



Sri Lanka Institute of Information Technology

## Vulnerability Assessment – Web Audit

<https://www.tiktok.com>

**Individual Assignment**  
**IE2062 – Web Security**

Submitted by:

Student Registration Number	Student Name
<b>IT19013756</b>	<b>M. H. D. V. JAYASINGHE</b>

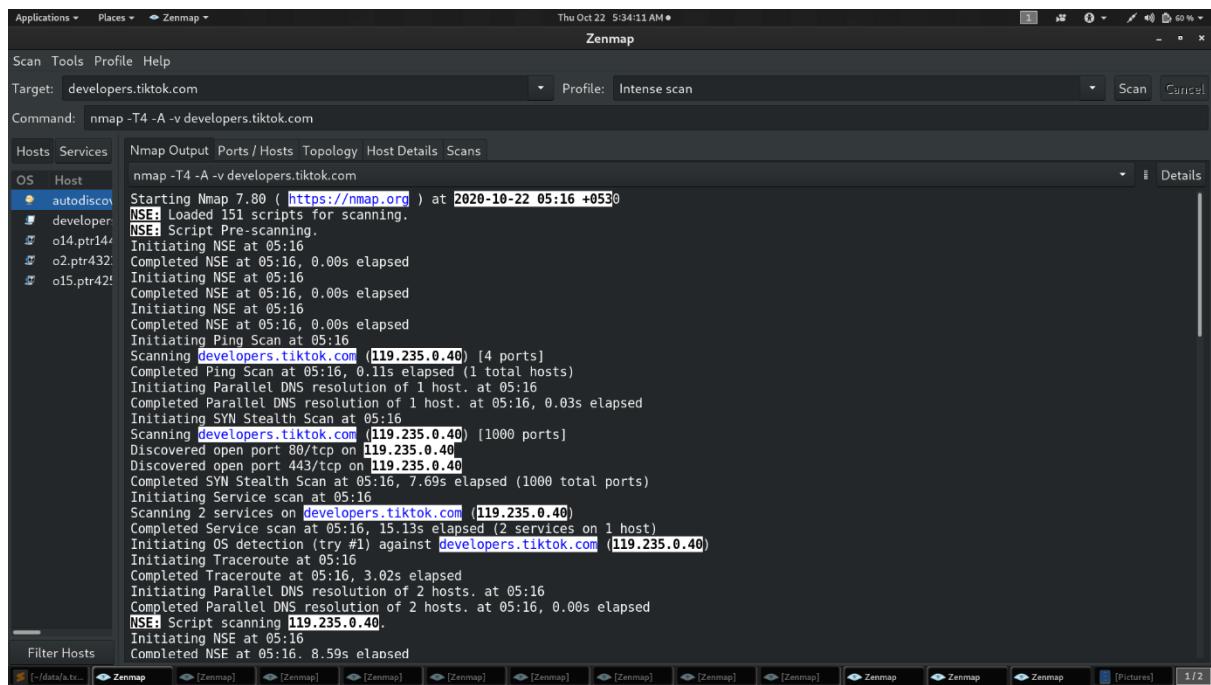
Date of submission  
24<sup>th</sup> of October in 2020

## **Acknowledgement**

I would like to express my deep gratuity for his invaluable guidance and advice, Dr. Lakmal rupasinghe the lecture in charge of Web security, which was vital to the initiation of this web audit.

I also want to thank Ms. Chethna Lyanapathirana, Ms. Lanisha Ruggahakotuwa and Ms. Chathu Udagedra for the help and guidance they have given us during this Web audit.

## 1. developers.tiktok.com



The screenshot shows the Zenmap interface with the following details:

- Top bar: Applications, Places, Zenmap (selected), Thu Oct 22 5:34:11 AM •, Scan, Cancel.
- Toolbar: Scan, Tools, Profile, Help.
- Scan parameters: Target: developers.tiktok.com, Profile: Intense scan, Command: nmap -T4 -A -v developers.tiktok.com.
- Host list: OS, Host, autodiscovery, developer, o14.ptr14, o2.ptr432, o15.ptr425.
- Output pane: Displays the Nmap command and its execution log, including the discovery of host 119.235.0.40 and the identification of two services (80/tcp and 443/tcp) on that host.
- Bottom status bar: Shows multiple Zenmap instances running and a page number indicator [1/2].

The screenshot shows the Zenmap interface with the following details:

- Toolbar:** Applications, Places, Zenmap, Thu Oct 22 5:34:21 AM, Scan, Cancel.
- Header:** Scan, Tools, Profile, Help.
- Target:** developers.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v developers.tiktok.com
- Hosts Services:** Hosts (selected), Services.
- OS Host:** autodisco (blue dot).
- Host List:** developer, o14.ptr44, o2.ptr432, o15.ptr42.
- Nmap Output:**
  - Completed parallel DNS resolution of 2 hosts. At 05:16, 0.00s elapsed.
  - NSE: Script scanning 119.235.0.40.
  - Initiating NSE at 05:16.
  - Completed NSE at 05:16, 8.59s elapsed.
  - Initiating NSE at 05:16.
  - Completed NSE at 05:16, 0.58s elapsed.
  - Initiating NSE at 05:16.
  - Completed NSE at 05:16, 0.00s elapsed.
- Scan Report:** Nmap scan report for [developers.tiktok.com](http://developers.tiktok.com) (119.235.0.40)  
Host is up (0.027s latency).  
Other addresses for [developers.tiktok.com](http://developers.tiktok.com) (not scanned): 119.235.0.41  
rDNS record for 119.235.0.40: a119-235-0-40.deploy.akamaitechnologies.com  
Not shown: 998 filtered ports
- Ports:**
  - PORT STATE SERVICE VERSION  
80/tcp open http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
    - | http-methods:
      - |\_ Supported Methods: GET HEAD POST OPTIONS
    - | http-server-header: nginx
    - | http-title: Did Not Follow Redirect to <https://developers.tiktok.com/>
  - 443/tcp open ssl/https AkamaiGHost
    - | http-favicon: Unknown favicon MD5: FAFB7D2F29F05D703CD8C55136E4D74B
    - | http-methods:
      - Supported Methods: GET HEAD POST OPTIONS
    - | http-server-header:
      - |\_ AkamaiGHost
    - | nginx
    - | http-tranx-info: Problem with XML parsing of /evox/about
    - | ssl-cert: Subject: commonName=tiktok.com
    - | Subject Alternative Name: DNS:tiktok.com, DNS:tiktok.com
    - | Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US

Scan Tools Profile Help

Target: developers.tiktok.com | Profile: Intense scan | Scan | Cancel

Command: nmap -T4 -A -v developers.tiktok.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host autodisco... developer o14.ptr44... o2.ptr432... o15.ptr42...

| tls-alpn:  
| http/1.1  
| tls-nextprotoneg:  
| http/1.1  
| http/1.0

**Warning:** OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

**Device type:** specialized[WAP/phone]

**Running:** iPXE 1.0.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded

**OS CPE:** cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux\_kernel:2.4.20 cpe:/o:linux:linux\_kernel:2.6.22 cpe:/h:sonyericsson:u8i\_vivaz

**OS details:** iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

**Network Distance:** 9 hops

TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 2.56 ms homerouter.cpe (192.168.8.1)  
2 ... 8  
9 30.60 ms a119-235-0-40.deploy.akamaitechnologies.com (119.235.0.40)

**NSE:** Script Post-scanning.  
Initiating NSE at 05:16  
Completed NSE at 05:16, 0.00s elapsed  
Initiating NSE at 05:16  
Completed NSE at 05:16, 0.00s elapsed  
Initiating NSE at 05:16  
Completed NSE at 05:16, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap  
OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.  
**Nmap done:** 1 IP address (1 host up) scanned in 38.99 seconds  
Raw packets sent: 2108 (95.736KB) | Rcvd: 14 (722B)

## 2. effect.tiktok.com

```
Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 5:34:53 AM ▾ 1 60% ×
Scan Tools Profile Help
Target: effect.tiktok.com ▾ Profile: Intense scan ▾ Scan Cancel
Command: nmap -T4 -A -v effect.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans ▾ Details
OS Host
effect.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:17 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:17
Completed NSE at 05:17, 0.00s elapsed
Initiating NSE at 05:17
Completed NSE at 05:17, 0.00s elapsed
Initiating NSE at 05:17
Completed NSE at 05:17, 0.00s elapsed
Initiating NSE at 05:17
Completed NSE at 05:17, 0.00s elapsed
Initiating Ping Scan at 05:17
Scanning effect.tiktok.com [103.136.221.164] [4 ports]
Completed Ping Scan at 05:17, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:17
Completed Parallel DNS resolution of 1 host. at 05:17, 13.01s elapsed
Initiating SYN Stealth Scan at 05:17
Scanning effect.tiktok.com [103.136.221.164] [1000 ports]
Discovered open port 443/tcp on 103.136.221.164
Discovered open port 80/tcp on 103.136.221.164
Increasing send delay for 103.136.221.164 from 0 to 5 due to 11 out of 14 dropped probes since last increase.
SYN Stealth Scan Timing: About 44.60% done; ETC: 05:19 (0:00:39 remaining)
Increasing send delay for 103.136.221.164 from 5 to 10 due to 11 out of 15 dropped probes since last increase.
Completed SYN Stealth Scan at 05:21, 182.68s elapsed (1000 total ports)
Initiating Service scan at 05:21
Scanning 2 services on effect.tiktok.com [103.136.221.164]
Completed Service scan at 05:21, 0.80s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against effect.tiktok.com [103.136.221.164]
Initiating Traceroute at 05:21
Completed Traceroute at 05:21, 9.07s elapsed
NSE: Script scanning 103.136.221.164.
Initiating NSE at 05:21
Filter Hosts
```

The screenshot shows the Zenmap interface with a scan report for the target `effect.tiktok.com`. The command used was `nmap -T4 -A -v effect.tiktok.com`. The report details the following findings:

- Scanning 2 services on `effect.tiktok.com` (103.136.221.164)**
- Completed Service scan at 05:21, 0.80s elapsed (2 services on 1 host)
- Initiating OS detection (try #1) against `effect.tiktok.com` (103.136.221.164)
- Initiating Traceroute at 05:21
- Completed Traceroute at 05:21, 9.07s elapsed
- NSE:** Script scanning 103.136.221.164.
- Initiating NSE at 05:21
- Completed NSE at 05:21, 16.85s elapsed
- Initiating NSE at 05:21
- Completed NSE at 05:21, 5.14s elapsed
- Initiating NSE at 05:21
- Completed NSE at 05:21, 0.00s elapsed
- Nmap scan report for `effect.tiktok.com` (103.136.221.164)
- Host is up (0.084s latency).
- Other addresses for `effect.tiktok.com` (not scanned): 103.136.221.168 103.136.220.181 103.136.220.180
- Not shown: 998 filtered ports
- PORT STATE SERVICE VERSION**

PORT	STATE	SERVICE	VERSION
80/tcp	open	tcpwrapped	
443/tcp	open	tcpwrapped	

- Warning:** OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
- Device type:** specialized/WAP/phone
- Running:** iPXE 1. X, Linux 2.4.X|2.6.X, Sony Ericsson embedded
- OS CPE:** cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux\_kernel:2.4.20 cpe:/o:linux:linux\_kernel:2.6.22 cpe:/h:sonyericsson:u8i\_vivaz
- OS details:** iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson Ubi Vivaz mobile phone

At the bottom, there is a section titled "TRACEROUTE (using port 443/tcp)" showing a hop list from the target to the scanner.

```
Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 5:35:00 AM • Zenmap
Scan Tools Profile Help
Target: effect.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v effect.tiktok.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
effect.tiktok
Completed NSE at 05:21, 0.00s elapsed
Nmap scan report for effect.tiktok.com (103.136.221.164)
Host is up (0.004s latency).
Other addresses for effect.tiktok.com (not scanned): 103.136.221.168 103.136.220.181 103.136.220.180
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  tcpwrapped
443/tcp   open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|WAP|phone
Running: iPXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1  ... 30

NSE: Script Post-scanning.
Initiating NSE at 05:21
Completed NSE at 05:21, 0.00s elapsed
Initiating NSE at 05:21
Completed NSE at 05:21, 0.00s elapsed
Initiating NSE at 05:21
Completed NSE at 05:21, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 231.28 seconds
Raw packets sent: 2257 (102.292KB) | Rcvd: 10 (404B)
```

### 3. experiment.tiktok.com

The screenshot shows the Zenmap interface with the target set to "experiment.tiktok.com". The command entered is "nmap -T4 -A -v experiment.tiktok.com". The output window displays the Nmap 7.80 scan results, starting with the banner:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:18 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
```

It then details the scanning process, including parallel DNS resolution, SYN Stealth Scan, and service detection for port 80/tcp and 443/tcp. The output concludes with OS detection results for the host.

The screenshot shows the Zenmap interface with the target set to "experiment.tiktok.com". The command entered is "nmap -T4 -A -v experiment.tiktok.com". The output window displays the completed Nmap scan results, including the SYN Stealth Scan, service detection for port 80/tcp (tcpwrapped), and OS details for the host. The output also includes a warning about the unreliability of OS scan results due to missing ports.

```
Completed SYN Stealth Scan at 05:23, 275.04s elapsed (1000 total ports)
Initiating Service scan at 05:23
Completed Service scan at 05:23, 0.98s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against experiment.tiktok.com [119.235.0.40]
Initiating Traceroute at 05:23
Completed Traceroute at 05:23, 9.09s elapsed
NSE: Script scanning 119.235.0.40.
Initiating NSE at 05:23
Completed NSE at 05:23, 16.86s elapsed
Initiating NSE at 05:23
Completed NSE at 05:23, 6.14s elapsed
Initiating NSE at 05:23
Completed NSE at 05:23, 0.00s elapsed
Nmap scan report for experiment.tiktok.com [119.235.0.40]
Host is up (0.058s latency).
Other addresses for experiment.tiktok.com (not scanned): 119.235.0.41
rDNS record for 119.235.0.40: al19-235-0-40.deploy.akamaitechnologies.com
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  tcpwrapped
443/tcp   open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|WAP|phone
Running: iPXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:ipxe:ipxe:1.0.0#2b cpe:/o:linux:linux kernel:2.4.20 cpe:/o:linux:linux kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone
TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
```

The screenshot shows the Zenmap interface with the following details:

- Target:** experiment.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v experiment.tiktok.com
- Hosts Services** tab is selected.
- OS Host** section shows:
  - activity.tiktok (business-s)
  - experiment (experim)
- Nmap Output** tab is selected, displaying the scan results:
  - Nmap scan report for experiment.tiktok.com (119.235.0.40)**
  - Host is up (0.058s latency).
  - Other addresses for experiment.tiktok.com (not scanned): 119.235.0.41
  - rDNS record for 119.235.0.40: a119-235-0-40.deploy.akamaitechnologies.com
  - Not shown:** 998 filtered ports
  - PORT STATE SERVICE VERSION**
  - 80/tcp open tcpwrapped
  - 443/tcp open tcpwrapped
  - Warning:** OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
  - Device type:** specialized|WAP|phone
  - Running:** iPXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded
  - OS CPE:** cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux\_kernel:2.4.20 cpe:/o:linux:linux\_kernel:2.6.22 cpe:/h:sonyericsson:u8i\_vivaz
  - OS details:** iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone
- TRACEROUTE (using port 443/tcp)**
  - HOP RTT ADDRESS
  - 1 ... 30
- NSE:** Script Post-scanning.
  - Initiating NSE at 05:23
  - Completed NSE at 05:23, 0.00s elapsed
  - Initiating NSE at 05:23
  - Completed NSE at 05:23, 0.00s elapsed
  - Initiating NSE at 05:23
  - Completed NSE at 05:23, 0.00s elapsed
- Read data files from:** /usr/bin/../share/nmap
- OS and Service detection performed.** Please report any incorrect results at <https://nmap.org/submit/>.
- Nmap done:** 1 IP address (1 host up) scanned in 313.45 seconds
- Raw packets sent:** 2305 (104.404KB) | Rcvd: 7 (308B)

#### **4. feelgood-api.tiktok.com**

```
Applications Places Zenmap Thu Oct 22 6:37:13 AM • Zenmap
Scan Tools Profile Help Target: feelgood-api.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v feelgood-api.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans Details
OS Host
feelgood- Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:19 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:19
Completed NSE at 06:19, 0.00s elapsed
Initiating NSE at 06:19
Completed NSE at 06:19, 0.00s elapsed
Initiating NSE at 06:19
Completed NSE at 06:19, 0.00s elapsed
Initiating NSE at 06:19
Completed NSE at 06:19, 0.00s elapsed
Initiating Ping Scan at 06:19
Scanning feelgood-api.tiktok.com [104.75.84.63] [4 ports]
Completed Ping Scan at 06:19, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:19
Completed Parallel DNS resolution of 1 host. at 06:19, 0.02s elapsed
Initiating SYN Stealth Scan at 06:19
Scanning feelgood-api.tiktok.com [104.75.84.63] [1000 ports]
Discovered open port 443/tcp on 104.75.84.63
Completed SYN Stealth Scan at 06:20, 13.06s elapsed (1000 total ports)
Initiating Service scan at 06:20
Scanning 1 service on feelgood-api.tiktok.com [104.75.84.63]
Completed Service scan at 06:20, 13.34s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against feelgood-api.tiktok.com [104.75.84.63]
Retrying OS detection (try #2) against feelgood-api.tiktok.com [104.75.84.63]
Initiating Traceroute at 06:20
Completed Traceroute at 06:20, 4.06s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 06:20
Completed Parallel DNS resolution of 7 hosts. at 06:20, 13.00s elapsed
NSE: Script scanning 104.75.84.63.
Initiating NSE at 06:20
Completed NSE at 06:20, 2.44s elapsed
Filter Hosts
```

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 6:37:16 AM ▾

**Zenmap**

Scan Tools Profile Help

Target: feelgood-api.tiktok.com ▾ Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v feelgood-api.tiktok.com

Hosts Services

**feelgood-api.tiktok.com**

Completed Parallel DNS resolution of 7 hosts. at 06:20, 13.00s elapsed

NSE: Script scanning 104.75.84.63.

Initiating NSE at 06:20

Completed NSE at 06:20, 2.44s elapsed

Initiating NSE at 06:20

Completed NSE at 06:20, 0.49s elapsed

Initiating NSE at 06:20

Completed NSE at 06:20, 0.00s elapsed

Nmap scan report for [feelgood-api.tiktok.com](#) (104.75.84.63)

Host is up (0.036s latency).

Other addresses for [feelgood-api.tiktok.com](#) (not scanned): 104.75.84.56

rDNS record for 104.75.84.63: a104-75-84-63.deploy.static.akamaitechnologies.com

Not shown: 998 filtered ports

PORT	STATE	SERVICE	VERSION
53/tcp	closed	domain	
443/tcp	open	ssl/http	AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
http-methods:			
_ Supported Methods: GET HEAD POST			
_http-server-header: nginx			
_http-title: 404 Not Found			
ssl-cert: Subject: commonName=*.tiktok.com			
Subject Alternative Name: DNS:*.tiktok.com, DNS:tiktok.com			
Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US			
Public Key type: rsa			
Public Key bits: 2048			
Signature Algorithm: sha256WithRSAEncryption			
Not valid before: 2019-11-14T00:00:00			
Not valid after: 2022-01-12T12:00:00			
MD5: 6042 e736 dd95 7460 aa10 bb3e 309f f719			
SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5			

Filter Hosts

-/data/a.txt - Sublime Text (UNRE... ▾ Pictures [Zenmap] [Zenmap] 1/2

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 6:37:21 AM ▾

**Zenmap**

Scan Tools Profile Help

Target: feelgood-api.tiktok.com ▾ Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v feelgood-api.tiktok.com

Hosts Services

**feelgood-api.tiktok.com**

| Subject Alternative Name: DNS:\*.tiktok.com, DNS:tiktok.com

| Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2019-11-14T00:00:00

| Not valid after: 2022-01-12T12:00:00

| MD5: 6042 e736 dd95 7460 aa10 bb3e 309f f719

| SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5

Device type: general purpose

Running (JUST GUESSING): Linux 2.6.X (85%)

OS CPE: cpe:/o:linux:linux\_kernel:2.6.28

Aggressive OS guesses: Linux 2.6.28 (85%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 13 hops

TRACEROUTE (using port 53/tcp)

HOP	RTT	ADDRESS
1	6.63 ms	<a href="#">homerrouter.cpe</a> (192.168.8.1)
2	...	3
4	20.17 ms	<a href="#">10.12.83.25</a>
5	24.42 ms	<a href="#">10.12.2.162</a>
6	24.63 ms	<a href="#">103.87.125.97</a>
7	...	
8	24.86 ms	<a href="#">103.87.125.18</a>
9	20.62 ms	<a href="#">222.165.175.70</a>
10	...	12
13	17.05 ms	<a href="#">a104-75-84-63.deploy.static.akamaitechnologies.com</a> (104.75.84.63)

NSE: Script Post-scanning.

-/data/a.txt - Sublime Text (UNRE... ▾ Pictures [Zenmap] [Zenmap] 1/2

```

Applications Scan Tools Profile Help
Target: feelgood-api.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v feelgood-api.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
feelgood-a
OS CPE: cpe:/o:linux:linux_kernel:2.6.28
Aggressive OS guesses: Linux 2.6.28 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops

TRACEROUTE (using port 53/tcp)
HOP RTT ADDRESS
1 6.63 ms home router.cpe (192.168.8.1)
2 ...
3
4 20.17 ms 10.12.83.25
5 24.42 ms 10.12.2.162
6 24.63 ms 103.87.125.97
7 ...
8 24.86 ms 103.87.125.18
9 20.62 ms 222.165.175.70
10 ...
11 17.05 ms a104-75-84-63.deploy.static.akamaitechnologies.com (104.75.84.63)

NSE: Script Post-scanning.
Initiating NSE at 06:20
Completed NSE at 06:20, 0.00s elapsed
Initiating NSE at 06:20
Completed NSE at 06:20, 0.00s elapsed
Initiating NSE at 06:20
Completed NSE at 06:20, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 57.00 seconds
Raw packets sent: 2182 (99.34KB) | Rcvd: 31 (2.516KB)

```

## 5. getstarted.tiktok.com

```

Applications Scan Tools Profile Help
Target: getstarted.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v getstarted.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
getstarted
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:31 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:31
Completed NSE at 06:31, 0.00s elapsed
Initiating NSE at 06:31
Completed NSE at 06:31, 0.00s elapsed
Initiating NSE at 06:31
Completed NSE at 06:31, 0.00s elapsed
Initiating NSE at 06:31
Completed NSE at 06:31, 0.00s elapsed
Initiating Ping Scan at 06:31
Scanning getstarted.tiktok.com (104.75.84.63) [4 ports]
Completed Ping Scan at 06:31, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:31
Completed Parallel DNS resolution of 1 host. at 06:31, 0.66s elapsed
Initiating SYN Stealth Scan at 06:31
Scanning getstarted.tiktok.com (104.75.84.63) [1000 ports]
Discovered open port 443/tcp on 104.75.84.63
Discovered open port 80/tcp on 104.75.84.63
Increasing send delay for 104.75.84.63 from 0 to 5 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 104.75.84.63 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 44.15% done; ETC: 06:32 (0:00:39 remaining)
Completed SYN Stealth Scan at 06:32, 72.82s elapsed (1000 total ports)
Initiating Service scan at 06:32
Scanning 2 services on getstarted.tiktok.com (104.75.84.63)
Completed Service scan at 06:33, 12.32s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against getstarted.tiktok.com (104.75.84.63)
Retrying OS detection (try #2) against getstarted.tiktok.com (104.75.84.63)
Initiating Traceroute at 06:33
Completed Traceroute at 06:33, 3.02s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 06:33

```

Applications ▾ Places ▾ Zenmap ▾

The Oct 22 6:37:51 AM •

**Zenmap**

Scan Tools Profile Help

Target: getstarted.tiktok.com ▾ Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v getstarted.tiktok.com

Hosts Services

OS Host

**getstarted**

