UNIVERSITAS NASIONAL

FAKULTAS TEKNOLOGI KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS NASIONAL

2024

DETEKSI DAN PENGUMPULAN ARTEFAK SERANGAN *WEB DEFACEMENT* PADA LINGKUNGAN BERBASIS *CLOUD* MENGGUNAKAN WAZUH DAN VELOCIRAPTOR SEBAGAI UPAYA PREVENTIF

Untuk memenuhi sebagai persyaratan memperoleh gelar Magister Komputer

Disusun Oleh :

Candra Kurniawan

NIM: 227064518014

PROGRAM STUDI MAGISTER TEKNOLOGI INFORMASI

FAKULTAS TEKNOLOGI KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS NASIONAL

TAHUN 2024

LEMBAR PENGESAHAN

JUDUL : DETEKSI DAN PENGUMPULAN ARTEFAK SERANGAN WEB DEFACEMENT PADA LINGKUNGAN BERBASIS CLOUD MENGGUNAKAN WAZUH DAN VELOCIRAPTOR SEBAGAI UPAYA PREVENTIF

Diajukan untuk memenuhi sebagai persyaratan

Memperoleh gelar Magister Komputer

Disusun Oleh :

Candra Kurniawan

227064518014

Tesis ini telah diuji dan dinyatakan lulus pada,

24 Agustus 2024

Telah diperiksa dan disetujui oleh :

Dosen Pembimbing	Ketua Program Studi
Dr. Agung Triayudi, S.Kom., M.Kom	Ir. Asrul Sani, S.T., M.T., M.Kom., Ph.D
NIDN. 0419068604	NIDN. 0303067003

PERNYATAAN ORISINALITAS

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah Tesis ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis disitasi dalam naskah ini dan disebutkan dalam daftar pustaka.

Apabila ternyata di dalam naskah Tesis ini dapat dibuktikan terdapat unsur-unsur plagiasi, saya bersedia Tesis ini digugurkan dan gelar akademik yang telah saya peroleh (Magister) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).

Jakarta, 26 Agustus 2024

Candra Kurniawan

227064518014

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah Subhanahu wa ta'ala karena atas rahmat serta karunia-Nya penulis dapat menyelesaikan Tesis yang berjudul "Deteksi dan Pengumpulan Artefak Serangan *Web defacement* pada Lingkungan Berbasis *Cloud* Menggunakan Wazuh dan Velociraptor sebagai Upaya Preventif". Selawat serta salam semoga tetap tercurah kepada Rasulullah Muhammad SAW, para sahabat dan pengikutnya hingga akhir zaman dan semoga kita mendapatkan syafaat di Yaumul Akhir nanti.

Penyusunan Tesis ini merupakan salah satu syarat dalam menyelesaikan Program Pendidikan S2 Magister Teknologi Informasi Universitas Nasional Jakarta. Penulis menyadari bahwa terselesainya penyusunan tugas akhir ini bukan hanya kerja penulis semata dan tidak akan berjalan lancar tanpa dukungan dan bantuan banyak pihak. Sehingga penulis bermaksud menyampaikan terima kasih kepada:

1. Allah Subhanahu Wa Ta'Ala;
2. Kedua orang tua penulis yang selalu memberikan doa, motivasi, kasih sayang, dan dukungan yang menjadi tekad semangat penulis dalam menyelesaikan Tesis;
3. Seluruh penyelenggara Pendidikan Universitas Nasional Jakarta yang telah memberikan dukungan dan fasilitas dalam menunjang Pendidikan;
4. Bapak Dr. Agung Triayudi S.Kom., M.Kom selaku Dekan FTKI sekaligus sebagai Dosen pembimbing yang telah memberikan bimbingan, arahan, motivasi, dan dukungan kepada penulis dalam pengerjaan Tesis;
5. Ibu Dr. Fauziah, S.Kom., MMSI dan Dr. Moh. Iwan Wahyuddin, S.T., M.T selaku penguji Tesis yang telah memberikan bimbingan dan arahan kepada penulis dalam pengerjaan Tesis;
6. Rekan-rekan S2 MTI Angkatan 2 yang telah berjuang bersama dan saling membantu menyelesaikan setiap tugas dan ujian yang dihadapi selama pendidikan;
7. Seluruh jajaran Direktorat Operasi Keamanan Siber khususnya Tim Incident Response yang telah memberikan dukungan informasi dan logistik yang dibutuhkan penulis untuk menyelesaikan Tesis ini.

8. Sholikah Sitihastusi S.Tr. Sos., M.H yang telah memberikan dukungan dan motivasi penulis dalam pengerjaan Tesis; dan
9. Seluruh pihak yang berjasa dan tidak dapat penulis sebutkan namanya satu persatu, semoga keikhlasannya dapat berbuah pahala yang berkali-kali lipat yang diberikan Allah Subhanahu Wa Ta'ala.

Penulis menyadari bahwa dalam penulisan Tesis masih jauh dari kata sempurna. Oleh karena itu, penulis menerima segala kritik dan saran demi kebaikan dan kesempurnaan Tesis yang telah disusun. Penulis berharap agar Tesis ini dapat bermanfaat bagi pembaca.

Jakarta, Agustus 2024

Penyusun

Candra K

ABSTRAK

Serangan siber di Indonesia mengalami peningkatan, khususnya pada sektor pemerintahan yang terdeteksi mengalami banyak serangan *web defacement* situs judi online. Observasi yang dilakukan selama satu bulan ditemukan setidaknya terdapat 1.279 situs pemerintah terdampak serangan ini. Insiden yang terjadi banyak dijumpai pada situs yang menggunakan layanan *cloud* pada pihak ketiga. Serangan tersebut salah satunya memanfaatkan kerentanan yang terdapat pada aplikasi *public facing* seperti *brute force* dan *file upload*. Penelitian yang dilakukan berhasil melakukan rekonstruksi serangan *web defacement* situs judi online pada server berbasis AWS dan GCP berdasarkan *framework* Mitre Att&ck dan melakukan deteksi menggunakan Wazuh yang diintegrasikan dengan Telegram dan menggunakan Velociraptor untuk melakukan isolasi dan pengumpulan artefak. Hasil rekonstruksi dan pengujian menunjukkan bahwa Wazuh dapat mendeteksi serangan secara *real-time* dengan rata-rata 1.2 s/alert dan mengirimkan notifikasi pada Telegram, sedangkan pengujian isolasi jaringan yang dilakukan menggunakan Velociraptor diketahui bahwa proses isolasi tidak berjalan pada server GCP dan berjalan dengan baik pada server AWS.

Kata Kunci : Artefact Collection, Deteksi, Wazuh, *Web defacement*, Velociraptor

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL