TUGAS

MID

KEAMANAN JARINGAN KOMPUTER

Oleh:

Elvatyara Rahmadiany Puteri

09121001034

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2016

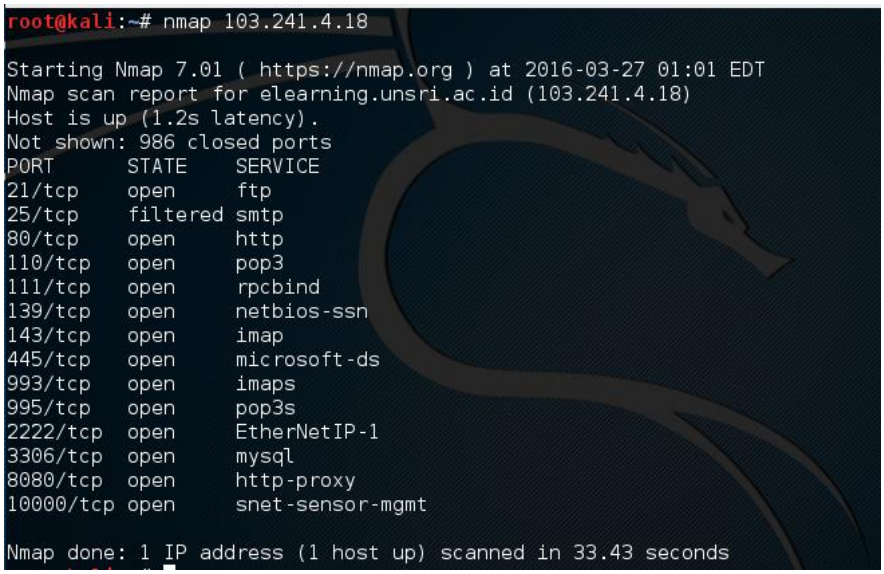
Target : www.elearning.unsri.ac.id

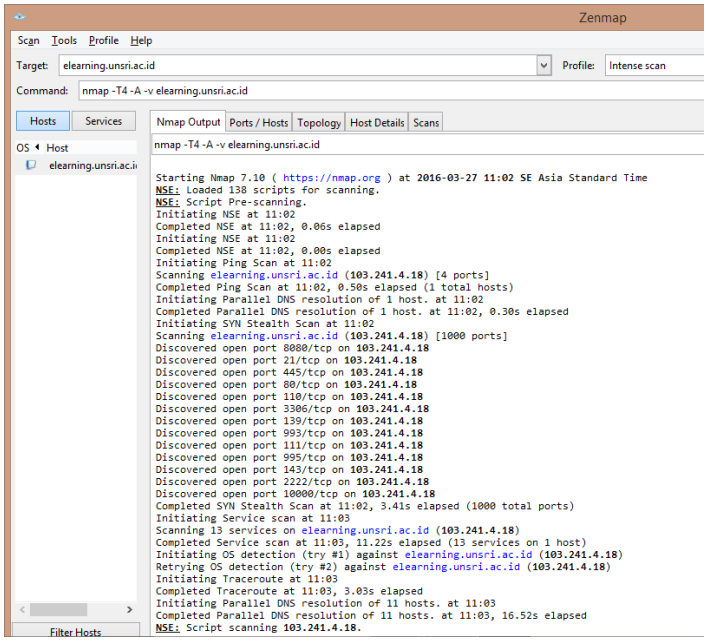
IP Address : 103.241.4.18

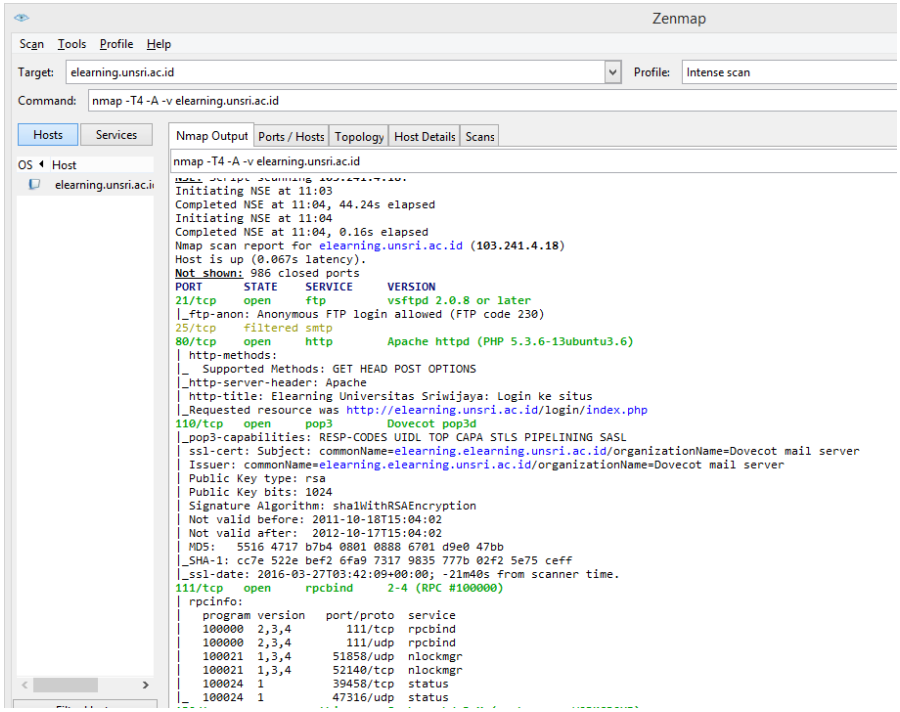
1. Scanning dengan menggunakan NMAP

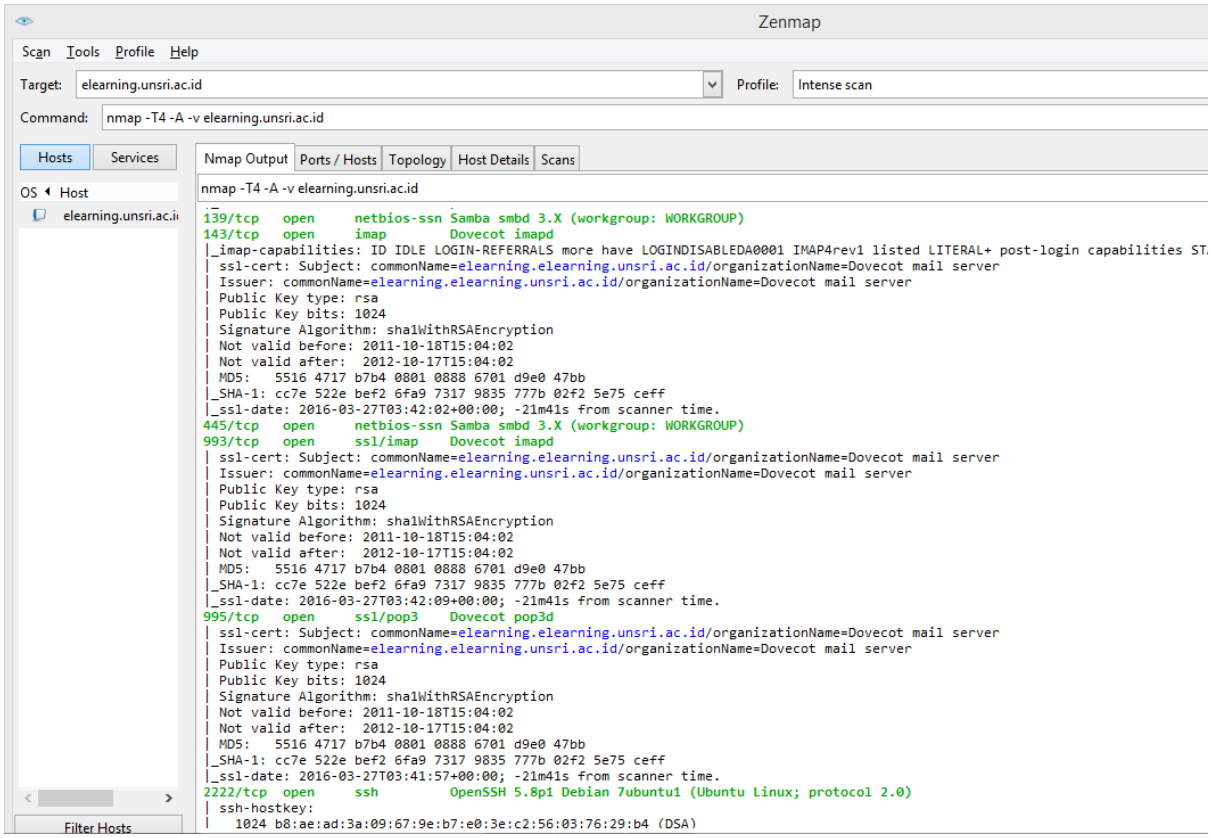
Nmap (Network Mapper) adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan *port scanning.