

Defense-in-Depth Security Lab: NGFW, WAF & SIEM Implementation

Prepared by: Saboor Ali

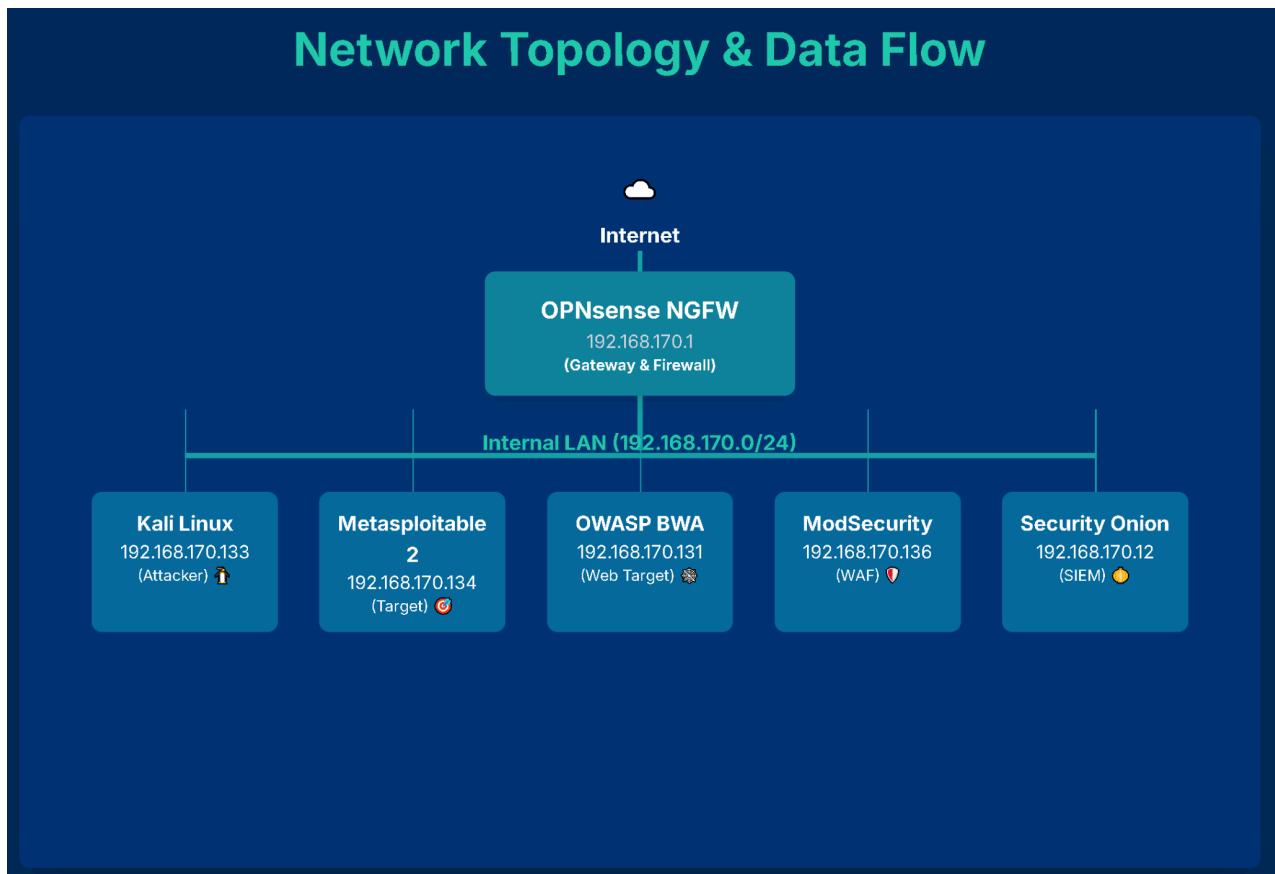
Date: September 27, 2025

Overview

This lab replicates a real-world enterprise environment to illustrate a defense-in-depth strategy combining a Next-Generation Firewall (NGFW), Web Application Firewall (WAF), and Security Information and Event Management (SIEM) to counter both network-level and web application attacks.

Lab Environment Setup

VMs include Kali Linux (attacker), Metasploitable 2, OWASP BWA/DVWA (vulnerable targets), OPNsense (NGFW), Security Onion (SIEM) and ModSecurity WAF. All IP assignments used DHCP; IPs vary in attack logs due to later changes—static IP steps are omitted as not essential to defense outcomes.



