IMPLEMENTASI DAN ANALISIS SECURITY AUDITING MENGGUNAKAN OPEN SOURCE SOFTWARE DENGAN FRAMEWORK MITRE ATT&CK

IMPLEMENTATION AND ANALYSIS OF SECURITY AUDITING USING OPEN SOURCE SOFTWARE WITH MITRE ATT&CK FRAMEWORK

Muhammad Athallariq Rabbani[1], Avon Budiyono[2], Adityas Widjajarto[3]

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

Abstrak

Security auditing merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi. Pada penelitian ini security auditing dilakukan berdasarkan analisa vulnerability dan threat agar dapat melihat hubungan yang terjadi antara vulnerability dan threat yang telah dilakukan pada aset IT tersebut. Pada penelitian ini objek yang digunakan yaitu vulnerable operating system (VulnOSv2) dengan tujuan untuk mengetahui vulnerability dan threat. Pada penilitian ini digunakan 10 walkthrough dengan tujuan dapat dilakukan analisis perbandingan pada masing masing walkthrough serta melihat efisiensi dari masing-masing tools yang digunakan.

Eksperimen dilakukan dengan menggunakan framework MITRE ATT&CK dimana digunakan sebagai dasar untuk pengembangan model dan metodologi ancaman. Open source software OpenVAS dapat diterapkan guna melihat hasil kuantitatif yang berdasarkan scanning eskploitasi berupa vulnerability. Sedangkan secara kualitatif dengan menyusun model attack trees. Framework MITRE ATT&CK yang dibuat dapat mengakomodasi model attack trees yaitu sebesar 80%.

Kata kunci : Security Auditing, Vulnerability, Threat, Risk, Framework MITRE ATT&CK

Abstract

Security auditing is the process of gathering and evaluating evidence to determine whether the computer system used has been able to protect the assets belonging to the organization. In this research, security auditing is conducted based on the analysis of vulnerability and threat in order to see the relationship that occurs between vulnerability and threats that have been carried out on these IT assets. In this study the object used is vulnerable operating system (VulnOSv2) with the aim to determine vulnerability and threat. In this research 10 walkthroughs are used with the aim that comparative analysis can be performed on each walkthrough and see the efficiency of each tool used.

Experiments were carried out using the MITRE ATT&CK framework which is used as a basis for developing threat models and methodologies. Open source software OpenVAS can be applied to see quantitative results based on exploitation scanning in the form of vulnerability. Whereas arranging attack tree models the MITRE ATT&CK Framework created can accommodate attack tree models, which is 80%.

Keywords : Security Auditing, Vulnerability, Threat, Risk, Framework MITRE ATT&CK

1. Pendahuluan

Keamanan sistem informasi adalah salah satu isu utama dalam perkembangan teknologi informasi dan komunikasi saat ini. Selain itu, bisnis penting untuk melindungi aset informasi organisasi dengan mengikuti pendekatan yang konprehensif dan terstruktur untuk memberikan perlindungan dari resiko organisasi yang mungkin di hadapi. Dalam upaya memecahkan masalah keamanan dibutuhkan penerapan metode yang dapat menjamin keamanan data, transaksi, dan komunikasi.

Untuk mendapatkan keamanan sistem informasi maka perlu melakukan evaluasi secara berkala terhadap keamanan sistem informasi. Evaluasi berkala dapat dilakukan dengan menggunakan audit internal terhadap keamanan sistem informasi tersebut. Audit internal maupun eksternal dapat menjadi salah satu cara untuk mengevaluasi keamanan informasi. Audit sistem informasi dilakukan untuk dapat menilai apakah teknologi informasi yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien[1].

Pada penelitian ini akan dilakukan implementasi *security auditing* menggunakan framework MITRE ATT&CK pada VulnOSv2. VulnOS merupakan virtual images yang tersedia pada website Vulnhub. VulnOS merupakan serangkaian sistem operasi yang dibuat khusus sebagai *virtual image* untuk meningkatkan ketrampilan pengujian penetrasi.

