



Laboratorio 5 - Ciberseguridad

Fabián Valero Duque

Integrantes: Alejandra Campo Archbold, María Fernanda Rodríguez, Jham Pool Murillo

19 de septiembre de 2022

Gestión de Riesgos Cibernéticos

Introducción

Procesos en Caldera: Ejercicio entre distribuciones de Linux

Tácticas, técnicas y procedimientos para comprometer al objetivo

Conclusiones

Gestión de Riesgos Cibernéticos

Introducción

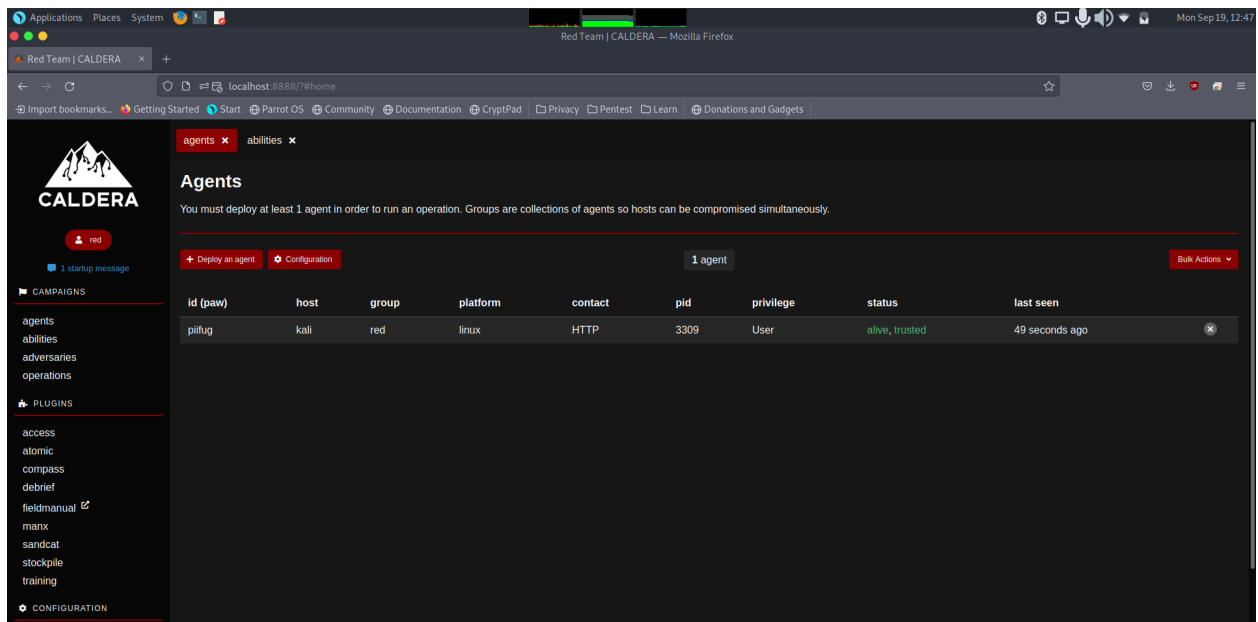
Caldera es un sistema automatizado de simulación de adversarios o simulación de brechas de seguridad libre permite ejecutar comportamientos o acciones posteriores al compromiso de un equipo dentro de las redes corporativas en ambientes Windows, Linux, macOS (Darwin).

