Seguridad en la gestión de información

David Ureba Moreno – Pablo Borrego Gutiérrez

Disclaimer

1. El objetivo de la charla es meramente educativo.

2. Se han eliminado partes para evitar su directa reproducción.

Please, don’t be evil.

Índice

- ❑Who is Mr. Robot?
- ❑Relación con la asignatura.
- ❑¿Qué ocurre en el episodio?
- ❑Prueba real.

Who is Mr. Robot?

- El protagonista es ***Eliot*, un joven hacker**.

- Trabaja como **ingeniero de seguridad informática** por el día y usa sus habilidades durante la noche.

- *Eliot* **es reclutado por un grupo de hackers** quienes quieren destruir a poderosos empresarios de multinacionales que están manejando el mundo.

Who is Mr. Robot?

- Se estrenó en junio de 2015 en USA Network.
- **Os recomendamos que la veáis.**

MR. ROBOT

Relación con la asignatura

- Tema 7: Calidad en la gestión de información.

- Nos centraremos en la seguridad en un CPD:
  - **Intrusión**.
- Motivación: Espionaje, hurto, **sabotaje**.
- Causado por: **Falta de seguridad física/lógica**, insatisfacción de los empleados, etc.

MR. ROBOT

Relación con la asignatura

- Tema 3: Calidad del producto.

- **ISO/IEC 25010 > Métrica > Seguridad**
  - Nivel aceptable de riesgo para personas, negocio, leyes y entorno.
  - Capacidad de protección de la información y los datos de manera que personas no autorizadas no puedan leerlos o modificarlos.

- Vamos a demostrar más adelante cómo puede no cumplirse.

MR. ROBOT

¿Qué ocurre en el episodio?

- Nos centraremos en el episodio 1x05.

- **El plan era borrar todos los datos de una gran empresa**, o cifrarlos para hacerlos inaccesibles.

- Para hacer esto posible, **accede físicamente en la empresa** e introduce una ***Raspberry Pi***.

MR. ROBOT

¿Qué ocurre en el episodio?

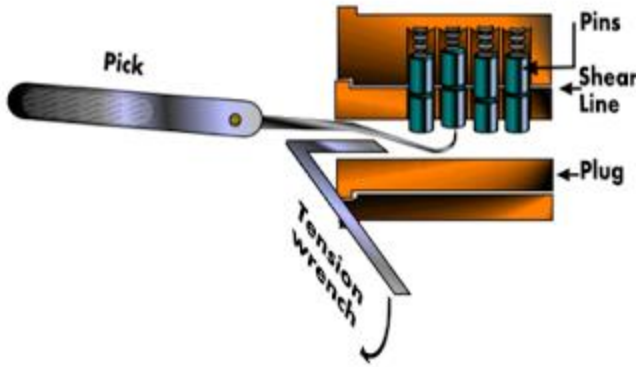
- Mediante **ingeniería social**, consigue acceder a la empresa.
- Una vez dentro, **accede a las escaleras** que dan al CPD **mediante *lockpicking***.
- El *lockpicking es* el **arte de abrir cerraduras sin su llave original utilizando ganzúas** u otro tipo de métodos no destructivos.

MR. ROBOT

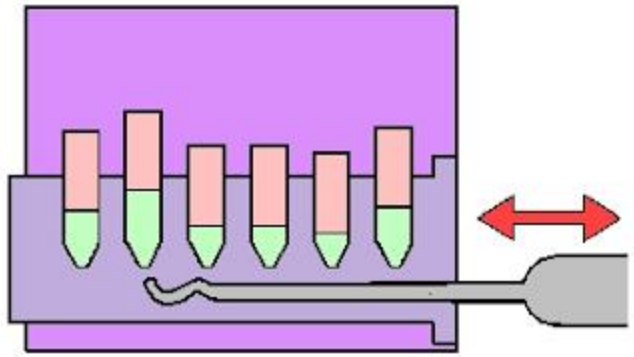
Lockpicking

Técnicas de apertura

- **Perno a perno (spool):**
  - Se aplica tensión en la cerradura hacia el lado de apertura.
  - Se pasa la ganzúa por todos los pernos, buscando el que primero se queda trabado.

