ATRAK - DOS

DEFACEMMENT ATTACK

DISCO DURO

MARCOS | DANIEL | PEDRO

CONTENIDO

ANÁLISIS DE DISCO

LOGS DEL SISTEMA

APACHE

Error.log

Que se ha encontrado en este log de errores en Apache:

- A las **06:25:02 a.m,** Apache se inicia y reanuda el funcionamiento normal, mostrando la línea de comando utilizada para iniciar el proceso.
- A las **11:08:46 a. m,** el cliente con dirección **IP 94.242.54.22** intentó acceder a los archivos **searchreplacedb2.php** y **Emergency.php,** pero no pudo encontrarlos ni leerlos. Estos intentos de acceso pueden ser parte de un intento de ataque, o simplemente un rastreador o un escáner de seguridad que intenta detectar problemas de configuración del sitio.
- A las **11:08:48 a. m,** Se produjo un error fatal de PHP en el mismo cliente, relacionado con la **función_deprecated_file()** en el archivo **rss-functions.php.** Esto podría indicar un problema con la instalación de WordPress o la configuración del servidor.
- A las **11:10:16 a.m,** se produjo otro error fatal de PHP en el mismo cliente. Esta vez se trata de la función **get_header()** en el archivo **index.php** del tema **Twenty Seventeen.** Esto puede indicar un problema con el tema de WordPress activo.

Error.log

```
[Mon Jul 23 06:25:02.066358 2018] [mpm_prefork:notice] [pid 27428] AH00163: Apache/2.4.18 (Ubuntu)
OpenSSL/1.0.2g configured -- resuming normal operations
[Mon Jul 23 06:25:02.066389 2018] [core:notice] [pid 27428] AH00094: Command line: '/usr/sbin/apache2'
[Mon Jul 23 11:08:46.122251 2018] [:error] [pid 6262] [client 94.242.54.22:53632] script
'/var/www/html/wordpress/searchreplacedb2.php' not found or unable to stat, referer:
https://ganga.site/
[Mon Jul 23 11:08:46.279207 2018] [:error] [pid 6262] [client 94.242.54.22:53632] script
'/var/www/html/wordpress/emergency.php' not found or unable to stat, referer: https://ganga.site/
[Mon Jul 23 11:08:48.309567 2018] [:error] [pid 6262] [client 94.242.54.22:53632] PHP Fatal error:
Uncaught Error: Call to undefined function _deprecated_file() in
/var/www/html/wordpress/wp-includes/rss-functions.php:8\nStack trace:\n#0 {main}\n  thrown in
/var/www/html/wordpress/wp-includes/rss-functions.php on line 8, referer: https://ganga.site/
[Mon Jul 23 11:10:16.670795 2018] [:error] [pid 6266] [client 94.242.54.22:53652] PHP Fatal error:
Uncaught Error: Call to undefined function get_header() in
/var/www/html/wordpress/wp-content/themes/twentyseventeen/index.php:18\nStack trace:\n#0 {main}\n
thrown in /var/www/html/wordpress/wp-content/themes/twentyseventeen/index.php on line 18, referer:
https://ganga.site/
```

Access.log

- Se realizaron múltiples solicitudes **GET** a archivos como **readme.txt**, **changelog.txt**, **CHANGELOG.md** y **changelog.md** en el directorio de complementos **reflex-gallery**.
- Se envió una solicitud **GET** al directorio de inicio **reflex-gallery** y al archivo **error_log**.
- Se realizaron múltiples solicitudes **POST** al archivo **FileUploader/php.php** dentro del directorio **reflex-gallery/admin/scripts/** con múltiples parámetros de solicitud (**año** y **mes**).
- La solicitud **GET** se envió a varios archivos **PHP** en el directorio **wp-content/uploads/2018/07/** con diferentes nombres de archivo, como **vmGAbaiewrSSuMs.php**, **XLPYhlEtQOyiMKb.php**, **yDdoSpsx.php**,**PLoeJFOEVoc.php**.
- Las solicitudes **GET** también se realizan a la página principal del sitio y otras páginas y recursos no relacionados con la **Galería Reflex**.
- Parece que se está usando **WPScan**, una herramienta de escaneo de seguridad para **WordPress**, para encontrar posibles vulnerabilidades en el complemento **reflex-gallery**. También parece que se está intentando descargar y ejecutar un archivo **PHP** malicioso en el servidor al explotar una vulnerabilidad en la subida de archivos del plugin.

