Open-Sec

They run automated tools, We have Pentesters

RED TEAM : BREAKING SECURITY FOR REAL

William Marchand
Pentester / Red Teamer
wmarchand@open-sec.com

Luis Morales
Pentester / Red Teamer
lmorales@open-sec.com

Alexis Torres
Pentester / Red Teamer
atorres@open-sec.com

Walter Cuestas
Pentester / Red Teamer
wcuestas@open-sec.com

CORE TEAM

Venimos desde

Research & Conferencias & Trainings

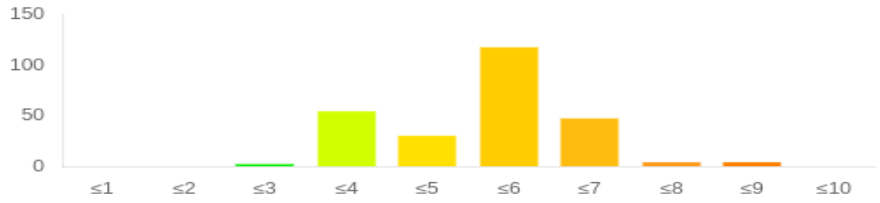
DEF CON 26 (2018)

Cuáles son las vulnerabilidades hoy día ?

CVSS Current Top 5 »

Top vulnerabilities with the highest **CVSSv3 temp scores** at the moment. The score is generated by separate values which are called vectors. Those vectors define the structure of the vulnerability. They rely on attack prerequisites and impact. The calculated score ranges between 0.0 and 10.0 whereas a high value declares a high risk. The main score is the base score which analyses the structure of the vulnerability only. The extended score called temp score introduces time-based aspects like exploit and countermeasure availability. Our moderators classify every entry to generate a CVSS score as accurate as posible.

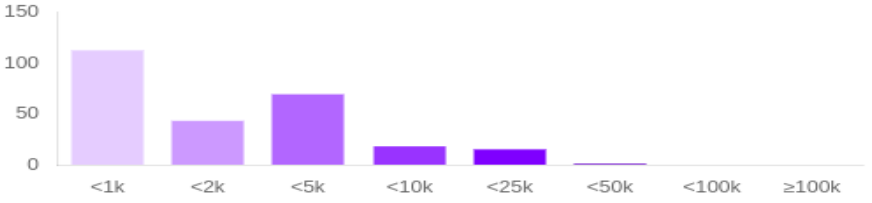
- 8.8 Cisco Prime Infrastructure/Evolved Programmable Network We...
- 8.8 Cisco Prime Infrastructure/Evolved Programmable Network We...
- 8.8 Cisco Prime Infrastructure/Evolved Programmable Network We...
- 8.4 Fujitsu PaperStream IP FJTWSVIC Service UninOldIS.dll Change...
- 7.5 UCMS ceditpost.php sql injection



Exploit Price Current Top 5 »

Top vulnerabilities with the highest **exploit price** at the moment. These price estimations are calculated prices based on mathematical algorithm. This algorithm got developed by our specialists over the years by observing the exploit market structure and exchange behavior of involved actors. It allows the prediction of generic prices by considering multiple technical aspects of the affected vulnerability. The more technical details are available the higher the accuracy of the reproducable approximation.

- $25k-$50k IBM WebSphere Application Server privilege escalation
- $10k-$25k IBM Cloud Private Kubernetes API Server HTTP Proxy un...
- $10k-$25k Cisco NX-OS CLI command injection memory corruption
- $10k-$25k QEMU commands*.c memory corruption
- $10k-$25k Cisco Prime Infrastructure/Evolved Programmable Netwo...

