# 30-Day Host-Based Full-Stack NIDS Project



This comprehensive timeline is designed to guide you through the deployment of a professional-grade host-based Network Intrusion Detection System (NIDS) using Suricata, ELK stack, and custom automation for threat intelligence and alerting.

## WEEK 1: Core NIDS Deployment (Days 1–5)



Day Goal Tasks



**lo**

**eth0**

1 Environment Setup Install Suricata, identify interface (e.g., , )

|  |  |  |
| --- | --- | --- |
| 2 | Suricata Tuning | Update default rules, enable JSON logging |
| 3 | Local Rules | Write/test custom Suricata rules (ICMP, HTTP scan, DNS tunnel) |
| 4 | Traffic Simulation | Use **nmap** , **netcat** , **curl** , and verify detections |
| 5 | Basic Log Parsing | Use **jq** , **grep** , or a Python script to summarize logs |

## WEEK 2: SIEM Stack Integration (Days 6–10)



Day Goal Tasks

|  |  |  |
| --- | --- | --- |
| 6 | Filebeat Setup | Install Filebeat, forward **eve.json** to Elasticsearch |
| 7 | Elasticsearch | Install & configure locally (limit heap usage for performance) |
| 8 | Kibana | Install UI, create Suricata index & visualizations |
| 9 | Dashboards | Build widgets: top alerts, IPs, ports, signatures |
| 10 | Correlation Testing | Simulate multi-stage attack, review detection flow |

## WEEK 3: Automation, Alerting & Hardening (Days 11–15)



Day Goal Tasks

|  |  |  |
| --- | --- | --- |
| 11 | Auto Start & Health | Configure Suricata/Filebeat systemd + health checks |
| 12 | Alerting | Use **ElastAlert** or custom Python to send email/Slack alerts |

Day Goal Tasks

|  |  |  |
| --- | --- | --- |
| 13 | Log Rotation | Set logrotate for Suricata & Filebeat logs |
| 14 | Rule Auto-Update | Cron **suricata-update** weekly, custom rule loader |
| 15 | Host Hardening | UFW, SSH audit, fail2ban, disable unused services |

## WEEK 4: Intelligence, Reporting & Finalization (Days 16–20)

Day Goal Tasks

|  |  |  |
| --- | --- | --- |
| 16 | Threat Intel | Add Abuse.ch, OTX lookups, or write feed parsers |
| 17 | IP Auto-Blocking | Python script: auto-block IPs from Suricata alerts |
| 18 | Report Generation | Daily/weekly summary script, generate HTML/PDF reports |
| 19 | Final Simulation | Launch multiple attacks, test full detection+alert chain |
| 20 | Documentation | Markdown/PDF: architecture, configs, lessons learned |

## WEEK 5: Threat Emulation & Response (Days 21–25)



Day Goal Tasks

|  |  |  |
| --- | --- | --- |
| 21 | MITRE ATT&CK  Mapping | Map Suricata rules and alerts to MITRE ATT&CK tactics/techniques |
| 22 | Adversary Simulation | Use tools like **Atomic Red Team** , **CALDERA** , or **Metasploit** |
| 23 | Response Playbooks | Create YAML/Markdown-based IR playbooks based on Suricata alerts |
| 24 | Endpoint Response Link | Use **osquery** or **Velociraptor** to pivot from alert → endpoint query |

## WEEK 6: Network Edge & Resume Polish (Days 26–30)



Day Goal Tasks

|  |  |  |  |
| --- | --- | --- | --- |
| 25 | Remote Log Collection | Use **rsyslog** , other hosts | **Filebeat** , or **Logstash** to collect logs from |

Day Goal Tasks

|  |  |  |
| --- | --- | --- |
| 26 | Encrypted Log Forwarding | Setup TLS on Filebeat → Logstash → Elasticsearch pipeline |
| 27 | Final Reporting & Portfolio | Export reports to PDF, build dashboards, GitHub README.md project page |
| 28 | Resume Highlight + GitHub | Create a section on your resume and GitHub showcasing architecture, tech used, results |

# Suggested Cron Jobs



Set up the following cron jobs to maintain system health and ensure automation:

* Suricata Rule Updates (weekly):

**03\*\*1/usr/bin/suricata-update>>/var/log/suricata/update.log2>&1**

* Custom Rule Loader (weekly):

**04\*\*1/opt/custom\_rules/loader.sh>>/var/log/suricata/custom\_loader.log2>&1**

* Log Rotation (daily):

**00\*\*\*/usr/sbin/logrotate/etc/logrotate.d/suricata**

* Report Generation (daily):

**08\*\*\*/opt/scripts/daily\_report.sh>>/var/log/suricata/report.log2>&1**

* IP Auto-Blocking (hourly):

**0\*\*\*\*/opt/scripts/auto\_block.sh>>/var/log/suricata/auto\_block.log2>&1**

# Final Deliverables:



* Live Suricata + Filebeat + ELK stack on host
* Custom detection rules
* Alert automation via email/Slack
* Threat dashboards & intelligence enrichment
* Scripts for auto-blocking, reporting, and maintenance
* MITRE ATT&CK aligned detection mapping
* Endpoint + Cloud visibility & response capability
* Professional documentation (can be shared on GitHub)
* Resume and GitHub-ready project portfolio

Let me know when you’re ready to start with Day 3, and I’ll generate custom rule templates or traffic simulation tools.