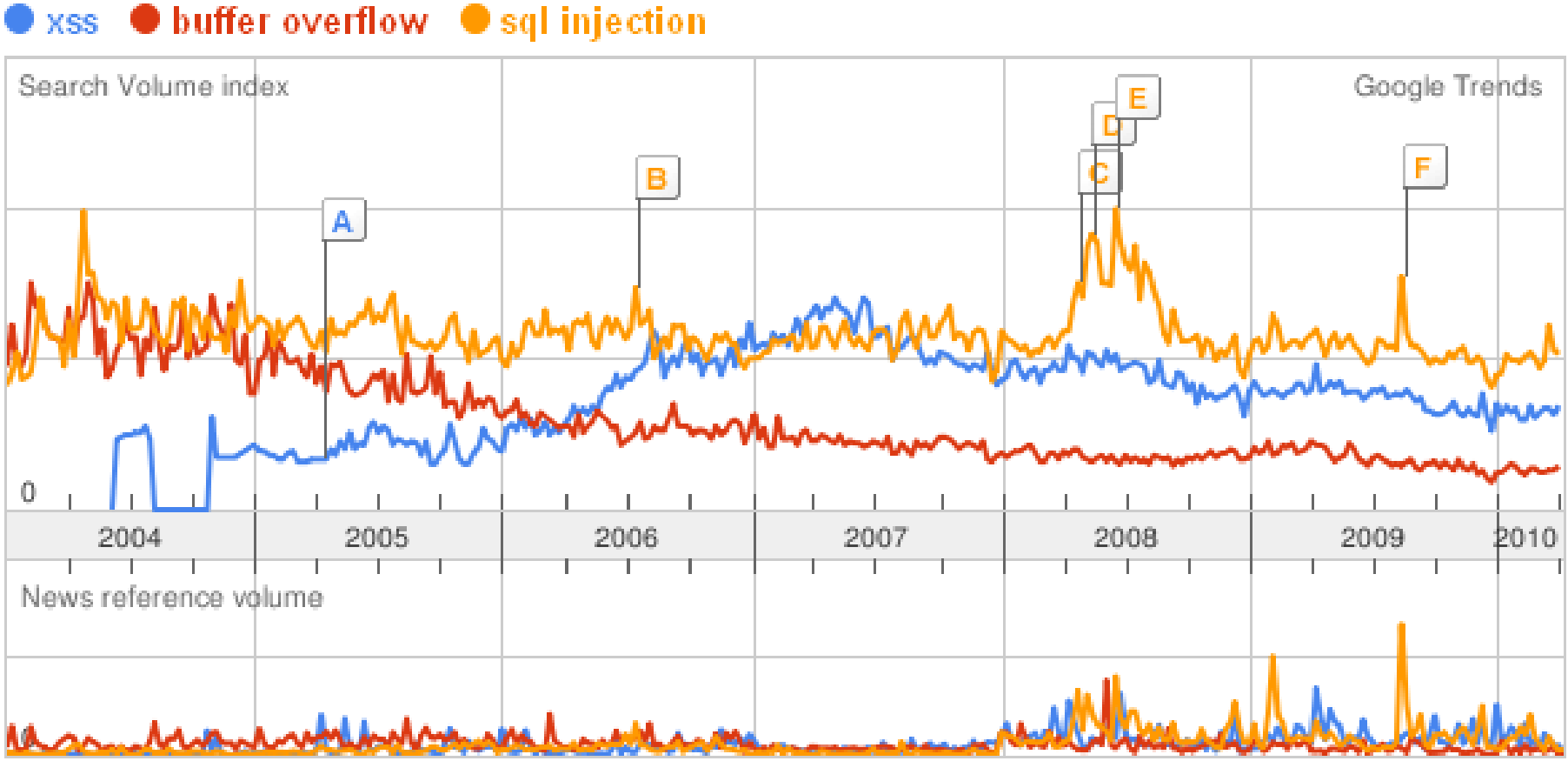
Web Applications - The next hacker frontier

About Me

- Robert Hansen - CEO
- SecTheory Ltd
  - Bespoke Boutique Internet Security
    - Web Application/Browser Security
    - Network/OS Security
    - http://www.sectheory.com/
- FallingRock Networks
- Advisory capacity to start-ups
- Founded the web application security lab
  - http://ha.ckers.org/ - the lab
  - http://sla.ckers.org/ - the forum

Going For It Anyway?

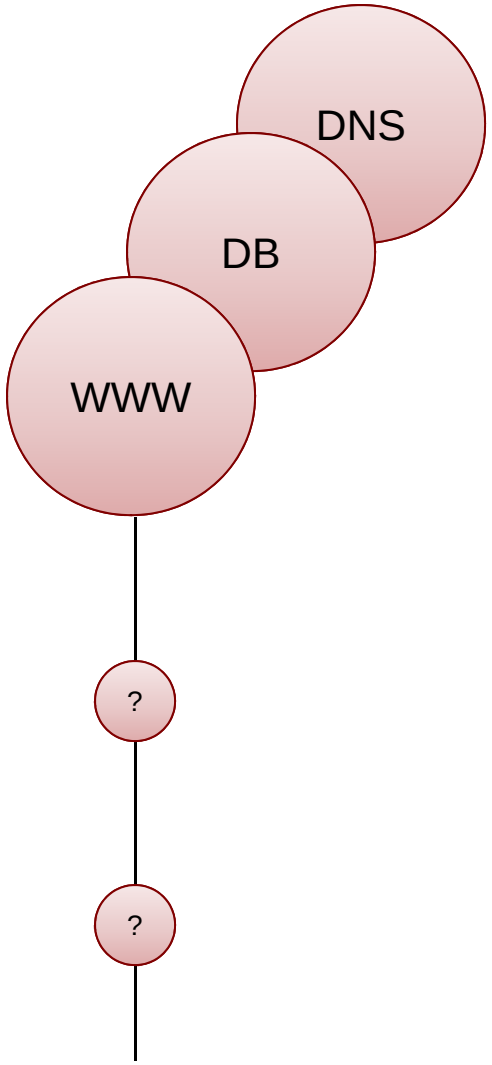

xss
buffer overflow
sql injection
Search Volume index
Google Trends
A
B
C
D
E
F
0
2004
2005
2006
2007
2008
2009
2010
News reference volume

