Digital Transformation Technology (Digitech) | e-ISSN: 2807-9000
Volume 6, **Number** 2, September 2026
https://doi.org/10.47709/digitech.v6i2.9328

Deteksi dan Mitigasi Bruteforce SMB pada Jaringan Workgroup dengan Fitur Bawaan Windows

Jose Mario Hendra[1]
[1]Institut Teknologi & Bisnis Sabda Setia, Indonesia
[1]jose.mariohendra@itbss.ac.id

open access
Histori Artikel:
Diajukan: 21 Juli 2026
Disetujui: 20 Oktober 2026
Dipublikasi: 28 Oktober 2028

Kata Kunci:
bruteforce SMB; Account Lockout Policy; Advanced Audit Policy; Windows Event Forwarding; Digital Forensic Readiness

Digital Transformation Technology (Digitech) *is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).*

Abstrak
Jaringan berskala kecil bertipe workgroup, seperti yang umum ditemui pada Usaha Mikro, Kecil dan Menengah (UMKM) serta laboratorium kampus, memiliki tingkat kematangan keamanan siber yang rendah sekaligus rentan terhadap serangan bruteforce pada protokol Server Message Block (SMB), tanpa dukungan Active Directory maupun Security Information and Event Management (SIEM) untuk memusatkan visibilitas log. Ketiadaan pemantauan terpusat menyebabkan deteksi serangan menjadi lambat dan jejak forensik mudah hilang begitu penyerang menguasai satu endpoint. Penelitian ini bertujuan menguji efektivitas kombinasi Account Lockout Policy (ALP), Advanced Audit Policy (AAP), dan Windows Event Forwarding (WEF) sebagai mekanisme native Windows untuk mendeteksi, memitigasi, dan mempertahankan integritas bukti serangan bruteforce SMB pada jaringan workgroup. Penelitian menggunakan pendekatan eksperimental kuantitatif pada lima mesin virtual dalam satu subnet, melalui enam skenario pengujian: baseline dan mitigasi bruteforce, sentralisasi log pada kondisi normal dan di bawah beban serangan, serta verifikasi integritas log sebelum dan sesudah kompromi. Hasil pengujian menunjukkan bahwa ALP menghentikan serangan pada percobaan ke-5 sehingga kredensial (posisi ke-28 pada wordlist) tidak ditemukan, AAP tetap merekam upaya akses pada akun yang terkunci, WEF mensentralisasi log Security dengan Event ID dan timestamp yang identik antara sumber dan collector pada resolusi detik, serta seluruh 797 event percobaan gagal tetap utuh pada collector meskipun log lokal VM sumber dihapus penyerang. Temuan ini menunjukkan bahwa kesiapan forensik digital yang utuh dapat dibangun sepenuhnya dari fitur bawaan Windows tanpa biaya lisensi tambahan, menjadikannya solusi realistis bagi organisasi berskala kecil.

PENDAHULUAN

Badan Siber dan Sandi Negara (2024) mencatat sebanyak 330.527.636 anomali trafik siber di Indonesia sepanjang tahun 2024, dengan jenis anomali tertinggi berupa aktivitas Mirai Botnet yang mencapai 81.286.596 kejadian, angka yang mencerminkan besarnya skala ancaman siber yang dihadapi Indonesia seiring pesatnya transformasi digital. Di samping ancaman yang bersifat masif tersebut, terdapat pula celah keamanan yang lebih spesifik dan bersifat teknis yang kerap dimanfaatkan penyerang, salah satunya protokol Server Message Block (SMB), yaitu fitur Windows yang digunakan untuk berbagi file antarkomputer dan kerap dijadikan jalur pergerakan lateral di dalam jaringan (Badan Siber dan Sandi Negara, 2024).

Kerentanan pada protokol SMB tersebut menjadi lebih signifikan ketika terjadi pada jaringan berskala kecil bertipe workgroup, yaitu arsitektur tanpa Active Directory yang umum dijumpai pada Usaha Mikro, Kecil dan Menengah (UMKM) maupun laboratorium kampus. Indonesia memiliki lebih dari 65 juta unit UMKM yang menyumbang 60,5% Produk Domestik Bruto nasional (Ajhari dkk., 2023), namun tingkat kematangan keamanan siber pelaku UMKM secara umum masih rendah. Hasil pengukuran Badan Siber dan Sandi Negara terhadap 964 UMKM di sembilan wilayah Indonesia sepanjang 2020–2022 menunjukkan bahwa hasil penilaian tiga tahun berturut-turut didominasi oleh kategori "Buruk" dan "Kurang" (Ajhari dkk., 2023). Karakteristik jaringan workgroup di UMKM maupun laboratorium kampus umumnya tidak memiliki server terpusat, kebijakan audit baku, maupun staf IT khusus, berbeda signifikan dari jaringan enterprise yang telah menerapkan Active Directory beserta mekanisme monitoring terintegrasi.

Ketiadaan Active Directory pada jaringan workgroup turut membawa konsekuensi pada sisi visibilitas keamanan. Setiap komputer menyimpan log aktivitasnya masing-masing secara mandiri, tanpa adanya pusat pemantauan yang terintegrasi. Kondisi ini menimbulkan dua kendala operasional utama: pertama, deteksi serangan menjadi lambat karena administrator harus memeriksa log secara manual pada setiap perangkat satu per satu;

kedua, integritas forensik menjadi rentan, sebab begitu penyerang berhasil menguasai satu komputer, log lokal pada perangkat tersebut dapat dengan mudah dihapus sehingga jejak serangan pun lenyap. Dengan demikian, jaringan yang justru memiliki kesiapan keamanan paling rendah adalah jaringan yang paling sulit melakukan deteksi dini maupun investigasi forensik ketika serangan bruteforce SMB terjadi.

Sejumlah penelitian terdahulu telah mengangkat isu audit keamanan dan sentralisasi log, namun belum ada yang secara khusus menjawab kebutuhan jaringan workgroup tanpa Active Directory seperti pada UMKM. Armansyah dkk. (2023) mengusulkan sentralisasi penyimpanan data melalui penerapan Active Directory dan pengaturan privileges pada jaringan sekolah, tetapi solusi tersebut secara inheren mensyaratkan infrastruktur AD yang justru menjadi hambatan biaya dan kompetensi teknis bagi UMKM maupun laboratorium kampus berskala kecil. Sajan dkk. (2025) mengkaji relevansi forensik lima jenis Windows event log, termasuk Forwarded Event Log yang dihasilkan oleh mekanisme WEF, dan menekankan pentingnya sentralisasi log bagi kesiapan forensik organisasi, namun kajian tersebut bersifat konseptual dan solusi praktis yang dirujuk mengandalkan integrasi dengan platform SIEM komersial seperti Splunk dan IBM QRadar, tanpa pengujian empiris terhadap efektivitas WEF sebagai mekanisme sentralisasi log mandiri dalam skenario serangan nyata. Sementara itu, Mahardika dkk. (2026) menguji efektivitas Account Lockout Policy dalam membatasi serangan bruteforce Hydra terhadap layanan SMB, dengan hasil validasi pada Windows 7 yang berhasil menghentikan serangan hanya dalam 6 percobaan, meski ditemukan keterbatasan konfigurasi pada Windows 10 Home yang tidak menyediakan Group Policy Editor; namun pengujian tersebut dilakukan pada masing-masing mesin target secara terisolasi, tanpa mekanisme forwarding atau korelasi log lintas-perangkat. Ketiga penelitian tersebut menyisakan gap yang konsisten: belum tersedia penelitian yang menguji kombinasi Advanced Audit Policy, Account Lockout Policy, dan Windows Event Forwarding secara terintegrasi sebagai mekanisme deteksi dan mitigasi bruteforce SMB pada jaringan workgroup tanpa SIEM maupun Active Directory.

