LNXnetwork
SOLUCIONES ALTERNATIVAS

Centro de Ethical Hacking & Security

Matriz Mitre ATT&CK

Para identificar ciberamenazas

Fases de un Ataque

LNXnetwork
SOLUCIONES ALTERNATIVAS

Centro de Ethical Hacking & Security

Mitre ATT&CK Cyber Kill Chain

LNXnetwork
SOLUCIONES ALTERNATIVAS

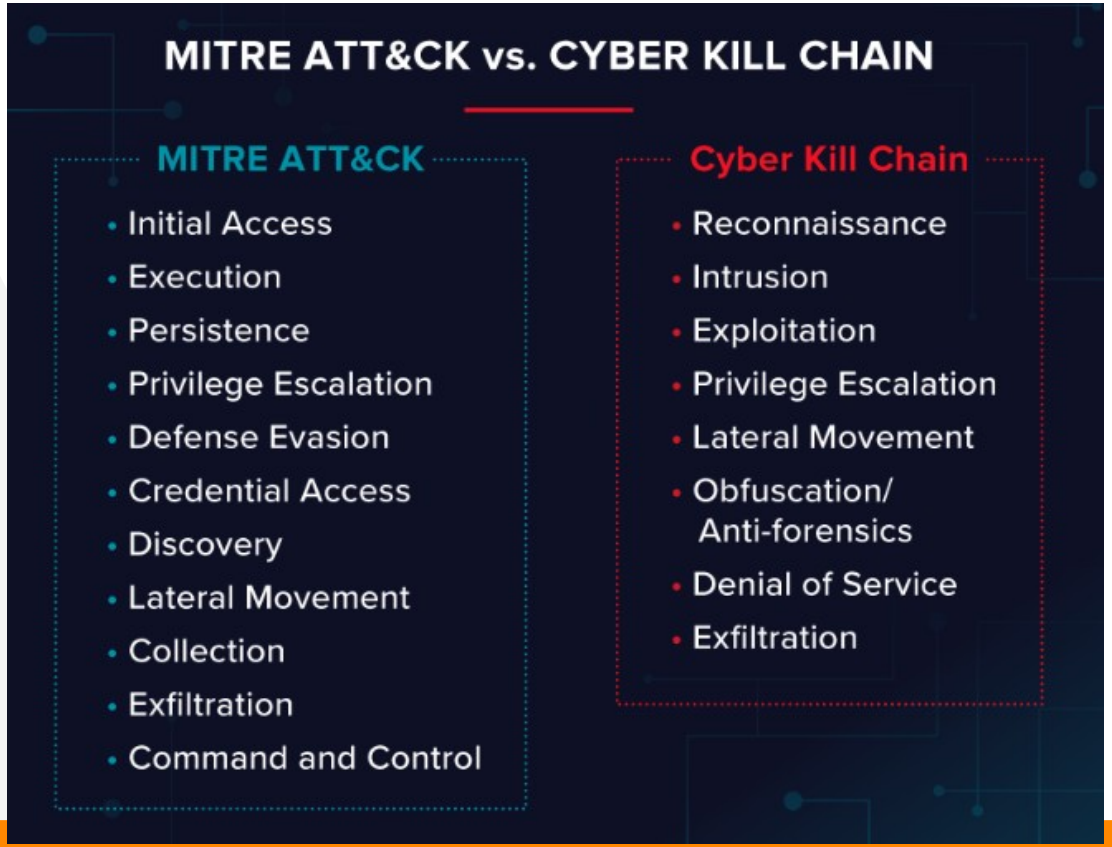
Mitre ATT&CK | Cyber Kill Chain

Uno de los puntos fundamentales en la ejecución del trabajo de Pentest o Ethical Hacking es seleccionar de acuerdo a nuestro alcance las tácticas, técnicas y conocimiento común de adversarios a usar.

Mitre ATT&CK
https://attack.mitre.org/

Cyber kill Chain
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Mitre ATT&CK | Cyber Kill Chain



Cyber Kill Chain

Termino Kill Chain (Cadena de muerte)

Es un concepto de seguridad militar “cadena de muerte” se usó originalmente como un concepto militar relacionado con la estructura de un ataque; que consiste en la identificación del objetivo, el envío forzado al objetivo, la decisión y la orden de atacar el objetivo, y finalmente la destrucción del objetivo.

