



Kampus
Merdeka
INDONESIA JAYA

Keamanan Siber

Pertemuan 4 – Vulnerability Assesment

I Wayan Ardiyasa-ITB STIKOM Bali 2024

Always The First





Introduction

- Perubahan yang sangat cepat, kadang kala melupakan developer dalam melakukan pengujian terhadap aplikasi yang dibangun.
- Pengujian merupakan proses yang sangat penting didalam pengembangan perangkat lunak yang berkualitas tinggi, karena dari beberapa kesalahan yang dianggap tidak penting beresiko sangat berbahaya hal ini menjadi celah (vulnerability) bagi attacker untuk memanfaatkan informasi yang di curi melalui serangan kepada aplikasi,



Introduction

- Kebutuhan akan **vulnerability assessment** selama ini biasanya dipandang sebelah mata, karena hanya dianggap sebagai kegiatan formalitas dan sedikit orang yang melakukan kegiatan ini.



Definisi Vulnerability

- **Vulnerability** adalah sebuah kelemahan, kekurangan atau celah pada sistem, yang dapat dimanfaatkan oleh satu atau lebih dari penyerang untuk melakukan serangan yang dapat membahayakan kerahasiaan, integritas, atau ketersediaan suatu sistem.

Definisi Vulnerability Assessment



- **Vulnerability Assessment** adalah analisa keamanan secara menyeluruh dan mendalam seperti pada keamanan informasi, hasil scanning jaringan, cara pengelolaan, konfigurasi pada sistem, kesadaran keamanan aktor yang terlibat dan keamanan fisik, untuk mengetahui seluruh potensi kelemahan kritis yang ada.

Definisi Vulnerability Assessment



- Vulnerability Assessment akan dilakukan dengan melakukan pemeriksaan secara terperinci dan sistematis pada infrastruktur komputasi suatu bisnis atau perusahaan untuk menentukan kelemahan atau celah yang mungkin bisa ditembus oleh pihak tidak bertanggung jawab dalam desai, implantasi atau prakteknya.

Tujuan Vulnerability Assessment



- Untuk melakukan proses identifikasi, evaluasi, dan klasifikasi tingkat kerentanan pada sistem keamanan yang ada pada ekosistem informasi teknologi.
- Hasil dari identifikasi, evaluasi, dan klasifikasi melalui Vulnerability Assessment akan memberikan pandangan kepada pemilik sistem yang mengadakan proses tersebut agar pengguna tahu bahwa ada celah yang bisa disalah gunakan oleh pihak yang tidak bertanggung jawab terkait data penting pengguna tersebut.



Jenis-Jenis Vulnerability Assesment

1. Host Assesment

Assesment akan dilakukan pada server, workstation, jaringan host lainnya dan keseluruhan infrastruktur digital

2. Network Assesment

Pemeriksaan pada jaringan (Kabel maupun nirkabel) dan untuk memastikan jaringan publik atau jaringan pribadi tidak diakses oleh orang yang tidak berwenang

3. Application Assesment

Melakukan pemeriksaan kerentanan dalam aplikasi

4. Database Assesment

Melakukan pemeriksaan untuk mendapatkan celah keamanan pada database.

Metode Vulnerability Assessment





Metode Vulnerability Assessment

- Identification Scope → Tahap untuk melakukan identifikasi ruang lingkup penelitian yaitu dengan memilih sistem target.
- Information Gathering → Tahap untuk mengumpulkan informasi publik, seperti IP Address, Port, host name.
- Vulnerability Scanning → Tahap untuk mencari kerentanan pada sistem informasi
- Vulnerability Analisis → Tahap untuk menganalisis informasi- informasi vulnerability yang ditemukan.
- Report → Terkait dengan dokumentasi kegiatan



Kampus
Merdeka
INDONESIA JAYA

PENETRATION TESTING



Finding Vulnerability

Always The First

I Wayan Ardiyasa-ITB STIKOM Bali 2024



Definisi Finding Vulnerability

- Suatu proses identifikasi celah keamanan pada suatu sistem, aplikasi, atau jaringan.
- Tujuannya yaitu untuk menemukan vulnerability yang bisa dieksploitasi.
- Teknik Finding Vulnerability yaitu :
 - Scanning Network
 - Scanning Vulnerability (Nessus, Nmap)



