

Network Management Workshop – APRICOT 2004, Malaysia

◆ Nessus www.nessus.org



- A security scanner
- Software to remotely audit a given network or servers
- Determine whether bad guys (aka 'crackers') may break into it, or misuse it in some way
- Unlike others, Nessus does not take anything for granted
- Will *not* consider that a service is running on a fixed port
- if you run your web server on port 1234, Nessus will detect it and test its security
- will not make its security tests by the version number, but will really attempt to exploit the vulnerability
- very fast, reliable and has a modular architecture that allows you to fit it to your needs

Network Management Workshop – APRICOT 2004, Malaysia

◆ Nessus Features

- **Plug-in architecture** - Each security test is written as an ext plugin
- **Up-to-date security vulnerability database** - updated on a *daily* basis with recent security holes/bugs and available on ftp servers
- **Client-server architecture** - a server, which performs the attacks, and a client which is the front-end, can be different systems
- **Can test an unlimited amount of hosts at the same time**
- **Smart service recognition** – services on non-standard ports
- **Test multiples services** - **two** web servers (or more) on same host
- **Tests cooperation** - so that no useless tests is made
- **Complete reports** – problems and their solutions, risk levels
- **Exportable reports** - as ASCII text, HTML, HTML (pies, graphs)
- **Full SSL support** – can test https, smtps, imaps services
- **Smart plugins** - determine the right plugins for the remote service
- **Non-destructive** - can enable the "safe checks" option
- **Independent developers** - not hide any security vulnerability

Network Management Workshop – APRICOT 2004, Malaysia

◆ Using Nessus

- Nessus is made up of two parts: a client and a server
- Server: a Unix-like system required : Linux will do
- Client: Unix-like system, Windows
- Comes as a standalone package that auto-installs itself
- download the script *nessus-installer.sh* and run it
- Create a nessusd account – to connect to server, run the scans
- Each user has a a set of restrictions to scan the network
- Configure your nessus daemon – standard file will work
- Start nessusd
- Fire up *nessus* client

