Keamanan Siber

Pertemuan 4 – Vulnerability Assesment

I Wayan Ardiyasa-ITB STIKOM Bali 2024

Always The First

Introduction

- Perubahan yang sangat cepat, kadang kala meluputkan 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 Assesment

- **Vulnerability Assesment** 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 Assesment

- 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 Assesment

- 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**

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

2. **Network Assesement**

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

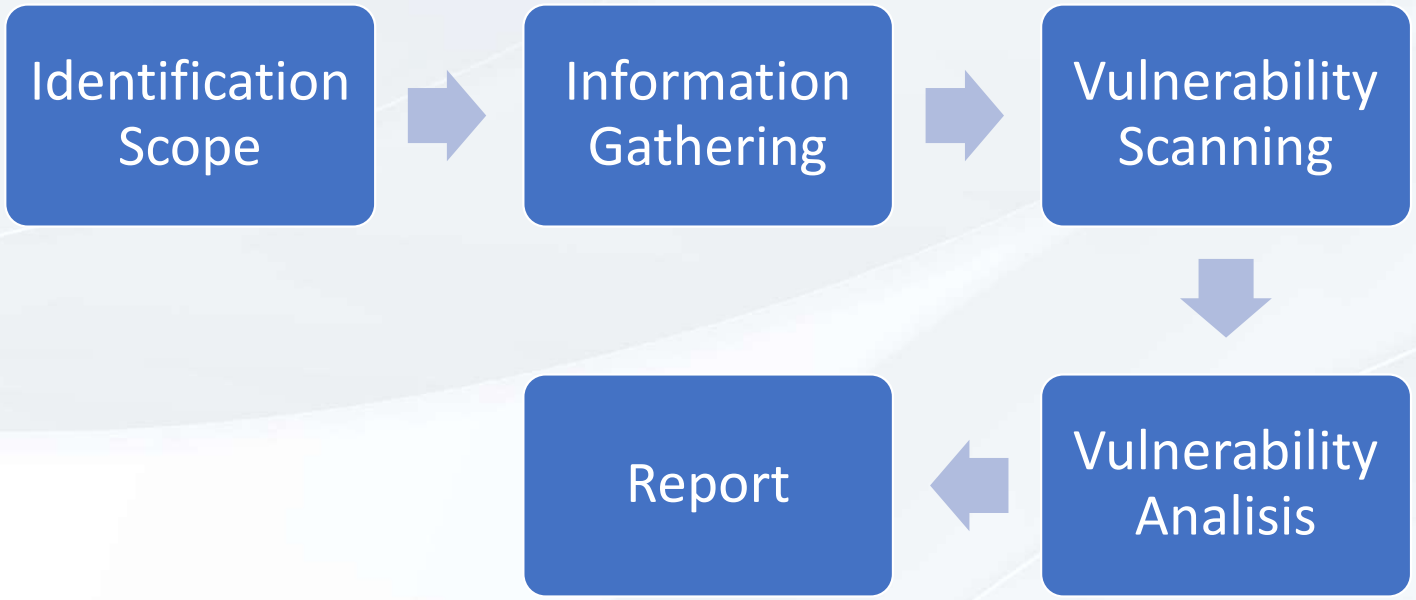
3. **Aplication Assesment**

   Melakukan pemeriksaan kerentanan dalam aplikasi

4. **Database Assesment**

   Melakukan pemeriksaan untuk mendapatkan celah keamanan pada database.