Berdasarkan kesenjangan tersebut, penelitian ini dirancang untuk menguji sejauh mana kombinasi ketiga mekanisme native Windows tersebut mampu mendeteksi dan memitigasi serangan bruteforce SMB, sekaligus mempertahankan integritas jejak forensik pada jaringan workgroup, tanpa bergantung pada Active Directory maupun SIEM berbayar. Rumusan masalah penelitian ini adalah: (1) sejauh mana efektivitas Advanced Audit Policy dan Account Lockout Policy dalam mendeteksi dan membatasi serangan bruteforce SMB pada jaringan workgroup; (2) sejauh mana Windows Event Forwarding mampu mensentralisasi log Security dari beberapa endpoint tanpa Active Directory, termasuk kesesuaian timestamp antara log sumber dan log terpusat; dan (3) sejauh mana korelasi Event ID pada log terpusat (Forwarded Events) mampu mempertahankan integritas jejak forensik meskipun endpoint sumbernya telah dikuasai penyerang.

Berdasarkan rumusan masalah tersebut, penelitian ini bertujuan untuk menganalisis efektivitas Account Lockout Policy dalam membatasi jumlah percobaan login pada serangan bruteforce SMB serta kemampuan Advanced Audit Policy dalam merekam jejak percobaan tersebut; mengevaluasi kemampuan Windows Event Forwarding dalam mensentralisasi log Security dari beberapa endpoint tanpa Active Directory, termasuk memeriksa kesesuaian timestamp antara log sumber dan log terpusat; dan menilai sejauh mana korelasi Event ID pada log terpusat mampu mempertahankan integritas jejak forensik meskipun endpoint sumbernya telah dikuasai penyerang. Bagi UMKM dan laboratorium kampus, hasil penelitian ini diharapkan dapat menjadi acuan dalam membangun deteksi serangan sekaligus menjaga keandalan bukti investigasi, tanpa perlu investasi tambahan untuk SIEM maupun Active Directory.

STUDI LITERATUR

Bruteforce SMB, Audit Policy, dan Account Lockout

Server Message Block (SMB) merupakan protokol jaringan yang digunakan untuk berbagi berkas, printer, dan sumber daya lainnya pada lingkungan Windows, beroperasi melalui port TCP 445 secara default sehingga kerap menjadi permukaan serangan yang signifikan, terutama melalui teknik brute force, yaitu upaya menebak kredensial secara sistematis dan berulang hingga ditemukan kombinasi yang valid.

Mahardika dkk. (2026) melakukan pengujian penetrasi terhadap layanan SMB pada Windows 7 dan Windows 10 menggunakan tool Hydra dengan wordlist rockyou.txt, dan berhasil menemukan kredensial pada kedua target dalam ribuan percobaan; mitigasi melalui Account Lockout Policy bawaan Windows menekan jumlah percobaan login dari ribuan menjadi hanya enam kali sebelum akun terkunci otomatis. Sementara itu, Fachri (2023) yang menguji kerentanan brute force pada web server institusi pendidikan menemukan bahwa port yang masih terbuka memungkinkan serangan serupa, namun mitigasinya bertumpu pada Fail2ban di Linux, bukan mekanisme native sistem operasi target.

Kesenjangan ini menunjukkan bahwa mitigasi brute force pada SMB berbasis Windows masih terbatas pada Account Lockout Policy secara parsial, tanpa integrasi dengan pencatatan seperti Advanced Audit Policy, sehingga penelitian ini mengeksplorasi keduanya secara terintegrasi tanpa tools pihak ketiga.

Selain kebijakan penguncian akun, Windows Server menyediakan mekanisme Advanced Audit Policy Configuration yang memungkinkan administrator mencatat aktivitas keamanan secara lebih granular

dibandingkan basic audit policy bawaan, mencakup kategori seperti Logon/Logoff, Account Management, hingga Object Access (Microsoft, 2026). Hal ini sejalan dengan temuan Rahman dkk. (2026), yang membangun sistem monitoring log terintegrasi menggunakan Wazuh SIEM dan Elastic Stack dan berhasil mengidentifikasi 59 dari 62 simulasi serangan dengan akurasi 95,2% dan latensi rata-rata 3,5 detik, jauh melampaui pemantauan manual yang hanya mencapai 60–70%. Meskipun mengandalkan SIEM eksternal, prinsipnya tetap relevan: efektivitas deteksi sangat bergantung pada kualitas dan granularitas audit log di sumbernya, sehingga perlu dikaji sejauh mana native Windows Event Log melalui Advanced Audit Policy, tanpa SIEM tambahan, memberikan visibilitas yang memadai pada skala jaringan UMKM.

Account Lockout Policy merupakan mekanisme keamanan bawaan Windows yang membatasi jumlah percobaan autentikasi gagal sebelum akun dikunci sementara, dikonfigurasi melalui tiga parameter utama: account lockout threshold, account lockout duration, dan reset account lockout counter after (Center for Internet Security [CIS], 2025). Efektivitas kebijakan ini didukung oleh temuan empiris Mahardika dkk. (2026): sebelum diterapkan, Hydra berhasil menemukan kredensial pada Windows 7 dalam sekitar 1.384 percobaan tanpa hambatan, namun setelah threshold dikonfigurasi sebesar 5 percobaan dengan durasi lockout 30 menit, serangan hanya mampu melakukan 6 percobaan sebelum akun terkunci otomatis. Ditemukan pula keterbatasan bahwa pada Windows 10 Home, konfigurasi melalui Group Policy Editor tidak tersedia karena fitur ini eksklusif untuk edisi Pro, Enterprise, dan Education, sehingga mitigasi harus dilakukan melalui command line (net accounts), menunjukkan bahwa cakupan proteksi Account Lockout Policy pada lingkungan non-domain sangat bergantung pada edisi sistem operasi yang digunakan.

