AUTOMASI KESELAMATAN WEB MENGGUNAKAN ANSIBLE PLAYBOOK DAN KEBERKESANANNYA

Nur Syafiqah Izzati binti Sha'aban[1*]

Wan Fariza Paizi@Fauzi[2]

[1,2]*Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor Darul Ehsan, Malaysia*

Abstrak

Aplikasi web kini menjadi aset penting bagi kebanyakan organisasi. Walau bagaimanapun, peningkatan serangan digital berlaku menyebabkan terhasil pelbagai jenis risiko keselamatan web aplikasi dan salah satunya adalah risiko kawalan akses rosak. Kelemahan aplikasi web dapat mengakibatkan pelanggaran data, reputasi perniagaan yang merundum, dan pendedahan maklumat pelanggan. Ini memberi imej yang tidak baik kepada sesebuah organisasi. Menjalankan tugas konfigurasi keselamatan secara manual seringkali menyebabkan ralat mudah berlaku. Untuk mengatasi masalah ini, sebuah *playbook* akan dibangunkan dengan menggunakan alat automasi Ansible. *Playbook* ini dibangunkan untuk web aplikasi yang baru dibangunkan dimana arahan keselamatan konfigurasi akan berpandukan 10 risiko keselamtan web aplikasi OWASP. Dengan *playbook* ini, pelayan web aplikasi yang baru dapat melakukan pengerasan awal pada sistem dengan lebih mudah dan efisien. Kajian ini menggunakan data dari artikel OWASP, RedHat, GitHub, dan sumber lain yang relevan. *Playbook* ini dapat membantu dalam melaksanakan tugas keselamatan secara automatik serta mengurangkan risiko keselamatan, dan memenuhi keperluan keselamatan web yang diperlukan. Hasil projek ini adalah keberjayaan dalam membangunkan modul keselamatan *playbook* yang berfungsi menggunakan alat automasi Ansible. Dengan pendekatan ini, diharapkan organisasi bukan untung dapat melakukan

pengerasan awal ke atas sistem mereka dengan lebih efisien, menjimatkan kos pengurusan dan meningkatkan keselamatan keseluruhan aplikasi web mereka.

Kata kunci: [*Playbook*, Automasi, Pengerasan, Konfigurasi]

Pengenalan

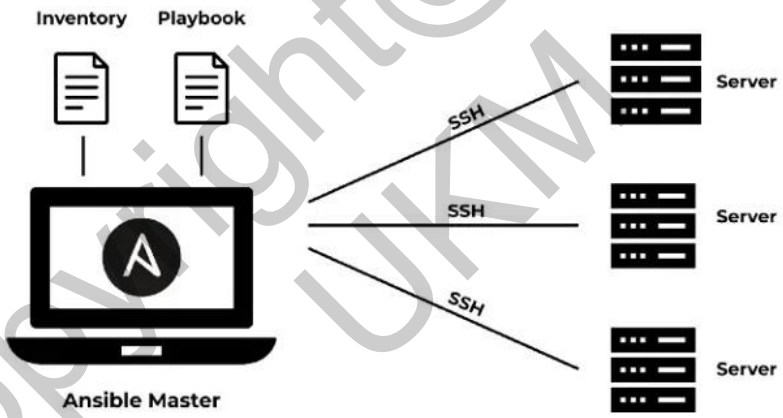
Laman web merupakan suatu keperluan bagi sesebuah organisasi untuk memudahkan urusan mereka untuk berhubung dengan klien. Akan tetapi kesedaran berkenaan pengerasan pelayan web aplikasi sesebuah organisasi selalu diambil mudah sehingalah laman web itu digodam oleh penyerang digital dan menyebabkan kerugian besar berlaku ke atas sesebuah organisasi teserbut. Masalah ini akan memberi kesan yang mendalam terhadap pihak pengguna dan juga pemilik laman web teserbut dimana data-data mereka akan dijadikan taruhan. Keselamatan siber adalah salah satu risiko utama yang dihadapi oleh organisasi di seluruh dunia. Daripada artikel yang bertajuk Cyber Attack: A real threat to NGO and and Non-profits (n.d, 2022) menyatakan pada tahun 2021, lebih 50% NGO dilaporkan menjadi sasaran serangan siber. Laporan terbaru Bank Dunia menunjukkan bahawa tidak ada sektor yang terlarang daripada penggodam. Antara sebab mengapa web Organisasi Bukan Untung (NPO) ini menjadi sasaran serangan siber adalah kerana penyerang ingin mendapat maklumat pihak ketiga ataupun penyerang mempunyai tujuan yang tersendiri. Kesimpulannya, small-medium enterprise (SMEs) dan Organisasi Bukan Untung (NPO) adalah salah satu sasaran utama bagi penggodam digital untuk mengancam sistem mereka dan ini memberi kesan buruk kepada ramai pihak terutamanya kepada klien mereka.

