

Parte IV - Tema D

Auditoría en GNU/Linux



Auditoría de Seguridad con GNU

Introducción a una auditoria

NESSUS

Otras herramientas

Auditoría de seguridad

Tipos

☐ Caja negra

Vulnerabilidades

Profundidad

Auditoria de DoS y otras incidencias.

☐ Caja blanca

Preanálisis y requisitos

Seguridad

Otros: Calidad, confidencialidad, etc..

☐ Otras: Físicas, social, basura, etc

Auditoría de seguridad II

Audidores

“Hacking ético”

Método vs Conocimiento

Otros

Click & Destroy

Click, cut and paste

Click & Forget

Nessus

¿Qué es?

Estructura

Demonio

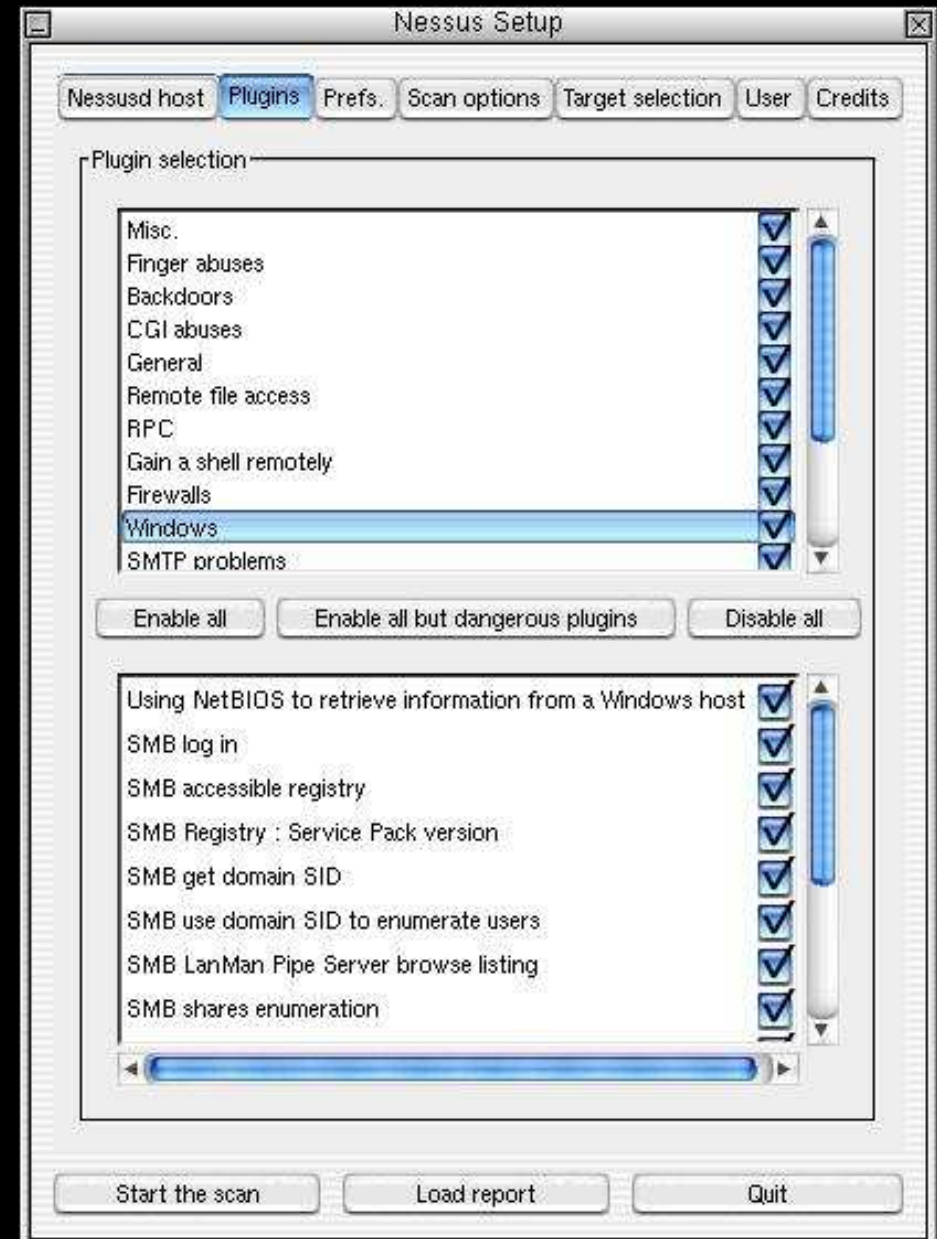
Consola

“Plugins”



