

Network Security and System Administration Essential

Mini-Capstone Project

Nguyen Duong

1. Monitoring and Design

Encryption and Segmentation:

All data transmitted between endpoints, mobile apps, and servers must use TLS 1.3 or higher. Data at rest on servers should be encrypted using AES-256. Segmentation of network traffic is critical, separate VLANs must be assigned to patient devices, IoT sensors, administrative workstations, and guest networks. This segmentation restricts lateral movement in case of compromise.

Access Control and Audit Trails:

Only authorized personnel should access protected health information (PHI). Implementing Role-Based Access Control (RBAC) ensures the principle of least privilege is followed. Each access to PHI should be logged and reviewed regularly to satisfy the audit control requirement of HIPAA.

Real-Time Monitoring and Alerts:

Integrate a Security Information and Event Management system to collect logs from firewalls, endpoint detection systems, and servers. Establish anomaly detection to identify suspicious patterns such as unusual traffic spikes or unauthorized access attempts.

Wireless Safeguards:

Wireless networks must use WPA3 encryption, disable WPS, and apply MAC filtering to limit device access. Captive portals should be used for guest access, and traffic should be entirely isolated from the primary LAN.

Incident Response and Backup:

HIPAA's contingency plan standard requires data backups and disaster recovery strategies. Regular, encrypted backups should be maintained offsite. An incident response team should be trained to identify, contain, and remediate breaches quickly.

With 1,200+ patients and over 2,000 sensor endpoints, MedSNet must continuously monitor all endpoints for compliance and security through layered controls that meet HIPAA standards.

2. Wired Monitoring

Given the expected scaling of MedSNet from 440 endpoints to possibly over 600 in the next 2 years, robust and scalable network monitoring is essential. Wired network monitoring in

healthcare settings must comply with HIPAA's technical safeguards, particularly around audit controls (§164.312(b)) and integrity (§164.312(c)(1)).

Selected Tools:

1. Nagios Core:

A highly customizable and lightweight monitoring tool ideal for wired infrastructure. It can monitor services like HTTP, SSH, disk usage, and ping responses. It supports email alerts and can be extended with plugins to meet specific needs, including uptime and performance monitoring for health-critical servers.

2. Zabbix:

While more resource-intensive, Zabbix offers comprehensive network monitoring, including bandwidth, device status, SNMP, and historical data analysis. It is web-interface based and requires backend components (e.g., MySQL, Apache), making it better suited for dedicated monitoring servers.

Installed Tool: Nagios Core on Kali Linux

Commands used:

- `sudo apt install nagios4 nagios-plugins-contrib nagios-nrpe-plugin`
- `sudo systemctl start nagios4`
- `sudo systemctl enable nagios4`
- `sudo systemctl status nagios4`

```
(nguyen@KaliLinux-DellLatitude7410)-[~]
$ sudo systemctl status nagios4
● nagios4.service - nagios4
   Loaded: loaded (/usr/lib/systemd/system/nagios4.service; enabled; preset: >
   Active: active (running) since Tue 2025-04-29 22:31:39 PDT; 12s ago
   Invocation: efe5da505c7f4fe9a1003c08fd24c3be
     Docs: man:nagios4
   Main PID: 36539 (nagios4)
     Tasks: 14 (limit: 18578)
   Memory: 4.7M (peak: 6.1M)
      CPU: 26ms
   CGroup: /system.slice/nagios4.service
           └─36539 /usr/sbin/nagios4 /etc/nagios4/nagios.cfg
              └─36542 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
                 └─36543 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
                    └─36544 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
                       └─36545 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
                          └─36546 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
                             └─36547 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
                                └─36548 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
                                   └─36549 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
                                      └─36550 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
                                         └─36551 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
                                            └─36552 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
                                               └─36553 /usr/sbin/nagios4 --worker /var/lib/nagios4/rw/nagios.qh
```

Figure 2.1: Nagios is enabled and running

Test Command:

- /usr/lib/nagios/plugins/check_ping -H 8.8.8.8 -w 100.0,20% -c 500.0,60%

```
(nguyen@KaliLinux-DellLatitude7410)-[~]
$ /usr/lib/nagios/plugins/check_ping -H 8.8.8.8 -w 100.0,20% -c 500.0,60%
PING OK - Packet loss = 0%, RTA = 19.72 ms|rta=19.716000ms;100.000000;500.000000;0.000000 pl=0%;20;60;0;
```

Figure 2.2: Test Monitoring command to check for connectivity

This command checks ICMP connectivity to Google's DNS and reports if latency or packet loss exceed thresholds.

3. Wireless Monitoring

Title: Wireless Network Monitoring and Intrusion Detection Using Kismet

Given the critical role of IoT and wireless patient devices at MedSNet, implementing robust wireless network monitoring is essential. Wireless traffic includes highly sensitive patient health data, and under HIPAA §164.312(e)(1), it must be monitored for unauthorized access and ensure encryption in transit.

