

Super Secret Sysadmin Roundtable September 2008

BEST PRICE ON NET

WORLDWIDE SHIPPING

VIAGRA LEVITRA CIALIS VIAGRA SOFT CIALIS SOFT SOMA TRAMADOL

VISA MasterCard

The advertisement features a light gray background with a red diagonal banner in the top right corner that reads "WORLDWIDE SHIPPING". In the center, the text "BEST PRICE ON NET" is displayed. Below this, seven medicine icons are arranged horizontally, each with its name underneath: VIAGRA (blue pill), LEVITRA (orange pill), CIALIS (yellow pill), VIAGRA SOFT (blue soft tablet), CIALIS SOFT (orange soft tablet), SOMA (white pill), and TRAMADOL (white pill). At the bottom center, the logos for VISA and MasterCard are shown.

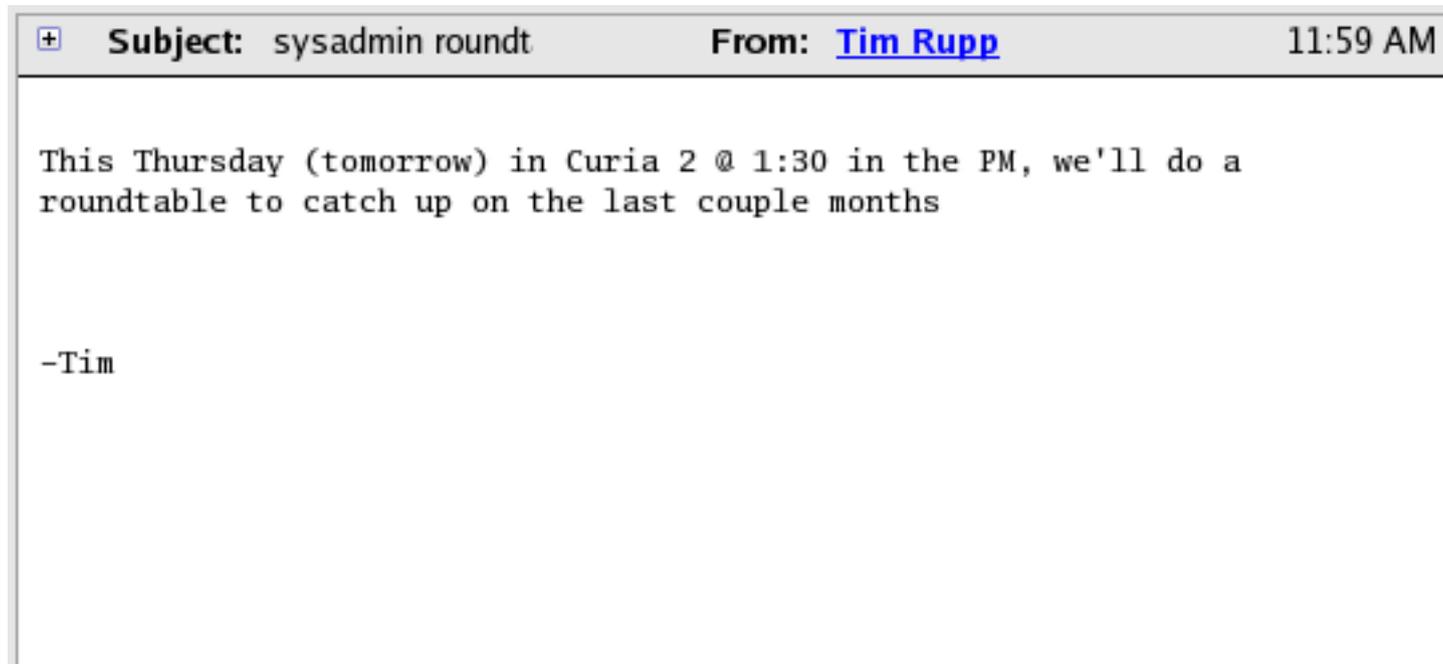
Please !

Answer this in your head!

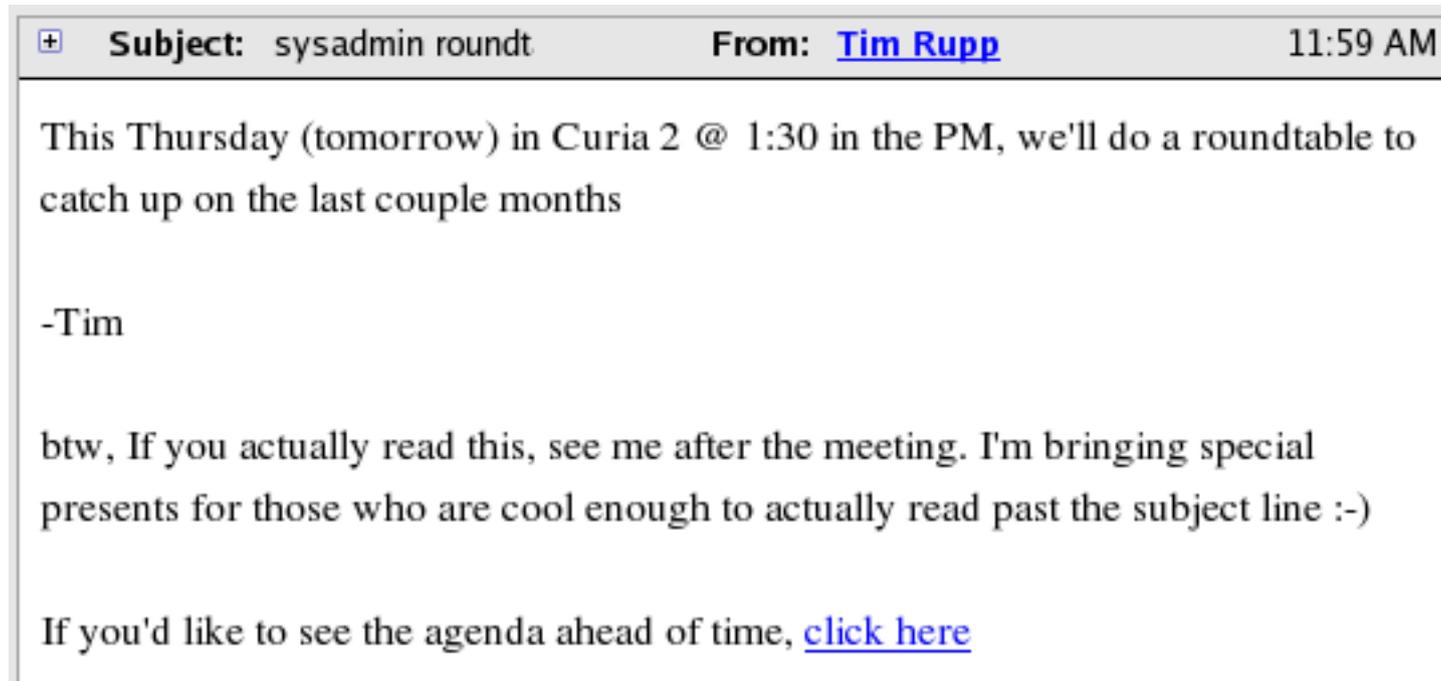
How many of you **are not** surprised that
there are cookies, a present, here today?

How many of you **are** surprised
that there are cookies here today?

After all, this is the email you got, right?



I sense that some of you think I'm crazy (I am)



Maybe those sensing, think that this email looks a little bit more like the email you received?

So why do this?

-CST wanted to get an idea, even if it was broad, of how many people read email in HTML

-

There are 1600 people on the sysadmin list

Of that, I can toss out about 30 because of
dead mailboxes that bounce back when I
send mail each month

I estimate that another hundred or so
just tag my mail as spam and never
get it

So a guesstimate of ~1400 people
receive the email with the
potential of “reading” it

Some may just up and delete it

Others may see the subject,
figure it does not apply to
them, and delete it.

I used both the known number and the guesstimate to come to the following, wildly un-scientific, conclusion

Somewhere between 36% and 42% on
people on that list read their mail
in HTML format

To those who did

We understand, that some
of you exercised diligence
when reading the mail

You may have

- Checked the headers; mail coming from on site
- Checked the “From”
- Noticed that it was a pretty typical format...for some of you
- Noticed it was sent at a pretty standard time of the month

And so, having been satisfied
that the email was likely
legit, clicked on links in it

Those predisposed to clicking

Are really those that we're
more concerned with

You know who you are.

We don't need to tell you

iPhone; U; CPU like Mac OS X; en) AppleWebKit/420.1 (KHTML, like Gecko) Version/3.0 Mobile/4A102 Safari/419.3
iPhone; U; CPU like Mac OS X; en) AppleWebKit/420.1 (KHTML, like Gecko)
Windows; U; Windows NT 5.1; en-US; rv:1.9.0.1) Gecko/2008070208 Firefox/3.0.1
Windows; U; Windows NT 5.1; en-US; rv:1.8.1.16) Gecko/20080708 Thunderbird/2.0.0.16
compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; InfoPath.1)
compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Macintosh; U; Intel Mac OS X 10_5_4; en-us) AppleWebKit/525.18 (KHTML, like Gecko)
compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)
Windows; U; Windows NT 5.1; en-US; rv:1.7.12) Gecko/20050915
Macintosh; U; Intel Mac OS X; en-US; rv:1.8.0.9) Gecko/20061207 Thunderbird/1.5.0.9
X11; U; Linux i686; en-US; rv:1.8.1.16) Gecko/20080724 Red Hat/2.0.0.16-1.el5 Thunderbird/2.0.0.16
X11; U; Linux i686; en-US; rv:1.8.0.12) Gecko/20080703 Red Hat/1.5.0.12-0.19.el4 Firefox/1.5.0.12 pango-text
X11; U; Linux i686; en-US; rv:1.9.0.1) Gecko/2008071611 Red Hat/3.0.1-1.el5 Firefox/3.0.1
Macintosh; U; PPC Mac OS X 10_4_11; en) AppleWebKit/525.18 (KHTML, like Gecko) Version/3.1.2 Safari/525.22
Windows; U; Windows NT 5.1; en-US; rv:1.8.0.14) Gecko/20071210 Thunderbird/1.5.0.14
compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322)
X11; U; Linux i686 (x86_64); en-US; rv:1.8.1.16) Gecko/20080716 Fedora/1.1.11-1.fc9 pango-text SeaMonkey/1.1.11
X11; U; Linux x86_64; en-US; rv:1.8.1.16) Gecko/20080723 Fedora/2.0.0.16-1.fc9 Thunderbird/2.0.0.16
Windows; U; Windows NT 5.1; en-US; rv:1.8.1.16) Gecko/20080708 Thunderbird/2.0.0.16
compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; InfoPath.2; MSOffice 12)
Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6
Windows; U; Windows NT 6.0; en-US; rv:1.8.1.16) Gecko/20080708 Thunderbird/2.0.0.16
X11; U; Linux i686; en-US; rv:1.8.0.12) Gecko/20071019 Red Hat/1.5.0.12-0.7.el4 Firefox/1.5.0.12 pango-text
Macintosh; U; PPC Mac OS X; en) AppleWebKit/312.9 (KHTML, like Gecko)
Mozilla
compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Windows; U; Windows NT 5.1; en-US; rv:1.7.6) Gecko/20050317 Thunderbird/1.0.2
Windows; U; Windows NT 5.1; en-US; rv:1.8.1.16) Gecko/20080702 SeaMonkey/1.1.11
compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; InfoPath.1; Windows-Media-
Player/10.00.00.3990)
X11; U; Linux i686; en-US; rv:1.8.1.16) Gecko/20080723 Fedora/2.0.0.16-1.fc9 Thunderbird/2.0.0.16
Windows; U; Windows NT 5.1; en-US; rv:1.7) Gecko/20040707 Firefox/0.9.2
compatible; Lotus-Notes/6.0; Windows-NT)
Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6
Windows; U; Windows NT 5.1; en-US; rv:1.8.1.16) Gecko/20080708 Lightning/0.8 Thunderbird/2.0.0.16
X11; U; Linux x86_64; en-US; rv:1.8.0.14eol) Gecko/20080802 Red Hat/1.0.9-24.el4 SeaMonkey/1.0.9
Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1.16) Gecko/20080707 Thunderbird/2.0.0.16
compatible; Konqueror/3.5; Linux) KHTML/3.5.9 (like Gecko) (Kubuntu)
compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705; Tablet PC 1.7; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30;
InfoPath.1; .NET CLR 3.0.04506.648)
Windows; U; Windows NT 5.1; en-US; rv:1.8.1.16) Gecko/20080708 Thunderbird/2.0.0.16 Mnenhy/0.7.5.0
compatible; MSIE 7.0; Windows NT 6.0; Trident/4.0; SLCC1; .NET CLR 2.0.50727; Tablet PC 2.0; InfoPath.2; WWTCClient2; Zune 2.5; .NET CLR
3.5.21022; .NET CLR 3.5.30729; .NET CLR 3.0.30618; MSOffice 12)
Windows; U; Windows NT 5.1; en-US; rv:1.7.2) Gecko/20040804 Netscape/7.2 (ax)

Some of my favorites from the list

Mozilla

Thunderbird/1.0.2

Firefox/0.9.2

To whom it should concern:

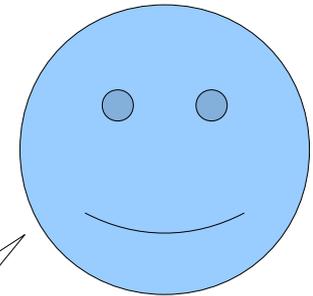
Please refer to the following links after the meeting

<http://www.mozilla.com/firefox>

<http://www.mozilla.com/thunderbird>

What about that link though?

You may say...



The links led to
the security pages!

Which leads me to the next topic

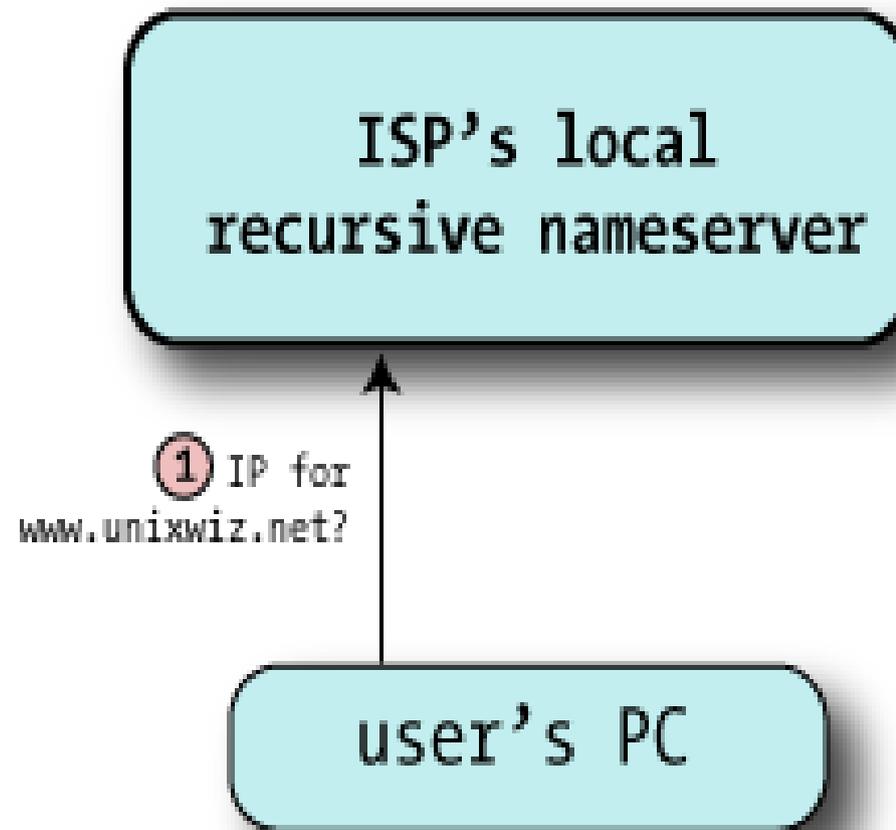
DNS Vulnerability

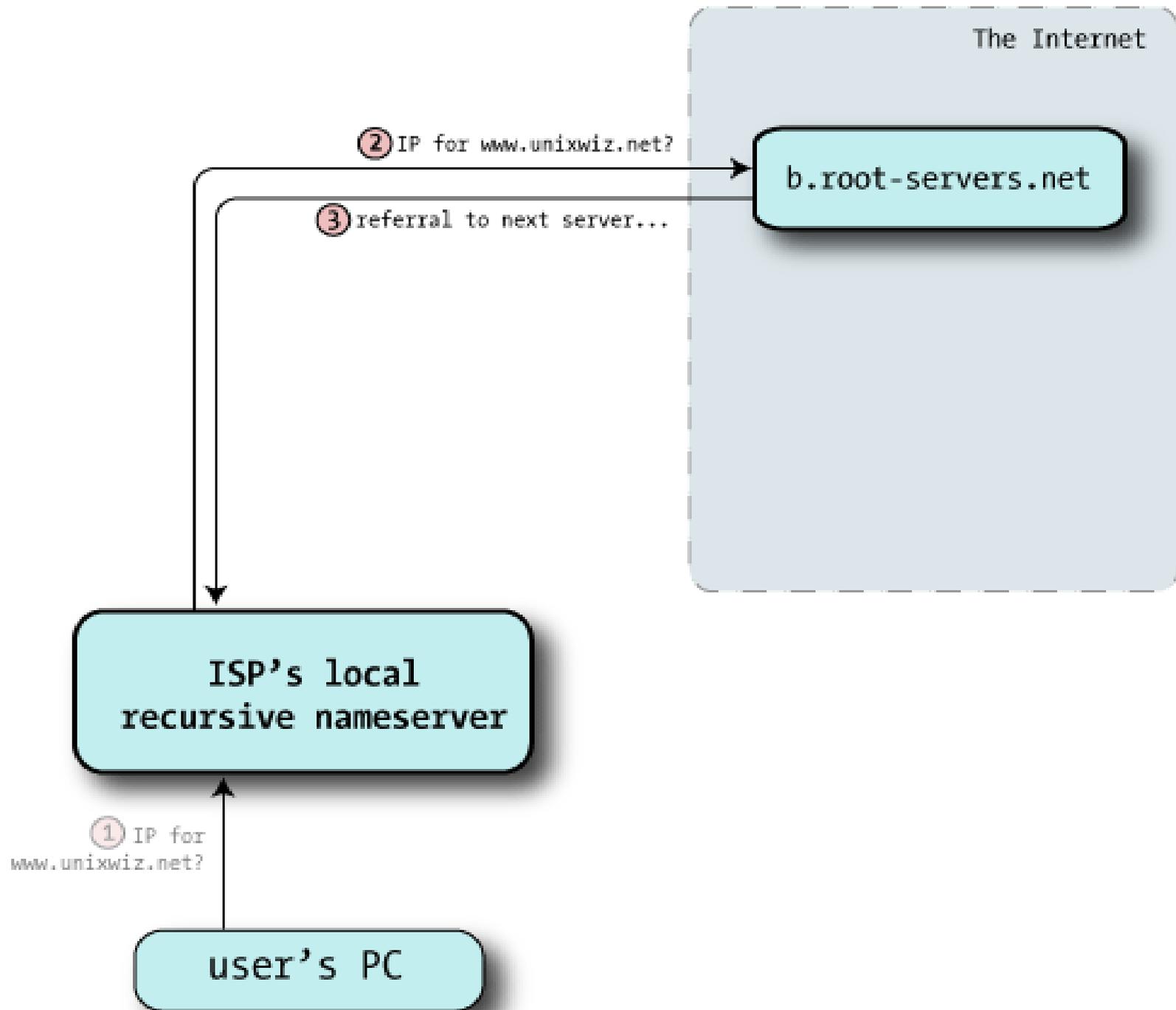
- Form of cache poisoning
- Patches are out for affected name servers
- FNAL has patched the DNS on site
- Friends of CST have seen an increase in underground chatter about the bug, but it's received surprisingly little attention

