Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 3, Agustus 2025
http://doi.org/10.33395/remik.v9i3.15104
e-ISSN : 2541-1330
p-ISSN : 2541-1332

# Mitigasi Keamanan *Webserver* Sistem Informasi Akademik Terhadap Serangan *Brute force* Menggunakan *Penetration Testing*

[1]Rizqi Abdullah, [2] Fahmi Fachri
[1,2]Universitas Ma'arif Nahdlatul Ulama
Kebumen, Indonesia

[1]arrizq.abdullah12@gmail.com, [2]fahmifachriumnu@gmail.com

*Penulis Korespondensi
Diajukan : 26/07/2025
Diterima : 29/07/2025
Dipublikasi : 01/08/2025

## ABSTRAK
Meningkatnya serangan siber dan pencurian data sensitif menjadi isu krusial seiring dengan semakin banyaknya aplikasi berbasis *web* yang menyimpan informasi pengguna. Salah satu aplikasi *web* yang banyak mengalami serangan kejahatan adalah system informasi akademik. Untuk mengatasi hal ini, peneliti mempunya tujuan yaitu untuk pengujian penetrasi pada *Web Server* Sistem Informasi Akademik dilakukan untuk mengidentifikasi dan mengeksploitasi celah keamanan secara terarah, selain itu peneliti melakukan mitigasi atau perbaikan terhadap *system* tersebut agar tidak bisa disusupi kembali. Metode penelitian yang digunakan adalah *penetration testing* meliputi *Intelligence Gathering, Vulnerability Analysis, Exploitation, Post Exploitation,* dan *Reporting*. Hasil pengujian menunjukkan adanya beberapa *port* terbuka yang berpotensi memfasilitasi serangan seperti *Brute force*, bahkan memungkinkan peretas mengambil alih sistem dengan mendapatkan *username* dan *password*. Oleh karena itu, mitigasi keamanan dilakukan melalui konfigurasi *file Web Server* yang berhasil mencegah akses penyusup dan memenuhi harapan peneliti dalam meningkatkan keamanan sistem.

**Kata Kunci**: *Brute force, web*ser, mitigasi, *penetration testing* , sistem informasi akademik

## I. PENDAHULUAN
Kemajuan teknologi informasi yang semakin kompleks menciptakan proses penyebaran informasi melaju dengan cepat. Keberadaan teknologi informasi menciptakan penerimaan update berita lebih mudah. Kemudahan tersebut diiringi dengan ancaman yang berpotensi menyusup dari berbagai sisi khususnya *website*. Terlebih, jika ancaman tersebut berada pada sistem layanan publik sehingga pengguna awam cenderung tidak menyadari bahwa data pribadi sudah terekam dan berpotensi disalahgunakan oleh pihak yang tidak jujur. Keamanan pada sistem *Web Server* untuk layanan publik memiliki peran yang penting dalam menjaga kerahasian data pengguna dari *Cyberattack*. Pada umumnya para hacker meretas keamanan *Web Server* dengan memanfaatkan kerentanan sistem yang mengakibatkan terbukanya celah untuk mengakses informasi pribadi dan strategis organisasi.

Kerentanan keamanan *Web Server* diklasifikasikan menjadi tiga tingkatan: tinggi, medium, dan rendah. Sering kali, celah keamanan ini dieksploitasi oleh pihak tak bertanggung jawab untuk meretas sistem *web*. Saat ini, aplikasi berbasis tugas yang berjalan di *Web Server* menjadi krusial karena tuntutan untuk menjaga integritas informasi yang disajikan kepada pengguna. Menurut pantauan serangan siber global yang dikumpulkan oleh Badan Siber dan Sandi Negara (BSSN), Indonesia merupakan nomor dua sebagai negara yang paling banyak diserang oleh *hacker* (Pusat Operasi Keamanan Siber Nasional, 2023) seperti ditunjukan pada Gambar 1.

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 3, Agustus 2025
http://doi.org/10.33395/remik.v9i3.15104
e-ISSN : 2541-1330
p-ISSN : 2541-1332


Gambar 1. Peta sebaran serangan siber dunia
Sumber gambar : Badan Siber dan Sandi Negara

Gambar 1 menyajikan data negara-negara dengan serangan *hacker* terbanyak pada *Web Server*. Terdapat lima negara yang mendapatkan serangan paling tinggi, yaitu China dengan 53.289 serangan, Indonesia 39.957, Vietnam 28.274, Malaysia 24.723, dan India 15.419. Data BSSN tahun 2023 menyatakan bahwa peluncuran *cyber* atau *Cyberattack* mengalami lonjakan lima kali lipat dari tahun sebelumnya, dengan jumlah serangan berkisar 98 juta. Data serangan siber tahun 2023 seperti ditunjukan pada Gambar 1.2.


