Analisa Kerentanan pada *Vulnerable docker* dengan metode *Vulnerability Scanning* dan *Penetration Testing* menggunakan *Opensource tools*

Laporan Tugas Akhir

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana
Informatika Universitas Muhammadiyah Malang

Abdurrahman Harish AlMauqy
201910137011316

Bidang Minat
Jaringan

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MALANG
2023

LEMBAR PERSETUJUAN

Analisa Kerentanan pada Vulnerable Docker dengan metode Vulnerability Scanning dan Penetration Testing menggunakan Opensource tools

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang

Menyetujui,
Malang, *29 Desember 2023*

Dosen Pembimbing 1	Dosen Pembimbing 2
Luqman Hakim S.Kom., M.Kom.	**No Name**
NIP. 10819030658PNS.	**NIP.**

LEMBAR PENGESAHAN

Analisa Kerentanan pada Vulnerable Docker dengan metode Vulnerability Scanning dan Penetration Testing menggunakan Opensource tools

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
InformatikaUniversitas Muhammadiyah Malang

Disusun Oleh :

Abdurrahman Harish Al Mauqy

201910370311316

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 29 Desember 2023

Menyetujui,

Dosen Penguji 1	Dosen Penguji 2
Ir Denar Regata Akbi S.Kom., M.Kom.	**Ir. Syaifuddin S.Kom., M.Kom., IPM, ASEAN Eng**
NIP. 10816120591PNS.	**NIP. 10816120590PNS.**

Mengetahui,
Ketua Jurusan Informatika

Ir. Galih Wasis Wicaksono S.kom. M.Cs.
NIP. 10814100541PNS.

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : **Abdurrahman Harish AlMauqy**
NIM : **201910370311316**
FAK./JUR. : **Informatika**

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"Analisa Kerentanan pada *Vulnerable Docker* dengan metode *Vulnerability Scanning* dan *Penetration Testing* menggunakan *Opensource tools*"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing

Luqman Hakim, S.Kom., M.Kom.

Malang, 19 Desember 2023
Yang Membuat Pernyataan

Abdurrahman Harish A

ABSTRAK

Salah satu teknologi dalam *deployment* yaitu *docker*. *Docker* adalah *open source projec*t yang dirancang untuk membantu *application deployment* dengan menggunakan *software containers*. Dengan hadirnya kontainer *Docker*, dan segala kemudahan didalamnya tentu juga perlu diperhatikan mengenai keamanan dan risiko dari penggunaan *Docker* tersebut. *Vulnerability Scanning* merupakan metode dalam mencari kerentanan terhadap objek yang akan diuji yaitu *vulnerable docker*. *Vulnerable docker* merupakan sebuah *virtual machine* berisi *Docker* yang rentan yang dibuat oleh perusahaan *NotSoSecure*. Kemudian dengan kombinasi metode *Penetration Testing* yang merupakan metode Pengujian penetrasi, yang melibatkan simulasi serangan nyata untuk menilai risiko yang terkait dengan potensi pelanggaran keamanan. Tujuan dari penelitian Untuk memperoleh kerentanan pada *vulnerable docker* dengan *tools scanning* dan mengkombinasi *Vulnerability scanning* dengan *Penetration Testing* dalam mencari kerentanan pada *Vulnerable Docker*. Hasil yang ditemukan pada *Vulnerability scanning* dengan *Trivy* sejumlah 883 *vulnerability, Nessus* 45 *vulnerability* yang telah dikategorikan sebagai kategori *Critical, High, Medium, Low*, dan Info. Pada *penetration testing* serangan yang dilakuan bruteforce user dan password *Wordpress*, ditemukan user dan *password* untuk masuk ke sistem *admin Wordpress.*

Kata kunci: *Vulnerable Docker, Vulnerability Scanning, Penetration Testing, Opensource tools.*

