Pertemuan Ke-14	TTD Dosen ACC:	Nilai dari Dosen:

LAPORAN AKHIR
MATA KULIAH
DESAIN DAN MANAJEMEN JARINGAN KOMPUTER

Muhammad Izzul Haq -
3130023044
Dosen Pengampu :
Rizqi Putri Nourma Budiarti, S.T., M.T

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS EKONOMI BISNIS DAN TEKNOLOGI DIGITAL
UNIVERSITAS NAHDLATUL ULAMA SURABAYA

A. TUJUAN PRAKTIKUM

1. Mahasiswa dapat memahami apa itu keamanan jaringan
2. Mahasiswa dapat mengetahui beberapa penggunaan dalam aplikasi keamanan jaringan.

B. ALAT DAN BAHAN

1. Seperangkat komputer / laptop (monitor, mouse, keyboard, dll)
2. Internet
3. Aplikasi Nmap / Zenmap
4. Aplikasi – aplikasi lainnya yang berpengaruh terhadap keamanan jaringan

C. LANDASAN TEORI

Dalam keamanan jaringan, Hacking adalah kegiatan memasuki system melalui system operasional lain yang dijalankan oleh Hacker. Tujuanya untuk mencari hole/bugs pada system yang akan dimasuki. Dalam arti lain mencari titik keamanan system tersebut. Hacker adalah sebutan untuk mereka yang memberikan sumbangan yang bermanfaat kepada jaringan komputer, membuat program kecil dan membagikannya dengan orang-orang di Internet. Para hacker biasanya melakukan penyusupan-penyusupan dengan maksud memuaskan pengetahuan dan teknik. Bila hacker berhasil masuk pada system itu, hacker dapat mengakses hal apapun sesuai keinginan hacker itu. Dari kegiatan yang mengacak system maupun kejahatan.

Ada dua jenis kegiatan hacking yaitu :

1. Social Hacking, yang perlu diketahui :

Informasi tentang system apa yang dipergunakan oleh server, siapa pemilik server, siapa Admin yang mengelola server, koneksi yang dipergunakan jenis apa lalu bagaimana server itu tersambung internet, mempergunakan koneksi siapa lalu informasi apa saja yang disediakan oleh server tersebut, apakah server tersebut juga tersambung dengan LAN di sebuah organisasi dan informasi lainnya

2. Technical Hacking,

Merupakan tindakan teknis untuk melakukan penyusupan ke dalam system, baik dengan alat bantu (tool) atau dengan mempergunakan fasilitas system itu sendiri yang
dipergunakan untuk menyerang kelemahan (lubang keamanan) yang terdapat dalam system Analisaatau service. Inti dari kegiatan ini adalah mendapatkan akses penuh ke dalam system dengan cara apapun dan bagaimana pun.

Tipe Hacker dapat dikelompokkan menjadi 4 golangan yaitu;

1. black hat hacker(hacker yang jahat)
2. white hat hacker(hacker yang baik)
3. gray hat hacker(hacker yang berada antara yang baik dan jahat/abu-abu) 4. suicid hat hacker

Ada beberapa tahapan aktifitas yang dilakukan dalam hacking

1. Reconnaissance merupakan tahap dimana kita mencari target.reconnainssance dibagi menjadi 2,yaitu raconnainssace passave(yang mana mencari target pada google atau jejaring sosial) dan reconnainssance aktif(mencari target html.
2. Pencarian exploit berdasarkan scamming google, archive milwarm , archive expoit DB, meta sploit framework, dark code.
3. Gaining acces exploitas remote execution disini terbagi manjadi 3 yaitu a)pada celah keamanan OS,b)pada celah keamanan aplikasi,c)pada celah web
4. Maintining acces,jika kita bisa masuk pada tahap ini kta bisa melakukan apaun pada sistem yang kita hack tadi,salah satunya kita bisa membangun backdoor,pada sistem teersebut,biasanya untuk model php itu lebih muda.backoor php antara lain: simple php shell, R57, C99/C100, ASP BACKDOOR, B 374 K
5. Covering track

Merupakan tahap akhir dalam proses ini,pada tahap ini hacker harus menghapus jajak yang di tinggalkan ketiaka ia menghack sisten tersebut,salah satunya pembersiahan berbagai explit.

