UNIVERSITAS GADJAH MADA

Sample Penetration Test Report
Example Company

Company: Customer Name
Date: 06 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 Sat Jul  6 19:05:49 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 (0.00012s 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
MAC Address: 00:50:56:97:49:B5 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.33.102.226
Host is up (0.00013s 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
MAC Address: 00:50:56:97:D8:D2 (VMware)
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 Sat Jul  6 19:05:57 2024 -- 2 IP addresses (2 hosts up)
scanned in 8.03 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

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

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

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.