Jurnal Ilmu Pendidikan (ILPEN) Halaman 8-12
e-ISSN 2830-3709 Volume 4 Nomor 2 Tahun 2025

Analisis Keamanan Web Server pada Infrastruktur Jaringan *Dual Router MikroTik*: Studi Penetration Testing dan Perumusan Kebijakan Keamanan

Ugan Suganda
Politeknik Istikom Bina Citra Informatika
e-mail : sugandaugan7@gmail.com

Abstrak

Penelitian ini bertujuan merancang topologi jaringan client-server menggunakan dua router MikroTik di lingkungan Proxmox, melakukan penetration testing untuk mengidentifikasi kerentanan pada web server, serta merumuskan kebijakan keamanan jaringan berdasarkan temuan. Metode yang digunakan meliputi setup infrastruktur virtual dengan 4 VM, konfigurasi routing statis, dan scanning menggunakan Nmap. Hasil penelitian menunjukkan 7 port terbuka dengan temuan kritis pada Port 9000 (Portainer) yang memiliki skor risiko 25, serta kerentanan tinggi pada Port 22 (OpenSSH) dengan skor 16. Kebijakan keamanan dirumuskan mencakup hardening server, manajemen akses, monitoring, dan respon insiden dengan prioritas pada mitigasi kerentanan kritis.

Kata kunci: Topologi Jaringan, *Mikrotik, Proxmox, Penetration Testing,* Kebijakan Keamanan

Abstract

This study aims to design a client-server network topology using two MikroTik routers in a Proxmox environment, conduct penetration testing to identify vulnerabilities in the web server, and formulate network security policies based on findings. The method includes virtual infrastructure setup with 4 VMs, static routing configuration, and Nmap scanning. Results showed 7 open ports with a critical finding on Port 9000 (Portainer) with a risk score of 25, and a high vulnerability on Port 22 (OpenSSH) with a score of 16. Security policies were formulated covering server hardening, access management, monitoring, and incident response with priority on mitigating critical vulnerabilities.

Keywords: *Network Topology, Mikrotik, Proxmox, Penetration Testing, Security Policy*

PENDAHULUAN

Perkembangan teknologi virtualisasi seperti Proxmox VE memungkinkan simulasi infrastruktur jaringan yang kompleks tanpa memerlukan perangkat fisik. Penggunaan dual router MikroTik dalam topologi client-server memberikan fleksibilitas dalam segmentasi jaringan dan kontrol akses. Web server sebagai penyedia layanan utama menghadapi berbagai ancaman keamanan. Hasil scan terhadap domain portofolio.daftartugasku.my.id menunjukkan penggunaan Cloudflare sebagai proxy, yang memberikan lapisan keamanan tambahan namun tetap menyisakan kerentanan pada layer internal. Berdasarkan latar belakang tersebut, rumusan masalah dalam penelitian ini adalah: (1) Bagaimana merancang topologi jaringan client-server menggunakan 2 router MikroTik di lingkungan Proxmox? (2) Kerentanan apa saja yang teridentifikasi pada server melalui penetration testing internal? (3) Bagaimana merumuskan kebijakan keamanan jaringan berdasarkan hasil analisis risiko? Tujuan penelitian ini adalah mengimplementasikan topologi jaringan dengan dual router MikroTik di Proxmox, mengidentifikasi dan menganalisis kerentanan server melalui penetration testing, serta menyusun kebijakan keamanan jaringan yang komprehensif. Penelitian dibatasi pada lingkungan simulasi menggunakan Proxmox VE, pengujian terbatas pada server dengan IP 192.168.100.20, metode pengujian menggunakan Nmap dan analisis konfigurasi, serta domain portofolio.daftartugasku.my.id dianalisis untuk konteks proxy.

