Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

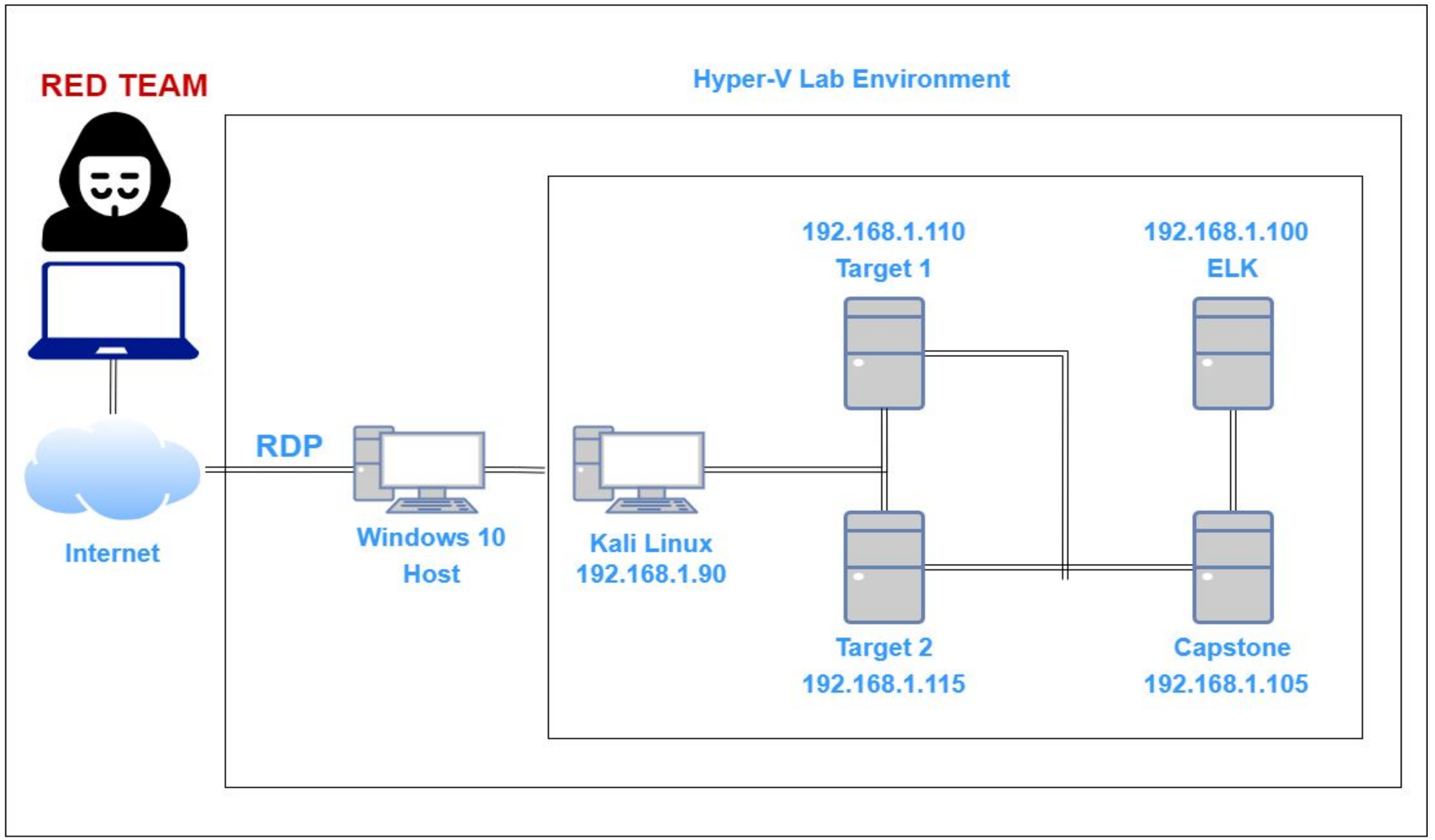
Alerts Implemented

Hardening

Implementing Patches

Network Topology & Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.1/24
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: kali

IPv4: 192.168.1.110
OS: Linux
Hostname: Target1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target2

