

# **LAPORAN PRAKTIKUM**

## **FOOTPRINTING & RECONNAISSANCE**



### **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 : Footprinting & Reconnaissance  
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

**LABORATORIUM: JARINGAN DAN MULTIMEDIA  
POLITEKNIK NEGERI LHOKSEUMAWE  
PENGUJIAN: FOOTPRINTING & RECONNAISSANCE**

**I. Capaian Praktikum/Kompetensi**

Setelah mengikuti praktikum *Footprinting & Reconnaissance*, diharapkan praktikan dapat:

1. Mahasiswa mampu mengetahui pengumpulan informasi (sistem, jaringan, organisasi) untuk keperluan keselamatan
2. Mahasiswa mampu mencari kelemahan-kelemahan sistem keamanan jaringan untuk mendukung persyaratan jaringan bisnis skala kecil hingga menengah
3. Mahasiswa mampu mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem keamanan yang berbasis informasi.
4. Mahasiswa mampu merekomendasikan kelemahan keamanan jaringan sesuai dengan kebutuhan pengguna jaringan komputer

**II. Keselamatan Kerja**

Praktikum *Footprinting & Reconnaissance* 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**

Keamanan komputer (bahasa Inggris: *computer security*) atau dikenal juga dengan sebutan *cybersecurity* atau IT security adalah keamanan informasi yang diaplikasikan kepada komputer dan jaringannya. Dalam pencarian jejak seorang penyerang yang telah berhasil mengumpulkan informasi merupakan sebuah seni

dari keselamatan dan keamanan dari dalam maupun dari luaran sistem. Pengumpulan informasi akan membantu mengatasi kelemahan dalam sebuah sistem, penyerang akan mengeksploitasi sistem agar dapat diakses. *Reconnaissance* adalah sebuah fase persiapan sebelum (*attacker*) melakukan penyerangan, dimana kegiatan intinya adalah mengumpulkan informasi sebanyak mungkin mengenai sasaran. Untuk menyusun strategi apa yang ditemukan (*blueprint* dari suatu jaringan), sehingga hacker akan mendapatkan gambaran yang jelas tentang sistem keamanan yang dimiliki target.

Sedangkan *Footprinting* adalah segala kegiatan mengumpulkan informasi target yang akan di-hack sistemnya, sebelum melakukan penguasaan sistem sesungguhnya. Informasi yang ditampilkan dari hasil kegiatan ini adalah berupa *network target*: TCP (*Transmission Control Protocol*) / IP (*Internet Protocol*).

#### IV. Alat dan Bahan


Berikut ini merupakan alat dan bahan yang digunakan pada pelaksanaan praktikum *Footprinting & Reconnaissance*, adalah sebagai berikut:

1. OS Server (Windows, Kali Linux)
2. OS Client (Windows XP/7/8/10)
3. Tools Software (Java 8, Maltego, Recong-ng, FOCA, Cmd, HTTrack, Metasploit).

#### V. Prosedur Praktikum

##### Percobaan 1: Pencarian informasi menggunakan *Maltego Tool Overview*

Dalam keamanan sistem menggunakan aplikasi *maltego*, prosedur praktikum sebagai berikut:

- a. Siapkan alat dan bahan yang digunakan dan pastikan *VMWare* sudah terinstall
- b. Pastikan semua sistem operasi sudah terinstall dalam *VMWare* dan Java versi 8, link: [https://java.com/en/download/help/windows\\_manual\\_download.xml](https://java.com/en/download/help/windows_manual_download.xml)
- c. Kemudian lakukan instal software *Maltego* (<https://www.paterva.com>)
- d. Jalankan aplikasi *maltego* yang telah diinstall di komputernya masing-masing.
- e. Pada laman utama *Maltego Community Edition (CE)*. Pada bagian atas, Klik ikon graf baru  untuk konfigurasi perangkat yang terhubung.

- f. Kemudian pilih *Entity Palette* muncul beberapa menu dari aplikasi *maltego*, mis: tambahkan domain dari *Entity Palette* dengan cara di Drag.
- g. Ubah *Domain* dan klik kanan pada Ikon domain lalu pilih opsi *Run Transform*, setelah dipilih opsi satu persatu (*All Transform*, *DNS from Domain*, *Domain Owner details*, *Email Addresses from Domain* dan *Files and Documents from Domain*) lalu amati dan analisa hasil yang akan ditampilkan.

