

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
MENGUNAKAN WAZUH DAN VELOCIRAPTOR SEBAGAI
UPAYA PREVENTIF

Diajukan untuk memenuhi sebagai persyaratan



Dosen Pembimbing

Dr. Agung Triayudi, S.Kom., M.Kom.
NIDN. 0419068604

Ir. Asrul Saifuddin, S.T., M.P., M.Kom., Ph.D
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. Sholikhah 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.



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

LEMBAR PENGESAHAN.....	iii
PERNYATAAN ORISINALITAS	iv
KATA PENGANTAR.....	v
ABSTRAK.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL.....	xiii
BAB 1 PENDAHULUAN	1
1.1 Latar belakang.....	1
1.2 Rumusan masalah.....	4
1.3 Tujuan	4
1.4 Manfaat	4
1.5 Batasan masalah	5
1.6 Sistematika pembahasan.....	5
BAB 2 LANDASAN KEPUSTAKAAN	7
2.1 Telaah Pustaka.....	7
2.1.1 <i>Cloud Environment</i>	7
2.1.2 <i>Artefact Collection</i>	8
2.1.3 <i>Velociraptor</i>	9
2.1.4 <i>Wazuh</i>	10
2.2 Penelitian Terkait	11
2.2.1 <i>Cloud Forensics: An Overview</i>	11

2.2.2 A Digital Forensic Process Model for Cloud Computing.....	11
2.2.3 Cloud Computing Digital Forensic Challenges	12
2.2.4 Cloud Incident Response: Challenges and Opportunities.....	12
2.2.5 Analysis of Modern Cloud Services to Ensure Cybersecurity	13
2.2.6 Forensic Analysis of Cloud Virtual Environments	14
BAB 3 METODOLOGI PENELITIAN	16
3.1 Metode Penelitian.....	16
3.2 Objek Penelitian	16
3.3 Tahap Penelitian.....	17
3.3.1 Persiapan	17
3.3.2 Perancangan	18
3.3.3 Implementasi.....	18
3.3.4 Pengujian	19
3.3.5 Analisis	20
BAB 4 HASIL PENELITIAN.....	21
4.1 Persiapan.....	21
4.2 Perancangan.....	23
4.2.1 Topologi Jaringan	23
4.3 Implementasi	24
4.3.1 Security Operation Center	24
4.3.2 Wazuh	24
4.3.3 Velociraptor	26
4.3.4 Integrasi Telegram-Wazuh.....	29
4.3.5 Perangkat Victim	30
4.3.6 Perangkat Attacker.....	31

4.4 Pengujian.....	31
4.5 Analisis.....	41
4.5.1 Deteksi.....	41
4.5.2 Containment.....	49
4.5.3 Pengumpulan Artefak.....	50
BAB 5 PENUTUP.....	56
5.1 Kesimpulan.....	56
5.2 Saran.....	57
DAFTAR PUSTAKA.....	58
LAMPIRAN.....	62



DAFTAR GAMBAR

Gambar 2. 1 Perbedaan Lingkungan Cloud dan On Premise	8
Gambar 2. 2 SANS Incident ResponsPlan	9
Gambar 2. 3 NIST Incident Handling Guide (Cichonski et al., 2012)	9
Gambar 2. 4 Dashboard Velociraptor	10
Gambar 2. 5 Incident Response Step By Ozer et.al	13
Gambar 3. 1 Tahap Penelitian	17
Gambar 3. 2 Skema Penelitian	18
Gambar 3. 3 Skema Implementasi	19
Gambar 3. 4 Skema Pengujian	20
Gambar 4. 1 Observasi Pencarian Situs Pemerintah Terdampak Judi Online	22
Gambar 4. 2 Topologi Jaringan	24
Gambar 4. 3 Dashboard Wazuh (Jumlah Agent)	26
Gambar 4. 4 Dashboard Velociraptor (Jumlah Agent)	26
Gambar 4. 5 Velociraptor Menampilkan Directory	27
Gambar 4. 6 Velociraptor Inspect File	28
Gambar 4. 7 Velociraptor Quarantine Host	28
Gambar 4. 8 Integrasi Notifikasi Telegram	30
Gambar 4. 9 Scanning NMAP pada Server AWS	33
Gambar 4. 10 Scanning NMAP pada Server GCP	34
Gambar 4. 11 Scanning WPScan pada Server AWS	35
Gambar 4. 12 Scanning WPScan pada Server GCP	36
Gambar 4. 13 Brute Force Valid Combinations Found	36
Gambar 4. 14 Upload File Backdoor	37
Gambar 4. 15 Akses Backdoor/Webshell	37
Gambar 4. 16 Pembuatan Username dan Kredensial Baru	38
Gambar 4. 17 Encoded Backdoor	39
Gambar 4. 18 File dan Sistem Discovery	40
Gambar 4. 19 Defacement Situs Judi Online	41

Gambar 4. 20 Deteksi Aktivitas Serangan	42
Gambar 4. 21 Deteksi Aktivitas Reconnaissance	42
Gambar 4. 22 Deteksi Aktivitas Password Guessing	43
Gambar 4. 23 Deteksi Aktivitas Upload Backdoor	44
Gambar 4. 24 Deteksi Aktivitas Slot Gacor	45
Gambar 4. 25 Notifikasi Aktivitas Serangan.....	46
Gambar 4. 26 Aktif Respons Blocking IP	49
Gambar 4. 27 Proses Quarantine pada Server AWS	50
Gambar 4. 28 Proses Quarantine pada Server GCP	50
Gambar 4. 29 Quarantine Velociraptor	51
Gambar 4. 30 Artefact Collection.....	51
Gambar 4. 31 Mode Recursive Download Files	53
Gambar 4. 32 Modul VirusTotal pada Velociraptor.....	54
Gambar 4. 33 Modul SSHLogin pada Velociraptor.....	55
Gambar 4. 34 Kustom Modul Thor	55



DAFTAR TABEL

Tabel 4. 1 Script Dorking	21
Tabel 4. 2 Pemodelan Serangan Mitre Att&ck.....	32
Tabel 4. 3 Tingkat Dampak Alert Wazuh.....	46
Tabel 4. 4 Perhitungan MTTD	48
Tabel 4. 5 Potensial Barang Bukti Digital.....	52

