

# Metodología de PenTesting

Miguel Angel Astor Romero

27 de septiembre de 2019

## Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

## Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

## Herramientas de Pen Testing

Escáneres

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

## Conclusiones

Conclusiones

Preguntas

Introducción

Metodología de PenTesting

Herramientas de PenTesting

Conclusiones

## Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

Metodología PTES

## Herramientas de PenTesting

Escáneres

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

## Conclusiones

Conclusiones

Preguntas

Miguel Angel  
Astor Romero

## Advertencia

## Definiciones y Conceptos

## Estándares y Recomendaciones

Metodología NIST  
800-115

## Metodología P TES

## Escáneres

## Herramientas On-Line para Recolección de Inteligencia

Suites de Ataques  
Distribuciones

## Conclusiones

## Preguntas



# Cuidado con lo que Hagan

Metodología de  
Pen Testing

Miguel Angel  
Astor Romero

## Introducción

### Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

## Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

## Herramientas de Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

## Conclusiones

Conclusiones

Preguntas





## Estándar NIST 800-155

PenTesting es el proceso de determinar que tan efectivamente una entidad (pe. un host, sistema, red, procedimiento, persona, etc.) cumple objetivos de seguridad específicos.



## Introducción

## Advertencia

## Definiciones y Conceptos

## Estándares y Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

Metodología PTES

## Herramientas de PenTesting

## Escáneres

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques  
Distribuciones

## Concl|usiones

## Conclusiones

## Preguntas

La recomendación ITU-T X.800 define un marco conceptual estándar para representar la seguridad de un sistema informático.

## Introducción

Advertencia

**Definiciones y Conceptos**

Estándares y  
Recomendaciones

## Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

## Herramientas de Pen Testing

Escáneres

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

## Conclusiones

Conclusiones

Preguntas

La recomendación ITU-T X.800 define un marco conceptual estándar para representar la seguridad de un sistema informático.

## Amenaza

Posibilidad de violación de la seguridad de un sistema.

### Introducción

Advertencia

**Definiciones y Conceptos**

Estándares y  
Recomendaciones

### Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

### Herramientas de Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

### Conclusiones

Conclusiones

Preguntas

La recomendación ITU-T X.800 define un marco conceptual estándar para representar la seguridad de un sistema informático.

## Amenaza

Posibilidad de violación de la seguridad de un sistema.

## Ataque

Acción que vulnera la seguridad de un sistema.

### Introducción

Advertencia

**Definiciones y Conceptos**

Estándares y  
Recomendaciones

### Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

### Herramientas de Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

### Conclusiones

Conclusiones

Preguntas



## Technical Guide to InfoSec Testing and Assessment

- Recomendación de metodologías, procedimientos y actividades para la evaluación de seguridad de sistemas informáticos.

### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

### Herramientas de Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

### Conclusiones

Conclusiones

Preguntas

## Main Page

LOG IN

Navigation

- Main page
- PTES Technical Guideline
- In the Media
- FAQ

Search

Search The Penetration T

Go Search

Tools

- What links here
- Related changes
- Special pages
- Printable version
- Permanent link
- Page information

main page view source history

### High Level Organization of the Standard

The penetration testing execution standard consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.

This version can be considered a v1.0 as the core elements of the standard are solidified, and have been "road tested" for over a year through the industry. A v2.0 is in the works soon, and will provide more granular work in terms of "levels" - as in intensity levels at which each of the elements of a penetration test can be performed at. As no pentest is like another, and testing will range from the more mundane web application or network test, to a full-on red team engagement, said levels will enable an organization to define how much sophistication they expect their adversary to exhibit, and enable the tester to step up the intensity on those areas where the organization needs them the most. Some of the initial work on "levels" can be seen in the intelligence gathering section.

