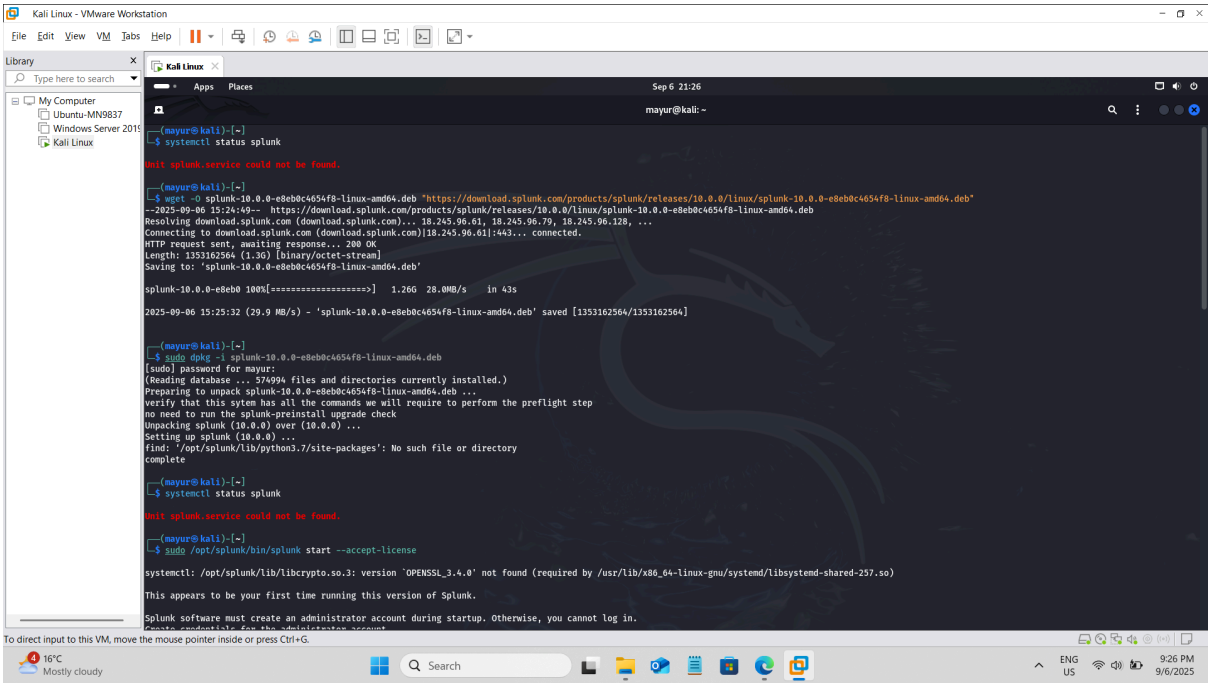
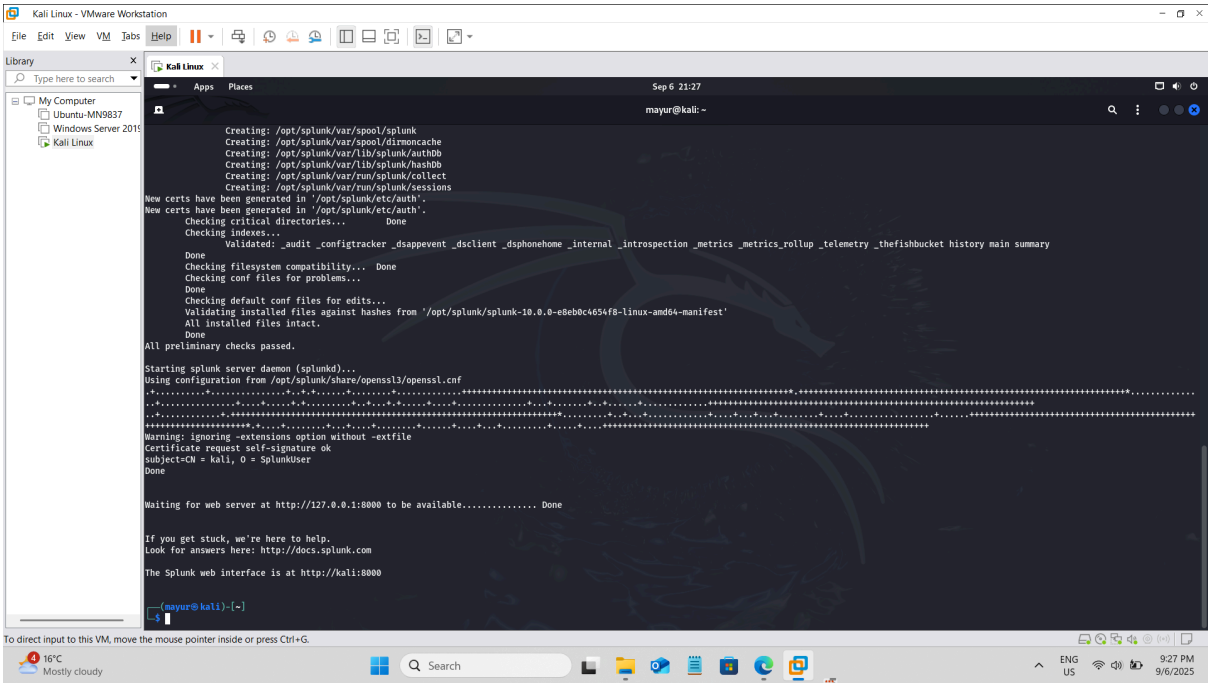
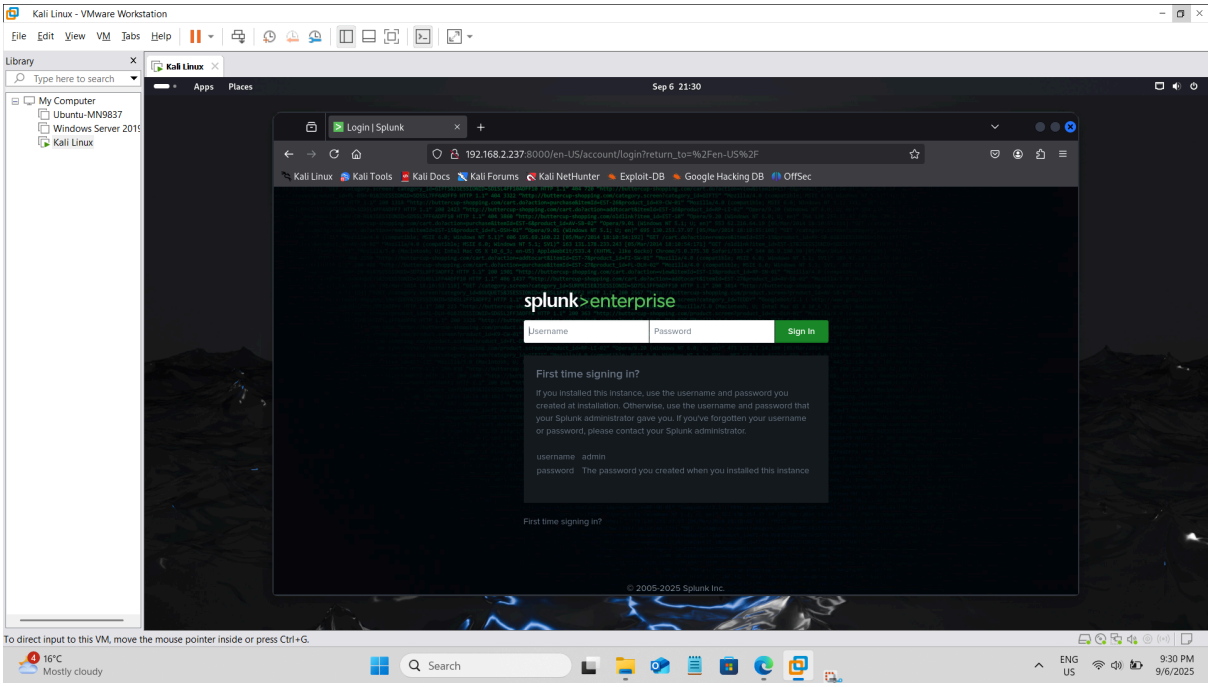
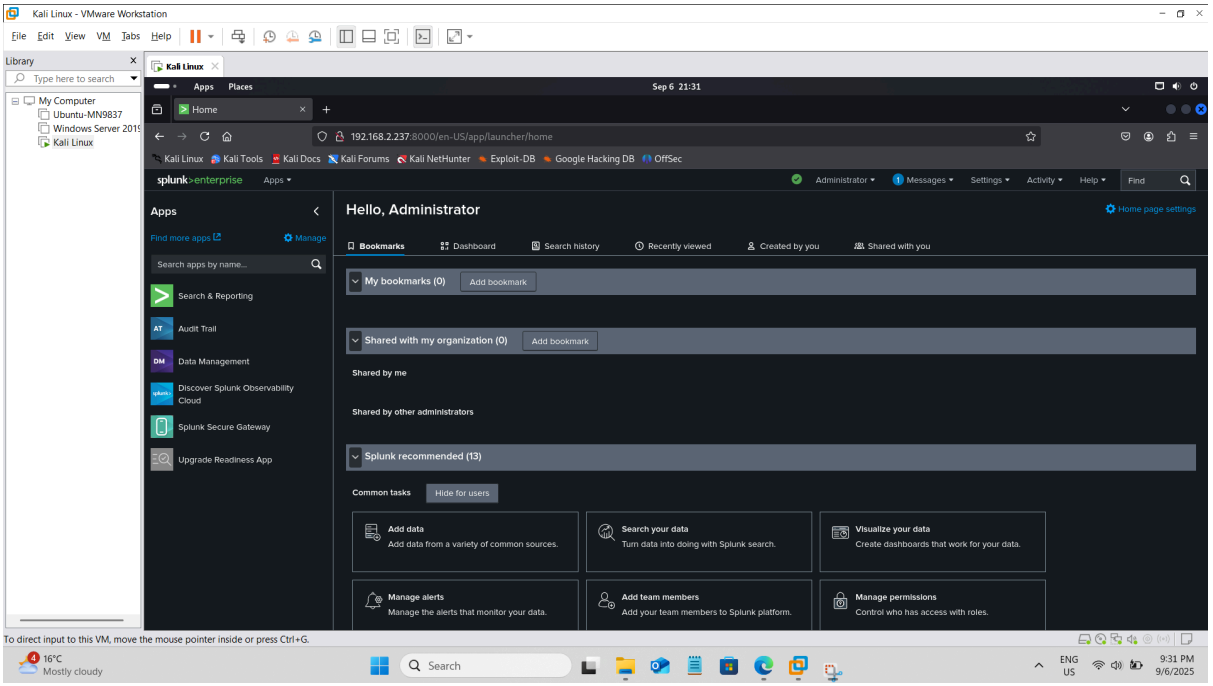
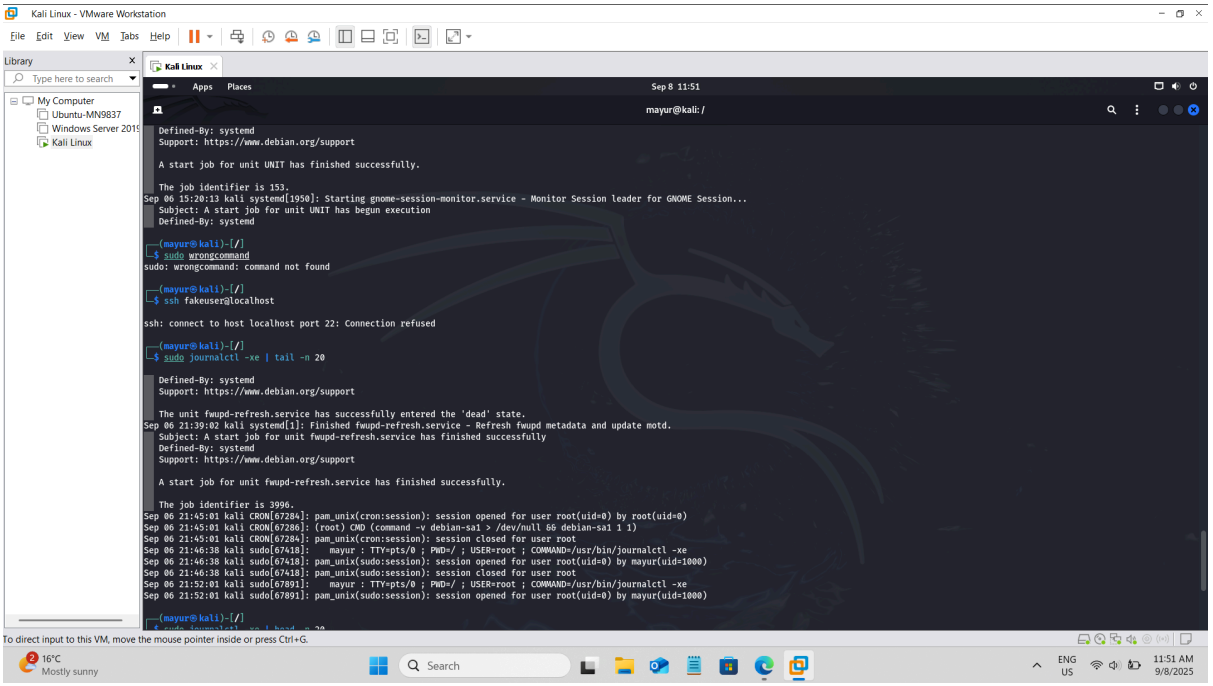
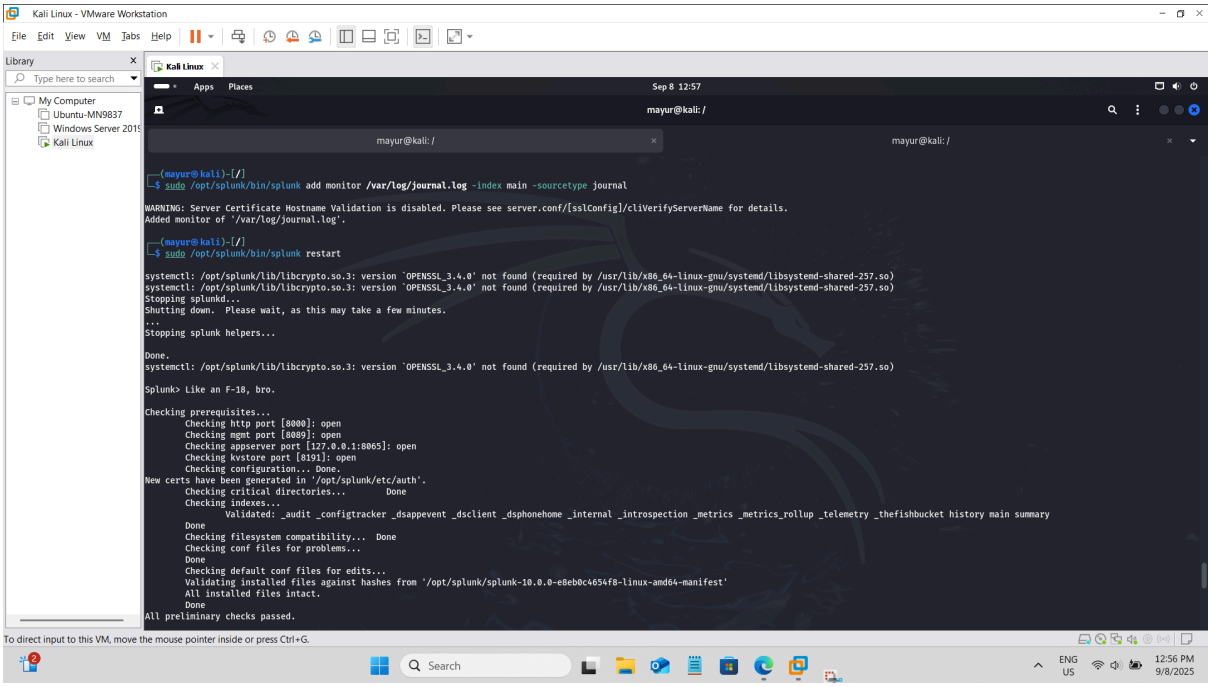

