

ICS 344
TERM 242

TEAM PROJECT
GROUP 7

Mohammed Al Lail => ID/202152850

Ali almatar => ID/202158190

Hassan Al Nasser => ID/202163950

Phase 2

Logs

- Failed passwords

>	4/30/25 10:44:21.000 PM	May 1 02:44:21 metasploitable3-ub1404 sshd[2687]: Failed password for invalid user msfadmin from 192.168.1.10 port 46841 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:44:19.000 PM	May 1 02:44:19 metasploitable3-ub1404 sshd[2685]: Failed password for invalid user msfadmin from 192.168.1.10 port 44849 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:44:11.000 PM	May 1 02:44:11 metasploitable3-ub1404 sshd[2656]: Failed password for vagrant from 192.168.1.10 port 44215 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:44:08.000 PM	May 1 02:44:08 metasploitable3-ub1404 sshd[2654]: Failed password for invalid user admin from 192.168.1.10 port 42727 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:44:06.000 PM	May 1 02:44:06 metasploitable3-ub1404 sshd[2652]: Failed password for invalid user admin from 192.168.1.10 port 34677 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:44:03.000 PM	May 1 02:44:03 metasploitable3-ub1404 sshd[2650]: Failed password for invalid user admin from 192.168.1.10 port 46825 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:44:00.000 PM	May 1 02:44:00 metasploitable3-ub1404 sshd[2648]: Failed password for invalid user admin from 192.168.1.10 port 38067 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:43:58.000 PM	May 1 02:43:58 metasploitable3-ub1404 sshd[2646]: Failed password for invalid user admin from 192.168.1.10 port 36763 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:43:56.000 PM	May 1 02:43:56 metasploitable3-ub1404 sshd[2644]: Failed password for root from 192.168.1.10 port 40457 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:43:49.000 PM	May 1 02:43:49 metasploitable3-ub1404 sshd[2642]: Failed password for root from 192.168.1.10 port 33789 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:43:47.000 PM	May 1 02:43:47 metasploitable3-ub1404 sshd[2640]: Failed password for root from 192.168.1.10 port 34789 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:43:45.000 PM	May 1 02:43:45 metasploitable3-ub1404 sshd[2638]: Failed password for root from 192.168.1.10 port 44031 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog
>	4/30/25 10:43:43.000 PM	May 1 02:43:43 metasploitable3-ub1404 sshd[2636]: Failed password for root from 192.168.1.10 port 38695 ssh2
	host = metasploitable3-ub1404	source = /var/log/auth.log sourcetype = syslog

New Search

Save As

Create Table View

Close

index= source="/var/log/auth.log" "Failed password"

All time

Q

21 events (before 5/1/25 11:36:31.000 AM)

No Event Sampling

Job

Smart Mode

Events (21)

Patterns

Statistics

Visualization

Format Timeline

Zoom Out

Zoom to Selection

Deconstruct

1 second per column

List

Format

50 Per Page

Hide Fields

All Fields

SELECTED FIELDS

host 1

source 1

sourcetype 1

INTERESTING FIELDS

date_hour 1

date_minute 1

date_minute 2

date_month 1

date_second 21

date_year 1

date_zone 1

index 1

filecount 1

pid 21

process 1

product 2

spunk_server 1

timeendpos 1

timestartpos 1

Time

Event

> 4/30/25 10:44:39.000 PM May 1 02:44:39 metasploitable3-ub1404 sshd[2703]: Failed password for invalid user user from 192.168.1.10 port 48837 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog

> 4/30/25 10:44:36.000 PM May 1 02:44:36 metasploitable3-ub1404 sshd[2701]: Failed password for invalid user user from 192.168.1.10 port 38457 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog

> 4/30/25 10:44:34.000 PM May 1 02:44:34 metasploitable3-ub1404 sshd[2699]: Failed password for invalid user user from 192.168.1.10 port 41883 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog

> 4/30/25 10:44:32.000 PM May 1 02:44:32 metasploitable3-ub1404 sshd[2697]: Failed password for invalid user user from 192.168.1.10 port 43491 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog

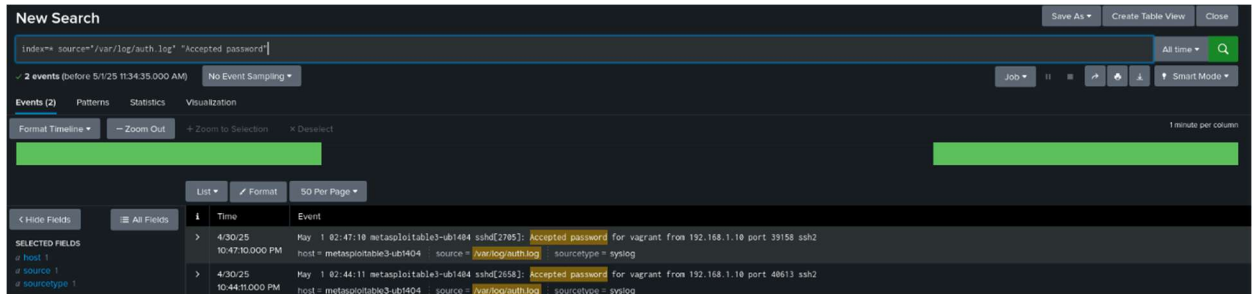
> 4/30/25 10:44:29.000 PM May 1 02:44:29 metasploitable3-ub1404 sshd[2695]: Failed password for invalid user user from 192.168.1.10 port 42613 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog

> 4/30/25 10:44:27.000 PM May 1 02:44:27 metasploitable3-ub1404 sshd[2693]: Failed password for invalid user msfadmin from 192.168.1.10 port 44133 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog

> 4/30/25 10:44:25.000 PM May 1 02:44:25 metasploitable3-ub1404 sshd[2691]: Failed password for invalid user msfadmin from 192.168.1.10 port 36771 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog

> 4/30/25 10:44:23.000 PM May 1 02:44:23 metasploitable3-ub1404 sshd[2689]: Failed password for invalid user msfadmin from 192.168.1.10 port 45217 ssh2 host = metasploitable3-ub1404 source = /var/log/auth.log sourcetype = syslog

- Accepted passwords



- Visualization