Workgroup, Windows Event Forwarding, dan Kondisi UMKM

Untuk mengatasi keterbatasan visibilitas log yang tersebar pada masing-masing komputer secara individual, Windows menyediakan mekanisme native bernama Windows Event Forwarding (WEF), yaitu kemampuan bawaan yang memungkinkan penerusan log peristiwa dari berbagai host dalam jaringan menuju satu server pengumpul log (Windows Event Collector) tanpa memerlukan perangkat lunak pihak ketiga (Australian Signals Directorate, 2021). WEF bekerja melalui dua peran utama: source computers yang mengirimkan log peristiwa, dan collector server yang menerima serta menyimpan log tersebut secara terpusat (Microsoft, 2025). Pada lingkungan berbasis domain, Taberima dan Ramayanti (2024) mendokumentasikan konfigurasi partisi log terpisah dan kebijakan audit granular pada server Active Directory untuk memantau aktivitas mencurigakan di seluruh server dan workstation melalui Event Viewer, menunjukkan bahwa sentralisasi audit log dapat dicapai secara efektif ketika infrastruktur domain sudah tersedia, kondisi yang tidak selalu berlaku pada jaringan skala UMKM yang masih beroperasi dalam model workgroup. Pendekatan berbasis SIEM eksternal maupun domain AD DS bergantung pada infrastruktur tambahan, sedangkan WEF menawarkan jalur ketiga: sentralisasi log native tanpa agen tambahan maupun biaya lisensi, sehingga berpotensi sesuai bagi UMKM dengan sumber daya TI terbatas.

Kerangka Teori

Digital Forensic Readiness (DFR) merupakan serangkaian langkah proaktif agar bukti digital tidak terubah, tidak tersedia, atau hilang ketika insiden terjadi (Tan, 2001, sebagaimana dikutip dalam Daubner dkk., 2023). Secara tradisional DFR lebih berfokus pada proses organisasi, dengan salah satu tugas utama mengidentifikasi bukti potensial serta menilai nilai pembuktiannya (Rowlingson, 2004, sebagaimana dikutip dalam Daubner dkk., 2023). Bukti potensial juga dapat disimpan pada aset yang berbeda dari sumber pembuatnya, misalnya melalui remote logging (Daubner dkk., 2023), prinsip yang menjadi fondasi utama penelitian ini.

Sebagai pembanding, NIST Cybersecurity Framework (CSF) 2.0 terdiri atas enam fungsi inti: Govern, Identify, Protect, Detect, Respond, dan Recover (National Institute of Standards and Technology, 2024). Fungsi Detect mendefinisikan deteksi dini kejadian keamanan siber, namun cakupannya strategis dan berorientasi tata kelola risiko organisasi, sehingga kurang memberikan panduan teknis terhadap mekanisme spesifik seperti audit trail granular atau penjagaan integritas log lintas-endpoint. DFR, sebaliknya, berfokus pada kesiapan pengumpulan dan preservasi bukti digital pada level yang lebih dekat ke teknis-operasional, sehingga lebih relevan sebagai lensa teori penelitian ini.

Relevansi DFR terhadap Windows event log telah disinggung oleh Sajan dkk. (2025), yang menegaskan bahwa sentralisasi log, termasuk Forwarded Event Log hasil WEF, penting bagi kesiapan forensik organisasi, meski kajiannya bersifat konseptual. Pada organisasi kecil-menengah, Vaseghipanah dkk. (2025) mengembangkan model peningkatan DFR berbasis game theory untuk UMKM dengan mengintegrasikan MITRE ATT&CK dan D3FEND, dan menunjukkan bahwa peningkatan logging dan preservasi forensik secara signifikan menekan keberhasilan taktik penyerang.

Penelitian ini menggunakan DFR sebagai kerangka teori dengan memetakan konsep forensic readiness (Daubner dkk., 2023) ke tiga tujuan penelitian. Konsep sumber bukti (evidence source) diwujudkan melalui pengujian Account Lockout Policy dan Advanced Audit Policy sebagai mekanisme deteksi sekaligus perekam jejak percobaan bruteforce SMB (tujuan pertama). Konsep penyimpanan bukti pada aset terpisah (evidence

storage) diwujudkan melalui evaluasi Windows Event Forwarding sebagai mekanisme sentralisasi log Security tanpa Active Directory, termasuk pemeriksaan kesesuaian timestamp log (tujuan kedua). Adapun ketersediaan bukti pasca-kompromi diwujudkan melalui penilaian korelasi Event ID pada log terpusat, untuk menguji sejauh mana jejak forensik tetap dapat dipertahankan meskipun endpoint sumbernya telah dikuasai penyerang (tujuan ketiga).

METODE

Jenis Penelitian

Penelitian ini menggunakan pendekatan eksperimental kuantitatif pada lingkungan virtual yang terisolasi, dengan setiap skenario dijalankan satu kali. Perlakuan berupa simulasi serangan bruteforce terhadap layanan SMB, dan efektivitas Account Lockout Policy (ALP), Advanced Audit Policy (AAP), serta WEF diukur melalui tiga indikator: jumlah percobaan login hingga akun terkunci, kesesuaian Event ID dan timestamp antara log sumber dan log terpusat sebagai indikator latensi forwarding, serta jumlah Event ID 4625 pada log lokal dan log terpusat sebelum dan sesudah penghapusan log.

Lingkungan dan Alat Penelitian

Pengujian dilakukan pada Oracle VirtualBox dengan lima mesin virtual (VM) dalam satu subnet 192.168.10.0/24 tanpa segmentasi, untuk merepresentasikan jaringan workgroup pada UMKM dan laboratorium kampus (Tabel 1). Serangan dijalankan dari VM5 menggunakan wordlist rockyou.txt. Hydra v9.6 gagal terhubung ke layanan SMB Windows 11 (galat invalid reply from target), yang mengindikasikan ketidaksesuaian dengan kebijakan SMB Windows 11 yang lebih ketat dibandingkan Windows 7/10 pada penelitian Mahardika dkk. (2026); serangan karenanya dijalankan dengan NetExec. Nmap digunakan untuk memverifikasi bahwa port 445/tcp pada VM1 dan VM4 berstatus terbuka. File and printer sharing diaktifkan pada VM target dengan password protected sharing tetap aktif, sehingga akses memerlukan kredensial akun lokal yang valid.

Tabel 1. Peran dan Alokasi IP Mesin Virtual dalam Lingkungan Penelitian

VM	Peran	Sistem Operasi	IP Address
VM1	File Server (Target Serangan 1 – Terproteksi)	Windows 11 Home	192.168.10.10
VM2	Legitimate Access (baseline traffic normal)	Windows 11 Home	192.168.10.20
VM3	WEF Collector	Windows 11 Home	192.168.10.30
VM4	Target Serangan 2 – Terkompromi	Windows 11 Home	192.168.10.40
VM5	Attacker	Kali Linux	192.168.10.50

