

King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2

King Fahd University of Petroleum & Minerals



ICS 344: Information Security (242)

Term 242

Project-P2

MOHMAD ALMAHDOOD	s202034660
ALI ALABDULJABBAR	s202027280
ALI ALMATROOD	s202040180

SECTION 5

February 30, 2025

King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2

Contents

Phase 2: Visual Analysis with a SIEM Dashboard.....	3
Step 1: install the SIEM tool (Splunk).....	3
Step 2: configure Splunk universal forwarder	5
Step 3: attacking the metasploit3 ssh service using brute force.....	8
Step 4: log analysis and visualization.....	9
Step 5: analyze patterns	10
Step 6: visualization.....	11
Summary:	11

King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2

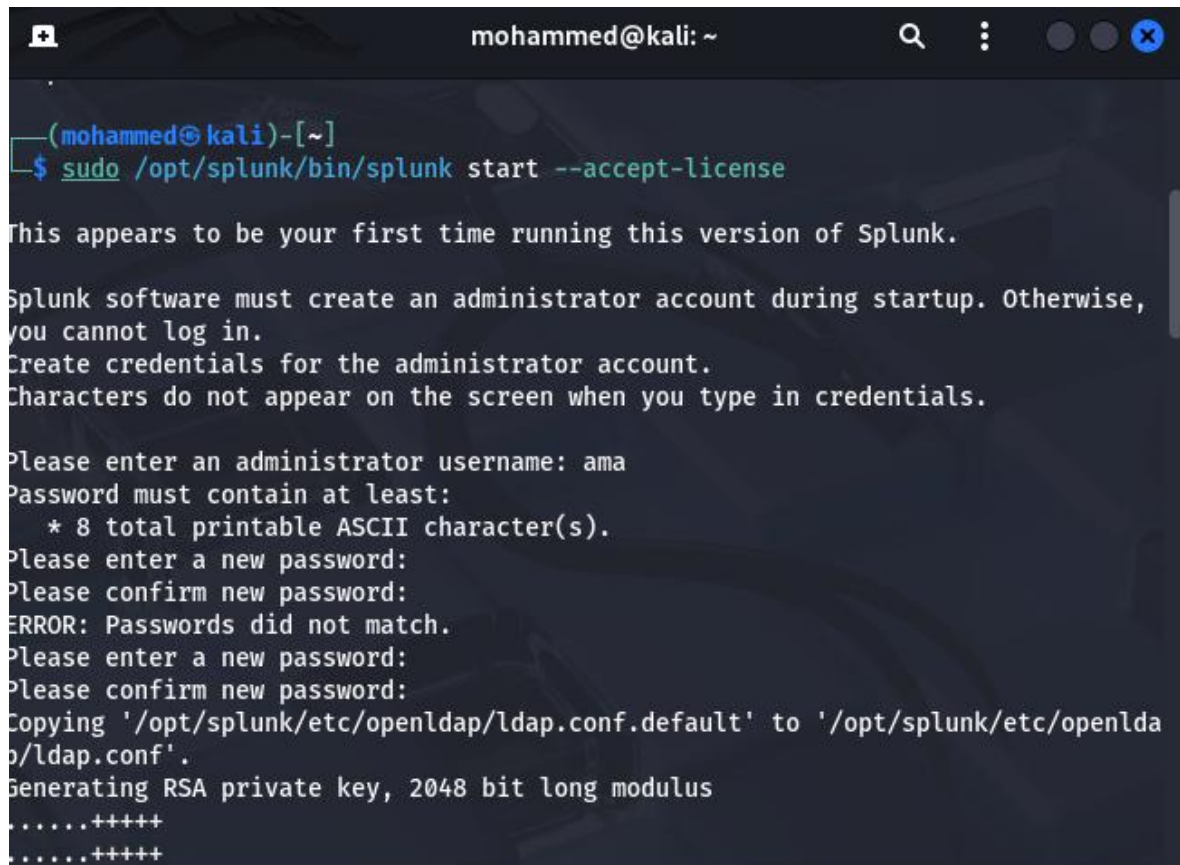
Phase 2: Visual Analysis with a SIEM Dashboard

