Ch 3: DNS Vulnerabilities

Updated 6-19-23

Causes of Vulnerabilities

- Configuration errors
- Architecture mistakes
- Vulnerable software implementations
- Protocol weaknesses
- Failure to use the security extensions in the protocol

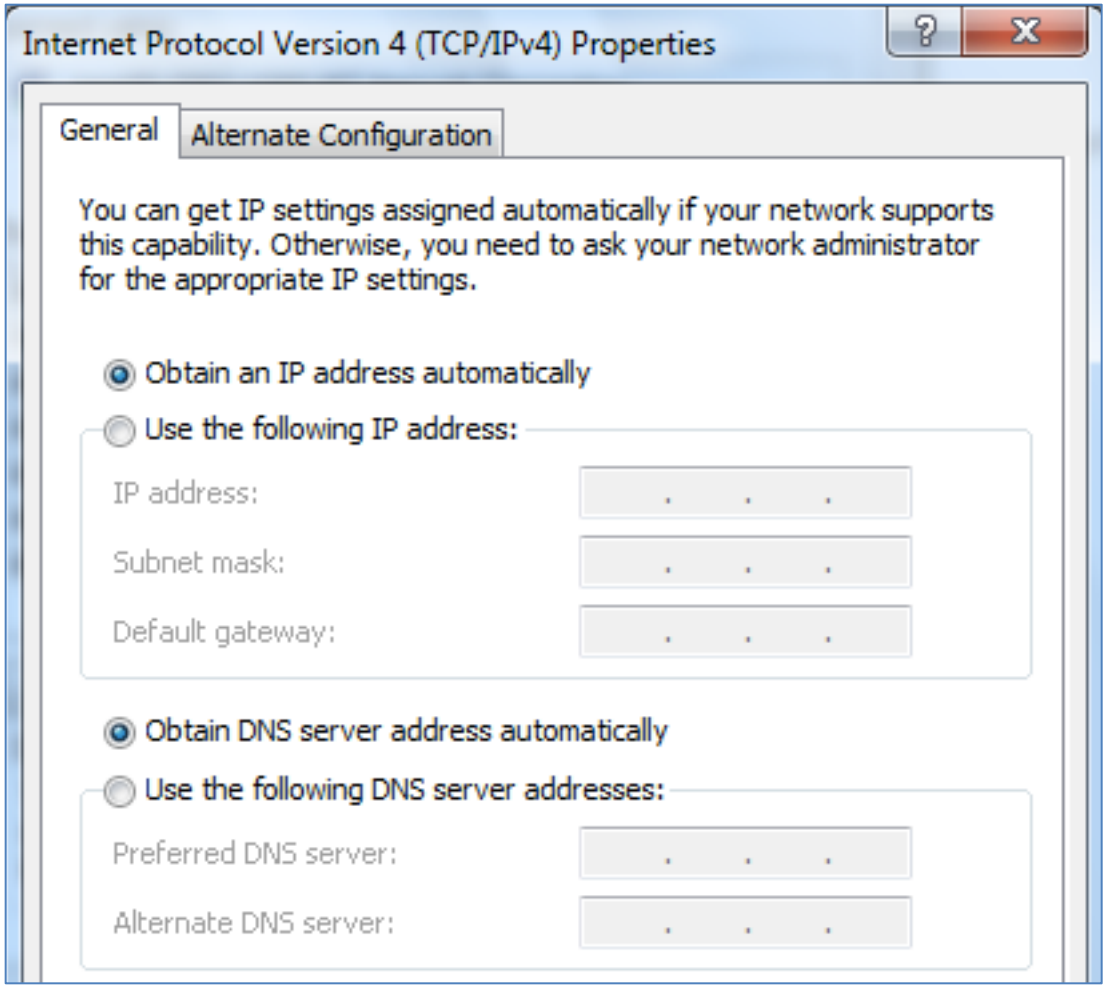
DNS Architecture Mistakes

Single Point of Failure

- The SOA could be a single server at a single site
  - If the server crashes, clients would be unable to resolve any of the domains in the zone
  - Also Internet connection outage, power failure, fire, storm, etc.
- If a single server is the recursive resolver for clients in an intranet
  - They'll all lose DNS service if it goes gown

Two Servers

- Many hosting providers do not allow delegation of DNS service to a single DNS server name
- End devices are typically provisioned with two DNS server addresses



