Implementasi dan Analisa *Attack Tree* pada *Vulnerable Machine* Sunset: 1 Berdasarkan Pendekatan Cubesat *Security Attack Tree Analysis* dan Sand *Gate*

1st Wahyu Limutu
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
wahyulimutu@student.telkomuniversity.ac.id

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

3rd Ahmad Almaarif
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
ahmadalmaarif@telkomuniversity.ac.id

Abstrak—Penelitian ini mengimplementasikan dan menganalisa *attack tree* pada Sunset: 1 *vulnerable machine* dengan menggunakan pendekatan CubeSat *Security* Attack *Tree Analysis* dan SAND *gate*. *Analisa attack tree* juga menggunakan perhitungan tiga komponen yaitu time *metric*, *cost metric*, dan *frequency metric*. Skenario eksploitasi pada *walkthrough* yang digunakan, memiliki tahapan yang sama. Tahapan tersebut adalah information gathering, scanning, enumeration, *exploitation*, dan *privilege escalation*. Dari proses tersebut bisa digambarkan *activity* diagram dan *attack tree*. Activity diagram digunakan sebagai dasar perhitungan cost *metric* dengan menghitung jumlah langkah yang ada di dalamnya. *Attack tree* mewakili berbagai tahapan eksploitasi dan dilakukan perangkingan berdasarkan *metrics*. *Metrics* tersebut menjadi dasar untuk mendapatkan perangkingan *attack tree*. Berdasarkan *time metric*, *attack tree* 1 merupakan jalur tercepat jika dibanding *attack tree* lainnya dengan nilai real time sebesar 64,895 detik. Berdasarkan *cost metric*, *attack tree* 1, 3, dan 4 memiliki nilai *cost* yang rendah dibandingkan *attack tree* lainnya dengan nilai *cost* 15. Berdasarkan *frequency metric*, *attack* tools John The Ripper dan Netdiscover memiliki persentase terbesar dalam penggunaannya di *attack tree* sebesar 40% dan 30% secara berurutan. Kelanjutan dari penelitian ini dapat dilakukan dengan menambahkan faktor kerentanan dengan melakukan pemindaian celah keamanan pada sistem.

Kata kunci— sunset: 1, *attack tree*, *time*, *cost*, *frequency*

I. PENDAHULUAN

Data-data komputer merupakan data yang berharga karena mengandung informasi penting. Oleh sebab itu dibutuhkan keamanan informasi untuk melindungi data-data tersebut. Keamanan informasi merupakan proses memproteksi informasi dan sistem informasi dari pengaksesan, pemakaian, pemublikasian, perubahan, atau perusakan secara ilegal [1]. Salah satu fungsi nyata dari keamanan informasi adalah untuk mengantisipasi penipuan atau menyadari penipuan pada sebuah sistem yang memiliki basis informasi, yang informasinya tidak memiliki arti fisik. Jika terdapat celah keamanan informasi, maka dengan mudah penyerang akan memanfaatkannya untuk masuk ke dalam sistem.

Penyerang adalah pelaku dalam tindakan mengidentifikasi dan mengeksploitasi kerentanan dalam sistem komputer atau jaringan, biasanya untuk mendapatkan akses tidak sah ke data pribadi atau organisasi [2]. Dengan semakin majunya teknologi, penyerang bisa memakai banyak jalur untuk memanfaatkan celah keamanan sistem komputer atau jaringan dengan tujuan mendapat keuntungan untuk dirinya sendiri. Pilihan terbaik yang bisa dipakai oleh penyerang untuk melalui jalur tercepat dalam peretasan adalah dengan memakai *attack tree*.

Attack tree adalah struktur data bercabang dan hierarkis yang mewakili serangkaian pendekatan potensial untuk mencapai suatu peristiwa di mana keamanan sistem ditembus atau disusupi dengan cara tertentu [3]. *Attack tree* memiliki bagian yang akan dihitung nilainya, bagian itu disebut metrics [4]. Perhitungan *metrics* diantaranya yaitu *time, cost, frequency, probability to successfully attack, skill level needed for attacks, special equipment needed for attacks,* dan *combinations of the above metrics* [4]. Hasil perhitungan dari *metrics* akan dijadikan landasan untuk perangkingan *attack tree*.

Penelitian ini bertujuan untuk mengetahui perumusan *attack tree* dengan menggunakan pendekatan CubeSat *Security Attack Tree Analysis* dan SAND-*gate*, serta mengetahui *attack tree* tercepat berdasarkan analisa *metrics.* Bagi penyerang, *attack tree* tercepat bisa digunakan untuk melakukan eksploitasi pada sistem dengan alokasi waktu sesedikit mungkin. Bagi pengelola server, *attack tree* bisa digunakan sebagai dasar penguatan keamanan sistem dengan menganalisis cara-cara di mana sistem dapat diserang. Perumusan *attack tree* ini menggunakan *vulnerable machine* Sunset: 1. Sunset: 1: adalah sebuah *vulnerable machine* sederhana yang dirilis oleh whitecr0wz pada 29 Juli 2019 di situs web vulnhub.com dengan tujuan memperkaya pengalaman dalam segmen eksperimen dan *penetration testing*.

II. KAJIAN TEORI

A. Keamanan Sistem Informasi

Karena komputer dan perangkat digital lainnya menjadi bagian yang sangat penting untuk bisnis, perdagangan, dan berbagai aspek kehidupan lainnya, kemungkinan mereka untuk diserang semakin tinggi. Agar bisnis atau individu dapat menggunakan perangkat komputasi dengan percaya

diri, pertama-tama mereka harus memastikan bahwa perangkat tersebut tidak disusupi dengan cara apa pun dan bahwa semua komunikasi aman [5].

