Design Deception Solutions

Team ID: 11
Project ID: CS_EGCERT2_2023
UOttawa university

Presented by:
Salwa Youssef Attia Attia – 300389878
Fatma Mohamed Ahmed Ibrahim Basal - 300389394
Mayar Mohamed Saad Abdellatif - 300389363
Manar Abdallah Tawfik Ibrahim - 300389404

Project Problem Definition:

- Deploy automated decoys and honeypots.
- Implement Real-Time Alerting system
- Create Centralized Logging System

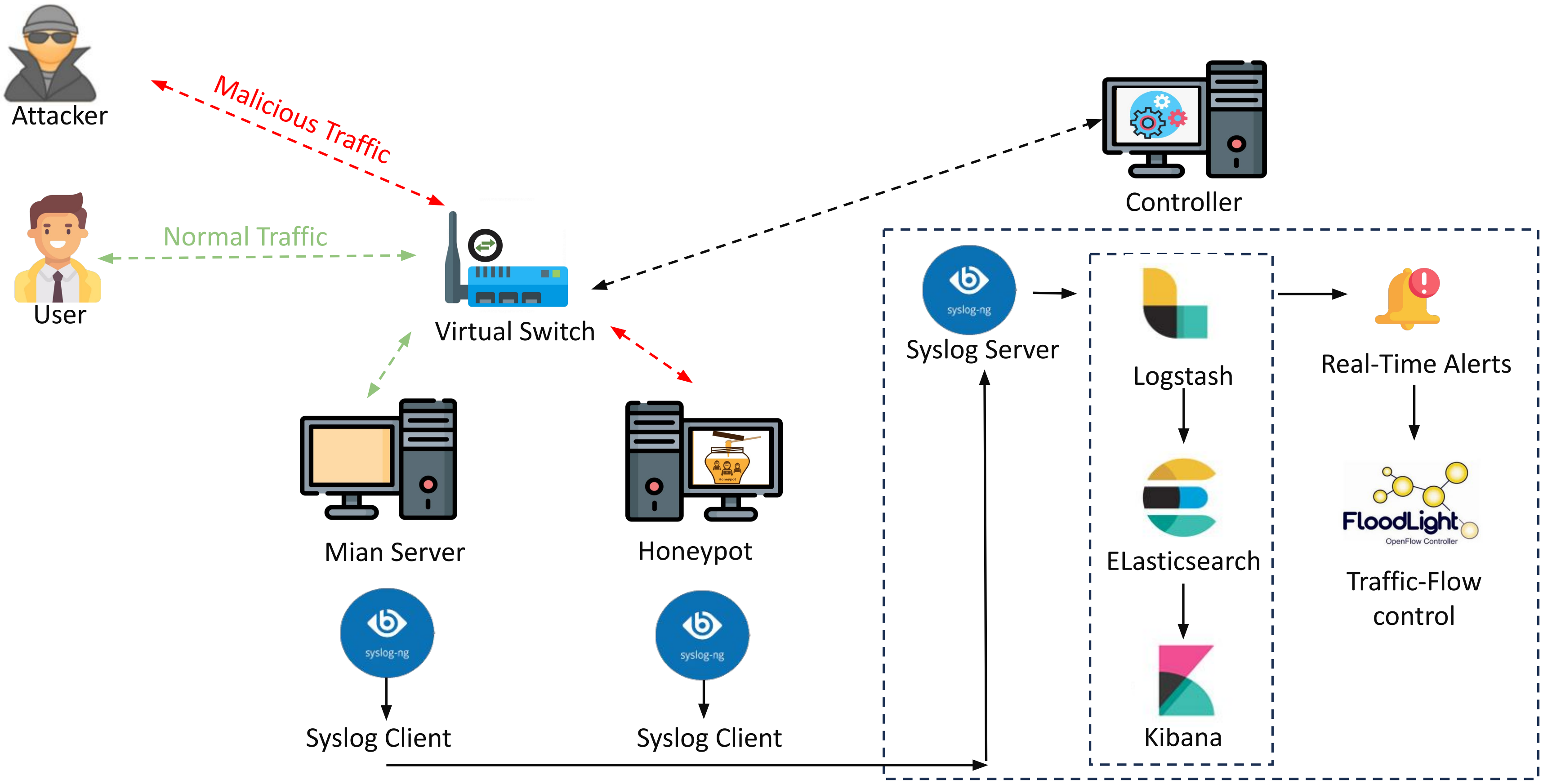
Potential Benefits to Sponsor/Users:

Identification of attackers

Real-time insights

Proactive cybersecurity

Project Mentor	Project Sponsor	Project uOttawa Support
Dr. Ahmed Hamdy	EG-CERT	Prof. Miguel Garzon



System Architecture

Critical Requirements:

Simulate Real Network

Enable Automated Traffic Flow Control

Solution Design:

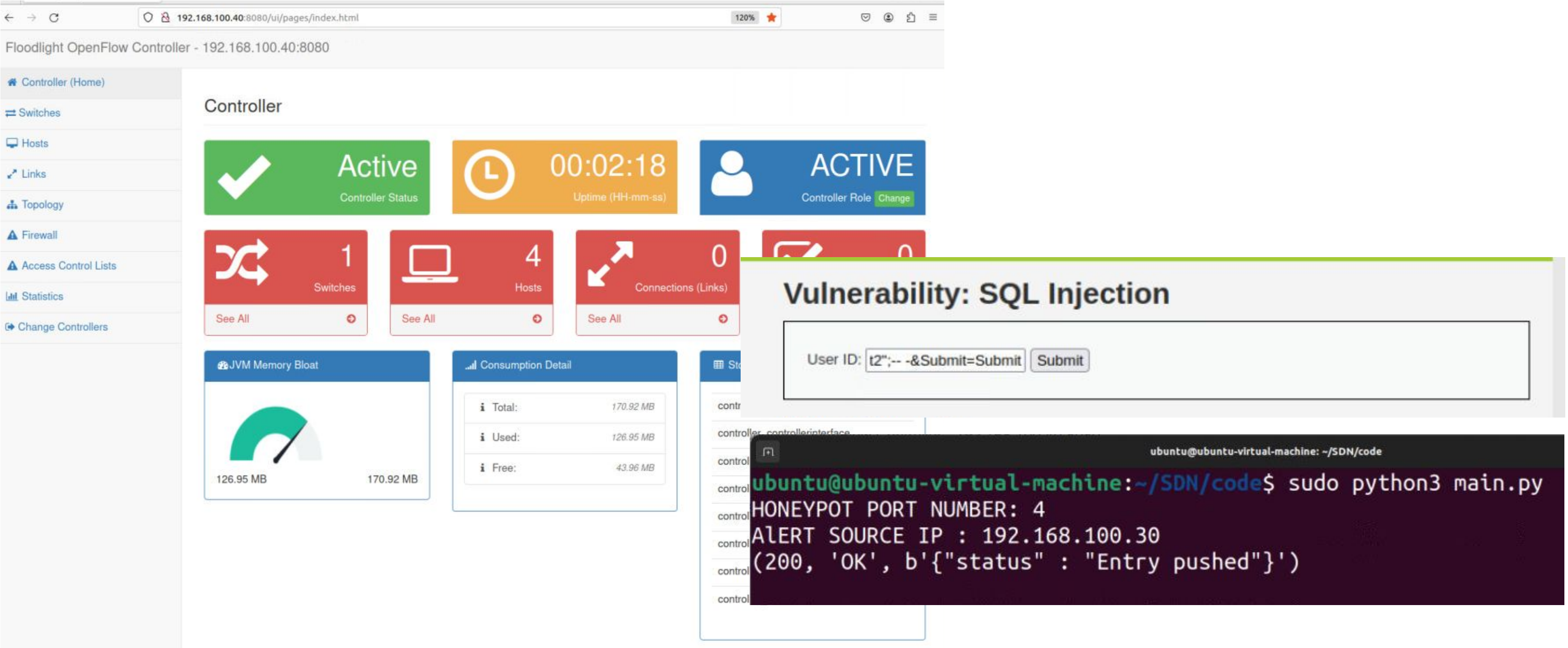
Simulate Real Network

Control The Traffic Flow Automatically

- Creating Virtual Network devices using Open VSwitch SDN.