Router or Link

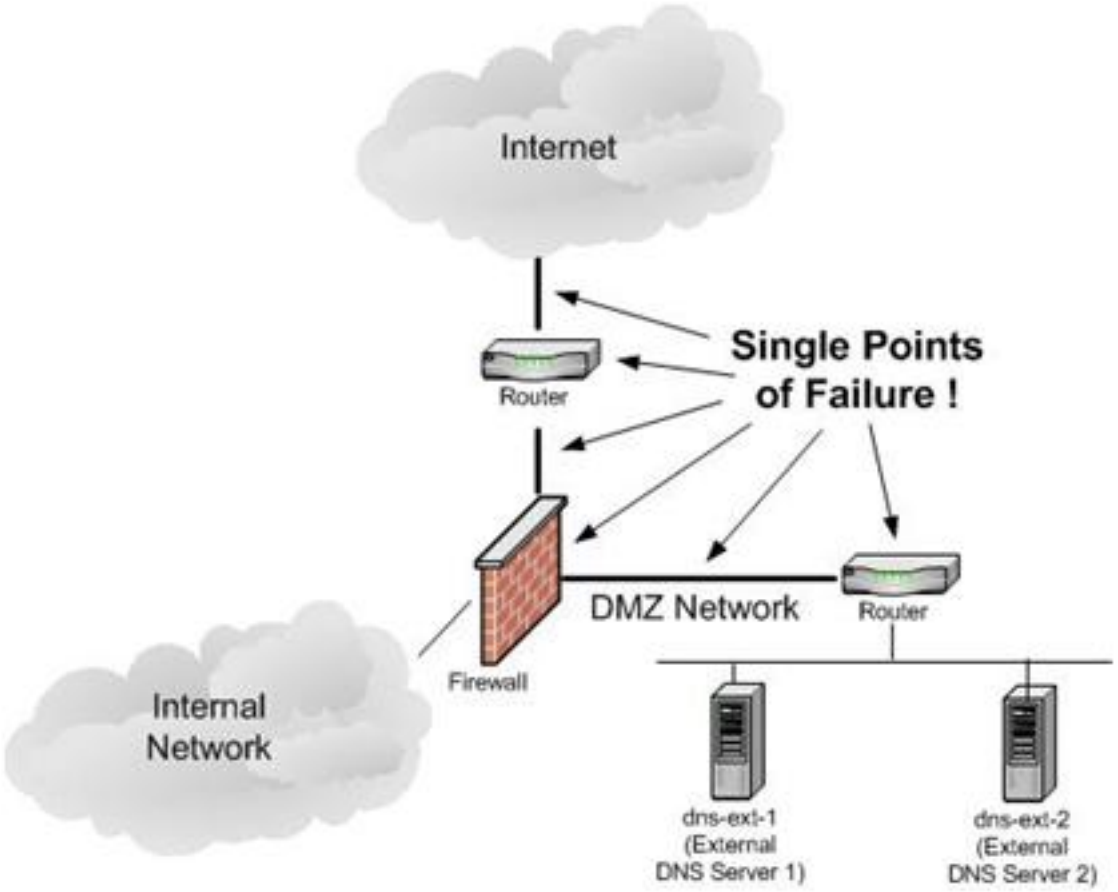


Figure 22: A DNS server architecture for DMZ servers with several router and link single points of failure. Such architecture should be avoided.

Data Center or Single Site

- If all DNS servers are at a single site or data center, a regional event could take them all down
  - Earthquake
  - Power failure
- The more critical the DNS service is, the more distributed servers should be
  - Geographically and topologically
  - Like the 13 root servers

Common Configuration Errors

Exposure of Internal Information

- Only public Web-facing servers should be in the external DNS zone files
- Your DNS server is a target of attack and may be compromised

