

Performing Active Reconnaissance (4e)

Ethical Hacking, Fourth Edition - Lab 02

Student:

Leandro Junior

Email:

juninhoromagnoli11@gmail.com

Time on Task:

2 hours, 40 minutes

Progress:

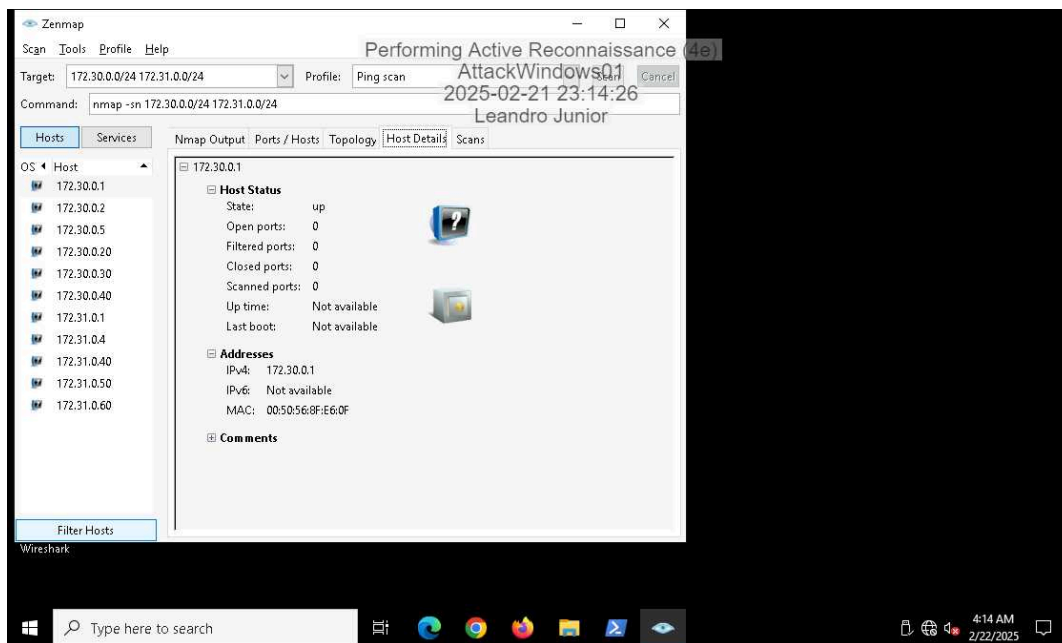
100%

Report Generated: Saturday, February 22, 2025 at 2:01 AM

