**Experiment No-01**

Understand commonly implemented Extensible Authentication Protocols (EAP)

**Objective**

The purpose of this lab is to provide hands-on experience with some commonly implemented Extensible Authentication Protocols (EAP) used in network security. By the end of this lab, you should understand how EAP works and be able to configure and analyze different EAP methods.

**Required Tools**

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Linux (e.g., Ubuntu)
  + FreeRADIUS server installed on Linux VM
  + Windows client VM
* Wireshark for packet analysis
* Network simulator (optional, e.g., GNS3)

**EAP Methods Covered**

1. EAP-MD5
2. EAP-TLS
3. EAP-TTLS
4. PEAP

**Lab Setup**

1. **Network Configuration**
   * Set up a virtual network where the Linux VM acts as the RADIUS server.
   * Connect the Windows VM as a client to this network.
2. **Install and Configure FreeRADIUS on Linux VM**

bash

Copy code

sudo apt-get update

sudo apt-get install freeradius

* + Edit the FreeRADIUS configuration files:
    - /etc/freeradius/3.0/clients.conf
    - /etc/freeradius/3.0/users
    - /etc/freeradius/3.0/eap.conf

1. **Install Wireshark**

bash

Copy code

sudo apt-get install wireshark

**Procedure**

**Part 1: EAP-MD5**

1. **Configure FreeRADIUS for EAP-MD5**
   * Edit eap.conf to enable EAP-MD5:

plaintext

Copy code

eap {

default\_eap\_type = md5

}

* + Add a test user in the users file:

plaintext

Copy code

testuser Cleartext-Password := "password"

1. **Connect the Windows Client**
   * Configure the Windows client to use EAP-MD5 for authentication.
   * Attempt to connect to the network.
2. **Analyze with Wireshark**
   * Capture the authentication packets and analyze the EAP-MD5 exchange.
   * Identify the challenge and response mechanism.

**Part 2: EAP-TLS**

1. **Configure FreeRADIUS for EAP-TLS**
   * Enable EAP-TLS in eap.conf:

plaintext

Copy code

eap {

default\_eap\_type = tls

tls-config tls-common {

private\_key\_password = yourpassword

private\_key\_file = ${certdir}/server.key

certificate\_file = ${certdir}/server.pem

ca\_file = ${cadir}/ca.pem

}

}

* + Generate server and client certificates.

1. **Connect the Windows Client**
   * Install the client certificate on the Windows machine.
   * Configure the Windows client to use EAP-TLS for authentication.
   * Connect to the network.
2. **Analyze with Wireshark**
   * Capture the authentication packets and analyze the EAP-TLS exchange.
   * Observe the mutual authentication process.

**Part 3: EAP-TTLS**

1. **Configure FreeRADIUS for EAP-TTLS**
   * Enable EAP-TTLS in eap.conf:

plaintext

Copy code

eap {

default\_eap\_type = ttls

ttls {

default\_eap\_type = md5

}

}

1. **Connect the Windows Client**
   * Configure the Windows client to use EAP-TTLS for authentication.
   * Attempt to connect to the network.
2. **Analyze with Wireshark**
   * Capture the authentication packets and analyze the EAP-TTLS exchange.
   * Observe the tunneled authentication mechanism.

**Part 4: PEAP**

1. **Configure FreeRADIUS for PEAP**
   * Enable PEAP in eap.conf:

plaintext

Copy code

eap {

default\_eap\_type = peap

peap {

default\_eap\_type = mschapv2

}

}

1. **Connect the Windows Client**
   * Configure the Windows client to use PEAP for authentication.
   * Attempt to connect to the network.
2. **Analyze with Wireshark**
   * Capture the authentication packets and analyze the PEAP exchange.
   * Observe the encapsulated EAP within PEAP.

**Post-Lab Analysis**

1. Compare the security features of each EAP method.
2. Discuss the potential vulnerabilities and appropriate use cases for each EAP type.
3. Write a summary report on the findings from Wireshark captures.

**Conclusion**

By completing this lab, you should have a better understanding of different EAP methods, their configurations, and their operations within a network. This knowledge is essential for designing and maintaining secure network authentication systems.

**Experiment No-02**

Implement Public-Key Infrastructure with ISE

**Objective**

The goal of this lab is to provide hands-on experience in implementing Public-Key Infrastructure (PKI) using Cisco Identity Services Engine (ISE). By the end of this lab, you will understand how to configure ISE for PKI, including setting up a Certificate Authority (CA), generating certificates, and configuring ISE to use these certificates for secure authentication.

**Required Tools**

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Cisco ISE
  + Microsoft Windows Server with Active Directory Certificate Services (AD CS)
  + Windows client VM
* Cisco AnyConnect Secure Mobility Client (optional)
* Wireshark for packet analysis
* Network simulator (optional, e.g., GNS3)

**Lab Setup**

1. **Network Configuration**
   * Set up a virtual network where the Windows Server acts as the Certificate Authority (CA).
   * Connect the Cisco ISE and Windows client to this network.
2. **Install and Configure AD CS on Windows Server**
   * Install the Active Directory Certificate Services role.
   * Configure the CA.
   * Create and issue a certificate template for user and machine authentication.

**Procedure**

**Part 1: Configure AD CS**

1. **Install AD CS**
   * Open Server Manager and add the Active Directory Certificate Services role.
   * Configure AD CS as an Enterprise CA.
2. **Create Certificate Templates**
   * Open the Certification Authority console.
   * Duplicate the "User" template and configure it for client authentication.
   * Duplicate the "Workstation Authentication" template for machine authentication.
   * Publish these templates.

**Part 2: Configure Cisco ISE**

1. **Install Cisco ISE**
   * Deploy the Cisco ISE VM and complete the initial setup.
2. **Configure ISE for PKI**
   * Log in to the Cisco ISE admin interface.
   * Navigate to **Administration > System > Certificates > Certificate Signing Requests**.
   * Generate a certificate signing request (CSR) for the ISE node.
   * Export the CSR.
3. **Obtain and Install Certificates**
   * Submit the CSR to the AD CS to get it signed.
   * Import the CA certificate into ISE.
   * Import the signed certificate into ISE.
   * Mark the certificates as trusted for client authentication.

**Part 3: Configure ISE Authentication Policies**

1. **Configure Certificate Authentication Profile**
   * Navigate to **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile**.
   * Create a new profile for certificate-based authentication.
2. **Configure Authentication and Authorization Policies**
   * Navigate to **Policy > Policy Sets**.
   * Create a new policy set for EAP-TLS or PEAP with certificate-based authentication.
   * Define the authentication rules to use the Certificate Authentication Profile.
   * Define authorization rules based on user certificates.

**Part 4: Configure Windows Client**

1. **Enroll for a User Certificate**
   * Open the MMC console and add the Certificates snap-in for the current user.
   * Request a new certificate using the template configured in AD CS.
2. **Configure Network Connection**
   * Open Network and Sharing Center.
   * Configure the network connection to use EAP-TLS or PEAP.
   * Select the user certificate for authentication.

**Part 5: Testing and Verification**

1. **Connect the Windows Client**
   * Connect the Windows client to the network and attempt to authenticate using the configured certificate.
2. **Analyze with Wireshark**
   * Capture the authentication packets and analyze the EAP-TLS or PEAP exchange.
   * Verify that the certificates are being used for authentication.
3. **Monitor Cisco ISE Logs**
   * Navigate to **Operations > Authentications** in the Cisco ISE admin interface.
   * Verify the successful authentication attempts and analyze any failed attempts.

**Post-Lab Analysis**

1. **Review Security Features**
   * Discuss the benefits of using PKI for authentication.
   * Compare PKI-based authentication with other methods.
2. **Troubleshooting**
   * Identify common issues that can occur during PKI implementation and how to resolve them.
3. **Summary Report**
   * Write a summary report detailing the configuration steps, verification results, and any troubleshooting steps taken.

**Conclusion**

By completing this lab, you should have a solid understanding of how to implement PKI with Cisco ISE, including configuring a Certificate Authority, generating and managing certificates, and using these certificates for secure network authentication.

**Experiment No-03**

Understand and implement internal and external authentication databases

## Objective

The aim of this lab is to provide hands-on experience with both internal and external authentication databases. By the end of this lab, you should understand how to configure and use internal databases for authentication and how to integrate external databases, such as LDAP and RADIUS, for secure authentication in a network environment.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Linux (e.g., Ubuntu) for FreeRADIUS server
  + Windows Server with Active Directory (AD)
  + Windows client VM
* Cisco Identity Services Engine (ISE) or a similar network access control device (optional)
* Wireshark for packet analysis
* Network simulator (optional, e.g., GNS3)

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network where the Linux VM acts as a FreeRADIUS server.
   * Connect the Windows Server VM as an Active Directory (AD) server.
   * Connect the Windows client VM to this network.
2. **Install and Configure Required Software**
   * Install FreeRADIUS on the Linux VM.
   * Install Active Directory and configure Domain Services on the Windows Server VM.
   * Install Wireshark on the client machine.

## Procedure

### Part 1: Internal Authentication Database

#### Step 1: Configure Internal Database on FreeRADIUS

1. **Install FreeRADIUS**

bash

Copy code

sudo apt-get update

sudo apt-get install freeradius

1. **Configure Users in FreeRADIUS**
   * Edit the users file located at /etc/freeradius/3.0/users:

plaintext

Copy code

testuser Cleartext-Password := "password"

* + Add multiple users as required.

1. **Configure FreeRADIUS Clients**
   * Edit the clients.conf file located at /etc/freeradius/3.0/clients.conf:

plaintext

Copy code

client localhost {

ipaddr = 127.0.0.1

secret = testing123

}

1. **Start FreeRADIUS Service**

bash

Copy code

sudo systemctl start freeradius

sudo systemctl enable freeradius

#### Step 2: Test Internal Authentication

1. **Install and Configure radtest**

bash

Copy code

sudo apt-get install freeradius-utils

radtest testuser password 127.0.0.1 0 testing123

1. **Verify Authentication**
   * Use Wireshark to capture and analyze the RADIUS packets.
   * Ensure the authentication is successful.

### Part 2: External Authentication Database (LDAP and Active Directory)

#### Step 1: Configure LDAP/Active Directory

1. **Install and Configure Active Directory**
   * On Windows Server VM, install Active Directory Domain Services.
   * Promote the server to a Domain Controller.
2. **Create Users in Active Directory**
   * Open Active Directory Users and Computers.
   * Create a test user (e.g., aduser) with a password.

#### Step 2: Integrate FreeRADIUS with Active Directory

1. **Install LDAP Module for FreeRADIUS**

bash

Copy code

sudo apt-get install freeradius-ldap

1. **Configure LDAP Module in FreeRADIUS**
   * Edit the mods-available/ldap file:

plaintext

Copy code

ldap {

server = "ldap://your\_ad\_server\_ip"

identity = "CN=Administrator,CN=Users,DC=yourdomain,DC=com"

password = yourpassword

base\_dn = "CN=Users,DC=yourdomain,DC=com"

filter = "(sAMAccountName=%{%{Stripped-User-Name}:-%{User-Name}})"

start\_tls = yes

tls {

ca\_file = /etc/ssl/certs/ca-certificates.crt

require\_cert = "allow"

}

}

1. **Enable LDAP Module**

bash

Copy code

sudo ln -s /etc/freeradius/3.0/mods-available/ldap /etc/freeradius/3.0/mods-enabled/

1. **Update Default Configuration to Use LDAP**
   * Edit the sites-available/default file and add ldap to the authorize section.
2. **Restart FreeRADIUS Service**

bash

Copy code

sudo systemctl restart freeradius

#### Step 3: Test External Authentication

1. **Test LDAP Authentication Using radtest**

bash

Copy code

radtest aduser password 127.0.0.1 0 testing123

1. **Verify Authentication**
   * Use Wireshark to capture and analyze the RADIUS packets.
   * Ensure the authentication is successful through LDAP/AD.

### Part 3: Cisco ISE Integration (Optional)

#### Step 1: Configure Cisco ISE for Internal Database

1. **Add Internal Users in ISE**
   * Navigate to **Administration > Identity Management > Identities**.
   * Add users with appropriate credentials.
2. **Configure Authentication Policies**
   * Navigate to **Policy > Policy Sets**.
   * Define authentication policies using the internal user database.

