Ujian Tengah Semester
Kemanan Jaringan Komputer

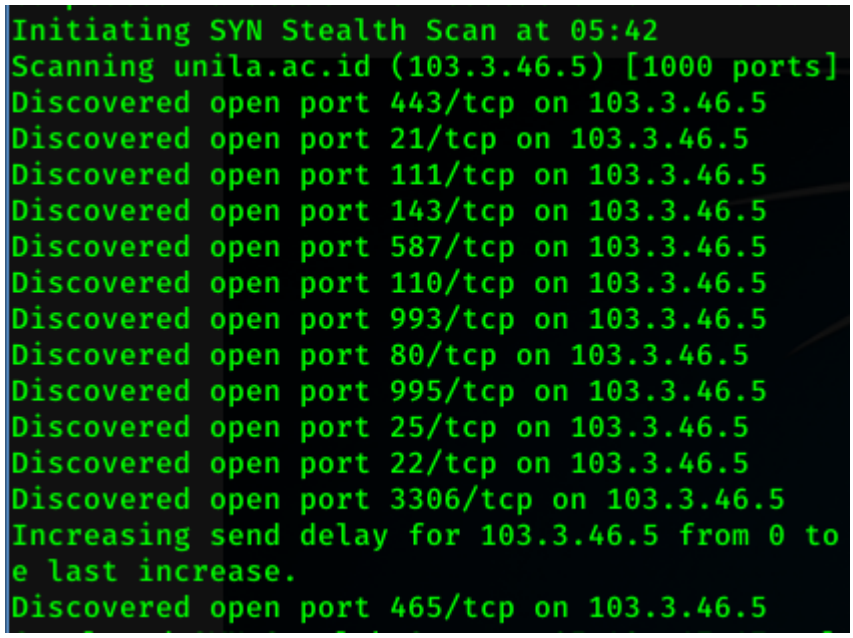
D
I
S
U
S
U
N

OLEH :
Nama : Candra Adi Winanto
Nim : 09121001042

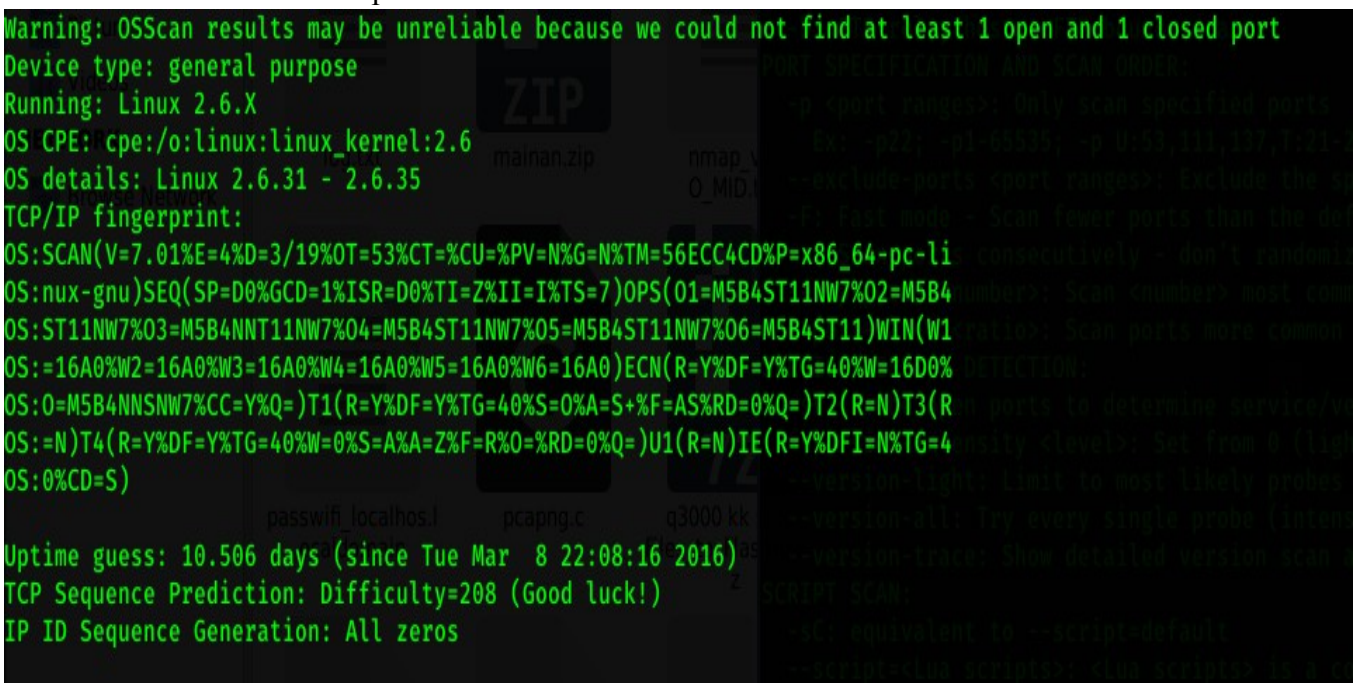
SISTEM KOMPUTER
FAKULTAS KOMPUTER
UNIVERSITAS SRIWIJAYA
INDRALAYA
TAHUN AJARAN 2016

