PENERAPAN SIEM UNTUK PROTEKSI, DETEKSI, DAN RESPON INSIDEN SERANGAN SIBER PADA SERVER WAZUH

Vatra Kusumah Khanza Antarariq [1)]
1) Program Studi Teknik Informatika Institut Teknologi Indonesia
Jl. Raya Puspiptek - Serpong, Tangerang Selatan, 15320
E-mail: khanzaantarariq@gmail.com

Abstrak

Membuat topologi jaringan dan konfigurasinya dengan menggunakan packet tracer berdasarkan poin-poin penilaian objektif PTSA Network Security yang dilakukan secara mandiri. Final project ini berkaitan dengan materi Network Security yang bukan hanya bertujuan untuk meningkatkan pengetahuan saja, namun juga dapat meningkatkan keterampilan (upskilling) peserta pelatihan. Balitbang SDM Kementerian Kominfo merupakan bagian dari Kementerian Komunikasi dan Informatika, selaku Kementerian teknis yang menangani bidang Teknologi Informasi dan Komunikasi yang melaksanakan arahan Presiden dengan meluncurkan program pendidikan tanpa gelar bertajuk Digital Talent Scholarship (DTS). Salah satu bidang pelatihan yang ada pada program tersebut adalah Talent Scouting Academy (TSA). Misi dari final project ini untuk meningkatkan pengetahuan dan keterampilan peserta dalam bidang network security dan meningkatkan daya saing untuk kebutuhan industri. Pelatihan dilaksanakan secara daring dengan melakukan pembelajaran bersama mentor dan mengerjakan exam, final exam, skill exam dan final project sebagai bentuk dari pencapaian pembelajaran. Program pelatihan TSA dengan tema Cybersecurity Analyst merupakan program Balitbang SDM Kementerian Kominfo dengan melakukan pembelajaran secara daring bersama mentor dan mengerjakan exam, final exam, skill exam dan final project yaitu membuat topologi jaringan dan konfigurasinya berdasarkan poin-poin objektif PTSA Network Security sebagai bentuk hasil dari pembelajaran.

Kata kunci: *PTSA Network Security, Talent Scouting Academy (TSA), Cyber Security.*

Pendahuluan

Dalam era ekonomi berbasis pengetahuan (knowledge-based economy), daya saing suatu negara bergantung pada kemampuannya untuk menciptakan, memanfaatkan, dan mendistribusikan ilmu pengetahuan dibandingkan dengan faktor produksi tradisional seperti sumber daya alam. Untuk alasan tersebut Organization of Economic Development and Cooperation (OECD) memasukkan pengembangan Sumber Daya Manusia sebagai satu dari empat pilar utama pendukung ekonomi berbasis pengetahuan, di samping economic and institutional system, information and communications technology (ICT) dan national innovation system (NIS). Sehubungan dengan hal itu, maka akselerasi pengembangan sumber daya manusia yang memiliki skill digital dalam rangka proses adaptasi dengan teknologi- teknologi baru ini merupakan hal yang tidak bisa ditunda lagi.

Kementerian Komunikasi dan Informatika, selaku kementerian teknis yang menangani bidang Teknologi Informasi dan komunikasi, melalui Badan Litbang SDM menerjemahkan arahan Bapak Presiden dengan meluncurkan program pendidikan tanpa gelar bertajuk Digital Talent Scholarship (DTS). Salah satu bidang pelatihan yang ada pada program tersebut adalah Talent Scouting Academy (TSA), bidang pelatihan ini baru dilaksanakan pada tahun 2021. TSA adalah peningkatan kompetensi dan pemberian kesempatan sertifikasi global bagi mahasiswa tingkat akhir yang terseleksi. Penyelenggaraan TSA tahun ini akan dilaksanakan secara daring. Dalam hal pelaksanaannya, Kementerian Kominfo bekerja sama dengan mitra perguruan tinggi, perusahaan teknologi global dan praktisi bidang Teknologi Informasi dan Komunikasi (TIK).

Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) merupakan sistem monitoring yang mampu mendeteksi serangan dan respons sistem keamanan terhadap serangan melalui analisis log dari berbagai event-log yang bersumber dari data secara real-time. Log merupakan informasi dari perangkat yang berisi kegiatan dari log tersebut, mulai dari lalu lintas jaringan, status dari perangkat dan lainnya.