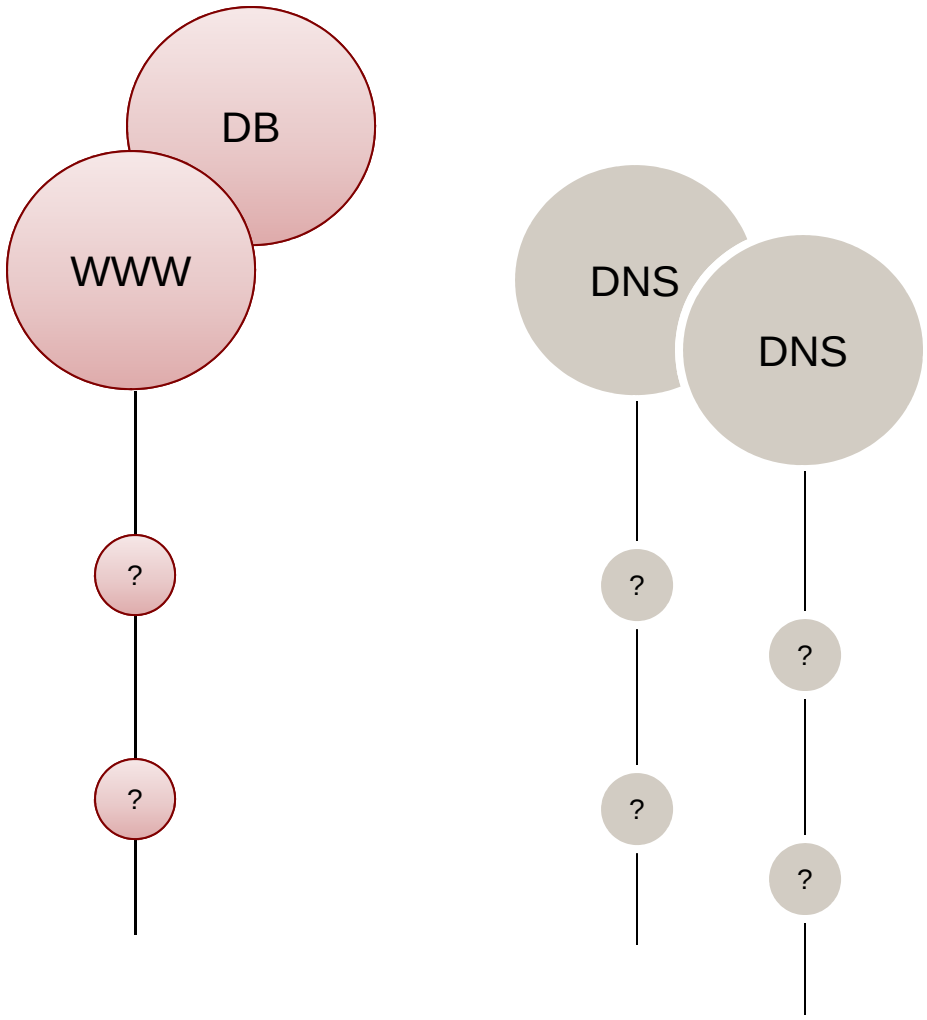
Overview

- Should be titled, “Why you’ll fail any real network/webappsec pen-test.”
- Web assessments are just like every other assessment – except they’re different. ☺
- What are the REAL risks of a determined adversary – and do I care about any other type?
- Let’s overcome some bad misconceptions we hear all the time.

"We only have one website. That's all that should be in scope. Right?"

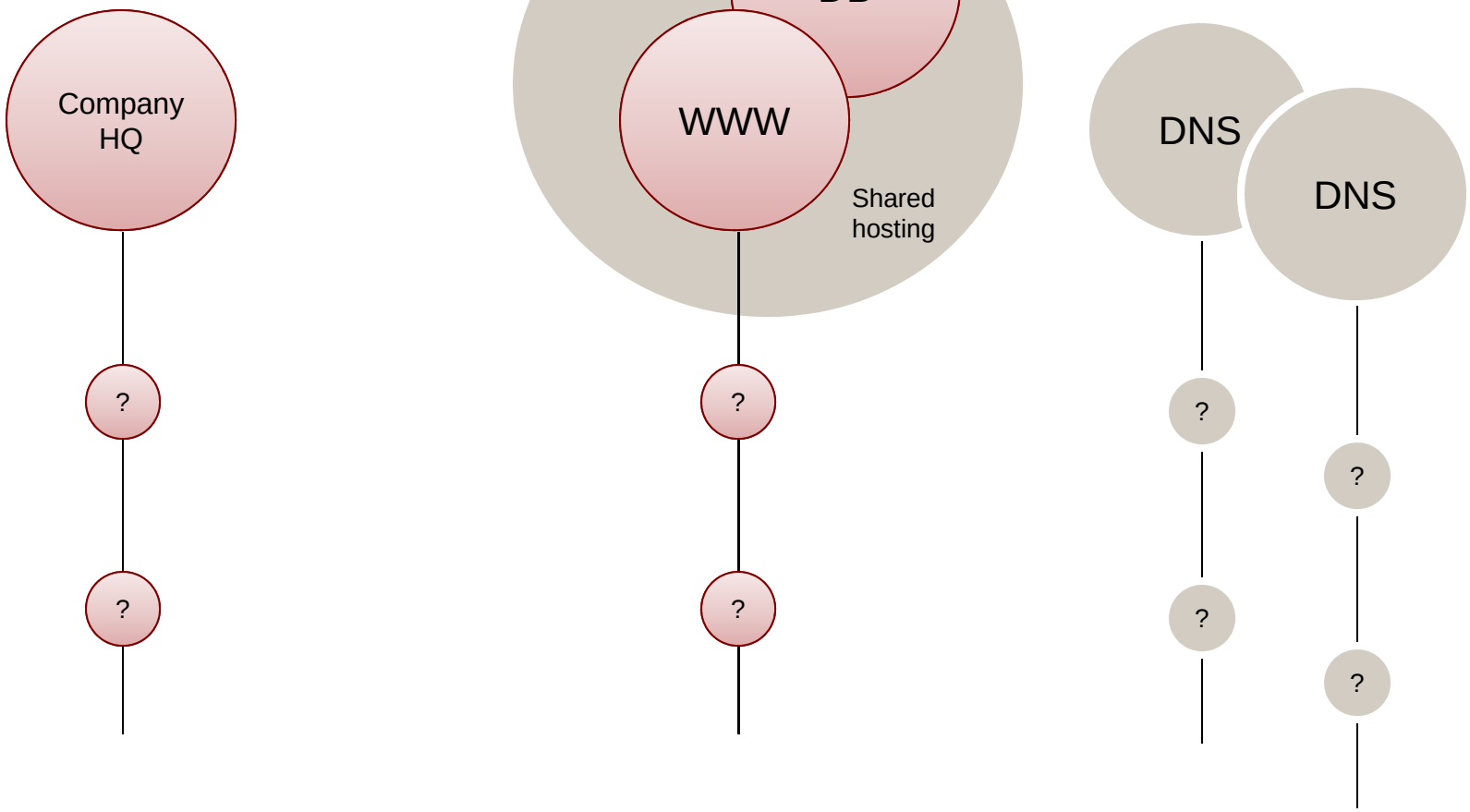
Answer: No. Absolutely, in no way is that correct… Not in a **REAL** pen test.

