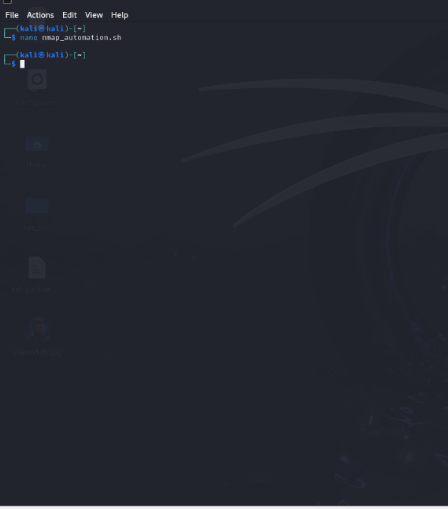
**Amrita Vishwa Vidyapeetham**

**24CYS682 – CYBER SECURITY LAB**

**Assignment 5: Automating the Nmap commands using BASH Scripting**

**Name: Rangineny sai kiran**

**RollNo. CYS24011**





**The script that we used in nmap\_automation.sh is:**

**#!/bin/bash**

**# Define target IPs and ranges**

**TARGET\_IP="10.0.2.4"**

**SUBNET="10.0.2.0/24"**

**RANGE="10.0.2.1-10.0.2.10"**

**echo "Starting automated Nmap scans..."**

**# Check if the host is up**

**echo "1. Checking if the host is up..."**

**nmap -sn $TARGET\_IP**

**# Scan specific ports (SSH, HTTP, HTTPS)**

**echo "2. Scanning specific ports (22, 80, 443)..."**

**nmap -p 22,80,443 $TARGET\_IP**

**# Perform a full TCP connection scan**

**echo "3. Performing a full TCP connection scan..."**

**nmap -sT $TARGET\_IP**

**# Conduct a stealthy SYN scan**

**echo "4. Conducting a stealthy SYN scan..."**

**nmap -sS $TARGET\_IP**

**# Detect service versions**

**echo "5. Detecting service versions..."**

**nmap -sV $TARGET\_IP**

**# Detect operating system**

**echo "6. Detecting the operating system..."**

**nmap -O $TARGET\_IP**

**# Perform an aggressive scan**

**echo "7. Performing an aggressive scan..."**

**nmap -A $TARGET\_IP**

**# Scan a range of IPs**

**echo "8. Scanning a range of IPs..."**

**nmap $RANGE**

**# Scan an entire subnet**

**echo "9. Scanning the entire subnet..."**

**nmap $SUBNET**

**# Scan common ports (1 to 1024)**

**echo "10. Scanning common ports (1 to 1024)..."**

**nmap -p 1-1024 $TARGET\_IP**

**echo "Nmap scans completed."**

**Now we have to Make the script executable:**

**chmod +x nmap\_automation.sh and run the command**

**./nmap\_automation.sh**

