DUAL STACK SECURITY

A simple proof of concept on IPv4/IPv6 stacks
Some thoughts about current dual stack setups

Eduardo Coelho
http://coelho.pro.br

SCENARIO

- virtual simulated environment
- 2 linux vms, 1 windows8 vm
- vmware built-in IPv4 DHCP server, host-only network
- simulated rogue IPv6 ra/dhcp/dns with regular linux software

DEMO

DUAL STACK MAY NOT BE SMOOTH FROM A SECURITY STAND POINT

IPV6 ADDRESSING

- global unicast
- link local
- unique local
- others: anycast, multicast, reserved and special

AUTOCONF IS A BIG THING

- lets try to understand how it works:
  - stateless autoconf
  - router advertisement and prefix distribution
  - IPv6 routing

DNS SETTINGS DELIVERY

- llmnr
- stateless dhcp6
- dns-ra (problem:windows non-compliance to rfc6106)
- remember naming is now more important than with ipv4, due to human difficulty manually handling ipv6 addresses

AUTOCONF CONCERNS

- rogue routers
- rogue dhcp servers
- sniffing
- spoofing (man in the middle attacks)

CONCLUSIONS

- we have provided a simple proof of concept for a rogue ra/dns server on a dual-stack ipv4/ipv6 environment

- ipv6 technologies should be very well understood, specially on dual-stack setups, which is how most of networks are set

- some of the security issues are not ipv6 specific, but have a greater impact due to current lack of precautions

- most issues are due to stack implementation or by design, which makes it difficult to mitigate

REFERENCES

Unique Local Address
http://en.wikipedia.org/wiki/Unique_local_address

Unique Local Unicast Addresses
http://tools.ietf.org/html/rfc4193

Deprecating Site Local Addresses
http://tools.ietf.org/rfc/rfc3879.txt

IPv6 Support in Home Routers
http://msdn.microsoft.com/en-us/library/windows/hardware/gg463251.aspx

Prefix delegation
http://en.wikipedia.org/wiki/Prefix_delegation

Requirements for IPv6 Prefix Delegation
http://tools.ietf.org/html/rfc3769

IPv6 Prefix Options for DHCP version 6
http://www.ietf.org/rfc/rfc3633.txt

IP Version 6 Addressing Architecture
http://tools.ietf.org/html/rfc4291

Internet powers flip the IPv6 switch (FAQ)
http://news.cnet.com/8301-1001_3-57445316-92/internet-powers-flip-the-ipv6-switch-faq/

IPv6-capable devices: Make sure they are ready
http://www.techrepublic.com/blog/networking/ipv6-capable-devices-make-sure-they-are-ready/2522

IPv6 Ready Logo Program
https://www.ipv6ready.org

IPv6: When do you really need to switch?
http://www.zdnet.com/blog/networking/ipv6-when-do-you-really-need-to-switch/2444

Portal IPv6 NIC.br
http://ipv6.br

IPv6
http://en.wikipedia.org/wiki/IPv6

IPv6 transition mechanisms
http://en.wikipedia.org/wiki/IPv6_transition_mechanisms

Comparison of IPv6 support in operating systems
http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems

Internet Protocol Version 6 Address Space
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Router Advertisement (radvd) configuration
http://wiki.openwrt.org/doc/uci/radvd

Does Win7 or W2K8 server support RFC 6106?
http://social.technet.microsoft.com/Forums/en-US/ipv6/thread/5757980a-5983-4efc-a5f3-27687b90fe41/

Delivering DNS via IPv6 Router
http://www.itdojo.com/2011/05/02/delivering-dns-via-ipv6-router-advertisements/