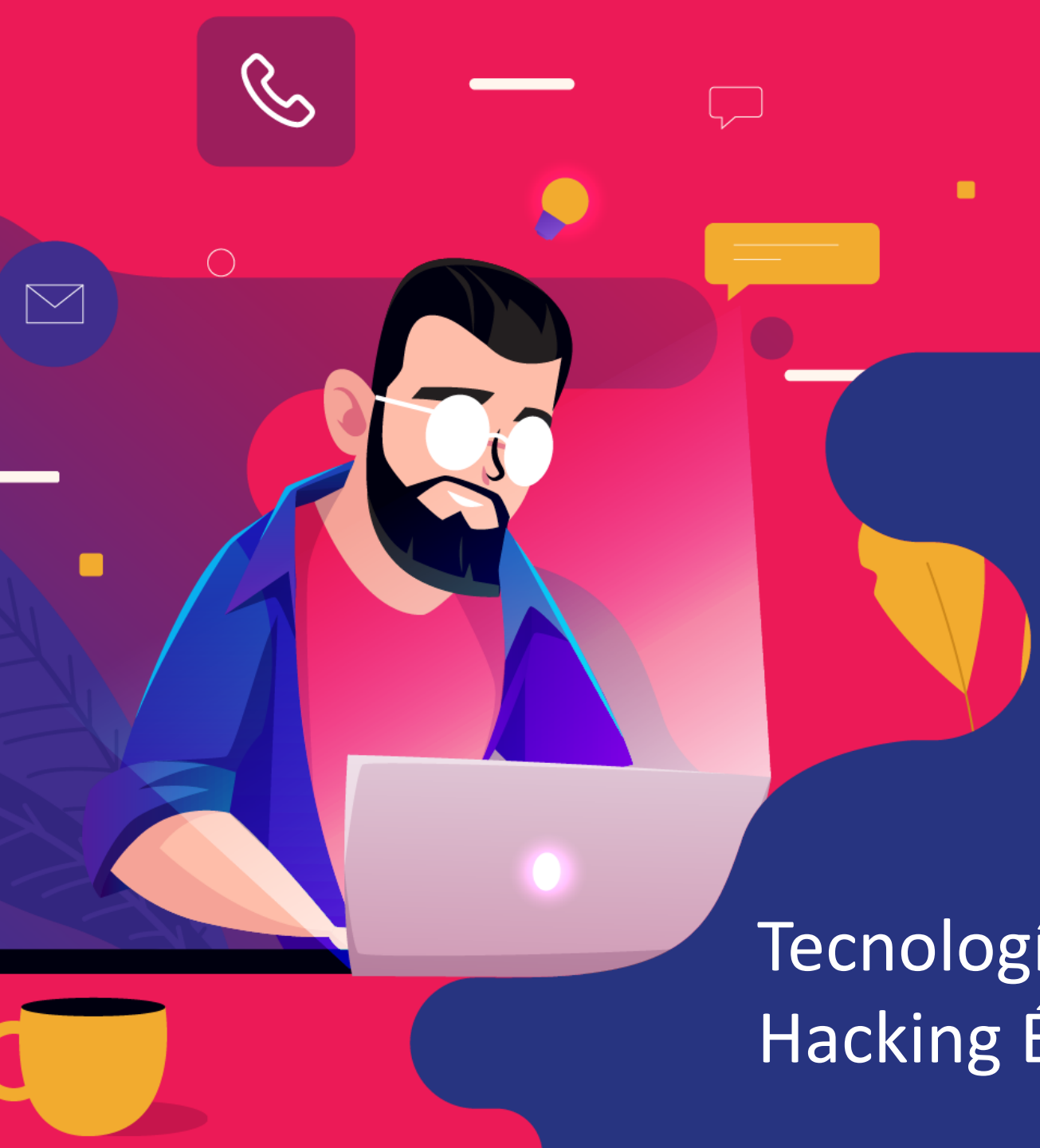


FIDE VIRTUAL

Principios de Ciberseguridad

Tecnologías de ataque a los sistemas - Hacking Ético

Introducción al módulo

- Estándares y regulaciones sobre seguridad en TI
  - ISO27001
  - COBIT
  - ITIL
  - Entes éticos reguladores
  - Ley en CR

