Escaneo de Redes

Octubre 2016

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

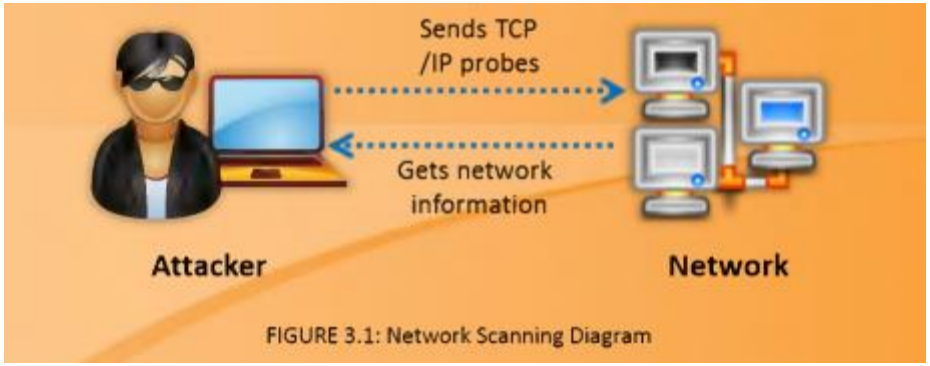
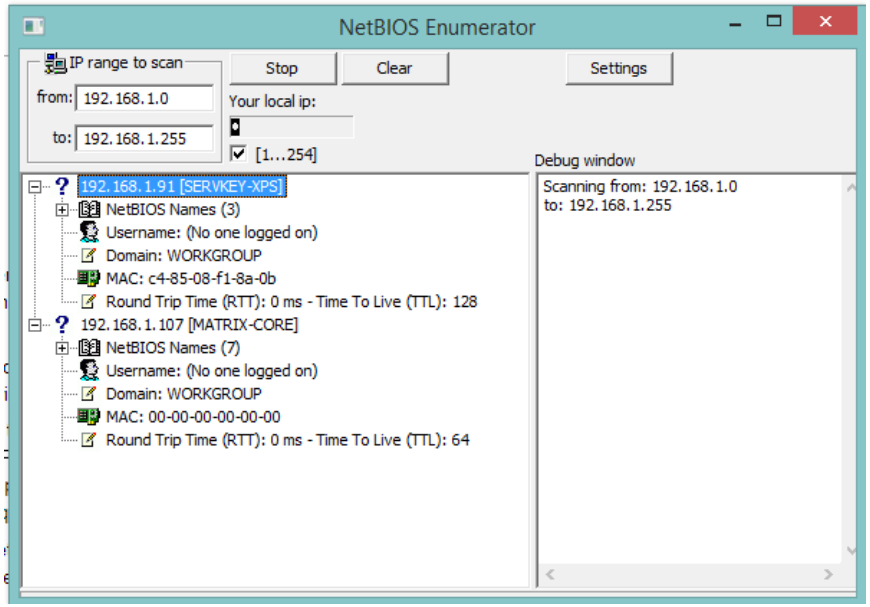


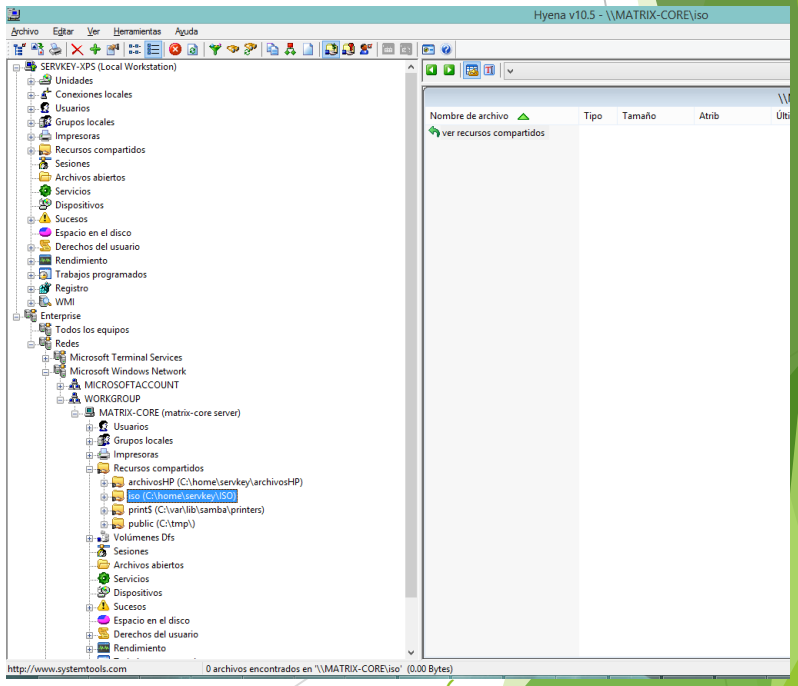
FIGURE 3.1: Network Scanning Diagram

Objetivos

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

Escaneo de una LAN - NetBIOS





Actividad

Buscar los siguientes conceptos

- **Equipo 1**
  - Email Tracking
  - NMAP – Zenmap y Hping
  - Herramientas para generar diagramas de una red objetivo – LANsurveyor, OpManager
- **Equipo 2**
  - Pentesting
  - Herramientas para escanear vulnerabilidades – Nessus, GFI LanGuard, SAINT, BackTrack