



MITM ALL THE IPv6 THINGS!

Scott Behrens & Brent Bandelgar

DEF CON 21

August 2, 2013

Who are we?

Scott Behrens

- Senior Security Consultant at Neohapsis
- Adjunct Professor at DePaul University



^- YES THIS IS PHOTOSHOPED

Brent Bandelgar

- Security Consultant at Neohapsis

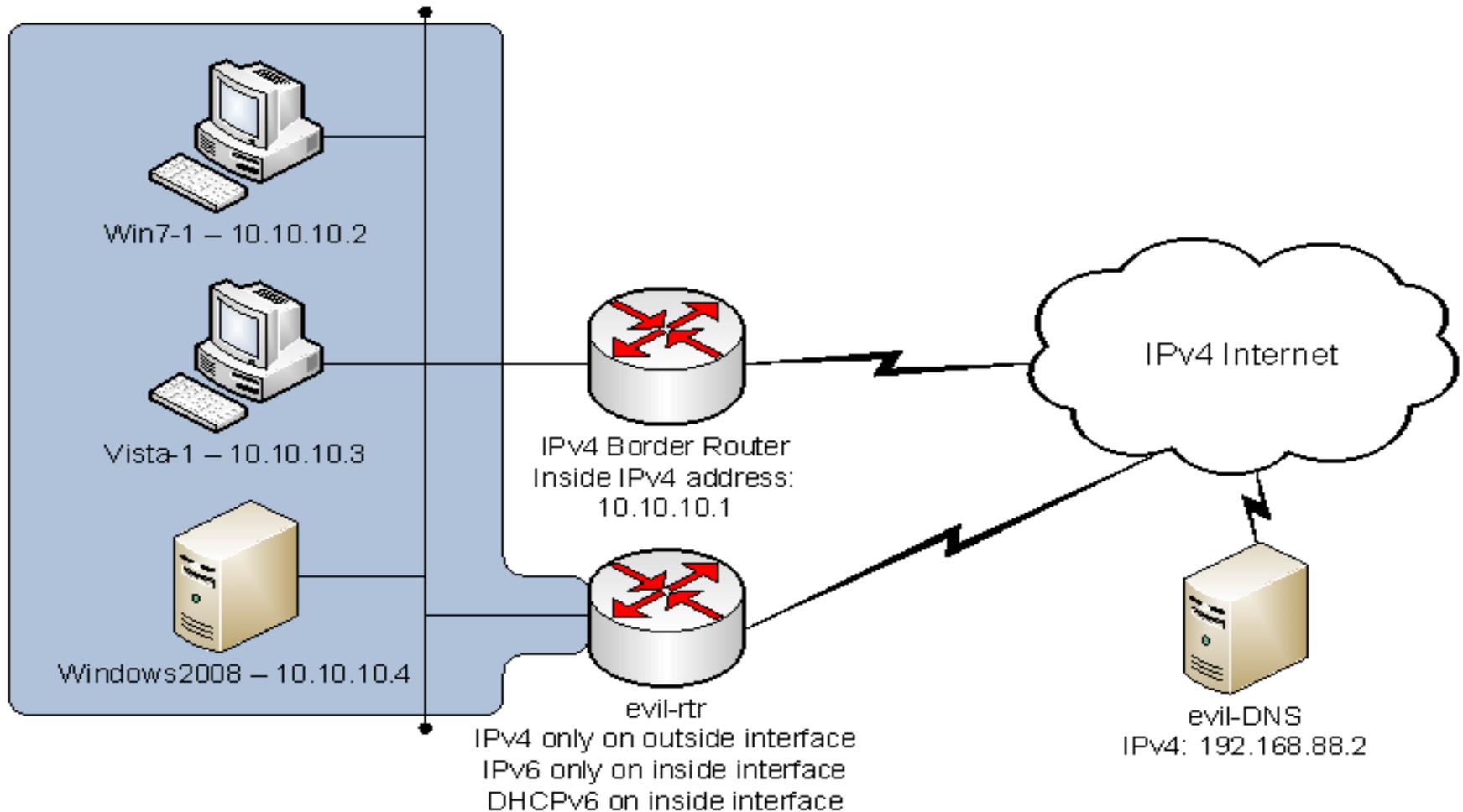


^- THIS ONE IS REAL

Nathaniel Couper-Noles

- Principal Security Consultant at Neohapsis

SLAAC Attack!



