Name : Hanzala Javaid
Reg No: 4288- FBAS/BSCS4/F20
Subject: Information Security
Submitted to: Sir Qaiser Javaid.

Assignment No: 2

(Q No. 1)

(a) Compare switched vs broadcast media LANS from security point of view, briefly explain which one is more advantageous and why?

Ans:- Switched and broadcast media LANS differ in terms of how they transmit data packets across the network, and this effect the security of the network.

In switched LAN, data packets are sent only to destination device, and other devices on the network do not recieve those packets. This means that the data is more secure. Because it is not exposed to all devices on network. Switched LANS also have the ability to segment the network into VLANS.

Broadcast media LANs transmit data packets to all devices on network, regardless of whether they are intended receipents or not.

⇒ Overall, Switched LANS are generally considered more advantegeous from a security perspective due to their ability to isolate and control network traffic, whereas broadcast media LANs can be more vulnerable to security breaches.

(Q No 1)(b) Is it possible to sniff network on both types of LAN's, if yes how?

Ans:- Yes, it is possible to sniff network on both LAN's. On switched LAN, an attacker would need to gain access to physical address network switch, while on broadcast media LAN, an attacker can use a network sniffer tool to capture and analyze network traffic as it passes through network. However, unauthorized sniffing of network traffic is unethical.

(Q No. 1)(c) How can hacker who has got a machine connected to a network, determine whether he is on switched or broadcast LAN?

Ans:- One way for a hacker to determine they or in which LAN is to use a network sniffer tool to capture and analyze network traffic. On switched LAN, tool would capture traffic intended for hacker's machine while on broadcast LAN, the tool would capture all traffic on network.

(Q No. 1)(d) To what extent can we provide protection against traffic analysis attacks and how?

Ans:- Protection against traffic analysis attacks can be provided to some extent through the use of encryption techniques (VPN's, SSL etc). Those techniques can help to obfuscate the contents of network traffic, making it more difficult for attackers to infer sensitive information from traffic patterns. However, it is important to note that no protection method can provide complete

Security against traffic analysis attack.

(Q No:2) (a) How can routing information be exploited for launching any security attacks?

Ans:- Routing information can be exploited for launching security attacks by allowing an attacker to intercept, modify, or redirect network traffic, enabling them to eavesdrop on communications, steal data, or perform man-in-middle attacks.

(b) How can RIP spoofing be avoided?

Ans:- RIP spoofing can be avoided by using authentication mechanisms, such as MD5 authentication, to ensure that only trusted routers can exchange routing information.

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

Ans:- An attacker can launch local attacks such as password guessing, priveledge escalation, and backdoor to become an illegal user and illegal root on a host. Remote attacks include exploiting vulnerabilities such as remote code execution or buffer overflow to gain unauthorized access.

(Q No:3) (a) When the hacker and the host are both on same network?

(4)

Ans:- In this scenario, hacker can intercept host's communication with site DNS spoofing in following steps:

(1) Hacker sets up fake DNS server on their machine, which responds to DNS requests from host.

(2) Hosts sends a DNS request to its own DNS server to resolve domain name of target site.

(3) DNS server responds with IP address of fake DNS server set by hackers.

(4) Hosts sends fake DNS request fake DNS server, which responds with a spoofed IP address for a target site.

(5) Hosts sends request to spoofed IP-address, which is intercepted and redirected by hacker.

(b) Describe two ways hacker may carry out DNS spoofing if hosts and hacker are on separate networks.

Ans:- The two ways are following:-

(1) The hacker can use technique called "cache poisoning" to corrupt DNS cache of a DNS server and redirect traffic to a fake website.

(2) The hacker can intercept DNS requests and responses using a tool such as DNS proxy or a packet sniffer and modify responses to redirect traffic to a fake website.

(Q No-4) Consider an attack on same local network as a host (client) ---------- and the default router?

Ans:- The sequence of messages exchanged between the attacker, the host and default router in this attack as follows:-

(1) The attacker sends a forged ICMP redirect messages to the host, pretending to be the default router.
(2) The host recieves ICMP redirect messages and updates its routing table, adding attackers IP address as the new next-hop gateway for the destination network.
(3) The host sends its outbound traffic to attacker's machine instead of default router.
(4) Attacker can intercept and inspect the traffic, modify it, or forward it to intended destination.
(5) The attacker can send the traffic to the default router to avoid detection, or it can drop the traffic to perform a DOS service.

(Q No-5) Consider e-commerce company, ---------- selection criteria?

The following are some advantages and disadvantages of various password selection schemes that can be considered:

(1) Length of Passwords:

Longer passwords are more secure than shorter ones. This is because longer passwords have a greater number of possible combinations, making them harder to guess a crack. For Example, a password of 10 characters is more secure than of 6 characters.

2. Randomness of passwords:-

Enforcing randomness of passwords characters can make it harder for attackers to guess or crack passwords. This can be achieved by mixing of uppercase, lowercase, numbers and symbols.

3. User Choice of characters:-

Allowing users to choose any characters they like for their passwords may make it easier for them to remember passwords. However, this can also lead to weak passwords that are easy to guess and crack.

4. Frequency of password changes:-

Forcing users to change their passwords every six months can improve security by reducing the likelihood of passwords being compromised. However, this can also lead to users choosing weaker passwords or writing down passwords to remember them.