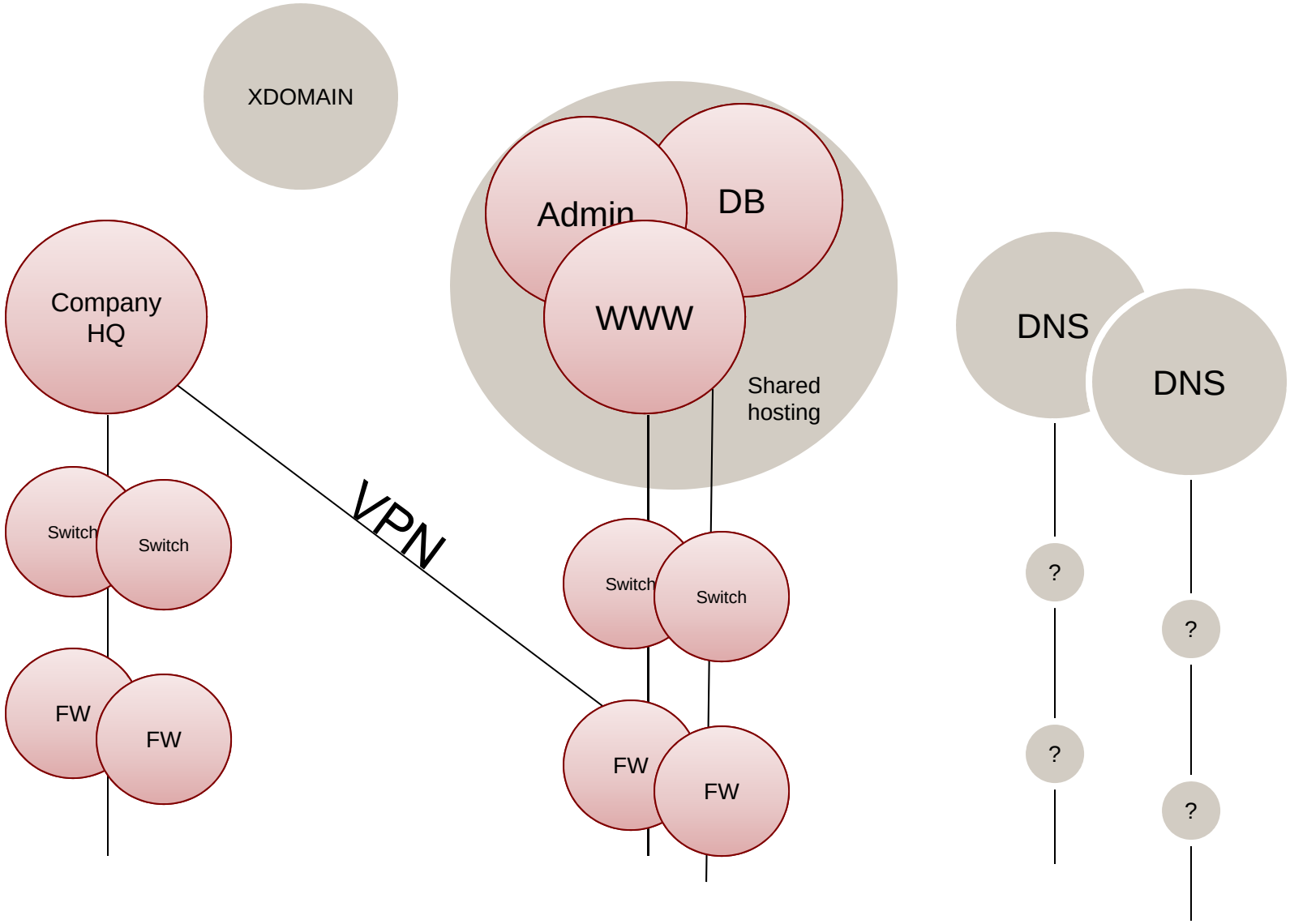

DNS
DB
WWW
?
?


DB
WWW
?
?
DNS
DNS
?
?
?
?

