Pentesting con Kali Linux

Taller de Seguridad Informática

Developer's Days 2015

Jonatan Ramón Gallardo

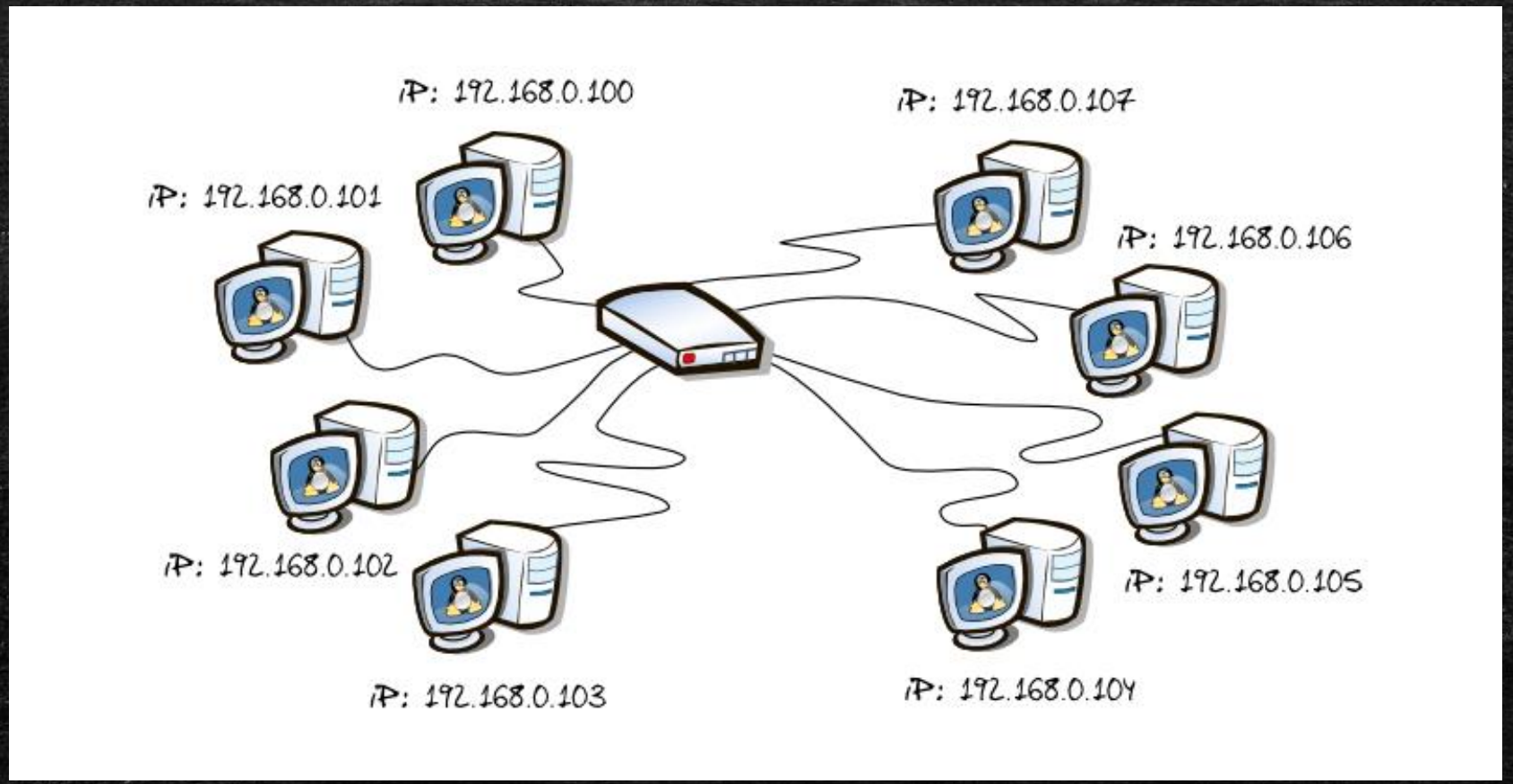
Contenido del taller

- Conceptos básicos de redes
- ¿Qué es Kali Linux?
- Escáner de redes con Nmap
  - Dibujar topología de red
  - Detección e identificación de intruso en la red
- Metasploit sobre máquina vulnerable
- Soluciones teóricas

Conceptos básicos de redes

- ¿Qué es una IP?
- ¿Qué es una mascara de red?
- ¿Qué es un puerto? ¿Qué es un protocolo de comunicación?

