UJI PENETRASI MENGGUNAKAN *HYDRA* DAN *METASPLOIT* PADA PROTOKOL SECURE SHELL

Muhammad Rizki Andrian Fitra, Ali Afrrahman S. Effendi, Selfi Audy Priscilia, Dedy Kiswanto
Ilmu Komputer, Universitas Negeri Medan
Jalan Williem Iskandar Pasar V, Medan, Sumatera Utara, Indonesia
Andrian25544@gmail.com

ABSTRAK

Perkembangan informasi dan teknologi yang semakin pesat telah mempercepat proses dalam semua kegiatan manusia. Perkembangan ini membawa manfaat besar namun juga timbulnya ancaman ketidakamanan data pada *web server*. Sebuah *web server harus* mempunyai standar keamanan internasional untuk mengurangi risiko tidak mempunyai standar keamanan dalam suatu *web* yang potensi bisa diserang oleh pihak ketiga. Kerentanan pada protokol *Secure Shell* dapat dengan mudah dimasuki oleh pihak tidak bertanggung jawab. Tujuan penelitian ini untuk mengidentifikasi kerentanan pada *web server* yang berjalan di sistem operasi Linux Ubuntu dengan menggunakan *Secure Shell*. Metode penelitian yang digunakan meliputi instalasi, konfigurasi alat penetrasi keamanan seperti *Hydra, Nikto, Nmap,* dan *Metasploit.* Hasil yang didapat menunjukkan bahwa teknik uji penetrasi yang digunakan efektif untuk mengidentifikasi celah keamanan pada *web server*.

Kata kunci : *Ubuntu, hydra, metasploit, ip address, ssh*

1. PENDAHULUAN

Perkembangan teknologi informasi yang terus meningkat telah mengubah drastis kehidupan manusia, terutama dengan kehadiran internet yang membantu untuk dapat mempermudah akses terhadap berbagai informasi baik itu melalui sebuah program aplikasi ataupun sebuah web internet. Kemampuan untuk menghubungkan jaringan komputer diseluruh dunia melalui internet membawa manfaat besar, namun juga menimbulkan tantangan baru terkait keamanan data dan informasi pada sebuah teknologi atau program [1].

Oleh karena itu, keamanan jaringan menjadi aspek yang sangat penting dengan meningkatnya volume data yang digunakan di internet. Setiap organisasi ataupun perusahaan dituntut untuk selalu menjaga kerahasiaan, integritas dan otentikasi data pada sebuah *web server* yang sesuai dengan standar keamanan internasional untuk mengurangi resiko kurangnya keamanan dalam sebuah program yang bisa berpotensi masuknya *hacker* kedalam program tersebut [2].

Salah satu keamanan jaringan yang paling sering digunakan oleh seorang administrator jaringan dalam pengelolaan server yaitu melalui *remote login* seperti *Secure Shell* (SSH). Port SSH banyak biasanya banyak digunakan dalam kemanan jaringan yang bahkan digunakan dalam keamanan jaringan sebuah perusahaan - perusahaan di Indonesia [3]. Identitas dalam sebuah jaringan komputer adalah IP Address yang merupakan protokol pengenal yang digunakan untuk memberi alamat pada tiap - tiap komputer dalam jaringan [4]. Maka karena itu dalam penelitian ini bertujuan untuk mengidentifikasi kerentanan pada *web server* yang berjalan pada sistem operasi Linux Ubuntu 20.4 dengan teknik uji penetrasi *Secure Shell* dan IP Address sebagai media pengujian kerentanan sistem keamanan pada *web server* yang ada.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terdahulu

Pada penelitian yang telah dilakukan oleh Zahra [5] membahas tentang penggunaan keamanan SSH atau *Secure Shell* dalam sistem dan juga untuk memastikan kemanan linux tidak mudah diretas dengan melibatkan dua konfigurasi sistem operasi Linux Ubuntu yang berfungsi sebagai target *Bruteforce* dan Kali Linux sebagai *Attacker* dengan menggunakan *Hydra*. Riyanti [6] menemukan bahwa keamanan *database website* masih bisa dieksploitasi melalui serangan SQL *Injection* pada sistem operasi Kali Linux yang mengungkapkan bahwa banyak *website* yang masih rentan terhadap jenis serangan SQL *Injection* sehingga mengakibatkan database yang di eksploitasi berhasil diretas. Rosaliah [7] melakukan pengujian untuk mencari sebuah celah keamanan *website* dengan melakukan testing terhadap 10 *standard* keamanan yang ada pada OWASP TOP 10 dan ditemukan sebuah celah keamanan *website* yang diperlukan untuk dilakukan perbaikan. Dewi [8] meneliti serta mencoba untuk melakukan pemindaian kerentanan *Web* profil sekolah dengan menggunakan RedHawk pada sistem operasi Kali Linux. Bimandaru [9] mengeksplorasi tentang analisis layanan keamanan hosting dengan memilih beberapa target *Website* desa.

2.2. Linux Ubuntu

Linux Ubuntu adalah salah satu sistem operasi mirip Unix yang bertujuan untuk memberi pengguna atau *user* PC sistem operasi gratis tingkat rendah yang sebanding dengan sistem Unix [10].

Ubuntu merupakan distribusi Linux yang terdiri dari banyak perangkat lunak bebas dan terbuka dan merupakan versi komersial dari Debian. Saat ini ada beberapa edisi Ubuntu, yang diperkenalkan pada 20 Oktober 2004, termasuk *Desktop*, *Server*, dan *Core* untuk dari perangkat *Internet of Things* dan robot.