Following are the main sections defined by the standard as the basis for penetration testing execution:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

As the standard does not provide any technical guidelines as far as how to execute an actual pentest, we have also created a technical guide to accompany the standard itself. The technical guide can be reached via the link below:

- Technical Guidelines

For more information on what this standard is, please visit:

- The Penetration Testing Execution Standard: FAQ

This page was last edited on 16 August 2014, at 20:14. Content is available under [GNU Free Documentation License 1.2](#) unless otherwise noted. [Privacy policy](#) [About The Penetration Testing Execution Standard](#) [Disclaimers](#)

Powered by [MediaWiki](#)

## Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
RecomendacionesMetodología de  
Pen TestingMetodología NIST  
800-115

Metodología PTES

Herramientas de  
Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

## Conclusiones

Conclusiones

Preguntas

```
10 GOSUB LOOK_FOR_HOLES
20 IF HOLE_FOUND = FALSE THEN GOTO 50
30 GOSUB FIX_HOLE
40 GOTO 10
50 GOSUB CONGRATULATE_SELF
60 GOSUB GET_HACKED_EVENTUALLY_ANYWAY
70 GOTO 10
```

## Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

## Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

## Herramientas de Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

## Conclusiones

Conclusiones

Preguntas

- ▶ Planificación
- ▶ Ejecución
- ▶ Post-Ejecución





## Planificación

- ▶ Desarrollar una política de evaluación de seguridad.
- ▶ Prioritizar y calendarizar las evaluaciones.
- ▶ Seleccionar técnicas de evaluación.
- ▶ Logística.
- ▶ Desarrollar un plan de evaluación.
- ▶ Analizar requisistos y regulaciones legales.
  - ▶ Obtener permisos.

### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de Pen Testing

**Metodología NIST  
800-115**

Metodología PTES

### Herramientas de Pen Testing

Escáneres

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

### Conclusiones

Conclusiones

Preguntas

## Planificación

- ▶ Desarrollar una política de evaluación de seguridad.
- ▶ Prioritizar y calendarizar las evaluaciones.
- ▶ Seleccionar técnicas de evaluación.
- ▶ Logística.
- ▶ Desarrollar un plan de evaluación.
- ▶ Analizar requisitos y regulaciones legales.
  - ▶ Obtener permisos.

## Ejecución

- ▶ Coordinar.
- ▶ Revisión del plan.
- ▶ Analisis de vulnerabilidades.
- ▶ Documentación.

### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de Pen Testing

**Metodología NIST  
800-115**

Metodología PTES

### Herramientas de Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques  
Distribuciones

### Conclusiones

Conclusiones

Preguntas

## Planificación

- ▶ Desarrollar una política de evaluación de seguridad.
- ▶ Prioritizar y calendarizar las evaluaciones.
- ▶ Seleccionar técnicas de evaluación.
- ▶ Logística.
- ▶ Desarrollar un plan de evaluación.
- ▶ Analizar requisitos y regulaciones legales.
  - ▶ Obtener permisos.

## Ejecución

- ▶ Coordinar.
- ▶ Revisión del plan.
- ▶ Analisis de vulnerabilidades.
- ▶ Documentación.

## Post-Ejecución

- ▶ Desarrollar recomendaciones.
- ▶ Reportar.
- ▶ Mitigar.

### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de PenTesting

**Metodología NIST  
800-115**

Metodología PTES

### Herramientas de PenTesting

Escáneres

Herramientas On-Line  
para Recolección de  
Inteligencia

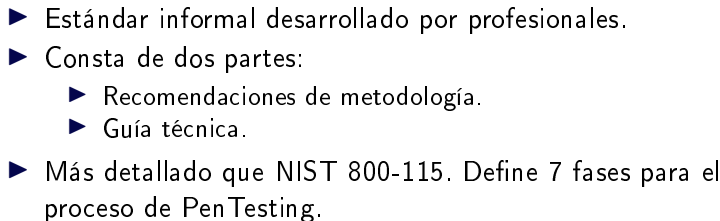
Suites de Ataques

Distribuciones

### Conclusiones

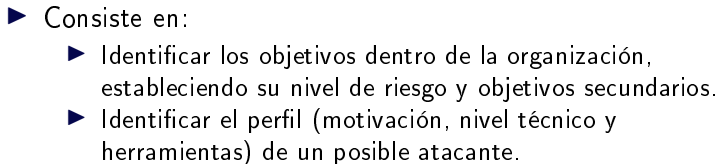
Conclusiones

Preguntas



-

-



-



- ▶ Uso de herramientas y *frameworks* para atacar las vulnerabilidades identificadas.
- ▶ Hay que tener conciencia de los riesgos:
  - ▶ Caidas de servicio.
  - ▶ Acceso y filtración de información sensible.



## Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

Metodología PTES

## Herramientas de PenTesting

Escáners

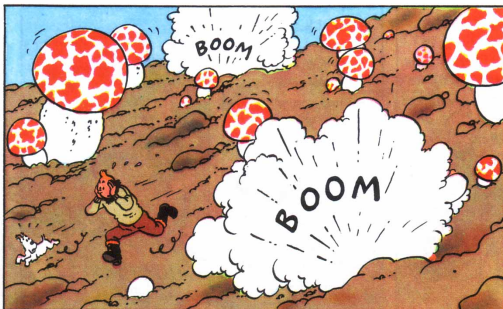
Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques  
Distribuciones

## Conclusiones

Conclusiones

Preguntas



► Consiste en:

- ▶ Identificar el valor de los sistemas y máquinas comprometidas en la fase de explotación.
- ▶ Identificar posibles vectores para otros ataques usando los sistemas comprometidos como pivote.

## Introducción

## Advertencia

## Definiciones y Conceptos

## Estándares y Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

## Metodología PTES

## Herramientas de PenTesting

Escáneres

## Herramientas On-Line para Recolección de Inteligencia

Suites de Ataques  
Distribuciones

## Conclusions

## Conclusiones

## Preguntas



- ▶ Hay que documentar todo lo que se haga con alto nivel de detalle:
  - ▶ La planificación.
  - ▶ Actividades realizadas.
  - ▶ Resultados obtenidos.
- ▶ Se suelen producir dos tipos de reportes:
  - ▶ Resúmenes ejecutivos.
  - ▶ Documentación técnica.
- ▶ **IMPORTANTE** Proteger los reportes a toda costa.

## Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

## Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

## Herramientas de Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

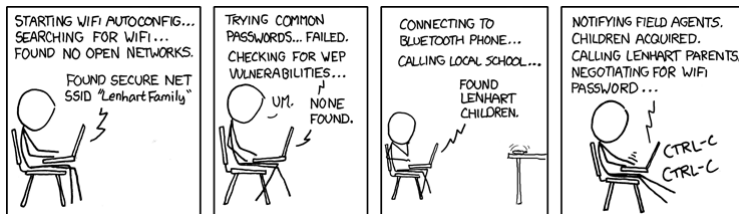
Suites de Ataques

Distribuciones

## Conclusiones

Conclusiones

Preguntas



- ▶ Herramientas básicas de UNIX
  - ▶ nslookup
  - ▶ dig
- ▶ NMAP
- ▶ Nessus
- ▶ Nikto
- ▶ Otras

## Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

## Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

## Herramientas de Pen Testing

### Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques  
Distribuciones

## Conclusiones

Conclusiones

Preguntas

## nslookup

- ▶ Programa de consulta a servidores de nombres.
- ▶ Funciona en modos automático e interactivo.
- ▶ Permite obtener información variada sobre *hosts* específicos mediante consultas DNS

### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

### Herramientas de Pen Testing

#### Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

### Conclusiones

Conclusiones

Preguntas

## nslookup

- ▶ Programa de consulta a servidores de nombres.
- ▶ Funciona en modos automático e interactivo.
- ▶ Permite obtener información variada sobre *hosts* específicos mediante consultas DNS

## dig

- ▶ Programa de consulta a servidores de nombres.
- ▶ Conceptualmente similar a nslookup, pero provee información más detallada y opciones más flexibles.
- ▶ Permite realizar transferencias de zona.

### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

### Herramientas de Pen Testing

#### Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques  
Distribuciones

### Conclusiones

Conclusiones

Preguntas

### Introducción

Advertencia  
Definiciones y Conceptos  
Estándares y Recomendaciones

### Metodología de Pen Testing

Metodología NIST  
800-115  
Metodología PTES

### Herramientas de Pen Testing

Escáners  
Herramientas On-Line para Recolección de Inteligencia  
Suites de Ataques  
Distribuciones

### Conclusiones

Conclusiones  
Preguntas

Scan Tools Profile Help

Target: 192.168.18.141 Profile: Intense scan [Scan] [Cancel]

Command: nmap -T4 -A -v 192.168.18.141

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.18.141

nmap -T4 -A -v 192.168.18.141 [Details]

Not shown: 977 closed ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
ftp-anon: Anonymous FTP login allowed (FTP code 230)			
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
ssh-hostkey:			
1024 60:0f:cf:e1:c8:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)			
2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)			
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd

| smtp\_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

| ssl-cert: Subject: commonName=ubuntu004-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Issuer: commonName=ubuntu004-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX

| Public Key type: rsa

| Public Key bits: 1024

| Signature Algorithm: sha1WithRSAEncryption

| Not valid before: 2010-03-17T14:07:45

| Not valid after: 2010-04-16T14:07:45

| MD5: dcd9 ad90 6c8f 2f73 74af 383b 2540 8828

|\_SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 264d 31c6

|\_ssl-date: 2017-04-05T23:15:14+00:00; -108d23h16m54s from scanner time.

|\_ssl\_v2:

|\_SSLv2 supported

|\_ciphers:

|\_SSL2\_DES\_64\_CBC\_WITH\_MD5

Filter Hosts



### Introducción

Advertencia  
Definiciones y Conceptos  
Estándares y Recomendaciones

### Metodología de Pen Testing

Metodología NIST  
800-115  
Metodología PTES

### Herramientas de Pen Testing

Escáners  
Herramientas On-Line para Recolección de Inteligencia  
Suites de Ataques  
Distribuciones

### Conclusiones

Conclusiones  
Preguntas

**Nessus** Scans Policies Greg

Metasploit  
CURRENT RESULTS TODAY AT 2:51 PM

Configure Audit Trail Launch Export Filter Vulnerabilities

Hosts > 128.198.44.210 > Vulnerabilities 15

Severity	Plugin Name	Plugin Family	Count
CRITICAL	Debian OpenSSH/OpenSSL Package Random Number Generator Wea...	Gain a shell remotely	1
CRITICAL	Rogue Shell Backdoor Detection	Backdoors	1
CRITICAL	Linux Operating System Unsupported Version Detection	General	1
CRITICAL	VNC/Server 'password' Password	Gain a shell remotely	1
MEDIUM	Apache HTTP Server httpOnly Cookie Information Disclosure	Web Servers	1
MEDIUM	HTTP TRACE / TRACK Methods Allowed	Web Servers	1
MEDIUM	NFS Exported Share Information Disclosure	RPC	1
MEDIUM	NFS Shares World Readable	RPC	1
MEDIUM	Samba Badlock Vulnerability	General	1
MEDIUM	SMB Signing Disabled	Misc.	1
MEDIUM	SMTP Service STARTTLS Plaintext Command Injection	SMTP problems	1

**Host Details**

IP: 128.198.44.210  
DNS: mh208-12.uccs.edu  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (gutsy)  
Start: Today at 2:47 PM  
End: Today at 2:51 PM  
Elapsed: 4 minutes  
KB: Download

