

1. Introduction

Enterprise networks are the backbone of every modern organization, playing a crucial role in everything from communication to essential infrastructure. As our dependence on interconnected digital systems increases, so does the risk of cyberattacks that take advantage of misconfigurations, outdated protocols, and weak identity controls. In fact, nearly 90% of enterprise breaches are linked to identity issues or configuration errors that could have been avoided. The rise of cloud services and the Internet of Things (IoT) only adds to the complexity, creating ongoing challenges for security teams.

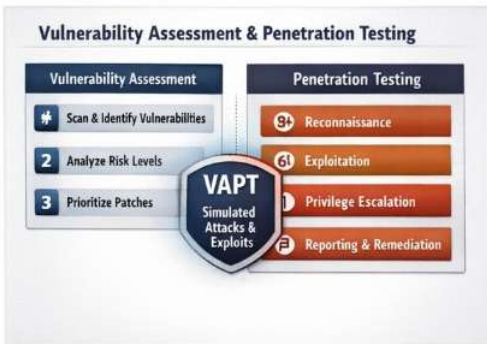
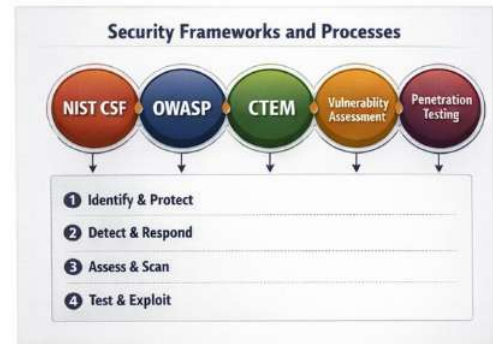
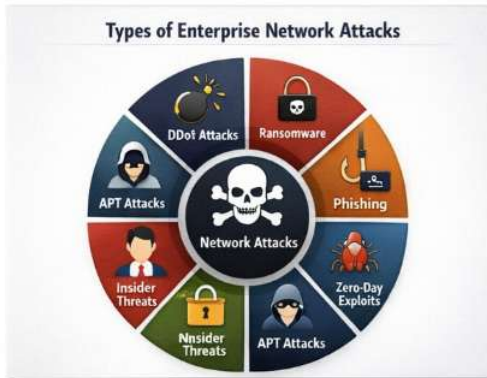
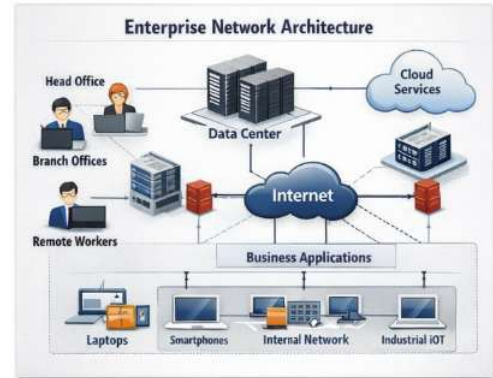


Fig. 1 – Enterprise Network Architecture, Attack Types & VAPT Framework

This project brings together literature from 2022 to 2026 and practical penetration testing in various environments, including Windows Server 2022, Windows 10, Debian Linux, and Kali Linux. The goal is to create a reliable framework for managing vulnerabilities.

2. Aim & Objectives

- To evaluate the security landscape, pinpoint vulnerabilities in enterprise networks, and put in place essential security measures, consider the following steps:
- Dive into academic and industry literature from 2022 to 2026 focused on enterprise network security.
 - Establish a solid methodology for Vulnerability Assessment and Penetration Testing (VAPT) tailored to the enterprise environment.
 - Create, implement, and document security controls that align with industry best practices.
 - Assess how effective your mitigation strategies are and tackle any remaining security gaps

3. Literature Review

Research from 2022 to 2026 consistently shows that the complexity of vulnerabilities is outpacing the capacity of security teams. More than a third of enterprise vulnerabilities are classified as High or Critical, with many being actively exploited for years before they get patched. Here are some key takeaways:

- Relying solely on CVSS isn't enough; having contextual threat intelligence can boost prioritization by as much as 95%
- AI and machine learning-driven anomaly detection are proving to be more effective than traditional signature-based methods for detecting advanced persistent threats (APTs)
- Supply chain and lateral movement attacks are managing to slip past perimeter defense
- Mixed operating system environments often lack a unified framework for cross-platform assessments