2. Dasar Teori

2.1 Aset IT

Aset IT merupakan pendukung operasional yang selalu terkait dalam setiap kegiatan yang ada, sehingga pengelolaannya memiliki fungsi yang penting untuk menjaga kondisi aset IT tersebut[2].

2.2 *Vulnerability*

Vulnerability merupakan kelemahan dalam suatu sistem yang memungkinkan penyerang untuk menjalankan sistem, mengakses data yang tidak sah, dan dapat melakukan serangan *Denial of Service* (DoS). Vulnerability dapat ditemukan di berbagai area dalam sistem Internet of Things (IoT)[3].

2.3 *Threat*

Threat merupakan tindakan yang memanfaatkan kelemahan keamanan dalam suatu sistem dan memiliki dampak negatif terhadapnya. *Threat* berasal dari dua sumber utama yaitu alam dan manusia. Ancaman alam seperti gempa bumi, angin topan dan kebakaran yang dapat menyebabkan kerusakan parah pada sitem komputer. Serta ancaman manusia adalah ancaman jahat yang terdiri dari ancaman internal (seseorang yang memiliki akses terhadap sistem) dan ancaman eksternal (individu tau organisasi yang bekerja pada luar jaringan) yang berusaha merusak dan mengganggu sistem [3].

2.4 *Risk*

Risk merupakan potensi kerugian atau kerusakan terhadap kerentanan akibat eksploitasi. *Risk* (resiko) merupakan kombinasi dari komponen kejadian yang menyangkut *threat* (ancaman), dan *vulnerability* (kelemahan).

2.5 *Security Auditing*

Audit secara umum adalah proses terpadu dalam pengumpulan dan penilaian terhadap informasi sebagai satu kesatuan organisasi oleh seorang ahli. Pengertian security auditing merupakan proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien[4].

2.6 *Penetrating Testing*

Penetration testing adalah tindakan pengujian sistem dengan cara mensimulasikan bentuk-bentuk serangan terhadap sistem tersebut sehingga akan diketahui tingkat kerentanannya. Pengujian dengan metode ini tentunya akan beresiko yang dapat mempengaruhi sistem[5].

2.7 *Walkthrough*

Walkthrough merupakan cara untuk melakukan identifikasi dan menilai sejak awal apakah desain yang diusulkan memenuhi persyaratan dan memenuhi tujuan. Tujuan *walkthrough* adalah untuk memberi pengguna kesempatan untuk membiasakan diri dengan sistem sebelum melakukan tes secara langsung[6].

2.8 *Threat Modelling*

Threat modelling adalah kumpulan aspek keamanan, serangkaian serangan yang masuk akal yang dapat mempengaruhi kinerja sistem komputer mana pun. Metodologi ini memungkinkan para pakar keamanan untuk mengidentifikasi risiko keamanan, dan mengembangkan langkah-langkah penanggulangan dalam fase desain, pengkodean, dan pengujian. Oleh karena itu, menganalisis dan memodelkan ancaman potensial yang dihadapi adalah langkah penting dalam proses merancang aplikasi yang aman[7].

2.9 *Activity Diagram*

Activity diagram merupakan diagram yang menggambarkkan *workflow* atau aktivitas dari sebuah sistem yang ada pada perangkat lunak[8].

2.10 *Data Flow Diagram*

Data Flow Diagram merupakan suatu model logika data atau proses yang dibuat untuk menggambarkan darimana asal data, dan kemana tujuan data yang keluar dari sistem, di mana data disimpan, proses apa yang menghasilkan data tersebut, dan interaksi antara data yang tersimpan, dan proses yang dikenakan pada data tersebut[9].