La IP son los nombres de un equipo en una red.



Una máscara de red configura las IP que pueden usarse en una red.

255.255.255.0

Un Puerto es la interfaz utilizada para comunicarse con la red.

Para poder asignar a que aplicación deben llegar los paquetes de la red se crean los puertos.

Por defecto los "puertos bien conocido" son puertos que no cambian:

Por ejemplo:

21-FTP

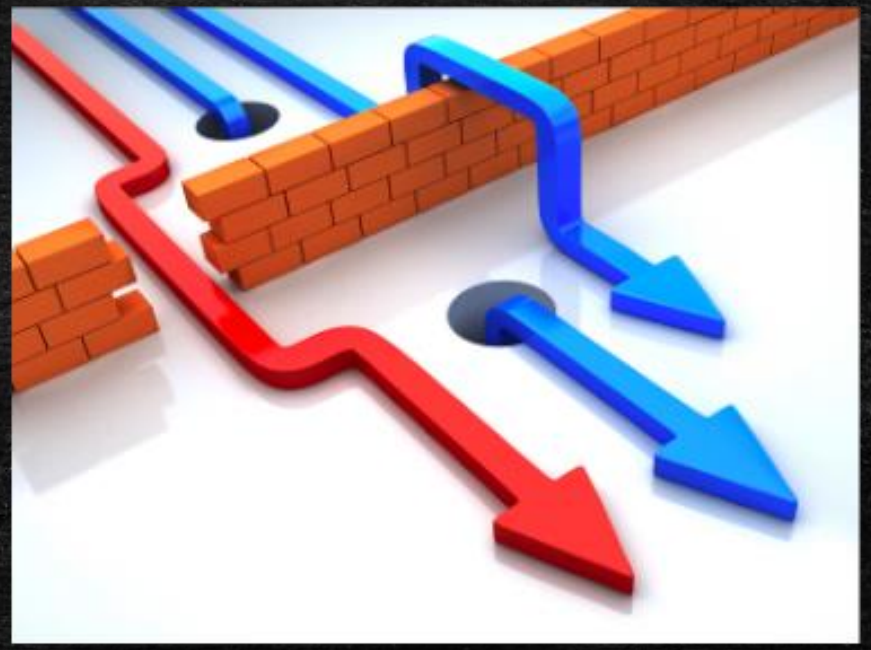
80-HTTP

631-UDP

Comenzando con Kali Linux

Exploit (del inglés *to exploit*, "explotar" o 'aprovechar') es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

Pentesting es un ataque a un equipo con intención de detectar y solucionar vulnerabilidades en un sistema.



Escáner de redes con nmap

Detección de intruso

- Realizar un escaneo de todos los equipos de la red
- Podremos conocer las IP de la red a partir de la máscara de red

Comandos útiles:

db_nmap Usaremos este comando para guardar la información en la base de datos.

db_nmap [Scan Type (s)] [Options] {target specification}

Argumentos:

Rangos de ip: 192.168.0-255.n-m

-sS Escáner silencioso con tramas SYN

-O Detección de sistemas operativos

Iniciando un ataque Metasploit

- Análisis de puertos y S.O.
  - db_nmap {dirección de objetivo} –p {rango de puertos}
- Análisis de versiones de servicios
  - -sV Permite identificar las versiones de los servicios encontrados
- Análisis de vulnerabilidades de un servicio consultando en la base de datos de KaliLinux
  - Search {contenido} Busca contenido en la base de datos de exploits
- Ejecución y configuración del expoit
  - Show options
  - Set {variable} {valor}
  - Exploit

Soluciones teóricas para evitar ataques

Crear una red segura, para evitar comunicación no deseada .

