Performing Active Reconnaissance (4e)

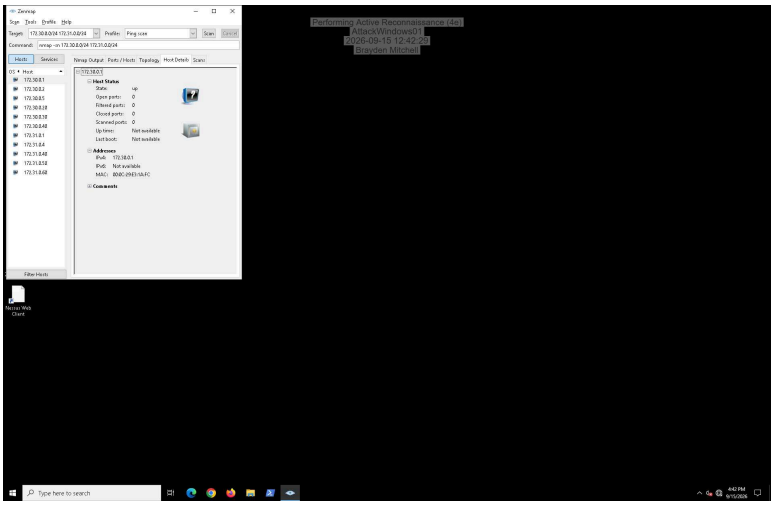
Ethical Hacking, Fourth Edition - Lab 02

Student: Brayden Mitchell
Email: brayden.m.mitchell@gmail.com
Time on Task: 3 hours, 1 minute
Progress: 100%
Report Generated: Thursday, September 17, 2026 at 7:53 PM

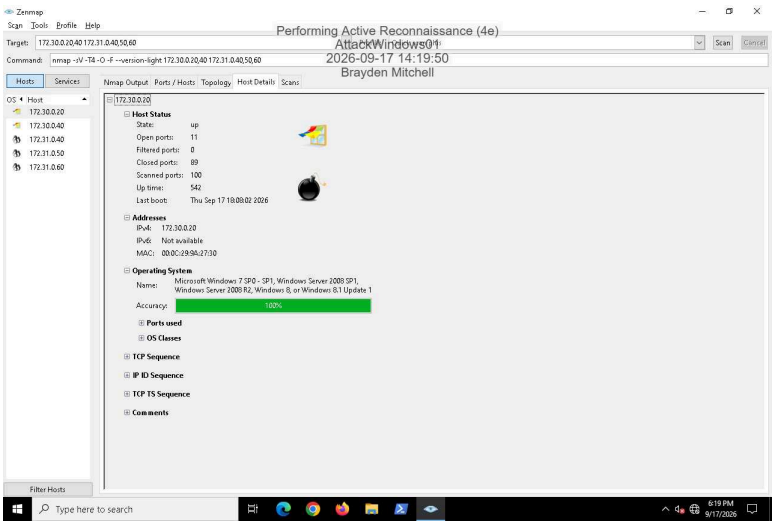
Section 1: Hands-On Demonstration

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**.

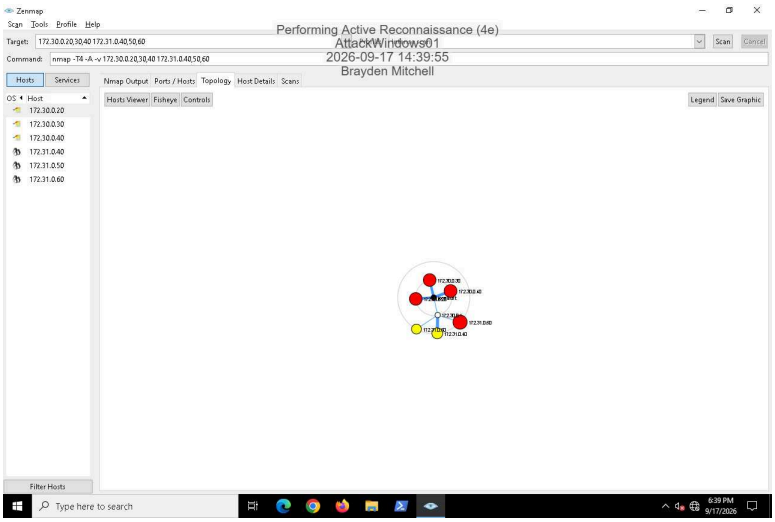


19. **Document** the **IP addresses and operating systems identified.**

172.31.0.40 Lunux 2.6.32
172.30.0.20 Microsoft Windows Version Unknown
172.30.0.30 Microsoft Windows Server 2012
172.30.0.40 Microsoft Windows Server 2016

