Metodología de PenTesting

Miguel Angel Astor Romero

27 de septiembre de 2019

Agenda

Introducción

Metodología de PenTesting

Herramientas de PenTesting

Conclusiones

Cuidado con lo que Hagan

Definición

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.

Conceptos ITU-T X.800

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

Conceptos ITU-T X.800

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.

Conceptos ITU-T X.800

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

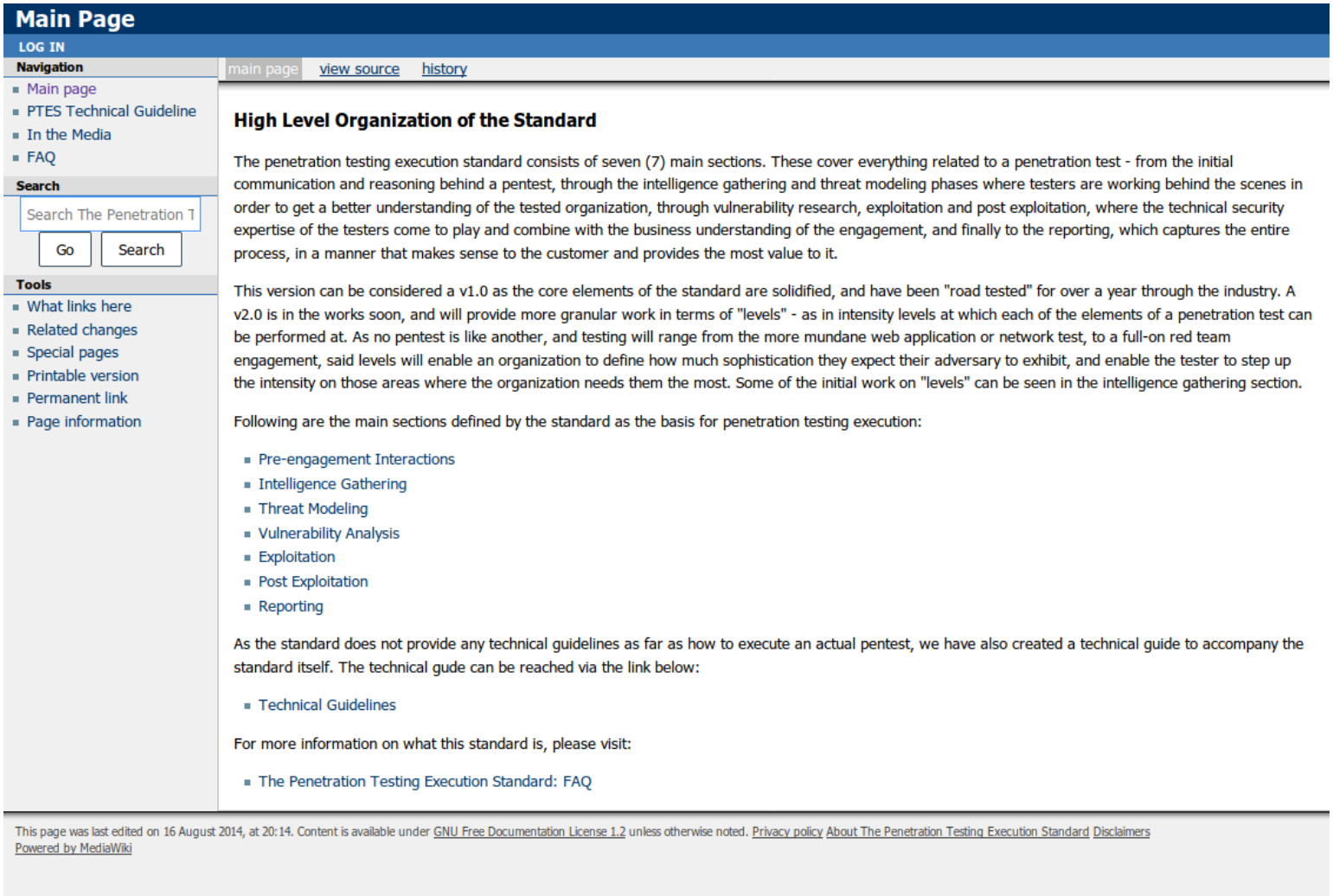
Acción que vulnera la seguridad de un sistema.

NIST 800-115

Technical Guide to InfoSec Testing and Assessment

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

PTES



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 gude 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

```
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
```

NIST 800-115

La recomendación NIST 800-115 establece 3 etapas para el proceso de PenTesting:

- Planificación
- Ejecución
- Post-Ejecución

Fases de NIST 800-115

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.

Fases de NIST 800-115

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.

Ejecución

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

Fases de NIST 800-115

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.

Ejecución

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

Post-Ejecución

- Desarrollar recomendaciones.
- Reportar.
- Mitigar.

Penetration Testing Execution Standard

- Estándar informal desarrollado por profesionales.
- Consta de dos partes:
  - Recomendaciones de metodología.
  - Guía técnica.
- Más detallado que NIST 800-115. Define 7 fases para el proceso de PenTesting.

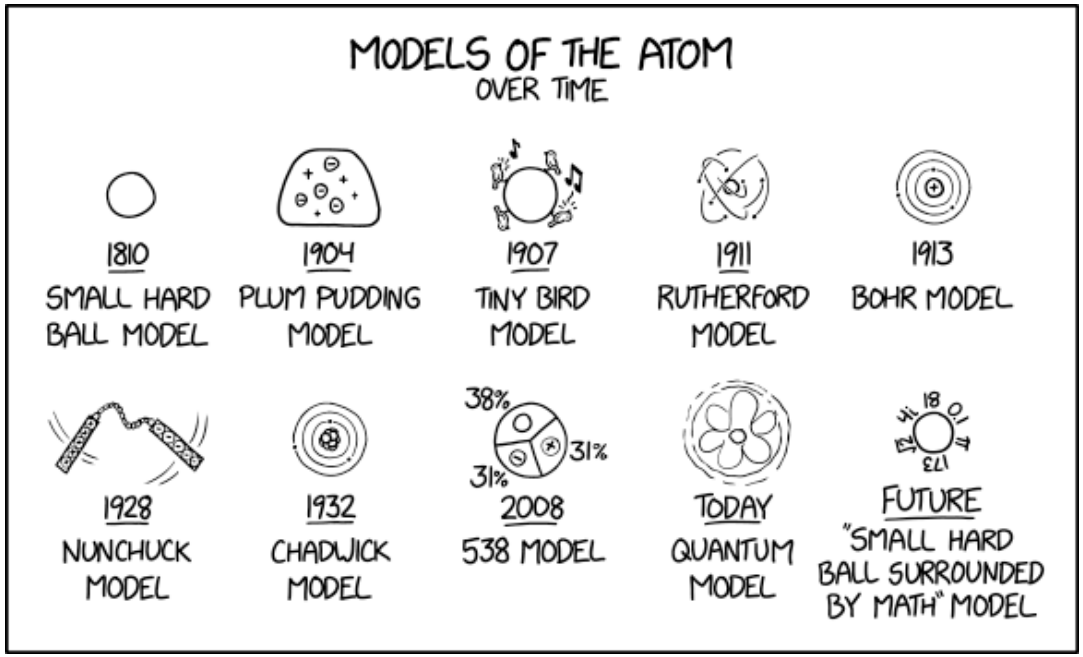
Interacciones Pre-Compromiso

- Reuniones previas a las pruebas.
- Se busca establecer:
  - Alcance.
  - Dominio de pruebas.
  - Marco de tiempo.
  - Costos.
  - Permisos.
  - Marco legal.

