MAY 2025

ALPHA CSA S.O.C ANALYST GROWTH INTERNSHIP PROJECT 02 REPORT.

PROJECT TITLE:

Network Vulnerability Assessment for a More Secured Environment

Presented by : FRIDAY OBI
(On behalf of the team)

PROJECT SCOPE:

The task requires leveraging network scanning and vulnerability assessment tools and simulated real-world environment to help the client organization O-Enterprises identify and address security gaps effectively

PROJECT OVERVIEW:

Objective:
To assess vulnerabilities in O-Enterprises' simulated network using Nmap and Nessus, identify risks, and provide actionable recommendations

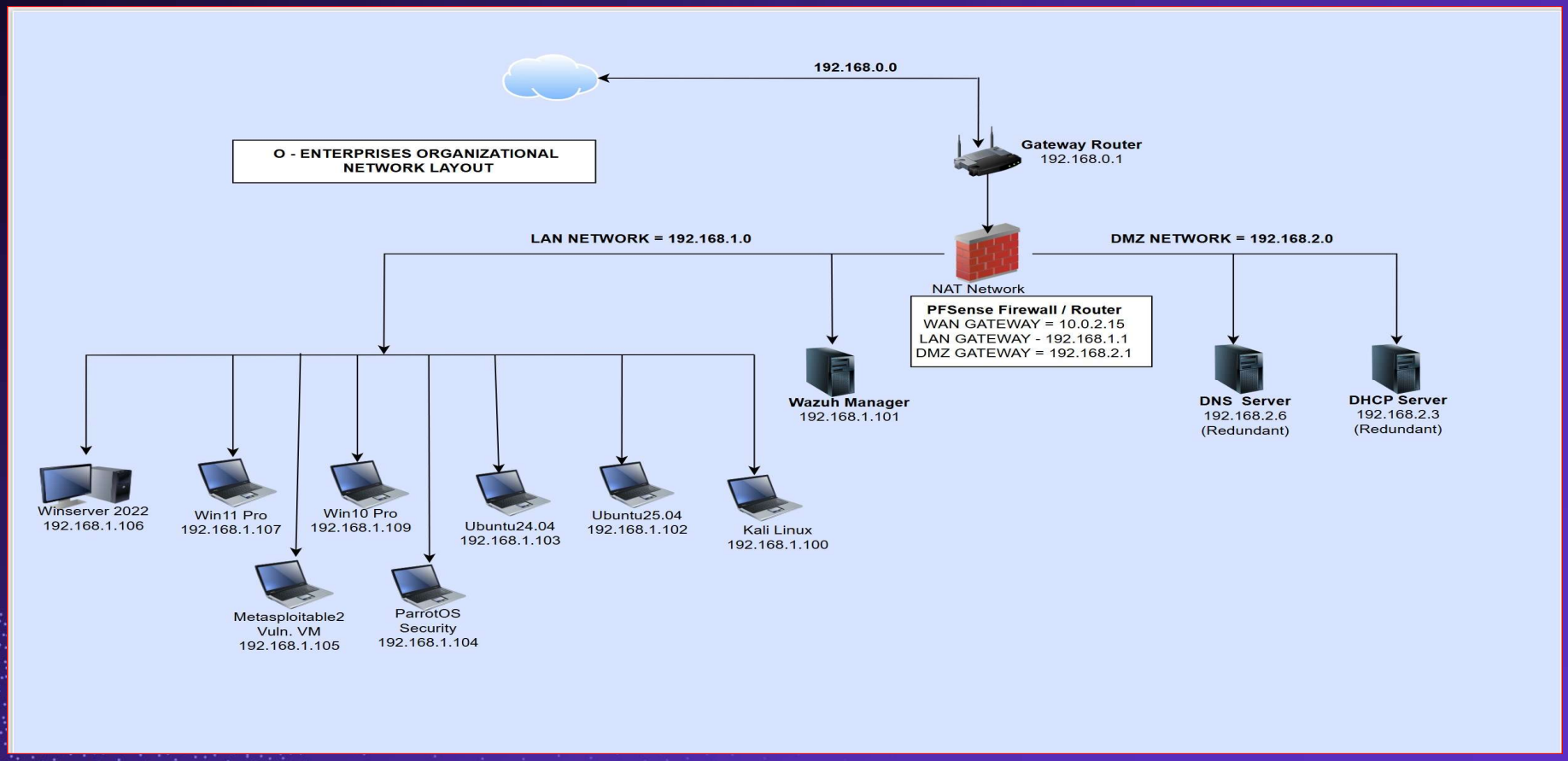
Scope:

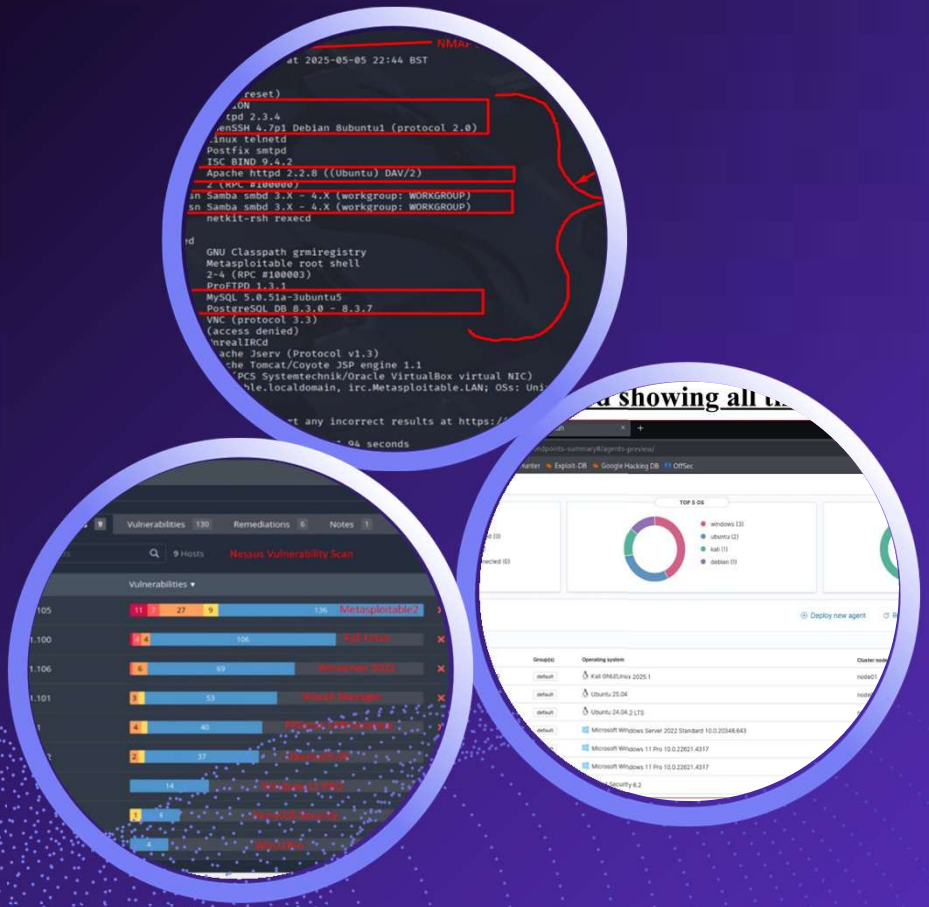
- Use of industry-standard tools (Nmap, Nessus)
- Scanning virtualized network environment
- Identifying open ports, misconfigurations, and CVEs

Tools Used:

- Nmap (Port Scanning)
- Tenable Nessus (Vulnerability Assessment)
- PFsense, Wazuh Dashboard

O-ENTERPRISE NETWORK LAYOUT





SCREENSHOT & VALIDATION:

- Network setup via Virtual Machines (Kali, Ubuntu, Windows)
- Nmap scans confirmed port/service exposure
- Nessus scans revealed vulnerabilities (with CVEs, CVSS scores)
- Results cross-validated and matched using Excel correlation sheet

KEY FINDINGS:

1 **Open Ports Detecte:**

- FTP (21), SSH (22), HTTP (80), HTTPS (443), SMB (139/445)

2 **Risk Categeries:**

- Critical: SSL cert untrusted (192.168.1.1:443)
- High: SMB signing disabled (192.168.1.102:445)
- Medium: Outdated OpenSSH (CVE-2025-32728)
- Low: TRACE/TRACK methods enabled (CVE-2010-0386)

EXECUTIVE SUMMARY:

Vulnerability assessment ID: CSA-SOC-MAY-2025-17
Assessment Risk Categories: Critical/High/Medium/Low Risks

-Enterprises noticed several discrepancies in its network environment possibly arising from misconfigurations and unpatched vulnerabilities from softwares and services in use. This gave rise to the need for a comprehensive vulnerability assessment using Nmap and Nessus to identify and mitigate these potential risks, improve overall network's security resilience and posture.

After setting up and studying the network environment, a thorough network scanning with Nmap was done. Several network ports were found to be open such Ports 21-FTP, 22-SSH, 80-HTTP, 443-HTTPS, 139/445-SMB and several others. Some of these ports are needed for day-to-day operations while some are not needed, left their current state due either misconfigurations or negligence.
Tenable-Nessus was also used to scan these hosts and the opened ports to determine the associate vulnerabilities and potential risk exposures. The identified risk categories ranged from critical to low and commensurate recommendations have been made to mitigate them before they are exploited by threat actors.

RECOMMENDATION:

- Replace untrusted SSL certificates (PFsense)
- Enforce SMB signing (Ubuntu25)
- Upgrade OpenSSH to version ≥10.0 (Kali)
- Disable TRACE/TRACK HTTP methods
- Close unused ports & fix misconfigurations immediately
- Track all remediation actions to closure

Next Steps:
Continue regular and more comprehensive vulnerability assessments, enforce patch management, and improve monitoring.

THANK YOU