Tema 1
Escaneo de puertos

1

Escaneo de puertos

2

2

Recopilación de información

- **Nmap**
- Herramienta muy importante para realizar escaneos de equipos
- También hace un descubrimiento de equipos vivos en la red como hace netdiscover
- Esto lo lleva a cabo mediante un barrido ping

Recopilación de información

- **Nmap**
- www.nmap.org
- Hay una interfaz gráfica llamada zenmap
- Las dos están instaladas en Kali

Recopilación de información

- Primer paso: Nmap puede hace un barrido de pings a una red entera, para ver qué equipos está “vivos”
  - nmap -sn 192.168.1.0/24 (notación CIDR)
- Esto realiza un descubrimiento de equipos enviando paquetes ICMP (echo/reply) -> ping sweep
- No es un escaneo de puertos, eso lo haremos después
- Sería como lo que hace el netdiscover

Recopilación de información

- Ojo que el Windows filtra los ping (paquetes ICMP) mediante si firewall
- En este caso hacer nmap –Pn 192.168.1.0/24

Técnicas de escaneo de puertos

- El escaneo de puertos es una de las técnicas más usadas en Seguridad para descubrir servicios que puedan ser comprometidos.
- Un potencial objetivo puede ejecutar muchos servicios que escuchan en puertos conocidos.
- Escaneando estos puertos podemos encontrar vulnerabilidades potenciales (por ejemplo por bugs conocidos de ese servicio)

Técnicas de escaneo de puertos

- ¿En qué consiste entonces un escaneo?
- En mandar paquetes sin datos, como si quisiésemos abrir una conexión a un puerto (servicio) que se supone que está abierto
- Si me contesta, ya sé que ese puerto está abierto.

Técnicas de escaneo de puertos

- ¿Dónde está la correspondencia puertos – servicio?
- Es decir, la lista de puertos conocidos
- /etc/services (en Linux)
- En C:\Windows\System32\drivers\etc\services (para Windows)

Optimizar la velocidad de nmap

- **Optimización: limitar las Ips escaneadas**
- Si queremos escanear solo unos equipos de la red a la que estoy conectado, una vez detectados con netdiscover hacer:
- nmap –Pn 10.10.0.13-20
- Escanearía desde la 10.10.0.13 hasta el 10.10.0.20
- Con la opción - -open solo se muestran los puertos abiertos, no los filtrados

Otras funciones de nmap

- **Optimización: Limitación de puertos escaneados**
- Puedo escanear sólo uno o varios puertos para que sea más rápido
  - nmap –nP -sS **–p 139,145** 10.10.1.13 (puertos netbios y smb)
  - En un sistema Windows siempre están abiertos y son dos de las puertas de acceso más comunes
- También **–p 1-400** (rango de puertos)
- Si ponemos –F hará un escaneo a los 100 puertos más conocidos.
- Si ponemos - -top-port=10 serían los 10 puertos más importantes para nmap

Optimizar la velocidad de nmap

- **Optimización: velocidad de escaneo**
- La opción –n es obligatoria porque evita la resolución DNS de la víctima (para saber su nombre DNS), y muchas veces los equipos en una LAN no tienen nombre DNS
- Si no tardará mucho en hacer esta resolución
- Si no queremos dejar mucha huella y que no nos pillen podemos usar –T1 (escaneo más lento) o –T5 (escaneo más rápido), pasando por –T2, T3 y T4.
- Con –T5 va muy rápido pero llama más la atención
- Si quiero ver por dónde va el escaneo puedo pulsar cualquier tecla mientras lo hace y nos lo dirá

Más información con nmap

- **Ampliando información**
- Nmap por defecto sólo muestra si tienes o no el puerto abierto, pero no dice nada sobre el servicio que se está ejecutando, su versión, etc…
- Si queremos obtener este tipo de información usaremos la opción –sV (muy utilizado)
- La opción –sV incluye el –O (detección del Sistema operativo)
- Aunque en este caso es mejor utilizar un escáner de vulnerabilidades como Nessus

Más información con nmap

- **Ampliando información**
- Una opción muy usada es –sC
- En este caso nmap utiliza unos scripts que están desarrollados para ciertos puertos (139,445) para interactuar con el servicio y sacar más información
- La opción –a es como poner –sV –sC -O

Anonimato

- **Intentar evitar que nos pillen**
- -D 10.0.0.22,10.0.0.25: se usa para que parezca que el escaneo se realiza desde estas IP, y no solo desde la mía
- La respuesta también le llegará a estos equipos señuelos
- Los señuelos deben estar activos (verlos en netdiscover)
- Probarlo y verlo con el Wireshark
- Otras opciones en el PDF del campus

Truco práctico: otra forma manual de escanear

- Y siempre nos queda la posibilidad de usar Zenmap (la interfaz gráfica de nmap)