Komunitas pengembang dan perusahaan British Canonical Ltd yang berkolaborasi untuk membuat sistem operasi Linux Ubuntu [11].

2.3. Web Server

Web server merupakan sebuah *software* yang akan memberikan layanan berbasis data dengan menggunakan protokol HTTP atau HTTPS dari *client* menggunakan aplikasi *web browser* untuk melakukan *request* data dan *server* akan mengirim data dalam bentuk halaman web dan pada umumnya berbentuk dokumen HTML [12].

Web server yang tangguh dalam segi kehandalan, kecepatan maupun peforma sudah menjadi hal yang wajib dimiliki oleh sebuah *Web server*. Pilihan server yang biasa dijadikan Web Server tersebut solusi terbaik adalah VPS atau Virtual Private Server, dimana user dapat me-manage sendiri dengan harga yang relatif murah [13].

2.4. Secure Shell

Secure Shell atau SSH merupakan sebuah protokol jaringan yang biasanya digunakan untuk melakukan koneksi aman ke sistem jarak jauh. SSH menyediakan mekanisme enkripsi yang aman untuk melakukan autentikasi dan mengirimkan data melalui jaringan. Protokol ini digunakan untuk mengakses sistem shell pada server atau perangkat jaringan, dan dapat juga digunakan untuk mengirim perintah dan menerima respons dari sistem jarak jauh [14].

SSH atau *Secure Shell* dibuat sebagai sebuah solusi pengganti protokol Telnet yang tidak aman, yang mentransmisikan data dalam bentuk teks biasa tanpa enkripsi, sehingga rentan terhadap penyadapan. Tujuan utama dari SSH adalah memberikan akses jarak jauh yang aman keperangkat atau server melalui jaringan yang tidak benar - benar aman, seperti Internet. Sehingga ini memungkinkan pengguna untuk mengontrol dan mengelola perangkat tanpa harus berada di lokasi fisik perangkat.Salah satu fitur utama SSH adalah enkripsi [15].

2.5. IP Address

IP Address adalah sebuah bilangan bulat biner 32 - bit yang dapat direpresentasikan sebagai empat kolom nilai desimal yang dipisahkan oleh titik. IP address harus digunakan secara unik, sehingga satu jaringan tidak boleh menggunakan IP Address yang sama [16].

IP Address merupakan sebuah pengidentifikasian dari setiap host di jaringan internet . Yang berarti hal ini akan menyebabkan tidak ada host lain yang dapat bergabung ke internet menggunakan IP Address yang sama. Untuk berkomunikasi satu sama lain, setiap komputer harus memiliki alamat yang disebut sebagai alamat IP [17].

2.6. Virtual Private Server

Virtual Private Server atau VPS adalah sebuah server pribadi yang dimana keseluruhan *resource* digunakan oleh satu user saja dan tidak dipengaruhi oleh user lainnya [18].

Setiap VPS memiliki IP *address*, *port number*, *tables*, *filtering*, dan *routing rules* sendiri yang ada pada VPS yang dimiliki oleh user yang menggunakan VPS untuk sebuah server. VPS juga dilengkapi dengan *control panel* untuk mengelola *script*, *users*, pemrosesan, file sistem *backup restore* dan fitur lainnya yang dimana VPS bekerja seperti sebuah server yang terpisah memiliki sebuah *processes*, *users*, *files* dan menyediakan *full root access* [19].

2.7. Hydra

Hydra adalah sebuah alat atau perangkat lunak *cracker login* yang digunakan di berbagai sistem operasi seperti Kali Linux, Parrot, serta Linux Ubuntu. *Hydra* bekerja dengan menggunakan serangan *brute force* untuk menebak kombinasi nama pengguna dan kata sandi yang tepat [20].

Hydra juga dapat digunakan untuk memecahkan password suatu server sehingga mengakibatkan resiko data - data penting tercuri dari server [21].

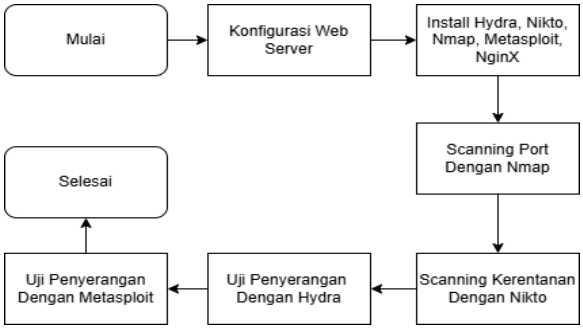
2.8. Metasploit

Metasploit adalah salah satu sebuah platform atau framework penetrasi *open source* yang menyediakan alat dan berbagai modul untuk melakukan pengujian keamanan dan eksploitasi pada server ataupun sebuah program pada internet [22].

Metasploit biasanya menyediakan antarmuka pengguna grafis atau biasa disebut dengan GUI dan baris perintah (*command line*), yang memungkinkan para pengguna untuk menentukan dan mengontrol pengujian penetrasi pada server dengan sedikit mudah melalui modul yang ada. *Metasploit* juga memiliki celah keamanan yang terus diperbarui sehingga cukup memudahkan pengguna untuk menemukan suatu celah keamanan pada sistem yang ingin mereka uji [23].