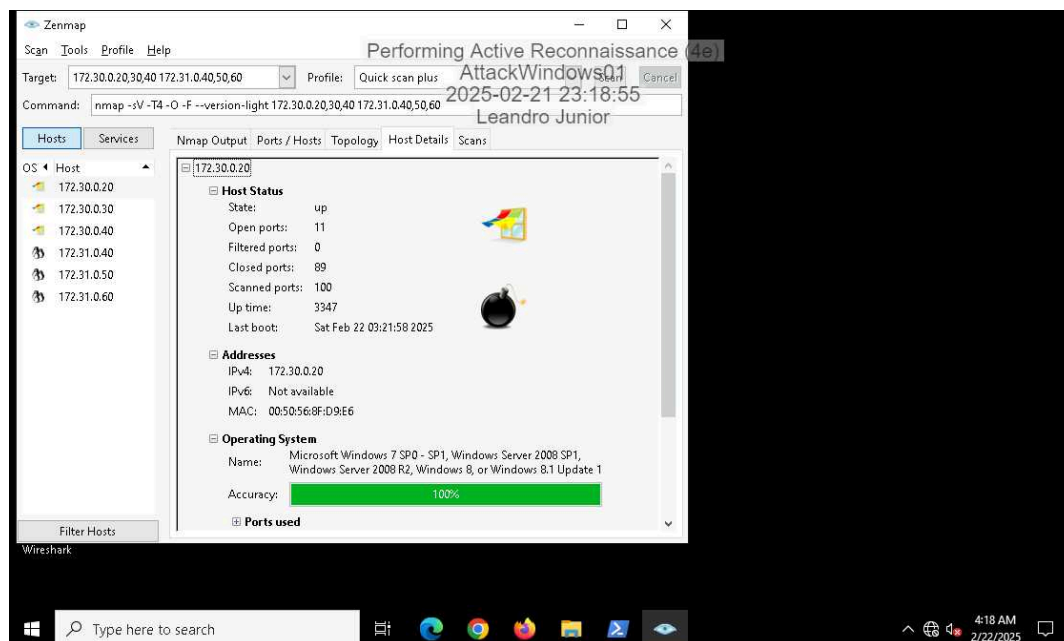
Section 1: Hands-On Demonstration

Part 1: Use Zenmap to Scan a Target Network

8. Make a screen capture showing the hosts identified by the Ping scan.



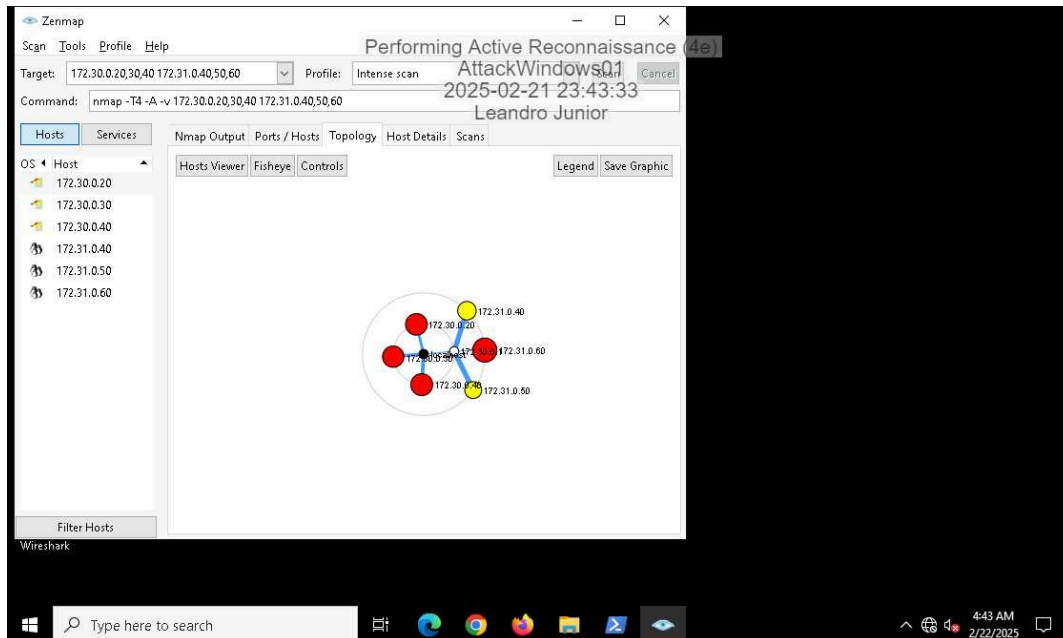
15. Make a screen capture showing the host details for 172.30.0.20 from Quick scan plus.