TINJAUAN LITERATUR

Proxmox Virtual Environment (Proxmox VE) adalah platform virtualisasi open-source yang mengintegrasikan KVM dan LXC, memungkinkan pengelolaan mesin virtual dan kontainer dengan antarmuka web terpadu (Proxmox, 2023). Platform ini dipilih karena kemampuannya dalam mensimulasikan jaringan kompleks dengan biaya rendah. MikroTik RouterOS merupakan sistem operasi berbasis Linux yang dirancang untuk fungsi routing, firewall, dan manajemen bandwidth. Dalam topologi dual router, masing-masing router dapat dikonfigurasi untuk segmentasi jaringan yang berbeda (MikroTik, 2024). Routing statis digunakan untuk jaringan sederhana karena konfigurasinya yang mudah dan prediktif. Cloudflare menyediakan layanan CDN dan keamanan dengan bertindak sebagai reverse proxy. Server asli (origin) tidak terekspos langsung ke internet, hanya IP Cloudflare yang terlihat publik. Hal ini memberikan perlindungan DDoS dan hide origin IP (Cloudflare, 2024). Namun perlindungan ini hanya efektif untuk serangan eksternal, tidak untuk serangan internal. Penetration testing adalah simulasi serangan terotorisasi untuk mengidentifikasi kerentanan. Nmap merupakan tool populer untuk port scanning dan service enumeration (Lyon, 2009). Analisis risiko menggunakan matriks Likelihood-Impact untuk menentukan prioritas penanganan, mengacu pada standar NIST SP 800-30. Kebijakan keamanan mengacu pada framework ISO 27001 dan NIST SP 800-53 yang mencakup aspek teknis, administratif, dan fisik (NIST, 2020). Kebijakan yang baik harus mencakup manajemen akses, patch management, monitoring, dan respon insiden.

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimental dengan pendekatan studi kasus. Tahapan penelitian meliputi setup infrastruktur, konfigurasi jaringan, penetration testing, analisis risiko, dan perumusan kebijakan. Alat dan bahan yang digunakan terdiri dari Proxmox VE 7.4-3 sebagai hypervisor utama, MikroTik RouterOS 7.10 untuk kedua router, Ubuntu Server 22.04 LTS sebagai web server, Puppy Linux Fossa64 9.5 sebagai client, serta Nmap 7.98 dan cURL 7.81 untuk pengujian. Topologi jaringan dibangun dengan empat virtual machine di Proxmox. MikroTik 1 memiliki dua network interface: ether1 terhubung ke server (vmbr1) dengan IP 192.168.10.1/24, dan ether2 terhubung ke MikroTik 2 (vmbr2) dengan IP 10.10.10.1/30. MikroTik 2 juga memiliki dua interface: ether1 terhubung ke MikroTik 1 (vmbr2) dengan IP 10.10.10.2/30, dan ether2 terhubung ke client (vmbr3) dengan IP 192.168.20.1/24. Server Ubuntu dikonfigurasi dengan IP 192.168.10.2/24 dan gateway 192.168.10.1. Client Puppy Linux menggunakan IP 192.168.20.2/24 dengan gateway 192.168.20.1.

Routing statis dikonfigurasi pada MikroTik 1 dengan perintah ip route add dst-address=192.168.20.0/24 gateway=10.10.10.2 dan pada MikroTik 2 dengan perintah ip route add dst-address=192.168.10.0/24 gateway=10.10.10.1. Pengujian dimulai dengan analisis eksternal menggunakan cURL terhadap domain portofolio.daftartugasku.my.id untuk memahami mekanisme proxy. Selanjutnya dilakukan scanning internal menggunakan Nmap dengan perintah nmap -sV 192.168.100.20 untuk mengidentifikasi port terbuka dan versi layanan. Hasil scanning dianalisis menggunakan matriks risiko dengan skala Likelihood 1-5 dan Impact 1-5, dimana skor risiko = Likelihood × Impact. Kategori risiko ditentukan sebagai Critical (20-25), High (12-16), Medium (6-10), dan Low (1-5).

