IPv6 Implications for Network Scanning
draft-ietf-v6ops-scanning-implications-00

Status of this Memo

Copyright Notice

Abstract

The 128 bits of IPv6 address space is considerably bigger than the 32 bits of address space in IPv4. In particular, the IPv6 subnets to which hosts attach will by default have 64 bits of host address space. As a result, traditional methods of remote TCP or UDP port scanning to discover open or running services on a host will potentially become far less computationally feasible, due to the larger search space in the subnet. This document discusses that property of IPv6 subnets, and describes related issues for site administrators of IPv6 networks to consider, which may be of

importance when planning site address allocation and management strategies. While traditional port scanning probes (whether by individuals or automated via network worms) may become less common, administrators should be aware of other methods attackers may use to discover IPv6 addresses on a target subnet, and take appropriate measures to preempt these.

Table of Contents

1. Introduction

One of the key differences between IPv4 and IPv6 is the much larger address space for IPv6, which also goes hand-in-hand with much larger subnet sizes. This change has a significant impact on the feasibility of TCP and UDP based port scanning probing, which is something that most of today's IPv4 sites are subjected to routinely around the clock.

The 128 bits of IPv6 [1] address space is considerably bigger than the 32 bits of address space in IPv4. In particular, the IPv6 subnets to which hosts attach will by default have 64 bits of host address space [3]. As a result, traditional methods of remote TCP or UDP port scanning to discover open or running services on a host will potentially become far less computationally feasible, due to the larger search space in the subnet. This document discusses that property of IPv6 subnets, and describes related issues for site administrators of IPv6 networks to consider, which may be of importance when planning site address allocation and management strategies.

This document complements the transition-centric discussion of the issues that can be found in Appendix A of the IPv6 Transition/ Co-existence Security Considerations [5] text, which takes a broad view of security issues for transitioning networks.

Port scanning is quite a prevalent tactic by would-be attackers. There are two general classes of such scanning. In one case, the probes are from an attacker outside a site boundary who is trying to find weaknesses on any system in that network which they then may subsequently compromise. The author observes that a typical university firewall may today generate many tens of megabytes of log files on a daily basis purely from port scanning activity.

The other case is scanning by worms that spread through (site) networks, looking for further hosts to compromise. Many worms, like Slammer, rely on such address scanning methods to propagate, whether they pick subnets numerically (and thus probably topologically) close to the current victim, or subnets in random remote networks.

It must be remembered that the defence of a network must not rely on the obscurity of the hosts on that network. Such a feature or property is only one measure in a set of measures that may be applied. However, with a growth in usage of IPv6 devices in open networks likely, and security becoming more likely an issue for the end devices, such obfuscation can be useful where its use is of little or no cost to the administrator. That said, the administrator must be aware of the context. What new methods may attackers use to

glean IPv6 address information, and how can these be mitigated against?

2. Target Address Space for Port Scanning

There are significantly different considerations for the feasibility of plain, brute force IPv4 and IPv6 address scanning.

2.1. IPv4

A typical IPv4 subnet may have 8 bits reserved for host addressing. In such a case, a remote attacker need only probe at most 256 addresses to determine if a particular open service is running on a host in that subnet. Even at only one probe per second, such a scan would take under 5 minutes to complete.

2.2. IPv6

A typical IPv6 subnet will have 64 bits reserved for host addressing. In such a case, a remote attacker needs to probe 2^64 addresses to determine if a particular open service is running on a host in that subnet. At a very conservative one probe per second, such a scan may take some 5 billion years to complete. A more rapid probe will still be limited to (effectively) infinite time for the whole address space, unless the attacker can deduce ways to reduce the address space to scan against within the target subnet.

2.3. Reducing the IPv6 Search Space

The IPv6 host address space through which an attacker may search can be reduced in at least two ways.

First, the attacker may rely on the administrator conveniently numbering their hosts from [prefix]::1 upward. This makes scanning trivial, and thus should be avoided unless the host's address is readily obtainable from other sources (for example it is the site's primary DNS or email MX server).