Metode Vulnerability Assesment



Metode Vulnerability Assesment

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

Finding Vulnerability

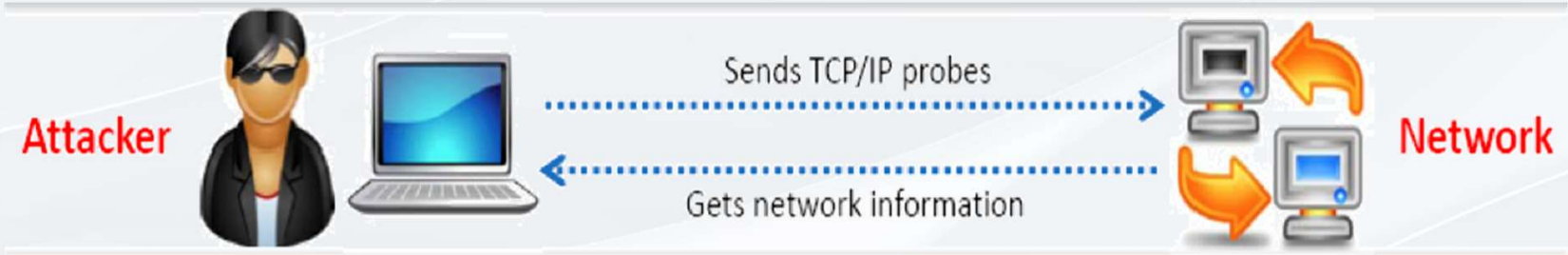
Definisi Finding Vulnerability

- 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



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 meisn target/ host didalam jaringan komputer.

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 –p0-200 127.0.0.1** → scanning untuk spesifik port

Scanning Vulnerability

Pengertian Vulnerability

Suatu kelemahan program/infrastruktur yang memungkinkan terjadinya exploitasi 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 dimasukan kedalam programnya.

Jenis Bug

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

Jenis Bug/Vulnerability pada Windows

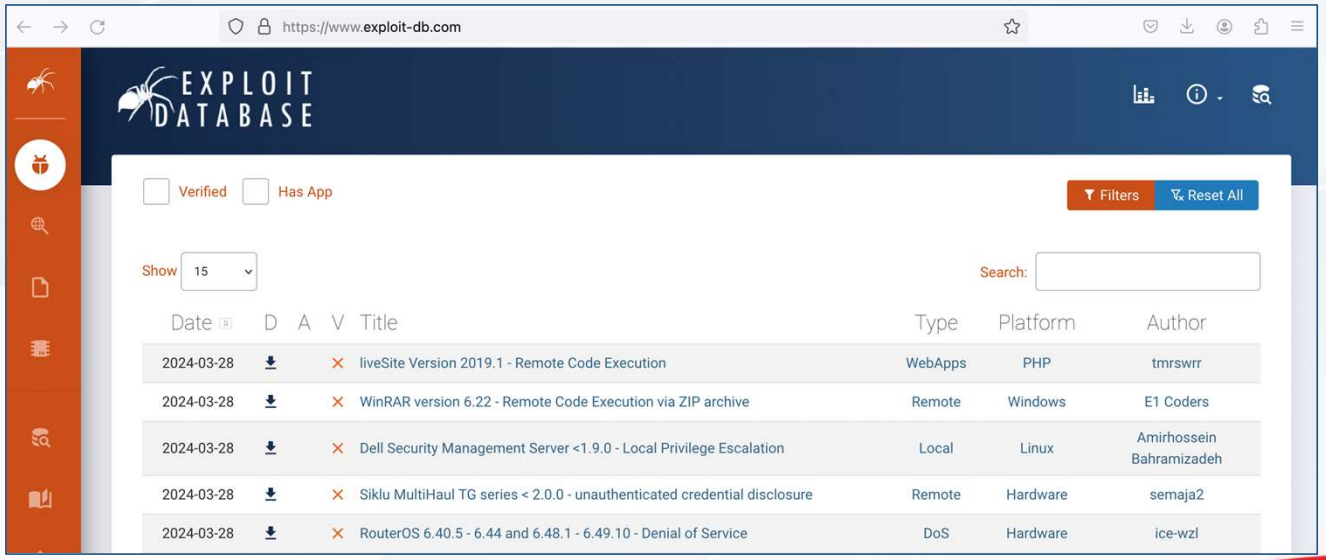
Windows xp vulnerability mso8-067 (Remote Vulnerability |Service vulnerability)

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/



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 ditemukan nya untuk mengexploitasi sistem yang tentan terhadap vulnerability yang telah ditemukan nya.

