



DAFTAR ISI

LEMBAR PENGESAHAN	iii
PERNYATAAN KEASLIAN PENELITIAN	iv
KATA PENGANTAR	v
DAFTAR ISI.....	vii
DAFTAR GAMBAR.....	x
DAFTAR TABEL	xv
INTISARI.....	xvi
<i>ABSTRACT</i>	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA	8
2.1 Tinjauan Pustaka	8
2.2 Dasar Teori.....	13
2.2.1 Komputasi Awan.....	13
2.2.2 Kubernetes & Containerization.....	13
2.2.3 Container Runtime Security	14
2.2.4 System call	15
2.2.5 eBPF	16
2.2.6 Falco	17



2.2.7	<i>OWASP Cloud Native Application Security Top 10</i>	19
2.2.8	<i>Remote Code Execution</i>	21
2.2.9	<i>Privileged container</i>	22
2.2.10	<i>Exfiltration Using Common Linux Binaries</i>	22
2.2.11	<i>Mean Time to Detect (MTTD)</i>	23
2.3	Hipotesis.....	24
BAB III METODE PENELITIAN.....		26
3.1	Bahan.....	26
3.2	Peralatan.....	26
3.3	Tahapan Penelitian.....	26
3.4	Instalasi dan Konfigurasi.....	29
3.4.1	Konfigurasi Digital Ocean Kubernetes (DOKS).....	29
3.4.2	Instalasi dan Konfigurasi Digital Ocean Droplets.....	37
3.4.3	Instalasi dan Konfigurasi Falco.....	40
3.5	Skenario Serangan Pada Kubernetes.....	42
3.5.1	<i>Remote Code Execution</i>	46
3.5.2	<i>Exfiltration Using Common Linux Binaries</i>	50
3.5.3	<i>Deployment of Privileged Container</i>	54
3.6	Pengujian Performa <i>Rules</i>	58
3.6.1	<i>Remote Code Execution</i>	58
3.6.2	<i>Exfiltration using Common Linux Binaries</i>	73
3.6.3	<i>Deployment of Privileged Container</i>	87
3.7	Pengujian <i>Mean Time to Detect (MTTD)</i>	91
BAB IV HASIL DAN PEMBAHASAN.....		94
4.1	Pengujian Fungsionalitas Sistem.....	94
4.2	Pengujian Performa <i>Rule Falco</i>	95



4.2.1	Skenario <i>Remote Code Execution</i>	95
4.2.2	Skenario <i>Exfiltration Using Common Linux Binaries</i>	96
4.2.3	Skenario <i>Deployment of Privileged Container</i>	99
4.3	Pengujian <i>Mean Time to Detect (MTTD)</i>	100
4.3.1	Skenario <i>Remote Code Execution</i>	100
4.3.2	Skenario <i>Exfiltration Using Common Linux Binaries</i>	101
4.3.3	Skenario <i>Deployment of Privileged Container</i>	103
BAB V PENUTUP		105
5.1	Kesimpulan	105
5.2	Saran	105
DAFTAR PUSTAKA		107



DAFTAR GAMBAR

Gambar 2. 1 Kapabilitas Keamanan yang diperlukan di Kubernetes (Redhat, 2022)	15
Gambar 2. 2 Cara Kerja System Call (Shah, 2023)	16
Gambar 2. 3 Alat Opensource Teratas Dalam Kubernetes Security	18
Gambar 2. 4 Logo Falco	19
Gambar 2. 5 Rumus MTTD (Plutora, 2023b).....	24
Gambar 3. 1 Diagram Alir Penelitian.....	27
Gambar 3. 2 Topologi Jaringan Sistem	29
Gambar 3. 3 Log in Digital Ocean	30
Gambar 3. 4 Pembuatan Digital Ocean Kubernetes (DOKS).....	30
Gambar 3. 5 Lokasi Datacenter dan Versi Kubernetes	31
Gambar 3. 6 Spesifikasi Klaster Kubernetes	31
Gambar 3. 7 Finalisasi Deployment DOKS.....	32
Gambar 3. 8 Panduan Menghubungkan Perangkat Penulis dengan DOKS.....	32
Gambar 3. 9 Konfigurasi API untuk Kubernetes	33
Gambar 3. 10 Pembuatan Token Baru	34
Gambar 3. 11 Konfigurasi Token Baru	34
Gambar 3. 12 Hasil Token yang Baru Dibuat	35
Gambar 3. 13 Autentikasi doctl Menggunakan Akses Token	35
Gambar 3. 14 Berpindah ke Akun doctl Lain	35
Gambar 3. 15 Verifikasi Akun doctl yang Digunakan	36
Gambar 3. 16 Import Kubeconfig DOKS ke Perangkat Penulis.....	36
Gambar 3. 17 Verifikasi Koneksi Antara Perangkat Penulis dengan DOKS	36
Gambar 3. 18 Log In Akun Digital Ocean	37
Gambar 3. 19 Menu untuk Konfigurasi Droplets	37
Gambar 3. 20 Lokasi Data Center Droplets	38
Gambar 3. 21 Sistem Operasi dan Jenis CPU Droplets	38
Gambar 3. 22 Spesifikasi Droplets yang Akan Digunakan.....	39
Gambar 3. 23 Jenis Metode Autentikasi Untuk Mengakses Droplets.....	39
Gambar 3. 24 Jumlah Droplets yang Akan Dibuat	40
Gambar 3. 25 Droplets Telah Berhasil Dibuat	40