```

nmap -T4 -A -v getstarted.tiktok.com
Initiating Traceroute at 06:33
Completed Traceroute at 06:33, 3.02s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 06:33
Completed Parallel DNS resolution of 9 hosts. at 06:33, 13.00s elapsed
NSE: Script scanning 104.75.84.63
Initiating NSE at 06:33
Completed NSE at 06:33, 8.65s elapsed
Initiating NSE at 06:33
Completed NSE at 06:33, 0.51s elapsed
Initiating NSE at 06:33
Completed NSE at 06:33, 0.00s elapsed
Nmap scan report for getstarted.tiktok.com (104.75.84.63)
Host is up (0.040s latency).
Other addresses for getstarted.tiktok.com (not scanned): 104.75.84.56
rDNS record for 104.75.84.63: a104-75-84-63.deploy.static.akamaitechnologies.com
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
53/tcp    closed domain
80/tcp    open  http   AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
| http-methods:
|_  Supported Methods: GET HEAD POST
| http-server-header: nginx
| http-title: Did not follow redirect to https://getstarted.tiktok.com/
443/tcp   open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
| http-methods:
|_  Supported Methods: HEAD POST
| http-robots.txt: 1 disallowed entry
|_/
| http-server-header: nginx
|_http-title: Get your business discovered on TikTok

```

Filter Hosts

-/data/a.txt - Sublime Text (UNRE... [Pictures] Zenmap Zenmap 1/2

Applications ▾ Places ▾ Zenmap ▾

The Oct 22 6:37:55 AM •

**Zenmap**

Scan Tools Profile Help

Target: getstarted.tiktok.com ▾ Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v getstarted.tiktok.com

Hosts Services

OS Host

**getstarted**

```

Supported Methods: HEAD POST
http-robots.txt: 1 disallowed entry
/
http-server-header: nginx
http-title: Get your business discovered on TikTok
http-trane-info: Problem with XML parsing of /evox/about
ssl-cert: Subject: commonName=*.tiktok.com
Subject Alternative Name: DNS:*.tiktok.com, DNS:tiktok.com
Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2019-11-14T00:00:00
Not valid after: 2022-01-12T12:00:00
MD5: 6042 e736 dd95 7460 aa10 bb3e 309f f719
SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5
Device type: general purpose|storage-misc|firewall
Running (JUST GUESSING): Linux 4.X|3.X|2.6.X (91%), Synology DiskStation Manager 5.X (86%), WatchGuard Fireware 11.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel cpe:/a:synology:diskstation_manager:5.1 cpe:/o:watchguard:fireware:11.8
Aggressive OS guesses: Linux 4.4 (91%), Linux 4.0 (91%), Linux 3.10 - 3.16 (90%), Linux 3.10 (89%), Linux 4.9 (88%), Linux 3.10 - 3.12 (88%), Linux 3.11 - 4.1 (87%), Linux 3.8 (87%), Linux 2.6.32 (87%), Linux 3.4 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1  2.34 ms  homerrouter.cpe (192.168.8.1)
2 ...
3  77.41 ms  10.12.90.85
```

Filter Hosts

-/data/a.txt - Sublime Text (UNRE... [Pictures] Zenmap Zenmap 1/2

```

Scan Tools Profile Help
Target: getstarted.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v getstarted.tiktok.com

Hosts Services
OS Host
getstarted
Aggressive OS guesses: Linux 4.4 (91%), Linux 4.0 (91%), Linux 3.10 - 3.16 (90%), Linux 3.10 (89%), Linux 4.9 (88%), Linux 3.10 - 3.12 (88%), Linux 3.11 - 4.1 (87%), Linux 3.8 (87%), Linux 2.6.32 (87%), Linux 3.4 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

TRACEROUTE (using port 53/tcp)
HOP RTT ADDRESS
1 2.34 ms homerouter.cpe (192.168.8.1)
2
3 77.41 ms 10.12.90.85
4 57.80 ms 10.12.83.25
5 59.02 ms 10.12.2.162
6 58.67 ms 103.87.125.97
7 41.89 ms 103.87.124.81
8 57.81 ms 103.87.125.18
9 41.67 ms 222.165.175.74
10 40.94 ms a104-75-84-63.deploy.static.akamaitechnologies.com (104.75.84.63)

NSE: Script Post-scanning.
Initiating NSE at 06:33
Completed NSE at 06:33, 0.00s elapsed
Initiating NSE at 06:33
Completed NSE at 06:33, 0.00s elapsed
Initiating NSE at 06:33
Completed NSE at 06:33, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 116.29 seconds
Raw packets sent: 2149 (97.240KB) | Rcvd: 48 (3.272KB)

```

## 6. login.tiktok.com

```

Scan Tools Profile Help
Target: login.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v login.tiktok.com

Hosts Services
OS Host
login.tiktok
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:59 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:59
Completed NSE at 05:59, 0.00s elapsed
Initiating NSE at 05:59
Completed NSE at 05:59, 0.00s elapsed
Initiating NSE at 05:59
Completed NSE at 05:59, 0.00s elapsed
Initiating NSE at 05:59
Completed NSE at 05:59, 0.00s elapsed
Initiating Ping Scan at 05:59
Scanning login.tiktok.com [103.136.221.168] [4 ports]
Completed Ping Scan at 05:59, 1.62s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:59
Completed Parallel DNS resolution of 1 host. at 06:00, 13.01s elapsed
Initiating SYN Stealth Scan at 06:00
Scanning login.tiktok.com [103.136.221.168] [1000 ports]
Discovered open port 443/tcp on 103.136.221.168
Discovered open port 80/tcp on 103.136.221.168
Increasing send delay for 103.136.221.168 from 0 to 5 due to 11 out of 20 dropped probes since last increase.
Completed SYN Stealth Scan at 06:00, 36.55s elapsed (1000 total ports)
Initiating Service scan at 06:00
Scanning 2 services on login.tiktok.com [103.136.221.168]
Completed Service scan at 06:00, 13.51s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against login.tiktok.com [103.136.221.168]
Retrying OS detection (try #2) against login.tiktok.com [103.136.221.168]
Initiating Traceroute at 06:01
Completed Traceroute at 06:01, 3.05s elapsed
Initiating Parallel DNS resolution of 10 hosts. at 06:01
Completed Parallel DNS resolution of 10 hosts. at 06:01, 13.02s elapsed
NSE: Script scanning 103.136.221.168.

```

```
Applications Places Zenmap Thu Oct 22 6:04:50 AM Zenmap
Scan Tools Profile Help Target: login.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v login.tiktok.com
Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS Host login.tiktok.com
Completed Parallel DNS resolution of 10 hosts. at 06:01, 13.02s elapsed
NSE: Script scanning 103.136.221.168.
Initiating NSE at 06:01
Completed NSE at 06:01, 3.28s elapsed
Initiating NSE at 06:01
Completed NSE at 06:01, 0.68s elapsed
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Nmap scan report for login.tiktok.com (103.136.221.168)
Host is up (0.075s latency).
Other addresses for login.tiktok.com (not scanned): 103.136.221.164 103.136.220.180 103.136.220.181
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp     open  http    nginx
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-title: Did Not Follow Redirect to https://login.tiktok.com/
443/tcp    open  ssl/http nginx
| http-favicon: Unknown favicon MD5: 01A542820B839CB59D6A2C3FE7342559
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-title: Log in | TikTok
|_ Requested resource was https://www.tiktok.com/login/
| http-tranx-info: Problem with XML parsing of /evox/about
| ssl-cert: Subject: commonName="tiktok.com"
|_ Subject Alternative Name: DNS:*.tiktok.com, DNS:tiktok.com
| Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
Filter Hosts
```

```

Thu Oct 22 6:04:58 AM • Zenmap
Scan Tools Profile Help
Target: login.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v login.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host login.tiktok.com
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 1.57 ms homerouter.cpe (192.168.8.1)
2 ...
3 26.16 ms 10.12.98.85
4 39.41 ms 10.12.83.25
5 35.45 ms 10.12.2.162
6 30.70 ms 103.87.125.97
7 26.16 ms 103.87.124.81
8 79.38 ms 103.87.124.74
9 79.36 ms 138699.sgw.equinix.com (27.111.229.190)
10 87.36 ms 172.18.6.101
11 ...
15 67.26 ms 103.136.221.168

NSE: Script Post-scanning.
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 91.28 seconds
Raw packets sent: 2143 (97.000KB) | Rcvd: 51 (4.398KB)

Filter Hosts

```

## 7. m.tiktok.com

```

Thu Oct 22 6:05:27 AM • Zenmap
Scan Tools Profile Help
Target: m.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v m.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host m.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:57 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:57
Completed NSE at 05:57, 0.00s elapsed
Initiating NSE at 05:57
Completed NSE at 05:57, 0.00s elapsed
Initiating NSE at 05:57
Completed NSE at 05:57, 0.00s elapsed
Initiating NSE at 05:57
Completed NSE at 05:57, 0.00s elapsed
Initiating Ping Scan at 05:57
Scanning m.tiktok.com (119.235.0.40) [4 ports]
Completed Ping Scan at 05:57, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:57
Completed Parallel DNS resolution of 1 host. at 05:57, 0.04s elapsed
Initiating SYN Stealth Scan at 05:57
Scanning m.tiktok.com (119.235.0.40) [1000 ports]
Discovered open port 80/tcp on 119.235.0.40
Discovered open port 443/tcp on 119.235.0.40
Increasing send delay for 119.235.0.40 From 0 to 5 due to 11 out of 16 dropped probes since last increase.
SYN Stealth Scan Timing: About 43.63% done; ETC: 05:59 (0:00:40 remaining)
Increasing send delay for 119.235.0.40 From 5 to 10 due to 11 out of 15 dropped probes since last increase.
Completed SYN Stealth Scan at 05:59, 95.41s elapsed (1000 total ports)
Initiating Service scan at 05:59
Scanning 2 services on m.tiktok.com (119.235.0.40)
Completed Service scan at 05:59, 5.00s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against m.tiktok.com (119.235.0.40)
Retrying OS detection (try #2) against m.tiktok.com (119.235.0.40)
Initiating Traceroute at 05:59
Completed Traceroute at 05:59, 3.02s elapsed
Initiating Parallel DNS resolution of 4 hosts. at 05:59

Filter Hosts

```

Scan Tools Profile Help

Target: m.tiktok.com Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v m.tiktok.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

m.tiktok.com

Initiating Parallel DNS resolution of 4 hosts. at 05:59 Completed Parallel DNS resolution of 4 hosts. at 06:00, 13.02s elapsed

NSE: Script scanning 119.235.0.40.

Initiating NSE at 06:00

Completed NSE at 06:00, 17.46s elapsed

Initiating NSE at 06:00

Completed NSE at 06:00, 0.91s elapsed

Initiating NSE at 06:00

Completed NSE at 06:00, 0.00s elapsed

Nmap scan report for m.tiktok.com (119.235.0.40)

Host is up (0.029s latency).

Other addresses for m.tiktok.com (not scanned): 119.235.0.41

rDNS record for 119.235.0.40: 119-235-0-40.deploy.akamaitechnologies.com

Not shown: 998 filtered ports

PORT	STATE	SERVICE	VERSION
80/tcp	open	tcpwrapped	
http-server-header:			
AkamaiGhost			
nginx			
http-title: Did not follow redirect to https://m.tiktok.com/			
443/tcp	open	tcpwrapped	
http-server-header:			
AkamaiGhost			
nginx			
ssl-cert: Subject: commonName=tiktok.com			
Subject Alternative Name: DNS:tiktok.com, DNS:tiktok.com			
Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US			
Public Key type: rsa			
Public Key bits: 2048			

Filter Hosts

```
Applications Places Zenmap Thu Oct 22 6:05:37 AM • Zenmap
Scan Tools Profile Help
Target: m.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v m.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host m.tiktok.com Details
ssl-cert: Subject: commonName=*.tiktok.com
Subject Alternative Name: DNS:*.tiktok.com, DNS:tiktok.com
issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2019-11-14T00:00:00
Not valid after: 2022-01-12T12:00:00
MD5: 6042 e736 dd95 7460 aa10 bb3e 309f f719
SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5
ssl-date: TLS randomness does not represent time
tls-alpn:
| http/1.1
| tls-nextprotoneg:
| | http/1.1
| | http/1.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|WAP|router
Running (JUST GUESSING): Linux 4.X|3.X|2.4.X|2.6.X (93%), MikroTik RouterOS 6.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3.13 cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6 cpe:/o:mikrotik:routertos:6.15
Aggressive OS guesses: Linux 4.4 (93%), Linux 4.0 (87%), Linux 3.13 (87%), Linux 3.11 - 4.1 (87%), Linux 3.8 (87%), Linux 3.10 (86%), Linux 3.10 - 3.16 (86%), Linux 3.10 - 3.12 (86%), Linux 3.16 (86%), Linux 4.9 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 6 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 2.78 ms homerouter.cpe (192.168.8.1)
2 ... 3
```

```

Scan Tools Profile Help
Target: m.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v m.tiktok.com
Hosts Services
OS Host
m.tiktok.com
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|WAP|router
Running (JUST GUESSING): Linux 4.X|3.X|2.4.X|2.6.X (93%), MikroTik RouterOS 6.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3.13 cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6 cpe:/o:mikrotik:routeros:6.15
Aggressive OS guesses: Linux 4.4 (93%), Linux 4.0 (87%), Linux 3.13 (87%), Linux 3.11 - 4.1 (87%), Linux 3.8 (87%), Linux 3.10 (86%), Linux 3.10 - 3.16 (86%), Linux 3.10 - 3.12 (86%), Linux 3.16 (86%), Linux 4.9 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 6 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 2.78 ms homerouter.cpe (192.168.8.1)
2 ... 3
4 47.07 ms 10.12.83.25
5 29.65 ms 10.12.2.162
6 24.39 ms a119-235-0-40.deploy.akamaitechnologies.com (119.235.0.40)

NSE: Script Post-scanning.
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 145.71 seconds
Raw packets sent: 3184 (143.028KB) | Rcvd: 163 (16.399KB)

```

## 8. media.tiktok.com

```

Scan Tools Profile Help
Target: media.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v media.tiktok.com
Hosts Services
OS Host
media.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:56 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:56
Completed NSE at 05:56, 0.00s elapsed
Initiating NSE at 05:56
Completed NSE at 05:56, 0.00s elapsed
Initiating NSE at 05:56
Completed NSE at 05:56, 0.00s elapsed
Initiating Ping Scan at 05:56
Scanning media.tiktok.com (103.136.220.163) [4 ports]
Completed Ping Scan at 05:56, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:56
Completed Parallel DNS resolution of 1 host. at 05:57, 13.09s elapsed
Initiating SYN Stealth Scan at 05:57
Scanning media.tiktok.com (103.136.220.163) [1000 ports]
SYN Stealth Scan Timing: About 39.00% done; ETC: 05:58 (0:00:48 remaining)
Completed SYN Stealth Scan at 05:58, 75.70s elapsed (1000 total ports)
Initiating Service scan at 05:58
Initiating OS detection (try #1) against media.tiktok.com [103.136.220.163]
Retrying OS detection (try #2) against media.tiktok.com [103.136.220.163]
WARNING: OS didn't match until try #2
Initiating Traceroute at 05:58
Completed Traceroute at 05:58, 3.02s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 05:58
Completed Parallel DNS resolution of 9 hosts. at 05:58, 13.02s elapsed
NSE: Script scanning 103.136.220.163.
Initiating NSE at 05:58
Completed NSE at 05:58, 0.00s elapsed
Initiating NSE at 05:58

```

Scan Tools Profile Help

Target: media.tiktok.com Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v media.tiktok.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

media.tiktok

nmap -T4 -A -v media.tiktok.com

INITIALIZING NSE at 03:30

Completed NSE at 05:58, 0.00s elapsed

Initiating NSE at 05:58

Completed NSE at 05:58, 0.00s elapsed

Initiating NSE at 05:58

Completed NSE at 05:58, 0.00s elapsed

Nmap scan report for media.tiktok.com (103.136.220.163)

Host is up (0.073s latency).

Other addresses for media.tiktok.com (not scanned): 103.136.221.185 103.136.221.184 103.136.220.162

All 1000 scanned ports on media.tiktok.com (103.136.220.163) are filtered

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6.18

OS details: Linux 2.6.18, Linux 2.6.28, Linux 2.6.30

Network Distance: 11 hops

TRACEROUTE (using proto 1/icmp)

HOP RTT ADDRESS

1	1.14 ms	homeroouter.cpe (192.168.8.1)
2	...	3
4	28.34 ms	10.12.83.25
5	28.58 ms	10.12.2.162
6	29.55 ms	103.87.125.97
7	28.92 ms	103.87.124.81
8	77.85 ms	103.87.124.74
9	74.45 ms	138699.sgw.equninx.com (27.111.229.190)
10	74.18 ms	172.18.6.133
11	69.24 ms	103.136.220.163

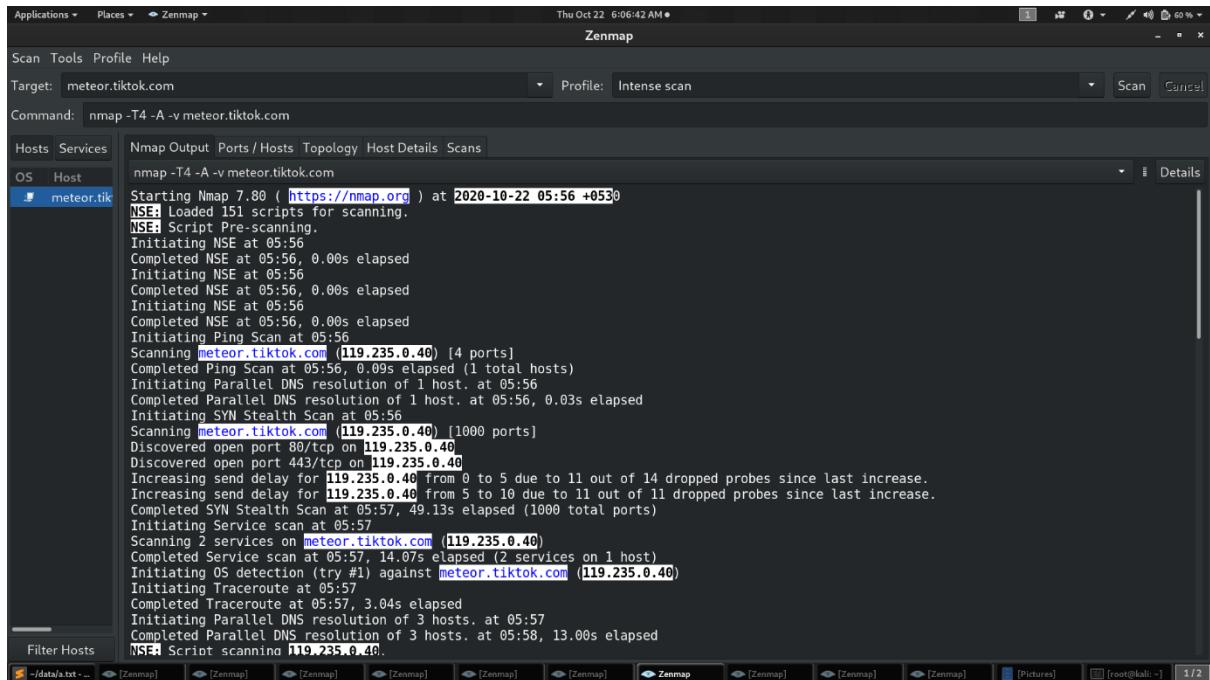
Filter Hosts

The screenshot shows the Zenmap interface with the following details:

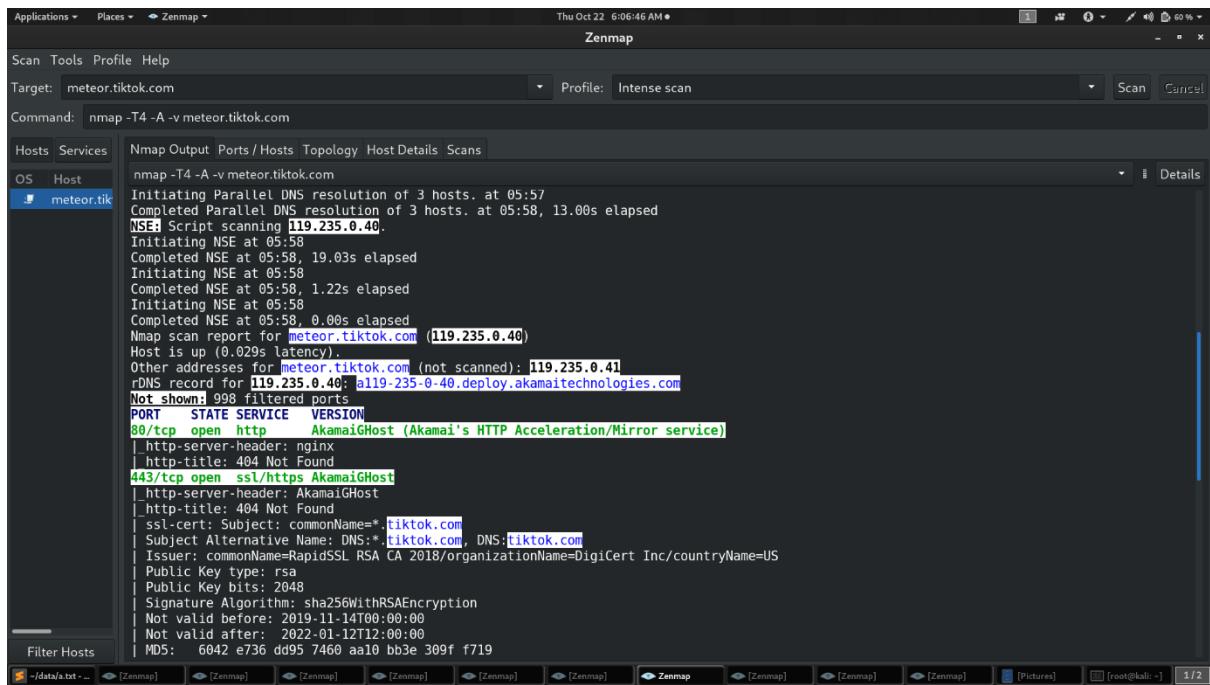
- Target:** media.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v media.tiktok.com
- Hosts Services:** Host media.tiktok.com
- OS:** Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux\_kernel:2.6.18  
OS details: Linux 2.6.18, Linux 2.6.28, Linux 2.6.30  
Network Distance: 11 hops
- Traceroute (using proto 1/icmp):**

HOP	RTT	ADDRESS
1	1.14 ms	homerouter.cpe (192.168.8.1)
2	... 3	
4	28.34 ms	10.12.83.25
5	28.58 ms	10.12.2.162
6	29.55 ms	103.87.125.97
7	28.92 ms	103.87.124.81
8	77.85 ms	103.87.124.74
9	74.45 ms	138699.sgw.equinix.com (27.111.229.190)
10	74.18 ms	172.18.6.133
11	69.24 ms	103.136.220.163
- NSE:** Script Post-scanning.  
Initiating NSE at 05:58  
Completed NSE at 05:58, 0.00s elapsed  
Initiating NSE at 05:58  
Completed NSE at 05:58, 0.00s elapsed  
Initiating NSE at 05:58  
Completed NSE at 05:58, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap
- OS and Service detection performed.** Please report any incorrect results at <https://nmap.org/submit/>.
- Nmap done:** 1 IP address (1 host up) scanned in 116.04 seconds  
Raw packets sent: 2069 (95.000KB) | Rcvd: 28 (2.160KB)

## 9. meteor.tiktok.com