Sistem SIEM bekerja dengan mengumpulkan data dari berbagai sumber dalam infrastruktur jaringan, termasuk dari jaringan, security, server, database, dan aplikasi untuk mengidentifikasi potensi ancaman, baik yang berasal dari eksternal ataupun internal. Perangkat-perangkat pemberi input SIEM dianggap sebagai sensor yang menangkap kejadian sesuai dengan tempatnya berada. Data yang berhasil dikumpulkan akan ditampilkan pada dashboard dalam bentuk chart sehingga lebih mudah dibaca dan dimengerti, ataupun lebih mudah menemukan suatu pola khusus. SIEM menyediakan penyimpanan jangka panjang, sehingga dapat dilakukan korelasi data dalam jangka waktu yang cukup lama. Teknologi SIEM dapat melakukan teknik korelasi yang terintegrasi dengan berbagai sumber data, sehingga data dapat diproses menjadi informasi yang bermanfaat.

Wazuh merupakan platform open source yang berfungsi sebagai sistem deteksi ancaman, pemantauan keamanan dan respons insiden. Platform Wazuh merupakan implementasi dari Security Information and Event Management (SIEM). Wazuh menyediakan berbagai fitur yang dapat menganalisis data log, intruksi dan deteksi malware, pemantauan integritas file, penilaian konfigurasi dan deteksi kerentanan sistem. Wazuh memiliki 3 buah komponen yaitu :

1. Wazuh Agent, merupakah sebuah end points seperti desktop, server, instans cloud atau mesin virtual, yang dapat melakukan pencegahan, deteksi, dan respons.
2. Wazuh Server, merupakan server yang bertugas menganalisis data yang diterima oleh agent dan memprosesnya melalui decoder dan aturan.
3. Elastis Stack, digunakan untuk melakukan pencarian dan analisis.

Wazuh agent akan mengirimkan log yang didapatkan ke Wazuh server untuk dilakukan analisis dan deteksi ancaman.Sebelum itu,wazuh agent akan membuat sebuah koneksi dengan layanan server.Kemudian wazuh server akan menerjemahkan log yang diterima menggunakan analysis engine.Log yang terdeteksi sebagai ancaman akan dibuatkan suatu alert yang menyimpan rule id dan rule name. Kemudian log tersebut akan ditampung ke dalam penyimpanan wazuh. Filebeat digunakan untuk mengirimkan alert dan log ke server Elasticsearch. Setelah data diterima oleh Elasticsearch, Kibana akan memvisualisaskan informasi yang didapatkan. Interface dari wazuh berjalan pada Kibana, sebagai plugin.

Tahapan Instalasi Wazuh pada Linux Ubuntu 22.04

Berikut ini adalah tahapan instalasi Wazuh pada Linux Ubuntu 22.04:

1. Kita akan menginstall wazuh pada mesin virtual kita, dengan menggunakan mesin linux ubuntu sebagai sistem operasi untuk menjadikan server ubuntu kita.
2. Sebelumnya, kita harus install sebuah command curl pada ubuntu $ sudo apt install curl (Fungsinya agar kita bisa menggunakan command curl diterminal kita).

Gambar 1. Instal Wazuh

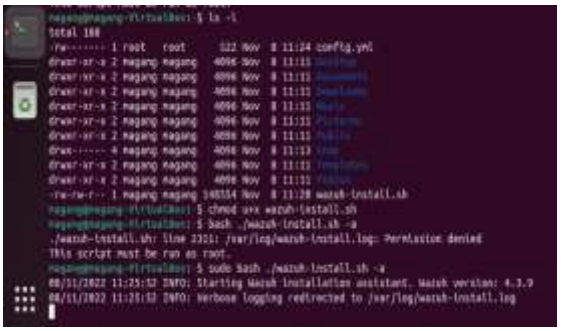
3. Kemudian masukkan perintah dibawah ini untuk download file wazuhnya. Kalian bisa melihatnya di website dokumentasi resmi wazuh (https://documentation.wazuh.com/current/installation-guide/wazuh-indexer/installation-assistant.html).

$ curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh

$ curl -sO https://packages.wazuh.com/4.3/config.yml

Ketika sudah download, coba kalian masukkan peintah di terminal,

$ ls (untuk listing isi dari directory yang aktif)



Gambar 2. File Wazuh

4. Ketika menggunakan command $ ls -l, dapat terlihat bahwa file wazuh- install.sh tidak mempunyai permission untuk execute dibagian usernya. Maka kalian kita menambahkan execute.