B. *Threat*

Threat adalah ancaman terhadap suatu sistem yang biasanya diidentifikasi oleh kerentanan yang ada di jaringan [6]. Untuk menanggulangi ancaman terhadap sistem, bisa menggunakan teknik pencegahan ancaman untuk yang dinamakan *countermeasures* [7].

C. Eksploitasi

Mengeksploitasi berarti mengambil keuntungan secara paksa. Mengeksploitasi adalah menggunakan kerentanan target untuk keuntungannya sendiri [8]. Eksploitasi komputer adalah serangan terhadap sistem komputer, terutama yang memanfaatkan celah keamanan tertentu [9].

D. Eksperimen

Dalam bentuknya yang paling sederhana, penelitian eksperimental melibatkan perbandingan dua kelompok pada satu ukuran hasil untuk menguji beberapa hipotesis mengenai sebab-akibat [10]. Eksperimen adalah sebagai suatu penelitian ilmiah dimana peneliti memanipulasi dan mengontrol satu atau lebih variabel bebas dan melakukan pengamatan terhadap variabel-variabel terikat untuk menemukan variasi yang muncul bersamaan dengan manipulasi terhadap variabel bebas tersebut [11].

E. *Walkthrough*

Walkthrough adalah panduan teknis yang berisi langkah dan prosedur dalam penyerangan untuk terlibat langsung dengan antarmuka aplikasi dalam memeriksa mekanisme teknologinya [12]. Panduan teknis berarti di dalam *walkthrough* langsung menyebut target yang akan diserang dan daftar *tools* yang dipakai secara rinci, berbeda dengan *attack vector* yang sekadar konsep

F. Lubuntu

Lubuntu adalah sistem operasi *open-source* yang merupakan varian dari Ubuntu yang menggunakan lingkungan *desktop environment*. Pada penelitian ini Lubuntu digunakan sebagai penyerang

G. *Vulnerable Machine* Sunset: 1

Vulnerable machine adalah mesin kerentanan yang dilengkapi dengan celah keamanan yang dibuat sebagai wadah untuk mempraktikkan pengujian penetrasi umum [13]. Sunset: 1 adalah sebuah *vulnerable machine* sederhana yang dirilis oleh whitecr0wz pada 29 Juli 2019 di situs web vulnhub.com dengan tujuan memperkaya pengalaman dalam segmen eksperimen dan *penetration testing*. Sunset: 1 merupakan edisi pertama dari series Sunset yang dibuat oleh pengembangnya.

H. *Activity Diagram*

Activity diagram adalah diagram konseptual yang digunakan untuk mengeksplorasi dan menggambarkan alur kerja, tindakan yang dilakukan dalam sebuah operasi, mirip dengan diagram alur program tradisional. Selain itu, *Activity diagram* digunakan untuk menggambarkan proses bisnis, alur kerja dalam konteks organisasi.

I. *Data Flow Diagram*

Data flow diagram adalah artefak utama dan wajib dibuat untuk setiap sistem dalam pendekatan terstruktur. Ini memiliki struktur hierarki, yang memberikan tingkat abstraksi yang berbeda, berguna dalam perancangan sistem. Selain itu, *data flow diagram* adalah artefak mendasar yang dengan jelas menunjukkan struktur suatu sistem. Artefak lain menggunakan informasi yang disediakan oleh *data flow diagram* untuk merepresentasikan aspek dinamis dari sistem [14].

J. Pengukuran *Walkthrough*

Pengukuran merupakan kegiatan membandingkan antara suatu besaran dengan besaran lain yang dijadikan acuannya. Pengukuran dapat didefinisikan sebagai suatu kegiatan untuk menetapkan besaran, dimensi, atau kapasitas yang dibandingkan dengan acuan yang digunakan sebagai standar. Pengukuran *walkthrough* adalah kegiatan perhitungan elemen pada *walkthrough* berdasarkan satuan yang sudah ada. Aspek yang diukur yaitu, *time, cost*, dan *frequency* dari penggunaan *tools*.

K. *Attack Tree*

Attack tree merupakan salah satu cara untuk menggambarkan bagaimana suatu sistem dapat diserang secara sistematis [15]. *Attack tree* berbentuk diagram konseptual yang memiliki struktur hierarkis dan representasi intuitif dari skenario serangan multi-langkah untuk menunjukkan bagaimana target dapat diserang [4].

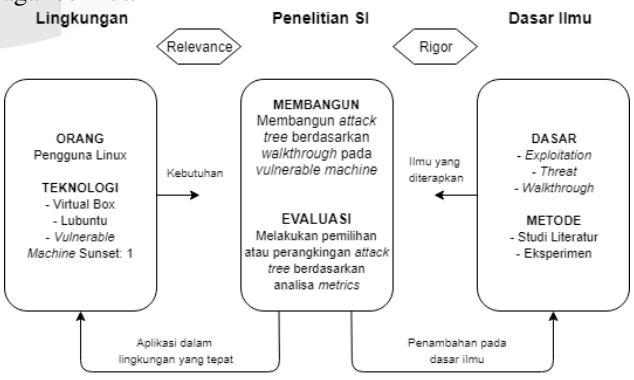
L. *Metrics*

Metrics adalah bagian dari *attack tree* yang akan dihitung nilainya [4]. Hasil perhitungan dari *metrics* ini akan dijadikan landasan untuk perangkingan *attack tree*. *Metrics* yang dipakai dalam penelitian ini adalah *time, cost*, dan *frequency* dari penggunaan *tools*.