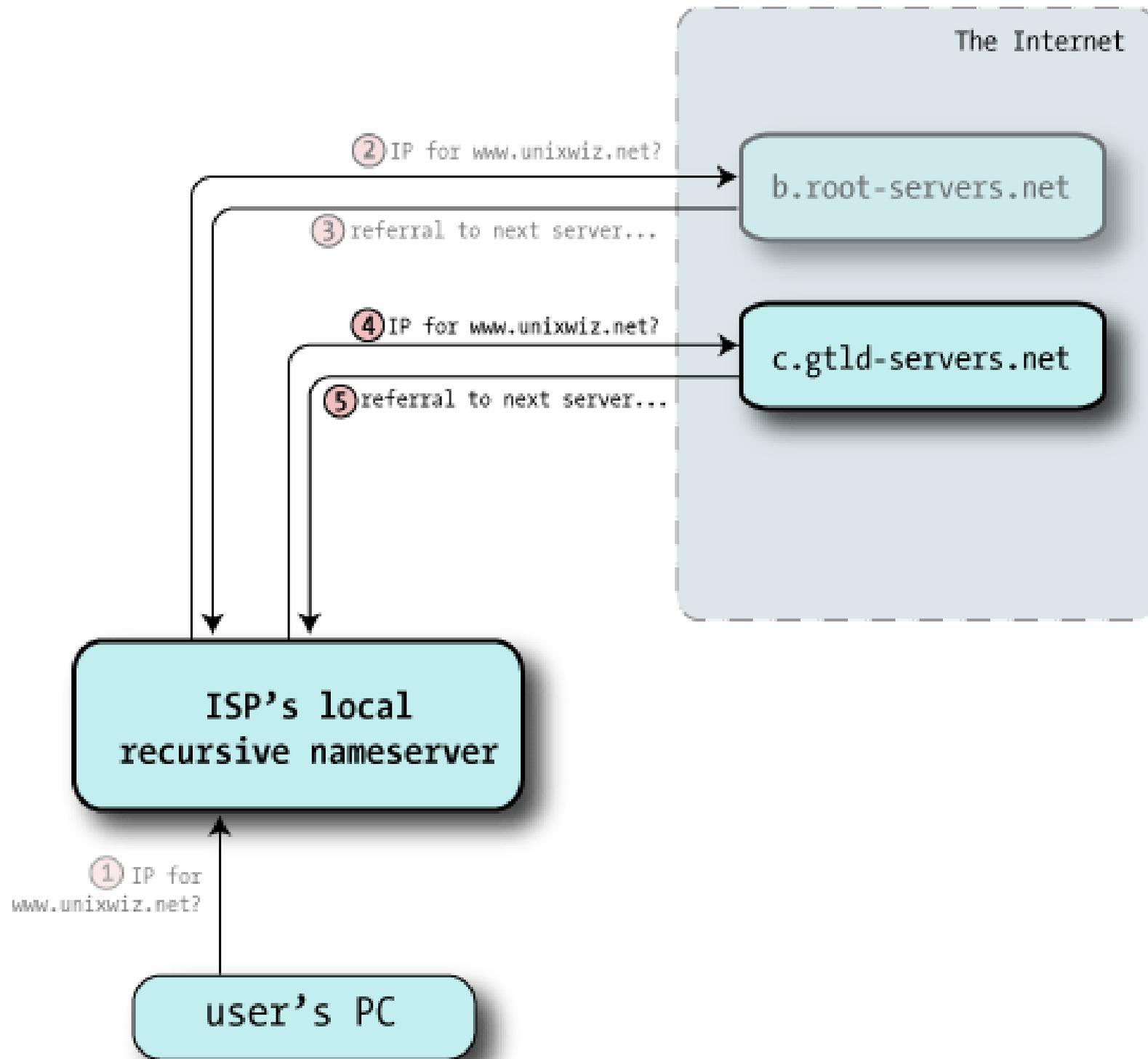
Understanding the problem

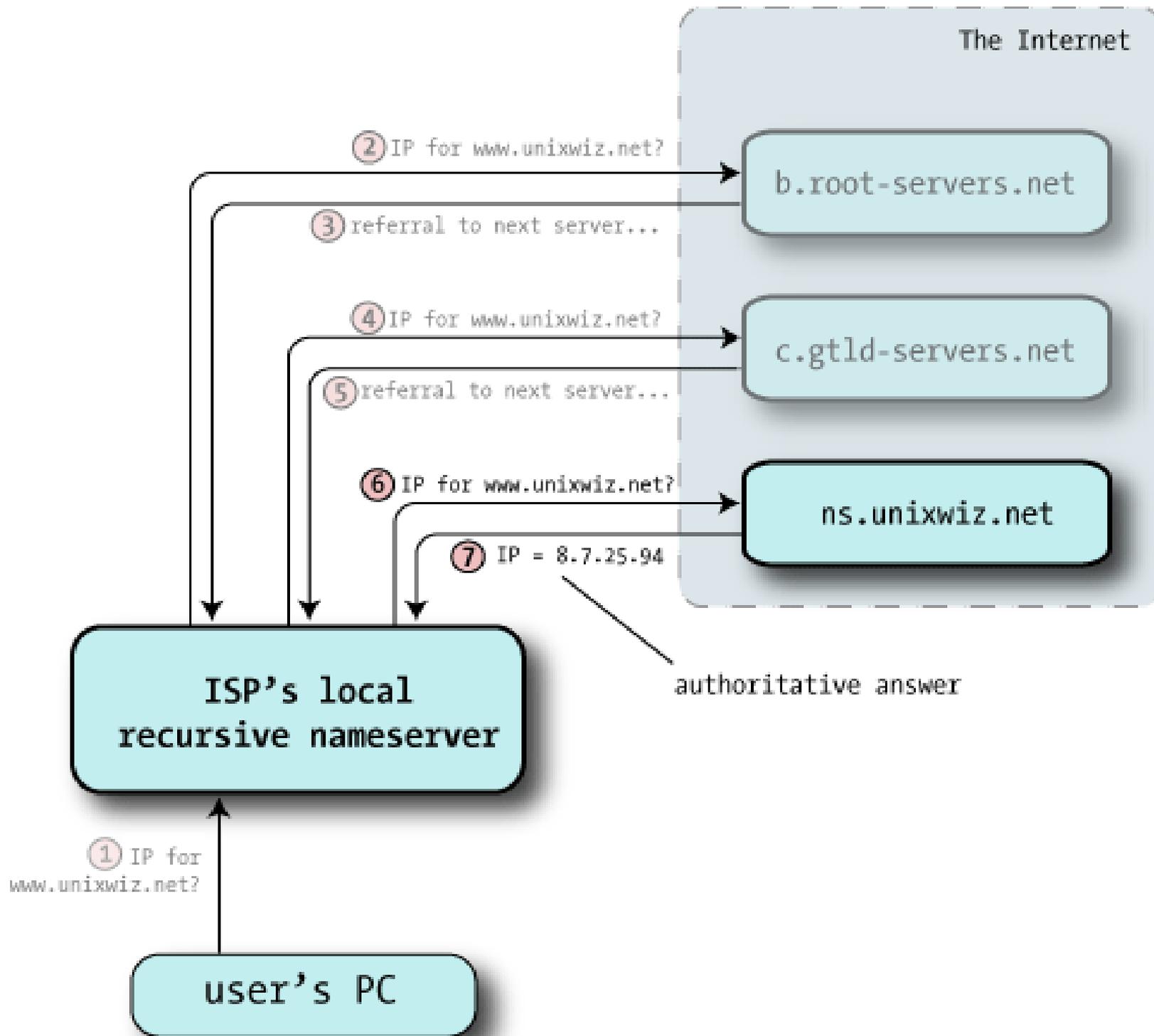
- **DNS is UDP; connectionless**
 - Resolver sends requests
 - Waits to be told an answer; from anyone
- **Requests are made with a query ID**
 - This ID is a number between 0 and 65536
- **QID answer must match QID in request**