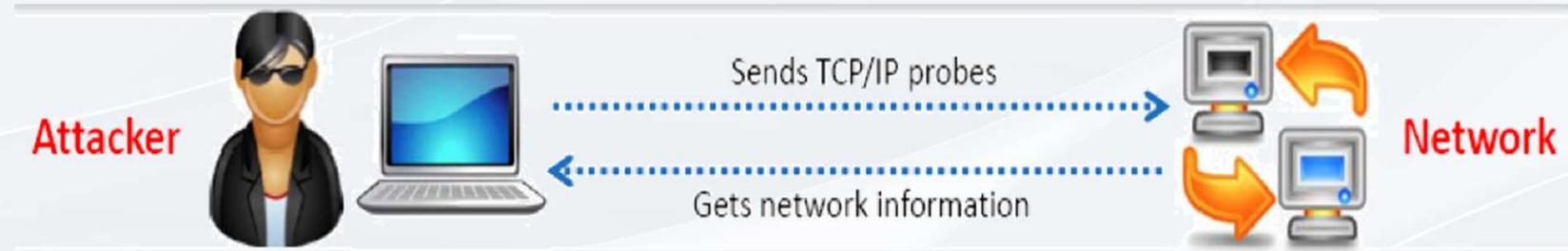
Definisi Scanning

- Teknik untuk mengidentifikasi **host, port number** dan **service** didalam sebuah jaringan.
- Scanning Network sebagai komponen **intelligence gathering** bagi seorang attacker untuk mengetahui arsitektur system dan jaringan suatu target.
- Output scanning network :
 - IP Address dan port number pada host;
 - Sistem Operasi serta arsitektur system;
 - Service yang berjalan pada host.

Gambaran umum Scanning



Kampus
Merdeka
INDONESIA JAYA



Teknik Scanning



- **Port Scanning**

- Mencari informasi tentang Port number serta service yang berjalan pada mesin target;

- **Network Scanning**

- Mencari informasi IP address pada mesin target/host yang terkoneksi pada jaringan komputer serta melakukan mapping jaringan;

- **Vulnerability Scanning**

- Mencari informasi vulnerability pada mesin target/ host didalam jaringan komputer.



Kampus
Merdeka
INDONESIA JAYA

Konsep Scanning

- Mengirimkan request **ICMP ECHO** ke host. Jika host dalam keadaan up/live, maka host akan mereplay **ICMP ECHO**.
- Teknik scanning ini, berguna untuk mencari perangkat aktif atau menentukan apakah **ICMP** melewati firewall
- Perintah nmap tool
 - **Nmap -v -sP 192.168.1.1/24**



Contoh Perintah Scanning

Berikut perintah scan dengan menggunakan aplikasi Nmap, yaitu :

- **nmap -v -A 127.0.0.1** → Mendapatkan Informasi lebih detail dari mesin target (ALL)
- **nmap -O 127.0.0.1** → Informasi OS yang digunakan target
- **nmap -sA 127.0.0.1** → Mendeteksi firewall pada mesin target
- **nmap -sP 127.0.0.1** → menemukan host yang aktif didalam jaringan
- **nmap -po-200 127.0.0.1** → scanning untuk spesifik port



Kampus
Merdeka
INDONESIA JAYA

PENETRATION TESTING



Scanning Vulnerability

Always The First

I Wayan Ardiyasa-ITB STIKOM Bali 2024

Pengertian Vulnerability



Suatu kelemahan program/infrastruktur yang memungkinkan terjadinya eksploitasi sistem. Kerentanan (*vulnerability*) ini terjadi akibat kesalahan dalam merancang, membuat atau mengimplementasikan sebuah sistem



Bagaimana terjadinya Bug

Vulnerability/bug terjadi ketika developer melakukan kesalahan logika koding atau menerapkan validasi yang tidak sempurna sehingga aplikasi yang dibuatnya mempunyai celah yang memungkinkan user atau metode dari luar sistem bisa dimasukkan kedalam programnya.

Jenis Bug



Kampus
Merdeka
INDONESIA JAYA

- Firmware (*Hardcoded software*)
- Software
- Brainware
- Web Sistem



Jenis Bug/Vulnerability pada Windows

Windows xp vulnerability mso8-067 (Remote Vulnerability [Service vulnerability])

Celah keamanan ini memungkinkan attacker untuk menjalankan malware secara remote dengan cara membuat paket request khusus.