   $ chmod u+x wazuh-install.sh
5. Ketika $ ls -l, maka file permisson pada user untuk execute sebuah file sudah bisa dilakukan. Karena isi file dari wazuh-install.sh adalah sebuah script, script bisa dijalankan ketika terdapat permission di filenya.

Gambar 3. File permission

6. Ketika Sudah selesai download, maka akan mendapatkan user dan password. Dapat dilihat bahwa semua sudah menjadi satu paket, Wazuh Indexer, Wazuh Server, Wazuh Dashboard sudah terinstall secara otomatis didalamnya. Kemudian masuk kedalam dashboard Wazuh kalian di web browser.
   - Login dan masuk kedalam Wazuh dashboard

Masuk kedalam web browser, dan cari https://localhost/

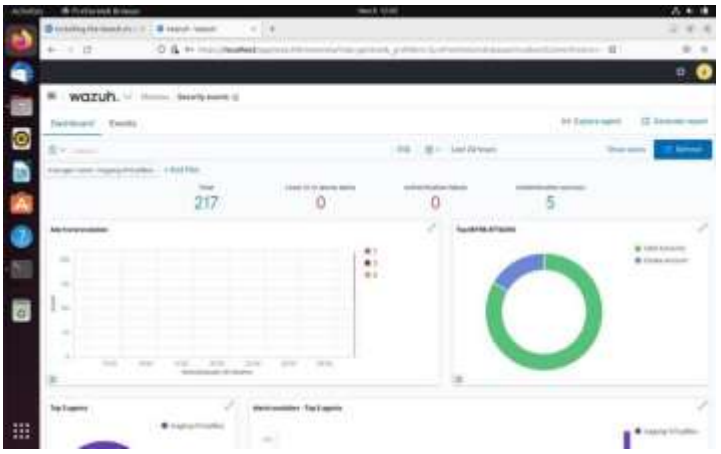
Gambar 4. Login Wazuh

- Masukkan user dan password yang sudah kalian dapat Ketika instalasi wazuh.

Gambar 5. User Wazuh

- Kemudian Wazuh akan mesinkronisasikan Wazuh server dengan server linux kalian.

Gambar 6. Wazuh server



Gambar 7. Tampilan dashboard Wazuh

7. Terlihat bahwa terdapat total 217 dengan Authetication success. Maksudnya adalah sebagai berikut: Authentication success adalah Ketika kita memasukkan sebuah perintah didalam terminal, dengan divalidasi oleh server linux bahwa user yang meng-input sebuah command adalah Valid. Sedangkan 217 total adalah sebuah log dari /var/log/dpkg.log yang berisikan sebuah log yang kita akses, karena kita tadi sedang mengunduh wazuh didalam mesin kita maka itu semua adalah log yang diakses.

Pembuktian Melakukan Beberapa Metode Serangan

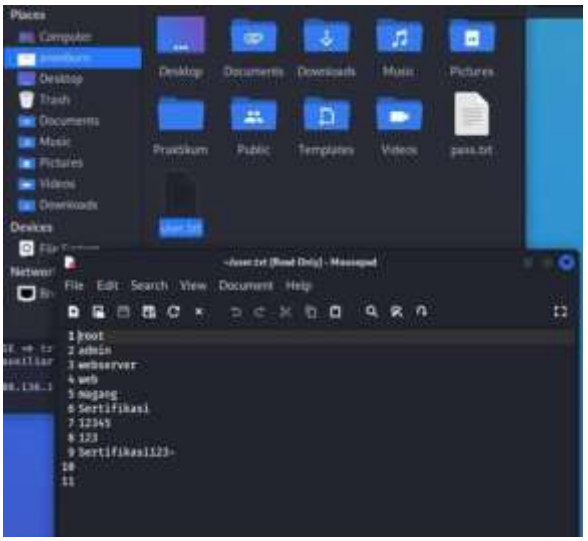
Melakukan Serangan Bruteforce dengan Metasploit

Pada kali ini kita akan masuk kedalam sebuah server ubuntu yang ter-sinkronisasi dengan wazuh. Kita akan menggunakan Teknik Brute Force untuk mengetahui username dan password pada user ubuntu target kali ini.

