Comenzado el	miércoles, 5 de junio de 2024, 16:40
Estado	Finalizado
Finalizado en	martes, 11 de junio de 2024, 14:21
Tiempo empleado	5 días 21 horas
Puntos	31,00/33,00
Calificación	**9,39** de 10,00 (**93,94**%)

Pregunta 1

Parcialmente correcta

Se puntúa 5,00 sobre 6,00

Analice la información de segudidad de la siguiente página web siguiendo los pasos indicados en la guía del trabajo práctico:

https://mail.ingenieria.uncuyo.edu.ar/mail/

Algoritmo de firma del certificado: SHA-256 con encriptación RSA ✓

Autoridad de certificación: Let's Encrypt ✓

Algoritmo de encriptación de clave pública: Curvas elípticas ✓

Algoritmo de encriptación de clave simétrica: AES ✓

Protocolo de seguridad: TSL 1.3 ✓

Podrá un impostor robar sus datos Si ✗

Pregunta 2

Parcialmente correcta

Se puntúa 5,00 sobre 6,00

Analice la información de segudidad de la siguiente página web siguiendo los pasos indicados en la guía del trabajo práctico:

https://hb.redlink.com.ar/bna/login.htm

Algoritmo de firma del certificado: SHA-256 con encriptación RSA ✓

Autoridad del certificado: DigiCert Inc ✓

Algoritmo de encriptación de clave pública: RSA ✓

Algoritmo de encriptación de clave simétrica: AES ✓

Protocolo de seguridad: TSL 1.1 ✗

Podrá un impostor robar sus datos No ✓

Pregunta 3

Correcta

Se puntúa 6,00 sobre 6,00

Analice la información de seguridad de la siguiente página web siguiendo los pasos indicados en la guía del trabajo práctico:

http://www.hipertexto.info/documentos/internet_tegn.htm

Algoritmo de firma del certificado: No posee certificado ni encripta ✓

Autoridad de certificación: No posee certificado ni encripta ✓

Algoritmo de encriptación de clave pública: No posee certificado ni encripta ✓

Algoritmo de encriptación de clave simétrica: No posee certificado ni encripta ✓

Protocolo de encriptación: No posee certificado ni encripta ✓

Podrá un impostor robar sus datos: Si ✓

Pregunta 4

Correcta

Se puntúa 12,00 sobre 12,00

Compare la página web original del Banco Patagonia respecto a una página web clonada corriendo en un servidor Apache en la red local del laboratorio de Ingeniería.

Página web clonada:

Algoritmo de firma del certificado: No posee certificado ni encripta ✓ .

Autoridad del certificado: No posee certificado ni encripta ✓ .

Algoritmo de encriptación de clave pública: No posee certificado ni encripta ✓ .

Algoritmo de encriptación de clave simétrica: No encripta ✓ .

¿La URL tiene la apariencia de ser una URL real de un banco? No ✓

Podrá un impostor robar sus datos Si ✓

Página web real:

Algoritmo de firma del certificado: SHA-256 con encriptación RSA ✓ .

Autoridad del certificado: DigiCert ✓ .

Algoritmo de encriptación de clave pública: RSA ✓ .

Algoritmo de encriptación de clave simétrica:

AES ✓ .

¿La URL tiene la apariencia de ser una URL real de un banco? Si

✓

Podrá un impostor robar sus datos No ✓

Pregunta 5

Correcta

Se puntúa 1,00 sobre 1,00

En la Actividad 4 "ARP spoofing" se pide ejecutar el comando:

sudo hping3 --flood --icmp --spoof [IP_a_atacar] [IP_a_atacar] --interval u1

¿Que acción realiza el comando?

Seleccione una:

a. Ninguna respuesta es correcta.

b. Envenena la tabla ARP de la máquina víctima, falsificando la dirección MAC de la entrada "IP router - MAC router".

c. Envenena la tabla ARP de la máquina víctima, falsificando la dirección IP de la entrada "IP router - MAC router".

d. Realiza un ataque DoS a la máquina víctima con paquetes ICMP, haciendo creer a la máquina víctima que ella misma se envía los paquetes. ✓

e. Realiza un ataque DoS a la máquina víctima con paquetes ICMP, haciendo creer a la máquina víctima que los paquetes provienen del router.

f. Envenena la tabla ARP del router, falsificando la dirección IP de la entrada "IP router - MAC router".

g. Realiza un ataque DoS al router con paquetes ICMP, haciendo creer al router que el mismo se envía los paquetes.

h. Envenena la tabla ARP del router, falsificando la dirección MAC de la entrada "IP router - MAC router".

Respuesta correcta

La respuesta correcta es:
Realiza un ataque DoS a la máquina víctima con paquetes ICMP, haciendo creer a la máquina víctima que ella misma se envía los paquetes.

Pregunta 6

Correcta

Se puntúa 1,00 sobre 1,00

En la Actividad 4 "ARP spoofing" se pide ejecutar el comando:

sudo nping --arp --count 1000 -arp-type ARP-reply --rate 10 --arp-sender-mac <Cualquier MAC> --arp-sender-ip <IP del access point o router> <IP atacada>

¿Que acción realiza el comando?

Seleccione una:

a. Envenena la tabla ARP del router, falsificando la dirección MAC de la entrada "IP router - MAC router".

b. Realiza un ataque DoS a la máquina víctima con paquetes ICMP, haciendo creer a la máquina víctima que los paquetes provienen del router.

c. Envenena la tabla ARP del router, falsificando la dirección IP de la entrada "IP router - MAC router".

d. Envenena la tabla ARP de la máquina víctima, falsificando la dirección IP de la entrada "IP router - MAC router".

e. Envenena la tabla ARP de la máquina víctima, falsificando la dirección MAC de la entrada "IP router - MAC router". ✓

f. Ninguna respuesta es correcta.

g. Realiza un ataque DoS al router con paquetes ICMP, haciendo creer al router que el mismo se envía los paquetes.

h. Realiza un ataque DoS a la máquina víctima con paquetes ICMP, haciendo creer a la máquina víctima que ella misma se envía los paquetes.

Respuesta correcta

La respuesta correcta es:
Envenena la tabla ARP de la máquina víctima, falsificando la dirección MAC de la entrada "IP router - MAC router".

Pregunta 7

Correcta

Se puntúa 1,00 sobre 1,00

En la actividad 3 del trabajo práctico se pide agregar un certificado a su página web, y luego ingresar a través de https. El navegador web muestra una advertencia indicando que el sitio no es seguro. ¿Porqué motivo el sitio web no es seguro?

Seleccione una:

- a. El certificado está firmado por alguien que no es una autoridad de certificación reconocida por su navegador. ✓
- b. La clave pública indicada en el certificado no le pertenece a la IP o DNS indicados.
- c. El certificado está firmado y la información está encriptada. El error no puede explicarse con los conceptos vistos en la materia.
- d. El certificado no está firmado.
- e. En el certificado no hay ninguna clave pública.
- f. Ninguna respuesta es correcta.
- g. La información intercambiada entre el cliente y el navegador no está encriptada y por lo tanto puede ser vista por terceros.
- h. Ninguna respuesta es correcta.

Respuesta correcta

La respuesta correcta es:
El certificado está firmado por alguien que no es una autoridad de certificación reconocida por su navegador.