Introduction

- IP Addresses
- MAC Addresses
- TCP and UDP
- Common Ports and Protocols
- The OSI Model
- Subnetting

Introduction

- Networking is the process of connecting two or more devices together to allow for communication and the sharing of resources.
- Penetration testers need to have a solid understanding of networking in order to be effective at their job.
- Networking concepts such as IP addresses, routing, and ports are important to understand in order to identify and exploit vulnerabilities in networked systems.

IP Addresses

- IP stands for Internet Protocol and is a unique identifier assigned to devices on a network.
- There are two versions of IP addresses: IPv4 and IPv6.
- IPv4 addresses are 32-bit numbers represented in decimal form, while IPv6 addresses are 128-bit numbers represented in hexadecimal form.
- IP addresses are used to route data packets across networks.
- IP addresses can be static or dynamic, meaning they can either be manually assigned or automatically assigned by a DHCP server.

MAC Addresses

- MAC stands for Media Access Control and is a unique identifier assigned to network interfaces.
- MAC addresses are used to identify devices on a local network.
- MAC addresses are 48-bit numbers represented in hexadecimal form.
- MAC addresses are assigned by the device manufacturer and cannot be changed.
- MAC addresses are used by the Address Resolution Protocol (ARP) to map IP addresses to MAC addresses.

TCP and UDP

- TCP stands for Transmission Control Protocol and is a connection-oriented protocol.
- TCP ensures reliable data transfer by providing error checking, flow control, and congestion control.
- TCP is used for applications that require reliable data transfer, such as web browsing and file transfer.
- UDP stands for User Datagram Protocol and is a connectionless protocol.
- UDP does not provide error checking or flow control, but it is faster than TCP.
- UDP is used for applications that can tolerate some packet loss, such as video streaming and online gaming.

Common Ports and Protocols

- TCP
  - FTP(21)
  - SSH(22)
  - Telnet(23)
  - SMTP(25)
  - DNS(53)
  - HTTP(80)/HTTPS(443)
  - POP3(110)
  - SMB(139+445)
  - IMAP(143)
- UDP
  - DNS(53)
  - DHCP(67,68)
  - TFTP(69)
  - SNMP(161)

The OSI Model

- The OSI (Open Systems Interconnection) model is a conceptual model used to describe how data is transmitted over a network.
- The OSI model consists of seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
- Each layer is responsible for a specific function in the data transmission process.
- The layers are organized in a hierarchical manner, with each layer relying on the layer below it for support.

Subnetting

- Subnetting is the process of dividing a network into smaller subnetworks.
- Subnetting allows for more efficient use of IP addresses and improves network performance.
- Subnet masks are used to determine the network portion and host portion of an IP address.
- CIDR (Classless Inter-Domain Routing) notation is commonly used to represent subnet masks.
- Pentesters may use subnetting to identify potential targets on a network and to limit the scope of their testing.