Implementasi dan Analisis *Attack Tree* pada *Vulnerable Machine* Hackable 2 Berdasarkan *Time Metric, Cost Metric,* dan *Frequency Metric*

1st M. Zaelani Sidiq
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
mzaelanis@student.telkomuniversity.ac.id

2nd Adityas Widjajarto
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
adtwjrt@telkomuniversity.ac.id

3rd M. Teguh Kurniawan
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
teguhkurniawan@telkomuniversity.ac.id

***Abstrak*—Penelitian ini bertujuan untuk melakukan analisis bagaimana implementasi attack tree terhadap vulnerable machine Hackable 2 berdasarkan time metric, cost metric, dan frequency metric yang menghasilkan nilai untuk dilakukan pemeringkatan, sehingga dapat mengetahui jalur tercepat untuk mengakses root target. Metode yang digunakan pada penelitian ini adalah pengujian eksploitasi berdasarkan walkthrough dan melakukan visualisasi menggunakan attack tree dengan pendekatan SAND gate. Hasil yang diperoleh dari seluruh tahapan eksploitasi pada vulnerable machine Hackable 2 adalah, berhasil mengakses root target. Seluruh tahapan yang dilakukan pada walkthrough dapat digambarkan dengan activity diagram dan alur data yang terjadi digambarkan dengan data flow diagram. Penggunaan attack tree, dapat mewakili seluruh tahapan eksploitasi berdasarkan walkthrough untuk dilakukan pemeringkatan berdasarkan metrics. Pemeringkatan berdasakan time metric menghasilkan attack tree wt 1 sebagai jalur tercepat dengan real time sebesar 718,52 detik. Seluruh attack tree memiliki nilai cost metric yang sama yaitu 29 langkah. Berdasarkan frequency metric, tools utama pada penelitian ini adalah Nmap dan Netcat yang digunakan pada seluruh walkthrough, dan tools yang paling efektif adalah Netdiscover, Nmap, Gobuster, dan Netcat.**

Kata kunci: **attack tree, metrics, hackable 2**

I. PENDAHULUAN

Peningkatan serangan siber semakin berkembang pesat. Perusahaan, organisasi, hingga individu memerlukan banyak sumber daya untuk melawan peretas dan menjamin keamanan sistem. Namun, kerentanan baru masih terus ditemukan. Maka eksploitasi merupakan cara terbaik untuk melindungi diri dari serangan siber [1]. Eksploitasi dapat membantu untuk melakukan identifikasi kerentanan pada sistem sebelum peretas melakukan eksploitasi terhadap sistem, sehingga dapat melindungi berbagai sumber daya yang terdapat pada sistem. Metode yang dapat digunakan untuk melakukan eksplotasi dengan waktu dan biaya yang terjangkau adalah dengan menggunakan *vulnerable machine*, kemudian melakukan analisis berdasarkan hasil eksploitasi yang dilakukan dengan menggunakan *attack tree*.

Attack tree merupakan model keamanan yang digunakan untuk memberikan gambaran secara visual terhadap serangkaian langkah yang perlu dilakukan oleh penyerang dengan tujuan untuk mengambil alih suatu sistem atau jaringan komputer. Pada *attack tree* setiap langkah serangan yang dilakukan, digambarkan sebagai simpul atau *node* dengan menggunakan struktur pohon dan menghasilkan nilai yang bisa dihitung menggunakan *metrics*. *Metrics* merupakan sebuah nilai yang digunakan untuk menggambarkan karakteristik atau sifat dari simpul pada *attack tree* seperti waktu, biaya, frekuensi, probabilitas keberhasilan serangan, tingkat kesulitan dalam melakukan serangan, peralatan khusus yang dibutuhkan dalam serangan, hingga kombinasi dari semua metrik tersebut. Penggunaan *metrics* dapat membantu untuk mengevaluasi risiko eksploitasi sistem secara lebih rinci dan objektif [2]. Hasil perhitungan *metrics* dapat digunakan sebagai dasar untuk memberikan peringkat pada *attack tree*. Dengan memberikan peringkat terhadap *attack tree*, dapat dilakukan identifikasi pada simpul-simpul yang paling rentan dan menentukan prioritas tindakan pencegahan untuk melindungi sistem dari serangan siber.

Penelitian ini berfokus pada implementasi dan analisis *attack tree* pada *vulnerable machine* Hackable 2 dengan menggunakan *time metric, cost metric,* dan *frequency metric*. Pada penelitian ini, menggunakan sebuah *vulnerable machine* bernama Hackable 2 sebagai objek untuk melakukan eksploitasi terhadap kerentanan. *Vulnerable machine* Hackable 2 merupakan sebuah sistem operasi berbasis Linux yang dirancang khusus oleh Elias Sousa pada tanggal 15 Juni 2021 sebagai sarana latihan untuk mengembangkan keterampilan serta wawasan mengenai penetrasi pada sistem atau jaringan komputer.

II. KAJIAN TEORI

A. Keamanan Sistem Informasi

Keamanan sistem informasi merupakan tindakan yang melibatkan langkah-langkah untuk mencegah upaya peretasan dari pengguna komputer, mengawasi akses jaringan yang tidak sah, serta mendeteksi aktivitas gangguan yang tak terdeteksi oleh sistem [3]. Berdasarkan [4], dalam pengelolaan serta pengendalian keamanan sistem informasi, perlu diperhatikan tiga elemen pokok keamanan informasi yang sering disebut sebagai CIA (*Confidentiality, Integrity, Availability*).

