IMPLEMENTASI DAN ANALISIS SECURITY AUDITING MENGGUNAKAN OPEN SOURCE SOFTWARE DENGAN FRAMEWORK STRIDE

IMPLEMENTATION AND ANALYSIS OF SECURITY AUDITING USING THE OPEN SOURCE SOFT WITH THE METHODOLOGY STRIDE

Ricky Yudisi Dwiaranda[1], Avon Budiyono[2], Adityas Widjajarto[3]

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

Abstrak

Security Auditing merupakan sistem evaluasi terhadap perilaku jaringan untuk pengguna atau peralatan, dan kemudian memberikan petunjuk untuk mencegah terjadinya serangan. Penelitian ini bertujuan untuk menentukan risiko dari vulnerability dan threat pada vulnerability operating system (VulnOSv2) dan merupakan salah satu komponen untuk penyusunan Security Auditing System. Dengan digunakannya 10 walkthrough, dapat dilakukannya analisis perbandingan pada setiap tahapan dan juga penerapan tools secara cepat, tepat dan akurat.

Simulasi yang dilakukan untuk menemukan vulnerability scanning dan attack pada walkthrough dengan menerapkan sebuah vulnerability operating system pada VirtualBox sebagai objek penelitian dan menggunakan open source software yaitu OpenVAS. Hasil analisis dari relasi antara data vulnerability dan threat berupa risiko secara kuantitatif dan kualitatif. Kemudian disusun dengan menggunakan attack tree yang dihubungkan berdsarkan Framework STRIDE untuk penyusunan Security Auditing system.

Kata kunci : ***Security Auditing, Open Source, Tools, Klasifikasi, Attack Tree, Framework STRIDE***

Abstract

Security Auditing is an evaluation system of the network behavior for the user or equipment, and then provides instructions to prevent the occurrence of an attack. The research aims to determine the risks of vulnerabilities and threats to operating system vulnerabilities (VulnOSv2) and denote as a component for the preparation of a security auditing system. With the use of 10 walkthroughs, comparative analysis can be done in Lot stages and also application of tools quickly, precisely and accurately.

The simulation was done to find the scanning vulnerability and attack on the Walkthrough by implementing on operating system vulnerabilities on VirtualBox as an object research and using open source software called OpenVAS. The results of the relationship analysis between vulnerability and threat data are risk of quantitative and qualitative. Then compiled by using an attack tree associated with the STRIDE Framework for preparing the Security Auditing system.

Keywords : Security Auditing, Open Source, Tools, Classification, Attack Tree, STRIDE Framework

1. Pendahuluan

Dengan banyaknya serangan cyber terhadap aset-aset organisasi seperti halnya aplikasi berbasis web yang merupakan salah satu yang sering rentan dari sistem informasi. Sifat aplikasi berbasis web yang dipaparkan melalui keterbukaan, aksebilitas, dan distribusi yang luas, mengakibatkan dijadikannya sasaran empuk bagi penyerang. VulnOS merupakan sebuah Vulnerability Operating System yang dibuat untuk dilakukan pengecekan keamanannya yang dapat diakses oleh semua orang. Akan tetapi adanya bugs dan juga celah keamanan pada suatu sistem yang dapat mengakibatkan diretasnya sistem tersebut sudah menjadi hal yang biasa.

Keamanan merupakan salah satu dari masalah utama sistem informasi. Dalam upaya untuk memecahkan masalah keamanan dan menerapkan peraturan yang berlaku, pakar keamanan telah mengembangkan berbagai metode jaminan keamanan yang mencakup bukti kebenaran desain berlapis, lingkungan rekayasa software dan uji penetrasi [1].

Maka dari itu, perlunya menerapkan keamanan informasi dan sistem audit wajib bagi VulnOS guna menghindari tindak kejahatan yang dilakukan oleh sebagian pihak lainnya. Mengingat menjaga keamanan itu penting, maka dibutuhkannya sebuah metode yang membahas tentang rangkaian yang menggambarkan tahapan mengenai serangan siber yang berkaitan dengan keamanan jaringan. Pada dasarnya dibutuhkan keamanan yang lebih optimal untuk melindungi data-data penting dengan melakukan evaluasi keamanan (security auditing).

Security Auditing merupakan sistem evaluasi terhadap perilaku jaringan untuk pengguna atau peralatan, dan kemudian memberikan bukti elektronik langsung untuk mencegah tindakan penyalahgunaan. Ini adalah bagian penting dari sistem keamanan informasi untuk melindungi. Sistem audit keamanan jaringan terdiri dari mengidentifikasi, merekam dan memeriksa [2].