3. METODE PENELITIAN

Metode yang digunakan pada penelitian ini melibatkan beberapa tahapan seperti proses konfigurasi, installasi, *scanning*, dan pengujian kerentanan dari *web server*. Tahapan - tahapan pada penelitian ini memanfaatkan program - program yang ada untuk melakukan penetrasi keamanan *web server*. Alur dari penelitian dapat dilihat pada gambar 1 :

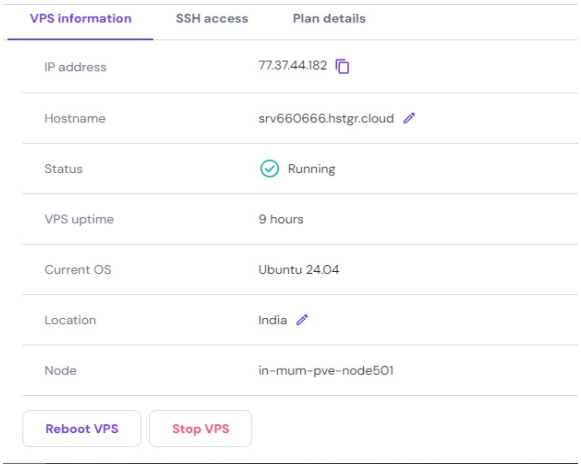


Gambar 1. Alur penelitian

Dapat dilihat pada Gambar 1. dapat dilihat alur penelitian yang dilakukan, yang pertama adalah dengan melakukan konfigurasi web server, kemudian melakukan proses installasi program - program yang digunakan untuk melakukan penetrasi yaitu *Hydra, Nikto, Nmap, Metasploit,* dan *NginX*.

3.1. Konfigurasi Web Server

Pada tahap pertama dilakukan pembelian *web server* pada website yang ingin dituju. Jika sudah masuk kedalam website yang ingin dituju kemudian login dengan menggunakan akun Google, setelah login pilih menu VPS lalu pilih "Get a new VPS plan" kemudian pilih kernel base virtual machined yang ingin digunakan. Disini peneliti memilih KVM 1, kemudian selesaikan transaksi dengan membayar menggunakan *E-Wallet* atau akun pembayaran virtual lainnya. Setelah melakukan pembayaran, kita akan memilih OS yang akan digunakan dan lokasi, pada penelitian ini menggunakan OS Ubuntu dan untuk lokasi berada di India. Setelah transaksi selesai maka pihak penyedia *web server* akan memberikan VPS information yang berisi IP Address, Hostname, dan SSH Access yang dapat dilihat pada Gambar 2 :

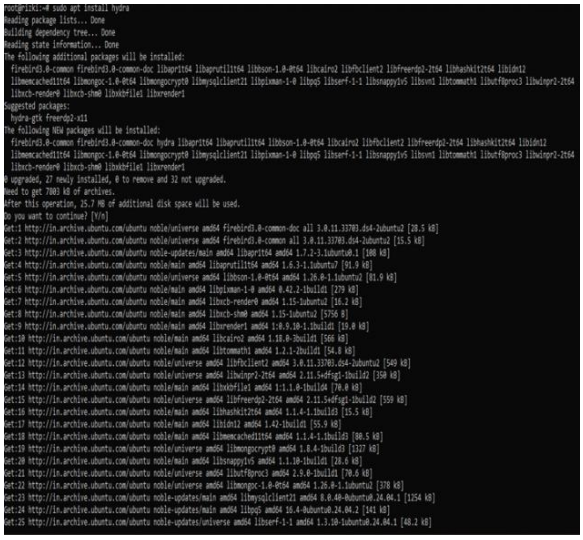


Gambar 2. Informasi vps

Dapat dilihat pada Gambar 2. dapat dilihat terdapat informasi VPS yang telah dibeli. Pada informasi VPS ini terdapat IP Address yang diberikan oleh pihak penyedia web server, kemudian ada Hostname, sistem operasi yang digunakan dan terdapat akses SSH yang berisi username dan password untuk masuk kedalam *web server*.

3.2. Installasi *Hydra*

Pada tahap kedua dilakukan installasi *Hydra* sebagai alat penetrasi yang akan berfungsi sebagai program yang akan menyerang SSH *web server* yang dapat dilihat pada Gambar 3 :



Gambar 3. Installasi *hydra*

Pada Gambar 3. dapat dilihat terdapat sebuah perintah untuk melakukan installasi program *Hydra* yang akan digunakan sebagai alat penetrasi uji keamanan *web* server dengan menggunakan SSH dan IP Address. Yang pertama masukkan perintah "sudo apt update", perintah ini berfungsi untuk memastikan sistem memiliki informasi terbaru tentang paket - paket yang tersedia dan versinya sebelum menginstall. Yang kedua masukkan perintah "sudo apt install hydra", perintah ini berfungsi untuk menginstall program *Hydra* yang akan melakukan *Bruteforce attack* terhadap berbagai layanan jaringan yang ada dengan mencari username dan password yang ada.

3.3. Installasi Nikto

Pada tahap ketiga dilakukan installasi *Nikto* sebagai alat penetrasi yang akan berfungsi sebagai scanning terhadap *web server* dan mengidentifikasi kerentanan yang terdapat pada *web server* yang dapat dilihat pada Gambar 4 :

Gambar 4. Installasi *nikto*

Pada Gambar 4. dapat dilihat terdapat perintah untuk melakukan installasi program Nikto yang akan berfungsi untuk melakukan scanning kerentanan yang lainnya yang dapat di eksploitasi. Yang pertama masukkan perintah "sudo apt install perl", perintah ini berfungsi untuk menginstall bahasa pemrograman pada sistem yang akan digunakan untuk Nikto. Yang kedua masukkan perintah "sudo apt install nikto" perintah ini berfungsi untuk melakukan pemindaian atau scanning terhadap web dan mengidentifikasi kerentanan yang ada.

