

Jalon 7 :

- **Rappels des conditions légales d'utilisation d'une application de scan :**

Le scan de port pouvant être utilisé à des fins légitime (comme un administrateur réseau voulant scanner ses machines pour repérer des logiciels indésirables sur son réseau) cependant le scan de port permet à une personne malintentionnée d'obtenir des informations sur des failles de sécurité par exemple.

C'est pour cela que nous pouvons seulement utiliser des applications de scan réseau dans notre propre réseau local dans lequel nous avons le droit d'en faire.

La condamnation pour l'utilisation d'un outil de scan de port tel que nmap dans un cadre non « légal » reste encore compliqué à sanctionné puisqu'il ne s'agit pas clairement d'un accès frauduleux malgré qu'il puisse signifier une étape préliminaire à une intrusion.

- **Scan des ports et IP avec nmap :**

- Scan des ports de tous les appareils du réseau = *nmap 192.168.33.0/24*
- Pour trouver les machines à découvrir (IP et ports) = *nmap 192.168.33.1-100* (d'IP 1 à 100).
- Voir les ports ouverts d'une machine en particulier : *nmap 192.168.33.90* (par exemple).

- **Adresse IP et numéro des ports ouverts sur le PC, le RPI ainsi que les 4 machines connectés à découvrir :**

- Sur le PC : *nmap @IpduPC*

IP : 192.168.33.131

Les ports ouverts : 22 (ssh)

- Sur le rspi : *nmap @IpduRSPI*

Les ports ouverts : 22 (ssh) ; 80 (http) ; 139 (netbio-ssn) ; 145 (microsoft-ds) ; 5900 (vnc).

IP : 192.168.33.194

- Les 4 machines avec les commandes qui est *nmap @IP* :

1ère : 192.168.33.90 (CAMERA)

Les ports ouverts : 21 (FTP) ; 80 ; 443 (https) ; 554 (rtsp) ; 49152 (unknow)

Thomas MIRBEY et RAYNAUD

2ème : 192.168.33.41 (BORNE WIFI)

Les ports ouverts : 22 ; 23 (telnet) ; 53 (domain) ; 80 ; 443.

The screenshot shows the dd-wrt control panel interface. The 'System Information' section displays router details: Router Name (SAE12), Router Model (TP-Link ARCHER-C7 v5), LAN MAC (D8:0D:17:AC:FA:08), WAN MAC (D8:0D:17:AC:FA:08), Wireless MAC (D8:0D:17:AC:FA:07), WAN IPv4 (Disabled), and LAN IP (192.168.33.41). The 'Wireless' section shows the interface as 'ath0', radio is off, mode is AP, network is disabled, SSID is 'dd-wrt', channel is unknown, TX power is off, and rate is disabled. The 'Wireless Packet Info' section shows 0 OK, no error for both received (RX) and transmitted (TX). The 'Services' section lists various services like DHCP Server, Samba, WRT-endsniff, CIFS Automount, Samba Agent, and USB Support, all of which are disabled. The 'Memory' section shows total available memory (128.0 MB / 128.0 MB) and usage for free, used, buffers, cached, active, and inactive states. The 'Space Usage' section shows NVRAM (24 KB / 64 KB) and CIFS (Not mounted). A blue arrow points from the 'Services' section to a text box at the bottom right.

Firmware: DD-WRT v3.0-r40932 std (09/07/19)
Time: 00:45:55 up 25 days, 23:46, load average: 0.44, 0.38, 0.20
WAN: Disabled

Copie d'écran du firmware et l'horaire

The screenshot shows the TP-Link Archer C7 product page. The page features a large image of the router, a list of key features, and a 'Garantie 3 ans' (3-year warranty) badge. The 'Acheter maintenant' (Buy now) button is prominently displayed. The page is in French and includes navigation links for 'Routeurs WiFi', 'Archer C7', 'Présentation', 'Spécifications', 'Revue de presse', and 'Support'.

