Project Overview

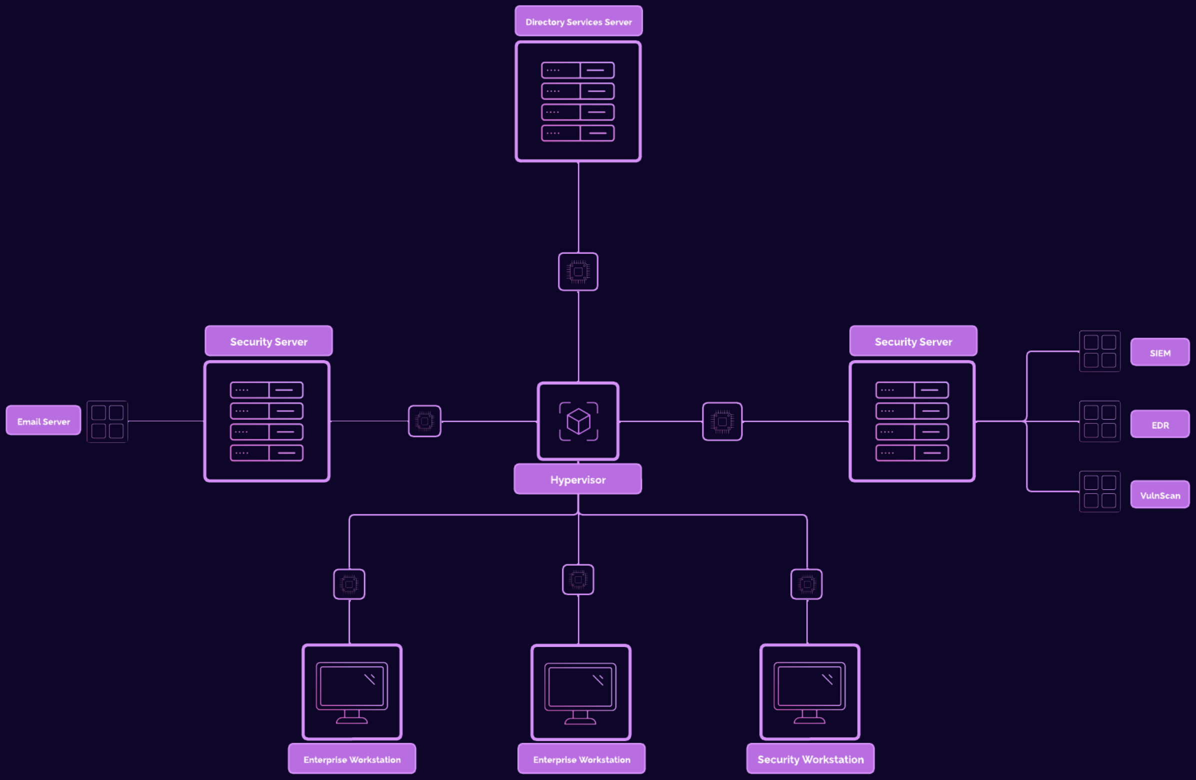
[Enterprise 101]

