Day 11

Exploitation Analyst

Hacking the SSL Network protocol:

Weak Cipher Suites:

What are Cipher Suites?

A cipher suite is a set of algorithms that define how secure communication happens over SSL/TLS. It includes:

- Key exchange algorithm (e.g., RSA, ECDHE): for securely exchanging encryption keys
- Authentication algorithm (e.g., RSA, ECDSA): to verify server identity
- Symmetric encryption algorithm (e.g., AES, ChaCha20): to encrypt the actual data
- MAC algorithm (e.g., SHA256): to ensure message integrity

How cipher suites are related to SSL?

When a client (like a browser) connects to a server over SSL/TLS, both sides agree on a cipher suite during the handshake. This determines how data will be encrypted and decrypted during the session.

Example:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

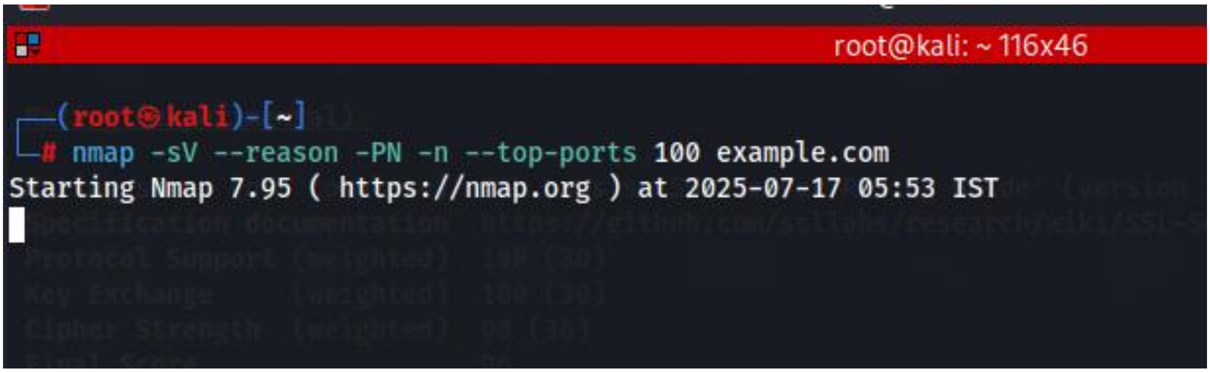
Breakdown:

- ECDHE: key exchange
- RSA: authentication
- AES_256_GCM: encryption
- SHA384: message integrity

Testing Cipher Strength:

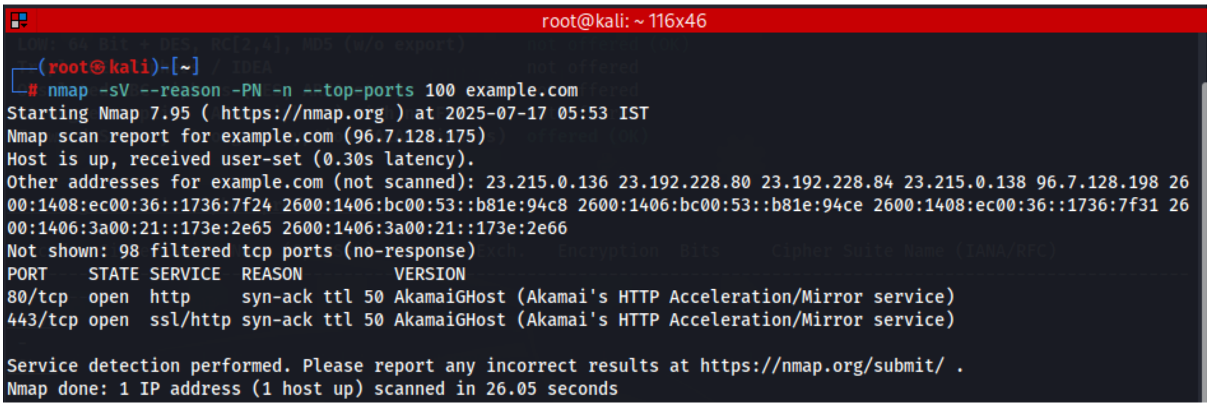
Steps:

First find out which services are running and using the SSL encryption?



```
┌──(root㉿kali)-[~]
└─# nmap -sV --reason -PN -n --top-ports 100 example.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 05:53 IST
```

