Lab 1 & 2: Setting Up the Lab Environment

Objective: The objective of this laboratory exercise was to establish a virtual environment for network simulation using GNS3, VirtualBox, and Linux Lite, focusing on understanding various virtual machine network modes and configuring network devices.

Part 1: VirtualBox Installation VirtualBox was acquired and installed from the VirtualBox Downloads page.

Part 2: Configuring Virtual Network Modes VirtualBox was launched, and the following path was followed: Preferences -> Network -> Host Only Networks. Here, Host-Only Network and Bridged Network modes were explored and configured.

Part 3: The GNS3 Installation and was downloaded from the GNS3 Download page, selecting the 'Free Download' for the relevant operating system, and installed with the default settings. A GNS3 Community Account was created for access.

Part 4: GNS3 VM Installation If not already installed, VirtualBox was set up. The GNS3 VM file was downloaded from the GNS3 VM Download section. The downloaded .zip file was extracted, and the GNS3 VM appliance was imported using VirtualBox via the File menu, maintaining all default import settings.

Part 5: Setting Up GNS3 GUI and VM: Launched the GNS3 GUI and accessed preferences through Edit -> Preferences. Activated the GNS3 VM and selected the corresponding VirtualBox VM named 'GNS3 VM'.

Conclusion: By the end of this session, a functional GNS3 setup was established, including VirtualBox and Kali Linux, among other components.

Lab 3: Analyzing Network Packets with tcpdump

Objective: The objective for the third day was to explore network packet analysis using the tcpdump utility to gain insights into network traffic.

Lab Steps:

1. Topology Creation:
    - Designed a simple network structure within GNS3.
2. Switch Setup:
    - Prepared the switch in the GNS3 setup for packet capturing.
3. Router Configuration:
    - Adjusted router settings in GNS3 to align with lab objectives.
4. Bridge Mode Adjustment:

- Modified GNS3 network connections to bridge mode for packet capture refinement.

5. Tcpdump Utilization:
    - Deployed tcpdump command on relevant interfaces with sudo privileges for network traffic logging.
6. Connectivity Checks from Kali Linux:
    - Conducted ping tests from Kali Linux to different devices in the GNS3 network to stimulate and observe network traffic.

Section 4: Network Traffic Capture with Tcpdump

- Utilized tcpdump to log network activity within the GNS3 network setup.
- Ran tcpdump with root access to thoroughly analyze network packets.

Lab Summary: The lab successfully demonstrated tcpdump usage for network packet analysis in a GNS3 environment. The team effectively configured the packet sniffer and adjusted the network setup to bridge mode, achieving desired outcomes.

Lab 4: Exploring Wireshark and MAC Flooding

Definition: Packet analysis involves capturing and examining live data traffic on a network.

Objectives:

- Understand the principles of network sniffing.
- Gain practical experience in capturing and analyzing network traffic with Wireshark.

Lab Setup:

- Prepared a virtual environment using GNS3 alongside virtual machines to simulate a network setting.

Virtual Network Setup with GNS3:

- Added two routers to the GNS3 workspace.
- Assigned IP addresses to routers.
- Conducted ping tests between routers to stimulate network traffic.
- Commenced capturing network traffic with Wireshark.

Network Traffic Capture:

- Generated network activity on the computer, either on physical or virtual networks.
- Started virtual machines within the GNS3 topology.

- Simulated network link information exchange between virtual machines, such as accessing the router via telnet.

Task 4: Network Analysis

- Conducted a network connection test using telnet to IP address 10.0.0.1.
- Examined network behavior and traffic details through packet analysis.

Conclusion: The exercise provided practical experience in packet analysis with Wireshark, offering insights into the effects of a MAC flooding attack. It emphasized recognizing packet irregularities for identifying network issues, detecting security threats, and enhancing network security measures. The knowledge gained is applicable to real-world network management and security evaluation.

Lab 5: Cryptography - Caesar Cipher

Introduction: The session delved into cryptography through the implementation of the Caesar cipher, which shifts each letter by a fixed number of positions.

