Implementasi dan Analisis *Attack Tree* pada *Vulnerable Machine* Metasploitable2 Berdasarkan *TimeMetric, Cost Metric,* dan *Frequency Metric*

1st Rheza Dewantara
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
rhezad@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 implementasi dan analisis dari attack tree terhadap vulnerable machine Metasploitable2 berdasarkan time metric, cost metric, dan frequency metric yang dilakukan untuk pemeringkatan, sehingga dapat mengetahui jalur tercepat untuk mengakses privileged environment access target. Metode yang digunakan pada penelitian ini adalah pengujian eksploitasi berdasarkan walkthrough dan melakukan penggambaran menggunakan attack tree dengan pendekatan SAND gate. Hasil akhir dari seluruh tahapan eksploitasi pada vulnerable machine Metasploitable2 adalah berhasil mengakses privileged environment access target. Seluruh langkah yang dilakukan pada walkthrough digambarkan dengan activity diagram dan alur data yang terjadi digambarkan dengan data flow diagram. Penggambaran attack tree mewakili seluruh tahapan eksploitasi berdasarkan walkthrough untuk dilakukan pemeringkatan berdasarkan metrics. Hasil pemeringkatan yang dilakukan berdasakan time metric menghasilkan attack tree WT 1 sebagai waktu tempuh tercepat dengan real time sebesar 718,52 detik. Pemeringkatan berdasarkan cost metric menghasilkan attack tree WT 1 sebagai peringkat pertama karena jalur paling pendek dengan total 20 langkah. Netdiscover, Nmap, dan Msfconsole menjadi peringkat pertama pada pemeringkatan berdasarkan frequency metric karena ketiga tools tersebut digunakan pada semua attack tree berdasarkan lima walkthrough yang telah dipilih.**

Kata kunci: **Metasploitable2, Attack Tree, Metrics**

I. PENDAHULUAN

Perkembangan teknologi telah mengakibatkan peningkatan serangan siber. Perusahaan-perusahaan memerlukan banyak sumber daya agar dapat melawan peretas dan menjamin keamanan sistem, namun kedapatan adanya kerentanan baru masih terus ditemukan. Oleh karena itu, pengujian eksploitasi merupakan cara terbaik untuk melindungi diri dari serangan siber [1]. Dengan pengujian eksploitasi, perusahaan ataupun organisasi dapat mengidentifikasi kerentanan pada sistem sebelum peretas mengeksploitasi, sehingga banyak sumber daya dapat diamankan. Cara yang dapat dilakukan untuk melakukan pengujian eksploitasi dengan waktu dan biaya yang terjangkau adalah dengan menggunakan *vulnerable machine*, kemudian menganalisisnya menggunakan *attack tree*.

Attack tree memberikan gambaran visual tentang bagaimana penyerang dapat mengeksploitasi kerentanan dalam sistem menjadi lebih mudah dipahami. *Attack tree* memiliki bagian yang dapat dihitung nilainya, yaitu metrics. *Metrics* merupakan nilai numerik yang menggambarkan karakteristik atau sifat dari simpul *attack tree* seperti waktu, biaya, frekuensi, probabilitas keberhasilan serangan, tingkat kesulitan dalam melakukan serangan, peralatan khusus yang dibutuhkan dalam serangan, dan kombinasi dari semua metrik tersebut. Dengan menggunakan *metrics*, ahli keamanan siber dapat mengevaluasi risiko keamanan sistem secara lebih rinci dan objektif [2]. *Metrics* yang dihitung dapat digunakan sebagai dasar untuk melakukan pemeringkat pada *attack tree* sehingga dapat mengidentifikasi pada simpul yang paling rentan dan menentukan prioritas tindakan pencegahan untuk melindungi sistem.

Penelitian ini berfokus pada implementasi dan analisis *attack tree* pada *vulnerable machine* Metasploitable2 dengan menggunakan *time metric, cost metric*, dan *frequency metric*. *Attack tree* dapat digunakan sebagai dasar untuk memperkuat keamanan sistem dengan menganalisis cara-cara serangan terhadap sistem tersebut, serta dapat menjadi panduan untuk mengetahui jalur tercepat dan biaya rendah dalam melakukan serangan berdasarkan pemilihan metrics.

II. KAJIAN TEORI

A. Keamanan Sistem Informasi

Keamanan sistem informasi adalah upaya untuk mencegah serangan oleh pengguna komputer, akses jaringan yang tidak sah, serta mendeteksi tindakan pengganggu yang tidak diidentifikasi oleh sistem [3]. Menurut Nurul [4], dalam usaha pengelolaan dan pengendalian keamanan sistem nformasi, perlu mempertimbangkan tiga aspek penting keamanan informasi yang dikenal sebagai CIA (*Confidentiality, Integrity, Availability*).

