

Ethical Hacking

Course



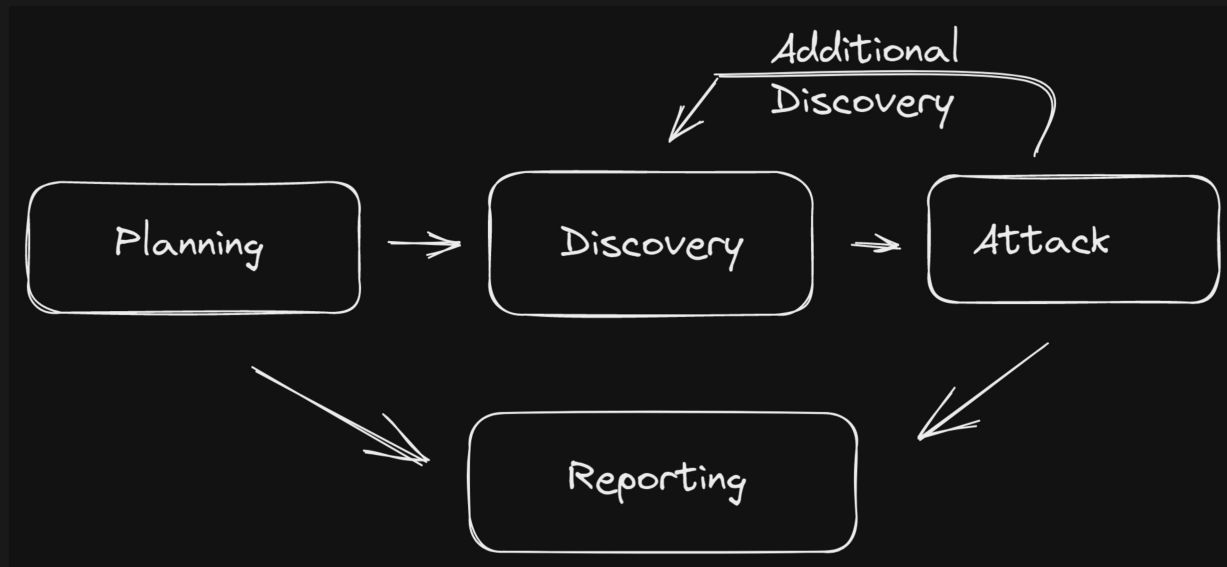
DÉFINITION

"We break into places to make sure people do not
break into places"

MAXIMUM SECURITY ENTRANCE



CYCLE D'UN PENTEST



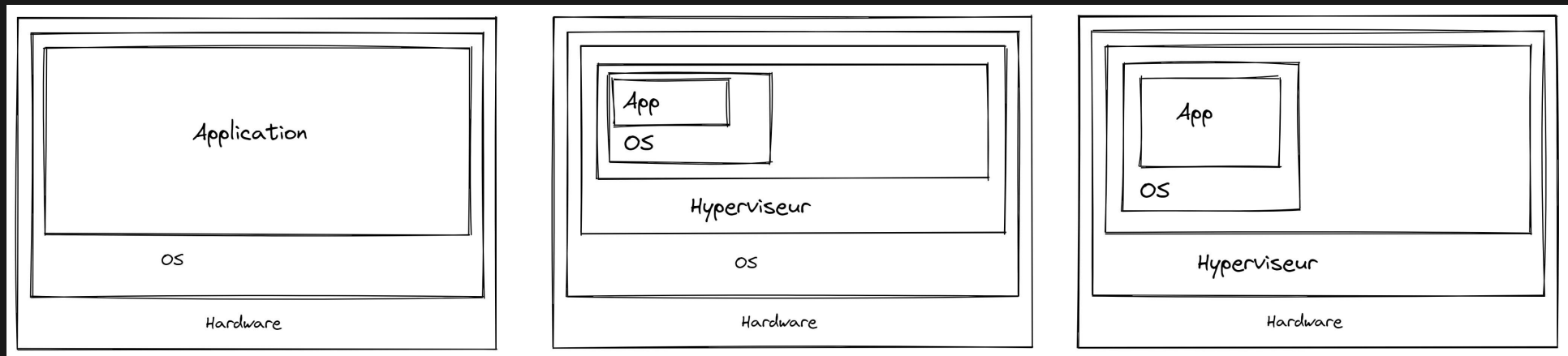
PRISE DE NOTES

- CherryTree
- Joplin
- OneNote
- Obsidian
- Evernote

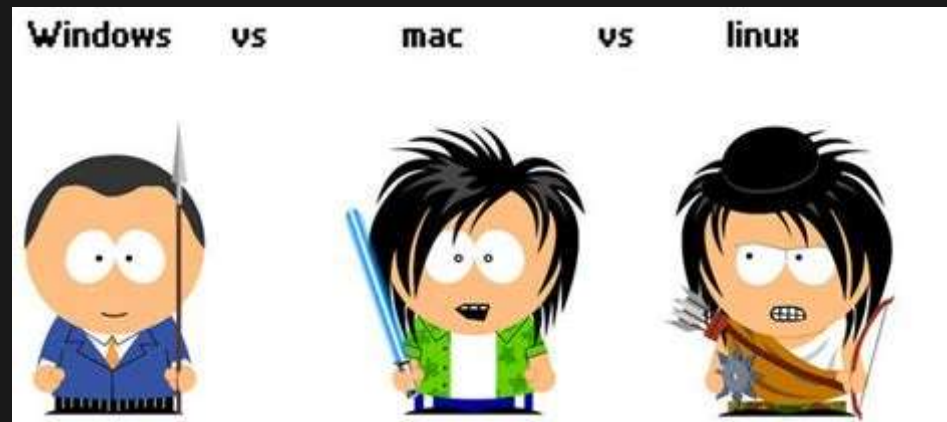
LE LABO

- VirtualBox
- VMWare Workstation
- ESXi
- Proxmox

VIRTUALISATION



QUEL OS CHOISIR ?



TÉLÉCHARGER KALI

<https://www.kali.org>

ISOs Vs Images

WINDOWS VM :

Rapide

<https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/>

WINDOWS ISO :

Plus de plateformes disponibles

<https://www.microsoft.com/fr-fr/software-download/windows10>

METASPLOITABLE

vulnhub

*WITH GREAT POWER
COMES GREAT
RESPONSIBILITY...*



LINUX



LINUX

Your grandma can do it.

