

# **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  
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

**LABORATORIUM: JARINGAN DAN MULTIMEDIA  
POLITEKNIK NEGERI LHOKSEUMAWE  
PENGUJIAN: SYSTEM HACKING**

**I. Capaian Praktikum/Kompetensi**

Setelah mengikuti praktikum *system hacking*, diharapkan praktikan dapat:

1. Mahasiswa mampu mengetahui adanya yang peretasan sistem (*System hacking*) untuk keperluan keselamatan
2. Mahasiswa mampu mencegah mendapatkan akses tidak sah ke sistem keamanan jaringan komputer.
3. Mahasiswa mampu merekomendasikan kelemahan keamanan jaringan sesuai dengan kebutuhan pengguna jaringan komputer
4. Mahasiswa mampu menggunakan beberapa jenis tool Hacking pada windows dan linux

**II. Keselamatan Kerja**

Praktikum *system hacking* 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**

*Hacking* suatu tindakan menemukan titik entri yang mungkin ada dalam sistem komputer atau jaringan komputer dan hingga berhasil mengambil alih. *Hacking* biasanya dilakukan untuk mendapatkan akses tidak sah ke sistem komputer atau jaringan komputer, baik untuk membahayakan sistem atau mencuri informasi sensitif yang tersedia pada komputer. *Hacking* dilakukan untuk menemukan

kelemahan dalam sistem komputer atau jaringan untuk tujuan pengujian, hal ini disebut *Ethical Hacking*.

Setelah mendapatkan informasi dari fase sebelumnya, sekarang lanjutkan ke fase peretasan sistem (*system hacking*). Proses peretasan sistem jauh lebih sulit dan kompleks daripada yang sebelumnya. Sebelum memulai fase peretasan sistem, peretas etis, atau pentester harus ingat bahwa Anda tidak dapat memperoleh akses ke sistem target dalam perjalanan. Anda harus menunggu apa yang Anda inginkan, mengamati dan berjuang secara mendalam; maka akan menemukan beberapa hasil. Proses peretasan Sistem diklasifikasikan ke dalam beberapa metode peretasan Sistem. Metode-metode ini juga disebut sebagai metodologi peretasan CEH oleh EC-Council. Metodologi ini meliputi:

1. Meretas kata sandi (*Cracking passwords*)
2. Hak akses yang lebih tinggi (*Escalating privileges*)
3. Menjalankan aplikasi (*Executing applications*)
4. Menyembunyikan file (*Hiding files*)
5. Menhilang jejak (*Covering tracks*)

#### **IV. Alat dan Bahan**

Berikut ini merupakan alat dan bahan yang digunakan pada pelaksanaan praktikum *system hacking*, adalah sebagai berikut:

1. VMWare
2. OS Server (Windows, Kali Linux)
3. OS Client (Windows XP/7/8/10)
4. Tools Software (*cirt, Winrtgen tool, Pwdump7 dan Ophcrack tool, NTFS Stream Manipulation, Steganography, Image Steganography, Clearing Audit Policies, Clearing logs*).

#### **V. Prosedur Praktikum**

##### **Percobaan 1: Online tool for default passwords**

Dalam peretasan sistem (*system hacking*), prosedur praktikum sebagai berikut:

- a. Siapkan alat dan bahan
- b. Cek perlengkapan dan pastikan VMWare sudah terinstall dengan benar

- c. Pastikan semua sistem operasi sudah terinstall di dalam *VMWare*
- d. Buka browser Internet, klik link ini <https://cirt.net/>, maka akan tampilan halaman website dari cirt.net yang digunakan untuk mencari kata sandi default perangkat
- e. Lakukan pilih manufaktur perangkat akan menampilkan daftar manufaktur, selanjutnya dapat dipilih salah satu yang ingin dilihat default password.
- f. Tampilkan semua kata sandi yang tersedia di semua perangkat oleh manufaktur.
- g. Terlihat User ID, Password, dan level lalu amati hasil yang akan ditampilkan.

