Chapter #3:

Scanning and Enumeration

Outline

- Understand EC-Council's scanning methodology
- Describe scan types and the objectives of scanning
- Understand the use of various scanning and enumeration tools
- Describe TCP communication (three-way handshake and flag types)
- Understand basic subnetting
- Understand enumeration and enumeration techniques
- Describe vulnerability scanning concepts and actions
- Describe the steps involved in performing enumeration

Phases of Hacking

- Scanning is the process of discovering systems on the network and taking a look at what open ports and applications may be running
- Footprinting – general network information about its makeup
- Scanning – goes into the network and start touching each device to find out more about them
Recipient system gets a frame
  - it checks the physical address
  - if the address is indeed correct, it opens the frame, checks to make sure the frame is valid
  - then ditches the header and trailer, passing the remainder up to the Network layer.

Layer 3 address is verified in the packet header and the header is stripped off
- The remaining PDU (Protocol Data Unit), now called a segment, is passed to Layer 4

At the Transport layer, a whole host of important stuff happens—end-to-end delivery, segment order, reliability, and flow control are all Layer 4 functions—including TCP flags and port numbering.

At the Transport layer, connectionless communication is accomplished with UDP
- It is a low-overhead, simple, and fast transport protocol
- Generally application protocols that use this transport method are moving small amounts of data
- Examples of protocols using UDP are TFTP, DNS (for lookups), and DHCP
TCP is a lot slower than connectionless but a much more orderly form of data exchange.

- Sender will establish connection before data transfer.
- Flow control during communication.
- Three-way handshake.
**TCP Header Flags**

- **SYN (Synchronize)** This flag is set during initial communication establishment. It indicates negotiation of parameters and sequence numbers.
- **ACK (Acknowledgment)** This flag is set as an acknowledgment to SYN flags. This flag is set on all segments after the initial SYN flag.
- **RST (Reset)** This flag forces a termination of communications (in both directions).
- **FIN (Finish)** This flag signifies an ordered close to communications.
- **PSH (Push)** This flag forces the delivery of data without concern for any buffering. In other words, the receiving device need not wait for the buffer to fill up before processing the data.
- **URG (Urgent)** When this flag is set, it indicates the data inside is being sent out of band. Cancelling a message mid-stream is one example.

---

**Ports**

- **Well-known ports** 0–1023
- **Registered ports** 1024–49,151
- **Dynamic ports** 49,152–65,535

---

**Active Ports**

```
Proto Local Address Foreign Address State PID
TCP 10.10.10.10:10100 10.10.10.10:10100 LISTENING
UDP 10.10.10.10:10100 10.10.10.10:10100 LISTENING
```

---

**Internet Assigned Numbers Authority**

The Internet Assigned Numbers Authority (IANA) is responsible for the global assignment of the addressing and other Internet protocol resources.
netstat

- netstat –a vs. netstat -an
- netstat –at vs. netstat –au
- netstat –lt vs. netstat –lu vs. netstat –lx
- netstat –s vs. netstat –st vs. netstat -su

Stay Alert!

There is no 100 percent secure system,
and there is nothing that is foolproof!