NEOHAPSIS

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

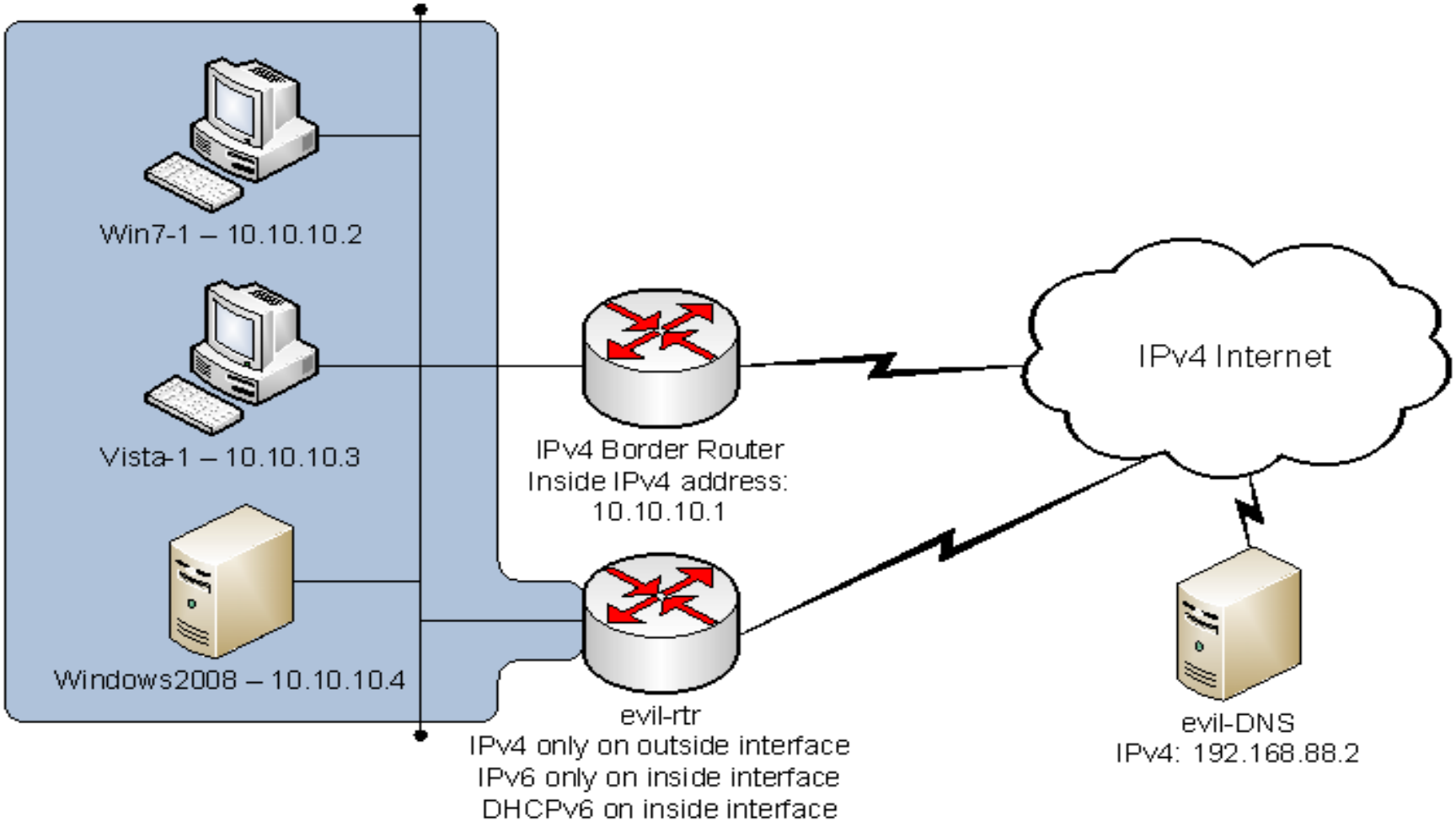
- Security Consultant at Neohapsis