* Aplikasi ini digunakan untuk meng-audit jaringan yang ada. Dengan menggunakan tool ini, kita dapat melihat host yang aktif, port yang terbuka, Sistem Operasi yang digunakan, dan feature-feature scanning lainnya. Pada awalnya, Nmap hanya bisa berjalan di sistem operasi Linux, namun dalam perkembangannya sekarang ini, hampir semua sistem operasi bisa menjalankan Nmap.

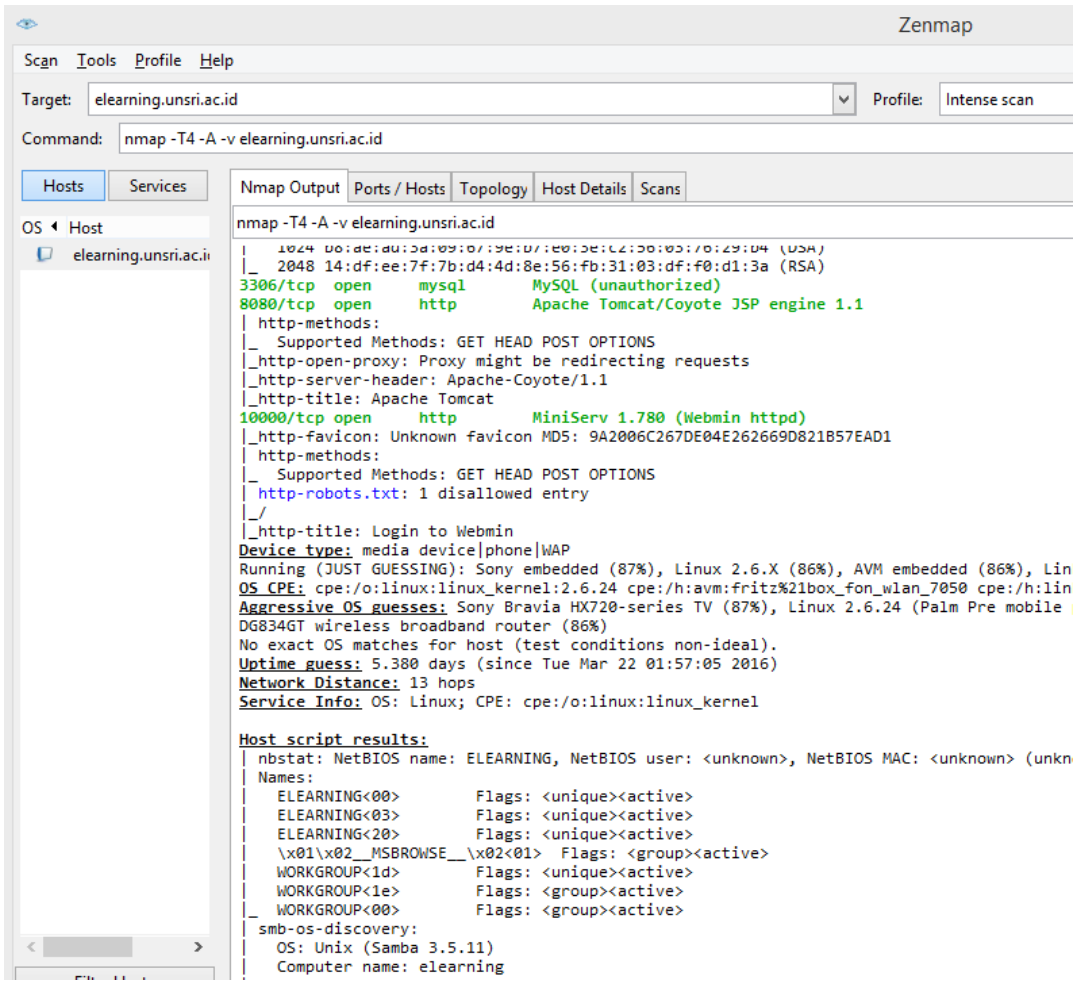
Hasil scanning web elearning unsri dengan menggunakan NMAP:



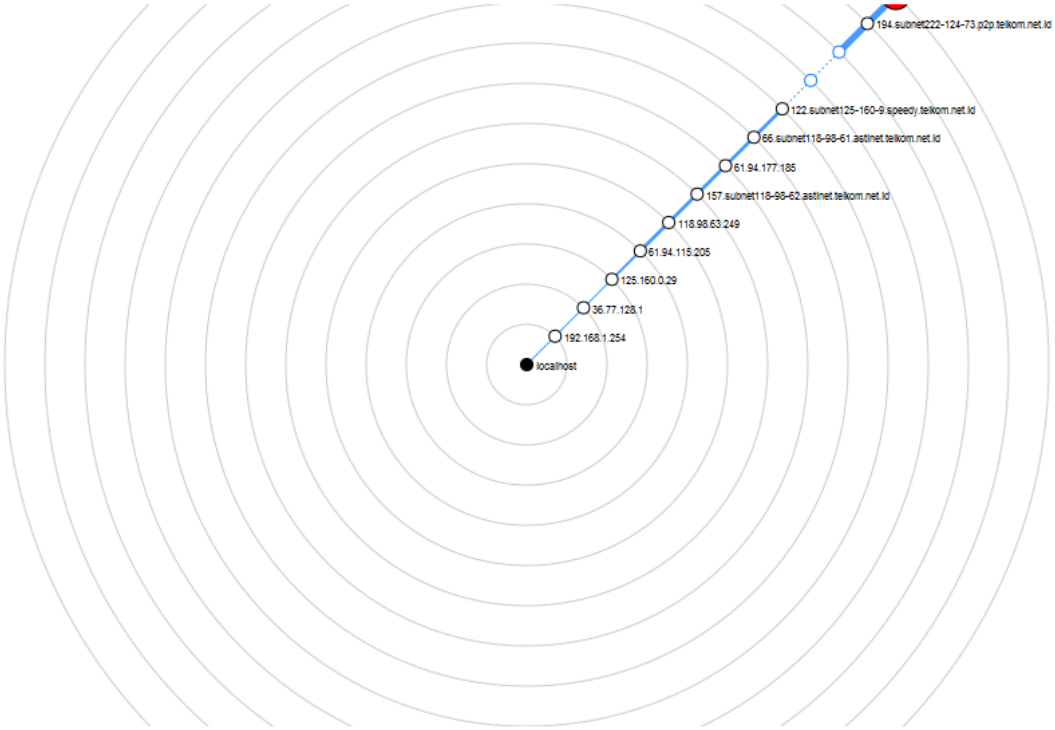

Zenmap
Scan Tools Profile Help
Target: elearning.unsri.ac.id
Profile: Intense scan
Command: nmap -T4 -A -v elearning.unsri.ac.id
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
elearning.unsri.ac.id
nmap -T4 -A -v elearning.unsri.ac.id
Starting Nmap 7.10 (https://nmap.org) at 2016-03-27 11:02 SE Asia Standard Time
NSE: Loaded 138 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:02
Completed NSE at 11:02, 0.06s elapsed
Initiating NSE at 11:02
Completed NSE at 11:02, 0.00s elapsed
Initiating Ping Scan at 11:02
Scanning elearning.unsri.ac.id (103.241.4.18) [4 ports]
Completed Ping Scan at 11:02, 0.50s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:02
Completed Parallel DNS resolution of 1 host. at 11:02, 0.30s elapsed
Initiating SYN Stealth Scan at 11:02
Scanning elearning.unsri.ac.id (103.241.4.18) [1000 ports]
Discovered open port 8080/tcp on 103.241.4.18
Discovered open port 21/tcp on 103.241.4.18
Discovered open port 445/tcp on 103.241.4.18
Discovered open port 80/tcp on 103.241.4.18
Discovered open port 110/tcp on 103.241.4.18
Discovered open port 3306/tcp on 103.241.4.18
Discovered open port 139/tcp on 103.241.4.18
Discovered open port 993/tcp on 103.241.4.18
Discovered open port 111/tcp on 103.241.4.18
Discovered open port 995/tcp on 103.241.4.18
Discovered open port 143/tcp on 103.241.4.18
Discovered open port 2222/tcp on 103.241.4.18
Discovered open port 10000/tcp on 103.241.4.18
Completed SYN Stealth Scan at 11:02, 3.41s elapsed (1000 total ports)
Initiating Service scan at 11:03
Scanning 13 services on elearning.unsri.ac.id (103.241.4.18)
Completed Service scan at 11:03, 11.22s elapsed (13 services on 1 host)
Initiating OS detection (try #1) against elearning.unsri.ac.id (103.241.4.18)
Retrying OS detection (try #2) against elearning.unsri.ac.id (103.241.4.18)
Initiating Traceroute at 11:03
Completed Traceroute at 11:03, 3.03s elapsed
Initiating Parallel DNS resolution of 11 hosts. at 11:03
Completed Parallel DNS resolution of 11 hosts. at 11:03, 16.52s elapsed
NSE: Script scanning 103.241.4.18.
Filter Hosts