Network Management Workshop – APRICOT 2004, Malaysia

◆ Nessus network setup



Nessus client
Linux / Windows



Nessus
Server

Scan hosts/services



Mail
server



DNS
server



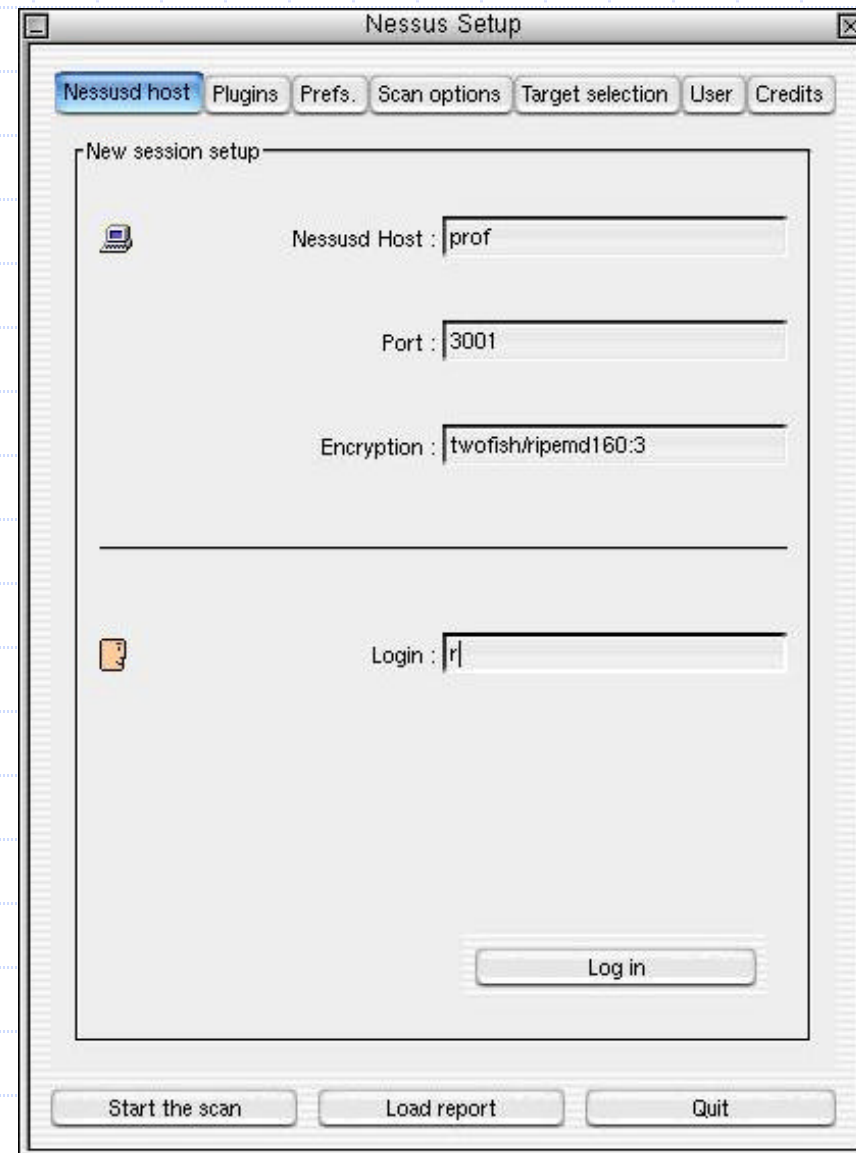
Web
server

Network Management Workshop – APRICOT 2004, Malaysia

◆ Nessus client login:

Click on **Login**, since this setup is correct. Since this is the first time connecting to this server, it will ask the password. The next time you connect to it, the public key will be enough.

Once connected, the **Log in** button changes to **Log out**, and a **Connected** label appears at its left.

