



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
IT19013756	M. H. D. V. JAYASINGHE

Date of submission
24th 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.

Contents

1.1.1.	Scans of REDHAWK tool	3
1.1.2.	Zenmap Scannings	5

1.1.1. Scans of REDHAWK tool

```
Applications Places Terminal Fri Oct 23 2:37:57 AM ● root@kali: ~/tools/RED_HAWK
File Edit View Search Terminal Help

All In One Tool For Information Gathering And Vulnerability Scanning

      . i i i .
      . | ( \ | \ | / ) | .
      | ( \ | / \ | / ) | .
      ( \ ) Ver 2.0.0 /
      \ \ \ \ / /
      | \ \ / |
      \ \ \ / /
      \ \ / /
      \ / /
      [ $ ] Shut Out - You ; )

{C} Coded By - R3D#X0R_2H1N A.K.A Tuhinshubhra

[!] cURL Module Is Missing! Try 'fix' command OR Install php-curl
[!] DOM Module Is Missing! Try 'fix' command OR Install php-xml

[#] Enter The Website You Want To Scan : tiktok.com

[#] Enter 1 For HTTP OR Enter 2 For HTTPS: 2
```

```

Applications ▾ Places ▾ Terminal ▾
Fri Oct 23 2:38:00 AM •
root@kali: ~/tools/RED_HAWK
File Edit View Search Terminal Help
+-----+
+          List Of Scans Or Actions          +
+-----+
Scanning Site : https://tiktok.com

[0] Basic Recon (Site Title, IP Address, CMS, Cloudflare Detection, Robots.txt Scanner)
[1] Whois Lookup
[2] Geo-IP Lookup
[3] Grab Banners
[4] DNS Lookup
[5] Subnet Calculator
[6] NMAP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQLi Scanner (Finds Links With Parameter And Scans For Error Based SQLi)
[10] Bloggers View (Information That Bloggers Might Be Interested In)
[11] WordPress Scan (Only If The Target Site Runs On WP)
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates
[B] Scan Another Website (Back To Site Selection)
[Q] Quit!

[#] Choose Any Scan OR Action From The Above List: □

```

[Pictures] [GitHub - Tahinshubhra/RED_HAWK] root@kali: ~/tools/RED_HAWK 1 / 2

Basic Recon

```

Applications ▾ Places ▾ Terminal ▾
Fri Oct 23 2:41:09 AM •
root@kali: ~/tools/RED_HAWK
File Edit View Search Terminal Help
[4] DNS Lookup
[5] Subnet Calculator
[6] NMAP Port Scan
[7] Subdomain Scanner
[8] Reverse IP Lookup & CMS Detection
[9] SQLi Scanner (Finds Links With Parameter And Scans For Error Based SQLi)
[10] Bloggers View (Information That Bloggers Might Be Interested In)
[11] WordPress Scan (Only If The Target Site Runs On WP)
[12] Crawler
[13] MX Lookup
[A] Scan For Everything - (The Old Lame Scanner)
[F] Fix (Checks For Required Modules and Installs Missing Ones)
[U] Check For Updates
[B] Scan Another Website (Back To Site Selection)
[Q] Quit!

[#] Choose Any Scan OR Action From The Above List: 0

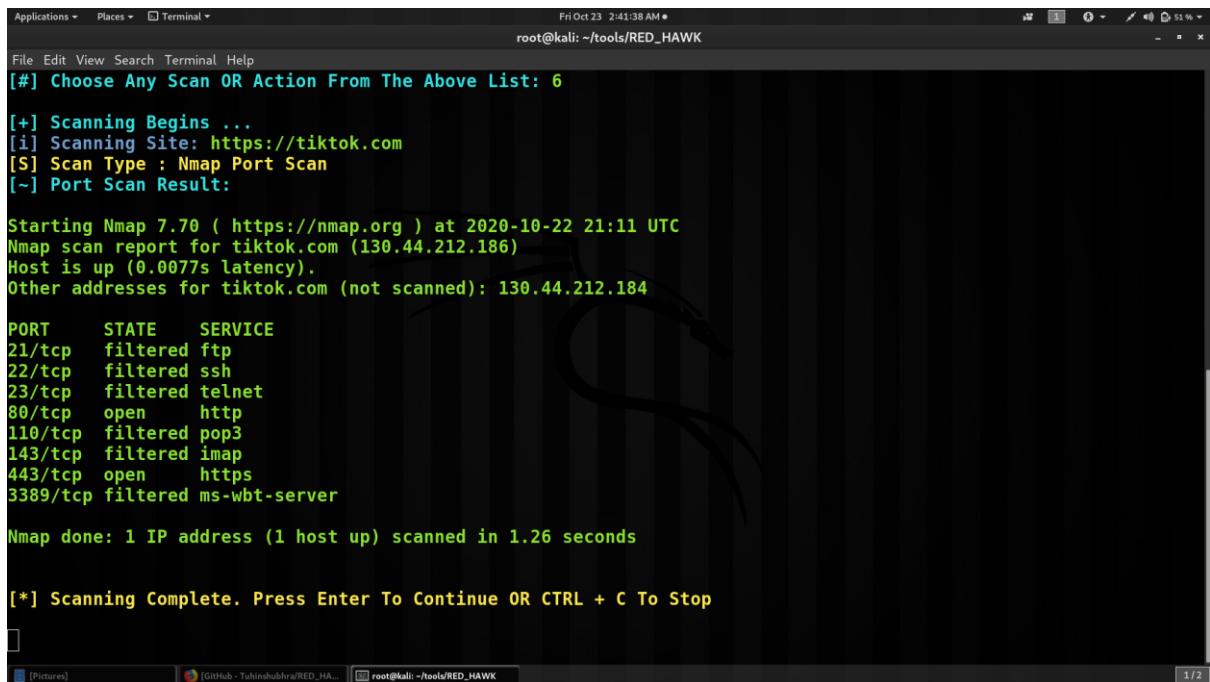
[+] Scanning Begins ...
[i] Scanning Site: https://tiktok.com
[S] Scan Type : BASIC SCAN

[iINFO] Site Title: TikTok - Make Your Day
[iINFO] IP address: 161.117.98.196
[iINFO] Web Server: nginx
[iINFO] CMS: Could Not Detect
[iINFO] Cloudflare: Not Detected
[iINFO] Robots File: root@kali:~/tools/RED_HAWK# □

```

[Pictures] [GitHub - Tahinshubhra/RED_HAWK] root@kali: ~/tools/RED_HAWK 1 / 2

Nmap port scan



The screenshot shows a terminal window on a Kali Linux system. The title bar indicates it's a terminal window from the Applications menu, running at Fri Oct 23 2:41:38 AM. The command being run is 'nmap -sT -T4 -p21-3389 https://tiktok.com'. The output shows the following details:

```
[#] Choose Any Scan OR Action From The Above List: 6
[+] Scanning Begins ...
[1] Scanning Site: https://tiktok.com
[S] Scan Type : Nmap Port Scan
[-] Port Scan Result:

Starting Nmap 7.70 ( https://nmap.org ) at 2020-10-22 21:11 UTC
Nmap scan report for tiktok.com (130.44.212.186)
Host is up (0.0077s latency).
Other addresses for tiktok.com (not scanned): 130.44.212.184

PORT      STATE    SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
80/tcp    open     http
110/tcp   filtered pop3
143/tcp   filtered imap
443/tcp   open     https
3389/tcp  filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds

[*] Scanning Complete. Press Enter To Continue OR CTRL + C To Stop
```

1.1.2. Zenmap Scannings

Zenmap is a cross-platform GUI (Graphical User Interface) for Nmap. This open-source tool is designed to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users.

The purpose of Zenmap is not to replace Nmap, but to make Nmap more useful. Here are some of the advantages Zenmap offers:

- Interactivity & intuitiveness – easy to use & simple graphical interface
- Repeatability – Using scan profiles is very easy to repeat scan with exact same settings
- Readability – It is possible to see scanned hosts in Topology

I implement the Zenmap scans for every subdomain in the tiktok.com

1. www.tiktok.com

Applications ▾ Places ▾ Zenmap ▾

The Oct 22 4:26:57 AM •

Zenmap

Scan Tools Profile Help

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

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

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host www.tiktok

```

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:21 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:21
Completed NSE at 04:21, 0.00s elapsed
Initiating NSE at 04:21
Completed NSE at 04:21, 0.00s elapsed
Initiating NSE at 04:21
Completed NSE at 04:21, 0.00s elapsed
Initiating NSE at 04:21
Completed NSE at 04:21, 0.00s elapsed
Initiating Ping Scan at 04:21
Scanning www.tiktok.com [119.235.0.40] [4 ports]
Completed Ping Scan at 04:21, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:21
Completed Parallel DNS resolution of 1 host. at 04:21, 0.02s elapsed
Initiating SYN Stealth Scan at 04:21
Scanning www.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 15 dropped probes since last increase.
Completed SYN Stealth Scan at 04:22, 40.77s elapsed (1000 total ports)
Initiating Service scan at 04:22
Scanning 2 services on www.tiktok.com [119.235.0.40]
Completed Service scan at 04:22, 12.22s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www.tiktok.com [119.235.0.40]
Retrying OS detection (try #2) against www.tiktok.com [119.235.0.40]
WARNING: OS didn't match until try #2
Initiating Traceroute at 04:22
Completed Traceroute at 04:22, 3.06s elapsed
NSE: Script scanning 119.235.0.40.
Initiating NSE at 04:22

```

Filter Hosts

[untitled - Sublime Text (UNREGISTERED)] [root@kali: ~] Zenmap Zenmap [data]

Applications ▾ Places ▾ Zenmap ▾

The Oct 22 4:27:12 AM •

Zenmap

Scan Tools Profile Help

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

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

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host www.tiktok

```

NSE: Script scanning 119.235.0.40.
Initiating NSE at 04:22
Completed NSE at 04:22, 5.21s elapsed
Initiating NSE at 04:22
Completed NSE at 04:22, 0.47s elapsed
Initiating NSE at 04:22
Completed NSE at 04:22, 0.00s elapsed
Nmap scan report for www.tiktok.com (119.235.0.40)
Host is up (0.035s latency).
Other addresses for www.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   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://www.tiktok.com/
443/tcp   open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
| http-favicon: Unknown favicon MD5: 9CEFE637DDFB594AC6DEE7FD68E85A95
| http-methods:
|_ Supported Methods: HEAD GET OPTIONS
|_ http-robots.txt: 1 disallowed entry
|_ http-server-header: nginx
|_ 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

```

Filter Hosts

[untitled - Sublime Text (UNREGISTERED)] [root@kali: ~] Zenmap Zenmap [data]

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 4:27:18 AM ▾

Zenmap

Scan Tools Profile Help

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

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

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

www.tikto

```
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
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: 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: 11 hops
```

TRACEROUTE (using port 443/tcp)
 HOP RTT ADDRESS
 1 ... 10
 11 45.53 ms [119.235.0.40](http://119.235.0.40.deploy.akamaitechnologies.com) (119.235.0.40)

NSE: Script Post-scanning.
 Initiating NSE at 04:22
 Completed NSE at 04:22, 0.00s elapsed
 Initiating NSE at 04:22
 Completed NSE at 04:22, 0.00s elapsed

Filter Hosts

[untitled - Sublime Text (UNREGISTERED)] [root@kali: ~] Zenmap Zenmap [data]

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 4:27:22 AM ▾

Zenmap

Scan Tools Profile Help

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

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

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

www.tikto

```
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: 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: 11 hops
```

TRACEROUTE (using port 443/tcp)
 HOP RTT ADDRESS
 1 ... 10
 11 45.53 ms [119.235.0.40](http://119.235.0.40.deploy.akamaitechnologies.com) (119.235.0.40)

NSE: Script Post-scanning.
 Initiating NSE at 04:22
 Completed NSE at 04:22, 0.00s elapsed
 Initiating NSE at 04:22
 Completed NSE at 04:22, 0.00s elapsed
 Initiating NSE at 04:22
 Completed NSE at 04:22, 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 68.08 seconds
 Raw packets sent: 2180 (100.218KB) | Rcvd: 23 (1.538KB)

Filter Hosts

[untitled - Sublime Text (UNREGISTERED)] [root@kali: ~] Zenmap Zenmap [data]

2. account.tiktok.com

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 4:28:33 AM ▾

Zenmap

Scan Tools Profile Help

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

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

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host account.tiktok.com

```

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:22 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:22
Completed NSE at 04:22, 0.00s elapsed
Initiating NSE at 04:22
Completed NSE at 04:22, 0.00s elapsed
Initiating NSE at 04:22
Completed NSE at 04:22, 0.00s elapsed
Initiating Ping Scan at 04:22
Scanning account.tiktok.com [209.127.230.14] [4 ports]
Completed Ping Scan at 04:22, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:22
Completed Parallel DNS resolution of 1 host. at 04:22, 0.04s elapsed
Initiating SYN Stealth Scan at 04:22
Scanning account.tiktok.com [209.127.230.14] [1000 ports]
SYN Stealth Scan Timing: About 37.50% done; ETC: 04:24 (0:00:52 remaining)
Increasing send delay for 209.127.230.14 from 0 to 5 due to 11 out of 23 dropped probes since last increase.
Completed SYN Stealth Scan at 04:24, 89.71s elapsed (1000 total ports)
Initiating Service scan at 04:24
Initiating OS detection (try #1) against account.tiktok.com (209.127.230.14)
Initiating Traceroute at 04:24
Completed Traceroute at 04:24, 3.36s elapsed
Initiating Parallel DNS resolution of 17 hosts. at 04:24
Completed Parallel DNS resolution of 17 hosts. at 04:24, 13.00s elapsed
NSE: Script scanning 209.127.230.14.
Initiating NSE at 04:24
Completed NSE at 04:24, 0.02s elapsed
Initiating NSE at 04:24
Completed NSE at 04:24, 0.00s elapsed

```

Filter Hosts

[untitled - Sublime Text (UNREGISTERED)] [root@kali: ~] Zenmap [Zenmap] [data] [Pictures] 1/2

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 4:30:20 AM ▾

Zenmap

Scan Tools Profile Help

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

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

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host account.tiktok.com

```

Initiating NSE at 04:24
Completed NSE at 04:24, 0.00s elapsed
Initiating NSE at 04:24
Completed NSE at 04:24, 0.00s elapsed
Nmap scan report for account.tiktok.com (209.127.230.14)
Host is up (0.26s latency).
rDNS record for 209.127.230.14: 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
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 2.6.30
Network Distance: 21 hops

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1  1.12 ms   homeroouter.cpe (192.168.8.1)
2  ...
3  36.27 ms  10.12.98.85
4  34.41 ms  10.12.83.25
5  118.09 ms 10.12.2.162
6  59.79 ms  103.87.125.97
7  60.18 ms  103.87.124.81
8  148.25 ms 103.87.124.38
9  147.76 ms te0-5-0-17.201.agr21.mrs01.atlas.cogentco.com (149.14.124.137)
10 ...

```

Filter Hosts

[untitled - Sublime Text (UNREGISTERED)] [root@kali: ~] Zenmap [Zenmap] [data] [Pictures] 1/2

```

Thu Oct 22 4:30:25 AM •
Zenmap
Scan Tools Profile Help
Target: account.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v account.tiktok.com
Hosts Services
OS Host
account.tiktok.com
3 36.27 ms 10.12.90.85
4 34.41 ms 10.12.83.25
5 118.09 ms 10.12.2.162
6 59.79 ms 103.87.125.97
7 60.18 ms 103.87.124.81
8 148.25 ms 103.87.124.38
9 147.76 ms te0-5-0-17.201.agr21.mrs01.atlas.cogentco.com (149.14.124.137)
10 136.32 ms be2346.ccr22.mrs01.atlas.cogentco.com (154.54.38.173)
11 141.51 ms be3223.ccr31.vlc02.atlas.cogentco.com (154.54.57.210)
12 192.31 ms be3355.ccr31.mad05.atlas.cogentco.com (154.54.57.229)
13 191.83 ms be2325.ccr32.bio02.atlas.cogentco.com (154.54.61.133)
14 260.54 ms be2332.ccr42.dca01.atlas.cogentco.com (154.54.85.245)
15 260.00 ms be2658.ccr22.iad02.atlas.cogentco.com (154.54.47.138)
16 260.54 ms be2962.rcr21.b00320-1.dca01.atlas.cogentco.com (154.54.46.114)
17 260.55 ms be3801.rcr21.b00320-1.dca01.atlas.cogentco.com (154.24.61.222)
18 ... 20
21 282.38 ms s01.bc.larksuite.com (209.127.230.14)

NSE: Script Post-scanning.
Initiating NSE at 04:24
Completed NSE at 04:24, 0.00s elapsed
Initiating NSE at 04:24
Completed NSE at 04:24, 0.00s elapsed
Initiating NSE at 04:24
Completed NSE at 04:24, 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 112.66 seconds
Raw packets sent: 3078 (136.386KB) | Rcvd: 41 (2.864KB)

```

3. o2.ptr4323.i.account.tiktok.com

```

Thu Oct 22 4:39:12 AM •
Zenmap
Scan Tools Profile Help
Target: o2.ptr4323.i.account.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v o2.ptr4323.i.account.tiktok.com
Hosts Services
OS Host
o2.ptr4323.i.account.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:34 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:34
Completed NSE at 04:34, 0.00s elapsed
Initiating NSE at 04:34
Completed NSE at 04:34, 0.00s elapsed
Initiating NSE at 04:34
Completed NSE at 04:34, 0.00s elapsed
Initiating NSE at 04:34
Completed NSE at 04:34, 0.00s elapsed
Initiating Ping Scan at 04:34
Scanning o2.ptr4323.i.account.tiktok.com [167.89.14.4] [4 ports]
Completed Ping Scan at 04:34, 0.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:34
Completed Parallel DNS resolution of 1 host. at 04:34, 0.03s elapsed
Initiating SYN Stealth Scan at 04:34
Scanning o2.ptr4323.i.account.tiktok.com [167.89.14.4] [1000 ports]
SYN Stealth Scan Timing: About 13.00% done; ETC: 04:38 (0:03:27 remaining)
SYN Stealth Scan Timing: About 25.50% done; ETC: 04:38 (0:02:58 remaining)
SYN Stealth Scan Timing: About 37.85% done; ETC: 04:38 (0:02:29 remaining)
SYN Stealth Scan Timing: About 50.00% done; ETC: 04:38 (0:02:01 remaining)
SYN Stealth Scan Timing: About 62.50% done; ETC: 04:38 (0:01:31 remaining)
SYN Stealth Scan Timing: About 74.55% done; ETC: 04:38 (0:01:02 remaining)
SYN Stealth Scan Timing: About 87.00% done; ETC: 04:38 (0:00:32 remaining)
Completed SYN Stealth Scan at 04:38, 243.93s elapsed (1000 total ports)
Initiating Service scan at 04:38
Initiating OS detection (try #1) against o2.ptr4323.i.account.tiktok.com [167.89.14.4]
Retrying OS detection (try #2) against o2.ptr4323.i.account.tiktok.com [167.89.14.4]
Initiating Traceroute at 04:38
Completed Traceroute at 04:38, 9.34s elapsed
Initiating Parallel DNS resolution of 8 hosts. at 04:38

