CS0424IT — LECTURE NOTES

CYBERSECURITY SPECIALIST

Simone La Porta

GitHub

Written in LaTeX

CONTENTS

1 INTRODUCTION

The Cybersecurity Specialist course aims to train professionals in the field of information security. These individuals will possess strong technical skills, providing added value to companies in the fight against cybercrime. The course is divided into three units:

1. **Unit 1** focuses on the theoretical prerequisites and technical skills necessary for an Ethical Hacker. It covers topics such as networking, operating systems, and an introduction to programming;

2. **Unit 2** centers on the phases of Penetration Testing, exploring the tools and techniques used by hackers in the real world;

3. **Unit 3** provides students with a comprehensive understanding of how to monitor security events, manage ongoing attacks, and adopt best practices at the enterprise level to minimize the impact on business activities.

In the past century, computing and the web were primarily the domain of experts, including hackers. The term *hacker*, often associated with digital piracy, encompasses three distinct types of hackers:

- **White Hat Hackers**, also known as "Ethical Hackers," operate with a strict adherence to ethical standards. Their work involves improving security with the consent of the system owner;

- **Grey Hat Hackers** operate in a legal and ethical gray area. They often act without the owner's permission but with the intent of improving security. While their actions can uncover vulnerabilities, they can also be controversial and sometimes illegal;

- **Black Hat Hackers** are criminals who break into computer networks with malicious intent. They may deploy malware to destroy files, steal information, hold computers hostage, or pilfer passwords, credit card numbers, and other personal data. Their motivations are typically opportunistic, such as financial gain. Stolen data is often sold on the dark web, where

items like credit card details, online payment system access, medical records, and even streaming service accounts are traded.

An Ethical Hacker is a cybersecurity expert capable of simulating cyber-attacks to identify potential vulnerabilities in a company's systems. These simulations, known as *Penetration Tests*, are crucial for detecting and fixing security issues in digital networks, software, and devices, thereby protecting enterprises and public entities from cybercriminal activities. Key responsibilities of an Ethical Hacker include:

- Conducting penetration tests on IT infrastructures and web applications;
- Ensuring the security of sensitive and private data, such as payment details, login credentials, and passwords.

It is crucial to emphasize that penetration testing should only be performed with the formal consent of the system or network owner. Conducting such tests without permission is illegal and can lead to severe legal consequences.

Part I

Unit 1: Fundamentals of Ethical Hacking

2 OPERATING SYSTEMS & PROGRAMMING LANGUAGES

Lecture 1 (4 hours)
3rd June 2024

A firewall is a crucial component in the realm of cybersecurity. It acts as a barrier that protects a network or system from external threats by managing and filtering incoming and outgoing network traffic. Essentially, a firewall serves as a gatekeeper between an internal network and the broader internet, analyzing network traffic and determining whether to allow or block data packets based on pre-established security rules.

2.1 *Key Classifications of Firewalls*

1. **Firewall Types by Implementation:**

    - **Hardware Firewalls:** These are physical devices dedicated to the task of network security. They are typically used by businesses and organizations with significant network traffic and complex security needs.

      Advantages: high performance due to dedicated resources, capable of handling large volumes of traffic, centralized security management.

      Disadvantages: higher cost and maintenance ,complexity in configuration and deployment.

    - **Software Firewalls:** These are programs installed on individual computers or servers. They provide a flexible and often more economical solution, especially for personal use or smaller networks.

      Advantages: cost-effective and easy to install, flexible and can be customized for specific needs, useful for personal devices and small businesses.

      Disadvantages: consumes system resources, which can affect performance, requires individual management on each device.

2. **Firewall Placement:**

    - **Perimeter Firewalls:** Positioned at the boundary of a network, perimeter firewalls are designed to safeguard the internal network from

external threats. They act as the first line of defense, regulating access between the internal network and the internet or other untrusted networks.

Advantages: provides a robust first line of defense, centralized point of security control for the entire network.

Disadvantages: cannot protect against threats that bypass the perimeter, such as internal attacks.

- **Host-based Firewalls:** These are installed on individual devices within the network. They monitor and control traffic to and from the device on which they are installed, providing an additional layer of security.

  Advantages: adds an extra layer of protection for individual devices, useful for controlling local traffic and internal threats.

  Disadvantages: requires installation and management on each individual device, potentially increases the complexity of the overall security infrastructure.

2.2 *Types of traffic filtering*

Firewalls implement various types of traffic filtering to control which data packets can pass through or be blocked. Each type of firewall and filtering mechanism offers different levels of security and control over the network traffic.