EMERGING THREATS

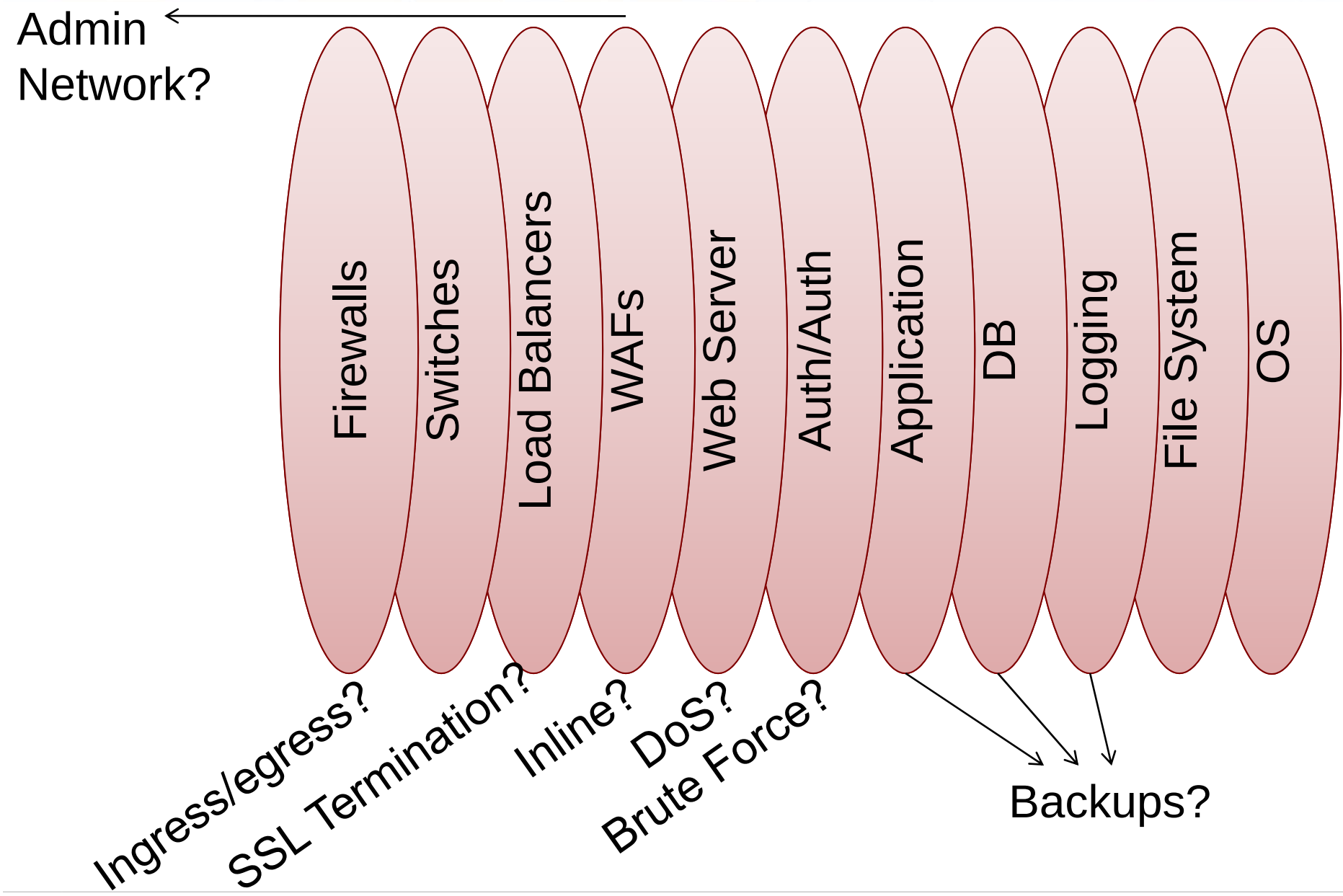
ADAPTIVE SECURITY STRATEGIES TO RESPOND TO EVOLVING THREATS




XDOMAIN
Admin
DB
WWW
Shared hosting
Company HQ
VPN
Switch
Switch
Switch
Switch
FW
FW
FW
FW
DNS
DNS
?
?
?
?

"We don't use shared hosting, so we're okay. We just use virtualization for our own sites."

Answer: Fine, but all your other sites are now in scope too – no cheating.

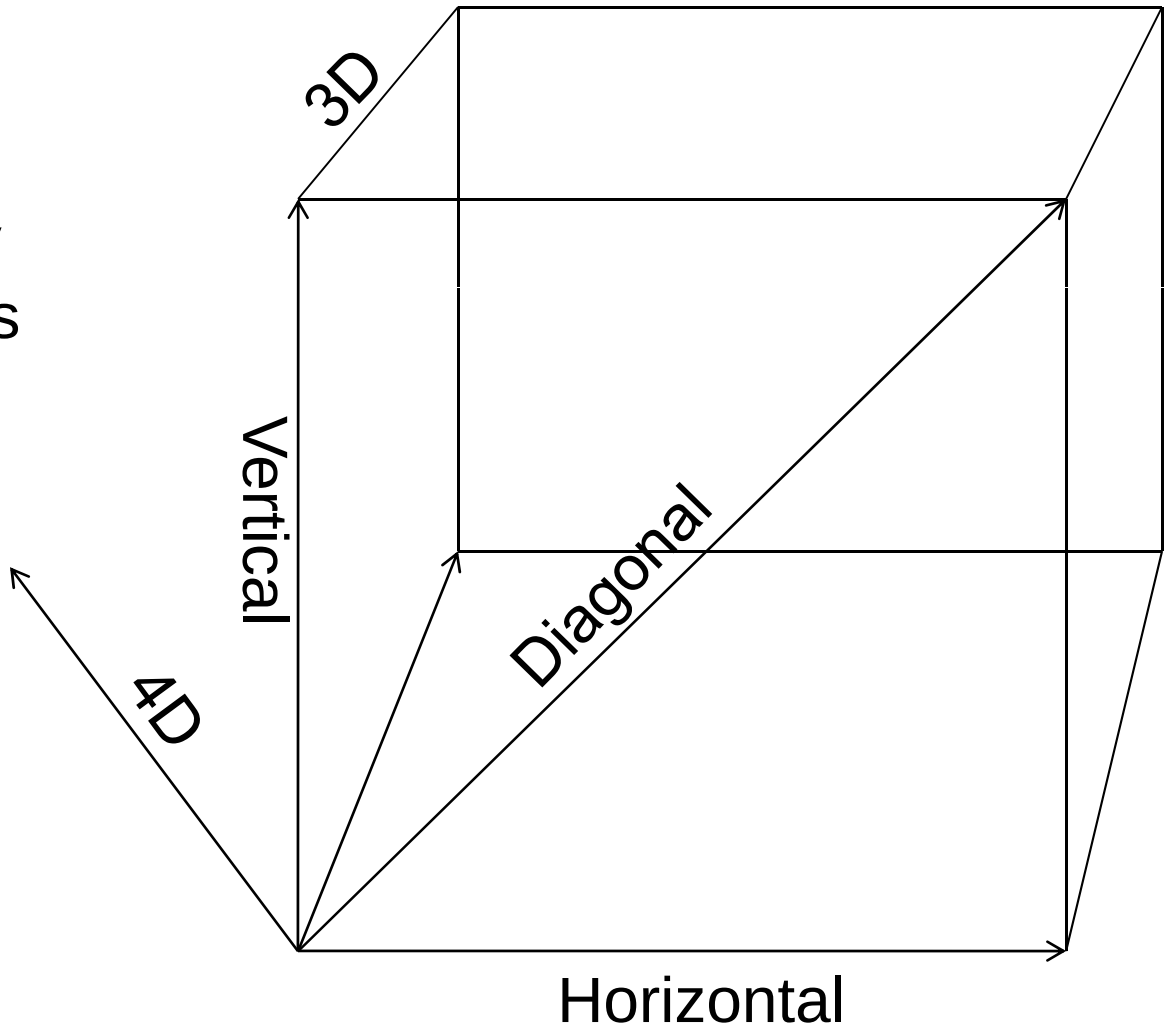

Admin Network?
Firewalls
Switches
Load Balancers
WAFs
Web Server
Auth/Auth
Application
DB
Logging
File System
OS
Ingress/egress?
SSL Termination?
Inline?
DoS?
Brute Force?
Backups?

"No, okay, wait, we wont host our own stuff after all. Our hosting provider will handle security for us. Do we <u>really</u> need to worry at that point?"

Answer: Yes – brute force alone is reason enough to worry.

- Vertical = many passwords & 1 username
- Horizontal = many usernames & 1 pass
- Diagonal = many usernames & passwords
- 3D = Many IPs
- 4D = Over long period of time
- Credential

- Solutions?



"This sounds hard. Can't we just offload this whole thing to the cloud? Everyone has this problem. Surely 'the cloud' is up to speed on security."

Answer: No. Most likely they're just as bad as you are & actually add even more attack points.