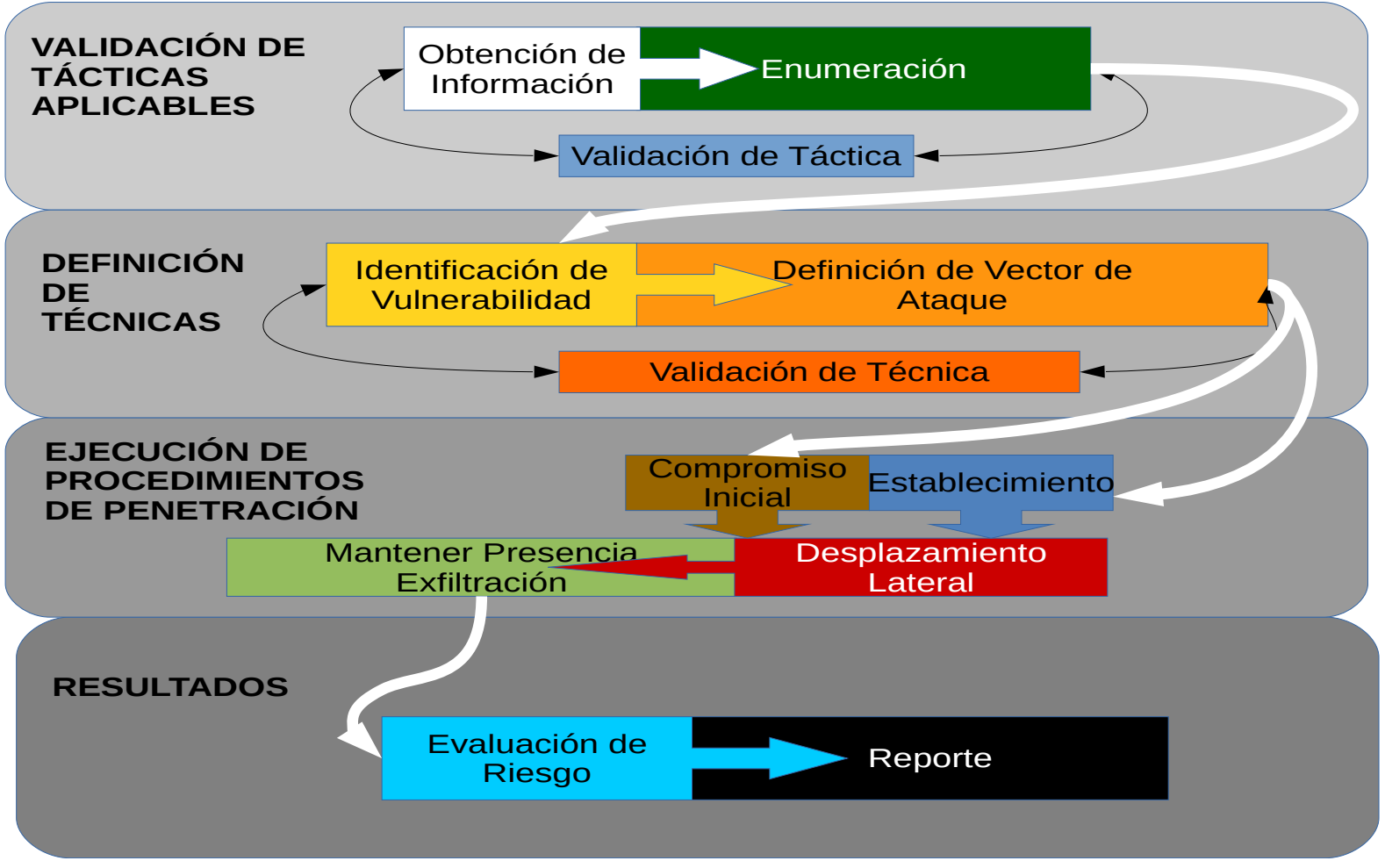


Nuestra perspectiva del Red Teaming

Qúe proponemos ?

- Realizar un proceso que permita evaluar :
  - Tiempo para Detectar (TTD)
  - Tiempo para Mitigar (TTM)
- Comprobar la eficacia de servicios Blue :
  - SOC
  - Blue Team (externo y/o interno)
  - Herramientas Tecnológicas (ML, AI, SIEM, etc.)
- Comprobar los procesos relacionados a seguridad a todo nivel
- Buscar valores diferenciales con respecto a un Pentest

