

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

Prepared by: Saboor Ali

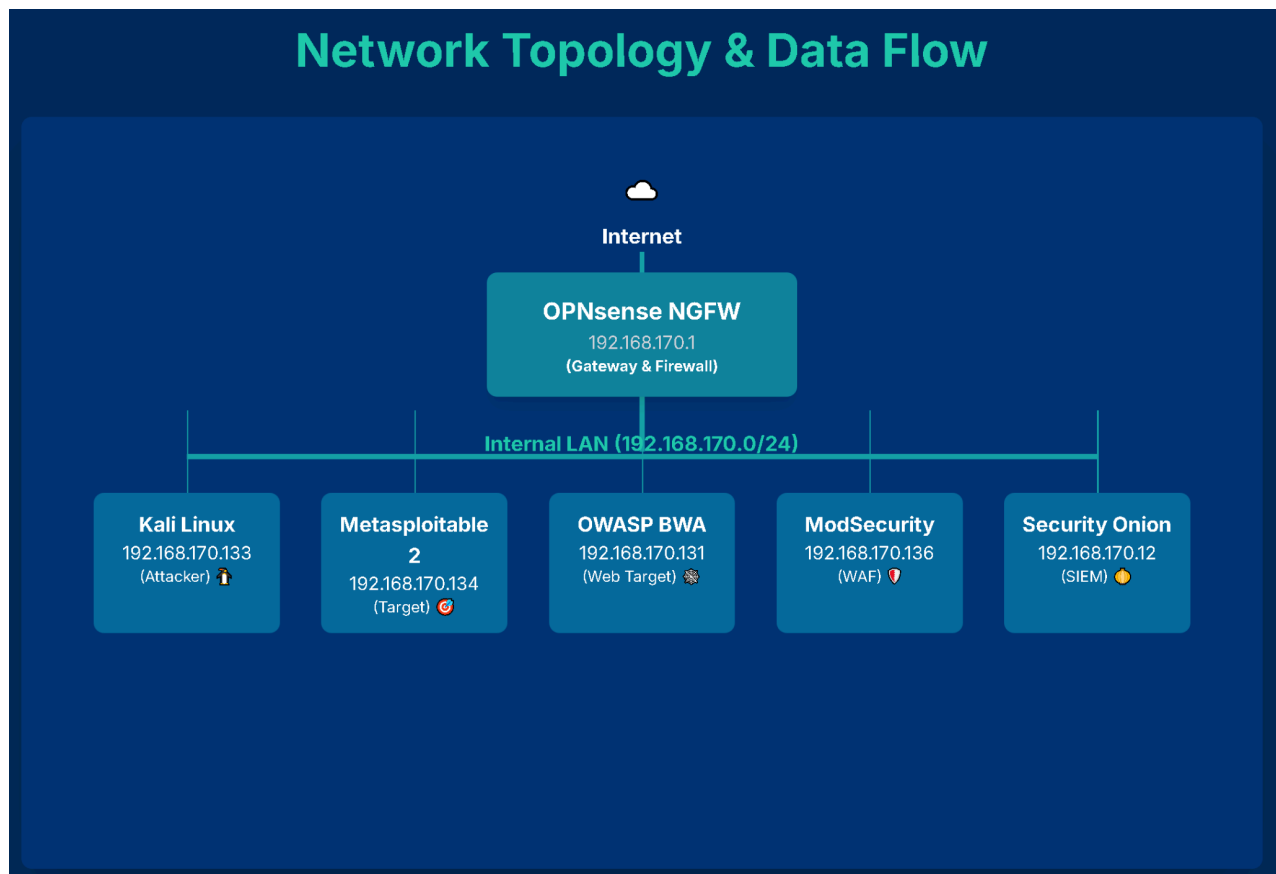
Date: September 27, 2025

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

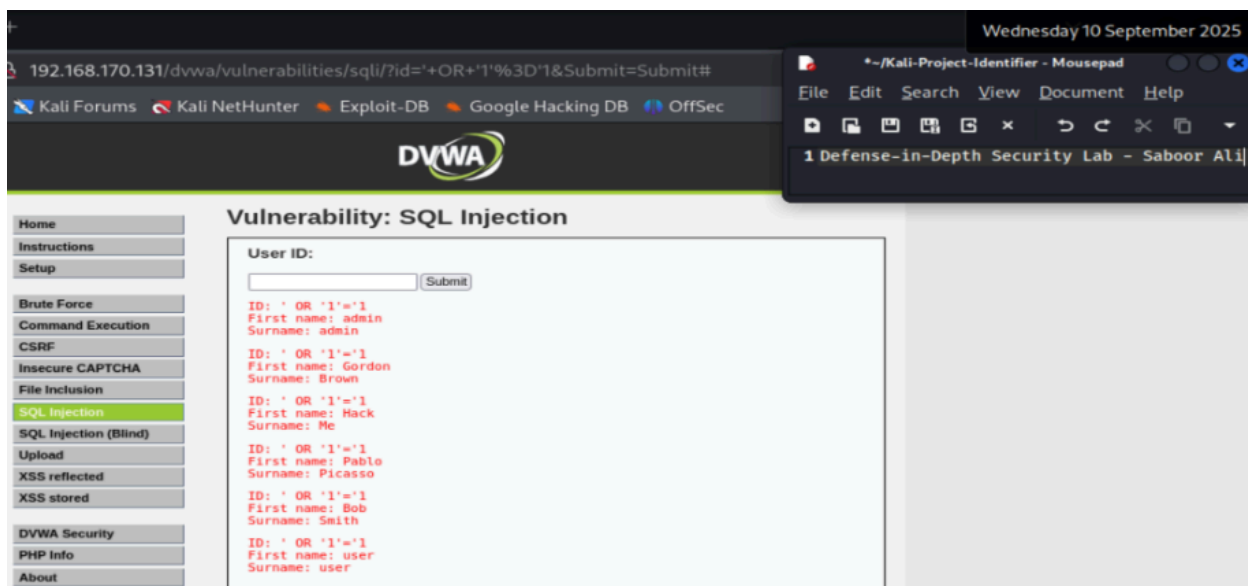
VMs include Kali Linux (attacker), Metasploitable 2, OWASP BWA/DVWA (vulnerable targets), OPNsense (NGFW), Security Onion (SIEM) and ModSecurity WAF. All IP assignments used DHCP; IPs vary in attack logs due to later changes—static IP steps are omitted as not essential to defense outcomes.