Please assess “mysite.com”

http://www.mysite.com

https://admin.mysite.com

http://mysite.akadns.net

http://mobile.mysite.com

http://mysite-api.partner.com

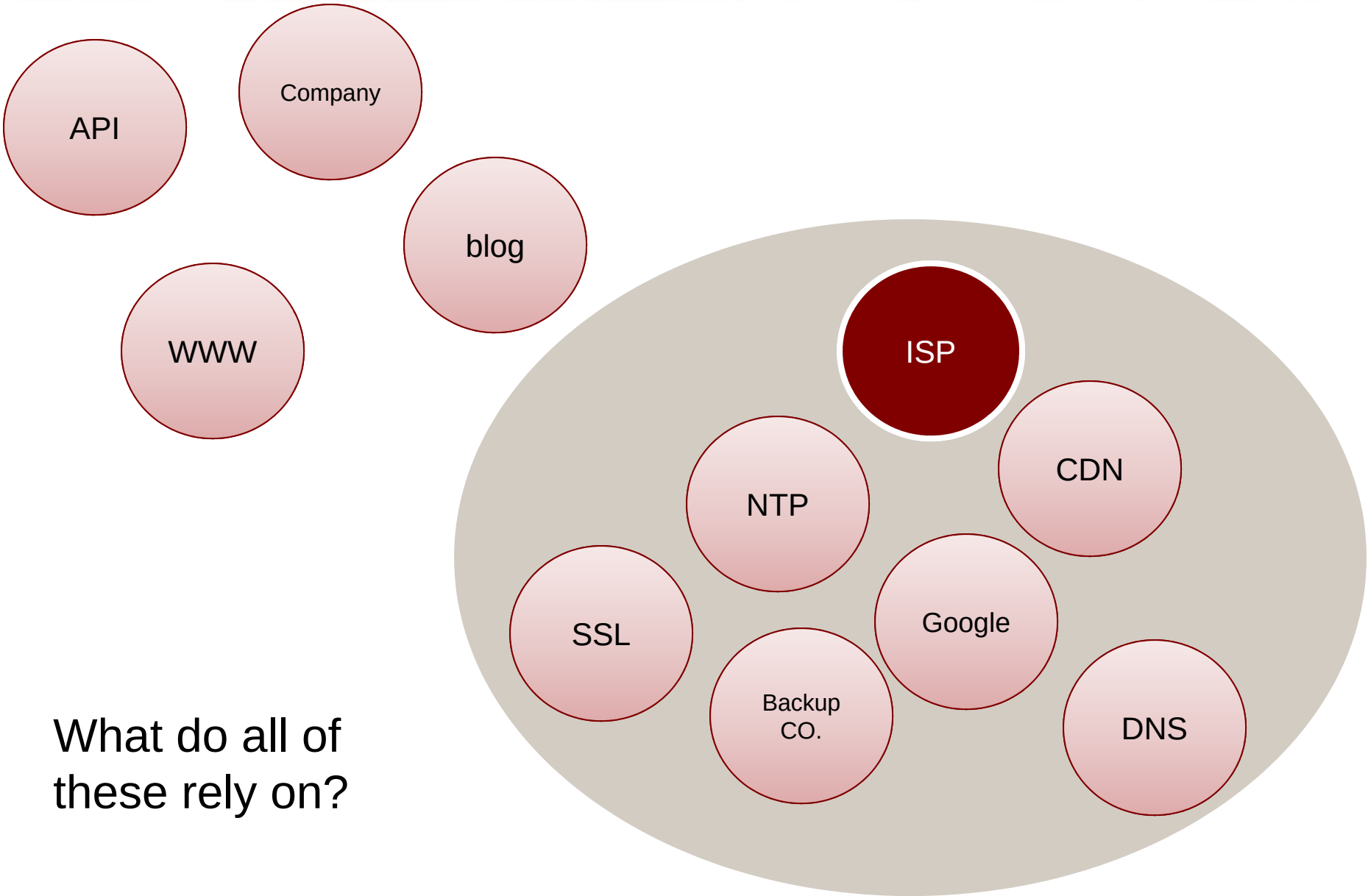
http://marcom-mysite.provider.com

http://www.google.com

dns1-mysite.provider.com

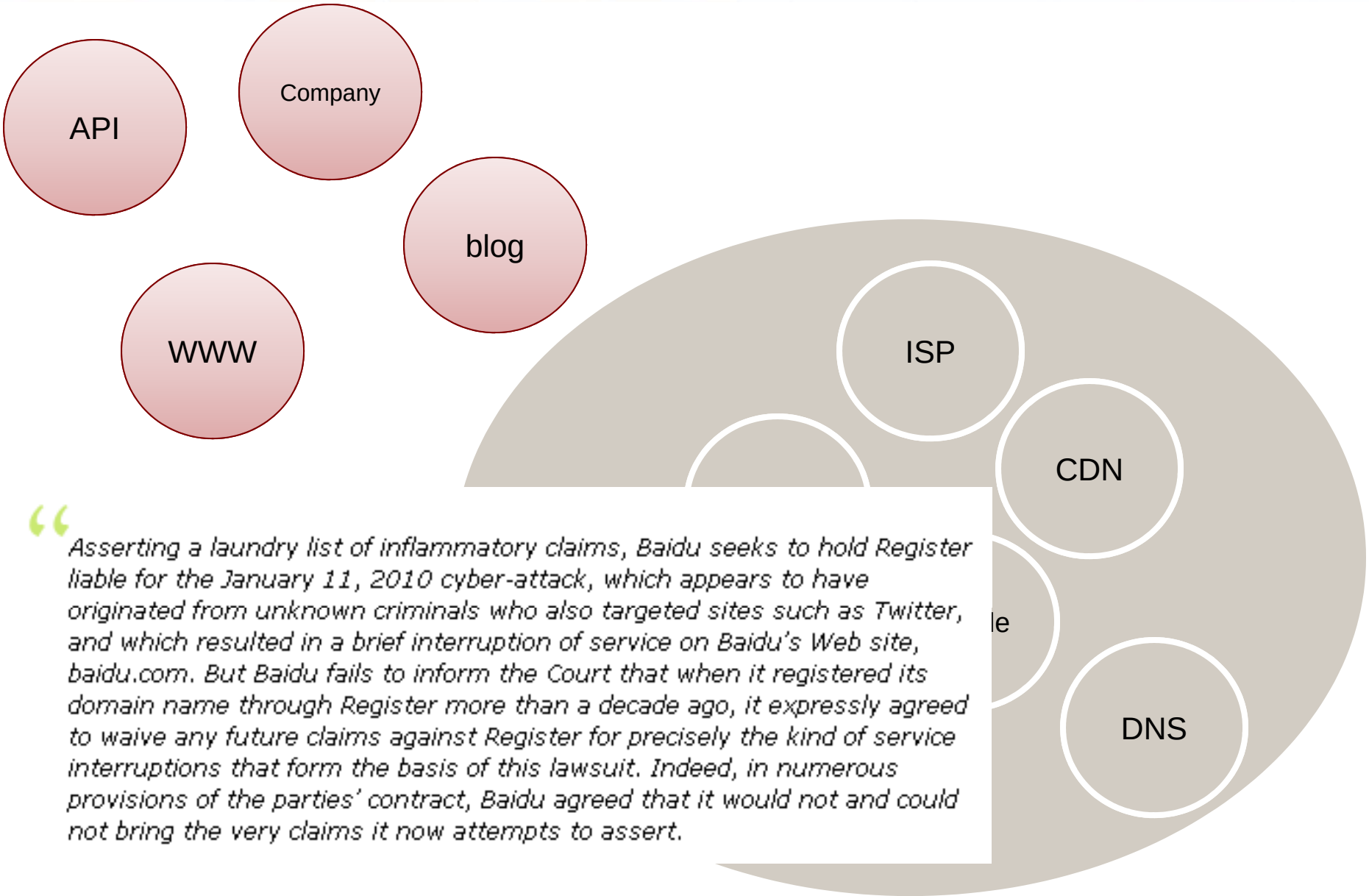
http://64.136.24.162/ (www.mysite.com)

Virtual hosts? Eg: http://www.yoursite.com



What do all of these rely on?