SYSTÈME DE FICHIERS

Tout est un fichier dans Linux

/bin /dev /etc /home /lib /media /mnt /opt /proc /sbin
/snap /sys /tmp /var

- **/bin** les exécutables se trouvent là
- **/dev** Devices (cpu, console, ...)
- **/etc** Fichiers de configuration
- **/home** Espace pour les utilisateurs
- **/lib** Fonctionnalités partagées entre programmes
- **/media** usb
- **/mnt** dd cd montés

- **/opt** bin+conf
- **/proc** mémoire du sytème (affiche les processus)
- **/sbin** système (gere l'OS)
- **/snap** permet d'installer des apps portables (un des choix)
- **/sys** equivalent de lib mais pour le système
- **/tmp** fichiers temporaires
- **/var** emplacement des logs

LES COMMANDES DE BASE

- man, apropos
- ls, pwd, cd, mkdir
- find, locate, which

Num	Description
1	Commandes utilisateur
2	appels système noyau
3	Interface prog C
4	Fichiers spéciaux (périphériques)
5	Formats de fichiers
6	Jeux
7	Divers
8	Commandes admin systeme

GESTION DES SERVICES

Deux exemples : SSH, Apache

GESTION DES LOGICIELS

apt, dpkg



- Variables d'environnement
- Auto-Complétions
- L'historique
- Pipes et Redirections
- Recherche et modification de texte
- Édition de fichiers



- comparaison de fichiers
- Gestion des processus
- Surveillance des fichiers
- Téléchargement de fichiers
- Personnalisation

PIPES ET REDIRECTIONS

Nom	Description
Standard Input (STDIN)	Données introduites dans le programme
Standard Output (STDOUT)	Sortie du programme (par défaut, terminal)
Standard Error (STDERR)	Messages d'erreur (par défaut : terminal)

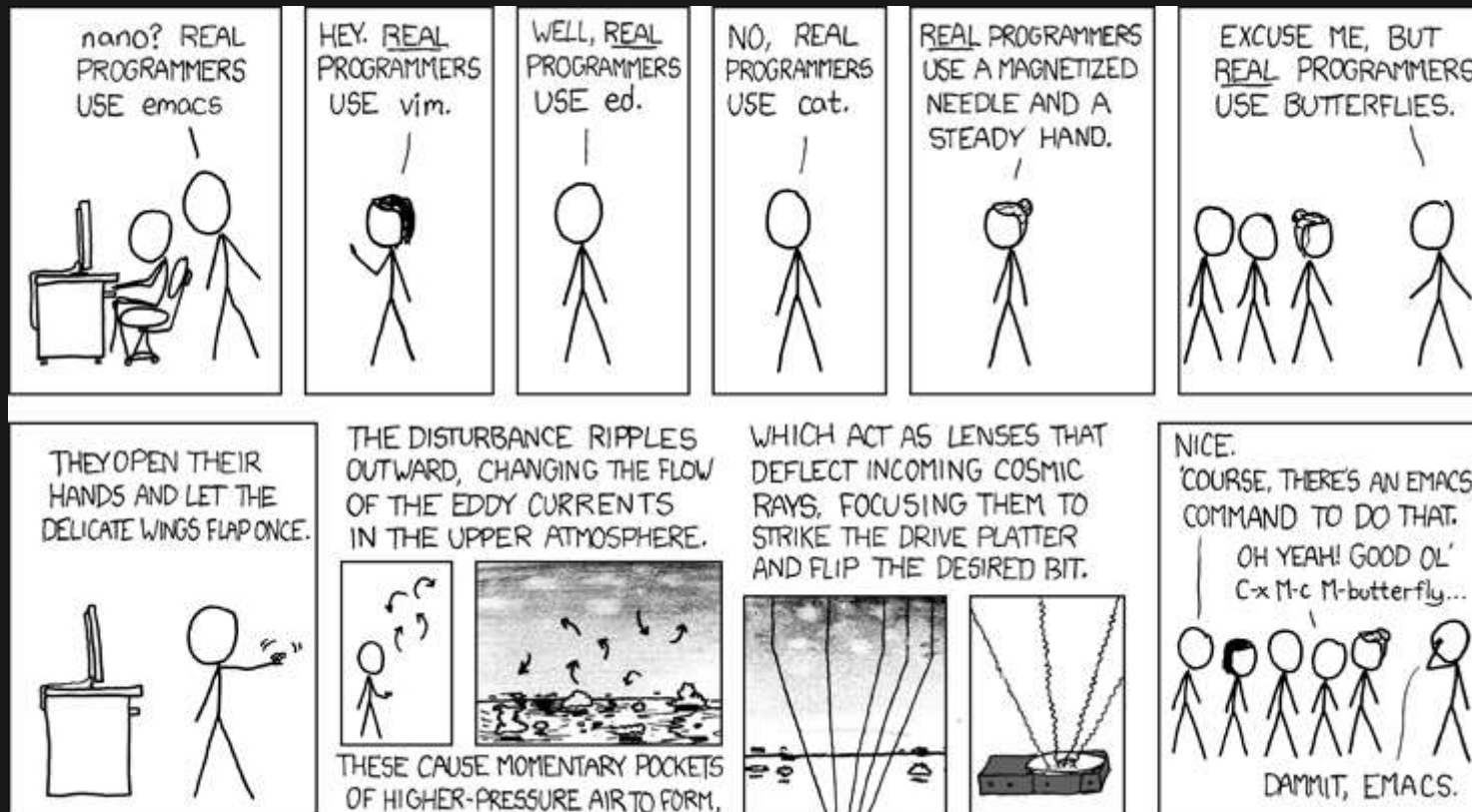
LES REGEX

```
^([a-zA-Z0-9_-.]+)@([a-zA-Z0-9_-.]+).([a-zA-Z]{2,5})$
```

RECHERCHE ET MODIFICATION DE TEXTE

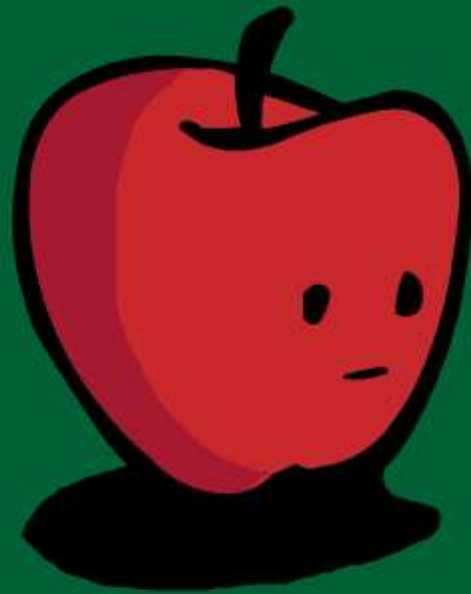
grep sed cut awk

EDITION DE FICHIERS



COMPARAISON DE FICHIERS

Well, we're both fruit.



GESTION DES PROCESS

SURVEILLANCE DES FICHIERS

LINUX TERMINAL FOR BEGINNERS


head



tail



cat

 t.me/dev_meme

You have started to learn it at
some cat... Point?

TELECHARGEMENT DE FICHIERS

PERSONNALISATION

SCRIPTS EN BASH

```
#!/bin/bash
```

LES VARIABLES

LES ARGUMENTS

```
ls -l /var/log
```

VARIABLES BASH SPÉCIALES

Nom de la variable	Description
\$0	Le nom du script Bash
1–9	Les 9 premiers arguments du script Bash
\$#	Nombre d'arguments passés au script Bash
\$@	Tous les arguments passés au script Bash

Nom de la variable

Description

\$?

Le statut de sortie du processus le plus récemment exécuté

\$

L'ID du processus du script actuel

\$USER

Le nom d'utilisateur de l'utilisateur qui exécute le script

\$HOSTNAME

Le nom d'hôte de la machine

\$RANDOM

Un nombre aléatoire

\$LINENO

Le numéro de la ligne actuelle dans le script

LES INSTRUCTIONS CONDITIONNELLES

```
if [ <un test> ]  
then  
    <une action>  
fi
```

```
if [ <un test> ]  
then  
    <une action>  
else  
    <une autre action>  
fi
```

Les opérateurs de tests disponibles sont, pour les chaînes :

- `c1 == c2`, vrai si `c1` et `c2` sont égales ;
- `c1 != c2`, vrai si `c1` et `c2` sont différentes ;
- `-z c`, vrai si `c` est une chaîne vide ;
- `-n c`, vrai si `c` n'est pas une chaîne vide.