### **Percobaan 2: Pencarian informasi menggunakan Recon-ng Overview**

Dalam keamanan sistem menggunakan sistem operasi *Kali Linux* dan *Recon-ng*, prosedur praktikum sebagai berikut:

- a. *Login* sebagai *root* pada *OS Kali Linux*, lalu jalankan *command terminal*, dan buka aplikasi *tools* ketik *Recon-ng* pada terminal, lalu tekan tombol *enter*.
- b. Maka akan muncul tampilan Awal *Recon-ng* sesuai versinya ditampilkan.
- c. Masukkan perintah command " *show modules* ".

Setelah itu ketikkan *Search Netcraft* pada *command interface* lalu tekan tombol *enter* yang berfungsi untuk mencari entitas/direktori *netcraft* dalam modules.

- d. Selanjutnya ketikkan "*use recon/domainhosts/Netcraft*" dan tekan tombol *enter*.
- e. Ketikkan "*show option*" maka dihasilkan tampilan pengaturan *netcraft* berupa *name*, *current value* yang bernilai *default*, *required*, dan sedikit deskripsi.
- f. Aturlah *source* dengan perintah "*set source [domain]*", contoh "*set source google.com*", lalu tekan tombol *enter* lanjutkan perintah "*Run*" setelah itu *enter*.
- g. Silakan amati tampilan yang dihasilkan dalam pencarian target.

### **Percobaan 3: Pencarian informasi menggunakan FOCA Tool**

Dalam pencarian informasi tersembunyi lainnya dapat ditemukan di halaman web menggunakan aplikasi *Fingerprinting Organisations with Collected Archives* (*FOCA*) Tools, prosedur praktikum sebagai berikut:

- a. Install dan jalankan aplikasi *FOCA*
- b. Kemudian buka lembar untuk membuat project baru (Project ~ New Project)
- c. Selanjutnya inputkan *project name*, *domain website* yang ingin dilacak, alternative domain, memilih direktori penyimpanan dokumen serta *note project*.
- d. Jika sudah selesai input, maka untuk memulai dapat dipilih/klik tombol "*Create*"

- e. Selanjutnya pilih menggunakan tombol *check list* lebih dari satu jenis *search engine* dan juga untuk jenis ekstensi yang diinginkan.
- f. Setelah klik *search*, gunakan domain [www.google.com](http://www.google.com) akan menghasilkan 98 file dokumen dengan ekstensi yang berbeda-beda. File tersebut dapat disimpan dengan klik kanan pada mouse, lalu memilih “*Download*”.

#### **Percobaan 4: Mendapatkan informasi menggunakan *Command Line Windows***

Dalam pencarian informasi tersembunyi lainnya mengenai target menggunakan aplikasi *Command Line Utility Windows*, prosedur praktikum sebagai berikut:

- a. Jalankan windows, lalu klik *Command Line Utility*
- b. Lakukan ping ke domain *example.com*.
- c. Lakukan pemeriksaan nilai fragmentasi yang diperlukan 1500 (mis. ping *example.com -f -l -1500*).
- d. Lakukan pemeriksaan nilai fragmentasi yang diperlukan dibawah 1500 (mis. Ping *Example.com -f -l -1400*)
- e. Tampilan setelah dilakukan pelacakan terhadap target yaitu *example.com* dengan menggunakan *tracert* (mis. *Tracert example.com*).

#### **Percobaan 5: Mendapatkan informasi menggunakan *Mebsite Copier tool (HTTrack)***

Untuk mendapatkan informasi bisa dilakukan dengan cara mem-back-up (*mendownload*) semua isi web atau blog menggunakan aplikasi *WinHTtrack (HTTrack di Windows)*, prosedur praktikum sebagai berikut:

- a. Install aplikasi *HTTrack* sampai finish, untuk versi windows silakan *download link*: <http://download.httrack.com/csery.php3?File=httrack.exe>
- b. Jalankan *WinHTTrack Website Copier* (Klik *Start – Program – Winhttrack – WinHTTrack Website Copier*), lalu klik *Next*
- c. Isikan Nama Proyek di *Project Name* (terserah saja namanya)
- d. Biarkan mengikuti standar penyimpanan proyek tersebut di *C:\My Web sites*, boleh diganti di folder lain, kemudian klik *Next*
- e. Atur konfigurasi target, pada *mirror mode* anda isikan alamat URL weblog yg akan dikopi di kotak *URL*. Kemudian tentukan *Action* atau pilih default saja.

- f. Lakukan setting limits dengan mengklik *Set option*, tujuannya agar apa yang kita unduh terbatas pada web, jika tidak dibatasi semua terunduh dan akhirnya bisa gak selesai-selesai. Untuk *maximum mirroring depth*, isikan 10 saja, kemudian pada *Maximum external depth* isikan 0 saja, agar link keluar web yang kita ingin unduh tidak turut terunduh. Max transfer rate isikan sebanyak-banyaknya sesuai bandwidth yang kita gunakan, kemudian klik tombol *Ok*.
- g. Klik *Next*.
- h. Klik *Finish*.

### **Percobaan 6: Mendapatkan informasi menggunakan Metasploit Framework**

Untuk mengumpulkan lebih banyak informasi mengenai target di dalam jaringan menggunakan aplikasi *Metasploit Framework* pada *OS Kali Linux*, prosedur praktikum sebagai berikut:

- a. Siapkan sebuah komputer sebagai penyerang!
- b. Unduh Metasploit Framework (<https://www.metasploit.com/download>)
- c. Buka *OS Kali Linux* dan jalankan *Metasploit Framework*
- d. Dengan menggunakan command interface kali linux, ketikkan *db\_status*
- e. Lakukan scan ping keseluruhan subnet 10.10.50/24 (IP sesuaikan) dengan perintah command *nmap -Pn -sS -A -oX Test 10.10.50.0/24*
- f. Untuk mengimport data host pada database, gunakan perintah “*db\_import Test*”.
- g. Jalankan *service scan*, ketik perintah command “*db\_nmap -sS -A 10.10.50.221*”.
- h. Lihat service yang tersedia, gunakan perintah command “*Services*”
- i. Ketikan command “*use scanner/smb/smb\_version*”
- j. Lakukan *scanning host/target* dengan perintah command “*run*” dan “*hosts*”, hasil yang tampil alamat ip, nama sistem operasi, dan informasi lainnya.

## VI. Data Percobaan

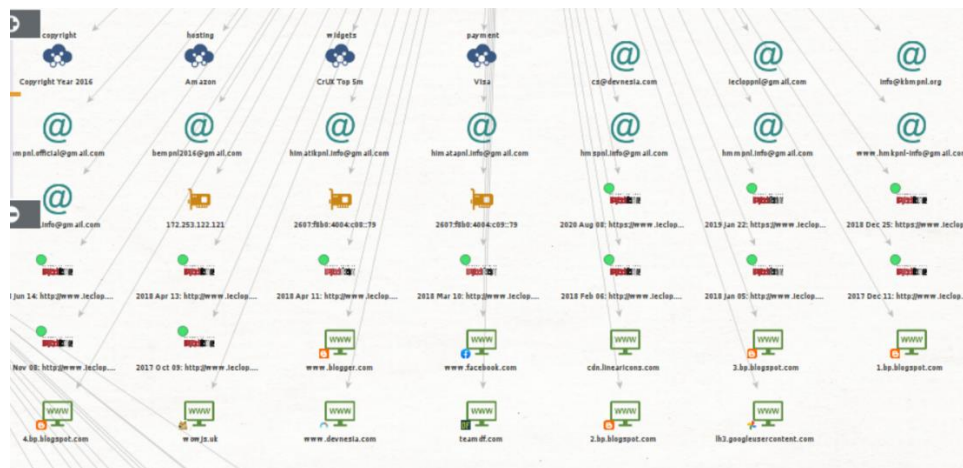
Setelah semua data diperoleh, maka data hasil pengamatan dan pengujian dimasukkan ke dalam tabel, sebagai berikut:

### Percobaan 1:

*Aplikasi :*

Maltego

*Output:*





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

Dalam melakukan percobaan dengan Maltego, dampaknya adalah memahami jejak digital, menganalisis keamanan, dan mendukung penelitian keamanan serta pengujian penetrasi.

### ***Outcomes:***

Manfaat dari penggunaan software Maltego mencakup analisis keamanan siber, investigasi forensik, intelijen bisnis, analisis jejak digital, manajemen risiko, penelitian keamanan, dan penelitian terbuka.

## **Percobaan 2:**

### ***Aplikasi:***

Recon-ng

### ***Output:***

```
[recon-ng][test] > modules load recon/domains-hosts/netcraft
[recon-ng][test][netcraft] > options set SOURCE google.com
SOURCE => google.com
[recon-ng][test][netcraft] > run

-----
GOOGLE.COM
-----
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=google.com
[*] No results found.
[recon-ng][test][netcraft] > █
```

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

Dalam melakukan percobaan dengan Kali Linux dan Recon-ng, dampaknya adalah menjelajahi entitas terkait Netcraft pada domain target, mengidentifikasi potensi kerentanan, dan mendukung pengujian keamanan.

### ***Outcomes:***

Dalam percobaan dengan Kali Linux dan Recon-ng, manfaatnya adalah mendapatkan informasi terkait target, analisis keamanan, pengujian penetrasi, pengumpulan intelijen keamanan, dan manajemen keamanan.