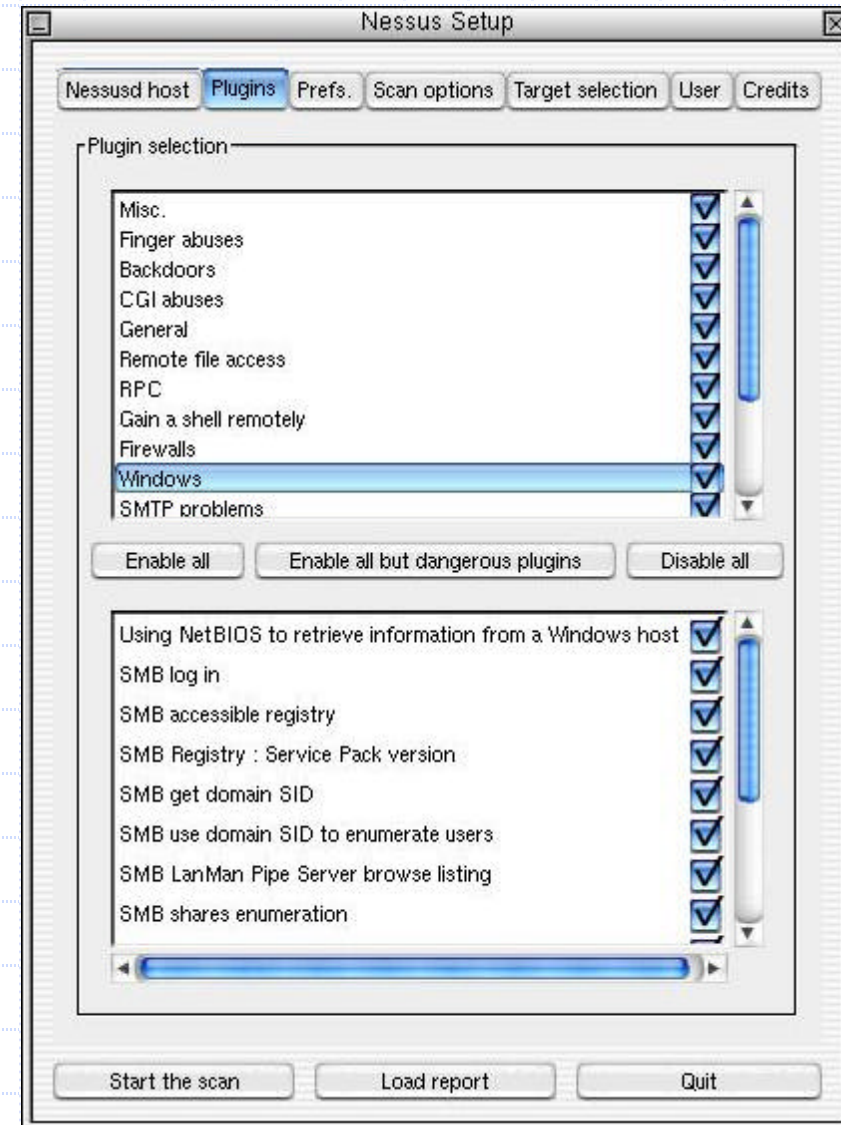


Network Management Workshop – APRICOT 2004, Malaysia

◆ Nessus security checks configuration:

Let all the security checks to be performed, except the **Denial of Service attacks**, because you do not want hosts to **crash**.

Clicking on a **plugin** name will pop up a window explaining what the plugin does.



Network Management Workshop – APRICOT 2004, Malaysia

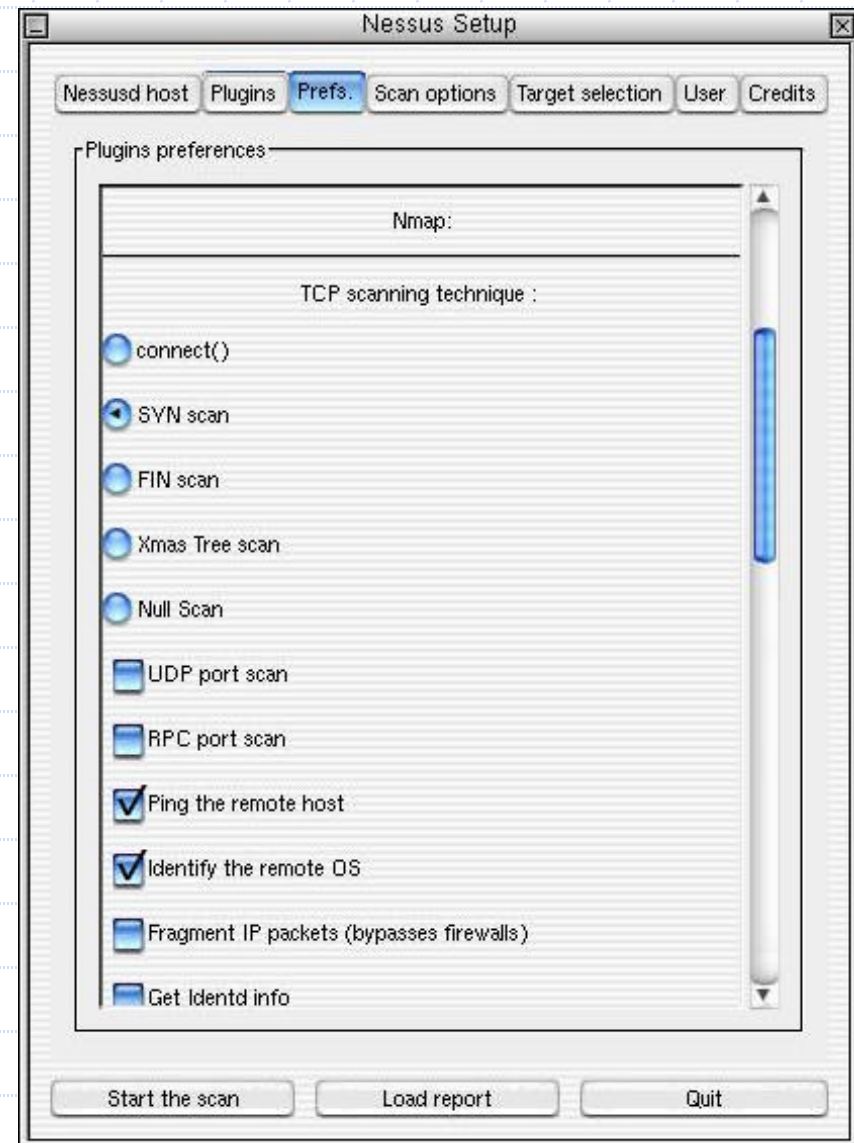
◆ Nessus plugins preferences :

