Northwest State Community College

System Hardening Basics

Made possible through support from the National Science Foundation (NSF) award number 1800929

Objectives

- Discuss System Hardening
- Examine Good Password Hygiene.
- Demonstrate the Importance of Applying Software Patches.
- Disable Unnecessary System Services.
- Discuss and Enable Local System Security Software.

What is System Hardening

- System hardening simply means implementing best practices and practicing good security hygiene
- System hardening can make even old, obsolete and inherently insecure systems more secure
- Failure to harden a system can make even the newest, inherently secure systems very insecure

Why Choose Good Passwords

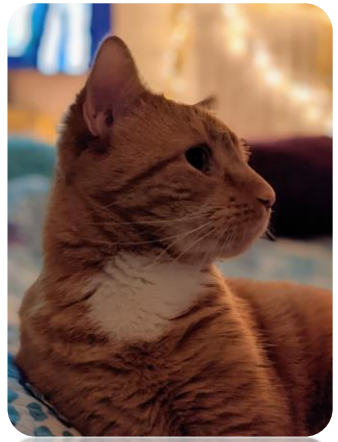
- Alibaba attack
  - Alibaba is a giant Chinese technology company offering services like eBay, Amazon, PayPal and others.
  - Hackers performed password attacks using a database of 99 million usernames
  - Hackers successfully compromised 1 in 5 which is approximately 21 million accounts

Poor Password Hygiene

- Poor password choices?
  - Short passwords
  - Dictionary words
  - Personal data
  - Recycled password

`ag6tb`

`secretpassword`



Ms.Nibbles

Passphrases

- Passphrase – A combination of several words or parts of words
  - Don’t choose common phrases
  - Use phrases that you can easily remember

    ICSTrainingFunInJuly
  - Include punctuation and spaces

    ICS Training Fun In July!
  - Convert some letters to numbers

    I3S Training Fun 1n July!
  - Use only some characters from each word

    I3TrFu1nJu!

Multifactor Authentication (MFA)

- MFA – To combine different types of authentication
  - Things you know

  - Things you have

  - Things you are

Password Managers - Convenient

- Browser based password managers
  - Convenient
  - Are likely accessible by anyone who can gain console access to the browser
  - Are likely accessible by malware running on computer
- Can set a “master” password in Firefox and Edge but not Chrome

Password Managers - Full Featured

- LastPass
  - Free account has severe limitations
    - Only a single device type supports (mobile or computer)
  - Has been compromised several times
- KeePass
  - Secure, lightweight, open-source password manager
  - Offline only
- Bitwarden
  - Free version is fairly comprehensive

Why Apply Patches

- Equifax attack
  - Equifax is one of the three consumer credit reporting agencies in the United States
  - Hackers took advantage of a previously reported but unpatched vulnerability in Apache Struts to gain access
    - Apache Structs is software used to create and manage web sites
  - 143 million records were compromised and many of those had never directly used Equifax

What are Patches

- What is a patch?
  - Often used to fix problems discovered after release.

  - Sometimes used to add functionality.

Why Are Patches Not Applied

- Patching can be time consuming
  - Sometimes system reboots are necessary meaning they must be applied outside regular business hours
  - Sometimes patching cannot be automated
  - Many IT departments are understaffed
- Patches can break things
- It can be difficult to know when patches are available
- Patches are not available for end-of-life products

Patching Best Practices

- Maintain system and software inventory
- Test Patches
- Automate where possible
  - Consider a patch management solution like Windows Software Update Service (WSUS)
- Create a rollback plan in case patching breaks things

Why Disable Unnecessary Services

- Equifax attack
  - Apache Struts was not needed on the servers that were initially attacked

Unnecessary Services

- Disabling unnecessary services:
  - Reduces the attack surface of systems which improves security
  - Improves system performance
  - Simplifies patch management
  - Should be done cautiously and with extensive testing to make sure critical services are not accidently disabled

Why Enable Local Security Software

- Colonial Pipeline Attack
  - Colonial pipeline is the largest pipeline system for refined oil in the United States
  - It is possible that this attack may have originated through a phishing attack
    - The attack may have stolen login credentials
    - The attack may have installed malware that installed a local backdoor
    - Properly installed, configured and updated antivirus software will stop many malware programs
    - Properly installed, configured and updated host-based firewalls will stop many backdoor programs
  - Caused fuel shortages, higher prices and panic for several day

Local Security Software

- Anti-virus
  - Anti-virus software should be installed, configured and regularly updated on individual host machines
- Host based firewalls
  - Host based firewalls should be installed, configured and regularly updated on individual host machines
- Logging
  - Logging should be enabled on host machines to make troubleshooting and forensic analysis easier

Summary

- Examine Good Password Hygiene.
- Demonstrate the Importance of Applying Software Patches.
- Disable Unnecessary System Services.
- Discuss and Enable Local System Security Software.

For More Information

- For further information go to https://www.nl.northweststate.edu/camo or contact:
  - Tony Hills – thills@northweststate.edu – 419-267-1354
  - Mike Kwiatkowski – mkwiatkowski@northweststate.edu – 419-267-1231

Made possible through support from the National Science Foundation (NSF) award number 1800929