

AUDITORIA INFORMÁTICA



Camilo Zapata @ccamilozt
Fernando Quintero @nonroot

#CPCO4 – 2011

Bogotá, Colombia



AUDITORÍA INFORMÁTICA

- Auditoría de seguridad:

Evaluar las debilidades de un sistema ...

Para qué?

- Conocer el estado de la seguridad actual
- Probar las medidas y controles existentes
- Mejora continua con el ciclo PHVA
- Certificar parte o todo el sistema
- ...



AUDITORÍA INFORMÁTICA

- Qué auditar?
 - Componentes de una organización

- Procesos
- Personas
- Aplicaciones
- Infraestructura (física y lógica)
- ...



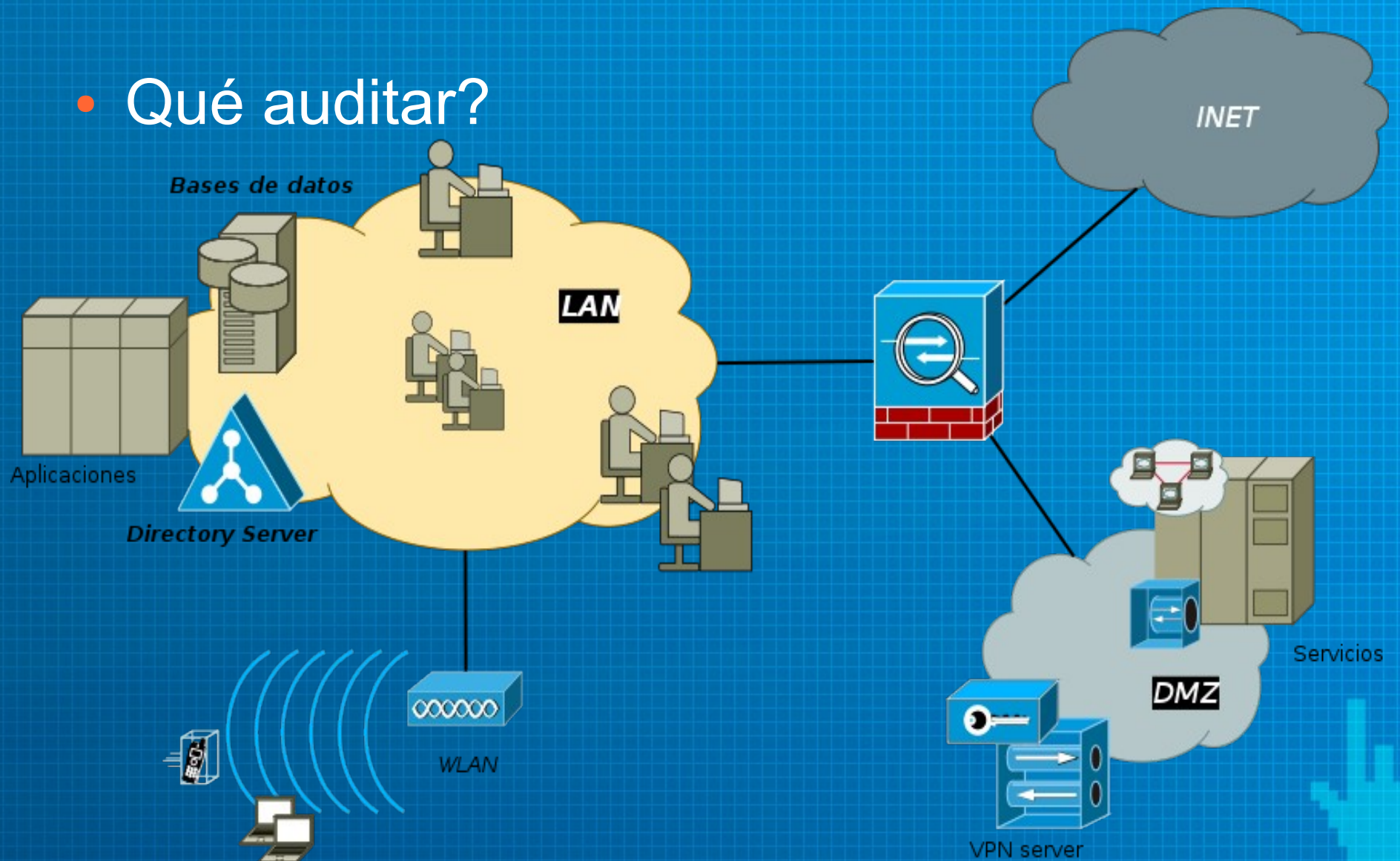
AUDITORÍA INFORMÁTICA

- Qué auditar?
 - Interfaces del sistema
 - Publicaciones (Sitios Web, Redes Sociales)
 - IPs públicas
 - Redes locales (LAN, WLAN)
 - Sucursales
 - Personas
 - ...



AUDITORÍA INFORMÁTICA

- Qué auditar?



AUDITORÍA INFORMÁTICA

- Qué necesito?
 - Tiempo, mucho tiempo