- Monitor and extract malicious IPs from alerts
- Create flow rule using Floodlight SDN controller

Test and Validation:



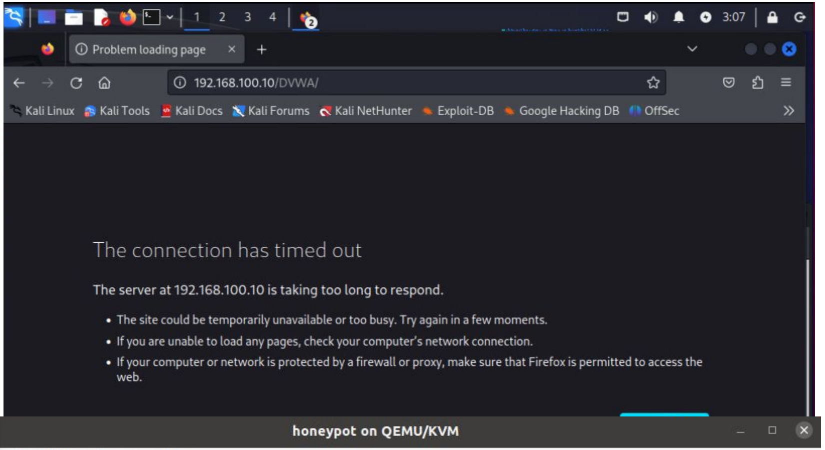
Vulnerability: SQL Injection

User ID: t2";-- -&Submit=Submit Submit

ubuntu@ubuntu-virtual-machine: ~/SDN/code

```
ubuntu@ubuntu-virtual-machine:~/SDN/code$ sudo python3 main.py
HONEYPOT PORT NUMBER: 4
ALERT SOURCE IP : 192.168.100.30
(200, 'OK', b'{"status" : "Entry pushed"}')
```

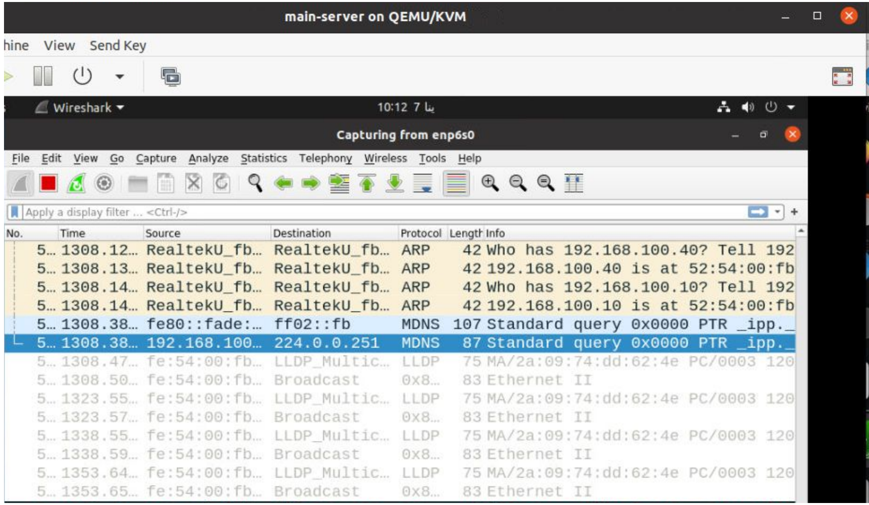
Test and Validation:



The connection has timed out

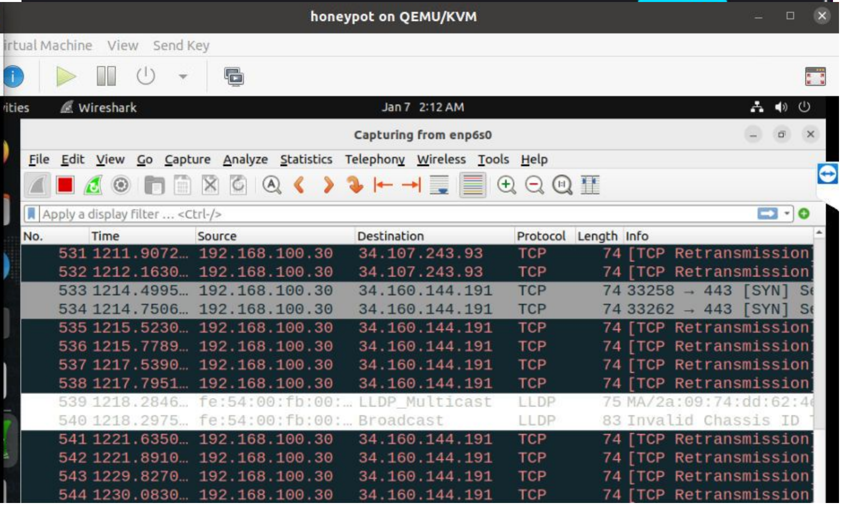
The server at 192.168.100.10 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.



Capturing from enp6s0

```
No.   Time      Source           Destination      Protocol Length Info
5…  1308.12…  RealtekU_fb…   RealtekU_fb…   ARP       42 Who has 192.168.100.40? Tell 192
5…  1308.13…  RealtekU_fb…   RealtekU_fb…   ARP       42 192.168.100.40 is at 52:54:00:fb
5…  1308.14…  RealtekU_fb…   RealtekU_fb…   ARP       42 Who has 192.168.100.10? Tell 192
5…  1308.14…  RealtekU_fb…   RealtekU_fb…   ARP       42 192.168.100.10 is at 52:54:00:fb
5…  1308.38…  fe80::fade:…   ff02::fb       MDNS     107 Standard query 0x0000 PTR _ipp._
5…  1308.38…  192.168.100…   224.0.0.251    MDNS      87 Standard query 0x0000 PTR _ipp._
5…  1308.47…  fe:54:00:fb…   LLDP_Multic…   LLDP      75 MA/2a:09:74:dd:62:4e PC/0003 120
5…  1308.50…  fe:54:00:fb…   Broadcast      0x8…      83 Ethernet II
5…  1323.55…  fe:54:00:fb…   LLDP_Multic…   LLDP      75 MA/2a:09:74:dd:62:4e PC/0003 120
5…  1323.57…  fe:54:00:fb…   Broadcast      0x8…      83 Ethernet II
5…  1338.55…  fe:54:00:fb…   LLDP_Multic…   LLDP      75 MA/2a:09:74:dd:62:4e PC/0003 120
5…  1338.59…  fe:54:00:fb…   Broadcast      0x8…      83 Ethernet II
5…  1353.64…  fe:54:00:fb…   LLDP_Multic…   LLDP      75 MA/2a:09:74:dd:62:4e PC/0003 120
5…  1353.65…  fe:54:00:fb…   Broadcast      0x8…      83 Ethernet II
```



