JuSIN
Jurnal Sistem Informasi

Website: ojs.itb-ad/index.php/JUSIN
E-ISSN: 2797-8516

ANALISIS PENERAPAN SANGFOR NGAF FIREWALL SEBAGAI KEAMANAN PADA JARINGAN INTERNET UNIVERSITAS MUHAMMADIYAH PURWOKERTO

Yusril Amru[1], Ermadi Satriya Wijaya[2(*)]

[1]*Universitas Muhammadiyah Purwokerto, Purwokerto*
[2]*Universitas Muhammadiyah Purwokerto, Purwokerto*

Abstract

Computer network technology is developing very rapidly, but as a result of these technological developments causing the exploitation of security gaps in network systems by exploiting security holes, unauthorized users can easily commit crimes in the cyber world known as Cyber Crime. Sniffing, Spoffing, DoS attacks. Sangfor NGAF is a network firewall security tool designed to filter and check across networks and applications, The analysis is intended to provide an overview of security vulnerabilities in network systems where these steps are important steps to determine the best way to close security holes in the network. In this analysis there are steps taken, namely Preparation, Observation, Data Collection, and Network Analysis. The results of this study are several servers that have been compromised, from the analysis results obtained there are various kinds of attacks including WebShell or Backlink, Bot Controlled, Brute-force, SQL Injection, and so on.

Kata Kunci: Firewall Sangfor NGAF, Bot Controlled, Webshell, Brute-force, SQL Injection

Juli - Desember 2022, Vol 3 (2) : hlm 55-66

(*) Korespondensi: *yusrilalamr21@gmail.com (Yusril Amru)*

PENDAHULUAN

Pemanfaatan layanan jaringan *interconnection networking* (internet) dan komputer berkembang secara pesat dalam berbagai bidang, sehinggamemberikan banyak kemudahan dalam mengakses berbagai macam informasi. Kebebasan dalam mengakses internet sehingga menyebabkan banyaknya serangan yang mengancam contohnya melalui virus atau pun worm dan spam, oleh karena itu Universitas Muhammadiyah Purwokerto mengimplementasikan firewall jenis Sangfor NGAF.

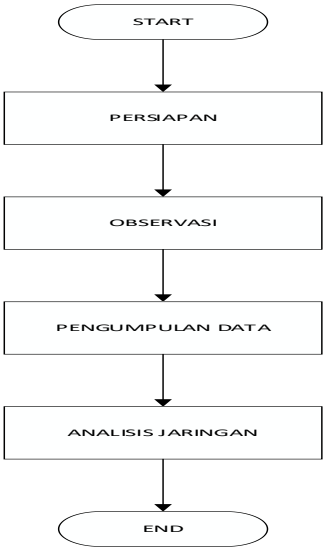
Sangfor NGAF adalah NGFW (Next-Generation Firewall) berkemampuan AI pertama di dunia, terintegrasi penuh dengan WAF (Web Application Firewall) dan Endpoint Secure (Next-Generation Endpoint Security), yang memberikan perlindungan menyeluruh dari semua ancaman dan didukung oleh deteksi malware dan perlindungan Neural-X dan Engine Zero. Sangfor NGAF adalah solusi keamanan gabungan yang mudah digunakan dan dirancang untuk melindungi organisasi dari ancaman internal, eksternal, saat ini, maupun masa depan. Selain itu, database NGAF diperbarui secara proaktif dan berkala untuk menjaga keamanan jaringan terhadap serangan baru ataupun serangan tidak dikenal..

Berdasarkan pembahasan di atas, diputuskan untuk melakukan penelitian pada Firewall Sangfor NGAF yang diimplementasikan Universitas Muhammadiyah Purwokerto. Analisis ditujukan untuk memberikan gambaran celah keamanan pada sistem jaringan dimana langkah ini adalah langkah penting untuk menentukan cara terbaik untuk menutup celah keamanan pada jaringan.