Pour les nombres :

- $n1 -eq\ n2$, vrai si $n1$ et $n2$ sont égaux (equal) ;
- $n1 -ne\ n2$, vrai si $n1$ et $n2$ sont différents (non equal);
- $n1 -lt\ n2$, vrai si $n1$ est strictement inférieur à $n2$ (lower than);
- $n1 -le\ n2$, vrai si $n1$ est inférieur ou égal à $n2$ (lower or equal);
- $n1 -gt\ n2$, vrai si $n1$ est strictement supérieur à $n2$ (greater than) ;
- $n1 -ge\ n2$, vrai si $n1$ est supérieur ou égal à $n2$ (greater or equal).

Les opérateurs de tests disponibles sont, pour les objets du système de fichiers :

- [-e \$FILE] vrai si l'objet désigné par \$FILE existe dans le répertoire courant,
- [-s \$FILE] vrai si l'objet désigné par \$FILE existe dans le répertoire courant et si sa taille est supérieure à zéro,

- [-f \$FILE] vrai si l'objet désigné par \$FILE est un fichier dans le répertoire courant,
- [-x \$FILE] vrai si l'objet désigné par \$FILE est un fichier exécutable dans le répertoire courant,
- [-d \$FILE] vrai si l'objet désigné par \$FILE est un répertoire dans le répertoire courant,
- [-L \$FILE] vrai si l'objet désigné par \$FILE est un lien.

```
if [ <un test> ]  
then  
    <une action>  
elif [ <un test> ]  
then  
    <une autre action>  
else  
    <encore une autre action>  
fi
```

OPÉRATEURS BOOLÉENS

- AND (&&)
- OR (||)

BOUCLES

```
for nom_variable in <liste>  
do  
    <une action>  
done
```

```
while [ <un test> ]  
do  
    <une action>  
done
```

LES FONCTIONS

```
function nom_fonction {  
  commandes...  
}
```

```
nom_fonction () {  
  commandes...  
}
```

LES OUTILS ESSENTIELS



NETCAT

Pour vérifier si un port est ouvert ou fermé.

Pour lire une bannière depuis le port.

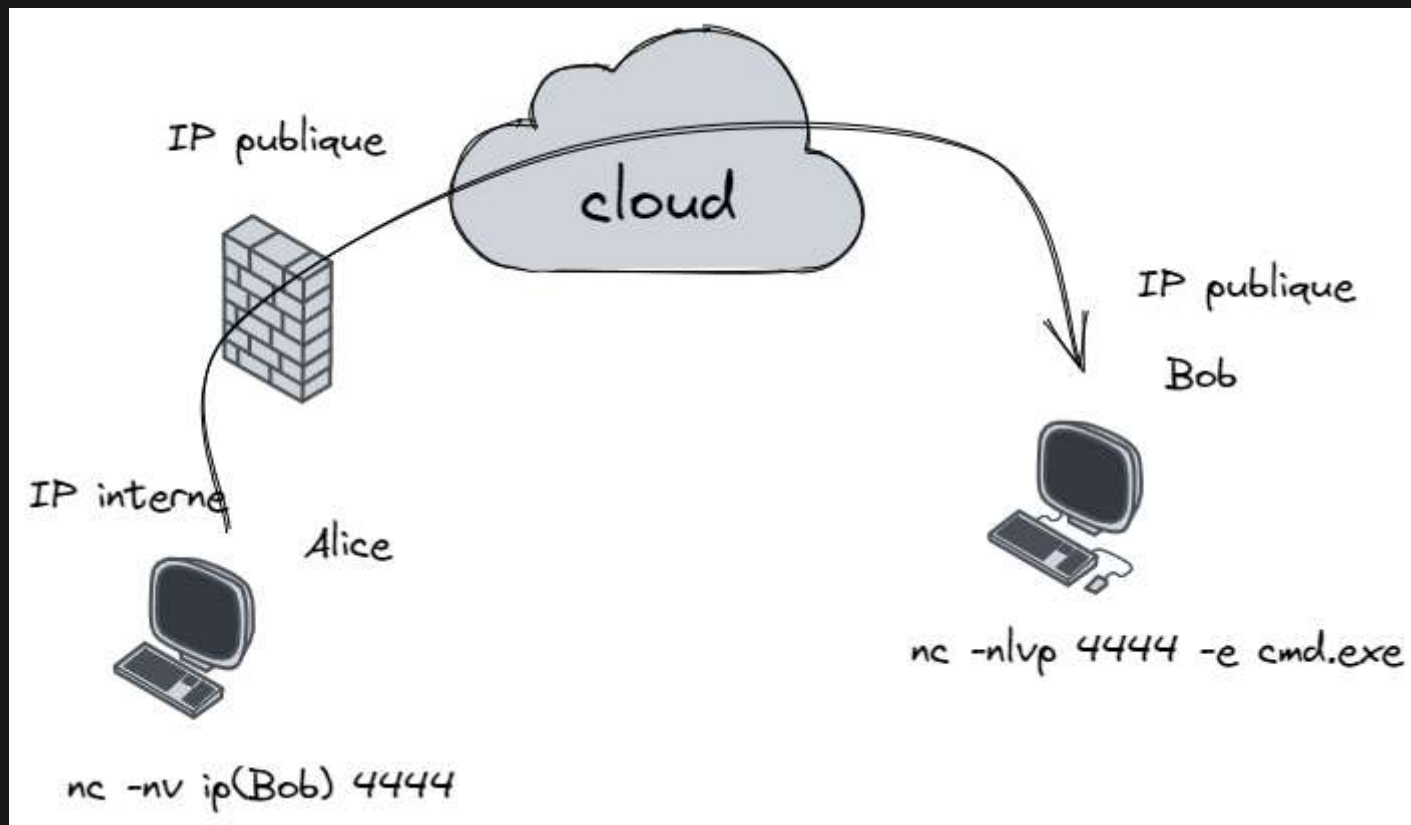
Pour vous connecter manuellement à un service réseau.

