IPv6 Security Training
April 13, 2011
• What is IPv6 and why do we need it?
• Comparison of IPv4 and IPv6
• Where is K-State situated with IPv6 deployment
• Security concerns and recommendations
• Questions....
What is IPv6?

- The next generation Internet Protocol
- Adds significant IP address space to address IPv4 address depletion (128 bits as opposed to 32 bits in IPv4)
- Was designed with security in mind
  - All implementations required to support authentication and encryption headers (using IPSec)
- A single interface may be assigned multiple IPv6 addresses (unicast, anycast, or multicast) – No broadcast
IPv4 limitations/IPv6 – Why do we need it?

- Attempts to prolong IPv4 depletion
  - NAT/CIDR/DHCP

- IPv4 was designed with interoperability in mind, not security

- IPv6-only sites

- Growth within the campus environment
  - Growth of wireless and portable, network-enabled devices
K-State’s IPv6 status

- Have IPv6 allocation: 2001:49D0:0040:0000:0000:0000:0000:0000/42
  - With 30,000 staff/students, that will allow for $2.579 \times 10^{21}$ IP addresses / person

- Core, Data Center, and some firewalls support IPv6 today. Others will require software updates

- Border routers, several aggregation switches support IPv6, but in software rather than hardware

- Procera support for IPv6 in Q1, 2011

- Investigating IPv6 deployment strategy – No IPv6 routing at this time
K-State’s IPv6 status

- Assessing hardware support throughout the enterprise to identify all needed hardware replacements and/or software upgrades
- Dual-stack deployment will be required for some time
- Need for deployment in test environment to get support infrastructure in place
- When purchasing new technologies, require and verify IPv6 support
IPv6 security implications

- Currently, many tools have limited or evolving support for IPv6
- IPv6 traffic is not being “watched”, so communication within a vlan typically occurs unchecked.
- IPv6 enabled by default on Windows 7, OS X, Linux, etc.
  - Recommended action is to disable IPv6 until deployed in the enterprise
  - Default rules, for instance, on OS X allow everything
    - 33300 deny log ipv6-icmp from any to any in icmptype 128
    - 65535 allow ipv6 from any to any
- Managing security on two fronts – IPv4 and IPv6
IPv6 security implications

- Scanning for vulnerable devices, or devices in general is more difficult
- ICMPv6 Neighbor discovery and neighbor solicitation for local segments
- ICMPv6 filtering to limit messages passed between the site and Internet
  - Filtering network discovery, for instance
Questions?