B. *Threat*/Ancaman

Ancaman merujuk pada peristiwa baru atau yang belum teridentifikasi yang memiliki potensi untuk merusak integritas keseluruhan sistem atau organisasi. Terdapat tiga kategori utama dari ancaman, mencakup ancaman alam, ancaman yang tidak disengaja seperti kesalahan akses informasi, serta ancaman yang disengaja seperti *spyware,*

malware, atau tindakan karyawan yang bertujuan merugikan [5] Dengan demikian, ancaman merupakan peristiwa yang bisa menimbulkan risiko pada sistem, dibagi menjadi tiga jenis, yakni ancaman alam, tidak disengaja, dan disengaja.

C. Eksploitasi

Eksplotasi merupakan metode yang digunakan dalam melakukan penetrasi serta mengakibatkan kerusakan pada sistem. Istilah ini bisa berupa kata kerja atau kata benda. Pelaku ancaman dapat berusaha untuk mengeksploitasi sistem atau aset informasi lain secara ilegal untuk keuntungan pribadi [6]. Dengan demikian, eksplotasi merupakan tindakan untuk merusak sistem dengan menggunakan kerentanan secara ilegal oleh pelaku ancaman demi kepentingan pribadi.

D. Kali Linux

Kali Linux adalah *software open-source* yang dirancang khusus untuk tujuan eksploitasi profesional dan evaluasi keamanan [7]. Kali Linux juga menyediakan berbagai alat untuk mendeteksi serta mengatasi kerentanan dalam sistem. Pengembangan Kali Linux dilakukan oleh *Offensive Security*. Pada penelitian ini Kali linux digunakan sebagai alat penyerangan.

E. *Vulnerable machine* Hackable 2

Pada penelitian ini, menggunakan sebuah *vulnerable machine* bernama Hackable 2 sebagai objek untuk melakukan eksperimen eksploitasi terhadap kerentanan. *Vulnerable machine* Hackable 2 merupakan sebuah sistem operasi berbasis Linux yang dirancang khusus oleh Elias Sousa pada tanggal 15 Juni 2021 sebagai sarana latihan untuk mengembangkan keterampilan serta wawasan mengenai penetrasi pada sistem atau jaringan komputer. Hackable 2 menyediakan lingkungan yang aman untuk menguji alat-alat keamanan dan strategi pertahanan.

F. Eksperimen

Metode eksperimen dalam ilmu merujuk pada cara yang diterapkan oleh peneliti guna mengidentidikasi hubungan atau dampak di antara beragam variabel di dalam lingkungan yang ketat dalam pengawasan. Metode penelitian eksperimen memerlukan perhatian khusus, terutama dalam penelitian yang melibatkan pengembangan perangkat lunak ataupun perangkat keras [8]. Dengan demikian, dapat diartikan bahwa eksperimen adalah proses yang memberikan pemahaman mengenai hubungan antara variabel pada suatu lingkungan yang terkendali.

G. Walkthrough

Walkthrough adalah serangkaian tindakan atau langkah-langkah yang dijalankan dengan tujuan untuk menguji, memahami, atau mengevaluasi sistem, perangkat lunak, atau prosedur tertentu, untuk mengidentifikasi masalah [9]. Dalam konteks penelitian ini, *walkthrough* adalah langkah-langkah yang diprakarsai oleh ahli untuk melakukan penetrasi atau serangan pada *vulnerable machine* Hackable 2, dengan tujuan mencapai *privileged environment access* atau hak akses root.

H. Activity Diagram

Activity Diagram merupakan salah satu representasi perilaku dalam notasi UML yang sangat berguna dalam menguji sistem, karena mampu menggambarkan urutan sistem secara keseluruhan [10]. Diagram ini mengilustrasikan visual mengenai langkah-langkah, keputusan, dan aktivitas yang terlibat dalam suatu proses. Umumnya digunakan untuk merepresentasikan alur kerja bisnis, proses sistem, atau situasi pengujian dalam pengembangan perangkat lunak.

I. Data Flow Diagram

Data flow diagram adalah metode yang mengilustrasikan elemen-elemen sistem serta pergerakan data di antara elemen-elemen tersebut, termasuk sumber, tujuan, dan penyimpanan data [11]. Dalam penelitian ini, *data flow diagram* sendiri menggambarkan bagaimana pergerakan data, sumber, serta tujuan yang terjadi ketika menjalankan masing-masing dari lima *walkthrough* yang telah dipilih.

J. *Attack tree*

Struktur serangan (*attack tree*) adalah sebuah format untuk mengkaji ancaman, menilai serangan yang berpotensi merugikan, serta membantu ahli keamanan melihat dari sudut pandang penyerang untuk menemukan kerentanan dalam sistem [12]. Karena itu, menggunakan *attack tree* memberikan banyak manfaat, termasuk mendukung analisis ancaman, penilaian serangan, serta memungkinkan pemahaman dari perspektif penyerang.

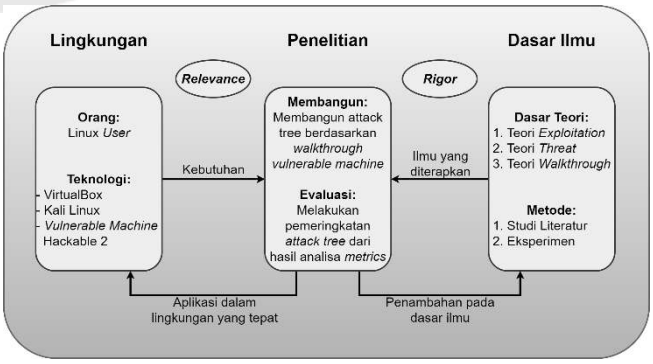
K. *Metrics*

Metrics merujuk pada nilai yang terdapat dalam bagian struktur serangan yang nantinya akan dihitung. Tujuan perhitungan pada penelitian ini adalah untuk dijadikan sebagai dasar pemeringkatan *attack tree*. Terdapat berbagai jenis *Metrics* yang dapat digunakan [2], meskipun dalam penelitian ini hanya tiga jenis *metrics* yang digunakan yaitu *time metric, cost metric, frequency metric*.