Baseline Vulnerability Testing (Pre-defense)

Vulnerability: SQL Injection

- A SQL Injection attack using the OR 1=1 payload against DVWA successfully bypassed authentication controls, resulting in unauthorized access and data exfiltration.

The screenshot shows two instances of the DVWA SQL Injection module. In the first instance, a user enters the payload '`OR '1'=1`' into the 'User ID' field and clicks 'Submit'. The response displays a list of user records from the database:

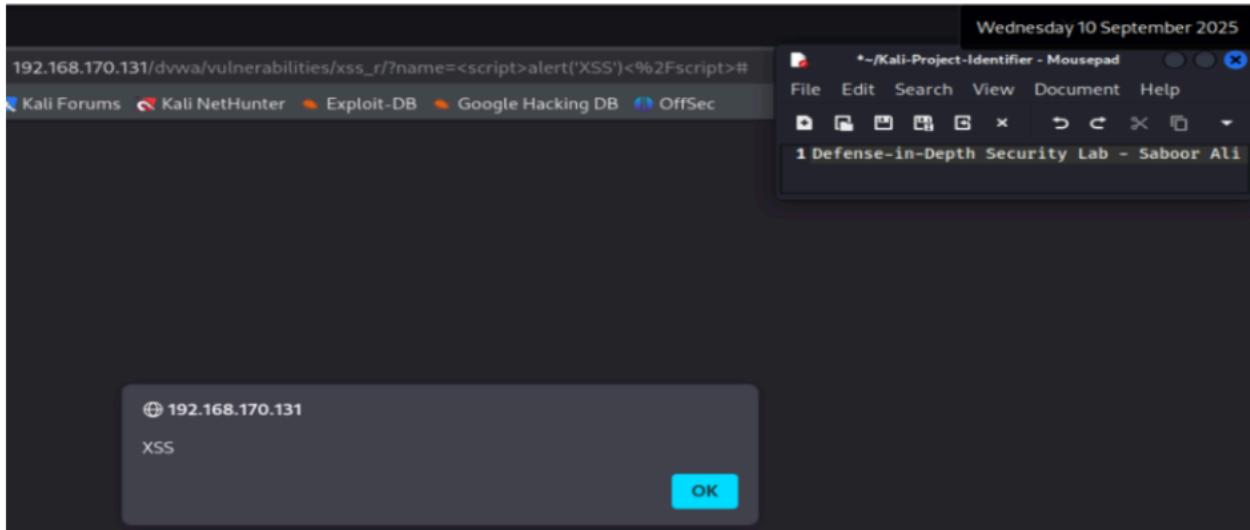
ID	First name	Surname
1	admin	admin
2	Gordon	Brown
3	Hack	Me
4	Pablo	Picasso
5	Bob	Smith
6	user	user

In the second instance, the same payload is submitted, and the results are identical, demonstrating the exploit's success.

Vulnerability: Cross-Site Scripting (XSS)

- `<script>alert('XSS')</script>` submitted to DVWA XSS module, browser displays pop-up.

The screenshot shows the DVWA Reflected XSS module. A user enters the payload '`<script>alert('XSS')</script>`' into the 'What's your name?' field and clicks 'Submit'. A browser window in the background shows a pop-up message: "XSS".



Vulnerability: Directory Traversal and Information Exposure

- Direct access to /phpinfo.php, /test/ confirms exposures.

System	Linux owaspbwa 2.6.32-25-generic-pae #44-Ubuntu SMP Fri Sep 17 21:57:48 UTC 2010 i686
Build Date	Apr 17 2015 15:01:49
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/owaspbwa/owaspbwa-svn/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/curl.ini, /etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/mcrypt.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API20090626.NTS
PHP Extension Build	API20090626.NTS
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

Vulnerability: Network Enumeration

- Nmap scan uncovers open services and banners on Metasploitable 2.

```
(kali㉿kali)-[~]
$ nmap -sS -sV 192.168.170.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-10 05:46 EDT
Nmap scan report for 192.168.170.128
Host is up (0.0078s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smptd
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec          netkit-rsh rexecd
513/tcp   open  login?       Netkit rshd
514/tcp   open  shell         GNU Classpath grmiregistry
1099/tcp  open  java-rmi     Metasploitable root shell
1524/tcp  open  bindshell    2-4 (RPC #100003)
2049/tcp  open  nfs          ProFTPD 1.3.1
2121/tcp  open  ftp          MySQL 5.0.51a-3ubuntu5
3306/tcp  open  mysql        PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp  open  postgresql   VNC (protocol 3.3)
5900/tcp  open  vnc          (access denied)
6000/tcp  open  X11          UnrealIRCd
6667/tcp  open  irc          UnrealIRCd
8180/tcp  open  unknown      MAC Address: 00:0C:29:68:BB:54 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 195.29 seconds

(kali㉿kali)-[~]
```

