Vulnerability and Exploits

Analyzing a Cyberattack

Cisco | Networking Academy®
Mind Wide Open™

Security Vulnerability and Exploits

- Software vulnerability
  - Errors in OS or application code
  - Project Zero
  - What can you do to protect yourself from software vulnerability?
- Hardware vulnerability
  - Hardware design flaws
  - RAM memory example: Rowhammer

    (https://www.youtube.com/watch?v=5dx0zWZvh6g

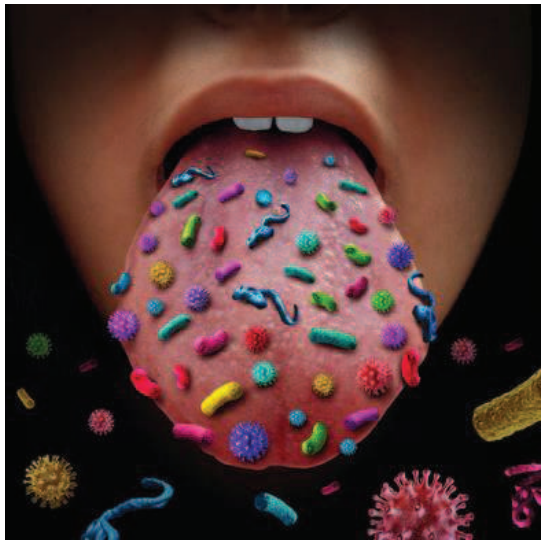
    https://www.youtube.com/watch?v=0U7511Fb4to)
  - What can you do to protect yourself from hardware vulnerability?

Types of Security Vulnerabilities

- Buffer Overflow
  - Data is written beyond the limits of a buffer
- Non-validated Input
  - Force programs to behave in an unintended way
- Race Conditions
  - Improperly timed events
- Weaknesses in Security Practices
  - Protect sensitive data through authentication, authorization, and encryption
- Access-control Problems
  - Access control to equipment and resources
  - Security practices

Types of Malware and Symptoms

- Types of Malware
  - Spyware
  - Bot
  - Ransomware
  - Scareware
  - Rootkit
  - Man-in-The Middle
- Symptoms of Malware
  - Deleted files
  - Modified files
  - Can you list more symptoms?

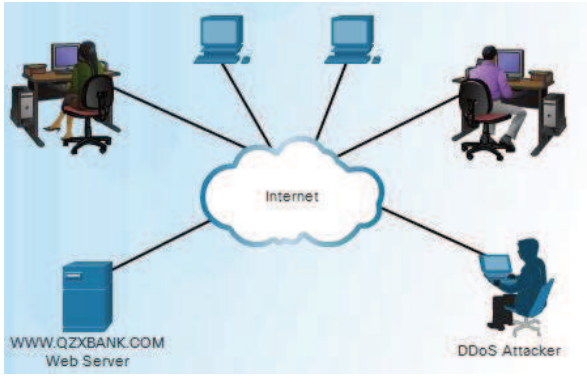


Methods of Infiltration

- Social Engineering – manipulation of individual
  - Pretexting
  - Tailgating
  - Something for something (Quid pro quo)
- Wi-Fi Password Cracking – Password discovery
  - Social engineering
  - Brute-force attacks
  - Network sniffing
- Phishing – sends fraudulent emails to trick users
- Vulnerability Exploitation – scan to find vulnerability to exploit

Denial of Service

- DoS – disruption of network services
  - Overwhelming quantity of traffic
  - Maliciously formatted packets
- DDoS
  - Similar to DoS
  - Originates from multiple, coordinated sources
- SEO Poisoning
  - Increase traffic to malicious sites
  - Force malicious sites to rank higher



Blended Attack

- What is a Blended Attack?
  - Uses multiple techniques to compromise a target
  - Worms, Trojan horses, spyware, keyloggers, spam and phishing schemes
  - Examples: Nimbda, BugBear, and Conficker

Impact Reduction

- What is a Impact Reduction?
  - Communicate the issue
  - Be sincere and accountable
  - Provide details
  - Understand the cause of the breach
  - Take steps to avoid another similar breach in the future
  - Ensure all systems are clean
  - Educate employees, partners and customers