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 STRIDE.

2. Dasar Teori /Material dan Metodologi/perancangan

2.1. *Vulnerability*

Vulnerability atau kerentanan adalah suatu poin kelemahan dimana suatu sistem rentan terhadap serangan [3]. Semua sistem yang telah dibuat pasti memiliki kerentanan dalam hal keamanan jaringan, dimana ada suatu celah yang lama-kelamaan akan ditemukan oleh hacker.

2.2 *Threat*

Threats atau ancaman adalah suatu hal yang berbahaya bagi keberlangsungan system [3]. Ancaman merupakan aksi yang dapat mengganggu keseimbangan suatu sistem baik dari dalam maupun dari luar yang dibagi menjadi 2 macam yaitu aktif dan pasif [4].

2.3 *Security Auditing*

Security Auditing merupakan sistem evaluasi terhadap perilaku jaringan untuk pengguna atau peralatan, dan kemudian memberikan bukti elektronik langsung untuk mencegah tindakan penyalahgunaan. Ini adalah bagian penting dari sistem keamanan informasi untuk melindungi. Sistem audit keamanan jaringan terdiri dari mengidentifikasi, merekam dan memeriksa [2].

Maksud dari mengidentifikasi adalah untuk menangkap paket jaringan, dan menganalisis paket berdasarkan protokol mereka. Maksud dari merekam berarti akan mengidentifikasi isi paket sesuai dengan tingkat kebijakan tertentu untuk penyimpanan. Maksud dari memeriksa berarti akan menanyakan data perilaku pengguna jaringan setelah mereka menggunakan Internet untuk akses, sehingga dapat memberikan audit keamanan jaringan berupa bukti jejak digital.

2.4 *Penetration Testing*

Penetration testing merupakan pengidentifikasian kerentanan keamanan dibawah keadaan yang dikendalikan sehingga dapat dihilangkan sebelum pengguna yang tidak berwenang melakukan eksploitasi [1]. Penetration testing ini sangat berguna untuk melakukan simulasi penyerangan agar dapat mengetahui titik celah yang rentan pada suatu sistem dan kemudian celah tersebut dapat diperbaiki.

2.5 *Framework* STRIDE

STRIDE merupakan singkatan dari spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. Framework ini merupakan kerangka ancaman yang terbaru yang telah diklasifikasikan sesuai dengan kategori dari STRIDE itu sendiri [5]. Tidak semua ancaman yang memungkinkan dapat memengaruhi sistem perangkat lunak, tetapi dapat digunakan untuk memantu pengembangan representasi ancaman dan juga klasifikasi tersebut. STRIDE juga dapat digunakan untuk membantu mencakup berbagai ancaman yang dapat dikontrol.

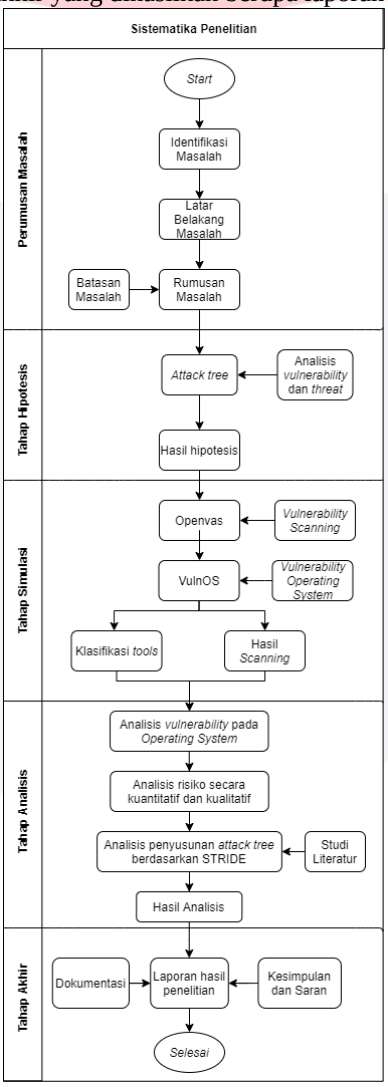
STRIDE-LM	Threat	Property	Definition	Controls
S	Spoofing	Authentication	Impersonating someone or something	Authentication Stores, Strong Authentication mechanisms
T	Tampering	Integrity / Access Controls	Modifying data or code	Crypto Hash, Digital watermark/ isolation and access checks
R	Repudiation	Non-repudiation	Claiming to have not performed a specific action	Logging infrastructure, full-packet-capture
I	Information Disclosure	Confidentiality	Exposing information or data to unauthorized individuals or roles	Encryption or Isolation
D	Denial of Service	Availability	Deny or degrade service	Redundancy, failover, QoS, Bandwidth throttle
E	Elevation of Privilege	Authorization / Least Privilege	Gain capabilities without proper authorization	RBAC, DACL, MAC; Sudo, UAC, Privileged account protections
LM	Lateral Movement	Segmentation / Least Privilege	Expand influence post-compromise; often dependent on Elevation of Privilege	Credential Hardening; Segmentation and Boundary enforcement; Host-based firewalls

Gambar 1 Kategori STRIDE [6]

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.

