SECURITY AUDITING PADA *VULNERABLE MACHINE* MENGGUNAKAN *SNORT INTRUISON DETECTION SYSTEM* DAN *GREENBONE OPENVAS* BERDASARKAN *NASIONAL INSTITUTE OF STANDART AND TECHNOLOGY CYBERSECURITY FRAMEWORK*

SECURITY AUDITING PADA *VULNERABLE MACHINE* MENGGUNAKAN *SNORT INTRUISON DETECTION SYSTEM* DAN GREENBONE *OPENVAS* BERDASARKAN *NASIONAL INSTITUTE OF STANDART AND TECHNOLOGY CYBERSECURITY FRAMEWORK*

Krisfian Adji Brata[1], Umar Yunan Kurnia Septo Hediyanto[2], Adityas Widjajarto[3]

[1,2,3] Universitas Telkom

adjikrisfian@student.telkomuniversity.ac.id[1], umaryunan@telkomuniversity.ac.id[2], adtwjrt@telkomuniversity.ac.id[3]

Abstrak :

Penelitian ini bertujuan untuk menganalisa kerentanan dan threat dalam menentukan profil resiko dari vulnerable machine. *Vulnerable machine* yang dipakai dalam penelitian ini yaitu *Typhoon OS* melalui proses *security auditing*. *Security Auditing* diperlukan untuk mengetahui seberapa besar resiko OS terkena serangan dan menyusun solusi untuk OS tersebut. *Framework* yang dipakai dalam penelitian ini yaitu *NIST cybersecurity framework*, karena *NIST cybersecurity framework* merupakan *framework* yang bersifat defensif dan cocok pada penelitian ini. Aplikasi yang dipakai dalam menunjang proses auditing ini yaitu *OpenVAS* dan *Snort*. *OpenVAS* dipakai karena memiliki database kerentanan yang cukup lengkap serta hasil scan mudah untuk dibaca. *Snort* dipakai karena memiliki tabel rules yang cukup lengkap dibanding *IDS* lain serta untuk akurasi deteksi seperti scanning port snort lebih unggul dibanding *IDS* lainnya. Untuk itu dilakukan analisa kerentanan yang ada dalam OS. Dengan melakukan analisa kerentanan, dapat diketahui model serangan apa saja yang bisa dipakai untuk melakukan penyerangan.kemudian dilakukan juga eksperimen penyerangan menggunakan literatur/walkthrough. Dari eksperimen akan dicari relasi antara vulnerability dan threat, dari hubungan antara *vulnerability* dan *threat,* akan diperoleh profil resiko. Dari hasil profil resiko, dapat diketahui seberapa besar bahaya dari setiap kerentanan yang ada pada OS. Kemudian setelah dilakukan pemecahan masalah dapat dilihat hasil bahwa "*CUPS < 2.0.3 Multiple Vulnerabilities*" merupakan *vulnerability* dengan kerentanan yang terbesar dari beberapa vulnerability yang ada yaitu dengan skor 30(50 %) dengan Nmap sebagai tools yang paling banyak terdeteksi yaitu 6 kali dari enam walkthrough yang dicoba. Dari hasil profil resiko juga menunjukkan bahwa *vulnerable machine* khususnya Typhoon memiliki resiko yang tinggi atas serangan siber.

Kata kunci : security auditing, vulnerable machine, framework, profil resiko,model serangan.

Abstract :

This research is to analyze vulnerabilities and threats in determining the risk profile of vulnerable machines. The Vulnerable machine used in this research is Typhoon OS through a security auditing process. Security Auditing is needed to find out how much risk the OS is exposed to and develop a solution for the OS. The framework used in this research is the NIST cybersecurity framework, because the NIST cybersecurity framework is a defensive framework and is suitable for this research. The applications used to support this auditing process are OpenVAS and Snort. OpenVAS is used because it has a fairly complete vulnerability database and the scan results are easy to read. Snort is used because it has a fairly complete rules table compared to other IDS and for detection accuracy

such as port scanning, Snort is superior to other IDS. For this reason, an analysis of existing vulnerabilities in the OS is carried out. By conducting a vulnerability analysis, it can be seen what attack models can be used to carry out attacks. Then an attack experiment using literature/walkthrough is also carried out. From the experiment, the relationship between vulnerability and threat will be searched, from the relationship between vulnerability and threat, a risk profile will be obtained. From the results of the risk profile, it can be seen how big the danger of each vulnerability that exists in the OS. Then after solving the problem, it can be seen that "CUPS < 2.0.3 Multiple Vulnerabilities" is a vulnerability with the greatest vulnerability of several existing vulnerabilities, namely with a score of 30 (50%) with Nmap as the most detected tool, which is 6 times out of six. Tried walkthrough. The results of the risk profile also show that vulnerable machines, especially Typhoons, have a high risk of cyber attacks.