Selected Tool: Kismet

Kismet is an open-source wireless network detector, sniffer, and intrusion detection system. It passively collects packets from wireless networks and is compatible with WPA/WPA2/WPA3 encrypted traffic (not for cracking, but for monitoring associations and unauthorized devices). Kismet works best on Kali Linux with a compatible wireless card that supports monitor mode.

Installation on Kali Linux:

- `sudo apt install kismet`

Launching the Tool:

- Kismet

```
(nguyen@KaliLinux-DellLatitude7410)-[~]
$ kismet
INFO: Including sub-config file: /etc/kismet/kismet_httpd.conf
INFO: Including sub-config file: /etc/kismet/kismet_memory.conf
INFO: Including sub-config file: /etc/kismet/kismet_alerts.conf
INFO: Including sub-config file: /etc/kismet/kismet_80211.conf
INFO: Including sub-config file: /etc/kismet/kismet_logging.conf
INFO: Including sub-config file: /etc/kismet/kismet_filter.conf
INFO: Including sub-config file: /etc/kismet/kismet_uav.conf
INFO: Loading config override file '/etc/kismet/kismet_package.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_package.conf
INFO: Loading config override file '/etc/kismet/kismet_site.conf'
INFO: Optional sub-config file not present: /etc/kismet/kismet_site.conf
INFO: Local config and cache directory '/home/nguyen/.kismet/' does not
      exist; creating it.
KISMET - Point your browser to http://localhost:2501 (or the address of this system) for the Kismet UI
```