INSTALASI DAN KONFIGURASI APLIKASI KEAMANAN JARINGAN

Petunjuk :

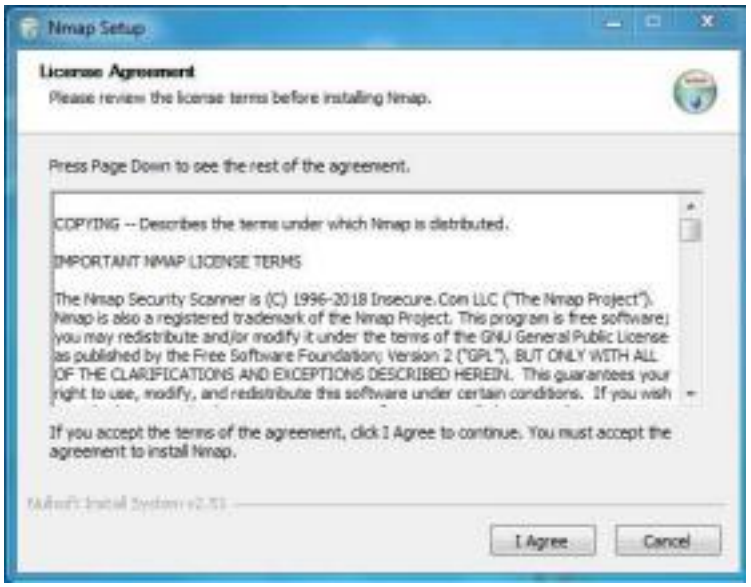
• Kerjakan dengan bantuan **internet**

• Aplikasi untuk keamanan jaringan yang harus dicari, diinstal dan dilakukan konfigurasi adalah: NMAP, Tracert atau Traceroute

3. Instalasi dan konfigurasi Aplikasi Nmap pada Laptop

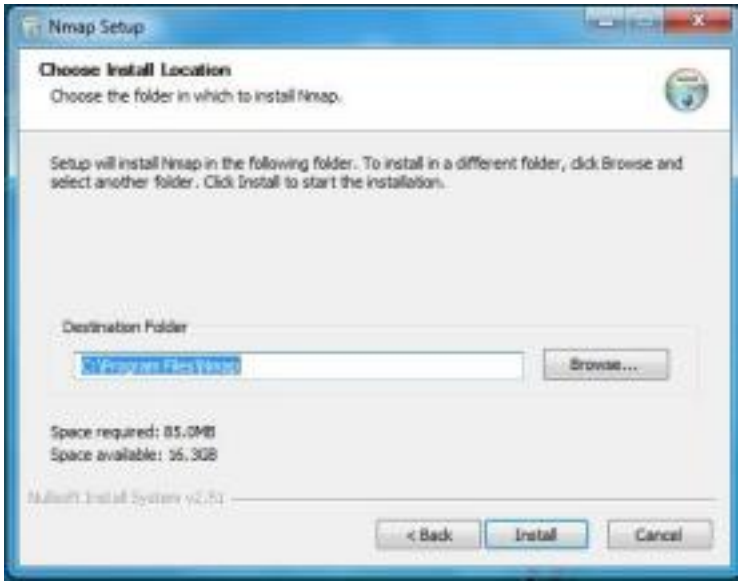
Instalasi

a. Klik “ I Agree”