B. Eksploitasi

Eksplotasi merupakan metode yang diterapkan untuk melakukan penyerangan dan merusak sistem. Istilah ini dapat berwujud kata kerja atau kata benda. Pelaku ancaman dapat berupaya mengeksploitasi sistem atau aset informasi lainnya secara ilegal demi keuntungan pribadi [5]. Jadi eksplotasi adalah teknik untuk merusak sistem dengan upaya ilegal

memanfaatkan kerentanan oleh pelaku ancaman demi keuntungan pribadi.

C. Kali Linux

Kali Linux merupakan software *open=source* yang dikhususkan untuk pengujian eksploitasi profesional dan pemeriksaan keamanan [6]. Kali Linux juga menyediakan alat-alat untuk mengidentifikasi dan mengatasi kerentanan dalam sistem. Kali Linux dikembangkan oleh Offensive Security. Dalam penelitian ini, Kali Linux digunakan sebagai penyerang.

D. *Vulnerable machine* Metasploitable2

Dalam penelitian ini, *vulnerable machine operating system* yang digunakan adalah Metasploitable2. Metasploitable2 dibuat oleh Rapid7, perusahaan keamanan siber, pada tanggal 12 Juni 2012. Tujuannya untuk digunakan sebagai alat pelatihan dan pengujian untuk pengembangan keahlian dalam mengidentifikasi, mengeksploitasi, dan melindungi sistem dari kerentanan dan ancaman keamanan. Metasploitable2 menyediakan lingkungan yang aman untuk menguji alat-alat keamanan dan strategi pertahanan.

E. Eksperimen

Metode eksperimen dalam ilmu komputer adalah pendekatan yang digunakan oleh peneliti untuk mengidentifikasi hubungan atau dampak antara berbagai variabel dalam lingkungan yang terkendali secara ketat. Metode penelitian eksperimen sangat penting untuk diberikan perhatian khusus, terutama dalam penelitian yang melibatkan pengembangan baik perangkat lunak maupun perangkat keras [7]. Jadi dapat disimpulkan bahwa eksperimen adalah sebuah proses mengidentifikasi hubungan antara variabel dalam lingkungan terkendali.

F. Walkthrough

Walkthrough merupakan proses atau langkah-langkah yang diikuti untuk menguji, memahami, atau mengevaluasi suatu sistem, perangkat lunak, atau prosedur. Ini melibatkan langkah-langkah terperinci yang diikuti secara sistematis untuk mengidentifikasi masalah, menguji fungsionalitas, atau memahami bagaimana suatu sistem beroperasi [8]. Pada penelitian ini¸ *walkthrough* sendiri merupakan langkah-langkah yang dibuat oleh seorang ahli untuk melakukan eksploitasi atau serangan terhadap *vulnerable machine* Metasploitable2 dengan tujuan mendapatkan *priviledge environment access* atau root.

G. Activity Diagram

Activity diagram adalah salah satu model perilaku UML yang sesuai untuk uji sistem, karena *activity diagram* dapat mengilustrasikan urutan seluruh sistem [9]. Diagram ini mengilustrasikan langkah-langkah, keputusan, dan aktivitas-aktivitas yang terlibat dalam suatu proses secara visual. Biasanya digunakan untuk memodelkan alur kerja bisnis, proses sistem, atau skenario pengujian dalam pengembangan perangkat lunak. Dalam penelitian ini, *activity diagram* digunakan dalam memodelkan skenario pengujian yang berasal dari lima *walkthrough* pilihan.

H. 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 [10]. 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.

I. *Attack tree*

Attack tree merupakan sebuah model untuk membantu menganalisis sebuah ancaman, mengevaluasi sebuah serangan yang dapat merugikan, dan juga membantu pakar keamanan untuk dapat melihat dari prespektif penyerang untuk mengungkap kerentanan dalam sistem [11]. Keuntungan menggunakan model *attack tree* sendiri mulai dari membantu menganalisis sebuah ancaman, mengevaluasi sebuah serangan, dan membantu melihat dari prespektif penyerang.

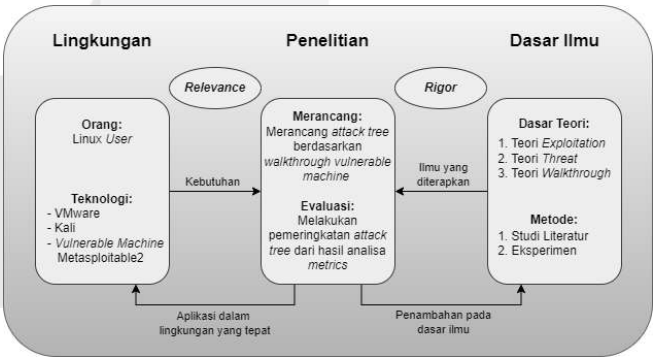
J. *Metrics*

Menurut Kuipers [2], *Metrics* merupakan sebuah nilai pada bagian *attack tree* yang nantinya dihitung. Tujuan dari perhitungan pada penelitian ini adalah untuk dijadikan landasan dalam pemeringkatan *attack tree*. Terdapat beberapa jenis *Metrics* [2], tetapi dalam penelitian ini hanya menggunakan tiga *metrics* saja yaitu *time metric, cost metric,* dan *frequency metric.*