HASIL DAN PEMBAHASAN

Implementasi Topologi

Topologi berhasil diimplementasikan dengan empat VM di Proxmox. Pengujian konektivitas menunjukkan client (192.168.20.2) dapat mencapai server (192.168.10.2) melalui kedua router dengan packet loss 0%, membuktikan routing statis berfungsi dengan baik. Waktu response rata-rata 2-3 ms menunjukkan performa jaringan yang optimal dalam lingkungan virtual.

Analisis Eksternal Domain

Pengujian terhadap domain portofolio.daftartugasku.my.id menggunakan cURL menghasilkan response header yang menunjukkan penggunaan Cloudflare sebagai proxy. Hal ini terlihat dari

header server: cloudflare dan cf-ray: 9d1b1a0389f6e244-MRS. Teknologi backend teridentifikasi sebagai PHP/8.2.30 dari header x-powered-by. Hasil nslookup menunjukkan domain mengarah ke IP Cloudflare yaitu 104.21.56.15 dan 172.67.175.176, serta alamat IPv6 2606:4700:3033::6815:380f dan 2606:4700:3035::ac43:afb0. Origin IP server tidak terekspos, memberikan perlindungan dari serangan langsung ke server asli.

Hasil Penetration Testing Internal

Scanning pada IP internal 192.168.100.20 menggunakan Nmap menghasilkan temuan sebagai berikut:

Tabel 1. Hasil Port Scanning pada Server Internal

Port	State	Service	Version
22/tcp	open	SSH	OpenSSH 8.9p1 Ubuntu
80/tcp	open	HTTP	OpenResty web app server
81/tcp	open	HTTP	OpenResty web app server
443/tcp	open	HTTPS	openresty
3030/tcp	open	HTTP	Apache httpd 2.4.65 ((Debian))
8080/tcp	open	HTTP	Apache httpd 2.4.66 ((Debian))
9000/tcp	open	HTTP	Golang net/http server

Port 9000 teridentifikasi sebagai Golang net/http server. Berdasarkan fingerprint Nmap, layanan ini menunjukkan karakteristik Portainer, yaitu web UI untuk manajemen Docker. Response header menunjukkan Content-Security-Policy yang ketat dengan referensi ke Matomo, HubSpot, dan Google reCAPTCHA, mengindikasikan lingkungan production yang kompleks.

Analisis Risiko

Analisis risiko dilakukan menggunakan matriks Likelihood dan Impact dengan hasil sebagai berikut:

Tabel 2. Analisis Risiko Kerentanan

Kerentanan	Likelihood	Impact	Skor	Level
Port 9000 - Portainer UI	5 (High)	5 (Critical)	25	Critical
Port 22 - OpenSSH 8.9p1	4 (High)	4 (High)	16	High
Port 3030 - Apache 2.4.65	3 (Medium)	3 (Medium)	9	Medium
Port 8080 - Apache 2.4.66	3 (Medium)	3 (Medium)	9	Medium
Port 80/81/443 - OpenResty	2 (Low)	3 (Medium)	6	Low-Medium

Temuan kritis pada Port 9000 disebabkan Portainer memberikan akses penuh ke lingkungan Docker. Jika dieksploitasi, attacker dapat mengontrol semua container, membuat container baru dengan akses host, atau mencuri data sensitif. Eksposur port ini ke jaringan internal, meskipun tidak publik, tetap berisiko tinggi jika attacker berhasil mengakses jaringan internal melalui client yang terkompromi. Port 22 dengan OpenSSH 8.9p1 memiliki risiko tinggi karena SSH adalah pintu masuk utama ke server. Serangan brute force atau exploitasi CVE pada versi ini dapat memberikan akses shell ke attacker. Meskipun versi 8.9p1 relatif baru, konfigurasi default seringkali lemah seperti mengizinkan login password dan root login. Apache pada port 3030 dan 8080 memberikan risiko medium. Risiko spesifik tergantung pada aplikasi web yang dihosting, namun keberadaan dua instance Apache memperluas attack surface dan memerlukan audit keamanan terpisah. OpenResty pada port 80, 81, dan 443 berfungsi sebagai reverse proxy. Risiko lebih rendah karena umumnya tidak menyimpan data langsung dan konfigurasi keamanan dapat diterapkan di layer proxy.

