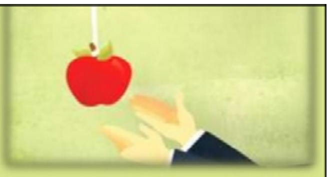
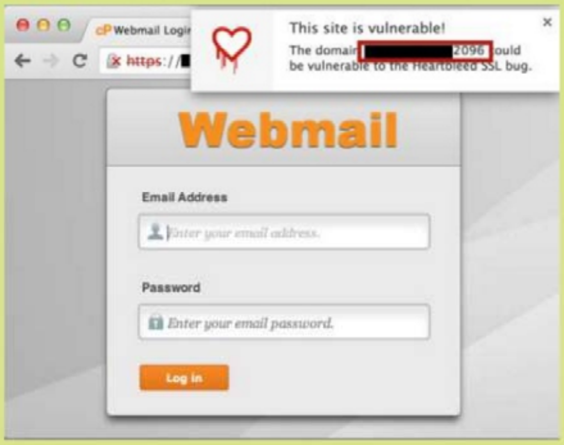
Low-Hanging Fruit

Chema Alonso

(@chemaalonso)

Low-Hanging Fruit means easy-to-find bugs





This site is vulnerable!

The domain [redacted]2096 could be vulnerable to the Heartbleed SSL bug.

Webmail

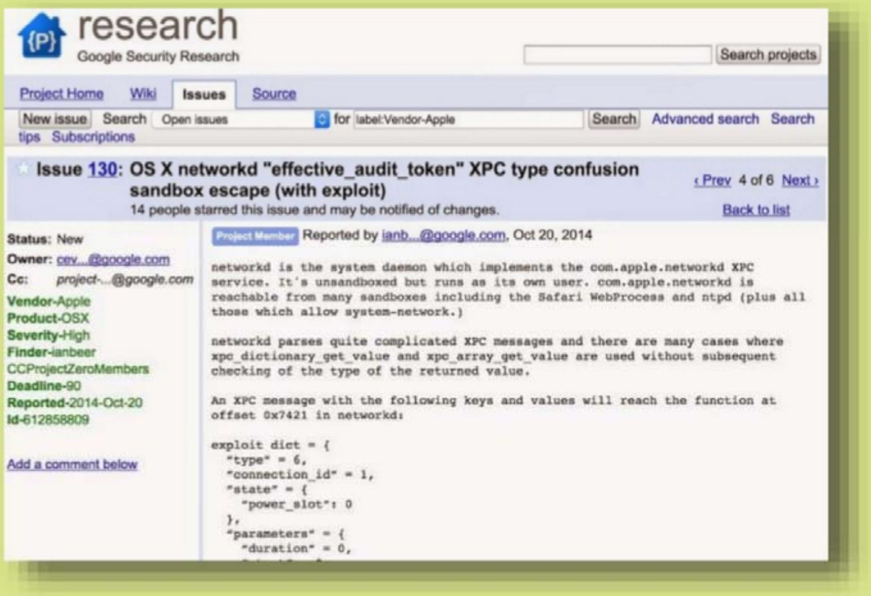
Email Address

Enter your email address.

Password

Enter your email password.

Google Project Zero



Issue 130: OS X networkd "effective_audit_token" XPC type confusion sandbox escape (with exploit)

14 people starred this issue and may be notified of changes.

Status: New
Owner: cev...@google.com
Cc: *project-...@google.com*
Vendor-Apple
Product-OSX
Severity-High
Finder-ianbeer
CCProjectZeroMembers
Deadline-90
Reported-2014-Oct-20
Id-612858809

Reported by ianb...@google.com, Oct 20, 2014

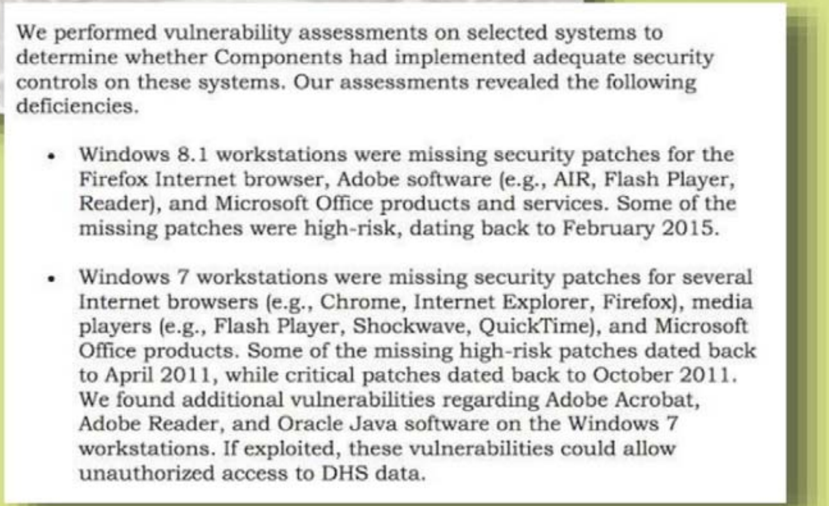
```
networkd is the system daemon which implements the com.apple.networkd XPC
service. It's unsandboxed but runs as its own user. com.apple.networkd is
reachable from many sandboxes including the Safari WebProcess and ntpd (plus all
those which allow system-network.)

networkd parses quite complicated XPC messages and there are many cases where
xpc_dictionary_get_value and xpc_array_get_value are used without subsequent
checking of the type of the returned value.

An XPC message with the following keys and values will reach the function at
offset 0x7421 in networkd:

exploit dict = {
  "type" = 6,
  "connection_id" = 1,
  "state" = {
    "power_slot": 0
  },
  "parameters" = {
    "duration" = 0,
```

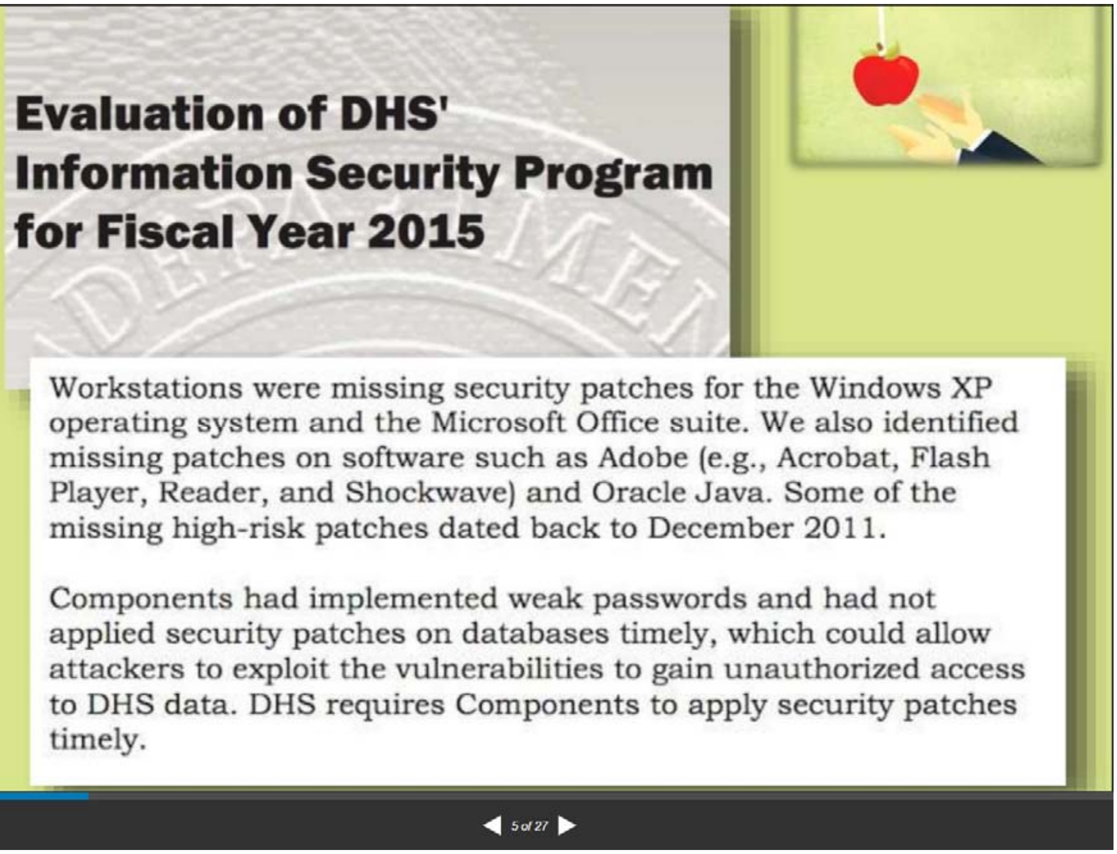
Evaluation of DHS' Information Security Program for Fiscal Year 2015



We performed vulnerability assessments on selected systems to determine whether Components had implemented adequate security controls on these systems. Our assessments revealed the following deficiencies.

