

# **Bloque 3.- Técnicas, herramientas y soluciones.**

**Mitre, Shodan, Kali**



# Tabla de contenidos

- Herramientas de ciberseguridad
- Mitre
- Shodan
- Kali

# Tabla de contenidos

- **Herramientas de ciberseguridad**
- Mitre
- Shodan
- Kali

# Herramientas de ciberseg.

- **Decodificadores de contraseñas**

Las herramientas para decodificar contraseñas a menudo se les conoce como herramientas de recuperación de contraseña y pueden ser usadas para decodificar o recuperar una contraseña. Los decodificadores de contraseñas hacen intentos repetidos para averiguar la contraseña. Ej: John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack y Medusa.

- **Herramientas de hacking inalámbrico**

Las herramientas de hacking inalámbrico se utilizan para hackear intencionalmente una red inalámbrica con el fin de detectar vulnerabilidades en la seguridad. Ej: Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep, and ViStumbler.

- **Escaneo de redes y herramientas de hacking**

Las herramientas de análisis de red se utilizan para sondear dispositivos de red, servidores y hosts para puertos TCP o UDP abiertos. Ej: Nmap, SuperScan, Angry IP Scanner y NetScanTools.

- **Herramientas para elaborar paquetes de prueba**

Estas herramientas se utilizan para sondear y probar la solidez de un firewall usando paquetes especialmente diseñados. Ej: Hping, Scapy, Socat, Yersinia, Netcat, Nping y Nemesis.

- **Sniffers de paquetes**

Estas herramientas se utilizan para capturar y analizar paquetes dentro de redes tradicionales LAN Ethernet o WLAN. Ej: Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy y SSLstrip.

# Herramientas de ciberseg.

- **Detectores de Rootkits**

Se trata de un comprobador de integridad de archivos y directorios utilizado por hackers de sombrero blanco para detectar rootkits instalados. Ej: AIDE, Netfilter y PF: OpenBSD Packet Filter.

- **Fuzzers para buscar vulnerabilidades**

Los fuzzers son herramientas usadas por los atacantes cuando intentan descubrir las vulnerabilidades de seguridad de una computadora. Ej: Skipfish, Wapiti y W3af.

- **Herramientas de informática forense**

Estas herramientas son utilizadas por los hackers de sombrero blanco para detectar cualquier rastro de evidencia existente en una computadora. Ej: Sleuth Kit, Helix, Maltego y Encase.

- **Depuradores**

Los hackers de sombrero negro utilizan estas herramientas para aplicar ingeniería inversa en archivos binarios cuando programan ataques. También las utilizan los sombreros blancos cuando analizan malware. Ej: GDB, WinDbg, IDA Pro e Immunity Debugger.

# Herramientas de ciberseg.

- **Sistemas Operativos para hacking**

Estos son sistemas operativos especialmente diseñados precargados con herramientas optimizadas para hacking. Ej: Kali Linux, BackBox Linux, parrot linux.

- **Herramientas de Cifrado**

Las herramientas de encriptación utilizan esquemas de algoritmo para codificar los datos a fin de prevenir el acceso no autorizado a los datos encriptados. Ej: VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN y Stunnel.

- **Herramientas para atacar vulnerabilidades**

Estas herramientas identifican si un host remoto es vulnerable a un ataque de seguridad. Ej: Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit y Netsparker.

- **Escáneres de vulnerabilidades**

Estas herramientas analizan una red o un sistema para identificar puertos abiertos. También pueden utilizarse para escanear vulnerabilidades conocidas y explorar máquinas virtuales, dispositivos BYOD y bases de datos de clientes. Ej: Nipper, Core Impact, Nessus, SAINT y OpenVAS.



# Tabla de contenidos

- Herramientas de ciberseguridad
- **Mitre**
- Shodan
- Kali

# Mitre Att&ct

- The **MITRE Corporation**, conocida comúnmente como MITRE es una organización estadounidense sin ánimo de lucro localizada en Bedford, Massachusetts y McLean, Virginia. (<https://www.mitre.org/about/our-history>)
  - **Mitre ATT&CK**: significa tácticas, técnicas del adversario (ATT). Su misión es capturar las técnicas, tácticas y procedimientos (TTP) de las amenazas persistentes avanzadas (APT) que se dirigen principalmente a dispositivos. (<https://attack.mitre.org/>)
  - **Mitre ATT&CK Navigator**: es una herramienta basada en la web para anotar y explorar las matrices ATT&CK. Puede utilizarse para visualizar la cobertura defensiva, la planificación del blue/red team, la frecuencia de las técnicas detectadas, etc. (<https://mitre-attack.github.io/attack-navigator/>)
  - **Mitre D3FEND**: herramienta para contramedidas. (<https://d3fend.mitre.org/>)



