TTL of a Penetration

Branson Matheson
sandinak [at] sandsite.org

Coming Up Next!

Coming Up Next!

- Who am I
- Us vs Them
- Anatomy of a penetration, Parts 1, 2 and 3
- Minimizing Impacts
- Q&A

Who is sandinak

Who is sandinak

- 24 Year Veteran of Information Technology
  - Naval Cryptologist
  - Network and System Administrator
  - Security and Systems Architect
  - Business Owner
  - Hacker of many hats
  - Technology Enthusiast

Who is sand
Technology Enthusiast

Who is sand
Technology Enthusiast

- Love to tinker and see how things work
- Love to push the mold
- Apply “Critical Thinking” to every day processes.
- “Tell me you can’t get X to work with Y, and I bet I can find a way”.

Who Are You?

Geeks?

System Administrators?

Network Administrators?

Security Administrators?

Hackers?

White Hat Hackers?

White Hat Hackers?

(c) 2012 sandSecurity

Black Hat Hackers?

(c) 2012 sandSecurity

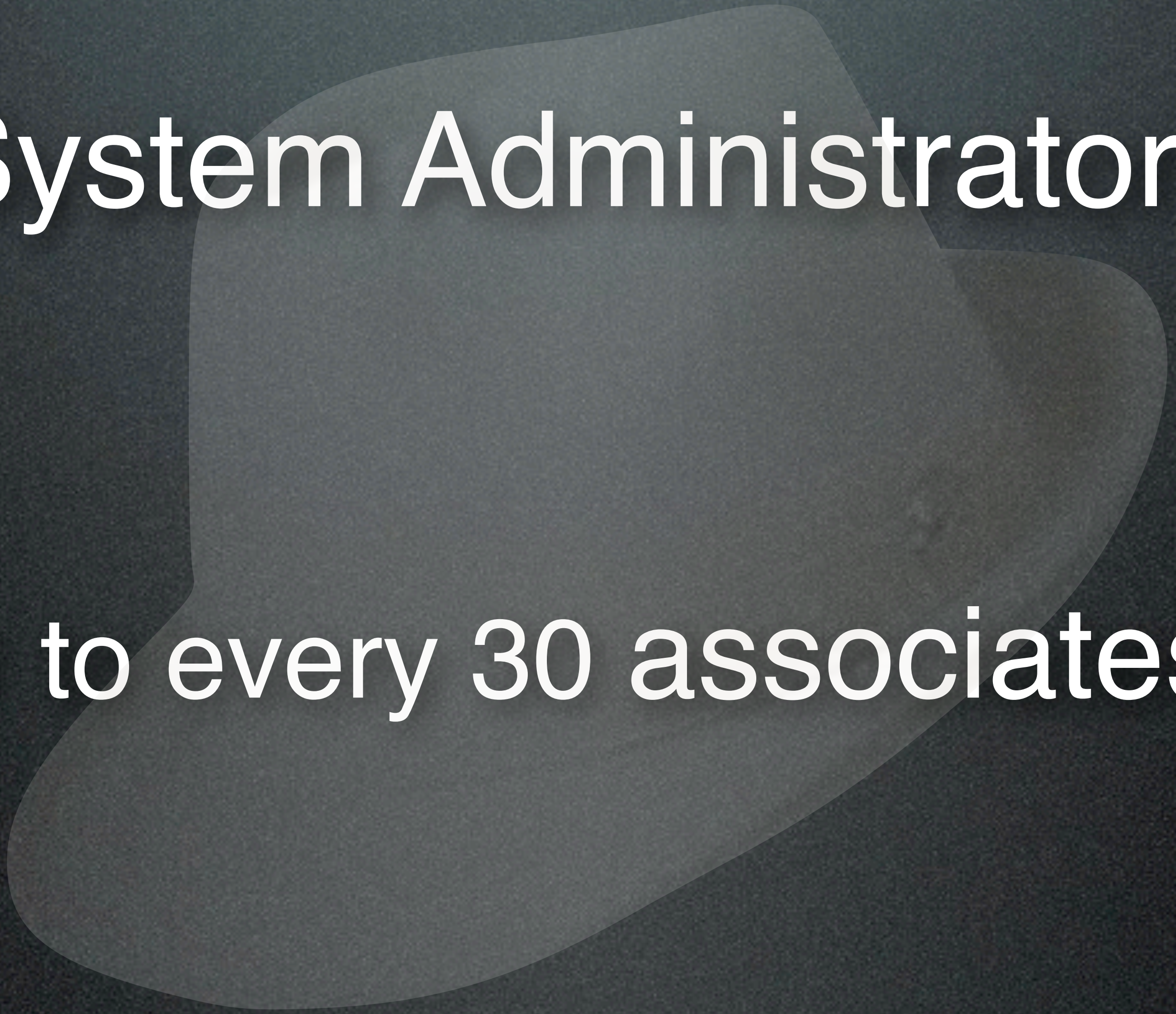
Lets look at some statistics...

“White Hats first”

“White Hats”

(c) 2012 sandSecurity

“White Hats”



System Administrators

1 to every 30 associates

“White Hats”

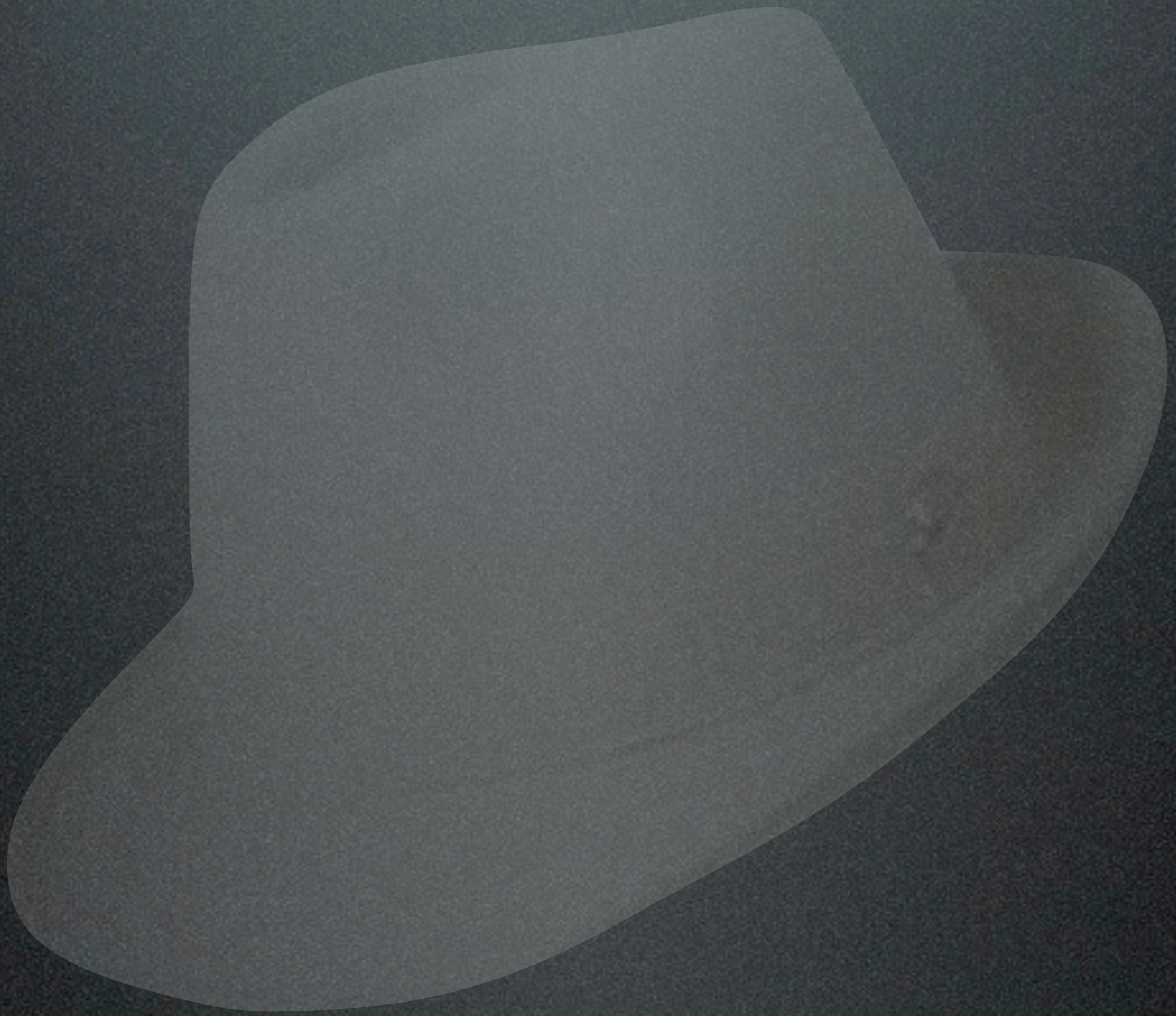
(c) 2012 sandSecurity

“White Hats”

Network Administrators

1 to every 200 associates

“White Hats”



(c) 2012 sandSecurity

“White Hats”

Security Administrators

1 to every 1200 associates

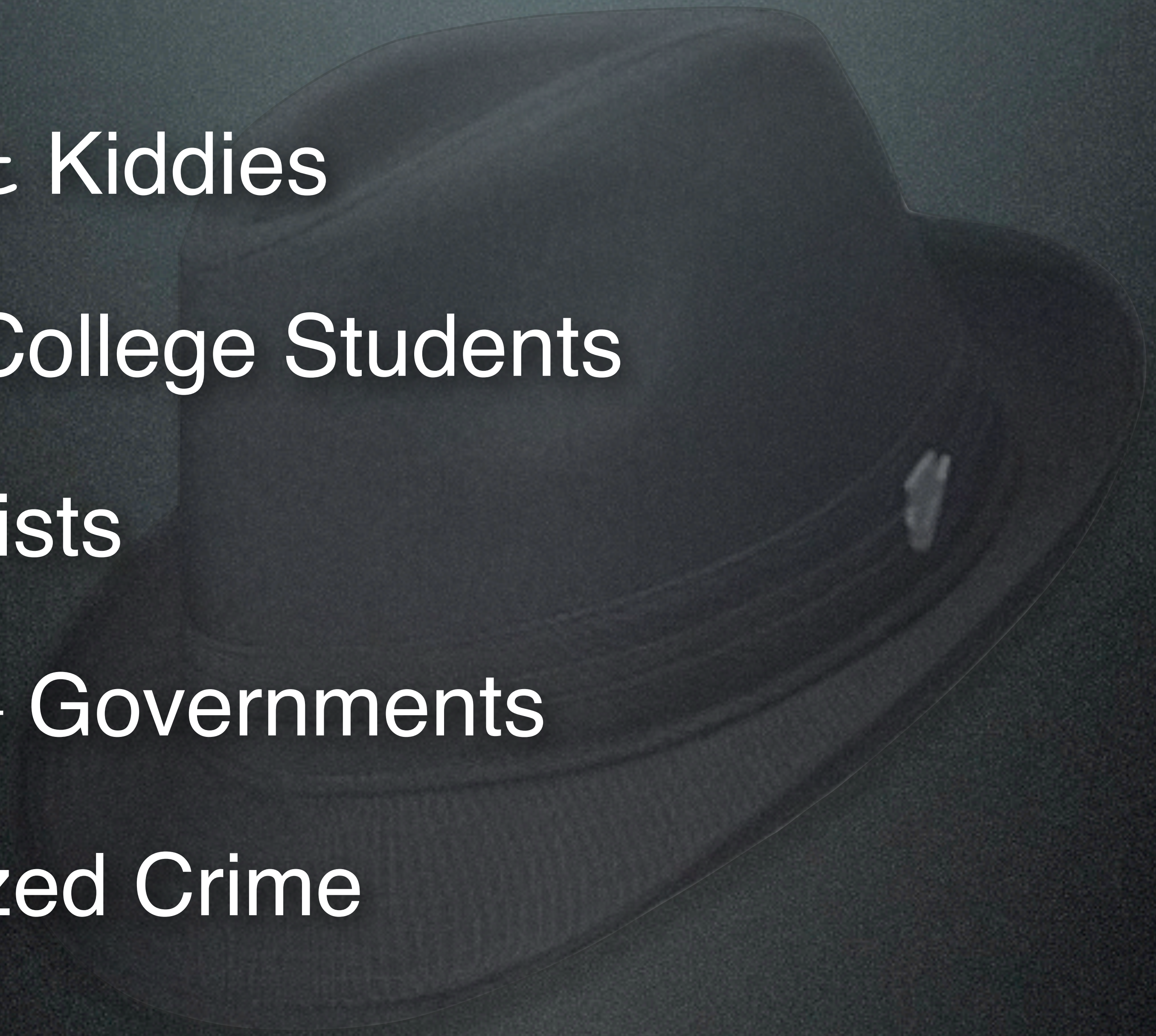
Who are ‘They’

Who are ‘They’

(c) 2012 sandSecurity

Who are ‘They’

Who are ‘They’



- `Skr1pt` Kiddies
- Bored College Students
- Hacktivists
- ~~Foreign~~ Governments
- Organized Crime

Who are ‘They’

- More of them than us… ?

VS

?

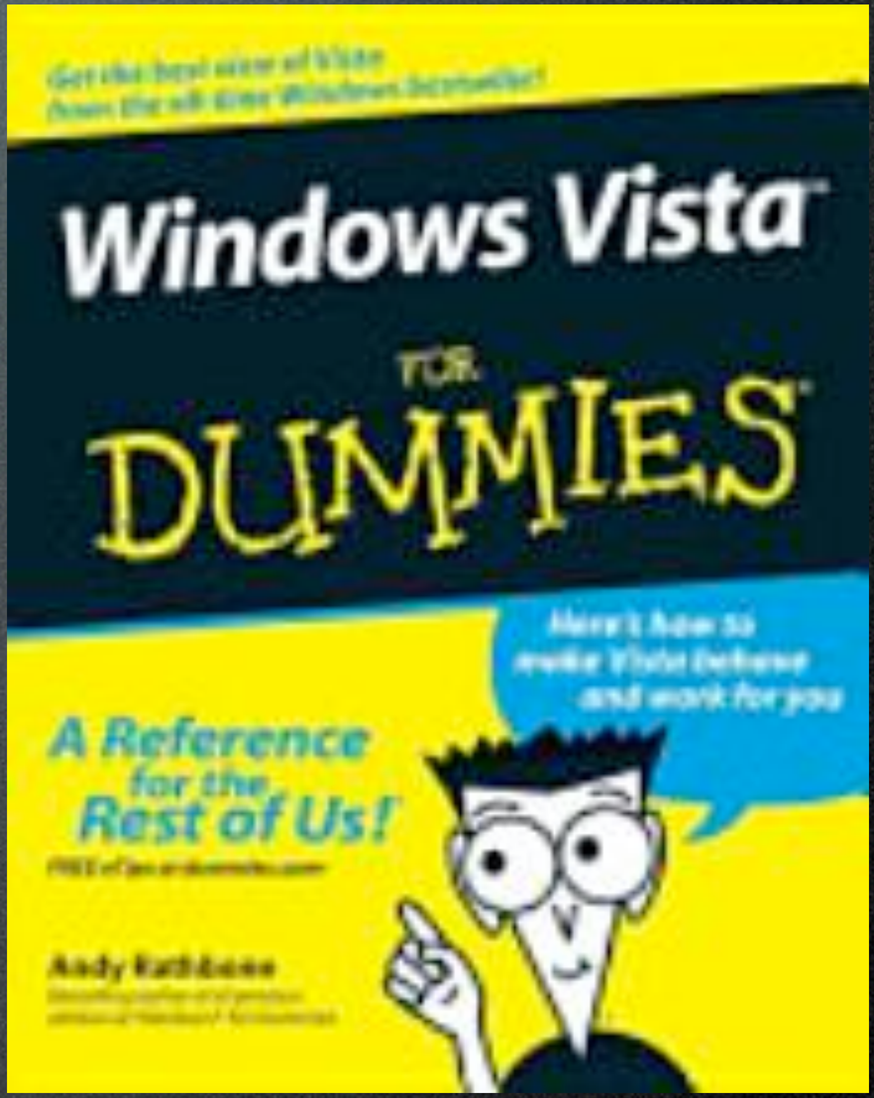
Who are ‘They’

Nope

VS

Who are ‘They’

Well...


Get the best view of Vista from the all-time Windows bestseller!
Windows Vista
FOR DUMMIES
Here's how to make Vista behave and work for you
A Reference for the Rest of Us!
Andy Rathbone

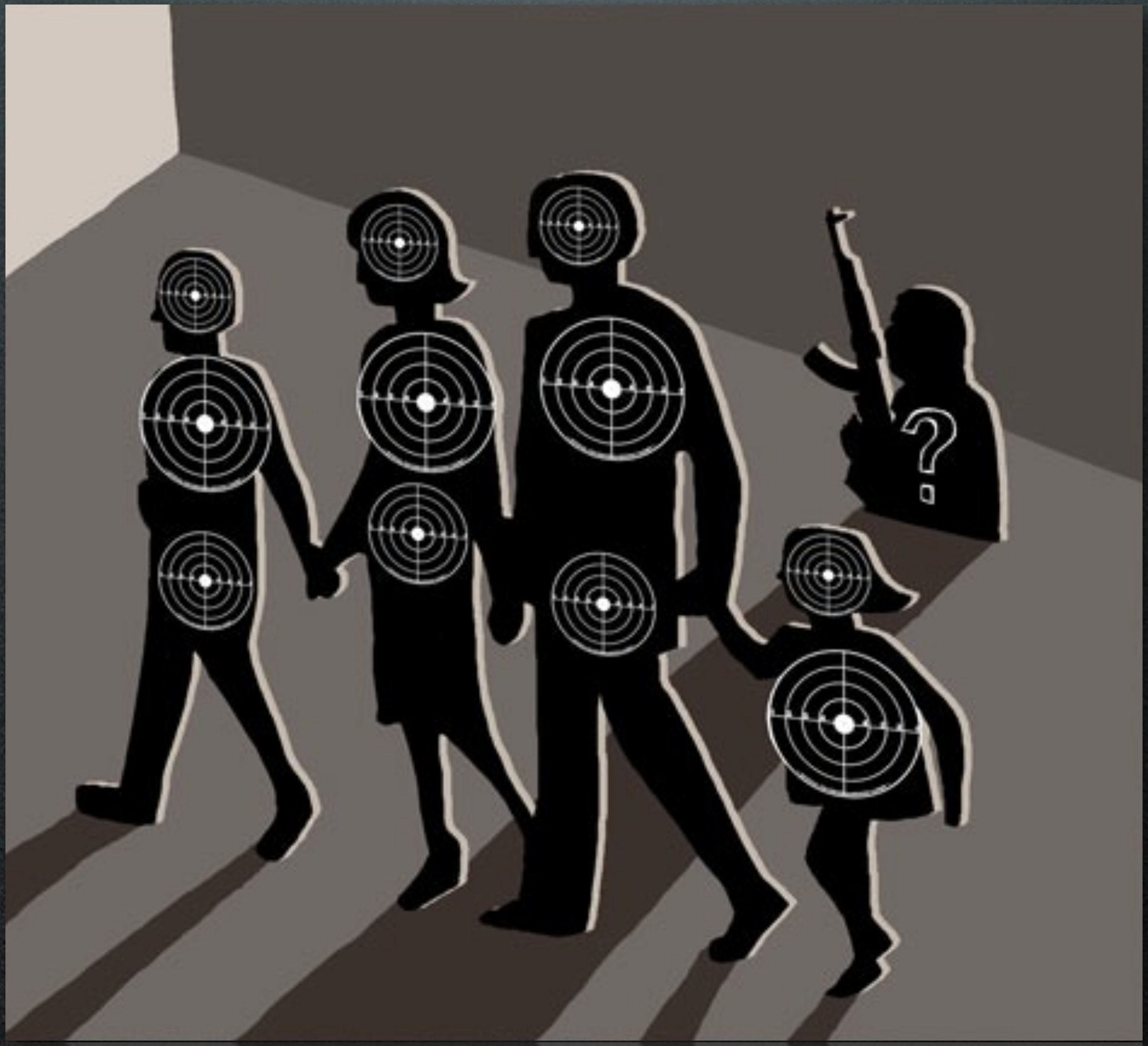
vs

vs

But…We’re Ahead Right??

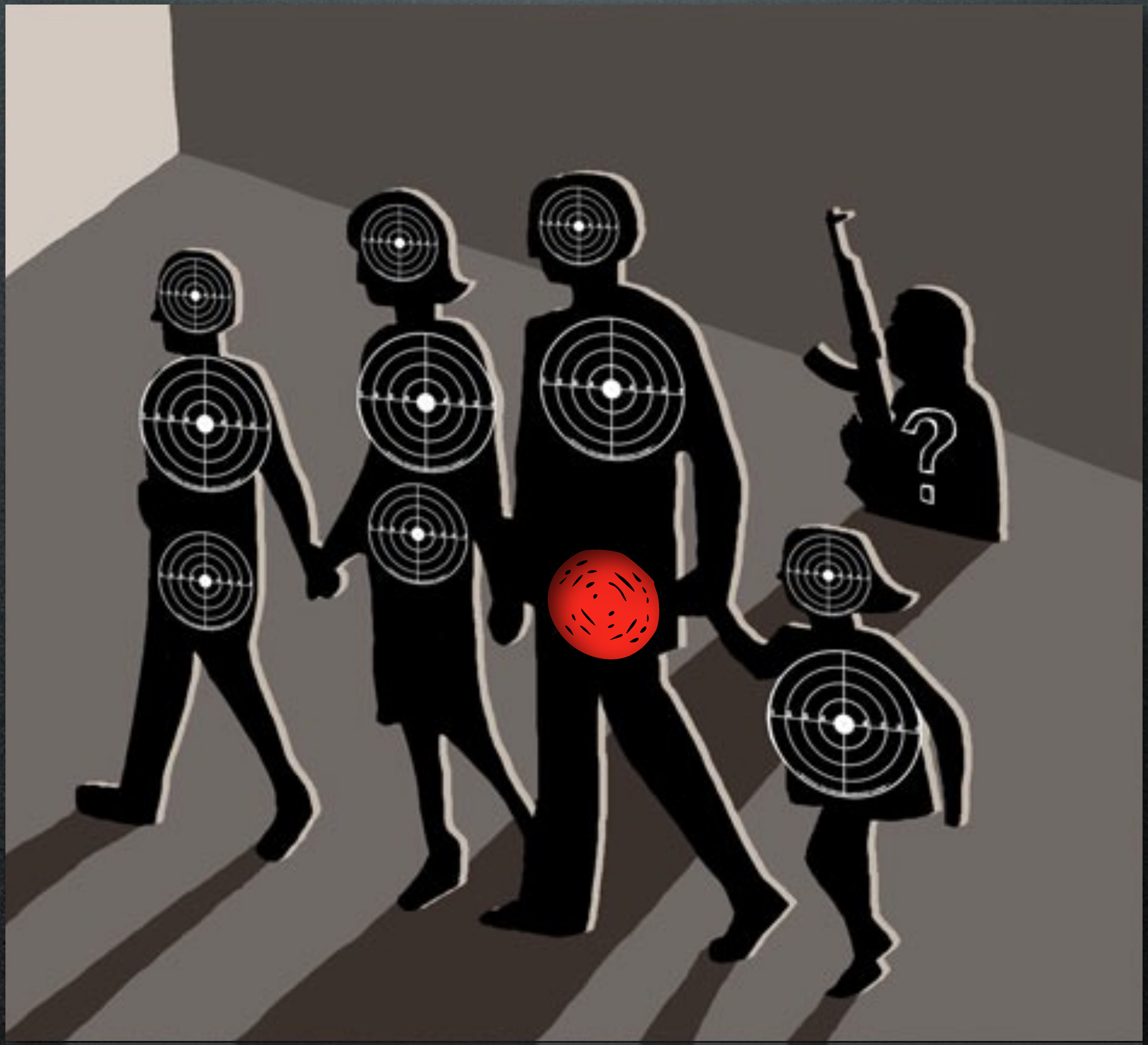
Nope!

Target Rich Environment



(c) 2012 sandSecurity

Target Rich Environment



What do you protect?

What do you protect?

What do you protect?

Network connections..

What do you protect?

[1]

[1] "IEEE Std 802-2001". IEEE. 2002-02-07. p. 19. Retrieved 2011-03-06. "The universal administration of LAN MAC addresses began with the Xerox Corporation administering Block Identifiers (Block IDs) for Ethernet addresses."

What do you protect?

Media Access Control (MAC)Addresses

48-bit MAC-address space contains potentially 281,474,976,710,656 possible addresses.[1]

(not out until 2100)

[1] "IEEE Std 802-2001". IEEE. 2002-02-07. p. 19. Retrieved 2011-03-06. "The universal administration of LAN MAC addresses began with the Xerox Corporation administering Block Identifiers (Block IDs) for Ethernet addresses."

What do you protect?

What do you protect?

IPv4 Addresses

255^4 = 4228250625

addresses available

(we’re out .. ish ... now ... ish ...)

What do you protect?

IPv6 Addresses

IPv6 uses six 128-bit addresses, for an address space of approximately 340 undecillion or 3.4×10^{38} addresses. [1]

[1] http://en.wikipedia.org/wiki/IPv6

What do you protect?

