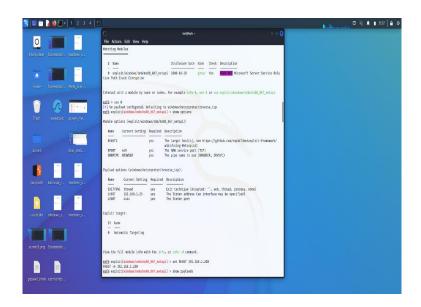


- Mettiamo in collegamento le macchine tra di loro su rete interna, ovvero KALI E WINDOWS XP rispettivamente con gli ip 192.168.1.25 e 192.168.1.200. Facciamo un ping di prova da kali verso windows.
- 2.) Tramite NESSUS facciamo una scansione delle vulnerabilità.
- 3.) Cerchiamo l'exploit per la vulnerabilità RPC, scegliamo l'unico exploit disponibile, notiamo che è previsto un payload di dafault.



4.) Settiamo l'RHOST, essendoci solo un payload di default ed è già settato, possiamo lanciare l'exploit



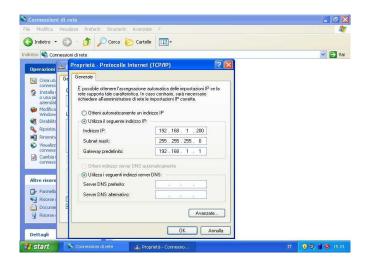
Otteniamo la shell di METERPRETER, a questo punto possiamo lanciare alcuni comandi di metepreter.



Con il comando webcam_list, vediamo che nn ci sono fotocamere connesse. IFCONFIG per recuperare alcune info.



Alcuni comandi di meterpreter



Con il comando screenshare recuperiamo un immagine del desktop del pc vittima.