#### Step 2: Configure Cisco ISE for External Database

1. **Add External Identity Source**
   * Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.
   * Connect and join the AD domain.
2. **Configure Authentication Policies**
   * Navigate to **Policy > Policy Sets**.
   * Define authentication policies using the AD identity source.

### Part 4: Testing and Verification

1. **Test Internal Authentication with Cisco ISE**
   * Connect a client and authenticate using internal ISE database.
   * Verify successful authentication in ISE logs.
2. **Test External Authentication with Cisco ISE**
   * Connect a client and authenticate using AD credentials.
   * Verify successful authentication in ISE logs.
3. **Analyze with Wireshark**
   * Capture authentication packets to analyze the flow of authentication requests and responses.

## Post-Lab Analysis

1. **Review Authentication Methods**
   * Discuss the advantages and disadvantages of internal versus external authentication databases.
   * Identify potential use cases for each method.
2. **Troubleshooting**
   * Identify common issues encountered during configuration and how to resolve them.
3. **Summary Report**
   * Write a summary report detailing the configuration steps, verification results, and any troubleshooting steps taken.

## Conclusion

By completing this lab, you should have a solid understanding of how to configure and use both internal and external authentication databases for secure network authentication. This knowledge is essential for designing and maintaining robust authentication systems in a network environment.

**Experiment No-04**

Implement Web Authentication and Guest Access

## Objective

The goal of this lab is to provide hands-on experience in implementing web authentication and guest access using Cisco Identity Services Engine (ISE). By the end of this lab, you will understand how to configure ISE for web authentication and guest access, create guest user accounts, and customize the guest portal.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Cisco ISE
  + Windows Server with Active Directory (optional for AD integration)
  + Windows client VM
* Cisco switch or wireless LAN controller (WLC) (optional)
* Wireshark for packet analysis
* Network simulator (optional, e.g., GNS3)

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network where the Cisco ISE, Windows Server, and Windows client VM are connected.
   * Ensure the network allows communication between the ISE server and the client devices.
2. **Install and Configure Cisco ISE**
   * Deploy the Cisco ISE VM and complete the initial setup.
   * Ensure that the ISE server is reachable from the client machine.

## Procedure

### Part 1: Configure Cisco ISE for Web Authentication

#### Step 1: Basic Setup of Cisco ISE

1. **Initial Setup**
   * Log in to the Cisco ISE admin interface.
   * Navigate to **Administration > System > Settings > Network Devices**.
   * Add the network devices (e.g., switch or WLC) that will redirect traffic to ISE for web authentication.
2. **Configure Network Device Profile**
   * Navigate to **Administration > Network Resources > Network Device Profiles**.
   * Ensure that the appropriate profile is selected for the network devices (e.g., Cisco Switch, WLC).

#### Step 2: Configure ISE for Web Authentication

1. **Enable Web Authentication**
   * Navigate to **Administration > System > Deployment**.
   * Select the ISE node and enable the **Policy Service** and **Guest Services**.
2. **Create a New Policy Set**
   * Navigate to **Policy > Policy Sets**.
   * Create a new policy set for web authentication.
   * Define the conditions for web authentication (e.g., using the default network access policy).
3. **Configure Authentication Policies**
   * Within the new policy set, define the authentication policies for web authentication.
   * Use the internal user database or an external identity source if required.
4. **Configure Authorization Policies**
   * Define authorization rules to redirect unauthenticated users to the web portal.
   * Set up rules to allow access for authenticated users.

### Part 2: Configure Guest Access

#### Step 1: Create Guest User Accounts

1. **Guest User Management**
   * Navigate to **Guest Access > Manage Accounts**.
   * Create a new guest user account.
   * Set the account details such as username, password, and validity period.

#### Step 2: Customize Guest Portal

1. **Guest Portal Settings**
   * Navigate to **Guest Access > Configure > Portals & Components > Guest Portals**.
   * Create a new guest portal or modify an existing one.
   * Customize the portal appearance, login page, and guest account creation settings.
2. **Portal Configuration**
   * Define the URL redirection settings and portal behavior.
   * Configure the guest self-registration and sponsor approval settings if needed.

### Part 3: Test Web Authentication and Guest Access

#### Step 1: Test Web Authentication

1. **Connect Client to Network**
   * Connect the Windows client VM to the network where web authentication is configured.
2. **Redirect to Web Portal**
   * Open a web browser on the client VM and try to access any HTTP website.
   * Verify that the client is redirected to the ISE web authentication portal.
3. **Authenticate User**
   * Log in using the credentials configured in the ISE internal user database or an external identity source.
   * Verify successful authentication and network access.

#### Step 2: Test Guest Access

1. **Guest User Login**
   * Open a web browser on the client VM and try to access any HTTP website.
   * Verify that the client is redirected to the guest portal.
2. **Guest Account Creation**
   * Use the guest account created earlier to log in.
   * If self-registration is enabled, create a new guest account and log in.
3. **Monitor ISE Logs**
   * Navigate to **Operations > Authentications** in the Cisco ISE admin interface.
   * Verify the successful guest user login attempts and analyze any failed attempts.

### Part 4: Analyze with Wireshark

1. **Capture Authentication Packets**
   * Use Wireshark on the client VM to capture and analyze the HTTP and HTTPS packets during web authentication and guest access.
2. **Verify Authentication Process**
   * Ensure that the redirection, authentication, and authorization processes are working as expected.

## Post-Lab Analysis

1. **Review Authentication Methods**
   * Discuss the advantages and disadvantages of web authentication and guest access.
   * Identify potential use cases for each method.
2. **Troubleshooting**
   * Identify common issues encountered during configuration and how to resolve them.
3. **Summary Report**
   * Write a summary report detailing the configuration steps, verification results, and any troubleshooting steps taken.

## Conclusion

By completing this lab, you should have a solid understanding of how to implement web authentication and guest access using Cisco ISE. This knowledge is essential for designing and maintaining secure guest access solutions in a network environment.

**Experiment No-05**

Designing and deploying Threat Defense solutions on a ASA utilizing access policy and application and identity based inspection

## Objective

The aim of this lab is to provide hands-on experience in designing and deploying threat defense solutions on a Cisco ASA. By the end of this lab, you should understand how to configure access policies, and application and identity-based inspection to enhance network security.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Cisco ASA device or ASA virtual appliance (ASAv)
* Cisco ASDM (Adaptive Security Device Manager) or CLI access to ASA
* Windows Server with Active Directory (optional for identity-based inspection)
* Windows client VM
* Network simulator (optional, e.g., GNS3)

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network where the Cisco ASA, Windows Server, and Windows client VM are connected.
   * Ensure the network allows communication between the ASA and the client devices.
2. **Install and Configure Cisco ASA**
   * Deploy the Cisco ASA device or ASAv and complete the initial setup.
   * Ensure that ASDM or CLI access to the ASA is configured and accessible.

## Procedure

### Part 1: Basic ASA Configuration

#### Step 1: Initial Configuration of ASA

1. **Basic Setup**
   * Access the ASA via CLI or ASDM.
   * Configure the inside and outside interfaces with appropriate IP addresses.

Example CLI commands:

shell

Copy code

interface GigabitEthernet0/0

nameif outside

security-level 0

ip address 192.168.1.1 255.255.255.0

interface GigabitEthernet0/1

nameif inside

security-level 100

ip address 10.0.0.1 255.255.255.0

1. **Configure NAT**
   * Set up Network Address Translation (NAT) for internal to external traffic.

Example CLI commands:

shell

Copy code

object network obj\_any

subnet 0.0.0.0 0.0.0.0

nat (inside,outside) dynamic interface

### Part 2: Configure Access Policies

#### Step 1: Define Access Control Lists (ACLs)

1. **Create ACLs**
   * Define ACLs to control traffic between different network segments.

Example CLI commands:

shell

Copy code

access-list OUTSIDE\_IN extended permit tcp any object-group WEB\_SERVERS eq 80

access-list OUTSIDE\_IN extended permit tcp any object-group WEB\_SERVERS eq 443

access-group OUTSIDE\_IN in interface outside

1. **Apply ACLs**
   * Apply the ACLs to the appropriate interfaces to enforce the access policies.

### Part 3: Application-Based Inspection

#### Step 1: Enable Application Inspection

1. **Configure Application Inspection**
   * Enable application inspection for protocols like HTTP, FTP, DNS, etc.

Example CLI commands:

shell

Copy code

policy-map global\_policy

class inspection\_default

inspect http

inspect ftp

inspect dns

1. **Verify Inspection Configuration**
   * Ensure that application inspection is enabled and properly configured.

### Part 4: Identity-Based Inspection

#### Step 1: Integrate with Active Directory

1. **Configure Identity Options**
   * Set up identity options to integrate the ASA with Active Directory for identity-based inspection.
2. **Configure LDAP Server**
   * Define the LDAP server and configure the ASA to use it for user authentication.

Example CLI commands:

shell

Copy code

ldap attribute-map map1

map-name sAMAccountName IETF-Radius-User-Name

aaa-server AD\_SERVER protocol ldap

aaa-server AD\_SERVER (inside) host 10.0.0.10

ldap-base-dn DC=yourdomain,DC=com

ldap-scope subtree

ldap-naming-attribute sAMAccountName

ldap-login-password yourpassword

ldap-login-dn CN=Administrator,CN=Users,DC=yourdomain,DC=com

#### Step 2: Configure Identity-Based Policies

1. **Define Identity-Based Rules**
   * Create identity-based rules to control access based on user identity.

Example CLI commands:

shell

Copy code

access-list IDENTITY\_ACL extended permit ip any any

access-group IDENTITY\_ACL in interface inside

1. **Apply Policies**
   * Apply the identity-based policies to the relevant interfaces or contexts.

### Part 5: Testing and Verification

#### Step 1: Test Access Policies

1. **Verify ACL Functionality**
   * Test access to services and ensure that the ACLs are working as intended.
   * Use a client machine to attempt connections to various services and verify that the connections adhere to the ACLs.

#### Step 2: Test Application Inspection

1. **Verify Application Inspection**
   * Test application-specific traffic (e.g., HTTP, FTP) to ensure it is being inspected and managed correctly.
   * Use tools like web browsers and FTP clients to generate traffic and verify the inspection logs.

#### Step 3: Test Identity-Based Inspection

1. **Verify Identity-Based Rules**
   * Test identity-based access by logging in with different user accounts.
   * Ensure that access is granted or denied based on the identity of the user.
   * Monitor the ASA logs to see the identity-based decisions.

### Part 6: Analyze with Wireshark

1. **Capture Traffic**
   * Use Wireshark on the client VM to capture and analyze traffic.
   * Verify that the traffic conforms to the configured access policies and inspections.
2. **Inspect Packet Details**
   * Analyze the packet captures to ensure that application and identity-based inspections are working as expected.

## Post-Lab Analysis

1. **Review Configuration**
   * Discuss the benefits of application and identity-based inspections.
   * Identify any potential weaknesses or areas for improvement in the configuration.
2. **Troubleshooting**
   * Identify common issues encountered during configuration and how to resolve them.
3. **Summary Report**
   * Write a summary report detailing the configuration steps, verification results, and any troubleshooting steps taken.

## Conclusion

By completing this lab, you should have a solid understanding of how to design and deploy threat defense solutions on a Cisco ASA using access policies and application and identity-based inspection. This knowledge is essential for enhancing network security and ensuring controlled access to network resources.

**Experiment No-06**

Describe the various VPN technologies and deployments as well as the cryptographic algorithms and protocols that provide VPN security

## Objective

The aim of this lab is to provide hands-on experience with various VPN technologies, deployments, and the cryptographic algorithms and protocols that ensure VPN security. By the end of this lab, you should understand how to configure and deploy different types of VPNs and how cryptographic algorithms and protocols secure VPN communications.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Linux (e.g., Ubuntu) for OpenVPN server
  + Windows Server for SSTP and L2TP/IPsec VPN
  + Windows client VM
* Cisco ASA device or ASAv for site-to-site and remote access VPNs (optional)
* Network simulator (optional, e.g., GNS3)

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network where the VPN servers and client VMs are connected.
   * Ensure the network allows communication between the VPN servers and client devices.
2. **Install and Configure VPN Servers**
   * Deploy the necessary VMs and complete the initial setup for each VPN server.