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Apps Places
Sep 6 21:26
mayur@kali: ~
┌──(mayur㉿kali)-[~]
└─$ systemctl status splunk
Unit splunk.service could not be found.
┌──(mayur㉿kali)-[~]
└─$ wget -O splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb "https://download.splunk.com/products/splunk/releases/10.0.0/linux/splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb"
--2025-09-06 15:24:49-- https://download.splunk.com/products/splunk/releases/10.0.0/linux/splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 18.245.96.61, 18.245.96.79, 18.245.96.128, ...
Connecting to download.splunk.com (download.splunk.com)|18.245.96.61|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1353162564 (1.3G) [binary/octet-stream]
Saving to: 'splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb'
splunk-10.0.0-e8eb0 100%[==========>] 1.26G 28.0MB/s in 43s
2025-09-06 15:25:32 (29.9 MB/s) - 'splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb' saved [1353162564/1353162564]
┌──(mayur㉿kali)-[~]
└─$ sudo dpkg -i splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb
[sudo] password for mayur:
(Reading database ... 574994 files and directories currently installed.)
Preparing to unpack splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb ...
verify that this sytem has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check
Unpacking splunk (10.0.0) over (10.0.0) ...
Setting up splunk (10.0.0) ...
find: '/opt/splunk/lib/python3.7/site-packages': No such file or directory
complete
┌──(mayur㉿kali)-[~]
└─$ systemctl status splunk
Unit splunk.service could not be found.
┌──(mayur㉿kali)-[~]
└─$ sudo /opt/splunk/bin/splunk start --accept-license
systemctl: /opt/splunk/lib/libcrypto.so.3: version `OPENSSL_3.4.0' not found (required by /usr/lib/x86_64-linux-gnu/systemd/libsystemd-shared-257.so)
This appears to be your first time running this version of Splunk.
Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
16°C
Mostly cloudy
Search
ENG
US
9:26 PM
9/6/2025

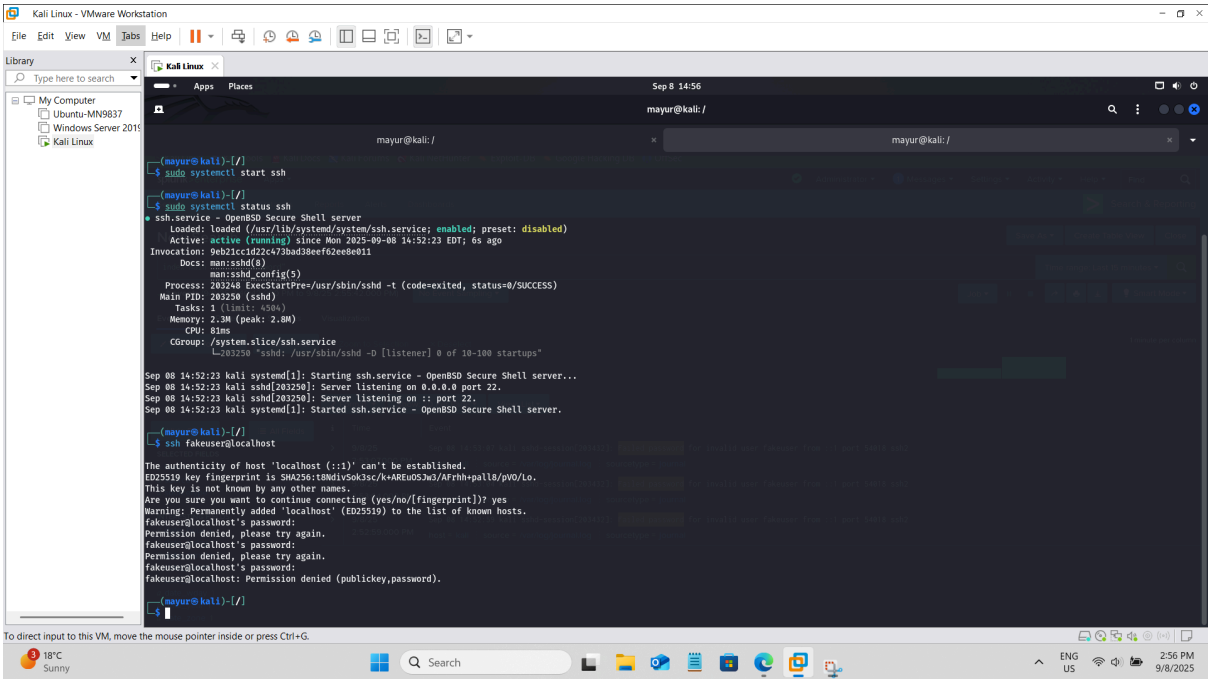

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Apps Places
Sep 6 21:27
mayur@kali: ~
Creating: /opt/splunk/var/spool/splunk
Creating: /opt/splunk/var/spool/dirmoncache
Creating: /opt/splunk/var/lib/splunk/authDb
Creating: /opt/splunk/var/lib/splunk/hashDb
Creating: /opt/splunk/var/run/splunk/collect
Creating: /opt/splunk/var/run/splunk/sessions
New certs have been generated in '/opt/splunk/etc/auth'.
New certs have been generated in '/opt/splunk/etc/auth'.
Checking critical directories... Done
Checking indexes...
Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
Done
Checking filesystem compatibility... Done
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunk/splunk-10.0.0-e8eb0c4654f8-linux-amd64-manifest'
All installed files intact.
Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
Using configuration from /opt/splunk/share/openssl3/openssl.cnf
Warning: ignoring -extensions option without -extfile
Certificate request self-signature ok
subject=CN = kali, O = SplunkUser
Done
Waiting for web server at http://127.0.0.1:8000 to be available..... Done
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com
The Splunk web interface is at http://kali:8000
┌──(mayur㉿kali)-[~]
└─$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
16°C
Mostly cloudy
Search
ENG
US
9:27 PM
9/6/2025

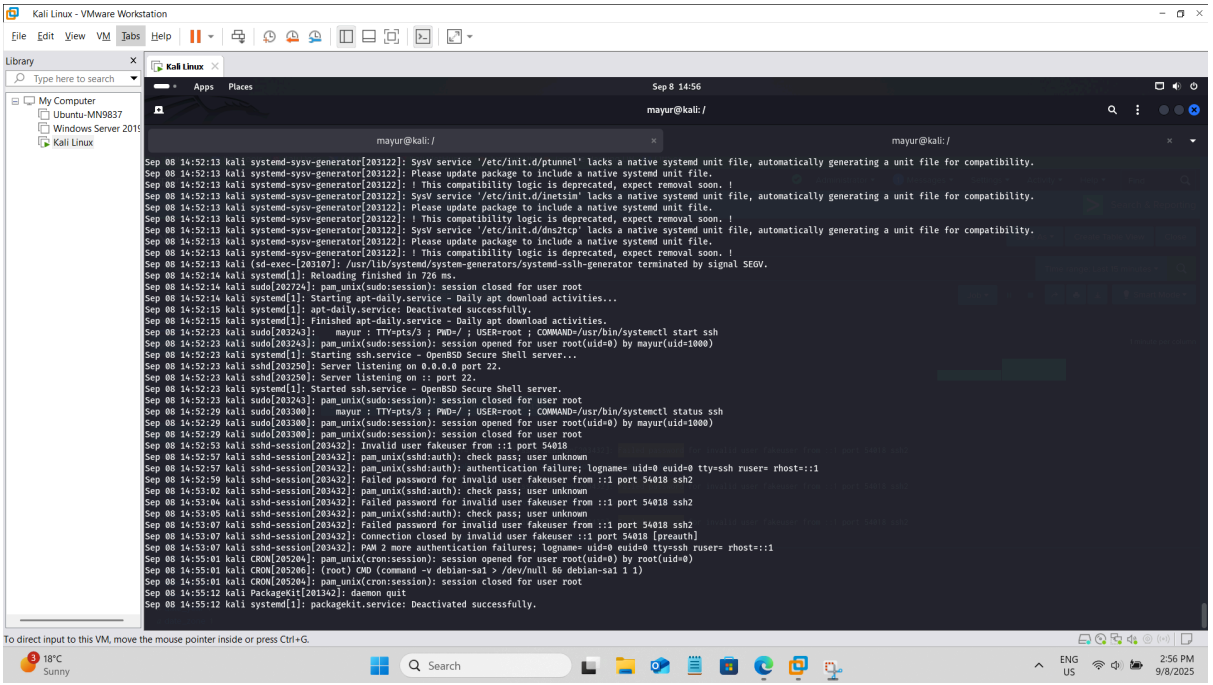

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Apps Places
Sep 6 21:30
Login | Splunk
192.168.2.237:8000/en-US/account/login?return_to=%2Fen-US%2F
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
splunk>enterprise
Username
Password
Sign In
First time signing in?
If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.
username admin
password The password you created when you installed this instance
First time signing in?
© 2005-2025 Splunk Inc.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
16°C
Mostly cloudy
Search
ENG
US
9:30 PM
9/6/2025

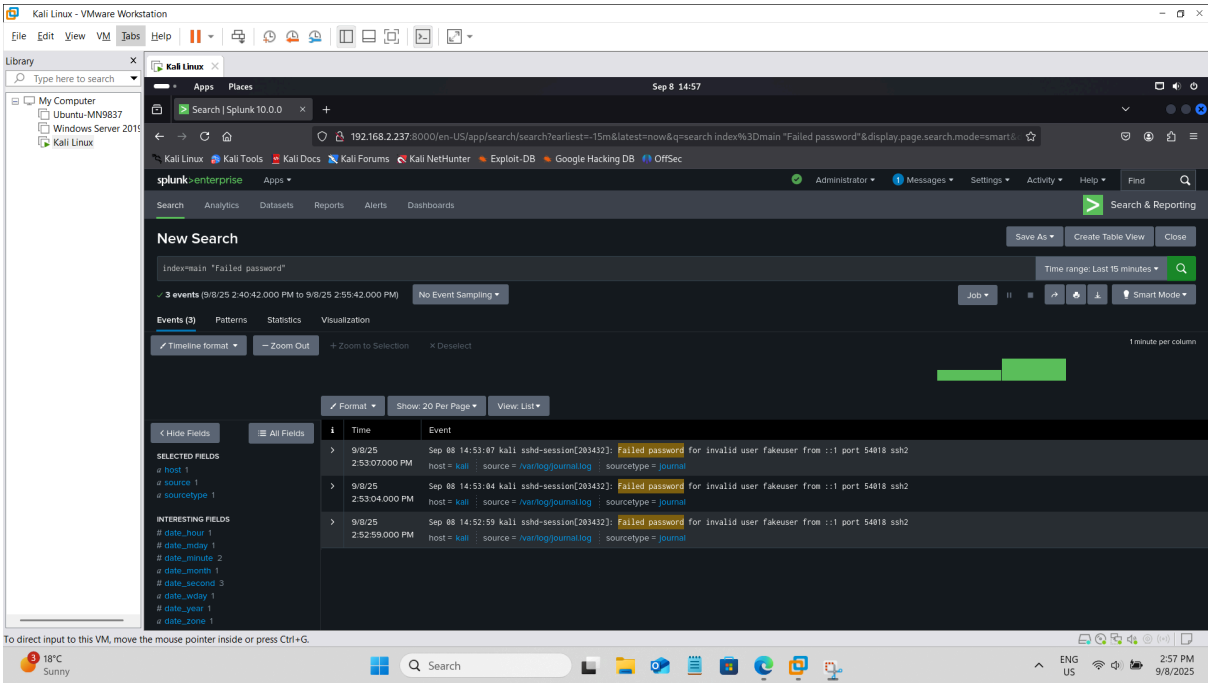

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Apps Places
Sep 6 21:31
Home
192.168.2.237:8000/en-US/app/launcher/home
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Find more apps
Manage
Search apps by name...
Search & Reporting
Audit Trail
Data Management
Discover Splunk Observability Cloud
Splunk Secure Gateway
Upgrade Readiness App
Hello, Administrator
Home page settings
Bookmarks
Dashboard
Search history
Recently viewed
Created by you
Shared with you
My bookmarks (0)
Add bookmark
Shared with my organization (0)
Add bookmark
Shared by me
Shared by other administrators
Splunk recommended (13)
Common tasks
Hide for users
Add data
Add data from a variety of common sources.
Search your data
Turn data into doing with Splunk search.
Visualize your data
Create dashboards that work for your data.
Manage alerts
Manage the alerts that monitor your data.
Add team members
Add your team members to Splunk platform.
Manage permissions
Control who has access with roles.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
16°C
Mostly cloudy
Search
ENG
US
9:31 PM
9/6/2025

