Mô hình mạng:

Kali: 10.3.40.3

Windows 10: 10.3.40.4

Windows Server 2016: 10.3.40.6

Windows Server 2019: 10.3.40.5

Ubuntu: 10.3.40.7

**Module 2 : Footprinting and Reconnaissance**

Lab 1: Perform Footprinting Through Search Engines

Task 1.1: Perform Advanced Google Hacking for Password Files

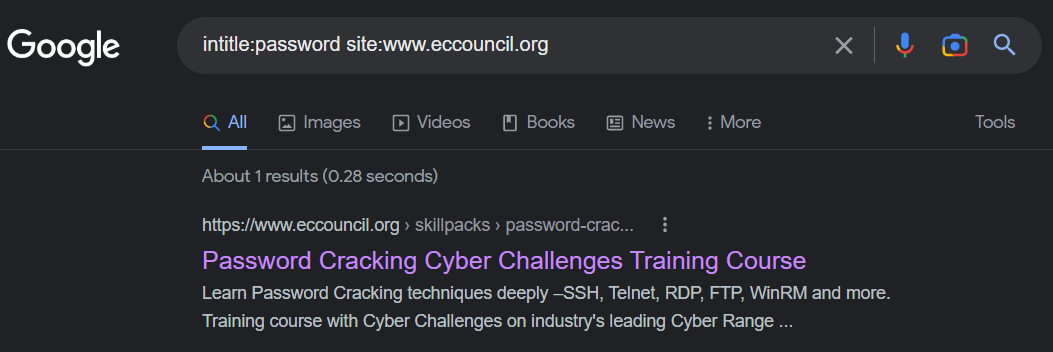


Image 2.1.1 Searching intitle:password site:www.eccouncil.org

Task 1.2: Perform Advanced Google Hacking for PDF Files

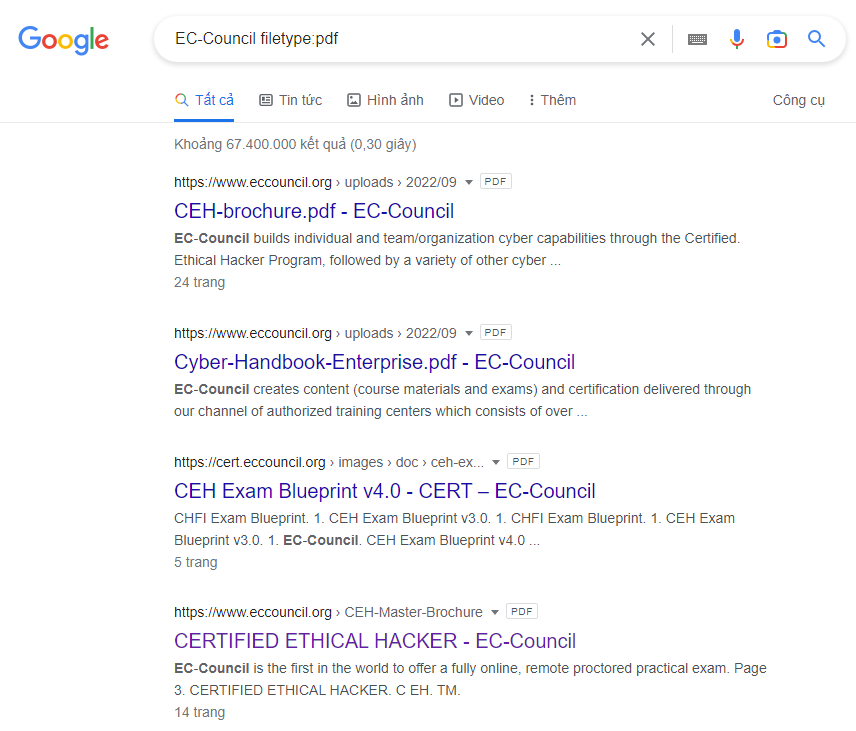


Image 2.1.2.1 Searching EC-Council filetype:pdf



Image 2.1.2.2 Result

Lab 2: Perform Footprinting Through Web Services

Task 1: Find the Company’s Domains and Sub-domains using Netcraft