Oleh yang demikian, pelayan web aplikasi telah menjadi aset digital yang penting bagi sesebuah organisasi dan memerlukan pengawasan keselamatan yang maksimum ke atasnya untuk memastikan penyerang digital tidak dapat melakukan serangan ke atas sistem. Daripada artikel (Banach, 2020), pengerasan sistem adalah praktis yang dilakukan dalam

menjaga keselamatan sesebuah sistem untuk mengurangkan peratusan diserang oleh penyerang digital. Keselamatan pelayan web aplikasi dilakukan dengan melakukan tugasan konfigurasi keselamatan ke atas pelayan web aplikasi dimana ia akan menetapkan peraturan untuk mengoptimumkan keselamatan, prestasi dan kemampuan web aplikasi teserbut berfungsi. Ia mudah untuk menghadapi ketidakselarasan konfigurasi disebabkan oleh langkah-langkah manual yang diambil, dan tiada cara untuk menangani perubahan konfigurasi kecuali dengan menjalankan semula senarai semak secara manual. Daripada analisis daripada pelbagai artikel (cth., RedHat, GitHub, OWASP), antara sebab permasalahan serangan digital keatas sesebuah sistem ini berlaku kerana kekurangan sumber kewangan syarikat untuk mengupah pakar keselamatan untuk mengeraskan sistem mereka. Selain itu, ancaman ini juga berlaku kerana konfigurasi keselamatan yang terdedah kepada ralat dan tindakan dilakukan secara perlahan kerana sysadmin menjalankan senarai semak tugas berkaitan keselamatan secara manual dan tidak akan lari daripada berlakunya ralat manusia. Ralat manusia ini merujuk kepada kesalahan dan atau kelalaian yang dibuat oleh manusia dalam melakukan sesuatu tugas. Ralat manusia adalah hal yang wajar kerana ia merupakan perkara yang semulajadi. Walau bagaimanapun, perkara ini perlu dibendung kerana perkara ini memberikan kesan yang buruk malah akan merugikan sesebuah organisasi jika ia kerap berlaku. Dalam kebanyakkan industri dan bidang, usaha yang dilakukan untuk mengurangkan ralat manusia berlaku adalah dengan melalui latihan, menetapkan prosedur yang lebih baik dan penggunaan teknologi yang lebih canggih.

Teknologi era kini menyediakan pelbagai kecanggihan teknologi yang memudahkan tugasan manusia. Tidak dapat dinafikan bawaha teknologi dapat melakukan tugasan secara konsistensi dimana ia merupakan aspek utama yang diperlukan untuk memastikan keselamatan sesebuah sistem dapat mencapai tahap keselamatan yang optimum. Bedasarkan artikel (5 Ways to Harden a New System with Ansible, 2020), alat automasi ansible adalah

alat automasi yang terbaik untuk melaksanakan tugas konfigurasi dalam mengautomasikan beberapa aspek mudah dalam persekitaran sistem. Ansible adalah alat automasi dan pengurusan konfigurasi yang membolehkan untuk mengatur, mengkonfigurasi dan mengautomatikkan tugas-tugas pada infrastruktur IT. Di dalam ansible terdapat beberapa komponen utama dimana *playbook* adalah salah satu daripadanya. *Playbook* adalah fail konfigurasi dalam format YAML yang mempunyai senarai tugas yang akan dijalankan pada kumpulan hos yang telah ditetapkan. Dengan bantuan *playbook* yang telah ditakrifkan ketika pembangunan *playbook* ini., Ansible dapat menjalankan konfigurasi secara automatik dari nod kawal kepada nod urus melalui SSH protokol dengan efisien. Rajah 1 menunjukkan gambaran bagaimana playbook yang dibangunkan akan berfungsi ke atas pelayan web aplikasi.



Rajah 1 *Playbook Ansible* berfungsi

Kajian ini dilakukan untuk membantu organisasi bukan untung (NPO) serta small-medium enterprise (SMEs) ataupun akademik university dalam melakukan pengerasan awal ke atas sistem mereka daripada diserang oleh individu yang tidak bertanggungjawab. Antara objektif utama dalam pembangunan projek ini ialah untuk menganalisis keperluan konfigurasi bagi sistem yang baru dibagunkan. Selain itu, untuk membangunkan *playbook* menngunakan alat automasi daripada sumber terbuka iaitu Ansible yang berfungsi

mengendalikan konfigurasi keselamatan ke atas pelayan web aplikasi yang berpandukan 10 ancaman web aplikasi OWASP dan menjadikan pengerasan sistem mencapai keperluan keselamatan web aplikasi yang minima. Akhir sekali, kajian ini dilakukan untuk mengenal pasti kerberkesanan *playbook* dalam melakukan konfigurasi ke atas berbilang sistem dan membuktikan Ansible adalah alat yang bersifat fleksibel.