**Vulnerabilities**

Legend: Critical (red), Medium (yellow), Low (green), Info (blue)

```

root@kali: ~
File Edit View Search Terminal Tabs Help

root@kali: ~ x root@kali: ~ x root@kali: ~ x

root@kali:~# nikto -host http://webscantest.com
- Nikto v2.1.6
-----
+ Target IP: 69.164.223.208
+ Target Hostname: webscantest.com
+ Target Port: 80
+ Start Time: 2018-03-23 13:11:33 (GMT3)
-----
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie TEST_SESSIONID created without the httponly flag
+ Cookie NB_SRVID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x65 0x52770f2c6d6a3
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positive s.
+ OSVDB-3092: /cart/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7449 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2018-03-23 14:50:58 (GMT3) (5965 seconds)
-----
+ 1 host(s) tested
root@kali:~#

```

## Introducción

Advertencia  
Definiciones y Conceptos  
Estándares y Recomendaciones

## Metodología de Pen Testing

Metodología NIST 800-115  
Metodología PTES

## Herramientas de Pen Testing

Escáners  
Herramientas On-Line para Recolección de Inteligencia  
Suites de Ataques  
Distribuciones

## Conclusiones

Conclusiones  
Preguntas

Es posible usar Google o buscadores especializados para realizar escaneo de vulnerabilidades.

- ▶ Shodan
- ▶ Google Hacking Database
- ▶ Exploit DB

## Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

## Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

## Herramientas de Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

## Conclusiones

Conclusiones

Preguntas

### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

### Herramientas de Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

### Conclusiones

Conclusiones

Preguntas

# System Shock

## Metodología de Pen Testing

Miguel Angel  
Astor Romero

## Introducción

## Advertencia

## Definiciones y Conceptos

Estándares y Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

## Metodología PTES

## Herramientas de PenTesting

Escáneres

## Herramientas On-Line para Recolección de Inteligencia

## Suites de Ataques

## Distribuciones

## Conclusions

## Conclusiones

## Preguntas



Miguel Angel  
Astor Romero

The screenshot shows the Exploit Database website interface. At the top, there's a navigation bar with the Exploit Database logo and a 'GET CERTIFIED' button. Below the navigation bar, there are filters for 'Verified' and 'Has App'. A 'Show' dropdown is set to '15'. A search bar is present. The main content is a table of exploits with columns: Date, D (Download), A (Add), V (Verify), Title, Type, Platform, and Author.

Date	D	A	V	Title	Type	Platform	Author
2019-09-27				WordPress Theme Zoner Real Estate - 4.1.1 Persistent Cross-Site Scripting	WebApps	PHP	m0ze
2019-09-27				V-SQL GPON/EPON OLT Platform 2.03 - Remote Privilege Escalation	WebApps	Hardware	LiquidWorm
2019-09-27				V-SQL GPON/EPON OLT Platform 2.03 - Cross-Site Request Forgery	WebApps	Hardware	LiquidWorm
2019-09-27				V-SQL GPON/EPON OLT Platform 2.03 - Unauthenticated Configuration Download	WebApps	Hardware	LiquidWorm
2019-09-27				thesystem App 1.0 - 'username' SQL Injection	WebApps	PHP	Anil Baran Yelken
2019-09-27				thesystem App 1.0 - Persistent Cross-Site Scripting	WebApps	PHP	Ismail Güngör
2019-09-27				thesystem App 1.0 - 'server_name' SQL Injection	WebApps	PHP	Sadik Cetin
2019-09-27				Mobatek MobaXterm 12.1 - Buffer Overflow (SEH)	Remote	Windows	Xavi Beltran
2019-09-27				InoERP 0.7.2 - Persistent Cross-Site Scripting	WebApps	PHP	strider
2019-09-26				citcodecraashers Pic-A-Point 1.1 - 'Consignment' SQL Injection	WebApps	PHP	cakes
2019-09-26				inoERP 4.15 - 'download' SQL Injection	WebApps	PHP	Semen