Alec Waters, InfoSec Institute 2011 <http://resources.infosecinstitute.com/slaac-attack/>

SLAAC Attack Win8 Fail :(

The image shows a Wireshark capture of network traffic on a VMware virtual network device. The filter is set to 'ipv6'. The packet list shows several ICMPv6 Router Advertisement (RA) packets from source 00:0c:29:0b:39:8d to destination fe80::20c:29ff:fe0b:ff02::1. A TCP packet is also visible, destined for port 49222. The packet details pane shows the selected packet is an Internet Protocol Version 6 (IPv6) packet with a destination address of fe80::20c:29ff:fe0b:ff02::1. The Network Connection Details window is open, showing the IP configuration for the interface. The IPv6 DNS Server field is circled in red, and the text 'Where's the DNS server?' is overlaid on the image.

Property	Value
Physical Address	00-0C-29-19-C7-B8
DHCP Enabled	Yes
IPv4 Address	192.168.99.103
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Monday, March 4, 2013 8:26:35 AM
Lease Expires	Monday, March 4, 2013 10:26:35 AM
IPv4 Default Gateway	192.168.99.1
IPv4 DHCP Server	192.168.99.1
IPv4 DNS Server	192.168.99.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
IPv6 Address	2001:db8:1:0:20d8:5852:4dbd:2fb3
Temporary IPv6 Address	2001:db8:1:0:d557:214a:cd7f:cb29
Link-local IPv6 Address	fe80::20d8:5852:4dbd:2fb3%12
IPv6 Default Gateway	fe80::20c:29ff:fe0b:398d%12
IPv6 DNS Server	

Where's the
DNS server?

SLAAC Attack in 2013...the Bad

- Non trivial setup
 - Configuration files
 - IP addresses/ranges
- It uses old and deprecated packages (NAT-PT)



InfoSec Institute Res x RFC 4862 - IPv6 State x

resources.infosecinstitute.com/slaac-attack/

store=persistent
(A.B.C.D being your corporate IP range & /112 assuming you have an IPv4 /16. Adjust to taste)

Duncan November 13, 2011 at 5:39 am - Reply

I never did get this to work and, yes, i did have a DHCPD6 server running successfully (with config file "dhcpd6.conf" / "dhcpd6.conf" and the subnet and broadcast address are ok (in your case the broadcast address would be 2001:6f8:608:fab::1:6f8:608:fab:)) otherwise the server would not have started in the first place.

There is also a feature in the Windows 7 DHCP client which only would expect if the DHCP server was asking for an IPv6 address. If the Windows machine has obtained a valid global IPv6 address and a valid Temporary IPv6 address and recognizes the Default Gateway IPv6 address. Therefore, the conclusion is that the Windows 7 box does not populate its DNS server cache with the information entered into the dhcpd6.conf file and therefore NAP-TD never gets to see any AAAA request to the fake DNS server. And regarding the link-local issue in my OP, my point was that your interface display did not match reality. As you mentioned, all IPv6 interfaces will have a link-local address auto-configured, yet your display did not which caused confusion. To illustrate, here's the cut-and-paste of your display:

```
root@evil-rtr:~# ifconfig eth1
eth1 Link encap:Ethernet HWaddr 00:25:4b:fd:91:73
inet6 addr: 2001:6f8:608:fab::1/64 Scope:Global
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
Notice that there is no line that says "inet6 addr: Scope:Link".
In general, a how-to article should have all information provided inside it be as accurate and complete as possible.
```

vox January 21, 2013 at 10:30 am - Reply

Hi, great article!!!
just trying to duplicate in a vm lab but cannot get naptd to compile -
did you use to make any changes to the naptd file to make it work
thks
v

DUNCAN COULDN'T GET IT TO WORK?!

VOX COULDN'T GET NAPTD TO COMPILE?!

SLAAC Attack in 2013

WE NEED

AUTOMATION DOMINATION

Solution: Sudden Six

- One Bash script to rule them all!
 - Install dependencies
 - Configure attack host
 - Works with Windows 7 and 8!
- No more depreciated libraries and packages
 - Currently tested on Ubuntu 12.04 LTS and Kali

Demo

- Demo video here

Known Issues

- Defenses
 - Disable IPv6 by policy
 - IPv6 network defenses (RFC 6105)
- Happy Eyeballs
 - IPv4 fallback (RFC 6555)
- DNS
 - Client race conditions

Future Work

- Configure IPv6 tunneling
- Automate basic network reconnaissance
- Detect IPv6 countermeasures
- Leverage THC IPv6 tools
- Specify MITM target scope

 **Download**

We would love your help!

<https://github.com/Neohapsis/suddensix>

Three semi-transparent globes are arranged in a diagonal line from the top-left to the bottom-right. The globe in the foreground is the most prominent and shows the continents of Africa and Europe. The other two globes are blurred and positioned behind it.

Thank You

www.neohapsis.com

labs.neohapsis.com