Final Engagement

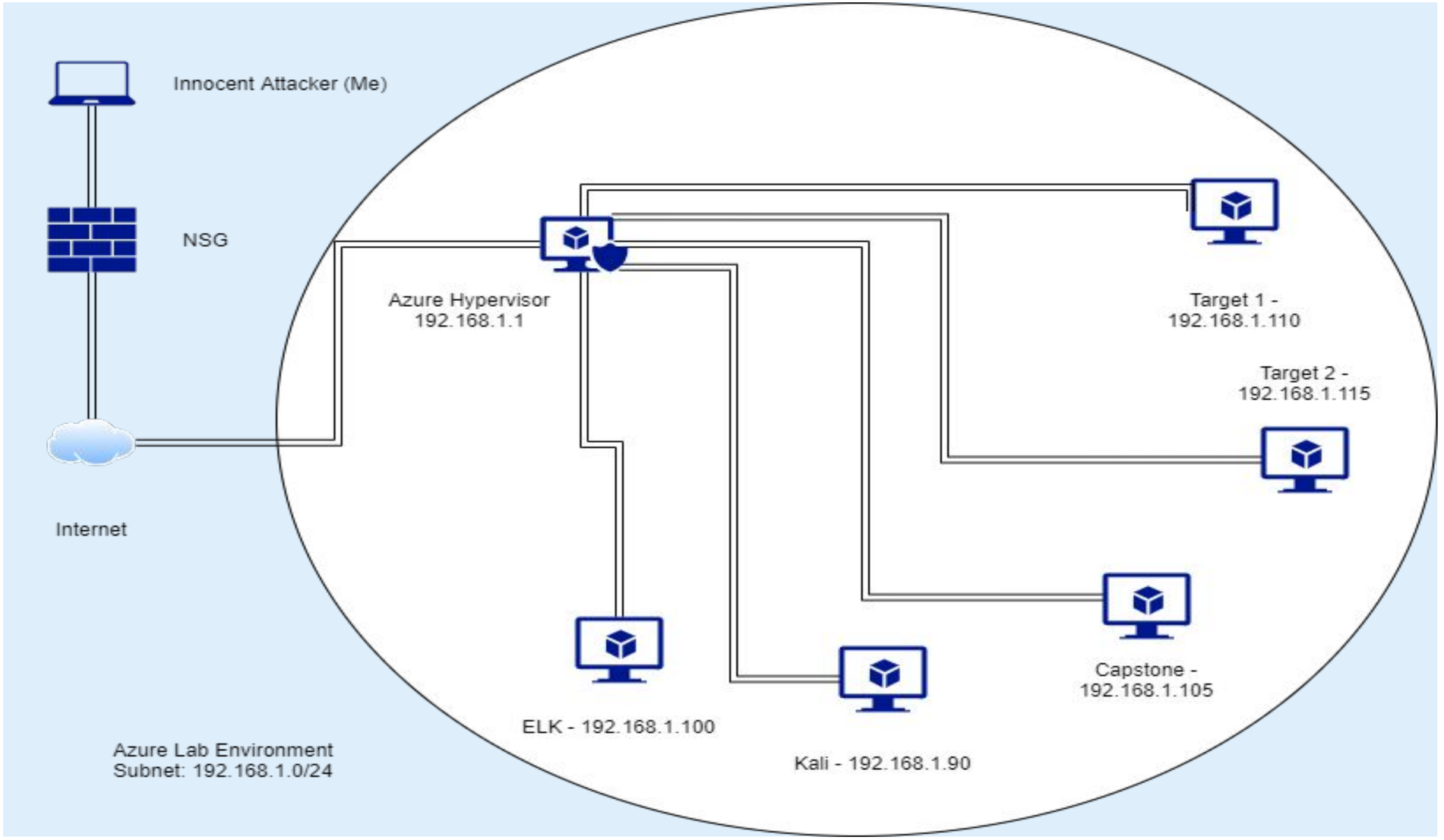
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 1
Gateway: 255

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.110
OS: Linux
Hostname: Target 1

IPv4: 192.168.1.115
OS: Linux
Hostname: Target 2

Critical Vulnerabilities: Target 1

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

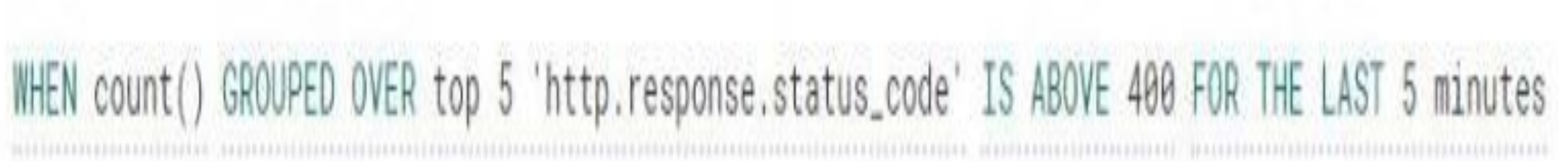
Vulnerability	Description	Impact
SSH open	Remote access to box via ssh	Brute force was possible
WordPress web server	WPScan Enumeration	Ability to find usernames without issue
MySQL root password	password in clear text	Allowed hashes to be found easily
Weak SU Permissions	python allowed SU access	Privilege escalation to root was possible

Alerts Implemented

[Excessive HTTP Errors]

Summarize the following:

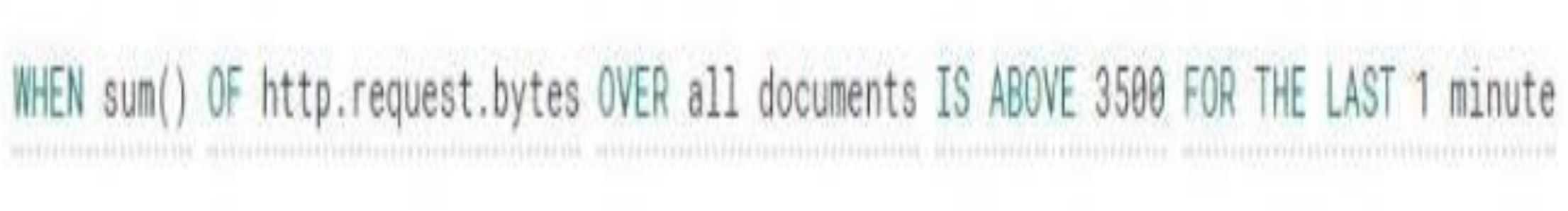
- Which **metric** does this alert monitor? By count
- What is the **threshold** it fires at? 400 + within 5 minutes from top 5 HTTP response status codes
- Provide a screenshot of the alert in action.



[HTTP Request Size Monitor]

Summarize the following:

- Which **metric** does this alert monitor? By sum
- What is the **threshold** it fires at? HTTP request bytes over all documents is over 3500 within 1 minute
- Provide a screenshot of the alert in action.



[CPU Usage Monitor]

Summarize the following:

- Which **metric** does this alert monitor? By max
- What is the **threshold** it fires at? CPU total utilization over all documents is about 50 percent for 5 minutes
- Provide a screenshot of the alert in action.

Hardening

Hardening Against [SSH password usage] on Target 1

Explain how to patch Target 1 against Vulnerability 1

- SSH using simple passwords is never a smart idea. Instead it is better to use SSH key pair:
  - There would no longer be an ability to brute force password access
  - Requires using the “ssh-keygen” command followed by “ssh-copy-id” to copy the key
  - Disable password login for root account

Hardening Against [HTTP] on Target 1

Explain how to patch Target 1 against Vulnerability 2. Include:

- Remove server version banner and directory browser listing:
  - This does not remove a vulnerability; this is to make enumeration and vulnerability identification more difficult
  - Banner removal: edit /etc/apache2/httpd.conf
  - ServerTokens > Prod
  - ServerSignature > Off
  - Disable browser listing: edit /etc/httpd/conf/httpd.conf
  - Options Indexes FollowSymLinks > remove “Indexes”

Hardening Against [Python SU permission] on Target 1

Explain how to patch Target 1 against Vulnerability 3

- Python SU permission is critical to taking root of target therefore critical to harden against.
  - If Steven needs SU privilege to Python then we must still remove this ability via sudoers file as it is configured to allow SU commands without SU password
  - sudo visudo > remove NOPASSWD setting replace with standard user settings