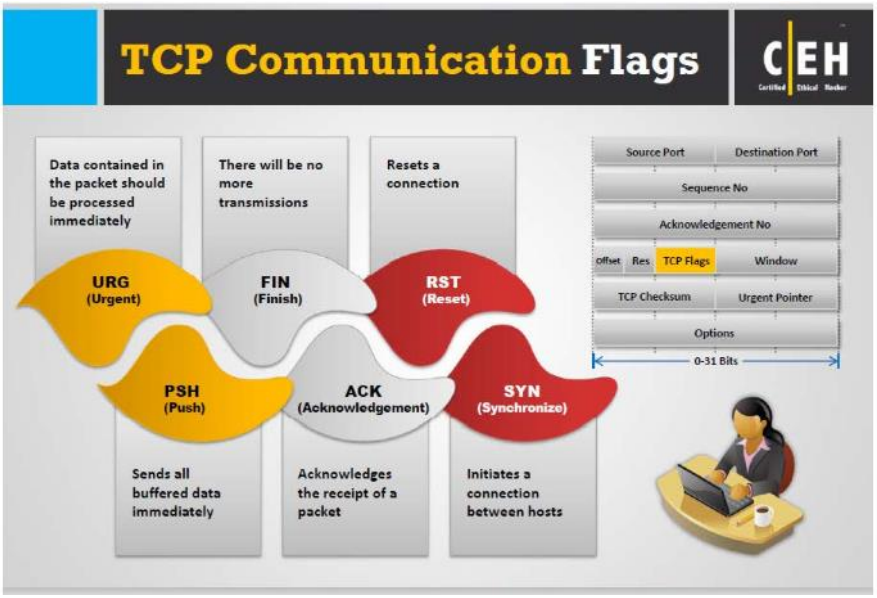
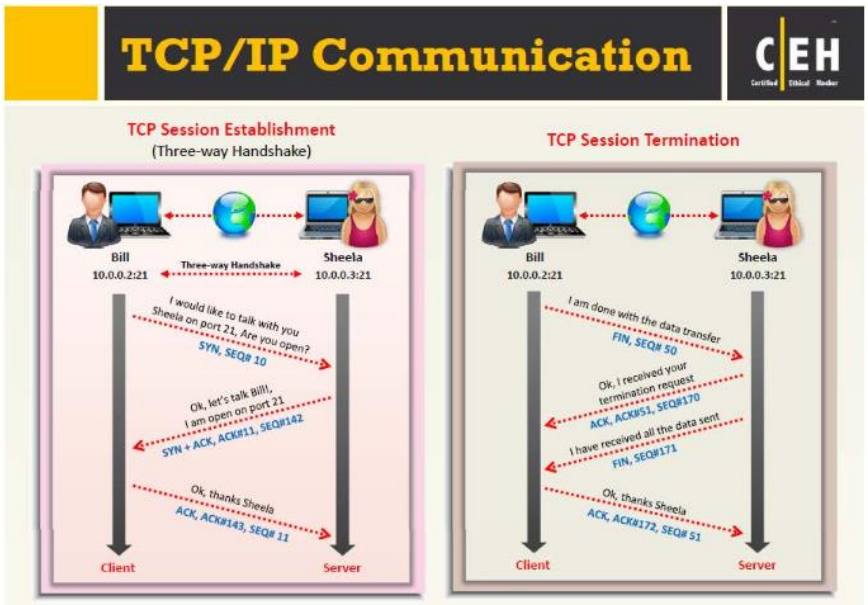
Analisis Network Scanning Phase Result dengan target Website the-gazette.com

Network scanning merujuk kepada serangkaian prosedur untuk identifikasi host, port, dan layanan dalam jaringan. Network scanning ialah salah satu bagian dari pengumpulan yang pintas seorang attacker yang gunakan untuk membuat profil dari organisasi target.

Objektif dari Network Scanning

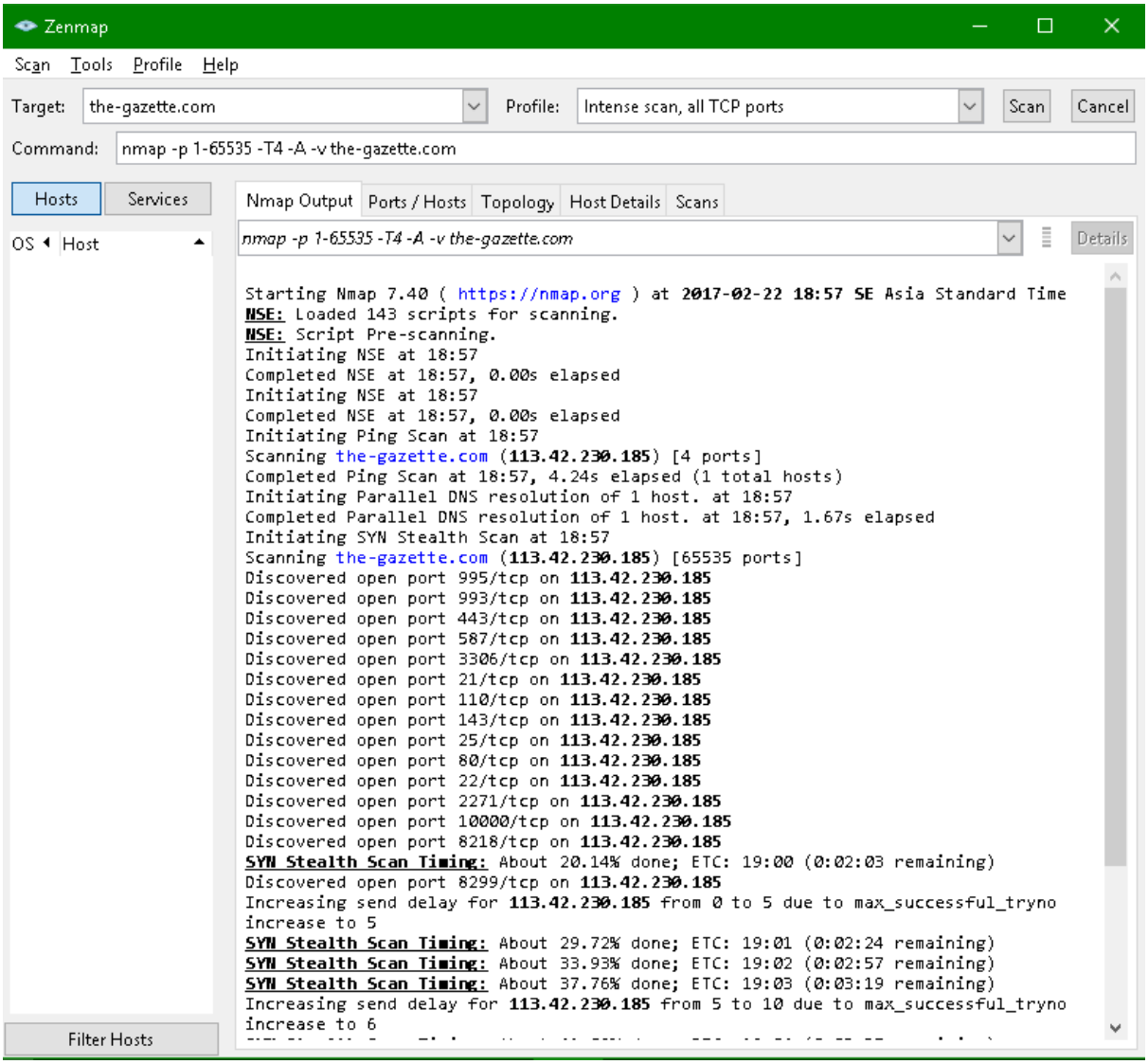
- Untuk menemukan host yang aktif, alamat IP, dan port-port dari host yang aktif
- Untuk menemukan OS dan arsitektur system
- Untuk menemukan layanan yang berjalan pada host
- Untuk menemukan kelemahan pada host yang aktif

