HW3

Problem R-5.3

Yes, the MAC address may be the same but it shouldn't happen because a MAC address is used to uniquely identify a device in a network. It is supposed to be unique in the same network so that the local network doesn't get confused about which device is actually communicating. However, the MAC address can be spoofed to be the same.

Problem R-5.5

IP address is a unique identifier of a device on the internet. If two devices should not have the same ip address, it will cause conflicts when two devices are trying to access the internet.

Problem C-5.4

I can encrypt my message with key K. The message would ask the server to apply its digital signature on the replied message with private key Ks. I can verify the signature with the public key Kp when I receive the reply. If the signature is valid, we are only sharing the key with the server.

Problem C-5.12

We can use VPN to prevent packets with spoofed IP addresses. The server will only allow the traffic through virtual NIC and reject the one through physical NIC. The physical NIC (network interface card) will create a virtual NIC by authentication. This process will be done and encrypted with the server's public key. First the VPN client website needs to check HTTPS to ensure the website. The clients encrypt the process with VPN public key, and encrypt symmetric session key using VPN public key. In this case, only the VPN server can decrypt using VPN private key.

Problem Mirai Botnet

DDoS attacks are intended to make a network source unavailable by sending large amounts of fake traffic from online devices.
The attacker can use some techniques to amplify the size of the request. In the example of DNS reflection, the attacker can send spoofed requests to the DNS servers that are misconfigured to allow requests from anywhere. Then, they send DNS requests whose response requires 60-70 times as large as the size of the request. This misuse of the DNS extension can cause huge traffic and result in denial of service.
In the attack on KrebsOnSecurity, the attacker first targeted vulnerable IoT devices to install the malware starting early 2015. Those infected online devices, called botnets, were under control of the attackers. Then, each IoT-based botnet would search for vulnerable devices and infect them with malware. The number of infected devices grew to a very large number by performing this process repeatedly.

One technique some companies use to secure communication and verify identity is called Generic routing encapsulation (GRE). It provides a point-to-point connection between network users and allows two users to share data privately. The feature that it cannot be faked or spoofed provides the server a way to identify the actual sender of the request. However, with this large number of infected systems, the attacker could easily pass the GRE check and generate overwhelming traffic with those devices.

Problem Network Pentesting

Based on the following article and your online research: Links to an external site.https://www.getastra.com/blog/security-audit/network-penetration-testing/
Briefly summarize the steps of network pentesting, the different types of network pentesting and the role of the following tools: Nessus, Nmap, Metasploit and Burpsuite.

Step 1: Reconnaissance
The security expert performs a vulnerability assessment on technical and human error perspectives. They will assess the system to find out possible vulnerabilities and increase employees' awareness on how to secure their information.
Step 2: Discovery
Based on information gathered from step1, tests are written and run to identify those vulnerabilities.
Step 3: Exploitation
Based on step 2, the expert will try to break into the system without being detected.

Different types of pentest:
1. Black Box. Without knowing how the system works, we mimic the real attack and try to conduct an attack.
2. Gray box. With the knowledge of the normal pattern of an attack, we simulate attacks to understand how our system behave in an average attack.
3. White box. With the knowledge of the system and its potential issues, we perform a more specific version of attacks.

Nessus is used to scan for the vulnerabilities. Usually used in step 1 to assess a system.
Nmap is used for network discovery, which is step 2.
Metasploit is used in step 3 to perform pentesting vulnerabilities in networks and servers.
Burpsuite is used to assess and discover vulnerability and perform pentesting in web apps.