Laporan *Penetration Testing*

Pada *Website* Pemerintah & Pemberitaan Tingkat Kampus

(banyuasinkab.go.id & gelorasriwijaya.co)

Oleh

Aris Pratiwi **09031181520121**

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

TARGET 1

1. Menentukan Target

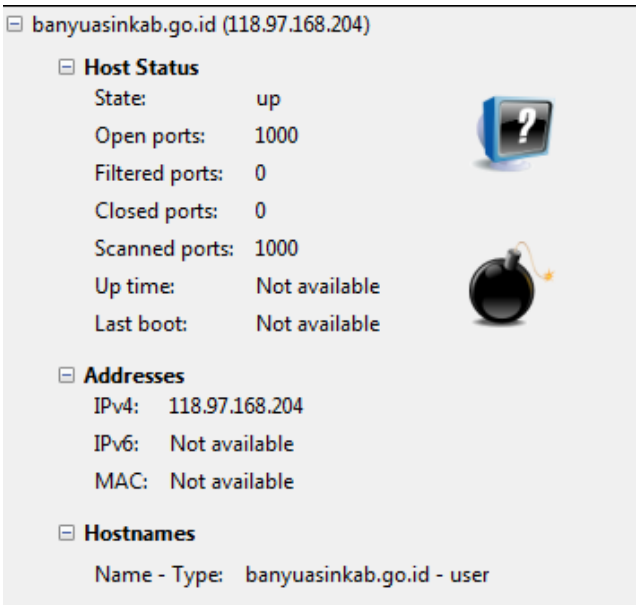
```
C:\Users\acer>ping banyuasinkab.go.id

Pinging banyuasinkab.go.id [118.97.168.204] with 32 bytes of data:
Reply from 118.97.168.204: bytes=32 time=221ms TTL=58
Reply from 118.97.168.204: bytes=32 time=258ms TTL=58
Reply from 118.97.168.204: bytes=32 time=395ms TTL=58
Reply from 118.97.168.204: bytes=32 time=252ms TTL=58

Ping statistics for 118.97.168.204:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 221ms, Maximum = 395ms, Average = 281ms
```

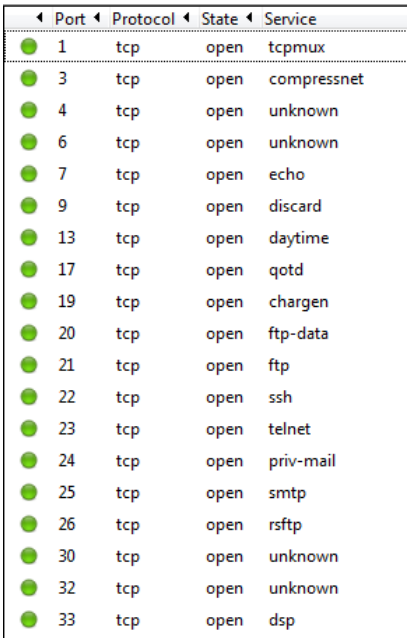
Target kali adalah banyuasinkab.go.id dengan IP address 118.97.168.204 alasan saya memilih targert ini karena saya ingin tahu keamanan dari *website* pemerintah daerah saya yaitu Kabupaten Banyuasin.

2. Data Collection

Data Collection dilakukan untuk mengumpulkan informasi (*information gathering*) dari targetnya, informasi yang di kumpulkan biasanya informasi ip, port, protokol, dns, record.

Kali ini saya akan melakukan tahap awal yaitu Pentest (*Penetration Testing*) *data collection* dengan menggunakan alat bantu atau *tools* seperti *nmap, nikto, netcraf* dan *nessus.* Pada kesempatan ini saya menggunakan *tools nmap* dan *netcraf,* setelah dilakukannya *scaning* didapatlah data bahwa *website* banyuasinkab.go.id dengan IP address 118.97.168.204 memiliki port terbuka sebanyak 1000 port.





