UTS
keamanan Jaringan Komputer

D
I
S
U
S
U
N

OLEH

NAMA : FAJRI AULIA RACHMAT

NIM : 09121001032

SISTEM KOMPUTER

FAKULTAS KOMPUTER

UNIVERSITAS SRIWIJAYA

INDRALAYA

TAHUN AJARAN

2015/2016

1. Scanning
   * NMAP
   -Open PORT & Service

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
49157	tcp	open	tcpwrapped	
49160	tcp	open	tcpwrapped	
49161	tcp	open	tcpwrapped	
49163	tcp	open	tcpwrapped	
49175	tcp	open	tcpwrapped	
50001	tcp	open	tcpwrapped	
50002	tcp	open	tcpwrapped	
50006	tcp	open	tcpwrapped	
50500	tcp	open	tcpwrapped	
52869	tcp	open	tcpwrapped	
54328	tcp	open	tcpwrapped	
56737	tcp	open	tcpwrapped	
57797	tcp	open	tcpwrapped	
58080	tcp	open	tcpwrapped	
65389	tcp	open	tcpwrapped	
22	tcp	open	ssh	OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
111	tcp	open	rpcbind	2-4 (RPC #100000)
3306	tcp	open	mysql	MySQL 5.5.29-0ubuntu0.12.04.1-log
9100	tcp	open	jetdirect	
9101	tcp	open	jetdirect	
9102	tcp	open	jetdirect	
9103	tcp	open	jetdirect	
80	tcp	open	http	Apache httpd (PHP 5.3.10-1ubuntu3.19)
443	tcp	open	http	Apache httpd
10000	tcp	open	http	MiniServ 1.780 (Webmin httpd)
21	tcp	open	ftp	vsftpd 2.0.8 or later
53	tcp	open	domain	

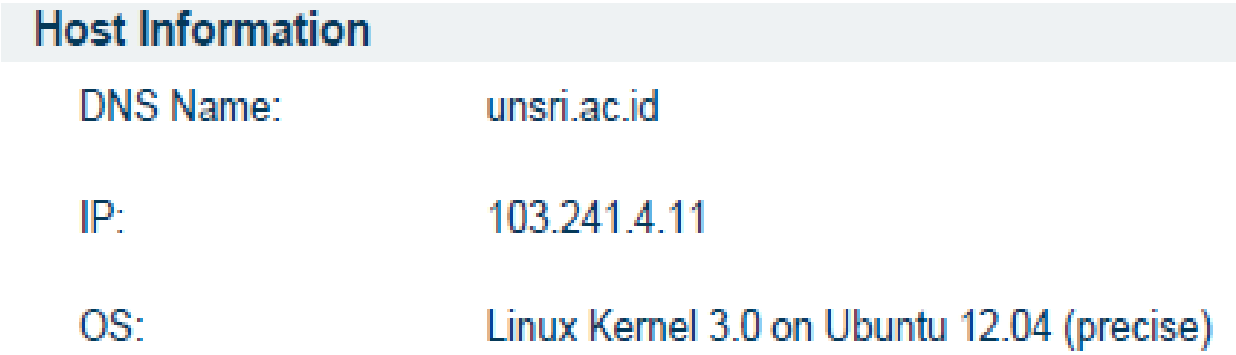
-Sistem Operasi

```
Device type: firewall
Running (JUST GUESSING): Netasq embedded (85%)
OS CPE: cpe:/h:netasq:u70
Aggressive OS guesses: Netasq U70 firewall (85%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 5.948 days (since Mon Mar 21 18:47:43 2016)
Network Distance: 11 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3389/tcp)
HOP RTT        ADDRESS
1   1.00 ms    172.20.10.1
2   ... 10
11  4209.00 ms 103.241.4.11

NSE: Script Post-scanning.
Initiating NSE at 17:32
Completed NSE at 17:32, 0.01s elapsed
Initiating NSE at 17:32
Completed NSE at 17:32, 0.00s elapsed
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 348.06 seconds
           Raw packets sent: 1221 (56.232KB) | Rcvd: 1047 (46.012KB)
```

