LAPORAN

Data Collection dan Vulnerability Assesment (VA)

Pada Website www.telkom.co.id & www.kejaksaan.go.id

Oleh

Nama	: Nadia Yuniarti
NIM	: 09031181520039
Kelas	: SI Reguler 6A

JURUSAN SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

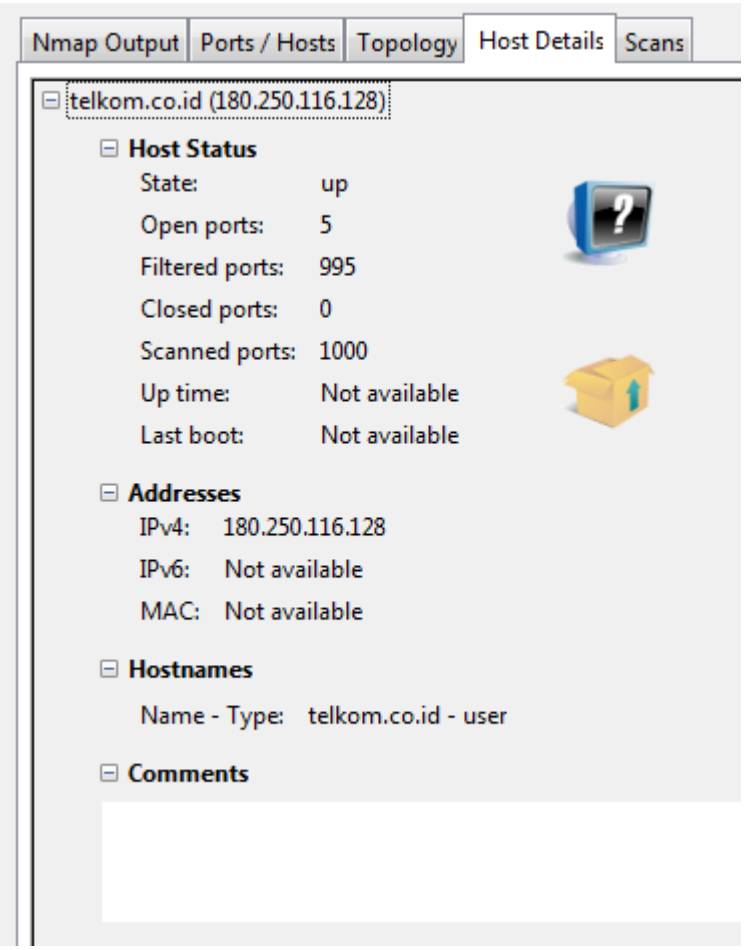
UNIVERSITAS SRIWIJAYA

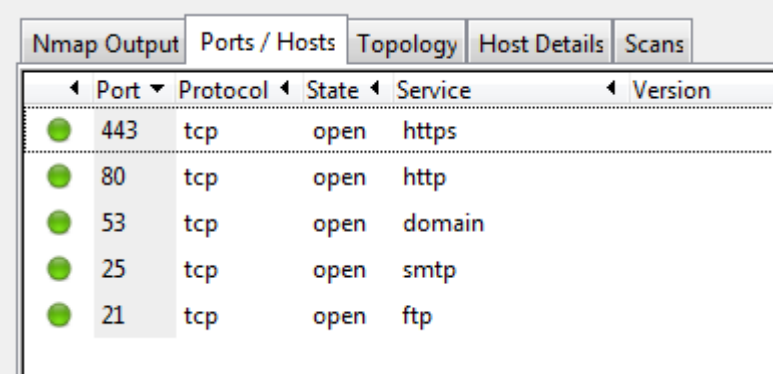
2018

Menentukan Target

Target yang digunakan www.telkom.co.id

Data Collection





Melakukan tahap awal yaitu Pentest (Penetration Testing) data collection dengan menggunakan tools seperti nmap dan netcraft. Setelah dilakukan scanning, didapatlah data bahwa telkom.co.id dengan IP address 180.250.116.128 memiliki port terbuka sebanyak 5 port.