Recolección de Inteligencia

- Recopilación de información sobre la organización, su entorno y sus sistemas.
- Se define en 3 niveles:
  - Dirigido por estándares (*compliance driven*).
  - Orientado a mejores prácticas.
  - Patrocinado por el estado.

Modelado de Amenazas



- Consiste en:
  - Identificar los objetivos dentro de la organización, estableciendo su nivel de riesgo y objetivos secundarios.
  - Identificar el perfil (motivación, nivel técnico y herramientas) de un posible atacante.

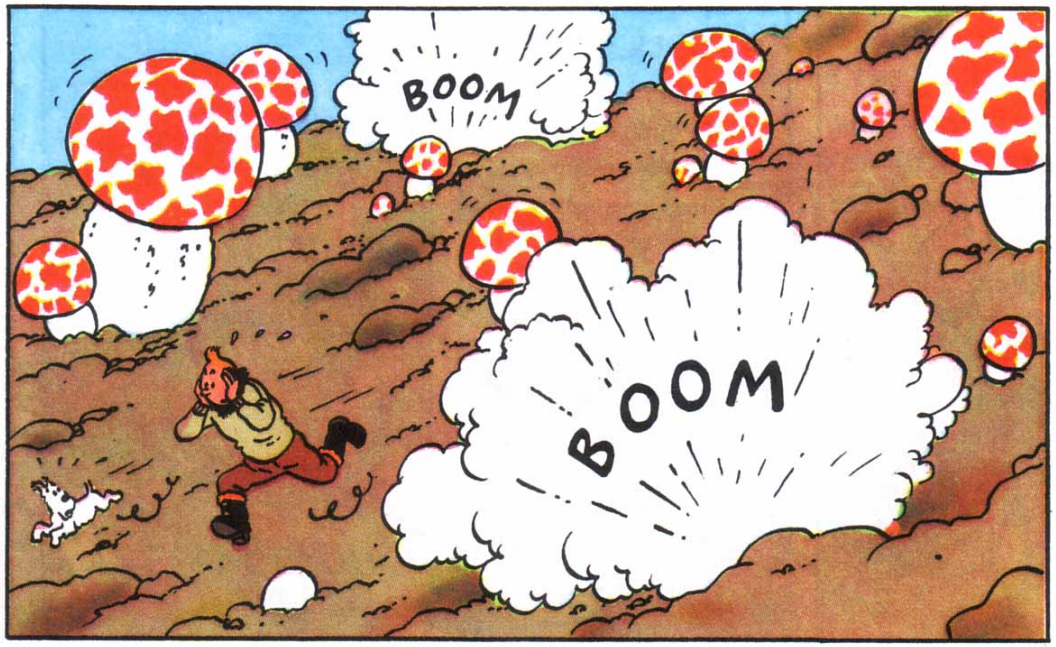
Análisis de Vulnerabilidades

- Uso de herramientas automatizadas (escáneres) y/o análisis manual para identificar amenazas.
- Puede hacerse a nivel de red, sistema operativo, aplicaciones y Web.

Explotación

- 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.

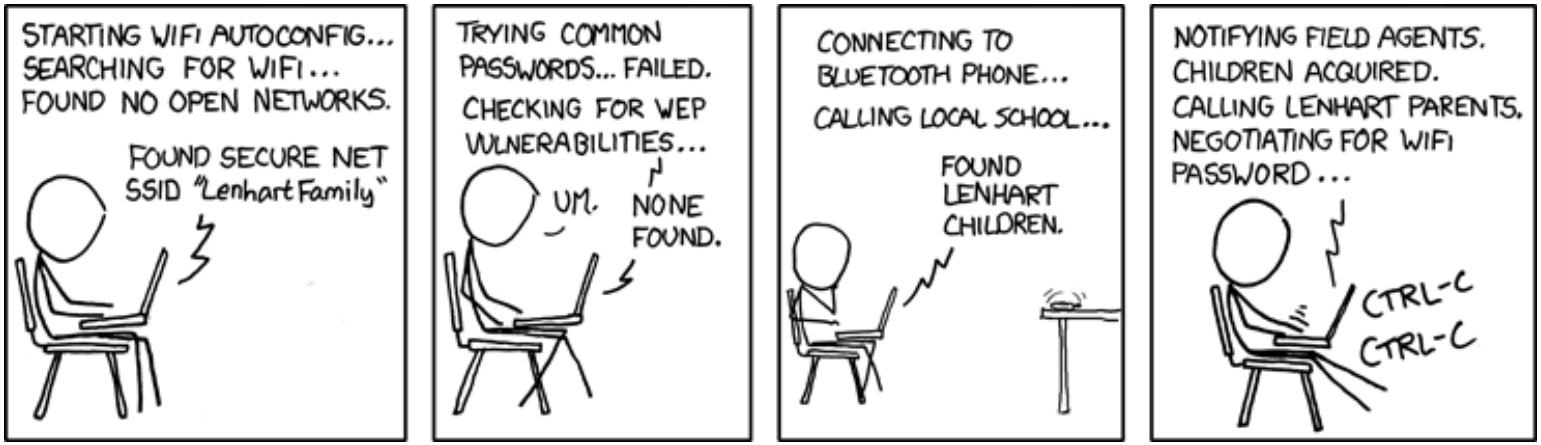
Post-Explotación



- 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.

Reporte

- 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.