## Procedure

### Part 1: Understanding VPN Technologies

#### Step 1: Overview of VPN Types

1. **Remote Access VPN**
   * Provides secure remote access to an organization's internal network.
   * Example technologies: SSL VPN, SSTP, L2TP/IPsec.
2. **Site-to-Site VPN**
   * Connects entire networks to each other over the internet securely.
   * Example technologies: IPsec VPN, DMVPN, GRE over IPsec.
3. **Client-to-Site VPN**
   * Individual clients connect securely to a remote site.
   * Example technologies: SSL VPN, IPsec VPN.

### Part 2: Cryptographic Algorithms and Protocols

#### Step 1: Overview of Cryptographic Concepts

1. **Symmetric Encryption**
   * Uses the same key for encryption and decryption.
   * Example algorithms: AES, DES, 3DES.
2. **Asymmetric Encryption**
   * Uses a pair of keys: a public key for encryption and a private key for decryption.
   * Example algorithms: RSA, ECC.
3. **Hashing**
   * Produces a fixed-size hash value from data input.
   * Example algorithms: MD5, SHA-1, SHA-2.
4. **Integrity and Authentication**
   * Ensures data is not tampered with and authenticates the data source.
   * Example protocols: HMAC, digital signatures.
5. **Key Exchange**
   * Securely exchanges cryptographic keys between parties.
   * Example protocols: Diffie-Hellman, IKE.

### Part 3: Deploying VPN Technologies

#### Step 1: OpenVPN Deployment (SSL VPN)

1. **Install OpenVPN on Linux**

bash

Copy code

sudo apt-get update

sudo apt-get install openvpn easy-rsa

1. **Configure OpenVPN Server**
   * Generate server keys and certificates using Easy-RSA.
   * Edit the OpenVPN server configuration file (/etc/openvpn/server.conf).
2. **Start OpenVPN Server**

bash

Copy code

sudo systemctl start openvpn@server

sudo systemctl enable openvpn@server

1. **Configure OpenVPN Client**
   * Generate client keys and certificates.
   * Configure the OpenVPN client configuration file.
2. **Connect to OpenVPN Server**
   * Use the OpenVPN client to connect to the server and verify the connection.

#### Step 2: SSTP Deployment (Windows Server)

1. **Install Remote Access Role on Windows Server**
   * Open Server Manager and add the Remote Access role.
   * Configure the Routing and Remote Access service.
2. **Configure SSTP VPN**
   * Set up SSL certificates for SSTP.
   * Configure VPN properties and allow SSTP connections.
3. **Configure VPN Client on Windows**
   * Add a new VPN connection on the Windows client.
   * Connect to the SSTP VPN and verify the connection.

#### Step 3: L2TP/IPsec Deployment (Windows Server)

1. **Configure L2TP/IPsec on Windows Server**
   * Enable L2TP/IPsec on the Routing and Remote Access service.
   * Configure IPsec settings and pre-shared keys.
2. **Configure VPN Client on Windows**
   * Add a new VPN connection using L2TP/IPsec.
   * Connect to the VPN and verify the connection.

#### Step 4: IPsec Site-to-Site VPN (Cisco ASA)

1. **Configure IPsec VPN on Cisco ASA**
   * Define IKE policies and IPsec transform sets.
   * Configure the VPN tunnel group and create the crypto map.

Example CLI commands:

shell

Copy code

crypto ikev1 policy 10

authentication pre-share

encryption aes

hash sha

group 2

lifetime 86400

crypto ipsec ikev1 transform-set MY\_TRANSFORM esp-aes esp-sha-hmac

crypto map MY\_MAP 10 ipsec-isakmp

set peer 192.168.2.1

set transform-set MY\_TRANSFORM

match address VPN\_ACL

access-list VPN\_ACL extended permit ip 10.0.0.0 255.255.255.0 192.168.2.0 255.255.255.0

tunnel-group 192.168.2.1 type ipsec-l2l

tunnel-group 192.168.2.1 ipsec-attributes

ikev1 pre-shared-key mysecretkey

1. **Configure IPsec VPN on Remote ASA**
   * Mirror the configuration on the remote ASA device.
2. **Verify the VPN Connection**
   * Check the tunnel status and ensure traffic is encrypted.

### Part 4: Testing and Verification

#### Step 1: Test VPN Connections

1. **Verify OpenVPN Connection**
   * Connect the OpenVPN client and check the connection status.
2. **Verify SSTP Connection**
   * Connect the SSTP client and check the connection status.
3. **Verify L2TP/IPsec Connection**
   * Connect the L2TP/IPsec client and check the connection status.
4. **Verify IPsec Site-to-Site Connection**
   * Ensure the site-to-site tunnel is up and passing traffic.

#### Step 2: Analyze with Wireshark

1. **Capture VPN Traffic**
   * Use Wireshark on the client and server sides to capture VPN traffic.
2. **Verify Encryption**
   * Inspect the packet captures to ensure the traffic is encrypted and secure.

### Part 5: Post-Lab Analysis

#### Step 1: Review VPN Technologies

1. **Discuss Use Cases**
   * Analyze the advantages and disadvantages of each VPN technology.
   * Identify scenarios where each type of VPN would be appropriate.
2. **Security Considerations**
   * Discuss the security benefits provided by each cryptographic algorithm and protocol.
   * Identify potential vulnerabilities and how to mitigate them.

#### Step 2: Troubleshooting

1. **Common Issues**
   * Identify common issues encountered during VPN setup and how to resolve them.
2. **Debugging Tools**
   * Use tools like ping, traceroute, and VPN-specific logs for troubleshooting.

#### Step 3: Summary Report

1. **Documentation**
   * Write a summary report detailing the configuration steps, verification results, and any troubleshooting steps taken.

## Conclusion

By completing this lab, you should have a solid understanding of various VPN technologies and the cryptographic protocols that secure them. This knowledge is essential for designing and deploying secure VPN solutions in a network environment.

**Experiment No-07**

Describe and implement Email Security Appliance

## Objective

The aim of this lab is to provide hands-on experience with understanding and implementing an Email Security Appliance (ESA). By the end of this lab, you should be able to configure and manage an ESA to secure email communications, filter spam, and protect against email-based threats.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Cisco Email Security Appliance (ESA) virtual appliance
* Windows Server with Active Directory (optional for LDAP integration)
* Windows client VM
* Email client software (e.g., Outlook, Thunderbird)

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network where the Cisco ESA, Windows Server, and Windows client VM are connected.
   * Ensure the network allows communication between the ESA and the client devices.
2. **Install and Configure Cisco ESA**
   * Deploy the Cisco ESA virtual appliance and complete the initial setup.
   * Ensure that the ESA is accessible from the client machine for management purposes.

## Procedure

### Part 1: Initial Configuration of Cisco ESA

#### Step 1: Basic Setup

1. **Access the ESA**
   * Access the ESA management interface via a web browser using the default IP address.
   * Log in with the default credentials (admin/admin) and change the password.
2. **Network Configuration**
   * Configure the IP settings for the ESA to match your network configuration.
   * Ensure the ESA has proper DNS and NTP settings.
3. **License and Update**
   * Apply the appropriate licenses for the ESA.
   * Update the ESA to the latest version using the **System Administration > Upgrade** menu.

### Part 2: Configuring Mail Policies

#### Step 1: Configure Incoming Mail Policies

1. **Add Mail Policies**
   * Navigate to **Mail Policies > Incoming Mail Policies**.
   * Create policies to define how incoming emails are processed.
2. **Anti-Spam and Anti-Virus**
   * Enable and configure anti-spam and anti-virus scanning for incoming emails.
   * Use the default anti-spam engine or enable additional engines if licensed.
3. **Content Filters**
   * Create content filters to scan incoming emails for specific content.
   * Define actions for detected content, such as quarantine or deletion.

#### Step 2: Configure Outgoing Mail Policies

1. **Add Mail Policies**
   * Navigate to **Mail Policies > Outgoing Mail Policies**.
   * Create policies to define how outgoing emails are processed.
2. **Data Loss Prevention (DLP)**
   * Enable and configure DLP policies to prevent sensitive information from being sent out.
   * Use predefined DLP policies or create custom ones.
3. **Encryption**
   * Configure email encryption settings for outgoing emails to ensure secure transmission.
   * Enable TLS for outgoing email communications.

### Part 3: User and Domain Management

#### Step 1: Configure Domains

1. **Add Accepted Domains**
   * Navigate to **Network > Domains**.
   * Add the domains for which the ESA will accept and process emails.
2. **Routing**
   * Configure email routing settings for the accepted domains.
   * Define mail routes to internal mail servers.

#### Step 2: Integrate with LDAP

1. **Configure LDAP Settings**
   * Navigate to **System Administration > LDAP**.
   * Add LDAP server details to integrate the ESA with Active Directory.
2. **LDAP Queries**
   * Create LDAP queries to fetch user and group information for email policies.
   * Test the LDAP integration to ensure it is working correctly.

### Part 4: Monitoring and Reporting

#### Step 1: Monitor Email Traffic

1. **Mail Logs**
   * Navigate to **Monitoring > Mail Logs**.
   * Review the logs to monitor incoming and outgoing email traffic.
2. **Message Tracking**
   * Use the **Message Tracking** tool to search for specific emails.
   * Analyze the delivery status and actions taken on emails.

#### Step 2: Generate Reports

1. **Scheduled Reports**
   * Navigate to **Monitoring > Scheduled Reports**.
   * Create and schedule reports to get regular updates on email security status.
2. **On-Demand Reports**
   * Generate on-demand reports to get insights into specific aspects of email security.
   * Review reports for spam, virus, and policy violations.

### Part 5: Testing and Verification

#### Step 1: Test Email Filtering

1. **Send Test Emails**
   * Send test emails from external and internal accounts to the domains configured on the ESA.
   * Verify that the emails are processed according to the incoming and outgoing mail policies.
2. **Check Spam and Virus Filtering**
   * Send emails containing spam-like content and known test viruses (e.g., EICAR test file).
   * Verify that the ESA correctly identifies and handles these emails.

#### Step 2: Test LDAP Integration

1. **User Policies**
   * Test user-specific policies by sending emails to users in the LDAP directory.
   * Verify that the policies are correctly applied based on LDAP information.
2. **Group Policies**
   * Test group-specific policies by sending emails to groups defined in LDAP.
   * Ensure that the group policies are enforced correctly.

### Part 6: Troubleshooting and Maintenance

#### Step 1: Common Issues

1. **Email Delivery Problems**
   * Check the mail logs for errors related to email delivery.
   * Verify DNS and routing configurations.
2. **Policy Misconfiguration**
   * Review the mail policies to ensure they are correctly configured.
   * Check for conflicts or overlaps in policy rules.

#### Step 2: Maintenance

1. **Regular Updates**
   * Ensure the ESA is regularly updated with the latest anti-spam and anti-virus definitions.
   * Apply software updates and patches as they become available.
2. **Backup and Restore**
   * Regularly back up the ESA configuration.
   * Test the backup and restore process to ensure it works as expected.

## Post-Lab Analysis

#### Step 1: Review Configuration

1. **Discuss Configurations**
   * Review the configurations made during the lab.
   * Discuss the rationale behind each configuration decision.
2. **Security Benefits**
   * Discuss the security benefits provided by the ESA.
   * Identify any potential improvements or additional features to be configured.

#### Step 2: Summary Report

1. **Documentation**
   * Write a summary report detailing the configuration steps, verification results, and any troubleshooting steps taken.

## Conclusion

By completing this lab, you should have a solid understanding of how to configure and manage an Email Security Appliance (ESA) to secure email communications, filter spam, and protect against email-based threats. This knowledge is essential for maintaining secure and reliable email systems in an organization.

**Experiment No-08**

Describe and implement Advanced Malware Protection

## Objective

The aim of this lab is to provide hands-on experience with understanding and implementing Advanced Malware Protection (AMP). By the end of this lab, you should be able to configure and manage AMP to detect, analyze, and block advanced threats across various network environments.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Windows Server for centralized management and reporting
  + Windows and Linux clients for testing AMP
* Cisco AMP for Endpoints or Cisco Firepower Threat Defense (FTD) appliances
* Internet access for downloading AMP software and updates

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network where the AMP appliances and client VMs are connected.
   * Ensure the network allows communication between the AMP appliances and client devices.
2. **Install and Configure AMP**
   * Deploy the Cisco AMP for Endpoints and/or Firepower Threat Defense appliances.
   * Complete the initial setup and ensure that AMP is accessible from the management console.