^- THIS ONE IS REAL

Nathaniel Couper-Noles

- Principal Security Consultant at Neohapsis

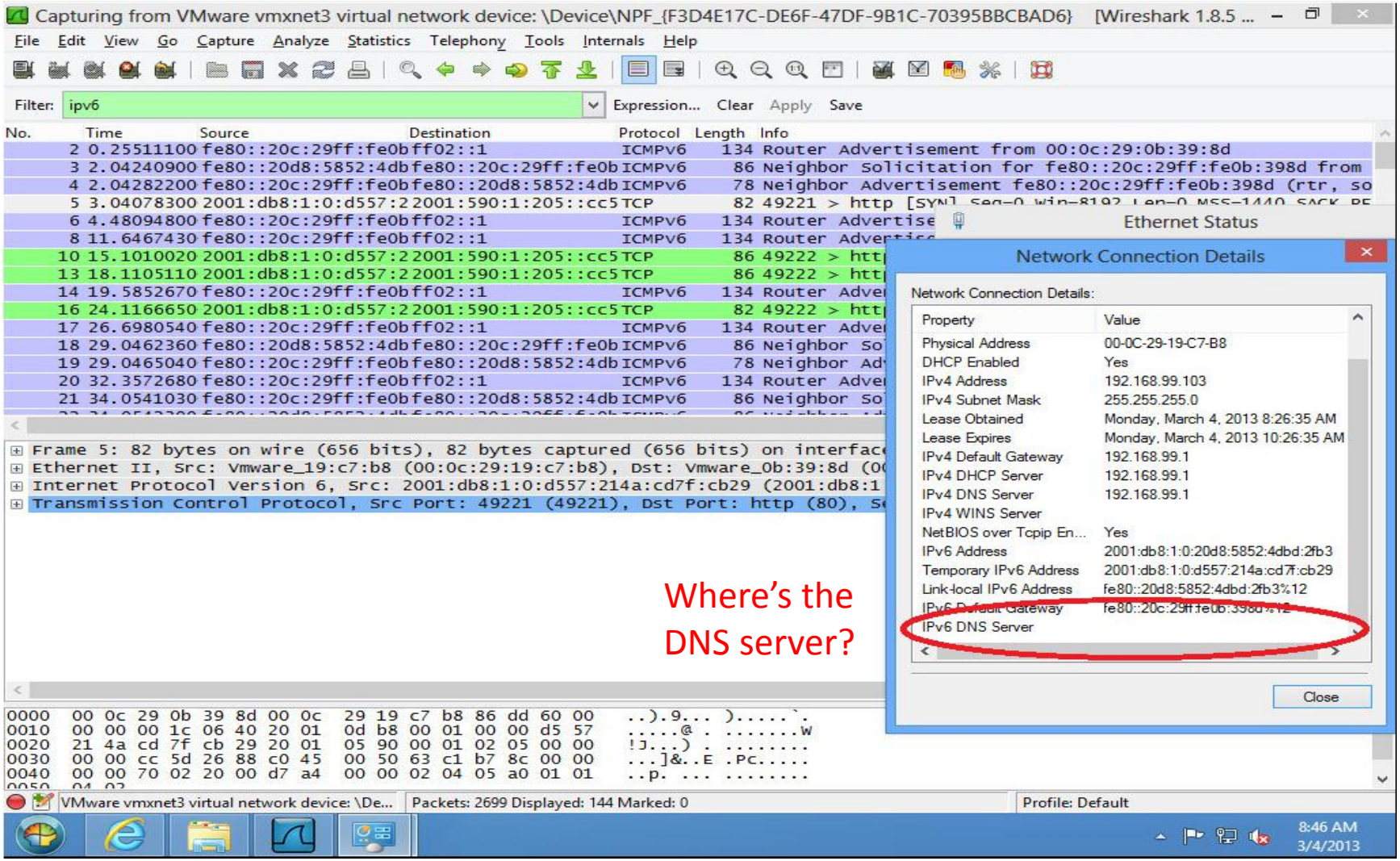
SLAAC Attack!



