Security A(r)t Work

www.securityartwork.es
www.s2grupo.es

S2 GRUPO

Securiza tu red con Snort y sus amigos

José Luis Chica Uribe
Técnico de seguridad IT
jchica@s2grupo.es

Índice

- Seguridad: conceptos
- Tipos de ataques
- ¿Cómo defenderse? Buenas prácticas
- IDS
  - Snort
  - OSSEC
- Openvas

Conceptos

- ¿De qué va esto? Seguridad de la información
- Información, elemento más valioso para una organización
- Imprescindible proteger el Sistema de Información de su acceso, uso, divulgación, o interrupción no autorizada

Conceptos 2

- Confidencialidad: visibilidad sólo a las personas autorizadas
- Integridad: fiable, sin errores, modificada ilegítimamente
- Disponibilidad: accesible siempre que se necesite
- Otros: autenticidad, trazabilidad, no repudio...

Amenazas

- Acceso no autorizado
  - Robo de datos
  - Pérdida de información
  - Interrupción del servicio
  - Interrupción de procesos de negocio
  - Deterioro de imagen corporativa

INYECCIÓN SQL

- Formulario de acceso con esta sentencia sql:

```
SELECT * FROM tablaLogin WHERE usuario='campoUser'
AND password='campoClave';
```

- ¿Qué pasaría si escribimos en el campo usuario: admin' or 1=1;--

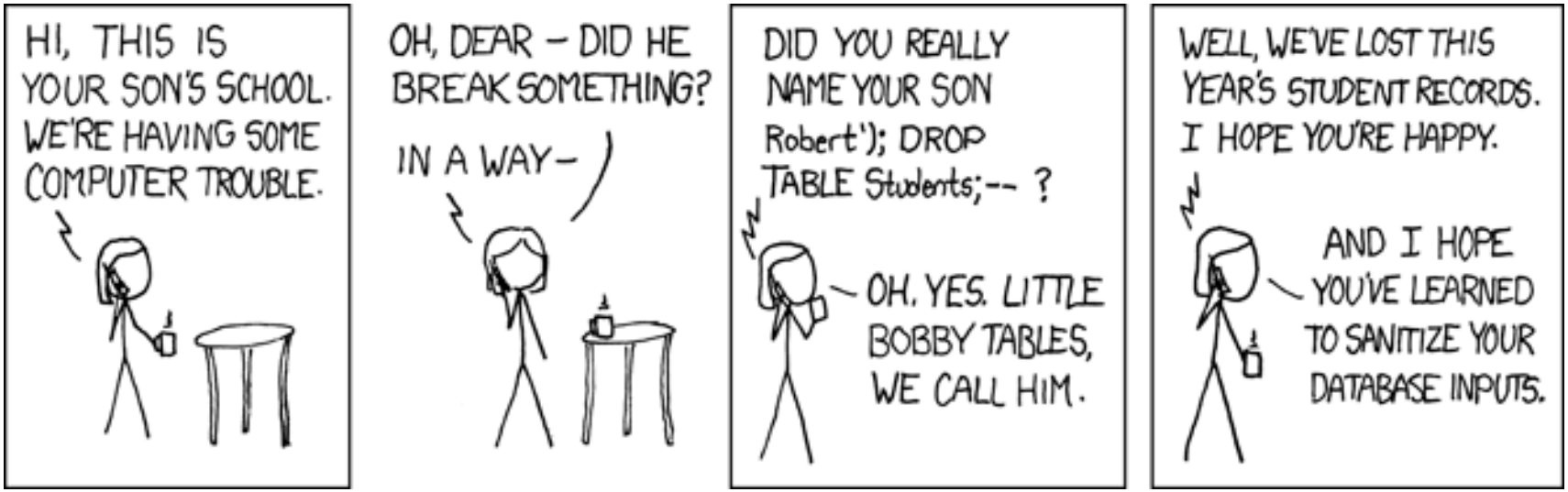
```
SELECT * FROM tablaLogin WHERE usuario='admin' or
1=1;-- AND password='';
```

- Hasta la cocina!

Solución?

- Sanear! Sanear! Sanear!

- Imprescindible comprobar todas las entradas que la aplicación recibe del usuario



Fuerza Bruta

- Servicio restringido con usuario y contraseña
- Cuentas con claves triviales o relacionadas con la persona (fecha de nacimiento, iniciales)
- Aplicaciones: thc-hydra, brutus, metasploit, prueban permutaciones o usando diccionario
- Malware también se aprovecha

Soluciones?