Encryption Process:

- Selected the message “meet me at noon” as the plaintext.
- Removed spaces and converted the message to lowercase for encryption.
- Defined functions to convert letters to numbers and vice versa.
- Shifted each letter of the plaintext by a predetermined key value to encrypt the message.

Decryption Process:

- Developed a decryption method to reverse the encryption and recover the original message.
- Analyzed the ciphertext to understand the encryption’s outcome.

Observations And Limitations:

- Acknowledged the Caesar cipher as a straightforward encryption method.
- Recognized its vulnerability to brute-force attacks due to the limited number of key choices.

Conclusion: The task provided hands-on experience in basic encryption and decryption processes using the Caesar cipher. It highlighted the cipher’s real-world applications and vulnerabilities, stressing the need for more secure cryptographic methods. Understanding cryptographic principles is essential for exploring advanced encryption techniques and their role in information security.

Lab 6: Investigating System Files in Kali Linux

Objective: The goal of this lab was to explore the /etc/passwd and /etc/shadow files within the Kali operating system to extract user account details and encrypted passwords, integrating this data with the extensive RockYou.txt wordlist.

Activity 1: File Exploration

- Initiated Kali Linux and used the cat command to display the contents of /etc/passwd and /etc/shadow.

Activity 2: File Merging

- Merged the contents of the passwd and shadow files using the unshadow command and saved the output to mypassword.txt.

Activity 3: Password Cracking

- Employed John the Ripper to attempt cracking the passwords by supplying the merged file along with the RockYou.txt wordlist.

Activity 4: Analysis of RockYou.txt

- Examined the RockYou.txt file, containing a vast collection of over 14 million unique passwords.

Activity 5: Password Cracking with JohnTheRipper

- Analyzed the size of the RockYou.txt wordlist and its effectiveness in cracking passwords.

Lab Instructions: Password Security Analysis

- Identified the five most frequently used passwords in the RockYou.txt file.
- Utilized Leafpad for content exploration.
- Searched for specific names within the RockYou.txt file.
- Attempted password cracking with JohnTheRipper.

Conclusions: This lab session offered practical insights into user account security and password encryption techniques within Kali systems. By examining system files, merging them, and cracking passwords using both conventional and extensive wordlists, participants deepened their understanding of password security. This knowledge is invaluable for professionals in network management, e-commerce, security, and privacy sectors, providing valuable skills for real-world applications.

Lab 7: Network Attacks

Introduction:

In the "Network Attacks" lab, various network intrusions were explored, encompassing techniques such as sniffing with TCPdump and Wireshark, MAC flooding, ARP cache poisoning, DHCP starvation, DHCP spoofing, and VLAN hopping. Each attack vector targets different vulnerabilities within network protocols and infrastructure, highlighting the importance of robust security measures.

ARP Cache Poisoning:

ARP cache poisoning, also known as ARP spoofing, exploits vulnerabilities in the Address Resolution Protocol (ARP) to intercept network traffic and perform man-in-the-middle attacks.

Procedure:

1. Set up the Kali (VirtualBox) network adapter to a Bridged Network.
2. Construct a network with at least three devices, including a Kali machine for the attack.
3. Use GNS3 for network setup.
4. Verify the ARP table on the host and Kali machine using arp -a.
5. Enable IP forwarding on the attacker’s machine to route packets using echo 1 > /proc/sys/net/ipv4/ip_forward.
6. Utilize Ettercap to automate IP forwarding.
7. Scan for hosts in the network and select a target for MITM poisoning.
8. Monitor traffic with Wireshark or tcpdump.

Preventive Measures:

- Use static ARP entries for critical servers.
- Implement secure protocols like SSH.
- Regularly update network devices and software with security patches.

DHCP Starvation & Spoofing:

The document likely continues with instructions on how to perform and prevent DHCP starvation and spoofing attacks, emphasizing the importance of understanding these attacks to secure network infrastructure and maintain data confidentiality and integrity.