Procesos en Caldera: Ejercicio entre distribuciones de Linux

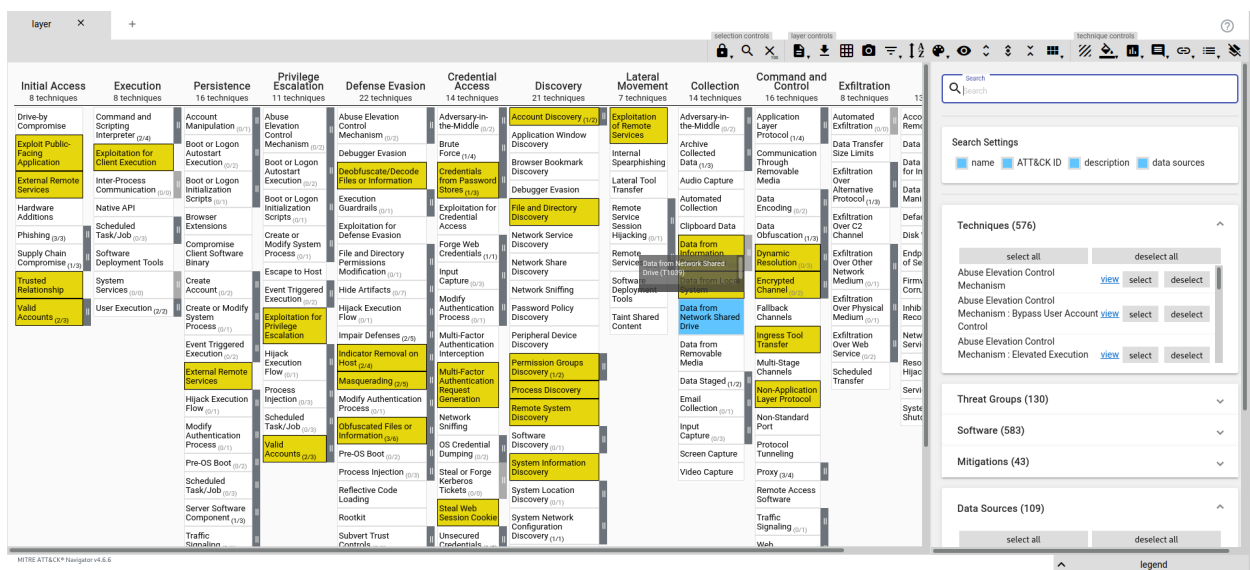
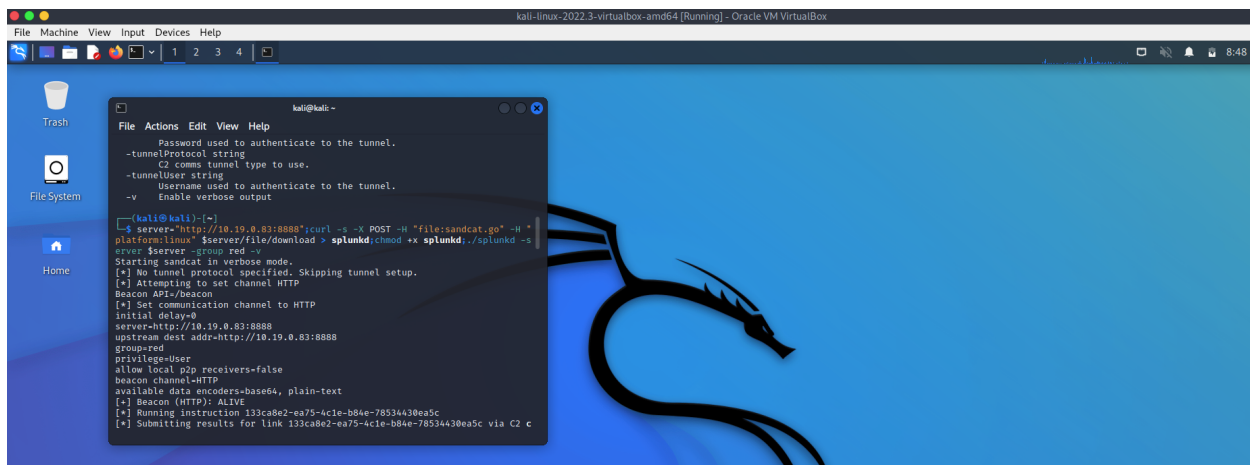
Para planear el ataque para un sistema operativo previamente se consulta la IP del computador atacante para luego cambiar los parámetros en Caldera e indicar el OS para atacar.