 - Experiencia
 - ¿ Autorización ?
 - ¿ Un plan ?
 - Equipos (Hardware y Software)
 - **Conocimiento! (Qué?, Cómo?, Cuando?)**



AUDITORÍA INFORMÁTICA

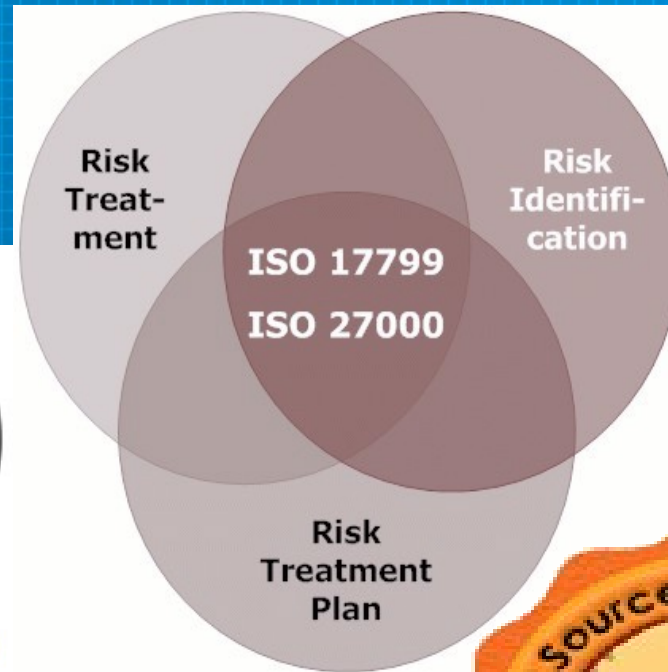
- Qué necesito?
 - Importante: El conocimiento ...
 - Libros (recomendado?)
 - Blogs (recomendados?)
 - Eventos, congresos !
 - Cursos, talleres !
 - Tutoriales??
 - RFCs (OK)
 - ...

HOWTO



AUDITORÍA INFORMÁTICA

- Tengo un plan?
 - Metodología



AUDITORÍA INFORMÁTICA

- Metodología

- Planeación

- Objetivos
 - Alcance (*scope*)
 - Tiempo estimado

- Preparación

- Acuerdos de confidencialidad
 - Contactos internos y externos
 - Presentación de metodología y profesionales
 - Definir horarios de auditoría



AUDITORÍA INFORMÁTICA

- Metodología
 - TEST (lo de siempre!)
 - Buscar y encontrar
 - Analizar
 - Evaluar
 - ¿ Explotar ?
 - Valorar (Impacto)