Archer C7

Routeur Gigabit WiFi bi-bande AC1750 Mbps

- Norme 802.11ac - WiFi haut débit
- Débit WiFi de 450 Mbps en 2.4 GHz et 1350 Mbps en 5 GHz pour une bande passante totale de 1.75 Gbps
- 4 ports LAN Gigabit assurent des vitesses de transferts maximales
- Compatible [OneMesh](#) pour créer votre réseau WiFi maillé avec d'autres produits OneMesh (ex : RE300)
- Le NAT matériel intégré : des liaisons rapides pouvant atteindre 900 Mbps entre WAN et LAN
- 3 antennes externes 5dBi et 3 antennes internes garantissent stabilité et couverture sans fil maximale
- Port USB - Partagez aisément imprimantes, fichiers ou médias avec vos amis ou votre famille localement ou via Internet
- Accès au réseau "Invités" sécurisé
- Compatible avec toutes les box du marché

GARANTIE 3 ANS

Acheter maintenant

Doc du constructeur avec les caractéristiques essentielles de cette borne

• 3ème : 192.168.33.33 (serveur multimédia)

Les ports ouverts : 23 ; 80

- 4ème : 192.168.33.10 (téléphone IP)

Les ports ouverts : 23 ; 80 ; 5060 (sip) ; 5061 (sip-tls)

• Le protocole de couche 4 est TCP

2938	9.663696038	192.168.33.194	192.168.33.196	TCP	74 52576 → 992 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944499 TSecr=0 WS=128
2939	9.665272931	192.168.33.194	192.168.33.131	TCP	74 52576 → 1076 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3862367291 TSecr=0 WS=128
2940	9.665319594	192.168.33.131	192.168.33.194	TCP	54 1076 → 52576 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2941	9.669522039	192.168.33.194	192.168.33.196	TCP	74 44674 → 888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944501 TSecr=0 WS=128
2942	9.670989343	192.168.33.194	192.168.33.131	TCP	74 40504 → 5051 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3862367296 TSecr=0 WS=128
2943	9.671029913	192.168.33.131	192.168.33.194	TCP	54 5051 → 40504 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2944	9.674471277	192.168.33.194	192.168.33.196	TCP	74 26722 → 1076 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944506 TSecr=0 WS=128
2945	9.679517783	192.168.33.194	192.168.33.196	TCP	74 56768 → 5051 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944511 TSecr=0 WS=128
2946	9.681874382	192.168.33.194	192.168.33.131	TCP	74 44138 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3862367307 TSecr=0 WS=128
2947	9.681922294	192.168.33.131	192.168.33.194	TCP	54 5432 → 44138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2948	9.684486951	192.168.33.194	192.168.33.196	TCP	74 53972 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944516 TSecr=0 WS=128
2949	9.686907874	192.168.33.194	192.168.33.131	TCP	74 44886 → 1501 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3862367312 TSecr=0 WS=128
2950	9.686955366	192.168.33.131	192.168.33.194	TCP	54 1501 → 48886 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2951	9.691124776	192.168.33.194	192.168.33.196	TCP	74 69374 → 1501 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944523 TSecr=0 WS=128
2952	9.692627630	192.168.33.194	192.168.33.131	TCP	74 46468 → 2190 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3862367318 TSecr=0 WS=128
2953	9.692675192	192.168.33.131	192.168.33.194	TCP	54 2190 → 46468 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2954	9.696104070	192.168.33.194	192.168.33.196	TCP	74 42186 → 2190 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4145944528 TSecr=0 WS=128
2955	9.697581851	192.168.33.194	192.168.33.131	TCP	74 59088 → 2135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3862367323 TSecr=0 WS=128
2956	9.697645896	192.168.33.131	192.168.33.194	TCP	54 2135 → 59088 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

On voit clairement que c'est le protocole TCP à la couche 4.

• Le protocole de couche 3 est ARP

No.	Time	Source	Destination	Protocol	Length	Info
123	23.88507224	192.168.33.10	192.168.33.1	ARP	60	Who has 192.168.33.125? Tell 192.168.33.1
473	23.886310062	HwlettP_4e:a1:0a	Broadcast	ARP	60	Who has 192.168.33.125? Tell 192.168.33.1
474	23.886578844	Tp-LinkT_2c:fa:08	Broadcast	ARP	60	Who has 192.168.33.147? Tell 192.168.33.1
481	24.882432905	Tp-LinkT_2c:fa:08	Broadcast	ARP	60	Who has 192.168.33.147? Tell 192.168.33.1
513	25.882450048	Tp-LinkT_2c:fa:08	Broadcast	ARP	60	Who has 192.168.33.147? Tell 192.168.33.1
514	25.899554474	Dell_48:8f:f9	Broadcast	ARP	60	Who has 192.168.33.17? Tell 192.168.33.125