Kajian ini memfokuskan kepada dua skop iaitu 10 ancaman teratas keselamatan siber aplikasi web yang telah dinyatakan oleh OWASP dan website baru bagi organisasi bukan untung (NPO) yang menggunakan pelayan jenis Apache. Skop ini berkait antara satu sama lain dimana skop yang pertama dijadikan panduan untuk melakukan pembangunan produk untuk kegunaan pelayan web aplikasi yang baru agar organisasi ini dapat mempraktikan pengerasan awal ke atas sistem mereka. Pemilihan skop ini dilakukan untuk menumpukan kepada amalan pengerasan sistem pada peringkat awal sesebuah sistem dibangunkan. Kajian ini dilakukan untuk membantu setiap organisasi yang memiliki sistem yang baru dibangunkan dalam mengamalkan melakukan pengerasan awal ke atas sistem mereka untuk mengurangkan potensi digodam oleh pengguna yang tidak bertanggungjawab. Kajian ini menyumbang manfaat yang besar keatas industri keselamtan siber dimana industri ini adalah sektor yang terus berkembang seiring dengan peningkatan ancaman siber yang dihadapi oleh seluruh organisasi seluruh dunia.

Bedasarkan kajian oleh S. (2022) dan Pranav et al. (2021), mereka memfokuskan penggunaan alat automasi Ansible untuk mengautomasikan konfigurasi pelayan web dan pengeraskan sistem di lingkungan awan. Kajian tersebut menyatakan bahawa pentingnya automasi dalam meningkatkan efisiensi, mengurangi kesalahan manusia, dan meningkatkan keamanan dalam pengelolaan pelayan web. Ansible, sebagai alat konfigurasi sumber terbuka yang popular, membantu mencapai konfigurasi dan pengelolaan yang lebih konsisten dan efisien, menghemat waktu dan sumber daya, serta mengurangi risiko serangan siber dan

masalah kesalahan konfigurasi. Ini membuktikan bahawa, alat automasi Ansible ini adalah alat yang berkesan untuk melakukan tugas konfigurasi secara automasi.

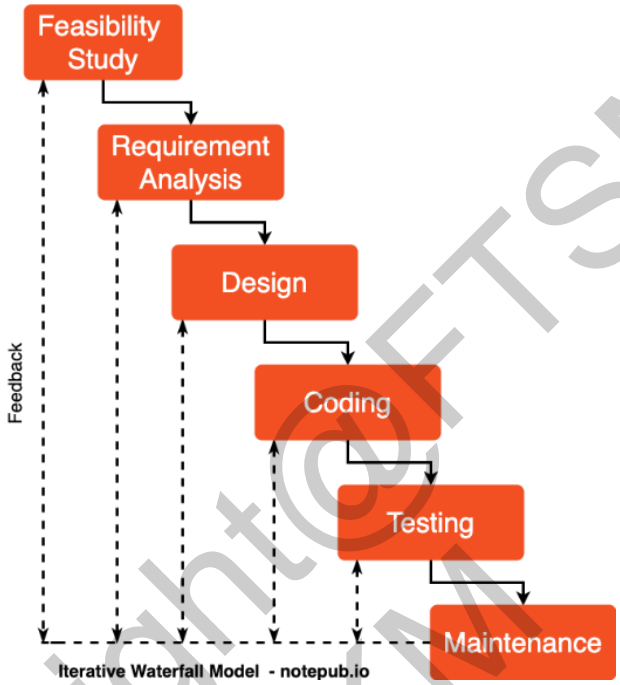
Metodologi yang digunapakai dalam pembangunan *playbook* ini adalah model Air Terjun Iteratif. Ini kerana dalam projek pembangunan perisian praktikal, model air terjun klasik sukar digunakan. Jadi, model air terjun iteratif boleh dianggap sebagai menggabungkan perubahan yang diperlukan kepada model air terjun klasik untuk menjadikannya boleh digunakan dalam projek pembangunan perisian praktikal. Ia hampir sama dengan model air terjun klasik kecuali beberapa perubahan dibuat untuk meningkatkan kecekapan pembangunan perisian.

Pembangunan *playbook* ini diharapkan dapat menjadi salah satu alternatif yang baru kepada sysadmin dalam meningkatkan prestasi dalam melakukan tugasan konfigurasi keselamatan dalam melakukan pengerasan awal ke atas sistem mereka. Dalam laporan teknikal ini terdiri daripada beberapa unsur yang memberi penerangan terhadap pembangunan *playbook* ini secara ringkas seperti pengenalan, metodologi kajian, keputusan dan perbincangan, kesimpulan dan penghargaan.