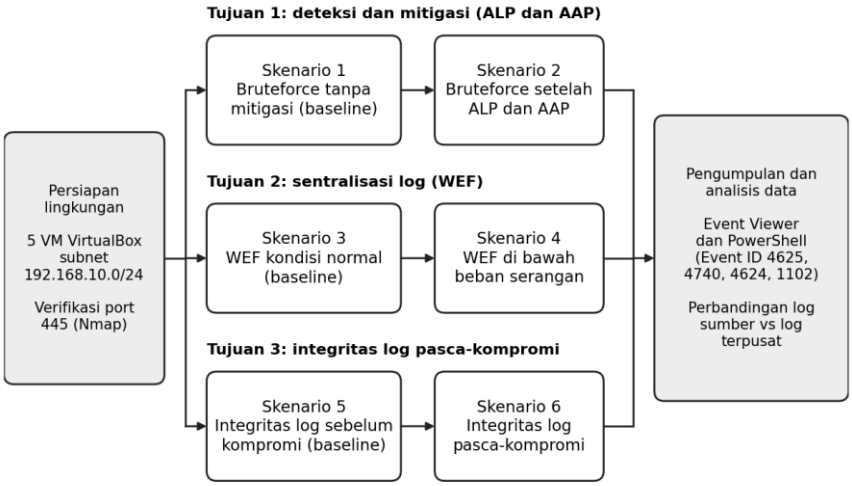
Tahapan dan Skenario Penelitian

Penelitian terdiri atas persiapan lingkungan, enam skenario pengujian, dan analisis data (Gambar 1). Skenario 1 dan 2 menjawab tujuan pertama (deteksi dan mitigasi bruteforce oleh ALP dan AAP), Skenario 3 dan 4 menjawab tujuan kedua (sentralisasi log oleh WEF), dan Skenario 5 dan 6 menjawab tujuan ketiga (integritas log pasca-kompromi). Pada setiap tujuan, skenario pertama berperan sebagai baseline bagi skenario kedua. Data dikumpulkan melalui Event Viewer dan PowerShell, kemudian dianalisis dengan membandingkan jumlah percobaan, kesesuaian Event ID dan timestamp, serta jumlah event pada log sumber dan log terpusat. Rincian tiap skenario disajikan pada Tabel 2.

Tabel 2. Rincian Skenario Pengujian

No	Skenario	Perlakuan	Indikator pengukuran
1	Bruteforce tanpa mitigasi (baseline)	Target VM1; ALP nonaktif (threshold 0); log Security dibersihkan	Jumlah Event ID 4625 hingga kredensial ditemukan
2	Bruteforce setelah ALP dan AAP	Target VM1; ALP threshold 5, durasi lockout 30 menit; AAP pada Logon dan Account Lockout; serangan identik dengan Skenario 1	Jumlah Event ID 4625 sebelum 4740; status akun; pencatatan percobaan setelah lockout

3	Sentralisasi log WEF, kondisi normal	Sumber VM1 dan VM2, collector VM3 (subscription WEF_VM1 dan WEF_VM2)	Kesesuaian Event ID dan timestamp antara log sumber dan Forwarded Events
4	Sentralisasi log WEF di bawah beban serangan	VM1 diserang (ALP nonaktif sementara) sementara VM2 melakukan satu logon normal	Kelengkapan event VM1 dan timestamp event VM2 pada VM3
5	Integritas log sebelum kompromi	Sumber VM4, collector VM3 (WEF_VM4); bruteforce dari VM5 hingga kredensial ditemukan	Jumlah Event ID 4625 log lokal VM4 vs Forwarded Events VM3 (acuan 797)
6	Integritas log pasca-kompromi	Penghapusan log Security VM4 secara remote (atexec)	Jumlah Event ID 4625 dan 1102 pada log lokal vs Forwarded Events



Gambar 1. Alur Tahapan Penelitian

Konfigurasi ALP, AAP, dan Perintah Serangan (Skenario 1 dan 2)

Pada Skenario 1, ALP dinonaktifkan (lockout threshold 0), akun vm1 diaktifkan, dan log Security dibersihkan agar data murni berasal dari eksperimen. Pada Skenario 2, ALP diatur dengan threshold 5 percobaan serta durasi lockout dan observation window masing-masing 30 menit, sedangkan AAP diaktifkan pada subkategori Logon dan Account Lockout untuk mencatat keberhasilan dan kegagalan:

```
net accounts /lockoutthreshold:5 /lockoutduration:30 /lockoutwindow:30
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Account Lockout" /success:enable /failure:enable
wevtutil cl Security
```

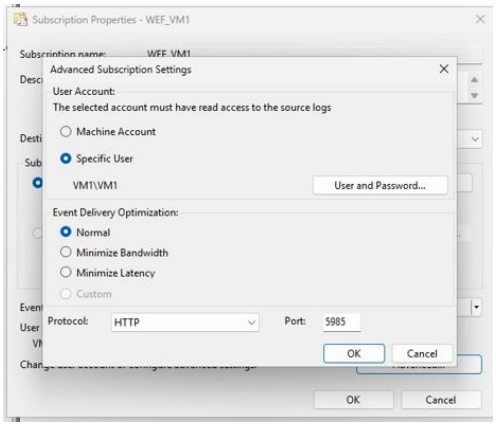
Kedua skenario menggunakan perintah serangan dan wordlist yang identik agar hasilnya dapat dibandingkan. Opsi --ignore-pw-decoding mengatasi galat decoding karakter non-UTF-8 pada rockyou.txt, dan --timeout 10 membatasi waktu tunggu tiap koneksi:

```
netexec smb 192.168.10.10 -u vm1 -p /usr/share/wordlists/rockyou.txt --ignore-pw-
decoding --timeout 10
```

Konfigurasi WEF (Skenario 3 dan 4)

Karena lingkungan tidak memiliki Active Directory, subscription WEF dibuat bertipe Collector Initiated dengan autentikasi Specific User (kredensial lokal) sebagai pengganti Kerberos, dan WinRM dikonfigurasi dengan Basic Authentication pada VM1, VM2, dan VM3. Pada VM3 dibuat satu subscription per sumber dengan query filter log Security (Audit Success dan Audit Failure), optimasi pengiriman Normal, dan protokol HTTP port 5985 (Gambar 2). Verifikasi dilakukan dengan membandingkan log Security sumber dan Forwarded Events pada VM3 untuk Event ID 4624, 4625, 4634, 4648, dan 4672 (Microsoft, 2024). Pada Skenario 4, serangan dijalankan

dengan perintah yang sama sementara satu logon normal dilakukan secara manual pada VM2.



Gambar 2. Advanced Subscription Settings pada subscription WEF_VM1 (autentikasi Specific User, optimasi pengiriman Normal, protokol HTTP port 5985)

Pengujian Integritas Log (Skenario 5 dan 6)

Pada Skenario 5, log Security VM4 dibersihkan, subscription WEF_VM4 dibuat dengan skema yang sama, lalu serangan dijalankan dari VM5 ke VM4 (username vm4) hingga kredensial ditemukan. Posisi kata sandi pada wordlist diverifikasi dengan grep -n; password2 berada pada baris ke-798, sehingga acuan jumlah percobaan gagal adalah 797. Jumlah Event ID 4625 pada VM4 dan VM3 dihitung menggunakan PowerShell (Get-WinEvent). Pada Skenario 6, dengan kredensial tersebut, penghapusan log Security VM4 dijalankan secara remote melalui metode atexec (Windows Task Scheduler), kemudian jumlah Event ID 4625 dan 1102 pada log lokal VM4 dan Forwarded Events VM3 dibandingkan:

```
netexec smb 192.168.10.40 -u vm4 -p 'password2' -x "wevtutil cl Security" --exec-method atexec
```

HASIL

Bagian ini menyajikan hasil pengujian terhadap enam skenario eksperimen yang telah dilaksanakan sebagaimana diuraikan pada bagian Metode, mencakup efektivitas Account Lockout Policy (ALP) dan Advanced Audit Policy (AAP) dalam memitigasi dan mendeteksi serangan bruteforce SMB (Skenario 1 dan 2), efektivitas Windows Event Forwarding (WEF) dalam mensentralisasi log Security pada jaringan workgroup tanpa Active Directory (Skenario 3 dan 4), serta integritas log pasca-kompromi sebagai wujud pelestarian bukti digital (Skenario 5 dan 6). Ringkasan hasil seluruh skenario disajikan pada Tabel 3, sedangkan satu bukti utama untuk tiap skenario ditampilkan pada Gambar 3 sampai Gambar 8.