Access.log

```
[23/Jul/2018:11:10:12 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-admin/js/updates.js HTTP/1.1 79108
"https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:12 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-includes/css/customize-preview-rtl.css
HTTP/1.1 6497 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:13 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /feed/ HTTP/1.1 280 "https://ganga.site/"
"WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:13 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /feed/rdf/ HTTP/1.1 284
"https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:13 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /feed/atom/ HTTP/1.1 285
"https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:13 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /readme.html HTTP/1.1 7413
"https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:13 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /sitemap.xml HTTP/1.1 286
"https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:13 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-links-opml.php HTTP/1.1 223
"https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:14 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/themes/twentyseventeen/style.css HTTP/1.1 82584 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:15 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/themes/twentyseventeen/readme.txt HTTP/1.1 319 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:15 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/themes/twentyseventeen/README.txt HTTP/1.1 3219 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:16 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/themes/twentyseventeen/changelog.txt HTTP/1.1 322 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:16 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/themes/twentyseventeen/CHANGELOG.md HTTP/1.1 321 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:16 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/themes/twentyseventeen/changelog.md HTTP/1.1 321 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:16 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-content/themes/twentyseventeen/
HTTP/1.1 - "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:17 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/themes/twentyseventeen/error_log HTTP/1.1 318 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:18 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/plugins/reflex-gallery/readme.txt HTTP/1.1 8632 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:18 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/plugins/reflex-gallery/changelog.txt HTTP/1.1 322 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:18 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/plugins/reflex-gallery/CHANGELOG.md HTTP/1.1 321 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:19 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/plugins/reflex-gallery/changelog.md HTTP/1.1 321 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:19 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-content/plugins/reflex-gallery/
HTTP/1.1 3482 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:10:19 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/plugins/reflex-gallery/error_log HTTP/1.1 318 "https://ganga.site/" "WPScan v2.9.5-dev (http://wpscan.org)"
[23/Jul/2018:11:20:20 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/plugins/reflex-gallery/readme.txt HTTP/1.1 8632 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

```
[23/Jul/2018:11:20:26 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 POST
/wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php?Year=2018&Month=07 HTTP/1.1 55 "-" "Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1)"
218.211.168.176 - - [23/Jul/2018:11:22:49 +0000] "GET / HTTP/1.1" 200 606 "-" "Mozilla/5.0"
[23/Jul/2018:11:22:57 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/plugins/reflex-gallery/readme.txt HTTP/1.1 8632 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
[23/Jul/2018:11:23:04 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 POST
/wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php?Year=2018&Month=07 HTTP/1.1 54 "-" "Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1)"
[23/Jul/2018:11:23:56 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 POST
/wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php?Year=2018&Month=07 HTTP/1.1 61 "-" "Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1)"
[23/Jul/2018:11:20:28 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-content/uploads/2018/07/PSMOfbPom.php
HTTP/1.1 2 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
[23/Jul/2018:11:23:57 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/uploads/2018/07/XLPYhlEtQOyiMKb.php HTTP/1.1 2 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
[23/Jul/2018:11:25:35 +0000] ganga.site 88.0.112.115 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 POST
/wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php?Year=2018&Month=07 HTTP/1.1 61 "-" "Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1)"
[23/Jul/2018:11:23:05 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-content/uploads/2018/07/yDdoSpsx.php
HTTP/1.1 2 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
88.132.175.225 - - [23/Jul/2018:11:41:11 +0000] "GET / HTTP/1.0" 200 982 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64;
Trident/5.0)"
[23/Jul/2018:11:25:35 +0000] ganga.site 88.0.112.115 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/uploads/2018/07/vmGAbaiewrSSuMs.php HTTP/1.1 2 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
[23/Jul/2018:11:53:18 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:53:18 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:53:18 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:53:50 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:53:50 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:53:51 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:53:58 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:54:18 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:54:31 +0000] ganga.site 88.0.112.115 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET
/wp-content/plugins/reflex-gallery/readme.txt HTTP/1.1 8632 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
[23/Jul/2018:11:54:34 +0000] ganga.site 88.0.112.115 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 POST
/wp-content/plugins/reflex-gallery/admin/scripts/FileUploader/php.php?Year=2018&Month=07 HTTP/1.1 57 "-" "Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1)"
[23/Jul/2018:12:00:25 +0000] ganga.site 88.0.112.115 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET / HTTP/1.1 191819 "-" "Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0"
[23/Jul/2018:11:54:34 +0000] ganga.site 88.0.112.115 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-content/uploads/2018/07/PLoeJFOEVoc.php
HTTP/1.1 2 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
86.60.204.220 - - [23/Jul/2018:12:45:33 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
[23/Jul/2018:14:07:36 +0000] ganga.site 184.105.247.196 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET / HTTP/1.1 259510 "-" "-"
[23/Jul/2018:14:45:29 +0000] ganga.site 13.56.248.111 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /ws/2/ HTTP/1.1\n 303 "-" "-"
46.48.233.147 - - [23/Jul/2018:15:28:19 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
143.208.184.92 - - [23/Jul/2018:16:04:06 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
115.78.133.167 - - [23/Jul/2018:16:43:58 +Sv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET / HTTP/1.1 191819 "-" "Mozilla/5.0 (Macintosh; Intel Mac
OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36"
[23/Jul/2018:19:17:10 +0000] ganga.site 5.188.210.7 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /?q=node/2 HTTP/1.0 259510
"https://ganga.site/?q=node/2" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84
Safari/537.36"0000] "GET /manager/html HTTP/1.1" 404 450 "-" "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)"
89.111.244.174 - - [23/Jul/2018:16:45:44 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36"
185.10.68.233 - - [23/Jul/2018:17:27:17 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
[23/Jul/2018:18:26:24 +0000] ganga.site 13.57.233.99 TL
138.186.147.94 - - [23/Jul/2018:19:55:25 +0000] "GET / HTTP/1.0" 200 982 "-" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64;
Trident/5.0)"
137.74.30.57 - - [23/Jul/2018:20:50:07 +0000] "GET / HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/41.0.2228.0 Safari/537.36"
92.38.46.186 - - [23/Jul/2018:22:09:06 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
31.202.42.113 - - [23/Jul/2018:22:46:51 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
187.101.58.33 - - [23/Jul/2018:23:21:39 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
```

BTMP

Se observa todos los intento fallidos que se ha intentado conectar por SSH, con lo cual se muestra lo siguiente usuarios que se ha intentado acceder realizando un ataque de fuerza bruta o por diccionario.

- **admin**: 155.12.57.222, 143.255.153.97, 131.108.166.224, 211.72.111.206, 59.124.22.241, 197.44.3.22, 210.13.64.18, 118.163.71.225, 211.107.97.253, 180.183.128.213, 103.99.1.140, 186.47.175.7, 200.71.90.124, 58.82.129.141, 220.180.89.90, 14.111.111.119, 78.4.139.110, 5.101.40.81, 197.42.22.156, 119.201.84.153, 197.50.219.6, 113.190.235.155, 123.20.90.211, 41.238.241.99
- **user**: 5.101.40.81
- **user1**: 5.101.40.81
- **ubnt**: 211.72.111.206, 59.124.22.241, 197.44.3.22, 196.218.27.188, 197.50.219.6
- **support**: 211.72.111.206, 59.124.22.241, 197.44.3.22, 103.99.1.140, 197.50.219.6
- **operator**: 103.99.1.140, 103.99.1.140
- **test**: 103.99.1.140, 103.99.1.140
- **1234**: 5.101.40.81
- **PlcmSpIp**: 49.51.85.33
- **dave**: 49.51.85.33
- **monitor**: 49.51.85.33

Error.log