Metodologi Kajian

Model yang digunapakai dalam membangunkan keselamatan automatik *playbook* ini ialah model Air Terjun Iteratif. Dalam projek pembangunan perisian praktikal, model air terjun klasik sukar digunakan. Bedasarkan artikel (Software Engineering | Iterative Waterfall Model - GeeksforGeeks, 2018), model ini akan berulang kali menyediakan laluan maklum balas daripada setiap fasa ke fasa sebelumnya. Ini merupakan perbezaan yang besar berbanding model air terjun yang klasik. Apabila ralat dikesan pada beberapa fasa kemudian, laluan maklum balas ini membenarkan pembetulan ralat yang dilakukan oleh pengaturcara semasa beberapa fasa. Laluan maklum balas membenarkan fasa diolah semula di mana ralat

dilakukan dan perubahan ini ditunjukkan dalam fasa kemudian. Tetapi, tiada laluan maklum balas ke peringkat - kajian kebolehlaksanaan, kerana sebaik sahaja projek telah diambil, tidak mudah melepaskan projek itu. Model ini sangat berguna untuk projek yang kecil dan kehendak projek dapat difahami dengan sebaiknya.



Rajah 2 Model Air Terjun Iteratif

Rajah 2 menunjukkan gambaran bagaimana model pembanguna ini berfungsi. Fasa pembangunan model air terjun iteratif ni dimulakan dengan menganalisis bahan ilmiah seperti artikel dan jurnal berkenaan dengan keselamatan automasi, ancaman web aplikasi, jenis ancaman keselamatan siber, kes ancaman keselamatan siber dan sewaktu dengannya. Objektif projek dikaji untuk penyelesaian yang efektif. Ini membentuk asas fasa-fasa seterusnya dalam proses penyelidikan. Seterusnya adalah fasa reka bentuk,dimana pada fasa ini kita akan merangka reka bentuk projek agar pembangun dan pengguna dapat melihat gambaran projek sebelum projek ini dibangunkan pada fasa pembangunan. Fasa pembangunan merupakan tahap kritis yang memerlukan waktu yang cukup panjang untuk membangunkan produk. Pada fasa ini kita akan mengunakan segala bahan yang telah

dikumpulkan pada fasa-fasa sebelum ini sebagai panduan semasa pembangunan dilakukan. Pada tahap pengujian, produk diuji terhadap pengguna untuk mengumpulkan data tentang keberhasilan dan kesesuaian produk, serta untuk memastikan bahwa tujuan projek tercapai dan masalah yang dikenal pasti dapat diselesaikan. Terdapat tiga jenis ujian: alfa, beta, dan penerimaan. Penyelenggaraan adalah tahap yang paling penting dalam kitaran hayat perisisan dan konsepnya dibahagi menjadi tiga bahagian: pembetulan, sempurna, dan adaptif. Penyelenggaraan adaptif penting untuk meningkatkan produk dalam jangka waktu yang panjang, ini kerana protokol keselamatan web akan sentiasa berubah mengikut keperluan semasa. Ini kerana, dunia keselamatan siber akan terus berkembang pesat dimana akan wujud lebih banyak risiko keselamatan web aplikasi yang akan mengancam keselamatan pelayan web aplikasi sesebuah organisasi. Oleh yang demikian *playbook* ini perlu sentiasa dikemaskini memgikut keperluan semasa.

Pada tahap pembangunan automasi *playbook* ini, keperluan perkakasan dan perisian yang digunakan adalah seperti berikut:

Jenis	Perincian
Pemprosesan (CPU)	Intel Core™ i5-10210U CPU @ 1.60GHz
Memori (RAM)	8.0 GB
Sistem Operasi	Windows 10
Penyimpanan	475 GB
Penggunaan Internet	Ya