Step 1: install the SIEM tool (Splunk)

```
(mohammed@kali)-[~]  
$ sudo dpkg -i splunk-*.deb  
(Reading database ... 500075 files and directories currently installed.)  
Preparing to unpack splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb ...  
This looks like an upgrade of an existing Splunk Server. Attempting to stop the  
installed Splunk Server...  
splunkd is not running.  
Unpacking splunk (9.3.2) over (9.3.2) ...  
Setting up splunk (9.3.2) ...  
complete
```

Step 1.1 start Splunk and choose admin name and password

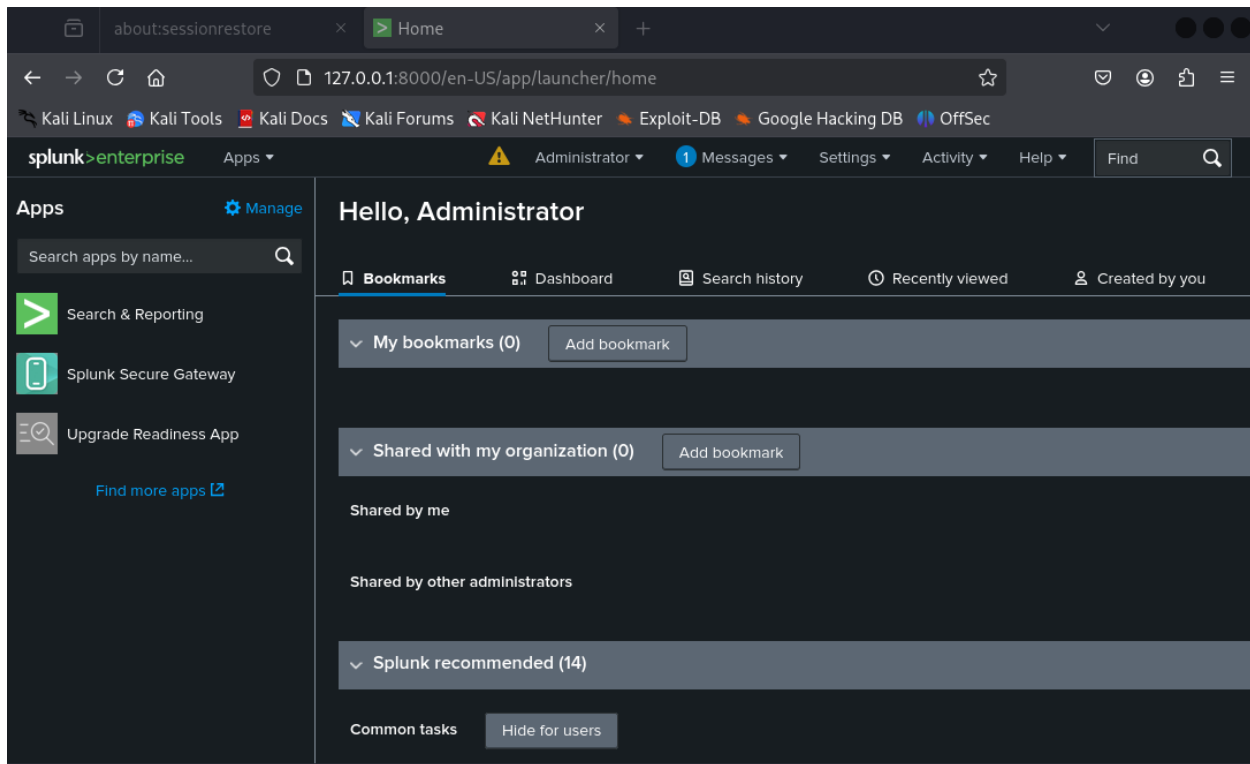
King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2

A terminal window titled 'mohammed@kali: ~' showing the execution of 'sudo /opt/splunk/bin/splunk start --accept-license'. The output indicates it's the first time running this version of Splunk, requiring administrator account creation. It prompts for a username (ama) and a password, which is confirmed. It then copies the default LDAP configuration and generates a 2048-bit RSA private key, represented by two lines of dots.

```
mohammed@kali: ~  
(mohammed@kali)-[~]  
$ sudo /opt/splunk/bin/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: ama  
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:  
Copying '/opt/splunk/etc/openldap/ldap.conf.default' to '/opt/splunk/etc/openlda  
p/ldap.conf'.  
Generating RSA private key, 2048 bit long modulus  
.....+++++  
.....+++++
```