```
ssh:notty
admin
155.12.57.222
ssh:notty
admin
143.255.153.97
ssh:notty
admin
131.108.166.224
ssh:notty
user
5.101.40.81
ssh:notty
user1
5.101.40.81
ssh:notty
ubnt
211.72.111.206
ssh:notty
admin
211.72.111.206
ssh:notty
support
211.72.111.206
ssh:notty
...
```

ARCHIVOS DEL SISTEMA

INDEX.HTML

Este es el archivo que subió al servidor web, con el que se realizó el defacement, se obtuvo con exiftool los metadatos del archivo, como de la imágen que se encontraba en este.

INDEX.HTML

METADATOS INDEX.HTML

```
C:\Users\Usuario.DANIEL\Desktop\exiftool>metadato.exe "D:\autopsy\Analisis Disco\Export\index.html"
ExifTool Version Number         : 12.59
File Name                       : index.html
Directory                       : D:/autopsy/Analisis Disco/Export
File Size                       : 260 kB
File Modification Date/Time     : 2023:04:02 20:04:02+02:00
File Access Date/Time           : 2023:04:02 20:06:46+02:00
File Creation Date/Time         : 2023:04:02 20:04:02+02:00
File Permissions                : -rw-rw-rw-
File Type                       : HTML
File Type Extension             : html
MIME Type                       : text/html
```

METADATOS IMAGE.PNG

```
C:\Users\Usuario.DANIEL\Desktop\exiftool>metadato.exe "D:\autopsy\Analisis Disco\Export\image.png"
ExifTool Version Number         : 12.59
File Name                       : image.png
Directory                       : D:/autopsy/Analisis Disco/Export
File Size                       : 197 kB
File Modification Date/Time     : 2023:04:02 19:36:37+02:00
File Access Date/Time           : 2023:04:02 20:16:30+02:00
File Creation Date/Time         : 2023:04:02 19:36:37+02:00
File Permissions                : -rw-rw-rw-
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 1200
Image Height                    : 1200
Bit Depth                       : 8
Color Type                      : RGB
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Image Size                      : 1200x1200
Megapixels                      : 1.4
```

PHP.PHP

Este es el archivo de configuración que utiliza el plugin **reflex-gallery** , el cual, es vulnerable a subidas de archivos ejecutables.

- Se verifica si la extensión del archivo es permitido comparándolo con la lista de extensiones permitidas, en caso de no tener una extensión compatible devuelve un error.
- Se indica no sobreescribir el archivo si ya existe con el mismo nombre, se genera un nuevo nombre para almacenar dicho archivo añadiendo un número aleatorio al final.
- Se guarda el archivo en el directorio **uploads**
- Se muestra una lista de las extensiones permitidas.
- No filtra los archivos subidos de manera adecuada, provocando que puedan realizarse subidas de archivos maliciosos cambiando la información de la cabecera donde se encuentra la extensión antes de enviar la petición.

PHP.PHP

