P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

# Pemantauan dan Pengawasan Serangan Siber SSH Brute Force di Indonesia dengan IBM QRadar Community Edition

[1]William Christoper, [2]Rafli Zufargian Hermawan
[1]Informatika, Persada Indonesia University Y.A.I, Jakarta
[2]Informatika, Persada Indonesia University Y.A.I, Jakarta

E-mail: [1]william.christoper@upi-yai.ac.id, [2]2144190008_rafli@upi-yai.ac.id

## ABSTRAK

Indonesia, sebagai salah satu negara dengan pertumbuhan ekonomi yang pesat dan diiringi oleh kemajuan teknologi yang cepat dan semakin maju, membuatnya dihadapi tantangan yang semakin besar juga dalam menjaga keamanan jaringan dan sistem. Pada penelitian ini, metodologi yang digunakan adalah studi literatur dan eksperimental. Studi literatur adalah proses pengumpulan dan analisis informasi dari berbagai sumber yang relevan dengan topik penelitian. Berbagai percobaan dilakukan melalui kegiatan eksperimental. Tujuannya adalah untuk membuktikan kemampuan IBM QRadar Community Edition untuk mendeteksi ancaman keamanan dan mengidentifikasi serangan. Hasil yang diberikan pada penelitian ini, IBM QRadar Community Edition dapat memberikan sebuah log yang terjadi kepada security analys ketika pengguna diserang oleh penyerang menggunakan SSH Brute Force.Dalam penelitian ini, dapat diambil kesimpulan bahwa pemantau dan pengawasan sebuah sistem dan jaringan sangat penting untuk melindungi dari berbagai serangan yang merugikan berasal dari penyerang. IBM QRadar Community Edition dapat dijadikan solusi untuk melakukan hal tersebut. Dengan mengimplementasikan IBM QRadar Community Edition ini dapat secara efektif dalam mendeteksi sebuah anomali yang terjadi, dan hal ini dapat mengurangi risiko yang terjadi terhadap sebuah data dan meminimalkan kerugian yang terjadi.

**Kata kunci :** ***IBM QRadar Community Edition, SSH Brute Force, log***

## *ABSTRACT*

Indonesia, as one of the countries with rapid economic growth and accompanied by rapid and increasingly advanced technological advances, makes it face increasingly greater challenges in maintaining network and system security. In this research, the methodology used is literature and experimental studies. Literature study is the process of collecting and analyzing information from various sources relevant to the research topic. Various experiments were conducted through experimental activities. The goal is to prove the ability of IBM QRadar Community Edition to detect security threats and identify attacks. The results given in this study, IBM QRadar Community Edition can provide a log that occurs to security analysts when users are attacked by attackers using SSH Brute Force.In this study, it can be concluded that monitoring and supervision of a system and network is very important to protect against various harmful attacks originating from attackers. IBM QRadar Community Edition can be used as a solution to do this. By implementing IBM QRadar Community Edition, it can effectively detect anomalies that occur, and this can reduce the risk to data and minimize losses.

**Keyword :** ***IBM QRadar Community Edition, SSH Brute Force, log***

https://doi.org/10.37817/tekinfo.v25i2
P-ISSN: 1411-3635
E-ISSN: 2962-5645

## 1. PENDAHULUAN

Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara (BSSN) mencatat jumlah serangan siber yang terjadi di Indonesia antara Januari hingga Juli 2021 sebanyak 741.441.648 kali (Andi Nugroho, 2021).


Gambar 1.Grafik serangan siber di Indonesia tahun 2021
Sumber :
https://cyberthreat.id/gbr_artikel/siber-bssn.jpg

Indonesia merupakan negara peringkat ketiga yang masuk dalam radar sasaran serangan siber (daon001, 2018). Oleh karena itu, semakin maju teknologi di Indonesia, harus diiringi juga tingkat, kemananan, dan teknik keamanan sebuah sistem dan jaringan.

Indonesia, sebagai salah satu negara dengan pertumbuhan ekonomi yang pesat dan diiringi oleh kemajuan teknologi yang cepat dan semakin maju, membuatnya dihadapi tantangan yang semakin besar juga dalam menjaga keamanan jaringan dan sistem.

