

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Student Info Name Arun Reddy Student ID Email babaddama9@mail.sacredheart.edu |  |  |  |  |

Scanning the network on the LAN

CY-660-A/ Lab 3

Table of Contents

* Executive summary
* Lab description details
* Supporting evidence
* Conclusion & wrap up

# Executive Summary

This lab is focused on scanning and assessing the syetems on a local area network using tools like Nmap, zenmap, Metasploit and Armitage within a kali linux environment. Goal is to identify hosts on the network, detect the open ports and services, and simulate the exploitation of the known vulnerabilities. The tasks align with CEH domains on analysis and assessment of tools usage.

## Highlights

* ARP scanning for identifying active hosts
* Nmap and zenmap scnanning for ports and os fingerprints.
* Metasploit and Armitage used for exploiting PostgreSQL vulnerabilities.
* Credentials cracking and system compromise through Telnet, Psexec and SSH.

|  |  |
| --- | --- |
|  |  |

## Objectives

* Network discovery using ARP and Nmap.
* Using Zenmap for graphical visualization of open services.
* Identify and exploit vulnerabilities using Metasploit and Armitage.
* Capturing flags and demonstrating compromise of systems.

|  |  |
| --- | --- |
|  |  |

# Lab Description Details

1. **Initial ARP scan:**

* Command used: arp-scan 192.168.1.0/24

A screenshot of a computer

AI-generated content may be incorrect.

1. **Nmap TCP scanning :**

* Command used : arp-scan 192.168.1.0/24
* Detects all ips that are available on the subnet.

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**root@kali2:~# nmap –sT 192.168.1.254**

**A screenshot of a computer

AI-generated content may be incorrect.**

1. **OS fingerprinting:**

* command used

**root@kali2:~# nmap –O 192.168.1.10 | tail**

determining operating systems of target machines.

**A screenshot of a computer screen

AI-generated content may be incorrect.**

**A screenshot of a computer screen

AI-generated content may be incorrect.**

1. **Zenmap scanning:**

* Launmching Zenmap
* Performing an instense scan on the entire subnet of 192.168.1.\*
* Analyzing port banners for each host.

**A screenshot of a computer

AI-generated content may be incorrect.**

A screenshot of a computer

AI-generated content may be incorrect.

1. **Metasploit & arimitage exploitation:**

* Starting services and launched GUI:
* Service postgresql start
* ./Armitage

**A screenshot of a computer

AI-generated content may be incorrect.**

* Msfconsole

**A screenshot of a computer

AI-generated content may be incorrect.**

* using db\_nmap and selected exploits such as java\_rmi\_server,telnet,psexec and ssh.

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

1. **Compromised Hosts:**
   * **192.168.1.10 via Telnet**
   * **192.168.1.20 via Psexec**
   * **192.168.1.30 via Java RMI**
   * **192.168.1.254 via SSH using default pfSense credentials**

**A screenshot of a computer

AI-generated content may be incorrect.**

# A screenshot of a computer AI-generated content may be incorrect.

# A screenshot of a computer AI-generated content may be incorrect.

# A screenshot of a computer program AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

# Conclusion & Wrap-Up

## this lab demonstrated how various open source tools can be usedto conduct a network reconnaissance, vulnerabilityscanning and exploitation within a LAN. It emphasized the importance of timely patching up and changing the default credentials.

**Success:**

* Successfully discovered all hosts and exploited each one using proper tools.
* Gained the access to shadow file and cracked hashes.

**Failures:**

* Some machines were initially slow to respond to the scans.
* Armitage has failed quite a few times while we were detecting OS