Labs 8 and 9: AAA Implementation

Local AAA Implementation:

Local AAA involves configuring authentication and authorization services directly on the router.

Advantages:

- Simplicity: Users are defined directly on the router.
- Scalability: Manages multiple routers based on usernames and privilege levels without additional servers.

Disadvantages:

- Scalability limitations.
- Security concerns: User credentials are stored on the router.

Centralized AAA:

Centralized AAA utilizes a dedicated server to manage authentication, authorization, and accounting for various network devices.

Benefits:

- Scalability.
- Enhanced security.
- Centralized reporting.

Drawbacks:

- Requires additional hardware and software.
- More complex setup compared to local AAA.

Linux - Authentication, Authorization, Accounting:

This section teaches appropriate methods for authorization, authentication, and access control in Linux, alongside managing accounts based on best practices.

Lab 10: Access Control Lists (ACLs)

Abstract:

The lab involved setting up ACLs in a simulated network environment using GNS3, aiming to configure the network, apply the ACLs, and conduct tests to verify their effectiveness.

Introduction:

ACLs play a vital role in network security by allowing selective traffic flow based on set criteria. Our objective was to establish ACLs to protect the network perimeter and control internal traffic.

Task 1 - Initial Setup:

- Configured interfaces on Routers R1, R2, and R3 for interconnectivity.
- Activated RIP routing protocol across all routers for network communication.

- Assigned IP addresses to Virtual PCs to emulate network endpoints.

Task 2 - Standard ACL Setup:

Implemented commands on R3 to deny and permit specific traffic, applying the ACL to the interface.

Task 3 - Extended ACL Configuration:

Further commands were implemented on R3 for extended ACL setup, enhancing the network's security measures.

Secure VPN Connection Implementation

Overview:

The lab focused on establishing a secure VPN connection utilizing Cisco IOS technology. Participants configured fundamental device settings and set up a site-to-site IPsec VPN tunnel between routers.

Segments:

- Initial setup concentrated on device configurations such as hostnames, IP addresses, routing protocols, and passwords.
- The subsequent part involved setting up a site-to-site IPsec VPN tunnel between routers using IKE Phase 1 and 2 policies.

Insights:

The lab underscored the critical role VPNs play in securely transmitting data across public networks. Participants gained hands-on experience in implementing IKE and IPsec parameters, configuring network devices, and confirming VPN functionality. Notable modifications included the adoption of the MD5 hash algorithm, creation of a transform set, and application of encryption algorithms for enhanced security.

Lab 11: Secure VPN Connection Implementation

Overview:

Lab 11 focused on establishing a secure VPN connection utilizing Cisco IOS technology. The lab was divided into two segments: initial configuration and setting up a site-to-site IPsec VPN tunnel between routers.

Initial Configuration:

The initial part concentrated on fundamental device configurations, including:

- Setting hostnames
- Assigning IP addresses

- Configuring routing protocols
- Setting passwords
- Verifying network connectivity

Setting up Site-to-Site IPsec VPN Tunnel:

The subsequent part was dedicated to setting up a site-to-site IPsec VPN tunnel between routers. This involved employing IKE Phase 1 and 2 policies for secure communication.

Insights:

A significant insight from this exercise was the critical role VPNs play in securely transmitting data across public networks like the Internet. By adhering to provided guidelines, participants successfully created a secure VPN connection, ensuring confidentiality and integrity of data.

Hands-On Experience:

Participants acquired hands-on experience in implementing IKE and IPsec parameters to establish secure VPN tunnels. They honed their skills in configuring network devices, initiating secure communication channels, and confirming VPN functionality.

Notable Modifications:

Notable modifications in the Cisco lab documentation included:

- Adoption of the MD5 hash algorithm instead of SHA for configuring IKE Phase 1 ISAKMP policy on routers R1 and R3.
- Creation of a transform set tagged R1-R3.
- Application of an ESP transform with an AES 256 cipher within ESP.
- Application of a crypto map in step 6 to enhance security measures.