```
if($this->allowedExtensions && !in_array(strtolower($ext), $this->allowedExtensions)){
            $these = implode(', ', $this->allowedExtensions);
            return array('error' => 'File has an invalid extension, it should be one of '. $these .
'.');
        }

        if(!$replaceOldFile){
            /// don't overwrite previous files that were uploaded
            while (file_exists($uploadDirectory . $filename . '.' . $ext)) {
                $filename .= rand(10, 99);
            }
        }

        if ($this->file->save($uploadDirectory . $filename . '.' . $ext)){
            $uploadDir = str_replace("../../../../../uploads/", "/", $uploadDirectory);
            return array('success'=>true, 'fileName'=>$uploadDir . $filename . '.' . $ext);
        } else {
            return array('error'=> 'Could not save uploaded file.' .
                'The upload was cancelled, or server error encountered');
        }

    }
}
// list of valid extensions, ex. array("jpeg", "xml", "bmp")
$allowedExtensions = array();
```

SSH_CONFIG

Este es el archivo donde se encuentra la configuración del servicio **SSH**, siendo susceptible a que se puedan realizar ataques de diccionario para acceder al servicio, ya que no limita la cantidad de **logins**, ni tampoco especifica direcciones **IP** que permitan únicamente realizar la conexión.

- El puerto SSH se establece en **Port 22**
- Se establecen como permitidas las opciones de autenticación para **RSA** y contraseñas.
- Se indica que las opciones de configuración se apliquen a todos los hosts.
- Se establece **PermitLocalCommand no** por lo que no se permitirá la ejecución de comandos locales en el host remoto.

SSH_CONFIG

```
Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   RhostsRSAAuthentication no
#   RSAAuthentication yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
```

```
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/identity
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Protocol 2
#   Cipher 3des
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
    GSSAPIDelegateCredentials no
```

CVE-2015-4133

La vulnerabilidad utilizada por el atacante en el sistema se basa en la carga de archivos sin restricciones en **admin/scripts/FileUploader/php.php** en el plugin **Reflex-Gallery** utilizado en wordpress, permitiendo al atacante ejecutar código arbitrario de **PHP** al cargar un archivo con la extensión **PHP** y accediendo con una solicitud directa a la ruta de dicho archivo para ejecutarlo en el sistema como el usuario **www-data**.

ANEXO

ERROR.LOG

ERROR.LOG	error.log	
CAPTURA	[Mon Jul 23 06:25:02.066358 2018] [mpm_prefork:notice] [pid 27428] AH00163: Apache/2.4.18 (Ubuntu) OpenSSL/1.0.2g configured -- resuming normal operations [Mon Jul 23 06:25:02.066389 2018] [core:notice] [pid 27428] AH00094: Command line: '/usr/sbin/apache2' [Mon Jul 23 11:08:46.122251 2018] [:error] [pid 6262] [client 94.242.54.22:53632] script '/var/www/html/wordpress/searchreplacedb2.php' not found or unable to stat, referer: https://ganga.site/ [Mon Jul 23 11:08:46.279207 2018] [:error] [pid 6262] [client 94.242.54.22:53632] script '/var/www/html/wordpress/emergency.php' not found or unable to stat, referer: https://ganga.site/ [Mon Jul 23 11:08:48.309567 2018] [:error] [pid 6262] [client 94.242.54.22:53632] PHP Fatal error: Uncaught Error: Call to undefined function _deprecated_file() in /var/www/html/wordpress/wp-includes/rss-functions.php:8\nStack trace:\n#0 {main}\n thrown in /var/www/html/wordpress/wp-includes/rss-functions.php on line 8, referer: https://ganga.site/ [Mon Jul 23 11:10:16.670795 2018] [:error] [pid 6266] [client 94.242.54.22:53652] PHP Fatal error: Uncaught Error: Call to undefined function get_header() in /var/www/html/wordpress/wp-content/themes/twentyseventeen/index.php:18\nStack trace:\n#0 {main}\n thrown in /var/www/html/wordpress/wp-content/themes/twentyseventeen/index.php on line 18, referer: https://ganga.site/	
HASH	SHA1	064fdd82955e34d2872aede4aa97fc983f830fb6
	MD5	496044572974077b25d87ecc950ec4bc

ACCESS.LOG

ACCESS.LOG

access.log

CAPTURA