3.4. Installasi *Nmap*

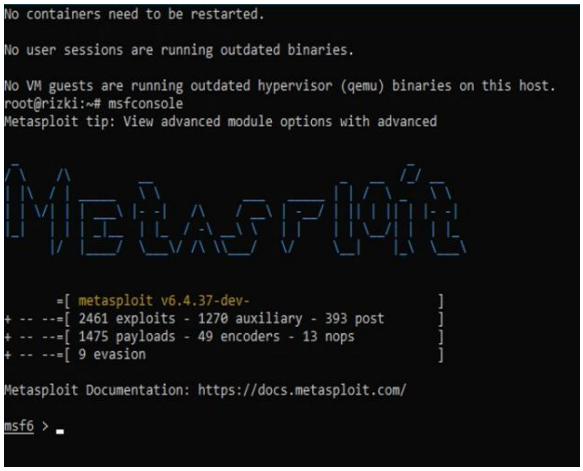
Pada tahap keempat dilakukan installasi *Nmap* sebagai alat penetrasi yang akan berfungsi sebagai scanning terhadap *web server* dan mengidentifikasi perangkat yang terdapat pada *web server* yang dapat dilihat pada Gambar 5 :

Gambar 5. Installasi *nmap*

Pada Gambar 5. dapat dilihat bahwa dilakukan proses intallasi paket yang akan digunakan yaitu *Nmap*. Yang pertama masukkan perintah "sudo apt update", perintah ini berfungsi untuk memastikan sistem memiliki informasi terbaru tentang paket - paket yang tersedia dan versinya sebelum menginstall. Yang kedua masukkan perintah "sudo apt install nmap", perintah ini berfungsi untuk menginstall program map yang akan melakukan pemindaian atau *scanning* jaringan, mengidentifikasi perangkat keras, dan menganalisis jaringan.

3.5. Installasi *Metasploit*

Pada tahap kelima akan dilakukan installasi *Metasploit* yang akan menjadi sebuah alat yang membantu untuk melakukan sebuah pengujian keamanan dan berbagai percobaan penyerangan terhadap *web* yang dapat dilihat pada Gambar 6 :

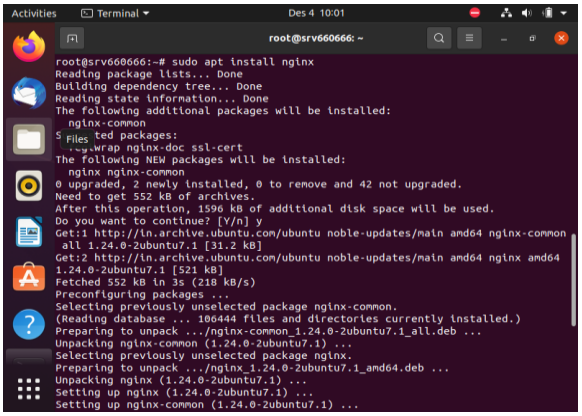


Gambar 6. Installasi *metasploit*

Pada Gambar 6. dapat dilihat bahwa penginstallan Metasploit berhasil dilakukan. Adapun terdapat beberapa langkah - langkah untuk melakukan installasi Metasploit. Yang pertama masukkan perintah "sudo apt update", yang berfungsi untuk memastikan sistem memiliki informasi terbaru tentang paket yang tersedia dan versinya sebelum menginstal. Yang kedua masukkan perintah "sudo apt install -y curl gnupg2", yang berfungsi untuk menginstall dua paket perangkat lunak curl dan gnupg2 yang berfungsi untuk melakukan transfer data dan interaksi dengan API dan gnupg yang berguna untuk enkripsi yang penting untuk keamanan data. Yang ketiga masukkan sebuah perintah untuk mengakses key yaitu "curl https://apt.metasploit.com/metasploit-framework.gpg.key|sudo apt-key add-", yang berfungsi untuk menambahkan kunci akses GPG untuk repositori Metasploit Framework kedalam sistem operasi. Yang keempat masukkan perintah "echo "deb http://apt.metasploit.com/buster main"| sudo tee /etc/apt/sources.list.d/metasploit-framework.list", untuk menambahkan repositori Metasploit . Yang kelima masukkan kembali perintah "sudo apt update". Yang keenam masukkan perintah "sudo apt install metasploit-framework",untuk menginstall Metasploit Framework di sistem operasi yang berfungsi untuk melakukan pengujian keamanan.

3.6. Installasi *NginX*

Pada tahap keenam dilakukan installasi *NginX* yang akan berfungsi sebagai *web server* dalam sistem operasi Linux Ubuntu yang dapat dilihat pada Gambar 7 :

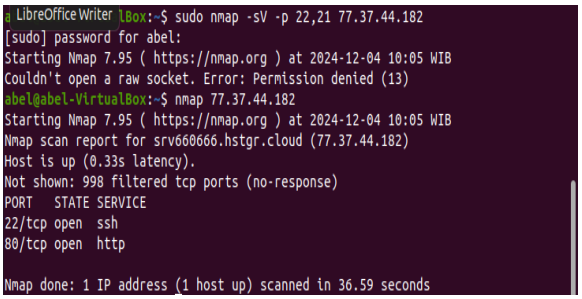


Gambar 7. Installasi *nginx*

Dapat dilihat pada Gambar 7. dapat dilihat bahwa diperlukan installasi *NginX* untuk berfungsi sebagai *web server* pada sistem operasi. Untuk melakukan installasi *NginX* dapat dilakukan dengan memasukkan perintah "sudo apt install nginx", yang berfungsi untuk menginstall program nginx kedalam sistem operasi yang digunakan.