Herramientas para Escaneo de Vulnerabilidades

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

`nslookup`

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

Herramientas Básicas

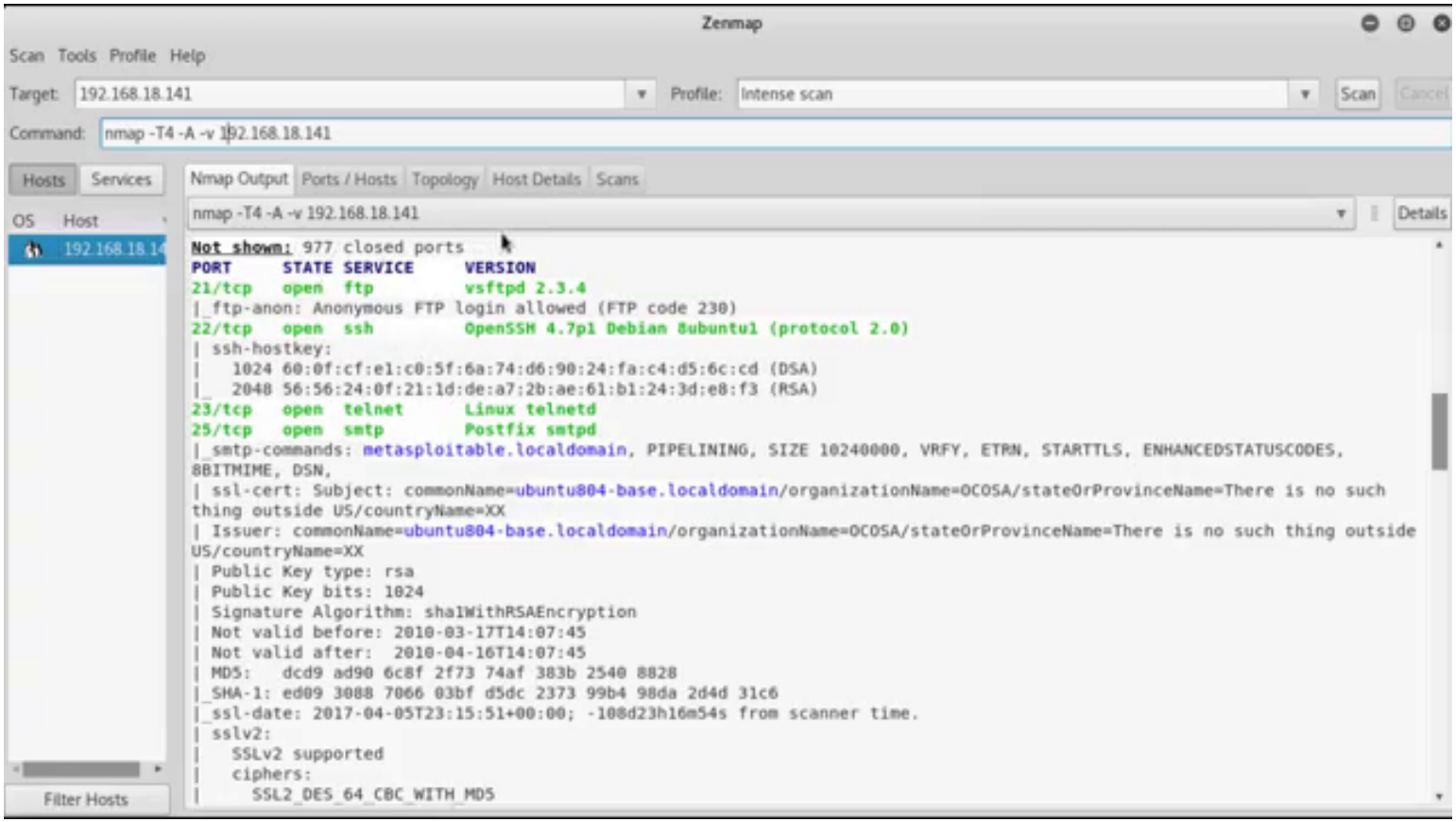
`nslookup`

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

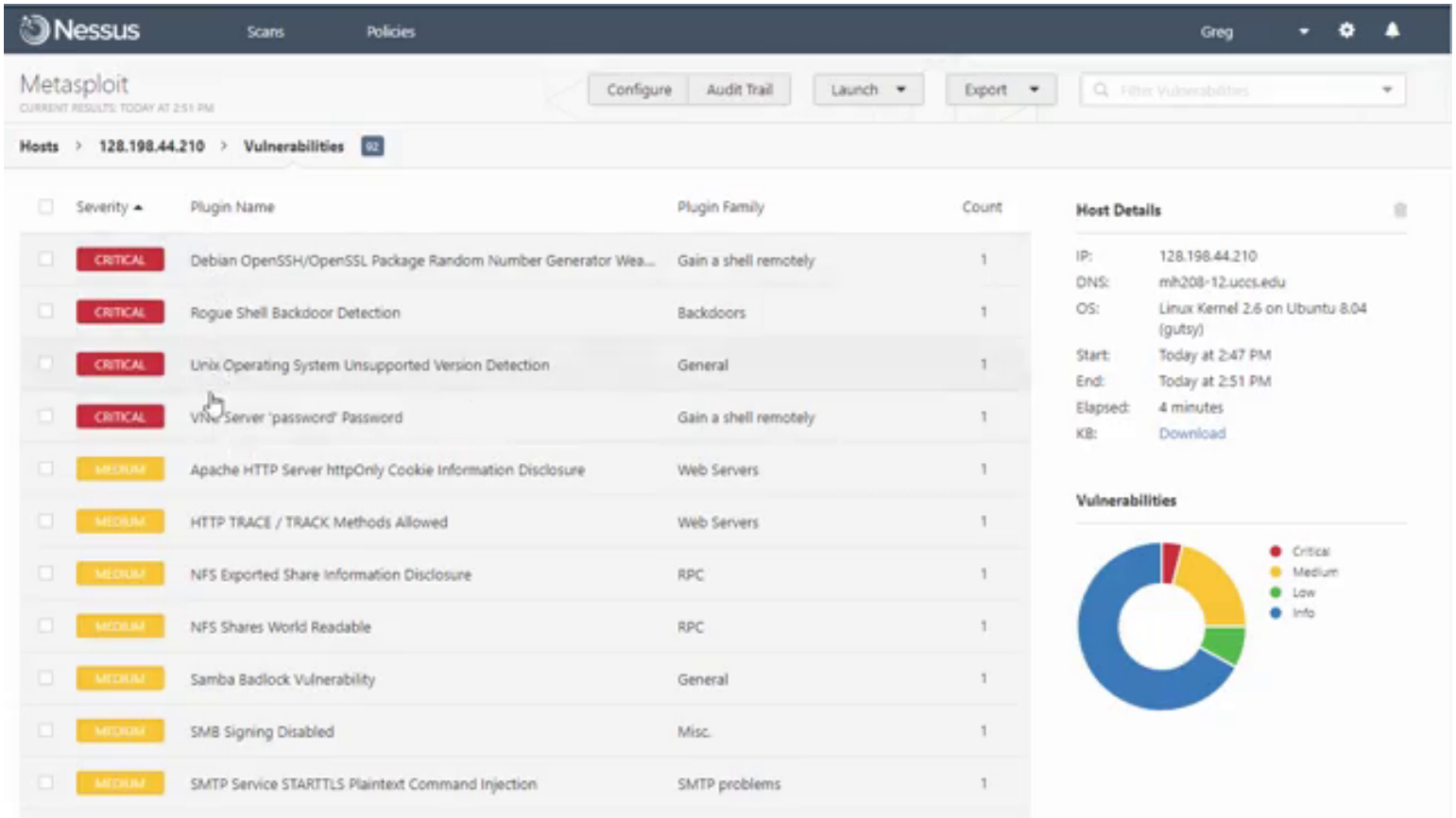
`dig`

- 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.