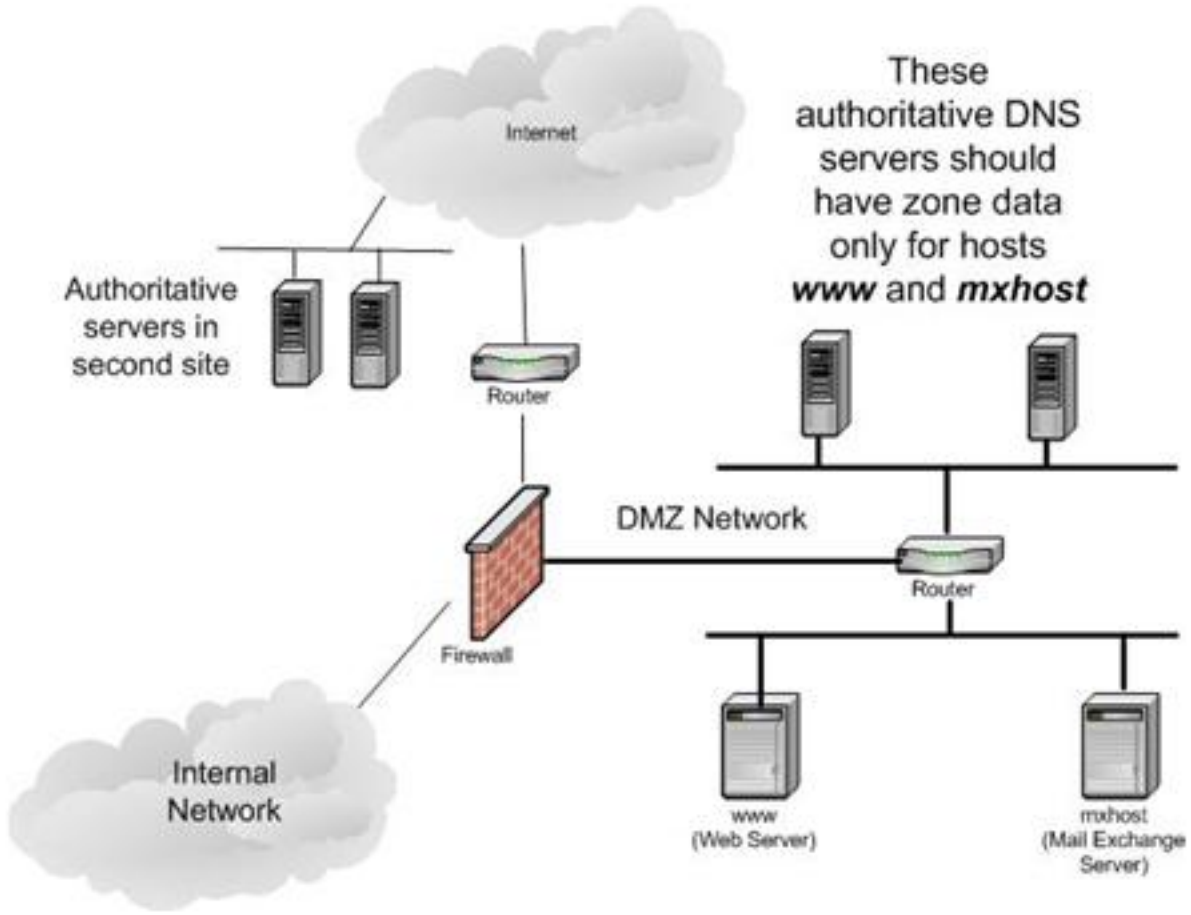


Figure 23: Authoritative servers should have zone data only for Internet-facing servers of the domain.

Leakage of Internal Queries to the Internet

- Some Windows DHCP clients leak dynamic DNS updates to the Internet
  - Link Ch 3a

Table 1: Logical steps of sending DNS updates (not all packet exchanges are shown)

	From	To	Content
1	DHCP Clt	Broadcast	DHCP Request
2	DHCP Srv	DHCP Clt	DHCP ACK: 192.168.0.2
3	DHCP Clt	LDNS	Query: SOA? hostname.ex.com
4	LDNS	DHCP Clt	Response: SOA dns.ex.com
5	DHCP Clt	dns.ex.com	Update:A hostname.ex.com
6	DHCP Clt	LDNS	Query:SOA? 2.0.168.192.in-addr.arpa
7	LDNS	DHCP Clt	Response:SOA prisoner.iana.org
8	DHCP Clt	prisoner	Update:PTR 2.0.168.192.in-addr.arpa

Win Server 2008

- Stupid queries to see if private addresses are registered in public DNS
- Expose internal information

Source	Destination	Protocol	Length	Source Port	Info
192.168.119.191	192.175.48.6	DNS	84	65105	Standard query 0x416c SOA 119.168.192.in-addr.arpa
192.168.119.191	192.175.48.6	DNS	84	65105	Standard query 0x416c SOA 119.168.192.in-addr.arpa
192.168.119.191	192.175.48.6	DNS	84	65105	Standard query 0x416c SOA 119.168.192.in-addr.arpa
192.168.119.191	192.175.48.6	DNS	84	65105	Standard query 0x416c SOA 119.168.192.in-addr.arpa
192.175.48.6	192.168.119.191	DNS	161	53	Standard query response 0x416c No such name
192.168.119.191	192.175.48.1	DNS	162	52387	Dynamic update 0x67a9 SOA 168.192.in-addr.arpa
192.168.119.191	192.175.48.1	DNS	162	52387	Dynamic update 0x67a9 SOA 168.192.in-addr.arpa
192.168.119.191	192.175.48.1	DNS	162	52387	Dynamic update 0x67a9 SOA 168.192.in-addr.arpa
192.168.119.191	192.175.48.1	DNS	162	52387	Dynamic update 0x67a9 SOA 168.192.in-addr.arpa
192.175.48.6	192.168.119.191	DNS	161	53	Standard query response 0x416c No such name
192.175.48.6	192.168.119.191	DNS	161	53	Standard query response 0x416c No such name
192.175.48.6	192.168.119.191	DNS	161	53	Standard query response 0x416c No such name
192.175.48.1	192.168.119.191	DNS	80	53	Dynamic update response 0x67a9 Refused
192.175.48.1	192.168.119.191	DNS	80	53	Dynamic update response 0x67a9 Refused

Fixing the Problem

- To prevent this, configure local DNS servers not to refer internal machines to external name servers
  - And block DNS requests directly to the Internet

Unnecessary Recursiveness

- Not all name servers need to be recursive
  - Authoritative servers don't need to
  - Recursion is complex and burdens servers
  - Added function means more potential vulnerabilities
- Recursion may be on by default
  - Thousands of open recursive resolvers on the Internet