<https://technet.microsoft.com/en-us/library/security/mso8-067.aspx>



Informasi bug dan vulnerability up-to-date

- Exploit DB : <https://www.exploit-db.com/>

The screenshot shows the Exploit Database website interface. The header includes the site name 'EXPLOIT DATABASE' and navigation icons. Below the header, there are filter options for 'Verified' and 'Has App', a 'Show 15' dropdown, and a search bar. The main content is a table of vulnerabilities with columns for Date, D, A, V, Title, Type, Platform, and Author.

Date	D	A	V	Title	Type	Platform	Author
2024-03-28	↓	×		liveSite Version 2019.1 - Remote Code Execution	WebApps	PHP	tmswrr
2024-03-28	↓	×		WinRAR version 6.22 - Remote Code Execution via ZIP archive	Remote	Windows	E1 Coders
2024-03-28	↓	×		Dell Security Management Server <1.9.0 - Local Privilege Escalation	Local	Linux	Amirhossein Bahramizadeh
2024-03-28	↓	×		Siklu MultiHaul TG series < 2.0.0 - unauthenticated credential disclosure	Remote	Hardware	semaja2
2024-03-28	↓	×		RouterOS 6.40.5 - 6.44 and 6.48.1 - 6.49.10 - Denial of Service	DoS	Hardware	ice-wzl



Kategori Temuan Bug

- **Zero Day Vulnerability** → vulnerability yang ditemukan oleh hacker sedangkan pihak developer tidak mengetahuinya, dan hacker mengambil keuntungan dari vulnerability tersebut untuk menyebarkan malware atau masuk ke sistem secara ilegal.
- **Zero day Exploit** → exploit yang dibuat hacker berdasar zero day vulnerability yang ditemukannya untuk mengexploitasi sistem yang rentan terhadap vulnerability yang telah ditemukannya.



Scanning Vulnerability

Scanning vulnerability → mencari/memindai kerentanan di seluruh sistem informasi (termasuk komputer, sistem jaringan, sistem operasi, dan aplikasi perangkat lunak) yang mungkin berasal dari vendor, kegiatan administrasi sistem, atau aktivitas pengguna



Tools Scanning Vulnerability

- Tools yang digunakan antara lain :
 1. Nessus
 2. Nikto
 3. OpenVAS
 4. Acunetix
 5. W3AF



Teknik Scanning Vuln : Nessus

- Untuk mengakses Nessus, bisa melakukan via browser dengan url : <https://localhost:8834/#/>
- Untuk menjalankan nessus perlu dilakukan start nessus dengan command :
 - **#!/etc/init.d/nessusd start**
- Untuk menghentikan proses nessus lakukan dengan perintah berikut :
 - **#!/etc/init.d/nessusd stop**



Kampus
Merdeka
INDONESIA JAYA

Teknik Scanning Vuln : Nessus

- Halaman Login
- Untuk login akun menggunakan username & password yang sudah didaftarkan melalui web nesus yaitu tenable

Nessus ™

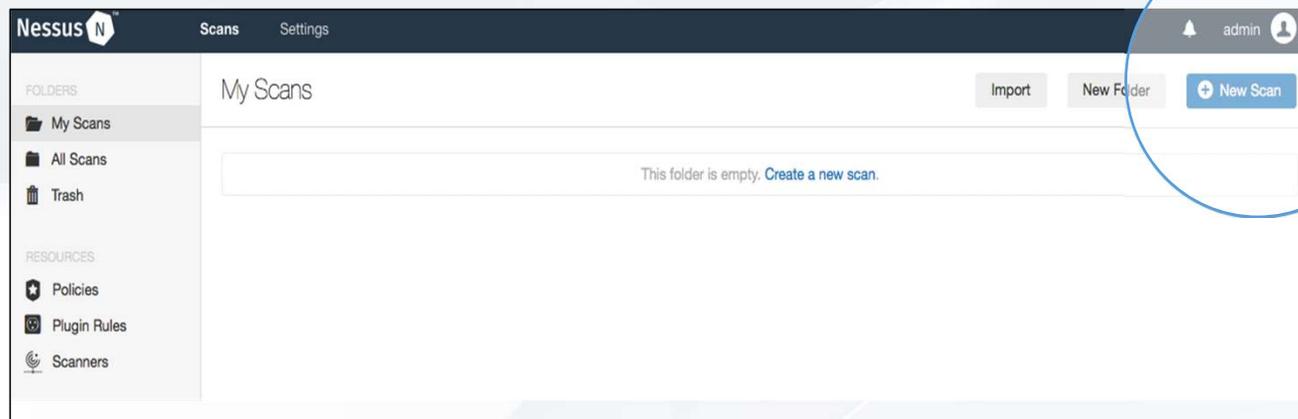


Remember Me



Teknik Scanning Vuln : Nessus

- Untuk melakukan scan, Klik Button New Scan pada gambar berikut :