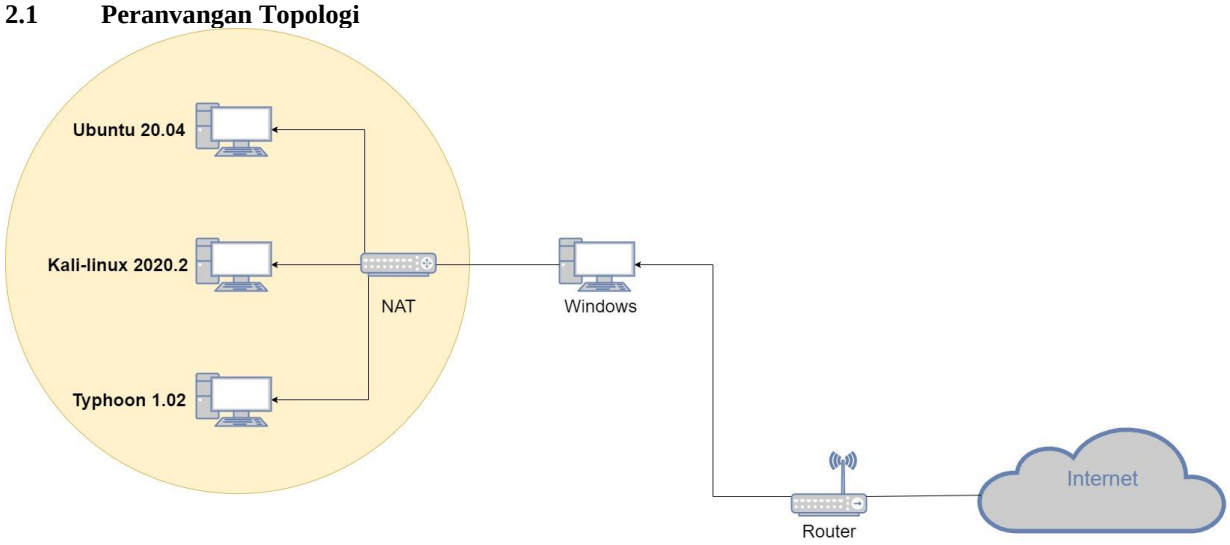
Keyword : security auditing, vulnerable machines, framework, risk profile, attack model

1. Pendahuluan

Proses atau aktivitas *security auditing* kerentanan sistem operasi sangat penting untuk mencegah serta mengurangi dampak kerusakan karena akibat adanya serangan dari pihak yang tidak bertanggung jawab. Hal ini menjadi dasar untuk meningkatkan kesadaran dan melakukan langkah awal untuk mendeteksi, mengidentifikasi dan mempelajari kelemahan yang dimiliki dari suatu sistem operasi. Faktor-faktor internal dan eksternal yang menjadi kelemahan tersebut adalah kurangnya kesadaran pemilik sistem operasi dan kurangnya *maintenance* serta pembaruan untuk sistem operasi tersebut. Openvas merupakan alat bantu uji kerentanan dengan sumber kode terbuka yang mampu menjadi salah satu solusi untuk memberikan gambaran dari sebuah penelusuran celah keamanan. IDS adalah *tool*, metode atau sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan computer. Melakukan uji kerentanan akan mampu membantu proses identifikasi kelemahan dalam sistem sebelum serangan dapat terjadi serta dapat menjadi langkah pencegahan dalam meningkatkan keamanan terhadap sebuah sistem. Diperlukan suatu upaya untuk mengauditing sistem operasi. Salah satu upaya tersebut adalah *security auditing* berdasarkan National Institute of Standard Technology (NIST), terhadap *vulnerablemachine*. Penelitian ini menyajikan tentang pengendalian terhadap ancaman serangan pada sistem dengan memberikan solusi perbaikan untuk menahan resiko melalui vulnerability assessment.

