# Cybersecurity Analyst Course - Class 1

This document provides an overview of the fundamental concepts in cybersecurity and practical instructions for setting up your lab environment.

## 1. Cybersecurity Fundamentals

### 1.1 The CIA Triad

The CIA Triad is a foundational model in information security, guiding policies for information security within an organization. It consists of three key principles:

* **Confidentiality:** This principle ensures that information is accessible only to those authorized to have access. It prevents sensitive data from being disclosed to unauthorized individuals, entities, or processes. Methods to ensure confidentiality include encryption, access controls, and data classification.
* **Integrity:** Integrity ensures the accuracy and completeness of information and its methods of processing. It means that data has not been altered or destroyed in an unauthorized manner. Techniques like hashing, digital signatures, and intrusion detection systems help maintain data integrity.
* **Availability:** This principle ensures that authorized users have reliable and timely access to information and resources when needed. It focuses on maintaining the functionality of information systems and preventing disruptions. Redundancy, backups, and disaster recovery plans are crucial for ensuring availability.

## 2. Difference between Information Security and Cybersecurity

While often used interchangeably, information security and cybersecurity have distinct focuses:

* **Information Security (InfoSec):** This is a broader field that deals with the protection of all information assets, regardless of their format (digital or physical). It encompasses the confidentiality, integrity, and availability (CIA triad) of data, as well as policies, procedures, and practices to manage information risks. InfoSec aims to protect information from unauthorized access, use, disclosure, disruption, modification, or destruction.
* **Cybersecurity:** This is a subset of information security that specifically focuses on protecting digital information and systems from cyber threats. It deals with securing computer systems, networks, programs, and data from digital attacks, damage, or unauthorized access. Cybersecurity primarily addresses threats that originate from the cyber domain, such as malware, phishing, hacking, and denial-of-service attacks.

In essence, cybersecurity is concerned with the digital realm of information protection, while information security covers all aspects of information protection, including physical security, human factors, and compliance.

## 3. Different Domains of Security

Cybersecurity is a vast field with various specialized domains, each focusing on protecting different aspects of an organization’s digital assets:

### 3.1 Application Security

Application security focuses on making applications more secure by finding, fixing, and preventing security vulnerabilities in software. This involves security measures implemented throughout the software development lifecycle (SDLC), from design and development to deployment and maintenance. The goal is to protect applications from threats that could exploit weaknesses in their code, design, or configuration.

Key aspects of application security include:

* **Secure Coding Practices:** Developers follow guidelines to write code that is resistant to common vulnerabilities like SQL injection, cross-site scripting (XSS), and buffer overflows.
* **Security Testing:** This involves various testing methods such as static application security testing (SAST), dynamic application security testing (DAST), and penetration testing to identify vulnerabilities.
* **Web Application Firewalls (WAFs):** These protect web applications from common web exploits by filtering and monitoring HTTP traffic between a web application and the Internet.
* **API Security:** Securing the application programming interfaces (APIs) that allow different software systems to communicate.

### 3.2 Network Security

Network security involves protecting the underlying network infrastructure and data as it travels across the network. It aims to prevent unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

Key components of network security include:

* **Firewalls:** Act as a barrier between a trusted internal network and untrusted external networks, controlling incoming and outgoing network traffic.
* **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** IDS monitors network traffic for suspicious activity and alerts administrators, while IPS actively blocks or prevents detected threats.
* **Virtual Private Networks (VPNs):** Create a secure, encrypted connection over a less secure network, like the internet.
* **Network Segmentation:** Dividing a network into smaller, isolated segments to limit the spread of breaches.

### 3.3 Cloud Security

Cloud security refers to the set of policies, controls, procedures, and technologies that work together to protect cloud-based systems, data, and infrastructure. As organizations increasingly adopt cloud computing, securing these environments becomes critical.