What do you protect?

Nodes...

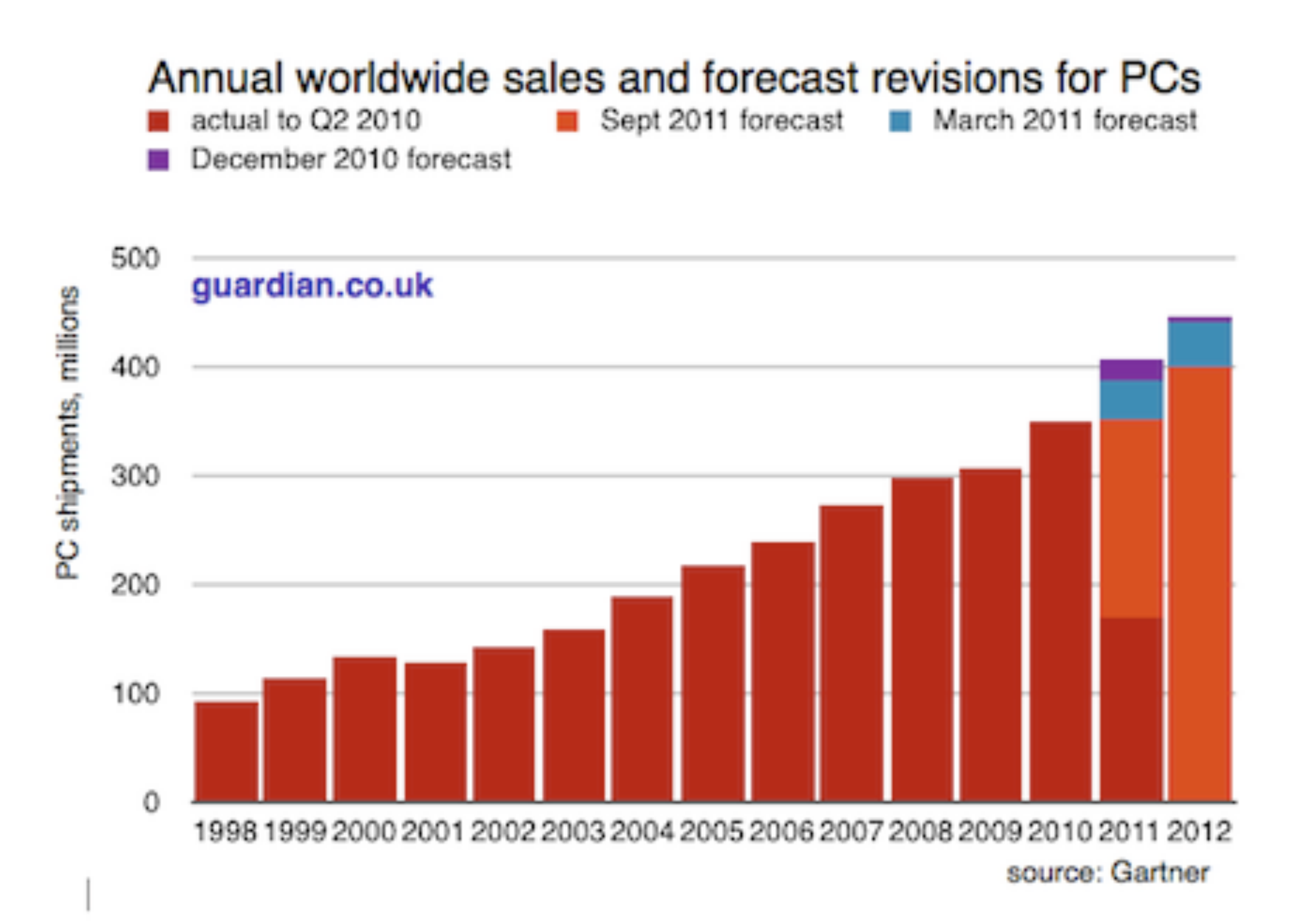
What do you protect?

What do you protect?

- More than 80% of households have least 1 computer on average in USA (195 million)[1]..
- this discounts cell phones, tablets, and other portable devices.

[1] 2006 - http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/overview-of-home-internet-access-in-the-us-jan-6.pdf

What do you protect?



source: Gartner

What do you protect?

What do you protect?

Software...

What do you protect?

What do you protect?

Parallels
Sun VirtualBox
AIX
maemo.org
iOS
symbian OS
hp
redhat
solaris
CentOS

at least ~40 different OS's
(not including variants)

What do you protect?

SMB HTTP SMTP AFP FTP NFS Jabber IRC AIM
IMAP Finger POP LDAP

What do you protect?

Each system having many services

SMB HTTP SMTP AFP FTP NFS Jabber IRC AIM IMAP Finger POP LDAP

What do you protect?

What do you protect?

Each User has multiple local applications

What do you protect?

What do you protect?

Each User uses many web applications every day.

What do you protect?

What do you protect?

Users...

What do you protect?
Users...

At Work

Type of user	Count
Professional	52,163,000
Service	33,527,000
Total	**85,690,000**

http://www.bls.gov/news.release/empsit.t13.htm

What do you protect?
Users...

At Work

Type of user	Count
Professional	52,163,000
Service	33,527,000
Total	**85,690,000**

http://www.bls.gov/news.release/empsit.t13.htm

At Home

Type of user	Count
Broadband	69,902,289
Total	**239,893,600**

http://www.internetworldstats.com/am/us.htm

What do you protect?

Users...

What do you protect?
Users...

How’s the math workout?

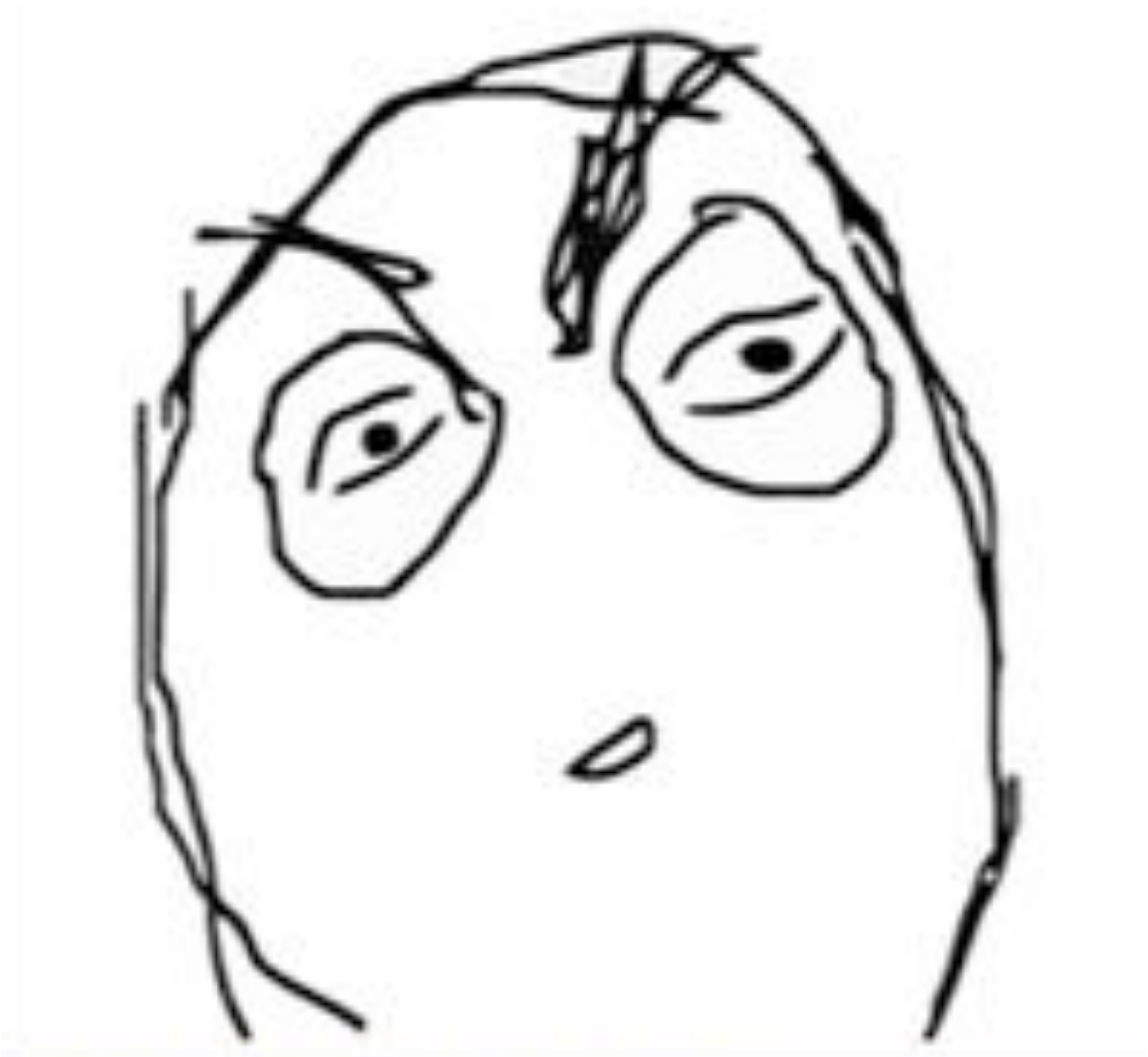
How’s the math workout?

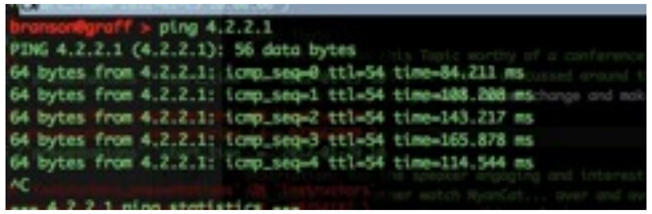
- No firm numbers on actual number of hackers *duh*
- No firm numbers on actual number of White Hats *more with the duh*
- Conservatively Estimating 1 million real hackers in the USA alone.
- 1:240 ratio

Pretty good eh?

But what is our life like?

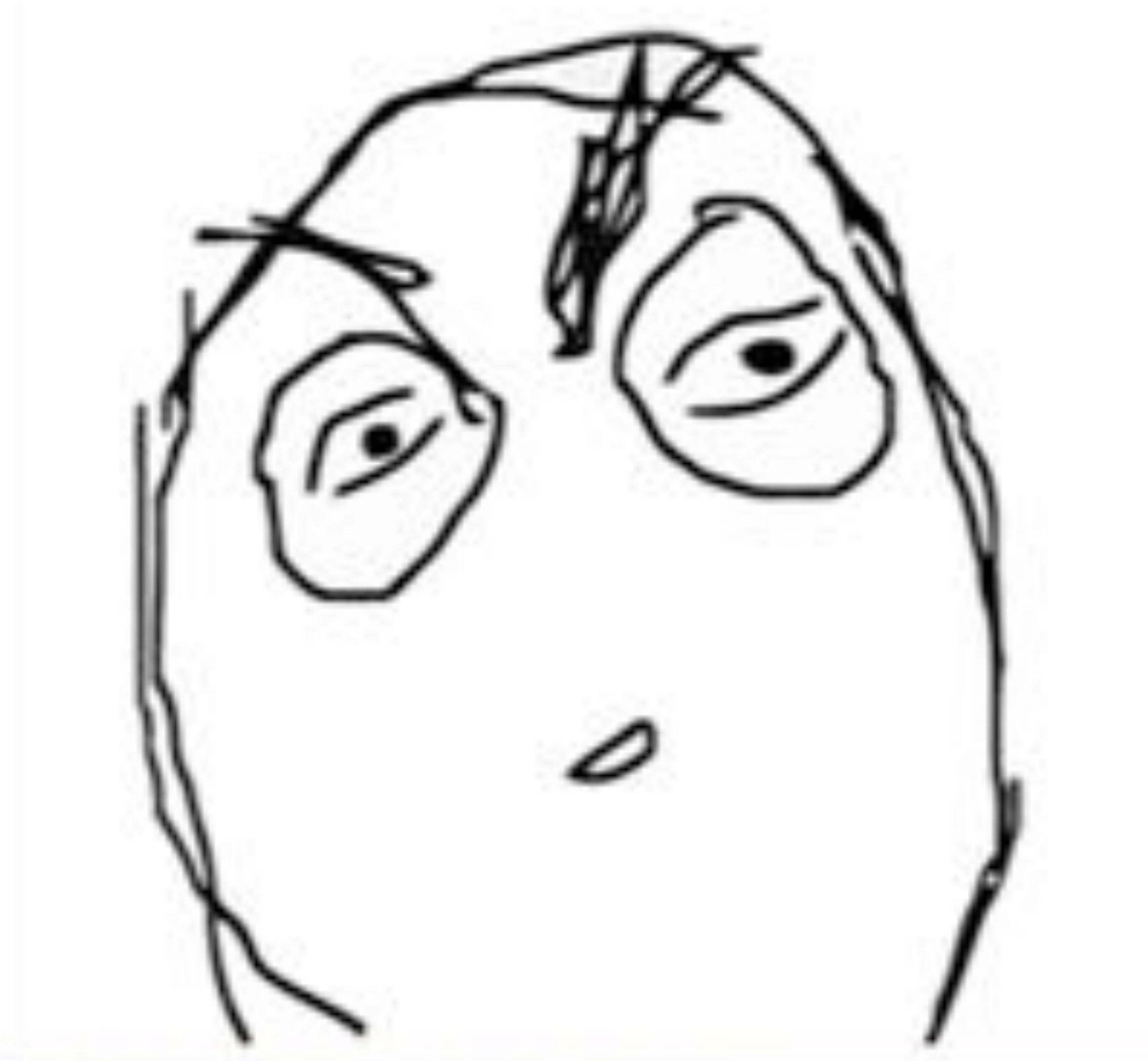
Hmmmm.....

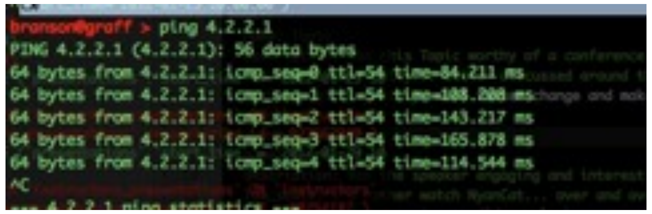




```
bronson@graff > ping 4.2.2.1
PING 4.2.2.1 (4.2.2.1): 56 data bytes
64 bytes from 4.2.2.1: icmp_seq=0 ttl=54 time=84.211 ms
64 bytes from 4.2.2.1: icmp_seq=1 ttl=54 time=108.208 ms
64 bytes from 4.2.2.1: icmp_seq=2 ttl=54 time=143.217 ms
64 bytes from 4.2.2.1: icmp_seq=3 ttl=54 time=165.878 ms
64 bytes from 4.2.2.1: icmp_seq=4 ttl=54 time=114.544 ms
^C
--- 4.2.2.1 ping statistics ---
```

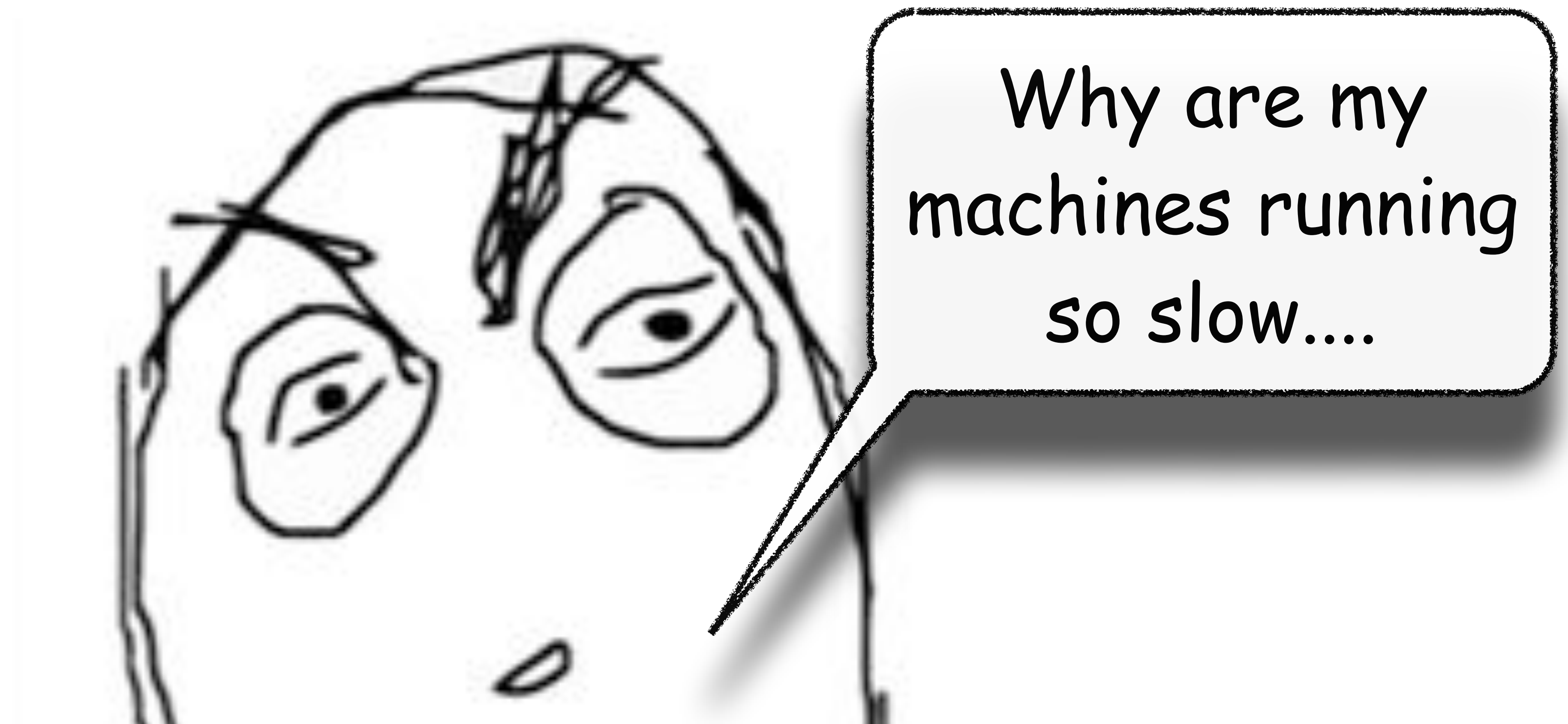
White Hat

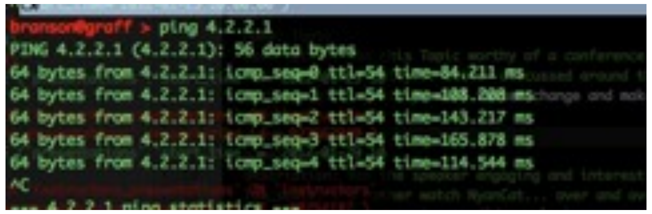




```
bronson@graff > ping 4.2.2.1
PING 4.2.2.1 (4.2.2.1): 56 data bytes
64 bytes from 4.2.2.1: icmp_seq=0 ttl=54 time=84.211 ms
64 bytes from 4.2.2.1: icmp_seq=1 ttl=54 time=108.208 ms
64 bytes from 4.2.2.1: icmp_seq=2 ttl=54 time=143.217 ms
64 bytes from 4.2.2.1: icmp_seq=3 ttl=54 time=165.878 ms
64 bytes from 4.2.2.1: icmp_seq=4 ttl=54 time=114.544 ms
^C
--- 4.2.2.1 ping statistics ---
```

White Hat

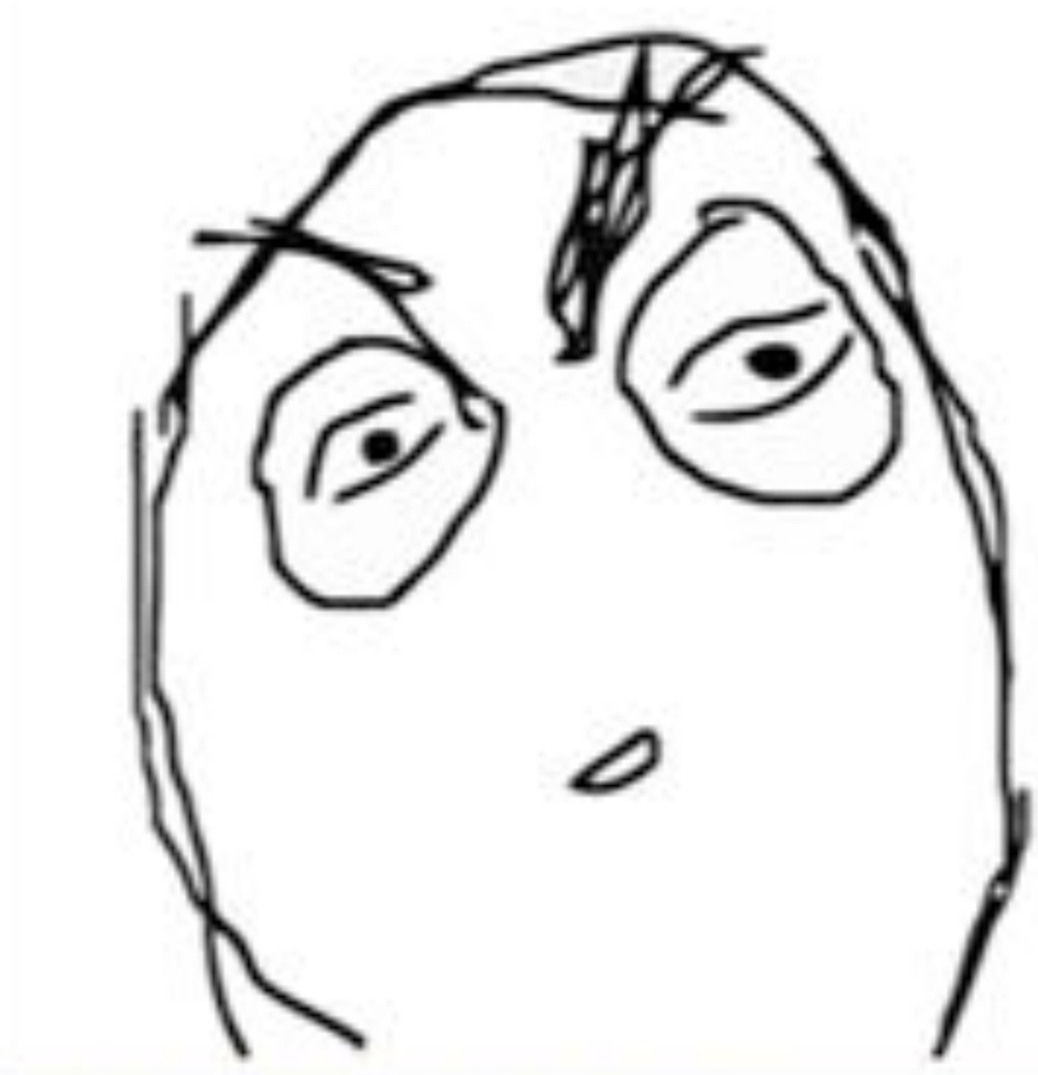


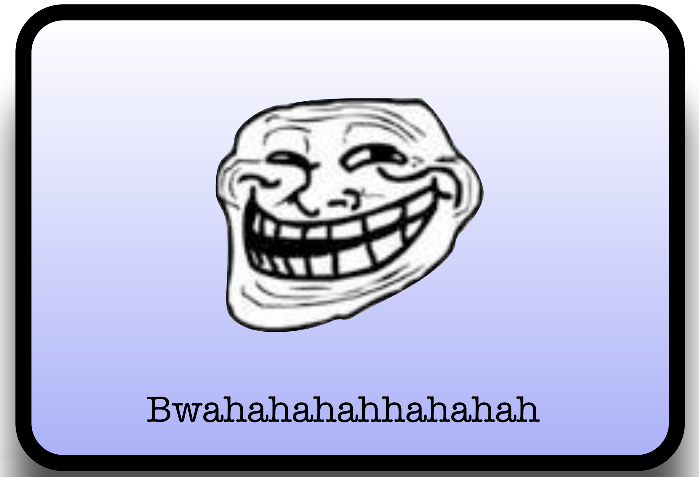


```
bronson@graff > ping 4.2.2.1
PING 4.2.2.1 (4.2.2.1): 56 data bytes
64 bytes from 4.2.2.1: icmp_seq=0 ttl=54 time=84.211 ms
64 bytes from 4.2.2.1: icmp_seq=1 ttl=54 time=108.208 ms
64 bytes from 4.2.2.1: icmp_seq=2 ttl=54 time=143.217 ms
64 bytes from 4.2.2.1: icmp_seq=3 ttl=54 time=165.878 ms
64 bytes from 4.2.2.1: icmp_seq=4 ttl=54 time=114.544 ms
^C
--- 4.2.2.1 ping statistics ---
```

