

Exploiting IPv6

- The Internet is running out of addresses
 - Specifically ASIA
- Government mandate for IPv6 support
 - June 30, 2008. IPv6 on backbones
- Networking vendors supporting IPv6
 - Slower, buggier, incomplete (IPSEC).
- Consumer operating systems
 - Default: Vista, OS X, Ubuntu
 - Supported: XP, Linux, BSD

- Nobody actually cares*
 - Very little market demand
 - A “checkbox” feature
 - Few real endpoints

* Except Asia, US Government, Internet2

- IPv6 is already here, sorta.
 - IPv6 is deployed at the backbone level
 - IPv6 is deployed at the consumer level
 - ISPs are the only missing link
 - Tunnel services bridge this

Hacking IPv6

- Finding “public” IPv6 systems
 - Network sweeping is infeasible (64 bit subnets)
 - Discovery depends on DNS, known addresses
 - Look for AAAA records for known sites
 - Otherwise you are SOL...

Hacking IPv6

- Port scanning “public” IPv6 systems
 - No raw IPv6 port scanners (Nmap works OK)
 - Nmap depends on native IPv6 stack
 - UDP probes... just Nmap.
 - Other IPv6 tools
 - ping6 (ping, just plain ping)
 - netcat6 (fork of the old netcat tool)
 - ncat (nmap's netcat replacement)
 - socat (supports ipv6 and tons more)

Hacking IPv6

- Exploiting “public” IPv6 systems
 - Exploits can be ported or relayed
 - xinetd, socat, ncat, proxies, etc
 - Shellcode just kinda sucks
 - Bind, Reverse code needs to be ported
 - Reverse needs to support link-local

Hacking IPv6

- Firewalls and IPv6
 - Some firewall products work
 - Windows Firewall
 - Norton Internet Security 2009 Beta
 - Some firewall products don't
 - ZoneAlarm
 - IPTables (without specific IPv6 rules)
 - IPS products a mixed bag
 - Support for some sigs, some transports
 - 6in4, Torpedo, tunnel services, etc

Practicality

- What would you pen-test?
 - Few orgs run IPv6 servers
 - Host discovery is hard
- Firewalls and public servers
 - Do they firewall IPv6 correctly?
 - Look for AAAA DNS records
- OK, now what...
 - This might be useful someday
 - But who cares now?

Local IPv6 Networks

- IPv6 and Modern Operating Systems
 - Vista, Mac OS X, Ubuntu, Solaris
 - Link-local and Site-local addresses
 - Linux distros
 - `# modprobe "ipv6"`
 - Windows XP
 - `C:\> ipv6 install`
- Tons of networking gear
 - Cisco switches, routers
 - NAS storage devices

Link-Local and Auto-Configuration

- IPv6 interfaces have default addresses
 - **FE80:0000:0000:0000:XXXX:XXFF:FEXX:XXXX**
 - **2000:0000:0000:0000:XXXX:XXFF:FEXX:XXXX**
- Link-local prefix is FE80::EUI-64
- Site-local prefix is 2000::EUI-64
 - EUI64: Ethernet MAC address + 2 bytes
- Magic broadcast addresses
 - FF02::1 is link-local all nodes (FF02::2 is routers)
 - FF05::1 is site-local all nodes

IPv6 Local Discovery

- ARP is replaced by Neighbor Discovery
 - ICMPv6 with special broadcast addresses
 - # `ping6 -I eth0 FF02::1`
- THC Attack Toolkit's "alive6"
 - Send 3 probes to detect local IPv6
 - # `alive6 eth0`
- Work network, we don't use IPv6...
 - Over 30 active IPv6 hosts
 - One active IPv6 router

IPv6 Broadcast + UDP

- IPv4 UDP Services
 - Most listen on 0.0.0.0::PORT
 - Handle all unicast requests
- IPv6 UDP Services
 - Most listen on :::PORT (:::0 or 0::0)
 - Handle all unicast requests
 - Handle local broadcast requests!
- Using “broadcast” BIND DNS
 - \$ `dig www.domain.com @FF02::1`

Local IPv6 Exploitation

- Cut through crappy firewalls
 - Portscan with Nmap and Metasploit (aux)
 - Exploit systems with standard modules
- Confuse your system administrators
 - Exploit attempt from ***what*** source address?
- Probe all IPv6 UDP services at once
 - Send packets to FF02::1
 - Easy reconnaissance

More to come...

- Abusing IPv4 compatibility addresses
 - ::A.B.C.D, ::FFFF:A.B.C.D
- IPv6 and web browsers
 - `http://[2000::XXXX:XXFF:FEXX:XXXX]/`
- MITM fun with THC-IPv6