III. METODE

A. Model Konseptual

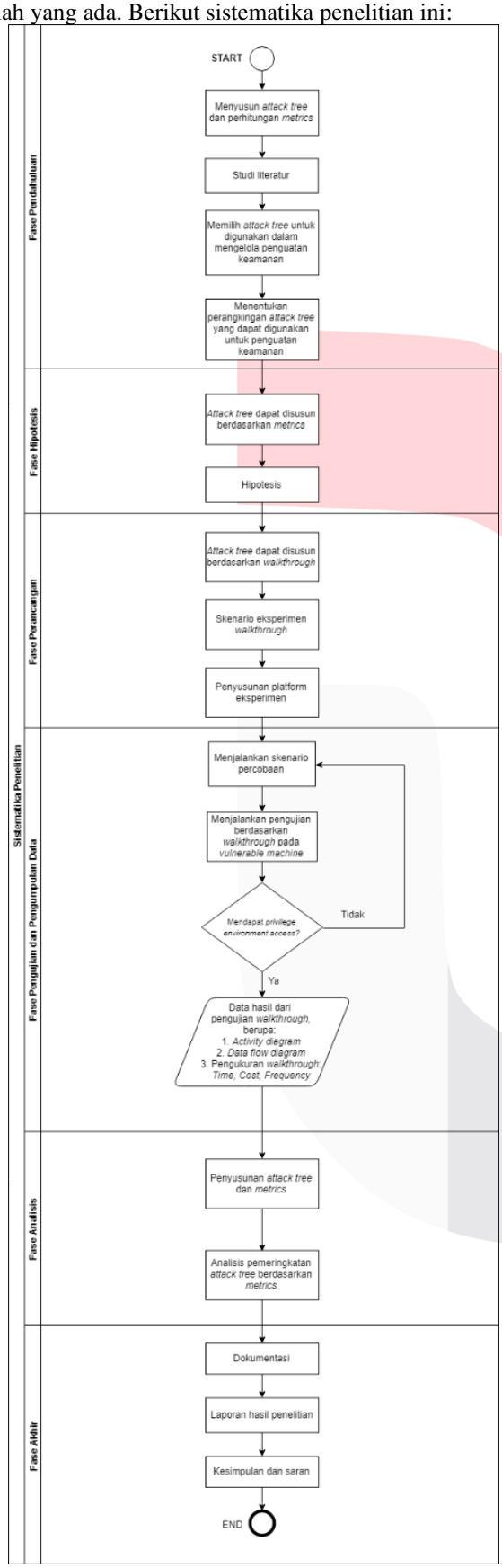
Model konseptual adalah gambaran untuk memahami, melaksanakan, dan mengevaluasi penelitian sistem informasi [16]. Model konseptual juga merupakan sudut pandang penulis yang memudahkan penyelesaian rumusan masalah yang dihadapi. Model konseptual penelitian ini adalah sebagai berikut:



GAMBAR III.1
MODEL KONSEPTUAL

B. Sistematika Penyelesaian Masalah

Sistematika penelitian berisi tentang bagaimana alur penelitian dari awal sampai akhir untuk menyelesaikan masalah yang ada. Berikut sistematika penelitian ini:



GAMBAR III.2
SISTEMATIKA PENYELESAIAN MASALAH

IV. HASIL DAN PEMBAHASAN

Untuk mencapai tujuan penelitian eksperimen berupa pengujian penetrasi berdasarkan *walkthrough*, memerlukan *hardware* dan *software*. *Hardware* dan *software* digunakan sebagai sarana pengumpulan data. Lingkungan sistem yang digunakan adalah Lubuntu dan *vulnerable machine* Sunsetv1 sebagai wadah eksperimen.

A. *Hardware*

TABEL IV.1
HARDWARE

Komponen	**Informasi**	
Spesifikasi Perangkat Keras: Asus Vivobook S14 A411UF	*Processor*	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz (8 CPUs), ~1.8GHz
	Memory	8GB RAM
	System Type	*64-bit operating system, x64-based processor*
	Operating System	*Windows 11 Home Single Language 64-bit* (*Main* OS)
	Hard Disk	1TB

B. *Software*

Software di bawah ini merupakan sarana dan prasarana yang digunakan menguji dan mendapatkan data tentang celah keamanan. Beberapa software berikut dikelompokkan menjadi *operating system, IT asset, attack tools,* dan *vulnerability scanner*. Berikut rinciannya:

TABEL IV.2
SOFTWARE

Type	***Software***	***Version***
Operating System	Lubuntu • *Base memory*: 1024 MB • *Network: Bridge Adaptor*	18.04
IT Asset	*Vulnerable Machine* Sunset • *Base memory*: 1024 MB • *Network: Bridge Adaptor*	1
Attack Tools	Nmap	7.60
	Netdiscover	0.3
	Arp-scan	1.9
	John The Ripper	1.8.0

Eksperimen pada TA ini menggunakan *operating system, IT asset, attack tools,* dan *vulnerability scanner*. Rincian *tools* yang dipakai adalah seperti di bawah ini:

1. *Operating System*
   a. Lubuntu
      Lubuntu adalah sistem operasi *open-source* yang merupakan varian dari Ubuntu yang menggunakan lingkungan *desktop environment*. Pada penelitian ini Lubuntu digunakan sebagai penyerang
2. *IT Asset*
   a. Sunset: 1
      Sunset: 1 adalah sebuah *vulnerable machine* yang dibuat dengan tujuan memperkaya pengalaman dalam segmen eksperimen. Sunset: 1 dirancang memiliki kerentanan pada layanan sistemnya agar bisa digunakan sebagai objek eksploitasi.
3. *Attack Tools*
   a. Nmap
      Nmap adalah *tool* yang biasa digunakan untuk melakukan pemindaian *port*.
   b. Netdiscover