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

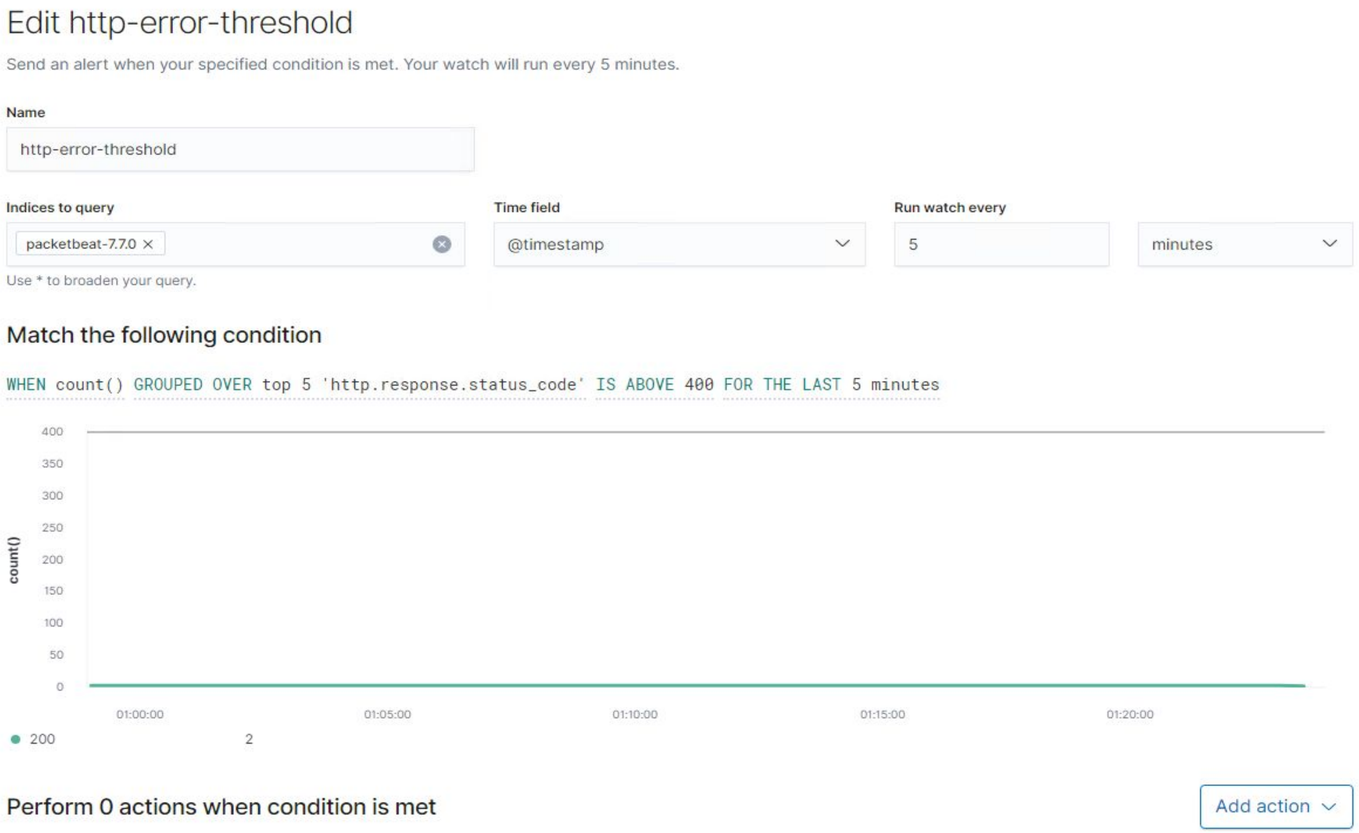
Vulnerability	Description	Impact
Wordpress Core not updated	Security Patches needed	High
AntiMalware/AV	Install needed	High
No Firewall Rules	WAF needed	High

Alerts Implemented

Alert 1: HTTP Error Threshold

Condition: WHEN count() GROUPED OVER top 5 ‘http.response.status_code IS ABOVE 400