Vulnerability: FTP Backdoor Exploit (Metasploitable)

- Metasploit is used to execute a backdoor exploit against Metasploitable, successfully opening a shell.

```
File Actions Edit View Help
[*] exploit(unix/ftp/vsftpd_234_backdoor)
[*] 192.168.170.128:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.170.128:21 - USER: 331 Please specify the password.
[+] 192.168.170.128:21 - Backdoor service has been spawned, handling ...
[+] 192.168.170.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.170.130:45839 → 192.168.170.128:6200) at 20
5-09-10 06:14:05 -0400

whoami
root
hostname
metasploitable
```

Security Controls Deployment

1. NGFW (OPNsense) Setup

- OPNsense VM is installed and configured with dual interfaces. Web UI confirms system status.

```
Website: https://opnsense.org/
Handbook: https://docs.opnsense.org/
Forums: https://forum.opnsense.org/
Code: https://github.com/opnsense
Reddit: https://reddit.com/r/opnsense

*** OPNsense.internal: OPNsense 25.7 (amd64) ***

LAN (em1)      -> v4: 192.168.170.1/24
WAN (em0)      -> v4/DHCP4: 192.168.221.142/24

HTTPS: sha256 7F A6 0F 8E 12 67 58 DC 5E B0 B4 FF D9 B1 7A 3D
       02 B2 3F D9 F1 18 93 4F 51 38 3D 4D EC 19 06 23

0) Logout          7) Ping host
1) Assign interfaces 8) Shell
2) Set interface IP address 9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system 12) Update from console
6) Reboot system 13) Restore a backup

Enter an option: [
```

The screenshot shows the OPNsense web interface at https://192.168.170.1/index.php?wizard_done. The page displays a success message: "Finished initial configuration!". It also includes a note about running in live media mode and enabling SSH remote login for users "root" and "installer". The sidebar on the left shows navigation links like Lobby, Dashboard, License, Password, Logout, Reporting, System, Interfaces, Firewall, VPN, Services, Power, and Help. The main content area features the OPNsense logo and a message congratulating the user on successful configuration.

- **LAN rules:** Allow only HTTP(S), SSH for management; FTP restricted—Brute-force countermeasures implemented with address block alias and connection thresholds.

- **Intrusion Prevention and Detection:** Suricata was activated within the OPNsense dashboard to provide real-time alerting and proactive blocking of known malicious signatures.

We strongly advise to use policies instead of single rule based changes to limit the size of the configuration (available here)

General Settings

- Enabled**
- IPS mode**
- Promiscuous mode**

Interfaces LAN

Clear All Select All

- **Mitigation Example:** A detected vsFTPD backdoor attack is promptly blocked by a custom drop rule.

Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert
2025-09-17T11:15:33.470879+0000	900001	blocked	em1	192.168.170.133	33159	192.168.170.134	6200	Possible vsftpd backdo
2025-09-17T11:15:33.470879+0000	900001	blocked	em1	192.168.170.133	33159	192.168.170.134	6200	Possible vsftpd backdo

2. Web Application Firewall (WAF) ModSecurity

- Configured for Nginx reverse proxy in front of DVWA/OWASP BWA targets.

```

GNU nano 6.2                                     nginx.conf *

server {
    listen      80;
    server_name 192.168.170.136;
    root /usr/local/nginx/html;

    # Enable ModSecurity
    modsecurity on;
    modsecurity_rules_file /usr/local/nginx/conf/modsecurity.conf;
    #charset koi8-r;
    #access_log logs/host.access.log main;
    location / {
        proxy_pass http://192.168.170.131;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    }
}