```

```
Applications Places Zenmap Thu Oct 22 4:39:17 AM
Scan Tools Profile Help
Target: o2.ptr4323.i.account.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v o2.ptr4323.i.account.tiktok.com

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS Host o2.ptr4323.i.account.tiktok.com [Details]
Completed traceroute at 04:38, 9.34s elapsed
Initiating Parallel DNS resolution of 8 hosts. at 04:38
Completed Parallel DNS resolution of 8 hosts. at 04:38, 13.00s elapsed
NSE: Script scanning 167.89.14.4.
Initiating NSE at 04:38
Completed NSE at 04:38, 0.00s elapsed
Initiating NSE at 04:38
Completed NSE at 04:38, 0.00s elapsed
Initiating NSE at 04:38
Completed NSE at 04:38, 0.00s elapsed
Nmap scan report for o2.ptr4323.i.account.tiktok.com (167.89.14.4)
Host is up (0.24s latency).
All 1000 scanned ports on o2.ptr4323.i.account.tiktok.com (167.89.14.4) are filtered
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto icmp)
HOP RTT ADDRESS
1 2.52 ms homerouter.cpe (192.168.8.1)
2 ...
3 32.57 ms 10.12.90.85
4 27.82 ms 10.12.83.25
5 27.85 ms 10.12.2.162
6 28.47 ms 103.87.125.97
7 34.52 ms 103.87.124.81
8 21.38 ms 103.87.124.21
9 42.19 ms ix-xe-1-0-3-0.tcore1.mlv-mumbai.as6453.net (180.87.38.182)
10 ... 30

NSE: Script Post-scanning.
Initiating NSE at 04:38
Filter Hosts
```

```
Applications Places Zenmap Thu Oct 22 4:39:19 AM • Zenmap
Scan Tools Profile Help
Target: o2.ptr4323.i.account.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v o2.ptr4323.i.account.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans Details
OS Host o2.ptr4323
nmap -T4 -A -v o2.ptr4323.i.account.tiktok.com
Nmap scan report for o2.ptr4323.i.account.tiktok.com (167.89.14.4)
Host is up (0.24s latency).
All 1000 scanned ports on o2.ptr4323.i.account.tiktok.com (167.89.14.4) are filtered
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.52 ms homerouter.cpe (192.168.8.1)
2 ...
3 32.57 ms 10.12.90.85
4 27.82 ms 10.12.83.25
5 27.85 ms 10.12.2.162
6 28.47 ms 103.87.125.97
7 34.52 ms 103.87.124.81
8 21.38 ms 103.87.124.2
9 42.19 ms ix-xe-1-0-3-0.tcore1.mlv-mumbai.as6453.net (180.87.38.182)
10 ... 30

NSE: Script Post-scanning.
Initiating NSE at 04:38
Completed NSE at 04:38, 0.00s elapsed
Initiating NSE at 04:38
Completed NSE at 04:38, 0.00s elapsed
Initiating NSE at 04:38
Completed NSE at 04:38, 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 281.48 seconds
Raw packets sent: 2126 (96.896KB) | Rcvd: 29 (1.942KB)
```

4. o14.ptr1445.account.tiktok.com

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:39 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:39
Completed NSE at 04:39
Completed Ping Scan at 04:39, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:39
Completed Parallel DNS resolution of 1 host. at 04:39, 0.04s elapsed
Initiating SYN Stealth Scan at 04:39
Scanning o14.ptr1445.account.tiktok.com (167.89.2.255) [1000 ports]
SYN Stealth Scan Timing: About 12.05% done; ETC: 04:44 (0:03:46 remaining)
SYN Stealth Scan Timing: About 24.50% done; ETC: 04:44 (0:03:08 remaining)
SYN Stealth Scan Timing: About 36.50% done; ETC: 04:44 (0:02:38 remaining)
SYN Stealth Scan Timing: About 48.10% done; ETC: 04:44 (0:02:12 remaining)
SYN Stealth Scan Timing: About 60.50% done; ETC: 04:44 (0:01:39 remaining)
SYN Stealth Scan Timing: About 72.50% done; ETC: 04:44 (0:01:09 remaining)
SYN Stealth Scan Timing: About 84.50% done; ETC: 04:44 (0:00:39 remaining)
Completed SYN Stealth Scan at 04:44, 252.86s elapsed (1000 total ports)
Initiating Service scan at 04:44
Initiating OS detection (try #1) against o14.ptr1445.account.tiktok.com (167.89.2.255)
Retrying OS detection (try #2) against o14.ptr1445.account.tiktok.com (167.89.2.255)
Initiating Traceroute at 04:44
Completed Traceroute at 04:44, 3.25s elapsed
Initiating Parallel DNS resolution of 17 hosts. at 04:44

```

```
Completed Traceroute at 04:44, 3.25s elapsed
Initiating Parallel DNS resolution of 17 hosts. at 04:44
Completed Parallel DNS resolution of 17 hosts. at 04:44, 13.45s elapsed
NSE: Script scanning 167.89.2.255.
Initiating NSE at 04:44
Completed NSE at 04:44, 0.01s elapsed
Initiating NSE at 04:44
Completed NSE at 04:44, 0.00s elapsed
Initiating NSE at 04:44
Completed NSE at 04:44, 0.00s elapsed
Nmap scan report for o14.ptr1445.account.tiktok.com (167.89.2.255)
Host is up (0.26s latency).
All 1000 scanned ports on o14.ptr1445.account.tiktok.com (167.89.2.255) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 22 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1  2.57 ms   homeroouter.cpe (192.168.8.1)
2  ...
3  45.04 ms  10.12.90.85
4  31.10 ms  10.12.83.25
5  31.43 ms  10.12.2.162
6  27.62 ms  103.87.125.97
7  27.66 ms  103.87.124.209
8  26.31 ms  103.87.124.130
9  53.49 ms  ix-xe-1-0-3-0.tcore1.mlv-mumbai.as6453.net (180.87.38.182)
10 159.62 ms if-ae-5-2.tcore1.wyn-marseille.as6453.net (80.231.217.29)
11 155.59 ms if-ae-21-2.tcore1.pye-paris.as6453.net (80.231.154.208)
12 151.65 ms if-ae-11-2.tcore1.nvu-paris.as6453.net (80.231.153.49)
```

```

Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 4:45:55 AM • Zenmap
Scan Tools Profile Help
Target: o14.ptr1445.account.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v o14.ptr1445.account.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host nmap -T4 -A -v o14.ptr1445.account.tiktok.com
10.12.83.25
10.12.2.162
103.87.125.97
103.87.124.209
103.87.124.130
180.87.38.182
80.231.217.29
80.231.154.208
80.231.153.49
64.125.14.49
64.125.29.4
64.125.29.49
64.125.31.173
208.185.154.78
167.89.2.255
NSE Script Post-scanning.
Initiating NSE at 04:44
Completed NSE at 04:44, 0.00s elapsed
Initiating NSE at 04:44
Completed NSE at 04:44, 0.00s elapsed
Initiating NSE at 04:44
Completed NSE at 04:44, 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 283.78 seconds
Raw packets sent: 2082 (94.764KB) | Rcvd: 24 (1.762KB)

```

5. o15.ptr425.account.tiktok.com

```

Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 4:54:37 AM • Zenmap
Scan Tools Profile Help
Target: o15.ptr425.account.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v o15.ptr425.account.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host nmap -T4 -A -v o15.ptr425.account.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:46 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:46
Completed NSE at 04:46, 0.00s elapsed
Initiating NSE at 04:46
Completed NSE at 04:46, 0.00s elapsed
Initiating NSE at 04:46
Completed NSE at 04:46, 0.00s elapsed
Initiating NSE at 04:46
Completed NSE at 04:46, 0.00s elapsed
Initiating Ping Scan at 04:46
Scanning o15.ptr425.account.tiktok.com (168.245.49.201) [4 ports]
Completed Ping Scan at 04:46, 0.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:46
Completed Parallel DNS resolution of 1 host. at 04:46, 0.16s elapsed
Initiating SYN Stealth Scan at 04:46
Scanning o15.ptr425.account.tiktok.com (168.245.49.201) [1000 ports]
SYN Stealth Scan Timing: About 12.50% done; ETC: 04:50 (0:03:37 remaining)
SYN Stealth Scan Timing: About 24.50% done; ETC: 04:50 (0:03:08 remaining)
SYN Stealth Scan Timing: About 36.50% done; ETC: 04:50 (0:02:38 remaining)
SYN Stealth Scan Timing: About 48.50% done; ETC: 04:50 (0:02:08 remaining)
SYN Stealth Scan Timing: About 60.50% done; ETC: 04:50 (0:01:39 remaining)
SYN Stealth Scan Timing: About 72.50% done; ETC: 04:50 (0:01:09 remaining)
SYN Stealth Scan Timing: About 84.50% done; ETC: 04:50 (0:00:39 remaining)
Completed SYN Stealth Scan at 04:50, 251.69s elapsed (1000 total ports)
Initiating Service scan at 04:50
Initiating OS detection (try #1) against o15.ptr425.account.tiktok.com (168.245.49.201)
Retrying OS detection (try #2) against o15.ptr425.account.tiktok.com (168.245.49.201)
Initiating Traceroute at 04:50
Completed Traceroute at 04:50, 3.34s elapsed
Initiating Parallel DNS resolution of 16 hosts. at 04:50

```

```
Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 4:54:44 AM • Zenmap
Scan Tools Profile Help
Target: o15.ptr425.account.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v o15.ptr425.account.tiktok.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host Nmap -T4 -A -v o15.ptr425.account.tiktok.com
Completed traceroute at 04:50, 0.04s elapsed
Initiating Parallel DNS resolution of 16 hosts. at 04:50
Completed Parallel DNS resolution of 16 hosts. at 04:50, 13.00s elapsed
NSE: Script scanning 168.245.49.201.
Initiating NSE at 04:50
Completed NSE at 04:50, 0.01s elapsed
Initiating NSE at 04:50
Completed NSE at 04:50, 0.00s elapsed
Initiating NSE at 04:50
Completed NSE at 04:50, 0.00s elapsed
Nmap scan report for o15.ptr425.account.tiktok.com (168.245.49.201)
Host is up (0.26s latency).
rDNS record for 168.245.49.201: o21.ptr8239.account.cherie.com
All 1000 scanned ports on o15.ptr425.account.tiktok.com (168.245.49.201) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 22 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.96 ms homerouter.cpe (192.168.8.1)
2 ...
3 34.34 ms 10.12.90.85
4 33.82 ms 10.12.83.25
5 33.88 ms 10.12.2.162
6 34.19 ms 103.87.125.97
7 36.27 ms 103.87.124.81
8 31.71 ms 103.87.124.2
9 47.82 ms ix-xe-1-0-3-0.tcore1.mlv-mumbai.as6453.net (180.87.38.182)
10 154.86 ms if-ae-5-2.tcore1.wyn-marseille.as6453.net (80.231.217.29)
11 ...
12 ...
13 ...
14 ...
15 ...
16 ...
17 ...
18 ...
19 ...
20 ...
21 ...
22 ...

Filter Hosts
```

6. url7709.account.tiktok.com

```
Thu Oct 22 4:58:04 AM •
Zenmap
Scan Tools Profile Help
Target: url7709.account.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v url7709.account.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
url7709.ac url7709.ac
nmap -T4 -A -v url7709.account.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:54 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:54
Completed NSE at 04:54, 0.00s elapsed
Initiating NSE at 04:54
Completed NSE at 04:54, 0.00s elapsed
Initiating NSE at 04:54
Completed NSE at 04:54, 0.00s elapsed
Initiating Ping Scan at 04:54
Scanning url7709.account.tiktok.com (167.89.123.54) (4 ports)
Completed Ping Scan at 04:54, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:54
Completed Parallel DNS resolution of 1 host. at 04:54, 1.68s elapsed
Initiating SYN Stealth Scan at 04:54
Scanning url7709.account.tiktok.com (167.89.123.54) [1000 ports]
Discovered open port 80/tcp on 167.89.123.54
Discovered open port 443/tcp on 167.89.123.54
SYN Stealth Scan Timing: About 28.05% done; ETC: 04:56 (0:01:20 remaining)
Increasing send delay for 167.89.123.54 from 0 to 5 due to 11 out of 19 dropped probes since last increase.
Completed SYN Stealth Scan at 04:56, 73.58s elapsed (1000 total ports)
Initiating Service scan at 04:56
Scanning 2 services on url7709.account.tiktok.com (167.89.123.54)
Completed Service scan at 04:56, 13.51s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against url7709.account.tiktok.com (167.89.123.54)
Initiating Traceroute at 04:56
Completed Traceroute at 04:56, 9.07s elapsed
Initiating Parallel DNS resolution of 1 host. at 04:56
Completed Parallel DNS resolution of 1 host. at 04:56, 0.00s elapsed
NSE: Script scanning 167.89.123.54.
NSE: Script scanning 167.89.123.54.
```

```
Thu Oct 22 4:58:17 AM •
Zenmap
Scan Tools Profile Help
Target: url7709.account.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v url7709.account.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
url7709.ac url7709.ac
Completed Parallel DNS resolution of 1 host. at 04:56, 0.00s elapsed
NSE: Script scanning 167.89.123.54.
Initiating NSE at 04:56
Completed NSE at 04:56, 13.47s elapsed
Initiating NSE at 04:56
Completed NSE at 04:57, 30.77s elapsed
Initiating NSE at 04:57
Completed NSE at 04:57, 0.00s elapsed
Nmap scan report for url7709.account.tiktok.com (167.89.123.54)
Host is up (0.25s latency).
Other addresses for url7709.account.tiktok.com (not scanned): 167.89.118.52
rDNS record for 167.89.123.54: 1016789123x54.outbound-mail.sendgrid.net
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx
| http-title: 404 Not Found
|_http-methods:
|   Supported Methods: GET
|_http-title: 400 The plain HTTP request was sent to HTTPS port
|_ssl-cert: Subject: commonName=*.sendgrid.net
|_Subject Alternative Name: DNS:*.sendgrid.net, DNS:sendgrid.net
|_Issuer: commonName=Go Daddy Secure Certificate Authority - G2/organizationName=GoDaddy.com, Inc./stateOrProvinceName=Arizona/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-12-08T14:10:29
| Not valid after: 2021-02-06T22:39:04
| MD5: fe87 4e26 4d86 95f5 e3b0 bbb9 d6f1 e9a7
| SHA-1: afff 984f 7059 e954 d867 e406 baa7 cb49 3d2b 21a0
|_http-methods:
```

```

Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 4:58:19 AM •
Zenmap
Scan Tools Profile Help
Target: url7709.account.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v url7709.account.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
url7709.ac url7709.ac
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-12-08T14:10:29
| Not valid after: 2021-02-06T22:39:04
| MD5: fe87 4e26 4d86 95f5 e3b0 b6f1 e9a7
| SHA-1: afff 984f 7059 e954 d867 e400 baa7 cb49 3d2b 21a0
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: iPAE 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: iPAE 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 3.27 ms homerouter.cpe (192.168.8.1)
2 ... 30
NSE: Script Post-scanning.
Initiating NSE at 04:57
Completed NSE at 04:57, 0.00s elapsed
Initiating NSE at 04:57
Completed NSE at 04:57, 0.00s elapsed
Initiating NSE at 04:57
Completed NSE at 04:57, 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 147.88 seconds
Raw packets sent: 2187 (99.164KB) | Rcvd: 61 (4.644KB)

```

7. activity.tiktok.com

```

Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 4:59:20 AM •
Zenmap
Scan Tools Profile Help
Target: activity.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v activity.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
activity.tkt activity.tkt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:48 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:48
Completed NSE at 04:48, 0.00s elapsed
Initiating NSE at 04:48
Completed NSE at 04:48, 0.00s elapsed
Initiating NSE at 04:48
Completed NSE at 04:48, 0.00s elapsed
Initiating NSE at 04:48
Completed NSE at 04:48, 0.00s elapsed
Initiating Ping Scan at 04:48
Scanning activity.tiktok.com (104.75.84.56) [4 ports]
Completed Ping Scan at 04:48, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:48
Completed Parallel DNS resolution of 1 host. at 04:48, 0.12s elapsed
Initiating SYN Stealth Scan at 04:48
Scanning activity.tiktok.com (104.75.84.56) [1000 ports]
Discovered open port 443/tcp on 104.75.84.56
Completed SYN Stealth Scan at 04:49, 22.12s elapsed (1000 total ports)
Initiating Service scan at 04:49
Scanning 1 service on activity.tiktok.com (104.75.84.56)
Completed Service scan at 04:49, 12.10s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against activity.tiktok.com (104.75.84.56)
Initiating Traceroute at 04:49
Completed Traceroute at 04:49, 3.02s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 04:49
Completed Parallel DNS resolution of 9 hosts. at 04:49, 13.05s elapsed
NSE: Script scanning 104.75.84.56.
Initiating NSE at 04:49
Completed NSE at 04:49, 3.32s elapsed
Initiating NSE at 04:49

```

The screenshot shows the Zenmap interface with the following details:

- Toolbar:** Applications, Places, Zenmap, Thu Oct 22 4:59:37 AM.
- Header:** Scan Tools Profile Help, Target: activity.tiktok.com, Profile: Intense scan, Scan, Cancel.
- Command:** nmap -T4 -A -v activity.tiktok.com
- Hosts Services:** Hosts (selected), Services, Nmap Output, Ports / Hosts, Topology, Host Details, Scans.
- OS Host:** OS (selected), Host.
- Host Details:** activity.tiktok.com
- Services:** 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-ICPv7-80%:7/0>10/22%Time=5F9001FC%P=x86_64-pc-linux-gnu%r(55
SF:LSessionReq,7,\x15\x03\x03\0\x02\x02P";
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:1.0.92b 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
Uptime guess: 13,322 days (since Thu Oct 8 21:06:48 2020)
Network Distance: 10 hops
IP ID Sequence Generation: All zeros
- Traceroute:** (using port 443/tcp)
HOP RTT ADDRESS
1 4.62 ms homerouter.cpe (192.168.8.1)
2 ...
3 39.60 ms 10.12.90.85
4 32.57 ms 10.12.83.25
5 38.08 ms 10.12.2.162
6 33.03 ms 103.87.125.97
7 38.29 ms 103.87.124.81
8 27.80 ms 103.87.125.18
9 41.10 ms 222.165.175.74
10 26.78 ms a104-75-84-56.deploy.static.akamaitechnologies.com (104.75.84.56)
- NSE:** Script Post-scanning.
Initiating NSE at 04:49
Completed NSE at 04:49, 0.00s elapsed
Initiating NSE at 04:49
- Filter Hosts:** [data/a.txt...]