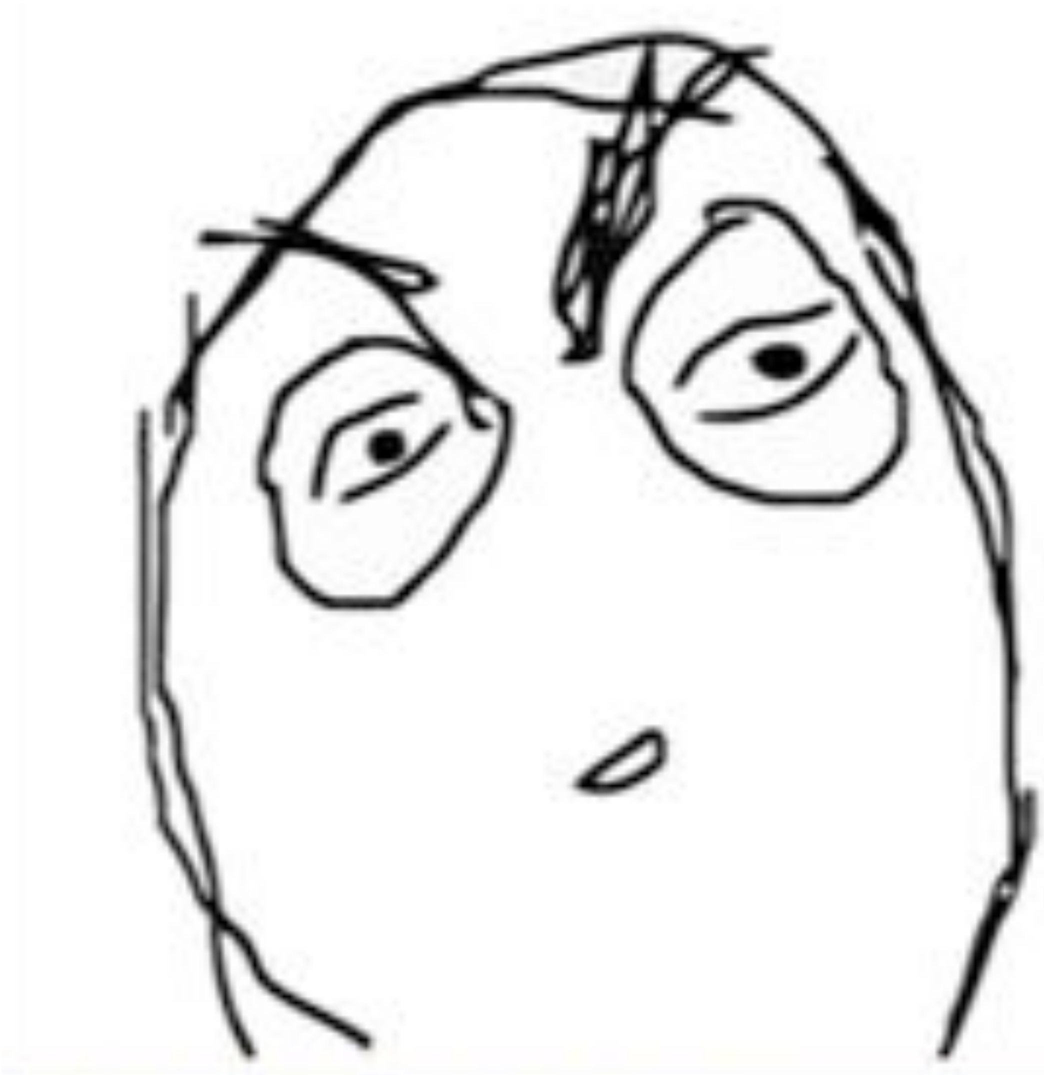
White Hat

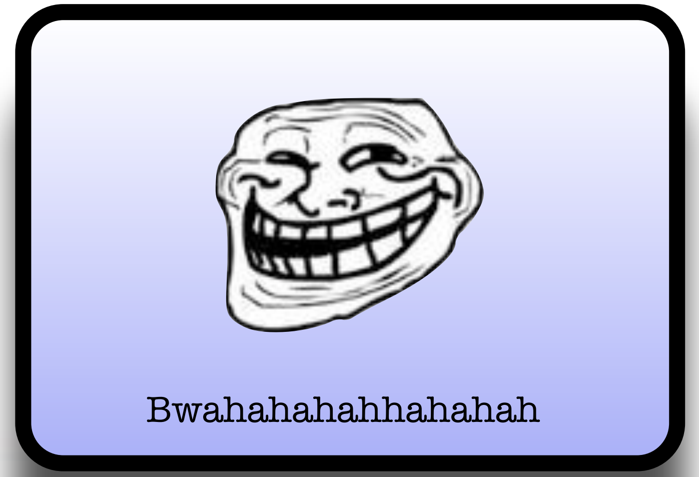
Hmmmm.....





White Hat



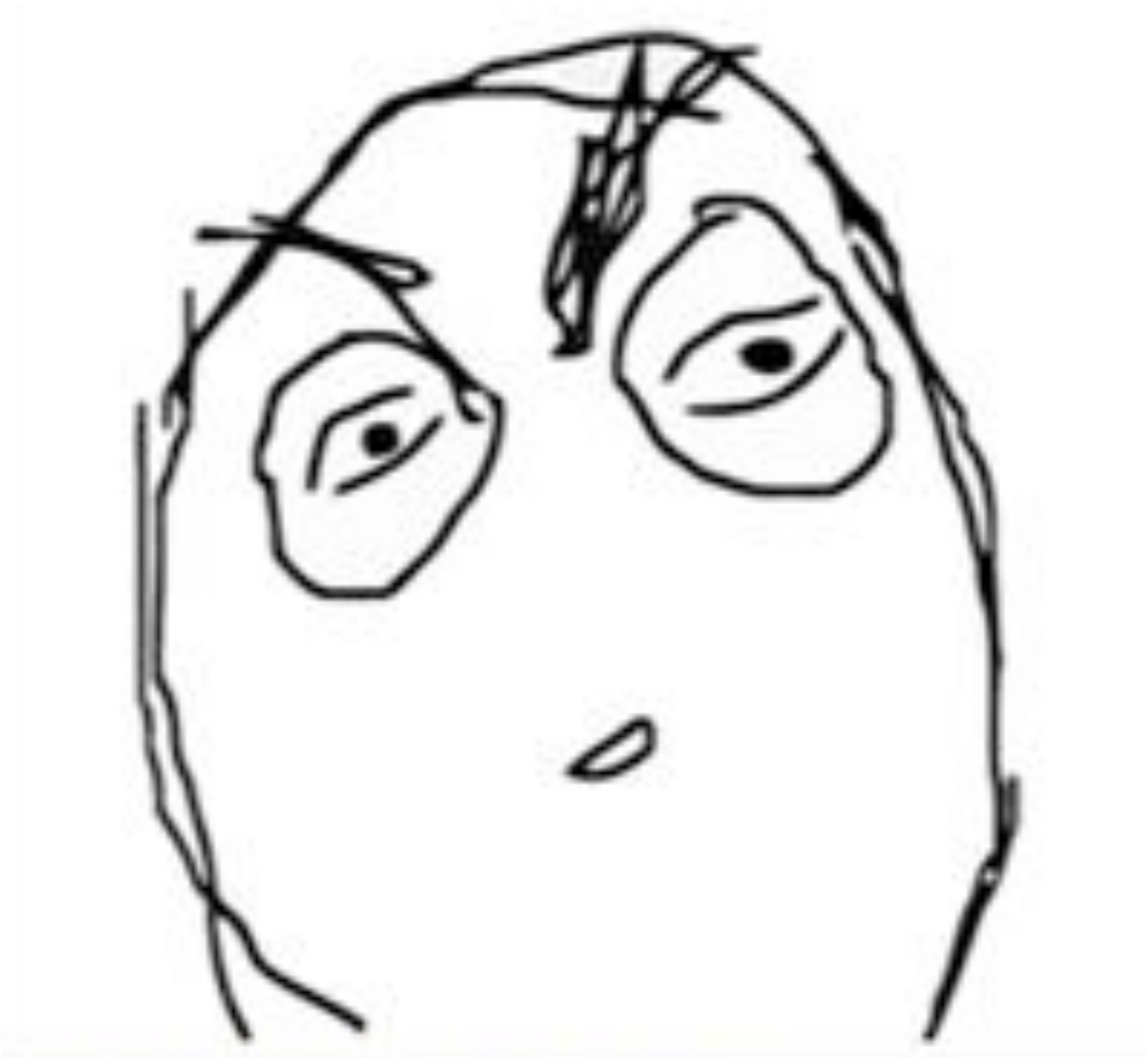


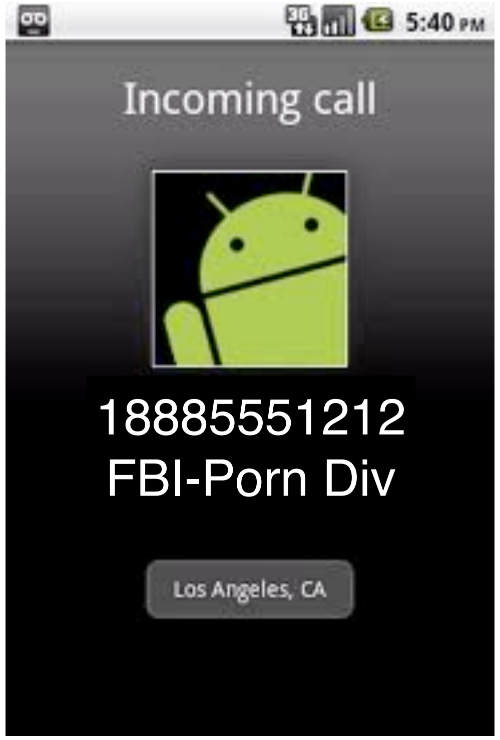
White Hat

Why is my users background laughing at me?
Bwahahahahhahahah

White Hat

Hmmmm.....



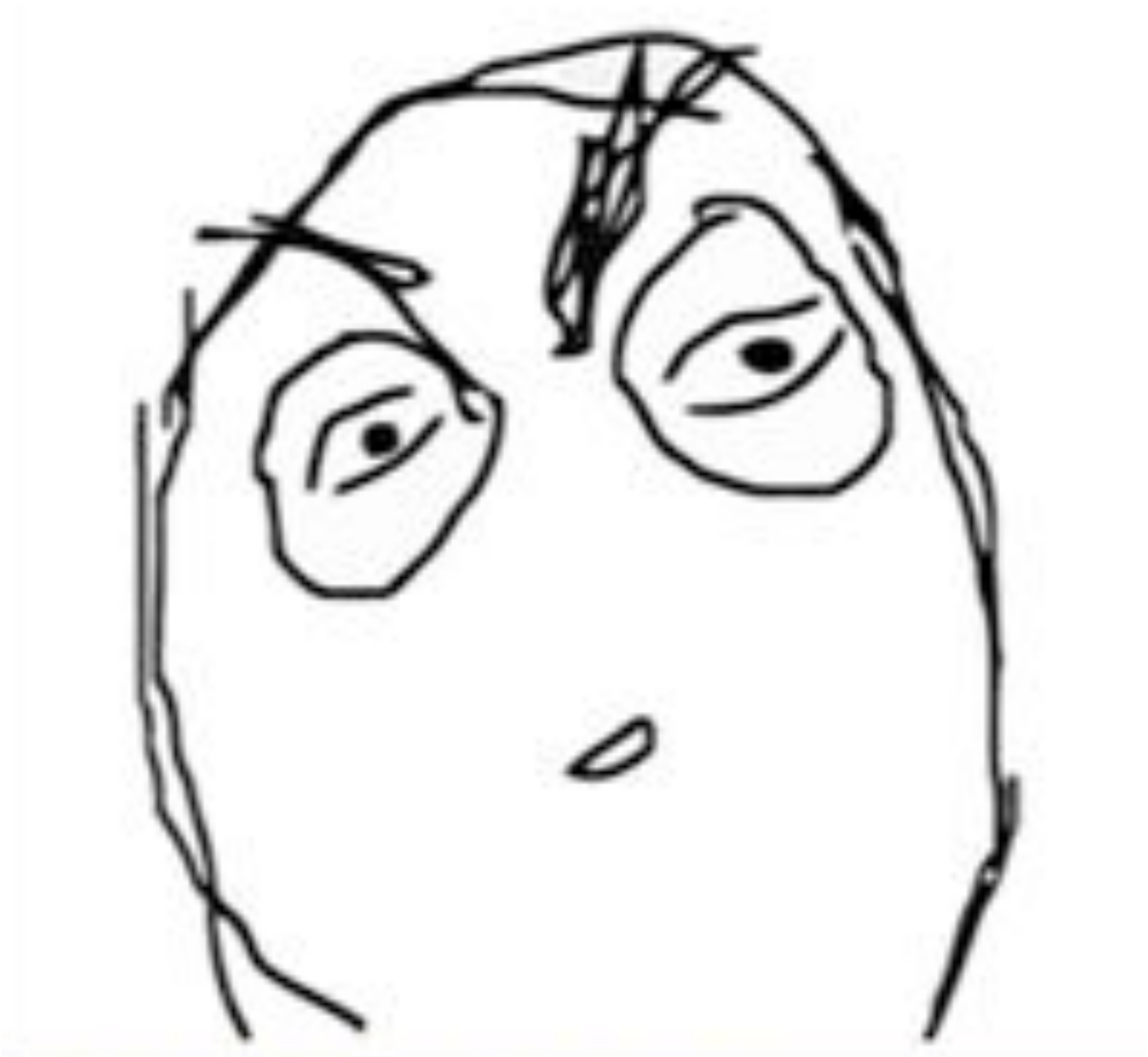


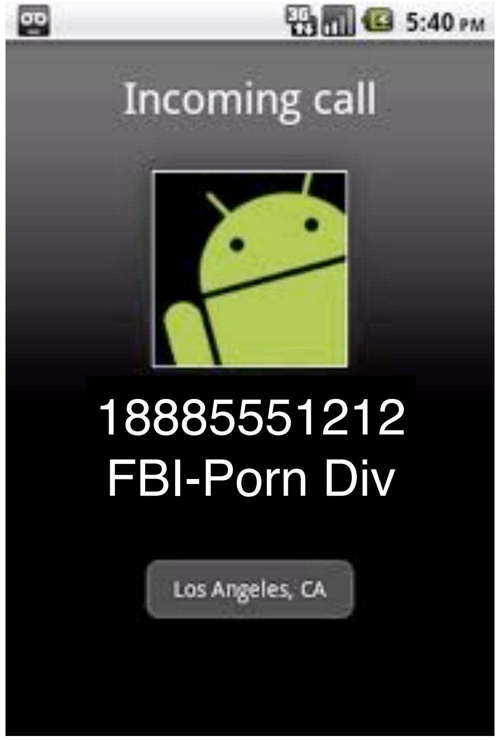
Incoming call

18885551212
FBI-Porn Div

Los Angeles, CA

White Hat



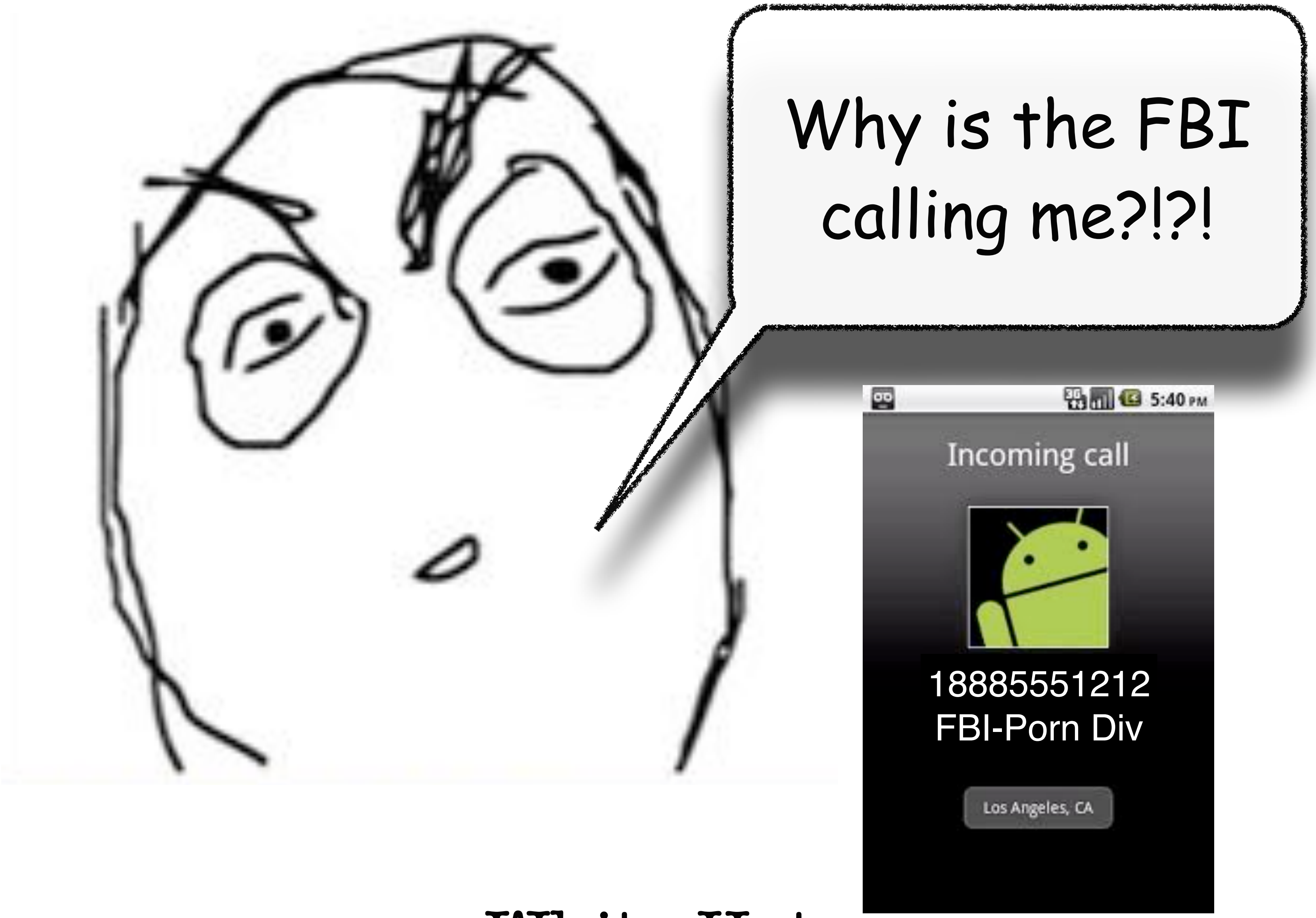


Incoming call

18885551212
FBI-Porn Div

Los Angeles, CA

White Hat

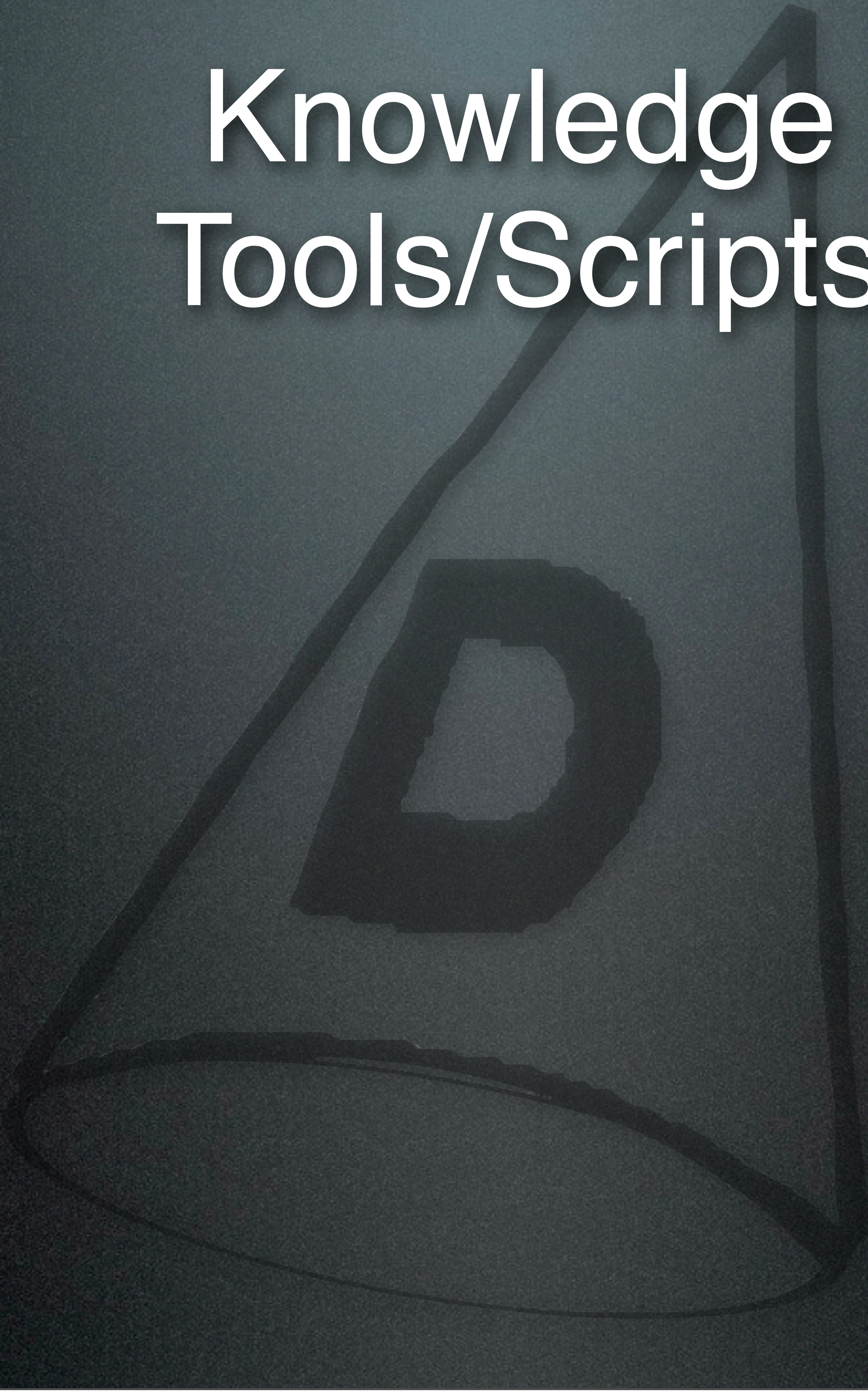

Why is the FBI calling me?!?!
5:40 PM
Incoming call
18885551212
FBI-Porn Div
Los Angeles, CA

White Hat

Advantage: BlackHat

Knowledge

Knowledge
Tools/Scripts

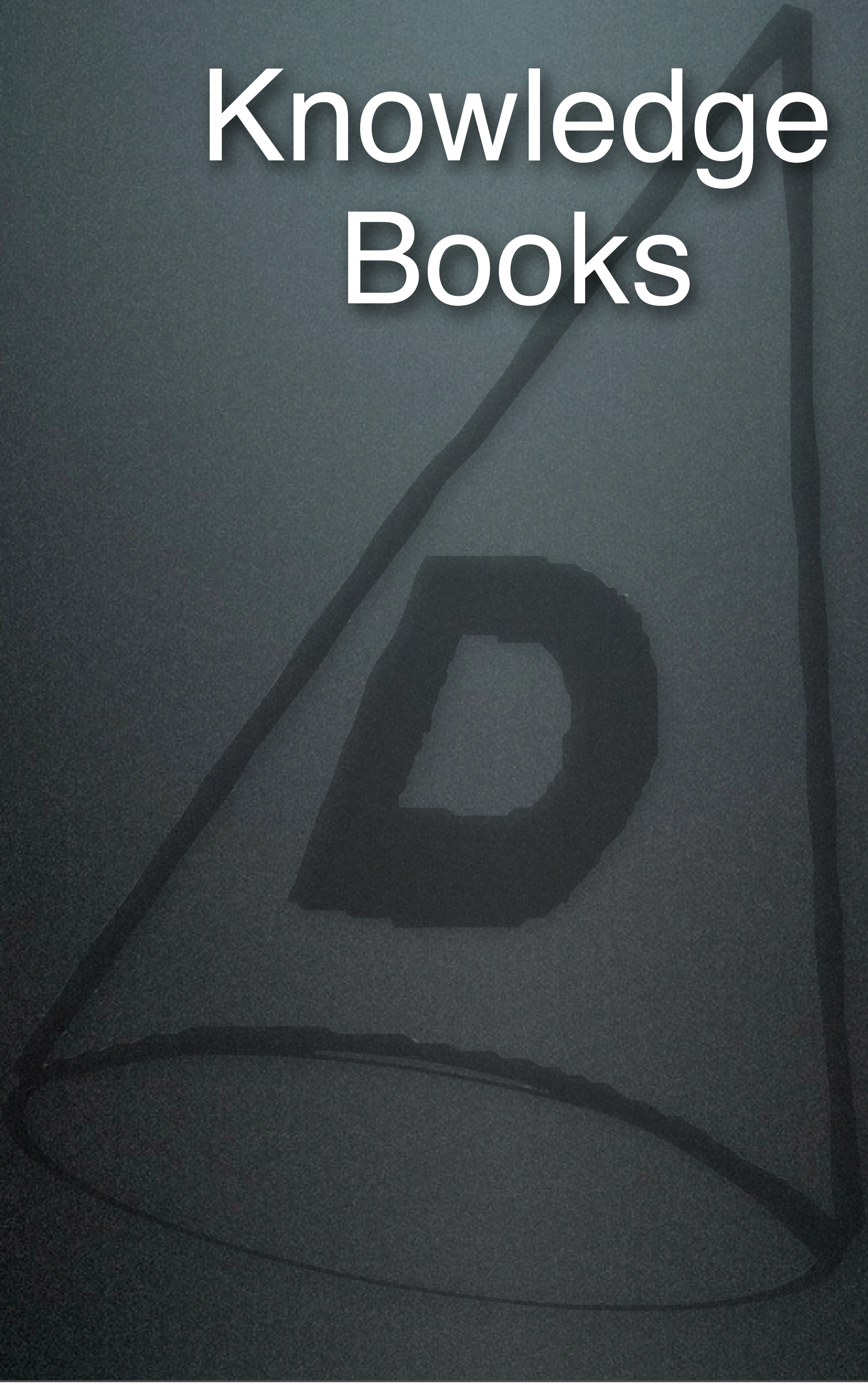


Knowledge
Tools/Scripts

Nmap
AirPwn
Metasploit
AutoPwn
Ettercap
dsniff
maltego

pig
fping
hping3
Saint/Satan
Nessus
corkscrew
netcat
etc...

