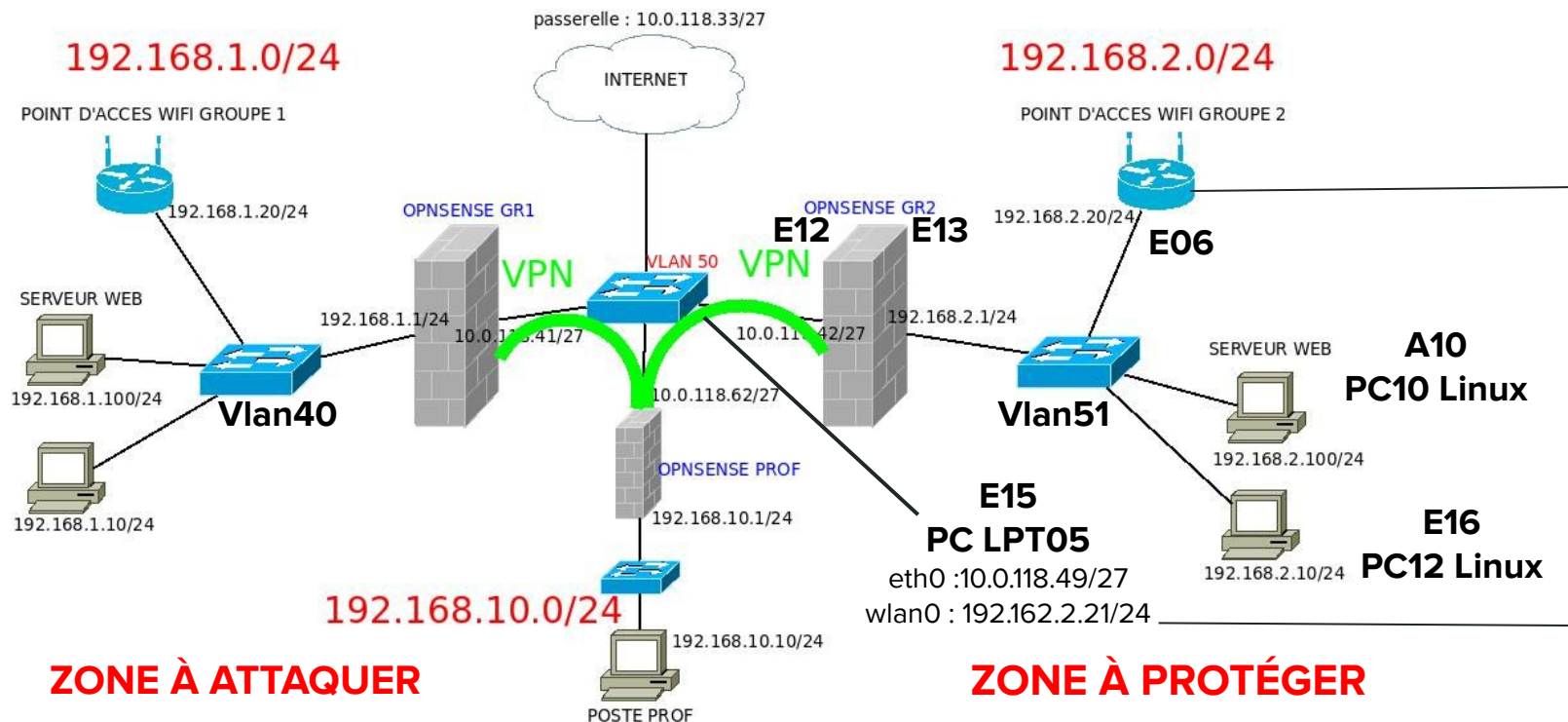


Présentation du travail

Equipe 2

Déploiement de l'architecture



Serveur web PC10

En restant connecté au réseau du lycée :

- `sudo apt update`
- `sudo apt-get install apache2`

Dans le fichier `phpinfo.php` situé à `/var/www/html` :

```
<? php
```

```
phpinfo()
```

```
?>
```

Changement d'IP du PC afin de fonctionner sur l'architecture réseau :

