GASSENDI



mardi 17 novembre 2020



llo Olub Informatique Cassandi

TP monde connecté : cours du 12/11/2020 : NetScan et Putty

Élaboration

17 novembre 2020

Jean D

GASSENDI

Animateur

Administration informatique

Nom du fichier

TP_monde_connecte_cours_12_11_20 20_generalites_Raspbian_installation_ V0.1.odt

But :

Cet utilitaire affiche la liste des adresses logiciel (<u>IPV4/IPV6</u>) et des adresses physique (<u>MAC</u>) de tous les matériels informatique connectés au réseau local.

Il existe un autre outil en open-source cf. angry

Installation:

1. Allez sur le site suivant: https://www.softperfect.com/



SoftPerfect Software Products



SoftPerfect Network Scanner

Windows macOS From 29,00 €

A universal IPv4/IPv6 scanner that can ping computers, scan ports, discover shared folders and comes with flexible filtering and display options. It can retrieve practically any information about network devices via WMI, SNMP, HTTP, SSH and PowerShell, and has many other features.

2. Choisir dans la fenêtre « Download »

Soft				
Perfect	Products	Download	Order	Support
Terms of use				

Download Centre

Here you can download trial versions of our software, free apps and updates.

- Without a licence key, the downloaded package will function as a free trial.
- If you have a valid licence key, simply enter the key into the trial to make it a licensed product.
- To update your current activated version, check its remaining update period, download the latest trial and install it over the current installation it will recognise the existing key. Some applications need to be closed <u>before updating</u>.

Please be assured that our products do not contain any viruses, trojans, adware or malware of any kind. If your antivirus reports something suspicious, it is a <u>false</u> positive and you can safely ignore it.

Product	Download link	Version	Description
	Windows installer	7.2.8	Applicatif installé en fixe sur PC
Network Scanner	Windows portable	7.2.8	A fast multipurpose IPv4/IPv6 scanner with WMI, SNMP, HTTP, SSH and PowerShell support and many other features.
	macOS disk image	1.0.1	
			Applicatif non installé en fixe sur PC

3. Cliquer sur « Windows portable » pour télécharger le dossier :



5. Ouvrir le « netscan.exe » choisit

Icône



Paramétrage de Netscan:



SoftPerfe	ect Network Scanner [PORTABLE]	<u>369</u> 7	
Fichier Vue	Actions Options Signets Aide		
👔 📒 🔚	🔁 🖆 🏫 💼 📷 🏋 🛠 🛒 💡 🐺 🚥 💕 🔅 🛄 🎫 🚨 🥝	٢	
IPv4 depuis	🧕 . 0 . 0 . 0 à 🛛 0 . 0 . 0 . 0 🕂 🛪 🛹 📁 🗹 🔹 Þ Lancer le sca	an	Ш
Adresse IP	Adresse MAC Temps de réponse Nom d'hôte		





Résultat :



Outil Angryip

Installation:

1. Allez sur le site suivant: https://www.angryip.org/

			Vie	ew on G	itHub 🌍
Angry IP Scanner					
Fast and friendly network scanner	About	Screenshots	Download	FAQ	Contribute

Features

- Scans local networks as well as Internet
- IP Range, Random or file in any format
- Exports results into many formats
- Extensible with many data fetchers
- Provides command-line interface
- Over 29 million downloads
- Free and open-source
- Works on Windows, Mac and Linux
- Installation not required

Free Download

DIP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range:	195.80.11	6.0	to	195.80.116.255		IP Range
Hostname:	e-estonia	com	IPt	/24	~	
IP		Ping		Hostname		Ports (
9195.80.1	16.226	[n/a]		[n/s]		
9 195.80.1	16.227	9 ms		[n/a]		
9195.80.1	16.228	10 ms		[n/a]		
9195.80.1	16.229	9 ms		[n/a]		
9 195.80.1	16.230	13 ms		mx3.rmk.ee		
9 195.80.1	16.231	10 ms		mx4.rmk.ee		
9195.80.1	16.232	[n/a]		[n/s]		
9195.80.1	16.233	[n/a]		[n/s]		
9195.80.1	16.234	[n/a]		[n/s]		
9195.80.1	16.235	9 ms		[n/a]		
9195.80.1	16.236	[n/a]		[n/s]		
105 80 1	16 237	In/al		In/cl		
Ready				Display: All		Threads: 0.