2.2.1 Static Packet Filtering

Static packet filtering is a type of network traffic filtering where decisions to permit or block traffic are based on static criteria, such as IP addresses, source and destination ports, and protocols.

- **Static Rules**: The firewall is configured with static rules created by the network administrator. These rules specify the criteria based on which the firewall evaluates the traffic.

- **Traffic Evaluation**: When the firewall receives a data packet, it compares the packet against the static rules. For example, it can check if the source and destination IP addresses are allowed, if the destination port is authorized, and if the protocol used is permitted.
- **Blocking or Permitting Decisions**: Based on these static rules, the firewall decides whether to permit or block the packet. If the packet matches the specified rules, it is allowed through; otherwise, it is blocked.

2.2.2 Stateful Filtering

Stateful filtering is an advanced type of filtering. Its distinguishing feature is the ability to track the state of network connections, enabling the firewall to make decisions based on contextual information about the connection.

- **Initiated Connections**: A stateful firewall keeps track of connections initiated from the internal network and allows outgoing traffic associated with these connections.
- **Established Connections**: After detecting an initial connection, the stateful firewall maintains a list of established connections. This list contains information such as source and destination IP addresses, ports, and the current state of the connection.
- **Subsequent Packets**: When the firewall receives subsequent packets that are part of a previously established connection, it compares them with the connection information and decides whether to permit or block them. For example, if a packet is part of an established connection, it will usually be permitted.

2.3 *Web Application Firewall (WAF)*

A Web Application Firewall (WAF) is a cybersecurity component specifically designed to protect web applications from various online threats and attacks. This tool focuses on the application layer, analyzing incoming and outgoing web traffic to identify and block suspicious or dangerous activities.

2.4 *Next-Generation Firewall (NGFW)*

A Next-Generation Firewall (NGFW) is an advanced cybersecurity solution that combines traditional firewall functions with other advanced features and deep traffic inspection capabilities to provide more sophisticated protection against cyber threats.

2.5 *Proxy*

A proxy, or proxy server, is an intermediary server between a client (e.g., a computer or device) and a server the client wants to access. The proxy acts as a middleman between the client and the destination server, forwarding the client's requests and returning responses from the server.

2.5.1 Functions of a Proxy

- **IP Address Hiding**: A proxy can hide the client's IP address from the destination server. When the client sends a request through the proxy, the proxy's IP address appears as the sender of the request to the server.

- **Content Filtering**: Some proxies are configured to filter traffic based on certain rules. For example, they can block access to specific websites or limit access to certain types of content.

- **Caching**: Proxies can locally store responses to client requests. This process allows the proxy to return responses to requests without having to forward them to the destination server, improving efficiency and speed.

- **Anonymity and Security**: Some proxies offer a degree of anonymity and security. For example, a proxy can hide the client's identity, making it more difficult for websites to track the user.

- **Remote Access**: Proxies can be used to allow remote access to internal network resources while protecting the security of the network.

2.5.2 Reverse Proxy

A reverse proxy is a type of proxy server that sits between client devices and a web server, handling requests from clients on behalf of the web server. It acts as an intermediary, forwarding client requests to the appropriate backend server and then returning the server's response to the client. Here is a detailed explanation of its functioning:

1. **Client Request Handling**:
    - When a client sends a request to access a web application or resource, the request is first received by the reverse proxy server instead of the actual web server.
    - The client perceives the reverse proxy as the actual server, not knowing that their request is being handled by an intermediary.
2. **Request Forwarding**:
    - The reverse proxy examines the client request and determines which backend server is best suited to handle the request. This determination can be based on various factors, such as load balancing policies, server health, or specific application logic.
    - After identifying the appropriate backend server, the reverse proxy forwards the client request to this server.
3. **Response Handling**:
    - Once the backend server processes the request, it sends the response back to the reverse proxy.
    - The reverse proxy then sends this response to the client, making it appear as though the response originated from the reverse proxy itself.
4. **Load Balancing**:

- One of the key functions of a reverse proxy is to distribute incoming client requests across multiple backend servers to ensure no single server becomes overwhelmed with traffic. This process is known as load balancing.
- Load balancing can be implemented using various algorithms, such as round-robin, least connections, or IP hash, to effectively distribute the traffic load.

5. **Caching**:

   - A reverse proxy can cache responses from backend servers. When subsequent requests for the same resource are received, the reverse proxy can serve the cached response instead of forwarding the request to the backend server, reducing latency and server load.