>projectsecurity_

Project Overview

Network Topologies

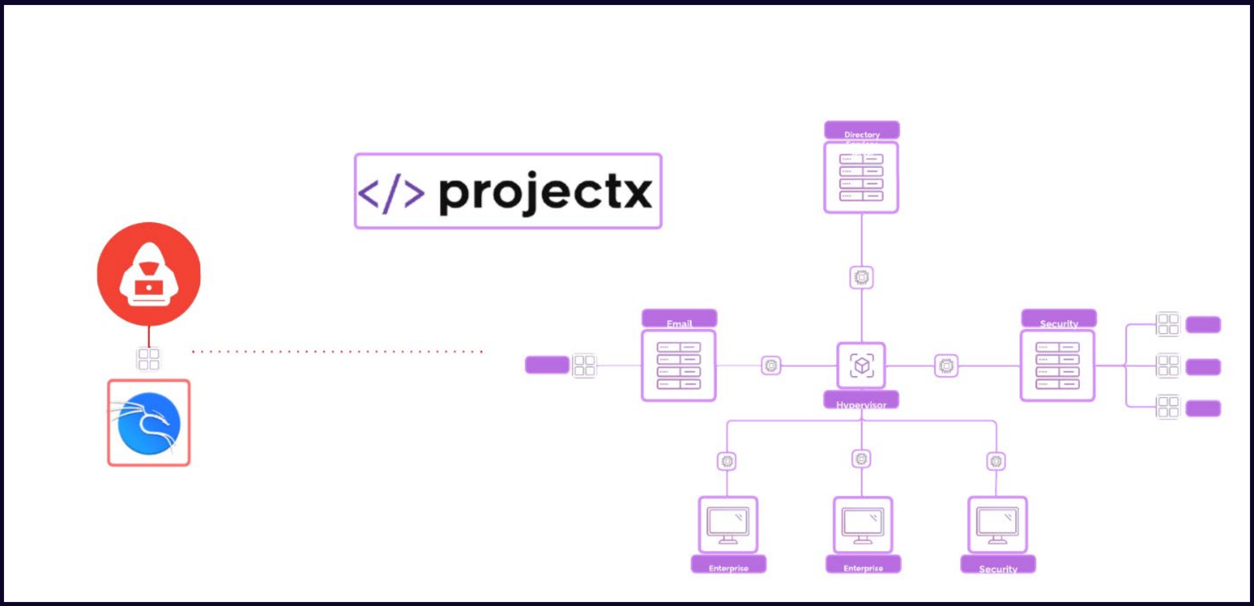
Base



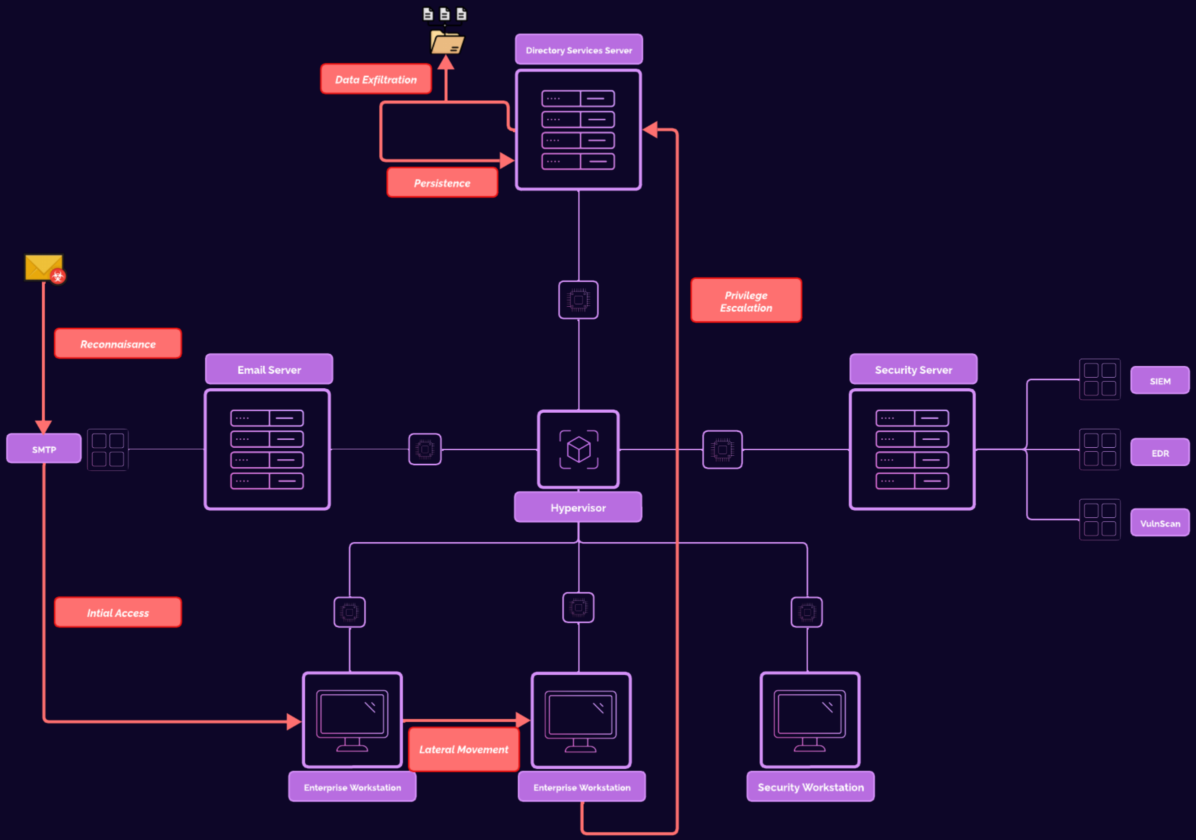
NAT Network

- Name: `project-x-nat` (NatNetwork)
- IP Address Range: `10.0.0.0/24`
  - Usable Range: `10.0.0.1 – 10.0.0.254`
  - DHCP Dynamic Scope: `10.0.0.100 – 10.0.0.200`

Attacker



Cyber Attack Simulation



Hosts

Hostname [project-x-...]	IP Address	Function
-dc (corp.project-x-dc.com)	10.0.0.5	Domain Controller (DNS, DHCP, SSO)
email-svr	10.0.0.8	SMTP Relay Server
-sec-box	10.0.0.10	Dedicated Security Server
-sec-work	10.0.0.103 or (dynamic)	Security Playground
-win-client	10.0.0.100 or (dynamic)	Windows Workstation
-linux-client	10.0.0.101 or (dynamic)	Linux Desktop Workstation
attacker	dynamic	Attacker Environment

