SECURITY AUDITING PADA VULNERABLE MACHINE MENGGUNAKAN OPEN SOURCE IDS DAN VULNERABILITY SCANNER BERDASARKAN NIST CYBERSECURITY FRAMEWORK

SECURITY AUDITING IN VULNERABLE MACHINE USING OPEN SOURCE IDS AND VULNERABILITY SCANNER BASED ON NIST CYBERSECURITY FRAMEWORK

Heri Sultan Fransiscus Sitinjak[1], Umar Yunan Kurnia Septo Hediyanto[2], Adityas Widjajarto[3]

Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom

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

Abstrak :

Penelitian ini bertujuan untuk 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 untuk penelitian ini. Aplikasi yang dipakai dalam menunjang proses auditing penelitian ini yaitu OpenVAS dan suricata. OpenVAS dipakai karena memiliki database kerentanan yang cukup lengkap serta hasil scan mudah untuk dibaca. Suricata dipakai karena memiliki tabel rules yang cukup lengkap dibanding IDS lain serta ukurannya aplikasi lebih kecil dibanding aplikasi IDS lain. 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. Setelah memodelkan serangan, dilakukan eksperimen penyerangan menggunakan literatur/walkthrough. Dari eksperimen akan dicari relasi antara vulnerability dan threat. Kemudian, 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. Hasil dari analisa profil resiko menunjukkan bahwa vulnerability "GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerabilities" memiliki resiko terbesar atas serangan siber sebesar 85,71%, serta menunjukkan bahwa Typhoon OS 25,40% lebih beresiko dibanding dengan OS lain. Dari hasil profil resiko juga menunjukkan bahwa vulnerable machine memiliki resiko yang tinggi atas serangan siber.

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

Abstract :

This research is to determine the risk profile of a vulnerable machine. The vulnerable machine used in this study is Typhoon OS through a security audit process. Security audits are needed to find out the importance of the OS required by the attack and compile a solution for the OS. The framework used in this study is the NIST cybersecurity framework, because the NIST cybersecurity framework is a defensive framework and is suitable for this research. Applications used to support the research audit process are OpenVAS and Suricata. OpenVAS is used because it has a complete database with easy-to-read scans. Suricata was purchased because it has fairly complete table rules for other IDS and the application size is smaller than other IDS applications. To do the analysis in the OS. By doing a repair analysis, we can find out what attack models can be used to carry out attacks. After modeling the attack, an assault attempt was carried out using literature / walkthrough. From the experiment we will look for the relationship between vulnerability and threat. Then, from the relationship between vulnerability and threats, a risk profile will be obtained. From the results of the risk profile, it can be seen the great danger from every consideration in the OS. The vulnerability of the "GNU Bash Environment Handling Variable Shell Remote Command Exulability Vulnerabilities" had the greatest risk of cyber attacks of 85.71%, and also showed Typhoon OS 25.40% more risky than with other OS. From the results of the risk profile also shows that vulnerable machines have a high risk of cyber attacks.

Keywords: ***security auditing, vulnerable machines, framework, risk profile, attack model***