Gambar 2. Peta sebaran serangan siber dunia
Sumber gambar : Badan Siber dan Sandi Negara

Gambar 2 memberikan informasi data serangan yang terjadi pada periode Januari sampai Desember 2023 sebanyak 495.337.202 kasus. Berdasarkan data tersebut, Indonesia menghadapi tantangan besar dalam menjaga keamanan *Web Server*-nya dari berbagai ancaman. Beberapa kasus serangan siber terhadap *Web Server* yaitu *phising, DDOS, Brute force , defacing, security policy, SQL injection database, XSS, broken authentication, credential reuse,* dan *malware.*

Salah satu target serangan siber yaitu *Web Server* Sistem Informasi Akademik (SIA). *Web Server* SIA adalah sistem informasi krusial milik perguruan tinggi yang berfungsi sebagai repositori data akademik mahasiswa. Sistem ini mengelola berbagai jenis data yang sangat penting dan bersifat pribadi. Berangkat dari data serangan dan isu keamanan yang ada, penelitian ini berupaya

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 3, Agustus 2025 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v9i3.15104 p-ISSN : 2541-1332

untuk menguji keamanan *Web Server* SIA menggunakan metode penetration testing (pentest).

Penetration testing adalah fase pengujian yang melibatkan serangan berturut-turut terhadap *website* (Tjiptabudi & Ndaumanu, 2024). Tujuan *penetration testing* adalah untuk mengetahui celah kerentanan pada keamanan sistem. Penelitian ini memulai pengujian penetrasi dengan studi literatur komprehensif tentang metode pengujian yang relevan, diikuti dengan diskusi dan wawancara bersama pengelola *website.*

Penerapan metode tersebut untuk memberikan evaluasi terhadap keamanan *website* yang dibangun dalam virtual environment. Proses evaluasi melalui simulasi atau skenario *Cyberattack* dengan mencari kerentanan sistem. Penelitian ini dimulai dengan tahap pertama yaitu membangun *virtual environment* sesuai kebutuhan. Tahap kedua proses evaluasi keamanan dengan metode pentest untuk menemukan kerentanan sistem. Tahap ketiga melakukan analisis *Cyberattack* terhadap kerentanan dan melakukan Mitigasi keamanan pada *Web Server* SIA.

## II. STUDI LITERATUR

### 2.1 Penelitian Terdahulu

#### 2.1.1 (Alallah et al., 2025)

Penelitian menggunakan *penetration testing* dengan *OWASP Top-10* 2021 untuk menganalisis kerentanan pada *website* edukasi perusahaan *XYZ* yang menyimpan data sensitif pengguna. Penelitian ini mempertegas pentingnya penerapan *OWASP* sebagai acuan pengujian keamanan pada platform layanan pendidikan digital.

#### 2.1.2 (Dasmen et al., 2023)

Melakukan Pengujian Penetrasi Pada *Website elearning2.binadarma.ac.id* Dengan Metode Ptes *(Penetration Testing Execution Standard)*. Penelitian ini bertujuan untuk menguji keamanan *website elearning2.binadarma.ac.id* menggunakan metode *Black Box* dan *Penetration Testing Execution Standard (PTES)*. Hasilnya, teridentifikasi adanya kerentanan *Cross-Site Scripting (XSS)* yang cukup berbahaya pada *website* tersebut. Untuk penanganannya, disarankan melakukan pengecekan kerentanan *website* secara rutin.

#### 2.1.3 (Mulyanto & Algi Fari, 2022)

Penelitian ini menganalisis keamanan login router Mikrotik di SMKN 2 Sumbawa dari serangan *bruteforce* menggunakan metode *penetration testing*. Hasil *trial attack* berhasil mengekspos celah keamanan dengan mendapatkan *username* dan *password login*. Studi ini juga menyajikan solusi pencegahan serangan *bruteforce* sebagai rekomendasi bagi admin jaringan.

### 2.2 Kajian Pustaka

#### 2.2.1 Virtualisasi

*Virtualisasi* merupakan teknologi yang mengubah bentuk fisik menjadi *virtual* (Sheila, 2024). Teknologi ini berfungsi untuk menghemat sumber daya komputasi dan mengurangi biaya penelitian. Contoh pemanfaatan teknologi ini adalah simulasi jaringan komputer, penyimpanan, ujicoba serangan siber, pengembangan aplikasi, dan lain-lain. Teknologi tersebut mengurangi biaya penelitian dengan membuat sumber daya tunggal sehingga memungkinkan untuk memberikan gambaran nyata melalui *vitual reality*.

Penelitian ini menggunakan *virtualisasi* untuk membangun *lab environment* dan *Web Server* SIA sebagai wadah penelitian Mitigasi keamanan *Web Server*. Virtualisasi dalam penelitian ini membangun jaringan komputer dan *Web Server* yang bekerja seperti pada dunia nyata. Virtualisasi terdiri dari struktur *hypervisor*, perangkat keras, sistem operasi tamu, dan aplikasi.

#### 2.2.2 Penetration Testing

Pengujian penetrasi adalah tahap krusial dalam mengidentifikasi celah keamanan sistem melalui serangkaian simulasi serangan pada *website*. Tujuan utamanya adalah menemukan kerentanan yang mungkin ada. Dalam penelitian ini, proses *penetration testing* diawali dengan studi literatur komprehensif mengenai metode pengujian yang relevan, dilanjutkan dengan diskusi dan wawancara mendalam bersama pihak pengelola *website*. Kedua dengan memindai *port* dan penilaian kerentanan. Analisis akan dilakukan berdasarkan informasi yang dikumpulkan. Kontrol pada sistem akan diambil alih setelah eksploitasi karena kekerasan atau

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 3, Agustus 2025 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v9i3.15104 p-ISSN : 2541-1332

*rekayasa social* (Tahir & Risky, 2024).