Firewall físico.

Cerrar puertos innecesarios en el Router para evitar intrusiones externas.

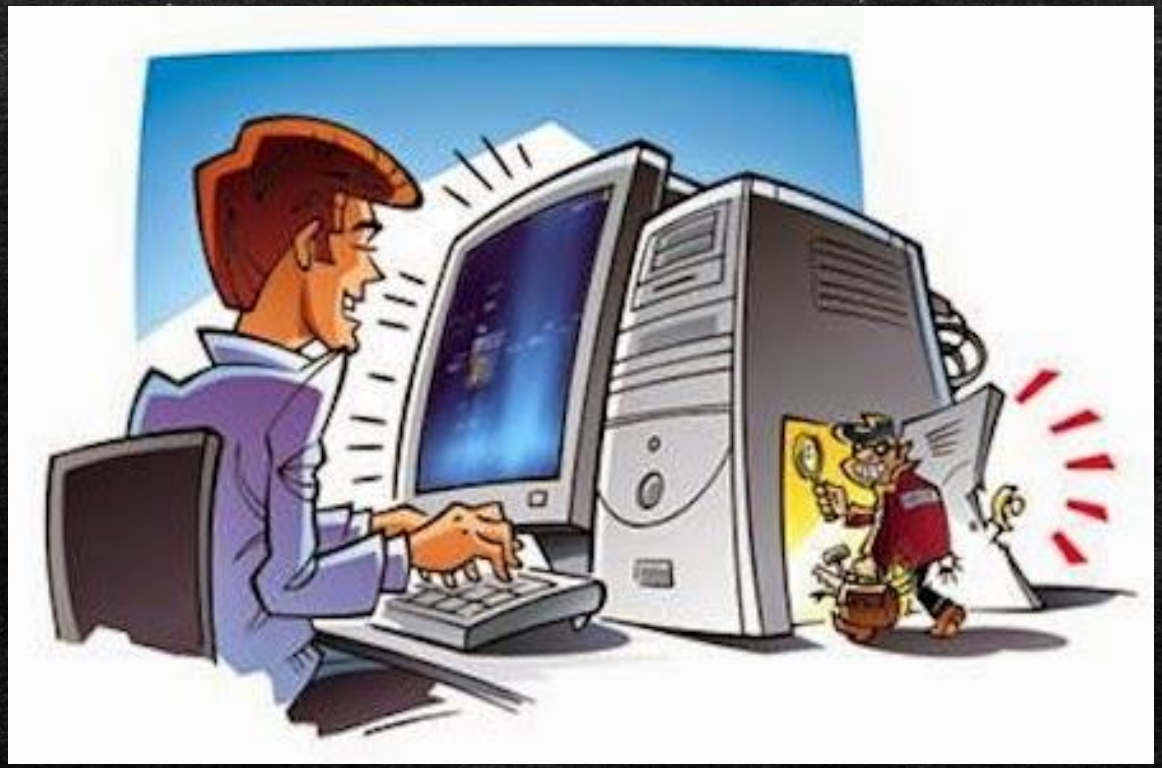
Mantener actualizadas el sistema operativo y los servicios

El 80% de las actualizaciones son parches de seguridad.

Disminuir la cantidad de Software de un sistema

Cada vez que instalas un nuevo software, aumentas las vulnerabilidades de un sistema, ya que no hay un software totalmente seguro.

OJO!: Los antivirus no son el remedio definitivo, es solo una capa más de seguridad. La capa más importante de seguridad la creamos nosotros como usuarios, así que debemos ser conscientes de los peligros.



¡Seguid disfrutando del evento mañana!

11.30 PONENCIA DE JJ MERELO
"BIG DATA Y SOFTWARE LIBRE"
[AULA 1.8]
12.30 PONENCIA DE RICARDO GALLI
"CANON AEDE, O QUE EMPRENDAN LOS OTROS" [AULA 1.8]
13.30 CLAUSURA [AULA 1.8]

Developer's Days 2015 IEEE SB UMH

Jonatan Ramón Gallardo