(2024), 2 (11): 136–150 **Scientica** 3021-8209
Jurnal Ilmiah Sain dan Teknologi

ANALISIS KEAMANAN JARINGAN PADA *WEB SERVER* MENGGUNAKAN *METASPLOIT FRAMEWORK* DENGAN METODE *INFORMATION SYSTEM SECURITY ASSESMENT FRAMEWORK* (ISSAF) PADA SMKN XYZ

Priatna Sandika [1], Yusuf Muhyidin [2], Dayan Singasatia [3]
Program Studi Teknik Informatika S1, Fakultas Teknik, Sekolah Tinggi Teknologi Wastukancana
Jl. Cikopak No.53, Sadang, Purwakarta, Jawa Barat, Indonesia

Abstract
This research aims to analyze the network security of a web server using the Metasploit Framework with the Penetration Testing and ISSAF (Information System Security Assessment Framework) methods. The case study was conducted on the web server of SMKN XYZ. The research methodology employed was penetration testing, involving several stages from planning and preparation, assessment, to cleanup and artifact removal. This study successfully identified several security vulnerabilities on the web server that could be exploited by malicious actors. Using the Metasploit Framework, the researchers simulated attacks to exploit the discovered vulnerabilities and tested the effectiveness of the mitigation measures taken. The results indicate that implementing the security measures recommended by ISSAF can significantly reduce security risks and enhance protection against attacks. The conclusion of this research is that the use of the Metasploit Framework together with ISSAF is an effective approach to identifying and addressing security vulnerabilities on web servers. These findings are expected to serve as a reference for other educational institutions in strengthening their network security.

Article History
Submitted:19 Juli 2024
Accepted: 24 Juli 2024
Published: 25 Juli 2024

Key Words
Network Security, Web Server, Metasploit Framework, Penetration Testing, ISSAF

Abstrak
Penelitian ini bertujuan untuk menganalisis keamanan jaringan pada *web server* menggunakan Metasploit Framework dengan metode Penetration Testing dan ISSAF (*Information System Security Assessment Framework*). Studi kasus dilakukan di *web server* SMKN XYZ. Metode penelitian yang digunakan adalah *penetration testing*, yang melibatkan beberapa tahapan mulai dari perencanaan dan persiapan, penilaian, hingga pembersihan dan penghapusan artefak. Penelitian ini berhasil mengidentifikasi beberapa celah keamanan pada *web server* yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Dengan menggunakan Metasploit Framework, peneliti melakukan simulasi serangan untuk mengeksploitasi kerentanan yang ditemukan dan menguji efektivitas tindakan mitigasi yang diambil. Hasilnya menunjukkan bahwa penerapan langkah-langkah keamanan yang direkomendasikan oleh ISSAF dapat secara signifikan mengurangi resiko keamanan dan meningkatkan perlindungan terhadap serangan. Kesimpulan dari penelitian ini adalah bahwa penggunaan Metasploit Framework bersama dengan ISSAF merupakan pendekatan yang efektif dalam mengidentifikasi dan mengatasi kerentanan keamanan pada *web server*.

Sejarah Artikel
Submitted: 19 Juli 2024
Accepted: 24 Juli 2024
Published: 25 Juli 2024

Kata Kunci
Keamanan Jaringan, *Web Server*, Metasploit Framework, *Penetration Testing*, ISSAF

PENDAHULUAN

Dalam berkembang pesatnya di era digital, *web server* telah menjadi infrastruktur yang sangat vital dalam mendukung berbagai layanan *online*, mulai dari situs *web* hingga aplikasi *web* yang kompleks. Namun, tidak boleh diabaikan bahwa penggunaan internet juga mempunyai resiko dan kerugian salah satu contohnya ancaman dari oknum tidak bertanggung jawab yang dikenal dengan sebutan *hacker* (Mamuriyah et al., 2024).

Menurut Lanskap BSSN Top 5 CVE Nasional adalah daftar 5 (lima) jenis kerentanan yang memiliki jumlah *hit* terbanyak di Indonesia pada tahun 2023. Kerentanan-kerentanan ini memiliki tingkat dampak dari *High* hingga *Critical*. Pada laporan CVE-2022-26377 memiliki

nilai CVSS 7,5 dengan tingkat dampak *HIGH*. Penyebab utama kerentanan ini yaitu adanya interpretasi yang tidak konsisten pada HTTP *request* (kerentanan HTTP *request Smuggling*) dalam *mod_proxy_ajp*. Kerentanan ini dapat dimanfaatkan *threat actor* untuk menyisipkan request ke *server* AJP tempat *request* diteruskan. Dampak dari adanya kerentanan ini adalah *threat actor* dapat mengancam sistem target dan melakukan perubahan data sehingga mempengaruhi aspek integritas. Sektor Terdampak, Sektor yang paling banyak berpotensi terdampak kerentanan ini adalah Sektor Teknologi Informasi dan Komunikasi sebesar 66.80%, Sektor Lainnya sebesar 18.43%, dan Sektor Administrasi Pemerintahan sebesar 12.17%.

SMKN XYZ telah mengambil langkah maju dengan mengintegrasikan teknologi *website* dalam menyediakan layanan informasi kepada siswa, orang tua, dan staf sekolah. Namun, keberadaan *website* tersebut juga memperkenalkan risiko keamanan yang perlu diperhatikan secara serius.

Tiap *website* pasti memiliki data-data yang biasanya tertanam pada *Web Server* agar para pengunjung dari seluruh dunia bisa mengakses *website* tersebut. Jika keamanan dari suatu *website* tidak bagus maka bukan hal yang sulit bagi para penjahat bisa mendapatkan data-data dari *website* tersebut. (Artha Kusuma, 2021).