### **Percobaan 3:**

#### ***Aplikasi:***

FOCA

#### ***Output:***

Id	Type	URL	Download	Download Date	Size	Meta
0		https://ojs.unimal.ac.id/na/article/download/4920/pdf	✗	-	-	✗
1		https://ojs.unimal.ac.id/jspm/issue/download/308/pdf_1	✗	-	-	✗
2		https://ojs.unimal.ac.id/na/article/download/4925/pdf	✗	-	-	✗
3	pdf	https://fk.unimal.ac.id/wp-content/uploads/2022/01/PA...	✗	-	-	✗
4	pdf	https://ilmupolitik.fisip.unimal.ac.id/dokumen/89355529....	✗	-	1,21 MB	✗
5	pdf	https://fisip.unimal.ac.id/images/EBOOK_Buku_-_PAND...	✗	-	2,85 MB	✗
6		https://ojs.unimal.ac.id/jimfh/article/download/4261/pdf	✗	-	-	✗
7	pdf	https://material.unimal.ac.id/dokumen/teknikunimal-122...	●	09/19/2023 14:40:16	800.78 KB	✗
8		https://ojs.unimal.ac.id/agrium/article/download/2349/1...	✗	-	-	✗
9		https://ojs.unimal.ac.id/cejs/article/download/3528/pdf	✗	-	-	✗
10		https://ojs.unimal.ac.id/jimfh/article/download/6346/pdf	✗	-	-	✗

Time	Source	Severity	Message
14:40:02	FingerPrinting	debug	HTTP FingerPrinting on https://tm.unimal.ac.id:443
14:40:16	MetadataSearch	low	Downloaded document: https://material.unimal.ac.id/dokumen/teknikunimal-12240-buku-pa
14:40:16	MetadataSearch	debug	All documents have been downloaded
14:40:16	MetadataSearch	debug	All documents have been downloaded

Settings Deactivate AutoScroll Clear Save log to File

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

Dalam percobaan dengan FOCA Tools, dampaknya adalah mengumpulkan informasi terkait domain target, memahami jejak digital, dan mendukung analisis keamanan.

### ***Outcomes:***

Manfaat dari percobaan dengan FOCA adalah pemetaan organisasi, pengumpulan informasi tersembunyi, analisis informasi, dan pengumpulan data yang dapat digunakan untuk analisis keamanan siber. Penggunaan harus etis dan sesuai hukum, serta menjaga privasi dan hak cipta.

### **Percobaan 4:**

#### ***Aplikasi:***

CMD

#### ***Output:***

```
Command Prompt
Approximate round trip times in milli-seconds:
  Minimum = 195ms, Maximum = 393ms, Average = 259ms
C:\Users\dikic>Tracert example.com

Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  10.0.2.2
  1  299 ms  44 ms  41 ms  192.168.110.1
  2   8 ms   9 ms  17 ms  196.97.customer.permananet-as131746 [103.248.196.97]
  3  39 ms  76 ms 107 ms  10.40.1.49
  4  21 ms  47 ms  65 ms  196.5.customer.permananet-as131746 [103.248.196.5]
  5  54 ms  48 ms  95 ms  36.91.237.125
  6   *    21 ms  *    180.240.193.93
  7   *    *    *    Request timed out.
  8  68 ms  46 ms  48 ms  180.240.204.70
  9   *    *    22 ms  snge-b5-link.ip.twelve99.net [62.115.162.250]
 10 195 ms 196 ms 196 ms  sjo-b23-link.ip.twelve99.net [62.115.141.126]
 11 193 ms 202 ms 196 ms  edgio-ic-325098.ip.twelve99-cust.net [62.115.155.87]
 12 196 ms 204 ms 203 ms  ae-65.core1.sab.edgecastcdn.net [152.195.84.131]
 13 194 ms 195 ms 203 ms  93.184.216.34
 14

Trace complete.
C:\Users\dikic>
```

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

Dalam melakukan percobaan ini, dampaknya adalah mendapatkan informasi jaringan dan fragmentasi data dari domain target (example.com) serta pemahaman jalur data melalui jaringan.

