Activity 5.3 : Network Security

Dominik Gonzales
Will Zhang
Shashank
Connor Caroll

Exercises 17.1, 17.3, 17.6, 17.7

17.1 The Address Resolution Protocol (ARP) associates hardware addresses with IP addresses. This association may change over time. Each network node keeps an ARP cache of corresponding IP and hardware addresses. Cache entries expire after a few minutes. A node trying to find the hardware address for an IP address that is not in its cache broadcasts an ARP request that also contains its own IP and hardware address. The node with the requested IP address replies with its hardware address. All other nodes may ignore the request. How could ARP spoofing be performed? What defences can be used against spoofing?

Answer: ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

17.3 Consider a DNS resolver that does not keep track of host names it is currently trying to resolve. Several queries for the same host name may thus be active at the same time. How can this situation be exploited by a cache poisoning attack? What is the probability of success of your attack?

Answer: The only unique introduced variable is that it doesn't keep track of the fact it already has multiple simultaneous requests from the same hostname. Sounds like it is still susceptible to standard cache poisoning attacks, just at an increased likelihood of success due to there being multiple valid responses waiting for it.

17.6 Why is dynamic port allocation a potential problem for packet filtering firewalls? Suggest a solution for requests coming from the internal network that expect answers on a dynamically allocated port. Suggest a solution for protocols where the responder specifies the port number where further queries are expected to arrive.

Answer: Dynamic Allocation is a firewall facility that can monitor the state of active connections and use this information to determine which network packets to allow through the firewall. By recording session information such as IP addresses and port numbers, a dynamic packet filter can implement a much tighter security posture than a static packet filter. To solve this problem, by tracking and matching requests and replies, a dynamic packet filter can screen for replies that don't match a request. When a request is recorded, the dynamic packet filter opens up a small inbound hole so only the expected data reply is let back through. Once the reply is received, the hole is closed. This dramatically increases the security capabilities of the firewall.

17.7 End-to-end encryption is a potential problem for application-level proxies. Suggest a solution so that a protocol encrypting its payloads can traverse an application-level proxy

Answer: A protocol encrypting its payloads can traverse through an application-level proxy by using protocol tunneling. Protocol tunneling provides a quick and easy solution, and does not require a firewall. Since only port 80 is open, it becomes a lot easier to manage the contents of the protocol.