Kerentanan *web server* pada *website* SMKN XYZ memungkinkan adanya celah keamanan yang rentan terhadap eksploitasi, kurangnya keamanan pada perangkat lunak yang digunakan , kurangnya dalam konfigurasi keamanan dan kurangnya pembaruan perangkat lunak yang menyebabkan kerentanan keamanan.

Sistem yang *down* ini tentunya akan berdampak pada terbukanya celah untuk seorang hacker atau oknum tak bertanggung jawab melakukan peretasan *website* berlandaskan demi keuntungan pribadi pelaku. (Ariyadi et al., 2023).

KAJIAN PUSTAKA

Jaringan Komputer

Jaringan komputer merupakan kesatuan dari berbagai komponen *hardware*, *software* maupun protokol komunikasi yang digunakan untuk menghubungkan dan memungkinkan pertukaran data antara perangkat yang berbeda secara efisien(Natsir et al., 2023).

Keamanan Jaringan

Keamanan jaringan secara umum adalah komputer yang terhubung ke *network*, mempunyai ancaman keamanan lebih besar dari pada komputer yang tidak terhubung kemana-mana. Dengan pengendalian yang teliti, resiko tersebut dapat dikurangi, namun *network security* biasanya bertentangan dengan *network access*, dimana bila *network access* semakin mudah, maka *network security* semakin rawan, begitu pula sebaliknya (Santoso, 2019).

WEB Server

Web server merupakan software yang melayani akses ke suatu file seperti *Hypertext Markup Language* (HTML) , *Perl* dan *Javascript*. *Web server* memproses *request* dari *browser client* seperti *google chrome*, *firefox*, *safari* dan *software browser* lainnya lalu menampilkan hasil dari proses berupa data-data yang dibutuhkan *client* kembali ke *web browser* (Amrullah et al., 2023).

Keamanan *WEB Server*

Keamanan web server merupakan aspek penting dalam menjaga keamanan server yang digunakan di seluruh domain web atau Internet. Keamanan ini biasanya diimplementasikan melalui beberapa metode dan lapisan seperti kemananan sistem operasi (OS), keamanan aplikasi dan keamanan jaringan. *Server* merupakan bagian integral dari *back-end* aplikasi

yang mengelola data, merespon permintaan pengguna, dan menentukan perilaku aplikasi. Baik organisasi yang menyebarkan aplikasi mereka menggunakan *server* fisik atau *virtual*, mengamankan *server* menjadi prioritas utama selama pengembangan aplikasi *web* (Faatihah et al., 2024).

Serangan Siber

Serangan siber yang biasa dikenal sebagai serangan jaringan komputer adalah eksploitasi yang disengaja terhadap sistem komputer, perusahaan, dan jaringan yang bergantung pada teknologi. Para penyerang menggunakan kode berhaya untuk mengubah kode, logika, atau data komputer yang menghasilkan konsekuensi yang mengganggu yang dapat membahayakan data dan mengarah pada kejahatan siber, seperti pencurian informasi dan identitas (Kurniawan et al., 2024)

***Information Sistem Security Assessment Framework* (ISSAF)**

Framework ISSAF dikembangkan oleh OISSG (*Open Information System Security Group*). Metodologi uji penetrasi melalui *Framework ISSAF* dibuat untuk mengevaluasi jaringan, sistem dan kontrol aplikasi memberikan tahapan proses pengujian penetrasi secara optimal yang bertujuan memberikan arahan kepada auditor melakukan pengujian secara lengkap dan benar, serta menghindari kesalahan dalam melakukan pengujian serangan yang bersifat acak (Ary et al., 2020).

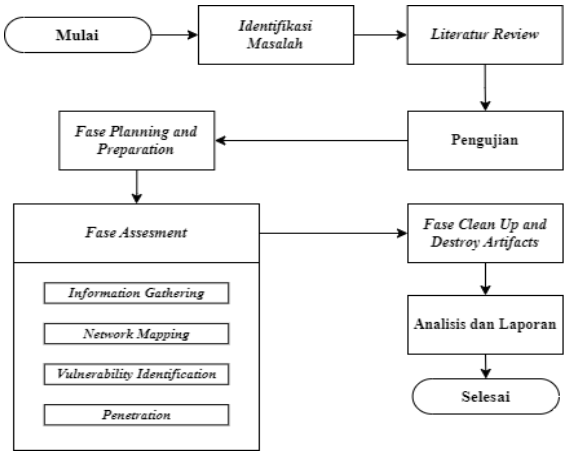
Metasploit Framework

Metasploit framework adalah *platform* pengujian dan pengembangan penetrasi *open source* yang memberi akses ke kode *exploit* untuk berbagai aplikasi, sistem operasi dan platform. Ditulis dalam Bahasa *scripting Ruby* dengan sifat status *Ruby* sebagai Bahasa berorientasi objek. Selain itu, *metasploit* dianggap *multi-platform* berjalan pada sebagian besar variasi *unix* dan *windows*. *Metasploit framework* menghasilkan cara kerja yang luar biasa, tetapi bagi pengguna baru terbilang sulit untuk digunakan karena *metasploit* di linux tidak menyediakan *graphic user-interface* (GUI) karena itu perlu mengetahui sintaks dan perintah untuk menggunakan *metasploit* secara efektif (Dwiananda et al., 2019).

METODE PENELITIAN

Kerangka Penelitian

Adapun kerangka penelitian yang akan dijalankan sebagai berikut:



Gambar 1 Kerangka Penelitian

Idenfitikasi Masalah

Identifikasi masalah dilakukan untuk mendapatkan permasalahan yang diperlukan dalam proses penelitian. Keamanan pada *web server* SMKN XYZ, seperti banyak institusi lainnya, telah mengadopsi teknologi website untuk layanan informasi. Namun, memungkinkan *web server* mereka rentan terhadap eksploitasi karena berbagai celah kerentanan yang ada.