EMERGING THREATS ADAPTIVE SECURITY STRATEGIES TO RESPOND TO EVOLVING THREATS



> *Asserting a laundry list of inflammatory claims, Baidu seeks to hold Register liable for the January 11, 2010 cyber-attack, which appears to have originated from unknown criminals who also targeted sites such as Twitter, and which resulted in a brief interruption of service on Baidu's Web site, baidu.com. But Baidu fails to inform the Court that when it registered its domain name through Register more than a decade ago, it expressly agreed to waive any future claims against Register for precisely the kind of service interruptions that form the basis of this lawsuit. Indeed, in numerous provisions of the parties' contract, Baidu agreed that it would not and could not bring the very claims it now attempts to assert.*

"We use XYZ port scanner. We already know what we're running. Running it again is pointless. What can you tell me that I don't already know?"

Answer: There's a good chance you have no idea what you're really running.

	Try 1	Try 2	Try 3	Average	Total Missed Open-Ports	Total Missed Hosts	Total Packets Received by Filter
Unicornscan	323.119	328.559	330.116	327.265	0	0	25165794
Nmap	1750.187	1759.392	1760.001	1756.527	4	0	25166117
PortBunny	1705.272	1660.928	1735.395	1700.532	0	114	3812202

http://blog.robertlee.name/2008/01/port-scanner-challenge-revisited-nmap.html

EMERGING THREATS

ADAPTIVE SECURITY STRATEGIES TO RESPOND TO EVOLVING THREATS

Visible Externally

- API — 8181
- www — 443
- www — 81 - admin
- www — 80

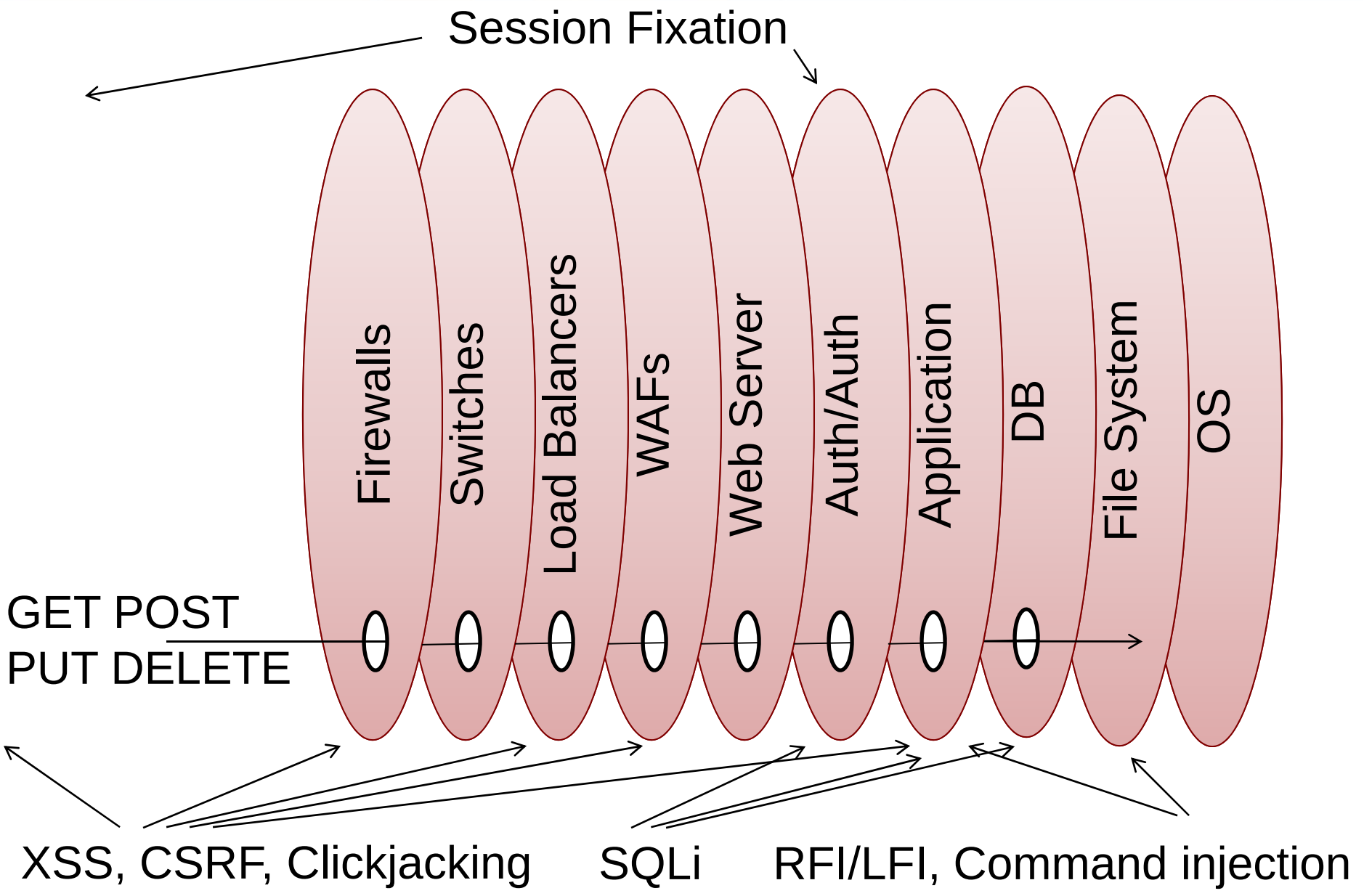
Invisible Externally

- FW/ Switch — 22, 23, 161, 443
- DB — 22, 1521
- www — 22
- www — 21

"But wait. We do IP based protections on our admin port because we're clever and awesome. How can you possibly get our IP? And forget about ARP spoofing."