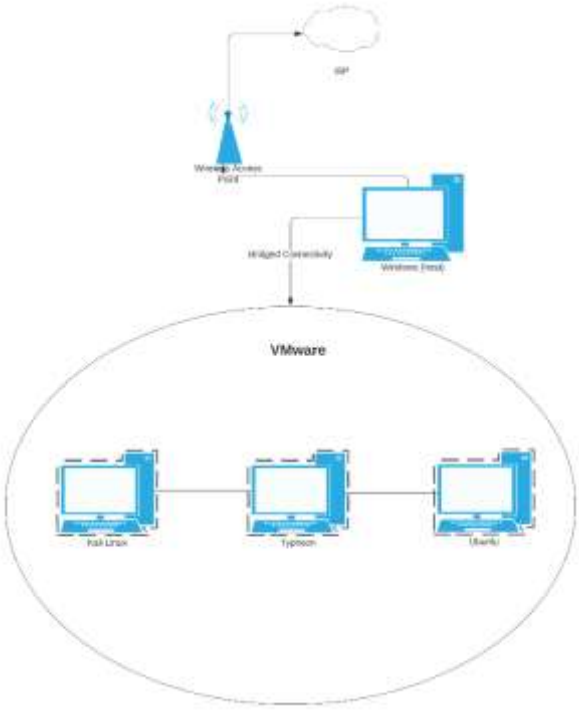
1. Pendahuluan

Aktivitas security auditing kerentanan sistem operasi sangat penting untuk mencegah serta mengurangi dampak kerusakan karena akibat adanya serangan dari pihak yang tidak bertanggung jawab. 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 untuk penelitian ini Hal ini menjadi dasar untuk meningkatkan kesadaran dan melakukan langkah awal untuk mendeteksi, mengidentifikasi dan mempelajari kelemahan yang dimiliki dari suatu sistem operasi. Berdasarkan kasus tersebut maka sangat penting untuk menerapkan uji kerentanan yang dilakukan dengan menggunakan vulnerability scanner seperti openvas, serta menggunakan aplikasi IDS (Intrusion Detection System) untuk membantu mendeteksi ujicoba serangan yang dilakukan terhadap OS serta mengelompokkan jenis-jenis serangan yang dilakukan. Openvas merupakan alat bantu uji kerentanan dengan sumber kode terbuka yang mampu menjadi salah satu solusi untuk memberikan gambaran dari sebuah penelusuran celah keamanan[1]. Intrusion Detection System (IDS) adalah tool, metode atau sumber daya yang memberikan bantuan untuk melakukan identifikasi, memberikan laporan terhadap aktivitas jaringan computer[2]. 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. Menggunakan vulnerability scanner memungkinkan untuk pendeteksian dini dan sekaligus dapat dilakukan penanganan yang sudah diketahui kerentanannya serta mudah untuk mengidentifikasi kerentanan yang ada pada jaringan. Kerentanan tersebut memungkinkan timbulnya resiko yang berpotensi dieksploitasi. Karena itu, diperlukan suatu upaya untuk mengauditing sistem operasi. Salah satu upaya tersebut adalah security auditing, terhadap vulnerable machine.

2. Perancangan Eksperimen dan Implementasi

2.1 Perancangan Topologi

Penelitian ini memakai topologi star dimana satu os yang menjadi host untuk ketiga Virtual OS nya. Untuk topologinya bisa digambarkan sebagai berikut :



2.2 Skenario Pengujian

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 :

- Walkthrough 1 – MongoDB dari https://www.hackingarticles.in/typhoon-1-02-vulnhub-walkthrough
- Walkthrough 2 – LotusCMS dari https://medium.com/@tusharroutray/typhoon-1-02-a-vulnhub-vm-walkthrough-8ebd86cc3f74
- Walkthrough 3 – Netcat dari https://hackso.me/typhoon-1.02-walkthrough
- Walkthrough 4 – Bruteforce dari https://hackso.me/typhoon-1.02-walkthrough
- Walkthrough 5 – Drupal dari https://resources.infosecinstitute.com/typhoon-ctf-walkthrough/#gref
- Walkthrough 6 – Tomcat dari https://www.hackingarticles.in/typhoon-1-02-vulnhub-walkthrough
- Walkthrough 7 – WebCalendar dari https://www.sevenlayers.com/index.php/126-vulnhub-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 Eksperimen Hasil OpenVAS

No	*Vulnerability*	CVE *Number*	CVSS *Score*
1.	*GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerabilities*	CVE-2014-6271	10.0
2.	*CUPS < 2.0.3 Multiple Vulnerabilities*	CVE-2015-1158	10.0
3.	*WebCalendar Local File Include and PHP code Injection Vulnerabilities*	CVE-2012-1495	7.5
4.	*Drupal Core Critical Remote Code Execution Vulnerability*	CVE-2018-7600	7.5
5.	*FTP Brute Force Logins Reporting*	CVE-2005-0798	7.5
6.	*Apache Tomcat servlet/JSP container default files*	CVE-2017-12617	6.8
7.	*Anonymous FTP Login Reporting*	CVE-2017-1000254	6.4
8.	*LotusCMS PHP Code Execution Vulnerabilities*	CVE-2011-0518	5.1
9.	*SSL/TLS: Report Vulnerable Cipher Suites for HTTPS*	CVE-2016-2183	5.0
10.	*WebCalendar User Account Enumeration Disclosure Issue*	CVE-2006-2247	5.0
11.	*Cleartext Transmission of Sensitive Information via HTTP*	CVE-2019-6845	4.8
12.	*SSH Weak Encryption Algorithms Supported*	CVE-2017-5243	4.3
13.	*SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability*	CVE-2014-3566	4.3
14.	*jQuery < 1.9.0 XSS Vulnerability*	CVE-2012-6708	4.3
15.	*SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection*	CVE-2016-0800	4.3
16.	*SSL/TLS: Report Weak Cipher Suites*	CVE-2013-2566	4.3