# Mitre Att&ct

- **Objetivo:**
  - ¿Cómo entra el atacante?
  - ¿Cómo se mueve?
  - Identificar técnicas específicas de los adversarios
  - Nivel de visibilidad del entorno contra ataques dirigidos
- **Tácticas, técnicas y procedimientos (TTP):**
  - Las **técnicas (Txxxx)** son las herramientas.
  - La **táctica (TAxxx)** es la forma de combinar esas herramientas para hacer un determinado trabajo.
  - El **procedimiento** es la guía a seguir para hacer el trabajo.

# Mitre Att&ct

- **Técnicas:**
  - Cada táctica (forma de combinar) tiene un determinado número de técnicas (herramientas) e incluso sub-técnicas que llevan finalmente al procedimiento para el ataque.

**TÁCTICA**

MitRE ATT&CK® Navigator

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
Drive-by Compromise	AppleScript	bash_profile and bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Compiled HTML File	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	add to selection	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Component Object Model and Distributed COM	AppCert DLLs	AppCert DLLs	Bypass User Account Control	Credential Dumping	remove from selection	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Control Panel Items	Application Shimming	Application Shimming	Clear Command History	Credential from Web Browser	select all	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Dynamic Data Exchange	Authentication Package	Authentication Package	Code Signing	Credential Files	invert selection	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Execution through API	BITS Jobs	Dylib Hijacking	Compiled HTML File	Cryptocurrency Wallets	view technique	Network Sniffing	Data from Removable Media	Data Obfuscation	Firmware Corruption	
Spearphishing via Service	Execution through Module Load	Bootkit	Dylib Hijacking	Component Firmware	Exploitation for Credential Access	Network Sniffing	Pass the Hash	Exfiltration Over Other Network Medium	Exfiltration Over Physical Medium	Inhibit System Recovery	
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Elevated Execution with Prompt	Connection Proxy	Forced Authentication	Permission Groups	Process Discovery	Exfiltration Over Scheduling Transfer	Exfiltration Over Scheduling Transfer	Network Denial of Service	
Trusted Relationship	InstallUtil	Change Default File Association	Emond	Control Panel Items	Hooking	Input Capture	Query Registry	Resource Hijacking	Runtime Data Manipulation	Service Stop	
Valid Accounts	Launchctl	Component Object Model Hijacking	DCShadow	Deobfuscate/Decode Files or Information	Kerberoasting	Input Prompt	Remote System Discovery	Stored Data Manipulation	System Shutdown/Reboot	System Shutdown/Reboot	
	Local Job Scheduling	Create Account	Deobfuscate/Decode Files or Information	Disabling Security Tools	Keychain	LLMNR/NBT-NS Poisoning and Relay	Software Discovery	System Shutdown/Reboot	Transmitted Data Manipulation	Transmitted Data Manipulation	
	LSASS Driver	DLL Search Order Hijacking	DLL Search Order Hijacking	DLL Side-Loading	Network Sniffing	System Information	Third-party				
	Mshta	Dylib Hijacking	Hooking	Execution Guardrails							
	PowerShell										

**TÉCNICA**

**PROCEDIMIENTO (view technique)**



# Mitre Att&ct

- **Tácticas (I):**
  - **Reconocimiento:** recopilación de información para planificar futuras operaciones del adversario (información sobre la organización objetivo).
  - **Desarrollo de recursos:** establecer recursos para respaldar las operaciones (establecer una infraestructura de comando y control).
  - **Acceso inicial:** intentar ingresar a su red (phishing, ...).
  - **Ejecución:** intentar ejecutar código malicioso (ejecutar una herramienta de acceso remoto).
  - **Persistencia:** tratar de mantener su punto de apoyo (cambiar configuraciones).
  - **Escalada de privilegios:** intentar obtener permisos de nivel superior (aprovechar una vulnerabilidad para elevar el acceso).
  - **Defense Evasion:** tratar de evitar ser detectado (utilizar procesos confiables para ocultar malware).

# Mitre Att&ct

- **Tácticas (II):**
  - **Acceso a credenciales:** robo de nombres y contraseñas de cuentas (registro de teclas, ...).
  - **Descubrimiento:** tratar de descubrir su entorno (explorar lo que pueden controlar).
  - **Movimiento lateral:** moverse a través de su entorno (usar credenciales legítimas para el uso de múltiples sistemas).
  - **Recopilación:** recopilar datos de interés para el objetivo del adversario (acceder a los datos en el almacenamiento en la nube).
  - **Comando y control:** comunicarse con sistemas comprometidos para controlarlos (imitar el tráfico web normal para comunicarse con una red de víctimas).
  - **Exfiltración:** robar datos (transferir datos a una cuenta en la nube).
  - **Impacto:** manipular, interrumpir o destruir sistemas y datos (cifrar datos con ransomware).