```

Thu Oct 22 4:59:39 AM •
Zenmap
Scan Tools Profile Help
Target: activity.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v activity.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
activity.tiktok
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
Uptime guess: 13.322 days (since Thu Oct 8 21:06:48 2020)
Network Distance: 10 hops
IP ID Sequence Generation: All zeros
TrACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 4.62 ms homerouter.cpe (192.168.8.1)
2 ..
3 39.60 ms 10.12.90.85
4 32.57 ms 10.12.83.25
5 38.08 ms 10.12.2.162
6 33.03 ms 103.87.125.97
7 38.29 ms 103.87.124.81
8 27.80 ms 103.87.125.18
9 41.10 ms 222.165.175.74
10 26.78 ms 104.75.84.56.deploy.static.akamaitechnologies.com (104.75.84.56)

NSE: Script Post-scanning.
Initiating NSE at 04:49
Completed NSE at 04:49, 0.00s elapsed
Initiating NSE at 04:49
Completed NSE at 04:49, 0.00s elapsed
Initiating NSE at 04:49
Completed NSE at 04:49, 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 57.21 seconds
Raw packets sent: 2093 (94.900KB) | Rcvd: 23 (1.192KB)

```

8. ads.tiktok.com

```

Thu Oct 22 5:00:14 AM •
Zenmap
Scan Tools Profile Help
Target: ads.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v ads.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
ads.tiktok
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:55 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:55
Completed NSE at 04:55, 0.00s elapsed
Initiating NSE at 04:55
Completed NSE at 04:55, 0.00s elapsed
Initiating NSE at 04:55
Completed NSE at 04:55, 0.00s elapsed
Initiating NSE at 04:55
Completed NSE at 04:55, 0.00s elapsed
Initiating Ping Scan at 04:55
Scanning ads.tiktok.com (104.75.84.63) [4 ports]
Completed Ping Scan at 04:55, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:55
Completed Parallel DNS resolution of 1 host. at 04:55, 0.02s elapsed
Initiating SYN Stealth Scan at 04:55
Scanning ads.tiktok.com (104.75.84.63) [1000 ports]
Discovered open port 80/tcp on 104.75.84.63
Discovered open port 443/tcp on 104.75.84.63
Completed SYN Stealth Scan at 04:55, 11.74s elapsed (1000 total ports)
Initiating Service scan at 04:55
Scanning 2 services on ads.tiktok.com (104.75.84.63)
Completed Service scan at 04:55, 5.00s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against ads.tiktok.com [104.75.84.63]
Retrying OS detection (try #2) against ads.tiktok.com [104.75.84.63]
Initiating Traceroute at 04:55
Completed Traceroute at 04:55, 3.02s elapsed
Initiating Parallel DNS resolution of 3 hosts. at 04:55
Completed Parallel DNS resolution of 3 hosts. at 04:56, 13.00s elapsed
NSE: Script scanning 104.75.84.63.
Initiating NSE at 04:56

```

```
Applications Places Zenmap Thu Oct 22 5:00:18 AM • Zenmap
Scan Tools Profile Help
Target: ads.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v ads.tiktok.com
Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans Details
OS Host ads.tiktok.com
Completed parallel DNS resolution of 3 hosts. at 04:50, 15.00s elapsed
NSE: Script scanning 104.75.84.63.
Initiating NSE at 04:56
Completed NSE at 04:56, 41.87s elapsed
Initiating NSE at 04:56
Completed NSE at 04:56, 0.47s elapsed
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Nmap scan report for ads.tiktok.com (104.75.84.63)
Host is up (0.028s latency).
Other addresses for ads.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
80/tcp      open  tcpwrapped
| http-methods:
|_ Supported Methods: POST OPTIONS
| http-server-header:
|_ AkamaiGhost
| nginx
| http-title: Did not follow redirect to https://ads.tiktok.com/
443/tcp     open  tcpwrapped
| http-methods:
|_ Supported Methods: HEAD
| 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
Filter Hosts
```

The screenshot shows the Zenmap interface with the following details:

- Target:** ads.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v ads.tiktok.com
- Hosts Services** tab is selected.
- OS Host** tab is selected under the hosts section.
- Host:** ads.tiktok.com
- Details:** Shows the following OS detection results:
 - Subject Alternative Name: DNS:ads.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 309f f719
 - SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5
- 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 (98%)
- OS CPE:** cpe:/o:linux:linux_kernel:4.4
- Aggressive OS guesses:** Linux 4.4 (98%), Linux 4.0 (88%)
- No exact OS matches for host (test conditions non-ideal).**
- Network Distance:** 10 hops
- TRACEROUTE (using port 443/tcp)**

HOP	RTT	ADDRESS
1	2.39 ms	homeroouter.cpe (192.168.8.1)
2	...	3
4	26.38 ms	10.12.83.25
5	...	9
10	26.50 ms	a104-75-84-63.deploy.static.akamaitechnologies.com (104.75.84.63)
- NSE:** Script Post-scanning.
 - Initiating NSE at 04:56
 - Completed NSE at 04:56, 0.00s elapsed
 - Initiating NSE at 04:56
 - Completed NSE at 04:56, 0.00s elapsed
- Filter Hosts** button

```

    Applications ▾ Places ▾ Zenmap ▾
    Thu Oct 22 5:00:22 AM •
    Zenmap
    Scan Tools Profile Help
    Target: ads.tiktok.com Profile: Intense scan
    Command: nmap -T4 -A -v ads.tiktok.com
    Hosts Services
    OS Host
    ads.tiktok.
    Nmap Output Ports / Hosts Topology Host Details Scans
    nmap -T4 -A -v ads.tiktok.com
    | MD5: 6042 e736 dd95 7460 aa10 bb3e 309f f719
    | SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5
    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 (98%)
    OS CPE: cpe:/o:linux:linux kernel:4.4
    Aggressive OS guesses: Linux 4.4 (98%), Linux 4.0 (88%)
    No exact OS matches for host (test conditions non-ideal).
    Network Distance: 10 hops

    TRACEROUTE (using port 443/tcp)
    HOP RTT ADDRESS
    1 2.39 ms homerouter.cpe (192.168.8.1)
    2 ... 3
    4 26.38 ms 10.12.83.25
    5 ... 9
    10 26.50 ms a104-75-84-63.deploy.static.akamaitechnologies.com (104.75.84.63)

    NSE: Script Post-scanning.
    Initiating NSE at 04:56
    Completed NSE at 04:56, 0.00s elapsed
    Initiating NSE at 04:56
    Completed NSE at 04:56, 0.00s elapsed
    Initiating NSE at 04:56
    Completed NSE at 04:56, 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 83.57 seconds
    Raw packets sent: 2152 (99.814KB) | Rcvd: 39 (3.292KB)
  
```

9. ads-sg.tiktok.com

```

    Applications ▾ Places ▾ Zenmap ▾
    Thu Oct 22 5:01:19 AM •
    Zenmap
    Scan Tools Profile Help
    Target: ads-sg.tiktok.com Profile: Intense scan
    Command: nmap -T4 -A -v ads-sg.tiktok.com
    Hosts Services
    OS Host
    ads-sg.tiktok.
    Nmap Output Ports / Hosts Topology Host Details Scans
    nmap -T4 -A -v ads-sg.tiktok.com
    Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:49 +0530
    NSE: Loaded 151 scripts for scanning.
    NSE: Script Pre-scanning.
    Initiating NSE at 04:49
    Completed NSE at 04:49, 0.00s elapsed
    Initiating NSE at 04:49
    Completed NSE at 04:49, 0.00s elapsed
    Initiating NSE at 04:49
    Completed NSE at 04:49, 0.00s elapsed
    Initiating NSE at 04:49
    Completed NSE at 04:49, 0.00s elapsed
    Initiating Ping Scan at 04:49
    Scanning ads-sg.tiktok.com (103.136.221.161) [4 ports]
    Completed Ping Scan at 04:49, 0.12s elapsed (1 total hosts)
    Initiating Parallel DNS resolution of 1 host. at 04:49
    Completed Parallel DNS resolution of 1 host. at 04:49, 13.00s elapsed
    Initiating SYN Stealth Scan at 04:49
    Scanning ads-sg.tiktok.com (103.136.221.161) [1000 ports]
    Discovered open port 443/tcp on 103.136.221.161
    Discovered open port 80/tcp on 103.136.221.161
    Completed SYN Stealth Scan at 04:49, 27.35s elapsed (1000 total ports)
    Initiating Service scan at 04:49
    Scanning 2 services on ads-sg.tiktok.com (103.136.221.161)
    Completed Service scan at 04:50, 5.00s elapsed (2 services on 1 host)
    Initiating OS detection (try #1) against ads-sg.tiktok.com (103.136.221.161)
    Retrying OS detection (try #2) against ads-sg.tiktok.com (103.136.221.161)
    Initiating Traceroute at 04:50
    Completed Traceroute at 04:50, 6.04s elapsed
    Initiating Parallel DNS resolution of 4 hosts. at 04:50
    Completed Parallel DNS resolution of 4 hosts. at 04:50, 13.01s elapsed
    NSE: Script scanning 103.136.221.161.
    Initiating NSE at 04:50
  
```

The screenshot shows the Zenmap interface with the following details:

- Applications:** Applications, Places, Zenmap
- Date:** Thu Oct 22 5:01:28 AM •
- Profile:** Intense scan
- Target:** ads-sg.tiktok.com
- Command:** nmap -T4 -A -v ads-sg.tiktok.com
- Hosts Services:** Hosts, Services, Nmap Output, Ports / Hosts, Topology, Host Details, Scans (selected)
- OS Host:** ads-sg.tiktok.com
- Host Details:**
 - Not valid before: 2020-07-00T00:00:00
 - Not valid after: 2022-07-07T12:00:00
 - MDS: e593 3d6a c7a4 d4af 432b a997 b7ff 24c4
 - SHA-1: d4e0 fcbb 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
- Device type:** general purpose
- Running (JUST GUESSING):** Linux 4.X|3.X|2.6.X (86%)
- OS CPE:** cpe:/o:linux:linux_kernel:4.9 cpe:/o:linux:linux_kernel:3.18 cpe:/o:linux:linux_kernel:2.6
- Aggressive OS guesses:** Linux 4.9 (86%), Linux 3.18 (85%), Linux 2.6.18 - 2.6.22 (85%)
- No exact OS matches for host (test conditions non-ideal).**
- Network Distance:** 15 hops
- Traceroute (using port 443/tcp):**

HOP	RTT	ADDRESS
1	1.13 ms	homeroouter.cpe (192.168.8.1)
2	...	
3	30.85 ms	10.12.90.85
4	...	9
10	82.72 ms	172.18.6.133
11	...	14
15	86.32 ms	103.136.221.161
- NSE:** Script Post-scanning.
Initiating NSE at 04:50
Completed NSE at 04:50, 0.00s elapsed
- Filter Hosts:** [-/data/a.txt...]

```

Thu Oct 22 5:01:30 AM •
Zenmap
Scan Tools Profile Help
Target: ads-sg.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v ads-sg.tiktok.com
Hosts Services
OS Host
ads-sg.tiktok.com
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v ads-sg.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 (JUST GUESSING): Linux 4.X|3.X|2.6.X (86%)
OS CPE: cpe:/o:linux:linux kernel:4.9 cpe:/o:linux:linux kernel:3.18 cpe:/o:linux:linux kernel:2.6
Aggressive OS guesses: Linux 4.9 (86%), Linux 3.18 (85%), Linux 2.6.18 - 2.6.22 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 1.13 ms homerouter.cpe (192.168.8.1)
2 ...
3 30.85 ms 10.12.90.85
4 ...
10 82.72 ms 172.18.6.133
11 ...
14
15 86.32 ms 103.136.221.161

NSE: Script Post-scanning.
Initiating NSE at 04:50
Completed NSE at 04:50, 0.00s elapsed
Initiating NSE at 04:50
Completed NSE at 04:50, 0.00s elapsed
Initiating NSE at 04:50
Completed NSE at 04:50, 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 79.19 seconds
Raw packets sent: 2159 (97.920KB) | Rcvd: 157 (12.025KB)

Filter Hosts

```

10.analytics.tiktok.com

```

Thu Oct 22 5:03:38 AM •
Zenmap
Scan Tools Profile Help
Target: analytics.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v analytics.tiktok.com
Hosts Services
OS Host
analytics.tiktok.com
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v analytics.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:01 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating Ping Scan at 05:01
Scanning analytics.tiktok.com (104.75.84.63) [4 ports]
Completed Ping Scan at 05:01, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:01
Completed Parallel DNS resolution of 1 host. at 05:01, 1.73s elapsed
Initiating SYN Stealth Scan at 05:01
Scanning analytics.tiktok.com (104.75.84.63) [1000 ports]
Completed SYN Stealth Scan at 05:02, 30.50s elapsed (1000 total ports)
Initiating Service scan at 05:02
Initiating OS detection (try #1) against analytics.tiktok.com (104.75.84.63)
Initiating Traceroute at 05:02
Completed Traceroute at 05:02, 3.03s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 05:02
Completed Parallel DNS resolution of 2 hosts. at 05:02, 0.00s elapsed
NSE: Script scanning 104.75.84.63.
Initiating NSE at 05:02
Completed NSE at 05:02, 0.01s elapsed
Initiating NSE at 05:02
Completed NSE at 05:02, 0.00s elapsed
Initiating NSE at 05:02
Completed NSE at 05:02, 0.00s elapsed

```

```

Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 5:03:47 AM ▾
Zenmap
Scan Tools Profile Help
Target: analytics.tiktok.com ▾ Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v analytics.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
analytics.tiktok.com
Completed NSE at 05:02, 0.00s elapsed
Nmap scan report for analytics.tiktok.com (104.75.84.63)
Host is up (0.027s latency).
Other addresses for analytics.tiktok.com (not scanned): 104.75.84.56
rDNS record for 104.75.84.63: a104-75-84-63.deploy.static.akamaitechnologies.com
All 1000 scanned ports on analytics.tiktok.com (104.75.84.63) 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: 10 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 2.33 ms homerule.cpe (192.168.8.1)
2 ... 9
10 24.32 ms a104-75-84-63.deploy.static.akamaitechnologies.com (104.75.84.63)

NSE: Script Post-scanning.
Initiating NSE at 05:02
Completed NSE at 05:02, 0.00s elapsed
Initiating NSE at 05:02
Completed NSE at 05:02, 0.00s elapsed
Initiating NSE at 05:02
Completed NSE at 05:02, 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 36.98 seconds
Raw packets sent: 2053 (91.738KB) | Rcvd: 52 (4.008KB)

```

11.analytics-sg.tiktok.com

```

Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 5:08:16 AM ▾
Zenmap
Scan Tools Profile Help
Target: analytics-sg.tiktok.com ▾ Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v analytics-sg.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
analytics-sg.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:04 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Script Post-scanning.
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Initiating Ping Scan at 05:04
Scanning analytics-sg.tiktok.com (103.136.221.160) [4 ports]
Completed Ping Scan at 05:04, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:04
Completed Parallel DNS resolution of 1 host. at 05:04, 13.01s elapsed
Initiating SYN Stealth Scan at 05:04
Scanning analytics-sg.tiktok.com (103.136.221.160) [1000 ports]
SYN Stealth Scan Timing: About 40.10% done; ETC: 05:05 (0:00:46 remaining)
Completed SYN Stealth Scan at 05:05, 77.55s elapsed (1000 total ports)
Initiating Service scan at 05:05
Initiating OS detection (try #1) against analytics-sg.tiktok.com (103.136.221.160)
Initiating Traceroute at 05:05
Completed Traceroute at 05:05, 3.04s elapsed
Initiating Parallel DNS resolution of 10 hosts. at 05:05
Completed Parallel DNS resolution of 10 hosts. at 05:06, 13.01s elapsed
NSE: Script scanning 103.136.221.160.
Initiating NSE at 05:06
Completed NSE at 05:06, 0.01s elapsed
Initiating NSE at 05:06
Completed NSE at 05:06, 0.00s elapsed
Initiating NSE at 05:06

```

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 5:08:21 AM ▾

Zenmap

Scan Tools Profile Help

Target: analytics-sg.tiktok.com ▾ Profile: Intense scan ▾ Scan Cancel

Command: nmap -T4 -A -v analytics-sg.tiktok.com

Hosts Services

OS Host

analytics-sg.analytics-sg

Initiating NSE at 05:06, 0.00s elapsed
 Completed NSE at 05:06, 0.00s elapsed
 Initiating NSE at 05:06
 Completed NSE at 05:06, 0.00s elapsed
 Nmap scan report for **analytics-sg.tiktok.com** (103.136.221.160)
 Host is up (0.075s latency).
 Other addresses for **analytics-sg.tiktok.com** (not scanned): 103.136.221.161
 All 1000 scanned ports on **analytics-sg.tiktok.com** (103.136.221.160) 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 1.40 ms **homerouter.cpe** (192.168.8.1)
 2 ...
 3 43.78 ms 10.12.90.85
 4 46.71 ms 10.12.83.25
 5 69.29 ms 10.12.2.162
 6 43.82 ms 103.87.125.97
 7 45.33 ms 103.87.124.81
 8 93.15 ms 103.87.124.74
 9 75.36 ms 136699.sgw.equinix.com (27.111.229.190)
 10 83.69 ms 172.18.6.109
 11 75.54 ms 103.136.221.160

NSE: Script Post-scanning.

-/data/a.txt - Zenmap 1/2

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 5:08:24 AM ▾

Zenmap

Scan Tools Profile Help

Target: analytics-sg.tiktok.com ▾ Profile: Intense scan ▾ Scan Cancel

Command: nmap -T4 -A -v analytics-sg.tiktok.com

Hosts Services

OS Host

analytics-sg.analytics-sg

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

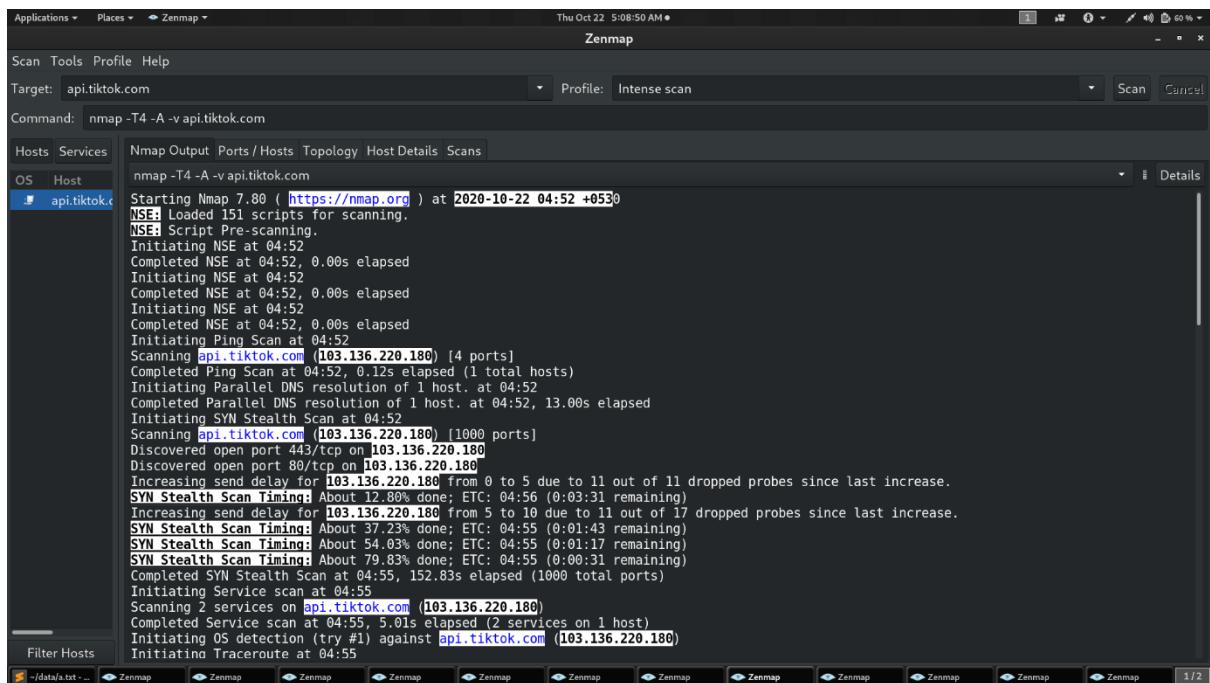
TRACEROUTE (using proto 1/icmp)
 HOP RTT ADDRESS
 1 1.40 ms **homerouter.cpe** (192.168.8.1)
 2 ...
 3 43.78 ms 10.12.90.85
 4 46.71 ms 10.12.83.25
 5 69.29 ms 10.12.2.162
 6 43.82 ms 103.87.125.97
 7 45.33 ms 103.87.124.81
 8 93.15 ms 103.87.124.74
 9 75.36 ms 136699.sgw.equinix.com (27.111.229.190)
 10 83.69 ms 172.18.6.109
 11 75.54 ms 103.136.221.160

NSE: Script Post-scanning.
 Initiating NSE at 05:06
 Completed NSE at 05:06, 0.00s elapsed
 Initiating NSE at 05:06
 Completed NSE at 05:06, 0.00s elapsed
 Initiating NSE at 05:06
 Completed NSE at 05:06, 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 112.99 seconds
 Raw packets sent: 2045 (91.514KB) | Rcvd: 21 (1.568KB)

Filter Hosts

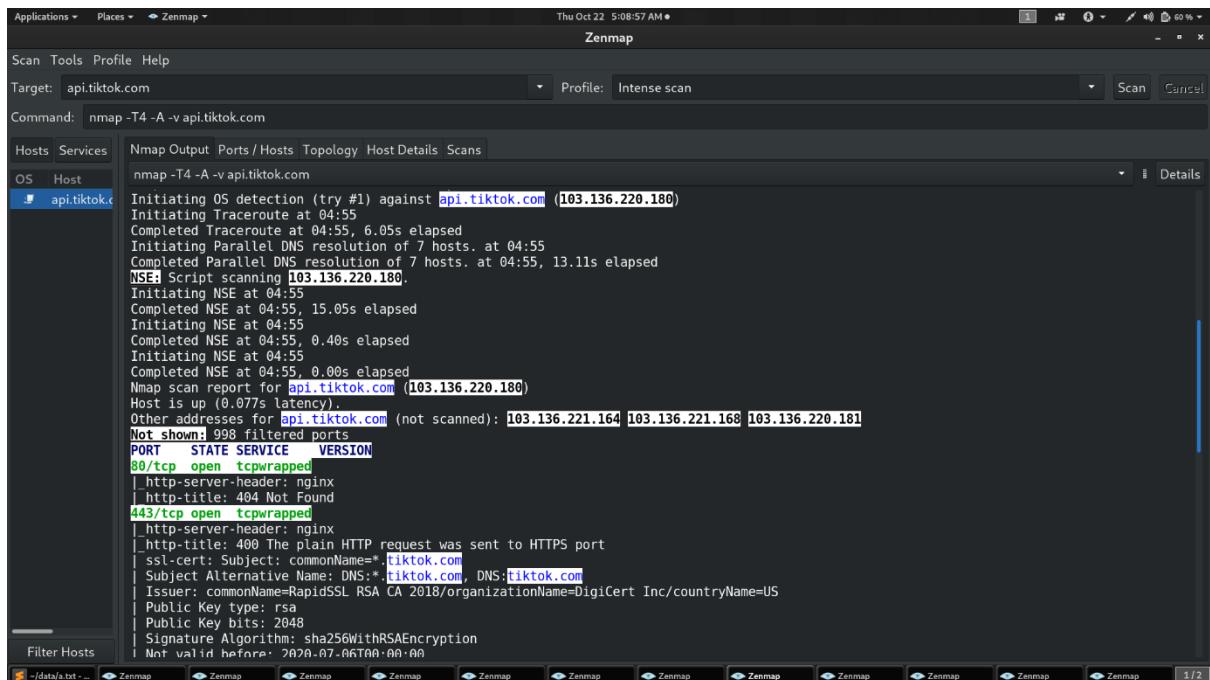
-/data/a.txt - Zenmap 1/2

12.api.tiktok.com



The screenshot shows the Zenmap interface performing an Nmap scan on the target host `api.tiktok.com`. The command used is `nmap -T4 -A -v api.tiktok.com`. The output window displays the following log:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:52 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:52
Completed NSE at 04:52, 0.00s elapsed
Initiating NSE at 04:52
Completed NSE at 04:52, 0.00s elapsed
Initiating NSE at 04:52
Completed NSE at 04:52, 0.00s elapsed
Initiating Ping Scan at 04:52
Scanning api.tiktok.com [103.136.220.180] (4 ports)
Completed Ping Scan at 04:52, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:52
Completed Parallel DNS resolution of 1 host. at 04:52, 13.00s elapsed
Initiating SYN Stealth Scan at 04:52
Scanning api.tiktok.com [103.136.220.180] (1000 ports)
Discovered open port 443/tcp on 103.136.220.180
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 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 12.80% done; ETC: 04:56 (0:03:31 remaining)
Increasing send delay for 103.136.220.180 from 5 to 10 due to 11 out of 17 dropped probes since last increase.
SYN Stealth Scan Timing: About 37.23% done; ETC: 04:55 (0:01:43 remaining)
SYN Stealth Scan Timing: About 54.03% done; ETC: 04:55 (0:01:17 remaining)
SYN Stealth Scan Timing: About 79.83% done; ETC: 04:55 (0:00:31 remaining)
Completed SYN Stealth Scan at 04:55, 152.83s elapsed (1000 total ports)
Initiating Service scan at 04:55
Scanning 2 services on api.tiktok.com [103.136.220.180]
Completed Service scan at 04:55, 5.01s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against api.tiktok.com [103.136.220.180]
Initiating Traceroute at 04:55
```