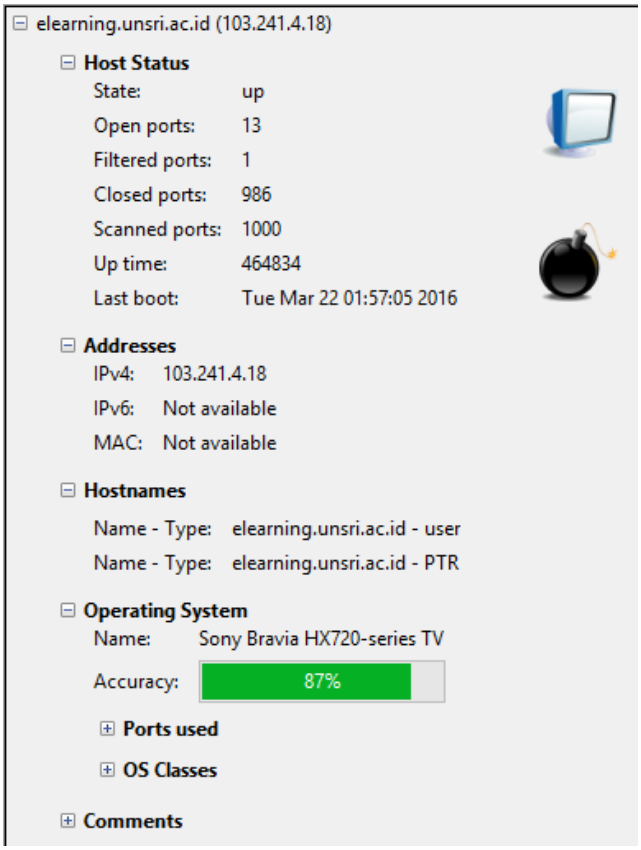

Zenmap
Scan Tools Profile Help
Target: elearning.unsri.ac.id
Profile: Intense scan
Command: nmap -T4 -A -v elearning.unsri.ac.id
Hosts Services
Nmap Output Ports / Hosts Topology Host Details Scans
OS Host
elearning.unsri.ac.id
nmap -T4 -A -v elearning.unsri.ac.id
Initiating NSE at 11:03
Completed NSE at 11:04, 44.24s elapsed
Initiating NSE at 11:04
Completed NSE at 11:04, 0.16s elapsed
Nmap scan report for elearning.unsri.ac.id (103.241.4.18)
Host is up (0.067s latency).
Not shown: 986 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.0.8 or later
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
25/tcp filtered smtp
80/tcp open http Apache httpd (PHP 5.3.6-13ubuntu3.6)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
| http-title: Elearning Universitas Sriwijaya: Login ke situs
|_Requested resource was http://elearning.unsri.ac.id/login/index.php
110/tcp open pop3 Dovecot pop3d
|_pop3-capabilities: RESP-CODES UIDL TOP CAPA STLS PIPELINING SASL
| ssl-cert: Subject: commonName=elearning.elearning.unsri.ac.id/organizationName=Dovecot mail server
| Issuer: commonName=elearning.elearning.unsri.ac.id/organizationName=Dovecot mail server
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-10-18T15:04:02
| Not valid after: 2012-10-17T15:04:02
| MD5: 5516 4717 b7b4 0801 0888 6701 d9e0 47bb
|_SHA-1: cc7e 522e bef2 6fa9 7317 9835 777b 02f2 5e75 ceff
|_ssl-date: 2016-03-27T03:42:09+00:00; -21m40s from scanner time.
111/tcp open rpcbind 2-4 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100021 1,3,4 51858/udp nlockmgr
| 100021 1,3,4 52140/tcp nlockmgr
| 100024 1 39458/tcp status
|_ 100024 1 47316/udp status


Zenmap
Scan Tools Profile Help
Target: elearning.unsri.ac.id
Profile: Intense scan
Command: nmap -T4 -A -v elearning.unsri.ac.id
Hosts Services
OS Host
elearning.unsri.ac.i
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v elearning.unsri.ac.id
139/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
143/tcp open imap Dovecot imapd
|_imap-capabilities: ID IDLE LOGIN-REFERRALS more have LOGINDISABLEDA0001 IMAP4rev1 listed LITERAL+ post-login capabilities ST
| ssl-cert: Subject: commonName=elearning.elearning.unsri.ac.id/organizationName=Dovecot mail server
| Issuer: commonName=elearning.elearning.unsri.ac.id/organizationName=Dovecot mail server
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-10-18T15:04:02
| Not valid after: 2012-10-17T15:04:02
| MD5: 5516 4717 b7b4 0801 0888 6701 d9e0 47bb
|_SHA-1: cc7e 522e bef2 6fa9 7317 9835 777b 02f2 5e75 ceff
|_ssl-date: 2016-03-27T03:42:02+00:00; -21m41s from scanner time.
445/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
993/tcp open ssl/imap Dovecot imapd
| ssl-cert: Subject: commonName=elearning.elearning.unsri.ac.id/organizationName=Dovecot mail server
| Issuer: commonName=elearning.elearning.unsri.ac.id/organizationName=Dovecot mail server
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-10-18T15:04:02
| Not valid after: 2012-10-17T15:04:02
| MD5: 5516 4717 b7b4 0801 0888 6701 d9e0 47bb
|_SHA-1: cc7e 522e bef2 6fa9 7317 9835 777b 02f2 5e75 ceff
|_ssl-date: 2016-03-27T03:42:09+00:00; -21m41s from scanner time.
995/tcp open ssl/pop3 Dovecot pop3d
| ssl-cert: Subject: commonName=elearning.elearning.unsri.ac.id/organizationName=Dovecot mail server
| Issuer: commonName=elearning.elearning.unsri.ac.id/organizationName=Dovecot mail server
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2011-10-18T15:04:02
| Not valid after: 2012-10-17T15:04:02
| MD5: 5516 4717 b7b4 0801 0888 6701 d9e0 47bb
|_SHA-1: cc7e 522e bef2 6fa9 7317 9835 777b 02f2 5e75 ceff
|_ssl-date: 2016-03-27T03:41:57+00:00; -21m41s from scanner time.
2222/tcp open ssh OpenSSH 5.8p1 Debian 7ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 b8:ae:ad:3a:09:67:9e:b7:e0:3e:c2:56:03:76:29:b4 (DSA)
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: elearning.unsri.ac.id
Profile: Intense scan
Command: nmap -T4 -A -v elearning.unsri.ac.id
Hosts Services
OS Host
elearning.unsri.ac.i
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v elearning.unsri.ac.id
| 1024 b8:ae:ad:3a:09:67:9e:b7:e0:3e:c2:56:03:76:29:b4 (DSA)
|_ 2048 14:df:ee:7f:7b:d4:4d:8e:56:fb:31:03:df:f0:d1:3a (RSA)
3306/tcp open mysql MySQL (unauthorized)
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat
10000/tcp open http MiniServ 1.780 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 9A2006C267DE04E262669D821B57EAD1
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Login to Webmin
Device type: media device|phone|WAP
Running (JUST GUESSING): Sony embedded (87%), Linux 2.6.X (86%), AVM embedded (86%), Lin
OS CPE: cpe:/o:linux:linux_kernel:2.6.24 cpe:/h:avm:fritz%21box_fon_wlan_7050 cpe:/h:lin
Aggressive OS guesses: Sony Bravia HX720-series TV (87%), Linux 2.6.24 (Palm Pre mobile
DG834GT wireless broadband router (86%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 5.380 days (since Tue Mar 22 01:57:05 2016)
Network Distance: 13 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
| nbstat: NetBIOS name: ELEARNING, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unkn
| Names:
| ELEARNING<00> Flags: <unique><active>
| ELEARNING<03> Flags: <unique><active>
| ELEARNING<20> Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| WORKGROUP<1d> Flags: <unique><active>
| WORKGROUP<1e> Flags: <group><active>
|_ WORKGROUP<00> Flags: <group><active>
| smb-os-discovery:
| OS: Unix (Samba 3.5.11)
| Computer name: elearning