• Copie d'écran des réponses des broadcast :

- Broadcast réseau

```
pi@thomas:~$ ping 192.168.33.255 -b
WARNING: pinging broadcast address
PING 192.168.33.255 (192.168.33.255) 56(84) bytes of data.
64 bytes from 192.168.33.10: icmp_seq=1 ttl=64 time=0.628 ms
64 bytes from 192.168.33.102: icmp_seq=1 ttl=64 time=4.10 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=1 ttl=64 time=5.67 ms (DUP!)
64 bytes from 192.168.33.10: icmp_seq=2 ttl=64 time=0.361 ms
64 bytes from 192.168.33.33: icmp_seq=2 ttl=64 time=0.361 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=2 ttl=64 time=0.872 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=3 ttl=64 time=0.370 ms
64 bytes from 192.168.33.10: icmp_seq=3 ttl=64 time=0.445 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=3 ttl=64 time=1.40 ms (DUP!)
^C
--- 192.168.33.255 ping statistics ---
3 packets transmitted, 3 received, +6 duplicates, 0% packet loss, time 78ms
rtt min/avg/max/mdev = 0.361/1.578/5.666/1.832 ms
pi@thomas:~$
```

→ Les adresses qui répondent sont 192.168.33.10 // 192.168.33.102 // 192.168.33.33

- Broadcast universel

```
pi@thomas:~$ ping 255.255.255.255 -b
WARNING: pinging broadcast address
PING 255.255.255.255 (255.255.255.255) 56(84) bytes of data.
64 bytes from 192.168.33.33: icmp_seq=1 ttl=64 time=0.417 ms
64 bytes from 192.168.33.10: icmp_seq=1 ttl=64 time=0.475 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=1 ttl=64 time=0.924 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=2 ttl=64 time=0.399 ms
64 bytes from 192.168.33.10: icmp_seq=2 ttl=64 time=0.399 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=2 ttl=64 time=0.951 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=3 ttl=64 time=0.392 ms
64 bytes from 192.168.33.10: icmp_seq=3 ttl=64 time=0.392 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=3 ttl=64 time=0.950 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=4 ttl=64 time=0.397 ms
64 bytes from 192.168.33.10: icmp_seq=4 ttl=64 time=0.398 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=4 ttl=64 time=0.900 ms (DUP!)
64 bytes from 192.168.33.10: icmp_seq=5 ttl=64 time=0.393 ms
64 bytes from 192.168.33.33: icmp_seq=5 ttl=64 time=0.473 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=5 ttl=64 time=0.888 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=6 ttl=64 time=0.337 ms
64 bytes from 192.168.33.10: icmp_seq=6 ttl=64 time=0.410 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=6 ttl=64 time=0.932 ms (DUP!)
64 bytes from 192.168.33.33: icmp_seq=7 ttl=64 time=0.348 ms
64 bytes from 192.168.33.10: icmp_seq=7 ttl=64 time=0.414 ms (DUP!)
64 bytes from 192.168.33.102: icmp_seq=7 ttl=64 time=0.928 ms (DUP!)
^C
```

→ Les adresses qui répondent sont 192.168.33.10 // 192.168.33.102 // 192.168.33.33

- **Copie d'écran de chaque service auquel vous aurez accédé.**

- Serveur multimédia : (l'additionneur)