2.3.2 Data Hasil Serangan 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 Suricata (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 (-)

2.3.3 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
Dan untuk penjelasan dari setiap vulnerability adalah sebagai berikut :

1. GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerabilities (80/tcp) : Host diinstal dengan GNU Bash Shell dan rentan terhadap kerentanan eksekusi perintah jarak jauh.
2. CUPS < 2.0.3 Multiple Vulnerabilities (631/tcp) : Berbagai versi CUPS rentan terhadap peningkatan hak istimewa karena kesalahan manajemen memori.
3. WebCalendar Local File Include and PHP code Injection Vulnerabilities (80/tcp) : WebCalendar rentan terhadap beberapa kerentanan validasi input karena gagal untuk membersihkan dengan benar input yang disediakan pengguna.

4. Drupal Core Critical Remote Code Execution Vulnerability (80/tcp) : Host menjalankan Drupal dan rentan terhadap kerentanan eksekusi kode jauh kritis.
5. FTP Brute Force Logins Reporting (21/tcp) : Dimungkinkan untuk masuk ke server FTP jarak jauh menggunakan kredensial yang lemah / diketahui.
6. Apache Tomcat servlet/JSP container default files (8080/tcp) : Wadah Apache Tomcat servlet / JSP telah menginstal file default.
7. Anonymous FTP Login Reporting (21/tcp) : Laporan jika Server FTP jarak jauh memungkinkan login anonim.
8. LotusCMS PHP Code Execution Vulnerabilities (80/tcp) : Host menjalankan LotusCMS dan rentan terhadap kerentanan eksekusi kode php.
9. SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (631/tcp) : Kerentanan ini melaporkan semua suite sandi SSL / TLS yang diterima oleh layanan di mana vektor serangan hanya ada pada layanan HTTPS.
10. WebCalendar User Account Enumeration Disclosure Issue (80/tcp) : Masalah Pengungkapan Enumerasi Akun Pengguna WebCalendar.
11. Cleartext Transmission of Sensitive Information via HTTP (8080/tcp) : Tuan rumah / aplikasi mengirimkan informasi sensitif (nama pengguna, kata sandi) dalam teks lengkap melalui HTTP.
12. SSH Weak Encryption Algorithms Supported (22/tcp) : Host/aplikasi mengirimkan informasi sensitif (nama pengguna, kata sandi) dalam teks lengkap melalui HTTP.
13. SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (631/tcp) : Host rentan terhadap kerentanan pengungkapan informasi.
14. jQuery < 1.9.0 XSS Vulnerability (80/tcp) : jQuery sebelum 1.9.0 rentan terhadap serangan Cross-site Scripting (XSS). Fungsi jQuery (strInput) tidak membedakan pemilih dari HTML dengan cara yang dapat diandalkan.
15. SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (5432/tcp) : Memungkinkan untuk mendeteksi penggunaan protokol SSLv2 dan / atau SSLv3 yang sudah usang pada sistem ini.
16. SSL/TLS: Report Weak Cipher Suites (5432/tcp) : Kerentanan ini melaporkan semua suite cipher SSL / TLS yang lemah yang diterima oleh suatu layanan.

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 / 7

- a = Berapa kali tools dipakai dalam satu walkthrough (satu walkthrough maks 1 kali)
- 7 = Jumlah keseluruhan dari walkthrough

Setelah didapatkan rumus frekuensi tools, maka dapat dibuat tabel frekuensi tools sebagai berikut :

No	Nama *Tools*	a	Hasil
1.	Nmap	7	1 (100%)
2.	Msf	3	0.42 (42,85%)
3.	Searchsploit	2	0.28 (28,57%)
4.	Nikto	2	0.28 (28,57%)
5.	Hydra	2	0.28 (28,57%)
6.	Netcat	1	0.14 (14,28%)
7.	Dirb	1	0.14 (14,28%)
8.	Msfvenom	1	0.14 (14,28%)
9.	Gobuster	1	0.14 (14,28%)
10	Phpinject	1	0.14 (14,28%)
11	Hashcat	1	0.14 (14,28%)

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 Suricata IDS dirancang agar bisa mendeteksi scan dari Nmap. Dilihat dari tabel hasil pencobaan walkthrough diatas bahwa Suricata IDS dapat mendeteksi serangan Nmap sehingga Suricata IDS dapat dianggap sebagai IDS yang bagus.