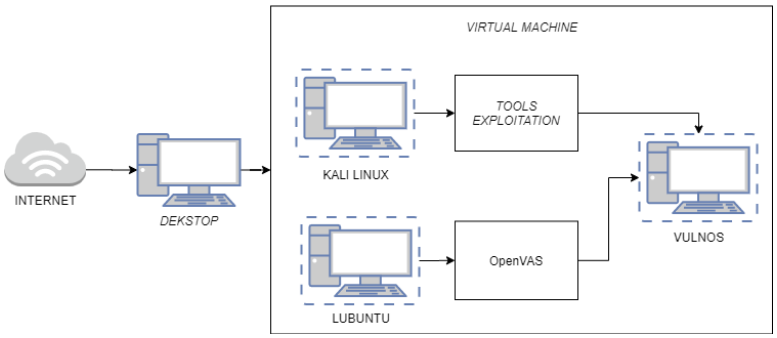
Pada tahap awal dimulai dengan melakukan identifikasi masalah terhadap latar belakang yang bertujuan untuk menggambarkan masalah yang akan diselesaikan. Setelah itu didapatkan perumusan masalah dari penelitian ini dan akan mendapatkan batasan masalah. Batasan masalah bertjuan untuk mebuat penelitian ini menjadi lebih efektif, efisien, dan tidak menyimpang dari topik penelittian ini. Pada tahap hipotesis, dilakukannya proses yang bersifat perkiraan sementara pada penelitian yang akan dilakukan, yang kemudian hasilnya berbentuk prasangka yang dibuktikan lagi kebenarannya. Untuk hipotesis yang diteliti adalah tentang bagaimana bisa untuk mendapatkan risiko dari data vulnerability dan threat berdasarkan penyusunan attack tree. Dari proses tersebut akan menghasilkan hipotesis. Pada tahap simulasi ini dlakukannya klasifikasi pada tools yang digunakan dalam setiap walkthrough dan scanning vulnerability pada VulnOS menggunakan software OpenVAS. Hasil yang didapat dari scannig vulnerability akan dihubungkan dengan tools yang kemudian diklasifikasikan sesuai dengan urutan dan tingkat kerentanan. Pada tahap selanjutnya adalah tahap analisis hasil simulasi. Data yang diperoleh dari tahap simulasi akan dianalisis dengan menggunakan hasil dari risiko secara kuantitatif dan dilanjutkan menggunakan hasil dari risiko secara kualitatif dalam bentuk attack tree berdasarkan Framework STRIDE. Tahap terakhir adalah mendapatkan hasil analisis sebagai kesimpulan untuk tahap akhir. Pada tahap akhir ini, hasil simulasi dan hasil analisis dapat dijadikan sebagai referensi untuk laporan hasil penelitian. Dokumentasi dari penelitian yang dilakukan mendukung laporan hasil penelitian serta memberikan kesimpua dan saran. Output akhir yang dihasilkan berupa laporan dari hasil penelitian.