- Windows 8.1 workstations were missing security patches for the Firefox Internet browser, Adobe software (e.g., AIR, Flash Player, Reader), and Microsoft Office products and services. Some of the missing patches were high-risk, dating back to February 2015.

- Windows 7 workstations were missing security patches for several Internet browsers (e.g., Chrome, Internet Explorer, Firefox), media players (e.g., Flash Player, Shockwave, QuickTime), and Microsoft Office products. Some of the missing high-risk patches dated back to April 2011, while critical patches dated back to October 2011. We found additional vulnerabilities regarding Adobe Acrobat, Adobe Reader, and Oracle Java software on the Windows 7 workstations. If exploited, these vulnerabilities could allow unauthorized access to DHS data.

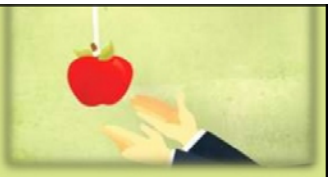


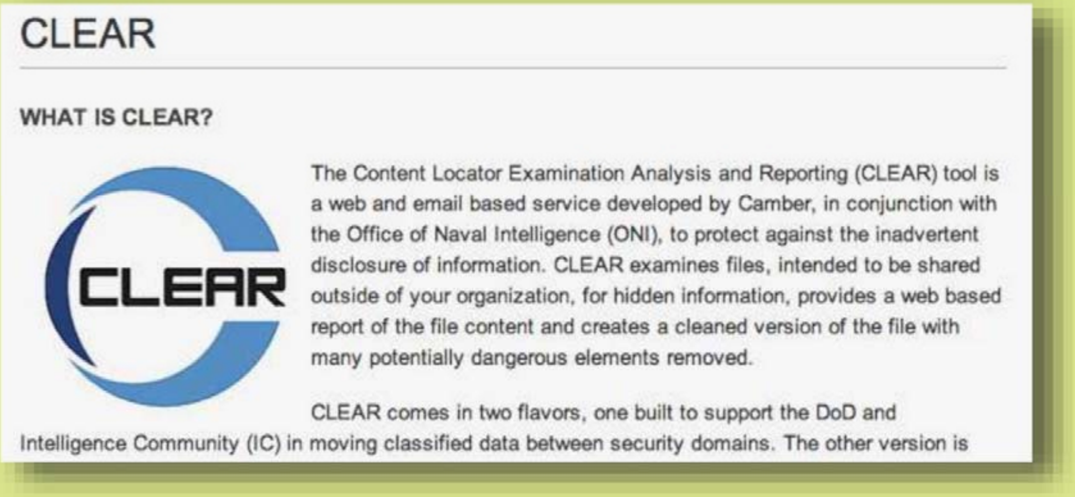
Evaluation of DHS' Information Security Program for Fiscal Year 2015

Workstations were missing security patches for the Windows XP operating system and the Microsoft Office suite. We also identified missing patches on software such as Adobe (e.g., Acrobat, Flash Player, Reader, and Shockwave) and Oracle Java. Some of the missing high-risk patches dated back to December 2011.

Components had implemented weak passwords and had not applied security patches on databases timely, which could allow attackers to exploit the vulnerabilities to gain unauthorized access to DHS data. DHS requires Components to apply security patches timely.

Clear





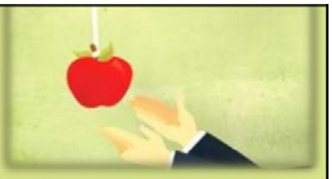
CLEAR

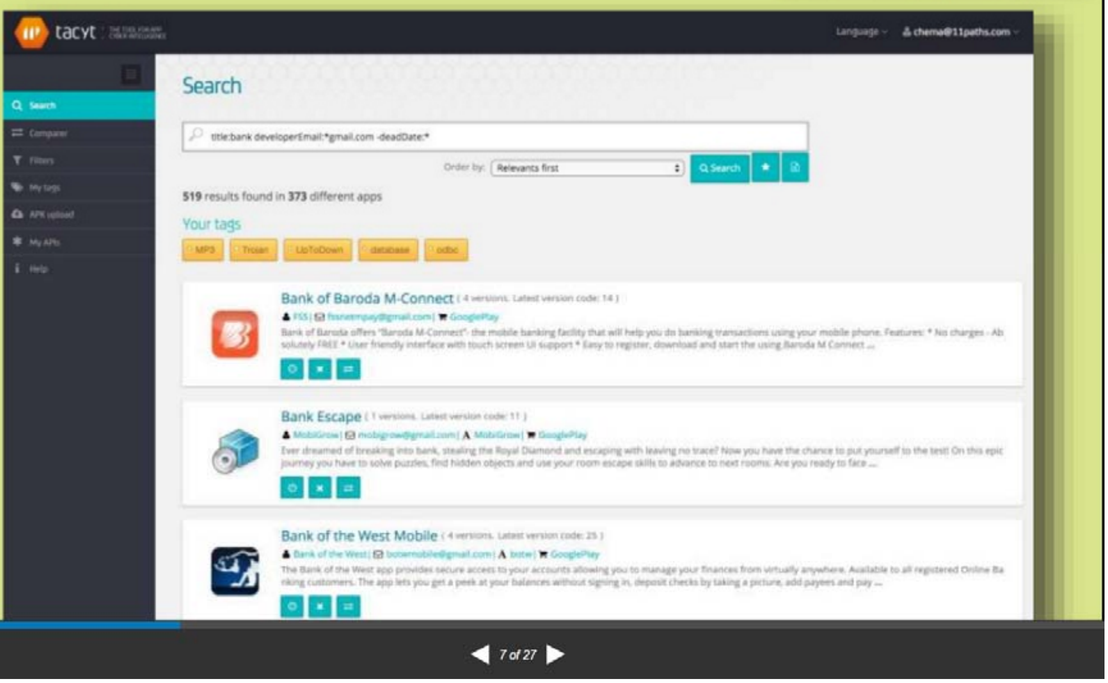
WHAT IS CLEAR?

The Content Locator Examination Analysis and Reporting (CLEAR) tool is a web and email based service developed by Camber, in conjunction with the Office of Naval Intelligence (ONI), to protect against the inadvertent disclosure of information. CLEAR examines files, intended to be shared outside of your organization, for hidden information, provides a web based report of the file content and creates a cleaned version of the file with many potentially dangerous elements removed.

CLEAR comes in two flavors, one built to support the DoD and Intelligence Community (IC) in moving classified data between security domains. The other version is

Yet another App!!





Search

title:bank developerEmail:*gmail.com -deadDate:*

Order by: Relevants first

519 results found in **373** different apps

Your tags

Bank of Baroda M-Connect (4 versions. Latest version code: 14)

FSS | fssnetmpay@gmail.com | GooglePlay

Bank of Baroda offers "Baroda M-Connect"- the mobile banking facility that will help you do banking transactions using your mobile phone. Features: * No charges - Absolutely FREE * User friendly interface with touch screen UI support * Easy to register, download and start the using Baroda M Connect ...