2. Perancangan Eksperimen dan Implementasi

2.1 Peranvangan Topologi



2.2 Skenario pengujian yang akan dilakukan pada penelitian ini terbagi menjadi 2, yaitu skenario pengujian menggunakan OpenVAS dan skenario peyerangan menggunakan threat model/walkthrough.

2.2.1 Skenario Pengujian Menggunakan OpenVAS

Pada skenario pengujian, dilakukan vulnerability scanning pada Typhoon OS untuk mendeteksi setiap kerentanan/vulnerability yang ada didalam Typhoon OS. Skenario Pengujian dapat dilakukan sebagai berikut :

1. Memasukkan IP address yang akan di-scanning
2. Setelah proses scanning selesai, maka keluar hasil scan Typhoon OS
3. Klik salah satu vulnerability untuk melihat detail kerentanan

2.2.2 Skenario Penyerangan Menggunakan Walkthrough

Pada skenario penyerangan, dilakukan ujicoba serangan terhadap Typhoon OS berdasarkan threat model/walkthrough yang ada. Pada penelitian ini, skenario pengujian serangan yang dipakai yaitu walkthrough dari tujuh sumber, yaitu dari :

1. Walkthrough 1 *https://www.hackingarticles.in/typhoon-1-02-vulnhub-walkthrough*
2. Walkthrough 2 https://medium.com/@tusharroutray/typhoon-1-02-a-vulnhub-vm-walkthrough
3. Walkthrough 3 *https://www.sevenlayers.com/index.php/126-vulnhub-typhoon-1-02-walkthrough*
4. Walkthrough 4 *https://resources.infosecinstitute.com/typhoon-ctf-walkthrough/#gref*
5. Walkthrough 5 https://www.hackingarticles.in/typhoon-1-02-vulnhub-walkthrough/

6. Walkthrough 6 https://hackso.me/typhoon-1.02-walkthrough/

2.3 Data Eksperimen

Setelah dilakukan skenario pengujian dengan OpenVAS dan skenario penyerangan menggunakan walkthrough, maka didapatkan data hasil eksperimen sesuai skenario yang telah dilakukan. Data eksperimen dapat dijabarkan sebagai berikut :

2.3.1 Data Keluaran Hasi Uji *Walktrough* ke Typhoon OS

Setelah dilakukan proses penyerangan sesuai dengan yang telah di skenariokan sebelumnya, maka didapat data hasil eksperimen sebagai berikut :

No	*Step* Serangan	Hasil Scan Snort (berhasil/tidak)
1.	Melakukan *netdiscover*	Negatif (-)
2.	Scan os korban menggunakan Nmap	Positif (+)
3.	Membuka mongoadmin dari Kali Linux	Negatif (-)
4.	Mencari username dan password typhoon di database mongoDB	Negatif (-)
5.	Setelah mendapat username dan password, masuk kedalam typhoon melalui ssh	Negatif (-)
6.	Mencari *Exploit* menggunakan searchsploit	Negatif (-)
7.	Copy *Exploit* kedalam mesin Kali Linux	Negatif (-)
8.	Menjalankan SimpleHTPPServer	Negatif (-)
9.	Mengunduh file *Exploit* kedalam directory /tmp di typhoon menggunakan wget	Positif (-)
10.	Meng-*compile* file *Exploit* yang telah diunduh di sebelumnya	Negatif (-)
11.	Mengubah file permission dari file *Exploit* yang telah *compile* sebelumnya	Negatif (-)
12.	Menjalankan file *Exploit*	Negatif (-)
13.	Mencari flag root	Negatif (-)

2.3.2 Data Keluaran Hasil Uji Openvas

No	*Vulnerability*	CVE Number	CVSS Score
1.	CUPS < 2.0.3 Multiple Vulnerabilities	CVE-2015-1158	10.0
2.	PostgreSQL weak password	CVE-2007-3279	9.0
3.	*Redis Server No Password*	-	7.5
4.	*Apache Tomcat servlet/JSP container default files*	CVE-2017-12617	6.8
5.	*Anonymous FTP Login Reporting*	CVE-2017-1000254	6.4
6.	SSL/TLS: Report Weak Cipher Suites	CVE-2015-2808	5.0
7.	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	CVE-2016-2183	5.0
8.	Check if Mailserver answer to VRFY and EXPN requests	-	5.0
9.	WebCalendar User Account Enumeration Disclosure Issue	CVE-2012-1495	5.0

