Final Engagement

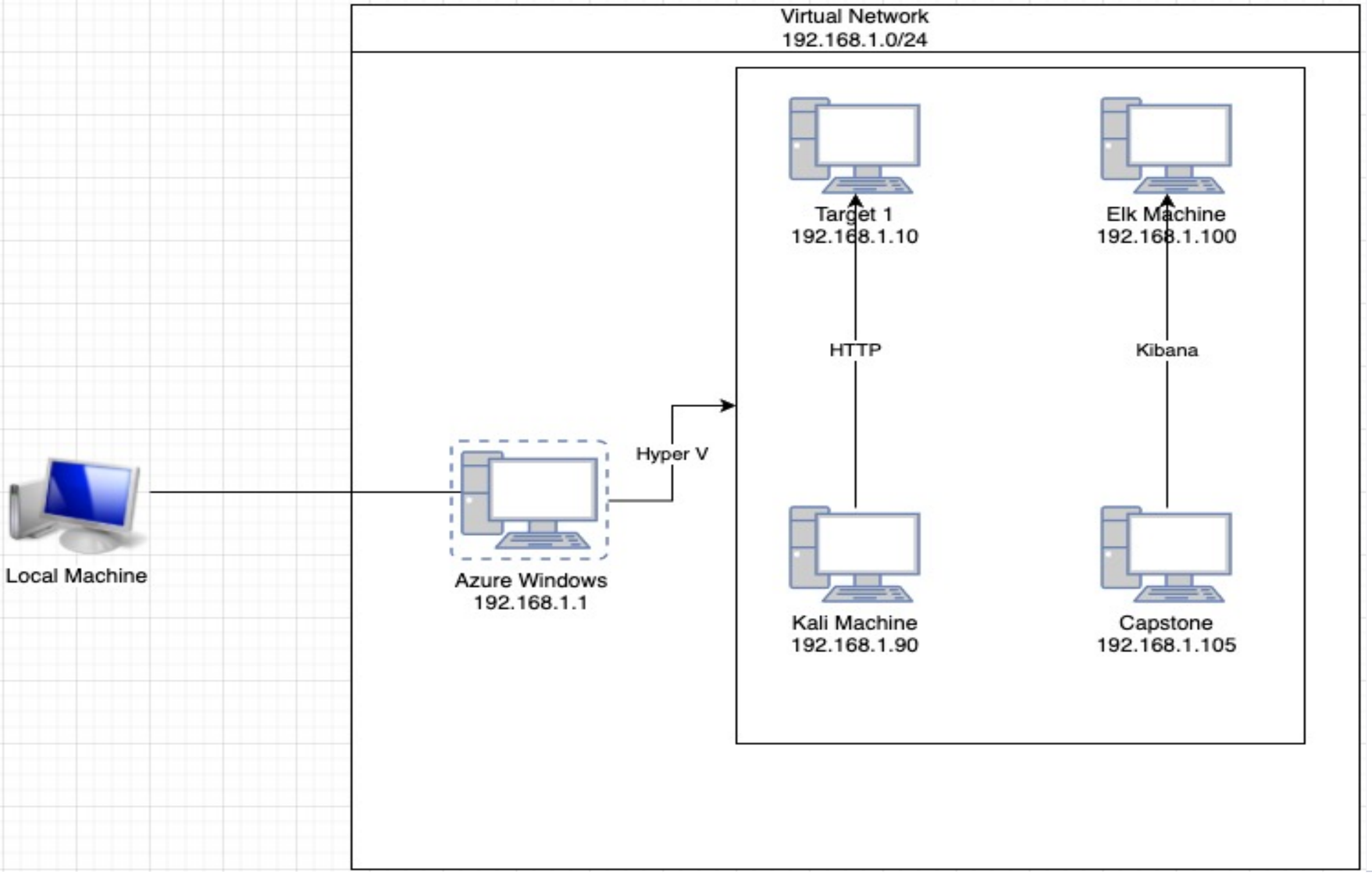
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: ML-RefV-68 4427

