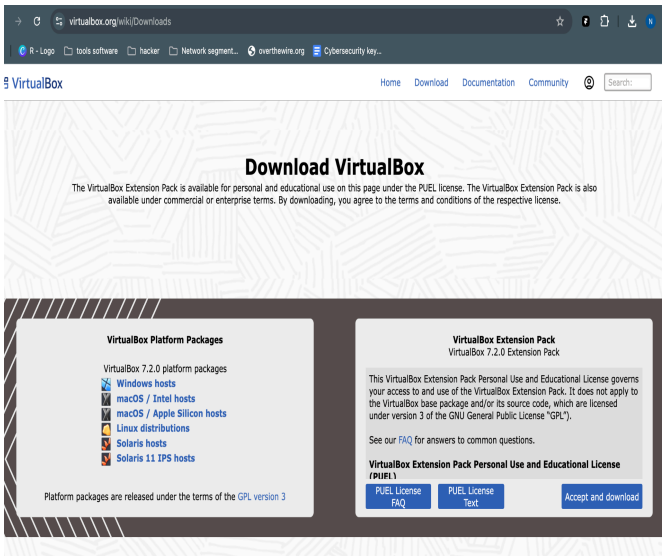
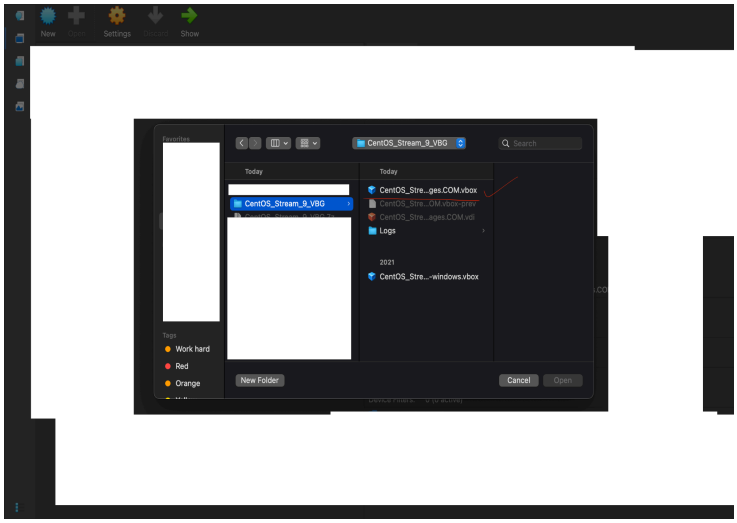
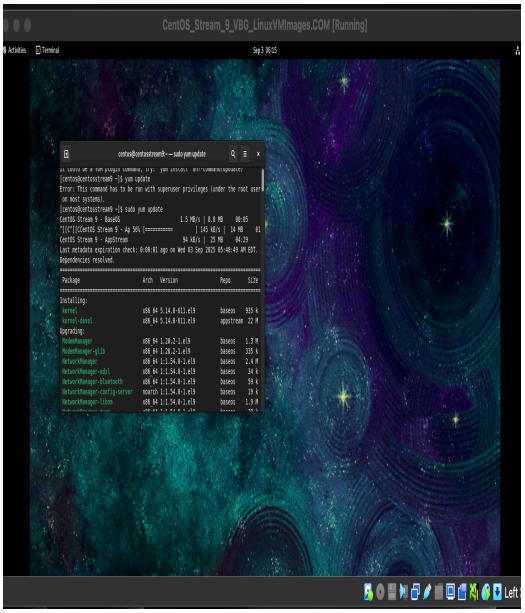
Course End Project