```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:56 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:56
Completed NSE at 05:56, 0.00s elapsed
Initiating NSE at 05:56
Completed NSE at 05:56, 0.00s elapsed
Initiating NSE at 05:56
Completed NSE at 05:56, 0.00s elapsed
Initiating NSE at 05:56
Completed NSE at 05:56, 0.00s elapsed
Initiating Ping Scan at 05:56
Scanning meteor.tiktok.com (119.235.0.40) [4 ports]
Completed Ping Scan at 05:56, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:56
Completed Parallel DNS resolution of 1 host. at 05:56, 0.03s elapsed
Initiating SYN Stealth Scan at 05:56
Scanning meteor.tiktok.com (119.235.0.40) [1000 ports]
Discovered open port 80/tcp on 119.235.0.40
Discovered open port 443/tcp on 119.235.0.40
Increasing send delay for 119.235.0.40 from 0 to 5 due to 11 out of 14 dropped probes since last increase.
Increasing send delay for 119.235.0.40 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
Completed SYN Stealth Scan at 05:57, 49.13s elapsed (1000 total ports)
Initiating Service scan at 05:57
Scanning 2 services on meteor.tiktok.com (119.235.0.40)
Completed Service scan at 05:57, 14.07s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against meteor.tiktok.com (119.235.0.40)
Initiating Traceroute at 05:57
Completed Traceroute at 05:57, 3.04s elapsed
Initiating Parallel DNS resolution of 3 hosts. at 05:57
Completed Parallel DNS resolution of 3 hosts. at 05:58, 13.00s elapsed
NSE: Script scanning 119.235.0.40.
```



```
Initiating Parallel DNS resolution of 3 hosts. at 05:57
Completed Parallel DNS resolution of 3 hosts. at 05:58, 13.00s elapsed
NSE: Script scanning 119.235.0.40.
Initiating NSE at 05:58
Completed NSE at 05:58, 19.03s elapsed
Initiating NSE at 05:58
Completed NSE at 05:58, 1.22s elapsed
Initiating NSE at 05:58
Completed NSE at 05:58, 0.00s elapsed
Nmap scan report for meteor.tiktok.com (119.235.0.40)
Host is up (0.029s latency).
Other addresses for meteor.tiktok.com (not scanned): 119.235.0.41
rDNS record for 119.235.0.40: al19-235-0-40.deploy.akamaitechnologies.com
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   AkamaiGhost (Akamai's HTTP Acceleration/Mirror service)
|_http-server-header: nginx
|_http-title: 404 Not Found
443/tcp   open  ssl/https AkamaiGhost
|_http-server-header: AkamaiGhost
|_http-title: 404 Not Found
| ssl-cert: Subject: commonName=tiktok.com
| Subject Alternative Name: DNS=tiktok.com, DNS=tiktok.com
| Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-11-14T00:00:00
| Not valid after: 2022-01-12T12:00:00
| MD5: 6042 e736 dd95 7460 aa10 bb3e 309f f719
```

The screenshot shows the Zenmap interface with the target set to `meteor.tiktok.com`. The command entered is `nmap -T4 -A -v meteor.tiktok.com`. The results tab is selected, showing the following details for the host `meteor.tiktok.com`:

- Subject Alternative Name: DNS=tiktok.com, DNS=tiktok.com
- Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US
- Public Key type: rsa
- Public Key bits: 2048
- Signature Algorithm: sha256WithRSAEncryption
- Not valid before: 2019-11-14T00:00:00
- Not valid after: 2022-01-12T12:00:00
- MDS: 6042 e736 dd95 7460 aa10 bb3e f719
- SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5
- SSL date: TLS randomness does not represent time
- tls-alpn:
  - http/1.1
  - tls-nextprotoneg:
  - http/1.1
  - http/1.0
- Warning:** OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
- Device type:** specialized|WAP|phone
- Running:** iPXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded
- OS CPE:** cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux\_kernel:2.4.20 cpe:/o:linux:linux\_kernel:2.6.22 cpe:/h:sonyericsson:u8i\_vivaz
- OS details:** iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone
- Network Distance:** 6 hops

Below this, the **TRACEROUTE** section shows the path from the target to the router:

HOP	RTT	ADDRESS
1	3.01 ms	homeroouter.cpe (192.168.8.1)
2	... 3	
4	31.58 ms	10.12.83.25
5	...	
6	25.51 ms	a119-235-0-40.deploy.akamaitechnologies.com (119.235.0.40)

Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 6:06:53 AM ▾ 90 %

Scan Tools Profile Help

Target: meteor.tiktok.com Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v meteor.tiktok.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host meteor.tiktok.com

| tls-nextprotoneg:  
| http/1.1  
| http/1.0

**Warning:** OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

**Device type:** specialized|WAP|phone

**Running:** iPXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded

**OS CPE:** cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux\_kernel:2.4.20 cpe:/o:linux:linux\_kernel:2.6.22 cpe:/h:sonyericsson:u8i\_vivaz

**OS details:** iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

**Network Distance:** 6 hops

TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 3.01 ms homerouter.cpe (192.168.8.1)  
2 ...  
4 31.58 ms 10.12.83.25  
5 ...  
6 25.51 ms a119-235-0-40.deploy.akamaitechnologies.com (119.235.0.40)

**NSE:** Script Post-scanning.  
Initiating NSE at 05:58  
Completed NSE at 05:58, 0.00s elapsed  
Initiating NSE at 05:58  
Completed NSE at 05:58, 0.00s elapsed  
Initiating NSE at 05:58  
Completed NSE at 05:58, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap  
OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.  
**Nmap done:** 1 IP address (1 host up) scanned in 103.58 seconds  
Raw packets sent: 2135 (96.924KB) | Rcvd: 27 (1.382KB)

## 10.mg.tiktok.com

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:58 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:58
Completed NSE at 05:58, 0.00s elapsed
Initiating NSE at 05:58
Completed NSE at 05:58, 0.00s elapsed
Initiating NSE at 05:58
Completed NSE at 05:58, 0.00s elapsed
Initiating Ping Scan at 05:58
Scanning mg.tiktok.com [103.136.221.164] (4 ports)
Completed Ping Scan at 05:58, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:58
Completed Parallel DNS resolution of 1 host. at 05:58, 13.01s elapsed
Initiating SYN Stealth Scan at 05:58
Scanning mg.tiktok.com [103.136.221.164] (1000 ports)
SYN Stealth Scan Timing: About 43.00% done; ETC: 05:59 (0:00:41 remaining)
Completed SYN Stealth Scan at 05:59, 69.82s elapsed (1000 total ports)
Initiating Service scan at 05:59
Initiating OS detection (try #1) against mg.tiktok.com [103.136.221.164]
Retrying OS detection (try #2) against mg.tiktok.com [103.136.221.164]
Initiating Traceroute at 06:00
Completed Traceroute at 06:00, 3.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 06:00
Completed Parallel DNS resolution of 2 hosts. at 06:00, 13.00s elapsed
NSE: Script scanning 103.136.221.164.
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
```

```
Completed NSE at 06:00, 0.00s elapsed
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Nmap scan report for mg.tiktok.com (103.136.221.164)
Host is up (0.070s latency).
Other addresses for mg.tiktok.com (not scanned): 103.136.221.168 103.136.220.181 103.136.220.180
All 1000 scanned ports on mg.tiktok.com [103.136.221.164] are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 11 hops

TRACEROUTE (using proto icmp)
HOP RTT      ADDRESS
1  2.71 ms  homerouter.cpe [192.168.8.1]
2  ... 10
11 78.27 ms 103.136.221.164

NSE: Script Post-scanning.
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 107.85 seconds
Raw packets sent: 2080 (95.458KB) | Rcvd: 16 (1.562KB)
```

**11.musician.tiktok.com**

```
Applications Places Zenmap Thu Oct 22 6:09:01 AM • Zenmap
Scan Tools Profile Help Target: musician.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v musician.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host Details
musician.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:58 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:58
Completed NSE at 05:58, 0.00s elapsed
Initiating NSE at 05:58
Completed NSE at 05:58, 0.00s elapsed
Initiating NSE at 05:58
Completed NSE at 05:58, 0.00s elapsed
Initiating NSE at 05:58
Completed NSE at 05:58, 0.00s elapsed
Initiating Ping Scan at 05:58
Scanning musician.tiktok.com [103.136.220.180] [4 ports]
Completed Ping Scan at 05:58, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:58
Completed Parallel DNS resolution of 1 host. at 05:58, 13.00s elapsed
Initiating SYN Stealth Scan at 05:58
Scanning musician.tiktok.com [103.136.220.180] [1000 ports]
SYN Stealth Scan Timing: About 41.10% done; ETC: 06:00 (0:00:44 remaining)
Increasing send delay for 103.136.220.180 from 0 to 5 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 103.136.220.180 from 5 to 10 due to 11 out of 15 dropped probes since last increase.
Completed SYN Stealth Scan at 06:00, 91.07s elapsed (1000 total ports)
Initiating Service scan at 06:00
Initiating OS detection (try #1) against musician.tiktok.com [103.136.220.180]
Retrying OS detection (try #2) against musician.tiktok.com [103.136.220.180]
WARNING: OS didn't match until try #2
Initiating Traceroute at 06:00
Completed Traceroute at 06:00, 9.09s elapsed
Initiating Parallel DNS resolution of 6 hosts. at 06:00
Completed Parallel DNS resolution of 6 hosts. at 06:00, 13.00s elapsed
NSE: Script scanning 103.136.220.180.
Initiating NSE at 06:00
```

The screenshot shows the Zenmap interface with the following details:

- Applications**: Scan Tools Profile Help
- Target**: `musician.tiktok.com`
- Profile**: Intense scan
- Command**: `nmap -T4 -A -v musician.tiktok.com`
- Hosts Services** tab selected.
- OS Host** table:

OS	Host
musician.t	musician.tiktok.com (103.136.220.180)
- Nmap Output** tab content:

```
Initiating Traceroute at 06:00
Completed Traceroute at 06:00, 9.09s elapsed
Initiating Parallel DNS resolution of 6 hosts. at 06:00
Completed Parallel DNS resolution of 6 hosts. at 06:00, 13.00s elapsed
NSE: Script scanning 103.136.220.180
Initiating NSE at 06:00
Completed NSE at 06:00, 0.01s elapsed
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
NSE: Script scanning 103.136.220.180
Nmap scan report for musician.tiktok.com (103.136.220.180)
Host is up (0.081s latency).
Other addresses for musician.tiktok.com (not scanned): 103.136.220.181 103.136.221.168 103.136.221.164
All 1000 scanned ports on musician.tiktok.com [103.136.220.180] are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.18
OS details: Linux 2.6.18, Linux 2.6.28, Linux 2.6.30
Network Distance: 12 hops

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 2.41 ms homerouter.cpe (192.168.8.1)
2 ...
3 57.08 ms 10.12.90.85
4 42.88 ms 10.12.83.25
5 42.67 ms 10.12.2.162
6 47.28 ms 103.87.125.97
```
- Filter Hosts** button.

```
Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 6:09:07 AM ▾ 60 %
Scan Tools Profile Help
Target: musician.tiktok.com ▾ Profile: Intense scan ▾ Scan Cancel
Command: nmap -T4 -A -v musician.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
musician.tiktok.com
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.18
OS details: Linux 2.6.18, Linux 2.6.28, Linux 2.6.30
Network Distance: 12 hops

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 2.41 ms homeroouter.cpe (192.168.8.1)
2 ...
3 57.08 ms 10.12.90.85
4 42.88 ms 10.12.83.25
5 42.67 ms 10.12.2.162
6 47.28 ms 103.87.125.97
7 44.12 ms 103.87.124.81
8 ... 30

NSE: Script Post-scanning.
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Initiating NSE at 06:00
Completed NSE at 06:00, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 129.99 seconds
Raw packets sent: 2168 (98.958KB) | Rcvd: 36 (3.488KB)
```

12.newsroom.tiktok.com

```
Applications ▾ Places ▾ ➔ Zenmap ▾ Thu Oct 22 6:09:24 AM ▾ 1 2 3 4 5 6 7 8 9 0 60% Scan Tools Profile Help Target: newsroom.tiktok.com ▾ Profile: Intense scan Scan Cancel Command: nmap -T4 -A -v newsroom.tiktok.com Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans OS Host ▾ Details Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:59 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:59
Completed NSE at 05:59, 0.00s elapsed
Initiating NSE at 05:59
Completed NSE at 05:59, 0.00s elapsed
Initiating NSE at 05:59
Completed NSE at 05:59, 0.00s elapsed
Initiating NSE at 05:59
Completed NSE at 05:59, 0.00s elapsed
Failed to resolve "newsroom.tiktok.com".
NSE: Script Post-scanning.
Initiating NSE at 05:59
Completed NSE at 05:59, 0.00s elapsed
Initiating NSE at 05:59
Completed NSE at 05:59, 0.00s elapsed
Initiating NSE at 05:59
Completed NSE at 05:59, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.38 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

**13.notifications.tiktok.com**

```
Applications Places Zenmap Thu Oct 22 6:10:43 AM • 1 60% Scan Tools Profile Help Scan Cancel Target: notifications.tiktok.com Profile: Intense scan Command: nmap -T4 -A -v notifications.tiktok.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans OS Host notification
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:03 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:03
Completed NSE at 06:03, 0.00s elapsed
Initiating NSE at 06:03
Completed NSE at 06:03, 0.00s elapsed
Initiating NSE at 06:03
Completed NSE at 06:03, 0.00s elapsed
Initiating NSE at 06:03
Completed NSE at 06:03, 0.00s elapsed
Initiating Ping Scan at 06:03
Scanning notifications.tiktok.com (130.44.213.67) [4 ports]
Completed Ping Scan at 06:03, 0.36s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:03
Completed Parallel DNS resolution of 1 host. at 06:03, 0.55s elapsed
Initiating SYN Stealth Scan at 06:03
Scanning notifications.tiktok.com (130.44.213.67) [1000 ports]
Discovered open port 53/tcp on 130.44.213.67
SYN Stealth Timing] About 47.80% done; ETC: 06:05 (0:00:34 remaining)
Completed SYN Stealth Scan at 06:04, 41.85s elapsed (1000 total ports)
Initiating Service scan at 06:04
Scanning 1 service on notifications.tiktok.com (130.44.213.67)
Completed Service scan at 06:04, 2.59s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against notifications.tiktok.com (130.44.213.67)
Retrying OS detection (try #2) against notifications.tiktok.com (130.44.213.67)
Initiating Traceroute at 06:04
Completed Traceroute at 06:04, 3.34s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 06:04
Completed Parallel DNS resolution of 2 hosts. at 06:04, 0.00s elapsed
NSE: Script scanning 130.44.213.67.
Initiating NSE at 06:04
```

Scan Tools Profile Help

Target: notifications.tiktok.com Profile: Intense scan

Command: nmap -T4 -A -v notifications.tiktok.com

Hosts Services

OS Host

notification Initiating Parallel DNS resolution of 2 hosts. at 06:04  
Completed Parallel DNS resolution of 2 hosts. at 06:04, 0.00s elapsed  
NSE Script scanning [130.44.213.67].  
Initiating NSE at 06:04  
Completed NSE at 06:05, 10.47s elapsed  
Initiating NSE at 06:05  
Completed NSE at 06:05, 0.00s elapsed  
Initiating NSE at 06:05  
Completed NSE at 06:05, 0.00s elapsed  
Nmap scan report for notifications.tiktok.com [130.44.213.67]  
Host is up (0.30s latency).  
rDNS record for [130.44.213.67]: info.larksuite.com  
Not shown: 997 filtered ports

PORT	STATE	SERVICE	VERSION
53/tcp	open	tcpwrapped	
80/tcp	closed	http	
443/tcp	closed	https	

Device type: general purpose|firewall|broadband router  
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (92%), WatchGuard Fireware 11.X (86%), IPFire 2.X (86%)  
OS CPE: cpe:/o:linux:linux\_kernel:3 cpe:/o:linux:linux\_kernel:4 cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux\_kernel:2.6.32 cpe:/o:ipfire:ipfire:2.11  
Aggressive OS guesses: Linux 3.11 - 4.1 (92%), Linux 3.16 (91%), Linux 4.4 (91%), Linux 3.10 - 3.16 (90%), Linux 3.13 (89%), Linux 3.2 - 3.8 (86%), WatchGuard Fireware 11.8 (86%), Linux 3.10 (86%), IPFire 2.11 firewall (Linux 2.6.32) (86%), Linux 2.6.32 (85%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 12 hops

TRACEROUTE (using port 443/tcp)  
HOP RTT ADDRESS  
1 2.28 ms homerouter.cpe (192.168.8.1)

Filter Hosts

```

Scan Tools Profile Help
Target: notifications.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v notifications.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host notification
53/tcp open tcpwrapped
80/tcp closed http
443/tcp closed https
Device type: general purpose|firewall|broadband router
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (92%), WatchGuard Fireware 11.X (86%), IPFire 2.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:watchguard:fireware:11.8 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:ipfire:ipfire:2.11
Aggressive OS guesses: Linux 3.11 - 4.1 (92%), Linux 3.16 (91%), Linux 4.4 (91%), Linux 3.10 - 3.16 (90%), Linux 3.13 (89%), Linux 3.2 - 3.8 (86%), WatchGuard Fireware 11.8 (86%), Linux 3.10 (86%), IPFire 2.11 firewall (Linux 2.6.32) (86%), Linux 2.6.32 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 12 hops

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 2.28 ms homerouter.cpe (192.168.8.1)
2 ... 11
12 330.74 ms info.larksuite.com (130.44.213.67)

NSE: Script Post-scanning.
Initiating NSE at 06:05
Completed NSE at 06:05, 0.00s elapsed
Initiating NSE at 06:05
Completed NSE at 06:05, 0.00s elapsed
Initiating NSE at 06:05
Completed NSE at 06:05, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 78.03 seconds
Raw packets sent: 2157 (99.496KB) | Rcvd: 37 (2.048KB)

```

## 14.open-api.tiktok.com

```

Scan Tools Profile Help
Target: open-api.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v open-api.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host open-api.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:33 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:33
Completed NSE at 06:33, 0.00s elapsed
Initiating NSE at 06:33
Completed NSE at 06:33, 0.00s elapsed
Initiating NSE at 06:33
Completed NSE at 06:33, 0.00s elapsed
Initiating NSE at 06:33
Completed NSE at 06:33, 0.00s elapsed
Initiating Ping Scan at 06:33
Scanning open-api.tiktok.com (119.235.0.40) [4 ports]
Completed Ping Scan at 06:33, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:33
Completed Parallel DNS resolution of 1 host. at 06:33, 0.03s elapsed
Initiating SYN Stealth Scan at 06:33
Scanning open-api.tiktok.com (119.235.0.40) [1000 ports]
Discovered open port 80/tcp on 119.235.0.40
Discovered open port 443/tcp on 119.235.0.40
Completed SYN Stealth Scan at 06:33, 8.42s elapsed (1000 total ports)
Initiating Service scan at 06:33
Scanning 2 services on open-api.tiktok.com (119.235.0.40)
Completed Service scan at 06:33, 13.31s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against open-api.tiktok.com (119.235.0.40)
Retrying OS detection (try #2) against open-api.tiktok.com (119.235.0.40)
Initiating Traceroute at 06:33
Completed Traceroute at 06:33, 3.02s elapsed
Initiating Parallel DNS resolution of 5 hosts. at 06:33
Completed Parallel DNS resolution of 5 hosts. at 06:34, 13.02s elapsed
NSE: Script scanning 119.235.0.40.
Initiating NSE at 06:34

```

Applications ▾ Places ▾ Zenmap ▾

The Oct 22 6:38:15 AM •

Zenmap

Scan Tools Profile Help

Target: open-api.tiktok.com ▾ Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v open-api.tiktok.com

Hosts Services

OS Host open-api.tiktok.com

Initiating Parallel DNS resolution of 5 hosts. at 06:33  
Completed Parallel DNS resolution of 5 hosts. at 06:34, 13.02s elapsed  
NSE Script scanning 119.235.0.40.  
Initiating NSE at 06:34  
Completed NSE at 06:34, 2.84s elapsed  
Initiating NSE at 06:34  
Completed NSE at 06:34, 0.42s elapsed  
Initiating NSE at 06:34  
Completed NSE at 06:34, 0.00s elapsed  
Nmap scan report for open-api.tiktok.com (119.235.0.40)  
Host is up (0.03s latency).  
Other addresses for open-api.tiktok.com (not scanned): 119.235.0.41  
rDNS record for 119.235.0.40: a119-235-0-40.deploy.akamaitechnologies.com  
Not shown: 998 filtered ports

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
			http-methods: Supported Methods: GET HEAD POST OPTIONS http-server-header: nginx http-title: Did not follow redirect to https://open-api.tiktok.com/
443/tcp	open	ssl/http	AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
			http-methods: Supported Methods: GET HEAD POST http-server-header: nginx http-title: 404 Not Found ssl-cert: Subject: commonName=tiktok.com Subject Alternative Name: DNS:tiktok.com, DNS:tiktok.com Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US Public Key type: rsa Public Key bits: 2048

Filter Hosts

-/data/a.txt - Sublime Text (UNRE... [Pictures] Zenmap 1/2

Applications ▾ Places ▾ Zenmap ▾

The Oct 22 6:38:21 AM •

Zenmap

Scan Tools Profile Help

Target: open-api.tiktok.com ▾ Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v open-api.tiktok.com

Hosts Services

OS Host open-api.tiktok.com

Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US  
Public Key type: rsa  
Public Key bits: 2048  
Signature Algorithm: sha256WithRSAEncryption  
Not valid before: 2019-11-14T00:00:00  
Not valid after: 2022-01-12T12:00:00  
MD5: 6042 e736 dd95 7460 aa10 bb3e 309f f719  
SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5  
ssl-date: TLS randomness does not represent time  
tls-alpn:  
http/1.1  
tls-nextprotoneg:  
http/1.1  
http/1.0  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose|WAP|router  
Running (JUST GUESSING): Linux 4.X|3.X|2.4.X|2.6.X (93%), MikroTik RouterOS 6.X (85%)  
OS CPE: cpe:/o:linux:linux\_kernel:4.4 cpe:/o:linux:linux\_kernel:3.13 cpe:/o:linux:linux\_kernel:2.4.20 cpe:/o:linux:linux\_kernel:2.6 cpe:/o:mikrotik:routers:6.15  
Aggressive OS guesses: Linux 4.4 (93%), Linux 4.0 (87%), Linux 3.13 (87%), Linux 3.11 - 4.1 (87%), Linux 3.8 (87%), Linux 3.10 (86%), Linux 3.10 - 3.16 (86%), Linux 3.10 - 3.12 (86%), Linux 3.16 (86%), Linux 4.9 (86%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 6 hops

TRACEROUTE (using port 80/tcp)  
HOP RTT ADDRESS  
1 3.00 ms homerouter.cpe (192.168.8.1)  
2 ...  
3 63.31 ms 10.12.90.85  
4 36.98 ms 10.12.83.25

Filter Hosts

-/data/a.txt - Sublime Text (UNRE... [Pictures] Zenmap 1/2

