Have you filled in the speaker evaluation form?

Sexy Defense

Maximizing the Home-Field Advantage

Iftach Ian Amit

Image credit: IDF Spokesperson

Agenda

- Whoami
- Background - the Red Team was here...
- What do they actually say? Reading reports 101
- Methodology - flipping the Red-Team
- Map
- Correlate
- Act
- Examples
- Conclusions

Iftach Ian Amit

Background

You had a vulnerability assessment done.

Background

And you passed a pentest.

Background

What did you ACTUALLY get?

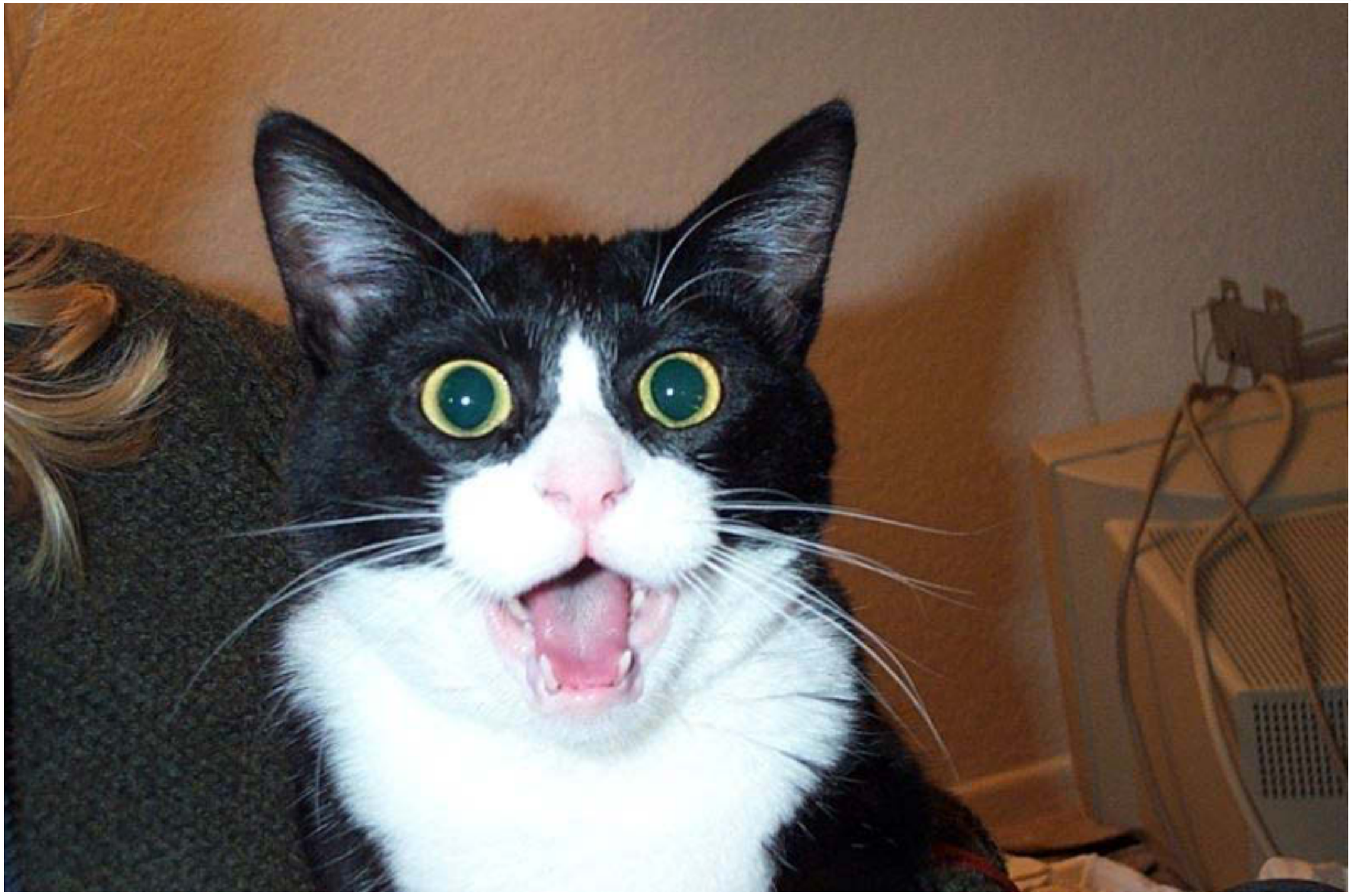
Pros	Cons
Compliance? +++	Security Posture? ---

Background

And then you had a Red-Team test come in and wreck havoc...

