CURSO HACKING ÉTICO

INTRODUCCIÓN

"Si conoces al enemigo y te conoces a ti mismo, no temas el resultado de cien batallas; si te conoces a ti mismo, pero no conoces al enemigo, por cada batalla ganada perderás otra; si no conoces al enemigo ni a ti mismo, perderás cada batalla "

- Sun Tzu, El Arte de la Guerra

INTRODUCIÓN AL HACKING ÉTICO

- Definición de Hacking Ético
- Fundamentos de la Seguridad de la Información
- Amenazas de seguridad y vectores de ataque
- Tipos de Pen Test
- Metodología
- Fases
- Como construir un laboratorio seguro para practicar

DEFINICIÓN DE HACKING ÉTICO

Entendemos por Hacking Ético la práctica de atacar sistemas con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas.

¿ **Es legal** ?

El Pentesting es totalmente legal siempre y cuando los ataques que realicemos sean dirigidos hacia equipos propios o de nuestros clientes (bajo su consentimiento **expreso y firmado**).

De no ser así, sí que podríamos usar de forma correcta la terminología “hackear”, cosa que en la mayoría de países **es un acto penado con prisión**.

Diferenciamos el Hacking Ético, del Hacking, en que el primero con-tamos con el permiso y aprobación del propietario del sistema a ata-car, mientras que durante un ataque no consentido por el propietario incurriremos en un delito de Hacking.

Recuerda que existen sistemas de detección de intrusiones (o IDS de sus siglas en inglés Intrusion Detection System). Son programas de detección de accesos no autorizados a un computador o a una red.

Tipos de IDS

- **HIDS (HostIDS):**—Detectan modificaciones en el equipo infectado.
- **NIDS (NetworkIDS):**—Detectan ataques a todo el segmento de la red.

Las leyes importan. Asesórate !!!

- Directiva 2006/24/CE del Parlamento Europeo y del Consejo, 15 de marzo de 2006. Directiva 2006/24/CE.

- El Tribunal de Justicia declara inválida la Directiva sobre la conservación de datos. **Luxemburgo, 8 de abril de 2014** Comunicado de prensa nº 54/14

Fundamentos Seguridad de la información

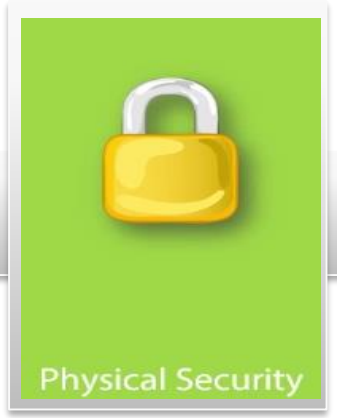
- Authenticity
- Integrity
- Availability
- Confidentiality