19. Document the IP addresses and operating systems identified.

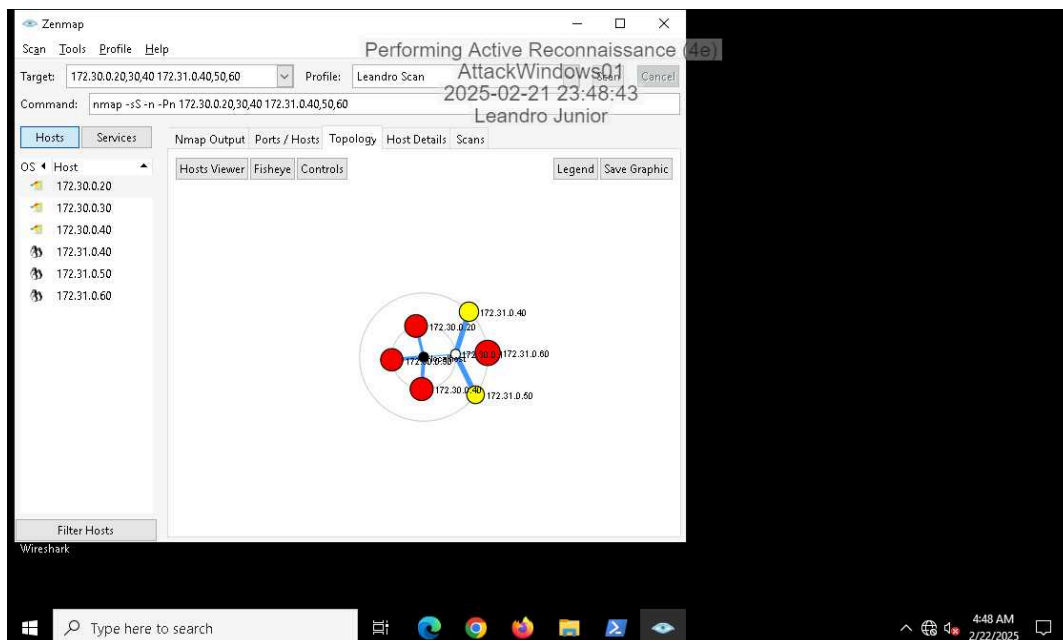
172.30.0.20 – Microsoft Windows 7 SP0 – SP1, Windows Server 2008 SP1, Window Server 2008 R2, Windows 8 or Windows 8.1 Update 1
172.30.0.30 – Microsoft Windows Server 2012 R2 Update 1
172.30.0.40 – Microsoft Windows Server 2016
172.31.0.40 – Linux 2.6.32
172.31.0.50 – Linux 3.11 – 4.1
172.31.0.60 – Linux 2.6.15 – 2.6.26 (likely embedded)