6. **SSL Termination**:

   - Reverse proxies often handle SSL termination, which involves decrypting incoming SSL/TLS connections and forwarding the decrypted requests to the backend servers. This offloads the encryption/decryption overhead from the backend servers, improving their performance.

7. **Security and Anonymity**:

   - Reverse proxies enhance security by hiding the identity and structure of the backend servers. Clients interact only with the reverse proxy, making it difficult for attackers to target the actual backend servers.
   - They can also implement additional security measures such as Web Application Firewall (WAF) functionality, filtering malicious requests, and protecting backend servers from attacks.

8. **Compression**:

   - Reverse proxies can compress responses from backend servers before sending them to clients. This reduces the amount of data transmitted

over the network, improving load times and reducing bandwidth usage.

9. **Monitoring and Logging**:

    - Reverse proxies can monitor and log traffic between clients and backend servers, providing valuable insights into performance, usage patterns, and potential security issues. These logs can be used for troubleshooting, capacity planning, and security auditing.

Overall, a reverse proxy acts as a mediator between clients and backend servers, enhancing performance, security, and scalability while simplifying the client-server interaction.

2.6 *Firewall Policies*

A firewall operates at various levels of the ISO/OSI model, providing diverse functionalities and security measures. The primary function of the firewall is to filter incoming or outgoing packets based on established rules known as firewall policies. These policies can filter packets based on:

- **Source or Destination IP Address**
- **Destination Protocol or Port**
- **Geolocation** (origin of the request)
- **Application Used**
- **Type of Client**

When a firewall inspects a packet, it can decide how to handle it with the following actions:

- **Allow**: The firewall lets the packet pass.
- **Drop**: The firewall discards the packet without sending any diagnostic message to the source.

- **Deny**: The firewall blocks the packet and informs the source.

These actions are specified in the firewall policies. For example, a policy might drop a packet directed to `google.com` on port 443 (HTTPS).

2.6.1 Top-Down Policy Application

Firewalls apply policies within the policy set using a top-down approach. For a given communication between a source and a destination, the firewall searches the policy set for a rule that manages the traffic. Once found, the firewall stops searching.

Source IP	Destination IP	Port	Action
192.168.1.15	10.10.10.10	443	DENY
192.168.1.24	10.11.11.12	80, 53	ACCEPT
192.168.23.40	10.10.11.11	0-1023	ACCEPT
192.168.23.40-41	192.168.33.54	443, 444, 445	DENY
10.10.10.0/24	Group-ip-microsoft	443, 1234, 998	DROP
Object-google-ip	10.10.10.0/24	High-ports-group	DENY
ANY	ANY	ANY	DENY

Policy Evaluation Example Consider the following example:

- The firewall intercepts a flow and examines the policy set to determine the appropriate action.
- It first checks the policy set's top rule. If it doesn't match the flow, the firewall moves to the next rule.
- If the third rule includes the traffic flow, the firewall handles the flow according to the "ACTION" parameter, allowing the traffic to pass ("ACCEPT").

2.6.2 Source and Destination IP Fields

The source and destination IP fields can include:

- Multiple IP addresses
- Subnets
- Groups / Objects

If the firewall does not find any rules that manage the flow, it discards the flow using a default rule. This rule, present in all policy sets and not modifiable, rejects all communications that do not match any other rule.

2.6.3 Default Rule Scenario

What happens if this default policy is placed at the top of the policy set?

If the default deny rule is the first rule evaluated by the firewall, all traffic will be blocked because it matches the "ANY ANY ANY DENY" rule. This setup would effectively prevent all communications through the firewall.

2.7 *Intrusion Detection and Prevention Systems*

2.7.1 Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a cybersecurity tool designed to detect and report suspicious activities or intrusions in networks or computer systems. It continuously monitors network traffic, system logs, and other events to identify anomalies that may indicate a security threat.

- **Traffic Analysis**: IDS analyzes network traffic or system logs to identify known attack signatures, anomalous behaviors, or policy violations.
- **Alert Generation**: When a potential threat is detected, IDS generates alerts or notifications for security administrators to take appropriate actions.
- **Passive System**: IDS does not take direct action to stop an attack; it only provides alerts.

2.7.2 Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is a cybersecurity tool that, unlike an IDS, can take active measures to block or prevent detected attacks. IPS operates in

real-time to immediately interrupt malicious or unwanted activities.