## Procedure

### Part 1: Understanding Advanced Malware Protection

#### Step 1: Overview of AMP

1. **Introduction to AMP**
   * Advanced Malware Protection (AMP) provides continuous analysis, monitoring, and protection against malware threats.
   * AMP uses various technologies like file reputation, file sandboxing, and retrospective security to detect and block threats.
2. **Components of AMP**
   * AMP for Endpoints: Protects devices such as desktops, laptops, and mobile devices.
   * AMP for Networks: Integrates with network security devices to protect the network perimeter.
   * AMP for Email: Protects email systems by scanning attachments and links for malware.
3. **Key Features of AMP**
   * Continuous analysis and monitoring
   * File reputation scoring
   * File sandboxing
   * Retrospective security
   * Threat intelligence and analytics

### Part 2: Deploying AMP for Endpoints

#### Step 1: Install AMP for Endpoints

1. **Access the AMP Console**
   * Log in to the Cisco AMP for Endpoints console using the provided credentials.
2. **Create Policies**
   * Navigate to **Management > Policies**.
   * Create a new policy or modify an existing one to define how endpoints are protected.
   * Configure settings such as file blocking, quarantine, and scan schedules.
3. **Download and Install Connectors**
   * Navigate to **Management > Download Connector**.
   * Download the appropriate connectors for Windows and Linux clients.
   * Install the connectors on the client machines.

Example for Windows installation:

powershell

Copy code

msiexec /i AMP\_Connector\_Install\_Package.msi /quiet /norestart

1. **Verify Installation**
   * Ensure that the AMP connector is running on the client machines.
   * Verify that the clients appear in the AMP console under **Computers**.

### Part 3: Deploying AMP for Networks

#### Step 1: Install AMP on Firepower Threat Defense (FTD)

1. **Access the Firepower Management Center (FMC)**
   * Log in to the FMC console using the provided credentials.
2. **Configure AMP for Networks**
   * Navigate to **Devices > Device Management**.
   * Select the FTD device and go to the **Policies > Access Control** tab.
   * Create or modify an access control policy to enable AMP for file analysis.
3. **Enable File Policies**
   * Under the access control policy, go to **Advanced > File Policy**.
   * Enable file inspection and configure rules for file types and actions.
4. **Apply Policy to FTD**
   * Save and deploy the policy to the FTD device.
   * Verify that the AMP for Networks settings are active on the FTD.

### Part 4: Configuring AMP Policies

#### Step 1: Create Custom Detection Policies

1. **File and Process Monitoring**
   * In the AMP console, navigate to **Management > Policies**.
   * Create custom policies to monitor specific files and processes.
   * Configure actions for detected threats, such as quarantine or alerting.
2. **Network File Trajectory**
   * Enable network file trajectory to track the movement and spread of files across the network.
   * Use this information to understand the impact and source of malware.
3. **Retrospective Security**
   * Configure retrospective security to analyze past events and alerts.
   * Enable the AMP console to provide alerts on newly discovered threats in historical data.

### Part 5: Testing and Verification

#### Step 1: Test Malware Detection

1. **Test with EICAR File**
   * Download the EICAR test file on the client machines.
   * Verify that AMP detects and blocks the file.
2. **Simulate Real-World Threats**
   * Use malware samples from a controlled environment to test AMP's detection capabilities.
   * Ensure that AMP correctly identifies and handles the threats.
3. **Check AMP Console**
   * Monitor the AMP console for alerts and logs related to the test files.
   * Verify that the console provides detailed information about the detected threats.

#### Step 2: Analyze Threat Data

1. **Review File Trajectory**
   * Use the file trajectory feature to analyze the movement of malicious files.
   * Identify how the malware entered the network and which systems were affected.
2. **Generate Reports**
   * Navigate to **Reports** in the AMP console.
   * Generate reports on detected threats, endpoint status, and network security.

### Part 6: Troubleshooting and Maintenance

#### Step 1: Common Issues

1. **Connector Installation Issues**
   * Verify that the connector installation completes successfully on client machines.
   * Check for connectivity issues between the client and AMP console.
2. **Policy Misconfiguration**
   * Review AMP policies to ensure they are correctly configured.
   * Check for conflicting or missing policy rules.

#### Step 2: Maintenance

1. **Regular Updates**
   * Ensure that AMP connectors and appliances are regularly updated with the latest threat intelligence.
   * Apply software updates and patches as they become available.
2. **Backup and Restore**
   * Regularly back up the AMP configuration and policies.
   * Test the backup and restore process to ensure it works as expected.

## Post-Lab Analysis

#### Step 1: Review Configuration

1. **Discuss Configurations**
   * Review the configurations made during the lab.
   * Discuss the rationale behind each configuration decision.
2. **Security Benefits**
   * Discuss the security benefits provided by AMP.
   * Identify any potential improvements or additional features to be configured.

#### Step 2: Summary Report

1. **Documentation**
   * Write a summary report detailing the configuration steps, verification results, and any troubleshooting steps taken.

## Conclusion

By completing this lab, you should have a solid understanding of how to configure and manage Advanced Malware Protection (AMP) to detect, analyze, and block advanced threats. This knowledge is essential for maintaining a secure network environment and protecting against evolving malware threats.

**Experiment No-09**

Implement enterprise Internet connectivity

## Objective

The aim of this lab is to provide hands-on experience with setting up and managing enterprise Internet connectivity. By the end of this lab, you should be able to configure and verify Internet connectivity for an enterprise network, including setting up routing, NAT, and security measures.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Linux or Windows Server for network services
  + Client machines (Windows/Linux)
* Network simulator (optional, e.g., GNS3 or Cisco Packet Tracer)
* Cisco routers and switches (physical or virtual) for simulating enterprise network

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network where the routers, switches, servers, and client machines are connected.
   * Ensure the network allows communication between devices as required for the lab.
2. **Internet Connection**
   * Simulate an Internet connection using a separate VM or network segment representing the ISP.

## Procedure

### Part 1: Configuring Basic Network Infrastructure

#### Step 1: Setup the Enterprise Network

1. **Configure Routers and Switches**
   * Use Cisco IOS commands to configure basic settings on routers and switches.
   * Assign IP addresses to interfaces and configure VLANs as needed.

Example CLI commands:

shell

Copy code

enable

configure terminal

hostname Router1

interface GigabitEthernet0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

1. **Configure DHCP**
   * Set up a DHCP server on the network to assign IP addresses to client devices.

Example for Cisco router:

shell

Copy code

ip dhcp pool CLIENTS

network 192.168.1.0 255.255.255.0

default-router 192.168.1.1

dns-server 8.8.8.8

#### Step 2: Configure Routing

1. **Static Routing**
   * Configure static routes to direct traffic between different network segments.

Example CLI commands:

shell

Copy code

ip route 0.0.0.0 0.0.0.0 192.168.2.1

1. **Dynamic Routing Protocols**
   * Set up a dynamic routing protocol (e.g., OSPF, EIGRP) to manage routing in the enterprise network.

Example for OSPF:

shell

Copy code

router ospf 1

network 192.168.1.0 0.0.0.255 area 0

### Part 2: Configuring Internet Connectivity

#### Step 1: Configure NAT (Network Address Translation)

1. **Configure NAT on the Enterprise Router**
   * Set up NAT to translate private IP addresses to a public IP address for Internet access.

Example CLI commands for PAT (Port Address Translation):

shell

Copy code

access-list 1 permit 192.168.1.0 0.0.0.255

interface GigabitEthernet0/1

ip nat outside

interface GigabitEthernet0/0

ip nat inside

ip nat inside source list 1 interface GigabitEthernet0/1 overload

1. **Verify NAT Configuration**
   * Use commands to verify that NAT is working correctly.

Example CLI commands:

shell

Copy code

show ip nat translations

show ip nat statistics

#### Step 2: Set Up a Firewall

1. **Configure Basic Firewall Rules**
   * Use access control lists (ACLs) to configure basic firewall rules on the router.

Example CLI commands:

shell

Copy code

access-list 100 permit tcp any any established

access-list 100 permit icmp any any echo-reply

access-list 100 deny ip any any log

interface GigabitEthernet0/1

ip access-group 100 in

1. **Advanced Firewall Configuration (Optional)**
   * If available, configure an advanced firewall appliance (e.g., Cisco ASA) for more granular security.

### Part 3: Configuring Redundancy and Failover

#### Step 1: Configure Redundant Internet Connections

1. **Dual WAN Configuration**
   * Configure the router to use two WAN interfaces for redundancy.

Example CLI commands:

shell

Copy code

interface GigabitEthernet0/1

ip address 192.168.2.2 255.255.255.0

ip nat outside

interface GigabitEthernet0/2

ip address 192.168.3.2 255.255.255.0

ip nat outside

1. **Configure Load Balancing and Failover**
   * Use routing protocols or policy-based routing to manage traffic between the WAN connections.

Example for load balancing with OSPF:

shell

Copy code

router ospf 1

network 192.168.2.0 0.0.0.255 area 0

network 192.168.3.0 0.0.0.255 area 0

#### Step 2: Verify Redundancy and Failover

1. **Test Failover**
   * Simulate a failure on one of the WAN connections and verify that traffic switches to the secondary connection.

Example CLI commands to shut down an interface:

shell

Copy code

interface GigabitEthernet0/1

shutdown

1. **Monitor Redundancy Configuration**
   * Use monitoring tools to ensure that both WAN connections are active and failover is working correctly.

### Part 4: Configuring DNS and Web Proxy

#### Step 1: Configure DNS Server

1. **Set Up a Local DNS Server**
   * Configure a DNS server on the network to resolve internal and external domain names.

Example for BIND on Linux:

bash

Copy code

sudo apt-get install bind9

sudo nano /etc/bind/named.conf.local

1. **Configure DNS Forwarding**
   * Set up DNS forwarding to forward requests for external domains to an ISP’s DNS server.

Example BIND configuration:

bash

Copy code

forwarders {

8.8.8.8;

8.8.4.4;

};

#### Step 2: Configure Web Proxy (Optional)

1. **Set Up a Web Proxy Server**
   * Configure a web proxy server (e.g., Squid) to manage and filter web traffic.

Example for Squid on Linux:

bash

Copy code

sudo apt-get install squid

sudo nano /etc/squid/squid.conf

1. **Configure Proxy Settings**
   * Configure client machines to use the web proxy for Internet access.

### Part 5: Testing and Verification

#### Step 1: Verify Internet Connectivity

1. **Ping External Websites**
   * Use the ping command to verify connectivity to external websites from client machines.

Example:

shell

Copy code

ping www.google.com

1. **Test Web Browsing**
   * Open a web browser on a client machine and access several websites to ensure Internet connectivity.

#### Step 2: Verify Security and Redundancy

1. **Test Firewall Rules**
   * Attempt to access blocked services and verify that firewall rules are enforced.
2. **Test Redundant Connections**
   * Simulate a WAN failure and verify that traffic seamlessly switches to the backup connection.

### Part 6: Troubleshooting and Maintenance

#### Step 1: Common Issues

1. **Connectivity Problems**
   * Check the physical and logical network configurations.
   * Verify IP addressing, routing, and NAT settings.
2. **Security Issues**
   * Review and update firewall rules and security policies.
   * Monitor logs for suspicious activity.

#### Step 2: Maintenance

1. **Regular Updates**
   * Ensure that network devices and servers are regularly updated with the latest software and firmware.
   * Apply security patches as needed.
2. **Backup and Restore**
   * Regularly back up configurations for routers, switches, and servers.
   * Test the backup and restore process to ensure it works as expected.

## Post-Lab Analysis

#### Step 1: Review Configuration

1. **Discuss Configurations**
   * Review the configurations made during the lab.
   * Discuss the rationale behind each configuration decision.
2. **Security and Performance**
   * Analyze the security measures implemented and their effectiveness.
   * Evaluate the performance of the Internet connectivity setup.