Gambar 2 Sistematika Penelitian

4. Perancangan Sistem

4.1 Topologi Fisik



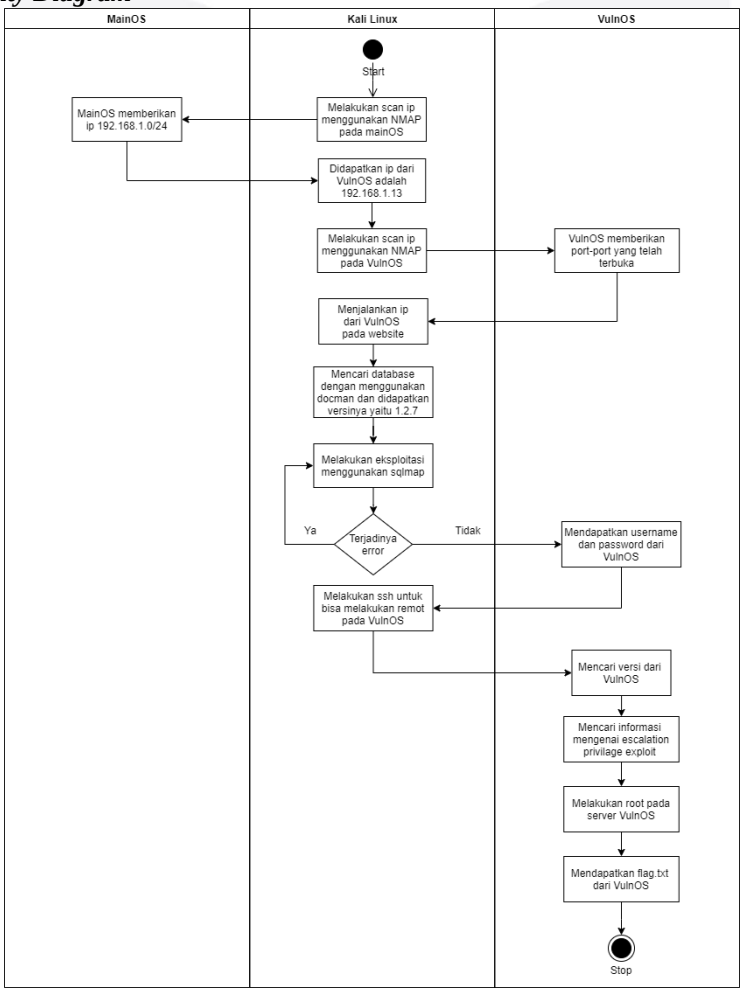
Gambar 3 Topologi Jaringan

Pada Gambar 2 dijelaskan bahwa topologi fisik pada penelitian ini terdiri dari 1 Internet, 1 Dekstop, 1 Kali Linux, 1 Lubuntu, Tools Exploitation, dan 1 Vulnerability Operating System.

Internet terhubung koneksinya menuju Dekstop yang sudah terpasang Virtual Machine yang didalamnya terdapat Tools Exploitation. Internet disini memiliki fungsi sebagai penghubung antara Dekstop dan Virtual Machine untuk mempermudah pencarian IP karena berada pada jaringan yang sama, sehingga dapat dilakukannya analisis perbandingan tools pada Vulnerability Operating System.

Kali Linux terhubung dengan VulnOS agar dapat digunakan untuk identifikasi IP dan selanjutnya dapat dilakukannya eksploitasi menggunakan tools untuk mengetahui kerentanan pada VulnOS. Kemudian pada Lubuntu terhubung dengan VulnOS digunakan untuk melakukan scanning vulnerability dengan menggunakan OpenVAS. Masing-masing rincian dari perangkat dapat dilihat pada table dibawah ini.

4.2 Perumusan *Activity Diagram*



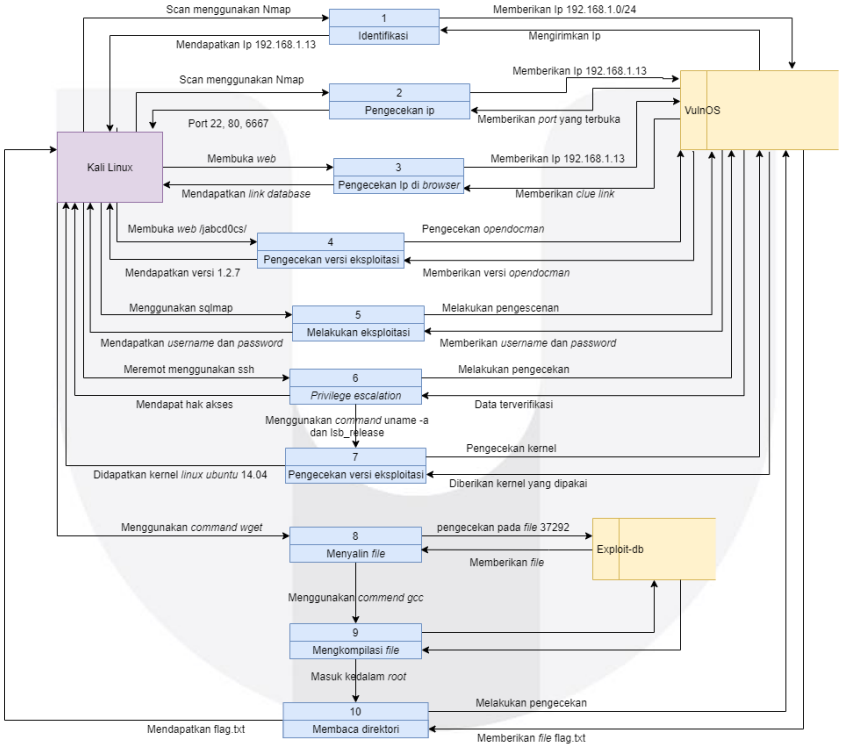
Gambar 4 *Activity Diagram* pada *Walkthrough*