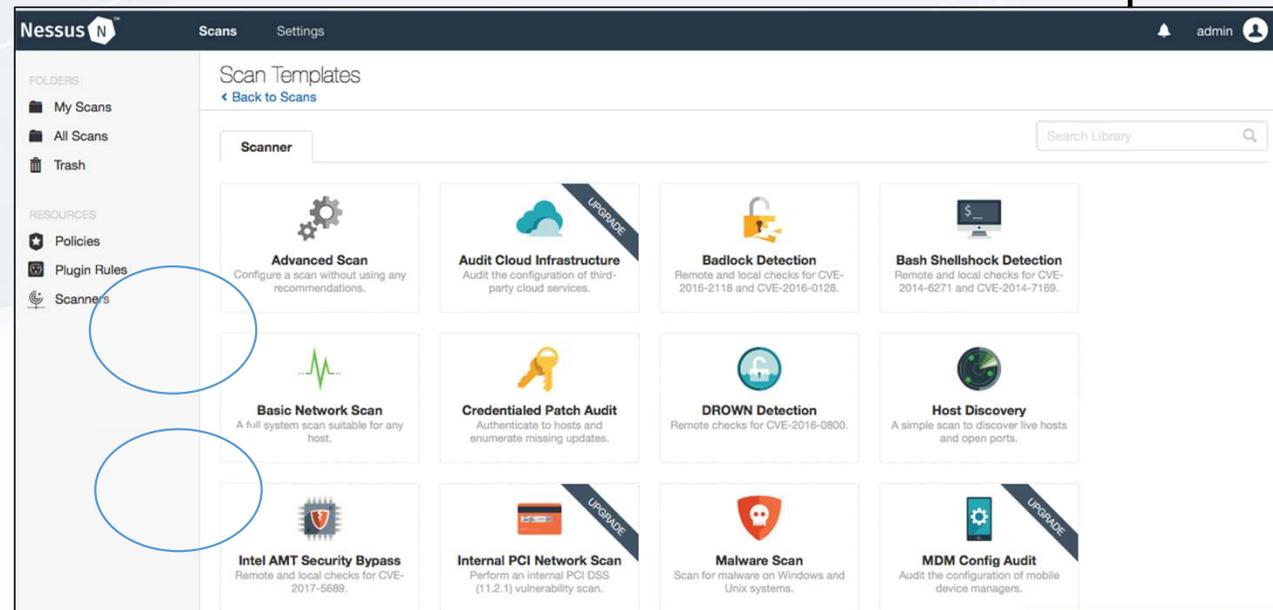




Kampus
Merdeka
INDONESIA JAYA

Teknik Scanning Vuln : Nessus

Selanjutnya itu pilih **advanced scan** atau **Basic Network Scan** pada **Scan Templates**





Kampus
Merdeka
INDONESIA JAYA

Teknik Scanning Vuln : Nessus

Pada mode scan yang dipilih, isi pada isian yang diminta. Seperti gambar dibawah ini :

The screenshot shows the Nessus web interface for configuring a new scan. The page title is "New Scan / Advanced Scan" with a "Back to Scan Templates" link. The "Settings" tab is selected, showing a left-hand navigation menu with categories like "BASIC", "DISCOVERY", "ASSESSMENT", "REPORT", and "ADVANCED". The main form contains the following fields:

- Name:** Test Scanning
- Description:** (empty text area)
- Folder:** My Scans (dropdown menu)
- Targets:** 192.168.231.132 (text area)