Knowledge Books



Knowledge
Books

- HackingExposed
- Hacking: Art of exploitation
- Wi-Foo
- The Cuckoos Egg
- Ghost in the Wires
- Hacking for Dummies

Yes .. Really.

Knowledge Websites

- hackaday
- hackthissite
- cyberxtreme
- hackinthebox
- evilzone
- astalavista.box.sk

Knowledge Certification Courses

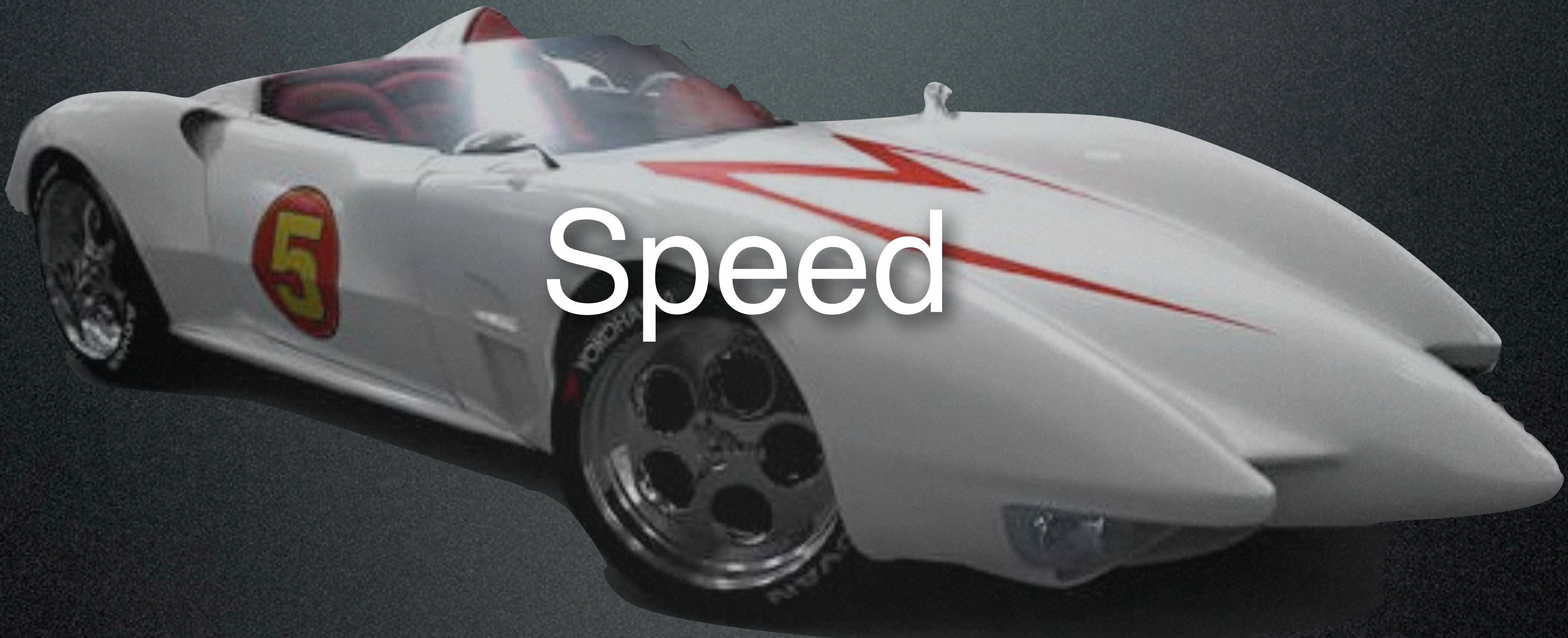
- SANS GSEC/GCIA
- Certified ~~Ethical~~ Hacker
- CompTIA Security+
- ISC^2 - CISSP/CAP

Knowledge
Conferences

- ShmooCon (duh!)
- DefCon/Blackhat
- CarolinaCon
- B-Sides
- USENIX Security Conferences
- DerbyCon

Advantage: BlackHat

Speed

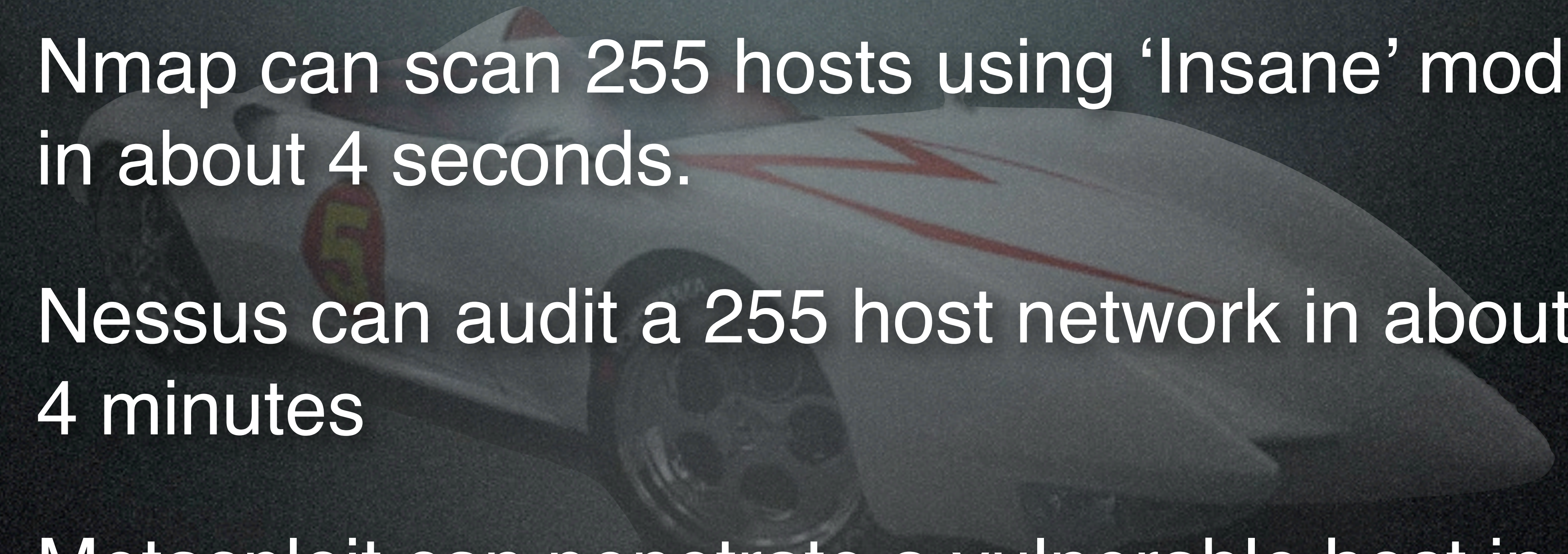


Speed

How Fast...

(c) 2012 sandSecurity

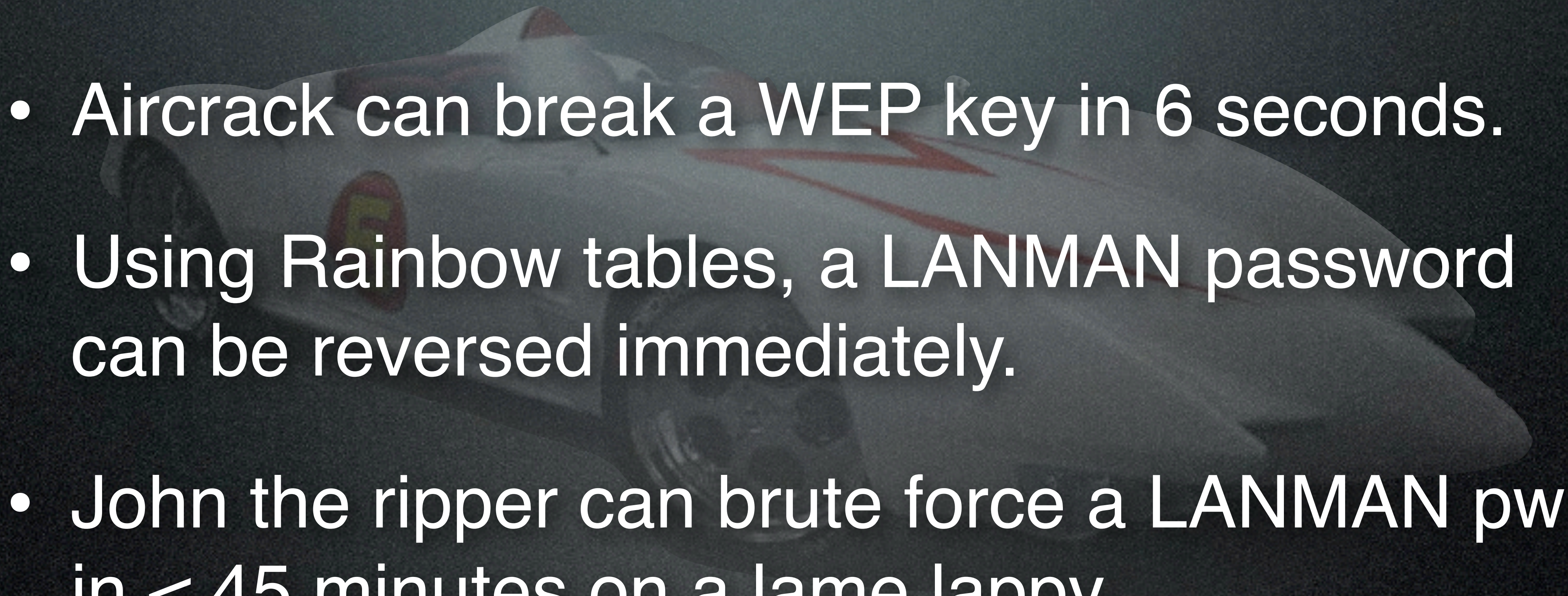
How Fast...



- Nmap can scan 255 hosts using ‘Insane’ mode in about 4 seconds.
- Nessus can audit a 255 host network in about 4 minutes
- Metasploit can penetrate a vulnerable host in < 1 second.

How Fast...

How Fast...

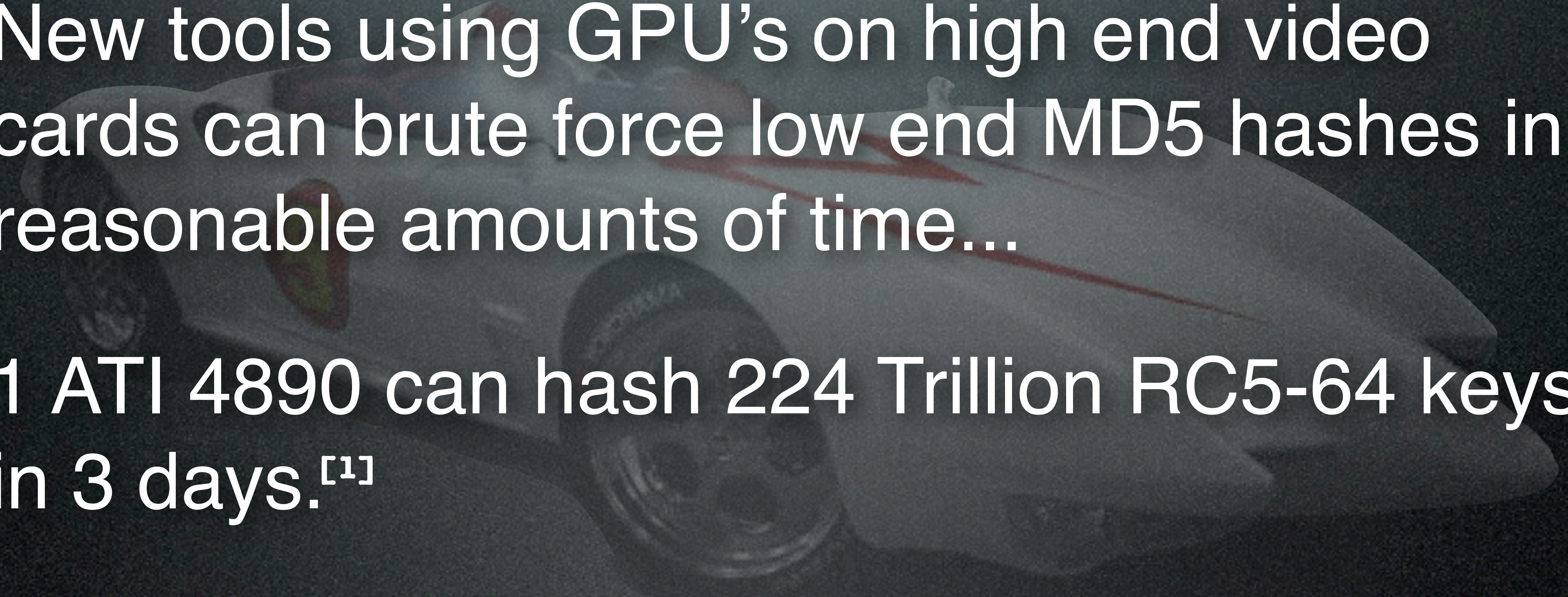


- Aircrack can break a WEP key in 6 seconds.
- Using Rainbow tables, a LANMAN password can be reversed immediately.
- John the ripper can brute force a LANMAN pw in < 45 minutes on a lame lappy.

How Fast...

(c) 2012 sandSecurity

How Fast...



- New tools using GPU’s on high end video cards can brute force low end MD5 hashes in reasonable amounts of time...
- 1 ATI 4890 can hash 224 Trillion RC5-64 keys in 3 days.[1]

[1] http://www.slideshare.net/SecurityTyue.net/gpu-vs-cpu-supercomputing-security-shootout

Advantage: BlackHat

Rules

Advantage: BlackHat

Your machines belong to us

Have a nice day.

Not Ahead

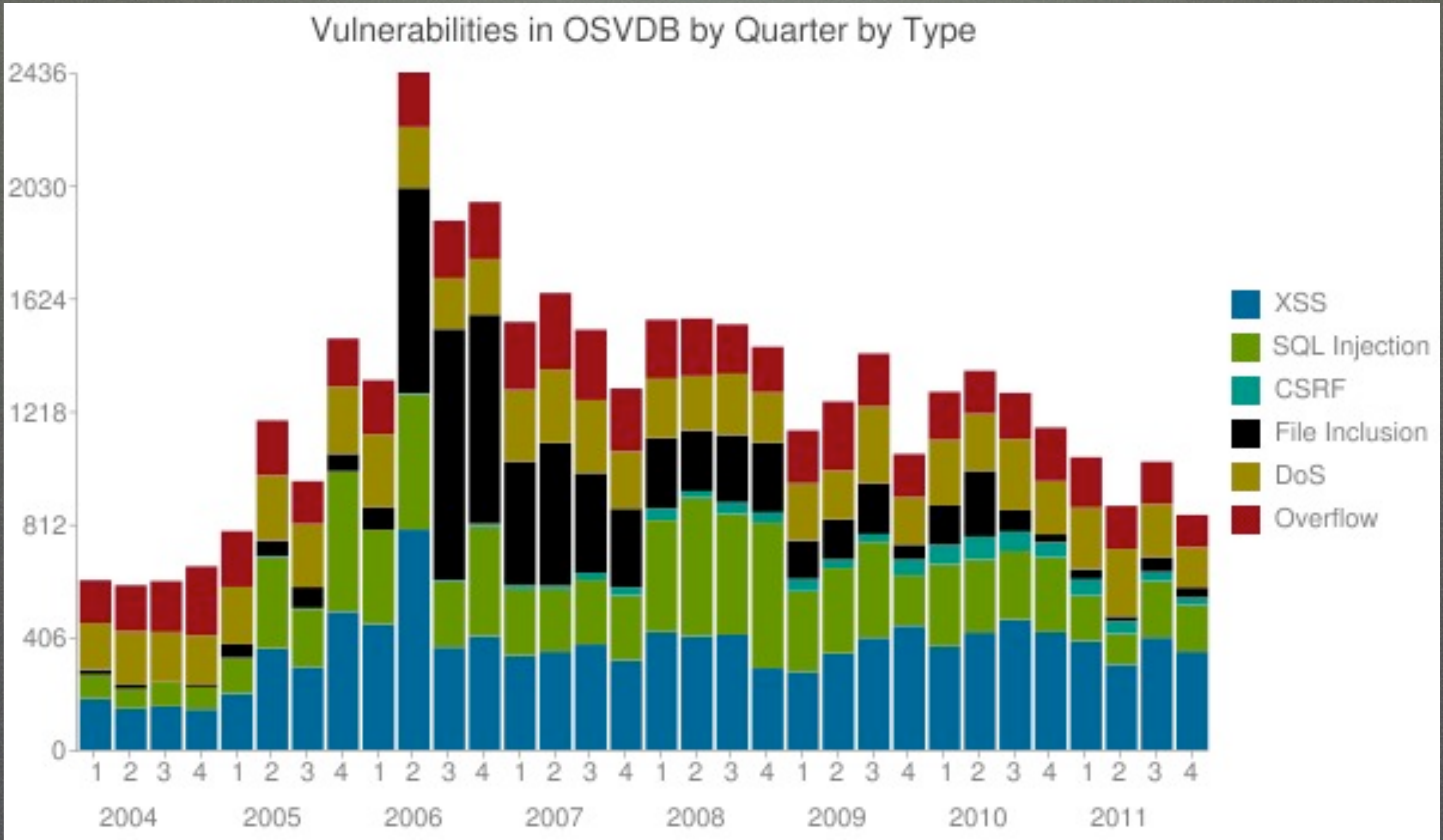
Not Ahead

(c) 2012 sandSecurity

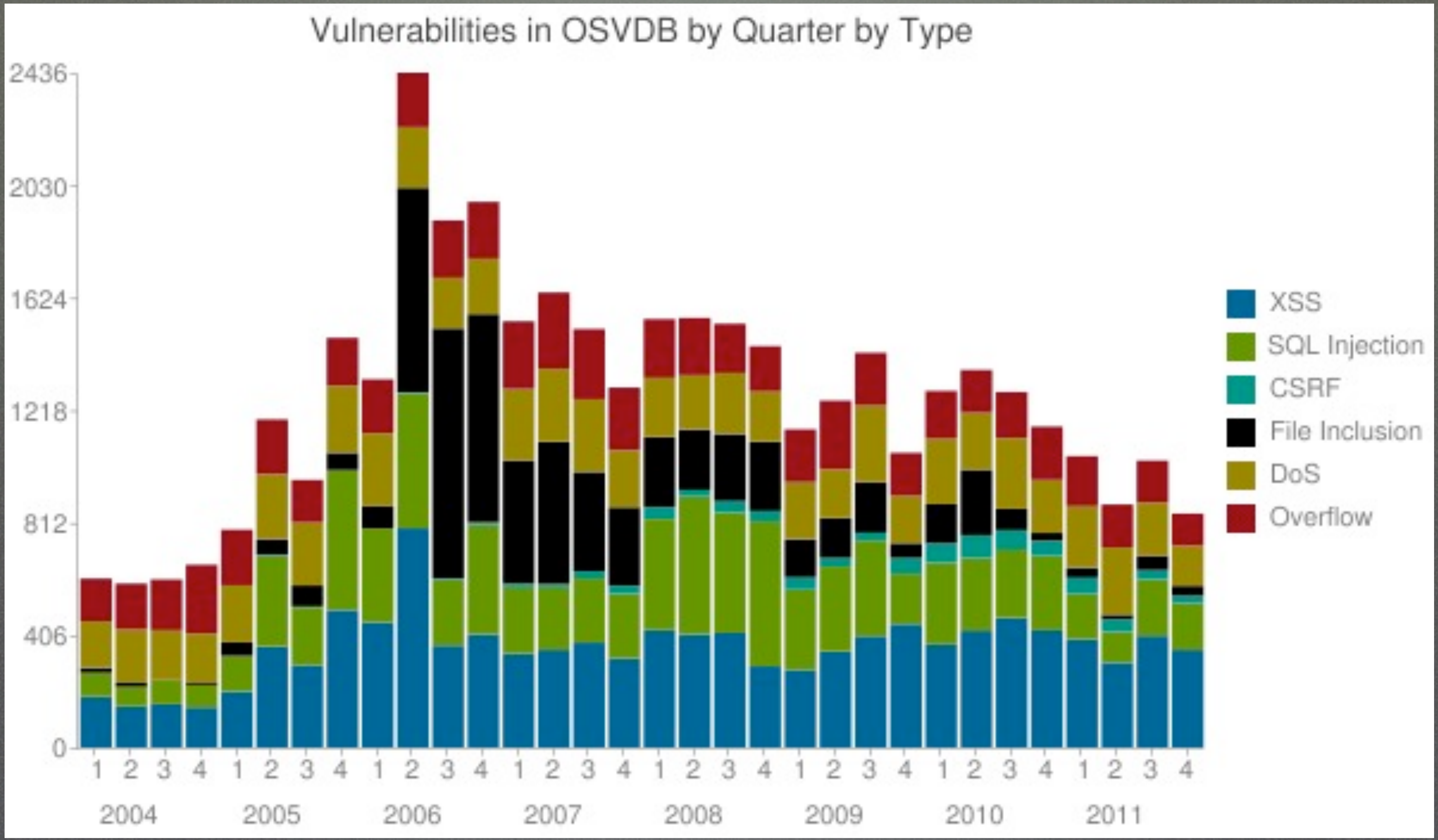
Bar for entry is getting lower every day.

How do we know they’re ahead?

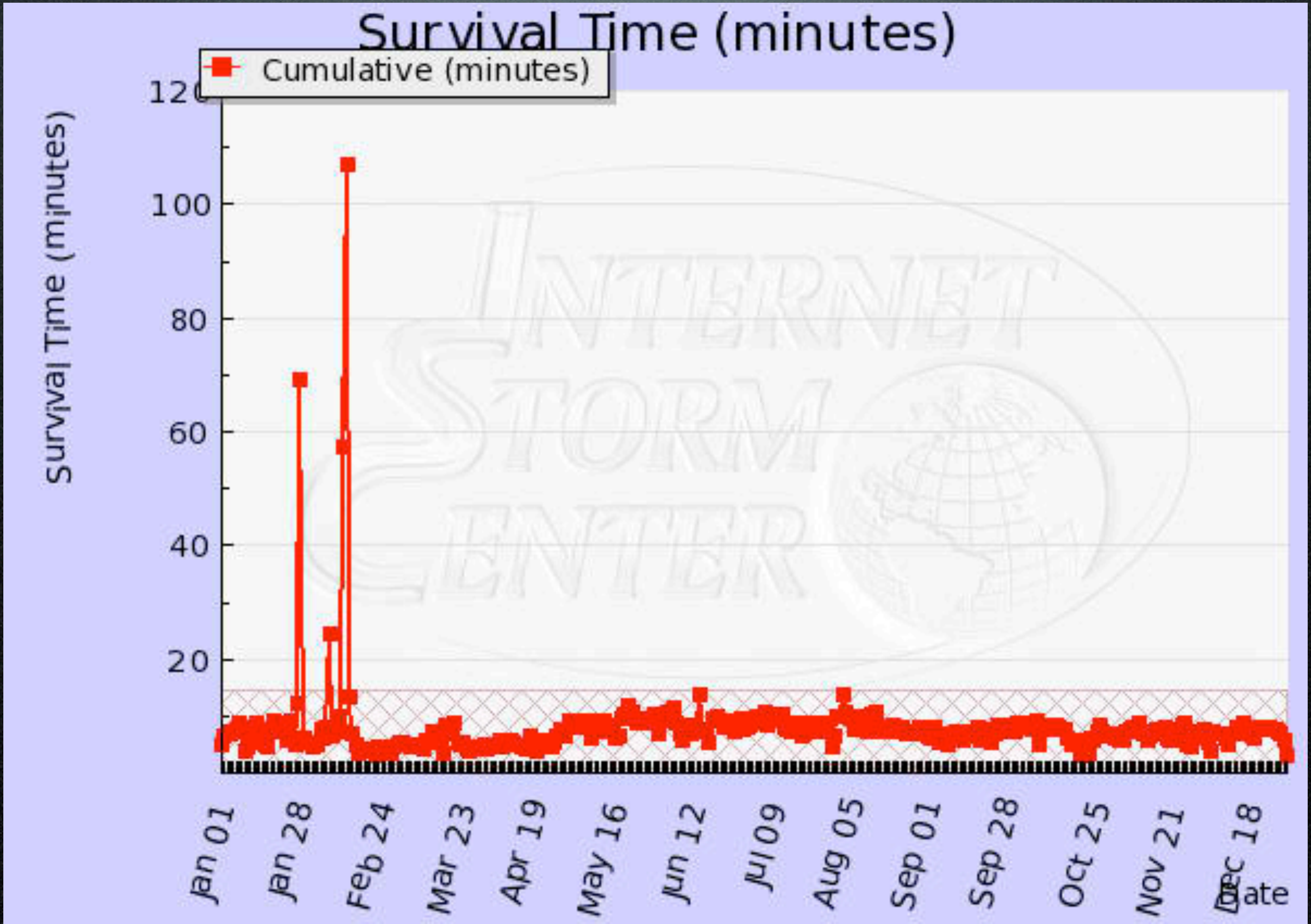
They can just use what's available.