1. Scaning
   - NMAP

     -Open Port



     -Sistem Operasi



-Service

```
PORT     STATE    SERVICE  REASON         VERSION
21/tcp   open     ftp      syn-ack ttl 55 Pure-FTPd
22/tcp   open     ssh      syn-ack ttl 55 OpenSSH 5.3 (protocol 2.0)
25/tcp   open     smtp?    syn-ack ttl 55
53/tcp   filtered domain   no-response
80/tcp   open     http     syn-ack ttl 55 Apache httpd 2.2.26 ((Unix) mod_ssl/2.2.26 OpenSSL/1.0.1e-fips mod_bwlimited/1.4)
110/tcp  open     pop3     syn-ack ttl 55 Dovecot pop3d
111/tcp  open     rpcbind  syn-ack ttl 55 2-4 (RPC #100000)
143/tcp  open     imap     syn-ack ttl 55 Dovecot imapd
443/tcp  open     ssl/http syn-ack ttl 55 Apache httpd 2.2.26 (mod_ssl/2.2.26 OpenSSL/1.0.1e-fips mod_bwlimited/1.4)
465/tcp  open     ssl/smtp syn-ack ttl 55 Exim smtpd 4.86_1
587/tcp  open     smtp     syn-ack ttl 55 Exim smtpd 4.86_1
993/tcp  open     ssl/imap syn-ack ttl 55 Dovecot imapd
995/tcp  open     ssl/pop3 syn-ack ttl 55 Dovecot pop3d
3306/tcp open     mysql    syn-ack ttl 55 MySQL (unauthorized)
Service Info: Host: unila.ac.id
```