Metasploit Framework merupakan framework yang paling umum dipakai untuk menguji sebuah *exploit*. Metasploit juga sebuah framework open source yang membantu kita untuk kerentanan pada sebuah webserver dan pengembangan exploitasi.Ssh adalah Secure Shell sebuah protokol jaringan kriptografi untuk komunikasi data yang aman, login antarmuka baris perintah, perintah eksekusi jarak jauh, dan layanan jaringan lainnya antara dua jaringan komputer. Kemudian bruteforce Dalam kriptografi, Serangan brutal adalah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci. Penyerang secara sistematis memeriksa semua kemungkinan kata sandi dan frasa sandi sampai yang benar ditemukan. Jadi dapat di simpulkan ssh bruteforce adalah kita memaksa masuk kedalam sebuah port ssh untuk melakukan percobaan terhadap semua kunci sampai ketemu kata sandi dan username yang kita inginkan.

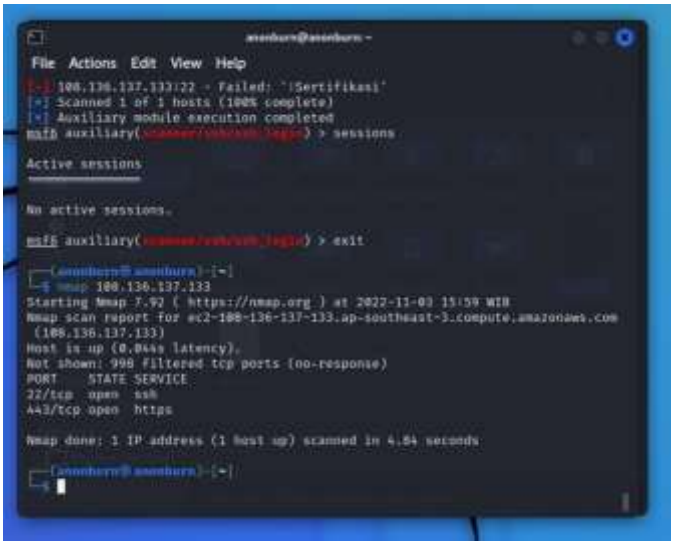
Langkah – langkahnya :

- Sebelum kita masuk kedalam serangan, siapkan sebuah dua file, password.txt dan username.txt
- Kemudian masukkan didalamnya isi username yang umumnya orang gunakan dan masukkan juga di file password.txt isi password yang umumnya orang lain gunakan. Contohnya :



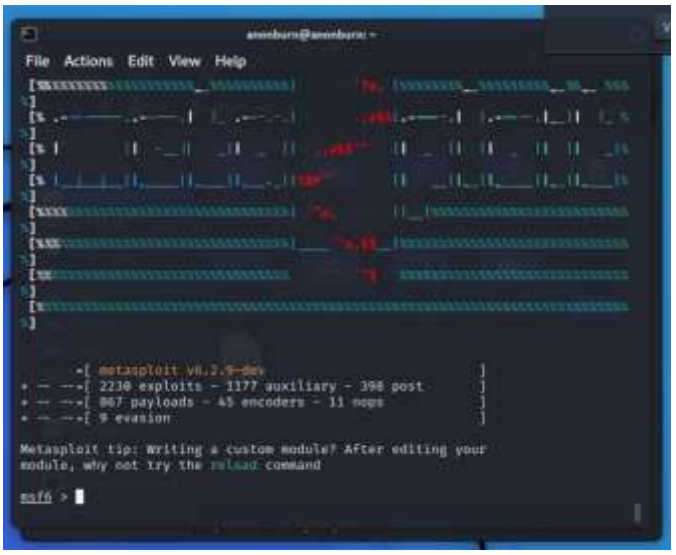
Gambar 8. File serangan

- Gunakan perintah ping untuk mengetahui IP dari https://wazuh-magang.site
- Kemudian, dapat kita ketahui bahwa IP target adalah 108.136.137.133
- Untuk melihat port mana saja yang terbuka maka kita menggunakan perintah nmap$ nmap 108.136.137.133