Step 1.2: sign in to the Splunk server with the credentials we made

King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2



Step 2: configure Splunk universal forwarder

1. Install the Splunk universal forwarder on the metasploitable3 VM

```
Metasploitable3-ub1404 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
releases/9.1.2/linux/splunkforwarder-9.1.2-b6b9c8185839-linux-2.6-and64.deb
Resolving download.splunk.com (download.splunk.com)... 52.84.45.44, 52.84.45.15, ...
Connecting to download.splunk.com (download.splunk.com):52.84.45.44:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 33329822 (32M) [binary/octet-stream]
Saving to: 'splunkforwarder.deb'

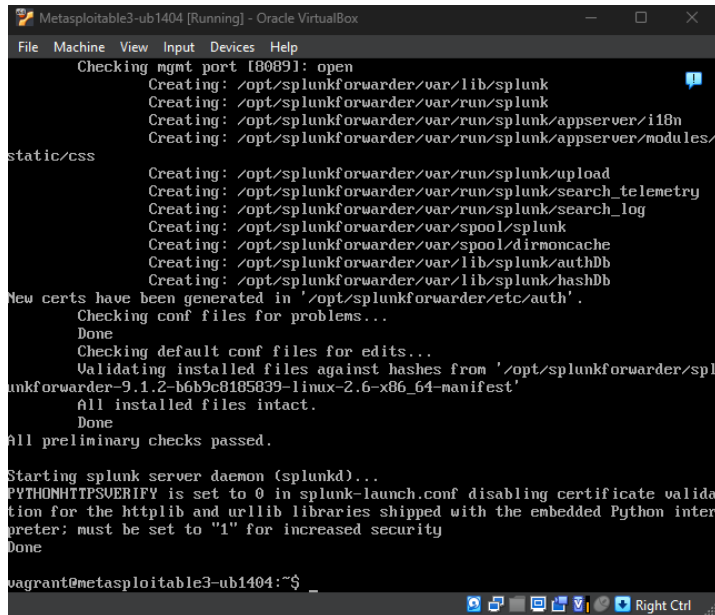
100%[=====>] 33,329,822  14.4MB/s   in 2.2s

2025-04-29 20:15:22 (14.4 MB/s) - 'splunkforwarder.deb' saved [33329822/33329822]

vagrant@metasploitable3-ub1404:~$ sudo dpkg -i splunkforwarder.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 127930 files and directories currently installed.)
Preparing to unpack splunkforwarder.deb ...
Unpacking splunkforwarder (9.1.2) ...
Setting up splunkforwarder (9.1.2) ...
complete
vagrant@metasploitable3-ub1404:~$ sudo apt-get -f install
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  amd64-microcode linux-modules-extra-3.13.0-170-generic
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 171 not upgraded.
vagrant@metasploitable3-ub1404:~$
```

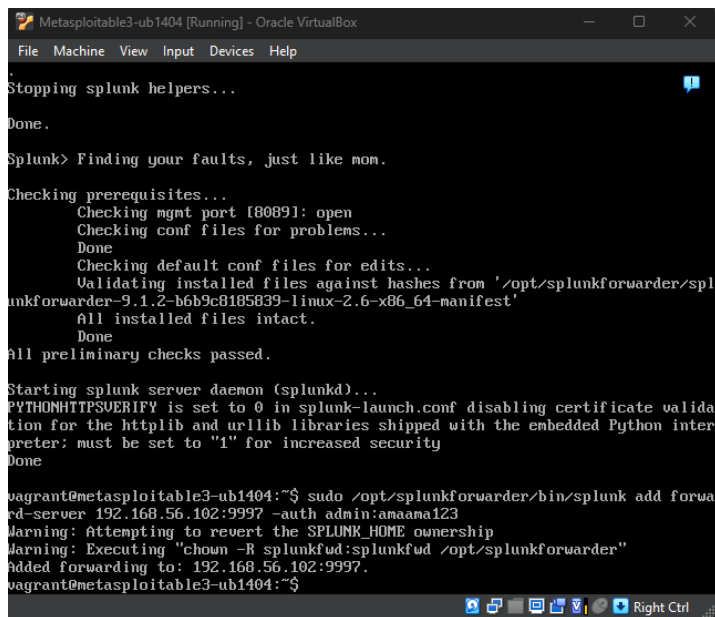
King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2