Failure to Restrict Access

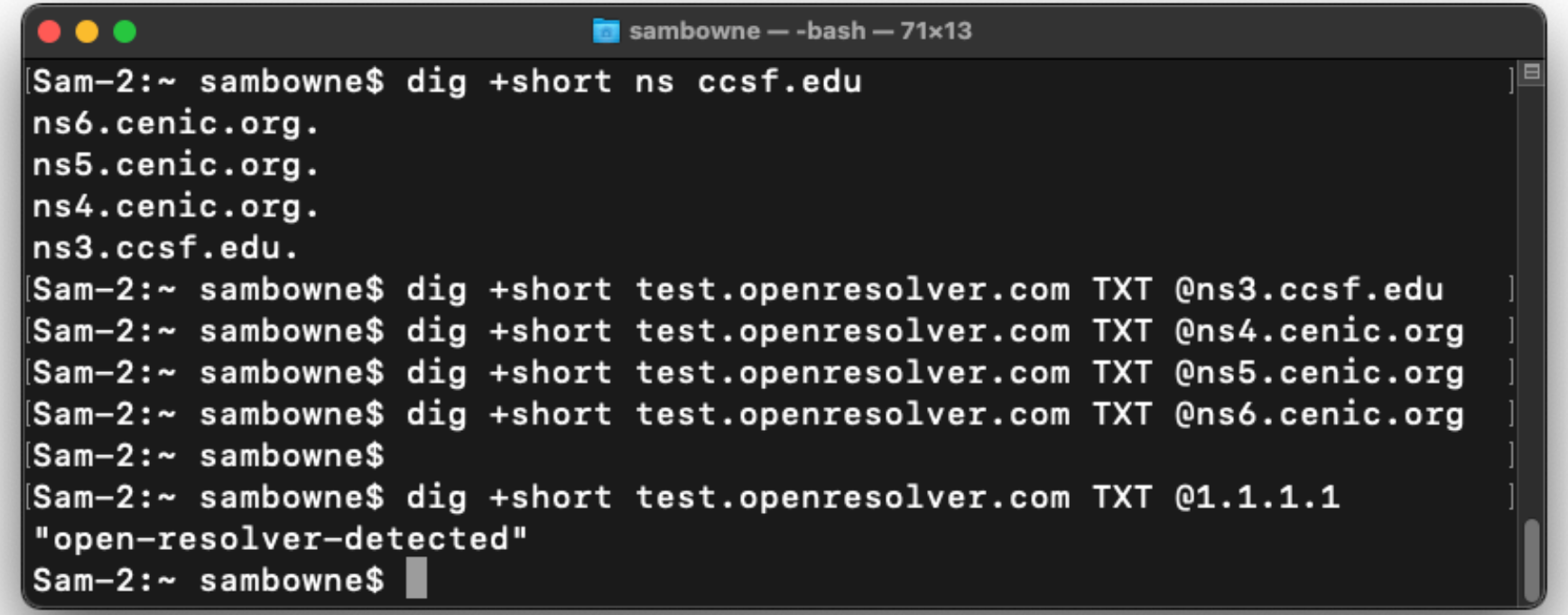
- Recursive DNS servers should only accept queries from your own clients
  - Block outside addresses with access control lists

Testing for Open Resolvers

- dig +short test.openresolver.com TXT @1.2.3.4

Testing CCSF's DNS Servers in 2023

- All are closed



Unprotected Zone Transfers

- Data transfers from a master to a slave authoritative server
  - Update the zone files on the slave
- Can be requested by any other host
- Reveals information about all hosts in the zone
  - Information disclosure vulnerability

North Korea

North Korea .kp TLD Zone Data

On Sept 19, 2016 at approximately 10:00PM (PDT), one of North Korea's top level nameservers was accidentally configured to allow global DNS zone transfers. This allows anyone who performs an `AXFR` (zone transfer) request to the country's `ns2.kptc.kp` nameserver to get a copy of the nation's top level DNS data. This was detected by the TLDR Project - an effort to attempt zone transfers against all top level domain (TLD) nameservers every three hours and keep a running Github repo with the resulting data. This data gives us a better picture of North Korea's domains and top level DNS.