METODE PENELITIAN

Jenis penelitian yang digunakan pada penelitian ini adalah penelitian kualitatif. Penelitian kualitatif adalah metode penelitian yang digunakan untuk melihat sistem yang ada pada objek penelitian yang akan diteliti, dengan berdasarkan analisis yang difokuskan pada fungsi kualitas dari sistem yang ada pada lokasi penelitian. Untuk desain alur penelitian dapat di lihat pada

Gambar 1.



Gambar 1 Desain Alur Penelitian

1.1 Persiapan

Dalam tahapan persiapan yang dilakukan penulis, meliputi perumusan permasalahan yang akanditeliti, kemudian penentuan objek yang akan diteliti, juga menyiapkan semua instrumen penelitian.

1.1 Observasi

Langkah selanjutnya adalah melakukan observasi pada objek yang dituju, dimana pada penelitian ini, penulis mengambil gambaran objek secara umum sebagai contoh untuk pengembangan sistem yang lebih optimal dari sistem yang berjalan.

HASIL DAN PEMBAHASAN

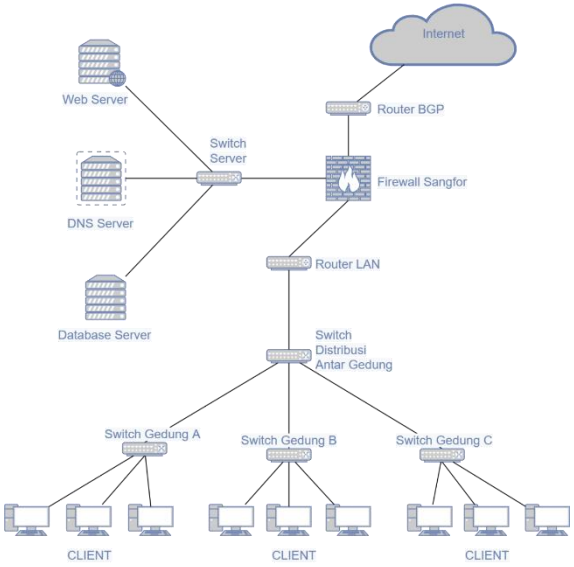
1. Pengumpulan Data

Teknik pengumpulan data yang digunakan yaitu observasi dan wawancara, pada proses observasi dilakukan peninjauan lapangan berupa peninjauan penerapan sistem instalasi jaringan yang ada di lokasi penelitian yang dituju. Pada proses wawancara pengambilan data dilakukan dengan memberikan pertanyaan kepada pihak yang terkait langsung dengan manajemen jaringan yang ada di lokasi penelitian dimana dari hasil wawancara tersebut didapatkan data sebagai berikut:

a. Jenis Firewall

Universitas Muhammadiyah Purwokerto adalah firewall jenis NGAF (Next-Generation Firewall) 5600 yang diproduksi oleh sangfor. Sangfor Technologies adalah vendor global terkemuka untuk solusi infrastruktur IT, yang mengkhususkan pada Cloud Computing & Network Security dengan berbagai macam produk & layanan.

b. Topologi Jaringan contoh topologi jaringan yang ada di Universitas Muhammadiyah Purwokerto dapat dilihat pada Gambar 2.