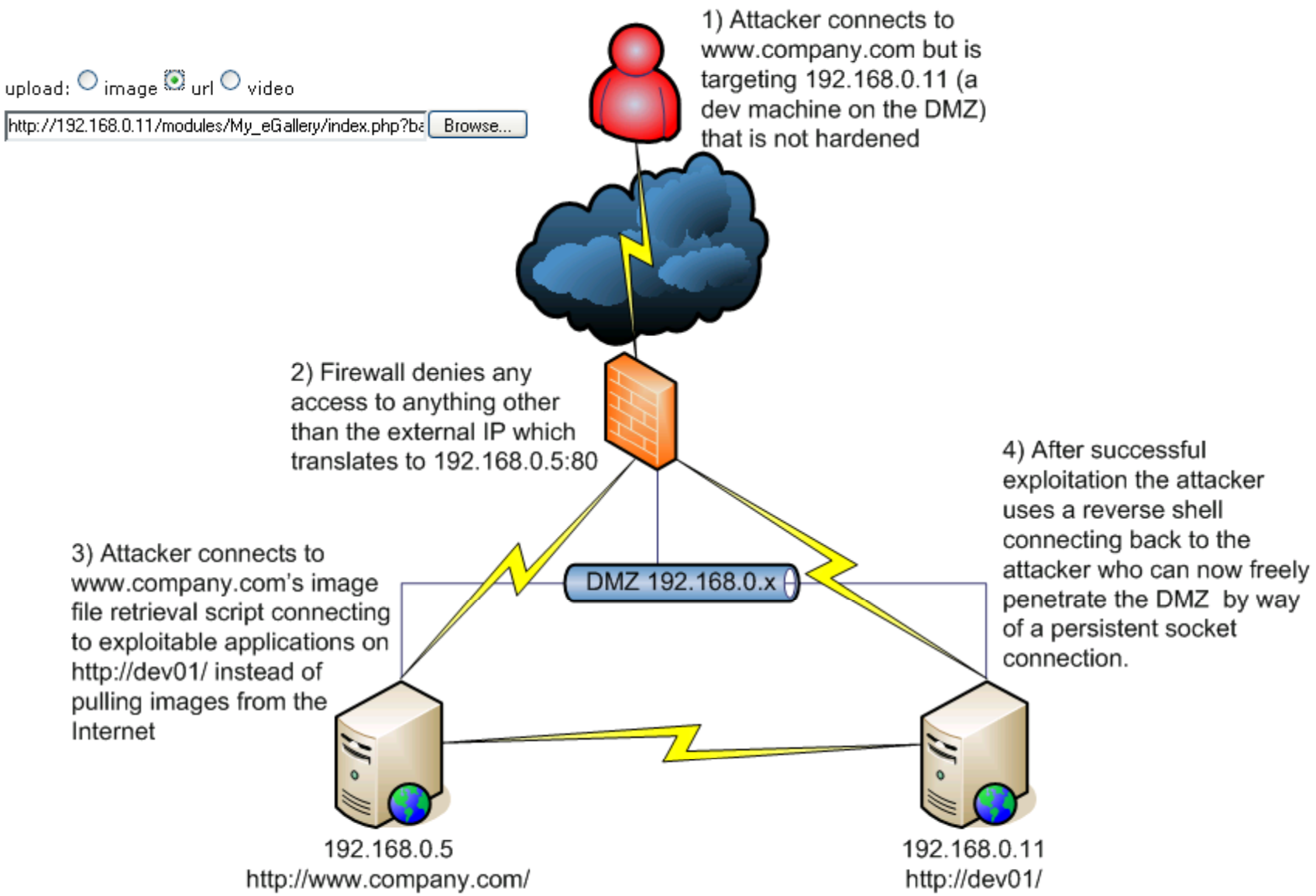
Answer: CSRF + DNS Rebinding, duh.

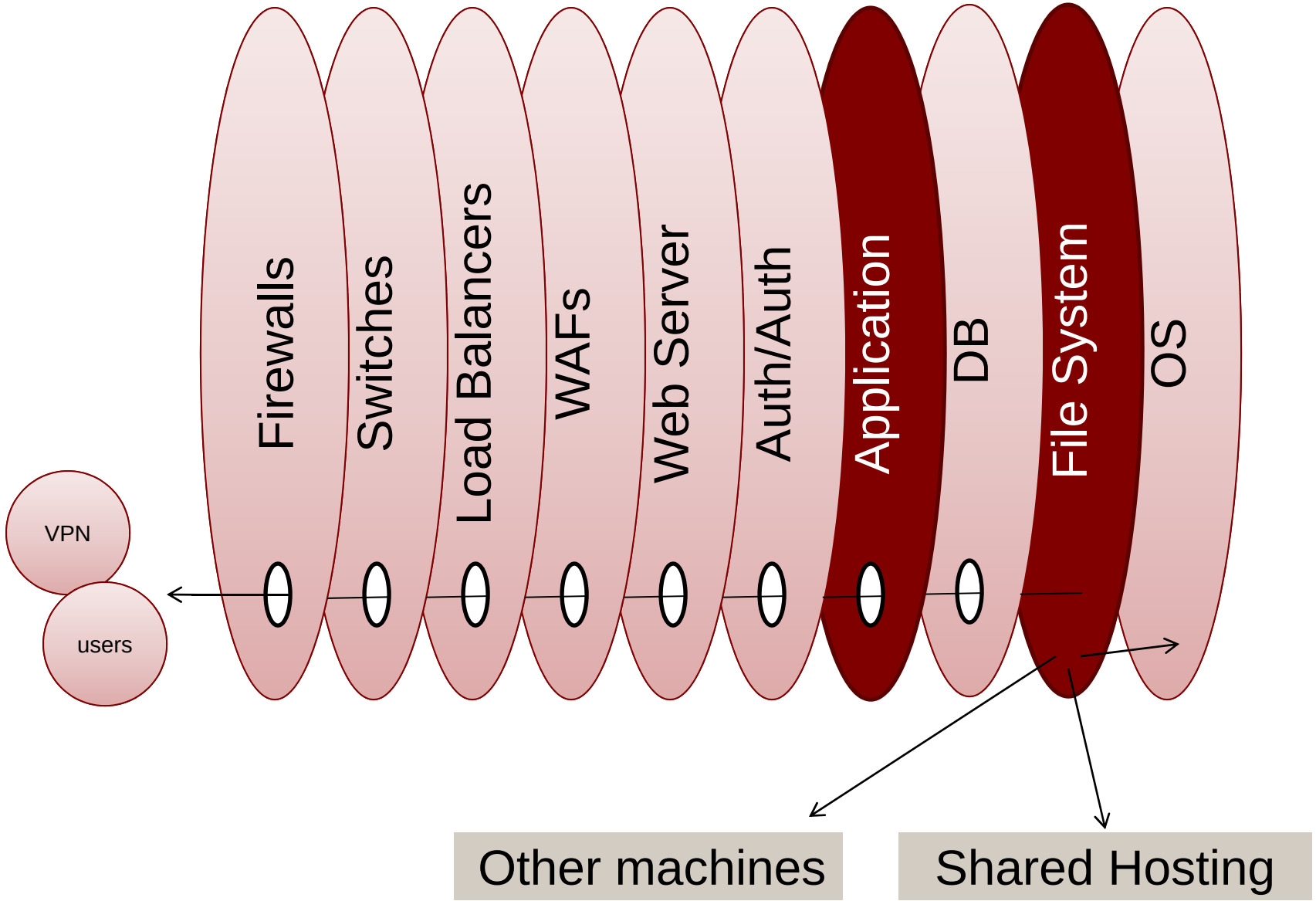
- Request www.site.com
- Responds with TTL (1 sec) and IP
- Browser requests content from IP
- Site responds with JS saying connect back to me in 2 sec.
- Site firewalls off browser
- Browser re-requests DNS
- DNS responds with intranet.
- Browser connects to intranet
- Browser can send data back out to the internet.
- Rebinding sends wrong host header or correct cookies