Key considerations in cloud security include:

* **Data Security:** Protecting data stored and processed in the cloud through encryption, access controls, and data loss prevention (DLP).
* **Identity and Access Management (IAM):** Managing and controlling user access to cloud resources.
* **Cloud Security Posture Management (CSPM):** Continuously monitoring cloud environments for misconfigurations and compliance violations.
* **Cloud Workload Protection Platforms (CWPP):** Securing workloads (e.g., virtual machines, containers) running in cloud environments.

### 3.4 OT Security

Operational Technology (OT) security focuses on protecting industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and other operational technologies used in critical infrastructure and industrial environments. Unlike IT security, OT security prioritizes availability and safety, as disruptions can have severe physical consequences.

Key aspects of OT security include:

* **Asset Inventory and Management:** Identifying and cataloging all OT devices and systems.
* **Network Segmentation:** Isolating OT networks from IT networks to prevent IT-based threats from impacting operational systems.
* **Vulnerability Management:** Identifying and mitigating vulnerabilities in OT systems, often requiring specialized tools and processes due to the unique nature of OT devices.
* **Incident Response:** Developing specific incident response plans for OT environments to minimize downtime and ensure safety.

## 4. Basic Terminologies

### 4.1 Encryption

Encryption is a form of data security in which information is converted to ciphertext. Only authorized people who have the key can decipher the code and access the original plaintext information.

In even simpler terms, encryption is a way to render data unreadable to an unauthorized party. This serves to thwart cybercriminals, who may have used quite sophisticated means to gain access to a corporate network—only to find out that the data is unreadable and therefore useless.

Encryption not only ensures the confidentiality of data or messages but it also provides authentication and integrity, proving that the underlying data or messages have not been altered in any way from their original state.

**How Encryption Works:**

Original information, or plain text, might be something as simple as “Hello, world!” As cipher text, this might appear as something confusing like 7\*#0+gvU2x—something seemingly random or unrelated to the original plaintext.

Encryption, however, is a logical process, whereby the party receiving the encrypted data—but also in possession of the key—can simply decrypt the data and turn it back into plaintext.

For decades, attackers have tried by brute force—essentially, by trying over and over again—to figure out such keys. Cybercriminals increasingly have access to stronger computing power such that sometimes, when vulnerabilities exist, they are able to gain access.

Data needs to be encrypted when it is in two different states: “at rest,” when it is stored, such as in a database; or “in transit,” while it is being accessed or transmitted between parties.

An encryption algorithm is a mathematical formula used to transform plaintext (data) into ciphertext. An algorithm will use the key to alter the data in a predictable way. Even though the encrypted data appears to be random, it can actually be turned back into plaintext by using the key again. Some commonly used encryption algorithms include Blowfish, Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4), RC5, RC6, Data Encryption Standard (DES), and Twofish.

Encryption has evolved over time, from a protocol that was used only by governments for top-secret operations to an everyday must-have for organizations to ensure the security and privacy of their data.

**Types Of Encryption:**

There are many different types of encryption, each with its own benefit and use case.