Port	Protocol	State	Service
1	tcp	open	tcpmux
3	tcp	open	compressnet
4	tcp	open	unknown
6	tcp	open	unknown
7	tcp	open	echo
9	tcp	open	discard
13	tcp	open	daytime
17	tcp	open	qotd
19	tcp	open	chargen
20	tcp	open	ftp-data
21	tcp	open	ftp
22	tcp	open	ssh
23	tcp	open	telnet
24	tcp	open	priv-mail
25	tcp	open	smtp
26	tcp	open	rsftp
30	tcp	open	unknown
32	tcp	open	unknown
33	tcp	open	dsp

Gambar 2.1 Detail Scaning

2.3 Gambar Topologi IP ke Localhost

Background

Site title	Portal Resmi Pemerintah Kabupaten Banyuasin	**Date first seen**	June 2006
Site rank		**Primary language**	Indonesian
Description	*Not Present*		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	0/10		

Network

Site	http://banyuasinkab.go.id	**Netblock Owner**	PT Telkom Indonesia's customer
Domain	banyuasinkab.go.id	**Nameserver**	ns1.banyuasinkab.go.id
IP address	118.97.168.204	**DNS admin**	hostmaster@banyuasinkab.go.id
IPv6 address	*Not Present*	**Reverse DNS**	204.subnet118-97-168.static.astinet.telkom.net.id
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	PT Telekomunikasi Indonesia Tbk
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	Enabled
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
PT Telkom Indonesias customer	118.97.168.204	Linux	Apache/2	5-May-2014
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	75.126.30.10	-	Apache	6-Mar-2007
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	75.126.30.10	Linux	Apache/1.3.37 Unix mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 FrontPage/5.0.2.2635.SR1.2 PHP-CGI/0.1b	5-Mar-2007
SoftLayer Technologies Inc. 1950 N Stemmons Freeway Dallas TX US 75207	75.126.30.10	Linux	Apache	3-Mar-2007
PT Cakraperdana Proniagatama Gedung Elektrindo Lt 10 JL. Kuningan Barat no 8 Jakarta 12710	202.145.6.242	-	Apache/1.3.36 Unix PHP/5.1.4 mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 FrontPage/5.0.2.2635.SR1.2 mod_ssl/2.8.27 OpenSSL/0.9.7e-p1 PHP-CGI/0.1b	15-Aug-2006
PT Cakraperdana Proniagatama Gedung Elektrindo Lt 10 JL. Kuningan Barat no 8 Jakarta 12710	202.145.6.242	Linux	unknown	14-Aug-2006
PT Cakraperdana Proniagatama Gedung Elektrindo Lt 10 JL. Kuningan Barat no 8 Jakarta 12710	202.145.6.242	unknown	Apache/1.3.36 Unix PHP/5.1.4 mod_auth_passthrough/1.8 mod_log_bytes/1.2 mod_bwlimited/1.4 FrontPage/5.0.2.2635.SR1.2 mod_ssl/2.8.27 OpenSSL/0.9.7e-p1 PHP-CGI/0.1b	7-Aug-2006

2.4 Gambar Detail dengan *Netcraf*

3. *Vulnerability Assesment* (VA)

Vulnerability Assesment (VA) merupakan adalah pengukuran kelemahan atas serangan dari luar. Semakin kuat serangan yang datang dari luar, maka akan semakin banyak celah yang ditemukan. Jika serangan yang dilancarkan lemah, maka pentest tidak akan berjalan maksimal. Port-port yang terbuka bisa kita cari tingkat kelemahannya dengan menggunakan CVE.

Berikut Hasil *Vulnerability Assesment* dengan CVE (*Common Vurnerabilities and Exposures*) karena terdapat banyak port maka saya hanya menganalisa 10 port.

1) Port 1

Name	Description
CVE-2013-4342	xinetd does not enforce the user and group configuration directives for TCPMUX services, which causes these services to be run as root and makes it easier for remote attackers to gain privileges by leveraging another vulnerability in a service.
CVE-2012-0862	builtins.c in Xinetd before 2.3.15 does not check the service type when the tcpmux-server service is enabled, which exposes all enabled services and allows remote attackers to bypass intended access restrictions via a request to tcpmux port 1.