- Link Ch 3i

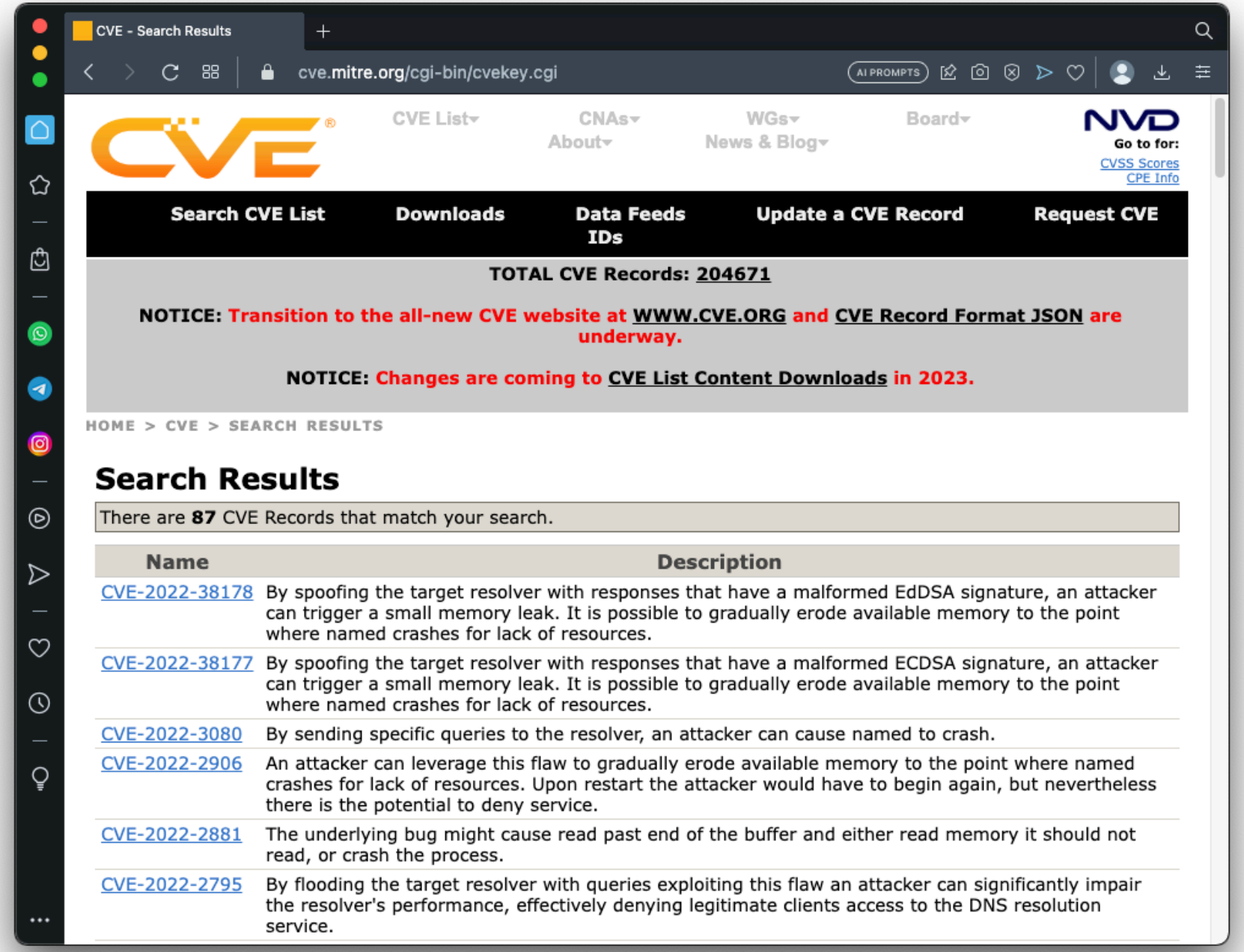

Kahoot!

Running Server in Privileged Mode

- root on Unix/Linux
- Administrator on Windows
  - Makes any security flaws more dangerous
  - Attacker who owns DNS then owns the server

Weakness in Software Implementations

- DNS servers have bugs and vulnerabilities
  - Buffer overflows
  - Other errors
- Search CVE List for "ISC Bind"
- https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=isc+bind


CVE - Search Results
cve.mitre.org/cgi-bin/cvekey.cgi
AI PROMPTS
CVE List
CNAs
About
WGs
News & Blog
Board
NVD
Go to for:
CVSS Scores
CPE Info
Search CVE List
Downloads
Data Feeds
IDs
Update a CVE Record
Request CVE
TOTAL CVE Records: 204671
NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.
NOTICE: Changes are coming to CVE List Content Downloads in 2023.
HOME > CVE > SEARCH RESULTS
Search Results
There are 87 CVE Records that match your search.
Name
Description
CVE-2022-38178
By spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources.
CVE-2022-38177
By spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources.
CVE-2022-3080
By sending specific queries to the resolver, an attacker can cause named to crash.
CVE-2022-2906
An attacker can leverage this flaw to gradually erode available memory to the point where named crashes for lack of resources. Upon restart the attacker would have to begin again, but nevertheless there is the potential to deny service.
CVE-2022-2881
The underlying bug might cause read past end of the buffer and either read memory it should not read, or crash the process.
CVE-2022-2795
By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service.

Severe 2008 Bind Vulnerability

CVE-2008-0122

VU#203611

Summary: Off-by-one error in the inet_network function in libbind in ISC BIND 9.4.2 and earlier, as used in libc in FreeBSD 6.2 through 7.0-PRERELEASE, allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted input that triggers memory corruption.