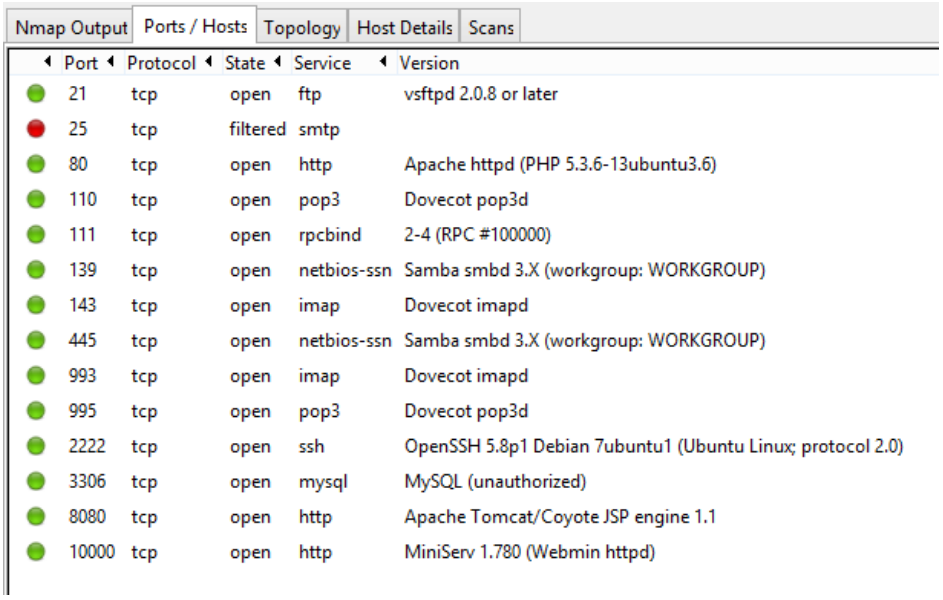
```
|   NetBIOS computer name:
|   Domain name: unsri.ac.id
|   FQDN: elearning.unsri.ac.id
|_  System time: 2016-03-27T10:41:59+07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol

TRACEROUTE (using port 256/tcp)
HOP RTT      ADDRESS
1   0.00 ms  192.168.1.254
2   0.00 ms  36.77.128.1
3   0.00 ms  125.160.0.29
4   16.00 ms 61.94.115.205
5   31.00 ms 118.98.63.249
6   31.00 ms 157.subnet118-98-62.astinet.telkom.net.id (118.98.62.157)
7   31.00 ms 61.94.177.185
8   31.00 ms 66.subnet118-98-61.astinet.telkom.net.id (118.98.61.66)
9   31.00 ms 122.subnet125-160-9.speedy.telkom.net.id (125.160.9.122)
10  ... 11
12  79.00 ms 194.subnet222-124-73.p2p.telkom.net.id (222.124.73.194)
13  79.00 ms elearning.unsri.ac.id (103.241.4.18)

NSE: Script Post-scanning.
Initiating NSE at 11:04
Completed NSE at 11:04, 0.01s elapsed
Initiating NSE at 11:04
Completed NSE at 11:04, 0.00s elapsed
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 91.58 seconds
           Raw packets sent: 1105 (50.720KB) | Rcvd: 1078 (45.484KB)
```





Analisa:

Dari scanning yang telah dilakukan dapat diketahui bahwa web elearning UNSRI memiliki 1000 port yang bisa discanning. Host status dari web ini adalah up, namun dari 1000 port yang tersedia, port yang dalam kondisi terbuka hanya 13 port, port dalam kondisi filtered ada 1 port, dan sisanya 986 adalah port yang tertutup. Gambar dibawah ini menunjukkan detail dari port-port yang terbuka dan port yang dalam kondisi filtered.

