POSIBLES PREGUNTAS TEST 2 PRÁCTICAS.

1. **¿Que permisos necesita un ca en su certificado?**
   -Firmar otros certificados
   -Emitir CRLs(Listas de certificados revocados)[gesionar y publicar]
   -extensiones críticas de CA (CA:true)
2. **¿Que permisos necesita un usuario?**
   -Autenticación
   -Cifrado
   -Firma digital
3. **¿Para qué sirve el campo X509X3 Key Usage?**
   Indica el uso que se puede hacer del certificado.
4. **CRL, cómo sabemos cuántos certificados se han revocado:**
   Certificate Revocation List (CRL):
   Version 2 (0x1)
   Signature Algorithm: sha256WithRSAEncryption
   Issuer: CN = Example CA
   Last Update: Dec 11 12:00:00 2024 GMT
   Next Update: Dec 18 12:00:00 2024 GMT
   Revoked Certificates:
   Serial Number: 01
   Revocation Date: Dec 01 12:00:00 2024 GMT
   Serial Number: 02
   Revocation Date: Dec 05 12:00:00 2024 GMT
   Serial Number: 03
   Revocation Date: Dec 07 12:00:00 2024 GMT
   3 certificados revocados.

5. **A la hora de crear un certificado qué apartado no es obligatorio?:**
   a.periodo de utilidad
   b.país de origen <-
   c.clave privada
   d.nombre
6. **Al exportar a pormato PKCS#12 porqué se pone una contraseña?**
   El formato incluye tanto la clave privada como el certificado empaquetado en un archivo, la contraseña se utiliza para proteger la clave privada (sólo las personas autorizadas pueden importar el archivo).

7. **Al exportar en formato CTR porqué no se pone una contraseña?**
   El formato CRT sólo incluye el certificado público, que no es sensible. No incluye la clave privada luego no hay necesidad de protegerlo con una contraseña.

8. **¿Qué usos de clave debe tener un certificado de CA?**
   -Certificate Sign
   -CRL sign

9. **Qué usos de clave NO debe tener un certificado de usuario?**
   -Certificate Sign
   -CRL sign

10. **¿Sería correcto exportar un certificado de firma (es decir, que contenga la clave privada y se utilice para firmar documentos) en formato PKCS#12?**
    Sí, **sería correcto exportar un certificado de firma en formato PKCS#12**, siempre y cuando incluya tanto la **clave privada** como el **certificado de la firma** y cualquier **cadena de certificados intermedios** necesarios para la validación del mismo.

Une con flechas el programa con su objetivo:

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

John the Ripper: Herramienta de prueba de fuerza bruta para crackeo de contraseñas, capaz de descifrar contraseñas débiles o robadas.
Metasploit: Framework para realizar ataques de seguridad, incluyendo exploits y payloads para vulnerabilidades conocidas en sistemas y aplicaciones.
Nmap: Herramienta para el descubrimiento de servicios y escaneo de redes, útil para identificar dispositivos y servicios activos en una red.
Wireshark: Herramienta de análisis de tráfico de red, que permite capturar y analizar paquetes para investigar problemas de seguridad o rendimiento.

