Redes y comunicación de Datos 2

Sesión 12

Ciclo: Agosto 2024

Universidad Tecnológica del Perú

Temario

- Presentación del logro de la sesión.
- Dinámica: Lluvia de ideas sobre los Puertos lógicos.
- Análisis de Puertos.
- Análisis de Vulnerabilidades.
- **Actividad:**
  - ***Explicar sobre Puertos y Vulnerabilidades.***

Logro general

Al finalizar el curso, el estudiante implementa soluciones para problemas de redes y comunicaciones de área local y extendida, empleando tecnología de interconexión y seguridad, según las necesidades planteadas.

Logro de aprendizaje de la sesión

Al finalizar la unidad, el estudiante explica cómo las vulnerabilidades ponen en riesgo la seguridad LAN, para mitigar algunos ataques informáticos, a través de ejemplos desarrollados en clase.

Buenas Prácticas

Buenas Prácticas

Con respecto a la Sesión 11

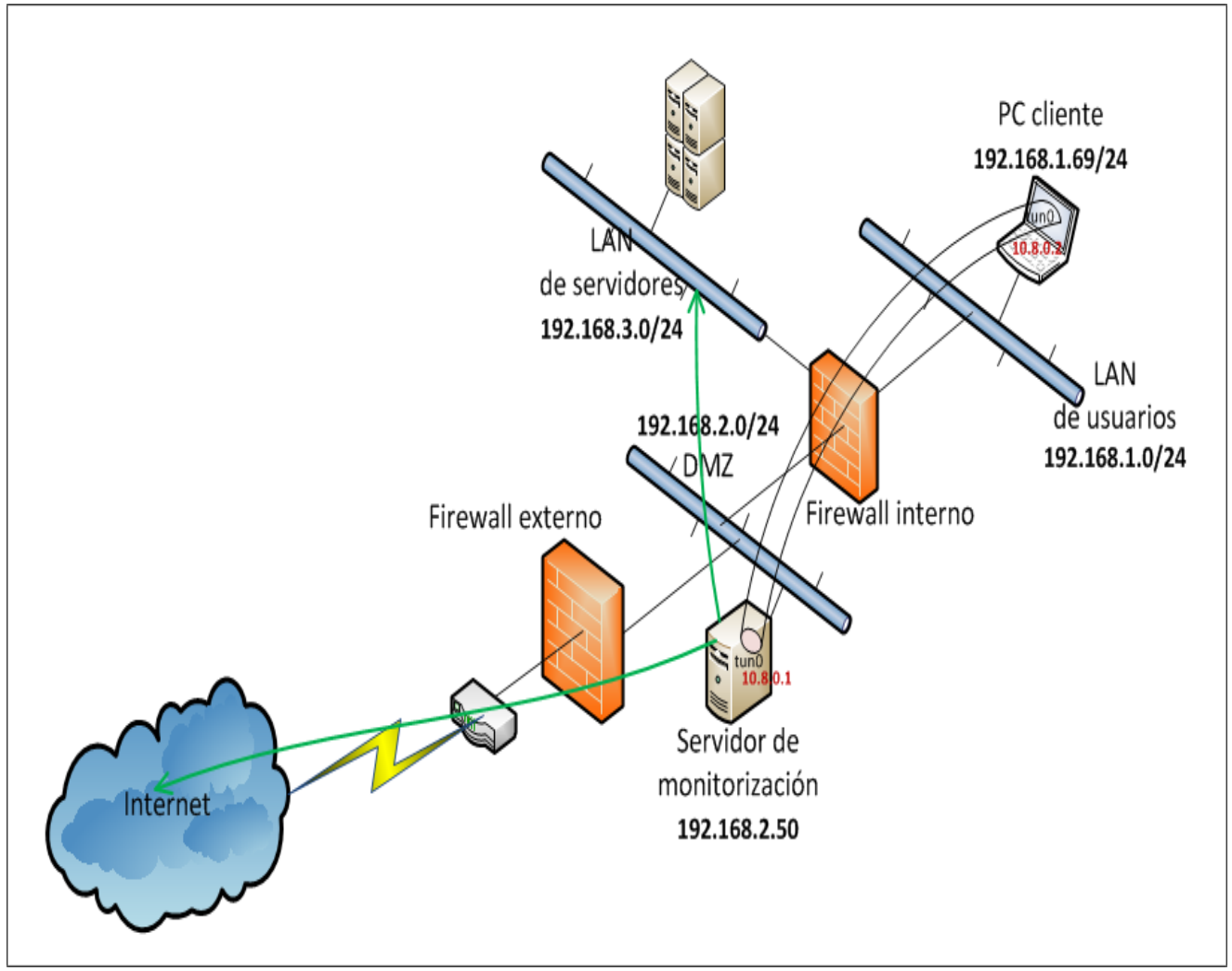
- ¿Qué temas desarrollamos?
- Podrias comentarme de manera breve por favor.