Literatur Review

Studi literatur dalam penelitian ini yaitu dengan proses mempelajari jurnal penelitian terdahulu yang telah dilakukan dengan maksud untuk memperoleh teori-teori yang dibutuhkan dan sebagai landasan dilakukan nya kegiatan penelitian. Studi literatur dapat mengarahkan penelitian dalam menyusun kerangka penelitian yang jelas dan terarah sehingga penelitian memiliki referensi yang jelas dalam pemecahan masalahnya.

Pengujian

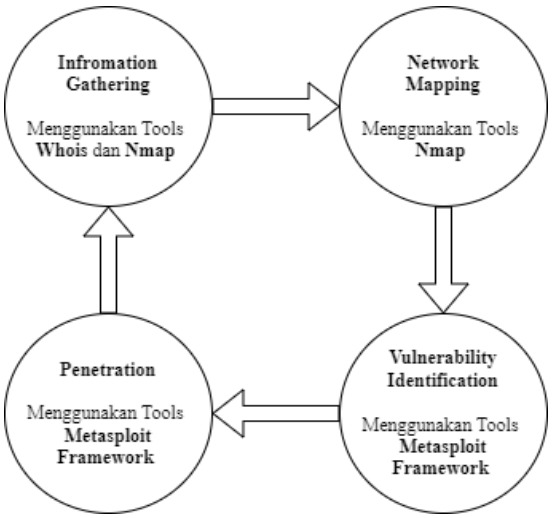
Tahap pengujian ini memiliki 3 *fase* utama yang akan digunakan pada penelitian yaitu antara lain :

Fase Planning dan Preparation

Pada tahap ini yaitu mempersiapkan sistem yang akan menjadi sasaran penelitian ini. Setelah mempersiapkan sistem informasi sekolah yang ada dilakukan penyusunan rencana untuk pengujian dari sistem informasi tersebut.

Fase Assesment

Pada *fase Assesment* adalah *fase* dimana melakukan pengujian pada website dengan 4 *fase* yang akan dilakukan uji coba bisa dilihat pada gambar 3. 3 sebagai berikut :



Gambar 2 Fase Assesment

1. *Information Gathering*

Tahap *information gathering* merupakan tahapan pengumpulan informasi secara umum yang dilakukan pada target. Informasi yang dikumpulkan meliputi informasi mengenai IP target, informasi mengenai registrant dan admin, informasi mengenai *reverse* DNS dan IP *lookup*, dan informasi umum lainnya.

2. Network Mapping

Tahap *network mapping* merupakan tahapan pengumpulan informasi secara spesifik mengenai jaringan pada target. Salah satu informasi yang dikumpulkan pada tahap ini meliputi informasi mengenai port TCP dan UDP pada sistem target.

3. *Vulnerability Identification*

Tahap *vulnerability identification* merupakan tahapan pemindaian *website* target untuk mengetahui kerentanan keamanan didalamnya. Pengujian pada penelitian ini *menggunakan Metasploit Framework Tools* sebagai proses *scanning* untuk mengetahui kerentanan keamanan pada *website*.

4. *Penetration*

Tahap *penetration* merupakan tahapan simulasi serangan yang dilakukan pada *website* target menggunakan *metasploit framework* yang bertujuan untuk memperoleh celah pada keamanan sistem.

Penetration Test yang akan dilakukan pada fase ini untuk melakukan *security assessment*, dengan menggunakan 4 *tool*, yaitu:

a. Kali linux

Kali linux digunakan pada penelitian ini untuk mengetahui keamanan jaringannya jika dilakukan *Penetration Test* menggunakan Kali linux sebagai *Tool*, dengan, menggunakan *Metasploit Framework, Whois dan Nmap*.

b. *Metasploit Framework*

Metasploit Framework digunakan untuk menguji keamanan *website* dengan melakukan pengujian penetrasi meliputi identifikasi kerentanan potensial dalam aplikasi *web*, mencari eksploitasi yang relevan, dan menguji keamanan keseluruhan infrastruktur *website*.

c. *Whois*

Whois digunakan untuk mengetahui basis data publik untuk informasi terkait dengan nama domain atau alamat IP. Informasi yang dapat ditemukan melalui Whois termasuk informasi pemilik domain, informasi kontak teknis dan administratif, informasi register domain, serta informasi terkait status domain.

d. *Nmap*

Nmap memiliki tujuan untuk mengetahui *port* yang terbuka dengan status yang sudah ada yaitu terbuka (*open*), di-filter (*filtered*), tertutup (*closed*), atau tidak di-filter (*unfiltered*).

Fase Clean Up and Destroy Artifacts

Pada tahapan ini setiap informasi yang dibuat atau dimasukkan ke dalam sistem harus dihapus. Jika ini tidak memungkinkan pada sistem jarak jauh, pihak yang diuji harus memberikan informasi ini setelah menerima laporan.

Analisis dan Laporan

Pada tahap ini dilakukan analisis terhadap pengujian yang sudah dilakukan dan merangkumnya ke dalam sebuah laporan untuk mengetahui kerentanan yang ada pada *website*.

HASIL DAN PEMBAHASAN

Pengujian

Pada tahap pengujian ini peneliti melakukan uji terhadap *website* SMKN XYZ dengan beberapa fase yang akan dilakukan antara lain *Fase Planning and Preparation, Fase Assesment* dan *Fase Clean Up and Destroy Artifacts*.