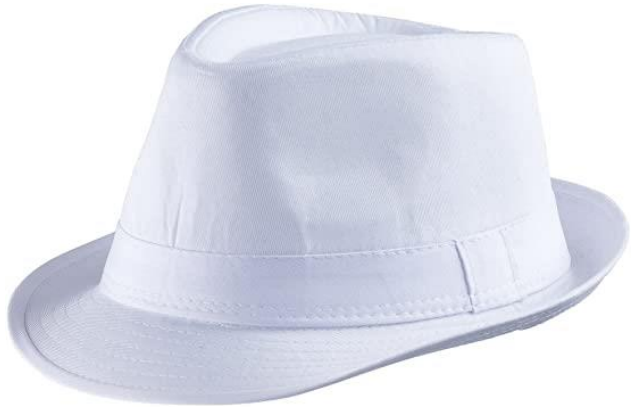
COBIT®

ITIL®

FIDE VIRTUAL

Introducción al módulo

- Tecnologías de ataque a los sistemas - Hacking Ético
  - Amenazas a la seguridad
  - Que es el Hacking Ético
  - Quien es el Ethical Hacker
  - Fases de ejecución y herramientas de penetración
  - Ejemplo de informe



FIDE VIRTUAL

Amenazas a la seguridad informática

- Una **vulnerabilidad** (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

FIDE VIRTUAL

Amenazas a la seguridad informática

- Una **amenaza** es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas

FIDE VIRTUAL

Amenazas a la seguridad informática

- Dentro de las amenazas a la Seguridad Informática que se pueden mencionar serían:

  - **Manipulación de datos:**
    - Ingreso de datos: una persona manipula datos al ingreso de los mismos con el fin de obtener un beneficio.
    - Procesamiento de datos: manipulación de la información durante el procesamiento, alterando el resultado final
    - Datos de Salida: una vez emitida la información se pueden obtener datos sensibles.

  - **Manipulación de programas:** el autor no manipula ni altera los datos de la computadora, sino que por el contrario la manipulación se hace en el programa

FIDE VIRTUAL

Amenazas a la seguridad informática

- **Intromisión en bases de datos:** consiste en el acceso ha información almacenada en Bases de Datos, que no son de acceso público.

- **Sabotaje informático:** tiene como objetivo la afectación o destrucción tanto de programas como datos almacenados en la computadora. Puede provocarse el daño al hardware o disco duro del pc, pero la forma mas común de comisión es a través del deterioro de los datos almacenados y los programas

FIDE VIRTUAL

Amenazas a la seguridad informática

- **Daños o modificaciones de programas o datos computarizados:**
  - **Virus**: Un virus informático es un software diseñado para causar daños de diferente tipo en una computadora o una red de computadoras, alterando el código del software original que tenía la computadora y haciendo que ésta trabaje de manera anormal

  - **Gusanos**: Un gusano informático (también llamado IWorm por su contracción en inglés, "I" de Internet, Worm de gusano) es un malware que tiene la propiedad de duplicarse a sí mismo.

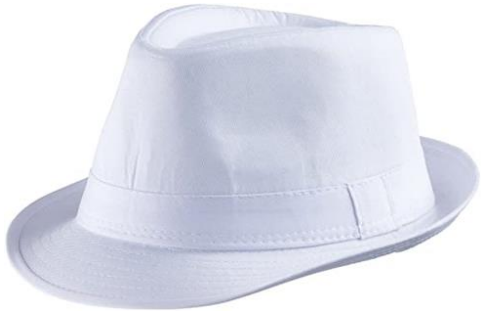
FIDE VIRTUAL

Amenazas a la seguridad informática

- **Daños o modificaciones de programas o datos computarizados:**
  - **Espionaje**: implica una intención la de imponerse de secretos industriales, comerciales, políticos, económicos o militares ya sea de una empresa o el estado.

Que es el Hacking Ético

- Hacking ético es una forma de referirse al acto de una persona de usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.
- O bien la simulación de diferentes escenarios donde se generan ataques controlados con el fin de mejorar la seguridad de las redes o sistemas que la conforman.