3.3 Analisa Estimasi Resiko

Dari daftar tabel vulnerability dan attack tree, dapat dibuat tabel perhitungan resiko dari setiap vulnerability yang ada di OS typhoon. Perhitungan resiko dapat dibuat dengan formula :

Resiko = vulnerability x threat

- Vulnerability = Skor CVSS
- Threat = Frekuensi (setiap walkthrough maks 1 CVE)

- Skor maksimal = 70 (100%)

Setelah mendapatkan rumus perhitungan resikonya, dapat dibuat tabel sebagai berikut :

No	Daftar Kerentanan	*Vulnerability*	*Threat*	Skor
1.	*GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerabilities*	10.0	6	60 (85,71%)
2.	*CUPS < 2.0.3 Multiple Vulnerabilities*	10.0	2	20 (28,57%)
3.	*WebCalendar Local File Include and PHP code Injection Vulnerabilities*	7.5	1	7.5 (10,71%)
4.	*Drupal Core Critical Remote Code Execution Vulnerability*	7.5	1	7.5 (10,71%)
5.	*FTP Brute Force Logins Reporting*	7.5	0	0
6.	*Apache Tomcat servlet/JSP container default files*	6.8	1	6.8 (9,71%)
7.	*Anonymous FTP Login Reporting*	6.4	2	12,8 (18,28%)
8.	*LotusCMS PHP Code Execution Vulnerabilities*	5.1	2	10.2 (14,57%)
9.	*SSL/TLS: Report Vulnerable Cipher Suites for HTTPS*	5.0	0	0
10.	*WebCalendar User Account Enumeration Disclosure Issue*	5.0	0	0
11.	*Cleartext Transmission of Sensitive Information via HTTP*	4.8	4	19.2 (27,42%)
12.	*SSH Weak Encryption Algorithms Supported*	4.3	3	12.9 (18,42%)
13.	*SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability*	4.3	7	30.1 (43%)
14.	*jQuery < 1.9.0 XSS Vulnerability*	4.3	0	0
15.	*SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection*	4.3	0	0
16.	*SSL/TLS: Report Weak Cipher Suites*	4.3	2	8.6 (12,28%)

Dapat dilihat dari tabel diatas bahwa kerentanan/vulnerability “GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerabilities “ dengan CVE-2014-6271 yang memiliki resiko terbesar karena memiliki hasil yang besar yaitu 85,71%. Dan untuk perhitungan resiko keberhasilan serangan terhadap Typhoon OS yaitu :

Resiko Keberhasilan Serangan ke Typhoon : (Total skor)/(Jumlah maksimal skor) / x 100

- Total Skor = 195,6
- Jumlah Maksimal Skor = 1120

Setelah dilakukan perhitungan, maka resiko keberhasilan serangan terhadap Typhoon OS sebesar 17,46% lebih besar dibanding default OS (dengan asumsi keamanan default OS 100%).

3.4 Perumusan Attack Tree

Jika dihubungkan dengan implementasi serangan yang sudah dilakukan sebelumnya, dapat dibuat attack tree dari setiap walkthroughnya. Attack tree merupakan sebuah grafik yang mewakili serangan menggunakan struktur pohon, di mana simpul akar adalah tujuan penyerang (atau subgoal) dan simpul daun adalah bentuk yang mewakili semua cara yang memungkinkan penyerang dapat mencapai tujuan. Berikut perumusan attack tree dari setiap walkthrough : (gambar terlampir)

- Walkthrough 1

Walkthrough pertama yang terdiri dari 12 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