IP del computador atacante (Parrot OS distribución Linux basada en Debian).

```
Parrot Terminal
File Edit View Search Terminal Help
[alejandra@darksoca]-[-]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp12s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN
   group default qlen 1000
   link/ether 84:a9:38:a6:c0:bd brd ff:ff:ff:ff:ff:ff
3: wlp0s20f3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
   group default qlen 1000
   link/ether 1c:c1:0c:f1:70:34 brd ff:ff:ff:ff:ff:ff
   inet 10.19.0.83/24 brd 10.19.0.255 scope global dynamic noprefixroute wlp0s20f3
       valid_lft 2930sec preferred_lft 2930sec
   inet6 fe80::e968:8146:dd15:1e1a/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[alejandra@darksoca]-[-]
$
```



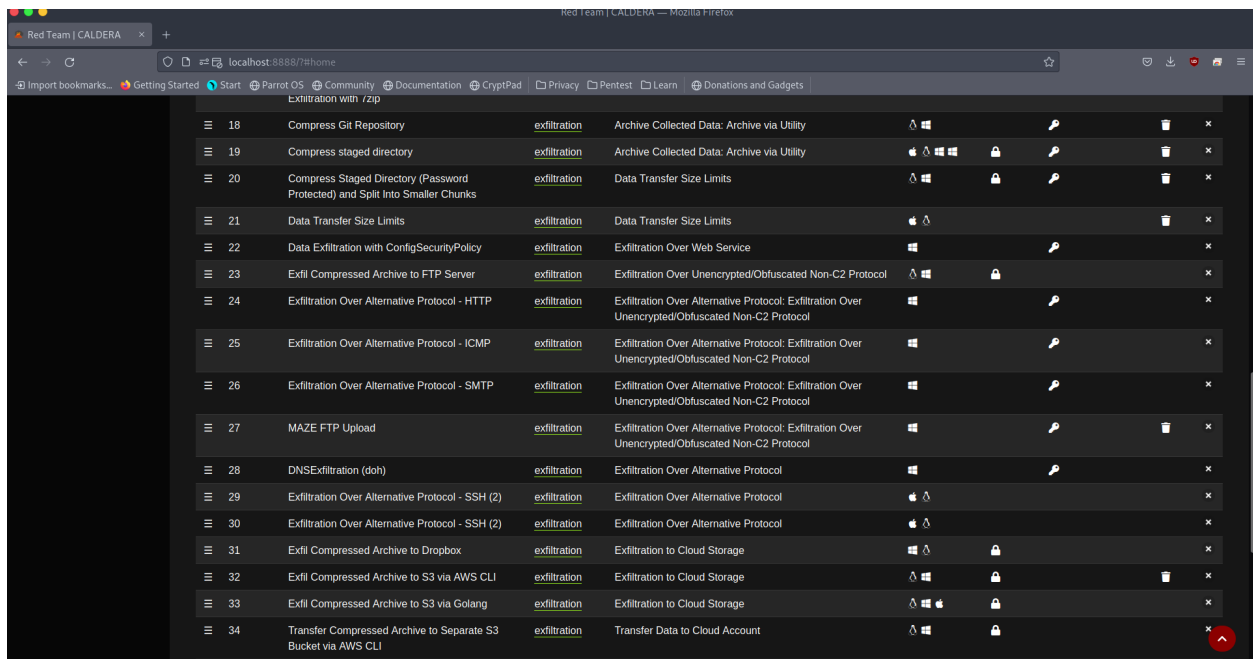
Para el ejercicio, optamos por atacar a un sistema Debian llamada Kali (Linux)