Amenazas de seguridad y vectores de ataque

- Hosts
- Aplicaciones
- Humanos
- Redes

Hosts


Footprinting


Physical Security


windows8user
Windows 8
Passwords


Malware

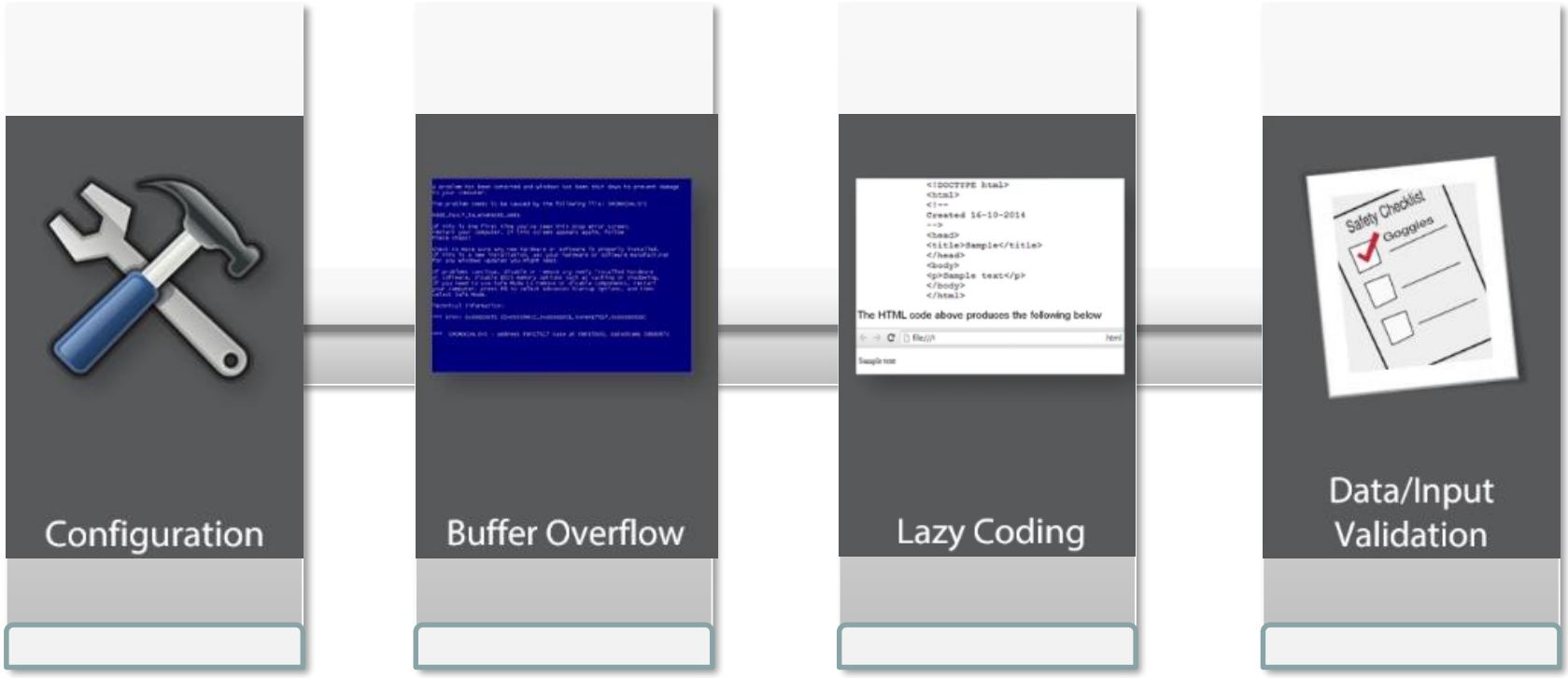

Denial of Service


Unauthorized Access

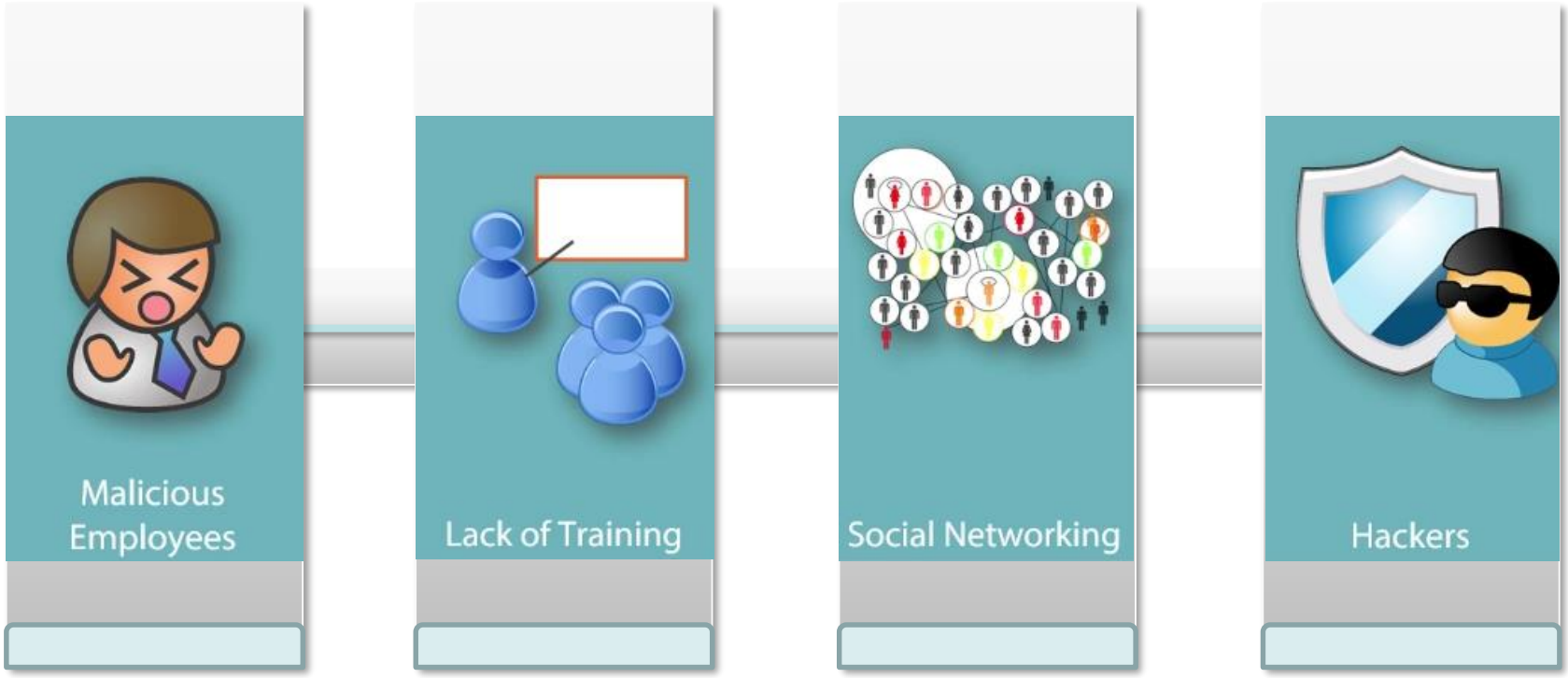

Privilege Escalation


Back Doors

Aplicaciones



Humanos


Malicious Employees
Lack of Training
Social Networking
Hackers

Redes

¿ De qué eres consciente ?

