Nama : **M.Mahbubbillah**

NIM : **222011569**

No. Absen : **16**

Kelas : **3SI1**

Mata Kuliah : **Sistem Jaringan Komunikasi dan Data**

Tugas Pertemuan 13

```
[root@localhost ~]# nmap 1.1.1.1
Starting Nmap 7.70 ( https://nmap.org ) at 2022-12-06 14:09 WIB
Nmap scan report for one.one.one.one (1.1.1.1)
Host is up (0.053s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 9.37 seconds
```

Lakukan dan elaborasi hasil scanning pada situs web diatas terkait hal-hal berikut, laporan dibuat oleh masing-masing mahasiswa:

a. Sistem operasi yang digunakan oleh server target

Ruangguru (Swasta)

```
[root@localhost ~]# nmap -O --osscan-guess ruangguru.com
Starting Nmap 7.70 ( https://nmap.org ) at 2022-12-06 14:19 WIB
Nmap scan report for ruangguru.com (104.18.3.2)
Host is up (0.010s latency).
Other addresses for ruangguru.com (not scanned): 104.18.2.2 2606:4700::6812:202 2606:4700::6812:302
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Crestron XPanel control system (91%), ASUS RT-N56U WAP (Linux 3.4) (89%), Linux 3.1 (89%), Linux 3.16 (89%), Linux 3.2 (89%),
 AXIS 210A or 211 Network Camera (Linux 2.6.17) (88%), HP P2000 G3 NAS device (88%), Linux 4.10 (87%), Linux 2.6.32 (87%), Vodavi XTS-IP PBX (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.00 seconds
```

Aggressive OS guesses:

- Crestron XPanel control system (91%),
- ASUS RT-N56U WAP (Linux 3.4) (89%),
- Linux 3.1 (89%),
- Linux 3.16 (89%),
- Linux 3.2 (89%),
- AXIS 210A or 211 Network Camera (Linux 2.6.17) (88%),
- HP P2000 G3 NAS device (88%),
- Linux 4.10 (87%),
- Linux 2.6.32 (87%),
- Vodavi XTS-IP PBX (86%).

Pelatihan Kemnaker (Pemerintah)

```
[root@localhost ~]# nmap -O --osscan-guess digitalent.kominfo.go.id
Starting Nmap 7.70 ( https://nmap.org ) at 2022-12-06 14:30 WIB
Nmap scan report for digitalent.kominfo.go.id (103.168.134.11)
Host is up (0.012s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.81 seconds
```

Hasil :

- No OS matches for host

b. Port apa saja yang terbuka

Ruangguru (Swasta)

```
[root@localhost ~]# nmap ruangguru.com
Starting Nmap 7.70 ( https://nmap.org ) at 2022-12-06 14:32 WIB
Nmap scan report for ruangguru.com (104.18.3.2)
Host is up (0.0095s latency).
Other addresses for ruangguru.com (not scanned): 104.18.2.2 2606:4700::6812:202 2606:4700::6812:302
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 21.93 seconds
```

Pelatihan Kemnaker (Pemerintah)

```
[root@localhost ~]# nmap digitalent.kominfo.go.id
Starting Nmap 7.70 ( https://nmap.org ) at 2022-12-06 14:35 WIB
Nmap scan report for digitalent.kominfo.go.id (103.168.134.11)
Host is up (0.013s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```

c. Layanan yang disediakan oleh server tersebut

Ruangguru (Swasta)

```
[root@localhost ~]# nmap -T4 ruangguru.com
Starting Nmap 7.70 ( https://nmap.org ) at 2022-12-06 14:47 WIB
Nmap scan report for ruangguru.com (104.18.2.2)
Host is up (0.017s latency).
Other addresses for ruangguru.com (not scanned): 104.18.3.2 2606:4700::6812:302 2606:4700::6812:202
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 14.01 seconds
```

Pelatihan Kemnaker (Pemerintah)

```
[root@localhost ~]# nmap -T4 digitalent.kominfo.go.id
Starting Nmap 7.70 ( https://nmap.org ) at 2022-12-06 14:50 WIB
Nmap scan report for digitalent.kominfo.go.id (103.168.134.11)
Host is up (0.012s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 308.09 seconds
```

d. Cari celah kemanan berdasarkan parameter –script vuln di server tersebut

Ruangguru (Swasta)

```
[root@localhost ~]# nmap -Pn --script vuln ruangguru.com
Starting Nmap 7.70 ( https://nmap.org ) at 2022-12-06 14:58 WIB
Nmap scan report for ruangguru.com (104.18.3.2)
Host is up (0.058s latency).
Other addresses for ruangguru.com (not scanned): 104.18.2.2 2606:
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp  open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:
8080/tcp open  http-proxy
|_http-passwd: ERROR: Script execution failed (use -d to debug)
8443/tcp open  https-alt
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_sslv2-drown:

Nmap done: 1 IP address (1 host up) scanned in 223.15 seconds
```

Vulnerability :

- Tidak Terdapat Vulnerability

```
Nmap done: 1 IP address (1 host up) scanned in 223.15 seconds
[root@localhost ~]# nmap -Pn --script vuln digitalent.kominfo.go.id
Starting Nmap 7.70 ( https://nmap.org ) at 2022-12-06 15:03 WIB
Nmap scan report for digitalent.kominfo.go.id (103.168.134.11)
Host is up (0.014s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp open  https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

```
|_  /README.txt: Interesting, a readme.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_sslv2-drown:
```

Vulnerability :

- Slowloris DOS attack

  | State: LIKELY VULNERABLE

  | IDs: CVE:CVE-2007-6750

  | Slowloris tries to keep many connections to the target web server open and hold

  | them open as long as possible. It accomplishes this by opening connections to

  | the target web server and sending a partial request. By doing so, it starves

  | the http server's resources causing Denial Of Service.