III. METODE

A. Model Konseptual

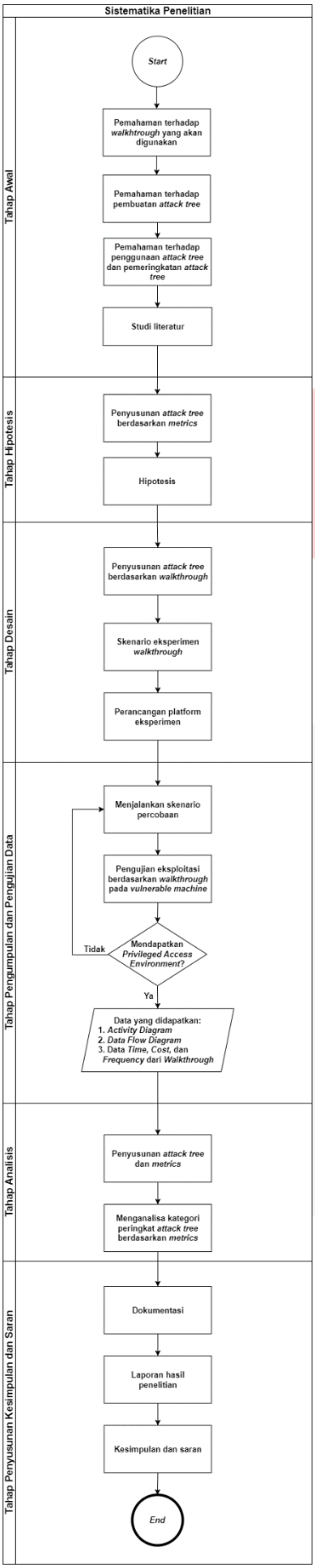
Model konseptual adalah representasi abstrak yang menggambarkan hubungan antara berbagai konsep, dengan tujuan memberikan gambaran dan pedoman terkait dengan asumsi yang terkait dengan variabel yang akan diselidiki. Model konseptual yang digunakan dalam penelitian ini adalah sebagai berikut.



GAMBAR III.1
MODEL KONSEPTUAL

B. Sistematika Penelitian

Sistematika penelitian yang diterapkan dalam penelitian ini diuraikan secara lengkap sesuai dengan langkah-langkah yang dijalani. Sistematika penelitian pada penelitian ini adalah sebagai berikut.



GAMBAR III.2
SISTEMATIKA PENELITIAN

IV. HASIL DAN PEMBAHASAN

Untuk mencapai tujuan penelitian melalui eksperimen berupa pengujian eksploitasi berdasarkan *walkthrough* yang telah dilakukan, diperlukan beragam komponen berupa *software* (perangkat lunak) dan *hardware* (perangkat keras) untuk mendukung pengumpulan data dari penelitian ini. Dalam penelitian ini, Kali Linux dan vulnerable machine Metasploitable2 digunakan sebagai alat untuk melaksanakan penelitian tersebut.

A. *Hardware* dan *Software*

1. *Hardware*

Rincian *Hardware* yang digunakan yang digunakan dalam penelitian ini adalah sebagai berikut.

TABEL IV.1
TABEL *HARDWARE*

Komponen	**Informasi**	
Spesifikasi Perangkat Keras: Acer Aspire E5-475G	*Processor*	Intel Core™ i5-7200U CPU @ 2.50 GHz (4CPUs), ~2.7 GHz
	Memory	12288 MB RAM
	System Types	64-*bit Operating System*, x64-*based processor*
	Operating System	Windows 10 Pro 64-Bit (10.0, Build 19041)
	Storage	SSD 256 GB

2. *Software*

Rincian s*oftware* yang digunakan yang digunakan dalam penelitian ini adalah sebagai berikut.

TABEL IV.2
TABEL *SOFTWARE*

Type	***Software***
Operating System	Kali Linux • Memory : 2 GB • Network : NAT
IT *Asset*	*Vulnerable machine* Metasploitable2 • Memory : 512 MB • Network : NAT
Tools	• Netdiscover • Nmap • Msfconsole • Netcat • Searchsploit • Grep

Operating System, IT asset, dan *Tools* merupakan *software* yang digunakan dalam penelitian ini. Penjelasan mengenai spesifikasi dari setiap *software* yang digunakan pada penelitian ini adalah sebagai berikut.

a. *Operating System*

Kali Linux merupakan sebuah *operating system* yang didesain khusus untuk melakukan pengujian keamanan dan eksploitasi. Maka dari itu, Kali Linux disini berfungsi sebagai alat penyerangan.

b. *IT Asset*

Metasploitable2 merupakan sebuah *operating system* yang dirancang untuk memiliki sejumlah celah keamanan yang dapat dieksploitasi, juga didesain sebagai target uji coba bagi