The screenshot shows the Zenmap interface performing an Nmap scan on the target host `api.tiktok.com` with OS detection enabled. The command used is `nmap -T4 -A -v -O api.tiktok.com`. The output window displays the following log:

```
Initiating OS detection (try #1) against api.tiktok.com [103.136.220.180]
Initiating Traceroute at 04:55
Completed Traceroute at 04:55, 6.05s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 04:55
Completed Parallel DNS resolution of 7 hosts. at 04:55, 13.11s elapsed
NSE: Script scanning 103.136.220.180.
Initiating NSE at 04:55
Completed NSE at 04:55, 15.05s elapsed
Initiating NSE at 04:55
Completed NSE at 04:55, 0.40s elapsed
Initiating NSE at 04:55
Completed NSE at 04:55, 0.00s elapsed
Nmap scan report for api.tiktok.com (103.136.220.180)
Host is up (0.077s latency).
Other addresses for api.tiktok.com (not scanned): 103.136.221.164 103.136.221.168 103.136.220.181
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp    open  tcpwrapped
|_http-server-header: nginx
|_http-title: 404 Not Found
443/tcp   open  tcpwrapped
|_http-server-header: nginx
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| 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
```

The screenshot shows the Zenmap interface with a scan completed for the target `api.tiktok.com`. The command used was `nmap -T4 -A -v api.tiktok.com`. The results tab is selected, displaying the following details:

- OS:** api.tiktok.com
- Public Key bits:** 2048
- Signature Algorithm:** sha256WithRSAEncryption
- Not valid before:** 2020-07-06T00:00:00
- Not valid after:** 2022-07-07T12:00:00
- MD5:** e593 3d6a 7ca4 d4f 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

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:u81_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: 18 hops

TCP Sequence Prediction: Difficulty=257 (Good luck!)

IP ID Sequence Generation: All zeros

TRACEROUTE (using port 443/tcp)

HOP	RTT	ADDRESS
1	3.63 ms	homerouter.cpe (192.168.8.1)
2	...	
3	27.36 ms	10.12.90.85
4	...	
5	34.24 ms	10.12.2.162
6	27.30 ms	103.87.125.97
7	...	8
9	70.64 ms	1386999.sgw.equinix.com (27.111.229.190)

The screenshot shows the Zenmap interface. The target is set to `api.tiktok.com`. The command entered is `nmap -T4 -A -v api.tiktok.com`. The results tab is selected, displaying the following output:

```
nmap -T4 -A -v api.tiktok.com
[ICP Sequence Prediction: Difficulty=257 (Good luck!)]
[IP ID Sequence Generation: All zeros]

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 3.63 ms homerouter.cpe (192.168.8.1)
2 ...
3 27.36 ms 10.12.90.85
4 ...
5 34.24 ms 10.12.2.162
6 27.30 ms 103.87.125.97
7 ...
8 ...
9 70.64 ms 138699.sgw.equinix.com (27.111.229.190)
10 ...
11 71.08 ms 100.124.112.0
12 ...
13 17 ...
14 78.10 ms 103.136.220.180

NSE: Script Post-scanning.
Initiating NSE at 04:55
Completed NSE at 04:55, 0.00s elapsed
Initiating NSE at 04:55
Completed NSE at 04:55, 0.00s elapsed
Initiating NSE at 04:55
Completed NSE at 04:55, 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 208.53 seconds
Raw packets sent: 3209 (143.554KB) | Rcvd: 73 (4.848KB)
```

13.api-m.tiktok.com

```
Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 5:09:41 AM ●
Zenmap
Scan Tools Profile Help
Target: api-m.tiktok.com
Profile: Intense scan
Command: nmap -T4 -A -v api-m.tiktok.com
Hosts Services
OS Host
api-m.tiktok.com
api-m.tiktok.com
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v api-m.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:55 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:55
Completed NSE at 04:55, 0.00s elapsed
Initiating NSE at 04:55
Completed NSE at 04:55, 0.00s elapsed
Initiating NSE at 04:55
Completed NSE at 04:55, 0.00s elapsed
Initiating Ping Scan at 04:55
Scanning api-m.tiktok.com (130.44.212.194) [4 ports]
Completed Ping Scan at 04:56, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:56
Completed Parallel DNS resolution of 1 host. at 04:56, 13.01s elapsed
Initiating SYN Stealth Scan at 04:56
Scanning api-m.tiktok.com (130.44.212.194) [1000 ports]
Discovered open port 443/tcp on 130.44.212.194
SYN Stealth Scan Timing: About 1.9% done; ETC: 05:22 (0:25:45 remaining)
Discovered open port 80/tcp on 130.44.212.194
SYN Stealth Scan Timing: About 14.50% done; ETC: 05:03 (0:06:00 remaining)
Increasing send delay for 130.44.212.194 from 0 to 5 due to 11 out of 17 dropped probes since last increase.
SYN Stealth Scan Timing: About 43.23% done; ETC: 04:59 (0:01:59 remaining)
SYN Stealth Scan Timing: About 53.83% done; ETC: 04:59 (0:01:44 remaining)
Increasing send delay for 130.44.212.194 from 5 to 10 due to 11 out of 15 dropped probes since last increase.
SYN Stealth Scan Timing: About 69.47% done; ETC: 04:59 (0:01:06 remaining)
Completed SYN Stealth Scan at 04:59, 197.83s elapsed (1000 total ports)
Initiating Service scan at 04:59
Scanning 2 services on api-m.tiktok.com (130.44.212.194)
Completed Service scan at 04:59, 13.40s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against api-m.tiktok.com (130.44.212.194)
Filter Hosts
Zenmap Zenmap
1 / 2
```

```
Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 5:09:47 AM ●
Zenmap
Scan Tools Profile Help
Target: api-m.tiktok.com
Profile: Intense scan
Command: nmap -T4 -A -v api-m.tiktok.com
Hosts Services
OS Host
api-m.tiktok.com
api-m.tiktok.com
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v api-m.tiktok.com
Completed service scan at 04:59, 13.40s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against api-m.tiktok.com (130.44.212.194)
Retrying OS detection (try #2) against api-m.tiktok.com (130.44.212.194)
Initiating Traceroute at 04:59
Completed Traceroute at 04:59, 6.28s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 04:59
Completed Parallel DNS resolution of 7 hosts. at 05:00, 13.01s elapsed
NSE: Script scanning 130.44.212.194.
Initiating NSE at 05:00
Completed NSE at 05:00, 17.47s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 2.00s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Nmap scan report for api-m.tiktok.com (130.44.212.194)
Host is up (0.23s latency).
Other addresses for api-m.tiktok.com (not scanned): 130.44.212.186 130.44.212.184 130.44.212.192
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx
443/tcp   open  ssl/http nginx
http-methods:
|_ Supported Methods: GET HEAD
|_ Http-title: 400 The plain HTTP request was sent to HTTPS port
|_ 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
Zenmap Zenmap
1 / 2
```

```
Applications Places Zenmap Thu Oct 22 5:09:56 AM • Zenmap
Scan Tools Profile Help Target: api-m.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v api-m.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host OS Host
api-m.tiktok Aggressive OS guesses: Linux 4.9 (87%), Linux 3.18 (86%), AVtech Room Alert 26W environmental monitor (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 24 hops
TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 2.08 ms homeroouter.cpe (192.168.8.1)
2 ...
3 32.73 ms 10.12.90.85
4 ...
5 32.39 ms 103.87.125.97
6 ...
7 ...
13 161.23 ms be2325.ccr32.bio02.atlas.cogentco.com [154.54.61.133]
14 242.82 ms be2332.ccr42.dca01.atlas.cogentco.com [154.54.85.245]
15 245.41 ms be3084.ccr41.lad02.atlas.cogentco.com [154.54.38.66]
16 ...
24 227.02 ms 130.44.212.194
NSE: Script Post-scanning.
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 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 271.85 seconds
Raw packets sent: 3225 (146.504KB) | Rcvd: 78 (5.118KB)
```

14.api-t.tiktok.com

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:56 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating Ping Scan at 04:56
Scanning api-t.tiktok.com [103.136.221.168] [4 ports]
Completed Ping Scan at 04:56, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:56
Completed Parallel DNS resolution of 1 host. at 04:56, 13.00s elapsed
Initiating SYN Stealth Scan at 04:56
Scanning api-t.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
Completed SYN Stealth Scan at 04:56, 22.31s elapsed (1000 total ports)
Initiating Service scan at 04:56
Scanning 2 services on api-t.tiktok.com [103.136.221.168]
Completed Service scan at 04:57, 20.60s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against api-t.tiktok.com [103.136.221.168]
Retrying OS detection (try #2) against api-t.tiktok.com [103.136.221.168]
Initiating Traceroute at 04:57
Completed Traceroute at 04:57, 5.08s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 04:57
Completed Parallel DNS resolution of 7 hosts. at 04:57, 13.00s elapsed
NSE: Script scanning 103.136.221.168.
Initiating NSE at 04:57
```

```
NSE: Script scanning 103.136.221.168.
Initiating NSE at 04:57
Completed NSE at 04:57, 16.48s elapsed
Initiating NSE at 04:57
Completed NSE at 04:57, 2.08s elapsed
Initiating NSE at 04:57
Completed NSE at 04:57, 0.00s elapsed
Nmap scan report for api-t.tiktok.com [103.136.221.168]
Host is up (0.079s latency).
Other addresses for api-t.tiktok.com (not scanned): 103.136.221.164 103.136.220.181 103.136.220.180
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=*.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
| MD5: 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-nextProtocols:
```

The screenshot shows the Zenmap interface with the following details:

- Target:** api.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v api.tiktok.com
- Hosts Services** tab is selected.
- Host:** api.tiktok.com (status: Up)
- Ports Output** tab is selected.
- Open ports:**
 - [ssl] 443/tcp (https)
 - [http] 80/tcp (http)
- Warning:** OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
- Device type:** WAP|general purpose|specialized
- Running OS:** Linux 2.4.X|2.6.X (91%), iPXE 1.X (90%)
- OS CPE:** cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/o:linux:linux_kernel:2.6.28 cpe:/o:ipxe:ipxe:1.0.0%2b
- Aggressive OS guesses:** Tomato 1.28 (Linux 2.4.20) (91%), Tomato firmware (Linux 2.6.22) (91%), Linux 2.6.28 (90%), iPXE 1.0.0+ (90%)
- No exact OS matches for host (test conditions non-ideal).**
- Network Distance:** 15 hops
- Traceroute (using port 443/tcp):**

HOP	RTT	ADDRESS
1	1.39 ms	homeroouter.cpe (192.168.8.1)
2	...	4
5	41.49 ms	10.12.2.162
6	41.85 ms	103.87.125.97
7	...	
8	92.86 ms	103.87.124.74
9	81.61 ms	138699.sgw.equinix.com (27.111.229.190)
10	86.64 ms	172.18.6.109
11	...	14
15	71.35 ms	103.136.221.168
- NSE:** Script Post-scanning.
Initiating NSE at 04:57
Completed NSE at 04:57, 0.00s elapsed
Initiating NSE at 04:57
Completed NSE at 04:57, 0.00s elapsed

```
Applications ▾ Places ▾ ◀ Zenmap ▾ Thu Oct 22 5:10:56 AM ⓘ Zenmap
Scan Tools Profile Help
Target: api-t.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v api-t.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans ⓘ Details
OS Host
api-t.tiktok.com OS [CPE] cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/o:linux:linux_kernel:2.6.28 cpe:/o:ipxe:ipxe:l.0.0%2b Aggressive OS guesses Tomato 1.28 (Linux 2.4.20) (91%), Tomato firmware (Linux 2.6.22) (91%), Linux 2.6.28 (90%), iPXE 1.0.0+ (90%) No exact OS matches for host (test conditions non-ideal). Network Distance: 15 hops
TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 1.39 ms homerouter.cpe (192.168.8.1)
2 ...
5 41.49 ms 10.12.2.162
6 41.85 ms 103.87.125.97
7 ...
8 92.86 ms 103.87.124.74
9 81.61 ms 138699.sgw.equinix.com (27.111.229.190)
10 86.64 ms 172.18.6.109
11 ...
15 71.35 ms 103.136.221.168

NSE: Script Post-scanning.
Initiating NSE at 04:57
Completed NSE at 04:57, 0.00s elapsed
Initiating NSE at 04:57
Completed NSE at 04:57, 0.00s elapsed
Initiating NSE at 04:57
Completed NSE at 04:57, 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 102.18 seconds
Raw packets sent: 2195 (100.900KB) | Rcvd: 38 (2.724KB)
```

15.artist.tiktok.com

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:56 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating Ping Scan at 04:56
Completed Ping Scan at 04:56
Scanning artist.tiktok.com (103.136.221.168) [4 ports]
Completed Ping Scan at 04:56, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:56
Completed Parallel DNS resolution of 1 host. at 04:56, 13.01s elapsed
Initiating SYN Stealth Scan at 04:56
Scanning artist.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 14 dropped probes since last increase.
SYN Stealth Scan Timing: About 17.35% done; ETC: 04:59 (0:02:28 remaining)
Increasing send delay for 103.136.221.168 from 5 to 10 due to 11 out of 13 dropped probes since last increase.
SYN Stealth Scan Timing: About 24.95% done; ETC: 05:00 (0:03:03 remaining)
SYN Stealth Scan Timing: About 36.65% done; ETC: 05:00 (0:02:48 remaining)
SYN Stealth Scan Timing: About 57.17% done; ETC: 05:00 (0:01:35 remaining)
SYN Stealth Scan Timing: About 67.62% done; ETC: 05:00 (0:01:15 remaining)
SYN Stealth Scan Timing: About 82.75% done; ETC: 05:00 (0:00:39 remaining)
Completed SYN Stealth Scan at 04:59, 211.24s elapsed (1000 total ports)
Initiating Service scan at 04:59
Scanning 2 services on artist.tiktok.com (103.136.221.168)
Completed Service scan at 05:00. 20.66s elapsed (2 services on 1 host)
```

```
Scanning 2 services on artist.tiktok.com (103.136.221.168)
Completed Service scan at 05:00. 20.66s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against artist.tiktok.com (103.136.221.168)
Retrying OS detection (try #2) against artist.tiktok.com (103.136.221.168)
Initiating Traceroute at 05:00
Completed Traceroute at 05:00, 5.07s elapsed
Initiating Parallel DNS resolution of 6 hosts. at 05:00
Completed Parallel DNS resolution of 6 hosts. at 05:00, 13.00s elapsed
NSE: Script scanning 103.136.221.168.
Initiating NSE at 05:00
Completed NSE at 05:00, 3.27s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 0.68s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Nmap scan report for artist.tiktok.com (103.136.221.168)
Host is up (0.078s latency).
Other addresses for artist.tiktok.com (not scanned): 103.136.220.180 103.136.220.181 103.136.221.164
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://www.tiktok.com/404
443/tcp   open  ssl/http nginx
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-title: TikTok
| Requested resource was https://www.tiktok.com/404
| ssl-cert: Subject: commonName=*.tiktok.com
```