Cyber Kill Chain

Por ejemplo un modelo de cadena de muerte militar, podría ser:

- Buscar: identifica un objetivo. Encuentre un objetivo dentro de los datos de vigilancia o reconocimiento o mediante medios de inteligencia.
- Fijar: Fijar la ubicación del objetivo. Obtenga coordenadas específicas para el objetivo a partir de datos existentes o mediante la recopilación de datos adicionales.
- Seguimiento: supervisa el movimiento del objetivo. Mantenga un registro del objetivo hasta que se tome la decisión de no atacar al objetivo o hasta que el objetivo sea exitoso.
- Objetivo: seleccione un arma o recurso apropiado para usar en el objetivo para crear los efectos deseados. Aplicar las capacidades de mando y control para evaluar el valor del objetivo y la disponibilidad de armas adecuadas para atacarlo.
- Comprometer: aplica el arma al objetivo.
- Evaluar: evalúe los efectos del ataque, incluida la información recopilada en el lugar.

Este es un proceso integrado de extremo a extremo que se describe como una "cadena" porque una interrupción en cualquier etapa puede interrumpir todo el proceso.

Cyber Kill Chain

Fases de ataque y contramedidas

Una cadena de muerte cibernética (cyber kill chain) revela las fases de un ciberataque: desde el reconocimiento temprano hasta el objetivo de la exfiltración de datos.

La cadena de eliminación también se puede utilizar como una herramienta de gestión para ayudar a mejorar continuamente la defensa de la red.