Recuerda que es importante que revises el material de clases de cada semana.

Conceptos de seguridad de la LAN

La seguridad de red es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos.

- Incluye tecnologías de hardware y software.
  - Está orientada a diversas amenazas.
    - Evita que ingresen o se propaguen por la red.
  - La seguridad de red eficaz administra el acceso a la red.



La figura del Hacker

¿Qué tipos de hackers existen en función de los objetivos que tienen?

Black Hat Hackers

White Hat Hackers

Gray (Grey) Hat Hackers

Buenas Prácticas

Sesión 9

Lluvia de ideas sobre la capa enlace de datos

- ¿Qué es un análisis de puertos?
- ¿Para qué sirve el análisis de puertos?

Análisis de puertos

Análisis de puertos

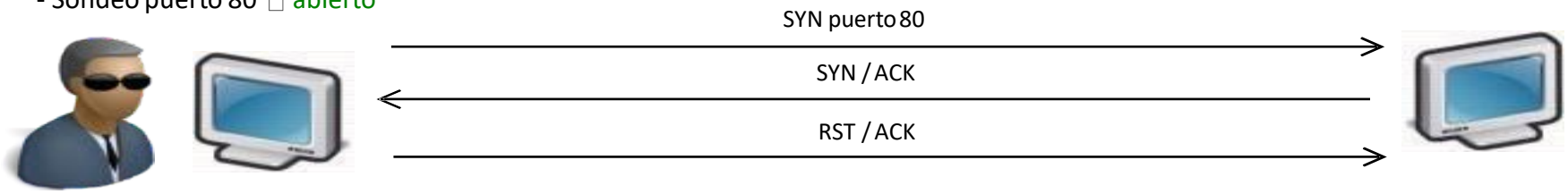
- **¿Qué información puede obtener un atacante?**

El análisis de puertos se utiliza para comprobar qué puertos de la red están abiertos y pueden recibir o enviar datos. También se utiliza para enviar paquetes a puertos concretos de un anfitrión y analizar respuestas para identificar vulnerabilidades.

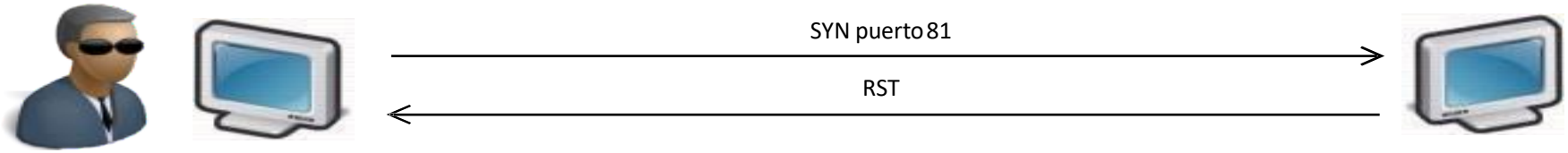
Análisis de puertos

¿Cómo se realiza el análisis de puertos?

