

Oracle VM VirtualBox Manager

FileMachineHelp

NewOpenSettingsDiscardShow

kali linux

Running

metasploitable

Running

Details

General

Name:metasploitable  
Operating System:Oracle Linux (64 bit)

System

Base Memory:1506 MB  
Boot Order:Floppy, Optical, Hard Disk  
Acceleration:Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory:16 MB  
Graphics Controller:VM SVGA  
Remote Desktop Server:Disabled  
Recording:Disabled

Storage

Controller:IDE  
IDE Primary Device 0:[Optical Drive] Empty  
IDE Primary Device 1:Metasploitable.vmdk (Normal, 8.00 GB)  
Controller:SATA  
SATA Port 0:metasploitable.vdi (Normal, 8.84 GB)

Audio

Host Driver:Default  
Controller:ICH AC97

Network

Adapter 1:Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter #2')

USB

USB Controller:OHCI, EHCI  
Device Filters:0 (0 active)


Shared folders

None

Description


None

Preview



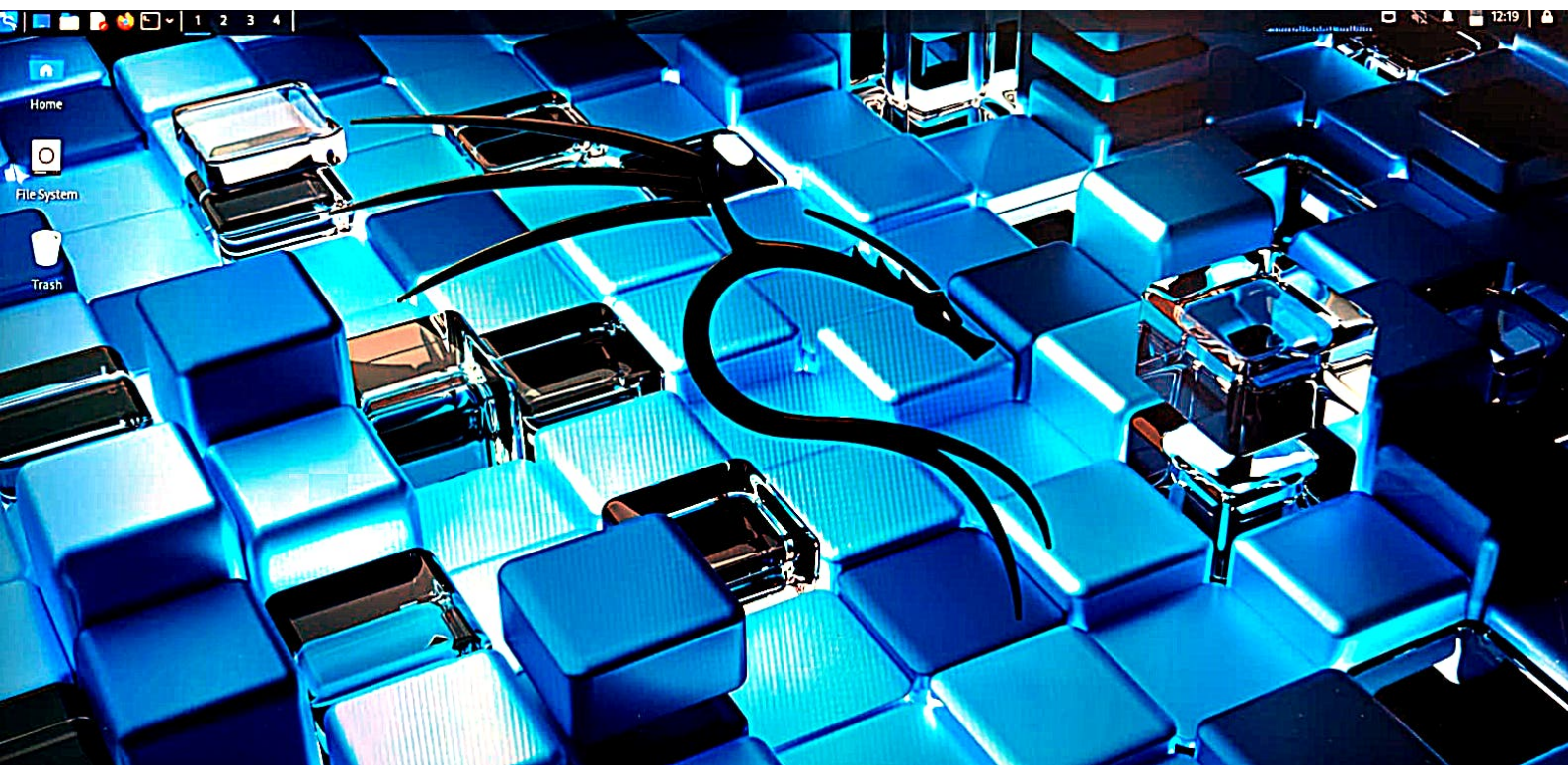
30°C  
Mostly cloudy

Search



ENG  
IN

11:51  
30-09-2025





```
1 2 3 4
Session Actions Edit View Help
(bangaram@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:b4:9d:91 brd ff:ff:ff:ff:ff:ff
    inet 192.168.121.3/24 brd 192.168.121.255 scope global dynamic noprefixroute eth0
        valid_lft 504sec preferred_lft 504sec
    inet6 fe80::a00:27ff:feb4:9d91/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(bangaram@kali)-[~]
$
```



[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](#)

Username: admin  
Security Level: high  
PHPIDS: disabled

## 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'

Contact: [msfdevlat@metasploit.com](mailto:msfdevlat@metasploit.com)

Login with msfadmin/msfadmin to get started

metasploitable login: msaadmin  
Password:

Login incorrect

metasploitable login: msfadmin  
Password:

Last login: Tue Sep 30 05:21:26 EDT 2025 on tty1

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/\*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.

To access official Ubuntu documentation, please visit:

<http://help.ubuntu.com/>

to mail,

msfadmin@metasploitable:~\$

Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
VirtualBox Host-Only Ethernet Adapter	192.168.56.1/24		Enabled
VirtualBox Host-Only Ethernet Adapter #2	192.168.121.4/24		Enabled

Adapter

DHCP Server

☒ Configure Adapter Automatically

☐ Configure Adapter Manually

IPv4 Address:

192.168.56.1

IPv4 Network Mask:

255.255.255.0

IPv6 Address:

fe80::86c4:726c:e67b:fc5d

IPv6 Prefix Length:

64

Apply

Reset



Session Actions Edit View Help

3 packets transmitted, 3 received, 0% packet loss, time 2003ms  
rtt min/avg/max/mdev = 2.182/3.804/6.758/2.091 ms

(bangaram@kali)-[~]

\$ ping -c 10 192.168.29.230

PING 192.168.29.230 (192.168.29.230) 56(84) bytes of data:  
64 bytes from 192.168.29.230: icmp\_seq=1 ttl=64 time=1.66 ms  
64 bytes from 192.168.29.230: icmp\_seq=2 ttl=64 time=1.65 ms  
64 bytes from 192.168.29.230: icmp\_seq=3 ttl=64 time=2.62 ms  
64 bytes from 192.168.29.230: icmp\_seq=4 ttl=64 time=2.02 ms  
64 bytes from 192.168.29.230: icmp\_seq=5 ttl=64 time=2.07 ms  
64 bytes from 192.168.29.230: icmp\_seq=6 ttl=64 time=2.01 ms  
64 bytes from 192.168.29.230: icmp\_seq=7 ttl=64 time=2.03 ms  
64 bytes from 192.168.29.230: icmp\_seq=8 ttl=64 time=2.49 ms  
64 bytes from 192.168.29.230: icmp\_seq=9 ttl=64 time=2.53 ms  
64 bytes from 192.168.29.230: icmp\_seq=10 ttl=64 time=2.50 ms

— 192.168.29.230 ping statistics —

10 packets transmitted, 10 received, 0% packet loss, time 9011ms  
rtt min/avg/max/mdev = 1.652/2.157/2.619/0.337 ms

(bangaram@kali)-[~]

\$ ip -4 -o addr show

1: lo inet 127.0.0.1/8 scope host lo valid\_lft forever preferred\_lf  
t forever  
2: eth0 inet 192.168.29.48/24 brd 192.168.29.255 scope global dynamic nopr  
efixroute eth0 valid\_lft 6936sec preferred\_lft 6936sec

(bangaram@kali)-[~]

\$ sudo ping -I enp0s8 -c 5 192.168.29.230

[sudo] password for bangaram:

ping: SO\_BINDTODEVICE enp0s8: No such device

(bangaram@kali)-[~]

\$ ping -c 5 -W 2 192.168.29.230

PING 192.168.29.230 (192.168.29.230) 56(84) bytes of data:  
64 bytes from 192.168.29.230: icmp\_seq=1 ttl=64 time=10.4 ms  
64 bytes from 192.168.29.230: icmp\_seq=2 ttl=64 time=1.49 ms  
64 bytes from 192.168.29.230: icmp\_seq=3 ttl=64 time=1.84 ms  
64 bytes from 192.168.29.230: icmp\_seq=4 ttl=64 time=1.31 ms  
64 bytes from 192.168.29.230: icmp\_seq=5 ttl=64 time=1.34 ms

— 192.168.29.230 ping statistics —

5 packets transmitted, 5 received, 0% packet loss, time 4006ms



Session Actions Edit View Help

64 bytes from 192.168.29.230: icmp\_seq=4 ttl=64 time=1.31 ms  
64 bytes from 192.168.29.230: icmp\_seq=5 ttl=64 time=1.34 ms

— 192.168.29.230 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4000ms  
rtt min/avg/max/mdev = 1.305/3.279/10.416/3.973 ms

(bangaram@kali)-[~]

```
$ ip -4 addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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 fq_codel state UP group default qlen 1000
    inet 192.168.29.48/24 brd 192.168.29.255 scope global dynamic noprefixroute eth0
        valid_lft 6610sec preferred_lft 6610sec
```

(bangaram@kali)-[~]

```
$ ip route
default via 192.168.29.1 dev eth0 proto dhcp src 192.168.29.48 metric 100
192.168.29.0/24 dev eth0 proto kernel scope link src 192.168.29.48 metric 100
```

(bangaram@kali)-[~]

```
$ ip neigh show
192.168.29.230 dev eth0 lladdr 08:00:27:09:df:a8 STALE
192.168.29.1 dev eth0 lladdr 04:ab:08:dc:2b:01 STALE
fe80::6ab:8ff:fedc:2b01 dev eth0 lladdr 04:ab:08:dc:2b:01 router STALE
```

(bangaram@kali)-[~]

```
$ ip -4 addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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 fq_codel state UP group default qlen 1000
    inet 192.168.29.48/24 brd 192.168.29.255 scope global dynamic noprefixroute eth0
        valid_lft 6462sec preferred_lft 6462sec
```

(bangaram@kali)-[~]

```
$ sudo nmap -Pn -sV -p 80,443,22 192.168.29.230
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-30 17:10 IST
Nmap scan report for 192.168.29.230
Host is up (0.0015s latency).
```

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------



Session Actions Edit View Help  
valid\_lft 6610sec preferred\_lft 6610sec  
(bangaram@kali)-[~]  
\$ ip route  
default via 192.168.29.1 dev eth0 proto dhcp src 192.168.29.48 metric 100  
192.168.29.0/24 dev eth0 proto kernel scope link src 192.168.29.48 metric 100

(bangaram@kali)-[~]  
\$ ip neigh show  
192.168.29.230 dev eth0 lladdr 08:00:27:69:df:a8 STALE  
192.168.29.1 dev eth0 lladdr 04:ab:08:dc:2b:01 STALE  
fe80::6ab:8ff:fedc:2b01 dev eth0 lladdr 04:ab:08:dc:2b:01 router STALE

(bangaram@kali)-[~]  
\$ ip -4 addr show  
1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
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 fq\_codel state UP group default qlen 1000  
inet 192.168.29.48/24 brd 192.168.29.255 scope global dynamic noprefixroute eth0  
valid\_lft 6462sec preferred\_lft 6462sec

(bangaram@kali)-[~]  
\$ sudo nmap -Pn -sV -p 80,443,22 192.168.29.230  
Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-09-30 17:10 IST  
Nmap scan report for 192.168.29.230  
Host is up (0.0015s latency).