**2.2.3 *Tools* Penetration Testing**

Penelitian ini secara keseluruhan menggunakan beberapa *tools* utama. Tiga dari empat *tools* berfungsi untuk *penetration testing*, *Brute force*, dan *Nmap*. *Tool* selanjutnya adalah *Wireshark* yang berfungsi sebagai alat untuk menganalisis serangan siber yang dilancarkan terhadap *Web Server* SIA. Setiap *tool* memiliki peran masing-masing sebagai berikut:

**2.2.3.1 *Brute force***

*Brute force* merupakan metode penyerangan siber di mana penyerang mencoba semua kemungkinan kombinasi *username* dan *password* untuk mendapatkan akses paksa ke sistem atau jaringan secara aktif untuk mengidentifikasi hingga mengeksploitasi kerentanan (Rahmah, 2023). Pada penelitian ini menggunakan *tool* Medusa sebagai media penyerangan terhadap *Web Server*. Medusa melakukan pemindaian aktif dengan mengirimkan berbagai permintaan yang dibuat ke aplikasi secara random, kemudian *tool* tersebut menganalisis tanggapan untuk mengumpulkan data. Data itu kemudian dimanfaatkan untuk menentukan *username* dan *password*.

**2.2.3.2 *Nmap***

*Nmap* (Network Mapper) adalah alat terbuka yang secara khusus digunakan untuk penjelajahan jaringan dan pemeriksaan keamanan suatu jaringan. *Nmap* pertama kali dikembangkan oleh Fyodor Vaskovich pada tanggal 1 september 1997 (Prana Walidin et al., 2024). Aplikasi ini digunakan untuk melakukan eksplorasi dan mengaudit jaringan yang ada. Prinsip kerja *Nmap* yaitu dengan mengirimkan paket ke target menggunakan IP asli secara kompleks sehingga dapat menentukan host yang aktif. Selain itu, *Nmap* juga melakukan serangan *Brute force* pada daftar port-nya, yang nantinya akan difilter, ditutup atau dibuka untuk menentukan status port host yang sedang aktif. Aplikasi ini mampu melihat sistem operasi lengkap dengan versi yang digunakan atau terinstal pada perangkat.

**2.2.3.3 *Wireshark***

*Wireshark* adalah alat analisis jaringan yang sangat populer, sering digunakan oleh administrator jaringan untuk berbagai keperluan. Program ini berfungsi untuk membantu pemecahan masalah jaringan, melakukan analisis mendalam, mendukung pengembangan perangkat lunak dan protokol komunikasi, serta sebagai sarana edukasi. Salah satu fitur utama *Wireshark* adalah kemampuannya untuk merekam semua paket jaringan yang melintas. Selanjutnya, *Wireshark* dapat menyeleksi dan menampilkan data tersebut dengan sangat rinci, bahkan hingga aktivitas login yang melibatkan *username* dan *password*. Ini menjadikannya alat yang tak ternilai untuk memahami lalu lintas jaringan secara detail (Rakhmadi Rahman, 2024).

**2.2.4. Mitigasi *Web Server***

Mitigasi *Web Server* dalam penelitian ini memanfaatkan metode penetration testing untuk memperoleh data kerentanan yang terdapat pada *Web Server* SIA. Penelitian ini melakukan Mitigasi keamanan berdasarkan *Vulnerability Analysis*, *Secure Code*, dan network attack behavior. Berikut penjelasan detail perihal data tersebut.

**2.2.4.1 *Vulnerability Analysis***

*Vulnerability* adalah suatu kerentanan maupun suatu kelemahan yang dapat membahayakan bagi nilai integrity (konsistensi dan keutuhuan), *confidentiality* (kerahasiaan), dan *availability* (ketersediaan dan hak akses) dari suatu *web*. Penetration testing atau yang biasa disebut pentest merupakan suatu metode yang bisa dipakai guna melaksanakan analisis dan evaluasi pada suatu jaringan maupun *website*. Selain itu, *Vulnerability* analisis penting dilakukan untuk melaksanakan prosedur perbaikan keamanan *web* dan jaringan (Hardiansyah et al., 2024). Pengujian *Vulnerability* berfungsi untuk untuk meningkatkan kesadaran pentingnya keamanan informasi (Firdaus, 2024).

**2.2.4.2 *Secure Code***

*Secure Code* merupakan teknik mengamankan sistem atau aplikasi dari *Cyberattack* menggunakan kode tertentu yang sesuai dengan prinsip keamanan dan antarmuka. Pengodean yang aman (*Secure Code*) itu sangat penting untuk keamanan karena kode adalah fondasi dari setiap aplikasi. Sama seperti membangun rumah, jika

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 3, Agustus 2025
http://doi.org/10.33395/remik.v9i3.15104
e-ISSN : 2541-1330
p-ISSN : 2541-1332

fondasinya rapuh, seluruh bangunan akan rentan terhadap kerusakan. Dalam konteks aplikasi, kode yang tidak aman membuka pintu bagi berbagai jenis serangan siber (Saragih & Zebua, 2023).

**2.2.4.3 *Network Attack Behavior***

*Cyberattack* pada umumnya selalu meninggalkan jejak ketika melakukan aktivitas. Sistem keamanan jaringan komputer pada umumnya melakukan monitoring aktivitas jaringannya untuk troubleshooting atau merekam beberapa perilaku user yang mencurigakan. Perilaku tersebut meliputi infeksi malware, serangan DOS, ransomware. Oleh karena itu salah satu pengembangan sistem keamanan berdasarkan network behavior yang di-generate dari perilaku yang mencurigakan. Setiap tindakan serangan siber menghasilkan log pada sistem jaringan komputer.