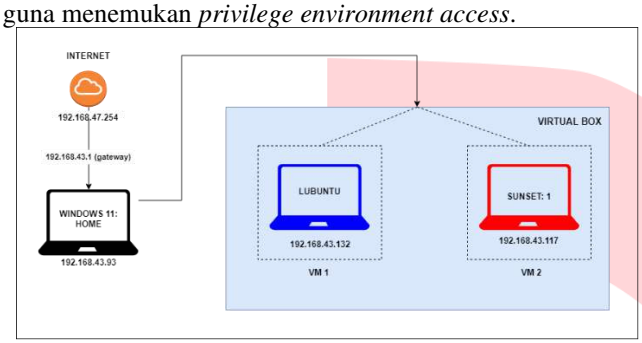
Netdiscover adalah *tool* yang dipakai untuk menampilkan mana saja host yang sedang aktif dalam jaringan local.

c. Arp-scan
Arp-scan adalah *tool* perintah CLI yang digunakan untuk memantau identitas host yang tersambung ke dalam jaringan.

d. John The Ripper
John The Ripper adalah *open-source tool* yang dipakai untuk mengaudit keamanan kata sandi yang tersedia untuk banyak sistem operasi.

C. Platform Eksperimen

Untuk menjalankan pengujian pada *vulnerable machine* guna menemukan *privilege environment access*.



GAMBAR IV.1
PLATFORM EKSPERIMEN

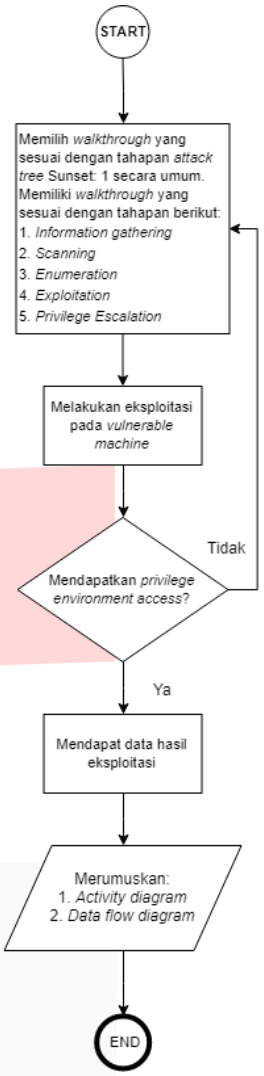
D. Daftar IP Address

TABEL IV.3
DAFTAR IP ADRESS

Type	***Software***	***Default Gateway***	***IP Address***
Main OS	Windows 11	192.168.43.1	192.168.43.93
VM1	Lubuntu		192.168.43.132
VM2	Sunset		192.168.43.117

E. Skenario Perumusan *Activity Diagram* dan *Data Flow Diagram* Berdasarkan Pengujian *Walkthrough*

Di bawah ini adalah skenario pengujian yang digunakan:



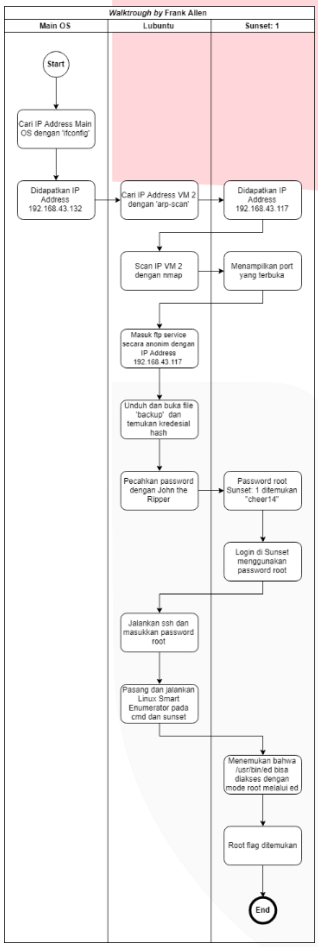
GAMBAR IV.2
SKENARIO PERUMUSAN *ACTIVITY DIAGRAM* DAN *DATA FLOW DIAGRAM* BERDASARKAN PENGUJIAN *WALKTHROUGH*

F. *Activity diagram*

Activity diagram digunakan untuk menunjukkan langkah-langkah menuju *privilege environment access.* Percobaan pertama pada penelitian ini menggunakan *walkthrough* dari Frank Allen.

1. Pertama memindai alamat IP pada *Main OS* dengan menjalankan perintah CLI *ifconfig*.
2. Pada tahap ke dua didapatkan alamat IP Main OS.
3. Ke tiga, pastikan Sunset sudah menyala dengan menggunakan *arp-scan* sekaligus mendapatkan alamat IP-nya. Jika ada, maka Sunset sudah tergabung dalam satu jaringan.
4. Didapatkan alamat IP dari Sunset.
5. Gunakan nmap untuk memindai port *Transmission Control Protocol* (TCP) spesifik mana saja yang terbuka pada alamat IP Sunset.
6. Selanjutnya mendapatkan port yang terbuka.
7. Masuk ke dalam mode *root* dan jalankan ftp service dengan menggunakan alamat IP Sunset yang telah didapatkan sebelumnya.
8. Masih di dalam ftp, tampilkan daftar file apa saja yang ada di dalamnya. Ditemukan bahwa ada file backup, kemudian unduh.