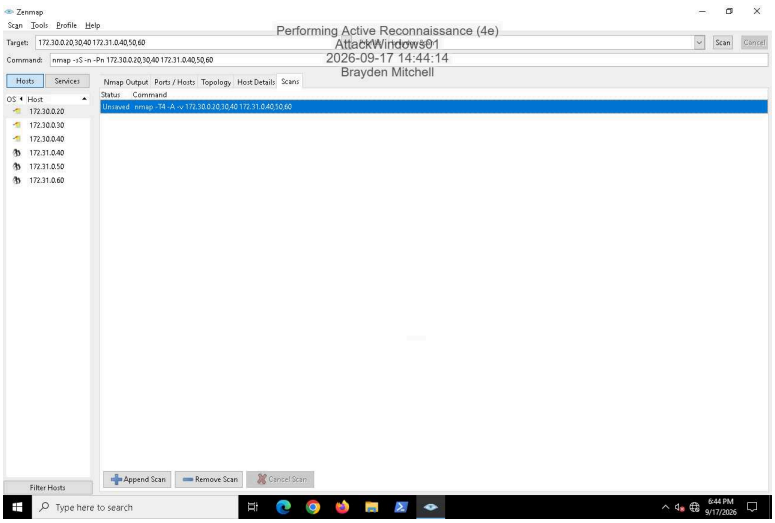
172.31.0.50 Linux 3.11-4.1
172.31.0.60
Lunux 2.6.15-2.6.26

26. **Make a screen capture** showing the **network topology**.

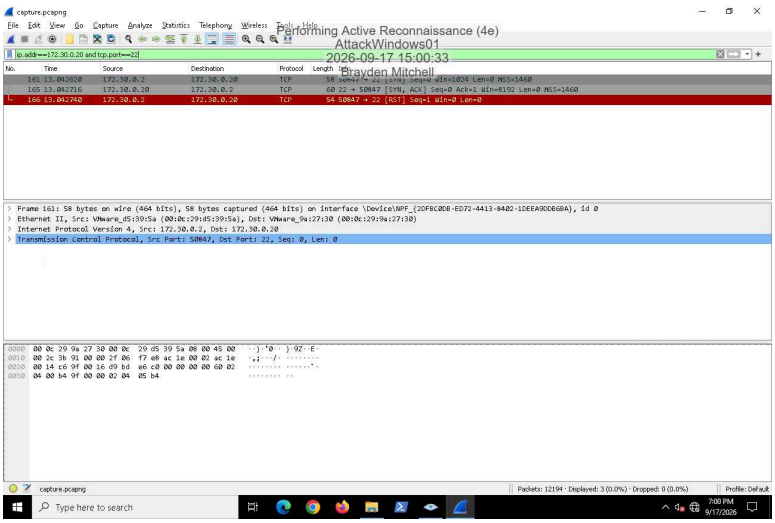


Part 2: Examine Scan Traffic with Wireshark

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

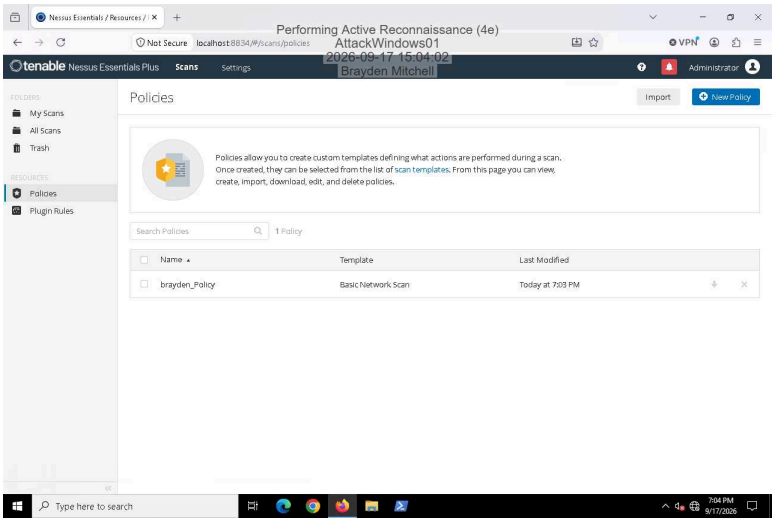


21. **Make a screen capture** showing the **3-packet sequence for the SYN scan of 172.30.0.20 port 22**.