## III. METODE

### 3.1 Metode Penelitian

Metode penelitian menjelaskan langkah-langkah terurut dan sistematis tentang bagaimana penelitian dilakukan dan sebagai pedoman yang jelas untuk memecahkan masalah serta membuat analisis terhadap hasil penelitian. Metode yang digunakan dalam penelitian ini yaitu Penetration Testing.Adapun tahapan pada penelitian ini dapat dilihat pada gambar 3.


Gambar 3. Tahapan metode penetration testing
Sumber gambar : (Tahir & Risky, 2024)

Berikut adalah penjelasan tahap dari metode *penetration testing*:

1. *Intelligence Gathering* atau *Network Reconnaissance* merupakan pengumpulan informasi sebanyak mungkin tentang target sebelum melakukan serangan. Hal ini bisa lebih lanjut dibagi menjadi Aktif dan Pasif. Tahap ini melibatkan pengumpulan informasi dengan transaksi langsung seperti rekayasa sosial dan kemudian terjadi tanpa hubungan langsung.
2. *Vulnerability Analysis* atau *Service Discovery* mengacu pada identifikasi semua yang terbuka dan yang tertutup port dan bahkan untuk kerentanan yang diketahui pada target mesin. Analisis kerentanan meliputi tingkat *operating system* (OS), sistem atau bahkan jaringan.
3. *Exploitation* adalah tindakan menyerang kelemahan yang teridentifikasi dalam suatu sistem untuk menguji dan menembus keamanannya. Peretas berusaha mendapatkan eskalasi hak istimewa untuk melakukan *cracking* kata sandi, *buffer overflows*, serangan DoS, dan lain-lain. Peretas berusaha untuk mempertahankan kendali atas target dengan *backdoor*, *rootkit* atau Trojan. Mesin yang dikompromikan bahkan dapat digunakan sebagai *Bot* dan *Zombie* untuk serangan selanjutnya.
4. *Post Exploitation* yaitu perbaikan dan menerapkan solusi yang tepat sesuai kerentanan pada sistem, selanjutnya dilakukan pengujian kembali untuk memastikan kerentanan telah ditambal.
5. *Reporting* adalah memberikan ringkasan informasi secara keseluruhan mengenai kerentanan berdasarkan hasil *scanning*, pengujian, dan analisis sebelum dan sesudah perbaikan.

### 3.2 Alat dan bahan

Alat dan bahan yang digunakan dalam penelitian ini dapat dilihat sepeti pada Tabel 3.1.

Tabel 1. Alat penelitian

| No | Perangkat Smartphone | Jenis | Spesifikasi | Keterangan |
|---|---|---|---|---|

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 3, Agustus 2025
http://doi.org/10.33395/remik.v9i3.15104
e-ISSN : 2541-1330
p-ISSN : 2541-1332

| | | | | |
|---|---|---|---|---|
| 1 | Laptop Acer | *Hardware* | Aspire E5-475G | Alat Utama Penelitian |
| 2 | Parrot | *Software* | 5.10 | *Operating System* |
| 3 | Ubuntu | *Software* | 20.05 | *Operating System* |
| 4 | Apache2 | *Software* | 4.4.1 | DBMS |
| 5 | Mysql | *Software* | 7.4.3 | *Database* |
| 6 | PHP | *Software* | 7.4 | *Core Web Server* |

Sumber tabel : Peneliti

Tabel 1 menunujukkan kebutuhan selama proses penelitian. Sistem operasi parrot berfungsi sebagai komputer penyerang dan ubuntu berperan sebagai basis *Web Server*. Software untuk membangun *website* server yang meliputi PHP, Mysql, dan Apache2. Beberapa software yang digunakan untuk mendukung penelitian dalam mencari kerentanan pada sistem *Web Server* diperlihatkan pada Tabel 3.2. Software yang digunakan terbagi menjadi software scanning, attack, dan analisis.

Tabel 2. Software pendukung

| No | Software | Versi | Keterangan |
|---|---|---|---|
| 1 | *WHOIS* | *Web* App | *Software test IP Address* |
| 2 | Nikto | 2.1.6 | *Tool Scanning* |
| 3 | *Nmap* | 7.9.1 | *Tool Scanning* |
| 4 | Acunetix | 11.0 | *Tool Analysis* |
| 5 | *Wireshark* | 3.4.3 | *Tool Analysis* |
| 6 | Bruteforce | 2.2 | *Tool Pentest* |
| 7 | JavaScript | 2015 | *Generate XSS Script* |

Sumber tabel : Peneliti

Tabel 2 memberikan informasi software pendukung dalam penelitian ini. Software tersebut terdiri dari software *WHOIS* yang berfungsi untuk mengetahui IP Address public. *Nmap* merupakan *tool* yang dimanfaatkan untuk memindai kerentanan pada jaringan komputer. Acunetix dan *Wireshark* berperan sebagai *tool* analisis jaringan untuk mengetahui hal yang terjadi di dalam jaringan. *Brute force* dan JavaScript merupakan alat yang berfungsi sebagai penyerangan terhadap *website* server.

## V. HASIL DAN PEMBAHASAN

Pada simulasi kasus dilakukan kegiatan simulasi serangan dengan melakukan peninjauan dan evaluasi Sistem Informasi Akademik pada server.

