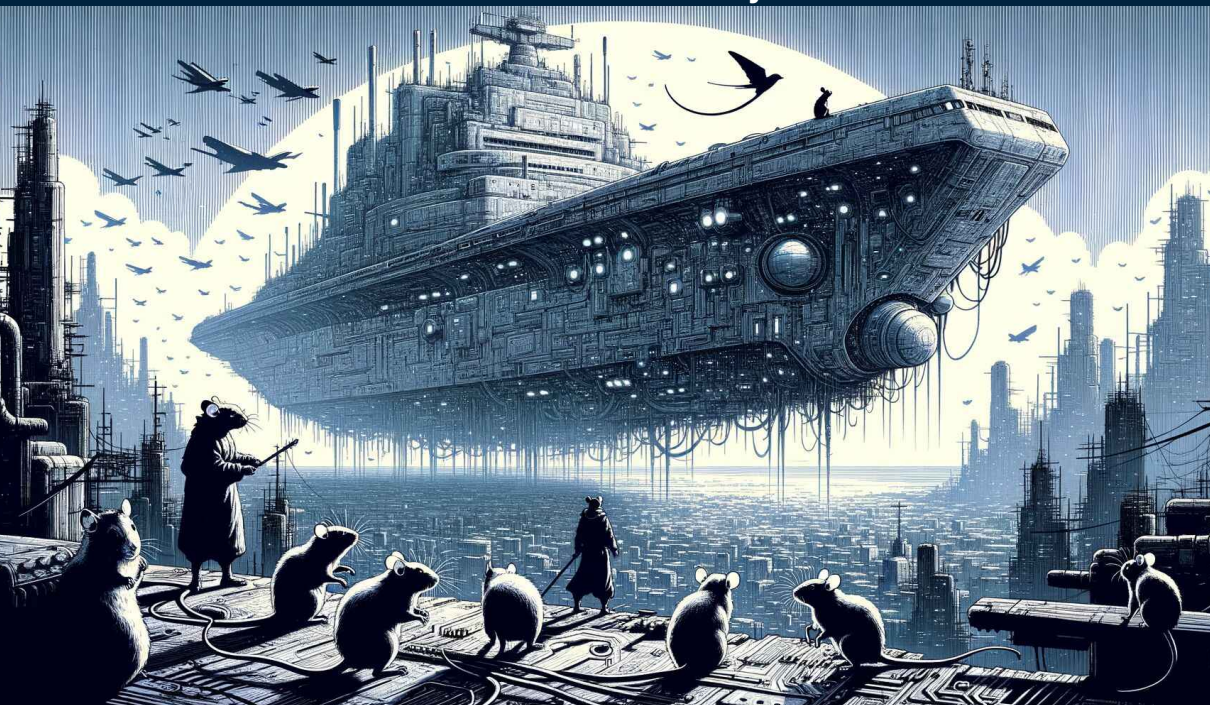
El terreno ciber: las ratas y el leviatán



Contexto

Charla introductoria de 30 minutos.

- Sobre el paisaje de la ciberseguridad en Chile 2024.
- Destinada a alumnos académicos del DUOC.
- Presentada por un Pentester profesional de Dreamlab Technologies.

Contenido

No.	Sección	Descripción
1	Definición	Que es la ciberseguridad?
2	Demo	Como se hace un ataque?
3	Paisaje	Quienes son los actores de la ciberseguridad?

Que significa Ciber-Seguridad?

Raíz	Definición
Ciber	Computador
Seguridad	Pelea

Pelea con computadores

Pelea con computadores

La Ciber (o computación)

1. Desarrollo de Software
2. Administración de Sistemas
3. Redes y Comunicaciones
4. Ciencia de Datos
5. Nube
6. Seguridad

Para participar en el terreno Ciber, hay que saber ocupar un computador.

La Seguridad

Fecha	Terreno	Ejemplo	Lugar
-8000	Tierra	masa, bastón	África, China
-2200	Mar	botes de papiro	Egipto
1911	Aire	avión de hélice	Francia
1957	Espacio	satélite espía	Rusia, USA
2010	Ciber	gusano informático	Irán

El terreno ciber

N.	Terreno	Permite	Como
1	Nuevo	El llega primero reclama	colonización
2	Barato	un terreno donde todos pueden acceder.	agua
3	Conectado	Y se puede apuntar lejos	telescopio
4	Rápido	a la velocidad luz	relámpago
5	Anonimizado	sin que nadie sepa quien fue.	invisibilidad

La ciberseguridad tiene el viento a favor.

La ciberseguridad tiene el viento a favor.

Un terreno asimétrico

Un terreno asimétrico

Atacar y defender son dos profesiones distintas.

La ciberdefensa

Hay que saber atacar para poder defender!

Por ejemplo, para buscar extraterrestres, meterse en el lugar de extraterrestres que buscarían humanos. (tener una metodología pragmática, tener humildad).