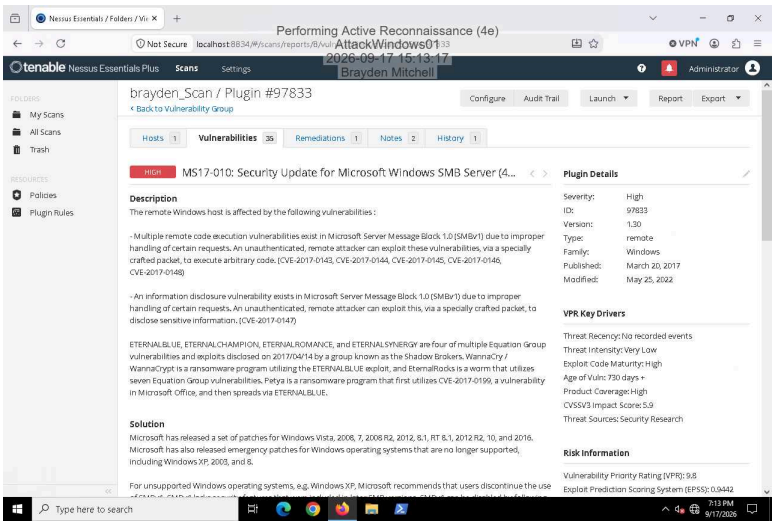


Part 3: Run a Vulnerability Scan with Nessus

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



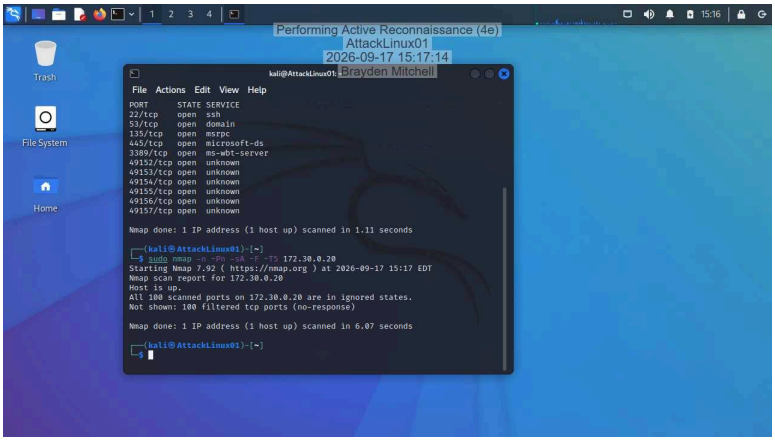
22. **Make a screen capture** showing the **vulnerability title** and the **Plugin information** for MS17-010.



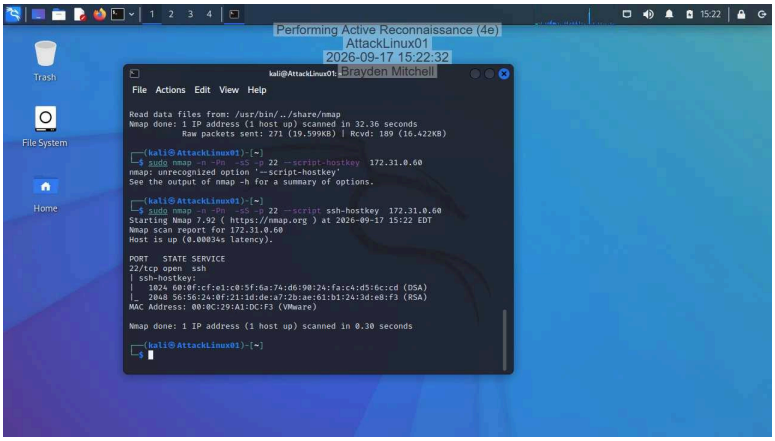
Section 2: Applied Learning

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**.

