The background of the slide features a blue-toned collage. In the upper center, there is a large, textured padlock icon. To its left, a portion of a globe is visible, showing the Americas. Above the globe, the text 'https://www' is partially visible, suggesting a web address. The overall theme is digital security.

Los mecanismos de seguridad convencionales ya no  
son suficientes



**OWASP**

The Open Web Application Security Project



**OWASP**

The Open Web Application Security Project

- Yered Céspedes
- Ingeniero en sistemas
- CISSP, CISA, CEH, CISM, ITIL Security+
- Pentester
- Finalista de Global Cyberlympics
- 5 años en el área



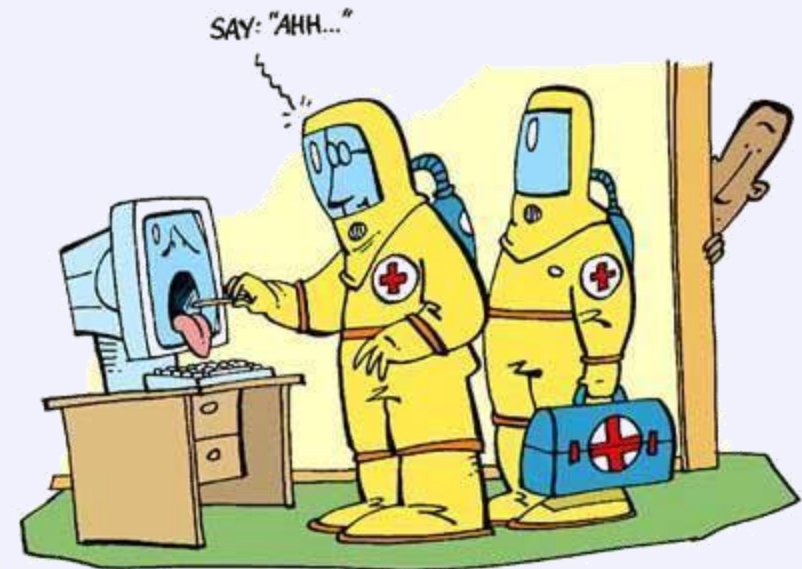
- Introducción a los sistemas convencionales de seguridad
- Ataques focalizados
- Demostración
- Recomendaciones



# Introducción a los mecanismos convencionales



- Un poco de historia:
  - Core War en 1949
  - Creeper en 1972 | Reaper
  - Introducción de “virus” en 1983

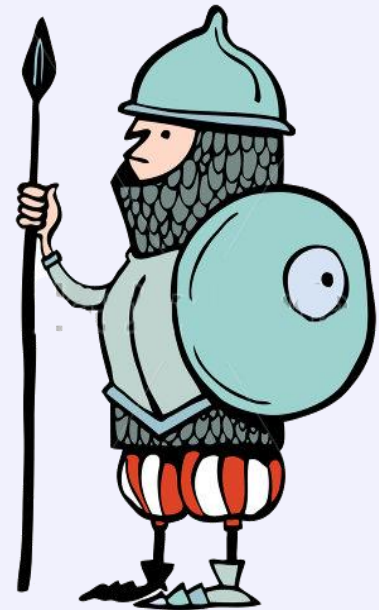




# Introducción a los mecanismos convencionales



- Antivirus
- Firewalls
- IPS
- Pero... como es que funcionan?



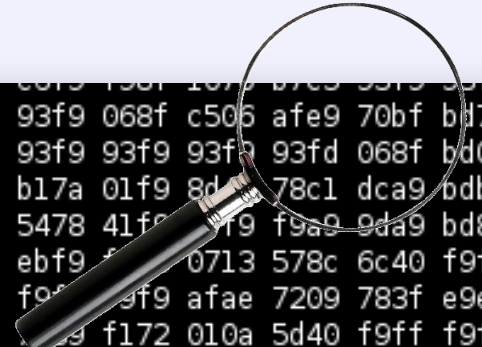


- Detección basada en firmas: Consiste en una base de datos de virus que ya han sido identificados, el software antivirus realiza una comparación entre el archivo a escanear y su base de datos para corroborar si existe alguna coincidencia.
- Detección heurística
  - Sandbox: los programas se ejecutan y analizan en un ambiente cerrado, si no se detectan comportamientos maliciosos son ejecutados posteriormente de forma normal.
  - Análisis de archivos: Se analizan el código del programa en búsqueda de comportamientos que resulten sospechosos.
  - Detección por firmas genéricas: utilizado usualmente para detectar virus que modifican su propio código. Trabajan con firmas genéricas o “plantillas” para analizar similitudes.