Capturing from enp6s0

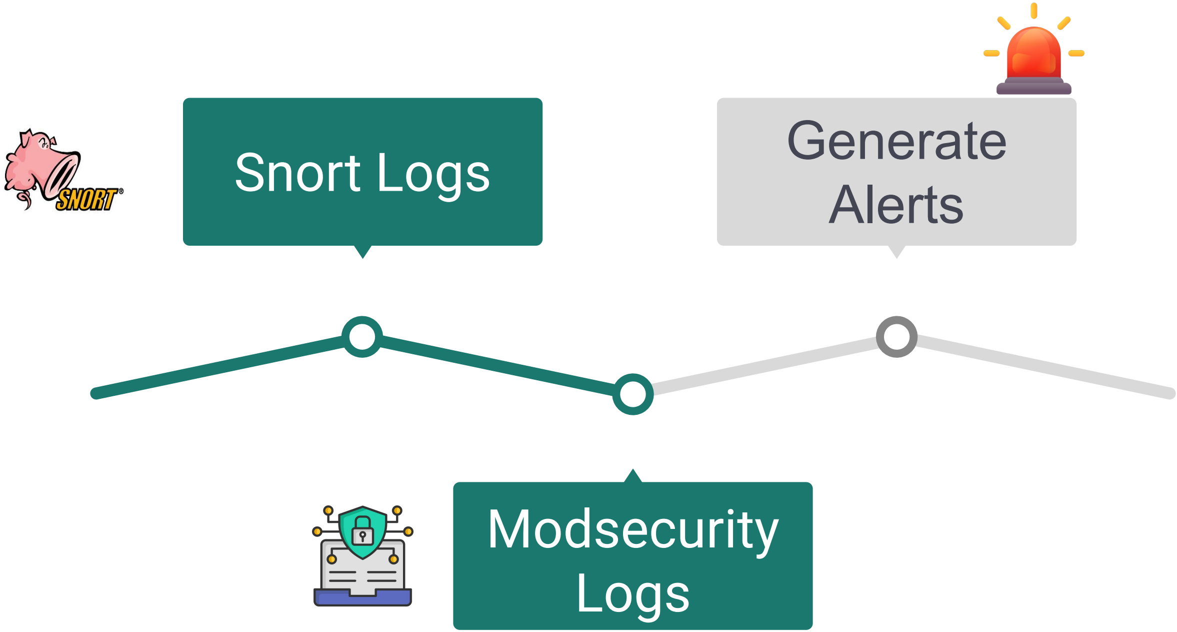
```
No.  Time          Source            Destination      Protocol Length Info
531 1211.9072…  192.168.100.30    34.107.243.93    TCP        74 [TCP Retransmission]
532 1212.1630…  192.168.100.30    34.107.243.93    TCP        74 [TCP Retransmission]
533 1214.4995…  192.168.100.30    34.160.144.191   TCP        74 33258 → 443 [SYN] Se
534 1214.7506…  192.168.100.30    34.160.144.191   TCP        74 33262 → 443 [SYN] Se
535 1215.5230…  192.168.100.30    34.160.144.191   TCP        74 [TCP Retransmission]
536 1215.7789…  192.168.100.30    34.160.144.191   TCP        74 [TCP Retransmission]
537 1217.5390…  192.168.100.30    34.160.144.191   TCP        74 [TCP Retransmission]
538 1217.7951…  192.168.100.30    34.160.144.191   TCP        74 [TCP Retransmission]
539 1218.2846…  fe:54:00:fb:00:…  LLDP_Multicast   LLDP       75 MA/2a:09:74:dd:62:4
540 1218.2975…  fe:54:00:fb:00:…  Broadcast        LLDP       83 Invalid Chassis ID
541 1221.6350…  192.168.100.30    34.160.144.191   TCP        74 [TCP Retransmission]
542 1221.8910…  192.168.100.30    34.160.144.191   TCP        74 [TCP Retransmission]
543 1229.8270…  192.168.100.30    34.160.144.191   TCP        74 [TCP Retransmission]
544 1230.0830…  192.168.100.30    34.160.144.191   TCP        74 [TCP Retransmission]
```

Critical Requirements:

Secure Web-server

Secure server assets

Solution Design:



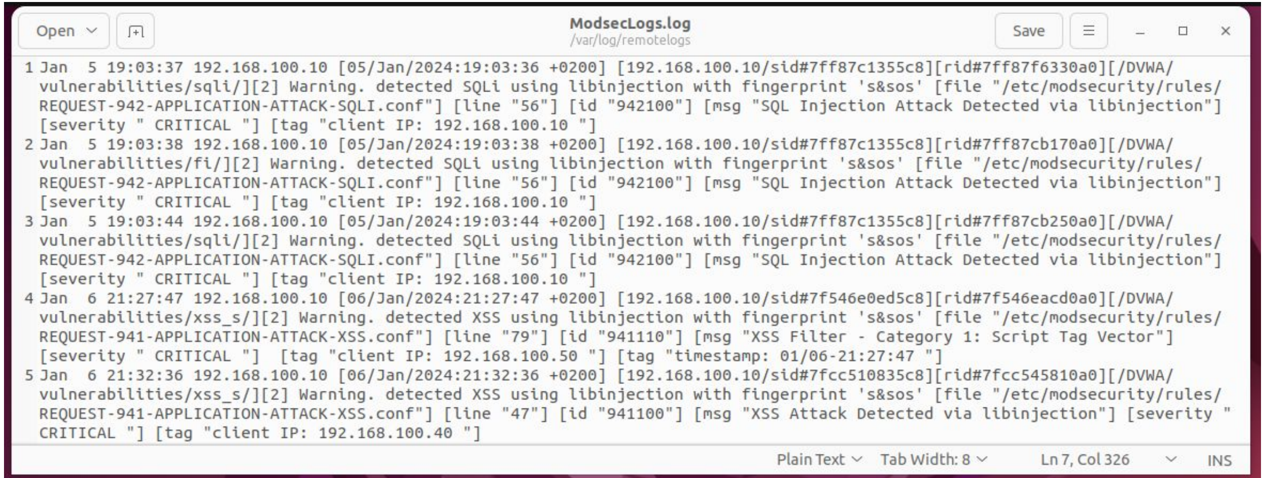
Snort Logs

Generate Alerts

Modsecurity Logs

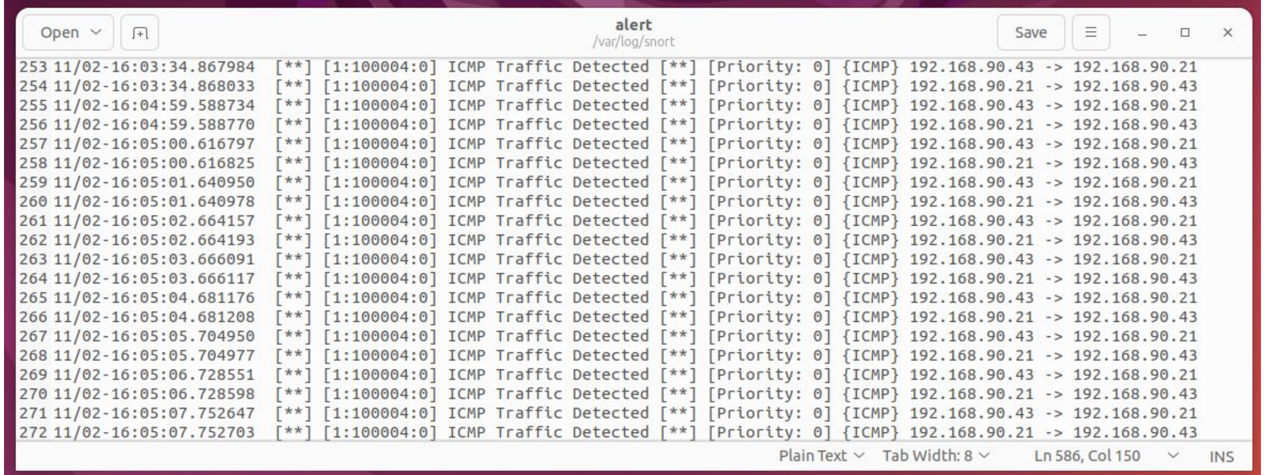
Test and Validate

ModSecurity Logs



```
Jan  5 19:03:37 192.168.100.10 [05/Jan/2024:19:03:36 +0200] [192.168.100.10/sid#7ff87c1355c8][rid#7ff87f6330a0][/DVWA/vulnerabilities/sqli/][2] Warning. detected SQLi using libinjection with fingerprint 's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "56"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity " CRITICAL "] [tag "client IP: 192.168.100.10 "]
Jan  5 19:03:38 192.168.100.10 [05/Jan/2024:19:03:38 +0200] [192.168.100.10/sid#7ff87c1355c8][rid#7ff87cb170a0][/DVWA/vulnerabilities/fi/][2] Warning. detected SQLi using libinjection with fingerprint 's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "56"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity " CRITICAL "] [tag "client IP: 192.168.100.10 "]
Jan  5 19:03:44 192.168.100.10 [05/Jan/2024:19:03:44 +0200] [192.168.100.10/sid#7ff87c1355c8][rid#7ff87cb250a0][/DVWA/vulnerabilities/sqli/][2] Warning. detected SQLi using libinjection with fingerprint 's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "56"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity " CRITICAL "] [tag "client IP: 192.168.100.10 "]
Jan  6 21:27:47 192.168.100.10 [06/Jan/2024:21:27:47 +0200] [192.168.100.10/sid#7f546e0ed5c8][rid#7f546eacd0a0][/DVWA/vulnerabilities/xss_s/][2] Warning. detected XSS using libinjection with fingerprint 's&sos' [file "/etc/modsecurity/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "79"] [id "941110"] [msg "XSS Filter - Category 1: Script Tag Vector"] [severity " CRITICAL "]  [tag "client IP: 192.168.100.50 "] [tag "timestamp: 01/06-21:27:47 "]
Jan  6 21:32:36 192.168.100.10 [06/Jan/2024:21:32:36 +0200] [192.168.100.10/sid#7fcc510835c8][rid#7fcc545810a0][/DVWA/vulnerabilities/xss_s/][2] Warning. detected XSS using libinjection with fingerprint 's&sos' [file "/etc/modsecurity/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "47"] [id "941100"] [msg "XSS Attack Detected via libinjection"] [severity " CRITICAL "] [tag "client IP: 192.168.100.40 "]
```

Snort Logs



```
11/02-16:03:34.867984  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.43 -> 192.168.90.21
11/02-16:03:34.868033  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.21 -> 192.168.90.43
11/02-16:04:59.588734  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.43 -> 192.168.90.21
11/02-16:04:59.588770  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.21 -> 192.168.90.43
11/02-16:05:00.616797  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.43 -> 192.168.90.21
11/02-16:05:00.616825  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.21 -> 192.168.90.43
11/02-16:05:01.640950  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.43 -> 192.168.90.21
11/02-16:05:01.640978  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.21 -> 192.168.90.43
11/02-16:05:02.664157  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.43 -> 192.168.90.21
11/02-16:05:02.664193  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.21 -> 192.168.90.43
11/02-16:05:03.666091  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.43 -> 192.168.90.21
11/02-16:05:03.666117  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.21 -> 192.168.90.43
11/02-16:05:04.681176  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.43 -> 192.168.90.21
11/02-16:05:04.681208  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.21 -> 192.168.90.43
11/02-16:05:05.704950  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.43 -> 192.168.90.21
11/02-16:05:05.704977  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.21 -> 192.168.90.43
11/02-16:05:06.728551  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.43 -> 192.168.90.21
11/02-16:05:06.728598  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.21 -> 192.168.90.43
11/02-16:05:07.752647  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.43 -> 192.168.90.21
11/02-16:05:07.752703  [**] [1:100004:0] ICMP Traffic Detected [**] [Priority: 0] {ICMP} 192.168.90.21 -> 192.168.90.43
```

Critical Requirements:

Apply Penetration Testing

Create Centralized Logging system

Solution Design:

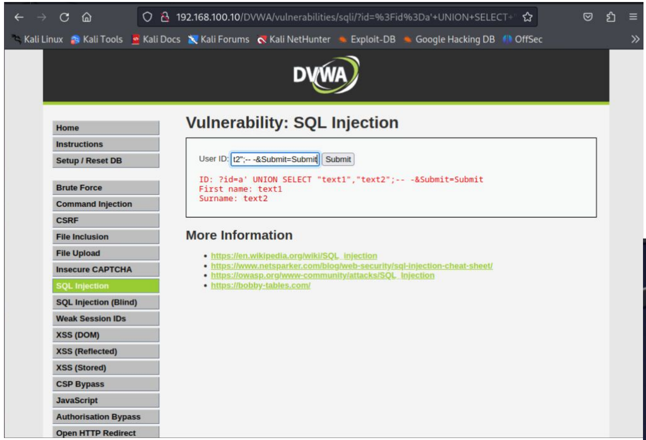
Simulating Attacks

Create Centralized Logging system

- Creating attacks on the network and the servers

- Creating client-server system using syslog-ng

Test and Validation:



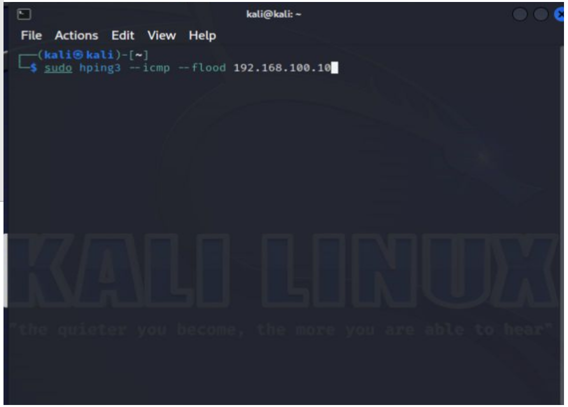
Vulnerability: SQL Injection

User ID: t2";-- -&Submit=Submit

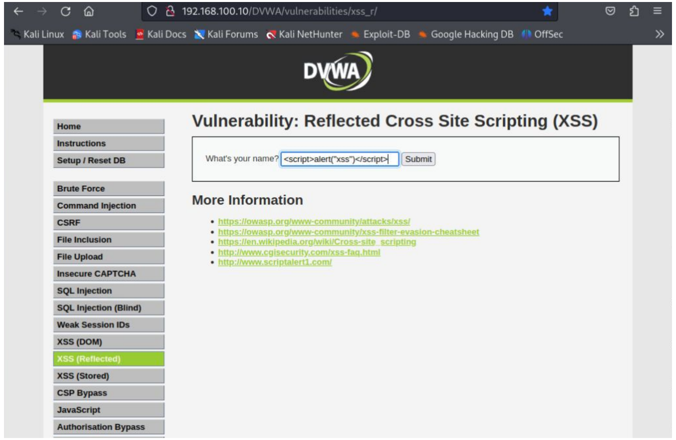
```
ID: ?id=a' UNION SELECT "text1","text2";-- -&Submit=Submit
First name: text1
Surname: text2
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --icmp --flood 192.168.100.10
```



