SecureSet Prep
Introduction to Network Security 2

Glenn Webb, CISSP, GSEC

Table of Contents

MAC and IP addresses

MAC addresses vs. IP addresses

- A MAC (media access control) address of a device is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment.
    - A MAC address is comprised of six bytes
        - An example of a MAC address is 50-E5-49-39-15-D0
        - You can find your MAC address by typing `ip link`
        - A MAC broadcast address is FF:FF:FF:FF:FF:FF
- An IP (Internet Protocol) address is a numerical label assigned to each device connected to a computer network which uses the Internet Protocol for communication.
    - An IPv4 address is comprised of four bytes, dot separated, displayed in decimal
        - An example of an IPv4 address is 207.140.16.212
        - Your can find your IPv4 address by typing `ip addr`
        - An IPv4 broadcast address is one where the host portion of the IPv4 address is all one's
    - An IPv6 address is comprised of sixteen bytes, colon separated, displayed in hex
        - An example of an IPv6 address is `2001:0db8:85a3:0000:0000:8a2e:0370:7334`
        - This address can also be written as `2001:0db8:85a3::8a2e:0370:7334`

ARP

Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address associated with a given IPv4 address, a critical function in the Internet protocol suite.

ARP is used for mapping a network address such as an IPv4 address, to a physical address, such as a MAC address.

ARP Request Example

Two computers in an office (computer 1 and computer 2) are connected to each other in a local area network by Ethernet cables and network switches, with no intervening gateways or routers. Computer 1 has a packet to send to Computer 2. Through DNS, it determines that Computer 2 has the IP address `192.168.0.55`. To send the message, it also requires Computer 2's MAC address. First, Computer 1 uses a cached ARP table to look up `192.168.0.55` for any

existing records of Computer 2's MAC address (`00:eb:24:b2:05:ac`). If the MAC address is found, it sends an Ethernet frame with destination address `00:eb:24:b2:05:ac`, containing the IP packet onto the link. If the cache did not produce a result for `192.168.0.55`, Computer 1 has to send a broadcast ARP message (destination `FF:FF:FF:FF:FF:FF` MAC address), which is accepted by all computers, requesting an answer for `192.168.0.55`. Computer 2 responds with its MAC and IP addresses. Computer 2 may insert an entry for Computer 1 into its ARP table for future use. Computer 1 caches the response information in its ARP table and can now send the packet.

ARP tables

Each computer maintains a database of the mapping of Layer 3 addresses (IP addresses) to Layer 2 addresses (MAC addresses), which is maintained primarily by the reception of ARP packets form the local network link. Thus, it is often called the ARP cache or ARP table.

ARP Spoofing

This is a technique by which an attacker sends spoofed ARP messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead.

ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic. Often the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks.

The attack is confined to the local network segment that uses ARP and requires the attacker to gain direct access.

In-class Exercise

ARP spoof demonstration using arpspoof and dsniff

Port Forwarding

NAT (network address translation)

Network address translation (NAT) is a method of remapping one IP address space into another by modifying network address information in IP header of packets while they are in transit across a traffic routing device.

The technique was originally used as a shortcut to avoid the need to readdress every host when a network was moved. It has become a popular and essential tool in conserving global address space in the face of IPv4 address exhaustion. One Internet-routable IP address of a NAT gateway can be used for an entire private network.

IP masquerading is a technique that hides an entire IP address space, usually consisting of private IP addresses, behind a single IP address in another, usually public address space. The address that has to be hidden is changed into a single (public) IP address as "new" source address of the outgoing IP packet so it appears as originating not from the hidden host but from the routing device itself. Because of the popularity of this technique to conserve IPv4 address space, the term NAT has become virtually synonymous with IP masquerading.

NAT security

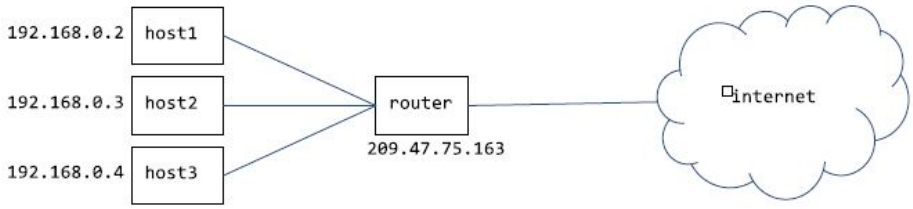
NAT provides a measure of security by limiting visibility of the devices inside the local network from the rest of the Internet.

NAT tables

The router responsible for doing NAT handles traffic from many devices. Furthermore, it handles traffic from many different source ports on each device.

The following diagrams illustrate how NAT tables containing source IP and ports of internal devices keep track of these translations.

NAT Table (handling ports)



Source IP address (private)	Source Port (private)	Source IP address (public)	Source Port (public)
192.168.0.2	50542	209.47.75.163	50542
192.168.0.3	48798	209.47.75.163	48798
192.168.0.4	50542	209.47.75.163	50544

The router tries to maintain the same source port

Suppose two devices use the same source port

The NAT table is necessary to keep track of changes

In-class discussion

What do the headers on the outbound packets from the router look like?

Port Forwarding

Local port forwarding

Allows you to access resources behind a firewall which are not exposed on the internet. Suppose you have a database server at work you want to access from home but you cannot because the corporate firewall does not allow incoming connections to the database server. Also suppose there is an SSH server at work you can access through the corporate firewall. The way to access the database server is to create an SSH tunnel using the SSH client on your home PC and the SSH server at the office.

To do this you establish an SSH connection with the SSH server and tell the client to forward traffic from a specific port from your home PC to the address of the database server and its port on the office network.

```
ssh -L 9521:192.168.0.203:1521 glenn@ssh.companyXYZ.com
```

If the database server was running on the SSH server you would use this command

```
ssh -L 9521:localhost:1521 glenn@ssh.companyXYZ.com
```

Dynamic port forwarding

This is similar to local port forwarding and is done using an SSH SOCKS proxy. The SSH client will create a SOCKS proxy you can configure applications (like your web browser) to use. This takes local traffic sent to a specific port on your PC and sends it over the SSH connection to a remote server.

For example, let's say you are using a public Wi-Fi network and you want to browse securely without being snooped on. If you have access to an SSH server at home you could connect to it and use dynamic port forwarding. The SSH client will create a SOCK proxy on your PC and all traffic sent to that proxy will be sent encrypted over the SSH connection.

```
ssh -D 8080 glenn@glennwebb.net
```

DHCP

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on TCP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters (default gateway, domain name, DNS server, and NTP servers) to each device on a network so they can communicate with other IP networks. A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices. In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address.

DHCP can be implemented on networks ranging in size from home networks to large campus networks and regional Internet service provider networks. A router or a residential gateway can be enabled to act as a DHCP server. Most residential network routers receive a globally unique IP address within the ISP network. Within a local network, a DHCP server assigns a local IP address to each device connected to the network.

The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, and time servers.

References:

https://en.wikipedia.org/wiki/IP_address
https://en.wikipedia.org/wiki/MAC_address
https://en.wikipedia.org/wiki/Address_Resolution_Protocol
https://en.wikipedia.org/wiki/ARP_spoofing
https://en.wikipedia.org/wiki/Network_address_translation
https://secureset.instructure.com/courses/383/files/5077/download?download_frd=1
https://www.howtogeek.com/168145/how-to-use-ssh-tunneling/