Screenshot

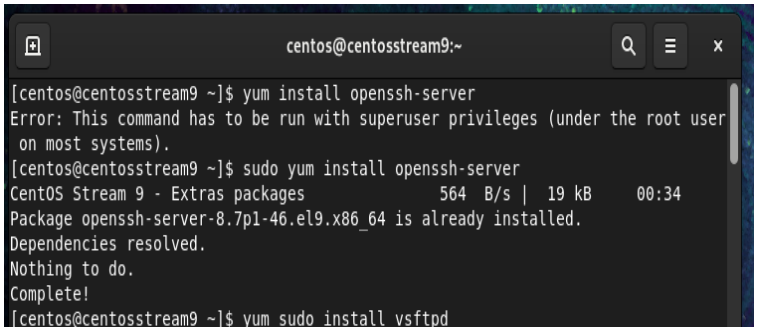
Setup

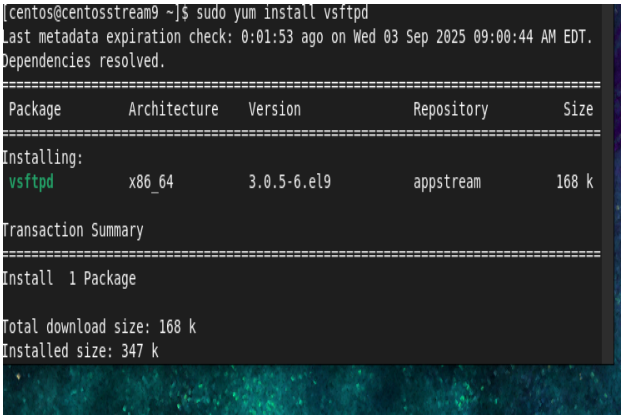


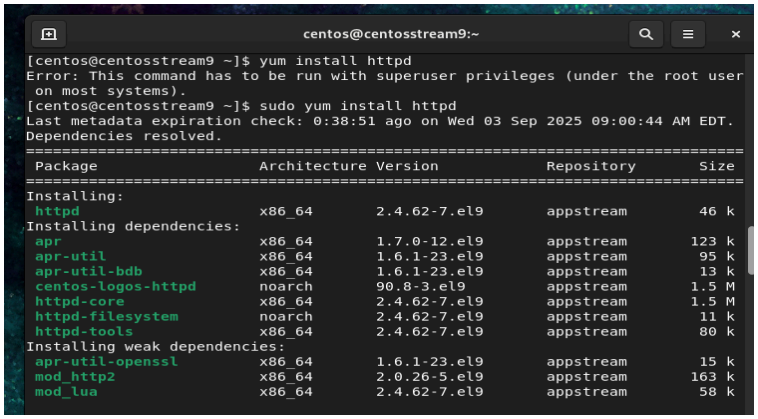


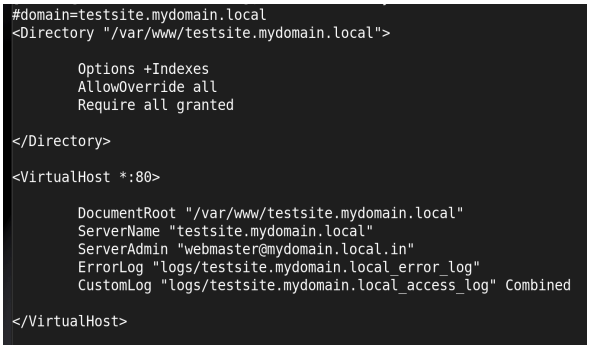


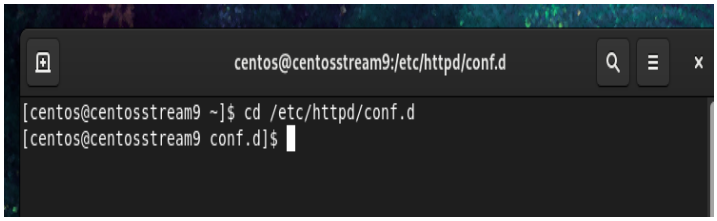
Honeypot deployment

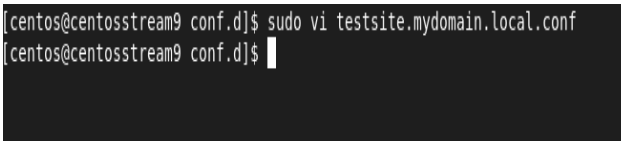


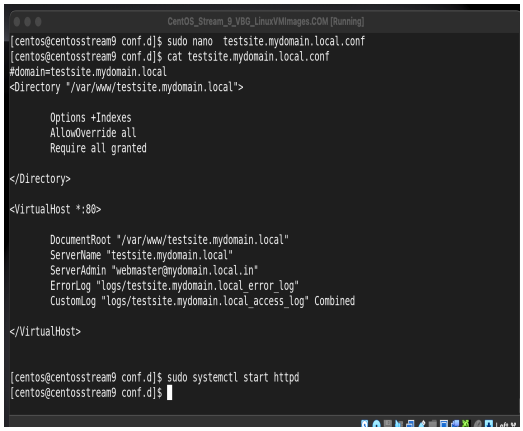


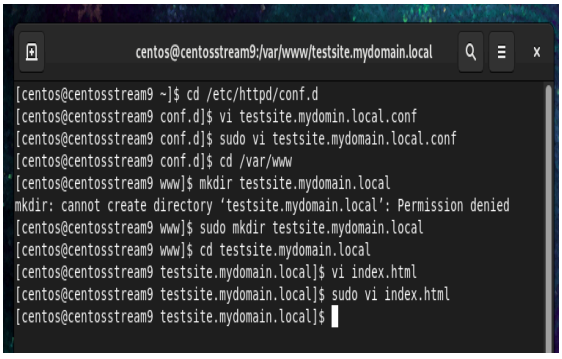










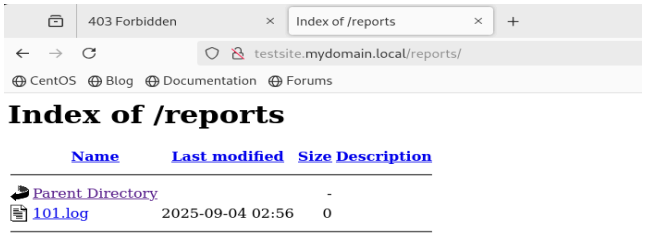


```
Complete!
[centos@centosstream9 testsite.mydomain.local]$ ls
index.html  reports
[centos@centosstream9 testsite.mydomain.local]$ sudo systemctl start httpd
[centos@centosstream9 testsite.mydomain.local]$
```

```
index.html  reports
[centos@centosstream9 testsite.mydomain.local]$ sudo systemctl start httpd
[centos@centosstream9 testsite.mydomain.local]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/
httpd.service.
[centos@centosstream9 testsite.mydomain.local]$ firefox http://testsite.mydomain.local
```


```
[centos@centosstream9 testsite.mydomain.local]$ sudo chcon unconfined_u:object_r:ht
tpd_sys_content_t:s0 /reports/
[centos@centosstream9 testsite.mydomain.local]$
```


```
[centos@centosstream9 www]$ cd testsite.mydomain.local/
[centos@centosstream9 testsite.mydomain.local]$ touch /reports/101.log
touch: cannot touch '/reports/101.log': Permission denied
[centos@centosstream9 testsite.mydomain.local]$ sudo touch /reports/101.log
[centos@centosstream9 testsite.mydomain.local]$
```



Harden SSH Configuration

```
  GNU nano 5.6.1                                  /etc/
# /etc/ssh/sshd_config.d/  which will be automa
Include /etc/ssh/sshd_config.d/*.conf

# If you want to change the port on a SELinux sy
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUM
#
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none
```

```
  GNU nano 5.6.1                                  /etc/ssh/sshd c
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
MaxAuthTries 3
#MaxSessions 10

^G Help      ^O Write Out  ^W Where Is   ^K Cut
^X Exit      ^R Read File  ^\ Replace    ^U Paste
```

```
D/--deleteall is required
[centos@centosstream9 testsite.mydomain.local]$ sudo semanage port -l
SELinux Port Type              Proto    Port Number

afs3_callback_port_t           tcp      7001
afs3_callback_port_t           udp      7001
afs_bos_port_t                 udp      7007
afs_fs_port_t                  tcp      2040
afs_fs_port_t                  udp      7000, 7005
afs_ka_port_t                  udp      7004
afs_pt_port_t                  tcp      7002
afs_pt_port_t                  udp      7002
afs_vl_port_t                  udp      7003
agentx_port_t                  tcp      705
```

```
soundd_port_t                  tcp      8000, 9433, 16001
spamd_port_t                   tcp      783, 10026, 10027
speech_port_t                  tcp      8036
squid_port_t                   tcp      3128, 3401, 4827
squid_port_t                   udp      3401, 4827
ssdp_port_t                    tcp      1900
ssdp_port_t                    udp      1900
ssh_port_t                     tcp      2222, 22
statsd_port_t                  udp      8125
svn_port_t                     tcp      3690
svn_port_t                     udp      3690
svrloc_port_t                  tcp      427
```

```
centos@centosstream9:/var/www/testsite.mydomain.local — sudo systemctl status sshd
● sshd.service - OpenSSH server daemon
     Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled;
     Active: active (running) since Thu 2025-09-04 05:02:09 EDT; 9s
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 23654 (sshd)
      Tasks: 1 (limit: 10516)
     Memory: 2.1M (peak: 2.5M)
        CPU: 14ms
     CGroup: /system.slice/sshd.service
             └─23654 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-10

Sep 04 05:02:09 centosstream9.linuxvmimages.local systemd[1]: Start
```

```
[centos@centosstream9 testsite.mydomain.local]$ sudo firewall-cm
d --permanent --zone=public --add-port=2222/tcp
success
[centos@centosstream9 testsite.mydomain.local]$
```

```
centos@centosstream9:/var/www/testsite.mydomain.local
[centos@centosstream9 testsite.mydomain.local]$ sudo firewall-cm
d --reload
success
[centos@centosstream9 testsite.mydomain.local]$
```

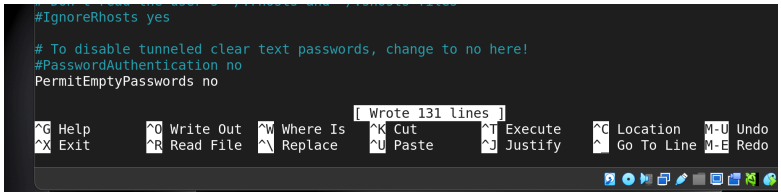
```
centos@centosstream9:~
[centos@centosstream9 ~]$ sudo adduser user1
[centos@centosstream9 ~]$ sudo passwd user1
Changing password for user user1.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
[centos@centosstream9 ~]$ sudo passwd user1
Changing password for user user1.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[centos@centosstream9 ~]$ sudo adduser user2
[centos@centosstream9 ~]$ sudo passwd user2
Changing password for user user2.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[centos@centosstream9 ~]$
```

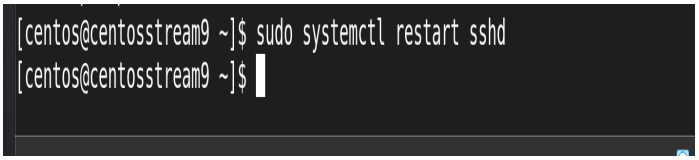
```
[centos@centosstream9 ~]$ sudo nano /etc/ssh/sshd_config
[centos@centosstream9 ~]$ sudo cat /etc/ssh/sshd_config
```

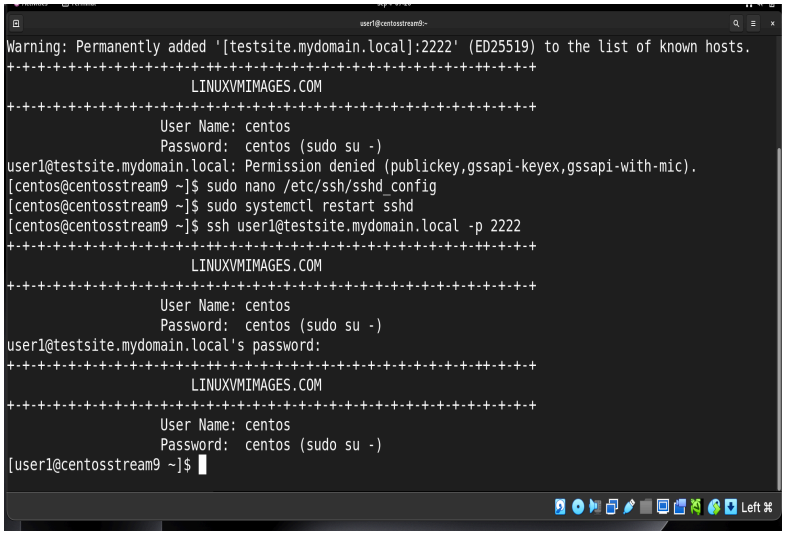
```
# and KbdInteractiveAuthenticatio
# WARNING: 'UsePAM no' is not sup
# problems.
#UsePAM no
AllowUsers user1 user2
#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
```

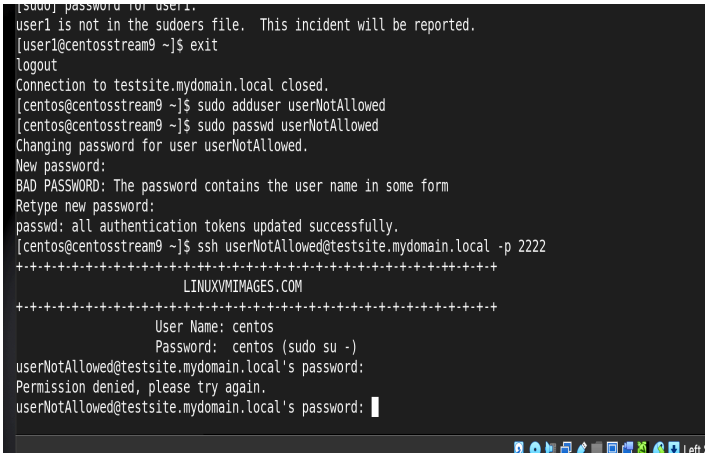
```
[centos@centosstream9 ~]$ sudo systemctl restart sshd
[centos@centosstream9 ~]$
```