– CVSS Scores & Vulnerability Types

CVSS Score	4.3
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	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Bypass a restriction or similar
CWE ID	20

2) Port 21

Name	Description
CVE-2015-7261	The FTP service in QNAP iArtist Lite before 1.4.54, as distributed with QNAP Signage Station before 2.0.1, has hardcoded credentials, which makes it easier for remote attackers to obtain access via a session on TCP port 21.
CVE-2015-3968	The FTP service on Janitza UMG 508, 509, 511, 604, and 605 devices has a default password, which makes it easier for remote attackers to read or write to files via a session on TCP port 21.

– 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)	
CWE ID	255

3) Port 22

Name	Description
CVE-2017-3819	A privilege escalation vulnerability in the Secure Shell (SSH) subsystem in the StarOS operating system for Cisco ASR 5000 Series, ASR 5500 Series, ASR 5700 Series devices, and Cisco Virtualized Packet Core could allow an authenticated, remote attacker to gain unrestricted, root shell access. The vulnerability is due to missing input validation of parameters passed during SSH or SFTP login. An attacker could exploit this vulnerability by providing crafted user input to the SSH or SFTP command-line interface (CLI) during SSH or SFTP login. An exploit could allow an authenticated attacker to gain root privileges access on the router. Note: Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability can be triggered via both IPv4 and IPv6 traffic. An established TCP connection toward port 22, the SSH default port, is needed to perform the attack. The attacker must have valid credentials to login to the system via SSH or SFTP. The following products have been confirmed to be vulnerable: Cisco ASR 5000/5500/5700 Series devices running StarOS after 17.7.0 and prior to 18.7.4, 19.5, and 20.2.3 with SSH configured are vulnerable. Cisco Virtualized Packet Core - Single Instance (VPC-SI) and Distributed Instance (VPC-DI) devices running StarOS prior to N4.2.7 (19.3.v7) and N4.7 (20.2.v0) with SSH configured are vulnerable. Cisco Bug IDs: CSCva65853.

– CVSS Scores & Vulnerability Types

CVSS Score	9.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required 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)	Gain privileges
CWE ID	264

4) Port 23

Name	Description
CVE-2017-15376	The TELNET service in Mobatek MobaXterm 10.4 does not require authentication, which allows remote attackers to execute arbitrary commands via TCP port 23.
CVE-2014-7279	The Konke Smart Plug K does not require authentication for TELNET sessions, which allows remote attackers to obtain "equipment management authority" via TCP traffic to port 23.

– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
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
CWE ID	94

5) Port 7

Name	Description
CVE-2006-0374	Advantage Century Telecommunication (ACT) P202S IP Phone 1.01.21 running firmware 1.1.21 has multiple undocumented ports available, which (1) might allow remote attackers to obtain sensitive information, such as memory contents and internal operating-system data, by directly accessing the VxWorks WDB remote debugging ONCRPC (aka wdbrpc) on UDP 17185, (2) reflect network data using echo (TCP 7), or (3) gain access without authentication using rlogin (TCP 513).

– 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	User
Vulnerability Type(s)	Obtain Information
CWE ID	287

6) Port 9

Name	Description
CVE-2002-2148	Lucent Ascend MAX Router 5.0 and earlier, Lucent Ascend Pipeline Router 6.0.2 and earlier and Lucent DSLTerminator allows remote attackers to obtain sensitive information such as hostname, MAC, and IP address of the Ethernet interface via a discard (UDP port 9) packet, which causes the device to leak the information in the response.

– 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)	Obtain Information
CWE ID	CWE id is not defined for this vulnerability

7) Port 25

Name	Description
CVE-2006-1966	An unspecified Fortinet product, possibly Fortinet28, allows remote attackers to cause a denial of service via a "small synflood" to the SMTP port (TCP port 25), as demonstrated by a 10-microsecond wait between sending packets. NOTE: this issue has been disputed in followup posts that suggest that a protection feature is triggering a RST.
CVE-2004-2583	SMTP service in SmarterTools SmarterMail 1.6.1511 and 1.6.1529 allows remote attackers to cause a denial of service (CPU consumption) via a large number of simultaneous open connections to TCP port 25.

