

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Student Info Name Arun Reddy Student ID Email bbbbaddabaddama9@mail |  |  |  |  |

Performing reconnaissance from the WAN

LAB assignment #1

Table of Contents

1. [Executive Summary 2](#_Toc409378035)

information security assessment process

information security tools

1. [Lab Description Details 2](#_Toc409378038)

[Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives](#_Toc409378039)

1. [Supporting Evidence 2](#_Toc409378040)
2. [Conclusion & Wrap-Up 3](#_Toc409378041)

[Summary with observations, Success & Failures, Challenges](#_Toc409378042)

# Executive Summary

## Highlights

In this lab we performed an external reconnaissance on a simulated network from kali linux vm. We used some fo tools like namp, telnet, netcat and john the ripper to scan for open ports, grab banners, to analyze service, capturing credentials and gaining remote desktop access to a windows server.

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

## Objectives

* Performing external scanning from the WAN using nmap
* Netcat and telnet for banner grabbing
* Identifying open ports and services
* Capurting and crack password hashes using john the ripper
* Gain remote access via RDP with capturing credentials.

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

# Lab Description Details

**Step 1:**

* Booted into kali as root.
* Used nmap [www.campus.edu](http://www.campus.edu) to perform a port scan
* Used net cat and tel net to connect to services like
  + FTP
  + telnet
  + SMTP
  + HTTP
  + POP3
  + HTTP
* Grabbing service banner like 220 microsoft ftp service and ok pop3.

**Step 2:**

* ran detailed service scans with script

nmap -sV -sC www.campus.edu -p 21,23,25,80,110,443,1099,3306,3389,5432,8180

* identifying version of running services.

**Step 3:**

* connected to telnet on port 23 using

telnet [www.campus.edu](http://www.campus.edu)

* logging in using default credentials msfadmin/ msfadmin
* viewed contents of /etc/shadow

sudo tail /etc/shadow

**step 4:**

* saved the hash to a file pass.txt using leafpad
* using john pass.txt to crack the password

**step 5:**

* performed RDP scans
* used rdesktop to cxonnect
* logged in with [administrator@campus.edu/P@ssw0rd](mailto:administrator@campus.edu/P@ssw0rd)
* gained full desktop access to the windows server.

# Supporting Evidence

* Open ports on [www.campus.edu](http://www.campus.edu) includes a flag on 8180 indicating potential vulnerabilities.

A screenshot of a computer

AI-generated content may be incorrect.

* Connection to port 23 on [www.campus.edu](http://www.campus.edu) with metaspoilt login.

A screenshot of a computer

AI-generated content may be incorrect.

* The screenshots reveal the active but insecure services posing critical security risks like interception and exploistsA 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

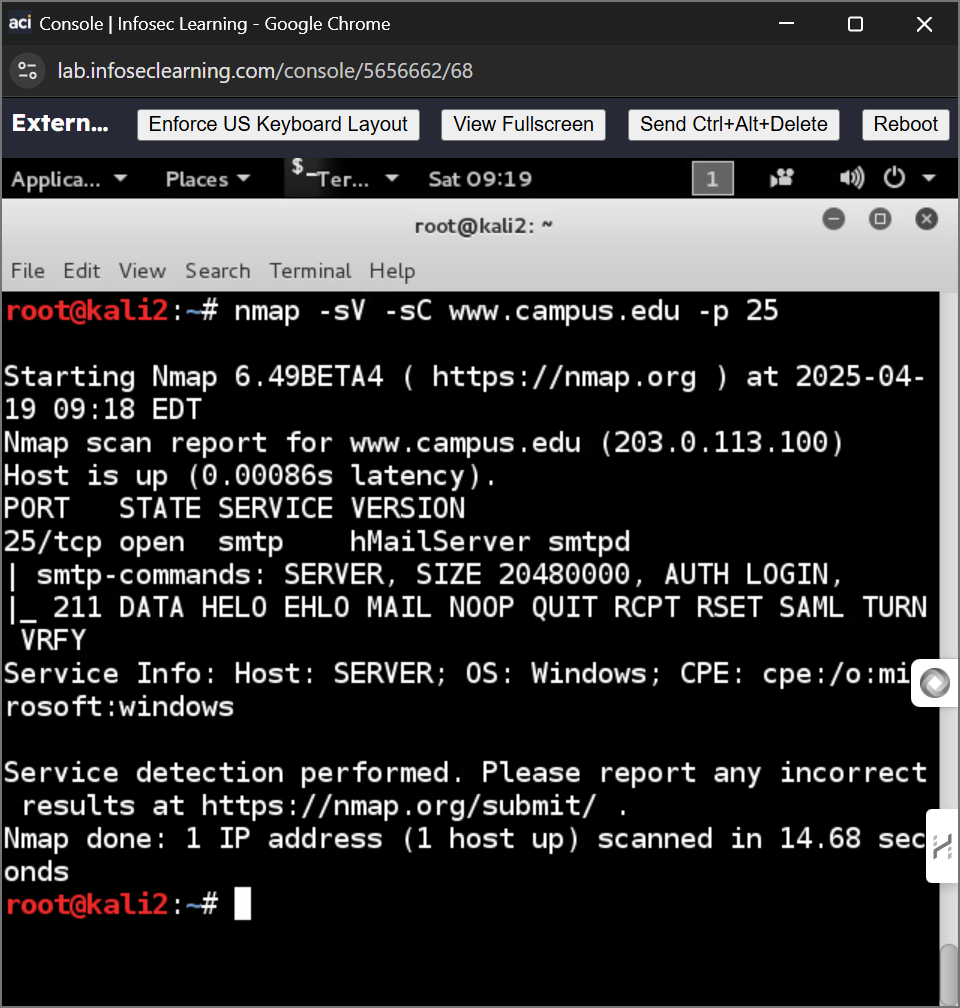
  AI-generated content may be incorrect.
* Given all nmap scans below

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

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

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.A screenshot of a computer

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.A screenshot of a computer

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

AI-generated content may be incorrect.

* /etc/shadow file view
* Cracked password from john output

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 screen

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

AI-generated content may be incorrect.

* RDP session into Windows Server

# 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.

# Conclusion & Wrap-Up

## Summary

This lab demonstrated the process of performing an external reconnaissance using real worlds tools, every stage from banner grabbing to the remote system access shown us a penetration testing work.

**Success and failure**

* Successes: we gained access to both linux and windows system
* Failure: all functions are successfully executed.

**Security level : low**

* Use of insecure protocols
* Banner grabbing enabled
* No authentication
* Access to critical files
* RDP is open to WAN

**Recommendations:**

* Disable insecure services like telnet and ftp
* Implement strong password protection
* Configure firewall rules and restrictions
* Harden banner configurations
* Encrypt sensitive files and enforce file permissions