Baseline Vulnerability Testing (Pre-defense)

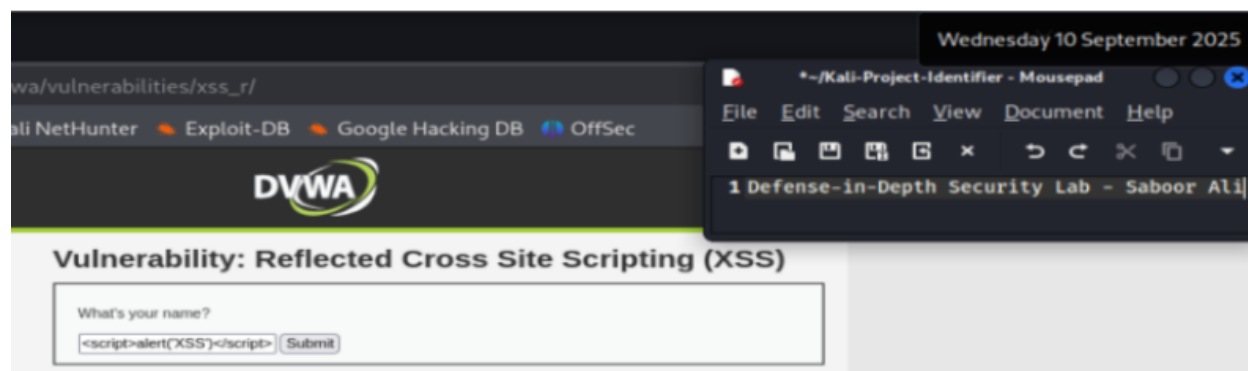
Vulnerability: SQL Injection

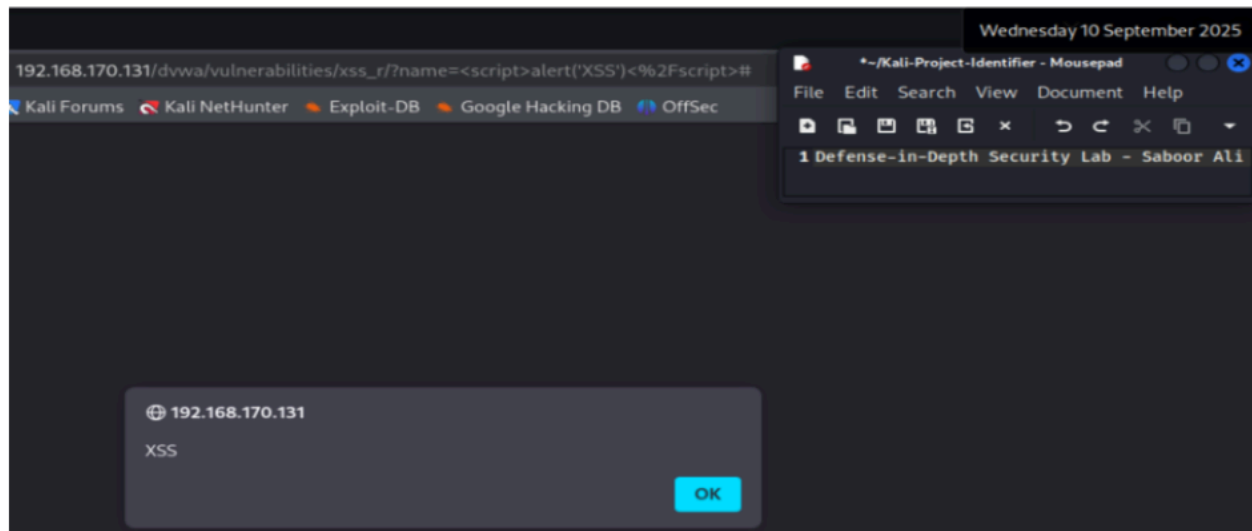
- A SQL Injection attack using the OR 1=1 payload against DVWA successfully bypassed authentication controls, resulting in unauthorized access and data exfiltration.



