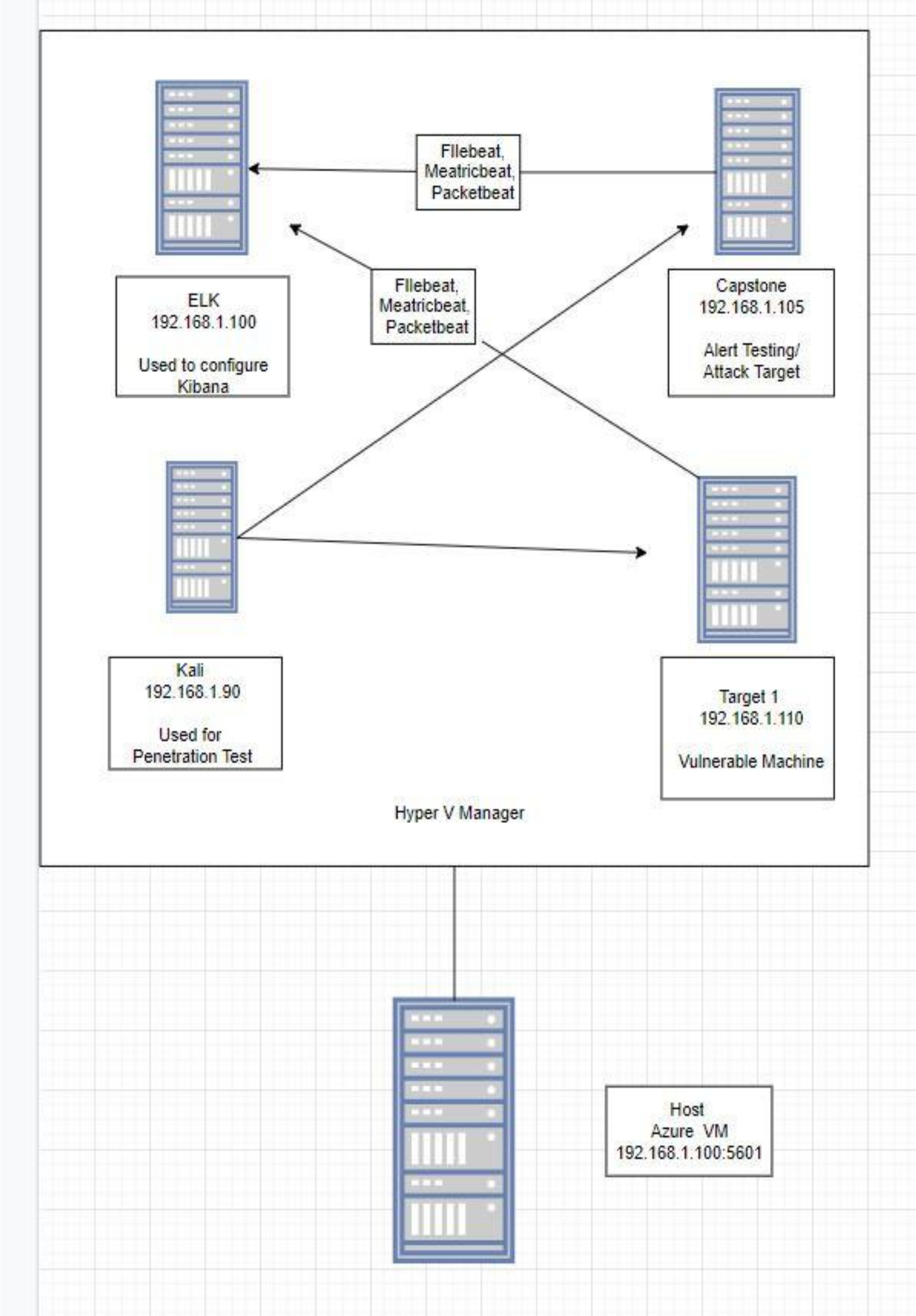
Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities



Network Topology

Network Range: 192.168.1.0/24
Host: Azure VM

Machine 1: Elk
IP: 192.168.1.100

Machine 2: Capstone
IP: 192.168.1.105

Machine 3: Kali
192.168.1.90

Mahine 4: Target 1
IP: 192.168.1.110

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Open SSH	Open Port 22	allows for remote access
Open Port 80	HTTP	access to company website
Weak Passwords	Passwords are easy to guess	Hackers can gain user access easily
Root Access	Employees have access to everything	Employees who are hacked give attackers root privileges

