Student:	Email:
Courtney Watson	courtney.watson55@gmail.com

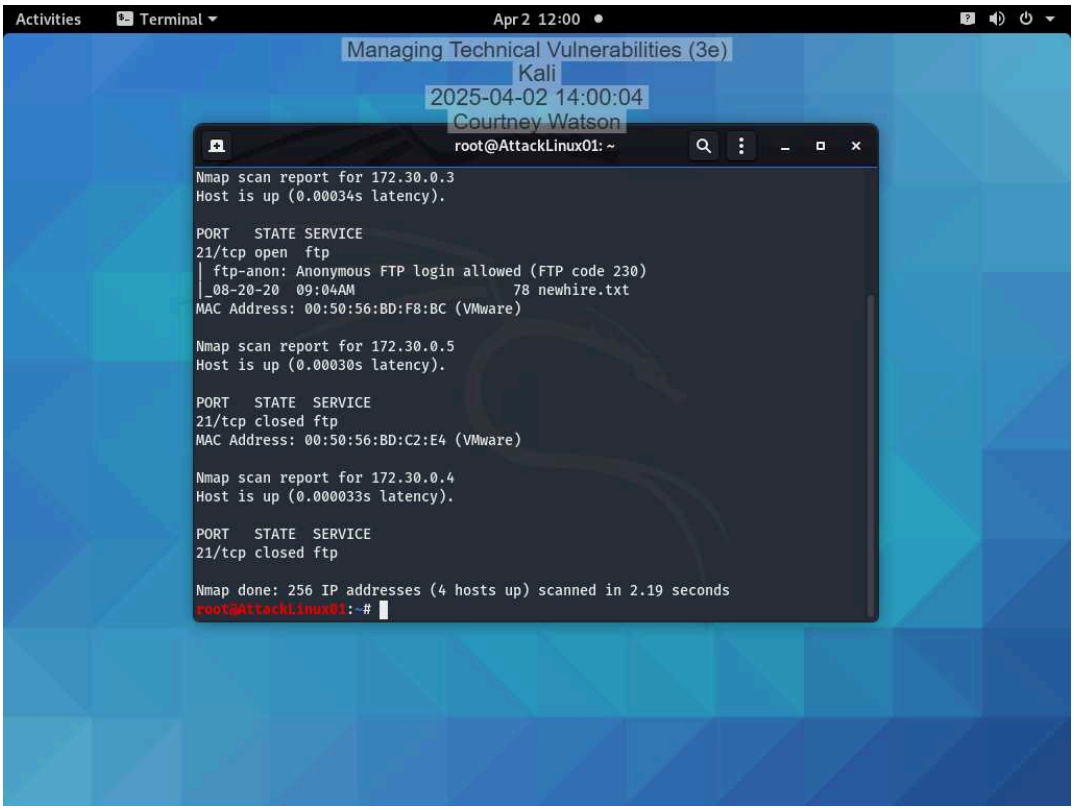
Time on Task:	Progress:
17 hours, 12 minutes	100%