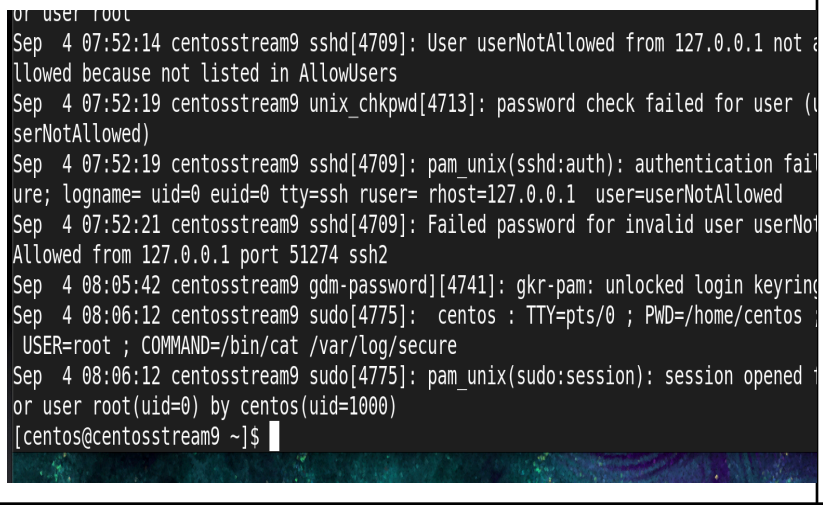
```
[centos@centosstream9 ~]$ ssh user1@testsite.mydomain.local -p 2222
The authenticity of host '[testsite.mydomain.local]:2222 ([127.0.0.1]:2222)' can't be established.
ED25519 key fingerprint is SHA256:CWCMdUrZadeJ8s3ihT4rws05cwAOSUJ0z8DTHPmcW8U.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[testsite.mydomain.local]:2222' (ED25519) to the list of known hosts.
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    LINUXVMIMAGES.COM
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                User Name: centos
                Password:  centos (sudo su -)
user1@testsite.mydomain.local: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[centos@centosstream9 ~]$
```











Automated IP Blocking

```
[centos@centosstream9 testsite.mydomain.local]$ sudo yum install
 epel-release
Last metadata expiration check: 0:41:50 ago on Thu 04 Sep 2025 0
5:10:22 AM EDT.
Dependencies resolved.
================================================================
 Package             Arch     Version     Repository       Size
================================================================
Installing:
 epel-release        noarch   9-7.el9     extras-common    19 k
Installing weak dependencies:
 epel-next-release   noarch   9-7.el9     extras-common   8.1 k

Transaction Summary
================================================================
Install  2 Packages

Total download size: 27 k
```

```
Complete!
[centos@centosstream9 ~]$ sudo systemctl start fail2ban
[centos@centosstream9 ~]$ sudo systemctl enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /usr/lib/systemd/syst
em/fail2ban.service.
[centos@centosstream9 ~]$
```

```
  GNU nano 5.6.1                          /etc/fail2b
[sshd]
enabled = true
port = 2222
filter = sshd
logpath = /var/log/secure
maxretry = 3
bantime = 3600
```

```
cat: /etc/fail2ban/jail.local: No such file or directory
[centos@centosstream9 ~]$ sudo nano /etc/fail2ban/jail.local
[centos@centosstream9 ~]$ sudo systemctl start fail2ban
[centos@centosstream9 ~]$ sudo systemctl enable fail2ban
[centos@centosstream9 ~]$
```

```
[centos@centosstream9 ~]$ sudo cat  /etc/fail2ban/jail.local
[sshd]
enabled = true
port = 2222
filter = sshd
logpath = /var/log/secure
maxretry = 3
bantime = 3600
[centos@centosstream9 ~]$ sudo systemctl restart fail2ban
[centos@centosstream9 ~]$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[centos@centosstream9 ~]$
```

```
[centos@centosstream9 ~]$ sudo yum install firewalld -y
Last metadata expiration check: 4:16:53 ago on Fri 05 Sep 2025 06:52:28 AM EDT.
Package firewalld-1.3.4-15.el9.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
```

```
[centos@centosstream9 ~]$ sudo systemctl enable firewalld
[centos@centosstream9 ~]$ sudo systemctl start firewalld
[centos@centosstream9 ~]$
```

```
[centos@centosstream9 ~]$ sudo systemctl enable firewalld
[centos@centosstream9 ~]$ sudo systemctl start firewalld
[centos@centosstream9 ~]$
```

```
[centos@centosstream9 ~]$ sudo nano /etc/fail2ban/jail.local
[centos@centosstream9 ~]$
```

```
[centos@centosstream9 ~]$ cat /etc/fail2ban/jail.local
[sshd]
enabled = true
port = 2222
filter = sshd
logpath = /var/log/secure
maxretry = 3
bantime = 3600
action = firewallcmd-ipset
[centos@centosstream9 ~]$
```

```
action = firewallcmd-ipset
[centos@centosstream9 ~]$ sudo systemctl restart firewalld
[centos@centosstream9 ~]$
```

```
[centos@centosstream9 ~]$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
[centos@centosstream9 ~]$
```

```
Sep 05 11:24:07 centosstream9.linuxvmimages.local systemd[1]: Starting firewalld -
Sep 05 11:24:08 centosstream9.linuxvmimages.local systemd[1]: Started firewalld -
[centos@centosstream9 ~]$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
[centos@centosstream9 ~]$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-sessio
n
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
[centos@centosstream9 ~]$
```

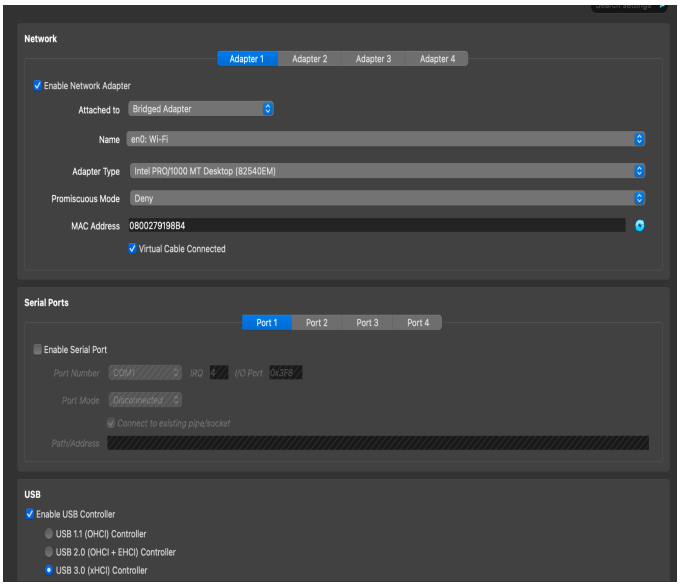
```
   `- Banned IP list:
[centos@centosstream9 ~]$ ssh -p 2222 user1@testsite.mydomain.local
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                    LINUXVMIMAGES.COM
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                User Name: centos
                Password:  centos (sudo su -)
user1@testsite.mydomain.local's password:
Permission denied, please try again.
user1@testsite.mydomain.local's password:
Permission denied, please try again.
user1@testsite.mydomain.local's password:
Received disconnect from 127.0.0.1 port 2222:2: Too many authentication failures
Disconnected from 127.0.0.1 port 2222
[centos@centosstream9 ~]$
```

```
sshd'
2025-09-05 11:24:08,308 fail2ban.jail          [3272]: INFO    Jail 'sshd' uses sy
stemd {}
2025-09-05 11:24:08,308 fail2ban.jail          [3272]: INFO    Initiated 'systemd'
backend
2025-09-05 11:24:08,309 fail2ban.filter        [3272]: INFO      maxLines: 1
2025-09-05 11:24:08,325 fail2ban.filtersystemd [3272]: INFO    [sshd] Added journa
l match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session'
2025-09-05 11:24:08,325 fail2ban.filter        [3272]: INFO      maxRetry: 3
2025-09-05 11:24:08,325 fail2ban.filter        [3272]: INFO      findtime: 600
2025-09-05 11:24:08,325 fail2ban.actions       [3272]: INFO      banTime: 3600
2025-09-05 11:24:08,325 fail2ban.filter        [3272]: INFO      encoding: UTF-8
2025-09-05 11:24:08,327 fail2ban.filtersystemd [3272]: INFO    [sshd] Jail is in o
peration now (process new journal entries)
2025-09-05 11:24:08,329 fail2ban.jail          [3272]: INFO    Jail 'sshd' started
2025-09-05 11:42:30,237 fail2ban.filter        [3272]: INFO    [sshd] Ignore 127.0
.0.1 by ignoreself rule
2025-09-05 11:42:34,118 fail2ban.filter        [3272]: INFO    [sshd] Ignore 127.0
.0.1 by ignoreself rule
2025-09-05 11:42:40,105 fail2ban.filter        [3272]: INFO    [sshd] Ignore 127.0
.0.1 by ignoreself rule
2025-09-05 11:42:41,368 fail2ban.filter        [3272]: INFO    [sshd] Ignore 127.0
.0.1 by ignoreself rule
centos@centosstream9 ~]$
```