Bank Escape (1 versions. Latest version code: 11)

MobiGrow | mobigrow@gmail.com | MobiGrow | GooglePlay

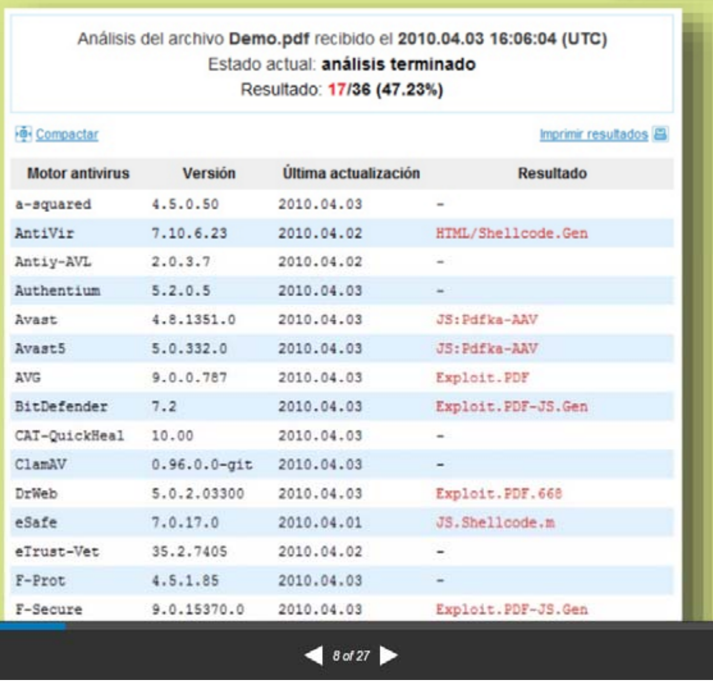
Ever dreamed of breaking into bank, stealing the Royal Diamond and escaping with leaving no trace? Now you have the chance to put yourself to the test! On this epic journey you have to solve puzzles, find hidden objects and use your room escape skills to advance to next rooms. Are you ready to face ...

Bank of the West Mobile (4 versions. Latest version code: 25)

Bank of the West | botwmobile@gmail.com | botw | GooglePlay

The Bank of the West app provides secure access to your accounts allowing you to manage your finances from virtually anywhere. Available to all registered Online Banking customers. The app lets you get a peek at your balances without signing in, deposit checks by taking a picture, add payees and pay ...

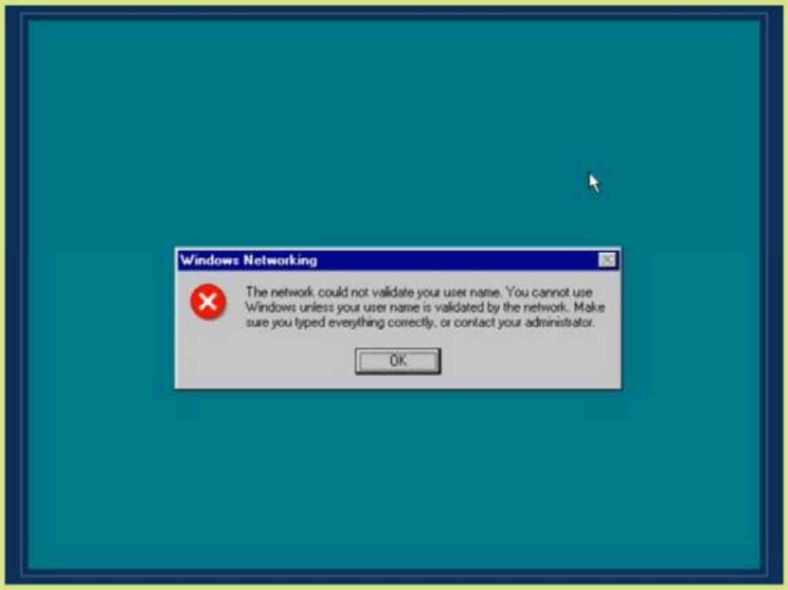
Security Boundaries



Análisis del archivo **Demo.pdf** recibido el **2010.04.03 16:06:04 (UTC)**
Estado actual: **análisis terminado**
Resultado: **17/36 (47.23%)**

Motor antivirus	Versión	Última actualización	Resultado
a-squared	4.5.0.50	2010.04.03	-
AntiVir	7.10.6.23	2010.04.02	HTML/Shellcode.Gen
Antiy-AVL	2.0.3.7	2010.04.02	-
Authentium	5.2.0.5	2010.04.03	-
Avast	4.8.1351.0	2010.04.03	JS:Pdfka-AAV
Avast5	5.0.332.0	2010.04.03	JS:Pdfka-AAV
AVG	9.0.0.787	2010.04.03	Exploit.PDF
BitDefender	7.2	2010.04.03	Exploit.PDF-JS.Gen
CAT-QuickHeal	10.00	2010.04.03	-
ClamAV	0.96.0.0-git	2010.04.03	-
DrWeb	5.0.2.03300	2010.04.03	Exploit.PDF.668
eSafe	7.0.17.0	2010.04.01	JS.Shellcode.m
eTrust-Vet	35.2.7405	2010.04.02	-
F-Prot	4.5.1.85	2010.04.03	-
F-Secure	9.0.15370.0	2010.04.03	Exploit.PDF-JS.Gen

Bypassing Security



The network could not validate your user name. You cannot use Windows unless your user name is validated by the network. Make sure you typed everything correctly, or contact your administrator.