III. METODE

A. Model Konseptual

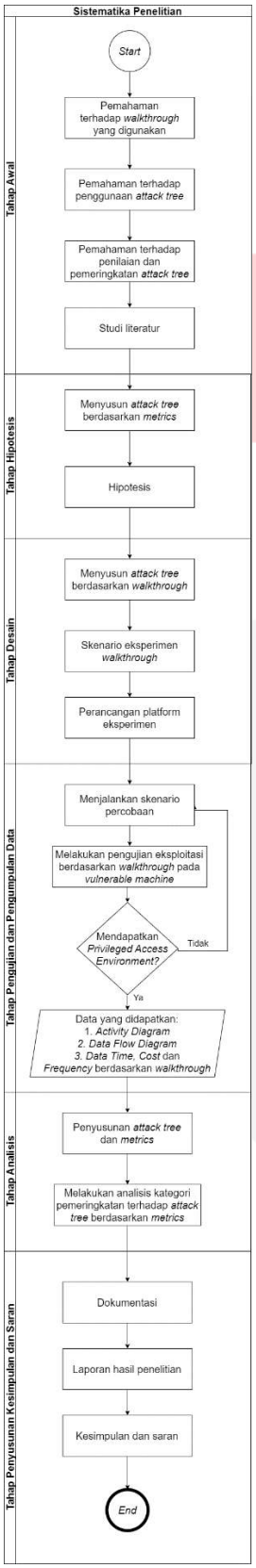
Kerangka atau model konseptual merupakan sebuah alur pemikiran pada suatu hubungan antara konsep satu dengan konsep lainnya dengan tujuan memberikan gambaran serta panduan terhadap asumsi yang berkaitan dengan variabel yang akan diteliti. Berikut ini merupakan model konseptual yang digunakan pada penelitian ini.



GAMBAR III.1
MODEL KONSEPTUAL

B. Sistematika Penelitian

Adapun sistematika penelitian yang digunakan pada penelitian ini digambarkan secara detail sesuai dengan tahap-tahap yang dilalui. Berikut ini merupakan sistematika penelitian pada penelitian ini.



GAMBAR III.2
SISTEMATIKA PENELITIAN

IV. HASIL DAN PEMBAHASAN

Untuk mencapai tujuan penelitian melalui eksperimen dalam bentuk *penetration testing* berdasarkan *walkthrough* yang sudah dilakukan, diperlukan berbagai arsitektur yang terdiri dari *software* dan *hardware* untuk mendukung pengumpulan data dari penelitian yang dilakukan. Pada penelitian ini menggunakan Kali Linux dan *vulnerable machine* Hackable 2 sebagai sarana untuk melakukan penelitian ini.

A. *Hardware* dan *Software*

1. *Hardware*

Berikut adalah rincian *hardware* yang digunakan:

TABEL IV.1
TABEL *HARDWARE*

Component	***Information***	
Hardware Spesification: Lenovo Legion 5 15IMH05	*Processor*	Intel Core™ i7-10750U CPU @ 2.60GHz (12 CPUs), ~2.6GHz
	Memory	16 GB RAM
	System Types	64-*bit Operating System*, x64-*based processor*
	Operating System	Windows 11 Home Single Language 64-Bit (10.0, Build 22621)
	Storage	SSD 512 GB

2. *Software*

Berikut adalah rincian *software* yang digunakan:

TABEL IV.2
TABEL *SOFTWARE*

Type	***Software***
Operating System	Kali Linux • Memory : 2 GB • Network : Bridge
IT Asset	*Vulnerable Machine* Hackable2 • Memory : 512 MB • Network : Bridge
Attack Tools	• Netdiscover • network_scanner.py • Nmap • Gobuster • FFUF • Dirsearch • Netcat

Pada penelitian ini, digunakan sejumlah *software* termasuk *Operating System, IT asset,* dan *Attack Tools*. Berikut adalah penjelasan mengenai spesifikasi dari setiap *software* yang digunakan pada penelitian ini:

1. *Operating System*

Kali Linux merupakan sistem operasi yang digunakan untuk melakukan pengujian terhadap keamanan dan melakukan penetration testing. Pada penelitian ini, Kali Linux digunakan sebagai alat penyerangan.

2. *IT Asset*

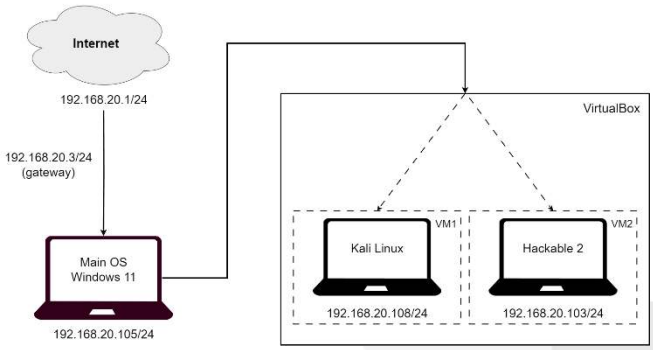
Hackable 2 adalah *vulnerable machine* yang dirancang untuk pelatihan dan latihan dalam bidang keamanan siber dan eksploitasi, menyediakan kerentanan yang disengaja untuk memungkinkan peneliti melakukan pengujian dan meningkatkan keterampilan. Pada penelitian kali ini Hackable 2 digunakan sebagai objek untuk melakukan eksploitasi.