They can just use what's available.



killing baby seals....



Anatomy of a Penetration

Anatomy of a Penetration

Part 1 - What a hacker sees.
(a view to a kill)

Lets break down a penetration...

Lets break down a penetration...

- Target Determination
- Reconnaissance
- Probing
- Exploit!
- Hide!
- Reap Benefits...

Target Determination

Target Determination

- Have something I want
- Are doing something I don’t want
- Appear easy to attack
- Would be a ‘notch in the saddle’ if I get em.
- Paid to do it

Reconnaissance

Reconnaissance

- Information Gathering
  - Teh Goog - google.com
  - War Driving/Hotspot Location - kismet
  - NetCraft - bw usage
  - Pig - Passive Network Information Gathering
  - Maltego - Information gathering

Reconnaissance

Reconnaissance

- Social Engineering
  - Calling support line - “can I change my password?”
  - Opening a fake account - jimmy_buffet2123
- Researching Geographical Region

Probing

- Nmap
- Nessus
- Xprobe2++
- Saint
- Telnet
- OWASP

Exploit

- Metasploit - Hundreds of exploits and payloads.
- hydra - brute force on unprotected services
- Several thousand hacking scripts..

Cover Tracks

- clean out access logs
- install root-kits (user , kernel, BIOS ...)
- hide code
- obfuscate network traffic
- disable monitoring systems

Collect Reward

- Access local useful information
- Use as part of a bot-net
- Keyboard logging for more opportunities
- Pivot against other local hosts
- Access to another tier for attack

Anatomy of a Penetration

Anatomy of a Penetration

Part 2 - What the hacked sees.
(it's a matter of time...)

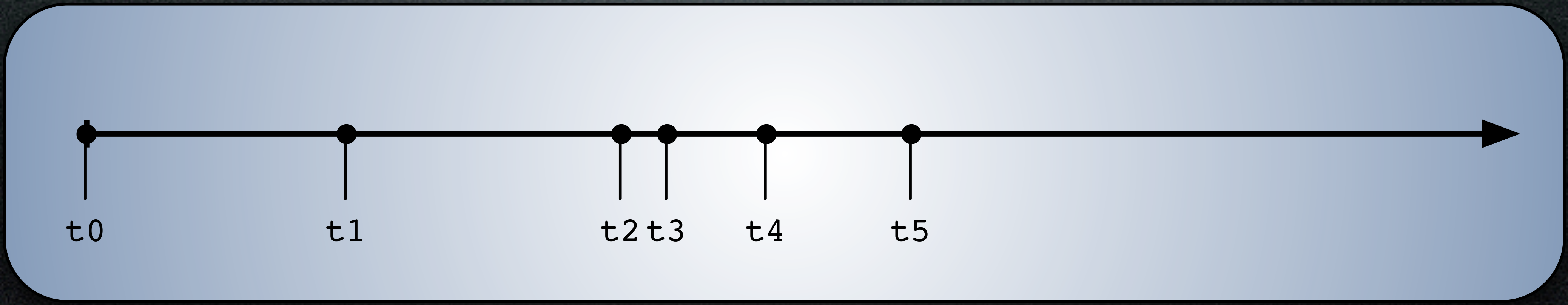
Anatomy of a Penetration

Part 2 - What the hacked sees.
(it’s a matter of time...)

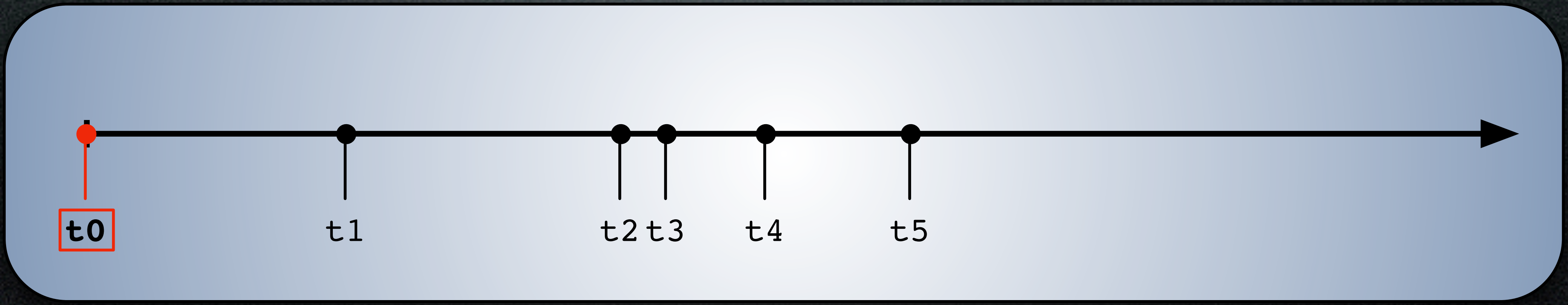
TTL

Timeline

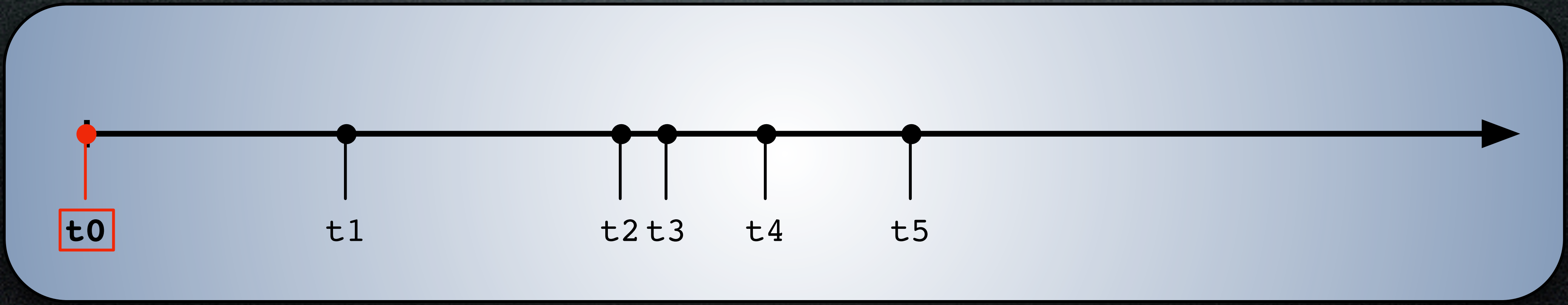
- Each point in time of an attack is significant



Timeline



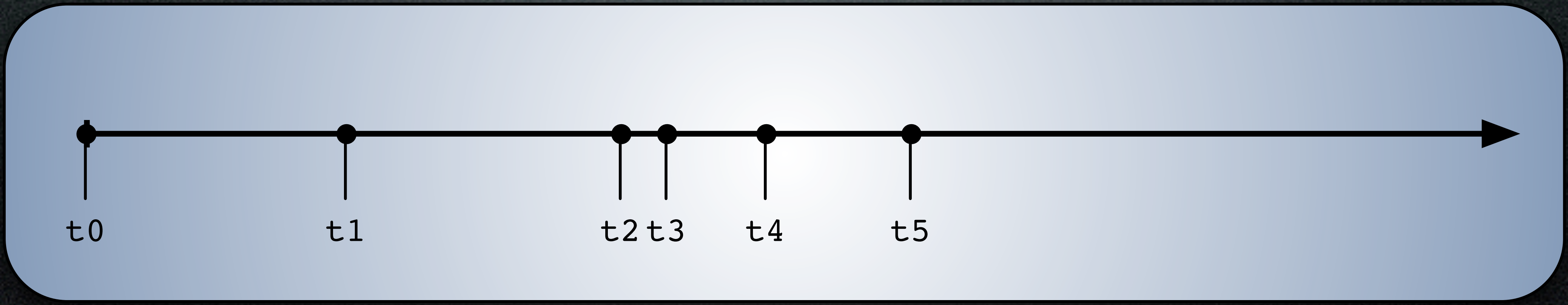
Timeline



- t0 - 23:59:59 Dec 31, 1969

Timeline

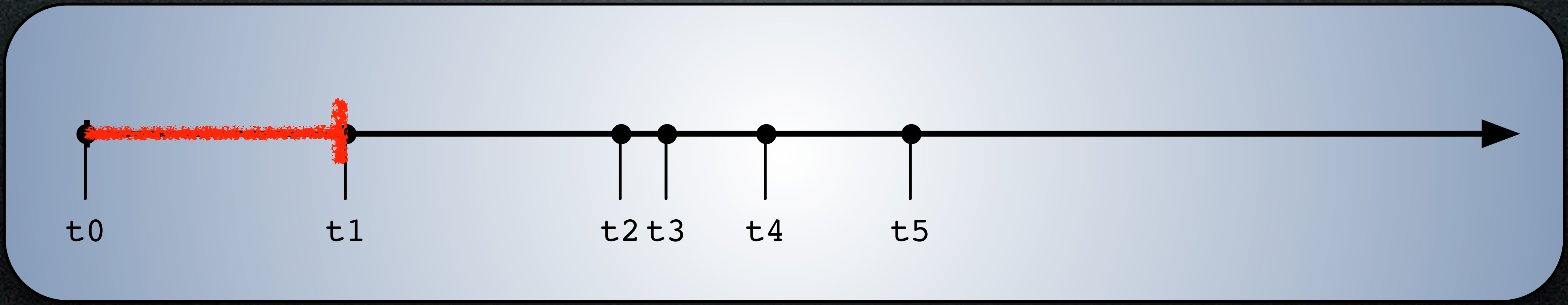
Who should I attack?



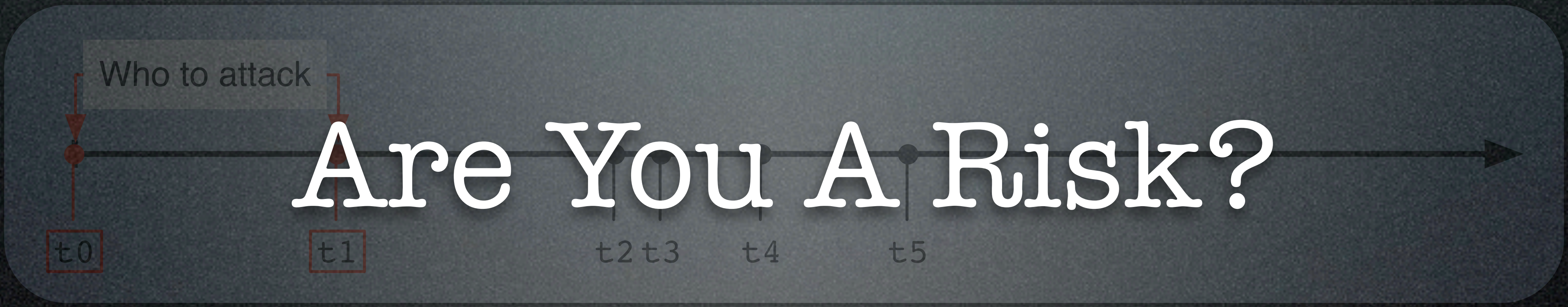
(c) 2012 sandSecurity

Timeline

Who should I attack?



Who to attack



Are You A Risk?

Who to attack

“ Risk is the probability of a loss tied to an asset.”

Risk...

Have something I want...

- **Government**
- **Financial**
- **Commercial**
- **Internet Service Provider**
- **Media Provider**
- **Other**

Risk...

Have something **others** want...

- **Internet Services**
- **Security Company**

- **Software development**
- **Commercial**
- **FOSS**

Risk...

Doing something I don't like...

- Internet Service Provider
- Financial Institution
- Government(s)
- Commercial Entity
- Security Company doing bad stuff

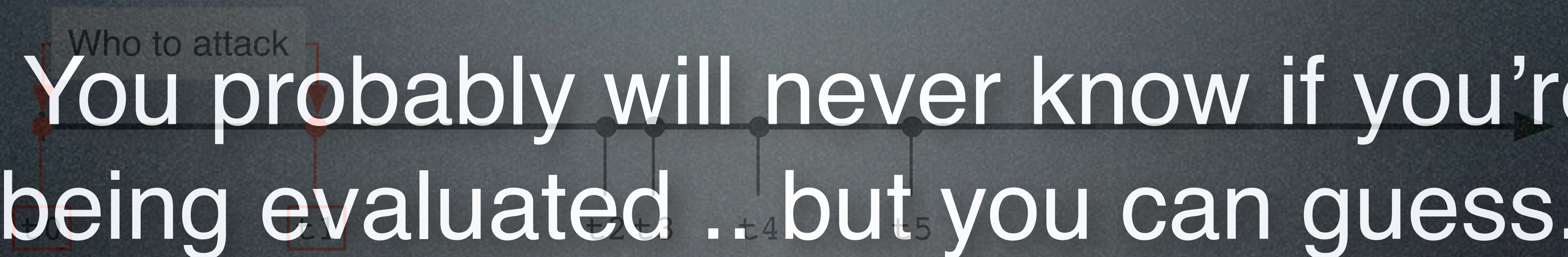
Timeline
Using something I can easily hack or exploit....

- Unpatched OS
- Facebook
- Flash
- Email

- Windows
- Android
- iOS
- OSX

Who to attack
t0
t1
t2
t3
t4
t5

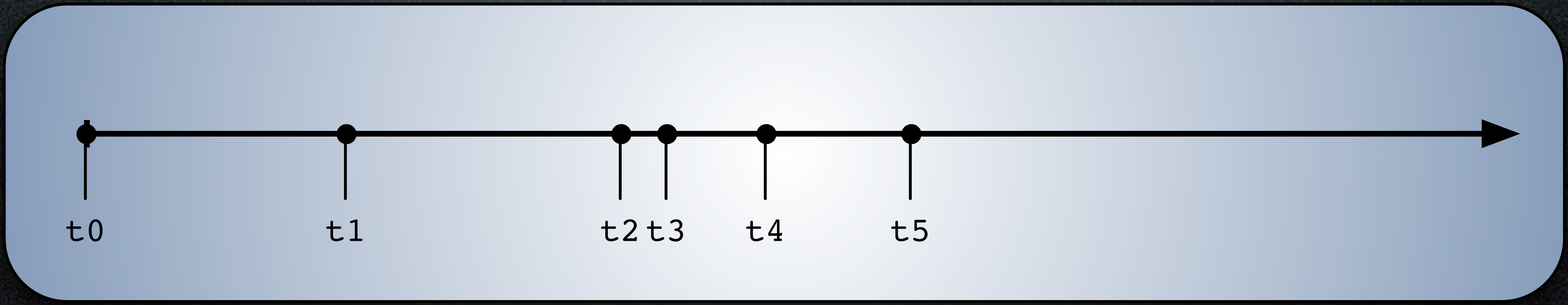
Timeline



You probably will never know if you’re being evaluated ... but you can guess...

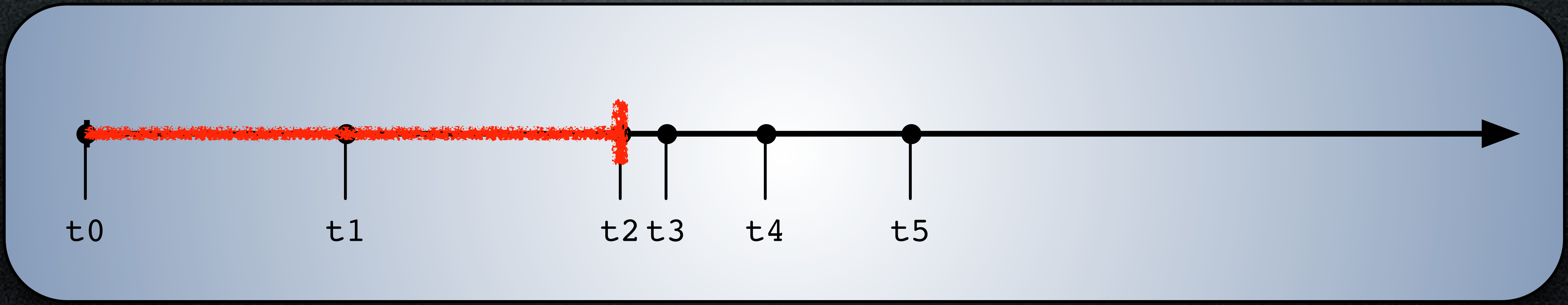
Timeline

Reconnaissance...

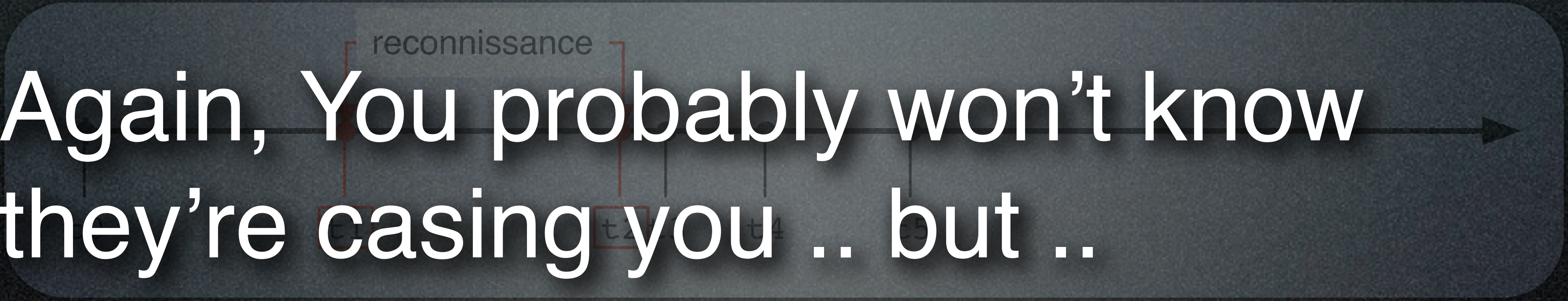


Timeline

Reconnaissance...



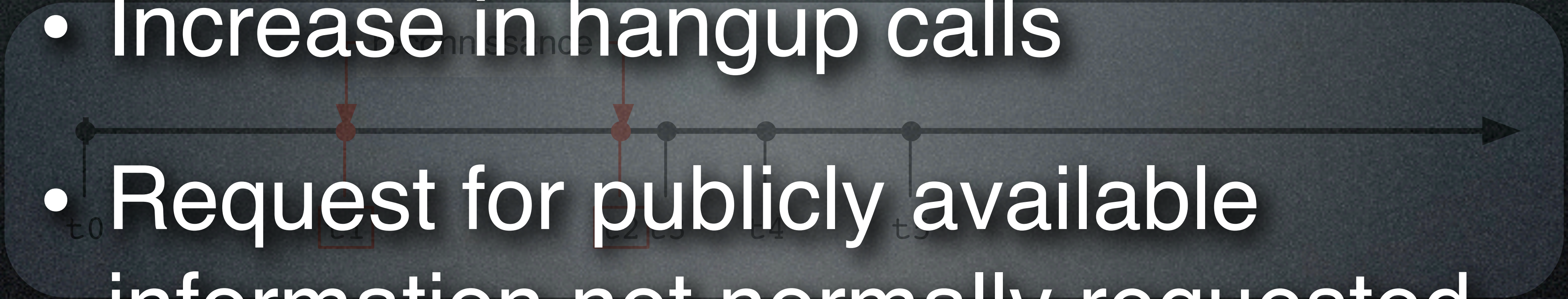
t2 - Reconnaissance



Again, You probably won’t know they’re casing you .. but ..

t2 - Reconnaissance

- Business Indicators
  - Increase in hangup calls
  - Request for publicly available information not normally requested.
  - Invalid support calls



t2 - Reconnaissance

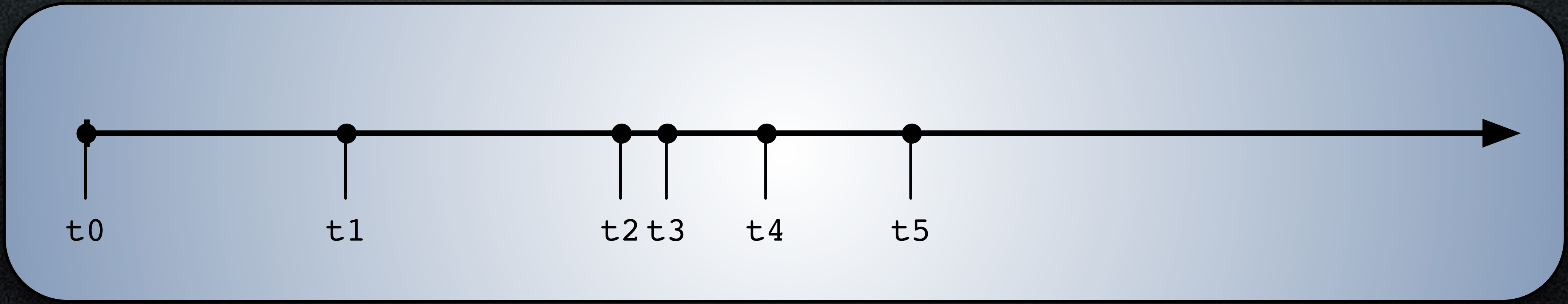
- Non-direct Indicators
  - Distinct, un-warranted increase in “valid” web or email traffic.
  - Increase Friend requests (AIM, skype, facebook ..etc) to business AND associates.

reconnissance
t0
t1
t2
t3
t4
t5

(c) 2012 sandSecurity

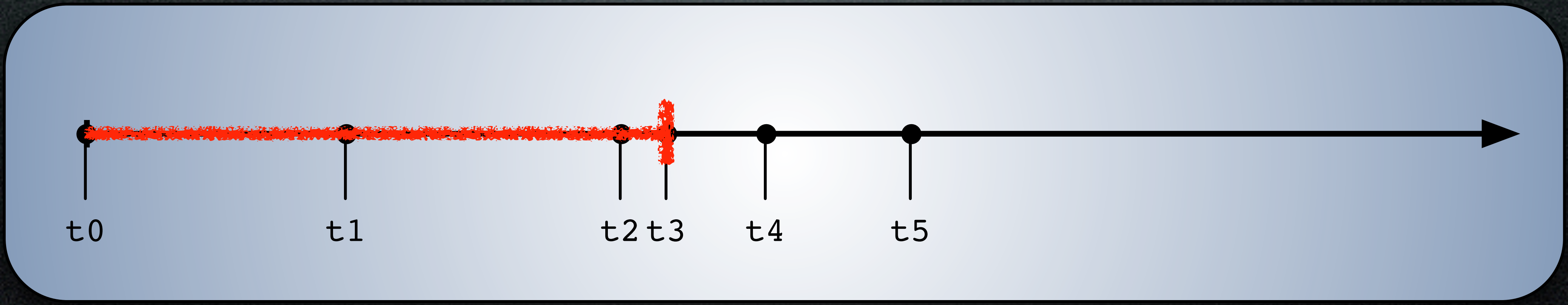
Timeline

Probing...



Timeline

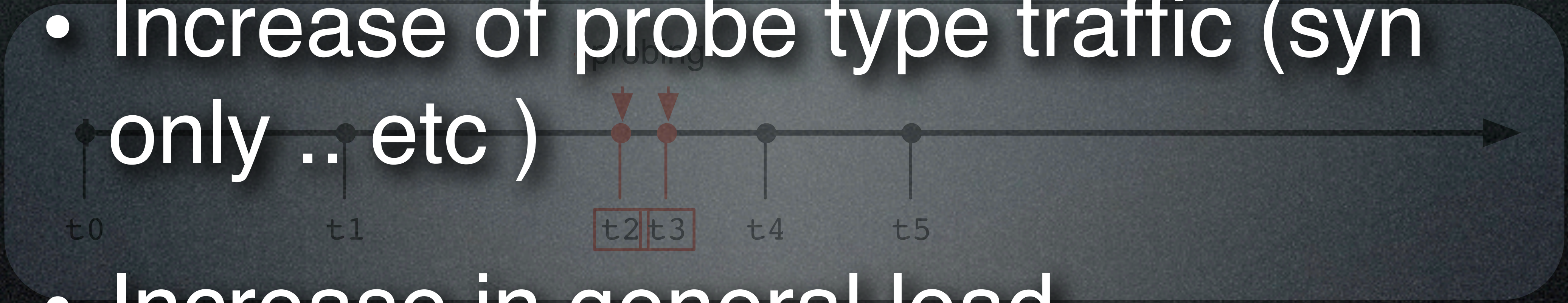
Probing...