10.	Cleartext Transmission of Sensitive Information via HTTP	CVE-2019-6845	4.8
11.	FTP Unencrypted Cleartext Login	-	4.8
12.	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	-	4.3
13.	SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	-	4.3
14.	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	CVE-2014-3566	4.3
15.	SSH Weak Encryption Algorithms Supported	CVE-2017-5243	4.3
16.	jQuery < 1.9.0 XSS Vulnerability	CVE-2012-6708	4.3
17.	ISC BIND Security Bypass Vulnerability (Remote)	CVE-2017-3143	4.3
18.	TCP timestamps	CVE-2019-18625	2.6
19.	SSH Weak MAC Algorithms Supported	CVE-2008-5161	2.6

2.3.3 Perumusan Activity Diagram berdasarkan Walkthrough

Setelah melakukan serangan terhadap Typhoon OS, dapat dilakukan perumusan activity diagram berdasarkan walkthrough yang telah dipakai. Activity Diagram berfungsi untuk memperlihatkan urutan aktivitas yang dilakukan berdasarkan langkah-langkah penyerangan walkthrough agar walkthrough lebih mudah dipahami. Pada penelitian ini, Activity Diagram berfungsi untuk memodel serangan/walkthrough. (Activity Diagram Terlampir)

2.3.4 Perumusan Data Flow Diagram berdasarkan Walkthrough

Setelah membuat activity diagram dari setiap walkthrough yang dibuat, dapat dibuat Data Flow Diagram. Data Flow Diagram berfungsi memberitahu aliran data dari setiap walkthrough yang dibuat. (Data Flow Diagram Terlampir)

2.3.5 Perumusan Data Security Auditing

Pada bagian ini, akan dilakukan proses security auditing menggunakan NIST Cysbersecurity Framework (CSF) yang dikembangkan oleh WatkinsConsulting. WatkinsConsulting adalah perusahaan konsultan akuntansi dan manajemen forensik yang berspesialisasi dalam semua aspek industri Layanan Keuangan dan sektor Pemerintah Federal. WatkinsConsulting sendiri menyusun framework NIST Cybersecurity agar bisa dipakai dalam proses security auditing. Perumusan data dilakukan dengan menjawab pertanyaan yang ada didalam lembar excel. Pilihan jawaban ada 4, yaitu : Yes, No, N/A, dan blank.

3. Pembahasan

3.1. Analisa Vulnerability

No	Vulnerability	Severity	Kategori	Qod	CVE	Impact	Port	Detail Vulnerability	Solution
1.	CUPS < 2.0.3 Multiple Vulnerabilities	10.0	High	100 %	CVE-2015-1158	Memungkinkan penyerang yang tidak diautentikasi mendapatkan priviledge untuk melakukan akses di server CUPS.	631 / tcp	Berbagai CUPS rentan terhadap priviledge escalation karena keslahan malakukan manajemen memori.	Harus melakukan update terhadap CPU yang terbaru/competible
2.	PostgreSQL weak password	9.0	High	9.8%	CVE-2007-3279	Akun pengguna mungkin mudah dapat digunakan dengan leluasa oleh	5432/tcp	Pengguna dapat dimungkinkan masuk kePostgreSQL	Dianjurkan untuk sesegera mungkin