```

Scan Tools Profile Help
Target: open-api.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v open-api.tiktok.com
Hosts Services
OS Host
open-api.tiktok.com
Device type: general purpose/WAP/router
Running (JUST GUESSING): Linux 4.X|3.X|2.4.X|2.6.X (93%), MikroTik RouterOS 6.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3.13 cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6 cpe:/o:mikrotik:routers:6.15
Aggressive OS guesses: Linux 4.4 (93%), Linux 4.0 (87%), Linux 3.13 (87%), Linux 3.11 - 4.1 (87%), Linux 3.8 (87%), Linux 3.10 (86%), Linux 3.10 - 3.16 (86%), Linux 3.10 - 3.12 (86%), Linux 3.16 (86%), Linux 4.9 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 6 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 3.00 ms homerouter.cpe (192.168.8.1)
2 ...
3 63.31 ms 10.12.90.85
4 36.98 ms 10.12.83.25
5 54.54 ms 10.12.2.162
6 54.24 ms a119-235-0-40.deploy.akamaitechnologies.com (119.235.0.40)

NSE: Script Post-scanning.
Initiating NSE at 06:34
Completed NSE at 06:34, 0.00s elapsed
Initiating NSE at 06:34
Completed NSE at 06:34, 0.00s elapsed
Initiating NSE at 06:34
Completed NSE at 06:34, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 46.61 seconds
Raw packets sent: 2103 (95.256KB) | Rcvd: 37 (2.784KB)

```

## 15.promotion-useast2a.tiktok.com

```

Scan Tools Profile Help
Target: promotion-useast2a.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v promotion-useast2a.tiktok.com
Hosts Services
OS Host
promotion
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:04 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:04
Completed NSE at 06:04, 0.00s elapsed
Initiating NSE at 06:04
Completed NSE at 06:04, 0.00s elapsed
Initiating NSE at 06:04
Completed NSE at 06:04, 0.00s elapsed
Initiating NSE at 06:04
Completed NSE at 06:04, 0.00s elapsed
Initiating Ping Scan at 06:04
Scanning promotion-useast2a.tiktok.com [147.160.184.50] (4 ports)
Completed Ping Scan at 06:04, 0.34s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:04
Completed Parallel DNS resolution of 1 host. at 06:04, 13.01s elapsed
Initiating SYN Stealth Scan at 06:04
Scanning promotion-useast2a.tiktok.com [147.160.184.50] (1000 ports)
Discovered open port 80/tcp on 147.160.184.50
SYN Stealth Scan Timing: About 6.85% done; ETC: 06:12 (0:07:02 remaining)
SYN Stealth Scan Timing: About 23.70% done; ETC: 06:09 (0:03:16 remaining)
Increasing send delay for 147.160.184.50 from 0 to 5 due to 11 out of 18 dropped probes since last increase.
Completed SYN Stealth Scan at 06:06, 102.59s elapsed (1000 total ports)
Initiating Service scan at 06:06
Scanning 1 service on promotion-useast2a.tiktok.com [147.160.184.50]
Completed Service scan at 06:06, 6.54s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against promotion-useast2a.tiktok.com [147.160.184.50]
Retrying OS detection (try #2) against promotion-useast2a.tiktok.com [147.160.184.50]
Initiating Traceroute at 06:06
Completed Traceroute at 06:06, 9.09s elapsed
Initiating Parallel DNS resolution of 1 host. at 06:06
Completed Parallel DNS resolution of 1 host. at 06:06, 0.00s elapsed

```

```
Applications Places Zenmap Thu Oct 22 6:11:36 AM • Zenmap
Scan Tools Profile Help
Target: promotion-useast2a.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v promotion-useast2a.tiktok.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host promotion Details
NSE: Script scanning 147.160.184.50.
Initiating NSE at 06:06
Completed Traceroute at 06:06, 9.09s elapsed
Initiating Parallel DNS resolution of 1 host. at 06:06
Completed Parallel DNS resolution of 1 host. at 06:06, 0.00s elapsed
NSE: Script scanning 147.160.184.50.
Initiating NSE at 06:06
Completed NSE at 06:07, 9.21s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 1.00s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Nmap scan report for promotion-useast2a.tiktok.com (147.160.184.50)
Host is up (0.24s latency).
Other addresses for promotion-useast2a.tiktok.com (not scanned): 147.160.184.34
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp      open  http    nginx
|_ http-methods:
|_ Supported Methods: GET HEAD OPTIONS
|_ http-title: Error
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1  2.58 ms  homerouter.cpe (192.168.8.1)
2  ... 30

NSE: Script Post-scanning.
Filter Hosts
```

```
Applications Places Zenmap Thu Oct 22 6:11:37 AM • Zenmap
Scan Tools Profile Help
Target: promotion-useast2a.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v promotion-useast2a.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans Details
OS Host promotion
nmap -T4 -A -v promotion-useast2a.tiktok.com
Nmap scan report for promotion-useast2a.tiktok.com (147.160.184.50)
Host is up (0.24s latency).
Other addresses for promotion-useast2a.tiktok.com (not scanned): 147.160.184.34
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx
|_ http-methods:
|   Supported Methods: GET HEAD OPTIONS
|_ http-title: Error
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1  2.58 ms  homerouter.cpe (192.168.8.1)
2  ... 30

NSE: Script Post-scanning.
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 155.86 seconds
Raw packets sent: 2206 (101.492KB) | Rcvd: 103 (6.707KB)
```

16.s16-ies.tiktok.com

The screenshot shows the Zenmap interface with the following details:

- Target:** s16-ies.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v s16-ies.tiktok.com
- Hosts:** login.tiktok (Up), s16-ies.tiktok (Up)
- Services:** Nmap Output, Ports/Hosts, Topology, Host Details, Scans (selected)
- OS:** Host
- Scans:** Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:05 +0530  
NSE: Loaded 151 scripts for scanning.  
NSE Script Pre-scanning.  
Initiating NSE at 06:05  
Completed NSE at 06:05, 0.00s elapsed  
Initiating NSE at 06:05  
Completed NSE at 06:05, 0.00s elapsed  
Initiating NSE at 06:05  
Completed NSE at 06:05, 0.00s elapsed  
Initiating NSE at 06:05  
Completed NSE at 06:05, 0.00s elapsed  
Initiating Ping Scan at 06:05  
Scanning s16-ies.tiktok.com (119.235.0.40) [4 ports]  
Completed Ping Scan at 06:05, 0.06s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 06:05  
Completed Parallel DNS resolution of 1 host. at 06:05, 0.04s elapsed  
Initiating SYN Stealth Scan at 06:05  
Scanning s16-ies.tiktok.com (119.235.0.40) [1000 ports]  
Discovered open port 443/tcp on 119.235.0.40  
Discovered open port 80/tcp on 119.235.0.40  
Increasing send delay for 119.235.0.40 from 0 to 5 due to 11 out of 14 dropped probes since last increase.  
Increasing send delay for 119.235.0.40 from 5 to 10 due to 11 out of 11 dropped probes since last increase.  
Completed SYN Stealth Scan at 06:06, 69.23s elapsed (1000 total ports)  
Initiating Service scan at 06:06  
Scanning 2 services on s16-ies.tiktok.com (119.235.0.40)  
Completed Service scan at 06:06, 12.19s elapsed (2 services on 1 host)  
Initiating OS detection (try #1) against s16-ies.tiktok.com (119.235.0.40)  
Retrying OS detection (try #2) against s16-ies.tiktok.com (119.235.0.40)  
Initiating Traceroute at 06:06  
Completed Traceroute at 06:06, 3.01s elapsed  
Initiating Parallel DNS resolution of 2 hosts. at 06:06  
Completed Parallel DNS resolution of 2 hosts. at 06:06, 0.00s elapsed

Scan Tools Profile Help

Target: s16-ies.tiktok.com Profile: Intense scan

Command: nmap -T4 -A -v s16-ies.tiktok.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

login.tiktok  
s16-ies.tiktok

Completed Traceroute at 06:06, 3.01s elapsed  
Initiating Parallel DNS resolution of 2 hosts. at 06:06  
Completed Parallel DNS resolution of 2 hosts. at 06:06, 0.00s elapsed  
NSE: Script scanning 119.235.0.48.  
Initiating NSE at 06:06  
Completed NSE at 06:07, 15.99s elapsed  
Initiating NSE at 06:07  
Completed NSE at 06:07, 0.32s elapsed  
Initiating NSE at 06:07  
Completed NSE at 06:07, 0.00s elapsed  
Nmap scan report for s16-ies.tiktok.com (119.235.0.40)  
Host is up (0.029s latency).  
Other addresses for s16-ies.tiktok.com (not scanned): 119.235.0.41  
rDNS record for 119.235.0.40: a119-235-0-40.deploy.akamaitechnologies.com  
Not shown: 998 filtered ports

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	AkamaiGhost (Akamai's HTTP Acceleration/Mirror service)
		http-server-header:	nginx
		http-title:	Site doesn't have a title (application/octet-stream).
443/tcp	open	ssl/http	AkamaiGhost (Akamai's HTTP Acceleration/Mirror service)
		http-server-header:	nginx
		ssl-cert: Subject: commonName=tiktok.com	
		Subject Alternative Name: DNS=tiktok.com	
		Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US	
		Public Key type: rsa	
		Public Key bits: 2048	
		Signature Algorithm: sha256WithRSAEncryption	
		Not valid before: 2019-11-14T00:00:00	
		Not valid after: 2022-01-12T12:00:00	
		MDS: 6042 e736 dd95 7460 a018 bb3e 309f f719	

Filter Hosts

[data/a.txt...]

1/2

Target: s16-ies.tiktok.com Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v s16-ies.tiktok.com

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans

OS Host

login.tiktok

s16-ies.tiktok

| Issuer: Name=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US  
| Public Key type: rsa  
| Public Key bits: 2048  
| Signature Algorithm: sha256WithRSAEncryption  
| Not valid before: 2019-11-14T00:00:00  
| Not valid after: 2022-01-12T12:00:00  
| MD5: 6642 e736 dd95 7460 aa10 bb3e 309f f719  
| SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5  
| ssl-date: TLS randomness does not represent time  
| lls-alpn:  
| http/1.1  
| tls-nextprotoneg:  
| http/1.1  
| http/1.0  
Warning: OScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: WAP|general purpose|router|phone  
Running (JUST GUESSTING): Linux 2.4.X|2.6.X|3.X (92%), MikroTik RouterOS 6.X (92%), Nokia Symbian OS (85%)  
OS CPE: cpe:/o:linux:linux\_kernel:2.4.20 cpe:/o:linux:linux\_kernel:2.6 cpe:/o:linux:linux\_kernel:3.2.0 cpe:/o:mikrotik:ruteros:6.15 cpe:/o:linux:linux\_kernel:4.4 cpe:/o:nokia:symbian\_os  
Aggressive OS guesses: Tomato 1.27 - 1.28 (Linux 2.4.20) (92%), Linux 2.6.18 - 2.6.22 (92%), Linux 3.2.0 (92%), MikroTik RouterOS 6.15 (Linux 3.3.5) (92%), Linux 4.4 (87%), Linux 2.6.18 (86%), Linux 2.6.31 - 2.6.32 (86%), Linux 2.6.28 (85%), Nokia E70 or N86 mobile phone (Symbian OS) (85%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 6 hops

TRACEROUTE (using port 443/tcp)  
HOP RTT ADDRESS  
1 2.97 ms homerouter.cpe (192.168.8.1)  
2 ... 5  
6 27.88 ms 110.235.0.40 denbyz.akamaittechnologies.com (110.235.0.40)

Filter Hosts

```
Applications Places Zenmap Thu Oct 22 6:11:58 AM •
Scan Tools Profile Help
Target: s16-ies.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v s16-ies.tiktok.com
Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans Details
OS Host login.tiktok
4 s16-ies.tiktok
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|general purpose|router|phone
Running (JUST GUESSING): Linux 2.4.X|2.6.X|3.X (92%), MikroTik RouterOS 6.X (92%), Nokia Symbian OS (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3.2.0 cpe:/o:mikrotik:routertos:6.15 cpe:/o:linux:linux_kernel:4.4 cpe:/o:nokia:symbian_os
Aggressive OS guesses: Tomato 1.27 - 1.28 (Linux 2.4.20) (92%), Linux 2.6.18 - 2.6.22 (92%), Linux 3.2.0 (92%), MikroTik RouterOS 6.15 (Linux 3.3.5) (92%), Linux 4.4 (87%), Linux 2.6.18 (86%), Linux 2.6.31 - 2.6.32 (86%), Linux 2.6.28 (85%), Nokia E70 or N86 mobile phone (Symbian OS) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 6 hops

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 2.97 ms homerouter.cpe (192.168.8.1)
2 ... 5
6 27.88 ms al19-235-0-40.deploy.akamaitechnologies.com (119.235.0.40)

NSE: Script Post-scanning.
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 106.35 seconds
Raw packets sent: 2157 (97.640KB) | Rcvd: 35 (2.814KB)
```

## 17.service.tiktok.com

```
Applications ▾ Places ▾ Zenmap ▾ Sat Oct 24 1:29:02 AM • Zenmap
Scan Tools Profile Help
Target: service.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v service.tiktok.com
Hosts Services OS Host Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v service.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-24 01:19 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:19
Completed NSE at 01:19, 0.00s elapsed
Initiating NSE at 01:19
Completed NSE at 01:19, 0.00s elapsed
Initiating NSE at 01:19
Completed NSE at 01:19, 0.00s elapsed
Initiating Ping Scan at 01:19
Scanning service.tiktok.com [209.127.230.15] [4 ports]
Completed Ping Scan at 01:19, 0.31s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:19
Completed Parallel DNS resolution of 1 host. at 01:19, 0.67s elapsed
Initiating SYN Stealth Scan at 01:19
Scanning service.tiktok.com [209.127.230.15] [1000 ports]
SYN Stealth Scan Timing: About 45.05% done; ETC: 01:20 (0:00:38 remaining)
Increasing send delay for 209.127.230.15 from 0 to 5 due to 11 out of 23 dropped probes since last increase.
Completed SYN Stealth Scan at 01:21, 91.13s elapsed (1000 total ports)
Initiating Service scan at 01:21
Initiating OS detection (try #1) against service.tiktok.com (209.127.230.15)
Initiating Traceroute at 01:21
Completed Traceroute at 01:21, 9.22s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 01:21
Completed Parallel DNS resolution of 2 hosts. at 01:21, 0.00s elapsed
NSE: Script scanning 209.127.230.15.
Initiating NSE at 01:21
Completed NSE at 01:21, 0.00s elapsed
Initiating NSE at 01:21
Completed NSE at 01:21, 0.00s elapsed
Filter Hosts
[root@kali: /usr/lib/zenmap/Java-1.8-0... [-/data/a.txt - Sublime Text (UNRE... Zenmap
1/2
```

```
Applications ▾ Places ▾ Zenmap ▾ Sat Oct 24 1:29:12 AM • Zenmap
Scan Tools Profile Help
Target: service.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v service.tiktok.com
Hosts Services OS Host Filter Hosts
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v service.tiktok.com
Completed NSE at 01:21, 0.00s elapsed
Nmap scan report for service.tiktok.com (209.127.230.15)
Host is up (0.24s latency).
rDNS record for 209.127.230.15: s01.bc.larksuite.com
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    closed http
443/tcp   closed https
1935/tcp  closed rtmp
Too many fingerprints match this host to give specific OS details
Network Distance: 23 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  2.76 ms   homerouter.cpe (192.168.8.1)
2  ... 22
23 227.28 ms s01.bc.larksuite.com (209.127.230.15)

NSE: Script Post-scanning.
Initiating NSE at 01:21
Completed NSE at 01:21, 0.00s elapsed
Initiating NSE at 01:21
Completed NSE at 01:21, 0.00s elapsed
Initiating NSE at 01:21
Completed NSE at 01:21, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 107.35 seconds
Raw packets sent: 3136 (140.240KB) | Rcvd: 27 (1.112KB)
Filter Hosts
[root@kali: /usr/lib/zenmap/Java-1.8-0... [-/data/a.txt - Sublime Text (UNRE... Zenmap
1/2
```

## 18.03.ptr1888.i.service.tiktok.com

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:06 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:06
Completed NSE at 06:06, 0.00s elapsed
Initiating NSE at 06:06
Completed NSE at 06:06, 0.00s elapsed
Initiating NSE at 06:06
Completed NSE at 06:06, 0.00s elapsed
Initiating Ping Scan at 06:06
Scanning 03.ptr1888.i.service.tiktok.com [167.89.111.205] [4 ports]
Completed Ping Scan at 06:06, 0.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:06
Completed Parallel DNS resolution of 1 host. at 06:06, 0.74s elapsed
Initiating SYN Stealth Scan at 06:06
Scanning 03.ptr1888.i.service.tiktok.com [167.89.111.205] [1000 ports]
SYN Stealth Scan Timing: About 12.50% done; ETC: 06:10 (0:03:37 remaining)
SYN Stealth Scan Timing: About 24.50% done; ETC: 06:10 (0:03:11 remaining)
SYN Stealth Scan Timing: About 36.05% done; ETC: 06:10 (0:02:43 remaining)
SYN Stealth Scan Timing: About 48.50% done; ETC: 06:10 (0:02:10 remaining)
SYN Stealth Scan Timing: About 60.05% done; ETC: 06:10 (0:01:41 remaining)
SYN Stealth Scan Timing: About 72.50% done; ETC: 06:10 (0:01:09 remaining)
SYN Stealth Scan Timing: About 84.50% done; ETC: 06:10 (0:00:39 remaining)
Completed SYN Stealth Scan at 06:10, 252.85s elapsed (1000 total ports)
Initiating Service scan at 06:10
Initiating OS detection (try #1) against 03.ptr1888.i.service.tiktok.com [167.89.111.205]
Retrying OS detection (try #2) against 03.ptr1888.i.service.tiktok.com [167.89.111.205]
Initiating Traceroute at 06:11
Completed Traceroute at 06:11, 3.05s elapsed
Initiating Parallel DNS resolution of 10 hosts. at 06:11

```

```
Initiating OS detection (try #1) against 03.ptr1888.i.service.tiktok.com [167.89.111.205]
Retrying OS detection (try #2) against 03.ptr1888.i.service.tiktok.com [167.89.111.205]
Initiating Traceroute at 06:11
Completed Traceroute at 06:11, 3.05s elapsed
Initiating Parallel DNS resolution of 10 hosts. at 06:11
Completed Parallel DNS resolution of 10 hosts. at 06:11, 13.00s elapsed
NSE: Script scanning 167.89.111.205.
Initiating NSE at 06:11
Completed NSE at 06:11, 0.01s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Nmap scan report for 03.ptr1888.i.service.tiktok.com [167.89.111.205]
Host is up (0.25s latency).
All 1000 scanned ports on 03.ptr1888.i.service.tiktok.com [167.89.111.205] are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 13 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.21 ms homerouter.cpe (192.168.8.1)
2 ...
3 154.84 ms 10.12.90.85
4 30.48 ms 10.12.83.25
5 30.44 ms 10.12.2.162
6 24.55 ms 103.87.125.97
7 25.19 ms 103.87.124.209
8 141.62 ms 103.87.124.146
9 137.42 ms 213.242.115.81

```

The screenshot shows the Zenmap interface with the following details:

- Target:** o3.ptr1888.i.service.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v o3.ptr1888.i.service.tiktok.com
- Hosts Services** tab selected.
- OS Host** section shows media.tiktok as the target host.
- Network Distance:** 13 hops
- Traceroute (using proto 1/icmp):**

HOP	RTT	ADDRESS
1	2.21 ms	homerouter.cpe (192.168.8.1)
2	...	
3	154.84 ms	10.12.90.85
4	30.48 ms	10.12.83.25
5	30.44 ms	10.12.2.162
6	24.55 ms	103.87.125.97
7	25.19 ms	103.87.124.209
8	141.62 ms	103.87.124.146
9	137.42 ms	213.242.115.81
10	...	
11	226.81 ms	4.16.72.70
12	...	
13	226.84 ms	o3.ptr1888.i.service.tiktok.com (167.89.111.205)
- NSE:** Script Post-scanning.  
Initiating NSE at 06:11  
Completed NSE at 06:11, 0.00s elapsed  
Initiating NSE at 06:11  
Completed NSE at 06:11, 0.00s elapsed  
Initiating NSE at 06:11  
Completed NSE at 06:11, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap
- OS and Service detection performed.** Please report any incorrect results at <https://nmap.org/submit/>.
- Nmap done:** 1 IP address (1 host up) scanned in 289.51 seconds
- Raw packets sent:** 2072 (94.634KB) | **Rcvd:** 35 (3.034KB)

**19.017.ptr1147.service.tiktok.com**

```
Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 6:14:59 AM ▾ 60 %  
Zenmap  
Scan Tools Profile Help  
Target: o17.ptr1147.service.tiktok.com ▾ Profile: Intense scan ▾ Scan Cancel  
Command: nmap -T4 -A -v o17.ptr1147.service.tiktok.com  
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans ▾ Details  
OS Host meteor.tiktok.com  
o17.ptr1147.service.tiktok.com  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:07 +0530  
NSE: Loaded 151 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating NSE at 06:07  
Completed NSE at 06:07, 0.00s elapsed  
Initiating NSE at 06:07  
Completed NSE at 06:07, 0.00s elapsed  
Initiating NSE at 06:07  
Completed NSE at 06:07, 0.00s elapsed  
Initiating Ping Scan at 06:07  
Scanning o17.ptr1147.service.tiktok.com [149.72.239.242] [4 ports]  
Completed Ping Scan at 06:07, 0.27s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 06:07  
Completed Parallel DNS resolution of 1 host. at 06:07, 0.60s elapsed  
Initiating SYN Stealth Scan at 06:07  
Scanning o17.ptr1147.service.tiktok.com [149.72.239.242] [1000 ports]  
SYN Stealth Scan Timing: About 13.00% done; ETC: 06:11 (0:03:27 remaining)  
SYN Stealth Scan Timing: About 26.50% done; ETC: 06:10 (0:02:49 remaining)  
SYN Stealth Scan Timing: About 39.50% done; ETC: 06:10 (0:02:19 remaining)  
SYN Stealth Scan Timing: About 52.55% done; ETC: 06:10 (0:01:49 remaining)  
SYN Stealth Scan Timing: About 66.00% done; ETC: 06:10 (0:01:18 remaining)  
SYN Stealth Scan Timing: About 79.10% done; ETC: 06:10 (0:00:48 remaining)  
Completed SYN Stealth Scan at 06:10, 229.13s elapsed (1000 total ports)  
Initiating Service scan at 06:10  
Initiating OS detection (try #1) against o17.ptr1147.service.tiktok.com [149.72.239.242]  
Retrying OS detection (try #2) against o17.ptr1147.service.tiktok.com [149.72.239.242]  
Initiating Traceroute at 06:11  
Completed Traceroute at 06:11, 4.06s elapsed  
Initiating Parallel DNS resolution of 10 hosts. at 06:11  
Completed Parallel DNS resolution of 10 hosts. at 06:11, 13.00s elapsed  
Filter Hosts
```

The screenshot shows the Zenmap interface with the following details:

- Target:** o17.ptr1147.service.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v o17.ptr1147.service.tiktok.com
- Hosts Services** tab selected.
- OS Host** section:
  - meteortik (Status: Up)
  - o17.ptr114 (Status: Up)
- Nmap Output** tab selected, displaying the following output:

```
nmap -T4 -A -v o17.ptr1147.service.tiktok.com
Completed Traceroute at 06:11, 4.06s elapsed
Initiating Parallel DNS resolution of 10 hosts. at 06:11
Completed Parallel DNS resolution of 10 hosts. at 06:11, 13.00s elapsed
NSE: Script scanning 149.72.239.242.
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Nmap scan report for o17.ptr1147.service.tiktok.com (149.72.239.242)
Host is up (0.23s latency).
All 1000 scanned ports on o17.ptr1147.service.tiktok.com (149.72.239.242) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 13 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.26 ms homerouter.cpe (192.168.8.1)
2 ...
3 26.52 ms 10.12.90.85
4 26.25 ms 10.12.83.25
5 35.40 ms 10.12.2.162
6 35.32 ms 103.87.125.97
7 35.83 ms 103.87.124.209
8 152.04 ms 103.87.124.146
9 151.55 ms 213.242.115.81
10 ...
11 237.35 ms SENDGRID-IN.earl.Washington12.Level3.net (4.16.72.70)
12 ...
```
- Scans** tab is also visible.

```
Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 6:15:07 AM • Zenmap
Scan Tools Profile Help
Target: o17.ptr1147.service.tiktok.com ▾ Profile: Intense scan ▾ Scan Cancel
Command: nmap -T4 -A -v o17.ptr1147.service.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans ▾ Details
OS Host Network Distance: 13 hops
meteortik
o17.ptr1147
TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.26 ms homeroouter.cpe (192.168.8.1)
2 ...
3 26.52 ms 10.12.90.85
4 26.25 ms 10.12.83.25
5 35.40 ms 10.12.2.162
6 35.32 ms 103.87.125.87
7 35.83 ms 103.87.124.209
8 152.04 ms 103.87.124.146
9 151.55 ms 213.242.115.81
10 ...
11 237.35 ms SENDGRID-IN.earl.Washington12.Level3.net (4.16.72.70)
12 ...
13 233.83 ms o17.ptr1147.service.tiktok.com (149.72.239.242)

NSE: Script Post-scanning.
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Read data files from: /usr/bin/.../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 265.25 seconds
Raw packets sent: 2080 (94.858KB) | Rcvd: 42 (2.622KB)
```

## 20.o13.ptr2902.service.tiktok.com

The screenshot shows the Zenmap interface with the target set to `o13.ptr2902.service.tiktok.com`. The command entered is `nmap -T4 -A -v o13.ptr2902.service.tiktok.com`. The output window displays the Nmap 7.80 scan results, starting at 06:07 on Oct 22, 2020. It shows the host `o13.ptr2902.service.tiktok.com` (IP `149.72.180.219`) with OS fingerprinting and script scanning. The scan includes SYN Stealth Scan, Traceroute, and parallel DNS resolution. The output concludes with a note about too many fingerprints matching the host.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:07 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Initiating NSE at 06:07
Completed NSE at 06:07, 0.00s elapsed
Initiating Ping Scan at 06:07
Scanning o13.ptr2902.service.tiktok.com (149.72.180.219) [4 ports]
Completed Ping Scan at 06:07, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:07
Completed Parallel DNS resolution of 1 host. at 06:07, 0.16s elapsed
Initiating SYN Stealth Scan at 06:07
Scanning o13.ptr2902.service.tiktok.com (149.72.180.219) [1000 ports]
SYN Stealth Scan Timing: About 13.00% done; ETC: 06:11 (0:03:27 remaining)
SYN Stealth Scan Timing: About 26.00% done; ETC: 06:11 (0:02:54 remaining)
SYN Stealth Scan Timing: About 38.95% done; ETC: 06:11 (0:02:23 remaining)
SYN Stealth Scan Timing: About 52.00% done; ETC: 06:11 (0:01:52 remaining)
SYN Stealth Scan Timing: About 65.00% done; ETC: 06:11 (0:01:21 remaining)
SYN Stealth Scan Timing: About 78.00% done; ETC: 06:11 (0:00:51 remaining)
Completed SYN Stealth Scan at 06:11, 233.81s elapsed (1000 total ports)
Initiating Service scan at 06:11
Initiating OS detection (try #1) against o13.ptr2902.service.tiktok.com (149.72.180.219)
Retrying OS detection (try #2) against o13.ptr2902.service.tiktok.com (149.72.180.219)
Initiating Traceroute at 06:11
Completed Traceroute at 06:11, 3.05s elapsed
Initiating Parallel DNS resolution of 10 hosts. at 06:11
Completed Parallel DNS resolution of 10 hosts. at 06:11, 13.00s elapsed
NSE: Script scanning 149.72.180.219.
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Nmap scan report for o13.ptr2902.service.tiktok.com (149.72.180.219)
Host is up (0.23s latency).
All 1000 scanned ports on o13.ptr2902.service.tiktok.com (149.72.180.219) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 13 hops
TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1  2.06 ms   homerouter.cpe (192.168.8.1)
2 ...
3  27.62 ms  10.12.90.85
4  26.77 ms  10.12.83.25
5  27.38 ms  10.12.2.162
6  27.19 ms  103.87.125.97
7  27.18 ms  103.87.124.81
8  136.06 ms 103.87.124.38
9  156.21 ms  213.242.115.81
10 ...
11 223.67 ms SENDGRID-IN.ear1.Washington12.Level3.net (4.16.72.70)
```

The screenshot shows the Zenmap interface with the target set to `o13.ptr2902.service.tiktok.com`. The command entered is `nmap -T4 -A -v o13.ptr2902.service.tiktok.com`. The output window displays the Nmap 7.80 scan results, starting at 06:11 on Oct 22, 2020. It shows the host `o13.ptr2902.service.tiktok.com` (IP `149.72.180.219`) with OS fingerprinting and script scanning. The scan includes SYN Stealth Scan, Traceroute, and parallel DNS resolution. The output concludes with a note about too many fingerprints matching the host.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:11 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script scanning 149.72.180.219.
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Nmap scan report for o13.ptr2902.service.tiktok.com (149.72.180.219)
Host is up (0.23s latency).
All 1000 scanned ports on o13.ptr2902.service.tiktok.com (149.72.180.219) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 13 hops
TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1  2.06 ms   homerouter.cpe (192.168.8.1)
2 ...
3  27.62 ms  10.12.90.85
4  26.77 ms  10.12.83.25
5  27.38 ms  10.12.2.162
6  27.19 ms  103.87.125.97
7  27.18 ms  103.87.124.81
8  136.06 ms 103.87.124.38
9  156.21 ms  213.242.115.81
10 ...
11 223.67 ms SENDGRID-IN.ear1.Washington12.Level3.net (4.16.72.70)
```

Target: o13.ptr2902.service.tiktok.com Profile: Intense scan

Command: nmap -T4 -A -v o13.ptr2902.service.tiktok.com

Hosts Services

OS Host mg.tiktok.com

mg.tiktok.com Network Distance: 13 hops

TRACEROUTE (using proto 1/icmp)

HOP	RTT	ADDRESS
1	2.06 ms	homerouter.cpe (192.168.8.1)
2	...	
3	27.62 ms	10.12.90.85
4	26.77 ms	10.12.83.25
5	27.38 ms	10.12.2.162
6	27.19 ms	103.87.125.97
7	27.18 ms	103.87.124.81
8	136.06 ms	103.87.124.38
9	156.21 ms	213.242.115.81
10	...	
11	223.67 ms	SENDGRID-IN.ear1.Washington12.Level3.net (4.16.72.70)
12	...	
13	220.04 ms	o13.ptr2902.service.tiktok.com (149.72.180.219)

NSE: Script Post-scanning.

Initiating NSE at 06:11

Completed NSE at 06:11, 0.00s elapsed

Initiating NSE at 06:11

Completed NSE at 06:11, 0.00s elapsed

Initiating NSE at 06:11

Completed NSE at 06:11, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

05 and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 262.34 seconds

Raw packets sent: 2071 (94.456KB) | Rcvd: 65 (4.210KB)

**21.019.ptr4023.service.tiktok.com**

The screenshot shows the Zenmap interface with the following details:

- Target:** o19.ptr4023.service.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v o19.ptr4023.service.tiktok.com
- Hosts Services** tab selected.
- OS Host** section:
  - musician.t (o19.ptr4023.service.tiktok.com)
- Nmap Output** tab selected, displaying the scan results:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:09 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:09
Completed NSE at 06:09, 0.00s elapsed
Initiating NSE at 06:09
Completed NSE at 06:09, 0.00s elapsed
Initiating NSE at 06:09
Completed NSE at 06:09, 0.00s elapsed
Initiating NSE at 06:09
Completed NSE at 06:09, 0.00s elapsed
Initiating Ping Scan at 06:09
Scanning o19.ptr4023.service.tiktok.com [149.72.241.86] [4 ports]
Completed Ping Scan at 06:09, 1.77s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:09
Completed Parallel DNS resolution of 1 host. at 06:09, 0.17s elapsed
Initiating SYN Stealth Scan at 06:09
Scanning o19.ptr4023.service.tiktok.com [149.72.241.86] [1000 ports]
SYN Stealth Scan Timing: About 12.55% done; ETC: 06:13 (0:03:36 remaining)
SYN Stealth Scan Timing: About 26.00% done; ETC: 06:13 (0:02:54 remaining)
SYN Stealth Scan Timing: About 38.75% done; ETC: 06:13 (0:02:24 remaining)
SYN Stealth Scan Timing: About 51.55% done; ETC: 06:13 (0:01:54 remaining)
SYN Stealth Scan Timing: About 64.90% done; ETC: 06:13 (0:01:22 remaining)
SYN Stealth Scan Timing: About 77.50% done; ETC: 06:13 (0:00:53 remaining)
Completed SYN Stealth Scan at 06:13, 233.48s elapsed (1000 total ports)
Initiating Service scan at 06:13
Initiating OS detection (try #1) against o19.ptr4023.service.tiktok.com [149.72.241.86]
Retrying OS detection (try #2) against o19.ptr4023.service.tiktok.com [149.72.241.86]
Initiating Traceroute at 06:13
Completed Traceroute at 06:13, 3.27s elapsed
Initiating Parallel DNS resolution of 3 hosts. at 06:13
Completed Parallel DNS resolution of 3 hosts. at 06:13, 3.53s elapsed
```

The screenshot shows the Zenmap interface with the following details:

- Target:** o19.ptr4023.service.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v o19.ptr4023.service.tiktok.com
- Hosts Services** tab selected.
- OS Host** section:
  - musician.b (IP: 192.168.8.1)
  - o19.ptr40. (IP: 149.72.241.86)
- Nmap Output** tab selected.
  - Completed traceroute at 06:13, 3.27s elapsed.
  - Initiating Parallel DNS resolution of 3 hosts. at 06:13
  - Completed Parallel DNS resolution of 3 hosts. at 06:13, 3.53s elapsed.
  - NSE:** Script scanning 149.72.241.86.
  - Initiating NSE at 06:13
  - Completed NSE at 06:13, 0.00s elapsed
  - Initiating NSE at 06:13
  - Completed NSE at 06:13, 0.00s elapsed
  - Initiating NSE at 06:13
  - Completed NSE at 06:13, 0.00s elapsed
  - Nmap scan report for o19.ptr4023.service.tiktok.com (149.72.241.86)
  - Host is up (0.23s latency).
  - All 1000 scanned ports on o19.ptr4023.service.tiktok.com (149.72.241.86) are filtered
  - Too many fingerprints match this host to give specific OS details
  - Network Distance:** 13 hops
  - TRACEROUTE (using proto 1/icmp)**

HOP	RTT	ADDRESS
1	2.13 ms	homeroouter.cpe (192.168.8.1)
2	... 10	
11	238.38 ms	SENDGRID-IN.earl.Washington12.Level3.net (4.16.72.70)
12	...	
13	218.98 ms	o19.ptr4023.service.tiktok.com (149.72.241.86)
  - NSE:** Script Post-scanning.
  - Initiating NSE at 06:13
  - Completed NSE at 06:13, 0.00s elapsed
  - Initiating NSE at 06:13
  - Completed NSE at 06:13, 0.00s elapsed
  - Initiating NSE at 06:13
- Filter Hosts** button.
- Scan** and **Cancel** buttons.

```
Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 6:16:02 AM ⓘ
Zenmap

Scan Tools Profile Help
Target: o19.ptr4023.service.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v o19.ptr4023.service.tiktok.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans ⓘ Details
OS Host
musician.t
o19.ptr4023.service.tiktok.com
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Nmap scan report for o19.ptr4023.service.tiktok.com (149.72.241.86)
Host is up (0.23s latency).
All 1000 scanned ports on o19.ptr4023.service.tiktok.com (149.72.241.86) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 13 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.13 ms homerouter.cpe (192.168.8.1)
2 ... 10
11 238.38 ms SENDGRID-IN.earl.Washington12.Level3.net (4.16.72.70)
12 ...
13 218.98 ms o19.ptr4023.service.tiktok.com (149.72.241.86)

NSE: Script Post-scanning.
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Initiating NSE at 06:13
Completed NSE at 06:13, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 260.36 seconds
Raw packets sent: 2092 (95.234KB) | Rcvd: 76 (4.752KB)
```

## 22.o20.ptr6684.service.tiktok.com

The screenshot shows the Zenmap interface with the target set to "o20.ptr6684.service.tiktok.com". The "Profile" is set to "Intense scan". The "Command" field contains "nmap -T4 -A -v o20.ptr6684.service.tiktok.com". The "Nmap Output" tab is selected, displaying the full nmap scan log. The log shows the scan starting at 06:10 on Oct 22, 2020, and completing at 06:14. It details various NSE scripts, SYN Stealth Scan timing, OS detection, and traceroute results. The output ends with a note about network distance and a traceroute table.

```
nmap -T4 -A -v o20.ptr6684.service.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:10 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:10
Completed NSE at 06:10, 0.00s elapsed
Initiating NSE at 06:10
Completed NSE at 06:10, 0.00s elapsed
Initiating NSE at 06:10
Completed NSE at 06:10, 0.00s elapsed
Initiating Ping Scan at 06:10
Scanning o20.ptr6684.service.tiktok.com (149.72.53.129) [4 ports]
Completed Ping Scan at 06:10, 1.81s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:10
Completed Parallel DNS resolution of 1 host. at 06:10, 0.18s elapsed
Initiating SYN Stealth Scan at 06:10
Scanning o20.ptr6684.service.tiktok.com (149.72.53.129) [1000 ports]
SYN Stealth Scan Timing: About 12.50% done; ETC: 06:14 (0:03:37 remaining)
SYN Stealth Scan Timing: About 24.50% done; ETC: 06:14 (0:03:11 remaining)
SYN Stealth Scan Timing: About 36.10% done; ETC: 06:14 (0:02:43 remaining)
SYN Stealth Scan Timing: About 48.15% done; ETC: 06:14 (0:02:11 remaining)
SYN Stealth Scan Timing: About 60.50% done; ETC: 06:14 (0:01:39 remaining)
SYN Stealth Scan Timing: About 72.50% done; ETC: 06:14 (0:01:09 remaining)
SYN Stealth Scan Timing: About 84.50% done; ETC: 06:14 (0:00:39 remaining)
Completed SYN Stealth Scan at 06:14, 251.75s elapsed (1000 total ports)
Initiating Service scan at 06:14
Initiating OS detection (try #1) against o20.ptr6684.service.tiktok.com (149.72.53.129)
Retrying OS detection (try #2) against o20.ptr6684.service.tiktok.com (149.72.53.129)
Initiating Traceroute at 06:14
Completed Traceroute at 06:14, 6.04s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 06:14

```

This screenshot shows the same Zenmap session but with a different portion of the nmap output displayed. It continues from the previous log, showing the completion of the traceroute, the start of service scanning, and the beginning of OS detection. The output then shifts to show the Nmap scan report for the host, noting that all 1000 scanned ports are filtered and too many fingerprints match. It concludes with a detailed traceroute table.

```
Nmap scan report for o20.ptr6684.service.tiktok.com (149.72.53.129)
Host is up (0.25s latency).
All 1000 scanned ports on o20.ptr6684.service.tiktok.com (149.72.53.129) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 20 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1  2.10 ms   homeroouter.cpe (192.168.8.1)
2 ...
3  44.21 ms   10.12.90.85
4 ...
10 167.69 ms  if-ae-2-2.tcore2.mlv-mumbai.as6453.net (180.87.38.2)
11 181.09 ms  if-ae-12-2.tcore1.l78-london.as6453.net (180.87.39.21)
12 170.65 ms  if-ae-17-2.tcore1.ldn-london.as6453.net (80.231.130.130)
13 283.15 ms  80.231.62.2
14 ...
15 290.99 ms  ae5.cs3.lga5.us.eth.zayo.com (64.125.29.126)
16 ...
17 312.22 ms  ae8.er1.ord2.us.zip.zayo.com (64.125.31.173)
```

```

Applications Scan Tools Profile Help
Target: o20.ptr6684.service.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v o20.ptr6684.service.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host o20.ptr6684.service.tiktok.com
TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.10 ms homerouter.cpe (192.168.8.1)
2 ...
3 44.21 ms 10.12.90.85
4 ...
10 167.69 ms if-ae-2-2.tcore2.mlv-mumbai.as6453.net (180.87.38.2)
11 181.09 ms if-ae-12-2.tcore1.l78-london.as6453.net (180.87.39.21)
12 170.65 ms if-ae-17-2.tcore1.ldn-london.as6453.net (80.231.130.130)
13 283.15 ms 80.231.62.2
14 ...
15 290.99 ms ae5.cs3.lg45.us.eth.zayo.com (64.125.29.126)
16 ...
17 312.22 ms ae8.er1.ord2.us.zip.zayo.com (64.125.31.173)
18 ...
19 ...
20 248.95 ms o20.ptr6684.service.tiktok.com (149.72.53.129)

NSE: Script Post-scanning.
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 291.42 seconds
Raw packets sent: 2100 (95.608KB) | Rcvd: 108 (7.744KB)

```

## 23.o18.ptr8067.service.tiktok.com

```

Applications Scan Tools Profile Help
Target: o18.ptr8067.service.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v o18.ptr8067.service.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host o18.ptr8067.notification
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:11 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating Ping Scan at 06:11
Scanning o18.ptr8067.service.tiktok.com (149.72.218.44) [4 ports]
Completed Ping Scan at 06:11, 1.77s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:11
Completed Parallel DNS resolution of 1 host. at 06:11, 1.17s elapsed
Initiating SYN Stealth Scan at 06:11
Scanning o18.ptr8067.service.tiktok.com (149.72.218.44) [1000 ports]
SYN Stealth Scan Timing: About 13.00% done; ETC: 06:15 (0:03:27 remaining)
SYN Stealth Scan Timing: About 25.90% done; ETC: 06:15 (0:02:55 remaining)
SYN Stealth Scan Timing: About 38.50% done; ETC: 06:15 (0:02:25 remaining)
SYN Stealth Scan Timing: About 51.50% done; ETC: 06:15 (0:01:54 remaining)
SYN Stealth Scan Timing: About 63.60% done; ETC: 06:15 (0:01:26 remaining)
SYN Stealth Scan Timing: About 76.95% done; ETC: 06:15 (0:00:54 remaining)
Completed SYN Stealth Scan at 06:15, 235.71s elapsed (1000 total ports)
Initiating Service scan at 06:15
Initiating OS detection (try #1) against o18.ptr8067.service.tiktok.com (149.72.218.44)
Retrying OS detection (try #2) against o18.ptr8067.service.tiktok.com (149.72.218.44)
Initiating Traceroute at 06:15
Completed Traceroute at 06:15, 4.05s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 06:15
Completed Parallel DNS resolution of 7 hosts. at 06:15, 13.01s elapsed

```

The screenshot shows the Zenmap interface with the following details:

- Target:** o18.ptr8067.service.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v o18.ptr8067.service.tiktok.com
- Hosts Services** tab selected.
- OS Host notification** section shows "o18.ptr8067.service.tiktok.com" as a host.
- Nmap Output** tab content:
  - nmap -T4 -A -v o18.ptr8067.service.tiktok.com
  - Retrying OS detection (try #2) against o18.ptr8067.service.tiktok.com (149.72.218.44)
  - Initiating Traceroute at 06:15
  - Completed Traceroute at 06:15, 4.05s elapsed
  - Initiating parallel DNS resolution of 7 hosts. at 06:15
  - Completed Parallel DNS resolution of 7 hosts. at 06:15, 13.01s elapsed
  - NSE: Script scanning 149.72.218.44.
  - Initiating NSE at 06:15
  - Completed NSE at 06:15, 0.00s elapsed
  - Initiating NSE at 06:15
  - Completed NSE at 06:15, 0.00s elapsed
  - Initiating NSE at 06:15
  - Completed NSE at 06:15, 0.00s elapsed
  - Initiating NSE at 06:15
  - Completed NSE at 06:15, 0.00s elapsed
  - Initiating NSE at 06:15
  - Completed NSE at 06:15, 0.00s elapsed
  - Nmap scan report for o18.ptr8067.service.tiktok.com (149.72.218.44)
  - Host is up (0.23s latency).
  - All 1000 scanned ports on o18.ptr8067.service.tiktok.com (149.72.218.44) are filtered
  - Too many fingerprints match this host to give specific OS details
  - Network Distance: 13 hops
- TRACEROUTE (using proto 1/icmp)**

HOP	RTT	ADDRESS
1	2.11 ms	homerouter.cpe (192.168.8.1)
2	.	
3	21.78 ms	10.12.90.85
4	16.74 ms	10.12.83.25
5	21.79 ms	10.12.2.162
6	21.79 ms	103.87.125.97
7	21.79 ms	103.87.124.81
8	...	12
13	218.60 ms	o18.ptr8067.service.tiktok.com (149.72.218.44)

The screenshot shows the Zenmap interface with the following details:

- Target:** o18.ptr8067.service.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v o18.ptr8067.service.tiktok.com
- Hosts Services** tab selected.
- OS Host** table:
  - notification (o18.ptr8067.service.tiktok.com) is up (0.23s latency).
  - o18.ptr8067.service.tiktok.com is up (149.72.218.44). All 1000 scanned ports are filtered. Too many fingerprints match this host to give specific OS details. Network Distance: 13 hops.
- Nmap Output** section:
  - Traceroute (using proto 1/icmp):

HOP	RTT	ADDRESS
1	2.11 ms	homerouter.cpe (192.168.8.1)
2	...	
3	21.78 ms	10.12.90.85
4	16.74 ms	10.12.83.25
5	21.79 ms	10.12.2.162
6	21.79 ms	103.87.125.97
7	21.79 ms	103.87.124.81
8	...	12
13	218.60 ms	o18.ptr8067.service.tiktok.com (149.72.218.44)
  - NSE: Script Post-scanning.  
Initiating NSE at 06:15  
Completed NSE at 06:15, 0.00s elapsed  
Initiating NSE at 06:15  
Completed NSE at 06:15, 0.00s elapsed  
Initiating NSE at 06:15  
Completed NSE at 06:15, 0.00s elapsed  
Read data files from: /usr/bin/.../share/nmap
  - OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
  - Nmap done: 1 IP address (1 host up) scanned in 273.49 seconds
  - Raw packets sent: 2084 (95.010KB) | Rcvd: 117 (8.112KB)

## 24.o16.ptr9230.service.tiktok.com

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:11 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating Ping Scan at 06:11
Completed Ping Scan at 06:11, 1.78s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:11
Completed Parallel DNS resolution of 1 host. at 06:11, 1.42s elapsed
Initiating SYN Stealth Scan at 06:11
Scanning o16.ptr9230.service.tiktok.com (149.72.42.48) [4 ports]
Completed Ping Scan at 06:11, 1.78s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:11
Completed Parallel DNS resolution of 1 host. at 06:11, 1.42s elapsed
Initiating SYN Stealth Scan at 06:11
Scanning o16.ptr9230.service.tiktok.com (149.72.42.48) [1000 ports]
SYN Stealth Scan Timing: About 12.05% done; ETC: 06:15 (0:03:46 remaining)
SYN Stealth Scan Timing: About 24.50% done; ETC: 06:15 (0:03:08 remaining)
SYN Stealth Scan Timing: About 36.50% done; ETC: 06:15 (0:02:38 remaining)
SYN Stealth Scan Timing: About 48.50% done; ETC: 06:15 (0:02:08 remaining)
SYN Stealth Scan Timing: About 60.50% done; ETC: 06:15 (0:01:39 remaining)
SYN Stealth Scan Timing: About 72.15% done; ETC: 06:15 (0:01:10 remaining)
SYN Stealth Scan Timing: About 84.20% done; ETC: 06:15 (0:00:40 remaining)
Completed SYN Stealth Scan at 06:15, 251.79s elapsed (1000 total ports)
Initiating Service scan at 06:15
Initiating OS detection (try #1) against o16.ptr9230.service.tiktok.com (149.72.42.48)
Retrying OS detection (try #2) against o16.ptr9230.service.tiktok.com (149.72.42.48)
Initiating Traceroute at 06:15
Completed Traceroute at 06:15, 3.23s elapsed
Initiating Parallel DNS resolution of 13 hosts. at 06:15

```

```
Initiating Traceroute at 06:15
Completed Traceroute at 06:15, 3.23s elapsed
Initiating Parallel DNS resolution of 13 hosts. at 06:15
Completed Parallel DNS resolution of 13 hosts. at 06:16, 13.00s elapsed
NSE: Script scanning 149.72.42.48.
Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
Nmap scan report for o16.ptr9230.service.tiktok.com (149.72.42.48)
Host is up (0.26s latency).
All 1000 scanned ports on o16.ptr9230.service.tiktok.com (149.72.42.48) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 20 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.63 ms homerouter.cpe (192.168.8.1)
2 ...
3 43.13 ms 10.12.90.85
4 37.93 ms 10.12.83.25
5 38.02 ms 10.12.2.162
6 39.12 ms 103.87.125.97
7 41.40 ms 103.87.124.209
8 38.46 ms 103.87.124.130
9 59.49 ms ix-xe-1-0-3-0.tcore1.mlv-mumbai.as6453.net (180.87.38.182)
10 187.22 ms if-ae-2-2.tcore2.mlv-mumbai.as6453.net (180.87.38.2)
11 ...