### **Percobaan 2: Password Cracking menggunakan Pwdump7 & Ophcrack tool**

Dalam peretasan sistem (*system hacking*) untuk Password Cracking menggunakan aplikasi Pwdump7 dan Ophcrack tool, prosedur praktikum sebagai berikut:

- a. Download dan install Pwdump7 dan Ophcrack tool
- b. Jalankan aplikasi Pwdump7 tool pada OS windows
- c. Buka *Command Prompt* dengan administrator mode, masuk ke direktori users.
- d. Gunakan perintah *command dos* `wmic useraccount get name, sid` maka akan menampilkan semua pengguna dan kata sandi hash
- e. Buka direktori di mana pwdump7 berada dan dijalankan, contoh:  
`C:\Users\trkj\Desktop\pwdump7>pwdump7.exe`
- f. Buka hasil data hash yang telah diperoleh akan disalin ke file teks, buka di folder  
`C:\Users\ trkj\ Desktop\Hashes.txt`
- g. Hasil dalam format notepad yang diberinama hashes.txt.
- h. Jalankan aplikasi Ophcrack tool pada OS windows
- i. Klik tombol Load, lalu pilih File PWDUMP dari menu drop-down untuk mencari file hashes.txt, lakukan crack sehingga menemukan password target.
- j. Tampil hasil file hashes.txt telah kelihatan pada ophcrack terdapat 4 data dengan NT Hash berisi teks yang berupa kode untuk password
- k. Klik tombol Tables, contoh: tabel Vista free, lalu Pilih dan klik Instal
- l. Klik tombol “Crack”, selanjutnya menunggu hingga proses cracking selesai
- m. Tampil hasil proses crack selesai dilakukan, , dapat dilihat seperti gambar
- n. Login ke windows dengan user “trkj” (sesuaikan di komputer masing2) memasukkan kata sandi “khansa”.
- o. Masuk ke menu windows.

### **Percobaan 3: Menyembunyikan data menggunakan NTFS (New Technology File System) Stream Manipulation**

Menyembunyikan data/informasi menggunakan aplikasi NTFS (New Technology File System) Stream Manipulation, prosedur praktikum sebagai berikut:

- a. Buka CMD, buat file bernama Testfile.txt, menggunakan *notepad Testfile.txt*
- b. Isikan tulisan teks, seperti: “Tes File Normal”, selanjutnya simpan ~ klik close.
- c. Periksa ukuran file menggunakan command dos dengan perintah `dir Namafile.txt` maka akan ditampilkan seperti Volume drive c, volume serial number, directory, tanggal, jumlah file beserta ukuran file.
- d. Buat file yang bersifat tersembunyi pada direktori yang anda tentukan, kemudian gunakan perintah: `notepad Testfile.txt: hidden.txt`.
- e. Tulis teks pada notepad Testfile.txt: hidden.txt dengan tulisan teks “File tersembunyi”, selanjutnya file disimpan, dan Notepad di close.
- f. Pemeriksaan kembali ukuran file dengan perintah yang sama dengan sebelumnya. Hasil dari perintah tersebut tidak berubah, ukuran sama seperti sebelumnya, seperti Volume drive c, volume serial number, directory, tanggal, jumlah file beserta ukuran file.
- g. Ketik perintah `type Testfile.txt: hidden.txt`, maka hasil diperoleh incorrect.
- h. Periksa direktori (File explorer), maka tidak kelihatan ada file tambahan yang dibuat. File hidden tidak terdapat pada direktori tersebut).
- i. Gunakan utilitas seperti *Makestrm.exe* untuk mengekstrak informasi tersembunyi dari aliran ADS.
- j. Jalankan Aplikasi Spy ADS (NTFS Stream Detection)
- k. Pilih opsi jika ingin: Quick Scan, Full Scan, Scan Specific Folder dan lakukan scan untuk mengecek file tersembunyi pada suatu direktori, akan kita gunakan opsi “Scan Only This Folder” dan lalu klik Browse Filenya.
- l. Lakukan centang opsi “ignore safe system .....
- m. Pilihlah dan klik "Scan the system for ....”.