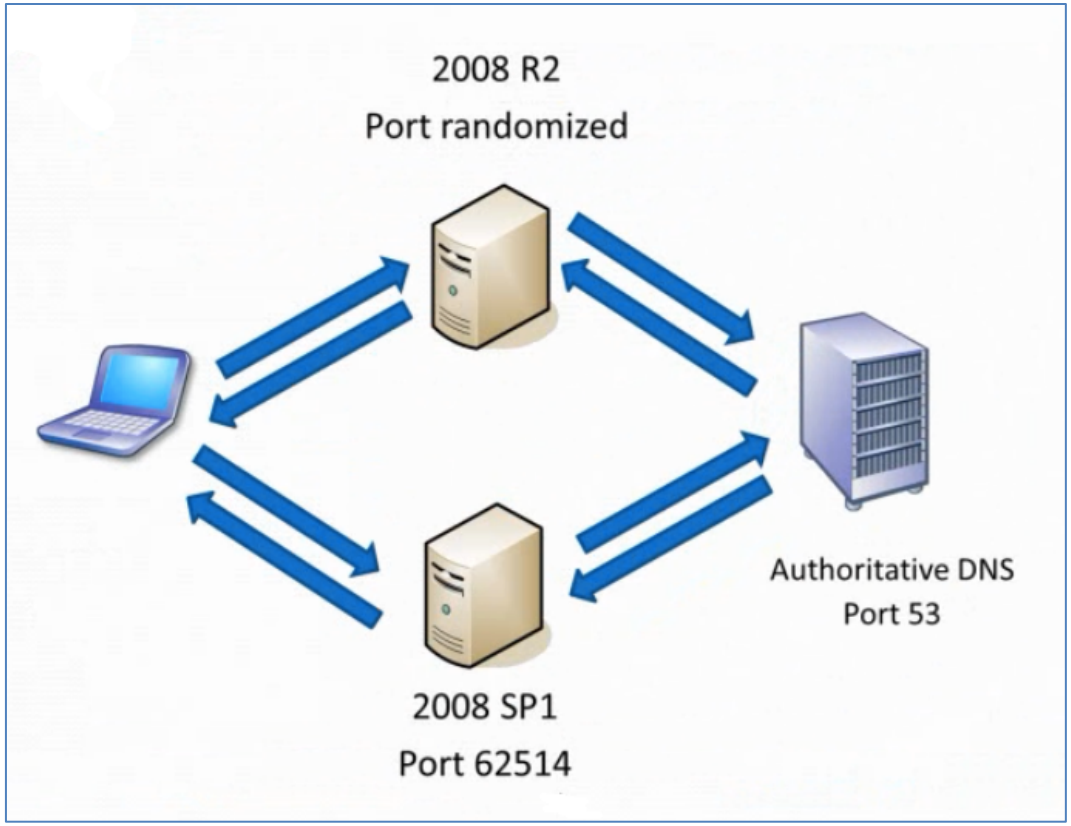
Published: 01/16/2008

CVSS Severity: 10.0 (HIGH)

- Attack used an IP address like
  - 1.2.3.4.xxxxxxxx-exploit-code-here-xxxx
- Another list of DNS vulns at link Ch 3d

Source Port Randomization

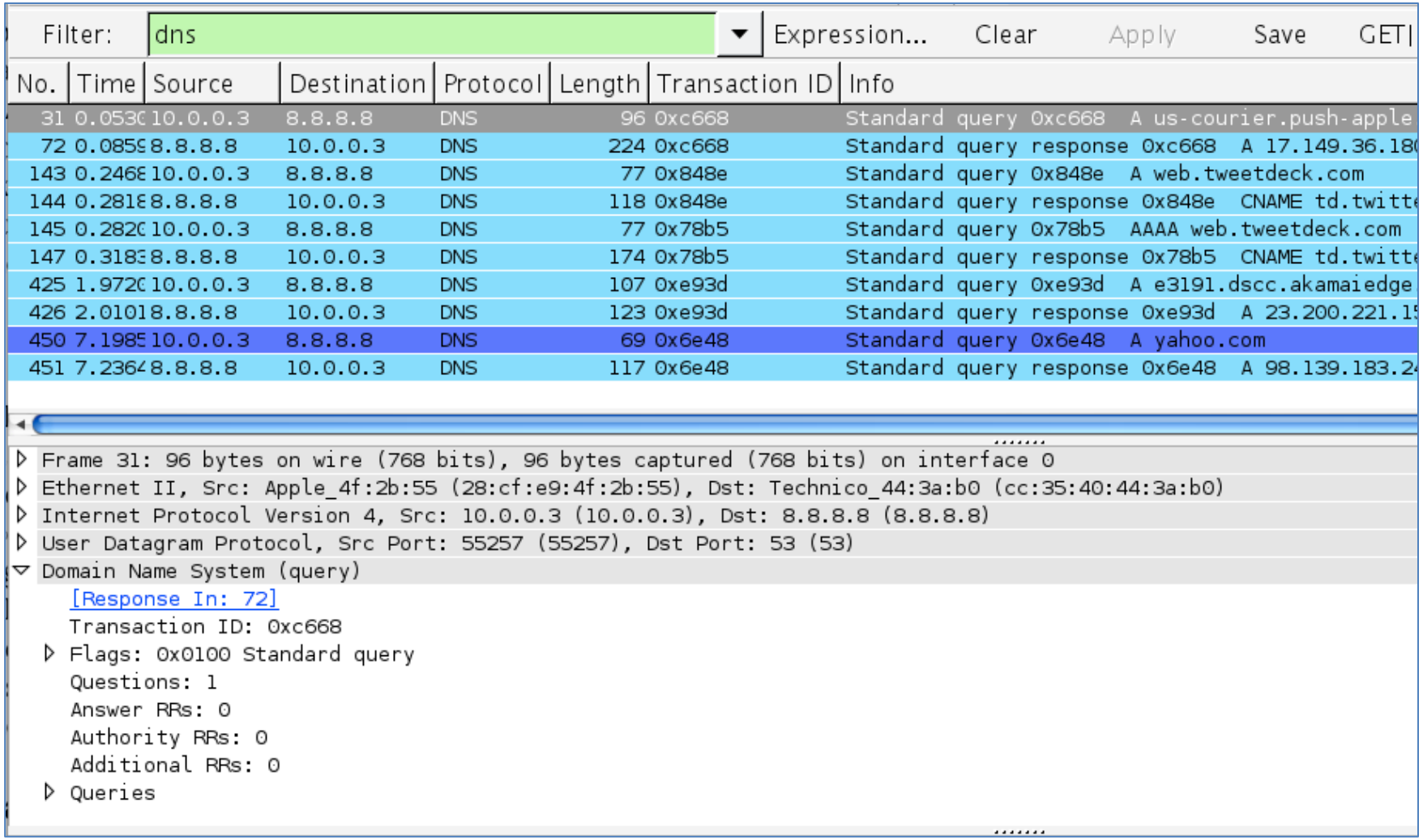
- Good video
- Link Ch 3e



Randomness of Transaction ID

- Each DNS query and response has a TXID field
  - 16 bits long (65,536 possible values)
  - Should be random
- Bind 8 & 9 used predictable transaction IDs
  - So only ten guesses were needed to spoof the reply

Randomness of Transaction ID



Tricking a Target into Using Your DNS Server

- Run a domain *evil.com* with a SOA you control *ns1.evil.com*
  - Send the target an email with a link to *server.evil.com* and hope someone clicks it
  - Send email from *joe@evil.com* to target email address
    - The server will automatically perform a reverse lookup to detect spam

Tricking a Target into Making Multiple DNS Queries

- CNAME Chaining
  - *www.evil.com* is a CNAME for *www1.evil.com*
  - *www1.evil.com* is a CNAME for *www2.evil.com*
  - *www2.evil.com* is a CNAME for *www3.evil.com*
  - etc.