#### Step 2: Summary Report

1. **Documentation**
   * Write a summary report detailing the configuration steps, verification results, and any troubleshooting steps taken.

## Conclusion

By completing this lab, you should have a solid understanding of how to configure and manage enterprise Internet connectivity, including routing, NAT, redundancy, and security measures. This knowledge is essential for maintaining a reliable and secure Internet connection for an enterprise network.

**Experiment No-10**

Implement external authentication providers

## Objective

The aim of this lab is to provide hands-on experience with configuring and managing external authentication providers for an enterprise network. By the end of this lab, you should be able to integrate external authentication services such as RADIUS, TACACS+, and LDAP with your network infrastructure.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Linux or Windows Server for hosting external authentication services
  + Client machines (Windows/Linux)
* Cisco routers and switches (physical or virtual) for simulating enterprise network
* Internet access for downloading necessary software and updates

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network where the routers, switches, servers, and client machines are connected.
   * Ensure the network allows communication between devices as required for the lab.
2. **Authentication Servers**
   * Set up VMs to act as external authentication servers (e.g., RADIUS, TACACS+, LDAP).

## Procedure

### Part 1: Configuring External Authentication Servers

#### Step 1: Set Up a RADIUS Server

1. **Install FreeRADIUS on a Linux Server**
   * Use the following commands to install FreeRADIUS:

bash

Copy code

sudo apt-get update

sudo apt-get install freeradius freeradius-mysql

1. **Configure FreeRADIUS**
   * Edit the FreeRADIUS configuration files to define clients and users.
   * Configure the /etc/freeradius/3.0/clients.conf file to define network devices:

plaintext

Copy code

client router1 {

ipaddr = 192.168.1.1

secret = testing123

}

* + Configure the /etc/freeradius/3.0/users file to define user accounts:

plaintext

Copy code

testuser Cleartext-Password := "password123"

1. **Start and Test FreeRADIUS**
   * Start the FreeRADIUS service:

bash

Copy code

sudo systemctl start freeradius

* + Test the RADIUS server using the radtest command:

bash

Copy code

radtest testuser password123 localhost 0 testing123

#### Step 2: Set Up a TACACS+ Server

1. **Install TACACS+ on a Linux Server**
   * Use the following commands to install TACACS+:

bash

Copy code

sudo apt-get update

sudo apt-get install tacacs+

1. **Configure TACACS+**
   * Edit the TACACS+ configuration file located at /etc/tacacs+/tac\_plus.conf:

plaintext

Copy code

key = testing123

user = testuser {

default service = permit

login = cleartext password123

}

1. **Start and Test TACACS+**
   * Start the TACACS+ service:

bash

Copy code

sudo systemctl start tacacs+

* + Test the TACACS+ server using the tac\_plus -C command to check the configuration:

bash

Copy code

sudo tac\_plus -C /etc/tacacs+/tac\_plus.conf

#### Step 3: Set Up an LDAP Server

1. **Install OpenLDAP on a Linux Server**
   * Use the following commands to install OpenLDAP:

bash

Copy code

sudo apt-get update

sudo apt-get install slapd ldap-utils

1. **Configure OpenLDAP**
   * Use dpkg-reconfigure slapd to set up the LDAP directory and administrator password.
   * Add LDAP entries for users using ldapadd and LDIF files.

Example LDIF file (new\_user.ldif):

plaintext

Copy code

dn: uid=testuser,ou=users,dc=example,dc=com

objectClass: inetOrgPerson

uid: testuser

sn: User

cn: Test User

userPassword: password123

Command to add the user:

bash

Copy code

ldapadd -x -D cn=admin,dc=example,dc=com -W -f new\_user.ldif

### Part 2: Integrating External Authentication with Network Devices

#### Step 1: Configure a Cisco Router for RADIUS Authentication

1. **Enable AAA**

shell

Copy code

enable

configure terminal

aaa new-model

1. **Configure the RADIUS Server**

shell

Copy code

radius-server host 192.168.1.100 key testing123

1. **Set Up Authentication for Login**

shell

Copy code

aaa authentication login default group radius local

1. **Test RADIUS Authentication**
   * Log out and log back into the router to test RADIUS authentication with the test user credentials.

#### Step 2: Configure a Cisco Router for TACACS+ Authentication

1. **Enable AAA**

shell

Copy code

enable

configure terminal

aaa new-model

1. **Configure the TACACS+ Server**

shell

Copy code

tacacs-server host 192.168.1.101 key testing123

1. **Set Up Authentication for Login**

shell

Copy code

aaa authentication login default group tacacs+ local

1. **Test TACACS+ Authentication**
   * Log out and log back into the router to test TACACS+ authentication with the test user credentials.

#### Step 3: Configure a Cisco Router for LDAP Authentication

1. **Enable AAA**

shell

Copy code

enable

configure terminal

aaa new-model

1. **Configure the LDAP Server**
   * Note: Cisco routers do not support LDAP natively. You would typically use RADIUS/TACACS+ servers to authenticate against LDAP. Ensure your RADIUS/TACACS+ server is configured to use LDAP as its backend authentication source.

### Part 3: Testing and Verification

#### Step 1: Verify RADIUS Authentication

1. **Log in to the Router**
   * Use the test user credentials configured on the RADIUS server.
   * Verify successful login and check logs on the RADIUS server.

#### Step 2: Verify TACACS+ Authentication

1. **Log in to the Router**
   * Use the test user credentials configured on the TACACS+ server.
   * Verify successful login and check logs on the TACACS+ server.

#### Step 3: Verify LDAP Authentication (Indirect)

1. **Log in to the Router via RADIUS/TACACS+**
   * Ensure the RADIUS/TACACS+ server is configured to authenticate against LDAP.
   * Verify successful login and check logs on the LDAP server.

### Part 4: Troubleshooting and Maintenance

#### Step 1: Common Issues

1. **Connectivity Problems**
   * Verify network connectivity between the router and the authentication servers.
   * Check firewall rules and ACLs that might block communication.
2. **Configuration Errors**
   * Review the configuration files on the RADIUS, TACACS+, and LDAP servers.
   * Check for syntax errors or incorrect parameters.
3. **Authentication Failures**
   * Ensure that user credentials are correctly configured on the authentication servers.
   * Check server logs for error messages and troubleshoot accordingly.

#### Step 2: Maintenance

1. **Regular Updates**
   * Ensure that authentication servers and network devices are regularly updated with the latest software and firmware.
   * Apply security patches as needed.
2. **Backup and Restore**
   * Regularly back up configurations for authentication servers and network devices.
   * Test the backup and restore process to ensure it works as expected.

## Post-Lab Analysis

#### Step 1: Review Configuration

1. **Discuss Configurations**
   * Review the configurations made during the lab.
   * Discuss the rationale behind each configuration decision.
2. **Security and Performance**
   * Analyze the security measures implemented and their effectiveness.
   * Evaluate the performance of the external authentication setup.

#### Step 2: Summary Report

1. **Documentation**
   * Write a summary report detailing the configuration steps, verification results, and any troubleshooting steps taken.

## Conclusion

By completing this lab, you should have a solid understanding of how to configure and manage external authentication providers, including RADIUS, TACACS+, and LDAP. This knowledge is essential for maintaining a secure and scalable authentication system for an enterprise network.

**Experiment No-11**

Understand basic cryptography principles. Understand endpoint attacks, including interpreting log data to identify events in Windows and Linux

## Objective

The aim of this lab is to provide hands-on experience with basic cryptography principles and understanding endpoint attacks by interpreting log data to identify events in both Windows and Linux systems. By the end of this lab, you should be able to understand and apply basic cryptographic techniques and identify potential security incidents through log analysis.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Linux (e.g., Ubuntu)
  + Windows (e.g., Windows Server or Windows 10)
* Basic cryptography tools (e.g., OpenSSL for Linux, Windows PowerShell for cryptographic operations)
* Log analysis tools (e.g., Splunk, ELK Stack, or native OS log viewers)

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network where the Linux and Windows VMs are connected.
   * Ensure network connectivity between the VMs for potential log forwarding and monitoring.
2. **Software Installation**
   * Install necessary cryptographic tools and log analysis software on both Linux and Windows systems.

## Procedure

### Part 1: Understanding Basic Cryptography Principles

#### Step 1: Symmetric Encryption

1. **Linux - OpenSSL**
   * Encrypt a file using AES encryption:

bash

Copy code

openssl enc -aes-256-cbc -salt -in plain.txt -out encrypted.txt

* + Decrypt the file:

bash

Copy code

openssl enc -aes-256-cbc -d -in encrypted.txt -out decrypted.txt

1. **Windows - PowerShell**
   * Encrypt a string using AES:

powershell

Copy code

$Key = (1..32) | ForEach-Object { [char](65 + (Get-Random -Maximum 25)) } -join ''

$SecureString = ConvertTo-SecureString "plain text" -AsPlainText -Force

$EncryptedString = ConvertFrom-SecureString $SecureString -Key (1..32)

* + Decrypt the string:

powershell

Copy code

$DecryptedString = ConvertTo-SecureString $EncryptedString -Key (1..32)

[Runtime.InteropServices.Marshal]::PtrToStringAuto([Runtime.InteropServices.Marshal]::SecureStringToBSTR($DecryptedString))

#### Step 2: Asymmetric Encryption

1. **Linux - OpenSSL**
   * Generate RSA keys:

bash

Copy code

openssl genpkey -algorithm RSA -out private\_key.pem -pkeyopt rsa\_keygen\_bits:2048

openssl rsa -pubout -in private\_key.pem -out public\_key.pem

* + Encrypt and decrypt a file:

bash

Copy code

openssl rsautl -encrypt -inkey public\_key.pem -pubin -in plain.txt -out encrypted.txt

openssl rsautl -decrypt -inkey private\_key.pem -in encrypted.txt -out decrypted.txt

1. **Windows - PowerShell**
   * Generate RSA keys:

powershell

Copy code

$rsa = New-Object System.Security.Cryptography.RSACryptoServiceProvider(2048)

$PublicKey = $rsa.ToXmlString($false)

$PrivateKey = $rsa.ToXmlString($true)

* + Encrypt and decrypt a string:

powershell

Copy code

$EncryptedText = [Convert]::ToBase64String($rsa.Encrypt([System.Text.Encoding]::UTF8.GetBytes("plain text"), $true))

$DecryptedText = [System.Text.Encoding]::UTF8.GetString($rsa.Decrypt([Convert]::FromBase64String($EncryptedText), $true))

#### Step 3: Hashing

1. **Linux - OpenSSL**
   * Generate a SHA-256 hash of a file:

bash

Copy code

openssl dgst -sha256 plain.txt

1. **Windows - PowerShell**
   * Generate a SHA-256 hash of a string:

powershell

Copy code

$string = "plain text"

$bytes = [System.Text.Encoding]::UTF8.GetBytes($string)

$sha256 = [System.Security.Cryptography.SHA256]::Create()

$hash = $sha256.ComputeHash($bytes)

[BitConverter]::ToString($hash) -replace '-'

### Part 2: Understanding Endpoint Attacks

#### Step 1: Windows Event Logs

1. **Enable Windows Logging**
   * Ensure that logging is enabled for various event categories (Application, Security, System):

powershell

Copy code

wevtutil el

1. **Generate Sample Events**
   * Create sample security events by performing various actions (e.g., login attempts, file access):

powershell

Copy code

Get-EventLog -LogName Security -Newest 5

1. **Analyze Event Logs**
   * Open Event Viewer and navigate to Windows Logs to analyze recent events:

shell

Copy code

eventvwr

1. **Interpret Logs**
   * Identify key events such as login attempts, failed logins, and account lockouts:
   * Event ID 4624: Successful logon
   * Event ID 4625: Failed logon
   * Event ID 4740: Account lockout

#### Step 2: Linux Log Files

1. **Enable Logging**
   * Ensure that system logging is enabled and configured in /etc/rsyslog.conf.
2. **Generate Sample Events**
   * Perform actions to generate logs (e.g., SSH login attempts, file access):

bash

Copy code

sudo tail -f /var/log/auth.log

1. **Analyze Log Files**
   * Use commands to view and analyze log files:

bash

Copy code

cat /var/log/auth.log

grep "Failed password" /var/log/auth.log

grep "Accepted password" /var/log/auth.log

1. **Interpret Logs**
   * Identify key events such as SSH login attempts, failed logins, and sudo commands:
   * sshd logs for login attempts
   * /var/log/auth.log for authentication-related events

### Part 3: Integrating Log Data for Centralized Analysis

#### Step 1: Install and Configure Log Analysis Tools

1. **Splunk**
   * Install Splunk on a dedicated VM or server.
   * Configure data inputs to collect logs from Windows and Linux machines.
2. **ELK Stack (Elasticsearch, Logstash, Kibana)**
   * Install ELK Stack on a dedicated VM or server.
   * Configure Logstash to collect and parse logs from Windows and Linux machines.
   * Use Kibana to visualize and analyze log data.