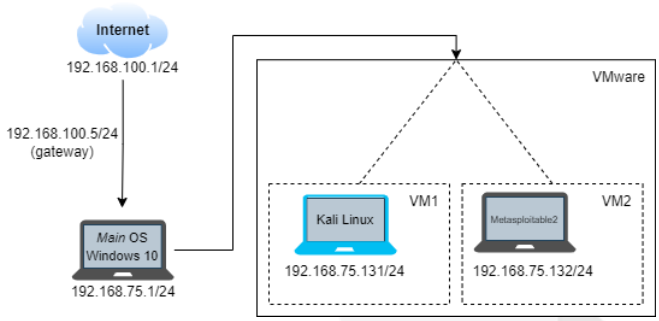
ethical hacker dan peneliti keamanan dalam menguji keamanan jaringan dan sistem informasi. Metasploitable2 pada penelitian ini digunakan sebagai objek eksploitasi.

c. *Attack Tools*

1) Netdiscover adalah alat pemindaian jaringan *open-source* yang digunakan untuk mengidentifikasi dan menampilkan alamat IP dalam jaringan lokal.
2) Nmap adalah alat pemindaian jaringan yang digunakan untuk mengidentifikasi perangkat, *port*, dan layanan yang berjalan dalam jaringan komputer.
3) Msfconsole adalah antarmuka baris perintah yang digunakan dalam kerangka kerja Metasploit untuk mengelola dan meluncurkan serangan eksploitasi.
4) Netcat (atau nc) adalah utilitas jaringan serbaguna berbasis baris perintah yang digunakan untuk membuka, mengirim, dan menerima koneksi jaringan serta berfungsi sebagai alat untuk mengirim data melalui jaringan.
5) Searchsploit adalah alat baris perintah yang digunakan untuk mencari dan mengeksplorasi basis data eksploitasi, membantu peneliti keamanan dalam menemukan eksploitasi yang ada untuk kerentanan tertentu.
6) Grep adalah perintah baris perintah yang digunakan untuk mencari dan mengekstrak baris teks yang cocok dengan pola tertentu dari berkas teks atau *output* teks.

B. Platform eksperimen

Platform eksperimen yang digunakan dalam penelitian ini adalah sebagai berikut.



GAMBAR IV.1
Platform Eksperimen

C. Daftar IP *Address*

Penjelasan daftar IP adrress pada penelitian ini adalah sebagai berikut.

TABEL IV.3
Ip *Address*

Type	***Host***	***Default Gateway***	***IP Address***
Virtual machine 1 (VM 1)	Kali Linux	192.168.100.5/24	192.168.75.131/24
Virtual vulnerable machine 2 (VM 2)	Metasploitable 2		192.168.75.132/24

D. Skenario Pengujian

Skenario pengujian yang diterapkan menggunakan data yang berasal dari hasil eksperimen berdasarkan *walkthrough*. Perumusan *activity diagram* dan *data flow diagram* berdasarkan *walkthrough* pada penelitan ini adalah sebagai berikut.