9. Jalankan *John The Ripper password cracker* yang sudah diinstal sebelumnya untuk mendapatkan *password* dari Sunset.
10. Setelah itu, *password* Sunset ditemukan dan bisa digunakan untuk proses lebih lanjut.
11. Login di direktori Sunset menggunakan *root password* yang didapatkan sebelumnya.
12. Jalankan ssh dengan memasukan *root password* sebagai autentikasi agar bisa masuk.
13. Jalankan Linux Smart Enumerator pada cmd Lubuntu dan direktori Sunset.
14. Ditemukan bahwa /usr/bin/ed bisa diakses dengan mode *root* melalui ed
15. *Privileged environment access* berhasil ditemukan.

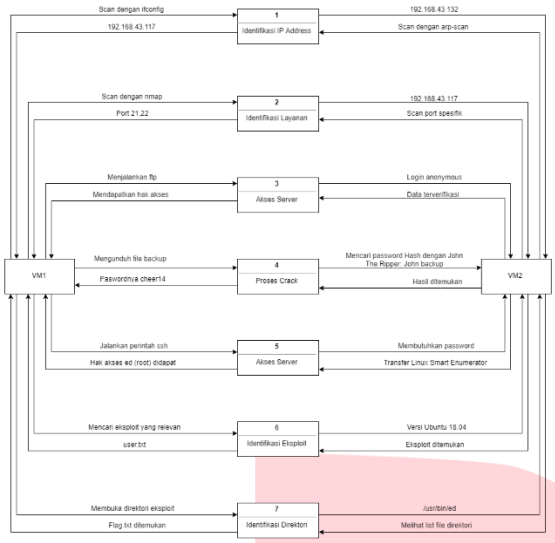


GAMBAR IV.3
ACTIVITY DIAGRAM DARI *WALKTHROUGH* FRANK ALLEN

G. *Data flow diagram*

Data flow diagram merupakan diagram yang berisi data masukan dan data keluaran untuk menuju *Privilege Environment Access*. Percobaan pertama pada penelitian ini menggunakan *walkthrough* dari Frank Allen.

1. Tahap pertama, pindai alamat IP dari *Main OS* dengan *ifconfig* lalu didapatkan IP 192.168.43.132. *Command ifconfig* digunakan untuk memindai IP *address* pada *OS*.
2. Tahap ke dua lakukan pemindaian menggunakan *command* arp-scan -l untuk mengetahui *host discovery* yang terhubung ke sistem. Dari pemindaian ini didapatkan alamat IP Sunset yaitu 192.168.43.117. *Command arp-scan* digunakan untuk melihat identitas *host* yang tersambung dengan komputer utama, semisal *vulnerable machine* tersambung ke *Main OS*.
3. Tahap ke tiga gunakan nmap sebagai *tool* pemindaian untuk melihat mana saja port TCP yang terbuka. *Command* nmap yang dipakai adalah ./nmapAutomator.sh 192.168.43.117 All. Ditemukan bahwa *port* yang terbuka adalah *port* 21 dan 22.
4. Tahap ke empat masuk ke akses ftp 192.168.43.117 dengan *login* menggunakan *user* anonymous dan *null password (enter).* Masuk ke ftp dengan *anonymous* dilakukan untuk mengakses file yang ada di direktori secara anonim.
5. Tahap ke lima tampilkan isi dari direktori ftp terdapat file *backup* yang kemudian diunduh. Setelah file *backup* dibuka, ditemukan bahwa ada kredensial *hash* untuk setiap pengguna di mesin Sunset.
6. Tahap ke enam yaitu memecahkan file *backup* menggunakan John The Ripper untuk mencari *password* dari *user* sunset. *Command* yang digunakan adalah john backup. Setelah itu ditemukan *password* sunset "cheer14". John The Ripper biasa digunakan untuk memecahkan dan atau mengecek kekuatan *password*.
7. Tahap ke tujuh jalankan ssh sunset@192.168.43.117 untuk mengakses jaringan terenkripsi pada sistem Sunset. Langkahnya dengan memasukkan *password* yang didapat pada proses sebelumnya.
8. Tahap ke delapan transfer *Linux Smart Enumerator* dengan menjalankan command berbeda di Lubuntu dan ssh. Pada lubuntu jalankan python -m SimpleHTTPServer 1234, sedangkan pada ssh jalankan:
   wget http://192.168.43.117:1234/lse.sh
   chmod +x lse.sh
   ./lse.sh
   Ditemukan bahwa "ed" bisa dijalankan sebagai *root*.
9. Tahap ke sembilan mencari eksploit yang relevan, lalu ditemukanlah file user.txt.
10. Tahap ke sepuluh buka direktori /usr/bin/ed, jalankan sudo ed test dan !/bin/bash untuk masuk ke mode *root*.
11. Tahap terakhir yaitu jalankan *command* cat /root/flag.txt untuk menampilkan isinya, dengan begitu *privileged environment access* berhasil didapatkan



GAMBAR IV.4
DATA FLOW DIAGRAM DARI *WALKTHROUGH* FRANK ALLEN

H. Pengukuran Time Walkthrough

Pengukuran *Time* pada *walkthrough* dilakukan untuk mendapatkan *real time, user time,* dan *system time*. Berikut merupakan pengukuran *Time* dari *walkthrough* Frank Allen:\

