Final Engagement

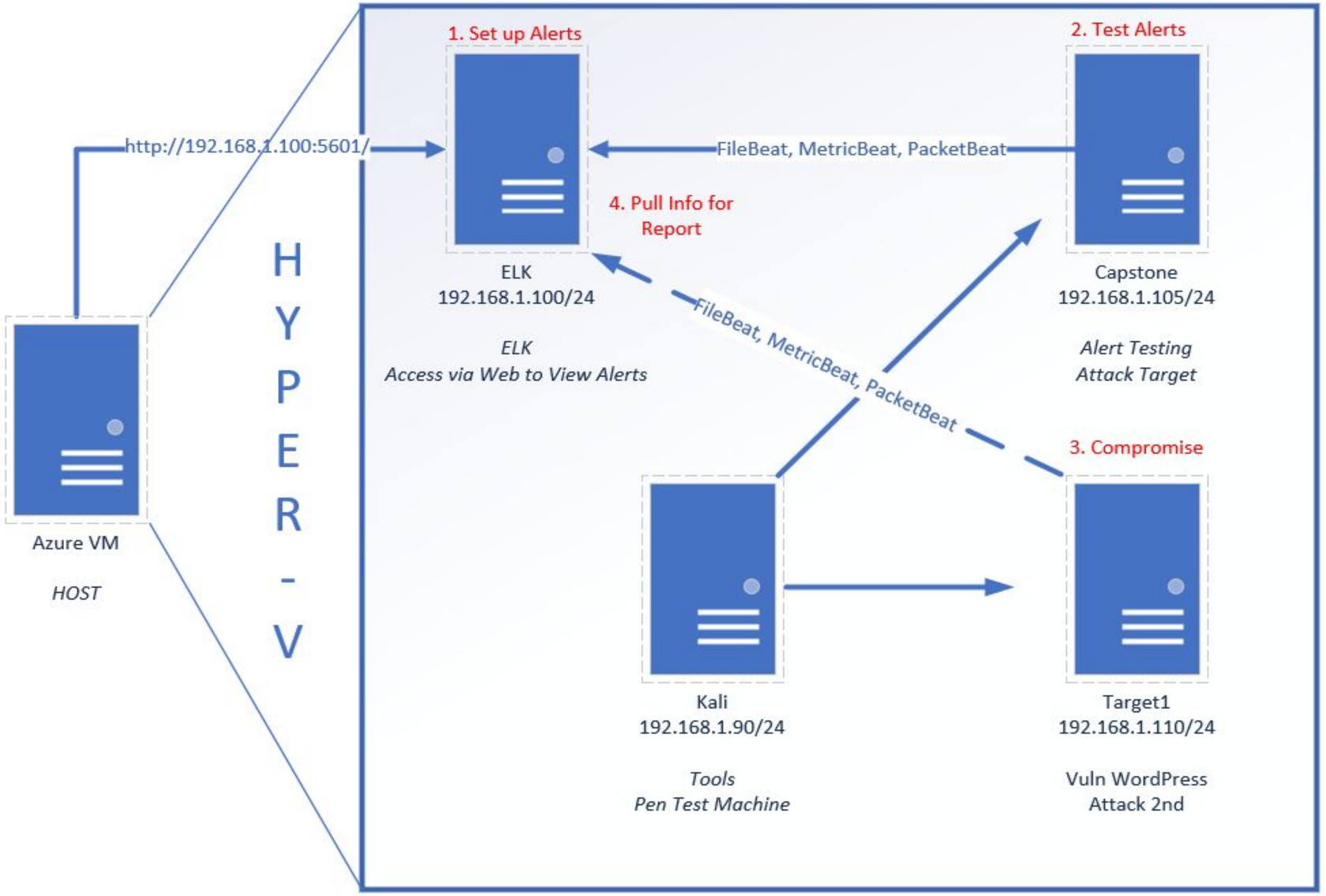
Attack, Defense & Analysis of a Vulnerable Network

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
IPv4:192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.110
OS: Linux
Hostname: Target1

