TUGAS SCANNING
KEAMANAN JARINGAN KOMPUTER

Devi Purnama

09011281320016

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

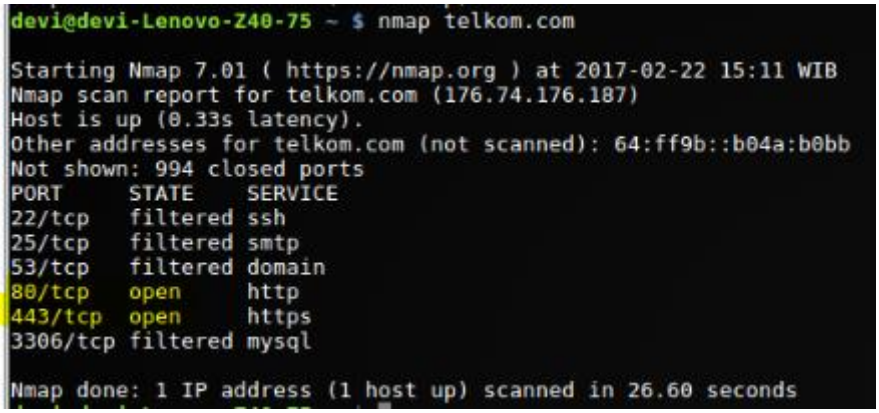
2017

Hasil Scanning pada

Nama Domain : Telkom.Com

IP Address : 176.74.176.186

- Scaning yaitu sebuah teknik untuk mencari port atau pintu masuk yang terbuka dari target. Scanning adalah metode bagaimana caranya mendapatkan informasi sebanyak-banyaknya dari IP/Network korban. Biasanya "scanning" dijalankan secara otomatis mengingat scanning pada multiple-host sangat menyita waktu.
- Untuk mengetahui domain yang ingin kita ketahui maka kita harus mengetahui nama domain, IP Address.
- Untuk mengetahui port yang aktf pada telkom.com maka bisa menggunakan nmap telkom.com maka akan muncul port yang di buka dapat kita lihat pada hasil di bawah ini.



```
Starting Nmap 6.00 ( http://nmap.org ) at 2017-02-22 10:07 EET
NSE: Loaded 17 scripts for scanning.
Initiating SYN Stealth Scan at 10:07
Scanning telkom.com (176.74.176.187) [100 ports]
Discovered open port 80/tcp on 176.74.176.187
Discovered open port 443/tcp on 176.74.176.187
Completed SYN Stealth Scan at 10:07, 1.24s elapsed (100 total ports)
Initiating Service scan at 10:07
Scanning 2 services on telkom.com (176.74.176.187)
Completed Service scan at 10:07, 12.10s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against telkom.com (176.74.176.187)
Retrying OS detection (try #2) against telkom.com (176.74.176.187)
Initiating Traceroute at 10:07
Completed Traceroute at 10:07, 0.01s elapsed
NSE: Script scanning 176.74.176.187.

[+] Nmap scan report for telkom.com (176.74.176.187)
Host is up (0.0060s latency).
Not shown: 96 closed ports

PORT     STATE    SERVICE  VERSION
22/tcp   filtered ssh
80/tcp   open     http     Apache httpd 2.2.22 ((Ubuntu))
443/tcp  open     ssl/http Apache httpd 2.2.22 ((Ubuntu))
3306/tcp filtered mysql

Device type: WAP|media device|general purpose|webcam|specialized|storage-misc
Running (JUST GUESSING): Netgear embedded (96%), Western Digital embedded (96%), Linux 2.6.X|3.X|
OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3 cpe:/o:axis:linux:2.6 cpe:/o:crestron:2_ser

Aggressive OS guesses: Netgear DG834G WAP or Western Digital WD TV media player (96%), Linux 2.6.

Aggressive OS guesses: Netgear DG834G WAP or Western Digital WD TV media player (96%), Linux 2.6.
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 99.120 days (since Tue Nov 15 07:13:52 2016)
Network Distance: 6 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros


TRACEROUTE (using port 113/tcp)
HOP RTT     ADDRESS
1   1.00 ms router1-lon.linode.com (212.111.33.229)
2   1.84 ms switch-lonr1.linode.com (109.74.207.4)
3   1.05 ms 109.74.207.9
4   2.65 ms 10ge.xe-1-0-0.ldn-eqx-cor-1.peer1.net (216.187.112.182)
5   4.48 ms 10ge.xe-0-1-0.por-5ltp1ops-dis-3.peer1.net (216.187.113.157)
6   4.91 ms 176.74.176.187

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit.

Nmap done: 1 IP address (1 host up) scanned in 18.39 seconds
           Raw packets sent: 156 (8.484KB) | Rcvd: 146 (7.840KB)
```

