Chapter 27

Securing Computers

Episode: **Threats**

Objective(s):

Core 2: 2.1 Summarize various security measures and their purposes.

Core 2: 2.4 Explain common social-engineering attacks, threats, and vulnerabilities.

Core 2: 3.2 Given a scenario, troubleshoot common personal computer (PC) security issues.

Episode Description

You can't protect your networks unless you understand the threats they face. Using the concept of security shells makes it easier to categorize and mitigate threats.

Key Terms

- 2:07 - Objective term - Man-in-the-middle (on-path) attack
- 3:30 - Objective term - Spoofing
- 4:26 - Objective term - Denial of Service (DoS)
- 5:25 - Objective term - Distributed Denial of Service (DDoS)
- 5:51 - Zombie
- 6:46 - Objective term - Zero day
- 7:47 - Objective term - Renamed system files
- 8:13 - Objective term - Disappearing files

Quick Review

- The term "security" encompasses host-based, network-based, and physical security
- Common threats include man-in-the-middle (on-path), Denial of Service (DoS), and Distributed DoS (DDoS) attacks
- Symptoms of such attacks include renamed system files, missing files, and more

Episode: **Dealing with Threats**

Objective(s):

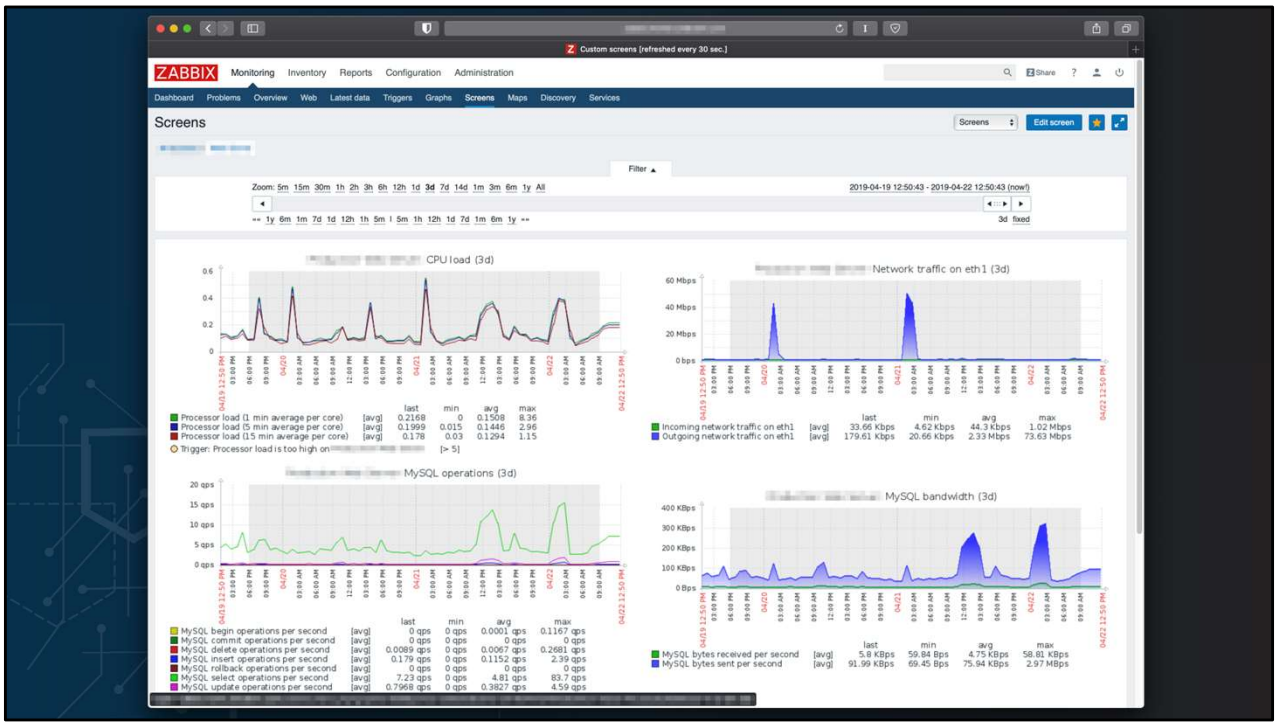
- Core 1: 2.4 Summarize services provided by networked hosts.
- Core 1: 2.8 Given a scenario, use networking tools.
- Core 2: 2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.
- Core 2: 2.4 Explain common social-engineering attacks, threats, and vulnerabilities.