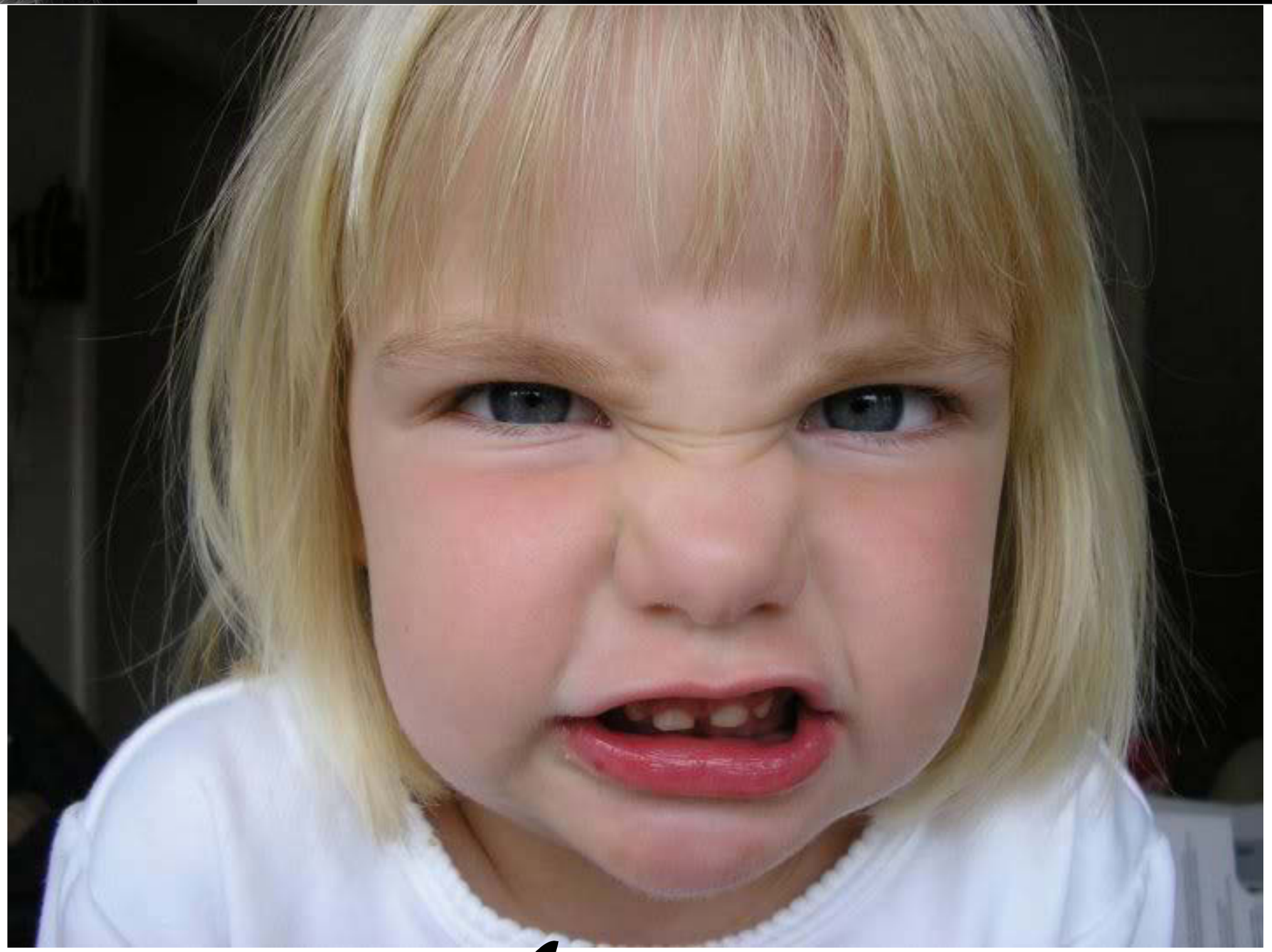
Background

How does that make you feel?



Shock

Denial



Anger

Resistance

Acceptance?

Reading bad reports

- Here comes the boring part... Terminology...
  - vulnerability
  - exposure
  - threat
  - risk
  - (yeah - you gotta be able to do suite talk to get the $$$).

Vulnerability

You'll find a lot of these in reports...

"An issue with a **software** component that, when abused (exploited) can lead to anything from the software crashing, to compromising the system on which the software is installed so that the attacker can have full control over it. Additionally, vulnerabilities also refer to **logic** and **operational** issues – whether in **computing systems**, in **processes** and **procedures** related to the **business** operations, patch management, or even password policies."

Exposure

- Say what?
- Usually will connect **vulnerabilities** to a **threat model** relevant for the tested organization

Threat

"Anything capable of acting against an asset in a manner that could result in harm"

Defined by: Threat Community, Threat Agents.

- Capabilities
- Accessibility to assets

Risk

Ever seen one of these in a report? A **real** one?

- The **probability** of *something bad*™ happening to an organization's asset.
  - Yes, **probability** == math. Coherently formulate the elements (vuln, exposure, threat) into a risk score.
    - Repeatable, and defensible from a logical perspective

Methodology

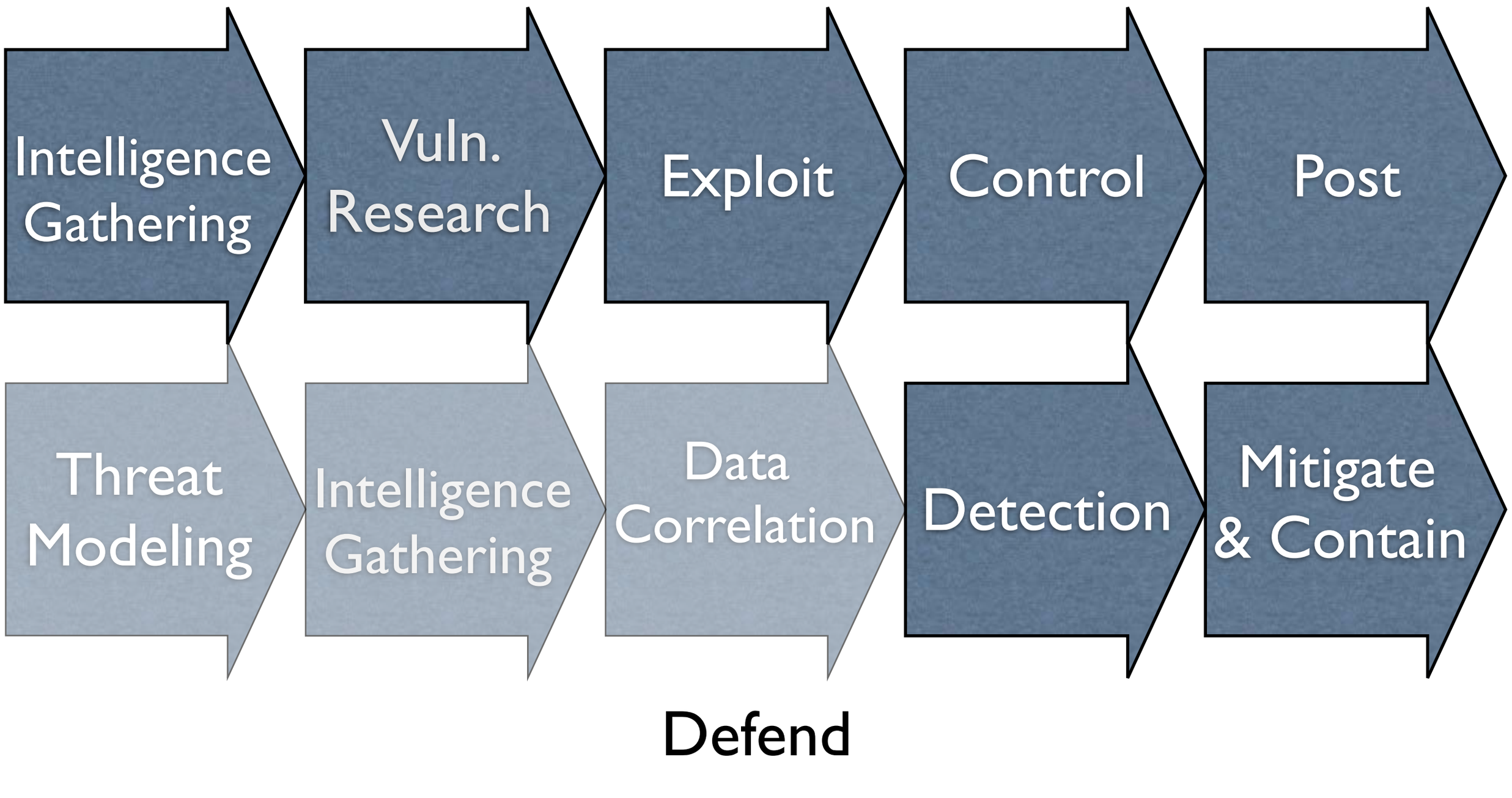
Take a look at how we have been practicing attack and defense.