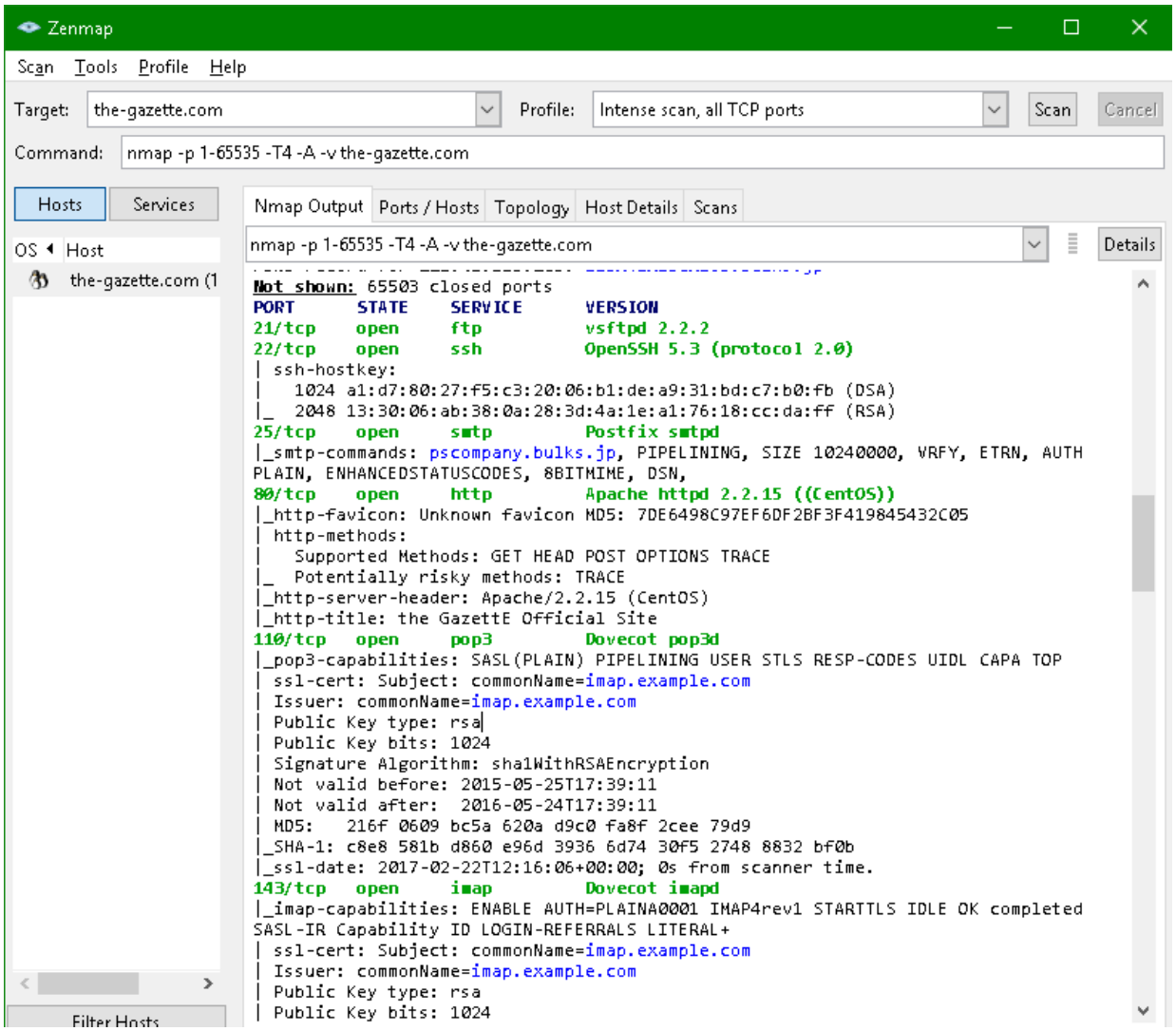


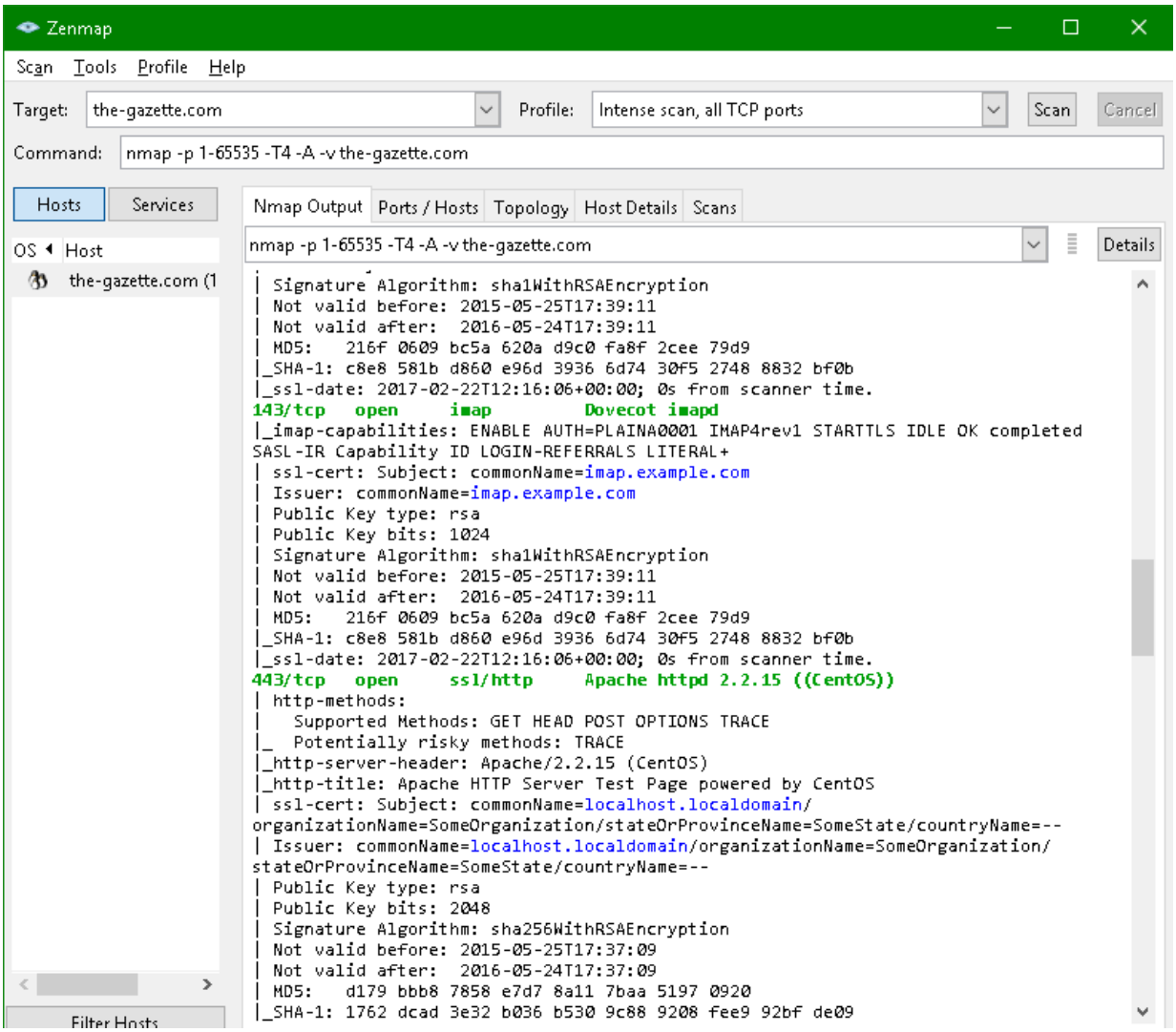


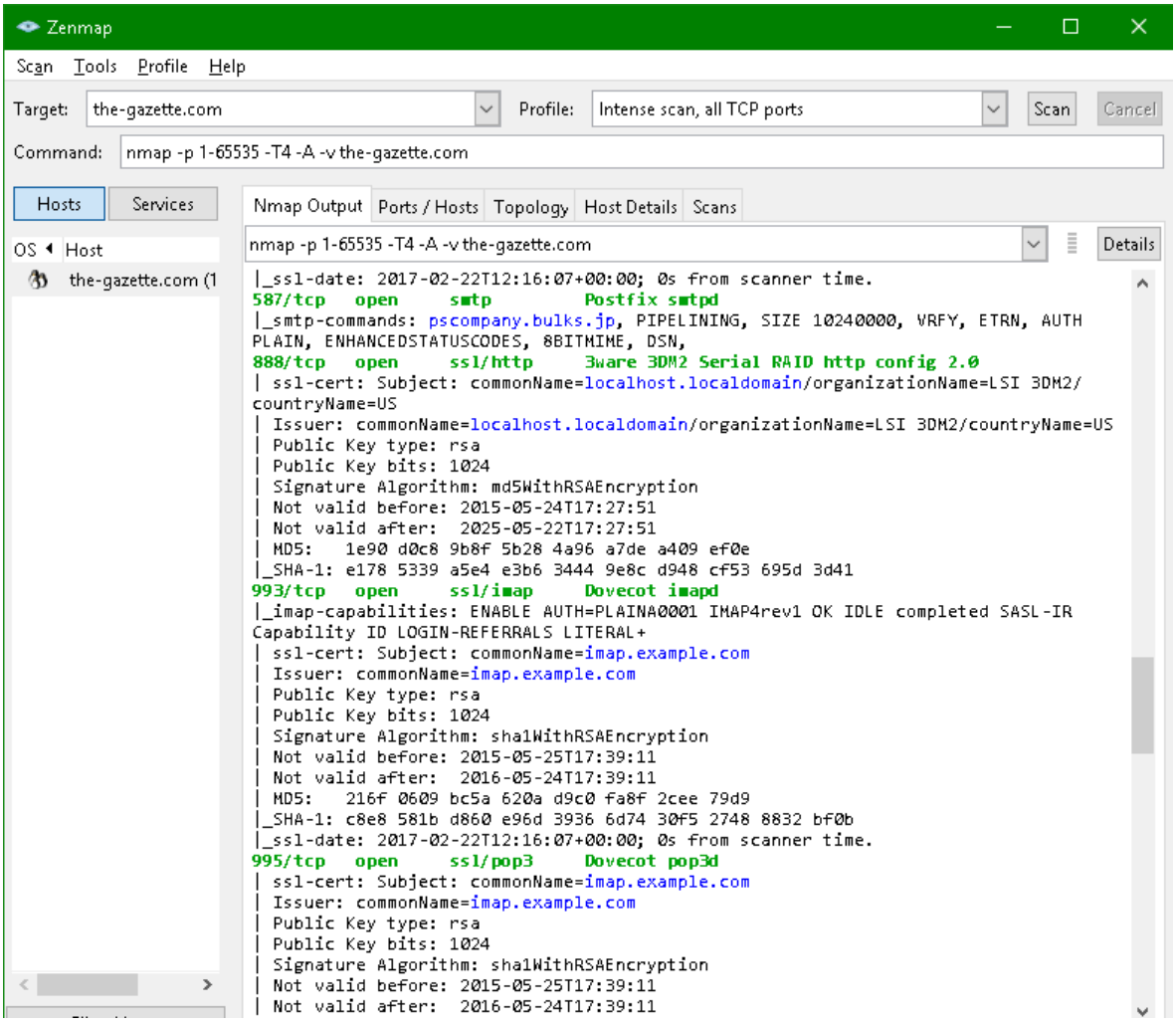