2.11 *Framework* MITRE ATT&CK

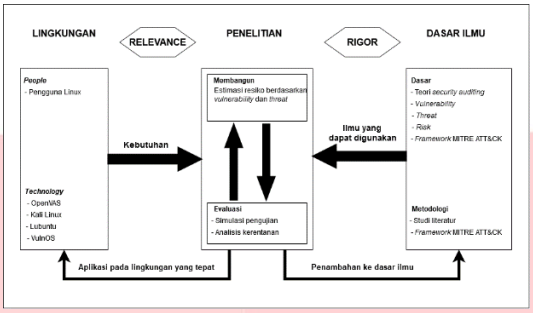
MITRE ATT&CK (*Adversary Technique Tactic & Common Knowledge*) merupakan basis pengetahuan yang

dapat diakses secara global dari taktik dan teknik yang berdasarkan pengamatan dunia nyata. Basis pengetahuan ATT&CK digunakan sebagai dasar untuk pengembangan model dan metodologi ancaman khusus di sektor swasta, sektor pemerintah, dan dalam komunitas produk dan layanan keamanan siber. Tujuan dari *framework* ini untuk meningkatkan pendeteksian, memecah dan mengklasifikasikan serangan secara konsisten dan jelas agar memudahkan untuk melihat kontras para penyerang serta menemukan bagaimana penyerang mengeksploitasi serta menembus jaringan[10].

3. Metodologi Penelitian

3.1 Model Konseptual Penelitian

Pada Gambar 1 dijelaskan bahwa model konseptual dibagi menjadi tiga bagian yaitu lingkungan, penelitian, dan dasar ilmu, selain itu dalam setiap bagian, memiliki entitasnya masing-masing.

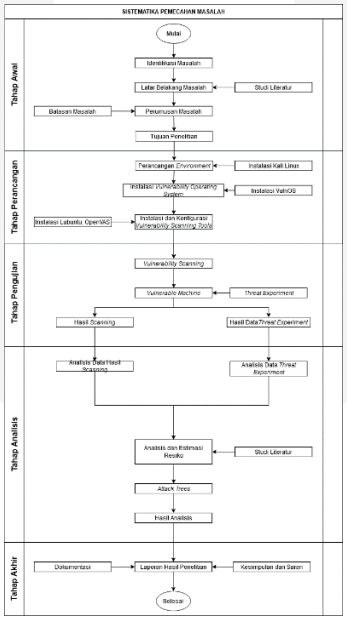


Gambar 1 Model Konseptual Penelitian

Dapat diketahui bahwa terdapat tiga ruang lingkup yaitu lingkungan, penelitian, dan dasar Ilmu. Pada aspek besar lingkungan yang dipengaruhi oleh faktor people dan technology diamana faktor tersebut mempengaruhi kemampuan, proses, dan infrastruktur dari VulnOS. Penelitian dilakukan untuk menganalisis estimasi resiko berdasarkan *vulnerability* dan *threat*. Dasar Ilmu berdasarkan teori *security auditing*, *vulnerability*, *threat* dan *risk*, serta *framework* MITRE ATT&CK.

3.2 Sistematika Pemecahan Masalah

Sistematika pemecahan masalah digunakan untuk memberikan penjelasan dan gambaran mengenai alur suatu penelitan agar dapat berjalan secara benar. Berikut merupakan tahapan sistematika pemecahan masalah pada penelitian ini:

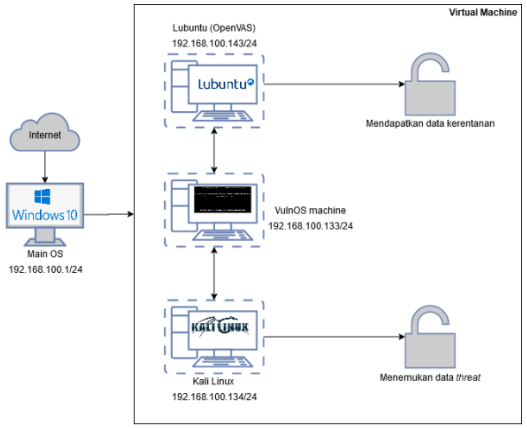


Gambar 2 Sistematika Pemecahan Masasalah

4. Perancangan Sistem dan Skenario Pengujian

4.1 Platform Eksperimen

Dalam melakukan suatu kegiatan dimana akan disimulasikan langkah-langkah yang bisa dilakukan untuk menemukan kerentanan yang terdapat pada *operating system*, berikut merupakan platform eksperimen yang dapat dilihat pada Gambar 3 di bawah ini:



Gambar 3 Platform Eksperimen

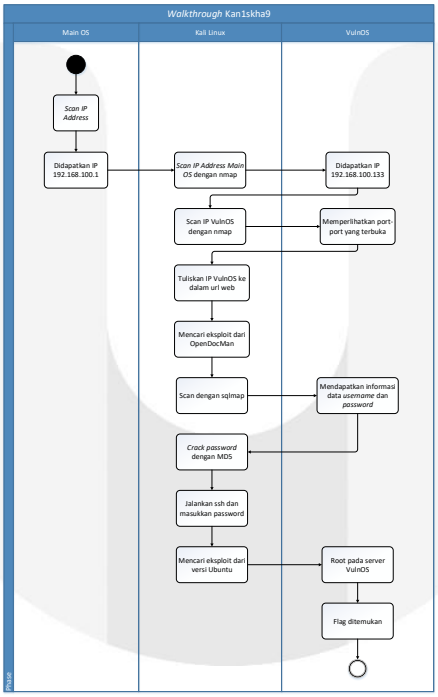
4.2 Daftar IP *Address*

Pada Tabel 1 di bawah ini, akan dijelaskan IP *address* yang digunakan pada penelitian kali ini:

Tabel 1 Daftar *IP Address*

Nama	*Host*	*Default Gateway*	*IP Address*
Main OS	Windows 10	192.168.100.1/24	192.168.100.1/24
VM1	Kali Linux		192.168.100.134/24
VM2	VulnOS		192.168.100.133/24
VM3	Lubuntu		192.168.100.143/24

4.3 Perumusan *Activity Diagram*



Gambar 4 Hasil Perumusan *Activity Diagram* Berdasarkan *Walkthrough*

Berikut merupakan penjelasan *activity diagram* dari Gambar 4 diatas. Pada penelitian ini akan dilakukan percobaan pertama mengikuti *walkthrough* milik Kan1skha9.

1. Tahap pertama lakukan *scan* IP *address* terlebih dahulu pada *Main* OS.
2. Tahap kedua lakukan *scan* IP *address* yang telah ditemukan pada *Main* OS menggunakan nmap pastikan VulnOS sudah menyala. IP *address* yang telah didapatkan merupakan IP *address* dari VulnOS gunanya untuk mengecek IP yang terdapat dalam satu jaringan.
3. Lalu lakukan *scan* menggunakan nmap, gunanya untuk memperlihatkan koneksi *port Transmission Control Protocol* (TCP) yang terbuka dan spesifik *port* yang digunakan.
4. Selanjutnya tuliskan IP tersebut pada *Uniform Resource Locator* (*url)* web, lalu akan dialihkan ke dalam *website* VulnOS.
5. Pada *website* VulnOS terdapat *hyperlink* yang akan membentuk jalan pintas langsung menuju *website* Jabc.
6. Pada *website* jabc klik bagian *documentation*, pada bagian tersebut akan ditemukan sebuah *clue* yang bertuliskan /jabcd0cs.

7. Tambahkan *clue* yang sudah ditemukan pada *url* web, lalu akan dialihkan ke dalam *website* OpenDocMan.
8. Selanjutnya lakukan analisis terhadap *website* OpenDocMan dan menemukan eksploit berdasarkan versi dari web tersebut yaitu OpenDocMan 1.2.7.
9. Lakukan pencarian terhadap ekpsloit yang relevan, lalu ditemukan eksploit berupa SQL *Injection*.
10. Tahap berikutnya adalah melakukan *scan* menggunakan sqlmap tujuannya adalah mencari kerentanan. Hasil *scan* yang didapatkan memperlihatkan data informasi penting didalamnya.
11. Langkah selanjutnya lakukan *hash* pada *password* yang ditemukan menggunakan MD5.
12. Selanjutnya adalah menjalankan perintah ssh, dengan tujuan untuk mengakses jaringan yang terenkripsi.
13. Lalu masukkan *password* yang sudah ditemukan sebelumnya, dengan begitu akses masuk berhasil dilakukan.
14. Selanjutnya mencari informasi tentang distro Linux yang digunakan. Lakukan pencarian terhadap eksploit yang relevan.
15. Selanjutnya lakukan pindah direktori ke dalam *root* pada VulnOS.
16. Setelah berhasil melakukan akses ke dalam *root*, maka *flag* berhasil ditemukan.