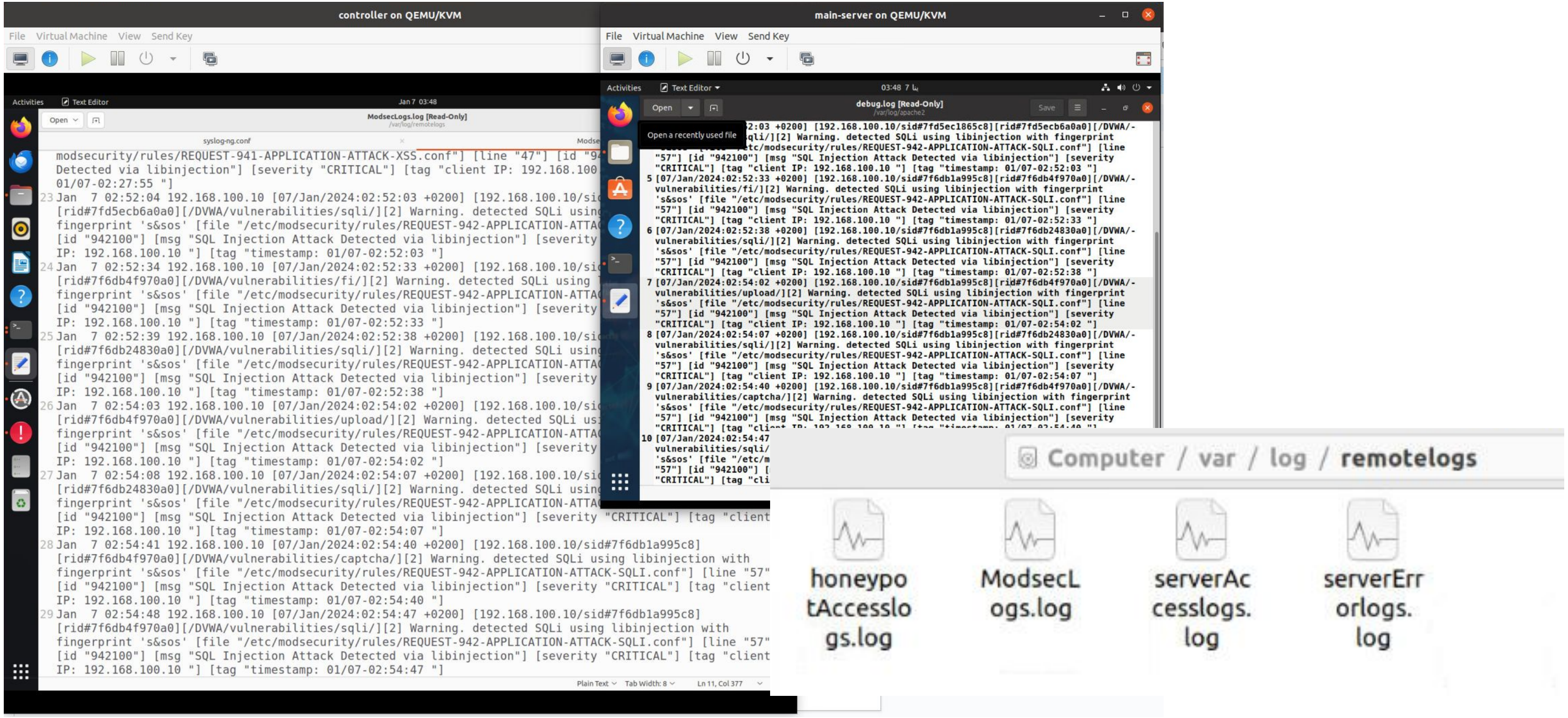
Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? <script>alert("xss")</script>

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/

Test and Validation:



```
modsecurity/rules/REQUEST-941-APPLICATION-ATTACK-XSS.conf"] [line "47"] [id "94
Detected via libinjection"] [severity "CRITICAL"] [tag "client IP: 192.168.100
01/07-02:27:55 "]
Jan  7 02:52:04 192.168.100.10 [07/Jan/2024:02:52:03 +0200] [192.168.100.10/si
[rid#7fd5ecb6a0a0][/DVWA/vulnerabilities/sqli/][2] Warning. detected SQLi usin
fingerprint 's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTA
[id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity
IP: 192.168.100.10 "] [tag "timestamp: 01/07-02:52:03 "]
Jan  7 02:52:34 192.168.100.10 [07/Jan/2024:02:52:33 +0200] [192.168.100.10/si
[rid#7f6db4f970a0][/DVWA/vulnerabilities/fi/][2] Warning. detected SQLi using
fingerprint 's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTA
[id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity
IP: 192.168.100.10 "] [tag "timestamp: 01/07-02:52:33 "]
Jan  7 02:52:39 192.168.100.10 [07/Jan/2024:02:52:38 +0200] [192.168.100.10/si
[rid#7f6db24830a0][/DVWA/vulnerabilities/sqli/][2] Warning. detected SQLi usin
fingerprint 's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTA
[id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity
IP: 192.168.100.10 "] [tag "timestamp: 01/07-02:52:38 "]
Jan  7 02:54:03 192.168.100.10 [07/Jan/2024:02:54:02 +0200] [192.168.100.10/si
[rid#7f6db4f970a0][/DVWA/vulnerabilities/upload/][2] Warning. detected SQLi us
fingerprint 's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTA
[id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity
IP: 192.168.100.10 "] [tag "timestamp: 01/07-02:54:02 "]
Jan  7 02:54:08 192.168.100.10 [07/Jan/2024:02:54:07 +0200] [192.168.100.10/si
[rid#7f6db24830a0][/DVWA/vulnerabilities/sqli/][2] Warning. detected SQLi usin
fingerprint 's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTA
[id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity "CRITICAL"] [tag "client
IP: 192.168.100.10 "] [tag "timestamp: 01/07-02:54:07 "]
Jan  7 02:54:41 192.168.100.10 [07/Jan/2024:02:54:40 +0200] [192.168.100.10/sid#7f6db1a995c8]
[rid#7f6db4f970a0][/DVWA/vulnerabilities/captcha/][2] Warning. detected SQLi using libinjection with
fingerprint 's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "57"
[id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity "CRITICAL"] [tag "client
IP: 192.168.100.10 "] [tag "timestamp: 01/07-02:54:40 "]
Jan  7 02:54:48 192.168.100.10 [07/Jan/2024:02:54:47 +0200] [192.168.100.10/sid#7f6db1a995c8]
[rid#7f6db4f970a0][/DVWA/vulnerabilities/sqli/][2] Warning. detected SQLi using libinjection with
fingerprint 's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "57"
[id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity "CRITICAL"] [tag "client
IP: 192.168.100.10 "] [tag "timestamp: 01/07-02:54:47 "]
```