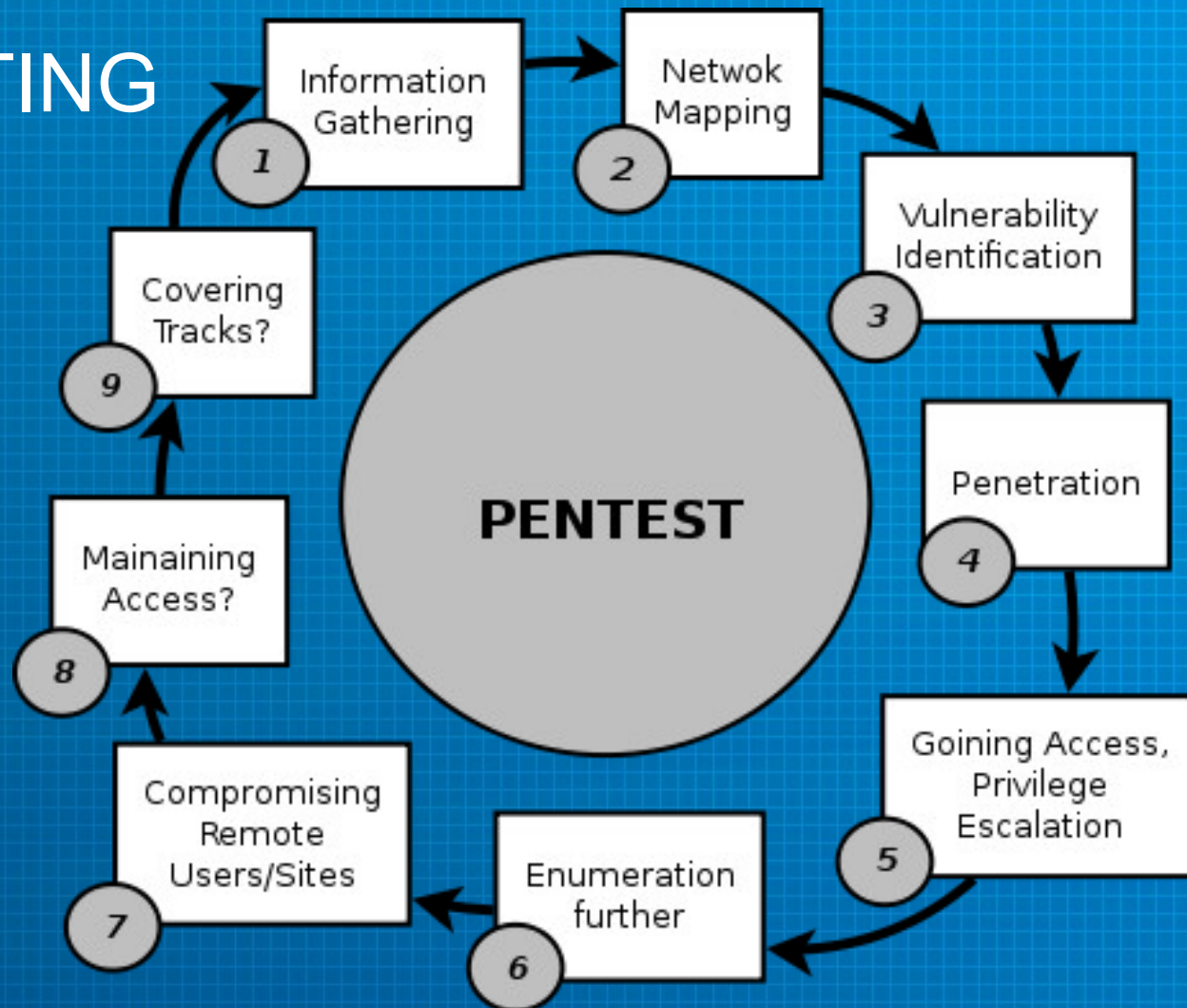


Caja negra, Caja blanca, Caja Gris, ...



AUDITORÍA INFORMÁTICA

- TESTING



AUDITORÍA INFORMÁTICA

- Herramientas
 - Cuál es la herramienta más importante que debo obtener?
 - Conocimiento
 - Saber que estoy buscando o saber que lo es cuando lo encuentre



Got
Root?

!Tener acceso privilegiado no es suficiente!