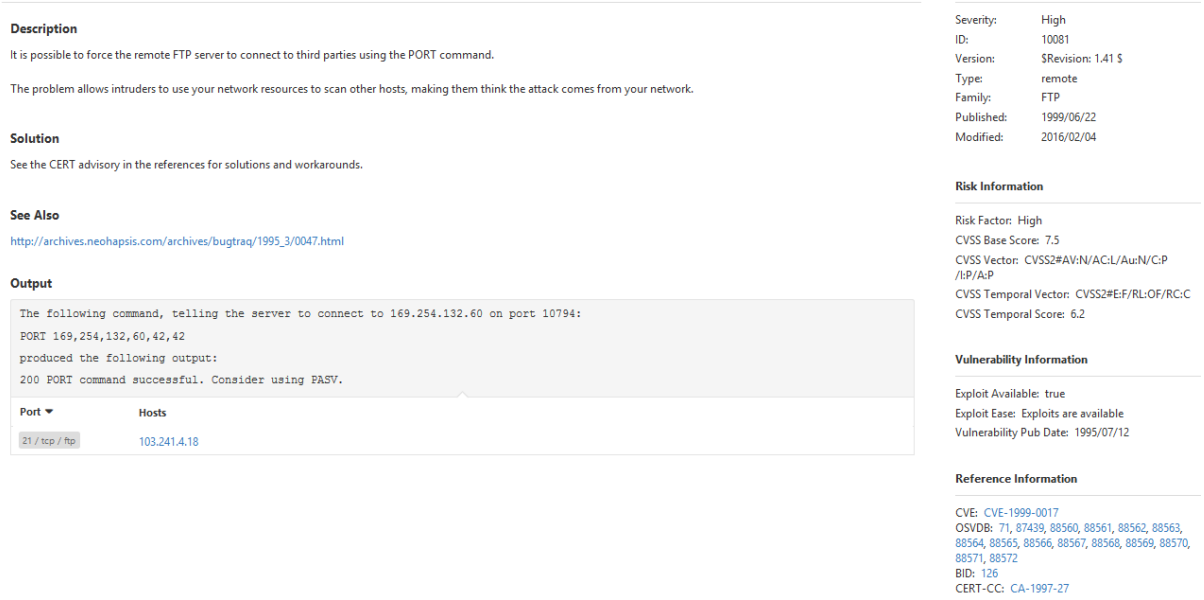


Port	Protocol	State	Service	Version
21	tcp	open	ftp	vsftpd 2.0.8 or later
25	tcp	filtered	smtp	
80	tcp	open	http	Apache httpd (PHP 5.3.6-13ubuntu3.6)
110	tcp	open	pop3	Dovecot pop3d
111	tcp	open	rpcbind	2-4 (RPC #100000)
139	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
143	tcp	open	imap	Dovecot imapd
445	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
993	tcp	open	imap	Dovecot imapd
995	tcp	open	pop3	Dovecot pop3d
2222	tcp	open	ssh	OpenSSH 5.8p1 Debian 7ubuntu1 (Ubuntu Linux; protocol 2.0)
3306	tcp	open	mysql	MySQL (unauthorized)
8080	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
10000	tcp	open	http	MiniServ 1.780 (Webmin httpd)

2. Scanning dengan menggunakan Nessus

Nessus *dibuat oleh Renaud Deraison pada tahun 1998. Nessus adalah* salah satu scanner keamanan jaringan yang harus digunakan oleh administrator system. Nessus merupakan sebuah software scanning, yang dapat digunakan untuk meng-audit kemanan sebuah sistem, seperti vulnerability, misconfiguration, security patch yang belum diaplikasikan, default password, dan denial of serviceNessus berfungsi untuk monitoring lalu-lintas jaringan.

Dikarenakan fungsi dari Nessus dapat digunakan untuk mendeteksi adanya kelemahan ataupun cacat dari suatu sistem maka Nessus menjadi salah satu tool andalan ketika melakukan audit keamanan suatu sistem. Sebelum Nessus versi 3, aplikasi ini bersifat open source dan menjadi salah satu primadona di dunia open source. Namun sekarang mulai Nessus versi 3 oleh Teenable Security dijadikan sebagai aplikasi propietary dan closed source. Dibawah ini merupakan hasil daripada scanning dengan menggunakan Nessus:



Description

It is possible to force the remote FTP server to connect to third parties using the PORT command.

The problem allows intruders to use your network resources to scan other hosts, making them think the attack comes from your network.

Solution

See the CERT advisory in the references for solutions and workarounds.

See Also

http://archives.neohapsis.com/archives/bugtraq/1995_3/0047.html

Output

```
The following command, telling the server to connect to 169.254.132.60 on port 10794:
PORT 169,254,132,60,42,42
produced the following output:
200 PORT command successful. Consider using PASV.
```

Port	Hosts
21 / tcp / ftp	103.241.4.18

Severity:	High
ID:	10081
Version:	$Revision: 1.41 $
Type:	remote
Family:	FTP
Published:	1999/06/22
Modified:	2016/02/04

Risk Information

Risk Factor: High
CVSS Base Score: 7.5
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Vector: CVSS2#E:F/RL:OF/RC:C
CVSS Temporal Score: 6.2

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: 1995/07/12

Reference Information

CVE: CVE-1999-0017
OSVDB: 71, 87439, 88560, 88561, 88562, 88563, 88564, 88565, 88566, 88567, 88568, 88569, 88570, 88571, 88572
BID: 126
CERT-CC: CA-1997-27

Output

```
The following certificate was part of the certificate chain
sent by the remote host, but has expired :

|-Subject   : O=Dovecot mail server/OU=elearning.elearning.unsri.ac.id/CN=elearning.elearning.unsri.ac.id
/E=root@elearning.elearning.unsri.ac.id
|-Not After : Oct 17 15:04:02 2012 GMT

The following certificate was at the top of the certificate
chain sent by the remote host, but is signed by an unknown
certificate authority :

|-Subject : O=Dovecot mail server/OU=elearning.elearning.unsri.ac.id/CN=elearning.elearning.unsri.ac.id
/E=root@elearning.elearning.unsri.ac.id
|-Issuer  : O=Dovecot mail server/OU=elearning.elearning.unsri.ac.id/CN=elearning.elearning.unsri.ac.id
/E=root@elearning.elearning.unsri.ac.id
```