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

Critical Vulnerabilities: Target 1

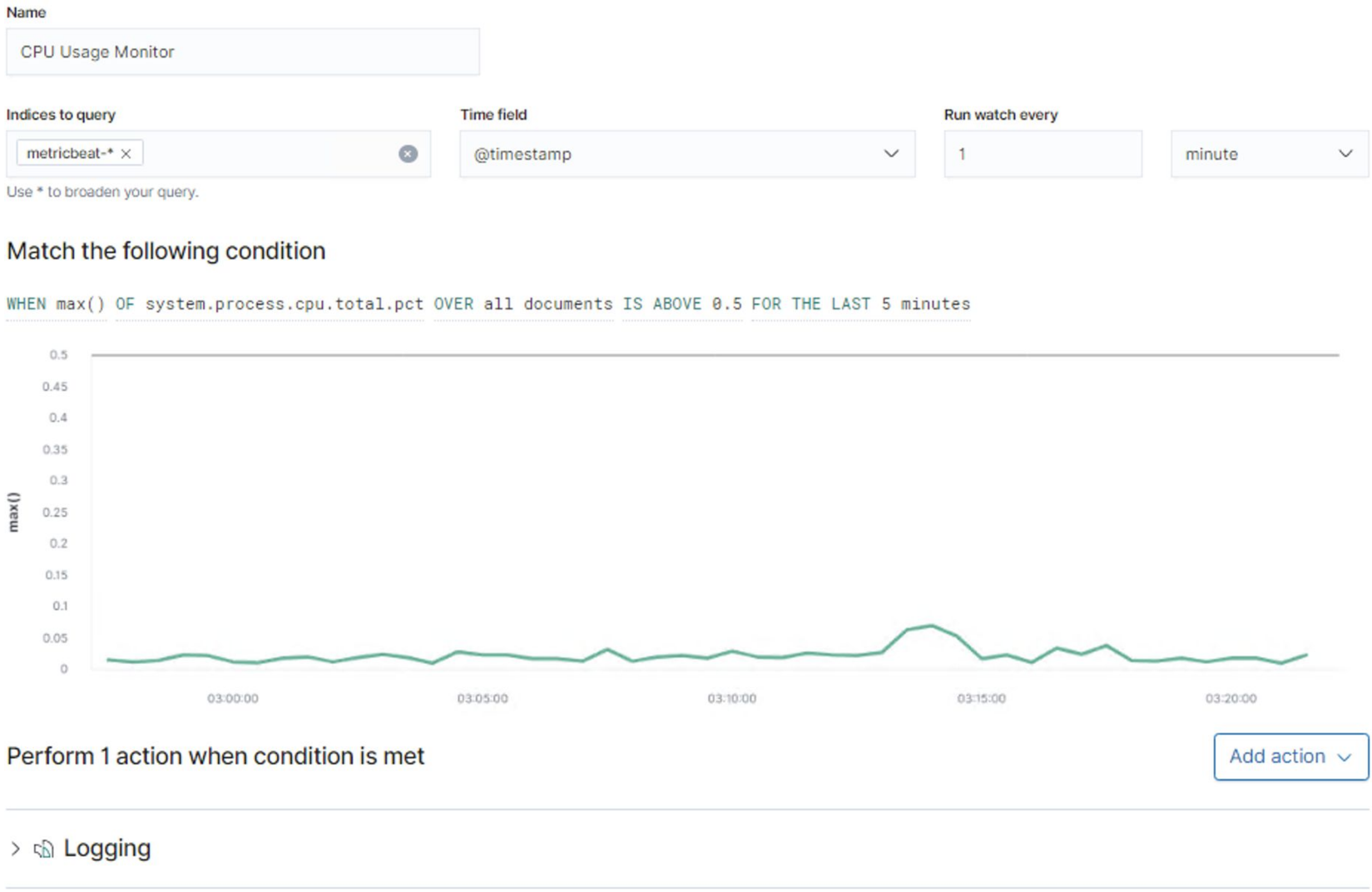
Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
A05:2021 – Security Misconfiguration	Ports 22, 80, 111, 139, 445 were open and unfiltered	Allowed full service scan and later SSH access
A07:2021 – Identification and Authentication Failures	User had a simple guessable password	Gained SSH access
Password Plaintext Storage	MySQL database password and login were stored in plaintext file with no access controls	Gained access to database with website content and password hashes
A01:2021 – Broken Access Control	User had sudo privileges to run python	Gained unlimited root access from unauthorized user account