Vulnerability: Cross-Site Scripting (XSS)

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





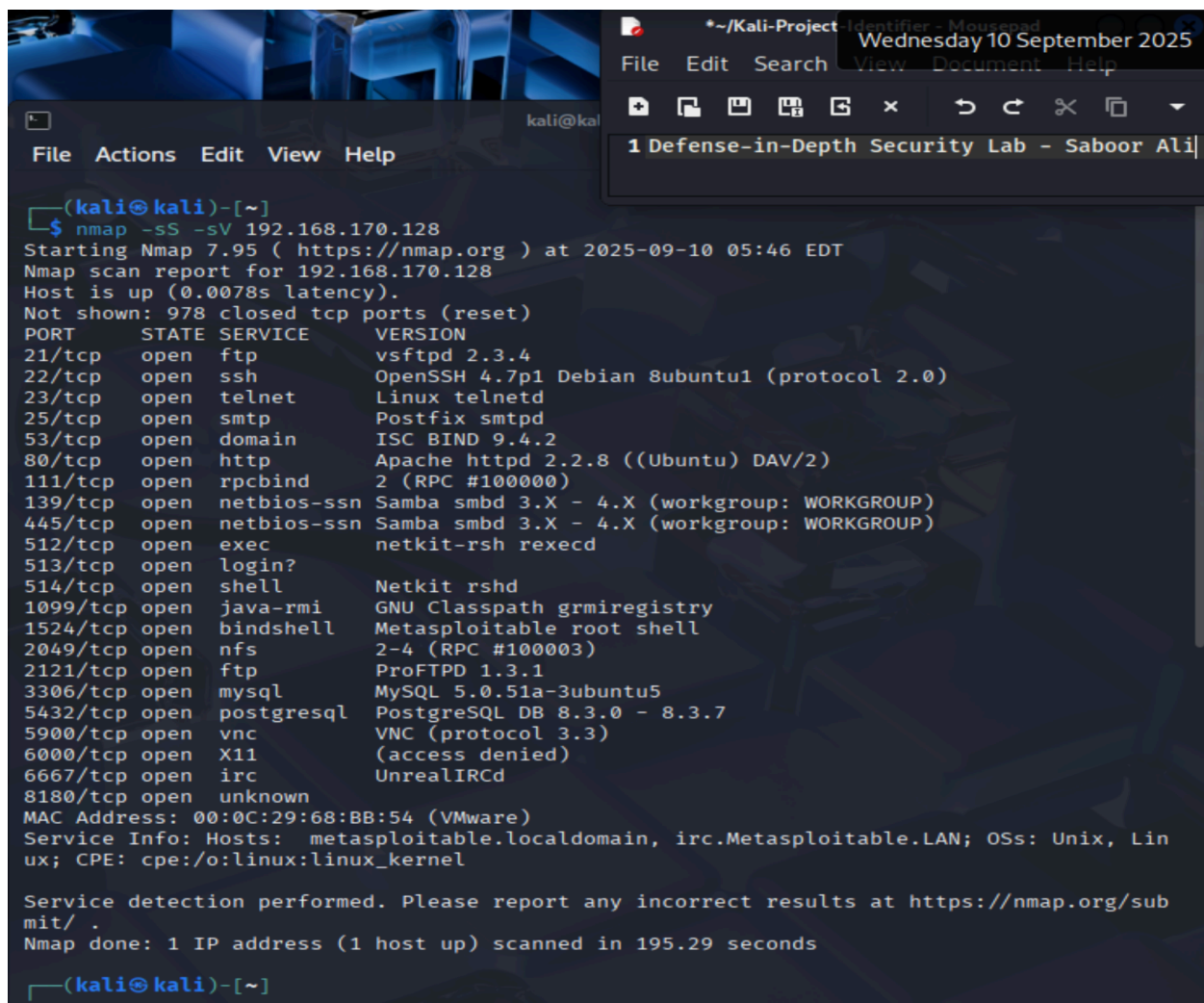
Vulnerability: Directory Traversal and Information Exposure

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

PHP Version 5.3.2-1ubuntu4.30	
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_mysql.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626.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.



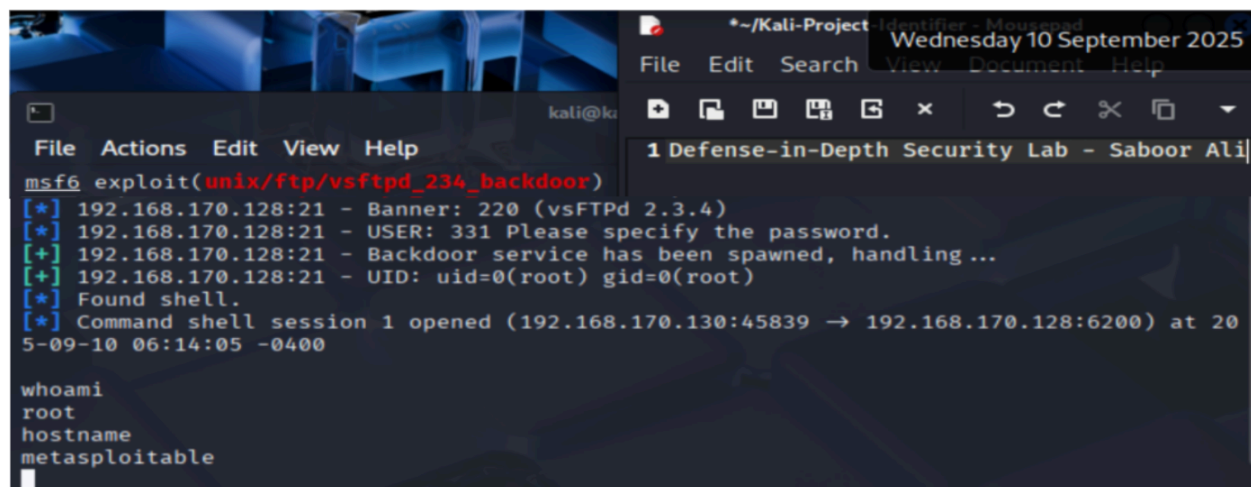
```
(kali@kali)-[~]
$ nmap -sS -sV 192.168.170.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-10 05:46 EDT
Nmap scan report for 192.168.170.128
Host is up (0.0078s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
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?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
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, Lin
ux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
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.