### **Percobaan 4: Menyembunyikan file/informasi menggunakan Steganography**

Untuk Menyembunyikan file/informasi menggunakan Steganography pada OS Windows, prosedur praktikum sebagai berikut:

- a. Buka notepad, lalu isi file singkat seperti pada gambar 7.
- b. File disimpan dengan nama Snowfile.txt di folder c:\user\user\desktop\snow\
- c. Ubahan direktori melalui *Command Prompt* dengan mengetikkan perintah Snow -C -m "text to be hide" -p "password" <Sourcefile><Destination.
- d. Buka direktori (file explorer), terlihat ada file baru dengan nama HelloWorld.txt. Buka file tersebut yang memiliki teks yang sama dengan file asli tanpa informasi tersembunyi, file ini dapat dikirim ke target.
- e. Recovering Hidden Information, penerima dapat mengungkapkan informasi dengan menggunakan perintah Snow -C -p "password2121" HelloWorld.txt.
- f. File akan menampilkan informasi tersembunyi di bagian sebelumnya.

### **Percobaan 5: Menghapus Jejak Dengan *Clearing Audit Policies on Windows***

Untuk Menghapus jejak informasi menggunakan *Clearing Audit Policies* pada *OS Windows*, prosedur praktikum sebagai berikut:

- a. Buka OS Windows
- b. Buka command dos (cmd) dengan mode administrator
- c. Ketikkan perintah C:\Windows\system32> auditpol /?
- d. Muncul beberapa perintah dan penjelasan dari masing-masing perintah tersebut.
- e. Perintah yang tersedia diantaranya adalah /?, /get, /set, /list, /backup, /restore, /clear, /remove, /resourceSACL.
- f. Untuk mengaktifkan audit untuk Log masuk Sistem dan Akun, dapat ketikkan perintah berikut C:\Windows\system32>auditpol / set / kategori: "System", "Account logon" / success:enable /failure:enable, lalu enter
- g. Audit diaktifkan, ketikkan C:\Windows\system32>auditpol/get/category: "Account logon","System", lalu enter.
- h. Hapus kebijakan audit dengan mengetikkan perintah berikut C:\Windows\system32>auditpol / clear, tekan enter, selanjutnya ketik Y.
- i. Periksa audit, ketikkan perintah berikut: C:\Windows\system32>auditpol / get / Category: "logon", "System", lalu tekan tombol enter.
- j. Hasil dari perintah tersebut dari dengan category/subkategori berupa sistem dan akun login serta setting dari masing-masing hasil yaitu No Auditing.
- k. Hal ini dikarenakan kebijakan audit telah dihapus, analisa hasilnya.

## VI. Data Percobaan

Setelah semua data diperoleh, maka data hasil pengamatan dan pengujian dimasukkan ke lampiran di bawah ini, sebagai berikut:

### Percobaan 1:

Aplikasi:

- Cirt.net

Output :

3. Capricorn Infotech India - eToken Pro	
User ID	(none)
Password	1234567890
Level	Administrator
Doc	<a href="http://www.isecurity.info/downloads/eToken_Basic_Operation_Guide_1.0.pdf">http://www.isecurity.info/downloads/eToken_Basic_Operation_Guide_1.0.pdf</a>

4. Conceptronic - C100BRS4H	
Method	HTTP
User ID	admin
Password	1234
Level	Administrator
Doc	

5. Draytek - Vigor3300v	
Method	HTTP
User ID	Draytek
Password	1234
Level	Administrator
Doc	

Impact/Indicator:

Pencarian default passwords dan penghapusan kebijakan audit tanpa izin dapat memiliki dampak serius, termasuk potensi akses ilegal ke perangkat, risiko terhadap keamanan jaringan, dan konsekuensi hukum.

Outcomes :

Tujuan percobaan tersebut untuk identifikasi kelemahan keamanan, pengujian



keamanan sistem, menilai kesadaran keamanan, dan memberikan pemahaman tentang praktik keamanan yang baik kepada pengguna atau administrator sistem.