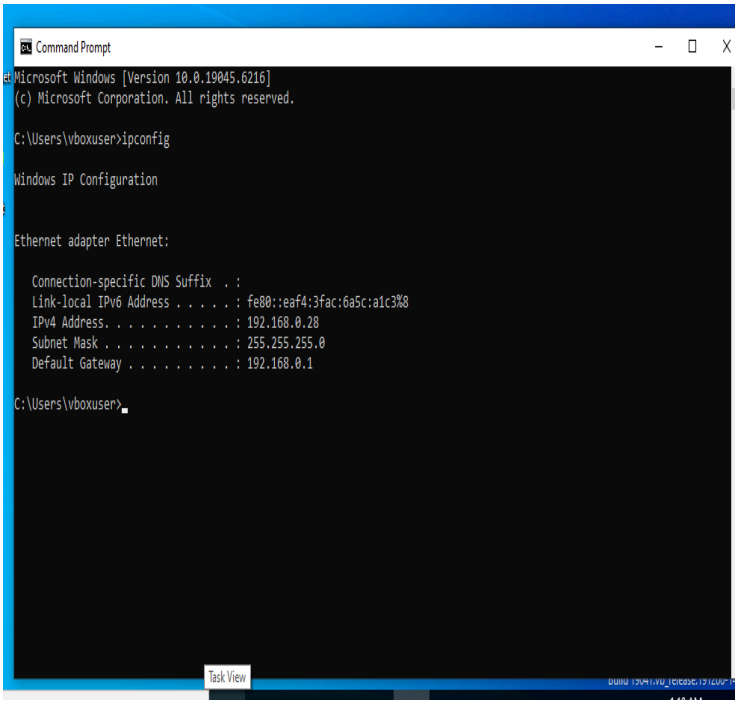
```
[centos@centosstream9 ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports: 2222/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[centos@centosstream9 ~]$ sudo firewall-cmd --list-ips
usage: 'firewall-cmd --help' for usage information or see firewall-cmd(1) man page
firewall-cmd: error: unrecognized arguments: --list-ips
[centos@centosstream9 ~]$ sudo firewall-cmd --list-all | grep banned
[centos@centosstream9 ~]$ sudo tail -n 50 /var/log/fail2ban.log
```

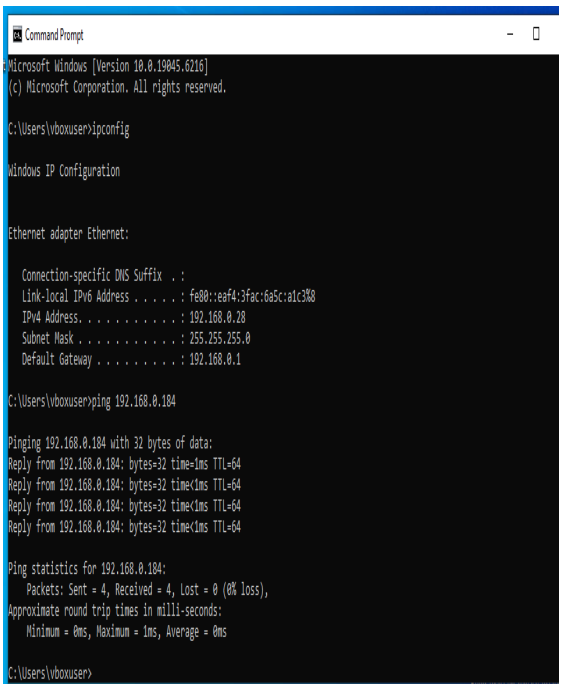
```
centos@centosstream9:~
[centos@centosstream9 ~]$ cat /var/log/fail2ban.log
cat: /var/log/fail2ban.log: Permission denied
[centos@centosstream9 ~]$ sudo cat /var/log/fail2ban.log
2025-09-04 06:09:26,818 fail2ban.server        [4042]: INFO    ----------------
------------------------------
2025-09-04 06:09:26,818 fail2ban.server        [4042]: INFO    Starting Fail2ban v
1.1.0
2025-09-04 06:09:26,819 fail2ban.observer      [4042]: INFO    Observer start...
2025-09-04 06:09:26,824 fail2ban.database      [4042]: INFO    Connected to fail2b
an persistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2025-09-04 06:09:26,825 fail2ban.database      [4042]: WARNING New database create
d. Version '4'
2025-09-04 06:21:53,449 fail2ban.transmitter   [4042]: ERROR   Command ['status',
'sshd'] has failed. Received UnknownJailException('sshd')
2025-09-04 06:40:32,834 fail2ban.server        [4042]: INFO    Shutdown in progres
s...
2025-09-04 06:40:32,835 fail2ban.observer      [4042]: INFO    Observer stop ... t
ry to end queue 5 seconds
2025-09-04 06:40:32,858 fail2ban.observer      [4042]: INFO    Observer stopped, 0
 events remaining.
2025-09-04 06:40:32,917 fail2ban.server        [4042]: INFO    Stopping all jails
2025-09-04 06:40:32,917 fail2ban.database      [4042]: INFO    Connection to datab
ase closed.
2025-09-04 06:40:32,917 fail2ban.server        [4042]: INFO    Exiting Fail2ban
```

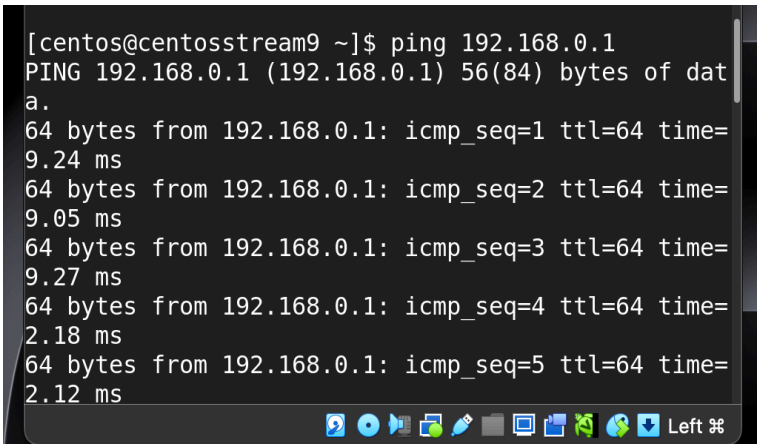
Manual Attack

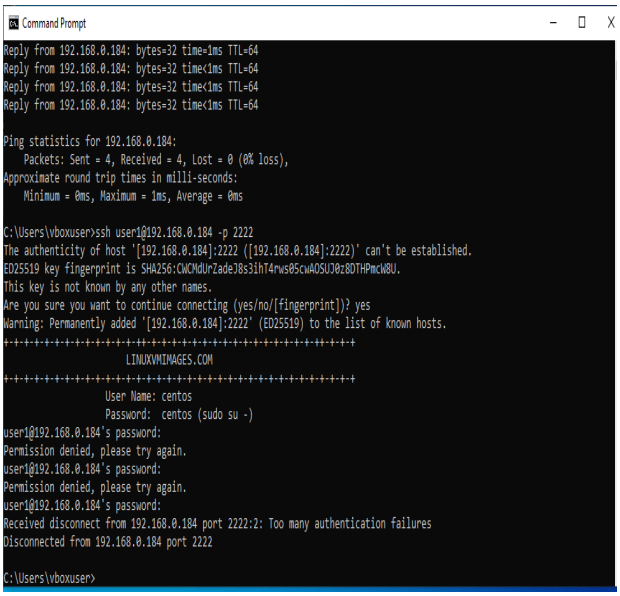



```
centos@centosstream9:~
[centos@centosstream9 ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
ult qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:53:e7:0d brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.184/24 brd 192.168.0.255 scope global dynamic noprefixroute
 enp0s3
       valid_lft 6653sec preferred_lft 6653sec
    inet6 fe80::a00:27ff:fe53:e70d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[centos@centosstream9 ~]$
```


Command Prompt
Microsoft Windows [Version 10.0.19045.6216]
(c) Microsoft Corporation. All rights reserved.
C:\Users\vboxuser>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::eaf4:3fac:6a5c:a1c3%8
IPv4 Address. . . . . : 192.168.0.28
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
C:\Users\vboxuser>
Task View


Command Prompt
Microsoft Windows [Version 10.0.19045.6216]
(c) Microsoft Corporation. All rights reserved.
C:\Users\vboxuser>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::eaf4:3fac:6a5c:a1c3%8
IPv4 Address. . . . . : 192.168.0.28
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
C:\Users\vboxuser>ping 192.168.0.184
Pinging 192.168.0.184 with 32 bytes of data:
Reply from 192.168.0.184: bytes=32 time=1ms TTL=64
Reply from 192.168.0.184: bytes=32 time<1ms TTL=64
Reply from 192.168.0.184: bytes=32 time<1ms TTL=64
Reply from 192.168.0.184: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.0.184:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\vboxuser>


[centos@centosstream9 ~]$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of dat
a.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=
9.24 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=
9.05 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=
9.27 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=
2.18 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=
2.12 ms
Left ⌘

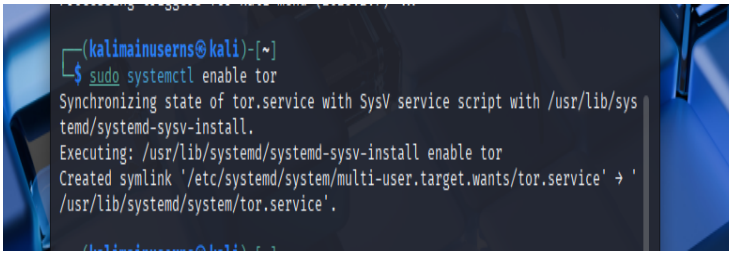

Command Prompt
Reply from 192.168.0.184: bytes=32 time=1ms TTL=64
Reply from 192.168.0.184: bytes=32 time<1ms TTL=64
Reply from 192.168.0.184: bytes=32 time<1ms TTL=64
Reply from 192.168.0.184: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.0.184:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\vboxuser>ssh user1@192.168.0.184 -p 2222
The authenticity of host '[192.168.0.184]:2222 ([192.168.0.184]:2222)' can't be established.
ED25519 key fingerprint is SHA256:CWCMdUrZadeJ8s3ihT4rws05cwAOSU0z8DTHPmcW8U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.0.184]:2222' (ED25519) to the list of known hosts.
LINUXVMIMAGES.COM
User Name: centos
Password: centos (sudo su -)
user1@192.168.0.184's password:
Permission denied, please try again.
user1@192.168.0.184's password:
Permission denied, please try again.
user1@192.168.0.184's password:
Received disconnect from 192.168.0.184 port 2222:2: Too many authentication failures
Disconnected from 192.168.0.184 port 2222
C:\Users\vboxuser>

```
centos@centosstream9:~
[centos@centosstream9 ~]$ sudo fail2ban-client sta
tus sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 1
|  |- Total failed:     4
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service
 + _COMM=sshd + _COMM=sshd-session
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.0.28
[centos@centosstream9 ~]$
```

```
C:\Users\vboxuser>ssh user1@192.168.0.184 -p 2222
ssh: connect to host 192.168.0.184 port 2222: Connection timed out
```

Pen Testing using Kali and Tor


```
(kalimainuserns㉿kali)-[~]
$ sudo apt install tor
Installing:
  tor

Installing dependencies:
  libtorsocks  tor-geoipdb  torsocks

Suggested packages:
  mixmaster  torbrowser-launcher  apparmor-utils  nyx  obfs4proxy

Summary:
  Upgrading: 0, Installing: 4, Removing: 0, Not Upgrading: 943
  Download size: 4,563 kB
  Space needed: 26.6 MB / 8,635 MB available

Continue? [Y/n] yes
```




```
(kalimainuserns㉿kali)-[~]
$ sudo apt install proxychains
Installing:
  proxychains

Installing dependencies:
  libproxychains3

Summary:
  Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 943
  Download size: 22.7 kB
  Space needed: 74.8 kB / 8,608 MB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libproxychains3 amd64
 3.1-9+b2 [13.6 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 proxychains all 3.1-9
 [9,140 B]
Fetched 22.7 kB in 1s (20.0 kB/s)
Selecting previously unselected package libproxychains3:amd64.
(Reading database ... 411997 files and directories currently installed.)
Preparing to unpack .../libproxychains3_3.1-9+b2_amd64.deb ...
Unpacking libproxychains3:amd64 (3.1-9+b2) ...
Selecting previously unselected package proxychains.
Preparing to unpack .../proxychains_3.1-9_all.deb ...
```

```
┌──(kalimainuserns㉿kali)-[~]
└─$ sudo nano /etc/proxychains.conf

┌──(kalimainuserns㉿kali)-[~]
└─$ sudo cat /etc/proxychains.conf
# proxychains.conf  VER 3.1
#
#        HTTP, SOCKS4, SOCKS5 tunneling proxifier with DNS
```

```
tcp_connect_time_out 8000

# ProxyList format
#       type  host  port [user pass]
#       (values separated by 'tab' or 'blank')
#
#
#        Examples:
#
#               socks5  192.168.67.78   1080    lamer   secret
#               http    192.168.89.3    8080    justu   hidden
#               socks4  192.168.1.49    1080
#               http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
```

```
  0          60572      26512/tor

┌──(kalimainuserns㉿kali)-[~]
└─$ proxychains curl https://check.torproject.org/
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  check.torproject.org:443  ...  OK
<!doctype html>
<html lang="en_US">
<head>
  <meta charset="utf-8" />
  <meta name="viewport" content="width=device-width, initial-scale=1.0" />
  <title>

      Congratulations. This browser is configured to use Tor.

</title>
  <link rel="icon" type="image/x-icon" href="/torcheck/img/tor-not.png" />
  <style>
    html { height: 100%; }
```

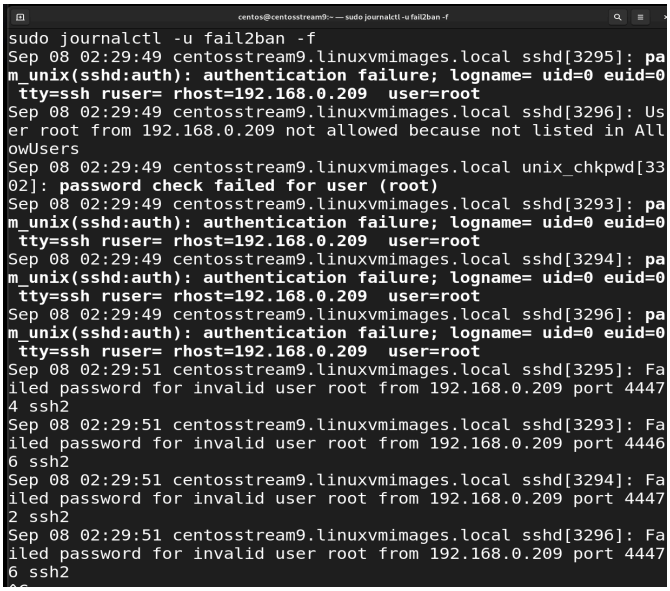
```
┌──(kalimainuserns㉿kali)-[~]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz

┌──(kalimainuserns㉿kali)-[~]
└─$
```

