

Forum:[Hack Forums](#)

Thread: [\[TUT\] Discover IPv6 Network Range & Hosts from an IPv6 Enabled Network](#)

ReverseZ - May 7, 2020, 3:10 pm

Welcome to my first official tutorial here on HackForums. I am a 22-year-old pen-tester from Belgium.

You will see many tutorials here on HackForums that are written by me.

Passive_discovery6 passively sniffs the network and dump all client's IPv6 addresses detected. Passive_discovery6 simply sniffs for the neighbor-advertisement packet in IPv6 networks.

You have to understand the basics of IPv6 networks first. Assuming that you know about IPv4 and what an ARP is, neighbor-advertisement & neighbor-solicitation packets replace the ARP(IPv4) in IPv6.

A neighbor-solicitation is the packet sent from a host to a multicast in-order to get information from neighbors just like an ARP request("Who is at 192.168.0.1 tell 192.168.0.2") to broadcast in IPv4.

The neighboring hosts reply with neighbor-advertisement which contains all info including the link-layer address(MAC). Unlike arp, this happens in an asynchronous/irregular pattern in an IPv6 network.

Unlike arp, these packets are continuously transmitted throughout the network.

So what passive_discovery6 does is simply grab the neighbor-solicitation packet and display the information on the terminal. This is very simple to use & provides excellent results when combined with parasite6. Click here to view tutorial on parasite6.

Homepage: https://github.com/mmoya/pkg-thc-ipv6/blob/master/passive_discovery6.c

Note: This tutorial was written when Kali 1.0.9 was the latest. In newer versions (Kali Sana & Kali Rolling) the command has changed to atk6-tool. For example, you are using passive_discovery6, in newer version becomes atk6-passive_discovery6.

Options:

PHP Code

```
<?php
```

Syntax: passive_discovery6 interface options

-D do also dump destination addresses (does not work with -m)

-s do only print the addresses, no other output

-m maxhop the maximum number of hops a target which is dumped may be away.

0 means local only, the maximum amount to make sense is usually 5

-R prefix exchange the defined prefix with the link local prefix

Lab: Discover IPv6 network & Devices

Well, this is simple, just get all your interface names & run the tool on them.

Scenario: I am connected to an IPv6 network with range fc00::00/64 and a couple of hosts are also connected to it.

Command:

Code passive_discovery6 eth0<replace with yours>

Wait for a couple of minutes as the advertisement packets only appear after solicitation packets & that too in an irregular manner. Here is the screenshot

SIM-32901749 - May 7, 2020, 3:28 pm

thank you for this you put some good work into it :)

ReverseZ - May 7, 2020, 4:24 pm

(May 7, 2020 03:28 PM)SIM-32901749 Wrote: [\[CITE\]](#) thank you for this you put some good work into it :)

Thank you, I'm writing other tutorials as well currently.

Today is a productive day.