26. Make a screen capture showing the network topology.

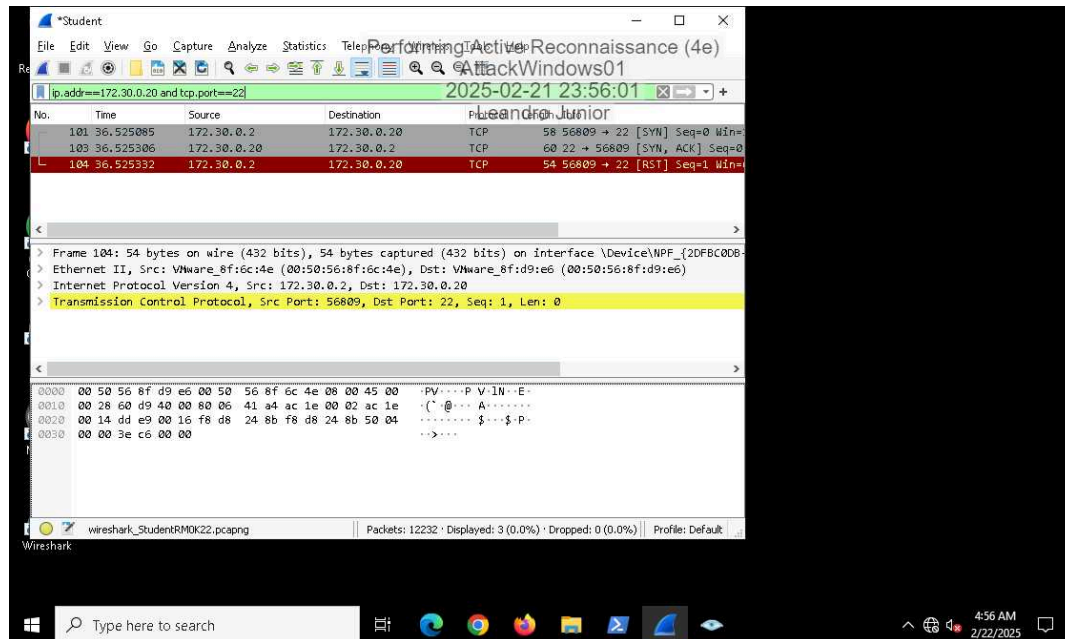


Part 2: Examine Scan Traffic with Wireshark

11. Make a screen capture showing the new scan profile selected with the corresponding nmap command line.

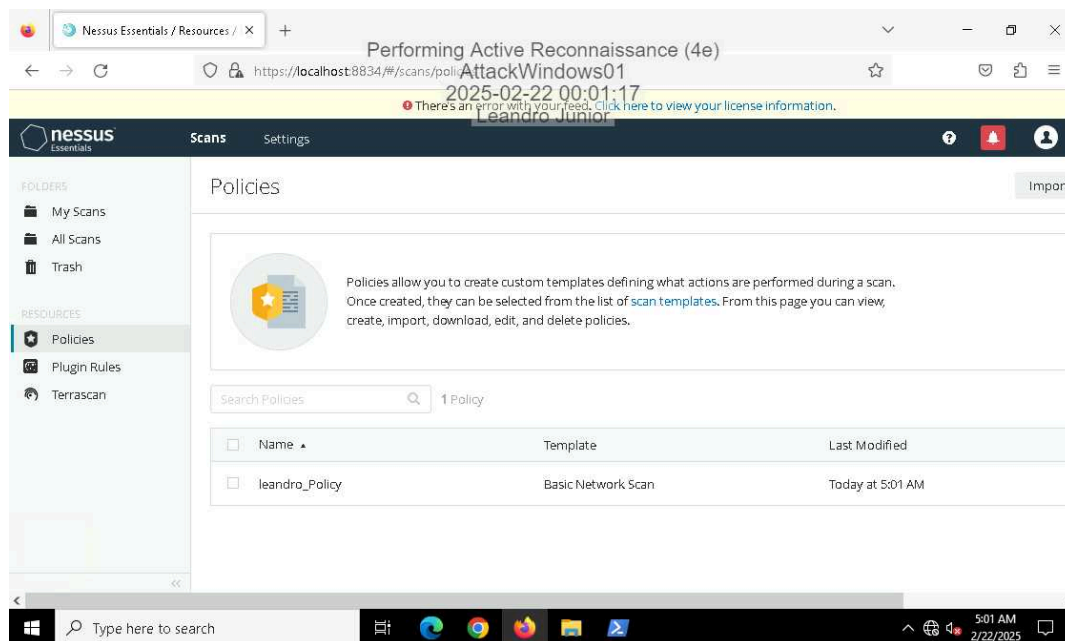


21. Make a screen capture showing the 3-packet sequence for the SYN scan of 172.30.0.20 port 22.



Part 3: Run a Vulnerability Scan with Nessus

10. Make a screen capture showing the new Nessus policy.



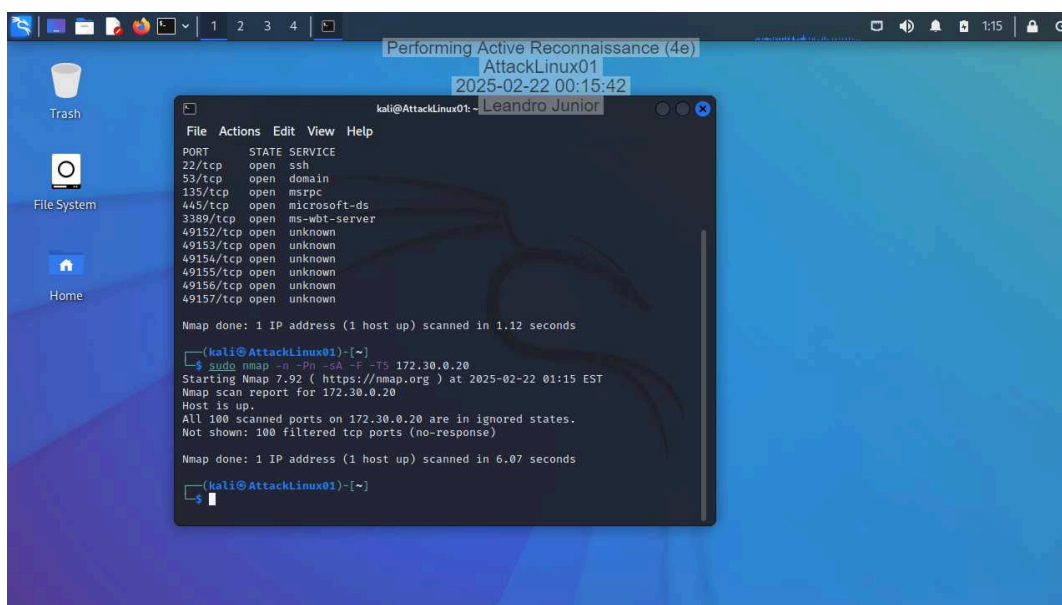
22. Make a screen capture showing the **vulnerability title** and the **Plugin information** for MS17-010.