### 5.1. *Intelligence Gathering*

Langkah pertama adalah *Intelligence Gathering*, yaitu salah satu proses yang paling penting dari pengujian penetrasi, karena tahap pertama di mana tindakan langsung terhadap target diambil (Ferby Septian et al., 2024)). *Intelligence Gathering* bertujuan menyelidiki masalah dan menentukan *tools* yang tepat untuk fase berikutnya. Proses pengumpulan information *Intelligence Gathering* menggunakan *tools WHOIS*, seperti pada Gambar 4

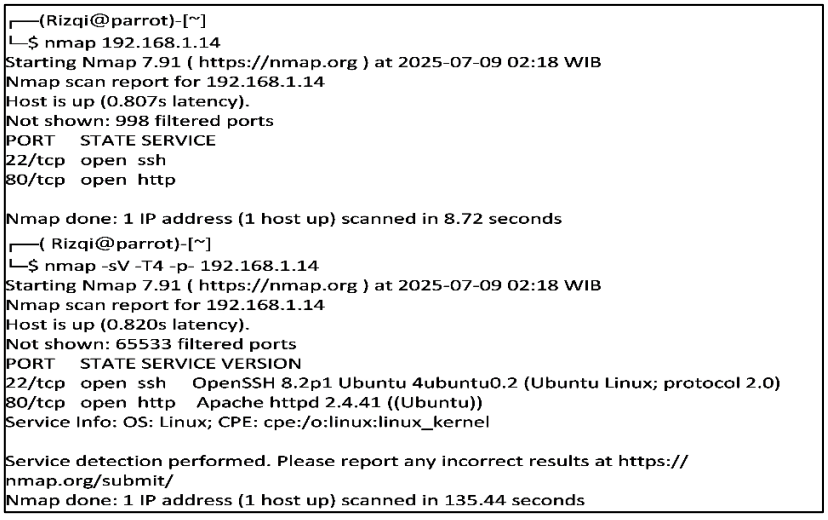
Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 3, Agustus 2025
http://doi.org/10.33395/remik.v9i3.15104
e-ISSN : 2541-1330
p-ISSN : 2541-1332


Gambar 4. Tampilan *back end Web Server*
Sumber gambar : Linux, Parrot OS

Gambar 4 menunjukkan halaman *web* pada bagian belakang atau *back-end Web Server* yang menginformasikan mengenai *server* pada saat pertama kali dibangun, mencakup tanggal didaftarkannya *Domain Name Server*, menjelaskan informasi mengenai otoritatif zona *domain* yang mengelola dan menampilkan waktu untuk *domain* kapan akan kadaluarsa dan pembaharuan pada *server*. Selain itu, aplikasi ini juga berfungsi untuk memberikan informasi terkait suatu *domain* yang tersedia atau sudah diambil oleh orang lain.

### 5.2. *Vulnerability Analysis*

Langkah kedua yaitu *Vulnerability Analysis*. *Vulnerability Analysis* adalah proses identifikasi, mengklasifikasikan, dan memprioritaskan kerentanan dalam sistem komputer, aplikasi, dan infrastruktur jaringan dan memberikan organisasi melakukan penilaian dengan pengetahuan (Dd Hassel Putra Q et al., 2025). Pencarian kerentanan pada server menggunakan *NMAP*, seperti pada Gambar 5




Gambar 5. Scanning *NMAP*
Sumber gambar : Linux, Parrot OS

Gambar 5 memberikan informasi bahwa hasil pemindaian menggunakan *Nmap* pada *server* SIA yaitu mengenai *port* pada sistem masih terbuka, salah satunya *port* 22 SSH (*Secure Shell*) dan *port* 80 HTTP (*Hypertext Transfer Protocol*) yang berjalan pada IP 192.168.1.14. *Port 22*

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 3, Agustus 2025 e-ISSN : 2541-1330
http://doi.org/10.33395/remik.v9i3.15104 p-ISSN : 2541-1332

merupakan port default untuk SSH (Secure Shell) dan SFTP (SSH File Transfer Protocol), sangat bisa digunakan untuk serangan *Brute force,* bahkan salah satu target paling umum untuk serangan *Brute force.*

### 5.3 *Exploitation*

Langkah ketiga setelah menemukan kerentanan yaitu melakukan eksploitasi, untuk melanggar semua jenis keamanan dan mengambil alih kendali jarak jauh akses jaringan, aplikasi atau sistem (Kuswara & Facrhi, 2025). Pada penelitian ini menggunakan Kerangka kerja Medusa untuk mengeksploitasi kerentanan. Melalui medusa, pentester bisa mendapatkan akses jarak jauh dari sistem. Berikut *session* serangan medusa, seperti gambar 6.

```
┌──(Rizqi@parrot)-[~]
└─$ medusa -h 192.168.1.14 -U username.txt -P password.txt -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
```

Gambar 6. Medusa *tool*
Sumber gambar : Linux, Parrot OS

Gambar 6 menampilkan perintah menjalankan *tool* Medusa untuk meretas sistem dengan berusaha mendapatkan akses masuk kedalam sistem target. Proses ini dilakukan untuk mencari *username* dan *password* dengan memasukkan beberapa kemungkinan user secara acak yang telah dibuat pada file *username*.txt. Hasil peretasan menggunakan *tool* Medusa seperti pada Gambar 7

```
ACCOUNT CHECK: [ssh] Host: 192.168.1.14 (1 of 1, 0 complete) User: server (1 of 1, 0 complete)
Password: toor123 (1271 of 2000 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.1.14 User: server Password: toor123 [SUCCESS]
┌──(Rizqi@parrot)-[~]
└─$
```