Jadual 1 Keperluan Perkakasan

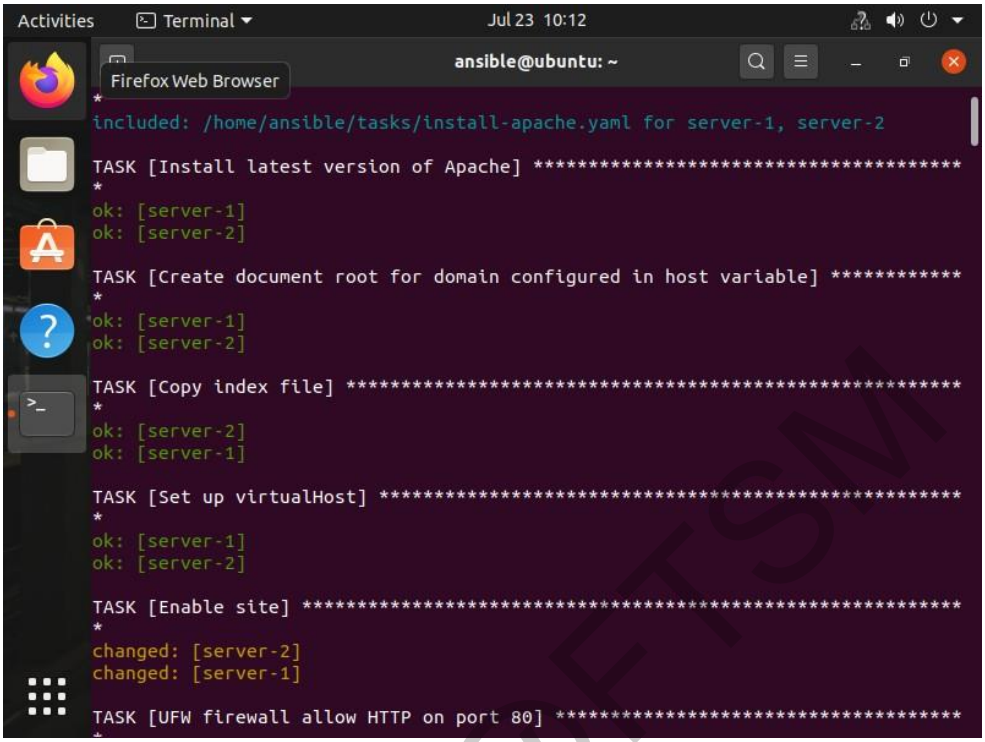
Jenis	Perincian
Sistem Operasi	Ubuntu-Based Linux
Alat sumber terbuka	Ansible
Mesin Maya	VMware

Jadual 2 Keperluan Perkakasan

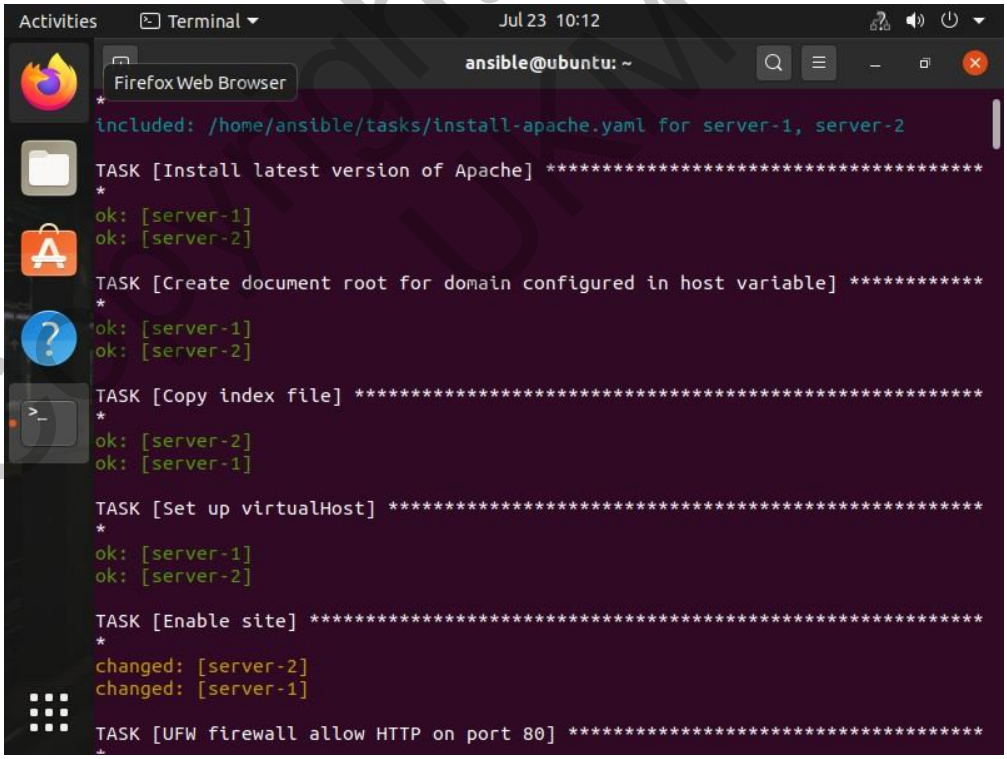
Dengan sumber daya perkakasan dan perisian yang dinyatakan dalam jadual 1 dan jadual 2, proses pembangunan dan automasi *playbook* dapat dijalankan dengan lancar dan membolehkan pengguna mengkonfigurasi dan menguruskan sistem pelayan web secara lebih cekap serta meningkatkan keselamatan keseluruhan sistem.