Tricking a Target into Making Multiple DNS Queries

- NS Referral Chaining and NS Chains
  - *a.a.a.a.evil.com* has SOA *ns.evil.com*
  - *ns.evil.com* delegates to *ns.a.evil.com*
  - *ns.a.evil.com* delegates to *ns.a.a.evil.com*
  - etc.

Protocol Design Weaknesses

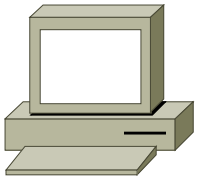
Weak Authentication

- DNS uses these elements to match a request and a response
  - Transaction ID (16 bits)
  - Question
  - Source and destination IP
  - Source and destination ports
    - But request destination port is known (53)
- Client accepts the first response that meets these criteria, and caches the result

DNS Cache Poisoning

- A false response that tricks the client puts a false entry into its cache

DNS Cache Poisoning



Attacker
1.2.3.4

Where is www.yahoo.com?

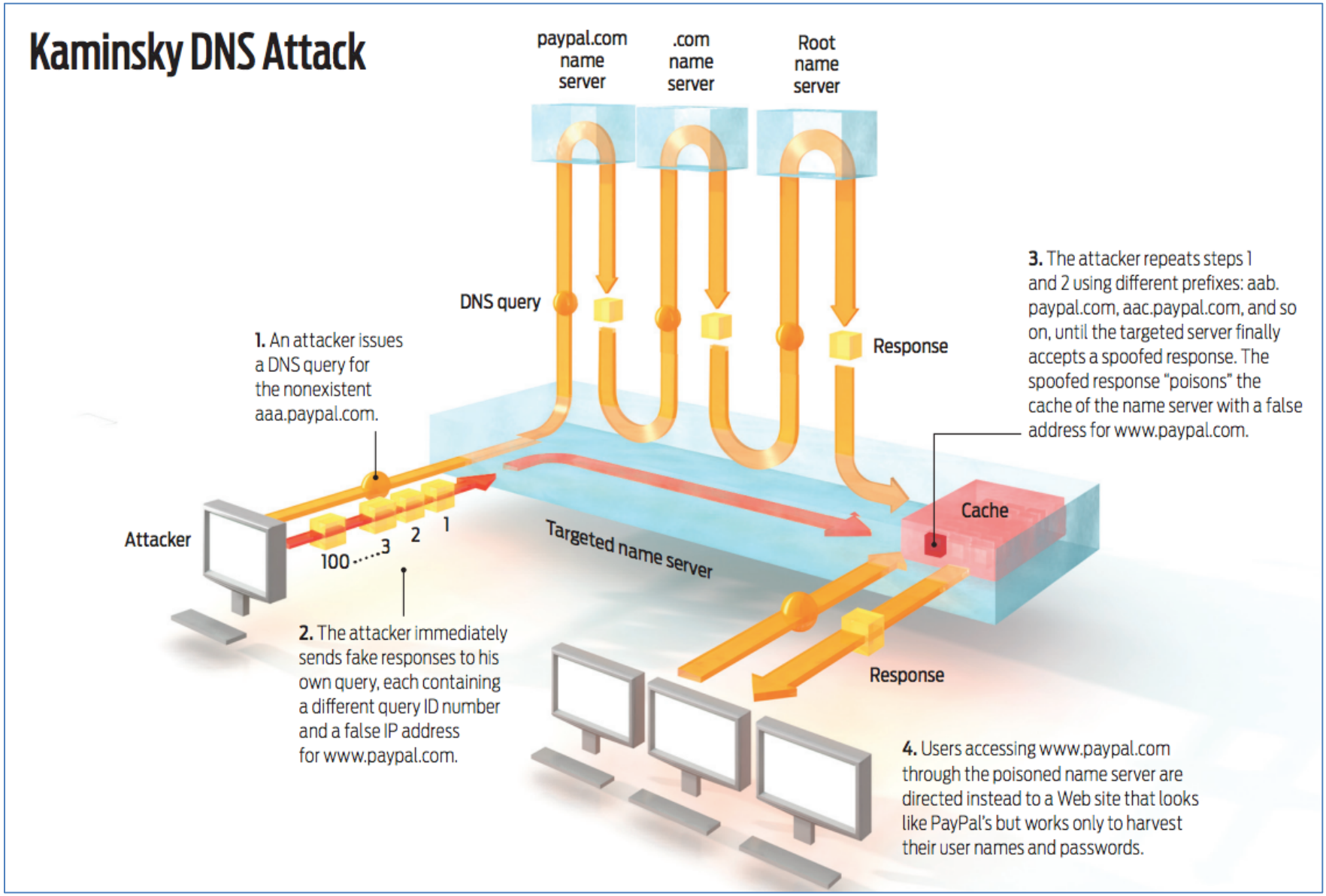
www.yahoo.com is at 1.2.3.4

DNS
Resolver

Target

Where is www.yahoo.com?