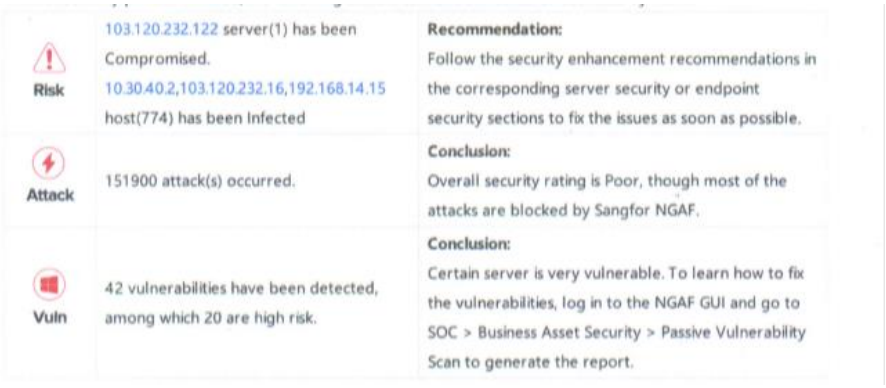


Gambar 2
Tipografi Jaringan

2. Analisis Jaringan

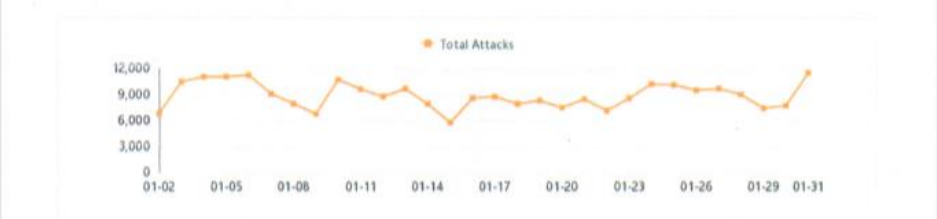
Gambar 3 Security Summary

Pada gambar 3 menunjukan bahwa keamanan Pra-Perlindungan bersetatus buruk sedangkan keamanan Pasca-Perlindungan bersetatus sangat baik atau lebih tepatnya keamanan tanpa firewall NGAF bersetatus buruk, sedangkan dengan firewall NGAF bersetatus sangat baik.



Gambar 4 Without Security

Pada Gambar 4. menjelaskan bahwa server 103.120.232.122 telah disusupi dimana 774 host telah terinfeksi. Terdapat 151900 serangan yang terjadi dimana 42 kerentanan telah terditeksi, 20 diantaranya beresiko tinggi.

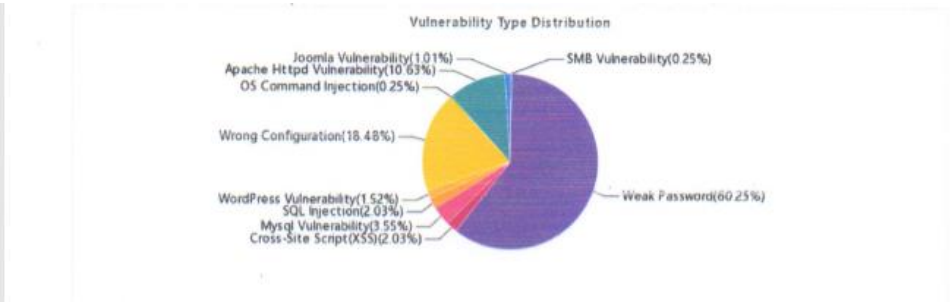


Gambar 5 Total Attack

Gambar 5. menunjukan jumlah total serangan terhadap zona yang dilindungi dimana dalam kurun waktu satu bulan terdapat lebih dari 12000 serangan.

Gambar 6 Attack Trends

Gambar 6. menunjukan total serangan yang terjadi, kejadian serangan dan kerentanan. Seiring dengan meningkatnya jumlah serangan, tingkat keamanan jaringan menurun. Lebih banyak peristiwa serangan menunjukkan serangan yang lebih sering menargetkan server tertentu. Demikian juga, semakin banyak kerentanan, semakin rentan server, dan semakin besar kemungkinan intrusi dapat terjadi.