Gambar 7 Session Medusa
Sumber gambar : Linux, Parrot OS

Gambar 7 memberikan informasi dengan indikator *"ACCOUNT FOUND"* pada ssh host 192.168.1.14 yang berarti serangan *Brute force* berhasil mendapatkan *username* dan *password* untuk mengakses sistem di dalam server. Peretas dapat mengambil alih *website* dan mendapatkan semua informasi yang ada. Peretas dapat sepenuhnya mengubah, menghapus, dan memanipulasi data pada *Web Server* SIA.

### 5.4 *Post Exploitation*

Setelah tahapan *Exploitation*, maka langkah keempat yaitu *Post Exploitation*. Tahapan ini dilakukan proses perbaikan (Mitigasi) pada *Web Server* berdasarkan solusi yang tepat untuk mengatasi kerentanan dan serangan yang terjadi (Fattah et al., 2024). Penyelesaian permasalahan *password* cracking dengan menggunakan algoritma *Brute force* akan menempatkan dan mencari semua kemungkinan *password* dengan masukan karakter dan panjang *password* tertentu tentunya dengan banyak sekali kombinasi *password* (Mubarok & Romli, 2024). Cara terbaik untuk mengatasi permasalahan tersebut adalah dengan sistem untuk mencegah dari serangan atau penyusupan. *Fail2ban* merupakan paket program untuk mendeteksi usaha login yang gagal dan kemudian memblokir alamat IP host asal (M. Ridho et al., 2025).

1. Perbaikan pada *Web Server*
   Konfigurasi ssh pada rule *fail2ban* dengan perintah "sudo nano /etc/*fail2ban*/jail.local"

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 3, Agustus 2025
http://doi.org/10.33395/remik.v9i3.15104
e-ISSN : 2541-1330
p-ISSN : 2541-1332

```
  GNU nano 4.8                /etc/fail2ban/jail.local                Modified

[ssh]
enabled  = true
port     = ssh
filter   = sshd
action   = %(action_mwl)s
logpath  = /var/log/auth.log
banaction = iptables

maxretry  = 3
findtime  = 300
bantime   = 300
```

Gambar 8 Konfigurasi ssh pada file2ban
Sumber gambar : Linux, Parrot OS

Gambar 8 merupakan isi file jail.local untuk mengatur rule dan membatasi jumlah kegagalan hingga batas waktu ip addres terblokir dan deteksi pencegahan pada service ssh. Selanjutnya Konfigurasi banaction berfungsi mengirimkan informasi serangan kedalam database, dengan perintah ”sudo nano /etc/*fail2ban*/ action.d/iptables.conf

```
  GNU nano 4.8          /etc/fail2ban/action.d/iptables.conf          Modified
# Fail2Ban configuration file
#
# Author: Rizqi Abdullah
#

[INCLUDES]
before = iptables-common.conf

[Definition]

# Option:  actionstart
# Notes:   command executed on demand at the first ban (or at the start of Fail2Ban)
# Values:  CMD
actionstart = <iptables> -N f2b-<name>
              <iptables> -A f2b-<name> -j <returntype>
              <iptables> -I <chain> -p <protocol> --dport <port> -j f2b-<name>

# Option:  actionstop
# Notes:   command executed at the stop of jail (or at the end of Fail2Ban)
# Values:  CMD
actionstop = <iptables> -D <chain> -p <protocol> --dport <port> -j f2b-<name>
```

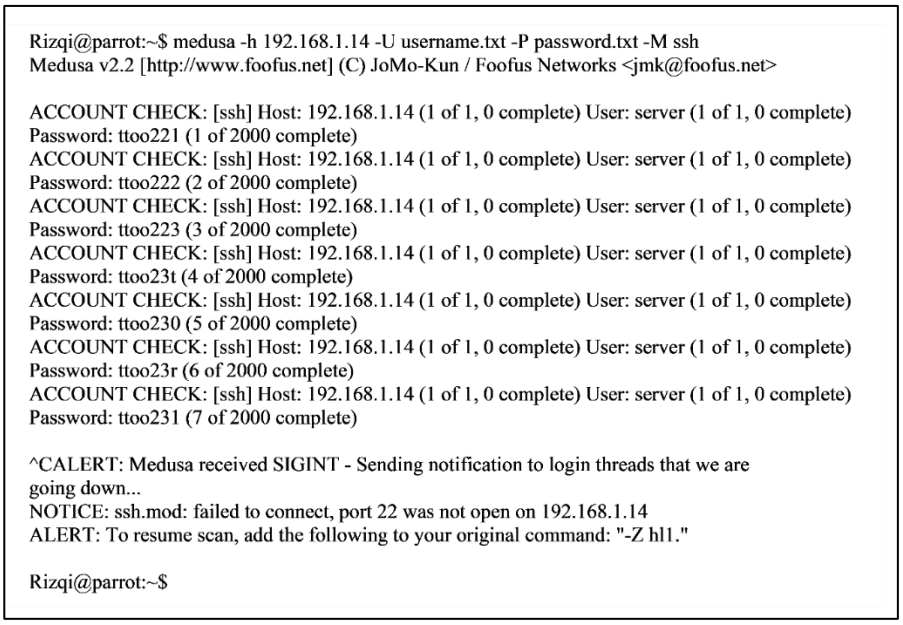
Gambar 9 Konfigurasi banaction ssh pada file2ban
Sumber gambar : Linux, Parrot OS

Pada tahap ini dilakukan agar file *fail2ban* yang bertanggung jawab untuk mengirimkan informasi ke database dapat berjalan dan membaca suatu serangan.