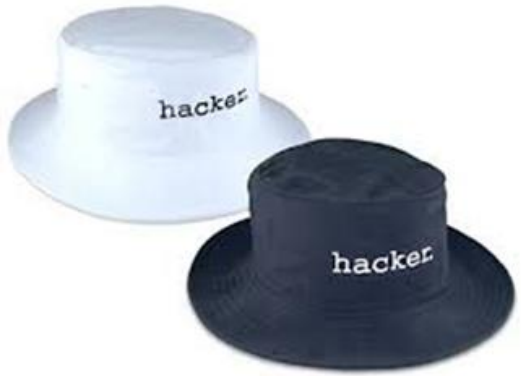


FIDE VIRTUAL

Quien es el Ethical Hacker

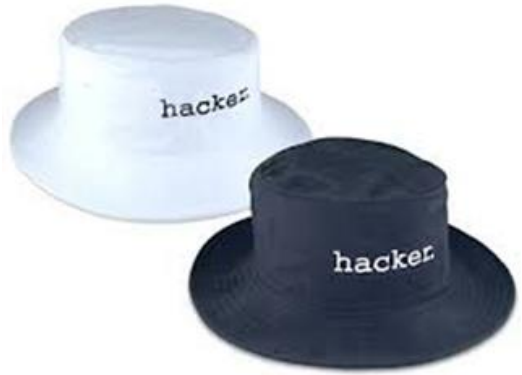
- El Hacker Ético es aquella persona que ejecuta las pruebas de penetración con las mismas herramientas que utilizaría un Hacker malintencionado con el fin de burlar la seguridad con la diferencia que es un ambiente controlado y al final el mismo genera las oportunidades de mejora y posibles recomendaciones.

- Como diferenciar al Hacker Ético del malintencionado: Autorización, Motivación, Intención



FIDE VIRTUAL

Quien es el Ethical Hacker



- Al hacker o también denominado pirata informático se le puede clasificar de la siguiente manera:
  - Hacker: individuo que sin derecho penetra un sistema informático solo por gusto o para poder probar sus habilidades. Usualmente no tiene fines delictivos graves este tipo de intrusión.
  - Cracker: Derivado del hacking, es una persona que sin derecho penetra un sistema informático con el fin de robar o destruir información valiosa, realizar transacciones ilícitas o impedir el buen funcionamiento de redes informáticas o computadoras.
  - Preacker: persona que penetra ilícitamente sistemas telefónicos o de telecomunicaciones con el fin de obtener beneficios o causar perjuicios a terceros.

FIDE VIRTUAL

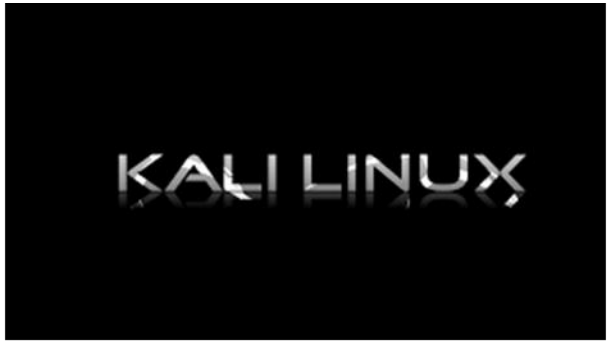
Fases de ejecución y herramientas de penetración

- Fase I – Reconocimiento:
  - Se trata de obtener la mayor cantidad de información incluyendo: Rangos de IP, Subredes, Host Activos, entre otros.
  - Tipos de Reconocimiento:
    - Activo: existe interacción directa con el objetivo, por lo general se crea alguna evidencia de la actividad
    - Pasivo: se obtiene información de forma indirecta (de la web), no hay interacción con el objetivo y no se genera evidencia o es difícil de obtenerla.