Otro ejemplo, para tapar 1000 hoyos de manera industrial, primero tapar un hoyo de manera artesanal. (no hacer optimización prematura, ensuciar sus manos).

El ciberataque

1. Buscar victimas (humanas).
2. Buscar superficie de exposición de sus victimas.
3. Buscar vulnerabilidades en la superficie.
4. Explotar vulnerabilidades.
5. Mantener persistencia en los computadores infectados.
6. Robar dinero.

La explotación de vulnerabilidad

Un ciber-ataque se hace mediante la explotación de una vulnerabilidad.

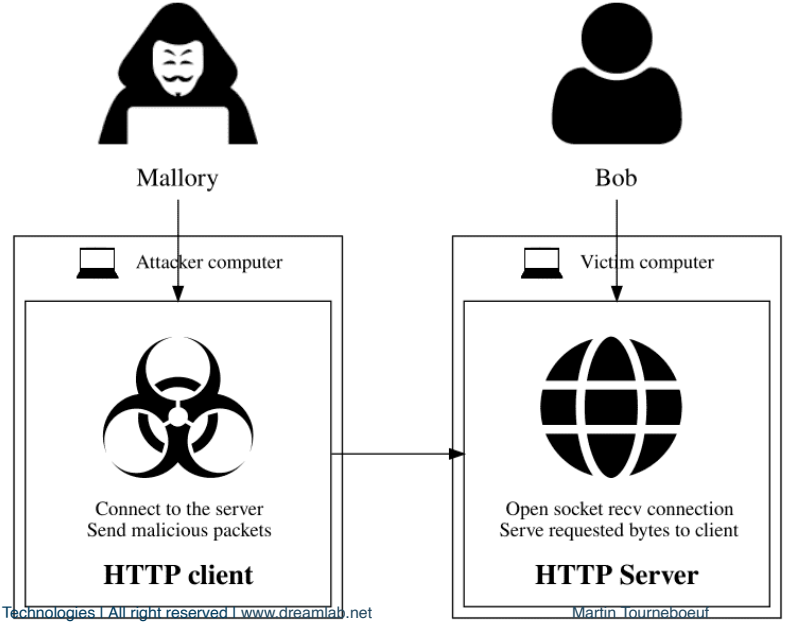
Una vulnerabilidad informática es lo que permite que un programa haga algo que sus usuarios no habían contemplado.

La búsqueda de vulnerabilidad

Una vulnerabilidad informática es lo que permite que un programa haga algo que sus usuarios no habían contemplado.

1. Que hace el programa?
2. Como lo implementa?
3. Como lo implementaría yo para que sea seguro?
4. Lo implementa de mi forma? Sino, porque?

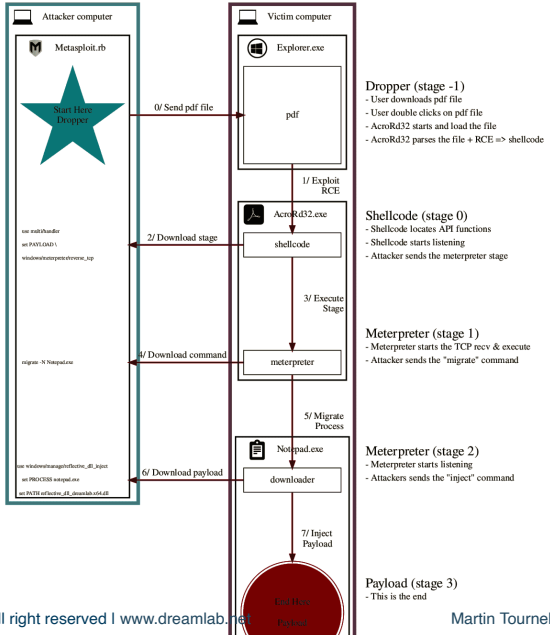
Escenario: Bob y Mallory



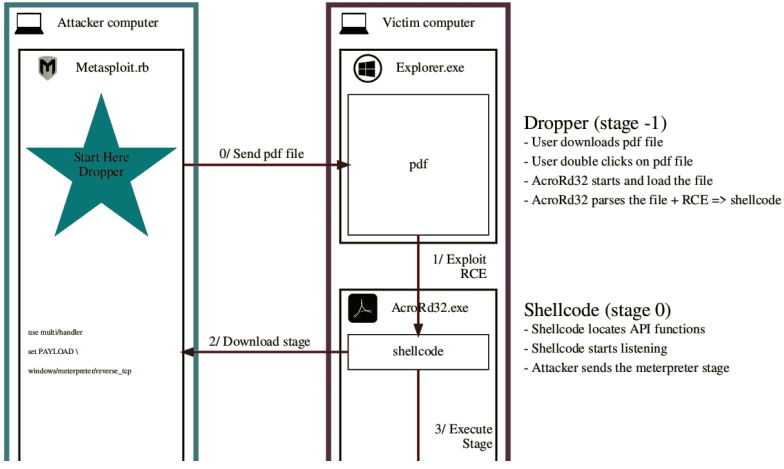
Etapas del ataque

1. Reconocimiento (pasivo)
2. Escaneo (activo)
3. Intrusión (o explotación)
4. Consolidación (o persistencia)
5. Carga (o *payload*)