Pada Gambar 3 menjelaskan mengenai alur penyerang mendapatkan flag dengan melakukan eksploitasi pada VulnOS yang dirancang dalam bentuk activity diagram. Langkah yang dilakukan pertama kali oleh penyerang yaitu

dengan melakukan scan IP pada MainOS menggunakan Netdiscover agar dapat diketahui IP dari VulnOS tersebut sudah terhubung ke dalam satu jaringan yang sama dengan Kali Linux. Setelah mendapatkan IP dari VulnOS dilakukan scanning ulang menggunakan Nmap untuk mencari port-port yang terbuka. Dikarenakan dari hasil scan terdapat port 80 yang berarti HTTP, maka langkah selanjutnya dilakukan pengecekan IP pada sebuah website. Setelah dilakukannya penelusuran pada website yang dibuka, ditemukannya website dari VulnOS sendiri yaitu jabcd0cs yang diteruskan ke halaman OpenDocMan. Pada halaman tersebut ditemukannya versi dari OpenDocMan yaitu 1.2.7, setelah itu dilakukannya pencarian untuk eksploitasi yang relevan di Internet. Pada langkah selanjutnya dengan melakukan SQL Injection menggunakan Sqlmap untuk mendapatkan username dan password dari VulnOS. Apabila terdapat error pada SQL injection, maka dilakukan pengecekan kembali pada command yang tertera dan setelah itu dapat dijalankan kembali. Apabila proses yang dijalankan tidak terdapat kendala, maka setelah itu melakukan login pada VulnOS dengan menggunakan OpenSSH. Setelah itu dilakukan pengecekan dan didapatkan file yang tersembunyi yaitu post.tar.gz yang kemudian diekstrak dan juga ditemukannya direktori vulnosadmin. Selanjutnya melakukan pemeriksaan layanan yang terdapat pada jaringan lokal dan didapatkan postgresql dan mysql. Menjalankan OpenSSH kembali pada VulnOS tetapi dengan menggunakan port 5432, kemudian dilanjutkan dengan menjalankan Metasploit Framework terhadap localhost 5432. Kembali pada bagian Kali Linux untuk melakukan ekstrak pada database postgres menggunakan pg_dumpall yang kemudian didapatkan password dari vulnosadmin. Lanjut ke bagian VulnOS dan login pada vulnosadmin menggunakan password yang telah didapatkan. Setelah itu melakukan pengecekan pada direktori dan ditemukannya file r00t.blend, agar dapat dibuka maka file tersebut dipindahkan ke Kali Linux. Pada bagian Kali Linux dilakukannya instalasi aplikasi blender 3D dan buka file r00t.blend. File tersebut berbentuk kubus dan dilakukan pengcekan secara detail dikarenakan terdapat password root didalam kubus tersebut. Selanjutnya menggunakan OpenSSH untuk login ke dalam root VulnOS menggunakan password yang sudah didapat. Setelah berhasil masuk ke dalam root, maka penyerang dapat menemukan flag didalam root tersebut.

5. Pengujian Sistem dan Analisis

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



Gambar 5 *Data Flow Diagram* pada *Walkthrough*

Pada Gambar 4 dijelaskan mengenai proses bagaimana penyerang mengoperasikan tools yang digunakan untuk melakukan eksploitasi pada VulnOS yang dirancang dalam bentuk Data Flow Diagram. Langkah pertama menggunakan Nmap dengan command “nmap -sn” pada IP MainOS yaitu 192.168.1.0/24 yang berfungsi untuk mengetahui daftar-daftar host yang tersedia pada jaringan tersebut, setelah itu mendapatkan hasil dari IP pada VulnOS yaitu 192.168.1.13. Selanjutnya dengan melakukan identifikasi layanan yang berjalan pada VulnOS menggunakan scanning Nmap dengan command “nmap -sT -sV -A -O -v -p 1-65535 192.168.1.13”. Fungsi pada -sT digunakan untuk mengetahui TCP pada Nmap, fungsi pada -sV digunakan untuk mendekteksi informasi layanan dan versi, fungsi pada -A digunakan untuk mendeteksi informasi OS tentang host yang diuji, pada fungsi -O digunakan untuk kemungkinan mendeteksi OS untuk host atau rentang host, pada fungsi -v digunakan untuk menambahkan verbositas ekstra untuk mendapatkan informasi tambahan pada pencarian yang telah dilakukan, pada fungsi -p 1-65535 digunakan untuk melakukan scanning pada jaringan localhost untuk semua port umum. Pada scan tersebut didapatkan hasil berupa port 22, 80, 6667 yang berarti secara berurutan yaitu Open SSH, Open HTTP, dan Open IRC.

