Suites de cifrado TLS/SSL (Parte II)

Por mikiminoru el 15 sept 2020 con 0 comentarios

Good meowrning! Dado que en el anterior post estuvimos comentando en qué consistía cada sección de una suite de cifrado, en este vamos a listar un conjunto de herramientas que nos ayudan a comprobar las suites de cifrado que acepta un servidor SSL/TLS, y si dicha configuración contiene vulnerabilidades asociadas.

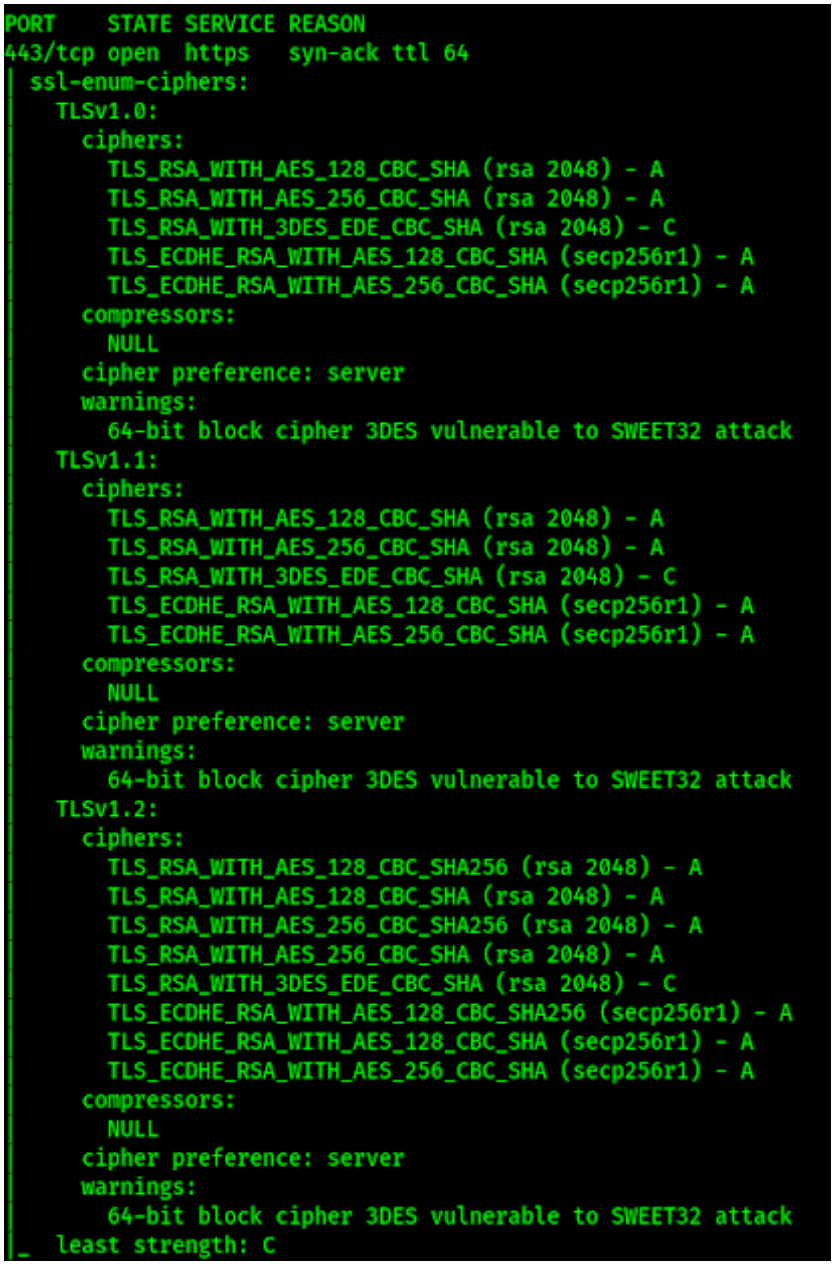
- Con herramientas online como:

- SSL Labs
- crt.sh
- Toolbox
- Cipherli.st

- Con herramientas a importar en nuestra máquina Kali/Parrot/Arch, tenemos las siguientes, que nos permiten solicitar un mayor nivel de detalle de las vulnerabilidades obtenidas.

