3-2 Routing attack

Types of Router Attacks

https://www.youtube.com/watch?v=IvxE6Y6qAcg

1. **Denial of Service attacks**: – The DoS attack is done by the attacker who has the motive الدافعof flooding request to the router يغرق الراوتر بطلب الخدمات or other devices affecting the availability. Sending more number of ICMP packets from multiple sources makes the router unable to process traffic.

   The Internet Control Message Protocol (ICMP) is used by network devices, including routers, to send error messages and operational information indicating. For example, a requested service is not available or a host or router could not be reached. ICMP differs from transport protocols such as TCP and UDP, it is not typically used to exchange data between systems, nor it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and trace route).

   If the router is unable to process traffic it is unable to provide services in the network and the whole network goes down affecting daily activity of organization.

   https://www.youtube.com/watch?v=glPuwhMNQ2s

2. **Packet Mistreating Attacks**: – In this type of attack after the router is injected with malicious codes, the router simply mistreats يعامل بصورة خاطئة the packets. Router cannot handle its own routing process and starts

mishandling the packet. The malfunctioned router is unable to process the packets properly and probably creates loops, denial-of-service, congestion ازدحام in the network and so on. This type of attack is very difficult to find and debug.

3. **Routing table poisoning**: – Routers use routing table to send packets in the network. The router moves the packets by looking into the routing table. The routing table is formed by exchanging routing information between routers. Routing Table Poisoning means the unwanted or malicious change in routing table of the router. This is done by editing the routing information. This attack can cause severe damage تلف كبير in the network by entering wrong routing table entries in the routing table.
4. **Hit-and-Run Attacks**: – This attack is also called Test Attack, where the attacker injects malicious packets into the router and sees if the network is online and functioning or not. If yes, the attacker sends further more malicious packets to harm the router. This attack can cause router to do unusual activities that depends on the code injected by the attacker. This type of attack is hard to identify and can cause severe damage تلف (كبير) حادto the router's work.
5. **Persistent Attacks**: – Unlike hit and run attack in this attack the attacker repeatedly injects malicious packets into the router causing the router to be unfunctionable. This attack is very severe in nature and can cause heavy damage. The router can stop functioning because of continuous malicious packet injection. This type of attack is easier to detect compared to other router attack.

3-3 Traffic Redirection

Tons of internet traffic is being deliberately diverted تحويل مقصود through locations which is not supposed to be. This attack utilize the BGP protocol.

BGP (Border Gateway Protocol) is a core routing protocol that maps out the connections for internet traffic to flow through, from source to destination. BGP has no built-in security, routers may accept dodgy متحايل connection routes advertised by peers, internet exchanges or transit suppliers.

These suspect routes, once accepted, can have local, regional or global effects. **Routers look for the shortest *logical* path (the least number of hops) and place blind trust in any path that's advertised معلن عنه.** The shortest logical path can take weird and wonderful physical geographical routes.

Reference is:
https://www.theregister.co.uk/2013/11/22/net_traffic_redirection_attacks/

3-3-1 BGP (Border Gateway Protocol) مهم

BGP (Border Gateway Protocol) is protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers. BGP directs packets between autonomous systems (AS) -networks managed by a single enterprise or service provider -. Traffic that is routed within a single network AS is referred to as internal BGP, or iBGP. More often, BGP is used to connect one AS to other autonomous systems, and then referred to as an external BGP, or eBGP

What is BGP used for?

BGP offers network stability that guarantees routers quickly adapt to send packets through another reconnection if one internet path goes down. BGP makes routing decisions based on paths, rules or network policies configured by a network administrator. Each BGP router maintains a standard routing table used for direct packets in transit. This table is used in conjunction with a separate routing table, known as the routing information base (RIB), which is a data table stored on a server on the BGP router. The RIB contains route information both from directly connected external peers, as well as internal peers, and continually updates the routing table as changes occur. BGP is based on TCP/IP and uses client-server topology to communicate routing information

BGP sends updated router table information only when something changes, and even then, it sends only the affected information. BGP has no automatic discovery mechanism, which means connections between peers have to be set up manually, with peer addresses programmed in at both ends.

BGP makes best-path decisions based on current reachability, hop counts and other path characteristics. In situations where multiple paths are available -- as within a major hosting facility -- BGP can be used to communicate an organization's own preferences in terms of what path traffic should follow in.

http://searchtelecom.techtarget.com/definition/BGP

Q: what is the ICMP?

Q: What is the difference between ICMP and TCP or UDP protocol?