2. Start the Splunk universal forwarder and accept the licenses



```
Metasploitable3-ub1404 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
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
Creating: /opt/splunkforwarder/var/spool/splunk
Creating: /opt/splunkforwarder/var/spool/dirmoncache
Creating: /opt/splunkforwarder/var/lib/splunk/authDb
Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.1.2-b6b9c8185839-linux-2.6-x86_64-manifest'
All installed files intact.
Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done
vagrant@metasploitable3-ub1404:~$
```

3. Configure the forwarder to send data to our Splunk server



```
Metasploitable3-ub1404 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Stopping splunk helpers...
Done.
Splunk> Finding your faults, just like mom.
Checking prerequisites...
Checking mgmt port [8089]: open
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.1.2-b6b9c8185839-linux-2.6-x86_64-manifest'
All installed files intact.
Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.56.102:9997 -auth admin:anaana123
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added forwarding to: 192.168.56.102:9997.
vagrant@metasploitable3-ub1404:~$
```

King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2

4. Add the SSH authentication logs to be monitored

```
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log -sourcetype linux_secure
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/auth.log'.
vagrant@metasploitable3-ub1404:~$
```

5. Restart the Splunk forwarder to apply the changes and verify the forwarder is running

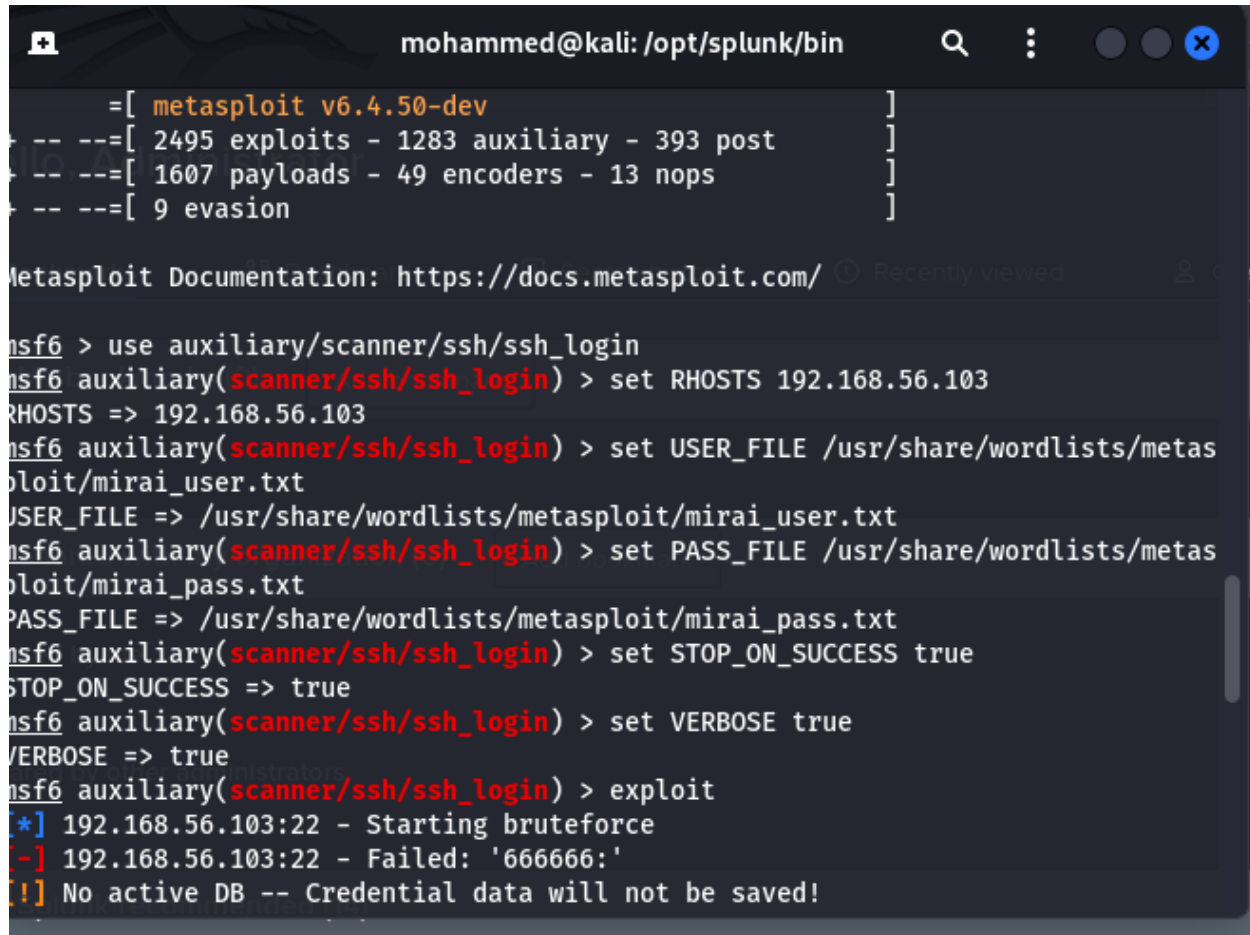
```
Metasploitable3-ub1404 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Stopping splunk helpers...
Done.
Splunk> Finding your faults, just like mom.
Checking prerequisites...
  Checking mgmt port [8089]: open
  Checking conf files for problems...
  Done
  Checking default conf files for edits...
  Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.1.2-b6b9c8185839-linux-2.6-x86_64-manifest'
  All installed files intact.
  Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done
vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk status
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
splunkd is running (PID: 2721).
splunk helpers are running (PIDs: 2722).
vagrant@metasploitable3-ub1404:~$

vagrant@metasploitable3-ub1404:~$ sudo /opt/splunkforwarder/bin/splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid. Please login.
Splunk username: admin
Password:
Active forwards:
  192.168.56.102:9997
Configured but inactive forwards:
  None
vagrant@metasploitable3-ub1404:~$
```