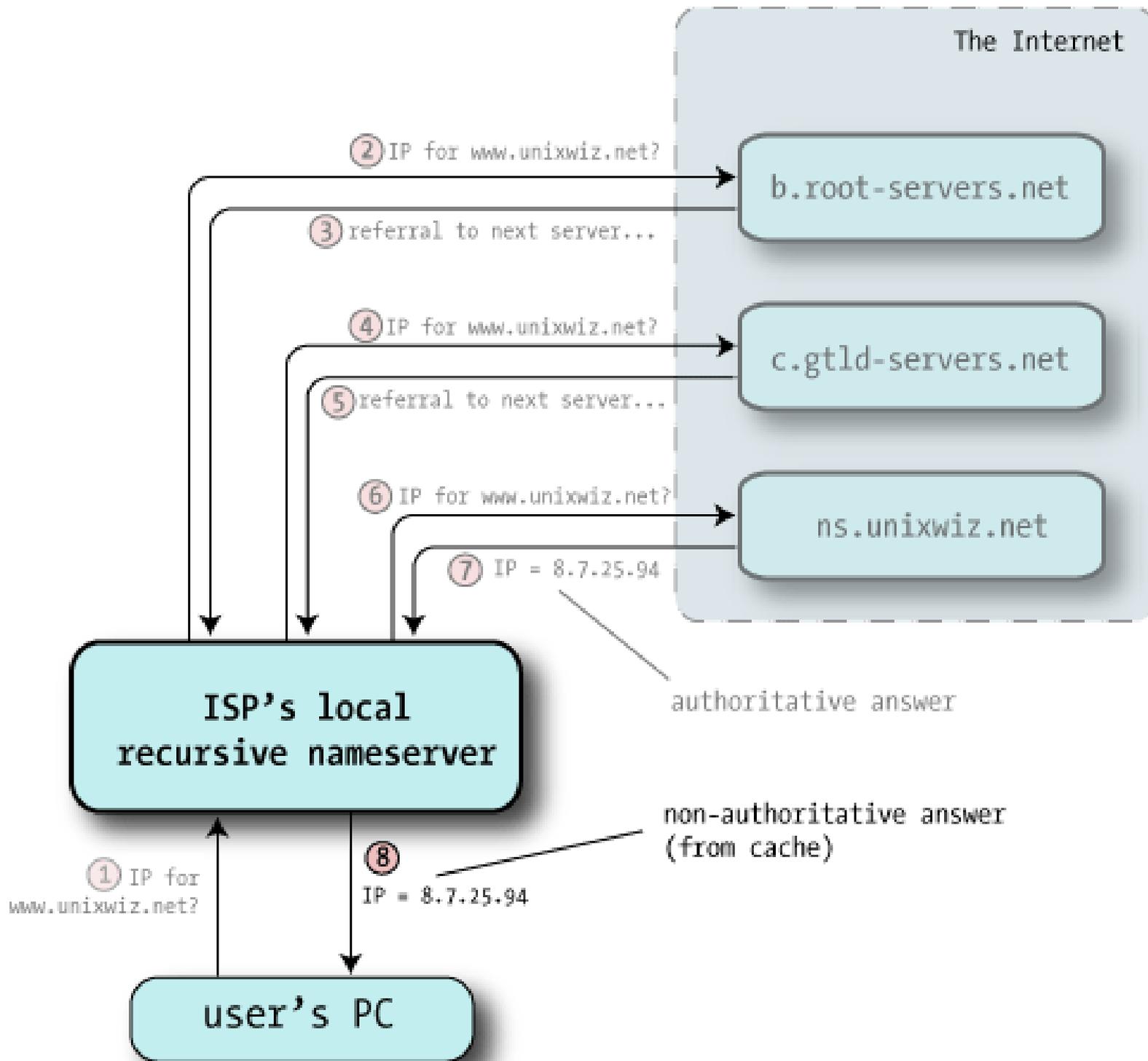
- A Simple DNS Query



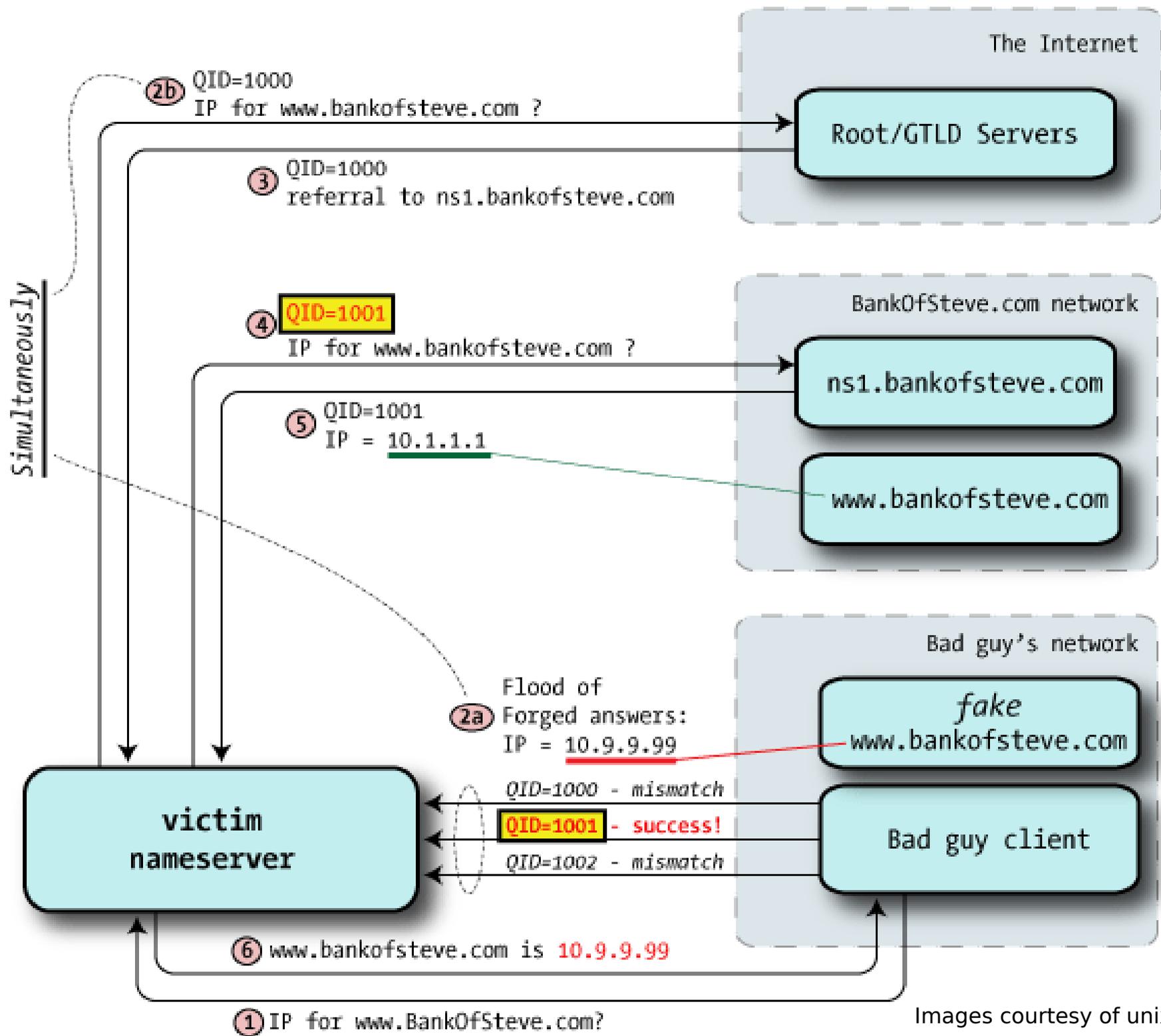








- Cache Poisoning a DNS name



The problem

- Race condition
- Bad guy needs to be able to respond faster than the legit server
- Small key space makes QID guessable

Problems with poisoning only 1 host

- Obviously, only able to poison a specific name
- Rely on real host names to poison. This means that your potential attack space is small
 - organizations only have so many real host names
- Harder to hack all hostnames

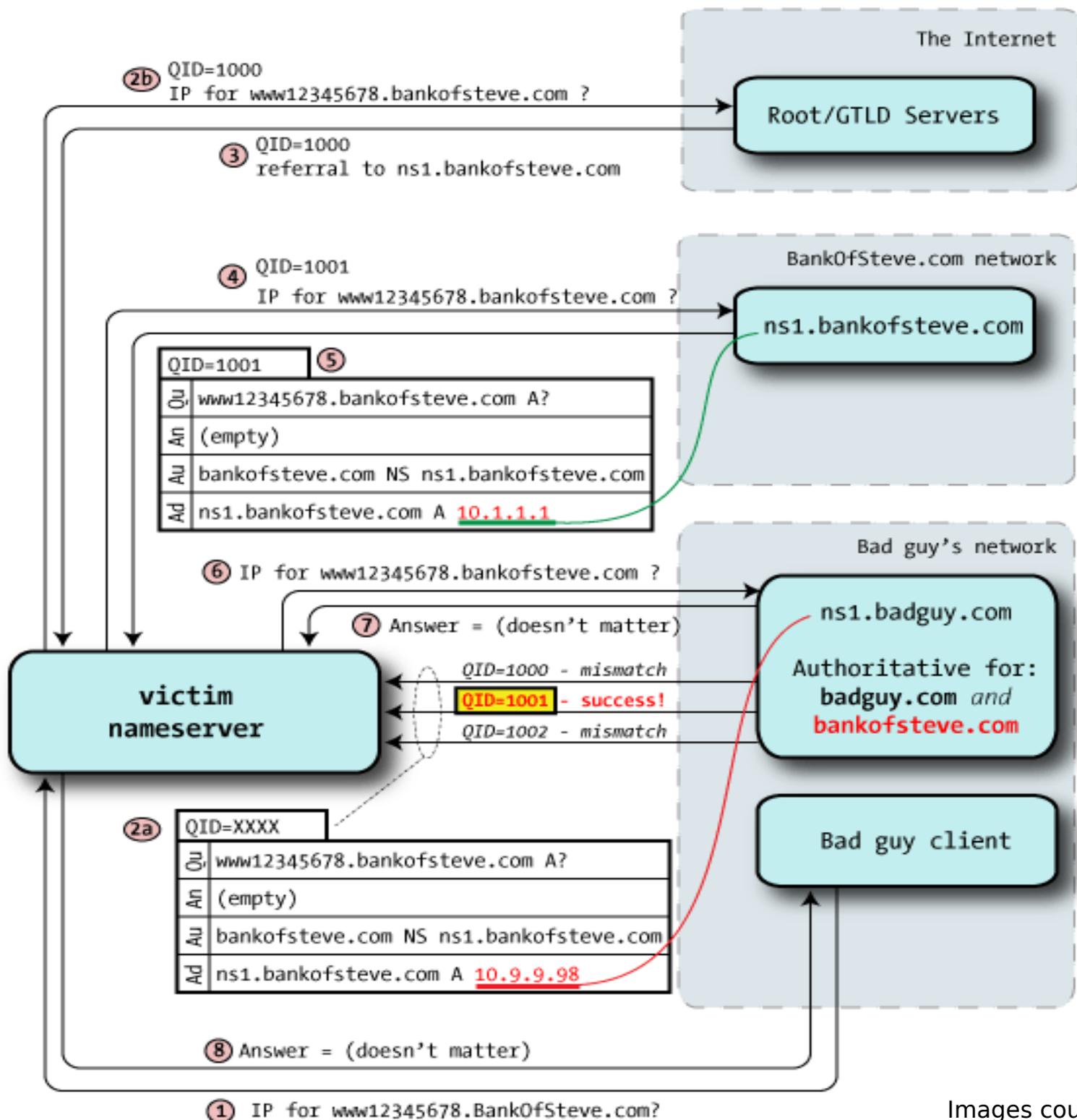
- Kaminsky DNS Poisoning

Preparation

- Set up your own DNS server that is authoritative for the domain you want to poison
 - Anyone can do this
 - But not just anyone will send you questions

- Do the same as before with normal cache poisoning
 - But request random hostnames in victim domain
 - Instead of replying with what IP is associated with that hostname, specify your DNS server as being authoritative for that realm

The next slide may hurt your eyes



Result of attack

Bad guy owns the entire domain

Not just a single host

Fun things to do when DNS is compromised



We got hosed, Tommy.
We got hosed.