3.7. Scanning Port Dengan *Nmap*

Pada tahap ketujuh akan dilakukan *scanning* atau pemindaian dengan menggunakan *Tools Nmap* yang dapat dilihat pada Gambar 8 :

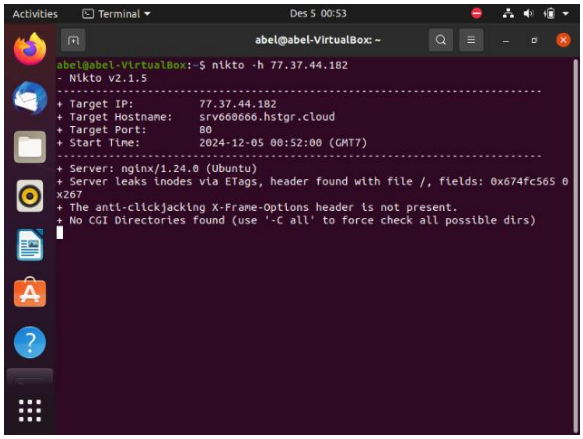


Gambar 8. Scanning port dengan nmap

Dapat dilihat pada Gambar 8. dapat dilihat bahwa dengan menggunakan perintah "sudo nmap -sv -p 22,21 (IP Address yang dituju)", maka *tools nmap* akan mengakses serta akan mencari port ssh dan http yang terbuka. Pada gambar dikatakan bahwa port 22 terbuka sehingga proses penetrasi akan dilanjutkan dengan menggunakan *nikto* untuk dilakukan pemindaian pada IP Address.

3.8. Scanning Dengan *Nikto*

Pada tahap yang kedelapan akan dilakukan pemindaian untuk mencari kerentanan lainnya pada *web server* dengan menggunakan *Tools Nikto* yang dapat dilihat pada gambar 9 :

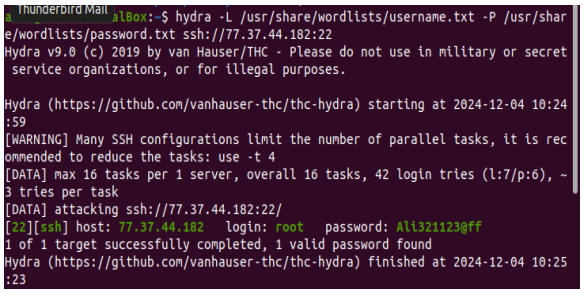


Gambar 9. *Scanning ip address* dengan *nikto*

Dapat dilihat pada Gambar 9. proses *scanning* untuk mencari kerentanan pada *web server* berhasil dilakukan melalui kelemahan pada IP Address dengan perintah "nikto -h (IP Address yang dituju).

3.9. Uji Penyerangan *Hydra*

Pada tahap yang kesembilan akan dilakukan uji penyerangan dengan menggunakan *Tools Hydra* dengan menggunakan algoritma *Bruteforce* yang dapat dilihat pada Gambar 10 :

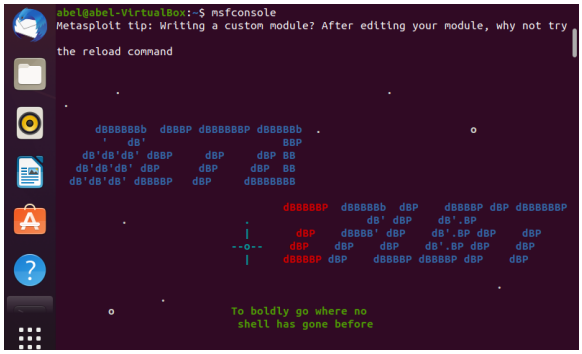


Gambar 10. Uji penyerangan *hydra*

Dapat dilihat pada Gambar 10. dapat dilihat penyerangan dengan menggunakan *Hydra* dan menyerang port SSH dengan menggunakan *Bruteforce* akan mencari seluruh data secara acak kemudian data akan dikumpulkan kembali dan dicocokan untuk mencari hasil yang valid. Untuk melakukan pengujian serangan *Hydra* dengan menggunakan perintah "hydra -L/usr/share/wordlists/username.txt -P /usr/share/wordlists/password.txt SSH://(Ip Address yang dituju):(Port SSH yang dituju). Proses pengujian dimulai dengan pemindaian awal menggunakan *Nmap* untuk mengidentifikasi port yang terbuka. Setelah itu, *tools hydra* akan menyerang menggunakan *Bruteforce* terhadap SSH dengan mencoba berbagai kombinasi file username dan password yang telah dibuat didalam direktori wordlists. Kemudian pada tahap selanjutnya, setelah username dan password berhasil didapatkan, maka penyerang dapat melakukan apa saja terhadap *web server* yang ada pada sistem operasi.