The screenshot shows the Nessus Essentials web interface in a browser window. The browser's address bar displays the URL `https://localhost:8834/#/scans/reports/AttackWindows013514/97833`. The page title is "Performing Active Reconnaissance (4e)". A yellow banner at the top of the interface contains a message: "There's an error with your feed. Click here to view your license information." The main content area is titled "leandro_Policy / Plugin #97833" and includes buttons for "Configure", "Audit Trail", "Launch", and "Rep". Below this, a navigation bar shows tabs for "Hosts", "Vulnerabilities", "Remediations", "Notes", "VPR Top Threats", and "History". The "Vulnerabilities" tab is active, displaying a list of vulnerabilities. The first entry is "MS17-010: Security Update for Microsoft Windows SMB Server (4...)" with a severity of "HIGH". The "Description" section states: "The remote Windows host is affected by the following vulnerabilities: - Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148) - An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147) ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group". The "Plugin Details" section on the right lists: Severity: High, ID: 97833, Version: 1.30, Type: remote, Family: Windows, Published: March 20, 2017, Modified: May 25, 2022. The "Risk Information" section shows: Risk Factor: High, CVSS v3.0 Base Score 8.1. The left sidebar contains "FOLDERS" (My Scans, All Scans, Trash) and "RESOURCES" (Policies, Plugin Rules, Terrascan). The Windows taskbar at the bottom shows the time as 5:11 AM on 2/22/2025.

