Phase 2 Group 3 Project:

Become a Security Sleuth: Build a Multi-Subnet Training Lab with Open Source Tools

Awa, Edgardo, Giovanni, Jaelin, Jasmine, Jesus, Takala

Long-term cost of cyber attacks

Reputation Damage:

Once news of a breach or attack spreads, stakeholders may lose trust in the affected company. Rebuilding this trust can take years and significant investment. Additionally, it can lead to decreased customer loyalty and a loss of competitive advantage.

Legal and Regulatory Costs:

Organizations may face lawsuits, and the cost can accumulate over time. Compliance requirements may also become more stringent, avoid future breaches and maintain regulatory compliance.

Intellectual Property Theft and Innovation Impact:

Stolen Intellectual Property (IP) can be used by competitors to replicate products or services. Protecting intellectual property through robust cybersecurity measures is essential for preserving a company's competitive edge and sustaining long-term success.

Purpose

01

This project builds a hands-on cybersecurity training lab using free and company tools. Participants will explore network security by segmenting the lab, deploying security tools, and launching simulated attacks. Findings will be shared, and the role of AWS in security will be discussed.

Setting up the Training Lab

Follow these steps to set up the multi-subnet training lab:

1. Determine the number of subnets needed based on the training requirements.
2. Set up the virtualization platform, where we used AWS to create our lab.
3. Create EC2 instances, ensuring that the network settings are configured correctly.
4. Install the required operating systems on each, such as Ubuntu or CentOS.
5. Configure the network settings for each instance, assigning the appropriate IP addresses and subnet masks.

Setting up the Training Lab Continue

Follow these steps to set up the multi-subnet training lab:

6. Set up EC2 instances and copy their IP addresses to individually identify them.
7. Install and configure the necessary security tools on each EC2, using kali, ubuntu
8. Test the connectivity between the instances to ensure proper network communication.
9. Document the lab setup and configurations for future reference.
10. Regularly update and maintain the training lab to ensure optimal performance and security.

Creation of Route Table and Association for Internet Gateway

Create a new route table

Create a new route table and associate it with the subnet that you want to route traffic out of the internet gateway (IGW).

Add a route

Add a route in the new route table with the destination CIDR block 0.0.0.0/0 and the target as the IGW.

Associate the route table

Associate the new route table with the subnet that you want to route traffic out of the IGW.

Verify connectivity

Verify connectivity by pinging an external IP address from an instance in the subnet. You should receive a response.

Components of Training Lab

METASPLOITABLE

Metasploitable is a virtual machine that is intentionally vulnerable to security attacks. It is commonly used for testing and learning purposes in the field of cybersecurity.

Purpose

Metasploitable allows security professionals and enthusiasts to practice and develop their skills in identifying vulnerabilities and conducting penetration testing in a secure, controlled environment.

Amazon EC2 (Elastic Compute Cloud)

Amazon EC2 is a web service for scalable cloud computing. It enables easy resource scaling and offers virtual servers, or instances, for diverse applications.

Key Features

- EC2 resources are scalable.
- Flexible: Choose from various instance types, OS, and software configurations.
- Ensures app security with encryption and network measures.
- Integrates with AWS services, for complex and scalable app development.

PRIVATE SUBNET– WITH METASPLOITABLE2, WAZUH, KALI SANDBOX

Private Subnet

❏ THE PRIVATE SUBNET PROVIDES A SECURE ENVIRONMENT FOR RUNNING SENSITIVE APPLICATIONS AND SERVICES.

❏ IT IS ISOLATED FROM THE PUBLIC INTERNET AND CAN ONLY BE ACCESSED THROUGH THE VPC'S INTERNAL NETWORK.

Metasploitable, WAZUH, and Kali Sandbox

❏ THE PRIVATE SUBNET INCLUDES INSTANCES OF METASPLOITABLE, WAZUH, AND KALI SANDBOX.

❏ THESE INSTANCES ARE USED FOR ETHICAL HACKING AND PENETRATION TESTING PURPOSES, ALLOWING SECURITY PROFESSIONALS TO IDENTIFY VULNERABILITIES AND STRENGTHEN THE NETWORK'S SECURITY.

Configuring Subnets and Network Segmentation

Configure Subnets
Implement Network Segmentation

Configure Subnets

- Determine the IP address range for each subnet.
- Assign unique IP addresses to devices within each subnet.
- Set up routing tables to allow communication between subnets.

Implement Network Segmentation

- Identify the different security zones or segments within the network.
- Set up access controls and firewall rules to restrict communication between segments.
- Implement VLANs or virtual networks to further isolate traffic.

Conclusion

MAIN POINTS:

- BUILDING A MULTI-SUBNET TRAINING LAB WITH OPEN SOURCE TOOLS PROVIDES A SECURE ENVIRONMENT FOR TRAINING AND TESTING.
- IT ALLOWS FOR REALISTIC SIMULATIONS OF REAL-WORLD SCENARIOS AND HELPS IMPROVE SECURITY SKILLS.
- OPEN SOURCE TOOLS OFFER FLEXIBILITY, COST-EFFECTIVENESS, AND A VIBRANT COMMUNITY FOR SUPPORT AND COLLABORATION.

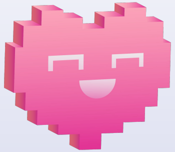
IMPORTANCE OF MULTI-SUBNET TRAINING LAB:

- A MULTI-SUBNET TRAINING LAB HELPS ORGANIZATIONS STAY AHEAD OF EMERGING SECURITY THREATS.
- IT ENABLES SECURITY PROFESSIONALS TO GAIN HANDS-ON EXPERIENCE AND DEVELOP EFFECTIVE STRATEGIES.
- BY USING OPEN SOURCE TOOLS, ORGANIZATIONS CAN REDUCE COSTS AND CUSTOMIZE THEIR TRAINING ENVIRONMENT.

TAKEAWAY:

- BUILDING A MULTI-SUBNET TRAINING LAB WITH OPEN SOURCE TOOLS IS ESSENTIAL FOR ENHANCING SECURITY SKILLS AND STAYING AHEAD IN THE EVER-EVOLVING THREAT LANDSCAPE.

Thanks!



CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**