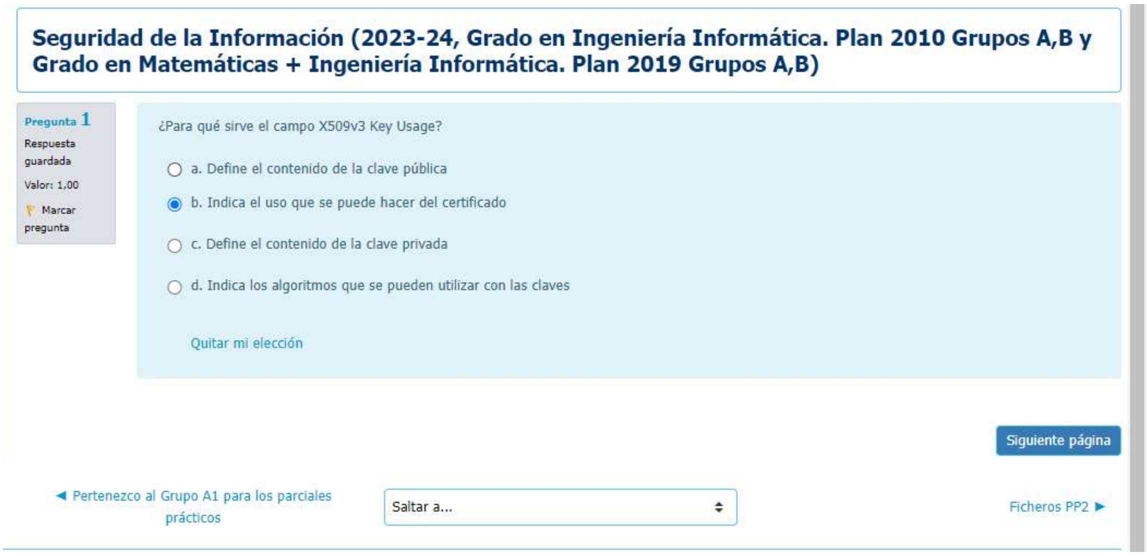


Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

Pregunta 1 Respuesta guardada Valor: 1,00

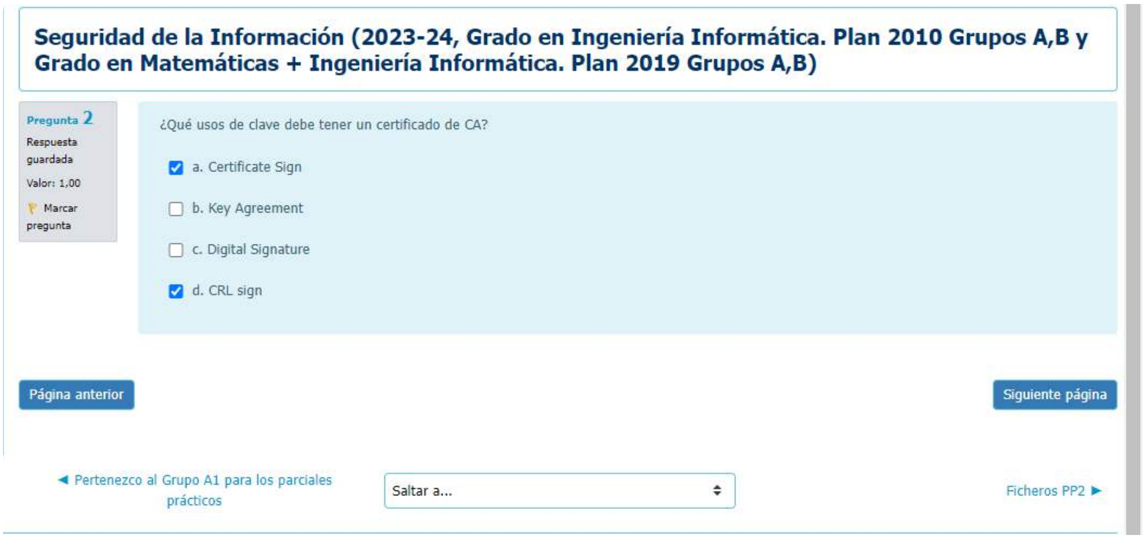
¿Para qué sirve el campo X509v3 Key Usage?