- `sudo su`
- `sudo systemctl stop NetworkManager`
- `killall dhclient`
- `sudo ip addr flush dev eth0`
- `sudo ip address add 192.168.2.100/24 brd + dev eth0`
- `sudo ip route add default via 192.168.2.1`

Serveur web PC10

Test d'accès au serveur :

PHP 7.4.3 - phpinfo() - Mozilla Firefox

192.168.2.100/phpinfo.php

PHP Version 7.4.3

System	Linux 1114-PC10-SNIR 5.4.0-104-generic #118-Ubuntu SMP Wed Mar 2 19:02:41 UTC 2022 x86_64
Build Date	Mar 2 2022 15:36:52
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqld.ini, /etc/php/7.4/apache2/conf.d/10-openssl.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/15-xml.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-dom.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-gmp.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-ldap.ini, /etc/php/7.4/apache2/conf.d/20-mbstring.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-simplexml.ini, /etc/php/7.4/apache2/conf.d/20-smtp.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-xmlreader.ini, /etc/php/7.4/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.4/apache2/conf.d/20-xsl.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902.NTS
PHP Extension Build	API20190902.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tls1.0, tls1.1, tls1.2, tls1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine.

Serveur web PC10

Changement du mot de passe : “Tunevasjamaistrouvercemotdepasse%&”

Dans un terminal :

- passwd local
- local
- Tunevasjamaistrouvercemotdepasse%&
- Tunevasjamaistrouvercemotdepasse%&

```
local@1114-PC10-SNIR:~$ passwd local
Changement du mot de passe pour local.
Mot de passe actuel :
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : le mot de passe a été mis à jour avec succès
```

Point d'accès wifi

Réinitialiser l'AP à sa configuration d'origine.

Se connecter avec un câble console au port console du routeur pour lui définir une adresse IP sur l'interface fastethernet0.

```
ap#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#interface BV
ap(config)#interface BVI1
ap(config-if)#ip address 192.168.2.20 255.255.255.0
```

```
interface BVI1
 ip address 192.168.2.20 255.255.255.0
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
!
```

Point d'accès wifi

Configuration du SSID :

Hostname ap

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >

HackezMoi

SSID: HackezMoi

VLAN: < NONE > [Define VLANs](#)

Backup 1:

Backup 2:

Backup 3:

Interface: ☒ Radio0-802.11G

Network ID: (0-4096)

Delete

Client Authentication Settings

Methods Accepted:

☒ Open Authentication: < NO ADDITION >

☐ Shared Authentication: < NO ADDITION >

☐ Network EAP: < NO ADDITION >

Point d'accès wifi

Configuration de la clé WPA2 :

Client Authenticated Key Management

Key Management:

Mandatory ▾

☐ CCKM

☒ WPA

WPA Pre-shared Key:

.....

☒ ASCII ☐ Hexadecimal

PC LPT05 E15

Paramétrage de l'adresse IP de la machine :

```
local@lptxx:~$ sudo ip addr flush dev eth0
local@lptxx:~$ sudo ip addr add 10.0.118.49/27 brd + dev eth0
local@lptxx:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.118.49 netmask 255.255.255.224 broadcast 10.0.118.63
    ether 14:fe:b5:c5:b9:d6 txqueuelen 1000 (Ethernet)
    RX packets 1667 bytes 239097 (239.0 KB)
    RX errors 0 dropped 91 overruns 0 frame 0
    TX packets 496 bytes 36110 (36.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ajout de la passerelle par défaut :