3.10. Uji Penyerangan *Metasploit*

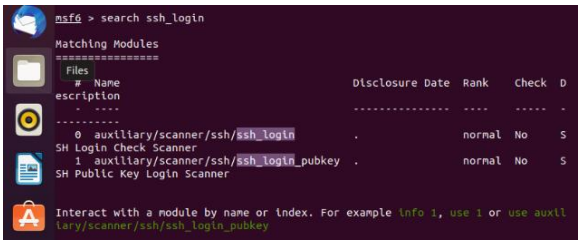
Pada tahap kesepuluh dilakukan sebuah uji coba penyerangan dengan menggunakan *Metasploit* yang dapat dilihat pada Gambar 11 :



Gambar 11. Masuk ke *metasploit*

Dapat dilihat pada Gambar 11. Untuk melakukan penyerangan menggunakan *metasploit* hal pertama yang dilakukan adalah masuk ke *metasploit* dengan menggunakan perintah "msfconsole", maka pengguna akan masuk kedalam *framework metasploit*.

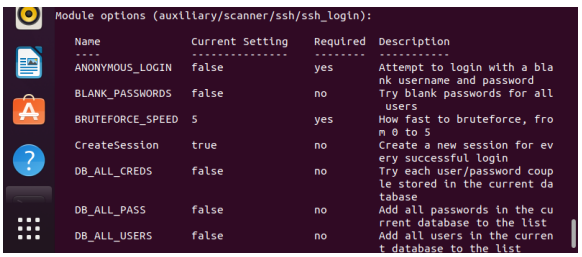
Setelah masuk ke *framework metasploit* lakukan *search* modul untuk melakukan eksploitasi terhadap SSH dengan menggunakan perintah "ssh_login" yang dapat dilihat pada Gambar 12 :



Gambar 12. SSH_login

Dapat dilihat pada Gambar 12. Terdapat 2 modul yang dapat digunakan untuk melakukan eksploitasi terhadap SSH, untuk langkah selanjutnya adalah dengan memilih modul yang sesuai dengan menggunakan perintah "use (nomor modul)".

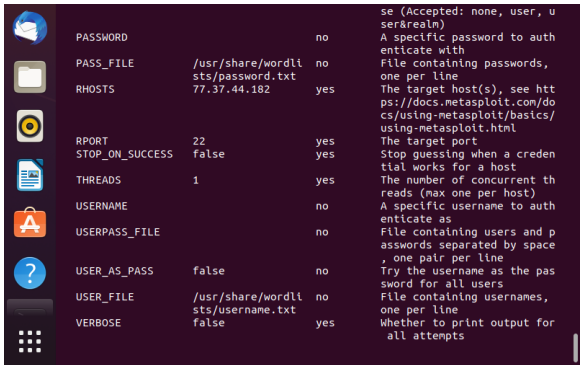
Setelah memilih modul yang sesuai, maka akan dilakukan sebuah cek yang akan memastikan bahwa *required* (syarat) pada modul sudah terisi terutama pada modul yang pada bagian *required* menyatakan yes, yang dapat dilihat pada Gambar 13 :



Gambar 13. Ubah *required*

Dapat dilihat pada Gambar 13. Pengguna harus melakukan konfigurasi parameter RHOSTS pada modul untuk menentukan alamat IP yang igin dieksploitasi dengan menggunakan perintah "set RHOSTS (IP Address)". Setelah melakukan setting RHOSTS kemudian lakukan hal yang sama pada USER_FILE untuk daftar username dengan perintah "set USER_FILE /usr/share/wordlists/username.txt". Setelah melakukan setting pada USER_FILE maka selanjutnya adalah melakukan setting pada PASS_FILE untuk dafttar password dengan menggunakan perintah "set PASS_FILE /usr/share/wordlists/password.txt.

Setelah melakukan megubah setting pada *required* yang dituju dan terisi dengan benar, maka selanjutnya akan melihat kembali dengan perintah "options", yang akan menampilkan seluruh modul yang ada pada modul 0, yang dapat dilihat pada Gambar 14 :



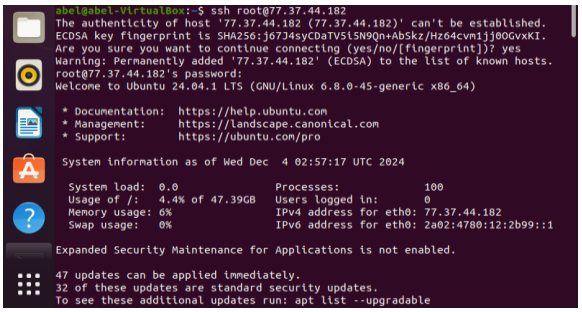
Gambar 14. *Required* setelah diubah

Dapat dilihat pada Gambar 14. Perubahan yang dilakukan pada RHOSTS, USER_FILE dan PASS_FILE telah berhasil diubah dengan ketentuan yang telah dilakukan.

4. HASIL DAN PEMBAHASAN

Setelah melakukan seluruh konfigurasi serta penginstalan *tools* dan juga melakukan pengaturan sistem yang dibutuhkan untuk pengujian penetrasi *web server*, maka akan dilakukan pengecekan yang menampilkan bahwa uji penetrasi telah berhasil dilakukan dalam mengidentifikasi kerentanan keamanan *web server*, seperti port yang terbuka. Alat - alat yang digunakan pada penelitian seperti *Nmap*, *Nikto*, *Hydra*, dan juga *Metasploit* digunakan untuk menemukan sebuah kerentanan melalui tindakan eksploitasi dengan serangan *Bruteforce*.

