



Ciberseguridad



Red/Blue/Purple Team



#SOMOSVALLIANS



00

Quién Soy?

accenture



José Antonio Garcia Cartagena

Solutions Architect @AWS

01

Fundamentos

¿Qué son los Equipos de Seguridad?



No son enemigos, son colaboradores con roles diferentes



RED TEAM - El Atacante Ético

Función: Equipo de ataque ofensivo.

Objetivo: Simular adversarios reales para encontrar vulnerabilidades y brechas de seguridad antes de que un atacante las explote.

Actividades: Realizan pruebas de penetración, simulan ataques técnicos y buscan activamente fallos en las defensas.



Cyber Kill Chain





BLUE TEAM – El Defensor

Función: Los «defensores» que protegen los sistemas y redes de la organización.

Objetivo: Detectar amenazas, responder a incidentes de seguridad y mantener la postura de seguridad general de la organización.

Actividades: Supervisión de la red, respuesta a incidentes, gestión de vulnerabilidades y aplicación de parches y correcciones de seguridad.



PURPLE TEAM – El Colaborador

Función: Los «colaboradores» que actúan como puente entre los equipos rojo y azul.

Objetivo: Mejorar la seguridad general mediante la creación de un ciclo de retroalimentación continua en el que ambos equipos comparten información y trabajan juntos para reforzar las defensas y mejorar las capacidades de detección.

Actividades: Ejercicios conjuntos en los que el equipo azul conoce las acciones del equipo rojo, lo que permite el análisis y la comunicación en tiempo real sobre las técnicas de ataque y las respuestas defensivas. El equipo morado se asegura de que las lecciones aprendidas de los ataques del equipo rojo se incorporen rápidamente a las estrategias defensivas del equipo azul.



MITRE ATT&CK Framework

Marco de referencia para tácticas y técnicas de adversarios

TÁCTICAS (Qué quieren lograr):

Reconocimiento → Acceso Inicial → Ejecución
Persistencia → Escalada → Evasión
Movimiento Lateral → Exfiltración → Impacto

14 tácticas | 193 técnicas | 401 sub-técnicas

MITRE ATT&CK vs. CYBER KILL CHAIN

MITRE ATT&CK

- Acceso inicial
- Ejecución
- Persistencia
- Escalada de privilegios
- Evasión de defensa
- Acceso a credenciales
- Descubrimiento
- Movimiento lateral
- Recopilación
- Exfiltración
- Comando y control

CYBER KILL CHAIN

- Reconocimiento
- Intrusión
- Explotación
- Escalada de privilegios
- Movimiento lateral
- Ofuscación / Antiforense
- Negación de servicio
- Exfiltración



Casos Reales de Red Team

Caso 1: Penetración Física + Cyber

Red Team infiltra oficinas y conecta dispositivo

Lección: Seguridad física es crucial

Caso 2: Phishing Dirigido

Email falso de CEO solicita transferencia

Lección: Entrenar contra ingeniería social

Caso 3: Explotación de API

API sin rate limiting permite enumeración

Lección: Asegurar todas las interfaces

68% de organizaciones realizan ejercicios Red Team



Try Hack Me!





¡Kahoot Time!





¡GRACIAS!



Jose Antonio Garcia Cartagena



Jantcart@amazon.es



thevallians.com

v