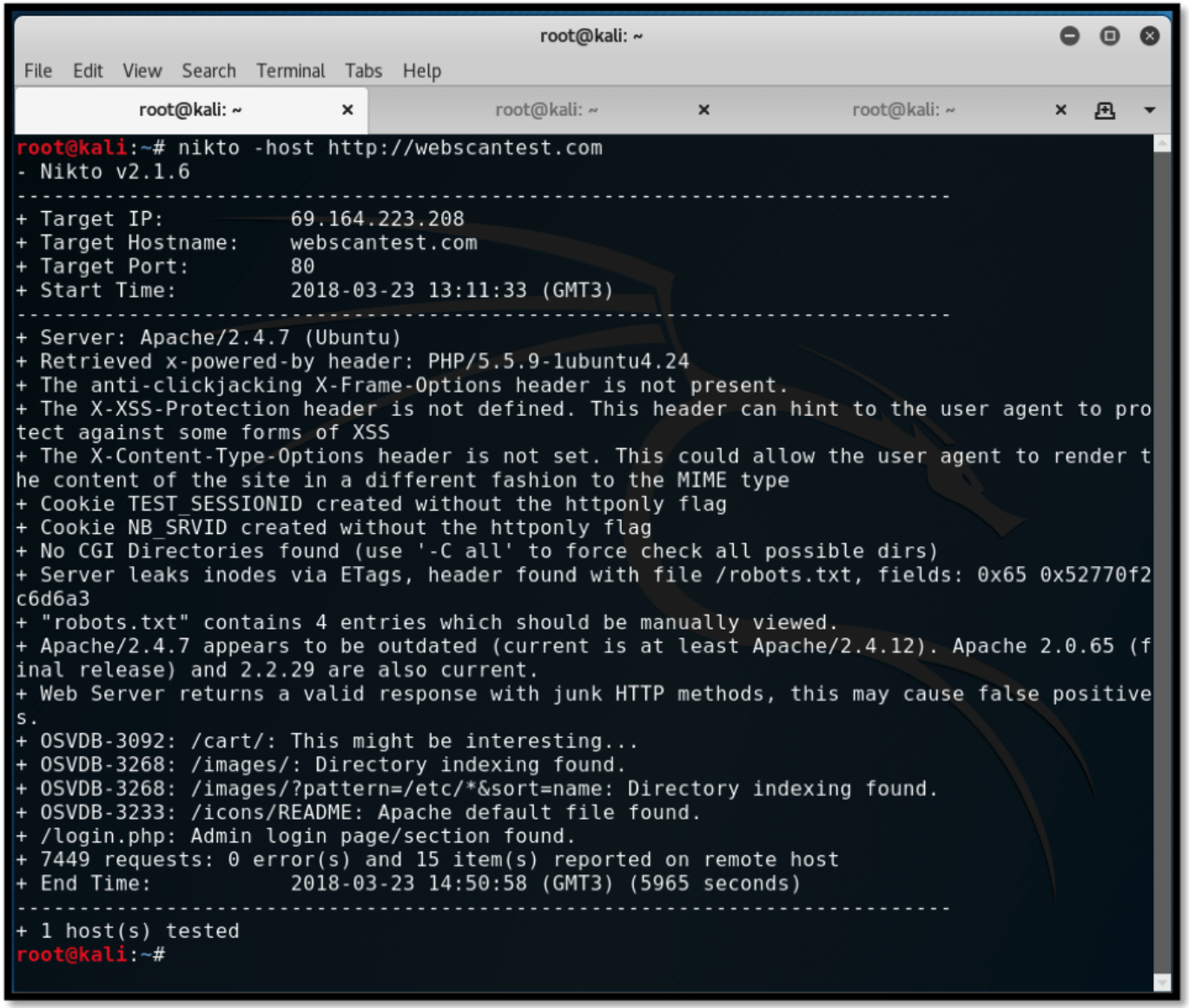
NMAP



Nessus



Nikto

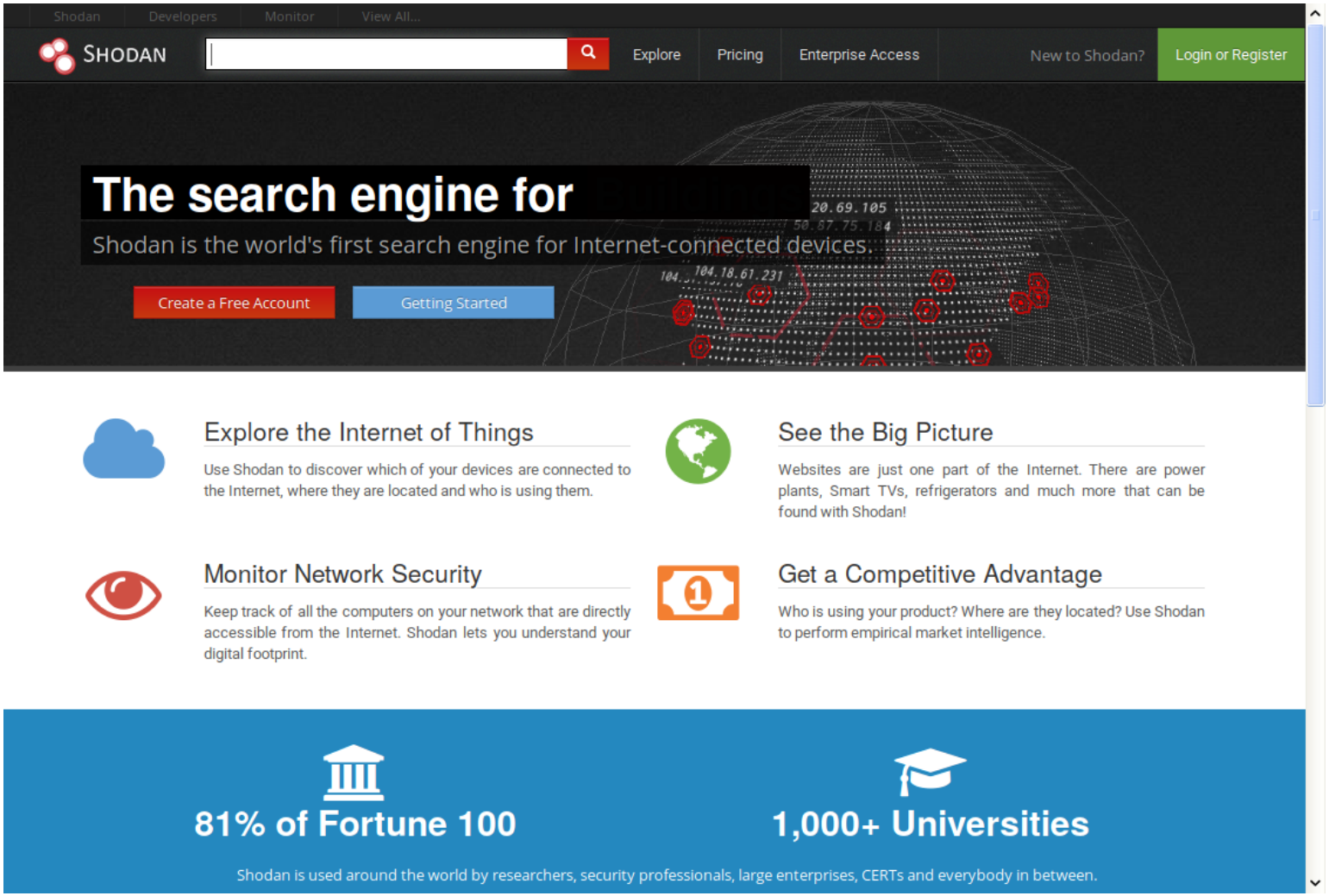


Recolección de Inteligencia On-Line