Gambar 7 Type Vulnerability

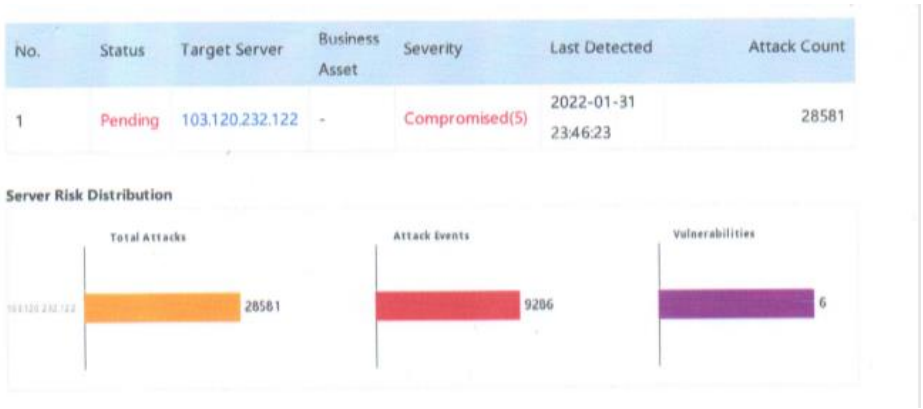
Gambar 7. menunjukan Distribusi Jenis Kerentanan yang terdeteksi di zona lindung tertentu , hasil dari Distribusi terdapat 42 kerentanan yang terjadi pada server 20 diantaranya beresiko tinggi dan 22 beresiko sedang kerentanan tersebut diantaranya:

Jenis Kerentanan	**Presentase Kerentanan**
Server Message Box (SMB)	0,25%
Joomla	1,01%,
Apache Httpd	10,63%,
OS Command Injection	0,25%,
Wrong Configuration	18,48%,

Week Pssword	60,25%,

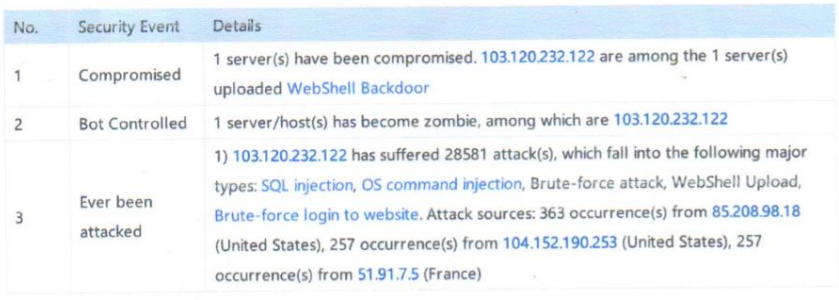
Tabel 1. Jenis Kerentanan

WordPress	1,52%,
SQL Injection	2,03%,
Mysql	3,55%,
Cross-site Script (XSS)	2,03%.



Gambar 8 Server Risk Distribution

Gambar 8. menunjukan server yang paling sering diserang yaitu server 103.120.232.122 dimana dapat disimpulkan bahwa tertadapat 28581 jumlah serangan yang bersetatus tertunda dengan 5 server yang berhasil disusupi diamana terahir terditeksi pada 31 Januari 2022 pukul 23:46:23. Pada distribusi resiko server dapat dilihat terdapat 28581 total serangan, 9286 kejadian serangan dan 6 kerentanan.



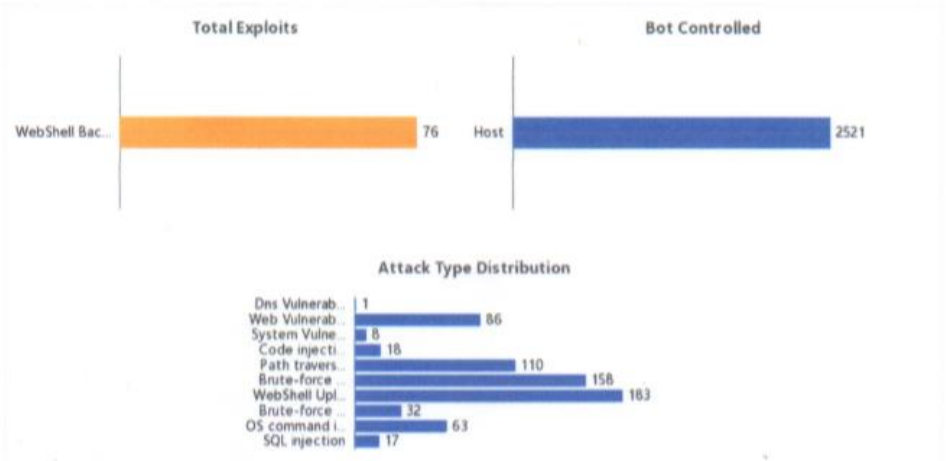
No.	Security Event	Details
1	Compromised	1 server(s) have been compromised. 103.120.232.122 are among the 1 server(s) uploaded WebShell Backdoor
2	Bot Controlled	1 server/host(s) has become zombie, among which are 103.120.232.122
3	Ever been attacked	1) 103.120.232.122 has suffered 28581 attack(s), which fall into the following major types: SQL injection, OS command injection, Brute-force attack, WebShell Upload, Brute-force login to website. Attack sources: 363 occurrence(s) from 85.208.98.18 (United States), 257 occurrence(s) from 104.152.190.253 (United States), 257 occurrence(s) from 51.91.7.5 (France)