Episode Description

Once you understand threats, you can mitigate those threats by reducing vulnerabilities. This episode covers the core tools and actions you must do as a tech to reduce threats. These tools and actions include patching software, running anti-malware, and installing firewalls and intrusion detection/prevention systems.

Key Terms

- 0:47 - Objective term - Patch your system!
- 1:43 - Objective term - Run anti-malware and antivirus
- 1:58 - Objective term - Run a host-based software firewall
- 2:41 - Intrusion detection systems (IDS)
- 3:43 - Intrusion prevention systems (IPS)
- 5:02 - Endpoint management
- 5:55 - Objective term - Unified Threat Management (UTM)


Custom screens [refreshed every 30 sec.]
ZABBIX
Monitoring
Inventory
Reports
Configuration
Administration
Dashboard
Problems
Overview
Web
Latest data
Triggers
Graphs
Screens
Maps
Discovery
Services
Screens
Edit screen
Filter
Zoom: 5m 15m 30m 1h 2h 3h 6h 12h 1d 3d 7d 14d 1m 3m 6m 1y All
2019-04-19 12:50:43 - 2019-04-22 12:50:43 (now!)
CPU load (3d)
Processor load (1 min average per core) [avg] 0.2168 0 0.1508 8.36
Processor load (5 min average per core) [avg] 0.1999 0.015 0.1446 2.96
Processor load (15 min average per core) [avg] 0.178 0.03 0.1294 1.15
Trigger: Processor load is too high on [> 5]
Network traffic on eth1 (3d)
Incoming network traffic on eth1 [avg] 33.66 Kbps 4.62 Kbps 44.3 Kbps 1.02 Mbps
Outgoing network traffic on eth1 [avg] 179.61 Kbps 20.66 Kbps 2.33 Mbps 73.63 Mbps
MySQL operations (3d)
MySQL begin operations per second [avg] 0 qps 0 qps 0.0001 qps 0.1167 qps
MySQL commit operations per second [avg] 0 qps 0 qps 0 qps 0 qps
MySQL delete operations per second [avg] 0.0089 qps 0 qps 0.0067 qps 0.2681 qps
MySQL insert operations per second [avg] 0.179 qps 0 qps 0.1152 qps 2.39 qps
MySQL rollback operations per second [avg] 0 qps 0 qps 0 qps 0 qps
MySQL select operations per second [avg] 7.23 qps 0 qps 4.81 qps 83.7 qps
MySQL update operations per second [avg] 0.7968 qps 0 qps 0.3827 qps 4.59 qps
MySQL bandwidth (3d)
MySQL bytes received per second [avg] 5.8 KBps 59.84 Bps 4.75 KBps 58.81 KBps
MySQL bytes sent per second [avg] 91.99 KBps 69.45 Bps 75.94 KBps 2.97 MBps

Quick Review

- Host-based security includes patching, anti-malware/antivirus, and firewalls
- Network-based security includes intrusion detection (IDS), intrusion prevention (IPS), and firewalls
- Unified Threat Management (UTM) includes IDS/IPS, firewalls, and anti-malware all in one and is often available in the Cloud

Episode: **Physical Security**

Objective(s):

- Core 1: 3.4 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
- Core 2: 1.7 Given a scenario, apply application installation and configuration concepts.
- Core 2: 2.1 Summarize various security measures and their purposes.
- Core 2: 2.6 Given a scenario, configure a workstation to meet best practices for security

Episode Description

Secure your assets in three layers: perimeter, rooms, individual devices. Mike explores options for each layer, from security guards at the perimeter to cable locks on individual devices.