– CVSS Scores & Vulnerability Types

CVSS Score	5.0
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	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)	Denial Of Service
CWE ID	CWE id is not defined for this vulnerability

8) Port 33

Name	Description
CVE-2016-6422	Cisco IOS 12.2(33)SXJ9 on Supervisor Engine 32 and 720 modules for 6500 and 7600 devices mishandles certain operators, flags, and keywords in TCAM share ACLs, which allows remote attackers to bypass intended access restrictions by sending packets that should have been recognized by a filter, aka Bug ID CSCuy64806.

– CVSS Scores & Vulnerability Types

CVSS Score	4.3
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	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Bypass a restriction or similar
CWE ID	20

9) Port 19

Name	Description
CVE-2015-6510	Multiple cross-site scripting (XSS) vulnerabilities in pfSense before 2.2.3 allow remote attackers to inject arbitrary web script or HTML via the (1) srctrack, (2) use_mfs_tmp_size, or (3) use_mfs_var_size parameter to system_advanced_misc.php; the (4) port, (5) snaplen, or (6) count parameter to diag_packet_capture.php; the (7) pppoe_resethour, (8) pppoe_resetminute, (9) wpa_group_rekey, or (10) wpa_gmk_rekey parameter to interfaces.php; the (11) pppoe_resethour or (12) pppoe_resetminute parameter to interfaces_ppps_edit.php; the (13) member[] parameter to interfaces_qinq_edit.php; the (14) port or (15) retry parameter to load_balancer_pool_edit.php; the (16) pkgrepourl parameter to pkg_mgr_settings.php; the (17) zone parameter to services_captiveportal.php; the port parameter to (18) services_dnsmasq.php or (19) services_unbound.php; the (20) cache_max_ttl or (21) cache_min_ttl parameter to services_unbound_advanced.php; the (22) sshport parameter to system_advanced_admin.php; the (23) id, (24) tunable, (25) descr, or (26) value parameter to system_advanced_sysctl.php; the (27) firmwareurl, (28) repositoryurl, or (29) branch parameter to system_firmware_settings.php; the (30) pfsyncpeerip, (31) synchronizetoip, (32) username, or (33) passwordfld parameter to system_hasync.php; the (34) maxmss parameter to vpn_ipsec_settings.php; the (35) ntp_server1, (36) ntp_server2, (37) wins_server1, or (38) wins_server2 parameter to vpn_openvpn_csc.php; or unspecified parameters to (39) load_balancer_relay_action.php, (40) load_balancer_relay_action_edit.php, (41) load_balancer_relay_protocol.php, or (42) load_balancer_relay_protocol_edit.php.

– CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
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	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Cross Site Scripting
CWE ID	79

10) Port 20

CVE-2014-4309	Multiple cross-site scripting (XSS) vulnerabilities in Openfiler 2.99 allow remote attackers to inject arbitrary web script or HTML via the (1) TinkerAjax parameter to uptime.html, or remote authenticated users to inject arbitrary web script or HTML via the (2) MaxInstances, (3) PassivePorts, (4) Port, (5) ServerName, (6) TimeoutLogin, (7) TimeoutNoTransfer, or (8) TimeoutStalled parameter to admin/services_ftp.html; the (9) dns1 or (10) dns2 parameter to admin/system.html; the (11) newTgtName parameter to admin/volumes_iscsi_targets.html; the User-Agent HTTP header to (12) language.html, (13) login.html, or (14) password.html in account/; or the User-Agent HTTP header to (15) account_groups.html, (16) account_users.html, (17) services.html, (18) services_ftp.html, (19) services_iscsi_target.html, (20) services_rsync.html, (21) system_clock.html, (22) system_info.html, (23) system_ups.html, (24) volumes_editpartitions.html, or (25) volumes_iscsi_targets.html in admin/.