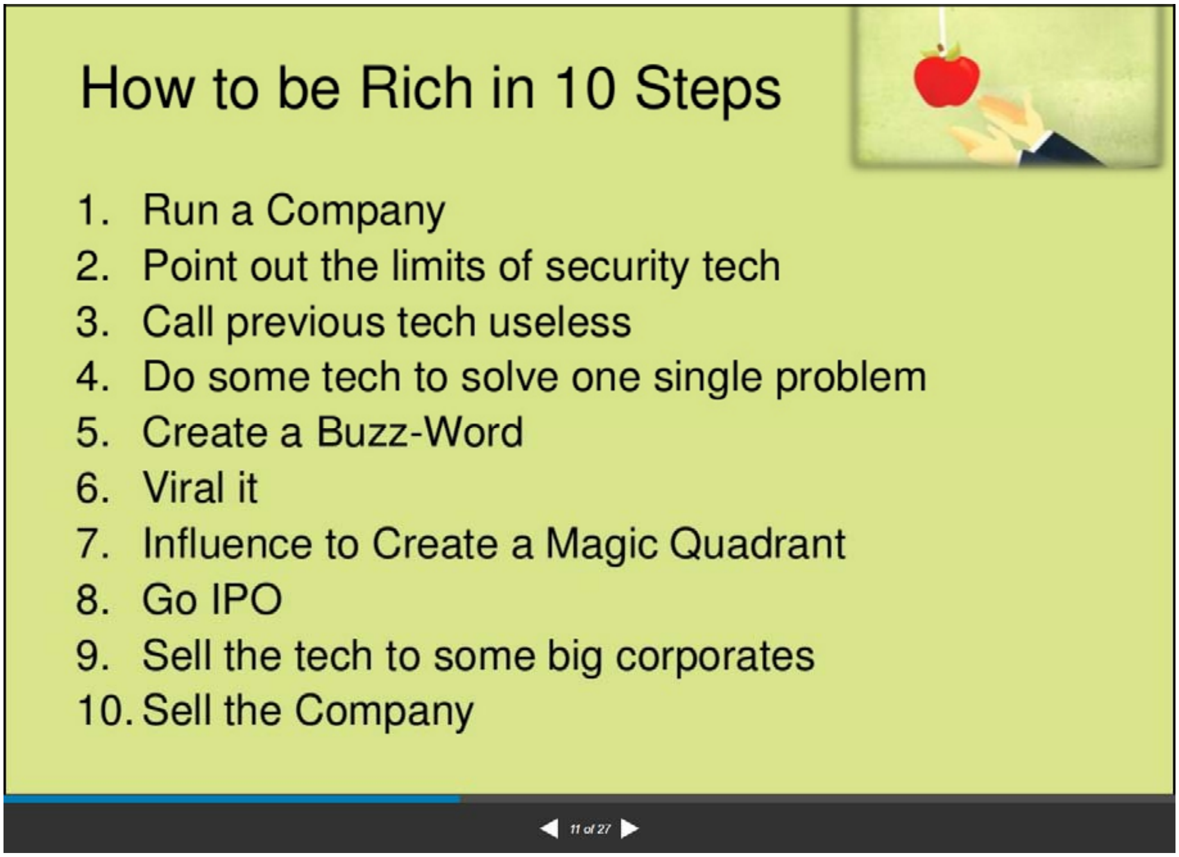
"Buzz-Words"-Tech

Post-Quantum Cryptography

Anti-APT

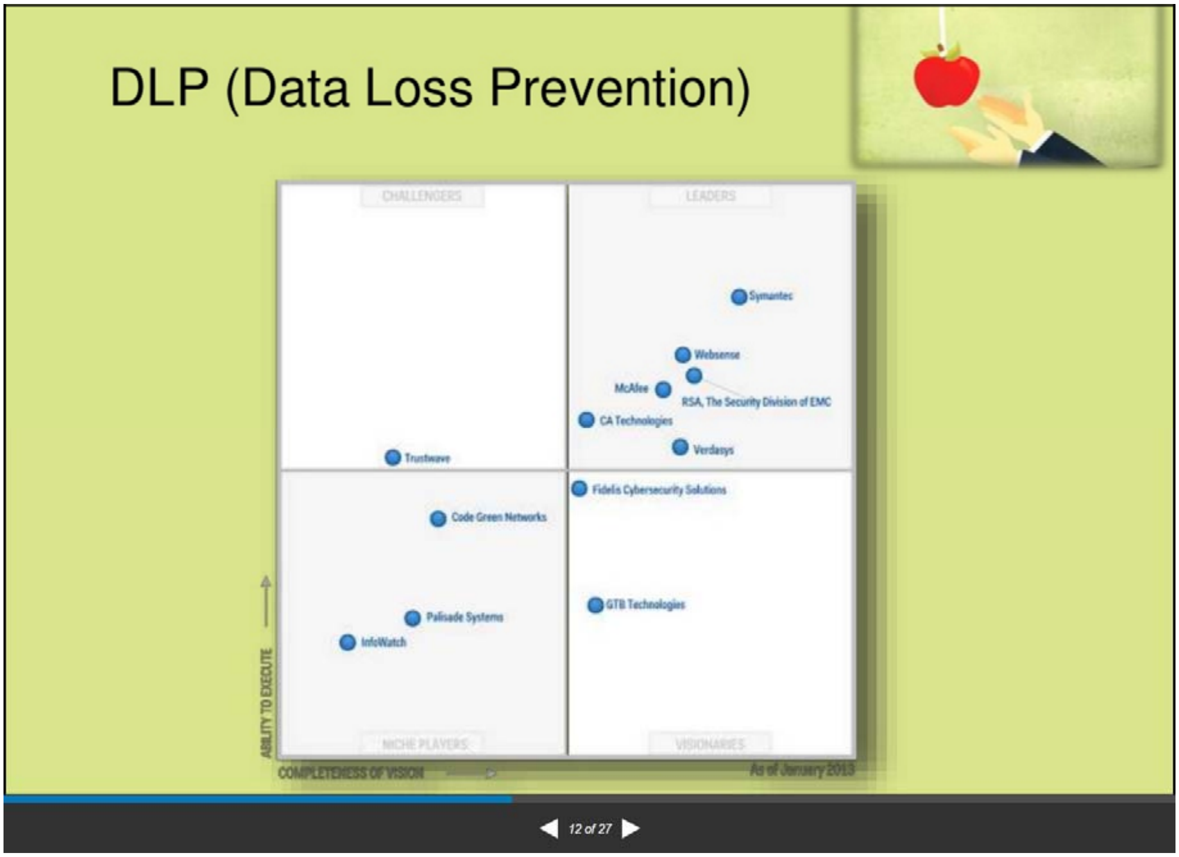
Machine Learning

Cyber-resilience



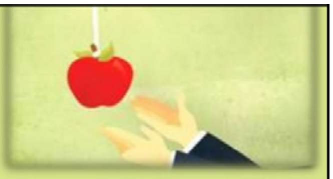
How to be Rich in 10 Steps

1. Run a Company
2. Point out the limits of security tech
3. Call previous tech useless
4. Do some tech to solve one single problem
5. Create a Buzz-Word
6. Viral it
7. Influence to Create a Magic Quadrant
8. Go IPO
9. Sell the tech to some big corporates
10. Sell the Company



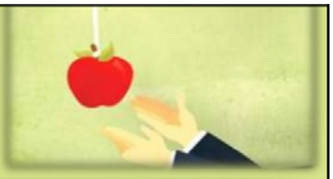
DLP (Data Loss Prevention)

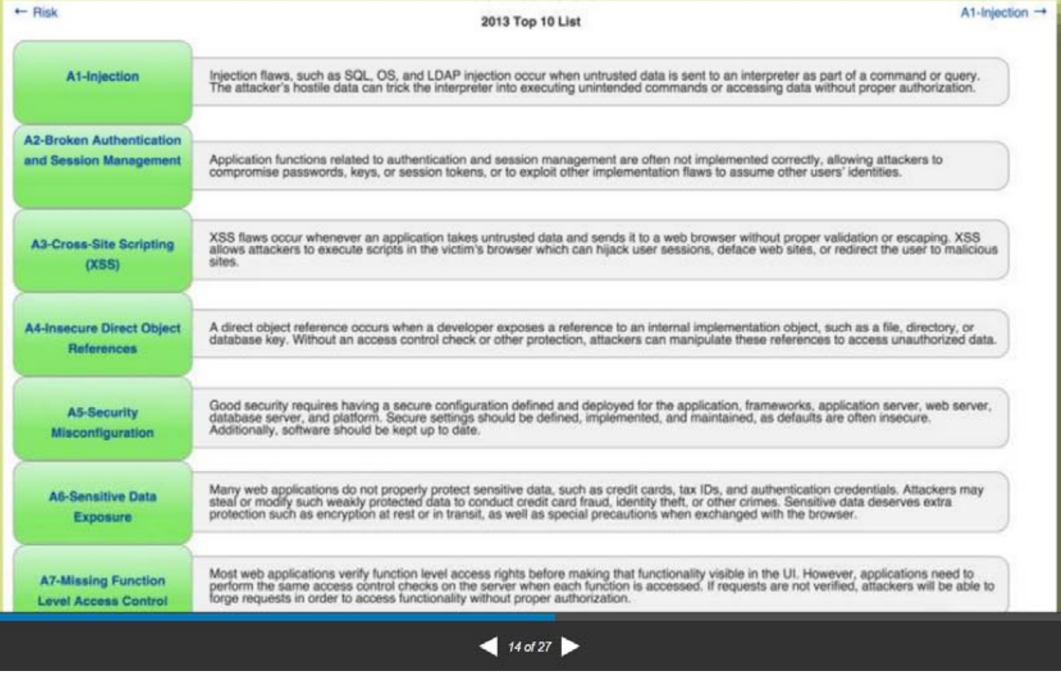
DLP (Data Loss Prevention)



Empresa	Nº de documentos	Usuarios	Directorios	Impresoras	Software	Correos	SSOO	Total metadatos
DLP1	1263	528	450	101	148	28	10	1265
DLP2	1247	323	330	47	101	10	6	817
DLP3	757	228	44	10	98	6	8	394
DLP4	214	93	115	30	42	0	4	284
DLP5	291	62	19	6	67	0	4	158
DLP6	154	18	7	1	42	0	1	69
DLP7	95	8	0	0	19	0	0	27
DLP8	61	20	1	0	13	0	0	34
DLP9	43	6	1	0	23	0	0	30
DLP10	18	4	0	0	12	0	0	16
DLP11	4	1	0	0	4	0	0	5
DLP12	1	0	0	0	1	0	0	1