Seiring dengan perkembangan ini, penggunaan *Secure Shell (SSH)* sebagai cara dan sarana untuk mengakses, mengelola, dan berkomunikasi dengan server jarak jauh telah menjadi sangat umum. *SSH* memberikan keamanan dan teknik enkripsi yang kuat, menjadikannya pilihan utama dalam mengakses sistem.

Namun, terdapat kerentanan pada penggunaan *SSH* ini, yaitu serangan *SSH Brute Force*. Penyalahgunaan sistem dengan serangan ini dapat menyebabkan masalah besar, seperti kebocoran data, kerusakan sistem, dan pelanggaran keamanan.

Serangan *SSH Brute Force* merupakan serangan upaya secara terus menerus untuk menebak sebuah nama pengguna dan kata sandi dengan mencoba berbagai kombinasi sevata otomatis.

Meningkatnya insiden serangan *SSH Brute Force* merupakan masalah utama yang dihadapi oleh organisasi, pemerintah, dan masyarakat di Indonesia. Penyerang siber, baik yang ada di Indonesia maupun internasional, berusaha melakukan penyerangan ke server dan infrastruktur jaringan yang ada di Indonesia.

Untuk mencegah serangan ini, sangat penting untuk melakukan pemantauan dan pengawasan pada lalu lintas jaringan dengan cermat dan secepat mungkin menemukan serangan *SSH Brute Force*. *IBM QRadar Community Edition* menjadi relevan disini.

*IBM QRadar Community Edition* adalah sebuah platform yang dapat membantu pengguna untuk memantau, mendeteksi, dan menanggapi serangan siber dengan cepat. *IBM QRadar Community Edition* akan menampilkan sebuah log dan memberikan notifikasi kepada pengguna jika terjadi anomali atau keanehan berdasarkan sebuah aturan yang telah dibuat sebelum nya untuk melakukan pendeteksian pada sebuah sistem dan jaringan.

Melalui penelitian ini, akan dibahas penerapan dan penggunaan *IBM QRadar Community Edition* sebagai platform penting untuk mengawasi sistem dan

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

jaringan di Indonesia dari serangan *SSH Brute Force*.

## 2. LANDASAN TEORI

### 2.1 SERANGAN SIBER

Serangan siber adalah upaya yang disengaja untuk mencuri, mengekspos, mengubah, melumpuhkan, atau menghancurkan data, aplikasi, atau aset lainnya melalui akses tidak sah ke jaringan, sistem komputer, atau perangkat digital (IBM, n.d.).

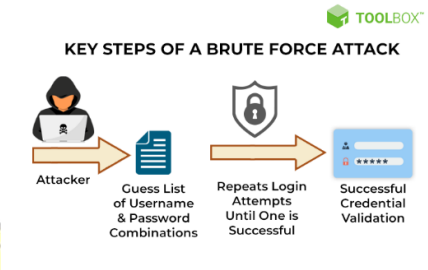
Serangan siber dapat mengganggu, merusak, dan menghancurkan sebuah bisnis, organisasi, dan pemerintahan. Serangan siber dapat membahayakan sebuah informasi berupa indentitas pribadi, seperti NIK, nomor rekening, tempat tinggal, dan data pribadi lainnya.

Serangan siber bisa terjadi karena penyerang memiliki sebuah alasan atau motivasi seperti tindak kriminal, politik, dan pribadi. Penyerang akan melakukan pemerasan kepada korban dengan menyandra atau mengancam korban untuk membayar sejumlah uang agar data nya tidak di sebar.

Perusahaan, organisasi, dan pemerintahan dapat mengurangi serangan siber dengan cara menerapkan sebuah sistem keamanan siber seperti melakukan: pencegahan serangan siber untuk melakukan identifikasi dan melindungi aset nya. Melakukan pendeteksian dengan pemantauan keamanan berkelanjutan dan deteksi serangan.