## Percobaan 2:

Aplikasi :

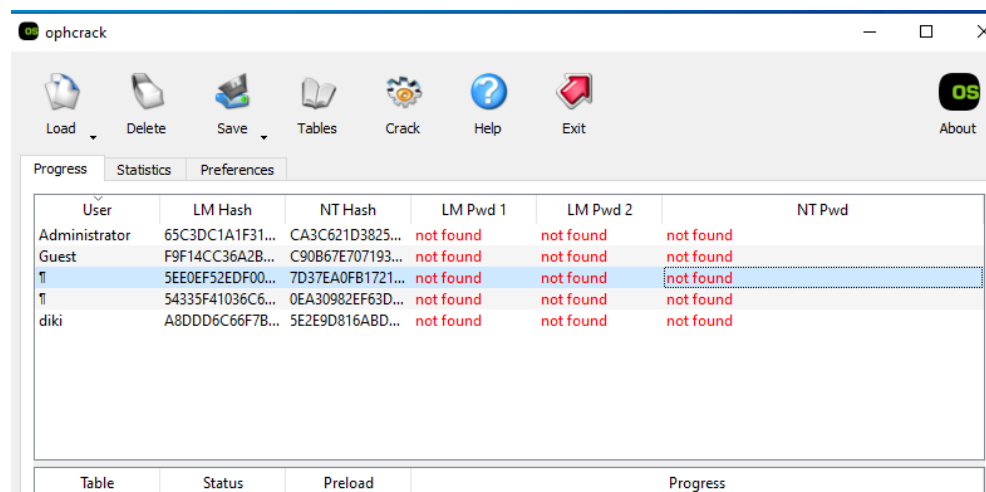
- Pwdump7 dan ophcrack

Output:

```
C:\Users\diki\Downloads\pwdump7 (1)>pwdump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:65C3DC1A1F313AAC27782875ED31DE09:CA3C621D38252C90460DEDF1002BF547:::
Guest:501:F9F14CC36A2B5B47ED21C867AF7122B5:C90B67E707193C4078846829DA41C137:::
j:503:5EE0EF52EDF00F73A16DE4109274472A:7D37EA0FB1721CC34626BF36540E40B6:::
j:504:54335F41036C635164147E496B0BAF4B:0EA30982EF63DE1A12B62D70BD5417A0:::
diki:1001:A8DD6C66F7BE71AFFCA47547891611A:5E2E9D816ABDF6FAA661647D41243A45:::

C:\Users\diki\Downloads\pwdump7 (1)>
```



The screenshot shows the ophcrack application window. It has a menu bar with icons for Load, Delete, Save, Tables, Crack, Help, Exit, and an About button. Below the menu bar are tabs for Progress, Statistics, and Preferences. The main area displays a table with the following data:

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator	65C3DC1A1F31...	CA3C621D3825...	not found	not found	not found
Guest	F9F14CC36A2B...	C90B67E707193...	not found	not found	not found
j	5EE0EF52EDF00...	7D37EA0FB1721...	not found	not found	not found
j	54335F41036C6...	0EA30982EF63D...	not found	not found	not found
diki	A8DD6C66F7B...	5E2E9D816ABD...	not found	not found	not found

At the bottom of the window, there are four buttons: Table, Status, Preload, and Progress.

Impact/Indicator:

Percobaan ini melibatkan tindakan cracking password tanpa izin menggunakan Pwdump7 dan Ophcrack, yang dapat menyebabkan pelanggaran privasi, penggunaan ilegal informasi, pembajakan akun, pelanggaran kebijakan keamanan, kerugian kepercayaan, dan konsekuensi hukum serius.

Outcomes:

Tujuan dari operasi yang dijelaskan dalam percobaan tersebut terlihat merupakan

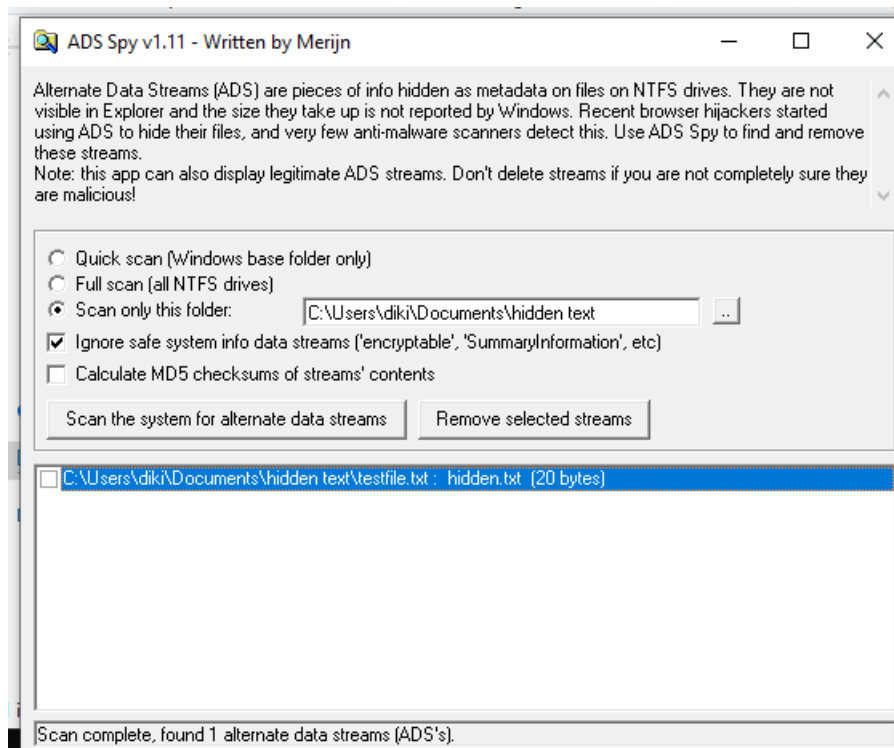
upaya untuk melakukan cracking password dengan menggunakan alat-alat seperti Pwdump7 dan Ophcrack, operasi semacam ini mencoba mendapatkan akses tidak sah ke akun atau sistem dengan mengidentifikasi atau meng-crack password.

### Percobaan 3:

Aplikasi:

- NTFS Stream Manipulation

Output :



Impact/Indicator:

Percobaan ini bertujuan menyembunyikan data menggunakan NTFS Stream Manipulation. Hasilnya melibatkan pembuatan file tersembunyi, perubahan yang tidak terlihat pada ukuran file, ketidakbisaan membaca informasi tersembunyi dengan perintah umum, dan ketidakterlihatan file di File Explorer. Penggunaan utilitas eksternal seperti Spy ADS membantu mendeteksi informasi tersembunyi dari aliran ADS pada sistem NTFS.

Outcomes:

Tujuan dari operasi tersebut adalah untuk menyembunyikan data menggunakan NTFS Stream Manipulation. Ini mungkin dilakukan untuk pengujian keamanan, pendidikan dan pelatihan, serta penelitian keamanan dan forensik digital.

#### **Percobaan 4:**

Aplikasi :

-Snow

Output:

```
C:\Users\dikis\Documents\TUGAS KULIAH SEMESTER 3!!!!\ETHICAL HACKING\snwdos
32>snow -C -m "text to be hidden" -p "password" trkj.txt helloworld.txt
Compressed by 45.59%
Message exceeded available space by approximately 252.38%.
An extra 2 lines were added.
```

```
C:\Users\dikis\Documents\TUGAS KULIAH SEMESTER 3!!!!\ETHICAL HACKING\snwdos
32>Snow -C -p "password" helloworld.txt
text to be hidden
```

Impact/Indicator:

Percobaan ini menggunakan Steganography dengan aplikasi Snow untuk menyembunyikan informasi dalam file teks. Langkah-langkah melibatkan pembuatan file tersembunyi, perubahan direktori melalui Command Prompt, dan penggunaan perintah Snow untuk proses penyembunyian dan pengungkapan.

Outcomes:

Tujuan dari operasi tersebut adalah untuk menguji dan memahami penggunaan teknik Steganography. Percobaan ini mencakup pembuatan file tersembunyi, demonstrasi langkah-langkah proses steganography, dan menyoroti pentingnya keamanan informasi. Penggunaan Steganography dalam konteks ini dimaksudkan untuk menunjukkan cara menyampaikan pesan rahasia atau informasi sensitif tanpa menarik perhatian yang tidak diinginkan.