← → ↻ 🏠 ⚠ Not secure | 192.168.33.33

📱 Apps 🌐 Debian.org 🌐 Latest News 🌐 Help

A simple html+cgi example

Enter first number

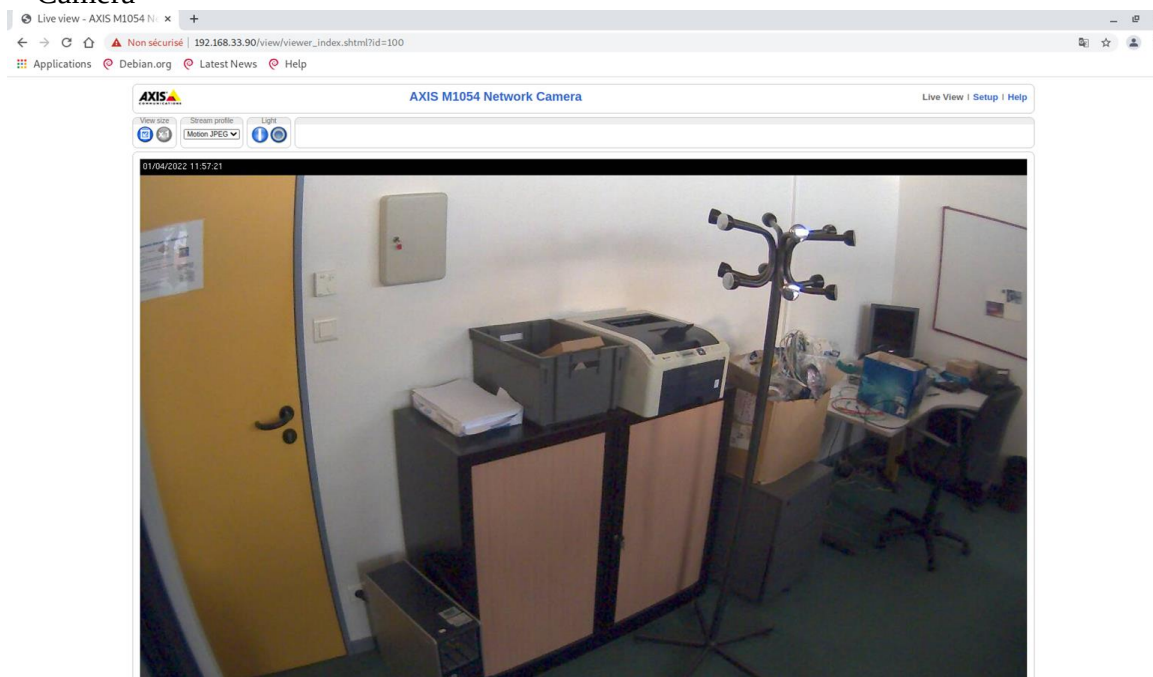
Enter second number

← → ↻ 🏠 ⚠ Not secure | 192.168.33.33/cgi-bin/sum.cgi?number1=1&number2=1

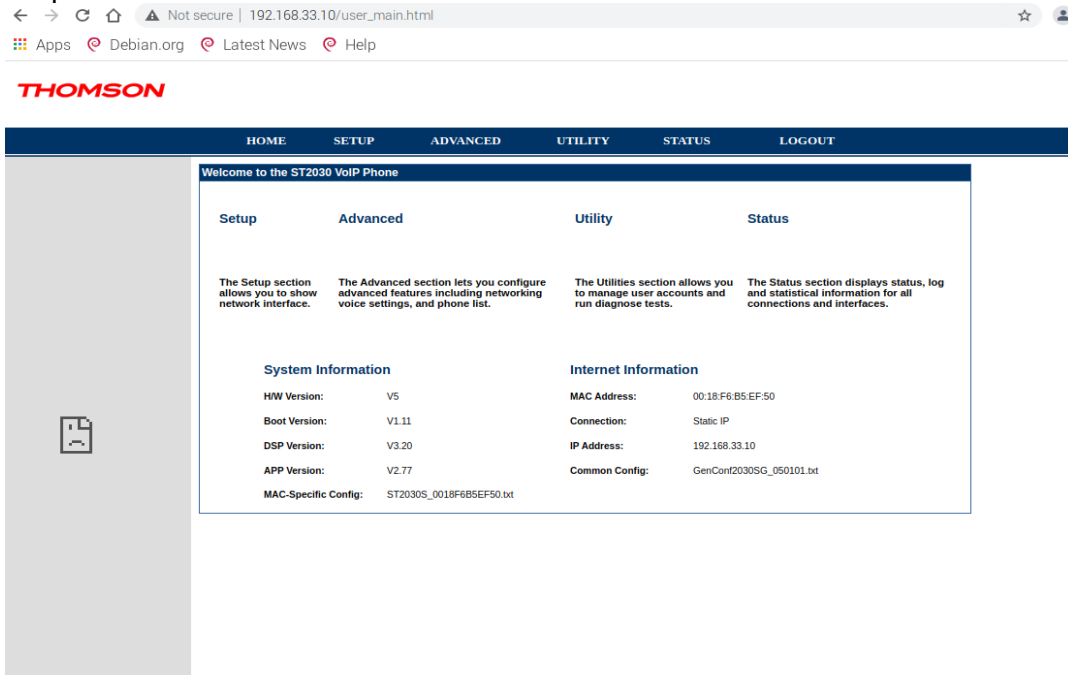
📱 Apps 🌐 Debian.org 🌐 Latest News 🌐 Help