2. Simulasi dan Uji coba serangan

Simulasi serangan *Brute force* menggunakan *tools* medusa seperti awal dengan perintah “medusa -h 192.168.1.14 -U *username*.txt –P *password*.txt –M ssh”. Medusa adalah pemaksa *Brute force* yang digunakan untuk memaksa kredensial agar mengarah pada eksekusi dictionary atau list *password* untuk mencoba masuk (Kamil et al., 2025).

Remik: Riset dan E-Jurnal Manajemen Informatika Komputer
Volume 9, Number 3, Agustus 2025
http://doi.org/10.33395/remik.v9i3.15104
e-ISSN : 2541-1330
p-ISSN : 2541-1332




Gambar 10 Serangan ssh setelah *Fail2ban*
Sumber gambar : Linux, Parrot OS

Gambar 10 memberikan Informasi bahwa ketika File2ban dinonaktifkan maka semua serangan berhasil masuk kedalam system untuk menemukan *username* dan *password* yang valid, hal ini berbeda seperti gambar diatas bahwa *Fail2ban* dalam status Active maka semua serangan tidak berhasil masuk kedalam system untuk menemukan *username* dan *password*

### 5.5 Reporting

Tahap kelima atau terakhir dari metode Penetration testing ini yaitu reporting. Seperti pada Tabel 3. reporting.

Tabel 3. Reporting

| No | *Tools* | Exploitasi | Setelah Perbaikan |
|---|---|---|---|
| **1.** | Medusa | Sukses | Failed |
| **2.** | File2ban | Aktive | Block |

Sumber tabel : Peneliti

Tabel 3. Menampilkan Laporan pengujian kerentanan menghasilkan penerapan solusi terhadap jenis serangan *Brute force* yang dapat ditingkatkan dari yang sebelumnya bisa mendapatkan akses masuk kedalam system menjadi lebih baik dan mendapatkan penolakan saat penyusup mencoba masuk ke server dan penutupan port 22 ssh dengan status was not open. Metode Penetration testing berhasil diterapkan pada system *Web Server*.

## V. KESIMPULAN

Penerapan *Fail2ban* pada *Web Server* terbukti berhasil mencegah serangan *Brute force* dengan memblokir upaya attacker. Sebelumnya, simulasi serangan menggunakan Parrot OS dan *tools* Medusa berhasil menembus sistem dan mendapatkan *username* serta *password*, memungkinkan akses tidak sah. Oleh karena itu, perbaikan sistem dilakukan melalui konfigurasi *Fail2ban* pada server, yang sukses menggagalkan akses attacker dengan menutup celah keamanan. Metode penetration testing yang digunakan dalam simulasi serangan ini memberikan informasi penting mengenai kerentanan, membantu tim IT dalam menangani serangan pada Sistem Informasi Akademik secara lebih terstruktur dan sistematis. Hasil perbaikan *Web Server* ini telah memenuhi

e-ISSN : 2541-1330
p-ISSN : 2541-1332

harapan peneliti..

## VI. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan dan kontribusi dalam penulisan artikel ini. Secara khusus, apresiasi disampaikan kepada beliau Fahmi Fachri, S.M., M.Kom. selaku pembimbing, atas masukan dan saran yang berharga dalam penyusunan artikel ini. Penulis juga menyampaikan terima kasih kepada UMNU Kebumen, yang telah memberikan fasilitas dan dukungan selama proses penelitian dan penulisan berlangsung. Segala bentuk bantuan, baik secara langsung maupun tidak langsung, sangat penulis hargai. Semoga artikel ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan di bidang yang relevan.

## VII. REFERENSI

Alallah, A. H., Nasrullah, M., & Alhari, M. I. (2025). Penetration Testing Pada Sebuah *Website* Perusahaan Education Development Dengan Framework Owasp Top-10 Penetration Testing on an Education Development Company ' S. *Jurnal Sistem Informasi Dan Bisnis Cerdas*, *18*(2), 154–163.

Dasmen, R. N., Rasmila, R., Widodo, T. L., Kundari, K., & Farizky, M. T. (2023). Pengujian Penetrasi Pada *Website* Elearning2.Binadarma.Ac.Id Dengan Metode Ptes (Penetration Testing Execution Standard). *Jurnal Komputer Dan Informatika*, *11*(1), 91–95. https://doi.org/10.35508/jicon.v11i1.9809

Dd Hassel Putra Q, Ilham Ammarul Aziz, Eginna Gresia Br Purba, Dewa Made Wiharta, & I Gusti Ayu Garnita Darmaputri. (2025). Evaluasi Celah Keamanan dengan Metodologi *Vulnerability* Assessment Sebagai Penilaian Tingkat Kerentanan pada Domain Unud.Ac.Id. *Jural Riset Rumpun Ilmu Teknik*, *4*(1), 422–447. https://doi.org/10.55606/jurritek.v4i1.5004

Fattah, F., Putri, A. M., & Azis, H. (2024). Implementasi Metode Penetration Testing pada Layanan Keamanan Sistem Kartu Transaksi Elektronik Wahana Permainan. *Techno.Com*, *23*(1), 284–293. https://doi.org/10.62411/tc.v23i1.9488

Ferby Septian, Arfian, M. H., Asri, J. S., & Budi Tjahjono. (2024). Pengujian Keamanan *Website* dengan Metode Penetration Testing (Studi Kasus: Universitas Esa Unggul). *INNOVATIVE: Journal Of Social Science Research*, *4*(5), 3629–3647.