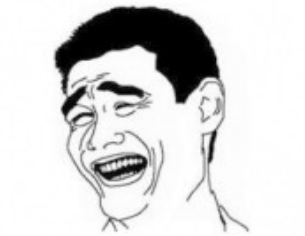
- Política de contraseñas
  - Mayúsculas, dígitos, caracteres especiales (#$&! @)
  - Longitud mínima
  - Impedir uso de iniciales, o palabras de diccionario
- Añadir retardo
- Evitar usar la misma contraseña para todo, en especial para servicios críticos
- Usar bóveda de contraseñas
- Desactivar cuenta o banear IP (peligroso)

Explotación de Vulnerabilidades

- Fallos en la implementación de software que produce agujeros de seguridad
  - Denegación de servicio
  - Ejecución de código remoto
  - Control total de la máquina

- Software antiguo, sin parchear
- Igualmente, uso frecuente de malware

¿Soluciones?

- Despedir al sysadmir 
- Realizar periódicamente auditorías de revisión de software
- Paradas programadas del servicio para actualizar el software

Y muchos más.....

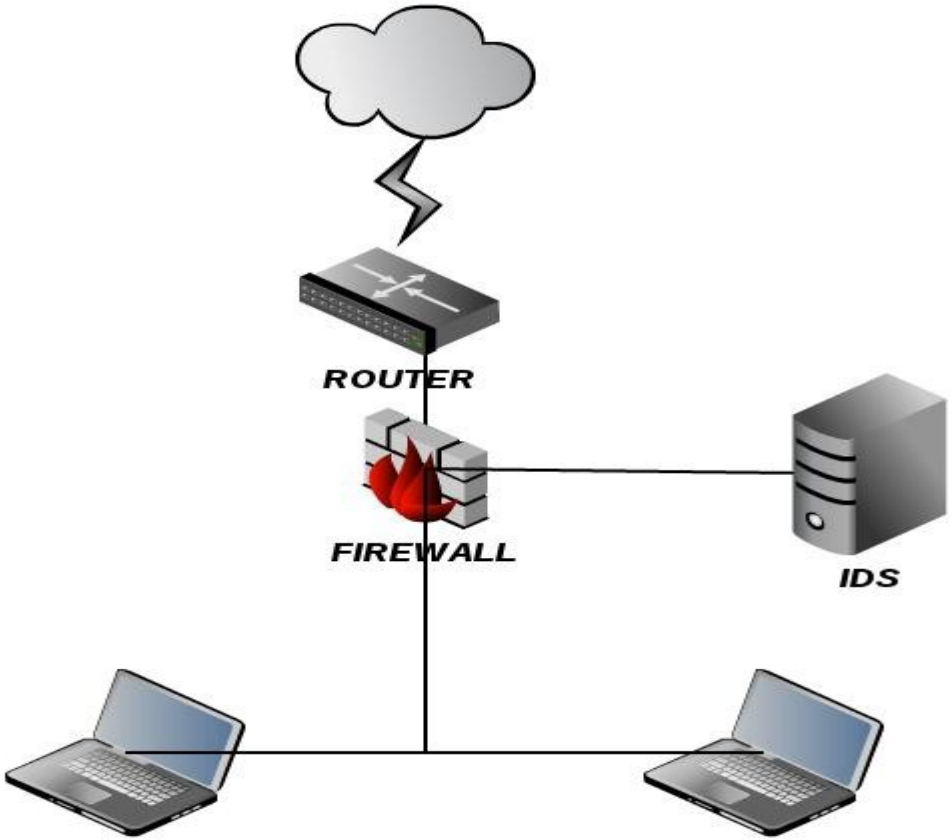
- XSS
- Directorio transversal
- Denegación de servicio
- Denegación de servicio distribuido
- DNS amplification attack

