SSLscan

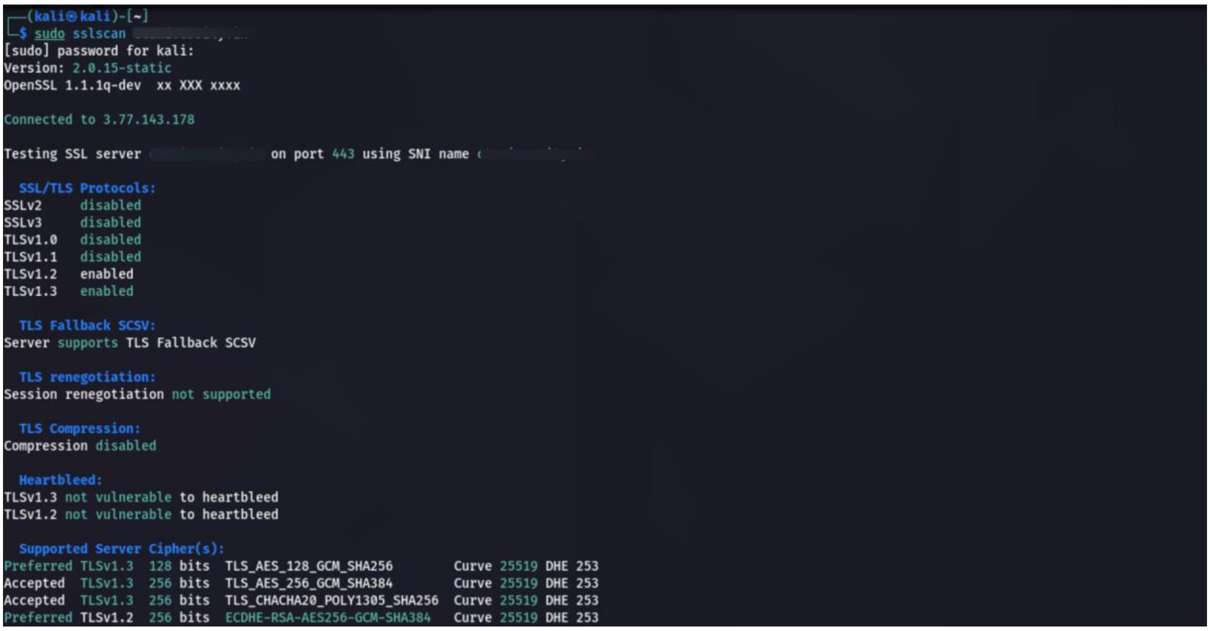
sslscan is a command-line tool used to check the SSL/TLS configuration of a server. It helps in identifying the supported ciphers, protocols, and other SSL/TLS settings of a server, which is useful for ensuring the security and compliance of web services.

Features

1. **Protocol Support**: sslscan tests for support across various SSL/TLS protocol versions, including SSLv2, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3.
2. **Cipher Suite Testing**: It identifies which cipher suites are supported by the server and whether they are considered secure or deprecated.
3. **Certificate Details**: The tool retrieves and displays details about the server's SSL certificate, such as the issuer, validity period, and subject information.
4. **Renegotiation Support**: sslscan checks if the server supports secure renegotiation, a critical feature to prevent certain types of attacks.
5. **Fallback Scsv**: It tests for support of the TLS Fallback Signaling Cipher Suite Value (SCSV), which helps in mitigating protocol downgrade attacks.
6. **Key Exchange Groups**: The tool identifies the key exchange groups supported by the server, which is essential for ensuring the strength of the encryption.