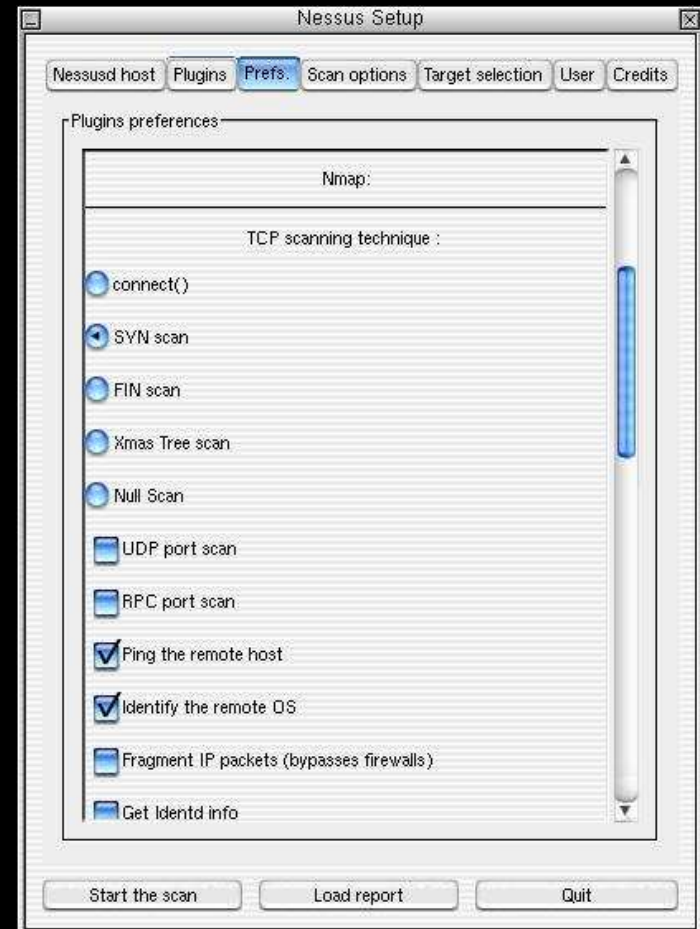
Nessus II

Políticas



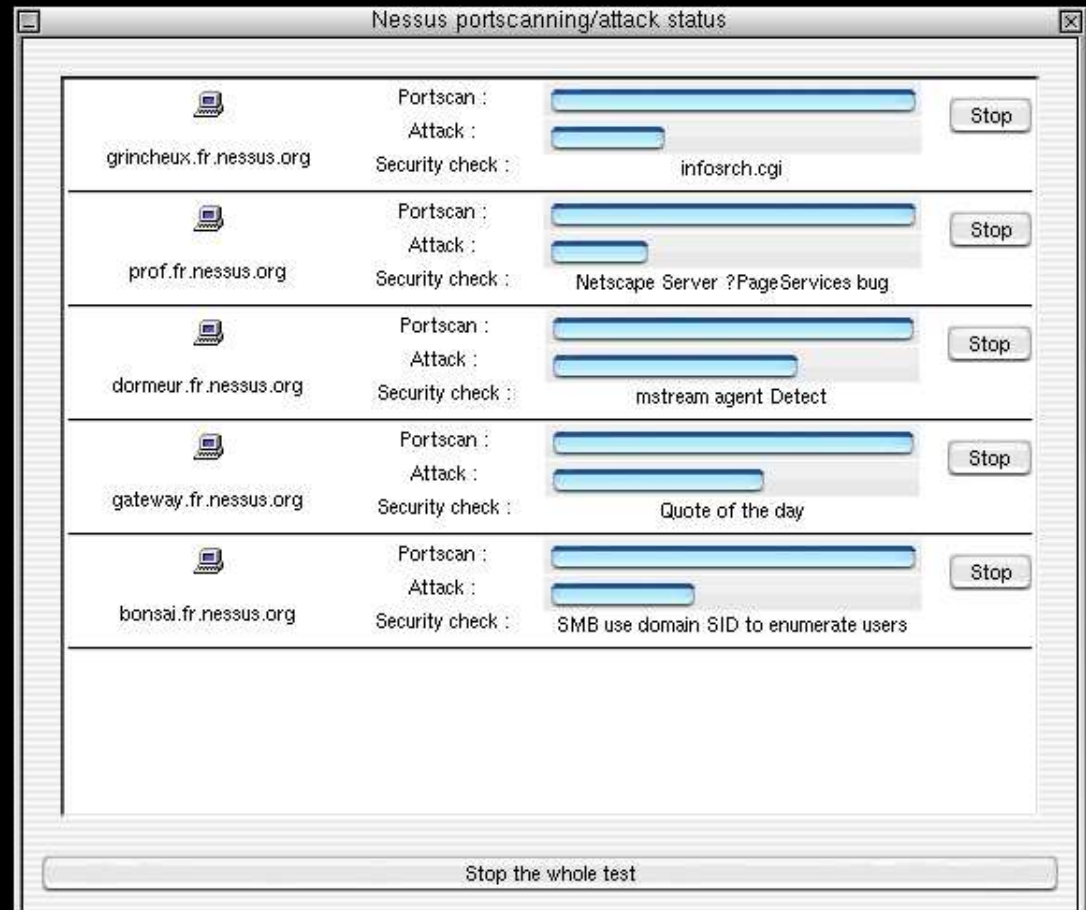
Nessus III

Scanning/NMAP



Nessus IV

“Click”



Nessus V

“and go...”

The screenshot shows the 'Nessus Report' window. On the left, a 'Summary' section indicates that 5 hosts were tested, 17 security holes were found, and 93 security warnings were identified. A list of hosts is shown, with 'bonsai.fr.nessus.org' selected. The main area displays details for a selected vulnerability: 'netbios-ssn (139/tcp)'. The solution is to 'install all the latest Microsoft Security Patches'. The risk factor is 'Serious' and the CVE is 'CVE-1999-0278'. Below this, a tree view shows 'Security warnings' expanded, with a specific warning selected: 'The remote registry can be accessed remotely using the login / password combination used for the SMB tests.' The risk factor for this warning is 'Low', and the domain SID is 'INTRANET : 5-21-20333150-368275040-1648912389'. At the bottom, there are buttons for 'Save as...', 'Save as HTML with Pies', and 'Close'.



Otras herramientas de auditoria.

Scanner de puertos

NMAP

FSCAN

Scanner de CGI's

CGIScan

Whisker

Rivat

Varios

Datapool (DoS)

SAINT, Messala, RvScan, Sara, landguard
(A.V.S)