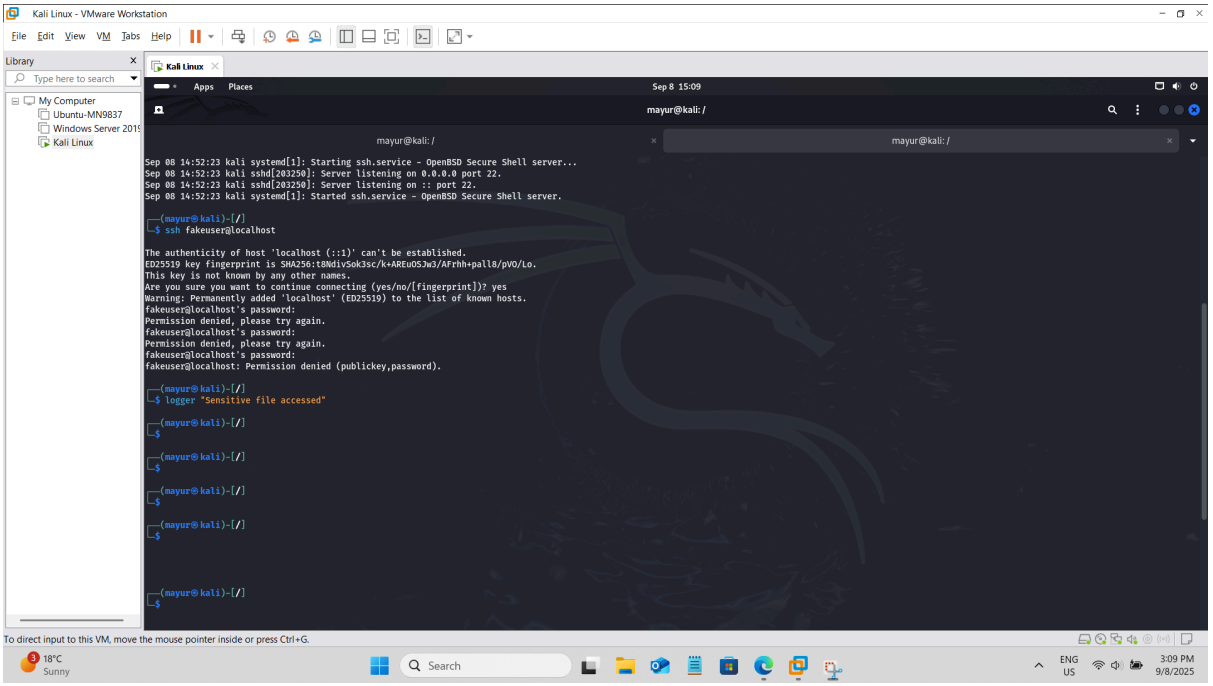

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Apps Places
Sep 8 11:51
mayur@kali: /
Defined-By: systemd
Support: https://www.debian.org/support
A start job for unit UNIT has finished successfully.
The job identifier is 153.
Sep 06 15:20:13 kali systemd[1950]: Starting gnome-session-monitor.service - Monitor Session leader for GNOME Session...
Subject: A start job for unit UNIT has begun execution
Defined-By: systemd
┌──(mayur㉿kali)-[/]
└─$ sudo wrongcommand
sudo: wrongcommand: command not found
┌──(mayur㉿kali)-[/]
└─$ ssh fakeuser@localhost
ssh: connect to host localhost port 22: Connection refused
┌──(mayur㉿kali)-[/]
└─$ sudo journalctl -xe | tail -n 20
Defined-By: systemd
Support: https://www.debian.org/support
The unit fwupd-refresh.service has successfully entered the 'dead' state.
Sep 06 21:39:02 kali systemd[1]: Finished fwupd-refresh.service - Refresh fwupd metadata and update motd.
Subject: A start job for unit fwupd-refresh.service has finished successfully
Defined-By: systemd
Support: https://www.debian.org/support
A start job for unit fwupd-refresh.service has finished successfully.
The job identifier is 3996.
Sep 06 21:45:01 kali CRON[67284]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Sep 06 21:45:01 kali CRON[67286]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Sep 06 21:45:01 kali CRON[67284]: pam_unix(cron:session): session closed for user root
Sep 06 21:46:38 kali sudo[67418]: mayur : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/journalctl -xe
Sep 06 21:46:38 kali sudo[67418]: pam_unix(sudo:session): session opened for user root(uid=0) by mayur(uid=1000)
Sep 06 21:46:38 kali sudo[67418]: pam_unix(sudo:session): session closed for user root
Sep 06 21:52:01 kali sudo[67891]: mayur : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/journalctl -xe
Sep 06 21:52:01 kali sudo[67891]: pam_unix(sudo:session): session opened for user root(uid=0) by mayur(uid=1000)
┌──(mayur㉿kali)-[/]
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
16°C
Mostly sunny
Search
ENG
US
11:51 AM
9/8/2025

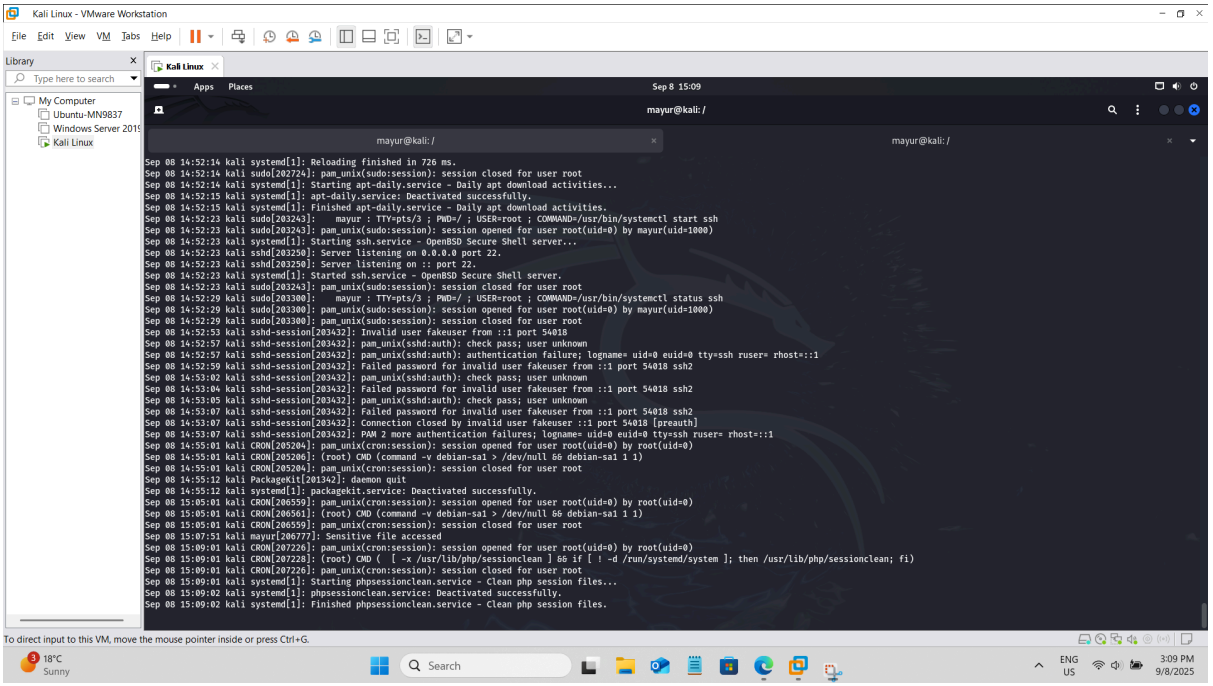

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Apps Places
Sep 8 12:57
mayur@kali: /
mayur@kali: /
mayur@kali: /
┌──(mayur㉿kali)-[/]
└─$ sudo /opt/splunk/bin/splunk add monitor /var/log/journal.log -index main -sourcetype journal
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Added monitor of '/var/log/journal.log'.
┌──(mayur㉿kali)-[/]
└─$ sudo /opt/splunk/bin/splunk restart
systemctl: /opt/splunk/lib/libcrypto.so.3: version `OPENSSL_3.4.0' not found (required by /usr/lib/x86_64-linux-gnu/systemd/libsystemd-shared-257.so)
systemctl: /opt/splunk/lib/libcrypto.so.3: version `OPENSSL_3.4.0' not found (required by /usr/lib/x86_64-linux-gnu/systemd/libsystemd-shared-257.so)
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.
...
Stopping splunk helpers...
Done.
systemctl: /opt/splunk/lib/libcrypto.so.3: version `OPENSSL_3.4.0' not found (required by /usr/lib/x86_64-linux-gnu/systemd/libsystemd-shared-257.so)
Splunk> Like an F-18, bro.
Checking prerequisites...
Checking http port [8000]: open
Checking mgmt port [8089]: open
Checking appserver port [127.0.0.1:8065]: open
Checking kvstore port [8191]: open
Checking configuration... Done.
New certs have been generated in '/opt/splunk/etc/auth'.
Checking critical directories... Done
Checking indexes...
Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
Done
Checking filesystem compatibility... Done
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunk/splunk-10.0.0-e8eb0c4654f8-linux-amd64-manifest'
All installed files intact.
Done
All preliminary checks passed.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
ENG
US
12:56 PM
9/8/2025

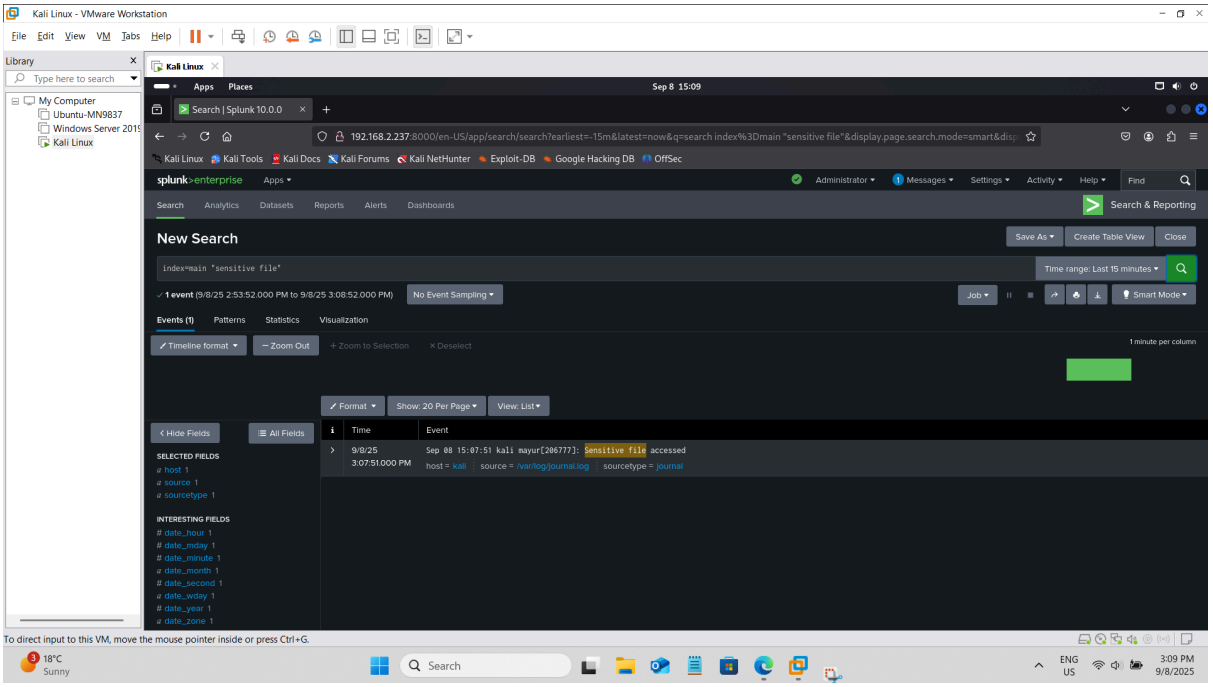

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Apps Places
Sep 8 14:56
mayur@kali: /
mayur@kali: /
mayur@kali: /
(mayur㉿kali)-[/]
$ sudo systemctl start ssh
(mayur㉿kali)-[/]
$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
Active: active (running) since Mon 2025-09-08 14:52:23 EDT; 6s ago
Invocation: 9eb21cc1d22c473bad38eef62ee8e011
Docs: man:sshd(8)
man:sshd_config(5)
Process: 203248 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
Main PID: 203250 (sshd)
Tasks: 1 (limit: 4504)
Memory: 2.3M (peak: 2.8M)
CPU: 81ms
CGroup: /system.slice/ssh.service
└─203250 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
Sep 08 14:52:23 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Sep 08 14:52:23 kali sshd[203250]: Server listening on 0.0.0.0 port 22.
Sep 08 14:52:23 kali sshd[203250]: Server listening on :: port 22.
Sep 08 14:52:23 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
(mayur㉿kali)-[/]
$ ssh fakeuser@localhost
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:t8NdivSok3sc/k+AREuOSJw3/AFrhh+pall8/pVO/Lo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
fakeuser@localhost's password:
Permission denied, please try again.
fakeuser@localhost's password:
Permission denied, please try again.
fakeuser@localhost's password:
fakeuser@localhost: Permission denied (publickey,password).
(mayur㉿kali)-[/]
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
18°C
Sunny
Search
ENG
US
2:56 PM
9/8/2025