Tabel 3. Ringkasan Hasil Keenam Skenario

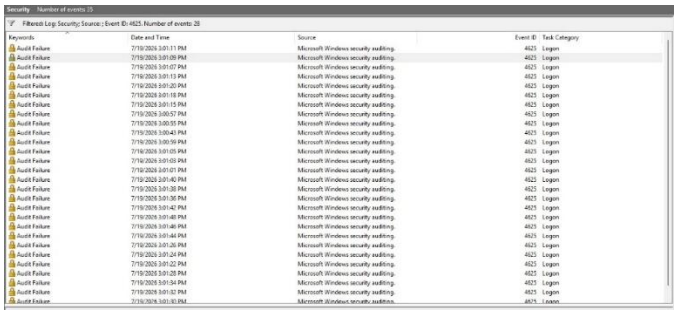
Skenario	Perlakuan	Hasil utama	Catatan
1	Bruteforce tanpa ALP (threshold 0)	28 event 4625 sampai password1 ditemukan	Baris ke-28 rockyou.txt
2	ALP threshold 5 dan AAP	5 event 4625, lalu 4740; akun terkunci	Kredensial tidak ditemukan; percobaan lanjutan tetap tercatat
3	WEF kondisi normal (VM1 dan VM2 ke VM3)	Event ID dan timestamp identik dengan log sumber	Resolusi detik
4	WEF saat VM1 diserang	27 event 4625 VM1 tercatat berurutan di VM3; logon VM2 (07:14:08) identik	Pengaruh beban terhadap VM2 belum teruji
5	Sebelum kompromi (VM4 ke VM3)	797 event 4625 pada log lokal sama dengan 797 pada Forwarded Events	Sesuai baris ke-798 wordlist
6	Setelah log VM4 dihapus	Log lokal 4 event; 4625 di VM3 tetap 797; 1102 tercatat 6 kali	Rincian pada Tabel 4

Hasil Skenario 1: Serangan Bruteforce SMB Tanpa Mitigasi (Baseline)

NetExec berhasil mengidentifikasi kredensial VM1\vm1 dengan password password1.

Hasil ini konsisten dengan posisi password1 pada baris ke-28 wordlist rockyou.txt. Verifikasi lebih lanjut

dilakukan melalui Event Viewer pada VM1, dengan memfilter log Security berdasarkan Event ID 4625 (kegagalan logon) (Microsoft, 2024). Hasil filter menunjukkan sebanyak 28 kejadian Event ID 4625 (Gambar 3) tercatat sebelum kredensial berhasil ditemukan, sesuai dengan posisi password1 dalam wordlist.



Gambar 3. Hasil filter Event Viewer VM1 menunjukkan 28 kejadian Event ID 4625 (Audit Failure)

Temuan ini menunjukkan bahwa tanpa penerapan Account Lockout Policy, serangan bruteforce dapat dilakukan tanpa hambatan hingga kredensial yang sesuai ditemukan, sejalan dengan temuan Mahardika dkk. (2026) pada pengujian serupa terhadap Windows 7 dan Windows 10.

Hasil Skenario 2: Serangan Bruteforce SMB Setelah Penerapan ALP dan AAP

Berbeda dengan Skenario 1, pada Skenario 2 akun vm1 berstatus STATUS_ACCOUNT_LOCKED_OUT setelah beberapa percobaan awal. NetExec tetap melanjutkan percobaan terhadap kata sandi berikutnya, namun seluruh percobaan lanjutan tersebut ditolak akibat akun yang telah terkunci.

Verifikasi pada Event Viewer VM1, dengan memfilter Event ID 4625 dan 4740 (akun terkunci) (Microsoft, 2024), menunjukkan tercatat 5 kejadian Event ID 4625 secara berurutan sebelum Event ID 4740 muncul (Gambar 4), sesuai dengan lockout threshold yang dikonfigurasi. Percobaan login lanjutan yang dilakukan NetExec terhadap akun yang telah terkunci tetap tercatat sebagai Event ID 4625, namun dengan Task Category "Account Lockout" alih-alih "Logon", menandakan bahwa Advanced Audit Policy tetap merekam upaya akses meskipun akun dalam status terkunci.

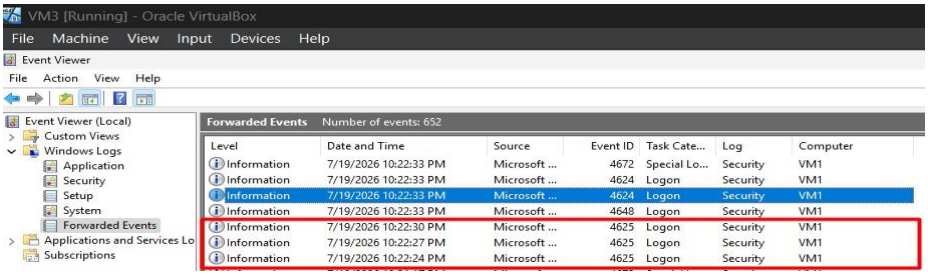


Gambar 4. Hasil filter Event Viewer VM1 — Event ID 4625 dan 4740 setelah ALP diterapkan

Hasil Skenario 3: Sentralisasi Log via WEF pada Kondisi Normal (Baseline)

Log Security pada VM1 mencatat rangkaian peristiwa logon, termasuk tiga kejadian Event ID 4625 pada pukul 22:22:24 hingga 22:22:30, diikuti Event ID 4624 (Audit Success) (Microsoft, 2024) pada pukul 22:22:33.

Log Forwarded Events pada VM3 menunjukkan rangkaian Event ID dan timestamp yang identik untuk sumber VM1 (Gambar 5).



Gambar 5. Forwarded Events pada VM3 untuk sumber VM1 — Event ID dan timestamp identik dengan log lokal

Pola yang sama turut diverifikasi pada VM2. Log Security lokal mencatat dua kejadian Event ID 4625 pada pukul 22:22:29 dan 22:22:30, diikuti Event ID 4624 pada pukul 22:22:32.

Kesamaan Event ID dan timestamp antara log sumber (VM1, VM2) dan log terpusat (VM3) pada resolusi menit dan detik menunjukkan bahwa WEF berhasil mensentralisasi log Security dari kedua endpoint tanpa selisih timestamp yang terdeteksi pada resolusi detik pada kondisi jaringan normal, sekalipun autentikasi memerlukan konfigurasi Specific User dan Basic Authentication sebagai pengganti mekanisme Kerberos.