b. Klik Next

c. Klik install



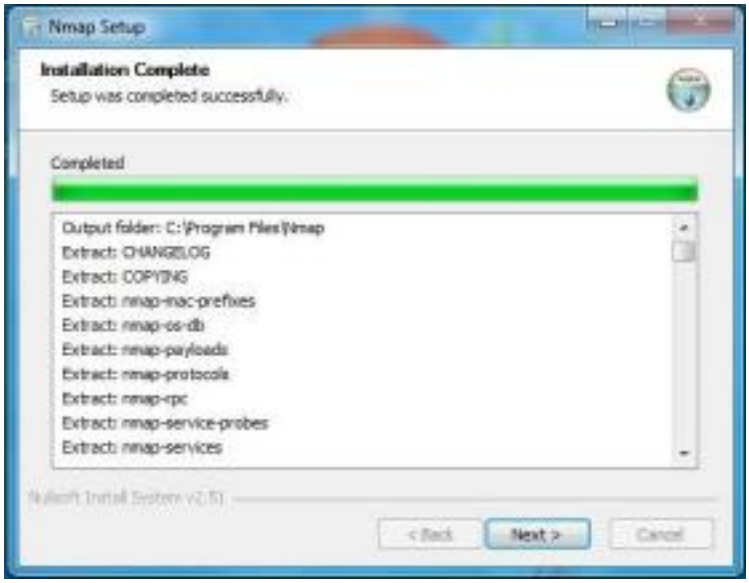
d. Tunggu proses intasalsi nmap

e. Pada Npcap OEM , klik " I Agree"

