PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Networks and Cybersecurity Essentials (ACCA4024)

Lab 10: Hardening

Cisco | Networking Academy®
Mind Wide Open™

Objectives

Use security auditing tool to harden a Linux system.

Tasks

1. Use “Lynis” an open source security auditing tool with an automated set of scripts developed to test a Linux system.

   Auditing a system for potential misconfigurations or unprotected services is an important aspect of system hardening.

Required Resources

- PC with Ubuntu 16.0.4 LTS installed in a VirtualBox or VMware virtual machine. (*Alternatively,* Any Linux Platform)
- Internet Connection to refer the outcomes
- References:
  - Lynis: https://cisofy.com/lynis/

Task 1

➔ Login as User Cisco.

➔ Go to Terminal and Type the following commands and examine

➔ Run The Lynis Tool by changing the directory to Downloads → Lynis

➔ At the command prompt, enter the following command and enter the password password when prompted:

```
cisco@ubuntu:~/Dowloads/lynis$ sudo ./lynis update info
```

This command verifies that this is the latest version and updates for the tool at the time of writing of this lab.

➔ Run the Tool: Type the following command in terminal and press Enter:

```
cisco@ubuntu:~/Downloads/lynis$ sudo ./lynis --auditor cisco
```

The tool will begin auditing using the user cisco as the auditor. Note: You will receive warnings.

➔ To continue with each stage of the audit press Enter.
➔ You will receive suggestions.
➔ You will receive a notification for any configuration that is weak

- ➔ You will receive detailed security enhancement suggestions as well as a final summary which provides the location where you can find the log file.
- ➔ **Review Results**
- ➔ **Scroll up to the results section after the tool is finished running.**

How many Warnings did you receive?

4

```
Warnings (4):
----------------------------
- Version of Lynis is very old and should be updated [LYNIS]
    https://cisofy.com/controls/LYNIS/

- apt-get check returned a non successful exit code. [PKGS-7390]
    https://cisofy.com/controls/PKGS-7390/

- Found one or more vulnerable packages. [PKGS-7392]
    https://cisofy.com/controls/PKGS-7392/

- Couldn't find 2 responsive nameservers [NETW-2705]
    https://cisofy.com/controls/NETW-2705/
```

How many Suggestions did you receive?

35

```
Suggestions (35):
----------------------------
- Set a password on GRUB bootloader to prevent altering boot configuration (e.
g. boot in single user mode without password) [BOOT-5122]
    https://cisofy.com/controls/BOOT-5122/
- Install a PAM module for password strength testing like pam_cracklib or pam_
passwdqc [AUTH-9262]
    https://cisofy.com/controls/AUTH-9262/
- Configure minimum password age in /etc/login.defs [AUTH-9286]
    https://cisofy.com/controls/AUTH-9286/
- Configure maximum password age in /etc/login.defs [AUTH-9286]
    https://cisofy.com/controls/AUTH-9286/
- Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
    https://cisofy.com/controls/AUTH-9328/
- Default umask in /etc/init.d/rc could be more strict like 027 [AUTH-9328]
    https://cisofy.com/controls/AUTH-9328/
- To decrease the impact of a full /home file system, place /home on a separat
ed partition [FILE-6310]
    https://cisofy.com/controls/FILE-6310/
- To decrease the impact of a full /tmp file system, place /tmp on a separated
```

Scroll through the suggestions and select one. You will research a suggestion that you can implement to address the issue.

Which suggestion are you addressing?

```
  - Set a password on GRUB bootloader to prevent altering boot configuration (e.
g. boot in single user mode without password) [BOOT-5122]
      https://cisofy.com/controls/BOOT-5122/
```

What is your suggested solution?

I suggest that a password is configured in grub. This password will help stop unauthorized personnel from changing core software or even the operating system. I suggest that the password is at least 8 characters long, with at least one number, one upper and lower case letter and a special symbol to ensure it is difficult to guess.

Learnings from tutorials so far:

Part 1 (Packet Tracer, Host Machines)

- ✓ ***Build a home Network***
- ✓ ***Understand and configure IP Address***
- ✓ ***Use Ping/ Trace route Utility to check the connection status***
- ✓ ***Use ipconfig /all command to determine the MAC address of a Windows computer on an Ethernet network.***
- ✓ ***Analyze a MAC address to determine the manufacturer.***
- ✓ ***Analyze the Wired and Wireless Network connection.***
- ✓ ***Analyze Address Resolution Protocol (ARP).***
- ✓ ***Connect to a Wireless Router and configure the basic settings in a wireless router and add security features.***
- ✓ ***Use nslookup command to understand the url to ip conversion.***
- ✓ ***Configure basic connectivity settings in Intermediate devices (Switch/ Router).***
- ✓ ***Work with SBA Packet Tracer Files/ environment***
- ✓ ***Configure ftp, web, email, dns, ntp and aaa Servers***

Part 2

- ✓ ***Set up a virtual lab environment***
- ✓ ***Troubleshooting the virtual lab environment***
- ✓ ***Working with virtual machines***
- ✓ ***Authentication, Authorization and Accounting***
- ✓ ***Threats and Vulnerabilities – Using NMAP***
- ✓ ***Hide and Seek – Use Steghide to hide a data file within an image file***
- ✓ ***Password Cracking using John the Ripper***
- ✓ ***Digital Signatures – Creating and Verifying.***
- ✓ ***System Hardening***