```
local@lptxx:~$ sudo ip route add default via 10.0.118.33
local@lptxx:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 octets de 8.8.8.8 : icmp_seq=1 ttl=114 temps=10.6 ms
64 octets de 8.8.8.8 : icmp_seq=2 ttl=114 temps=9.83 ms
^C
--- statistiques ping 8.8.8.8 ---
2 paquets transmis, 2 reçus, 0 % paquets perdus, temps 1001 ms
rtt min/avg/max/mdev = 9.830/10.197/10.565/0.367 ms
```

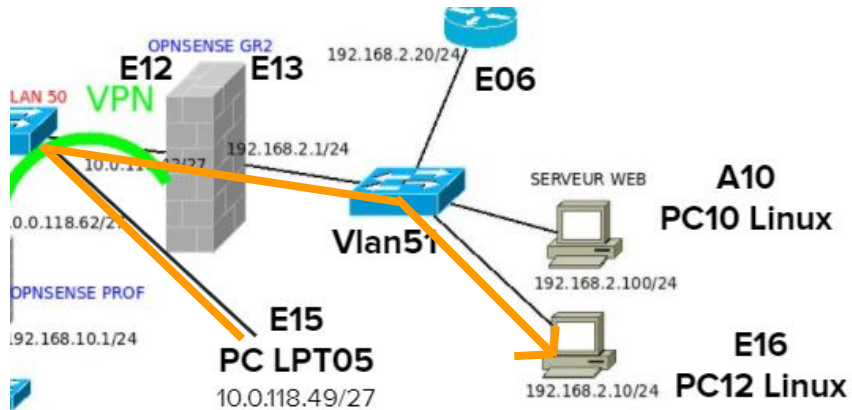
Route pour accéder au sous-réseau 192.168.2.0/24 :

```
local@lptxx:~$ sudo ip route add 192.168.2.0/24 via 10.0.118.42
local@lptxx:~$ route -n
Table de routage IP du noyau
```

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
0.0.0.0	10.0.118.33	0.0.0.0	UG	0	0	0	eth0
10.0.118.32	0.0.0.0	255.255.255.224	U	0	0	0	eth0
192.168.2.0	10.0.118.42	255.255.255.0	UG	0	0	0	eth0

PC LPT05 E15

Test de connectivité en local -> Ping du PC12 :



```
local@lptxx:~$ ping 192.168.2.10
PING 192.168.2.10 (192.168.2.10) 56(84) bytes of data.
64 octets de 192.168.2.10 : icmp_seq=1 ttl=63 temps=0.444 ms
64 octets de 192.168.2.10 : icmp_seq=2 ttl=63 temps=0.443 ms
64 octets de 192.168.2.10 : icmp_seq=3 ttl=63 temps=0.578 ms
64 octets de 192.168.2.10 : icmp_seq=4 ttl=63 temps=0.550 ms
^C
--- statistiques ping 192.168.2.10 ---
4 paquets transmis, 4 reçus, 0 % paquets perdus, temps 3075 ms
rtt min/avg/max/mdev = 0.443/0.503/0.578/0.061 ms
```

PC LPT05 E15

Modification dans le fichier resolv.conf pour le serveur DNS : `local@lptxx:/etc$ sudo nano resolv.conf`

```
nameserver 127.0.0.53
options edns0 trust-ad
nameserver 8.8.8.8
```

Ping de google.fr afin de tester la connectivité avec internet :

```
local@lptxx:/etc$ ping google.fr
PING google.fr (216.58.215.35) 56(84) bytes of data.
64 octets de par21s17-in-f3.1e100.net (216.58.215.35) : icmp_seq=1 ttl=114 temps
=9.52 ms
64 octets de par21s17-in-f3.1e100.net (216.58.215.35) : icmp_seq=2 ttl=114 temps
=9.65 ms
64 octets de par21s17-in-f3.1e100.net (216.58.215.35) : icmp_seq=3 ttl=114 temps
=9.69 ms
^C
--- statistiques ping google.fr ---
3 paquets transmis, 3 reçus, 0 % paquets perdus, temps 2002 ms
rtt min/avg/max/mdev = 9.518/9.621/9.694/0.075 ms
```

PC12 - Opnsense

Configuration




```
local@1114-PC12-SNIR:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.2.10 netmask 255.255.255.0 broadcast 192.168.2.255
    ether e4:54:e8:da:c9:26 txqueuelen 1000 (Ethernet)
    RX packets 169031 bytes 127360242 (127.3 MB)
    RX errors 0 dropped 161 overruns 0 frame 0
    TX packets 118055 bytes 10114481 (10.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
















lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Boucle locale)
    RX packets 17929 bytes 1597574 (1.5 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17929 bytes 1597574 (1.5 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

PC12 - VPN

Règles de VPN :