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 dgunakan antara lain :

1. Nessus
2. Nikto
3. OpenVAS
4. Acunetix
5. W3AF

Teknik Scanning Vuln : Nessus

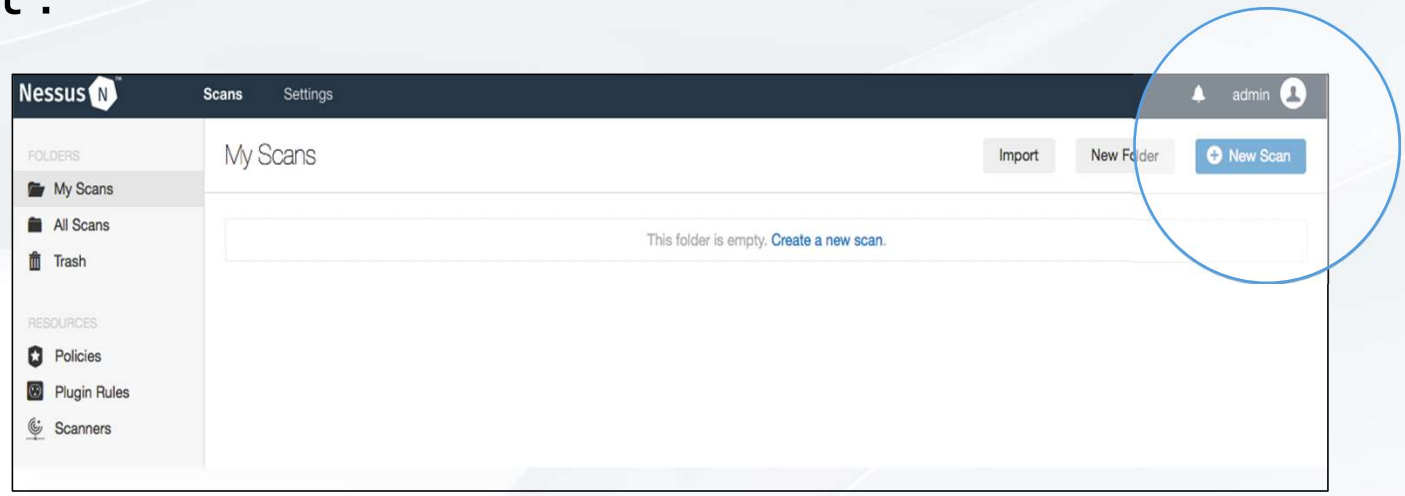
- Untuk mengakses Nessus, bisa melakukan via browser dengan url : https://localhost:8834/#/
- Untuk menjalankan nessus perlu dilakukan start nessus dengan command :
  - **#/etc/init.d/nessusd start**
- Untuk menghentikan proses nessus lakukan dengan perintah berikut :
  - **#/etc/init.d/nessusd stop**