For a VERY long time...

Defender view

Attacker view

What it means?



Remember!

It's not about:

- Egos
- People
- Skills

IT'S NOT FAIR!

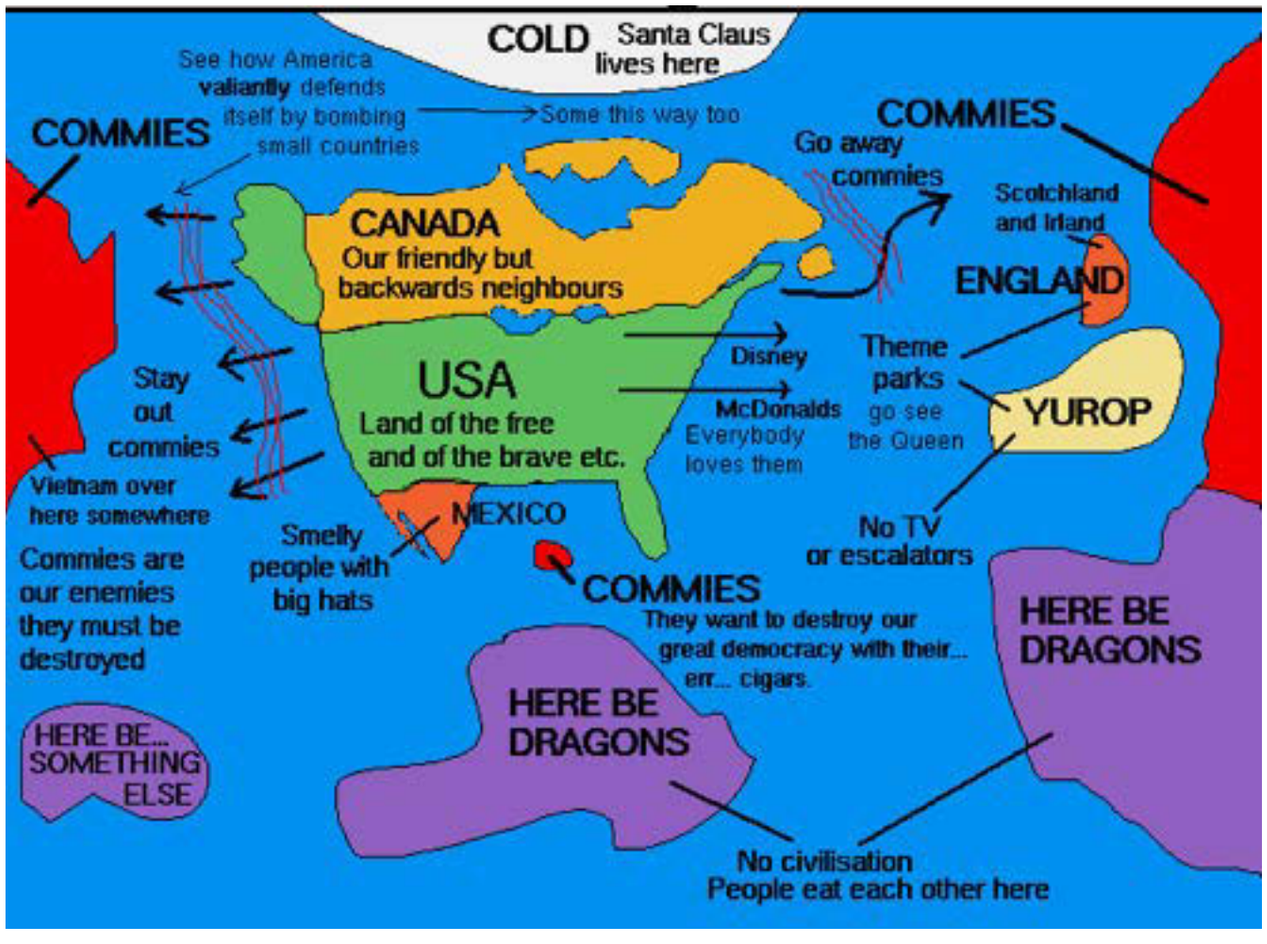
Having a mindset of constant improvement

There will always be gaps in the defense

- Identify
- Remediate
  - In the CONTEXT of RISK

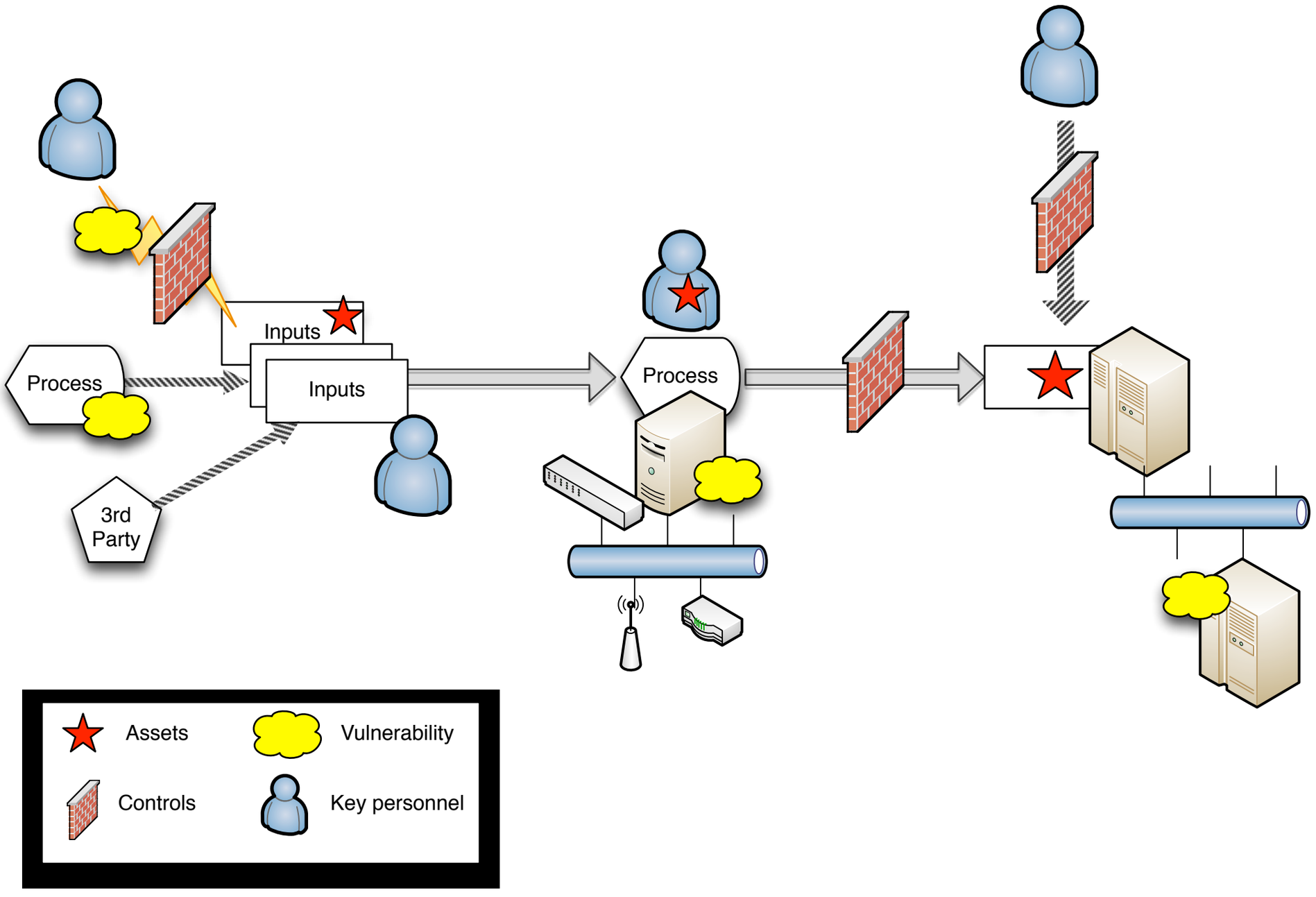
Map (information & Security assets)