VPN: IPsec: Tunnel Settings



	Type	Remote Gateway	Mode	Phase 1 Proposal	Authentication	Description	
		<i>Local Subnet</i>	<i>Remote Subnet</i>	<i>Phase 2 Proposal</i>			
<input type="checkbox"/>	 IPv4 IKEv2	WAN 10.0.118.62		AES (128 bits) + SHA256 + DH Group 14	Mutual PSK	vpn prof	    
<input type="checkbox"/>	 ESP IPv4 tunnel	LAN	192.168.10.0/24	AES (auto), Blowfish (auto), 3DES, CAST128 + MD5, SHA1 + off			   
							  

☒ Enable IPsec

Save

PC12 - Opnsense

Autorisation des réseaux privés :

 Block private networks	<input type="checkbox"/>
 Block bogon networks	<input type="checkbox"/>

Autorisation des réseaux privés :

<input type="checkbox"/>	   	IPv4 *	*	*	*	*	*	*	   
<input type="checkbox"/>	   	IPv4 *	*	*	*	*	*	*	   

PC12 - Opnsense

Firewall: NAT: Port Forward

Select category

The changes have been applied successfully.

			Source		Destination		NAT			
<input type="checkbox"/>	Interface	Proto	Address	Ports	Address	Ports	IP	Ports	Description	<div><div>+</div><div>←</div><div>🗑</div><div>✓</div><div>□</div></div>
<div>!</div>	LAN	TCP	*	*	LAN address	80, 443	*	*	Anti-Lockout Rule	<div><div>✎</div></div>
<input type="checkbox"/>	<div>↔</div> WAN	TCP	*	*	WAN address	22 (SSH)	192.168.2.55	22 (SSH)		<div><div>←</div><div>✎</div><div>🗑</div><div>📄</div></div>
<div>▶</div>	Enabled rule			<div>!</div>	No redirect			<div>↔</div>	Linked rule	
<div>▶</div>	Disabled rule			<div>!</div>	Disabled no redirect			<div>↔</div>	Disabled linked rule	
<div>☰</div>	Alias (click to view/edit)									

PC12 - Opnsense

Ping PC du professeur :

```
--- statistiques ping 192.168.10.10 ---  
2 paquets transmis, 2 reçus, 0 % paquets perdus, temps 1002 ms  
rtt min/avg/max/mdev = 1.699/1.700/1.701/0.001 ms  
local@1114-PC12-SNIR:~$ ping 192.168.10.10  
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.  
64 octets de 192.168.10.10 : icmp_seq=1 ttl=62 temps=1.73 ms  
64 octets de 192.168.10.10 : icmp_seq=2 ttl=62 temps=1.68 ms  
^C
```


Attaques



Aircrack

```
Aircrack-ng 1.6
[00:11:05] 3172685/14344391 keys tested (4837.82 k/s)
Time left: 38 minutes, 29 seconds                22.12%
Current passphrase: toob22

Master Key      : 33 AA 3F A1 6A 00 D8 E8 60 FE 3F C2 A5 0F 5F 64
                  DA 1C 31 85 F2 F1 9B E6 99 D7 C7 E9 40 FD 72 AD

Transient Key   : 2D E3 CF 3B 0A A6 39 03 9E A5 53 BD 62 47 1A 5C
                  FD DD D2 4B 8F 63 89 7A 3F B2 74 B8 BA F0 03 BC
                  AB 97 F4 01 2F 95 0C 42 9B C3 A9 32 E2 D3 50 05
                  5A 9D 7F 5F 04 F9 BE 32 12 69 75 07 E8 F4 1A 01

EAPOL HMAC     : 85 B1 AD 62 8F 2E 18 D7 50 28 52 D9 C7 28 20 8F
```

Tentative de plusieurs mdp pour se connecter au point d'accès WIFI ! Résultat : échec

NMAP en utilisant LPT05

Nmap :

```
local@1114-PC05-SNIR:~$ nmap -sV 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-30 14:53 CEST
Nmap scan report for _gateway (192.168.1.1)
Host is up (0.00029s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE  VERSION
53/tcp    open  domain   Unbound 1.13.1
80/tcp    open  http     OPNsense
443/tcp   open  ssl/https OPNsense
```

```
Nmap scan report for 192.168.1.20
Host is up (0.0026s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE  VERSION
23/tcp    open  telnet   Cisco router telnetd
80/tcp    open  http     Cisco IOS http config
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios
```

Port telnet ouvert sur le point d'accès !