#### Step 2: Forward Logs to Centralized Server

1. **Linux**
   * Use rsyslog to forward logs to a centralized log server:

bash

Copy code

\*.\* @logserver:514

1. **Windows**
   * Use Windows Event Forwarding (WEF) to forward logs to a centralized log server.
   * Configure a subscription to collect logs from multiple Windows machines.

#### Step 3: Analyze Centralized Logs

1. **Search and Correlate Events**
   * Use Splunk or Kibana to search for and correlate events across different machines.
   * Create dashboards to visualize key security events.
2. **Identify Security Incidents**
   * Analyze patterns and identify potential security incidents such as repeated failed logins, unusual login times, and unexpected changes to system files.

### Part 4: Troubleshooting and Maintenance

#### Step 1: Common Issues

1. **Cryptography Errors**
   * Ensure correct key usage and matching pairs for encryption/decryption.
   * Verify the syntax and parameters for cryptographic commands.
2. **Log Collection Issues**
   * Ensure that logging services are running on both Windows and Linux machines.
   * Check network connectivity between endpoints and the centralized log server.
3. **Log Analysis Problems**
   * Verify that logs are being correctly parsed and indexed by the log analysis tools.
   * Check for any configuration errors in the log forwarding setup.

#### Step 2: Maintenance

1. **Regular Updates**
   * Ensure that cryptographic tools and log analysis software are regularly updated with the latest security patches and features.
   * Apply updates to logging configurations as needed.
2. **Backup and Restore**
   * Regularly back up cryptographic keys and log analysis configurations.
   * Test the backup and restore process to ensure it works as expected.

## Post-Lab Analysis

#### Step 1: Review Configuration

1. **Discuss Configurations**
   * Review the cryptographic and logging configurations made during the lab.
   * Discuss the rationale behind each configuration decision.
2. **Security and Performance**
   * Analyze the security measures implemented and their effectiveness.
   * Evaluate the performance of the cryptographic operations and log analysis setup.

#### Step 2: Summary Report

1. **Documentation**
   * Write a summary report detailing the configuration steps, verification results, and any troubleshooting steps taken.

## Conclusion

By completing this lab, you should have a solid understanding of basic cryptographic principles and the ability to identify potential endpoint attacks through log analysis. This knowledge is essential for maintaining a secure and monitored enterprise network.

**Experiment No-12**

Develop knowledge in security monitoring, including identifying sources and types of data and events

## Objective

The aim of this lab is to provide hands-on experience with security monitoring, including identifying sources and types of data and events. By the end of this lab, you should be able to understand various sources of security data, collect and analyze logs, and identify different types of security events.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Linux (e.g., Ubuntu)
  + Windows (e.g., Windows Server or Windows 10)
* Security Information and Event Management (SIEM) tool (e.g., Splunk, ELK Stack)
* Network monitoring tools (e.g., Wireshark, Nmap)
* Endpoint security tools (e.g., antivirus, EDR solutions)

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network where the Linux and Windows VMs are connected.
   * Ensure network connectivity between the VMs for potential log forwarding and monitoring.
2. **Software Installation**
   * Install necessary security monitoring tools and SIEM software on both Linux and Windows systems.

## Procedure

### Part 1: Identifying Sources of Security Data

#### Step 1: Operating System Logs

1. **Windows Event Logs**
   * Enable logging for various event categories (Application, Security, System):

powershell

Copy code

wevtutil el

* + View recent logs using Event Viewer:

shell

Copy code

eventvwr

* + Generate sample events by performing actions such as login attempts, file access, and software installations:

powershell

Copy code

Get-EventLog -LogName Security -Newest 5

1. **Linux System Logs**
   * Ensure system logging is enabled and configured in /etc/rsyslog.conf.
   * View logs using commands:

bash

Copy code

cat /var/log/syslog

cat /var/log/auth.log

* + Generate sample events by performing actions such as SSH login attempts, file access, and system updates:

bash

Copy code

sudo tail -f /var/log/auth.log

#### Step 2: Network Data

1. **Network Traffic Capture**
   * Install and use Wireshark to capture network traffic:

bash

Copy code

sudo apt-get install wireshark

sudo wireshark

* + Capture traffic on a specific interface and analyze packet details.

1. **Network Scanning**
   * Install and use Nmap to perform network scans:

bash

Copy code

sudo apt-get install nmap

nmap -sP 192.168.1.0/24

1. **Firewall Logs**
   * Configure and view firewall logs on both Linux and Windows systems.
   * Linux (e.g., iptables):

bash

Copy code

sudo iptables -L -v -n

sudo tail -f /var/log/syslog | grep iptables

* + Windows Firewall:

powershell

Copy code

Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall"

#### Step 3: Application Logs

1. **Web Server Logs**
   * Set up a web server (e.g., Apache) on Linux and view access and error logs:

bash

Copy code

sudo apt-get install apache2

sudo tail -f /var/log/apache2/access.log

sudo tail -f /var/log/apache2/error.log

1. **Database Logs**
   * Set up a database server (e.g., MySQL) and view logs:

bash

Copy code

sudo apt-get install mysql-server

sudo tail -f /var/log/mysql/error.log

1. **Application Logs**
   * Configure and view logs for custom applications on both Linux and Windows.

### Part 2: Collecting and Analyzing Logs

#### Step 1: Install and Configure SIEM

1. **Splunk**
   * Install Splunk on a dedicated VM or server:

bash

Copy code

wget -O splunk-8.0.6-linux-2.6-amd64.deb 'https://www.splunk.com/page/download\_track?file=8.0.6/linux/splunk-8.0.6-ef1c838badc9-linux-2.6-amd64.deb&ac=&wget=true&name=wget&platform=linux&architecture=x86&version=8.0.6&product=splunk&typed=release'

sudo dpkg -i splunk-8.0.6-linux-2.6-amd64.deb

sudo /opt/splunk/bin/splunk start --accept-license

* + Configure data inputs to collect logs from Windows and Linux machines.

1. **ELK Stack (Elasticsearch, Logstash, Kibana)**
   * Install ELK Stack on a dedicated VM or server.
   * Configure Logstash to collect and parse logs from Windows and Linux machines.
   * Use Kibana to visualize and analyze log data.

#### Step 2: Forward Logs to SIEM

1. **Linux**
   * Use rsyslog to forward logs to a centralized log server:

bash

Copy code

\*.\* @logserver:514

1. **Windows**
   * Use Windows Event Forwarding (WEF) to forward logs to a centralized log server.
   * Configure a subscription to collect logs from multiple Windows machines.

#### Step 3: Analyze Logs in SIEM

1. **Search and Correlate Events**
   * Use Splunk or Kibana to search for and correlate events across different machines.
   * Create dashboards to visualize key security events.
2. **Identify Security Incidents**
   * Analyze patterns and identify potential security incidents such as repeated failed logins, unusual login times, and unexpected changes to system files.

### Part 3: Understanding Types of Security Events

#### Step 1: Operating System Events

1. **Windows Event IDs**
   * Event ID 4624: Successful logon
   * Event ID 4625: Failed logon
   * Event ID 4740: Account lockout
2. **Linux Event Types**
   * SSH login attempts
   * Sudo command usage
   * System reboots

#### Step 2: Network Security Events

1. **Intrusion Detection**
   * Detect unusual traffic patterns with Wireshark.
   * Identify potential intrusions using IDS/IPS logs.
2. **Firewall Events**
   * Monitor blocked and allowed traffic.
   * Analyze firewall logs for unauthorized access attempts.

#### Step 3: Application Security Events

1. **Web Server Events**
   * Monitor for common web attacks (e.g., SQL injection, XSS).
   * Analyze access logs for unusual patterns.
2. **Database Security Events**
   * Monitor for unauthorized database access.
   * Analyze database logs for suspicious queries.

### Part 4: Troubleshooting and Maintenance

#### Step 1: Common Issues

1. **Log Collection Problems**
   * Ensure logging services are running on both Windows and Linux machines.
   * Check network connectivity between endpoints and the centralized log server.
2. **Log Analysis Issues**
   * Verify that logs are being correctly parsed and indexed by the SIEM tools.
   * Check for any configuration errors in the log forwarding setup.
3. **Security Event Detection**
   * Ensure that SIEM rules and alerts are correctly configured.
   * Regularly update and refine detection rules to adapt to new threats.

#### Step 2: Maintenance

1. **Regular Updates**
   * Ensure that security monitoring tools and SIEM software are regularly updated with the latest security patches and features.
   * Apply updates to logging configurations as needed.
2. **Backup and Restore**
   * Regularly back up SIEM configurations and log data.
   * Test the backup and restore process to ensure it works as expected.

## Post-Lab Analysis

#### Step 1: Review Configuration

1. **Discuss Configurations**
   * Review the configurations made during the lab for log collection and analysis.
   * Discuss the rationale behind each configuration decision.
2. **Security and Performance**
   * Analyze the security measures implemented and their effectiveness.
   * Evaluate the performance of the log collection and SIEM setup.

#### Step 2: Summary Report

1. **Documentation**
   * Write a summary report detailing the configuration steps, verification results, and any troubleshooting steps taken.

## Conclusion

By completing this lab, you should have a solid understanding of security monitoring, including identifying sources and types of data and events, and analyzing logs to detect security incidents. This knowledge is essential for maintaining a secure and monitored enterprise network.

**Experiment No-13**

Describe the concepts, benefits, or operation of security policies Zone-based policies, Global policies ,Application firewall, Unified security policies, IPS/IDP ,Integrated user firewall

## Objective

This lab aims to provide hands-on experience with the concepts, benefits, and operations of various security policies, including zone-based policies, global policies, application firewalls, unified security policies, IPS/IDP, and integrated user firewalls. By the end of this lab, you should be able to understand and implement these security policies to enhance network security.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Linux (e.g., Ubuntu)
  + Windows (e.g., Windows Server or Windows 10)
* Network security appliances or virtual appliances (e.g., pfSense, Cisco ASAv)
* Security tools (e.g., Snort for IDS/IPS, application firewalls)

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network where the Linux and Windows VMs are connected.
   * Ensure network connectivity between the VMs and the security appliances for proper policy implementation.
2. **Software Installation**
   * Install necessary security tools and appliances on both Linux and Windows systems.

## Procedure

### Part 1: Zone-Based Policies

#### Step 1: Understanding Zone-Based Policies

* **Concept**: Zone-based policies divide the network into different zones (e.g., trusted, untrusted) and define policies to control traffic between these zones.
* **Benefits**: Enhanced security by isolating different network segments and simplified policy management.

#### Step 2: Configure Zone-Based Policies

1. **Setup Zones on pfSense**
   * Create zones (e.g., LAN, WAN, DMZ) in pfSense.
   * Navigate to Firewall > Aliases to create zone aliases.
   * Define the zones in Interfaces > Assignments.
2. **Define Policies**
   * Navigate to Firewall > Rules.
   * Add rules to control traffic between zones, e.g., allow HTTP/HTTPS traffic from LAN to WAN, block traffic from WAN to DMZ.
3. **Test the Configuration**
   * Verify the policy implementation by accessing services from different zones and checking if the rules are enforced.

### Part 2: Global Policies

#### Step 1: Understanding Global Policies

* **Concept**: Global policies apply to all traffic, regardless of source or destination zones.
* **Benefits**: Simplifies the application of common policies (e.g., block all traffic to a specific port) across the entire network.