Alerts Implemented

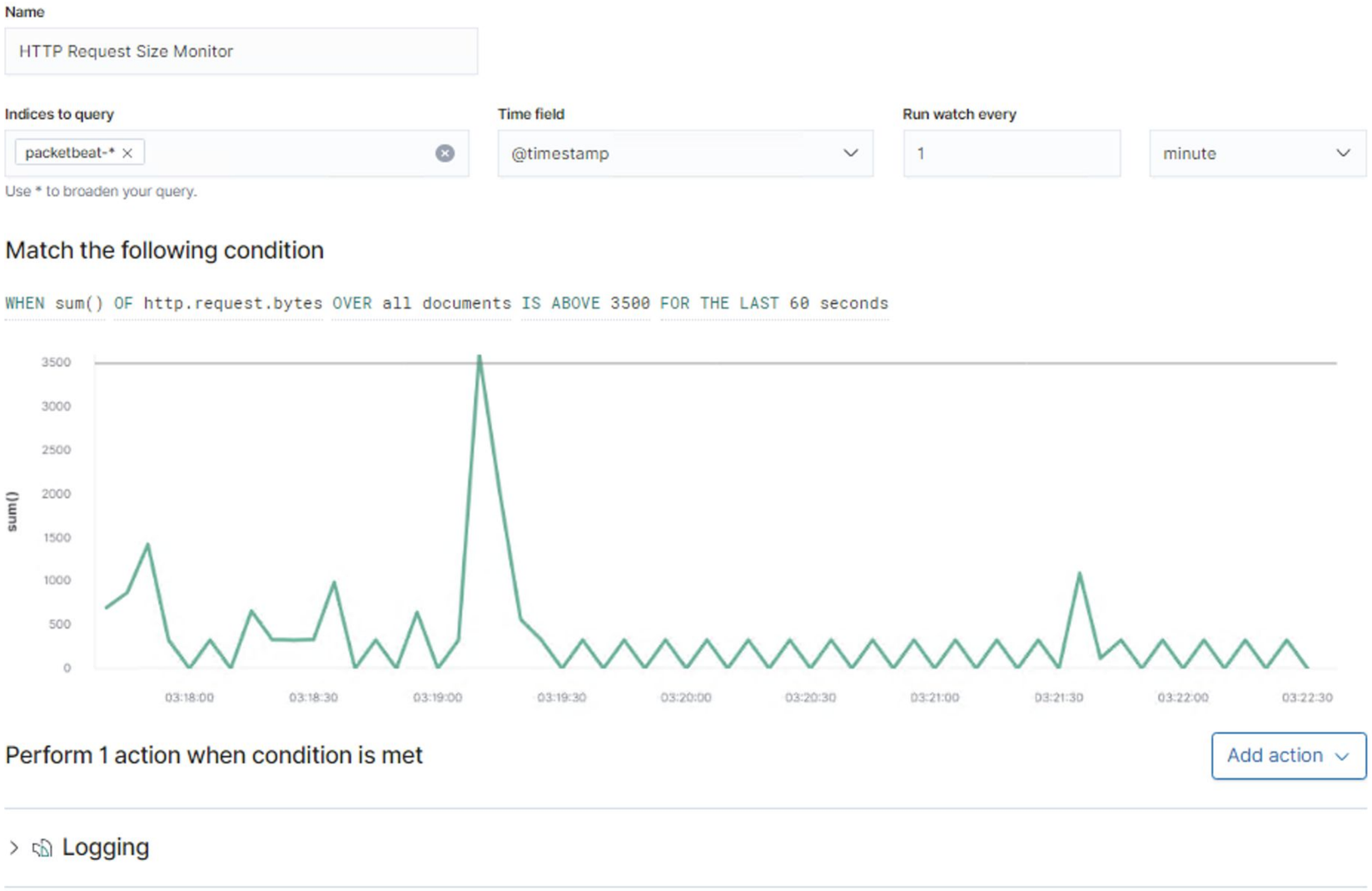
CPU Usage Monitor

- This alert monitors the percentage of CPU time used on the web server process
- This alert triggers if the CPU percentage is over 50% over 5 minutes