- Nessus
- Host



- Tingkat Vulnerability

Results Summary

Critical	High	Medium	Low	Info	Total
0	2	9	2	354	367

- Service dengan vulnerability

HIGH	OpenSSL 'ChangeCipherSpec' MiTM Vulnerability	Misc.	1
HIGH	OpenSSL Heartbeat Information Disclosure (Heartbleed)	Misc.	1
MEDIUM	Apache mod_status /server-status Information Disclosure	Web Servers	2
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
MEDIUM	SSL Certificate Signed Using Weak Hashing Algorithm	General	1
MEDIUM	SSL Medium Strength Cipher Suites Supported	General	1
MEDIUM	SSL RC4 Cipher Suites Supported (Bar Mitzva... Plugin ID: 57582	General	1
MEDIUM	SSL Self-Signed Certificate	General	1
MEDIUM	SSL Version 2 and 3 Protocol Detection	Service detection	1
MEDIUM	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (PO...	General	1
LOW	SSH Server CBC Mode Ciphers Enabled	Misc.	1
LOW	SSH Weak MAC Algorithms Enabled	Misc.	1

2. Analisa

2.1 Open Port dan Service

-Port 21

Port 21 pada server unsri.ac.id terbuka, ini membuktikan bahwa server UNSRI memiliki layanan ftp (file transfer protokol), yang dapat digunakan untuk berbagi file. Pada dasarnya port 21 adalah port yang sering digunakan untuk layanan ftp , namun layanan ini bisa digunakan ke port yang lain dalam konteks tidak menggunakan port yang telah digunakan oleh software lainnya. Layanan ftp ini merupakan layanan yang memberikan directory listing pada tampilannya yang digunakan oleh user untuk mencari file yang dibutuhkannya, walaupun mengijinkan directory listing, sistem ini hanya akan menampilkan file yang memang dibagikan dan dimiliki oleh user, sedangkan file sistem jauh dari jangkauan directory listing. Sistem berbeda dari sistem remot SSH, mungkin mirip namun ftp ini lebih ke layanan download, upload file dan drectory listing.

-Port 22

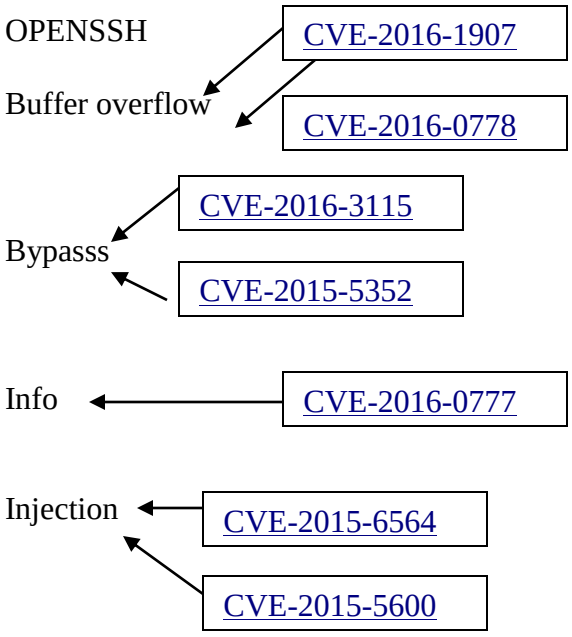
Port 22 pada unsri.ac.id terbuka, port ini dugunkan untuk remote service melalui protokol SSH (Secure Shell) yang merupakan protokol yang harus dimiliki oleh server. Maintanance jarak jauh (remote) biasanya dilakukan pada port ini (port 22) tanpa harus bersentuhan dengan fisik server . Untuk mengupload file secara aman dengan port 22 ini dapat menggunakan protokol SFTP yang merupakan versi aman dari protokol FTP. Dengan protokol SSH admin suatu server dapat login ke dalam sever dengan jaringan yang terenkripsi dan dapat melakaukan konfigurasi yang dibutuhkan seperti berhadapan langsung dengan komputer server tersebut.

