# IMPLEMENTASI DAN ANALISA SECURITY AUDITING MENGGUNAKAN OPEN SOURCE SOFTWARE KALI LINUX DENGAN FRAMEWORK CYBER KILL CHAIN

# IMPLEMENTATION AND ANALYSIS OF SECURITY AUDITING USING OPEN SOURCE SOFTWARE KALI LINUX WITH FRAMEWORK CYBER KILL CHAIN

**Reza Nugroho[1], Avon Budiyono[2], Adityas Widjajarto[3]**

[1,2,3] S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]rezanug@student.telkomuniversity.ac.id, [2]**adtwjrt@telkomuniveristy.ac.id** , [3]**avonbudi@telkomuniversity.ac.id**

**Abstrak**

Security Auditing merupakan evaluasi sistematis keamanan sistem informasi dengan mengukur seberapa baik dan sesuai dengan seperangkat kriteria yang ditetapkan. Salah satu framework dari Security Auditing adalah Cyber Kill Chain , framework ini memungkinkan seorang security analyst untuk fokus pada berbagai tahap pada sebuah serangan. Maka dari itu, dibuat implementasi dan analisa security auditing berdasarkan framework Cyber Kill Chain guna memberikan informasi tentang manfaat dari Security Auditing.

Penelitian ini dilakukan dengan menggunakan vulnerability operating system sebagai objek yang dilakukan scanning dengan aplikasi open source OpenVAS untuk melakukan vulnerability scan. Dari hasil penelitian yang dilakukan terhadap 10 walkthrough didapatkan hasil analisis berupa activity diagram dan dataflow diagram kemudian akan dilakukan pengelompokan berdasarkan perhitungan resiko yang didapat. Sehingga akan didapatkan klasifikasi berupa hubungan antara tools dan vulnerability berdasarkan framework Cyber Kill Chain.

**Kata kunci :** Security Auditing, *framework* Cyber Kill Chain, *attack tree, tools, Vulnerable.*

**Abstract**

Security Auditing is a systematic evaluation of information system security by measuring how well and in accordance with a set of established criteria. One of the frameworks of Security Auditing is Cyber Kill Chain, this framework allows a security analyst to focus on various stages of an attack. Therefore, security auditing implementation and analysis is made based on the Cyber Kill Chain framework to provide information about the benefits of Security Auditing.

This research was conducted by using the operating system vulnerability as an object that was scanned with the OpenVAS open source application to conduct a vulnerability scan. From the results of research conducted on 10 walkthroughs obtained the results of the analysis in the form of activity diagrams and data flow diagrams will then be grouped based on the calculation of the risks obtained. So that the classification will be obtained in the form of a relationship between tools and vulnerability based on the Cyber Kill Chain framework..

**Keywords : Security Auditing, *framework* Cyber Kill Chain, *attack tree, tools, Vulnerable***.

## 1. Pendahuluan

Perkembangan teknologi diikuti oleh pertambahan jumlah ancaman terhadap keamanan jaringan tersebut. Aktivitas- aktivitas illegal yang dikenal dengan *cyber crime* atau kejahatan cyber dalam bentuk *hacking, virus, spyware, trojan* dan lain sebagainya terus tumbuh. Selain bertumbuh dalam jumlah dan jenis, ancaman digital juga bertumbuh di sisi kualitas dan kompleksitas.

*Security Auditing* dan sistem informasi digunakan untuk menilai efektivitas kontrol TI dalam kehidupan sehari hari . Perlunya menerapkan keamanan informasi dan sistem audit wajib bagi semua organisasi maupun perusahaan. Mengingat pentingnya privasi dan kemanan bagi perusahaan dan organisasi, masalah memutuskan kapan harus melakukan audit keamanan dan menjadi bagian penting dari proses kontrol organisasi. Melihat pertimbangan ini, maka dibutuhkan sebuah framework yang membahas tentang rangkaian yang menggambarkan tahapan serangan cyber yang berkaitan dengan kemanan.

Mengacu dari fakta tersebut, diperlukan solusi keamanan yang efektif dan efisien. Untuk dapat mendapat keamanan jaringan yang optimal maka diperlukan visibilitas terhadap kemungkinan serangan di segala aspek jaringan. Hal ini dapat dipenuhi oleh Security Auditing yang dapat melakukan korelasi antara informasi yang dikumpulkan dari berbagai solusi keamanan jaringan yang ada dan melakukan analisa terhadap incident security yang terjadi.

Security Auditing merupakann suatu tim yang terorganisir dan mempunyai kemampuan dalam bidang keamanan *cyber* yang bertugas memantau dan meningkatkan postur keamanan organisasi dengan mencegah, mendeteksi, menganalisis, dan menanggapi insiden keamanan *cyber* dengan menggunakan teknologi dan proses yang telah disusun dengan baik. *Cyber Kill Chain* merupakan sebuah framework yang dimana memposisikan diri sebagai penyerang untuk mengetahui kekurangan dari suatu situs/sistem. Dengan *framework* ini *team security auditing* mempermudah melakukan pencarian

kekurangan dari objek yang nantinya dicoba. *CyberKillChain ini memiliki 7 tahapan diantaranya; Reconnaissance, Weaponize, Delivery, Exploitation, Installation, Command Control (C2), Act on Objectiv*e.