KATA PENGANTAR

Puji syukur ke hadirat Allah Yang Maha Pengasih Lagi Maha Penyayang atas rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir. Shalawat serta salam tidak lupa penulis hanturkan kepada junjungan kita, Nabi Muhammad Shallallahu 'alaihi wasallam. Laporan ini dibuat untuk memenuhi persyaratan kelulusan di Fakultas Teknik Informatika, Universitas Muhammadiyah Malang dengan judul "Analisa Kerentanan pada *Vulnerable docker* dengan metode *Vulnerability Scanning* dan *Penetration Testing* menggunakan *Opensource tools*". Penulis bersyukur dapat mengerjakan dengan maksimal dan menyampaikan ucapan terima kasih kepada semua pihak yang telah membantu dan memberikan dukungan selama proses pengerjaan, penulis juga mengucapkan terima kasih kepada :

1. Seluruh dosen Prodi Informatika yang telah mendampingi selama perkuliahan
2. Bapak Luqman Hakim, S.Kom., M.Kom. selaku Dosen Pembimbing Tugas Akhir
3. Kedua Orang Tua tercinta dan keluarga yang selalu mendukung dan mendoakan penulis
4. Teman seperjuangan Jalal, Yusuf, Hadid, Rafi dan Moriz yang telah berjuang bersama selama perkuliahan
5. Teman-teman kelas G dan lainnya yang selalu membersamai penulis selama perkuliahan

Semoga segala kebaikan dan dukungan semuanya mendapat balasan dari Allah Subhanahu wa ta'ala, dan akhirnya penulis menyadari bahwa skripsi ini masih jauh dari kata sempurna, karena keterbatasan ilmu yang penulis miliki. Untuk itu penulis dengan kerendahan hati mengharapkan saran dan kritik yang sifatnya membangun dari semua pihak demi membangun laporan penelitian ini.

Malang, Desember 2023

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR PUSTAKA

[1] M. Aminullah and M. Ali, "Perkembangan Teknologi Komunikasi Era 4.0," *Komunike*, vol. Volume XII, pp. 1–23, 2020.

[2] J. Turnbull, *The Docker Book*. 2014.

[3] F. Hanifah, A. Budiyono, and A. Widjajarto, "Analisa Kerentanan Pada Vulnerable *Docker* Menggunakan Alienvault Dan *Docker* Bench For Security Dengan Acuan Framework CIS Control," *e-Proceeding Eng.*, vol. 8, no. 5, pp. 8879–8885, 2021, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/15914.

[4] Z. Jian and L. Chen, "A defense method against *docker* escape attack," *ACM Int. Conf. Proceeding Ser.*, pp. 142–146, 2017, doi: 10.1145/3058060.3058085.

[5] T. Astriani, "Analisa Kerentanan Pada Vulnerable *Docker* Menggunakan Scanner Openvas Dan *Docker* Scan Dengan Acuan Standar Nist 800-115," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 4, pp. 2041–2050, 2021, doi: 10.35957/jatisi.v8i4.1232.

[6] M. Fatkhurozzi, "Analisa Keamanan Website Menggunakan Metode Footprinting Dan Vulnerability Scanning Pada Website Kampus," *Pros. Semin. Nas. Inform. Bela Negara*, vol. 2, pp. 144–148, 2021, doi: 10.33005/santika.v2i0.74.

[7] Y. Mulyanto, H. Herfandi, and R. Candra Kirana, "ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus:RS H.LMANAMBAI ABDULKADIR)," *J. Inform. Teknol. dan Sains*, vol. 4, no. 1, pp. 26–35, 2022, doi: 10.51401/jinteks.v4i1.1528.

[8] G. Weidman, *Penetration testing A Hands-On Introduction to Hacking*. 2014.

[9] S. Kwon and J. H. Lee, "DIVDS: *Docker* Image Vulnerability Diagnostic System," *IEEE Access*, vol. 8, pp. 42666–42673, 2020, doi: 10.1109/ACCESS.2020.2976874.

[10] M. Khulaimi *et al.*, “Management Konfigurasi Hotspot Local Area Network (LAN) SMK Darussholihin NW Kalijaga Menggunakan Metode Vulnerability Scanning,” *Digit. Transform. Technol. | e*, vol. 3, no. 2, pp. 418–425, 2023, [Online]. Available: https://doi.org/10.47709/digitech.v3i2.2855.

