Algoritmos y Estructura de Datos I

Taller de Programacion

Facultad de Ciencias Exactas y Naturales

2016

Menú del día

- Programación, Programación, Programación:

Menú del día

- Programación, Programación, Programación:
  - 1337 H4x0r (un poco descontextualizado)

Oh, noes!

La lucha contra Skynet continua...

Recibimos un comunicado de último momento! John Connor está en problemas! Se encuentra atrincherado junto a su equipo, en un edificio de la ciudad capital. Los T1000 mantienen el perímetro en posiciones defensivas. John Connor necesita de TU AYUDA para poder lanzar un contraataque y abrirse paso a través de las líneas enemigas. Debemos deshabilitar a los T1000, para romper el perímetro!

Anatomía del T1000

El T1000:

El T1000 es una máquina líquida. Virtualmente imparable.
John Connor descubrió su única vulnerabilidad en Marzo 2019:
Las máquinas utilizan WiFi encriptadas para comunicarse!

Anatomía del T1000

Anatomía del T1000

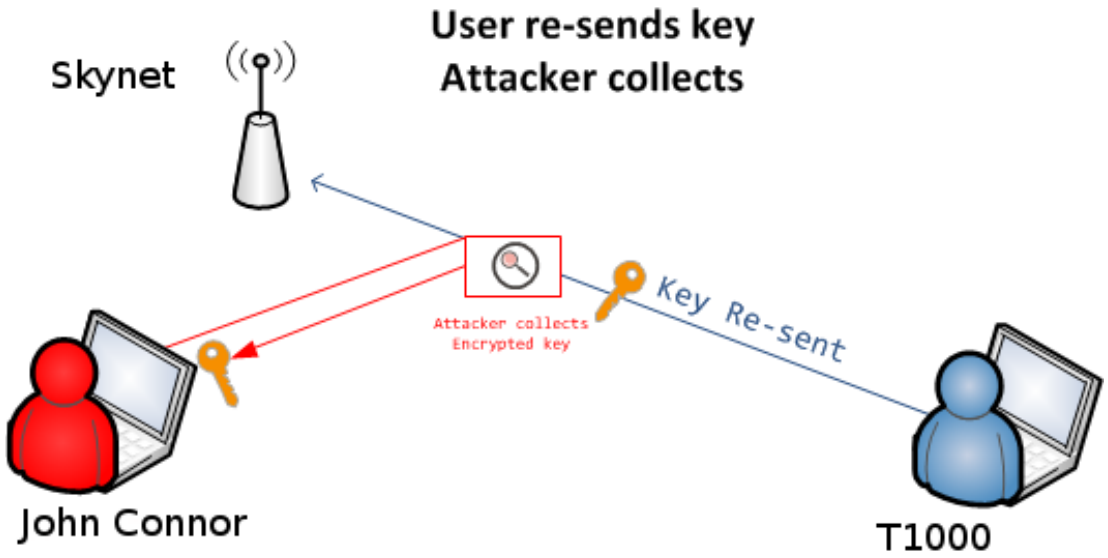
Sobre la situación actual:

Todo T1000 utiliza un enlace WiFi para comunicar y recibir ordenes. Para salvar la vida de John Connor debemos vulnerar al menos una máquina. El capitán nos ha conseguido los datos para que utilicemos nuestros equipos y podamos encontrar la vulnerabilidad.
Seria ideal poder vulnerar a todos los T1000 en orden para que John pueda moverse entre ellos y asi salvar todo su pelotón.

Salvando a John Connor

Sobre la Vulnerabilidad:

El capitán utilizó un dispositivo WiFi propio, para interceptar el tráfico entre los T1000 y Skynet, guardando todo en *handshakes.lst*. Consiguió, además, un archivo binario que nos permitiría imitar los handshakes!



Salvando a John Connor

Un Handshake es...

Un intercambio de mensajes cuyo formato fue formalmente pre-establecido.

Salvando a John Connor

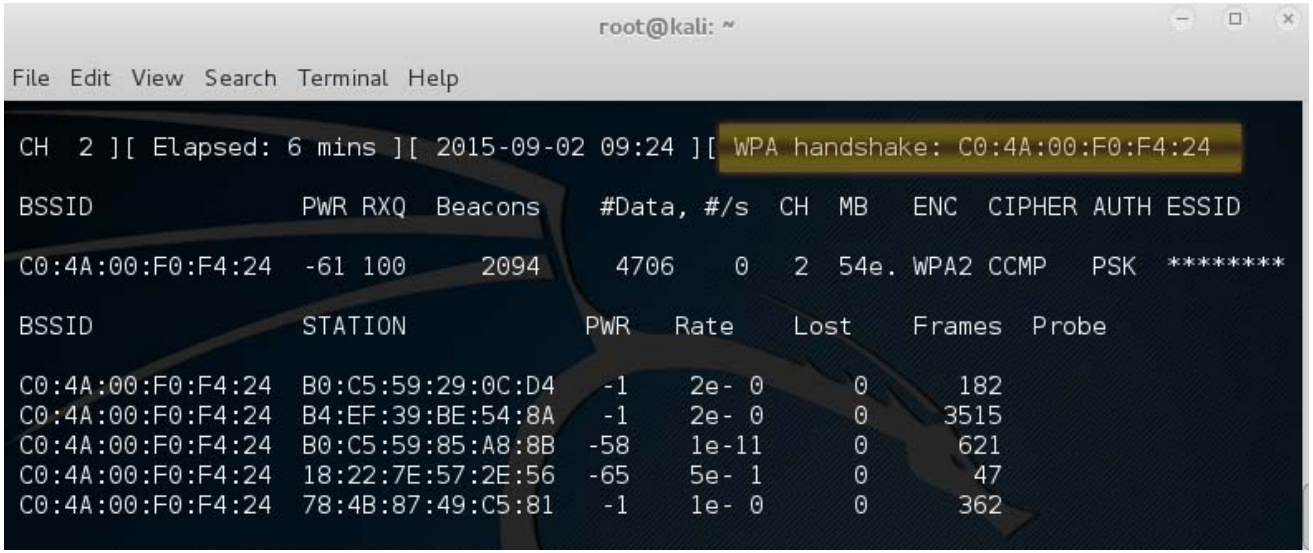
- Skynet subestima las capacidades de sus creadores