## Introducción

Advertencia

Definiciones y Conceptos

Estándares y

Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

Metodología PTES

## Herramientas de PenTesting

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

## Conclusiones

Conclusiones

Preguntas

# Google Hacking Database

Metodología de  
Pen Testing

Miguel Angel  
Astor Romero

The screenshot shows the Exploit Database website interface. At the top, there's a dark blue header with the 'EXPLOIT DATABASE' logo and a 'GET CERTIFIED' button. Below the header, the main content area is titled 'Google Hacking Database'. It features a search bar with a 'Quick Search' label and a 'Filters' button. A table of search results is displayed, with columns for 'Date Added', 'Dork', 'Category', and 'Author'. The table lists various search results, including entries for 'wp-settings.php', 'dana-na/ filetype:cgi', 'wp-admin/user-edit.php', 'wp-admin/install.php', 'Powered By vBulletin 5.5.4 inurl:forum', 'cgi-sys/suspendedpage.cgi', 'logs/error.log', 'server-status intext:Apache server status for', 'conf/httpd.conf', and 'index.of users.db'.

Date Added	Dork	Category	Author
2019-09-27	site:*/wp-settings.php	Files Containing Juicy Info	Reza Abasi
2019-09-27	inurl:/dana-na/ filetype:cgi	Pages Containing Login Portals	Francis Al Victoriano
2019-09-26	site:*/wp-admin/user-edit.php	Pages Containing Login Portals	Reza Abasi
2019-09-26	site:*/wp-admin/install.php intitle:WordPress Installation	Footholds	Reza Abasi
2019-09-26	intext:Powered By vBulletin 5.5.4 inurl:forum.	Advisories and Vulnerabilities	IdeaEngine007
2019-09-25	site:*/cgi-sys/suspendedpage.cgi intitle:"Account Suspended"	Error Messages	Reza Abasi
2019-09-25	site:*/logs/error.log	Files Containing Juicy Info	Reza Abasi
2019-09-24	site:*/server-status intext:"Apache server status for"	Web Server Detection	Reza Abasi
2019-09-24	site:*/*/conf/httpd.conf	Files Containing Juicy Info	Reza Abasi
2019-09-24	intitle:index.of "users.db"	Files Containing Usernames	Mayur Parmar
2019-09-24	intitle:index.of "users.db"	Pages Containing Login	Reza Abasi

## Introducción

Advertencia

Definiciones y Conceptos

Estándares y

Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

Metodología PTES

## Herramientas de PenTesting

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

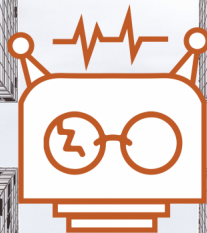
## Conclusiones

Conclusiones

Preguntas

Consider supporting the Cybersecurity Operations Center at The University of Texas at Austin.

[DONATE](#)



# Dorkbot

## Introducción

- Advertencia
- Definiciones y Conceptos
- Estándares y Recomendaciones

## Metodología de Pen Testing

- Metodología NIST 800-115
- Metodología PTES

## Herramientas de Pen Testing

- Escáners
- Herramientas On-Line para Recolección de Inteligencia
- Suites de Ataques
- Distribuciones

## Conclusiones

- Conclusiones
- Preguntas



Son *frameworks* que recopilan múltiples herramientas e implementaciones de ataques conocidos para su facil uso en pruebas de penetración.