[11] K. Paulina, “PENETRATION TESTING OPEN JOURNAL SYSTEMS (OJS) PADA APLIKASI WEB JURNAL JI-TECH,” vol. 1, no. 1, pp. 37–45, 2023.

[12] M. Hasibuan and A. M. Elhanafi, “Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box,” *sudo J. Tek. Inform.*, vol. 1, no. 4, pp. 171–177, 2022, doi: 10.56211/sudo.v1i4.160.

[13] G. Bussiness, “Apa itu Penetration Testing? Pengertian, Fungsi, dan Tahapannya,” *linknet*, 2023. https://www.linknet.id/article/penetration-testing.

[14] P. Saxena, “Container Image Security with Trivy and Istio Inter-Service Secure Communication in Kubernetes,” 2022.

[15] A. EFE, U. ASLAN, and A. M. KARA, “Securing Vulnerabilities in *Docker* Images,” *Int. J. Innov. Eng. Appl.*, vol. 4, no. 1, pp. 31–39, 2020, doi: 10.46460/ijiea.617181.

[16] P. R. Perkasa and E. Mailoa, “Adopsi Devsecops Untuk Mendukung Metode Agile Menggunakan Trivy Sebagai Security Scanner *Docker* Image Dan *Docker*file,” *J. Indones. Manaj. Inform. dan Komun.*, vol. 4, no. 3, pp. 856–863, 2023, doi: 10.35870/jimik.v4i3.291.

[17] D. C. Images, “Student Thesis Level : Bachelor *Docker* Container Images,” 2022.

[18] I. Chalvatzis, “Reproducible modelling and simulating security vulnerability scanners evaluation framework towards risk management assessment of small and medium enterprises business networks,” *Indian J. Sci. Technol.*, vol. 13, no. 37, pp. 3910–3943, 2020, doi: 10.17485/ijst/v13i37.868.

[19] M. A. Muin, K. Kapti, and T. Yusnanto, “Campus Website Security Vulnerability Analysis Using Nessus,” *Int. J. Comput. Inf. Syst.*, vol. 3, no.

2, pp. 79–82, 2022, doi: 10.29040/ijcis.v3i2.72.

[20] A. Mills, J. White, and P. Legg, “Longitudinal Risk-based Security Assessment of *Docker* Software Container Images,” *Comput. Secur.*, vol. 135, no. August, p. 103478, 2023, doi: 10.1016/j.cose.2023.103478.

[21] A. M. Dissanayaka, S. Mengel, L. Gittner, and H. Khan, “Security assurance of MongoDB in singularity LXCs: an elastic and convenient testbed using Linux containers to explore vulnerabilities,” *Cluster Comput.*, vol. 23, no. 3, pp. 1955–1971, 2020, doi: 10.1007/s10586-020-03154-7.

[22] Admin, “How to uninstall libcurl4-openssl-dev software package in Ubuntu.” https://www.thegeekdiary.com/how-to-uninstall-libcurl4-openssl-dev-software-package-in-ubuntu/.

[23] Wpscanteam, “What is a brute force attack?,” 2023. https://wpscan.com/blog/what-is-a-brute-force-attack/.

[24] Wpscanteam, “WPScan Brute Force,” 2021. https://wpscan.com/blog/wpscan-brute-force/.

UNIVERSITAS
MUHAMMADIYAH
MALANG

FAKULTAS TEKNIK

INFORMATIKA
informatika.umm.ac.id | informatika@umm.ac.id

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : **Abdurrahman Harish Al Mauqy**

NIM : **201910370311316**

Judul TA : **Analisa Kentanan pada *Vulnerable Docker* dengan metode *Vulnerability Scanning* dan *Penetration Testing* menggunakan *Opensource tools***

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	5 %
2.	Bab 2 – Daftar Pustaka	25 %	2 %
3.	Bab 3 – Analisis dan Perancangan	25 %	3 %
4.	Bab 4 – Implementasi dan Pengujian	15 %	6 %
5.	Bab 5 – Kesimpulan dan Saran	5 %	0 %
6.	Makalah Tugas Akhir	20%	15 %

Mengetahui,

Pemeriksa (Staff TU)

(NIP.....)