LNXnetwork
SOLUCIONES ALTERNATIVAS

Centro de Ethical Hacking & Security

Matriz Mitre ATT&CK

LNXnetwork
SOLUCIONES ALTERNATIVAS

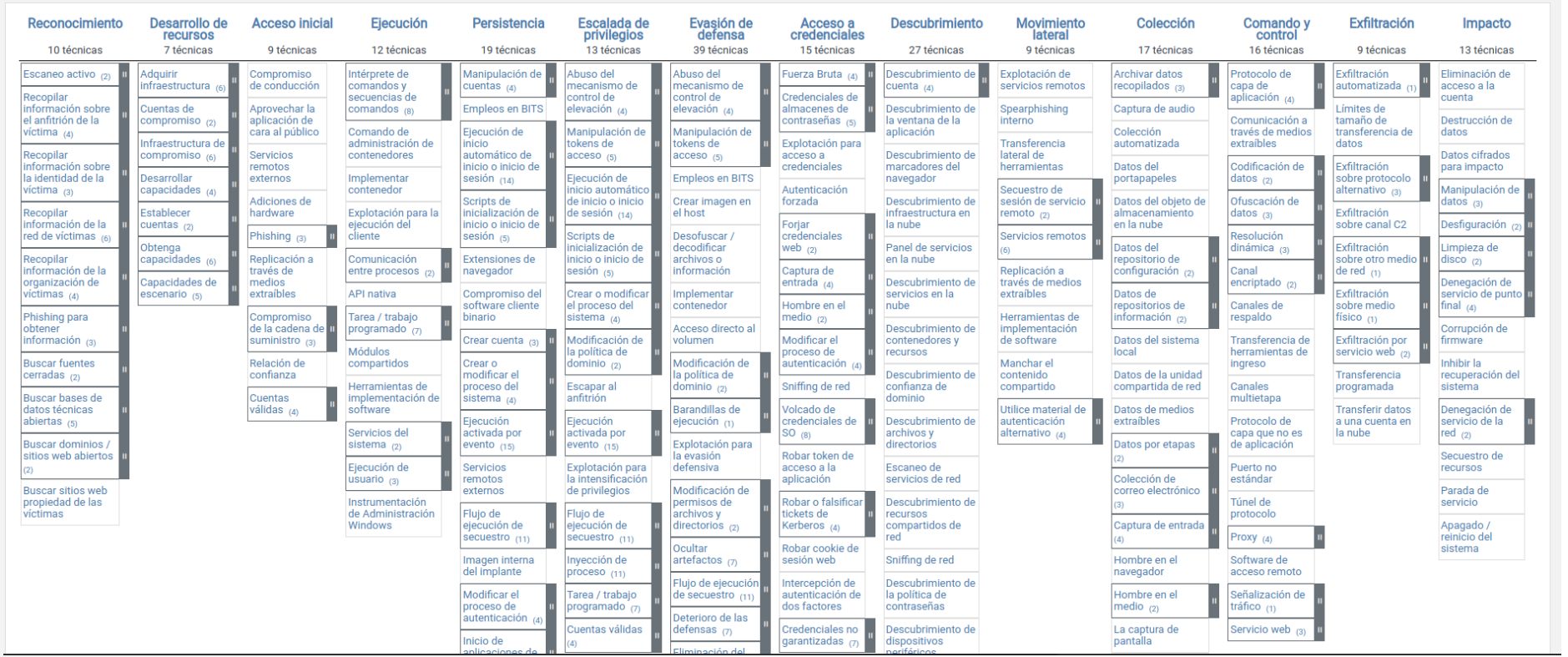
Mitre ATT&CK

Los pentesters pueden emular este comportamiento durante un compromiso para representar escenarios del mundo real y ayudar a sus clientes a determinar la efectividad de las contramedidas defensivas.

El marco ATT & CK tiene 3 matrices principales: Enterprise, Mobile e ICS (Sistema de Control Industrial). Enterprise Matrix tiene categorías para Windows, macOS, Linux y Cloud.

LNXnetwork

Mitre ATT&CK https://attack.mitre.org/



Mitre ATT&CK

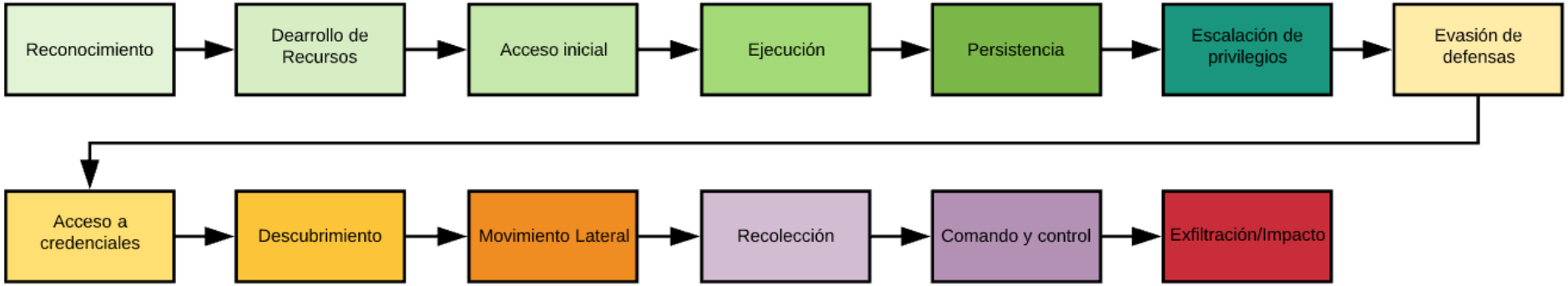
MITRE mantiene un marco de cadena de muerte conocido como MITRE ATT & CK®.

El marco modela tácticas, técnicas y procedimientos utilizados por actores maliciosos y es un recurso útil tanto para los equipos rojos como para los azules.

→ 14 tácticas

→ 228 técnicas

Mitre ATT&CK


Reconocimiento
Dearrollo de Recursos
Acceso inicial
Ejecución
Persistencia
Escalación de privilegios
Evasión de defensas
Acceso a credenciales
Descubrimiento
Movimiento Lateral
Recolección
Comando y control
Exfiltración/Impacto

Mitre ATT&CK

RECONOCIMIENTO

El adversario está tratando de recopilar información que pueda utilizar para planificar operaciones futuras.

El reconocimiento consiste en técnicas que recopilan de forma activa o pasiva información que se puede utilizar para respaldar la selección de objetivos. Dicha información puede incluir detalles de la organización, infraestructura o personal de la organización objetivo. El adversario puede aprovechar esta información para ayudar en otras fases, como el uso de la información recopilada para planificar y ejecutar el acceso inicial, para establecer el alcance y priorizar los objetivos posteriores al compromiso, o para impulsar y liderar más esfuerzos de reconocimiento.