PORT STATE SERVICE VERSION  
22/tcp open ssh OpenSSH 4.7p1 Debian Subuntu1 (protocol 2.0)  
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
443/tcp closed https  
MAC Address: 08:00:27:69:DF:A8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port==22&&ip.addr==192.168.29.230

No.	Time	Source	Destination	Protocol	Length	Info
5093	786.699176295	192.168.29.48	192.168.29.230	TCP	66	[TCP Keep-Alive] 35800 → 80 [ACK] Seq=334 Ack=1157 Win=63232 Len=0 TSval=2079691445 TSecr=204156
5094	786.701472422	192.168.29.230	192.168.29.48	TCP	66	[TCP Keep-Alive ACK] 80 → 35800 [ACK] Seq=1157 Ack=335 Win=6912 Len=0 TSval=205139 TSecr=2079681443
5122	791.922261812	192.168.29.230	192.168.29.48	TCP	66	80 → 35800 [FIN, ACK] Seq=1157 Ack=335 Win=6912 Len=0 TSval=205662 TSecr=2079681443
5123	791.922473610	192.168.29.48	192.168.29.230	TCP	66	35800 → 80 [FIN, ACK] Seq=335 Ack=1158 Win=63232 Len=0 TSval=2079696668 TSecr=205662
5124	791.924029669	192.168.29.230	192.168.29.48	TCP	66	80 → 35800 [ACK] Seq=1158 Ack=336 Win=6912 Len=0 TSval=205662 TSecr=2079696668
5449	849.023216380	192.168.29.48	192.168.29.230	TCP	74	54498 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2079753769 TSecr=0 WS=128
5450	849.026561285	192.168.29.230	192.168.29.48	TCP	74	22 → 54498 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=211363 TSecr=2079753769 WS=
5451	849.026585813	192.168.29.48	192.168.29.230	TCP	66	54498 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2079753772 TSecr=211363
5452	849.027439188	192.168.29.48	192.168.29.230	SSHv2	99	Client: Protocol (SSH-2.0-OpenSSH_10.0p2 Debian-8)
5453	849.028775541	192.168.29.230	192.168.29.48	TCP	66	22 → 54498 [ACK] Seq=1 Ack=34 Win=5888 Len=0 TSval=211363 TSecr=2079753773
5454	849.048221725	192.168.29.230	192.168.29.48	SSHv2	104	Server: Protocol (SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1)
5455	849.048269688	192.168.29.48	192.168.29.230	TCP	66	54498 → 22 [ACK] Seq=34 Ack=39 Win=64256 Len=0 TSval=2079753794 TSecr=211365
5456	849.049065845	192.168.29.48	192.168.29.230	SSHv2	1634	Client: Key Exchange Init
5457	849.050098759	192.168.29.230	192.168.29.48	TCP	66	22 → 54498 [ACK] Seq=39 Ack=1602 Win=8704 Len=0 TSval=211365 TSecr=2079753795
5458	849.053985403	192.168.29.230	192.168.29.48	SSHv2	850	Server: Key Exchange Init
5459	849.054506096	192.168.29.48	192.168.29.230	TCP	66	54498 → 22 [FIN, ACK] Seq=1602 Ack=823 Win=63488 Len=0 TSval=2079753800 TSecr=211365
5460	849.058538843	192.168.29.230	192.168.29.48	TCP	66	22 → 54498 [FIN, ACK] Seq=823 Ack=1603 Win=8704 Len=0 TSval=211366 TSecr=2079753800
5461	849.058564148	192.168.29.48	192.168.29.230	TCP	66	54498 → 22 [ACK] Seq=1603 Ack=824 Win=63488 Len=0 TSval=2079753804 TSecr=211366
6893	1155.5640371...	192.168.29.230	192.168.29.255	BROWSER	286	Local Master Announcement METASPLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Wo
6896	1155.5659114...	192.168.29.230	192.168.29.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum

Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0, id 0  
Ethernet II, Src: PCSSystemtec\_b4:9d:91 (08:00:27:b4:9d:91), Dst: PCSSystemtec\_69:df:a8 (08:00:27:69:df:a8)  
Internet Protocol Version 4, Src: 192.168.29.48, Dst: 192.168.29.230  
Internet Control Message Protocol

0000 08 00 27 69 df a8 08 00 27 b4 9d 91 08 00 45 00 ...1... ..E  
0010 00 54 8d 51 40 00 40 01 f0 f0 c0 a8 1d 30 c0 a8 ...T.Q0 0... ..0  
0020 1d e6 08 00 bf 6d 00 02 00 32 38 21 dd 68 00 00 ...m... ..281 h...  
0030 00 00 56 01 0e 00 00 00 00 00 10 11 12 13 14 15 ...V..... ..  
0040 18 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .....!#\$%  
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()\*+,-./012345  
0060 36 37 .....