

# **LAPORAN PRAKTIKUM**

## **VULNERABILITY AND SOCIAL ENGINEERING**



**DISUSUN OLEH :**

Nama : Diki Candra  
Nim : 2022903430010  
Kelas : TRKJ 2B  
Jurusan : Teknologi Informasi dan Komputer  
Program Studi : Teknologi Rekayasa Komputer Jaringan  
Dosen Pengajar : Aswandi, S.Kom, M.Kom.

**JURUSAN TEKNOLOGI INFORMASI DAN KOMUNIKASI**  
**PRODI TEKNOLOGI REKAYASA KOMPUTER DAN JARINGAN**  
**POLITEKNIK NEGERI LHOKSEUMAWE**  
**TAHUN 2022/2023**

## LEMBARAN PENGESAHAN

Laporan Yang Berjudul : Vulnerability And Social Engineering  
Disusun Oleh : Diki Candra  
NIM : 2022903430010  
Tanggal Praktikum : 18 September 2023  
Tanggal Penyerahan : 25 September 2023  
Jurusan : Teknologi Informasi & Komputer  
Program Studi : Teknologi Rekayasa Komputer Jaringan  
Mata Kuliah : Ethical Hacking  
Tabel Penilaian :



Mengetahui,

Dosen Pembimbing,

Penyusun,

Aswandi, S.Kom, M.Kom  
NIP. 197209242010121001

Diki Candra  
NIM. 2022903430010

<p style="text-align: center;"><b>LABORATORIUM: JARINGAN DAN MULTIMEDIA</b> <b>POLITEKNIK NEGERI LHOKSEUMAWE</b> <b>PENGUJIAN: VULNERABILITY AND SOCIAL ENGINEERING</b></p>
---

## **I. Capaian Praktikum/Kompetensi**

Setelah mengikuti praktikum *vulnerability dan social engineering*, diharapkan praktikan dapat:

1. Mahasiswa mampu mengidentifikasi kelemahan atau kerentanan sistem
2. Mahasiswa mampu mencari kelemahan sistem dan setelah ditemukan kemudian kelemahan sistem tersebut dicoba untuk dieksploitasi untuk mengetahui kemungkinan-kemungkinan dampak yang terjadi.
3. Mahasiswa mampu mendapatkan daftar kelemahan yang dimiliki oleh sistem kita dan penyebabnya serta rekomendasi untuk memperbaiki kelemahan ataupun menutup lubang keamanan yang masih ada.
4. Mengetahui apa yang perlu diperbaiki dari sistemnya agar sistemnya cukup tangguh dari potensi kegagalan ataupun potensi dibobol hacker/cracker
5. Mahasiswa mampu melakukan tindakan preventif untuk mencegah sistemnya dibobol dan ditipu oleh blackhat hacker (cracker).
6. Mahasiswa diharapkan mampu menggunakan software yang digunakan untuk *vulnerability dan social engineering* pada site yang terdeteksi.

## **II. Keselamatan Kerja**

Praktikum *vulnerability dan social engineering* diharapkan mengikuti aturan keselamatan kerja, sebagai berikut:

1. Gunakanlah pakaian praktik!
2. Gunakan alas kaki yang terbuat dari karet untuk menghindari tersengat listrik
3. Bacalah dan pahami petunjuk praktikum pada setiap lembar kegiatan belajar!
4. Hati-hati dalam melakukan praktik!
5. Gunakanlah peralatan praktikum sesuai fungsinya!
6. Setelah selesai praktikum, matikan semua peralatan praktik dengan benar dan rapikan kembali posisi kursi maupun meja komputer.

### III. Teori

*Vulnerability* (kerentanan) adalah merupakan suatu cacat pada sistem/infrastruktur yang memungkinkan terjadinya akses tanpa izin dengan meng *exploit*asi kecacatan sistem. Cacat (*threat*) ini terjadi akibat kesalahan dalam merancang, membuat atau mengimplementasikan sebuah sistem. *Vulnerability* digunakan sebagai dasar pembuatan *exploit* oleh hacker sebagai jalan untuk masuk kedalam sistem secara ilegal. Hacker biasanya akan membuat *Exploit* yang disesuaikan dengan *vulnerability* yang telah ditemukan nya. Setiap aplikasi (*service, desktop, web base*) pasti memiliki celah atau *vulnerability*, hanya saja belum ketauan, lambat laun akan ditemukan juga oleh hacker. Tidak semua hacker jahat, jika celah keamanan ditemukan oleh hacker jahat (*Black Hat*) kemungkinan akan digunakan untuk meng *exploit* system untuk dia gunakan sendiri, atau *exploit* tersebut akan dilelang di “*deep web*” dan dijual nya ke penawar tertinggi. Jika ditemukan oleh hacker baik (*white hat*) biasanya dia akan melaporkan celah keamanan tersebut ke developer aplikasi tesebut agar diperbaiki.