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 5:13:41 AM •

Zenmap

Scan Tools Profile Help

Target: artist.tiktok.com

Profile: Intense scan

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

Hosts Services

OS Host

artist.tiktok

```
nmap -T4 -A -v artist.tiktok.com
Nmap Output Ports / Hosts Topology Host Details Scans
[+] OS DISCOVERY
  Requested resource was https://www.tiktok.com/404
  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
  MD5: 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
  Aggressive OS guesses: Linux 3.10 (98%), Linux 3.10 - 3.16 (98%), Linux 4.0 (98%), Linux 4.4 (98%), Linux 3.10 - 3.12 (98%), Linux 3.11 - 4.1 (98%), Linux 3.16 (98%), Linux 3.18 (98%), Linux 4.9 (98%), Linux 2.6.32 (96%)
  No exact OS matches for host (test conditions non-ideal).
  Network Distance: 15 hops
  TCP Sequence Prediction: Difficulty=258 (Good luck!)
  IP ID Sequence Generation: All zeros

  TRACEROUTE (using port 443/tcp)
  HOP RTT      ADDRESS
  1  1.49 ms  homerouter.cpe (192.168.8.1)
  2  ...
  3  32.54 ms 10.12.90.85
  4
  5
  6
  7
  8
  9
  10
  11
  12
  13
  14
  15
```

Filter Hosts

[-/data/nmap] [Zenmap] [Pictures] [1/2]

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 5:13:43 AM •

Zenmap

Scan Tools Profile Help

Target: artist.tiktok.com

Profile: Intense scan

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

Hosts Services

OS Host

artist.tiktok

```
nmap -T4 -A -v artist.tiktok.com
Nmap Output Ports / Hosts Topology Host Details Scans
[+] OS DISCOVERY
  No exact OS matches for host (test conditions non-ideal).
  Network Distance: 15 hops
  TCP Sequence Prediction: Difficulty=258 (Good luck!)
  IP ID Sequence Generation: All zeros

  TRACEROUTE (using port 443/tcp)
  HOP RTT      ADDRESS
  1  1.49 ms  homerouter.cpe (192.168.8.1)
  2  ...
  3  32.54 ms 10.12.90.85
  4
  5  34.48 ms 10.12.2.162
  6
  7  33.81 ms 103.87.124.81
  8  73.24 ms 103.87.124.74
  9
  10
  11
  12
  13
  14
  15  80.74 ms 103.136.221.168

  NSE: Script Post-scanning.
  Initiating NSE at 05:00
  Completed NSE at 05:00, 0.00s elapsed
  Initiating NSE at 05:00
  Completed NSE at 05:00, 0.00s elapsed
  Initiating NSE at 05:00
  Completed NSE at 05:00, 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 273.54 seconds
  Raw packets sent: 4313 (194.732KB) | Rcvd: 603 (56.232KB)
```

Filter Hosts

[-/data/nmap] [Zenmap] [Pictures] [1/2]

16.artists.tiktok.com

```
Applications Places Zenmap Thu Oct 22 5:14:31 AM • Zenmap
Scan Tools Profile Help Target: artists.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v artists.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host 4 artists.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:56 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating Ping Scan at 04:56
Scanning artists.tiktok.com (103.136.221.168) [4 ports]
Completed Ping Scan at 04:56, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:56
Completed Parallel DNS resolution of 1 host. at 04:56, 13.00s elapsed
Initiating SYN Stealth Scan at 04:56
Scanning artists.tiktok.com (103.136.221.168) [1000 ports]
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 17 dropped probes since last increase.
Increasing send delay for 103.136.221.168 from 5 to 10 due to 11 out of 16 dropped probes since last increase.
Completed SYN Stealth Scan at 04:57, 76.47s elapsed (1000 total ports)
Initiating Service scan at 04:57
Scanning 1 service on artists.tiktok.com (103.136.221.168)
Completed Service scan at 04:57, 7.19s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against artists.tiktok.com (103.136.221.168)
Initiating Traceroute at 04:57
Completed Traceroute at 04:58, 9.06s elapsed
Initiating Parallel DNS resolution of 1 host. at 04:58
Completed Parallel DNS resolution of 1 host. at 04:58, 0.00s elapsed
NSE: Script scanning 103.136.221.168.
Initiating NSE at 04:58
```

The screenshot shows the Zenmap interface with an 'Intense scan' profile applied. The target is set to 'artists.tiktok.com'. The 'Nmap Output' tab is selected, displaying the following results:

```
nmap -T4 -A -v artists.tiktok.com
[+] Starting Nmap 7.6.1 ( https://nmap.org ) at 2023-10-22 05:14:39 AM
[+] Completed Parallel DNS resolution of 1 host. at 04:58
NSE: Script scanning 103.136.221.168
Initiating NSE at 04:58
Completed NSE at 04:58, 11.22s elapsed
Initiating NSE at 04:58
Completed NSE at 04:58, 0.31s elapsed
Initiating NSE at 04:58
Completed NSE at 04:58, 0.00s elapsed
Nmap scan report for artists.tiktok.com (103.136.221.168)
Host is up (0.076s latency).
Other addresses for artists.tiktok.com (not scanned): 103.136.221.164 103.136.220.180 103.136.220.181
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx
|_http-methods:
|   _Supported Methods: OPTIONS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|general purpose
Running: Google Android 7.X, Linux 3.X|2.6.X
OS CPE: cpe:/o:google:android:7.1.2 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:2.6
OS details: Android 7.1.2 (Linux 3.10), Linux 2.6.18 - 2.6.22
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)
HOP RTT          ADDRESS
1  3.72 ms  homerouter.cpe [192.168.8.1]
2  ... 30

NSE: Script Post-scanning.
Total: 1 script(s) run (1:ok, 0:erro
```

```

Scan Tools Profile Help
Target: artists.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v artists.tiktok.com
Hosts Services
OS Host
● artists.tiktok.com
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx
| http-methods:
|_ Supported Methods: OPTIONS
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|general purpose
Running: Google Android 7.X, Linux 3.X|2.6.X
OS CPE: cpe:/o:google:android:7.1.2 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:2.6
OS details: Android 7.1.2 (Linux 3.10), Linux 2.6.18 - 2.6.22
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  3.72 ms  homerouter.cpe (192.168.8.1)
2  ... 30

NSE: Script Post-scanning.
Initiating NSE at 04:58
Completed NSE at 04:58, 0.00s elapsed
Initiating NSE at 04:58
Completed NSE at 04:58, 0.00s elapsed
Initiating NSE at 04:58
Completed NSE at 04:58, 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 120.61 seconds
Raw packets sent: 2196 (99.352KB) | Rcvd: 312 (33.168KB)

```

17.autodiscover.tiktok.com

```

Scan Tools Profile Help
Target: autodiscover.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v autodiscover.tiktok.com
Hosts Services
OS Host
● autodiscover.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 04:56 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating NSE at 04:56
Completed NSE at 04:56, 0.00s elapsed
Initiating Ping Scan at 04:56
Scanning autodiscover.tiktok.com (52.98.42.168) [4 ports]
Completed Ping Scan at 04:56, 0.11s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:56
Completed Parallel DNS resolution of 1 host. at 04:56, 13.00s elapsed
Initiating SYN Stealth Scan at 04:56
Scanning autodiscover.tiktok.com (52.98.42.168) [1000 ports]
Discovered open port 80/tcp on 52.98.42.168
Increasing send delay for 52.98.42.168 from 0 to 5 due to 11 out of 15 dropped probes since last increase.
SYN Stealth Scan Timing: About 27.67% done; ETC: 04:58 (0:01:21 remaining)
Increasing send delay for 52.98.42.168 from 5 to 10 due to 11 out of 17 dropped probes since last increase.
SYN Stealth Scan Timing: About 37.10% done; ETC: 04:59 (0:01:43 remaining)
SYN Stealth Scan Timing: About 55.10% done; ETC: 04:59 (0:01:14 remaining)
SYN Stealth Scan Timing: About 75.33% done; ETC: 04:59 (0:00:44 remaining)
Completed SYN Stealth Scan at 04:59, 168.45s elapsed (1000 total ports)
Initiating Service scan at 04:59
Scanning 1 service on autodiscover.tiktok.com (52.98.42.168)
Completed Service scan at 04:59, 7.18s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against autodiscover.tiktok.com (52.98.42.168)
Retrying OS detection (try #2) against autodiscover.tiktok.com (52.98.42.168)
Initiating Traceroute at 04:59

```

The screenshot shows the Zenmap interface with the following details:

- Target:** autodiscover.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v autodiscover.tiktok.com
- Hosts Services:** Hosts (selected), Services, Nmap Output, Ports / Hosts, Topology, Host Details, Scans
- OS:** Host
- Autodiscover:** 192.168.8.1 (tcp closed submission, 995/tcp closed pop3s)
- o14.ptr144:** 192.168.8.2 (Device type: general purpose|load balancer|WAP, OS: OpenBSD 4.0 (92%), FreeBSD 6.0 (92%), Citrix embedded (91%), Apple embedded (90%), OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:freebsd:freebsd:6.2 cpe:/h:apple:airport extreme)
- o2.ptr432:** 192.168.8.3 (Aggressive OS guesses: OpenBSD 4.0 (92%), FreeBSD 6.2-RELEASE (92%), OpenBSD 4.3 (92%), Citrix NetScaler load balancer (91%), Apple Airport Extreme WAP (99%), Citrix NetScaler VPX load balancer (89%), No exact OS matches for host (test conditions non-ideal), Network Distance: 16 hops, Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows)
- o15.ptr42:** 192.168.8.4 (Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows)
- Traceroute (using port 587/tcp):**

HOP	RTT	ADDRESS
1	2.96 ms	homerrouter.cpe (192.168.8.1)
2	...	
3	44.57 ms	10.12.98.85
4	28.77 ms	10.12.83.25
5	...	
6	40.43 ms	103.87.125.97
7	29.04 ms	103.87.124.81
8	...	15
16	74.00 ms	52.98.42.168
- NSE:** Script Post-scanning.
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
- Filter Hosts:** ~data/a.txt

```

Scan Tools Profile Help
Target: autodiscover.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v autodiscover.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
autodiscover
o14.ptr14
o2.ptr432
o15.ptr42
Aggressive OS guesses: OpenBSD 4.0 (92%), FreeBSD 6.2-RELEASE (92%), OpenBSD 4.3 (92%), Citrix NetScaler load balancer (91%), Apple Airport Extreme WAP (90%), Citrix NetScaler VPX load balancer (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 16 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
TRACEROUTE (using port 587/tcp)
HOP RTT ADDRESS
1 2.96 ms homerouter.cpe (192.168.8.1)
2 ...
3 44.57 ms 10.12.90.85
4 28.77 ms 10.12.83.25
5 ...
6 40.43 ms 103.87.125.97
7 29.04 ms 103.87.124.81
8 ...
16 74.00 ms 52.98.42.168
NSE: Script Post-scanning.
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 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 231.28 seconds
Raw packets sent: 3261 (148.310KB) | Rcvd: 93 (5.578KB)

```

18.business.tiktok.com

```

Scan Tools Profile Help
Target: business.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v business.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
business.tiktok.com
url7709.ac
url7709.ac
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:00 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating Ping Scan at 05:01
Scanning business.tiktok.com (104.75.84.63) [4 ports]
Completed Ping Scan at 05:01, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:01
Completed Parallel DNS resolution of 1 host. at 05:01, 0.02s elapsed
Initiating SYN Stealth Scan at 05:01
Scanning business.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 18 dropped probes since last increase.
SYN Stealth Scan Timing: About 39.15% done; ETC: 05:02 (0:00:48 remaining)
Increasing send delay for 104.75.84.63 from 5 to 10 due to 11 out of 19 dropped probes since last increase.
Completed SYN Stealth Scan at 05:01, 47.89s elapsed (1000 total ports)
Initiating Service scan at 05:01
Scanning 2 services on business.tiktok.com (104.75.84.63)
Completed Service scan at 05:02, 14.39s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against business.tiktok.com (104.75.84.63)
Retrying OS detection (try #2) against business.tiktok.com (104.75.84.63)
Initiating Traceroute at 05:02
Completed Traceroute at 05:02, 3.02s elapsed
Initiating Parallel DNS resolution of 9 hosts. at 05:02

```

Applications ▾ Places ▾ Zenmap ▾

The Oct 22 5:17:09 AM •

Zenmap

Scan Tools Profile Help

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

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

Hosts Services

OS Host

business.tiktok.com

Completed Traceroute at 05:02, 3.02s elapsed
 Initiating Parallel DNS resolution of 9 hosts. at 05:02
 Completed Parallel DNS resolution of 9 hosts. at 05:02, 13.00s elapsed
NSE: Script scanning 104.75.84.63
 Initiating NSE at 05:02
 Completed NSE at 05:02, 13.16s elapsed
 Initiating NSE at 05:02
 Completed NSE at 05:02, 2.10s elapsed
 Initiating NSE at 05:02
 Completed NSE at 05:02, 0.00s elapsed
 Nmap scan report for **business.tiktok.com** (104.75.84.63)
 Host is up (0.026s latency).
 Other addresses for **business.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	AkameiGHHost (Akamai's HTTP Acceleration/Mirror service)
		http-methods:	
		Supported Methods: POST	
443/tcp	open	ssl/http	AkameiGHHost (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 aa10 bb3e 309f f719	
		SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5	
		Aggressive OS guesses: Linux 4.0 (91%), Linux 3.11 - 4.1 (90%), Linux 4.4 (90%), Linux 2.6.32 (89%), Linux 2.6.32 - 2.6.33 (89%), Linux 2.6.32 - 2.6.35 (89%), Linux 2.6.32 or 3.10 (89%), Linux 3.10 - 3.12 (89%), Linux 3.16 (89%), Linux 3.18 (89%) No exact OS matches for host (test conditions non-ideal).	
		Network Distance: 10 hops	
TRACEROUTE (using port 53/tcp)			
HOP	RTT	ADDRESS	
1	3.88 ms	homerrouter.cpe (192.168.8.1)	
2	...		
3	43.23 ms	10.12.90.85	
4	37.51 ms	10.12.83.25	
5	53.26 ms	10.12.2.162	
6	32.72 ms	103.87.125.97	
7	28.00 ms	103.87.124.81	
8	38.00 ms	103.87.125.18	
9	33.13 ms	222.165.175.70	
10	27.78 ms	a104-75-84-63.deploy.static.akamaitechnologies.com (104.75.84.63)	

Filter Hosts

-/data/a.txt ... Zenmap Pictures 1/2

Applications ▾ Places ▾ Zenmap ▾

The Oct 22 5:17:18 AM •

Zenmap

Scan Tools Profile Help

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

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

Hosts Services

OS Host

business.tiktok.com

Completed Traceroute at 05:02, 3.02s elapsed
 Initiating Parallel DNS resolution of 9 hosts. at 05:02
 Completed Parallel DNS resolution of 9 hosts. at 05:02, 13.00s elapsed
NSE: Script scanning 104.75.84.63
 Initiating NSE at 05:02
 Completed NSE at 05:02, 13.16s elapsed
 Initiating NSE at 05:02
 Completed NSE at 05:02, 2.10s elapsed
 Initiating NSE at 05:02
 Completed NSE at 05:02, 0.00s elapsed
 Nmap scan report for **business.tiktok.com** (104.75.84.63)
 Host is up (0.026s latency).
 Other addresses for **business.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	AkameiGHHost (Akamai's HTTP Acceleration/Mirror service)
		http-methods:	
		Supported Methods: POST	
443/tcp	open	ssl/http	AkameiGHHost (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 aa10 bb3e 309f f719	
		SHA-1: 5af3 3d2f 77c1 df1c addf 183c a017 92f5 08cf a4c5	
		Aggressive OS guesses: Linux 4.0 (91%), Linux 3.11 - 4.1 (90%), Linux 4.4 (90%), Linux 2.6.32 (89%), Linux 2.6.32 - 2.6.33 (89%), Linux 2.6.32 - 2.6.35 (89%), Linux 2.6.32 or 3.10 (89%), Linux 3.10 - 3.12 (89%), Linux 3.16 (89%), Linux 3.18 (89%) No exact OS matches for host (test conditions non-ideal).	
		Network Distance: 10 hops	
TRACEROUTE (using port 53/tcp)			
HOP	RTT	ADDRESS	
1	3.88 ms	homerrouter.cpe (192.168.8.1)	
2	...		
3	43.23 ms	10.12.90.85	
4	37.51 ms	10.12.83.25	
5	53.26 ms	10.12.2.162	
6	32.72 ms	103.87.125.97	
7	28.00 ms	103.87.124.81	
8	38.00 ms	103.87.125.18	
9	33.13 ms	222.165.175.70	
10	27.78 ms	a104-75-84-63.deploy.static.akamaitechnologies.com (104.75.84.63)	

Filter Hosts

-/data/a.txt ... Zenmap Pictures 1/2

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 5:17:19 AM •

Zenmap

Scan Tools Profile Help

Target: business.tiktok.com Profile: Intense scan

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

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

business.tiktok.com

Aggressive OS guesses: Linux 4.0 (91%), Linux 3.11 - 4.1 (90%), Linux 4.4 (90%), Linux 2.6.32 (89%), Linux 2.6.32 - 2.6.33 (89%), Linux 2.6.32 - 2.6.35 (89%), Linux 2.6.32 or 3.10 (89%), Linux 3.10 - 3.12 (89%), Linux 3.16 (89%), Linux 3.18 (89%)
No exact OS matches for host (test conditions non-ideal).

Network Distance: 10 hops

TRACEROUTE (using port 53/tcp)

HOP RTT ADDRESS

```

1  3.88 ms homerouter.cpe (192.168.8.1)
2
3  43.23 ms 10.12.90.85
4  37.51 ms 10.12.83.25
5  53.26 ms 10.12.2.162
6  32.72 ms 103.87.125.97
7  28.08 ms 103.87.124.81
8  38.05 ms 103.87.125.18
9  33.13 ms 222.165.175.70
10 27.78 ms a104-75-84-63.deploy.static.akamaitechnologies.com (104.75.84.63)

```

NSE Script Post-scanning.

Initiating NSE at 05:02

Completed NSE at 05:02, 0.00s elapsed

Initiating NSE at 05:02

Completed NSE at 05:02, 0.00s elapsed

Initiating NSE at 05:02

Completed NSE at 05:02, 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 181.03 seconds

Raw packets sent: 2168 (100.236KB) | Rcvd: 380 (43.147KB)

Filter Hosts

-/data/a.txt... Zenmap Pictures 1/2

19.business-sso.tiktok.com

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 5:17:56 AM •

Zenmap

Scan Tools Profile Help

Target: business-sso.tiktok.com Profile: Intense scan

Command: nmap -T4 -A -v business-sso.tiktok.com

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

activity.tiktok.com

Starting Nmap 7.80 (<https://nmap.org>) at 2020-10-22 04:59 +0530

NSE: Loaded 151 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 04:59

Completed NSE at 04:59, 0.00s elapsed

Initiating NSE at 04:59

Completed NSE at 04:59, 0.00s elapsed

Initiating NSE at 04:59

Completed NSE at 04:59, 0.00s elapsed

Initiating NSE at 04:59

Completed NSE at 04:59, 0.00s elapsed

Initiating Ping Scan at 04:59

Scanning business-sso.tiktok.com (104.75.84.63) [4 ports]

Completed Ping Scan at 04:59, 0.09s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 04:59

Completed Parallel DNS resolution of 1 host. at 04:59, 0.03s elapsed

Initiating SYN Stealth Scan at 04:59

Scanning business-sso.tiktok.com (104.75.84.63) [1000 ports]

Discovered open port 80/tcp on 104.75.84.63

Discovered open port 443/tcp on 104.75.84.63

Completed SYN Stealth Scan at 05:00, 26.20s elapsed (1000 total ports)

Initiating Service scan at 05:00

Scanning 2 services on business-sso.tiktok.com (104.75.84.63)

Completed Service scan at 05:00, 13.23s elapsed (2 services on 1 host)

Initiating OS detection (try #1) against business-sso.tiktok.com (104.75.84.63)

Retrying OS detection (try #2) against business-sso.tiktok.com (104.75.84.63)

Initiating Traceroute at 05:00

Completed Traceroute at 05:00, 3.02s elapsed

Initiating Parallel DNS resolution of 9 hosts. at 05:00

Completed Parallel DNS resolution of 9 hosts. at 05:00, 13.02s elapsed

NSE: Script scanning 104.75.84.63.

