



Curso de

Escaneo activo y análisis de vulnerabilidades

Dani Carvajal @Cisckoc



IP Logger

Recolección de inteligencia activa



Banner Grabbing

Recolección de inteligencia activa

Enumeración de subdominios

Recolección de inteligencia activa

Fingerprinting de aplicaciones web

Recolección de inteligencia activa



Identificación de WAF

Recolección de inteligencia activa



Ping y Traceroute

Recolección de inteligencia activa



Nslookup

Recolección de inteligencia activa



Netdiscover

Recolección de inteligencia activa



SSLscan

Recolección de inteligencia activa



Enum4Linux

Recolección de inteligencia activa

Análisis de dispositivos y puertos con Nmap

Inteligencia activa con Nmap

Parámetros y opciones de escaneo

Inteligencia activa con Nmap

Full TCP scan vs Stealth scan

Inteligencia activa con Nmap

FingerPrinting con Nmap

Inteligencia activa con Nmap

Escaneo agresivo con Zenmap

Inteligencia activa con Nmap

Análisis de Traceroute

Inteligencia activa con Nmap

Creación de perfiles de escaneo en Zenmap

Inteligencia activa con Nmap

Nmap scripting engine

Inteligencia activa con Nmap



Gobuster

Inteligencia misceláneos







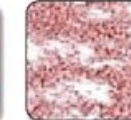






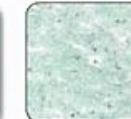

















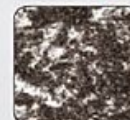










Dumpster Diving

Inteligencia misceláneos

Dumpster diving

This entails combing through someone else's trash to find treasures—or in the tech world, discarded sensitive information that could be used in an illegal manner. Information that should be securely discarded includes, but is not limited to:



P-1 ✓	P-2 ✓	P-3 ✓	P-4 ✓	P-5 ✓	P-6 ✓	P-7 ✓
						
Ancho de tira máx. 12 mm	Ancho de tira máx. 6 mm	Tamaño de partícula máx. 320 mm ²	Tamaño de partícula máx. 160 mm ²	Tamaño de partícula máx. 30 mm ²	Tamaño de partícula máx. 10 mm ²	Tamaño de partícula máx. 5 mm ²
O-1 ✓	O-2 ✓	O-3 ✓	O-4 ✓	O-5 ✓	O-6 ✓	O-7
						
Tamaño de partícula máx. 2000 mm ²	Tamaño de partícula máx. 800 mm ²	Tamaño de partícula máx. 160 mm ²	Tamaño de partícula máx. 30 mm ²	Tamaño de partícula máx. 10 mm ²	Tamaño de partícula máx. 5 mm ²	Tamaño de partícula máx. 0,2 mm ²
T-1 ✓	T-2 ✓	T-3 ✓	T-4 ✓	T-5 ✓	T-6 ✓	T-7
						
Utilizado mecánicamente	Tamaño de partícula máx. 2000 mm ²	Tamaño de partícula máx. 320 mm ²	Tamaño de partícula máx. 160 mm ²	Tamaño de partícula máx. 30 mm ²	Tamaño de partícula máx. 10 mm ²	Tamaño de partícula máx. 2,5 mm ²
E-1 ✓	E-2 ✓	E-3 ✓	E-4 ✓	E-5 ✓	E-6	E-7
						
Utilizado mecánicamente/ electrónicamente	Partido	Tamaño de partícula máx. 160 mm ²	Tamaño de partícula máx. 30 mm ²	Tamaño de partícula máx. 10 mm ²	Tamaño de partícula máx. 1 mm ²	Tamaño de partícula máx. 0,5 mm ²
F-1 ✓	F-2 ✓	F-3 ✓	F-4 ✓	F-5	F-6	F-7
						
Tamaño de partícula máx. 160 mm ²	Tamaño de partícula máx. 30 mm ²	Tamaño de partícula máx. 10 mm ²	Tamaño de partícula máx. 2,5 mm ²	Tamaño de partícula máx. 1 mm ²	Tamaño de partícula máx. 0,5 mm ²	Tamaño de partícula máx. 0,2 mm ²
H-1	H-2	H-3	H-4 ✓	H-5 ✓	H-6	H-7
						
Utilizado mecánicamente/ electrónicamente	Dañado	Deformado	Varias veces partido y deformado, Tamaño de partícula máx. 2000 mm ²	Varias veces partido y deformado, Tamaño de partícula máx. 320 mm ²	Varias veces partido y deformado, Tamaño de partícula máx. 10 mm ²	Varias veces partido y deformado, Tamaño de partícula máx. 5 mm ²



Ingeniería Social

Inteligencia misceláneos



Recolección de datos

- Solicitar información a través de medios oficiales.
- Solicitar información de acceso wifi en algún establecimiento.
- Complementar información.



Nmap

Análisis de vulnerabilidades



Joomscan

Análisis de vulnerabilidades



Wpscan

Análisis de vulnerabilidades



Nessus Essentials

Análisis de vulnerabilidades

Vega

Análisis de vulnerabilidades