```

- **Rules Activated:** OWASP CRS rules loaded (detect/block modes).

```

GNU nano 6.2                                     modsecurity.conf *
# Enable ModSecurity
SecRuleEngine On
SecRequestBodyAccess On
SecAuditEngine On
SecResponseBodyAccess Off
SecDataDir /usr/local/modsecurity/data
SecTmpDir /usr/local/modsecurity/tmp
SecAuditLog /usr/local/nginx/logs/modsec_audit.log
SecAuditLogParts ABIJDEFHZ
SecDebugLog /usr/local/nginx/logs/modsec_debug.log
SecLogLevel 3

# Include CRS setup
Include /usr/local/modsecurity-crs/crs-setup.conf
# Include all CRS rules
Include /usr/local/modsecurity-crs/rules/*.conf

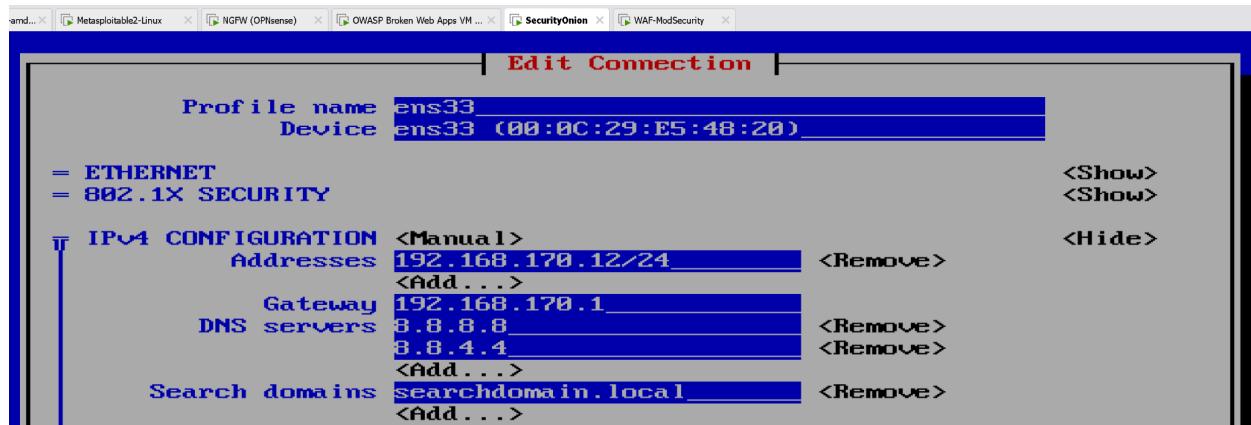
```

- **Example Mitigation:** SQL Injection attempts receive HTTP 403; detection logged.

```
waf@waf-modsecurity:/usr/local/nginx/logs$ tail modsec_audit.log
ModSecurity: Warning. Matched "Operator `Rx` with parameter `(?:(^([\\d.]+|\\[[\\da-f:]++\\]|[^da-f:]++)|([\\d]+)?$)`" against variable `REQUEST_HEADERS:Host` (Value: `192.168.170.136` ) [file "/usr/local/modsecurity-crs/rules/REQUEST-920-PROTOCOL-ENFORCEMENT.conf"] [line "711"] [id "920350"] [rev """] [msg "Host header is a numeric IP address"] [data "192.168.170.136"] [severity "4"] [ver "OWASP CRS/4.19.0-dev"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-protocol"] [tag "paranoia-level/1"] [tag "OWASP CRS"] [tag "OWASP CRS/PROTOCOL-ENFORCEMENT"] [tag "capec/1000/210/272"] [hostname "192.168.170.136"] [uri "/dvwa/vulnerabilities/sqli/] [unique_id "175764488172.546717"] [ref "o0,1500,15v86,15"]
ModSecurity: Warning. detected SQLi using libinjection. [file "/usr/local/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "46"] [id "942100"] [rev """] [msg "SQL Injection Attack Detected via libinjection"] [data "Matched Data: s&sos found within ARGS:id: ' OR '1'='1'" [severity "2"] [ver "OWASP CRS/4.19.0-dev"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP CRS"] [tag "OWASP CRS/ATTACK-SQLI"] [tag "capec/1000/152/248/66"] [hostname "192.168.170.136"] [uri "/dvwa/vulnerabilities/sqli/] [unique_id "175764488172.546717"] [ref "v35,11"]
ModSecurity: Access denied with code 403 (phase 2). Matched "Operator `Ge` with parameter `5` against variable `TX:BLOCKING_INBOUND_ANOMALY_SCORE` (Value: `8` ) [file "/usr/local/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "222"] [id "949110"] [rev """] [msg "Inbound Anomaly Score Exceeded (Total Score: 8)"] [data """] [severity "0"] [ver "OWASP CRS/4.19.0-dev"] [maturity "0"] [accuracy "0"] [tag "anomaly-evaluation"] [tag "OWASP CRS"] [hostname "192.168.170.136"] [uri "/dvwa/vulnerabilities/sqli/] [unique_id "175764488172.546717"] [ref """]
```

3. SIEM (Security Onion/Kibana OSSEC Integration)

- Security Onion setup steps, log collection configuration, and dashboard navigation are shown.