## OWASP

The Open Web Application Security Project



```
0000000: 00000a0: 93f9 068f c506 afe9 70bf bd7a 01f9 8d32
00000b0: 93f9 93f9 93f9 93fd 068f bd06 afed 70bf
00000c0: b17a 01f9 8d32 78c1 dca9 bdbf 72b7 c58c
00000d0: 5478 41f9 f9a9 9da9 bd8c 5878 41fd
00000e0: ebf9 f9f9 0713 578c 6c40 f9ff f9f9 7815
00000f0: f9f9 f9f9 afae 7209 783f e9eb f9f9 723d
0000100: f9f9 f172 010a 5d40 f9ff f9f9 b0b0 b0b0
0000110: 78cd f117 0707 167c 308c 08a6 a706 8fc5
0000120: 068f b106 8fbd 0619 acaf 9d58 c9f9 f9f9
0000130: 7c39 81ea c772 b9f5 c772 89e5 c772 a7f1
0000140: 54c7 7291 f112 f4c7 72b9 cdc7 7251 41f9
0000150: f9f9 ca22 723c a7a4 3bfd f9aa acaf aecf
0000160: 7295 dde1 cf72 bcc5 cf72 adfc 81fa 2cc7
0000170: 72b3 elc7 72a3 d9fa 241a c5b0 c772 cd72
0000180: fa0c ca06 05ca 3955 c33d 8dfe 3836 f4fa
0000190: 0112 0bcf c285 dded 8c26 723b 7a39 ddc7
00001a0: 72e1 fa24 9fc7 72f5 b2c7 72a3 e5fa 24c7
```

=



```
0000000: 00000a0: 93f9 068f c506 afe9 70bf bd7a 01f9 8d32
00000b0: 93f9 93f9 93f9 93fd 068f bd06 afed 70bf
00000c0: b17a 01f9 8d32 78c1 dca9 bdbf 72b7 c58c
00000d0: 5478 41f9 f9a9 9da9 bd8c 5878 41fd
00000e0: ebf9 f9f9 0713 578c 6c40 f9ff f9f9 7815
00000f0: f9f9 f9f9 afae 7209 783f e9eb f9f9 723d
0000100: f9f9 f172 010a 5d40 f9ff f9f9 b0b0 b0b0
0000110: 78cd f117 0707 167c 308c 08a6 a706 8fc5
0000120: 068f b106 8fbd 0619 acaf 9d58 c9f9 f9f9
0000130: 7c39 81ea c772 b9f5 c772 89e5 c772 a7f1
0000140: 54c7 7291 f112 f4c7 72b9 cdc7 7251 41f9
0000150: f9f9 ca22 723c a7a4 3bfd f9aa acaf aecf
0000160: 7295 dde1 cf72 bcc5 cf72 adfc 81fa 2cc7
0000170: 72b3 elc7 72a3 d9fa 241a c5b0 c772 cd72
0000180: fa0c ca06 05ca 3955 c33d 8dfe 3836 f4fa
0000190: 0112 0bcf c285 dded 8c26 723b 7a39 ddc7
00001a0: 72e1 fa24 9fc7 72f5 b2c7 72a3 e5fa 24c7
```

# Antivirus



**OWASP**

The Open Web Application Security Project





# Firewalls



**OWASP**

The Open Web Application Security Project





## OWASP

The Open Web Application Security Project

### Superfície de ataque = 10



# Ataques focalizados



## OWASP

The Open Web Application Security Project

Antes	Ahora
Por diversión	Crimen organizado
	Cyber-espionaje
Sin fines de lucro	Fines de lucro
El impacto en las organizaciones era menor	Afectar la imagen
Distribución masiva	Desarrollo focalizado
Destruir información o dejar inoperable el equipo	Utilizar los equipos para su beneficio (ej: DDoS, Zombies)





- La transición entre los ataques inofensivos a crimen organizado sido relativamente rápida
- Los ataques que han sonado más en los medios han sido desarrollados específicos para la empresa
- Qué es un ataque focalizado?