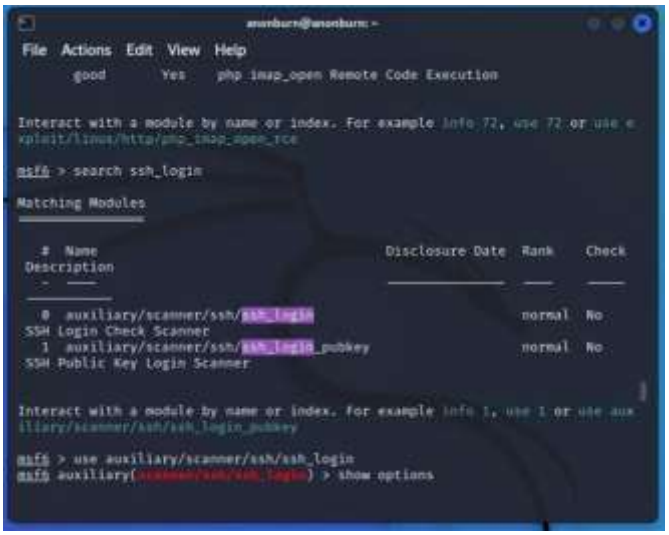
Gambar 9. Perintah Nmap

- Bisa dilihat bahwa port yang terbuka adalah port 22 untuk SSH dan port 443 untuk HTTPS.
- Disini kita akan Brute Force menggunakan SSH, maka kita memilih port 22 untuk masuk kedalamnya.
- Kemudian pada mesin Kali Linux ketikan perintah $ msfconsole untuk membuka metasploitnya.



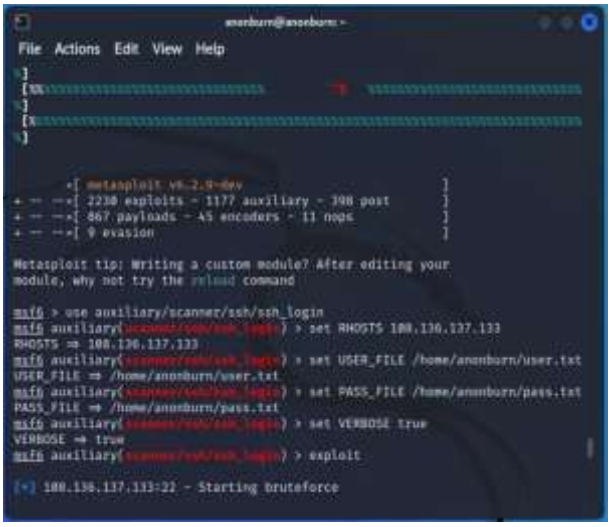
Gambar 10. Mesin kali linux

- Ini adalah tampilan dari Metasploit, kemudian masukkan perintah search ssh_login: Msf6 > search ssh_login



Gambar 11. Tampilan metasploit

- Tertampil modul yang bisa kita pakai untuk menyerang, nah disini kita akan pakai auxiliary/scanner/ssh/ssh_login



Gambar 12. Modul serang

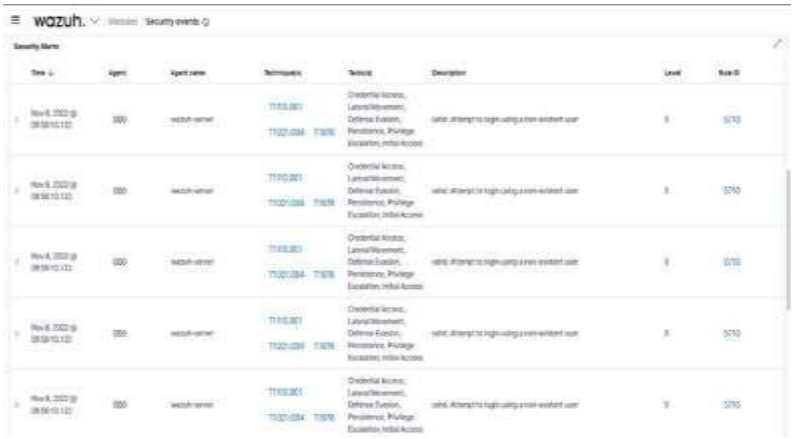
- Kemudian, masukkan IP target dengan perintah set RHOSTS.
- Masukkan file username.txt yang di buat sesuaikan alamat dimana menaruh file tersebut, gunakan perintah set USER_FILE (alamat file).
- Masukkan file password.txt yang sudah di buat dan sesuaikan alamat dimana menaruh file kalian tersebut, gunakan perintah set PASS_FILE (alamat file) Set VERBOSE true.
- Kemudian jalankan dengan perintah exploit/run.