5. Analisis

5.1 Analisis *Vulnerability Scanning* Berdasarkan Data dari OpenVAS

Berdasarkan pengujian yang dilakukan pada VulnOSv2 menggunakan *tool* OpenVAS didapatkan hasil seperti pada Tabel 2 sebagai berikut:

Tabel 2 Analisis Hasil Vulnerability Scanning dengan OpenVAS

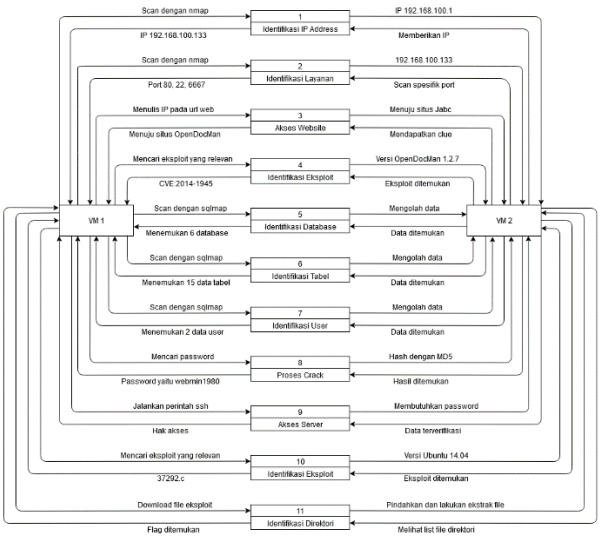
Host	*Threat Level*	*Total*
VulnOSv2	*High*	2
	Medium	1
	Low	2
	Log	0

Berdasarkan Tabel 2 diketahui bahwa hasil pengujian dengan OpenVAS pada VulnOSv2 ditemukan kerentanan dengan risiko *level high* sebanyak tiga, *level medium* sebanyak satu, *level low* sebanyak dua, dan level *log* sebanyak nol. Detail kerentanan yang ditemukan dari hasil pengujian menggunakan OpenVAS bisa dilihat pada Tabel 3 dibawah ini:

Tabel 3 Detail Analisis Hasil *Vulnerability Scanning* dengan OpenVAS

Description	*Service (Port)*	CVSS	*Threat Level*
Drupal Core Critical Remote Code Execution Vulnerability	80/tcp	7.5	*High*
SSH Brute Force Logins With Default Credentials Reporting	22/tcp	7.5	*High*
SSH Weak Encryption Algorithms Supported	22/tcp	4.3	*Medium*
SSH Weak MAC Algorithms Supported	22/tcp	2.6	*Low*
TCP timestamps	general/tcp	2.6	*Low*

5.2 Perancangan *Data Flow Diagram* Berdasarkan *Walkthrough*



Gambar 5 Hasil Data Flow Diagram Berdasarkan Walkthrough

Berikut merupakan penjelasan data flow diagram dari Gambar 5 diatas. Pada penelitian ini akan dilakukan percobaan pertama mengikuti walkthrough milik Kan1skha9.