Protecting Your Devices and Network

- Protect Your Computing Devices
  - Keep the Firewall on
  - Use Antivirus and antispyware
  - Manage Your Operating System and Browser
- Use Wireless Networks Safely
  - Use caution when using public Wi-Fi hotspots
  - Turn off Bluetooth when not in use
- Use Unique Passwords for Each Online Account
  - Prevents criminals from accessing all your online accounts using one stolen credentials
  - Use password managers
- Use Passphrase Rather Than a Password

Data Maintenance

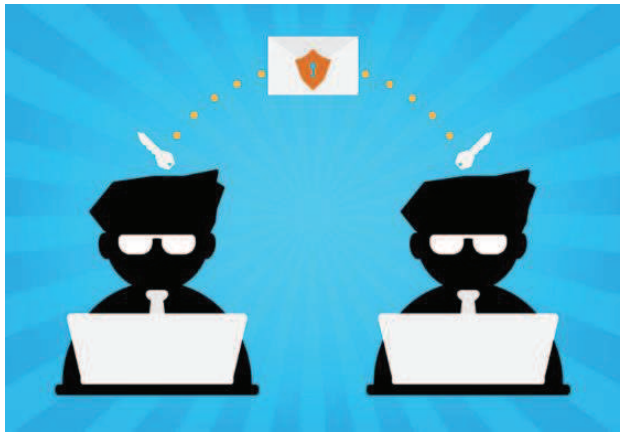
- Encrypt Your Data
  - Encrypted data can only be read with the secret key or password
  - Prevent unauthorized users from reading the content
- Back up Your Data
  - Local vs. Online (Cloud)
- Deleting Your Data Permanently
  - Use available tools to delete permanently: SDelete and Secure Empty Trash, for example
  - Delete the online versions

Strong Authentication

- Two Factor Authentication
  - Physical object
  - Biometric scan
- OAuth 2.0
  - open standard protocol
  - allows an end user's credentials to access third party applications without exposing the user's password.
  - acts as the middle man to decide whether to allow end users access to third party applications.

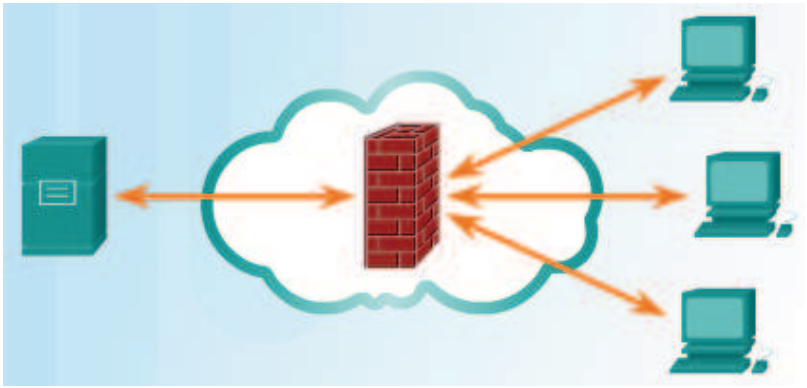
Sharing Too Much Information?

- Do Not Share Too Much on Social Media
  - Share as little as possible
  - Answer secret questions with false answers
- Email and Web Browser Privacy
  - Encrypt you emails
  - Use in-private browsing mode on your web browser