(c) 2012 sandSecurity

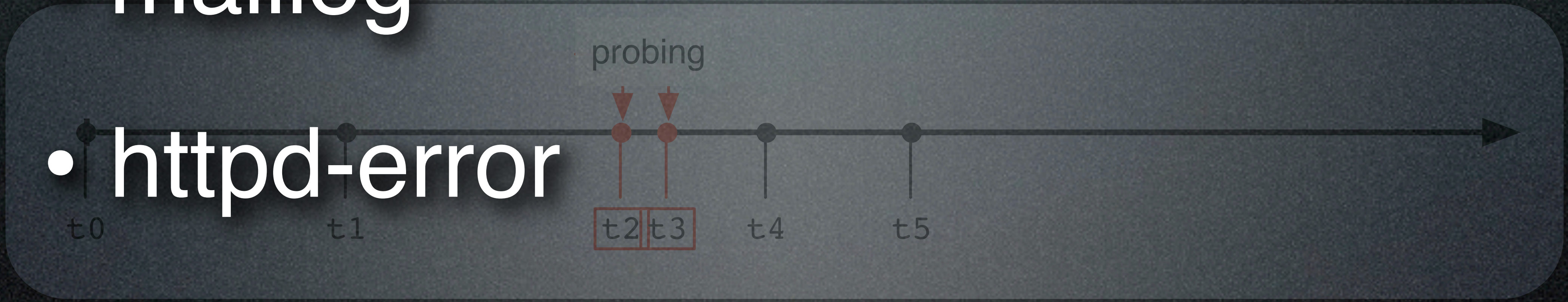
t3 - Probing

- Increased Network Load
  - Increase of probe type traffic (syn only .. etc)
  - Increase in general load
  - Increase in load on a specific port



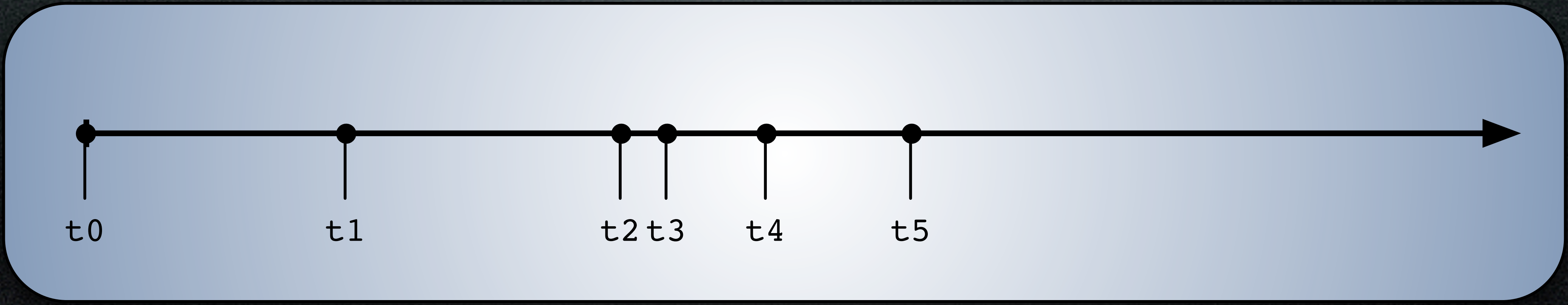
t3 - Probing

- Changes in Application Logs
  - maillog
  - httpd-error
  - EventLog
  - Firewall Logs



Timeline

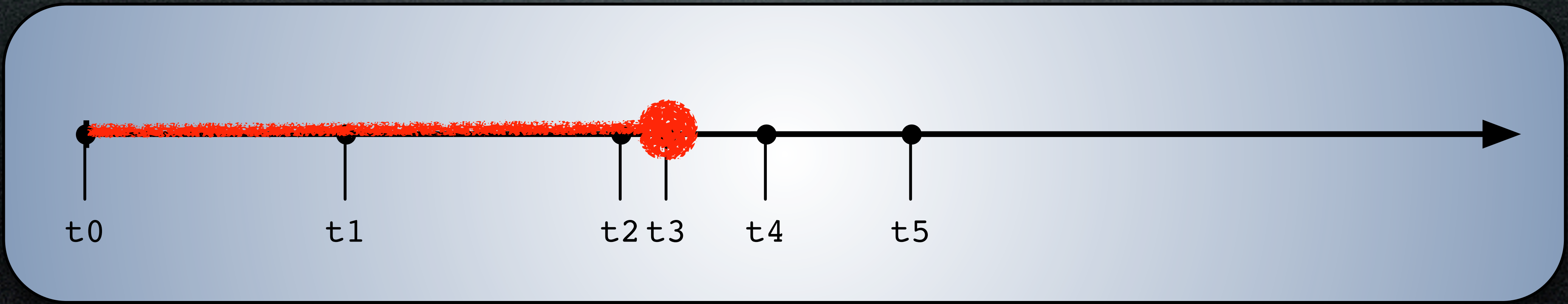
Exploit!



(c) 2012 sandSecurity

Timeline

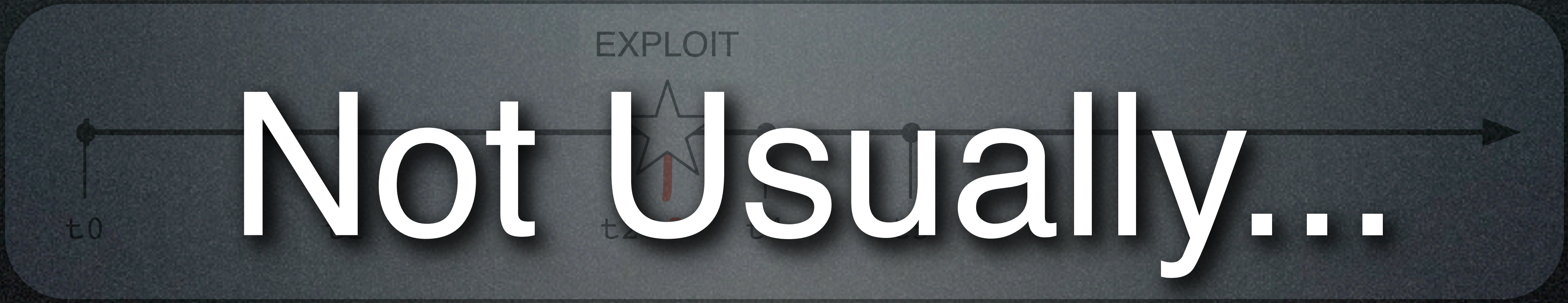
Exploit!



Timeline

Does anyone ever know right when they’re exploited...

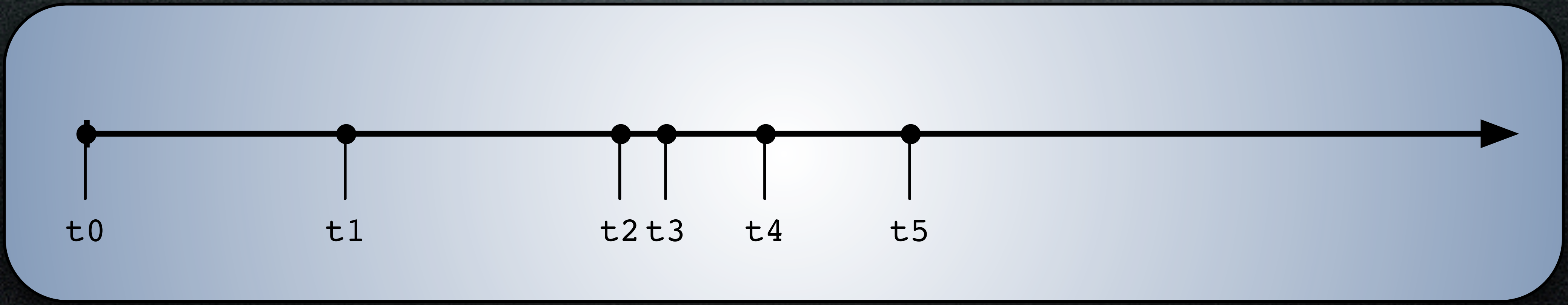
Timeline



Not Usually...

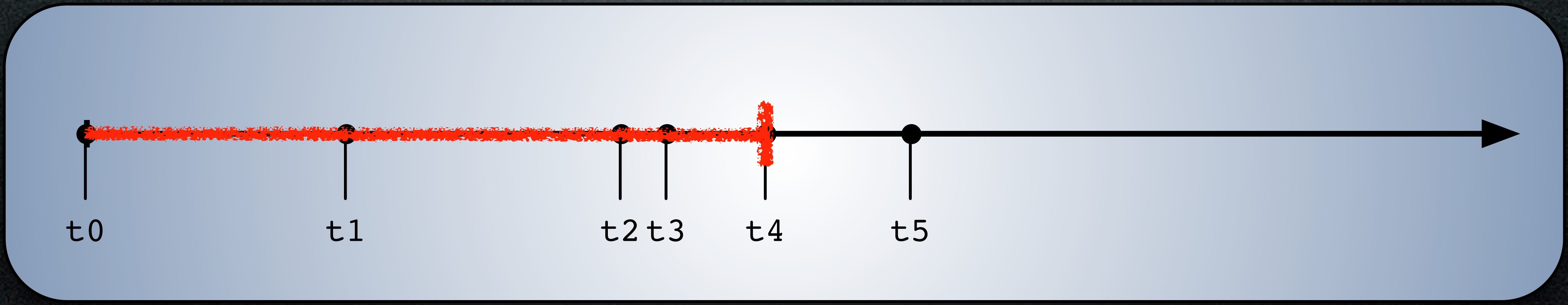
Timeline

Penetration...



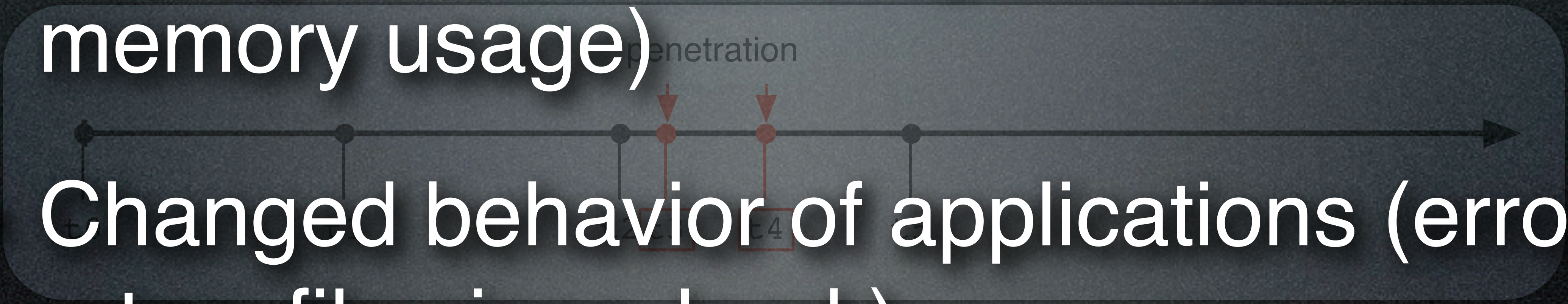
Timeline

Penetration...



t4 - penetration

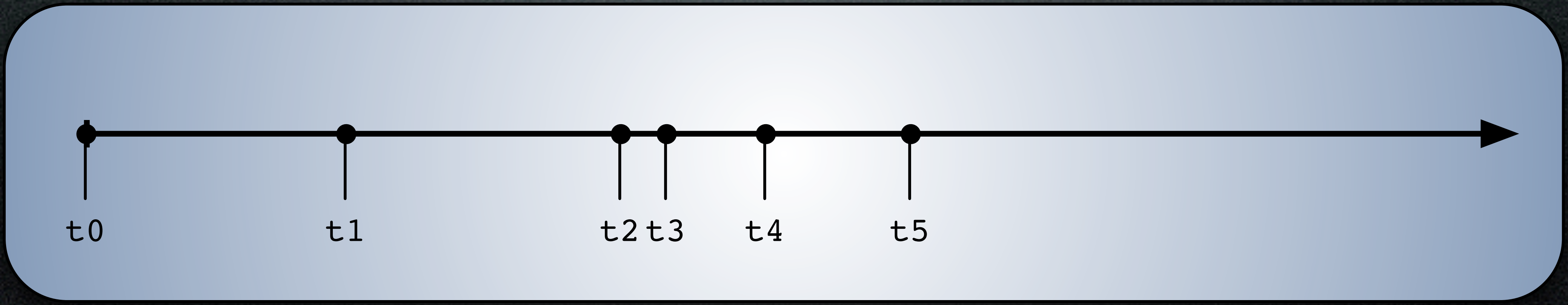
- Changed files on filesystem
- Changed behavior of system (load, memory usage)



- Changed behavior of applications (error rates, file sizes, load)
- Changed behavior of network traffic

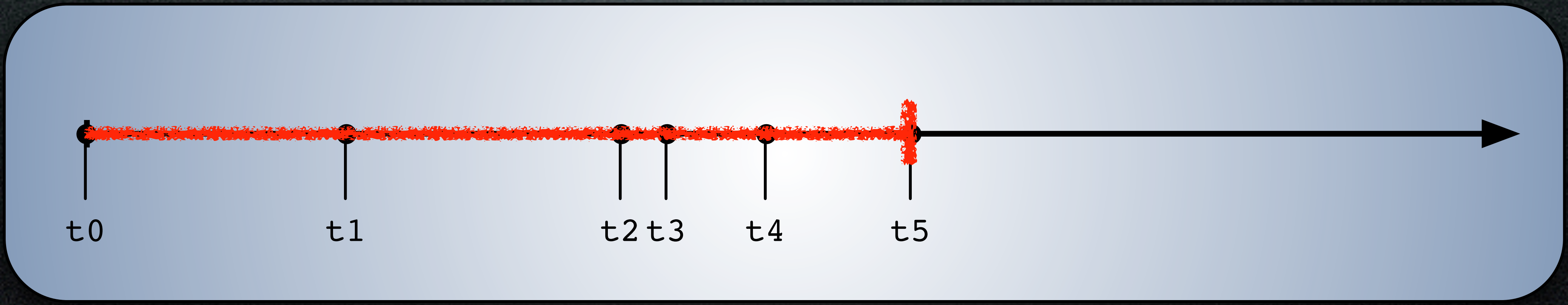
Timeline

Cleanup...



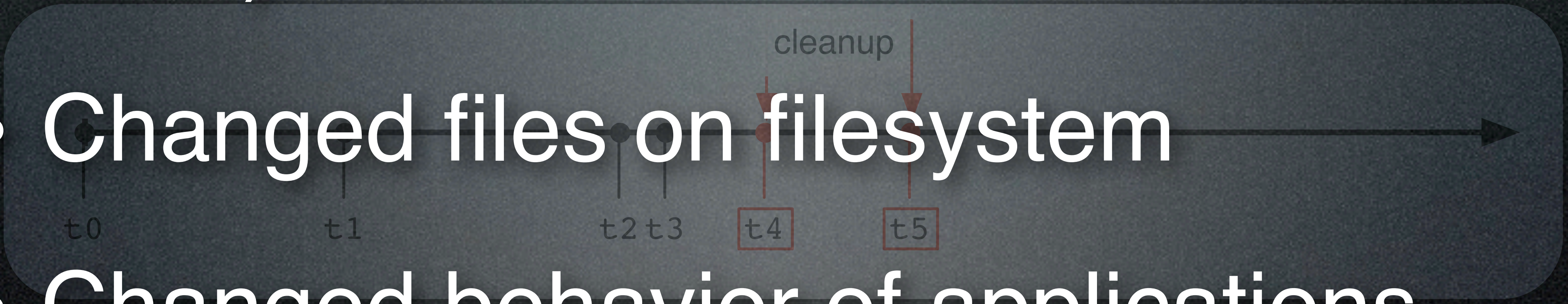
Timeline

Cleanup...



t5 - Cleanup

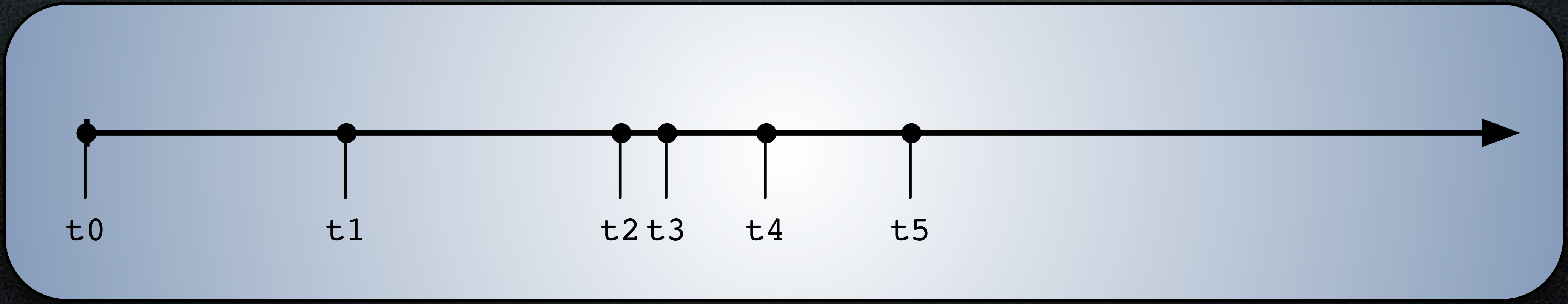
- Missing information in logs (holes in time)



- Changed files on filesystem
- Changed behavior of applications
- Changed behavior of network traffic

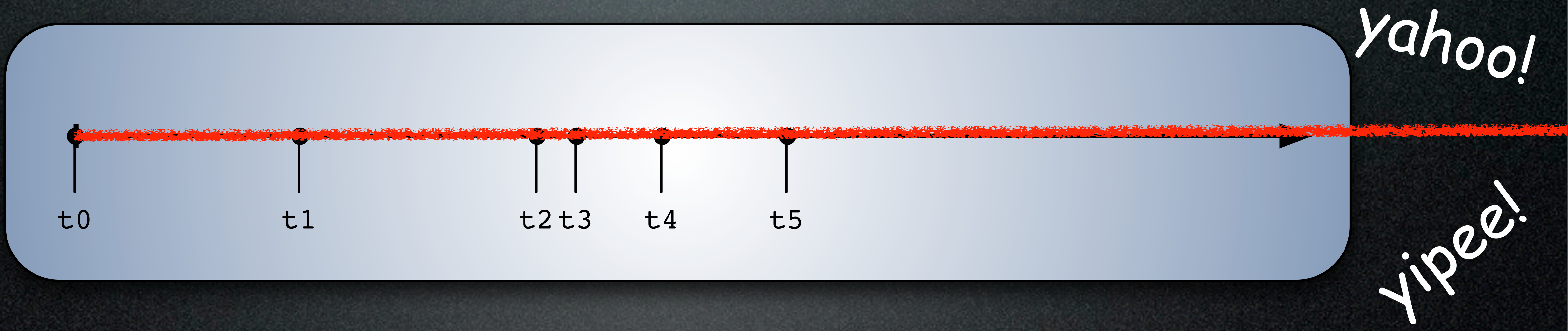
Timeline

Reap Reward...



Timeline

Reap Reward...



Once they’re in .. it’s VERY hard to know you’ve gotten them out.

Once they're in .. it's ~~VERY hard~~ **Almost Impossible!** to know you've gotten them out.

(c) 2012 sandSecurity

Penetration == BAD.

So .. how can you minimize risk?

Insert

yourself

in

the process.

Insert

in

the process.