- Burp Suite SSL Scanner.
- Nmap

```
root@miau# nmap --script=ssl-enum-ciphers -p 443 target
```



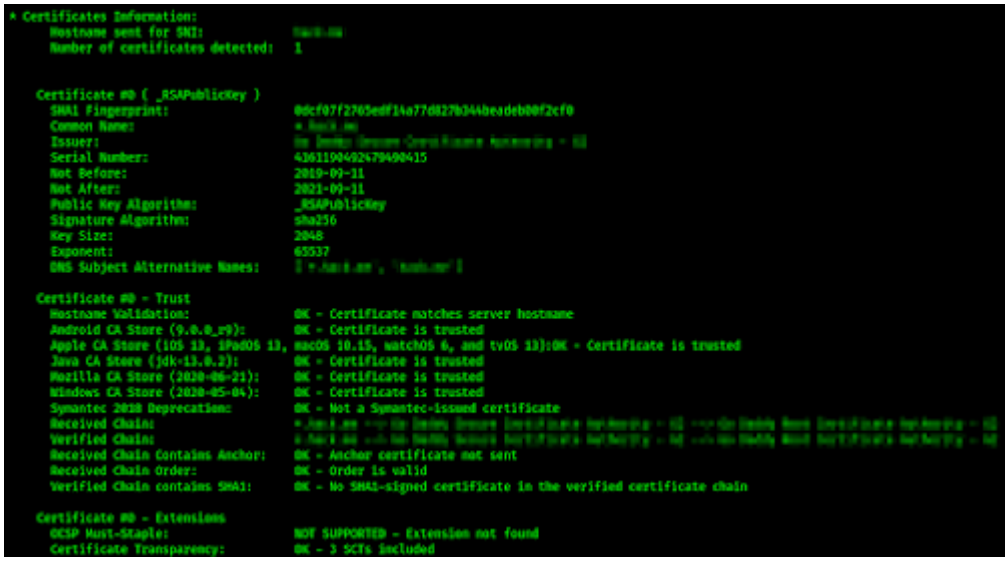
- sslscan

```
root@miau# sslscan target -p 443
```

```
  Supported Server Cipher(s):
Preferred TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  112 bits  DES-CBC3-SHA
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Preferred TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  256 bits  AES256-SHA
Accepted  TLSv1.1  112 bits  DES-CBC3-SHA
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Preferred TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
```

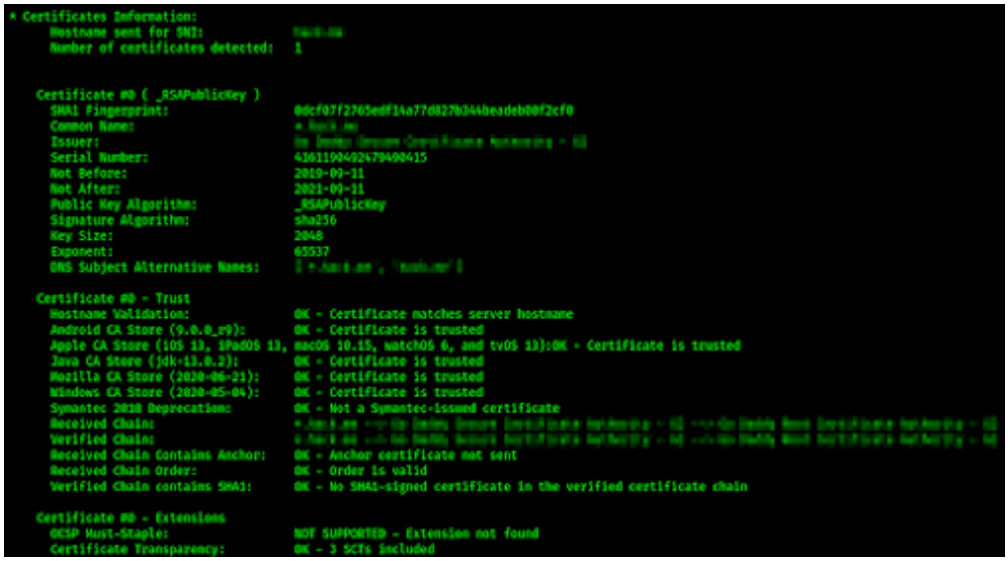
- testssl

```
root@miau# testssl target
```



- sslyze

```
root@miau# sslyze --regular target
```



En la última parte de este hilo hablaremos de las vulnerabilidades que obtenemos ante configuraciones incorrectas :)

Muchos maullidos!

M

SSL , TLS

Otros artículos relacionados

TLS1.3: ¿Qué hay de nuevo? (Parte I)

30 DE OCTUBRE DE 2020

Suites de TLS/SSL (Parte III)

21 DE SEPTIEMBRE DE 2020