```
[23/Jul/2018:11:20:28 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-content/uploads/
2018/07/PSMOfbPom.php HTTP/1.1 2 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
[23/Jul/2018:11:23:57 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-content/uploads/
2018/07/XLPYhlEtQOyiMKb.php HTTP/1.1 2 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
[23/Jul/2018:11:25:35 +0000] ganga.site 88.0.112.115 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 POST /wp-content/plugins/
reflex-gallery/admin/scripts/FileUploader/php.php?Year=2018&Month=07 HTTP/1.1 61 "-" "Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1)"
[23/Jul/2018:11:23:05 +0000] ganga.site 94.242.54.22 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-content/uploads/
2018/07/yDdoSpsx.php HTTP/1.1 2 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
88.132.175.225 - - [23/Jul/2018:11:41:11 +0000] "GET / HTTP/1.0" 200 982 "-" "Mozilla/5.0 (compatible; MSIE 9.0;
Windows NT 6.1; WOW64; Trident/5.0)"
[23/Jul/2018:11:25:35 +0000] ganga.site 88.0.112.115 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-content/uploads/
2018/07/vmGAbaiewrSSuMs.php HTTP/1.1 2 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
[23/Jul/2018:11:53:18 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:53:18 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:53:18 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:53:50 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:53:50 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:53:51 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:53:58 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:54:18 +0000] ganga.site 88.0.112.115 - - GET / HTTP/1.0 439 "-" "-"
[23/Jul/2018:11:54:31 +0000] ganga.site 88.0.112.115 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-content/plugins/
