FIDE VIRTUAL

Curso introductorio de Ethical Hacking

Semana 01

Profesor: Randall Barnett Villalobos

Aplicación de la etapa de Reconocimiento

Parte 02

FIDE VIRTUAL

Objetivos del módulo

- Familiarizar al estudiante con el término three-way-handshake.
- Familiarizar al estudiante con la estructura de diferentes escaneos.
- Familiarizar al estudiante con términos como TCP, UDP, DNS, dirección IP, puertos y protocolos.

Requerimientos iniciales

- Se requiere del estudiante aplicar los requerimientos de la parte 01, más los que se le indicarán a continuación.
- Se requiere del estudiante asegurarse que la máquina virtual de Kali Linux tenga acceso a Internet.

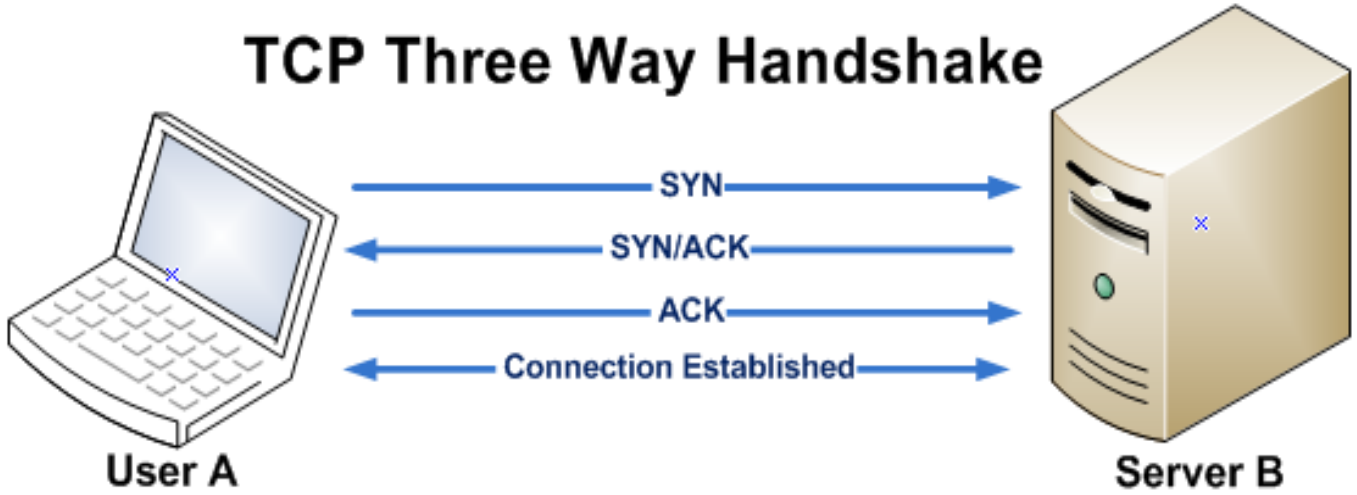
Three Way Handshake

Detalle el funcionamiento del Three-Way Handshake de TCP y su importancia.

FIDE VIRTUAL

¿Qué es Three-way Handshake?

- El proceso de "Three-way Handshake" es el procedimiento por el cual dos dispositivos intercambian una serie de mensajes a fin de poder establecer una sesión y sincronizar sus "Sequence Numbers".



¿Qué es el TCP?

- TCP o Protocolo de Control de Transmisión, es un protocolo de internet encargado de informar del destino de los datos permitiendo la creación de conexiones seguras. Aunque fue desarrollado entre 1973 y 1974, continúa siendo a día de hoy uno de los protocolos fundamentales en internet.
- TCP está basado en un modelo cliente/servidor, por lo que vamos a tener dos roles:
  - Passive Open
    - Es el rol que asume el proceso (o servicio) que está diseñado para usar TCP.
    - Espera a que los clientes se quieran conectar con el server.
  - Active Open
    - Un dispositivo envía un mensaje para iniciar una conexión (SYN)

Referencias: https://tools.ietf.org/html/rfc675

¿Qué es SYN y ACK?

- SYN. Se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo).

¿Qué es UDP?

- Intercambio de datagramas a través de una red. El protocolo de datagramas de usuario (en inglés: User Datagram Protocol o UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 o de Transporte del Modelo OSI).

¿Cuál es la diferencia entre el protocolo TCP y UDP?

- La principal diferencia entre TCP y UDP pasa fundamentalmente por el sistema de verificación de la transmisión de la información entre el dispositivo emisor y el dispositivo receptor.
- TCP es un protocolo de transporte orientado a conexión, mientras que el protocolo UDP no lo es.

Estructura de un escaneo

Tipos de escaneo.

FIDE VIRTUAL

Clasificación general de escaneos

- Activos: con los escaneos activos los resultados son más precisos pero dejamos huellas que pueden ser detectadas por firewalls o IDS activos.
- Pasivos: con los escaneos pasivos obtenemos resultados no tan precisos, pero es más difícil que seamos detectados.

Tipos de escaneos

- Escaneo Ping / Escaneo ARP: **nmap -sP -PR 192.168.1.1/24**
- Sondeo de lista: **nmap -sL 192.168.1.1/24**
- Escaneo TCP connect: **nmap -sT 192.168.1.2**
- Escaneo TCP SYN (half open): **nmap -sS 192.168.1.2**
- Escaneo TCP ACK: **nmap -sA 192.168.1.2**
- Escaneo a nivel de puertos (UDP): **nmap -PU 192.168.1.2**
- Escaneo FIN: **nmap -sF 192.168.1.2**
- Escaneo Xmas: **nmap -sX 192.168.1.2**

Mira el video

Ejecución de los comandos de escaneo.

Conclusión

FIDE VIRTUAL

Conclusión

- Recordemos que en esta fase, el objetivo es descubrir y recolectar la mayor cantidad de información del sistema objetivo del ataque, por eso es importante conocer conceots de redes como: TCP, UDP y otros.
- En esta fase mientras más ingenioso y minucioso se sea, mayores posibilidades hay de encontrar información importante para vulnerar.
- En la siguiente sesión daremos un paso más allá usando scripts y otras herramientas, que nos permitan escaneos más complejos.

Gracias