Report Generated: Wednesday, April 2, 2025 at 9:43 PM

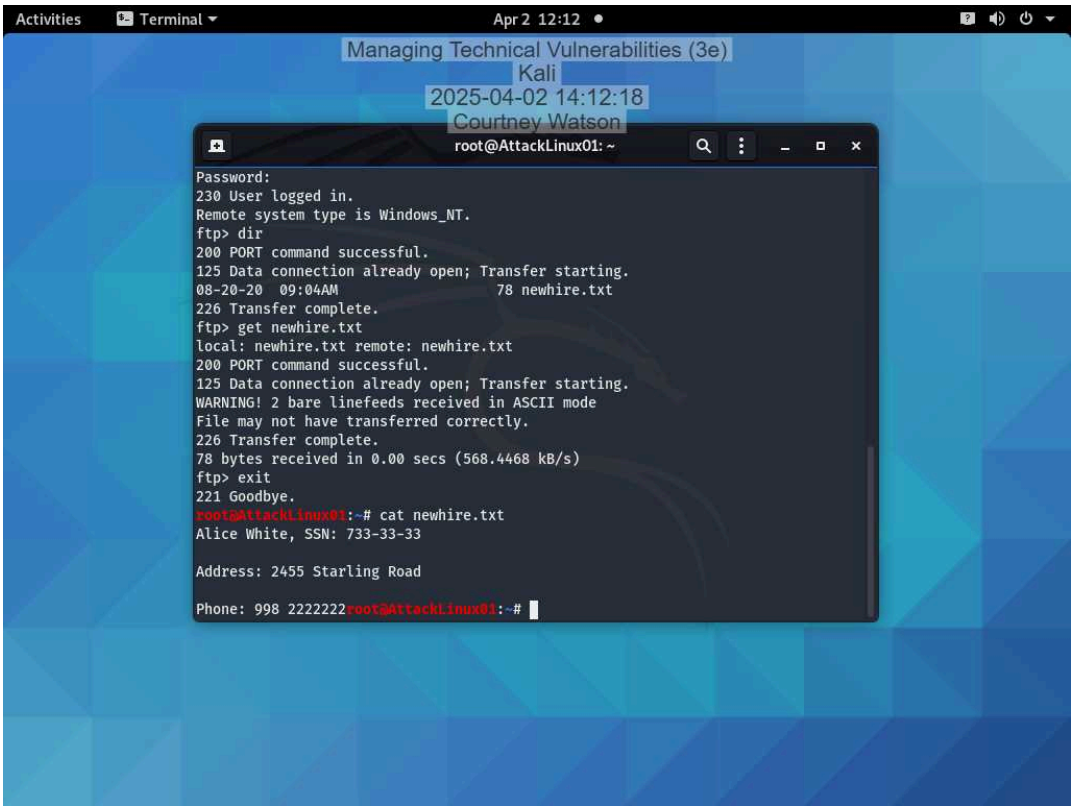
Guided Exercises

Part 1: Perform a Vulnerability Scan with Nmap

6. **Make a screen capture** showing **nmap results indicating that anonymous FTP is enabled for one of the hosts in the network**.



14. **Make a screen capture** showing the **contents of the newhire.txt file**.

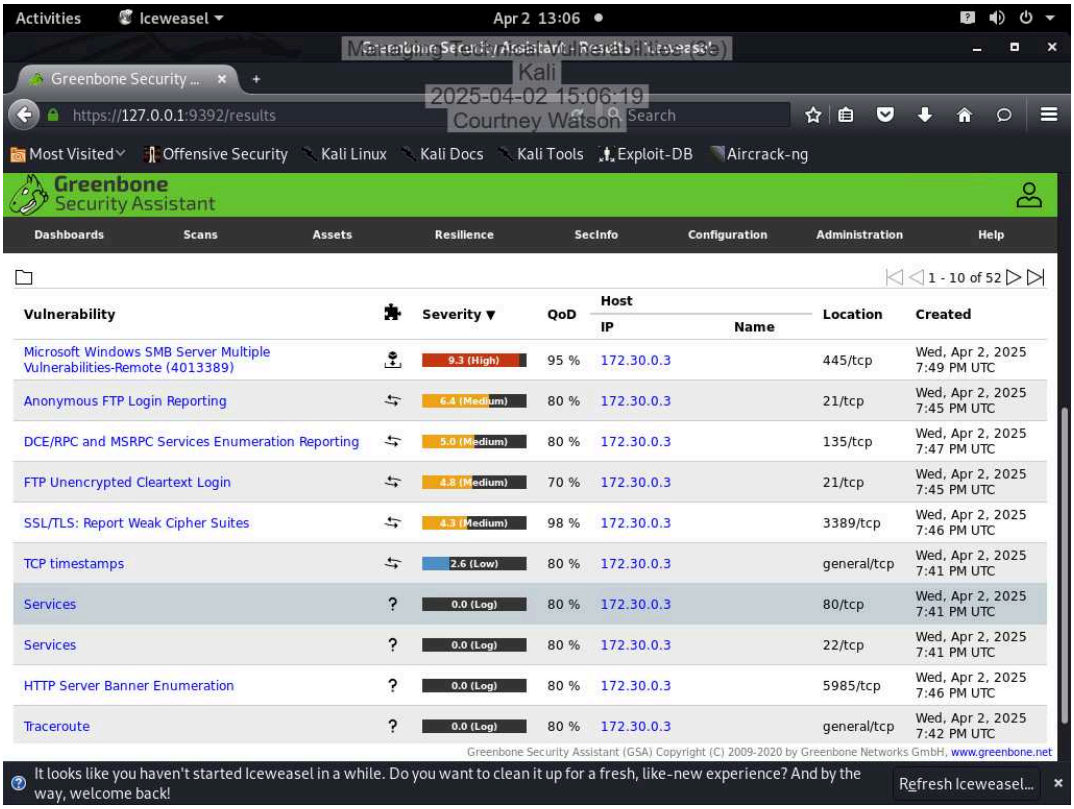


17. **Record** whether each IP address has port 445 open or closed and whether it is also vulnerable to an SMB vulnerability.