– CVSS Scores & Vulnerability Types

CVSS Score	4.3
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
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	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Cross Site Scripting
CWE ID	79

No	Port	CVSS Score	Colour	Access Complexity
1.	1	4.3		Low
2.	21	7.5		Low
3.	22	9.0		Low
4.	23	10.0		Low
5.	7	7.5		Low
6.	9	5.0		Low
7.	25	5.0		Low
8.	33	4.3		Low
9.	19	4.3		Low
10.	20	4.3		Low

Tabel 3.1 Ringkasan *Vulnerability* dengan CVE

Target 2

1) Menentukan Target

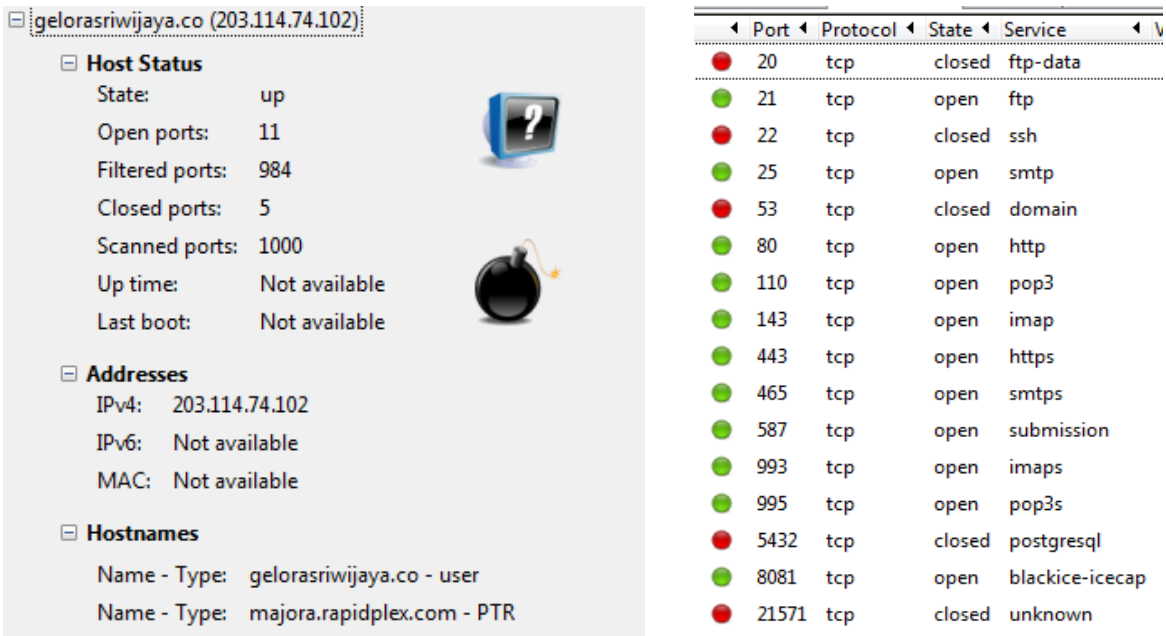
```
C:\Users\acer>ping gelorasriwijaya.co

Pinging gelorasriwijaya.co [203.114.74.102] with 32 bytes of data:
Reply from 203.114.74.102: bytes=32 time=121ms TTL=52
Reply from 203.114.74.102: bytes=32 time=113ms TTL=52
Reply from 203.114.74.102: bytes=32 time=146ms TTL=52
Reply from 203.114.74.102: bytes=32 time=117ms TTL=52

Ping statistics for 203.114.74.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 113ms, Maximum = 146ms, Average = 124ms
```

Target kali adalah gelorasriwijaya.co dengan IP address 203.114.74.102 alasan saya memilih targert ini karena saya ingin tahu keamanan dari *website* pemberitaaan mahasiswa yang mana LPMGS Unsri (Lembaga Pers Gelora Sriwijaya) merupakan salah satu organisasi yang saya ikuti.

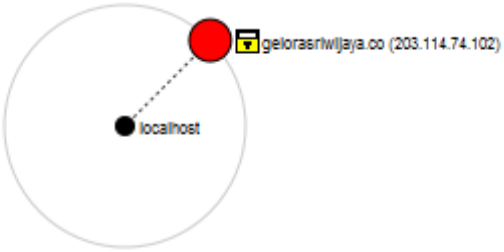
2) Data Collection

Data Collection dilakukan untuk mengumpulkan informasi (*information gathering*) dari targetnya, informasi yang di kumpulkan biasanya informasi ip, port, protokol, dns, record.