11. **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()
```

tipo de servidor: HTTP
puerto: 4567

12. **Captura de nmap con preguntas de que es qué.**

13. **La regla iptables: ¨ıptables -I OUTPUT -p tcp –dport 80 -j DROP”**
    Se aplica al tráfico que sale directamente del cortafuegos

    `iptables`: Es la herramienta de filtrado de paquetes que se utiliza en sistemas Linux para gestionar las tablas de filtrado del tráfico de red. Las reglas de `iptables` se utilizan para bloquear o permitir el tráfico según diversas condiciones.

    `-I OUTPUT`: El `-I` (o `--insert`) indica que la regla debe ser insertada en la cadena especificada. Si no se proporciona un número de línea específico, la regla se inserta al principio de la cadena.**`OUTPUT`** es la cadena de salida (output chain). Esto significa que la regla afecta al tráfico de salida desde el sistema local hacia otros hosts en la red.

    `-p tcp`: Este es el parámetro que especifica el **protocolo** del tráfico. En este caso, se está indicando que la regla se aplica solo al tráfico de tipo **TCP**.

    `--dport 80`: **`--dport`** es un parámetro que indica que la regla debe aplicar a los paquetes cuyo destino sea un puerto específico. **`80`** es el puerto de destino. El puerto 80 es el puerto estándar para el **HTTP**, es decir, tráfico web sin cifrar.

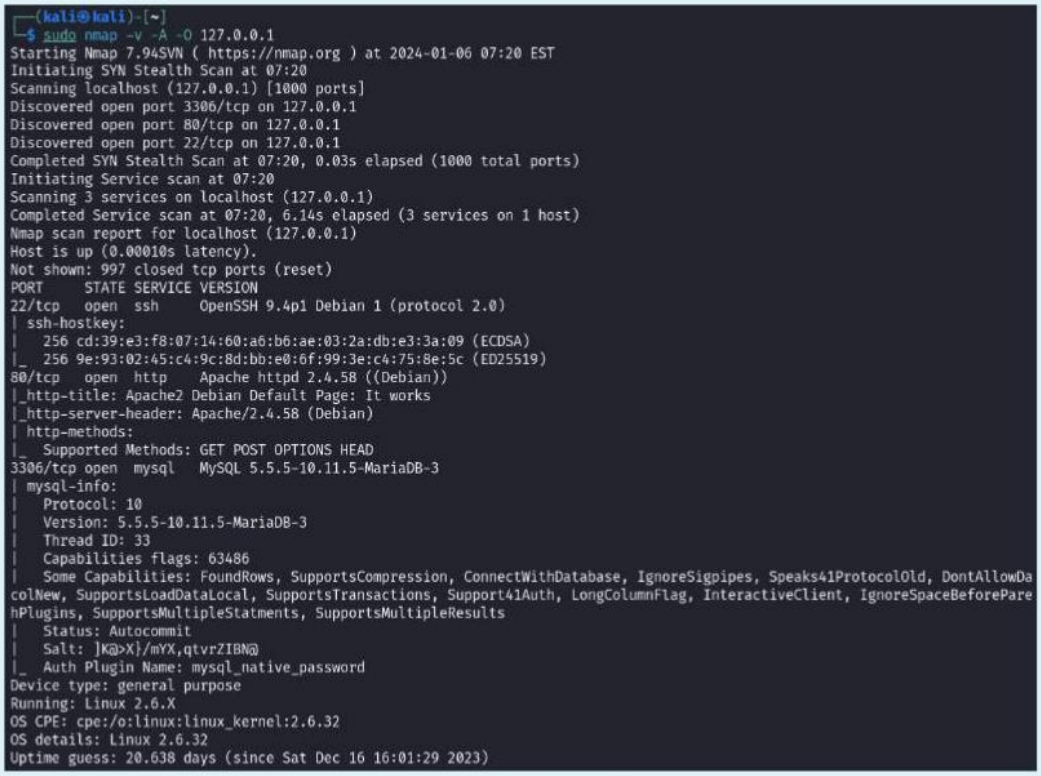
    `-j DROP`: **`-j`** es el parámetro que indica la **acción** a tomar cuando un paquete coincide con la regla. **`DROP`** es la acción que indica que el paquete debe ser **rechazado** sin enviar ninguna respuesta al emisor (es decir, el tráfico será bloqueado).

14. **La regla iptables: iptables -I INPUT -p tcp --dport 80 -j DROP**
    regla para tráfico entrante (puerto 80, HTTP)

15. **La regla iptables: iptables -I FORWARD -p tcp --dport 80 -j DROP**
    Se aplica al tráfico que se reenvía al puerto 80

16. **La regla iptables: iptables -I INPUT -i eth1 -p tcp --dport 80 -j DROP**
    Se aplica al tráfico que entra en la Zona Desmilitarizada (DMZ)

17. **Indica:**



```
┌──(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"?

1) 127.0.0.1

2) 5.5.5-10.11.5-MariaDB-3

3) ssh con puerto 22/tcp , http con puerto 80/tcp

4) Completed SYN Stealth Scan at blablablá -> 0.03 segundos