Hasil Skenario 4: Sentralisasi Log via WEF di Bawah Beban Serangan

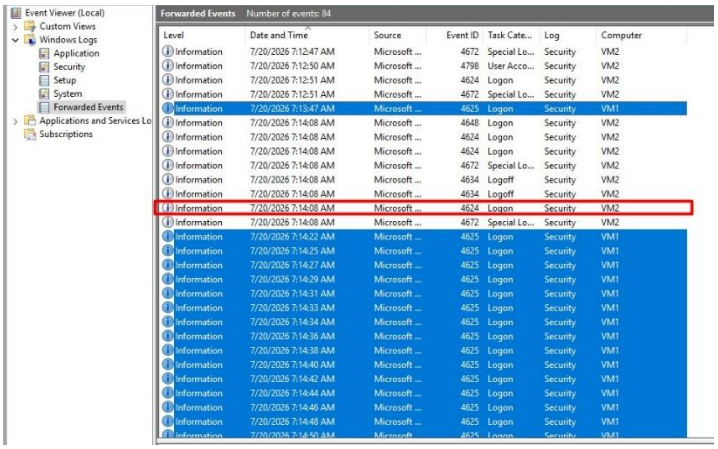
Log Security pada VM1 mencatat rangkaian Event ID 4625 dengan interval rata-rata sekitar dua detik, berlangsung dari pukul 07:14:22 hingga 07:15:16 (27 kejadian), didahului satu kejadian pada 07:13:47, sebelum tercatat Event ID 4624 pukul 07:15:18 saat kredensial ditemukan.

Sebelum serangan dimulai (07:14:22), VM2 mencatat satu sesi logon normal (Event ID 4648, 4624, 4672) pada pukul 07:14:08.

Verifikasi pada log Forwarded Events di VM3 menunjukkan bahwa sesi logon normal dari VM2 tetap tercatat dengan timestamp yang identik (Gambar 6), dan seluruh percobaan gagal dari VM1 tercatat berurutan tanpa indikasi kehilangan event (event drop).

Temuan ini menunjukkan bahwa event VM1 selama serangan tercatat berurutan pada VM3 tanpa indikasi event drop, dan event VM2 tetap diteruskan dengan timestamp identik. Karena logon VM2 terjadi sebelum serangan dimulai, pengamatan ini belum menguji pengaruh beban serangan terhadap forwarding endpoint lain.

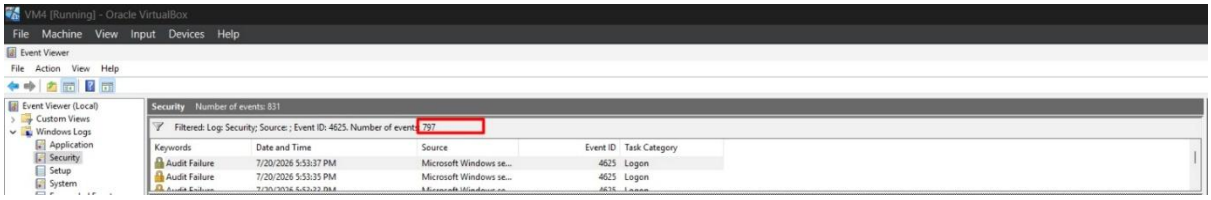
Batas tafsir hasil ini perlu dicermati. Logon normal VM2 pada pukul 07:14:08 tercatat sebelum serangan dimulai, sehingga yang terbukti hanyalah bahwa event VM2 tidak hilang dan timestamp-nya tidak bergeser ketika collector kemudian menerima rangkaian event 4625 dari VM1. Hasil ini belum menunjukkan apakah event VM2 yang terjadi bersamaan dengan serangan tetap diteruskan tanpa penundaan, dan ketiadaan event drop hanya berlaku pada laju serangan yang diuji (interval sekitar dua detik per percobaan) dalam satu kali pengujian.



Gambar 6. Forwarded Events pada VM3 — event VM2 (normal) dan VM1 (diserang) berdampingan

Hasil Skenario 5: Verifikasi Integritas Log Sebelum Kompromi

Jumlah Event ID 4625 pada log Security lokal VM4 diperiksa menggunakan PowerShell (Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4625}).Count. Hasilnya menunjukkan 797 event (Gambar 7).



Gambar 7. Filter Event ID 4625 pada log Security lokal VM4 menunjukkan 797 events

Pemeriksaan yang sama dengan PowerShell pada log Forwarded Events di VM3 untuk sumber VM4 juga

menghasilkan 797 event Event ID 4625 (Tabel 3).

Jumlah Event ID 4625 pada log lokal VM4 dan log terforward pada VM3 menunjukkan angka yang identik (797 = 797), konsisten secara matematis dengan posisi kredensial pada wordlist (baris ke-798), yaitu 797 percobaan gagal sebelum percobaan yang berhasil. Hasil ini menunjukkan bahwa WEF berhasil mereplikasi seluruh event logon failure dari VM4 ke VM3 tanpa terjadi kehilangan data selama proses forwarding berlangsung, sehingga kondisi baseline sebelum simulasi kompromi pada Skenario 6 dapat dinyatakan valid. Ditemukan pula bahwa Event ID 1102 (Audit log cleared) (Microsoft, 2024), yang tercatat pada saat log VM4 dibersihkan sebagai bagian dari tahap persiapan, turut berhasil diteruskan ke VM3.

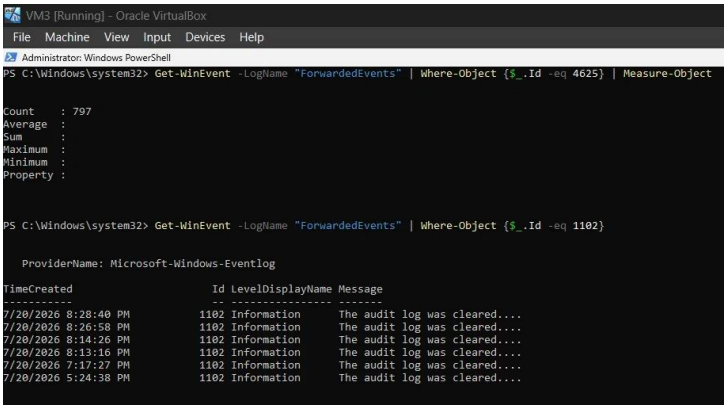
Angka 797 = 797 memiliki makna analitis yang lebih kuat daripada sekadar kesamaan jumlah. Karena password2 berada pada baris ke-798 wordlist dan NetExec mencoba kata sandi secara berurutan, jumlah percobaan gagal yang seharusnya terekam adalah tepat 797. Log lokal VM4 mencatat 797 event, sehingga Advanced Audit Policy merekam setiap percobaan tanpa ada yang terlewat, dan log terforward pada VM3 juga mencatat 797 event, sehingga WEF tidak menghilangkan satu pun event. Kecocokan tiga angka dari sumber berbeda (posisi pada wordlist, log lokal, dan log terpusat) memberikan verifikasi silang yang tidak bergantung pada satu sumber, sekaligus menjadi pembanding bagi Skenario 6: setiap perubahan jumlah pada collector setelah penghapusan dapat dikaitkan langsung dengan penghapusan log.

