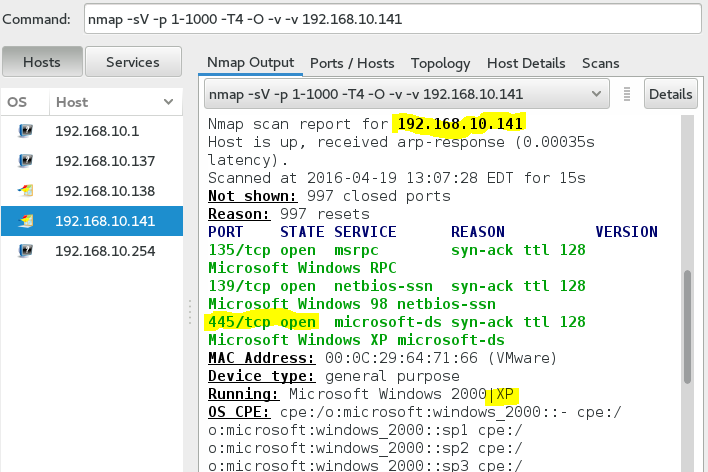
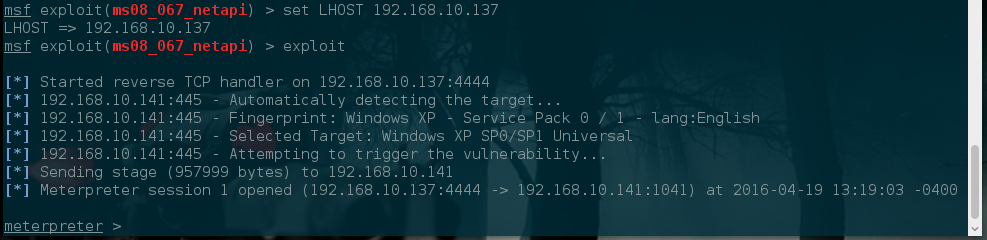
Metasploit and Meterpreter shell

By Thor Kristiansen

Zenmap result:

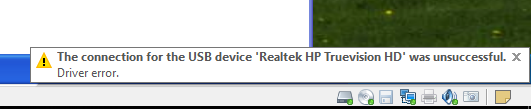


Yes, open for business. Just too easy. Now for metasploit.

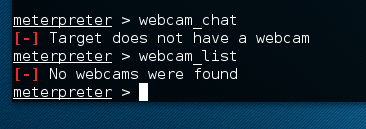


Yes! we have meterpreter reverse IP shell running. Dream hack situation. Now for post exploitation.

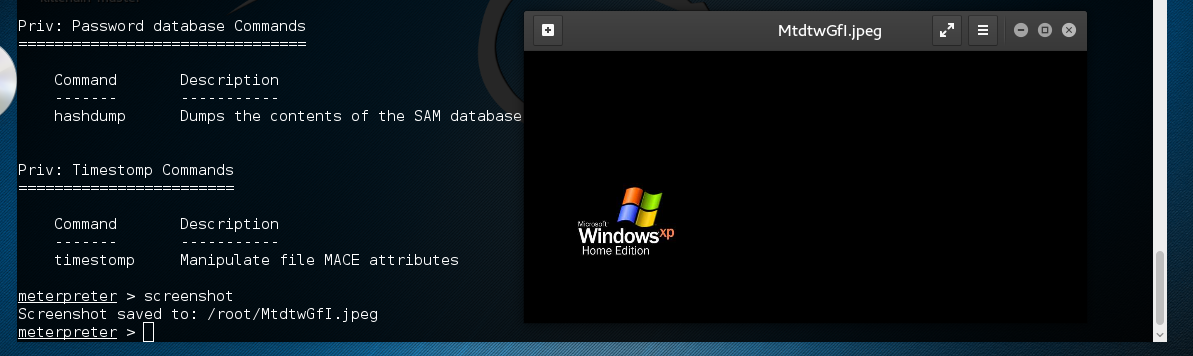
Sadly, windows xp does not support my build-in web-cam:



Of course no webcam is listed either:

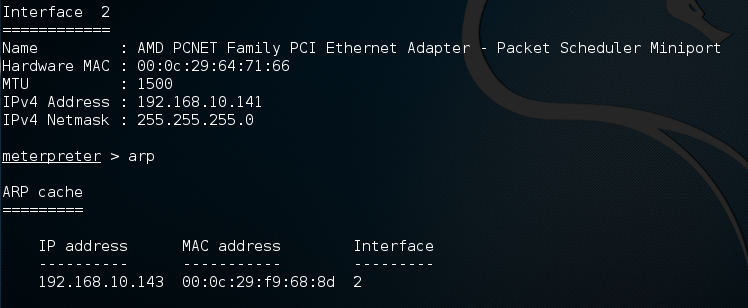


Not to worry, other stuff might be possible. Like screenshot.

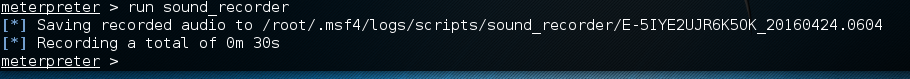


Seems screensaver is on.

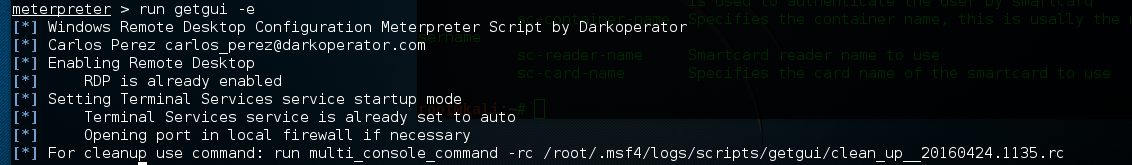
Ifconfig and arp cache dump:



Sound recorder works good:



Seems run getgui -e is different from step 19 in lab document.



And step 20 fails.