Mac Address 00:50:56:BD:CE:A6 port is open and not vulnerable MAC address 00:50:56:BD:F8:BC port is open and vulnerable MAC address 00:50:56:BD:C2:E4 port is closed 172.30.0.4 port is closed

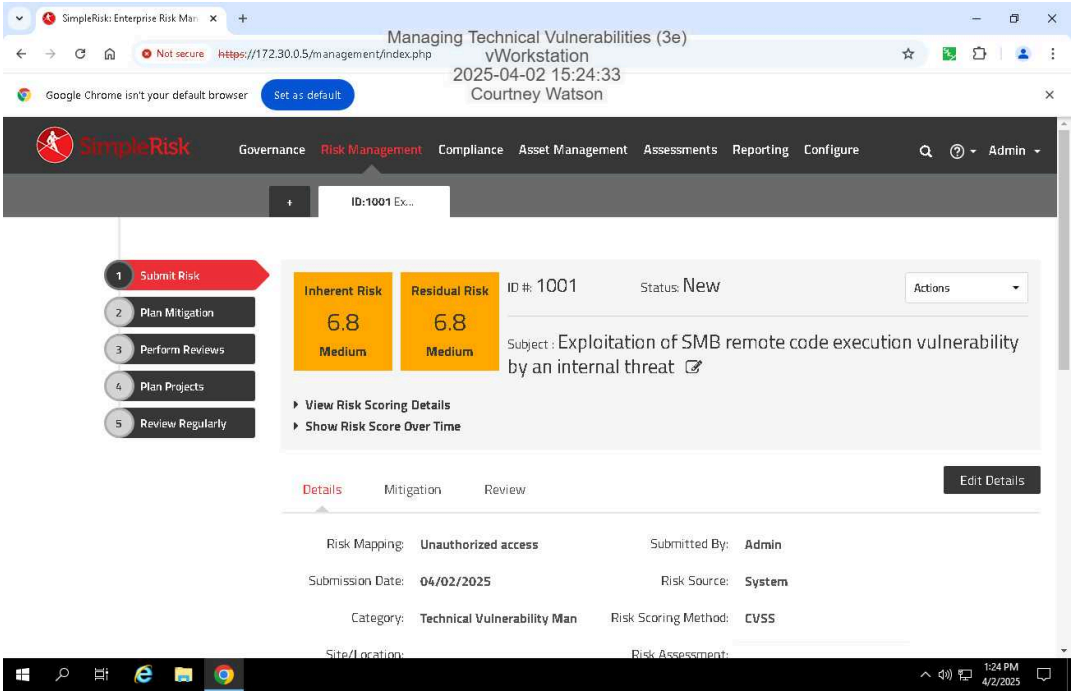
Part 2: Perform a Vulnerability Scan with the GVM Framework

15. **Make a screen capture** showing the **first page of detected vulnerabilities in the Greenbone Security Assistant.**



Part 3: Document Vulnerabilities with SimpleRisk

24. **Make a screen capture** showing the **submitted SMB remote code execution risk, including the Inherent and Residual Risk values**.



Challenge Exercise

Host 1 - IP address, operating system, and open ports

IP address: 172.30.0.2 Operating system: Microsoft Windows Server 2012 Open ports: 135-139-445-3389-5901-5985 and listed below

Host 2 - IP address, operating system, and open ports

172.30.0.3 operating system windows server 2016 open ports 445, 636, 593, 3269, 88, 464, 389, 53, 139, 22, 3389, 21

Host 3 - IP address, operating system, and open ports

IP address 172.30.0.4 operating system linux all ports closed

Host 4 - IP address, operating system, and open ports

IP address 172.30.0.5 operating system VMWARE open ports 443, 80