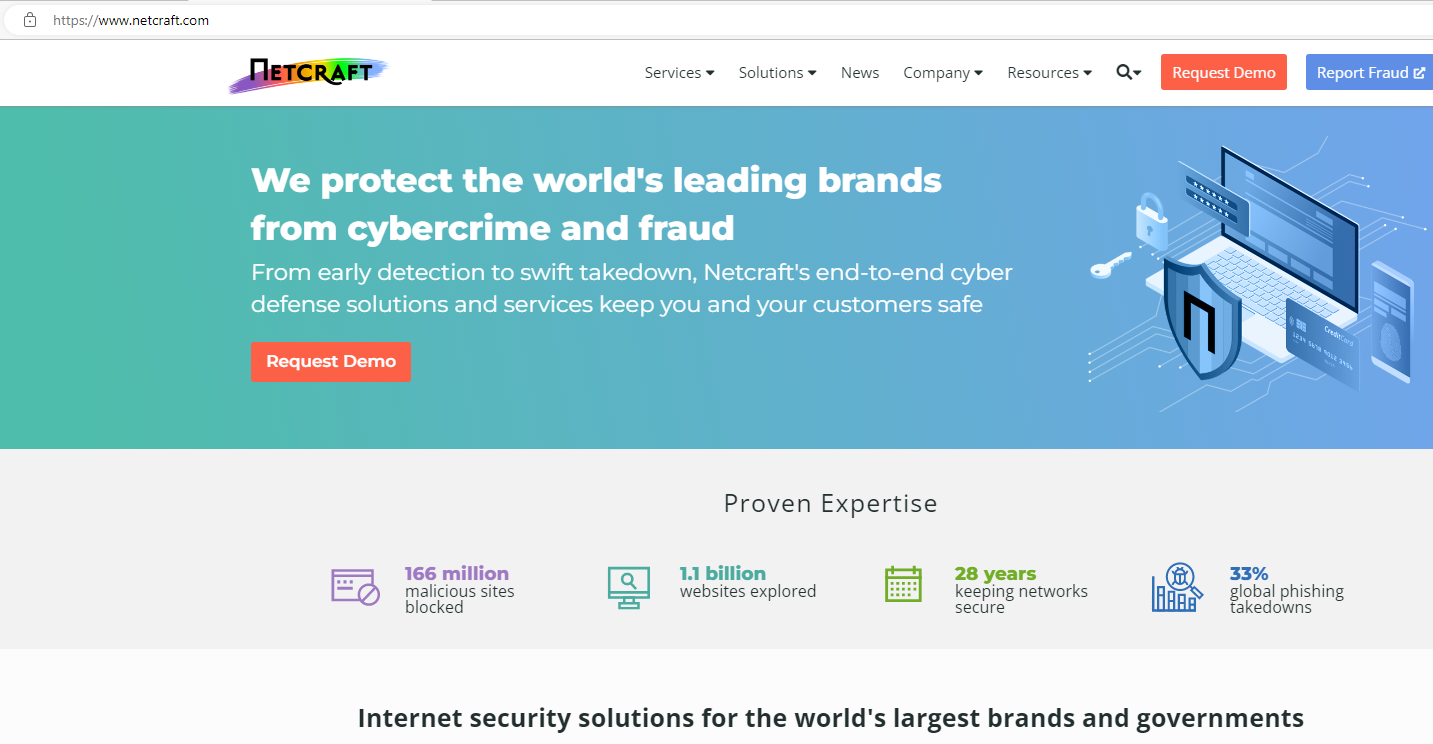


Image 2.2.1 Website <https://www.netcraft.com>

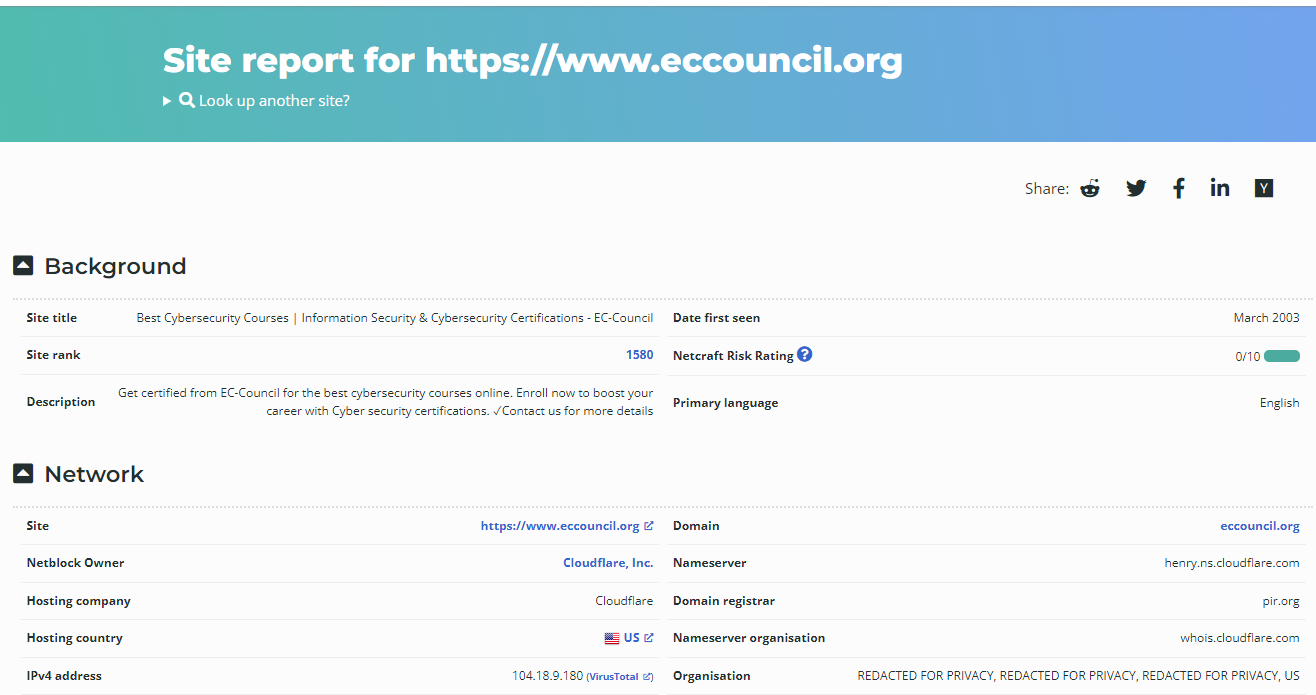


Image 2.2.2 Site report for <https://www.netcraft.com>

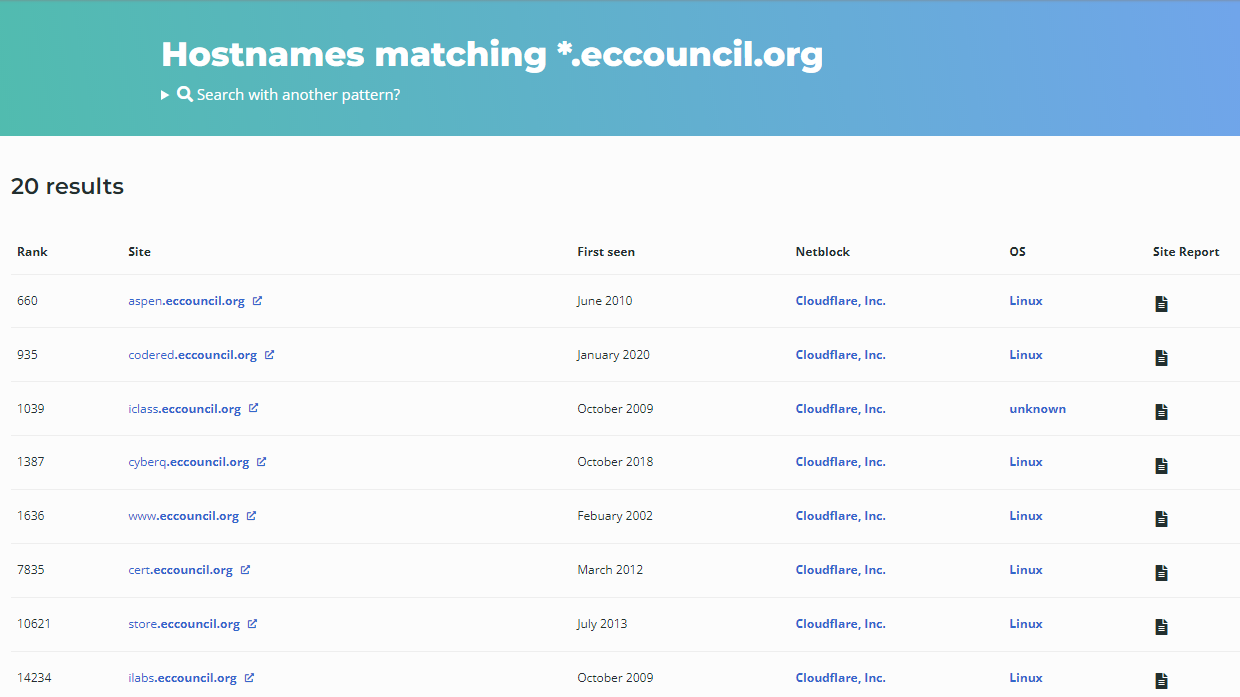


Image 2.2.3 Subdomains

Lab 4: Perform Website Footprinting

Task 4: Mirror a Target Website using HTTrack Web Site Copier

Task 4.1: Install HTTrack Web Site Copier

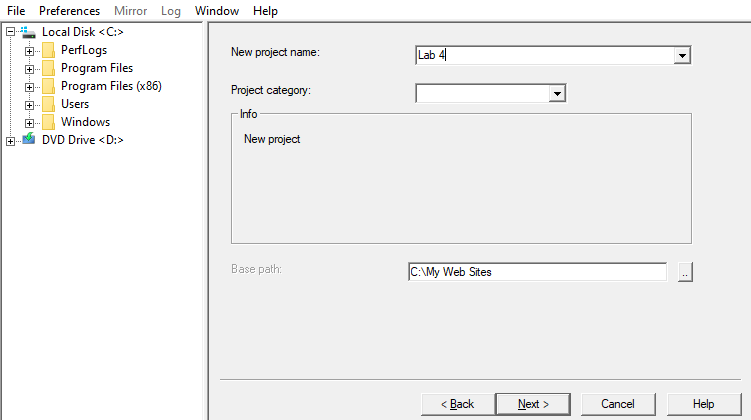


Image 2.4.4.1 App Interface

Task 4.2 Mirror the Target Website

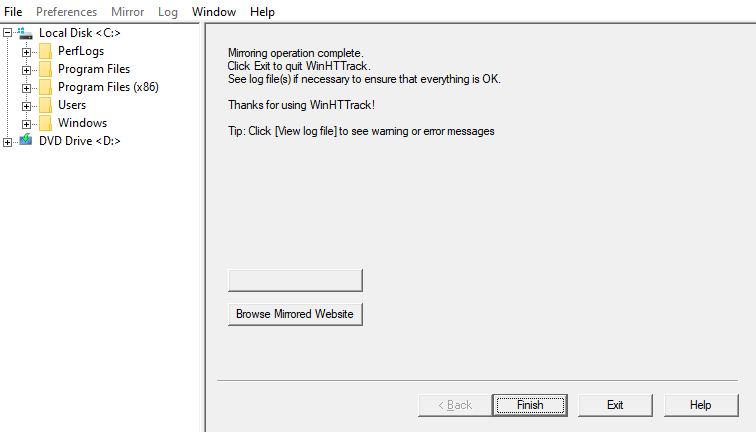


Image 2.4.4.2 Finish the site mirroring

Task 4.3 Browse the Mirrored Website



Image 2.4.4.3.1 The mirrored website for [www.certifiedhacker.com](http://www.certifiedhacker.com)