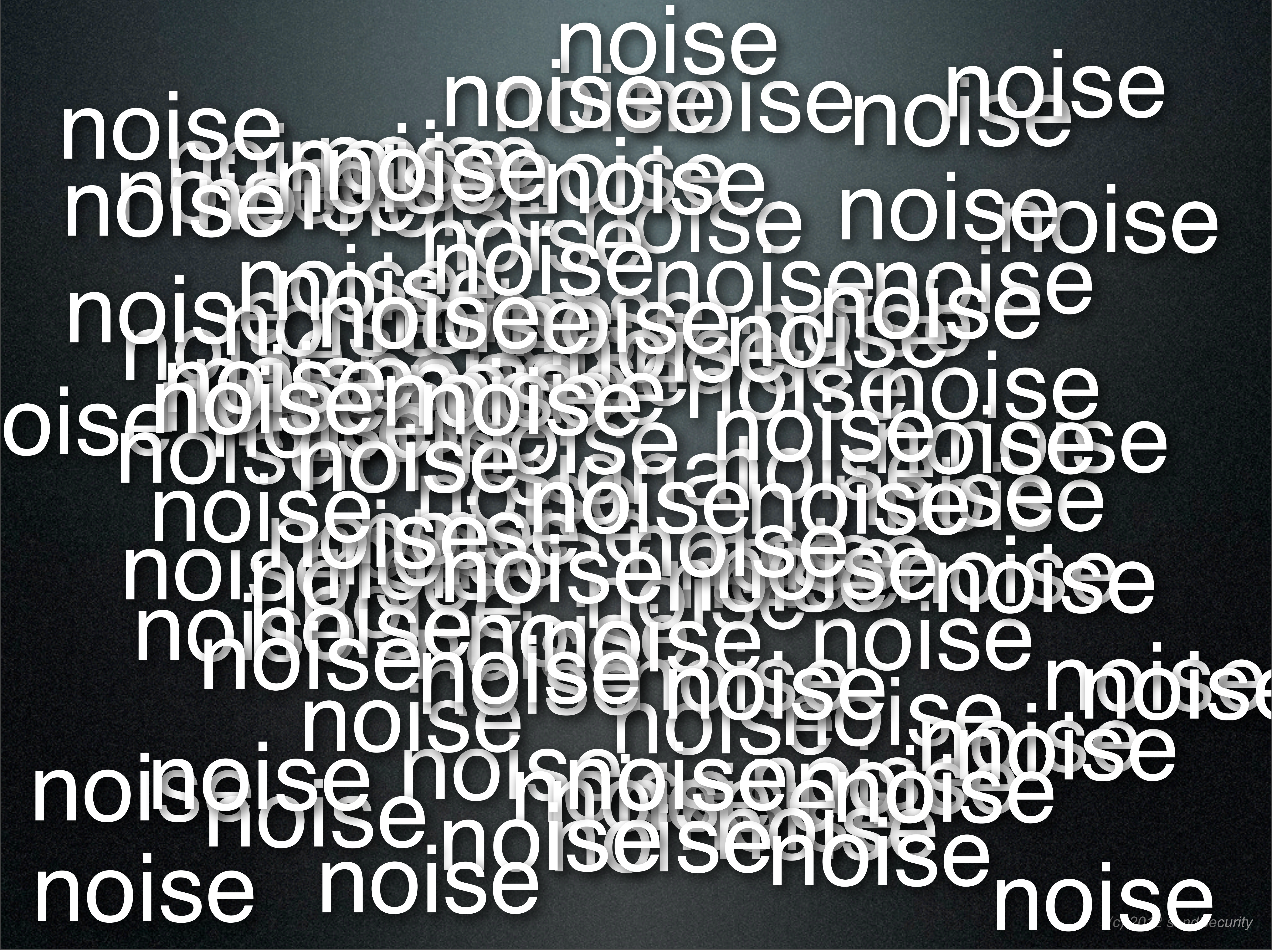
yourself

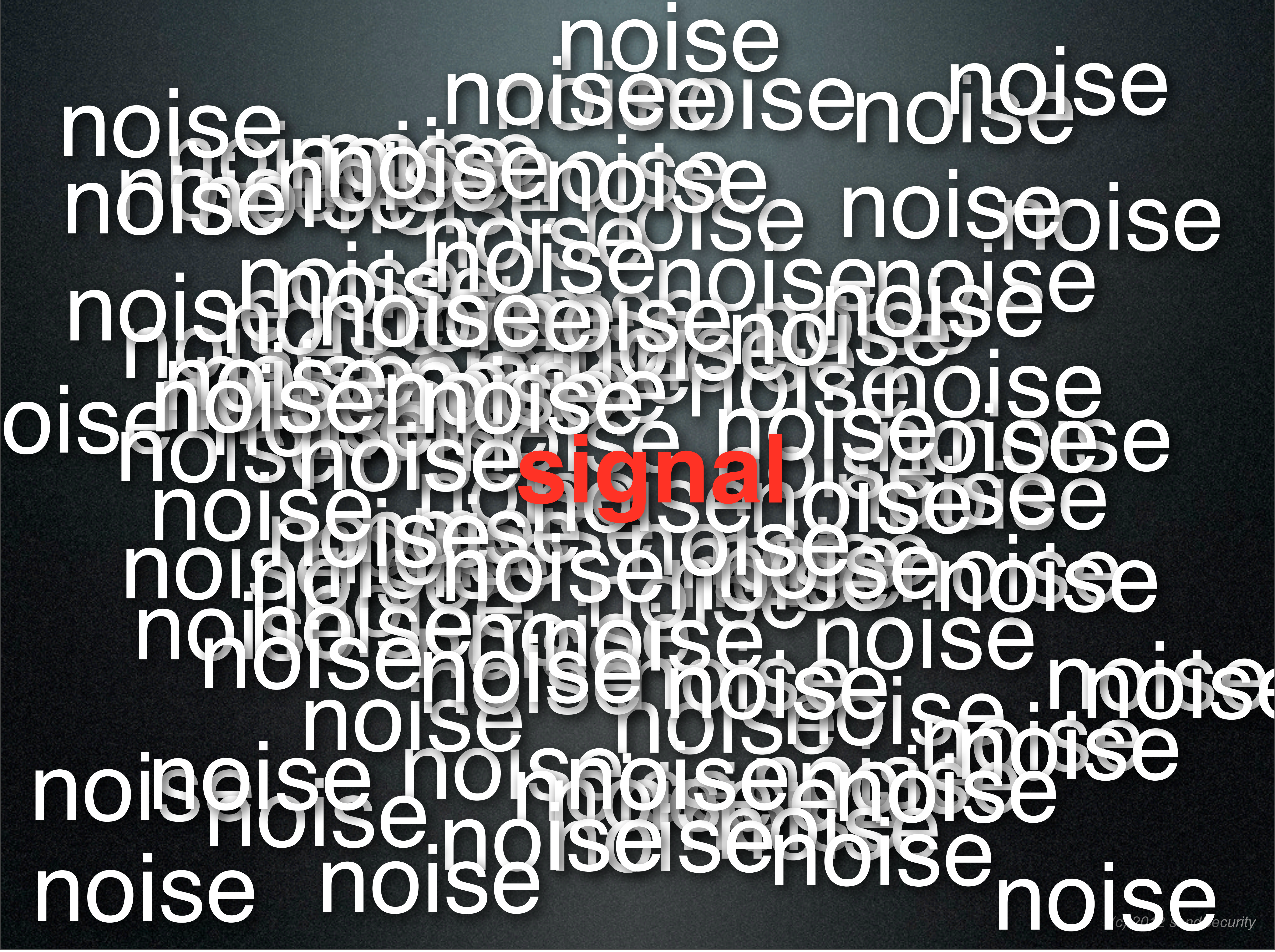
Anatomy of a Penetration

Anatomy of a Penetration

Part 3[3]- Insert Yourself

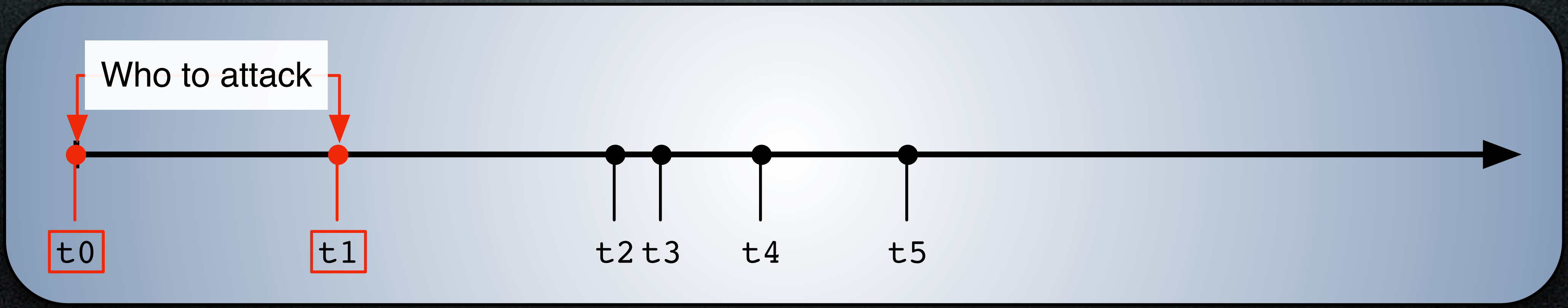
[3] ”... Then shalt thou count to three, no more, no less. Three shall be the number thou shalt count, and the number of the counting shall be three. Four shalt thou not count, neither count thou two, excepting that thou then proceed to three. Five is right out. Once the number three, being the third number, be reached, then lobbest thou thy Holy Hand Grenade of Antioch towards thy foe, who, being naughty in my sight, shall snuff it.”


noise


noise
signal

Baseline!

Timeline

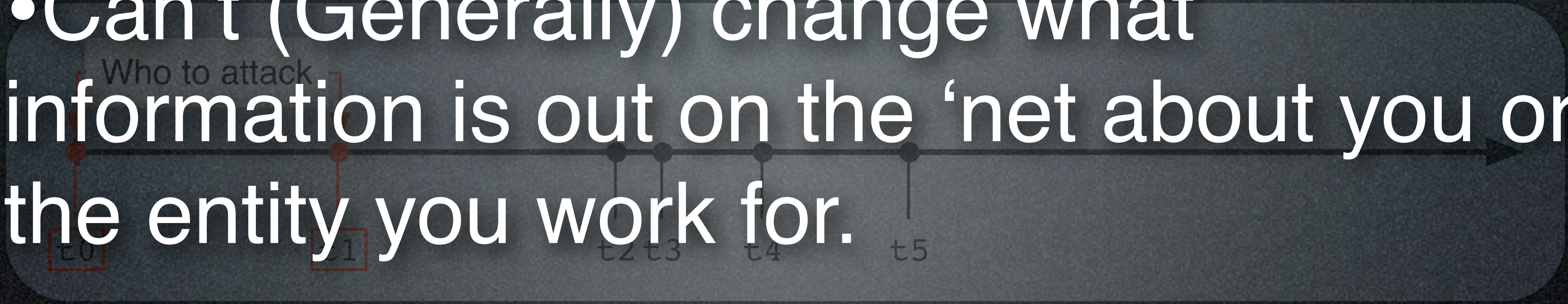


(c) 2012 sandSecurity

Who to attack Mitigations...

- Can’t change what kind of entity you work for ...

- Can’t (Generally) change what information is out on the ‘net about you or the entity you work for.



- Can change which entity you work for .. but that’s perilous in these economic times.

Who to attack

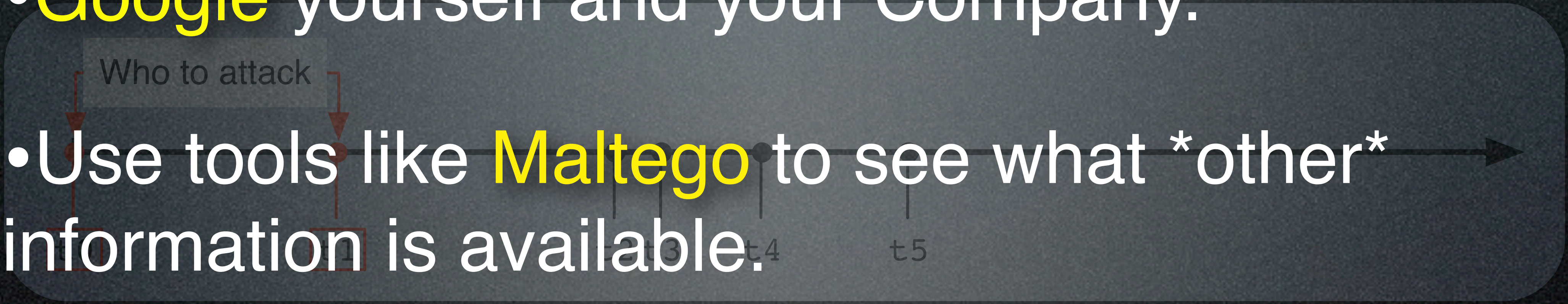
Who to attack
t0
t1
t2
t3
t4
t5

Baseline!

(c) 2012 sandSecurity

Who to attack Mitigations...

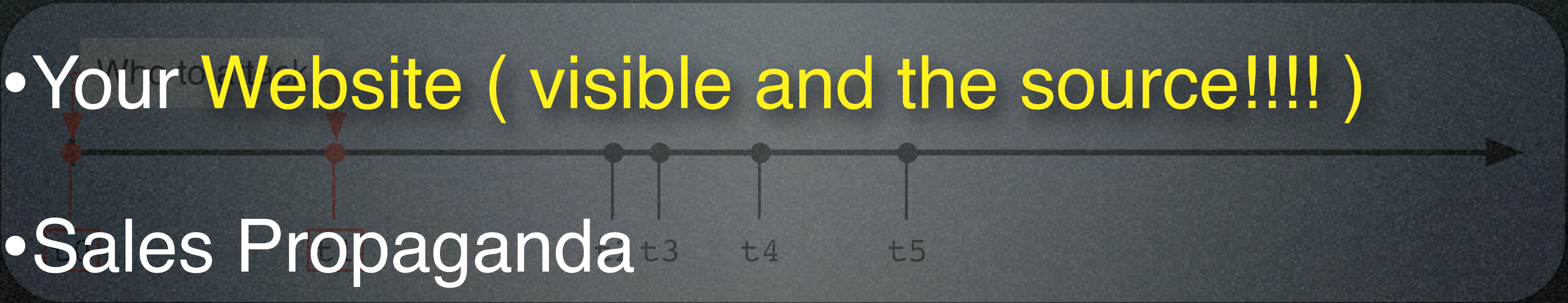
- Check Information Services on the ‘net often!
  - Google yourself and your Company.
  - Use tools like Maltego to see what *other* information is available.



  - Scan the social networks for information related to your company.

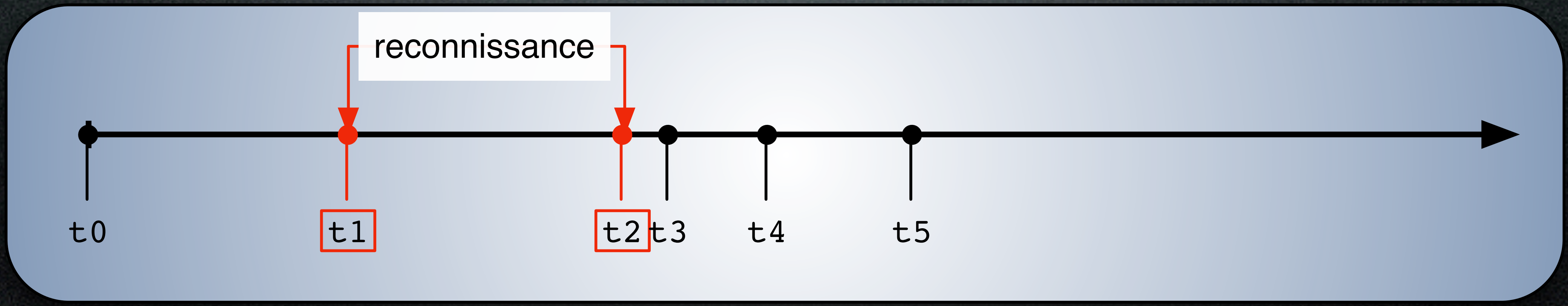
Who to attack Mitigations...

- Critically examine publicly available information



  - Your Website (visible and the source!!!!)
  - Sales Propaganda
  - White Papers

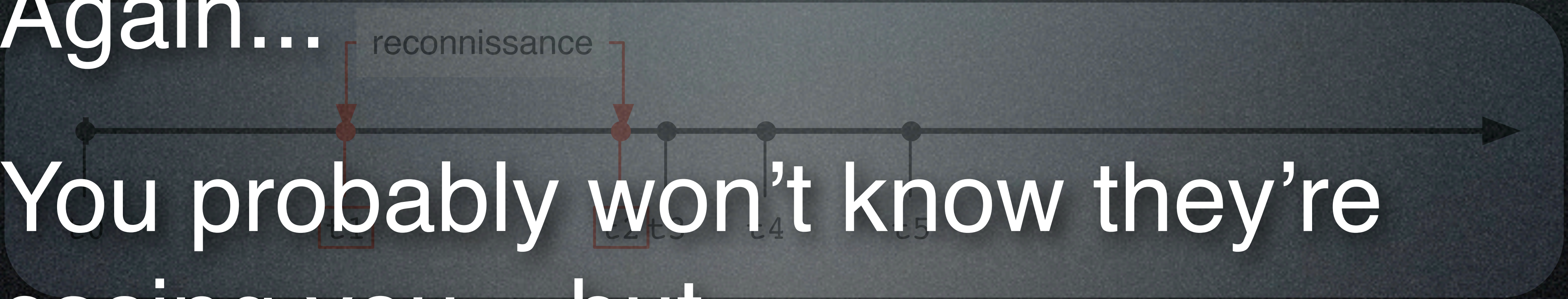
Timeline



(c) 2012 sandSecurity

t2 - Reconnaissance

Again...

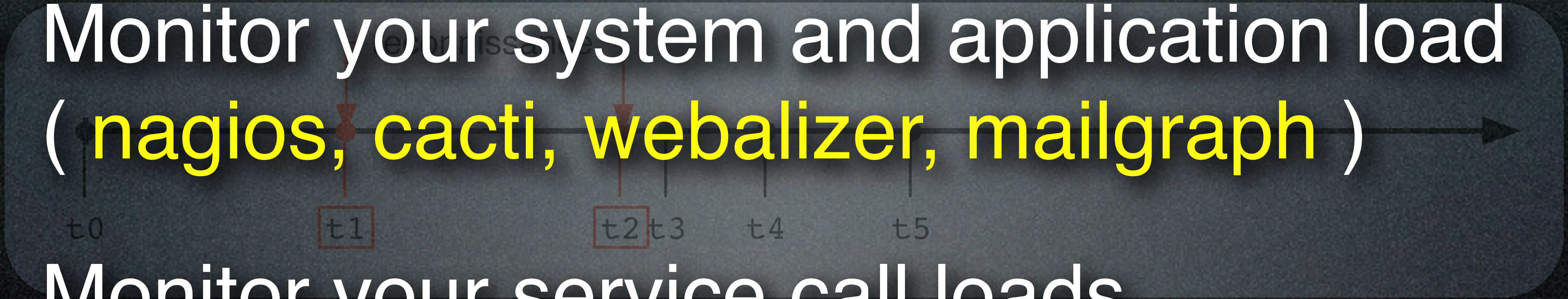


You probably won’t know they’re casing you .. but ..

Baseline!

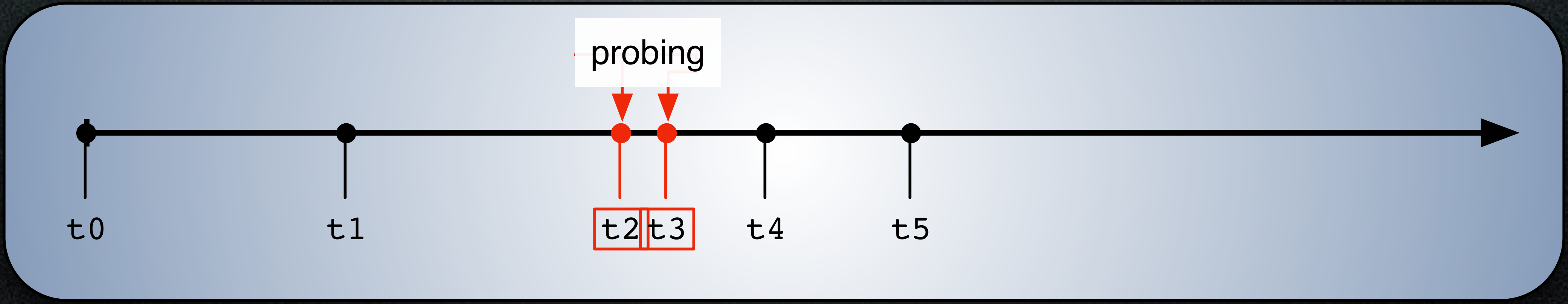
t2 - Reconnaissance

- Monitor your application logs (logly, logzilla, splunk)
- Monitor your system and application load (nagios, cacti, webalizer, mailgraph)



- Monitor your service call loads
  - use an issue tracking system! (trac, RT, Tivoli)

Timeline



(c) 2012 sandSecurity

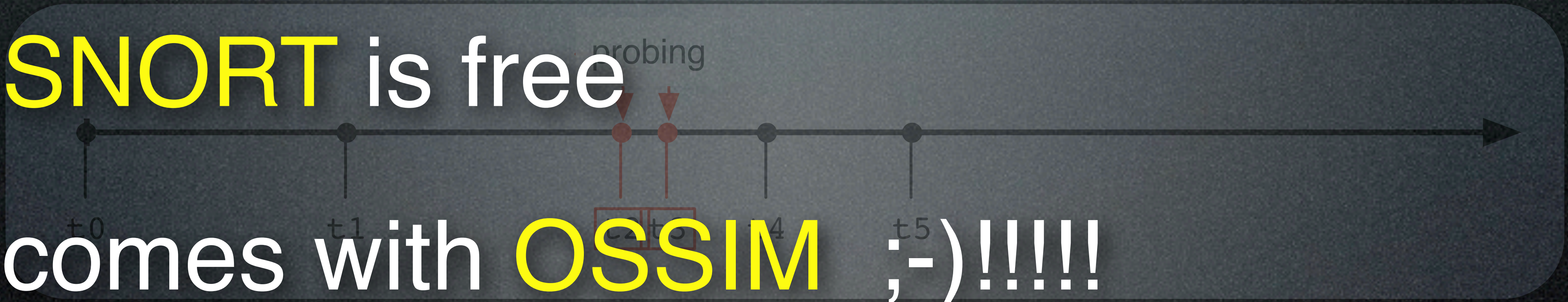
Sunday, January 29, 12

How will you know you’re being probed?

Baseline!

t3 - Probing

- Install an IDS
- SNORT is free
- comes with OSSIM ;-)!!!!!



(it’s not that hard ;-)

t3 - Probing

- Review Application Logs
  - maillog (awstats, mailgraph)
  - httpd (webalizer)
  - EventLog (EventLogExplorer)

probing
t0
t1
t2
t3
t4
t5

t3 - Probing

- Review System Logs
  - kernel, security logs (logwatch)
  - packet monitoring (ntop)

probing
t0
t1
t2
t3
t4
t5

t3 - Probing

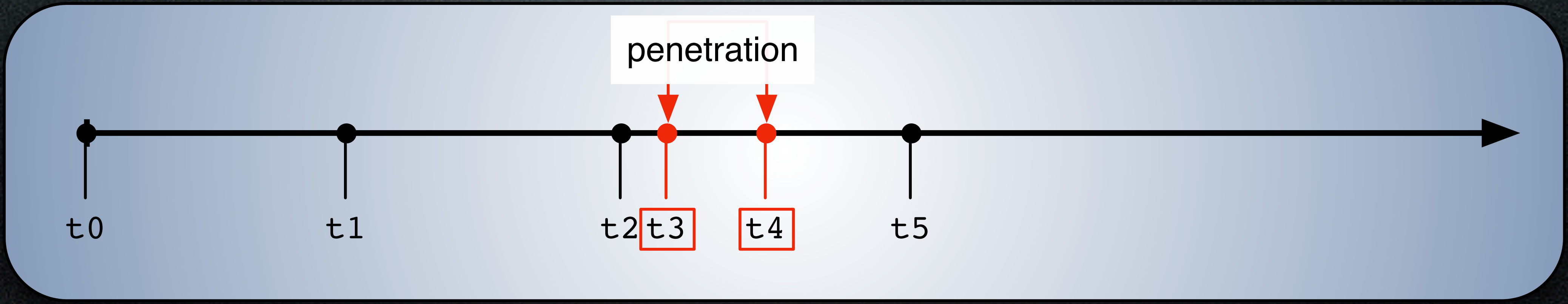
- Aggregate information

probing
t0
t1
t2
t3
t4
t5

  - Centralize System logs
  - install OSSIM

(it’s easy and free... ;-)

Timeline



How will you know you’re being penetrated?

Baseline!

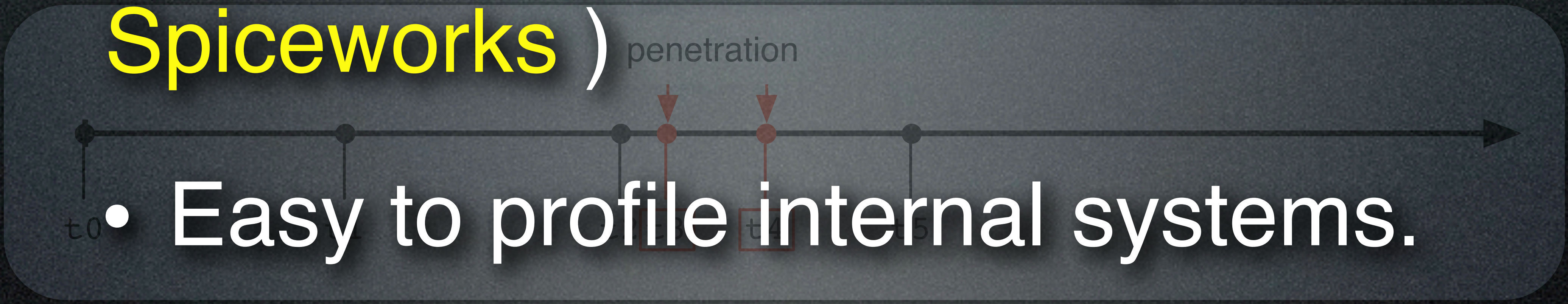
t4 - penetration

Network Monitoring..

- IDS on the *inside*
  - Way easier to baseline than external!
- Monitor interior traffic! (ntop, snort)
- Monitor network devices (OSSIM, Cacti)
- Manage signal-to-noise

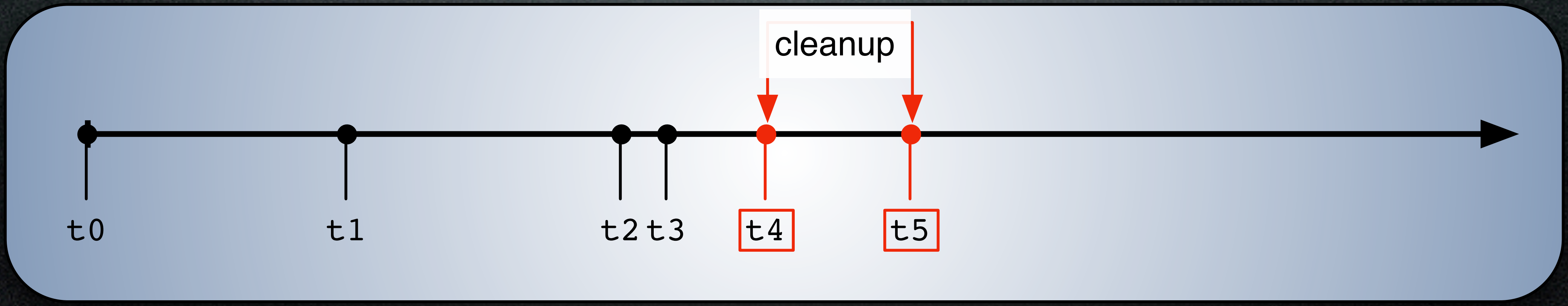
t4 - penetration

- System Monitoring
  - Load, Diskspace, etc (Nagios, Spiceworks)



    - Easy to profile internal systems.
  - Changes to key files (subversion, cfengine, chef, puppet, tripwire)

Timeline



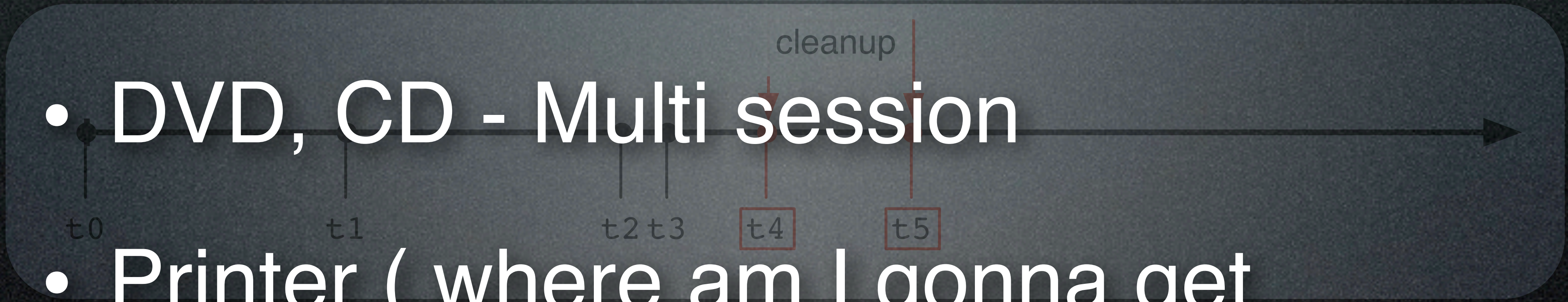
(c) 2012 sandSecurity

Sunday, January 29, 12

t5 - Cleanup

Centralize Information

- Archive to non-writable media

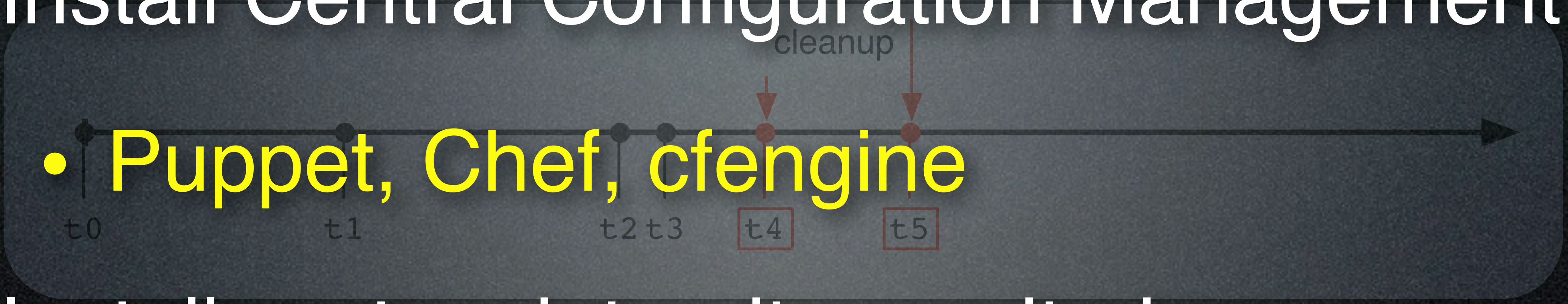


  - DVD, CD - Multi session
  - Printer (where am I gonna get greenbar?!?)
  - Isolated Access Machines (they exist?)

t5 - Cleanup

Monitor for Change

- Install Central Configuration Management
  - Puppet, Chef, cfengine
- Install system integrity monitoring
  - tripwire, OSSEC, osiris



t5 - Cleanup

Have A Plan

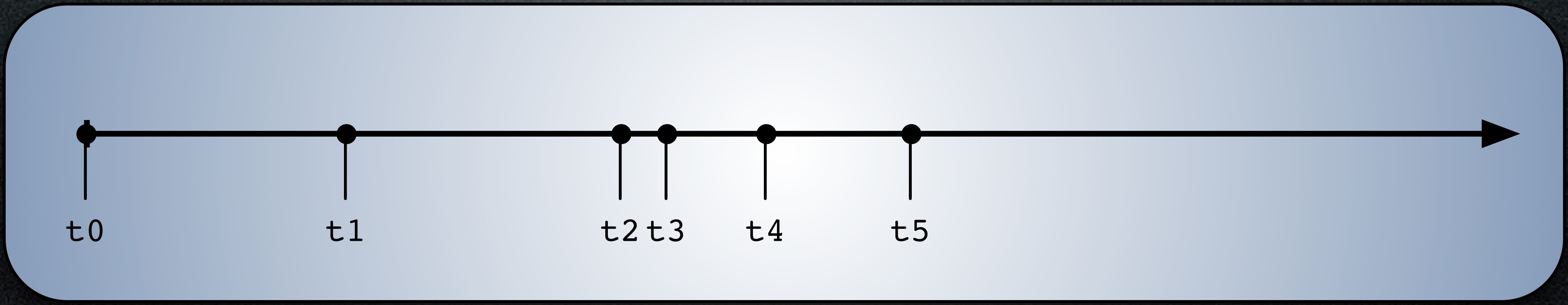
- Meet with Data and Business owners and build a Reaction Plan.
- Create a Security Awareness Plan for your associates.

