

How to Detect Sniffer on Your Network

 hackingarticles.in/detect-sniffer-network

Raj

June 28, 2016

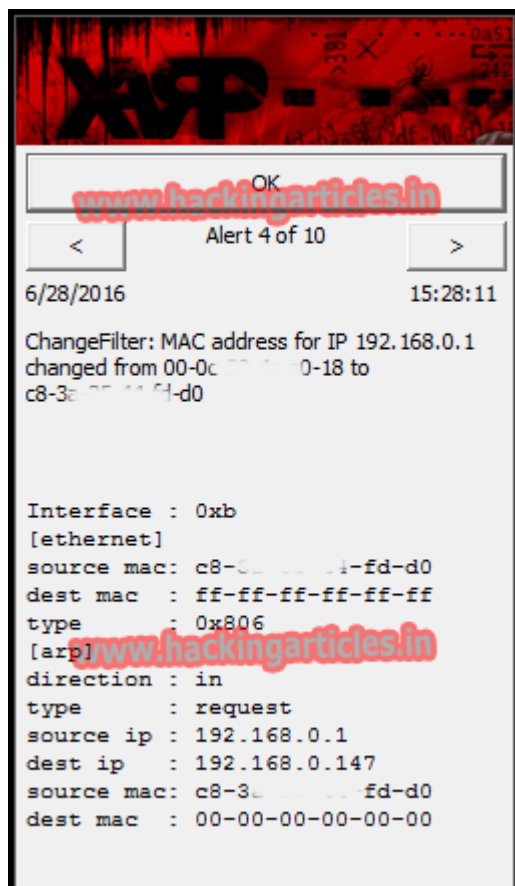
Xarp is an advanced anti-spoofing tool that flags all the spoofing attacks that might be using ARP(address resolution protocol) targeting your system. This includes documents, emails, and VoicelP conversations. ARP attacks allow a hacker to manipulate the data sent over the network. Xarp uses active and passive modules to detect hackers inside the network. Having such tools in the system is very important as the computer firewalls and OS security do not provide protection against ARP attacks.

Download latest Xarp version from <http://xarp.software.informer.com/download/>

After it gets downloaded, install it on your computer. Now, we will perform an attack on a system with Xarp installed To show this tool's effectiveness, we perform the attack with Bettercap


```
root@kali:~# bettercap -T 192.168.0.121 --proxy -P post
[+] Starting [ spoofing:✓ discovery:✗ sniffer:✓ tcp-proxy:✗ http-proxy:✓ https-proxy:✗ sslstrip
[W] You are running an unstable/beta version of this software, please update to a stable one if
[I] Found NetBIOS name 'LAB4-PC' for address 192.168.0.121
[I] [eth0] 192.168.0.123 : 00:0C:29:14:00:18 / eth0 ( VMware )
[I] [GATEWAY] 192.168.0.1 : C8:4F:3E:44:FD:D0 ( Tenda Technology )
[I] [DNS] Starting on 192.168.0.123:5300
[I] [TARGET] 192.168.0.121 : FC:A5:EA / LAB4-PC ( Giga-byte Technology )
[I] [HTTP] Proxy starting on 192.168.0.123:8080 ...
[192.168.0.110] GET http://dns2go.deerfield.net/status/index.cfm?fqdn=w... ( text/html ) [302]
```

As soon as Xarp detects an ARP attack, it shows an alert on the screen like this.



XArp - unregistered version

File XArp Professional Help

 **Status: ARP attacks detected!** Security level set to: basic

- [View detected attacks](#)
- [Read the 'Handling ARP attacks' help](#)
- [View XArp logfile](#)

[Get XArp Professional now!](#)
[Register XArp Professional](#)

aggressive
high
basic
minimal

The basic security level operates the default attack detection strategy that can detect all standard attacks. This is the suggested level for most environments.

	IP	MAC	Host	Vendor	Interface	Online	Cac
✓	169.254.35.85	d8-5d-10-59-44-cb	169.254.35.85	unknown	0xb - Realtek P...	unkno...	no
✗	169.254.170.164	fc-aa-10-6a-a4-e9	LAB1-PC	unknown	0xb - Realtek P...	unkno...	yes
✗	192.168.0.1	c8-3a-38-44-fd-d0	192.168.0.1	Tenda Technol...	0xb - Realtek P...	unkno...	yes
✓	192.168.0.102	fc-aa-10-6a-9e-e6	lab2-pc.rajab....	unknown	0xb - Realtek P...	unkno...	yes
✗	192.168.0.104	fc-aa-10-6a-a4-e8	dc1.rajab.com	unknown	0xb - Realtek P...	unkno...	yes
✓	192.168.0.110	fc-aa-10-6a-8c-ca	lab6-pc.rajab....	unknown	0xb - Realtek P...	unkno...	yes
✗	192.168.0.111	fc-aa-10-6a-a4-e9	lab1-pc.rajab....	unknown	0xb - Realtek P...	unkno...	no
✓	192.168.0.116	60-6d-cb-1c-19-89	win-an96v36m...	unknown	0xb - Realtek P...	unkno...	yes
✓	192.168.0.119	74-d4-3d-11-be-77	pc7-PC	unknown	0xb - Realtek P...	unkno...	yes
✓	192.168.0.120	60-6d-cb-1c-19-89	192.168.0.120	unknown	0xb - Realtek P...	unkno...	yes
✗	192.168.0.121	fc-aa-10-6a-a5-ea	lab4-PC.rajab....	unknown	0xb - Realtek P...	unkno...	no
✓	192.168.0.122	00-08-87-00-e5-16	lab5-pc.rajab....	Avilinks Sa	0xb - Realtek P...	unkno...	yes
✗	192.168.0.123	00-0c-27-1c-a0-18	192.168.0.123	Vmware, Inc.	0xb - Realtek P...	unkno...	yes
✓	192.168.0.126	b8-2a-2d-1a-65-64	DELL-PC	unknown	0xb - Realtek P...	unkno...	yes
✓	192.168.0.128	8c-77-1c-53-30-d8	192.168.0.128	unknown	0xb - Realtek P...	unkno...	yes
✓	192.168.0.129	74-a5-10-79-62-3b	192.168.0.129	unknown	0xb - Realtek P...	unkno...	yes
✓	192.168.0.134	00-0c-27-1c-50-6b	192.168.0.134	Vmware, Inc.	0xb - Realtek P...	unkno...	yes
✓	192.168.0.136	00-0c-27-1c-a5-13	192.168.0.136	Vmware, Inc.	0xb - Realtek P...	unkno...	yes
✓	192.168.0.138	74-d4-3d-11-be-4e	lab8-pc.rajab....	unknown	0xb - Realtek P...	unkno...	yes

XArp 2.2.2 - 29 mappings - 3 interfaces - 21 alerts

It is to be noted that there was no such alert or blocking from both windows firewall and defender, but Xarp detects the intrusion and warns about it.

Author- Shivam Yadav is a certified ethical hacker, an enthusiast and a researcher in this field.