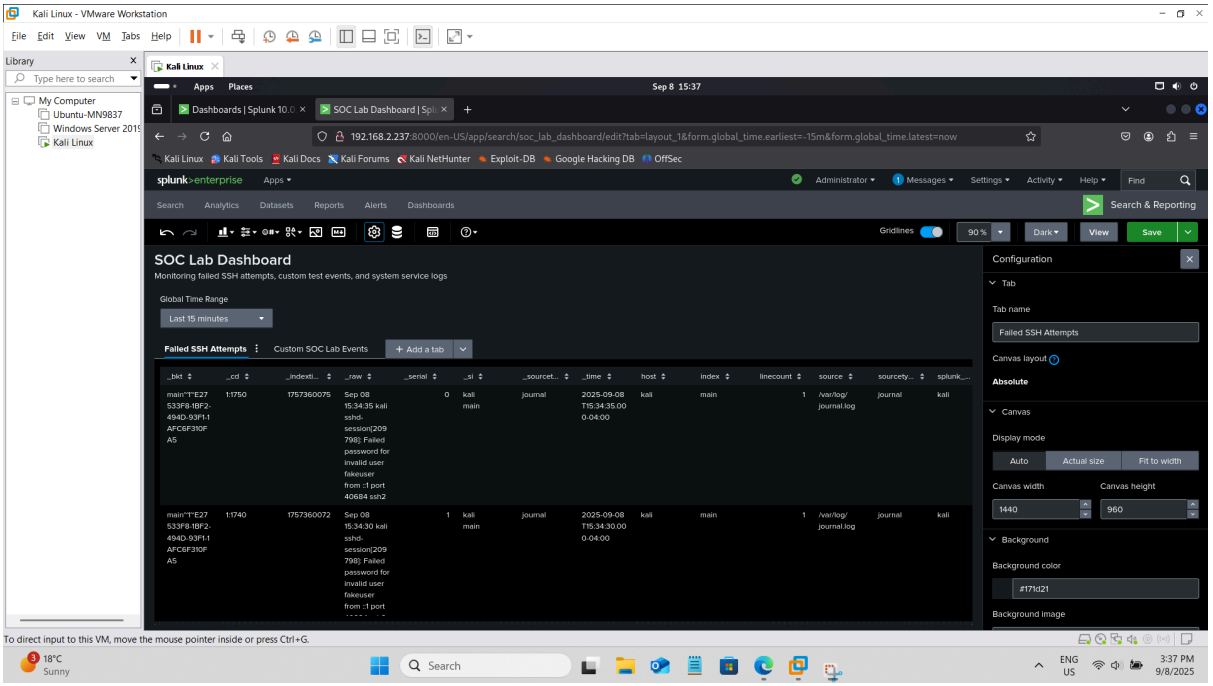

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Apps Places
Sep 8 14:56
mayur@kali: /
mayur@kali: /
mayur@kali: /
Sep 08 14:52:13 kali systemd-sysv-generator[203122]: SysV service '/etc/init.d/ptunnel' lacks a native systemd unit file, automatically generating a unit file for compatibility.
Sep 08 14:52:13 kali systemd-sysv-generator[203122]: Please update package to include a native systemd unit file.
Sep 08 14:52:13 kali systemd-sysv-generator[203122]: ! This compatibility logic is deprecated, expect removal soon. !
Sep 08 14:52:13 kali systemd-sysv-generator[203122]: SysV service '/etc/init.d/inetsim' lacks a native systemd unit file, automatically generating a unit file for compatibility.
Sep 08 14:52:13 kali systemd-sysv-generator[203122]: Please update package to include a native systemd unit file.
Sep 08 14:52:13 kali systemd-sysv-generator[203122]: ! This compatibility logic is deprecated, expect removal soon. !
Sep 08 14:52:13 kali systemd-sysv-generator[203122]: SysV service '/etc/init.d/dns2tcp' lacks a native systemd unit file, automatically generating a unit file for compatibility.
Sep 08 14:52:13 kali systemd-sysv-generator[203122]: Please update package to include a native systemd unit file.
Sep 08 14:52:13 kali systemd-sysv-generator[203122]: ! This compatibility logic is deprecated, expect removal soon. !
Sep 08 14:52:13 kali (sd-exec-[203107]: /usr/lib/systemd/system-generators/systemd-sslh-generator terminated by signal SEGV.
Sep 08 14:52:14 kali systemd[1]: Reloading finished in 726 ms.
Sep 08 14:52:14 kali sudo[202724]: pam_unix(sudo:session): session closed for user root
Sep 08 14:52:14 kali systemd[1]: Starting apt-daily.service - Daily apt download activities...
Sep 08 14:52:15 kali systemd[1]: apt-daily.service: Deactivated successfully.
Sep 08 14:52:15 kali systemd[1]: Finished apt-daily.service - Daily apt download activities.
Sep 08 14:52:23 kali sudo[203243]: mayur : TTY=pts/3 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/systemctl start ssh
Sep 08 14:52:23 kali sudo[203243]: pam_unix(sudo:session): session opened for user root(uid=0) by mayur(uid=1000)
Sep 08 14:52:23 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Sep 08 14:52:23 kali sshd[203250]: Server listening on 0.0.0.0 port 22.
Sep 08 14:52:23 kali sshd[203250]: Server listening on :: port 22.
Sep 08 14:52:23 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Sep 08 14:52:23 kali sudo[203243]: pam_unix(sudo:session): session closed for user root
Sep 08 14:52:29 kali sudo[203300]: mayur : TTY=pts/3 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/systemctl status ssh
Sep 08 14:52:29 kali sudo[203300]: pam_unix(sudo:session): session opened for user root(uid=0) by mayur(uid=1000)
Sep 08 14:52:29 kali sudo[203300]: pam_unix(sudo:session): session closed for user root
Sep 08 14:52:53 kali sshd-session[203432]: Invalid user fakeuser from ::1 port 54018
Sep 08 14:52:57 kali sshd-session[203432]: pam_unix(sshd:auth): check pass; user unknown
Sep 08 14:52:57 kali sshd-session[203432]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=::1
Sep 08 14:52:59 kali sshd-session[203432]: Failed password for invalid user fakeuser from ::1 port 54018 ssh2
Sep 08 14:53:02 kali sshd-session[203432]: pam_unix(sshd:auth): check pass; user unknown
Sep 08 14:53:04 kali sshd-session[203432]: Failed password for invalid user fakeuser from ::1 port 54018 ssh2
Sep 08 14:53:05 kali sshd-session[203432]: pam_unix(sshd:auth): check pass; user unknown
Sep 08 14:53:07 kali sshd-session[203432]: Failed password for invalid user fakeuser from ::1 port 54018 ssh2
Sep 08 14:53:07 kali sshd-session[203432]: Connection closed by invalid user fakeuser ::1 port 54018 [preauth]
Sep 08 14:53:07 kali sshd-session[203432]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=::1
Sep 08 14:55:01 kali CRON[205204]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Sep 08 14:55:01 kali CRON[205206]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Sep 08 14:55:01 kali CRON[205204]: pam_unix(cron:session): session closed for user root
Sep 08 14:55:12 kali PackageKit[201342]: daemon quit
Sep 08 14:55:12 kali systemd[1]: packagekit.service: Deactivated successfully.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
18°C
Sunny
Search
ENG
US
2:56 PM
9/8/2025

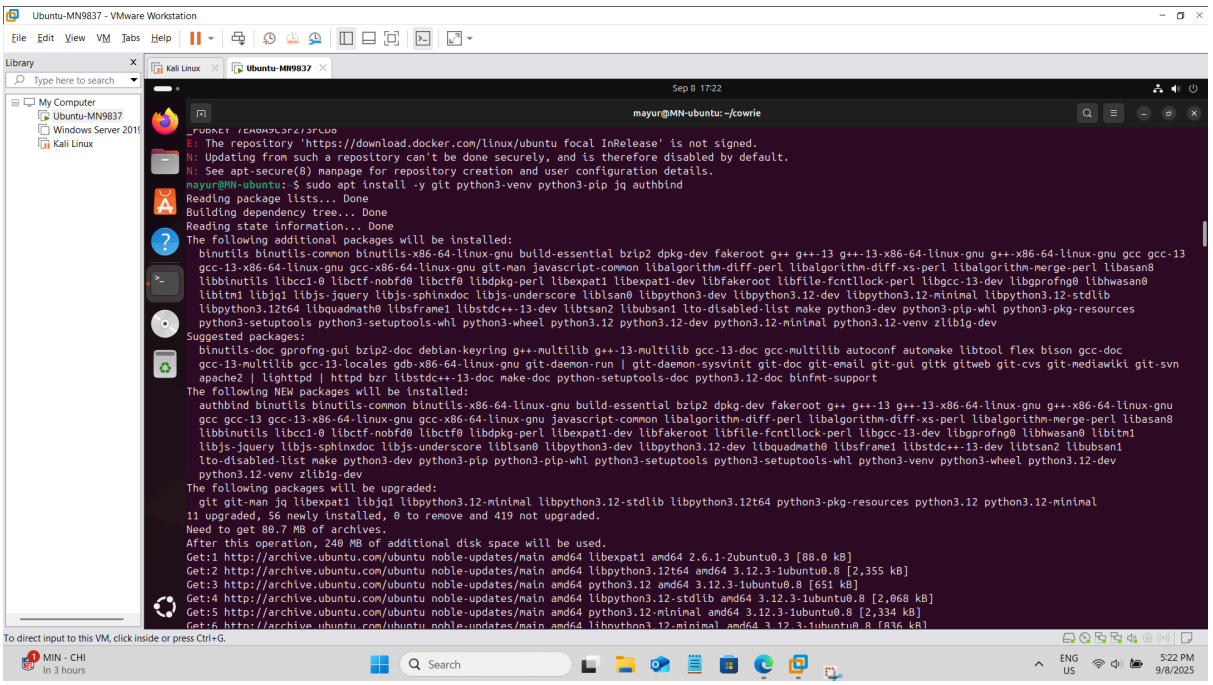

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Apps Places
Sep 8 14:57
Search | Splunk 10.0.0
192.168.2.237:8000/en-US/app/search/search?earliest=-15m&latest=now&q=search index%3Dmain "Failed password"&display.page.search.mode=smart&
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
splunk>enterprise Apps
Administrator Messages Settings Activity Help Find
Search Analytics Datasets Reports Alerts Dashboards
Search & Reporting
New Search
Save As Create Table View Close
index=main "Failed password"
Time range: Last 15 minutes
3 events (9/8/25 2:40:42.000 PM to 9/8/25 2:55:42.000 PM)
No Event Sampling
Job Smart Mode
Events (3) Patterns Statistics Visualization
Timeline format Zoom Out Zoom to Selection Deselect
1 minute per column
Format Show: 20 Per Page View: List
Hide Fields All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 2
date_month 1
date_second 3
date_wday 1
date_year 1
date_zone 1
Time Event
9/8/25 2:53:07.000 PM
Sep 08 14:53:07 kali sshd-session[203432]: Failed password for invalid user fakeuser from ::1 port 54018 ssh2
host = kali source = /var/log/journal.log sourcetype = journal
9/8/25 2:53:04.000 PM
Sep 08 14:53:04 kali sshd-session[203432]: Failed password for invalid user fakeuser from ::1 port 54018 ssh2
host = kali source = /var/log/journal.log sourcetype = journal
9/8/25 2:52:59.000 PM
Sep 08 14:52:59 kali sshd-session[203432]: Failed password for invalid user fakeuser from ::1 port 54018 ssh2
host = kali source = /var/log/journal.log sourcetype = journal
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
18°C Sunny
Search
ENG US
2:57 PM 9/8/2025

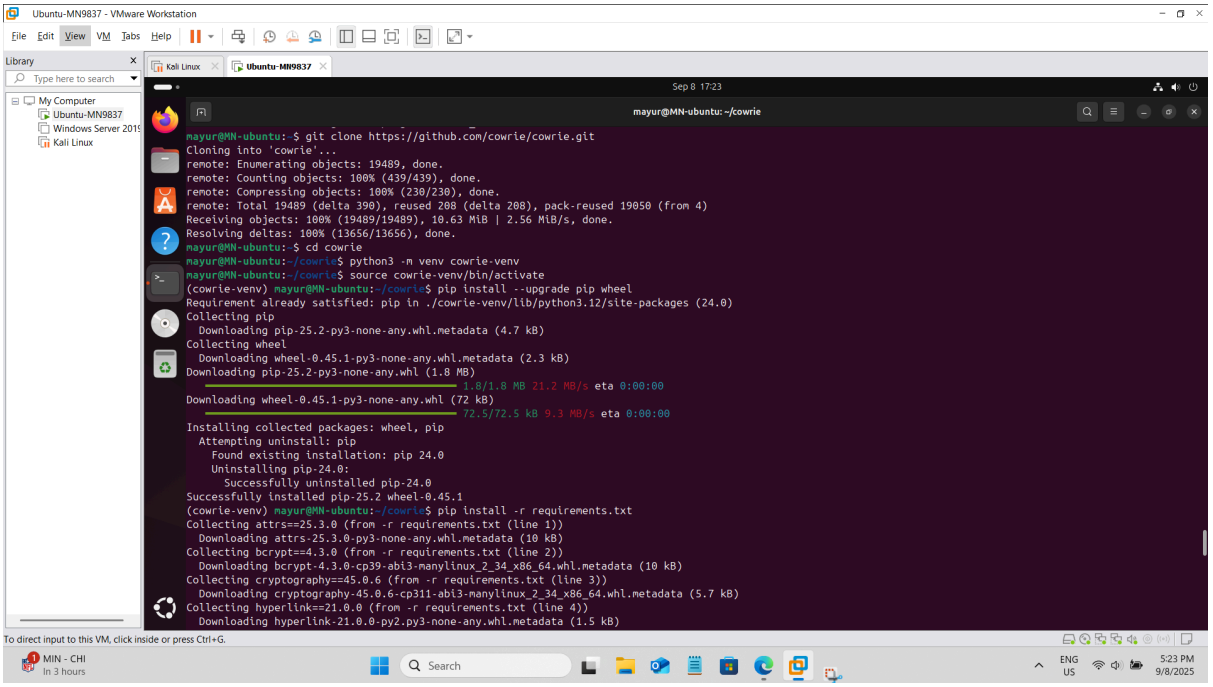

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Apps Places
Sep 8 15:09
mayur@kali: /
mayur@kali: /
mayur@kali: /
Sep 08 14:52:23 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Sep 08 14:52:23 kali sshd[203250]: Server listening on 0.0.0.0 port 22.
Sep 08 14:52:23 kali sshd[203250]: Server listening on :: port 22.
Sep 08 14:52:23 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
┌──(mayur㉿kali)-[/]
└─$ ssh fakeuser@localhost
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:t8NdivSok3sc/k+AREuOSJw3/AFrhh+pall8/pVO/Lo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
fakeuser@localhost's password:
Permission denied, please try again.
fakeuser@localhost's password:
Permission denied, please try again.
fakeuser@localhost's password:
fakeuser@localhost: Permission denied (publickey,password).
┌──(mayur㉿kali)-[/]
└─$ logger "Sensitive file accessed"
┌──(mayur㉿kali)-[/]
└─$
┌──(mayur㉿kali)-[/]
└─$
┌──(mayur㉿kali)-[/]
└─$
┌──(mayur㉿kali)-[/]
└─$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
18°C Sunny
Search
ENG US
3:09 PM 9/8/2025