- 1st - What is the **business** doing anyway?
  - How does it make **$**?
  - Processes, assets, people, technology, 3rd parties...
- **Security** and **Intelligence** assets...



Map (exposures & Issues)

- Start from a report (vuln, pt, red-team).
  - Work up from there while weeding out all the irrelevancies



- Simplified mapping of assets, processes, people, vulnerabilities, and controls

Logs

- Everywhere, from everything.
- Storage != $
- Measure twice, cut once == get all logs, filter later

Raw intelligence

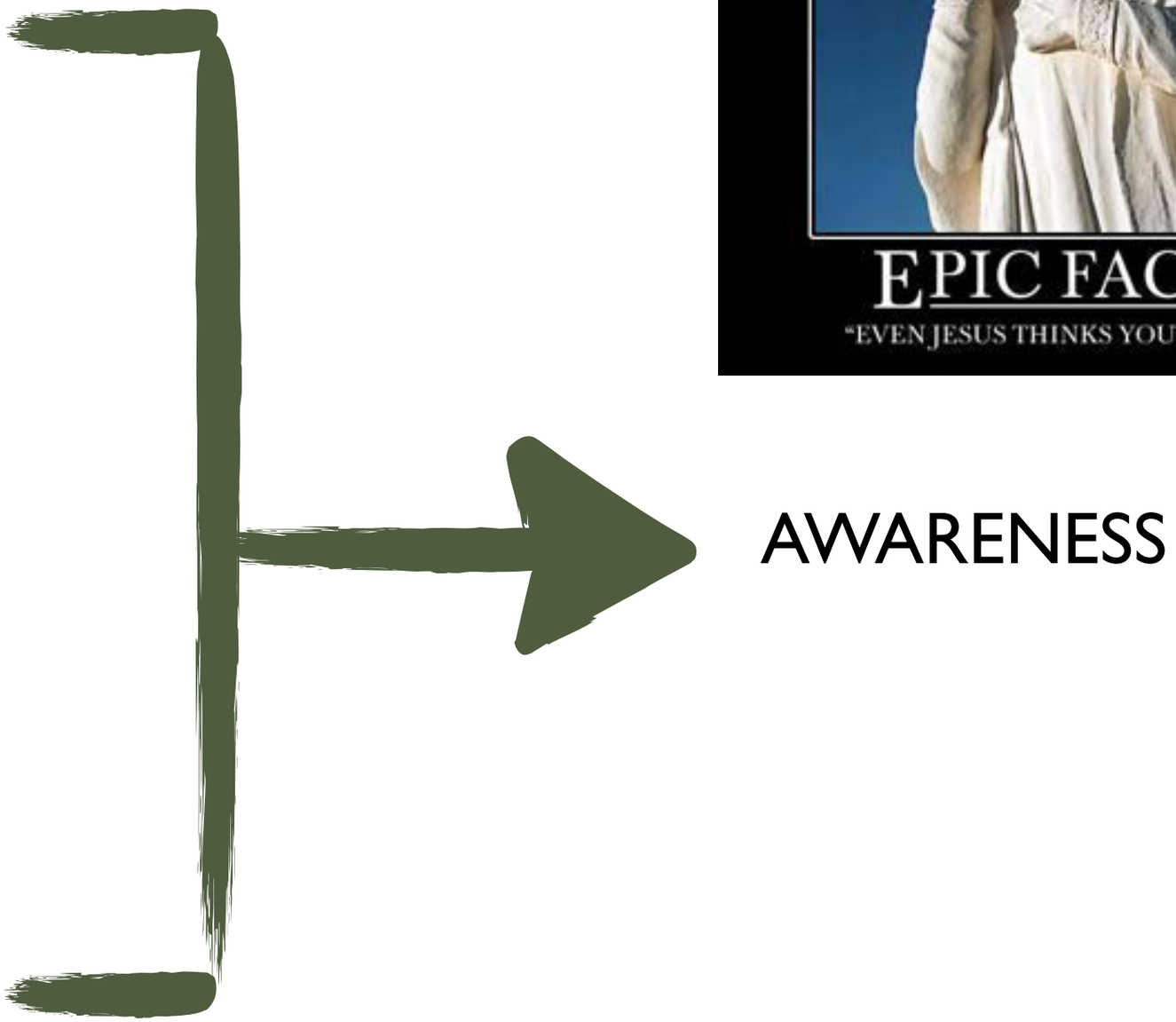
- Marketing
- Sales
- Business Development
- Competitors
- Partners
- Customers
- Analysis
- CERTS
- Market news
- Forums