Background

Site title	*Not Present*	**Date first seen**	October 1996
Site rank		**Primary language**	Unknown
Description	*Not Present*		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://telkom.co.id	**Netblock Owner**	PT TELKOM INDONESIA
Domain	telkom.co.id	**Nameserver**	ns1.telkom.net.id
IP address	180.250.116.128	**DNS admin**	hostmaster@telkom.net.id
IPv6 address	2001:4488:4:600d:0:0:0:3	**Reverse DNS**	*unknown*
Domain registrar	pandi.or.id	**Nameserver organisation**	whois.pandi.or.id
Organisation	PT. Telekomunikasi Indonesia, Jl. Kebon Sirih No. 12, DKI Jakarta, 10340, Indonesia	**Hosting company**	PT Telekomunikasi Indonesia Tbk
Top Level Domain	Indonesia (.co.id)	**DNS Security Extensions**	Enabled
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
PT TELKOM INDONESIA Menara Multimedia Lt. 7 Jl. Kebonsirih No.12 JAKARTA	180.250.116.128	unknown	BigIP	6-Mar-2018
PT TELKOM INDONESIA Menara Multimedia Lt. 7 Jl. Kebonsirih No.12 JAKARTA	180.250.116.128	Linux	Apache/2.4.6 Red Hat	27-Jun-2017
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	202.134.0.219	Linux	Apache/2.2.15 Red Hat	7-Mar-2017
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	202.134.0.219	F5 BIG-IP	unknown	31-Jul-2015
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	202.134.0.219	Linux	Apache/2.2.15 Red Hat	6-May-2014
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	202.134.0.219	unknown	Apache/2.2.15 Red Hat	10-Jan-2014
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	202.134.0.219	Linux	Apache/2.2.15 Red Hat	7-Jan-2014
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	202.134.0.219	unknown	Apache/2.2.15 Red Hat	13-Dec-2013
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	202.134.0.219	Linux	Apache/2.2.15 Red Hat	12-Dec-2013
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	202.134.0.219	unknown	Apache/2.2.15 Red Hat	11-Dec-2013

Vulnerability Assesment (VA)

Berikut hasil Vulnerability Assesment dengan CVE :

CVE-2012-3000

CVE-2012-3000	Multiple SQL injection vulnerabilities in sam/admin/reports/php/saveSettings.php in the (1) APM WebGUI in F5 BIG-IP LTM, GTM, ASM, Link Controller, PSM, APM, Edge Gateway, and Analytics and (2) AVR WebGUI in WebAccelerator and WOM 11.2.x before 11.2.0-HF3 and 11.2.x before 11.2.1-HF3 allow remote authenticated users to execute arbitrary SQL commands via the defaultQuery parameter.

– CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code Sql Injection
CWE ID	89

CVE-2012-1493

CVE-2012-1493	F5 BIG-IP appliances 9.x before 9.4.8-HF5, 10.x before 10.2.4, 11.0.x before 11.0.0-HF2, and 11.1.x before 11.1.0-HF3, and Enterprise Manager before 2.1.0-HF2, 2.2.x before 2.2.0-HF1, and 2.3.x before 2.3.0-HF3, use a single SSH private key across different customers' installations and do not properly restrict access to this key, which makes it easier for remote attackers to perform SSH logins via the PubkeyAuthentication option.

– CVSS Scores & Vulnerability Types

CVSS Score	7.8
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	255

CVE-1999-1550

CVE-1999-1550	bigconf.conf in F5 BIG/ip 2.1.2 and earlier allows remote attackers to read arbitrary files by specifying the target file in the "file" parameter.