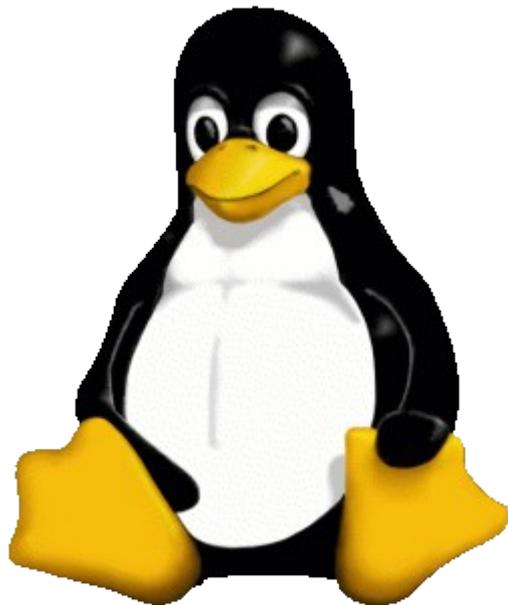


OH, Davey!

Steal linux farms en masse

warning: rpmts_HdrFromFdno:
V3 DSA signature: NOKEY,
key ID db42a60e

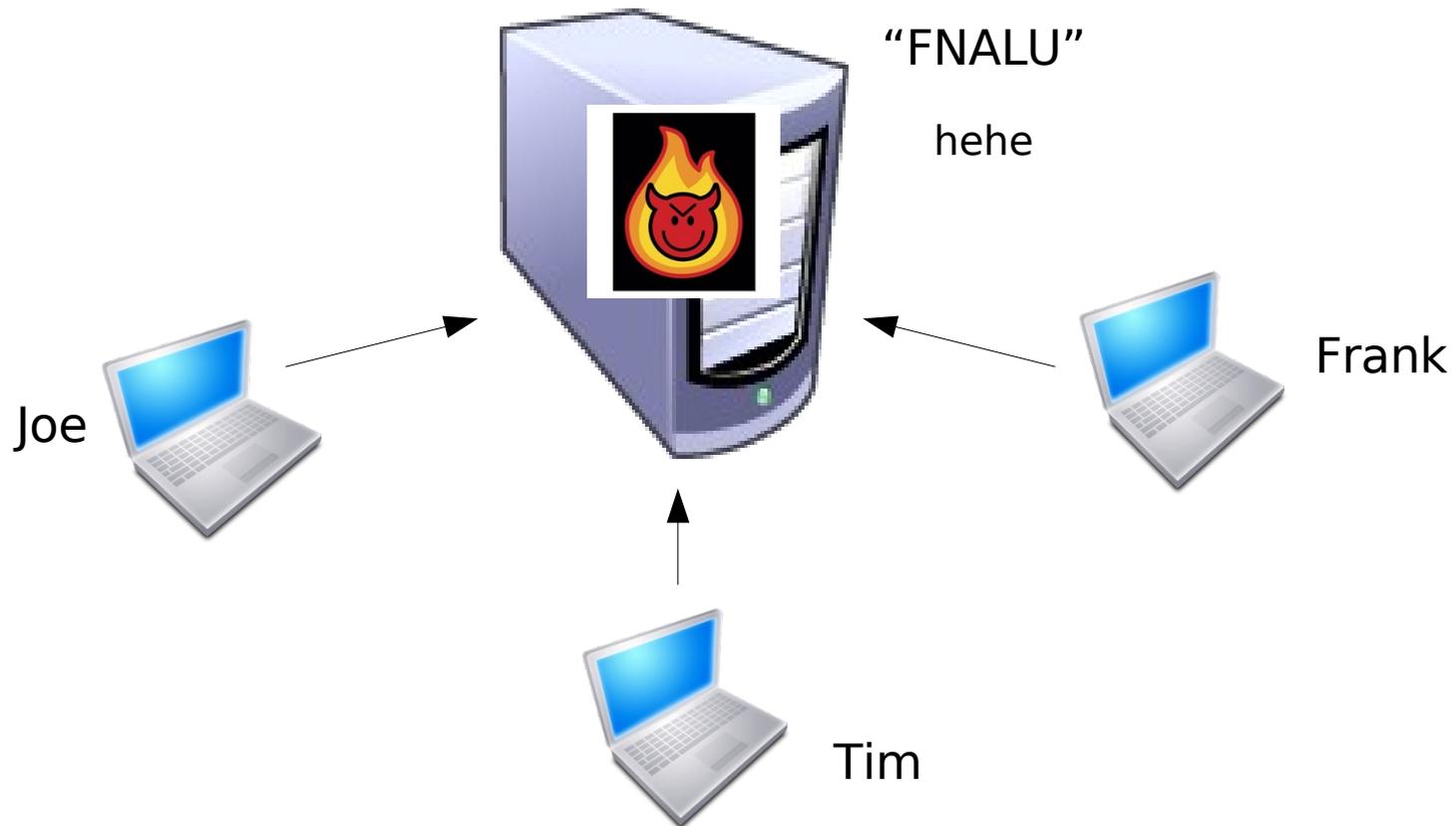
yum
yellowdog updater modified



because who seriously pays
attention to warnings like that?

Mass credential theft via a central service

@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@



But that's a warning too. Warnings are harmless...

Make spam with legit domains



Dear Chase customer,

Security and confidentiality are at the heart of Chase Bank. Your details (and your money) is protected by a number of technologies, including Secure Sockets Layer (SSL) encryption.

We would like to notify you that Chase Bank carries out client details verification procedure that is compulsory for all our customers. This procedure is attributed to a routine banking software update.

Please visit our Customer Confirmation Page using the link below and follow the instructions on the screen

<http://www.chase.com/ccp/index.php?session=ncsvjjDorcyOahg>

Chase Bank Customer Service



<http://www.chase.com/ccp/index.php?session=ncsvjjDorcyOahg>

Further Reading

<http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>

was-i-scanned

- Self-service tool to check when you were, and what type of scan was run.
- Randy gets this question often, so this was the next logical step.

<https://clogger.fnal.gov/wasiscanned>

Was I scanned?