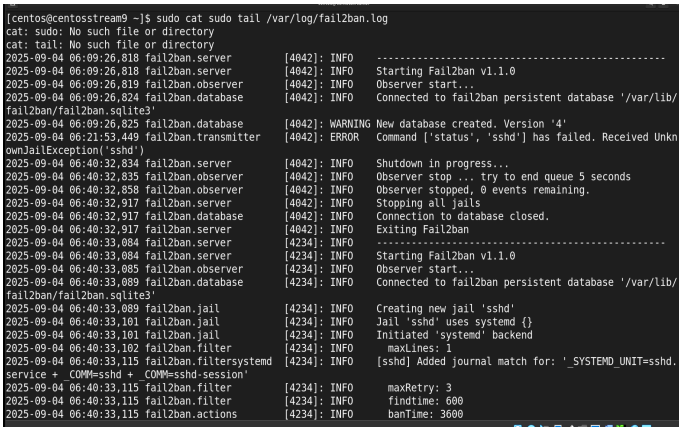
```
kalimainuserns@kali: ~
File  Actions  Edit  View  Help
┌──(kalimainuserns㉿kali)-[~]
└─$ nano ~/usernames.txt

┌──(kalimainuserns㉿kali)-[~]
└─$ cat ~/usernames.txt
root
admin
kali

┌──(kalimainuserns㉿kali)-[~]
└─$
```

```
centos@192.168.0.184's password:

┌──(kalimainuserns㉿kali)-[~]
└─$ hydra -L ~/usernames.txt -P /usr/share/wordlists/rockyou.txt ssh://192.168.0.184 -s 2222 -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 2025-09-08 02:29:25
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43033197 login tries (l:3/p:14344399), ~10758300 tries per task
[DATA] attacking ssh://192.168.0.184:2222/
[STATUS] 12.00 tries/min, 12 tries in 00:01h, 43033185 to do in 59768:19h, 4 active
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-08 02:31:33

┌──(kalimainuserns㉿kali)-[~]
└─$
```

```
[centos@centosstream9 ~]$ sudo tail -f /var/log/secure
Sep  8 02:29:49 centosstream9 unix_chkpwd[3302]: password check
failed for user (root)
Sep  8 02:29:49 centosstream9 sshd[3293]: pam_unix(sshd:auth): a
uthentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhos
t=192.168.0.209  user=root
Sep  8 02:29:49 centosstream9 sshd[3294]: pam_unix(sshd:auth): a
uthentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhos
t=192.168.0.209  user=root
Sep  8 02:29:49 centosstream9 unix_chkpwd[3304]: password check
failed for user (root)
Sep  8 02:29:49 centosstream9 sshd[3296]: pam_unix(sshd:auth): a
uthentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhos
t=192.168.0.209  user=root
Sep  8 02:29:51 centosstream9 sshd[3295]: Failed password for in
valid user root from 192.168.0.209 port 44474 ssh2
Sep  8 02:29:51 centosstream9 sshd[3293]: Failed password for in
valid user root from 192.168.0.209 port 44466 ssh2
Sep  8 02:29:51 centosstream9 sshd[3294]: Failed password for in
valid user root from 192.168.0.209 port 44472 ssh2
Sep  8 02:29:51 centosstream9 sshd[3296]: Failed password for in
valid user root from 192.168.0.209 port 44476 ssh2
Sep  8 02:30:22 centosstream9 sudo[3283]: pam_unix(sudo:session)
: session closed for user root
Sep  8 02:30:26 centosstream9 sudo[3328]:  centos : TTY=pts/0 ;
PWD=/home/centos ; USER=root ; COMMAND=/bin/tail -f /var/log/sec
ure
Sep  8 02:30:26 centosstream9 sudo[3328]: pam_unix(sudo:session)
: session opened for user root(uid=0) by centos(uid=1000)
^C
```

```
^C
[centos@centosstream9 ~]$ sudo journalctl -u sshd -f
sudo journalctl -u fail2ban -f
Sep 08 02:29:49 centosstream9.linuxvmimages.local sshd[3295]: pa
m_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
 tty=ssh ruser= rhost=192.168.0.209  user=root
Sep 08 02:29:49 centosstream9.linuxvmimages.local sshd[3296]: Us
er root from 192.168.0.209 not allowed because not listed in All
owUsers
Sep 08 02:29:49 centosstream9.linuxvmimages.local unix_chkpwd[33
02]: password check failed for user (root)
Sep 08 02:29:49 centosstream9.linuxvmimages.local sshd[3293]: pa
m_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
 tty=ssh ruser= rhost=192.168.0.209  user=root
Sep 08 02:29:49 centosstream9.linuxvmimages.local sshd[3294]: pa
m_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
 tty=ssh ruser= rhost=192.168.0.209  user=root
Sep 08 02:29:49 centosstream9.linuxvmimages.local sshd[3296]: pa
m_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
 tty=ssh ruser= rhost=192.168.0.209  user=root
Sep 08 02:29:51 centosstream9.linuxvmimages.local sshd[3295]: Fa
iled password for invalid user root from 192.168.0.209 port 4447
4 ssh2
Sep 08 02:29:51 centosstream9.linuxvmimages.local sshd[3293]: Fa
iled password for invalid user root from 192.168.0.209 port 4446
6 ssh2
Sep 08 02:29:51 centosstream9.linuxvmimages.local sshd[3294]: Fa
iled password for invalid user root from 192.168.0.209 port 4447
2 ssh2
Sep 08 02:29:51 centosstream9.linuxvmimages.local sshd[3296]: Fa
iled password for invalid user root from 192.168.0.209 port 4447
```





```
2025-09-06 04:36:36,715 fail2ban.database        [1159]: INFO    Connected to fail2ban persistent database '/var/lib/
fail2ban/fail2ban.sqlite3'
2025-09-06 04:36:36,716 fail2ban.jail            [1159]: INFO    Creating new jail 'sshd'
2025-09-06 04:36:36,737 fail2ban.jail            [1159]: INFO    Jail 'sshd' uses systemd {}
2025-09-06 04:36:36,756 fail2ban.jail            [1159]: INFO    Initiated 'systemd' backend
2025-09-06 04:36:36,761 fail2ban.filter          [1159]: INFO      maxLines: 1
2025-09-06 04:36:36,825 fail2ban.filtersystemd   [1159]: INFO    [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.
service + _COMM=sshd + _COMM=sshd-session'
2025-09-06 04:36:36,830 fail2ban.filter          [1159]: INFO      maxRetry: 3
2025-09-06 04:36:36,830 fail2ban.filter          [1159]: INFO      findtime: 600
2025-09-06 04:36:36,830 fail2ban.actions         [1159]: INFO      banTime: 3600
2025-09-06 04:36:36,830 fail2ban.filter          [1159]: INFO      encoding: UTF-8
2025-09-06 04:36:36,832 fail2ban.filtersystemd   [1159]: INFO    [sshd] Jail is in operation now (process new journal
 entries)
2025-09-06 04:36:36,836 fail2ban.jail            [1159]: INFO    Jail 'sshd' started
2025-09-06 04:51:57,725 fail2ban.filter          [1159]: INFO    [sshd] Found 192.168.0.28 - 2025-09-06 04:51:57
2025-09-06 04:52:04,838 fail2ban.filter          [1159]: INFO    [sshd] Found 192.168.0.28 - 2025-09-06 04:52:04
2025-09-06 04:52:10,109 fail2ban.filter          [1159]: INFO    [sshd] Found 192.168.0.28 - 2025-09-06 04:52:09
2025-09-06 04:52:10,578 fail2ban.actions         [1159]: NOTICE  [sshd] Ban 192.168.0.28
2025-09-06 04:52:11,606 fail2ban.filter          [1159]: INFO    [sshd] Found 192.168.0.28 - 2025-09-06 04:52:11
2025-09-06 05:52:09,701 fail2ban.actions         [1159]: NOTICE  [sshd] Unban 192.168.0.28
2025-09-07 02:45:26,812 fail2ban.server          [1165]: INFO    --------------------------------------------------
2025-09-07 02:45:26,820 fail2ban.server          [1165]: INFO    Starting Fail2ban v1.1.0
2025-09-07 02:45:26,820 fail2ban.observer        [1165]: INFO    Observer start...
2025-09-07 02:45:26,831 fail2ban.database        [1165]: INFO    Connected to fail2ban persistent database '/var/lib/
fail2ban/fail2ban.sqlite3'
2025-09-07 02:45:26,833 fail2ban.jail            [1165]: INFO    Creating new jail 'sshd'
2025-09-07 02:45:26,870 fail2ban.jail            [1165]: INFO    Jail 'sshd' uses systemd {}
2025-09-07 02:45:26,871 fail2ban.jail            [1165]: INFO    Initiated 'systemd' backend
2025-09-07 02:45:26,873 fail2ban.filter          [1165]: INFO      maxLines: 1
2025-09-07 02:45:26,925 fail2ban.filtersystemd   [1165]: INFO    [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.
```

```
2025-09-08 02:04:28,440 fail2ban.filtersystemd   [1183]: INFO    [sshd] Jail is in operation now (process new journa
 entries)
2025-09-08 02:04:28,454 fail2ban.jail            [1183]: INFO    Jail 'sshd' started
2025-09-08 02:27:57,956 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:27:57
2025-09-08 02:29:49,323 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:49
2025-09-08 02:29:49,528 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:49
2025-09-08 02:29:49,850 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:49
2025-09-08 02:29:49,851 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:49
2025-09-08 02:29:49,854 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:49
2025-09-08 02:29:49,884 fail2ban.actions         [1183]: NOTICE  [sshd] Ban 192.168.0.209
2025-09-08 02:29:51,851 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:51
2025-09-08 02:29:51,853 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:51
2025-09-08 02:29:51,854 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:51
2025-09-08 02:29:51,854 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:51
[centos@centosstream9 ~]$ sudo tail -f /var/log/fail2ban.log
2025-09-08 02:29:49,323 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:49
2025-09-08 02:29:49,528 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:49
2025-09-08 02:29:49,850 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:49
2025-09-08 02:29:49,851 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:49
2025-09-08 02:29:49,854 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:49
2025-09-08 02:29:49,884 fail2ban.actions         [1183]: NOTICE  [sshd] Ban 192.168.0.209
2025-09-08 02:29:51,851 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:51
2025-09-08 02:29:51,853 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:51
2025-09-08 02:29:51,854 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:51
2025-09-08 02:29:51,854 fail2ban.filter          [1183]: INFO    [sshd] Found 192.168.0.209 - 2025-09-08 02:29:51
^C
```