Dari permasalahan yang muncul, dapat diketahui penelitian ini dilakukan bertujuan untuk penyusunan Security Auditing yang digunakan untuk mengklarifikasikan tools. Pada penelitian ini akan digunakannya metode yang cocok untuk mengatasi pemecahan masalah dan juga melakukan pengelompokkan berdasarkan *framework Cyber Kill Chain*

## 2. Dasar Teori /Material dan Metodologi/perancangan

### 2.1. *Vulnerability*

Vulnerability atau kerentanan adalah suatu poin kelemahan dimana suatu sistem rentan terhadap serangan. *Vulnerability* terbagi menjadi 3 *High, Medium, Low*. Semakin tinggi kerentanan berarti kelemahan yang bersifat signifikan akan membuat sangat rentan terhadap ancaman. Kerentanan menengah berarti kelemahan yang jelas akan meningkatkan kerentanan pada ancaman dan kerentanan rendah berarti kelemahan kecil akan sedikit meningkatkan kerentanan pada ancaman(Hao & Yang, 2010).

### 2.2 *Threat*

*Threats* atau ancaman merupakan hal yang sangat berbahaya bagi keberlangsungan sistem(Juardi, 2017). Ancaman merupakan suatu hal yang dapat mengancam keseimbangan dari suatu sistem dari luar maupun dalam, ancaman dalam sistem informasi dibagi menjadi 2 macam yaitu ancaman pasif dan ancaman aktif(Mokodompit & Nurlaela, 2017).

### 2.3 *Security Auditing*

*Security Auditing* merupakan evaluasi sistematis keamanan sistem informasi perusahaan dengan mengukur seberapa baik itu sesuai dengan seperangkat kriteria yang ditetapkan. Audit menyeluruh biasanya menilai keamanan konfigurasi fisik dan lingkungan sistem, perangkat lunak, proses penanganan informasi, dan praktik pengguna.

Sistem audit keamanan jaringan terdiri dari mengidentifikasi, merekam dan memeriksa. Identifikasi untuk menangkap paket jaringan, dan menganalisis paket berdasarkan protokol mereka. Ada tiga jenis diagnostic yaitu , audit kemanan, penilaian kerentanan, dan pengujian penetrasi .

### 2.4 OpenVAS

OpenVas merupakan software yang digunakan untuk melakukan *scanning* dalam menangani *vulnerability* dalam jaringan terhadap gangguan berdasarkan statistik serangan yang terjadi. OpenVAS digunakan untuk melakukan deteksi terhadap celah keamanan dan dapat menyajikan laporan tingkat resiko.