OWASP Top Ten 10

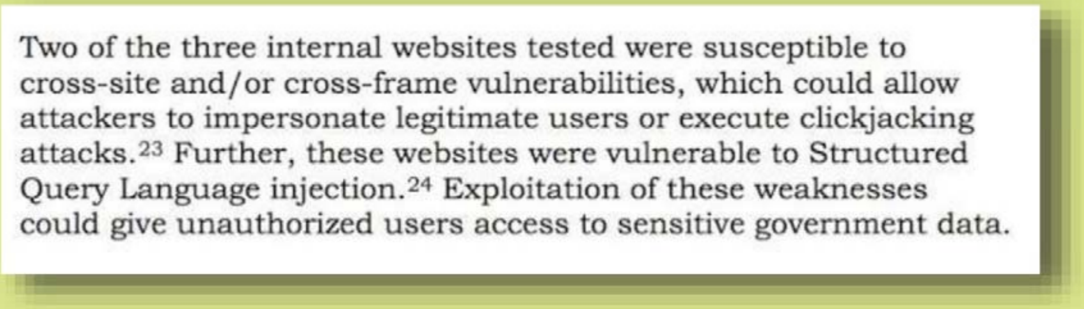




2013 Top 10 List

A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2-Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4-Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
A5-Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
A6-Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
A7-Missing Function Level Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

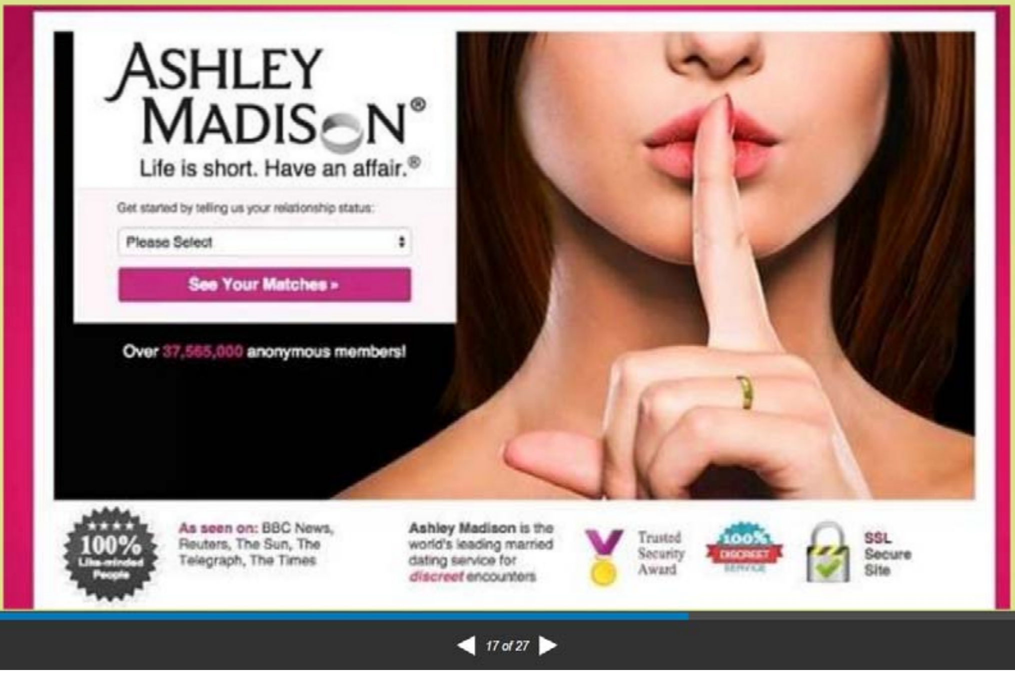
Department of Homeland Security



Two of the three internal websites tested were susceptible to cross-site and/or cross-frame vulnerabilities, which could allow attackers to impersonate legitimate users or execute clickjacking attacks.[23] Further, these websites were vulnerable to Structured Query Language injection.[24] Exploitation of these weaknesses could give unauthorized users access to sensitive government data.

Be Secure or Feel Secure

Pretending to be Secure



Life is short. Have an affair.®

Get started by telling us your relationship status:

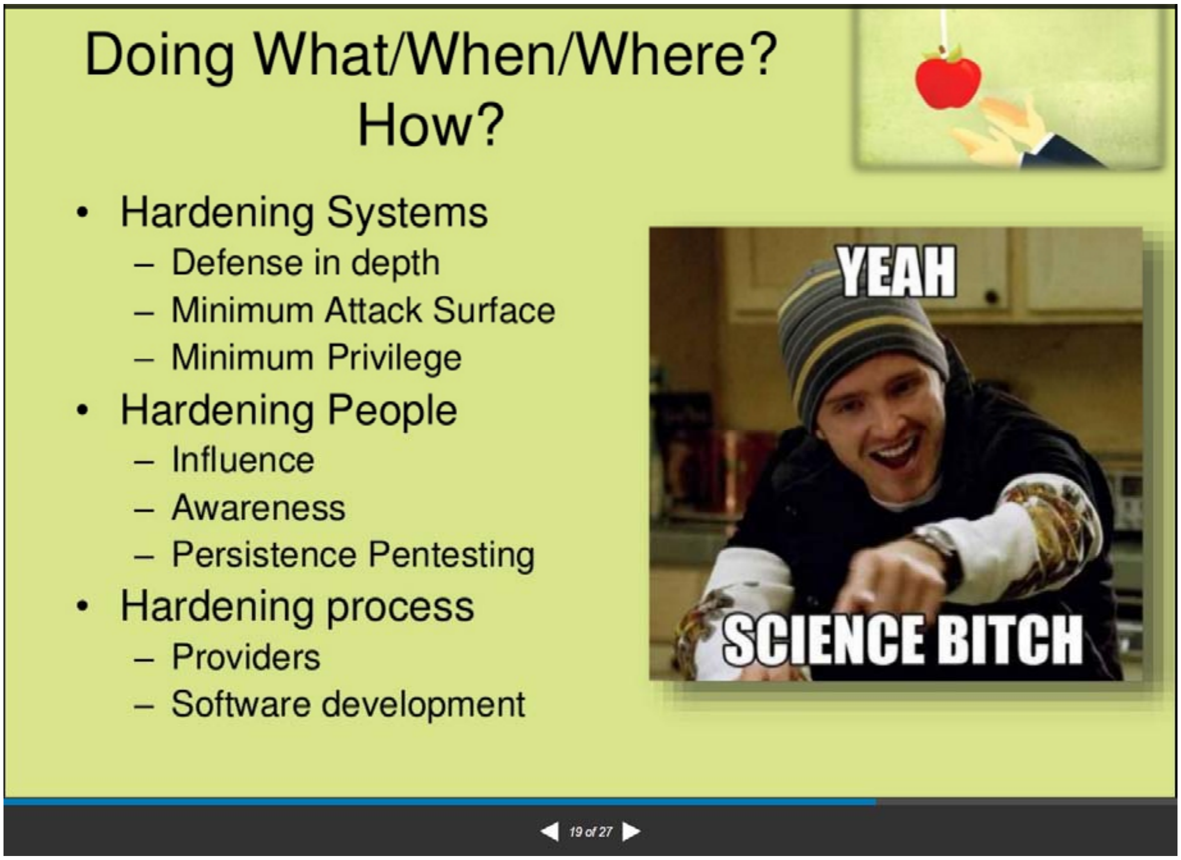
Over 37,565,000 anonymous members!

