

Nama :Muhammad Aunillah Alghifari

NIM : 20102265

kelas : S1IF08T11

1 & 2.1. Footprinting adalah mencari informasi dari sebuah web. Footprinting yang saya pakai yaitu nmap dan whois

```
(maunillaha@kali)-[~]
$ nmap ampta.ac.id
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-22 16:59 WIB
Nmap scan report for ampta.ac.id (103.253.212.218)
Host is up (0.000013s latency).
Other addresses for ampta.ac.id (not scanned): 2001:df0:27b:2::3:82d9
rDNS record for 103.253.212.218: udawa.dua.rumahweb.com
Not shown: 476 filtered tcp ports (net-unreach), 460 filtered tcp ports (no-response), 54 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
Nmap done: 1 IP address (1 host up) scanned in 39.34 seconds
```

dari nmap ini, didapatkan sebuah ipnya, port2 apa saja yang open.

List port yang open :

port	service	fungsi
21	ftp	protokol yang melayani user untuk melakukan transfer data dua arah
25	smtp	email yang ingin dikirimkan oleh pengirim akan diterima dengan mudah oleh penerimanya
80	http	Mengatur format dan bagaimana data ditransmisikan
110	pop3	Jenis protokol yang digunakan untuk mengirim email
143	imap	Memungkinkan mengakses email di mana saja dan diperangkat mana saja
443	https	Sama dengan http tetapi memiliki tingkat keamanan yang lebih baik
465	smtps	Sama dengan smtp tetapi dengan tingkat keamanan yang lebih baik
587	submission	Port yang bisa digunakan untuk relaying, seperti komunikasi antar mail server
993	imaps	Sama seperti imap tetapi dengan tingkat keamanan yang lebih baik
995	pop3s	Sama seperti pop3 tetapi dengan tingkat keamanan yang lebih baik

```
(maunillaha@kali)-[~]
$ whois 103.253.212.218
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '103.253.212.0 - 103.253.215.255'

% Abuse contact for '103.253.212.0 - 103.253.215.255' is 'abuse@rumahweb.com'

inetnum:        103.253.212.0 - 103.253.215.255
netname:        IDNIC-DIGITALREGISTRA-ID
descr:          PT Digital Registra Indonesia
descr:          Corporate / Direct Member IDNIC
descr:          Citylofts Sudirman LT 25, Unit 2526
descr:          Jakarta Pusat
admin-c:        AP370-AP
tech-c:         AP370-AP
country:        ID
mnt-by:         MNT-APJII-ID
mnt-irt:        IRT-DIGITALREGISTRA-ID
mnt-routes:     MAINT-ID-DIGITALREGISTRA
status:         ASSIGNED PORTABLE
last-modified:  2013-11-22T10:02:01Z
source:         APNIC

irt:            IRT-DIGITALREGISTRA-ID
address:        PT Digital Registra Indonesia
address:        Citylofts Sudirman LT 25, Unit 2526
address:        Jakarta Pusat
e-mail:         abuse@rumahweb.com
abuse-mailbox:  abuse@rumahweb.com
admin-c:        AP370-AP
tech-c:         AP370-AP
auth:           # Filtered
mnt-by:         MAINT-ID-DIGITALREGISTRA
last-modified:  2018-05-31T22:30:22Z
source:         APNIC

person:         Agung Priaprabakti
address:        Jl. Lemponsari 39 C
address:        Sariharjo, Ngaglik, Sleman 55581
address:        DI Yogyakarta - Indonesia
country:        ID
phone:          +62-274-882257
fax-no:         +62-274-4463621
e-mail:         noc@rumahweb.co.id
nic-hdl:        AP370-AP
mnt-by:         MAINT-ID-RUMAHWEB
last-modified:  2011-12-08T04:47:31Z
source:         APNIC

% Information related to '103.253.212.0 - 103.253.215.255'

inetnum:        103.253.212.0 - 103.253.215.255
```

```

last-modified: 2011-12-08T04:47:31Z
source: APNIC

% Information related to '103.253.212.0 - 103.253.215.255'

inetnum: 103.253.212.0 - 103.253.215.255
netname: IDNIC-DIGITALREGISTRA-ID
descr: PT Digital Registra Indonesia
descr: Corporate / Direct Member IDNIC
descr: Citylofts Sudirman LT 25, Unit 2526
descr: Jakarta Pusat
admin-c: AP370-AP
tech-c: AP370-AP
country: ID
mnt-by: MNT-APJII-ID
mnt-irt: IRT-DIGITALREGISTRA-ID
mnt-routes: MAINT-ID-DIGITALREGISTRA
status: ASSIGNED PORTABLE
last-modified: 2013-11-22T10:02:01Z
source: IDNIC

irt: IRT-DIGITALREGISTRA-ID
address: PT Digital Registra Indonesia
address: Citylofts Sudirman LT 25, Unit 2526
address: Jakarta Pusat
e-mail: abuse@rumahweb.com
abuse-mailbox: abuse@rumahweb.com
admin-c: AP370-AP
tech-c: AP370-AP
auth: # Filtered
mnt-by: MAINT-ID-DIGITALREGISTRA
last-modified: 2013-10-18T07:38:48Z
source: IDNIC

person: Agung Priaprabakti
address: Jl. Lemponsari 39 C
address: Sariharjo, Ngaglik, Sleman 55581
address: DI Yogyakarta - Indonesia
country: ID
phone: +62-274-882257
fax-no: +62-274-4463621
e-mail: noc@rumahweb.co.id
nic-hdl: AP370-AP
mnt-by: MAINT-ID-RUMAHWEB
last-modified: 2011-12-08T04:47:31Z
source: IDNIC

% This query was served by the APNIC Whois Service version 1.88.16 (WHOIS-JP1)