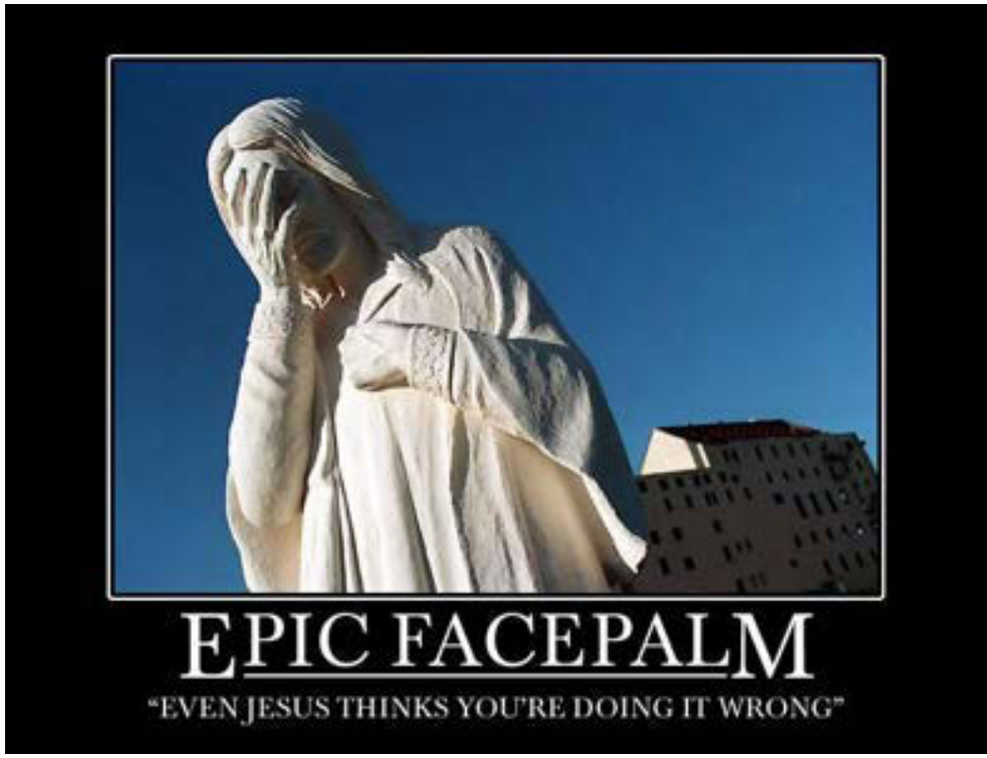
Early warning signs

- Weird PC behavior
- Volume of calls to support
- Physical elements around the office
- Sales inquiries
- Probes on a website
- File permissions
- Access to specific files on network storage
- Employee awareness
- ...

People

- Stalkers
- Tailgaters
- Smokers
- Construction
- Sales leads
- IT guys





Correlate

external events and timelines

Local news,

Sports, entertainment, financial

Regional news

National events

International stuff

[INSERT]

Examples timeline of actual events

Act

- Building up your defense mojo
- Training people to identify, report, react
- Combining technology into the mix
- Working with others (peers, vendors, intel sources, government?)

Assess where YOU are!

- Get a clear view of your current security posture
- Lying to yourself isn't going to make you feel better
  - At least in long run... :-|

Constant development

- Expect changes
  - Processes, partners, customers, 3rd parties, internal services/products, people, culture,
- Embrace changes - **never** "sign off" into a finite strategy document. Make it a "living" document.
  - Educate people about it.
  - Show how it adapts according to the business. TO SUPPORT IT!

Align outwards

- Compare notes with peers
- Keep track of what's new on the offensive side
  - And how it relates to you
- Never accept a successful audit or compliance to regulation as a sign of effective defense
  - Will usually prove the opposite
    - Great - you are now one with the **lowest common denominator of the lowest bidders**...

It's not about:

Tech

People

Skill

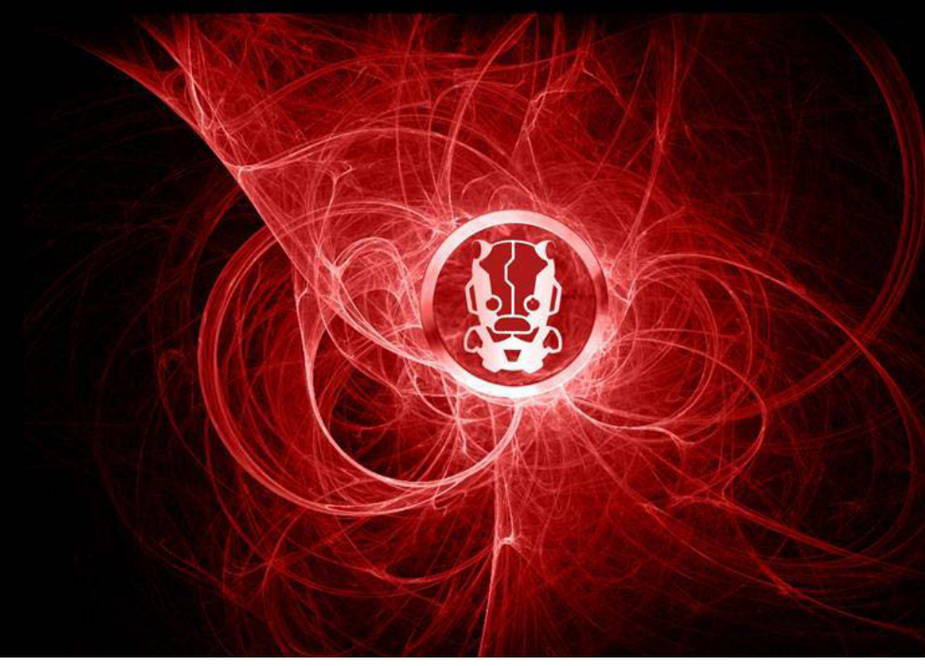
It's about:

Cat Herding

Counter-intel

- Own up to YOUR information
- Set traps
  - Intelligence
  - Technology
- Booby-trap tools, work with LE, and most importantly: LEGAL
  - IANAL!

IOActive™



Examples

1. Identify your threat communities / agents
2. Locate their "hangouts" (where they get toolz)
3. Infiltrate to get info
4. Manipulate "stuff"
    1. Backdoor it.
    2. Make sure it leaves a distinct signature.
5. Update custom signature in detection systems
6. Kick back, and watch the fun

بسم الله الرحمن الرحيم

. : منظمة الهكر العربي : .