* **Symmetric encryption:** In this simple encryption method, only one secret key is used to both cipher and decipher information. While the oldest and best-known encryption technique, the main drawback is that both parties need to have the key used to encrypt the data before they can decrypt it. Symmetric encryption algorithms include AES-128, AES-192, and AES-256. Because it is less complex and executes faster, symmetric encryption is the preferred method for transmitting data in bulk.
* **Asymmetric encryption:** Also known as public key cryptography, asymmetric encryption is a relatively new method that uses two different but related keys to encrypt and decrypt data. One key is secret and one key is public. The public key is used to encrypt data, and the private key is used to decrypt (and vice versa). Security of the public key is not needed because it is publicly available and can be shared over the internet.
* **Data Encryption Standard (DES):** DES is a deprecated symmetric key method of data encryption. DES works by using the same key to encrypt and decrypt a message, so both the sender and the receiver must have access to the same private key. DES has been superseded by the more secure AES algorithm. It was adopted by the U.S. government as an official standard in 1977 for the encryption of government computer data. It can be said that DES was the impetus for the modern cryptography and encryption industry.
* **Triple Data Encryption Standard (3DES):** The Triple Data Encryption Standard involved running the DES algorithm three times, with three separate keys. 3DES was largely seen as a stopgap measure, as the single DES algorithm was increasingly becoming seen as too weak to stand up to brute force attacks and the stronger AES was still under evaluation.
* **RSA:** Rivest-Shamir-Adleman (RSA) is an algorithm and the basis of a cryptosystem—a suite of cryptographic algorithms used for specific security services or purposes. This enables public key encryption and is often used by browsers to connect to websites and by virtual private networks (VPNs). RSA is asymmetric, in which two different keys are used for encryption: one public and one private. If decryption is carried out with the public key, encryption is performed with the private key, or vice versa.
* **Advanced Encryption Standard (AES):** Developed in 1997 by the National Institute of Standards and Technology (NIST) as an alternative to the Data Encryption Standard, the Advanced Encryption Standard is a cipher chosen by the U.S. government to protect sensitive information. AES has three different key lengths to encrypt and decrypt a block of messages: 128-bit, 192-bit, and 256-bit. AES is widely used for protecting data at rest in such applications as databases and hard drives.
* **Encryption in the cloud:** Cloud encryption is a service offered by cloud storage providers in which data is first encrypted using algorithms before being pushed to a storage cloud. Customers of a cloud storage provider must be aware of and comfortable with the level of depth of the provider’s policies and procedures for encryption and encryption key management.
* **End-to-End encryption (E2EE):** E2EE ensures that only the two users communicating with one another can read the messages. Even the intermediary, such as the telecom or internet service provider, cannot decrypt the messages. E2EE is generally seen as the most secure way to communicate privately and securely online.

### 4.3 Intrusion Prevention System (IPS)

An intrusion prevention system (IPS) monitors network traffic for potential threats and automatically blocks them by alerting the security team, terminating dangerous connections, removing malicious content or triggering other security devices.

IPS solutions evolved from intrusion detection systems (IDSs), which detect and report threats to the security team. An IPS has the same threat detection and reporting functions as an IDS plus automated threat prevention abilities, hence they are sometimes called “intrusion detection and prevention systems” (IDPS).

Because an IPS can directly block malicious traffic, it can lighten workloads for security teams and security operations centers (SOCs), allowing them to focus on more complex threats. IPSs can help enforce network security policies by blocking unauthorized actions from legitimate users, and they can support compliance efforts. For example, an IPS fulfills the Payment Card Industry Data Security Standard (PCI-DSS) requirement for intrusion detection measures.

**IPS threat detection methods:**

IPSs use three primary threat detection methods, exclusively or in combination, to analyze traffic.

* **Signature-based detection:** Analyzes network packets for attack signatures—unique characteristics or behaviors that are associated with a specific threat. A sequence of code that appears in a particular malware variant is an example of an attack signature.
* **Anomaly-based detection:** Uses artificial intelligence and machine learning to create and continually refine a baseline model of normal network activity. The IPS compares ongoing network activity to the model and responds when it finds deviations, like a process that uses more bandwidth than typical or a device that opens a port that’s usually closed.
* **Policy-based detection:** Based on security policies set by the security team. Whenever a policy-based IPS detects an action that violates a security policy, it blocks the attempt.

**IPS threat prevention methods:**

When an IPS detects a threat, it logs the event and reports it to the SOC. But the IPS doesn’t stop there. It automatically takes action against the threat by using techniques such as:

* **Blocking malicious traffic:** An IPS may end a user’s session, block a specific IP address or even block all traffic to a target. Some IPSs can redirect traffic to a honeypot, a decoy asset that makes the hackers think they’ve succeeded when, really, the SOC is watching them.
* **Removing malicious content:** An IPS may allow traffic to continue but scrub the dangerous parts, such as by dropping malicious packets from a stream or removing a malicious attachment from an email.
* **Triggering other security devices:** An IPS may prompt other security devices to act, such as by updating firewall rules to block a threat or changing router settings to prevent hackers from reaching their targets.
* **Enforcing security policies:** Some IPSs can prevent attackers and unauthorized users from doing anything that violates company security policies. For example, if a user tries to transfer sensitive information out of a database it’s not supposed to leave, the IPS would block them.