Connection SSH sur le PC 192.168.1.12

Observation des dossiers présents sur le pc ennemi :

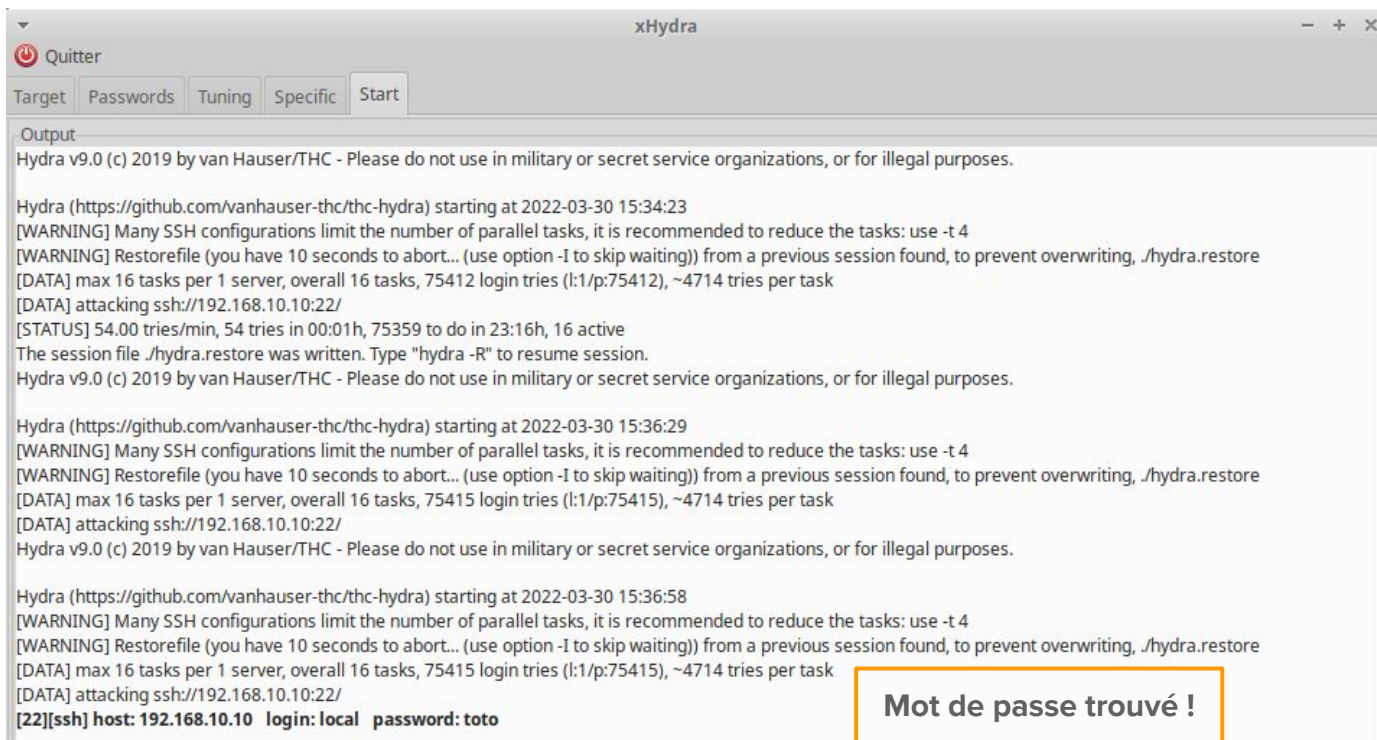
```
local@1114-PC05-SNIR:~$ ls
Bureau          Musique
Documents       pt
Images          Public
Kismet-20211217-13-50-29-1.alert  sent
Kismet-20211217-13-50-29-1.gpsxml  Téléchargements
Kismet-20211217-13-50-29-1.nettxt  TP2BEST
Kismet-20211217-13-50-29-1.netxml  Vidéos
Kismet-20211217-13-50-29-1.pcapdump xubuntu-20.04.3-desktop-amd64.iso
Modèles
```