السلام عليكم ورحمة الله وبركاته

برنـــامج Nj-RaT v0.2.2

طبعا البرنامج يستقبل الضحايا على Irc يعني مايحتاج فتح بورت ولا No-ip

المميزات

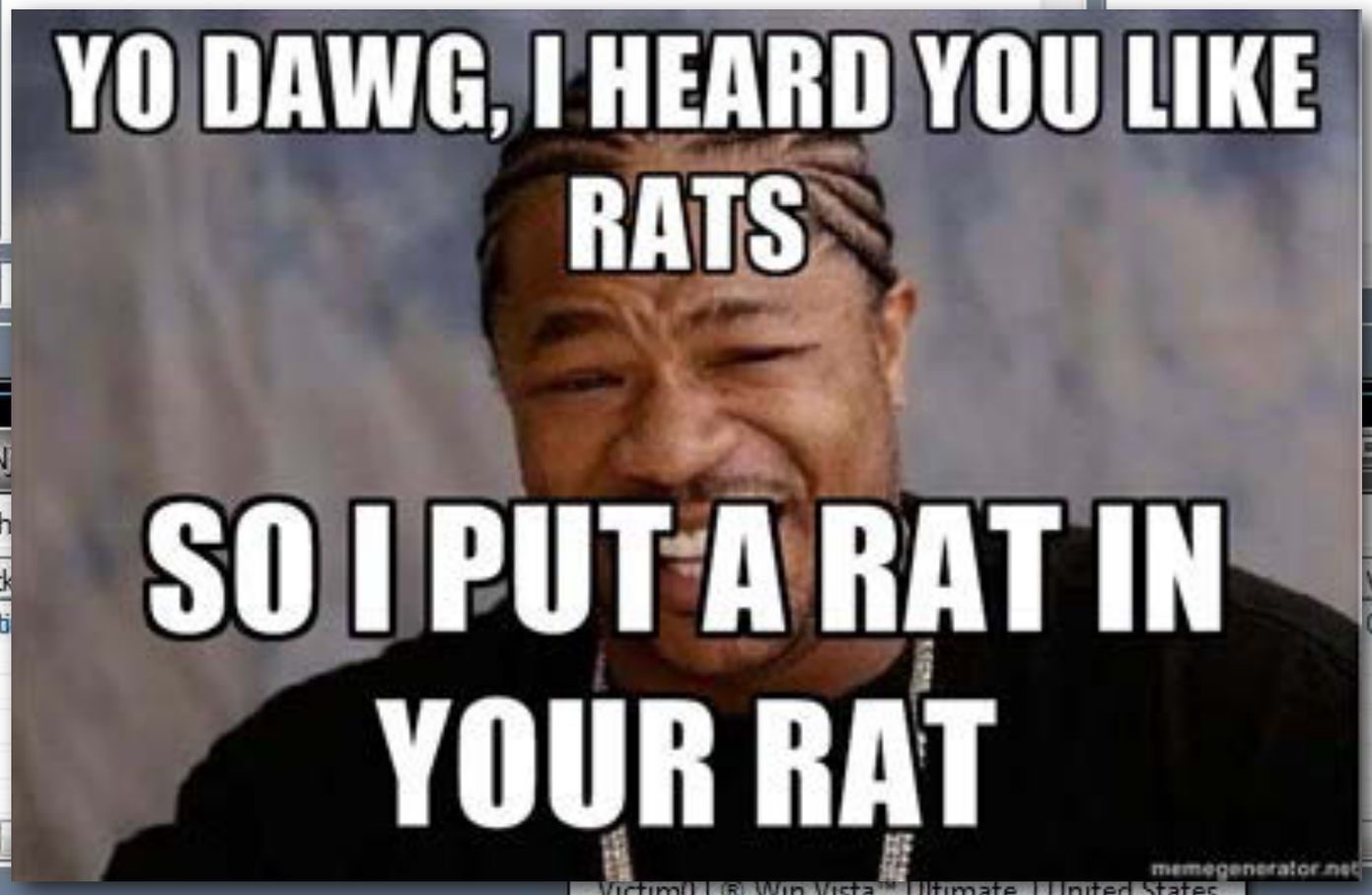
_ التبليغ على IRC
_ تصوير شاشه + الكتابه بالكيبورد
_ إداره ملفات
_ سحب باسوردات Firefox + No-ip + dynDns + Filezella + IMVU + Pidgin
_ اداره الـ Process
_ اداره النوافذ (تغير عناوين النوافذ ++ ارسال من الكيبورد الى نافذه معينه ++ إغلاق نافذه)
_ تشغيل اكواد برمجيه بجهاز الضحيه مثل VBS + CMD + BAT
_ تحميل من رابط و إختار إمتداد التشغيل >

البرنامج شغال %100 على انظمه
Win7
Vista
XP SP3
بس الانظمه الاقدم مثل Xp sp2 اوو Win2000 يحتاج تحديثات الـ framework 2.0
اتركم مع الصوور ;
يفضل تغير النك نيم و الـ Channel عند الإستخدام "