Melihat Log pada Wazuh

- Pertama-tama kita membuka wazuh, kemudian isikan username dan password yang sudah terdaftar, username nya adalah nama mesin linux kita, dan password nya kita akan dapat Ketika kita sudah mendownload wazuh dashboard kedalam mesin linux, akan generate secara otoatis untuk medapatkan passwordnya.

Gambar 13. Login Wazuh

- Kemudian klik Modul, dan pilih Security Events.
- Didalam Modul Security Events, kita bisa melihat alerts Ketika kita mengubah sesuatu, atau ada serangan yang masuk kedalam server kita, atau juga seseorang yang mencoba untuk mengubah permission dan hal lainnya.



Gambar 14. Alerts Wazuh

- Ini adalah alert alert yang tertampil di Wazuh kita. Karena kita tadi melakukan bruteforce kedalam server dengan IP 108.136.137.133, maka bisa kita lihat dibagian description yaitu, sshd: Attempt to login using non-existent user. Maksudnya ada seseorang yang tidak terdaftar mencoba masuk kedalam server.

Gambar 15. Alerts Wazuh 2

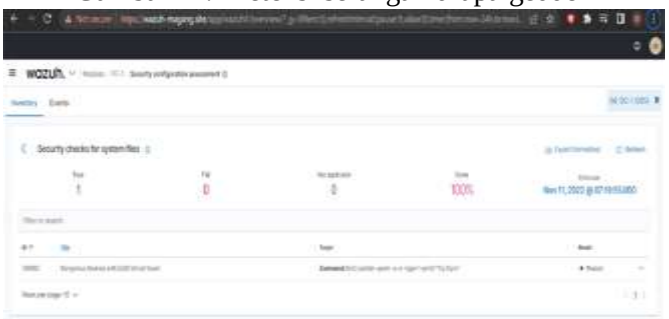
Gambar 16. Alerts Wazuh 3

- Ketika kita klik salah satu dari alert tersebut maka informasi yang didapatkan semakin rinci, kita dapat melihat location, hostname, agent_id, sourceport, kemudian tipe serangan, level dari serangan, kemudian apa yang diserang.

Deteksi Serangan Drupalgeddon Menggunakan Wazuh

Jika masuk ke pilihan Security Configuration Assessment, tampilan awal akan seperti dibawah ini. Ini menampilkan kegiatan peninjauan konfigurasi yang sudah dilakukan serta status lolos (Pass) atau gagal (Fail). Untuk contoh pada gambar dibawah ini ada 3 Peninjauan, yaitu CIS Benchmark For Debian/Linux 7, Security Check For Drupal, dan Security Checks For System Files. Serta terdapat 3 hasil yang berbeda. lolos 37% atau lolos sebagian, ada yang lolos 0% atau gagal semua, serta ada yang mencapai lolos 100% atau lolos semua.

Gambar 17. Deteksi serangan drupalgeddon



Gambar 18. Security checks for system file

Saat peninjauan system perdapat 1 command dan pass (lolos) dari pemeriksaan atau sesuai dengan kebijakan yang diatur.

Hasil Security Configuration Assessment (SCA) yang Membuktikan Adanya Dangerous Binary Permission SUID

a. Terdapat Dangerous Permission, sebagai berikut:

Gambar 19. Dangerous permissi

Ini dapat menyebabkan pengguna non-root yang membaca parameter boot mungkin dapat mengidentifikasi kelemahan keamanan boot dan dapat mengeksploitasinya.

b. Selain itu, masih ada lagi seperti dibawah ini

Gambar 20. CIS benchmark

Core dump adalah memori dari program yang dapat dieksekusi. Ini umumnya digunakan untuk menentukan mengapa suatu program dibatalkan. Itu juga dapat digunakan untuk mengumpulkan informasi rahasia dari file inti.

c. Selanjutnya, ada celah bagi penyerang seperti gambar dibawah ini

Gambar 21. CIS benchmark

Penyerang dapat menggunakan host yang disusupi untuk mengirim pengalihan ICMP yang tidak valid ke perangkat router lain dalam upaya untuk merusak router dan meminta pengguna mengakses sistem yang disiapkan oleh penyerang sebagai lawan dari sistem yang valid.