Scanning Tool Nmap

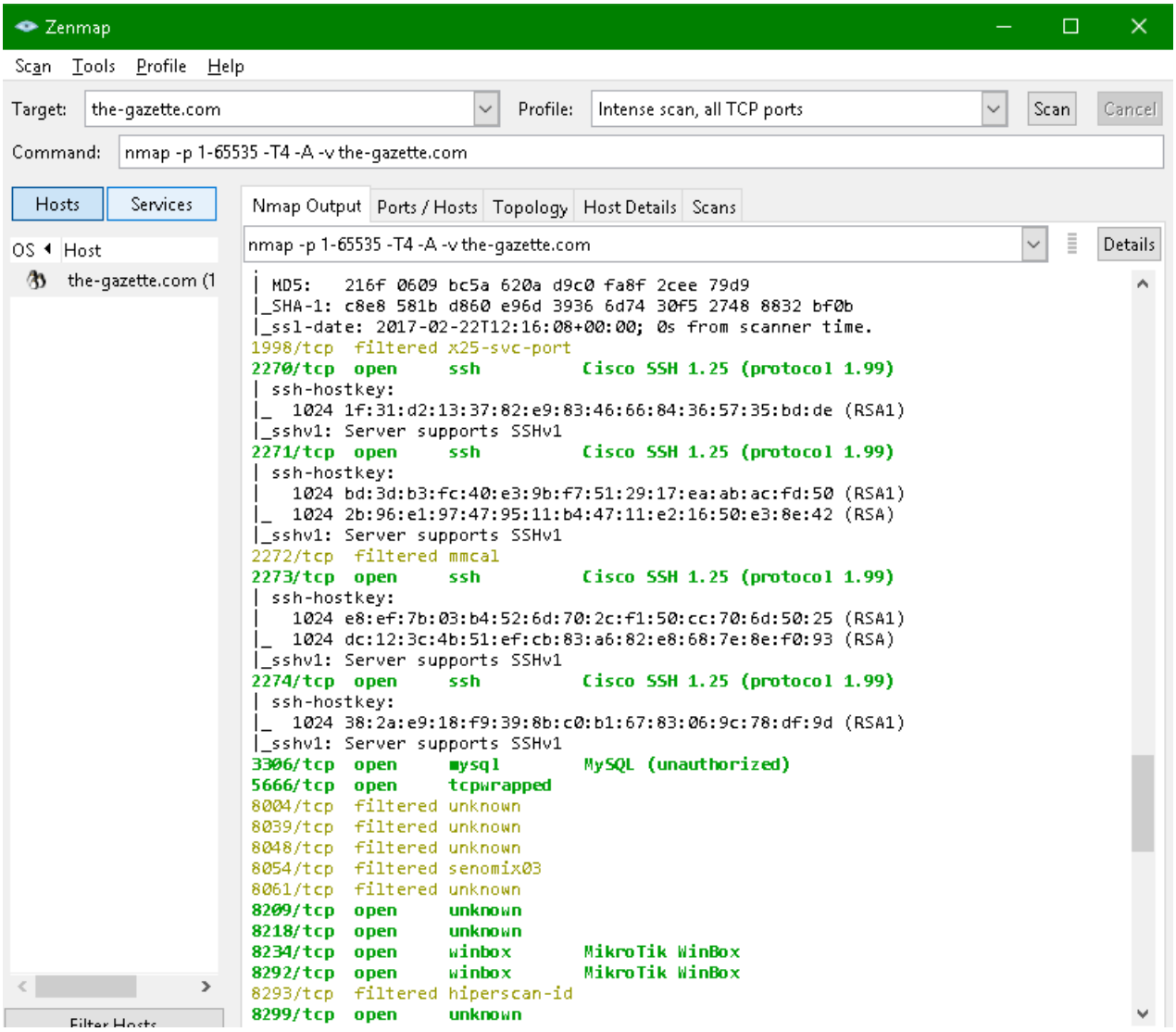
Attacker menggunakan Nmap untuk mengambil inti sari informasi seperti host aktif pada jaringan, layanan-layanan(nama aplikasi dan versinya), type dari paket filter/firewall, OS dan versinya.