As seen on: BBC News, Reuters, The Sun, The Telegraph, The Times

Ashley Madison is the world's leading married dating service for *discreet* encounters

Complexity of Security

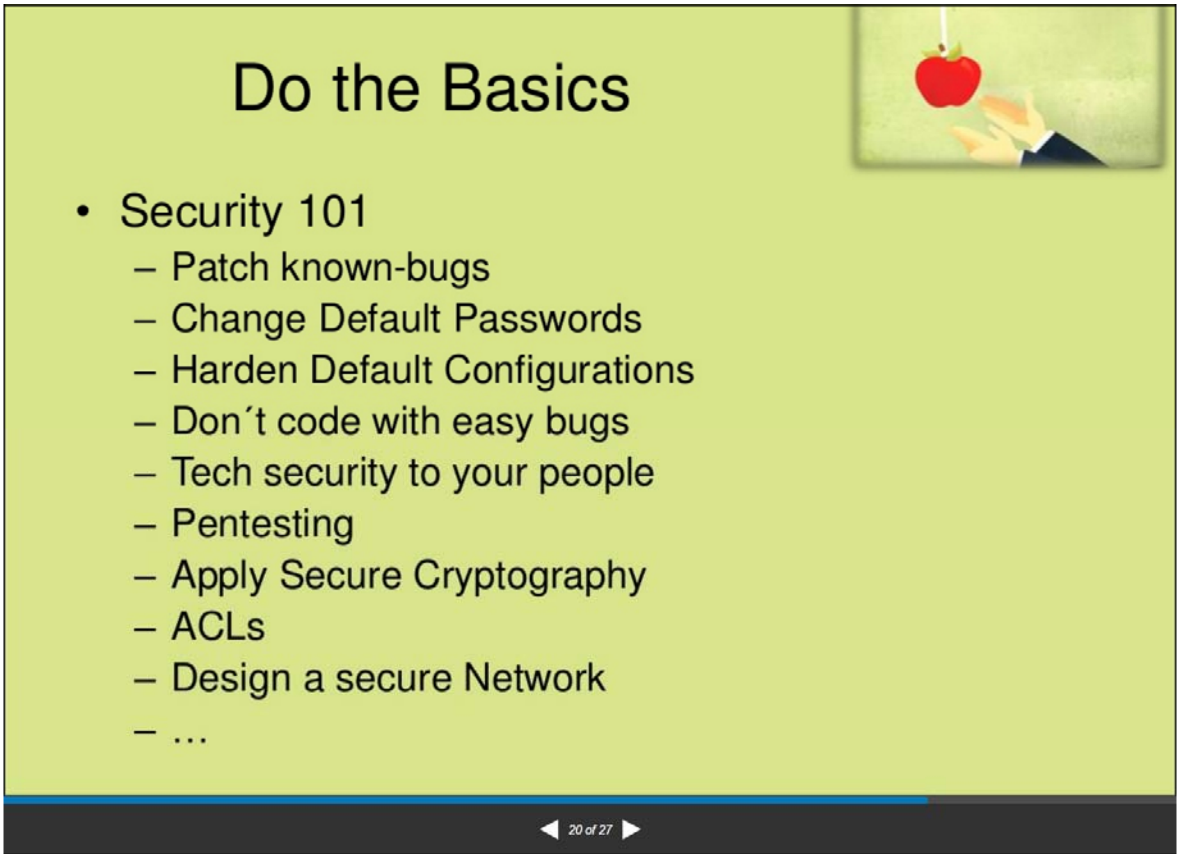
- Manage
  - People
  - Tech
  - Process
- To get
  - Integrity
  - Confidentiality
  - Availability
- Reaching
  - Acceptable Risk
  - Resilience
  - Compliance



Doing What/When/Where? How?

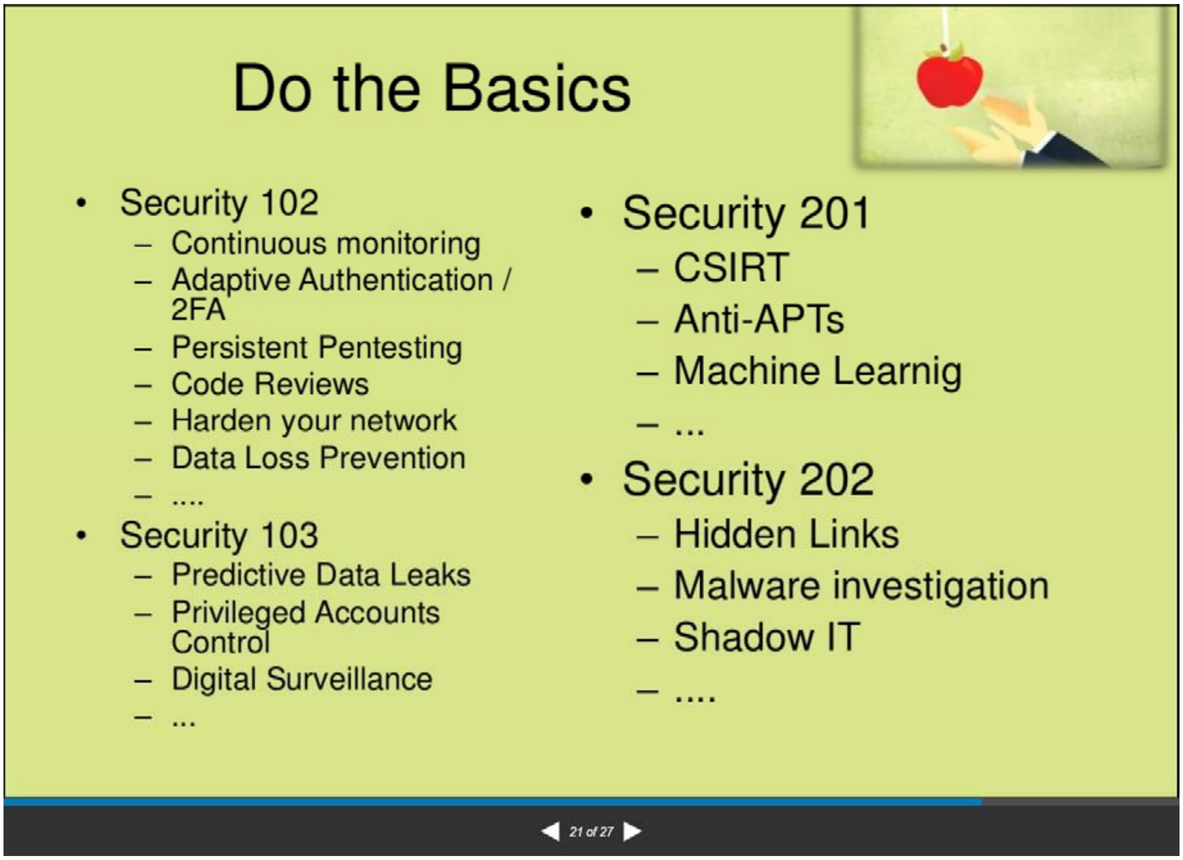
- Hardening Systems
  - Defense in depth
  - Minimum Attack Surface
  - Minimum Privilege
- Hardening People
  - Influence
  - Awareness
  - Persistence Pentesting
- Hardening process
  - Providers
  - Software development

