

Building VPN with OpenVPN

dpazet@DonsLaptop:~\$ sudo apt info openvpn → package.

using Nmap + nmap

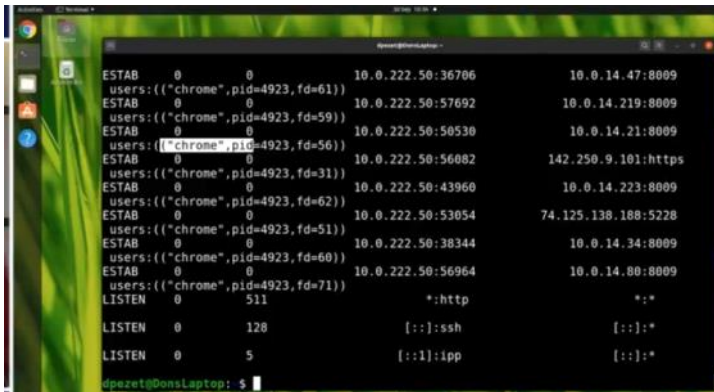
* Netstat & ss (software statistics) Socket statistics

↳ udp not always interesting

↳ ss -t (shows tcp connections)

→ a (all ports) even listening ports

→ P (shows process using it)



Nmap

Till time 7:26

~

sudo nmap -p 1-1024 10.0.222.50-54

Port states open, closed, filtered

closed

filtered

it's like the drop in ip tables. Nmap does not know what happened with packet

it's like the rejected ip tables

happened with packet |

windows 10 blocks ping by default

we can configure in nmap what is the scan type

-PN stealth mode

-S → scan type

-T → will try to
connect to a port
will fetch more information
on the port which it can
connect to (like ssh server version)

SSH connections

23 July 2024 06:47

*copies the ssh key to server,
& then can login via ssh.*

```
dpezet@Dons-Laptop:~$ ssh-copy-id dpezet@10.222.0.51
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out
at are already installed
/usr/bin/ssh-copy-id: INFO: 2 key(s) remain to be installed -- if you are prompted n
is to install the new keys
dpezet@10.222.0.51's password:
Number of key(s) added: 2
Now try logging into the machine, with: "ssh 'dpezet@10.222.0.51'"
and check to make sure that only the key(s) you wanted were added.
```

it works by adding to authorized keys

ssh server keys ref/ssh

*better to have my own ssh keys [eg if we have cloned systems
then same keys in many machine]*

we can say what encryption algo are supported

We can configure which users are allowed to be connection

*There are host.deny & host.allow files. | But better to
do it with firewall.*

ftp

23 July 2024 07:15

There is vsftpd which is a secure version of ftp
written by a security expert

Sftp is more secure

it supports ssl based file transfer.

Pure FTP

- * very feature rich examples ↗

- * for every 5gb down ↑ upload

- * move files to tmp & only on admin approval
move to other folder

- * can run just as user space application

Till 3.30

- * may have to allow firewall

/etc/pure-ftpd/ config file is there as usual

- * this is a conf folder → inside we can create files

```
dpezet@Ubuntu-Server: /etc/pure-ftpd$ cd conf
dpezet@Ubuntu-Server: /etc/pure-ftpd/conf$ ls
AltLog      MinUID      PAMAuthentication  TLSCipherSuite
FSCharset   NoAnonymous PureDB             UnixAuthentication
dpezet@Ubuntu-Server: /etc/pure-ftpd/conf$
dpezet@Ubuntu-Server: /etc/pure-ftpd/conf$
dpezet@Ubuntu-Server: /etc/pure-ftpd/conf$ cat NoAnonymous
yes
dpezet@Ubuntu-Server: /etc/pure-ftpd/conf$
dpezet@Ubuntu-Server: /etc/pure-ftpd/conf$ sudoedit NoAnonymous
dpezet@Ubuntu-Server: /etc/pure-ftpd/conf$
dpezet@Ubuntu-Server: /etc/pure-ftpd/conf$
dpezet@Ubuntu-Server: /etc/pure-ftpd/conf$ cat NoAnonymous
no
dpezet@Ubuntu-Server: /etc/pure-ftpd/conf$
dpezet@Ubuntu-Server: /etc/pure-ftpd/conf$ echo 10000 20000 | sudo tee /etc/pure-ftpd/conf/
PassivePortRange
10000 20000
```

notice files contain config

Alt log setting \rightarrow there are setting like
cls, w3f, stats

we can Pure-ftps

openvpn

28 July 2024 22:31

Open client same as server package openvpn
certificate created at server side needs
to be synced.

this will create an interface (virtual) with an
interface

DNS

Sunday, 28 July 2024 10:42 PM

BIND → v9, named (another name)
not normally is not installed by default

ss -natp

systemd-resolved (normally installed now.)

bind9-utils	{	bind9-dnsutils
*dnsutils		dns client utils
*server(side)		

service is called in his case named.service

named-local.conf → configure address

ACL list (to determine who is allowed to copy the zone files)

```
//=====
// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.isc.org/bind-keys
//=====
dnssec-validation auto;
listen-on port 53 { 127.0.0.1; 10.0.222.51 };
listen-on-v6 { any; };
allow-query { trusted-hosts; };
allow-transfer { none; };
};

acl "trusted-hosts" {
    localhost;
    localnets;
```

We can configure recursive lookup

hosted zones.

normally when i buy a domain & want to maintain the dns by ourselves.

There are zone files
create a file called hosted zone.

SOA, TTL, Name server, are there in this file
Host Records

```
GNU nano 4.8 /var/tmp/lab.itpro.tvXXGQmboB.dns Modified
$TTL 604800
@ IN SOA dns1.lab.itpro.tv. admin.lab.itpro.tv (
1; Serial Number
86400; Refresh
7200; Retry
57600; Expire
3600); Cache TTL
@ IN NS dns1.lab.itpro.tv.
web1 IN A 10.0.222.52
www IN CNAME web1.lab.itpro.tv
mail IN A 10.0.222.53
dns1 IN A 10.0.222.51
```

points to a domain name instead of IP

add the new zone file ^{entry} into the default conf
file

Reverse . lookup zone (IP to a name)