#### Step 2: Configure Global Policies

1. **Define Global Policies on pfSense**
   * Navigate to Firewall > Rules.
   * Add rules in the Floating tab to apply them globally.
2. **Example Global Policy**
   * Create a rule to block all incoming traffic on port 23 (Telnet) globally.
   * Ensure the rule is enabled and saved.
3. **Test the Configuration**
   * Verify the policy by attempting to access Telnet services from any zone and confirming that the connection is blocked.

### Part 3: Application Firewall

#### Step 1: Understanding Application Firewalls

* **Concept**: Application firewalls control traffic based on application-level protocols and can inspect traffic for application-specific threats.
* **Benefits**: Provides deep packet inspection, protects against application-layer attacks, and enforces application-specific policies.

#### Step 2: Configure an Application Firewall

1. **Setup ModSecurity on Apache (Linux)**
   * Install ModSecurity:

bash

Copy code

sudo apt-get install libapache2-mod-security2

* + Enable ModSecurity:

bash

Copy code

sudo a2enmod security2

* + Configure ModSecurity by editing /etc/modsecurity/modsecurity.conf.

1. **Define Application Rules**
   * Enable and configure the OWASP ModSecurity Core Rule Set (CRS) for comprehensive application-layer protection.
2. **Test the Configuration**
   * Verify the application firewall by accessing web services and observing the firewall logs for blocked attacks.

### Part 4: Unified Security Policies

#### Step 1: Understanding Unified Security Policies

* **Concept**: Unified security policies combine various security controls (e.g., firewall, IDS/IPS, application control) into a single policy framework.
* **Benefits**: Simplifies policy management, provides comprehensive security coverage, and improves operational efficiency.

#### Step 2: Implement Unified Security Policies

1. **Setup a UTM Appliance (e.g., pfSense with Snort)**
   * Install Snort package on pfSense.
   * Navigate to Services > Snort to configure IDS/IPS rules.
2. **Define Unified Policies**
   * Combine firewall rules, IDS/IPS rules, and application control rules into a cohesive policy set.
   * Example: Block malicious traffic identified by Snort, and enforce firewall rules for allowed traffic.
3. **Test the Configuration**
   * Generate test traffic and verify that unified policies are correctly enforced.

### Part 5: IPS/IDP (Intrusion Prevention/Detection Systems)

#### Step 1: Understanding IPS/IDP

* **Concept**: IDS/IPS monitor network traffic for suspicious activity and can take action to block detected threats.
* **Benefits**: Enhances network security by detecting and preventing attacks in real-time.

#### Step 2: Configure IPS/IDP

1. **Setup Snort on pfSense**
   * Install and configure Snort as described in the previous section.
   * Enable IPS mode to actively block detected threats.
2. **Define IDS/IPS Rules**
   * Configure rules to detect common threats (e.g., SQL injection, cross-site scripting).
   * Enable automatic rule updates to stay current with emerging threats.
3. **Test the Configuration**
   * Simulate attacks using tools like Metasploit or custom scripts and verify that Snort detects and blocks them.

### Part 6: Integrated User Firewall

#### Step 1: Understanding Integrated User Firewall

* **Concept**: Integrated user firewalls apply security policies based on user identity rather than IP addresses.
* **Benefits**: Provides granular control over user access, enhances policy enforcement based on user roles.

#### Step 2: Configure Integrated User Firewall

1. **Setup User Authentication on pfSense**
   * Configure a user directory service (e.g., LDAP, RADIUS).
   * Navigate to System > User Manager to add users and groups.
2. **Define User-Based Policies**
   * Create firewall rules that apply based on user identity.
   * Example: Allow specific users to access certain network resources.
3. **Test the Configuration**
   * Verify the policy by logging in with different user accounts and checking access to resources.

### Part 7: Troubleshooting and Maintenance

#### Step 1: Common Issues

1. **Policy Conflicts**
   * Check for conflicting rules that may override each other.
   * Ensure the correct order of rule application.
2. **Rule Effectiveness**
   * Regularly review and update security policies to address new threats.
   * Monitor logs to ensure that rules are being correctly enforced.

#### Step 2: Maintenance

1. **Regular Updates**
   * Keep security tools and appliances up to date with the latest patches and rule sets.
   * Review and refine security policies periodically.
2. **Backup and Restore**
   * Regularly back up security appliance configurations.
   * Test the backup and restore process to ensure quick recovery in case of failure.

## Post-Lab Analysis

#### Step 1: Review Configuration

1. **Discuss Configurations**
   * Review the configurations made during the lab for each type of security policy.
   * Discuss the rationale behind each configuration decision.
2. **Security and Performance**
   * Analyze the security measures implemented and their effectiveness.
   * Evaluate the performance of the network with the applied security policies.

#### Step 2: Summary Report

1. **Documentation**
   * Write a summary report detailing the configuration steps, verification results, and any troubleshooting steps taken.

## Conclusion

By completing this lab, you should have a solid understanding of the concepts, benefits, and operations of various security policies including zone-based policies, global policies, application firewalls, unified security policies, IPS/IDP, and integrated user firewalls. This knowledge is essential for implementing effective security measures in an enterprise network.

**Experiment No-14**

Traffic Analysis Tools (for example, Wireshark), Malicious traffic detection

## Objective

The purpose of this lab is to provide hands-on experience with traffic analysis tools, such as Wireshark, and techniques for detecting malicious traffic. By the end of this lab, you should be able to capture network traffic, analyze it for anomalies, and identify signs of malicious activity.

## Required Tools

* A computer with Wireshark installed
* Virtual machines (VMs) with:
  + Linux (e.g., Ubuntu)
  + Windows (e.g., Windows Server or Windows 10)
* Network simulation environment (e.g., GNS3, Packet Tracer)
* Sample PCAP files containing both normal and malicious traffic (optional)

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network with multiple VMs connected to a virtual switch.
   * Ensure network connectivity between the VMs for proper traffic flow.
2. **Software Installation**
   * Install Wireshark on the analysis machine.
   * Ensure necessary permissions are granted to capture network traffic.

## Procedure

### Part 1: Capturing Network Traffic with Wireshark

#### Step 1: Understanding Wireshark Basics

* **Concept**: Wireshark is a network protocol analyzer that captures and displays data traveling back and forth on a network.
* **Benefits**: Allows detailed inspection of network traffic, aids in troubleshooting, and helps in detecting malicious activity.

#### Step 2: Setting Up Wireshark for Traffic Capture

1. **Launch Wireshark**
   * Open Wireshark on your machine.
2. **Select Network Interface**
   * Choose the network interface you want to capture traffic from (e.g., Ethernet, Wi-Fi).
   * Click on the interface to start capturing.
3. **Start Capturing Traffic**
   * Observe packets being captured in real-time.
   * Stop the capture after collecting sufficient data for analysis.

### Part 2: Analyzing Network Traffic

#### Step 1: Filtering Traffic

* **Concept**: Filtering helps in narrowing down the packets of interest from the large volume of captured traffic.
* **Benefits**: Makes it easier to focus on relevant data, such as HTTP requests, DNS queries, or specific IP addresses.

#### Step 2: Applying Filters in Wireshark

1. **Basic Filters**
   * Use display filters to isolate specific traffic types.
   * Examples:
     + http to filter HTTP traffic
     + ip.addr == 192.168.1.1 to filter traffic to/from a specific IP address
2. **Complex Filters**
   * Combine filters to narrow down further.
   * Example: http and ip.addr == 192.168.1.1
3. **Save Filters**
   * Save commonly used filters for quick access in future analyses.

#### Step 3: Inspecting Packets

1. **Packet Details**
   * Click on a packet to view detailed information.
   * Inspect different layers (e.g., Ethernet, IP, TCP/UDP, Application).
2. **Follow Streams**
   * Use the "Follow TCP Stream" feature to reconstruct the data flow between two endpoints.
3. **Exporting Data**
   * Export specific packets or streams for further analysis.

### Part 3: Detecting Malicious Traffic

#### Step 1: Recognizing Common Indicators of Compromise (IoCs)

* **Concept**: Indicators of Compromise are artifacts observed on a network or in an operating system that indicate a potential intrusion.
* **Benefits**: Helps in early detection and response to malicious activities.

#### Step 2: Identifying Malicious Traffic Patterns

1. **Unusual Traffic Patterns**
   * Look for abnormal traffic volumes, unexpected IP addresses, or strange protocols.
   * Example: A high volume of ICMP requests from a single IP address (indicative of a potential DDoS attack).
2. **Known Malicious Indicators**
   * Compare traffic against known IoCs such as suspicious domain names, IP addresses, or file hashes.
   * Utilize online databases like VirusTotal or Threat Intelligence feeds.
3. **Suspicious Payloads**
   * Inspect packet payloads for signs of exploits, malware, or data exfiltration.
   * Example: Base64-encoded payloads in HTTP requests could indicate data exfiltration.

#### Step 3: Practical Examples

1. **Detecting a SYN Flood Attack**
   * Filter for tcp.flags.syn == 1 and tcp.flags.ack == 0 to identify SYN packets.
   * Look for a high number of SYN packets without corresponding ACK packets.
2. **Identifying a DNS Amplification Attack**
   * Filter for udp.port == 53 to isolate DNS traffic.
   * Check for a high volume of DNS response traffic compared to requests.
3. **Spotting a Malware Infection**
   * Analyze HTTP traffic for unusual GET/POST requests.
   * Inspect payloads for signs of command-and-control (C2) communication.

### Part 4: Hands-On Exercise

#### Exercise 1: Capture and Analyze Network Traffic

1. **Capture Traffic**
   * Start a capture session in Wireshark.
   * Generate network traffic by browsing the web, downloading files, and running applications.
2. **Analyze Traffic**
   * Apply filters to isolate different types of traffic.
   * Inspect packets for detailed information.

#### Exercise 2: Detect Malicious Traffic in Sample PCAP Files

1. **Download Sample PCAP Files**
   * Obtain PCAP files containing known malicious traffic (e.g., from Malware Traffic Analysis).
2. **Analyze Sample Traffic**
   * Use Wireshark to open and inspect the sample PCAP files.
   * Identify malicious patterns and IoCs.

### Part 5: Reporting and Documentation

#### Step 1: Documenting Findings

1. **Create a Report**
   * Document the steps taken during the analysis.
   * Include screenshots of Wireshark filters, packet details, and findings.
2. **Summarize Results**
   * Provide a summary of the analysis, including identified IoCs and potential security incidents.

#### Step 2: Sharing Insights

1. **Internal Presentation**
   * Prepare a presentation to share findings with your team.
   * Highlight key points and lessons learned.
2. **Collaboration**
   * Collaborate with peers to discuss findings and improve detection techniques.

## Conclusion

By completing this lab, you should have a solid understanding of how to use Wireshark for traffic analysis and malicious traffic detection. This knowledge is essential for network security professionals to effectively monitor, analyze, and secure network environments.

**Experiment No-15**

Network Security Monitoring, Attack logging and analysis Attack mitigation

## Objective

The purpose of this lab is to provide hands-on experience with network security monitoring, attack logging, analysis, and mitigation techniques. By the end of this lab, you should be able to set up and configure network security monitoring tools, log and analyze attack data, and implement mitigation strategies.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Linux (e.g., Ubuntu)
  + Windows (e.g., Windows Server or Windows 10)
* Network security tools (e.g., Snort, Suricata, ELK Stack, Splunk, Firewalls)
* Sample attack scripts or tools (e.g., Metasploit, Nmap)

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network with multiple VMs connected to a virtual switch.
   * Ensure network connectivity between the VMs for proper traffic flow and monitoring.
2. **Software Installation**
   * Install network security monitoring tools on appropriate VMs.
   * Ensure necessary permissions are granted to capture and analyze network traffic.

## Procedure

### Part 1: Network Security Monitoring

#### Step 1: Understanding Network Security Monitoring

* **Concept**: Network security monitoring involves the continuous observation of network traffic for signs of malicious activity, performance issues, or policy violations.
* **Benefits**: Helps in early detection of security incidents, improves network performance, and ensures compliance with security policies.

#### Step 2: Setting Up Network Security Monitoring

1. **Install and Configure Snort**
   * Install Snort on a Linux VM:

bash

Copy code

sudo apt-get install snort

* + Configure Snort by editing the configuration file located at /etc/snort/snort.conf.