Fase Planning and Prepartion

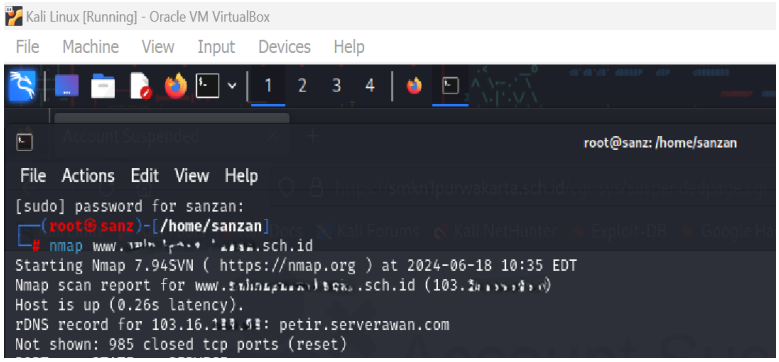
Pada tahap ini peneliti melakukan persiapan mengenai sistem yang akan dilakukan pengujian terhadap *website* SMKN XYZ termasuk perangkat lunak untuk pemindaian kerentanan, alat uji penetrasi, dan metode pengumpulan data untuk melakukan tahap uji coba akandilakukan pada *fase* selanjutnya.

Fase Assesment

Pada tahap ini peneliti melakukan uji coba terhadap *website* dengan melakukan 4 tahapan yang akan dilakukan meliputi *Information Gathering, Network Mapping, Vulnerability Identification dan Penetration*. Setiap tahapan ini bertujuan untuk mengidentifikasi dan mengevaluasi berbagai aspek keamanan dari *website* yang akan diuji.

1. *Information Gathering*

Pada tahap ini, peneliti mengumpulkan informasi sebanyak mungkin tentang target *website*. Pengumpulan informasi ini menggunakan *tools* Nmap dan *tools* Whois dengan perintah *nmap <link target>* dan *whois <IP target>* bisa dilihat pada gambar dibawah ini sebagai berikut :



Gambar 3 IP Target

Pada Gambar 3 memperlihatkan IP dengan perintah *nmap www.smknxyz.sch.id* dan mendapatkan alamat IP 103.16.XXX.XX untuk selanjutnya IP ini akan digunakan mengumpulkan beberapa informasi.

2. *Network Mapping*

Pada tahap *network mapping* ini peneliti menggunakan *tools Nmap* dengan perintah *nmap <ip target>* untuk mengetahui *port* terbuka pada target IP. *Network mapping* merupakan langkah penting untuk mengidentifikasi layanan yang berjalan dan potensi kerentanan pada sistem target bisa dilihat pada gambar dibawah ini sebagai berikut :

Hasil penggunaan Nmap memperlihatkan layanan dan *port* yang terbuka dengan melakukan perintah *nmap 103.16.XXX.XX* dan medapatkan hasil bisa dilihat sebagai berikut :

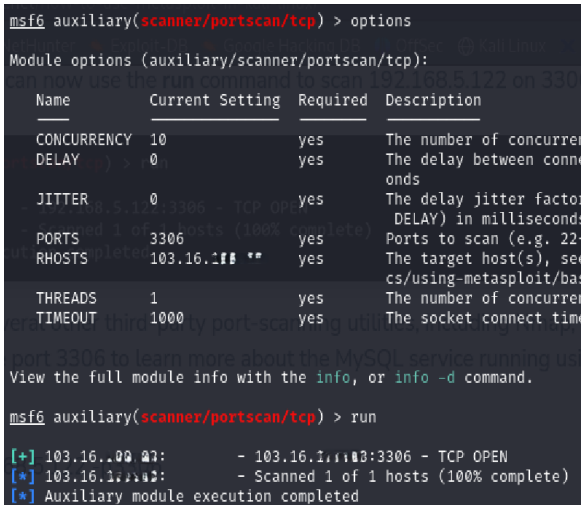
(2024), 2 (11): 136–150 **Scientica** 3021-8209
Jurnal Ilmiah Sain dan Teknologi

Table 1 Hasil *Tools Whois*

PORT	***STATE***	***SERVICE***
21/tcp	*Open*	FTP
25/tcp	*Filtered*	SMTP
26/tcp	*Open*	RSTP
53/tcp	*Open*	Domain
80/tcp	*Open*	HTTP
110/tcp	*Open*	POP3
111/tcp	*Open*	Rpcbind
143/tcp	*Open*	Imap
443/tcp	*Open*	HTTPS
465/tcp	*Open*	Submission
587/tcp	*Open*	Imaps
993/tcp	*Open*	POP3S
3306/tcp	*Open*	MySQL
5678/tcp	*Filtered*	RRAC

3. Vulnerability Identification

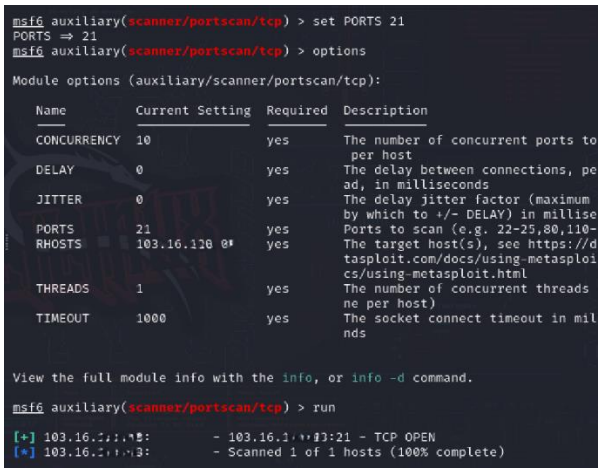
Pada tahap *vulnerability identification* peneliti menggunakan *tools metasploit framework* untuk mengetahui kerentanan dengan melakukan *scanning* terhadap *website* SMKN XYZ dan melakukan serangkaian proses identifikasi kerentanan terhadap 4 *port* yang akan di jalankan bisa dilihat pada gambar dibawah ini sebagai berikut :



Gambar 4 Hasil Scanning Port 3306

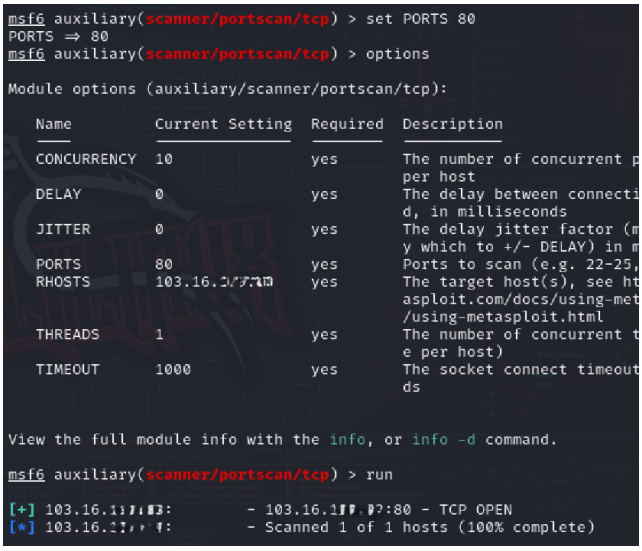
Pada Gambar 4 hasil menjalankan *scanning port 3306* memeperlihatkan Pemindaian port dengan perintah *msf> run* terhadap target host *103.16.XXX.XX* berhasil dilakukan menggunakan port TCP 3306. Hasil pemindaian menunjukkan bahwa port 3306 dalam keadaan terbuka pemindaian ini dapat memberikan informasi penting tentang layanan yang berjalan di *port* tersebut yaitu MySQL.

(2024), 2 (11): 136–150 **Scientica** 3021-8209
Jurnal Ilmiah Sain dan Teknologi



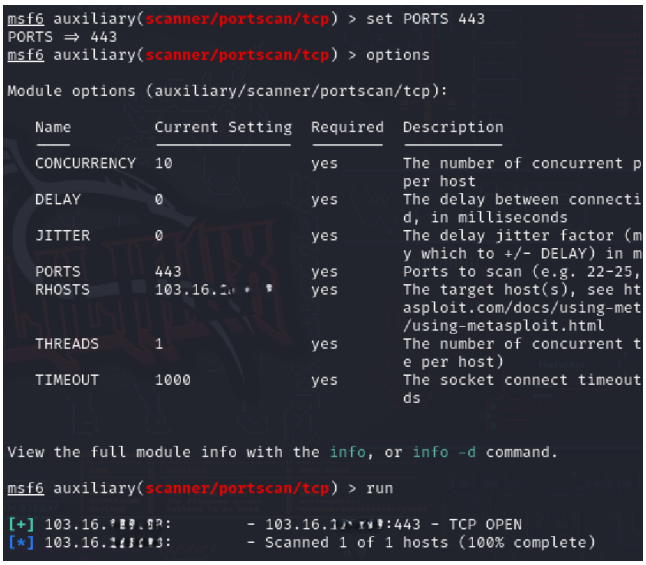
Gambar 5 Hasil Scanning Port 21

Pada Gambar 5 hasil Menjalankan *Scanning Port* 21 memperlihatkan pemindaian *port* terhadap target *host* 103.16.XXX.XX berhasil dilakukan menggunakan *port* TCP 21. Hasil pemindaian menunjukkan bahwa port 21 dalam keadaan terbuka *port* 21 ini dengan layanan FTP (*File Transfer Protocol*). Pemindaian *port* ini dapat memberikan informasi penting tentang layanan yang mungkin berjalan pada target *host*. Langkah selanjutnya dapat melibatkan pengujian lebih lanjut terhadap layanan FTP untuk mengidentifikasi potensi kerentanan.



Gambar 6 Hasil Scanning Port 80

Pada Gambar 6 hasil Menjalankan *Scanning Port* 80 memperlihatkan pemindaian *port* terhadap target *host* 103.16.XXX.XX berhasil dilakukan menggunakan *port* TCP 80. Hasil pemindaian menunjukkan bahwa *port* 80 dalam keadaan terbuka *port* 80 digunakan untuk layanan HTTP (*Hypertext Transfer Protocol*), yang merupakan protokol utama untuk mentransfer halaman web. Pemindaian *port* ini dapat memberikan informasi penting tentang layanan web yang mungkin berjalan pada target *host*.

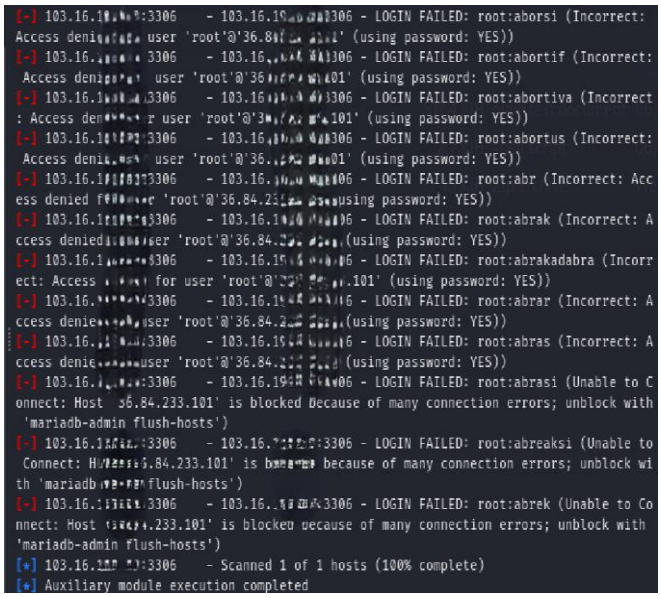


Gambar 7 Hasil Scanning Port 443

Pada Gambar 7 hasil menjalankan *scanning port* 443 memperlihatkan pemindaian *port* terhadap target *host* 103.16.XXX.XX berhasil dilakukan menggunakan *port* TCP 443. Hasil pemindaian menunjukkan bahwa *port* 443 dalam keadaan terbuka *port* 443 digunakan untuk layanan HTTPS (*Hypertext Transfer Protocol Secure*), yang merupakan protokol utama untuk *transfer* halaman web yang aman. Pemindaian *port* ini terbuka dapat memberikan informasi penting tentang layanan web aman yang mungkin berjalan pada target *host*. Langkah selanjutnya dapat melibatkan pengujian lebih lanjut terhadap layanan HTTPS untuk mengidentifikasi potensi kerentanan.