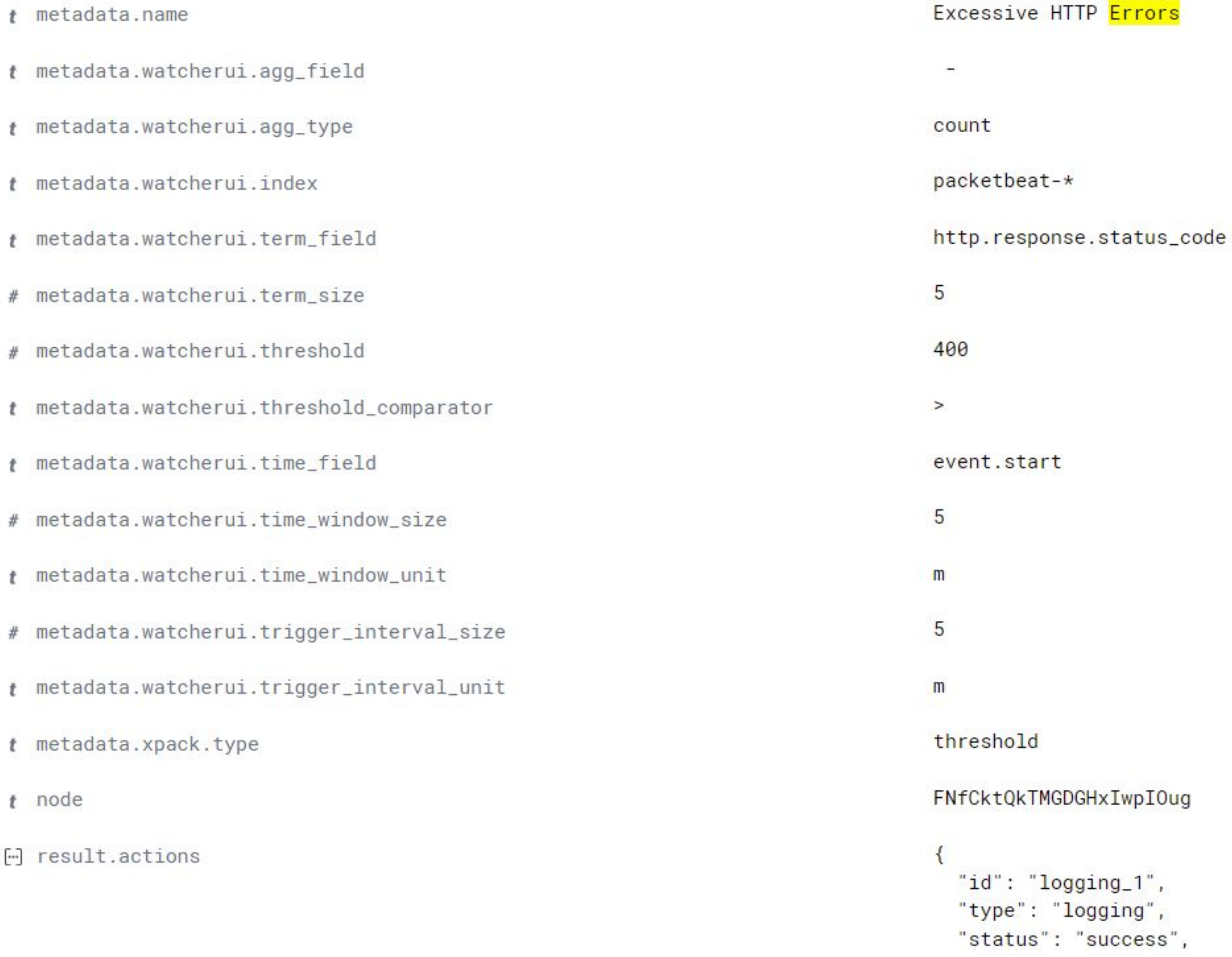
Alerts Implemented

Excessive HTTP Errors

Summarize the following:

- Which **metric** does this alert monitor? Packetbeat
- What is the **threshold** it fires at? + 400 for the last 5 minutes