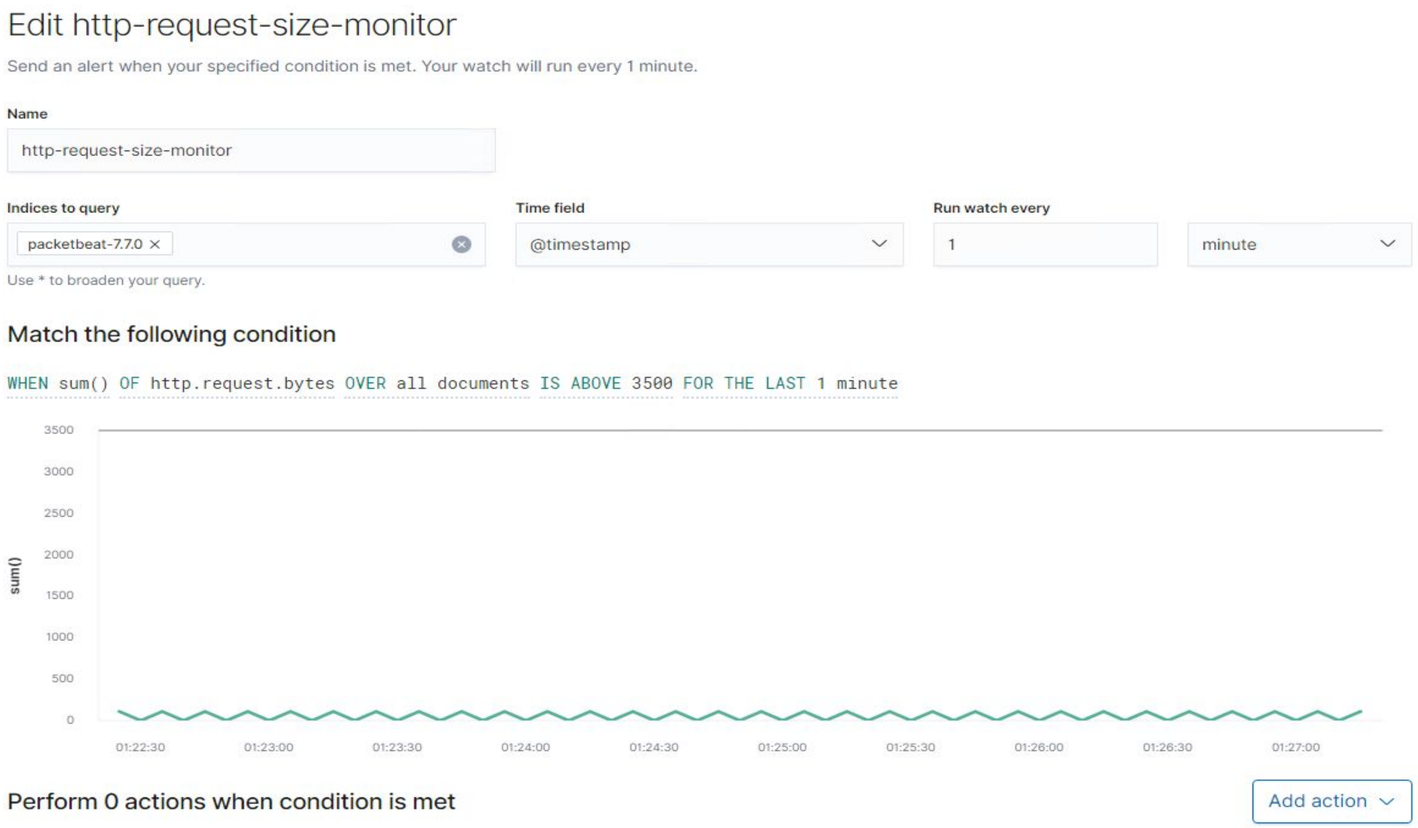
Vulnerability Detected: This is alert is used to measure http error codes 400 and above. This will help in detecting attacks like Enumeration and Brute Force Attacks.



Alert 2: CPU Usage Monitor

Condition: WHEN max() of system.process.cpu.total.pct OVER all documents IS ABOVE 0.5