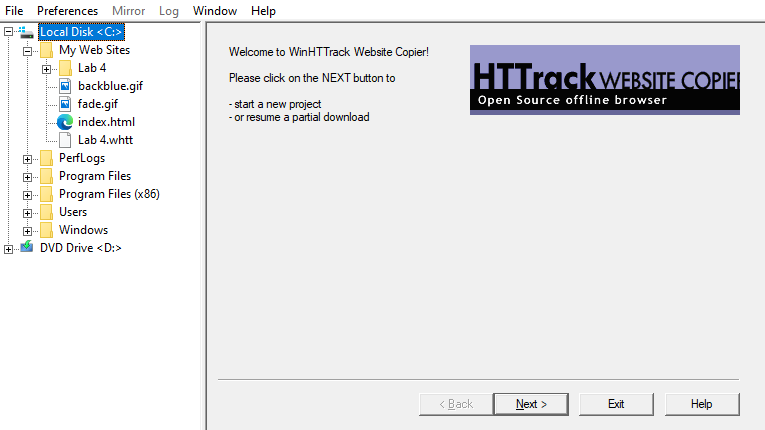


Image 2.4.4.3.2 Mirrord website location

Lab 6: Perform Whois Footprinting

Task 1: Perform Whois Lookup using DomainTools

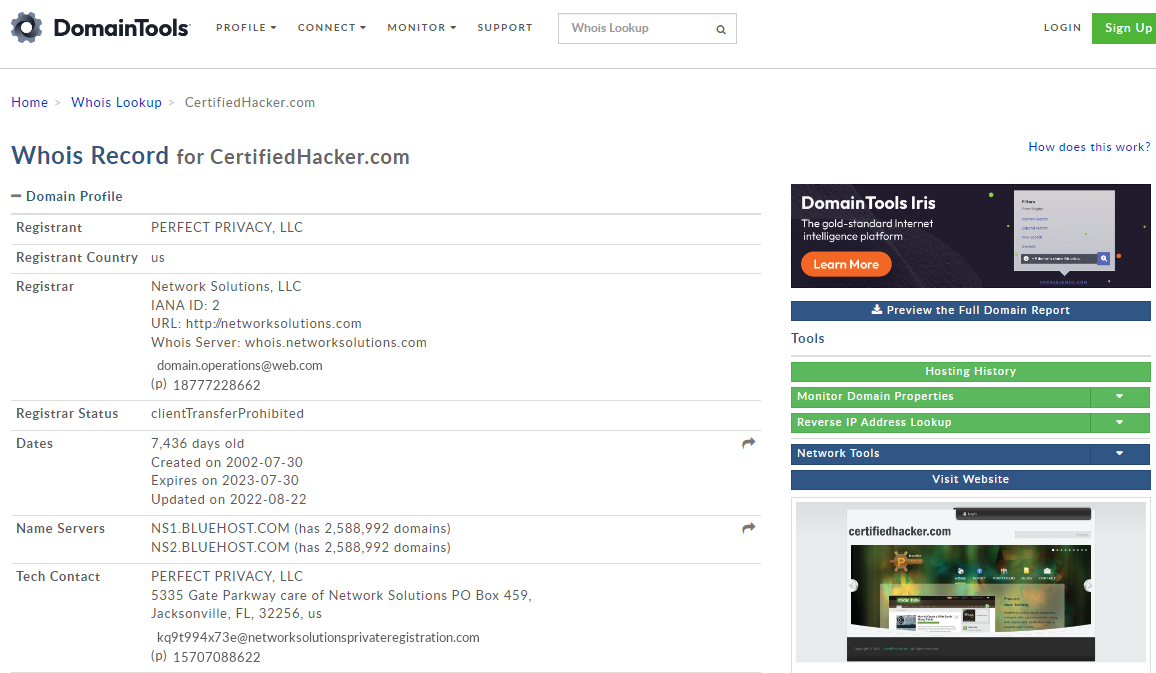


Image 2.6.1.1 Search results

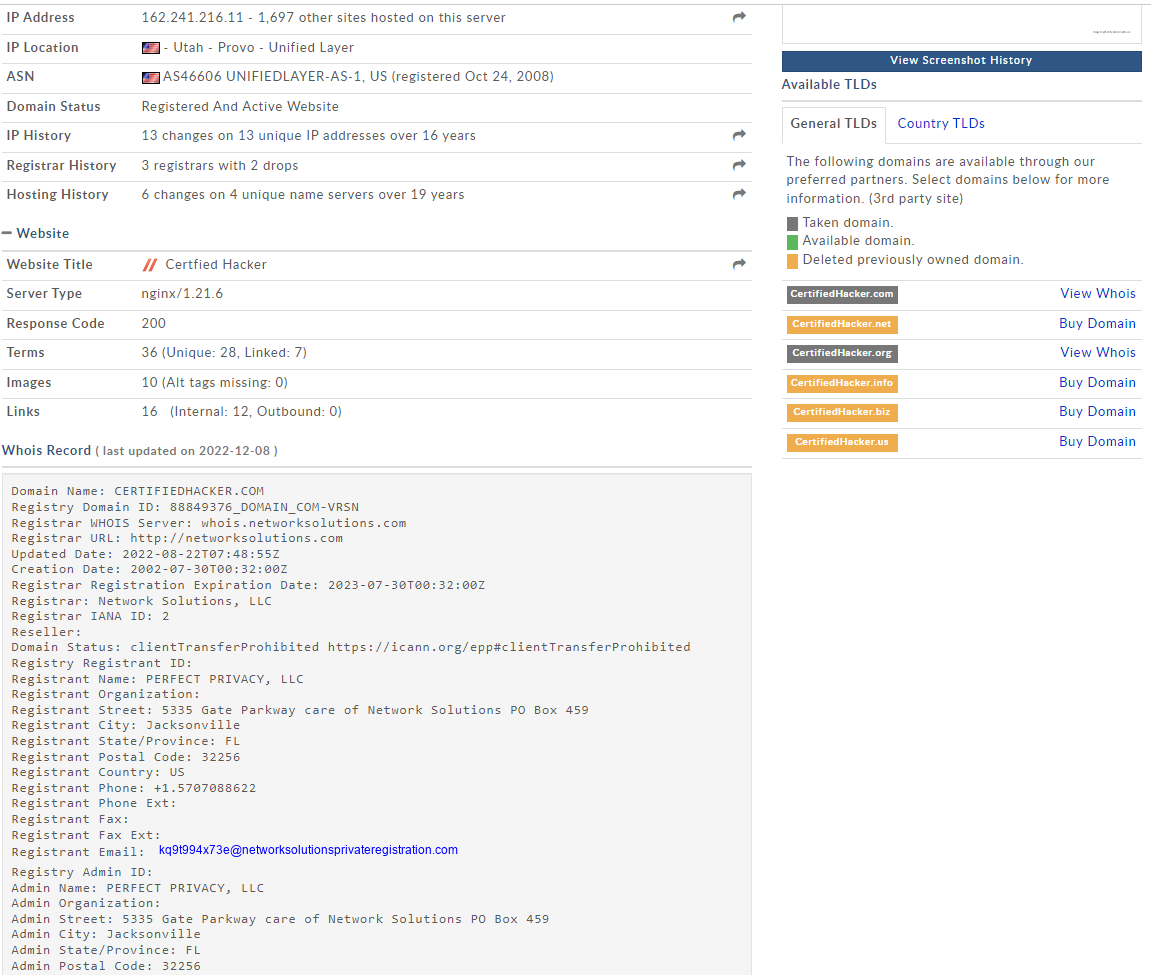


Image 2.6.1.2 Search results

Lab 7: Perform DNS Footprinting

Task 1: Gather DNS Information using nslookup Command Line Utility and Online Tool