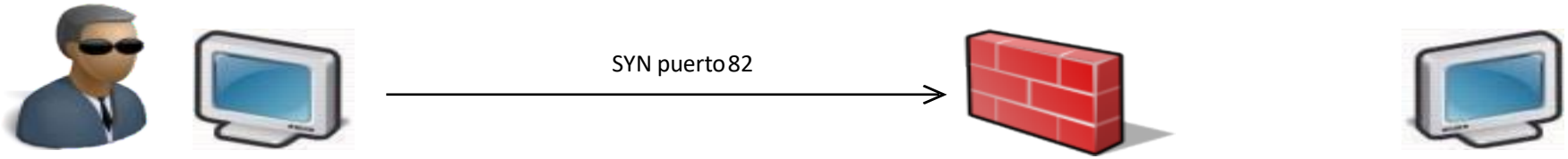
- Sondeo puerto 80 □ abierto



- Sondeo puerto 81 □ cerrado



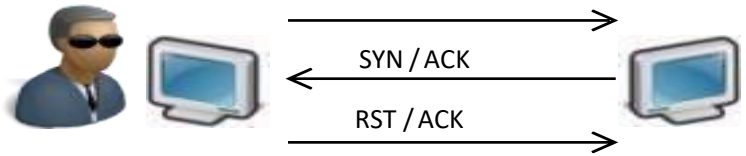
- Sondeo puerto 82 □ filtrado



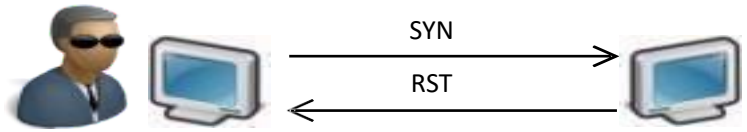
Análisis de puertos

Tipos de escaneos de puertos (I)

- Existen varios tipos de escaneos de puertos con distintas características:
  - Robustos.
  - De evaluación de firewalls.
  - De evasión de firewalls.
  - Silenciosos.
  - Ocultación.
  - Etc.
- TCP Scan:
  - Establecimiento completo de una conexión.
  - 3-way handshake.



Abierto

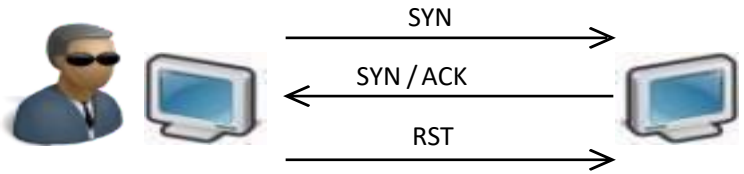


Cerrado

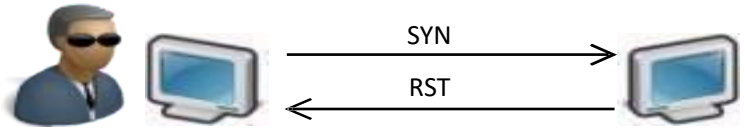
Análisis de puertos

Tipos de escaneos de puertos (II)

- **Stealth Scan (Half-Open Scan):**

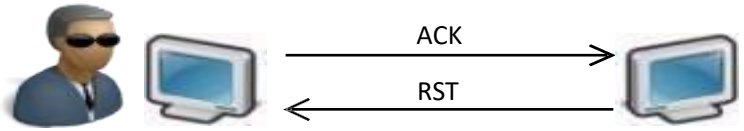


Abierto

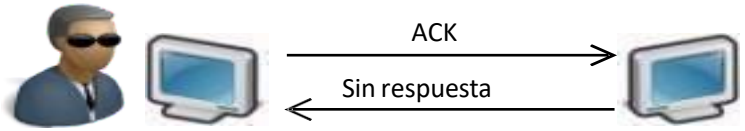


Cerrado

- **ACK Scan:**



Sin firewall

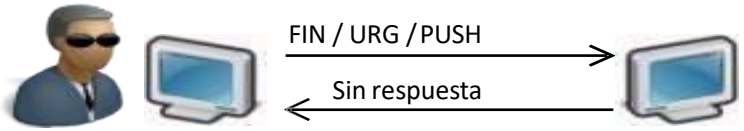


Firewall

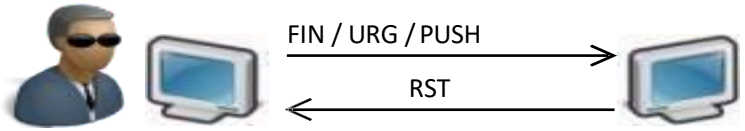
Análisis de puertos

Tipos de escaneos de puertos (III)

