

**take the screenshots from inside this documentation and place them appropriately in the new documentation with appropriate descriptions and steps**

The screenshots from your "Screenshots.pdf" show every critical step, validation, and alert as the lab environment was configured and defense mechanisms deployed. These will be placed throughout the new documentation with concise context and explanations for each technique and mitigation step.[[1]](#fn1)

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

Prepared by: Saboor Ali  
Date: September 10, 2025

**Overview**

This lab replicates a real-world enterprise setup to showcase defense-in-depth controls—Next-Generation Firewall (NGFW), Web Application Firewall (WAF), and Security Information and Event Management (SIEM)—against network and web application attacks. VMware orchestrates the attacker (Kali Linux), vulnerable targets (Metasploitable 2, OWASP BWA/DVWA), and security VMs. Screenshots are provided at critical steps.[[1]](#fn1)

**Lab Environment Setup**

* VM layout and static IP configuration is shown in screenshots confirming network assignments (eth0 for Metasploitable, eth0/eth1 for firewall, LAN/WAN for OPNsense).[[1]](#fn1)
  + [Lab and network configuration screenshot][[1]](#fn1)

**Baseline Vulnerability Testing (Pre-Defense)**

**Vulnerability: SQL Injection**

* DVWA is set to low security and attacked using OR 1=1 payload to bypass authentication.
* Screenshot evidence of successful unauthorized login and dumped user data is provided.
  + [Screenshot: SQL Injection leading to login bypass][[1]](#fn1)

**Vulnerability: Cross-Site Scripting (XSS)**

* <script>alert('XSS')</script> submitted in the DVWA XSS module successfully triggers a JavaScript pop-up in the browser.
* Validation: Web browser displays execution of injected script.
  + [Screenshot: Reflected XSS popup][[1]](#fn1)

**Vulnerability: Brute-Force Attack**

* Hydra is used to perform brute-force password guessing against ftp192.168.170.134.
* Output confirms msfadmin/msfadmin credentials were discovered.
  + [Screenshot: Hydra brute-force result][[1]](#fn1)

**Vulnerability: Directory Traversal and Information Exposure**

* Access to /phpinfo.php and /test/ directly shows PHP info and test directory.
  + [Screenshot: phpinfo.php and test directory results][[1]](#fn1)

**Vulnerability: Network Enumeration**

* Nmap scans reveal extensive open services and version banners on Metasploitable.
  + [Screenshot: Nmap scan output][[1]](#fn1)

**Security Controls Deployment**

**1. NGFW (OPNsense) Setup**

* OPNsense VM is installed and configured with dual interfaces. Web UI confirms system status.
  + [Screenshot: OPNsense dashboard][[1]](#fn1)
* **LAN rules:** Allow only HTTP(S), SSH for management; FTP restricted. Brute-force countermeasures implemented with address block alias and connection thresholds.
  + [Screenshot: OPNsense firewall rule/alias setup][[1]](#fn1)
* **IPS/IDS Setup:** Suricata enabled in OPNsense dashboard with alerting and blocking of known malicious signatures.
  + [Screenshot: Suricata alert logs][[1]](#fn1)
* **Mitigation Example:** A detected vsFTPd backdoor attack is promptly blocked by custom drop rule and surfaced in SIEM dashboard.
  + [Screenshot: Blocked vsFTPd backdoor alert][[1]](#fn1)

**2. Web Application Firewall (WAF) ModSecurity**

* ModSecurity enabled for Nginx reverse proxy in front of DVWA/OWASP BWA targets. Configuration files and rules verified in shell and nano editor.
  + [Screenshot: ModSecurity configuration][[1]](#fn1)
* **Rules Activated:** OWASP CRS loaded, including detection-only and blocking modes.
* **Example Mitigation:** SQL Injection attempts immediately result in HTTP 403 Forbidden; log entries confirm SQLi detection with libinjection and CRS rules.
  + [Screenshot: 403 Forbidden from ModSecurity and log extract][[1]](#fn1)
* **XSS:** Payloads containing scripts are blocked; ModSecurity audit logs and browser show denied requests.
  + [Screenshot: XSS payload blocked, log evidence][[1]](#fn1)

**3. SIEM (Security Onion/Kibana OSSEC Integration)**

* Security Onion setup steps, log collection configuration, and dashboard navigation are shown.
  + [Screenshot: Security Onion setup and dashboard][[1]](#fn1)
* Suricata and ModSecurity logs are sent to Kibana, where real-time alerts for brute-force and exploit attempts are displayed.
  + [Screenshot: SIEM alert showing brute-force detected][[1]](#fn1)
* FTP brute-force attempts, web attacks, and privilege escalation are all correlated in SIEM and visualized on timeline.
  + [Screenshot: Multi-vector alert correlation in SIEM][[1]](#fn1)

**Post-Defense Attack Testing & Validation**

* **SQL Injection and XSS**: Attack requests instantly blocked by WAF, with 403 code seen on user browser and explanation lines in the logs.
  + [Screenshot: Browser 403, SIEM SQLi/XSS alert][[1]](#fn1)
* **Brute-force attempts**: OPNsense and Suricata coordinate to lock out sources after a set number of failures; corresponding SIEM alerts logged.
  + [Screenshot: Suricata/Firewall brute-force mitigation][[1]](#fn1)
* **Directory Traversal**: ModSecurity logs and denies attack attempts for sensitive file and directory probes.
  + [Screenshot: 403 on directory traversal, ModSecurity logs][[1]](#fn1)
* **Exploit Attempts**: SIEM and firewall dashboards show drop events, source IPs, and signatures for blocked attacks like vsFTPd and payload delivery.
  + [Screenshot: SIEM forensic timeline for exploit][[1]](#fn1)

**Mapping of Screenshots to Steps**

|  |  |  |
| --- | --- | --- |
| Step/Threat | Screenshot Description | Reference |
| Network assignment/config | NIC and interface setup | [[1]](#fn1) |
| SQLi exploit | DVWA login bypass & dump | [[1]](#fn1) |
| XSS | Browser popup, blocked response | [[1]](#fn1) |
| Hydra brute-force | Terminal output, ftp login found | [[1]](#fn1) |
| phpinfo/test directory | Browser/file explorer listing | [[1]](#fn1) |
| Nmap scan | Nmap result output | [[1]](#fn1) |
| OPNsense firewall/alerts | Rules, dashboard UI, IPS alerts | [[1]](#fn1) |
| ModSecurity config/logs | Blocked (403) response, log detail | [[1]](#fn1) |
| Security Onion/Kibana | SIEM UI, alert tracker, timelines | [[1]](#fn1) |

Each screenshot and its description is placed directly within its relevant procedure or validation section for maximum clarity, following industry best practices for technical documentation.[[2]](#fn2)[[1]](#fn1)

⁂

1. Screenshots.pdf

1. <https://www.archbee.com/blog/screenshots-in-technical-documentation>