Session Fixation
Firewalls
Switches
Load Balancers
WAFs
Web Server
Auth/Auth
Application
DB
File System
OS
GET POST
PUT DELETE
XSS, CSRF, Clickjacking
SQLi
RFI/LFI, Command injection

This doesn't take into account:

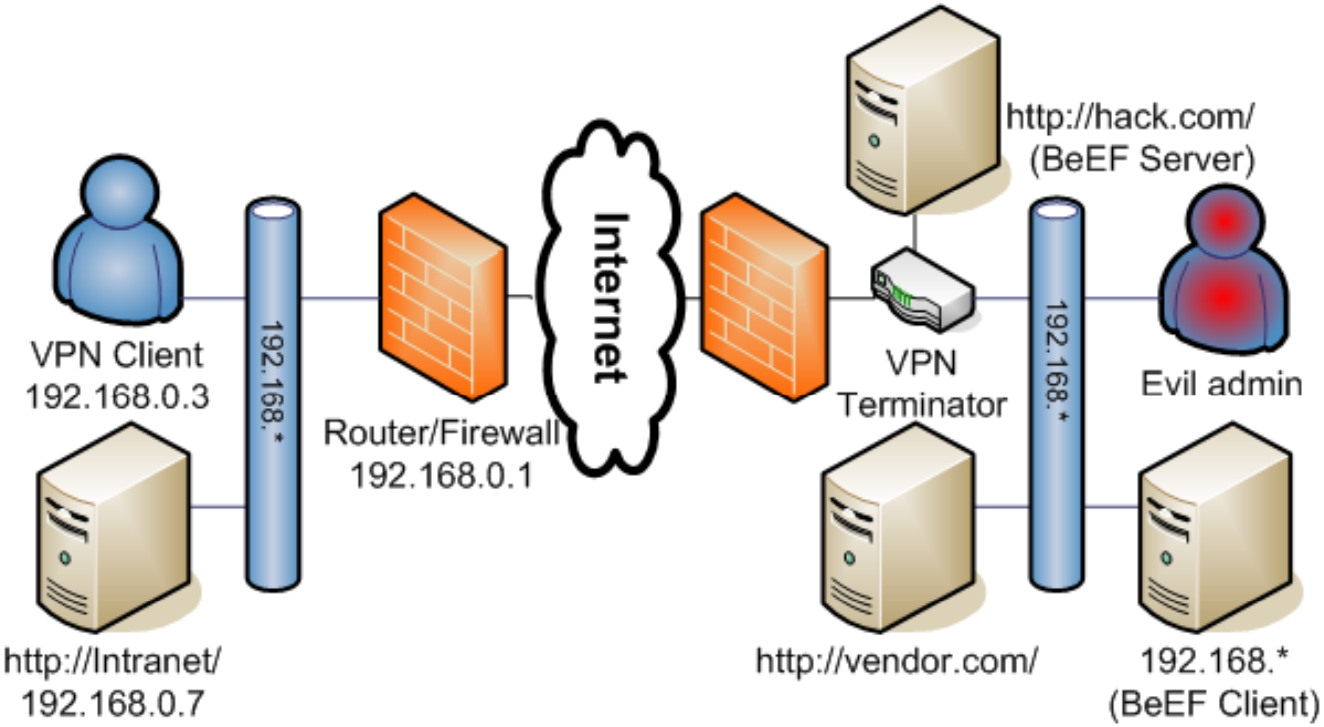
- Mail issues (Apache.org)
  - Phishing
  - Spear Phishing
- MITM
- Fraud
  - User Community
  - Logic flaws
  - Read "**Detecting Malice**"
- Etc… Etc…


upload: image url video
http://192.168.0.11/modules/My_eGallery/index.php?ba
Browse...
1) Attacker connects to www.company.com but is targeting 192.168.0.11 (a dev machine on the DMZ) that is not hardened
2) Firewall denies any access to anything other than the external IP which translates to 192.168.0.5:80
3) Attacker connects to www.company.com's image file retrieval script connecting to exploitable applications on http://dev01/ instead of pulling images from the Internet
DMZ 192.168.0.x
4) After successful exploitation the attacker uses a reverse shell connecting back to the attacker who can now freely penetrate the DMZ by way of a persistent socket connection.
192.168.0.5
http://www.company.com/
192.168.0.11
http://dev01/


Firewalls
Switches
Load Balancers
WAFs
Web Server
Auth/Auth
Application
DB
File System
OS
VPN
users
Other machines
Shared Hosting

"You can't hack our main site, that's just our blog/forum/dev environment/vendor/something we can pretend isn't a big deal. Who cares about that?"

Answer: If you ignore the fact that the passwords are probably the same, and cookies may be shared, RFC1918 Cache Poisoning



Step 1) Attacker does DNS recon and finds intranet server is called http://Intranet/
Step 2) User visits http://Intranet/ (DNS pinning occurs in the user's browser)
Step 3) User instantiates client VPN to Vendor's network
Step 4) Evil admin pushes all RFC1918 routes to connect to his own network
Step 5) User connects to http://vendor.com/ and renders an iframe to http://Intranet/
Step 6) User connects to evil network instead of the real Intranet page (also giving attacker access to the user's cookies)
Step 7) Evil admin delivers a BeEF client payload and requests that the user reconnect to the same page in several seconds.
Step 8) Evil admin turns off the VPN client forcing the routes to change back to their original settings (depending on the client).
Step 9) User connects to http://Intranet/ within his own network, but now under the control of the BeEF client payload.
Step 10) The BeEF client payload request C&C instructions from http://hack.com
Step 11) Upon successful connection of the BeEF client to the BeEF server the Evil Admin allows the user to reconnect to the VPN, but pushes only necessary routes.

"I wasn't paying attention. What should I have learned?"

- Everything is in scope (in a *real* pen-test)
  - Don't assume anyone is better at security (they aren't)
- Assume you'll get hacked and then protect from that
  - Browsers, networks, applications, DBs, etc…
  - Learn these two words, "least privilege"
- Check and sanitize input and output before use
- Forklift upgrades are expensive! Build it right first – it's cheaper! It's also more stable!
- You're insecure. ☹ Now, go find yourself a good architect.

Thank you!

- Robert Hansen
  - http://www.sectheory.com – the company
  - http://ha.ckers.org – the lab
  - http://sla.ckers.org – the forum
  - **Detecting Malice** – the eBook
  - **XSS Exploits** – the book
  - robert@sectheory.com – the email