Key Terms

- 1:35 - Objective term - Security guard
- 2:00 - Objective term - Mantrap (access control vestibule)
- 2:41 - Objective term - Locking doors
- 2:51 - Objective term - Need a key
- 2:53 - Entry control roster

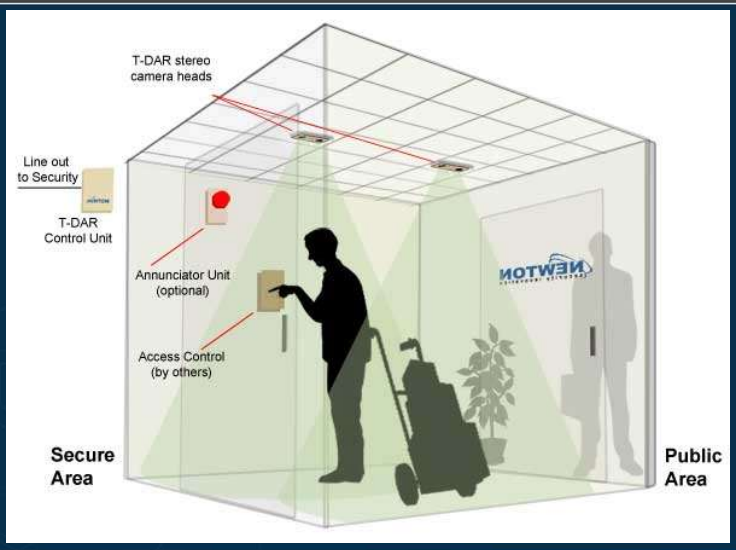
Key Terms

- 3:25 - Objective term - Badge reader
- 3:26 - RFID-chips embedded in badges
- 3:54 - Objective term - Smart card
- 4:12 - Objective term - Biometric scanners/locks
- 4:52 - Objective term - Cable locks to secure hardware

Key Terms

- 5:20 - Objective term - Server lock
- 5:50 - Objective term - USB locks
- 6:26 - Privacy screens
- 7:05 - Objective term - Key fobs
- 7:15 - Objective term - Hardware token/ Hardware Security Module (HSM)

Mantrap (Access Control Vestibule)



Source: https://www.newtonsecurityinc.com/datacenter_landing.html

Quick Review

- Physical security includes perimeter security, room locks, and individual device security
- Security guards and mantraps help perimeter security
- Locks, badges, smart cards, and biometrics enable room-level security
- Device security devices include server locks, USB locks, and screen filters

Episode: **Passwords and Authentication**

Objective(s):

Core 2: 2.1 Summarize various security measures and their purposes.

Core 2: 2.4 Explain common social-engineering attacks, threats, and vulnerabilities.

Core 2: 2.6 Given a scenario, configure a workstation to meet best practices for security.

Episode Description

Password security can be compromised by many attack types, such as brute force, dictionary, and rainbow tables. This episode explores options for creating very secure passwords and using multifactor authentication.

Key Terms

- 0:55 - Hash
- 3:37 - Objective term - Brute-force
- 5:44 - Objective term - Dictionary attack
- 7:16 - Rainbow tables
- 9:09 - Objective term - Password best practices
- 9:13 - Objective term - 1. Set strong passwords

Key Terms

- 9:16 - Objective term - Make complex passwords with upper- and lowercase letters and use different character types
- 9:36 - Objective term - Looooong passwords
- 10:37 - Objective term - 2. Password expiration
- 10:54 - Objective term - (Also...make sure your employees aren't taping their passwords to their monitors...)