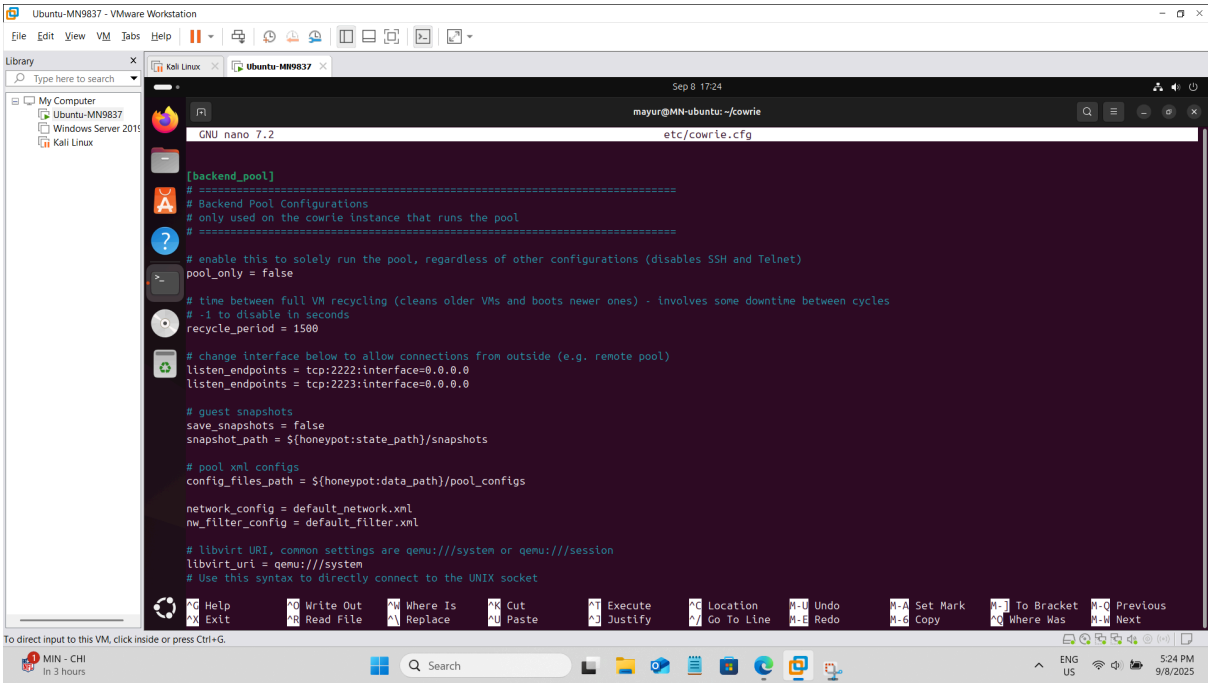

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Apps Places
Sep 8 15:09
mayur@kali: /
mayur@kali: /
mayur@kali: /
Sep 08 14:52:14 kali systemd[1]: Reloading finished in 726 ms.
Sep 08 14:52:14 kali sudo[202724]: pam_unix(sudo:session): session closed for user root
Sep 08 14:52:14 kali systemd[1]: Starting apt-daily.service - Daily apt download activities...
Sep 08 14:52:15 kali systemd[1]: apt-daily.service: Deactivated successfully.
Sep 08 14:52:15 kali systemd[1]: Finished apt-daily.service - Daily apt download activities.
Sep 08 14:52:23 kali sudo[203243]: mayur : TTY=pts/3 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/systemctl start ssh
Sep 08 14:52:23 kali sudo[203243]: pam_unix(sudo:session): session opened for user root(uid=0) by mayur(uid=1000)
Sep 08 14:52:23 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Sep 08 14:52:23 kali sshd[203250]: Server listening on 0.0.0.0 port 22.
Sep 08 14:52:23 kali sshd[203250]: Server listening on :: port 22.
Sep 08 14:52:23 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Sep 08 14:52:23 kali sudo[203243]: pam_unix(sudo:session): session closed for user root
Sep 08 14:52:29 kali sudo[203300]: mayur : TTY=pts/3 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/systemctl status ssh
Sep 08 14:52:29 kali sudo[203300]: pam_unix(sudo:session): session opened for user root(uid=0) by mayur(uid=1000)
Sep 08 14:52:29 kali sudo[203300]: pam_unix(sudo:session): session closed for user root
Sep 08 14:52:53 kali sshd-session[203432]: Invalid user fakeuser from ::1 port 54018
Sep 08 14:52:57 kali sshd-session[203432]: pam_unix(sshd:auth): check pass; user unknown
Sep 08 14:52:57 kali sshd-session[203432]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=::1
Sep 08 14:52:59 kali sshd-session[203432]: Failed password for invalid user fakeuser from ::1 port 54018 ssh2
Sep 08 14:53:02 kali sshd-session[203432]: pam_unix(sshd:auth): check pass; user unknown
Sep 08 14:53:04 kali sshd-session[203432]: Failed password for invalid user fakeuser from ::1 port 54018 ssh2
Sep 08 14:53:05 kali sshd-session[203432]: pam_unix(sshd:auth): check pass; user unknown
Sep 08 14:53:07 kali sshd-session[203432]: Failed password for invalid user fakeuser from ::1 port 54018 ssh2
Sep 08 14:53:07 kali sshd-session[203432]: Connection closed by invalid user fakeuser ::1 port 54018 [preauth]
Sep 08 14:53:07 kali sshd-session[203432]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=::1
Sep 08 14:55:01 kali CRON[205204]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Sep 08 14:55:01 kali CRON[205206]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Sep 08 14:55:01 kali CRON[205204]: pam_unix(cron:session): session closed for user root
Sep 08 14:55:12 kali PackageKit[201342]: daemon quit
Sep 08 14:55:12 kali systemd[1]: packagekit.service: Deactivated successfully.
Sep 08 15:05:01 kali CRON[206559]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Sep 08 15:05:01 kali CRON[206561]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Sep 08 15:05:01 kali CRON[206559]: pam_unix(cron:session): session closed for user root
Sep 08 15:07:51 kali mayur[206777]: Sensitive file accessed
Sep 08 15:09:01 kali CRON[207226]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Sep 08 15:09:01 kali CRON[207228]: (root) CMD ([-x /usr/lib/php/sessionclean] && if [! -d /run/systemd/system]; then /usr/lib/php/sessionclean; fi)
Sep 08 15:09:01 kali CRON[207226]: pam_unix(cron:session): session closed for user root
Sep 08 15:09:01 kali systemd[1]: Starting phpsessionclean.service - Clean php session files...
Sep 08 15:09:02 kali systemd[1]: phpsessionclean.service: Deactivated successfully.
Sep 08 15:09:02 kali systemd[1]: Finished phpsessionclean.service - Clean php session files.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
18°C Sunny
Search
ENG US
3:09 PM 9/8/2025

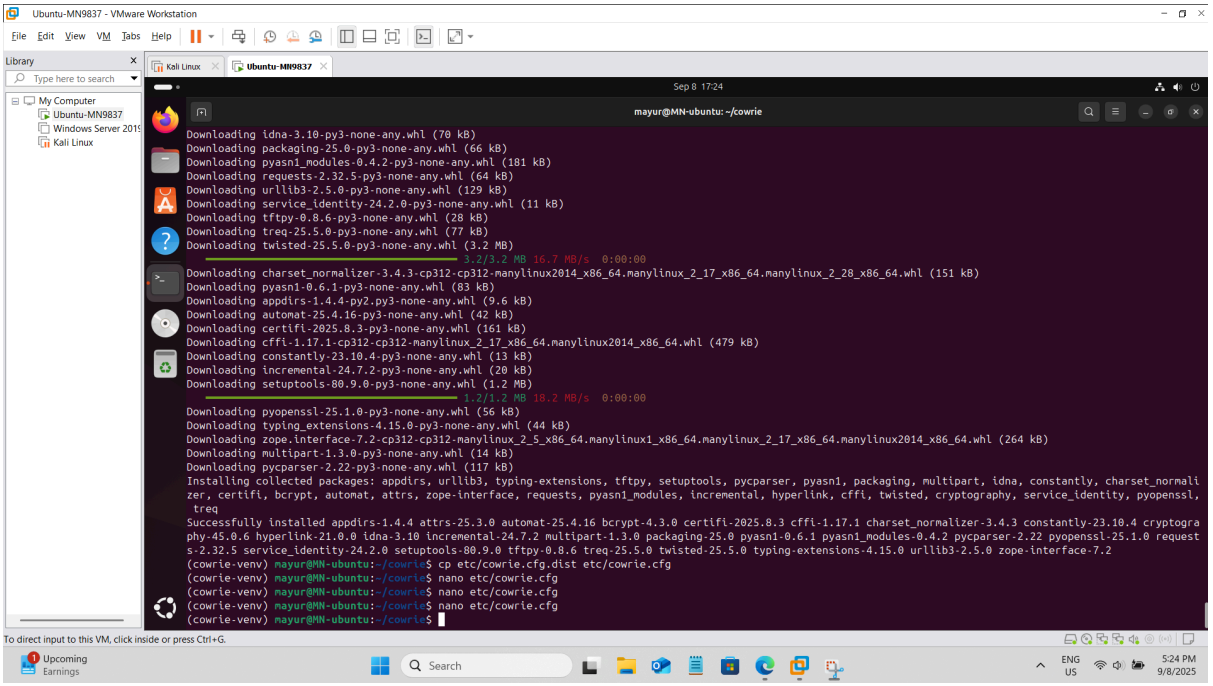

Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Apps Places
Sep 8 15:09
Search | Splunk 10.0.0
192.168.2.237:8000/en-US/app/search/search?earliest=-15m&latest=now&q=search index%3Dmain "sensitive file"&display.page.search.mode=smart&disp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
splunk>enterprise Apps
Administrator Messages Settings Activity Help Find
Search Analytics Datasets Reports Alerts Dashboards
Search & Reporting
New Search
Save As Create Table View Close
index=main "sensitive file"
Time range: Last 15 minutes
1 event (9/8/25 2:53:52.000 PM to 9/8/25 3:08:52.000 PM)
No Event Sampling
Job Smart Mode
Events (1) Patterns Statistics Visualization
Timeline format Zoom Out Zoom to Selection Deselect
1 minute per column
Format Show: 20 Per Page View: List
Hide Fields All Fields
Time Event
9/8/25 3:07:51.000 PM
Sep 08 15:07:51 kali mayur[206777]: Sensitive file accessed
host = kali source = /var/log/journal.log sourcetype = journal
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 1
date_month 1
date_second 1
date_wday 1
date_year 1
date_zone 1
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
18°C Sunny
Search
ENG US
3:09 PM 9/8/2025

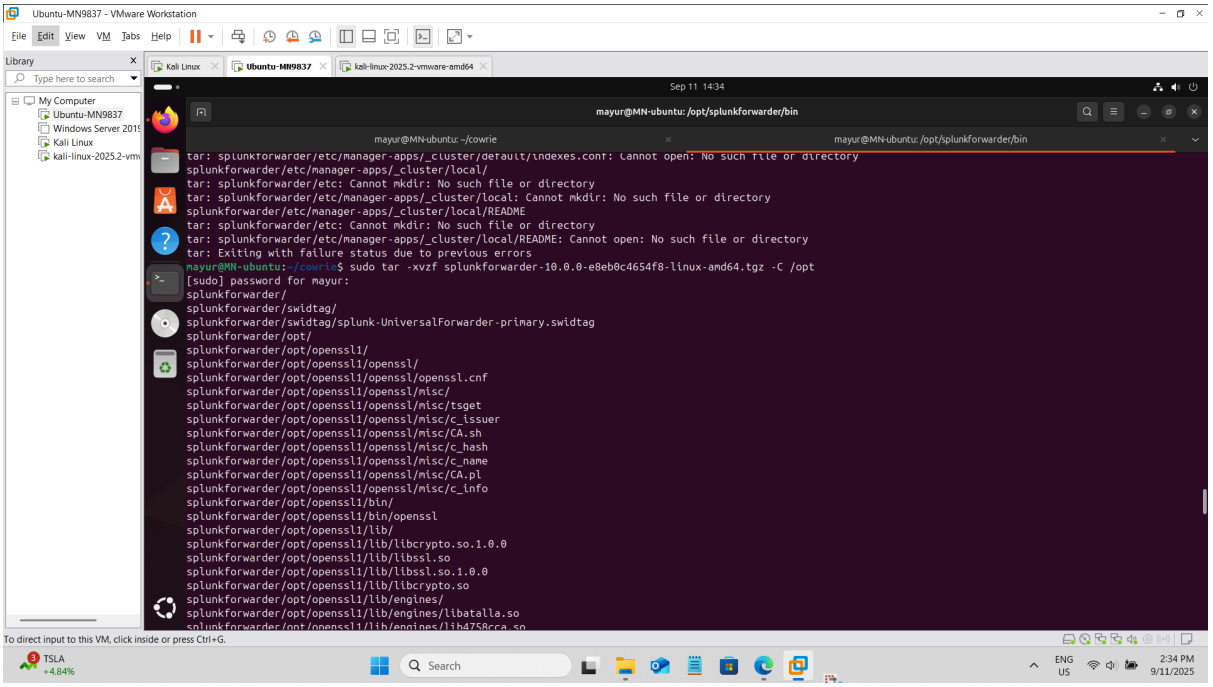

Kali Linux - VMware Workstation
SOC Lab Dashboard
Monitoring failed SSH attempts, custom test events, and system service logs
Failed SSH Attempts
Custom SOC Lab Events
Configuration
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