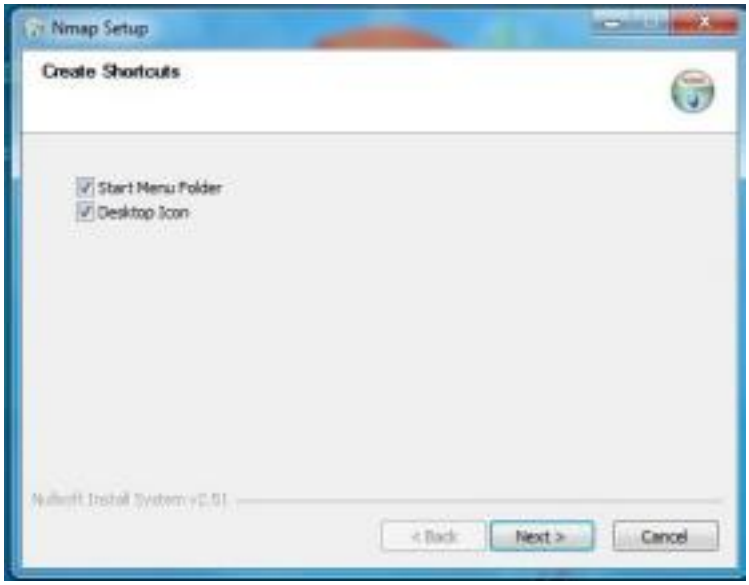
f. Klik install

g. Npcap selesai di install → klik next → lalu finish

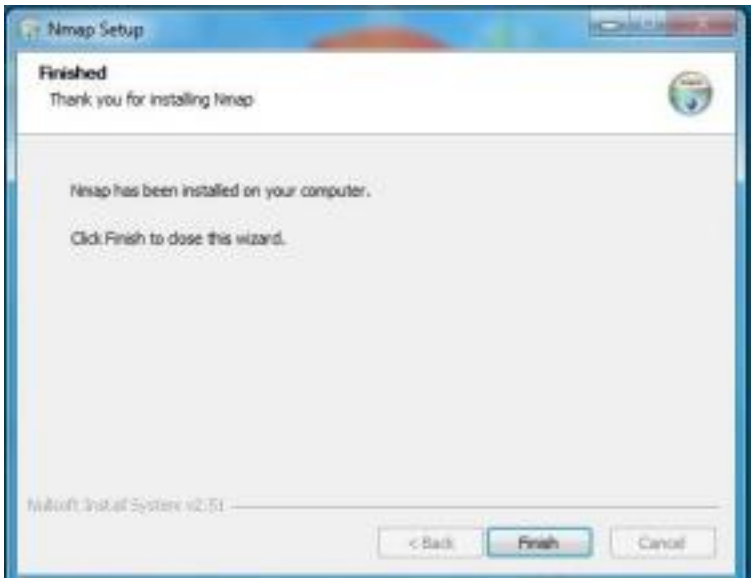
h. Klik next



i. Klik next



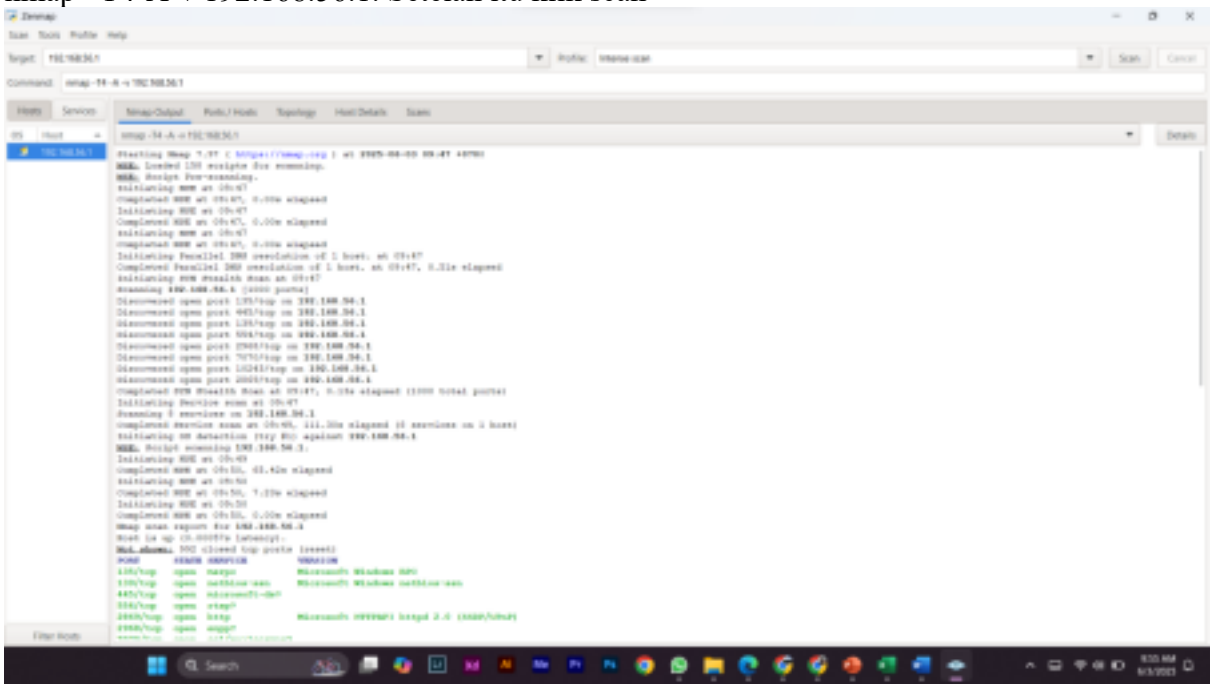
j. Nmap selesai di instal → Klik finish



Konfigurasi pada Zenmap

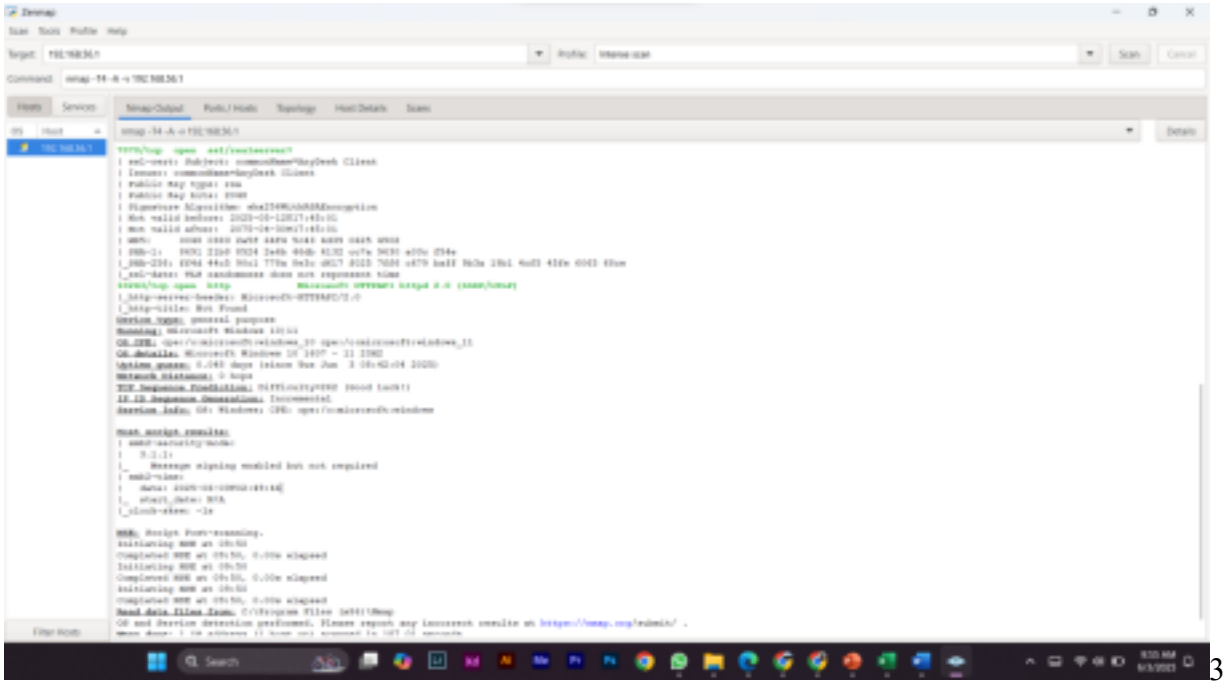
1. Konfigurasi pada Zenmap dengan IP laptop 192.168.56.1