Outil Angryip

Download for Windows, Mac or Linux

Windows

Current

Download version 3.7.3 below or browse more releases or even older releases.

• 32/64-bit Installer - autodetects 32/64-bit Java, for Windows 7/8/10

• Executable for 64-bit Java, for 64-bit Java (eg AdoptOpenJDK) on Windows 7/8/10

• Executable for 32-bit Java - for older installations of Oracle Java for Windows

At least Java/OpenJDK 8 is required on your machine, but 11 is recommended.

Applicatif non installé en fixe sur PC



@IPv4/IPv6

IP : Internet Protocol

Rubrique	Nb bits	Nb d'adresses	Constitution			
IPv4	32	4.3 10 ^{^9} 4 294 967 296	192.168.1.72			
Codage	4 octets	128-64-32-16-8-4-2-1 1 1 0 0 0 0 0 0	128-64-32-16-8-4-2-1 128-64-32-16-8-4-2-1 128-64-32-16-8-4-2-1 1 0 1 0 0 0			
Localhost			127.0.0.1			
IPv6	128	3.4 10 ^{^38} 3 402 823 669 209 380 10 ^{^23}	FE80:: 3D45: 345: E844: 69F2%16			

Détail d'allocation des adresses IPv4

Classe A : pour réseaux de grande envergures de l'@ 1.0.0.0 à l'@ 126.0.0.0 soit 126 réseaux de 16 777 214 machines 1 octet fixe pour réseaux moyens (universités) de l'@ 128.1.0.0 à l'@ 191.254.0.0 soit 16 382 réseaux de 65 535 machines Classe C : pour réseaux régionaux (PME/PMI) de l'@ 192.0.1.0 à l'@ 223.255.254.0 soit 2 097 150 réseaux de 254 machines 3 octets fixe

@IPv4/IPv6

Pour connaître son IP privée ou locale de son PC

1. Clique droit sur :



- 2. Ouvrir une console en sélectionnant « Windows PowerShell »
- 3. Taper la commande: cmd /k ipconfig
- 4. Résultat



@IPv4/IPv6

Votre box haut débit possède une adresse IP privée et une adresse IP publique.

Adresse IP publique

C'est l'adresse IP « tournée vers l'extérieur » et matérialisant l'adresse de la box sur le réseau Internet.

Les adresses IP publique servent aux ordinateurs du réseau pour communiquer entre eux. Ainsi, chaque ordinateur d'un réseau possède une adresse IP unique. C'est cette adresse que « voit » par exemple un serveur sur lequel vous allez faire des transactions.

Adresse IP privée

C'est l'adresse IP « tournée vers l'intérieur », c'est-à-dire permettant de connecter un ou plusieurs ordinateurs.

Comment connaître son IP publique

L'adresse IP publique est délivrée par votre FAI (Fournisseur d'Accès à Internet) au moment de l'installation et synchronisation de la box.

Voici comment faire pour connaître son IP publique :

Se connecter sur sa box :

Allez dans Mes Services \rightarrow Accès Internet \rightarrow État de la connexion Internet

Ou allez sur le site : <u>http://www.whatismyip.com</u>



MAC : Media Access Control

Les adresses MAC sont des adresses physiques uniques propres à chaque périphérique réseau. Elles sont inscrites dans la trame normée 802.3 qui en gère l'accès.