Nj-RaT v0.2.2 Beta

Channel ( ) | Victims (0) | Status | Builder | Setting

Nick njnj | Channel #nj-02j | irc.newnet.net | 6667 | Connect



Victim0 | ® Win Vista™ Ultimate | United States

Nj-RaT v0.2.2 Beta

Channel (2) | Victims (1) | Status | Builder | Setting

IRC

Host irc.newnet.net | Port 6667

Victim Nick | Hacker Nick

install

Copy

Path Temp

Demo time

1. Take RAT
2. Find appropriate location
3. Insert RAT
4. Release
5. Profit?

foro.udtools.net/showthread.php?5450-Fungus-Keylogger-FUD

+ Responder tema

Tema: Fungus Keylogger FUD

25/03/2012, 09:27

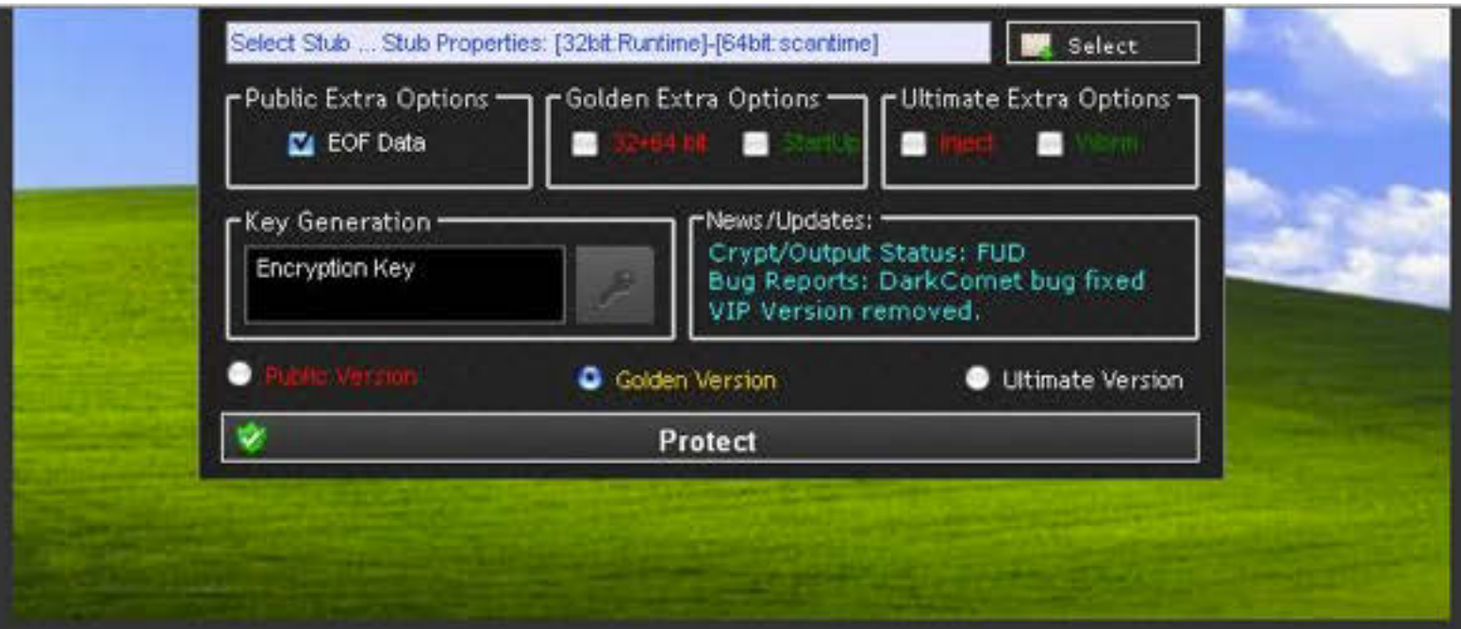
Leoric

Usuari@ Habitual

Fecha de ingreso: 23 feb, 11
Ubicación: México
Mensajes: 548

Fungus Keylogger FUD

Hola señores de Udtools,
les traigo esta humilde modificación que terminé hace un par de minutos..
No es la gran cosa, pero bueno.. hago la lucha :)



[•]Selection of stub. [3 Stubs Included]
[•]Encryption Key (Generate)
[•]Clean & Professional GUI.
[•]Small .Net 2.0 Dependency
[•]Scan & Runtime FUD
[•]Works on all Windows OS (XP/Vista/7)
[•]Strong Encryption
[•]Crypts 100% FUD Output
and much more.

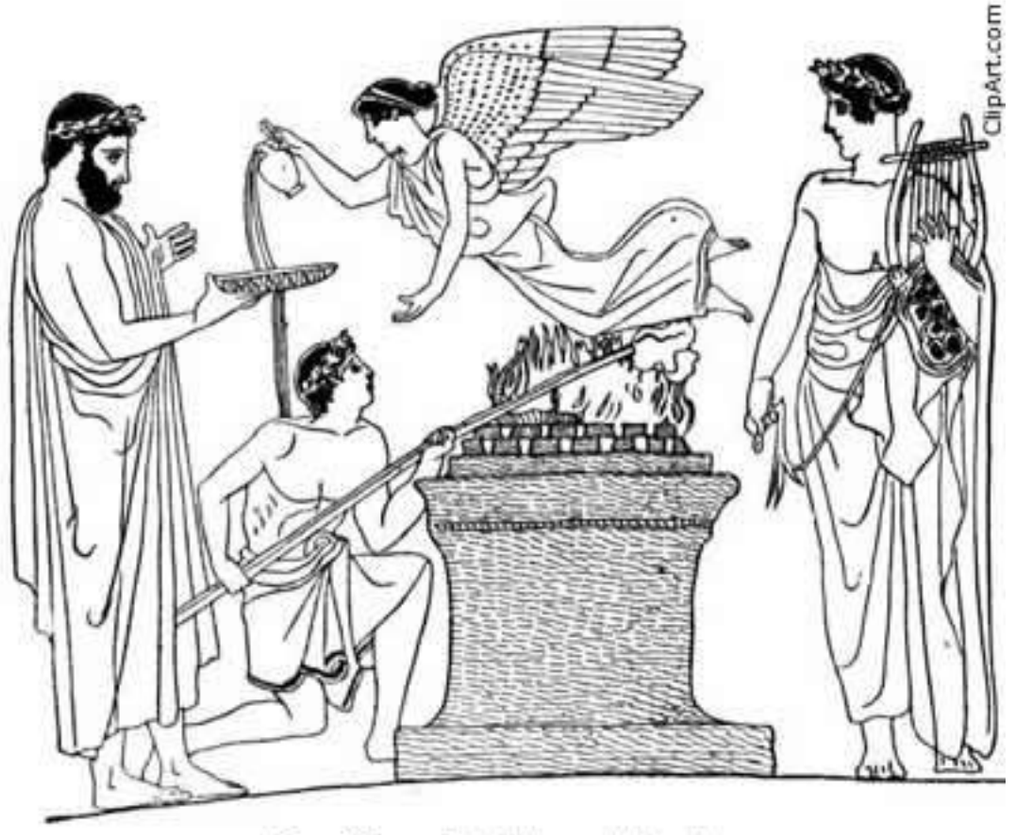
Scan url: http://vscan.novirusthanks.org/analysis/17186851a939f50457b1e1bc8a2c1367/aGYtaG9wc2luLWV4ZQ==/

Download:
http://www.mediafire.com/?129a7qm95n717f3
or
http://incredible-downloads.net

You can request 1 password of 1 stub only. Do NOT PM me.
P.S I'll send the password(s) to the ones i feel they deserve to. Your post amount nor your reputation counts so don't bother or whine. I can deny anyone for any reason.