○ a. Define el contenido de la clave pública

● b. Indica el uso que se puede hacer del certificado

○ c. Define el contenido de la clave privada

○ d. Indica los algoritmos que se pueden utilizar con las claves



Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

Pregunta 2 Respuesta guardada Valor: 1,00

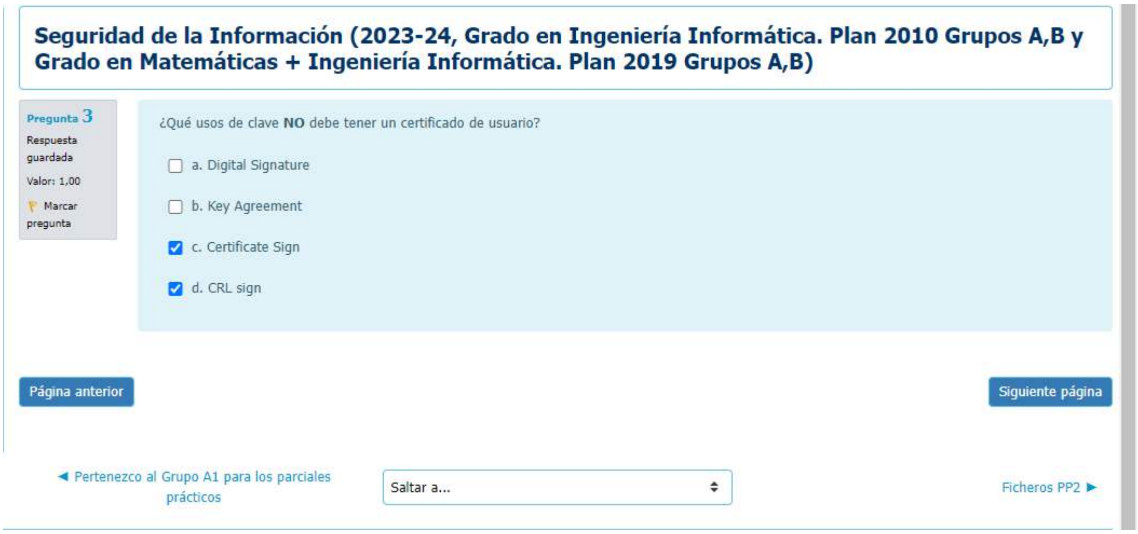
¿Qué usos de clave debe tener un certificado de CA?

☑ a. Certificate Sign

□ b. Key Agreement

□ c. Digital Signature

☑ d. CRL sign



Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

Pregunta 3 Respuesta guardada Valor: 1,00

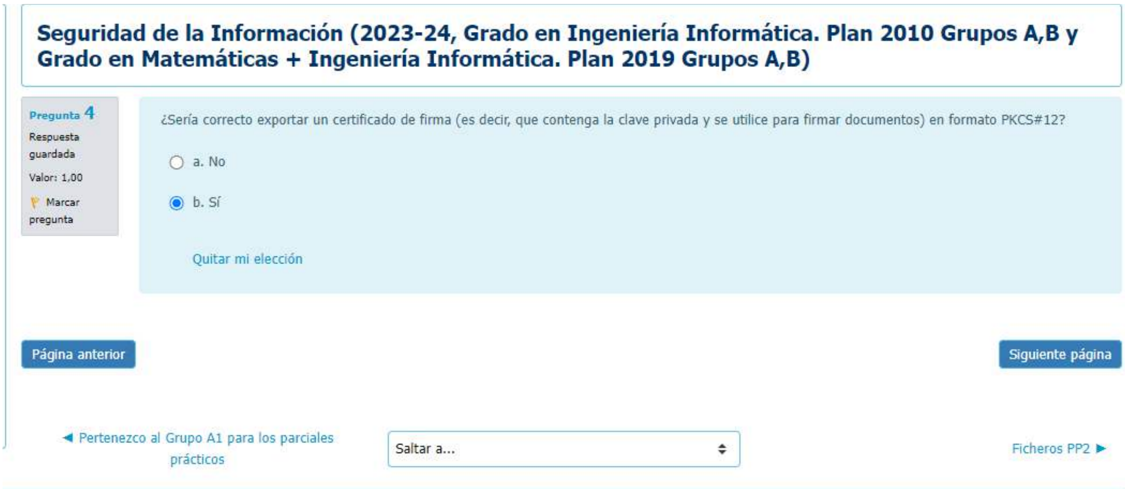
¿Qué usos de clave **NO** debe tener un certificado de usuario?

□ a. Digital Signature

□ b. Key Agreement

☑ c. Certificate Sign

☑ d. CRL sign



Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

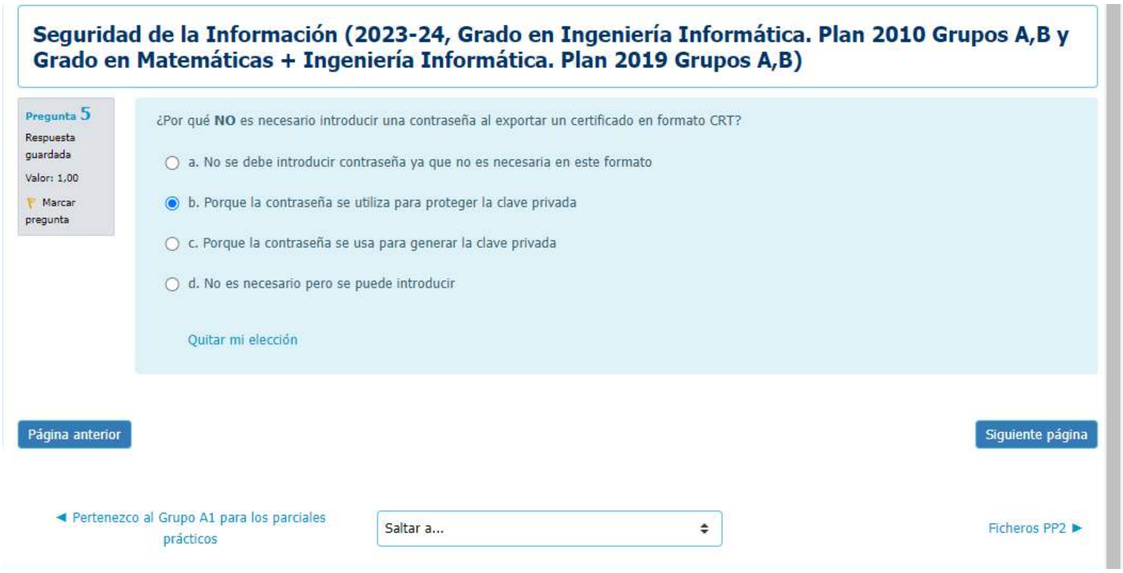
Pregunta 4
Respuesta guardada
Valor: 1,00
Marcar pregunta