**Types of intrusion prevention systems:**

IPS solutions can be software applications installed on endpoints, dedicated hardware devices connected to the network or delivered as cloud services. Because IPSs must be able to block malicious activity in real time, they’re always placed “inline” on the network, meaning traffic passes directly through the IPS before reaching its destination.

IPSs are categorized based on where they sit in a network and what kind of activity they monitor. Many organizations use multiple types of IPSs in their networks.

* **Network-based intrusion prevention systems (NIPS):** Monitors inbound and outbound traffic to devices across the network, inspecting individual packets for suspicious activity. NIPS monitors are placed at strategic points in the network. They often sit immediately behind firewalls at the network perimeter so they can stop malicious traffic breaking through. NIPS’s may also be placed inside the network to monitor traffic to and from key assets, like critical data centers or devices.
* **Host-based intrusion prevention systems (HIPS):** Installed on a specific endpoint, like a laptop or server, and monitors only traffic to and from that device. HIPS are usually used in conjunction with NIPS to add extra security to vital assets. HIPS can also block malicious activity from a compromised network node, like ransomware spreading from an infected device.
* **Network behavior analysis (NBA):** Solutions that monitor network traffic flows. NBAs may inspect packets like other IPSs but many NBAs focus on higher-level details of communication sessions, such as source and destination IP addresses, ports used and the number of packets transmitted.
* **Wireless intrusion prevention systems (WIPS):** Monitors wireless network protocols for suspicious activity, like unauthorized users and devices accessing the company’s wifi. If a WIPS detects an unknown entity on a wireless network, it can terminate the connection. A WIPS can also help detect misconfigured or unsecured devices on a wifi network and intercept man-in-the-middle attacks, where a hacker secretly spies on users’ communications.