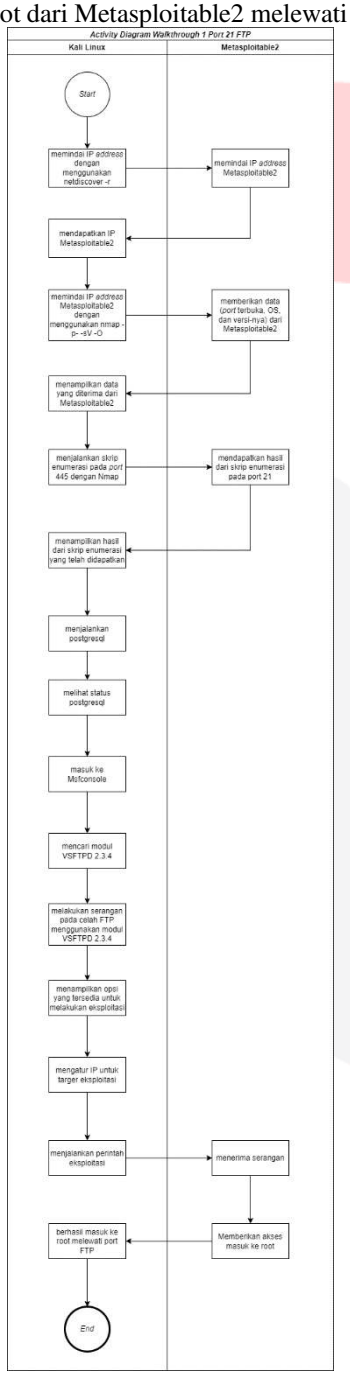
GAMBAR IV.2
SKENARIO PENGUJIAN

E. *Activity Diagram*

Activity diagram digunakan untuk menjelaskan langkah dari awal hinga menuju root. Pada percobaan pertama berdasarkan pada *walkthrough* Metasploitable2 dari YouTube *channel* bernama Lognuk Security. Adapun *tools* yang digunakan pada *walkthrough* ini adalah Netdiscover, Nmap, dan Msfconsole dengan modul VSFTPD 2.3.4. Modul VSFTPD berfungsi untuk mengeksploitasi kerentanan *backdoor* pada layanan FTP. *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. Melakukan pemindaian jaringan dengan tujuan untuk menemukan alamat IP dengan menggunakan Netdiscover.
2. Memindai alamat IP Metasploitable2.
3. Mendapatkan alamat IP dari Metasploitable untuk dijadikan target.
4. Melakukan pemindaian *port* terbuka, sistem operasi, dan versi-nya dari alamat IP Metasploitable2 yang telah didapat dengan menggunakan Nmap.
5. Metasploitable2 merespon dengan memberikan hasil dari pemindaian dengan menggunakan Nmap tersebut.
6. Kali Linux menampilkan hasil respon dari Metasploitable2 yang telah didapat.
7. Menjalankan sebuah skrip enumerasi pada *port* 445 dengan menggunakan Nmap.
8. Metasploitable2 merespon dengan memberikan hasil skrip enumerasi yang telah berjalan tersebut.
9. Kali Linux menampilkan hasil dari skrip enumerasi yang telah diberikan dari Metasploitable2.
10. Lalu menjalankan postgresql pada Kali inux.
11. Melihat status dari prostgresql tersebut.
12. Langkah selanjutnya, masuk ke Msfconsole pada Kali Linux.
13. Mencari modul VSFTPD 2.3.4 pada Msfconsole untuk serangan ke *port* 21 FTP.

14. Memilih modul tersebut untuk dilakukan pengaturan selanjutnya.
15. Menampilkan opsi untuk melakukan eksploitasi.
16. Selanjutnya, atur alamat IP yang menjadi target untuk eksploitasi.
17. Menjalankan perintah eksploitasi dengan modul yang telah ditentukan.
18. Metasploitable2 menerima serangan dari modul tersebut.
19. Hasil dari serangan tersebut adalah Metasploitable2 memberikan akses masuk ke root.
20. Kali Linux menampilkan sebuah prompt saat berhasil masuk ke root dari Metasploitable2 melewati *port* FTP.



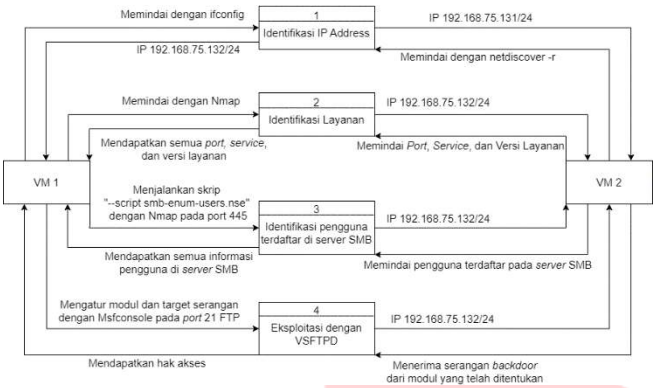
GAMBAR IV.3
Activity Diagram

F. *Data Flow Diagram*

D*ata flow diagram* dibuat berdasarkan bagaimana informasi atau data mengalir pada setiap *walkthrough.* Hasil *data flow diagram* berdasarkan *walkthrough* pertama adalah sebagai berikut.

