

**Air Force Association's CyberPatriot**  
The National High School Cyber Defense Competition



**How to Mitigate and Stay Safe**  
**Module 5**



# Patching



- Patches
  - Software ‘fixes’ for vulnerabilities in operating systems and applications
- Why Patch?
  - Keep your system secure
  - Viruses and worms usually attack known vulnerabilities
  - Hackers can easily attack systems that have not been patched



# Patching

- For Windows systems and Microsoft applications
  - Can be automatically downloaded and installed
    - For Windows, configure Windows Update program
    - Click Start -> Settings -> Control Panel -> System and Security -> Windows Update -> Turn automatic updating on or off
  - Use Windows Update to find latest patches
    - Click Start -> All Programs -> Windows Update
  - Install manually from [www.Microsoft.com](http://www.Microsoft.com)
- For specific applications, visit vendor websites to check for updates
- Utilize websites showing the latest patches
  - <http://www.softwarepatch.com/>
- Monitor websites with vulnerability alerts
  - <http://www.us-cert.gov/cas/alerts/index.html>



# Patching

- Linux

- Patches are also known as “packages”
- Package Managers
  - GUI used to keep OS and applications up to date
  - Used to install, uninstall, search for, or update packages
- Command Line interface (CLI)
  - Download the source for every out of date program, then compile and install
  - If a program had any dependencies, you have to hunt down the dependency
  - Use the “apt-get” command or “yum” depending on distro



tomshardware.com

- Unix

- Solaris
  - Command line (pkgadd, pkgrm, pkginfo)
- HP-UX
  - Software Package Builder (SPB) – provides both GUI and CLI



# Objectives

- Keep in mind when patching in high availability environments
  - Make sure patch is relevant
  - Keep patch level consistent on all servers
  - Test patches before applying to avoid the 'fix' breaking another business critical function
  - Have a backup plan in place
    - Back up your system prior to patching so you can restore if necessary



Geek-easy.com



# Anti-Virus Software

- Anti-virus
  - Software that can detect and block malware before it infects your computer
  - Looks for patterns based on the signatures, or definitions, of known viruses
  - Must be kept up to date
    - New viruses appear daily therefore signature database must be updated on a regular basis
  - Use to scan your system either manually or automatically
    - Scan file system of the computer
    - Scan email attachments, downloaded documents, cds, usb drives, etc. before opening or using them
- Anti-virus software packages are discussed in the 'Threats and Vulnerabilities' module



# Spyware

- Spyware
  - Malware installed on a system that collects information about users without their knowledge
  - Tracks users' Internet activity for marketing purposes
  - May use cookies in your Internet browser to track
  - May cause added CPU activity, disk usage and network traffic on a system
- Detect and remove
  - Anti-spyware programs
    - Stand alone or additions to anti-virus software
    - Provide real time protection or detect and remove existing spyware
    - Scans the windows registry and files and removes those that match signature files
    - Keep signature database up to date



# Auditing

- Audit regularly
  - Setting up audit policies is critical to the security of an organization's assets (Remember policies set up in Windows and Unix Modules)
  - Helps you measure the adequacy and effectiveness of controls in place
- Auditable items
  - Users
    - Permissions, activities
  - Files and Objects
    - Accessibility
    - Manipulation
    - Integrity
  - Logs
    - Captures defined events and activity





# Monitoring

- Monitor

- Systems can be monitored for all kinds of things provided logs are stored and accessible

Logs will show activities in regards to the following (\*\*Logs capture events based on the policies set up in Windows and Unix Modules)

- Users
  - Violating security policies, attempting unauthorized access
- Files and Objects
  - Monitor access by unauthorized users

- Monitoring on a regular basis ensures confidentiality, integrity, availability and authenticity



# Vulnerability Assessment

- Vulnerability
  - *“A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. “*
    - *National Institute of Standards and Technology*
- Vulnerability Assessment
  - Identify potential vulnerabilities and evaluate the effectiveness of various security controls implemented within the infrastructure
  - Regularly run a network scan to identify infrastructure gap and non hardened devices
  - Run a vulnerability scanner on a regular basis