FIDE VIRTUAL

Fases de ejecución y herramientas de penetración

- Fase I – Reconocimiento: herramientas utilizadas



FIDE VIRTUAL

Fases de ejecución y herramientas de penetración

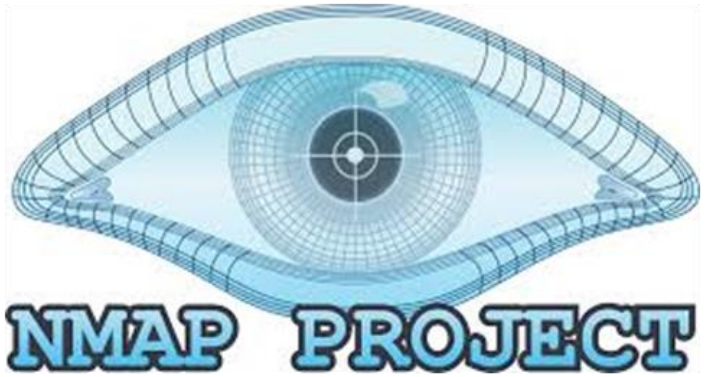
- Fase II – Exploración:
  - Ya se tiene identificada cierta información de la fase anterior, principalmente los equipos o sistemas.

  - En la fase de exploración se puede subdividir en las siguientes tareas:
    - Determinar si el sistema responde
    - Escaneo de puertos
    - Escaneo de vulnerabilidades

FIDE VIRTUAL

Fases de ejecución y herramientas de penetración

- Fase II – Exploración: herramientas




```
31337
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

FIDE VIRTUAL

Fases de ejecución y herramientas de penetración

- FASE III – Explotación o Aprovechamiento:
  - Es la fase donde se toma control sobre el equipo o sistema.
  - Usualmente se hace a través de un “exploit”, es la forma de aprovechar fallas de seguridad o evadir los controles de seguridad. Básicamente lograr que el equipo ejecute nuestros propios comandos accediendo a ciertos niveles de administración sobre el mismo.

FIDE VIRTUAL

Fases de ejecución y herramientas de penetración

- Fase IV – Después del Aprovechamiento o Manteniendo el Acceso:
  - Una vez que se hace un aprovechamiento de algún equipo es necesario descubrir si se puede mantener la comunicación y lo mismo lo podemos hacer de varias formas:

    - Backdoor: es una pieza de software que permite conectarse al equipo en el momento que el hacker lo requiera. Normalmente es un proceso oculto y permanente.

    - Rootkit: es un tipo de software que permite incrustarse profundamente en el SO y realizar una serie de tareas, entre las mismas ocultar procesos y programas.

Fases de ejecución y herramientas de penetración

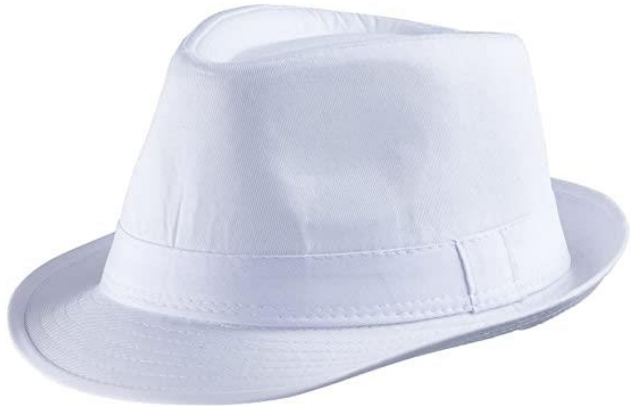
- Fase V – Terminando las Pruebas de Penetración (Conclusión):
  - Finalizadas todas las pruebas de penetración y habiendo detectado todos las posibles mejoras de seguridad es de suma importancia transmitir de una adecuada manera la información encontrada. Para lo mismo se recomienda crear reportes con la siguiente estructura o formato:
    - Resumen ejecutivo: es un resumen de lo mas importante del análisis, no excede en mas de 2 paginas, normalmente no contiene información técnica.
    - Informe detallado: contiene la información completa del análisis y pruebas, contiene todo el detalle técnico incluyendo las recomendaciones de mejoras.

Informe de Ejemplo

- Dirigirse a la plataforma y descargar el formato de ejemplo denominado: Informe Ejemplo

Culminación del módulo

- Tecnologías de ataque a los sistemas - Hacking Ético
  - Amenazas a la seguridad
  - Que es el Hacking Ético
  - Quien es el Ethical Hacker
  - Fases de ejecución y herramientas de penetración
  - Ejemplos de informe



FIDE VIRTUAL

Gracias