Guardia Civil

Mando de Apoyo

Jefatura de Servicios Técnicos

Seguridad en las Tecnologías de la Información y la comunicación

LAB Comandos Linux útiles para practicar CIBERSEGURIDAD

ACADEMIA DE INGENIEROS

Cap. Jesús Cano Carrillo

Estado de alarma, junio de 2020

LINUX;-?

Linux Images

https://sourceforge.net/projects/linuxvmimag/

Community
ENTerprise
Operating **S**ystem

https://netcologne.dl.sourceforge.net/project/linuxvmimages/VirtualBox/C/8/CentOS_8.0.1905_VBG.zip

We generate fresh Kali Linux image files every few months, which we ma
Linux in its latest official release. For a release history, check our Kali Li
releases at http://cdimage.kali.org/kali-weekly/. Downloads are **rate limite**

+ KALI LINUX VMWARE IMAGES

− KALI LINUX VIRTUALBOX IMAGES

Image Name	Torrent	Version	Size
Kali Linux VirtualBox 64-Bit	Torrent	**2020.2**	3.3G
Kali Linux VirtualBox 32-Bit	Torrent	**2020.2**	2.9G

Información Linux: uname -a

Información memoria: free

Volcado de variables del kernel: sysctl –a

Variables del sistema: set

Disco y particiones: df –h

Estimación de espacio: du – h

Limites del sistema: ulimit –a

Drivers instalados: lsmod

Información del sistema

Información de red: ifconfig –a

Rutas: route –n

Puertos abiertos: netstat –tulpn

Log de seg. : vi /var/log/secure

Interfaz levantada: ping 0

Cuánto tiempo el sistema encendido: uname

Quién está logado: who

Monitor de tareas: top

Procesos: ps aux

Software instalado: rpm –qa (dkpg -–list)

Avisa si está vivo: ping –a web.institutomilitar.com

Por intervalos: ping –i 5 web.ins…

Inundación de ping –f web….

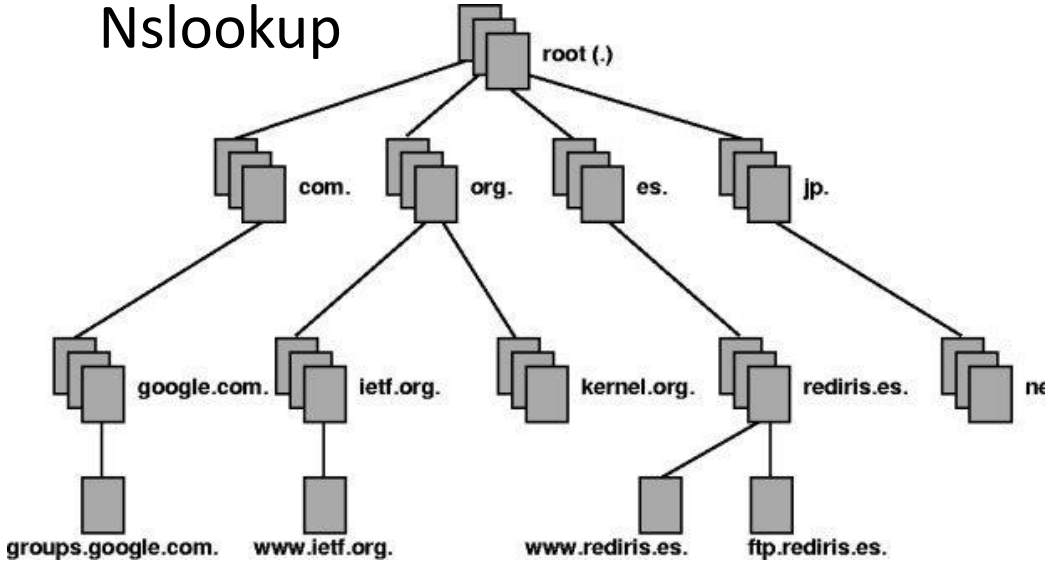
Aumentar tamaño (prueba routers): ping –s 100

Tracear: ping –R

Otra alternativa: traceroute

Demoras de trafico: mtr

Nslookup



Diagnosticar la red

Más de DNS

dig www.institut... ANY

dig +trace www.inst...

Dig –x 82.223.84.176

Dig –f fichero_lote.txt

Dig any Google.com

Dig @8.8.8.8 Google.com

Dig –x 8.8.8.8

set type=A, para buscar registros IP.

type=PTR, búsqueda inversa.