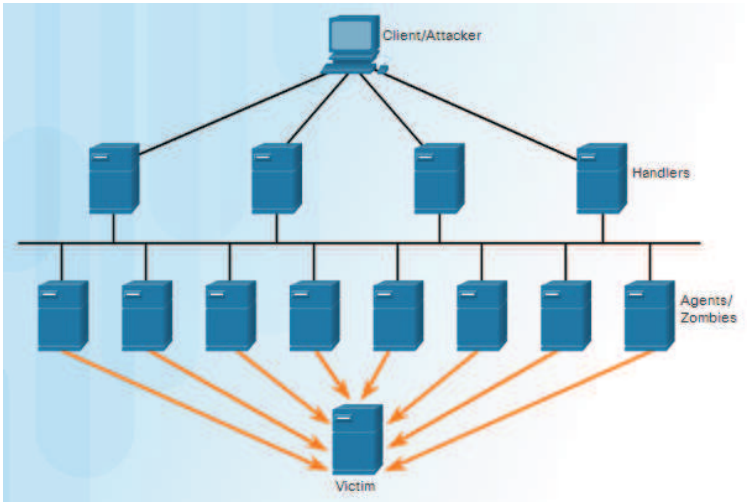
Firewall Types

- Firewall Types
  - Control or filter incoming or outgoing communications on a network or device
  - Can you name a few types of firewalls?
- Port Scanning
  - Process of probing a computer, server or other network hosts for open ports
  - Port numbers are assigned to each running application on a device.
  - Reconnaissance tool to identify running OS and services



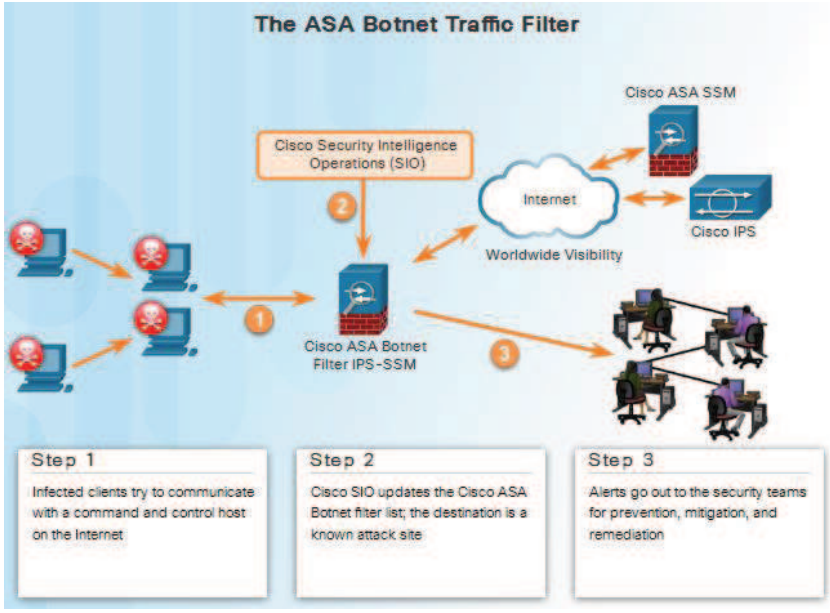
Detecting Attacks in Real Time

- Detect and response to zero-day attacks
- Real Time Scanning from Edge to Endpoint
  - Actively scan for attacks using firewall and IDS/IPS network devices
  - Malware detection
  - Detect network anomalies using context-based analysis and behavior detection
- DDoS Attacks requires real time response and detection