Key Terms

- 11:22 - Objective term - 3. Require screensavers with password login on desktops
- 11:49 - Objective term - 4. Require lock screens with passwords on mobile devices
- 12:20 - Objective term - 5. BIOS/UEFI passwords
- 12:36 - 6. Require passwords everywhere!
- 13:01 - Objective term - 7. Multifactor authentication (MFA)

Password Cracking Websites

- How Secure is My Password?
  - https://howsecureismypassword.net
- CrackStation
  - https://crackstation.net/

Download Kali Linux

A+

- This is a bit beyond A+ and more into Security+, but if you're interested in hacking, password cracking, cyber attacks, and more, check out Kali Linux. You can download the iso and run it on your virtual machine manager of choice:
  - https://www.kali.org/get-kali/

CompTIA

Quick Review

- Modern password security relies on passwords and hashes
- Methods for cracking passwords and hashes include brute force, dictionary attacks, and rainbow tables
- Use best password practices, such as upper- and lowercase letters, numbers, non-alphanumeric characters, and making long passwords

Episode: **Multifactor Authentication (MFA)**

Objective(s):

Core 1: 1.1 Given a scenario, install and configure laptop hardware and components.

Core 1: 2.4 Summarize services provided by networked hosts.

Core 2: 2.1 Summarize various security measures and their purposes.

Core 2: 2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

Episode Description

A+

Multifactor authentication (MFA) is the process of proving you are who you say you are using unique identifiers that only you have or know. This episode explores the different options for MFA, as well as some interesting biometrics like fingerprint, facial, and retinal scanning.

CompTIA

Key Terms

- 0:15 - Objective term - Multifactor authentication (MFA)
- 0:21 - Something you know
- 0:49 - Two-factor authentication (2FA)
- 0:55 - Something you have
- 1:06 - Objective term - Hardware token
- 1:13 - Objective term - Authenticator application
- 1:36 - Something you are

Key Terms

- 1:40 - Objective term - Biometrics such as fingerprint, palmprint, or retinal scanners
- 1:54 - Objective term - Facial recognition
- 1:59 - Somewhere you are
- 2:11 - Objective term - Supervisory Control and Data Acquisition (SCADA)
- 3:17 - Objective term - OS login options include facial recognition, fingerprint recognition, and personal identification number (PIN)

Quick Review

- Multifactor authentication (MFA) is a mechanism to help verify access to a particular resource using multiple forms of proof
- MFA includes one or more of the following: something you know, something you have, something you are, or somewhere you are
- Modern MFA can utilize unique biometric details, like retinal, fingerprint, or facial scans, or even detect your exact location

Episode: **Malware**

Objective(s):

Core 2: 2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.

Core 2: 3.2 Given a scenario, troubleshoot common personal computer (PC) security issues.

Core 2: 3.4 Given a scenario, troubleshoot common mobile OS and application issues.

Episode Description

Malware comes in many forms; infestations have many symptoms. This episode describes malware in all its lovely shades of ugly, from viruses and worms to spontaneous application crashes and invalid certificate errors.

Key Terms

- 1:15 - Objective term - Virus
- 2:24 - Worm
- 2:58 - Objective term - Trojan horse
- 3:42 - Objective term - Rootkit (boot sector virus)
- 4:26 - Objective term - Ransomware

Key Terms

- 4:43 - Objective term - Rogue antivirus
- 5:37 - Botnet
- 6:28 - Objective term - Keylogger
- 7:12 - Objective term - Spyware
- 8:31 - Objective term - Pop-ups
- 9:10 - Objective term - Browser redirection

Key Terms

- 9:45 - Objective term - Security/desktop alerts
- 10:06 - Objective term - OS update failure
- 10:27 - Spam
- 11:17 - Hijacked e-mail
- 11:35 - Automated replies
- 12:01 - Objective term - Invalid certificates
- 13:12 - Objective term- Network LAN tap

Quick Review

- Worms propagate via a network
- Trojans masquerade as benign programs, but carry a payload for later
- Ransomware attacks lock down systems in exchange for money
- Malware infestations manifest as browser redirection, application crashes, update failures, and more

Episode: **Anti-Malware**

Objective(s):

Core 2: 2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.

Core 2: 3.1 Given a scenario, troubleshoot common Windows OS problems.

Core 2: 3.3 Given a scenario, use best practice procedures for malware removal.

