Escaneo de Redes

Marzo 2014

Características

- Una vez obtenida la información de un sitio potencial, la siguiente fase es explotar y analizar posibles vulnerabilidades en los servicios ofrecidos

- Normalmente explotando los canales de comunicación disponibles

Tipos

- Escaneo de Puertos – Servicios abiertos
- Escaneo de Red – Direcciones IP’s
- Escaneo de vulnerabilidades – Conocer debilidades de los sistemas

Escaneo de Redes

- Es una de las fases más importantes
- Se puede obtener información sobre un equipo con una IP específica
    - Arquitectura, sistema operativo, servicios en ejecución

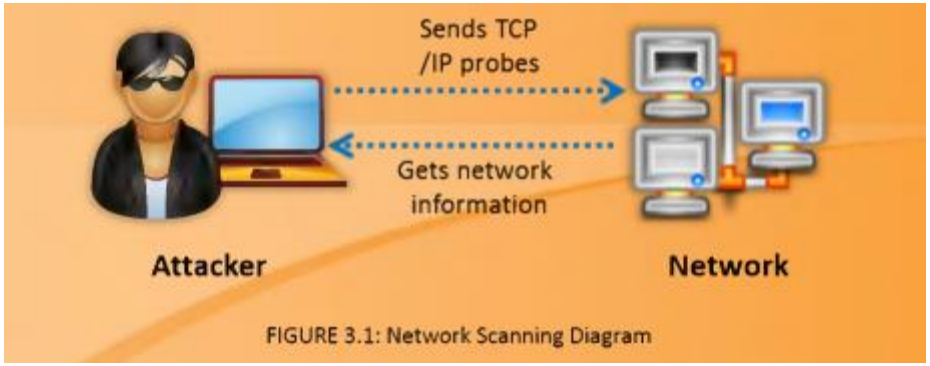
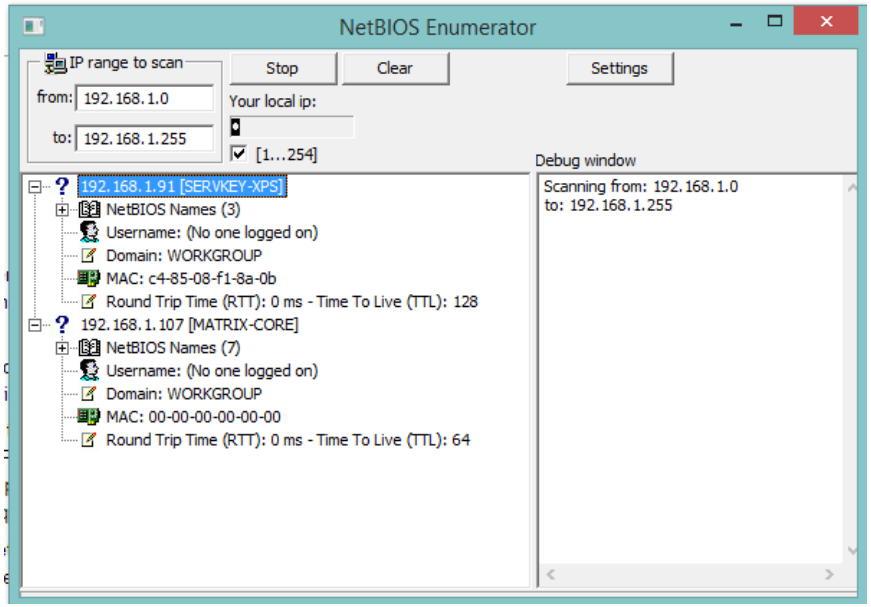


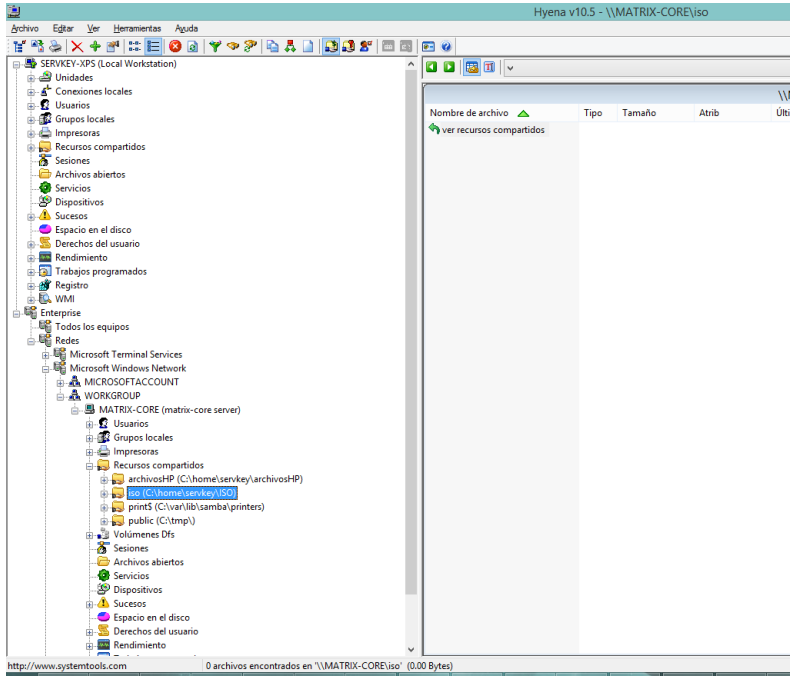
FIGURE 3.1: Network Scanning Diagram

Objetivos

- Descubrir equipos disponibles (direcciones IP) y puertos abiertos
- Descubrir sistemas operativos
- Detectar servicios de red
- Identificar vulnerabilidades

Escaneo de una LAN - NetBIOS





Actividad en clase

Buscar los siguientes conceptos

- **Equipo 1**
  - Email Tracking
  - ICMP (Internet Control Message Protocol)
  - NMAP – Zenmap y Hping
- **Equipo 2**
  - Pentesting
  - Herramientas para escanear vulnerabilidades – Nessus, GFI LanGuard, SAINT
  - Herramientas para generar diagramas de una red objetivo – LANsurveyor, OpManager

Lab 07 – Escaneo de equipos

- Implementar una aplicación gráfica que haga un escaneo de una red LAN

  - El objetivo es identificar los host activos en la red
  - Deberás poder obtener información como: arquitectura, sistema operativo, dirección MAC, nombre de equipo (ver especificación de NETBIOS)
  - 1era parte: Barrido de equipos activos
    - 1 de abril
  - 2da parte: Obtener información NETBOIS
    - 8 de abril