¿Sería correcto exportar un certificado de firma (es decir, que contenga la clave privada y se utilice para firmar documentos) en formato PKCS#12?

○ a. No

● b. Sí

Quitar mi elección



Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

Pregunta 5
Respuesta guardada
Valor: 1,00
Marcar pregunta

¿Por qué **NO** es necesario introducir una contraseña al exportar un certificado en formato CRT?

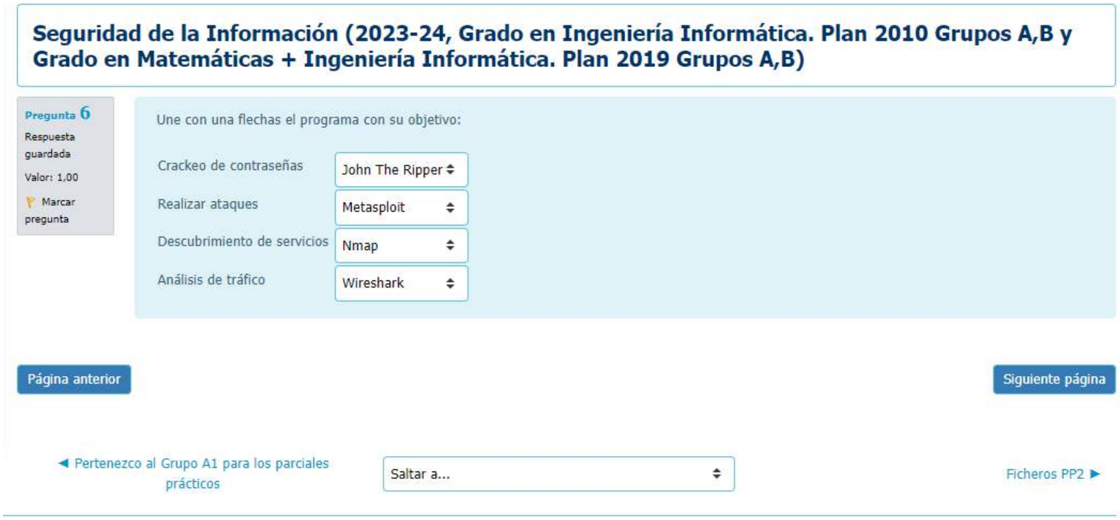
○ a. No se debe introducir contraseña ya que no es necesaria en este formato

● b. Porque la contraseña se utiliza para proteger la clave privada

○ c. Porque la contraseña se usa para generar la clave privada

○ d. No es necesario pero se puede introducir

Quitar mi elección

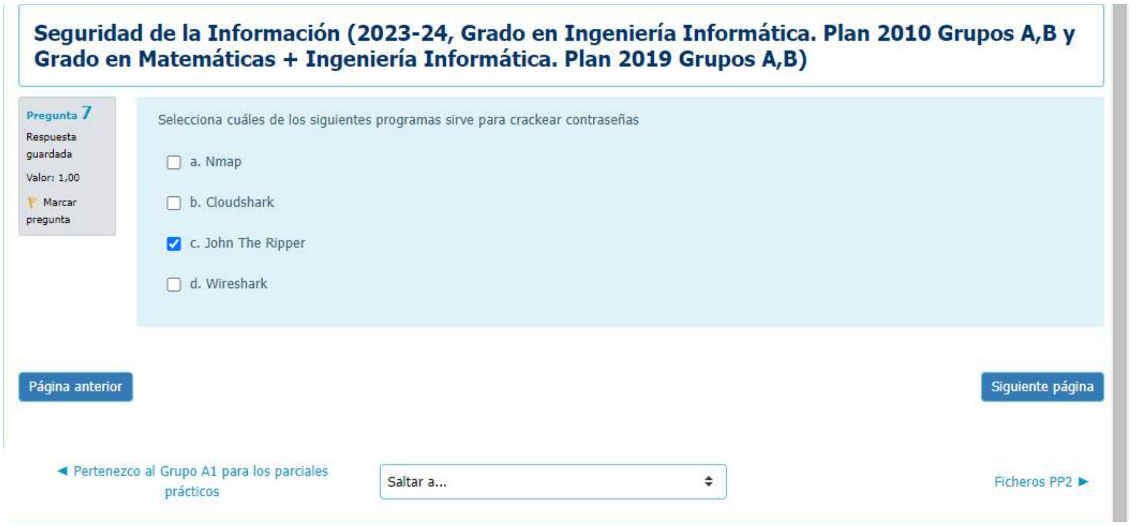


Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

Pregunta 6
Respuesta guardada
Valor: 1,00
Marcar pregunta

Une con una flechas el programa con su objetivo:

Crackeo de contraseñas	John The Ripper
Realizar ataques	Metasploit
Descubrimiento de servicios	Nmap
Análisis de tráfico	Wireshark



Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

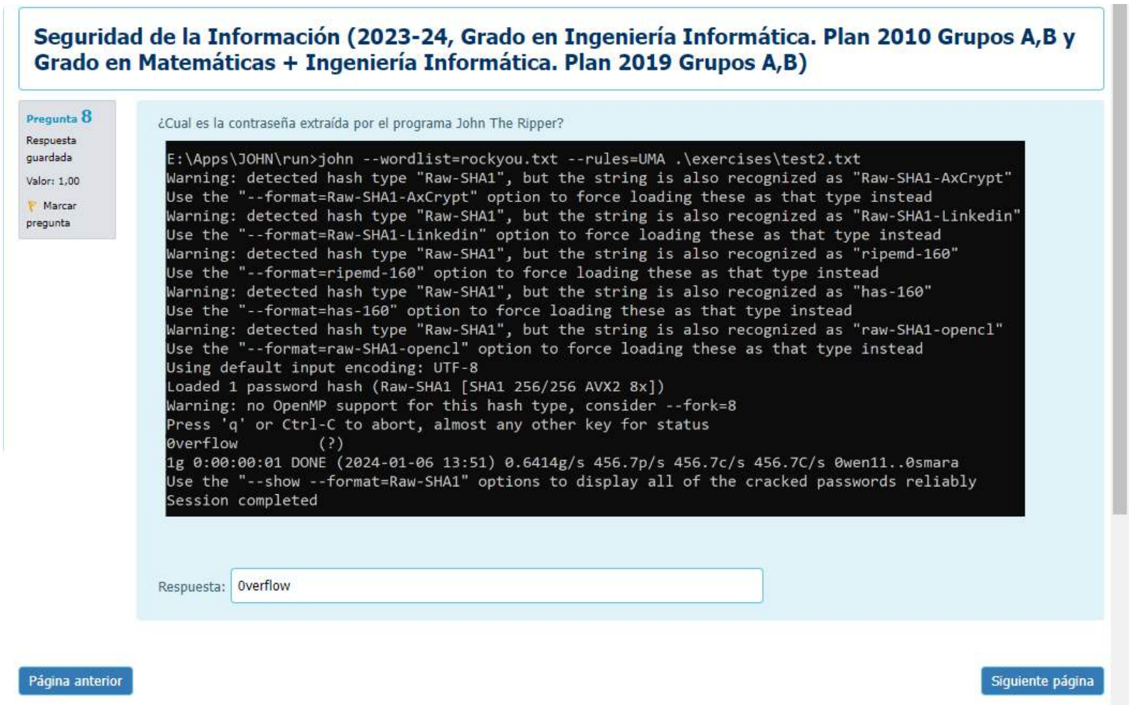
Selecciona cuáles de los siguientes programas sirve para crackear contraseñas