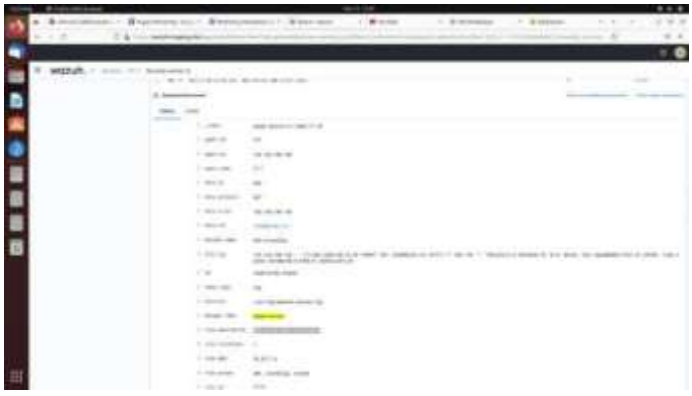
Membuktikan Serangan Port Scanning

Gambar 22. Serangan port scanning

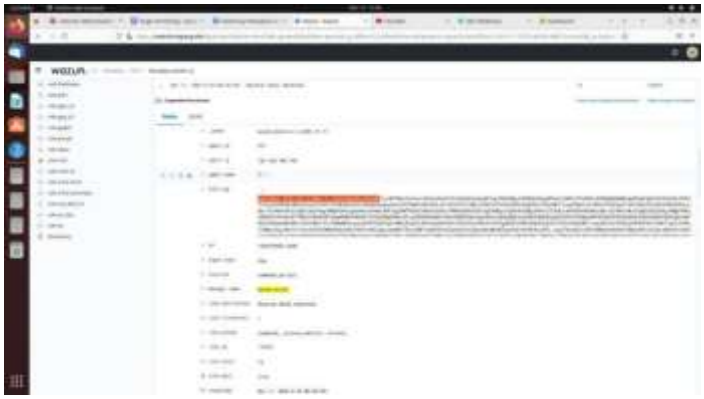
Pada full_log diatas dapat dilihat terdapat informasi “Nmap scripting Engine; https://nmap.org/book/nse.html “ dimana informasi tersebut membuktikan bahwa serangan port scanning terjadi. Nmap merupakan alat bantu yang sangat berguna dalam melakukan scanning. Terdapat banyak teknik scanning Nmap. Masing-masing teknik memiliki kelebihan dan kekurangan sendiri. Beberapa diantaranya adalah:

a. **TCP SYN Scan (-sS)** teknik ini melakukan scanning port dengan cepat. Teknik ini dapat membedakan status port Open, closed dan filtered. Cara kerjanya adalah dengan mengirimkan sebuah paket SYN, kemudian menunggu jawaban dari sistem target. Bila kita mendapat jawaban paket SYN/ACK berarti port tersebut open, bila kita mendapat paket RST berarti port closed. Bila kita tidak mendapat jawaban seteah beberapa saat, maka port ditandai filtered.
b. **TCP connect() Scan (-sT)** teknik ini digunakan bila kita tidak memiliki privilege (admin/root). Scanning ini menggunakan fungsi system call connect pada OS. Metode ini membutuhkan waktu lebih lama dan umumnya dapat terbaca oleh IDS.
c. **UDP Scan –sU** teknik ini digunakan untuk mengidentifikasi port UDP. Layanan DNS, SNMP dan DHCP adalah beberapa layanan yang menggunakan paket UDP.
d. **FIN Scan (-sF), Xmas Tree Scan (-sX) dan Null Scan (-sN)** teknik ini digunakan pada jaringan yang dilindungi Firewall. Teknik ini tidak dapat digunakan pada komputer dengan OS Windows. Selain itu hasil scan akan sulit membedakan status open dan filtered.
e. **Ping Scan (-sP)** teknik ini merupakan teknik scanning yang paling cepat. Teknik ini tidak melakukan port scanning, umumya digunakan untuk menemukan host yang hidup pada suatu jaringan.
f. **Scan IP Protocol (-sO)** teknik ini dapat menemukan protokol IP pada komputer target, misalnya ICMP, TCP, dan UDP
g. **Scan ACK (-sA)** teknik ini tidak dapat digunakan untuk menemukan port yang terbuka, tapi berguna pada jaringan yang dilindungi firewall maupun packet filter. Hasil scanning bisa digunakan untuk menentukan tipe firewal yang digunakan apakah statefull atau tidak serta port mana yang difilter.