Start Date

September 2008						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
<<	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4

End Date

September 2008						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
<<	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	1	2	3	4

Start Time

Hour

Minute

Second

End Time

Hour

Minute

Second

Check for scans

Search Results for catbot.dhcp.fnal.gov (131.225.82.104)

[Search Again](#)

Time the scan occurred	Scan info
2008-09-04T07:17:26.000-05:00	SSH: No issue found
2008-09-04T07:16:29.000-05:00	SSH-auth(port=22): No issue found
2008-09-04T07:09:05.000-05:00	NEW: -sS -P0 -T4 --osscan-limit --osscan-guess --host-timeout 15m -O2 NONE: 1711 ports are closed:
2008-09-04T05:33:25.000-05:00	SSH: No issue found
2008-09-04T05:26:38.000-05:00	SSH-auth(port=22): No issue found
2008-09-04T05:23:20.000-05:00	AGED: -sS -p 1-65535 -P0 -T5 --osscan-limit --osscan-guess --host-timeout 15m -A NONE: 65530 ports are closed:
2008-09-04T03:13:23.000-05:00	AGED: -sS -p 1-65535 -P0 -T5 --osscan-limit --osscan-guess --host-timeout 15m -A NONE: 65530 ports are closed:
2008-09-04T01:21:50.000-05:00	SSH: No issue found
2008-09-04T01:17:47.000-05:00	SSH-auth(port=22): No issue found
2008-09-04T01:06:36.000-05:00	AGED: -sS -p 1-65535 -P0 -T5 --osscan-limit --osscan-guess --host-timeout 15m -A NONE: 65530 ports are closed:
2008-09-03T23:24:54.000-05:00	SSH: No issue found
2008-09-03T23:03:28.000-05:00	SSH: No issue found
2008-09-03T22:56:39.000-05:00	SSH-auth(port=22): No issue found
2008-09-03T22:52:33.000-05:00	NEW: -sS -P0 -T4 --osscan-limit --osscan-guess --host-timeout 15m -O2 NONE: 1711 ports are closed:
2008-09-03T22:06:46.000-05:00	NEW: -sS -P0 -T4 --osscan-limit --osscan-guess --host-timeout 15m -O2 NONE: 1711 ports are closed:
2008-09-03T22:01:24.000-05:00	NEW: -sS -P0 -T4 --osscan-limit --osscan-guess --host-timeout 15m -O2 NONE: 1711 ports are closed:
2008-09-03T20:10:41.000-05:00	NEW: -sS -P0 -T4 --osscan-limit --osscan-guess --host-timeout 15m -O2 NONE: 1711 ports are closed:
2008-09-03T19:56:33.000-05:00	NEW: -sS -P0 -T4 --osscan-limit --osscan-guess --host-timeout 15m -O2 NONE: 1711 ports are closed:
2008-09-03T17:42:39.000-05:00	NEW: -sS -P0 -T4 --osscan-limit --osscan-guess --host-timeout 15m -O2 NONE: 1711 ports are closed:

Done

clogger.fnal.gov



[Adblock](#)

Web proxies

- Soon to be in production
- Will be transparent (no browser config)

FIRE 1

The standard default configuration

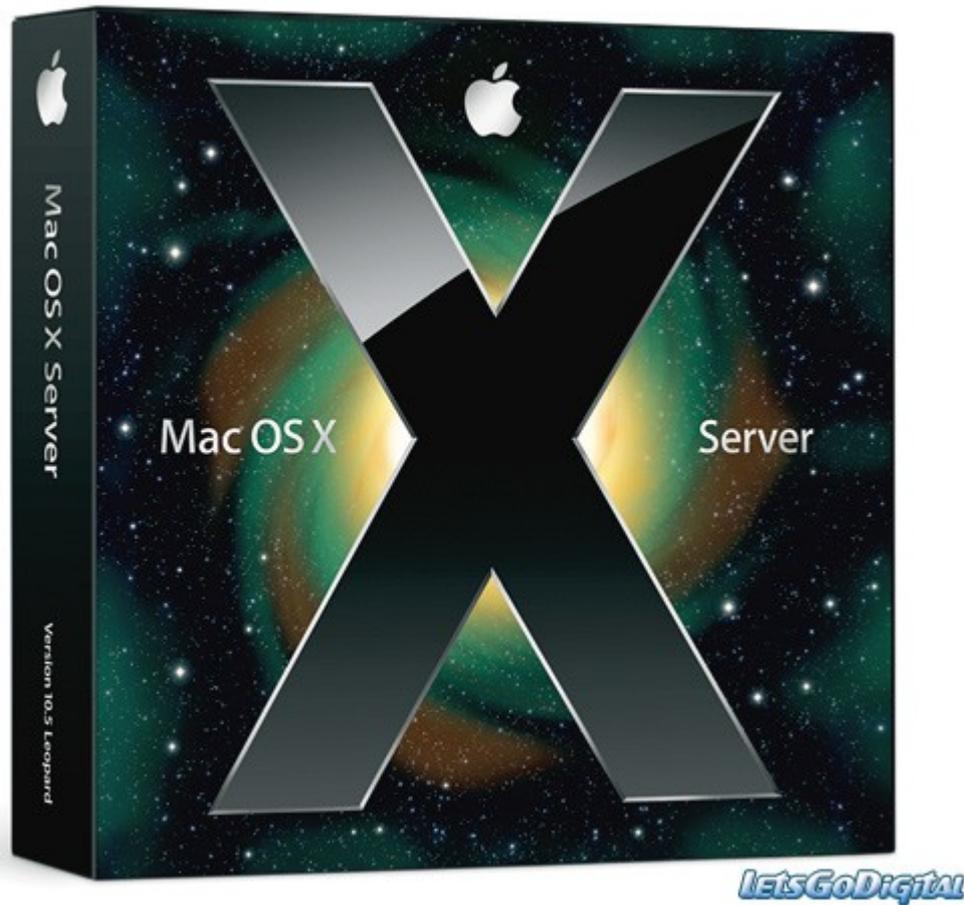
Our intrepid sysadmin

(who we'll call Joe Klemencic...to protect the innocent)

Was casually going about their business for the day



Their goal; to do a standard installation of Leopard server



Nothing fancy

Strong Auth scanner got wind of the install

This is relatively common
though with vanilla installs of
UNIX-like systems



Anyways, a block was issued

The sysadmin powered down the machine for the weekend



Then powered up midway through next week

Put the machine on the net

And configured Kerberos

About 8 hours later...

...the machine was compromised





This is backwards from other systems

Upon closer examination

It was determined, that by not explicitly denying root login and empty passwords, the default was to allow them!