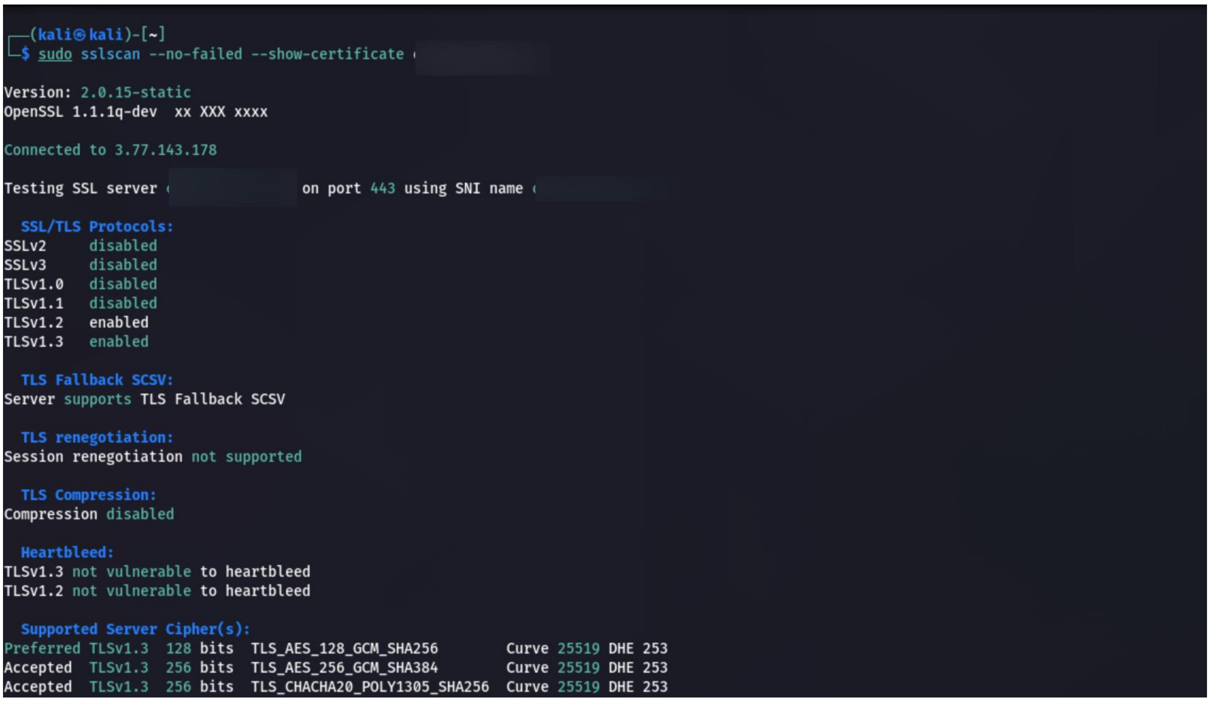
Example: -

1. The basic usage of sslscan involves running the tool against a specified host and port. By default, it checks port 443, which is the default port for HTTPS.



```
┌──(kali㉿kali)-[~]
└─$ sudo sslscan [redacted]
[sudo] password for kali:
Version: 2.0.15-static
OpenSSL 1.1.1q-dev  xx XXX xxxx

Connected to 3.77.143.178

Testing SSL server [redacted] on port 443 using SNI name [redacted]

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.3  128 bits  TLS_AES_128_GCM_SHA256        Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_AES_256_GCM_SHA384        Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_CHACHA20_POLY1305_SHA256  Curve 25519 DHE 253
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve 25519 DHE 253
```

2. This command will only show the ciphers supported by the server (--no-failed) and will display the server's certificate details (--show-certificate).



```
┌──(kali㉿kali)-[~]
└─$ sudo sslscan --no-failed --show-certificate [redacted]

Version: 2.0.15-static
OpenSSL 1.1.1q-dev  xx XXX xxxx

Connected to 3.77.143.178

Testing SSL server [redacted] on port 443 using SNI name [redacted]

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     disabled
TLSv1.0   disabled
TLSv1.1   disabled
TLSv1.2   enabled
TLSv1.3   enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.3  128 bits  TLS_AES_128_GCM_SHA256        Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_AES_256_GCM_SHA384        Curve 25519 DHE 253
Accepted  TLSv1.3  256 bits  TLS_CHACHA20_POLY1305_SHA256  Curve 25519 DHE 253
```