100daysofcybersecurity Week 1 breakdown and resources

Introduction

Week 1 focused on foundational cybersecurity concepts and building a comprehensive cybersecurity home lab. This setup forms the core environment for all offensive, defensive, cloud, and SOC-related tasks in the coming weeks.

Day 1: Program Overview + Virtualization Setup

	Topic	Resourcess
1.	13-week overview	[Resource](#)
2.	Terms to get familiar with: Operating system(s), Virtualization, Hypervisor, Virtual Machine(s). Short dive	[Resource](#)
3.	Install VirtualBox/VMware/UTM	[Resource1](#), [Resource2](#), [Resource3](#)
4.	Downloaded Kali, Ubuntu, and Windows OS images	[Resource1](#), [Resource2](#), [Resource3](#)
5.	Review the CIA triad and Defence-in-Depth	[Resource](#)

Day 2: Kali Linux Installation

	Topic	Resources
1.	Install Kali Linux with 2 CPUs, 4–8GB RAM	[Windows](#), [MAC](#)

2.	Update packages and installed tools: Nmap, Wireshark, Git, Python3	[Resource](#)
3.	Practice Linux terminal basics	[Resource1](#), [Resource2](#)

Day 3: Windows 10 VM Setup

	Topic	Resources
1.	Install Windows 10	[Resource](#)
2.	Add Sysinternals Suite, 7zip, Chrome	[Resource](#)
3.	Learn Windows logs and Event Viewer fundamentals	[Resource](#)

Day 4: Ubuntu Server Installation

	Topic	Resources
1.	Install Ubuntu Server and enable OpenSSH	[Install](#), [OpenSSH](#)
2.	Configure a static IP address	[Resource](#)
3.	Practice SSH remote access	[Resource](#)

Day 5: Networking Configuration

	Topic	Resources
1.	Build an internal lab network using Host-Only + NAT adapters	[Resource](#)

2.	Verify connectivity using ping between all VMs	Resource
3.	Learn IP addressing and subnetting basics	Resource

Day 6: Wireshark & Packet Analysis

	Topic	Resources
1.	Install Wireshark on Kali and Windows	Resource
2.	Capture DNS and HTTP packets	Resource
3.	Learn to apply filters (dns, http, ip.src)	

Day 7: Compilation