Task 1.1: Launch nslookup Terminal

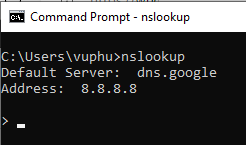


Image 2.7.1.1 Cmd with nslookup

Task 1.2 Obtain the IP Address of the Target Domain using nslookup

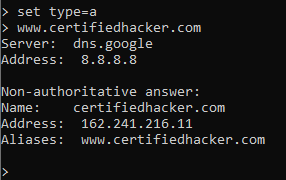


Image 2.7.1.2 Result with type=a

Task 1.3 Find Cname

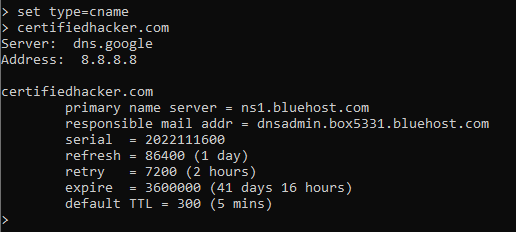


Image 2.7.1.3 Result with type=cname

Task 1.4: Obtain the IP Address of the Primary Name Server

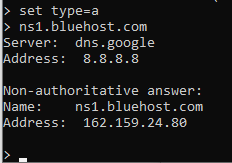


Image 2.7.1.4 Result

Task 5: Perform DNS Footprinting using NSLOOKUP Online Utility

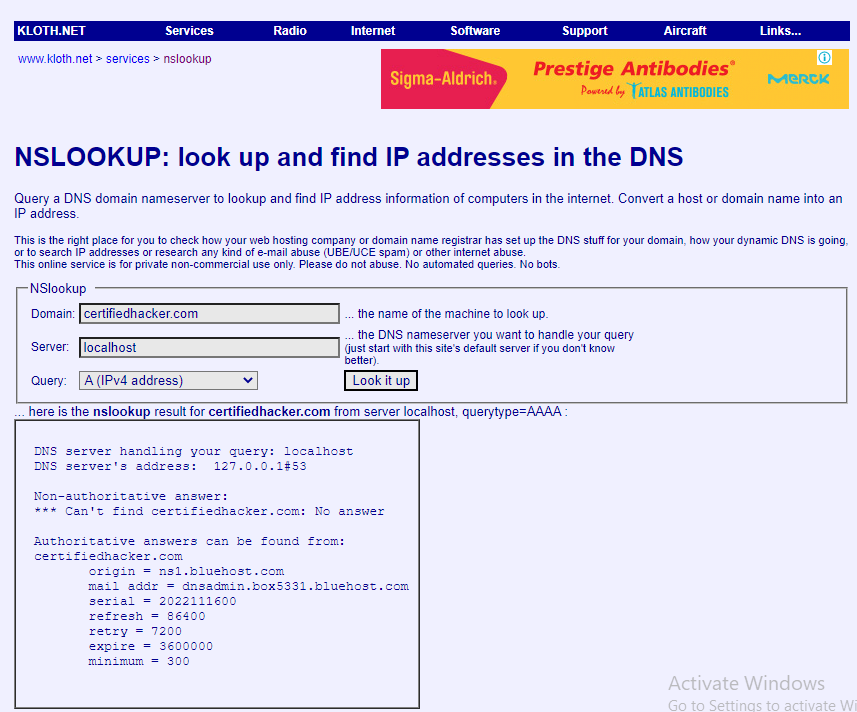


Image 2.7.1.5 IPv6 query results

Lab 8: Perform Network Footprinting

Task 1: Locate the Network Range

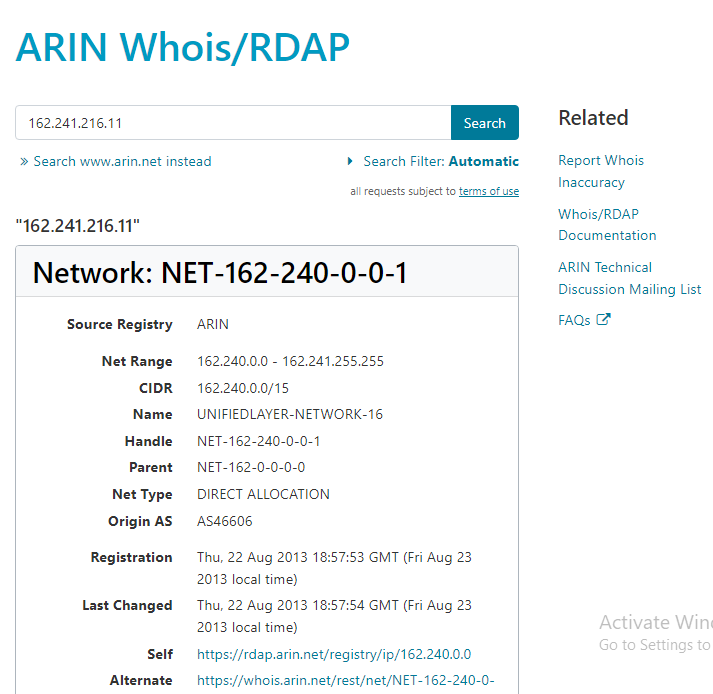


Image 2.8.1 Network range information

**Module 3 : Scanning Networks**

Lab 1: Perform Host Discovery

Task 1: Perform Host Discovery using Nmap

Task 1.1: Install Nmap

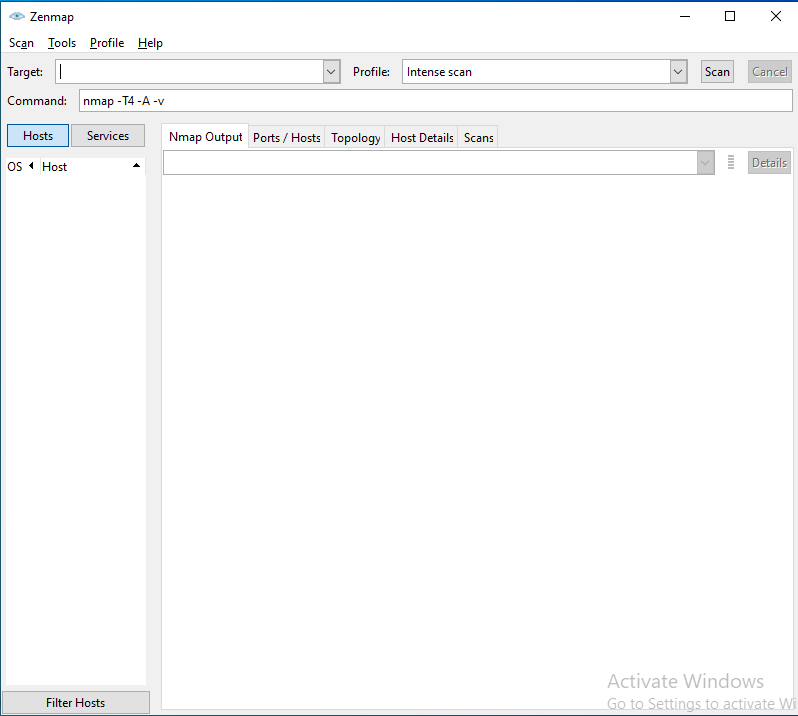


Image 3.1.1.1 Zenmap interface

Task 1.2: Perform ARP Ping Scan

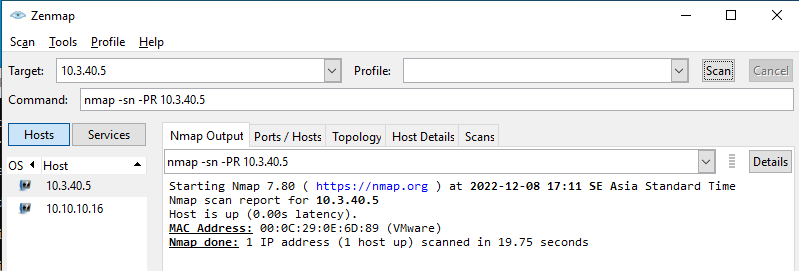


Image 3.1.1.2 Result for ARP ping scan

Task 1.3: Perform UDP Ping Scan

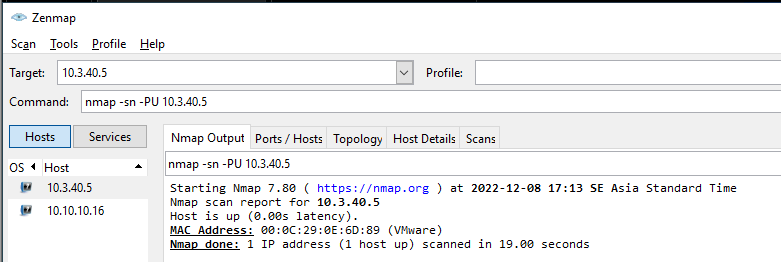


Image 3.1.1.3 Results for USP ping scan

Task 1.4 Perform ICMP ECHO Ping Scan

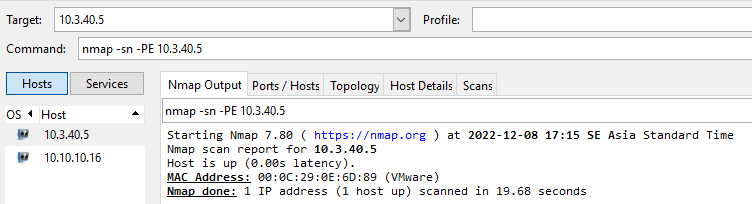


Image 3.1.1.4 Results for ICMP ECHO ping scan

Task 1.5: Perform ICMP ECHO Ping Sweep

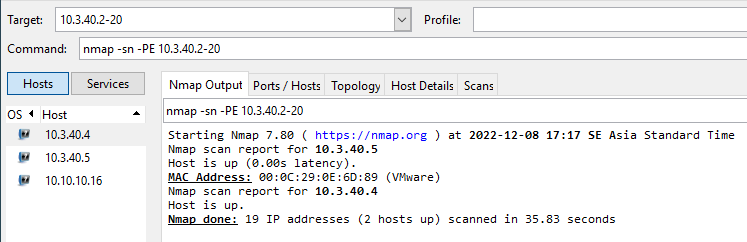