www.yahoo.com is at 1.2.3.4


Kaminsky DNS Attack
paypal.com name server
.com name server
Root name server
DNS query
Response
1. An attacker issues a DNS query for the nonexistent aaa.paypal.com.
3. The attacker repeats steps 1 and 2 using different prefixes: aab.paypal.com, aac.paypal.com, and so on, until the targeted server finally accepts a spoofed response. The spoofed response "poisons" the cache of the name server with a false address for www.paypal.com.
Attacker
100
3
2
1
Targeted name server
Cache
2. The attacker immediately sends fake responses to his own query, each containing a different query ID number and a false IP address for www.paypal.com.
Response
4. Users accessing www.paypal.com through the poisoned name server are directed instead to a Web site that looks like PayPal's but works only to harvest their user names and passwords.

- Link Ch 3f

Imagine that a resolver asks for the IP address of doesnotexist.example.com. An attacker sends back a response that looks like this:

```
$ dig doesnotexist.example.com
;; ANSWER SECTION:
doesnotexist.example.com.  120    IN  A    10.10.10.10

;; AUTHORITY SECTION:
example.com.               86400  IN  NS   www.example.com .

;; ADDITIONAL SECTION:
www.example.com .          604800   IN  A    10.10.10.20
```

An attacker is trying to trick the resolver into believing that **www.example.com** now lives at 10.10.10.20, and to remember that for 604800 seconds (7 days). This

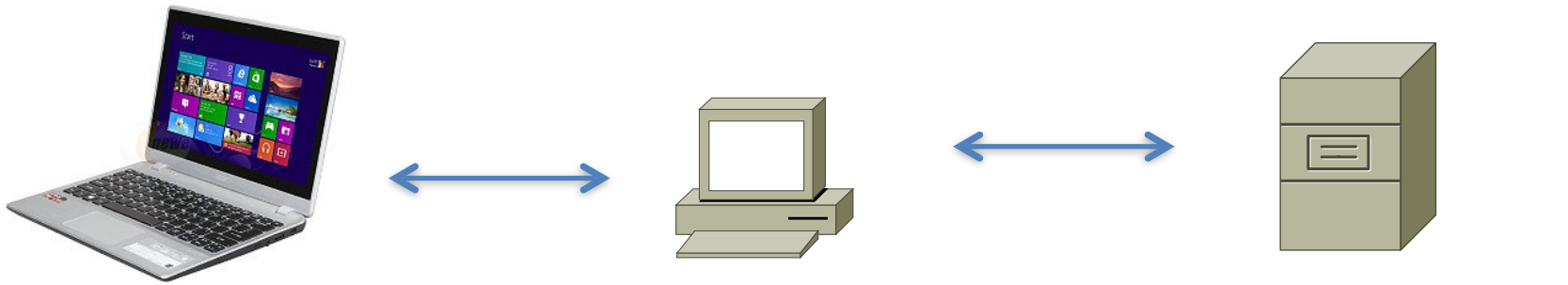
- Link Ch 3g

Consequences of the Kaminsky Attack

- Attack can be placed in a Web page
  - Many img tags
  - <img src=aaaa.paypal.com>
  - <img src=aaab.paypal.com>
  - <img src=aaac.paypal.com>
  - <img src=aaad.paypal.com>
  - etc.
- If one Comcast customer views that page, all other Comcast customers will be sent to the fake paypal.com
- Poisoning can take as few as 10 seconds

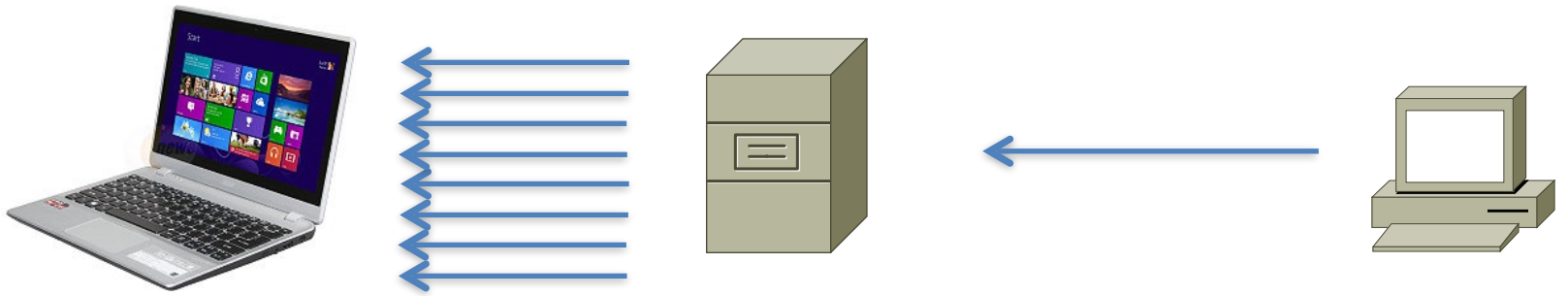
Man-in-the-Middle Attacks

- Attacker in the middle has enough info to perfectly forge responses
  - Unless DNSSEC is used



DNS as a DoS Amplifier

- Small requests lead to large responses
- UDP allows spoofing the source IP address



Target Open DNS Resolver Attacker


Kahoot!