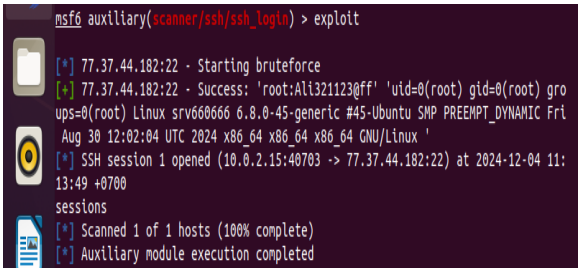
Berikut adalah hasil dari uji coba penetrasi *web server* dengan menggunakan *Tools Hydra* yang terdapat pada Gambar 15 :



Gambar 15. Login root dengan SSH

Dapat dilihat pada Gambar 15. Percobaan login root *web server* dengan menggunakan SSH yang telah diperoleh melalui *Hydra.* Kombinasi username dan password ditemukan setelah sejumlah besar percobaan *Bruteforce* dengan menggunakan wordlists. Setelah username dan password berhasil didapatkan, maka penyerang akan masuk kedalam sistem dengan login menggunakan SSH username dan password, yang dimana setelah penyerang berhasil login kedalam *web server* melalui root maka penyerang dapat melakukan apa saja terhadap sistem operasi yang ada di *web server* pengguna.

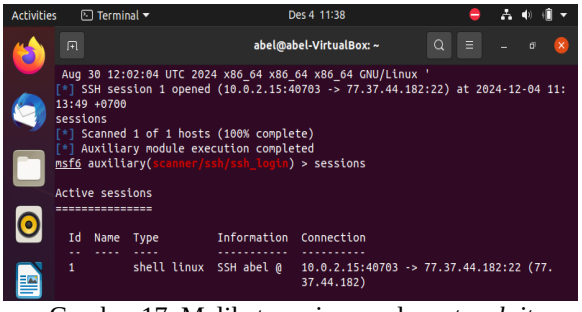
Kemudian berikut adalah hasil uji coba penetrasi *web server* dengan menggunakan *Tools Metasploit* yang terdapat pada Gambar 16 :



Gambar 16. Penetrasi web dengan *metasploit*

Dapat dilihat pada Gambar 16. Penetrasi web telah berhasil dilakukan yang dimana *Metasploit* akan menampilkan hasil pemindaian yang telah berhasil mendapatkan data yang diperlukan serta menunjukkan sebuah informasi username dan password dari pengguna.

Selanjutnya, penyerang akan melihat *sessions* yang aktif pada *web server* pengguna setelah kredensial login ditemukan yang terdapat pada Gambar 17 :



Gambar 17. Melihat *sessions* pada *metasploit*

Dapat dilihat pada Gambar 17. Jika eksploitasi dengan *metasploit* berhasil dilakukan maka penyerang bisa melihat *sessions* atau periode waktu penggunaan *web server* yang dimana pada *sessions*, sistem akan menampilkan informasi dan koneksi dari IP Address yang digunakan pada sistem operasi.

5. KESIMPULAN DAN SARAN

Berdasarkan pengujian penetrasi *web server* dengan menggunakan berbagai alat keamanan, yaitu *Nmap*, *Nikto*, *Hydra*, dan *Metasploit*. *Nmap* berhasil mengidentifikasi port yang terbuka pada *web server* penggun. *Nikto* melakukan pemindaian terhadap *web server* dan berhasil menemukan sejumlah kerentanan. Selanjutnya, Hydra menerapkan metode Bruteforce untuk menemukan kredensial login SSH dengan menggunakan wordlists, dan berhasil menemukan kombinasi username dan password. Metasploit digunakan untuk melanjutkan eksploitasi dan berhasil mendapatkan sessions aktif di web server pengguna. Dari sini, penyerang dapat melakukan apa saja terhadap web server pengguna. Oleh karena itu, pengujian penetrasi web server dapat dianggap berhasil dilakukan dengan hasil penyerang masuk ke dalam sistem pengguna dengan username dan password SSH yang berhasil ditemukan.. Selain itu, disarankan untuk penelitian lebih lanjut, diharapkan untuk melakukan mencoba mengembangkan sistem keamanan dari serangan *Hydra* dan *Metasploit* serta diharapkan untuk melakukan pengujian teknik penetrasi *web* lebih lanjut dengan menggunakan *tools* yang lain seperti SQL Map ataupun dengan menggunakan Dirb.

DAFTAR PUSTAKA

[1] G. Pradita and A. Pramono, “Implementasi Monitoring Keamanan Jaringan Pada Server Ubuntu Menggunakan Snort Intrusion Detection Prevention System (Idps) Dan Telegram Bot Sebagai Media Notifikasi Di Pt Ss Utama,” *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 4, pp. 5827–5834, 2024, doi: 10.36040/jati.v8i4.10069.

[2] F. Fachri, A. Fadlil, and I. Riadi, “Analisis Keamanan Webserver menggunakan Penetration Test,” *J. Inform.*, vol. 8, no. 2, pp. 183–190, 2021, doi: 10.31294/ji.v8i2.10854.

[3] R. Wiryadinata, R. Bangun Keamanan, and K. Kunci, “Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode Port Knocking INFORMASI ARTIKEL ABSTRAK,” *Jikomsi*, vol. 5, no. 1, pp. 28–33, 2022.

[4] D. R. Az Zahra, F. P. Ilham, H. N. Ramdhani, and A. Setiawan, “Penerapan dan Pengujian Keamanan SSH Pada Server Linux menggunakan Hydra,” *J. Internet Softw. Eng.*, vol. 1, no. 3, p. 10, 2024, doi: 10.47134/pjise.v1i3.2627.