Pour connaître l'adresse MAC de son PC

Aller sur le site : http://coffer.com/mac_find/

Ou :

- 1. Clique droit sur :
- 2. Ouvrir une console en sélectionnant « Windows PowerShell (admin) »
- 3. Taper la commande: ipconfig /all
- 4. Résultat

@MAC

27 Administrateur : Windows PowerShell		
PS C:\WINDOWS\system32> ipconfig /all		
Configuration IP de Windows		
Nom de l'hôte : Dinozzo-PC		
Suffixe DNS principal :		
Type de noeud Hybride		
Routage IP activé Non		
Proxy WINS activé Non		
Liste de recherche du suffixe DNS.: home		
Contra Ethonest Consultant ou official local a	Ethernet	
Carte Ethernet Connexion au reseau local :		
Statut du média Média déconnecté	\checkmark	
Surfixe das propre à la connexion.		
Description	I-E Gigabit Ethernet (NDIS 6	5.20)
Adresse physique		
Unce active.		
Configuration automatique activee : Oui		
Carte Ethernet Ethernet :		
Statut du média Média déconnecté		
Suffixe DNS propre à la connexion		
Description Kaspersky Security Data Escort Adapter		
Adresse physique		
DHCP activé		
Configuration automatique activée: Oui	AC WI-FI	
Calce reseau sans til connexion reseau sans til p		
Suffixe DNS pronne & la connevion + home	<u>¥</u>	
Description Périphérique sans fil Realtek 8185 Extensibl	802.11b/g	
Adresse physique		
DHCP activé.		
Configuration automatique activée : Oui		
Adresse IPv6 de liaison locale : fe80::3d45:345:e844:69f2%16(préféré)		
Adresse IPv4		
Masque de sous-réseau		
Bail obtenu dimanche 28 juin 2020 11:01:00		
Bail expirant		
Passerelle par detaut		
Serveur Unit P		
Control De Chiefer DeCPV6		
Serveurs DNS		
NetRIOS sus Train		
HELDING SUI TEPAPACA A A A A A A A A A A A A ALLANE		

@MAC

Constitution de la Trame 802.3 qui porte l'@ MAC



I'@ MAC est constituée de 6 octets soit 48 bits



Raspberry

Glossaire

Sigle				
CRC	Cyclic Redundancy Check (Check-Sum)			
FAI	Fournisseur d'Accès à Internet			
FCS	Frame Check Sequence (Code Détection d'Erreurs)			
IP	Internet Protocol			
MAC	Media Access Control			
MSB	Most Significant Bit			

PuTTY / SSH

Généralité :

Une des grandes forces de Linux est que l'on peut s'en servir même si l'on est à des centaines de kilomètres de la machine.

Aujourd'hui, si j'habite à Paris, je peux très bien contrôler un ordinateur sous Linux situé à Tokyo, en même temps qu'un autre ordinateur situé à San Francisco. Je peux même ordonner à l'ordinateur de Tokyo d'envoyer un fichier à celui de San Francisco.

Le PC qui se connecte au serveur est appelé le client



Nota: pour plus d'informations sur SSH cliquer <u>SSH</u>

But :

Cet utilitaire permet à un client Windows de se connecter directement à des serveurs distants Linux à travers une liaison Ethernet sécurisé (SSH).

Ci-dessous le résultat de l'accès à la Raspberry Pi en mode console depuis un PC Windows.



Installation:

1. Allez sur le site suivant: https://www.putty.org/

2. Choisir la version à télécharger :

Packa	ge files		Applicatif ave	c installeur pour PC 32 bits ou	64 bits
You pro (Not su MSI (* 32-bit:	obably want on are whether you Windows Inst	ne of these. They in u want the 32-bit o caller')	nclude version r the 64-bit ve	ns of all the PuTTY utilersion? Read the <u>FAQ e</u> (or by FTP)	ities. ntry.) (signature)
64-bit:	p	utty-64bit-0.74	-installer	.msi (or by FTP)	(signature)
Unix so	ource archive				
.tar.g	iz: D	utty-0.74.tar.o		(or by FTP)	<u>(signature)</u>
		Pour Linux, il fa	ut décompresser	le fichier	
Alternative	binary files	Applica	tif pour PC 32 bi	ts ou 64 bits	
The installer pa	ackages above will pro	wide versions of all of these (except PuTTYtel), bi	ut you can download standalone bina	ries one by one if you prefer.
Not sure whet	ther you want the 32-bi	it or the 64-bit version? Read	the <u>FAQ entry</u> .)		
putty.exe (th	e SSH and Telnet clie	ent itself)			
32-bit:	putty.exe	(or by	y FTP) (signa	<u>iture)</u>	
54-bit:	putty.exe	(or b	y FTP) (signa	<u>iture)</u>	