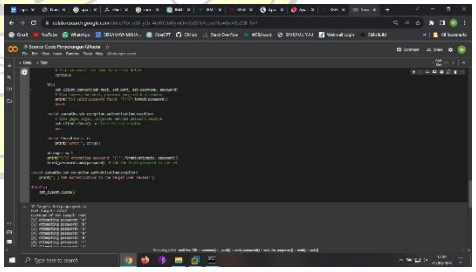
### 2.1.1 SSH BRUTE FORCE

Serangan *SSH Brute Force* adalah teknik peretasan yang melibatkan berulang kali mencoba kombinasi nama pengguna dan kata sandi yang berbeda hingga penyerang mendapatkan akses ke server jarak jauh (Chiradeep BasuMallick, 2022). Penyerang menggunakan alat otomatis seperti *Hydra* atau *Medusa* yang dapat mencoba ribuan kombinasi nama pengguna dan kata sandi dalam hitungan detik, menjadikannya cara yang cepat dan efektif untuk membobol server.




Gambar 2.Serangan SSH BRUTE FORCE
Sumber: https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-brute-force-attack/

Penyerang yang melakukan serangan *SSH Brute Force* biasanya memanfaatkan daftar kata sandi yang umum digunakan atau melakukan serangan kamus dengan mencoba kombinasi kata sandi yang ada dalam daftar tertentu. Selain itu, mereka juga dapat menggunakan teknik kombinasi kata sandi yang terdiri dari karakter acak untuk meningkatkan kemampuan serangan mereka.



Gambar 3.Contoh Serangan SSH BRUTE FORCE
Sumber : Dokumen Pribadi

Pada Gambar 3 merupakan contoh upaya penyerangan menggunakan SSH BRUTE FORCE ke server tujuan. Menggunakan bahasa pemrograman

*python.* Saat penyerangan, akan diminta memasukan IP Tujuan, setelahnya akan dilakukan BRUTE FORCE untuk mencoba masuk ke server target.

## 2.2 SECURE SHELL (SSH)

*Secure Shell* atau biasa disingkat *SSH* merupakan sebuah protokol jaringan yang digunakan untuk melakukan komunikasi perangkat jarak jauh yang aman menggunakan kriptografi. Dalam komunikasi nya, *SSH* melakukan enkripsi dan autentikasi yang aman, jadi data yang dikirim oleh pengirim sampai ke penerima terenkripsi.


Gambar 4.Ilustrasi SSH
Sumber : Dokumen Pribadi

Protokol ini digunakan untuk mengakses, mengendalikan, mengelola, dan mentransfer sebuah data secara aman pada suatu perangkat didalam jaringan.

Untuk memastikan data yang dikirim antara perangkat, SSH menggunakan enkripsi kunci publik dan privat. Konsep ini serupa dengan pengiriman surat melalui pos, hanya orang yang memiliki kunci yang tepat yang dapat membuka surat.

Salah satu fitur utama SSH adalah keamanannya. Dengan menggunakan enkripsi, SSH memastikan bahwa data yang dikirim antara perangkat tidak dapat dibaca oleh pihak ketiga yang tidak sah. Dalam kasus di mana seorang pengguna menggunakan koneksi SSH untuk mengirimkan data sensitif, seperti kata sandi, informasi tersebut akan dienkripsi, sehingga hanya server yang dituju yang dapat membacanya. Langkah penting dalam menjaga keamanan data adalah melakukan enkripsi data.

## 2.3 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Security Information and Event Management (SIEM) adalah pendekatan yang digunakan oleh organisasi untuk mengelola dan menganalisis data keamanan dari berbagai sumber.

Contoh nyata dari penggunaan SIEM adalah ketika sebuah perusahaan menggunakan platform SIEM untuk memantau aktivitas jaringan mereka dan mendeteksi ancaman keamanan potensial. Teori di balik SIEM melibatkan pengumpulan data dari berbagai log dan perangkat keamanan, analisis data ini untuk mengidentifikasi pola aneh atau aktivitas mencurigakan, dan memberikan respons yang cepat terhadap ancaman yang terdeteksi.