☐ a. Nmap

☐ b. Cloudshark

☑ c. John The Ripper

☐ d. Wireshark

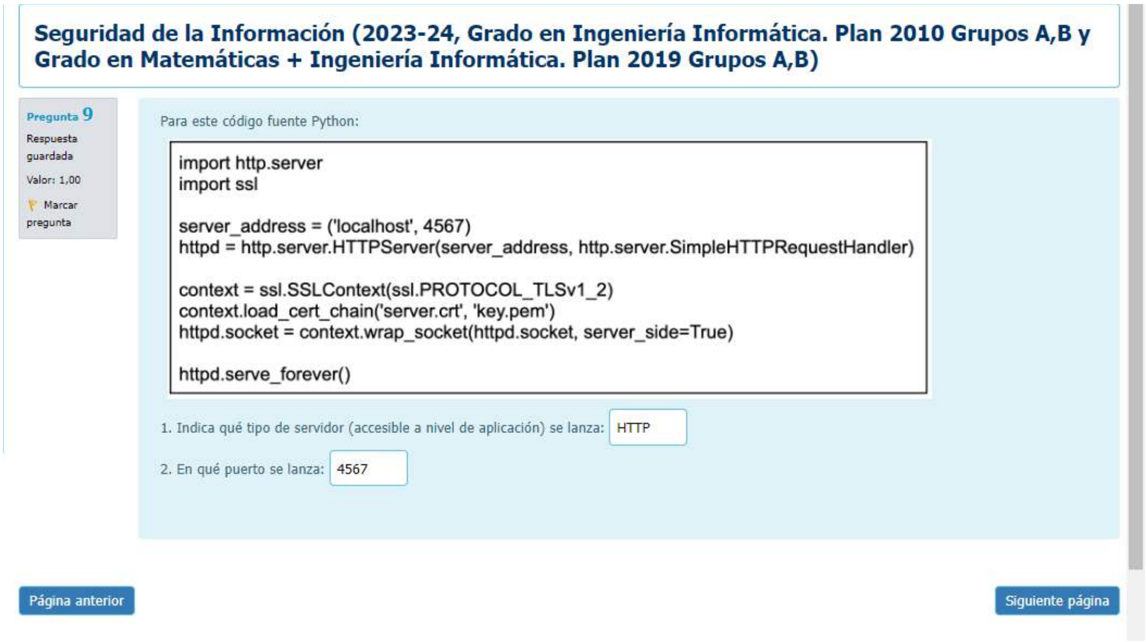


Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

¿Cual es la contraseña extraída por el programa John The Ripper?

```
E:\Apps\JOHN\run>john --wordlist=rockyou.txt --rules=UMA .\exercises\test2.txt
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-Linkedin"
Use the "--format=Raw-SHA1-Linkedin" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "has-160"
Use the "--format=has-160" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "raw-SHA1-opencl"
Use the "--format=raw-SHA1-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
0verflow         (?)
1g 0:00:00:01 DONE (2024-01-06 13:51) 0.6414g/s 456.7p/s 456.7c/s 456.7C/s 0wen11..0smara
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

Respuesta: 0verflow



Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

Pregunta 9

Respuesta guardada

Valor: 1,00

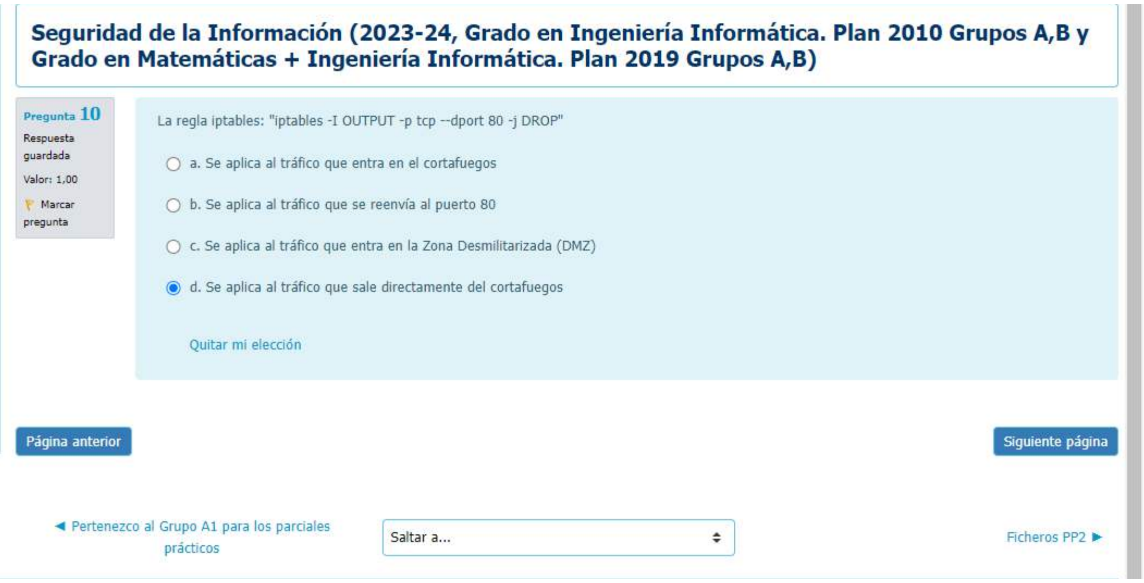
Marcar pregunta

Para este código fuente Python:

```
import http.server
import ssl

server_address = ('localhost', 4567)
httpd = http.server.HTTPServer(server_address, http.server.SimpleHTTPRequestHandler)

context = ssl.SSLContext(ssl.PROTOCOL_TLSv1_2)
context.load_cert_chain('server.crt', 'key.pem')
httpd.socket = context.wrap_socket(httpd.socket, server_side=True)