-Port 3306

Port 80 pada unsri.ac.id juga terbuka yang membuktikan bahwa server ini memiliki layanan web server, yang menyediakan info seputar kampus universitas sriwisaja . Port ini mengguanakan protokol http sebagai media komunikasinya dengan user. Protokol ini tidak aman, karena protokol ini akan mengirimkan file plaintext melalui jaringan internet. Web server ini merupakan sistem yang bertanggung jawab untuk menjalankan script language yang mana diantaranya php, html, java script, dll.
Web server juga dapat menjalankan web CGI yaitu web yang menggunakan bahasa pemrograman C,C++,dll untuk menjalankan layanan (penganti PHP) server side. Biasanya layanan http ini dikombinasikan dengan port 443 yang meruapakn port SSL (Secure Socket Layer) yang berfungsi untuk melakukan enkripsi traffic protokol http yang digunakan oleh layanan web menajdi https.

3. CVE

- Port 22


OPENSSH
Buffer overflow
CVE-2016-1907
CVE-2016-0778
Bypasss
CVE-2016-3115
CVE-2015-5352
Info
CVE-2016-0777
Injection
CVE-2015-6564
CVE-2015-5600

- Port 80

Buffer overflow ← CVE-2014-0001

CVE-2014-0384

CVE-2014-4274
CVE-2014-0437

CVE-2014-6463

CVE-2014-6469

CVE-2014-6484

CVE-2014-6494

CVE-2014-6496

CVE-2014-6505

CVE-2014-6520

CVE-2014-6551

CVE-2014-6559

CVE-2015-0374

CVE-2015-0382

CVE-2015-0411

CVE-2015-0433

CVE-2015-0499

CVE-2015-0505

CVE-2014-1466
CVE-2014-0386

CVE-2014-0401

Injection

CVE-2014-4258
CVE-2014-4260
CVE-2014-2419

CVE-2014-4287

CVE-2014-6464

CVE-2014-6478

CVE-2014-6491

CVE-2014-6495

CVE-2014-6500

CVE-2014-6507

CVE-2014-6530

CVE-2014-6555

CVE-2014-6568

CVE-2015-0381

CVE-2015-0391

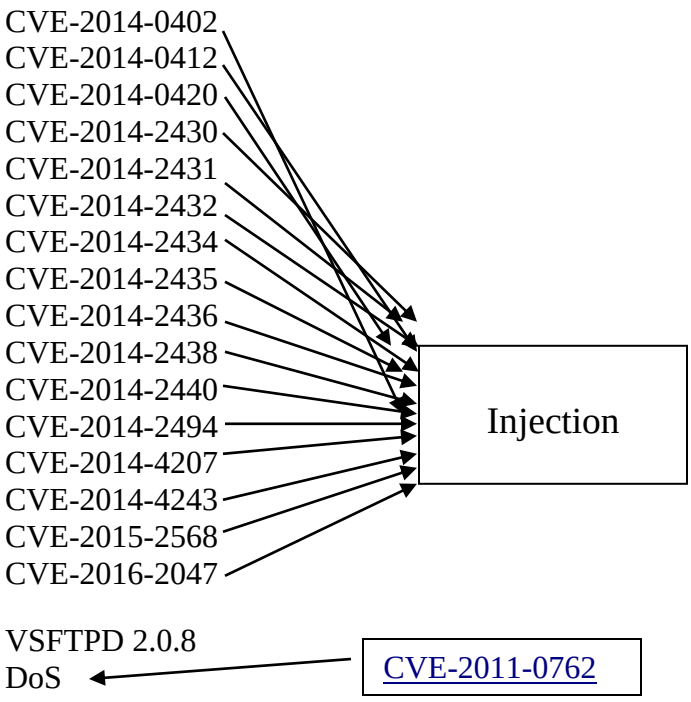
CVE-2015-0432

CVE-2015-0441

CVE-2015-0501

CVE-2014-2351

CVE-2014-0393


CVE-2014-0402
CVE-2014-0412
CVE-2014-0420
CVE-2014-2430
CVE-2014-2431
CVE-2014-2432
CVE-2014-2434
CVE-2014-2435
CVE-2014-2436
CVE-2014-2438
CVE-2014-2440
CVE-2014-2494
CVE-2014-4207
CVE-2014-4243
CVE-2015-2568
CVE-2016-2047
Injection

VSFTPD 2.0.8
DoS
CVE-2011-0762

DAFTAR PUSTAKA

- http://cve.mitre.org
- https://www.exploit-db.com/
- http://cvedetails.com