TABEL IV.4
PENGUKURAN *TIME* DARI *WALKTHRPUGH* FRANK ALLEN

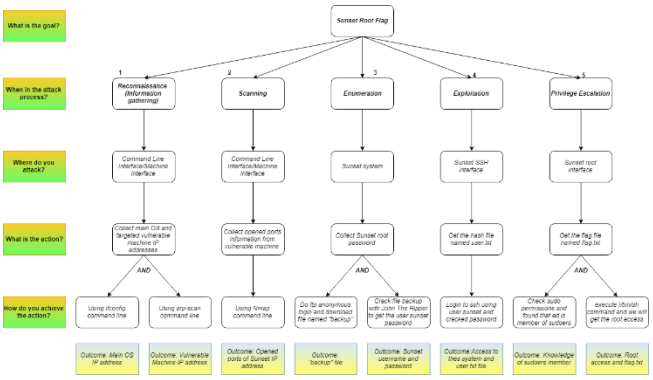
Step (Command)	***Time (s)***			***Hosts Scanned Time (s)***
	Real	***User***	***System***	
Ifconfig	0,183	0,005	0,001	*null*
Arp-scan -l	1,886	0,16	0,007	1,883
Nmap	13,116	1,35	0,106	13,11
Ftp	25,769	0,001	0,014	*null*
Login (anonymous)	6	0	0	*null*
Get backup	0,19	0	0	*null*
File backup	0,486	0,003	0	*null*
Vim backup	0,002	0,001	0,001	*null*
John backup	11,5	0	0	*null*
Ssh sunset login with password	5,454	0,603	0	*null*
Cat user.txt	0,003	0	0	*null*
Ed	0,002	0	0	*null*
Id	0,003	0	0	*null*
Cd root	0,002	0	0	*null*
Cat flag.txt	0,389	0	0	*null*
Total	**64,895**	**2,126**	**0,126**	**14,993**

null: nilainya tidak muncul pada hasil *scanning*.

V. ANALISIS

A. *Attack Tree*

Attack tree merupakan salah satu cara untuk menggambarkan bagaimana suatu sistem dapat diserang secara sistematis (Mauw & Oostdijk, 2006). *Attack tree* berbentuk diagram konseptual yang memiliki struktur hierarkis dan representasi intuitif dari skenario serangan multi-langkah untuk menunjukkan bagaimana target dapat diserang (Kuipers, 2020). Berikut ini adalah *attack tree* 1 berdasarkan *walkthrough* dari Frank Allen:

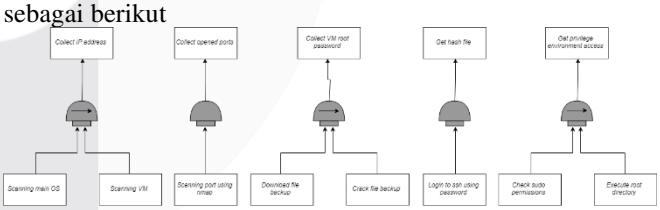


GAMBAR V.1
ATTACK TREE BERDASARKAN *WALKTHROUGH FRANK ALLEN* VERSI CUBESAT

Secara keseluruhan, *attack tree* dalam penelitian ini memiliki rincian sebagai berikut:

1. *What is the goal?*
   Bertujuan untuk mengambil alih sistem dari *vulnerable machine* Sunset: 1, dengan mengakses *root privileged environment access.*
2. *Where do you attack?*
   Penyerangan dilakukan pada level sistem operasi pada *vulnerable machine* Sunset: 1.
3. *What is the action?*
   Mengambil alih *root privileged environment access.*
4. *How do you achieve the action?*
   Aksi untuk mendapat *privileged environment access* langkah yang dilakukan secara berurutan yaitu memindai IP *address* dan *port* yang terbuka, masuk melalui ftp, menyambungkan sistem melalui ssh, dan memanfaatkan *sudo rights*.
5. *Outcome*
   Outcome pada penelitian ini terbatas pada *privileged environment access* yang telah berhasil diambil alih oleh penyerang.

Proses berurutan dari *attack tree walkthrough* 1 (Frank Allen) lebih jelasnya dengan menggunakan SAND *gate* adalah sebagai berikut



GAMBAR V.2 *Attack Tree* Berdasarkan *Walkthrough Frank Allen* versi SAND *gate*

1. *Information gathering*
   Information gathering digambarkan menggunakan SAND gate untuk menunjukkan urutan proses pada *attack tree* dari kiri ke kanan pada setiap cabang. Simpul "*Collect IP address"* terhubung dengan cabangnya menggunakan SAND gate. Sebelum memindai IP address VM, harus memindai IP address dari main *OS*.
2. *Scanning*
   Pada tahap *scanning* ini bertujuan untuk mendapatkan port-port yang terbuka, *command* yang dipakai adalah nmap.
3. *Enumeration*

Pada *enumeration* terdapat dua Langkah yang harus dilakukan untuk mendapatkan password dari VM. Penggunaan SAND *gate* untuk menunjukkan langkah dari kiri ke kanan, sehingga yang pertama dilakukan adalah *download file backup*, baru kemudian memecahkan *password*nya menggunakan *tool*.

4. *Exploitation*

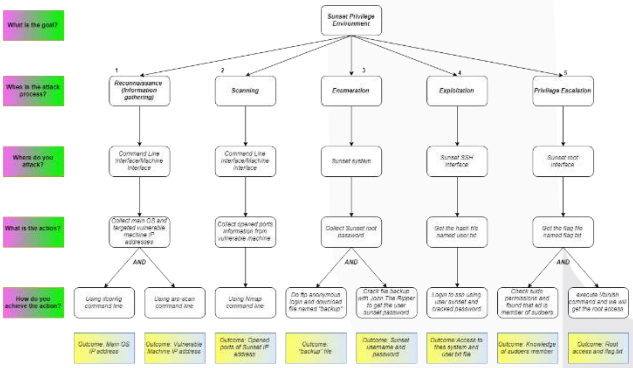
   Di tahap ini, *exploitation* bertujuan untuk mendapatkan hash file berupa file user.txt. Untuk mendapatkannya perlu dilakukan login pada ssh menggunakan password yang sudah didapat sebelumnya.