## 5. Setting up the Operating System

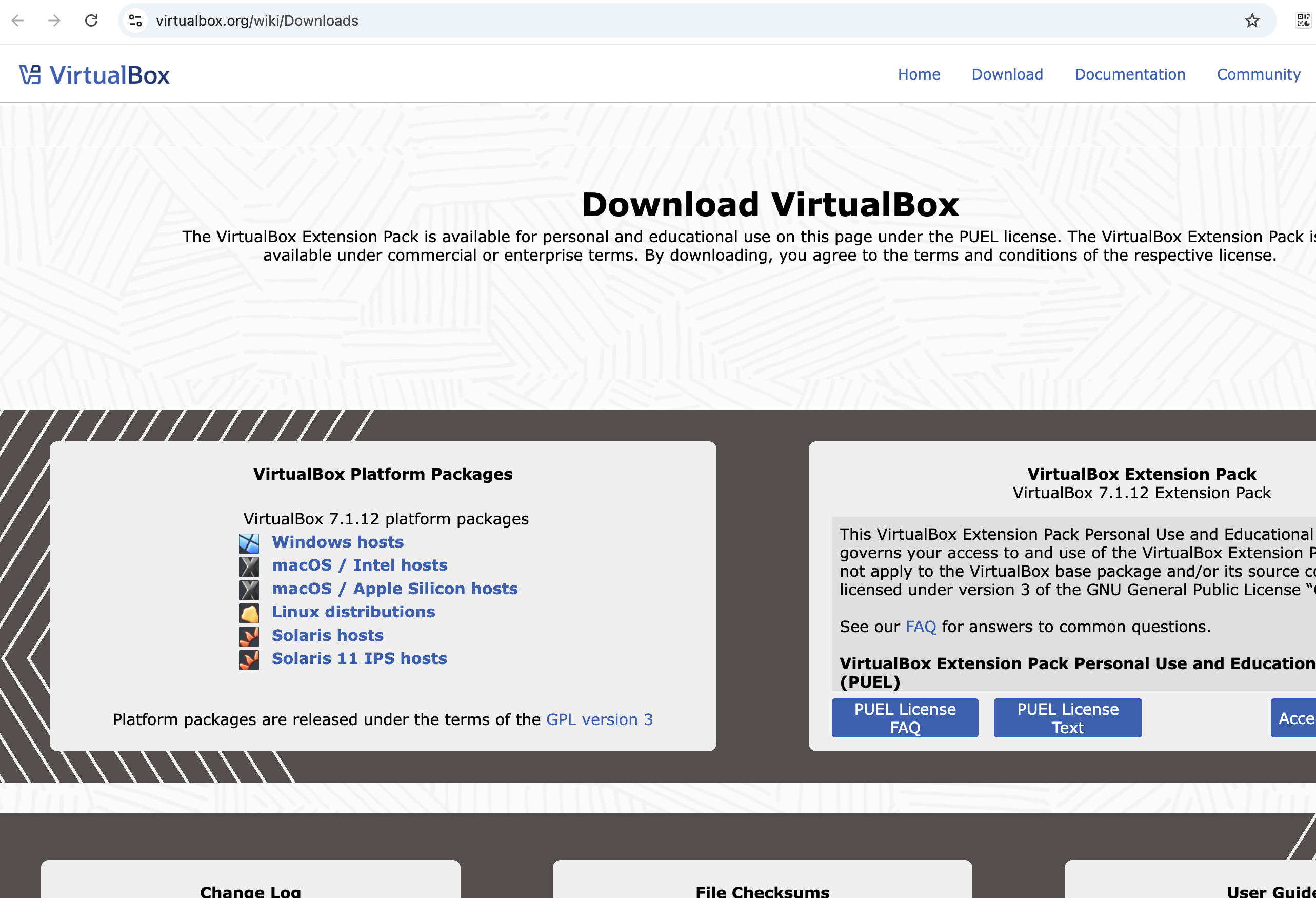
This section will guide you through the process of setting up your virtualized lab environment using VirtualBox and Kali Linux. This setup is crucial for hands-on practice in cybersecurity.

### 5.1 VirtualBox and Extension Pack Download and Installation

VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 3.

**Step 1: Download VirtualBox**

1. Open your web browser and navigate to the official VirtualBox downloads page: <https://www.virtualbox.org/wiki/Downloads>

* 
* VirtualBox Downloads Page

1. Under the “VirtualBox Platform Packages” section, click on the link corresponding to your host operating system. For Windows users, click on “Windows hosts”.

* [Windows Hosts Download Link](https://download.virtualbox.org/virtualbox/7.1.12/VirtualBox-7.1.12-169651-Win.exe)

**Step 2: Download VirtualBox Extension Pack**

1. On the same VirtualBox downloads page, scroll down to the “VirtualBox Extension Pack” section.
2. Click on the “All supported platforms” link to download the Extension Pack. This single package works for all supported platforms.

* **Important:** By downloading the Extension Pack, you agree to the terms and conditions of the Personal Use and Educational License (PUEL).
* [VirtualBox Extension Pack Download Link](https://download.virtualbox.org/virtualbox/7.1.12/Oracle_VirtualBox_Extension_Pack-7.1.12.vbox-extpack)