YEAH
SCIENCE BITCH



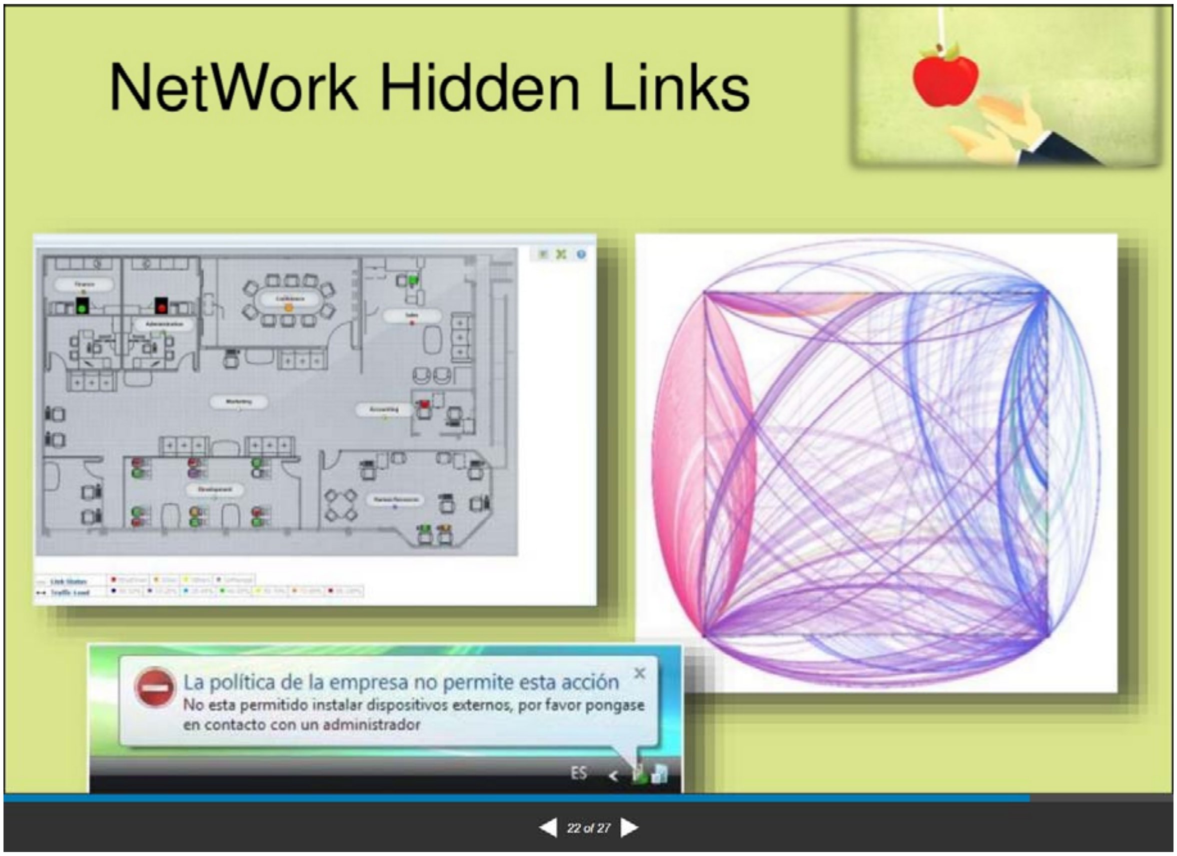
Do the Basics

- Security 101
  - Patch known-bugs
  - Change Default Passwords
  - Harden Default Configurations
  - Don´t code with easy bugs
  - Tech security to your people
  - Pentesting
  - Apply Secure Cryptography
  - ACLs
  - Design a secure Network
  - …



Do the Basics

- Security 102
  - Continuous monitoring
  - Adaptive Authentication / 2FA
  - Persistent Pentesting
  - Code Reviews
  - Harden your network
  - Data Loss Prevention
  - ....
- Security 103
  - Predictive Data Leaks
  - Privileged Accounts Control
  - Digital Surveillance
  - ...
- Security 201
  - CSIRT
  - Anti-APTs
  - Machine Learnig
  - ...
- Security 202
  - Hidden Links
  - Malware investigation
  - Shadow IT
  - ....

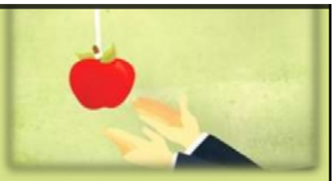


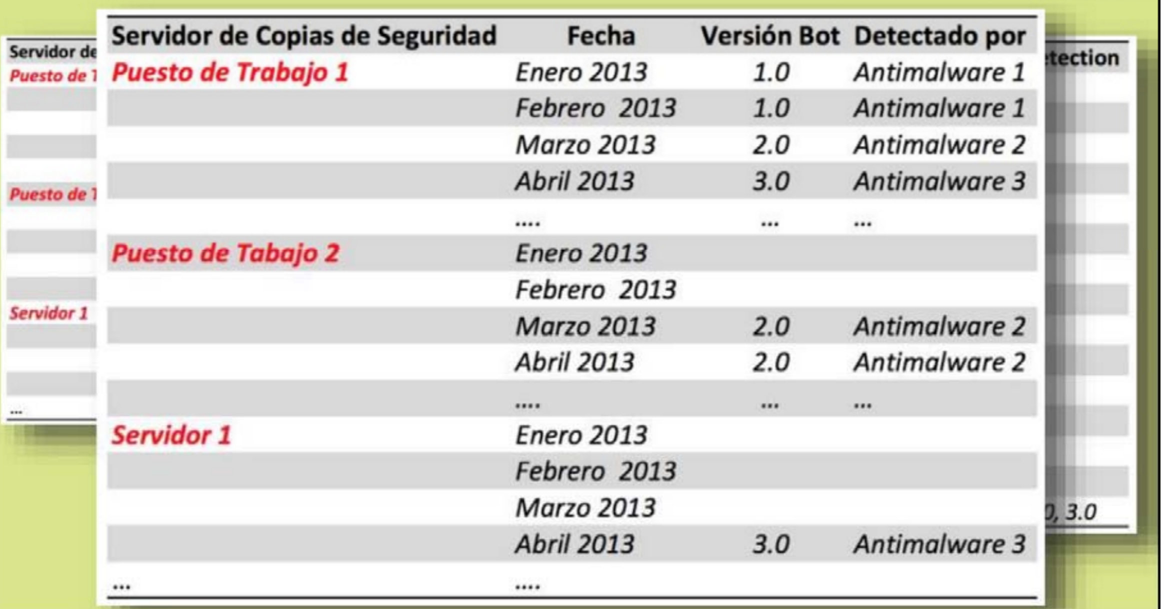
NetWork Hidden Links

La política de la empresa no permite esta acción

No esta permitido instalar dispositivos externos, por favor pongase en contacto con un administrador