- **Xmas Scan:**

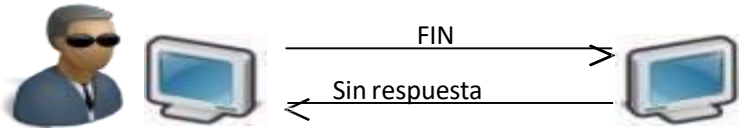


Abierto

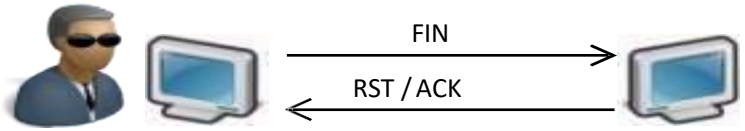


Cerrado

- **FIN Scan:**



Abierto

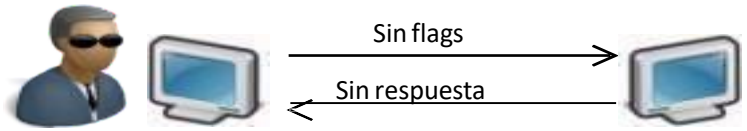


Cerrado

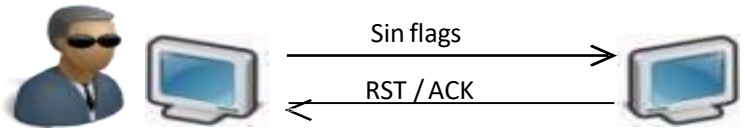
Análisis de puertos

Tipos de escaneos de puertos (IV)

- **NULL Scan:**

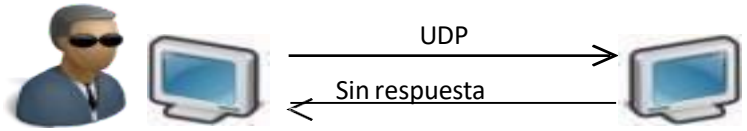


Abierto

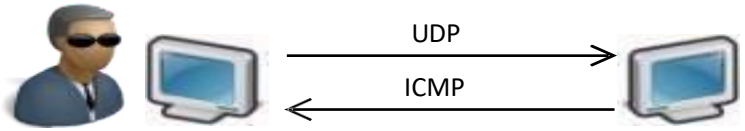


Cerrado

- **UDP Scan:**



Abierto

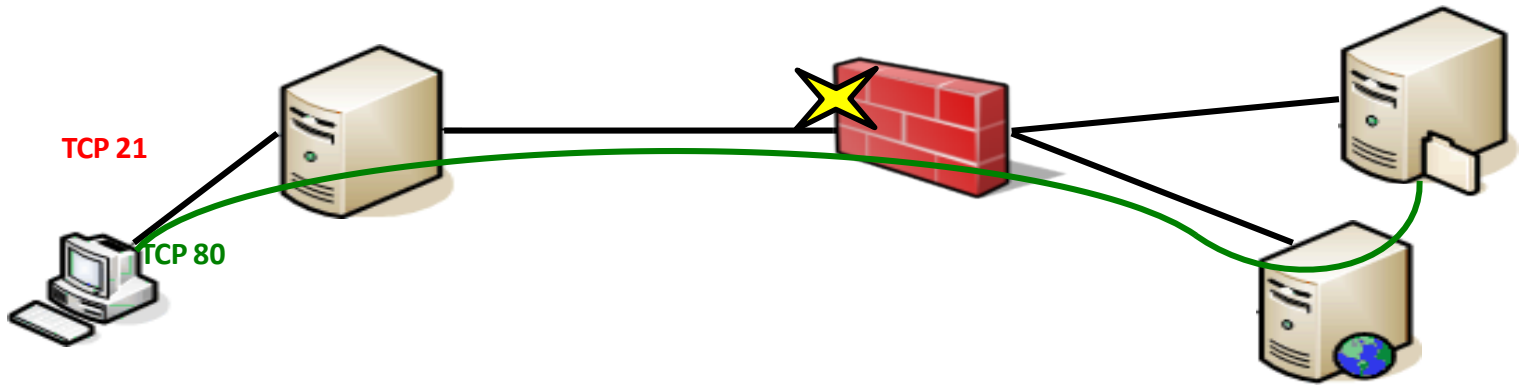


Cerrado

Análisis de puertos

Otras técnicas de análisis de puertos (II)

- **Port tunneling:** Técnica que combinada con el análisis de Puerto, permite:

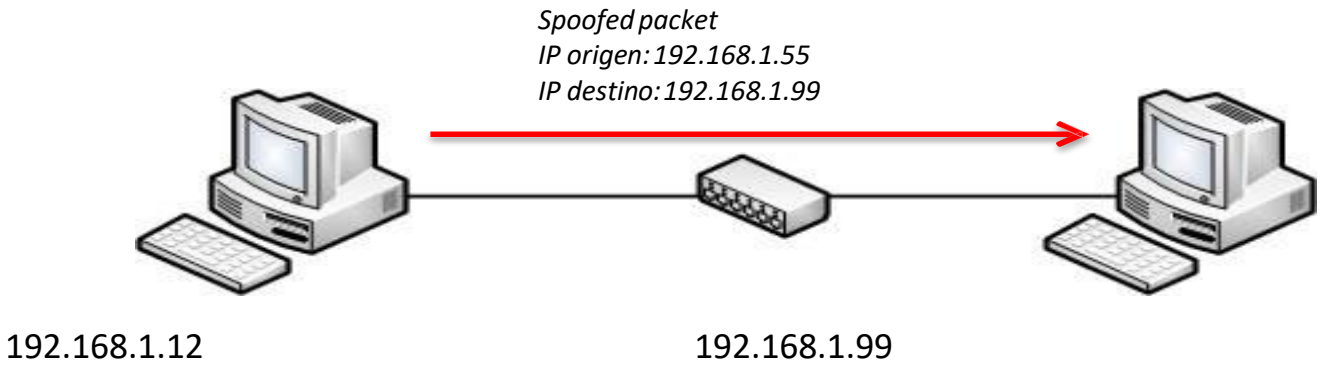


- Ejemplo de reglas del firewall:
  - Deniega todo el tráfico que provenga de fuera de la red.
  - Excepto el dirigido al servidor web por el puerto 80.

Análisis de puertos

Otras técnicas de análisis de puertos (III)

- **IP Spoofing:** Técnica que combinada con el análisis de Puerto, permite:



- Cuando se realiza IP Spoofing, la respuesta de la víctima se dirige a la IP falseada.
- Esta técnica se suele utilizar para denegaciones de servicio o si el sistema de la IP falseada está bajo nuestro control.

Análisis de puertos

Banner grabbing

- El banner grabbing consiste en la extracción de información de los puertos abiertos.
- Esta información está relacionada con el servicio y versión que se está ejecutando en dicho puerto.
- De esta manera, se extrae información de los posibles vectores de ataque que tenemos.
- Ejemplo:
  - Banner de un puerto 80 que está ejecutando el servicio http.

(Status-Line)	HTTP/1.1 200 OK
Cache-Control	max-age=432000
Content-Length	348
Content-Type	image/png
Last-Modified	Thu, 29 May 2014 14:42:30 GMT
Accept-Ranges	bytes
Etag	"08fbe374c7bcf1:39c2"
Server	Microsoft-IIS/6.0
X-Powered-By	ASP.NET
Date	Thu, 04 Sep 2014 11:29:45 GMT
Connection	Keep-Alive
Age	0

Análisis de Vulnerabilidades

Análisis de vulnerabilidades

¿Qué es?

¿Qué quiere decir vulnerable?

Ejemplo:

- Una página web está soportada por un servidor web Apache.
- La versión de dicho servidor posee una vulnerabilidad conocida y documentada.
- Un atacante utiliza la documentación citada para obtener el control del servidor.