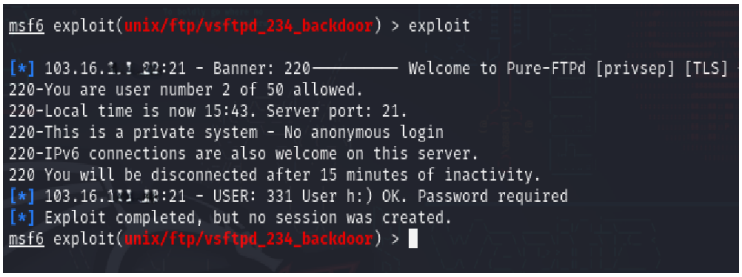
4. Penetration

Pada tahap *penetration* peneliti melakukan uji penetrasi dan eksploitasi terhadap 4 *port* yaitu *port* 3306, 21, 80 dan 443 hasil dan penjelasan dari setiap langkah yang akan dilakukan pada masing-masing *port* bisa dilihat pada gambar dibawah ini :



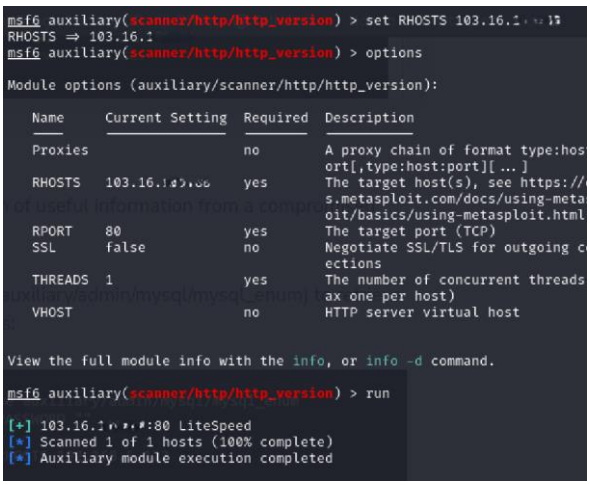
Gambar 8 Hasil Menjalankan *mysql_login*

Pada Gambar 8 hasil menjalankan *mysql_login* memperlihatkan hasil Percobaan login ke *server MySQL* pada target host 103.16.XXX.XX dengan berbagai kombinasi *username root* dan kata sandi yang diuji gagal. Semua upaya menghasilkan pesan kesalahan yang menyatakan "*Access denied for user 'root'@'36.84.XXX.XXX' (using password: YES)*". Setelah beberapa percobaan gagal, *host* sumber (36.84.XXX.XXX) diblokir oleh *server* target karena terlalu banyak percobaan koneksi yang gagal, dan memerlukan intervensi administratif (*mariadb-admin flush-hosts*) untuk membuka blokir tersebut.



Gambar 9 Hasil Exploit Port 21

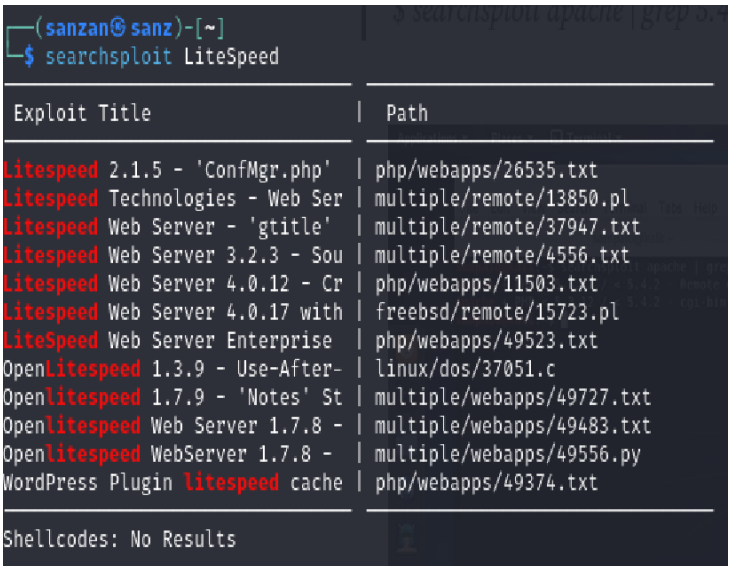
Pada Gambar 9 melakukan *exploit port* 21 FTP memperlihatkan hasil dan telah dijalankan terhadap *server* FTP di IP 103.16.XXX.XX. Meskipun *exploit* berhasil dieksekusi sampai tahap *login*, namun tidak berhasil membuat sesi yang dapat digunakan untuk mengakses lebih lanjut sistem target. Ini dapat disebabkan oleh beberapa faktor seperti *patching* pada target, *firewall*, atau konfigurasi keamanan yang lebih ketat.