### ***Outcomes:***

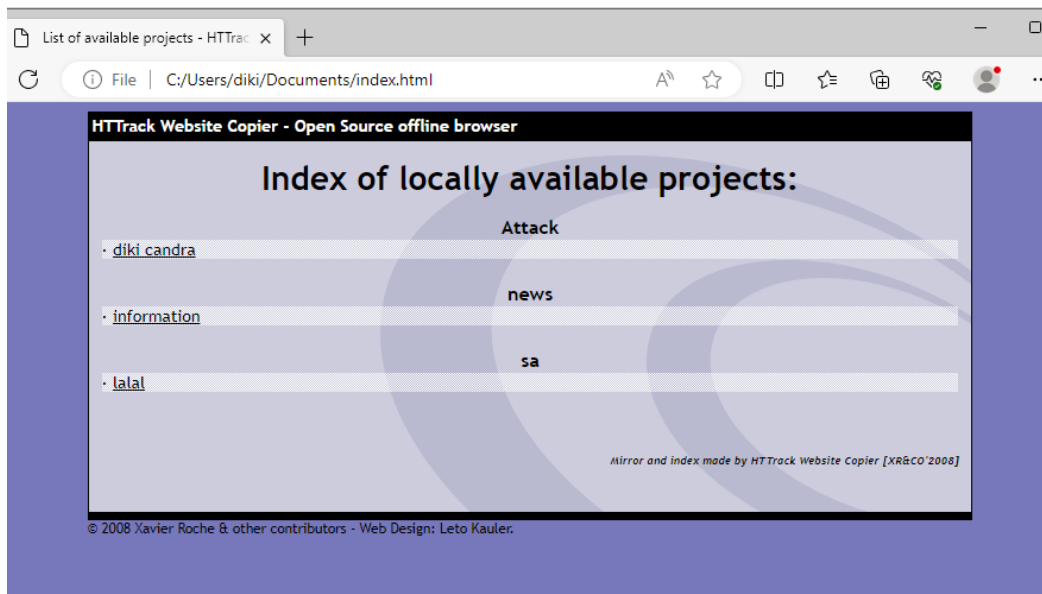
Melakukan percobaan ini membantu Anda memahami penggunaan Command Line Windows, mengukur konektivitas dan latensi jaringan melalui ping, memahami fragmentasi paket data, serta melacak rute data ke target (traceroute). Ini mengembangkan keterampilan administrasi sistem, analisis jaringan, dan penelitian keamanan.

### **Percobaan 5:**

#### ***Aplikasi:***

HTTrack

#### ***Output:***



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

Dalam percobaan dengan WinHTTrack (HTTrack), dampaknya adalah pengunduhan lengkap isi situs web atau blog, penyimpanan lokal, dan penyediaan cadangan situs.

### ***Outcomes:***

Manfaat dari percobaan dengan WinHTTrack (HTTrack) adalah dapat mencadangkan dan menyimpan isi situs web atau blog untuk keperluan penelitian, akses offline, dan pemeliharaan konten. Dapat membantu pemahaman struktur situs web dan melindungi dari perubahan konten.

## **Percobaan 6:**

### ***Aplikasi:***

Metasploit

### ***Output:***

```
msf6 auxiliary(scanner/smb/smb_version) > hosts

Hosts
=====
address      mac      name      os_name  os_flavor  os_sp  purpose  info  comments
-----
10.0.2.15    10.0.2.15  Unknown  device
```

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

Dalam percobaan dengan Metasploit Framework pada Kali Linux, dampaknya adalah pengumpulan informasi lebih lanjut tentang target, pemindaian jaringan, dan analisis keamanan.

### ***Outcomes:***

Manfaat dari percobaan dengan Metasploit Framework adalah pengumpulan informasi, analisis keamanan, penelitian keamanan, dan pengujian penetrasi yang membantu dalam pemahaman dan identifikasi kerentanan target.

## VII. Analisa dan Kesimpulan

Percobaan Footprinting & Reconnaissance ini melibatkan pengumpulan informasi terkait target dalam jaringan. Langkah-langkah mencakup pengenalan target, penggunaan Metasploit Framework, scanning menggunakan Nmap, import data host, scanning service, dan penggunaan modul Metasploit. Hasilnya memberikan pemahaman tentang sistem operasi, layanan, dan alamat IP yang berjalan pada host. Penting untuk selalu mengikuti etika, hukum, dan perizinan yang sesuai.

## 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.

## **VII. Analisa dan Kesimpulan**

Percobaan Footprinting & Reconnaissance ini melibatkan pengumpulan informasi terkait target dalam jaringan. Langkah-langkah mencakup pengenalan target, penggunaan Metasploit Framework, scanning menggunakan Nmap, import data host, scanning service, dan penggunaan modul Metasploit. Hasilnya memberikan pemahaman tentang sistem operasi, layanan, dan alamat IP yang berjalan pada host. Penting untuk selalu mengikuti etika, hukum, dan perizinan yang sesuai.

## **VIII. Daftar Pustaka**

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

Mitchell, John. (2015), “*Computer and Network 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.