Análisis de vulnerabilidades

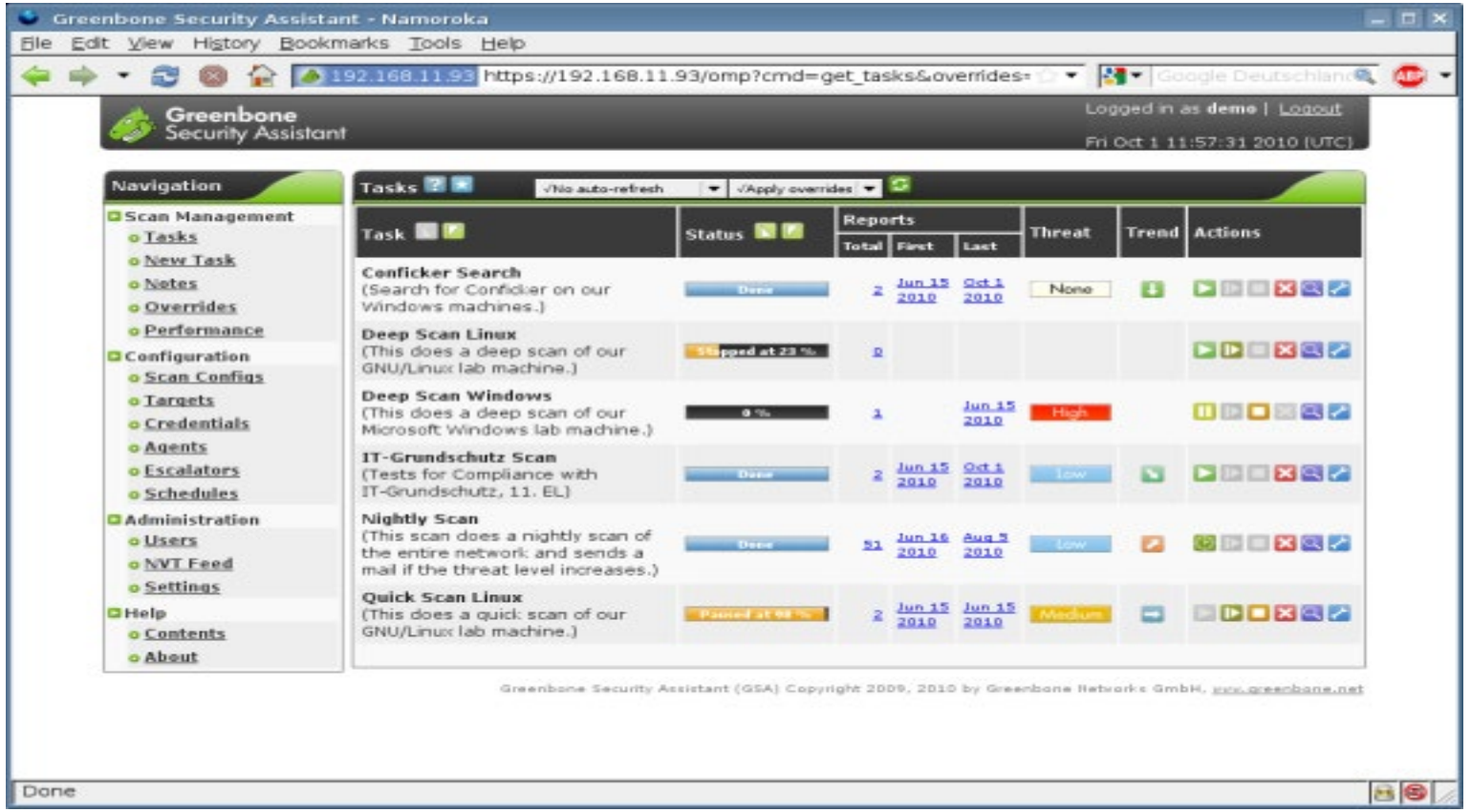
¿Cómo se realiza?

- **El descubrimiento y análisis de servicios en internet vulnerables está basado en:**
  - Análisis de puertos.
  - Banner Grabbing.
- **Una vez obtenidos los puertos abiertos, los servicios en ejecución y sus versiones:**
  - Se comparan las versiones y servicios con una base de datos de vulnerabilidades conocidas.
  - Si alguna coincide, se considera vulnerable al servicio.
  - Es posible que existan falsos positivos y que realmente no sea vulnerable.
- **Este proceso se automatiza mediante programas que realizan las siguientes fases:**
  - Análisis de puertos.
  - Banner Grabbing.
  - Comparación con base de datos de vulnerabilidades.

Análisis de vulnerabilidades

OpenVAS

- El escáner de vulnerabilidades abierto:



Fuente: *www.openvas.org*

Explotación de Vulnerabilidades

Explotación de vulnerabilidades

¿En qué consiste?

- Aprovechar las vulnerabilidades de un servicio o protocolo para realizar una acción no permitida en el sistema:
  - Obtener acceso al sistema o a la base de datos.
  - Obtener información confidencial.
  - Modificar, eliminar o añadir información.
  - Causar daños en el sistema.
  - Etc.

¿Cómo se realiza?

- Tanto de forma manual, como utilizando exploits.

Explotación de vulnerabilidades

¿Qué es un exploit?