Lesson

Never assume the value of “default”
means what you think it means

Always explicitly state your
intent in the config files

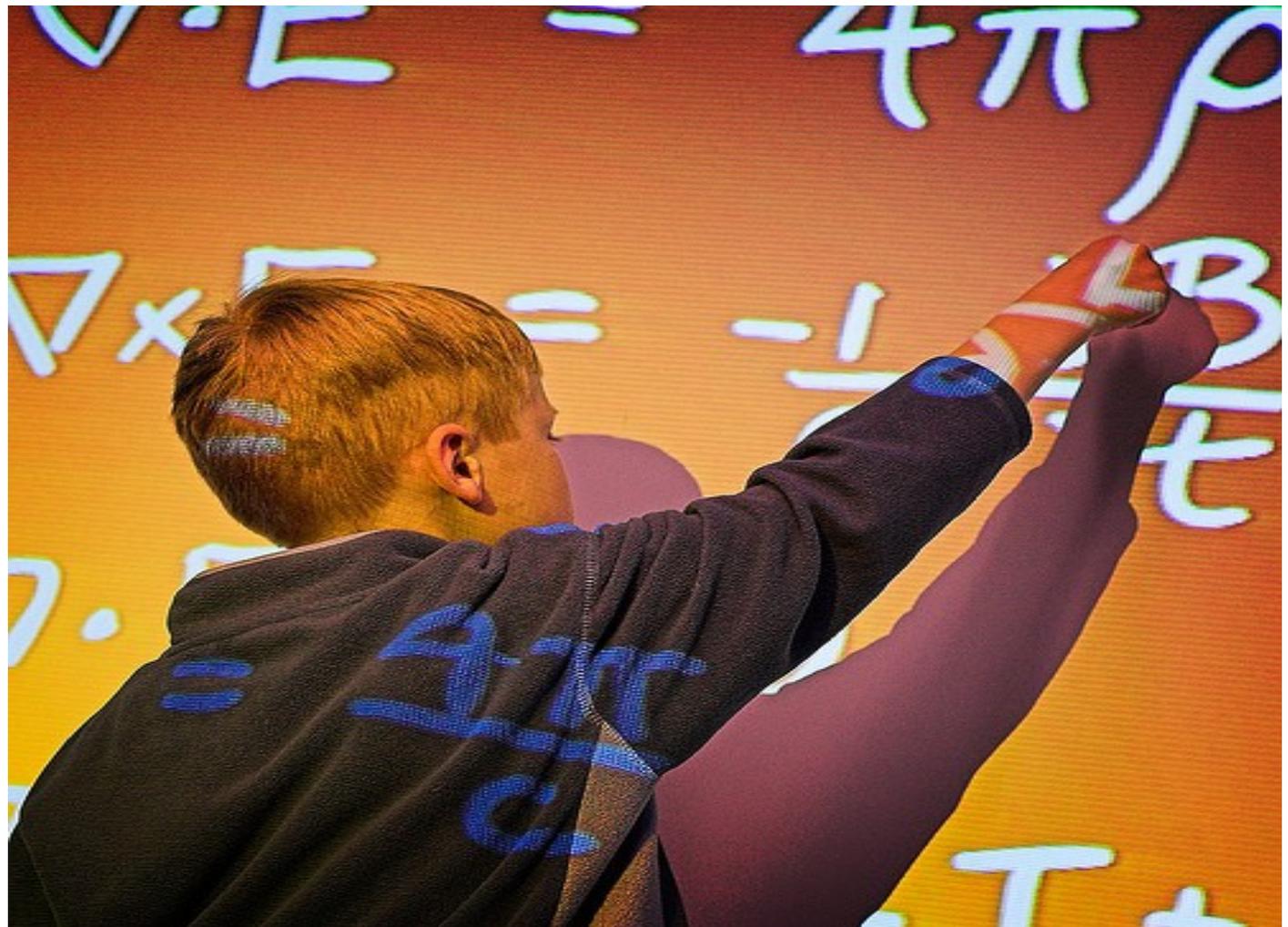
FIRE 2

Under the net

Our gallant physicist

(who we'll call Joe Klemencic...to protect the innocent)

Was casually going about their business for the day



While doing the clicky-clicky through the HTML maily-maily

Their computer contracted
something deviant



When asked if they were able to provide any info that would help us confirm or deny the report, our protagonist reported that he...

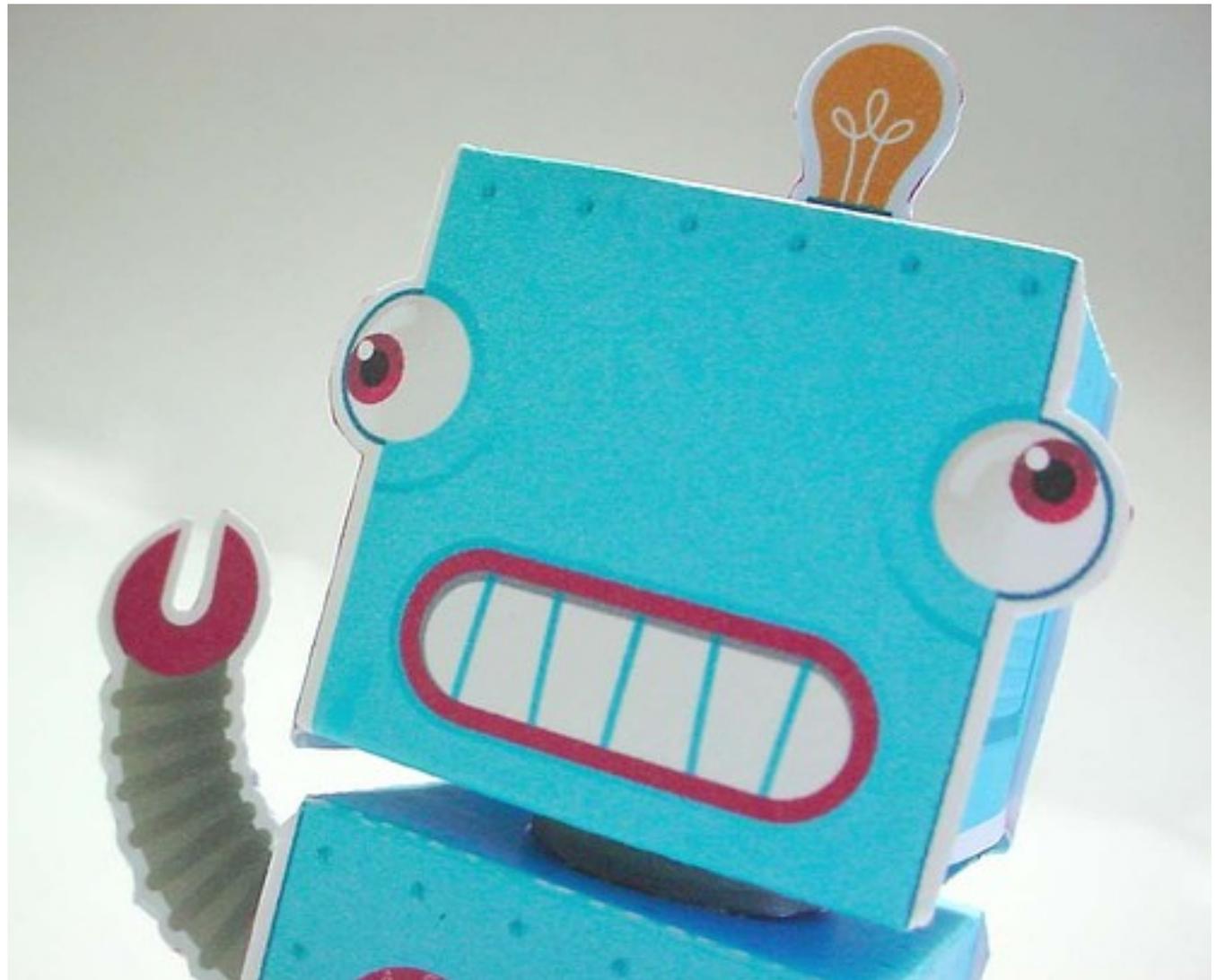


...did open a strange mail that he wasn't sure if he recognized the sender or not...

Oh boy, that's a problem

Sure enough, after examining the logs and the machine

It was determined that
an IRC bot had been
installed



Lesson

A couple clicks is all it takes these days to pop a machine

Employ a healthy dose of skepticism, and be diligent when clicking links

FIRE 3

Shareware with free shareware!

Our valorous engineer

(who we'll call Joe Klemencic...to protect the innocent)

Was casually going about their business for the day



They were perplexed.

How does one convert this AVI to an MPEG?



Ahh, no fear, no fear

The Internet
will have
the answer

The first attempt resulted in an application that only converted 10 files until needing a license



Searching the net continued, yielding two more sites.



This is about the
time that the flood
gates opened

AV alerted the admin's
of the machine

Result of incident? Wipe and re-install. Tsk tsk

Lesson

There's a good reason to use a less privileged account during day to day computer use

Running as local admin can be destructive and inconvenient if you find yourself on the wrong end of a rootkit

Policies

- Remote desktop (like VNC, Timbuktu, etc) switched from warning to blocking
- RDP being detected off site; will start at warning, then become blocking
- SSH cert is warning; will become blocking
- Few blocks now that incur a zero hour block. Most have a 1 hour delay

Reminders

e-cards

Friends and family,

don't let friends and family...

- Read
- Send
- Think about
- Contemplate opening
- Link to

e-cards.

Even if it is from “family” and...

- Says
- Insinuates
- Hints at
- Suggests
- Blatantly claims
- Joe says it



has cute animals in it



Please be mindful of where you are

```
if (  instanceof  ) {  
    echo "  
        Piracy probably not a wise move  
    ";  
}
```

Said with tongue firmly implanted in cheek

CST utilizes only the most
advanced proverbial new-age
technology, to safeguard the lab,
and help people better understand
the threats that are wrapped in
cute cuddly packets

Advanced Technology

Exhibit A

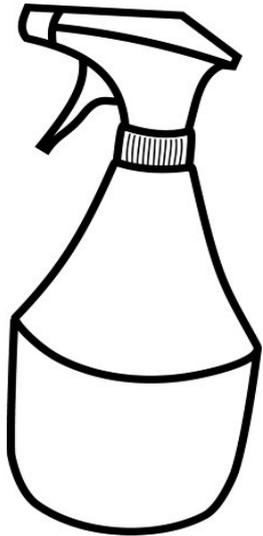


Exhibit B



Exhibit C



Exhibit D



Joe



Policy

