Intro to System Hardening

oresec.mines.edu/attend
Cybersecurity Awareness Month Survey

Please fill out this anonymous form:

Sent in Discord and Matrix

https://forms.gle/WkQvWxaxU4rhm8ZA8
What is Hardening?

- Act of securing a computer system or network of systems to make them more secure
  - Patching
  - Altering settings of system and programs
  - Removing unneeded features/access
  - Adding additional security features
Why is System Hardening Important

- Default settings are rarely the most secure
- Users may need to be culled
- Old programs may need to be removed
- Newly discovered vulnerabilities may need to be fixed
- Security might need to be enhanced
How do I go about this?

Firstly, update your device or program!

- **Linux: pretty easy**
  - package manager (sudo apt update && sudo apt update)
  - Manually check for updates

- **Windows: a little harder**
  - Windows Update
  - Updater Tools
  - Searching for updates in a program
  - Manually checking for updates
Speaking of updates

Should I setup automatic updates?

- In most cases, yes
  - Get security updates as soon as possible
  - But, at the mercy of developers

- Production or highly-secure environments, likely no
  - Must be manually monitoring vulnerabilities and patches
  - Likely you will test updates before pushing to these environments
On to the fun stuff, but first...

You must consider the system you are securing...

- What is its purpose?
- How is it accomplishing that?
- Who should have access?
- What should they have access to?
- How is access granted?
- How is this system connected to everything else?
Users & Groups

- Users that shouldn’t be there should be removed
- Legitimate users need sufficient protections
  - Good password (managed by password rules)
  - Some systems may need MFA
- Users need to have proper permissions
  - You don’t want every user to have administrative access to the computer
- Groups should only contain users with need to be in it
  - Administrators / sudoers / wheel / etc.
- Groups also have certain permissions that need to be maintained
How to change users

Linux

- useradd (add a user)
- usermod (modify a user, like groups)
- userdel (delete a user)
- /etc/group (groups and users in them)
- /etc/passwd (user info)
- /etc/shadow (hashed passwords)
- /etc/login.defs (settings for above commands)
- Libpam (authentication module commonly used)

Windows

Via Computer Management, Local Security Policy, CMD

- **GUI Method**
  - Local Users and Groups
  - Right-click or double-click to change user
  - Edit user rules via Local Security Policy

- **CMD Method**
  - net user <user> /<option> (modify users)
  - net accounts /<option> (modify settings)
  - net group <group> /option (modify group)

- **On Active Directory Systems:**
  - Active Directory Users and Groups app
  - Very similar to GUI above
  - Edit settings via AD Group Policy Editor
Programs

- **Systems have a specific purpose or job**
  - Programs assist the system in performing this
  - Like: apache -> web server
- **Additional programs can introduce vulnerabilities**
  - You don’t need telnet everywhere
- **Programs need to have access to certain info**
  - But should be limited to as little info as possible
- **Certain parts of operating systems can schedule programs to run automatically**
- **System access services are often the easiest or only way into system (ssh, rdp, ftp, etc.)**
Securing programs/processes

**Linux**

- Again, package manager
  - `apt list --installed` (list installed)
  - `apt remove` (remove package)
- `ps` (shows running processes)
  - `ps -eF`
- **Cron**
  - Linux job scheduler
  - Can schedule commands to run periodically or on startup
  - You can often view these in `/etc`
- Manually look/scan for malicious binaries

**Windows**

Via: Group Policy or Local Security Policy

- Under Local Policies
- Audit Policies: Success, Failure for all
- User Rights Assessment:
  - Disable log on as service
  - Only Admins able to take ownership of files
- Security Options:
  - Use existing GPO or hardening guide
  - Disable default admin/user account
  - Network Security/Network Access
- `taskmgr` to find programs (startup!)
- `C:/Program Files, C:/Program Files (x86)`
- Task Scheduler for scheduled jobs
Securing files

- There are two major parts of this:
  - Securing access to critical files and directories in the filesystem
  - Removing malicious or unwanted files from the filesystem

- Files are typically managed through an Access Control List (ACL)
  - Permissions can be changed on files such that only specific users or groups can access them
  - Minimum required access should be followed

- Malicious files, once on a filesystem can then be accessed by programs and cause harm to the system
  - Files can also violate acceptable use and shouldn’t be allowed on systems
How to secure files

Linux

● `ls -l` (shows file permissions)
● `chmod` (change file permissions)
  ○ `chmod 777 <file>`
  ○ Grants read-write-execute permission to everyone (not typically good)

Windows

● Right-Click -> Properties -> Security Tab
● SYSTEM, Admins should have full access
● Special places like C:\Windows should be Admins/SYSTEM only
● `cacls` (change file permissions)
Networking Security

- Host firewalls protect the system from malicious connections and programs
  - Here you can manually block programs from listening on ports
  - You can also drop external traffic destined for certain ports
  - Linux: Everything is built on iptables
    - Programs like UFW can simplify firewall rules
- If the firewall rules are relaxed, you can use other tools to view open ports
  - Linux & Windows: netstat - allows you to view all programs that are listening
  - External: Other tools can scan a host computer to see which ports respond to traffic like nmap
Additional Security Enhancements

- Manually going through settings and checking files isn’t efficient and is rarely the best option
  - Antivirus software can help to scan files and find malicious files
  - Rootkit detection software can help look through settings and critical parts of the operating system to detect malicious configurations
  - So many production-grade software for detecting and fixing issues

- Logging software is useful to install in larger systems/networks
  - Solutions like Splunk and Graylog help to conglomerate logs and help infer info

- So much more can be put in place
  - Proxies, network encryption, sandboxing, etc..
  - Often times these take a lot of time/and or a good amount of money
Barely scratching the surface

- Everything has settings
  - Operating system, programs, etc.
  - Can follow hardening guides for the most secure settings
- New vulnerabilities pop up all the time
  - Updating isn’t always an option (not released yet, incompatibilities)
  - May require in-house solutions