The screenshot shows the Security Onion web interface. The left sidebar contains a navigation menu with the following items:

- Overview
- Alerts
- Dashboards
- Hunt
- Cases
- Detections
- PCAP
- Grid
- Downloads
- Administration

Below this, under "Tools", are links to Kibana, Elastic Fleet, Osquery Manager, InfluxDB, CyberChef, and Navigator.

The main content area has a title "Overview" and a section titled "Getting Started". It includes a brief introduction, instructions for using the Alerts interface, and links to the Dashboard, Network Connection Overview, DNS, Files, HTTP, and SSL sections.

On the right side, there is a sidebar with the heading "Brought to you by: Security Onion SOLUTIONS". It lists three premium services: "Security Onion Pro", "Enterprise Applia...", and "Premium Support".

Kibana Data Views Setup

To enable efficient exploration and visualization of Suricata and ModSecurity logs, custom data views (formerly called index patterns) were created in Kibana. Data views define the set of Elasticsearch indices from which Kibana reads data and specify the time field for time-based analysis.

- For Suricata alerts, the data view named "Suricata Alerts" was created using the pattern `logs-suricata.alerts-so*`. This data view aggregates all alert indices that Security Onion streams into Elasticsearch, enabling focused monitoring of network intrusion alerts.

The screenshot shows the Elasticsearch Stack Management interface. On the left sidebar, there are several sections: Management, Ingest Pipelines, Data (Index Management, Lifecycle Policies, Snapshot and Restore, Rollup Jobs, Transforms, Remote Clusters, Migrate), Alerts and Insights (Alerts, Rules, Cases, Reporting, Maintenance Windows), and Security (Users, Roles, API keys). The main area is titled "Data Views" and contains a sub-section "Create data view". The "Name" field is set to "Suricata Alerts". The "Index pattern" field shows "logs-suricata.alerts-sc*". The "Timestamp field" is set to "@timestamp". A list of index patterns is shown below, including "logs-*", "elastalert_status*", "logstash-*", "logstash-beats-*", "so-*", ".alerts-security.alerts-default", ".apm-*", ".transaction", ".kibana-event-log-*", "Beats metrics", "ES Stack Monitoring", and "Latest Cloud Security Misconfigurations - default". There is also a "Rows per page: 10" dropdown at the bottom.

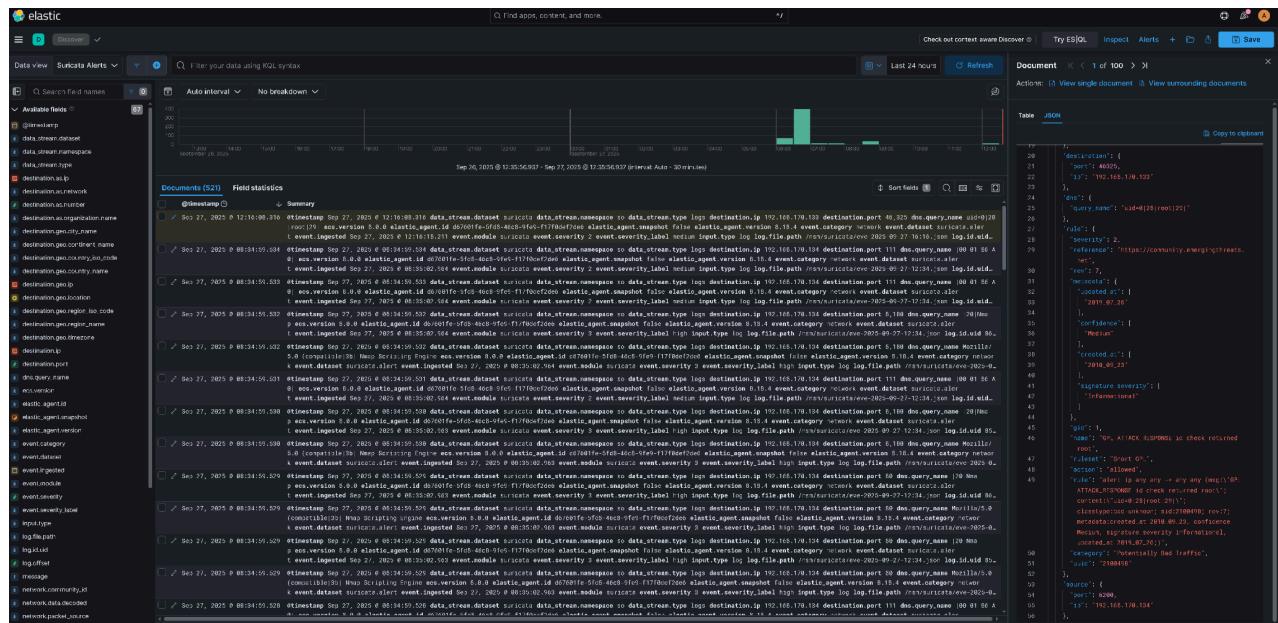
- For host and application logs forwarded via Filebeat (including ModSecurity logs), a data view named "Filebeat Logs" was created with the pattern `logs-elastic_agent.filebeat-default*`. This provides a consolidated view of host-based events and WAF activity.

