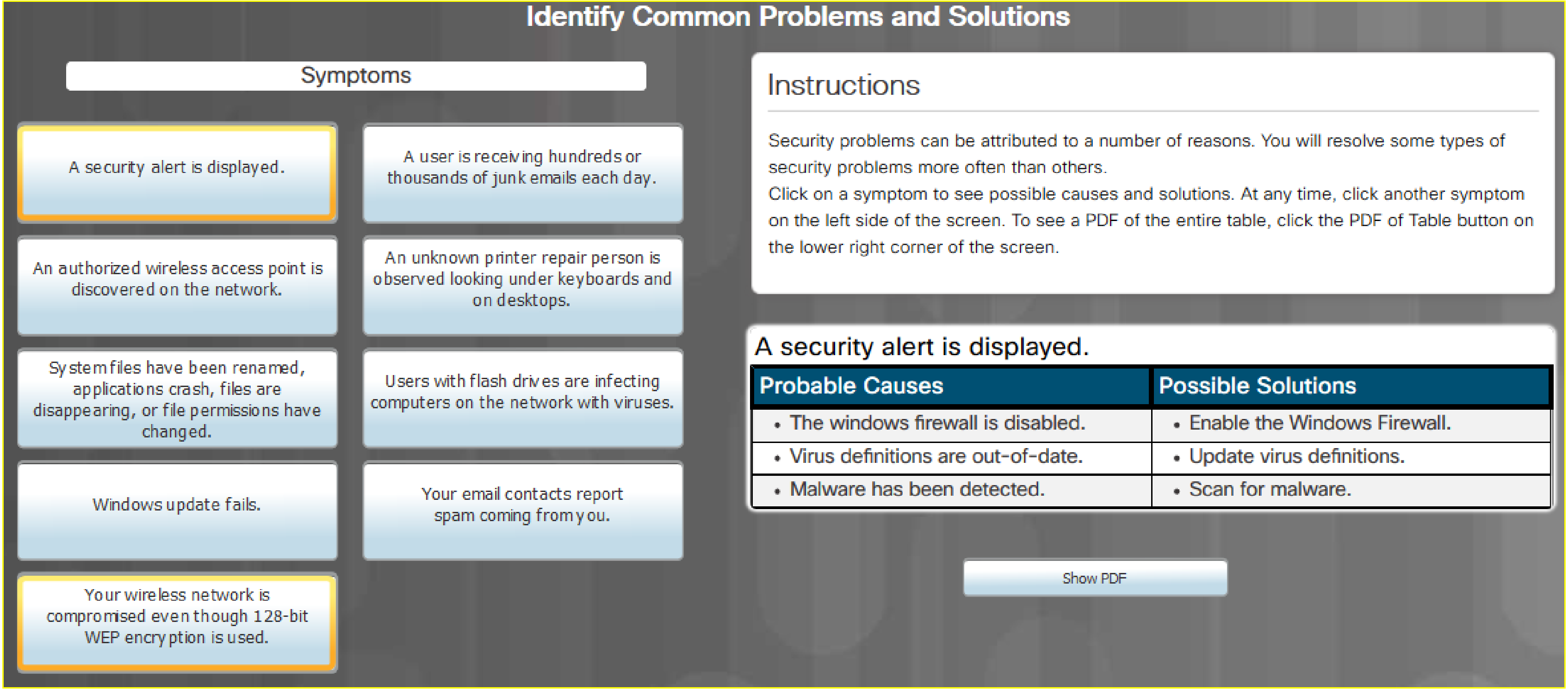


Step 6: Document Findings, Actions, and Outcomes	
Document your findings, actions, and outcomes	• Discuss the solution implemented with the customer. • Have the customer verify problem has been solved. • Provide the customer with all paperwork. • Document the steps taken to solve the problem in the work order and technician's journal. • Document any components used in the repair. • Document the time spent to solve the problem.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Common Problems and Solutions for Security

Identify Common Problems and Solutions



Identify Common Problems and Solutions

Symptoms
A security alert is displayed.
A user is receiving hundreds or thousands of junk emails each day.
An authorized wireless access point is discovered on the network.
An unknown printer repair person is observed looking under keyboards and on desktops.
System files have been renamed, applications crash, files are disappearing, or file permissions have changed.
Users with flash drives are infecting computers on the network with viruses.
Windows update fails.
Your email contacts report spam coming from you.
Your wireless network is compromised even though 128-bit WEP encryption is used.

Instructions

Security problems can be attributed to a number of reasons. You will resolve some types of security problems more often than others.

Click on a symptom to see possible causes and solutions. At any time, click another symptom on the left side of the screen. To see a PDF of the entire table, click the PDF of Table button on the lower right corner of the screen.

A security alert is displayed.

Probable Causes	Possible Solutions
• The windows firewall is disabled.	• Enable the Windows Firewall.
• Virus definitions are out-of-date.	• Update virus definitions.
• Malware has been detected.	• Scan for malware.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Document Customer Information in a Work Order

In this lab, you will document customer information in a work order.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.6 Chapter Summary

Conclusion

Chapter 13: Security

- Explain common security threats and how to prevent and recover from threats.
- Identify the purpose and use of security procedures in protecting physical equipment and data.
- Secure Windows workstations within the BIOS, Operating System, and firewall.
- Configure wireless security settings on a small office / home office router.
- Troubleshoot common problems for security

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

cisco