3.5. Perumusan Security Auditing berdasarkan NIST CSF

Function	*Function Score*	*Cat ID*	*No*	*Yes*	*N/A*	*blank*	*Score*
IDENTIFY	0,24137931	ID.AM	5	1	0	0	0,166666667
		ID.BE	4	1	0	0	0,2
		ID.GV	4	0	0	0	0
		ID.RA	1	5	0	0	0,833333333
		ID.RM	3	0	0	0	0
		ID.SC	5	0	0	0	0
PROTECT	0,12821	PR.AC	4	3	0	0	0,428571429
		PR.AT	5	0	0	0	0
		PR.DS	8	0	0	0	0
		PR.IP	11	1	0	0	0,083333333
		PR.MA	2	0	0	0	0
		PR.PT	4	1	0	0	0,2
DETECT	0,555555556	DE.AE	1	4	0	0	0,8
		DE.CM	3	5	0	0	0,625
		DE.DP	4	1	0	0	0,2
RESPOND	0,3125	RS.RP	1	0	0	0	0
		RS.CO	4	1	0	0	0,2
		RS.AN	2	3	0	0	0,6
		RS.MI	2	1	0	0	0,333333333
		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

Dapat dilihat fungsi Detect merupakan fungsi dengan skor yang paling besar, yaitu 56%, yang menandakan bahwa Fungsi deteksi yang telah terlaksana dengan baik. Untuk rata-rata keseluruhan dari hasil security auditing terhadap Typhoon OS menggunakan NIST CSF yaitu 31%.

3.6 Mitigasi dari Kompilasi Attack Tree

Setelah membuat attack tree, didapatkan bahwa setiap walkthrough memiliki cara yang berbeda-beda dalam meng-explore vulnerability yang ada di Typhoon OS. Maka dari itu, diperlukan solusi untuk membantu mencegah terjadinya serangan serta memberitahu kerentanan mana yang harus diutamakan untuk diperbaiki. Berikut solusi untuk setiap vulnerability yang ada di Typhoon OS :

1. Vulnerability : GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerabilities
   Solusi : Tambah patch terbaru yang dibutuhkan atau upgrade ke versi yang terbaru (versi sekarang GNU Bash 4.3)
   Tipe Solusi : Perbaikan Developer
2. Vulnerability : CUPS < 2.0.3 Multiple Vulnerabilities
   Solusi : Dikarenakan versi CUPS di typhoon masih dibawah versi 2.0.3, maka harus diupdate ke versi terbaru. Patch yang mengatasi masalah ini telah dirilis untuk semua versi CUPS yang didukung.
   Tipe Solusi : Perbaikan Developer
3. Vulnerability : WebCalendar Local File Include and PHP code Injection Vulnerabilities
   Solusi : Pembaruan ke versi terbaru
   Tipe Solusi : Perbaikan Developer
4. Vulnerability : Drupal Core Critical Remote Code Execution Vulnerability
   Solusi : Tingkatkan ke Drupal core versi 8.3.9, 8.4.6, 8.5.1, 7.58 atau lebih baru. (Drupal typhoon versi 8.0)
   Tipe Solusi : Perbaikan Developer
5. Vulnerability : FTP Brute Force Logins Reporting
   Solusi : Ganti kata sandi sesegera mungkin
   Tipe Solusi : Mitigasi
6. Vulnerability : Apache Tomcat servlet/JSP container default files
   Solusi : Hapus file default, contoh JSP dan Servlet dari wadah Tomcat Servlet / JSP
   Tipe Solusi : Mitigasi
7. Vulnerability : Anonymous FTP Login Reporting
   Solusi : Jika tidak ingin berbagi file, maka nonaktifkan fitur login anonim