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

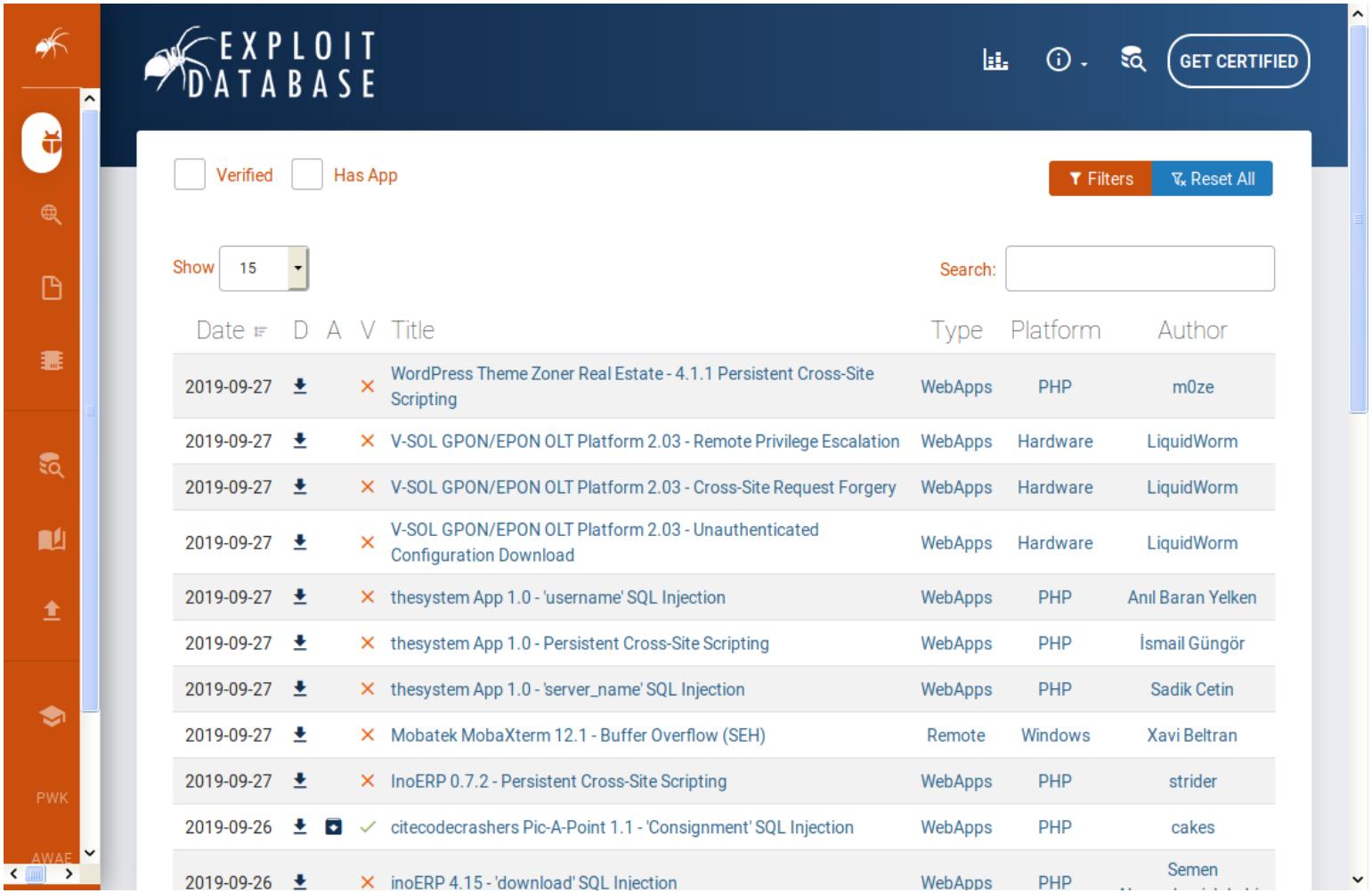
- Shodan
- Google Hacking Database
- Exploit DB