Some security checks will require extra arguments.

For instance, the **pop2 overflow** security test needs a **valid pop account**. The plugin which tests whether a FTP directory is **writeable** or not asks if it should just trust the permissions or really attempt to store a file.

And so on...

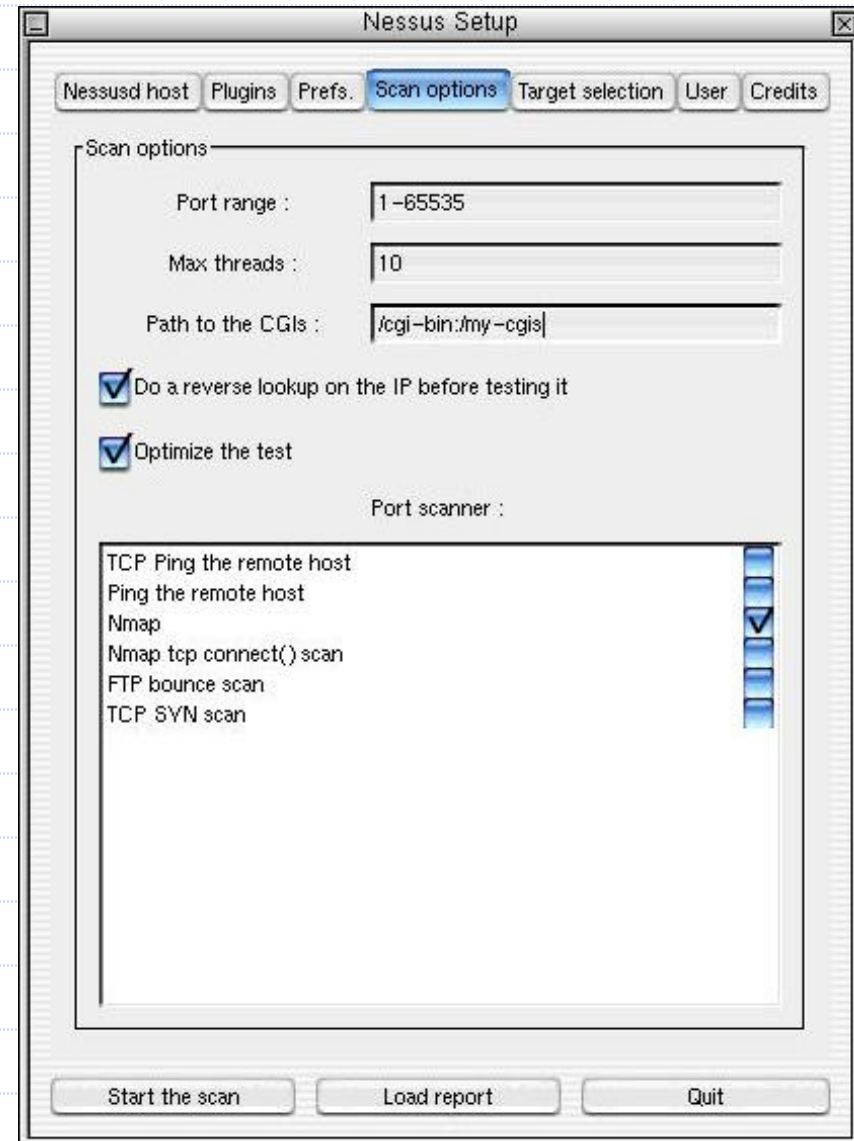
This screen shot shows the configuration of **Nmap**



Network Management Workshop – APRICOT 2004, Malaysia

◆ Nessus scan options :

Here you choose which **port scanner** you want to use. Prefer to use the **Nmap tcp connect** scanner, since it's the **fastest**.