Gambar 9 Attack Event

Dari gambar 9. dapat disimpulkan :

a. 1 server telah disusupi. 103.120.232.122 termasuk di antara 1 server yang diunggah WebShell Backdoor.
b. 1 server/host telah menjadi zombie, di antaranya adalah 103.120.232.122.

c. 103.120.232.122 telah mengalami 28581 serangan, yang termasuk dalam jenis utama berikut: injeksi SQL, injeksi perintah OS, serangan Brute-force, Upload WebShell, login Brute-force ke situs web. Sumber serangan: 363 kejadian dari 85.208.98.18 (Amerika Serikat), 257 kejadian dari 104.152.190.253 (Amerika Serikat), 257 kejadian dari 51.91.7.5 (Prancis). Sumber serangan dibawah ini adalah sumber serangan yang paling banyak melancarkan serangan terhadap server.



Gambar 10 Attack Type Distribution

Gambar 10 menunjukan detail keamanan pada server 103.120.232.122 dimana peringkat keamanan keseluruhan server tersebut bersetatus disusupi. Server 103.120.232.122 dikendalikan oleh penyerang dan telah menderita 28.581 serangan, dan 6 kerentanan telah terdeteksi. Penyerang telah mengunggah 76 WebShell backdoor dengan total bot yang terkendali adalah 252.

2.1.2 Vulnerabilities

No.	Vulnerability Name	Total Vulnerabilities	Threat Level	Exploits	Status
1	Weak Password	134	High	0	Protected
2	Joomla Vulnerability	3	High	0	Protected
3	SQL Injection	8	High	0	Protected
4	WordPress Vulnerability	1	High	0	Protected
5	Cross-Site Script(XSS)	1	High	0	Protected
6	Wrong Configuration	7	Medium	0	Protected

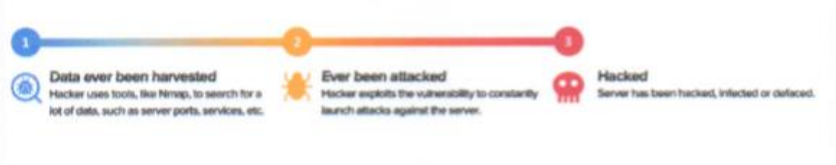
Gambar 11 Vulberabilities

Gambar 11 menunjukan kerentanan yang terdapat pada server 103.120.232.122 dimana terdapat 6 poin kerentanan yaitu Week Password, Joomla Vunerability, SQL Injection, WordPress Vulnerability, Cross-Site Script (XSS) dan Wrong Configuration. 5 diantaranya berlevel kerentanan tinggi dan satu berlevel kerentanan sedang dengan setatus terlindungi.

No.	Attack Source	Attack Type	Source Location	Attack Count
1	85.208.98.18	Website scan(363)	United States	363
2	104.152.190.253	Web site vulnerabilities(257)	United States	257
3	51.91.7.5	Web site vulnerabilities(208) Path traversal(48) Access by hacker IP(1)	France	257
4	52.11.217.175	Access by hacker IP(211) Web Vulnerability(10) OS command injection(10) Code injection(6) Information disclosure(3)	United States	242
5	45.146.165.37	Access by hacker IP(177) WebShell Upload(2) Web site vulnerabilities(1) Path traversal(1) XSS attack(1)	European Region	182

Gambar 12 Attack Source

Gambar 12 menunjukan sumber utama serangan yang diluncurkan terhadap 103.120.232.122, total 28581 serangan. Berikut adalah rekomendasi peningkatan keamanan terhadap server yang telah diserang.