- **Real-Time Response**: IPS not only detects threats but also takes proactive actions to stop them, such as blocking suspicious traffic or disconnecting users.
- **Preventive Actions**: When a threat is detected, IPS can block traffic, issue alerts, or take other actions to prevent the attack from causing damage.
- **Active System**: The primary goal of IPS is to prevent cyber attacks from harming the system or network before any damage occurs. However, careful configuration is required to avoid false positives, which could block legitimate traffic.

2.8 *Network Zoning for Enhanced Security*

After discussing some network security devices, let's explore a commonly used technique to significantly enhance network security: zoning. This technique involves dividing the network into different zones.

2.8.1 Principle of Zoning

- **Application Area**: A zone dedicated to applications.
- **User PCs Area**: A zone dedicated to user PCs.
- **Admin PCs Area**: A zone dedicated to administrators' PCs.

Clearly, a network can have areas or zones that require higher levels of security due to their sensitivity.

2.8.2 Zoning Implementation

- **Segregation**: Networks are segmented into zones based on asset criticality and the required security level.
- **Security Levels**: Different zones have varying security measures, ensuring that sensitive areas have stricter controls.

2.9 *Multi-Tier DMZ Structure*

Cyber threats primarily originate from the internet, prompting many organizations to implement a multi-tier DMZ (Demilitarized Zone) network structure. This setup involves:

2.9.1 Multi-Tier DMZ Structure

- **Zone Division**: The network is divided into zones based on the criticality of assets on each segment.
- **Multiple Security Layers**: Additional security layers, such as firewalls, proxies, or other security devices, are added.

2.10 *Encryption: Meaning and Types*

2.10.1 What Does Encryption Mean?

Encryption refers to the process of converting data or a message into an unreadable or unintelligible format unless one possesses a specific key or method to decrypt it. The main goal of encryption is to protect sensitive or confidential information, making it inaccessible to unauthorized individuals. Encryption can be used for various purposes, including:

- **Communication Security**: To protect the privacy of online communications, such as during financial transactions or instant messaging, ensuring that only the authorized sender and recipient can read the message.
- **Data Storage Protection**: To secure data stored on devices like hard drives, USB flash drives, or servers, so that if someone physically accesses the data, they cannot read it without the correct access key.
- **Authentication and Digital Signatures**: To verify the authenticity of messages or digital documents and ensure they have not been altered during transmission or storage.
- **Protection of Trade Secrets**: In businesses, encryption is often used to protect trade secrets, customer data, and other sensitive information.

2.10.2 Main Approaches in Modern Encryption

There are two main approaches in modern computer encryption: symmetric key encryption and asymmetric key encryption.

SYMMETRIC KEY ENCRYPTION Symmetric key encryption is like a lock with a single key. Both the sender and recipient share the same secret key to encrypt and decrypt the data.

- **Encryption Process**: The sender uses the secret key to transform plaintext into an unreadable format.
- **Decryption Process**: The recipient uses the same secret key to decrypt the message and restore it to its original form.
- **Efficiency**: This method is fast and efficient but requires secure key management.

Symmetric Key Encryption Example Using AES:

1. **Preparation**:
    - **Plaintext Message**: "HELLO WORLD!"
    - **Secret Key**: "SECRETKEY123456"
2. **Encryption Process**:
    - **Algorithm**: AES uses multiple rounds of substitution, permutation, and combination.
    - **Combination**: Plaintext and secret key are combined through several rounds to generate ciphertext.
    - **Result**: Ciphertext is a seemingly random sequence of data.
3. **Decryption Process**:
    - **Secret Key**: The same key used for encryption.

- **Inverse Operations**: AES performs the inverse operations to restore plaintext from ciphertext.
- **Decrypted Message**: The original message "HELLO WORLD!" is obtained.

Asymmetric Key Encryption (Public/Private Key Encryption) Asymmetric key encryption, also known as public/private key encryption, involves two distinct keys that work complementarily to encrypt and decrypt data.

- **Public Key**:
  - Available publicly and can be distributed widely.
  - Each user has their own public key, which can be freely shared with others.
  - Used to encrypt data before sending it to a recipient.
- **Private Key**:
  - Kept secret and known only to the owner.
  - Used to decrypt data encrypted with the corresponding public key.
- **Digital Signatures**:
  - Used to create digital signatures, serving as an "electronic seal" that verifies the sender's authenticity and the integrity of the data.
  - The process includes key pair generation, document hashing, signing, and verification, as shown in Figure 1.