4. Methodology

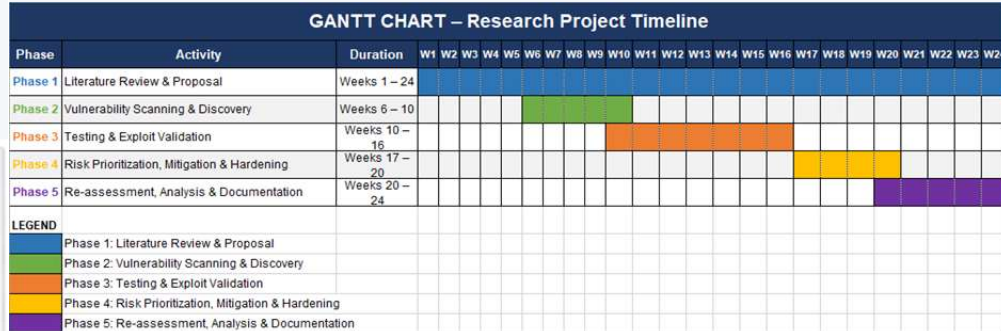


Fig. 2 – Gantt Chart: 5-Phase Research Project Timeline

Philosophy: It's all about pragmatism, mixing hard numbers like CVSS scores and vulnerability counts with the valuable insights from analysts. Strategy: We're running an experimental project within a controlled Oracle VirtualBox virtual enterprise network, allowing us to compare results before and after.

Five Sequential Phases:

- Phase 1: Reconnaissance & environment setup : host discovery, OS fingerprinting via Nmap
- Phase 2: Vulnerability scanning : Nessus Essentials credentialed/uncredentialed + NSE scripts
- Phase 3: Penetration testing : Metasploit exploit validation, PTES methodology, Dradis docs
- Phase 4: Risk prioritisation & mitigation : CVSS ranking, patching, hardening, ACL changes
- Phase 5: Reassessment & reporting : repeat scans, comparative before/after analysis

5. Design & Implementation

A virtualised SME-grade enterprise network on subnet 192.168.1.0/24 with four VMs reflecting a realistic mixed-OS enterprise:

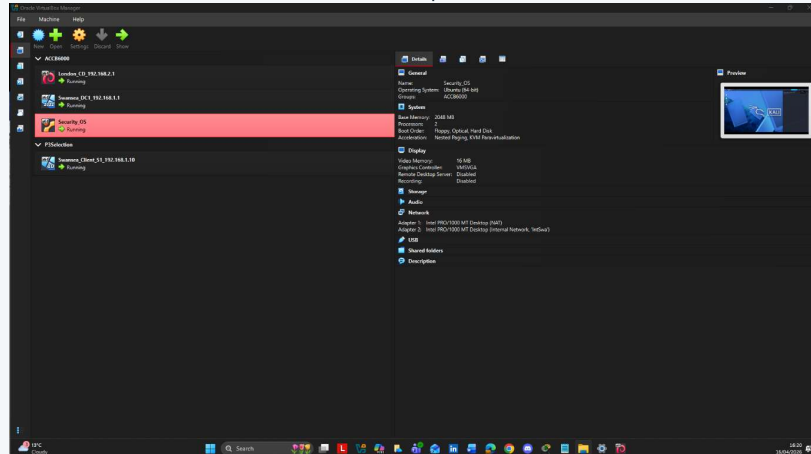


Fig. 3 – Oracle VirtualBox Manager showing all 4 VMs running

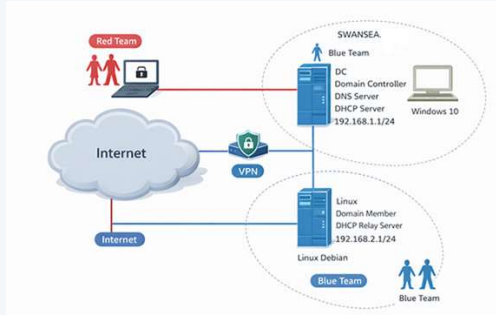


Fig. 4 – Enterprise Network Topology (Red Team vs Blue Team)