						penyerang.		dari jarak jauh PostgreSQL masihh menggunakan credential yang lemah.	untuk mengubah password.
3	*Redis Server No Password*	7.5	Medium	100 %	-	Masalah ini dapat dimanfaatkan oleh penyerang jarak jauh untuk mendapatkan keuntungan mengakses informasi sensitif atau mengubah konfigurasi sistem.	6379/tcp	Server Redis jarak jauh tidak dilindungi dengan kata sandi, dimana memungkinkan penyerang masuk tanpa kasa sandi.	Memberi atau Mengatur ulang password.
4.	*Apache Tomcat servlet/JSP container default files*	6.8	Medium	99%	CVE-2017-12617	File-file ini harus dihapus karena dapat membantu penyerang menebak file yang tepat dari Apache Tomcat yang berjalan di host ini dan mungkin memberikan informasi berguna lainnya.	8080/tcp	Wadah Apache Tomcat servlet / JSP telah menginstal file default.	Hapus file default, contoh JSP dan Servlet dari Tomcat Servlet/JSP.
5.	*Anonymous FTP Login Reporting*	6.4	Medium	80%	CVE-2017-1000254	Berdasarkan file yang dapat diakses melalui login FTP anonim, penyerang mungkin dapat melakukan akses ke file sensitive dam mengunggah atau menghapus file.	21/tcp	Melaporkan jika Server FTP jarak jauh memungkinkan login anonim.	Jika kita tidak ingin berbagi file keuser lain lebih baik kita menonaktifkan login sebagai anonim
6.	SSL/TLS: Report Weak Cipher Suites	5.0	Medium	98%	CVE-2015-2808	Tidak ada dampak hanya saja agar lebih memperhatikan untuk membuat laporan rutin prihal rangkaian sandi SSL/TLS lemah yang diterima oleh suatu layanan.	110 / tcp	Kerentanan ini melaporkan semua suite cipher SSL / TLS yang lemah yang diterima oleh suatu layanan.	Konfigurasi layanan ini harus diubah sehingga tidak lagi menerima rangkaian sandi lemah yang terdaftar.
7.	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0	Medium	98%	CVE-2016-2183	Berdampak terhadap layanan yang menerima rangkaian sandi SSL/TLS yang rentan melalui HTTPS	631 / tcp	Kerentanan ini melaporkan semua suite sandi SSL / TLS yang diterima oleh layanan di mana vektor serangan hanya ada pada layanan HTTPS.	Konfigurasi layanan ini harus diubah sehingga tidak lagi menerima rangkaian sandi lemah yang terdaftar.

8.	Check if Mailserver answer to VRFY and EXPN requests	5.0	Medium	99%	-	SMPT Problem	25/tcp	Mailserver pada host ini menjawab permintaan VRFY dan/atau EXPN.	Nonaktifkan VRFY dan/atau EXPN di Mailserver Anda.
9.	WebCalendar User Account Enumeration Disclosure Issue	5.0	Medium	99%	CVE-2012-1495	-	80/tcp	Masalah Pengungkapan Enumerasi Akun PenggunaWebCalendar.	Diharapkan untuk mengupdate versi.
10.	Cleartext Transmission of Sensitive Information via HTTP	4.8	Medium	80%	CVE-2019-6845	Seseorang dapat menyalah gunakan akun serta dapat mengorek informasi secara paksa melalui komunikasi http antar klien.	8080/tcp	Tuan rumah / aplikasi mengirimkan informasi sensitif (nama pengguna, kata sandi) dalam teks lengkap melalui HTTP.	Pastikan host/aplikasi mengarahkan semua pengguna ke koneksi SSL/TLS yang aman sebelum mengizinkan masuk kedalam data sesitif
11.	FTP Unencrypted Cleartext Login	4.8	Medium	70 %	-	Penyerang dapat menemukan nama login dan sandi dengan mengendus lalu lintas ke Layanan FTP.	21/tcp	Remote host menjalankan layanan FTP yang memungkinkan login cleartext melalui koneksi yang tidak terenkripsi.	Aktifkan FTPS atau terapkan koneksi melalui perintah AUTH TLS.
12.	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3	Medium	98%	-	Penyerang mungkin dapat menggunakan kelemahan kriptografi yang diketahui untuk menguping koneksi antara klien dan layanan untuk mendapatkan akses ke data sensitif yang ditransfer dalam koneksi aman.	5432/tcp	Memungkin untuk mendeteksi penggunaan protokol SSLv2 dan/atau SSLv3 yang tidak digunakan lagi pada sistem ini.	Disarankan untuk menonaktifkan protokol SSLv2 dan/atau SSLv3 yang tidak digunakan lagi yang mendukung protokol TLSv1

3.2 Analisa Frekuensi Tools Serangan

Setelah mengetahui jenis-jenis vulnerability dari Typhoon OS, dapat dilakukan pembuatan tabel dari daftar frekuensi tools serangan yang dipakai untuk melakukan serangan ke typhoon. Daftar frekuensi tools dapat dibuat dengan formula :