AUDITORÍA INFORMÁTICA

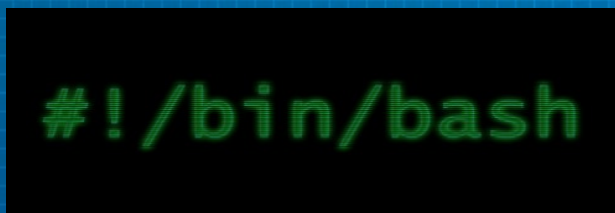
- Herramientas

- Las herramientas no hacen el trabajo por si solas (*no siempre*)
- **Tener herramientas no es suficiente**
 - Saber cuando usarlas?
 - Donde usarlas?
 - Para qué usarlas?
 - Y Cómo usarlas? ...



AUDITORÍA INFORMÁTICA

- Herramientas ...



Y miles más ...



AUDITORÍA INFORMÁTICA

Escenario para el taller:
HOST



AUDITORÍA INFORMÁTICA

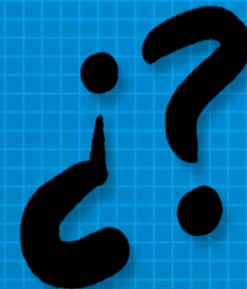
Objetivo:

Extraer documentos confidenciales
(Ofimática, BD, etc)



AUDITORÍA INFORMÁTICA

- Es un HOST, que puedo hacer?
 - Escanear en busca de puertos abiertos
 - Identificar el sistema operativo instalado



Categoría: *Network Scanners*

Herramientas: nmap, scanrand, p0f, unicorn





The screenshot shows a web browser window with the following elements:

- Address Bar:** `http://taller.2011.campus-party.co/`
- Page Title:** Home
- Navigation Menu:** HOME (selected), SAMPLE SITES, JOOMLA.ORG
- Main Content:** Joomla!™
Open Source Content Management



```
MariaCamila>nmap -sV taller.2011.campus-party.co
```

```
Starting Nmap 5.50 ( http://nmap.org ) at 2011-06-27 23:33 COT
```

```
Nmap scan report for taller.2011.campus-party.co (174.129.169.115)
```

```
Host is up (0.089s latency).
```

```
Not shown: 998 closed ports
```

```
PORT      STATE SERVICE VERSION
```

```
22/tcp    open  ssh      OpenSSH 5.1p1 Debian 5 (protocol 2.0)
```

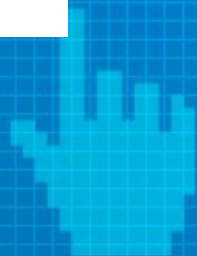
```
80/tcp    open  http     Apache httpd 2.2.9 ((Debian) PHP/5.2.6-1+lenn  
with Suhosin-Patch)
```

```
Service Info: OS: Linux
```

```
Service detection performed. Please report any incorrect results a  
ttp://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 8.27 seconds
```

```
MariaCamila>
```



AUDITORÍA INFORMÁTICA

- Encuentro puertos abiertos, que puedo hacer?
 - Identificar los servicios disponibles

Categoría: *banner grabbers, fingerprinting*

Herramientas: nmap, nikto, etc.