- ▶ Metasploit
- ▶ Burp Suit
- ▶ Otros

## Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

## Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

## Herramientas de Pen Testing

Escáneres

Herramientas On-Line  
para Recolección de  
Inteligencia

**Suites de Ataques**

Distribuciones

## Conclusiones

Conclusiones

Preguntas

## Introducción

## Advertencia

## Definiciones y Conceptos

## Estándares y Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

## Metodología PTES

## Herramientas de PenTesting

## Escáneres

## Herramientas On-Line para Recolección de Inteligencia

### Suites de Attaques

## Distribuciones

## Conclusions

## Conclusiones

## Preguntas

```
[*] Starting Metasploit Console...

[##### $a, #####]
[##### $S`?a, #####]
[##### `?a, #####]
[##### ,a$# #####]
[##### ,a$S"" #####]
[##### $SP" #####]
[##### `a, #####]
[##### "a,$$ #####]
[##### "a$ #####]
[##### #####]

=[ metasploit v4.11.10-dev ]
+ -- --[ 1529 exploits - 974 auxiliary - 273 post ]
+ -- --[ 437 payloads - 38 encoders - 8 nops ]
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[+]
[+] Metasploit Pro extensions have been activated
[+]
[*] Successfully loaded plugin: pro
```

# Burp Suite

## Metodología de Pen Testing

Miguel Angel  
Astor Romero

### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

### Herramientas de Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

### Conclusiones

Conclusiones

Preguntas

The screenshot displays the Burp Suite interface with the following components:

- Top Menu:** Burp, Project, Intruder, Repeater, Window, Help.
- Navigation Bar:** Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options.
- Tasks Panel (Left):**
  - 1. Live passive crawl from Proxy (all traffic): Items added to site map: 380, Responses processed: 866, Responses queued: 100.
  - 12. Crawl of Default configuration: Requests: 56, Errors: 0.
  - 13. Crawl of Crawl strategy - most complete: Requests: 56, Errors: 0.
  - 17. Audit of Default configuration: Issues: 2, Requests: 19,168, Errors: 0.
- Issue Activity Panel (Right):** A table listing detected issues with columns for ID, Task, Time, Info, Issue type, Host, and Path. Issues include 'Unencrypted communications', 'Cleartext submission of password', 'Session token in URL', and 'SQL injection'.
- Event Log (Bottom Left):** A table showing system events with columns for Time, Type, Source, and Message. It includes messages about authentication failures and audit term pauses.
- Alert Detail (Bottom Right):** A detailed view of an 'SQL Injection' issue. It shows the severity as 'High', confidence as 'Certain', and the host as 'http://www.youranattack.com'. The issue details state: 'The username parameter appears to be vulnerable to SQL injection attacks. A single quote was submitted in the username parameter, and a database error message was returned. Two single quotes were then submitted and the error message disappeared. You should review the contents of the error message, and the application's handling of other input, to confirm whether a vulnerability is present.' The payload used was '\*(select\*(from(select(sleep(20)))a))'.

- ▶ Kali Linux
- ▶ Parrot Security
- ▶ Blackarch Linux
- ▶ Backbox
- ▶ Fedora Security Spin

## Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

Metodología PTES

## Herramientas de PenTesting

Escáneres

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

## Conclusiones

Conclusiones

Preguntas



### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

### Herramientas de Pen Testing

Escáneres

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

### Conclusiones

Conclusiones

Preguntas

Miguel Angel  
Astor Romero



### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de PenTesting

Metodología NIST  
800-115

Metodología PTES

### Herramientas de PenTesting

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

### Conclusiones

Conclusiones

Preguntas



### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

### Herramientas de Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

### Conclusiones

Conclusiones

Preguntas

### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de Pen Testing

Metodología NIST  
800-115

Metodología PTES

### Herramientas de Pen Testing

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

### Conclusiones

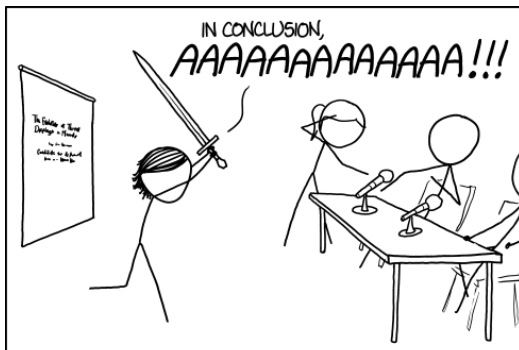
Conclusiones

Preguntas









THE BEST THESIS DEFENSE IS A GOOD THESIS OFFENSE.