3. *Attack Tools*

a. Netdiscover adalah alat *open-source* yang digunakan untuk pemindaian jaringan dan mendeteksi perangkat terhubung dalam jaringan lokal.
b. Network_scanner.py adalah sebuah skrip atau program yang ditujukan untuk melakukan pemindaian jaringan (*network scanning*). Alat ini di dibagikan oleh dharmil18 melalui repository GitHub.
c. Nmap adalah *tools open-source* yang digunakan untuk melakukan pemindaian jaringan dan mengidentifikasi *host, port* terbuka, layanan yang berjalan, dan mendeteksi kerentanan.
d. Gobuster adalah sebuah *tools open-source* yang digunakan untuk melakukan enumerasi (pemindaian) direktori dan *file* pada situs web.
e. FFUF (*Fuzz Faster U Fool*) adalah sebuah *tools open-source* yang digunakan dalam eksploitasi dan pengujian keamanan web. Alat ini digunakan untuk melakukan serangan kamus (*wordlist attack*).
f. Dirsearch, merupakan sebuah *tools* yang digunakan untuk mengidentifikasi potensi celah keamanan atau informasi sensitif yang dapat ditemukan melalui akses ke direktori atau *file*.
g. Netcat, atau biasa dikenal sebagai "nc," adalah alat jaringan serbaguna yang digunakan untuk menyediakan konektivitas jaringan, *transfer file,* dan berkomunikasi dengan protokol jaringan pada eksploitasi dan administrasi sistem.

B. Platform eksperimen

Berikut ini adalah patform eksperimen yang digunakan:



GAMBAR IV.1
Platform Eksperimen

C. Daftar IP *Address*

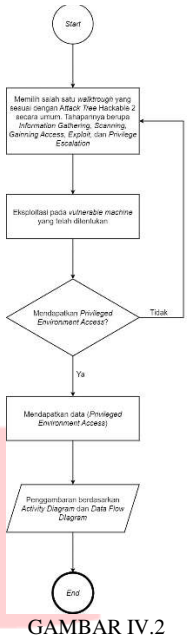
Berikut adalah IP adrress yang digunakan:

TABEL IV.3
Ip *Address*

Type	*Host*	*Default Gateway*	IP *Address*
Vulnerable Machine 1 (VM 1)	Kali Linux	192.168.20.3/24	192.168.20.108/24
Vulnerable Machine 2 (VM 2)	Hackable2		192.168.30.103/24

D. Skenario Pengujian

Skenario pengujian yang digunakan menggunakan data hasil eksperimen berdasarkan *walkthrough.* Berikut ini perumusan *activity diagram* dan *data flow diagram* berdasarkan *walkthrough:*



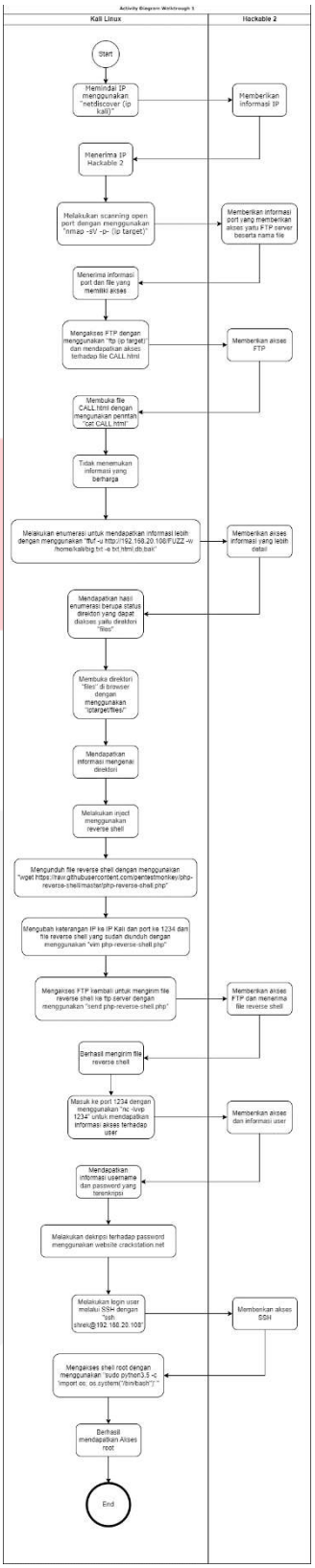
GAMBAR IV.2
SKENARIO PENGUJIAN

E. *Activity Diagram*

Activity diagram digunakan untuk menjelaskan tahap menuju *privileged environment access.* Pada percobaan pertama berdasarkan pada *walkthrough* Hackable 2 dari Pwn3r. Adapun *attack tools* yang digunakan pada *walkthrough* ini adalah Netdiscover, Nmap, FFUF, dan Netcat. Pada percobaan pertama ini menggunakan FFUF untuk mencari kerentanan dan informasi tersembunyi. *Attack tools* yang digunakan dapat berjalan pada Kali Linux dan diakses melalui *command prompt*. Berikut merupakan *activity diagram* yang telah dibuat berdasarkan *walkthrough* pertama.

1. Tahap pertama adalah melakukan pemindaian (*scanning*) pada jaringan lokal untuk menemukan alamat IP Hackable 2 dengan menggunakan perintah Netdiscover pada Kali Linux. Pastikan Hackable 2 berada dalam kondisi menyala.
2. Tahap ke dua berupa Hackable 2 yang mengirimkan informasi alamat IP.
3. Lalu, mendapatkan informasi alamat IP dari Hackable 2 sebagai target.
4. Setelah itu, melakukan pemindaian menggunakan Nmap untuk mencari informasi mengenai semua *port* yang tersedia, dan versi dari layanan dari *port* yang terbuka pada alamat IP Hackable 2 yang telah didapat.
5. Kemudian, Hackable 2 mengirimkan hasil dari pemindaian berupa informasi *port* yaitu melalui FTP *server* beserta nama *file* yang dapat memberikan akses.
6. Menerima informasi *port* dan *file* lalu menampilkan hasil dari Hackable 2 yang telah didapat.
7. Lalu, mengakses FTP *server* untuk mendapatkan akses terhadap *file* CALL.html.
8. Hackable 2 merespon dengan memberikan akses melalui FTP *server*.
9. Lalu, Kali Linux membuka *file* CALL.html.
10. Tidak menemukan informasi yang berharga untuk menjadi sebuah *clue*.
11. Selanjutnya, melakukan enumerasi dengan menggunakan FFUF untuk mencari informasi lebih.
12. Hackable 2 memberikan informasi yang lebih detail.

