

Forum: [Hack Forums](#)

Thread: [dnsspoof on kali issue](#)

kdls - August 26, 2016, 10:13 am

Hi, I just tried dnsspoof on Kali, and it did not work in an interesting way. Here is what I did, I start the arpspoof first, with ip forwarding, the man in the middle works. Then I started the apache server, and the dnsspoof with a config file, mapping some address to kali local ip. And this is what I got when the target is trying to connect those address

```
Code root@kali:~# dnsspoof -i eth0 -f dnshost.spoof
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.0.112]
192.168.0.108.56523 > 192.168.1.1.53: 26782+ A? somelinkhere
192.168.0.108.56523 > 192.168.1.1.53: 26782+ A? somelinkhere
192.168.0.108.57090 > 192.168.1.1.53: 21153+ A? somelinkhere
192.168.0.108.57090 > 192.168.1.1.53: 21153+ A? somelinkhere
```

```
^Croot@kali:~# gedit dnshost.spoof
```

```
root@kali:~# dnsspoof -i eth0 -f dnshost.spoof
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.0.112]
192.168.0.108.62281 > 192.168.1.1.53: 10039+ A? someotherlinkhere
192.168.0.108.62281 > 192.168.1.1.53: 10039+ A? someotherlinkhere
192.168.0.108.62281 > 192.168.0.1.53: 10039+ A? someotherlinkhere
192.168.0.108.62281 > 192.168.0.1.53: 10039+ A? someotherlinkhere
```

Now this is why I thought to be interesting, target ip is 192.168.0.108, kali ip is 192.168.0.112, but there are two layers of router, one router is connected to wan directly, and it has a gateway 192.168.1.1, under it, there is a second router with a gateway of 192.168.0.1. The target was not redirected to kali's apache, but still able to reach the right web.

I am not sure how the dnsspoof works on kali, but theoretically, regardless if the request from target is going through the outter router or not, the real webpage package should always pass through kali, and with the dnsspoof running, it should be stopped, if I understand it correctly.

Is this issue due to the two layers of router? Should I arpspoof between the outter one and the target? Please, any idea will be appreciated, thanks!

Goodies - August 26, 2016, 2:54 pm

I'm not quite sure what you're talking about with the routers... but it seems to me that the two IP's, assuming a mask of 255.255.255.0 (/24 CIDR), the two devices are in the same subnet.

The way ARP works is via layer 2. Any victim must be both within your same layer 2 broadcast domain and IP subnet. That does not work when there is an intermediary router (i.e. the victim is in a different VLAN).

However, this seems moot because I would assume that your devices ARE in the same VLAN. You should be spoofing the IP of your default gateway. I.E. 192.168.0.1. NOT 192.168.1.1.

Now, if the IP address of the DNS server is 192.168.1.1, that means its in a subnet different to the one in which the victim is. That means it STILL has to go out of its default gateway. For that, you should set up a virtual interface (or even sub interface) with that IP, but you should not at all be sending spoof ARP packets to 192.168.1.1.

kdlsw - August 26, 2016, 7:59 pm

(Aug 26, 2016 02:54 PM)Goodies Wrote: [\[CITE\]](#) I'm not quite sure what you're talking about with the routers... but it seems to me that the two IP's, assuming a mask of 255.255.255.0 (/24 CIDR), the two devices are in the same subnet.

The way ARP works is via layer 2. Any victim must be both within your same layer 2 broadcast domain and IP subnet. That does not work when there is an intermediary router (i.e. the victim is in a different VLAN).

However, this seems moot because I would assume that your devices ARE in the same VLAN. You should be spoofing the IP of your default gateway. I.E. 192.168.0.1. NOT 192.168.1.1.

Now, if the IP address of the DNS server is 192.168.1.1, that means its in a subnet different to the one in which the victim is. That means it STILL has to go out of its default gateway. For that, you should set up a virtual interface (or even sub interface) with that IP, but you should not at all be sending spoof ARP packets to 192.168.1.1.

I am sorry for my unclear description, allow me explain again. There is an router A (192.168.1.1), connected to WAN directly (I think it's a router function integrated modem), and there is another router B (192.168.0.1), connected to A, I saw the WAN IP in its config page as 192.168.1.2, and all the PC and other devices are connected to B, because I can see them in router B's DHCP list.

The victim and attacker are definitely both under the same layer of LAN, their ip are both 192.168.0.x, actually the attacker kali is a VM running on the victim. I am also quite confused why the victim has direct interaction with router A.

Goodies - August 27, 2016, 11:53 am

(Aug 26, 2016 07:59 PM)kdls Wrote: [\[CITE\]](#) I am sorry for my unclear description, allow me explain again. There is an router A (192.168.1.1), connected to WAN directly (I think it's a router function integrated modem), and there is another router B (192.168.0.1), connected to A, I saw the WAN IP in its config page as 192.168.1.2, and all the PC and other devices are connected to B, because I can see them in router B's DHCP list.

The victim and attacker are definitely both under the same layer of LAN, their ip are both 192.168.0.x, actually the attacker kali is a VM running on the victim. I am also quite confused why the victim has direct interaction with router A.

The first thing I'm going to do is recommend you get one of the routers the fuck out of there. Double NAT-ing is just about always a very bad and completely unnecessary idea.

The issue is most likely due to the fact that the kali machine is on the host you're attacking. If you're using any kind of bridge or NAT adapter, then you should expect issues. The only way to prevent that is to detach the host's adapter from the Kali machine completely and use an external USB wireless card for the Kali machine. As of now, the host machine's ARP table is all kinds of fucked up, and if it is NAT-ed to the Kali VM, that will just cause more problems...

Use separate machines or a separate NIC and it should clear up.