Mitre ATT&CK

DESARROLLO DE RECURSOS

El adversario está tratando de implementar recursos que puedan utilizar para apoyar las operaciones.

El desarrollo de recursos consiste en técnicas que involucran a los adversarios que crean, compran o comprometen/roban recursos que pueden usarse durante el ciberataque. Dichos recursos incluyen infraestructura, cuentas de usuario o capacidades técnicas. El adversario puede aprovechar estos recursos para ayudar en otras fases, como el uso de dominios comprados para usarlos en Comando y Control, cuentas de correo electrónico para phishing como parte del acceso inicial, o el robo de certificados de firma de código para ayudar con la evasión de defensas.

Mitre ATT&CK

ACCESO INICIAL

El adversario está tratando de ingresar a la red.

El acceso inicial consiste en técnicas que utilizan varios vectores de entrada para obtener su punto de acceso inicial dentro de una red. Las técnicas utilizadas para establecerse incluyen el phishing y el ataque a servidores web. Los puntos de acceso obtenidos mediante el acceso inicial pueden permitir el acceso continuo, como cuentas válidas y el uso de servicios remotos externos, o pueden tener un uso limitado debido al cambio de contraseñas.

Mitre ATT&CK

EJECUCIÓN

El adversario está intentando ejecutar código malicioso.

La ejecución consiste en técnicas que dan como resultado un código controlado por el adversario que se ejecuta en un sistema local o remoto. Las técnicas que ejecutan código malicioso a menudo se combinan con técnicas de todas las demás tácticas para lograr objetivos más amplios, como explorar una red o robar datos. Por ejemplo, un adversario podría usar una herramienta de acceso remoto para ejecutar una secuencia de comandos de PowerShell que realiza detección remota de sistemas dentro de la red.

Mitre ATT&CK

PERSISTENCIA

El adversario está tratando de mantenerse en la red.

La persistencia consiste en técnicas que los adversarios utilizan para mantener el acceso a los sistemas a través de reinicios, credenciales modificadas y otras interrupciones que podrían bloquear su acceso. Las técnicas utilizadas para la persistencia incluyen cualquier cambio de acceso, acción o configuración que les permita mantener su posición en los sistemas.

Mitre ATT&CK

ESCALACIÓN DE PRIVILEGIOS

El adversario está tratando de obtener permisos de mayor nivel.

La escalación de privilegios consiste en técnicas que los adversarios utilizan para obtener permisos de mayor nivel en un sistema o red. Los adversarios a menudo pueden ingresar y explorar una red con acceso sin privilegios, pero requieren permisos elevados para cumplir sus objetivos. Los enfoques comunes son aprovechar las debilidades del sistema, las configuraciones incorrectas y las vulnerabilidades.

Mitre ATT&CK

EVASIÓN DE DEFENSAS

El adversario está tratando de evitar ser detectado.

La evasión de defensa consiste en técnicas que los adversarios utilizan para evitar ser detectados durante la intrusión. Las técnicas utilizadas para la evasión de la defensa incluyen la desinstalación o desactivación del software de seguridad o la ofuscación y cifrado de datos y scripts. Los adversarios también aprovechan y abusan de procesos confiables para ocultar y enmascarar su malware.

Mitre ATT&CK

ACCESO A CREDENCIALES

El adversario está tratando de robar nombres de cuenta y contraseñas.

Acceso a Credenciales consiste en técnicas para robar credenciales como nombres de cuenta y contraseñas. Las técnicas utilizadas para obtener credenciales incluyen el registro de claves o el volcado de credenciales. El uso de credenciales legítimas puede dar a los adversarios acceso a los sistemas, hacerlos más difíciles de detectar y brindar la oportunidad de crear más cuentas para ayudarlos a alcanzar sus objetivos.

Mitre ATT&CK

MOVIMIENTO LATERAL

El adversario está tratando de moverse a través de la red.