This screenshot is identical to the one above, showing the "Create data view" page. The "Name" field is now set to "Filebeat logs", and the "Index pattern" field shows "logs-elastic_agent.filebeat-default*". The rest of the interface, including the sidebar and the list of index patterns, remains the same.

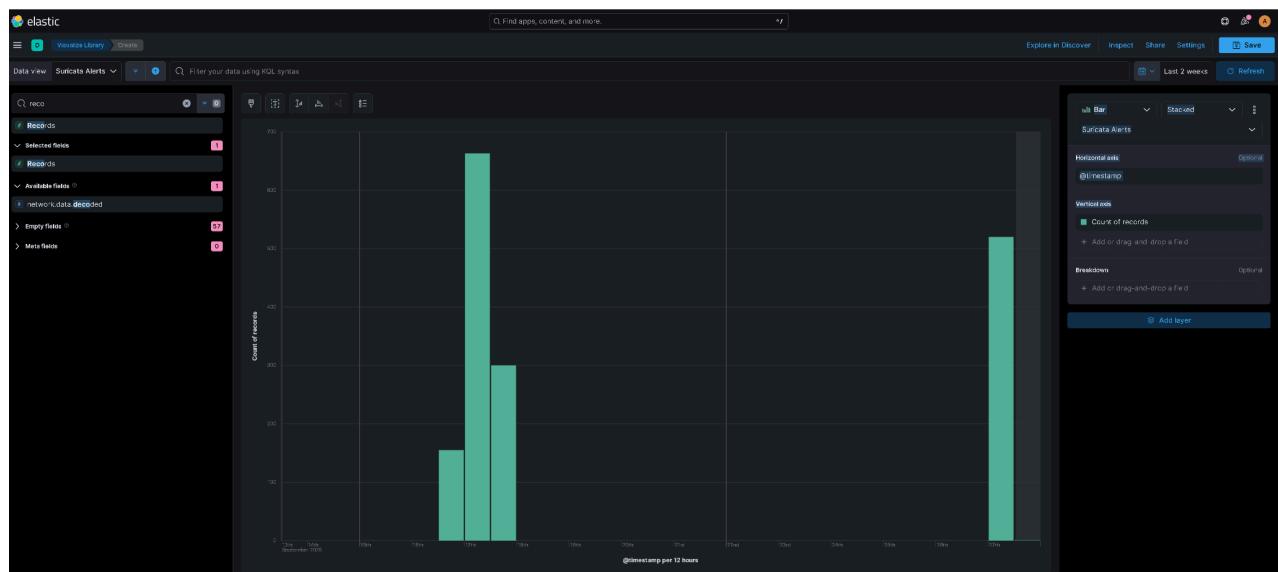
Both data views use the `@timestamp` field as the primary time filter, allowing temporal correlation and timeline visualizations of security events.

By isolating these datasets with tailored data views, Kibana enables detailed discovery queries, customized dashboards, and rapid incident investigation.

- Suricata and ModSecurity logs are sent to Kibana, where real-time alerts for brute-force and exploit attempts are displayed.