Second, in the case of statelessly autoconfiguring [1] hosts, the host part of the address will take a well-known format that includes the Ethernet vendor prefix and the "fffe" stuffing. For such hosts, if the Ethernet vendor is known, the search space may be reduced to 24 bits (with a one probe per second scan then taking 194 days). Even where the exact vendor is not known, using a set of common vendor prefixes can reduce the search space. In addition, many nodes in a site network may be procured in batches, and thus have sequential or near sequential MAC addresses; if one node's

autoconfigured address is known, scanning around that address may yield results for the attacker. Any form of sequential host addressing should be avoided if possible.

2.4. Dual-stack Networks

Full advantage of the increased IPv6 address space in terms of resilience to port scanning may not be gained until IPv6-only networks and devices become more commonplace, given that most IPv6 hosts are currently dual stack, also with (more readily scannable) IPv4 connectivity. However, many applications or services (e.g. new peer-to-peer applications) on the (dual stack) hosts may emerge that are only accessible over IPv6, and that thus can only be discovered by IPv6 address scanning.

2.5. Defensive Scanning

The problem faced by the attacker for an IPv6 network is also faced by a site administrator looking for vulnerabilities in their own network's systems. The administrator should have the advantage of being on-link for scanning purposes though.

3. Alternatives for Attackers

If IPv6 port-scanning becomes relatively infeasible, attackers will need to find new methods to identify IPv6 addresses for subsequent port scanning. In this section, we discuss some possible paths attackers may take. In these cases, the attacker will attempt to identify specific IPv6 addresses for subsequent targeted probes.

3.1. On-link Methods

If the attacker is on link, then traffic on the link, be it Neighbour Discovery or application based traffic, can invariably be observed, and target addresses learnt. In this document we are assuming the attacker is off link, but traffic to or from other nodes (in particular server systems) is likely to show up if an attacker can gain a presence on any one subnet in a site's network.

IPv6-enabled hosts on local subnets may be discovered through probing the "all hosts" link local multicast address. Likewise any routers on link may be found via the "all routers" link local multicast address.

Where a host has already been compromised, its Neighbour Discovery cache is also likely to include information about active nodes on link, just as an ARP cache would do for IPv4.

3.2. Multicast or Other Service Discovery

A site may also have site or organisational scope multicast configured, in which case application traffic, or service discovery, may be exposed site wide. An attacker may choose to use any other service discovery methods supported by the site.

3.3. Log File Analysis

IPv6 addresses may be harvested from recorded logs such as web site logs. Anywhere else where IPv6 addresses are explicitly recorded may prove a useful channel for an attacker, e.g. by inspection of the (many) Received from: or other header lines in archived email or Usenet news messages.

3.4. DNS Advertised Hosts

Any servers that are DNS listed, e.g. MX mail relays, or web servers, will remain open to probing from the very fact that their IPv6 addresses will be published in the DNS. Where a site uses sequential host numbering, publishing just one address may lead to a threat upon the other hosts.

3.5. DNS Zone Transfers

In the IPv6 world a DNS zone transfer is much more likely to narrow the number of hosts an attacker needs to target. This implies restricting zone transfers is (more) important for IPv6, even if it is already good practice to restrict them in the IPv4 world.

3.6. Application Participation

More recent peer-to-peer applications often include some centralised server which coordinates the transfer of data between peers. The BitTorrent application builds swarms of nodes that exchange chunks of files, with a tracker passing information about peers with available chunks of data between the peers. Such applications offer an attacker a source of peer IP addresses to probe.

3.7. Transition Methods

Specific knowledge of the target network may be gleaned if that attacker knows it is using 6to4, ISATAP, Teredo, or other techniques that derive low-order bits from IPv4 addresses (though in this case, unless they are using IPv4 NAT, the IPv4 addresses may be probed anyway). For example, the current Microsoft 6to4 implementation uses the address 2002:V4ADDR::V4ADDR while older Linux and FreeBSD implementations default to 2002:V4ADDR::1. This leads to specific

knowledge of specific hosts in the network. Given one host in the network is observed as using a given transition technique, it is likely that there are more.