Gambar 3. 26 Verifikasi Deployment Droplets.....	40
Gambar 3. 27 Verifikasi Instalasi Helm	41
Gambar 3. 28 Pembuatan Namespace Untuk Falco.....	41
Gambar 3. 29 Verifikasi Deployment Falco.....	42
Gambar 3. 30 Diagram Alir Proses Tuning Rule	44
Gambar 3. 31 Topologi Serangan.....	46
Gambar 3. 32 Diagram YAML Rule RCE Sebelum Tuning	47
Gambar 3. 33 Rule RCE - Sebelum Tuning.....	48
Gambar 3. 34 Diagram YAML Rule RCE Setelah Tuning	49
Gambar 3. 35 Rule RCE - Setelah Tuning.....	50
Gambar 3. 36 Diagram YAML Rule Exfiltration Using Common Linux Binaries Sebelum Tuning.....	51
Gambar 3. 37 Rule Eksfiltrasi - Sebelum Tuning	52
Gambar 3. 38 Diagram YAML Rule Exfiltration Using Common Linux Binaries Setelah Tuning.....	53
Gambar 3. 39 Rule Eksfiltrasi - Setelah Tuning	54
Gambar 3. 40 Diagram YAML Rule Deployment of Privileged Container Sebelum Tuning	55
Gambar 3. 41 Rule Deployment Privileged Container - Sebelum Tuning.....	56
Gambar 3. 42 Diagram YAML Rule Deployment of Privileged Container Sebelum Tuning	57
Gambar 3. 43 Rule Deployment Privileged Container - Setelah Tuning.....	58
Gambar 3. 44 Diagram Alir Pengujian Performa Rule dari Skenario RCE.....	62
Gambar 3. 45 Membangun Listener Jaringan Pada VM Penyerang – Socat 1	62
Gambar 3. 46 Payload RCE Menggunakan Socat 1	63
Gambar 3. 47 Periksa Koneksi Remote Shell Pada VM Penyerang – Socat 1	63
Gambar 3. 48 Notifikasi Falco Menggunakan Rule Setelah Tuning – Socat 1	63
Gambar 3. 49 Membangun Listener Jaringan Pada VM Penyerang – Socat 2	63
Gambar 3. 50 Payload RCE Menggunakan Socat 2	64
Gambar 3. 51 Periksa Koneksi Remote Shell Pada VM Penyerang – Socat 2	64
Gambar 3. 52 Notifikasi Falco Menggunakan Rule Setelah Tuning – Socat 2	64
Gambar 3. 53 Membuat Listener Jaringan Pada VM Penyerang – Sqlite3 NC MKFIFO. 65	



