Traccia: Hacking MS08-067

Sulla base della teoria, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

Una volta ottenuta la sessione, lo studente dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows XP

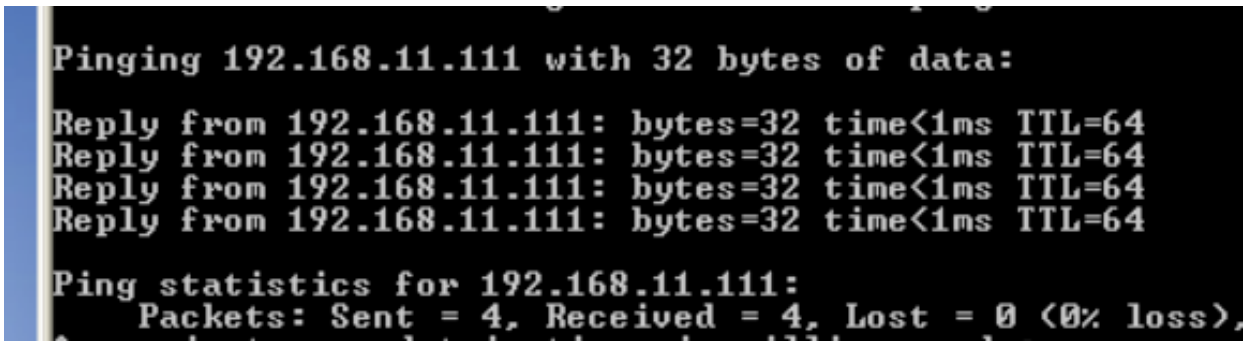
- Accedere a webcam/fare dump della tastiera/provare altro

Svolgimento:

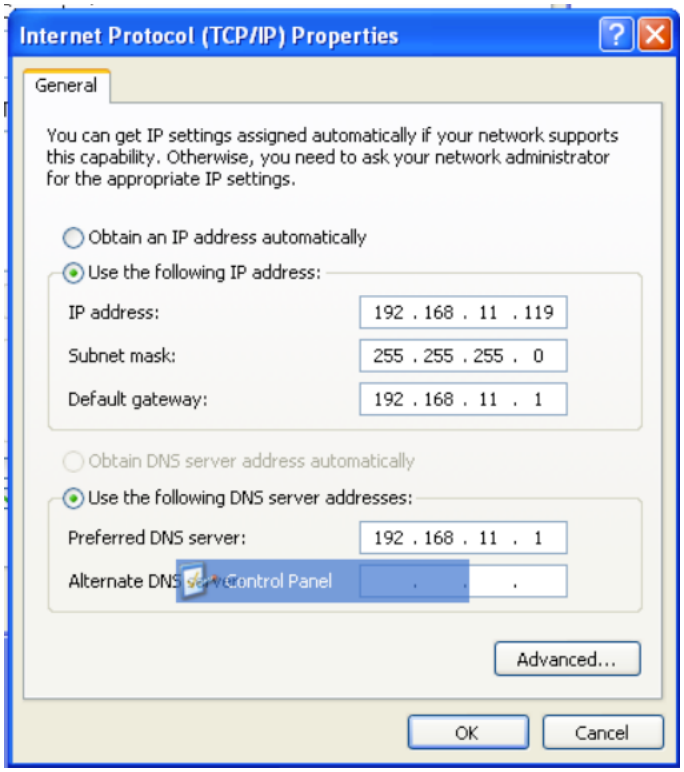
Dato che abbiamo una macchina Windows XP x64 per svolgere l'esercizio utilizziamo un exploit differente da quello della traccia ma andiamo a svolgere gli stessi task rispetto alle vulnerabilità.

L'exploit utilizzato è " exploit/windows/smb/ms17_010_psexec "

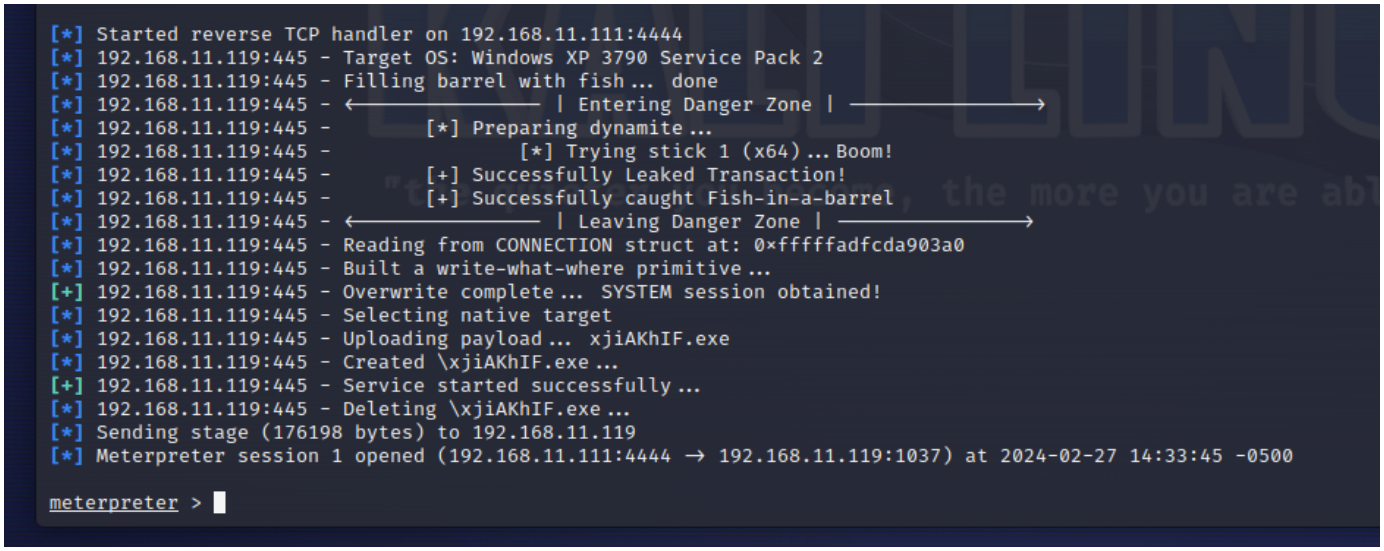
Comunicazione dalla macchina Windows verso la macchina Kali



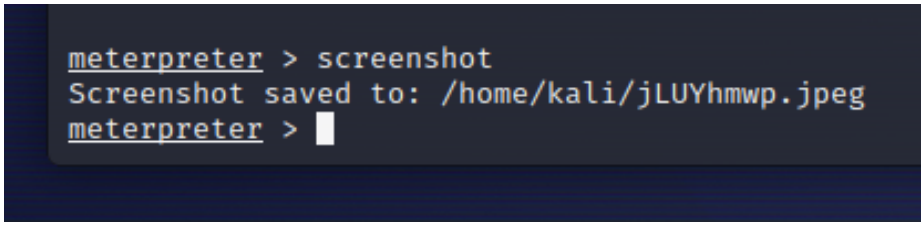
Settings delle impostazioni di rete sulla macchina Windows

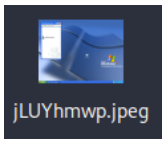


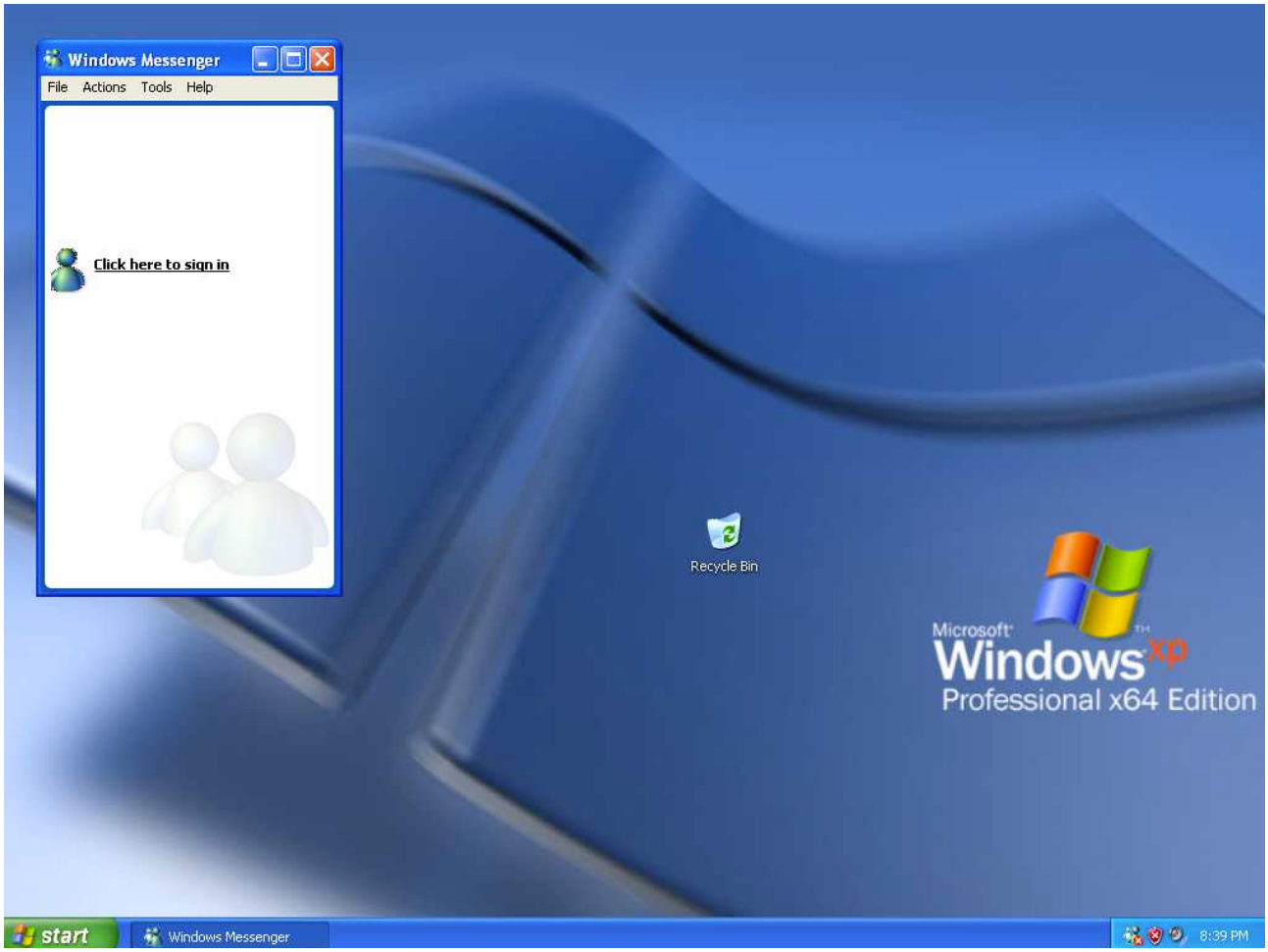
Avvio dell'exploit riportato in cima alle slide con ottenimento della sessione Meterpreter



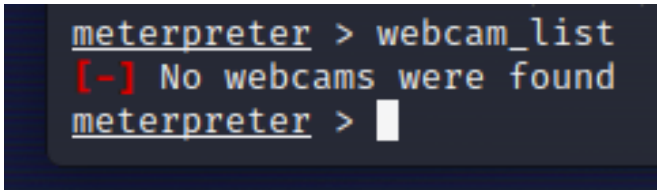
Cattura di uno screenshot







Individuazione di eventuali webcam



Dump della tasiera non eseguito in quanto l'utente Windows XP è Administrator e quindi al pari livello di SYSTEM. In questo modo non ci è consentito eseguire il migrate al processo notepade che appartiene ad Administrator.