### 2.5 *Framework* CyberKillChain

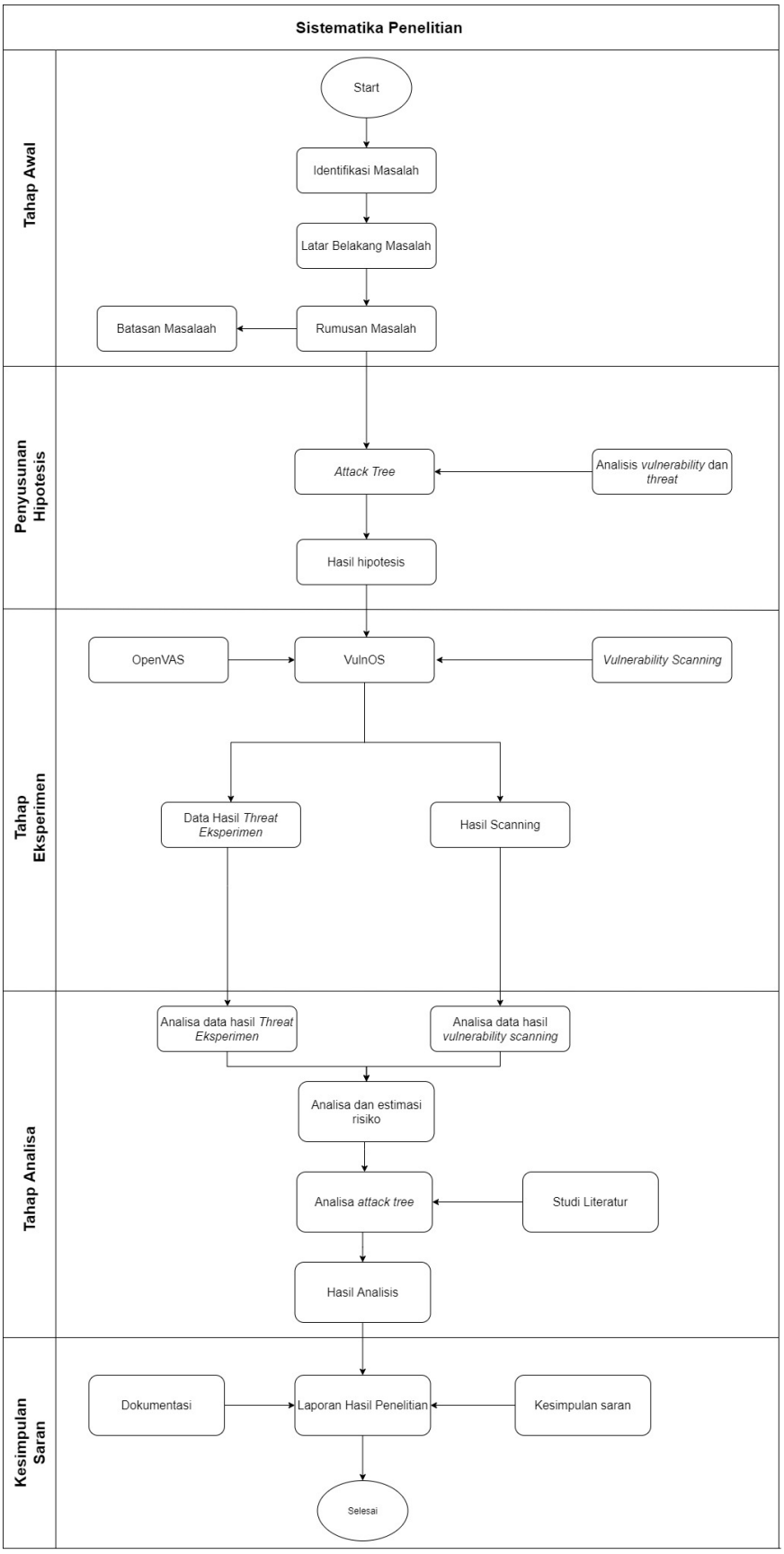
Cyber kill chain adalah sebuah model bagi penyelidik forensik digital dan analis malware. Memahami rantai cyber kill dengan cara memodelkan dan menganalisis tindakan yang akan dilakukan oleh seorang cyberattacker. Penggunaan framework ini dapat membuat seseorang berpikir pada jalur yang sama dengan penyerang. Setiap fase rantai penyerangan itu sendiri adalah area penelitian yang luas untuk diatasi dan dianalisis. Beberapa fase yang dilakukan menggunakan *framework Cyber Kill Chain* adalah *Reconnaissance, Weaponize, Delivery, Exploitation, Installation, Command Control (C2), Act on Objectiv*e.

## 3. Metodologi

Metode yang digunakan untuk melakukan penelitian ini terbagi menjadi lima tahap yaitu perumusan masalah, tahap hipotesis, tahap simulasi, tahap analisis ,dan tahap akhir.

Pada tahap awal dimulai dengan melakukan identifikasi masalah terhadap latar belakang masalah yang bertujuan untuk menggambarkan masalah yang hendak diselesaikan. Setelah itu didapatkan rumusan masalah yang lebih jelas dan mengacu pada batasan masalah. Batasan masalah bertujuan untuk membuat penelitian menjadi efektif, efisien dan tidak melenceng dari topik penelitian itu sendiri Pada tahap hipotesis, dilakukan proses yang bersifat perkiraan sementara pada penelitian yang akan dilakukan, dan hasilnya berbentuk praduga yang dibuktikan lagi kebenarannya. Untuk hipotesis yang diteliti adalah tentang menyusun resiko berdasarkan analisis *vulnerability* dan *threat* kemudian dihasilkan *attack tree.* Pada tahap simulasi dilakukan *Scanning* menggunakan *software open source* yaitu OpenVAS dan melakukan *scanning* menuju *vulnerability operating system* yaitu VulnOS kemudian didapatkan hasil berupa klasifikasi *tools* dan hasil *scanning*. Pada tahap selanjutnya adalah tahap analisis hasil eksperimen. Dilakukan analisis berdasarkan *walkthrough* yang digunakan kemudian dilakukan analisis resiko. Setelah dilakukan