In Summary
Let me ‘splain...

No ... there is too much,
let me sum up!

Timeline

- Your TTL is dependent on how involved you are with the information that's available.

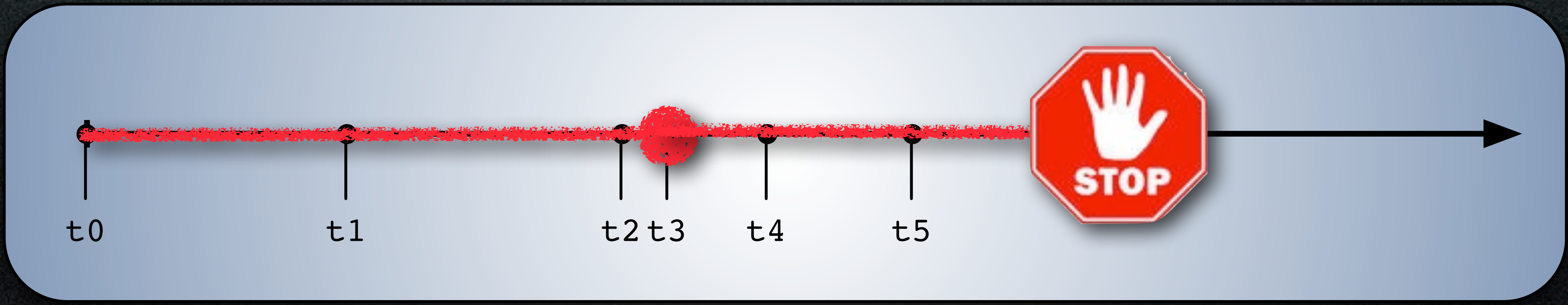


VS.

(c) 2012 sandSecurity

Timeline

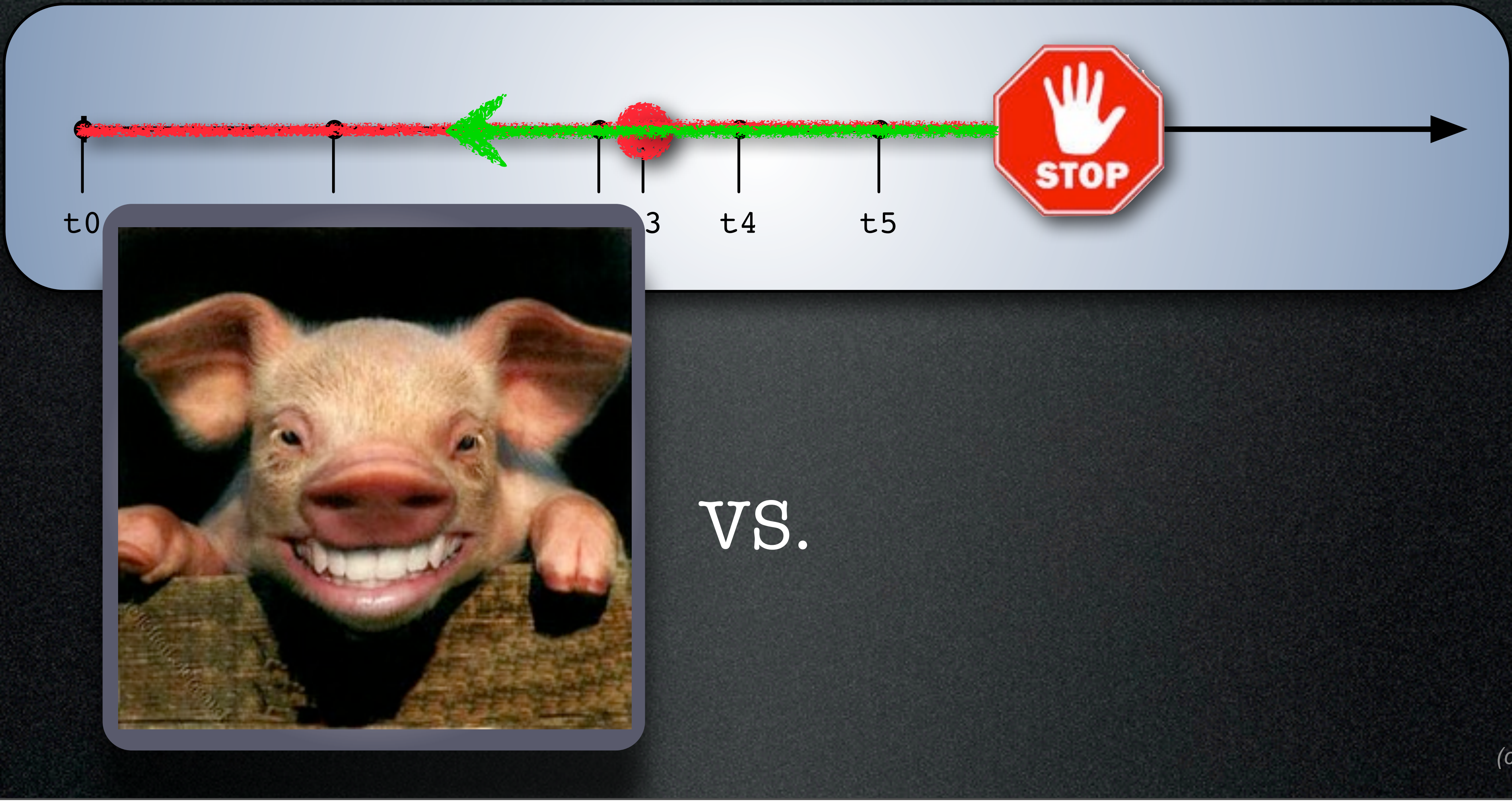
- Your TTL is dependent on how involved you are with the information that's available.



vs.

Timeline

- Your TTL is dependent on how involved you are with the information that’s available.

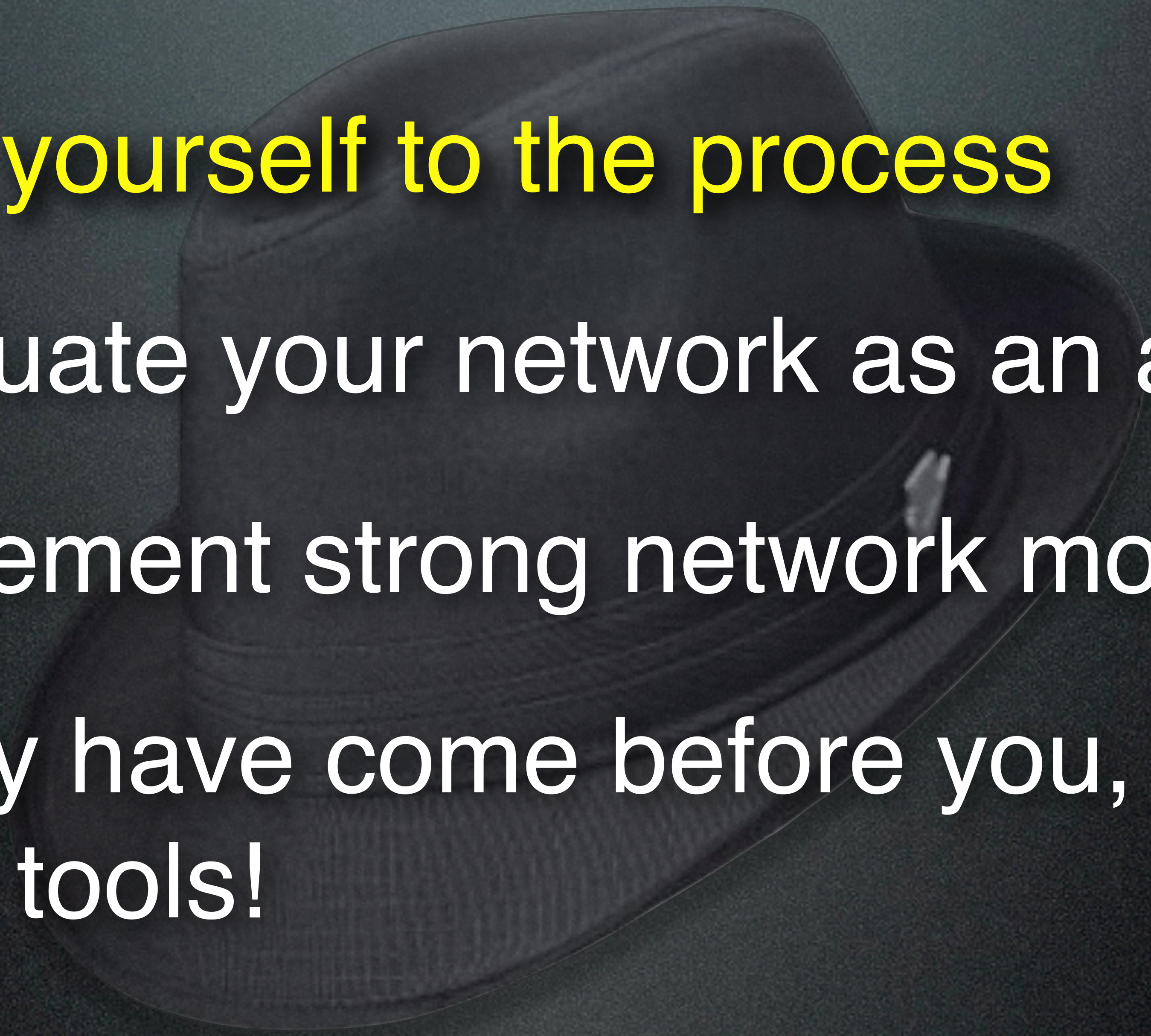


vs.

Minimizing t1 -> detection

- Insert yourself to the process
  - Evaluate your network as an attacker
  - Implement strong network monitoring
  - Many have come before you, use their tools!

Minimizing t1 -> detection

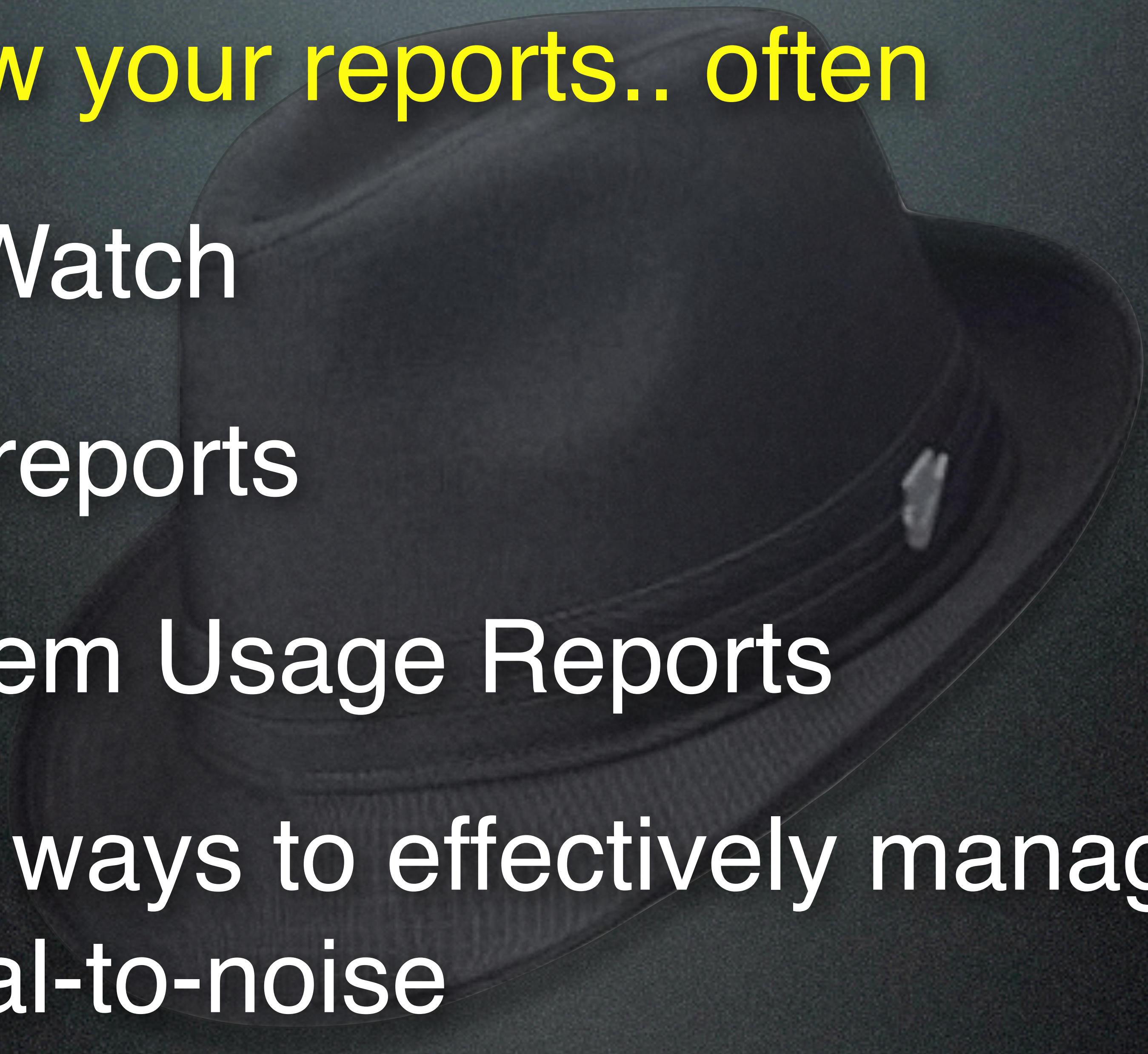


- Insert yourself to the process
  - Evaluate your network as an attacker
  - Implement strong network monitoring
  - Many have come before you, use their tools!

Minimizing t1 -> detection

- Review your reports.. often
  - LogWatch
  - IDS reports
  - System Usage Reports
  - Find ways to effectively manage signal-to-noise

Minimizing t1 -> detection

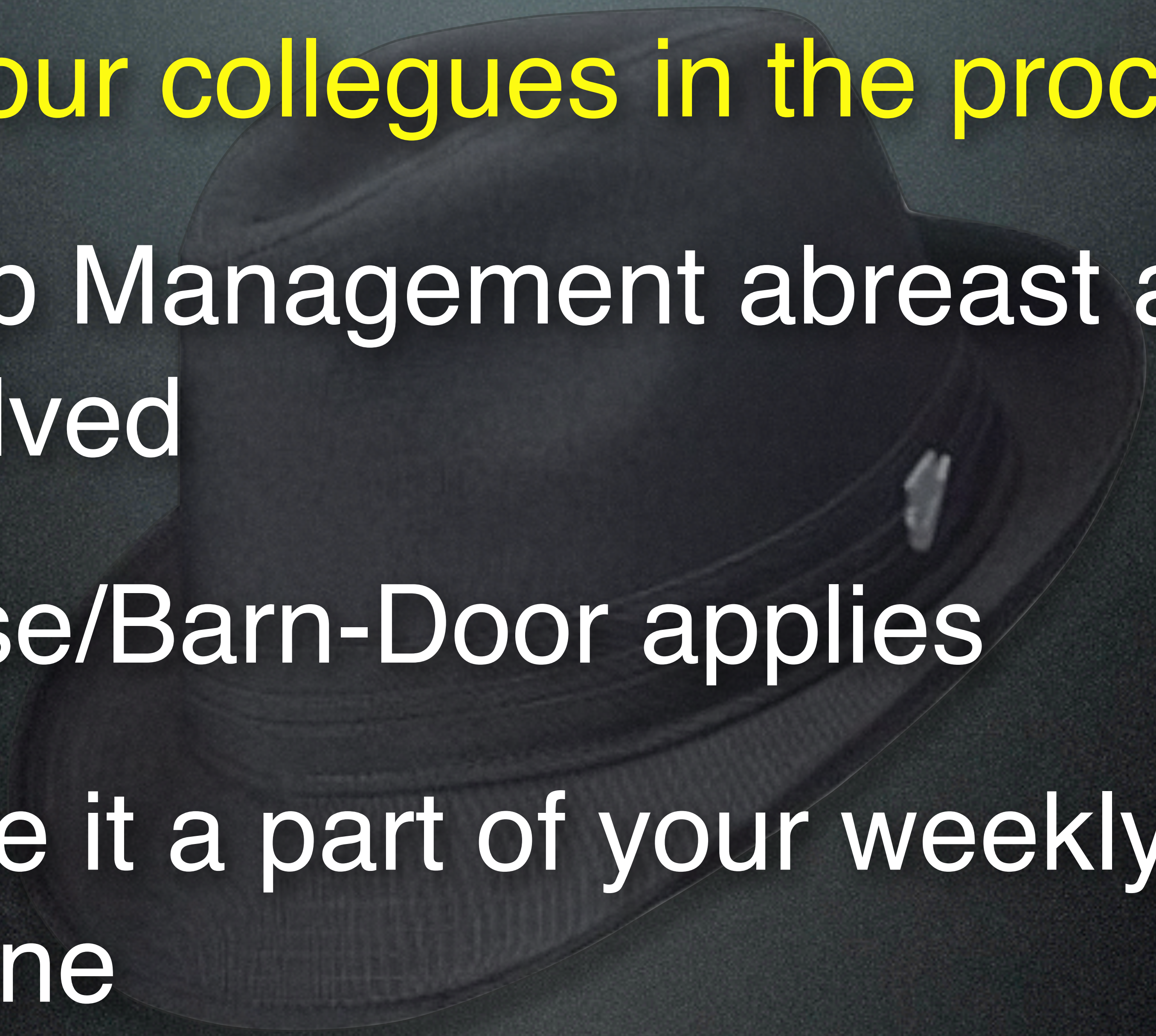


- Review your reports.. often
  - LogWatch
  - IDS reports
  - System Usage Reports
  - Find ways to effectively manage signal-to-noise

Minimizing t1-> detection

- Get your collegues in the process
  - Keep Management abreast and involved
  - Horse/Barn-Door applies
  - Make it a part of your weekly work routine

Minimizing t1-> detection

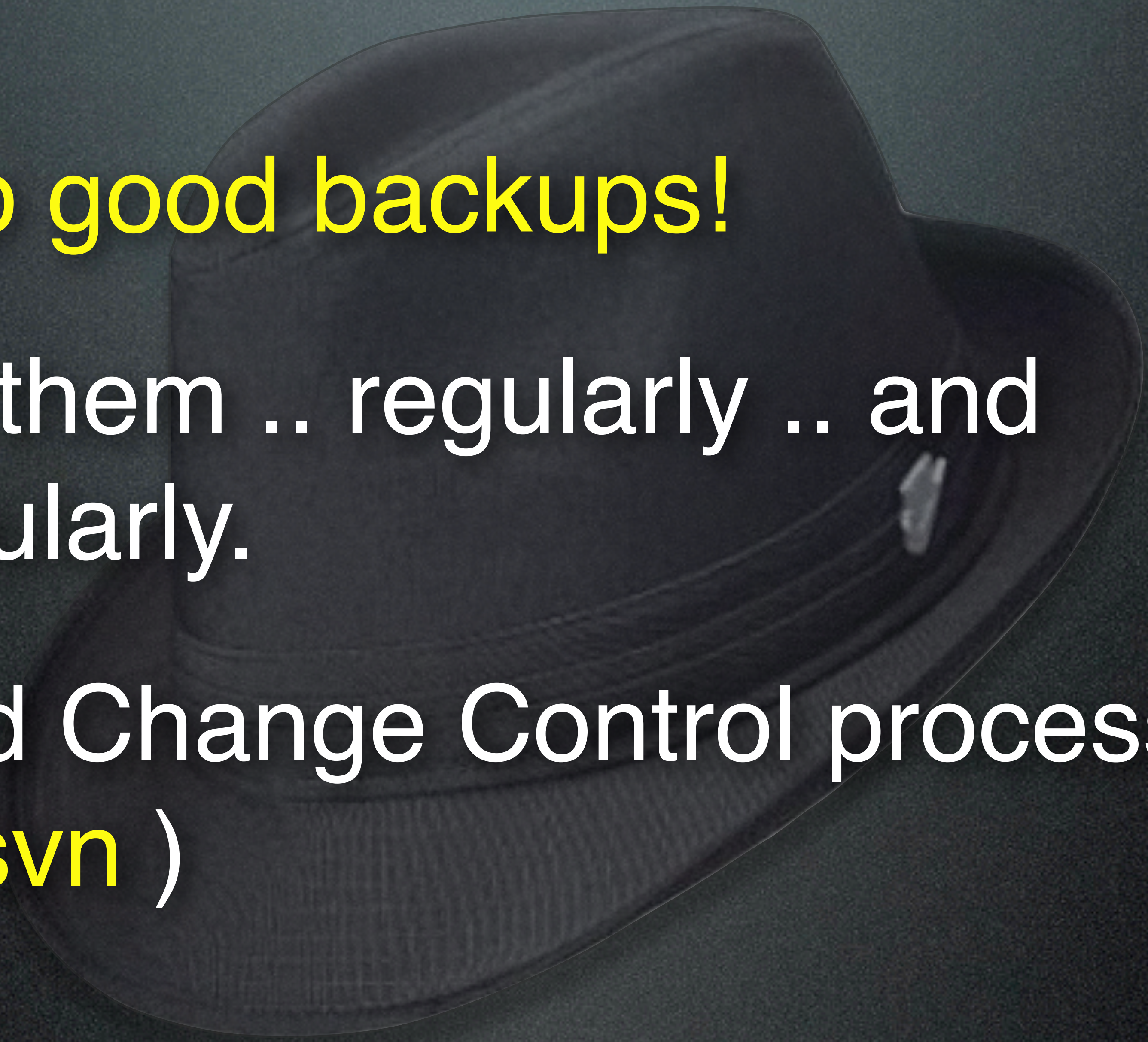


- Get your collegues in the process
  - Keep Management abreast and involved
  - Horse/Barn-Door applies
  - Make it a part of your weekly work routine

Minimizing t4-> cleanup

- Keep good backups!
- Test them .. regularly .. and irregularly.
- Good Change Control processes (I like svn)

Minimizing t4-> cleanup



- Keep good backups!
- Test them .. regularly .. and irregularly.
- Good Change Control processes (I like svn)

In Short ...

Stay Involved.

Stay Involved.

And....

Baseline!!!!

Questions?

@sandinak

Branson Matheson

branson [at] sandsite.org