Pembahasan

Penggunaan Cloudflare memberikan lapisan keamanan yang efektif untuk serangan eksternal. Hal ini terkonfirmasi dari tidak terekspos nya origin IP dalam response header dan DNS lookup. Namun penting dipahami bahwa Cloudflare hanya melindungi traffic publik. Jika origin IP bocor melalui DNS history, misconfiguration, atau internal leak, semua perlindungan menjadi tidak berlaku. Selain itu, Cloudflare tidak memberikan perlindungan terhadap serangan yang berasal dari dalam jaringan internal. Temuan tujuh port terbuka pada server internal menunjukkan praktik keamanan yang perlu ditingkatkan. Port yang tidak diperlukan seharusnya ditutup atau dibatasi aksesnya. Khusus untuk Port 9000, idealnya tidak diekspos sama sekali ke jaringan dan hanya diakses melalui SSH tunneling atau VPN. Kombinasi dual router MikroTik memberikan segmentasi jaringan yang baik, namun routing statis yang digunakan tidak memiliki kemampuan failover atau load balancing. Untuk lingkungan production, protokol routing dinamis seperti OSPF dapat dipertimbangkan.

.

SIMPULAN DAN SARAN

Berdasarkan penelitian yang dilakukan, dapat disimpulkan bahwa topologi jaringan dengan dual router MikroTik di Proxmox berhasil diimplementasikan dengan routing statis, memungkinkan client mengakses server melalui dua hop router. Penetration testing mengungkapkan tujuh port terbuka dengan temuan kritis pada Port 9000 (Portainer) skor risiko 25, dan kerentanan tinggi pada Port 22 (OpenSSH) skor 16. Penggunaan Cloudflare pada domain publik memberikan perlindungan origin IP namun tidak melindungi dari serangan internal. Kebijakan keamanan dirumuskan mencakup hardening teknis, manajemen akses, monitoring, dan respon insiden dengan prioritas mitigasi kerentanan kritis. Saran untuk penelitian selanjutnya adalah melakukan penetration testing lebih mendalam dengan tools seperti Burp Suite, Metasploit, dan OWASP ZAP untuk mengeksploitasi kerentanan yang ditemukan. Implementasi sistem monitoring terpusat seperti ELK Stack atau Prometheus perlu dievaluasi efektivitasnya. Untuk praktisi, disarankan segera membatasi akses Port 9000 dengan firewall rule, melakukan hardening SSH sesuai rekomendasi, dan memasang fail2ban untuk perlindungan brute force.

DAFTAR PUSTAKA

Ary, D., Jacobs, L.C. & Razavieh, A. 1976. *Pengantar Penelitian Pendidikan.* Terjemahan oleh Arief Furchan. 1982. Surabaya: Usaha nasional

Cloudflare. 2024. *What is a reverse proxy?*. Cloudflare Learning Center. https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy/

Kansil, C.L. 2002. Orientasi Baru Penyelenggaraan Pendidikan Program Profesional dalam Memenuhi Kebutuhan Dunia Idustri. *Transpor*, XX(4): 54-61

Lyon, G.F. 2009. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure

MikroTik. 2024. *RouterOS Manual*. MikroTik Documentation. https://wiki.mikrotik.com/wiki/Manual

NIST. 2020. *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53, Revision 5

OWASP Foundation. 2023. *OWASP Top 10:2021*. OWASP. https://owasp.org/Top10/

Proxmox. 2023. *Proxmox VE Administration Guide*. Proxmox Server Solutions GmbH. https://pve.proxmox.com/wiki/Main_Page

Stallings, W. 2017. *Network Security Essentials: Applications and Standards*. Pearson

Waseso, M.G. 2001. *Isi dan Format Jurnal Ilmiah*. Makalah disajikan dalam Seminar Lokakarya Penulisan artikel dan Pengelolaan jurnal Ilmiah, Universitas Lambungmangkurat.