Shodan

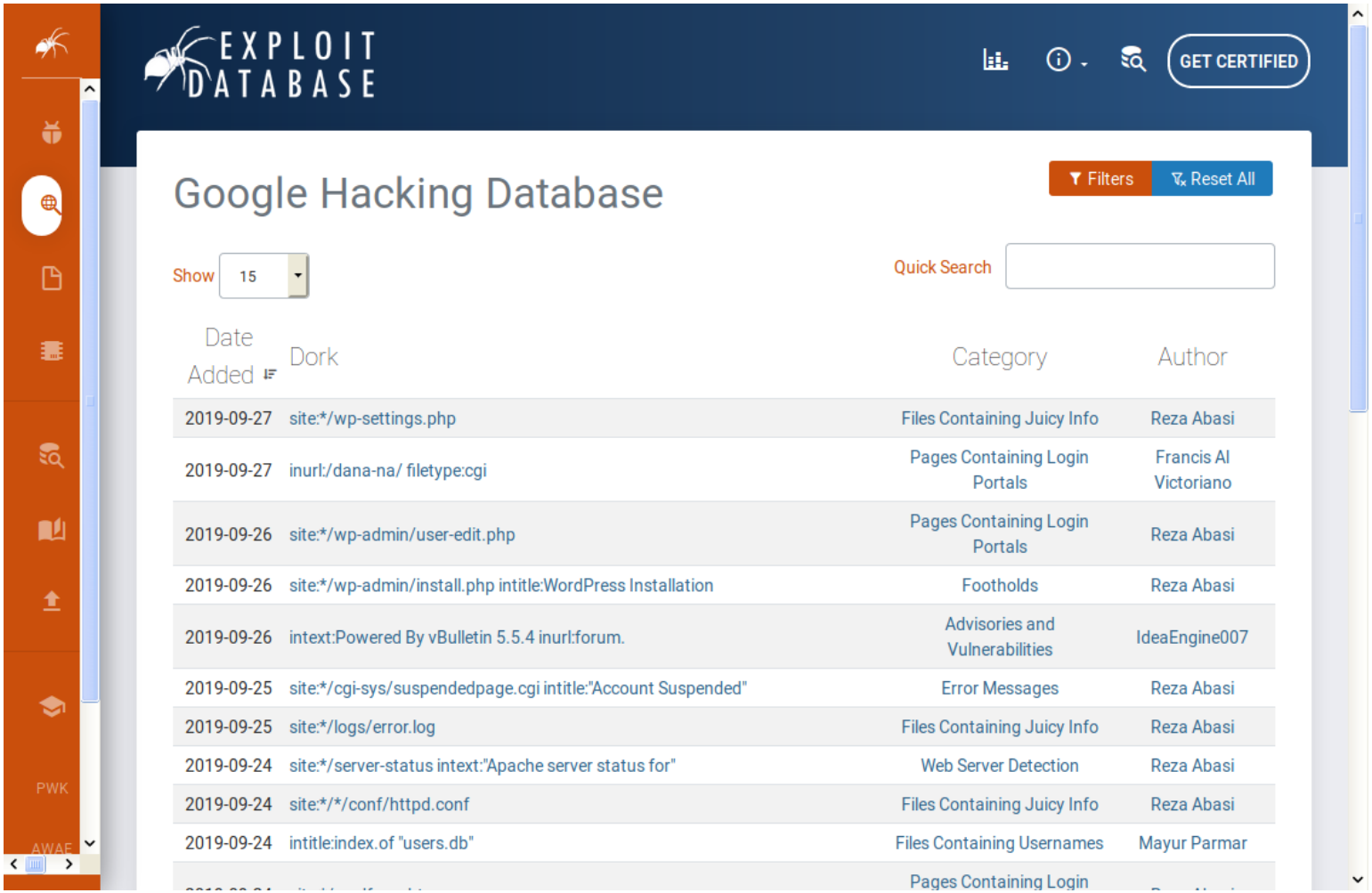


System Shock

Exploit DB



Google Hacking Database



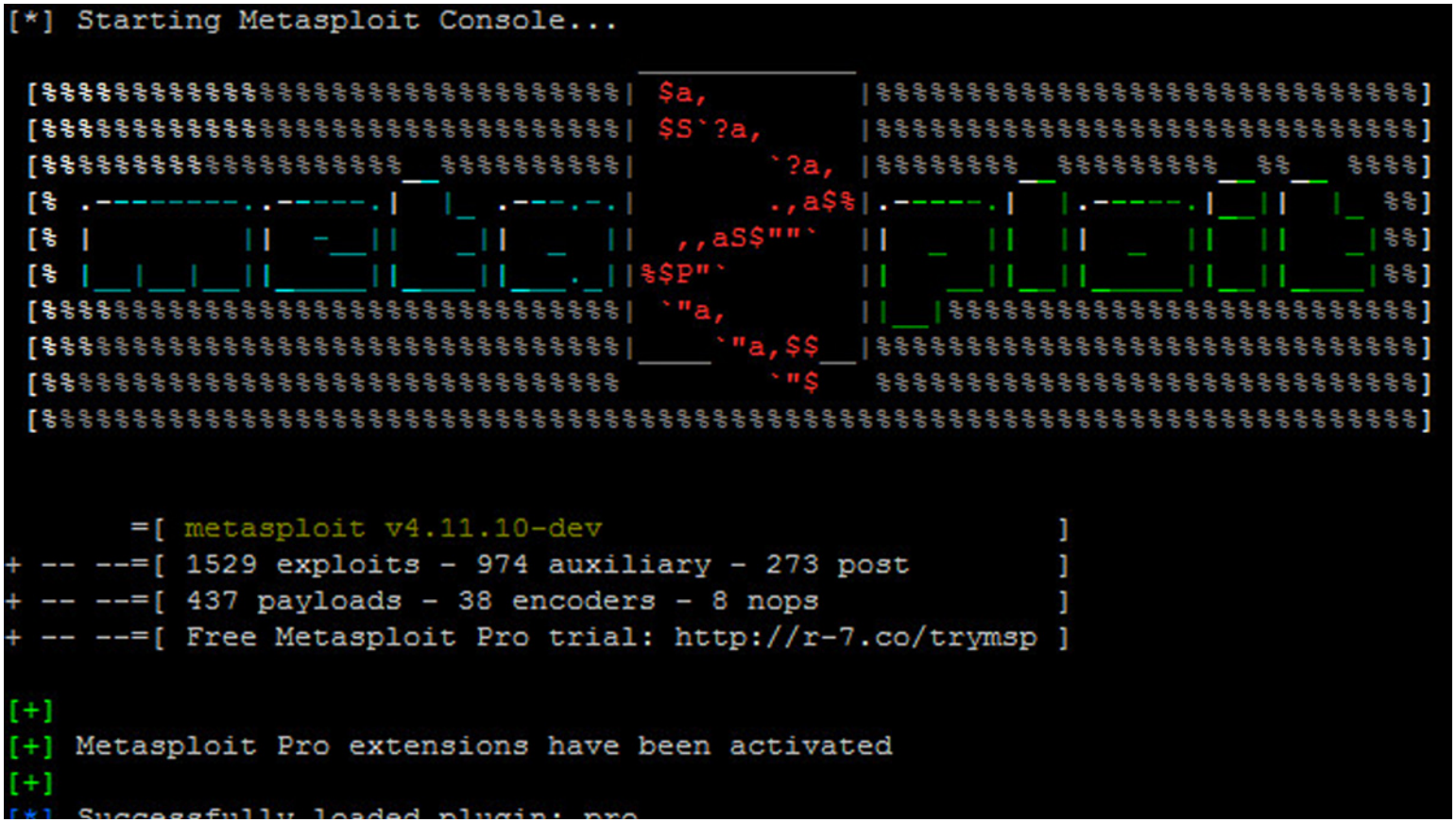
Dorkbot

Suites de Ataques

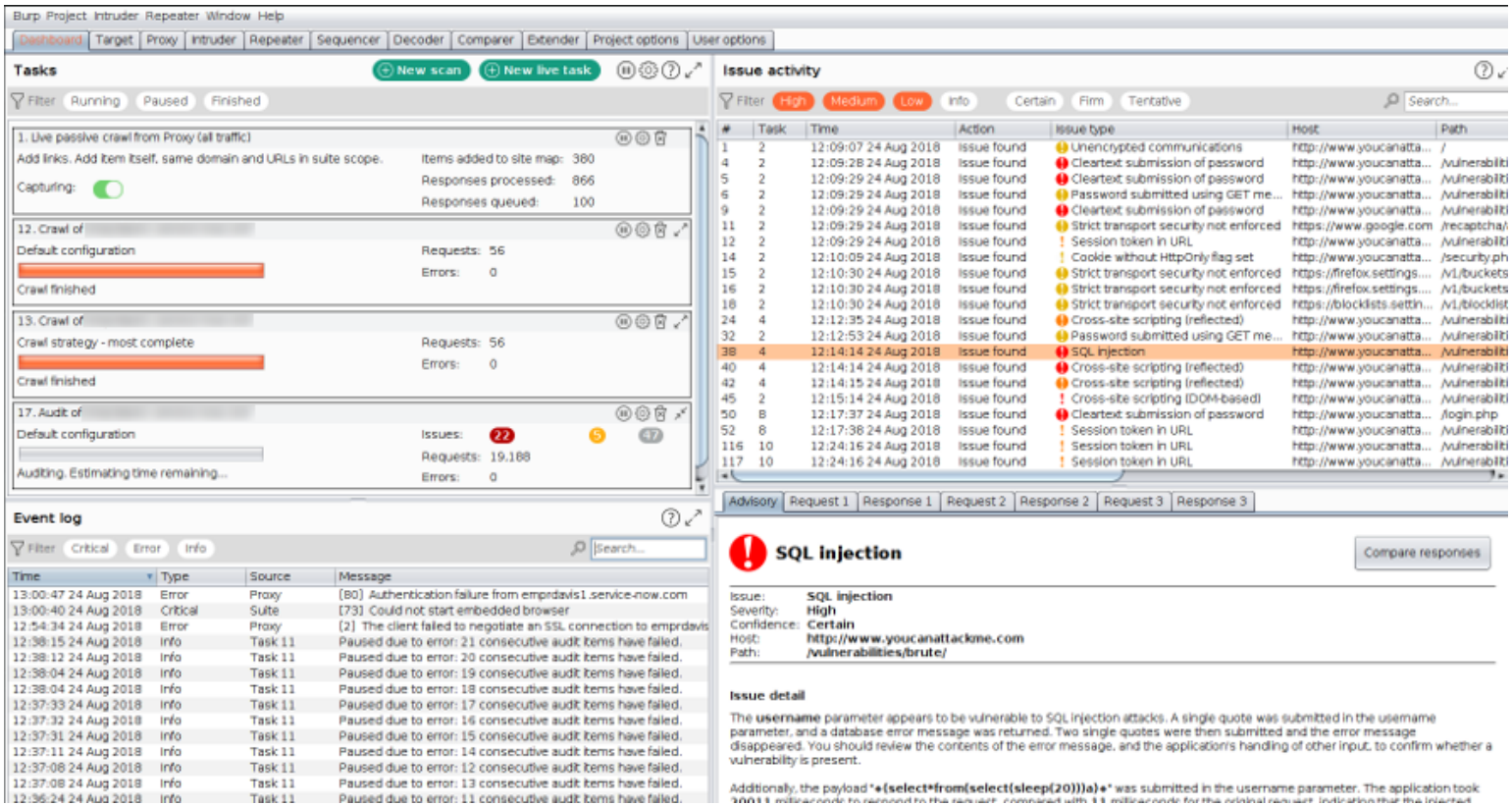
Son *frameworks* que recopilan múltiples herramientas e implementaciones de ataques conocidos para su facil uso en pruebas de penetración.

- Metasploit
- Burp Suit
- Otros

Metasploit


[*] Starting Metasploit Console...
=[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
[+]