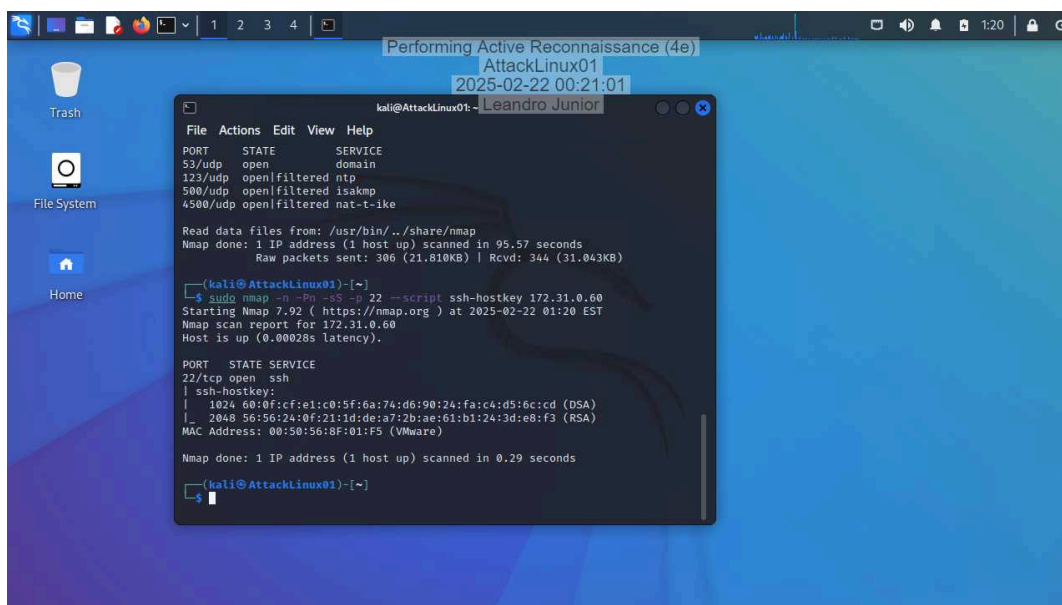
Section 2: Applied Learning

Part 1: Use Nmap to Scan a Target Network

7. Make a screen capture showing the results of the ACK scan on 172.30.0.20.

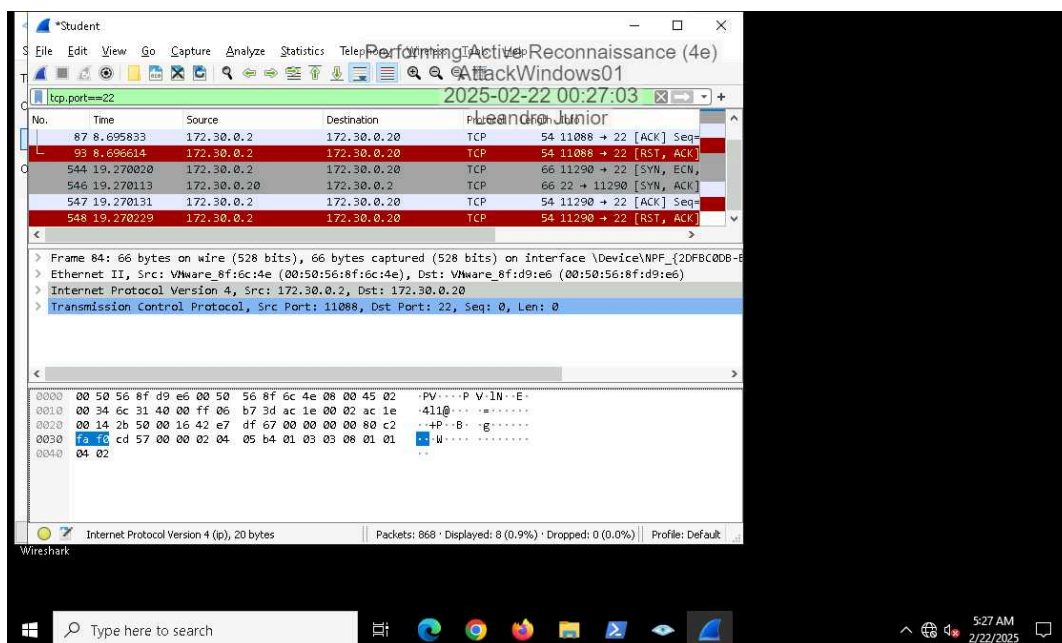


11. Make a screen capture showing the results of the scan with the ssh-hostkey script.



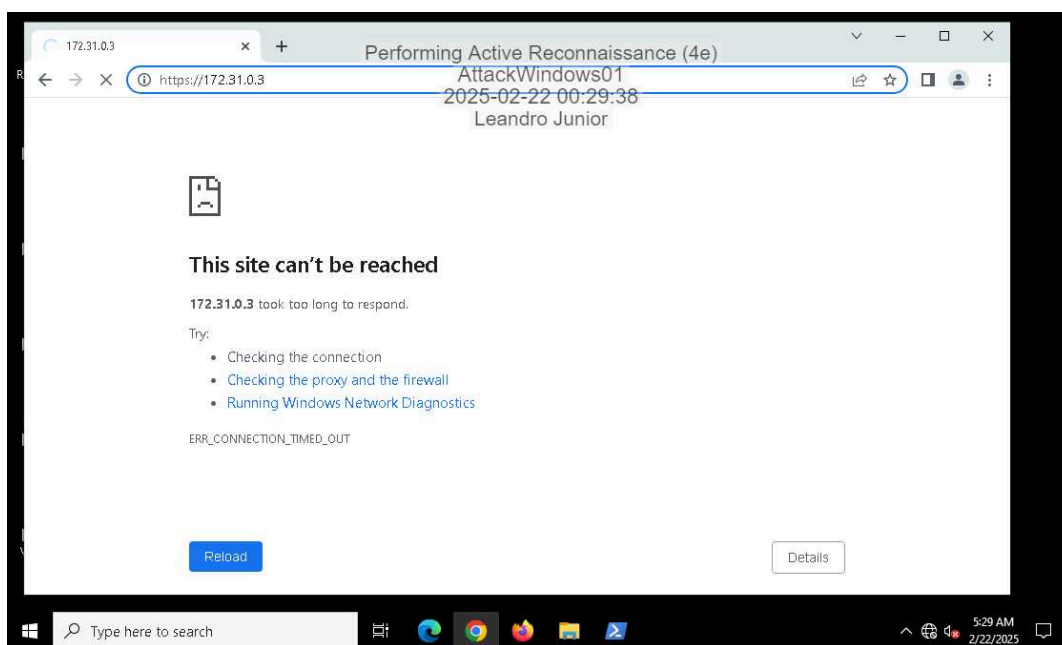
Part 2: Capture Traffic for a TCP Connect Scan