Gambar 3. 54 Payload RCE Menggunakan Sqlite3 NC MKFIFO	65
Gambar 3. 55 Periksa Koneksi Remote Shell Pada VM Penyerang – Sqlite3 NC MKFIFO	65
Gambar 3. 56 Notifikasi Falco Menggunakan Rule Setelah Tuning – Sqlite3 NC MKFIFO	65
Gambar 3. 57 Membuat Listener Jaringan Pada VM Penyerang – NC MKFIFO	66
Gambar 3. 58 Payload RCE Menggunakan NC MKFIFO.....	66
Gambar 3. 59 Periksa Koneksi Remote Shell Pada VM Penyerang – NC MKFIFO	66
Gambar 3. 60 Notifikasi Falco Menggunakan Rule Setelah Tuning - NC MKFIFO	67
Gambar 3. 61 Membangun Listener Jaringan Pada VM Penyerang – PHP Shell Exec	67
Gambar 3. 62 Payload RCE Menggunakan PHP Shell Exec	67
Gambar 3. 63 Periksa Koneksi Remote Shell Pada VM Penyerang – PHP Shell Exec.....	67
Gambar 3. 64 Notifikasi Falco Menggunakan Rule Sebelum Tuning – PHP Shell Exec..	68
Gambar 3. 65 Notifikasi Falco Menggunakan Rule Setelah Tuning – PHP Shell Exec	68
Gambar 3. 66 Membangun Listener Jaringan Pada VM Penyerang – Telnet	68
Gambar 3. 67 Payload RCE Menggunakan Telnet	68
Gambar 3. 68 Periksa Koneksi Remote Shell Pada VM Penyerang - Telnet.....	68
Gambar 3. 69 Notifikasi Falco Menggunakan Rule Setelah Tuning - Telnet	69
Gambar 3. 70 Membangun Listener Jaringan Pada VM Penyerang – Python.....	69
Gambar 3. 71 Payload RCE Menggunakan Python	69
Gambar 3. 72 Periksa Koneksi Remote Shell Pada VM Penyerang - Python	70
Gambar 3. 73 Notifikasi Falco Menggunakan Rule Sebelum Tuning - Python	70
Gambar 3. 74 Notifikasi Falco Menggunakan Rule Setelah Tuning - Python.....	70
Gambar 3. 75 Membangun Listener Jaringan Pada VM Penyerang – Ruby	70
Gambar 3. 76 Payload RCE Menggunakan Ruby.....	71
Gambar 3. 77 Periksa Koneksi Remote Shell Pada VM Penyerang - Ruby	71
Gambar 3. 78 Notifikasi Falco Menggunakan Rule Sebelum Tuning - Ruby	71
Gambar 3. 79 Notifikasi Falco Menggunakan Rule Setelah Tuning - Ruby	71
Gambar 3. 80 Membangun Listener Jaringan Pada VM Penyerang – ZSH	72
Gambar 3. 81 Payload RCE Menggunakan ZSH.....	72
Gambar 3. 82 Periksa Koneksi Remote Shell Pada VM Penyerang - ZSH	72
Gambar 3. 83 Notifikasi Falco Menggunakan Rule Sebelum Tuning - ZSH	72



Gambar 3. 84	Notifikasi Falco Menggunakan Rule Setelah Tuning - ZSH	72
Gambar 3. 85	Diagram Alir Pengujian Performa Rule dari Skenario Eksfiltrasi	76
Gambar 3. 86	Membangun Listener Jaringan Pada VM Penyerang – Wget	76
Gambar 3. 87	Payload Eksfiltrasi Menggunakan Wget	76
Gambar 3. 88	Hasil Eksfiltrasi menggunakan Wget	77
Gambar 3. 89	Notifikasi Falco Menggunakan Rule Sebelum Tuning - Wget	77
Gambar 3. 90	Membangun Listener Jaringan Pada VM Penyerang – Whois.....	78
Gambar 3. 91	Payload Eksfiltrasi Menggunakan Whois	78
Gambar 3. 92	Hasil Eksfiltrasi menggunakan Whois	78
Gambar 3. 93	Notifikasi Falco Menggunakan Rule Setelah Tuning – Whois.....	78
Gambar 3. 94	Membangun Listener Jaringan Pada VM Penyerang – Bash.....	79
Gambar 3. 95	Payload Eksfiltrasi Menggunakan Bash.....	79
Gambar 3. 96	Hasil Eksfiltrasi menggunakan Bash	79
Gambar 3. 97	Notifikasi Falco Menggunakan Rule Setelah Tuning - Bash	80
Gambar 3. 98	Hasil Eksfiltrasi menggunakan Openssl.....	80
Gambar 3. 99	Payload Eksfiltrasi Menggunakan Openssl.....	81
Gambar 3. 100	Hasil Eksfiltrasi menggunakan Openssl.....	81
Gambar 3. 101	Notifikasi Falco Menggunakan Rule Setelah Tuning - Openssl.....	81
Gambar 3. 102	Membangun Listener Jaringan Pada VM Penyerang – Curl.....	82
Gambar 3. 103	Payload Eksfiltrasi Menggunakan Curl	82
Gambar 3. 104	Hasil Eksfiltrasi menggunakan Curl	82
Gambar 3. 105	Notifikasi Falco Menggunakan Rule Setelah Tuning - Curl.....	82
Gambar 3. 106	Membangun Listener Jaringan Pada VM Penyerang – KSH.....	83
Gambar 3. 107	Payload Eksfiltrasi Menggunakan KSH.....	83
Gambar 3. 108	Hasil Eksfiltrasi menggunakan ZSH.....	83
Gambar 3. 109	Notifikasi Falco Menggunakan Rule Setelah Tuning – KSH	84
Gambar 3. 110	Payload Eksfiltrasi Menggunakan Rsync.....	84
Gambar 3. 111	Hasil Eksfiltrasi menggunakan Rsync.....	84
Gambar 3. 112	Notifikasi Falco Menggunakan Rule Sebelum Tuning – Rsync	85
Gambar 3. 113	Notifikasi Falco Menggunakan Rule Setelah Tuning – Rsync.....	85
Gambar 3. 114	Payload Eksfiltrasi Menggunakan KSH.....	85
Gambar 3. 115	Hasil Eksfiltrasi menggunakan ZSH	85