Initiating NSE at 05:00

Filter Hosts

-/data/a.txt... Zenmap Pictures 1/2

Applications ▾ Places ▾ Zenmap ▾

The Oct 22 5:18:01 AM •

Zenmap

Scan Tools Profile Help

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

Command: nmap -T4 -A -v business-sso.tiktok.com

Hosts Services

OS Host

activity.tkt business-s

Completed Parallel DNS resolution of 9 hosts. at 05:00, 13.02s elapsed

[NSE] Script scanning 104.75.84.63.

Initiating NSE at 05:00

Completed NSE at 05:01, 2.11s elapsed

Initiating NSE at 05:01

Completed NSE at 05:01, 0.38s elapsed

Initiating NSE at 05:01

Completed NSE at 05:01, 0.00s elapsed

Nmap scan report for business-sso.tiktok.com (104.75.84.63)

Host is up (0.025s latency).

Other addresses for business-sso.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 OPTIONS
		http-server-header:	nginx
		http-title:	Site doesn't have a title (text/plain).
443/tcp	open	ssl/http	AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
		http-methods:	
		Supported Methods:	GET HEAD POST OPTIONS
		http-server-header:	nginx
		http-title:	Site doesn't have a title (text/plain).
		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 ... [Zenmap] Pictures 1/2

Applications ▾ Places ▾ Zenmap ▾

The Oct 22 5:18:08 AM •

Zenmap

Scan Tools Profile Help

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

Command: nmap -T4 -A -v business-sso.tiktok.com

Hosts Services

OS Host

activity.tkt business-s

http-title: Site doesn't have a title (text/plain).

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

MDS: 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/WAP]

Running (JUST GUESSING): Linux 4.X|3.X|2.6.X|2.4.X (91%), Synology DiskStation Manager 5.X (86%), WatchGuard Fireware 11.X (86%)

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 cpe:/o:linux:linux_kernel:2.4

Aggressive OS guesses: Linux 4.4 (91%), Linux 4.0 (91%), Linux 3.10 - 3.12 (90%), Linux 3.10 (90%), Linux 4.9 (89%), Linux 3.10 - 3.16 (89%), Linux 3.11 - 4.1 (87%), Linux 3.8 (87%), Linux 2.6.32 (87%), Linux 2.6.32 or 3.10 (87%)

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

Network Distance: 10 hops

TRACEROUTE (using port 53/tcp)

HOP	RTT	ADDRESS
1	3.41 ms	homerouter.cpe (192.168.8.1)
2	...	
3	42.91 ms	10.12.90.85
4	42.88 ms	10.12.83.25
5	42.92 ms	10.12.2.162
6	34.17 ms	103.87.125.97
7	33.62 ms	103.87.124.81
8	33.61 ms	103.87.125.18

Filter Hosts

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

```

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

Hosts Services
OS Host
activity.tiktok
business-sso.tiktok

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

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

TRACEROUTE (using port 53/tcp)
HOP RTT ADDRESS
1 3.41 ms homerouter.cpe (192.168.8.1)
2 ..
3 42.91 ms 10.12.90.85
4 42.88 ms 10.12.83.25
5 42.92 ms 10.12.2.162
6 34.17 ms 103.87.125.97
7 33.62 ms 103.87.124.81
8 33.61 ms 103.87.125.18
9 33.31 ms 222.165.175.74
10 30.17 ms a104-75-84-63.deploy.static.akamaitechnologies.com (104.75.84.63)

NSE: Script Post-scanning.
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 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 63.62 seconds
Raw packets sent: 3112 (139.61KB) | Rcvd: 514 (43.294KB)

```

20.business-useast2a.tiktok.com

```

Scan Tools Profile Help
Target: business-useast2a.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v business-useast2a.tiktok.com

Hosts Services
OS Host
ads.tiktok
business-t

Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v business-useast2a.tiktok.com

Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:00 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Initiating NSE at 05:00
Completed NSE at 05:00, 0.00s elapsed
Initiating Ping Scan at 05:00
Scanning business-useast2a.tiktok.com (147.160.184.34) [4 ports]
Completed Ping Scan at 05:00, 0.33s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:00
Completed Parallel DNS resolution of 1 host. at 05:00, 13.01s elapsed
Initiating SYN Stealth Scan at 05:00
Scanning business-useast2a.tiktok.com (147.160.184.34) [1000 ports]
Discovered open port 443/tcp on 147.160.184.34
Discovered open port 80/tcp on 147.160.184.34
NSE: SYN Stealth Scan Timing: About 46.00% done; ETC: 05:02 (0:00:36 remaining)
Completed SYN Stealth Scan at 05:01, 44.57s elapsed (1000 total ports)
Initiating Service scan at 05:01
Scanning 2 services on business-useast2a.tiktok.com (147.160.184.34)
Completed Service scan at 05:01, 14.68s elapsed (2 services on 1 host)
Initiating OSS detection (try #1) against business-useast2a.tiktok.com (147.160.184.34)
Initiating Traceroute at 05:02
Completed Traceroute at 05:02, 6.04s elapsed
Initiating Parallel DNS resolution of 3 hosts. at 05:02
Completed Parallel DNS resolution of 3 hosts. at 05:02, 13.10s elapsed
NSE: Script scanning 147.160.184.34.
Initiating NSE at 05:02

```

The screenshot shows the Zenmap interface with the following details:

- Target:** business-useast2a.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v business-useast2a.tiktok.com
- Hosts Services** tab is selected.
- OS Host** section shows:
 - ads.tiktok.com (IP: 147.160.184.34)
 - business-useast2a.tiktok.com (IP: 147.160.184.50)
- Nmap Output** tab is selected, displaying the following output for business-useast2a.tiktok.com:
 - Completed Parallel DNS resolution of 3 hosts. at 05:02, 13.10s elapsed
 - NSE: Script scanning 147.160.184.34.
 - Initiating NSE at 05:02
 - Completed NSE at 05:02, 17.81s elapsed
 - Initiating NSE at 05:02
 - Completed NSE at 05:02, 2.58s elapsed
 - Initiating NSE at 05:02
 - Completed NSE at 05:02, 0.00s elapsed
 - Nmap scan report for business-useast2a.tiktok.com (147.160.184.34)
 - Host is up (0.25s latency).
 - Other addresses for business-useast2a.tiktok.com (not scanned): 147.160.184.50
 - Not shown: 998 filtered ports
- Scans** tab is visible.
- Details** button is present.

Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 5:19:13 AM ▾

Zenmap

Scan Tools Profile Help

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

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

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host ads.tiktok

business-useast2a.tiktok.com

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: 16 hops

TRACEROUTE (using port 443/tcp)

HOP	RTT	ADDRESS
1	3.45 ms	homeroouter.cpe (192.168.8.1)
2	... 12	
13	232.88 ms	172.17.9.70
14	... 15	
16	244.15 ms	147.160.184.34

NSE: Script Post-scanning.

Initiating NSE at 05:02

Completed NSE at 05:02, 0.00s elapsed

Initiating NSE at 05:02

Completed NSE at 05:02, 0.00s elapsed

Initiating NSE at 05:02

Completed NSE at 05:02, 0.00s elapsed

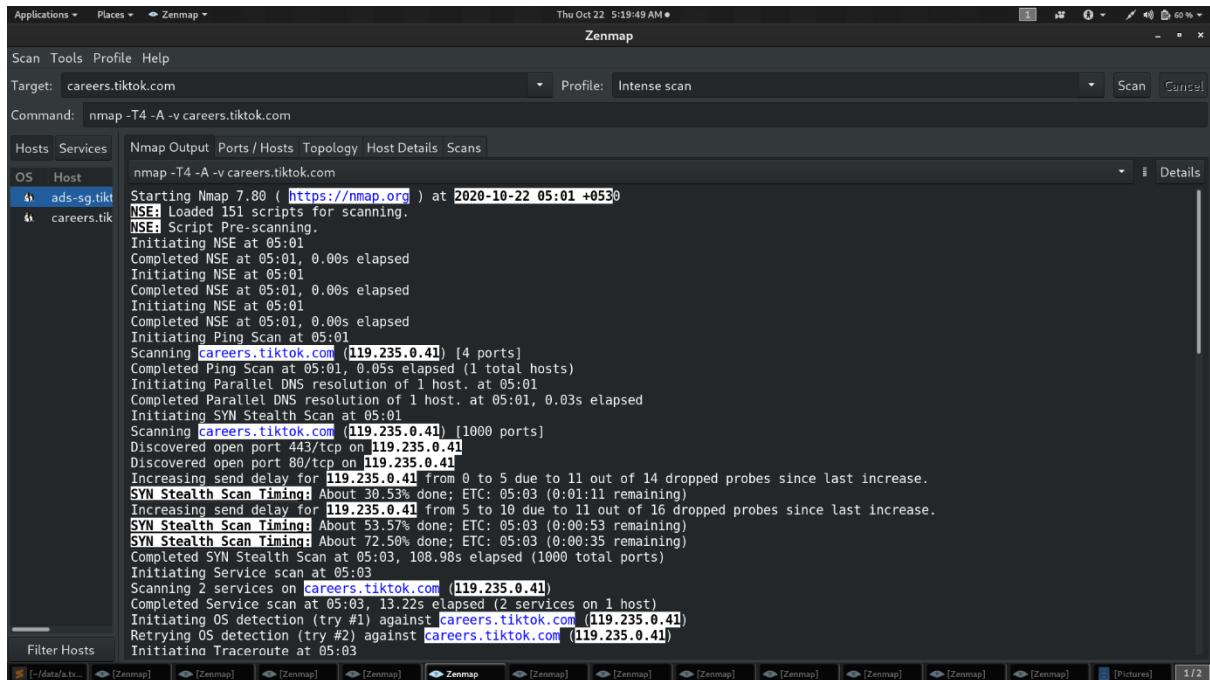
Read data files from: /usr/bin/../share/nmap

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

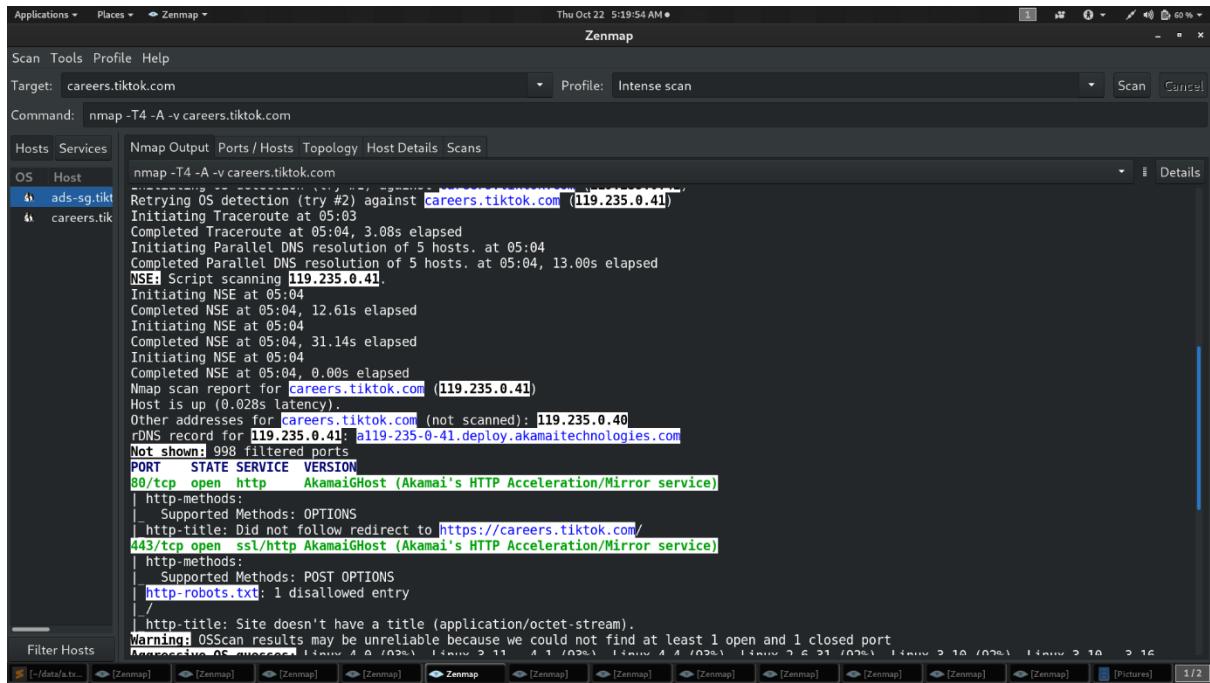
Nmap done: 1 IP address (1 host up) scanned in 118.95 seconds

Raw packets sent: 2143 (96.936KB) | Rcvd: 50 (2.920KB)

21.careers.tiktok.com



```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:01 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating NSE at 05:01
Completed NSE at 05:01, 0.00s elapsed
Initiating Ping Scan at 05:01
Scanning careers.tiktok.com [119.235.0.41] [4 ports]
Completed Ping Scan at 05:01, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:01
Completed Parallel DNS resolution of 1 host. at 05:01, 0.03s elapsed
Initiating SYN Stealth Scan at 05:01
Scanning careers.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 14 dropped probes since last increase.
SYN Stealth Scan Timing: About 30.53% done; ETC: 05:03 (0:01:11 remaining)
Increasing send delay for 119.235.0.41 from 5 to 10 due to 11 out of 16 dropped probes since last increase.
SYN Stealth Scan Timing: About 53.57% done; ETC: 05:03 (0:00:53 remaining)
SYN Stealth Scan Timing: About 72.50% done; ETC: 05:03 (0:00:35 remaining)
Completed SYN Stealth Scan at 05:03, 108.98s elapsed (1000 total ports)
Initiating Service scan at 05:03
Scanning 2 services on careers.tiktok.com [119.235.0.41]
Completed Service scan at 05:03, 13.22s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against careers.tiktok.com [119.235.0.41]
Retrying OS detection (try #2) against careers.tiktok.com [119.235.0.41]
Initiating Traceroute at 05:03
```



```
Retrying OS detection (try #2) against careers.tiktok.com [119.235.0.41]
Initiating Traceroute at 05:03
Completed Traceroute at 05:04, 3.08s elapsed
Initiating Parallel DNS resolution of 5 hosts. at 05:04
Completed Parallel DNS resolution of 5 hosts. at 05:04, 13.00s elapsed
NSE: Script scanning 119.235.0.41.
Initiating NSE at 05:04
Completed NSE at 05:04, 12.61s elapsed
Initiating NSE at 05:04
Completed NSE at 05:04, 31.14s elapsed
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Nmap scan report for careers.tiktok.com [119.235.0.41]
Host is up (0.028s latency).
Other addresses for careers.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-methods:
|_  Supported Methods: OPTIONS
| http-title: Did not follow redirect to https://careers.tiktok.com/
443/tcp   open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
| http-methods:
|_  Supported Methods: POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
| http-title: Site doesn't have a title (application/octet-stream).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

```

Applications Places Zenmap
Thu Oct 22 5:19:58 AM • Zenmap
Scan Tools Profile Help
Target: careers.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v careers.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
ads-sg.tiktok | http-robots.txt: 1 disallowed entry
|_ /
career.tiktok | http-title: Site doesn't have a title (application/octet-stream).
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: 6 hops

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 2.92 ms homerouter.cpe (192.168.8.1)
2 ...
3 34.69 ms 10.12.90.85
4 31.37 ms 10.12.83.25
5 31.64 ms 10.12.2.162
6 28.63 ms a119-235-0-41.deploy.akamaitechnologies.com (119.235.0.41)

NSE: Script Post-scanning.
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Initiating NSE at 05:04
Completed NSE at 05:04, 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 187.74 seconds
Raw packets sent: 3181 (142.732KB) | Rcvd: 91 (6.188KB)

```

22.cc.tiktok.com

```

Applications Places Zenmap
Thu Oct 22 5:20:49 AM • Zenmap
Scan Tools Profile Help
Target: cc.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v cc.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
analytics.tiktok | Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:04 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Initiating NSE at 05:04
Completed NSE at 05:04, 0.00s elapsed
Initiating Ping Scan at 05:04
Scanning cc.tiktok.com (119.235.0.40) [4 ports]
Completed Ping Scan at 05:04, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:04
Completed Parallel DNS resolution of 1 host. at 05:04, 0.03s elapsed
Initiating SYN Stealth Scan at 05:04
Scanning cc.tiktok.com (119.235.0.40) [1000 ports]
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 19 dropped probes since last increase.
Completed SYN Stealth Scan at 05:04, 37.68s elapsed (1000 total ports)
Initiating Service scan at 05:04
Scanning 2 services on cc.tiktok.com (119.235.0.40)
Completed Service scan at 05:05, 14.07s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against cc.tiktok.com (119.235.0.40)
Initiating Traceroute at 05:05
Completed Traceroute at 05:05, 3.01s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 05:05
Completed Parallel DNS resolution of 2 hosts. at 05:05, 0.00s elapsed
NSE: Script scanning 119.235.0.40.
Initiating NSE at 05:05

```



```

Thu Oct 22 5:21:01 AM •
Zenmap
Scan Tools Profile Help
Target: cc.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v cc.tiktok.com
Hosts Services
OS Host
analytics.cc.tiktok.com
| 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|WAPI phone
Running: iPAE 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: iPAE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone
Network Distance: 7 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 3.85 ms homerouter.cpe (192.168.8.1)
2 ... 6
7 33.60 ms a119-235-0-40.deploy.akamaitechnologies.com (119.235.0.40)