Excessive HTTP Errors ScreenShot



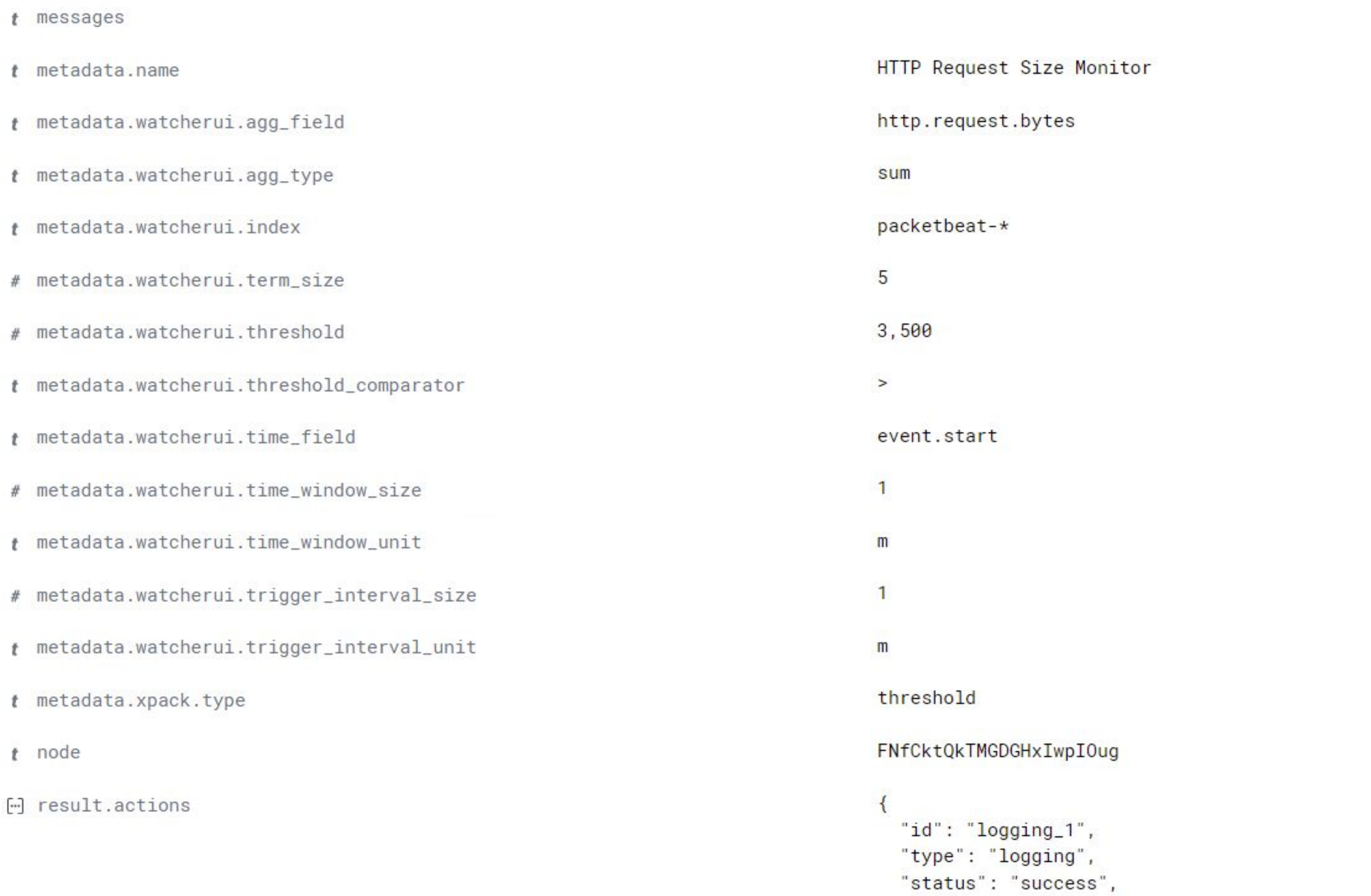
t	metadata.name	Excessive HTTP Errors
t	metadata.watcherui.agg_field	-
t	metadata.watcherui.agg_type	count
t	metadata.watcherui.index	packetbeat-*
t	metadata.watcherui.term_field	http.response.status_code
#	metadata.watcherui.term_size	5
#	metadata.watcherui.threshold	400
t	metadata.watcherui.threshold_comparator	>
t	metadata.watcherui.time_field	event.start
#	metadata.watcherui.time_window_size	5
t	metadata.watcherui.time_window_unit	m
#	metadata.watcherui.trigger_interval_size	5
t	metadata.watcherui.trigger_interval_unit	m
t	metadata.xpack.type	threshold
t	node	FNfCktQkTMGDGHxIwpIOug
[-]	result.actions	{ "id": "logging_1", "type": "logging", "status": "success",

HTTP Request Size Monitor

Summarize the following:

- Which **metric** does this alert monitor? Packetbeat
- What is the **threshold** it fires at? + 3500 in the last 1 minute