Tipe Solusi : Mitigasi

8. Vulnerability : LotusCMS PHP Code Execution Vulnerabilities
   Solusi : Tidak ada solusi yang diketahui tersedia untuk setidaknya satu tahun sejak pengungkapan kerentanan ini. Kemungkinan tidak akan disediakan lagi. Pilihan solusi umum adalah meningkatkan ke rilis yang lebih baru, menonaktifkan fitur masing-masing, menghapus produk atau mengganti produk dengan yang lain
   Tipe Solusi : Tidak bisa Diperbaiki
9. Vulnerability : SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
   Solusi : Konfigurasi layanan ini harus diubah sehingga tidak lagi menerima cipher suites yang telah didaftarkan.
   Tipe Solusi : Mitigasi
10. Vulnerability : WebCalendar User Account Enumeration Disclosure Issue
    Solusi : Tingkatkan ke WebCalendar 1.0.4 atau yang lebih baru.
    Tipe Solusi : Perbaikan Developer
11. Vulnerability : Cleartext Transmission of Sensitive Information via HTTP
    Solusi : Melakukan transmisi data sensitif melalui koneksi SSL / TLS terenkripsi. Selain itu pastikan host / aplikasi mengarahkan ulang semua pengguna ke koneksi SSL / TLS yang diamankan sebelum mengizinkan untuk memasukkan data sensitif ke dalam fungsi yang disebutkan.
    Tipe Solusi : Mitigasi
12. Vulnerability : SSH Weak Encryption Algorithms Supported
    Solusi : Nonaktifkan algoritma enkripsi yang lemah.
    Tipe Solusi : Mitigasi
13. Vulnerability : SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability
    Solusi : Matikan SSLV3 dan nonaktifkan cipher suites yang mendukung mode CBC
    Tipe Solusi : Mitigasi
14. Vulnerability : jQuery < 1.9.0 XSS Vulnerability
    Solusi : Perbarui ke versi 1.9.0 atau lebih tinggi.
    Tipe Solusi : Perbaikan Developer
15. Vulnerability : SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
    Solusi : Dianjurkan untuk menonaktifkan protokol SSLv2 dan / atau SSLv3 yang sudah ketinggalan zaman demi protokol TLSv1 +.
    Tipe Solusi : Mitigasi
16. Vulnerability : SSL/TLS: Report Weak Cipher Suites
    Solusi : Konfigurasi layanan ini harus diubah sehingga tidak lagi menerima suite sandi lemah yang terdaftar.
    Tipe Solusi : Mitigasi

Dari daftar solusi diatas, dapat diketahui bahwa tipe solusi mitigasi yang paling banyak (9 dari 16 solusi = 56,25%). Solusi tipe mitigasi muncul paling banyak karena memang Typhoon OS didesain banyak vulnerability untuk tujuan pendidikan dan penelitian.

4. Kesimpulan

Dari hasil penelitian diatas, dapat diambil kesimpulan sebagai berikut :

1. Resiko kerberhasilan serangan ke Typhoon OS yaitu sebesar 17,46% lebih besar dibanding dengan default OS dan Kerentanan/vulnerability “GNU Bash Environment Variable Handling Shell Remote Command Execution Vulnerabilities “ dengan CVE-2014-6271 yang memiliki resiko terbesar karena memiliki hasil yang besar yaitu 85,71%. Dengan begitu, kerentanan ini merupakan prioritas utama yang harus segera diperbaiki agar tidak terjadi serangan siber.
2. Dan hasil security auditing NIST CSF terhadap Typhoon OS sebesar 31%.
3. 5 Fungsi Framework NIST yang menjadi dasar pengerjaan penelitian ini, yaitu :

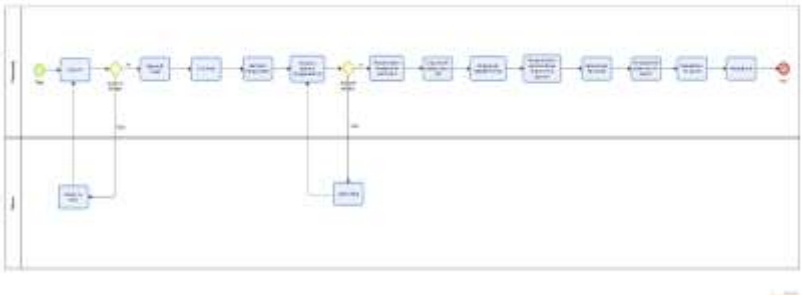
1. Identify : Mengidentifikasi OS Typhoon serta kelemahan
   - Protect : Memberikan informasi tentang apa saja yang telah dilakukan sebelumnya untuk merawat Typhoon OS
   - Detect : Melakukan scanning vulnerability pada Typhoon OS
   - Respond : Bagaimana Respon Typhoon OS terhadap serangan yang telah dilakukan.
   - Recover : Melakukan mitigasi dan memberikan solusi setiap vulnerability di Typhoon OS

Pada fungsi Detect merupakan fungsi dengan skor yang paling besar, yaitu 56%, yang menandakan bahwa fungsi deteksi yang telah terlaksana dengan baik. Untuk rata-rata keseluruhan dari hasil security auditing terhadap Typhoon OS menggunakan NIST CSF yaitu 31%.