13. Kemudian, mendapatkan informasi yang lebih detail berupa direktori yang dapat diakses yaitu direktori /files.
14. Mengakses direktori /files melalui browser pada Kali Linux.
15. Lalu, mendapatkan informasi mengenai isi dari direktori /files.
16. Selanjutnya, melakukan tindakan penyuntikan (*incjection)* berupa *reverse shell* untuk mendapatkan koneksi secara langsung antara Kali Linux dengan Hackable 2.
17. Kemudian, mengunduh *file reverse shell* pada Kali Linux melalui *command prompt* dengan perintah wget.
18. Setelah *file reverse shell* berhasil diunduh, lalu buka *file* tersebut dan ubah pada bagian keterangan IP menjadi IP Kali Linux dan keterangan *port* menjadi 1234 dengan menggunakan perintah vim.
19. Lalu, akses kembali FTP untuk mengirimkan *file reverse shell* ke direktori *files* melalui FTP *server* dengan menggunakan perintah *send*.
20. Hackable 2 memberikan akses FTP dan menerima *file reverse shell*.
21. *File reverse shell* berhasil dikirimkan dan tersedia pada direktori *files.*
22. Selanjutnya, masuk ke *port* 1234 sesuai dengan keterangan yang sudah diubah pada *file* reverse shell untuk mendapatkan informasi mengenai *user* Hackable 2 berupa *username* dan *password.*
23. Hackable 2 memberikan informasi username dan password.
24. Lalu, Kali Linux menerima informasi mengenai *username* yaitu shrek dan *password* terenkripsi yang digunakan oleh Hackable 2.
25. Selanjutnya, mengakses *website* crackstation.net melalui *browser* untuk melakukan dekripsi terhadap *password* Hackable 2 yang terenkripsi.
26. Kemudian, melakukan login ke Hackable 2 melalui Kali Linux dengan menggunakan SSH.
27. Hackable 2 memberikan akses melalui SSH.
28. Lalu, Kali Linux berhasil mengakses Hackable 2 dengan menggunakan SSH dan mengakses *shell* root.
29. Tahap terakhir, berhasil untuk mendapatkan akses terhadap root, sehingga *privileged environment access* berhasil dilakukan.



GAMBAR IV.3
Activity Diagram

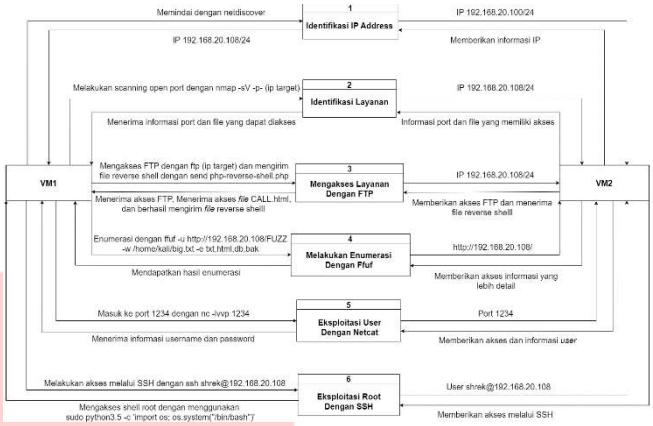
F. *Data Flow Diagram*

Pada penelitian ini, pembuatan *data flow diagram* dibuat berdasarkan bagaimana informasi atau data mengalir pada setiap *walkthrough.* Berikut merupakan *data flow diagram* berdasarkan *walkthrough* dari Pwn3r.

1. Tahap pertama adalah melakukan pemindaian IP target dengan menggunakan perintah "netdiscover

192.168.20.100". Alamat IP 192.168.20.100/24 sebagai target pemindaian, yang berarti Netdiscover mencoba menemukan perangkat atau *host* yang aktif pada alamat IP tersebut atau di sekitar alamat tersebut dalam jaringan lokal. Lalu didapatkan alamat IP 192.168.20.108/24 sebagai IP target.

