sustantiva
CON•SENTIDO

Energiza!

Técnicas Avanzadas de Reconocimiento y Escaneo

Introducción

- Reconocimiento y escaneo son fases clave del Ethical Hacking
- Permiten identificar sistemas, servicios y debilidades desde fases tempranas
- Herramientas como Nmap, Shodan, OpenVAS o Nessus facilitan esta labor
- Se requiere siempre autorización y responsabilidad ética

Reconocimiento – Definición y tipos

Reconocimiento – Definición y tipos

🔎 **Reconocimiento: Proceso de recolección de información previa al ataque**

📂 **Tipos:**

- **Pasivo:** Sin interacción directa con el objetivo
- **Activo:** Requiere consultas dirigidas hacia el sistema objetivo

Reconocimiento – Pasivo y Activo

Reconocimiento – Pasivo y Activo

🔎 Reconocimiento Pasivo:

- WHOIS: Datos del dominio y DNS
- TheHarvester: Emails, subdominios, redes sociales
- Shodan: Dispositivos conectados y servicios expuestos
    - 📌 Ejemplo: **theharvester -d empresaobjetivo.com -l 200 -b google**

🌐 Reconocimiento Activo:

- NSLookup: **nslookup -type=MX empresaobjetivo.com**
- DIG: **dig empresaobjetivo.com any**
    - 📡 Interacción directa para descubrir detalles DNS

Escaneo de Puertos y Servicios – Nmap

Escaneo de Puertos y Servicios – Nmap

🔍 **Objetivo:** detectar puertos abiertos, servicios y versiones
🧪 **Comandos clave:**

- **nmap -sS 192.168.1.100** (TCP SYN Scan)
- **nmap -sV 192.168.1.100** (Versión de servicios)
- **nmap --script=vuln IP** (Detección de vulnerabilidades)

📌 **Ejemplo completo:**
nmap -sS -sV --script=vuln www.empresaobjetivo.com
✅ Resultado: puertos abiertos, versiones y CVEs detectadas

Análisis de Vulnerabilidades – Nessus

Análisis de Vulnerabilidades – Nessus y OpenVAS

🔬 **Escáneres avanzados:**
🧰 **Nessus (comercial):**
- CVEs y configuraciones inseguras

🧰 **OpenVAS (open-source):**
- Auditoría integral, reportes visuales

📊 **Flujo de trabajo con OpenVAS:**
1. Accede a interfaz web
2. Define objetivo
3. Ejecuta análisis completo
4. Revisa el reporte

📌 **Ideal para entornos corporativos**

Simulación de Ataques + Ética Profesional

Simulación de Ataques + Ética Profesional

🎯 **Simulación controlada:**

- Metasploit: explotación de vulnerabilidades
- Sqlmap: pruebas de inyección SQL
  - 📂 Basado en hallazgos de Nmap, OpenVAS o Nessus
  - ⚠️ Solo en entornos aislados y con permiso

⚖️ **Ética Profesional:**

- Autorización y consentimiento
- Respeto a la privacidad
- Cumplimiento legal
  - ⛔ Uso indebido = consecuencias graves

Conclusión

Conclusión

✅ El reconocimiento y escaneo son pilares del análisis de seguridad

✅ Kali Linux ofrece todas las herramientas necesarias

✅ Usadas con ética, estas técnicas fortalecen la postura defensiva


Energiza!