- Vulnerability Scanners
  - A tool that scans devices for vulnerabilities such as allowing unauthorized access to sensitive data, misconfigurations, default passwords not changed, etc.
- Types
  - Host based
    - Tool scans an individual computer for vulnerabilities
  - Network based
    - Tool scans network for vulnerabilities
  - Database
    - Scans for vulnerabilities in the database server(s)



## ● Vulnerability Scanners

### ● Netstat

- This tool is used on the local host to identify its open ports
- Command within Unix and Windows

### ● SuperScan (Port Scanner)

- A freeware tool for Windows which will perform a UDP and TCP port scan
- <http://www.mcafee.com/us/downloads/free-tools/superscan.aspx>

### ● Nessus

- Free for personal use in a limited “home” license
- <http://www.tenable.com/products>

### ● Internet Security Scanner (ISS)

- A network security scanner that can be used for Windows
- <http://its.virginia.edu/network/issdoc.html>



## ● Vulnerability Scanners (more)

- Microsoft Baseline Security Analyzer (MBSA)
  - Evaluates a system's configuration and provides a report with specific recommendations to improve security. Also recommends missing hotfixes and configuration changes. This should be run regularly to check for new vulnerabilities.
  - <http://www.microsoft.com/download/en/details.aspx?id=19892>
- RPCDump (rpcdump.exe)
  - This tool helps determine which RPC services have which ports open
- Fport
  - A great tool from [www.foundstone.com](http://www.foundstone.com) used to scan the system to see what is open
  - <http://www.mcafee.com/us/downloads/free-tools/fport.aspx>
- Security Auditor's Research Assistant (SARA)
  - A tool derived from the infamous (at least in 1995) SATAN scanner
  - Last release date was May 2009 (<http://www-arc.com/sara/>)



# Perform a Scan

- First, be certain you have permission to scan network or hosts
- Choose a tool
  - Discover your network devices (servers, firewalls, applications, etc.)
    - Know the IP address range you want to scan
  - Prioritize your assets
    - Critical to non-critical
  - Identify vulnerabilities
    - Run a scan using the tool
  - Analyze threats
    - You may choose to accept the risk rather than remediate a vulnerability due to a valid business reason
  - Remediate
    - Apply patches, turn off services, etc.
  - Eliminate your vulnerabilities
    - Run your scan again to make sure your vulnerabilities no longer exist



# Perform a Scan

- Examples and 'how to'

- Scans in Nessus:

- <http://www.symantec.com/connect/articles/introduction-nessus>
- [http://netsecurity.about.com/od/stepbystep/ss/nessus\\_scan.htm](http://netsecurity.about.com/od/stepbystep/ss/nessus_scan.htm)

- Scan using Fport:

- <http://www.mcafee.com/us/downloads/free-tools/fport.aspx>

- Simple scan using Kaspersky:

<http://support.kaspersky.com/kav2012/settings/scan?qid=208284603>



# Protective Measures

## Examples of Protective Security Measures per SANS

- Access controls
  - User IDs and passwords, appropriate password and security policies, separation of duties
- User authentication, with appropriate use of controls, where possible (e.g. smart cards, biometrics, etc.)
- Workstation lock screens
- Encryption
- Proper registry permissions
- Proper directory and file permissions
- Properly defined user rights
- Social engineering prevention
- Applying patches/updates
- Firewalls
- VPN tunneling
- Screening routers







# Protective Measures

- **More examples of Protective Security Measures per SANS**
  - Anti-virus software
  - Prompt removal of terminated/transferred employee accounts, default passwords, and unnecessary services running on the system
  - Implementing and enforcing change control policy to limit activity to authorized users only
  - Review and management signoffs of user authorizations
  - Use of checksums with attendant software to report file modifications
  - Enable audit logging and perform log reviews
  - Review of open ports and services
  - Properly configured routers
  - Searching for and disconnecting unauthorized or poorly configured modem services



# References

- <http://www.softwarepatch.com/>
- <http://www.us-cert.gov/cas/alerts/index.html>
- [http://www.sans.org/reading\\_room/whitepapers/basics/vulnerability-assessment\\_421](http://www.sans.org/reading_room/whitepapers/basics/vulnerability-assessment_421)
- <http://netsecurity.about.com/od/freesecuritytools/a/aafreevulns-can.htm>
- <http://sectools.org/vuln-scanners.html>
- <http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>