5. *Privileged Escalation*

   Privilege Escalation digambarkan menggunakan SAND gate untuk menunjukkan urutan proses pada *attack tree* dari kiri ke kanan pada setiap cabang. Tahap akhir *Privilege Escalation* bertujuan untuk mendapatkan privileged environment access. Ada dua langkah yang harus dilakukan, yaitu mengecek sudo permissions, kemudian membuka direktori root.

A.2Perumusan *Attack Tree* Gabungan Berdasarkan 5 *Walkthrough*

Tujuan dari perumusan *attack tree* gabungan ini adalah untuk menemukan estimasi waktu tersingkat dalam melakukan penyerangan terhadap *vulnerable machine* Sunset: 1. *Attack tree* gabungan tersebut digambarkan dengan pendekatan CubeSat Security *Attack Tree Analysis* dengan hasil sebagai berikut:



GAMBAR V.3
PERUMUSAN *ATTACK TREE* GABUNGAN BERDASARKAN 5 *WALKTHROUGH*

B. Analisis Perbandingan *Metrics*

Pada sub-bab ini akan dibandingkan *metrics* dari kelima *walkthrough* yang telah dicoba. *Metrics* tersebut yaitu *time, cost*, dan *frequency* dari penggunaan *tools.*

1. Analisis Perbandingan *Time Metrics*

Disini akan dijabarkan perbandingan time metric dari masing-masing *attack tree*. Karena *user time* dan *system time* merupakan bagian dari *real time*, maka hanya *real time* yang perlu dianalisis lebih lanjut. Perhitungan *time metric* menggunakan akumulasi dari *real time* yang digunakan pada *attack tree*, dengan perumusan sebagai berikut:

$$\sum_{i=1}^{n} \mathrm{r} = \mathrm{r}_1 + \mathrm{r}_2 + \ldots + \mathrm{r}_n \quad \ldots\ldots \text{(i)}$$

dimana:

r = *real time*
i = indeks penjumlahan
n = batas atas penjumlahan

Berikut ini merupakan rangking *attack tree* berdasarkan *time metric*:

TABEL V.1
RANGKING *ATTACK TREE* BERDASARKAN *TIME METRIC*

Rank	*Attack Tree*	*Time metric (s)*
1	*Attack Tree* 1	64,895
2	*Attack Tree* 2	73,647
3	*Attack Tree* 5	92,630
4	*Attack Tree* 4	92,728
5	*Attack Tree* 3	96,393

Berdasarkan hasil perangkingan pada Tabel V.B.1, *attack tree* 1 merupakan jalur yang paling cepat secara relatif dibanding *attack tree* lain. Untuk melakukan serangan terhadap *vulnerable machine* Sunset: 1, *attack tree* 1 membutuhkan waktu 64,895 detik. Penyebab *attack tree* 1 memiliki waktu tersingkat yaitu penggunaan penggunaan *attack tools* yang lebih singkat dalam mengambil data.

2. Analisis Perbandingan *Cost Metrics*

Cost metric adalah nilai yang dihitung dari jumlah langkah yang digunakan pada suatu proses. Dalam penelitian ini *cost metric* diambil dari jumlah langkah yang ada pada *activity diagram* setiap *walkthrough. Metric* ini didapatkan dari jumlah langkah yang ada pada *activity diagram.*

Berikut ini merupakan rangking *attack tree* berdasarkan *cost metric*:

TABEL V.2
RANGKING *ATTACK TREE* BERDASARKAN *COST METRIC*

Rank	*Attack Tree*	*Cost metric (step)*
1	*Attack Tree* 1	15
1	*Attack Tree* 3	15
1	*Attack Tree* 4	15
2	*Attack Tree* 2	16
2	*Attack Tree* 5	16

Berdasarkan hasil perangkingan pada Tabel V.B.2, *attack tree* 1, 3, dan 4 merupakan jalur yang memiliki langkah paling singkat secara relatif dibanding *attack tree* lain. Untuk melakukan serangan hingga mendapatkan *privileged environment access* pada *vulnerable machine* Sunset: 1, *attack tree* 1, 3, dan 4 membutuhkan 15 langkah. Jumlah langkah yang paling singkat ini menyebabkan attack tree 1, 3, dan 4 mendapatkan nilai *cost metric* yang paling sedikit.

3. Analisis Perbandingan *Frequency Metrics*

Frequency adalah seberapa sering (%) sebuah tools digunakan dalam proses penyerangan. Disini frekuensi digunakan untuk menghitung berapa sering suatu *tools* digunakan dalam 5 *walkthrough.*

Dari 5 *attack tree* yang sudah dijalankan, didapatkan jumlah penggunaan tools keseluruhan sebanyak 10. Netdiscover muncul sebanyak 3 kali, arpscan muncul sebanyak 2 kali, John The Ripper muncul sebanyak 4 kali, dan Hashcat muncul sebanyak 1 kali.