Kali ini saya akan melakukan tahap awal yaitu Pentest (*Penetration Testing*) *data collection* dengan menggunakan alat bantu atau *tools* seperti *nmap, nikto, netcraf* dan *nessus.* Pada kesempatan ini saya menggunakan *tools nmap* dan *netcraf*, setelah dilakukannya *scaning* didapatlah data bahwa *website* gelorasriwijaya.co dengan IP address 203.114.74.102 memiliki port terbuka sebanyak 11 port.



Gambar 2.1 Detail Scaning



a. **Gambar** Topologi IP ke Localhost

Background

Site title	LPMGS UNSRI (PERS MAHASISWA UNIVERSITAS SRIWIJAYA)	**Date first seen**	May 2017
Site rank		**Primary language**	Indonesian
Description	LPMGS UNSRI (Lembaga Pers Mahasiswa Gelora Sriwijaya) adalah Unit Kegiatan Mahasiswa tingkat Universitas yang bergerak dalam bidang jurnalistik.		
Keywords	*Not Present*		
Netcraft Risk Rating [FAQ]	1/10		

Network

Site	http://gelorasriwijaya.co	**Netblock Owner**	CLDR DS ID Cloud
Domain	gelorasriwijaya.co	**Nameserver**	ns1.domainesia.net
IP address	203.114.74.102	**DNS admin**	admin@domainesia.com
IPv6 address	*Not Present*	**Reverse DNS**	majora.rapidplex.com
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	Dediserve
Top Level Domain	Colombia (.co)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
CLDR DS ID Cloud	203.114.74.102	Linux	nginx	6-Mar-2018

b. **Gambar** Detail dengan *Netcraf*

3) *Vulnerability Assesment* (VA)

Vulnerability Assesment (VA) merupakan adalah pengukuran kelemahan atas serangan dari luar. Semakin kuat serangan yang datang dari luar, maka akan semakin banyak celah yang ditemukan. Jika serangan yang dilancarkan lemah, maka pentest tidak akan berjalan maksimal. Port-port yang terbuka bisa kita cari tingkat kelemahannya dengan menggunakan CVE.

Berikut Hasil *Vulnerability Assesment* dengan CVE (*Common Vurnerabilities and Exposures*)

1. Port 21

Name	Description
CVE-2017-6872	A vulnerability was discovered in Siemens OZW672 (all versions) and OZW772 (all versions) that could allow an attacker with access to port 21/tcp to access or alter historical measurement data stored on the device.
CVE-2015-7261	The FTP service in QNAP iArtist Lite before 1.4.54, as distributed with QNAP Signage Station before 2.0.1, has hardcoded credentials, which makes it easier for remote attackers to obtain access via a session on TCP port 21.
CVE-2015-3968	The FTP service on Janitza UMG 508, 509, 511, 604, and 605 devices has a default password, which makes it easier for remote attackers to read or write to files via a session on TCP port 21.
CVE-2013-6920	Siemens SINAMICS S/G controllers with firmware before 4.6.11 do not require authentication for FTP and TELNET sessions, which allows remote attackers to bypass intended access restrictions via TCP traffic to port (1) 21 or (2) 23.

– CVSS Scores & Vulnerability Types

CVSS Score	6.4
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	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	264

2. Port 25

CVE-2010-1103	Integer overflow in Stainless allows remote attackers to bypass intended port restrictions on outbound TCP connections via a port number outside the range of the unsigned short data type, as demonstrated by a value of 65561 for TCP port 25.
CVE-2010-1102	Integer overflow in OmniWeb allows remote attackers to bypass intended port restrictions on outbound TCP connections via a port number outside the range of the unsigned short data type, as demonstrated by a value of 65561 for TCP port 25.
CVE-2010-1101	Integer overflow in Alexander Clauss iCab allows remote attackers to bypass intended port restrictions on outbound TCP connections via a port number outside the range of the unsigned short data type, as demonstrated by a value of 65561 for TCP port 25.
CVE-2010-1100	Integer overflow in Arora allows remote attackers to bypass intended port restrictions on outbound TCP connections via a port number outside the range of the unsigned short data type, as demonstrated by a value of 65561 for TCP port 25.
CVE-2010-1099	Integer overflow in Apple Safari allows remote attackers to bypass intended port restrictions on outbound TCP connections via a port number outside the range of the unsigned short data type, as demonstrated by a value of 65561 for TCP port 25.