1. Tahapan pertama yaitu melakukan pemindaian pada Kali Linux dengan perintah "ifconfig", lalu didapatkan alamat IP 192.168.75.131/24. Perintah "ifconfig" digunakan untuk melihat alamat IP pada sebuah sistem operasi.
2. Tahap ke dua yaitu melakukan pemindaian dengan perintah "netdiscover -r 192.168.75.0/24", lalu didapatkan alamat IP 192.168.75.132/24. Perintah "netdiscover -r []" digunakan untuk melakukan pemindaian jaringan ARP dalam rentang IP 192.168.75.1 hingga 192.168.75.254 untuk mengidentifikasi perangkat yang terhubung dalam jaringan lokal.
3. Tahap ke tiga yaitu melakukan pemindaian dengan perintah "nmap -p -sV -O" dengan alamat IP yang target yang dituju yaitu 192.168.75.132/24. Perintah "nmap –p -sV -O 192.168.75.132" digunakan untuk melakukan pemindaian *port*, mendeteksi versi layanan, dan mencoba mengidentifikasi sistem operasi yang digunakan oleh host dengan alamat IP 192.168.75.132/24.
4. Tahap ke empat yaitu melakukan pemindaian *port*, layanan, dan versi dari layanan tersebut, lalu didapatkan semua *port*, layanan, dan versi layanan yang dibutuhkan.
5. Tahap ke lima yaitu menjalankan skrip pada Nmap dengan perintah "nmap -script smb-enum-*user*s.nse -p 445" dengan alamat IP target yang dituju yaitu 192.168.75.132/24. Perintah "nmap -script smb-enum-*user*s.nse -p 445 192.168.75.132" digunakan untuk melakukan pemindaian pada *port* 445 (*port default* untuk layanan SMB - *Server* Message Block) pada host dengan alamat IP 192.168.75.132/24, dan menjalankan skrip Nmap smb-enum-*user*s.nse untuk mengidentifikasi dan menampilkan daftar pengguna (*user*s) yang mungkin ada dalam layanan SMB di host tersebut.
6. Tahap ke enam yaitu melakukan pemindaian pengguna yang terdaftar pada *server* SMB, lalu mendapatkan semua informasi pengguna di *server* SMB.
7. Tahap ke tujuh yaitu melakukan pengaturan modul dan alamat IP target dengan *tool* Msfconsole untuk menyerang *port* 21 FTP. Modul yang digunakan adalah vsftpd_234_*backdoor*, digunakan untuk mengeksploitasi kerentanan *backdoor* pada layanan FTP vsftpd versi 2.3.4 yang memungkinkan penyerang mendapatkan akses root ke sistem target tanpa perlu otentikasi yang sah. Alamat IP targetnya yaitu 192.168.75.132/24. Msfconsole merupakan sebuah console dari Metasploit Framework yang digunakan untuk melakukan uji eksploitasi dan mengembangkan keamanan jaringan. Msfconsole menyediakan antarmuka teks yang kuat dan fleksibel yang memungkinkan peneliti keamanan dan penyerang untuk menjalankan modul eksploitasi, payload, dan skrip untuk menguji dan mengevaluasi kerentanan di berbagai sistem atau jaringan.
8. Tahap yang terakhir adalah target menerima serangan *backdoor* dari modul yang telah ditentukan, lalu

mendapatkan hak akses ke root melalui *port* 21 FTP ditandai dengan session yang terbuka.



GAMBAR IV.4
Data Flow Diagram

G. Pengukuran *Time Walkthrough*

Pengukuran waktu dalam walkthrough pertama mencakup tindakan mengamati, mencatat, dan menghitung durasi setiap perintah yang dieksekusi. Hasil pengukuran waktu dari setiap perintah dalam walkthrough pertama mencakup *real time*, *user time*, dan *system time*. Hasil *time walkthrough* pertama adalah sebagai berikut.

TABEL IV.4
Time Walkthrough

No.	*Command*	***Time walkthrough* satu (satuan detik/s)**		
		real	***user***	***sys***
1	netdiscover -r []	18,49	0,01	0,06
2	nmap -p- -sV -O []	139,26	1,23	3,33
3	nmap -script smb-enum-users.nse -p 445 []	0,66	0,41	0,24
4	service postgresql start	3,68	0,02	0,01
5	service postgresql status	2,91	0,01	0
6	msfconsole : - search vsftpd 2.3.4 - use exploit/unix/ftp/vsftpd_234_backdoor - show options - set RHOSTS [] - exploit	695,79	14,27	4,86
Total		860,79	15,95	8,5
Total dengan satuan menit		14,35	0,27	0,142

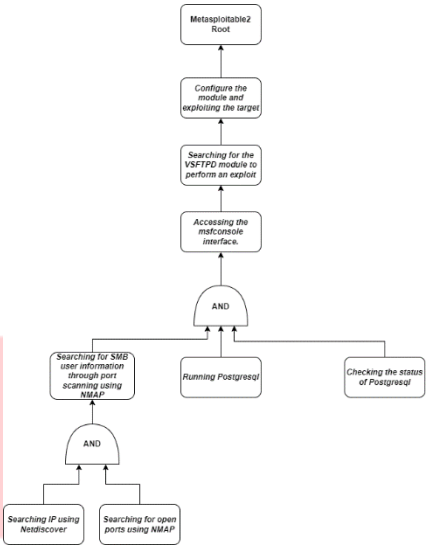
Berdasarkan *time walkthrough* pertama, terdapat total waktu dalam satuan detik sebagai berikut.

- *Real time* : 860,79 s
- *User time* : 15,95 s
- *System time* : 8,5 s

V. ANALISIS

A. *Attack Tree* Berdasarkan *SAND Gate*

Attack tree memberikan sejumlah keuntungan, termasuk mendukung evaluasi risiko ancaman, penilaian serangan, dan memberikan pemahaman dari sudut pandang pelaku serangan. Hasil *attack tree* yang dibuat berdasarkan *walkthrough* pertama dengan pendekatan SAND *gate* adalah sebagai berikut.



GAMBAR V.1
Attack Tree Berdasarkan *Walkthrough* Pertama Dengan Pendekatan Sand *Gate*

Penjelasan dari *attack tree* berdasarkan *walkthrough* pertama dengan pendekatan SAND *gate* adalah sebagai berikut.