Frekuensi tools = a / jumlah maksimal tools x 100

a = Berapa kali tools dipakai dalam satu walkthrough (satu walkthrough maks 1 kali) Setelah didapatkan rumus frekuensi tools, maka dapat dibuat tabel frekuensi tools sebagai berikut :

No	Nama *Tools*	a	Hasil

1.	Nmap	6	1 (100%)
2.	exploit	5	0.83 (83.3%)
3.	Msf	3	0.5 (50%)
4.	Nikto	2	0.33 (33.3%)
5.	Hydra	2	0.33 (33.3%)
6.	dirb	1	0.125 (16.6%)
7.	Phpinject	1	0.16 (16.6%)
8.	gobuster	1	0.16 (16.6%)
9.	Hashcat	1	0.16 (16.6%)
10.	Msfvenom	1	0.16 (16.6%)

Dapat dilihat dari tabel frekuensi *tools* diatas bahwa Nmap merupakan tools yang paling sering dipakai untuk melakukan penyerangan. Karena frekuensi pemakaian Nmap 100% disetiap *walkthrough*, maka Snort IDS dirancang agar bisa mendeteksi scan dari Nmap. Dilihat dari tabel hasil pencobaan *walkthrough* diatas bahwa Snort IDS dapat mendeteksi serangan Nmap sehingga Snort IDS dapat dianggap sebagai IDS yang mumpuni dalam pendeteksian serangan.

3.3 Permusan Attack Tree

Jika dihubungkan dengan implementasi serangan yang sudah dilakukan sebelumnya, dapat dibuat *attack tree* dari setiap *walkthroughnya*. Berikut perumusan *attack tree* dari setiap *walkthrough* :

- Walkthrough 1

Walkthrough pertama yang terdiri dari 13 step memiliki lima Common Vulnerabilities Exposures (CVE) atau memiliki lima kerentanan dari daftar kerentanan yang ada di dalam typhoon dengan rincian :

- CVE-2014-3566 dengan skor CVSS 4.3
- CVE-2019-6845 dengan skor CVSS 4.8
- CVE-2017-5243 dengan skor CVSS 4.3
- CVE-2014-3566 dengan skor CVSS 4.3
- CVE-2014-6271 dengan skor CVSS 10.0

- Walkthrough 2

Walkthrough kedua yang terdiri dari 14 step memiliki tujuh Common Vulnerabilities Exposures (CVE) atau memiliki tujuh kerentanan dari daftar kerentanan yang ada di dalam typhoon dengan rincian :

- CVE-2014-3566 dengan skor CVSS 4.3
- CVE-2017-1000254 dengan skor CVSS 6.4
- CVE-2017-12617 dengan skor CVSS 6.8
- CVE-2014-3566 dengan skor CVSS 4.3
- CVE-2011-0518 dengan skor CVSS 5.1
- CVE-2014-3566 dengan skor CVSS 4.3
- CVE-2014-6271 dengan skor CVSS 10.0

- Walkthrough 3

Walkthrough ketiga yang terdiri dari 12 step memiliki delapan Common Vulnerabilities Exposures (CVE) atau memiliki delapan kerentanan dari daftar kerentanan yang ada di dalam typhoon dengan rincian :

- CVE-2014-3566 dengan skor CVSS 4.3
- CVE-2014-3566 dengan skor CVSS 4.3
- CVE-2019-6845 dengan skor CVSS 4.8
- CVE-2012-1495 dengan skor CVSS 5.0
- CVE-2019-6845 dengan skor CVSS 4.8
- CVE-2015-2808 dengan skor CVSS 5.0
- CVE-2015-2808 dengan skor CVSS 5.0

- CVE-2014-6271 dengan skor CVSS 10.0

➢ *Walkthrough* 4

Walkthrough keempat yang terdiri dari 10 step memiliki lima *Common Vulnerabilities Exposures* (CVE) atau memiliki lima kerentanan dari daftar kerentanan yang ada di dalam typhoon dengan rincian :