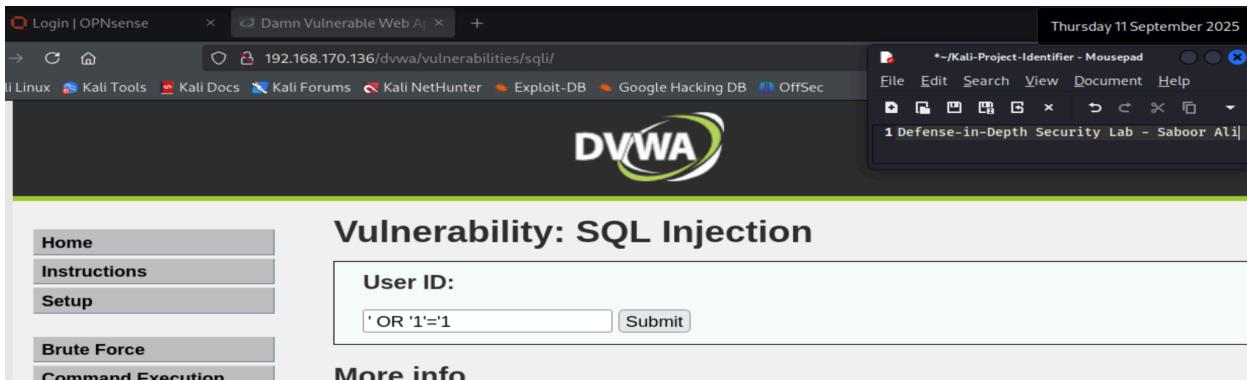
- FTP brute-force attempts, web attacks, and privilege escalation are all correlated in SIEM and visualized on a timeline.



Post-Defense Attack Testing & Validation

Attack Type	Prevented?	Visible in SIEM?	Comments
SQL Injection	Yes	Yes	WAF blocks, alert logged
XSS	Yes	Yes	WAF blocks, alert logged
Directory Traversal	Yes	Yes	WAF blocks, alert logged
Nmap Scans	No	Yes	Detected, not blocked
FTP Brute Force/Backdoor	No	Yes	Alerts log shell attempts

- Post-deployment testing verified that SQL Injection and Cross-Site Scripting attempts were intercepted and blocked by the WAF, returning HTTP 403 Forbidden responses.

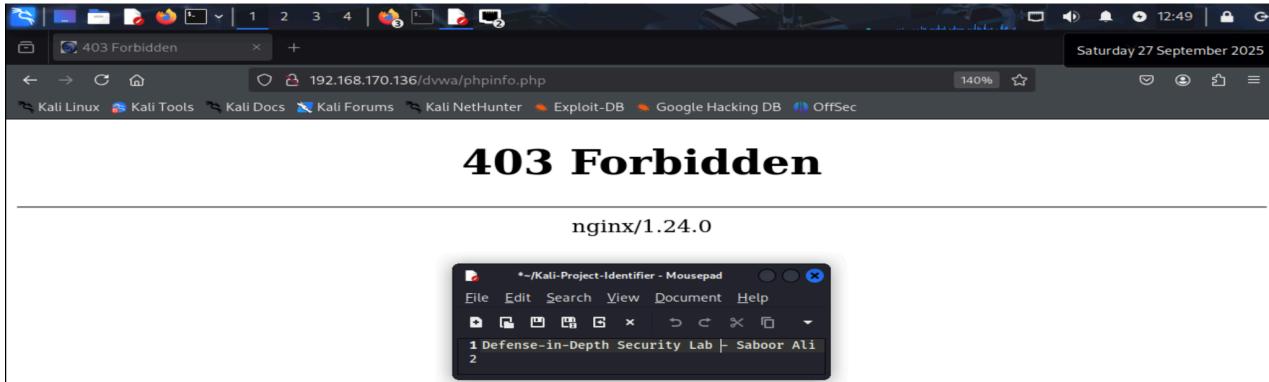


The screenshot shows a browser window for 'Damn Vulnerable Web App' at the URL '192.168.170.136/dvwa/vulnerabilities/sqli/'. The title bar says 'Login | OPNsense' and 'Thursday 11 September 2025'. The main content is titled 'Vulnerability: SQL Injection'. A sidebar on the left has links for Home, Instructions, Setup, Brute Force, and Command Execution. The main form has a 'User ID:' field containing "' OR '1'='1" and a 'Submit' button. Below the form is a 'More info' section. To the right is a mousepad application window titled '1 Defense-in-Depth Security Lab - Saboor Ali'.