httpd.serve_forever()
```

1. Indica qué tipo de servidor (accesible a nivel de aplicación) se lanza: HTTP

2. En qué puerto se lanza: 4567



Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

Pregunta 10

Respuesta guardada

Valor: 1,00

Marcar pregunta

La regla iptables: "iptables -I OUTPUT -p tcp --dport 80 -j DROP"

○ a. Se aplica al tráfico que entra en el cortafuegos

○ b. Se aplica al tráfico que se reenvía al puerto 80

○ c. Se aplica al tráfico que entra en la Zona Desmilitarizada (DMZ)

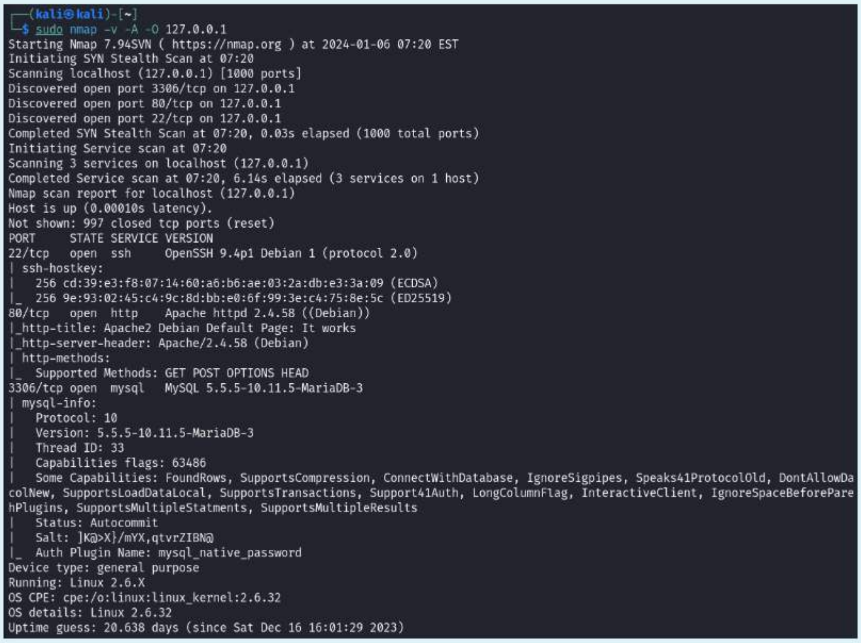
● d. Se aplica al tráfico que sale directamente del cortafuegos

Pregunta 11

Respuesta guardada

Valor: 2,00

Marcar pregunta



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -v -A -O 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-06 07:20 EST
Initiating SYN Stealth Scan at 07:20
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 22/tcp on 127.0.0.1
Completed SYN Stealth Scan at 07:20, 0.03s elapsed (1000 total ports)
Initiating Service scan at 07:20
Scanning 3 services on localhost (127.0.0.1)
Completed Service scan at 07:20, 6.14s elapsed (3 services on 1 host)
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00010s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.4p1 Debian 1 (protocol 2.0)
| ssh-hostkey:
|   256 cd:39:e3:f8:07:14:60:a6:b6:ae:03:2a:db:e3:3a:09 (ECDSA)
|_  256 9e:93:02:45:c4:9c:8d:bb:e0:6f:99:3e:c4:75:8e:5c (ED25519)
80/tcp   open  http    Apache httpd 2.4.58 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.58 (Debian)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
3306/tcp open  mysql   MySQL 5.5.5-10.11.5-MariaDB-3
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.11.5-MariaDB-3
|   Thread ID: 33
|   Capabilities flags: 63486
|   Some Capabilities: FoundRows, SupportsCompression, ConnectWithDatabase, IgnoreSigpipes, Speaks41ProtocolOld, DontAllowDa
colNew, SupportsLoadDataLocal, SupportsTransactions, Support41Auth, LongColumnFlag, InteractiveClient, IgnoreSpaceBeforePare
hPlugins, SupportsMultipleStatments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: ]K@>X}/mYX,qtvrZIBN@
|_  Auth Plugin Name: mysql_native_password
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Uptime guess: 20.638 days (since Sat Dec 16 16:01:29 2023)
```

Responde a las siguientes preguntas relacionadas con la salida del programa "nmap":

1) Indica la dirección IP del equipo analizado.

2) Indica la versión del servicio MySQL.

3) Indica qué servicios son accesibles en el servidor aparte de MySQL (no es necesario incluir sus versiones), y en qué puertos se encuentran.

4) ¿Cuánto tiempo ha tardado nmap en ejecutar el escaneo de puertos mediante la técnica de "SYN Stealth Scan"?

Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

Pregunta 12

Respuesta guardada

Valor: 2,00

Marcar pregunta

Utiliza el programa "Wireshark" para responder a las siguientes preguntas sobre la captura "telnet-raw.pcap":