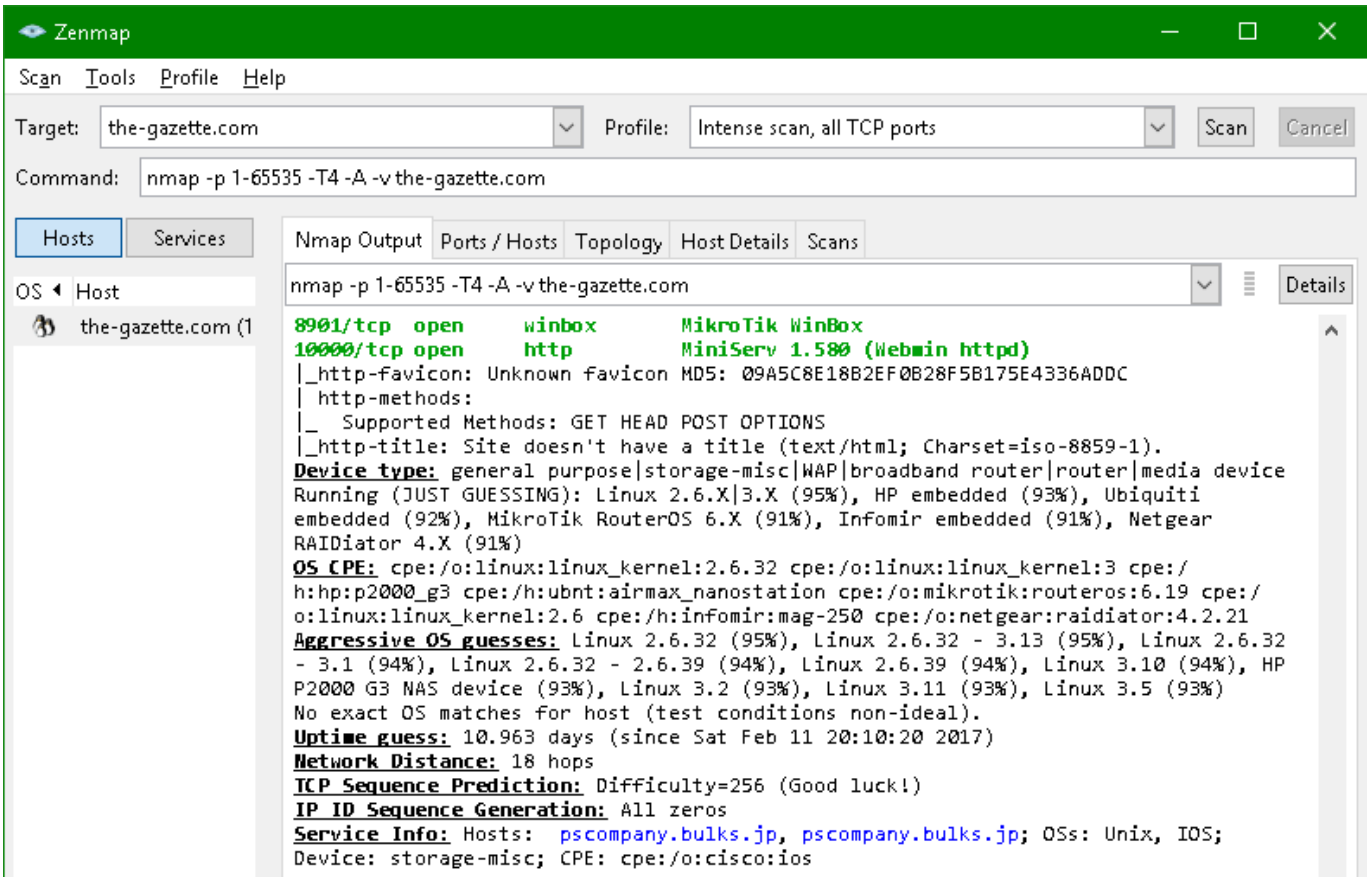



Zenmap
Scan Tools Profile Help
Target: the-gazette.com
Profile: Intense scan, all TCP ports
Scan
Cancel
Command: nmap -p 1-65535 -T4 -A -v the-gazette.com
Hosts
Services
OS Host
the-gazette.com (1
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p 1-65535 -T4 -A -v the-gazette.com
Details
Not shown: 65503 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.2.2
22/tcp open ssh OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
| 1024 a1:d7:80:27:f5:c3:20:06:b1:de:a9:31:bd:c7:b0:fb (DSA)
|_ 2048 13:30:06:ab:38:0a:28:3d:4a:1e:a1:76:18:cc:da:ff (RSA)
25/tcp open smtp Postfix smtpd
|_smtp-commands: pscompany.bulks.jp, PIPELINING, SIZE 10240000, VRFY, ETRN, AUTH PLAIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
80/tcp open http Apache httpd 2.2.15 ((CentOS))
|_http-favicon: Unknown favicon MD5: 7DE6498C97EF6DF2BF3F419845432C05
| http-methods:
| Supported Methods: GET HEAD POST OPTIONS TRACE
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.15 (CentOS)
|_http-title: the GazettE Official Site
110/tcp open pop3 Dovecot pop3d
|_pop3-capabilities: SASL(PLAIN) PIPELINING USER STLS RESP-CODES UIDL CAPA TOP
| ssl-cert: Subject: commonName=imap.example.com
| Issuer: commonName=imap.example.com
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-05-25T17:39:11
| Not valid after: 2016-05-24T17:39:11
| MD5: 216f 0609 bc5a 620a d9c0 fa8f 2cee 79d9
|_SHA-1: c8e8 581b d860 e96d 3936 6d74 30f5 2748 8832 bf0b
|_ssl-date: 2017-02-22T12:16:06+00:00; 0s from scanner time.
143/tcp open imap Dovecot imapd
|_imap-capabilities: ENABLE AUTH=PLAINA0001 IMAP4rev1 STARTTLS IDLE OK completed SASL-IR Capability ID LOGIN-REFERRALS LITERAL+
| ssl-cert: Subject: commonName=imap.example.com
| Issuer: commonName=imap.example.com
| Public Key type: rsa
| Public Key bits: 1024


Zenmap
Scan Tools Profile Help
Target: the-gazette.com
Profile: Intense scan, all TCP ports
Scan
Cancel
Command: nmap -p 1-65535 -T4 -A -v the-gazette.com
Hosts
Services
OS Host
the-gazette.com (1
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p 1-65535 -T4 -A -v the-gazette.com
Details
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-05-25T17:39:11
| Not valid after: 2016-05-24T17:39:11
| MD5: 216f 0609 bc5a 620a d9c0 fa8f 2cee 79d9
|_SHA-1: c8e8 581b d860 e96d 3936 6d74 30f5 2748 8832 bf0b
|_ssl-date: 2017-02-22T12:16:06+00:00; 0s from scanner time.
143/tcp open imap Dovecot imapd
|_imap-capabilities: ENABLE AUTH=PLAINA0001 IMAP4rev1 STARTTLS IDLE OK completed SASL-IR Capability ID LOGIN-REFERRALS LITERAL+
| ssl-cert: Subject: commonName=imap.example.com
| Issuer: commonName=imap.example.com
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-05-25T17:39:11
| Not valid after: 2016-05-24T17:39:11
| MD5: 216f 0609 bc5a 620a d9c0 fa8f 2cee 79d9
|_SHA-1: c8e8 581b d860 e96d 3936 6d74 30f5 2748 8832 bf0b
|_ssl-date: 2017-02-22T12:16:06+00:00; 0s from scanner time.
443/tcp open ssl/http Apache httpd 2.2.15 ((CentOS))
| http-methods:
| Supported Methods: GET HEAD POST OPTIONS TRACE
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.15 (CentOS)
|_http-title: Apache HTTP Server Test Page powered by CentOS
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2015-05-25T17:37:09
| Not valid after: 2016-05-24T17:37:09
| MD5: d179 bbb8 7858 e7d7 8a11 7baa 5197 0920
|_SHA-1: 1762 dcad 3e32 b036 b530 9c88 9208 fee9 92bf de09