```
msf6 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.

```
kali-linux-2025.1a-vmware-amd... Metasploit2-Linux NGFW (OPNsense) OWASP Broken Web Apps VM ... SecurityOnion WAF-ModSecurity

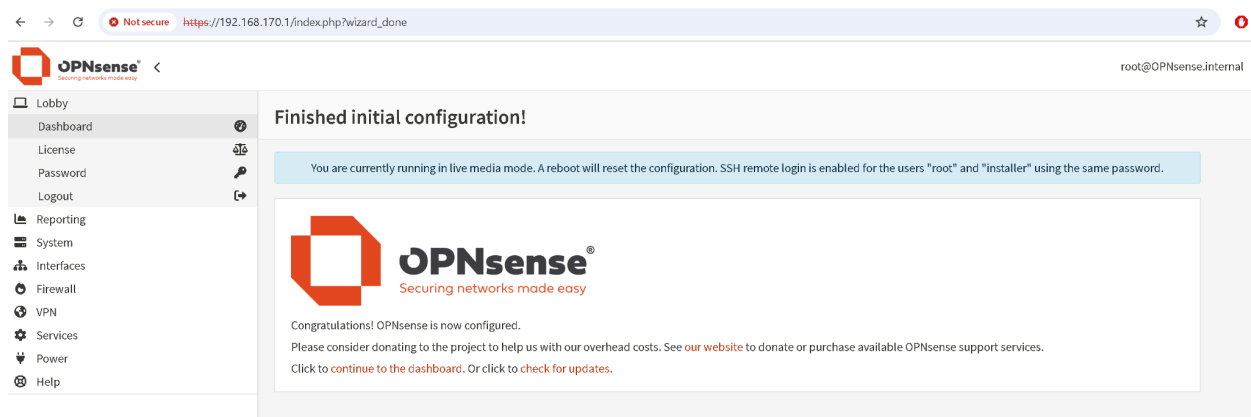
: Website:      https://opnsense.org/      :
: Handbook:    https://docs.opnsense.org/  :
: Forums:      https://forum.opnsense.org/ :
: Code:        https://github.com/opnsense :
: Reddit:      https://reddit.com/r/opnsense :
: -----
:
*** OPNsense.internal: OPNsense 25.7 (amd64) ***

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
3) Reset the root password
4) Reset to factory defaults
5) Power off system       10) Firewall log
6) Reboot system          11) Reload all services
                          12) Update from console
                          13) Restore a backup

Enter an option: 
```



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

The screenshot displays the OPNsense Firewall Rules configuration for the LAN interface. The interface shows a list of rules with columns for Protocol, Source, Port, Destination, Port, Gateway, Schedule, and Description. Rules include ICMP, TCP, and UDP configurations for various ports and protocols, with some rules marked as disabled or active.

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
ICMP	IPV4-6 *	*	*	*	*	*	Default deny / state-violation rule
ICMP	IPV4-6-ICMP	*	*	*	*	*	IPv6 RFC4890 requirements (ICMP)
ICMP	IPV4-6-ICMP	(self)	fe80::10, fe80::16	*	*	*	IPv6 RFC4890 requirements (ICMP)
ICMP	IPV4-6-ICMP	fe80::10	fe80::10, fe80::16	*	*	*	IPv6 RFC4890 requirements (ICMP)
ICMP	IPV4-6-ICMP	fe80::16	fe80::10	*	*	*	IPv6 RFC4890 requirements (ICMP)
ICMP	IPV4-6-ICMP	*	fe80::16	*	*	*	IPv6 RFC4890 requirements (ICMP)
TCP/UDP	IPV4-6 TCP/UDP	*	0	*	*	*	block all targeting port 0
TCP/UDP	IPV4-6 TCP/UDP	*	*	0	*	*	block all targeting port 0
TCP	IPV4-6 TCP	~sshlockout~	(self)	22 (SSH)	*	*	sshlockout
TCP	IPV4-6 TCP	~sshlockout~	(self)	443 (HTTPS)	*	*	sshlockout
TCP	IPV4-6 TCP	~sshlockout~	*	*	*	*	vsftpd overload table
UDP	IPV4-6 UDP	*	68	255, 255, 255, 255	67	*	allow access to DHCP server
UDP	IPV4-6 UDP	*	68	(self)	67	*	allow access to DHCP server
UDP	IPV4-6 UDP	(self)	67	*	68	*	allow access to DHCP server
UDP	IPV4-6 UDP	fe80::10	fe80::10, fe80::16	546	*	*	allow access to DHCP server
UDP	IPV4-6 UDP	fe80::10	fe80::10	547	*	*	allow access to DHCP server
UDP	IPV4-6 UDP	fe80::10	(self)	546	*	*	allow access to DHCP server
UDP	IPV4-6 UDP	(self)	547	fe80::10	*	*	allow access to DHCP server
TCP	IPV4-6 *	*	*	*	*	*	let out anything from firewall host itself
TCP	IPV4-6 TCP	*	(self)	80 (HTTP)	*	*	anti-lockout rule
TCP	IPV4-6 TCP	*	(self)	443 (HTTPS)	*	*	anti-lockout rule
TCP	IPV4-6 *	(any)	*	! WAN net	WAN_DHCP	*	let out anything from firewall host itself (force gw)
TCP	IPV4 TCP	ftp_bruteforce_block	*	21 (FTP)	*	*	Block brute force FTP
TCP	IPV4 *	LAN net	*	*	*	*	Default allow LAN to any rule
TCP	IPV6 *	LAN net	*	*	*	*	Default allow LAN IPv6 to any rule