Salvando a John Connor

- Skynet subestima las capacidades de sus creadores
- Los handshake entre T1000 no están encriptados

Salvando a John Connor

- Skynet subestima las capacidades de sus creadores
- Los handshake entre T1000 no están encriptados
- Es decir, son fáciles de interpretar.



Especificaciones técnicas

- Las capturas constan de tres partes:

Especificaciones técnicas

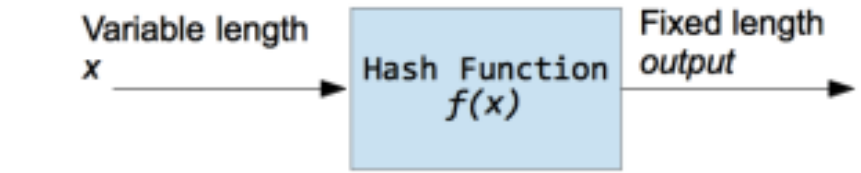
- Las capturas constan de tres partes:
- Nombre (ID) del WiFi, intensidad de señal y el Hash del password encriptado

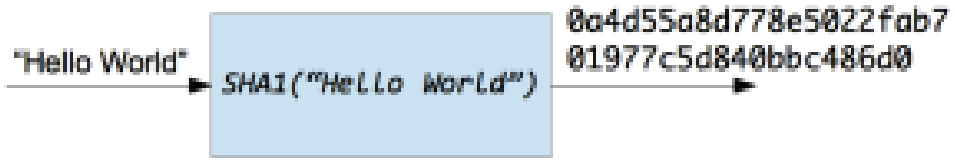
```
s/src/handshakes.lst
[Juanjo,-34,63494b1130f6979ea6b61980b6fa03049502078b];[TemilCito,-65,c58a8278bfd
7f5590356eabe1490fa2f2bb44989];[Adriana,-10,ce1ce7bbcda7d1265600c4e533fbf38e8936
2ebd];[GabiWiFiGratis,-59,2a4c1c0528637d2f887fdc688e4badb29901db63];[Ikki,-66,26
326f63c52dc75e08e68bba7bb4fc2eeadbdb8e];[LiderT1000,-1,9f4161996a44da8bccf08f872
f15e47807316cae];[VamoACalmarno,-11,62b7b605d0ebde09ada0a8453d4a14ec992e3d02];[u
berH4x0r,-18,ea6b01acd23edf9867ecef92d29b4a993dea9308];[lasT1000Vueltas,-88,6a1a
479612067d7436f775cb67a2779ff344cc24];[SalvameJebus,-5,d0ae3407452768a7d1f42713a
8e9d0a793df1b3a];[elRojo,-2,d98cfb31286a9b2aa6ceab9479c53c9824b6bad6];[OdoDS9,-9
,de64b18f4f9e65c3b2720fee55c19cc81ed275bb];[WalterWhite,-77,fbc7b800af800a2662ff
3921b6828d3143bd53b6]
```

Sobre Hashes y otras yerbas

Qué es un hash?

Una función de Hashes es una función que toma como entrada un string de longitud variable y lo convierte a otro string de longitud fija. Es función en solo un sentido. Si f(x) es una función de hashes, calcular un hash es rapido y simple... pero encontrar la inversa puede tomar mucho esfuerzo.





Cómo podemos salvar a John Connor?

El trabajo de hoy:

Cómo podemos salvar a John Connor?

El trabajo de hoy:

- Contamos con un archivo de capturas enviado por el capitán.

Cómo podemos salvar a John Connor?

El trabajo de hoy:

- Contamos con un archivo de capturas enviado por el capitán.
- Contamos con el resultado ordenado de la clase pasada *Spanish.dic*

Cómo podemos salvar a John Connor?

El trabajo de hoy:

- Contamos con un archivo de capturas enviado por el capitán.
- Contamos con el resultado ordenado de la clase pasada *Spanish.dic*
- Contamos con un objeto binario que nos permite generar hashes como los T1000 (*hash.o*)

Cómo podemos salvar a John Connor?

El trabajo de hoy:

- Contamos con un archivo de capturas enviado por el capitán.
- Contamos con el resultado ordenado de la clase pasada *Spanish.dic*
- Contamos con un objeto binario que nos permite generar hashes como los T1000 (*hash.o*)

No olvidemos:

Si logramos encontrar todas las passwords, podríamos dar vuelta la batalla! John Connor podria deshabilitar a todos los T1000, uno por uno!

La consigna:

1. Utilizar la estructura cap_t para levantar un vector de handshakes
2. Ordenar el vector de acuerdo al valor del int
3. Levantar Spanish.dic en otro vector
4. Iterar hasheando las palabras, y comparar los hashes con el primer vector
5. Si hay coincidencia, guardar la password
6. Devolver todos los hashes crackeados en orden, para salvar a John Connor

Salvemos a John Connor!

Preguntas?