Probing for Open DNS Resolvers

John Kristoff

jtk@depaul.edu

Midwest Security Workshop

Open Resolvers

- Recursive - open access to a full resolver
- Forwarder - proxy access to a full resolver
- Caching-only - recursion disabled, but cache data accessible
- Restricted - resolver, but limited access, at most authoritative data

Security Implications of Open Resolvers

- Reflection attacks through spoofing
- Small queries can solicit large answers for amplication attack
- Cache enumeration and spying enabled
- Remote cache poisoning difficulty is reduced
- Resolver and network resource theft

Selecting probe destinations

- Hosts querying our resolvers and servers
- Name servers listed in available TLD zone files
- Sources of DNS amplification and reflection attacks
- Authority and additional section RRs from answers to our queries
- Full scanning of the routable IPv4 address space
- Lists from colleagues, collaborators and other projects

Open Resolver Probing Challenges

- Checking the ra bit is an unreliable indictator
- An open resolver may not return a NXDOMAIN for a bogus TLD
- Low or TTL adherence is not guaranteed
- Identical queries to the same destination may be handled differently
- Rate limiting, filters or policy may apply to certain queries

Our Multifaceted Probing Approach

- Query for uniquely processed whoareyou and whoami names
- Query for unique, but bogus TLD
- Fingerprint with fpdns
- Query for unique name in a zone we are authoritative for and monitor
- Query for popular names and NS RRsets
- Query for unique, but bogus name in popular zones and TLDs
- Query using UDP and TCP
- Query with and without EDNS0 support enabled
- Distribute probe sources
- Send queries with and without recursion desired (rd) bit set

Recent Results

- About 60% of a set of 52,000 attackers from Feb 2006 are still open
- Answers that contain loopback answers may trigger black list handling
- About 65-75% of open resolvers are running some flavor of ISC BIND
- `http://layer9.com/~jtk/tmp/dns-fp.txt`
- `http://layer9.com/~jtk/tmp/dns-id.txt`
- Only a single email complaint after over about 4 million probes

Probe Response Data Collection and Dissemination

- Probe from a dedicated address and pcap everything to/from it
- Pcap all queries for our unique names in our zones
- Maintain database of timestamps, qname and answer data
- Schedule continual re-testing of probes
- Web interface for database lookup and feedback loop
- Automated reports grouped by source ASN seen in current route table

References and Credit

- `http://condor.depaul.edu/~jkristof/orns/`
- `http://www.net-dns.org`
- `http://www.rfc.se/fpdns/`
- `http://dns.measurement-factory.com`
- Project collaborators:
  - Duane Wessels , The Measurement Factory
  - Roy Arends, Nomimet UK
- Special thanks to DePaul University colleagues
  - Professor Ehab Al-Shaer
  - Nicola Foggi, Network Engineer
  - Bill Weaheart, Security Coordinator
- For the research-oriented position and salary, Neustar Ultra Services