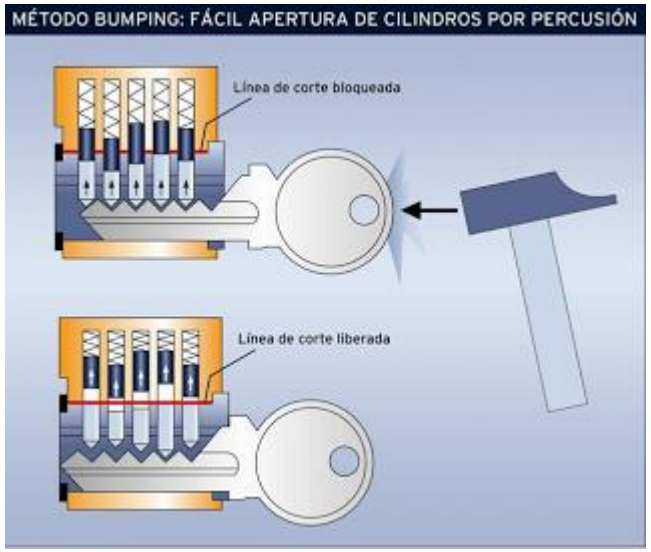


- **Rastrillado (raking):**
  - Similar al *spool*, pero pasando la ganzúa por TODOS los pernos.
  - Es más rápido en cerraduras simples.

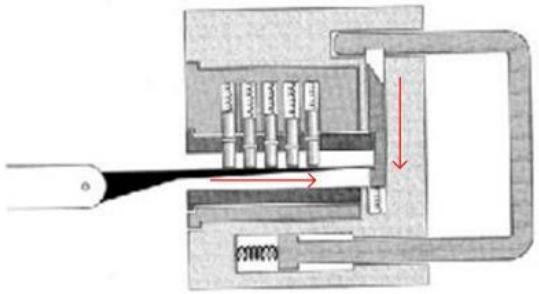

A rake pick is raked in and out of the lock quickly

Técnicas de apertura

- **Impacto o Bumping:**
  - La más usada por cerrajeros.
  - Se inserta una llave con los cortes muy bajos.
  - Se golpea con un objeto.



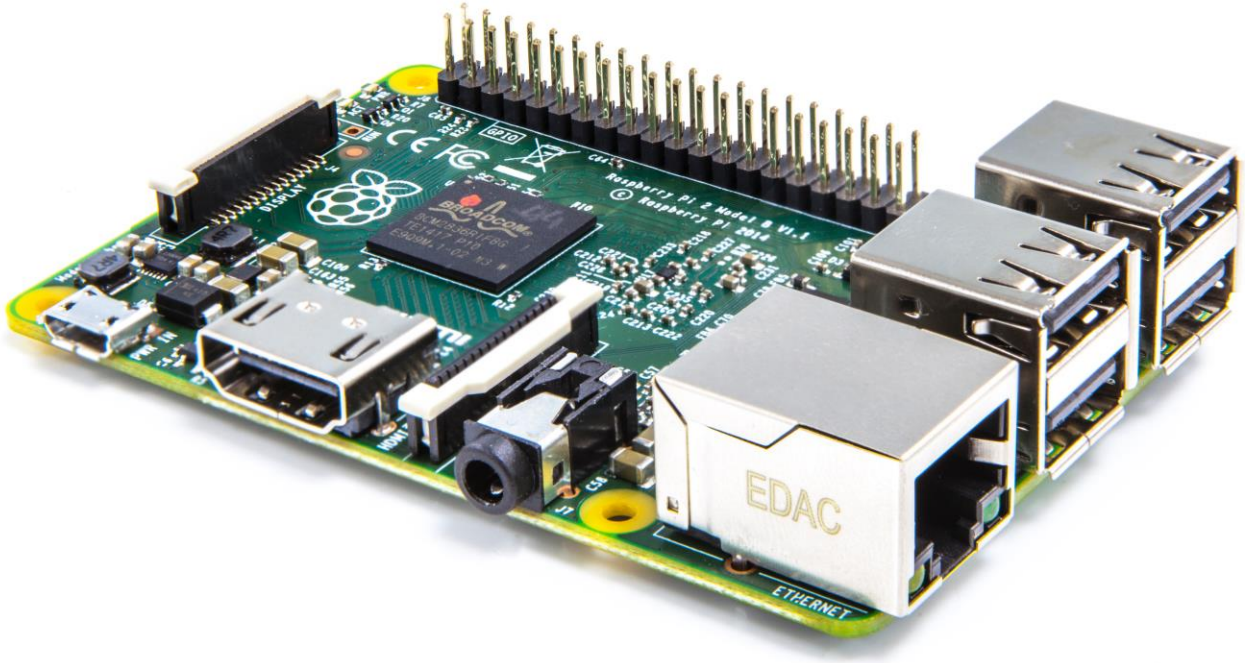
- **Bypass:**
  - **Shimming:** Abrir deslizando un material plano y rígido entre la puerta y el pestillo.
  - **Bypass picking:** Ignorar los pernos y accionar el gancho de seguridad.



