

**Name : Meshari Alrasheedi**

**ID : 412111606**

**Course: CS451**

**Topic: Home work**

**Q16: When a new domain is created, for example, yourdomain.com, a table in the .com domain has to receive an entry for yourdomain. What security attack might someone try against the registrar of .com (the administrator of the .com table) during the creation of yourdomain.com?**

**Ans 16:** When [invalid URL removed] was being created, the registrar of.com might have been the target of the following security attacks:   
  
The attacker may attempt to build a fictitious domain name that bears a striking resemblance to [invalid URL removed]. This could entail utilizing International Domain Names (IDNs) with characters that resemble the letters in the intended domain name, or typosquatting (e.g., replacing "o" with "0"). The purpose of this is to fool visitors into providing their details on the phony website.   
DNS hijacking: This attack involves hacking into the registrar's system to divert traffic intended for [invalid URL deleted] to a rogue website under the attacker's control. This might be utilized for phishing scams, virus distribution, or user data theft.   
Denial-of-Service (DoS) Attack: This type of attack involves flooding the registrar's system with requests, preventing genuine users from registering domains, including yours.  
Through social engineering, an attacker may attempt to fool a registrar staff member into providing them with system access or divulging private information required for registration [invalid URL removed]. Phishing emails, phone calls, or taking the identity of a real user could all be part of this.   
Exploiting software flaws in the registrar: Cybercriminals are always looking for software flaws in the registrars' software. If they locate one, they might use it to their advantage to enter the system without authorization, register [invalid URL removed] themselves, or carry out other nefarious deeds.Through social engineering, an attacker may attempt to fool a registrar staff member into providing them with system access or divulging private information required for registration [invalid URL removed]. Phishing emails, phone calls, or taking the identity of a real user could all be part of this.

**Q27: A distributed denial-of-service attack requires zombies running on numerous machines to perform part of the attack simultaneously. If you were a system administrator looking for zombies on your network, what would you look for?**

**Ans 27:** Zombies, as used in the context of network security, are compromised machines that are a member of a botnet that is utilized maliciously. A system administrator might check for the following signs to determine whether zombies are present on their network:   
Atypical Network Behavior:  
High resource consumption by idle machines: Look for hardware that uses a lot of memory or CPU but not a lot of network traffic. This can be a sign of a compromised system that is exchanging large amounts of data maliciously.   
Untrustworthy communication styles: Seek out gadgets that are interacting via odd ports or IP addresses that aren't usually connected to everyday activities.   
Ping sweeps: Use ping sweeps to find the network's active devices. Unexpected replies or unresponsive devices reported for further examination.   
Software inconsistencies:   
Unauthorized or outdated software Determine which devices are using apps that are not permitted to be used on the network or software versions that are known to have vulnerabilities.   
Security Tool Understanding:   
Alerts from security software: Use intrusion detection/prevention (IDS/IPS) or endpoint detection and response (EDR) systems to receive notifications about unusual activity or malware infestations.   
Remember: In order to confirm that a system has been compromised, more research is required. These are merely indicators. It's critical to isolate questionable devices and perform security assessments.   
It's crucial to remember that locating zombies calls for access to specific security tools and a certain degree of network management knowledge. It is best to get professional assistance if you think your personal network may be infected by zombies.

**Q30 :** **Suppose you have a high-capacity network connection coming into your home and you also have a wireless network access point. Also suppose you do not use the full capacity of your network connection. List three reasons you might still want to prevent an outsider from obtaining free network access by intruding into your wireless network.**

**Ans 30:** These are the three reasons you might want to safeguard your home Wi-Fi, even with a high-capacity connection:  
1. Security: Vulnerabilities on your devices may be exploited by others on your network to steal data or launch attacks. This could include access to other devices on your network, financial data, or private papers.  
2. Performance: Even with a high-capacity connection, unauthorized devices have the potential to consume bandwidth. This may cause your internet speeds to drop, particularly while you're streaming or playing games that demand a lot of bandwidth.  
3. Liability: Your IP address may be linked to illicit activity carried out by an unauthorized user on your network. Keeping your network secure reduces this risk.

**Q32 :** For large applications, some websites use load balancers to distribute traffic evenly among several equivalent servers. For example, a search engine might have a massive database of content and URLs, and several front-end processors that formulate queries to the database manager and format results to display to an inquiring client. A load balancer would assign each incoming client request to the least busy front-end processor. What is a security advantage of using a load balancer?

**Ans32:** Using a load balancer offers several security benefits, one of which is that it provides an additional line of defense for your vital application servers:

* Obscures Backend Infrastructure: All incoming traffic is handled by the load balancer, which serves as the public face. This conceals your backend infrastructure's specifics, including the quantity and placement of your actual application servers. Since specific application vulnerabilities are frequently the goal of attackers, concealing this information makes it more difficult for them to identify a weak point.
* Single Point of Failure Mitigation: A load balancer reduces the possibility of a single point of failure by dividing traffic among several servers. The load balancer only directs requests to the remaining operational servers in the event that an attacker is able to take down one server. This guarantees that your application will always be accessible and functional.
* Defense Against Distributed Denial-of-Service (DDoS) Attacks: Load balancers can be set up to recognize and lessen DDoS attacks. By analyzing traffic patterns and rerouting suspicious surges away from servers that are overloaded, they can save the program from going down altogether.

It's crucial to keep in mind that load balancers themselves are potential targets even when they provide security benefits. For the load balancer itself, proper configuration and security measures are still essential.

**Q43 : Do firewall rules have to be symmetric? That is, does a firewall have to block a particular traffic type both inbound (to the protected site) and outbound (from the site)? Why or why not?**

**Ans 43:** No, symmetric firewall rules are not usually required. This implies that you can permit a particular kind of data to leave your network while preventing the same data from entering it.   
  
Here's why it's not always required to use symmetric rules:   
1- Stateful Firewalls: A lot of contemporary firewalls are stateful. This implies that they do not require an explicit inbound rule because they keep track of existing connections and permit return traffic for outbound connections. For instance, in the event that a machine within your network starts a web surfing session, the firewall will permit the website's response traffic to return.

2- Security Policies: Depending on the inbound and outbound traffic, different rules may be imposed by network security policies. Users on your network may be able to access the internet (outbound traffic) but incoming connections may only be permitted to reach certain ports or services that are required for proper operation.  
  
The following are some possible disadvantages of symmetric rules:  
  
1- Complexity: Especially for large networks, managing symmetric rules for all forms of traffic can become difficult and time-consuming.  
  
2- Superfluous Restrictions: Symmetric rules have the ability to obstruct valid incoming traffic, such as updates or correspondence with outside services, which you may wish to permit.  
  
In conclusion, firewalls provide greater flexibility through asymmetric rules, enabling you to customize security policies to meet your unique requirements.