Hasil Skenario 6: Analisis Integritas Log Pasca-Kompromi

Setelah perintah penghapusan dieksekusi, log Security lokal pada VM4 diperiksa melalui Event Viewer. Hasil pemeriksaan menunjukkan bahwa log Security hanya menyisakan 4 event, yaitu 3 kejadian Event ID 4634 (Logoff) dan 1 kejadian Event ID 1102 (Log clear).

Seluruh jejak serangan bruteforce sebelumnya, termasuk 797 kejadian Event ID 4625 yang tercatat pada Skenario 5, telah hilang sepenuhnya dari log lokal VM4. Untuk menilai apakah tindakan penghapusan log lokal turut menghilangkan jejak bukti pada sisi collector, dilakukan pemeriksaan pada log Forwarded Events di VM3 menggunakan PowerShell, memeriksa jumlah Event ID 4625 dan Event ID 1102 yang diterima dari VM4 (Gambar 8).

Hasil query pertama menunjukkan Count sebesar 797, identik dengan jumlah Event ID 4625 yang tercatat pada Skenario 5 sebelum log lokal VM4 dihapus. Hasil query kedua menunjukkan enam kejadian Event ID 1102 tercatat pada log Forwarded Events, dengan lima kejadian pertama merupakan hasil aktivitas pembersihan log pada pengujian pendahuluan sebelum Skenario 5, sementara kejadian terakhir bersesuaian dengan waktu eksekusi perintah penghapusan log oleh penyerang.



Gambar 8. Verifikasi log Forwarded Events pada VM3 — jumlah Event ID 4625 tetap 797 dan enam kejadian Event ID 1102 tercatat lengkap

Tabel 4. Perbandingan Log Lokal dan Log Terforward Pasca-Penghapusan (Skenario 6)

Sumber	**Kondisi Setelah Penghapusan**	**Event ID 4625**	**Event ID 1102**
Log lokal VM4 (Security)	Dihapus oleh penyerang (wevtutil cl Security)	0 (hilang)	1 (hanya kejadian terakhir)
Log terforward VM3 (Forwarded Events)	Tidak terpengaruh, forwarding terjadi sebelum log lokal dikosongkan	797 (tetap utuh)	6 (seluruh riwayat tercatat)

Perbandingan pada Tabel 4 menunjukkan kontras signifikan antara kondisi log lokal dan log terpusat pasca-kompromi. Ketika penyerang berhasil menghapus log lokal VM4, seluruh 797 jejak percobaan bruteforce hilang sepenuhnya dari sumbernya, namun salinan log yang telah diteruskan ke WEF Collector pada VM3 tetap utuh karena proses forwarding bersifat near real-time dan telah berlangsung sebelum log lokal dikosongkan.

Event ID 1102 memiliki nilai forensik tersendiri. Event ini dicatat Windows setiap kali log audit dihapus, sehingga keberadaannya pada collector membuktikan bahwa penghapusan terjadi, kapan terjadi, dan berapa kali terjadi, meskipun isi log yang dihapus telah hilang dari sumbernya. Pada log lokal VM4 hanya tersisa satu event 1102, yaitu hasil penghapusan terakhir, sedangkan collector menyimpan enam event sehingga riwayat pembersihan sebelumnya tetap dapat ditelusuri. Dengan data collector, penyelidik dapat memisahkan apa yang dilakukan penyerang sebelum penghapusan (797 percobaan gagal) dari kapan penyerang berupaya menghilangkan jejak (timestamp 1102 terakhir). Batasnya, WEF hanya melindungi event yang sempat diteruskan sebelum penghapusan, dan pengujian ini tidak mencakup skenario ketika penyerang menghentikan layanan forwarding terlebih dahulu.

PEMBAHASAN

Secara keseluruhan, hasil pada Skenario 1 dan 2 menunjukkan bahwa Account Lockout Policy dan Advanced Audit Policy, ketika diterapkan secara terintegrasi, membentuk lapisan pertahanan yang saling melengkapi terhadap serangan bruteforce SMB: ALP membatasi ruang gerak penyerang secara otomatis (serangan terhenti pada percobaan ke-5 sehingga kredensial pada posisi ke-28 wordlist tidak pernah ditemukan), sementara AAP memastikan setiap upaya akses tetap terekam sebagai jejak forensik, termasuk upaya yang terjadi setelah akun dikunci. Temuan ini memperkuat hasil Mahardika dkk. (2026), sekaligus melengkapinya: penelitian tersebut menunjukkan efektivitas ALP pada level akun namun tanpa audit trail terdokumentasi, sedangkan penelitian ini menunjukkan bahwa mitigasi dan deteksi pada layanan SMB berbasis Windows tidak harus dipandang sebagai dua kebutuhan terpisah yang masing-masing memerlukan tools tambahan, melainkan dapat dicapai sekaligus melalui konfigurasi mekanisme native yang sudah tersedia pada sistem operasi itu sendiri, bahkan pada Windows 11, yang menuntut penyesuaian tool serangan (dari Hydra ke NetExec) dibandingkan pengujian pada Windows 7/10 oleh Mahardika dkk. (2026).

Hasil pada Skenario 3 dan 4 menunjukkan bahwa Windows Event Forwarding mampu mensentralisasi log Security dari beberapa endpoint ke satu collector secara andal pada jaringan workgroup, tanpa bergantung pada Active Directory maupun SIEM komersial, dan mencatat seluruh event endpoint yang sedang diserang tanpa kehilangan event. Temuan ini sejalan dengan prinsip sentralisasi log yang ditekankan Rahman dkk. (2026) dan Taberima serta Ramayanti (2024), namun menunjukkan bahwa efektivitas serupa dapat dicapai tanpa investasi pada SIEM eksternal maupun infrastruktur domain penuh. Implikasinya, keterbatasan infrastruktur bukan lagi alasan yang sah bagi organisasi kecil untuk sepenuhnya mengabaikan visibilitas log terpusat, sentralisasi dapat dicapai pada level fitur bawaan sistem operasi.

Hasil pada Skenario 5 dan 6 menunjukkan bahwa kombinasi AAP dan WEF mampu mempertahankan integritas bukti digital sekalipun endpoint sumber telah dikompromikan sepenuhnya dan log lokalnya dihapus oleh penyerang. Kontras antara 0 event yang tersisa pada log lokal VM4 dan 797 event yang tetap utuh pada collector VM3 menjadi wujud operasional langsung dari prinsip Digital Forensic Readiness (Daubner dkk., 2023): kesiapan forensik pada dasarnya bukan soal seberapa canggih alat yang dimiliki suatu organisasi, melainkan soal apakah salinan bukti telah ditempatkan di luar jangkauan pihak yang berpotensi mengompromikannya sebelum insiden terjadi. Temuan ini juga memperluas kajian konseptual Sajan dkk. (2025) mengenai relevansi forensik Forwarded Event Log, dengan menyediakan bukti empiris pada skenario serangan nyata tanpa SIEM komersial.