King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2

Step 3: attacking the metasploit3 ssh service using brute force

We will conduct the same attack in phase 1 to visualize the logs



```
mohammed@kali: /opt/splunk/bin

=[ metasploit v6.4.50-dev ]
-- --[ 2495 exploits - 1283 auxiliary - 393 post ]
-- --[ 1607 payloads - 49 encoders - 13 nops ]
-- --[ 9 evasion ]

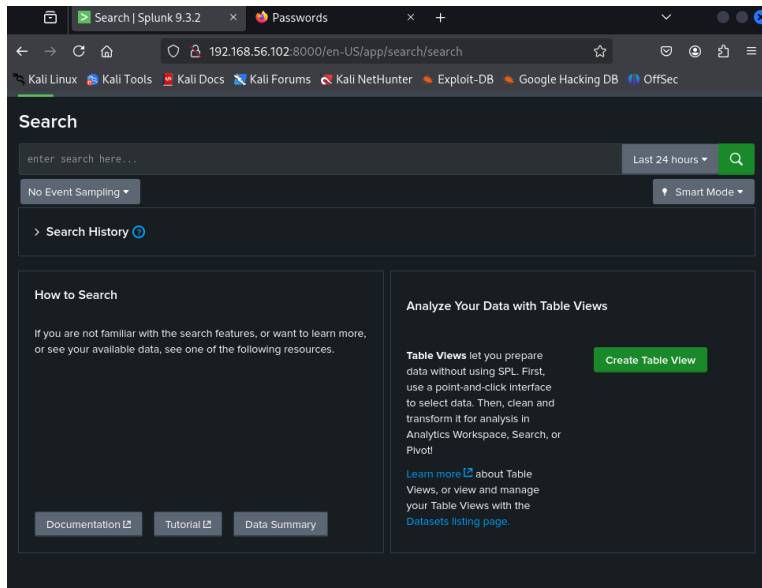
Metasploit Documentation: https://docs.metasploit.com/ Recently viewed

msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /usr/share/wordlists/metasploit/mirai_user.txt
USER_FILE => /usr/share/wordlists/metasploit/mirai_user.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/metasploit/mirai_pass.txt
PASS_FILE => /usr/share/wordlists/metasploit/mirai_pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] 192.168.56.103:22 - Starting bruteforce
[-] 192.168.56.103:22 - Failed: '666666:'
[!] No active DB -- Credential data will not be saved!
```