11. Make a screen capture showing the 4-packet sequence for the TCP Connect scan on 172.30.20 port 22.



Part 3: Run a Vulnerability Scan with OpenVAS

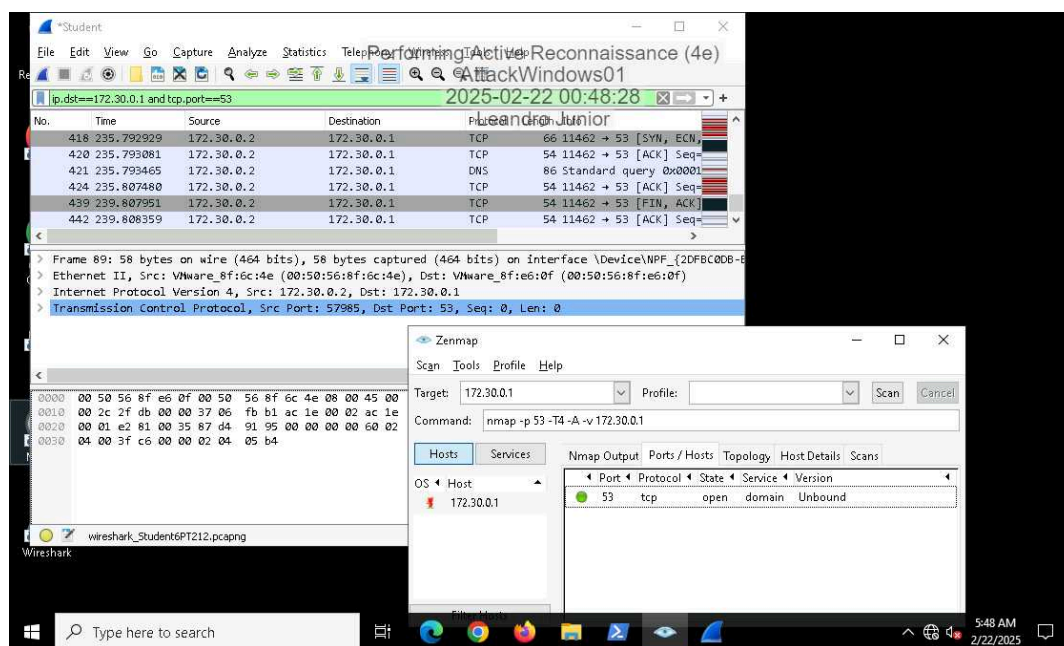
17. Make a screen capture showing the details of the MySQL / MariaDB vulnerability, including the Detection Result and the Solution.



Section 3: Challenge and Analysis

Part 1: Capture Traffic for a UDP Scan

Make a screen capture showing the **sequence of packets** from the **UDP scan** of port 53 on 172.30.0.1.



Part 2: Create a New Zenmap Profile

Performing Active Reconnaissance (4e)

Ethical Hacking, Fourth Edition - Lab 02

Make a screen capture showing the new profile selected in Zenmap and the results of using the profile to scan 172.31.0.60.