Image 3.1.1.5 Results for ICMP ECHO ping sweep scan

Lab 2: Perform Port and Service Discovery

Task 3: Explore Various Network Scanning Techniques using Nmap

Task 3.1: Perform TCP Connect/Full Open Scan

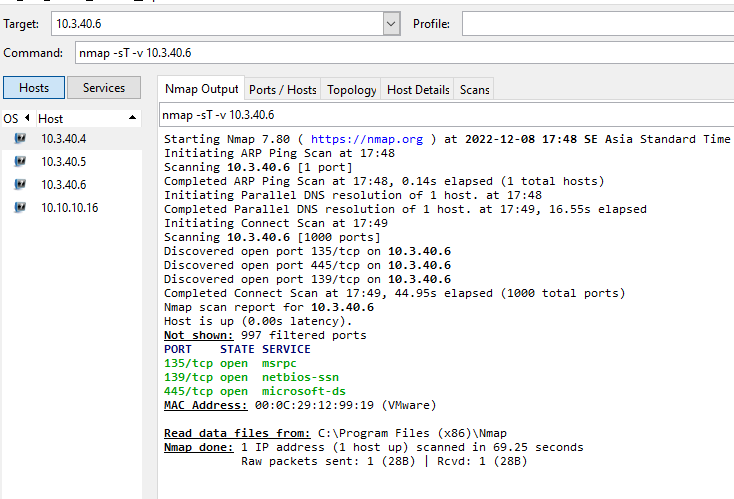


Image 3.2.3.1 Results for TCP conncect scan

Task 3.2: Perform Stealth Scan/TCP Half Open Scan

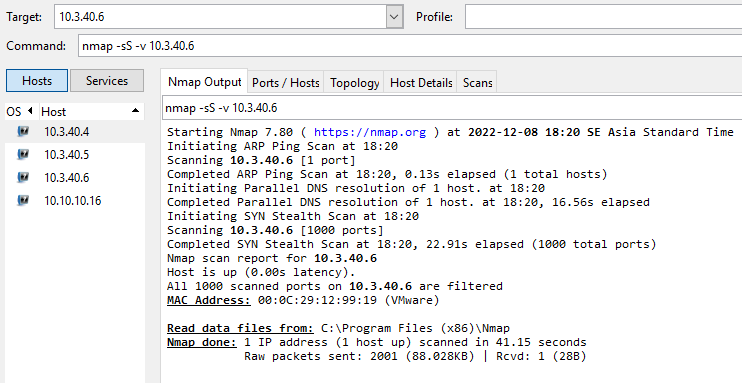


Image 3.2.3.2 Results for Stealth scan

Task 3.3: Perform Xmas Scan

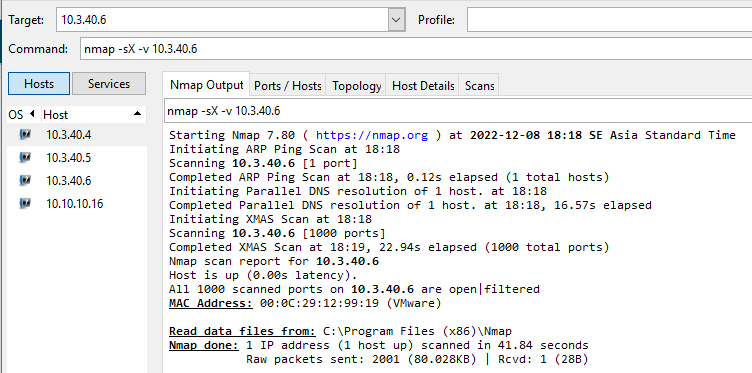


Image 3.2.3.3 Results for Xmas scan

Task 3.4: Perform TCP Maimon Scan

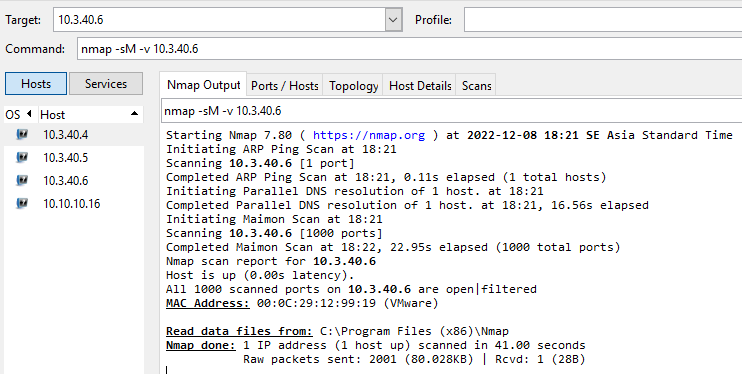


Image 3.2.3.4 Results for Maimon scan

Task 3.5: Perform ACK Flag Probe Scan

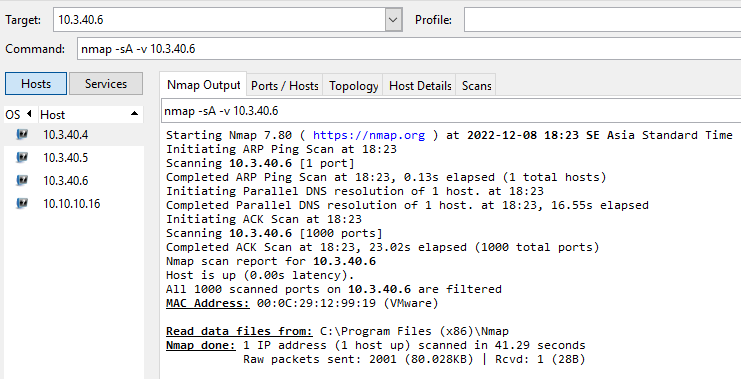


Image 3.2.3.5 Results for Stealth scan

Task 3.6: Perform UDP Scan

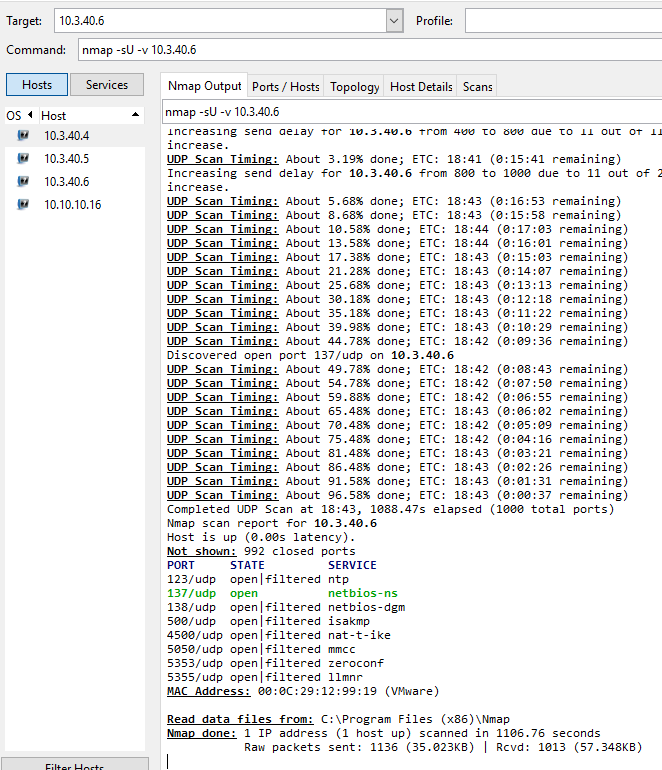


Image 3.2.3.6 Results for UDP scan

Task 3.7: Create a Scan Profile

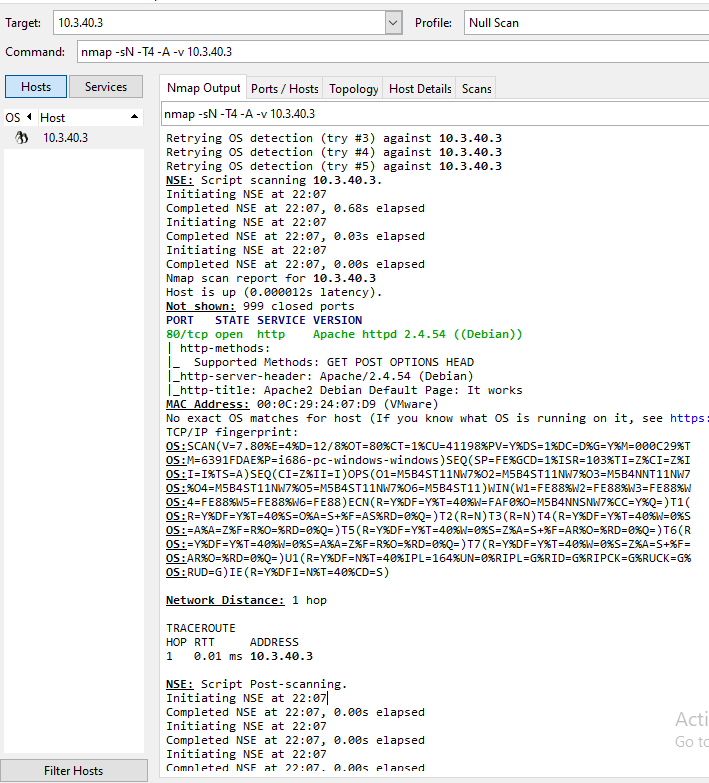


Image 3.2.3.7 Null Scan Result in Kali (10.3.40.3)

Task 3.8: Perform Service Version Discovery

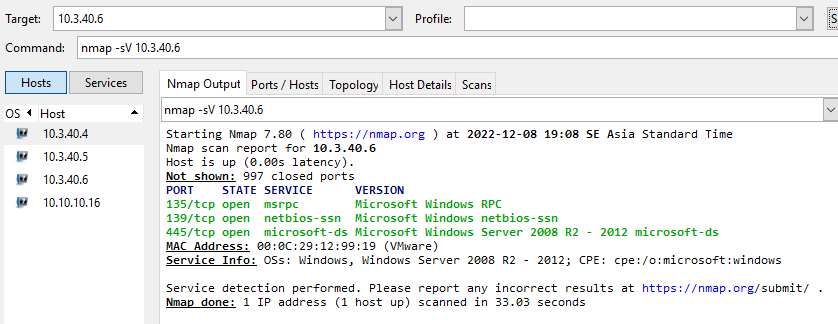


Image 3.2.3.8 Results for Service Version Discovery

Task 3.9: Scan a Whole Subnet

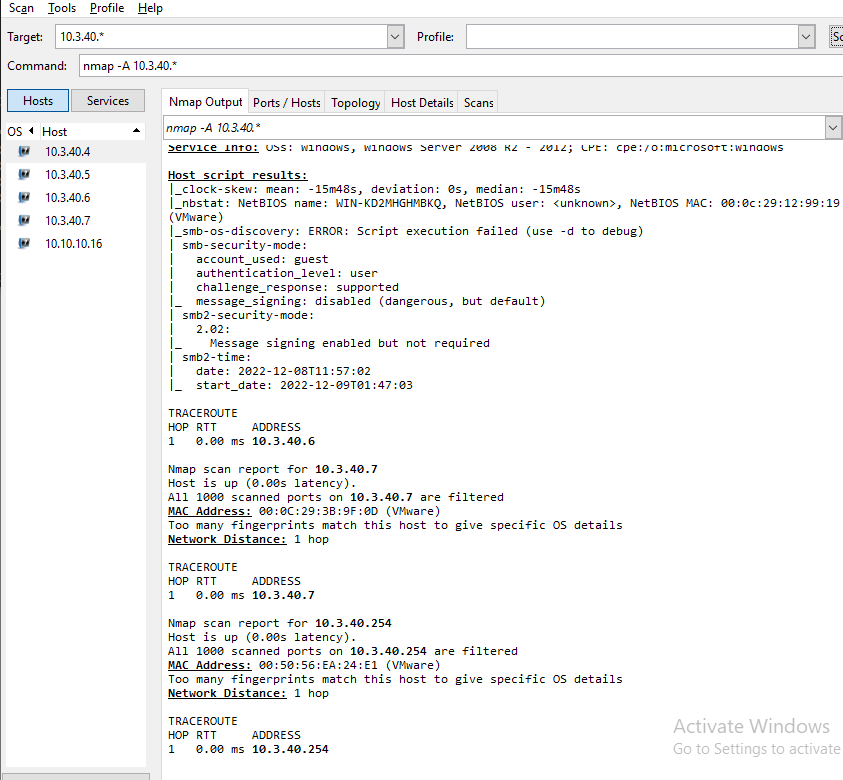


Image 3.2.3.9.1 Results for a Whole Subnet Scan

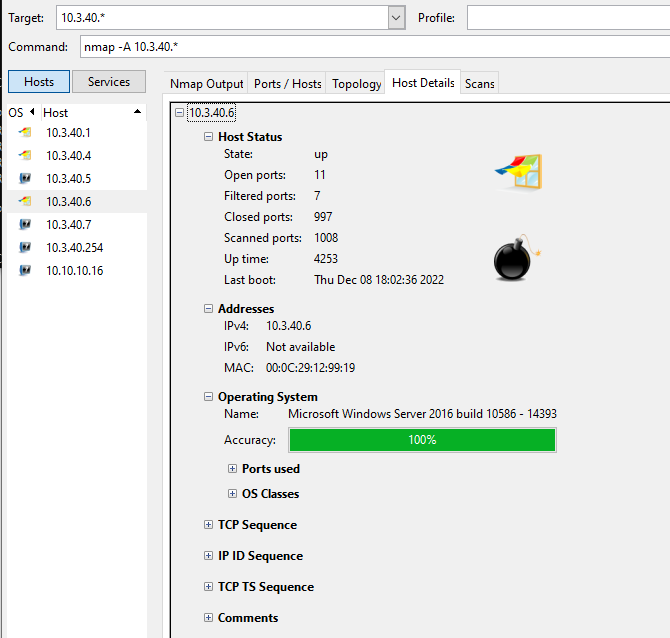


Image 3.2.3.9.2 The Open Ports under Posts/Hosts tab

Lab 3: Perform OS Discovery

Task 2: Perform OS Discovery using Nmap Script Engine (NSE)