Gambar 3. 116 Notifikasi Falco Menggunakan Rule Setelah Tuning – KSH.....	86
Gambar 3. 117 Notifikasi Falco Menggunakan Rule Setelah Tuning – KSH.....	86
Gambar 3. 118 Payload Eksfiltrasi Menggunakan SFTP.....	86
Gambar 3. 119 Hasil Eksfiltrasi menggunakan SFTP.....	87
Gambar 3. 120 Notifikasi Falco Menggunakan Rule Setelah Tuning – SFTP	87
Gambar 3. 121 Notifikasi Falco Menggunakan Rule Setelah Tuning – SFTP	87
Gambar 3. 122 Diagram Alir Pengujian Performa Rule dari Skenario Privileged container	89
Gambar 3. 123 Notifikasi Falco Sebelum Tuning – Privileged container Menggunakan Manifest file.....	90
Gambar 3. 124 Notifikasi Falco Setelah Tuning – Privileged container Menggunakan Manifest file.....	90
Gambar 3. 125 Notifikasi Falco Sebelum Tuning – Privileged container Menggunakan CMD	90
Gambar 3. 126 Notifikasi Falco Setelah Tuning – Privileged container Menggunakan CMD	90
Gambar 3. 127 Notifikasi Falco Sebelum Tuning – Developer Privileged container.....	91
Gambar 3. 128 Notifikasi Falco Setelah Tuning – Developer Privileged container.....	91
Gambar 3. 129 Format Informasi Waktu Ketika Payload Dijalankan Pada VM Penyerang	92
Gambar 3. 130 Contoh Payload untuk MTTD.....	92
Gambar 3. 131 Informasi Waktu Pada VM Penyerang.....	92
Gambar 3. 132 Informasi Waktu Pada Log Falco	92
Gambar 3. 133 Diagram Alir Pengujian MTTD	93
Gambar 4. 1 Hasil Pengujian Fungsionalitas Falco	94
Gambar 4. 2 Grafik Komparasi Performa Rule Sebelum dan Setelah Tuning - RCE	96
Gambar 4. 3 Grafik Komparasi Performa Rule Sebelum dan Setelah Tuning - Eksfiltrasi	98
Gambar 4. 4 Grafik Komparasi Performa Rule Sebelum dan Setelah Tuning – Privileged Container	99



DAFTAR TABEL

Tabel 2. 1 Ringkasan Jurnal Penelitian	10
Tabel 3. 1 Spesifikasi Aset	26
Tabel 4. 1 Hasil Pengujian Performa Rule - RCE.....	95
Tabel 4. 2 Hasil Pengujian Performa Rule - Eksfiltrasi	97
Tabel 4. 3 Hasil Pengujian Performa Rule - Privileged container	99
Tabel 4. 4 Hasil Pengujian MTTD - RCE	100
Tabel 4. 5 Hasil Pengujian MTTD - Eksfiltrasi	102
Tabel 4. 6 Hasil Pengujian MTTD - Privileged container	103