```

Dari whois ini, didapatkan data data nama pemilik dari web seperti alamat, email, nama perusahaan hingga nomer telepon

## 2.1

```
(maunillaha@kali)-[~]
$ nmap ampta.ac.id
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-22 16:59 WIB
Nmap scan report for ampta.ac.id (103.253.212.218)
Host is up (0.000013s latency).
Other addresses for ampta.ac.id (not scanned): 2001:df0:27b:2::3:82d9
rDNS record for 103.253.212.218: udawa.dua.rumahweb.com
Not shown: 476 filtered tcp ports (net-unreach), 460 filtered tcp ports (no-response), 54 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 39.34 seconds
```

Port	service	step-hacking
21	ftp	MSF
25	smtp	Nmap dan Sntp-user-enum tools
80	http	nmap, nikto dan cadaver
110	pop3	capa
143	imap	imap bruteforce
443	https	
465	smtps	
587	submission	
993	imaps	
995	pop3s	

## 2.2. mencari vulnerabilities dari acunetix

acunetix Administrator

Scan

Stop Scan Pause Scan Generate Report WAF Export

Scan Information	Vulnerabilities	Site Structure	Events
Severity	Vulnerability	URL	Parameter Status Confidence %
🔧	Directory listing	http://www.ampta.ac.id/lib/animate/	Open 100
🔧	HTML form without CSRF protection	http://www.ampta.ac.id/	<empty> Open 80
🔧	HTML form without CSRF protection	http://www.ampta.ac.id/alumni/2022/0/0/alumni-ampta.html	form_cari Open 80
🔧	HTML form without CSRF protection	http://www.ampta.ac.id/alumni/2022/0/0/alumni-ampta.html	<empty> Open 80
🔧	HTML form without CSRF protection	http://www.ampta.ac.id/galeri/0/0/0/galeri.html	form_cari Open 80
🔧	HTML form without CSRF protection	http://www.ampta.ac.id/menu/2022/52/0/informasi-pendaftaran-stp-a mpta-2022-2023.html	form_cari Open 80
🔧	HTML form without CSRF protection	http://www.ampta.ac.id/contact.html	<empty> Open 80
🔧	Slow HTTP Denial of Service Attack	http://www.ampta.ac.id/	Open 95
🔧	Clickjacking: X-Frame-Options header missing	http://www.ampta.ac.id/	Open 95
🔧	Email address found	http://www.ampta.ac.id/alumni/2022/0/0/alumni-ampta.html	Open 95

Items per page: 20 1 - 10 of 10

Administrator

- Dashboard
- Targets
- Vulnerabilities
- Scans**
- Reports
- Users
- Scan Types
- Network Scanner
- Issue Trackers
- Email Settings
- Engines

Stop Scan
Pause Scan
Generate Report
WAF Export

Scan Information		Vulnerabilities	Site Structure	Events	
Severity	Vulnerability	URL	Parameter	Status	Confidence %
High	Cross site scripting	http://www.ampta.ac.id/galeri/		Open	95
Medium	Directory listing	http://www.ampta.ac.id/lib/bootstrap/		Open	100
Medium	Directory listing	http://www.ampta.ac.id/lib/bootstrap/css/		Open	100
Medium	Directory listing	http://www.ampta.ac.id/lib/font-awesome/		Open	100
Medium	Directory listing	http://www.ampta.ac.id/lib/font-awesome/css/		Open	100
Medium	Directory listing	http://www.ampta.ac.id/css/uploads/		Open	100
Medium	Directory listing	http://www.ampta.ac.id/lib/animate/		Open	100

Administrator

- Dashboard
- Targets
- Vulnerabilities
- Scans**
- Reports
- Users
- Scan Types
- Network Scanner
- Issue Trackers
- Email Settings
- Engines

Stop Scan
Pause Scan
Generate Report
WAF Export

Scan Information		Vulnerabilities	Site Structure	Events	
Severity	Vulnerability	URL	Parameter	Status	Confidence %
High	HTML form without CSRF protection	http://www.ampta.ac.id/	<empty>	Open	80
High	HTML form without CSRF protection	http://www.ampta.ac.id/alumni/2022/0/0/alumni-ampta.html	form_cari	Open	80
High	HTML form without CSRF protection	http://www.ampta.ac.id/alumni/2022/0/0/alumni-ampta.html	<empty>	Open	80
Medium	Slow HTTP Denial of Service Attack	http://www.ampta.ac.id/		Open	95
Medium	Clickjacking: X-Frame-Options header missing	http://www.ampta.ac.id/		Open	95
Medium	Possible virtual host found	http://www.ampta.ac.id/		Open	95
Medium	Unencrypted connection	http://www.ampta.ac.id/		Open	100
Low	Content Security Policy (CSP) not	...			

Setelah discan, terdapat vulnerabilities level 3, high level, yaitu cross site scripting (XSS). XSS ini adalah eksploitasi keamanan dimana penyerang menempatkan malicious client-end code ke laman web. Biasanya menggunakan script php.

Terdapat vurnerabilities level 2, medium level, yaitu directory listing. Cara hackingnya yaitu menggunakan dirbuster.