```

```

Scan Tools Profile Help
Target: o16.ptr9230.service.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v o16.ptr9230.service.tiktok.com

Hosts Services
OS Host
v16-web.ti
o16.ptr923

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v o16.ptr9230.service.tiktok.com
1 2.63 ms homerouter.cpe (192.168.8.1)
2 ...
3 43.13 ms 10.12.90.85
4 37.93 ms 10.12.83.25
5 38.02 ms 10.12.2.162
6 39.12 ms 103.87.125.97
7 41.40 ms 103.87.124.209
8 38.46 ms 103.87.124.130
9 59.49 ms ix-xe-1-0-3-0.tcore1.mlv-mumbai.as6453.net (180.87.38.182)
10 187.22 ms if-ae-2-2.tcore2.mlv-mumbai.as6453.net (180.87.38.2)
11 ...
12 175.18 ms if-ae-17-2.tcore1.ldn-london.as6453.net (80.231.130.130)
13 286.48 ms 80.231.62.2
14 ...
15 279.69 ms ae8.er1.ord2.us.zip.zayo.com (64.125.31.173)
16 ...
17 271.31 ms o16.ptr9230.service.tiktok.com (149.72.42.48)

NSE: Script Post-scanning.
Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 290.95 seconds
Raw packets sent: 2090 (95.628KB) | Rcvd: 141 (10.482KB)

```

## 25.spotlight.tiktok.com

```

Scan Tools Profile Help
Target: spotlight.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v spotlight.tiktok.com

Hosts Services
OS Host
spotlight.ti
promotion

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v spotlight.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:11 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating Ping Scan at 06:11
Scanning spotlight.tiktok.com [103.136.220.180] [4 ports]
Completed Ping Scan at 06:11, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:11
Completed Parallel DNS resolution of 1 host. at 06:11, 13.00s elapsed
Initiating SYN Stealth Scan at 06:11
Scanning spotlight.tiktok.com [103.136.220.180] [1000 ports]
Discovered open port 80/tcp on 103.136.220.180
Increasing send delay for 103.136.220.180 from 0 to 5 due to 11 out of 15 dropped probes since last increase.
SYN Stealth Scan Timing: About 19.37% done; ETC: 06:14 (0:02:09 remaining)
Increasing send delay for 103.136.220.180 from 5 to 10 due to 11 out of 12 dropped probes since last increase.
SYN Stealth Scan Timing: About 25.13% done; ETC: 06:15 (0:03:02 remaining)
SYN Stealth Scan Timing: About 37.56% done; ETC: 06:15 (0:02:32 remaining)
SYN Stealth Scan Timing: About 48.30% done; ETC: 06:16 (0:02:10 remaining)
SYN Stealth Scan Timing: About 64.10% done; ETC: 06:15 (0:01:25 remaining)
Completed SYN Stealth Scan at 06:15, 194.29s elapsed (1000 total ports)
Initiating Service scan at 06:15
Scanning 1 service on spotlight.tiktok.com [103.136.220.180]
Completed Service scan at 06:15, 6.15s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against spotlight.tiktok.com [103.136.220.180]
Retriving OS detection (trv #2) against spotlight.tiktok.com [103.136.220.180]

```

The screenshot shows the Zenmap application window. The top bar displays the title 'Zenmap' and the system status 'Thu Oct 22 6:17:41 AM'. The main interface includes a 'Scan Tools Profile Help' menu, a 'Target' dropdown set to 'spotlight.tiktok.com', a 'Profile' dropdown set to 'Intense scan', and 'Scan' and 'Cancel' buttons. Below the menu is a 'Command' field containing 'nmap -T4 -A -v spotlight.tiktok.com'. The main pane has tabs for 'Hosts', 'Services', 'Nmap Output', 'Ports / Hosts', 'Topology', 'Host Details', and 'Scans'. The 'Nmap Output' tab is selected, displaying the following scan results:

```
nmap -T4 -A -v spotlight.tiktok.com
Completed Service scan at 06:15, 6.15s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against spotlight.tiktok.com (103.136.220.180)
Retrying OS detection (try #2) against spotlight.tiktok.com (103.136.220.180)
Initiating Traceroute at 06:15
Completed Traceroute at 06:15, 6.06s elapsed
Initiating Parallel DNS resolution of 6 hosts. at 06:15
Completed Parallel DNS resolution of 6 hosts. at 06:15, 13.01s elapsed
NSE: Script scanning 103.136.220.180.
Initiating NSE at 06:15
Completed NSE at 06:15, 18.26s elapsed
Initiating NSE at 06:15
Completed NSE at 06:16, 2.00s elapsed
Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
Nmap scan report for spotlight.tiktok.com [103.136.220.180]
Host is up (0.001s latency).
Other addresses for spotlight.tiktok.com (not scanned): 103.136.220.181 103.136.221.164 103.136.221.168
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|3.X (87%)
OS CPE: cpe:/o:linux:linux_kernel:4.9 cpe:/o:linux:linux_kernel:3.18
Aggressive OS guesses: Linux 4.9 (87%), Linux 3.18 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 17 hops
```

At the bottom, there are buttons for 'Filter Hosts' and 'HOP RTT ADDRESS'.

The screenshot shows the Zenmap interface with the following details:

- Target:** spotlight.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v spotlight.tiktok.com
- OS Host:** spotlight.tiktok.com (promotion)
- Network Distance:** 17 hops
- TRACEROUTE (using port 443/tcp):**

HOP	RTT	ADDRESS
1	1.97 ms	homerouter.cpe (192.168.8.1)
2		
3	30.72 ms	10.12.90.85
4	..	
5	25.28 ms	10.12.2.162
6	25.58 ms	103.87.125.97
7	31.13 ms	103.87.124.81
8	... 16	
17	105.46 ms	103.136.220.180

- NSE:** Script Post-scanning.  
Initiating NSE at 06:16  
Completed NSE at 06:16, 0.00s elapsed  
Initiating NSE at 06:16  
Completed NSE at 06:16, 0.00s elapsed  
Initiating NSE at 06:16  
Completed NSE at 06:16, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap
- OS and Service detection performed.** Please report any incorrect results at <https://nmap.org/submit/>.
- Nmap done:** 1 IP address (1 host up) scanned in 258.99 seconds
- Raw packets sent:** 3275 (148.632KB) | Rcvd: 137 (8.946KB)

## 26.suggestions.tiktok.com

The screenshot shows the Zenmap interface with the following details:

- Target:** suggestions.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v suggestions.tiktok.com
- Hosts Services** tab is selected.
- OS Host** section lists three hosts:
  - login.tiktok (IP: 119.235.0.41)
  - s16-ies.tiktok (IP: 119.235.0.41)
  - suggestions.tiktok (IP: 119.235.0.41)
- Nmap Output** tab is selected, displaying the scan results:
  - Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:12 +0530
  - NSE: Loaded 151 scripts for scanning.
  - NSE Script Pre-scanning.
  - Initiating NSE at 06:12
  - Completed NSE at 06:12, 0.00s elapsed
  - Initiating NSE at 06:12
  - Completed NSE at 06:12, 0.00s elapsed
  - Initiating NSE at 06:12
  - Completed NSE at 06:12, 0.00s elapsed
  - Initiating NSE at 06:12
  - Completed NSE at 06:12, 0.00s elapsed
  - Initiating Ping Scan at 06:12
  - Scanning suggestions.tiktok.com (119.235.0.41) [4 ports]
  - Completed Ping Scan at 06:12, 0.07s elapsed (1 total hosts)
  - Initiating Parallel DNS resolution of 1 host. at 06:12
  - Completed Parallel DNS resolution of 1 host. at 06:12, 0.02s elapsed
  - Initiating SYN Stealth Scan at 06:12
  - Scanning suggestions.tiktok.com (119.235.0.41) [1000 ports]
  - Discovered open port 443/tcp on 119.235.0.41
  - Discovered open port 80/tcp on 119.235.0.41
  - Increasing send delay for 119.235.0.41 from 0 to 5 due to 11 out of 20 dropped probes since last increase.
  - Increasing send delay for 119.235.0.41 from 5 to 10 due to 11 out of 15 dropped probes since last increase.
  - Completed SYN Stealth Scan at 06:14, 104.12s elapsed (1000 total ports)
  - Initiating Service scan at 06:14
  - Scanning 2 services on suggestions.tiktok.com (119.235.0.41)
  - Completed Service scan at 06:14, 13.20s elapsed (2 services on 1 host)
  - Initiating OS detection (try #1) against suggestions.tiktok.com (119.235.0.41)
  - Retrying OS detection (try #2) against suggestions.tiktok.com (119.235.0.41)
  - Initiating Traceroute at 06:14
  - Completed Traceroute at 06:14, 3.03s elapsed
  - Initiating Parallel DNS resolution of 5 hosts. at 06:14
  - Completed Parallel DNS resolution of 5 hosts. at 06:14, 13.00s elapsed
- Filter Hosts** button is visible.
- Scan** and **Cancel** buttons are visible.

```
Applications Places Zenmap Thu Oct 22 6:18:17 AM • Zenmap
Scan Tools Profile Help Target: suggestions.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v suggestions.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host login.tiktok
  Initiating Parallel DNS resolution of 5 hosts. at 06:14
  Completed Parallel DNS resolution of 5 hosts. at 06:14, 13.00s elapsed
  NSE Script scanning [19.235.0.41].
    Initiating NSE at 06:14
    Completed NSE at 06:15, 18.42s elapsed
    Initiating NSE at 06:15
    Completed NSE at 06:15, 2.06s elapsed
    Initiating NSE at 06:15
    Completed NSE at 06:15, 0.00s elapsed
    Nmap scan report for suggestions.tiktok.com [19.235.0.41]
    Host is up (0.025s latency).
    Other addresses for suggestions.tiktok.com (not scanned): [19.235.0.40]
    rDNS record for [19.235.0.41]: [a]19-235-0-41.deploy.akamaitechnologies.com
    Not shown: 998 filter ports
PORT STATE SERVICE VERSION
80/tcp open http AkamaiGhost (Akamai's HTTP Acceleration/Mirror service)
443/tcp open ssl/http AkamaiGhost (Akamai's HTTP Acceleration/Mirror service)
| http-methods:
|_ Supported Methods: HEAD POST
| http-title: 404 Not Found
| ssl-cert: Subject: commonName=suggestions.tiktok.com
| Subject Alternative Name: DNS:suggestions.tiktok.com
| Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigitCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-11-14T00:00:00
| Not valid after: 2022-01-12T12:00:00
| MD5: 6042 e736 dd791 7460 aa10 bb3e 309f f719
| SHA-1: 5af9 8d9f 77e1 af1f xd4f 183r a017 02f5 88rf a4e5
Filter Hosts
```

```
Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 6:18:24 AM ▾
Zenmap
Scan Tools Profile Help
Target: suggestions.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v suggestions.tiktok.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
login.tiktok
s16-ies.tiktok
suggestor

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.0 (93%), Linux 3.11 - 4.1 (93%), Linux 4.4 (93%), Linux 2.6.31 (92%), Linux 3.10 (92%), Linux 3.10 - 3.16 (92%), Linux 2.6.32 (92%), Linux 2.6.32 - 2.6.33 (92%), Linux 2.6.32 - 2.6.35 (92%), Linux 2.6.32 or 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 5.306 days (since Fri Oct 16 22:54:54 2020)
Network Distance: 6 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 3.31 ms homerouter.cpe (192.168.8.1)
2 ...
3 33.36 ms 10.12.90.85
4 20.59 ms 10.12.83.25
5 20.87 ms 10.12.2.162
6 20.02 ms a119-235-0-41.deploy.akamaitechnologies.com (119.235.0.41)

NSE: Script Post-scanning.
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 161.96 seconds
Raw packets sent: 3200 (144.632KB) | Rcvd: 77 (4.874KB)
```

**27.support.tiktok.com**

The screenshot shows the Zenmap interface with the following details:

- Target:** support.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v support.tiktok.com
- Hosts Services** tab is selected.
- Nmap Output** tab is selected.
- Scans** tab is visible.
- OS Host** tab is visible.
- Ports / Hosts** tab is visible.
- Topology** tab is visible.
- Host Details** tab is visible.
- Scan Cancel** buttons are visible.

The main pane displays the Nmap scan results for support.tiktok.com (119.235.0.40):

```
nmap -T4 -A -v support.tiktok.com
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:18
Completed NSE at 06:18, 0.00s elapsed
Initiating NSE at 06:18
Completed NSE at 06:18, 0.00s elapsed
Initiating NSE at 06:18
Completed NSE at 06:18, 0.00s elapsed
Initiating NSE at 06:18
Completed NSE at 06:18, 0.00s elapsed
Initiating Ping Scan at 06:18
Scanning support.tiktok.com (119.235.0.40) [4 ports]
Completed Ping Scan at 06:18, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:18
Completed Parallel DNS resolution of 1 host. at 06:18, 1.75s elapsed
Initiating SYN Stealth Scan at 06:18
Scanning support.tiktok.com (119.235.0.40) [1000 ports]
Discovered open port 80/tcp on 119.235.0.40
Increasing send delay for 119.235.0.40 from 0 to 5 due to 11 out of 16 dropped probes since last increase.
Completed SYN Stealth Scan at 06:19, 37.62s elapsed (1000 total ports)
Initiating Service scan at 06:19
Scanning 1 service on support.tiktok.com (119.235.0.40)
Completed Service scan at 06:19, 6.06s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against support.tiktok.com (119.235.0.40)
Retrying OS detection (try #2) against support.tiktok.com (119.235.0.40)
Initiating Traceroute at 06:19
Completed Traceroute at 06:19, 3.02s elapsed
Initiating Parallel DNS resolution of 5 hosts. at 06:19
Completed Parallel DNS resolution of 5 hosts. at 06:19, 13.00s elapsed
NSE: Script scanning 119.235.0.40.
Initiating NSE at 06:19
```

```

Scan Tools Profile Help
Target: support.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v support.tiktok.com

Hosts Services
OS Host
m.tiktok.co
service.tiktok

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v support.tiktok.com

Device type: general purpose/WAP/router
Running (JUST GUESSING): Linux 4.X|3.X|2.4.X|2.6.X (93%), MikroTik RouterOS 6.X (85%)
OS CPE: cpe:/o:linux:linux kernel:4.4 cpe:/o:linux:linux_kernel:3.13 cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6 cpe:/o:mikrotik:routers:6.15
Aggressive OS guesses: Linux 4.4 (93%), Linux 4.0 (87%), Linux 3.13 (87%), Linux 3.11 - 4.1 (87%), Linux 3.8 (87%), Linux 3.10 (86%), Linux 3.10 - 3.16 (86%), Linux 3.10 - 3.12 (86%), Linux 3.16 (86%), Linux 4.9 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 6 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 2.84 ms homerouter.cpe (192.168.8.1)
2 ...
3 46.33 ms 10.12.90.85
4 32.72 ms 10.12.83.25
5 34.70 ms 10.12.2.162
6 30.14 ms a119-235-0-40.deploy.akamaitechnologies.com (119.235.0.40)

NSE: Script Post-scanning.
Initiating NSE at 06:19
Completed NSE at 06:19, 0.00s elapsed
Initiating NSE at 06:19
Completed NSE at 06:19, 0.00s elapsed
Initiating NSE at 06:19
Completed NSE at 06:19, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 81.22 seconds
Raw packets sent: 2127 (96.320KB) | Rcvd: 73 (5.790KB)

Filter Hosts

```

## 28.t.tiktok.com

```

Scan Tools Profile Help
Target: t.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v t.tiktok.com

Hosts Services
OS Host
media.tiktok
t.tiktok.com
o3.ptr1888

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v t.tiktok.com

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:14 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:14
Completed NSE at 06:14, 0.00s elapsed
Initiating NSE at 06:14
Completed NSE at 06:14, 0.00s elapsed
Initiating NSE at 06:14
Completed NSE at 06:14, 0.00s elapsed
Initiating NSE at 06:14
Completed NSE at 06:14, 0.00s elapsed
Initiating Ping Scan at 06:14
Scanning t.tiktok.com (119.235.0.41) [4 ports]
Completed Ping Scan at 06:14, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:14
Completed Parallel DNS resolution of 1 host. at 06:14, 3.76s elapsed
Initiating SYN Stealth Scan at 06:14
Scanning t.tiktok.com (119.235.0.41) [1000 ports]
Discovered open port 443/tcp on 119.235.0.41
Discovered open port 80/tcp on 119.235.0.41
Completed SYN Stealth Scan at 06:15, 23.78s elapsed (1000 total ports)
Initiating Service scan at 06:15
Scanning 2 services on t.tiktok.com (119.235.0.41)
Completed Service scan at 06:15, 13.22s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against t.tiktok.com (119.235.0.41)
Retrying OS detection (try #2) against t.tiktok.com (119.235.0.41)
Initiating Traceroute at 06:15
Completed Traceroute at 06:15, 3.02s elapsed
Initiating Parallel DNS resolution of 4 hosts. at 06:15
Completed Parallel DNS resolution of 4 hosts. at 06:15, 13.00s elapsed
NSE: Script scanning 119.235.0.41.
Initiating NSE at 06:15

Filter Hosts

```

Targets: t.tiktok.com

Profile: Intense scan

Command: nmap -T4 -A -v t.tiktok.com

OS Host

media.tiktok.com

t.tiktok.com

o3.ptr1888

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans

OS Host

media.tiktok.com

t.tiktok.com

o3.ptr1888

| ssl-cert: Subject: commonName=tiktok.com  
| Subject Alternative Name: DNS:\*.tiktok.com, DNS:tiktok.com  
| Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US  
| Public Key type: rsa  
| Public Key bits: 2048  
| Signature Algorithm: sha256WithRSAEncryption  
| Not valid before: 2019-11-14T00:00:00  
| Not valid after: 2022-01-12T12:00:00  
| MD5: 6042 e736 dd95 7460 aa10 bb3e 309f f719  
| SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5  
| ssl-date: TLS randomness does not represent time  
| tls-alpn:  
| http/1.1  
| tls-nextprotoneg:  
| http/1.1  
| http/1.0  
| http/1.0  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: WAP|general purpose|router|phone  
Running (JUST GUESSING): Linux 2.4.X|2.6.X|3.X (92%), MikroTik RouterOS 6.X (92%), Nokia Symbian OS (85%)  
OS CPE: cpe:/o:linux:linux\_kernel:2.4.20 cpe:/o:linux:linux\_kernel:2.6 cpe:/o:linux:linux\_kernel:3.2.0 cpe:/o:mikrotik:routeros:6.15 cpe:/o:linux:linux\_kernel:4.4 cpe:/o:nokia:symbian\_os  
Aggressive OS guesses: Tomato 1.27 - 1.28 (Linux 2.4.20) (92%), Linux 2.6.18 - 2.6.22 (92%), Linux 3.2.0 (92%), MikroTik RouterOS 6.15 (Linux 3.3.5) (92%), Linux 4.4 (87%), Linux 2.6.18 (86%), Linux 2.6.31 - 2.6.32 (86%), Linux 2.6.28 (85%), Nokia E70 or N86 mobile phone (Symbian OS) (85%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 6 hops

TRACEROUTE (using port 443/tcp)

HOP RTT ADDRESS

1 6.95 ms homerouter.cpe (192.168.8.1)

**29.test-business-useast2a.tiktok.com**

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 6:22:50 AM ▾

Zenmap

Scan Tools Profile Help

Target: test-business-useast2a.tiktok.com ▾ Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v test-business-useast2a.tiktok.com

Hosts Services

OS	Host
meteor.tik	test-business-useast2a.tiktok.com
o17.ptr114	

Nmap Output Ports / Hosts Topology Host Details Scans

```
nmap -T4 -A -v test-business-useast2a.tiktok.com
Initiating Parallel DNS resolution of 11 hosts. at 06:21
Completed Parallel DNS resolution of 11 hosts. at 06:21, 13.01s elapsed
NSE: Script scanning 147.160.184.56
Initiating NSE at 06:21
Completed NSE at 06:21, 10.78s elapsed
Initiating NSE at 06:21
Completed NSE at 06:21, 2.29s elapsed
Initiating NSE at 06:21
Completed NSE at 06:21, 0.00s elapsed
Nmap scan report for test-business-useast2a.tiktok.com (147.160.184.56)
Host is up (0.26s latency).
Other addresses for test-business-useast2a.tiktok.com (not scanned): 147.160.184.40
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx
|_http-title: 502 Bad Gateway
443/tcp   open  ssl/http nginx
|_http-title: 502 Bad Gateway
|_ssl-cert: Subject: commonName=*.tiktok.com
|_Subject Alternative Name: DNS:*.tiktok.com, DNS:tiktok.com
|_Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US
|_Public Key type: rsa
|_Public Key bits: 2048
|_Signature Algorithm: sha256WithRSAEncryption
|_Not valid before: 2020-07-06T00:00:00
|_Not valid after: 2022-07-07T12:00:00
|MDS: e593 3d6a 7ca4 da4f 432b a997 7bbf 24c4
|_SHA-1: d4e0 fcbl 815c 8020 1471 cb7a 564b 19a8 9e6a 3d1f
|_ssl-date: TLS randomness does not represent time
|_tls-alpn:
|_http/1.1
|_tls-nextprotoneg:
|_http/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 16 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1  2.62 ms  homeroouter.cpe (192.168.8.1)
2 ...
3  29.09 ms  10.12.90.85
4  31.47 ms  10.12.83.25
5  29.36 ms  10.12.2.162
6  31.25 ms  103.87.125.97
7  27.50 ms  103.87.124.81
8  148.29 ms 103.87.124.146
9  147.56 ms 213.242.115.81
10 214.23 ms ae-2-3610.edge5.Washington12.Level3.net [4.69.220.26]
11 ...