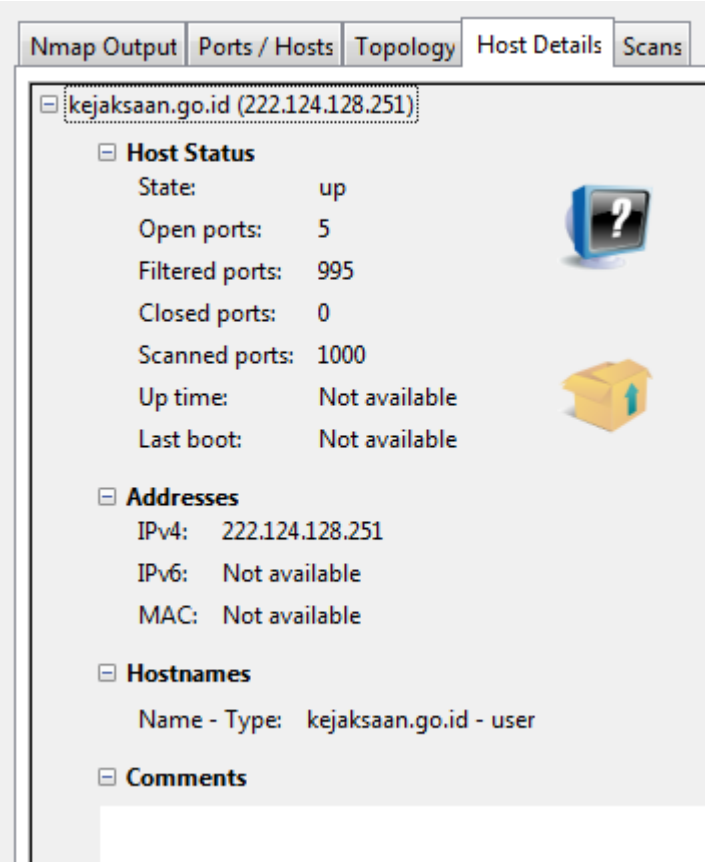
– CVSS Scores & Vulnerability Types

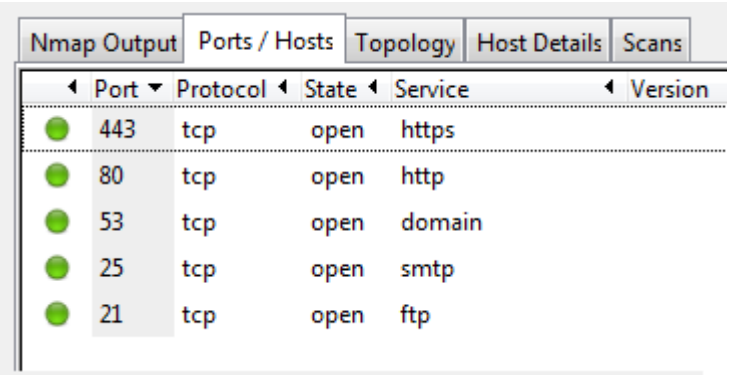
CVSS Score	**5.0**
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	CWE id is not defined for this vulnerability

Menentukan Target

Target yang digunakan www.kejaksaan.go.id

Data Collection





Melakukan tahap awal yaitu Pentest (Penetration Testing) data collection dengan menggunakan tools seperti nmap dan netcraft. Setelah dilakukan scanning, didapatlah data bahwa kejaksaan.go.id dengan IP address 222.124.128.251 memiliki port terbuka sebanyak 5 port.