1. *Goals and Contexts*

Dalam *attack tree* berdasarkan *walkthrough* satu ini, target serangannya adalah *priviledge environment access* atau root dari *vulnerable machine* Metasploitable2. Dengan root sendiri berarti memiliki akses penuh dan kontrol atas seluruh sistem, termasuk berkas, direktori, konfigurasi, proses, dan pengaturan sistem lainnya.

2. *Target*

Dalam *attack tree* berdasarkan *walkthrough* satu ini, target serangannya adalah *priviledge environment access* atau root dari *vulnerable machine* Metasploitable2. Dengan root sendiri berarti memiliki akses penuh dan kontrol atas seluruh sistem, termasuk berkas, direktori, konfigurasi, proses, dan pengaturan sistem lainnya.

3. *Attack Level*

Attack tree pada *walkthrough* satu ini berfokus melakukan serangan pada *port* 21 FTP. Penyerangan tersebut dilakukan dengan *tools* Msfconsole modul VSFTPD 2.3.4. Alasannya karena *port* 21 FTP merupakan salah satu *port* yang terbuka pada *vulnerable machine* Metasploitable2.

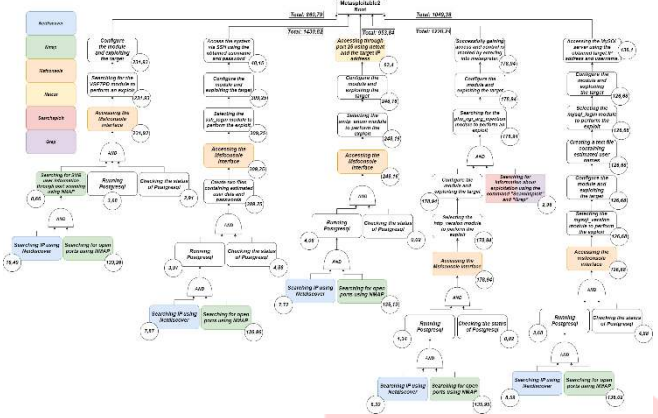
4. *Node*

Penjelasan dari setiap simpul atau *node* pada *attack tree* berdasarkan *walkthrough* pertama.

a. Searching IP using Netdiscover
b. Searching for open port using Nmap
c. Searching for SMB user information through port scanning using Nmap
d. Running Postgresql
e. Checking the status of Postgresql
f. Accessing the Msfconsole interface
g. Searching for the VSFTPD module to perform an exploit
h. Configure the module and exploiting the target
i. Metasploitable2 Root

B. Pemeringkatan Berdasarkan *Metrics*

Pemeringkatan dilaksanakan dengan membandingkan lima *attack tree* berdasarkan *walkthrough*, menggunakan tiga metrik, yaitu *time metric, cost metric,* dan *frequency metric.*



GAMBAR V.2
Pemeringkatan Berdasarkan *Metrics*

Hasil pemeringkatan *time metric, cost metric,* dan *frequency metric* berdasarkan lima *attack tree* adalah sebagai berikut.

1. Pemeringkatan Berdasarkan *Time Metric*

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

TABEL V.1
Pemeringkatan Berdasarkan Time Metric

Ranking	*Attack tree*	*Time metric(s)*
1	*Attack tree* WT 1	860,79
2	*Attack tree* WT 3	953,84
3	*Attack tree* WT 5	1049,38
4	*Attack tree* WT 4	1220,24
5	*Attack tree* WT 2	1430,82

Hasil pemeringkatan *time metric* dapat disimpulkan bahwa, *attack tree* WT 1 memiliki waktu tempuh yang paling singkat dibandingkan dengan yang lainnya, sehingga menduduki peringkat pertama. Hal ini disebabkan oleh kecepatan waktu pada setiap proses dalam *attack tree* WT 1 yang lebih cepat dibandingkan dengan yang lainnya. Selain itu, penggunaan *tool* pada *attack tree* WT 1 juga menjadi faktor kunci yang menyebabkan kecepatan tersebut.

2. Pemeringkatan Berdasarkan *Cost Metric*

Cost metric adalah ukuran atau metrik yang digunakan untuk mengukur biaya yang terlibat dalam suatu tugas, proses, atau aktivitas. Dalam penelitian ini, *cost metric* dihitung dari jumlah aktivitas dari awal hingga selesai pada *activity diagram.* Hasil yang diperoleh dari pemeringkatan berdasarkan *cost metric* adalah sebagia berikut.

TABEL V.2
Pemeringkatan Berdasarkan Cost Metric

Ranking	*Attack tree*	*Cost metric(step)*
1	*Attack tree* WT 1	20
2	*Attack tree* WT 3	22
3	*Attack tree* WT 2	29
4	*Attack tree* WT 4	30
5	*Attack tree* WT 5	31

Hasil pemeringkatan *cost metric*, *Attack tree WT* 1 menjadi jalur paling cepat dibandingkan dengan yang lainnya. Proses dari awal hingga selesai pada *attack tree* WT 1 hanya memiliki *cost* sebesar 20 saja, sehingga dapat menjadikannya sebagai peringkat pertama, disusul dengan *attack tree* WT 3 dengan *cost* sebesar 22, *attack tree* WT 2 sebesar 29, *attack tree* WT 4 sebesar 30, dan *attack tree* WT 5 sebesar 31.