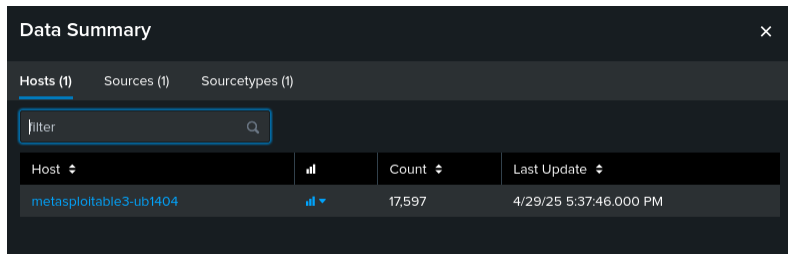

King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2

Step 4: log analysis and visualization

1. Open the search Splunk

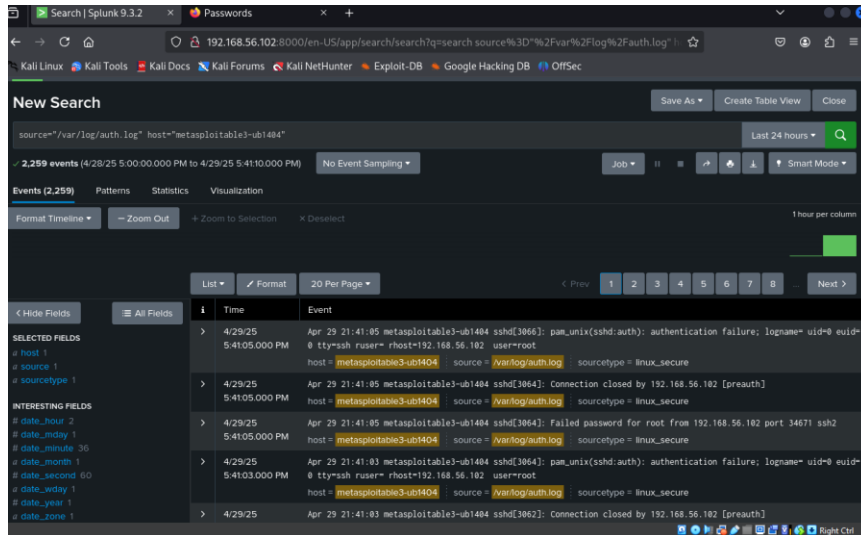


2. Chose data summary



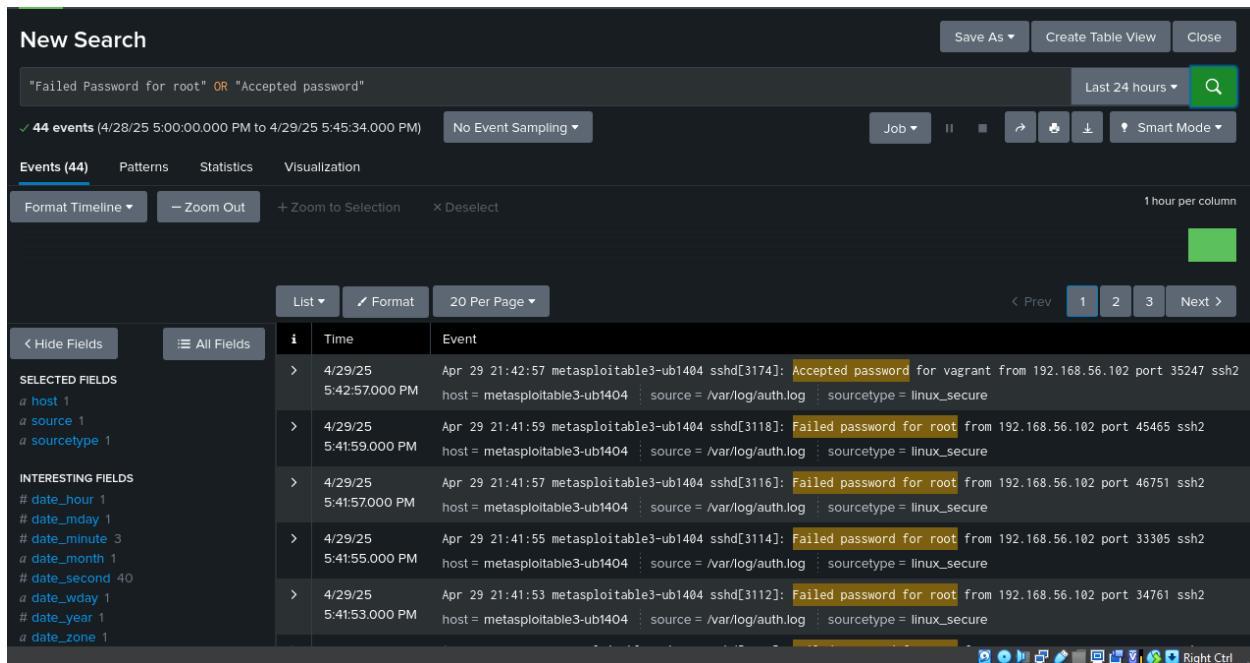
King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2