Pada langkah selanjutnya membuka url dari IP VulnOS di browser, setelah memasuki url tersebut kemudian mengikuti hyperlink yang ada pada halaman tersebut. Di halaman selanjutnya pada menu dokumentasi memberikan beberapa informasi tentang situs baru dan ditemukannya /jabcd0cs/ yang kemudian diteruskan pada halaman OpenDocMan. Versi dari OpenDocMan tersebut adalah 1.2.7, kemudian penyerang mencoba mencari di Internet mengenai eksploitasi pada versi tersebut. Pada informasi yang didapat bahwa odm_user rentan terhadap SQL injection. Jadi pada langkah selanjutnya menjalankan Sqlmap dengan command sebagai berikut:

1. root@kali:~# sqlmap -u "http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" --dbs --level=5 --risk=3

Pada command tersebut, fungsi pada -u digunakan untuk target pada url, dan fungsi pada --dbs digunakan untuk mengambil semua nama database pada server yang kemudian dilakukan dengan pencarian pada tingkatan dan risiko untuk melakukan tes yang maksimal yaitu 5 dan 3. Setelah berhasil dijalankan, output yang didapatkan diantaranya drupal7, information_shcema, jabcd0cs, mysql, performance_schema, dan phpmyadmin.

2. root@kali:~# sqlmap -u "http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" -D jabcd0dcs --tables

Pada command tersebut digunakan untuk mengambil semua tabel dari database jabcd0cs. Output yang didapatkan diantaranya odm_access_log, odm_admin, odm_category, odm_data, odm_department, odm_dept_perms, odm_dept_reviewer, odm_filetypes, odm_log, odm_odmsys, odm_rights, odm_settings, odm_udf, odm_user, dan odm_user_perms.

3. root@kali:~# sqlmap -u "http://192.168.1.13/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" -D jabcd0cs -T odm_user --dump

Pada command tersebut digunakan untuk menampilkan semua kolom dari tabel odm_user yang aada pada database jabcd0cs. Output yang didapatkan berupa isi dari tabel odm_user yang didalamnya terdapat username webmin dan password yang berbentuk hash MD5. Ketika dikonversi password tersebut menjadi "webmin1980".

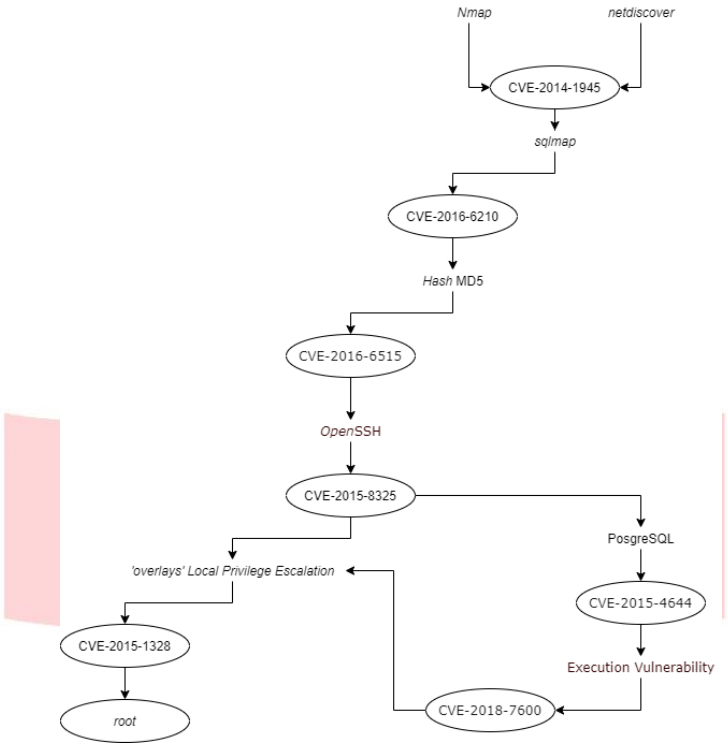
Selanjutnya melakukan login pada mesin dengan Open SSH menggunakan command "ssh webmin@192.168.1.13". Setelah berhasil login dilakukannya pengecekan pada id dan menggunakan command "$ python -c 'import pty;pty.spawn("/bin/bash")'" untuk memasuki shell pada webmin@VulnOSv2. Setelah berhasil dilakukannya pengecekan menggunakan command "uname -a" untuk mengentahui kernel yang digunakan yaitu linux 3.13 dan menggunakan command "cat /etc/lsb-release" untuk mengetahui versi linux yang digunakan yaitu Ubuntu 14.04. Melakukan browsing di Internet pada kedua versi tersebut untuk mengetahui informasi dari privilege escalation. Pada langkah terakhir melakukan root pada server, masuk ke direktori /tmp dan setelah itu melakukan wget file 37292 dari exploit-db. Setelah berhasil dilakukan mengecekan menggunakan "ls", apabila sudah tersedia pada direktori tersebut maka dilakukannya rename pada file tersebut menjadi ofs.c. Selanjutnya melakukan compile pada file yang sudah di rename tersebut, dilakukannya execute pada shell VulnOS untuk bisa memasuki root. Setelah itu menggunakan command "cat /root/flag.txt" dan penyerang berhasil mendapatkan flag dari VulnOS.