```

Filter Hosts

[data/a.txt - Su... [Zenmap] 1/2

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 6:22:55 AM ▾

Zenmap

Scan Tools Profile Help

Target: test-business-useast2a.tiktok.com ▾ Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v test-business-useast2a.tiktok.com

Hosts Services

OS	Host
meteor.tik	test-business-useast2a.tiktok.com
o17.ptr114	

Nmap Output Ports / Hosts Topology Host Details Scans

```
nmap -T4 -A -v test-business-useast2a.tiktok.com
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2020-07-06T00:00:00
Not valid after: 2022-07-07T12:00:00
MDS: e593 3d6a 7ca4 da4f 432b a997 7bbf 24c4
SHA-1: d4e0 fcbl 815c 8020 1471 cb7a 564b 19a8 9e6a 3d1f
ssl-date: TLS randomness does not represent time
tls-alpn:
http/1.1
tls-nextprotoneg:
http/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 16 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1  2.62 ms  homeroouter.cpe (192.168.8.1)
2 ...
3  29.09 ms  10.12.90.85
4  31.47 ms  10.12.83.25
5  29.36 ms  10.12.2.162
6  31.25 ms  103.87.125.97
7  27.50 ms  103.87.124.81
8  148.29 ms 103.87.124.146
9  147.56 ms 213.242.115.81
10 214.23 ms ae-2-3610.edge5.Washington12.Level3.net [4.69.220.26]
11 ...

```

Filter Hosts

[data/a.txt - Su... [Zenmap] 1/2

```
Applications Places Zenmap Thu Oct 22 6:22:57 AM • Zenmap
Scan Tools Profile Help Target: test-business-useast2a.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v test-business-useast2a.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host meteor.tik
  test-business
  o17.ptr114
  TRACEROUTE (using port 443/tcp)
  HOP RTT ADDRESS
  1 2.62 ms homerouter.cpe (192.168.8.1)
  2 ...
  3 29.09 ms 10.12.90.85
  4 31.47 ms 10.12.83.25
  5 29.36 ms 10.12.2.162
  6 31.25 ms 103.87.125.97
  7 27.50 ms 103.87.124.81
  8 148.29 ms 103.87.124.146
  9 147.50 ms 213.242.115.81
  10 214.23 ms ae-2-3610.edge5.Washington12.Level3.net (4.69.220.26)
  11 ... 12
  13 234.05 ms 172.17.9.78
  14 ... 15
  16 232.70 ms 147.160.184.56

NSE: Script Post-scanning.
Initiating NSE at 06:21
Completed NSE at 06:21, 0.00s elapsed
Initiating NSE at 06:21
Completed NSE at 06:21, 0.00s elapsed
Initiating NSE at 06:21
Completed NSE at 06:21, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 132.17 seconds
Raw packets sent: 2139 (98.544KB) | Rcvd: 73 (5.318KB)
```

30.tv.tiktok.com

The screenshot shows the Zenmap interface with the following details:

- Target:** tv.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v tv.tiktok.com
- Hosts Services** tab is selected.
- OS Host** section lists:
  - mg.tiktok.com (Host)
  - tv.tiktok.cc (Host)
  - o13.ptr29c (Host)
- Nmap Output** tab is selected, displaying the scan results:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:15 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Initiating Ping Scan at 06:15
Scanning tv.tiktok.com [104.75.84.56] (4 ports)
Completed Ping Scan at 06:15, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:15
Completed Parallel DNS resolution of 1 host. at 06:15, 0.04s elapsed
Initiating SYN Stealth Scan at 06:15
Scanning tv.tiktok.com [104.75.84.56] (1000 ports)
Discovered open port 443/tcp on [104.75.84.56]
Completed SYN Stealth Scan at 06:16, 23.86s elapsed (1000 total ports)
Initiating Service scan at 06:16
Scanning 1 service on tv.tiktok.com [104.75.84.56]
Completed Service scan at 06:16, 12.09s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against tv.tiktok.com ([104.75.84.56])
Retrying OS detection (try #2) against tv.tiktok.com ([104.75.84.56])
Initiating Traceroute at 06:16
Completed Traceroute at 06:16, 3.02s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 06:16
Completed Parallel DNS resolution of 9 hosts. at 06:16, 13.00s elapsed
NSE: Script scanning 104.75.84.56.
Initiating NSE at 06:16
Completed NSE at 06:16, 8.08s elapsed
```

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 6:23:16 AM ▾

Zenmap

Scan Tools Profile Help

Target: tv.tiktok.com ▾ Profile: Intense scan ▾ Scan Cancel

Command: nmap -T4 -A -v tv.tiktok.com

Hosts Services

OS Host

- mg.tiktok.c
- tv.tiktok.co
- o13.ptr290

Nmap Output Ports / Hosts Topology Host Details Scans

```
nmap -T4 -A -v tv.tiktok.com
Completed parallel DNS resolution of 3 hosts. at 00:10, 15.00s elapsed
NSE: Script scanning 104.75.84.56.
Initiating NSE at 06:16
Completed NSE at 06:16, 8.00s elapsed
Initiating NSE at 06:16
Completed NSE at 06:16, 0.63s elapsed
Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
Nmap scan report for tv.tiktok.com (104.75.84.56)
Host is up (0.032s latency).
Other addresses for tv.tiktok.com (not scanned): 104.75.84.63
rDNS record for 104.75.84.56: a104-75-84-56.deploy.static.akamaitechnologies.com
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
443/tcp    open  https   AkamaiGHost
| http-methods:
|_ Supported Methods: GET HEAD
| http-server-header:
|_ AkamaiGHost
| nginx
| http-title: 404 Not Found
| ssl-cert: Subject: commonName=*.tiktok.com
| Subject Alternative Name: DNS:*.tiktok.com, DNS:tiktok.com
| Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-11-14T00:00:00
| Not valid after: 2022-01-12T12:00:00
| MD5: 6042 e736 dd95 7460 aa10 bb3e 309f f719

```

Filter Hosts

[-/data/n.txt - Subli... [Zenmap] 1/2

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 6:23:20 AM ▾

Zenmap

Scan Tools Profile Help

Target: tv.tiktok.com ▾ Profile: Intense scan ▾ Scan Cancel

Command: nmap -T4 -A -v tv.tiktok.com

Hosts Services

OS Host

- mg.tiktok.c
- tv.tiktok.co
- o13.ptr290

Nmap Output Ports / Hosts Topology Host Details Scans

```
| not vuln after: 2022-01-12T12:00:00
| MD5: 6042 e736 dd95 7460 aa10 bb3e 309f f719
|_ SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service:
SF-Port443-TCP-V=7.80%F=10/22%T=time=5F900659%P=x86_64-pc-linux-gnu%R(SS
SF1_SessionReq,7,"x15\x03\x03\x01\x02\x02P");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|WAP|router
Running (JUST GUESSING): Linux 4.X|3.X|2.4.X|2.6.X (93%), MikroTik RouterOS 6.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3.13 cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6 cpe:-o:mikrotik:routertos:6.15
Aggressive OS guesses: Linux 4.4 (93%), Linux 4.0 (87%), Linux 3.13 (87%), Linux 3.11 - 4.1 (87%), Linux 3.8 (87%), Linux 3.10 (86%), Linux 3.10 - 3.16 (86%), Linux 3.10 - 3.12 (86%), Linux 3.16 (86%), Linux 4.9 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1  6.38 ms  homerouter.cpe (192.168.8.1)
2 ...
3  41.30 ms  10.12.98.85
4  39.28 ms  10.12.83.25
5  41.21 ms  10.12.2.162
6  41.20 ms  103.87.125.97
7  39.74 ms  103.87.124.81
8  39.34 ms  103.87.125.18
9  28.55 ms  222.165.175.74
10 28.31 ms a104-75-84-56.deploy.static.akamaitechnologies.com (104.75.84.56)
```

Filter Hosts

[-/data/n.txt - Subli... [Zenmap] 1/2

```

Thu Oct 22 6:23:22 AM • Zenmap
Scan Tools Profile Help
Target: tv.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v tv.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
tv.tiktok.com
Aggressive OS guesses: Linux 4.4 (93%), Linux 4.0 (87%), Linux 3.13 (87%), Linux 3.11 - 4.1 (87%), Linux 3.8 (87%), Linux 3.10 (86%), Linux 3.10 - 3.16 (86%), Linux 3.10 - 3.12 (86%), Linux 3.16 (86%), Linux 4.9 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 10 hops
TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 6.38 ms homerouter.cpe (192.168.8.1)
2 ...
3 41.30 ms 10.12.90.85
4 39.28 ms 10.12.83.25
5 41.21 ms 10.12.2.162
6 41.20 ms 103.87.125.97
7 39.74 ms 103.87.124.81
8 39.34 ms 103.87.125.18
9 28.55 ms 222.165.175.74
10 28.31 ms 104.75-84-56.deploy.static.akamaitechnologies.com (104.75.84.56)

NSE: Script Post-scanning.
Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 68.25 seconds
Raw packets sent: 3129 (141.956KB) | Rcvd: 66 (4.896KB)

```

## 31.v.tiktok.com

```

Thu Oct 22 6:23:36 AM • Zenmap
Scan Tools Profile Help
Target: v.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v v.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
v.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:16 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
NSE: Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
NSE: Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
NSE: Initiating NSE at 06:16
Completed NSE at 06:16, 0.00s elapsed
NSE: Initiating Ping Scan at 06:16
Scanning v.tiktok.com (103.136.221.168) [4 ports]
Completed Ping Scan at 06:16, 0.12s elapsed (1 total hosts)
NSE: Initiating Parallel DNS resolution of 1 host. at 06:16
Completed Parallel DNS resolution of 1 host. at 06:16, 13.01s elapsed
NSE: Initiating SYN Stealth Scan at 06:16
Scanning v.tiktok.com (103.136.221.168) [1000 ports]
NSE: Discovered open port 80/tcp on 103.136.221.168
NSE: Discovered open port 443/tcp on 103.136.221.168
NSE: Completed SYN Stealth Scan at 06:16, 18.64s elapsed (1000 total ports)
NSE: Initiating Service Scan at 06:16
Scanning 2 services on v.tiktok.com (103.136.221.168)
NSE: Completed Service scan at 06:16, 12.46s elapsed (2 services on 1 host)
NSE: Initiating OS detection (try #1) against v.tiktok.com (103.136.221.168)
NSE: Retrying OS detection (try #2) against v.tiktok.com (103.136.221.168)
NSE: Initiating Traceroute at 06:17
NSE: Completed Traceroute at 06:17, 3.06s elapsed
NSE: Initiating Parallel DNS resolution of 9 hosts. at 06:17
NSE: Completed Parallel DNS resolution of 9 hosts. at 06:17, 13.00s elapsed
NSE: Script scanning 103.136.221.168
NSE: Initiating NSE at 06:17

```

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 6:23:39 AM •

**Zenmap**

Scan Tools Profile Help

Target: v.tiktok.com ▾ Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -vv.v.tiktok.com

Hosts Services

OS Host

- musician.t**
- v.tiktok.co
- o19.ptr40:

Initiating Parallel DNS resolution of 9 hosts. at 06:17  
Completed Parallel DNS resolution of 9 hosts. at 06:17, 13.00s elapsed  
**NSE:** Script scanning 103.136.221.168.

Initiating NSE at 06:17  
Completed NSE at 06:17, 7.35s elapsed  
Initiating NSE at 06:17  
Completed NSE at 06:17, 0.66s elapsed  
Initiating NSE at 06:17  
Completed NSE at 06:17, 0.00s elapsed  
Nmap scan report for **v.tiktok.com** (103.136.221.168)  
Host is up (0.082s latency).  
Other addresses for **v.tiktok.com** (not scanned): 103.136.220.181 103.136.220.180 103.136.221.164  
Not shown: 998 filtered ports

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	nginx
http-title: 404 Not Found			
443/tcp	open	ssl/http	nginx
http-title: 404 Not Found			
ssl-cert: Subject: commonName=*			
snssdk.com			
Subject Alternative Name: DNS:*.snssdk.com, DNS:snssdk.com			
Issuer: commonName=Encryption Everywhere DV TLS CA - G1/organizationName=DigiCert Inc/countryName=US			
Public Key type: rsa			
Public Key bits: 2048			
Signature Algorithm: sha256WithRSAEncryption			
Not valid before: 2020-09-18T00:00:00			
Not valid after: 2021-09-19T12:00:00			
MD5: ff70 f6e3 a828 c2ad 0b49 7149 0984 6246			
_SHA-1: 8ffe e042 84bf b4de 2d3c a5b7 56df 3420 153a c2f9			
_ssl-date: TLS randomness does not represent time			
_tls-alpn:			

Filter Hosts

[-/data/s.txt - Sublime ...] [Zenmap] [Zenmap] [Zenmap] [Zenmap] [Zenmap] [Pictures] [Zenmap] [Zenmap] [Zenmap] [Zenmap] 1/2

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 6:23:44 AM •

**Zenmap**

Scan Tools Profile Help

Target: v.tiktok.com ▾ Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -vv.v.tiktok.com

Hosts Services

OS Host

- musician.t**
- v.tiktok.co
- o19.ptr40:

Public Key bits: 2048  
Signature Algorithm: sha256WithRSAEncryption  
Not valid before: 2020-09-18T00:00:00  
Not valid after: 2021-09-19T12:00:00  
MD5: ff70 f6e3 a828 c2ad 0b49 7149 0984 6246  
\_SHA-1: 8ffe e042 84bf b4de 2d3c a5b7 56df 3420 153a c2f9  
ssl-date: TLS randomness does not represent time  
tls-alpn:  
http/1.1  
tls-nextprotoneg:  
http/1.1  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running (JUST GUESSING): Linux 4.X (85%)  
OS CPE: cpe:/o:linux:linux\_kernel:4.9  
Aggressive OS guesses: Linux 4.9 (85%)  
No exact OS matches for host (test conditions non-ideal).  
Network Distance: 13 hops

TRACEROUTE (using port 80/tcp)

HOP	RTT	ADDRESS
1	1.65 ms	homerouter.cpe (192.168.8.1)
2	44.75 ms	10.12.90.85
3	41.82 ms	10.12.83.25
4	44.50 ms	10.12.2.162
6	30.80 ms	103.87.125.97
7	44.47 ms	103.87.124.81
8	89.27 ms	103.87.124.74
9	88.44 ms	138699.sgw.equinix.com (27.111.229.190)

Filter Hosts

[-/data/s.txt - Sublime ...] [Zenmap] 1/2

```

Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 6:23:46 AM •
Zenmap
Scan Tools Profile Help
Target: v.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v v.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host nmap -T4 -A -v v.tiktok.com
Aggressive OS guesses: Linux 4.9 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 1.65 ms homerouter.cpe (192.168.8.1)
2 ...
3 44.75 ms 10.12.90.85
4 41.82 ms 10.12.83.25
5 44.50 ms 10.12.2.162
6 30.80 ms 103.87.125.97
7 44.47 ms 103.87.124.81
8 89.27 ms 103.87.124.74
9 88.44 ms 138699.sgw.equinix.com (27.111.229.190)
10 ... 12
13 82.35 ms 103.136.221.168
NSE: Script Post-scanning.
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 88.77 seconds
Raw packets sent: 3123 (141.264KB) | Rcvd: 74 (7.280KB)

```

Filter Hosts

[-/data/a.txt - Sublime Text ... [Zenmap] 1/2

## 32.v16-web.tiktok.com

```

Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 6:24:01 AM •
Zenmap
Scan Tools Profile Help
Target: v16-web.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v v16-web.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host nmap -T4 -A -v o20.ptr6684.service.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:10 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:10
Completed NSE at 06:10, 0.00s elapsed
Initiating NSE at 06:10
Completed NSE at 06:10, 0.00s elapsed
Initiating NSE at 06:10
Completed NSE at 06:10, 0.00s elapsed
Initiating NSE at 06:10
Completed NSE at 06:10, 0.00s elapsed
Initiating Ping Scan at 06:10
Scanning o20.ptr6684.service.tiktok.com (149.72.53.129) [4 ports]
Completed Ping Scan at 06:10, 1.81s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:10
Completed Parallel DNS resolution of 1 host. at 06:10, 0.18s elapsed
Initiating SYN Stealth Scan at 06:10
Scanning o20.ptr6684.service.tiktok.com (149.72.53.129) [1000 ports]
SYN Stealth Scan Timing: About 12.50% done; ETC: 06:14 (0:03:37 remaining)
SYN Stealth Scan Timing: About 24.50% done; ETC: 06:14 (0:03:11 remaining)
SYN Stealth Scan Timing: About 36.10% done; ETC: 06:14 (0:02:43 remaining)
SYN Stealth Scan Timing: About 48.15% done; ETC: 06:14 (0:02:11 remaining)
SYN Stealth Scan Timing: About 60.50% done; ETC: 06:14 (0:01:39 remaining)
SYN Stealth Scan Timing: About 72.50% done; ETC: 06:14 (0:01:09 remaining)
SYN Stealth Scan Timing: About 84.50% done; ETC: 06:14 (0:00:39 remaining)
Completed SYN Stealth Scan at 06:14, 251.75s elapsed (1000 total ports)
Initiating Service scan at 06:14
Initiating OS detection (try #1) against o20.ptr6684.service.tiktok.com (149.72.53.129)
Retrying OS detection (try #2) against o20.ptr6684.service.tiktok.com (149.72.53.129)
Initiating Traceroute at 06:14
Completed Traceroute at 06:14, 6.04s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 06:14

```

Filter Hosts

[-/data/a.txt - Sublime Text ... [Zenmap] 1/2

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 6:24:07 AM •

**Zenmap**

Scan Tools Profile Help

Target: v16-web.tiktok.com ▾ Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v v16-web.tiktok.com

Hosts Services

OS Host

**o20.ptr668**

```

Initiating Traceroute at 06:14
Completed Traceroute at 06:14, 6.04s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 06:14
Completed Parallel DNS resolution of 9 hosts. at 06:15, 13.00s elapsed
NSE: Script scanning 149.72.53.129.
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Nmap scan report for o20.ptr6684.service.tiktok.com [149.72.53.129]
Host is up (0.25s latency).
All 1000 scanned ports on o20.ptr6684.service.tiktok.com [149.72.53.129] are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 20 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.10 ms homerouter.cpe (192.168.8.1)
2 ...
3 44.21 ms 10.12.90.85
4 ...
10 167.69 ms if-ae-2-2.tcore2.mlv-mumbai.as6453.net (180.87.38.2)
11 181.09 ms if-ae-12-2.tcore1.l78-london.as6453.net (180.87.39.21)
12 170.65 ms if-ae-17-2.tcore1.ldn-london.as6453.net (80.231.130.130)
13 283.15 ms 80.231.62.2
14 ...
15 290.99 ms ae5.cs3.lga5.us.eth.zayo.com (64.125.29.126)
16 ...

```

Filter Hosts

[-/data/s.txt - Sublime Text... ] [Zenmap] [Zenmap] [Zenmap] [Zenmap] [Pictures] [Zenmap] [Zenmap] [Zenmap] 1/2

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 6:24:11 AM •

**Zenmap**

Scan Tools Profile Help

Target: v16-web.tiktok.com ▾ Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v v16-web.tiktok.com

Hosts Services

OS Host

**o20.ptr668**

```

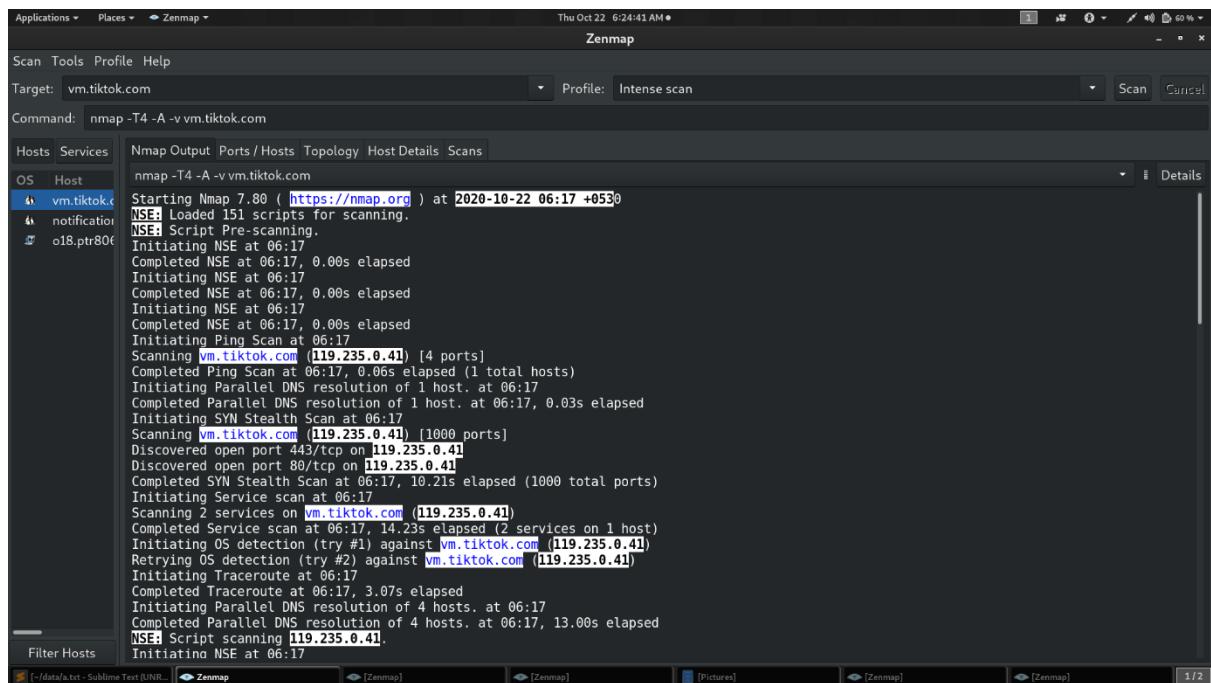
TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.10 ms homerouter.cpe (192.168.8.1)
2 ...
3 44.21 ms 10.12.90.85
4 ...
10 167.69 ms if-ae-2-2.tcore2.mlv-mumbai.as6453.net (180.87.38.2)
11 181.09 ms if-ae-12-2.tcore1.l78-london.as6453.net (180.87.39.21)
12 170.65 ms if-ae-17-2.tcore1.ldn-london.as6453.net (80.231.130.130)
13 283.15 ms 80.231.62.2
14 ...
15 290.99 ms ae5.cs3.lga5.us.eth.zayo.com (64.125.29.126)
16 ...
17 312.22 ms ae8.er1.ord2.us.zip.zayo.com (64.125.31.173)
18 ...
19 ...
20 248.95 ms o20.ptr6684.service.tiktok.com (149.72.53.129)