– CVSS Scores & Vulnerability Types

CVSS Score	5.0
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
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	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)	Overflow Bypass a restriction or similar
CWE ID	189

3. Port 80

CVE-2017-9944	A vulnerability has been identified in Siemens 7KT PAC1200 data manager (7KT1260) in all versions < V2.03. The integrated web server (port 80/tcp) of the affected devices could allow an unauthenticated remote attacker to perform administrative operations over the network.
CVE-2017-6869	A vulnerability was discovered in Siemens ViewPort for Web Office Portal before revision number 1453 that could allow an unauthenticated remote user to upload arbitrary code and execute it with the permissions of the operating-system user running the web server by sending specially crafted network packets to port 443/TCP or port 80/TCP.

– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
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
CWE ID	264

4. Port 110

CVE-2004-2168	BaSoMail 1.24 allows remote attackers to cause a denial of service (CPU consumption) via multiple connections to TCP port (1) 25 (SMTP) or (2) 110 (POP3).
CVE-2002-2404	Buffer overflow in IISPop email server 1.161 and 1.181 allows remote attackers to cause a denial of service (crash) via a long request to the POP3 port (TCP port 110).
CVE-2002-1945	Buffer overflow in SmartMail Server 1.0 Beta 10 allows remote attackers to cause a denial of service (crash) via a long request to (1) TCP port 25 (SMTP) or (2) TCP port 110 (POP3).
CVE-2002-1349	Buffer overflow in pop3trap.exe for PC-cillin 2000, 2002, and 2003 allows local users to execute arbitrary code via a long input string to TCP port 110 (POP3).

– CVSS Scores & Vulnerability Types

CVSS Score	5.0
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	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)	Denial Of Service Overflow
CWE ID	CWE id is not defined for this vulnerability

5. Port 143

CVE-2008-1713	MailServer.exe in NoticeWare Email Server 4.6.1.0 allows remote attackers to cause a denial of service (application crash) via a long string to IMAP port (143/tcp).
CVE-2007-5466	Multiple buffer overflows in eXtremail 2.1.1 and earlier allow remote attackers to (1) have an unknown impact by sending multiple long strings to the IMAP port (143/tcp); (2) execute arbitrary code via a long string in an IMAP AUTHENTICATE PLAIN action, involving the ifParseAuthPlain function; (3) execute arbitrary code via a long LOGIN command to the admin interface port (4501/tcp); or (4) execute arbitrary code via a long string in an IMAP AUTHENTICATE LOGIN (aka CRAM-MD5 authentication) action, involving the ifProcImapAuth1 function.

– CVSS Scores & Vulnerability Types

CVSS Score	5.0
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	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)	Denial Of Service
CWE ID	CWE id is not defined for this vulnerability

6. Port 443

Name	Description
CVE-2018-4837	A vulnerability has been identified in TeleControl Server Basic < V3.1. An attacker with access to the TeleControl Server Basic's webserver (port 80/tcp or 443/tcp) could cause a Denial-of-Service condition on the web server. The remaining functionality of the TeleControl Server Basic is not affected by the Denial-of-Service condition.

– CVSS Scores & Vulnerability Types

CVSS Score	5.0
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	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

7. Port 465

CVE-2011-4015	Cisco IOS 15.2S allows remote attackers to cause a denial of service (interface queue wedge) via malformed UDP traffic on port 465, aka Bug ID CSCts48300.

– CVSS Scores & Vulnerability Types

CVSS Score	5.0
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	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)	Denial Of Service
CWE ID	20

8. Port 587

CVE-2010-0471	SQL injection vulnerability in the comment submission interface (includes/comment.php) in Enano CMS before 1.0.6pl1 allows remote attackers to execute arbitrary SQL commands via unspecified parameters.

– 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

9. Port 993

CVE-2014-0138	The default configuration in cURL and libcurl 7.10.6 before 7.36.0 re-uses (1) SCP, (2) SFTP, (3) POP3, (4) POP3S, (5) IMAP, (6) IMAPS, (7) SMTP, (8) SMTPS, (9) LDAP, and (10) LDAPS connections, which might allow context-dependent attackers to connect as other users via a request, a similar issue to CVE-2014-0015.