Task 2.1: Perform OS Discovery Using A Parameter (Aggressive Scan)

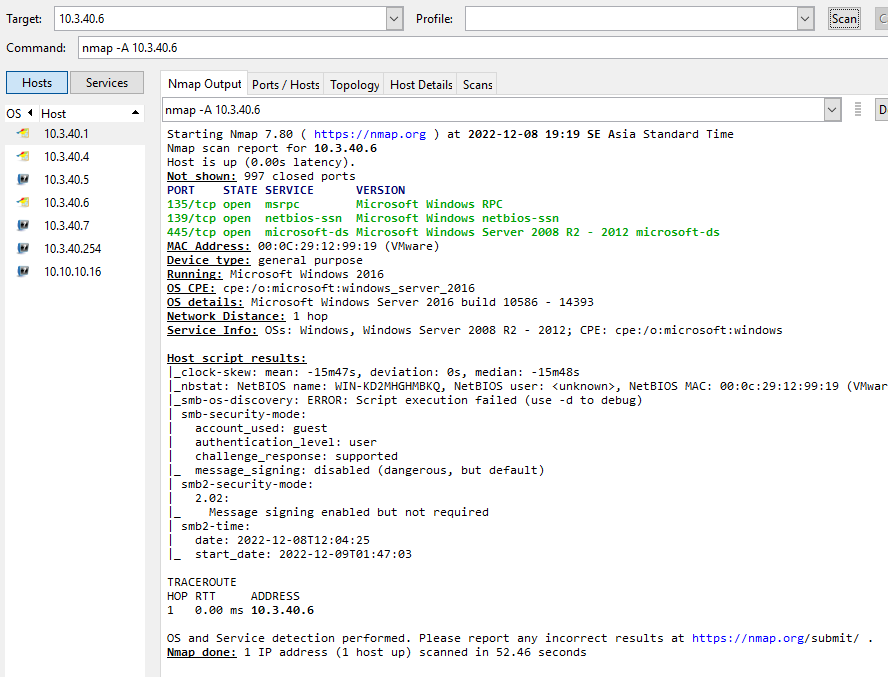


Image 3.3.2.1 Results for -A parameter

Task 2.2: Perform OS Discovery Using -O Parameter



Image 3.3.2.2 Results for -O parameter

Task 2.3: Perform OS Discovery using NSE

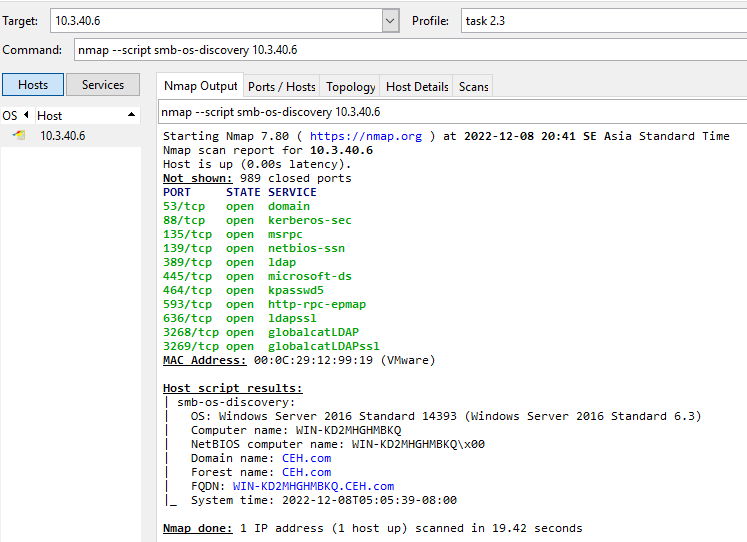


Image 3.3.2.3 Results for NSE

Lab 4: Scan beyond IDS and Firewall

Task 1: Scan beyond IDS/Firewall using various Evasion Techniques

Task 1.1 Turn in Windows Defender Firewall

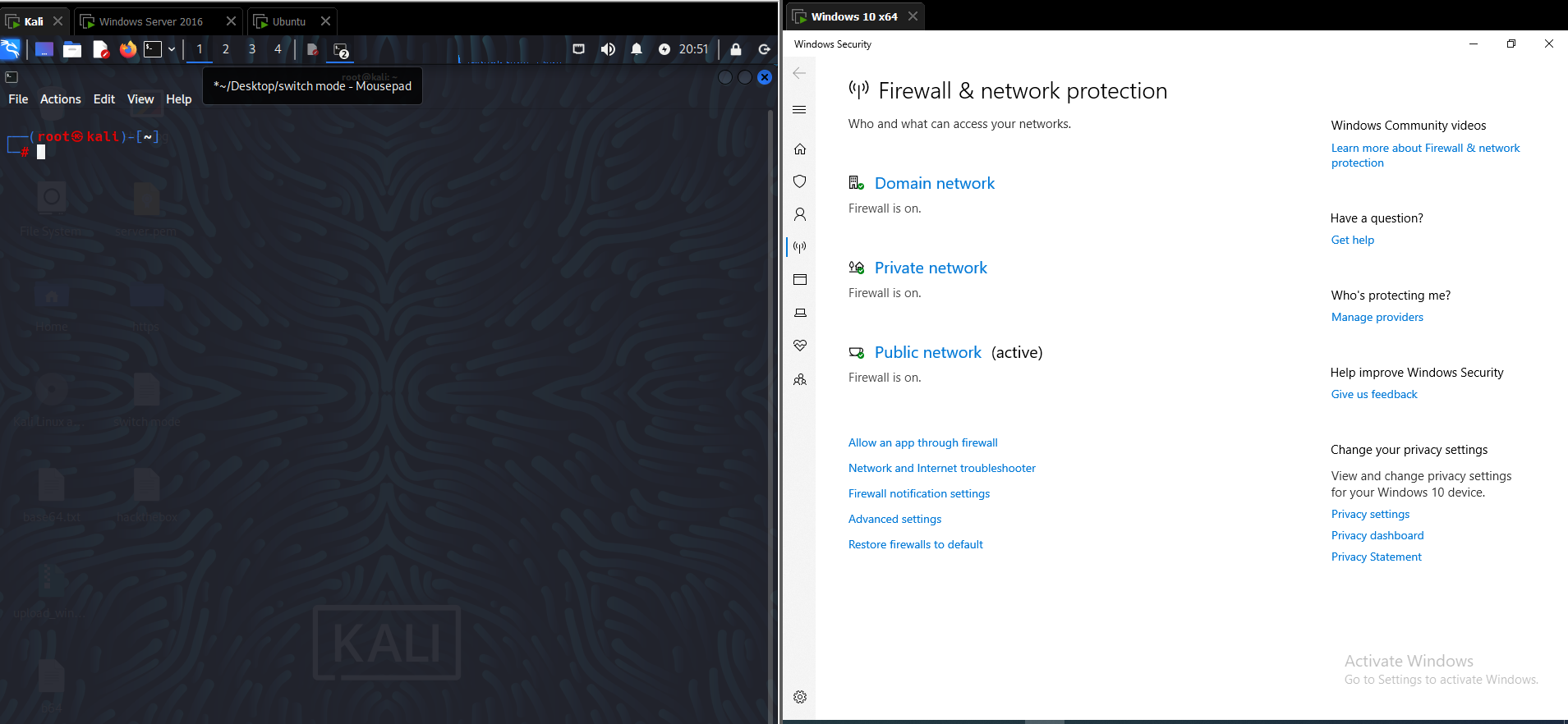


Image 3.4.1.1 Turn on firewall in Windows 10 and using root account to cd to /root