Figure 3.1: Kismet will be launched at <http://localhost:2501/>

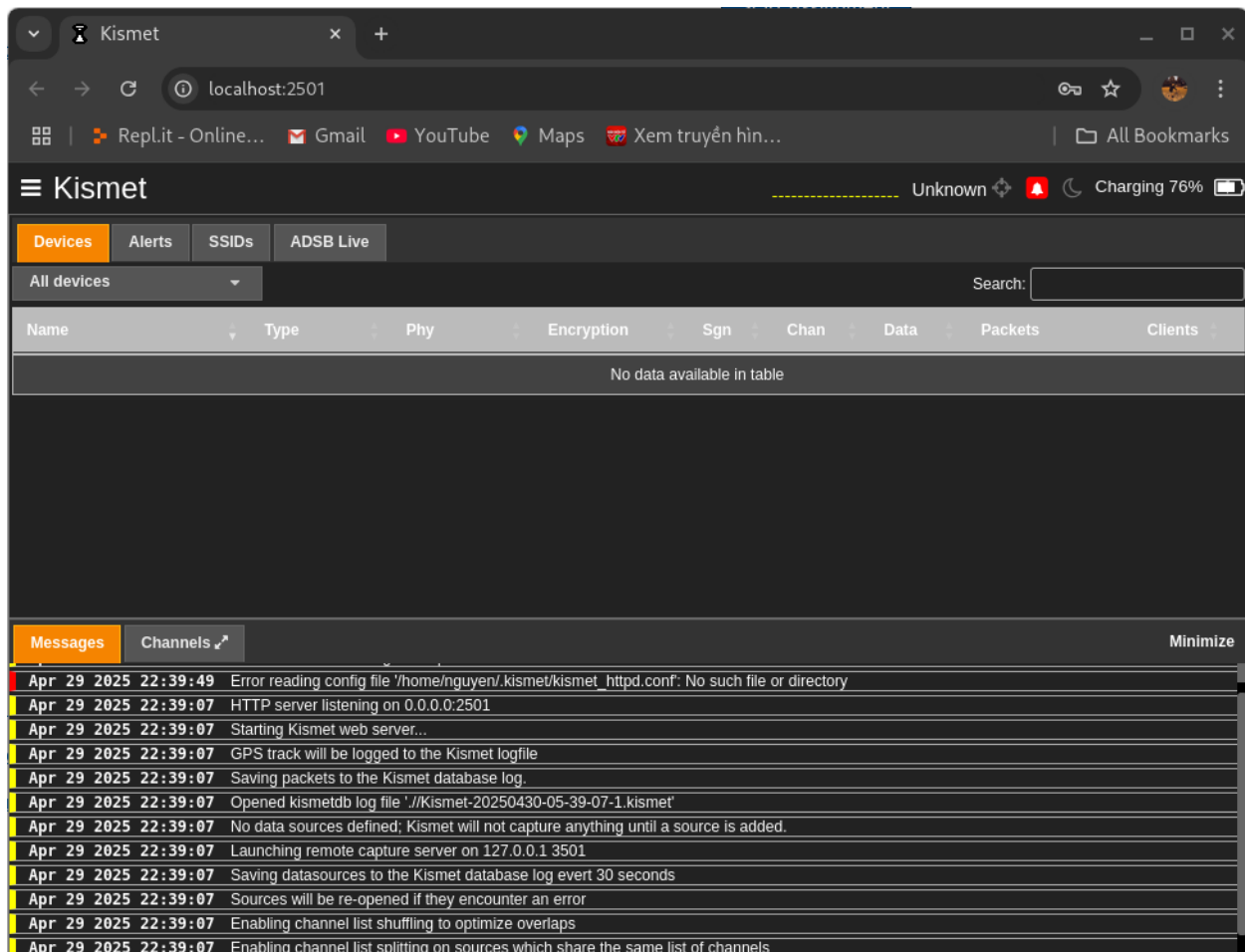


Figure 3.2: Kismet user interface

Kismet provides real-time visualization of wireless devices, SSIDs, access points, and client devices. It can alert on anomalies such as:

- Unusual beacon flooding.
- Unauthorized client association attempts
- Signal jamming or spoofing activities

4. Wired Firewall

To protect MedSNet's hybrid network of IoT sensors, patient workstations, and hospital servers, a HIPAA-compliant firewall must be deployed. Under the HIPAA Security Rule, organizations must protect against malicious software and unauthorized access through technical safeguards such as firewalls.

Selected Open-Source Firewalls:

1. pfSense

- Based on FreeBSD and widely used in healthcare networks.

- Offers deep packet inspection, stateful filtering, DNS-based blocking, and traffic shaping.
- HIPAA-aligned logging, VPN support, and blacklists via Snort or Suricata integration.

2. OPNsense

- Forked from pfSense, offering a more modern UI and integrated reporting dashboard.
- Provides firewall rules, Intrusion Prevention, DHCP server, and Netflow analytics.

3. IPFire

- Lightweight Linux-based firewall system that supports QoS, Intrusion Detection, and easy backup/restore.
- Suitable for small to mid-sized deployments, like branch clinics.

Firewall Rules to Blacklist Bots and Detect Anomalous Traffic:

Using pfSense or OPNsense, we can create sample rules:

Bot Blacklisting Rule:

- Action: Block
- Source: Known Malicious IPs
- Destination: Any
- Description: Block known bad bots

Traffic Volume Anomaly Rule:

- Action: Pass
- Interface: LAN
- Source: Any
- Destination: Any
- Advanced Options:
Max new connections per second: 20
Max connections per host: 100
- Description: Prevent DoS attack by limiting connection bursts

Geo-blocking Rule:

- Action: Block
- Source: GeoIP (block traffic from countries outside the U.S.)
- Destination: Any
- Description: Restrict international bot activity

Port-Based Blocking:

- Action: Block
- Port: 135, 137-139, 445 (SMB), 23 (Telnet)

- Description: Block legacy and vulnerable services
- These firewall measures help MedSNet prevent reconnaissance, malware propagation, and denial-of-service (DoS) attempts while supporting HIPAA's requirements for proactive threat mitigation and access control.

5. Wired IDPS

In alignment with HIPAA's Security Rule, healthcare providers must implement measures to detect and mitigate unauthorized access and anomalous activities. Suricata, an open-source, high-performance IDPS, supports real-time intrusion detection, traffic analysis, and rule-based packet inspection making it ideal for MedSNet's infrastructure.

Suricata Installation on Kali Linux

- `sudo apt update`
- `sudo apt install suricata`

Check installation:

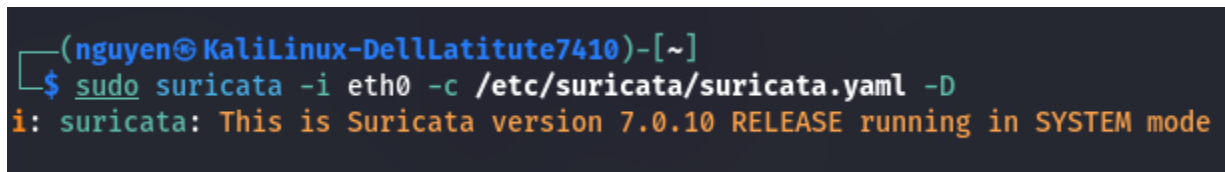
- `suricata --build-info`

Identify network interface:

- `ip addr`

Run Suricata live:

- `sudo suricata -i eth0 -c /etc/suricata/suricata.yaml -D`



```
(nguyen@KaliLinux-DellLatitude7410)-[~]
$ sudo suricata -i eth0 -c /etc/suricata/suricata.yaml -D
i: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
```