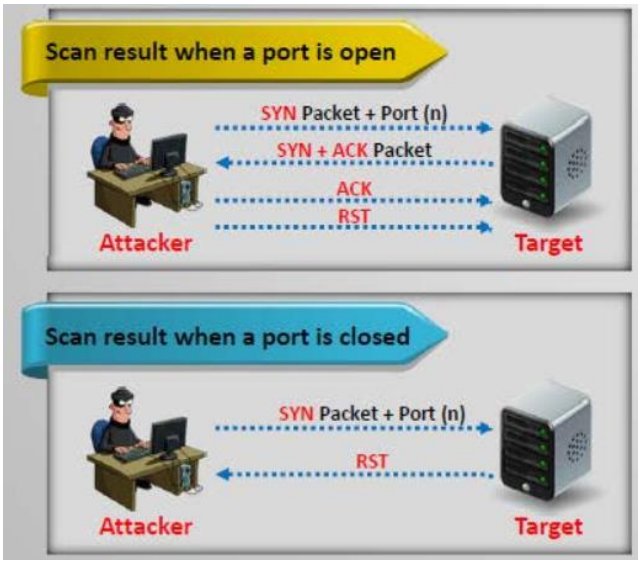

Zenmap
Scan Tools Profile Help
Target: the-gazette.com
Profile: Intense scan, all TCP ports
Scan
Cancel
Command: nmap -p 1-65535 -T4 -A -v the-gazette.com
Hosts
Services
OS Host
the-gazette.com (1
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p 1-65535 -T4 -A -v the-gazette.com
Details
|_ssl-date: 2017-02-22T12:16:07+00:00; 0s from scanner time.
587/tcp open smtp Postfix smtpd
|_smtp-commands: pscompany.bulks.jp, PIPELINING, SIZE 10240000, VRFY, ETRN, AUTH PLAIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
888/tcp open ssl/http 3ware 3DM2 Serial RAID http config 2.0
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=LSI 3DM2/countryName=US
| Issuer: commonName=localhost.localdomain/organizationName=LSI 3DM2/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2015-05-24T17:27:51
| Not valid after: 2025-05-22T17:27:51
| MD5: 1e90 d0c8 9b8f 5b28 4a96 a7de a409 ef0e
|_SHA-1: e178 5339 a5e4 e3b6 3444 9e8c d948 cf53 695d 3d41
993/tcp open ssl/imap Dovecot imapd
|_imap-capabilities: ENABLE AUTH=PLAINA0001 IMAP4rev1 OK IDLE completed SASL-IR Capability ID LOGIN-REFERRALS LITERAL+
| ssl-cert: Subject: commonName=imap.example.com
| Issuer: commonName=imap.example.com
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-05-25T17:39:11
| Not valid after: 2016-05-24T17:39:11
| MD5: 216f 0609 bc5a 620a d9c0 fa8f 2cee 79d9
|_SHA-1: c8e8 581b d860 e96d 3936 6d74 30f5 2748 8832 bf0b
|_ssl-date: 2017-02-22T12:16:07+00:00; 0s from scanner time.
995/tcp open ssl/pop3 Dovecot pop3d
| ssl-cert: Subject: commonName=imap.example.com
| Issuer: commonName=imap.example.com
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-05-25T17:39:11
| Not valid after: 2016-05-24T17:39:11

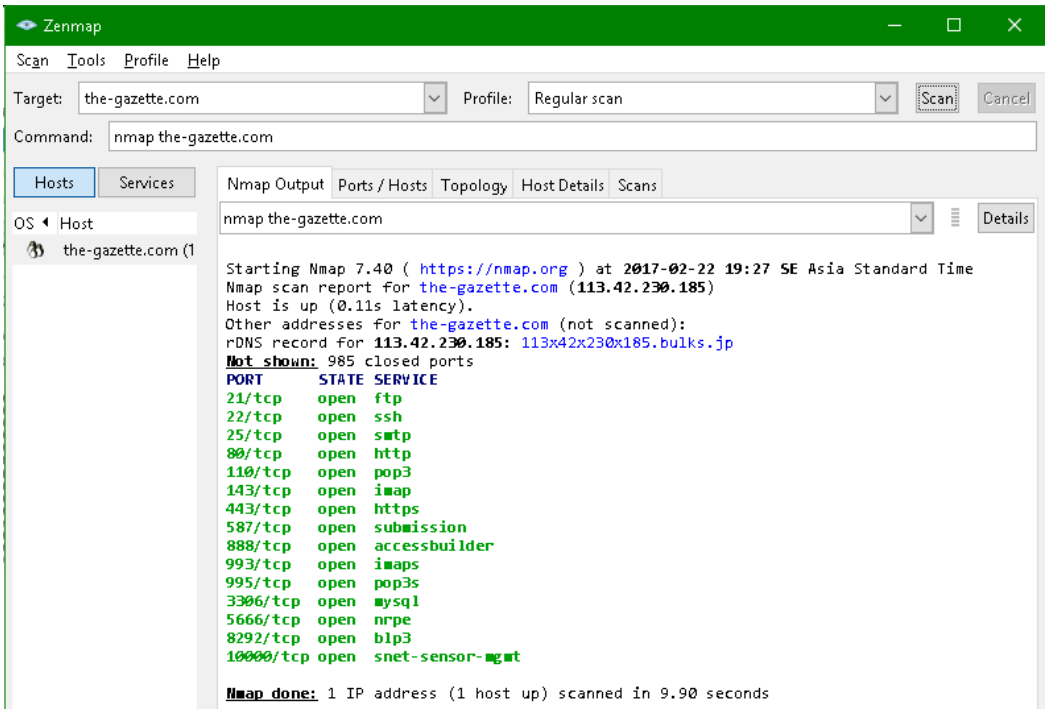

Zenmap
Scan Tools Profile Help
Target: the-gazette.com
Profile: Intense scan, all TCP ports
Scan
Cancel
Command: nmap -p 1-65535 -T4 -A -v the-gazette.com
Hosts
Services
OS Host
the-gazette.com (1
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p 1-65535 -T4 -A -v the-gazette.com
Details
| MD5: 216f 0609 bc5a 620a d9c0 fa8f 2cee 79d9
|_SHA-1: c8e8 581b d860 e96d 3936 6d74 30f5 2748 8832 bf0b
|_ssl-date: 2017-02-22T12:16:08+00:00; 0s from scanner time.
1998/tcp filtered x25-svc-port
2270/tcp open ssh Cisco SSH 1.25 (protocol 1.99)
| ssh-hostkey:
|_ 1024 1f:31:d2:13:37:82:e9:83:46:66:84:36:57:35:bd:de (RSA1)
|_sshv1: Server supports SSHv1
2271/tcp open ssh Cisco SSH 1.25 (protocol 1.99)
| ssh-hostkey:
| 1024 bd:3d:b3:fc:40:e3:9b:f7:51:29:17:ea:ab:ac:fd:50 (RSA1)
|_ 1024 2b:96:e1:97:47:95:11:b4:47:11:e2:16:50:e3:8e:42 (RSA)
|_sshv1: Server supports SSHv1
2272/tcp filtered mmcal
2273/tcp open ssh Cisco SSH 1.25 (protocol 1.99)
| ssh-hostkey:
| 1024 e8:ef:7b:03:b4:52:6d:70:2c:f1:50:cc:70:6d:50:25 (RSA1)
|_ 1024 dc:12:3c:4b:51:ef:cb:83:a6:82:e8:68:7e:8e:f0:93 (RSA)
|_sshv1: Server supports SSHv1
2274/tcp open ssh Cisco SSH 1.25 (protocol 1.99)
| ssh-hostkey:
|_ 1024 38:2a:e9:18:f9:39:8b:c0:b1:67:83:06:9c:78:df:9d (RSA1)
|_sshv1: Server supports SSHv1
3306/tcp open mysql MySQL (unauthorized)
5666/tcp open tcpwrapped
8004/tcp filtered unknown
8039/tcp filtered unknown
8048/tcp filtered unknown
8054/tcp filtered senomix03
8061/tcp filtered unknown
8209/tcp open unknown
8218/tcp open unknown
8234/tcp open winbox MikroTik WinBox
8292/tcp open winbox MikroTik WinBox
8293/tcp filtered hiperscan-id
8299/tcp open unknown
Filter Hosts