MR. ROBOT

Raspberry Pi

- *Eliot,* en el episodio introduce en la planta del CPD una ***Raspberry Pi***.
- **Este será el “caballo de Troya”.**
- Ahora veremos sus bondades.



Raspberry Pi

- Computador de placa reducida de bajo coste.

- Se alimenta con **5v y 1A – 2A**, en función del modelo.

- También podemos alimentarla con POE (**Power over Ethernet).**
  - Eso fue lo usado en la serie, aunque se da por hecho que el cable tiene POE.

MR. ROBOT

Power Raspberry Pi
with Power over Ethernet

RPi power supply

CAT5

PT-3
power lead

POE-PA2 Passive PoE Injector / Splitter

CAT5 up to 130 feet

CAT5

POE-PA2

PT-4
power lead

RPi power supply
connected to PT-4

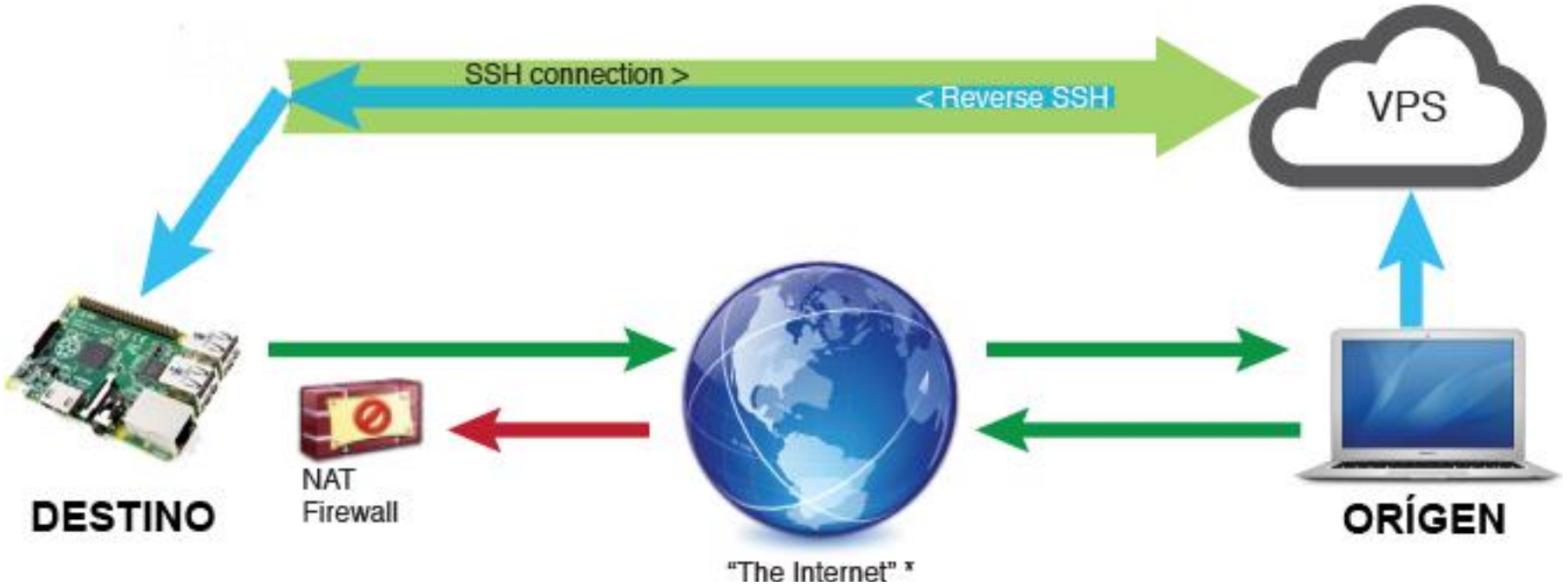
MR. ROBOT

Sí, muy bonito todo…
¿Pero cómo te conectas desde fuera?