## Introducción

## Advertencia

## Definiciones y Conceptos

## Estándares y Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

## Metodología PTES

## Herramientas de PenTesting

Escáneres

## Herramientas On-Line para Recolección de Inteligencia

### Suites de Attaques

## Distribuciones

## Conclusions

## Conclusiones

## Preguntas

- ▶ El PenTesting es una metodología, no un conjunto de herramientas.
- ▶ La planificación y el reporte son tan/más importantes que el análisis y la explotación en si.
- ▶ Siempre hay que tener permiso y apegarse a las regulaciones al hacer PenTesting.
- ▶ Siempre hay que tener permiso y apegarse a las regulaciones al hacer PenTesting.
- ▶ Siempre hay que tener permiso y apegarse a las regulaciones al hacer PenTesting.

## Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

Metodología PTES

## Herramientas de PenTesting

Escáners

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques  
Distribuciones

## Conclusiones

Conclusiones

Preguntas

Miguel Angel  
Astor Romero

coursera

Browse > Information Technology > Security

This course is part of the **Cybersecurity for Business Specialization**

Offered By



University of Colorado  
Boulder · Colorado Springs · Fort Collins · Research World Campus

## Proactive Computer Security

★★★★★ 4.6 98 ratings • 22 reviews

Go To Course

Already enrolled

3,047 already enrolled!

### Introducción

Advertencia

Definiciones y Conceptos

Estándares y Recomendaciones

### Metodología de Pen Testing

Metodología NIST 800-115

Metodología PTES

### Herramientas de Pen Testing

Escáneres

Herramientas On-Line para Recolección de Inteligencia

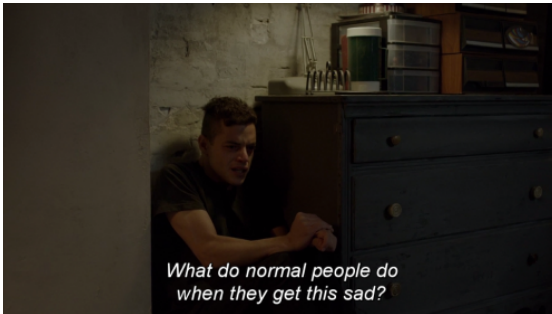
Suites de Ataques Distribuciones

### Conclusiones

Conclusiones

Preguntas

# Tarea



Leer la recomendación NIST 800-115 y hacer un resumen de a lo sumo 10 páginas de su contenido.

Fecha de entrega Lunes 14 de octubre de 2019.

## Introducción

## Advertencia

## Definiciones y Conceptos

Estándares y Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

## Metodología PTES

## Herramientas de PenTesting

## Escáneres

## Herramientas On-Line para Recolección de Inteligencia

## Suites de Ataques

### Distribuciones

## Conclusiones

## Conclusiones

## Preguntas

## Taller de PenTesting



### Introducción

Advertencia

Definiciones y Conceptos

Estándares y  
Recomendaciones

### Metodología de PenTesting

Metodología NIST  
800-115

Metodología PTES

### Herramientas de PenTesting

Escáneres

Herramientas On-Line  
para Recolección de  
Inteligencia

Suites de Ataques

Distribuciones

### Conclusiones

Conclusiones

Preguntas

## ¿Preguntas?

## Introducción

## Advertencia

## Definiciones y Conceptos

## Estándares y Recomendaciones

## Metodología de PenTesting

Metodología NIST  
800-115

## Metodología PTES

## Herramientas de PenTesting

## Escáneres

## Herramientas On-Line para Recolección de Inteligencia

## Suites de Attaques

## Distribuciones

## Conclusions

## Conclusiones

## Preguntas