Tcp Connect/Full Open Scan

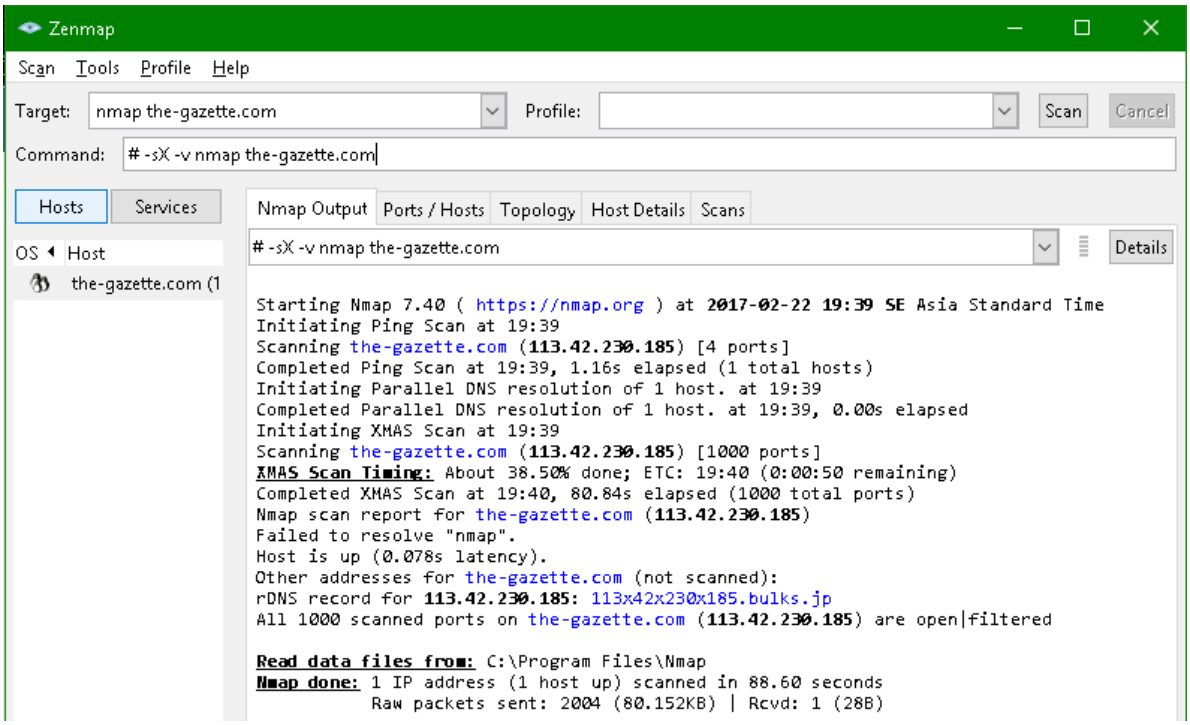
Scanning Tcp Connect mendeteksi apabila sebuah port terbuka dengan melengkapi three-way handshake. Scanning TCP Connect dapat membangun koneksi penuh dan meruntuhkannya dengan mengirim paket RST dan tidak membutuhkan hak khusus super user





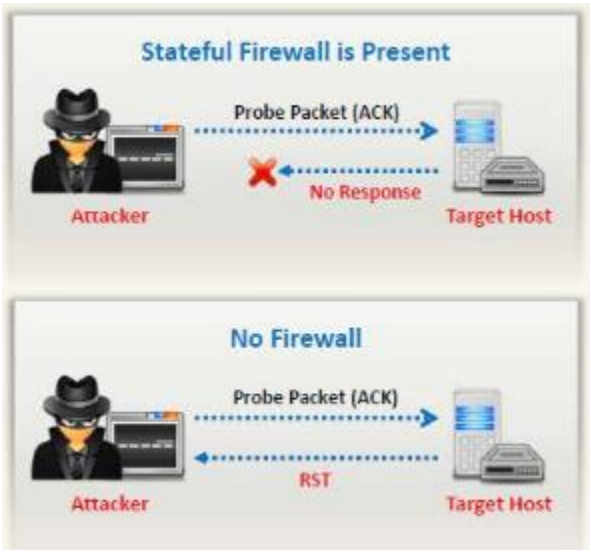
Xmas Scan

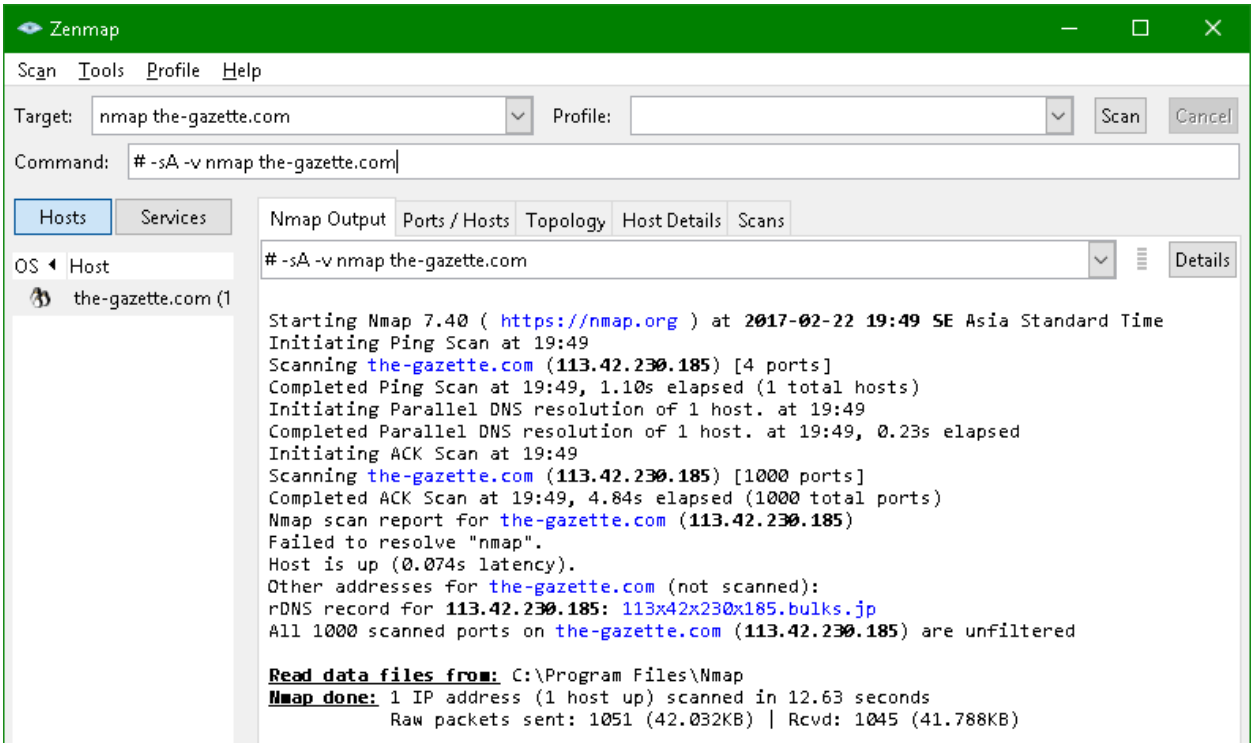
Pada Xmas scan, attacker mengirim sebuah frame TCP ke sebuah remote device dengan flag set FIN, URG, dan PUSH. FIN scan hanya bekerja pada OS dengan implementasi TCP/IP basis RFC 793. Dan tidak akan bekerja terhadap versi apapun Microsoft Windows yang sekarang.