Keputusan dan Perbincangan

Playbook ini merupakan modul pengerasan pelayan web yang telah ditakrifkan setiap satu konfigurasi keselamatan ke atas fail-fail *sub-playbook* yang dibangunkan dan berpandukan 10 risiko teratas web aplikasi yang dinyatakan oleh OWASP. *Playbook* yang dihasilkan ini dibangunkan khusus kepada organisasi bukan untung (NPO) yang memiliki pelayan web aplikasi yang baru dibangunkan dan menggunakan pelayan jenis Apache. Dengan *playbook* ini, pengguna dapat melakukan langkah awal dalam melakukan pengerasan ke atas sistem mereka. Ini adalah untuk mengurangkan risiko sistem mereka digodam oleh individu yang tidak bertanggungjawab dan memastikan kesedaran untuk mengamalkan pengerasan ke atas pelayan web aplikasi mereka secara konsisten. Dengan *playbook* ini, konfigurasi keselamatan ke atas sesebuah pelayan web aplikasi dapat dilakukan dengan mudah dimana hanya perlu melaksanakan satu *playbook* sahaja tetapi dapat melakukan pelbagai jenis konfigurasi keselamatan. Secara tidak langsung, *playbook* ini dapat menjimatkan masa sysadmin dalam melakukan tugasan konfigurasi malah dapat melakukan tugasan dengan lebih efisien serta mengurangkan risiko berlakunya ralat mudah ataupun ralat manusia.