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.110
OS: Ubuntu
Hostname: Target 1

IPv4: 192.168.105
OS: Ubuntu
Hostname: Capstone

Critical Vulnerabilities: Target 1

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

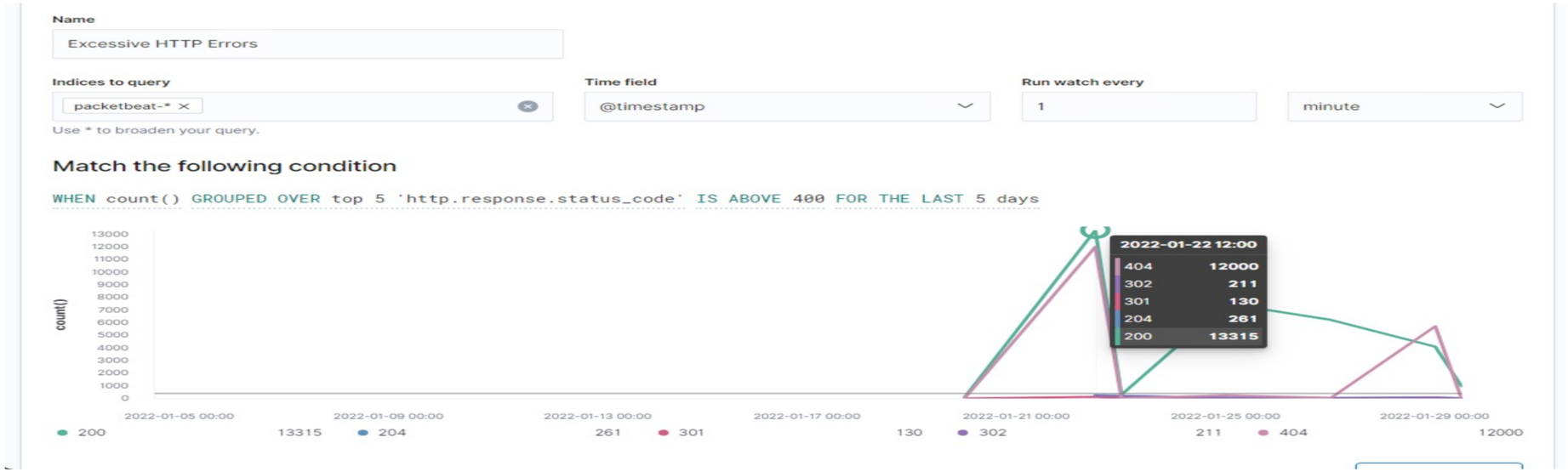
Vulnerability	Description	Impact
Network Mapping	*Nmap is used to find open ports available for exploit*	*Attackers can see which ports are open and attack targe machines*
Weak Passwords	*Basic passwords that a simple to crack and don't require any additional programs (Michael/Michael)*	*Were easily able to access Michael's machine because of the weak password*
WordPress Enumeration	*Wpscan seaches for user hashes within wordpress*	*Identified users on wp by exploiting this vulnerability*

Alerts Implemented

Excessive HTTP Errors

Summarize the following:

- Which **metric** does this alert monitor?
  - *Excessive HTTP Errors*
- What is the **threshold** it fires at?
  - *Will trigger after 400 or more responses in 5 minutes (the below screenshot is when the actual attack took place. Notice the spike on the 1/22/22).*