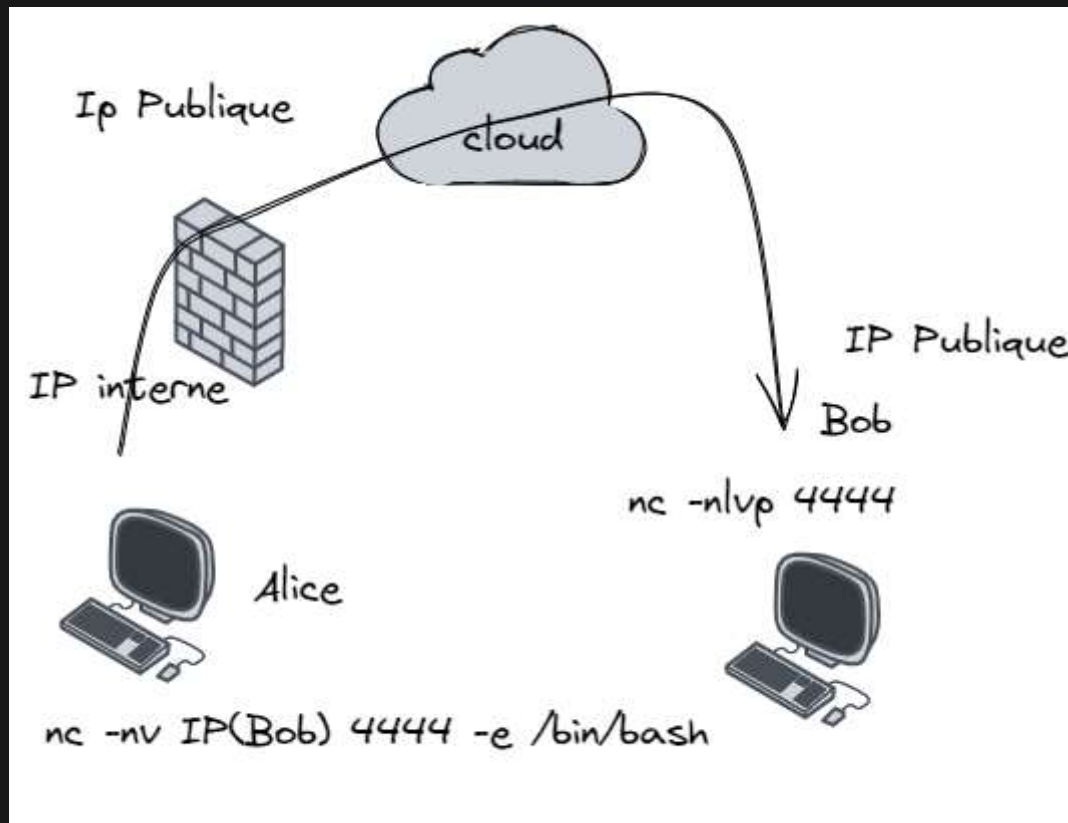
NETCAT

Transfer de fichiers avec Netcat

NETCAT

Administration à distance





NETCAT

Bind Shell

NETCAT

Reverse Shell

Ncat

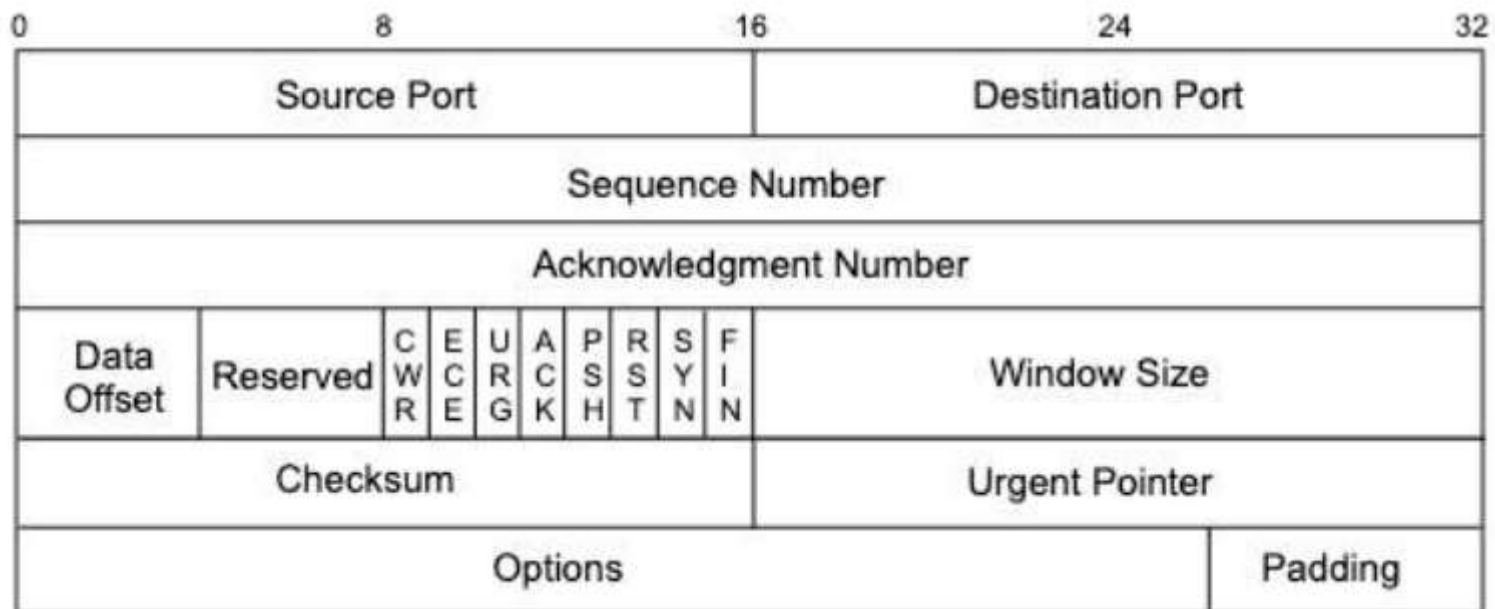
Socat

Powershell

Powercat

Wireshark

TCPdump



COLLECTE PASSIVE D'INFORMATIONS

"renseignements obtenus via des sources
d'information publiques sans jamais interagir avec la
cible"



WHOIS



GOOGLE



RECON-NG

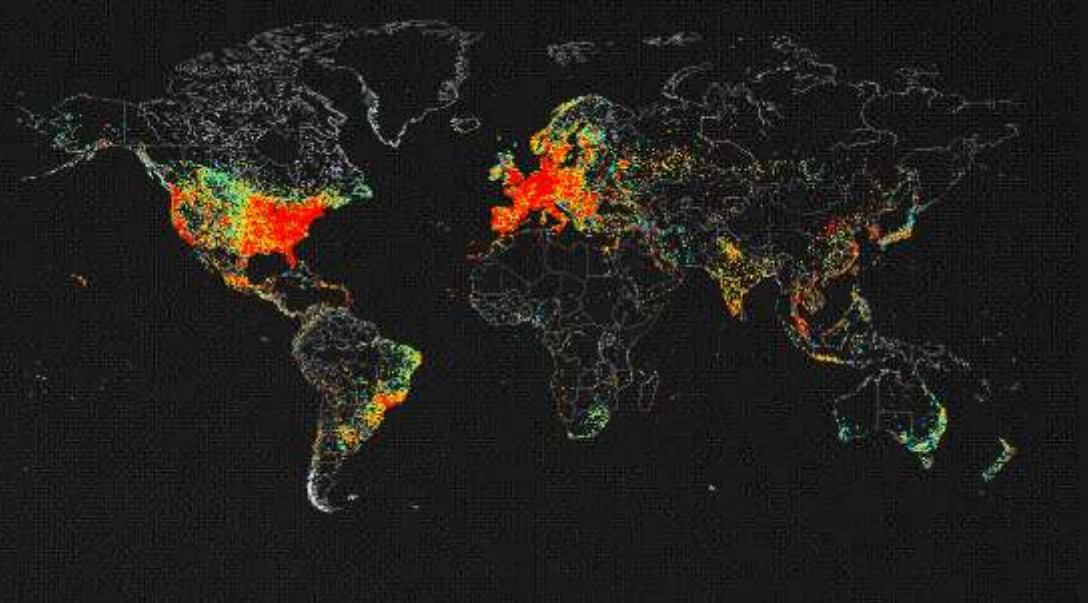


CODE OPEN SOURCE

SHODAN

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.