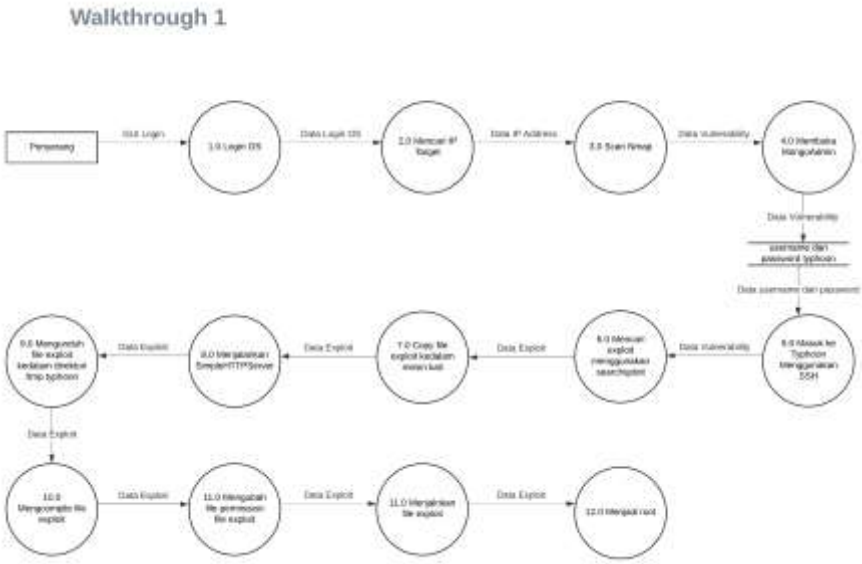
Daftar Pustaka:

[1] Richard Pangalila, Agustinus Noertjahyana, Justinus Andjarwirawan . (2015). Penetration Testing Server Sistem Informasi Manajemen dan Website Universitas Kristen Petra. Jurnal Infra 3.2, 271-276.
[2] Rozenblum, D. (2020). Understanding Intrusion Detection Systems. SANS Institute Information Security Reading Room.

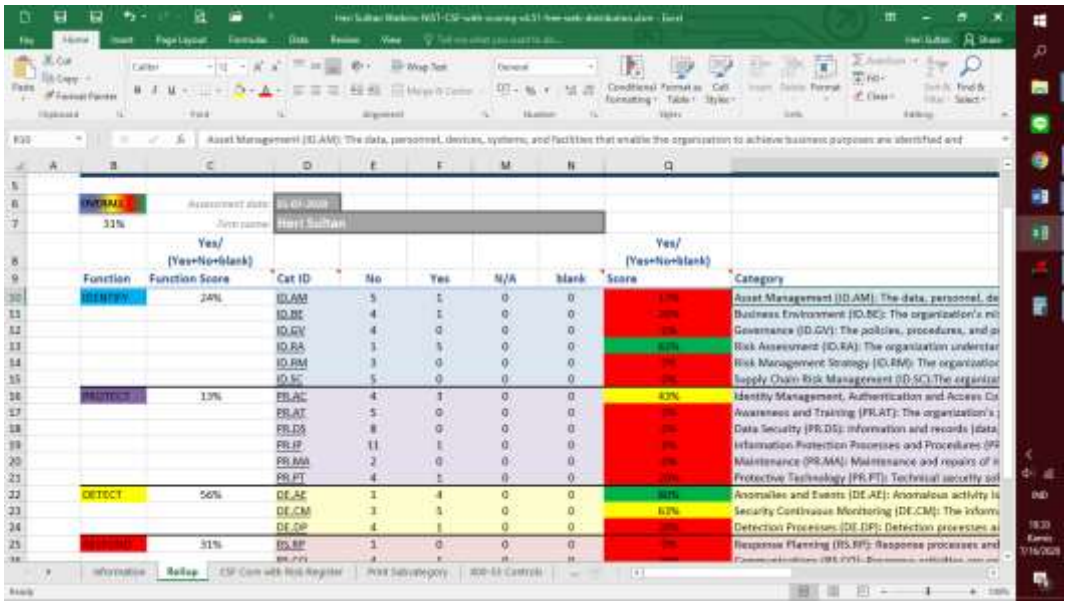
Lampiran



Lampiran 2 Activity Diagram Walkthrough 1



Lampiran 1 Data Flow Diagram Walkthrough 1



Lampiran 3 Hasil Security Auditing Menggunakan NIST CSF