- CVE-2014-3566 dengan skor CVSS 4.3
- CVE-2017-1000254 dengan skor CVSS 6.4
- CVE-2019-6845 dengan skor CVSS 4.8
- CVE-2018-7600 dengan skor CVSS 5.0
- CVE-2014-6271 dengan skor CVSS 10.0

➢ *Walkthrough* 5 (Sebagai referensi)

Walkthrough kelima yang terdiri dari 10 step memiliki empat *Common Vulnerabilities Exposures* (CVE) atau memiliki empat kerentanan dari daftar kerentanan yang ada di dalam typhoon dengan rincian :

- CVE-2014-3566 dengan skor CVSS 4.3
- CVE-2017-12617 dengan skor CVSS 6.8
- CVE-2015-1158 dengan skor CVSS 10.0
- CVE-2017-1000254 dengan skor CVSS 6.4
- CVE-2014-6271 dengan skor CVSS 10.0

➢ *Walkthrough* 6 (sebagai referensi)

Walkthrough keenam yang terdiri dari 8 step memiliki empat *Common Vulnerabilities Exposures* (CVE) atau memiliki empat kerentanan dari daftar kerentanan yang ada di dalam typhoon dengan rincian :

- CVE-2014-3566 dengan skor CVSS 4.3
- CVE-2015-2808 dengan skor CVSS 5.0
- CVE-2017-5243 dengan skor CVSS 10.0

3.4 Analisa Estimasi Resiko

Dari data yang ada dapat dibuat sebuah tabel perhitungan resiko dari setiap *velnerability* yang terdapat pada OS Typhoon, Adapun formula yang digunakan adalah sebagai berikut :

- *Vulnerability* = Skor CVSS
- *Threat* = Frekuensi dari setiap walkthrough
- Skor maksimal = 60 (100%) (Chunlin Liu, Chong-Kuan Tan, Yea-Saen Fang, Tat-Seng Lok, 2012)
- *Asset* = Total Resource

Maka akan didapat perhitungan sebagai berikut :

Resiko = *vulnerability x threat* / skor maksimal x 100 x *asset*

No	Daftar Kerentanan	*Vulnerability*	*Threat*	Skor
1	CUPS < 2.0.3 Multiple Vulnerabilities	10.0	3	30 (50%)
2	PostgreSQL weak password	9.0	0	0
3	*Redis Server No Password*	7.5	0	0
4	*Apache Tomcat servlet/JSP container default files*	6.8	1	6.8 (11,3%)
5	*Anonymous FTP Login Reporting*	6.4	2	12.8 (11,3%)
6	SSL/TLS: Report Weak Cipher Suites	5.0	1	5 (8.33%)
7	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0	0	0
8	Check if Mailserver answer to VRFY and EXPN requests	5.0	0	0
9	WebCalendar User Account Enumeration Disclosure Issue	5.0	1	5 (8.33%)

10	Cleartext Transmission of Sensitive Information via HTTP	4.8	4	19.2 (32%)
11	FTP Unencrypted Cleartext Login	4.8	0	0
12	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3	0	0
13	SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	4.3	0	0
14	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	4.3	6	25.8 (43%)
15	SSH Weak Encryption Algorithms Supported	4.3	2	8.6 (14.3%)
16	jQuery < 1.9.0 XSS Vulnerability	4.3	0	0
17	ISC BIND Security Bypass Vulnerability (Remote)	4.3	0	0
18	TCP timestamps	2.6	0	0
19	SSH Weak MAC Algorithms Supported	2.6	0	0

Kemudian didapat hasil dari perhitungan tabel diatas bahwa kerentanan atau *vulnerability* dari "*CUPS < 2.0.3 Multiple Vulnerabilities"* dengan CVE-2015-1158 memiliki resiko terbesar karena memiliki hasil perhitung paling besar diantara yang lainnya yaitu sebesar 50%.

