Lab 2
Baseline Security

Due Date: September 16, 2020 at 11:59pm
Submission Location: iLearn for documents, cyber range environment for systems
Points Available: 8

Objectives

1. Understand how to install software on both Windows and Linux systems.
2. Understand the importance of virus/malware scanning software through the installation/configuration of anti-virus/anti-malware software on multiple platforms.
3. Understand how to establish a baseline security level for the team's systems using common tools.
4. Understand basic incident response and change management procedures.

Checklist

1. Add DEVOPS user to Windows Domain
2. Add DEVOPS user to WWW server
3. Install Malwarebytes Free on Windows DC
4. Install Clam AV on WWW server
5. Scan both Windows and WWW server
6. Install and run lynis on WWW server
7. Install and run openvas

Outcomes

1. Students will become familiar with malware/virus scanning software on both Windows and Linux based systems.
2. Students will become familiar with vulnerability scanning using Nessus.
3. Students will understand the importance of documentation and how to better document changes.

CAE Topics Addressed

- CSF - 4 Basic Risk Assessment
- CSF - 10 CIAAA-NP
- CSF - 13 Security Mechanisms
- CSF - 14 Malicious Activity Detection
- CSP - 1A - 1N Core Cyber Principles
- ISC - 1A Non-Storage Devices
- ISC - 2 Storage Devices
- ISC - 3A-3B Virtualization / Cloud
- ISC - 5 Networks
- ISC - 12A OS and Application Updates
- ISC - 13A Vulnerability Windows
- BNW - 4 Common Network Devices
- BNW - 6 Network Services
- BNW - 6 Network Applications
- BNW - 8 Use of basic network administration tools

- LSA - 2 User Accounts Management
- LSA - 3 Command Line Interfaces
- LSA - 4 Configuration Management
- LSA - 5 Updates and Patches
- LSA - 7 Managing System Services
- LSA - 8 Virtualization
- OSA - 2 User Accounts Management
- OSA - 3 Command Line Interfaces
- OSA - 4 Configuration Management
- OSA - 5 Updates and Patches
- OSA - 7 Managing System Services
- OSA - 8 Virtualization
- WSA - 2 User Accounts Management
- WSA - 3 Command Line Interfaces
- WSA - 4 Configuration Management
- WSA - 5 Updates and Patches
- WSA - 7 Managing System Services
- WSA - 8 Virtualization

NICE Framework Categories

- Securely Provision (SP)
- Operate and Maintain (OM)
- Analyze (AN)

Instructions

1. Add “devops” user to the Windows domain with admin privileges. Set the password to “Password123!”
2. Add “devops” user to WWW server with sudo privileges. Set password to “Password123!”
3. Install ClamAV on WWW server and run a scan:

   https://www.howtoforge.com/tutorial/clamav-ubuntu/

a. Install with '**sudo apt install clamav**'

b. If you get an error when running '**sudo freshclam**' then run '**sudo rm /var/log/clamav/freshclam.log**' and re-run.

4. Install Lynis on the WWW server and run it.

   a. Install using **apt install lynis**

   b. Run a system scan with Lynis using the following command as root or sudo "**lynis –c –Q**". The results of the scan will be placed in a log file located at "/var/log/lynis.log".

   c. Analyze the list of suggestions given by Lynis by issuing the command as root or sudo "**grep -i Suggestion /var/log/lynis.log | less**".

5. Install Malwarbytes Free on Windows Server 16 'dc' and Windows 10 'wrk' machine and run a scan.

6. Install openvas9 on the WWW server.

   a. '**sudo apt install software-properties-common'** on ubuntu.

   b. Follow the guide below on installing and running openvas after installing the above package. **Note:** when running the 'sync' commands in step 5 of the guide below may take a while to run.
   https://www.fosslinux.com/7320/how-to-install-and-configure-openvas-9-on-ubuntu.htm

   c. You can skip **step 8** in the guide above.

   d. **From Windows** (either box will work) go to https://192.168.x.130:4000 in a browser. This will be your openvas instance. username/password is **admin/admin**

   e. Run two scans using the guide provided above:

      i. Windows Server 2016: 192.168.x.2

ii. Branch office Linux server: 10.0.1.250 **Note:** this is a branch office server that you are only allowed to scan. The regular admin is on vacation this week.

Deliverables

Submit as one submission for each team. PDFs ONLY

1. Screenshot the result from each step. (should be 7 screenshots for 6 instructions) Step 6 needs 2 screenshots.
2. Describe 3 of the vulnerabilities that openvas finds and come up with a remediation plan.
3. List three of the suggestions given in the Lynis scan report and describe their importance in hardening the system against attacks.
4. Which of these hardening techniques have you used in this lab?
    a. WULAI
        i. Weed
        ii. Update
        iii. Log
        iv. Access
        v. Isolation
5. Continue extending your changelog throughout the labs and submitting it.

Resources

Linux

- Ubuntu Linux Tutorials - https://tutorials.ubuntu.com/
- Linux System Administration Basics - https://www.linode.com/docs/tools-reference/linux-system-administration-basics/#smtp-servers-and-email-issues
- Linux Security Tools - https://www.ubuntupit.com/best-20-linux-security-tools-recommendation-from-the-linux-experts/

Windows

- Windows Server 2016 Tutorial Step by Step Full - https://www.youtube.com/playlist?list=PLcRhfKiWZmM9F7lY6DRXVwiYpNB2RO6F9

- Using Windows Admin Tools Like a Pro Series - https://www.howtogeek.com/school/using-windows-admin-tools-like-a-pro/
- TutorialsPoint Windows Administration Tutorials - https://www.tutorialspoint.com/listtutorials/windows/administration/1

Documentation

- Cyborg Systems - Documentation is the Most Valuable Thing You Do - http://cyborginstitute.org/projects/administration/documentation/