reflex-gallery/readme.txt HTTP/1.1 8632 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
[23/Jul/2018:11:54:34 +0000] ganga.site 88.0.112.115 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 POST /wp-content/plugins/
reflex-gallery/admin/scripts/FileUploader/php.php?Year=2018&Month=07 HTTP/1.1 57 "-" "Mozilla/4.0 (compatible;
MSIE 6.0; Windows NT 5.1)"
[23/Jul/2018:12:00:25 +0000] ganga.site 88.0.112.115 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET / HTTP/1.1 191819 "-"
"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:54.0) Gecko/20100101 Firefox/54.0"
[23/Jul/2018:11:54:34 +0000] ganga.site 88.0.112.115 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /wp-content/uploads/
2018/07/PLoeJFOEVoc.php HTTP/1.1 2 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
86.60.204.220 - - [23/Jul/2018:12:45:33 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
[23/Jul/2018:14:07:36 +0000] ganga.site 184.105.247.196 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET / HTTP/1.1 259510
"-" "-"
[23/Jul/2018:14:45:29 +0000] ganga.site 13.56.248.111 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /ws/2/ HTTP/1.1\n
303 "-" "-"
46.48.233.147 - - [23/Jul/2018:15:28:19 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
143.208.184.92 - - [23/Jul/2018:16:04:06 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
115.78.133.167 - - [23/Jul/2018:16:43:58 +0000] "GET /manager/html HTTP/1.1" 404 450 "-" "Mozilla/5.0 (compatible;
MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)"
89.111.244.174 - - [23/Jul/2018:16:45:44 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36"
185.10.68.233 - - [23/Jul/2018:17:27:17 +0000] "GET / HTTP/1.1" 400 0 "-" "-"
[23/Jul/2018:18:26:24 +0000] ganga.site 13.57.233.99 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET / HTTP/1.1 191819 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100