SIEM memungkinkan organisasi untuk mengintegrasikan informasi dari berbagai sumber ke dalam satu platform yang terpusat, memungkinkan visibilitas yang lebih baik terhadap keamanan jaringan mereka. Dengan menggunakan SIEM, perusahaan dapat mengidentifikasi serangan keamanan yang mungkin terlewatkan oleh sistem keamanan tradisional. Analogi yang dapat digunakan untuk menjelaskan konsep SIEM adalah seperti detektif yang selalu waspada terhadap tindakan mencurigakan.

### 2.3.1 IBM QRADAR COMMUNITY EDITION

IBM QRadar Community Edition adalah platform keamanan yang dirancang untuk membantu organisasi mengelola dan menganalisis data keamanan mereka.

Platform ini memungkinkan pengguna untuk mendeteksi ancaman keamanan, mengidentifikasi serangan potensial, dan meresponsnya dengan cepat. Contoh nyata dari penggunaan IBM QRadar Community Edition adalah oleh perusahaan keamanan yang ingin melindungi data sensitif mereka dari serangan siber. Dengan menggunakan platform ini, mereka dapat memantau aktivitas jaringan mereka secara real-time dan mengambil tindakan yang diperlukan untuk melindungi informasi mereka.

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2

IBM QRadar Community Edition menggunakan berbagai teknik analisis data untuk mengidentifikasi pola aneh atau mencurigakan dalam lalu lintas jaringan. Salah satu teknik yang digunakan adalah analisis perilaku, di mana platform mempelajari pola aktivitas normal pengguna dan sistem untuk mendeteksi perubahan yang mencurigakan. Dengan memanfaatkan machine learning dan kecerdasan buatan, IBM QRadar Community Edition dapat secara otomatis mengklasifikasikan ancaman dan memberikan rekomendasi tindakan yang tepat.

## 3. METODOLOGI

Pada penelitian ini, metodologi yang digunakan adalah studi literatur dan eksperimental. Studi literatur adalah proses pengumpulan dan analisis informasi dari berbagai sumber yang relevan dengan topik penelitian. Salah satu contoh penerapan studi literatur dalam penelitian ini adalah ketika seorang peneliti mengumpulkan data dari jurnal ilmiah, buku, dan artikel yang berkaitan dengan topik penelitian.

Studi literatur memungkinkan peneliti untuk memperoleh pemahaman yang lebih baik tentang topik penelitian dan teori-teori yang relevan. Studi literatur juga memungkinkan peneliti untuk melihat bagaimana pengetahuan sebelumnya berkembang dan menemukan celah yang dapat dipenuhi dengan penelitian baru. Dengan menganalisis berbagai sumber informasi, peneliti dapat memperoleh pemahaman yang lebih luas dan mendalam tentang topik penelitian. Studi ini dapat memberikan dasar yang kuat untuk temuan penelitian yang akurat dan relevan.

Berbagai percobaan dilakukan melalui kegiatan eksperimental. Tujuannya adalah untuk membuktikan kemampuan IBM QRadar Community Edition untuk mendeteksi ancaman keamanan dan mengidentifikasi serangan. Studi ini akan mensimulasikan penyerangan SSH Brute Force ke sebuah user.

## 4. HASIL DAN PEMBAHASAN

Penerapan pemantauan dan identifikasi serangan akan menggunakan sistem SIEM dengan platform IBM Qradar Community Edition. Platform ini akan diinstal pada sebuah Virtual Machine (VM). Adapun spesifikasi yang dibutuhkan untuk meng-instal IBM Qradar Community Edition :

| | |
|---|---|
| CPU | 2 core atau 6 core (Rekomendasi) |
| RAM | Minimal 8 Gb |
| Storage | Minimal 250 Gb |
| Internet | Ya |

Tabel 1.Spesifikasi minimal perangkat

Setelah instalasi, platform ini akan digunakan untuk pendeteksian dan respon terhadap suatu serangan keamanan serta pengelolaan keamanan informasi pada penelitian ini.

Selanjutnya, akan dijabarkan aplikasi atau alat yang akan digunakan selama percobaan penelitian ini:

a) VMware Workstation Pro

Perangkat lunak virtualisasi VMware Workstation Pro memungkinkan pengguna membuat dan mengelola mesin virtual (VM) pada komputer mereka. Platform ini memungkinkan pengguna menjalankan beberapa sistem operasi pada satu perangkat fisik tanpa perlu menginstal sistem operasi tersebut secara langsung.