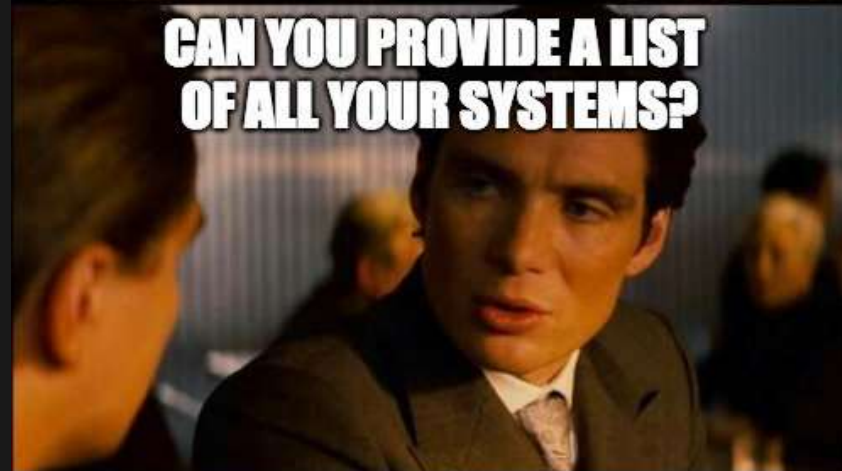
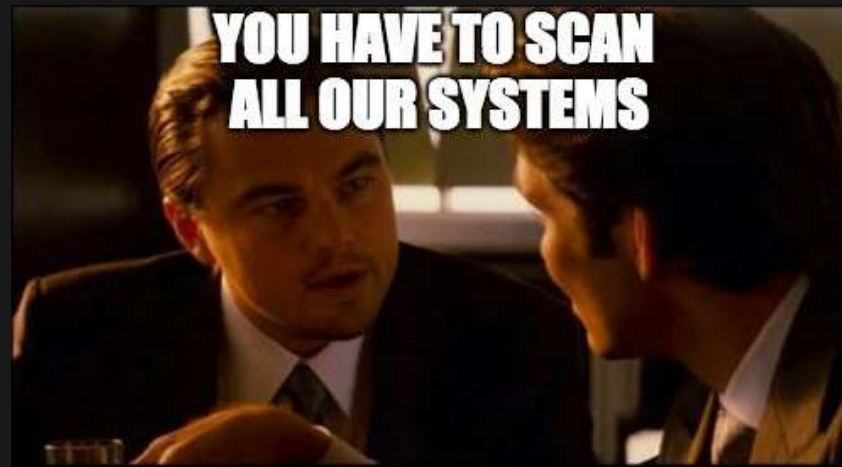
THE HARVESTER

SPIDERFOOT

<https://ohshint.gitbook.io/oh-shint-its-a-blog/>



COLLECTE ACTIVE D'INFORMATIONS



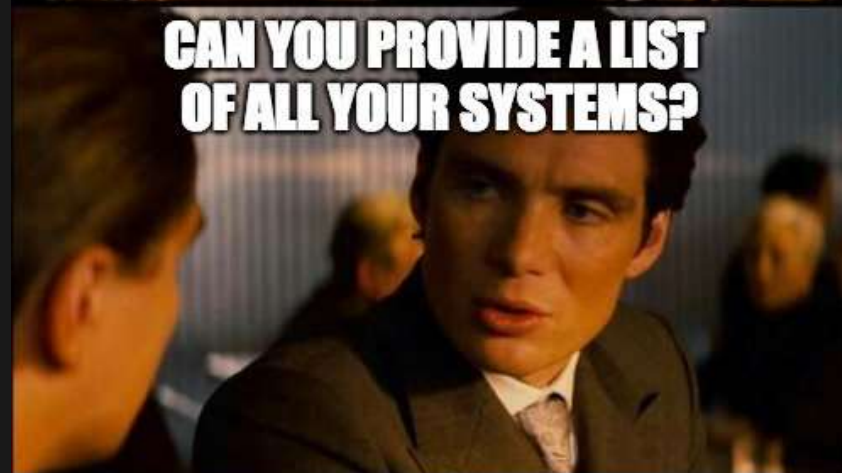
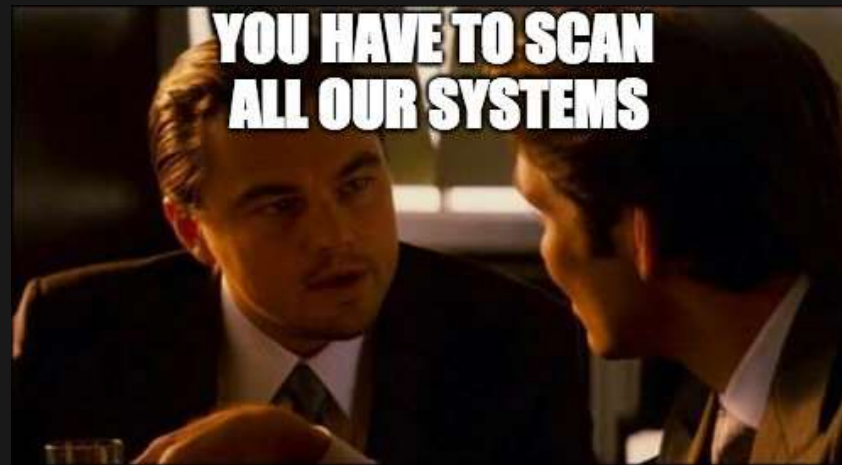
DNS



PORT SCAN







NMAP



NETBIOS

NFS

SMTP



LES SCANS AUTOMATISÉS

NIKTO

OPENVAS



LES EXPLOITS





METASPLOIT

```
IIIIII  
II  
II  
II  
II  
II  
IIIIII
```

```
dTb.dTb  
4' v 'B  
6. .P  
'T;. ;P'  
'T; ;P'  
'YvP'
```