Gambar 13 Stage Of Attack

Gambar 13 menunjukan tahap serangan sebagai berikut:

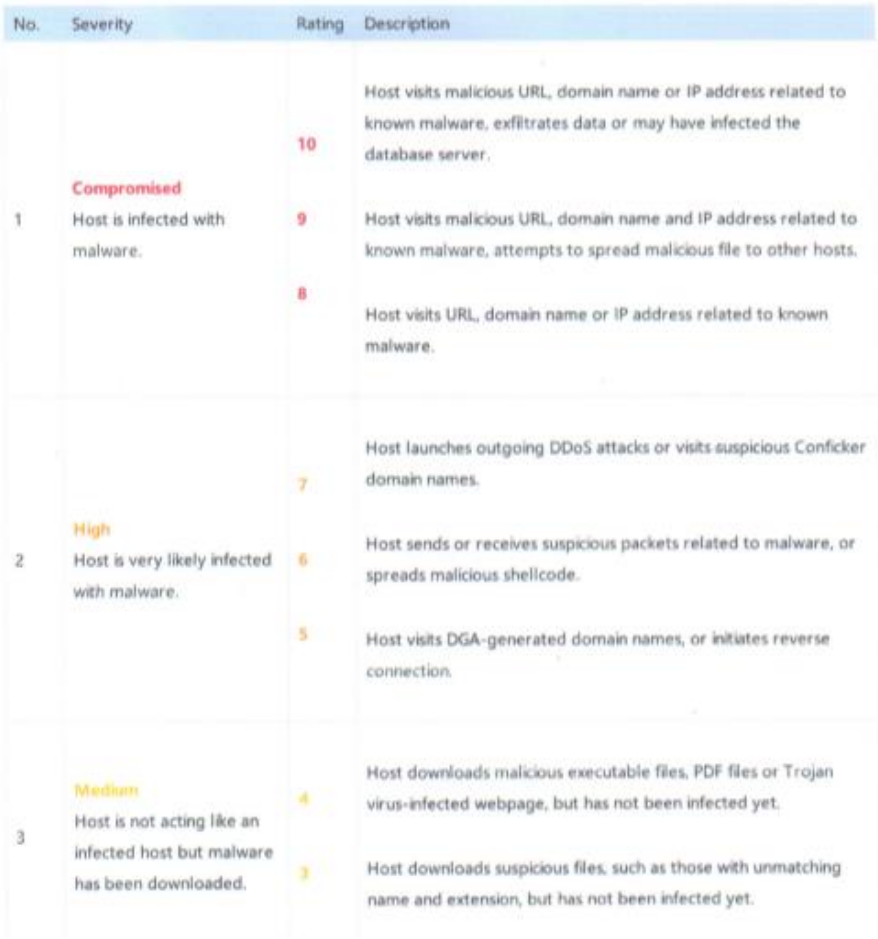
a. Data yang pernah diambil Hacker menggunakan alat, seperti Nmap, untuk mencari banyak data, seperti port server, layanan, dll.
b. Pernah diserang Hacker memanfaatkan kerentanan untuk terus meluncurkan serangan terhadap server.
c. Server yang Diretas telah diretas, terinfeksi, atau dirusak menggunakan alat, seperti Nmap, untuk mencari banyak data, seperti port server, layanan, dll.
d. Pernah diserang Hacker memanfaatkan kerentanan untuk terus meluncurkan serangan terhadap server.
e. Server yang Diretas telah diretas, terinfeksi, atau dirusak

No.	Severity	Description	Rating
1	Compromised	Server has been compromised with WebShell or backlink, etc.	5
2	Attacked	It is unknown if the server has been compromised, but log archives show evidence of SQL injection, brute-force login, Webshell upload, etc.	3-4
3	Data harvested	It is unknown if the server has been compromised, but there is evidence that data has been harvested.	2
4	Vulnerable	It is unknown if the server has been compromised, but it contains security vulnerabilities.	1

