

nmap??https????????

命令 nmap 主机 www.xxxxxxx.com 扫描 SSL/TLS 支持的 ciphers

```
nmap -sV -p 443 --script ssl-enum-ciphers www.xxxxxxx.com
```

输出结果

? ?????? ?????????????????

项目	结果
支持的 HTTPS	端口 443
支持的协议	△ "Lego Server" /
TLS 版本	支持 TLSv1.0 和 TLSv1.1
支持的加密套件	支持 3DES 和 IDEA
支持的密钥交换	支持 SWEET32 和

“ 支持的加密套件 3DES 和 IDEA ”

? ??????

1. ?????

```
SERVICE: Lego Server
_http-server-header_: Lego Server
```

- “Lego Server” 支持的 Web 服务器 Nginx Apache IIS
-

2. TLS ?????

TLSv1.0:

TLSv1.1:

- **TLS 1.0** **TLS 1.1**

- **2020**
- POODLE BEAST CRIME
- Chrome Firefox iOS Safari

“ TLS 1.0 TLS 1.1 TLS 1.2

3. Ciphers?

?

TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C

TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A

- **3DES** **Triple DES**

- “ ” **SWEET32**
- SWEET32 2^{32}

- **IDEA**

-

“ **Nmap**

warnings:

64-bit block cipher 3DES vulnerable to SWEET32 attack

64-bit block cipher IDEA vulnerable to SWEET32 attack

“

??

- **RSA** **ECDHE**

- ☐ ☐ **Forward Secrecy**
- ☐
- ☐ **CBC** ☐ ☐ AES_CBC ☐ 3DES_CBC ☐
 - ☐ GCM ☐ oracle ☐ BEAST ☐ POODLE ☐
 - ☐

4. Compressors?

compressors: NULL

- ☐ ☐ → ☐ CRIME/BREACH ☐
- ☐

5. Cipher Preference

cipher preference: server

- ☐
- ☐ ☐ ☐

SSL Labs

Item	Item	Item
TLS	TLS 1.0 / 1.1	TLS 1.2+ 1.3
	☐ 3DES ☐ IDEA ☐ CBC	☐ AEAD ☐ GCM/ChaCha20
	☐	☐
	☐ 3DES, IDEA	☐
	△ F / D	☐ A+

“ ☐ [SSL Labs Test](#) ☐

F ☐ **D** ☐

PCI-DSS ☐ GDPR

? ????????????

? 1. ?? TLS ??

```
ssl_protocols TLSv1.2 TLSv1.3;
```

“ TLS 1.0 1.1

? 2. ??????????

```
ssl_ciphers 'ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256';
```

“

- ECDHE
- AES-GCM ChaCha20-Poly1305
- SHA256/SHA384

? 3. ??????

```
ssl_ciphers '...'; #  
ssl_prefer_server_ciphers on;
```

? 4. ?? HSTS ? HTTP/2

```
add_header Strict-Transport-Security "max-age=63072000; includeSubDomains; preload" always;
```

? 5. ??????????????

- “Lego Server”
 -
-

? ??????????

■■■■■■■■■■

```
nmap -sV -p 443 --script ssl-enum-ciphers www.xxxxxxxxxx.com
```

■■■■■

- ■■■■ 3DES, IDEA
- ■ TLS 1.0/1.1
- ■ ECDHE + GCM ■ ChaCha20

■■■■

■ <https://www.ssllabs.com/ssltest/>

■■■■■■■■■■■■

? ??

■	■■■■	■
TLS ■	■ ■■■■ TLS 1.0/1.1■	■ ■■■■
■■■■	■ ■ 3DES■ IDEA■■■	■ ■■■■
■■■■	■ ■■	■ ■■■■ ECDHE
■■■	■ ■■■■ SWEET32 ■■■■	△ ■■■■
■■■■■	△ “Lego Server” ■■	■ ■■■■



■■■■■■■■■■■ Nginx ■■■■■■ TLS 1.3■ HSTS■ OCSP Stapling
■■■■■■■■■■■■■■■■■■■■ Let's Encrypt■■■■ HTTP/2■