NSE: Script Post-scanning.
Initiating NSE at 05:05
Completed NSE at 05:05, 0.00s elapsed
Initiating NSE at 05:05
Completed NSE at 05:05, 0.00s elapsed
Initiating NSE at 05:05
Completed NSE at 05:05, 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 74.02 seconds
Raw packets sent: 2129 (96.660KB) | Rcvd: 16 (696B)

```

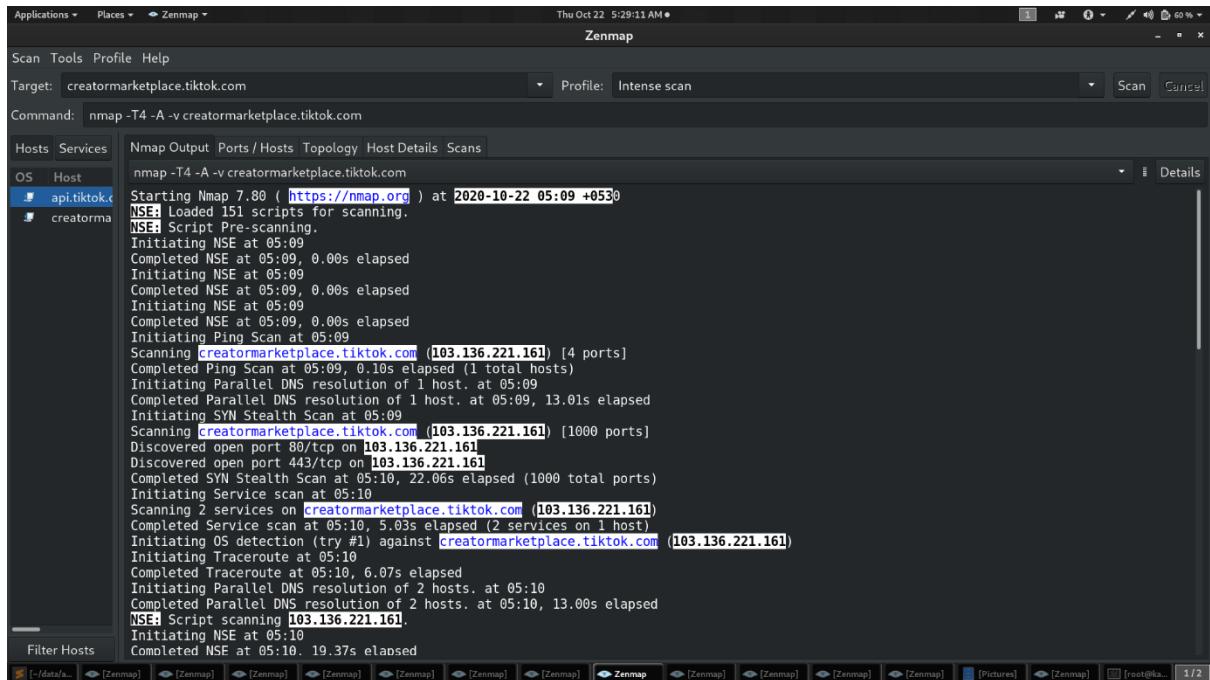
23.cc-test.tiktok.com

```

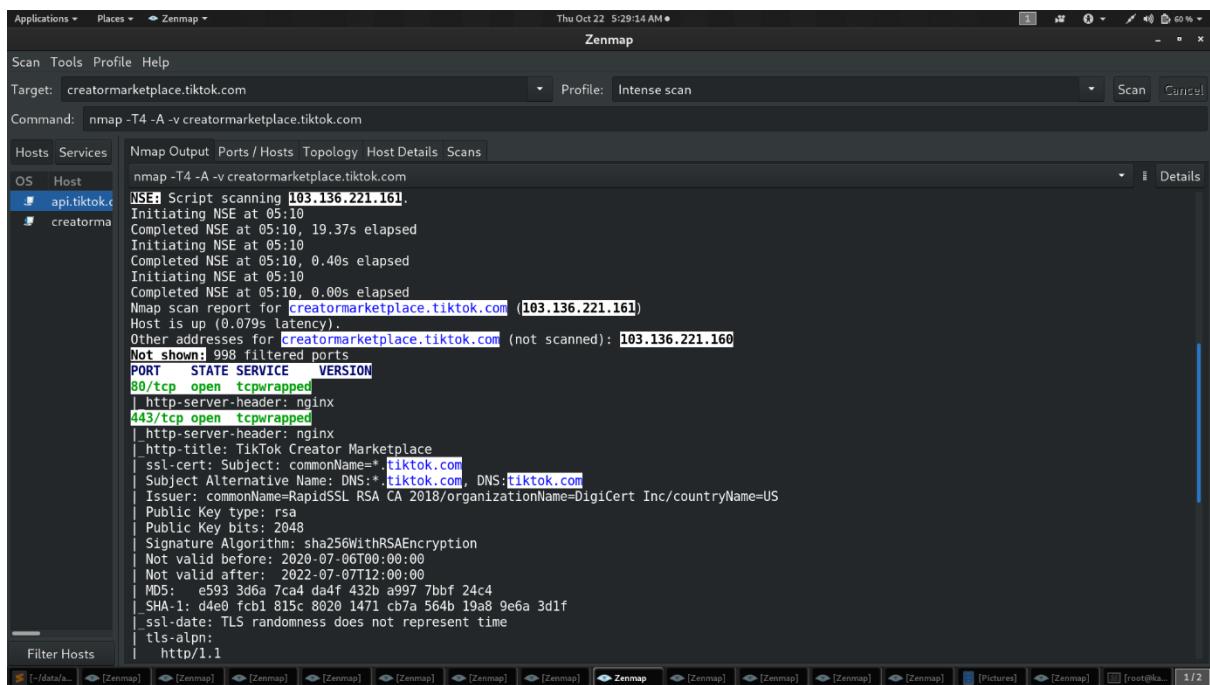
Thu Oct 22 5:22:43 AM •
Zenmap
Scan Tools Profile Help
Target: cc-test.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v cc-test.tiktok.com
Hosts Services
OS Host
analytics.cc-test.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:22 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:22
Completed NSE at 05:22, 0.00s elapsed
Initiating NSE at 05:22
Completed NSE at 05:22, 0.00s elapsed
Initiating NSE at 05:22
Completed NSE at 05:22, 0.00s elapsed
Failed to resolve "cc-test.tiktok.com".
NSE: Script Post-scanning.
Initiating NSE at 05:22
Completed NSE at 05:22, 0.00s elapsed
Initiating NSE at 05:22
Completed NSE at 05:22, 0.00s elapsed
Initiating NSE at 05:22
Completed NSE at 05:22, 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 5.44 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

```

24.creatormarketplace.tiktok.com

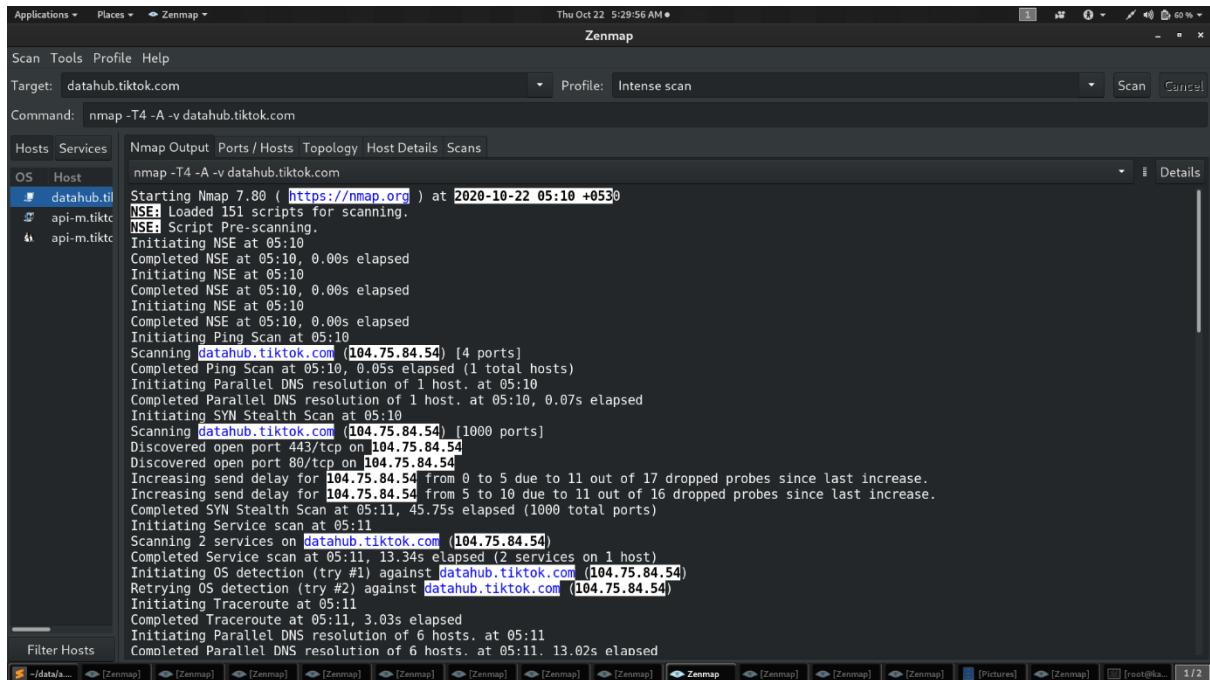


```
Thu Oct 22 5:29:11 AM • Zenmap
Scan Tools Profile Help
Target: creatormarketplace.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v creatormarketplace.tiktok.com
Hosts Services
OS Host
api.tiktok
creatorma
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v creatormarketplace.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:09 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:09
Completed NSE at 05:09, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 05:09
Completed Parallel DNS resolution of 1 host. at 05:09, 13.01s elapsed
Initiating SYN Stealth Scan at 05:09
Scanning creatormarketplace.tiktok.com [103.136.221.161] [1000 ports]
Discovered open port 80/tcp on 103.136.221.161
Discovered open port 443/tcp on 103.136.221.161
Completed SYN Stealth Scan at 05:10, 22.06s elapsed (1000 total ports)
Initiating Service scan at 05:10
Scanning 2 services on creatormarketplace.tiktok.com [103.136.221.161]
Completed Service scan at 05:10, 5.03s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against creatormarketplace.tiktok.com [103.136.221.161]
Initiating Traceroute at 05:10
Completed Traceroute at 05:10, 6.07s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 05:10
Completed Parallel DNS resolution of 2 hosts. at 05:10, 13.00s elapsed
NSE: Script scanning 103.136.221.161.
Initiating NSE at 05:10
Completed NSE at 05:10, 19.37s elapsed
1/2
```

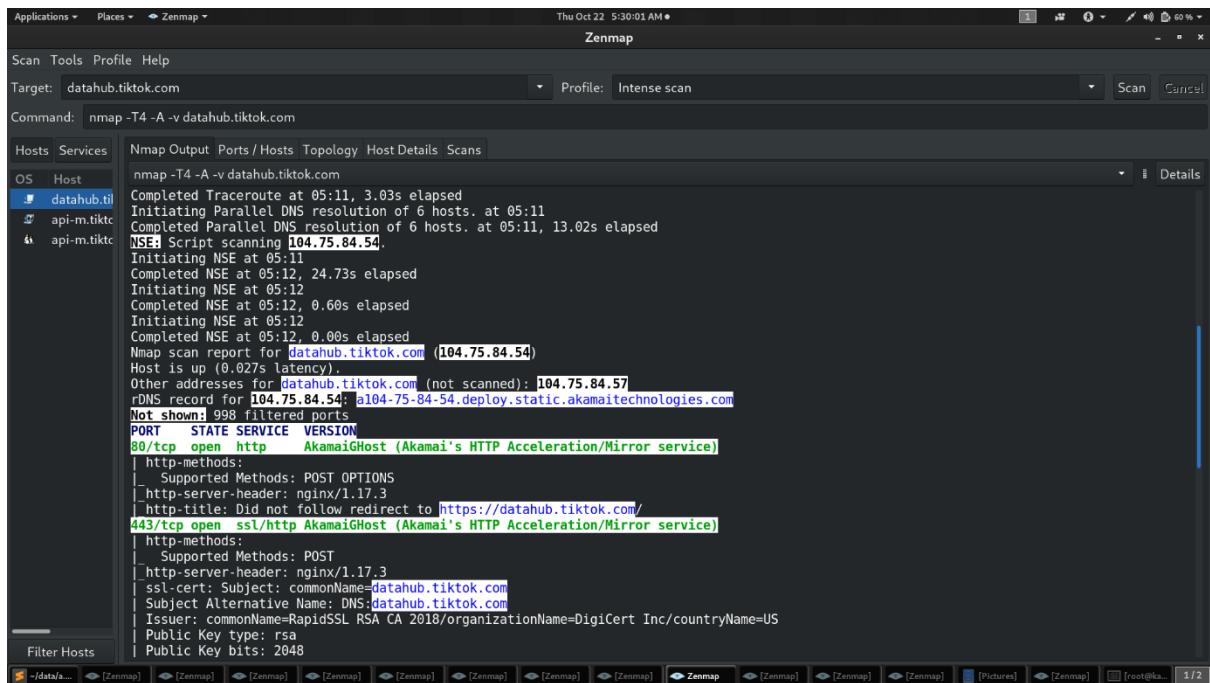


```
Thu Oct 22 5:29:14 AM • Zenmap
Scan Tools Profile Help
Target: creatormarketplace.tiktok.com Profile: Intense scan
Command: nmap -T4 -A -v creatormarketplace.tiktok.com
Hosts Services
OS Host
api.tiktok
creatorma
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v creatormarketplace.tiktok.com
NSE: Script scanning 103.136.221.161.
Initiating NSE at 05:10
Completed NSE at 05:10, 19.37s elapsed
Initiating NSE at 05:10
Completed NSE at 05:10, 0.40s elapsed
Initiating NSE at 05:10
Completed NSE at 05:10, 0.00s elapsed
Nmap scan report for creatormarketplace.tiktok.com [103.136.221.161]
Host is up (0.079s latency).
Other addresses for creatormarketplace.tiktok.com (not scanned): 103.136.221.160
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp      open  tcpwrapped
|_http-server-header: nginx
443/tcp     open  tcpwrapped
|_http-server-header: nginx
|_http-title: TikTok Creator Marketplace
|_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
1/2
```


25.datahub.tiktok.com



```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:10 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:10
Completed NSE at 05:10, 0.00s elapsed
Initiating NSE at 05:10
Completed NSE at 05:10, 0.00s elapsed
Initiating NSE at 05:10
Completed NSE at 05:10, 0.00s elapsed
Initiating Ping Scan at 05:10
Scanning datahub.tiktok.com [104.75.84.54] (4 ports)
Completed Ping Scan at 05:10, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:10
Completed Parallel DNS resolution of 1 host. at 05:10, 0.07s elapsed
Initiating SYN Stealth Scan at 05:10
Scanning datahub.tiktok.com [104.75.84.54] (1000 ports)
Discovered open port 443/tcp on 104.75.84.54
Discovered open port 80/tcp on 104.75.84.54
Increasing send delay for 104.75.84.54 from 0 to 5 due to 11 out of 17 dropped probes since last increase.
Increasing send delay for 104.75.84.54 from 5 to 10 due to 11 out of 16 dropped probes since last increase.
Completed SYN Stealth Scan at 05:11, 45.75s elapsed (1000 total ports)
Initiating Service scan at 05:11
Scanning 2 services on datahub.tiktok.com [104.75.84.54]
Completed Service scan at 05:11, 13.34s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against datahub.tiktok.com [104.75.84.54]
Retrying OS detection (try #2) against datahub.tiktok.com [104.75.84.54]
Initiating Traceroute at 05:11
Completed Traceroute at 05:11, 3.03s elapsed
Initiating Parallel DNS resolution of 6 hosts. at 05:11
Completed Parallel DNS resolution of 6 hosts. at 05:11, 13.02s elapsed
```



```
Completed Traceroute at 05:11, 3.03s elapsed
Initiating Parallel DNS resolution of 6 hosts. at 05:11
Completed Parallel DNS resolution of 6 hosts. at 05:11, 13.02s elapsed
NSE: Script scanning 104.75.84.54.
Initiating NSE at 05:11
Completed NSE at 05:12, 24.73s elapsed
Initiating NSE at 05:12
Completed NSE at 05:12, 0.60s elapsed
Initiating NSE at 05:12
Completed NSE at 05:12, 0.00s elapsed
Nmap scan report for datahub.tiktok.com (104.75.84.54)
Host is up (0.027s latency).
Other addresses for datahub.tiktok.com (not scanned): 104.75.84.57
rDNS record for 104.75.84.54: el04-75-84-54.deploy.static.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: POST OPTIONS
|_http-server-header: nginx/1.17.3
|_http-title: Did not follow redirect to https://datahub.tiktok.com/
443/tcp     open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-methods:
|_Supported Methods: POST
|_http-server-header: nginx/1.17.3
|_ssl-cert: Subject: commonName=datahub.tiktok.com
|_Subject Alternative Name: DNS:datahub.tiktok.com
|_Issuer: commonName=RapidSSL RSA CA 2018/organizationName=DigiCert Inc/countryName=US
|_Public Key type: rsa
|_Public Key bits: 2048
```

Scan Tools Profile Help

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

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

Hosts Services

OS Host

datahub.tiktok

api-m.tiktok

api-m.tiktok

Nmap Output Ports / Hosts Topology Host Details Scans

443/tcp Open ssl/http Akamai's HTTP Acceleration/Mirror Service

| http-methods:

| | Supported Methods: POST

| | http-server-header: nginx/1.17.3

| | ssl-cert: Subject: commonName=datahub.tiktok.com

| | Subject Alternative Name: DNS: datahub.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: 2020-06-25T00:00:00

| | Not valid after: 2022-06-26T12:00:00

| | MD5: f3ae 0411 cfab b401 c5a3 2d3b 7a91 f570

| | SHA-1: 9853 bac7 9d60 17e3 6f06 30a3 a760 dcbb 2a63 7e62

| | SHA-256: 33c9 3a20 3a20 3a20 3a20 3a20 3a20 3a20 3a20 3a20

| | SHA-3: 33c9 3a20 3a20 3a20 3a20 3a20 3a20 3a20 3a20 3a20

| | SHA-512: 33c9 3a20 3a20 3a20 3a20 3a20 3a20 3a20 3a20 3a20

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

Aggressive OS guesses: Cisco Unified Communications Manager VoIP adapter (93%), Linux 2.6.26 (PCLinuxOS) (93%), Linux 2.6.30 (93%), Linux 2.6.28 (93%), Linux 2.6.18 - 2.6.22 (92%), Linux 2.6.18 (88%), Linux 2.6.22.1-32.fc6 (x86, SMP) (87%), Linux 2.6.39 (87%), Oracle Enterprise Linux 6 (Linux 2.6.32) (87%), Linux 3.10 (87%)

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

Uptime guess: 33.296 days (since Fri Sep 18 22:05:16 2020)

Network Distance: 12 hops

TRACEROUTE (using port 443/tcp)

HOP RTT ADDRESS

1 3.24 ms homerouter.cpe (192.168.8.1)

2 ...

3 26.83 ms 10.12.90.85

4 ...

5 27.76 ms 10.12.2.162

6 28.79 ms 103.87.125.97

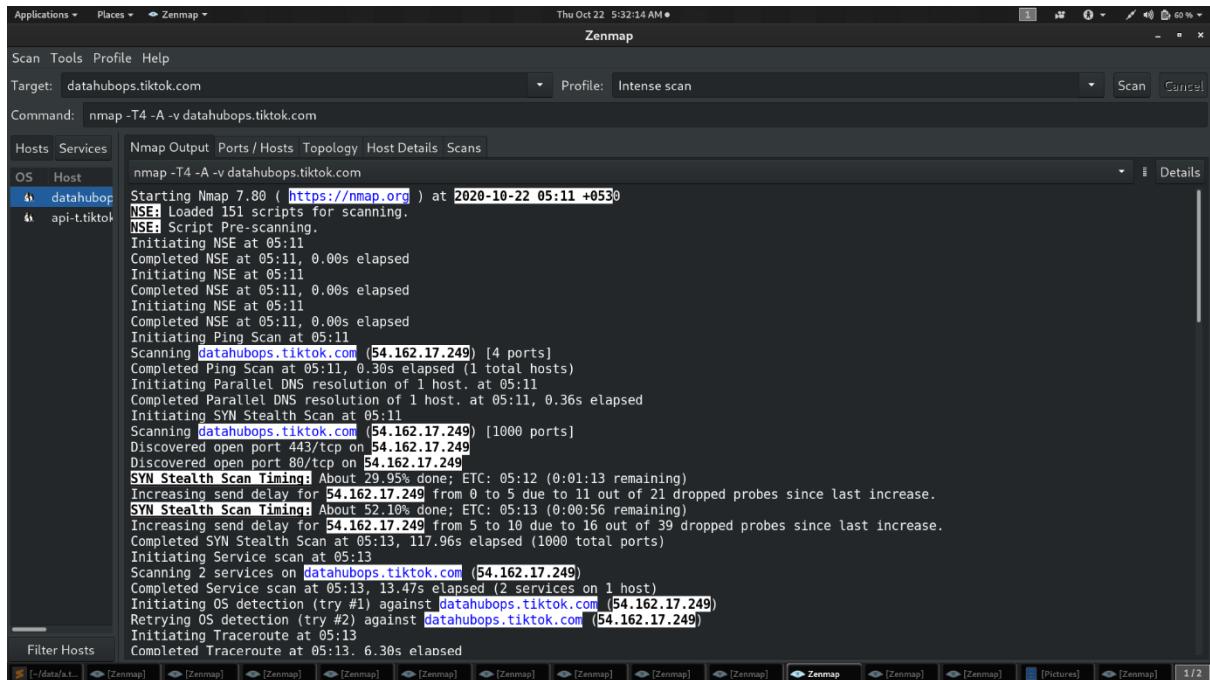
```
Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 5:30:10 AM ⓘ 90 %
Scan Tools Profile Help
Target: datahub.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v datahub.tiktok.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
datahub.tiktok Linux 6 (Linux 2.6.32) (87%), Linux 3.10 (87%)
api-m.tiktok No exact OS matches for host (test conditions non-ideal).
Uptime guess: 33,296 days (since Fri Sep 18 22:05:16 2020)
Network Distance: 12 hops