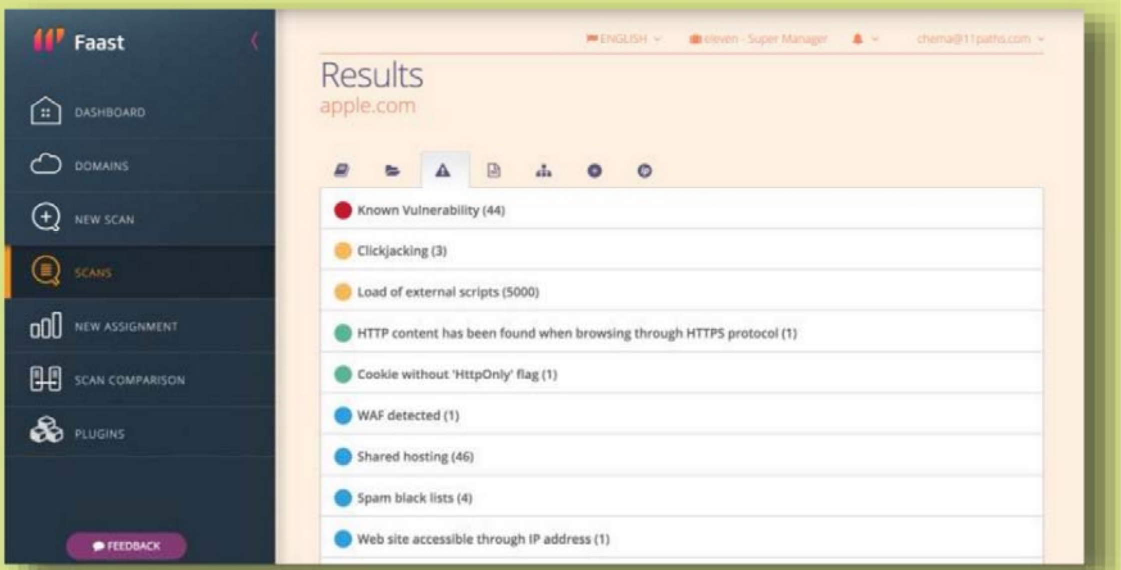
Malware Investigation





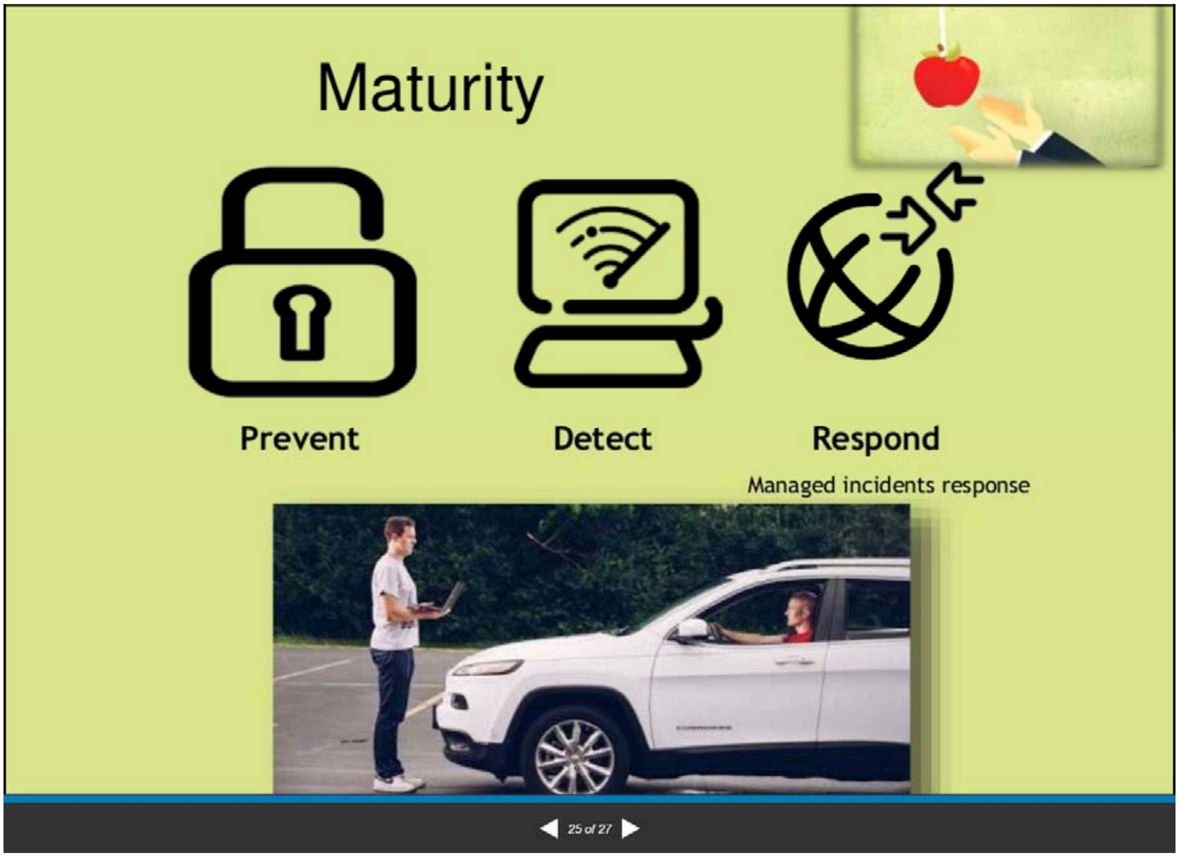
Servidor de Copias de Seguridad	Fecha	Versión Bot	Detectado por
Puesto de Trabajo 1	*Enero 2013*	*1.0*	*Antimalware 1*
	Febrero 2013	*1.0*	*Antimalware 1*
	Marzo 2013	*2.0*	*Antimalware 2*
	Abril 2013	*3.0*	*Antimalware 3*
	....	...	...
Puesto de Tabajo 2	*Enero 2013*		
	Febrero 2013		
	Marzo 2013	*2.0*	*Antimalware 2*
	Abril 2013	*2.0*	*Antimalware 2*
	....	...	...
Servidor 1	*Enero 2013*		
	Febrero 2013		
	Marzo 2013		
	Abril 2013	*3.0*	*Antimalware 3*
...	....		

Persistent Pentesting



Results
apple.com

- Known Vulnerability (44)
- Clickjacking (3)
- Load of external scripts (5000)
- HTTP content has been found when browsing through HTTPS protocol (1)
- Cookie without 'HttpOnly' flag (1)
- WAF detected (1)
- Shared hosting (46)
- Spam black lists (4)
- Web site accessible through IP address (1)



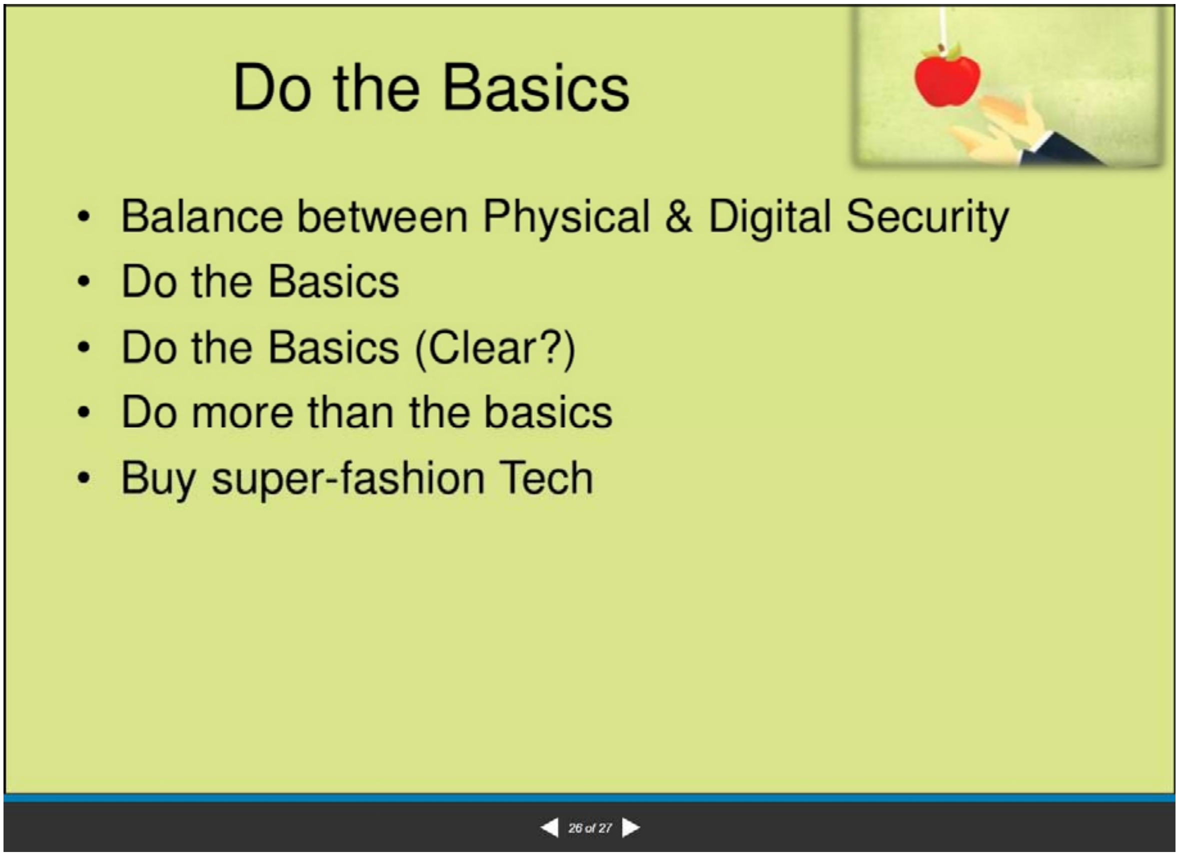
Maturity

Prevent

Detect

Respond

Managed incidents response



Do the Basics

- Balance between Physical & Digital Security
- Do the Basics
- Do the Basics (Clear?)
- Do more than the basics
- Buy super-fashion Tech

Questions?

- Chema Alonso
- @chemaalonso
- http://www.elladodelmal.com

27 of 27