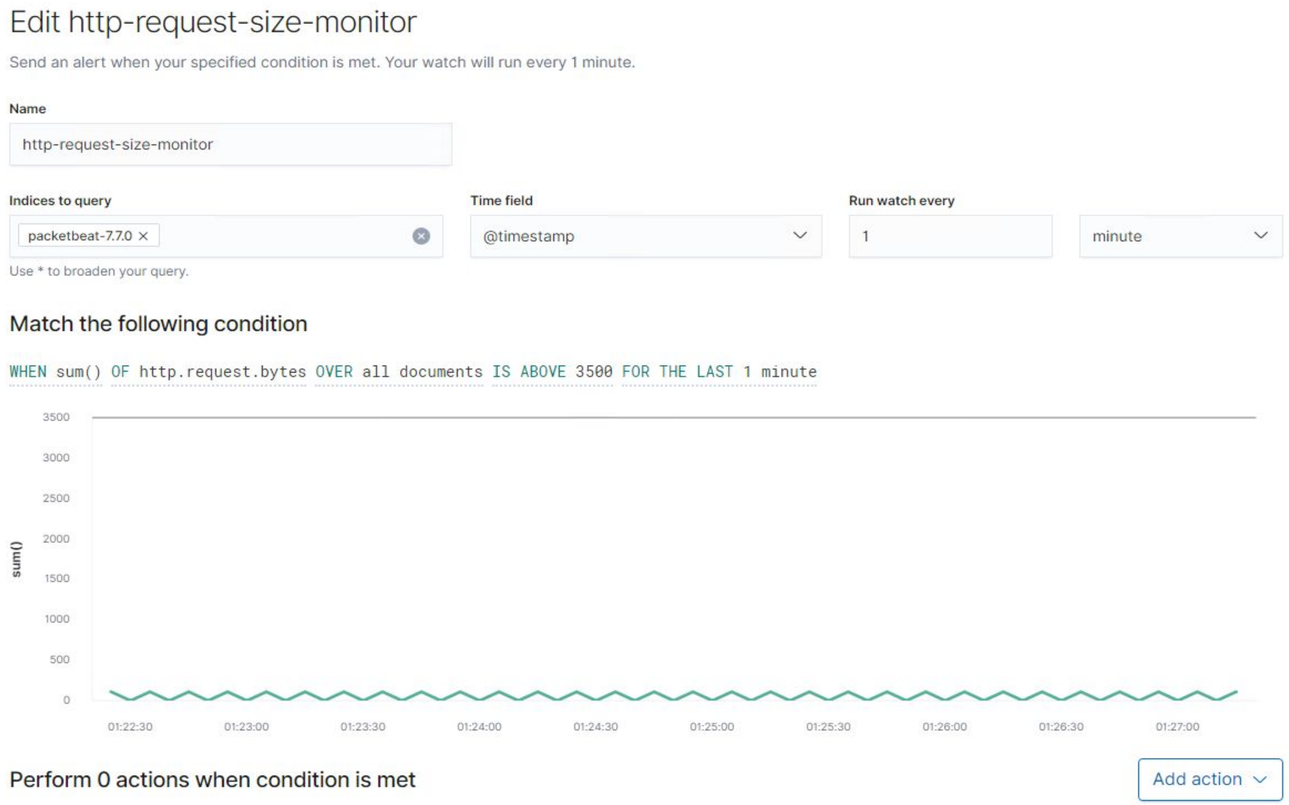
Vulnerability Detected: This is alert is used to measure cpu usage and can aid in detecting malware, spyware and keyloggers maliciously installed.



Alert 3: HTTP Request Size Monitor

Condition: WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 3500

Vulnerability Detected: This alert will help detect attacks such as DDoS and Code injections like CRLF and XSS.



Hardening

Hardening Against Wordpress Attacks on Target 1

Vulnerable Version of Wordpress

Patch: Wordpress Core updates and hardening

Why It Works: By installing latest Wordpress updates, it can fix security issues and known vulnerabilities. Also Wordpress can be hardened by using tools like Wordfence and disabling unused features and plugins. Additionally, if REST API is enabled, but not needed, WPScan takes advantage of this and is used to enumerate Wordpress. Disabling this feature can reduce this vulnerability.

Hardening Against Malware/Virus on Target 1

No Antivirus/Anti Malware Installed

Patch: Antivirus/Antimalware software Installation

Why It Works: High CPU usage is usually a good indicator that the device has been infected with malware or a keylogger virus/software. Having a good AV product installed on the host device can help mitigate this type of attack.

Hardening Against Malicious Web Traffic on Target 1

No Traffic Filtering

Patch: Deploy a WAF (Web Application Firewall)

Why It Works: WAFs are good at detecting, blocking and sanitizing HTTP traffic. Security rules can be configured to filter out specific traffic patterns that are consistent with attacks such as SQL-Injections, XSS, and DDoS.