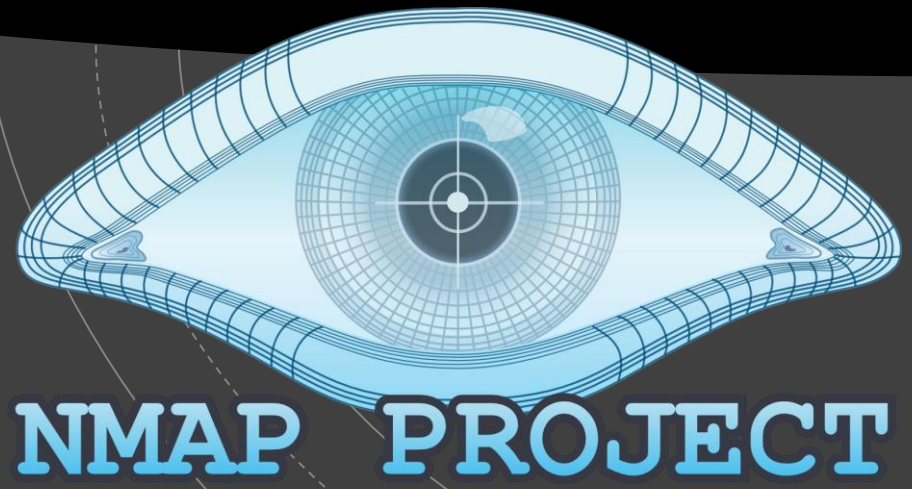
type=MX, Mail Exchange

Type=ns (name server)

type=any

-debug

nslookup -query=mx www.guardiac...

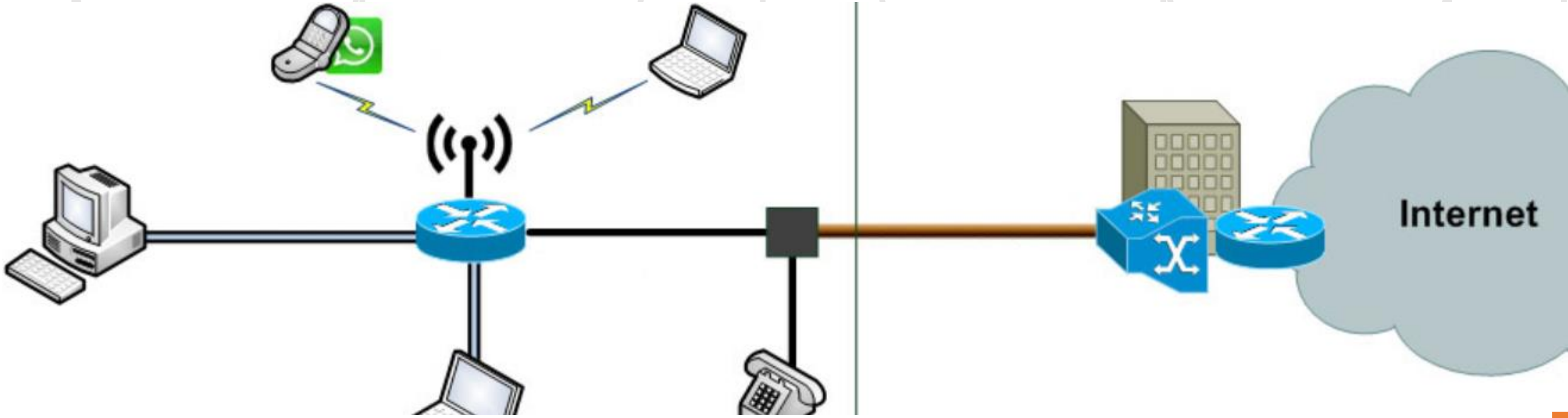


nmap

- CentOS. yum install nmap.
- Debian. apt-get install nmap.
- Ubuntu. sudo apt-get install nmap.
- Kali. Naaaaaaa, ya viene