Task 1.2: Perform Packet Fragmentation

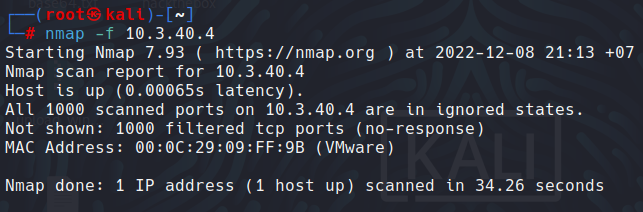


Image 3.4.1.2 All ports be filtered

Task 1.3: Perform Source Port Manipulation

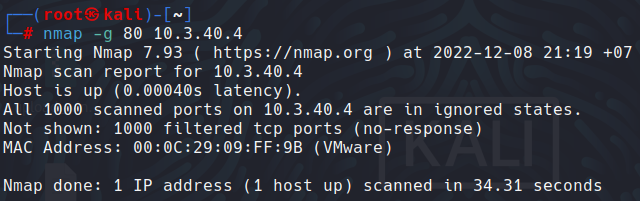


Image 3.4.1.3 All ports be filtered

Task 1.4: Perform Maximum Transmission Unit



Image 3.4.1.4 All ports be filtered

Task 1.5: Perform IP Address Decoy

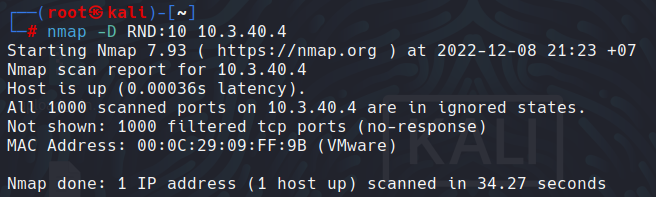


Image 3.4.1.5.1 All ports be filtered

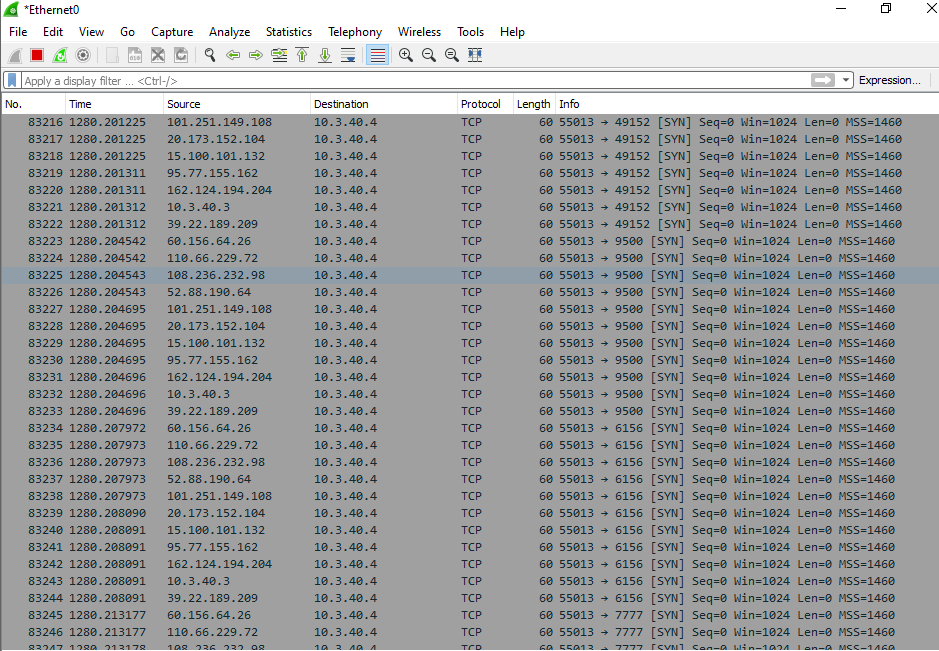


Image 3.4.1.5.2 Decoyed IP Address in Win 10 Wireshark

Task 3: Create Custom UDP and TCP Packets using Hping3 to Scan beyond IDS/Firewall