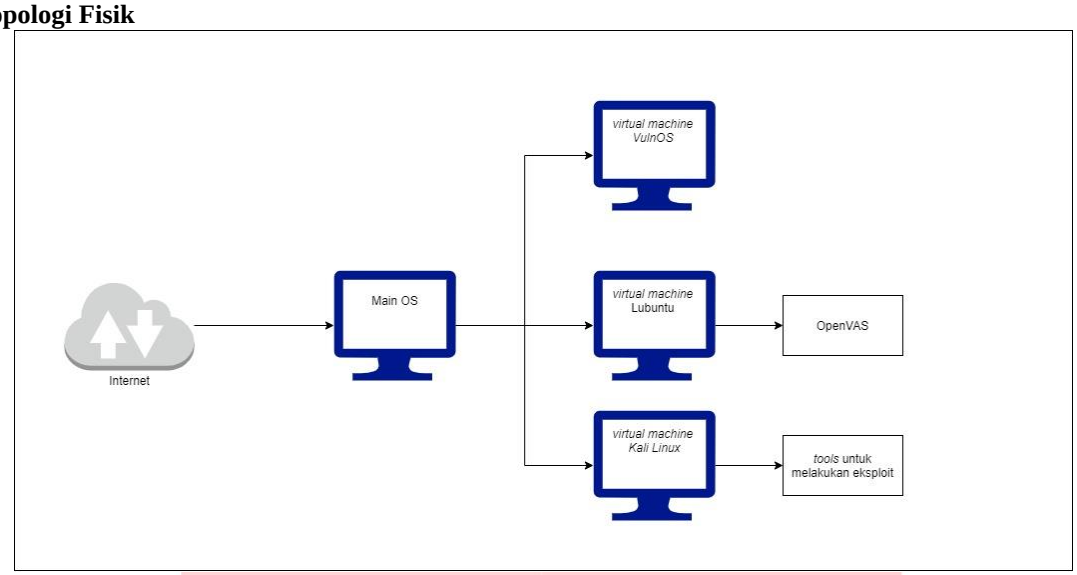
analisis resiko dilakukan pembuatan *attack tree* dan dilakukan analisis berdasarkan data yang telah didapatkan. Pada tahap ini merupakan tahapan terakhir dari penelitian yang dilakukan. Pada tahap ini, hasil analisis yang dapat dijadikan referensi laporan hasil penelitian. Laporan hasil penelitian didukung dengan dokumentasi dari penelitian yang dilakukan serta memberikan kesimpulan dan saran. *Output* akhir yang dihasilkan adalah berupa laporan dari hasil penelitian.




Gambar 1 Sistematika Penelitian

## 4. Perancangan Sistem

### 4.1 Topologi Fisik

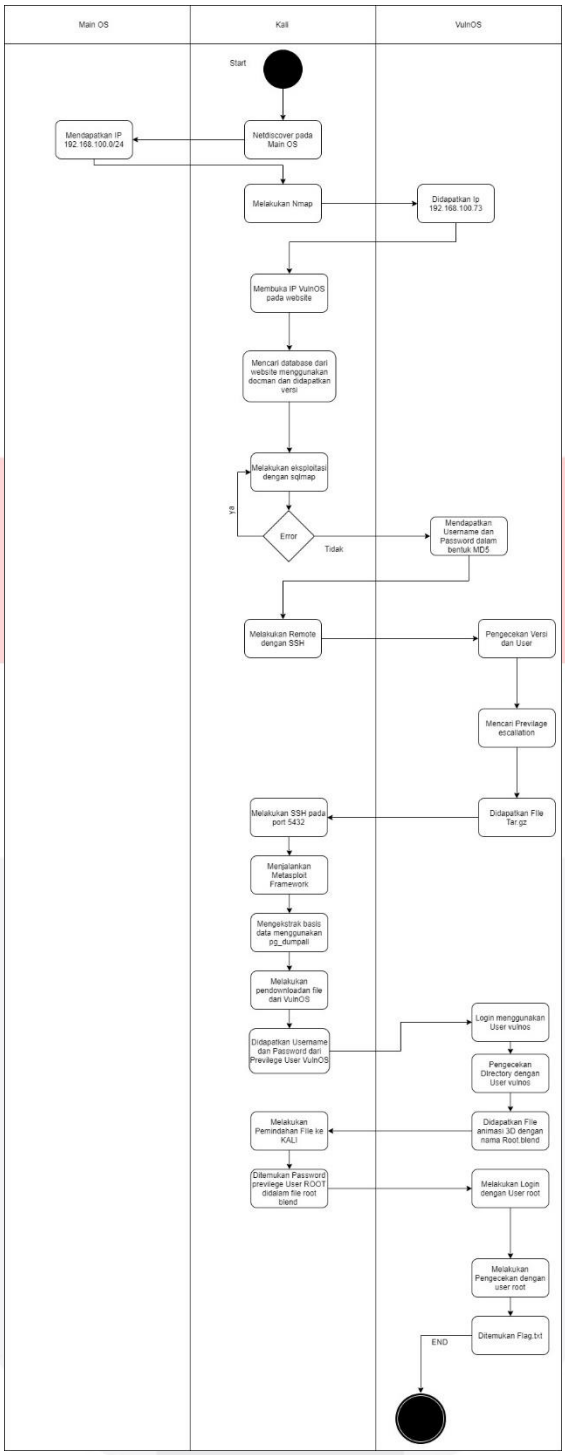



Gambar 2 Topologi Jaringan

Pada Gambar 2 dijelaskan tentang topologi fisik pada penelitian yang dilakukan yang terdiri dari Internet, *MainOs, virtual machine* Kali Linux, *virtual machine* VulnOS dan *virtual machine* Lubuntu.

