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

How many Suggestions did you receive?

35

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?

Harden compilers like restricting access to root user only.

Compilers turn source code into binary executable code. For a production system a compiler is usually not needed, unless package upgrades are performed by means of their source code.

What is your suggested solution?

When possible, removal of any unneeded compilers is the best option. This prevents users from compiling source code into binary programs. This is unusual for a production server, as most software comes precompiled. If you still need the compilers on your system, consider changing the file permissions or file ownership. This way only the root, or other privileged users, can use the compiler.

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***