Gambar 14 Serverity

Gambar 11 menunjukan tingkat keparahan penyerangan terhadap server, dengan hasil penyarengan sebagai berikut :

1. Disusupi, telah disusupi dengan WebShell atau Backlink, dll, dengan peringkat 5.
2. Diserang, Tidak diketahui apakah server telah disusupi, tetapi arsip log menunjukkan bukti injeksi SQL, login paksa, unggahan Webshell, dll, dengan peringkat 3-4.
3. Data, Tidak diketahui apakah server telah disusupi, tetapi ada bukti bahwa data telah diambil, dengan peringkat 2.
4. Rentan, Tidak diketahui apakah server telah disusupi, tetapi berisi kerentanan keamanan, dengan peringkat 1.



No.	Severity	Rating	Description
1	Compromised Host is infected with malware.	10	Host visits malicious URL, domain name or IP address related to known malware, exfiltrates data or may have infected the database server.
		9	Host visits malicious URL, domain name and IP address related to known malware, attempts to spread malicious file to other hosts.
		8	Host visits URL, domain name or IP address related to known malware.
2	High Host is very likely infected with malware.	7	Host launches outgoing DDoS attacks or visits suspicious Conficker domain names.
		6	Host sends or receives suspicious packets related to malware, or spreads malicious shellcode.
		5	Host visits DGA-generated domain names, or initiates reverse connection.
3	Medium Host is not acting like an infected host but malware has been downloaded.	4	Host downloads malicious executable files, PDF files or Trojan virus-infected webpage, but has not been infected yet.
		3	Host downloads suspicious files, such as those with unmatching name and extension, but has not been infected yet.

Gambar 15 Host Security Rating

Gambar 15 menunjukan peringkat keamanan host, dengan ketentuan sebagai berikut:

1. Compromised : Host yang disusupi terinfeksi
    a. Rating 10: Host mengunjungi URL berbahaya, nama domain, atau alamat IP yang terkait dengan malware yang diketahui, mengekstrak data atau mungkin telah menginfeksi server database.
    b. Rating 9: Host mengunjungi URL berbahaya, nama domain, dan alamat IP yang terkait dengan malware yang diketahui, mencoba menyebarkan file berbahaya ke host lain.
    c. Rating 8: Host mengunjungi URL, nama domain, atau alamat IP yang terkait dengan malware yang dikenal.
2. High : Host sangat mungkin terinfeksi malware.
    a. Rating 7: Host meluncurkan serangan DDoS keluar atau mengunjungi nama domain Conficker yang mencurigakan.
    b. Rating 6: Host mengirim atau menerima paket mencurigakan yang terkait dengan malware, atau menyebarkan shellcode berbahaya.
    c. Rating 5: Host mengunjungi nama domain yang dihasilkan DGA, atau memulai koneksi balik.
3. Medium : Host tidak bertindak seperti host yang terinfeksi tetapi malware telah diunduh.
    a. Rating 4: Host mengunduh file executable berbahaya, file PDF, atau halaman web yang terinfeksi virus Trojan, tetapi belum terinfeksi.
    b. Rating 3: Host mengunduh file yang mencurigakan, seperti file dengan

nama dan ekstensi yang tidak cocok, tetapi belum terinfeksi.

4. Low : Host mungkin terinfeksi malware.
    a. Rating 2: Host menggunakan protokol yang terkait dengan malware (seperti IRC, HFS, dll.) dan mengunjungi nama domain atau alamat IP yang mencurigakan terkait dengan malware
    b. Rating 1: Lalu lintas yang mencurigakan terdeteksi, seperti protokol SSL yang digunakan pada port selain port 443, tetapi tingkat keparahannya rendah. Host dapat mengunjungi situs web/email phishing yang mencuri informasi akun.