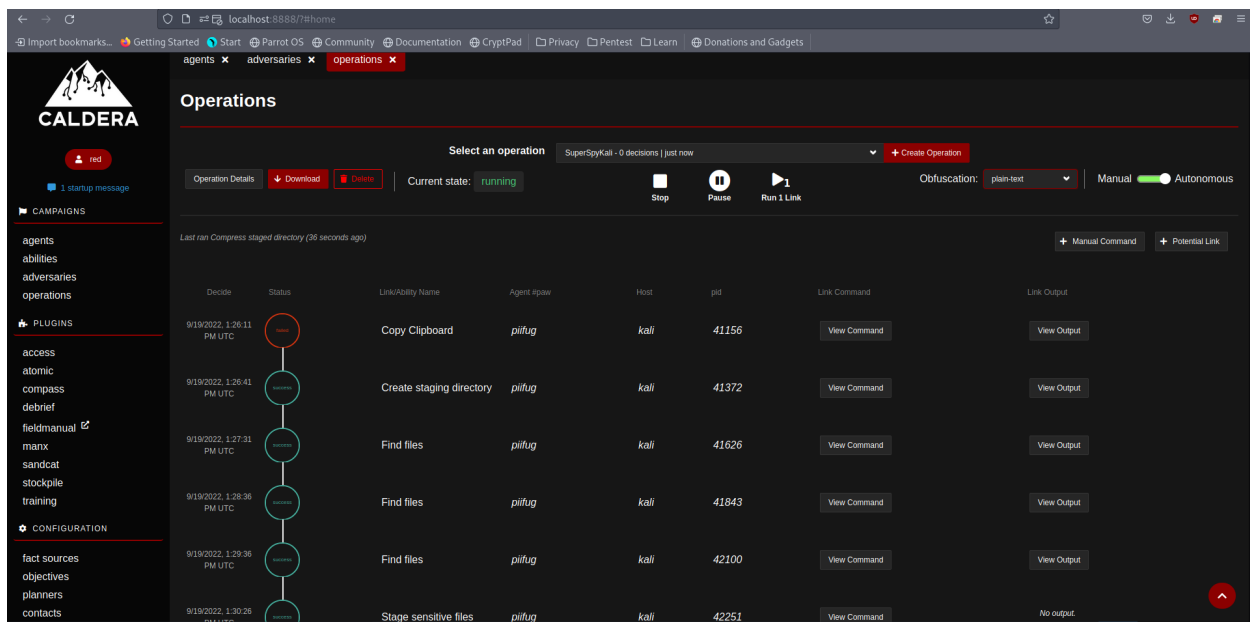


Tácticas, técnicas y procedimientos para comprometer al objetivo

1. Compress Git Repository (T1560.001)
2. Compress Staged Directory (Password Protected) and Split Into Smaller Chunks (T1030)
3. Compress staged directory (T1560.001)
4. Data Transfer Size Limits (T1030)
5. Exfil Compressed Archive to Dropbox (T1567.002)
6. Exfil Compressed Archive to FTP Server (T1048.003)

7. Exfil Compressed Archive to Github Gist (T1567.001)
8. Exfil Compressed Archive to Github Repository (T1567.001)
9. Exfil Compressed Archive to S3 via AWS CLI (T1567.002)
10. Exfil Compressed Archive to S3 via Golang (T1567.002)
11. Exfil Directory Files to GitHub (T1567.001)
12. Exfil staged directory (T1041)
13. Exfiltrate data HTTPS using curl linux (T1048.002)
14. Exfiltration Over Alternative Protocol - SSH (T1048)
15. Exfiltration Over Alternative Protocol - SSH (T1048)
16. Scheduled Exfiltration (T1029)
17. Transfer Compressed Archive to Separate S3 Bucket via AWS CLI (T1537)





Conclusiones

- Atacar mediante el uso de caldera es relativamente sencillo, con conocimientos básicos se puede llegar hacer daños a otro dispositivo(simulado).
- Llenando el excel nos dimos cuenta que es necesario pues nos ayuda a definir prioridades al momento de proporcionar los controles a los posibles ataques.
- Algunos ataques son más complicados de realizar que otros dependiendo la seguridad que tiene cada equipo, por eso son importantes las mitigaciones.
- Es bueno tener conocimiento sobre las ip de los dispositivos, de lo contrario va a ser complicado usar caldera.
- El uso de herramientas como mitre-attack fue importante al momento de definir cuales mitigaciones son las adecuadas dependiendo de la tecnica del ataque, ademas de proporcionarnos claridad en algunos conceptos.