1. Indica la dirección IP del cliente: 192.168.0.2

2. ¿Cuál es el nombre de usuario?: fake

3. ¿En qué nº de trama solicita el servidor la contraseña al cliente? 56

4. ¿Cuál es el segundo comando que ejecuta el cliente en el servidor? ls

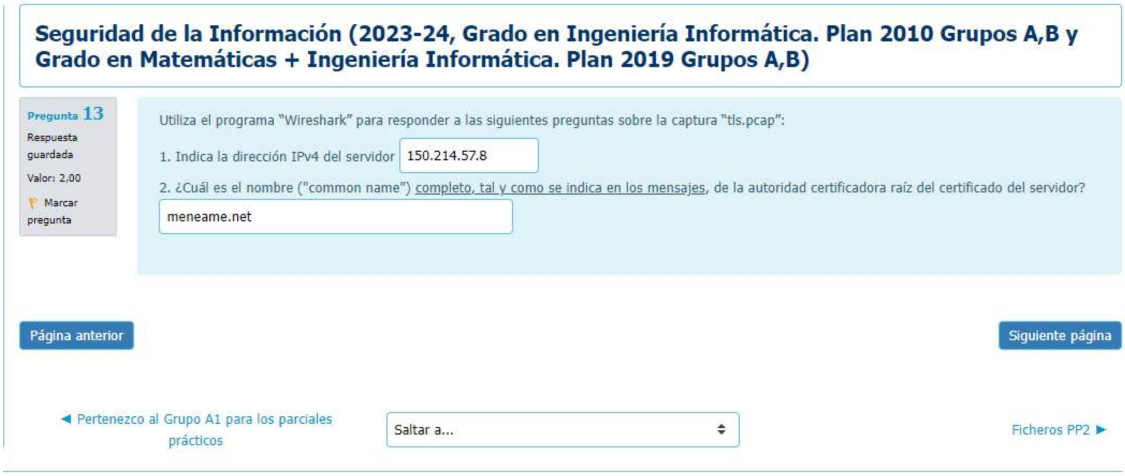
Página anterior

Siguiente página

◄ Pertenezco al Grupo A1 para los parciales prácticos

Saltar a... ⬍

Ficheros PP2 ►



Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

Pregunta 13

Respuesta guardada

Valor: 2,00

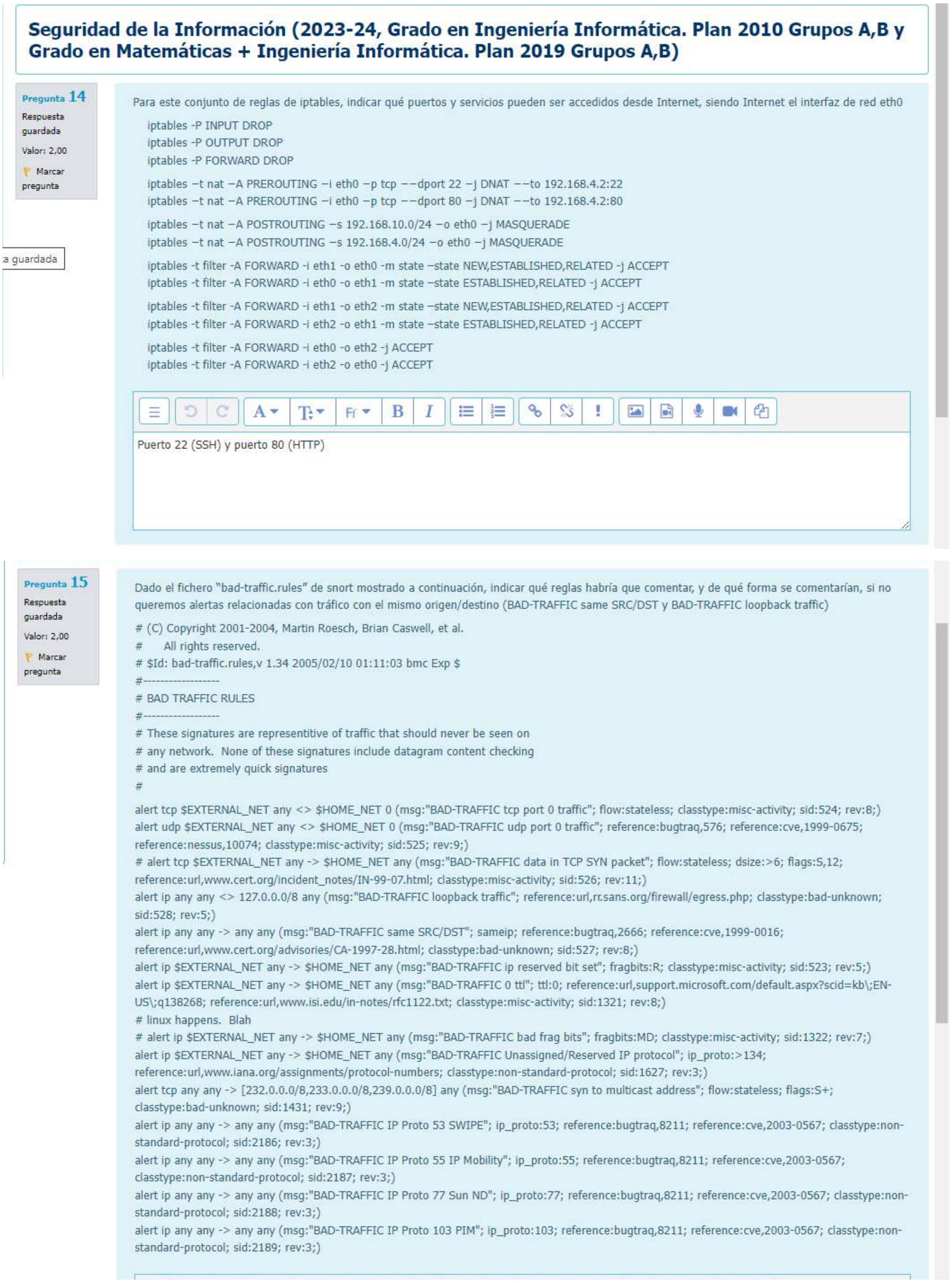
Marcar pregunta

Utiliza el programa "Wireshark" para responder a las siguientes preguntas sobre la captura "tls.pcap":

1. Indica la dirección IPv4 del servidor 150.214.57.8

2. ¿Cuál es el nombre ("common name") completo, tal y como se indica en los mensajes, de la autoridad certificadora raíz del certificado del servidor?

meneame.net



Seguridad de la Información (2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B)

Pregunta 14
Respuesta guardada
Valor: 2,00
Marcar pregunta

Para este conjunto de reglas de iptables, indicar qué puertos y servicios pueden ser accedidos desde Internet, siendo Internet el interfaz de red eth0