1. Tahap pertama lakukan *scan* IP terlebih dahulu pada Main OS lalu didapatkan IP 192.168.100.1.
2. Tahap kedua lakukan *scan* IP yang telah ditemukan pada Main OS menggunakan nmap dengan *command* nmap -sn 192.168.100.1/24 yang berfungsi hanya untuk mengetahui host discovery yang terdapat pada sistem dan menonaktifkan *port scanning*. Dari *scan* tersebut ditemukan IP VulnOS yaitu 192.168.100.133.
3. Selanjutnya lakukan *scan* menggunakan nmap dengan *command* nmap -sT -sV -A -O -v -p 1-65535 192.168.100.133 yang berfungsi untuk memperlihatkan koneksi port TCP yang terbuka, memperlihatkan versi layanan pada port yang terbuka, memperlihatkan versi OS dan traceroute, meningkatkan tingkat *level* pencarian, melakukan *scan* spesifik port menyeluruh dari server lokal maupun *remote server***.** Dan ditemukan *port-port* yang terbuka yaitu 22, 80, dan 6667.
4. Selanjutnya tuliskan IP pada url web, lalu dialihkan ke dalam *website* VulnOS.
5. Pada *website* VulnOS terdapat *hyperlink* yang akan membentuk jalan pintas langsung menuju *website* Jabc.
6. Pada *website* Jabc klik bagian *documentation*, pada bagian tersebut akan ditemukan sebuah *clue* yang bertuliskan /jabcd0cs.
7. Setelah itu tambahkan /jabcd0cs pada url web, maka kita akan dialihkan ke *website* OpenDocMan.
8. Pada *website* OpenDocMan kita dapat melakukan pencarian eksploit berdasarkan versi tersebut yaitu OpenDocMan 1.2.7. Maka ditemukanlah eskploit yaitu CVE-2014-1945. Eksploit ini berupa SQL *Injection*.
9. Tahap berikutnya adalah melakukan *scan* menggunakan sqlmap tujuannya adalah mencari kerentanan.
10. *Scan* pertama menggunakan *command* sqlmap -u "http://192.168.100.133/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" --dbs --*level*=5 --risk=3 yang berfungsi untuk melakukan *scan* pada url yang dituju, melakukan *enumerate database*, menunjukan tingkat *level* kerentanan, dan *level* resiko. Hasil yang didapatkan berupa informasi mengenai *database* yang tersedia pada *website* tersebut berjumlah enam.
11. *Scan* kedua menggunakan *command* sqlmap -u "http://192.168.100.133/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" -D jabcd0cs --tables yang berfungsi untuk melakukan *scan* pada *database* jabcd0cs dan memperlihatkan informasi didalamnya berbentuk tabel. Hasil yang didapatkan berupa informasi mengenai tabel yang terdapat pada *database* jabcd0cs berjumlah lima belas.
12. *Scan* ketiga menggunakan *command* sqlmap -u "http://192.168.100.133/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" -D jabcd0cs -T odm_user --dump yang berfungsi untuk melakukaan *scan* pada *database* jabcd0cs pada tabel odm_user dan melihat data yang terdapat didalamnya. Hasil yang didapatkan berupa informasi mengenai data *user* berupa *username* dan *password* yang terenkripsi berjumlah dua.
13. Lakukan *hash password* yang masih terenkripsi menggunakan MD5 sehingga ditemukan *username* webmin dan *password* yaitu webmin1980.
14. Langkah selanjutnya adalah menjalankan perintah ssh, dengan tujuan untuk mengakses jaringan yang terenkripsi. Menggunakan *command* ssh webmin@192.168.100.133. Pada tahap ini akan dilakukan akses pada sistem webmin, dengan memasukkan *password* yang telah ditemukan sebelumnya.
15. Seletah itu jalankan perintah python dengan *command* python -c 'import pty;pty.spawn("/bin/bash")' agar mendapatkan akses *privilege*, serta lakukan identifikasi terhadap sistem yang digunakan dengan *command* uname -a. Ditemukan versi linux pada VulnOSv2 yang digunakan yaitu 3.13.
16. Selanjutnya tuliskan *command* cat /etc/lsb-release. Sehingga ditemukan spesifikasi sistem yang digunakan yaitu Ubuntu 14.04.4 LTS.
17. Lalu lakukan pencarian eksploit yang relevan, sehingga ditemukan CVE-2015-1328 yang berisi *file* terenkripsi 37292.
18. Selanjutnya jalankan *command* cd /tmp untuk melakukan perpindahan direktori ke dalam tmp. Pada tahap ini kita sudah didalam root.
19. Lalu *download file* tersebut dengan *command* wget https://www.exploit-db.com/download/37292 tunggu hingga selesai, lalu lakukan cek menggunakan *command* ls dan melihat *file* berhasil di *download*.
20. Pindahkan *file* tersebut ke dalam folder ofs.c dengan *command* mv 37292 ofs.c.
21. Lakukan ekstrak *file* menggunakan *command* gcc ofs.c -o ofs. Selanjutnya tuliskan *command* ./ofs untuk melihat informasi yang terdapat didalamnya.
22. Tahap terakhir yaitu tuliskan *command* cat /root/flag.txt dengan begitu *flag* berhasil ditemukan.