Teknik Scanning Vuln : Nessus

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

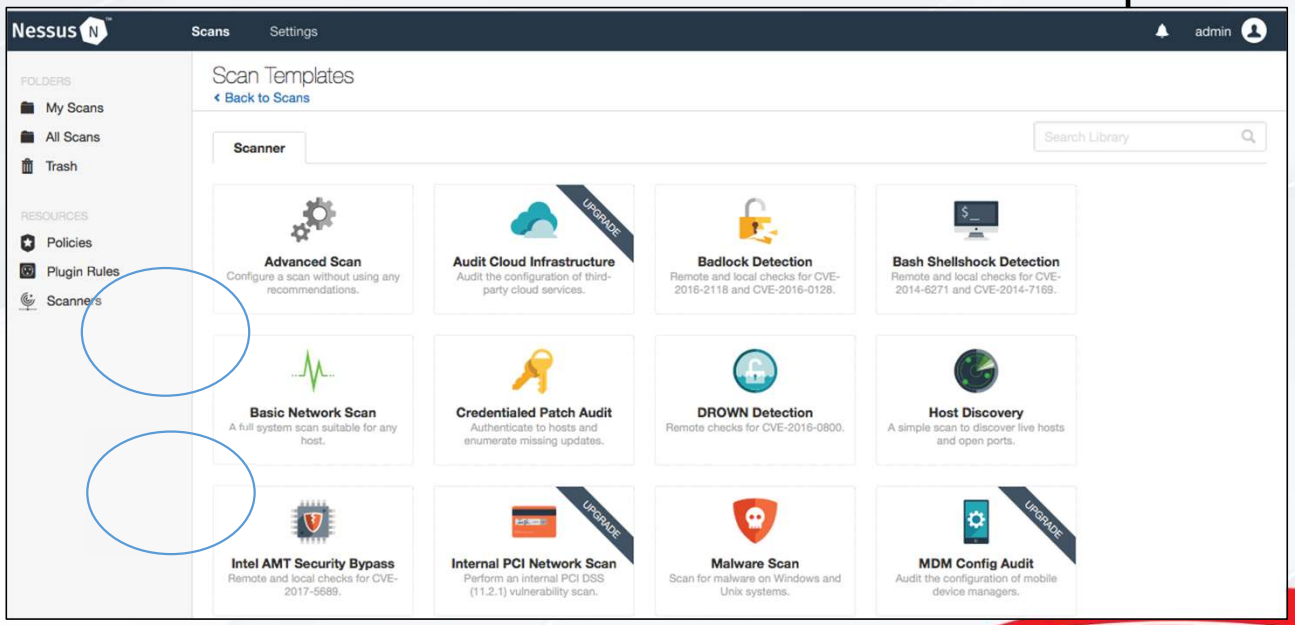
Teknik Scanning Vuln : Nessus

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



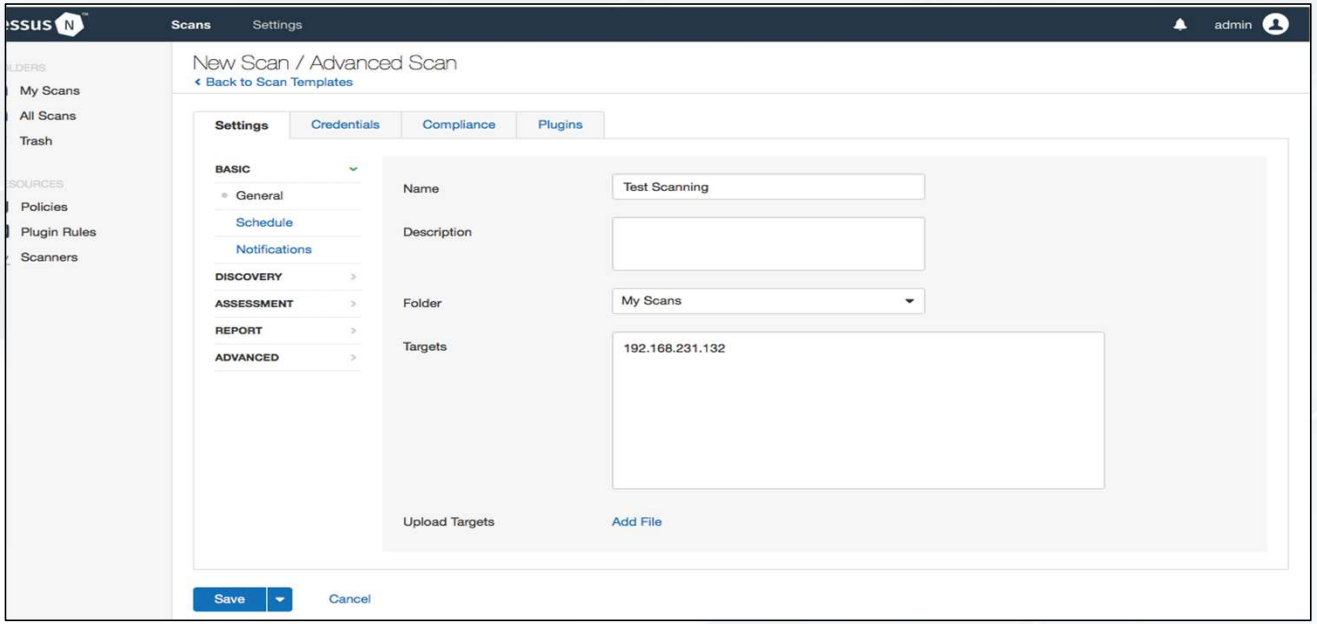
Teknik Scanning Vuln : Nessus

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