Gambar 10 Hasil HTTP Version Port 80

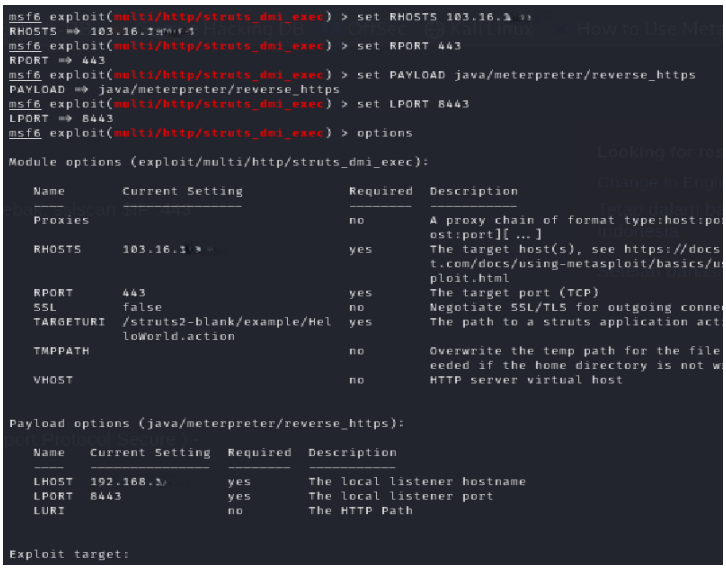
Pada Gambar 10 Melakukan *Setting* HTTP *Version* memperlihatkan hasil melakukan *setting* pada HTTP *Version* dengan perintah *set RHOST 103. 16.199.83* pada *port* 80 lalu melakukan *options* untuk melihat bahwa *setting* berhasil. Melakukan pemindaian dengan perintah *run* pada HTTP *Version* berhasil dan mendapatkan versi HTTP adalah *LiteSpeed.*

(2024), 2 (11): 136–150 **Scientica** 3021-8209
Jurnal Ilmiah Sain dan Teknologi



Gambar 11 Hasil Exploit Port 80

Pada Gambar 11 melakukan *exploit port* 80 memperlihatkan hasil Pencarian menggunakan perintah *searchsploit LiteSpeed* menunjukkan bahwa LiteSpeed *Web Server* dan *OpenLiteSpeed Web Server* memiliki beberapa kelemahan yang dapat dieksploitasi.



Gambar 12 Setting struts_dmi_exec

Pada Gambar 12 melakukan *setting struts_dmi_exec* memperlihatkan hasil dengan perintah *set RHOST 103.16.XXX.XX, set RPORT 443, set PAYLOAD java/meterpreter/reverse_https* dan *set LPORT 8443* lalu melakukan *options* untuk melihat bahwa *setting* berhasil.

Gambar 13 Hasil Exploit Port 443

Pada Gambar 13 hasil menjalankan *exploit port* 443 memperlihatkan hasil dengan perintah *run* pada percobaan ini, modul eksploitasi *multi/http/struts_dmi_exec* digunakan untuk menargetkan *server* di alamat 103.16.XXX.XX melalui *port* 443.

Fase Clean Up and Destroy Artifacts

Pada *fase* ini peneliti melakukan penghapusan jejak, *file* yang telah dibuat dan dimasukan terhadap *website* SMKN XYZ dengan IP 103.16.XXX.XX.

Analisis dan Laporan

Pada tahap ini peneliti telah membuat hasil dan analisis dari pengujian terhadap *website* SMKN XYZ sebagai berikut :

Hasil Analisis MySQL *Port* 3306

Hasil analisi terhadap MySQL pada *port* 3306 setelah melakukan pengujian memberikan hasil sebagai berikut :

1. Setiap kombinasi *username* (*root*) dan *password* gagal login dengan pesan "*Access denied*".
2. Setelah beberapa kali percobaan gagal, *host* 36.84.XXX.XXX diblokir oleh server MySQL target karena terlalu banyak kesalahan koneksi.
3. Pesan "Host '36.84.XXX.XXX' *is blocked because of many connection errors*" menunjukkan bahwa sistem target telah mengaktifkan mekanisme perlindungan untuk mencegah serangan *bruteforce* dengan cara memblokir IP percobaan setelah sejumlah kesalahan tertentu.
4. Pesan terakhir menyarankan untuk menggunakan perintah *mariadb-admin flush-hosts* untuk membuka blokir *host* yang telah diblokir. Namun, ini hanya bisa dilakukan jika memiliki akses administratif ke *server* target.

Hasil Analisis FTP *Port* 21

Hasil analisis terhadap FTP pada *port* 21 setelah melakukan pengujian bisa dilihat sebagai berikut :

Tabel 4. 1 Analisis *Port* 21

IP Target	Port	Modul	Status Eksekusi	Keterangan
103.16.XXX.XX	21	*unix/ftp/vsftpd_234_backdoor*	*Exploit Completed, No Session Created*	Berhasil terhubung ke *server* FTP dan menerima banner Pure-FTPd, namun tidak berhasil membuat sesi. Kemungkinan target telah dipatch atau dilindungi.

Hasil Analisis HTTP *Port* 80

Hasil analisis terhadap HTTP pada *port* 80 setelah melakukan pengujian bisa dilihat pada tabel sebagai berikut :

Tabel 4. 2 Analisis *Port* 80

Server	Versi	Kelemahan	Deskripsi	*Path*
LiteSpeed Web Server	2.1.5	*'ConfMgr.php'*	Kelemahan terkait pada 'ConfMgr.php' memungkinkan eksploitasi tertentu.	*php/webapps/26535.txt*
	4.0.12	*Remote Root Exploit*	Eksploitasi ini memungkinkan penyerang mendapatkan akses *root* dari jarak jauh.	*multiple/remote/13850.pl*
	3.2.3	*Source Code Disclosure*	Kelemahan ini memungkinkan pengungkapan kode sumber dari jarak jauh.	*multiple/remote/4556.txt*
	4.0.12	*Cross-Site Scripting (XSS)*	Kelemahan ini memungkinkan serangan XSS yang dapat digunakan untuk mencuri informasi pengguna.	*php/webapps/11503.txt*
	4.0.17	*Remote Code Execution* dengan PHP 5.2.0	Kelemahan ini memungkinkan eksekusi kode dari jarak jauh, yang bisa digunakan untuk mengambil alih *server*.	*freebsd/remote/15723.pl*
	Enterprise 5.4	*Directory Traversal*	Kelemahan ini memungkinkan penyerang melakukan traversal direktori dan mengakses *file* yang tidak diizinkan.	*php/webapps/49523.txt*

