Praktikum Sistem Jaringan Komputer dan Komunikasi Data

Modul 13

Kelompok 1 3SI2 :

1. Muhammad Afnan Falieh (222011494)
2. Rarisza Nabila (222011617)
3. Steven Fitraeka Setiawan S (221910702)
4. M. Taufiqqurrahman (222011361)
5. Arief Satrio Laksono (222011790)

- BRI (bri.co.id)
    - Sistem operasi yang digunakan oleh server target

```
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|5.X|2.6.X|3.X (92%)
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kern
el:3.10
Aggressive OS guesses: Linux 4.15 - 5.6 (92%), Linux 5.0 - 5.4 (92%), Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (92%), Li
nux 4.4 (92%), Linux 5.0 - 5.3 (90%), Linux 5.4 (90%), Linux 4.0 (90%), Linux 2.6.32 - 2.6.35 (88%), Linux 2.6.32 - 2.6.
39 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 8 hops
```

- Port apa saja yang terbuka

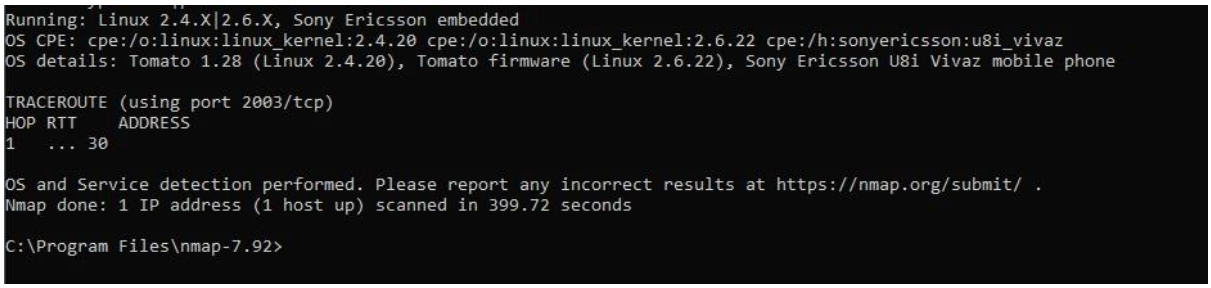
```
C:\Users\ACER>nmap --top-ports 20 bri.co.id
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 08:28 SE Asia Standard Time
Nmap scan report for bri.co.id (45.60.3.209)
Host is up (0.14s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   open     smtp
53/tcp   open     domain
80/tcp   open     http
110/tcp  filtered pop3
111/tcp  filtered rpcbind
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  open     https
445/tcp  filtered microsoft-ds
993/tcp  filtered imaps
995/tcp  open     pop3s
1723/tcp filtered pptp
3306/tcp open     mysql
3389/tcp open     ms-wbt-server
5900/tcp open     vnc
8080/tcp open     http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.33 seconds
```

- Layanan yang disediakan oleh server tersebut

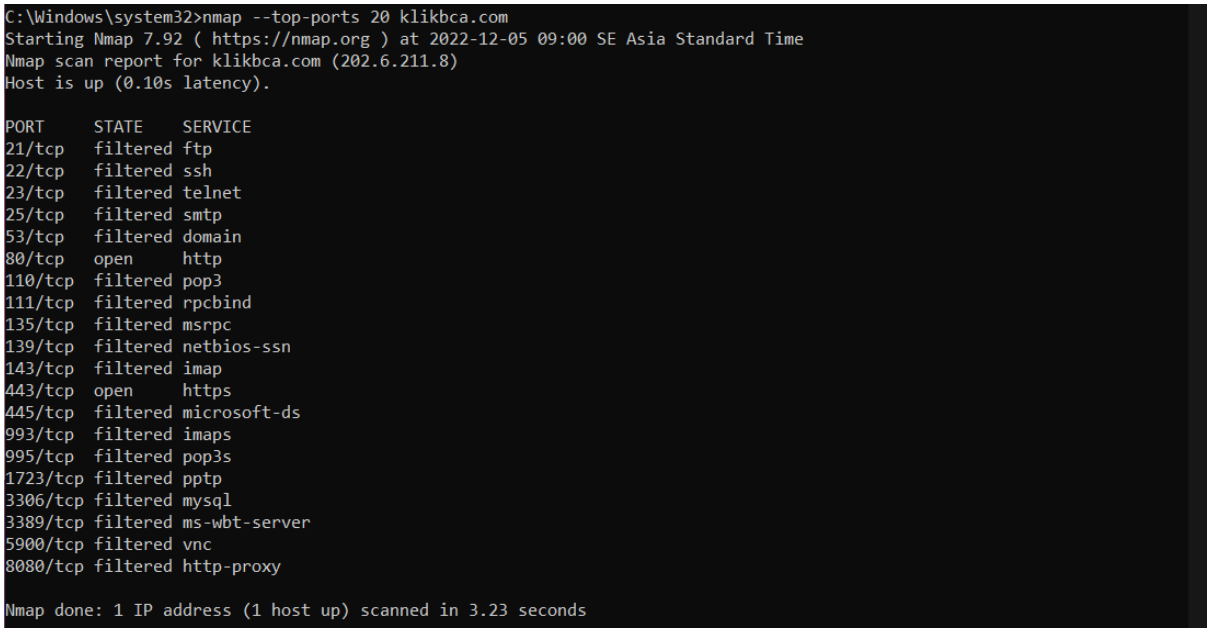
  HTTP, HTTPS, Fingerprint
- Celah keamanan berdasarkan parameter -script vuln di server tersebut

```
Nmap scan report for bri.co.id (45.60.3.209)
Host is up (0.085s latency).
Not shown: 689 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
37/tcp    open  time
53/tcp    open  domain
80/tcp    open  http
|_http-vuln-cve2013-7091: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_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)
81/tcp    open  hosts2-ns
82/tcp    open  xfer
83/tcp    open  mit-ml-dev
84/tcp    open  ctf
85/tcp    open  mit-ml-dev
88/tcp    open  kerberos-sec
89/tcp    open  su-mit-tg
90/tcp    open  dnsix
99/tcp    open  metagram
100/tcp   open  newacct
212/tcp   open  anet
389/tcp   open  ldap
443/tcp   open  https
|_http-vuln-cve2013-7091: ERROR: Script execution failed (use -d to debug)
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

- BCA (klikbca.com)
    - Sistem operasi yang digunakan oleh server target



    - Port apa saja yang terbuka



- Layanan yang disediakan oleh server tersebut

HTTP, HTTPS, Finger

- Celah keamanan berdasarkan parameter -script vuln di server tersebut

```
Nmap scan report for klikbca.com (202.6.211.8)
Host is up (0.12s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
443/tcp  open  https
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
2003/tcp open  finger

Nmap done: 1 IP address (1 host up) scanned in 257.23 seconds
```