Additional network protocols

In previous readings and videos, you learned how network protocols organize the sending and receiving of data across a network. You also learned that protocols can be divided into three categories: communication protocols, management protocols, and security protocols.

This reading will introduce you to a few additional concepts and protocols that will come up regularly in your work as a security analyst. Some protocols are assigned port numbers by the Internet Assigned Numbers Authority (IANA). These port numbers are included in the description of each protocol, if assigned.

Network Address Translation

The devices on your local home or office network each have a private IP address that they use to communicate directly with each other. However, in order for the devices with private IP addresses to communicate with the public internet, they need to have a single public IP address that represents all devices on the LAN to the public. For outgoing messages, the router can replace a private source IP address with its public IP address and perform the reverse operation for responses. This process is known as Network Address Translation (NAT) and it generally requires a router or firewall to be specifically configured to perform NAT. NAT is a part of layer 2 (internet layer) and layer 3 (transport layer) of the TCP/IP model.

Private IP Addresses

- Assigned by the router
- Unique only within private network
- No cost to use
- Address ranges:
    - 10.0.0.0-10.255.255.255
    - 172.16.0.0-172.31.255.255
    - 192.168.0.0-192.168.255.255

Public IP Addresses

- Assigned by ISP and IANA
- Unique address in global internet
- Costs to lease a public IP address
- Assignable address ranges:
    - 1.0.0.0-9.255.255.255
    - 11.0.0.0-126.255.255.255
    - 128.0.0.0-172.15.255.255
    - 172.32.0.0-192.167.255.255
    - 192.169.0.0-233.255.255.255

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is in the management family of network protocols. DHCP is an application layer protocol used on a network to configure devices. It works with the router to assign a unique IP address to each device and provide the addresses of the appropriate DNS server and default gateway for each device. DHCP servers operate on UDP port 67 while DHCP clients operate on UDP port 68.

Address Resolution Protocol

By now, you are familiar with IP and MAC addresses. You've learned that each device on a network has a public IP address, a private IP address, and a MAC address that identify it on the network. A device's IP address may change over time, but its MAC address is permanent because it is unique to a device's network interface card. The MAC address is used to communicate with devices within the same network, but sometimes, the MAC address is unknown. This is why the Address Resolution Protocol (ARP) is needed. ARP is mainly a network access layer protocol in the TCP/IP model used to translate the IP addresses that are found in data packets into the MAC address of the hardware device.

Each device on the network performs ARP and keeps track of matching IP and MAC addresses in an ARP cache. ARP does not have a specific port number since it is a layer 2 protocol and port numbers are associated with the layer 7 application layer.

Telnet

Telnet is an application layer protocol that is used to connect with a remote system. Telnet sends all information in clear text. It uses command line prompts to control another device similar to secure shell (SSH), but Telnet is not as secure as SSH. Telnet can be used to connect to local or remote devices and uses TCP port 23.

Secure shell

Secure shell protocol (SSH) is used to create a secure connection with a remote system. This application layer protocol provides an alternative for secure authentication and encrypted communication. SSH operates over the TCP port 22 and is a replacement for less secure protocols, such as Telnet.

Post office protocol

Post office protocol (POP) is an application layer (layer 4 of the TCP/IP model) protocol used to manage and retrieve email from a mail server. POP3 is the most commonly used version of POP. Many organizations have a dedicated mail server on the network that handles incoming and outgoing mail for users on the network. User devices will send requests to the remote mail server and download email messages locally. If you have ever refreshed your email application and had new emails populate in your inbox, you are experiencing POP and internet message access protocol (IMAP) in action. Unencrypted, plaintext authentication uses TCP/UDP port 110 and encrypted emails use Secure Sockets Layer/Transport Layer Security (SSL/TLS) over TCP/UDP port 995. When using POP, mail has to finish downloading on a local device before it can be read. After downloading, the mail may or may not be deleted from the mail server, so it does not guarantee that a user can sync the same email across multiple devices.

Internet Message Access Protocol (IMAP)

IMAP is used for incoming email. It downloads the headers of emails and the message content. The content also remains on the email server, which allows users to access their email from multiple devices. IMAP uses TCP port 143 for unencrypted email and TCP port 993 over the TLS protocol. Using IMAP

allows users to partially read email before it is finished downloading. Since the mail is kept on the mail server, it allows a user to sync emails across multiple devices.

Simple Mail Transfer Protocol

Simple Mail Transfer Protocol (SMTP) is used to transmit and route email from the sender to the recipient's address. SMTP works with Message Transfer Agent (MTA) software, which searches DNS servers to resolve email addresses to IP addresses, to ensure emails reach their intended destination. SMTP uses TCP/UDP port 25 for unencrypted emails and TCP/UDP port 587 using TLS for encrypted emails. The TCP port 25 is often used by high-volume spam. SMTP helps to filter out spam by regulating how many emails a source can send at a time.

Protocols and port numbers

Remember that port numbers are used by network devices to determine what should be done with the information contained in each data packet once they reach their destination. Firewalls can filter out unwanted traffic based on port numbers. For example, an organization may configure a firewall to only allow access to TCP port 995 (POP3) by IP addresses belonging to the organization.

As a security analyst, you will need to know about many of the protocols and port numbers mentioned in this course. They may be used to determine your technical knowledge in interviews, so it's a good idea to memorize them. You will also learn about new protocols on the job in a security position.

Key takeaways

As a cybersecurity analyst, you will encounter various common protocols in your everyday work. The protocols covered in this reading include NAT, DHCP, ARP, Telnet, SSH, POP3, IMAP, and SMTP. It is equally important to understand where each protocol is structured in the TCP/IP model and which ports they occupy.

Protocol	**Port**
DHCP	UDP port 67 (servers) UDP port 68 (clients)
ARP	none
Telnet	TCP port 23
SSH	TCP port 22
POP3	TCP/UDP port 110 (unencrypted) TCP/UDP port 995 (encrypted, SSL/TLS)
IMAP	TCP port 143 (unencrypted) TCP port 993 (encrypted, SSL/TLS)

Protocol	Port
SMTP	TCP/UDP Port 25 (unencrypted)
SMTPS	TCP/UDP port 587 (encrypted, TLS)