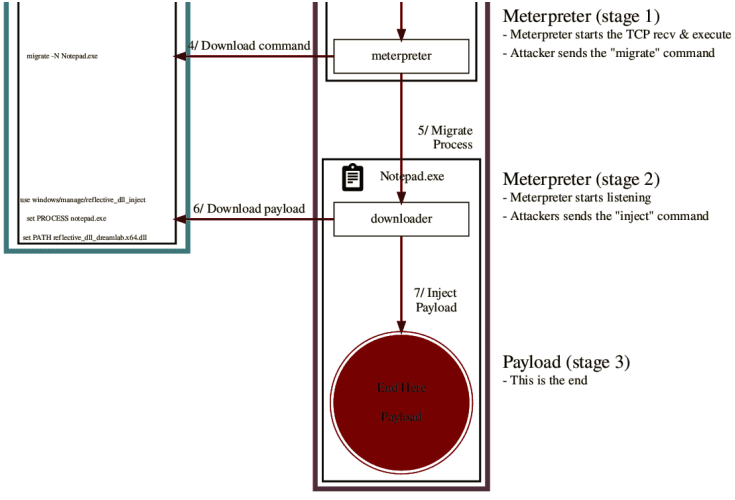
Explotación



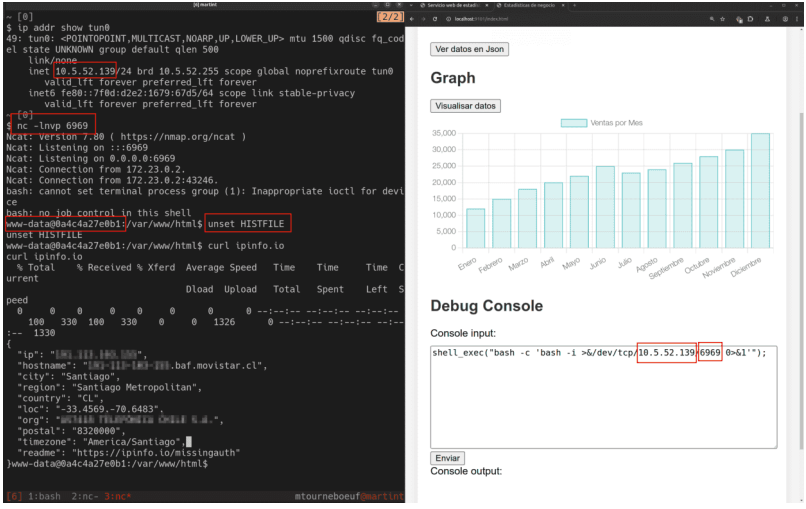
Post-explotación: parte 1



Post-explotación: parte 2



Demo (por fin)



Resultado

Mallory controla el computador de Bob.

Humanos contra humanos

Sujeto	Pre verbo	Verbo
Yo	no	me quiero hackear.
Mi circulo de confianza	probablemente no	me quiere hackear.
Los animales non humanos	no	me pueden hackear.
Los extraterrestres	no	me quieren hackear.
Todo los demás (8G humanos)	potencialmente	me quieren hackear

Actores internacionales

Actores nacionales

Comparar con el mapa de los actores estatales en Francia.

Sector	Ejemplo
Público	Gobierno, defensa, interior
Privado	Bancos, telecom, servicio
Universitario	Investigadores, practicantes
Independientes	Freelancer, mafia, RASS

(estos actores también saben usar un computador para otra cosa que pelear)

Lecciones aprendidas

1. La ciberseguridad, o pelea con computadores, opone **humanos**.
2. Hay que saber atacar para poder defender en el terreno ciber.
3. Un ciber-ataque se realiza mediante la explotación de una vulnerabilidad.
4. La ciberseguridad tiene el viento a favor por décadas.

Consejo

Como avanzar en el camino de la ciberdefensa?

1. Pensar como atacante.
2. Empezar la investigación con el camino legitimo.
3. Avanzar hipótesis.
4. Celebrar las pequeñas victorias.
5. No perder de vista su misión.

Más

Hacia donde avanzar en el camino de la ciberdefensa?

1. Búsqueda de vulnerabilidades interpretadas.
2. Explotación de vulnerabilidades binarias.
3. Desarrollo de *malware*.
4. Captura de *malware*.
5. Estudio de sistemas y flujos de trabajos.
6. Arquitectura segura.