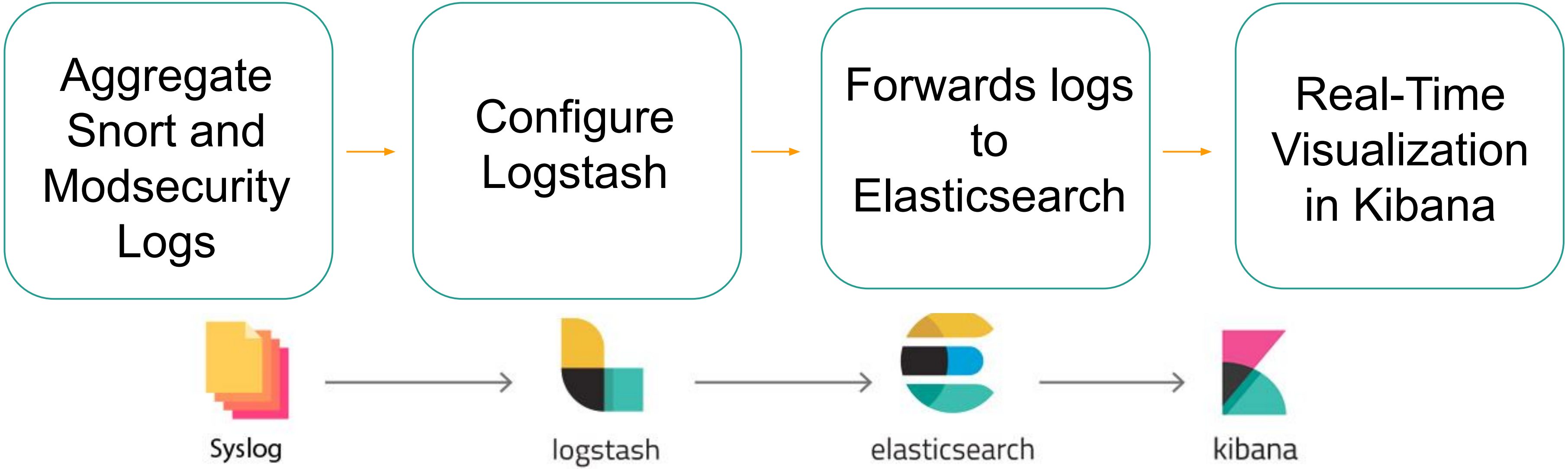
```
2:03 +0200] [192.168.100.10/sid#7fd5ec1865c8][rid#7fd5ecb6a0a0][/DVWA/-
qli/][2] Warning. detected SQLi using libinjection with fingerprint
tc/modsecurity/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line
"57"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity
"CRITICAL"] [tag "client IP: 192.168.100.10 "] [tag "timestamp: 01/07-02:52:03 "]
[07/Jan/2024:02:52:33 +0200] [192.168.100.10/sid#7f6db1a995c8][rid#7f6db4f970a0][/DVWA/-
vulnerabilities/fi/][2] Warning. detected SQLi using libinjection with fingerprint
's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line
"57"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity
"CRITICAL"] [tag "client IP: 192.168.100.10 "] [tag "timestamp: 01/07-02:52:33 "]
[07/Jan/2024:02:52:38 +0200] [192.168.100.10/sid#7f6db1a995c8][rid#7f6db24830a0][/DVWA/-
vulnerabilities/sqli/][2] Warning. detected SQLi using libinjection with fingerprint
's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line
"57"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity
"CRITICAL"] [tag "client IP: 192.168.100.10 "] [tag "timestamp: 01/07-02:52:38 "]
[07/Jan/2024:02:54:02 +0200] [192.168.100.10/sid#7f6db1a995c8][rid#7f6db4f970a0][/DVWA/-
vulnerabilities/upload/][2] Warning. detected SQLi using libinjection with fingerprint
's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line
"57"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity
"CRITICAL"] [tag "client IP: 192.168.100.10 "] [tag "timestamp: 01/07-02:54:02 "]
[07/Jan/2024:02:54:07 +0200] [192.168.100.10/sid#7f6db1a995c8][rid#7f6db24830a0][/DVWA/-
vulnerabilities/sqli/][2] Warning. detected SQLi using libinjection with fingerprint
's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line
"57"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity
"CRITICAL"] [tag "client IP: 192.168.100.10 "] [tag "timestamp: 01/07-02:54:07 "]
[07/Jan/2024:02:54:40 +0200] [192.168.100.10/sid#7f6db1a995c8][rid#7f6db4f970a0][/DVWA/-
vulnerabilities/captcha/][2] Warning. detected SQLi using libinjection with fingerprint
's&sos' [file "/etc/modsecurity/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line
"57"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [severity
"CRITICAL"] [tag "cli
[07/Jan/2024:02:54:47
vulnerabilities/sqli/
's&sos' [file "/etc/m
"57"] [id "942100"] [
"CRITICAL"] [tag "cli
```

Critical Requirements:

- Logs Analysis
- Logs Visualization
- Real-Time Alerting

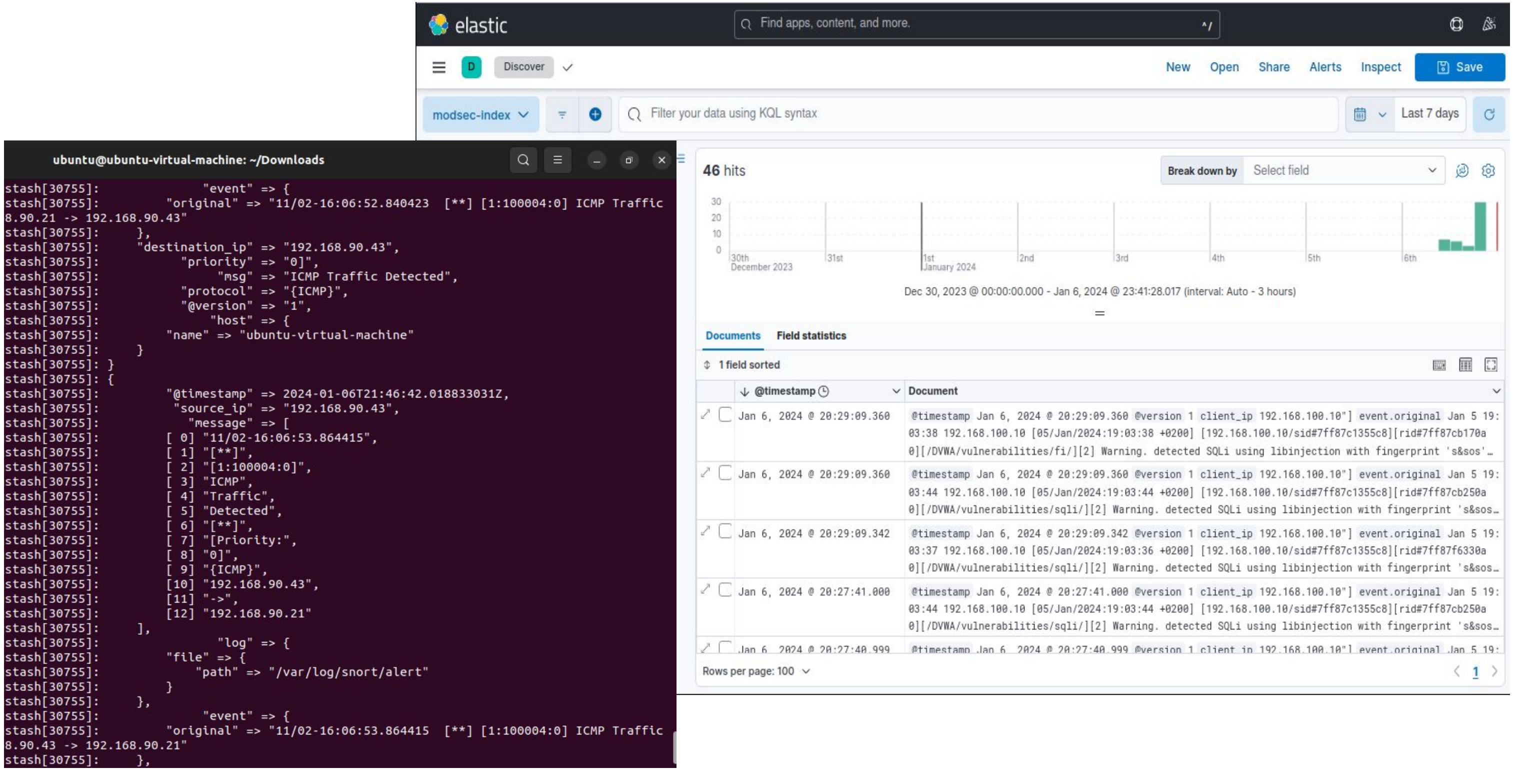
Solution Design:

- Integrate ELK with our system.