*Social engineering* adalah kegiatan untuk mendapatkan informasi rahasia/penting dengan cara menipu pemilik informasi tersebut. *Social engineering* umumnya dilakukan melalui telepon dan Internet. *Social engineering* merupakan salah satu metode yang digunakan oleh hacker untuk memperoleh informasi tentang targetnya, dengan cara meminta informasi itu langsung kepada korban atau pihak lain yang mempunyai informasi itu. *Social engineering* mengkonsentrasikan diri pada rantai terlemah sistem jaringan komputer, yaitu manusia. Seperti kita tahu, tidak ada sistem komputer yang tidak melibatkan interaksi manusia. Dan parahnya lagi, celah keamanan ini bersifat universal, tidak tergantung platform, sistem operasi, protokol, software ataupun hardware. Artinya, setiap sistem mempunyai kelemahan yang sama pada faktor manusia. Setiap orang yang mempunyai akses kedalam sistem secara fisik adalah ancaman, bahkan jika orang tersebut tidak termasuk dalam kebijakan keamanan yang telah disusun. Seperti metoda hacking yang lain, *social engineering* juga memerlukan persiapan, bahkan sebagian besar pekerjaan meliputi persiapan itu sendiri.

#### IV. Alat dan Bahan

Berikut ini merupakan alat dan bahan yang digunakan pada pelaksanaan praktikum *vulnerability dan social engineering*, adalah sebagai berikut:

1. VMWare
2. OS Server (Windows, Kali Linux)
3. OS Client (Windows XP/7/8/10)
4. Software (Nessus Vulnerability, Online tool, Winrtgen tool, Pwdump7, Ophcrack tool, NTFS, Steganography Kali Linux Social Engineering Toolkit).

#### V. Prosedur Praktikum

##### **Percobaan 1: Pencarian informasi menggunakan *Nessus Vulnerability Scanning Tool***

Dalam keamanan sistem menggunakan aplikasi *Nessus Vulnerability Scanning Tool*. Studi kasus: komputer yang akan di scan pada jaringan pribadi 10.10.10.0/24 untuk kerentanan menggunakan vulnerability scanning tool, prosedur praktikum sebagai berikut:

- a. Siapkan alat dan bahan
- b. Cek perlengkapan dan pastikan VMWare sudah terinstall dengan benar
- c. Pastikan sistem operasi Windows 10 sudah terinstall di dalam VMWare
- d. *Nessus* pada salah sistem operasi windows, download menggunakan link:  
<http://www.tenable.com/products/nessus/nessus-homefeed>
- e. Kemudian lakukan instal software *Nessus* yang telah didownload dari email
- f. Jalankan *service Nessus* yang telah diinstall di komputernya masing-masing, selanjutnya buka web <http://localhost:8834/WelcomeToNessus-Install/welcome>
- g. Lihat email dari *Tenable Nessus* yang berisi kode aktivasi yang berfungsi untuk registrasi akun nessus, lalu Inputkan *Activation Code*.
- h. Kemudian diharuskan memasukkan *username* dan *password* yang akan digunakan untuk login ke nessus sampai selesai.
- i. Lakukan konfigurasi jaringan, penyerang dan target berada pada satu jaringan
- j. Buat file policy baru dengan membuka *Tab pollicies* dan klik *create new policies*
- k. Kemudian muncul beberapa pilihan scan (pilih satu-satu untuk mengaturnya) untuk memilih jalur apa yang akan digunakan untuk mendeteksi *cybersecurity*

- l. Pada *Basic setting policy* terdapat dua textbox untuk menginput nama policy beserta deskripsi yang akan dibuat.
- m. Selanjutnya beralih ke “*My Scan*” dilanjutkan dengan memilih “*user defined*”, terlihat *file policy* yang telah dibuat pada tahap sebelumnya.
- n. Isikan data target seperti *name* (isikan dengan nama apapun), untuk *description* dapat diisi atau dikosongkan. Selanjutnya pada *target* diisi dengan alamat IP dari target yang ingin di scan, kemudian disimpan dengan klik *save*.
- o. Untuk memulai proses pemindaian, dapat dilakukan dengan *Launch* (icon panah kecil). Dan pengguna hanya perlu menunggu hingga proses selesai.
- p. Maka akan tampil hasil dari proses scanning salah alamat jaringan, terdapat pula detail scan beserta hasil scan dalam bentuk diagram.
- q. Untuk mengamati *vulnerability* yang terdeteksi, dapat dilakukan dengan klik pada *Tab Vulnerabilities*. Pengguna juga dapat memeriksa tab lain seperti *History* (riwayat) untuk mendapatkan detail lebih lanjut.
- r. Laporan hasil scanning dapat di export, caranya dengan membuka tab *Export* dan memilih format yang diperlukan.

