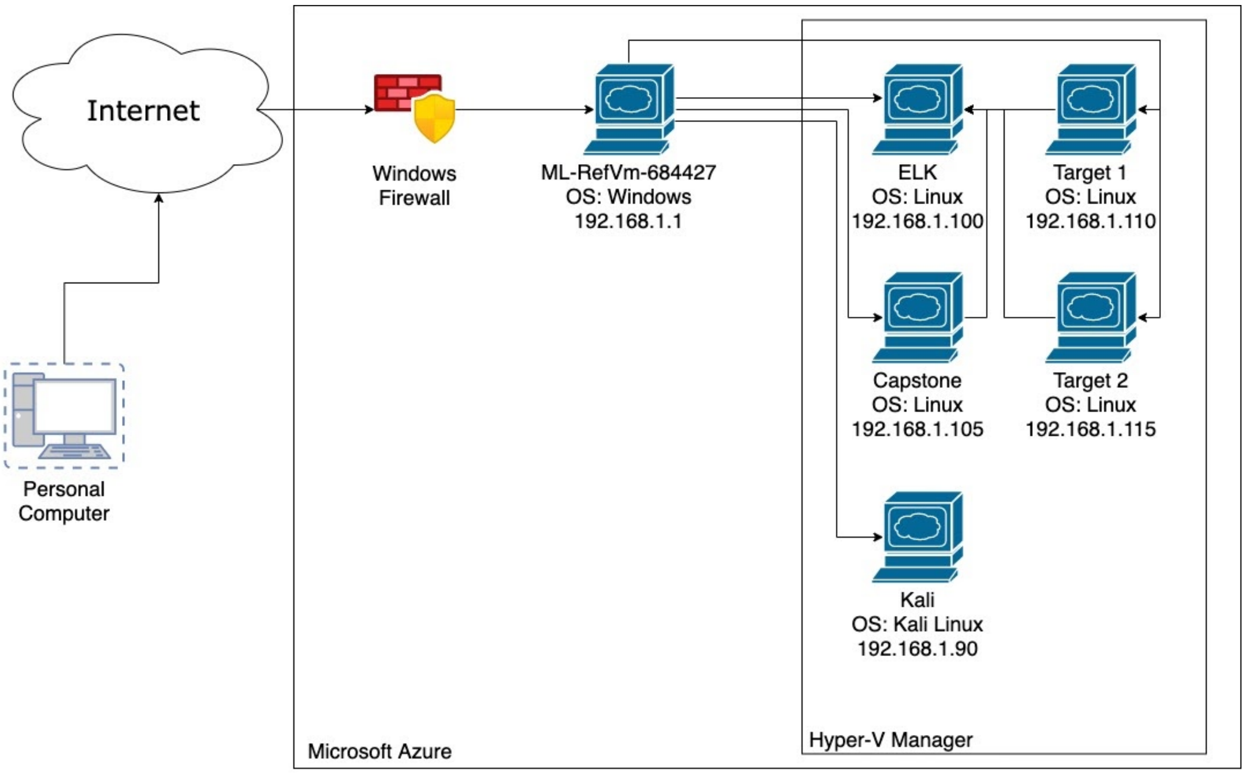
Blue Team: Summary of Operations

Table of Contents

- Network Topology
- Description of Targets
- Monitoring the Targets
- Patterns of Traffic & Behavior
- Suggestions for Going Further

Network Topology



The following machines were identified on the network:

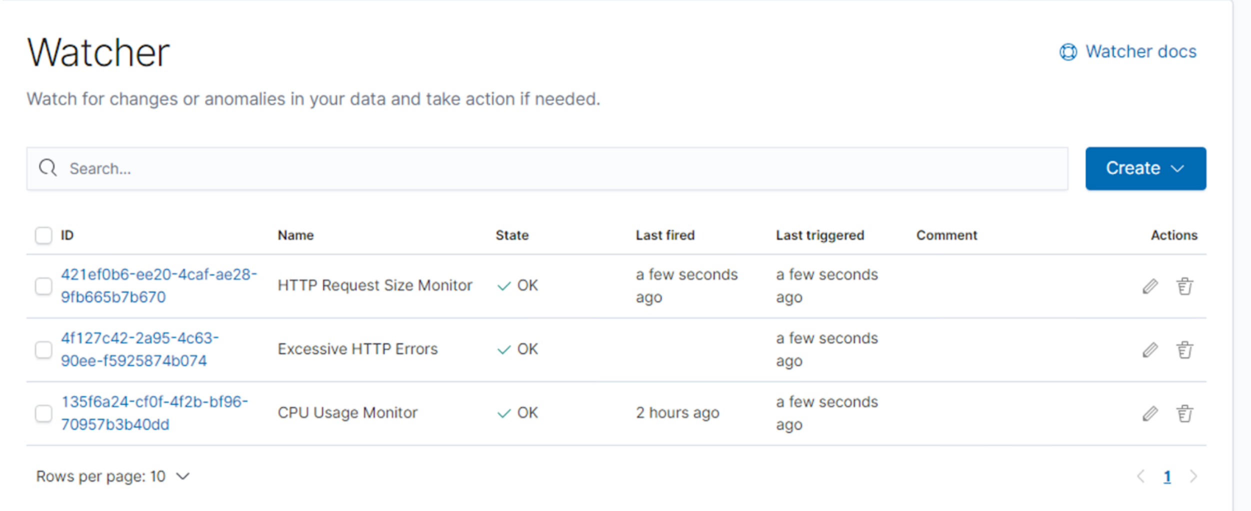
- ML-RdfVm-684427
  - **Operating System**: Windows
  - **Purpose**: Virtual Machine Host
  - **IP Address**: 192.168.1.1

- ELK
    - **Operating System**: Linux
    - **Purpose**: Kibana Server
    - **IP Address**: 192.168.1.100
- Capstone
    - **Operating System**: Linux
    - **Purpose**: Tests ELK alerts
    - **IP Address**: 192.168.1.105
- Kali
    - **Operating System**: Kali Linux
    - **Purpose**: Attack Machine
    - **IP Address**: 192.168.1.90
- Target 1 (Raven 1)
    - **Operating System**: Linux
    - **Purpose**: Web Server (Target 1 Machine)
    - **IP Address**: 192.168.1.110
- Target 2 (Raven 2)
    - **Operating System**: Linux
    - **Purpose**: Web Server (Target 2 Machine)
    - **IP Address**: 192.168.1.115

Description of Targets

The target of this attack was: Target 1 (192.168.1.110)

Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:



Watch for changes or anomalies in your data and take action if needed.

ID	Name	State	Last fired	Last triggered	Comment	Actions
421ef0b6-ee20-4caf-ae28-9fb665b7b670	HTTP Request Size Monitor	✓ OK	a few seconds ago	a few seconds ago		
4f127c42-2a95-4c63-90ee-f5925874b074	Excessive HTTP Errors	✓ OK		a few seconds ago		
135f6a24-cf0f-4f2b-bf96-70957b3b40dd	CPU Usage Monitor	✓ OK	2 hours ago	a few seconds ago		

Rows per page: 10

Monitoring the Targets

Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:

HTTP Request Size Monitor

Alert is implemented as follows:

- **Metric**: HTTP request bytes of all documents
- **Threshold**: Over 3500 requested bytes within a 1 minute timeframe
- **Vulnerability Mitigated**: Denial of Service Attacks
- **Reliability**: Medium Reliability

Excessive HTTP Errors

Alert is implemented as follows:

- **Metric**: HTTP errors
- **Threshold**: Over 400 during a 5 minute timespan
- **Vulnerability Mitigated**: Brute Force Attack
- **Reliability**: High Reliability

CPU Usage Monitor

Alert is implemented as follows:

- **Metric**: System Processor CPU usage
- **Threshold**: When usage is above 0.5 during a 5 minute timespan
- **Vulnerability Mitigated**: Malware Infection
- **Reliability**: Medium Reliability

Suggestions for Going Further

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

- Denial of Service Attack:
  - Patches
    - Install Load Balancer to help reduce stress on individual server
      - Balancing network traffic greatly reduces success of DoS Attacks
    - Implement an IP blocklist to block malicious IPs when attack occurs
      - Prevents attackers from continuing attack against the network.

- Brute Force Attack:
    - Patches
        - Implement an IP blocklist after numerous ‘failed logins’
            - Prevents attackers from continuing attack against the network.
        - Implement Multi-Factor Authentication
            - Ensures users have multiple factors of authentication prior to accessing the network
        - Use a Captcha on Login screen
            - Prevents Automated Attempts to login

- Malware:
    - Patches
        - Install Anti-Virus / Anti-Malware software
            - Protects system from malicious software
        - Educate Employees
            - Ensures employees know dangers of unauthorized applications
        - Regularly Update Systems, Software, and Applications
            - Helps harden the network