Host	OS / Role	IP / Services
WinServer_DC1	Win Server 2022 / DC	192.168.1.1 AD, DNS, SMB, RDP, IIS
WinClient_S1	Windows 10 Pro / Client	192.168.1.10 SMB, RDP
Kali_Security_OS	Kali Linux / Pen Test	192.168.1.30 Nmap, Nessus, MSF
London_CD	Debian Linux / Server	192.168.2.1 Segmented host

6. Results & Analysis

- Pre-mitigation Nessus scans revealed multiple Critical and High CVEs across the domain controller and Windows 10 client. Key attack vectors validated via Metasploit:
- SMB Relay Attack NTLM hashes captured via smb_relay (SMB signing disabled)
 - RDP Brute-Force Weak local admin credentials cracked via rdp_login module
 - IIS Information Disclosure Directory browsing exposed config files
 - Lateral Movement Pass-the-hash + PowerShell post-exploitation across hosts

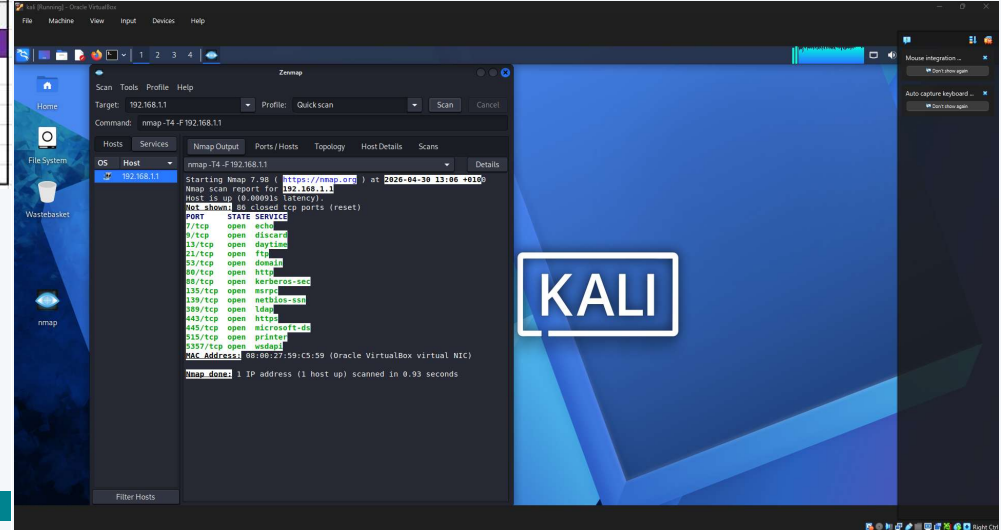


Fig. 5 – Nmap/Zenmap scan revealing open ports on DC (192.168.1.1)

Vulnerability Summary : Pre vs Post Mitigation:

Severity	Pre-Mitigation	Post-Mitigation
Critical	8	1 (~88%)
High	14	3 (~79%)
Medium	22	9 (~59%)
Low	11	5 (~55%)

Key Mitigations Applied:

- SMB signing enforced across all hosts via Group Policy
- RDP restricted to NLA; firewall ACL limits access by IP
- Windows cumulative updates applied; IIS directory browsing disabled
- Strong password policy + account lockout threshold enforced
- PowerShell execution policy → Restricted; Defender re-enabled

7. Conclusion

Post-mitigation reassessment confirmed measurable security improvements across all hosts. The five-phase VAPT methodology combining automated scanning with manual exploitation and risk-prioritised remediation proved highly effective.

The validated framework aligns with PTES and NIST SP 800-115 and provides a replicable security assessment model applicable to mixed-OS enterprise environments.

Future Work:

- Red team exercises with extended APT dwell-time simulations
- AI/LLM-driven automated vulnerability validation workflows
- Zero-trust architecture implementation & SIEM integration

8. References

- [1] Verizon DBIR 2023 Enterprise Network Threat Report
- [2] NIST SP 800-115 Technical Guide to IT Security Testing
- [3] Rapid7 Vulnerability Intelligence Report 2024
- [4] MITRE ATT&CK Framework v14 Lateral Movement Tactics
- [5] Shostack, A. (2022). Threat Modelling. Wiley