Episode Description

A+

The CompTIA A+ objectives outline a very detailed series of steps for dealing with a malware infestation. This episode looks at important pre-malware steps and then describes the CompTIA procedures.

CompTIA

Key Terms

- 0:36 - 1. No such thing as antivirus program
- 0:44 - Objective term - Anti-malware
- 1:13 - Objective term - Recovery console (now called Recovery mode on the objectives)
- 1:34 - Objective term - Backup/restore/ reimage
- 1:46 - Objective term - End-user education

Key Terms

- 2:08 - Objective term - Software firewalls
- 2:24 - Secure DNS
- 3:02 - 1. Non-ISP DNS servers
- 3:34 - 2. Encrypt DNS requests
- 5:35 - Objective term - 1. Identify and research (investigate and verify) malware symptoms
- 5:48 - Objective term - 2. Quarantine the infected systems
- 6:11 - Objective term - 3. Disable System Restore (in Windows)

Key Terms

- 6:38 - Objective term - 4. Remediate the infected systems
- 6:42 - Objective term - 4a. Update the anti-malware software
- 7:34 - Objective term - 4b. Scan and use removal techniques (safe mode, pre-installation environment)
- 9:52 - Objective term - 5. Schedule scans and run updates
- 10:27 - Objective term - 6. Enable System restore and create a restore point (in Windows)
- 10:56 - Objective term - 7. Educate the end user

Cloudflare Free DNS

- https://www.cloudflare.com/dns/

Quick Review

- Prepare for malware attacks with good backups, end-user education, and firewalls
- Use secure DNS options, such as a trusted third-party site and encryption
- Memorize the CompTIA A+ seven-step malware-recovery process

Episode: **Social Engineering**

Objective(s): Core 2: 2.4 Explain common social-engineering attacks, threats, and vulnerabilities.

Episode Description

Social engineering practices enable attackers to gain access to sensitive information through people. This episode highlights social engineering tactics, from tailgating to spear phishing.

Key Terms

- 0:42 - Objective term - Impersonation
- 2:14 - Objective term - Tailgating
- 2:56 - Unauthorized access
- 3:11 - Objective term - Shoulder surfing
- 3:40 - Objective term - Dumpster diving
- 4:44 - Objective term - Phishing (targets people via e-mail/websites)
- 4:44 - Objective term - Vishing (targets people via voice/phone calls)
- 4:59 - Objective term - Spear phishing (targeting specific people)
- 4:59 - Objective term - Whaling (targeting high-ranking people)

Quick Review

- Social engineering enables bad people to use information from people to gain access to sensitive information
- Social engineering attacks include phishing, vishing, shoulder surfing, spear phishing, whaling, tailgating, impersonation, and dumpster diving
- Phishing, vishing, spear phishing, and whaling attacks seek personal or financial information with targeted scams

Episode: **Licensing**

Objective(s): Core 2: 4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

Episode Description

Some software is free to use. Some is free for non-commercial use. Some requires a paid license for any purpose. Some licenses focus on the number of human users, while others focus on the number of systems, or even the number of processors! This episode explores them all.

Key Terms

- 0:49 - “An Open Letter to Hobbyist” - Bill Gates, 1976
- 0:56 - Required licensing fee for the BASIC programming language
- 1:01 - Licensing
- 1:11 - Objective term - End-user license agreement (EULA)
- 1:55 - Objective term - Digital rights management (DRM)
- 2:55 - Objective term - Commercial/corporate license
- 3:11 - Objective term - Open-source
- 3:32 - GNU General Personal license (GNU GPL)
- 5:13 - Objective term - Personal license
- 5:31 - Enterprise license
- 6:26 - Per-processor license for Windows

Quick Review

- An End-user license agreement (EULA) describes what users can do with licensed software
- Digital rights management (DRM) controls what users can do with some content
- Producers retain all rights to commercial software
- Open-source software enables users to change or modify the software

Episode: **Incident Response**

Objective(s): Core 2: 4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

Episode Description

Although procedures can vary among companies, the CompTIA A+ objectives follow a logical set of responses. This lesson describes each step.