Secara keseluruhan, ketiga kelompok temuan tersebut menunjukkan bahwa satu rangkaian kesiapan forensik yang utuh, mulai dari deteksi dan mitigasi, sentralisasi log, hingga pelestarian bukti pasca-kompromi, dapat dibangun sepenuhnya dari fitur bawaan Windows tanpa biaya lisensi tambahan. Implikasinya, organisasi dengan sumber daya TI terbatas, seperti UMKM maupun laboratorium kampus, tidak perlu menunggu hingga mampu berinvestasi pada SIEM atau Active Directory untuk mulai membangun kesiapan forensik digital.

Penelitian ini memiliki sejumlah keterbatasan yang relevan untuk diperhatikan dalam menginterpretasikan temuan di atas. Pertama, pengujian hanya melibatkan satu jenis vektor serangan, yaitu bruteforce SMB menggunakan satu wordlist tunggal, sehingga belum diketahui apakah pola temuan yang sama berlaku pada vektor serangan lain seperti RDP, WinRM, atau teknik lateral movement pasca-kompromi. Kedua, lingkungan pengujian dibangun pada skala terbatas (lima mesin virtual dalam satu subnet) dan satu edisi sistem operasi (Windows 11 Home), sehingga generalisasi temuan pada jaringan dengan jumlah endpoint yang jauh lebih besar, edisi Windows lain, atau lingkungan hybrid dengan sistem operasi non-Windows belum dapat dipastikan. Ketiga, arsitektur WEF pada penelitian ini hanya menggunakan satu collector tanpa mekanisme redundansi, sehingga ketahanan sentralisasi log terhadap skenario collector itu sendiri menjadi target serangan belum diuji. Keempat, latensi forwarding hanya dinilai secara kualitatif melalui kesesuaian timestamp pada resolusi detik,

tanpa pengukuran statistik terhadap distribusi latensi, dan logon normal pada Skenario 4 terjadi sebelum serangan dimulai sehingga pengaruh beban serangan terhadap forwarding endpoint lain belum teruji. Kelima, setiap skenario dijalankan satu kali tanpa pengulangan sehingga variabilitas hasil belum dapat dinilai. Keenam, WinRM menggunakan Basic Authentication melalui HTTP (port 5985) karena ketiadaan Kerberos pada workgroup, sehingga kredensial subscription tidak terenkripsi pada level transport.

KESIMPULAN

Penelitian ini menguji kombinasi Account Lockout Policy (ALP), Advanced Audit Policy (AAP), dan Windows Event Forwarding (WEF) untuk mendeteksi dan memitigasi bruteforce SMB pada jaringan workgroup tanpa Active Directory maupun SIEM. Pertama, ALP dengan threshold 5 menghentikan serangan pada percobaan ke-5, sehingga kredensial yang pada baseline ditemukan di percobaan ke-28 tidak diperoleh, sementara AAP tetap merekam seluruh percobaan, termasuk setelah akun terkunci. Kedua, WEF mensentralisasi log Security dengan Event ID dan timestamp identik terhadap log sumber pada resolusi detik dan mencatat seluruh event endpoint yang diserang tanpa kehilangan event; pengaruh beban serangan terhadap endpoint lain serta distribusi latensi belum teruji. Ketiga, seluruh 797 event percobaan gagal tetap utuh pada collector meskipun log lokal VM sumber dihapus penyerang, dan penghapusan log itu sendiri (Event ID 1102) turut terekam sehingga waktu upaya penghapusan jejak dapat ditelusuri. Temuan ini menunjukkan bahwa kesiapan forensik digital dasar dapat dibangun sepenuhnya dari fitur bawaan Windows tanpa biaya lisensi tambahan. Bagi UMKM dan laboratorium kampus, disarankan menerapkan ALP dan AAP pada seluruh endpoint SMB, menyiapkan satu collector WEF khusus, dan mendokumentasikannya sebagai prosedur baku. Karena setiap skenario dijalankan satu kali pada lima mesin virtual dalam satu subnet, penelitian selanjutnya disarankan mengulang pengujian, mengukur latensi secara kuantitatif, serta menguji vektor lain seperti RDP dan WinRM.

REFERENSI

Ajhari, A. A., Manaon, M. A., & Priambodo, D. F. (2023). Security awareness framework untuk usaha mikro, kecil dan menengah di Indonesia. *Jurnal Info Kripto, 17*(3).

Armansyah, Y., Khairil, & Aspriyono, H. (2023). Penggunaan metode Active Directory dan privileges pada jaringan komputer untuk penyimpanan data central pada SMA Muhammadiyah 1 Bengkulu. *Jurnal Komputer, 2*(1), 1–16.

Australian Signals Directorate. (2021). *Windows event logging and forwarding*. Cyber.gov.au.

Badan Siber dan Sandi Negara. (2024). *Lanskap keamanan siber Indonesia 2024*. Direktorat Operasi Keamanan Siber.

Center for Internet Security. (2025). *CIS Microsoft Windows 10 Stand-alone Benchmark* (v4.0.0).

Daubner, L., Macak, M., Matulevičius, R., Buhnova, B., Maksović, S., & Pitner, T. (2023). Addressing insider attacks via forensic-ready risk management. *Journal of Information Security and Applications, 73*, Article 103433. https://doi.org/10.1016/j.jisa.2023.103433

Fachri, F. (2023). Optimasi keamanan web server terhadap serangan brute-force menggunakan penetration testing. *Jurnal Teknologi Informasi dan Ilmu Komputer, 10*(1), 51–58. https://doi.org/10.25126/jtiik.2023105872

Mahardika, A. Z. A., Zain, A. M., Pramata, A. B., & Mahri, M. F. A. (2026). *Evaluasi serangan brute force menggunakan Hydra pada layanan SMB Windows 7 dan Windows 10* [Makalah tidak dipublikasikan]. Informatika, Universitas Pembangunan Nasional "Veteran" Jawa Timur.

Microsoft. (2024, 15 Juli). *Windows security audit events* [Spreadsheet Excel]. Microsoft Download Center.

Microsoft. (2025, 18 Agustus). *Use Windows Event Forwarding to help with intrusion detection*. Microsoft Learn.

Microsoft. (2026). *Set event log security locally or via Group Policy*. Microsoft Learn.

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce.

Rahman, R., Sairah, A. N., & Heryanti, A. P. (2026). Implementasi sistem monitoring keamanan jaringan menggunakan log analysis. *Jurnal Riset Sistem Informasi, 3*(2), 30–34.

Sajan, P. P., Rajesh, A. R., Jenani, S., Milina, S. S., Devi, V. R., & Prabha, V. P. (2025). Analytical study on forensic relevance of Windows event logs. *International Journal for Research in Applied Science & Engineering Technology, 13*(7), 308–315.

Taberima, G. M., & Ramayanti, D. (2024). Mengoptimalkan manajemen dan keamanan TI melalui implementasi layanan domain Active Directory: Studi kasus pada infrastruktur TI perusahaan. *Jurnal Informatika Teknologi dan Sains (JINTEKS), 6*(1), 79–89.

Vaseghipanah, M., Jabbehdari, S., & Navidi, H. (2025). A game-theoretic approach for quantification of strategic behaviors in digital forensic readiness. *Journal of Cybersecurity and Privacy, 5*(4), Article 105