Framework desarrollado por Open-Sec para Red Teaming



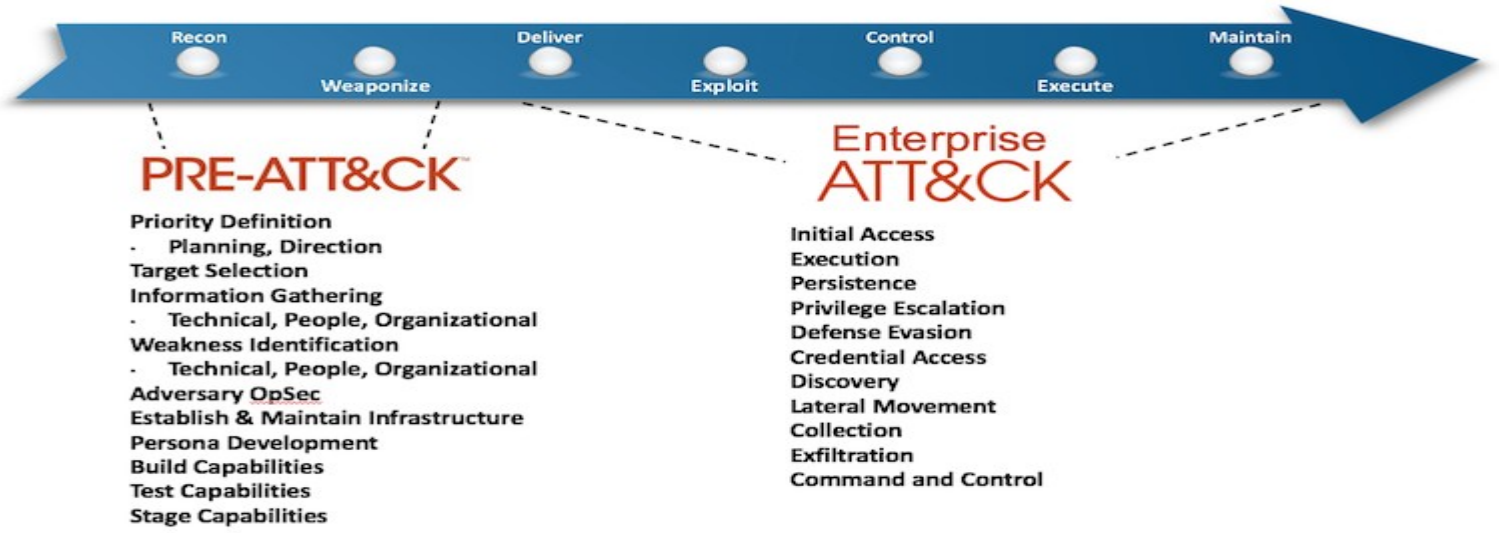
Modelos de Red Teaming según Madurez

- Madurez baja = Ejercicio Básico
  - Características
    - Superficie de ataque limitada
    - No se han hecho ejercicios previos
  - Desarrollar
    - Planificación en mesa de escenarios de pruebas
    - Definir Pruebas de Concepto
- Madurez media = Ejercicio Intermedio
  - Características
    - Han conducido pruebas de seguridad con una frecuencia y alcance establecidos como estándar
  - Desarrollar
    - Alinearse con pruebas de seguridad realizadas
- Madurez alta = Ejercicio Avanzado
  - Características
    - Presupuesto dedicado a pruebas de seguridad incluyendo red teaming
    - Se cuenta con protección **tipo** Blue Team
    - Escenarios sofisticados
    - Establecimiento de remediaciones durante el ejercicio
  - Desarrollo
    - Mayor tiempo de ejecución
    - Inclusión de pruebas "no planificadas"

Y ATT&CK para cuando ?

ATT&CK™

Adversarial Tactics, Techniques, and Common Knowledge



Todo esto es propiedad de MITRE, por si acaso...

Pero, los “blue” tienen mas estándares...

TIBER-EU FRAMEWORK

How to implement the
European framework for Threat
Intelligence-based Ethical
Red Teaming

May 2018

BANK OF ENGLAND

CBEST

CBEST Intelligence-Led Testing

CBEST Implementation Guide

Version 2.0

Cómo llevamos a cabo un Ejercicio de Red Teaming ?

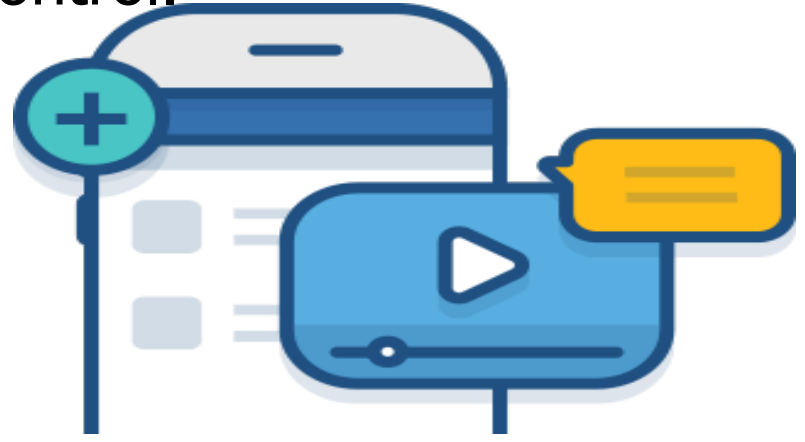
Siempre hay planificación, no es un ataque real

Definición de objetivos conjuntamente con el cliente.

Firma de acuerdos de confidencialidad.

Establecimiento de Puntos de Control.

Sustentación de Informe final.



Pero, ahora si, de verdad, que es un Red Teaming ?

Discovery EXTENSO : OSINT (o como le quieran llamar)

- DeepWeb ? SI !

Más opciones “pasivas”

- Redes sociales, por su puesto, pero, también recopilación de fuentes diversas respecto a :
  - Infraestructura tecnológica
  - Perfil de las personas
  - PROCESOS ←
  - ELEMENTOS DE DEFENSA ←
- No hay herramienta mágica, aún hay mucho esfuerzo manual en recopilar, analizar y elucubrar y funciona!

Y las “activas” para cuando ?

- Algo no cambia : activa en esta etapa es cualquier acción que “toca” el target
  - No recomendable
  - Si se realiza, debe ser después de tener definidos vectores de ataque y los posibles elementos de defensa
  - Evitar las herramientas “masivas”
    - Se requiere precisión, no precocidad…
  - Los servicios de Microsoft han sido buena opción en los últimos años
    - Office 365, Exchange/OWA, Sharepoint, Skype for Business
    - Password Spraying

Un alto : Se lad defensiva”

"Faking security is the path to the dark side. Faking leads to false hope. False hope leads to false security. False security leads to suffering."

Verídico de Star Wars


HOLA SOY CESAR
CUADRA DE
SOPORTE TECNICO Y
ESTAMOS MIGRANDO
EL CORREO
ELECTRONICO...

Open-Sec

"Sí te conoces a ti mismo y conoces a tu enemigo, no debes temer el resultado de cientos de batallas."

Sun Tzu, El Arte de la Guerra