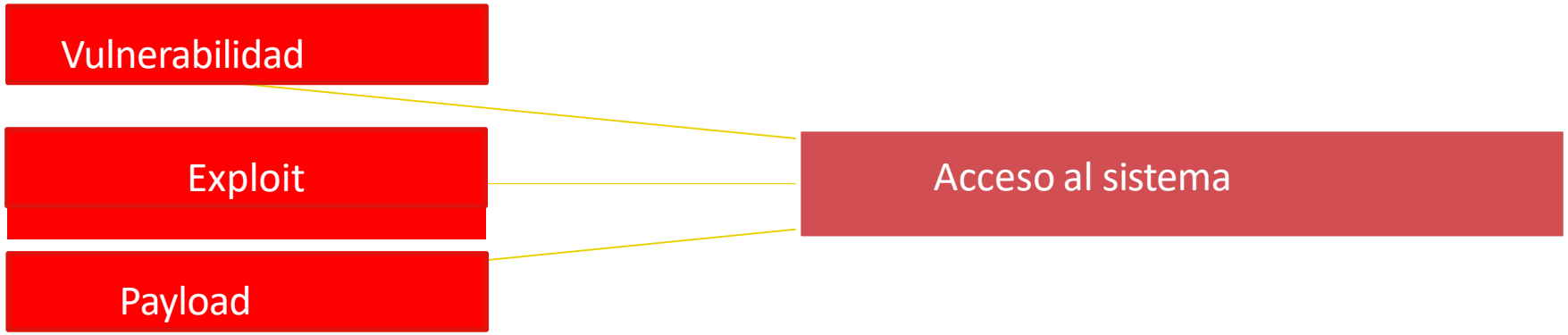
- Es un fragmento/parte de código especialmente preparado para explotar una vulnerabilidad para la cual:
  - Puede existir un parche que soluciona la vulnerabilidad.
  - No existe un parche para solucionar la vulnerabilidad, en cuyo caso se denomina 0-day.

- Normalmente, son pequeños programas en los que el atacante únicamente tiene que especificar:
  - IP destino.
  - Puerto destino.
  - Otros parámetros propios de la vulnerabilidad.
  - El payload.

Explotación de vulnerabilidades

¿Qué es un payload?

- Es otro fragmento de código que va siempre asociado al exploit.
- Mientras que con el exploit se explota una vulnerabilidad del programa, con el payload se ejecuta una acción provechosa para el atacante.
- Ejemplo:
  - Ejecutamos un exploit en un sistema vulnerable.
  - A ese exploit le asociamos un payload que, por ejemplo, va a crear un usuario administrador en el sistema con credenciales conocidas.



Post-explotación de Vulnerabilidades

Post-explotación de vulnerabilidades

¿Y ahora qué?

- Una vez se ha obtenido acceso al sistema, los atacantes tienen multitud de opciones:
  - Uso del sistema comprometido para saltar a otro sistema (pivoting).
  - Robo de información.
  - Modificación de datos.
  - Realización de daños al sistema.
  - Robo de identidad.
  - Espionaje.
  - Robo de datos personales.
  - Extorsión.
  - Fraude.
  - Etc.

¿Preguntas?

Actividades

Laboratorio especializado

Los estudiantes resuelven la siguiente actividad.

Actividades

- ¿Qué son los puertos?
- ¿Qué es un análisis de puerto?
- Conoces algunos tipos de escaneo de puertos.
- Conoces algunas técnicas de análisis de puertos.
- ¿Qué es la vulnerabilidad?
- ¿Qué es la explotación de la vulnerabilidad?

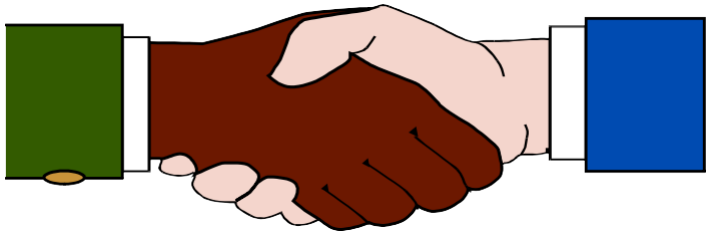
Conclusiones

¿Qué aprendí en esta sesión?

¿Qué aprendí en está sesión?

- Las políticas de seguridad de la red son creadas por empresas y organizaciones gubernamentales para proporcionar un marco a seguir para los empleados durante su trabajo diario.
- Los profesionales de la seguridad de la red a nivel de gestión son responsables de crear y mantener la política de seguridad de la red.
- Los ataques de red se clasifican fácilmente, aprenda sobre ellos y abórdelos de manera adecuada.
- Los virus, gusanos y caballos de Troya son tipos específicos de ataques de red. De manera más general, los ataques a la red se clasifican como ataques de reconocimiento, acceso o DoS.
- Mitigar los ataques de red es el trabajo de un profesional de seguridad de redes.

Gracias



Universidad
Tecnológica
del Perú