Network Management Workshop – APRICOT 2004, Malaysia

◆ Nessus targets:

Uncheck the 'Perform a DNS transfer zone' option.

Options to define the targets:

192.168.1.1

192.168.1.1-7

192.168.2.1-192.168.2.50

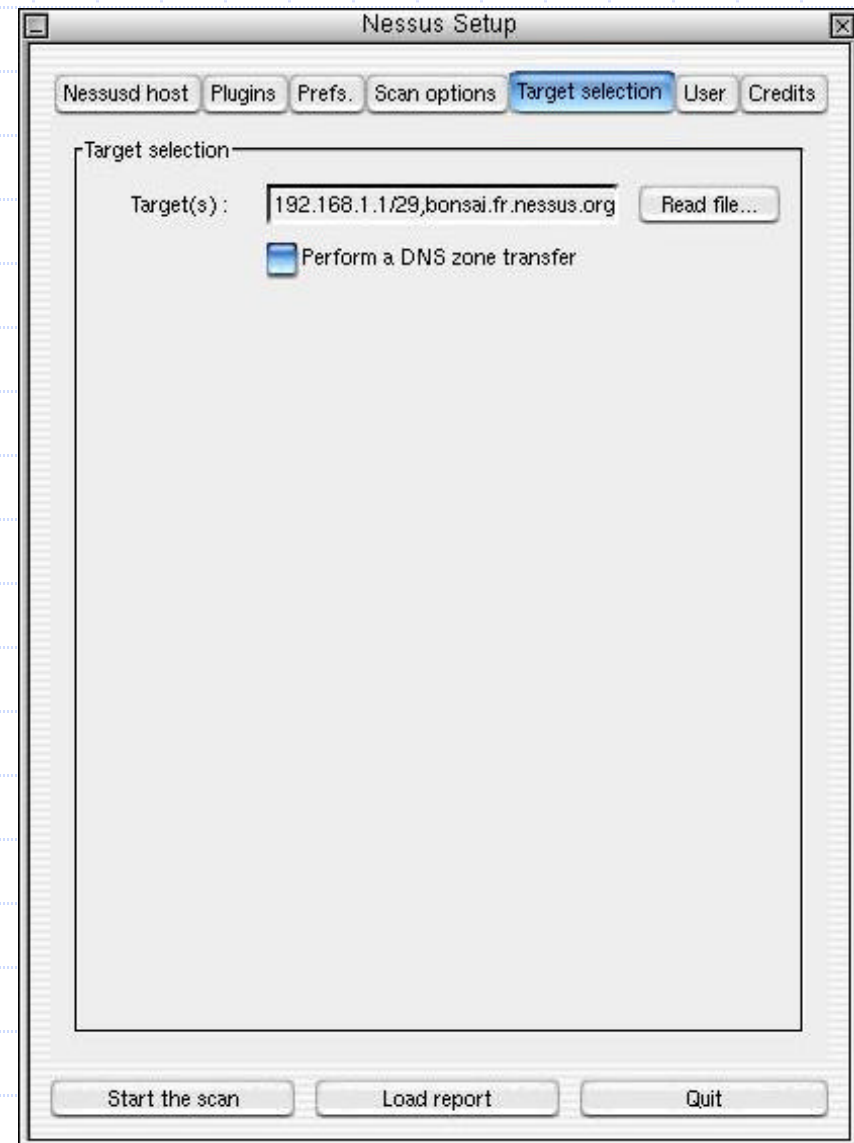
192.168.1.1/29

prof

prof.fr.nessus.org

prof, 192.168.1.1/29, ...