Figure 5.1: Suricata is capturing and analyzing packets in real time using configuration file.

```
(nguyen@KaliLinux-DellLatitude7410)-[~]
$ sudo tail -f /var/log/suricata/eve.json
{"timestamp":"2025-04-29T23:23:39.766926-0700","flow_id":1042125701188510,"in_iface":"eth0","event_type":"75.75.75.75","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"version":2,"type":"query","x_id":0,"opcode":0}}
{"timestamp":"2025-04-29T23:23:39.785145-0700","flow_id":1042014099597707,"in_iface":"eth0","event_type":"75.75.75.75","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"version":2,"type":"answer","opcode":0,"rrname":"doh.xfinity.com","rrtype":"A","rcode":"NOERROR","answers":[{"rrname":"doh.xfinity.com"}, {"rrname":"doh2.gslb2.xfinity.com","rrtype":"A","ttl":26,"rdata":"75.75.77.116"}],"grouped":[]}}
{"timestamp":"2025-04-29T23:23:39.786046-0700","flow_id":1041681459701080,"in_iface":"eth0","event_type":"75.75.75.75","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"version":2,"type":"answer","opcode":0,"rrname":"doh.xfinity.com","rrtype":"AAAA","rcode":"NOERROR","answers":[{"rrname":"doh.xfinity.com"}, {"rrname":"doh2.gslb2.xfinity.com","rrtype":"AAAA","ttl":22,"rdata":"2001:0558:feed:0443:0000:0000:0000:0115"}],"CNAME":["doh2.gslb2.xfinity.com"]}}
{"timestamp":"2025-04-29T23:23:39.787995-0700","flow_id":1042125701188510,"in_iface":"eth0","event_type":"75.75.75.75","dest_port":53,"proto":"UDP","pkt_src":"wire/pcap","dns":{"version":2,"type":"answer","opcode":0,"rrname":"doh.xfinity.com","rrtype":"HTTPS","rcode":"NOERROR","answers":[{"rrname":"doh.xfinity.com"}],"grouped":{"CNAME":["doh2.gslb2.xfinity.com"]},"authorities":[{"rrname":"gslb2.xfinity.com","rdata":"rthlake.il.ndcchgo.comcast.net","rname":"hostmaster.gtd02-d.northlake.il.ndcchgo.comcast.net","serial":1,"minimum":60}]}}
```

Figure 5.2: View JSON logs

Rule Configuration

Edit the Suricata rule file:

- `sudo nano /etc/suricata/rules/local.rules`

Detection Rules (alerts only):

1. Detect ICMP Ping (e.g., reconnaissance):

- `alert icmp any any -> any any (msg:"ICMP Ping Detected"; sid:100001; rev:1;)`

2. Detect Unencrypted Telnet traffic:

- `alert tcp any any -> any 23 (msg:"Telnet Traffic Detected - Unsecure Protocol"; sid:100002; rev:1;)`

Blocking Rules (inline mode):

1. Drop SMB traffic on port 445:

- `drop tcp any any -> any 445 (msg:"Block SMB (WannaCry/Ransomware Prevention)"; sid:100003; rev:1;)`

2. Drop FTP traffic on port 21:

- `drop tcp any any -> any 21 (msg:"Block FTP - Legacy Protocol"; sid:100004; rev:1;)`

Reload Suricata to activate rules:

- `sudo suricata -r /path/to/your.pcap -S /etc/suricata/rules/local.rules`

Or for live mode:

- `sudo systemctl restart suricata`

Advantage of Using Suricata:

- Real-time packet-level visibility over wired traffic.
- Easy integration with ELK stack or SIEMs for correlation and alerting.
- HIPAA-aligned with capabilities for log auditing, alerting, and risk mitigation.
- Block legacy, unencrypted, or vulnerable protocols that might expose PHI.

6. References

1. Open Information Security Foundation. (n.d.). Suricata documentation. Suricata.io. Retrieved April 29, 2025, from <https://suricata.io>
2. PfSense. (n.d.). pfSense documentation. Netgate. Retrieved April 29, 2025, from <https://docs.netgate.com/pfsense/en/latest/>
3. The Kismet Project. (n.d.). Kismet wireless network detector, sniffer, and IDS. Retrieved April 29, 2025, from <https://www.kismetwireless.net>
4. U.S. Department of Health and Human Services. (2013). Summary of the HIPAA security rule. HHS.gov. Retrieved April 29, 2025, from <https://www.hhs.gov/hipaa/for-professionals/security/index.html>
5. Zabbix LLC. (n.d.). Zabbix documentation 6.0. Retrieved April 29, 2025, from <https://www.zabbix.com/documentation>
6. Nagios Enterprises. (n.d.). Nagios Core documentation. Retrieved April 29, 2025, from <https://www.nagios.org/documentation/>
7. Acrylic WiFi. (n.d.). Acrylic WiFi Professional. Retrieved April 29, 2025, from <https://www.acrylicwifi.com/en/wlan-software/wifi-analyzer-acrylic-professional/>