4. Site Administrator Tools

There are some tools that site administrators can apply to make the task for IPv6 port scanning attackers harder. These methods arise from the considerations in the previous section.

The author notes that at his current (university) site, there is no evidence of general port scanning running across subnets. However, there is port-scanning over IPv6 connections to systems whose IPv6 addresses are advertised (DNS servers, MX relays, web servers, etc), which are presumably looking for other open ports on these hosts to probe.

4.1. IPv6 Privacy Addresses

By using the IPv6 Privacy Extensions [2] hosts in a network may only be able to connect to external systems using their current (temporary) privacy address. While an attacker may be able to port scan that address if they do so quickly upon observing the address, the threat or risk is reduced due to the time constrained value of the address. One implementation of RFC3041 already deployed has privacy addresses active for one day, but such addresses reachable for seven days.

Note that an RFC3041 host will usually also have a separate static global IPv6 address by which it can also be reached, and that may be DNS-advertised if an externally reachable service is running on it.

The implication is that while Privacy Addresses can mitigate the long-term value of harvested addresses, an attacker creating an IPv6 application server to which clients connect will still be able to probe the clients by their Privacy Address as and when they visit that server. In the general context of hiding the addresses exposed from a site, an administrator may choose to use IPv6 Privacy Addresses. The duration for which these are valid will impact on the usefulness of such observed addresses to an external attacker.

It may be worth exploring whether firewalls can be adapted to allow the option to block traffic initiated to a known IPv6 Privacy Address from outside a network boundary. While some applications may genuinely require such capability, it may be useful to be able to differentiate in some circumstances.

4.2. DHCP Service Configuration Options

The administrator should configure DHCPv6 so that the first addresses allocated from the pool begins much higher in the address space than [prefix]::1. DHCPv6 also includes an option to use Privacy Extension [2] addresses, i.e. temporary addresses, as described in Section 12 of the DHCPv6 [4] specification. It is desirable that allocated addresses are not sequential.

4.3. Rolling Server Addresses

Given the huge address space in an IPv6 subnet/link, and the support for IPv6 multiaddressing, whereby a node or interface may have multiple IPv6 valid addresses of which one is preferred for sending, it may be possible to periodically change the advertised addresses that certain long standing services use (where 'short' exchanges to those services are used).

For example, an MX server could be assigned a new primary address on a weekly basis, and old addresses expired monthly. Where MX server IP addresses are detected and cached by spammers, such a defence may prove useful to reduce spam volumes, especially as such IP lists may also be passed between potential attackers for subsequent probing.

5. Conclusions

Due to the size of IPv6 subnets attackers, whether they be in the form of automated port scanning or dynamic worm propagation, will need to use new methods to determine IPv6 host addresses to target. This document discusses the considerations a site administrator should bear in mind when considering IPv6 address planning issues and configuring various service elements. It highlights relevant issues and makes some informational recommendations for administrators.

6. Security Considerations

There are no specific security considerations in this document outside of the topic of discussion itself.

7. IANA Considerations

There are no IANA considerations for this document.

8. Acknowledgements

Thanks are due to people in the 6NET project for discussion of this topic, including Pekka Savola, Christian Strauf and Martin Dunmore, as well as other contributors from the IETF v6ops mailing list, including Tony Finch, David Malone and Fred Baker.

9. Informative References

[1] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[2] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[3] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[4] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[5] Davies, E., "IPv6 Transition/Co-existence Security Considerations", draft-ietf-v6ops-security-overview-04 (work in progress), March 2006.

Author's Address

Tim Chown
University of Southampton
Southampton, Hampshire SO17 1BJ
United Kingdom

Email: tjc@ecs.soton.ac.uk

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.