Burp Suite



Distros de Linux para PenTesting

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

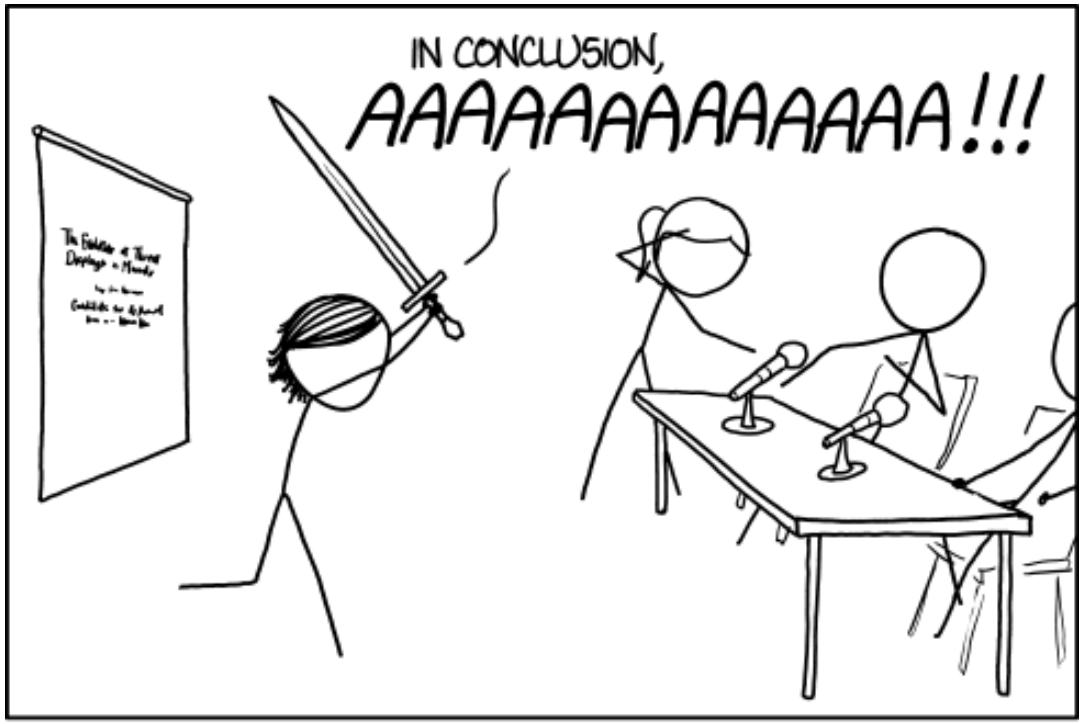
Kali Linux

Parrot Security

Blackarch Linux

Backbox

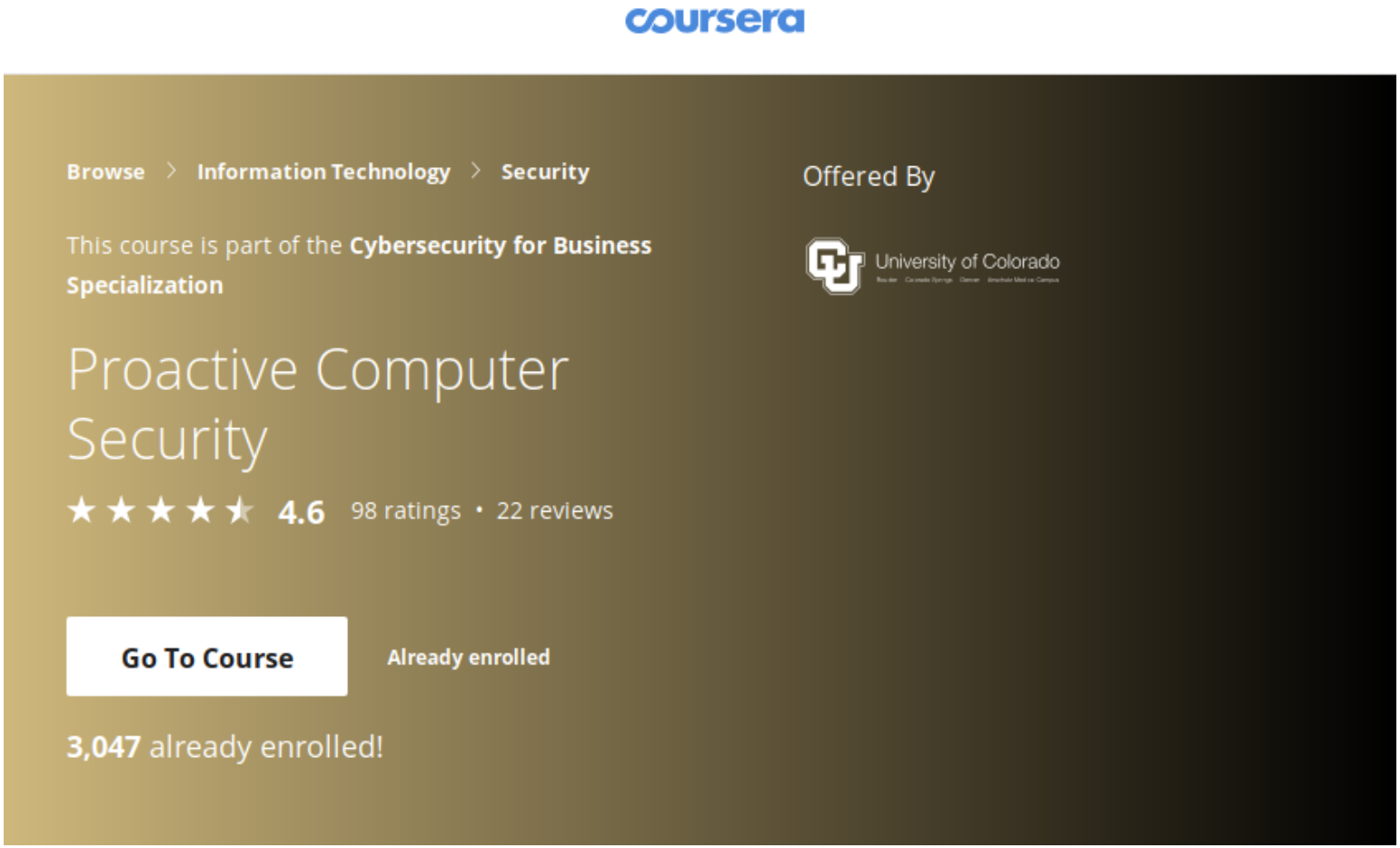
Backbox


IN CONCLUSION,
AAAAAAAAAAAAA!!!
THE BEST THESIS DEFENSE IS A GOOD THESIS OFFENSE.

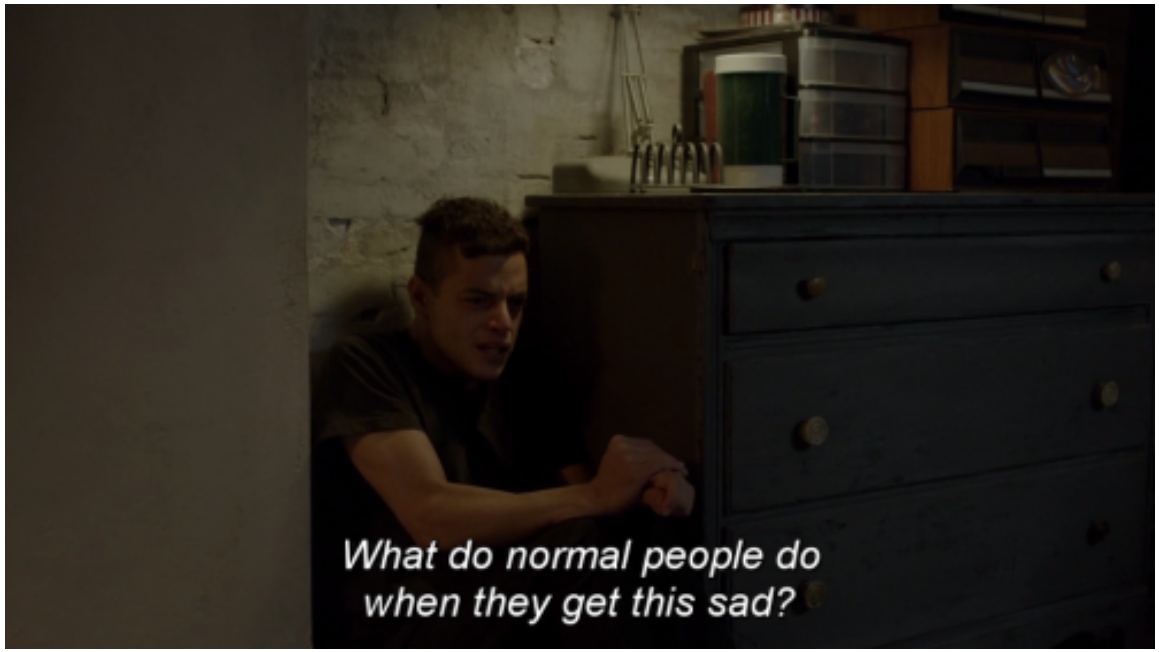
Conclusiones

- 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.

Curso Recomendado



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.

Próxima Clase

Taller de PenTesting

¿Preguntas?