The screenshot shows a browser window for '403 Forbidden' at the URL '192.168.170.136/dvwa/vulnerabilities/sqli/?id='+OR+'1'%3D1&Submit=Submit#'. The title bar says 'Login | OPNsense' and 'Thursday 11 September 2025'. The main content displays a large '403 Forbidden' error message. Below it is the text 'nginx/1.24.0'. To the right is a mousepad application window titled '1 Defense-in-Depth Security Lab - Saboor Ali'.

- Directory Traversal:** ModSecurity logs and denies attack attempts for sensitive file and directory probes.



The screenshot shows a browser window for '403 Forbidden' at the URL '192.168.170.136/dvwa/phpinfo.php'. The title bar says 'Login | OPNsense' and 'Saturday 27 September 2025'. The main content displays a large '403 Forbidden' error message. Below it is the text 'nginx/1.24.0'. To the right is a mousepad application window titled '1 Defense-in-Depth Security Lab - Saboor Ali'.

- Detected: Brute force and nmap attempts appear as alerts/events in SIEM, though prevention was incomplete.

- SIEM Forensics: Each attack, blocked or detected, is matched with corresponding forensic evidence in the SIEM dashboard.

The screenshot shows the Security Onion interface with the 'Alerts' tab selected. The main pane displays a list of alerts with columns for Count, rule.name, event.module, event.severity_label, and rule.uuid. A Notepad window titled 'Defense-In-Depth Security Lab - Saboor A11' is open in the top right corner, showing the text 'Total Found: 520'. The bottom right of the main interface shows 'Total Found: 520'.

Count	rule.name	event.module	event.severity_label	rule.uuid
348	GPL ICMP PING *NIX	suricata	low	2100386
99	ET INFO GNU/Linux APT User-Agent Outbound likely related to package management	suricata	low	2013504
36	GPL ICMP PING BSDtype	suricata	low	2100388
8	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	suricata	high	2009358
8	ET SCAN Possible Nmap User-Agent Observed	suricata	high	2024384
6	GPL RPC portmap listing TCP 111	suricata	medium	2100698
4	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010639
2	ET SCAN Suspicious inbound to MySQL port 3306	suricata	medium	2010937
2	GPL DNS named version attempt	suricata	medium	2100257
1	ET CHAT IRC authorization message	suricata	low	2000355
1	ET INFO RMI Request Outbound	suricata	high	2034718
1	ET SCAN Potential VNC Scan 5600-5820	suricata	medium	2002910
1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium	2010635
1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium	2010936
1	GPL RPC login login failure	suricata	high	2100611
1	GPL WEB_SERVER 403 Forbidden	suricata	medium	2101201

Limitations & Observations

- Certain attacks, such as Nmap scans and brute force attempts were effectively detected and correlated within the SIEM but not fully prevented by the existing controls.
 - The defense-in-depth approach demonstrated is most effective against known web exploitation vectors (SQL Injection, XSS, Directory Traversal) while challenges remain for network reconnaissance and credential-based brute force attacks.
 - This project represents the initial stage of security implementation. Further security automation and orchestration will be explored in upcoming phases using SOAR (Security Orchestration, Automation, and Response) platforms.
 - Planned improvements include integrating SOAR capabilities for automated alert triage, coordinated incident responses, and potentially enhanced blocking mechanisms to cover gaps left by traditional prevention systems.
-

Conclusion

This lab experimentally validates a robust layered security architecture combining network-level and application-layer controls with centralized security monitoring. Deploying OPNsense as a Next-Generation Firewall, ModSecurity as a Web Application Firewall, and Security Onion as a SIEM platform, this defense-in-depth model demonstrated the capacity to mitigate a broad spectrum of threats effectively.

Proactive configurations successfully blocked high-risk web attacks like SQL Injection, Cross-Site Scripting, and directory traversal attempts. At the same time, the SIEM environment enabled detection and correlation of reconnaissance and brute force activities, underscoring the importance of monitoring amidst evolving threat landscapes.

Visual tools such as the Kibana alert timeline allowed clear observation of attack patterns and temporal distributions, reinforcing data-driven analytics as central to modern cybersecurity practice. This layered approach reduces system exposure while enhancing visibility into attacker behaviors, creating a scalable and pragmatic security strategy.

Importantly, this project underscores the reality that no single control is sufficient; full resilience requires a fusion of prevention, detection, and continuous monitoring fortified by emerging technologies like SOAR. Future enhancements will leverage SOAR platforms to automate alert handling, orchestrate complex responses, and aim to mitigate currently unblocked attack vectors, further strengthening organizational defenses in an ever-shifting threat environment.