MR. ROBOT

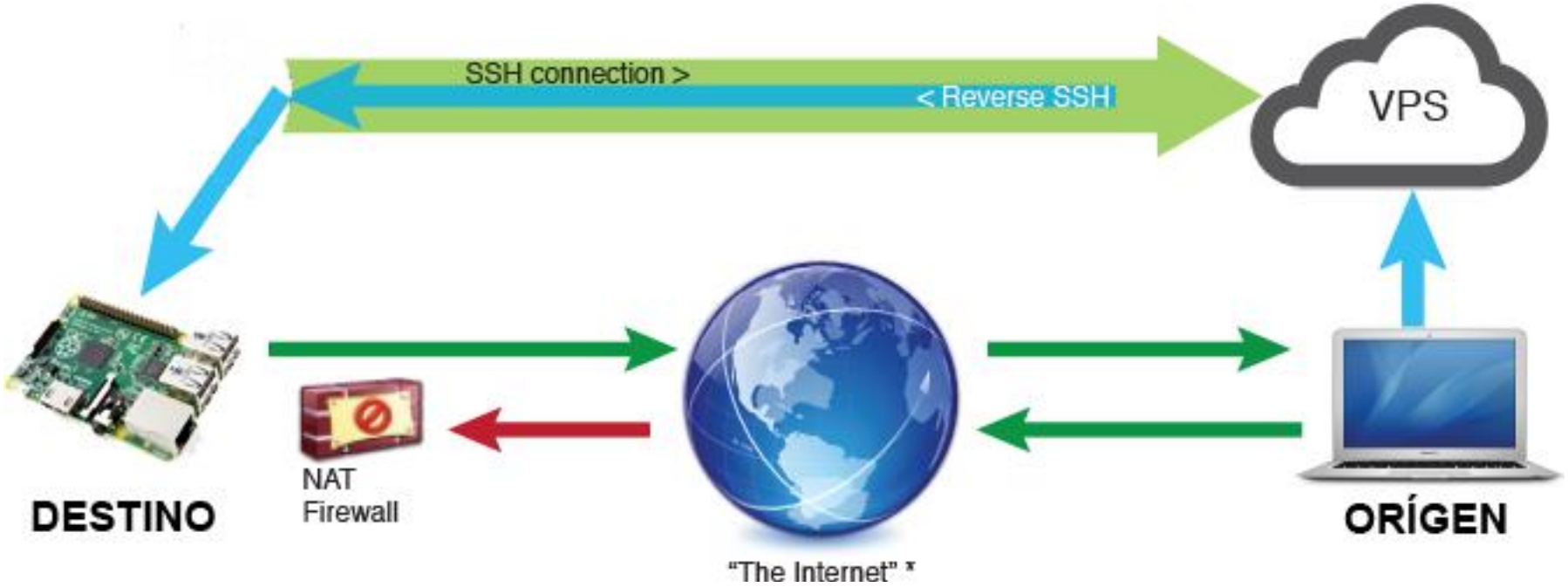
Reverse SSH Tunneling

- Una “sencilla” manera de **saltarnos el firewall** de la empresa.
- Sólo detectable mediante una inspección de paquetes.
- Fácilmente configurable.