CPU Usage Monitor

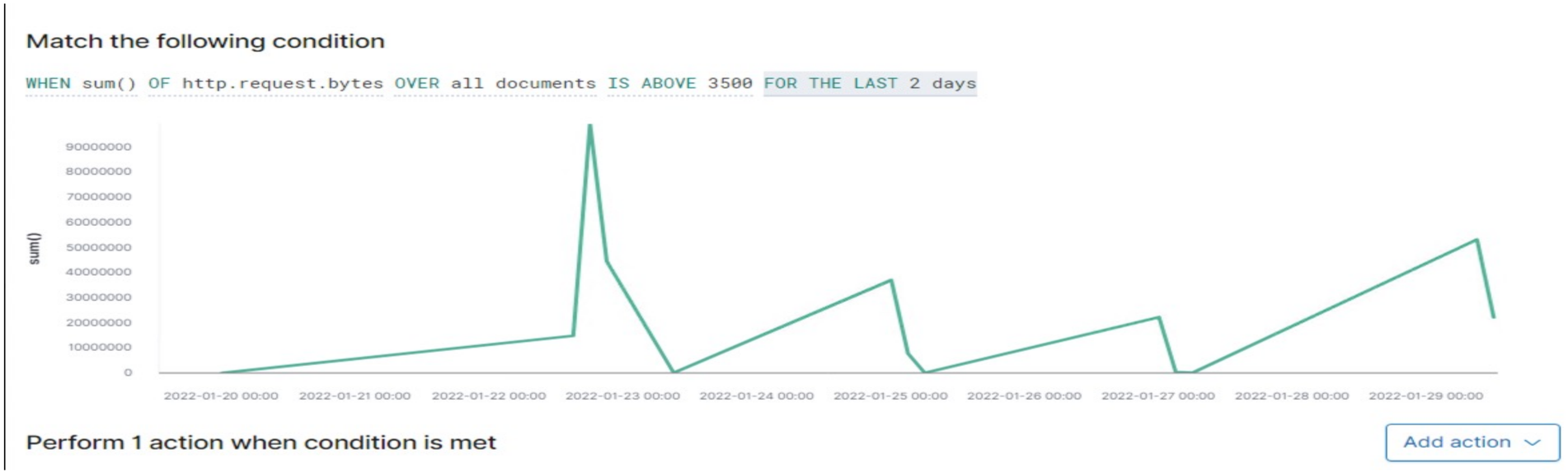
Summarize the following:

- Which **metric** does this alert monitor?
  - *CPU Usage*
- What is the **threshold** it fires at?
  - *Alert will trigger when CPU is above 0.5 in the last 5 minutes (example is from when the attack actually took place).*

HTTP Request Size Monitor

Summarize the following:

- Which **metric** does this alert monitor?
  - *HTTP Request size*
- What is the **threshold** it fires at?
  - *Will trigger from requests of 3500 bytes per minute. (screenshot is from when the attack took place).*



Hardening

Hardening Against NMAP on Target 1

Explain how to patch Target 1 against Vulnerability 1. Include:

- *Port 22 (SSH) was open to the public leaving it a vulnerability for an attacker to gain access to private data*
  - *One way to harden an open port in Linux is with IP Whitelisting*
    - *Escalate root privleges*
    - *Run the ‘iptables –A INPUT –s 192.168.1.1 –j ACCEPT’*
    - *Then save the iptables by running “service iptables save”*

Hardening Against Weak Passwords on Target 1

Strengthening a weak password makes the system way less vulnerable to attacks. It's also probably one of the most simple hardening methods there is. The following are techniques or actions one can take.

Creating a stronger password

- *Minimum 10 characters in length*
- *At least on number*
- *At least one uppercase*
- *Eliminating passwords that might be the same as your name or something you enjoy, birthday, ect…*

Hardening Against Wordpress Enumeration

Installing this plugin will not allow access to one's personal data if the wpscan –url ip/wordpress --enumerate command is ran.

Setup a Wordpress security plugin

- *There is a free WP Plugin that can be used for hardening and will stop WP enumeration. It's also free*
  - *Plugin can be found on https://wordpress.org/plugins/wp-security-hardening/*
  - *Install and activate plugin*
  - *Go to "Security Fixers" tab*
  - *Toggle to "Stop user enumeration"*