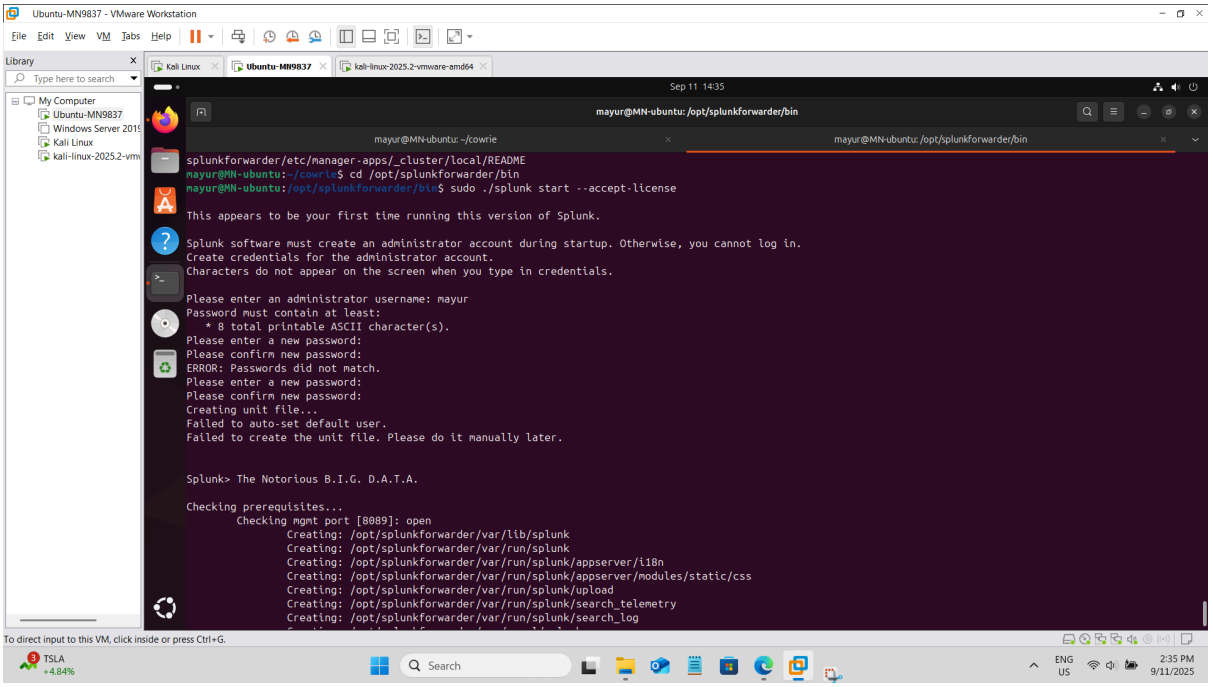

Ubuntu-MN9837 - VMware Workstation
mayur@MN-ubuntu: ~/cowrie
mayur@MN-ubuntu:~$ sudo apt install -y git python3-venv python3-pip jq authbind
To direct input to this VM, click inside or press Ctrl+G.

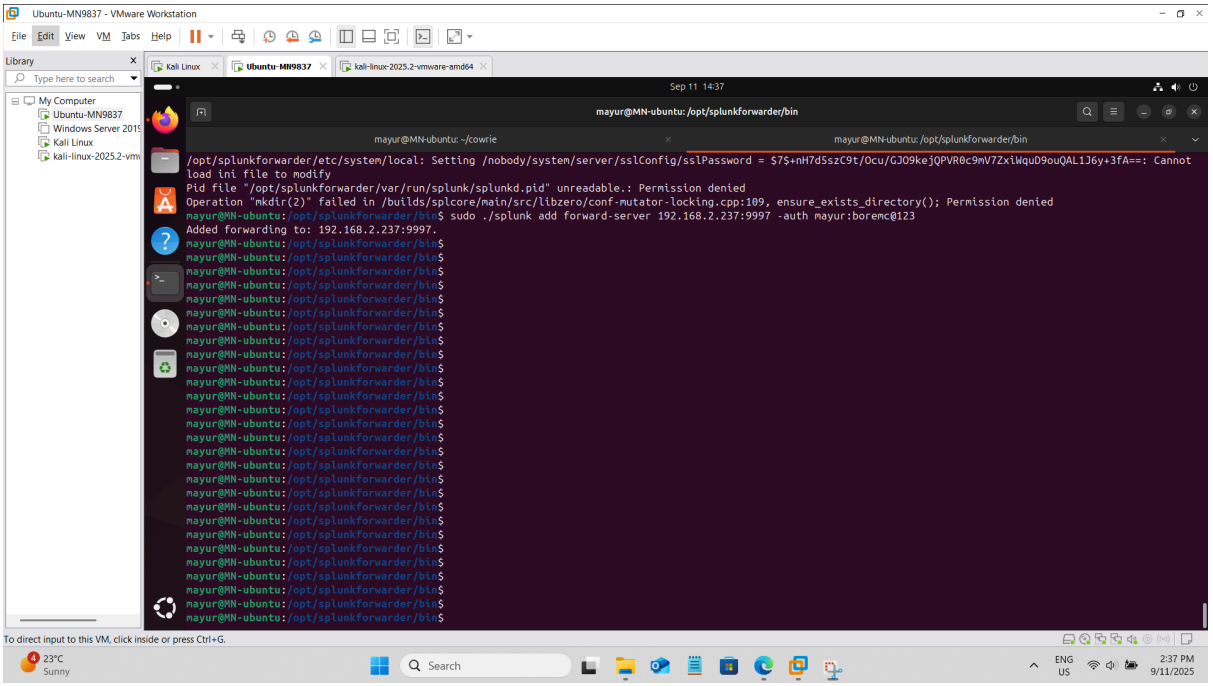

Ubuntu-MN9837 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Ubuntu-MN9837
Sep 8 17:23
mayur@MN-ubuntu: ~/cowrie
mayur@MN-ubuntu:~$ git clone https://github.com/cowrie/cowrie.git
Cloning into 'cowrie'...
remote: Enumerating objects: 19489, done.
remote: Counting objects: 100% (439/439), done.
remote: Compressing objects: 100% (230/230), done.
remote: Total 19489 (delta 390), reused 208 (delta 208), pack-reused 19050 (from 4)
Receiving objects: 100% (19489/19489), 10.63 MiB | 2.56 MiB/s, done.
Resolving deltas: 100% (13656/13656), done.
mayur@MN-ubuntu:~$ cd cowrie
mayur@MN-ubuntu:~/cowrie$ python3 -m venv cowrie-venv
mayur@MN-ubuntu:~/cowrie$ source cowrie-venv/bin/activate
(cowrie-venv) mayur@MN-ubuntu:~/cowrie$ pip install --upgrade pip wheel
Requirement already satisfied: pip in ./cowrie-venv/lib/python3.12/site-packages (24.0)
Collecting pip
Downloading pip-25.2-py3-none-any.whl.metadata (4.7 kB)
Collecting wheel
Downloading wheel-0.45.1-py3-none-any.whl.metadata (2.3 kB)
Downloading pip-25.2-py3-none-any.whl (1.8 MB)
1.8/1.8 MB 21.2 MB/s eta 0:00:00
Downloading wheel-0.45.1-py3-none-any.whl (72 kB)
72.5/72.5 kB 9.3 MB/s eta 0:00:00
Installing collected packages: wheel, pip
Attempting uninstall: pip
Found existing installation: pip 24.0
Uninstalling pip-24.0:
Successfully uninstalled pip-24.0
Successfully installed pip-25.2 wheel-0.45.1
(cowrie-venv) mayur@MN-ubuntu:~/cowrie$ pip install -r requirements.txt
Collecting attrs==25.3.0 (from -r requirements.txt (line 1))
Downloading attrs-25.3.0-py3-none-any.whl.metadata (10 kB)
Collecting bcrypt==4.3.0 (from -r requirements.txt (line 2))
Downloading bcrypt-4.3.0-cp39-abi3-manylinux_2_34_x86_64.whl.metadata (10 kB)
Collecting cryptography==45.0.6 (from -r requirements.txt (line 3))
Downloading cryptography-45.0.6-cp311-abi3-manylinux_2_34_x86_64.whl.metadata (5.7 kB)
Collecting hyperlink==21.0.0 (from -r requirements.txt (line 4))
Downloading hyperlink-21.0.0-py2.py3-none-any.whl.metadata (1.5 kB)
To direct input to this VM, click inside or press Ctrl+G.
MIN - CHI
In 3 hours
Search
ENG
US
5:23 PM
9/8/2025

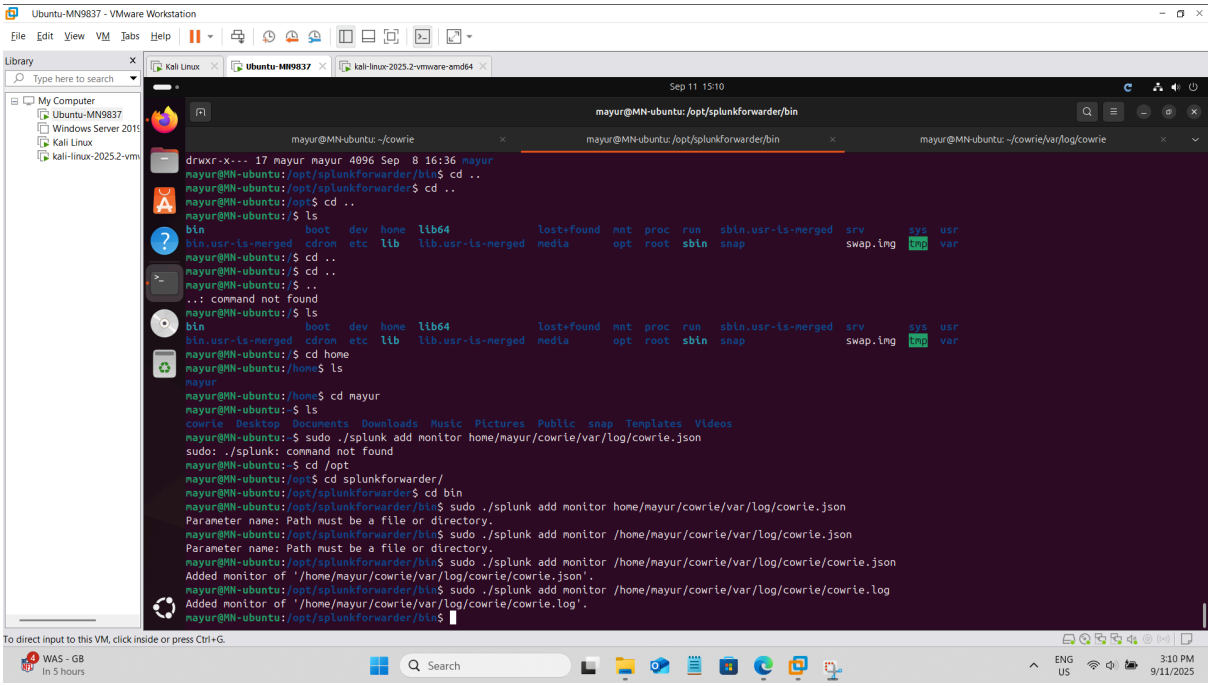

Ubuntu-MN9837 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Ubuntu-MN9837
Sep 8 17:24
mayur@MN-ubuntu: ~/cowrie
GNU nano 7.2
etc/cowrie.cfg
[backend_pool]
# ==
# Backend Pool Configurations
# only used on the cowrie instance that runs the pool
# ==
# enable this to solely run the pool, regardless of other configurations (disables SSH and Telnet)
pool_only = false
# time between full VM recycling (cleans older VMs and boots newer ones) - involves some downtime between cycles
# -1 to disable in seconds
recycle_period = 1500
# change interface below to allow connections from outside (e.g. remote pool)
listen_endpoints = tcp:2222:interface=0.0.0.0
listen_endpoints = tcp:2223:interface=0.0.0.0
# guest snapshots
save_snapshots = false
snapshot_path = ${honeypot:state_path}/snapshots
# pool xml configs
config_files_path = ${honeypot:data_path}/pool_configs
network_config = default_network.xml
nw_filter_config = default_filter.xml
# libvirt URI, common settings are qemu:///system or qemu:///session
libvirt_uri = qemu:///system
# Use this syntax to directly connect to the UNIX socket
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-W Next
To direct input to this VM, click inside or press Ctrl+G.
MIN - CHI
In 3 hours
Search
ENG
US
5:24 PM
9/8/2025