3. Téléchargement de la version « putty.exe » choisit:



4. Ouvrir la version « putty.exe » choisit:



Paramétrage de PuTTY:

Lorsque vous démarrez PuTTY, vous obtenez la boîte de dialogue ci-dessous :

		1 - renseigner la fenêtre Host Name avec l'@ IP de votre PI
		192.168.1.24 (@ donnée par Netscan)
Reputity Configuration		×
Category:		
Session	Basic options for your PuTTY session	
Logging	Specify the destination you want to connect to	2 – vérifier que la fenêtre Port affiche 22
E Keyboard	Host Name (or IP address)	SSH
Bell	22 🖌	
Features	Connection type:	
E-Window	O Raw O Teinet O Riogin SSH O Serial	
Behaviour	Load, save or delete a stored session	3 – vérifier que SSH soit coché
Translation	Saved Sessions	
Selection		
E Connection	Default Settings Load	4 – pour sauvegarder I @IP (option)
Data	maison	cliquer sur « Load »
Proxy	Datas	donner un nom significatif
Riogin	Delete	cliquer sur « Save »
SSH	1	
Serial	Close window on exit:	
	Always Never Only on clean exit	5 – lancer l'applicatif
About	Open Cancel	
1 30.2.2.2.		

5. Commandes système:

New Session démarre une nouvelle instance de PuTTY, et affiche la boîte de dialogue de configuration habituelle.

Duplicate Session démarre une session dans une nouvelle fenêtre, avec exactement les mêmes réglages que la session courante (connexion au même serveur, avec le même protocole, les mêmes réglages, etc.).

Restart Session utilisée dans une fenêtre inactive fait pareil que 'Duplicate Session', mais dans la fenêtre courante.

Reset Terminal provoque une réinitialisation complète de l'émulateur de terminal.

Le sous-menu **Saved Sessions** vous permet d'accéder rapidement à des ensembles de réglages de session sauvegardés auparavant.

7. Modification des réglages de session:

Change Settings

fait apparaître une version allégée de la boîte de dialogue de configuration initiale et permet d'ajuster la plupart des propriétés de la session en cours.

- . changer la taille du terminal,
- . la police de caractères,
- . les couleurs,
- . les actions associées à différentes combinaisons de touches, etc..
- . sauvegarder les réglages de la session courante.

6. Journal de session:

Logging permet de conserver la trace de tout ce qui s'affiche sur votre écran. Voir panneau *Logging* de la boîte de dialogue de configuration.

Pour enregistrer des traces de la session courante dans un journal de session, Cliquez sur *Change Settings*, dans le menu système, et allez dans le panneau *Logging*. Choisir un nom de fichier journal, et un mode d'enregistrement des traces (soit tout le trafic ou texte imprimable). Cliquez sur *Apply* pour démarrer l'enregistrement. Sélectionner *Logging turned off completely* pour arrêter l'enregistrement. Le fichier journal est lisible à la guise

7. Une fenêtre type « console » s'affiche

Affichage du nom de la machine hôte

		-	
	🧬 pioraspberrypi: ~	X	
	login as: pi pi@192.168.1.13's password: Linux raspberrypi 3.2.27+ #250 PREEMPT Thu Oct 18 19:03:02 BST 2012 armv61	~	
	The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.		
	Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Mon Dec 17 10:59:46 2012 from 192.168.1.6		
	<pre>pi@jean:~/Cours2 \$ ifconfig eth0</pre>		Affichage @MAC
Affichage @IPv4	inet adr:192.168.1.24 Bcast:192.168.1.255 Masque:255.255.255.0 adr inet6: fe80::e370:ef8e:b73f:d2d5/64 Scope:Lien		
Affichage @IPv6	UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:27825 errors:0 dropped:0 overruns:0 frame:0 TX packets:30425 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 lg file transmission:1000 RX bytes:3713111 (3.5 MiB) TX bytes:13753420 (13.1 MiB)		
		9	

Connection via SSH à partir de Windows (PuTTY) :