2. Tahap ke dua yaitu melakukan pemindaian *port* yang terbuka dan dapat memberikan akses dengan menggunakan perintah "nmap -sV -p- 192.168.20.108". Alamat IP 192.168.20.108/24 digunakan sebagai target pemindaian sehingga Nmap akan memindai semua *port* yang tersedia atau rentang seccara lengkap oleh karena itu menggunakan tambahan opsi perintah -p-. Lalu Nmap juga akan mengidentifikasi versi perangkat lunak atau protokol yang digunakan pada *port* yang terbuka, dengan menggunakan opsi perintah -sV. Sehingga didapatkan keterangan *port* yang terbuka yaitu FTP beserta informasi *file* yang dapat diakses.
3. Tahap ke tiga yaitu mengakses FTP dengan menggunakan perintah "ftp 192.168.20.108". Alamat IP 192.168.20.108/24 berperan sebagai *host*. FTP digunakan untuk melakukan *transfer file* antara dua perangkat melalui web *server*, pada penelitian ini kedua perangkat tersebut adalah Kali Linux dan Hackable 2. Layanan FTP digunakan untuk mengakses *file* CALL.html yang merupakan sebuah *clue* dan mengirimkan sebuah *file reverse shell* yang akan bekerja sebagai *backdoor* pada penelitian ini.
4. Tahap ke empat yaitu melakukan enumerasi untuk mendapatkan informasi lebih detail mengenai kerentanan yang terdapat pada target menggunakan perintah "ffuf -u http://192.168.20.108/FUZZ -w /home/kali/big.txt -e txt,html,db,bak". FFUF digunakan untuk melakukan serangan *brute force* untuk menguji direktori, nama *file*, atau parameter URL. Opsi perintah -u http://192.168.20.108/FUZZ digunakan untuk mendifinisikan URL target yang akan diserang. Opsi perintah -w /home/kali/big.txt digunakan untuk mendefinisikan di mana letak skrip *wordlist* yang akan digunakan pada penyimpanan Kali Linux. Opsi perintah -e txt,html,db,bak digunakan untuk mengatur ekstensi *file* yang akan diuji pada serangan. Sehingga didapatkan hasil enumerasi berupa direktori yang memiliki kerentanan.
5. Tahap ke lima yaitu melakukan eksploitasi untuk mendapatkan informasi *user* berupa *username* dan *password* dari Hackable 2 dengan menggunakan perintah nc -lvvp 1234. Netcat atau nc pada penelitian ini digunakan untuk melakukan *backdoor* sehingga dapat terkoneksi dengan target sehingga bisa mendapatkan informasi *user* yang diperlukan. Opsi -l digunakan untuk memulai mode *listening* sehingga Netcat mendengarkan setiap koneksi yang masuk, opsi -vv digunakan untuk memasuki mode *verbose* sehingga menampilkan informasi yang rinci mengenai koneksi dan aktivitas yang dilakukan, dan opsi -p 1234 digunakan untuk menentukan *port* yang digunakan yaitu *port* 1234. Sehingga melalui Netcat, bisa terkoneksi dengan target dan dapat mengakses target untuk mendapatkan informasi *username* dan *password* dari target.
6. Tahap ke enam yaitu melakukan eksploitasi terhadap root dengan menggunakan perintah "ssh shrek@192.168.20.108" dan "python3.5 -c 'import os; os.system("/bin/bash")". Pada penelitian ini, perintah ssh digunakan untuk melakukan *remote* atau mengendalikan Hackable 2 dari perangkat Kali Linux. Shrek merupakan *username* dari target. Lalu, setelah berhasil mengakses target dengan menggunakan *username* dan *password* yang sudah didapatkan, dilanjutkan dengan melakukan eksploitasi menggunakan perintah "python3.5 -c 'import os; os.system("/bin/bash")" untuk mendapatkan akses dan kontrol secara menyeluruh terhadap root.



GAMBAR IV.4
Data Flow Diagram

G. Pengukuran *Time Walkthrough*

Pengukuran waktu pada *walkthrough* satu meliputi tindakan mengamati, mencatat, dan mengitung durasi pada setiap perintah yang dijalankan. Adapun keterangan waktu yang didapat dari setiap perintah yang dijalankan pada *walkthrough* satu berupa keterangan *real time*, *user time*, dan *system time.* Berikut adalah *time walkthrough* satu:

TABEL IV.4
Time Walkthrough

No	*Command*	***Time walkthrough* satu (satuan detik/s)**		
		real	**user**	**sys**
1	netdiscover (IP kali)/24	16,58	0,07	0,38
2	nmap -sV -p- (IP target)	26,3	0,66	1,34
3	ftp (IP target): - get CALL.html	92,77	0	0,01
4	cat CALL.html	0	0	0
5	ffuf -u http://192.168.20.108/FUZZ -w /home/kali/big.txt -e txt,html,db,bak	29,19	0,01	0
6	wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php	0,72	0,02	0,01
7	vim php-reverse-shell.php	313	0,10	0,04
8	ftp (IP target) :	96,60	0,01	0

No	*Command*	*Time walkthrough* satu (satuan detik/s)		
		real	**user**	**sys**
	- send php-reverse-shell.php			
9	nc -lvvp 1234 : - cd /home - ls -al - cat important.txt - ls -l /.runme.sh - cat /.runme.sh	372,10	0	0
10	ssh shrek@192.168.20.108 : - -l - python3.5 -c 'import os; os.system("/bin/bash")' - cd /root - ls -al - cat root.txt	239,96	0,03	0,01
Total		718,52	1,61	4,51
Total dengan satuan menit		11,97	0,02	0,07

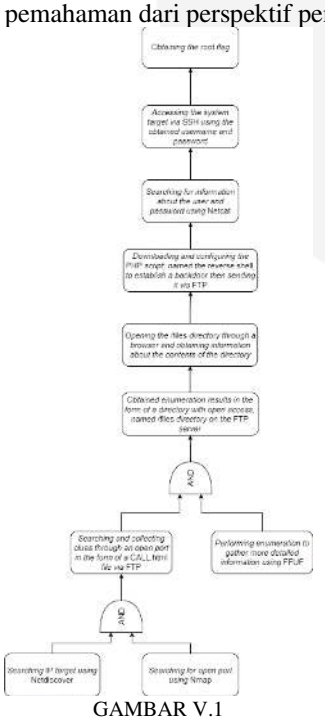
Berdasarkan *time walkthrough* satu, terdapat total waktu dalam satuan detik sebagai berikut.

- *Real time* : 718,52 s
- *User time* : 1,61 s
- *System time* : 4,51 s

V. ANALISIS

A. *Attack Tree* Berdasarkan *SAND Gate*

Attack tree memberikan banyak manfaat, termasuk mendukung analisis ancaman, penilaian serangan, serta memungkinkan pemahaman dari perspektif penyerang.



GAMBAR V.1
Attack Tree Berdasarkan Sand *Gate*

Berikut penjelasan dari *attack tree* berdasarkan SAND *gate:*

1. *Goals and Contexts*

Attack tree ini dibuat dengan tujuan untuk dilakukan analisis dengan cara melakukan perbandingan setiap *attack tree* berdasarkan *walkthrough* satu dengan yang lainnya. Setelah melakukan perbandingan, selanjutnya dilakukan pemeringkatan dengan harapan dapat membantu menghadapi ancaman yang terjadi.