Any combination of the above mentioned forms separated by a comma.



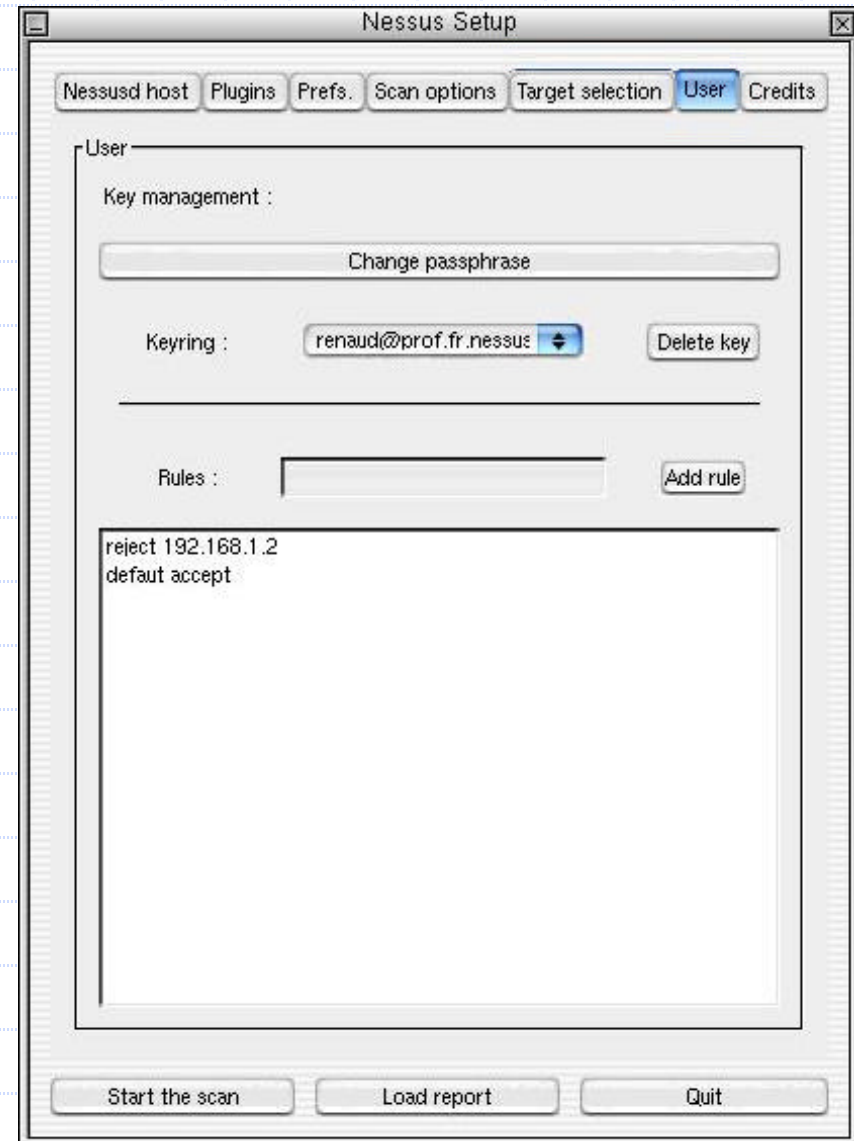
Network Management Workshop – APRICOT 2004, Malaysia

◆ Nessus rules section :

The rules allow a user to **restrict** his test.