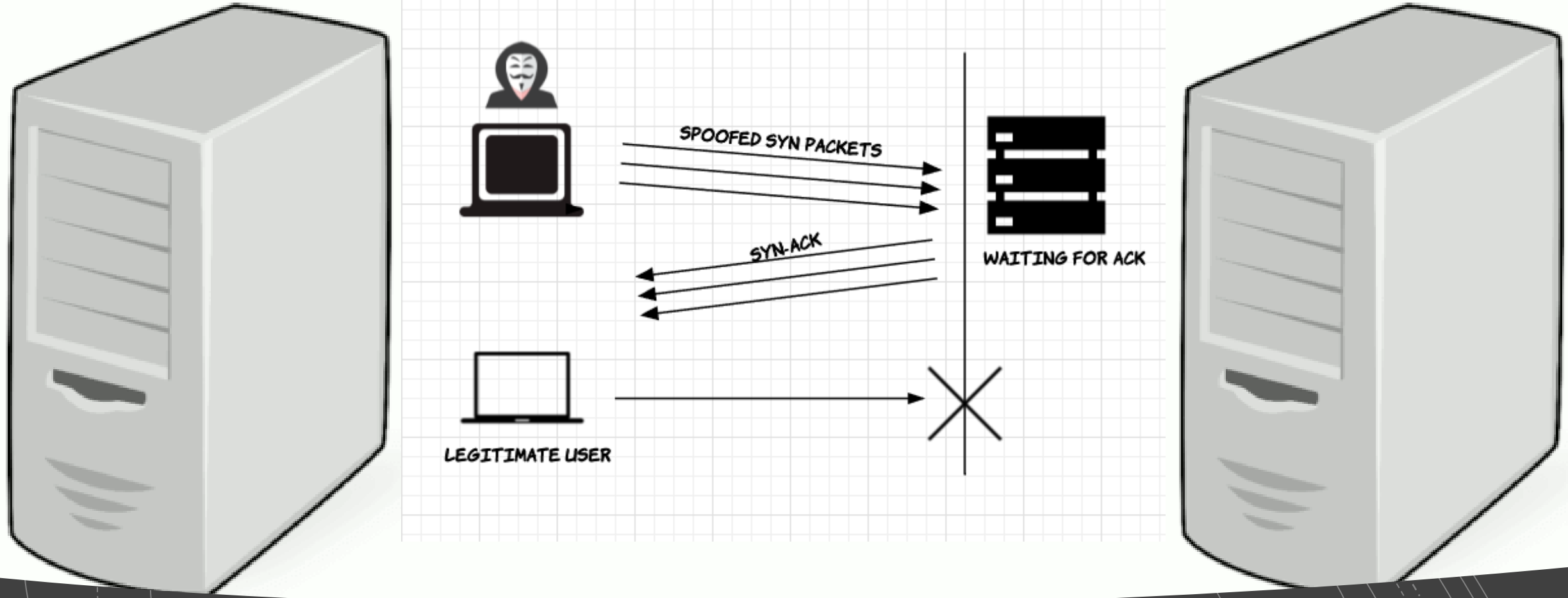
Explorar dispositivos terminales

nmap -PR 192.168.1.0/24



Sistema operativo de la víctima

nmap -sU 1 192.168.1.x



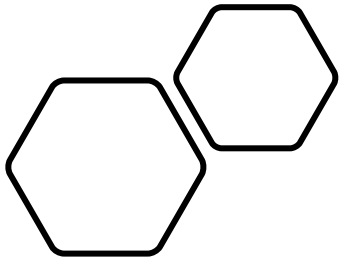
Puertos abiertos en remoto

- Hey, ¿cómo se veía en local?
- nmap -**sS** 192.168.1.x

Ataque TCP-SYN

¿Ataques DoS?

Puertos UDP abiertos



- UDP = no orientado a conexión = no handshake
  - ✓DNS utilizan TCP y UDP, en el puerto 53
  - ✓DHCP puerto 67 (UDP) del servidor y el puerto 68 (UDP) del cliente
  - ✓*NTP puerto* 123 UDP

nmap -sU 1 192.168.1.x

Software o servicios activos en una máq.

- nmap -Sv 192.168.1.x

Otros usos: subred, puertos típicos

nmap 192.168.10.0/24 (subred)
nmap 192.168.10.*

nmap -p 80,443 192.168.10.0/24
nmap --top-ports 25 192.168.10.0/24

Búsqueda de vulnerabilidades

Scripts previstos en */usr/share/nmap/scripts/* (Kali, naaaa ahí está)

nmap --script-help vuln

Ejemplo: nmap --script vuln scanme.nmap.org

nmap --script smb-* 192.168.10.5

Zenmap

Profile: Regular scan

Ports / Hosts | Topology | Host De

Host	Protocol	State	Service
92.168.1.1	cp	open	ssh
92.168.1.4	tcp	open	vnc-1
92.168.1.101	6001 tcp	open	X11:1

Prueba ZENMAP!

ACADEMIA DE INGENIEROS

Laboratorio sobre ciberseguridad, hoy con el pingüino