2. *Target*

Pada *attack tree* berdasarkan *walkthrough* satu ini, *vulnerable machine* Hackable 2 menjadi target serangan untuk mendapatkan *priviledge environment access* atau akses menyeluruh terhadap root. Dengan berhasilnya mendapatkan akses terhadap root maka penyerang memiliki akses dan kontrol penuh terhadap seluruh sistem, termasuk berkas, direktori, konfigurasi, proses, dan berbagai pengaturan sistem lainnya.

3. *Attack Level*

Attack tree pada *walkthrough* satu ini berfokus melakukan serangan melalui direktori yang terdapat pada FTP *server*. Penyerangan tersebut dilakukan dengan menggunakan *attack tools* FFUF untuk mencari kerentanan yang terdapat pada FTP *server*. Pada penelitian ini *port* FTP memiliki sebuah kerentanan sehingga bisa menjadi akses masuk menuju *vulnerable machine* Hackable 2.

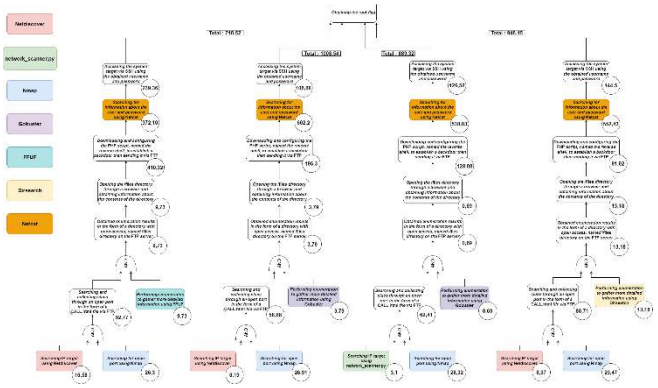
4. *Node*

Berikut adalah penjelasan dari setiap simpul atau *node* pada *attack tree* berdasarkan *walkthrough* satu.

a. Searching IP *target using* Netdiscover
b. Searching for open port using Nmap
c. Searching and collecting clues through an open port in the form of a CALL.html *file via* FTP
d. Performing enumeration to gather more detailed information using FFUF
e. Obtained enumeration results in the form of a directory with open access, named /files *directory on the* FTP *server*
f. Opening the /files *directory through a browser and obtaining information about the contents of the directory*
g. Downloading and configuring the PHP *script, named the* reverse shell*, to establish a backdoor then sending it via* FTP
h. Searching for information about the user and password using Netcat
i. Accessing the system target via SSH *using the obtained username and password*
j. Obtaining the root *flag*

B. Pemeringkatan Berdasarkan *Metrics*

Pemeringkatan dilakukan dengan perbandingan terhadap empat *attack tree* berdasarkan *walkthrough,* dengan menggunakan tiga *metrics,* yaitu *time metric, cost metric,* dan *frequency metric.*



GAMBAR V.2
PEMERINGKATAN BERDASARKAN *METRICS*

1. Pemeringkatan Berdasarkan *Time Metric*

Time metric merupakan ukuran atau metrik yang digunakan untuk mengukur waktu yang diperlukan untuk menyelesaikan suatu tugas, proses, atau aktivitas tertentu. Berikut adalah hasil yang diperoleh dari pemeringkatan berdasarkan *time metric*.

TABEL V.1
PEMERINGKATAN BERDASARKAN TIME METRIC

Ranking	*Attack tree*	*Time metric*(s)
1	*Attack tree* wt 1	718,52
2	*Attack tree* wt 3	889,32
3	*Attack tree* wt 4	946,15
4	*Attack tree* wt 2	1008,54

Dapat disimpulkan bahwa *attack tree* wt 1 memiliki waktu penyelesaian rangkaian tahap untuk mendapatkan akses root yang paling singkat dibandingkan dengan *attack tree* lainnya, sehingga menduduki peringkat pertama dengan total waktu 718,52 s. Hal ini disebabkan oleh kecepatan waktu pada proses yang dilakukan pada *attack tree* wt 1 lebih lebih cepat dibandingkan dengan yang lainnya. Selain itu, penggunaan *tools* pada *attack tree* wt 1 juga menjadi faktor kunci yang mempengaruhi kecepatan proses pada *attack tree* tersebut.

2. Pemeringkatan Berdasarkan *Cost Metric*

Cost metric merupakan ukuran atau metrik yang digunakan untuk mengukur biaya yang diperlukan pada suatu tugas, proses, atau aktivitas. Berikut adalah hasil yang diperoleh dari pemeringkatan berdasarkan *cost metric.*

TABEL V.2
Pemeringkatan Berdasarkan Cost Metric

Ranking	*Attack tree*	*Cost metric*(*step*)
1	*Attack tree* wt 1	29
	Attack tree wt 3	29
	Attack tree wt 2	29
	Attack tree wt 4	29

Pemeringkatan *attack tree* berdasarkan *cost metrics* adalah seluruh *attack tree* memiliki jumlah *cost metric* yang sama, sehingga seluruh *attack tree* berada pada peringkat pertama

3. Pemeringkatan Berdasarkan *Frequency Metric*

Frequency metric merupakan ukuran atau metrik yang digunakan untuk mengukur seberapa sering suatu alat atau *tools* digunakan pada aktivitas keamanan. Berikut adalah hasil yang diperoleh dari pemeringkatan berdasarkan *frequency metric.*

TABEL V.3
PEMERINGKATAN BERDASARKAN FREQUENCY METRIC

Ranking	*Tools*	*Frequency of Use*
1	Nmap	4 (*All walkthrough use it*)
	Netcat	
2	Netdiscover	3 (*Used by three walkthrough*)
3	Gobuster	2 (*Used by two walkthrough*)
4	network_scanner.py	1 (*Only used once in three walkthrough*)
	FFUF	
	Dirsearch	

Pemeringkatan *attack tree* berdasarkan *frequency metric*, terdapat dua *tools* yang menduduki peringkat pertama yaitu Nmap dan Netcat. Hal tersebut dikarenakan kedua *tools* tersebut digunakan pada empat *attack tree*. Peringkat ke dua memiliki satu *tools* yaitu Netdiscover. *Tools* pada peringkat ke dua tersebut digunakan pada tiga *attack tree*. Peringkat ke tiga memiliki satu *tools* yaitu Gobuster. *Tools* tersebut digunakan pada dua *attack tree*. Lalu yang terakhir, pada peringkat ke empat memiliki tiga *tools* yaitu Nertwork _scanner.py, FFUF, dan Dirsearch yang digunakan masing-masing satu kali pada tiga *attack tree*.