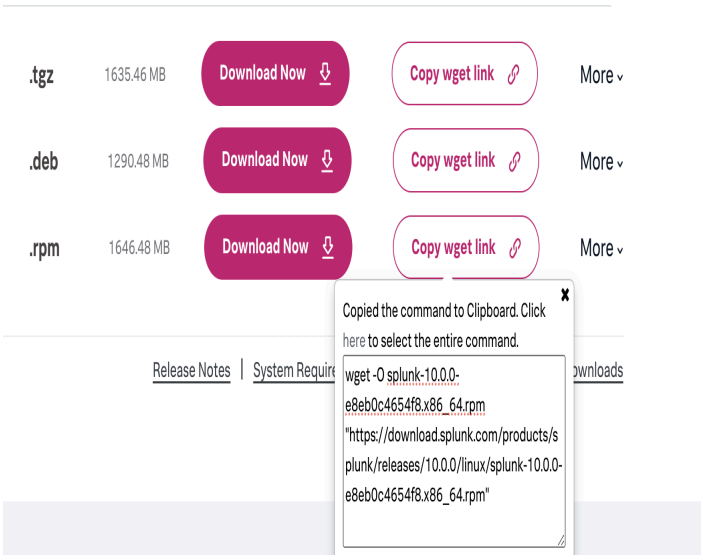
Automating Log Analysis

```
 GNU nano 5.6.1                    /home/centos/ssh_attack_report.sh
#!/bin/bash

REPORT_DIR="/var/reports"
LOG_FILE="/var/log/secure"
REPORT_FILE="$REPORT_DIR/ssh_attack_report_$(date +%F).txt"
TMP_IP_LIST="/tmp/ssh_failed_ips.txt"

mkdir -p $REPORT_DIR

# Extract all unique IPs with failed SSH logins
# wrong -->  grep "Failed password" $LOG_FILE | awk '{print $(NF-3)}' | sort | uniq > $TMP_IP_LIST
grep "Failed password" $LOG_FILE | awk '{print $(NF-3)}' | egrep '([0-9]{1,3}\.){3}[0-9]{1,3}' | sort | uniq > $TMP_IP_LIST

echo "SSH Attack Report (All-Time)" > $REPORT_FILE
echo "----------------------------------------" >> $REPORT_FILE
echo "Unique attacking IPs:" >> $REPORT_FILE
cat $TMP_IP_LIST >> $REPORT_FILE
echo "" >> $REPORT_FILE

for ip in $(cat $TMP_IP_LIST); do
  attempts=$(grep "$ip" $LOG_FILE | grep "Failed password" | wc -l)
  echo "IP: $ip | Attempts: $attempts" >> $REPORT_FILE
done

echo "" >> $REPORT_FILE
                                [ Read 27 lines ]
```

```
[centos@centosstream9 ~]$ chmod +x ~/ssh_attack_report.sh
chmod: changing permissions of '/home/centos/ssh_attack_report.sh': Operation not permitted
[centos@centosstream9 ~]$ sudo chmod +x ~/ssh_attack_report.sh
[centos@centosstream9 ~]$
```

```
[centos@centosstream9 /]$ sudo nano ~/ssh_attack_report.sh
[centos@centosstream9 /]$ sudo ~/ssh_attack_report.sh
[centos@centosstream9 /]$ cat /var/reports/ssh_attack_report_2025-09-08.txt
SSH Attack Report (All-Time)
----------------------------------------
Unique attacking IPs:
127.0.0.1
192.168.0.209
192.168.0.28
COMMAND=/bin/grep

IP: 127.0.0.1 | Attempts: 7
IP: 192.168.0.209 | Attempts: 4
IP: 192.168.0.28 | Attempts: 3
IP: COMMAND=/bin/grep | Attempts: 1

Report generated at Mon Sep  8 06:42:24 AM EDT 2025
[centos@centosstream9 /]$
```

Integrating Logs with SIEM Tool

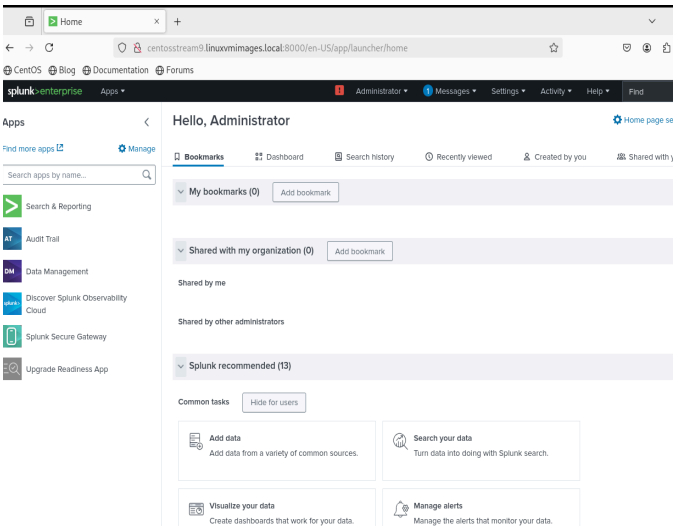


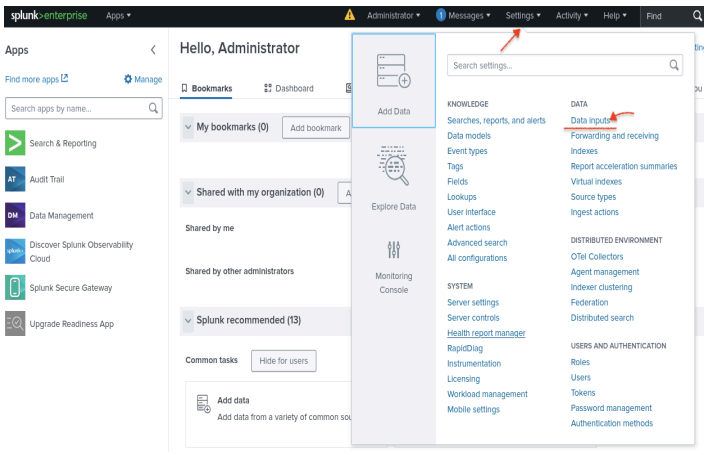

```
[centos@centosstream9 ~]$ wget -O splunk-10.0.0-e8eb0c4654f8.x86_64.rpm "https://do
wnload.splunk.com/products/splunk/releases/10.0.0/linux/splunk-10.0.0-e8eb0c4654f8.
x86_64.rpm"
--2025-09-08 10:48:23--  https://download.splunk.com/products/splunk/releases/10.0.
0/linux/splunk-10.0.0-e8eb0c4654f8.x86_64.rpm
Resolving download.splunk.com (download.splunk.com)... 18.66.57.35, 18.66.57.80, 18
.66.57.87, ...
Connecting to download.splunk.com (download.splunk.com)|18.66.57.35|:443... connect
ed.
HTTP request sent, awaiting response... 200 OK
Length: 1726454835 (1.6G) [binary/octet-stream]
Saving to: 'splunk-10.0.0-e8eb0c4654f8.x86_64.rpm'

splunk-10.0.0-e8eb0c 100%[===================>]   1.61G  21.1MB/s    in 82s

2025-09-08 10:49:47 (20.0 MB/s) - 'splunk-10.0.0-e8eb0c4654f8.x86_64.rpm' saved [17
26454835/1726454835]
```

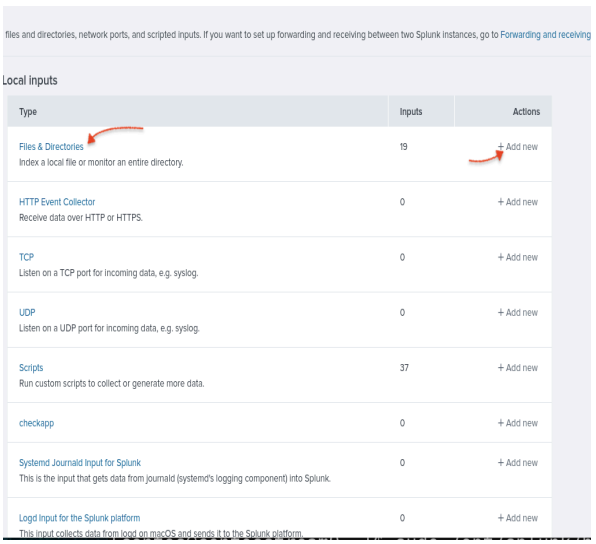
```
[centos@centosstream9 ~]$ ls
Desktop    Music     reports                          Templates
Documents  Pictures  splunk-10.0.0-e8eb0c4654f8.x86_64.rpm  Videos
Downloads  Public    ssh_attack_report.sh
[centos@centosstream9 ~]$ sudo rpm -ivh splunk-10.0.0-e8eb0c4654f8.x86_64.rpm
warning: splunk-10.0.0-e8eb0c4654f8.x86_64.rpm: Header V4 RSA/SHA256 Signature, key
 ID b3cd4420: NOKEY
Verifying...
```

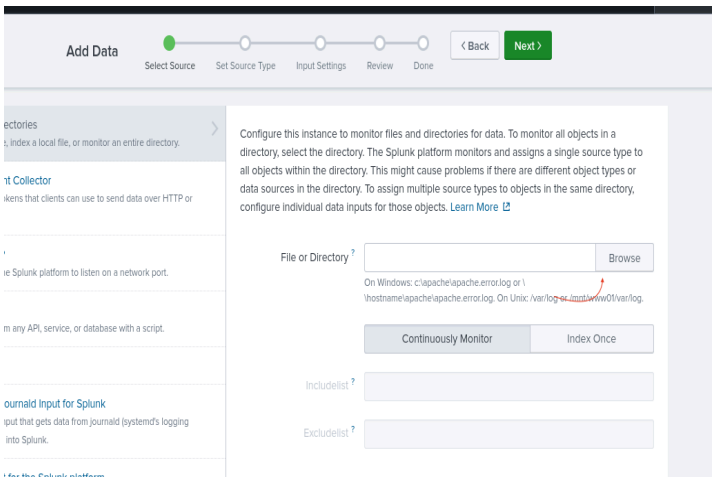
```
[centos@centosstream9 ~]$ sudo /opt/splunk/bin/splunk start --accept-license
systemctl: /opt/splunk/lib/libcrypto.so.3: version `OPENSSL_3.4.0' not found (requi
red by /usr/lib64/systemd/libsystemd-shared-252.so)

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.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
```