- Nessus

  -Host

Host Information

DNS Name:	unila.ac.id
IP:	103.3.46.5
OS:	Linux Kernel 2.6

-Tingkat Vulnerability

Summary

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	4	38	45

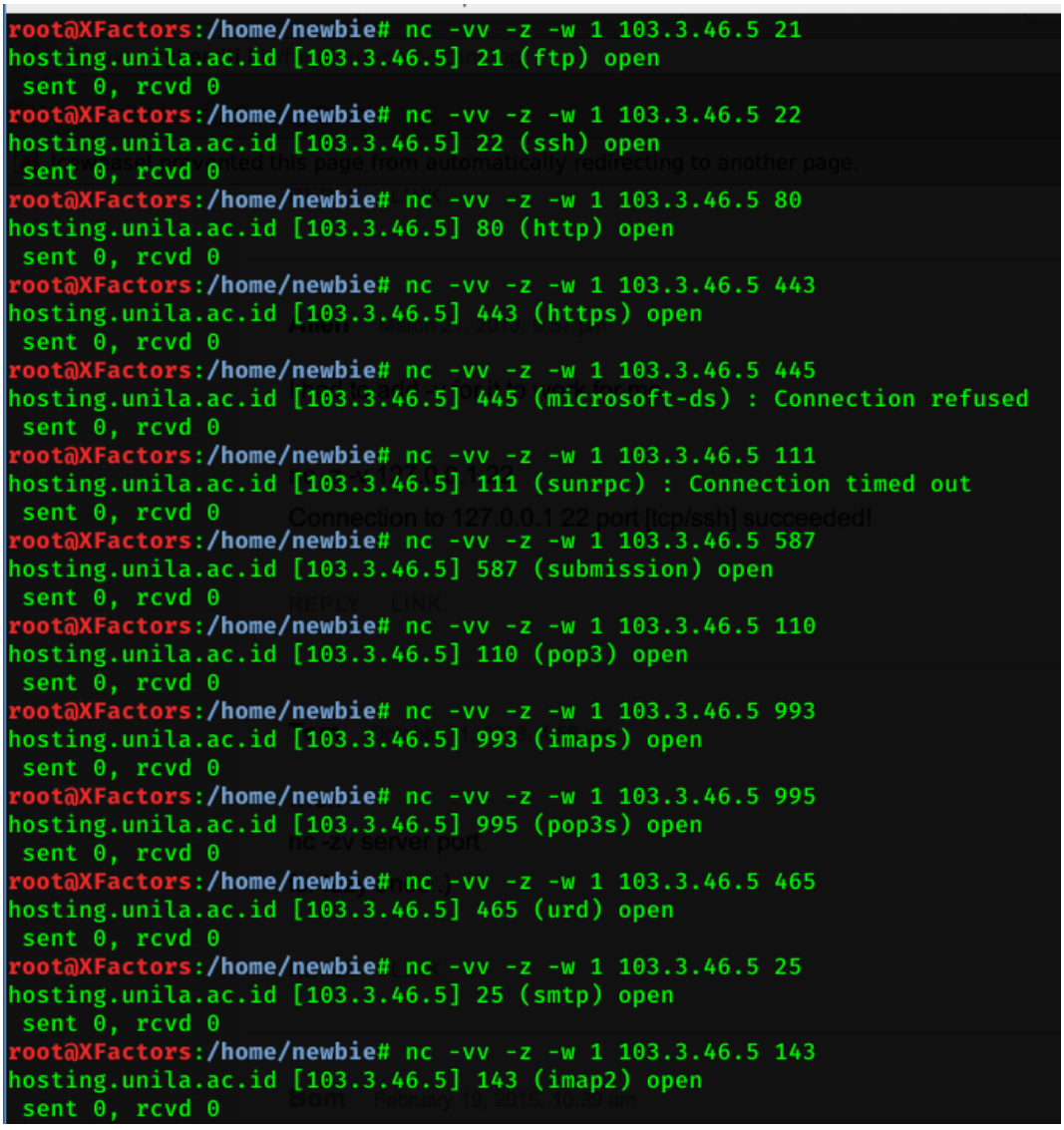
-Service dengan Vulnerability

Details

Severity	Plugin Id	Name
Medium (5.0)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low (2.6)	15855	POP3 Cleartext Logins Permitted
Low (2.6)	54582	SMTP Service Cleartext Login Permitted
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled

- Netcut

  -Open Port dan Service



2. Analisa

2.1 Open Port

-Port 21

Port 21 pada server unila.ac.id terbuka, ini mengindikasikan bahwa server unila memiliki layanan ftp (file transfer protokol), yang dapat digunakan untuk berbagi file. Port ini merupakan port standar ftp, port ini dapat diganti dengan port lain asalkan tidak menggangu layanan dari port lain tersebut.

-Port 22

Port 22 pada server unila.ac.id terbuka, ini mengindikasikan bahwa server ini memiliki layanan remote server melalui protokol SSH (Secure Shell) yan merupakan protokol wajib yang harus dimiliki oleh suatu server, protokol ini digunakan untuk mantainance dari jarak jauh (remote) server tanpa harus berhubungan langsung dengan mesin server. Port 22 merupakan alamat port standar yang digunakan, port ini dapat diganti dengan port lain selama tidak menggangu layanan lain yang ada di dalam server.

-Port 80

Port 80 pada server ini juga terbuka yang mengindikasikan bahwa server ini memiliki layanan web server, yang menyediakan informasi seputar kampus universitas lampung. Port ini mengguanakan protokol http sebagai media komunikasinya dengan user. Protokol ini tidak aman, karena protokol ini akan mengirimkan file plaintext melalui jaringan internet. Port 80 ini merupakan port standar yang menajalankan web server, port ini dapt diganti dengan port lain, selama tidak menggangu layanan lain dari server itu sendiri.