Internet yang digunakan untuk melakukan pengkoneksian dari MainOS menuju ke *virtual machine* dari VulnOS, Lubuntu, Kali Linux. Ketika Internet sudah terhubung kedalam masing masing OS yang telah ter-install mulai dilakukan eksploitasi menggunakan *tools* untuk mengetahui kerentanan yang ada pada VulnOS. Kemudian dilakukan *scanning vulnerability* menggunakan *software* OpenVAS yang berasal dari Lubuntu.

### 4.2 Perumusan *Activity Diagram*



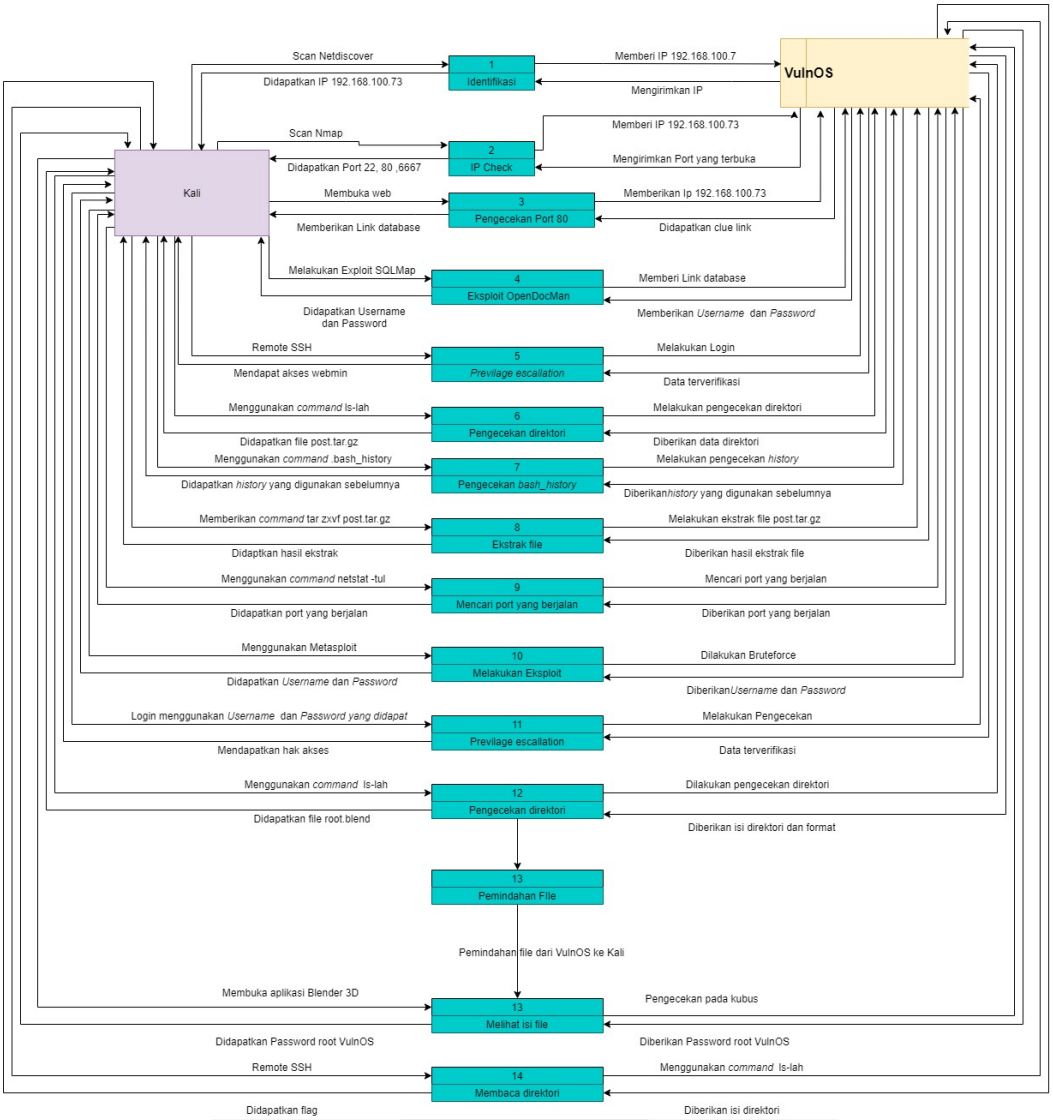

Gambar 3 *Activity Diagram* pada *Walkthrough*

Pada Gambar 3 dijelaskan tentang alur tata cara bagaiman mendapatkan flag dengan melakukan eksploitasi keVulnOS yang dirancang menggunakan activity diagram. Tahap yang dilakukan diantaranya yang pertama melakukan *Netdiscover* ke *MainOS* dan kemudian didapatkan Ip dari VulnOS. Berikutnya dilakukan *Nmap* ke VulnOS sendiri, setelah dilakukan Nmap didaptkan *Port* yang terbuka salah satunya adalah *Port 80*. *Port 80* ini menandakan Ip tersebut dapat diakses melalui website(*port* 80 merupakan *Port Http*). Selanjutnya buka Ip pada browser kemudian didapatkan /jabcdocs yang kemudian diarahkan ke halaman OpenDocMan. Pada halaman tersebut diketahui bahwa versi OpenDocMan yang digunakan adalah V.1.2.7. Kemudian dilakukan eksploitasi dengan menggunakan SQL Map untuk mendapatkan *Username* dan *Password* dari VulnOS, apabila terdapat error maka dapat dilakukan pengecekan kembali terhadap *command* atau perintah yang digunakan. Dan apabila tidak terdapat error maka akan didapatkan *Username* dan *Password* dari VulnOS, setelah didapatkan lakukan login ke VulnOS menggunakan *command* SSH. Setelah itu lakukan pengecekan pada tiap directory dan kemudian didapatkan file tersembunyi yaitu post.tar.gz yang kemudian di-ekstrak dan ditemukan directory VulnOSadmin. Kemudian lakukan SSH kembali ke VulnOS tetapi menggunakan port 5432. Kemudian kembali ke Kali Linux untuk melakukan ekstrak pada database *postgres* menggunakan pg_dumpall yang kemudian didapatkan *password* dari VulnOSadmin. Dilanjutkan dengan pengecekan

directory dan didapatkan file r00t.blend lakukan pemindahan file r00t.blend ke kali linux untuk dilakukan pengecekan. Lakukan pengecekan dengan menggunakan aplikasi blender 3D. Setelah itu didapatkan Username dan Password Root, kemudian lakukan login menggunakan SSH dengan username dan password yang telah didapat. Lakukan pengecekan directory dan ditemukan flag berupa file Root.txt .

## 5. Pengujian Sistem dan Analisis

### 5.1 Analisis *Attack* dan *Vulnerability* yang Dirumuskan Berdasarkan *Data Flow Diagram*




Gambar 4 *Data Flow Diagram* pada *Walkthrough*