NSE: Script Post-scanning.
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Initiating NSE at 06:15
Completed NSE at 06:15, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 291.42 seconds
Raw packets sent: 2100 (95.608KB) | Rcvd: 108 (7.744KB)
```

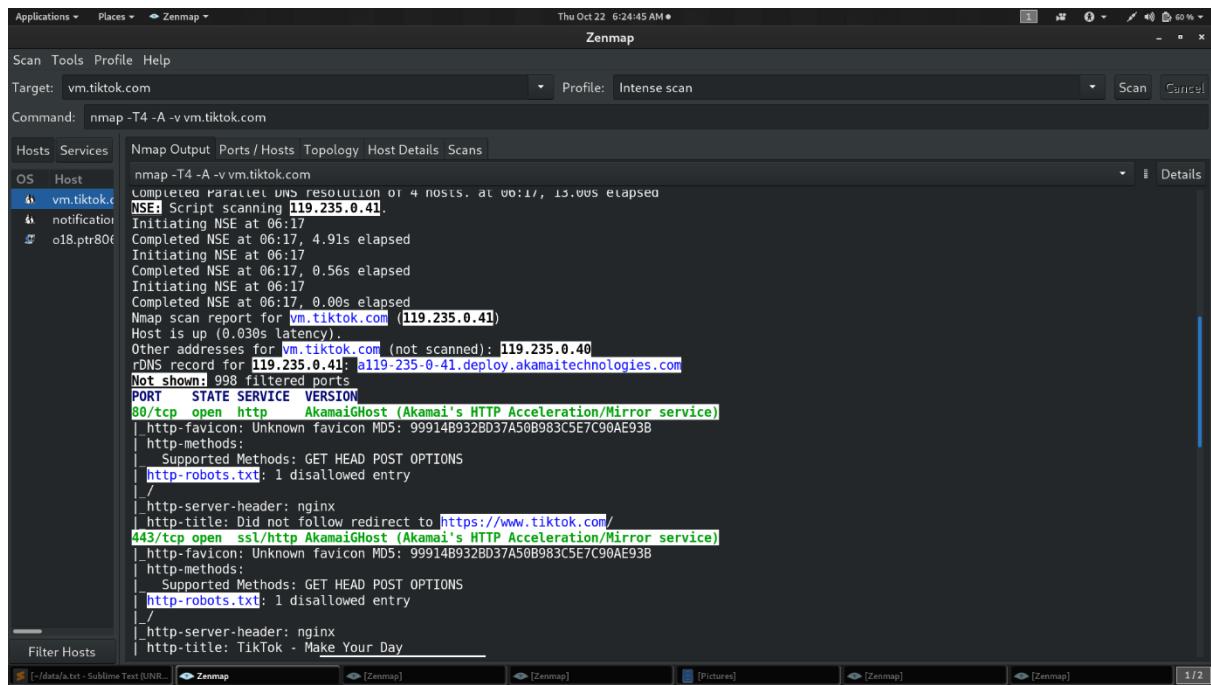
Filter Hosts

[-/data/s.txt - Sublime Text... ] [Zenmap] [Zenmap] [Zenmap] [Zenmap] [Pictures] [Zenmap] [Zenmap] [Zenmap] 1/2

## 33.vm.tiktok.com



```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:17 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating Ping Scan at 06:17
Scanning vm.tiktok.com [119.235.0.41] [4 ports]
Completed Ping Scan at 06:17, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:17
Completed Parallel DNS resolution of 1 host. at 06:17, 0.03s elapsed
Initiating SYN Stealth Scan at 06:17
Scanning vm.tiktok.com [119.235.0.41] [1000 ports]
Discovered open port 443/tcp on 119.235.0.41
Discovered open port 80/tcp on 119.235.0.41
Completed SYN Stealth Scan at 06:17, 10.21s elapsed (1000 total ports)
Initiating Service scan at 06:17
Scanning 2 services on vm.tiktok.com [119.235.0.41]
Completed Service scan at 06:17, 14.23s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against vm.tiktok.com [119.235.0.41]
Retrying OS detection (try #2) against vm.tiktok.com [119.235.0.41]
Initiating Traceroute at 06:17
Completed Traceroute at 06:17, 3.07s elapsed
Initiating Parallel DNS resolution of 4 hosts. at 06:17
Completed Parallel DNS resolution of 4 hosts. at 06:17, 13.00s elapsed
NSE: Script scanning 119.235.0.41.
Initiating NSE at 06:17
```



```
Completed parallel DNS resolution of 4 hosts. at 06:17, 15.00s elapsed
NSE: Script scanning 119.235.0.41.
Initiating NSE at 06:17
Completed NSE at 06:17, 4.91s elapsed
Initiating NSE at 06:17
Completed NSE at 06:17, 0.56s elapsed
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Nmap scan report for vm.tiktok.com [119.235.0.40]
Host is up (0.030s latency).
Other addresses for vm.tiktok.com (not scanned): 119.235.0.40
rDNS record for 119.235.0.41: a119-235-0-41.deploy.akamaitechnologies.com
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-favicon: Unknown favicon MD5: 99914B932BD37A50B983C5E7C90AE93B
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: nginx
|_http-title: Did not follow redirect to https://www.tiktok.com/
443/tcp   open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-favicon: Unknown favicon MD5: 99914B932BD37A50B983C5E7C90AE93B
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: nginx
|_http-title: TikTok - Make Your Day
```

Applications ▾ Places ▾ Zenmap ▾

The Oct 22 6:24:51 AM •

**Zenmap**

Scan Tools Profile Help

Target: vm.tiktok.com ▾ Profile: Intense scan ▾ Scan Cancel

Command: nmap -T4 -A -v vm.tiktok.com

Hosts Services

OS Host

- vm.tiktok.com
- notification
- o18.ptr806

```
nmap -T4 -A -v vm.tiktok.com
[+] http-methods:
[+] Supported Methods: GET HEAD POST OPTIONS
[+] http-robots.txt: 1 disallowed entry
[+]
[+] http-server-header: nginx
[+] http-title: TikTok - Make Your Day
[+] Requested resource was https://www.tiktok.com/
[+] http-trane-info: Problem with XML parsing of /evox/about
[+] ssl-cert: Subject: commonName=tiktok.com
[+] Subject Alternative Name: DNS:*.tiktok.com, DNS:tiktok.com
[+] Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US
[+] Public Key type: rsa
[+] Public Key bits: 2048
[+] Signature Algorithm: sha256WithRSAEncryption
[+] Not valid before: 2019-11-14T00:00:00
[+] Not valid after: 2022-01-12T12:00:00
[+] MD5: 6042 e736 dd95 7460 aa10 bb3e 309f f719
[+] SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5
[+] SSL-date: TLS randomness does not represent time
[+] tls-alpn:
[+] http/1.1
[+] tls-nextprotoneg:
[+] http/1.1
[+] http/1.0
[+] Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[+] Aggressive OS guesses: Linux 4.0 (93%), Linux 3.11 - 4.1 (93%), Linux 4.4 (93%), Linux 2.6.31 (92%), Linux 3.10 (92%), Linux 3.10 - 3.16 (92%), Linux 2.6.32 (92%), Linux 2.6.32 - 2.6.33 (92%), Linux 2.6.32 - 2.6.35 (92%), Linux 2.6.32 or 3.10 (92%)
[+] No exact OS matches for host (test conditions non-ideal).
[+] Network Distance: 7 hops
```

Filter Hosts

[/data/s.txt - Sublime Text UNR] [Zenmap] [Zenmap] [Zenmap] [Pictures] [Zenmap] [Zenmap] [Zenmap] 1/2

Applications ▾ Places ▾ Zenmap ▾

The Oct 22 6:24:56 AM •

**Zenmap**

Scan Tools Profile Help

Target: vm.tiktok.com ▾ Profile: Intense scan ▾ Scan Cancel

Command: nmap -T4 -A -v vm.tiktok.com

Hosts Services

OS Host

- vm.tiktok.com
- notification
- o18.ptr806

```
nmap -T4 -A -v vm.tiktok.com
[+] http/1.1
[+] http/1.0
[+] Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
[+] Aggressive OS guesses: Linux 4.0 (93%), Linux 3.11 - 4.1 (93%), Linux 4.4 (93%), Linux 2.6.31 (92%), Linux 3.10 (92%), Linux 3.10 - 3.16 (92%), Linux 2.6.32 (92%), Linux 2.6.32 - 2.6.33 (92%), Linux 2.6.32 - 2.6.35 (92%), Linux 2.6.32 or 3.10 (92%)
[+] No exact OS matches for host (test conditions non-ideal).
[+] Network Distance: 7 hops

[+] TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 2.51 ms homerouter.cpe (192.168.8.1)
2 ...
3 44.91 ms 10.12.90.85
4 ...
5 41.44 ms 10.12.2.162
6 ...
7 31.22 ms al19-235-0-41.deploy.akamaitechnologies.com (119.235.0.41)

[+] NSE: Script Post-scanning.
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 52.10 seconds
Raw packets sent: 2127 (96.488KB) | Rcvd: 33 (2.532KB)
```

Filter Hosts

[/data/s.txt - Sublime Text UNR] [Zenmap] [Zenmap] [Zenmap] [Pictures] [Zenmap] [Zenmap] [Zenmap] 1/2

## 34.vt.tiktok.com

```
Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 6:25:41 AM ●
Zenmap
Scan Tools Profile Help
Target: vt.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v vt.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
vt.tiktok.co v16-web.ti o16.ptr923
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:17 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating Ping Scan at 06:17
Scanning vt.tiktok.com [119.235.0.40] [4 ports]
Completed Ping Scan at 06:17, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:17
Completed Parallel DNS resolution of 1 host. at 06:17, 0.05s elapsed
Initiating SYN Stealth Scan at 06:17
Scanning vt.tiktok.com [119.235.0.40] [1000 ports]
Discovered open port 443/tcp on 119.235.0.40
Discovered open port 80/tcp on 119.235.0.40
Completed SYN Stealth Scan at 06:17, 10.43s elapsed (1000 total ports)
Initiating Service scan at 06:17
Scanning 2 services on vt.tiktok.com [119.235.0.40]
Completed Service scan at 06:17, 13.21s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against vt.tiktok.com [119.235.0.40]
Retrying OS detection (try #2) against vt.tiktok.com [119.235.0.40]
Initiating Traceroute at 06:17
Completed Traceroute at 06:18, 3.01s elapsed
Initiating Parallel DNS resolution of 5 hosts. at 06:18
Completed Parallel DNS resolution of 5 hosts. at 06:18, 13.00s elapsed
NSE: Script scanning 119.235.0.40.
Initiating NSE at 06:18
Filter Hosts
[~/data/n.txt - Sublime Text (UNRE)] [Zenmap] [Zenmap] Pictures [Zenmap] [Zenmap] 1/2
```

```
Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 6:25:45 AM ●
Zenmap
Scan Tools Profile Help
Target: vt.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v vt.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
vt.tiktok.co v16-web.ti o16.ptr923
Initiating Parallel DNS resolution of 5 hosts. at 06:18
Completed Parallel DNS resolution of 5 hosts. at 06:18, 13.00s elapsed
NSE: Script scanning 119.235.0.40.
Initiating NSE at 06:18
Completed NSE at 06:18, 14.82s elapsed
Initiating NSE at 06:18
Completed NSE at 06:18, 15.59s elapsed
Initiating NSE at 06:18
Completed NSE at 06:18, 0.00s elapsed
Nmap scan report for vt.tiktok.com [119.235.0.40]
Host is up (0.029s latency).
Other addresses for vt.tiktok.com (not scanned): 119.235.0.41
rDNS record for 119.235.0.40: all19-235-0-40.deploy.akamaitechnologies.com
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   AkamaiHost (Akamai's HTTP Acceleration/Mirror service)
| http-title: Did not follow redirect to https://www.tiktok.com/
443/tcp   open  ssl/http AkamaiHost (Akamai's HTTP Acceleration/Mirror service)
| ssl-cert: Subject: commonName=tiktok.com
| Subject Alternative Name: DNS:tiktok.com, DNS:tiktok.com
| Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-11-14T00:00:00
| Not valid after: 2022-01-12T12:00:00
| MD5: 6042 e736 dd95 7460 a810 bb3e 309f f719
| SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5
| tls-alpn:
|   h2, http/1.1
Filter Hosts
[~/data/n.txt - Sublime Text (UNRE)] [Zenmap] [Zenmap] Pictures [Zenmap] [Zenmap] 1/2
```

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 6:25:50 AM •

**Zenmap**

Scan Tools Profile Help

Target: vt.tiktok.com ▾ Profile: Intense scan ▾ Scan Cancel

Command: nmap -T4 -A -v vt.tiktok.com

Hosts Services

OS Host

- vt.tiktok.co
- v16-web.ti
- o16.ptr923

Nmap Output Ports / Hosts Topology Host Details Scans

```
nmap -T4 -A -v vt.tiktok.com
[...]
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2019-11-14T00:00:00
Not valid after: 2022-01-12T12:00:00
MD5: 6042 e736 dd95 7460 aa10 bb3e 309f f719
SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5
tls-alpn:
http/1.1
tls-nextprotoneg:
http/1.1
http/1.0
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|WAP|router
Running (JUST GUESSING): Linux 4.X|3.X|2.4.X|2.6.X (93%), MikroTik RouterOS 6.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3.13 cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6 cpe:/o:mikrotik:routeros:6.15
Aggressive OS guesses: Linux 4.4 (93%), Linux 4.0 (87%), Linux 3.13 (87%), Linux 3.11 - 4.1 (87%), Linux 3.8 (87%), Linux 3.10 (86%), Linux 3.10 - 3.16 (86%), Linux 3.10 - 3.12 (86%), Linux 3.16 (86%), Linux 4.9 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 6 hops

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 3.07 ms homerouter.cpe (192.168.8.1)
2 ...
3 54.62 ms 10.12.90.85
4 34.68 ms 10.12.83.25
5 44.90 ms 10.12.2.162
6 34.15 ms a119-235-0-40.deploy.akamaitechnologies.com (119.235.0.40)

NSE: Script Post-scanning.
```

Filter Hosts NSE: Script Post-scanning.

[-/data/s.txt - Sublime Text (UNRE)] [Zenmap] [Zenmap] [Pictures] [Zenmap] [Zenmap]

1/2

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 6:25:51 AM •

**Zenmap**

Scan Tools Profile Help

Target: vt.tiktok.com ▾ Profile: Intense scan ▾ Scan Cancel

Command: nmap -T4 -A -v vt.tiktok.com

Hosts Services

OS Host

- vt.tiktok.co
- v16-web.ti
- o16.ptr923

Nmap Output Ports / Hosts Topology Host Details Scans

```
nmap -T4 -A -v vt.tiktok.com
[...]
Device type: general purpose|WAP|router
Running (JUST GUESSING): Linux 4.X|3.X|2.4.X|2.6.X (93%), MikroTik RouterOS 6.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:4.4 cpe:/o:linux:linux_kernel:3.13 cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6 cpe:/o:mikrotik:routeros:6.15
Aggressive OS guesses: Linux 4.4 (93%), Linux 4.0 (87%), Linux 3.13 (87%), Linux 3.11 - 4.1 (87%), Linux 3.8 (87%), Linux 3.10 (86%), Linux 3.10 - 3.16 (86%), Linux 3.10 - 3.12 (86%), Linux 3.16 (86%), Linux 4.9 (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 6 hops

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 3.07 ms homerouter.cpe (192.168.8.1)
2 ...
3 54.62 ms 10.12.90.85
4 34.68 ms 10.12.83.25
5 44.90 ms 10.12.2.162
6 34.15 ms a119-235-0-40.deploy.akamaitechnologies.com (119.235.0.40)

NSE: Script Post-scanning.
Initiating NSE at 06:18
Completed NSE at 06:18, 0.00s elapsed
Initiating NSE at 06:18
Completed NSE at 06:18, 0.00s elapsed
Initiating NSE at 06:18
Completed NSE at 06:18, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 76.57 seconds
Raw packets sent: 2126 (97.392KB) | Rcvd: 72 (10.922KB)
```

Filter Hosts NSE: Script Post-scanning.

[-/data/s.txt - Sublime Text (UNRE)] [Zenmap] [Zenmap] [Pictures] [Zenmap] [Zenmap]

1/2

## 35.www-useast1a.tiktok.com

```
Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 6:26:08 AM ●
Zenmap
Scan Tools Profile Help
Target: www-useast1a.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v www-useast1a.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
spotlight. www-usea promotion
nmap -T4 -A -v www-useast1a.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 06:17 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating NSE at 06:17
Completed NSE at 06:17, 0.00s elapsed
Initiating Ping Scan at 06:17
Scanning www-useast1a.tiktok.com (130.44.212.186) [4 ports]
Completed Ping Scan at 06:17, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:17
Completed Parallel DNS resolution of 1 host. at 06:18, 13.01s elapsed
Initiating SYN Stealth Scan at 06:18
Scanning www-useast1a.tiktok.com (130.44.212.186) [1000 ports]
Discovered open port 80/tcp on 130.44.212.186
Discovered open port 443/tcp on 130.44.212.186
Increasing send delay for 130.44.212.186 from 0 to 5 due to 11 out of 20 dropped probes since last increase.
Completed SYN Stealth Scan at 06:19, 62.43s elapsed (1000 total ports)
Initiating Service scan at 06:19
Scanning 2 services on www-useast1a.tiktok.com (130.44.212.186)
Completed Service scan at 06:19, 14.59s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www-useast1a.tiktok.com [130.44.212.186]
Retrying OS detection (try #2) against www-useast1a.tiktok.com [130.44.212.186]
Initiating Traceroute at 06:19
Completed Traceroute at 06:19, 3.32s elapsed
Initiating Parallel DNS resolution of 17 hosts. at 06:19
Completed Parallel DNS resolution of 17 hosts. at 06:19, 13.06s elapsed
NSE: Script scanning 130.44.212.186.
Filter Hosts
[~/data/a.txt - Sublime Text (UNRE)] [Zenmap] [Pictures] [Zenmap] [Zenmap] 1/2
```

```
Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 6:26:14 AM ●
Zenmap
Scan Tools Profile Help
Target: www-useast1a.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v www-useast1a.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
spotlight. www-usea promotion
nmap -T4 -A -v www-useast1a.tiktok.com
Initiating Parallel DNS resolution of 17 hosts. at 06:19
Completed Parallel DNS resolution of 17 hosts. at 06:19, 13.06s elapsed
NSE: Script scanning 130.44.212.186.
Initiating NSE at 06:19
Completed NSE at 06:20, 17.92s elapsed
Initiating NSE at 06:20
Completed NSE at 06:20, 4.05s elapsed
Initiating NSE at 06:20
Completed NSE at 06:20, 0.00s elapsed
Nmap scan report for www-useast1a.tiktok.com (130.44.212.186)
Host is up (0.26s latency).
Other addresses for www-useast1a.tiktok.com (not scanned): 130.44.212.192 130.44.212.194 130.44.212.184
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp     open  http    nginx
| http-methods:
|_ Supported Methods: GET
|_ http-title: Did not follow redirect to https://www-useast1a.tiktok.com/
443/tcp    open  ssl/http nginx
| http-methods:
|_ Supported Methods: OPTIONS
| http-robots.txt: 1 disallowed entry
|_ /
|_ http-title: TikTok - Make Your Day
|_ ssl-cert: Subject: commonName=*.tiktok.com
|_ Subject Alternative Name: DNS:*.tiktok.com, DNS:tiktok.com
|_ Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US
|_ Public Key type: rsa
|_ Public Key bits: 2048
|_ Signature Algorithm: sha256WithRSAEncryption
Filter Hosts
[~/data/a.txt - Sublime Text (UNRE)] [Zenmap] [Pictures] [Zenmap] [Zenmap] 1/2
```

Applications ▾ Places ▾ Zenmap ▾

Scan Tools Profile Help

Target: www-useast1a.tiktok.com

Profile: Intense scan

Command: nmap -T4 -A -v www-useast1a.tiktok.com

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
OS	Host	nmap -T4 -A -v www-useast1a.tiktok.com				
<b>spotlightt</b>		4 45.50 ms 10.12.83.25				
<b>www-usea</b>		5 45.61 ms 10.12.2.162				
<b>promotion</b>		6 46.88 ms 103.87.125.97				
		7 46.42 ms 103.87.124.81				
		8 162.14 ms 103.87.124.146				
		9 162.11 ms teo-5.0-17.201.agr21.mrs01.atlas.cogentco.com (149.14.124.137)				
		10 161.58 ms be2345.ccr21.mrs01.atlas.cogentco.com (154.54.38.169)				
		11 163.10 ms be3222.ccr31.vlc02.atlas.cogentco.com (154.54.57.206)				
		12 156.79 ms be3355.ccr31.mad05.atlas.cogentco.com (154.54.57.229)				
		13 174.21 ms be2324.ccr31.blo02.atlas.cogentco.com (154.54.61.129)				
		14 249.69 ms be2331.ccr41.dca01.atlas.cogentco.com (154.54.85.241)				
		15 244.21 ms be3083.ccr41.iad02.atlas.cogentco.com (154.54.30.54)				
		16 ...				
		17 245.61 ms 10.8.253.130				
		18 239.65 ms 10.8.253.128				
		19 ... 23				
		24 273.65 ms 130.44.212.186				
		<b>NSE:</b> Script Post-scanning.				
		Initiating NSE at 06:20				
		Completed NSE at 06:20, 0.00s elapsed				
		Initiating NSE at 06:20				
		Completed NSE at 06:20, 0.00s elapsed				
		Initiating NSE at 06:20				
		Completed NSE at 06:20, 0.00s elapsed				
		Read data files from: /usr/bin/../share/nmap				
		OS and Service detection performed. Please report any incorrect results at <a href="https://nmap.org/submit/">https://nmap.org/submit/</a> .				
		<b>Nmap done:</b> 1 IP address (1 host up) scanned in 136.52 seconds				
		Raw packets sent: 2147 (98.848KB)   Rcvd: 64 (4.858KB)				

Filter Hosts

[data/s.txt - Sublime Text (UNRE)] [Zenmap] [Pictures] [Zenmap] [Zenmap] [Zenmap]

1/2

Applications ▾ Places ▾ Zenmap ▾

Scan Tools Profile Help

Target: www-useast1a.tiktok.com

Profile: Intense scan

Command: nmap -T4 -A -v www-useast1a.tiktok.com

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
OS	Host	nmap -T4 -A -v www-useast1a.tiktok.com				
<b>spotlightt</b>		Public Key bits: 2048				
<b>www-usea</b>		Signature Algorithm: sha256WithRSAEncryption				
<b>promotion</b>		Not valid before: 2020-07-06T00:00:00				
		Not valid after: 2022-07-07T12:00:00				
		MDS: e593 3d6a 7ca4 da4f 432b a997 7bbf 24c4				
		SHA-1: d4e0 fcbl 815c 8020 1471 cb7a 564b 19a8 9e6a 3d1f				
		-ssl-date: TLS randomness does not represent time				
		-tls-alpn:				
		http/1.1				
		-tls-nextprotoneg:				
		http/1.1				
		<b>Warning:</b> OSScan results may be unreliable because we could not find at least 1 open and 1 closed port				
		Device type: general purpose				
		Running (JUST GUESSING): Linux 4.X 3.X (89%)				
		OS CPE: cpe:/o:linux:linux_kernel:4.9 cpe:/o:linux:linux_kernel:3.18				
		Aggressive OS guesses: Linux 4.9 (89%), Linux 3.18 (86%)				
		No exact OS matches for host (test conditions non-ideal).				
		Network Distance: 24 hops				
		TRACEROUTER (using port 443/tcp)				
		HOP RTT ADDRESS				
		1 2.95 ms homerouter.cpe (192.168.8.1)				
		2 ...				
		3 46.87 ms 10.12.98.85				
		4 45.50 ms 10.12.83.25				
		5 45.61 ms 10.12.2.162				
		6 46.88 ms 103.87.125.97				
		7 46.42 ms 103.87.124.81				
		8 162.14 ms 103.87.124.146				
		9 162.11 ms teo-5.0-17.201.agr21.mrs01.atlas.cogentco.com (149.14.124.137)				

Filter Hosts

[data/s.txt - Sublime Text (UNRE)] [Zenmap] [Pictures] [Zenmap] [Zenmap] [Zenmap]

1/2