OS Hardening +
Malware, Viruses, Trojans, Spyware, Phishing

Change Default Accounts and Default Configuration

- Default accounts may have passwords that are not changed
  - For example, home router
- Good idea to change them but also restrict permissions

- Software may have default configuration that is insecure
- Or, additional configuration options can make it more secure
- Balance between usability and security

- Let's take a look at some ways we can harden our system ...

Log and Audit

- Operating systems have a central logging system
- Often, log aggregators like Splunk, can pull logs from different sources for a more unified picture
- On the operating system, multiple applications can log to a central system
- Let's take a look ...

Periodic Scanning

- Using tools like nmap to discover software/services on machines
- Can also use tools like OpenVAS
- Must be careful to use tools that might exploit server
- Let's take a look ...

Other OS Security Areas

- DEP - Data Execution Prevention
  - Prevent non-text region of process from being executed
- ASLR - Address Space Layout Randomization
  - Prevent attacks that depend on items being loaded in specific areas in memory
- OS Firewall
  - Can configure firewall rules on the OS, no hardware needed
  - Let's take a look ...
- Automated Services
  - Can install services that automate security
  - Let's take a look ...

Malware

- Broad categorization of software that is malicious
- This includes the following:
    - Viruses
    - Trojan Horses
    - Worms
    - etc

Viruses

- Spreads, self-replicates
- Can be sent in email, embedded within software, on a USB drive, etc
- Very easy to send emails with APIs (e.g. Microsoft Outlook)
- Example: WannaCry
    - Ransomware attack - request funds to unlock machine
    - Kill switch within virus if a URL was enabled
    - Person who discovered kill switch was praised
        - Until it was discovered they sold Trojan malware
        - https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/

Trojan Horses

- Taking a virus or other malware and making it appear as legitimate
- Can be sent via email or packaged as part of software
- Might install a key logger or open a backdoor (bind to a port and listen)

Spyware

- Monitors device such as web activity, key logger, or webcam
- Transmit data to another server
- Some applications misuse permissions, they can be considered in some sense spyware
    - But, the differentiation is whether permission was granted by the user
    - Or, the user is made somewhat aware of data being gathered
    - Recall: https://arstechnica.com/gadgets/2024/05/microsofts-new-recall-feature-will-record-everything-you-do-on-your-pc/
- Can gather passwords or other sensitive information
- Can be used in conjunction with ransomware

Short Survey

- Who completed the short survey?

Phishing

- Can be a mechanism to deliver malware
- Sending an email to an organization to have a user install software or click on a link
- Spear-phishing - Targeting specific people in an organization
  - Using whois service, company web pages, LinkedIn

What Can You Do?

- Install Antivirus software
- Do not open attachments from senders you do not know
  - Be wary of senders you *think* you know
- Only install software from trusted sources
- Verify email senders by checking domains
  - Be wary of emails with unexpected salutations, links to click on, urgency to act, grammar errors, sending gift cards for payment, princes or princesses in countries you have never been, etc
  - Helpful tips: https://www.crowdstrike.com/cybersecurity-101/phishing/spear-phishing/

Questions for Exam

- What questions do you have for the exam?