Disini saya akan melakukan pendekteksian terhadap port target yang terbuka yaitu dengan melakukan perintah : nmap –T4-A-v 192.168.56.1. Setelah itu klik scan

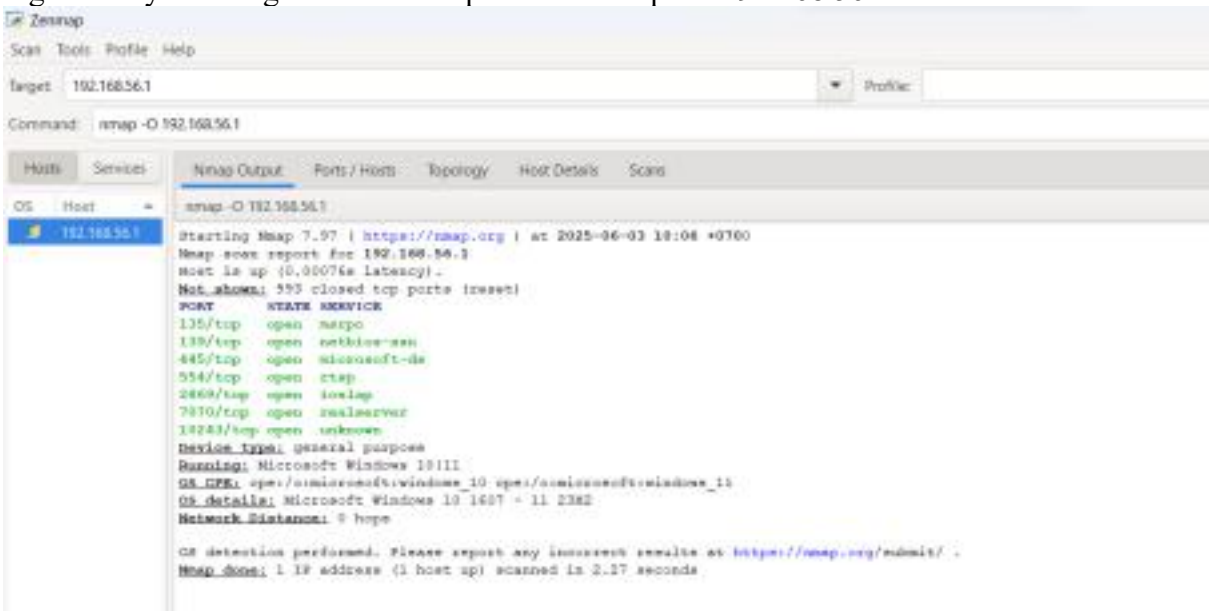


2. Dari hasil scanning ada 7 port yang terbuka

```
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
554/tcp   open  rtsp?
2869/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
2968/tcp  open  enpp?
7070/tcp  open  ssl/realserver?
| ssl-cert: Subject: commonName=AnyDesk Client
```



3. Disini saya juga akan melakukan pendekteksian terhadap sistem operasi target yang digunakan yaitu dengan melakukan perintah : nmap –O 192.168.56.1 Jika sudah klik scan



Nmap tidak bisa memberikan info pasti tentang OS, namun hanya terbatas menebak sistem operasi yang dipakai. Perhatikan hasil scan diatas, ip. Analisa 192.168.56.1 kemungkinan besar menggunakan Windows