Reverse SSH Tunneling

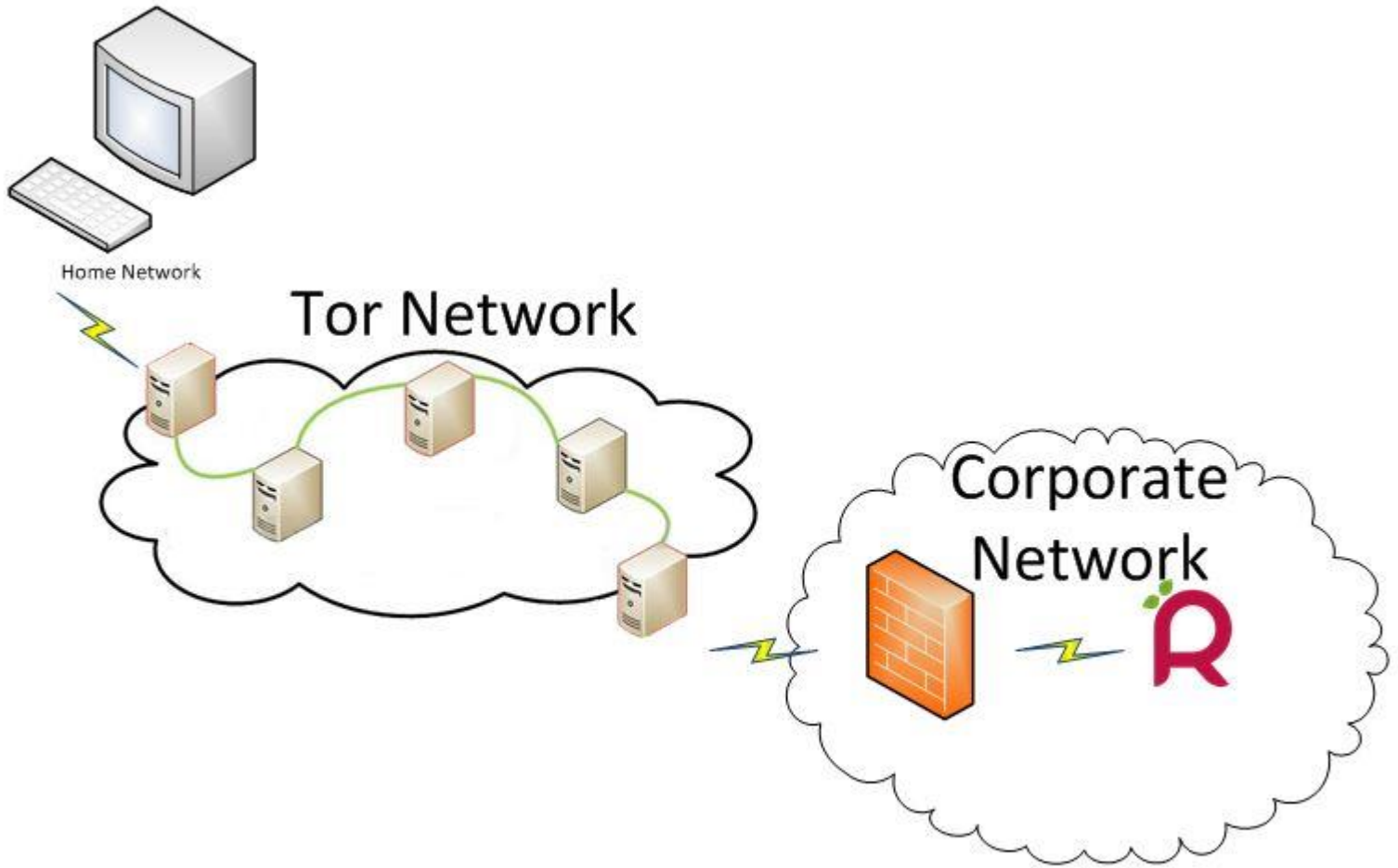
- **El VPS tiene una IP fija y es accesible** desde cualquier parte.
  - Este **será nuestro nodo común**.
  - La Raspberry se conectará automáticamente al VPS y deja una conexión a la inversa activa.



Reverse SSH Tunneling

- Reverse SSH Tunneling pasando el tráfico por **Tor**.

- También podemos usar un pool de proxies.



Y… ¿Por qué no montar una VPN?

- **Sin acceso al router, no podremos abrir puertos** o redirigir el tráfico.
- Muchas empresas **bloquean el tráfico por VPN** con un firewall.
- Es mucho **más sencillo instalar un túnel SSH** que una VPN.

MR. ROBOT

¿Cómo evitarlo?

- **Activando un DPI** (Deep Packet Inspection) del tráfico.

  ✓Se examinan los flujos de tráfico de datos.
  ✓Suele usarse para evitar fugas de información de la empresa.

  × No son 100% efectivos.
  × Necesitan configuración.

- **Bloqueando el tráfico SSH**, aunque perderemos esa funcionalidad en toda la empresa.

Prueba

¿Preguntas?