3.5 Perumusan *Security Auditing* berdasarkan NIST CSF

Function	***Function Score***	***Cat ID***	***No***	***Yes***	***N/A***	***blank***	***Score***
IDENTIFY	0,24137931	ID.AM	4	2	0	0	0.3333333
		ID.BE	4	1	0	0	0.2
		ID.GV	4	0	0	0	0
		ID.RA	1	5	0	0	0.8333333
		ID.RM	3	0	0	0	0
		ID.SC	3	0	0	2	0
PROTECT	0,12821	PR.AC	3	3	0	1	0.4285714
		PR.AT	5	0	0	0	0
		PR.DS	6	1	0	1	0.125
		PR.IP	9	1	0	2	0.0833333
		PR.MA	2	0	0	0	0
		PR.PT	3	1	0	1	0.25
DETECT	0,555555556	DE.AE	1	4	0	0	0.8
		DE.CM	3	5	0	0	0.625
		DE.DP	3	2	0	0	0.4
RESPOND	0,31255555	RS.RP	1	0	0	0	0
		RS.CO	3	1	0	1	0.25
		RS.AN	2	3	0	0	0.6
		RS.MI	2	1	0	0	0.3333333
		RS.IM	2	0	0	0	0
RECOVER	0,333333333	RC.RP	0	1	0	0	1

		RC.IM	1	1	0	0	0.5
		RC.CO	3	0	0	0	0

Dari data diatas makan dapat dilihat bahwa pada fungsi *Detect* memiliki score tertinggi yaitu sebanyak 61% dikarenakan fungsi deteksi lah yang paling efektif digunakan pada *typhoon os,* sedangkan untuk ratarata nilai dari keseluruhan data yang didapat adalah sebesar 34

3.6 Mitigasi data Attack Tree

Berdasarkan *vulnerability* yang di temukan, dikketahui ada berbagai cara dalam meng-*explore vulnerability* yang ada pada *Typhoon Os* dan setiap walkthrough juga memiliki cara penanganan yang berbeda. Berikut data analisis exploitasi *vulnerability* pada *Typhoon Os:*

No	*Type Control*	Jumlah banyak	Total
1	Mitigasi	11	57.8%
2	Perbaikan developer	5	26.3%
3	Workaround	3	15.7

Dari daftar solusi diatas, dapat diketahui bahwa tipe solusi mitigasi yang paling banyak (11 dari 19 solusi = 57.8%). Solusi tipe mitigasi muncul paling banyak karena memang Typhoon OS didesain banyak *vulnerability* untuk tujuan pendidikan dan penelitian.

4. Kesimpulan

1. Kerentanan atau *vulnerability* dari "*CUPS < 2.0.3 Multiple Vulnerabilities"* dengan CVE-2015-1158 memiliki resiko terbesar karena memiliki hasil perhitung paling besar diantara yang lainnya yaitu sebesar 50%.

2. Fungsi Framework NIST yang menjadi dasar pengerjaan penelitian ini, yaitu :
   - *Identify* : Mengidentifikasi OS Typhoon serta kelemahan
   - *Protect* : Memberikan informasi tentang apa saja yang telahdilakukan sebelumnya untuk merawat Typhoon OS
   - *Detect* : Melakukan *scanning vulnerability* pada Typhoon OS
   - *Respond* : Bagaimana Respon Typhoon OS terhadap serangan yangtelah dilakukan.
   - *Recover* : Melakukan mitigasi dan memberikan solusi setiap *vulnerability* di Typhoon OS

Pada fungsi *Detect* merupakan fungsi dengan skor yang palingbesar, yaitu 61%, yang menandakan bahwa fungsi deteksi yang telah terlaksana dengan baik. Untuk rata-rata keseluruhan dari hasil *securityauditing* terhadap Typhoon OS menggunakan NIST CSF yaitu 34%.

REFERENSI

Chadel, R. (2018, December 01). *Typhoon: 1.02 Vulnhub Walkthrough*. Retrieved september 05, 2020, from hackingartickel: https://www.hackingarticles.in/typhoon-1-02-vulnhub-walkthrough/

Elanda, A., & Tjahjadi, D. (2018, mei). Analisis Manajemen Resiko Sistem Keamanan Ids (Intrusion Detection System) Dengan Framework NIST. *Jurnal Ilmu-ilmu Informatika dan Manajemen STMIK, 12*(1), 1-13

Vatresia, A. (2017, Juni 21). Resort Based Management Web GIS Towards Cyber Conservation in Indonesia. *Journal of Environment and Sustainability, 1*(1), 11-12.

Sowmyashree A, D. H., SH, & Guruprasad. (May 2008). Evaluation and Analysis of Vulnerability Scanners: Nessus and. *Evaluation and Analysis of Vulnerability Scanners: Nessus*