**Step 3: Install VirtualBox and Extension Pack**

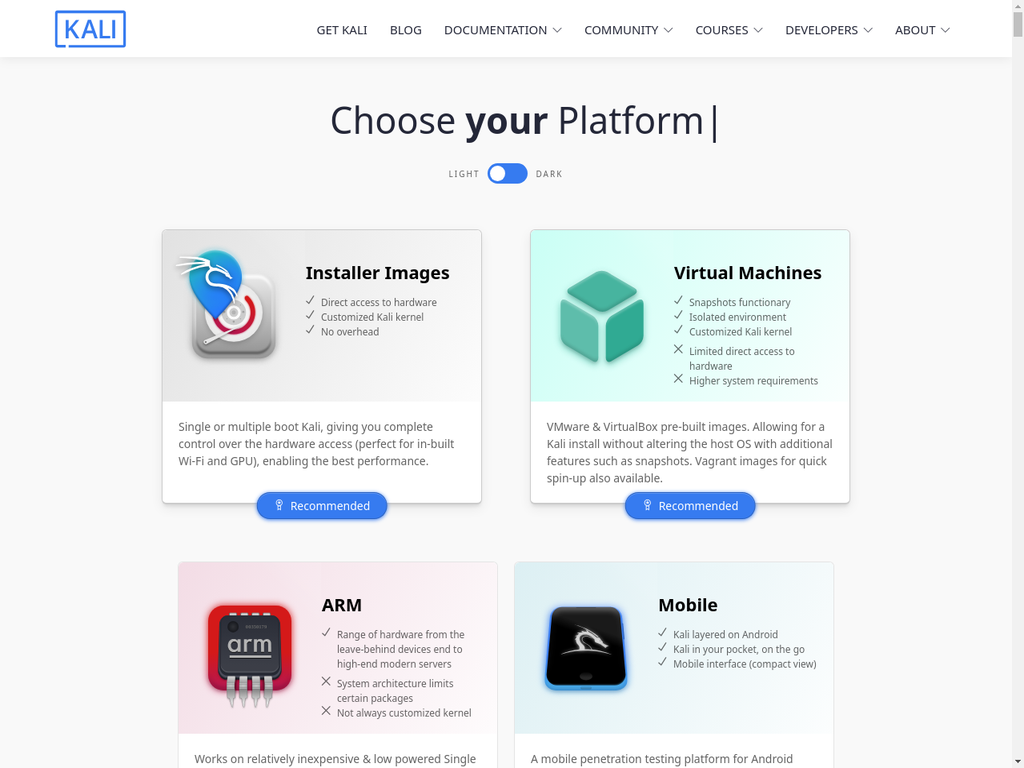
1. Run the downloaded VirtualBox installer and follow the on-screen instructions. The installation process is straightforward, typically involving clicking “Next” and accepting the default settings.
2. Once VirtualBox is installed, open it.
3. To install the Extension Pack, go to File > Tools > Extension Pack Manager in VirtualBox. Click on the “Install” button (usually a green plus sign) and select the downloaded Extension Pack file (.vbox-extpack). Accept the license agreement to complete the installation.

### 5.2 Kali Linux OVA Download and Installation

Kali Linux is a Debian-derived Linux distribution designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security.

**Step 1: Download Kali Linux OVA**

1. Open your web browser and go to the official Kali Linux download page: <https://www.kali.org/get-kali/>

* 
* [Kali Linux Download Page](https://old.kali.org/virtual-images/kali-2021.3/)

1. Scroll down to the “Pre-built Virtual Machines” section. Here you will find pre-built images for VMware & VirtualBox. Click on the “VirtualBox” link to download the OVA file.

[OVA File Link](https://old.kali.org/virtual-images/kali-2021.3/)

**Step 2: Import Kali Linux OVA into VirtualBox**

1. Open VirtualBox.
2. Go to File > Import Appliance...
3. Click the folder icon to browse and select the downloaded Kali Linux OVA file (.ova).
4. Click “Next” and review the appliance settings. You can adjust the allocated RAM and CPU cores if needed, but the default settings are usually sufficient to start.
5. Click “Import” and agree to the software license agreement.

* VirtualBox will now import the Kali Linux virtual machine. This process may take some time depending on your system’s performance.

**Step 3: Start Kali Linux and Login**

1. Once the import is complete, you will see the Kali Linux virtual machine listed in your VirtualBox Manager.
2. Select the Kali Linux VM and click the “Start” button (green arrow).
3. The Kali Linux VM will boot up. Once it reaches the login screen, the default credentials are:
   * **Username:** kali
   * **Password:** kali

* You can change these credentials later within the Kali Linux environment.

Your Kali Linux virtual machine is now set up and ready for use!