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

iptables –t nat –A PREROUTING –i eth0 –p tcp ––dport 22 –j DNAT ––to 192.168.4.2:22
iptables –t nat –A PREROUTING –i eth0 –p tcp ––dport 80 –j DNAT ––to 192.168.4.2:80

iptables –t nat –A POSTROUTING –s 192.168.10.0/24 –o eth0 –j MASQUERADE
iptables –t nat –A POSTROUTING –s 192.168.4.0/24 –o eth0 –j MASQUERADE

iptables -t filter -A FORWARD -i eth1 -o eth0 -m state –state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1 -m state –state ESTABLISHED,RELATED -j ACCEPT

iptables -t filter -A FORWARD -i eth1 -o eth2 -m state –state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -t filter -A FORWARD -i eth2 -o eth1 -m state –state ESTABLISHED,RELATED -j ACCEPT

iptables -t filter -A FORWARD -i eth0 -o eth2 -j ACCEPT
iptables -t filter -A FORWARD -i eth2 -o eth0 -j ACCEPT
```

Puerto 22 (SSH) y puerto 80 (HTTP)

Pregunta 15
Respuesta guardada
Valor: 2,00
Marcar pregunta

Dado el fichero "bad-traffic.rules" de snort mostrado a continuación, indicar qué reglas habría que comentar, y de qué forma se comentarían, si no queremos alertas relacionadas con tráfico con el mismo origen/destino (BAD-TRAFFIC same SRC/DST y BAD-TRAFFIC loopback traffic)

```
# (C) Copyright 2001-2004, Martin Roesch, Brian Caswell, et al.
#      All rights reserved.
# $Id: bad-traffic.rules,v 1.34 2005/02/10 01:11:03 bmc Exp $
#-----------------
# BAD TRAFFIC RULES
#-----------------
# These signatures are representitive of traffic that should never be seen on
# any network.  None of these signatures include datagram content checking
# and are extremely quick signatures
#
alert tcp $EXTERNAL_NET any <> $HOME_NET 0 (msg:"BAD-TRAFFIC tcp port 0 traffic"; flow:stateless; classtype:misc-activity; sid:524; rev:8;)
alert udp $EXTERNAL_NET any <> $HOME_NET 0 (msg:"BAD-TRAFFIC udp port 0 traffic"; reference:bugtraq,576; reference:cve,1999-0675; reference:nessus,10074; classtype:misc-activity; sid:525; rev:9;)
# alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"BAD-TRAFFIC data in TCP SYN packet"; flow:stateless; dsize:>6; flags:S,12; reference:url,www.cert.org/incident_notes/IN-99-07.html; classtype:misc-activity; sid:526; rev:11;)
alert ip any any <> 127.0.0.0/8 any (msg:"BAD-TRAFFIC loopback traffic"; reference:url,rr.sans.org/firewall/egress.php; classtype:bad-unknown; sid:528; rev:5;)
alert ip any any -> any any (msg:"BAD-TRAFFIC same SRC/DST"; sameip; reference:bugtraq,2666; reference:cve,1999-0016; reference:url,www.cert.org/advisories/CA-1997-28.html; classtype:bad-unknown; sid:527; rev:8;)
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"BAD-TRAFFIC ip reserved bit set"; fragbits:R; classtype:misc-activity; sid:523; rev:5;)
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"BAD-TRAFFIC 0 ttl"; ttl:0; reference:url,support.microsoft.com/default.aspx?scid=kb\;EN-US\;q138268; reference:url,www.isi.edu/in-notes/rfc1122.txt; classtype:misc-activity; sid:1321; rev:8;)
# linux happens.  Blah
# alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"BAD-TRAFFIC bad frag bits"; fragbits:MD; classtype:misc-activity; sid:1322; rev:7;)
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"BAD-TRAFFIC Unassigned/Reserved IP protocol"; ip_proto:>134; reference:url,www.iana.org/assignments/protocol-numbers; classtype:non-standard-protocol; sid:1627; rev:3;)
alert tcp any any -> [232.0.0.0/8,233.0.0.0/8,239.0.0.0/8] any (msg:"BAD-TRAFFIC syn to multicast address"; flow:stateless; flags:S+; classtype:bad-unknown; sid:1431; rev:9;)
alert ip any any -> any any (msg:"BAD-TRAFFIC IP Proto 53 SWIPE"; ip_proto:53; reference:bugtraq,8211; reference:cve,2003-0567; classtype:non-standard-protocol; sid:2186; rev:3;)
alert ip any any -> any any (msg:"BAD-TRAFFIC IP Proto 55 IP Mobility"; ip_proto:55; reference:bugtraq,8211; reference:cve,2003-0567; classtype:non-standard-protocol; sid:2187; rev:3;)
alert ip any any -> any any (msg:"BAD-TRAFFIC IP Proto 77 Sun ND"; ip_proto:77; reference:bugtraq,8211; reference:cve,2003-0567; classtype:non-standard-protocol; sid:2188; rev:3;)
alert ip any any -> any any (msg:"BAD-TRAFFIC IP Proto 103 PIM"; ip_proto:103; reference:bugtraq,8211; reference:cve,2003-0567; classtype:non-standard-protocol; sid:2189; rev:3;)
```