Création d'un fichier texte :

```
local@1114-PC05-SNIR:~$ mkdir GROUPE2BEST
local@1114-PC05-SNIR:~$ cd GROUPE2BEST/
local@1114-PC05-SNIR:~/GROUPE2BEST$ nano Hello.txt
local@1114-PC05-SNIR:~/GROUPE2BEST$ cat Hello.txt
Bande de nazes
```

Bruteforce depuis le PC serveur web 192.168.2.100

Tentative sur le PC professeur :



The screenshot shows the xHydra application window. The title bar is 'xHydra'. Below the title bar is a menu bar with 'Quitter' and a power icon. Below the menu bar are five tabs: 'Target', 'Passwords', 'Tuning', 'Specific', and 'Start'. The 'Output' tab is selected, showing the following text:

```
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-30 15:34:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 75412 login tries (l:1/p:75412), ~4714 tries per task
[DATA] attacking ssh://192.168.10.10:22/
[STATUS] 54.00 tries/min, 54 tries in 00:01h, 75359 to do in 23:16h, 16 active
The session file ./hydra.restore was written. Type "hydra -R" to resume session.
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-30 15:36:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 75415 login tries (l:1/p:75415), ~4714 tries per task
[DATA] attacking ssh://192.168.10.10:22/
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-30 15:36:58
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 75415 login tries (l:1/p:75415), ~4714 tries per task
[DATA] attacking ssh://192.168.10.10:22/
[22][ssh] host: 192.168.10.10 login: local password: toto
```

The last line of the output is highlighted with an orange box and contains the text: **Mot de passe trouvé !**

Manipulations depuis le PC professeur

Configuration réseau du pc professeur :

```
local@SNIR-12:~$ ifconfig
enp43s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.10.10  netmask 255.255.255.0  broadcast 192.168.10.255
    ether c0:25:a5:37:12:9c  txqueuelen 1000  (Ethernet)
    RX packets 36249  bytes 31585099 (31.5 MB)
    RX errors 0  dropped 413  overruns 0  frame 0
    TX packets 29046  bytes 4633480 (4.6 MB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Boucle locale)
    RX packets 4366  bytes 275799 (275.7 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 4366  bytes 275799 (275.7 KB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

local@SNIR-12:~$
```

Manipulations depuis le PC professeur

Depuis le PC professeur : tentative de connexion SSH sur l'interface 10.0.118.41 de l'Opsense groupe 1 :

Le ssh est bien ouvert mais il nous manque le mot de passe.

```
local@SNIR-12:~$ ifconfig
enp43s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.10.10 netmask 255.255.255.0 broadcast 192.168.10.255
    ether c0:25:a5:37:12:9c txqueuelen 1000 (Ethernet)
    RX packets 36249 bytes 31585099 (31.5 MB)
    RX errors 0 dropped 413 overruns 0 frame 0
    TX packets 29046 bytes 4633480 (4.6 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Boucle locale)
    RX packets 4366 bytes 275799 (275.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4366 bytes 275799 (275.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

local@SNIR-12:~$ ssh local@10.0.118.42
The authenticity of host '10.0.118.42 (10.0.118.42)' can't be established.
ECDSA key fingerprint is SHA256:u33WoE9QoMG7NSn4hMSv/cCqzSIPOuKkA8mJytnQhM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.118.42' (ECDSA) to the list of known hosts.
local@10.0.118.42's password:

local@SNIR-12:~$ ssh local@10.0.118.41
local@10.0.118.41's password: █
```

Manipulations depuis le PC professeur

Tentative de d'attaque brute force

```
local@SNIR-12:~/Téléchargements$ sudo hydra -l local -P  
kADFY qt-everywhere-src-6.1.2/  
local@SNIR-12:~/Téléchargements$ sudo hydra -l local -P
```

```
qt-everywhere-src-6.1.2.tar.xz
```

```
qt-unified-linux-x64-4.1.1-online.run
```

Echec