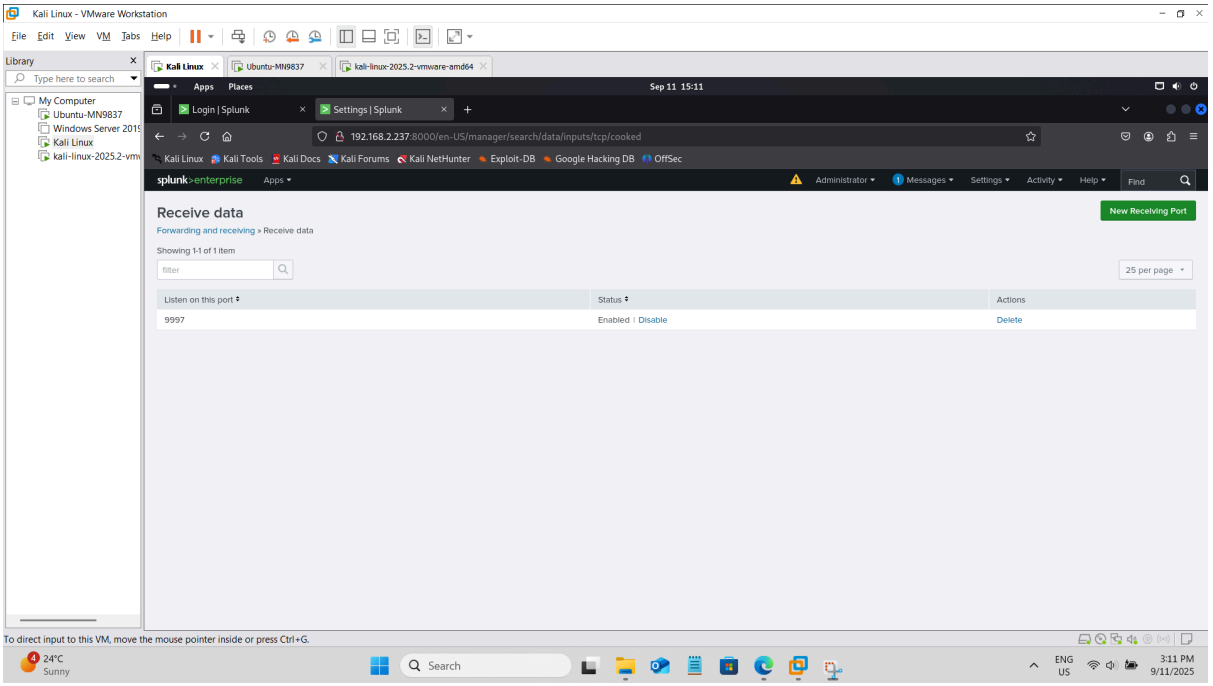

Ubuntu-MN9837 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
Kali Linux
Ubuntu-MN9837
Sep 8 17:24
mayur@MN-ubuntu: ~/cowrie
Downloading idna-3.10-py3-none-any.whl (70 kB)
Downloading packaging-25.0-py3-none-any.whl (66 kB)
Downloading pyasn1_modules-0.4.2-py3-none-any.whl (181 kB)
Downloading requests-2.32.5-py3-none-any.whl (64 kB)
Downloading urllib3-2.5.0-py3-none-any.whl (129 kB)
Downloading service_identity-24.2.0-py3-none-any.whl (11 kB)
Downloading tftpy-0.8.6-py3-none-any.whl (28 kB)
Downloading treq-25.5.0-py3-none-any.whl (77 kB)
Downloading twisted-25.5.0-py3-none-any.whl (3.2 MB)
3.2/3.2 MB 16.7 MB/s 0:00:00
Downloading charset_normalizer-3.4.3-cp312-cp312-manylinux2014_x86_64.manylinux_2_17_x86_64.manylinux_2_28_x86_64.whl (151 kB)
Downloading pyasn1-0.6.1-py3-none-any.whl (83 kB)
Downloading appdirs-1.4.4-py2.py3-none-any.whl (9.6 kB)
Downloading automat-25.4.16-py3-none-any.whl (42 kB)
Downloading certifi-2025.8.3-py3-none-any.whl (161 kB)
Downloading cffi-1.17.1-cp312-cp312-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (479 kB)
Downloading constantly-23.10.4-py3-none-any.whl (13 kB)
Downloading incremental-24.7.2-py3-none-any.whl (20 kB)
Downloading setuptools-80.9.0-py3-none-any.whl (1.2 MB)
1.2/1.2 MB 18.2 MB/s 0:00:00
Downloading pyopenssl-25.1.0-py3-none-any.whl (56 kB)
Downloading typing_extensions-4.15.0-py3-none-any.whl (44 kB)
Downloading zope.interface-7.2-cp312-cp312-manylinux_2_5_x86_64.manylinux1_x86_64.manylinux_2_17_x86_64.manylinux2014_x86_64.whl (264 kB)
Downloading multipart-1.3.0-py3-none-any.whl (14 kB)
Downloading pycparser-2.22-py3-none-any.whl (117 kB)
Installing collected packages: appdirs, urllib3, typing-extensions, tftpy, setuptools, pycparser, pyasn1, packaging, multipart, idna, constantly, charset_normalizer, certifi, bcrypt, automat, attrs, zope-interface, requests, pyasn1_modules, incremental, hyperlink, cffi, twisted, cryptography, service_identity, pyopenssl, treq
Successfully installed appdirs-1.4.4 attrs-25.3.0 automat-25.4.16 bcrypt-4.3.0 certifi-2025.8.3 cffi-1.17.1 charset_normalizer-3.4.3 constantly-23.10.4 cryptography-45.0.6 hyperlink-21.0.0 idna-3.10 incremental-24.7.2 multipart-1.3.0 packaging-25.0 pyasn1-0.6.1 pyasn1_modules-0.4.2 pycparser-2.22 pyopenssl-25.1.0 requests-2.32.5 service_identity-24.2.0 setuptools-80.9.0 tftpy-0.8.6 treq-25.5.0 twisted-25.5.0 typing-extensions-4.15.0 urllib3-2.5.0 zope-interface-7.2
(cowrie-venv) mayur@MN-ubuntu:~/cowrie$ cp etc/cowrie.cfg.dist etc/cowrie.cfg
(cowrie-venv) mayur@MN-ubuntu:~/cowrie$ nano etc/cowrie.cfg
(cowrie-venv) mayur@MN-ubuntu:~/cowrie$ nano etc/cowrie.cfg
(cowrie-venv) mayur@MN-ubuntu:~/cowrie$ nano etc/cowrie.cfg
(cowrie-venv) mayur@MN-ubuntu:~/cowrie$
To direct input to this VM, click inside or press Ctrl+G.
Upcoming Earnings
Search
ENG US
5:24 PM 9/8/2025

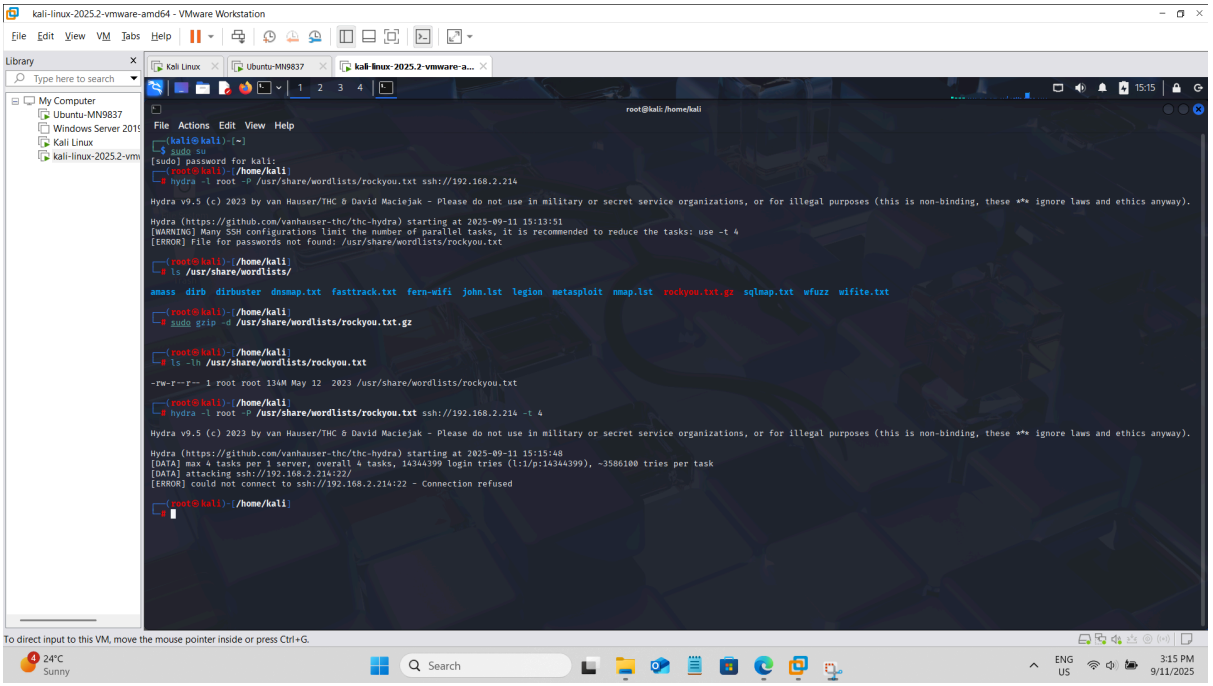

Ubuntu-MN9837 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
kali-linux-2025.2-vmw
Kali Linux
Ubuntu-MN9837
kali-linux-2025.2-vmware-amd64
Sep 11 14:34
mayur@MN-ubuntu: /opt/splunkforwarder/bin
mayur@MN-ubuntu: ~/cowrie
mayur@MN-ubuntu: /opt/splunkforwarder/bin
tar: splunkforwarder/etc/manager-apps/_cluster/default/indexes.conf: Cannot open: No such file or directory
splunkforwarder/etc/manager-apps/_cluster/local/
tar: splunkforwarder/etc: Cannot mkdir: No such file or directory
tar: splunkforwarder/etc/manager-apps/_cluster/local: Cannot mkdir: No such file or directory
splunkforwarder/etc/manager-apps/_cluster/local/README
tar: splunkforwarder/etc: Cannot mkdir: No such file or directory
tar: splunkforwarder/etc/manager-apps/_cluster/local/README: Cannot open: No such file or directory
tar: Exiting with failure status due to previous errors
mayur@MN-ubuntu:~/cowrie$ sudo tar -xvzf splunkforwarder-10.0.0-e8eb0c4654f8-linux-amd64.tgz -C /opt
[sudo] password for mayur:
splunkforwarder/
splunkforwarder/swidtag/
splunkforwarder/swidtag/splunk-UniversalForwarder-primary.swidtag
splunkforwarder/opt/
splunkforwarder/opt/openssl1/
splunkforwarder/opt/openssl1/openssl/
splunkforwarder/opt/openssl1/openssl/openssl.cnf
splunkforwarder/opt/openssl1/openssl/misc/
splunkforwarder/opt/openssl1/openssl/misc/tsget
splunkforwarder/opt/openssl1/openssl/misc/c_issuer
splunkforwarder/opt/openssl1/openssl/misc/CA.sh
splunkforwarder/opt/openssl1/openssl/misc/c_hash
splunkforwarder/opt/openssl1/openssl/misc/c_name
splunkforwarder/opt/openssl1/openssl/misc/CA.pl
splunkforwarder/opt/openssl1/openssl/misc/c_info
splunkforwarder/opt/openssl1/bin/
splunkforwarder/opt/openssl1/bin/openssl
splunkforwarder/opt/openssl1/lib/
splunkforwarder/opt/openssl1/lib/libcrypto.so.1.0.0
splunkforwarder/opt/openssl1/lib/libssl.so
splunkforwarder/opt/openssl1/lib/libssl.so.1.0.0
splunkforwarder/opt/openssl1/lib/libcrypto.so
splunkforwarder/opt/openssl1/lib/engines/
splunkforwarder/opt/openssl1/lib/engines/libatalla.so
To direct input to this VM, click inside or press Ctrl+G.
TSLA +4.84%
Search
ENG US
2:34 PM 9/11/2025

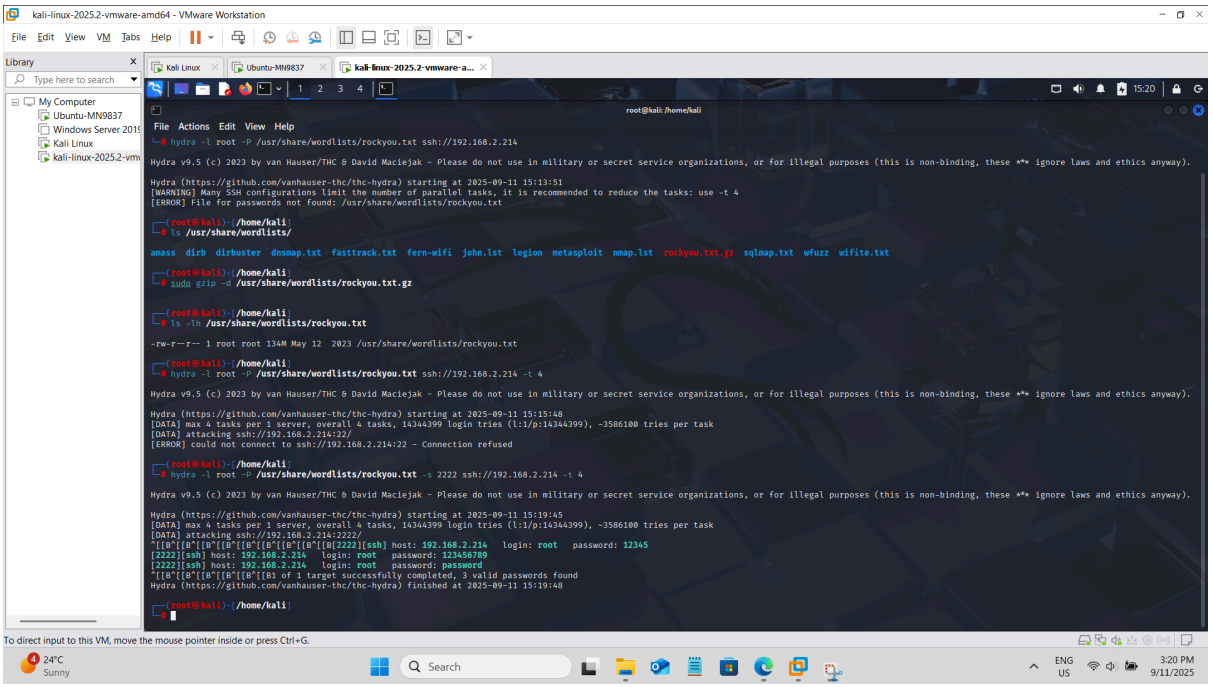

Ubuntu-MN9837 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
kali-linux-2025.2-vmw
Kali Linux
Ubuntu-MN9837
kali-linux-2025.2-vmware-amd64
Sep 11 14:35
mayur@MN-ubuntu: /opt/splunkforwarder/bin
mayur@MN-ubuntu: ~/cowrie
mayur@MN-ubuntu: /opt/splunkforwarder/bin
splunkforwarder/etc/manager-apps/_cluster/local/README
mayur@MN-ubuntu:~/cowrie$ cd /opt/splunkforwarder/bin
mayur@MN-ubuntu:/opt/splunkforwarder/bin$ sudo ./splunk start --accept-license
This appears to be your first time running this version of Splunk.
Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.
Please enter an administrator username: mayur
Password must contain at least:
* 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
ERROR: Passwords did not match.
Please enter a new password:
Please confirm new password:
Creating unit file...
Failed to auto-set default user.
Failed to create the unit file. Please do it manually later.
Splunk> The Notorious B.I.G. D.A.T.A.
Checking prerequisites...
Checking mgmt port [8089]: open
Creating: /opt/splunkforwarder/var/lib/splunk
Creating: /opt/splunkforwarder/var/run/splunk
Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
Creating: /opt/splunkforwarder/var/run/splunk/upload
Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
Creating: /opt/splunkforwarder/var/run/splunk/search_log
To direct input to this VM, click inside or press Ctrl+G.
TSLA
+4.84%
Search
ENG
US
2:35 PM
9/11/2025

