Lab- CyberPatriot Exhibition 2

Michael Herr
Hawaii CyberPatriot Boot Camp for Teachers
Honolulu Community College

July 25, 2013

VM Options

- Edit settings of VM
- Increase RAM if possible, 2 to 4GB
- Networking
  - Bridged is my preference, it puts the image on the same network as you. Easy to perform NMAP, scanning, etc from an external system
  - NAT (Network Address Translation) – Use this option of bridging does not work

Open Virtual Machine

- If you are prompted for “Move or Copy”, always select “I copied it”

Readme file

- Background information for the Exhibition Round 2 image:
- When you launch this image you should automatically be logged in as "user". The default password for this account is set to "password."
- This system is a Windows 7 based workstation that belongs to the Cabo Seafood Corporation.
- It is not part of a domain, nor does Cabo Seafood have any plans to join it to a domain in the near future. This workstation sits in a common work area of Cabo's headquarters office and is used by a number of personnel including the following:
- - Sheldon Jones
  - Priya Koothrappali
  - John Chan
  - Geraldo Rodriguez
  - Maria Lopez
  - Julie Spears
  - Amy Miskovsky
- The primary admin account for this workstation is called "user". Cabo Seafood has a very small IT staff consisting of John Chan and Priya Koothrappali. This is a "regular" workstation used only for standard office tasks such as checking email, word processing, spreadsheets, and web surfing. Cabo's security policies require that all user accounts be password protected, that all systems be fully patched with the latest operating system and application patches, and that remote connections to workstation systems are not allowed. Cabo Seafood also prohibits the presence of any media files and "hacking tools" on any workstations.

Information gathering

- Get the IP address of system and write it down
- Get open TCP and UDP ports
  - Open TCP – Nmap –sT <system ip address>
  - Open UDP – Nmap –sU <system ip address>
  - Interrogate Services – nmap –sV p1-65535
- User accounts

Methodolgy

- Under attack?
  - Outside in
- Normal conditions
  - Longest and multitask

Passwords—for competition purposes

- Students should come up with a common password scheme that will be used across all accounts
- This should be written down
- Technically, the same password could be used on all accounts – this is not best practice, but it typically works for the competition

Scoring System

- Near real-time scoring report located on desktop – Launch it
- During the competition, you be given clear instructions on how to register your team and image
- Check for
  - Internet Connection
  - CyberPatriot Connection Statsu
  - CyberPatriot Upload Status

Microsoft Baseline Security Analyzer

- Checks for common misconfigurations
- Download and install from
  - www.cyberhui.org/resources
- Double click icon on desktop to run
- Scan My Computer
  - Leave defaults
  - Click Start Scan
- Review Results and fix as necessary

Enable Windows Update

- Start
- Windows Update > click it
- Enable it

- Typically you would run it. Run it until there are no more updates available

- Today we are going to use WSUS Offline

Computer Management

- Click Start, right click My Computer and Click Manage
  - User Accounts and Groups
  - Services
  - Shares

  - Task Scheduler – see if rogue tasks are scheduled
  - Event Viewer – Check logs and log size/overwrite settingsd

Check Services

- Sort by description, look for blank and investigate further
  - Open Service and look at executable path
  - Find file, check properties
- Look for unauthorized services (IIS, Web, Telnet, etc)
  - Disable them
- For a question on a service, visit:
  http://www.theeldergeek.com/services_guide.htm#List of Services

Shares

- Click on Shared Folders > Shares
  - Admin Shares that should be ok to keep
    - ADMIN$
    - IPC$
    - C$
  - Check other shares to see if they are within policy

Check User Accounts and Groups

- Expand Local Users and Groups
- Things to look for
  - Unauthorized Accounts –don't delete, just disable (delete as a last resort)
  - Passwords that don't expire
  - Ensure guest is disabled
  - Bad group memberships
- Change all passwords

Check Add/Remove programs

- Removed unneeded applications
- Turn Windows Features on/off

- Check for 3rd party applications
  - Note and update them if required

Check folders for unauthorized content—policy violation

- User folders
- Root folders

- Skilled competitors could write a quick script to search the file system for media type files.
  - *.mp3, *.wmv, *.avi, etc.

Check for rogue services

- Download and run CrowdInspect
  - http://www.cyberhui.org/resources
- Extract file
- Run CrowdInspect
  - Sort by listening ports
  - Investigate Rogue applications/services
  - Kill
  - Delete associated files

Firewall

- Control Panel
  - Windows Firewall
- Make sure it is enabled, unless you have a third party firewall
- Check the rules
  - Inbound
  - Outbound

Check Startup

- Start
- Type msconfig
- Check startup

Antivirus, Antimalware, Antispyware

- Antivirus
  - Microsoft Security Essentials
    - Download, Install, Update, run
      - www.cyberhui.org/resources
  - Avast
  - AVG
  - ClamAV
  - Many other free versions. Pick one
- Antimalware / Antispyware
  - Malwarebytes

Local Security Policy

- Provides the ability to apply local security policy on the system
- Windows XP and below can use the Security Configuration and Analysis and Security Templates to compare
- Prerequisite – DISA Analyze Template
  - www.cyberhui.org/resources
  - Files are normally located at iase.disa.mil under STIGs

Local Security Policy

- Start > mmc
- File > Add/Remove Snap-in
- Find
  - Security Configuration and Analysis > Add
  - Security Templates > Add
- Locate the zip file you downloaded
- Extract the file to documents\security\templates
- Expand Security Templates right click the folder inside and click refresh

Local Security Policy

- Right click Security Configuration and Analysis and click Open Database
  - Type: security > Open
  - Browse and select template
- Right Click Security Configuration and Analysis and click Analyze now
  - Select OK to the log
- Review Settings differences

- Open Local Security Policy
  - Start > Type Local Security Policy > Click to Open

Other noteworthy areas

- Vulnerability Scanners
  - Nessus is free and can be ran within the image or external
  - Scan > Patch > Scan
- Secure Shares – Ensure share settings do not have full control for everyone
- Check for Rootkits (Rootkit buster)
- Remove Games
- Simple Network Management Protocol – If needed, check services and change community strings
- Browser hijacked > hijackthis (antimalware may fix too)

CyberPatriot 6 Exhibition Round 2

Report Generated At: 07/25/13 04:25:20 Central Daylight Time

Approximate Running Time: 50:24:32

Current Team ID: 000000000

100 out of 100 points received

Connection Status: GOOD

Internet Connectivity Check: OK
CyberPatriot Connection Status: OK
CyberPatriot Score Upload Status: OK

10 out of 10 known issues fixed:

Removed Prohibited MP3 file - 10 pts
Windows Service Pack 1 is installed - 10 pts
A minimum password length is required in the account policy - 10 pts
Windows Update service is enabled and running - 10 pts
Microsoft Telnet service has been stopped - 10 pts
A maximum password age has been configured that is less than 999 days - 10 pts
User Maria Lopez's account is now password protected - 10 pts
User Julie Spears' account is now password protected - 10 pts
Former employee Rick Lopez's account has been removed (rlopez) - 10 pts
Unnecessary account cabo has been removed - 10 pts

Want more info?

Cyber Hui

www.facebook.com/cyberhui

@cyber_hui

www.cyberhui.org

info@cyberhui.org

www.uscyberpatriot.org

Cyber Hui