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

Tabel 1 Klasifikasi *Tools* Berdasarkan *Vulnerability* pada VulnOS

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 6 *Attack Tree*

Berdasarkan dari penyusunan attack tree yang sudah dijelaskan mengenai proses bagaimana cara yang dilakukan untuk mendapatkan root dengan menggunakan tools atau attack yang sudah dihubungkan antara vulnerability dan threat pada suatu arah eksploitasi. Pada langkah pertama untuk mendapatkan informasi kerentanan yang terjadi pada OpenDocMan dibutuhkan Nmap dan Netdiscover untuk mengetahui identitas host yang menjadi target. Selain digunakan untuk serangan, Nmap dan Netdiscover dapat juga digunakan untuk pengecekan keamanan apabila terjadi penyisipan host yang tidak diketahui. Netdiscover sendiri dapat digunakan untuk mengetahui semua host yang berjalan pada jaringan yang sama, sedangkan pada Nmap sendiri dapat digunakan untuk mengetahui port yang terbuka dari host target. Dari proses ini dapat disimpulkan jika I dari STRIDE yang berarti Information Disclosure masuk ke dalam kategori ini, dikarenakan tujuan dari Information Disclosure adalah untuk membaca sebuah informasi tanpa izin. Jadi kategori ini merupakan tahap information gathering yang dilakukan sebelum serangan itu terjadi.

Kemudian pada tahap selanjutnya untuk mendapatkan database yang berisi username dan password dari VulnOS dibutuhkannya SQL injection, dikarenakan versi dari database tersebut terdapat kerentanan. Dengan menggunakan Sqlmap dapat digunakan untuk mengetahui dan mengeksploitasi kelemahan SQL injection dan mengambil laih semua isi yang ada didalam database tersebut. Dari proses serangan yang terjadi akibat SQL injection dapat disimpulkan jika R dari STRIDE yang berarti Repudiation masuk ke dalam kategori ini. Dikarenakan tujuan dari Repudiation adalah melemahkan suatu sistem dengan menyisipkan virus agar dapat diakses suatu saat. Cara kerja dari SQL injection dan tujuan dari Repudiation bisa dikatakan sangatlah mirip. Serangan seperti ini dapat diatasi dengan selalu melakukan pengcekan berkala pada server dan database, sehingga kemungkinan serangan yang terjadi sangatlah kecil.

Pada tahap selanjutnya untuk membaca atau mengetahui kode acak yang berupa hash, dibutuhkannya hash MD5 untuk melakukan decrypt yang digunakan untuk mengubah kode acak menjadi teks normal pada umumnya. Jadi peranan hash MD5 dalam kegiatan sehari-hari bisa digunakan untuk menyembunyikan data atau pesan dengan melakukan enkripsi, sehingga tidak dapat dilacak pada lalu lintas jaringan ketika data atau pesan tersebut sedang dikirimkan. Dapat disimpulkan pada proses tersebut jika I dari STRIDE yang berarti Information Disclosure masuk ke dalam kategori ini. Dikarenakan proses dari hash MD5 sendiri digunakan untuk mendapatkan suatu informasi ketika kode acak tersebut berhasil dilakukan decrypt yang menjadikannya teks biasa.