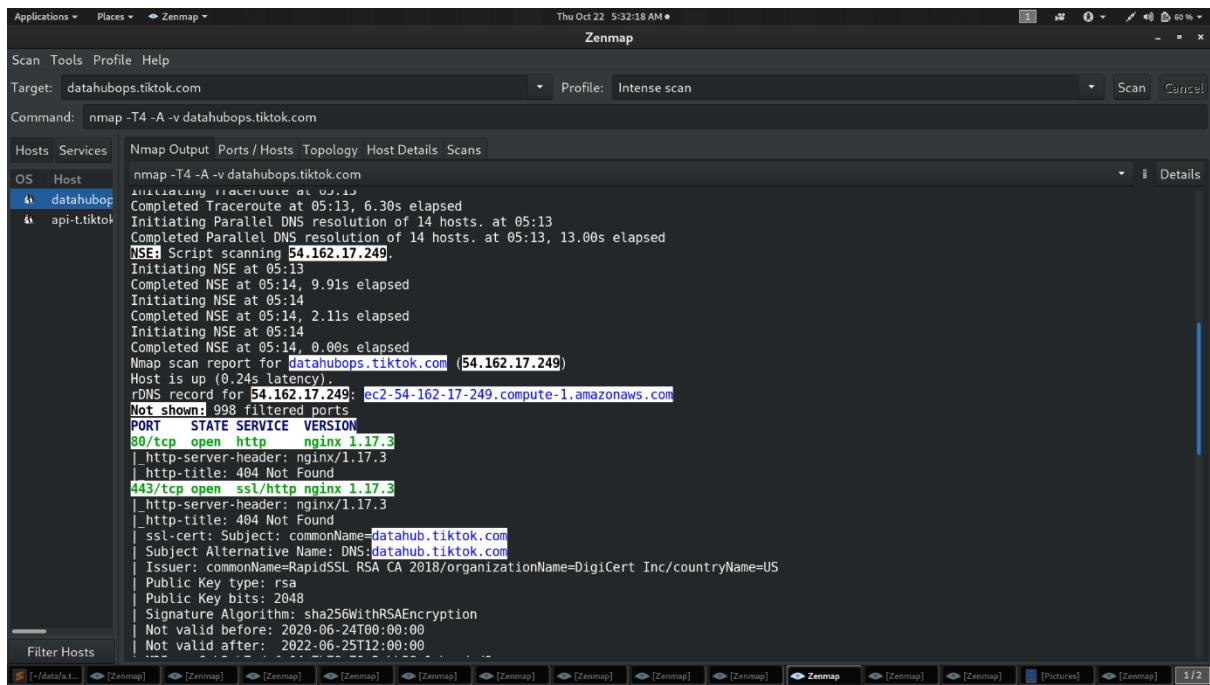
    TRACEROUTE (using port 443/tcp)
    HOP RTT      ADDRESS
    1  3.24 ms  homerouter.cpe (192.168.8.1)
    2 ...
    3  26.83 ms 10.12.90.85
    4 ...
    5  27.76 ms 10.12.2.162
    6  28.79 ms 103.87.125.97
    7 ...
    8  29.25 ms 103.87.125.18
    9 ...
   12  19.71 ms a104-75-84-54.deploy.static.akamaitechnologies.com (104.75.84.54)

NSE: Script Post-scanning.
Initiating NSE at 05:12
Completed NSE at 05:12, 0.00s elapsed
Initiating NSE at 05:12
Completed NSE at 05:12, 0.00s elapsed
Initiating NSE at 05:12
Completed NSE at 05:12, 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 112.65 seconds
Raw packets sent: 2176 (98.824KB) | Rcvd: 36 (2.708KB)
```

26.datahubops.tiktok.com



```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:11 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:11
Completed NSE at 05:11, 0.00s elapsed
Initiating NSE at 05:11
Completed NSE at 05:11, 0.00s elapsed
Initiating NSE at 05:11
Completed NSE at 05:11, 0.00s elapsed
Initiating Ping Scan at 05:11
Scanning datahubops.tiktok.com (54.162.17.249) [4 ports]
Completed Ping Scan at 05:11, 0.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:11
Completed Parallel DNS resolution of 1 host. at 05:11, 0.36s elapsed
Initiating SYN Stealth Scan at 05:11
Scanning datahubops.tiktok.com (54.162.17.249) [1000 ports]
Discovered open port 443/tcp on 54.162.17.249
Discovered open port 80/tcp on 54.162.17.249
SYN Stealth Scan Timing: About 29.95% done; ETC: 05:12 (0:01:13 remaining)
Increasing send delay for 54.162.17.249 from 0 to 5 due to 11 out of 21 dropped probes since last increase.
SYN Stealth Scan Timing: About 52.18% done; ETC: 05:13 (0:06:56 remaining)
Increasing send delay for 54.162.17.249 from 5 to 10 due to 16 out of 39 dropped probes since last increase.
Completed SYN Stealth Scan at 05:13, 117.96s elapsed (1000 total ports)
Initiating Service scan at 05:13
Scanning 2 services on datahubops.tiktok.com (54.162.17.249)
Completed Service scan at 05:13, 13.47s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against datahubops.tiktok.com (54.162.17.249)
Retrying OS detection (try #2) against datahubops.tiktok.com (54.162.17.249)
Initiating Traceroute at 05:13
Completed Traceroute at 05:13, 6.30s elapsed
```



```
Initiating Traceroute at 05:13
Completed Traceroute at 05:13, 6.30s elapsed
Initiating Parallel DNS resolution of 14 hosts. at 05:13
Completed Parallel DNS resolution of 14 hosts. at 05:13, 13.00s elapsed
NSE: Script scanning 54.162.17.249.
Initiating NSE at 05:13
Completed NSE at 05:14, 0.91s elapsed
Initiating NSE at 05:14
Completed NSE at 05:14, 2.11s elapsed
Initiating NSE at 05:14
Completed NSE at 05:14, 0.00s elapsed
Nmap scan report for datahubops.tiktok.com (54.162.17.249)
Host is up (0.24s latency).
rDNS record for 54.162.17.249: ec2-54-162-17-249.compute-1.amazonaws.com
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx 1.17.3
|_http-server-header: nginx/1.17.3
|_http-title: 404 Not Found
443/tcp   open  ssl/http nginx 1.17.3
|_http-server-header: nginx/1.17.3
|_http-title: 404 Not Found
| ssl-cert: Subject: commonName=datahub.tiktok.com
| Subject Alternative Name: DNS:datahub.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: 2020-06-24T00:00:00
| Not valid after:  2022-06-25T12:00:00
```

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 5:32:23 AM •

Zenmap

Scan Tools Profile Help

Target: `datahubops.tiktok.com` ▾ Profile: Intense scan Scan Cancel

Command: `nmap -T4 -A -v datahubops.tiktok.com`

Hosts Services

OS Host

- datahubop** ⓘ
- api-t.tiktok ⓘ

```
nmap -T4 -A -v datahubops.tiktok.com
[...]
|_ Not valid before: 2020-06-24T00:00:00
|_ Not valid after: 2022-06-25T12:00:00
|_ MD5: 6ab3 b7cd fc04 7b78 70a3 bb38 1cbe ded9
|_ SHA-1: 2364 9b5e 52e1 b51f 8993 72eb e416 d177 bab3 b104
|_ 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
Aggressive OS guesses: Linux 4.2 (98%), Linux 4.0 (97%), Linux 2.6.32 (97%), Linux 2.6.32 or 3.10 (97%), Linux 2.6.35 (97%), Linux 3.5 (97%), Linux 4.4 (97%), Linux 4.8 (97%), Synology DiskStation Manager 5.1 (97%), WatchGuard Fireware 11.8 (97%)
No exact OS matches for host (test conditions non-ideal).

TRACEROUTE (using port 443/tcp)
HOP RTT ADDRESS
1 2.32 ms homeroouter.cpe (192.168.8.1)
2 ...
3 52.25 ms 10.12.90.85
4 42.40 ms 10.12.83.25
5 44.78 ms 10.12.2.162
6 37.76 ms 103.87.125.97
7 37.06 ms 103.87.124.81
8 42.66 ms 103.87.124.130
9 52.72 ms ix-xe-1-0-3-tcore1.mlv-mumbai.as6453.net (180.87.38.182)
10 251.79 ms if-ae-2-2.tcore2.mlv-mumbai.as6453.net (180.87.38.2)
11 246.92 ms if-ae-12-2.tcore1.l78-london.as6453.net (180.87.39.21)
12 228.70 ms if-ae-66-2.tcore2.nto-newyork.as6453.net (80.231.130.106)
13 236.68 ms if-ae-12-2.tcore1.n75-newyork.as6453.net (66.110.96.5)
```

Filter Hosts

[1/2]

Applications ▾ Places ▾ Zenmap ▾

Thu Oct 22 5:32:25 AM •

Zenmap

Scan Tools Profile Help

Target: `datahubops.tiktok.com` ▾ Profile: Intense scan Scan Cancel

Command: `nmap -T4 -A -v datahubops.tiktok.com`

Hosts Services

OS Host

- datahubop** ⓘ
- api-t.tiktok ⓘ

```
nmap -T4 -A -v datahubops.tiktok.com
[...]
1 2.32 ms homeroouter.cpe (192.168.8.1)
2 ...
3 52.25 ms 10.12.90.85
4 42.40 ms 10.12.83.25
5 44.78 ms 10.12.2.162
6 37.76 ms 103.87.125.97
7 37.06 ms 103.87.124.81
8 42.66 ms 103.87.124.130
9 52.72 ms ix-xe-1-0-3-tcore1.mlv-mumbai.as6453.net (180.87.38.182)
10 251.79 ms if-ae-2-2.tcore2.mlv-mumbai.as6453.net (180.87.38.2)
11 246.92 ms if-ae-12-2.tcore1.l78-london.as6453.net (180.87.39.21)
12 228.70 ms if-ae-66-2.tcore2.nto-newyork.as6453.net (80.231.130.106)
13 236.68 ms if-ae-12-2.tcore1.n75-newyork.as6453.net (66.110.96.5)
14 232.58 ms 66.110.96.157
15 237.38 ms 52.93.31.35
16 222.01 ms 66.110.96.157
17 ... 30

NSE: Script Post-scanning.
Initiating NSE at 05:14
Completed NSE at 05:14, 0.00s elapsed
Initiating NSE at 05:14
Completed NSE at 05:14, 0.00s elapsed
Initiating NSE at 05:14
Completed NSE at 05:14, 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 171.33 seconds
Raw packets sent: 4086 (185.120KB) | Rcvd: 146 (8.990KB)
```

Filter Hosts

[1/2]

27.dev.tiktok.com

```
Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 5:32:44 AM ●
Zenmap
Scan Tools Profile Help
Target: dev.tiktok.com
Profile: Intense scan
Command: nmap -T4 -A -v dev.tiktok.com
Hosts Services
OS Host
Artist.tiktok
dev.tiktok.
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v dev.tiktok.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:14 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:14
Completed NSE at 05:14, 0.00s elapsed
Initiating NSE at 05:14
Completed NSE at 05:14, 0.00s elapsed
Initiating NSE at 05:14
Completed NSE at 05:14, 0.00s elapsed
Initiating Ping Scan at 05:14
Completed Ping Scan at 05:14, 0.27s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:14
Completed Parallel DNS resolution of 1 host. at 05:14, 0.97s elapsed
Initiating SYN Stealth Scan at 05:14
Scanning dev.tiktok.com [209.127.230.3] [1000 ports]
Completed SYN Stealth Scan at 05:14, 30.31s elapsed (1000 total ports)
Initiating Service scan at 05:14
Initiating OS detection (try #1) against dev.tiktok.com [209.127.230.3]
Retrying OS detection (try #2) against dev.tiktok.com [209.127.230.3]
Initiating Traceroute at 05:14
Completed Traceroute at 05:15, 6.01s elapsed
Initiating Parallel DNS resolution of 11 hosts. at 05:15
Completed Parallel DNS resolution of 11 hosts. at 05:15, 13.02s elapsed
NSE: Script scanning 209.127.230.3.
Initiating NSE at 05:15
Completed NSE at 05:15, 0.01s elapsed
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Filter Hosts
[1/2]
```

```
Applications ▾ Places ▾ Zenmap ▾
Thu Oct 22 5:32:48 AM ●
Zenmap
Scan Tools Profile Help
Target: dev.tiktok.com
Profile: Intense scan
Command: nmap -T4 -A -v dev.tiktok.com
Hosts Services
OS Host
Artist.tiktok
dev.tiktok.
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v dev.tiktok.com
Completed NSE at 05:15, 0.00s elapsed
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Nmap scan report for dev.tiktok.com (209.127.230.3)
Host is up (0.26s latency).
rDNS record for 209.127.230.3: s00.bc.larksuite.com
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    closed http
443/tcp   closed https
1935/tcp  closed rtmp
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 2.6.22 (90%), Linux 2.6.31 (90%), Linux 3.2 (90%), Cisco Wireless LAN controller (90%), Android 5.0.1 (90%), Linksys WET54G wireless bridge (90%), Linksys WRV200 wireless broadband router (90%), Linksys NAS200 NAS device (90%), DD-WRT v24-sp2 (Linux 2.4.36) (90%), Linux 2.6.18 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 21 hops
TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  1.72 ms  homeroouter.cpe (192.168.8.1)
2  ...
3  30.97 ms 10.12.98.85
4  32.78 ms 10.12.83.25
5  22.16 ms 10.12.2.162
6  26.98 ms 103.87.125.97
7  17.36 ms 103.87.124.81
8  136.74 ms 103.87.124.146
9  136.62 ms te0-5-0-17.201.agr21.mrs01.atlas.cogentco.com (149.14.124.137)
10  126.00 ms 103.87.124.146
[1/2]
```

The screenshot shows the Zenmap interface with the following details:

- Target:** dev.tiktok.com
- Profile:** Intense scan
- Command:** nmap -T4 -A -v dev.tiktok.com
- Hosts Services** tab is selected.
- OS Host** section shows:
 - Artist.tiktok (blue icon)
 - dev.tiktok (green icon)
- Network Distance:** 21 hops
- Traceroute (using port 80/tcp):**

HOP RTT	ADDRESS
1 1.72 ms	homeroouter.cpe (192.168.8.1)
2 ...	
3 30.97 ms	10.12.90.85
4 32.78 ms	10.12.83.25
5 22.16 ms	10.12.2.162
6 26.98 ms	103.87.125.97
7 17.36 ms	103.87.124.81
8 136.74 ms	103.87.124.146
9 136.62 ms	te0 5 0 17.201.agr21.mrs01.atlas.cogentco.com (149.14.124.137)
10 136.92 ms	be2345.ccr21.mrs01.atlas.cogentco.com (154.54.38.169)
11 148.50 ms	be3223.ccr31.vlc62.atlas.cogentco.com (154.54.57.210)
12 ... 20	
21 230.83 ms	s00.bc.larksuite.com (209.127.230.3)
- NSE:** Script Post-scanning.
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Initiating NSE at 05:15
Completed NSE at 05:15, 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 59.09 seconds
- Raw packets sent: 2099 (95.638KB) | Rcvd: 27 (2.422KB)

28.developer.tiktok.com

```
Applications ▾ Places ▾ Zenmap ▾ Thu Oct 22 5:33:27 2020 60 %
Zenmap
Scan Tools Profile Help
Target: developer.tiktok.com Profile: Intense scan Scan Cancel
Command: nmap -T4 -A -v developer.tiktok.com
Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
NSE
artist.tiktok
developer.tiktok
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-22 05:14 +0530
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Initiating Ping Scan at 05:15
Scanning developer.tiktok.com [130.44.212.161] [4 ports]
Completed Ping Scan at 05:15, 0.33s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:15
Completed Parallel DNS resolution of 1 host. at 05:15, 13.00s elapsed
Initiating SYN Stealth Scan at 05:15
Scanning developer.tiktok.com [130.44.212.161] [1000 ports]
Discovered open port 80/tcp on 130.44.212.161
Discovered open port 443/tcp on 130.44.212.161
Completed SYN Stealth Scan at 05:15, 28.88s elapsed (1000 total ports)
Initiating Service scan at 05:15
Scanning 2 services on developer.tiktok.com [130.44.212.161]
Completed Service scan at 05:15, 14.47s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against developer.tiktok.com [130.44.212.161]
Retrying OS detection (try #2) against developer.tiktok.com [130.44.212.161]
Initiating Traceroute at 05:16
Completed Traceroute at 05:16, 3.31s elapsed
Initiating Parallel DNS resolution of 15 hosts. at 05:16
Completed Parallel DNS resolution of 15 hosts. at 05:16, 13.01s elapsed
NSE: Script scanning [130.44.212.161].
Initiating NSE at 05:16
Filter Hosts
```


Scan Tools Profile Help

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

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

Hosts Services

OS Host

1 artists.tiktok.com

2 ...

3 53.26 ms 19.12.90.85

4 40.58 ms 19.12.83.25

5 40.84 ms 19.12.2.162

6 40.60 ms 103.87.125.97

7 32.96 ms 103.87.124.81

8 142.99 ms 103.87.124.38

9 153.60 ms te0-5-0-17.201.agr21.mrs01.atlas.cogentco.com (149.14.124.137)

10 144.53 ms be2345.ccr21.mrs01.atlas.cogentco.com (154.54.38.169)

11 154.75 ms be3222.ccr31.vlc02.atlas.cogentco.com (154.54.57.206)

12 151.70 ms be3356.ccr32.mad05.atlas.cogentco.com (154.54.57.241)

13 151.86 ms be2325.ccr32.bio02.atlas.cogentco.com (154.54.61.133)

14 222.78 ms be2331.ccr41.dca01.atlas.cogentco.com (154.54.85.241)

15 244.95 ms be3083.ccr41.lad02.atlas.cogentco.com (154.54.30.54)

16 ... 23

24 226.74 ms 130.44.212.161

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 102.20 seconds

Raw packets sent: 2145 (98.808KB) | Rcvd: 54 (3.528KB)