KESIMPULAN

Dari hasil penelitian "Analisa Penerapan Ferewall Sebagai Keamanan Pada Jaringan Internet Universitas Muhammadiyah Purwokerto", didapat bahwa peringkat keamanan secara keseluruhan buruk, meskipun sebagian besar serangan diblokir oleh Sangfor NGAF. Ada beberapa server dari Universitas Muhammadiyah Purwokerto yang diserang dan server yang paling parah terkena dampak serangan adalah server dengan alamat IP 103.120.232.122 dalam kurun waktu 30 Hari. Server tersebut dikendalikan oleh penyerang dan telah menderita 28.581 serangan, dan 6 kerentanan telah terdeteksi dimana penyerang telah mengunggah 76 WebShell backdoor.dan SQL Injection. WAF bekerja berdasarkan rule dan mekanisme pemindaian script atau request berbahaya. Selain itu memilik kemampuan penolakan terhadap script atau request sebagai pencegahan dari serangan berbahaya ke web server yang berisi request HTTP sesuai dengan aturan yangtelah ditetapkan.

DAFTAR PUSTAKA

Ahmad, F. (2014). " Analisis penerapan firewall sebagai sistem keamanan jaringan pada PT. PLN (Persero) penyaluran dan pusat pengatur beban Jawa - Bali (P3B)". http://repository.uinjkt.ac.id/dspace/handle/123456789/24457, diakses pada 14 Agustus 2021 pukul 07.26.

Arlis, S., & Sahari. (2019). " ANALISIS FIREWALL DEMILITARIZED ZONE DAN SWITCH PORT SECURITY PADA JARINGAN UNIVERSITAS PUTRA INDONESIA YPTK ". https://core.ac.uk/download/pdf/229586196.pdf, diakses pada 14 Agustus 2021 pukul 08.14..

Hamawari, M. S., & Kurniawan, I. F. (2019). " PENERAPAN IPTABLES FIREWALL PADA LINUX DENGAN MENGGUNAKAN FEDORA". https://jurnalmahasiswa.unesa.ac.id/index.php/jurnal-manajemen-informatika/article/view/18283, diakses pada 14 Agustus 2021 pukul 10.45..

Hidayat, R. P., Primananda, R., & Widasari, R. E. (2019). " Analisis Performa Centralized Firewall pada Multi Domain Controller di Arsitektur Software-Defined Networking (SDN)". https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/1674, diakses pada 2 Agustus 2021 pukul 08.51.

Langobelen, S. R., Rachmawati, Y., & Iswahyudi, C. (2019). "ANALISIS DAN OPTIMASI DARI SIMULASI KEAMANAN JARINGAN MENGGUNAKAN FIREWALL MIKROTIK STUDI KASUS DI TAMAN PINTAR YOGYAKARTA". https://journal.akprind.ac.id/index.php/jarkom/article/view/2253, diakses pada 2 Agustus 2021 pukul 11.07.

Purwoko, M., & Hilal, H. (2019). " Analisis Penerapan Firewall Nftables Sebagai Sistem Keamanan Server Pada Mesin Virtualisasi ". https://pdfs.semanticscholar.org/ccb5/e17cb34f7cacb1a203d198525ed539c7fadc.pdf, diakses pada 2 Agustus 2021 pukul 13.18.

Realize, & Hananti, U. (2017). " PENGARUH PENGGUNAAN IPTABLES FIREWALL DAN ACID TERHADAP KEAMANAN JARINGAN". https://www.google.com/url?client=internalelementcse&cx=001431978847466539083:xsldadcvvvo&q=http://ejournal.stkippgrisumbar.ac.id/index.php/eDikInformatika/article/download/1896/pdf&sa=U&ved=2ahUKEwiKhczV35jyAhUCH7cAHT_MDgMQFjABegQICRAB&usg=AOvVaw2scgPrHtp9I_H2I4oKteoU, diakses pada 2 Agustus 2021 pukul 16.27.

Rizal, R. Sumaryana, Y. 2020. Peningkatan Keamanan Aplikasi Web Menggunakan Web Aplication Firewall (WAF) Pada Sistem Informasi Manajemen Kampus Terintegrasi. Jurnal Information Communication & Technology. 20(2): 323-330.