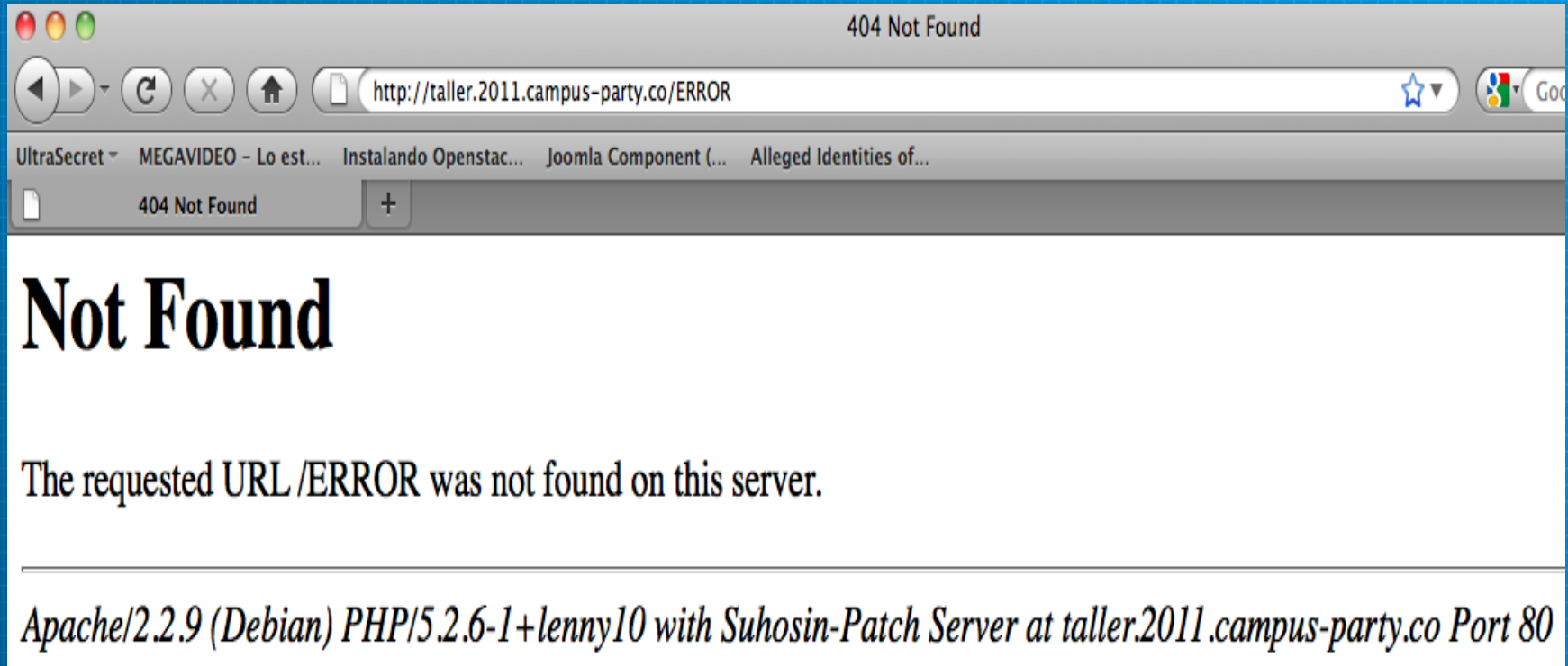
AUDITORÍA INFORMÁTICA

- Encuentro un servicio WEB, que puedo hacer?
 - Encontrar el nombre y versión del servidor WEB

Categoría:

HTTP Fingerprint, Error Disclosure Information





AUDITORÍA INFORMÁTICA

- Encuentro el Sistema Operativo, que puedo hacer?
 - Existen vulnerabilidades remotas?
 - Existen exploits?

Categoría: *Vulnerabilities, Exploits*

Herramientas: **exploit-db.com, CVE, BID**



Exploits Database by Offensive Security

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

UltraSecret ▾ MEGAVIDEO - Lo est... Instalando Openstac... Joomla Component (... Alleged Identities of...

Exploits Database by Offensive Se... +

EXPLOIT DATABASE



HOME BLOG GHDB FORUMS ABOUT REMOTE LOCAL WEB DOS



CVE - Common Vulnerabilities and Exposures (CVE)

http://cve.mitre.org/

UltraSecret ▾ MEGAVIDEO - Lo est... Instalando Openstac... Joomla Component (... Alleged Identities of...

CVE - Common Vulnerabilities an... +

CVE LIST **COMPATIBLE PRODUCTS** **NEWS - JUNE 10, 2011** **SEARCH**



Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names



SecurityFocus

http://www.securityfocus.com/bid

UltraSecret - MEGAVIDEO - Lo est... Instalando Openstac... Joomla Component (... Alleged Identities of...

SecurityFocus



Symantec Connect

A technical community for Symantec customers, end-users, developers, and partners.