## **Percobaan 2: Pencarian informasi dengan cara *Social Engineering* menggunakan *Kali Linux***

Dalam keamanan sistem menggunakan aplikasi *Kali Linux Social Engineering Toolkit* untuk mengkloning sebuah situs website dan mengirimkan tautan cloning kepada korbannya. Setelah itu korban akan mencoba masuk ke situs web menggunakan tautan (link), kredensialnya akan diekstraksi dari terminal Linux, prosedur praktikum sebagai berikut:

- a. Siapkan alat dan bahan
- b. Cek perlengkapan dan pastikan *VMWare* sudah terinstall dengan benar
- c. Pastikan sistem operasi *Kali Linux* sudah terinstall di dalam *VMWare*
- d. Buka *kali linux*, kemudian klik *applications* yang akan digunakan pada *kali linux*, pilih aplikasi ke-13 yaitu *social engineering tools* dan kemudian pilih *social engineering* dengan symbol tulisan *SET*
- e. Selanjutnya tekan tombol *Y* agar melanjutkan tahap selanjutnya untuk melihat serangan Rekayasa Sosial (*Social Engineering*) yang dapat kita dilakukan.

- f. Tampilan dibawahnya untuk melihat vektor serangan situs web.
- g. Muncul tampilan untuk metode serangan pemanen kredensial yang dapat dipilih nantinya untuk tindakan yang akan anda gunakan.
- h. Langkah selanjutnya tampil situs *Cloner* untuk memilih perintah apa yang akan gunakan, contoh: buat *site cloner* atau pilih nomor 2.
- i. Pilih perintah untuk mengcloningkan website apa saja yang pengguna inginkan.
- j. Memasukkan ip address yang akan di cloner sehinggaa akan mengkloning situs dari salah satu perusahaan terbesar didunia, misalnya facebook.
- k. Buka situs tersebut dengan ip yang telah menjadi *cloner* pada langkah diatas. Dan inilah hasilnya, tampilan ini akan keluar apabila pengguna benar melakukan langkah seperti diatas.

## VI. Data Percobaan

Setelah semua data diperoleh, maka data hasil pengamatan dan pengujian dimasukkan ke dalam tabel, sebagai berikut:

### Percobaan 1:

#### *Aplikasi:*

Nessus Vulnerability Scanning Tool

#### *Output:*

Detection Network

Configure

Audit Trail

[Back to My Scans](#)

Hosts 1









Vulnerabilities 4

History 1

Filter

Search Vulnerabilities

4 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	N...	Family	Count	
<input type="checkbox"/>	INFO			N...	Settings	1	 
<input type="checkbox"/>	INFO			E...	Misc.	1	 
<input type="checkbox"/>	INFO			E...	General	1	 
<input type="checkbox"/>	INFO			T...	General	1	 

### ***Impact/Indicator:***

Penggunaan Nessus Vulnerability Scanning Tool memungkinkan identifikasi kerentanan, pemantauan keamanan, dan pemahaman keamanan yang lebih baik. Namun, pemindaian dapat mempengaruhi kinerja jaringan, dan penggunaan alat semacam ini harus mematuhi hukum dan peraturan yang berlaku.