El movimiento lateral consiste en técnicas que los adversarios usan para ingresar y controlar sistemas remotos en una red. Seguir adelante con su objetivo principal a menudo requiere explorar la red para encontrar su objetivo y, posteriormente, obtener acceso a él. Alcanzar su objetivo a menudo implica moverse a través de múltiples sistemas. Los adversarios pueden instalar sus propias herramientas de acceso remoto para lograr el Movimiento Lateral o usar credenciales legítimas con herramientas ya instaladas dentro del sistema operativo, lo cual las hace más sigilosas.

Mitre ATT&CK

DESCUBRIMIENTO

El adversario está tratando de descubrir el entorno de tu red.

El descubrimiento consiste en técnicas que un adversario puede usar para obtener conocimiento sobre el sistema y la red interna. Estas técnicas ayudan a los adversarios a observar el entorno y a orientarse antes de decidir cómo actuar. También exploran lo que pueden controlar y lo que hay alrededor de su punto de entrada para descubrir cómo podría beneficiar su objetivo. Las herramientas instaladas del sistema operativo a menudo se utilizan para alcanzar este objetivo de recopilación de información.

Mitre ATT&CK

RECOLECCIÓN

El adversario está tratando de recopilar datos de interés para extracción.

La recopilación consiste en técnicas que los adversarios pueden usar para recopilar información. Con frecuencia, el siguiente objetivo después de recopilar datos es exfiltrar los datos. Los métodos comunes de recolección incluyen extracción de archivos, extracción de base de datos, toma de pantallazos, y registro del teclado.

Mitre ATT&CK

COMANDO Y CONTROL

El adversario está tratando de comunicarse con sistemas hackeados para controlarlos.

El comando y control consiste en técnicas que los adversarios pueden usar para comunicarse con los sistemas bajo su control dentro de una red Los adversarios suelen intentar imitar el tráfico normal esperado para evitar la detección. Hay muchas formas en que un adversario puede establecer el comando y el control con varios niveles de sigilo dependiendo de la estructura de red y las defensas de la víctima.

Mitre ATT&CK

EXFILTRACIÓN

El adversario está tratando de robar datos.

La exfiltración consiste en técnicas que los adversarios pueden usar para robar datos de tu red. Una vez que han recopilado datos, los adversarios a menudo los empaquetan para evitar ser detectados mientras se extraen. Esto puede incluir compresión y encriptación. Las técnicas para extraer datos de una red generalmente incluyen transferirlos a través de su canal de comando y control o un canal alternativo.