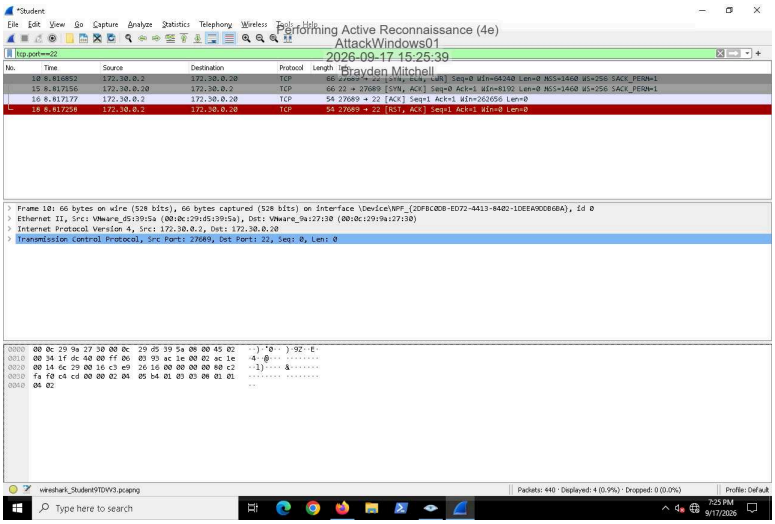


11. **Make a screen capture** showing the **results of the scan with the ssh-hostkey script**.



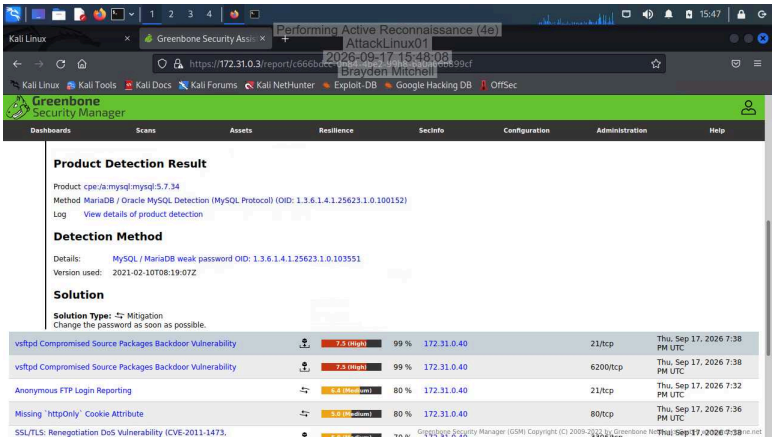
Part 2: Capture Traffic for a TCP Connect Scan

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

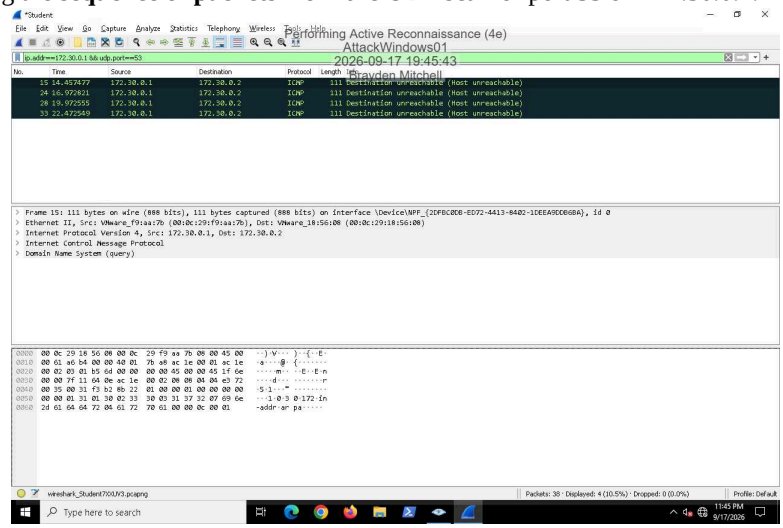
17. **Make a screen capture** showing the details of the **MySQL / MariaDB vulnerability**, including the Detection Result and the Solution.



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

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