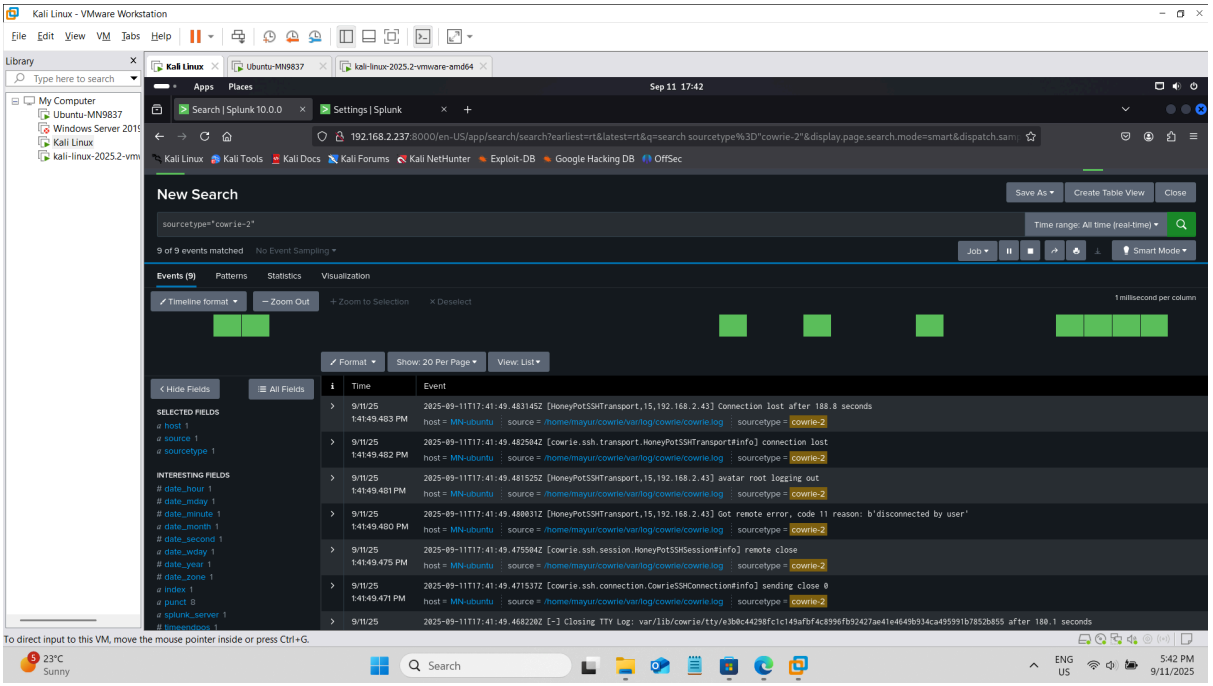

Ubuntu-MN9837 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
kali-linux-2025.2-vmw
Kali Linux
Ubuntu-MN9837
kali-linux-2025.2-vmware-amd64
Sep 11 14:37
mayur@MN-ubuntu: /opt/splunkforwarder/bin
mayur@MN-ubuntu: ~/cowrie
mayur@MN-ubuntu: /opt/splunkforwarder/bin
/opt/splunkforwarder/etc/system/local: Setting /nobody/system/server/sslConfig/sslPassword = 7+nH7d5szC9t/Ocu/GJO9kejQPVR0c9mV7ZxiWquD9ouQAL1J6y+3fA==: Cannot load ini file to modify
Pid file "/opt/splunkforwarder/var/run/splunk/splunkd.pid" unreadable.: Permission denied
Operation "mkdir(2)" failed in /builds/splcore/main/src/libzero/conf-mutator-locking.cpp:109, ensure_exists_directory(); Permission denied
mayur@MN-ubuntu:/opt/splunkforwarder/bin$ sudo ./splunk add forward-server 192.168.2.237:9997 -auth mayur:boremc@123
Added forwarding to: 192.168.2.237:9997.
mayur@MN-ubuntu:/opt/splunkforwarder/bin$
To direct input to this VM, click inside or press Ctrl+G.
23°C
Sunny
Search
ENG
US
2:37 PM
9/11/2025


Ubuntu-MN9837 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
kali-linux-2025.2-vmw
Kali Linux
Ubuntu-MN9837
kali-linux-2025.2-vmware-amd64
Sep 11 15:10
mayur@MN-ubuntu: /opt/splunkforwarder/bin
mayur@MN-ubuntu: ~/cowrie
mayur@MN-ubuntu: /opt/splunkforwarder/bin
mayur@MN-ubuntu: ~/cowrie/var/log/cowrie
drwxr-x--- 17 mayur mayur 4096 Sep 8 16:36 mayur
mayur@MN-ubuntu:/opt/splunkforwarder/bin$ cd ..
mayur@MN-ubuntu:/opt/splunkforwarder$ cd ..
mayur@MN-ubuntu:/opt$ cd ..
mayur@MN-ubuntu:/$ ls
bin boot dev home lib64 lost+found mnt proc run sbin.usr-is-merged srv sys usr
bin.usr-is-merged cdrom etc lib lib.usr-is-merged media opt root sbin snap swap.img tmp var
mayur@MN-ubuntu:/$ cd ..
mayur@MN-ubuntu:/$ cd ..
mayur@MN-ubuntu:/$ ..
..: command not found
mayur@MN-ubuntu:/$ ls
bin boot dev home lib64 lost+found mnt proc run sbin.usr-is-merged srv sys usr
bin.usr-is-merged cdrom etc lib lib.usr-is-merged media opt root sbin snap swap.img tmp var
mayur@MN-ubuntu:/$ cd home
mayur@MN-ubuntu:/home$ ls
mayur
mayur@MN-ubuntu:/home$ cd mayur
mayur@MN-ubuntu:~$ ls
cowrie Desktop Documents Downloads Music Pictures Public snap Templates Videos
mayur@MN-ubuntu:~$ sudo ./splunk add monitor home/mayur/cowrie/var/log/cowrie.json
sudo: ./splunk: command not found
mayur@MN-ubuntu:~$ cd /opt
mayur@MN-ubuntu:/opt$ cd splunkforwarder/
mayur@MN-ubuntu:/opt/splunkforwarder$ cd bin
mayur@MN-ubuntu:/opt/splunkforwarder/bin$ sudo ./splunk add monitor home/mayur/cowrie/var/log/cowrie.json
Parameter name: Path must be a file or directory.
mayur@MN-ubuntu:/opt/splunkforwarder/bin$ sudo ./splunk add monitor /home/mayur/cowrie/var/log/cowrie.json
Parameter name: Path must be a file or directory.
mayur@MN-ubuntu:/opt/splunkforwarder/bin$ sudo ./splunk add monitor /home/mayur/cowrie/var/log/cowrie/cowrie.json
Added monitor of '/home/mayur/cowrie/var/log/cowrie/cowrie.json'.
mayur@MN-ubuntu:/opt/splunkforwarder/bin$ sudo ./splunk add monitor /home/mayur/cowrie/var/log/cowrie/cowrie.log
Added monitor of '/home/mayur/cowrie/var/log/cowrie/cowrie.log'.
mayur@MN-ubuntu:/opt/splunkforwarder/bin$
To direct input to this VM, click inside or press Ctrl+G.
WAS - GB
In 5 hours
Search
ENG
US
3:10 PM
9/11/2025


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
kali-linux-2025.2-vmw
Kali Linux
Ubuntu-MN9837
kali-linux-2025.2-vmware-amd64
Apps Places
Sep 11 15:11
Login | Splunk
Settings | Splunk
192.168.2.237:8000/en-US/manager/search/data/inputs/tcp/cooked
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Receive data
New Receiving Port
Forwarding and receiving › Receive data
Showing 1-1 of 1 item
filter
25 per page
Listen on this port
Status
Actions
9997
Enabled | Disable
Delete
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
24°C
Sunny
Search
ENG
US
3:11 PM
9/11/2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
kali-linux-2025.2-vmw
Kali Linux
Ubuntu-MN9837
kali-linux-2025.2-vmware-a...
15:15
root@kali: /home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.2.214
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 15:13:51
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[ERROR] File for passwords not found: /usr/share/wordlists/rockyou.txt
(root㉿kali)-[/home/kali]
ls /usr/share/wordlists/
amass dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt.gz sqlmap.txt wfuzz wifite.txt
(root㉿kali)-[/home/kali]
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
(root㉿kali)-[/home/kali]
ls -lh /usr/share/wordlists/rockyou.txt
-rw-r--r-- 1 root root 134M May 12 2023 /usr/share/wordlists/rockyou.txt
(root㉿kali)-[/home/kali]
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.2.214 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 15:15:48
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.2.214:22/
[ERROR] could not connect to ssh://192.168.2.214:22 - Connection refused
(root㉿kali)-[/home/kali]
#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
24°C
Sunny
Search
ENG
US
3:15 PM
9/11/2025


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
kali-linux-2025.2-vmw
Kali Linux
Ubuntu-MN9837
kali-linux-2025.2-vmware-a...
15:20
root@kali: /home/kali
File Actions Edit View Help
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.2.214
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 15:13:51
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[ERROR] File for passwords not found: /usr/share/wordlists/rockyou.txt
(root㉿kali)-[/home/kali]
ls /usr/share/wordlists/
amass dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt.gz sqlmap.txt wfuzz wifite.txt
(root㉿kali)-[/home/kali]
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
(root㉿kali)-[/home/kali]
ls -lh /usr/share/wordlists/rockyou.txt
-rw-r--r-- 1 root root 134M May 12 2023 /usr/share/wordlists/rockyou.txt
(root㉿kali)-[/home/kali]
hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://192.168.2.214 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 15:15:48
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.2.214:22/
[ERROR] could not connect to ssh://192.168.2.214:22 - Connection refused
(root㉿kali)-[/home/kali]
hydra -l root -P /usr/share/wordlists/rockyou.txt -s 2222 ssh://192.168.2.214 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 15:19:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.2.214:2222/
[2222][ssh] host: 192.168.2.214 login: root password: 12345
[2222][ssh] host: 192.168.2.214 login: root password: 123456789
[2222][ssh] host: 192.168.2.214 login: root password: password
[81 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-11 15:19:48
(root㉿kali)-[/home/kali]
#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
24°C
Sunny
Search
ENG
US
3:20 PM
9/11/2025


Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu-MN9837
Windows Server 2019
Kali Linux
kali-linux-2025.2-vmw
Kali Linux
Ubuntu-MN9837
kali-linux-2025.2-vmware-amd64
Apps Places
Sep 11 17:42
Search | Splunk 10.0.0
Settings | Splunk
192.168.2.237:8000/en-US/app/search/search?earliest=rt&latest=rt&q=search sourcetype%3D"cowrie-2"&display.page.search.mode=smart&dispatch.sam
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
New Search
Save As
Create Table View
Close
sourcetype="cowrie-2"
Time range: All time (real-time)
9 of 9 events matched
No Event Sampling
Job
Smart Mode
Events (9)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 1
date_month 1
date_second 1
date_wday 1
date_year 1
date_zone 1
index 1
punct 8
splunk_server 1
timeendpos 1
Time
Event
9/11/25 1:41:49.483 PM
2025-09-11T17:41:49.483145Z [HoneyPotSSHTransport,15,192.168.2.43] Connection lost after 188.8 seconds
host = MN-ubuntu source = /home/mayur/cowrie/var/log/cowrie/cowrie.log sourcetype = cowrie-2
9/11/25 1:41:49.482 PM
2025-09-11T17:41:49.482504Z [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
host = MN-ubuntu source = /home/mayur/cowrie/var/log/cowrie/cowrie.log sourcetype = cowrie-2
9/11/25 1:41:49.481 PM
2025-09-11T17:41:49.481525Z [HoneyPotSSHTransport,15,192.168.2.43] avatar root logging out
host = MN-ubuntu source = /home/mayur/cowrie/var/log/cowrie/cowrie.log sourcetype = cowrie-2
9/11/25 1:41:49.480 PM
2025-09-11T17:41:49.480031Z [HoneyPotSSHTransport,15,192.168.2.43] Got remote error, code 11 reason: b'disconnected by user'
host = MN-ubuntu source = /home/mayur/cowrie/var/log/cowrie/cowrie.log sourcetype = cowrie-2
9/11/25 1:41:49.475 PM
2025-09-11T17:41:49.475504Z [cowrie.ssh.session.HoneyPotSSHSession#info] remote close
host = MN-ubuntu source = /home/mayur/cowrie/var/log/cowrie/cowrie.log sourcetype = cowrie-2
9/11/25 1:41:49.471 PM
2025-09-11T17:41:49.471537Z [cowrie.ssh.connection.CowrieSSHConnection#info] sending close 0
host = MN-ubuntu source = /home/mayur/cowrie/var/log/cowrie/cowrie.log sourcetype = cowrie-2
9/11/25
2025-09-11T17:41:49.468220Z [-] Closing TTY Log: var/lib/cowrie/tty/e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 after 180.1 seconds
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
23°C Sunny
Search
ENG US
5:42 PM 9/11/2025