MSFVENOM



POST EXPLOITATION



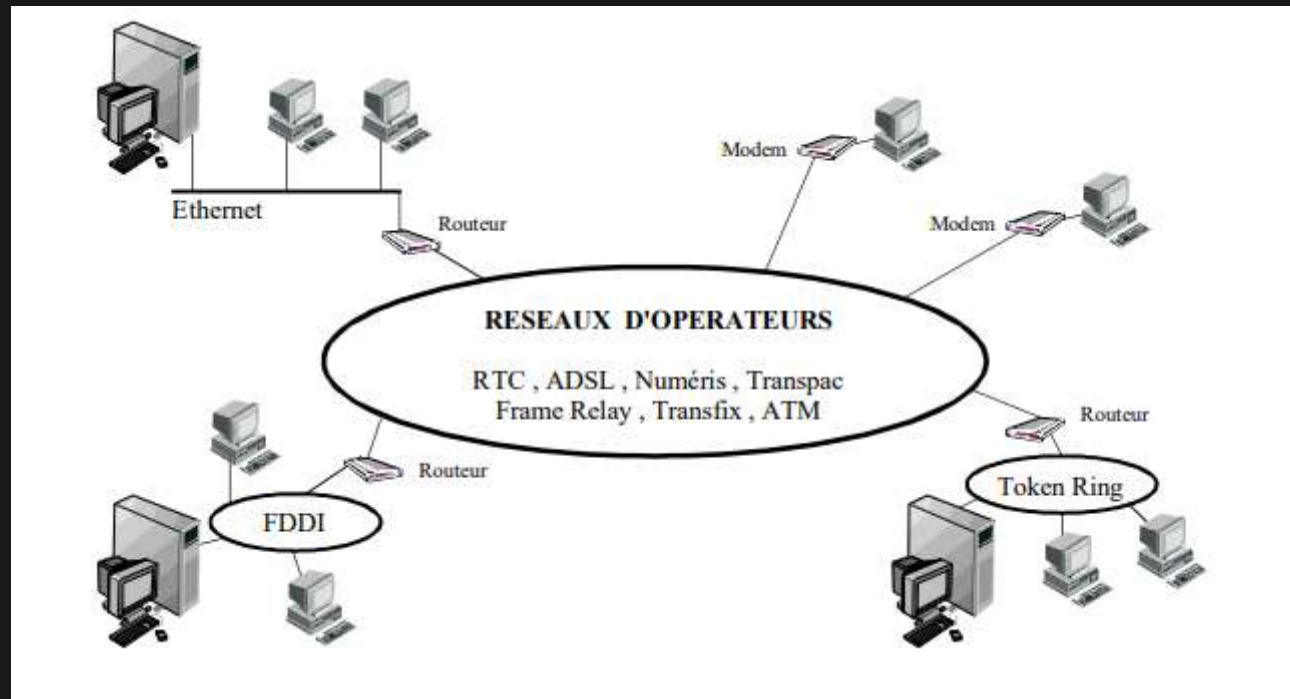


EDR - AV

Ils ne peuvent arrêter que ce qu'ils connaissent.