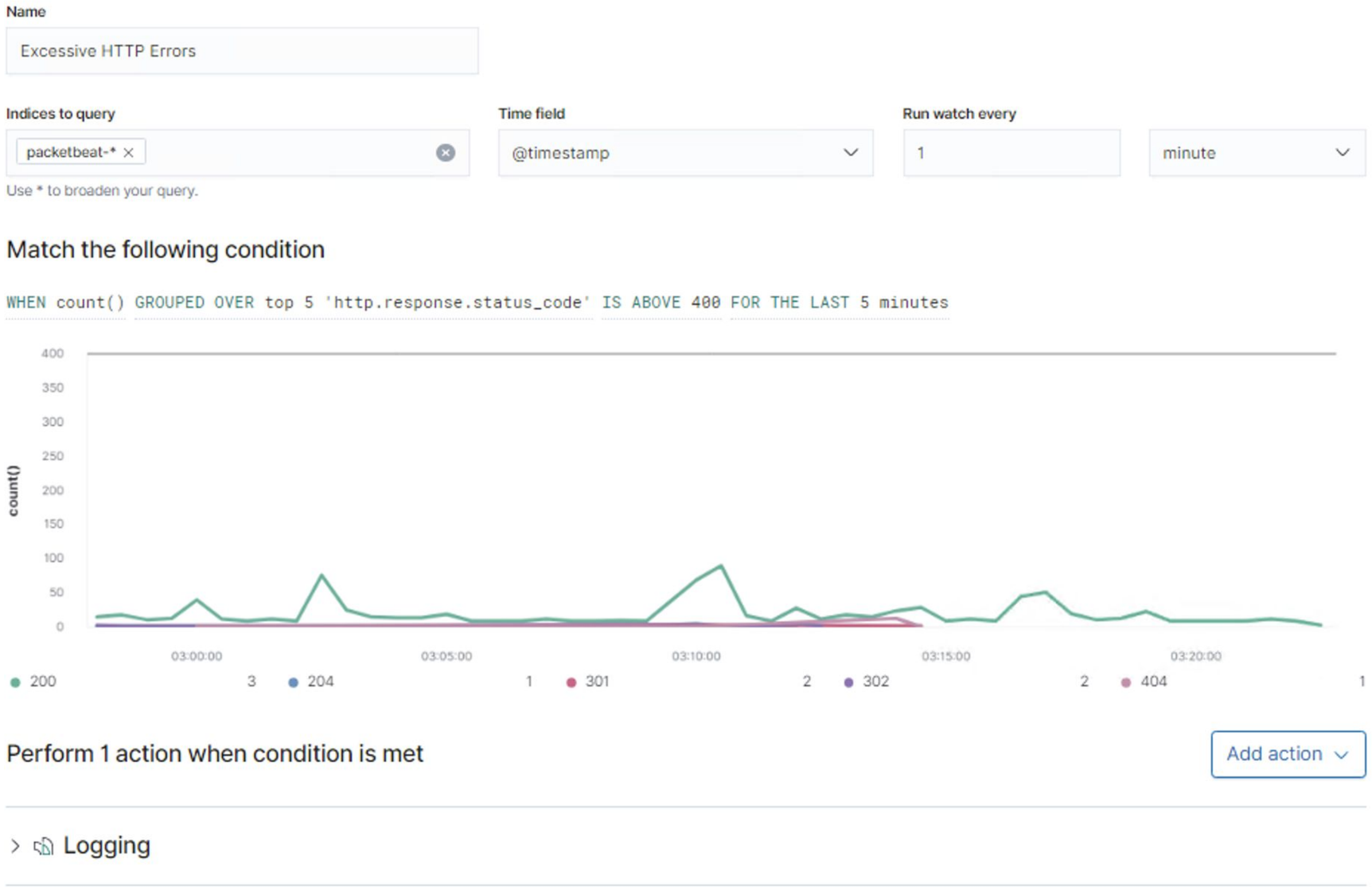
HTTP Request Size Monitor

- This alert measures the total size of http requests to the web server
- This alert triggers if the total bytes in requests in 60 seconds is 3500 or above



Excessive HTTP Errors Monitor

- This alert monitors the http response codes and triggers for error codes
- This alert triggers when there are over 400 instances over 5 minutes



Hardening

Hardening Against [A07:2021- Identification and Authentication Failures]

- Enforcing GPO policies to implement strong passwords, restricting old or reused passwords with minimal password characters(8).
- Disabling/Monitoring unneeded ports (Firewall).
- Multi-factor authentication with soft token or SMS messaging.
- These mitigations help prevent unauthorized access with brute force attacks and help protect against malicious hackers impacting data from being compromised or modified.

Hardening Against [A05:2021 - Security Misconfiguration]

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

- Implementation of FirewallD to control/block the flow the traffic through ports 22,80,111,139,445.
- With appropriate configuration the firewall will allow and deny traffic through the designated ports. This will protect against unauthorized SSH and other unwanted protocol.

Hardening Against [A01:2021 - Broken Access Control]

- Auditing users for least privilege monitoring permissions.
- Only root and sysadmin should be granted sudo permissions to mitigate unauthorized modifications and access to file structure.

Implementing Patches

Implementing Patches with Ansible

Playbook Overview

```
---
 - name: FirewallD
   hosts: localhost
   connection: local
   tasks:
    - name: FirewallD rules
      firewalld:
        permanent: yes
        immediate: yes
        port: "{{item.port}}/{{item.proto}}"
        state: "{{item.state}}"
        zone: "{{item.zone}}"
      with_items:
       - {port: "22,80,11,139,445", proto: "tcp", state: "disabled", zone: "public" }
```

This playbook blocks the vulnerable ports using firewalld

```
- name: Removing user inactive users
  user:
    name: "{{ item.username }}"
    state: absent
    remove: no        # Remove home user if yes; default no
    force: yes        # works with remove is yes
  with_items: "{{ remove_users }}"

- name: Removing from /etc/sudoers.d if existing
  file:
    path: /etc/sudoers.d/{{ item.username }}-allow-sudo
    state: absent
  with_items: "{{ remove_users }}"
```

With this playbook, a sysadmin can remove sudo access to a specific user which can help mitigate this kind of exploit