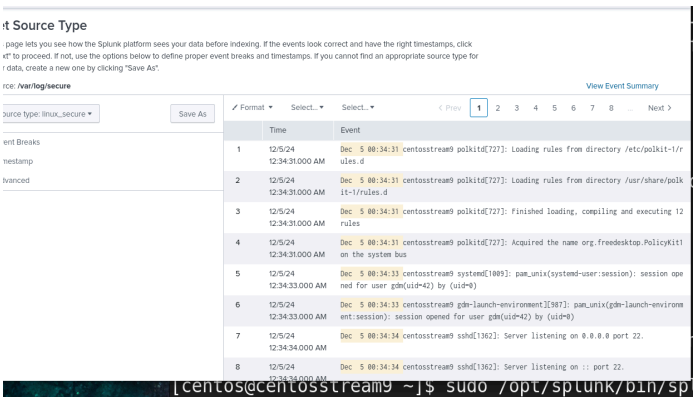
```
..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Warning: ignoring -extensions option without -extfile
Certificate request self-signature ok
subject=CN = centosstream9.linuxvmimages.local, O = SplunkUser
pDone


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://centosstream9.linuxvmimages.local:8000
```

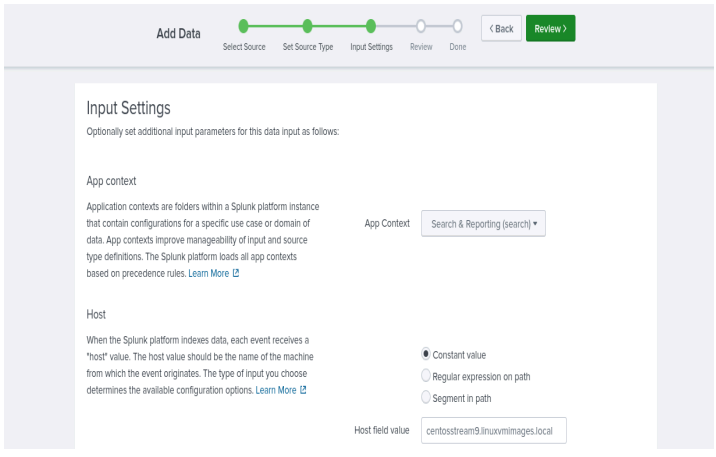


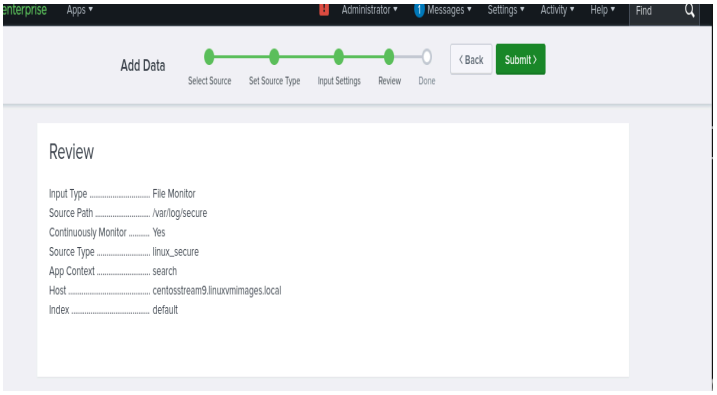

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Hello, Administrator
Search & Reporting
Audit Trail
Data Management
Discover Splunk Observability Cloud
Splunk Secure Gateway
Upgrade Readiness App
Bookmarks
Dashboard
My bookmarks (0)
Add bookmark
Shared with my organization (0)
Shared by me
Shared by other administrators
Splunk recommended (13)
Common tasks
Hide for users
Add data
Add Data
Explore Data
Monitoring Console
Search settings...
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Health report manager
RapidDiag
Instrumentation
Licensing
Workload management
Mobile settings
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Virtual indexes
Source types
Ingest actions
DISTRIBUTED ENVIRONMENT
OTel Collectors
Agent management
Indexer clustering
Federation
Distributed search
USERS AND AUTHENTICATION
Roles
Users
Tokens
Password management
Authentication methods

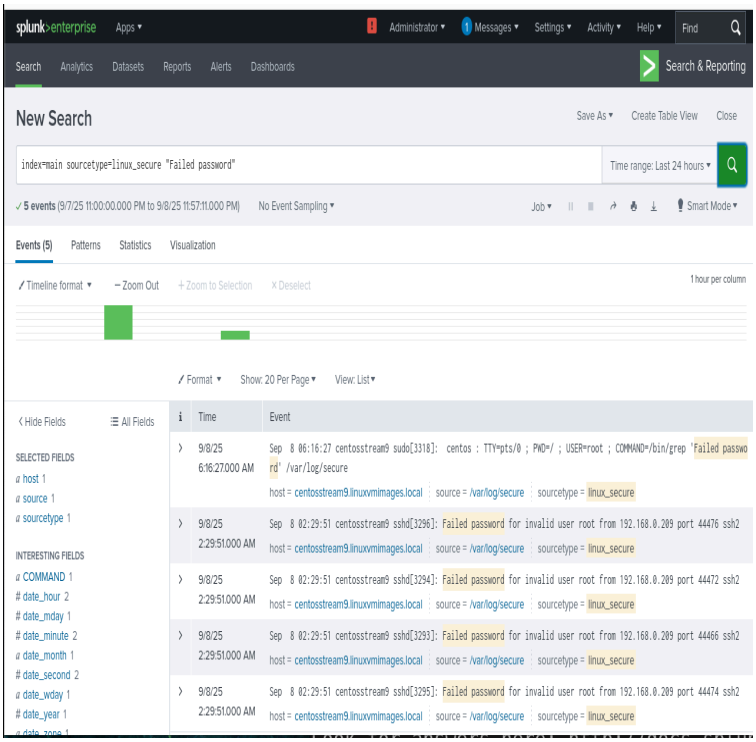

files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving
Local inputs
Type
Inputs
Actions
Files & Directories
Index a local file or monitor an entire directory.
19
+ Add new
HTTP Event Collector
Receive data over HTTP or HTTPS.
0
+ Add new
TCP
Listen on a TCP port for incoming data, e.g. syslog.
0
+ Add new
UDP
Listen on a UDP port for incoming data, e.g. syslog.
0
+ Add new
Scripts
Run custom scripts to collect or generate more data.
37
+ Add new
checkapp
0
+ Add new
Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.
0
+ Add new
Logd Input for the Splunk platform
This input collects data from logd on macOS and sends it to the Splunk platform.
0
+ Add new


Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More
File or Directory
Browse
On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.
Continuously Monitor
Index Once
Includelist
Excludelist


t Source Type
page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "t" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for data, create a new one by clicking "Save As".
rce: /var/log/secure
View Event Summary
Save As
Time
Event
[centos@centosstream9 ~]$ sudo /opt/splunk/bin/sp


Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Review
Input Settings
Optionally set additional input parameters for this data input as follows:
App context
Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More
App Context
Search & Reporting (search)
Host
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More
Constant value
Regular expression on path
Segment in path
Host field value
centosstream9.linuxvmimages.local


Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Submit
Review
Input Type ..... File Monitor
Source Path ..... /var/log/secure
Continuously Monitor ..... Yes
Source Type ..... linux_secure
App Context ..... search
Host centosstream9.linuxvmimages.local
Index ..... default


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 sourcetype=linux_secure "Failed password"
Time range: Last 24 hours
5 events (9/7/25 11:00:00.000 PM to 9/8/25 11:57:11.000 PM)
No Event Sampling
Job
Smart Mode
Events (5)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
COMMAND 1
date_hour 2
date_mday 1
date_minute 2
date_month 1
date_second 2
date_wday 1
date_year 1
Time
Event
9/8/25 6:16:27.000 AM
Sep 8 06:16:27 centosstream9 sudo[3318]: centos : TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=/bin/grep 'Failed password' /var/log/secure
host = centosstream9.linuxvmimages.local source = /var/log/secure sourcetype = linux_secure
9/8/25 2:29:51.000 AM
Sep 8 02:29:51 centosstream9 sshd[3296]: Failed password for invalid user root from 192.168.0.209 port 44476 ssh2
host = centosstream9.linuxvmimages.local source = /var/log/secure sourcetype = linux_secure
9/8/25 2:29:51.000 AM
Sep 8 02:29:51 centosstream9 sshd[3294]: Failed password for invalid user root from 192.168.0.209 port 44472 ssh2
host = centosstream9.linuxvmimages.local source = /var/log/secure sourcetype = linux_secure
9/8/25 2:29:51.000 AM
Sep 8 02:29:51 centosstream9 sshd[3293]: Failed password for invalid user root from 192.168.0.209 port 44466 ssh2
host = centosstream9.linuxvmimages.local source = /var/log/secure sourcetype = linux_secure
9/8/25 2:29:51.000 AM
Sep 8 02:29:51 centosstream9 sshd[3295]: Failed password for invalid user root from 192.168.0.209 port 44474 ssh2
host = centosstream9.linuxvmimages.local source = /var/log/secure sourcetype = linux_secure