- OWASP TOP 10
- Hispasec una al día

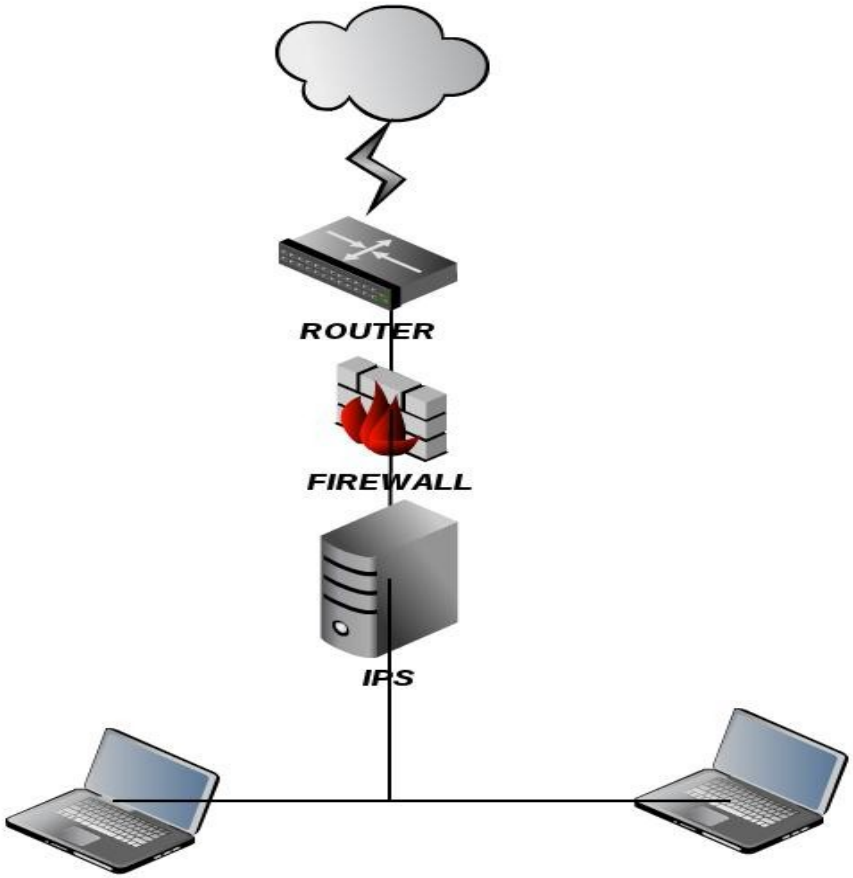
SNORT!

- Sistema de detección de intrusiones (IDS)
- Sistema de prevención de intrusiones (IPS)
- Analiza el tráfico en busca de anomalías o ataques
- Basado en patrones y reglas
- Opensource
- Muy extendido

ESQUEMA IDS



ESQUEMA IPS



¿Cómo funciona snort?

- Sniffer
  - Captura el tráfico
- Preprocesador
  - Lo hace entendible
- Motor de reglas
  - Busca patrones
- Procesador de salida
  - Loguea, escribe en BBDD...

Preprocesadores

- Frag3
  - Ensambla los datagramas fragmentados
- Stream5
  - Reensambla paquetes TCP
- http_inspect
  - Analiza sesiones web
- Smtp, ftp/telnet, ssh, rpc.....

Ya está bien de tanto rollo

»DEMO!

OSSEC

- Sistema de detección de intrusos basado en Host (HIDS)
- …. o en logs (LIDS)
- Monitoriza cambios en el sistema de ficheros
- Analiza logs en busca de eventos
- Basado en cliente – servidor
  - Clientes envían logs al servidor
  - Servidor analiza y busca patrones
- Capaz de correlar eventos
- Puede disparar comandos a los clientes

Estructura de OSSEC

- Rsyslog remoto
  - Recoge las reglas de los agentes
- Decoder
  - Las formatea en campos xml
- Motor de reglas
  - Busca patrones
- Output al log
  - Escribe a disco el evento generado

Ejemplo reglas

```
<rule id="5710" level="5">
  <if_sid>5700</if_sid>
  <match>illegal user|invalid user</match>
  <description>Attempt to login using a non-existent user</description>
  <group>invalid_login,authentication_failed,</group>
 </rule>

<rule id="5712" level="10" frequency="6" timeframe="120" ignore="60">
  <if_matched_sid>5710</if_matched_sid>
  <description>SSHD brute force trying to get access to </description>
  <description>the system.</description>
  <same_source_ip />
  <group>authentication_failures,</group>
 </rule>
```

»DEMO!

Openvas

- Scanner de vulnerabilidades
- Basado en Nessus
- Estructura cliente – servidor
- Integración con otras herramientas
  - Nikto
  - Nmap

»DEMO!

AENOR ER Empresa Registrada UNE-EN ISO 9001 ER-0343/2008
AENOR ER Seguridad Información UNE-ISO/IEC 27001 SI-0002/2006
AENOR ER Gestión Servicios TI UNE-ISO/IEC 20000-1 STI-0001/2011
AENOR ER Gestión I+D+i UNE 166002 IDI-0066/2010

GRACIAS

www.neuronasdigitales.com

Twitter: @BufferOverCat

S2 GRUPO

Ramiro de Maeztu, 7
46022 Valencia
Tel. (+34) 963 110 300
Fax (+34) 963 106 086

Orense, 85. Ed.Lexington
28020 Madrid
T. (+34) 915 678 488
F. (+34) 915 714 244

info@s2grupo.es
www.s2grupo.es
www.securityartwork.es