Background

Site title	Kejaksaan Republik Indonesia	**Date first seen**	July 1999
Site rank		**Primary language**	Malay
Description	*Not Present*		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://kejaksaan.go.id	**Netblock Owner**	PT Telkom Indonesia's customer.
Domain	kejaksaan.go.id	**Nameserver**	ns1.telkomhosting.com
IP address	222.124.128.251	**DNS admin**	hostmaster@telkom.net.id
IPv6 address	*Not Present*	**Reverse DNS**	251.subnet222-124-128.static.astinet.telkom.net.id
Domain registrar	*unknown*	**Nameserver organisation**	whois.onlinenic.com
Organisation	*unknown*	**Hosting company**	PT Telekomunikasi Indonesia Tbk
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
PT Telkom Indonesias customer.	222.124.128.251	Linux	Apache/2.4.7 Ubuntu	6-Mar-2018
PT TELKOM INDONESIA Menara Multimedia Lt. 7 Jl. Kebonsirih No.12 JAKARTA	118.98.73.5	Linux	Apache	26-Feb-2017
PT TELKOM INDONESIA Menara Multimedia Lt. 7 Jl. Kebonsirih No.12 JAKARTA	118.98.73.5	Linux	Apache/2.2.27 Unix mod_ssl/2.2.27 OpenSSL/0.9.8e-fips-rhel5 mod_bwlimited/1.4	22-Feb-2016
PT TELKOM INDONESIA Menara Multimedia Lt. 7 Jl. Kebonsirih No.12 JAKARTA	118.98.73.5	Linux	Apache/2.2.26 Unix mod_ssl/2.2.26 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635	19-May-2014
PT TELKOM INDONESIA Menara Multimedia Lt. 7 Jl. Kebonsirih No.12 JAKARTA	180.250.82.162	Linux	Apache/2.2.3 CentOS	10-Nov-2013
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	125.160.17.121	Linux	-	4-Oct-2013
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	125.160.17.121	Linux	Apache/2.0.63 Unix mod_ssl/2.0.63 OpenSSL/0.9.8e-fips-rhel5 mod_mono/2.6.3 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.9	16-Jul-2011
PT TELKOM DIVISI MULTIMEDIA TELECOMMUNICATIONS/COMMUNICATIONS JL. KEBON SIRIH No.12 - 7th FLOOR JAKARTA	125.160.17.121	Linux	Apache/2.0.63 Unix mod_ssl/2.0.63 OpenSSL/0.9.8e-fips-rhel5 mod_auth_passthrough/2.1 mod_bwlimited/1.4 FrontPage/5.0.2.2635 PHP/5.2.9	24-Mar-2011
PT. TELEKOMUNIKASI INDONESIA JL. KEBONSIRIH NO. 37 JAKARTA	222.124.11.244	Linux	Apache/2.0.40 Red Hat Linux	18-Jan-2005
JASA ANGKASA SEMESTA JAKARTA	202.152.3.74	unknown	Apache/1.3.19 Unix PHP/4.2.2	24-Feb-2004

Vulnerability Assesment (VA)

Berikut hasil Vulnerability Assesment dengan CVE :

CVE-2014-3528

CVE-2014-3528	Apache Subversion 1.0.0 through 1.7.x before 1.7.17 and 1.8.x before 1.8.10 uses an MD5 hash of the URL and authentication realm to store cached credentials, which makes it easier for remote servers to obtain the credentials via a crafted authentication realm.

– CVSS Scores & Vulnerability Types

CVSS Score	**4.0**
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	255

CVE-2014-3522

CVE-2014-3522	The Serf RA layer in Apache Subversion 1.4.0 through 1.7.x before 1.7.18 and 1.8.x before 1.8.10 does not properly handle wildcards in the Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof servers via a crafted certificate.

– CVSS Scores & Vulnerability Types

CVSS Score	**4.0**
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	297

CVE-2013-2071

CVE-2013-2071	java/org/apache/catalina/core/AsyncContextImpl.java in Apache Tomcat 7.x before 7.0.40 does not properly handle the throwing of a RuntimeException in an AsyncListener in an application, which allows context-dependent attackers to obtain sensitive request information intended for other applications in opportunistic circumstances via an application that records the requests that it processes.

– CVSS Scores & Vulnerability Types

CVSS Score	2.6
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	None (There is no impact to the availability of the system.)
Access Complexity	High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Obtain Information
CWE ID	200

CVE-2013-1862

CVE-2013-1862	mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

– CVSS Scores & Vulnerability Types

CVSS Score	5.1
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	310

CVE-2013-1845

CVE-2013-1845	The mod_dav_svn Apache HTTPD server module in Subversion 1.6.x before 1.6.21 and 1.7.0 through 1.7.8 allows remote authenticated users to cause a denial of service (memory consumption) by (1) setting or (2) deleting a large number of properties for a file or directory.

– CVSS Scores & Vulnerability Types

CVSS Score	2.1
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	High (Specialized access conditions exist. It is hard to exploit and several special conditions must be satisfied to exploit)
Authentication	Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)
Gained Access	None
Vulnerability Type(s)	Denial Of Service Overflow
CWE ID	119