Mitre ATT&CK

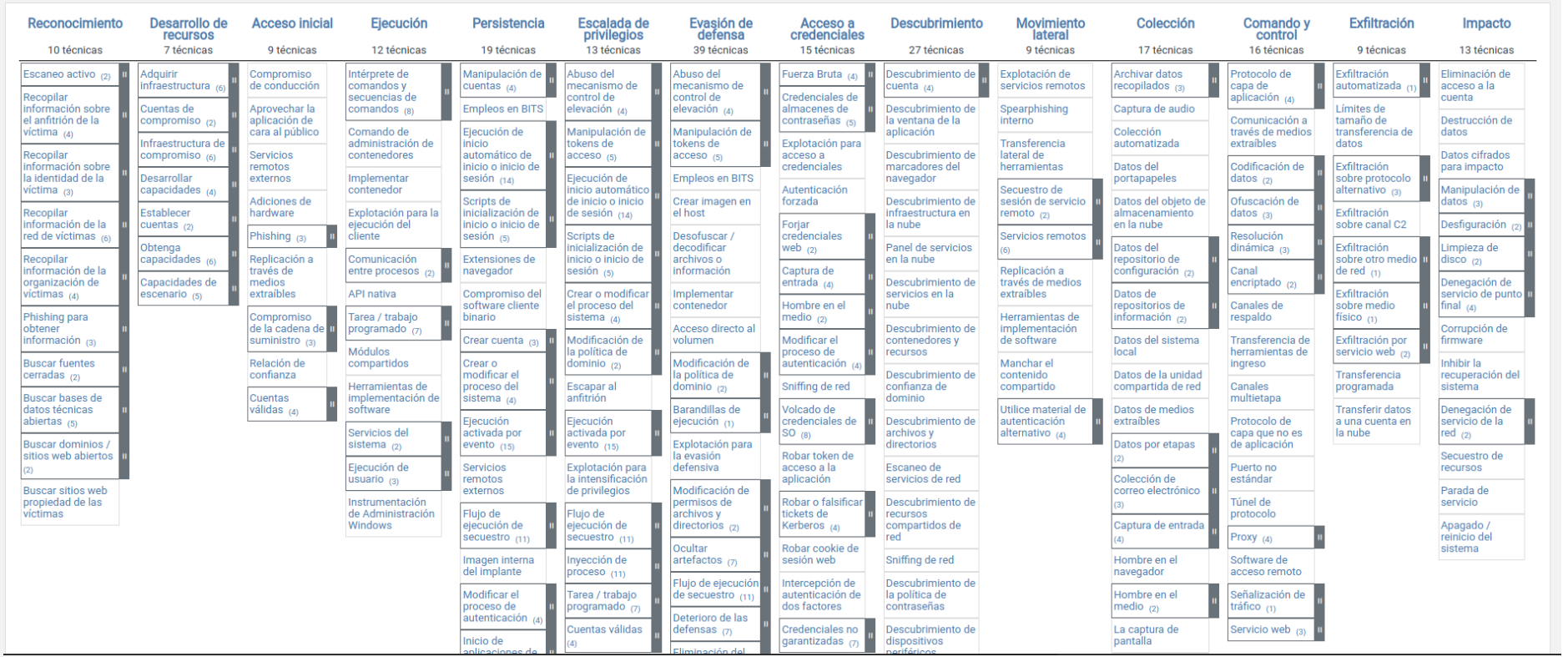
IMPACTO

El adversario está tratando de manipular, interrumpir o destruir tus sistemas y datos.

El impacto consiste en técnicas que los adversarios utilizan para interrumpir la disponibilidad o comprometer la integridad al manipular los procesos comerciales y operativos. Las técnicas utilizadas para el impacto pueden incluir destruir o alterar los datos.

LNXnetwork

Mitre ATT&CK https://attack.mitre.org/



LNXnetwork

Muchas Gracias!

Preguntas.-

Lic. Héctor Aguirre

Es instructor certificado por EC-Council (EC-Council certifica a profesionales en Certified Ethical Hacker (CEH), EC-Council Certified Security Analyst (ECSA), Certified SOC Analyst (CSA) Computer Hacking Forensic Investigator (CHFI), Certified Chief Information Security Officer (CCISO), entre otras del área de seguridad defensiva, ciberseguridad y seguridad ofensiva).

Es Director de LNXnetwork S.R.L. (Empresa Consultora Especializada en Ciberseguridad) y del Centro de Ethical Hacking & Security (Centro de Formación de profesionales en ciberseguridad), CSIRT/SOC (Centro de Respuestas a Incidentes Cibernéticos).

Consultor en Ciberseguridad y Ciberdefensa

haguirre@lnxnetwork.com | hector.antonio.aguirre@owasp.org

Lic. Héctor Aguirre

- Cuenta con certificaciones en Ethical Hacker (CEH), CCISO, ECSA (Analista de Ciberseguridad), CHFI (Hacker Forense Informático), CSA/SOC, ECSS (Especialista en Ciberseguridad), entre otras.
- Cuenta con 34 años de experiencia de la carrera de TI.
- Cuenta con 26 años de experiencia en Seguridad de la Informática/Información, Ciberseguridad y Ciberdefensa.
- Es intructor de Ciberseguridad y Ciberfensa en el IAEE (Instituto de Altos Estudios Estratégicos del Ministerio de Defensa).
- Participa a nivel técnico en las organizaciones LACNIC, LACNOC, OWASP, ISOC.

LNXnetwork

LNXnetwork
SOLUCIONES ALTERNATIVAS

Centro de Ethical Hacking & Security

LNXnetwork S.R.L. | Centro de Ethical Hacking & Security

Sitio web: https://www.lnxnetwork.com/

Oficina

Padre Buenaventura Suárez 1600 (Paseo Andemsan, Oficina 2) entre India Juliana y Alfredo Seiferheld - Asunción, Paraguay

Email

csirt@lnxnetwork.com

capacitacion@lnxnetwork.com

Llamadas Telefónicas

+595 21 327 4568

+595 961 614927

haguirre@lnxnetwork.com | Teléfono: 595 961 614927