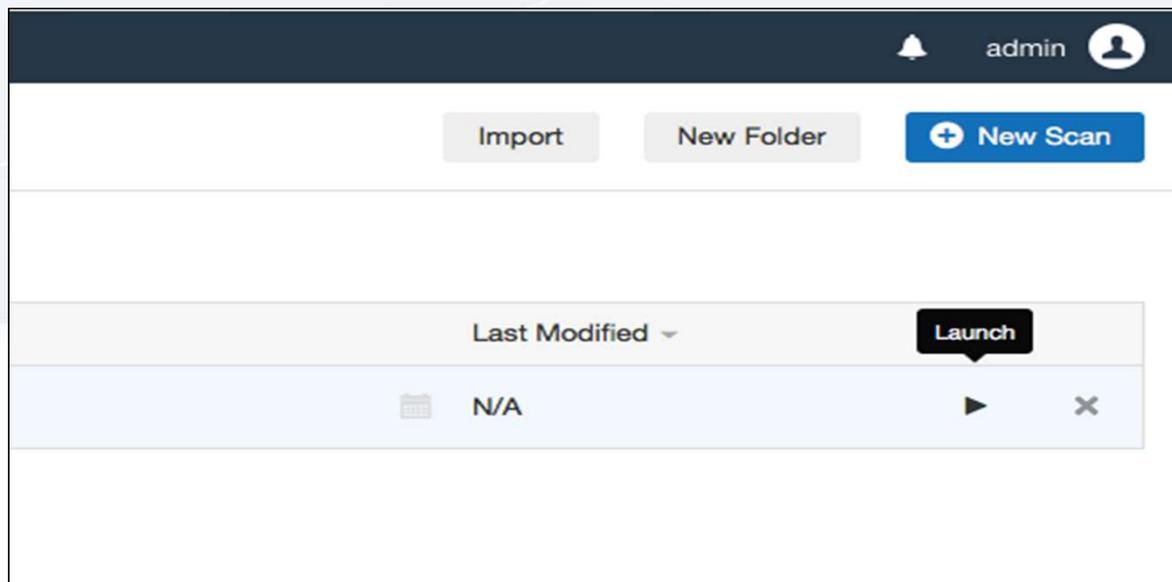
At the bottom of the form, there is an "Upload Targets" section with an "Add File" link. The "Save" button is highlighted in blue, and a "Cancel" button is also visible.



Kampus
Merdeka
INDONESIA JAYA

Teknik Scanning Vuln : Nessus

- Selanjutnya klik button ► pada halaman kerja, seperti Digambar dibawah ini :





Hasil Scanning dari Nessus

Output yang dihasilkan dari scanning terhadap mesin target yaitu apabila **CRITICAL** berarti mesin target tersebut memiliki *vulnerability*. Pada hasil scanning tersebut juga diberikan informasi dari exploit yang bisa digunakan untuk melakukan tahap gaining acces

The screenshot shows the Nessus Scans page with a list of 36 vulnerabilities. The table below represents the visible data in the screenshot.

Sev	Name	Family
CRITICAL	MS05-027: Vulnerability in SMB Could All...	Windows
CRITICAL	MS06-040: Vulnerability in Server Servic...	Windows
CRITICAL	MS08-067: Microsoft Windows Server Se...	Windows
CRITICAL	MS09-001: Microsoft Windows SMB Vuln...	Windows
CRITICAL	MS17-010: Security Update for Microsoft ...	Windows



Scanning Vulnerability dengan Nmap

- Didalam jaringan komputer terkait dengan mencari informasi vulnerability pada suatu host bisa menggunakan nmap dengan menggunakan option **--script vuln**, seperti dibawah ini :
- **nmap --script vuln 192.168.10.1**
- Ket :
 - **--script vuln**: Menjalankan script vuln pada target.



**Kampus
Merdeka**
INDONESIA JAYA

Single Degree Program

S2 - Sistem Informasi (M.Kom.)

S1 - Sistem Komputer (S.Kom.)

S1 - Sistem Informasi (S.Kom.)

S1 - Teknologi Informasi (S.Kom.)

S1 - Bisnis Digital (S.Bns.)

D3 - Manajemen Informatika (A.Md.Kom.)

Dual Degree International Program

S1 - Sistem Informasi (S.Kom., B.IT.)

(collaboration with HELP University)

S1 - Bisnis Digital (S.Bns., B.M.)

(collaboration with DNUI University)

Dual Degree National Program

S1 - Sistem Informasi (S.Kom., S.Ds.)

(collaboration with Universitas Teknologi Bandung)



www.stikom-bali.ac.id



info@stikom-bali.ac.id



(0361) 244445



STIKOMERS TV



STIKOM Bali



@stikombali

I Wayan, Always The First

I Wayan, Always The First STIKOM Bali 2023