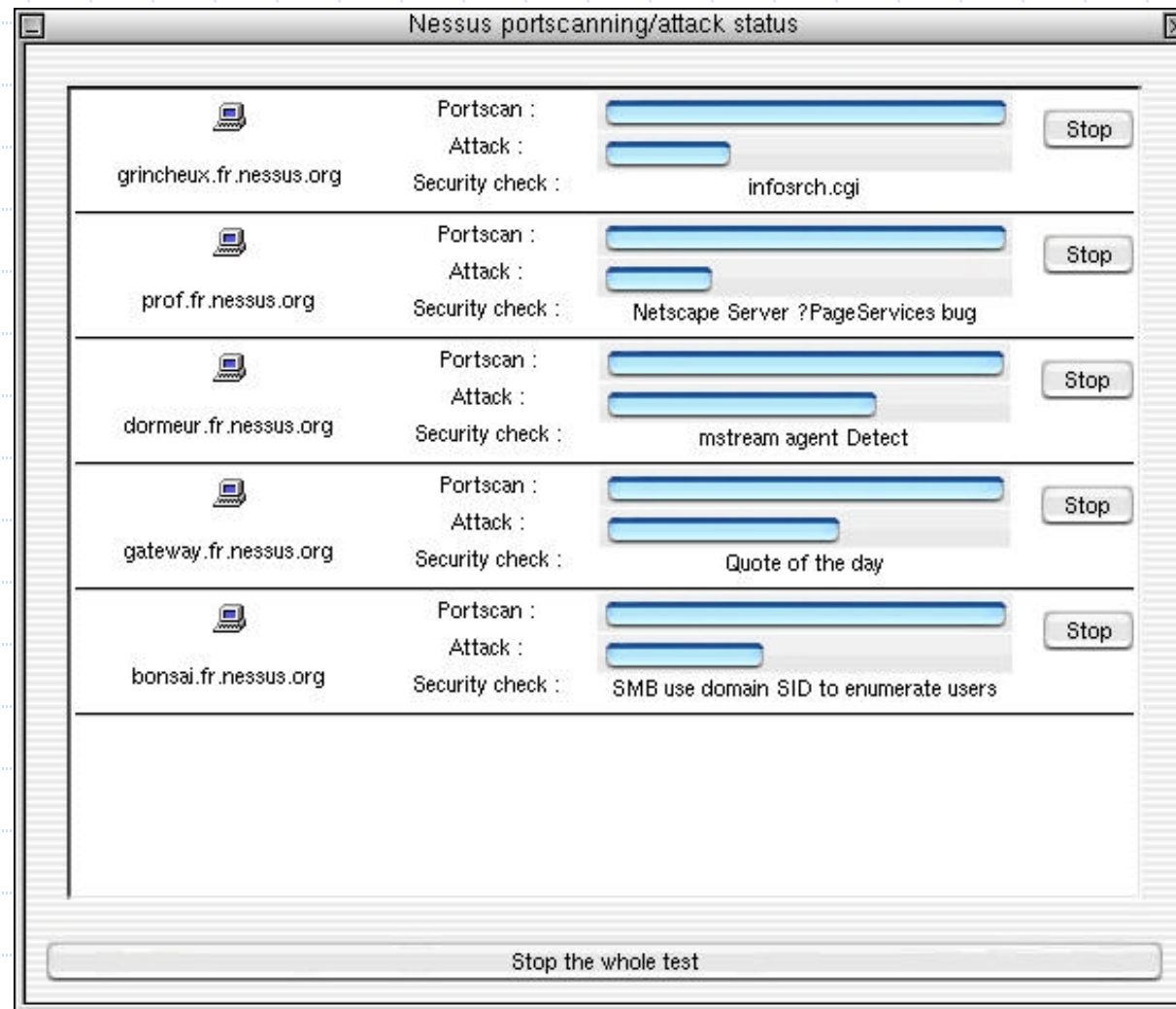
For instance, if you want to test 192.168.1.0/29, except 192.168.1.2. The rule set entered allows you to do that.

Once all of this is done,
Start the scan...