Pada Gambar dijelaskan mengenai proses bagaimana penyerang melakukan serangan sampai dengan tujuan akhir yaitu flag yang dirancang dalam bentuk *Data Flow Diagram*. Pada tahap pertama dilakukan scan jaringan menggunakan command ” netdiscover -i eth1 -r 192.168.100.0/24 “ perintah ini digunakan untuk melakukan pengecekan seluruh jaringan yang terkoneksi pada MainOS. Kemudian dijalankan perintah kedua ” nmap -T4 -A -v -p0-65535 192.168.100.73”, Ip 192.168.100.73 merupakan Ip dari VulnOS sendiri, -T4 -A -v merupakan perintah yang bertujuan untuk mencari info tentang host yang diuji. Pada perintah -p0-65535 digunakan untuk pengecekan port yang terbuka dari VulnOS. Pada *scan* tersebut didapatkan *port* yang terbuka adalah 22,80,dan 6667 yang berarti *port* 22 merupakan *port OpenSSH*, *port 80* merupakan *port HTTP*, *port 6667* merupakan *OpenRC*. Karena diberikan *port* 80 yang merupakan *port HTTP* dilakukan pengecekan pada *webbrowser* menggunakan Ip yang telah didapat, dilakukan analisis dari halaman *website* tersebut melalui *inspect element* dan ditemukan petunjuk yang menuju *path* /jabcd0cs. Dilakukan pengecekan dengan menambahkan /jabcd0cs pada Ip VulnOS dan halaman website dialihkan menuju OpenDocMan yang memiliki versi 1.2.7.

Selanjutnya dilakukan eksploit menggunakan SQLMap dengan *command "sqlmap --threads 10 --url "http://192.168.100.73/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user"* dan ditemukan tabel database yang berisikan *Username* dan *Password*. Selanjutnya dilakukan *remote* menggunakan SSH dengan perintah "ssh webmin@192.168.100.73" dan masuk menggunakan *password* yang telah didapat. Dilakukan pengecekan direktori menggunakan *command* "ls-lah" digunakannya perintah diatas adalah untuk melakukan pengecekan isi direktori beserta format akses izin tiap file dan direktori yang ada didalamnya. Dilanjutkan dengan melakukan ekstrak dari direktori menggunakan perintah "tar zxvf post.tar.gz" dan didapatkan beberapa file dan folder. Dilanjutkan dengan melakukan *scan* terhadap layanan yang sedang berjalan dengan *command* "netstat -tul" , setelah dilakukan pengecekan layanan dilakukan *remote* dengan perintah " ssh webmin@192.168.100.73 -L 5432:localhost:5432". Kemudian secara bersamaan dilakukan *Metasploit framework* terhadap localhost VulnOS dengan perintah "msf > use auxiliary/scanner/postgres/postgres_login" setelah itu dilakukan ditambahkan perintah "set Rhost 127.0.0.1" yang berarti melakukan set Rhost pada Ip 127.0.0.1.