Pada perangkat lunak inilah IBM Qradar Community Edition dan OS User (target) di instal

b) CentOS

https://doi.org/10.37817/tekinfo.v25i2
P-ISSN: 1411-3635
E-ISSN: 2962-5645

CentOS adalah varian Linux yang bersifat open-source dan berbasis kode sumber dari sistem operasi Red Hat Enterprise Linux (RHEL).

Pada penelitian ini, CentOS akan digunakan sebagai sistem operasi target serangan yang akan dilakukan oleh penyerang. Sistem operasi ini akan diintegrasikan dengan IBM Qradar Community Edition.

### c) Ngrok

NGROK adalah layanan tunnelling yang memberikan akses publik ke server lokal. Dengan kata lain, NGROK membangun jembatan aman antara server lokal dan internet, memungkinkan pengembang atau administrator sistem untuk mengakses aplikasi atau layanan lokal mereka melalui URL publik yang dapat diakses dari mana saja.

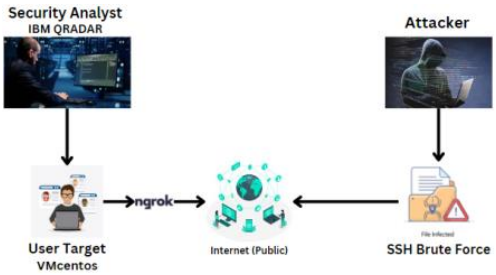
NGROK akan digunakan untuk membuat OS pengguna menjadi IP Publik sehingga dapat dilakukan sebuah percobaan serangan dari penyerang dengan jarak jauh.

### d) Google Colab

Google memberikan Google Colab, sebuah teks editor yang memungkinkan pengembang dan peneliti membuat, berbagi, dan menjalankan kode Python dalam lingkungan *cloud* secara gratis.

Tools ini akan digunakan oleh penyerang dengan menggunakan sebuah skrip phyton untuk melancarkan serangan nya kepada OS pengguna.

Adapun alur percobaan penyerangan dan pendeteksian yang akan dilakukan pada penelitian ini:




Gambar 5.Alur penyerangan dan pendeteksian

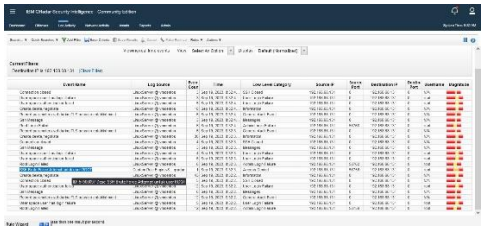
Security analyst memiliki peran dalam mengawasi sebuah jaringan komunikasi dengan menggunakan IBM Qradar Community Edition untuk memantau VM CentOS yang digunakan oleh user target.

Dalam workflow di atas, VM CentOS memiliki user target yang akan diserang oleh attacker menggunakan SSH Brute Force. VM CentOS pada workflow diatas sudah bersifat public dengan menggunakan NGROK sehingga VM CentOS tersebut sudah memiliki IP Public, sehingga Attacker akan mencoba menyerang user target melalui IP public tersebut dengan SSH Brute Force untuk mendapatkan password dari user ROOT pada VM CentOS user target.

User Target yang menggunakan VM CentOS harus mengintegrasikan logs nya ke IBM Qradar Community Edition sehingga dapat terhubung dan dapat diawasi jaringan nya. Setelah selesai terintegrasi dengan IBM Qradar Community Edition, Security analyst dapat melihat dan mengawasi secara real time terhadap data dan aliran jaringan yang terjadi pada VM CentOS.

Apabila terjadi sebuah serangan, Security Analyst akan mendapatkan sebuah Event Log atau Network Log berdasarkan aturan yang ada atau yang dibuat dibuat dalam IBM Qradar Community Edition apabila terjadi sebuah anomali atau serangan pada pengguna nya, yaitu VM CentOS.