### ***Outcomes:***

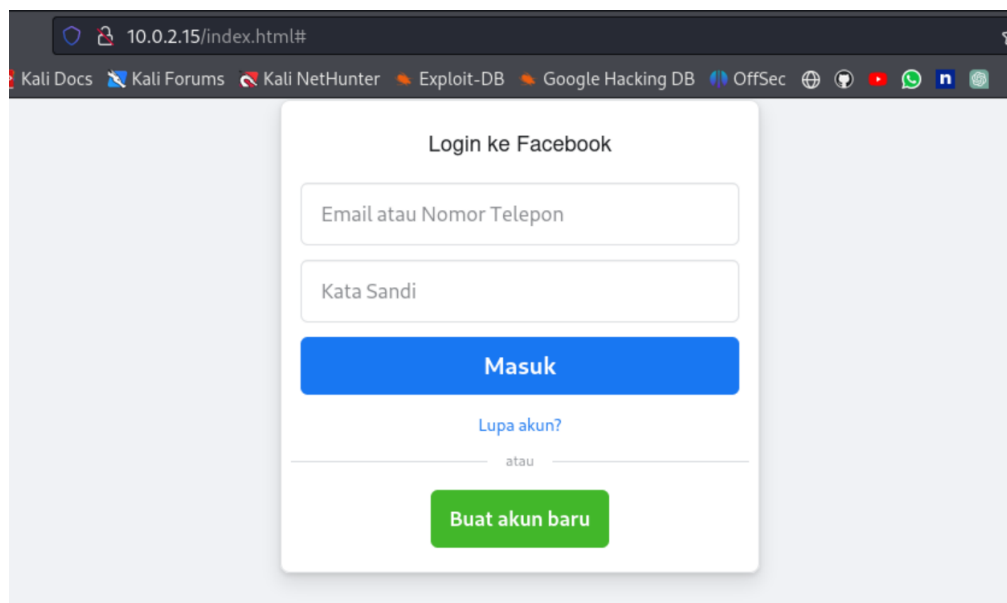
Manfaat dari percobaan menggunakan Nessus Vulnerability Scanning Tool adalah pemindaian dan identifikasi kerentanan potensial dalam jaringan, pemantauan keamanan yang lebih baik, pembuatan laporan yang membantu dalam perbaikan keamanan, konfigurasi jaringan yang lebih aman, pemenuhan persyaratan kepatuhan, dan pencegahan potensi risiko sebelum mereka dieksploitasi oleh penyerang.

## **Percobaan 2:**

### ***Aplikasi:***

Social Engineering

### ***Output:***





### ***Impact/Indicator:***

Percobaan dengan Social Engineering Toolkit di Kali Linux memungkinkan identifikasi kerentanan, pemahaman rekayasa sosial, kesadaran keamanan, tetapi juga menekankan pentingnya mematuhi hukum dan etika dalam penggunaan alat ini.

### ***Outcomes:***

Percobaan ini memberikan pemahaman tentang serangan rekayasa sosial dan meningkatkan kesadaran keamanan. Ini juga berfungsi sebagai pelatihan etis dan pengujian keamanan jika digunakan dengan benar. Namun, harus selalu digunakan dengan etika dan sah.

## **VII. Analisa dan Kesimpulan**

Percobaan Vulnerability Scanning (Nessus):

Percobaan menggunakan Nessus adalah pendekatan yang sah untuk mengidentifikasi kerentanan dalam jaringan atau sistem. Hasil pemindaian memberikan informasi tentang kerentanan yang perlu diperbaiki, dan itu dapat meningkatkan keamanan secara keseluruhan. Namun, pemindaian dapat mempengaruhi kinerja jaringan dan perlu dilakukan dengan hati-hati. Selain itu, penggunaan alat-alat semacam ini harus mematuhi hukum dan etika.

Percobaan Social Engineering (SET):

Percobaan dengan Social Engineering Toolkit (SET) menyoroti potensi serangan rekayasa sosial. Ini menunjukkan bagaimana serangan phishing dapat digunakan untuk mendapatkan kredensial pengguna. Hasil praktikum ini menggarisbawahi pentingnya kesadaran keamanan dan perlunya melindungi diri dari serangan semacam ini. Namun, penggunaan SET juga harus mematuhi hukum dan etika, karena penyalahgunaan dapat melanggar privasi dan keamanan.

Kesimpulan:

Percobaan Nessus membantu mengidentifikasi kerentanan dan memperbaiki keamanan, sementara percobaan Social Engineering Toolkit mengingatkan tentang serangan rekayasa sosial. Kedua percobaan menekankan pentingnya keamanan, pemahaman kerentanan, dan kesadaran.

### **VIII. Daftar Pustaka**

- Network, C., Fundamentals, D., Teare, B. D., & Paquet, C. (2005). Campus Network Design Fundamentals By Diane Teare, Catherine Paquet. In *Design*.
- Tiso, J., & Teare, D. (2011). *Designing Cisco Network Service Architectures (ARCH): Foundation Learning Guide*. Retrieved from <https://books.google.com/books?id=ISt9IXgcj0AC&pgis=1>
- Vachon, B., & Johnson, A. (2018). *Scaling networks: Companion guide*.