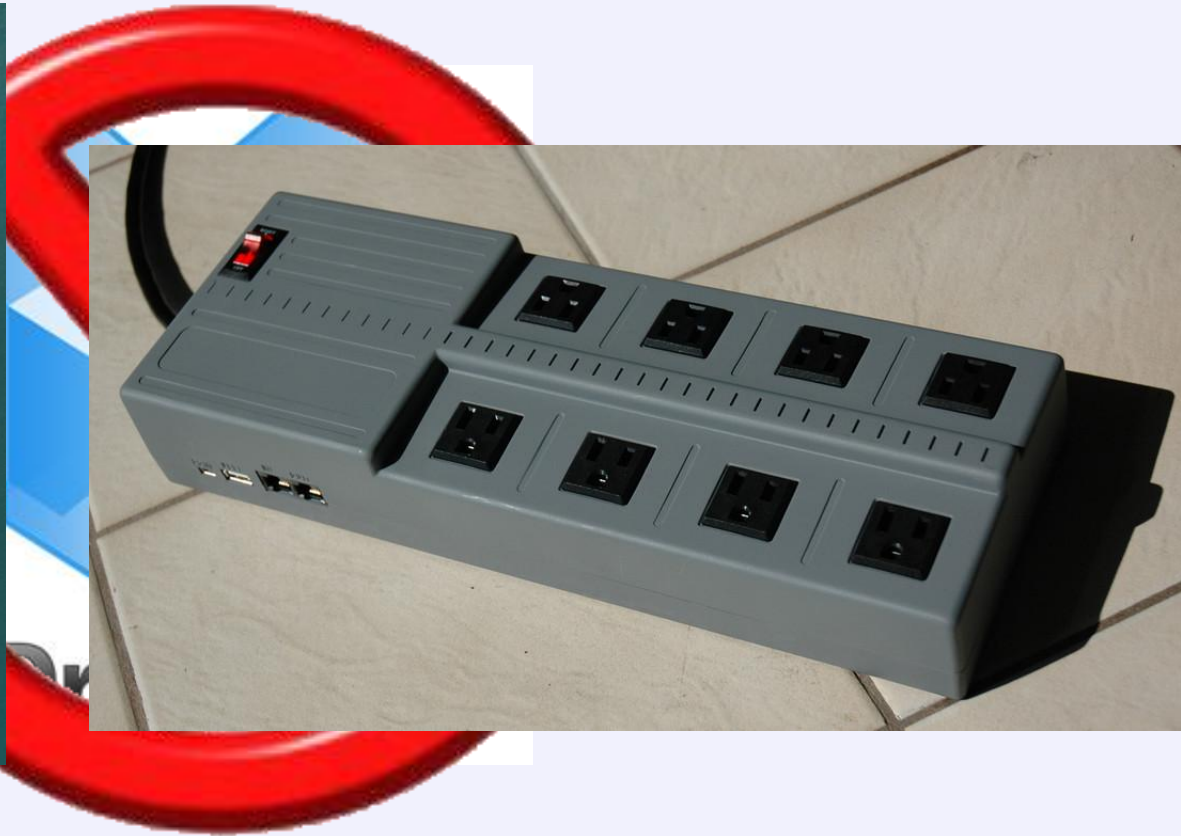
- Tendencias en los ataques:
  - En las organizaciones: ciber espionaje, uso de datos internos para realizar fraudes o simplemente dañar la imagen de la organización
  - Para los usuarios finales: robos en sus cuentas bancarias, man-in-the-browser, equipos zombie

# Ataques focalizados



**OWASP**

The Open Web Application Security Project



# Ataques focalizados



**OWASP**

The Open Web Application Security Project





- Que deben considerar las organizaciones para desarrollar sus aplicaciones para móviles?
  - Identificar y proteger los datos sensibles
  - Manejar de forma segura las credenciales del usuario
  - Asegurar que los datos sensibles son protegidos cuando sean transmitidos
  - Implementar de forma correcta la autorización, autenticación y manejo de sesiones
  - Asegurar la plataforma back-end





- De qué quiero protegerme?
  - Ataques comunes de virus, spam, bots?
  - Ataques focalizados y ciber espionaje?