Safari/537.36"
[23/Jul/2018:19:17:10 +0000] ganga.site 5.188.210.7 TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 GET /?q=node/2 HTTP/1.0
259510 "https://ganga.site/?q=node/2" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/63.0.3239.84 Safari/537.36"
138.186.147.94 - - [23/Jul/2018:19:55:25 +0000] "GET / HTTP/1.0" 200 982 "-" "Mozilla/5.0 (compatible; MSIE 9.0;
Windows NT 6.1; WOW64; Trident/5.0)"
137.74.30.57 - - [23/Jul/2018:20:50:07 +0000] "GET / HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36"
92.38.46.186 - - [23/Jul/2018:22:09:06 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
31.202.42.113 - - [23/Jul/2018:22:46:51 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
187.101.58.33 - - [23/Jul/2018:23:21:39 +0000] "GET / HTTP/1.1" 200 926 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
```

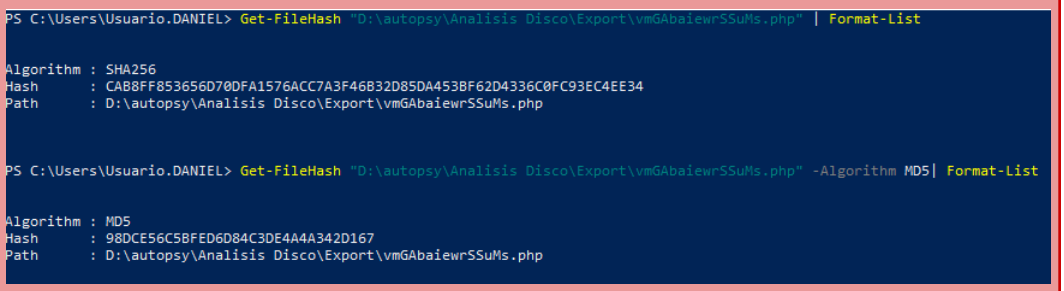
HASH

SHA1	b9008fda5c891b12fd3b9bdc3a8bd5f958341057
MD5	325d4e7fad4213e46faf58dcf76af017

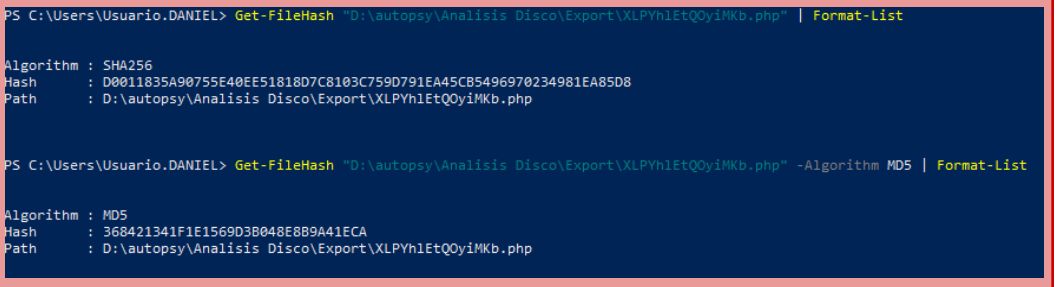
BTMP

BTMP		btmp
CAPTURA		103.99.1.140 ssh:notty ubnt 103.99.1.140 ssh:notty admin 103.99.1.140 ssh:notty operator 103.99.1.140 ssh:notty admin 103.99.1.140 ssh:notty test 103.99.1.140 7U[ssh:notty admin 197.42.22.156 ssh:notty admin 14.186.151.234 ssh:notty admin 119.201.84.153 ssh:notty ubnt 197.50.219.6 ssh:notty admin 197.50.219.6 ssh:notty support 197.50.219.6 ssh:notty admin 197.50.219.6 ssh:notty admin 113.190.235.155 ssh:notty admin 123.20.90.211 ssh:notty admin 41.238.241.99 ssh:notty 109.67.103.179 ssh:notty 109.67.103.179
HASH	SHA1	a7b0bc3abd6fb18940dbb6f6fe3b18160134b950
	MD5	de08163bc6f1bf28cb1df5729939890d

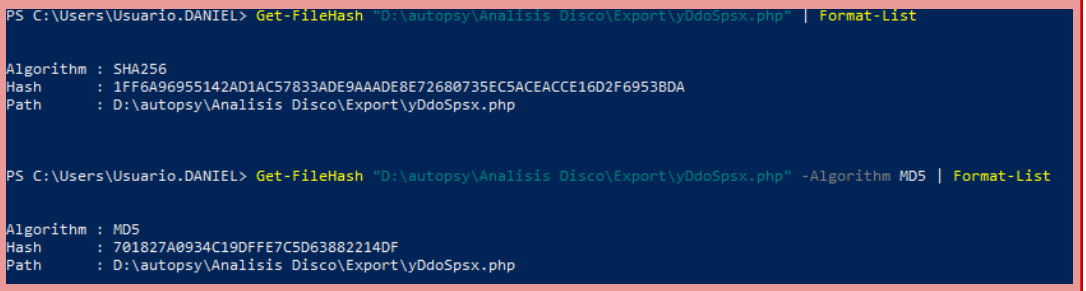
vmGAbaiewrSSuMs.php

vmGAbaiewrSSuMs.php	vmGAbaiewrSSuMs.php	
CAPTURA		
HASH	SHA-256	CAB8FF853656D70DFA1576ACC7A3F46B32D85DA453BF62D4336C0FC93EC4EE34