TCP Port Scan with Nmap

Test parameters: **Test date:** 22-Feb-2017, 10:07:02

- Host telkom.com
- Ports Top 100 common ports
- Ping host False
- Detect OS True
- Detect svc version True
- Traceroute True

Test result:

```
Starting Nmap 6.00 ( http://nmap.org ) at 2017-02-22 10:07 EET
NSE: Loaded 17 scripts for scanning.
Initiating SYN Stealth Scan at 10:07
Scanning telkom.com (176.74.176.187) [100 ports]
Discovered open port 80/tcp on 176.74.176.187
Discovered open port 443/tcp on 176.74.176.187
Completed SYN Stealth Scan at 10:07, 1.24s elapsed (100 total ports)
Initiating Service scan at 10:07
Scanning 2 services on telkom.com (176.74.176.187)
Completed Service scan at 10:07, 12.10s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against telkom.com (176.74.176.187)
Retrying OS detection (try #2) against telkom.com (176.74.176.187)
Initiating Traceroute at 10:07
Completed Traceroute at 10:07, 0.01s elapsed
NSE: Script scanning 176.74.176.187.

[+] Nmap scan report for telkom.com (176.74.176.187)

Host is up (0.0068s latency).
Not shown: 96 closed ports

PORT     STATE    SERVICE  VERSION

22/tcp   filtered ssh
80/tcp   open     http     Apache httpd 2.2.22 ((Ubuntu))
443/tcp  open     ssl/http Apache httpd 2.2.22 ((Ubuntu))
3306/tcp filtered mysql

Device type: WAP|media device|general purpose|webcam|specialized|storage-misc

Running (JUST GUESSING): Netgear embedded (96%), Western Digital embedded (96%), Linux 2.6.X|3.X|2.4.X (95%), AXIS Linux 2.6.X (92%), Crestron 2-Series (91%), HP embedded (89%)
OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3 cpe:/o:axis:linux:2.6 cpe:/o:crestron:2_series cpe:/o:linux:kernel:2.4.26

Aggressive OS guesses: Netgear DG834G WAP or Western Digital WD TV media player (96%), Linux 2.6.38 - 3.2 (95%), Linux 3.0 - 3.1 (94%), Linux 2.6.38 - 3.0 (94%), AXIS 210A or 211 Network

No exact OS matches for host (test conditions non-ideal).
Uptime guess: 99.128 days (since Tue Nov 15 07:13:52 2016)
Network Distance: 6 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros


TRACEROUTE (using port 113/tcp)

HOP RTT     ADDRESS
1   1.00 ms router1-lon.linode.com (212.111.33.229)
2   1.84 ms switch-lonr1.linode.com (109.74.207.4)
3   1.85 ms 109.74.207.9
4   2.65 ms 10ge.xe-1-0-0.ldn-eqx-cor-1.peer1.net (216.187.112.182)
5   4.48 ms 10ge.xe-0-1-0.por-5ltpiops-dis-3.peer1.net (216.187.113.157)
6   4.91 ms 176.74.176.187

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 18.39 seconds

          Raw packets sent: 156 (8.484KB) | Rcvd: 146 (7.848KB)
```

- http://toolbar.netcraft.com/site_report?url=telkom.com
- menggunakan alamat website yaitu toolbar netcraft, yang berfungi Untuk memberikan informasi website yang akan di kunjungi, informasi yang terdapat pada alamat ini bisa berupa Background, Network, Hosting History. pada network ini kita bisa mengetahui beberapa informasi yang terdapat pada network telkom.com seperti Site, Domain, IP address, domain register, Organisation, Top level domain. Pada Hosting History ada

beberapa informasi yang dapat kita lihat seperti Netblock owner Ip Address, OS, Web server, Last seen. Disini kita dapat mengetahui aplikasi/softwarenya untuk keperluan web server. Untuk mengetahui keperluan web server ada beberapa OS dan Web server yang di gunakan.