## Percobaan 5:

Aplikasi :

- Cmd

Output:

```
C:\Windows\system32>auditpol /set /subcategory:"Logon" /success:enable /failure:enable
The command was successfully executed.

C:\Windows\system32>auditpol /get /subcategory:"Logon"
System audit policy
Category/Subcategory          Setting
Logon/Logoff
  Logon                        Success and Failure

C:\Windows\system32>auditpol /clear
Are you sure (Press N to cancel or any other key to continue)?y
The command was successfully executed.

C:\Windows\system32>auditpol /get /subcategory:"Logon"
System audit policy
Category/Subcategory          Setting
Logon/Logoff
  Logon                        No Auditing
```

Impact/Indicator:

Percobaan ini bertujuan menghapus jejak informasi dengan membersihkan kebijakan audit pada Windows. Hasilnya, kebijakan audit untuk kategori "System" dan "Account Logon" diaktifkan, lalu dihapus. Dampaknya adalah sistem tidak lagi merekam jejak log masuk dan aktivitas sistem terkait.

Outcomes:

Tujuan utama mungkin mencakup menghindari deteksi atau menyembunyikan jejak aktivitas yang relevan dari pemantauan keamanan.

## VII. Analisa dan Kesimpulan

### Percobaan 1: Online Tool for Default Passwords

- Analisa:
  - Menggunakan alat online untuk mencari kata sandi default perangkat.
  - Melibatkan pilihan manufaktur perangkat untuk menampilkan kata sandi default.
- Kesimpulan:
  - Tindakan ini menunjukkan potensi risiko keamanan jika kata sandi default tidak diubah, memudahkan akses tanpa izin.

### Percobaan 2: Password Cracking menggunakan Pwdump7 & Ophcrack Tool

- Analisa:
  - Penggunaan alat untuk mendapatkan dan mencrack password dari hash.
  - Melibatkan Pwdump7 dan Ophcrack tool.
- Kesimpulan:
  - Demonstrasi risiko keamanan terhadap password lemah atau rentan terhadap teknik cracking.

### Percobaan 3: Menyembunyikan Data menggunakan NTFS Stream Manipulation

- Analisa:
  - Menyembunyikan data dalam aliran NTFS (ADS).
  - Penggunaan perintah CMD dan alat deteksi stream tersembunyi.
- Kesimpulan:
  - Menunjukkan potensi risiko penyembunyian data, yang dapat dimanfaatkan untuk tujuan tidak etis.

### Percobaan 4: Menyembunyikan File/Informasi menggunakan Steganography

- Analisa:
  - Menggunakan Steganography untuk menyembunyikan informasi dalam file.
  - Melibatkan penggunaan perintah Snow untuk menyembunyikan dan mengungkapkan informasi.
- Kesimpulan:
  - Menunjukkan cara menyembunyikan data sensitif, potensial untuk penggunaan baik atau buruk.

### Percobaan 5: Menghapus Jejak dengan Clearing Audit Policies on Windows

- Analisa:
  - Menghapus kebijakan audit untuk menghindari pemantauan.
  - Melibatkan perintah auditpol di Command Prompt.
- Kesimpulan:
  - Menunjukkan tindakan yang dapat digunakan untuk menghilangkan jejak aktivitas, yang dapat menciptakan celah keamanan.

### Kesimpulan Umum:

Praktikum ini membahas beberapa teknik yang dapat dimanfaatkan untuk tujuan peretasan dan menyadarkan tentang potensi risiko keamanan. Penting untuk menggunakan pengetahuan ini secara etis dan memahami bagaimana melindungi sistem dari potensi serangan. Kesadaran keamanan dan penerapan praktik keamanan yang baik sangat penting dalam menjaga integritas sistem dan data.

### **VIII. Daftar Pustaka**

Kurniawan, Agus. (2012). *Network Forensics – Panduan Analisis & Investigasi Paket Data Jaringan Menggunakan Wireshark*. Yogyakarta: ANDI

Mitchell, John. (2015), “*Computer and Networ Security*”, Spring

Saeed, A., Khan, Nouman Ahmed, Yousuf, M. (2018), *CEH v10: EC-Council Certified Ethical Hacker Complete Training Guide with Practice Labs*, Vol. 10, United Kingdom, IPSpecialis LTD.