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


OPNsense® <
 root@

- Reporting
- System
- Interfaces
- Firewall
- VPN
- Services
 - Captive Portal
 - DHCRelay
 - Dnsmasq DNS & DHCP
 - Intrusion Detection
 - Administration
 - Policy
 - Log File
 - ISC DHCPv4
 - ISC DHCPv6

Services: Intrusion Detection: Administration

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

Settings
Download
Rules
User defined
Alerts
Schedule

☒ advanced mode

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.


OPNsense® <
 root@OPNsense.internal

- Reporting
- System
- Interfaces
- Firewall
- VPN
- Services
 - Captive Portal
 - DHCRelay
 - Dnsmasq DNS & DHCP
 - Intrusion Detection
 - Administration
 - Policy
 - Log File

Services: Intrusion Detection: Administration

We strongly advise to use policies instead of single rule based changes to limit the size of the configuration. A list of all manual changes can be revised in the policy editor (available here)

Settings
Download
Rules
User defined
Alerts
Schedule

Search

☒
☒

2025/09/17 11:15

7

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 backdoor
2025-09-17T11:15:33.470879+0000	900001	blocked	em1	192.168.170.133	33159	192.168.170.134	6200	Possible vsftpd backdoor

2. Web Application Firewall (WAF) ModSecurity

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

7

```
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 ABIDDEFHZ
SecDebugLog /usr/local/nginx/logs/modsec_debug.log
SecDebugLogLevel 3

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

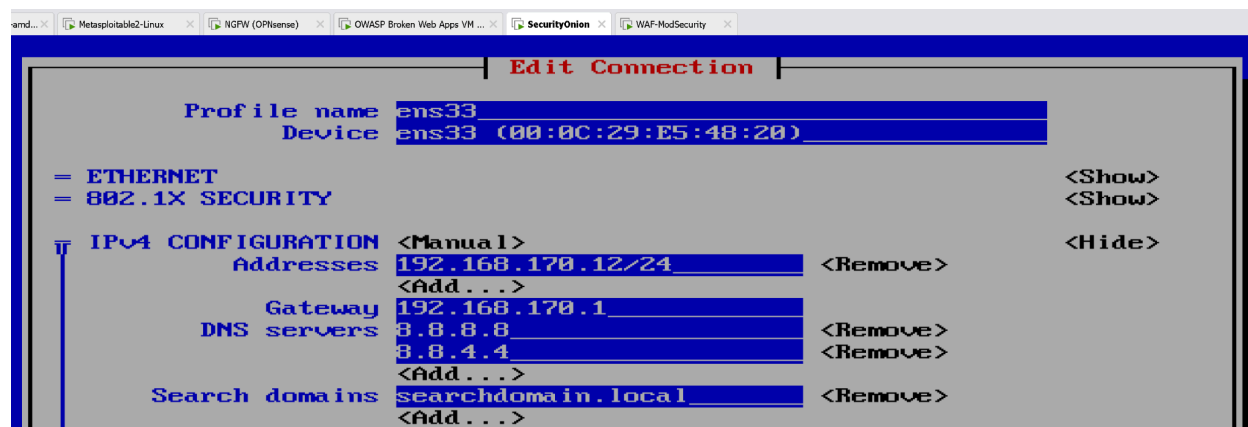
# Include all CRS rules
Include /usr/local/modsecurity-crs/rules/*.conf
```