	MD5	98DCE56C5BFED6D84C3DE4A4A342D167

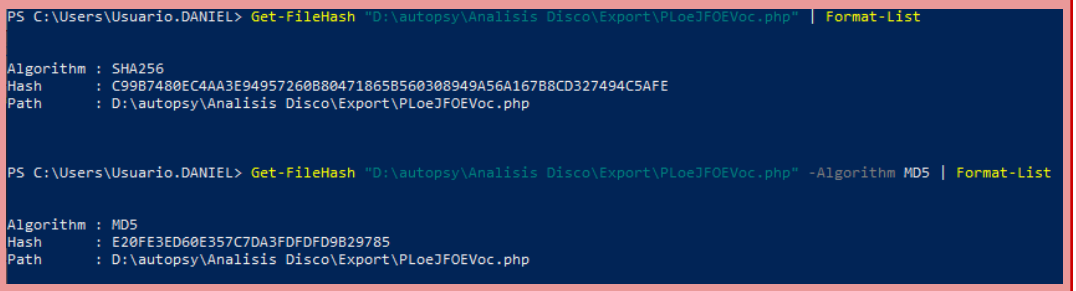
XLPYhlEtQOyiMKb.php

XLPYhlEtQOyiMKb.php	XLPYhlEtQOyiMKb.php	
CAPTURA		
HASH	SHA-256	D0011835A90755E40EE51818D7C8103C759D791EA45CB5496970234981EA85D8
	MD5	368421341F1E1569D3B048E8B9A41ECA

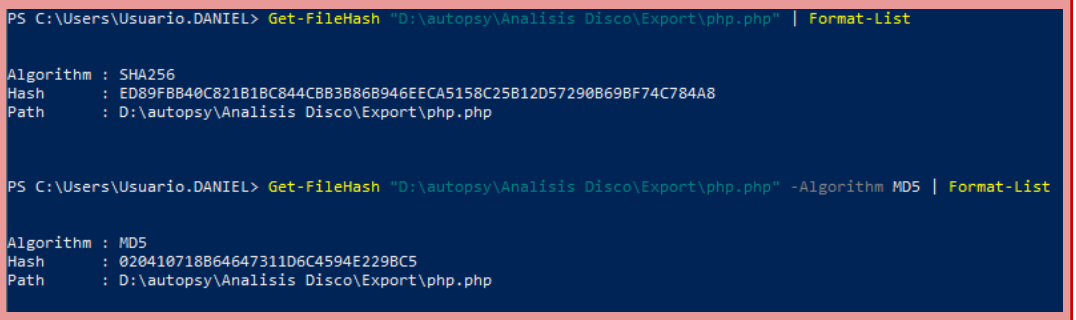
yDdoSpsx.php

yDdoSpsx.php	yDdoSpsx.php	
CAPTURA		
HASH	SHA-256	1FF6A96955142AD1AC57833ADE9AAADE8E72680735EC5ACEACCE16D2F6953BDA
	MD5	701827A0934C19DFFE7C5D63882214DF

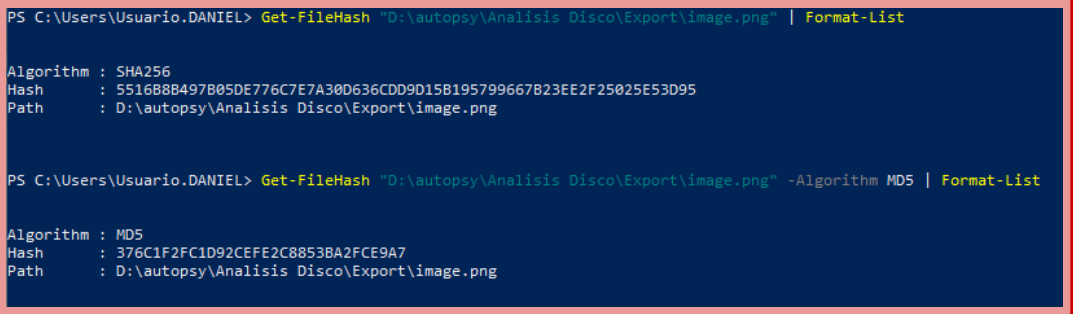
PLoeJFOEVoc.php

PLoeJFOEVoc.php	PLoeJFOEVoc.php	
CAPTURA		
HASH	SHA-256	C99B7480EC4AA3E94957260B80471865B560308949A56A167B8CD327494C5AFE
	MD5	E20FE3ED60E357C7DA3FDFDFD9B29785

PHP.PHP

PHP.php	php.php	
CAPTURA		
HASH	SHA-256	ED89FBB40C821B1BC844CBB3B86B946EECA5158C25B12D57290B69BF74C784A8
	MD5	020410718B64647311D6C4594E229BC5

SSH_CONFIG

SSH_CONFIG	ssh_config	
CAPTURA		
HASH	SHA-256	5516B8B497B05DE776C7E7A30D636CDD9D15B195799667B23EE2F25025E53D95
	MD5	376C1F2FC1D92CEFE2C8853BA2FCE9A7

index.html

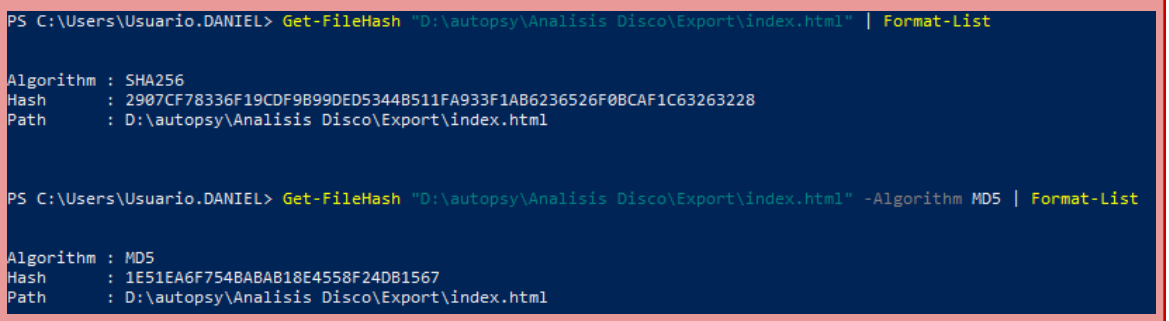
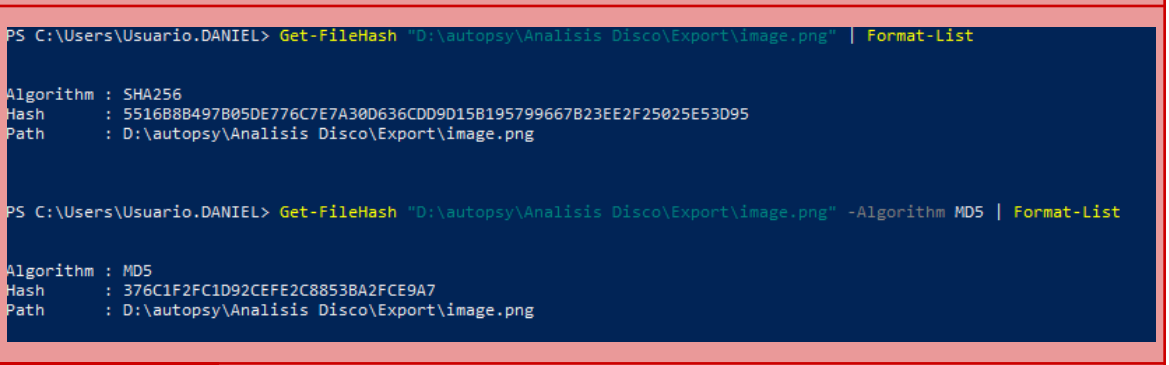
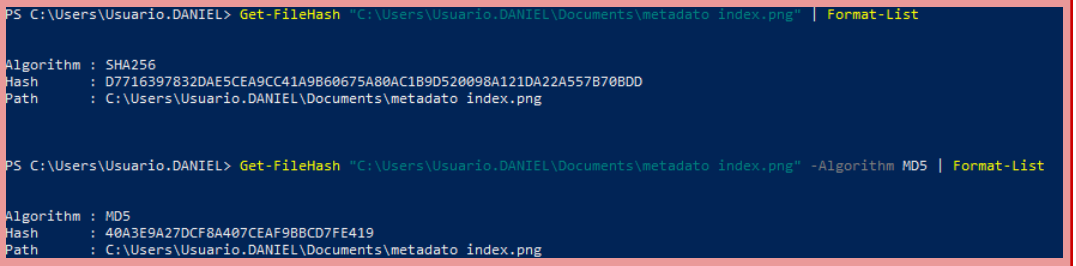
index.html	index	
CAPTURAS		
HASH	SHA-256	2907CF78336F19CDF9B99DED5344B511FA933F1AB6236526F0BCAF1C63263228
	MD5	1E51EA6F754BABAB18E4558F24DB1567

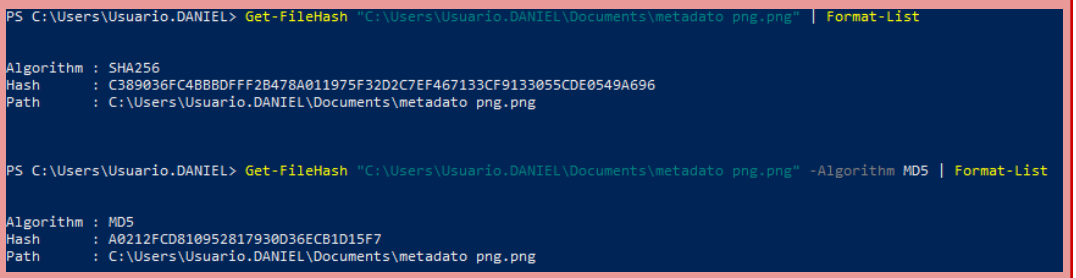
image.png

imagen.png	image.png	
CAPTURAS		
HASH	SHA-1	5516B8B497B05DE776C7E7A30D636CDD9D15B195799667B23EE2F25025E53D95
	MD5	376C1F2FC1D92CEFE2C8853BA2FCE9A7

METADATOS INDEX.HTML

METADATOS INDEX.HTML	metadato index.png	
CAPTURA		
HASH	SHA-256	D7716397832DAE5CEA9CC41A9B60675A80AC1B9D520098A121DA22A557B70BDD
	MD5	40A3E9A27DCF8A407CEAF9BBCD7FE419

METADATOS IMAGE.PNG

METADATOS IMAGE.PNG	metadato png.png	
CAPTURA		
HASH	SHA-256	C389036FC4BBBDFFF2B478A011975F32D2C7EF467133CF9133055CDE0549A696
	MD5	A0212FCD810952817930D36ECB1D15F7