Task 3.1 Perform UDP Packet Crafting



Image 3.4.3.1 Wireshark capturing UDP packets

Task 3.2: Send TCP SYN Request

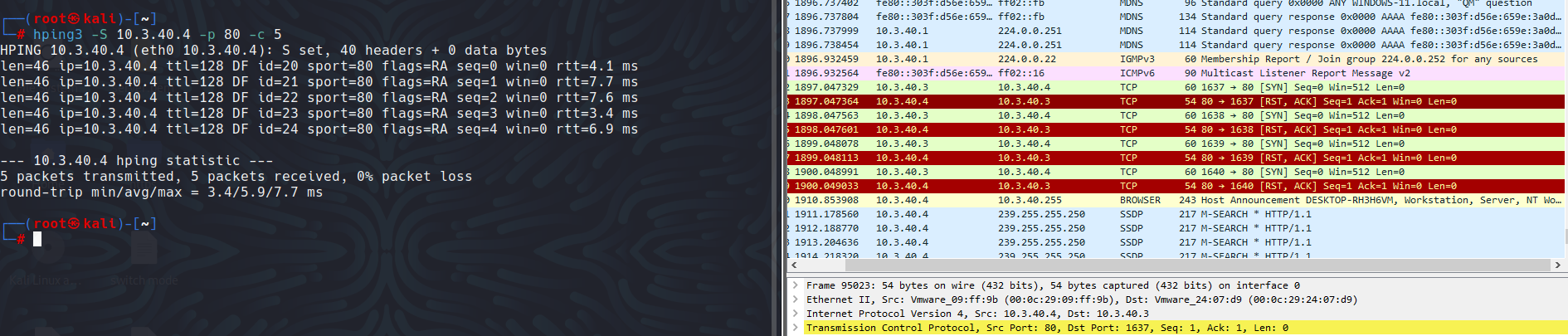


Image 3.4.3.2 Hping3 sending TCP SYN packets

Task 3.3: Perform TCP Flooding



Image 3.4.3.3.1 Hping3 sending TCP Flood

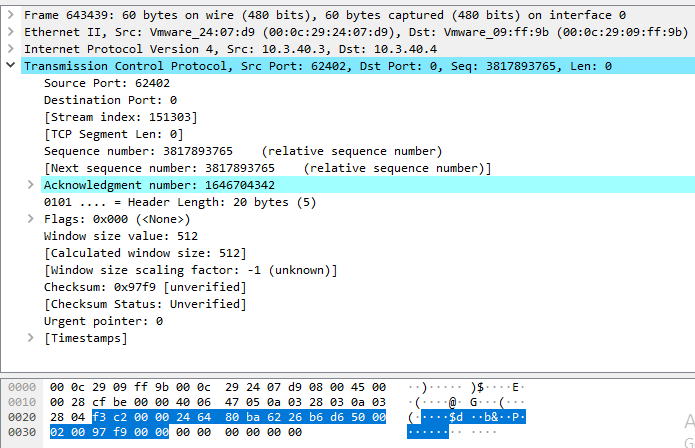


Image 3.4.3.3.2 TCP packet Stream information

**Module 4 : Enumeration**

Lab 1: Perform NetBIOS Enumeration

Task 1: Perform NetBIOS Enumeration using Windows Command-Line Utilities

Task 1.1: View the NetBIOS Name Table of a Remote Computer

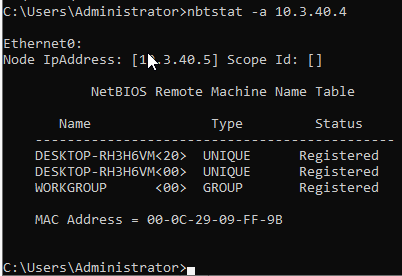


Image 4.1.1.1 Nbtstat Remote Machine Name Table

Task 1.2: View the Contents of the NetBios Name Cache

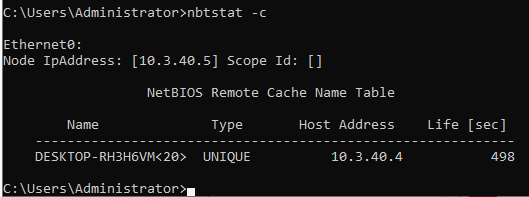


Image 4.1.1.2 Nbtstat Remote Cache Name Table

Task 1.3 View Shared Resources

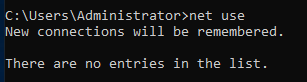


Image 4.1.1.3 No entries in the list

Lab 2: Perform SNMP Enumeration

Task 1: Perform SNMP Enumeration using snmp-check

Task 1.1: Check the SNMP Port Stattus

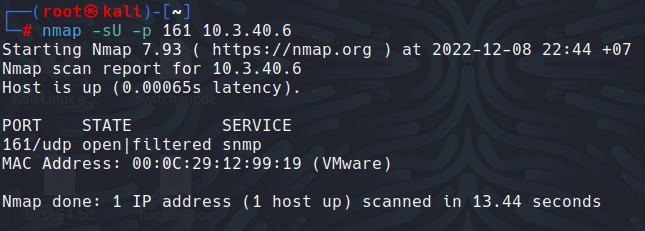


Image 4.2.1.1 Nmap UDP scan result

Task 1.2: Perform SNMP Enumeration

Lab 5: Perform DNS Enummeration

Task 1: Perform DNS Enummeration using Zone Transfer

Task 1.1 Gather Name Server Info using Dig

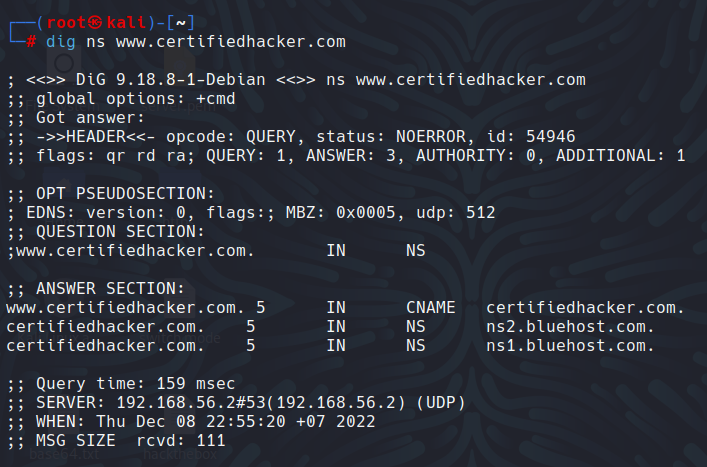


Image 4.5.1.1 Result of the dig ns command

Task 1.2: Perform Zone Transfer using Dig

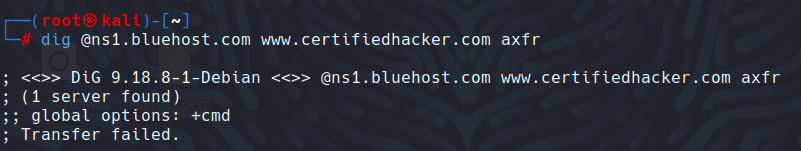


Image 4.5.1.2 Result of the dig axfr cmd result

Task 1.3: Gather Name Server Info using Nslookup

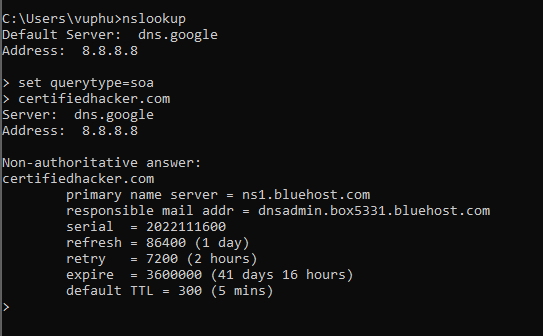


Image 4.5.1.3 Result of nslookup

Task 1.4: Perform Zone Transfer using Nslookup

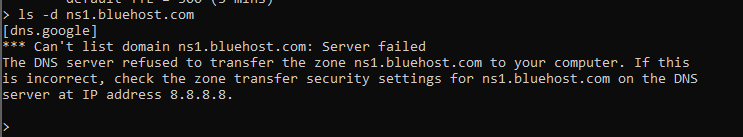


Image 4.5.1.4 Result if nslookup ls -d

**Module 5 : Vulnerability Analysis**

Lab 1: Perform Vulnerability Research with Vulnerability Scoring Systems and Databases

Task 1: Perform Vulnerability Research in Common Weakness Enummeration (CWE)

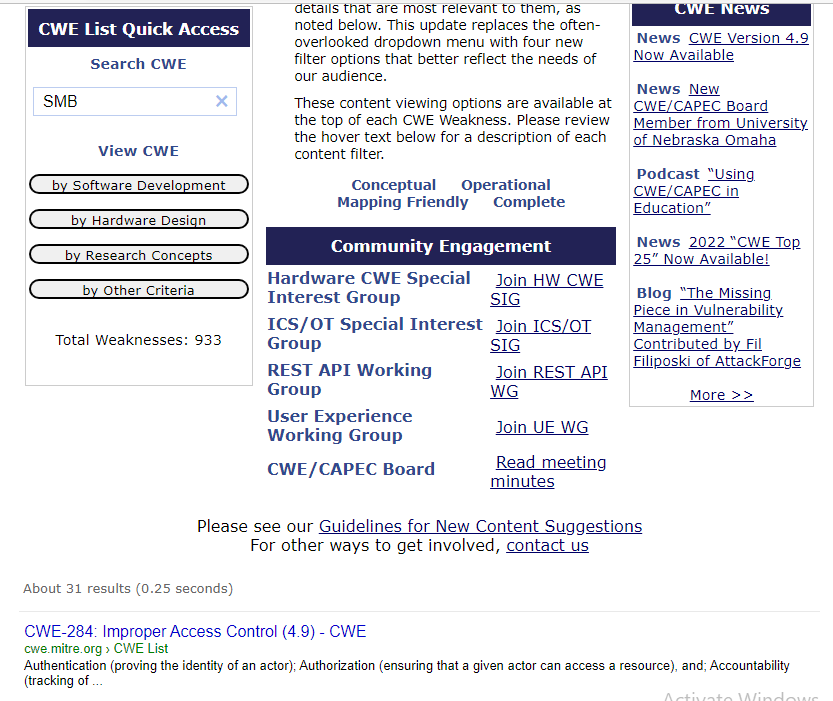


Image 5.1.1.1 Searching SMB

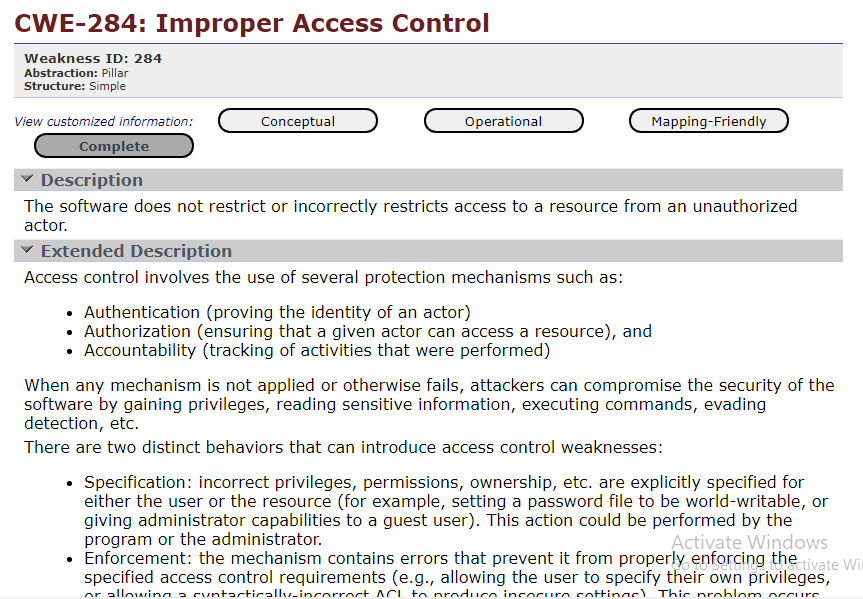


Image 5.1.1.2 CWE-284 Details

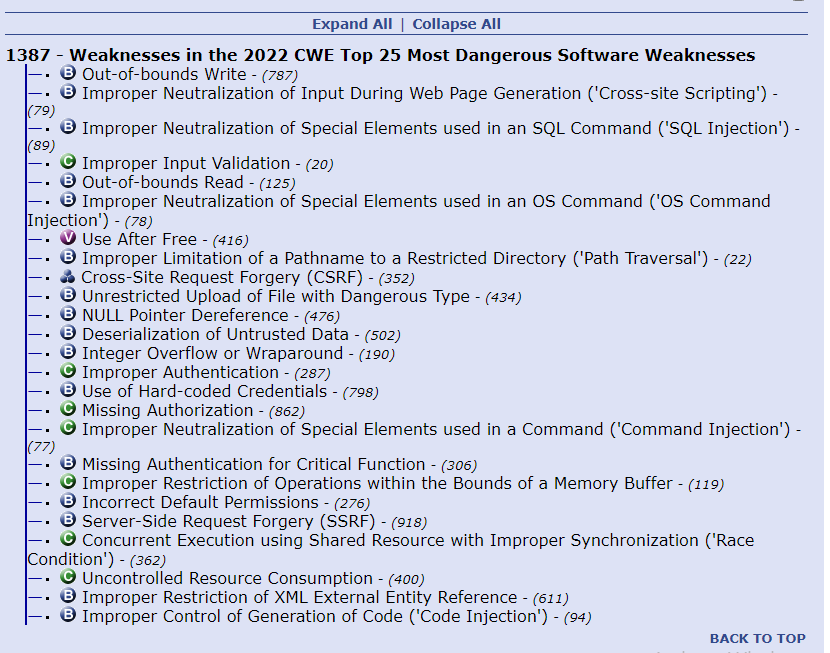


Image 5.1.1.3 CWE Top 25 Results

Lab 2: Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

Task 1: Perform Vulnerability Analys using Open VAS

Task 1.1: Open VAS Tool

Task 4: Perform Web Servers and Applications Vulnerbiltity Scanning using CGI Scanner Nikto

Task 4.1: launch Nikto Tool

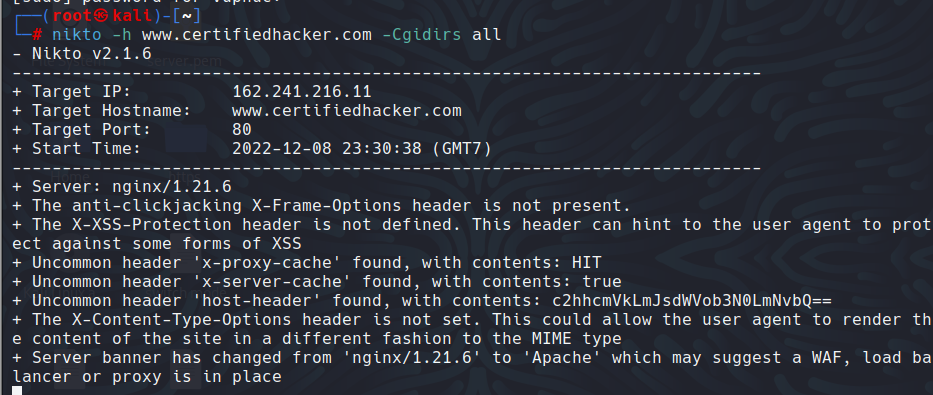


Image 5.4.1.1 Nikto option to scan CGI directories

Task 4.2: Save Scan Results