- Entornos de VM y Cloud
- Software y OS sin parchear
- Redes sociales
- Usuarios internos
- Malware
- Botnets
- Falta de políticas de seguridad
- Cumplimiento de normativas y leyes,
- Complejidad de la infraestructura de red.
- Dispositivos móviles

Tipos de Pen test

CAJA NEGRA

- No se entrega ningún tipo de información.
- Hay que descubrir los equipos y la infraestructura de la red, servicios, tecnologías , web, etc.

CAJA BLANCA

- Se entrega la información interna de la empresa.
- Mapa de red, firewalls, S,O, usuarios, etc.
- No se invierte tiempo en la fase de descubrimiento.

CAJA GRIS

- Mezcla características de las dos anteriores.
- Se da a conocer alguna información al pen tester.
- Útil para conocer ataques que puede hacer un usuario interno de la empresa con usuarios y privilegios específicos.

Tipos de Pen test

KILL-CHAING → Metodología de origen militar, (más info)

OSSTMM → Esta se basa en diferentes escenarios y cómo se debe de actuar ante cada uno (más info)

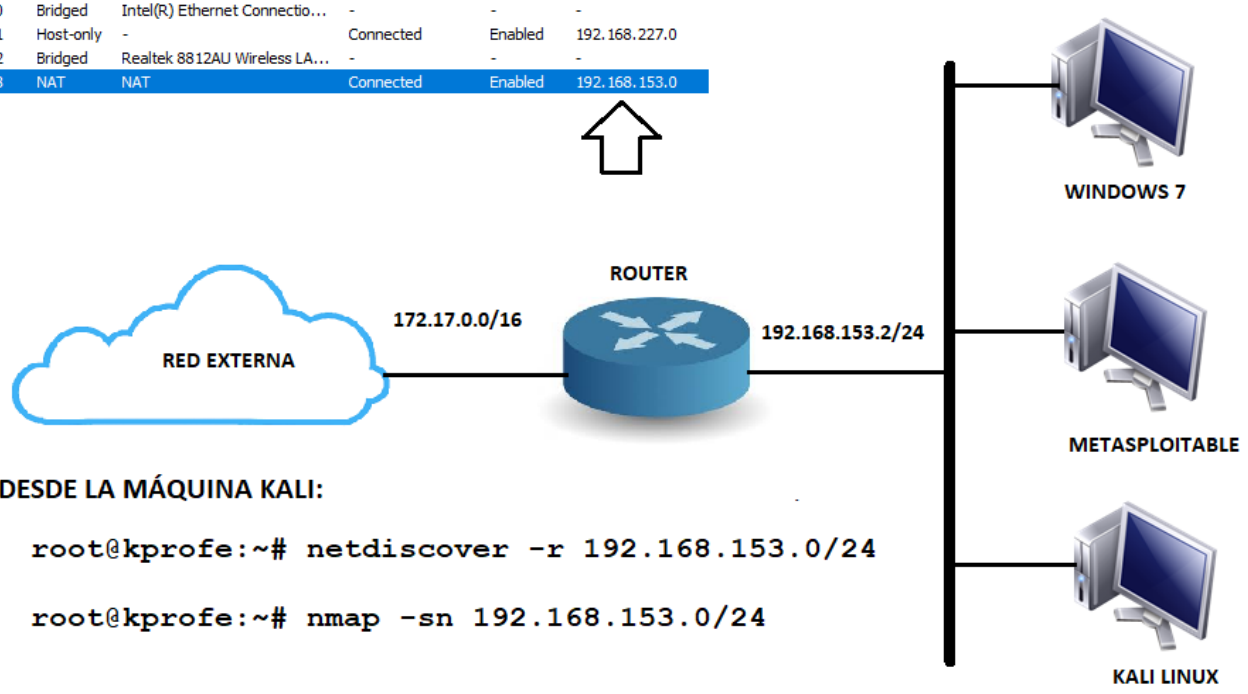
ISSAF → Esta se divide por escenarios que además incluyen tipo de servicios (si es MySQL, Oracle, etc…) (más info)

Fases de un Pen Test

El escaneo de puertos permite examinar redes o computadores en busca de objetivos o servicios que poder explotar.

Laboratorio de trabajo

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Intel(R) Ethernet Connectio...	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.227.0
VMnet2	Bridged	Realtek 8812AU Wireless LA...	-	-	-
VMnet8	NAT	NAT	Connected	Enabled	192.168.153.0



DESDE LA MÁQUINA KALI:

```
root@kprofe:~# netdiscover -r 192.168.153.0/24

root@kprofe:~# nmap -sn 192.168.153.0/24
```

VM WORKSTATION EN MODO NAT