4. Pemeringkatan Berdasarkan Seluruh *Metrics*

Analisis pemeringkatan berdasarkan perhitungan *metrics* gabungan (*time metric, cost metric* dan *frequency metric*) ini bertujuan untuk mendapatkan pemahaman mengenai sudut pandang penyerang dari aksi penyerangan yang terjadi berdasarkan *attack tree* dari empat *walkthrough* yang telah dipilih.

TABEL V.4
Pemeringkatan Berdasarkan Seluruh Metric

Ranking	*Attack tree*	*Time Metric* (s)	*Cost Metric* (Step)	*Frequency Metric* (*Tools*)
1	*Attack tree* WT 1	718,52	29	Netdiscover, Nmap, FFUF, Netcat
2	*Attack tree* WT 3	889,32	29	network_scanner.py, Nmap, Gobuster, Netcat
3	*Attack tree* WT 4	946,15	29	Netdiscover, Nmap, Dirsearch, Netcat
4	*Attack tree* WT 2	1008,54	29	Netdiscover, Nmap, Gobuster, Netcat

Pemeringakatan berdasarkan *metrics* gabungan (*time metric, cost metric* dan *frequency metric)*, dalam penggunaan ketiga *metrics* ini, prioritas lebih diberikan kepada jalur dengan waktu paling cepat. Dengan waktu paling cepat sebagai prioritas, menyebabkan penjaga keamanan memiliki sedikit waktu untuk melakukan pertahanan, sehingga peluang keberhasilan melakukan penyerangan meningkat. Peringkat pertama dengan jalur paling cepat yaitu *attack tree* wt 1 dengan *time metric* 718,52s atau 11,97 menit dan *cost metric* sebesar 29 langkah. Sedangkan *tools* yang paling efektif untuk

meningkatkan keberhasilan penyerangan adalah Netdiscover, Nmap, Gobuster, dan Netcat.

VI. KESIMPULAN

Tahap-tahap eksploitasi dapat digambarkan dengan menggunakan *activity diagram* dan *data flow diagram*. Penyusunan *attack tree* dapat dilakukan dengan menggunakan metode pendekatan SAND *gate. Attack tree* wt 1 menjadi peringkat pertama berdasarkan perhitungan *time metric* dan *cost metric*, karena menjadi jalur paling cepat dengan total *real time* 718,52 s dan total *cost metric* 29 langkah untuk melakukan eksploitasi dengan tujuan untuk mendapatkan *privileged environment access*. Nmap dan Netcat menjadi peringkat pertama karena merupakan *tools* yang digunakan pada semua *attack tree* berdasarkan empat *walkthrough* yang telah dipilih. Adapun *tools* yang paling efektif untuk melakukan tindakan penyerangan yaitu Netdiscover, Nmap, Gobuster, dan Netcat.

REFERENSI

[1] AWED, I. S. (2022). *Vulnerability Assessment and Penetration Testing of Web Application*.

[2] Kuipers, L. (2020). *Analysis of Attack trees: fast algorithms for subclasses*.

[3] Farizy, S., & Sita Eriana, E. (2022). Keamanan Sistem Informasi. www.unpam.ac.id

[4] Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi dan *Network (Literature Review Sim)*. *3*(5). https://doi.org/10.31933/jemsi.v3i5 Diakses pada 13 Agustus 2023

[5] Moedjahedy, J. (2023). Keamanan Sistem Informasi. https://www.research*gate*.net/publication/371530844 Diakses pada 13 Agustus 2023

[6] Wali, M. (2022). Keamanan Komputer. https://www.research*gate*.net/publication/370105381 14 Agustus 2023

[7] Cathcart, J., & Khan Mohd, T. (2023). *Password Hacking Analysis of Kali Linux Applications*. https://www.research*gate*.net/publication/370048764 Diakses pada 12 Agustus 2023

[8] Rikatsih, N., Andary, R. W., Shaleh, M., Hadiningrum, L. P., Dr. Irwandy, & Prisusanti, R. D. (2020). Metodologi Penelitian Di Berbagai Bidang.

[9] Candra, D., Tendri, M., & Rizta, A. (2018). Pengembangan Lembar Kerja Siswa (LKS) Materi Segiempat Berbasis Tahap Teori Van Hiele di SMP.

[10] Gutama, A., Arwan, A., & Fanani, L. (2019). Pengembangan Kakas Bantu Pembangkitan Kasus Uji pada *Model-Based Testing* Berdasarkan *Activity Diagram* (Vol. 3, Issue 9). http://j-ptiik.ub.ac.id Diakses pada 12 Agustus 2023

[11] Safwandi, Fadlisyah, Aulia, Z., & Zulfakhmi. (2021). Analisis Perancangan Sistem Informasi Sekolah Menengah Kejuruan 1 Gandapura Dengan Model Diagram Konteks dan *Data Flow Diagram*.

[12] Sonderen, T. (2019). *A Manual for Attack trees*. https://essay.utwente.nl/79133/1/Sonderen_MA_EEMCS.pdf Diakses pada 14 Agustus 2023