Aggregate Snort and Modsecurity Logs → Configure Logstash → Forwards logs to Elasticsearch → Real-Time Visualization in Kibana

Test and Validation



ubuntu@ubuntu-virtual-machine: ~/Downloads

```
stash[30755]:            "event" => {
stash[30755]:         "original" => "11/02-16:06:52.840423  [**] [1:100004:0] ICMP Traffic
8.90.21 -> 192.168.90.43"
stash[30755]:     },
stash[30755]:     "destination_ip" => "192.168.90.43",
stash[30755]:           "priority" => "0]",
stash[30755]:                "msg" => "ICMP Traffic Detected",
stash[30755]:           "protocol" => "{ICMP}",
stash[30755]:           "@version" => "1",
stash[30755]:               "host" => {
stash[30755]:         "name" => "ubuntu-virtual-machine"
stash[30755]:     }
stash[30755]: }
stash[30755]: {
stash[30755]:         "@timestamp" => 2024-01-06T21:46:42.018833031Z,
stash[30755]:          "source_ip" => "192.168.90.43",
stash[30755]:            "message" => [
stash[30755]:         [ 0] "11/02-16:06:53.864415",
stash[30755]:         [ 1] "[**]",
stash[30755]:         [ 2] "[1:100004:0]",
stash[30755]:         [ 3] "ICMP",
stash[30755]:         [ 4] "Traffic",
stash[30755]:         [ 5] "Detected",
stash[30755]:         [ 6] "[**]",
stash[30755]:         [ 7] "[Priority:",
stash[30755]:         [ 8] "0]",
stash[30755]:         [ 9] "{ICMP}",
stash[30755]:         [10] "192.168.90.43",
stash[30755]:         [11] "->",
stash[30755]:         [12] "192.168.90.21"
stash[30755]:     ],
stash[30755]:                "log" => {
stash[30755]:         "file" => {
stash[30755]:            "path" => "/var/log/snort/alert"
stash[30755]:         }
stash[30755]:     },
stash[30755]:              "event" => {
stash[30755]:         "original" => "11/02-16:06:53.864415  [**] [1:100004:0] ICMP Traffic
8.90.43 -> 192.168.90.21"
stash[30755]:     },
```

46 hits

Dec 30, 2023 @ 00:00:00.000 - Jan 6, 2024 @ 23:41:28.017 (interval: Auto - 3 hours)

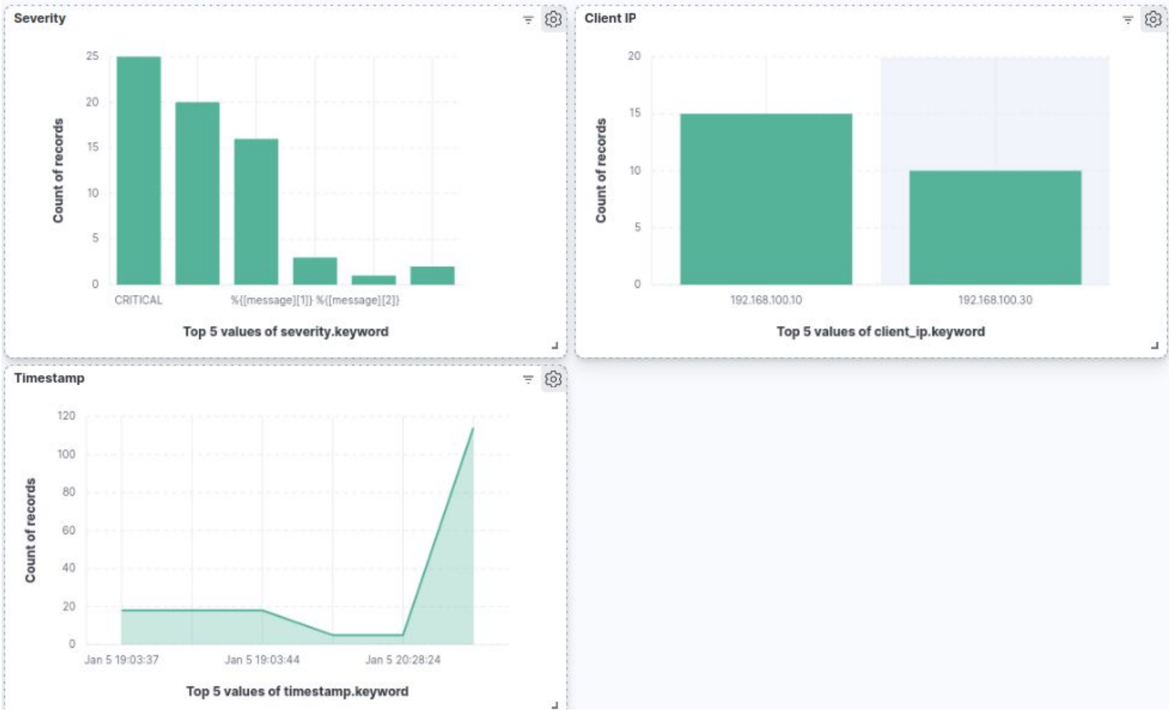
1 field sorted

@timestamp	Document
Jan 6, 2024 @ 20:29:09.360	@timestamp Jan 6, 2024 @ 20:29:09.360 @version 1 client_ip 192.168.100.10"] event.original Jan 5 19:03:38 192.168.100.10 [05/Jan/2024:19:03:38 +0200] [192.168.100.10/sid#7ff87c1355c8][rid#7ff87cb170a0][/DVWA/vulnerabilities/fi/][2] Warning. detected SQLi using libinjection with fingerprint 's&sos'…
Jan 6, 2024 @ 20:29:09.360	@timestamp Jan 6, 2024 @ 20:29:09.360 @version 1 client_ip 192.168.100.10"] event.original Jan 5 19:03:44 192.168.100.10 [05/Jan/2024:19:03:44 +0200] [192.168.100.10/sid#7ff87c1355c8][rid#7ff87cb250a0][/DVWA/vulnerabilities/sqli/][2] Warning. detected SQLi using libinjection with fingerprint 's&sos…
Jan 6, 2024 @ 20:29:09.342	@timestamp Jan 6, 2024 @ 20:29:09.342 @version 1 client_ip 192.168.100.10"] event.original Jan 5 19:03:37 192.168.100.10 [05/Jan/2024:19:03:36 +0200] [192.168.100.10/sid#7ff87c1355c8][rid#7ff87f6330a0][/DVWA/vulnerabilities/sqli/][2] Warning. detected SQLi using libinjection with fingerprint 's&sos…
Jan 6, 2024 @ 20:27:41.000	@timestamp Jan 6, 2024 @ 20:27:41.000 @version 1 client_ip 192.168.100.10"] event.original Jan 5 19:03:44 192.168.100.10 [05/Jan/2024:19:03:44 +0200] [192.168.100.10/sid#7ff87c1355c8][rid#7ff87cb250a0][/DVWA/vulnerabilities/sqli/][2] Warning. detected SQLi using libinjection with fingerprint 's&sos…
Jan 6, 2024 @ 20:27:40.999	@timestamp Jan 6, 2024 @ 20:27:40.999 @version 1 client_ip 192.168.100.10"] event.original Jan 5 19:

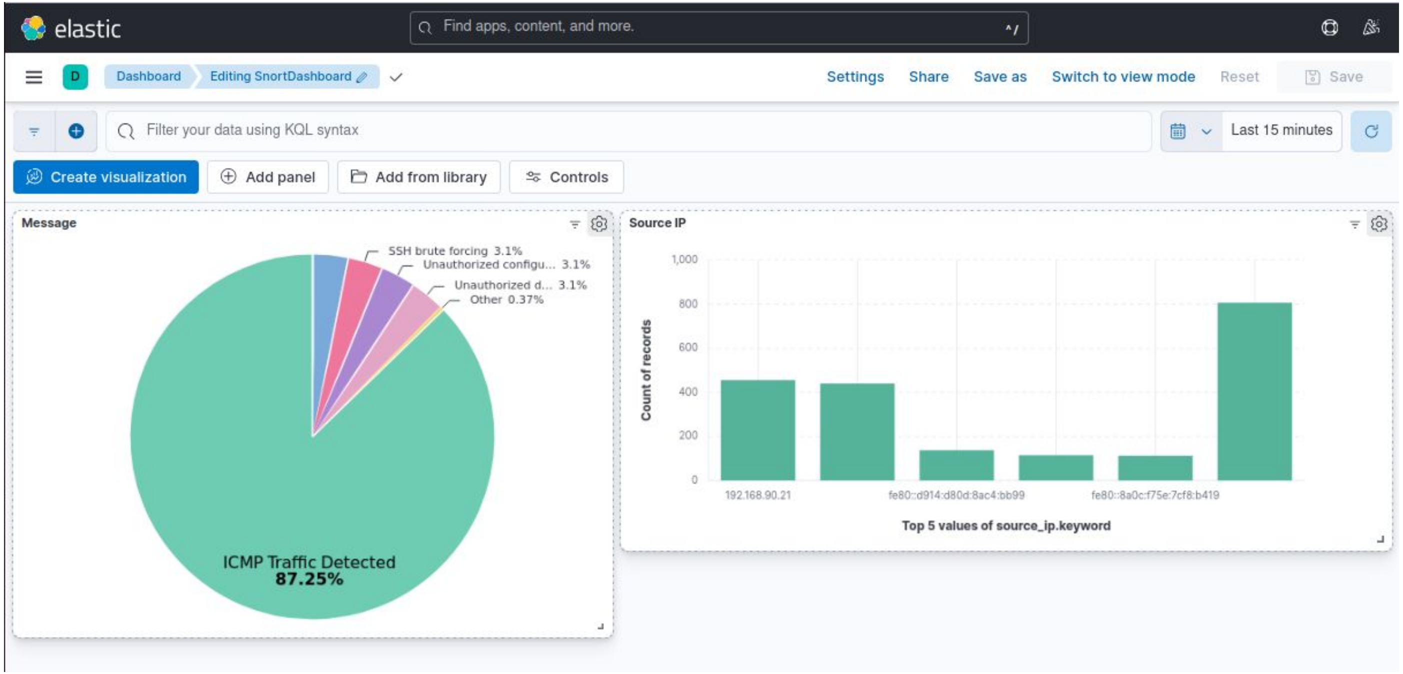
Rows per page: 100

1

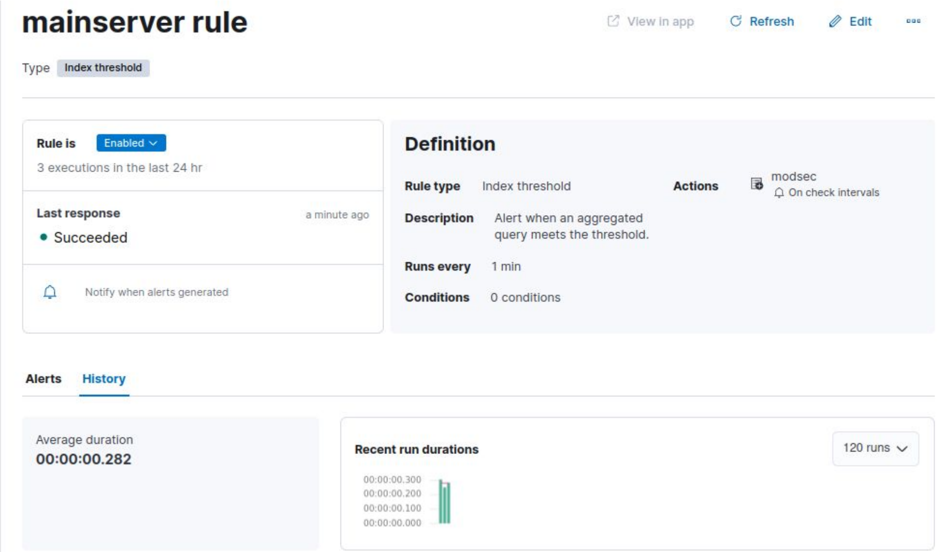
Test and Validation



Test and Validation



Test and Validation



mainserver rule

Type: Index threshold

Rule is Enabled

3 executions in the last 24 hr

Last response a minute ago

● Succeeded

Notify when alerts generated

Definition

Rule type Index threshold

Description Alert when an aggregated query meets the threshold.

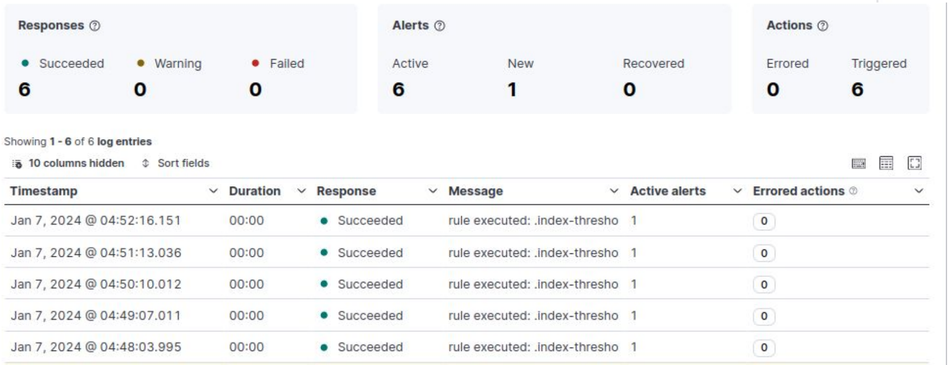
Runs every 1 min

Conditions 0 conditions

Actions modsec
On check intervals

Average duration
00:00:00.282

Recent run durations



Responses		
● Succeeded	● Warning	● Failed
6	0	0

Alerts		
Active	New	Recovered
6	1	0

Actions	
Errored	Triggered
0	6

Showing **1 - 6** of 6 **log entries**

Timestamp	Duration	Response	Message	Active alerts	Errored actions
Jan 7, 2024 @ 04:52:16.151	00:00	● Succeeded	rule executed: .index-thresho	1	0
Jan 7, 2024 @ 04:51:13.036	00:00	● Succeeded	rule executed: .index-thresho	1	0
Jan 7, 2024 @ 04:50:10.012	00:00	● Succeeded	rule executed: .index-thresho	1	0
Jan 7, 2024 @ 04:49:07.011	00:00	● Succeeded	rule executed: .index-thresho	1	0
Jan 7, 2024 @ 04:48:03.995	00:00	● Succeeded	rule executed: .index-thresho	1	0

Any Questions?

Thank you