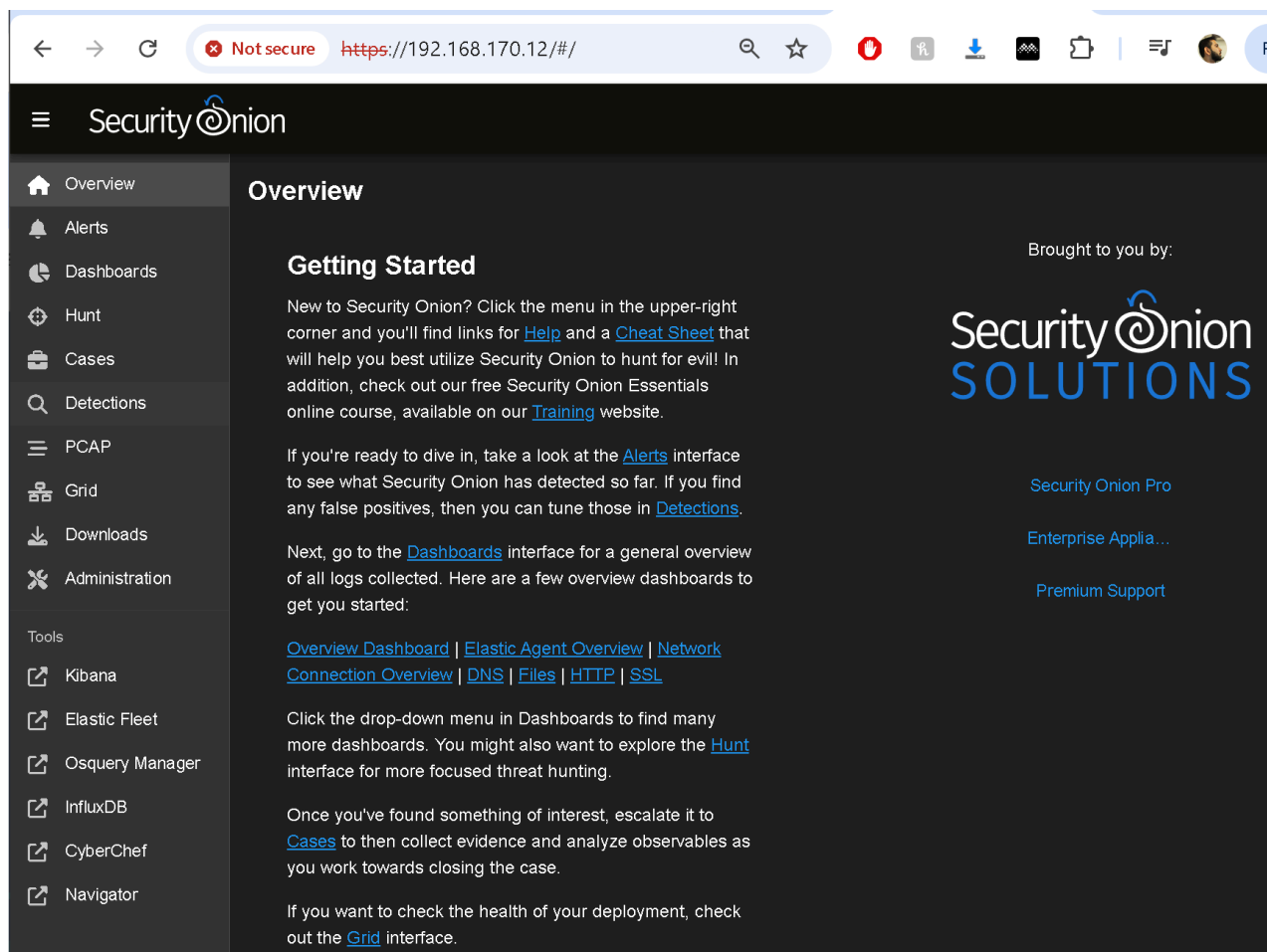

- **Example Mitigation:** SQL Injection attempts receive HTTP 403; detection logged.

```
waf@waf-modsecurity:/usr/local/nginx/logs$ tail modsec_audit.log
ModSecurity: Warning. Matched 'Operator `Rx' with parameter `(?^[Nd.]+\[\[\\da-f:]+\]\[\\da-f:]+\)(:([Nd.]+)?$)' 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 "o0,15o0,15v86,15"]
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.

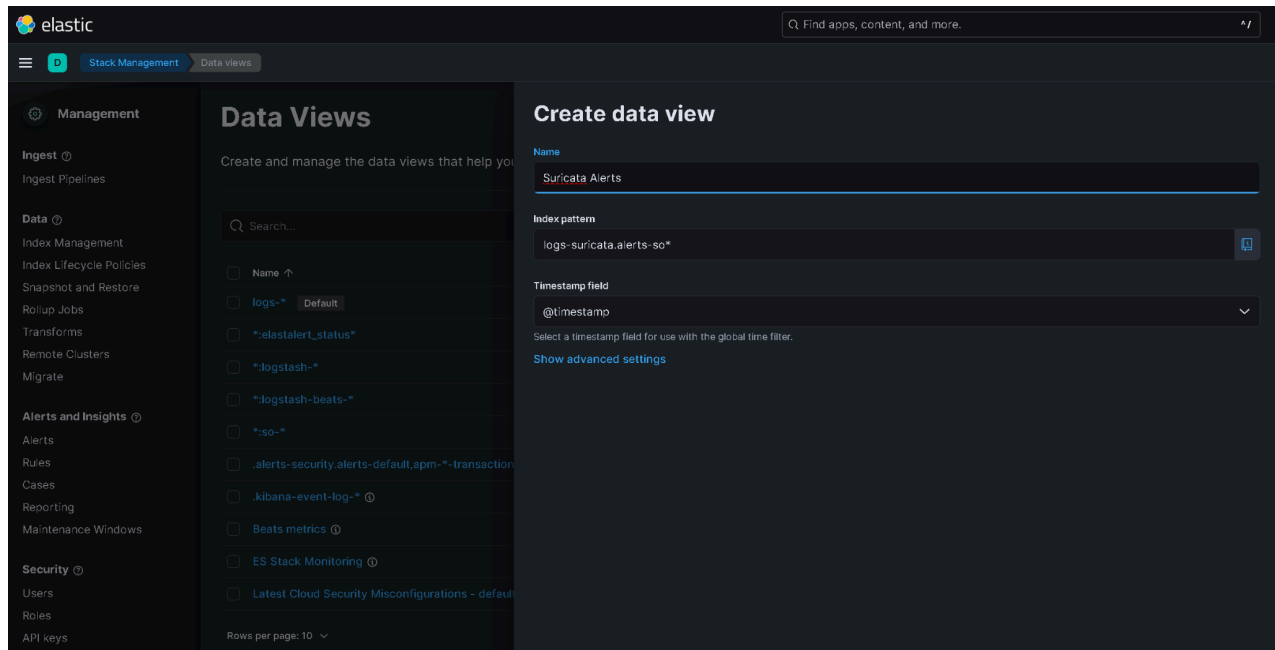




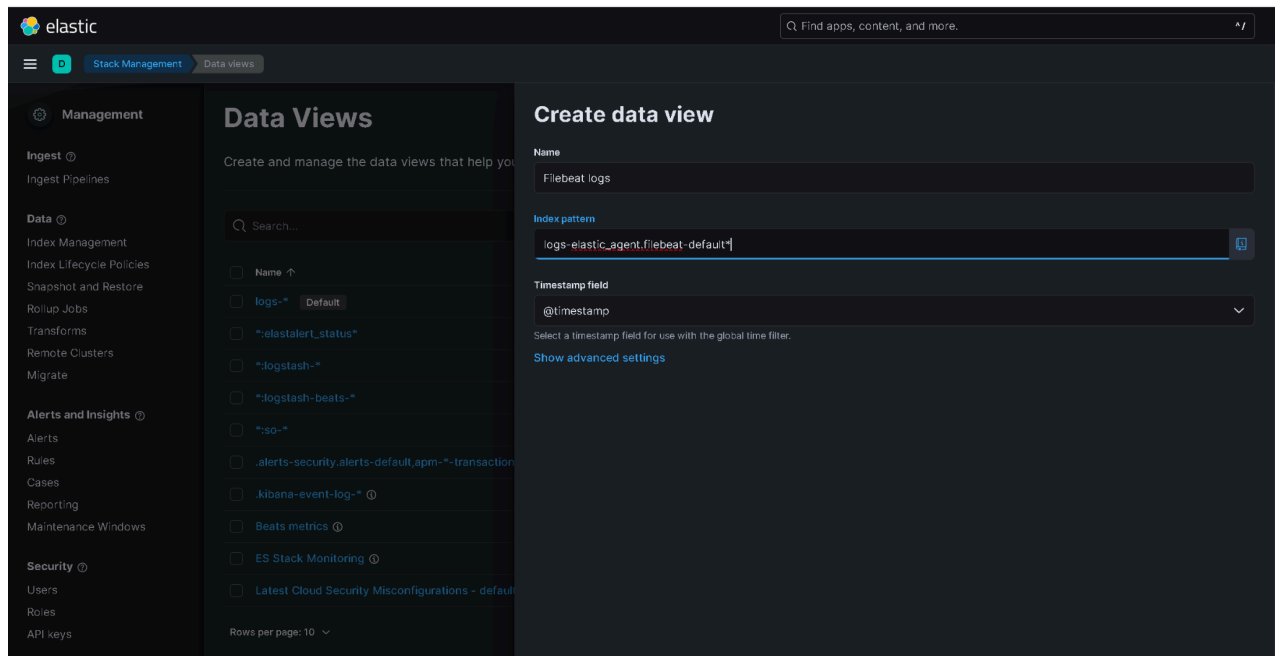
Kibana Data Views Setup

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.



- 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.



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.

- [illegible]

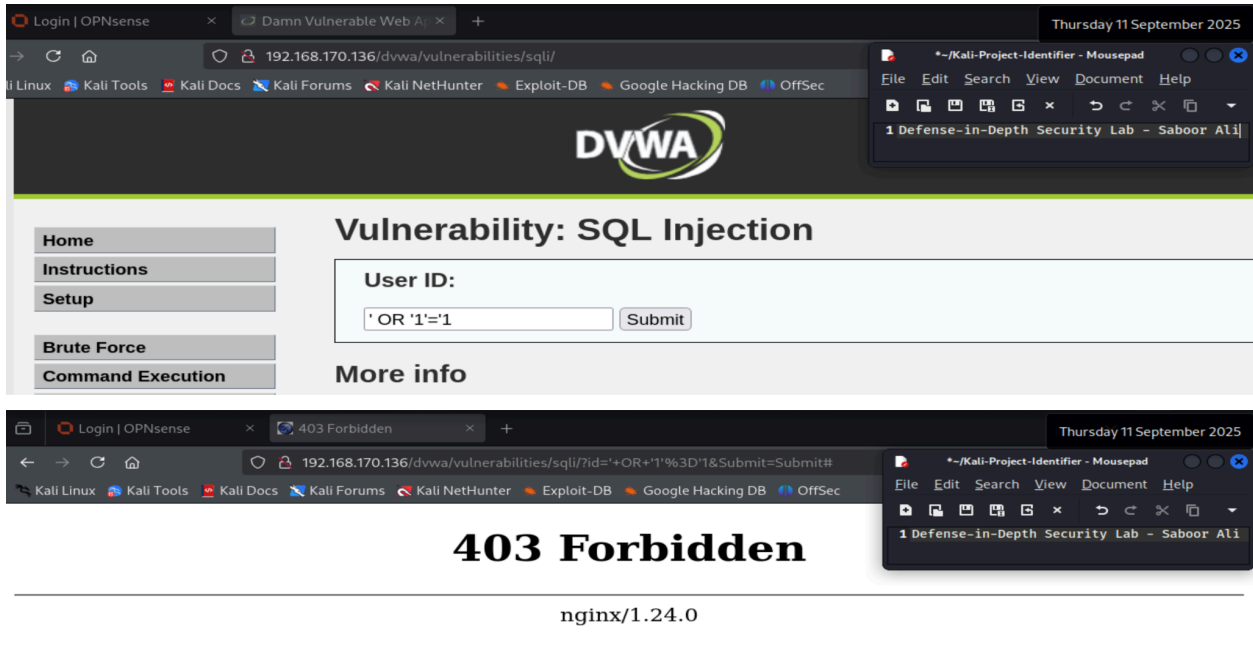
- The screenshot displays the Elastic Stack Kibana interface. At the top, the 'elastic' logo is visible. The main navigation bar includes 'Visualize Library', 'Visualize', 'Discover', 'Dashboard', and 'Settings'. The 'Visualize' tab is active, showing a bar chart titled 'Duplicate Alerts'. The chart's x-axis is labeled '@timestamp per 12 hours' and the