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

NEOHAPSIS

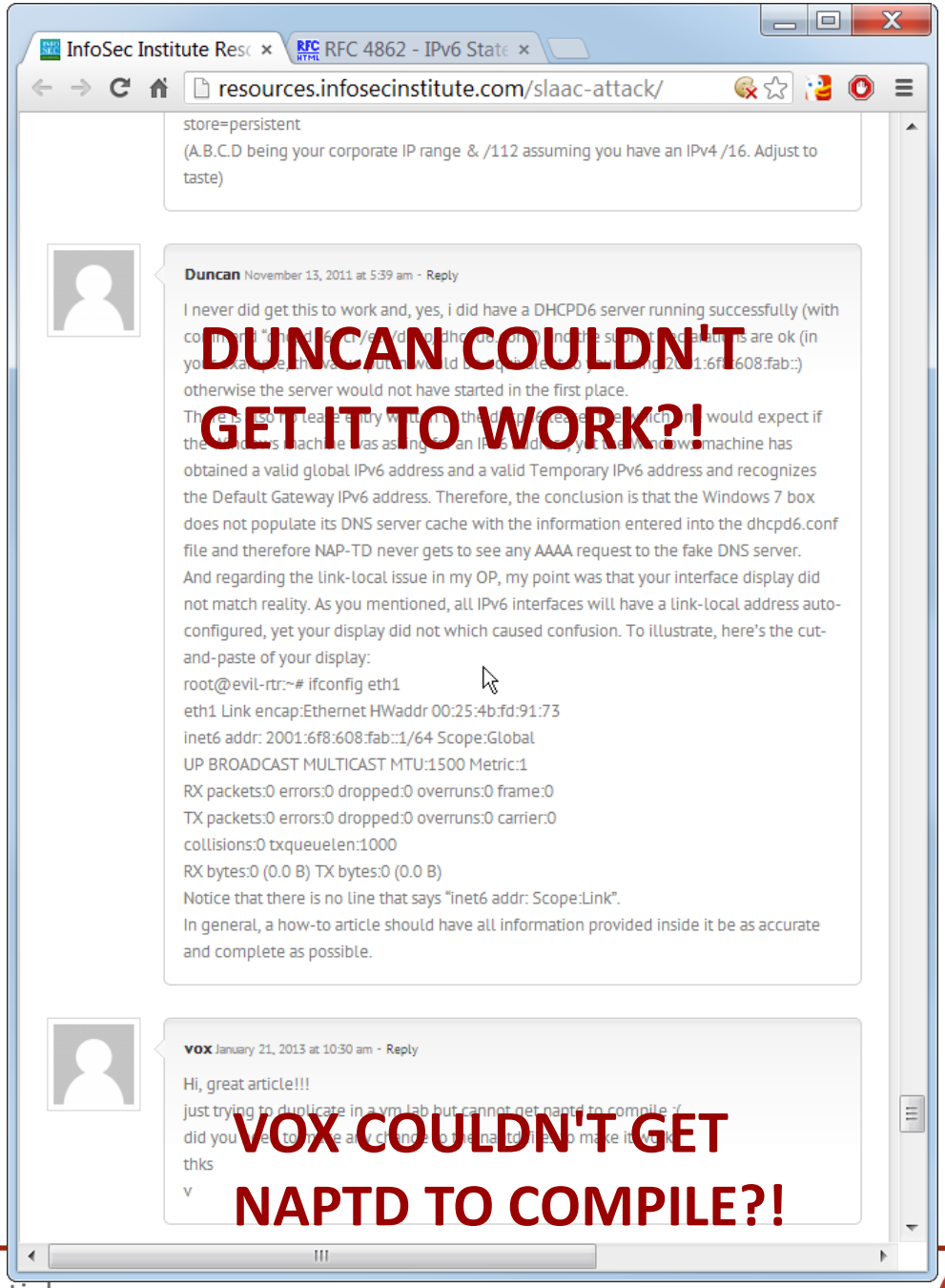
SLAAC Attack Win8 Fail :(



NEOHAPSIS

SLAAC Attack in 2013...the Bad

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



DUNCAN COULDN'T GET IT TO WORK?!

VOX COULDN'T GET NAPTD TO COMPILE?!

NEOHAPSIS

SLAAC Attack in 2013

WE NEED

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

NEOHAPSIS

Thank You

www.neohapsis.com
labs.neohapsis.com