Selanjutnya digunakan pg_dumpall untuk mengekstrak semua database yang ada pada localhost 5432 setelah dilakukannya *dumping* didapatkan *Username dan Password* lakukan pergantian user pada VulnOS berdasarkan *Username* dan *Password* yang telah didapat sebelumnya menggunakan *command* "su vulnosadmin" setelah login dilakukan pengecekan direktori dan didapatkan file animasi 3D dengan nama R00t.blend. Lakukan pemindahan file yang didapat kedalam Kali Linux untuk dilakukan eksekusi terhadap file tersebut. Setelah dipindahkan buka file animasi menggunakan aplikasi Blender 3D. Dengan dilakukan analisis dari file tersebut ditemukan *Password* dari root VulnOS yaitu "ab12fg//drg" .

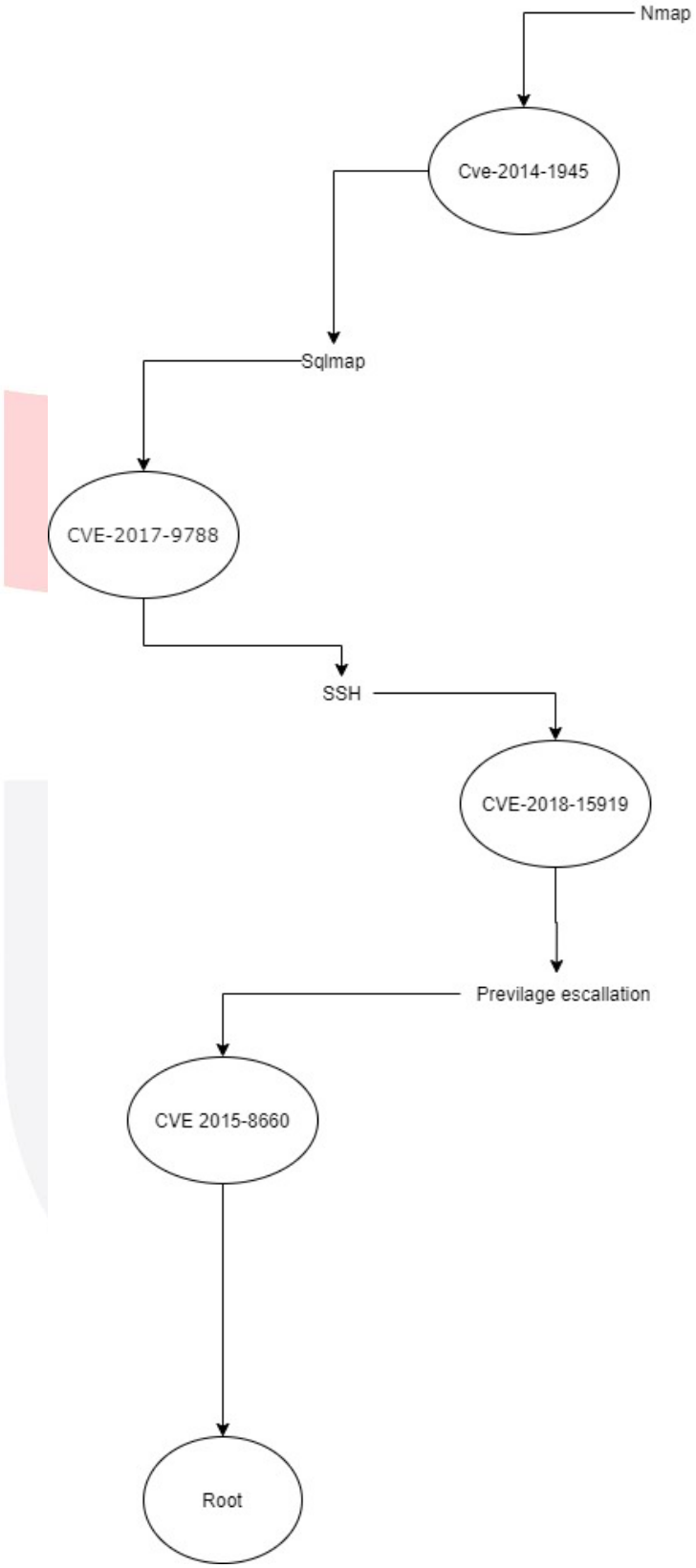
Dilakukan *remote* ulang dengan menggunakan user root "SSH root@192.168.100.73" dan masukkan *Password* yang telah didapat tadi. Lakukan pengecekan direktori dan didapatkan sebuah file yang bernama flag.txt lakukan eksekusi dan ditemukanlah tujuan akhir dari penyerang.