Port	Hosts
110 / tcp / pop3	103.241.4.18
143 / tcp / imap	103.241.4.18
993 / tcp / imap	103.241.4.18
995 / tcp / pop3	103.241.4.18

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

See Also

http://www.nessus.org/u?217a3666
http://cr.yp.to/talks/2013.03.12/slides.pdf
http://www.isg.rhul.ac.uk/tls/
http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Output

```
List of RC4 cipher suites supported by the remote server :

  High Strength Ciphers (>= 112-bit key)

    TLSv1
      RC4-MD5                     Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=MD5
      RC4-SHA                     Kx=RSA         Au=RSA      Enc=RC4(128)             Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

Port	Hosts
110 / tcp / pop3	103.241.4.18
143 / tcp / imap	103.241.4.18
993 / tcp / imap	103.241.4.18
995 / tcp / pop3	103.241.4.18

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

See Also

https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00

Output

```
Nessus determined that the remote server supports SSLv3 with at least one CBC
cipher suite, indicating that this server is vulnerable.

It appears that TLSv1 or newer is supported on the server. However, the
Fallback SCSV mechanism is not supported, allowing connections to be "rolled
back" to SSLv3.
```

Port	Hosts
110 / tcp / pop3	103.241.4.18
143 / tcp / imap	103.241.4.18
993 / tcp / imap	103.241.4.18
995 / tcp / pop3	103.241.4.18

Risk Information

Risk Factor: Medium
CVSS Base Score: 4.3
CVSS Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Vector: CVSS2#E:ND/RL:OF/RC:C
CVSS Temporal Score: 3.7

Vulnerability Information

Exploit Available: false
Exploit Ease: No known exploits are available
Vulnerability Pub Date: 2013/03/12
In the news: true

Reference Information

CVE: CVE-2013-2566, CVE-2015-2808
OSVDB: 91162, 117855
BID: 58796, 73684

CVSS2#E:ND/RL:OF/RC:C
CVSS Temporal Score: 3.7

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: 2014/10/14
In the news: true

Reference Information

CVE: CVE-2014-3566
OSVDB: 113251
BID: 70574
CERT: 577193

MEDIUM Anonymous FTP Enabled

Description

This FTP service allows anonymous logins. Any remote user may connect and authenticate without providing a password or unique credentials.
This allows a user to access any files made available on the FTP server.

Solution

Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure sensitive content is not available.

Output

```
No output recorded.
```

Port	Hosts
21 / tcp / ftp	103.241.4.18

Plugin Details

Severity:	Medium
ID:	10079
Version:	$Revision: 1.51 $
Type:	remote
Family:	FTP
Published:	1999/06/22
Modified:	2014/04/02

Risk Information

Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Vulnerability Information

Vulnerability Pub Date: 1993/07/01

Reference Information

CVE: CVE-1999-0497
OSVDB: 69

Output

```
Port 21/tcp was found to be open
```

Port	Hosts
21 / tcp / ftp	103.241.4.18

```
Port 80/tcp was found to be open
```

Port	Hosts
80 / tcp / www	103.241.4.18

```
Port 110/tcp was found to be open
```

Port	Hosts
110 / tcp / pop3	103.241.4.18

```
Port 111/tcp was found to be open
```

Port	Hosts
111 / tcp / rpc-portma...	103.241.4.18