1. **Start Snort**
   * Run Snort in IDS mode:

bash

Copy code

sudo snort -A console -q -c /etc/snort/snort.conf -i eth0

* + Ensure Snort is capturing and analyzing network traffic.

1. **Install and Configure Suricata**
   * Install Suricata on a Linux VM:

bash

Copy code

sudo apt-get install suricata

* + Configure Suricata by editing the configuration file located at /etc/suricata/suricata.yaml.

1. **Start Suricata**
   * Run Suricata in IDS mode:

bash

Copy code

sudo suricata -c /etc/suricata/suricata.yaml -i eth0

* + Ensure Suricata is capturing and analyzing network traffic.

1. **Install ELK Stack**
   * Install Elasticsearch, Logstash, and Kibana on a Linux VM.
   * Configure Logstash to receive logs from Snort or Suricata.
   * Visualize the data in Kibana.

### Part 2: Attack Logging and Analysis

#### Step 1: Logging Network Activity

* **Concept**: Logging involves recording details about network activity, which can be analyzed to detect and respond to security incidents.
* **Benefits**: Provides a historical record of network activity, helps in forensic analysis, and aids in compliance reporting.

#### Step 2: Setting Up Logging

1. **Configure Snort to Log Data**
   * Edit /etc/snort/snort.conf to enable logging:

bash

Copy code

output log\_tcpdump: tcpdump.log

1. **Configure Suricata to Log Data**
   * Edit /etc/suricata/suricata.yaml to enable logging:

yaml

Copy code

outputs:

- eve-log:

enabled: yes

filetype: regular

filename: eve.json

1. **Log Analysis with ELK**
   * Configure Logstash to parse Snort and Suricata logs.
   * Visualize and analyze logs in Kibana.

### Part 3: Attack Detection and Analysis

#### Step 1: Simulating Attacks

* **Concept**: Simulating attacks helps in testing the effectiveness of network security monitoring and understanding attack patterns.
* **Benefits**: Improves incident response, helps in tuning detection rules, and provides practical experience.

#### Step 2: Using Attack Tools

1. **Run Nmap Scan**
   * Perform a network scan from a Linux VM:

bash

Copy code

nmap -A 192.168.1.1

1. **Use Metasploit**
   * Launch a Metasploit attack:

bash

Copy code

msfconsole

use exploit/windows/smb/ms17\_010\_eternalblue

set RHOST 192.168.1.1

run

1. **Capture and Analyze Attacks**
   * Monitor the network with Snort or Suricata during the attacks.
   * Analyze the logs to identify attack patterns and indicators of compromise.

### Part 4: Attack Mitigation

#### Step 1: Understanding Attack Mitigation

* **Concept**: Attack mitigation involves implementing measures to reduce the impact of an attack or prevent it altogether.
* **Benefits**: Protects network assets, minimizes damage, and ensures business continuity.

#### Step 2: Implementing Mitigation Strategies

1. **Firewall Rules**
   * Configure firewall rules to block malicious traffic.
   * Example: Block all incoming traffic on port 445 (SMB):

bash

Copy code

sudo ufw deny in 445

1. **IPS Mode with Snort or Suricata**
   * Enable IPS mode to automatically block detected threats.
   * Snort example:

bash

Copy code

sudo snort -A console -q -c /etc/snort/snort.conf -i eth0 -Q

* + Suricata example:

bash

Copy code

sudo suricata -c /etc/suricata/suricata.yaml -i eth0 -q

1. **Patch Management**
   * Regularly update systems to patch known vulnerabilities.
   * Example: Update Windows using Windows Update or Linux using package managers:

bash

Copy code

sudo apt-get update && sudo apt-get upgrade

1. **Network Segmentation**
   * Segment the network to isolate critical assets and reduce the attack surface.
   * Example: Use VLANs to separate different types of traffic.
2. **Incident Response Plan**
   * Develop and implement an incident response plan to quickly respond to detected attacks.
   * Include steps for identification, containment, eradication, and recovery.

### Part 5: Reporting and Documentation

#### Step 1: Documenting Findings

1. **Create a Report**
   * Document the steps taken during monitoring, logging, analysis, and mitigation.
   * Include screenshots of configurations, logs, and mitigation measures.
2. **Summarize Results**
   * Provide a summary of detected attacks, identified IoCs, and mitigation steps implemented.

#### Step 2: Sharing Insights

1. **Internal Presentation**
   * Prepare a presentation to share findings with your team.
   * Highlight key points, lessons learned, and recommendations for improving network security.
2. **Collaboration**
   * Collaborate with peers to discuss findings, improve detection techniques, and enhance mitigation strategies.

## Conclusion

By completing this lab, you should have a solid understanding of network security monitoring, attack logging, analysis, and mitigation techniques. This knowledge is essential for effectively managing and securing network environments against potential threats.

**Experiment No-16**

SSL Proxy, Client Protection, Server Protection

## Objective

The purpose of this lab is to provide hands-on experience with SSL proxy configuration, client protection mechanisms, and server protection strategies. By the end of this lab, you should be able to configure SSL proxies, implement security measures to protect clients, and secure server environments against various threats.

## Required Tools

* A computer with virtualization software (e.g., VirtualBox, VMware)
* Virtual machines (VMs) with:
  + Linux (e.g., Ubuntu)
  + Windows (e.g., Windows Server or Windows 10)
* SSL proxy tools (e.g., Squid, Nginx)
* Security tools (e.g., antivirus software, firewalls, intrusion prevention systems)

## Lab Setup

1. **Network Configuration**
   * Set up a virtual network with multiple VMs connected to a virtual switch.
   * Ensure network connectivity between the VMs for proper traffic flow and monitoring.
2. **Software Installation**
   * Install necessary tools on appropriate VMs for SSL proxy, client protection, and server protection.

## Procedure

### Part 1: Implementing SSL Proxy

#### Step 1: Understanding SSL Proxy

* **Concept**: An SSL proxy intercepts SSL/TLS traffic, decrypts it, inspects the content, and then re-encrypts it before forwarding it to its destination.
* **Benefits**: Enhances security by allowing inspection of encrypted traffic for threats and enforcing security policies.

#### Step 2: Setting Up SSL Proxy with Squid

1. **Install Squid**
   * Install Squid on a Linux VM:

bash

Copy code

sudo apt-get install squid

1. **Generate SSL Certificates**
   * Generate a self-signed CA certificate:

bash

Copy code

sudo mkdir /etc/squid/ssl\_cert

sudo openssl req -new -newkey rsa:2048 -days 365 -nodes -x509 -keyout /etc/squid/ssl\_cert/squid.key -out /etc/squid/ssl\_cert/squid.crt

sudo cat /etc/squid/ssl\_cert/squid.crt /etc/squid/ssl\_cert/squid.key > /etc/squid/ssl\_cert/squid.pem

1. **Configure Squid for SSL Proxying**
   * Edit the Squid configuration file /etc/squid/squid.conf:

bash

Copy code

http\_port 3128 ssl-bump cert=/etc/squid/ssl\_cert/squid.pem

acl step1 at\_step SslBump1

ssl\_bump peek step1

ssl\_bump bump all

* + Restart Squid to apply the changes:

bash

Copy code

sudo systemctl restart squid

1. **Configure Client Browser**
   * Install the CA certificate on client machines to avoid SSL warnings.
   * Import the CA certificate into the browser's trusted certificate store.

### Part 2: Client Protection

#### Step 1: Understanding Client Protection

* **Concept**: Client protection involves implementing measures to safeguard end-user devices from various threats such as malware, phishing, and unauthorized access.
* **Benefits**: Ensures data integrity, privacy, and security for end-users.

#### Step 2: Implementing Antivirus and Endpoint Protection

1. **Install Antivirus Software**
   * Install antivirus software on client machines (e.g., ClamAV for Linux, Windows Defender for Windows).
2. **Configure Real-Time Protection**
   * Ensure real-time protection is enabled to detect and block threats as they occur.
   * Example for ClamAV:

bash

Copy code

sudo apt-get install clamav clamav-daemon

sudo freshclam

sudo systemctl start clamav-freshclam

sudo systemctl start clamav-daemon

1. **Schedule Regular Scans**
   * Configure the antivirus software to perform regular scans.
   * Example for ClamAV:

bash

Copy code

sudo clamscan -r /home/user

#### Step 3: Implementing Firewalls

1. **Configure Host-Based Firewalls**
   * Enable and configure firewalls on client machines (e.g., UFW for Linux, Windows Firewall for Windows).
2. **Define Firewall Rules**
   * Allow necessary traffic and block unwanted traffic.
   * Example for UFW:

bash

Copy code

sudo ufw allow 80/tcp

sudo ufw allow 443/tcp

sudo ufw enable

### Part 3: Server Protection

#### Step 1: Understanding Server Protection

* **Concept**: Server protection involves securing servers from threats such as unauthorized access, malware, and attacks.
* **Benefits**: Ensures the availability, integrity, and confidentiality of server data and services.

#### Step 2: Implementing Server Hardening

1. **Secure Configuration**
   * Disable unnecessary services and ports.
   * Example for Linux:

bash

Copy code

sudo systemctl disable telnet

sudo systemctl stop telnet

1. **Apply Security Patches**
   * Regularly update the server to apply security patches.
   * Example for Ubuntu:

bash

Copy code

sudo apt-get update && sudo apt-get upgrade

1. **Configure SSH Security**
   * Restrict SSH access and enhance its security.
   * Example:

bash

Copy code

sudo nano /etc/ssh/sshd\_config

# Set the following parameters

PermitRootLogin no

PasswordAuthentication no

AllowUsers your\_user

1. **Implement Intrusion Prevention Systems (IPS)**
   * Install and configure IPS to monitor and block malicious activities.
   * Example with Snort:

bash

Copy code

sudo apt-get install snort

sudo snort -A console -c /etc/snort/snort.conf -i eth0 -Q

#### Step 3: Monitoring and Logging

1. **Install Monitoring Tools**
   * Use tools like Nagios or Zabbix to monitor server health and performance.
   * Example for Nagios:

bash

Copy code

sudo apt-get install nagios3

1. **Configure Log Management**
   * Centralize logs using tools like ELK Stack or Splunk for better analysis.
   * Example for ELK Stack:
     + Install Elasticsearch, Logstash, and Kibana on a dedicated VM.
     + Configure Logstash to collect and parse server logs.
     + Visualize and analyze logs in Kibana.

### Part 4: Hands-On Exercise

#### Exercise 1: Implement SSL Proxy with Squid

1. **Configure SSL Proxy**
   * Follow the steps in Part 1 to configure Squid as an SSL proxy.
   * Test the configuration by accessing HTTPS websites from client machines.
2. **Inspect SSL Traffic**
   * Use Wireshark to capture and inspect decrypted SSL traffic passing through the proxy.

#### Exercise 2: Implement Client Protection Measures

1. **Install and Configure Antivirus**
   * Follow the steps in Part 2 to install and configure antivirus software on client machines.
   * Test the antivirus software by scanning for malware.
2. **Configure Firewall Rules**
   * Implement firewall rules on client machines to allow only necessary traffic.
   * Test the firewall configuration by attempting to access blocked ports.

#### Exercise 3: Implement Server Protection Measures

1. **Harden Server Configuration**
   * Follow the steps in Part 3 to harden the server configuration.
   * Test the server security by attempting to access disabled services.
2. **Configure IPS and Monitoring**
   * Install and configure an IPS on the server.
   * Set up monitoring tools to observe server performance and detect anomalies.

### Part 5: Reporting and Documentation

#### Step 1: Documenting Findings

1. **Create a Report**
   * Document the steps taken during SSL proxy configuration, client protection, and server protection.
   * Include screenshots of configurations, logs, and test results.
2. **Summarize Results**
   * Provide a summary of the implemented security measures and their effectiveness.

#### Step 2: Sharing Insights

1. **Internal Presentation**
   * Prepare a presentation to share findings with your team.
   * Highlight key points, lessons learned, and recommendations for improving security.
2. **Collaboration**
   * Collaborate with peers to discuss findings, improve security configurations, and enhance protection strategies.

## Conclusion

By completing this lab, you should have a solid understanding of how to implement SSL proxies, protect client devices, and secure server environments. This knowledge is essential for effectively managing and securing network environments against various threats.