Accounts & Passwords

Account	Password	Host
Administrator	@Deeboodah1!	...-dc
johnd@corp.project-x-dc.com	@password123!	...-win-client
janed@linux-client	@password123!	...-linux-client
project-x-sec-work	@password123!	...-sec-work
sec-work@sec-box	@password123!	...-sec-box
email-svr@project-x-email-svr	@password123!	...-email-svr
attacker@attacker	attacker	attacker

Operating Systems

Windows Server 2025: Designed to support enterprise-level applications and network management, and identity management. This will be used as the directory services server, acting as the central hub for network connection.

Windows 11 Enterprise: Desktop operating system optimized for everyday productivity. Most common operating system used in business environments for employees. This will be used to simulate a business user.

Ubuntu Desktop 22.04: General-purpose desktop. Commonly used for software development. This will be used to simulate an enterprise software development environment.

Security Onion: An open-source platform for security monitoring, log analysis, and intrusion detection, used by cybersecurity professionals to detect, investigate, and respond to network threats and incidents.

Ubuntu Server 2022: A Linux server operating system widely used for hosting applications, databases, and web services. This will be used as our email server.

Kali Linux: A Debian-based Linux distribution tailored for penetration testing and ethical hacking. It comes pre-installed with a wide range of tools for vulnerability assessment, exploitation, wireless testing, and digital forensics.

VirtualBox VMs

VirtualBox will be used as our hypervisor for virtualization. Reference below for Virtual Machine specifications.

VM Name	Operating System	Specs	Storage (minimum)
[project-x-dc]	Windows Server 2025	2 CPU / 4096 MB	50 GBs
[project-x-win-client]	Windows 11 Enterprise	2 CPU / 4096 MB	80 GBs
[project-x-linux-client]	Ubuntu 22.04 Desktop	1 CPU / 2048 MB	80 GBs
[project-x-sec-work]	Security Onion	1 CPU / 2048 MB	55 GBs
[project-x-sec-box]	Ubuntu 22.04 Desktop	2 CPU / 4096 MB	80 GBs
[project-x-email-svr]	Ubuntu Server 22.04	1 CPU / 2048 MB	25 GBs
[project-x-attacker]	Kali Linux 2024.2	1 CPU / 2048 MB	55 GBs

Tools

Enterprise Tools + Defense

Microsoft Active Directory: A directory service used for managing and organizing network resources, users, and permissions in a Windows environment.

Wazuh: An open-source security monitoring platform that provides intrusion detection, log analysis, vulnerability detection, and compliance reporting.

Postfix: A popular open-source mail transfer agent (MTA) used for sending and receiving email on Unix-like operating systems.

Offense

Evil-WinRM: A powerful Ruby-based Windows Remote Management (WinRM) client used by penetration testers to connect to and interact with Windows systems, often for post-exploitation tasks such as command execution and data extraction.

Hydra: A fast and flexible password-cracking tool designed to perform brute-force and dictionary-based attacks on various network protocols, including SSH, HTTP, FTP, and more.

SecLists: A comprehensive collection of penetration testing resources, including wordlists for usernames, passwords, web directories, and other payloads used in reconnaissance and exploitation phases.

NetExec: A network exploitation tool that enables remote command execution on target machines through various protocols, assisting in lateral movement and privilege escalation scenarios.

XFreeRDP: An open-source implementation of the Remote Desktop Protocol (RDP), enabling penetration testers to connect to and control Windows systems remotely for reconnaissance and post-exploitation purposes.

Guides Numerical Order

Below is the numerical order for the step-by-step guides. These guides serve as the basis for the project. It is recommended the respective guide is opened while following along in the program.

> 👉 If you prefer to follow content by reading, these guides will provide the same information as the video lectures.

Guides

1. [Guide] A Primer On Provisioning Virtual Machines with VirtualBox
2. [Guide] Build a Directory Service Server With Active Directory
3. [Guide] Provision & Setup Windows 11 Enterprise
4. [Guide] Provision & Setup Ubuntu Desktop 22.04
5. [Guide] Provision & Setup Ubuntu Server 22.04
6. [Tool Guide] Setup Postfix Mail Transfer Agent
7. [Guide] Provision & Setup Security Onion
8. [Guide] Security Server - Provision & Setup Ubuntu Desktop 22.04
9. [Tool Guide] Setup Wazuh
10. [Guide] Configure a Vulnerable Environment
11. [Guide] Setup The Attacker Machine
12. [Guide] Cyber Attack - Initial Access To Breached