2.11 *What Is a VPN?*

A VPN, or Virtual Private Network, is a technology that creates a secure connection over the internet between your device and a remote server or between two devices.

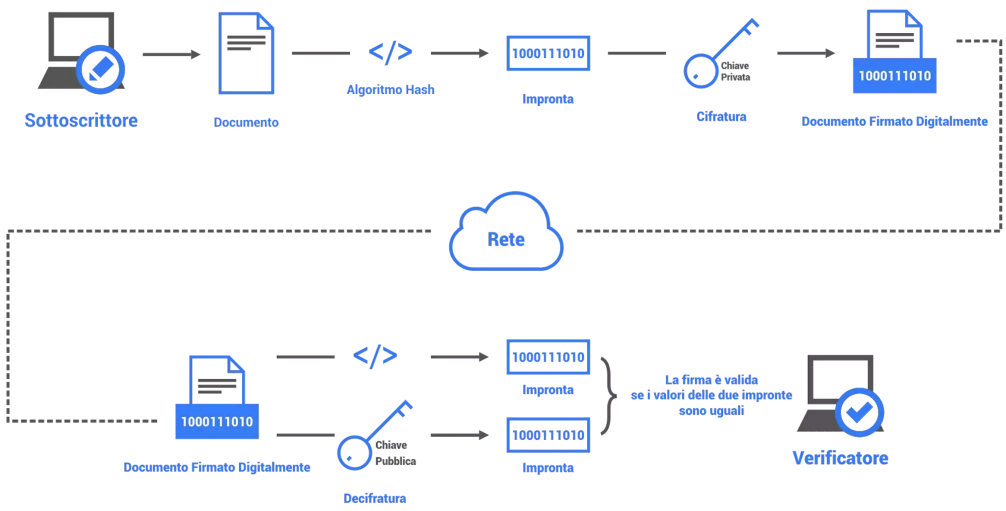

Figure 1: Digital signature schematics.

2.11.1 Main Functions of a VPN

- **Security**: Encrypts traffic between your device and the VPN server, ensuring intercepted data cannot be read or interpreted.
- **Privacy**: Hides your real IP address and geographic location, making it difficult for websites and online services to track your activity or location.
- **Access to Geo-Blocked Resources**: Allows you to choose a VPN server, enabling you to bypass geographic restrictions.
- **Public Network Security**: Protects you from potential attacks when connected to public Wi-Fi networks, such as in cafes or airports.

3 PYTHON FOR HACKERS AND WEB APPLICATIONS

4 BUILD WEEK 1: NETWORK SECURITY DESIGN

And this is a nice $$...$$ display environment:

$$\Delta v = \int_{t_0}^{t_1} a \, \mathrm{d}t$$

Maecenas ut nisi condimentum nisi iaculis porttitor eu sed metus. Proin faucibus aliquet odio, ac lobortis tortor. Mauris porta molestie tortor blandit pretium. Nulla pulvinar id mauris ut efficitur. Donec posuere tortor a odio pellentesque tincidunt. Nulla mi nunc, accumsan nec lectus ut, euismod vulputate libero. And finally we have the `align/align*` environment:

$$\begin{aligned} x_f - x_i &= \bar{v}t \\ \Rightarrow s &= \bar{v}t \end{aligned} \tag{1}$$

5 YET ANOTHER SECTION

5.1 *And a subsection beneath it*

Lecture 2 (1 hour)
13th June 2017

5.2 *And now a subsection*

5.2.1 With a subsubsection following it

Integer pharetra nulla scelerisque purus luctus iaculis. Mauris pulvinar erat non dui pretium, sed vestibulum sapien condimentum. Nam in urna quis sapien rhoncus placerat vitae sit amet odio. Vivamus finibus euismod nibh vestibulum lobortis. Integer arcu tortor, vestibulum sit amet iaculis ut, ullamcorper non ante. Pellentesque consectetur nec odio quis placerat. Vestibulum vehicula massa vel euismod blandit.

These ideas were probably discussed in lecture 1 in a parallel universe.

5.2.2 This subsubsection is all by itself

Table 2 courtesy of Mori, L.F. 'Tables in LaTeX2e: Packages and Methods'.

* * *

D (in)		P_u (lbs)	σ_N (psi)
5	test 1	285	38.00
	test 2	287	38.27
	test 3	230	30.67
10	test 1	430	28.67
	test 2	433	28.87
	test 3	431	28.73

Table 2: A table beautified by the booktabs package.