Open LiteSpeed Web Server	1.3.9	*Use-After-Free Denial of Service* (DoS)	Kelemahan ini dapat digunakan untuk menyebabkan *denial of service* pada server.	*linux/dos/37051.c*
	1.7.9	*Stored Cross-Site Scripting* (XSS) pada '*Notes*'	Kelemahan ini memungkinkan serangan XSS yang tersimpan, berpotensi mencuri informasi pengguna.	*multiple/webapps/49727.txt*
	1.7.8	*Directory Traversal*	Kelemahan ini memungkinkan penyerang melakukan traversal direktori dan mengakses *file* yang tidak diizinkan.	*multiple/webapps/49483.txt*
	1.7.8	*Multiple Vulnerabilities*	Beberapa kelemahan yang memungkinkan berbagai jenis serangan terhadap *server*.	*multiple/webapps/49556.py*
WordPress Plugin LiteSpeed Cache	2.9.9.2	*Arbitrary File Deletion*	Kelemahan ini memungkinkan penghapusan file sewenang-wenang, yang bisa digunakan untuk merusak instalasi WordPress atau menghapus file penting.	*php/webapps/49374.txt*

Hasil Analisis HTTPS *Port* 443

Hasil analisis pada *port* 443 HTTPS setelah melakukan pengujian bisa dilihat pada tabel 4. 6 dan tabel 4.7 sebagai berikut :

Tabel 4. 3 Analisis *Port* 443

IP Target	Port	Modul	Status Eksekusi	Keterangan
103.16.XXX.XX	80	*/http/multi/stuts_dmi_exec*	*Exploit Completed, No Session Created*	Berhasil mengunggah dan mengeksekusi *exploit*, namun gagal membuat sesi interaktif.

KESIMPULAN

Berdasarkan hasil penelitian ini dapat kesimpulan tentang keamanan *website* SMKN XYZ melalui tiga *fase* yaitu *Planning and Preparation, Assessment, Clean Up and Destroy Artifacts*. *Fase* ***Planning and Preparation*** peneliti menyiapkan sistem dan alat untuk pengujian. Target pengujian adalah *website* dengan IP 103.16.XXX.XX. *Fase* ***Assessment*** melakukan pengujian melalui *Information Gathering, Network Mapping, Vulnerability Identification,* dan *Penetration*. Informasi penting dikumpulkan, dan *port* terbuka diidentifikasi menggunakan Nmap. Metasploit mengidentifikasi kerentanan pada layanan di port tersebut. Eksploitasi menunjukkan sistem memiliki perlindungan baik terhadap serangan *brute force* dan eksploitasi lainnya, meskipun terdapat kelemahan pada *LiteSpeed Web Server* dan *OpenLiteSpeed Web Server*. *Fase* ***Clean Up and Destroy Artifacts*** menghapus jejak pengujian dan memastikan tidak ada artefak tertinggal pada sistem target. Penelitian ini berhasil mengidentifikasi beberapa kerentanan dan resiko keamanan pada *website* SMKN XYZ, meskipun sistem target menunjukkan perlindungan yang cukup baik terhadap eksploitasi.

REFERENSI

Adha, R. R., Rizal, M. F., Juli, S., & Ismail, I. (2021). *MEMBANGUN SISTEM KEAMANAN JARINGAN BERBASIS FIREWALL DAN IDS MENGGUNAKAN TOOLS OPNSENSE*.

Agustia Rahayuningsih, P. (2024). Modul Jaringan Komputer. *BINA SARANA INFORMATIKA*.

Amrullah, A., Nugroho, A., & Ramadhan, Z. (2023). PERBANDINGAN KINERJA WEBSERVER PADA PENYEDIA LAYANAN CLOUD MICROSOFT AZURE DAN AMAZON WEB SERVICES MENGGUNAKAN METODE BENCHMARKING. In *JINTEKS* (Vol. 5, Issue 1).

Andria. (2020). Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux. *Generation Journal*, *4*(2), 69. http://www.starrybyte.com

Andriyani, S., Fajar Sidiq, M., & Parga Zen, B. (2023). *Analisis Celah Keamanan Pada Website Dengan Menggunakan Metode Penetration Testing Dan Framework Issaf Pada Website SMK Al-Kautsar* (Vol. 2, Issue 1).

Anugerah Julyan Rahmat, R., Fahriani, N., Jl Raya Sutorejo No, S., Sutorejo, D., Mulyorejo, K., & Timur, J. (2023). Deteksi Serangan DDoS Dan Sniffing Pada Jaringan Wireless Di Lab Informatika Um Surabaya Dengan Metode Vulnerability Assessment. *SEMASTER: Seminar Nasional Teknologi Informasi & Ilmu Kompute*, *2*(1), 88–96.

Ariyadi, T., Langgeng Widodo, T., Apriyanti, N., & Sasti Kirana, F. (2023). *Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP Analysis of Bina Darma University Academic Information System Security Vulnerabilities Using the OWASP* (Vol. 22, Issue 2).

Artha Kusuma, G. H. (2021). Perancangan Skema Sistem Keamanan Jaringan Web Server menggunakan Web Application Firewall dan Fortigate untuk Mencegah Kebocoran Data di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing* , *2*(2).

Ary, G., Sanjaya, S., Made, G., Sasmita, A., Made, D., & Arsa, S. (2020). *Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF*.

Chandra, A. A., Turmudi Zy, A., & Nugroho, A. (2024). PENERAPAN TEKNIK PENETRATION TESTING TERHADAP CROSS SITE SCRIPTING (XSS) DALAM PENGEMBANGAN WEBSITE. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *9*(2), 262–270. https://doi.org/10.36341/rabit.v9i2.4822