Pada tahap selanjutnya untuk dapat memasuki shell dari webmin, dapat digunakannya Open SSH. Dikarenakan Open SSH berfungsi untuk memeungkinkan user mengakses sebuah sistem dalam jarak jauh dengan syarat masih dalam jaringan yang sama. Dalam kegiatan sehari-hari, Open SSH ini dapat berguna selain digunakan untuk melakukan serangan dapat juga digunakan untuk melakukan kontrol pada suatu sistem di sebuah organisasi, dengan adanya Open SSH dapat memudahkan seseorang untuk melakukan monitoring dalam jumlah besar. Dapat dismpulkan pada proses tersebut jika E dari STRIDE yang berarti Escalation of Privileges masuk ke dalam kategori ini. Tujuan dari Escalation of Privileges adalah mendapatkan hak akses pada suatu sistem yang tidak berwenang, sehingga apabila dikaitkan dengan Open SSH sangatlah mirip dari kegunannya sendiri yaitu untuk mendapatkan suatu hak akses.

Pada tahap selanjutnya untuk dapat menjalankan postgresql dapat menggunakan Hydra yang fungsinya untuk melakukan brute force sebagai vulnerability execution. Fungsi dari brute force sendiri digunakan untuk mendapatkan

hak akses dari suatu sistem yang dilakukan dengan cara mencoba-coba kata sandi sampai menemukan kode yang tepat, secara sederhana digunakan untuk mendapatkan hak akses secara paksa. Dapat disimpulkan pada proses ini jika D dari STRIDE yang berarti Denial of Service masuk ke dalam kategori ini. Tujuan dari Denial of Service digunakan untuk menggagalkan suatu sistem untuk sementara agar tidak dapat diakses oleh orang lain. Apabila dikaitkan dengan proses dari brute force sendiri sangatlah mirip yang dimana pada intinya fungsi dari keduanya digunakan untuk menggagalkan suatu sistem untuk kepentingan pribadi.

Pada tahap terakhir untuk mendapatkan hak akses dari root perlu dilakukannya tahapan pembuatan file dan atau melakukan pengambilan file dari hasil eksploitasi yang sudah ada. Dengan cara melakukan compile file yang sudah didapatkan dari hasil eksploitasi yang kemudian menjalankan file tersebut dengan perintah execute sehingga dapat digunakan untuk memasuki root. Dapat disimpulkan pada proses ini jika E dari STRIDE yang berarti Escalation of Privileges masuk dalam kategori ini. Seperti yang telah dijelaskan sebelumnya tujuan dari Escalation of Privileges untuk mendapatkan hak akses pada suatu sistem yang tidak berwenang. Adanya keterkaitan dari keduanya antara menjalankan file untuk memasuki sistem dengan Escalation of Privileges yang sama-sama menginginkan untuk mendapatkan hak akses.

6. Kesimpulan

Setelah dilakukannya pengujian dan memperoleh hasil analisis penyusunan Security Auditing menggunakan Framework STRIDE**,** Analisis dari hasil scanning menggunakan OpenVAS berupa 5 vulnerability yang masing-masing dikatergorikan ke dalam 3 bagian tingkatan kerentanan yaitu Low, Medium, dan High. Hasil dari OpenVAS itu sendiri disusun sehingga dapat dihubungkan dengan tools yang telah diklasifikasikan berdasarkan frekuensi penggunaan pada tiap walkthrough. Hasil dari gambaran attack model berupa activity diagram dan data flow diagram berdasarkan 10 walkthrough. Pada activity diagram dibentuk sesuai tahapan dari walkthrough secara garis besarnya, sedangkan data flow diagram dibentuk sesuai tahapan dengan menunjukkan input dan output dari setiap penggunaan attack atau tools. 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 STRIDE sesuai peran atau fungsi.

7. Daftar Pustaka

[1] B. V. Tarigan, A. Kusyanti, and W. Yahya, “Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 1, no. 3, pp. 206–214, 2017.

[2] J. Zhang, D. Fang, and L. Liu, “Intelligent content filtering model for network security audit system,” *Proc. - 2009 2nd Int. Work. Knowl. Discov. Data Mining, WKKD 2009*, pp. 546–548, 2009, doi: 10.1109/WKDD.2009.26.

[3] D. Juardi, “Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus,” vol. 6, no. 1, pp. 11–19, 2017.

[4] M. P. Mokodompit and N. Nurlaela, “Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000 (Studi Kasus Pada Peguruan Tinggi X),” *J. Sist. Inf. Bisnis*, vol. 6, no. 2, p. 97, 2016, doi: 10.21456/vol6iss2pp97-104.

[5] H. El-Hadary and S. El-Kassas, “Capturing security requirements for software systems,” *J. Adv. Res.*, vol. 5, no. 4, pp. 463–472, 2014, doi: 10.1016/j.jare.2014.03.001.

[6] M. Muckin and S. C. Fitch, “A Threat-Driven Approach to Cyber Security,” *Lockheed Martin*, pp. 1–45, 2014.