Key Terms

- 0:55 - Objective term - Incident response
- 1:12 - Know your responsibility
- 1:31 - Identify the problem
- 1:48 - Objective term - Report though the proper channels (inform management/law enforcement as necessary)

Key Terms

- 2:11 - Objective term - Data/device preservation (protect the data integrity)
- 2:43 - Objective term - Document the incident and surroundings
- 3:26 - Objective term - Document changes
- 3:36 - Objective term - Chain of custody

Quick Review

- Know your responsibilities
- Be sure to report the incident to the correct management and/or law enforcement agency based on company policies
- Preserve data integrity by copying the suspicious drive
- Exercise proper chain-of-custody procedures and always document, document, document

Episode: **Environmental Controls**

Objective(s):

Core 2: 4.4 Given a scenario, use common safety procedures.

Core 2: 4.5 Summarize environmental impacts and local environmental controls.

Episode Description

Controlling environmental factors enables you to create a safe computing space. This episode looks at options for disposing of waste such as old printer cartridges and controlling temperature and humidity. Mike describes proper ventilation, electrical safety, and much more.

Key Terms

- 0:46 - Objective term - Compliance to government regulations
- 0:59 - Occupational Safety and Health Administration (OSHA) in the US
- 1:53 - Objective term - Material safety data sheet (MSDS)
- 2:02 - Objective term - MSDSes include how to safely handle and dispose of materials and their environmental impacts

Key Terms

- 2:33 - Objective term - Temperature and humidity levels
- 3:17 - Objective term - Proper ventilation
- 3:36 - Objective term - Battery backup
- 3:42 - Objective term - Surge suppressor
- 3:53 - Objective term - Dust and debris

Key Terms

- 4:21 - Enclosures
- 4:29 - Objective term - Air filters/mask
- 4:50 - Objective term - Compressed air
- 5:01 - Objective term - Vacuums
- 5:22 - Objective term - Anti-static vacuum

Quick Review

- Check the MSDS for any spills or problems with equipment
- Monitor temperature and humidity levels
- Ensure proper ventilation
- Employ surge suppressors and UPS backup devices
- Clean systems with compressed air and specialized vacuums

Episode: **Malware in Action**

Objective(s):

Core 2: 3.1 Given a scenario, troubleshoot common Windows OS problems.

Core 2: 3.5 Given a scenario, troubleshoot common mobile OS and application security issues.

Core 2: 4.2 Explain basic change management best practices.

Episode Description

This episode demonstrates some destructive malware and ransomware applications to give you an idea of what to look for when you suspect a system has been infected. WARNING! If you attempt these at home, be sure you're in a sandbox or virtual machine that is appropriately segmented from your network. These viruses can cause real issues!

Key Terms

- 0:22 - Objective term - Sandbox testing
- 1:04 - MEMZ virus
- 2:06 - Objective term - Viruses can lead to applications crashing, unexpected application behavior, low memory warnings, system instability
- 2:26 - Objective term - Viruses can also lead to services not starting
- 2:34 - Objective term - Some viruses cause high network traffic which can lead to limited or no Internet connectivity

Key Terms

- 3:04 - Objective term - Data usage limit notification
- 3:29 - Objective term - Limited Internet connectivity
- 4:00 - Objective term - Fake security warnings
- 4:15 - Objective term - Leaked personal files/data
- 4:28 - Objective term - High number of ads
- Objective term - Frequent shutdowns
- Objective term - Sluggish response time

theZoo on GitHub

- You can use these malware files to practice in a VM or Windows Sandbox
- WARNING! Don't install these on your working machine. Each has a "destructive" and "non-destructive" version.
- https://github.com/ytisf/theZoo

Quick Review

- Windows Sandbox can be a safe and effective way to test potentially dangerous files, but always take the proper precautions beforehand
- Knowing how malware infects a system is critical in understanding how to stop it
- Symptoms of malware include applications crashing, low memory warnings, system instability, services not starting, unexplained high network traffic, fake security warnings, and high number of ads