1

Introduction
Throwback is an Active Directory (AD) lab that teaches the fundamentals and core concepts of attacking a Windows network. The network simulates a realistic corporate environment that has several attack vectors you would expect to find in today's organisations.
The lab uses a structured, hand-held approach to guide users through exploiting the network. The use of Windows to manage authentication and user identities in IT infrastructure today is so commonly used; as an aspiring security practitioner, it's crucial to understand how this works and the network's common weaknesses.
You will explore the following attacks:
• Phishing & OSINT
• Offensive Powershell
• Active Directory Basics
• Kerberos Abuse
• Custom Malicious Macros
• Active Directory Enumeration & Exploitation
• Attacking Mail Servers
• Firewall Pivoting
• C2 Frameworks
• Abusing Cross-Domain Trusts

This network has been designed to have multiple attack paths.

Accessing the Network
To access the network, you will need to first connect to our network using OpenVPN. Here is a mini walkthrough of connecting to the Throwback-specific network. You can also use the web-based Kali Linux or Kali Linux machine.

Answer the questions below

Go to your access page. Select 'Throwback' from the VPN servers (under the network tab) and download your configuration file

Question Done

Use an OpenVPN client to connect. This example shows the client on Linux, use this guide to connect using Windows or MacOS

Question Done

Return to your access page. You can verify you are connected by looking on your access page. Refresh the page. You should see a green tick next to Connected. It will also show you your internal IP address.

Question Done

Alternatively, you can deploy the web-based AttackBox or Kali machine

Question Done