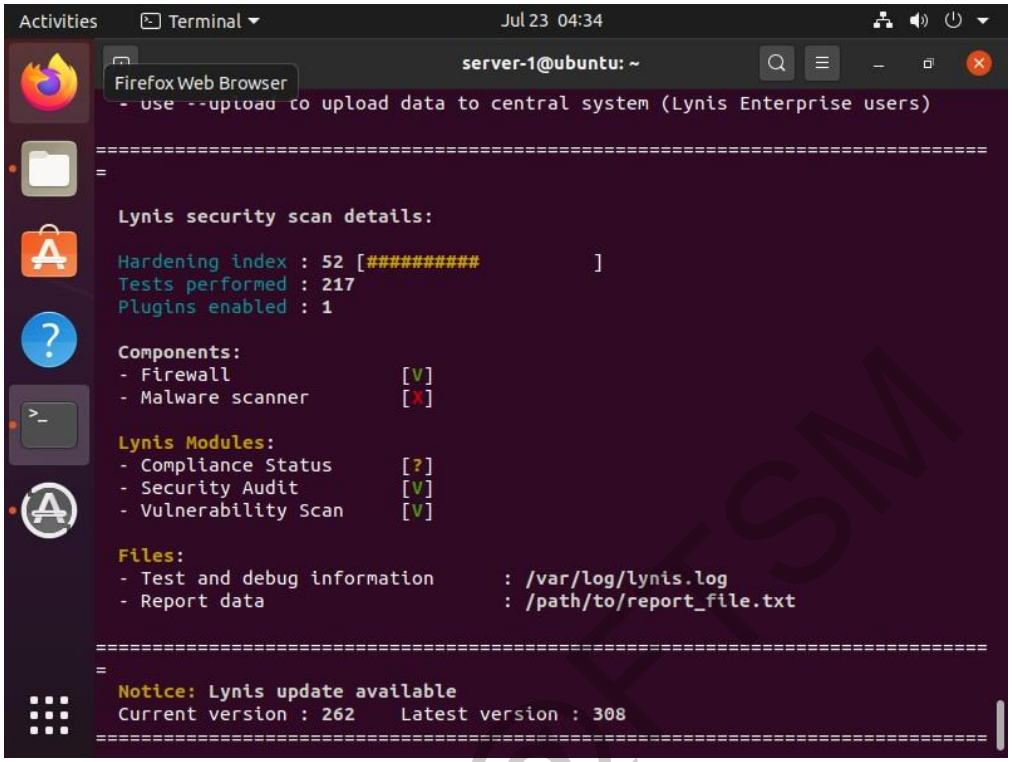
Rajah 3 Output



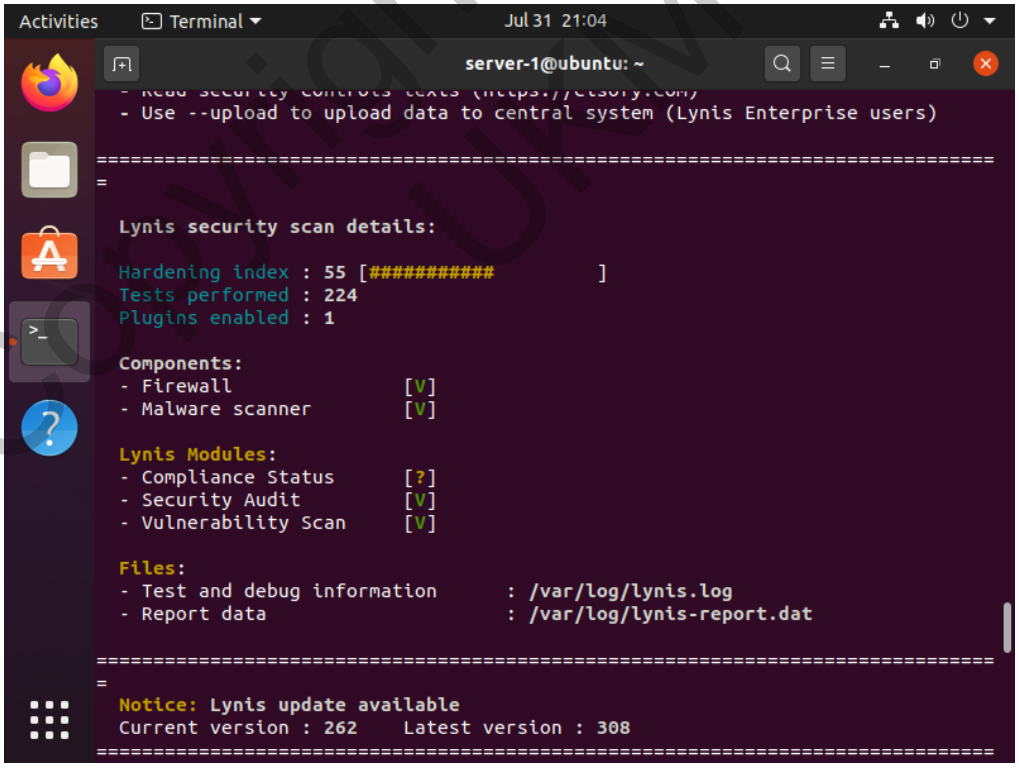
Rajah 4 Output

Berdasarkan gambar rajah 3 dan 4, ia merupakan antara output yang terhasil selepas melaksanakan *playbook* induk ke atas nod urus iaitu server-1 dan server-2. Ini menunjukkan bahawa play*book* induk yang telah dinamakan sebagai '*HWAS-playbook.yaml'* telah berjaya dalam melaksanakan tugasan konfigurasi ke atas nod urus secara automasi. Pelaksanaan *playbook* Ansible mempamerkan prestasi Ansible yang berjaya sebagai alat automasi untuk melakukan konfigurasi pada hos sasaran iaitu nod urus yang telah ditetapkan. Dengan bantuan playbook ini, satu siri tugas yang kompleks telah dicapai dengan cekap dan berkesan pada *server-1* dan *server-2*. Ini menujukkan bahawa, kesemua *sub-playbook* yang dibangunkan juga dapat digunakan dan berkesan dalam memberi arahan kepada Ansible.

Untuk lebih mengukuhkan keberkesanan *playbook* Ansible ini dalam melakukan konfigurasi keatas nod urus yang telah ditetapkan, audit keselamatan akan dilakukan ke atas nod urus untuk memastikan *playbook* ini berfungsi dalam melakukan konfigurasi yang dilaksanakan ke atas nod urus. Jadi, projek ini telah memilih alat keselamatan audit Lynis untuk melakukan pengimbasan keselamatan audit ke atas nod urus yang telah ditetapkan.



Rajah 5 Audit Keselamatan Sebelum Pelaksanaan *Playbook*



Rajah 6 Audit Keselamatan Selepas Pelaksanaan *Playbook*

Gambar rajah 5 menunjukkan keputusan keselamatan audit yang dilakukan sebelum pelaksanaan playbook dilkasanakan keatas nod urus pada server-1 manakala rajah 6 menunjukkan keputusan keselamatan audit selepas pelaksanaan playbook ke atas nod urus server-1. Selepas melaksanakan *playbook* untuk mengkonfigurasi sistem, terdapat peningkatan dalam keputusan imbasan keselamatan Lynis. Indeks pengerasan meningkat daripada 52 kepada 55, menunjukkan bahawa beberapa langkah keselamatan tambahan telah berjaya dilaksanakan, meningkatkan lagi postur keselamatan sistem. Bilangan ujian yang dilakukan juga meningkat daripada 217 kepada 224, yang bermakna lebih banyak aspek keselamatan sistem telah dinilai semasa imbasan terkini.

Selepas melakukan audit keselamatan sebelum dan selepas *playbook* ini dilaksankan, beberapa perkara dapat dikenal pasti. Hasil audit keselamatan selepas pelaksanaan *playbook* menunjukkan indeks pengerasan yang lebih baik, peningkatan bilangan ujian yang dilakukan dan kejayaan pelaksanaan komponen pengimbas perisian hasad, yang tiada dalam imbasan awal. Walau bagaimanapun, indeks itu belum mencapai keoptimum pengerasan sistem. Ia menunjukkan bahawa lebih banyak kerja mungkin diperlukan untuk memastikan sistem sejajar dengan piawaian keselamatan tertentu. Secara keseluruhannya, pelaksanaan *playbook* ini membawa kepada peningkatan ketara dalam keselamatan sistem, tetapi masih terdapat ruang untuk penambahbaikan dalam melakukan pengerasan ke atas sistem ini agar ia mencapai keoptimum pengerasan sistem yang lebih baik dari masa ke semasa.