The sum of the two numbers is 2

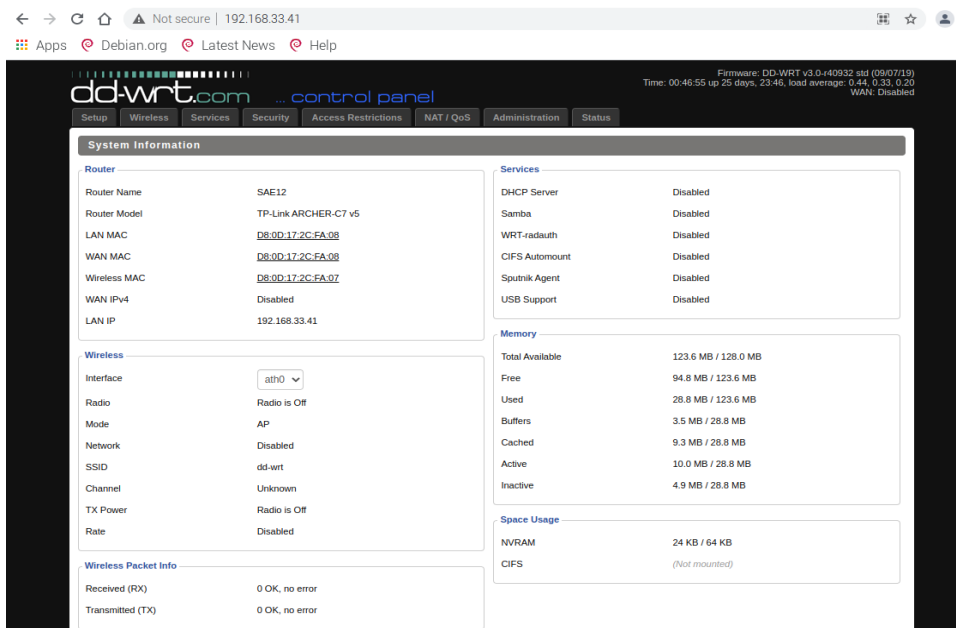
- **Caméra**



- Téléphone IP



- Borne wifi



- IP Passerelle
L'IP est 192.168.33.1

- IP réseau salle
→ 192.168.33.0/24

- Procédure d'installation et utilisation de nmap

→ `sudo apt install nmap`

ou

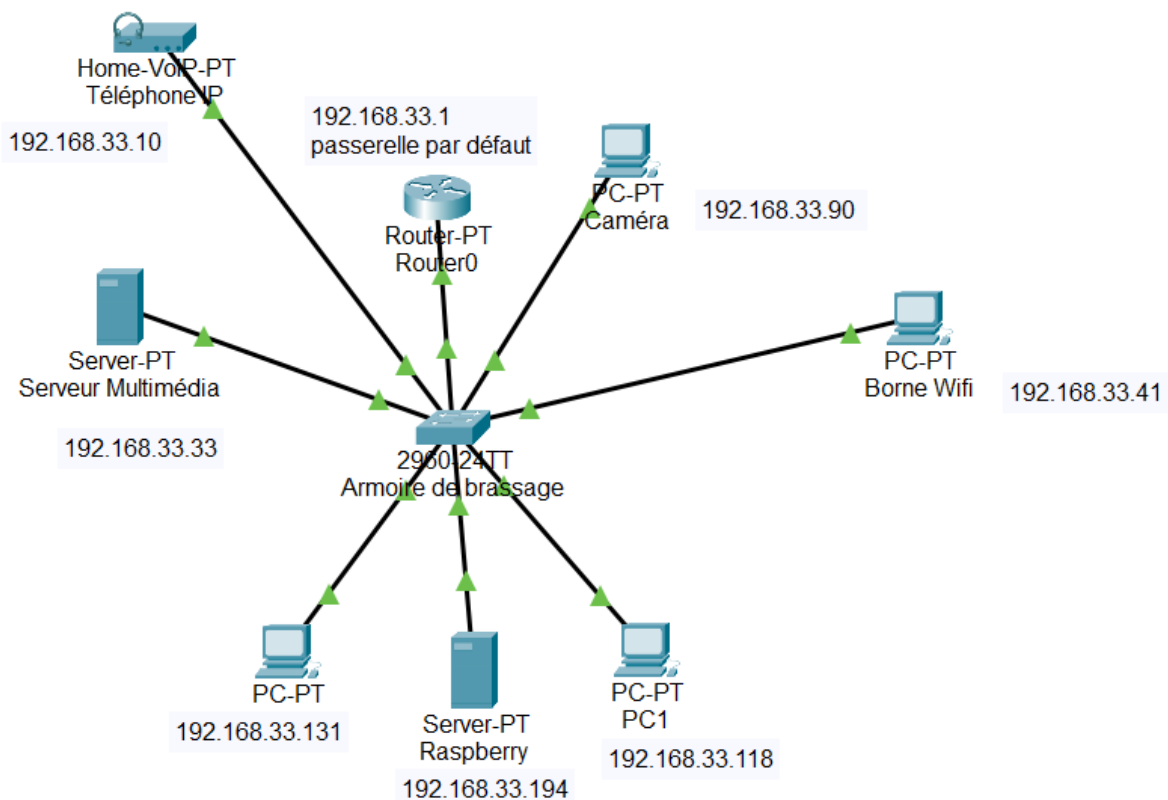
→ `sudo apt -get install nmap`

Afin de l'utiliser il faut taper des commandes précises dans le terminal. Si l'on souhaite se renseigner sur des commandes, on peut écrire dans le terminal soit *nmap* soit *nmap -help*.

On peut aussi se renseigner sur des sites tels que : <https://www.networklab.fr/scan-reseau-nmap/>

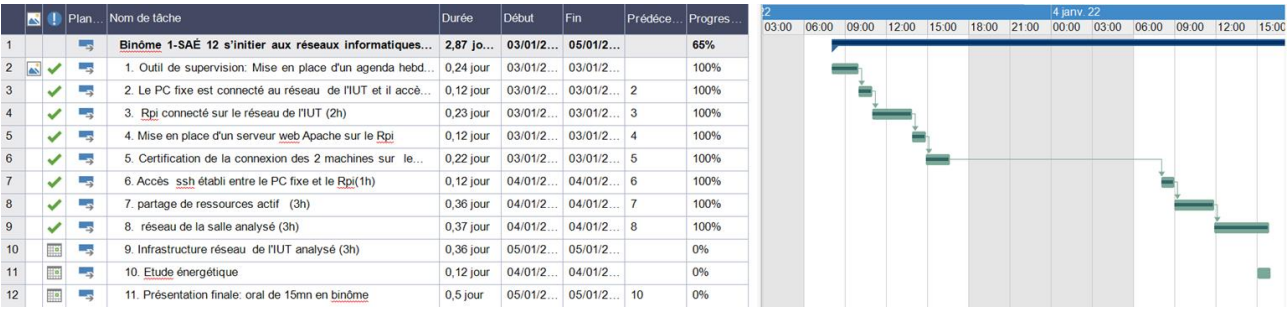
Et utiliser les commandes que nous avons utilisé précédemment.

- Simulation sous PT du réseau de la salle (IP du PC, IP du Rpi, IP passerelle)



Il faut aussi prendre en compte de nombreuses autres machines qui sont connectées au réseau par le switch. Et aussi se rendre compte que pour se connecter au réseau chaque utilisateur doit passer par un portail captif sur www.perdu.com .

• Copie de l'agenda hebdomadaire réactualisé :



		-	Le PC fixe est connecté au réseau de l'IUT et il accède sur l'extérieur : (1h)		
4	3	Rpi connecté sur le réseau de l'IUT (2h)	1	1	
5	4	Mise en place d'un serveur web Apache sur le Rpi	1	1	
6	5	Certification de la connexion des 2 machines sur le même réseau (2h)	1	1	
7	6	Accès ssh établi entre le PC fixe et le Rpi(1h)	1	1	
8	7	partage de ressources actif (3h)	1	1	
9	8	réseau de la salle analysé (3h)	1	1	
10	9	Infrastructure réseau de l'IUT analysé (3h)	1	1	