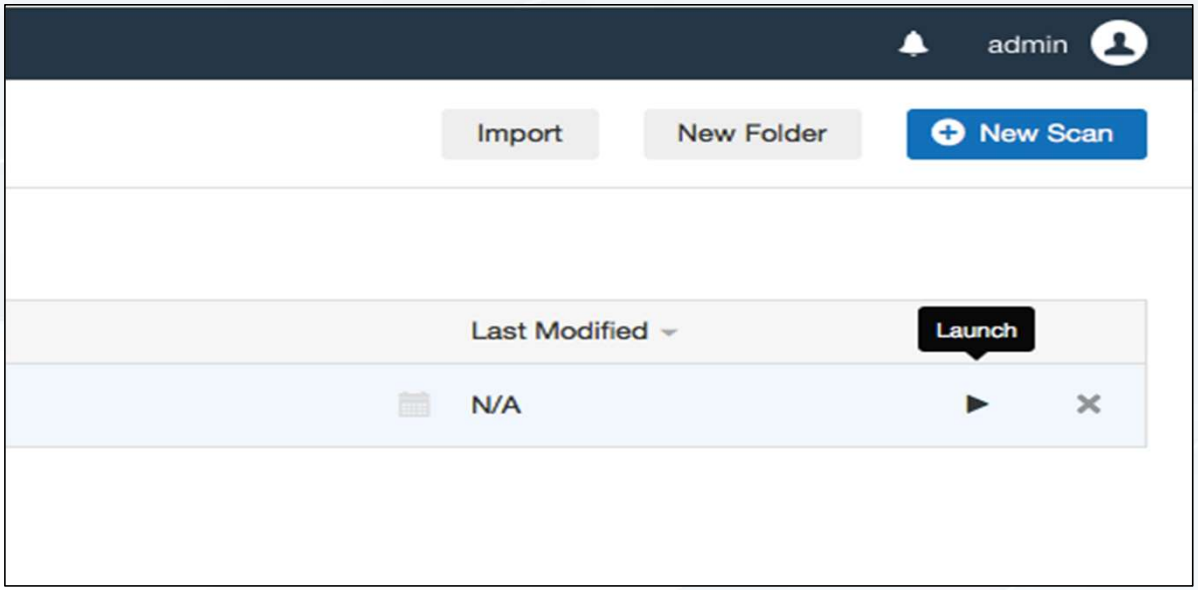
Teknik Scanning Vuln : Nessus

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



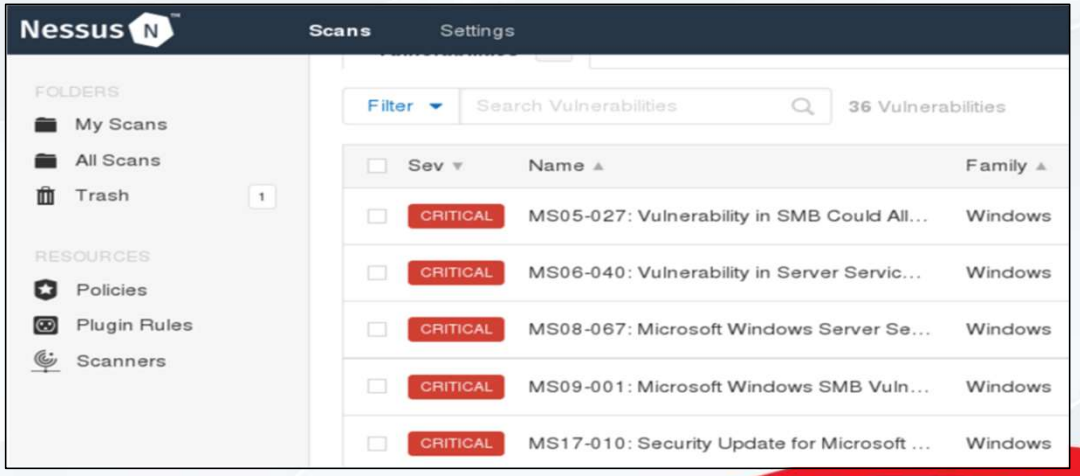
Teknik Scanning Vuln : Nessus

- 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



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.

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