IMPORTANT QUESTIONS

Compare switched LANs vs broadcast LANs from the security point of view, explain which one is more advantageous and why?

Ans:

Switched LANs and broadcast LANs are two common types of local area networks (LANs) used in networking. From a security perspective, switched LANs are generally considered more advantageous than broadcast LANs.

Switched LANs use switches to direct network traffic between devices, which means that data is only sent to the intended recipient. This enhances security by limiting the exposure of data to other devices on the network, reducing the risk of data interception and eavesdropping. In a switched LAN, each device has a unique media access control (MAC) address, which enables the switch to forward data only to the intended recipient.

In contrast, broadcast LANs use hubs to broadcast data to all devices on the network. This means that data is visible to all devices on the network, even if it is not intended for them. This makes it easier for an attacker to intercept data, leading to potential security breaches. Additionally, broadcast traffic can cause network congestion, which can lead to performance issues and make it easier for attackers to launch denial-of-service (DoS) attacks.

In conclusion, from a security perspective, switched LANs are more advantageous than broadcast LANs. Switched LANs limit data exposure to only the intended recipient, while broadcast LANs expose data to all

devices on the network. This makes switched LANs less susceptible to eavesdropping, interception, and DoS attacks.

Is it possible to sniff network on both types of LANs (switched LANs and broadcast LANs), if yes how?

Ans:

Yes, it's possible to sniff network traffic on both switched LANs and broadcast LANs. For broadcast LANs, network sniffers can be used to capture packets. For switched LANs, techniques like ARP poisoning and network taps can be used to intercept traffic. However, unauthorized network sniffing is generally illegal and unethical.

How can hacker who has got a machine connected to a network, determine whether he is on switched LAN or broadcast LAN?

Ans:

A hacker who has a machine connected to a network can determine whether it's on a switched LAN or broadcast LAN by using a network sniffer to capture traffic. On a broadcast LAN, the sniffer will capture all traffic on the network. On a switched LAN, the sniffer will only capture traffic intended for the hacker's machine and broadcast traffic. By analyzing the captured traffic, the hacker can determine whether it's on a switched or broadcast LAN.

To what extent can we provide protection against traffic analysis attacks and how?

Ans:

We can protect against traffic analysis attacks to some extent by using encryption, anonymizing services, and traffic obfuscation techniques, but these methods cannot completely eliminate the risk of such attacks.

How can the routing information be exploited for launching any security attack?

Ans:

Routing information can be exploited for launching security attacks by allowing attackers to intercept, modify, or redirect network traffic to unauthorized destinations. Attackers can use routing information to create fake routes, perform man-in-the-middle attacks, and conduct denial-of-service attacks by disrupting the routing of traffic. By manipulating routing information, attackers can gain unauthorized access to sensitive information, steal data, or take control of network resources. **OR** Routing information can be exploited to intercept, modify or redirect network traffic, leading to unauthorized access, data theft, and resource control by attackers.

How can RIP spoofing be avoided?

Ans:

RIP spoofing can be avoided by implementing various security measures, including:

Authentication: Implementing authentication mechanisms like MD5 authentication or using a shared secret key can prevent unauthorized routers from advertising incorrect routes.

Limiting access: Restricting access to routers by limiting physical access or using access control lists (ACLs) can prevent unauthorized access.

Implementing encryption: Implementing encryption like IPSec can protect routing information from being intercepted and modified by attackers.

Monitoring: Monitoring network traffic and analyzing router advertisements can help identify suspicious activities and alert network administrators.

Keeping software up-to-date: Keeping router software up-to-date can help ensure that known vulnerabilities are patched and updated, reducing the risk of exploitation.

What kinds of local/remote attacks can be launched by an attacker on a host to become an Illegal User and an Illegal Root on the said host?

Ans:

An attacker can launch various local/remote attacks to become an Illegal User or an Illegal Root on a host, including:

Password cracking: Attempting to guess or crack passwords to gain unauthorized access to the host.

Exploiting vulnerabilities: Exploiting vulnerabilities in the host's operating system or applications to gain unauthorized access or escalate privileges.

Social engineering: Using social engineering techniques to trick users into revealing their passwords or other sensitive information.

Phishing attacks: Using phishing attacks to trick users into clicking on malicious links or opening malicious attachments, leading to the installation of malware or other malicious software.

Denial-of-service attacks: Launching denial-of-service attacks against the host, causing it to become unresponsive or crash, which can potentially allow an attacker to gain unauthorized access or escalate privileges.

Consider two networks, each with its own DNS server running. A host on one network wants to get certain information from a specific site on the Internet. Using DNS spoofing, how can the hacker intercept the host's communication with the site? Give step by step procedure for the following scenarios:-

(a) When the hacker and the host are both on the same network?

Ans:

If the hacker and the host are on the same network, the hacker can intercept the host's communication with the site using DNS spoofing by setting up a fake DNS server that responds to the host's DNS requests with a spoofed IP address of the desired site, allowing the hacker to intercept and manipulate the traffic between the host and the site.