Kesimpulan

Kajian ini bertujuan untuk membantu organisasi yang memiliki sistem baru dalam menghadapi ancaman serangan siber dengan mengamalkan pengerasan awal ke atas sistem pelayan web aplikasi mereka. Penggunaan *playbook* yang dibangunkan menggunakan alat automasi Ansible dapat membantu menjalankan konfigurasi keselamatan secara otomatis dan konsisten ke atas berbilang sistem. Kajian ini mengenalpasti kekurangan sumber kewangan dan konfigurasi yang perlahan sebagai permasalahan utama yang menyebabkan keselamatan sistem pelayan web aplikasi sering diabaikan. Dengan membangunkan *playbook* yang efisien, organisasi dapat mengurangkan potensi digodam oleh penyerang digital dan meningkatkan keselamatan sistem mereka.

Namun, terdapat beberapa kekangan yang dihadapi dalam kajian ini, seperti keterhadapan *playbook* hanya sesuai untuk pelayan web Apache dan sistem yang baru dibangunkan. Untuk meningkatkan kebergunaan *playbook*, penambahbaikan perlu dilakukan dengan mengadaptasikannya untuk berbagai jenis pelayan web dan pelayan web yang sedia ada. Selain itu, kajian ini juga menunjukkan bahawa tidak semua konfigurasi keselamatan dapat dijalankan secara otomatis, dan organisasi masih perlu mengupah pakar keselamatan untuk aspek yang lebih kompleks. Walau bagaimanapun, kajian ini memberikan sumbangan penting dalam memahami kepentingan pengerasan awal ke atas sistem pelayan web aplikasi bagi melindungi organisasi daripada ancaman serangan siber. Dengan langkah-langkah yang disyorkan dan *playbook* yang dibangunkan, diharapkan organisasi dapat meningkatkan tahap pengerasan sistem mereka dan mengurangkan risiko menjadi sasaran serangan digital.

Penghargaan

Syukur kepada ALLAH SWT dengan izin-Nya saya dapat menyiapkan kajian ini bagi memenuhi keperluan Ijazah Sarjana Muda Sains Komputer. Dengan limpah dan kurnia-Nya, saya dapat menyiapkan kajian ini dengan lancar.

Setinggi penghargaan saya berikan kepada penyelia saya, Dr. Wan Fariza Fauzi diatas bimbingan dan nasihat yang telah diberikan sepanjang proses kajian ini dijalankan. Terima kasih Dr diatas segala ilmu baru yang dikongsikan dan tunjuk ajar yang diberikan oleh Dr. Dengan berkat kesabaran Dr ketika menyelia saya daripada tidak berapa mengetahui dunia keselamatan siber dan kini saya telah memahami aspek-aspek keselamatan siber yang secara amnya sangat luas ilmunya. Jasa Dr amat saya hargai, tanpa tunjuk ajar beliau saya tidak mampu menyiapkan kajian ini.

Tidak lupa juga kepada keluarga saya. Terima kasih di atas kasih sayang yang mereka curahkan sehingga saya mampu sampai ketahap ini. Tanpa sokongan, doa dan redha mereka, saya tidak akan sampai ke tahap ini.

Terima kasih juga kepada rakan perjuangan saya diatas nasihat serta tunjuk ajar yang dikongsikan sepanjang kajian ini dijalankan. Nasihat dan kata sokongan daripada rakan-rakansemua amat membantu saya dalam menyiapkan tugasan ini.

Akhir sekali, saya ingin mengucapkan jutaan terima kasih kepada semua pihak yang terlibat secara langsung atau tidak langsung sepanjang proses kajian ini disiapkan. Tanpa kalian, kajian ini tidak dapat disiapkan dengan lancar dan jayanya.

RUJUKAN

Banach, Z. (2020, January 14). *System Hardening for Your Web Applications*. Invicti. Retrieved January 10, 2023, from https://www.invicti.com/blog/web-security/system-hardening-for-your-web-applications/

Enable Sysadmin. (2020, September 22). *5 ways to harden a new system with Ansible*. Retrieved January 10, 2023, from Red Hat website: https://www.redhat.com/sysadmin/harden-new-system-ansible

GeeksforGeeks. (2018, March 18). *Software Engineering | Iterative Waterfall Model*. Retrieved January 10, 2023, from https://www.geeksforgeeks.org/software-engineering-iterative-waterfall-model/

S, L. (2022, June 30). *Automation of Server Configuration Using Ansible. International Journal for Research in Applied Science and Engineering Technology*, 10(6), 4109–4113. https://doi.org/10.22214/ijraset.2022.44840

Nur Syafiqah Izzati binti Sha'aban (A179571)
Ts. Dr. Wan Fariza Paizi@Fauzi
Fakulti Teknologi & Sains Maklumat,
Universiti Kebangsaan Malaysia.