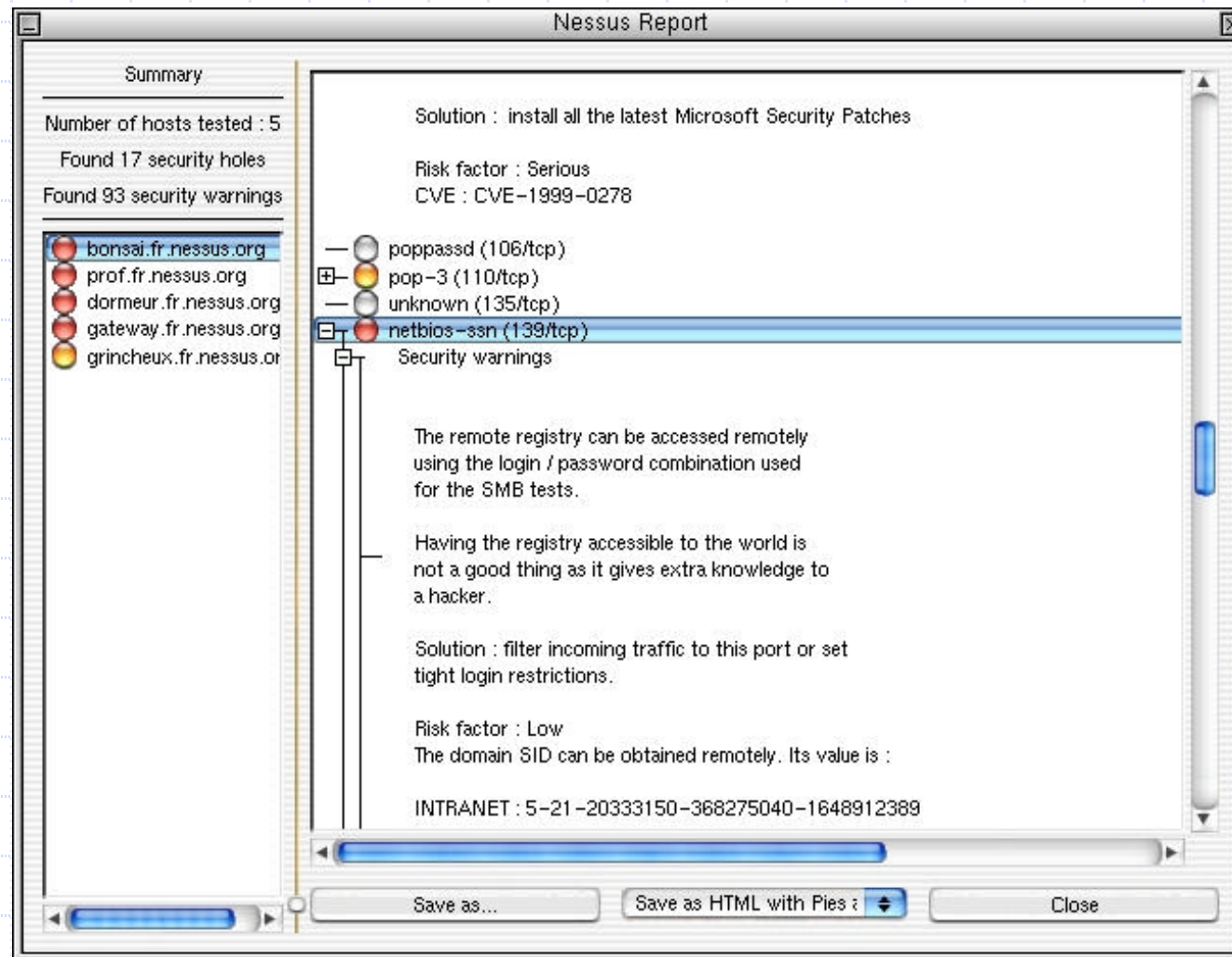
Network Management Workshop – APRICOT 2004, Malaysia

◆ Nessus scan in progress:



Network Management Workshop – APRICOT 2004, Malaysia

- ◆ Nessus report window just pops up after the scan is over:



Network Management Workshop – APRICOT 2004, Malaysia



Nessus lab

- Installation
- Configuring server
- Adding nessus users
- Configuring nessus client options
- Test scan
- Scan report