```
Port 139/tcp was found to be open
```

Port	Hosts
139 / tcp / smb	103.241.4.18

Port 143/tcp was found to be open

Port	Hosts
143 / tcp / imap	103.241.4.18

Port 445/tcp was found to be open

Port	Hosts
445 / tcp / cifs	103.241.4.18

Port 993/tcp was found to be open

Port	Hosts
993 / tcp / imap	103.241.4.18

Port 995/tcp was found to be open

Port	Hosts
995 / tcp / pop3	103.241.4.18

Port 2222/tcp was found to be open

Port	Hosts
2222 / tcp / ssh	103.241.4.18

Port 3306/tcp was found to be open

Port	Hosts
3306 / tcp / mysql	103.241.4.18

Port 8080/tcp was found to be open

Port	Hosts
8080 / tcp / www	103.241.4.18

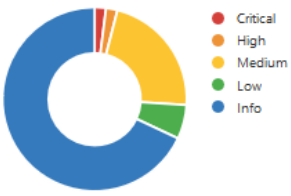
Port 10000/tcp was found to be open

Port	Hosts
10000 / tcp / www	103.241.4.18

Scan Details

Name:	elearning-basic
Status:	Completed
Policy:	Basic Network Scan
Scanner:	Local Scanner
Folder:	My Scans
Start:	Today at 11:14 AM
End:	Today at 11:46 AM
Elapsed:	32 minutes
Targets:	103.241.4.18

Vulnerabilities



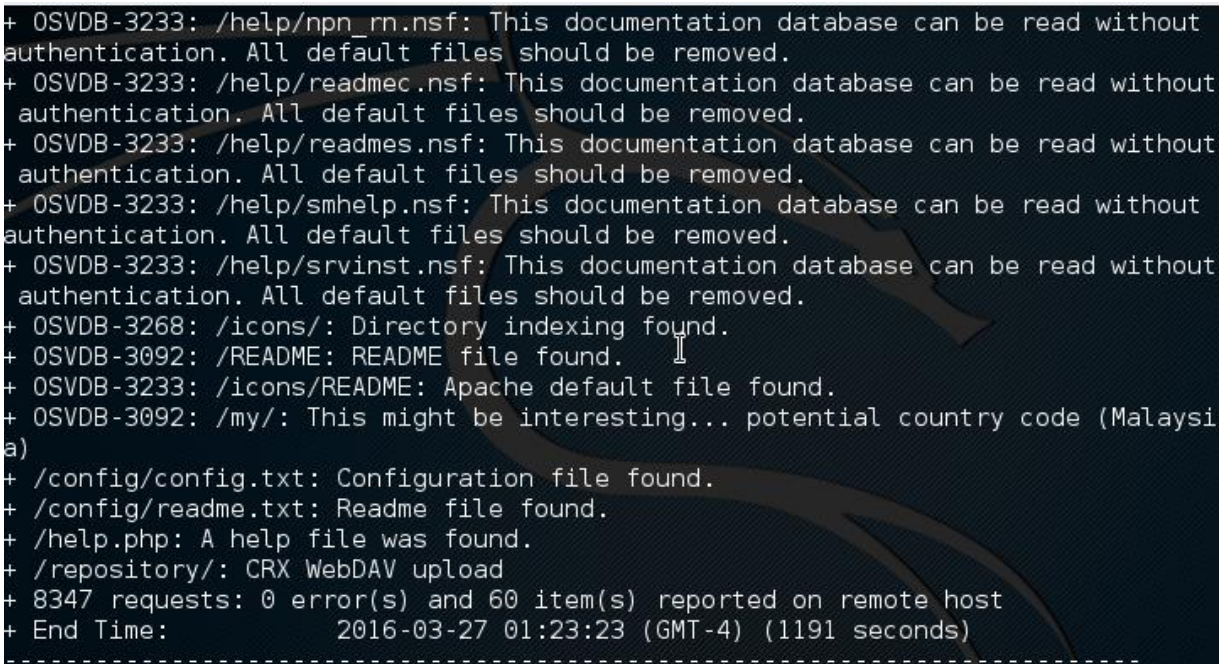
Analisa:

Sama dengan scanning dengan menggunakan Nmap sebelumnya, scanning dengan menggunakan Nessus juga menunjukkan bahwa port yang terbuka dan dapat diakses daripada situs elearning unsri ini berjumlah 13 port. Selain mengetahui port yang terbuka, kita juga mendapatkan info mengenai CVE Number yang digunakan oleh situs ini, yaitu:

- CVE-1999-0017
- CVE-2013-2566
- CVE-2015-2808
- CVE-2014-3566
- CVE-1999-0497
- CVE-1999-0024
- CVE-2006-0987
- CVE-1999-0505
- CVE-2008-5161

3. Scanning dengan menggunakan Nikto

Nikto adalah tools untuk pemeriksaan vulnerability pada apache. Jadi anda dapat mengetahui dimana letak hole pada suatu web server. Dibawah ini adalah hasil scanning situs elearning dengan menggunakan nikto:

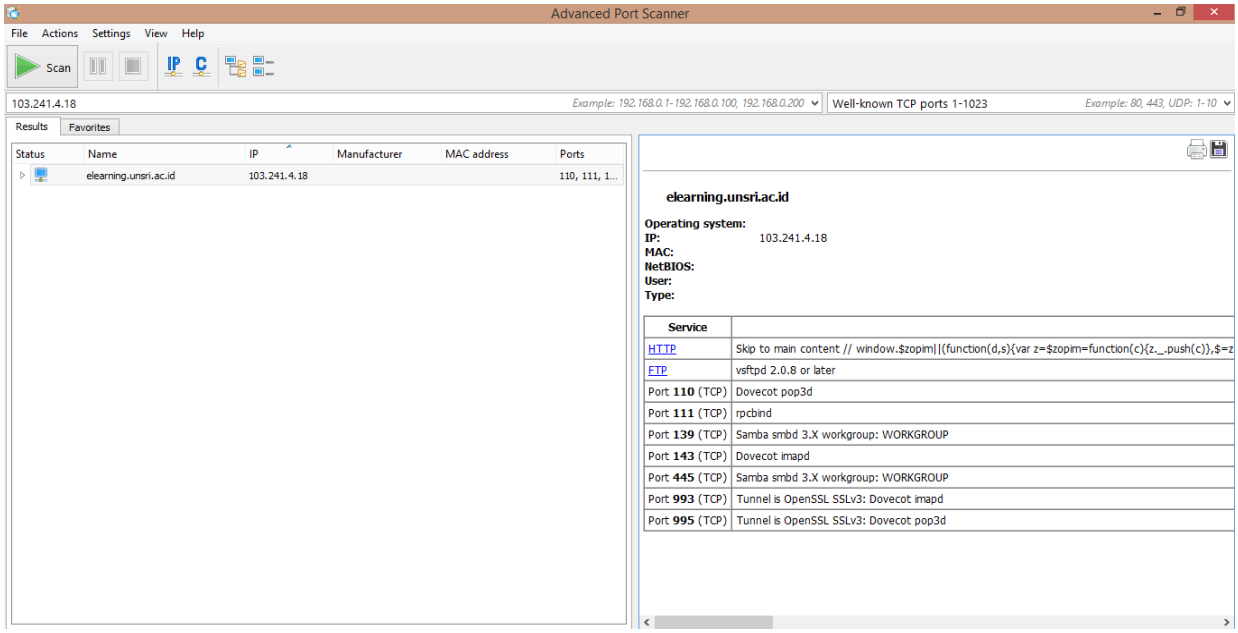


Analisa:

Dari scanning yang telah dilakukan dengan nikto, kita dapat melihat beberapa OSVDB dari situs elearning ini yang kemudian dapat kita gunakan untuk pencarian CVE Number.

4. Scanning dengan menggunakan Advance Port Scanner

Advanced Port Scanner adalah scanner jaringan gratis yang memungkinkan Anda untuk cepat menemukan port yang terbuka pada komputer jaringan dan mengambil versi program yang berjalan pada port terdeteksi. Program ini memiliki antarmuka yang user-friendly dan fungsionalitas yang kaya. Dibawah ini merupakan hasil daripada scanning dengan menggunakan Advanced Port Scanner:



Analisa:

Dari hasil scanning dengan menggunakan Advanced Port Scanner, kita dapat melihat daripada situs elearning unsri ini terdapat 7 port yang terbuka dan dapat diakses.

Mapping CVE Number