Background

Site title	telkom.com	**Date first seen**	April 1999
Site rank		**Primary language**	English
Description	*Not Present*		
Keywords	*Not Present*		

Network

Site	http://telkom.com	**Netblock Owner**	Schilling Aviation
Domain	telkom.com	**Nameserver**	ns1.uniregistrymarket.link
IP address	176.74.176.187	**DNS admin**	hostmaster@hostingnet.com
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	uniregistrar.com	**Nameserver organisation**	*unknown*
Organisation	Name Administration Inc. (BVI), Box 10518 Apo, Grand Cayman, KY1-1105, Cayman Islands	**Hosting company**	Cogeco Cable Canada
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	UK		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
DosArrest 600 West 7th Street Los Angeles CA US 90017	69.172.201.153	Linux	DOSarrest	19-Jun-2016
DosArrest 600 West 7th Street Los Angeles CA US 90017	69.172.201.208	unknown	nginx/1.7.5	17-Dec-2014
Secure Hosting Ltd. PO BOX CB13862 Nassau NP BS CB13862	208.87.35.104	Linux	Apache/2.2.22 Ubuntu	12-Feb-2014
Schilling Aviation	176.74.176.178	Linux	Apache/2.2.22 Ubuntu	10-Feb-2014
Secure Hosting Ltd. PO BOX CB13862 Nassau NP BS CB13862	208.87.35.108	Linux	Apache/2.2.17 Ubuntu	21-Nov-2012
Secure Hosting Ltd. PO BOX CB13862 Nassau NP BS CB13862	208.87.35.105	Linux	Apache/2.2.17 Ubuntu	22-Jun-2012
Secure Hosting Ltd. PO BOX CB13862 Nassau NP BS CB13862	208.87.35.104	Linux	Apache/2.2.17 Ubuntu	29-Feb-2012
Secure Hosting Ltd. PO BOX CB13862 Nassau NP BS CB13862	208.87.32.68	Linux	Apache/2.2.3 CentOS	1-Jun-2011
Secure Hosting Ltd. PO BOX CB13862 Nassau NP BS CB13862	208.87.32.68	Linux	Apache/2.2.3 Red Hat	12-Oct-2010
Secure Hosting Ltd. PO BOX CB13862 Nassau NP BS CB13862	208.87.32.74	Linux	Apache/2.2.3 Red Hat	1-Nov-2009

- Untuk mengetahui name dan description pada web server di atas maka bisa di buka pada CVE seperti gambar di bawah ini :
- Disini ada beberapa description dari web server pada telkom.com

1. Apache/2.2.22 Ubuntu
2. nginx/1.7.5
3. Apache/2.2.17 Ubuntu
4. Apache/2.2.3 CentOS

Apache/2.2.22 Ubuntu

Name	Description
CVE-2013-5704	The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."

nginx/1.7.5

Name	Description
CVE-2016-5677	NUUO NVRmini 2 1.7.5 through 3.0.0, NUUO NVRsolo 1.0.0 through 3.0.0, and NETGEAR ReadyNAS Surveillance 1.1.1 through 1.4.1 have a hardcoded qwe23622260 password for the nuuoeng account, which allows remote attackers to obtain sensitive information via an __nvr_status___.php request.
CVE-2016-5676	cgi-bin/cgi_system in NUUO NVRmini 2 1.7.5 through 2.x, NUUO NVRsolo 1.7.5 through 2.x, and NETGEAR ReadyNAS Surveillance 1.1.1 through 1.4.1 allows remote attackers to reset the administrator password via a cmd=loaddefconfig action.
CVE-2016-5675	handle_daylightsaving.php in NUUO NVRmini 2 1.7.5 through 3.0.0, NUUO NVRsolo 1.0.0 through 3.0.0, NUUO Crystal 2.2.1 through 3.2.0, and NETGEAR ReadyNAS Surveillance 1.1.1 through 1.4.1 allows remote attackers to execute arbitrary PHP code via the NTPServer parameter.
CVE-2016-5674	__debugging_center_utils___.php in NUUO NVRmini 2 1.7.5 through 3.0.0, NUUO NVRsolo 1.7.5 through 3.0.0, and NETGEAR ReadyNAS Surveillance 1.1.1 through 1.4.1 allows remote attackers to execute arbitrary PHP code via the log parameter.