y-axis is labeled 'Count of records'. The chart shows four bars of different heights, representing the count of duplicate alerts over time. The bars are colored in a light blue/grey shade. On the right side, there is a sidebar with a 'Visualize' panel. This panel contains a 'Visualize Alerts' section with a 'Horizontal axis' set to '@timestamp' and a 'Vertical axis' set to 'Count of records'. Below this, there are sections for 'Breakdowns' and 'Add layer'. The 'Breakdowns' section is currently empty. The 'Add layer' button is visible at the bottom of the sidebar.

@timestamp per 12 hours	Count of records
2020-10-20T00:00:00.000Z	150
2020-10-20T12:00:00.000Z	350
2020-10-20T24:00:00.000Z	200
2020-10-21T12:00:00.000Z	250

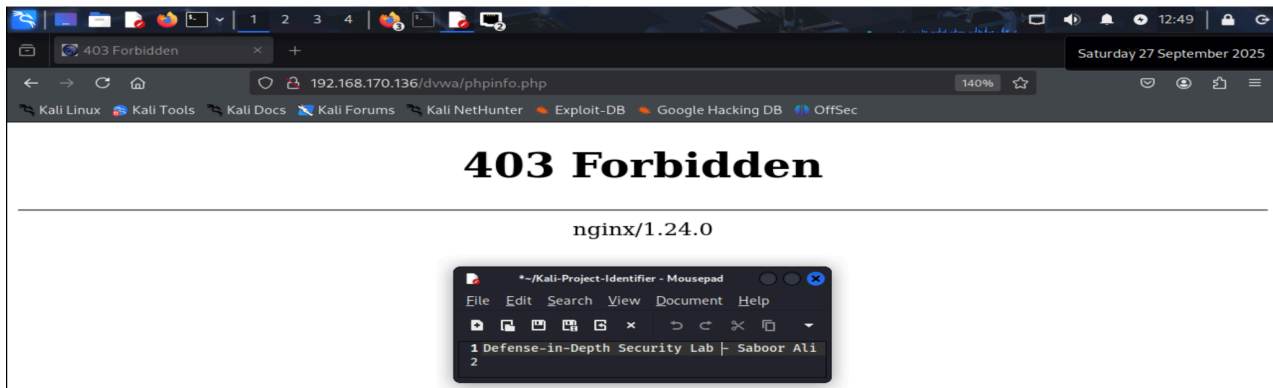
Post-Defense Attack Testing & Validation

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.



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



- [illegible]

- Security Onion

Overview

Alerts

Dashboards

Hunt

Cases

Detections

PCAP

Grid

Downloads

Administration

Tools

Kibana

Elastic Fleet

Osquery Manager

InfluxDB

CyberChef

Navigator

Alerts

Options

File Edit Format View Help

Defense-in-Depth Security Lab - Saboor Ali

Ln 1, Col 43 100% Windows (CRLF) UTF-8

Total Found: 62

Group By Name, Module

Fetch Limit 500

Filter Results

Click the clock icon to change to absolute time

hours

REFRESH

	Count	rule.name	event.module	event.severity_label	rule.sid
>	348	GPL ICMP PING *NIX	suricata	low	2100366
>	99	ET INFO GNU/Linux APT User-Agent Outbound likely related to package management	suricata	low	2013504
>	36	GPL ICMP PING BSDtype	suricata	low	2100368
>	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	2024364
>	6	GPL RPC portmap listing TCP 111	suricata	medium	2100598
>	4	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010939
>	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 5800-5820	suricata	medium	2002910
>	1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium	2010935
>	1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium	2010936
>	1	GPL RPC rlogin login failure	suricata	high	2100611
>	1	GPL WEB_SERVER 403 Forbidden	suricata	medium	2101201

Items per page: 50

1-16 of 16

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.