Firdaus, F. R. (2024). Pengembangan Sistem Informasi Sekolah Berbasis *Website* Dengan Pengujian *Website Vulnerability* dan Acceptance Testing. *The Indonesian Journal of Computer Science*, *13*(4), 6728–6742. https://doi.org/10.33022/ijcs.v13i4.4088

Hardiansyah, A., Rahmalia, M., & Putri, E. (2024). *ANALISIS KEAMANAN WEBSITE SIAKAD UNTIRTA MENGGUNAKAN TEKNIK FOOT PRINTING DAN VULNERABILITY SCANNING*. *4*(1), 26–35.

Kamil, A., Tahir, M., Juliah, S., Misfarah, M., Laviva Rahmat, A., & Dwi Mahendra, Y. (2025). Sistem Keamanan Berbasis Host-Based Intrusion Detection System (Hids) Menggunakan Wazuh. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(3), 5460–5466. https://doi.org/10.36040/jati.v9i3.14267

Kuswara, R., & Facrhi, F. (2025). Analisis Keamanan *Website* Di Smk Wongsorejo Gombong Terhadap Serangan Cross-Site Scripting (Xss) Menggunakan Penetration Testing. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(2), 2700–2707. https://doi.org/10.36040/jati.v9i2.13158

M. Ridho, M. R., Hafizh, A., Dani, I., & Ariyadi, T. (2025). Peningkatan Keamanan SSH Server Berbasis Linux melalui Implementasi *Fail2ban* dan Uji Serangan *Brute force*. *Jurnal*

e-ISSN : 2541-1330
p-ISSN : 2541-1332

*Penelitian Multidisiplin Bangsa*, *1*(12), 2206–2214. https://doi.org/10.59837/jpnmb.v1i12.431

Mubarok, K., & Romli, M. A. (2024). Implementasi Metode Rule Based dalam Mendeteksi Serangan *Brute force* pada Owncloud. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, *5*(1), 159–167. https://doi.org/10.57152/malcom.v5i1.1701

Mulyanto, Y., & Algi Fari, A. (2022). ANALISIS KEAMANAN LOGIN ROUTER MIKROTIK DARI SERANGAN BRUTEFORCE MENGGUNAKAN METODE PENETRATION TESTING (Studi Kasus: SMK NEGERI 2 SUMBAWA). *Jurnal Informatika, Teknologi Dan Sains*, *4*(3), 145–155. https://doi.org/10.51401/jinteks.v4i3.1897

Prana Walidin, A., Pebiana Putri, F., & Kiswanto, D. (2024). Kali Linux Sebagai Alat Analisis Keamanan Jaringan Melalui Penggunaan *Nmap*, *Wireshark*, Dan Metasploit. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(1), 1188–1196. https://doi.org/10.36040/jati.v9i1.12661

Rahmah, S. A. (2023). Efektifitas Penerapan Algoritma *Brute force* dan Penyalahgunaannya Dalam Sistem Berbasis *Web*. *Journal of Computers and Digital Business*, *2*(3), 112–119. https://jurnal.delitekno.co.id/index.php/jcbd/article/view/235/25

Rakhmadi Rahman, M. I. (2024). *Analisis jaringan internet menggunakan Wireshark pada warkop*. *1*, 0–3.

Saragih, N., & Zebua, T. (2023). Analisis Keamanan dan Implementasi *Secure Code* Pada Pengembangan Keamanan *Website*fikom-methodist.com Menggunakan Penetration Testing dan CVSS. *Jurnal Informatika Kaputama (JIK)*, *7*(2), 242–253. https://doi.org/10.59697/jik.v7i2.233

Sheila, S. (2024). Evaluasi Teknologi Virtualisasi Mesin Proxmox Untuk Mempersiapkan Infrastruktur Server. *(SINTESIA) : Jurnal Sistem Dan Teknologi Informasi Indonesia*, *4*(1), 11. https://journal.unj.ac.id/unj/index.php/SINTESIA/article/view/36418

Tahir, M., & Risky, M. (2024). Analisis Keamanan *Website* Dinas Pemerintahan Yogyakarta Dengan Metode PTES (Penetration Testing Execution Standard). *Jurnal Teknik Informatika UNIKA ST.Thomas (JTIUST)*, *9*, 2657–1501. https://ejournal.ust.ac.id/index.php/JTIUST/article/view/3334

Tjiptabudi, F. M. H., & Ndaumanu, R. I. (2024). Evaluasi Celah Keamanan *Website* Dana Pensiun X Melalui Penetration Testing Berdasarkan ISSAF Framework. *Jurnal Algoritma*, *21*(2), 9–17. https://doi.org/10.33364/algoritma/v.21-2.1644