5.2 Analisis Risiko Secara Kuantitatif Berdasarkan *Vulnerability* dan *Threat*

*Tabel 1*

| No | *Vulnerability* | CVSS | *Tools* | *Frequency* | *Risk* |
|---|---|---|---|---|---|
| 1 | Drupal Core Critical Remote Code Execution Vulnerability (SA-CORE-2018-002) (Active Check) | 7.5 | Nmap | 10 | 75 |
| | | | Searchsploit | 3 | |
| 2 | SSH Brute Force Logins With Default Credentials Reporting | 7.5 | Metasploit Framework | 2 | 15 |
| | | | Sqlmap | 10 | 75 |
| | | | Hydra | 1 | 7.5 |
| 3 | SSH Weak Encryption Algorithms Supported | 4.3 | Metasploit Framework | 2 | 8.6 |
| | | | Sqlmap | 10 | 43 |
| | | | SSH | 10 | 43 |
| 4 | SSH Weak MAC Algorithms Supported | 2.6 | SSH | 10 | 26 |
| | | | Netsdiscover | 3 | 7.8 |
| | | | Nikto | 2 | 5.2 |
| | | | DIRB | 3 | 7.8 |
| 5 | TCP timestamps | 2.6 | NMAP | 10 | 26 |

### 5.3 Analisis Risiko Secara Kualitatif Berdasarkan *Vulnerability* dan *Threat*




*Gambar 5*

Gambar 5 menjelaskan tentang attack tree, attack tree merupakan cara formal untuk menggambarkan keamanan sistem berdasarkan macam-macam serangan (Schneier, 1999). Diberikan tahapan yang dimulai dari Nmap dan Netdiscover menghasilkan CVE-2014-1945 digunakannya CVE ini karena membahas tentang OpenDocMan, kemudian dilanjutkan dengan sqlmap yang menghasilkan CVE-2017-9788 kemudian dilanjutkan dengan perintah SSH pada tahap ini digunakan CVE-2018-15919 yang dimana ketika melakukan remote harus memiliki autentikasi. Dilanjutkan dengan melakukan previlage escallation digunakan CVE-2015-8660.

Pada tahap pertama framework Cyber Kill Chain yang merupakan tahap reconnaissance dilakukan identifikasi terhadap VulnOS dengan mencari Ip dari VulnOS sendiri menggunakan netdiscovery dan Nmap. Kemudian pada tahap Weaponize dilakukan eksploit pada OpenDocMan yang memiliki versi 1.2.7 . kemudian pada tahap Delivery, delivery melakukan SqlInjection menggunakan SQLMap yang ditujukan ke website. Pada tahap Eksploitasi ini dilakukan pada tahap previlage escallation pada VulnOS, kemudian pada tahap Installation melakukan pemindahan file dari VulnOS menuju ke Kali Linux, dan kemudian di tahap Command and Control (C2) diaplikasikan pada setelah didapatkan user root penyerang dapat membuka semua hak akses dari VulnOS yang berarti penyerang memiliki akses terus menerus keVulnOS, dan pada tahap yang terakhir Act On Object pada tahap ini penyerang telah mendapatkan tujuan penyerangan yaitu file Flag.txt .

## 6. Kesimpulan

Setelah dilakukan pengujian didapatkan hasil analisis *Security Auditing* pada VulnOS dengan menggunakan *framework Cyber Kill Chain*, dapat diambil kesimpulan berupa :

1. Dilakukan analisis menggunakan OpenVAS berupa 5 *vulnerability* yang masing-masing dikategorikan menjadi 3 tingkatan yaitu *Low, Medium, dan High.* Dilakukan penghubungan antara *tools* yang telah di klasifikasikan dengan hasil dari OpenVAS berdasarkan frekuensi penggunaan tiap *walkthrough.*
2. Berdasarkan 10 *walkthrough* yang digunakan didapatkan analisa untuk *attack model* berupa *activity diagram* dan *dataflow diagram.* Yang dimana pada *activity diagram* dijelaskan tentang tahapan secara garis besar dan pada *dataflow diagram* dijelaskan secara lengkap baik dari perintah maupun alur serangan.
3. Hasil dari hubungan dan implementasi VulnOSv2 adalah risiko secara kualitatif yang disusun berdasarkan attack tree. Yang dimana penentuan CVE disesuaikan berdasarkan proses terjadinya serangan, kemudian attack atau tools tersebut dihubungkan dengan *Cyber Kill Chain* sesuai peran atau fungsi.

## 7. Daftar Pustaka

Hao, X., & Yang, N. (2010). IT operational risk assessment and control model based on Bayesian network. *Proceedings - 2010 6th International Conference on Natural Computation, ICNC 2010*, *3*(Icnc), 1105–1109. https://doi.org/10.1109/ICNC.2010.5583696

Juardi, D. (2017). *Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus*. *6*(1), 11–19.

Mokodompit, M. P., & Nurlaela, N. (2017). Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000 (Studi Kasus Pada Peguruan Tinggi X). *Jurnal Sistem Informasi Bisnis*, *6*(2), 97. https://doi.org/10.21456/vol6iss2pp97-104