ACK Flag Probe Scanning

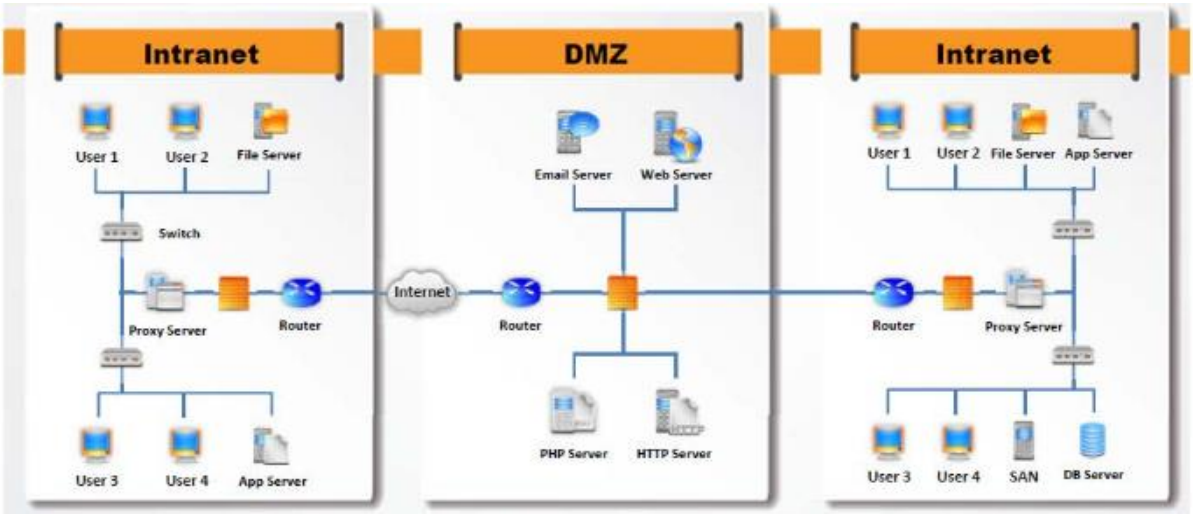
ACK Flag Probe Scanning juga di gunakan untuk mengecek filtering system dari target. Attackers mengirim paket ACK Probe dengan deret angka acak, tidak adanya respon berarti port terfilter(adanya stateful firewall) dan respon RST berarti port tidak terfilter.

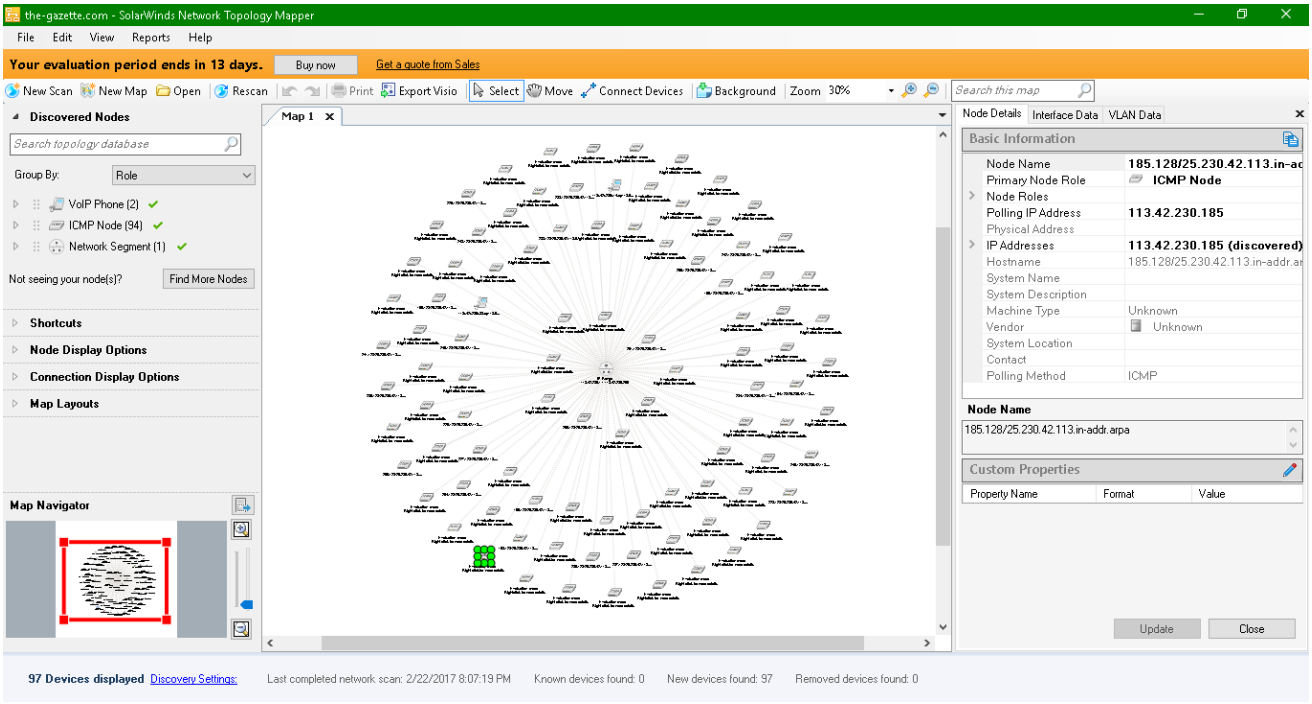




Mapping Network Diagram

Menggambarkan diagram network target memberikan informasi berharga mengenai network dan arsitekturnya kepada attacker. Diagram network menunjukkan jalan logical dan physical untuk target yang potensial.





Vulnerability Scanning

Vulnerability Scanning mengidentifikasi kelemahan dan celah dari system dan jaringan dalam urutan untuk menjelaskan bagaimana system bisa di exploitasi.

Analisis

Adanya port-port yang terbuka memungkinkan attacker untuk mengeksploitasi celah tersebut. Dalam beberapa scan lainnya terdapat celah-celah yang memenuhi persyaratan attacker untuk mengeksploitasinya.