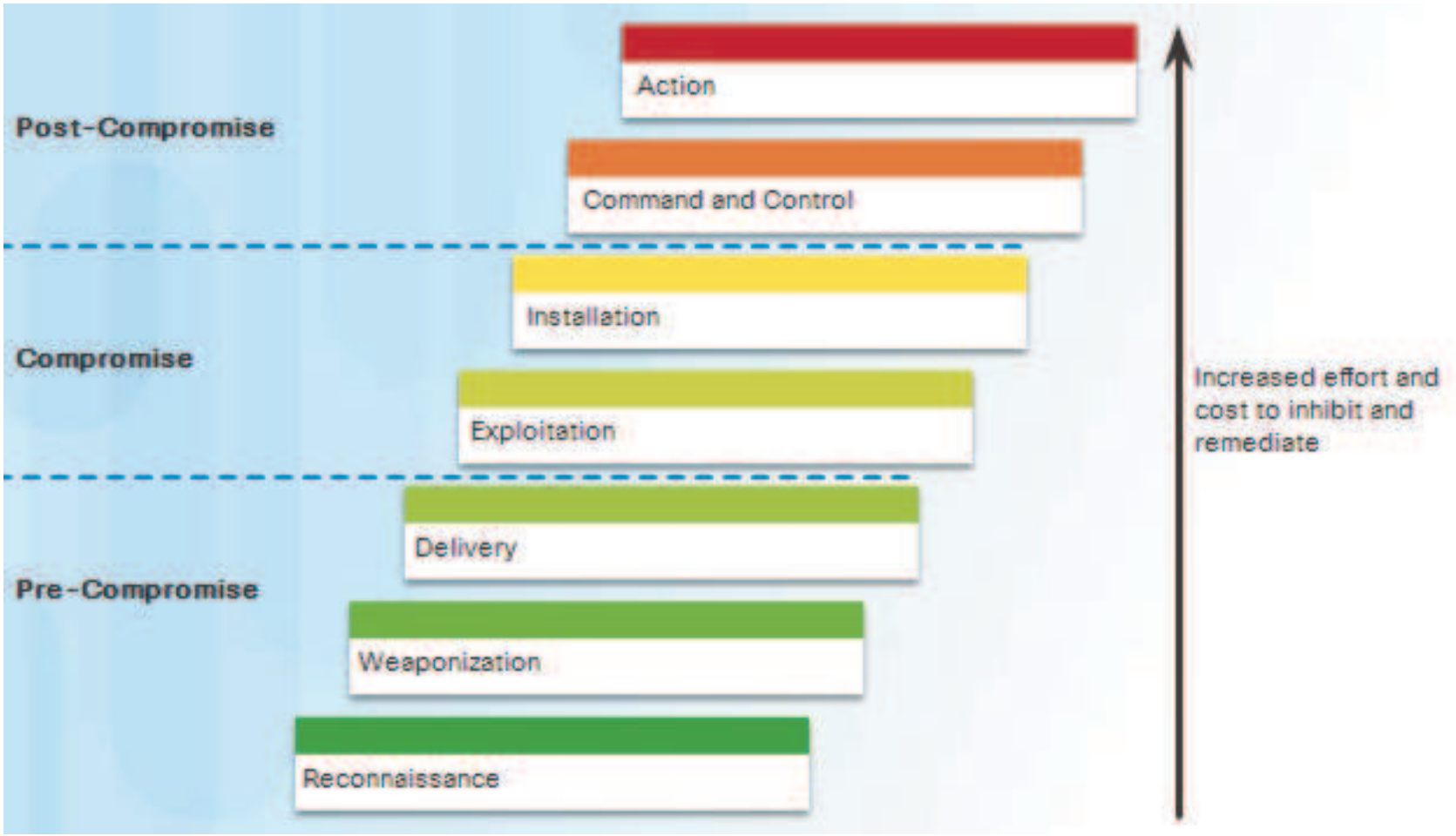
Botnet

- Botnet
  - A group of bots connect through the Internet
  - Controlled by malicious individuals or groups
- Bot
  - Typically infected by visiting a website, opening an email attachment, or opening an infected media file