La 1^{ére} fois que vous utilisez **SSH** pour vous connecter à un serveur, vous verrez ce message

fingerprint -	 The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is. The server's rsa2 key fingerprint is: ssh-rsa 2048 fd:d9:2d:e5:df:fd:80:bb:e9:eb:59:30:58:34:dc:f7 If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting. If you want to carry on connecting just once, without adding the key to the cache, hit No.
	If you do not trust this host, hit Cancel to abandon the connection. Oui Non Annuler Aide

Comme **PuTTY** n'a aucun moyen de savoir si la clé d'hôte envoyée par la machine distante est la bonne, ou pas, il vous affiche l'avertissement ci-dessus, et vous demande si oui ou non, vous estimez pouvoir faire confiance à cette clé d'hôte.

Cela sert à vous protéger d'une attaque réseau connue sous le nom de **spoofing** (usurpation d'identité).

Le *spoofing* consiste à détourner secrètement votre tentative de connexion vers un ordinateur autre que celui auquel vous voulez vous connecter, de façon à ce que le pirate qui est à l'origine de ce détournement puisse prendre connaissance de votre mot de passe, et s'en servir ensuite pour ouvrir une session sur la machine à laquelle vous vouliez vous connecter, en se faisant passer pour vous.

SSH affecte à chaque serveur un identifiant unique, que l'on appelle une clé d'hôte. Ces clés sont conçues de telle façon qu'il est impossible pour une machine de se fabriquer une clé d'hôte qui corresponde à une autre machine qu'elle-même, ceci empêche toute usurpation d'identité entre machines.

Ainsi, si vous essayez de vous connecter à un serveur et qu'il vous envoie une clé d'hôte différente de celle que vous attendiez, **PuTTY** peut vous prévenir que la machine distante n'est pas celle que vous pensez, et que vous faites peut-être l'objet d'une tentative de détournement de connexion.

Comme **PuTTY** garde trace, dans la base de registres de Windows, de la clé d'hôte de chaque serveur auquel vous vous connectez, donc à chaque fois que vous vous connectez à un serveur, il vérifie que la clé d'hôte envoyée par le serveur est bien la même que celle qu'il avait envoyée la dernière fois que vous vous y êtes connecté.

Si ce n'est pas le cas, vous verrez s'afficher un avertissement et vous aurez la possibilité d'abandonner la tentative de connexion avant même d'avoir envoyé à la machine distante quoi que ce soit de confidentiel, comme votre mot de passe, par exemple.

Activer le client SSH dans Windows :

Windows 10 prend en charge SSH mais il faut l'activer

client SSH se trouve dans « Gérer les fonctionnalités facultatives »

Procédure d'installation du client SSH :

Clic gauche pour ouvrir menu Windows



ouvrir Paramètres

suivre les étapes 1 - 2 - 3 - 4 de la planche suivante

Procédure d'installation du client SSH :



Généralités :

SSH est une technologie pour les réseaux qui facilite l'accès sécurisé à une session sur un ordinateur multi-utilisateurs, depuis un autre ordinateur.

Les systèmes d'exploitation multi-utilisateurs, présentent à l'utilisateur une interface de type console.



Avec ce type d'interface, pas besoin d'être assis devant la machine, les commandes, et leurs résultats, peuvent provenir d'une autre machine distante en transitant via un réseau.

Sur la machine devant laquelle vous êtes assis, vous utilisez ce qu'on appelle un *client*, qui établit une connexion réseau avec l'autre ordinateur, que l'on appelle le *serveur*. La connexion réseau achemine les séquences de touches et les commandes que vous tapez sur le clavier de la machine cliente jusqu'au serveur, et vous ramène en retour les réponses du serveur.

Résultat:

🔀 Windows PowerShell

Windows PowerShell Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS C:\Users\Dinozzo> ssh pi@192.168.1.23 ssh: connect to host 192.168.1.23 port 22: Connection timed out PS C:\Users\Dinozzo>

Pi non connecté

Les protocoles :

Pour communiquer entre eux en réseau, deux ordinateurs doivent utiliser le même protocole.