RÉSEAUX

Concepts de base



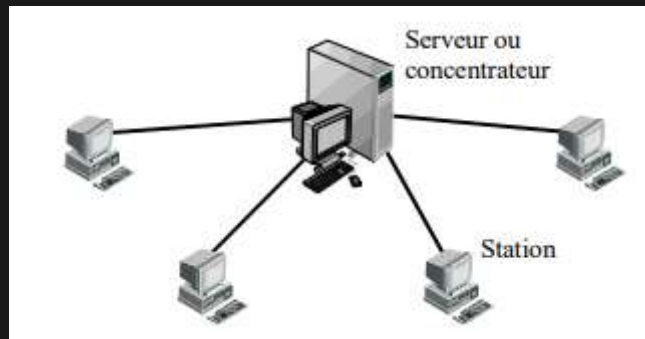
RÉSEAUX

LAN WAN

RÉSEAUX

Topologies

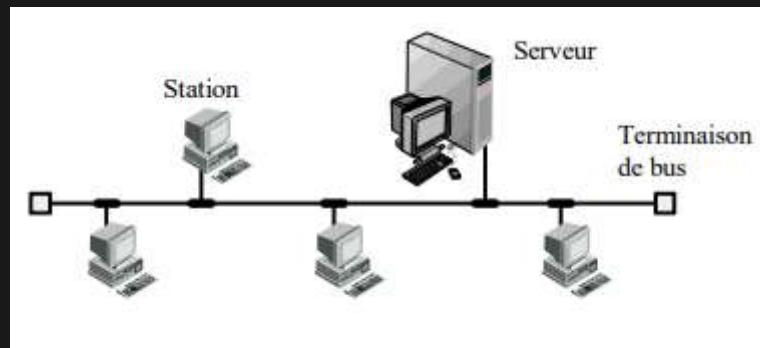
Etoile



RÉSEAUX

Topologie

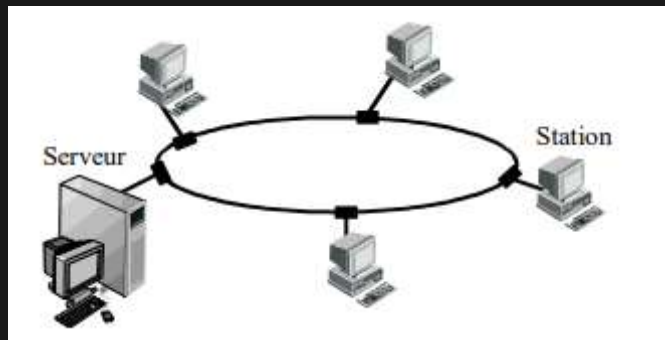
Bus



RÉSEAUX

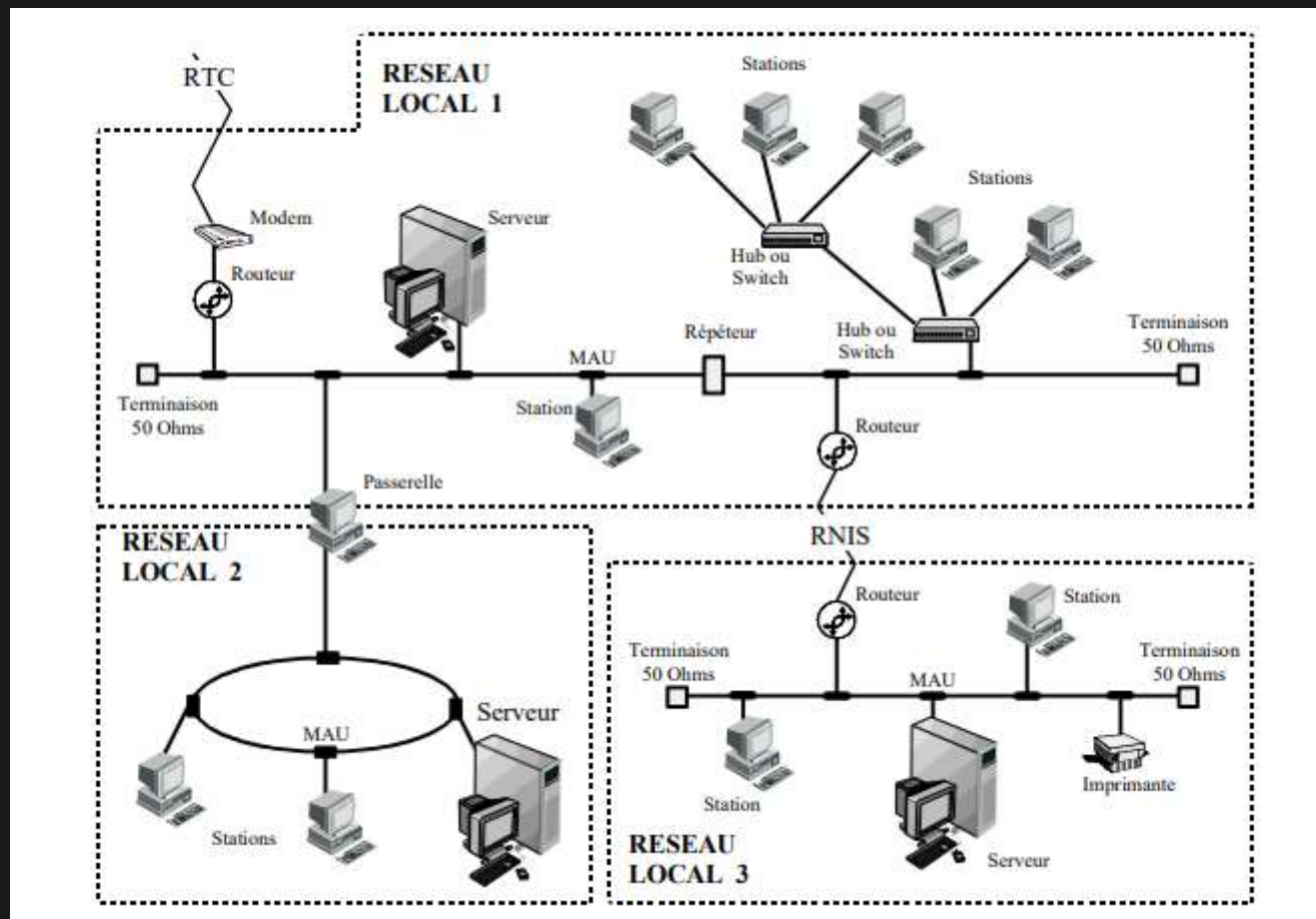
Topologie

Anneau



RÉSEAUX

Éléments



TCP/IP ET OSI

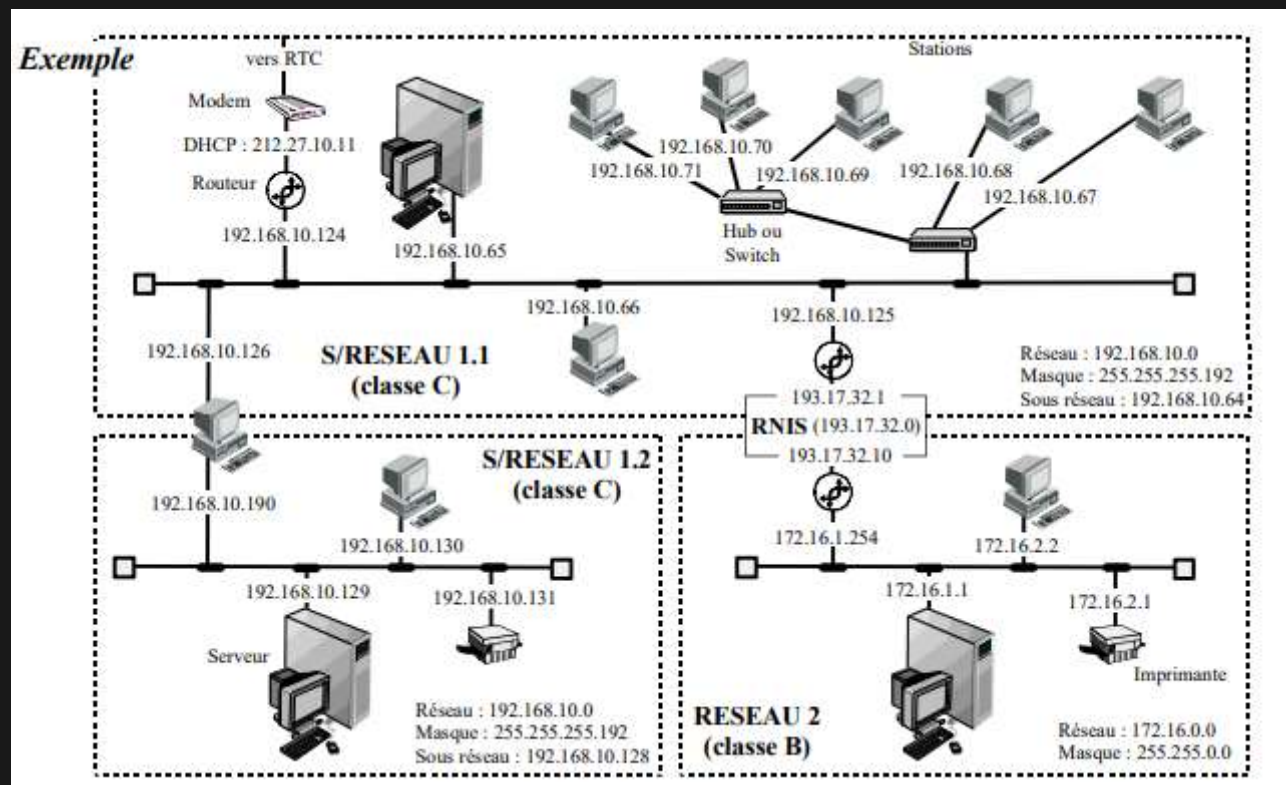
<i>OSI</i>		<i>DoD</i>	<i>Services et Protocoles</i>	
7	Application	Application	Telnet FTP NFS SMTP SNMP HTTP ...	
6	Présentation		XDR	
5	Session		socket	socket
4	Transport	Transport	port	port
3	Réseau	Internet	TCP UDP	
2	Liaison	Accès Réseau	RIP ICMP IP ARP RARP ...	
1	Physique		Ethernet FDDI SLIP PPP ATM ...	

IP

	31	24	23	16	15	8	7	0
Classe A	0	Id. réseau (7 bits)		Identificateur hôte (24 bits)				
Classe B	1	0	Identificateur réseau (14 bits)			Identificateur hôte (16 bits)		
Classe C	1	1	0	Identificateur réseau (21 bits)			Id. hôte (8 bits)	
Classe D	1	1	1	0	Adresse multicast (28 bits)			
Classe E	1	1	1	1	Format indéfini (28 bits)			

	Classe A	Classe B	Classe C
Premier réseau	1.x.x.x	128.1.x.x	192.0.1.x
Dernier réseau	126.x.x.x	191.254.x.x	223.255.254.x
Nombre de réseaux	126	16 382	2 097 150
Réseaux réservés à un usage privé	10.x.x.x	172.16.x.x à 172.31.x.x	192.168.0.x à 192.168.255.x
Adresse du réseau	x.0.0.0	x.x.0.0	x.x.x.0
Adresse de diffusion du réseau	x.255.255.255	x.x.255.255	x.x.x.255
Première machine	x.0.0.1	x.x.0.1	x.x.x.1
Dernière machine	x.255.255.254	x.x.255.254	x.x.x.254
Nombre de machines	16 777 214	65534	254
Masque de sous-réseau par défaut	255.0.0.0	255.255.0.0	255.255.255.0