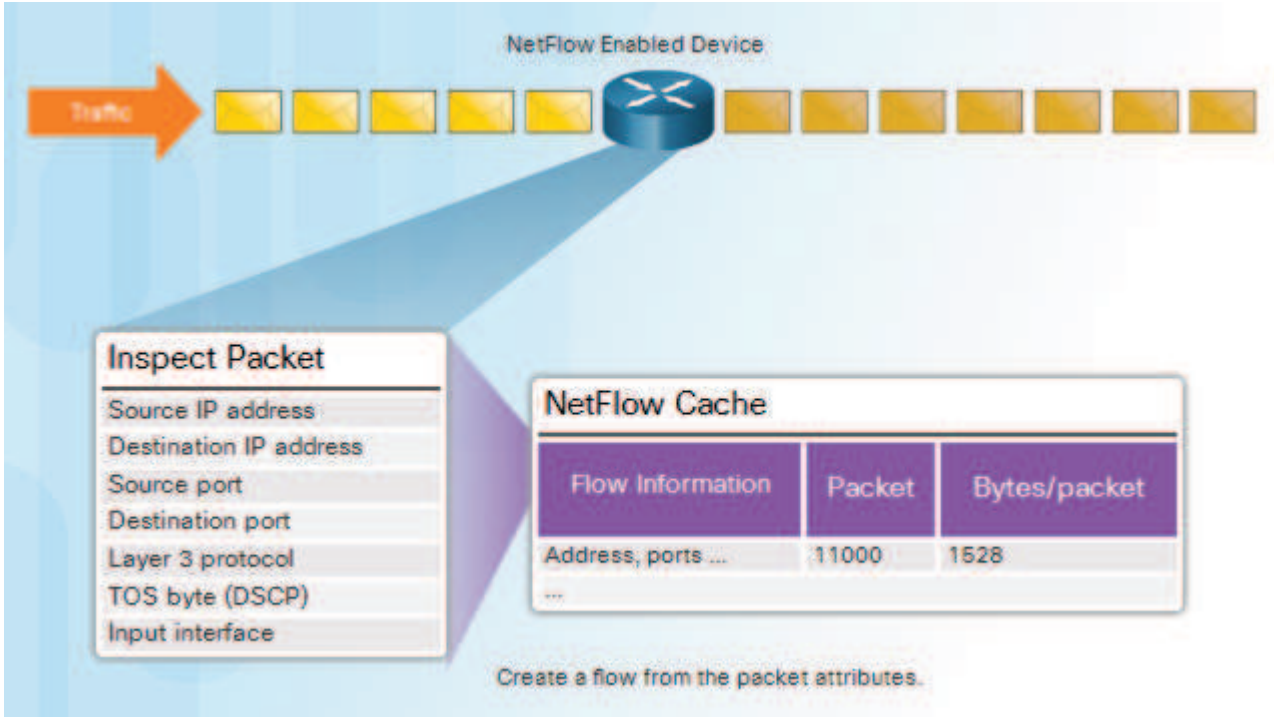
Kill Chain

- What are the stages in a Kill Chain?



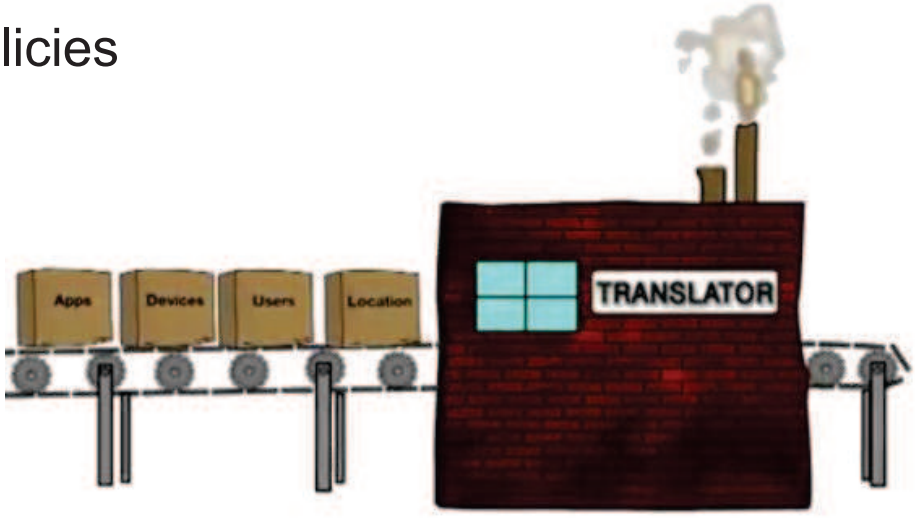
NetFlow and Cyberattacks

- NetFlow
  - Gather information about data flowing through a network
  - Important components in behavior-based detection and analysis
  - Establish baseline behaviors



Tools for Incident Prevention and Detection

- SIEM – Security Information and Event Management
  - Software that collects and analyzes security alerts, logs and other real time and historical data from security devices on the network
- DLP – Data Loss Prevention
  - Stops sensitive data from being stolen or escaped from the network
  - Designs to monitor and protect data in three different states
- Cisco Identity Services Engine (Cisco ISE) and TrustSec
  - Uses role-based access control policies



Infractiunile informatice prevazute de legea 161/2003 (art. 34 – 67)

- http://www.euroavocatura.ro/articole/164/Infractiunile_informatice_prevazute_de_legea_161_2003
- LEGE nr161 din 2003.pdf

- DDOS
- Real time: http://www.digitalattackmap.com/
- How many providers: https://www.safeskyhacks.com/Forums/showthread.php?39-Top-10-DDoser-s-(Booters-Stressers)
- How difficult it is: https://www.youtube.com/watch?v=15snm1GhdAo
- Quiz: https://prismcreate.typeform.com/to/L5XAQGIy