Untuk menghitung frekuensi penggunaan tools, perhitungannya memakai rumus (Majid, 2021):

$$f = \frac{jumlah\ penggunaan\ tools\ X}{jumlah\ penggunaan\ tools\ keseluruhan} \times 100\% \quad \ldots\ldots \text{(ii)}$$

dengan:
f = frekuensi penggunaan *tools* (%)

Tools X ={Arpscan, Netdiscover, John The Ripper, Hashcat} Berikut ini merupakan rangking penggunaan *tools* berdasarkan distribusi frekuensi dari tabel sebelumnya:

TABEL V.3
RANGKING FREKUENSI PENGGUNAAN *TOOLS* PADA *ATTACK TREE*

Rank	*Tools*	Frekuensi Penggunaan
1	John The Ripper	40%
2	Net-discover	30%
3	Arp-scan	20%
4	Hashcat	10%

Dari perhitungan frekuensi penggunaan *tool*, disimpulkan bahwa *tool* pemindaian IP yang sering digunakan adalah Netdiscover, dan *tool* pemecah *password* yang sering digunakan adalah John The Ripper. *Attack tool* netdiscover yang digunakan untuk memindai IP *address,* memiliki frekuensi penggunaan sebesar 30%. *Attack tool* John The Ripper yang digunakan untuk memindai memecahkan *password,* memiliki frekuensi penggunaan sebesar 40%. Penyebab pemindai IP *address* netdiscover lebih sering digunakan diduga karena data yang diperoleh lebih banyak. Kemudian penyebab *password cracker* John The Ripper lebih sering digunakan diduga karena waktu yang dgunakan lebih singkat.

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

TABEL V.4
PEMERINGKATAN *ATTACK TREE* BERDASARKAN PERHITUNGAN *TIME METRIC* DAN *COST METRIC*

Rank	*Attack Tree*	*Time metric (s)*	*Cost metric (steps)*
1	*Attack Tree* 1	64,895	15
2	*Attack Tree* 2	73,647	16
3	*Attack Tree* 5	92,630	15
4	*Attack Tree* 4	92,728	15
5	*Attack Tree* 3	96,393	15

Dalam perhitungan menggunakan kedua *metrics*, lebih diutamakan waktu tercepat. Dengan waktu tercepat, proses penyerangan lebih cepat selesai dan pengembang *vulnerable machine* tidak memiliki cukup waktu untuk menutup celah keamanan yang ada pada sistem. Sehingga kemungkinan berhasilnya proses penyerangan semakin tinggi.

VI. KESIMPULAN

Implementasi *walkthrough* dan penggambarannya dengan menggunakan *activity diagram* dan *data flow diagram* bisa digunakan untuk mendapatkan langkah-langkah eksploitasi pada *vulnerable machine* Sunset: 1. Penyusunan *attack tree* bisa dilakukan dengan menggunakan pendekatan CubeSat *Security Attack Tree Analysis* dan SAND-*gate* dari implementasi *walkthrough*. *Attack tree* 1 merupakan jalur tercepat untuk melakukan penyerangan dan mendapatkan *privileged environment access* berdasarkan perhitungan *time metric* dengan *real time* 64,895s . *Attack tree* 1, 3, dan 4 memiliki peringkat tertinggi berdasarkan perhitungan jumlah langkah pada *cost metric* dengan langkah sebanyak 15. John The Ripper dan Netdiscover merupakan tools yang paling sering digunakan berdasarkan perhitungan *frequency metric* dengan persentase 40% dan 30% secara berurutan.

REFERENSI

[1] S. Garfinkel, A. Schwartz and G. Spafford, Practical Unix & Internet Security, 3rd Edition, California: O' Reilly & Associates, Inc., 2003.

[2] A. K. Lab, "What is hacking? And How To Prevent it," 1 July 2022. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-hacking.

[3] A. P. Moore, R. J. Ellison and R. C. Linger, Attack Modeling for Information Security and Survivability, Pennsylvania: Carnegie Mellon University, 2001.

[4] L. Kuipers, "Analysis of Attack Trees: Fast Algorithms For Subclasses," *Bachelor Thesis Computing Science,* pp. 9-19, 2020.

[5] D. T. Bourgeois, Information Systems for Business and Beyond, Washington DC: Saylor Academy, 2014.

[6] R. Rezaee and A. G. Bafghi, "A Risk Estimation Framework for Security Threats in Computer Networks," *Journal of Computing and Security,* pp. 19-33, Journal of Computing and Security.

[7] R. Lehtinen, D. Russell and S. G. T. Gangemi, Computer Security Basics: Computer Security, 2nd Edition, California: O'Reilly Media, Inc., 2006.

[8] M. Zwolinski, "Structural Exploitation," *Social Philosophy & Policy Foundation,* pp. 154-179, 2012.

[9] B. Posey, "Computer Exploit," 28 September 2017. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/exploit.

[10] G. Marczyk, D. DeMatteo and D. Festinger, Essentials of Behavioral Science Series, New Jersey: John Wiley & Sons, Inc., 2005.

[11] F. N. Kerlinger and H. B. Lee, Foundations of Behavioral Research, Australia: Wadsworth, 1999.

[12] O. W. Bertelsen, "The Activity Walkthrough: An Expert Review Method Based on Activity Theory," *NordiCHI '04, October 23-27, 2004 Tampere, Finland Copyright 2004 ACM 1-58113-857-1/04/10,* pp. 251-254, 2004.

[13] P. Kirvan, "TechTarget," 8 November 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/Types-of-vulnerability-scanning-and-when-to-use-each.

[14] J. A. Kendall and E. J. Kendall, Systems Analysis and Design, New Jersey: Pearson Education, Inc., 2005.

[15] S. Mauw and M. Oostdijk, "Foundations of Attack Trees," *D. Won and S. Kim (Eds.): ICISC 2005, LNCS 3935 Springer-Verlag Berlin Heidelberg,* pp. 186-198, 2006.

[16] A. R. Hevner, S. T. March, J. Park and S. Ram, "Design Science in Information Systems Research," *MIS Quarterly, Vol. 28, No. 1 (Mar., 2004),* pp. 75-105, 2004.