Apache/2.2.17 Ubuntu

Name	Description
CVE-2017-6056	It was discovered that a programming error in the processing of HTTPS requests in the Apache Tomcat servlet and JSP engine may result in denial of service via an infinite loop. The denial of service is easily achievable as a consequence of backporting a CVE-2016-6816 fix but not backporting the fix for Tomcat bug 57544. Distributions affected by this backporting issue include Debian (before 7.0.56-3+deb8u8 and 8.0.14-1+deb8u7 in jessie) and Ubuntu.
CVE-2016-5387	The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.
CVE-2016-3092	The MultipartStream class in Apache Commons Fileupload before 1.3.2, as used in Apache Tomcat 7.x before 7.0.70, 8.x before 8.0.36, 8.5.x before 8.5.3, and 9.x before 9.0.0.M7 and other products, allows remote attackers to cause a denial of service (CPU consumption) via a long boundary string.
CVE-2016-1513	The Impress tool in Apache OpenOffice 4.1.2 and earlier allows remote attackers to cause a denial of service (out-of-bounds read or write) or execute arbitrary code via crafted MetaActions in an (1) ODP or (2) OTP file.
CVE-2016-0763	The setGlobalContext method in org/apache/naming/factory/ResourceLinkFactory.java in Apache Tomcat 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.M3 does not consider whether ResourceLinkFactory.setGlobalContext callers are authorized, which allows remote authenticated users to bypass intended SecurityManager restrictions and read or write to arbitrary application data, or cause a denial of service (application disruption), via a web application that sets a crafted global context.
CVE-2016-0714	The session-persistence implementation in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.M2 mishandles session attributes, which allows remote authenticated users to bypass intended SecurityManager restrictions and execute arbitrary code in a privileged context via a web application that places a crafted object in a session.
CVE-2016-0706	Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.M2 does not place org.apache.catalina.manager.StatusManagerServlet on the org/apache/catalina/core/RestrictedServlets.properties list, which allows remote authenticated users to bypass intended SecurityManager restrictions and read arbitrary HTTP requests, and consequently discover session ID values, via a crafted web application.

Apache/2.2.3 CentOS

Name	Description
CVE-2016-5425	The Tomcat package on Red Hat Enterprise Linux (RHEL) 7, Fedora, CentOS, Oracle Linux, and possibly other Linux distributions uses weak permissions for /usr/lib/tmpfiles.d/tomcat.conf, which allows local users to gain root privileges by leveraging membership in the tomcat group.
CVE-2012-1006	Multiple cross-site scripting (XSS) vulnerabilities in Apache Struts 2.0.14 and 2.2.3 allow remote attackers to inject arbitrary web script or HTML via the (1) name or (2) lastName parameter to struts2-showcase/person/editPerson.action, or the (3) clientName parameter to struts2-rest-showcase/orders.
CVE-2011-2087	Multiple cross-site scripting (XSS) vulnerabilities in component handlers in the javatemplates (aka Java Templates) plugin in Apache Struts 2.x before 2.2.3 allow remote attackers to inject arbitrary web script or HTML via an arbitrary parameter value to a .action URI, related to improper handling of value attributes in (1) FileHandler.java, (2) HiddenHandler.java, (3) PasswordHandler.java, (4) RadioHandler.java, (5) ResetHandler.java, (6) SelectHandler.java, (7) SubmitHandler.java, and (8) TextFieldHandler.java.
CVE-2011-1772	Multiple cross-site scripting (XSS) vulnerabilities in XWork in Apache Struts 2.x before 2.2.3, and OpenSymphony XWork in OpenSymphony WebWork, allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) an action name, (2) the action attribute of an s:submit element, or (3) the method attribute of an s:submit element.
CVE-2007-1743	suexec in Apache HTTP Server (httpd) 2.2.3 does not verify combinations of user and group IDs on the command line, which might allow local users to leverage other vulnerabilities to create arbitrary UID/GID owned files if /proc is mounted. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root." In addition, because this is dependent on other vulnerabilities, perhaps this is resultant and should not be included in CVE.
CVE-2007-1742	suexec in Apache HTTP Server (httpd) 2.2.3 uses a partial comparison for verifying whether the current directory is within the document root, which might allow local users to perform unauthorized operations on incorrect directories, as demonstrated using "html_backup" and "htmleditor" under an "html" directory. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root."
CVE-2007-1741	Multiple race conditions in suexec in Apache HTTP Server (httpd) 2.2.3 between directory and file validation, and their usage, allow local users to gain privileges and execute arbitrary code by renaming directories or performing symlink attacks. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root."