Laboratory_13: SSL/TLS Security Assessment using sslscan

This laboratory covers the usage of sslscan tool for assessing SSL/TLS configuration and identifying potential security vulnerabilities.

Installation

- sudo apt update
- sslscan
  - https://github.com/rbsec/sslscan
  - chmod +x sslscan
  - mv sslscan /usr/local/bin/
- openssl
  - openssl version -d
  - set req section
    - # In the [req] section or create a new section
    - [req]
    - default_bits = 512

Part 1: Basic SSL/TLS Scanning

Scanning a Local Server

1. First, create a test server with weak SSL/TLS configuration:

   ```
   mkdir -p ~/sslscan-lab
   cd ~/sslscan-lab
   ```

2. Generate a private key

```
openssl genrsa -out server.key 512
```

3. Generate a CSR:

```
openssl req -new -key server.key -out server.csr -subj
"/C=US/ST=State/L=City/O=Organization/CN=example.com" -config
/usr/lib/ssl/openssl.cnf
```

4. Generate certificate

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

5. Start the test server:

```
sudo openssl s_server -cert server.crt -key server.key -port 4433 –cipher
'ALL:NULL:@SECLEVEL=0' &
```

6. Scan the local server:

```
sslscan localhost:4433
```

   - Small key size (512-bit)
   - Weak ciphers accepted
   - NULL ciphers accepted
   - Possibly weak protocol versions supported

Part 2: Advanced Scanning Options

Protocol Version Testing

1. Test only SSLv3 (if supported):

```
sslscan --ssl3 localhost:4433
```

2. Test TLS versions:

```
sslscan --tls10 localhost:4433
sslscan --tls11 localhost:4433
sslscan --tls12 localhost:4433
```

Cipher Suite Analysis

1. Show cipher details:

```
sslscan --show-ciphers localhost:4433
```

2. Test specific cipher suites:

```
sslscan --cipher=AES256-SHA localhost:4433
```

Certificate Analysis

1. Show certificate details:

```
sslscan --show-certificate --no-ciphersuites github.com
```

2. Test certificate chain:

```
sslscan --show-certificate --show-times github.com
```

No CA detected

1. Review s_client:
   a. openssl s_client -connect localhost:4433

Cleanup

```
sudo pkill openssl
cd ~
rm -rf ~/sslscan-lab
```