Demo

1. Obtain crypter
2. Enhance [not in this demo]
3. Embed RAT
4. Release
5. Profit?



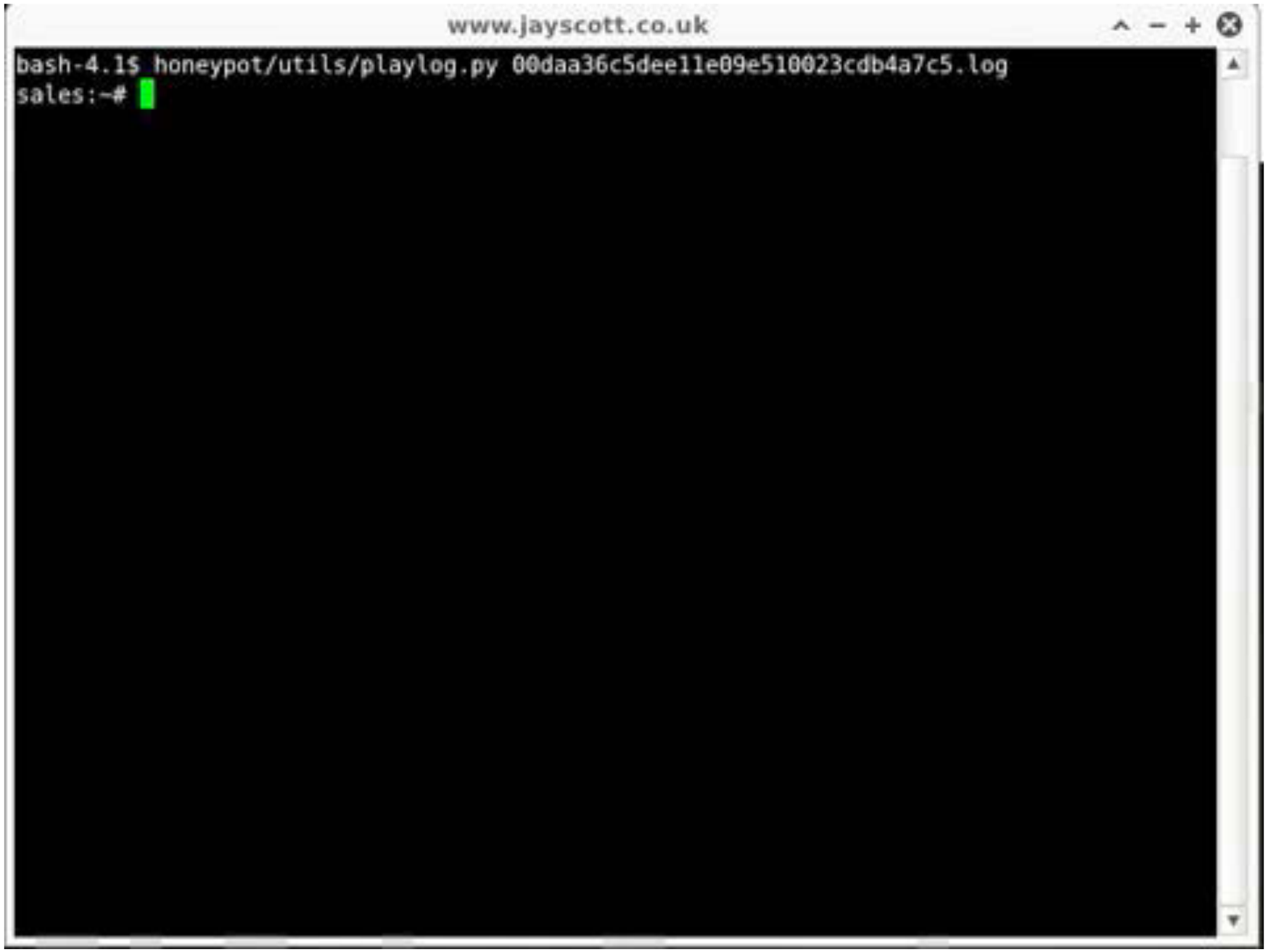
Sacrifice with Nike and Apollo

Law is hackable

- Don't think that it's impossible to get by with these things...

- Example: Microsoft's takedown of Bredolab - legal bypass by using **trademark infringement** claims
  - Directly affect infected computers!

Kippo



http://code.google.com/p/kippo/

Artillery

- Open up listeners on multiple ports
- Anything that touches them gets blacklisted
  - You can play with this to report instead of blacklist...
- Monitor filesystem changes and email diff to you.
- Block SSH brute-force attacks

svn co http://svn.secmaniac.com/artillery artillery/

Then: Technology

- Find stuff that works FOR you. Or make it.
  - SIEM/SOC would be a major focus
  - Other correlation engines
- Feed technology all the data it can handle
  - Financial info? Semantic data? Google Alerts? --> Anything goes...

Counter Intelligence Use-Case

Situation: Financial fraud being run from dormant accounts

Data: Account that have not been accessed in over a year are used for money laundering and international transfers. Fraud is either run internally or externally (not sure).

The bait: Create several tracked accounts, add to list of dormant accounts. Make copies of list and place on several network shares.

The catch: No unauthorized access to the copies of the account list. Dormant account list accessed through internal system, user account identified and tracked. Tracked account used for international transfer of funds. Internal user's pc was taken for maintenance. Forensic investigation uncovered a Trojan installed on it. Trojan tracked back to C&C in eastern Europe while continuous activity performed from it on internal financial systems. Criminal group identified and prosecuted.

Play nice with others

CERTS

Government

Peers

Competitors

Conclusions

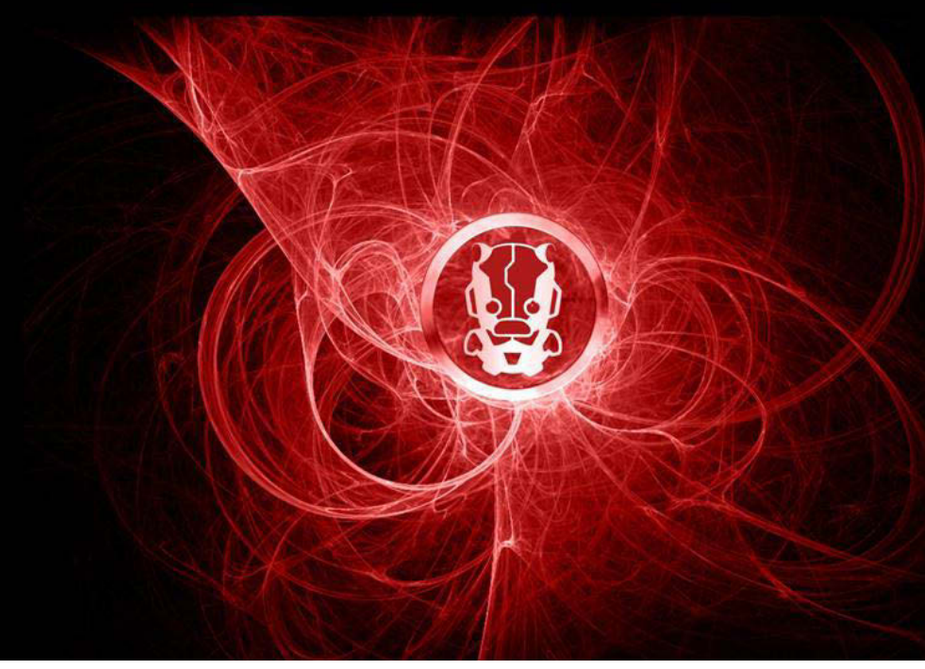
The whole is greater than the sum of its elements

Call for Action

- Vendors:
  - Start working on products that can "communicate" with information
  - Loosely typed data
  - Language processing of arbitrary data formats
  - Correlation across sources AND over time
- Defenders:
  - Own up to your data, network, and business
  - Gather intelligence on your potential adversaries
  - Focus your defenses on assets, not compliance or "best practices"
  - Take the initiative!

IOActive™

Speaker evaluation form
Y U no complete it?!



ktnxbye!
Questions?

Paper available at: http://iamit.org/docs/sexydefense.pdf

twitter: @iiamit

*Image credits: Google Images and the Internetz