

Forum:[Hack Forums](#)

Thread: [How to correctly restore ARP cache?](#)

daymon - September 21, 2018, 1:24 pm

I'm using Python3.6 on a Windows 7 Machine with Scapy.

I wanted to set up a system that intercepts traffic on the network and logs it, and potentially to venture into filtering it maybe. My ARP poisoning and logging works perfectly fine, but my attempt to restore the connection after seems to always fail and I have to manually reconnect to the network on the system I was ARP'ing.

Heres my code:

```
Code def restore_network(gateway_ip, gateway_mac, target_ip, target_mac):  
    send(ARP(op=2, hwdst=gateway_mac, pdst=gateway_ip, hwsrc=target_mac, psrc=target_ip),  
count=4)  
    send(ARP(op=2, hwdst=target_mac, pdst=target_ip, hwsrc=gateway_mac, psrc=gateway_ip),  
count=4)
```

I was originally trying to flush it out like so, but to no avail:

```
Code def restore_network(gateway_ip, gateway_mac, target_ip, target_mac):  
    send(ARP(op=2, hwdst="ff:ff:ff:ff:ff:ff", pdst=gateway_ip, hwsrc=target_mac, psrc=target_ip),  
count=4)  
    send(ARP(op=2, hwdst="ff:ff:ff:ff:ff:ff", pdst=target_ip, hwsrc=gateway_mac, psrc=gateway_ip),  
count=4)
```

I'm still learning about networking, so it may be something obvious, but nothing from google could help me. Any sort of pointers in the right direction would be greatly appreciated!

-nugget01 - November 28, 2018, 12:45 pm

When you are ARP poisoning someone you are attempting to change their ARP cache so that your mac address is affiliated with the routers IP and to the router vice versa. Given this freedom to change which mac correlates with which IP address the obvious thing to do when attempting to restore network connection on both ends is to send a broadcast gratuitous ARP with the correct mac correlated to the correct IP. In Scapy that is

Code for i in range(10):

```
    send(ARP(op=2, pdst=gateway_ip, psrc=target_ip, hwdst='ff:ff:ff:ff:ff:ff', hwsrc=target_mac))  
    send(ARP(op=2, pdst=target_ip, psrc=gateway_ip, hwdst='ff:ff:ff:ff:ff:ff', hwsrc=gateway_mac))
```

Notice how I am sending 10 ARP packets however this is to guarantee and make sure the system receives these ARP packets on its end.

daymon - November 29, 2018, 3:14 pm

(Nov 28, 2018 01:45 PM)-nugget01 Wrote: [\[CITE\]](#) When you are ARP poisoning someone you are attempting to change their ARP cache so that your mac address is affiliated with the routers IP and to the router vice versa. Given this freedom to change which mac correlates with which IP address the obvious thing to do when attempting to restore network connection on both ends is to send a broadcast gratuitous ARP with the correct mac correlated to the correct IP. In Scapy that is

Code for i in range(10):

```
    send(ARP(op=2,pdst=gateway_ip,psrc=target_ip,hwdst='ff:ff:ff:ff:ff:ff',hwsrc=target_mac))
```

```
    send(ARP(op=2,pdst=target_ip,psrc=gateway_ip,hwdst='ff:ff:ff:ff:ff:ff',hwsrc=gateway_mac))
```

Notice how I am sending 10 ARP packets however this is to guarantee and make sure the system receives these ARP packets on its end.

Thanks for the response! I didn't even think about packets dropping, I could try sending multiple gratuitous replays and see how it goes ?