# Mitre Att&ct

- **Procedimientos:**

- Describe la forma en que los adversarios o el software implementan una técnica (herramienta).
- Es una instancia particular de uso
- Puede ser muy útil para comprender exactamente cómo se usa la técnica (herramienta) y para la replicación de un incidente con la emulación del adversario y para obtener detalles sobre cómo detectar esa instancia.
- Ej: EternalBlue (CVE-2017-0144) – T1210 (Lateral Movement) – Technique Exploitation of Remote Services – Procedure: S0532 Lucifer can exploit multiple vulnerabilities including EternalBlue (CVE-2017-0144) and EternalRomance (CVE-2017-0144) (<https://attack.mitre.org/techniques/T1210/>)

# Tabla de contenidos

- Herramientas de ciberseguridad
- Mitre
- **Shodan**
- Kali



# Shodan

- Qué es Shodan:
  - Shodan es un motor de búsqueda para dispositivos conectados a Internet (no para buscar sitios webs – Google)
  - Recopila información pública sobre todos los dispositivos conectados a Internet a partir de sus banners.
  - Puede responder a preguntas como:
    - qué países están más conectados?
    - qué versión de Microsoft IIS es la más popular?
    - ...
  -

# Shodan

- Objeto banner:
  - Cada objeto banner puede tener distintas propiedades en función de la información pública del dispositivo. Ej:
    - data: respuesta principal sobre el dispositivo
    - ip\_str: dirección IP
    - port: puerto del servicio que proporciona el dispositivo
    - org: organización/empresa a la que pertenece el dispositivo
    - location.country\_code: código de país en el que está el dispositivo que está dentro de la propiedad "location".

```
{
  "data": "Moxa Nport Device
          Status: Authentication disabled
          Name: NP5232I_4728
          MAC: 00:90:e8:47:10:2d",
  "ip_str": "46.252.132.235",
  "port": 4800,
  "org": "SingTel Mobile",
  "location": {
    "country_code": "SG"
  }
}
```

# Shodan

- Objeto banner:
  - Otros ejemplos:

```
Copyright: Original Siemens Equipment
PLC name: S7_Turbine
Module type: CPU 313C
Unknown (129): Boot Loader          A
Module: 6ES7 313-5BG04-0AB0  v.0.3
Basic Firmware: v.3.3.8
Module name: CPU 313C
Serial number of module: S Q-D9U083642013
Plant identification:
Basic Hardware: 6ES7 313-5BG04-0AB0  v.0.3
```

```
HTTP/1.1 200 OK
Server: nginx/1.1.19
Date: Sat, 03 Oct 2015 06:09:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 6466
Connection: keep-alive
```

# Tabla de contenidos

- Herramientas de ciberseguridad
- Mitre
- Shodan
- Kali

# Kali

- Qué es Kali:
  - Kali Linux es una distribución de seguridad derivada de Debian y diseñada específicamente para la seguridad informática, el análisis forense informático y las pruebas de penetración avanzadas.
  - Desarrollada mediante la reescritura de la distribución de BackTrack por Mati Aharoni y Devon Kearns de Offensive Security.

# Kali

- Herramientas (categorías):
  - Recopilación de Información.
  - Análisis de Vulnerabilidades.
  - Análisis de Aplicaciones Web.
  - Evaluación de Bases de Datos.
  - Ataques de Contraseñas.
  - Ataques Wireless.
  - Ingeniería Inversa.
  - Herramientas de Explotación.
  - Sniffing y Spoofing.
  - Post Explotación.
  - Análisis Forense.
  - Herramientas de Reporte.
  - Herramientas de Ingeniería Social.



# Kali

- Metasploit
  - Metasploit Framework es un proyecto de código abierto que proporciona un recurso público para investigar vulnerabilidades y desarrollar código que permite a los profesionales de la seguridad infiltrarse en su propia red e identificar riesgos y vulnerabilidades de seguridad (<https://www.metasploit.com>).
  - Escanear una red o un entorno que no es el tuyo podría considerarse ilegal en algunos casos.

# Tabla de contenidos

- Herramientas de ciberseguridad
- Mitre
- Shodan
- Kali

# Técnicas, herramientas y soluciones