3. Pemeringkatan Berdasarkan *Frequency Metric*

Frequency metric merupakan ukuran atau metrik yang mengukur seberapa sering suatu alat atau *tool* digunakan dalam aktivitas keamanan. Pada penelitian ini, *frequency metric* dihitung dari seberapa sering sebuah *tools* digunakan pada setiap *attack tree* berdasarkan lima *walkthrough*. Hasil yang diperoleh dari pemeringkatan berdasarkan *frequency metric* adalah sebagai berikut.

TABEL V.3
Pemeringkatan Berdasarkan Frequency Metric

Ranking	*Tools*	*Frequency of Use*
1	Netdiscover	5 (*All walkthroughs use it*)
	Nmap	
	Msfconsole	
2	Netcat	1 (*Only used in one walkthrough*)
	Searchsploit	
	Grep	

Hasil Pemeringkatan *Frequency metric*, terdapat tiga *tools* yang menduduki peringkat pertama yaitu Netdiscover, Nmap, dan Msfconsole. Hal itu dikarenakan ketiga *tools* tersebut digunakan pada lima *attack tree*. Sedangkan, posisi peringkat ke dua memiliki tiga *tools* yaitu Netcat, Searchsploit, dan Grep. Ketiga *tools* yang menduduki peringkat ke dua tersebut hanya digunakan dalam satu *attack tree* saja. Netcat digunakan pada *attack tree* WT 3, Searchsploit dan Grep digunakan pada *attack tree* WT 4.

Khusus untuk Msfconsole digunakan pada lima *attack tree*, tetapi dengan modul yang berbeda-beda. Untuk *attack tree* WT 1 menggunakan Msfconsol dengan modul vsftpd 2.3.4, pada *attack tree* WT 2 menggunakan Msfconsole dengan modul ssh_login, pada *attack tree* WT 3 menggunakan Msfconsole dengan modul smtp_enum, pada *attack tree* WT 4 menggunakan Msfconsole dengan modul http_version dan php_cgi_arg_injection, dan yang terakhir pada *attack tree* WT 5 menggunakan Msfconsole dengan modul mysql_version dan mysql_login. Modul-modul tersebut memiliki fungsinya masing-masing sesuai dengan kebutuhannya.

4. Pemeringkatan Berdasarkan Perhitungan *Time Metric* dan *Cost Metric*

Analisis pemeringkatan berdasarkan perhitungan *metrics* gabungan (*time metric* dan *cost metric*) ini bertujuan untuk mendapatkan pemahaman lebih tentang sudut pandang seorang penyerang dari aksi penyerangan yang terjadi

berdasarkan *attack tree* dari lima *walkthrough* yang telah dipilih.

TABEL V.4
Pemeringkatan Berdasarkan Seluruh Metric

Attack tree	*Time metric (s)*	*Cost metric (step)*
Attack tree WT 1	860,79	20
Attack tree WT 2	1430,82	29
Attack tree WT 3	953,84	22
Attack tree WT 4	1220,24	30
Attack tree WT 5	1049,38	31

Hasil Pemeringkatan dari *Metrics* gabungan *Time metric* dan *Cost metric* dalam penggunaan ke dua *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* 860,79s atau 14,35 menit dan *cost metric* sebesar 20 langkah.

VI. KESIMPULAN

Dengan menggunakan *activity diagram* dan *data flow diagram*, membuat semua alur dari eksploitasi berdasarkan lima *walkthrough* pada *vulnerable machine* Metasploitable2 menjadi lebih mudah dipahami. Terdapat dua aktor dalam *activity diagram* pada penelitian ini yaitu Kali Linux sebagai alat untuk melakukan penyerangan dan Metasploitable2 sebagai alat untuk target uji coba penyerangan. Pendekatan SAND *gate* dari lima *walkthrough* yang telah dipilih dapat digunakan dalam penyusunan *attack tree* untuk mendapatkan jalur penyerangan dengan waktu tempuh tercepat dalam mencapai *privileged environment access*. *Attack tree* WT 1 menjadi peringkat pertama berdasarkan perhitungan *time metric* dan *cost metric*, karena menjadi jalur paling cepat dan terpendek dengan total *real time* 860,79 s dan total *cost metric* 20 langkah untuk melakukan eksploitasi dengan tujuan untuk mendapatkan *priviledge environment access*. Netdiscover, Nmap, dan Msfconsole menjadi peringkat pertama karena merupakan *tools* yang digunakan pada semua *attack tree* berdasarkan lima *walkthrough* yang telah dipilih. Khusus untuk Msfconsole digunakan pada semua *walkthrough,* tetapi dengan modul yang berbeda-beda sesuai dengan kebutuhan pada *walkthrough* tersebut.

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

[6] 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

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

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

[9] 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

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

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