5.3 Analisis Perhitungan *Vulnerability* Dengan CVSS Calculator v2

Berikut merupakan perhitungan *Common Vulnerability Scoring System Calculator* (CVSS) versi 2 dengan tujuan untuk mengetahui kerentanan dan dampak yang ditimbulkan didapatkan hasil seperti pada Tabel 4 sebagai berikut:

Tabel 4 Hasil Perhitungan Dengan CVSS *Calculator* v2

Description	**CVSS *Vector***
Drupal Core Critical Remote Code Execution Vulnerability	AV:N/AC:L/Au:N/C:P/I:P/A:P

SSH Brute Force Logins With Default Credentials Reporting	AV:N/AC:L/Au:N/C:P/I:P/A:P
SSH Weak Encryption Algorithms Supported	AV:N/AC:M/Au:N/C:P/I:N/A:N
SSH Weak MAC Algorithms Supported	AV:N/AC:H/Au:N/C:P/I:N/A:N
TCP timestamps	AV:N/AC:H/Au:N/C:P/I:N/A:N

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

Berikut merupakan perhitungan dari banyaknya pemakaian *tools* dari setiap *walkthrough*. Untuk menghitung risiko secara kuantitatif menurut Stephen Watts pada BMC dapat digunakan formulasi rumus sebagai berikut:

$$Risk = Threat \times Vulnerability$$

Tabel 5 Analisis Resiko Secara Kuantitatif

Description	**CVSS**	***Tools***	***Frequency***	***Risk***	***Total***
Drupal Core Critical Remote Code Execution Vulnerability	7.5	Sqlmap	10	75	135
		Dirb	5	37.5	
		Nikto	3	22.5	
SSH Brute Force Logins With Default Credentials Reporting	7.5	Sqlmap	10	75	84
		Hydra	1	7.5	
		Metasploit framework	2	15	
SSH Weak Encryption Algorithms Supported	4.3	Nikto	3	12.9	98,9
		Sqlmap	10	43	
		SSH	10	43	
SSH Weak MAC Algorithms Supported	2.6	SSH	10	26	39
		DIRB	5	13	
TCP timestamps	2.6	Nmap	10	26	26

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

Perancangan *attack trees* ini dilakukan untuk menggambarkan resiko secara kualitatif kemungkinan serangan pada suatu aset atau target dapat diwujudkan. Selain itu rancangan *security auditing* pada penelitian ini menggunakan dasar *attack tree* yang mengacu kepada *technical paper* berjudul "*Measuring the Overall Network Security by Combining CVSS Scores Based on Attack Graphs and Bayesian Networks*". Tahapan menyusun CVE menggunakan *Topological Vulnerability Analysis* (TVA). Dengan membuat *attack trees* sebagai grafik serangan yang akan memberikan informasi tentang hubungan antar komponen jaringan yang berfungsi untuk melihat kemungkinan potensi serangan yang akan terjadi. CVE tersebut ditentukan berdasarkan dari 10 *walkthrough* yang telah dijalankan. Penentuan CVE yang telah dibuat *attack trees* berdasarkan dari hasil *full report scanning* menggunakan OpenVAS.

Gambar 6 Hasil Perumusan *Attack Trees*

5.5 Analisis Resiko dan Perumusan *Attack Trees* Berdasarkan *Framework* MITRE ATT&CK

Tabel 6 Perumusan *Attack Tree* Berdasarkan *Framework* MITRE ATT&CK

CVE	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
CVE-2017-7679	X	X			X	X						X
CVE-2014-1945	X	X		X		X	X					X
CVE-2016-6515	X	X	X	X	X	X	X	X		X		X
CVE-2015-6564	X	X	X	X						X		X
CVE-2018-7600	X		X	X		X	X	X	X			X
CVE-2016-0777	X		X	X			X	X				
CVE-2015-5352	X	X	X		X	X				X		X
CVE-2015-8325	X	X	X	X	X	X				X		X
CVE-2015-1328	X	X	X	X			X					