– CVSS Scores & Vulnerability Types

CVSS Score	6.4
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	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	287

10. Port 995

Name	Description
CVE-2006-0995	EMC Dantz Retrospect 7 backup client 7.0.107, and other versions before 7.0.109, and 6.5 before 6.5.138 allows remote attackers to cause a denial of service (client termination and loss of backup service) via a malformed packet to TCP port 497, which triggers an assert error.

– CVSS Scores & Vulnerability Types

CVSS Score	5.0
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	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)	Denial Of Service
CWE ID	CWE id is not defined for this vulnerability

11. Port 8081

CVE-2017-16606	This vulnerability allows remote attackers to execute code by creating arbitrary files on vulnerable installations of NetGain Systems Enterprise Manager 7.2.730 build 1034. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the org.apache.jsp.u.jsp._3d.add_005f3d_005fview_005fdo_jsp servlet, which listens on TCP port 8081 by default. When parsing the filename parameter, the process does not properly validate a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code under the context of Administrator. Was ZDI-CAN-5197.
CVE-2017-16605	This vulnerability allows remote attackers to overwrite arbitrary files on vulnerable installations of NetGain Systems Enterprise Manager 7.2.730 build 1034. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the org.apache.jsp.u.jsp.db.save_005fattrs_jsp servlet, which listens on TCP port 8081 by default. When parsing the id parameter, the process does not properly validate a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to overwrite any files accessible to the Administrator. Was ZDI-CAN-5196.

– CVSS Scores & Vulnerability Types

CVSS Score	6.5
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	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)	Execute Code Bypass a restriction or similar
CWE ID	417

No	Port	CVSS Score	Colour	Access Complexity
	21	6.4		Low
	25	5.0		Low
	80	10.0		Low
	110	5.0		Low
	143	5.0		Low
	443	5.0		Low
	465	5.0		Low
	587	7.5		Low
	993	6.4		Low
	995	5.0		Low
	8081	6.5		Low

Tabel 3.1 Ringkasan *Vulnerability* dengan CVE

4) Kesimpulan

Sebenarnya ada 4 langkah melakukan *Penetration Testing* namun pada tugas kali ini hanya pada tahap *Data Collection* dan *Vulnerability Assesment*, pada *website* banyuasinkab.go.id terdapat 1000 port yang terbuka sedangkan pada *website* gelorasriwijaya.co terdapat 11 port yang terbuka.

Setelah dicari skor CVSS (*Common Vurnerability Scoring System)* yang digunakan untuk menetapkan skor kelemahan terhadap kerentanan. Skor dihitung berdasarkan formula yang bergantung pada beberapa matrik yang mendekati kemudahan mengeksploitasi dan dampak eksploitasi. Skor berkisar antara 0 sampai 10, dengan 10 adalah yang paling parah dan sangat rentan.

Pada *website* banyuasinkab.go.id dengan IP 118.97.168.204 terdapat 10 port hasil analisa bahwa ada 8 port memiliki skor 4.3 sampai 7.5 yang mana memiliki tingkat kerentanan medium dan 2 port dengan skor 9.0 sampai 10.0 yang memiliki kerentanan terhadap serangan yang sangat tinggi dan rentan.

Sedangkan pada *website* gelorasriwijaya.co dengan IP address 203.114.74.102 terdapat 10 port memiliki skor 5.0 sampai 7.5 yang mana memiliki tingkat kerentanan medium dan 1 port dengan skor 10.0 yang memiliki kerentanan terhadap serangan yang sangat tinggi dan rentan

DAFTAR PUSTAKA

http://cve.mitre.org/ diakses pada 7 maret 2018 pukul 17.00 WIB

https://www.cvedetails.com/ diakses pada 7 maret 2018 pukul 17.00 WIB

http://netcraft.com/ diakses pada 7 maret 2018 pukul 17.00 WIB

http://nmap.org/ diakses pada 7 maret 2018 pukul 17.00 WIB