**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

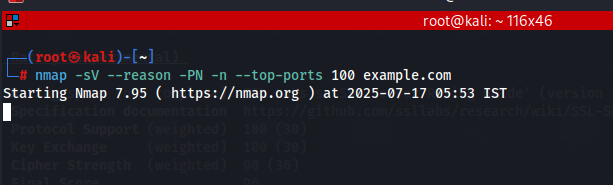
Breakdown:

* ECDHE: key exchange
* RSA: authentication
* AES\_256\_GCM: encryption
* SHA384: message integrity

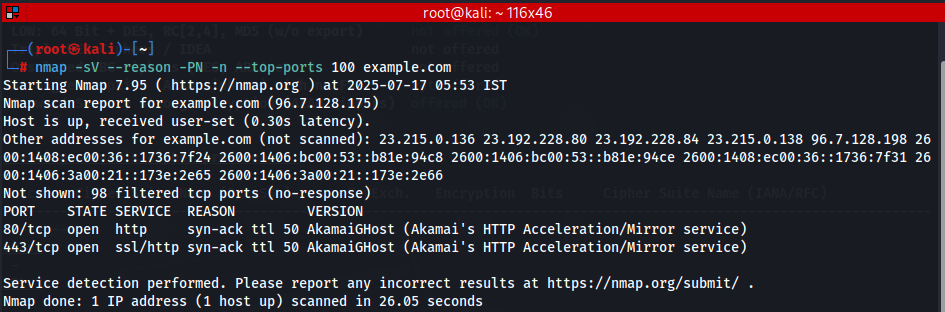
**Testing Cipher Strength:**

Steps:

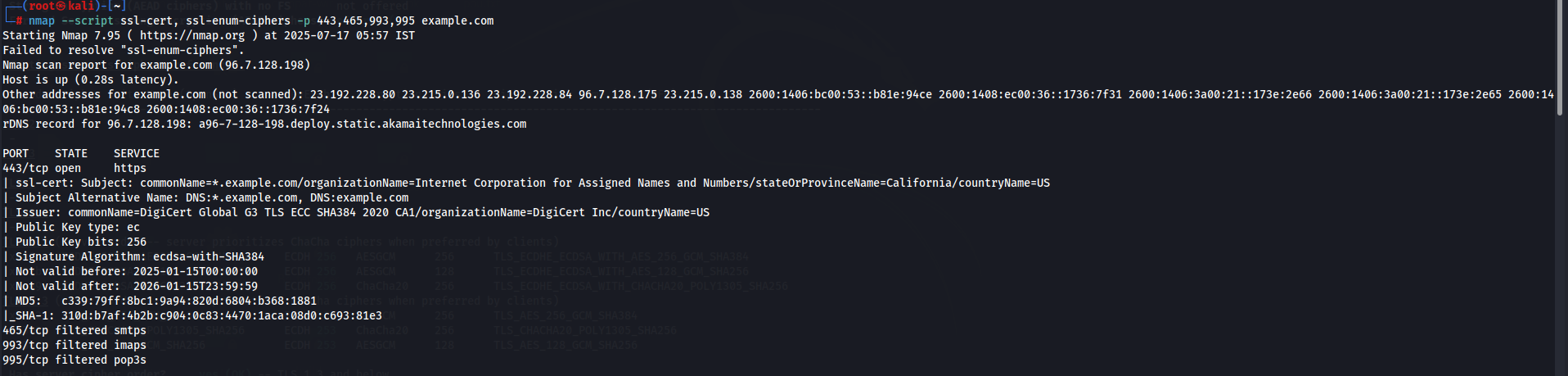
First find out which services are running and using the SSL encryption?



We get the following result:



To enumerate the ports:



**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--