2.2 Daemon (Service)

-Port 21 → Pure-FTPd

Port 21 meurpakan port standar dari layanan FTP yang mana dalam hal ini menggunakan software / daemon Pure-FTPd yang merupakan aplikasi ftp yang mengijinkan use ryang mempunyai akses untuk mengupload file, mendownload file. 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 → OpenSSH 5.3 (Protocol 2.0)

Port 22 ini merupakan port standar yang digunakan untuk layanan transfer file dan sistem remot secar aman. OpenSSH merupakan software / daemon yang memberikan layanan ini, dengan protokol SSH dimungkinkan user mengirimkan file dan melakukan kendali server jarak jauh dangan traffic yang terenkripsi, sehingga orang lain tidak mengetahui data apa yang dikirm oleh user yang menggunakan SSH. 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 80 → Apche httpd 2.2.26 ((unix) mod_ssl/2.2.26 OpenSSL/1.0.1e-fips mod_bwlimited/1.4)

Port 80 ini merupakan port standar yang digunakan untuk menjalankan web server, yang memberikana layanan pada user yang terkoneksi dengan port ini. Protokol ayng digunakan pada layanan ini adalah protokol http. Apache merupakan salah satu software yang memungkinkan layanan http ini dapat dijalankan. 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.

2.3 Vulnerability

-Port 21 → Directory Traversal

Pada port 21 ini nmap tidak dapat mendapatkan versi dari software yang digunakan pada server sehingga diperkirakan server ini menggunakan versi dari pure-FTPd 1.0.22, dari informasi CVE terdapat kelemahan pada sistem versi ini yang rentan terhadap serangan directory traversal yang mengakibatkan user lokal dapat mengubah hak akses dari file yang ada dalam server ftp ini dari vecktor yang tidak diketahui, serangan ini dimungkinkan ketika Netware OES remote server di aktifkan. Directory traversal merupakan bug yang mana user dapat mengakses directory lain yang bukan merupakan directory yang menjadi layanan dari sistem, sehingga user dapat mencuri hash password dari server.

-Port 22 → DoS Overflow

Pada port 22 ini nmap dapat mengenali versi dari software yang digunakan pada server, server ini menggunakan versi SSH dari software OpenSH 5.3, dari informasi ayng didapat dari CVE terdapat kelemahan dari versi ini hingga versi 7.x sebelum 7.1p2 yang dapat mengakibatkan software mengalami hang / crash yang mengakibatkan layanan remote tidak berjalan, kelamahan ini diakibatkan oleh bug heap-based buffer overflow yang dapat di ekspliotasi dengan mengirimkan paket yang besar terhadap layanan yang dikenal sebagi DoS, kelamahan ini akan terbuka jika proxy atau opsi forward di aktifkan. Buffer overflow merupakan bug yang terjadi di karenakan jumlah memori yang

dialokasikan untuk menampung sebuah data khususnya string tidak mampu menampung data tersebut dan berakibat melubernya data pada alamat memori lain yang mengakibatkan fungsi return pada program menjadi tidak berfungsi. Bug ini banyak terjadi pada program yang menggunakan bahasa pemrograman keluarga C/C++ untuk pengembangannya, dikarenakan kurang baerhati-hatinya dalam penanganan data yang string.

-Port 80 → DoS

Pada port 80 ini nmap dapat mengenali versi dari software yang digunakan pada server, server ini menggunakan versi webserver dari software Apche httpd 2.2.26 , dari informasi yang didapat dari CVE terdapat kelemahan dari versi ini sebelum versi 2.4.10, yaitu rentan terhadap serangan DoS yang dapat membuat sistem hang / crash sehingga layanan web terganggu yang dikarenakan versi ini tidak memiliki mekanisme timeout pada mod_cgid, serangan ini dapat dilakukan melalui permintaan script CGI yang mana tidak dibaca melalui stdin(standar input).