EXEMPLE



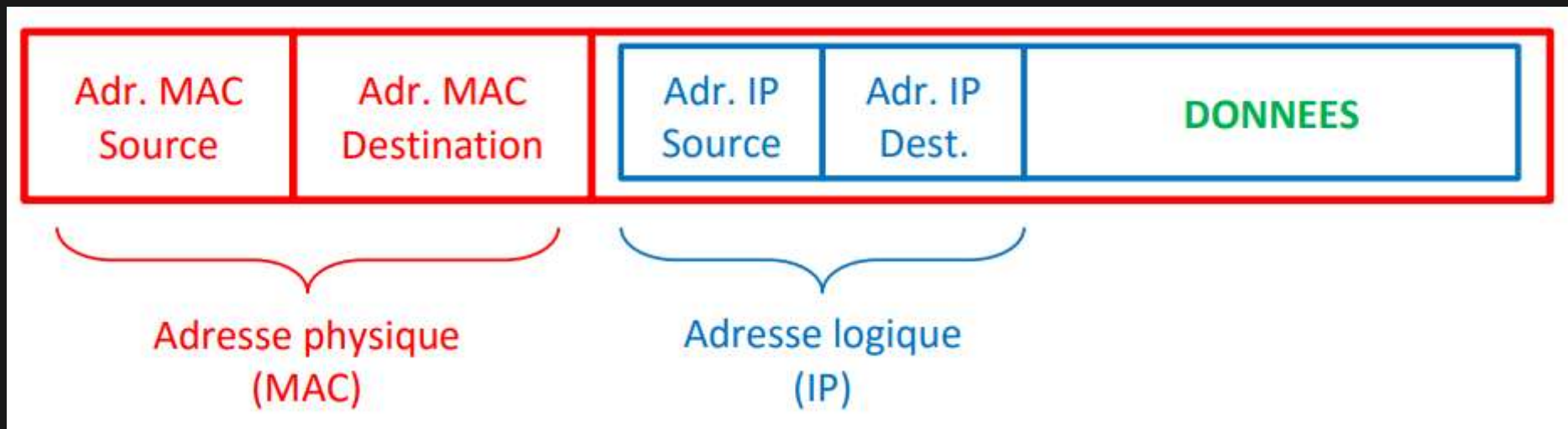
Adresse physique

Adr. MAC
Source

Adr. MAC
Destination

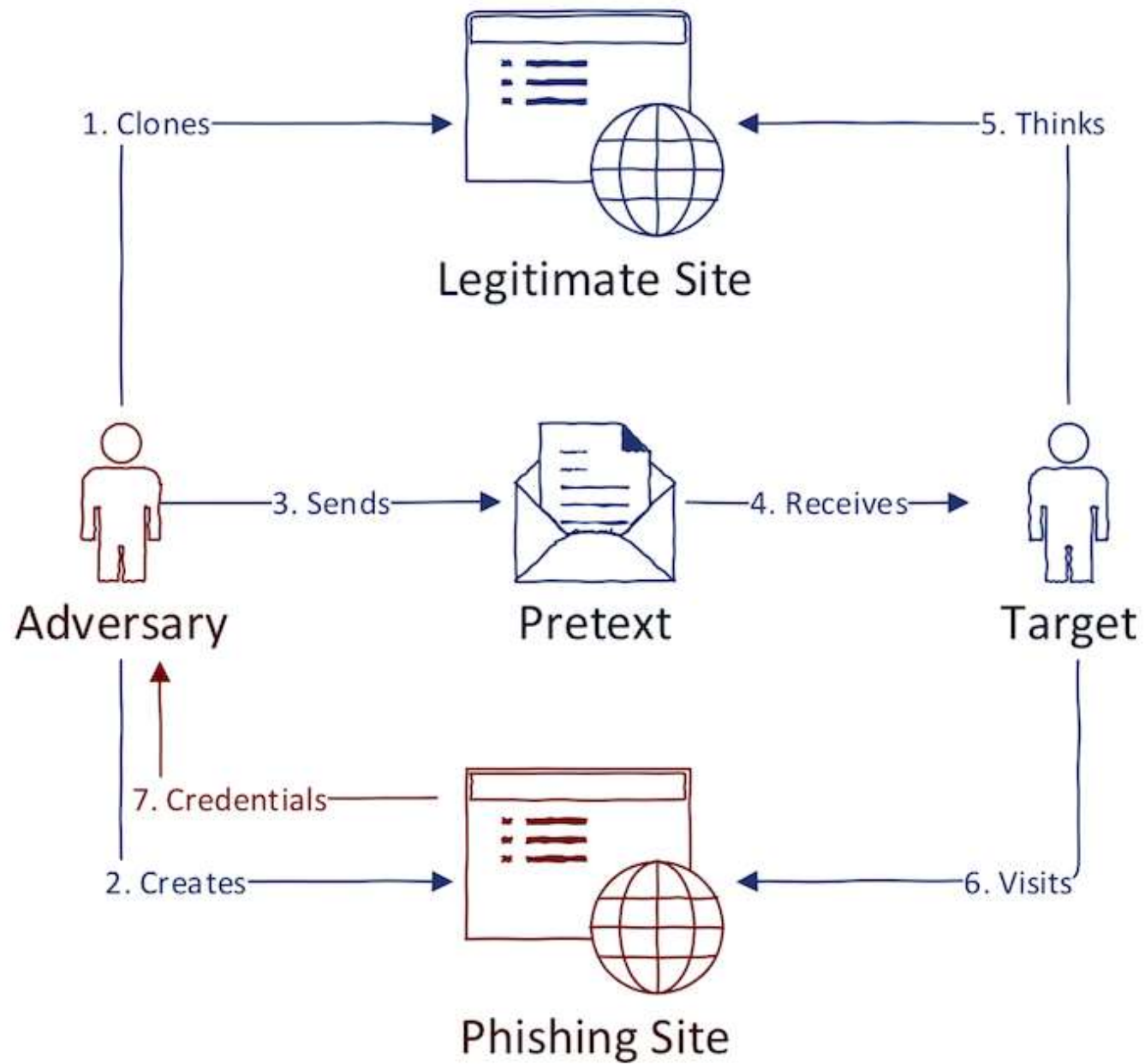
DONNEES

Adresse Logique



PHISHING







WEBAPP PENTEST



ET MAINTENANT ?





- Ip adresses
- MAC adresses
- TCP UDP
- Les ports
- Modèle OSI
- Sous-réseaux

WINDOWS

GUI

- TaskManager

CONNECTIONS RÉSEAU

- net view
- net use
- net session
- netstat (-naob)

NETVIEW

On regarde les partages réseau. Pourquoi ? La plupart des attaques vont viser un ordinateur individuel. Puis nous pivotons et allons sur le système suivant. Jusqu'à trouver ce que nous cherchons.

Les "shares" permettent de partager des dossiers et fichiers pour l'exfiltration ou charger des malwares par exemple.

NET SESSION

Est ce qu'un autre ordinateur a une session d'ouverte avec moi ?

Permet de trouver le patient 0.

NET USE

L'inverse de session

NETSTAT

netstat montre les connections réseau

- -a affiche toutes connections actives et les ports
- -n affiche les connection TCP actives.
- -o Affiche le PID (Process ID) pour chaque connection.
- -b affiche l'exécutable impliqué dans la création de chaque connection.

NETSTAT -F

Résout les adresses IP en nom de domaine quand 'est possible.

PROCESSUS

Exécutables qui tournent en arrière plan.

TASKLIST

- /SVC
- /m (ntdll.dll)

LES FILTRES

```
tasklist /m /fi "pid eq [proc_id]"
```

WMIC

- `/?`
- `wmic process list full`
- `wmic process get name, parentprocessid, processid`
- `wmic process where processid=<\pid> get commandline`

DeepBlue CLI

<https://github.com/sans-blue-team/DeepBlueCLI>

LAB