Par ex: HTTP (HyperText Transfer Protocol). Pages web

FTP (*File Transfer Protocol*, protocole de transfert de fichiers)

IMAP (Internet Message Access Protocol, utilisé pour s'échanger des e-mails)

SSH (Secure Socket Shell, utilisé pour sécuriser une liaison)



Internet est un environnement hostile, et la sécurité est notre l'affaire. Alors si vous vous connectez à une machine via Internet, il est recommandé d'utiliser le protocole **SSH** car c'est la solution pour sécuriser les données

La sécurité :



Avantages:

. SSH est un protocole hautement sécurisé qui fait appel à la cryptographie forte pour protéger votre connexion contre les écoutes, les détournements et autres attaques.

. La méthode employée par SSH est sûre, car pour accéder à votre compte utilisateur sur le serveur, *l'attaquant* doit d'abord réussir à accéder à votre machine client.

. SSH permet d'ouvrir une session sur le serveur sans avoir à taper un mot de passe.

. SSH vous permet de vous connecter au serveur et de passer une commande dans la foulée, de façon à ce que le serveur exécute la commande puis ferme la connexion tout de suite après, ce qui permet d'utiliser SSH pour des traitements automatisés, sans intervention humaine.

Le chiffrement :

Comment sont chiffrés les échanges avec SSH ?

SSH utilise les deux catégories suivantes de chiffrement pour garantir la sécurité.

- symétriques
- asymétriques

Le chiffrement symétrique:

Méthode de chiffrement la plus simple car facile à comprendre.

Utilisation d'une **clé** (un mot secret) pour chiffrer un message et le déchiffrer. (clé = topsecret)

Défaut : Il faut transmettre la clé de chiffrement (topsecret) discrètement sinon piratage



Le chiffrement asymétrique:

Pour palier la contrainte d'envoi de la clé de chiffrement discrètement, il faut chiffrer également la clé lors de l'envoi.

Pour chiffrer la clé de chiffrement symétrique, utilisation de la méthode : le chiffrement asymétrique.

Le chiffrement asymétrique, utilise une clé pour chiffrer, et une autre pour déchiffrer. (2 clés) une clé dite « **publique** » qui sert à **chiffrer**; une clé dite « **privée** » qui sert à **déchiffrer**.

Fonctionnement:

L'ordinateur génère une paire de clés : une privée et une publique. Elles vont ensemble. La clé publique peut être transmise en clair sur le réseau

La clé privée, qui permet donc de déchiffrer, doit rester secrète.



L'algorithme de chiffrement asymétrique le plus connu s'appelle **RSA**.

La création d'un tunnel sécurisé avec SSH

SSH utilise les deux chiffrements : asymétrique et symétrique dans cet ordre.

1. Utilisation d'abord du chiffrement asymétrique pour s'échanger discrètement une clé secrète de chiffrement symétrique.

2. Ensuite, utilisation tout le temps de la clé de chiffrement symétrique pour chiffrer les échanges.

Les ordinateurs s'échangent donc la clé de chiffrement symétrique de manière sécurisée (grâce au chiffrement asymétrique) et peuvent ensuite communiquer plus rapidement en utilisant en permanence le chiffrement symétrique.

Etapes

Au début de la communication les ordinateurs s'échangent donc la clé de chiffrement symétrique de manière sécurisée (grâce au chiffrement asymétrique)

ils peuvent ensuite communiquer plus rapidement en utilisant en permanence le chiffrement symétrique.

Les étapes de la création d'un canal sécurisé avec SSH en images



Le client et le serveur connaissent maintenant tous les deux la clé symétrique *topsecret,* et à aucun moment ils ne l'ont échangée en clair sur le réseau. Ils peuvent donc s'envoyer des messages chiffrés de manière symétrique en toute tranquillité.

Tout est chiffré grâce à la clé symétrique que le client et le serveur se sont astucieusement communiquée.

Maintenant qu'ils discutent de manière sécurisée, le client peut se connecter au serveur : il peut donner son login et son mot de passe sans craindre de se les faire voler par le pirate.



Glossaire

Sigle	
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IMAP	Internet Message Access Protocol
IP	Internet Protocol
MAC	Media Access Control
SSH	Secure Socket SHell