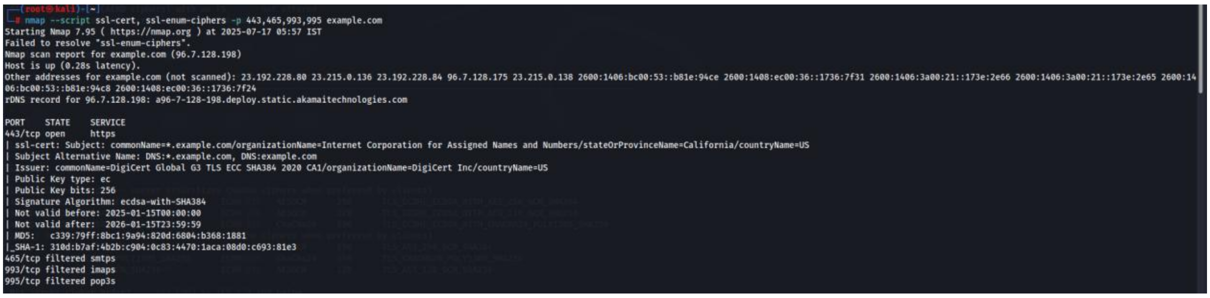
We get the following result:



```
┌──(root㉿kali)-[~]
└─# nmap -sV --reason -PN -n --top-ports 100 example.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 05:53 IST
Nmap scan report for example.com (96.7.128.175)
Host is up, received user-set (0.30s latency).
Other addresses for example.com (not scanned): 23.215.0.136 23.192.228.80 23.192.228.84 23.215.0.138 96.7.128.198 26
00:1408:ec00:36::1736:7f24 2600:1406:bc00:53::b81e:94c8 2600:1406:bc00:53::b81e:94ce 2600:1408:ec00:36::1736:7f31 26
00:1406:3a00:21::173e:2e65 2600:1406:3a00:21::173e:2e66
Not shown: 98 filtered tcp ports (no-response)
PORT    STATE SERVICE  REASON         VERSION
80/tcp  open  http     syn-ack ttl 50 AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
443/tcp open  ssl/http syn-ack ttl 50 AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.05 seconds
```

To enumerate the ports:



```
┌──(root㉿kali)-[~]
└─# nmap --script ssl-cert, ssl-enum-ciphers -p 443,465,993,995 example.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 05:57 IST
Failed to resolve "ssl-enum-ciphers".
Nmap scan report for example.com (96.7.128.198)
Host is up (0.28s latency).
Other addresses for example.com (not scanned): 23.192.228.80 23.215.0.136 23.192.228.84 96.7.128.175 23.215.0.138 2600:1406:bc00:53::b81e:94ce 2600:1408:ec00:36::1736:7f31 2600:1406:3a00:21::173e:2e66 2600:1406:3a00:21::173e:2e65 2600:14
06:bc00:53::b81e:94c8 2600:1408:ec00:36::1736:7f24
rDNS record for 96.7.128.198: a96-7-128-198.deploy.static.akamaitechnologies.com

PORT    STATE    SERVICE
443/tcp open     https
| ssl-cert: Subject: commonName=*.example.com/organizationName=Internet Corporation for Assigned Names and Numbers/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:*.example.com, DNS:example.com
| Issuer: commonName=DigiCert Global G3 TLS ECC SHA384 2020 CA1/organizationName=DigiCert Inc/countryName=US
| Public Key type: ec
| Public Key bits: 256
| Signature Algorithm: ecdsa-with-SHA384
| Not valid before: 2025-01-15T00:00:00
| Not valid after:  2026-01-15T23:59:59
| MD5:   c339:79ff:8bc1:9a94:820d:6804:b368:1881
|_SHA-1: 310d:b7af:4b2b:c904:0c83:4470:1aca:08d0:c693:81e3
465/tcp filtered smtps
993/tcp filtered imaps
995/tcp filtered pop3s
```

How to Protect

- Disable weak ciphers in server config.
- Disable SSLv2/SSLv3, TLS 1.0, TLS 1.1.
- Use strong TLS 1.2+ with modern ciphers (AES-GCM, ChaCha20, etc.).
- Regularly scan using tools like:
  - testssl.sh
  - sslyze
  - SSL Labs (Qualys)

--The End--