3. Chose the source and host to be metasploitable3 and var/log/auth.log



Step 5: analyze patterns

1. Make the search to show only failed passwords or accepted passwords

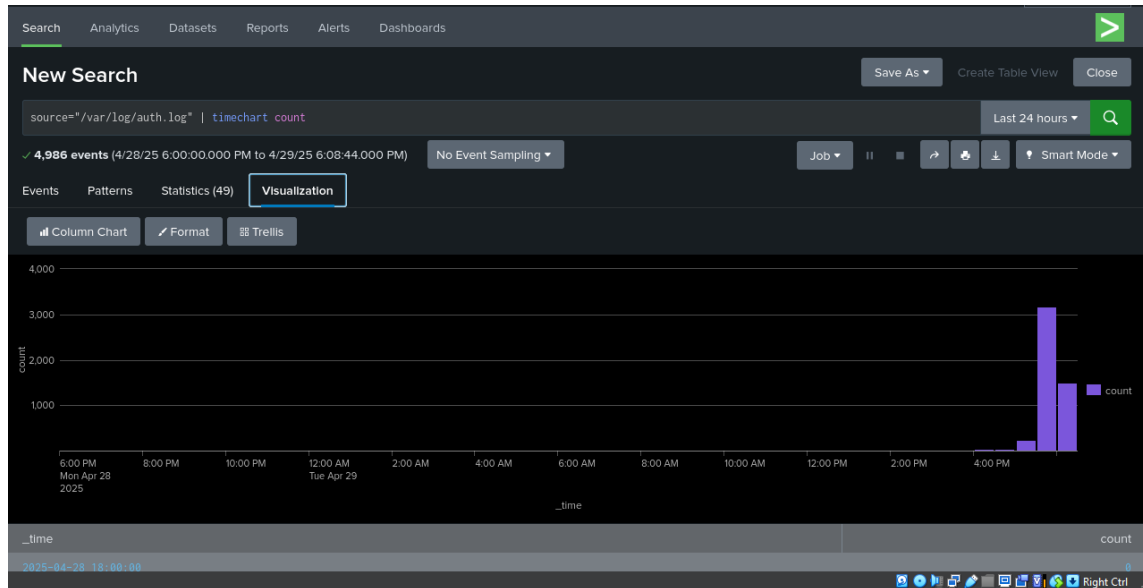


This will show only the logs for failed attempts and the only successful attempts.

King Fahd University of Petroleum & Minerals
College of Computing and Mathematics
ICS 344: Information Security (242)
Project-P2

Step 6: visualization

1. Set the timechart in the search query and click on visualization



The x axis shows the time and the y axis shows the count of logs registered

Summary:

In this phase we successfully downloaded Splunk to view the logs, configured the universal forwarder in the Metasploitable3 VM to forward all the ssh auth logs from the victim machine to the kali machine and can analyze, visualize the logs. Also, we can search for specific logs and search for specific patterns.