

Verificar versiones y ciphers soportados de TLS, SSL

Introducción

Una de los mayores problemas al que se enfrenta el soporte es lidiar con los clientes y los problemas derivados del uso de sistemas (windows, MacOSX, ios, Android, ...) obsoletos.

Verificar TLS soportado por un protocolo

```
h=nombre_del_host
p=port
## Tls 1.2
openssl s_client -connect $h:$p -tls1_2
### Tls 1.1
openssl s_client -connect $h:$p -tls1_1
### Tls 1
openssl s_client -connect $h:$p -tls1
```

El retorno debe tener una linea como esta

```
Verification: OK
```

Enumerar los ciphers ssl

```
h=nombre_del_host
p=port
nmap --script ssl-enum-ciphers -p $p $h
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-15 17:43 CEST
Nmap scan report for kvm468.ceinor.com (5.135.93.99)
Host is up (0.056s latency).
```

```
PORT      STATE SERVICE
```

```
465/tcp open  smtps
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|     compressors:
|       NULL
|     cipher preference: client
|_  least strength: A
```

Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds

Links y agradecimientos

- [Command prompt to check TLS version requiere by a host](#)
- [Checking ssl tls Version Support of a Remnote Host from Command line](#)

Revision #2

Created 15 May 2021 17:32:54 by Abkrim

Updated 22 June 2021 11:57:00 by Abkrim