Demo



**OWASP**

The Open Web Application Security Project

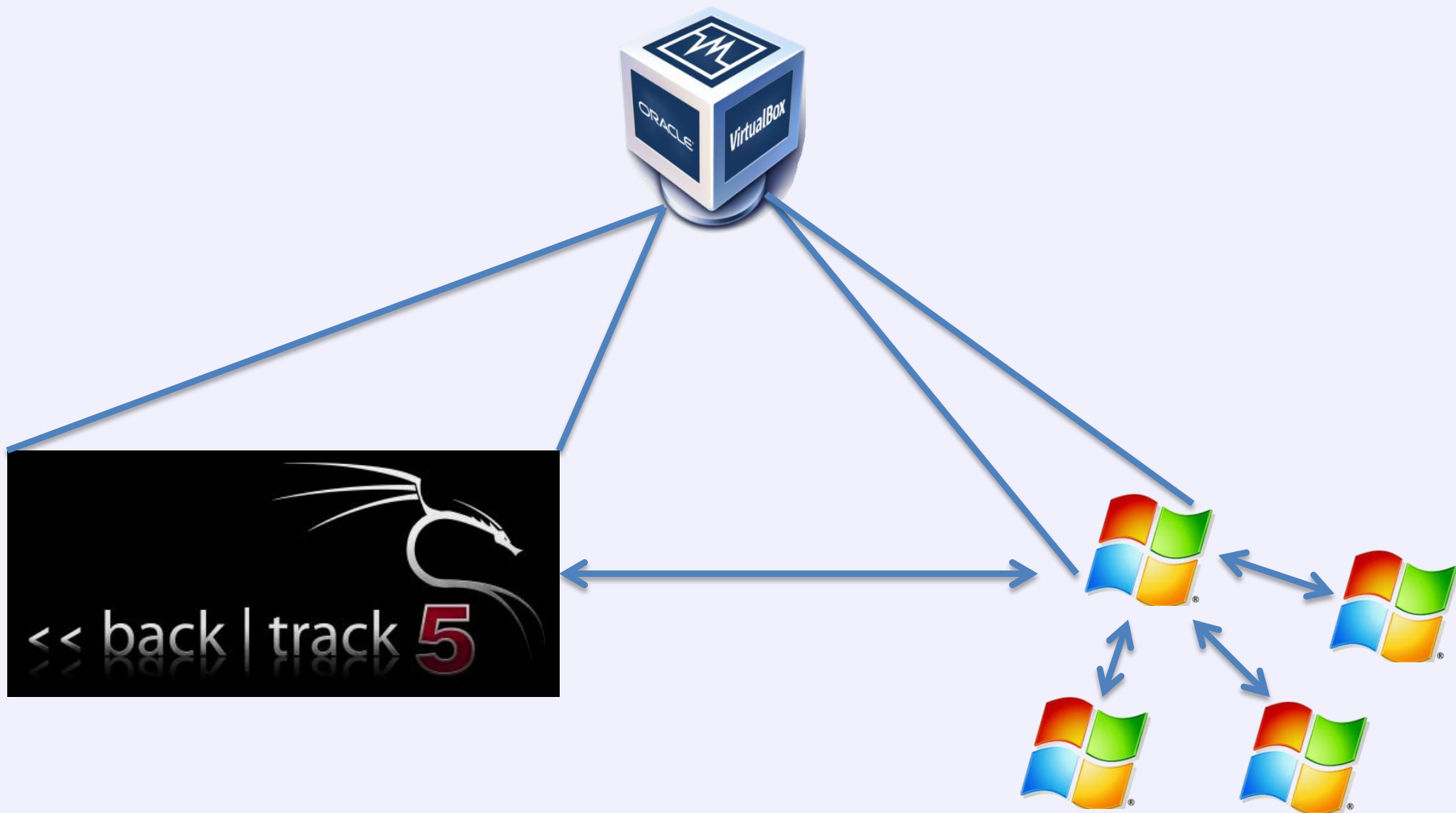
# Demostración

Demo



**OWASP**

The Open Web Application Security Project





- Como funciona?
  - No coincide con ninguna firma de los antivirus
  - Para conocer si se encuentra dentro de un sandbox intenta crear un archivo y conectarse a 127.0.0.1 en el puerto 445
  - Si no se encuentra dentro del sandbox ejecuta el código malicioso
  - Se copia a si mismo y se inicia automáticamente cuando el usuario inicia sesión





- Si su respuesta fue ataques focalizados y ciber espionaje:
  - Herramientas convencionales
  - NAC
  - SIEM
  - CSIRT
  - Monitoreo continuo
  - Gestión de parches / cambios en los equipos
  - Programas de capacitación para todo el personal
  - Políticas y procedimientos



## OWASP

The Open Web Application Security Project

- Clasifique su información
- Identifique todo aquello que acceda a su red
- Mantenga su infraestructura organizada y documentada
- Asegure físicamente todos los puntos de acceso a su red
- Realice pruebas que permitan medir de forma consistente su seguridad
- Implemente sistemas criptográficos para mantener la confidencialidad de los datos
- Establecer zonas de seguridad y segmentar la red
- Realmente todos los usuarios necesitan internet?



**OWASP**

The Open Web Application Security Project

# Preguntas?