[5] A. Riyanti, B. M. Rahmanto, D. R. Hardianto, R. D. A. Yuristiawan, and A. Setiawan, “Uji

Penetrasi Injeksi SQL terhadap Celah Keamanan Database Website menggunakan SQLmap," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 9, 2024, doi: 10.47134/pjise.v1i4.2623.

[6] J. J. B. H. Yum Thurfah Afifa Rosaliah, "Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM," *Senamika*, vol. 2, no. September, pp. 752–761, 2021.

[7] S. A. Dewi, M. Rizqi, W. Nor, P. Studi, S. Informasi, and F. Teknik, "Pemindaian Kerentanan Web Profil Sekolah Menggunakan RedHawk di Kali Linux Vulnerability Scanning Web Profile School Using RedHawk on Kali Linux," pp. 1–8, 2024.

[8] A. Bimandaru, A. Alamsyah, and A. Nugroho, "ANALISIS PENGUJIAN PENETRASI PADA LAYANAN HOSTING MENGGUNAKAN METODE BLACK BOX (Studi kasus : Blogspot, Wordpress dan Shared Hosting)," *Foristek*, vol. 14, no. 1, 2023, doi: 10.54757/fs.v14i1.238.

[9] Vivin Salama and Alfhian Makmur, "Pembatasan Hak Akses Kinerja Jaringan Wlan Berbasis Linux Ubuntu Pada Smk Kristen Padang Sappa," *BANDWIDTH J. Informatics Comput. Eng.*, vol. 2, no. 1, pp. 20–37, 2024, doi: 10.53769/bandwidth.v2i1.595.

[10] A. Hidayatullah *et al.*, "Impelementasi Sistem Operasi Server Linux Ubuntu untuk Server NAS menggunakan TRUENAS," vol. 3, pp. 11338–11346, 2024.

[11] G. H. A. Kusuma, "Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19," *J. Informatics Adv. Comput.*, vol. 2, no. 1–2, pp. 37–37, 2021, doi: 10.1515/zwf-1997-921-220.

[12] Fandy, Rosmasari, and G. M. Putra, "Pengujian Kinerja Web Server Atas Penyedia Layanan Elastic Cloud Compute (EC2) Pada Amazon Web Services (AWS)," *Adopsi Teknol. dan Sist. Inf.*, vol. 1, no. 1, pp. 21–35, 2022, doi: 10.30872/atasi.v1i1.45.

[13] T. Ariyadi, M. Rizky, M. K. Hadi, and A. A. Widodo, "Implementasi Firewall Pada Protokol SSH Linux Ubuntu Menggunakan Iptables," *Semin. Ris. Mahasiswa-Computer Electr. (SERIMA-CE*, vol. 1, no. 1, pp. 170–175, 2023.

[14] M. A. H. Usman, Ansharullah Patiroi, Rizki Yusliana Bakti, "Arus Jurnal Sains dan Teknologi (AJST) Optimalisasi Sistem Keamanan SSH dari Serangan Brute Force," *J. Sains dan Teknol.*, vol. 2, no. 1, pp. 116–122, 2024.

[15] R. Arfind, H. Supendar, and Riza Fahlapi, "Perancangan Virtual Private Network Dengan Metode PPTP Menggunakan Mikrotik," *Jka*, vol. 1, no. 3, pp. 108–116, 2023.

[16] Sikarti Sikarti, Feri Febrian Syah, Alifia Rukmi Candra Dewi, and Didik Aribowo, "Simulasi Perencanaan Jaringan Transport Metro Ethernet Menggunakan Aplikasi Cisco Packet Tracer Versi 6.2.0," *Simpati*, vol. 1, no. 2, pp. 31–39, 2023, doi: 10.59024/simpati.v1i2.152.

[17] C. Gea, K. J. D. Lase, and M. Syamsudin, "Implementasi Virtual Private Server untuk Mini Hosting," *J. Sains Dan Komput.*, vol. 7, no. 01, pp. 5–9, 2023, doi: 10.61179/jurnalinfact.v7i01.402.

[18] M. Syani and B. Saputro, "Implementasi Remote Monitoring Pada Virtual Private Server Berbasis Telegram Bot Api (Studi Kasus Politeknik Tedc Bandung," *J. SISKOM-KB (Sistem Komput. dan Kecerdasan Buatan)*, vol. 4, no. 2, pp. 94–111, 2021, doi: 10.47970/siskom-kb.v4i2.190.

[19] M. R. Sampurna, "NetPLG Journal of Network and Computer Applications Implementasi Hydra, FFUF, dan WFUZZ dalam Brute Force DVWA," *J. Netw. Comput.*, vol. 1, no. 2, pp. 102–112, 2022, [Online]. Available: https://jurnal.netplg.com/

[20] A. D. Batistuta, A. H. Hendrawan, and Ritzkal, "Analisis Keamanan Jaringan Server Terhadap Serangan Dictionary Menggunakan Tools Fail2Ban Dengan Notifikasi Telegram," *INFOTECH J.*, vol. 10, no. 1, pp. 64–73, 2024, doi: 10.31949/infotech.v10i1.8730.

[21] S. Alhidamkara and I. L. Kharisma, "Analisis Keamanan Dan Eksploitasi Kernel Android 13 Menggunakan Metasploit Reverse _ Tcp," vol. 5, no. 3, pp. 845–856, 2024.

[22] M. Fadhol and R. D. Marcus, "Implementasi Honeypot Dionaea Sebagai Uji Kerentanan dan Penunjang Keamanan Jaringan," *Semin. Nas. Sist. Inf.*, no. September, pp. 3807–3817, 2023.