P-ISSN: 1411-3635
E-ISSN: 2962-5645
https://doi.org/10.37817/tekinfo.v25i2



Gambar 6.Tampilan log pada IBM Qradar Community Edition pasca serangan SSH Brute Force

Log yang ditampilkan pada ‘Gambar 6 menunjukkan telah terjadi serangan SSH Brute Force ke pengguna. Kalimat yang ditampilkan adalah “SSH Brute Force Attempt untuk user ROOT”

Dengan menggunakan *IBM QRadar Community Edition*, peruusahan, kelompok, atau pemerintah dapat mengetahui apabila terjadi sebuah serangan yang kemudian akan ditindaklanjuti.

Hasil yang diberikan pada penelitian ini, *IBM QRadar Community Edition* dapat memberikan sebuah log yang terjadi kepada *security analys* ketika pengguna diserang oleh penyerang menggunakan SSH Brute Force.

Berdasarkan percobaan ini, peneliti menyarankan untuk menggunakan password yang tidak gampang ditebak, dan membatasi upaya login ke ssebuah server. Hal ini dapat mencegah terjadinya serangan yang dapat berakibat lebih fatal.

## 5. KESIMPULAN

Seiring dengan pertumbuhan teknologi infomasi yang cepat di Indonesia, dan penggunaan SSH sebagai sarana akses ke sebuah server. Namun, tedapat sebuah oknum atau individu yang ingin merugikan pihak lain dengan melakukan penyerangan ke sebuah server, salah satu nya dengan serangan SSH BRUTE FORCE. Hal ini dapat menjadi sebuah ancaman yang serius terhadap sistem, terlebih lagi ke sebuah data yang sensitive.

Dalam penelitian ini, dapat diambil kesimpulan bahwa pemantau dan pengawasan sebuah sistem dan jaringan sangat penting untuk melindungi dari berbagai serangan yang merugikan berasal dari penyerang.

*IBM QRadar Community Edition* dapat dijadikan solusi untuk melakukan hal tersebut. Dengan mengimplementasikan *IBM QRadar Community Edition* ini dapat secara efektif dalam mendeteksi sebuah anomali yang terjadi, dan hal ini dapat mengurangi risiko yang terjadi terhadap sebuah data dan meminimalkan kerugian yang terjadi.

## 6. UCAPAN TERIMA KASIH

Puji dan Syukur kepada Tuhan Yang Maha Esa, atas segala berkat dan karunia-Nya yang telah membantu penulis menyelesaikan penelitian ini.

Penulis menyadari bahwa masih banyak kekurangan dalam penelitian ini. Untuk itu penulis mengharapkan kritik dan saran atas hasil penelitian ini untuk menyempurnakan dimasa yang akan dating.

## DAFTAR PUSTAKA

Andi Nugroho. (2021, August 24). *Paruh Pertama 2021, Jumlah Serangan Siber di Indonesia Capai 741,44 Juta, Melebihi Total Serangan Tahun Lalu*. Https://Cyberthreat.Id/Read/12306/Paruh-Pertama-2021-Jumlah-Serangan-Siber-Di-Indonesia-Capai-74144-Juta-Melebihi-Total-Serangan-Tahun-Lalu.

Chiradeep BasuMallick. (2022, July 27). *What Is a Brute Force Attack? Definition, Types, Examples, and Prevention Best Practices in 2022*. Https://Www.Spiceworks.Com/It-Security/Cyber-Risk-Management/Articles/What-Is-Brute-Force-Attack/.

daon001. (2018, October 9). *Indonesia Negara Ketiga Paling Sering Terkena Serangan Siber*.

IBM. (n.d.). *Apa yang dimaksud dengan serangan siber?*

P-ISSN: 1411-3635
E-ISSN: 2962-5645

Https://Www.Ibm.Com/Id-Id/Topics/Cyber-Attack.

Mathilda Gian Ayu. (2021, August 24). *Teknologi SIEM dan IBM QRadar Dapat Menghalau Serangan Siber*. Https://Www.Cloudcomputing.Id/Berita/Teknologi-Siem-Dan-Ibm-Menghalau-Serangan-Siber.