Pada Tabel 6 ditemukan bahwa *framework* MITRE ATT&CK hanya dapat mengakomadasi *attack trees* sebanyak 83,3%. Angka ini didapatkan berdasarkan formulasi sebagai berikut:

$$\frac{10}{12} \times 100\% = 83{,}33333333333333\%$$

Hal ini disebabkan karena 12 karakterisitk yang harusnya bisa dipenuhi oleh masing-masing CVE ternyata dari seluruh CVE yang didapatkan paling banyak hanya memenuhi 10 dari 12 karakteristik saja. Artinya *framework* MITRE ATT&CK tidak mengakomodasi secara sempurna, namun hampir sempurna. Angka 83,3% terbilang cukup tinggi karena lebih dari 50% sudah mengakomodasi. Dimana CVE yang mewakili presentase tertinggi adalah CVE-2016-6515

6. Kesimpulan

Perhitungan risiko tertinggi secara kuantitatif terhadap *vulnerability* yang telah dibentuk ditemukan lima *vulnerability* yaitu *high*, l*ow*, dan *medium.* Dari kelima vulnerability ini nilai risiko paling tinggi sebesar 135 pada *Drupal Core Critical Remote Code Execution Vulnerability*. Framework MITRE ATT&CK dapat mengakomadasi *security auditing* berdasarkan risiko secara kualitatif sebesar 80%. Rincian CVE akan mempengaruhi hasil akurasi penentuan *security auditing*.

Daftar Pustaka:

[1] Herlinudinkhaji, D., & Daru, A. F. (2015). Audit Layanan Teknologi Informasi Berbasis Information Technology Infrastructure Library (ITIL). Jurnal Informatika UPGRIS Volume 1 No.2, 111-112.

[2] Rahman, Z., Widodo, A. P., & Sukmaaji, A. (2016). SISTEM INFORMASI MANAJEMEN ASET TI PADA KEMENTERIAN AGAMA KOTA PROBOLINGGO. JSIKA Vol. 5, No. 5. Tahun 2016,1.

[3] Abomhara, M., & Køien, G. M. (2015). Cyber Security and the Internet of Things Vulnerabilities, Threats, Intruders and Attacks. Cyber security and the Internet of Things, 71-72.

[4] Hanindito, G. A. (2017). Analisis dan Audit Sistem Manajemen Keamanan Informasi (SMKI) pada Instansi Perpustakaan dan Arsip Daerah Kota Salatiga. JURNAL NASIONAL TEKNOLOGI DAN SISTEM INFORMASI - VOL. 3 NO.2 (2017) 279-284 , 279.

[5] Pujiarto, B., Utami, E., & Sudamarwan. (2013). EVALUASI KEAMANAN WIRELESS LOCAL AREA NETWORK MENGGUNAKAN METODE PENETRATION TESTING (KASUS : UNIVERSITAS MUHAMMADIYAH MAGELANG). JURNAL DASI Vol. 14 No. 2 JUNI 2013, 16.

[6] Nieminen, M., & Koivunen, M. R. (1995). Visual Walkthrough. A short paper to be presented at HCI'95 at Huddersfield, UK, 1.

[7] Laorden, C., Sanz, B., Alvares, G., & Bringas, P. G. (2010). A Threat Model Approach to Threats and Vulnerabilities in On-line Social Networks. 2.

[8] Putra, D. W., & Andriani, R. (2019). Unified Modelling Language (UML) dalam Perancangan Sistem Informasi Permohonan Pembayaran Restitusi SPPD. Vol. 7 No. 1 April 2019, 33.

[9] Kristanto, A. (2008). Perancangan Sistem Informasi dan Aplikasinya. Yogyakarta : Gava Media.

[10] Pennington, A., Applebaum, A., Nickels, K., Schulz, T., Strom, B., & Wunder, J. (2019). GETTING STARTED WITH ATT&CK. United Stated: The MITRE Corporation.