[Join the conversation >](#)

Vulnerabilities

Vendor:

Title:

Version:



AUDITORÍA INFORMÁTICA

- Tengo identificado el servidor WEB,
que puedo hacer?
 - Buscar directorios y archivos comunes
 - Buscar aplicaciones instaladas

Categoría: *Spiders, Content Scanners*

- Herramientas: foca, dirb, nikto2



AUDITORÍA INFORMÁTICA

- Tengo la aplicación web identificada, que puedo hacer?
 - La versión de la aplicación es vulnerable a ataques remotos?, entonces usamos un exploit remoto.
 - No existen exploits remotos?, entonces creamos un exploit **ZeroDay** (exploit no público y no conocido).
 - Hacemos Ingeniería social para obtener acceso.



AUDITORÍA INFORMÁTICA

- Tengo la aplicación web, que mas puedo hacer?
 - Buscar otras aplicaciones instaladas en el mismo sistema, propias o de terceros.
 - Buscar otros hosts virtuales o instancias de otros servidores web con diferente o igual versión.

Categoría:

content scanners, dns scanners, vhosts scanners



AUDITORÍA INFORMÁTICA

- Identificada otra aplicación y su debilidad, que puedo hacer?
- -Explotarla e ingresar al sistema

Categoría: *web vulnerabilities*

Herramientas: Experiencia en explotación



http://localhost.2011.campus-party.co/?param=;ls -la

UltraSecret ▾ MEGAVIDEO - Lo est... Instalando Openstac... Joomla Component (... Alleged Identities of...

http://localhost...?param=;ls%20-la

```
index.php total 12 drwxr-xr-x 2 www-  
28 04:41 . drwxr-xr-x 15 root root 409  
-rw-r--r-- 1 www-data www-data 119  
-rw-r--r-- 1 www-data www-data 119
```



AUDITORÍA INFORMÁTICA

- Tengo acceso al HOST en modo no privilegiado, que puedo hacer?
 - Eliminarlo, borrar archivos, etc. (X)
 - Escalar privilegios (?)
 - Explorar el sistema y adquirir la información (OK)

Categoría: *Local exploits, sniffing, tracking*



AUDITORÍA INFORMÁTICA

- Cómo y dónde encuentro la información confidencial ?
 - Inspiración divina (...)
 - Aprender sobre los procesos internos (OK)
 - Ingeniería social interna y externa (OK)
 - Sniffing, logs, monitoreo del sistema y de la red (OK)

Herramientas: *tcpdump*, *sniff**, *experiencia*



AUDITORÍA INFORMÁTICA

- Una vez adquirida la información: usuarios, correos, procesos, registros, comportamientos, que puedo hacer?
 - Eliminar la información (X)
 - Modificar la información (X)
 - Extraer la información (?)

Categoría: *Plataformas, Sistemas Operativos*



AUDITORÍA INFORMÁTICA

- Finalmente encuentro la información importante, cómo la descargo?
 - Leerla directamente
 - Capturar *screenshots* + deco OCR
 - Descargarla por un protocolo de transferencia:
HTTP, FTP, NFS, SMB, RSYNC, etc.
(y si la información pesara 100 TB ?)



AUDITORÍA INFORMÁTICA

MINI RETO – TALLER

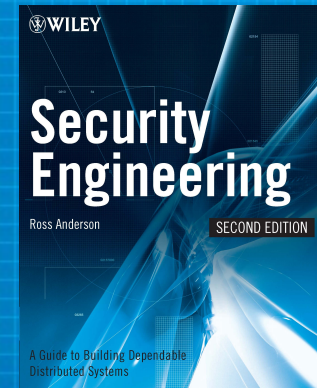
Escenario:

<http://tallerwg.2011.campus-party.co/>

Objetivo:

Extraer información sensible

Premio(1ro): Security Book XYZ



AUDITORÍA INFORMÁTICA

Mas información:

- <http://groups.google.com/group/ctf-colombian-team>
@nonroot , @jhosilvo , @ccamilozt



- <http://nonroot.blogspot.com/>
- **Video:** <http://tv.campus-party.org/player-bogota.php?v=DjJ3A-LsT3Y>