Membuktikan serangan menggunakan meterpreter



Gambar 23. Serangan menggunakan meterpreter



Gambar 24. Serangan menggunakan meterpreter 1

Meterpreter adalah sebuah shellcode yang di gunakan oleh hacker untuk membuat shell atau trojan untuk menyusup kedalam sistem , metodenyapun sangat banyak dan kreatif, banyak yang menggunakan meterpreter untuk mengambil akses seperti Administrator di windows dan Root dalam linux. Fungsi meterpreter adalah membuat code yang membuka port port berbahaya untuk meremote, upload dan juga download dari dalam sistem maupun luar sistem, disini meterpreter di gunakan untuk menerobos ke sistem tertinggi , bisa berupa trojan ataupun adons yang menyerang web browser.

Pada “rule_description” diatas terdapat informasi **web server 400 error code.** Juga terdapat informasi pada ”full_log” seperti **eval(base64_decode.** kita dapat menganggap bahwa proses yang mencoba mengevaluasi beberapa **base64 code** adalah situasi yang tidak biasa dan kita harus mewaspadainya. Jadi, kita akan menjalankan perintah yang mencantumkan proses di agen. Kemudian, kita akan membuat peringatan jika ada proses dengan string **eval(base64_decode.** Selain itu, Metasploit menghasilkan log di server Apache selama eksploitasi dan Wazuh rule engine akan mencocokkan log dengan kode **Web server 400 error code (ID: 31101)** yang menunjukkan kemungkinan serangan.

Membuktikan Pembuatan Akun Root Baru pada Linux

Dapat dilihat dari full_log pada Wazuh, bahwa Attacker berhasil menambahkan akun baru bernama “totalysafe”. Kami menganalisis bahwa tujuannya hacker menambahkan akun baru untuk melakukan sebuah backdoor. Hacker sudah berhasil mengambil alih seluruh server tersebut yang di buktikan dengan akun root baru dan login SSH.

Gambar 25. Akun root Baru

Dari gambar diatas hacker menambahkan user baru, sebelum menambahkan user baru hacker

telah mengambil alih shell dari mesin server pada tanggal 11 November 2022 dan jam 07:05:00, yang dimana level dari serangan nya berada ditingkatan 13.

Gambar 26. Security events

Kemudian pada log alert tersebut, diketahui bahwa DC-1 sshd[6693]: Accepted password for totallysafe from 192.168.100.148 port 46380 ssh2. Description : sshd : authentication success. Artinya, hacker sudah berhasil masuk kedalam mesin Linux dan bisa mengakses sebagai root.

Kesimpulan

Dari pemaparan diatas dapat disimpulkan bahwa Cybersecurity merupakan hal penting untuk melindungi perangkat, jaringan, program, dan data dari ancaman siber dan akses ilegal. Ancaman ini biasanya dilakukan oleh oknum yang tidak bertanggungjawab untuk berbagai macam kepentingan yang merugikan korban. Terlebih lagi *cybercrime* bukan hanya menjadi anacaman bagi perusahaan besar. Saat ini siapapun bisa jadi korban *cybercrime.*

Wazuh adalah salah satu dari sekian banyak aplikasi SIEM, tetapi Wazuh memiliki fitur yang yang sangat banyak dibandingkan dengan aplikasi open source sejenisnya. Dapat dilihat pula pada pemaparan diatas bahwa wazuh yang dapat mendeteksi bahkan untuk celah sebelum adanya serangan pada *Drupalgeddon*, serta mendeteksi serangan *bruteforce* yang dilakukan dengan memberikan deskripsi yang jelas mengenai celah dan serangan yang terdapat dalam sistem.

Daftar Pustaka

[1] Kominfo.go.id. (2022). Unit Kerja. Diakses pada 26 November 2022, dari https://www.kominfo.go.id/unit-kerja.

[2] Kelompok 2 ~ Kelas A. (2022, 8 November). Instalasi Wazuh Dan Mendeteksi Serangan Bruteforce. Diakses pada 27 November 2022, dari https://medium.com/@rvssd/pengertian-cara-menginstall-wazuh-dan- menyalakan-layanan-ssh-beserta-mendeteksi-serangan-brute- 4d19174e7c45.

[3] Kelompok 2 ~ Kelas A. (2022, 17 November). Deteksi Serangan Drupalgeddon Menggunakan Wazuh. Diakses pada 27 November 2022, dari https://medium.com/@rvssd/akses-wazuh-server-9df32ba296db

[4] Kampusmerdeka.kemdikbud.go.id. (2022). Laporan Mingguan. Diakses Pada 26 November 2022, dari https://kampusmerdeka.kemdikbud.go.id/activity/active