3. CVE

3.1 Risk Rating

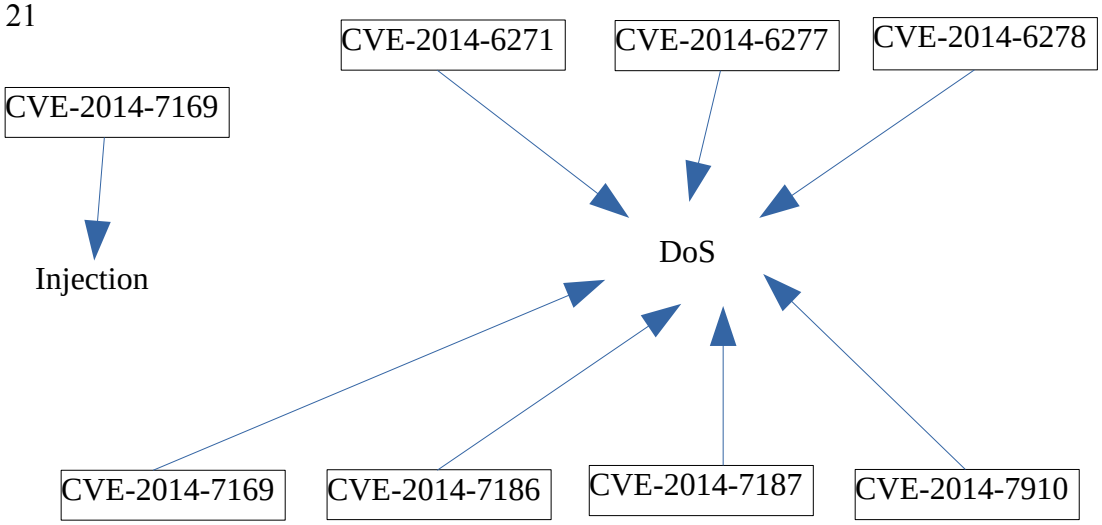
-Port 21 → 3.6

-Port 22 → 6.5

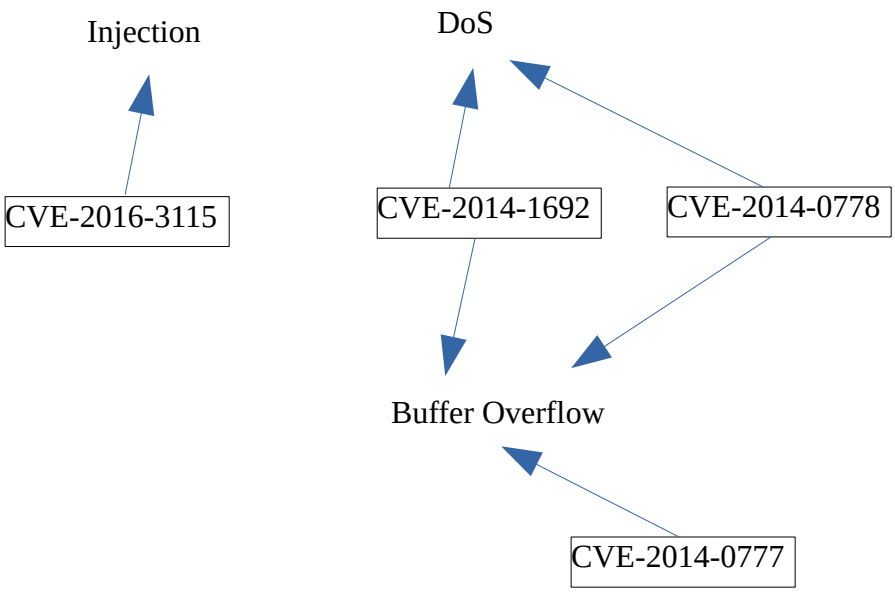
-Port 80 → 5.0

3.2 Map CVE

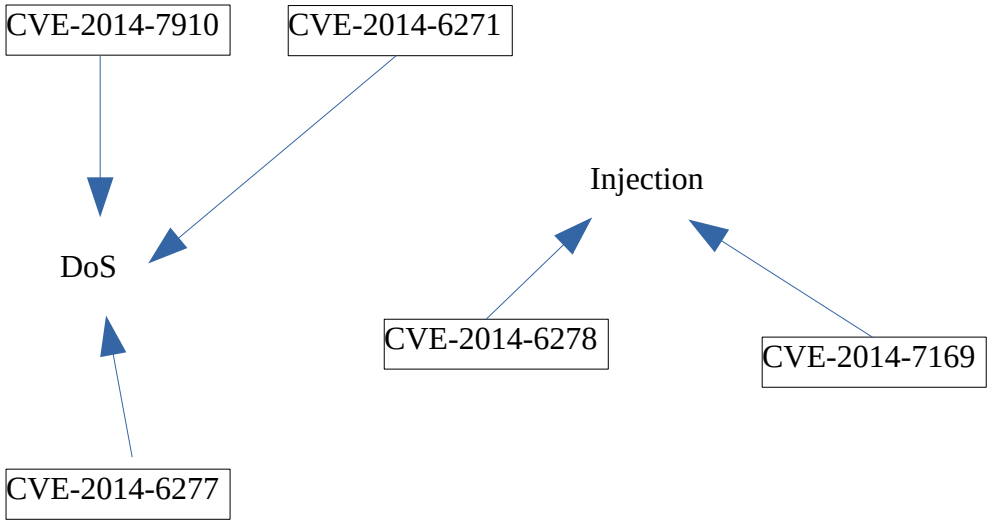
-Port 21



-Port 22



-Port 80



DAFTAR PUSTAKA

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