HTTP Request Size Monitor ScreenShot



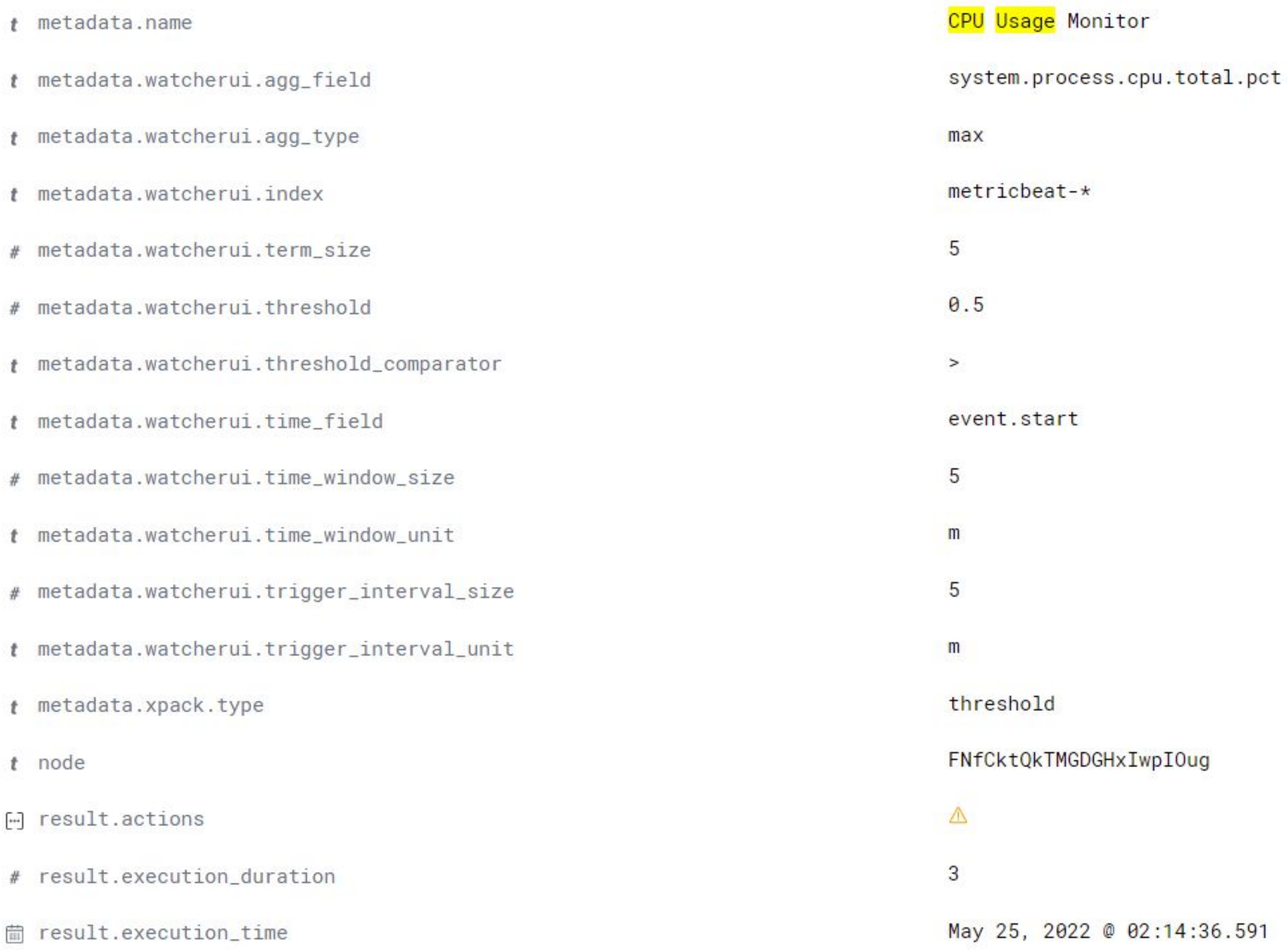
t	messages	
t	metadata.name	HTTP Request Size Monitor
t	metadata.watcherui.agg_field	http.request.bytes
t	metadata.watcherui.agg_type	sum
t	metadata.watcherui.index	packetbeat-*
#	metadata.watcherui.term_size	5
#	metadata.watcherui.threshold	3,500
t	metadata.watcherui.threshold_comparator	>
t	metadata.watcherui.time_field	event.start
#	metadata.watcherui.time_window_size	1
t	metadata.watcherui.time_window_unit	m
#	metadata.watcherui.trigger_interval_size	1
t	metadata.watcherui.trigger_interval_unit	m
t	metadata.xpack.type	threshold
t	node	FNfCktQkTMGDGHxIwpIOug
[⋯]	result.actions	{ "id": "logging_1", "type": "logging", "status": "success",

CPU Usage Monitor

Summarize the following:

- Which **metric** does this alert monitor? Metricbeat
- What is the **threshold** it fires at? +0.5 for the last 5 minutes

CPU Usage Monitor ScreenShot



t	metadata.name	CPU Usage Monitor
t	metadata.watcherui.agg_field	system.process.cpu.total.pct
t	metadata.watcherui.agg_type	max
t	metadata.watcherui.index	metricbeat-*
#	metadata.watcherui.term_size	5
#	metadata.watcherui.threshold	0.5
t	metadata.watcherui.threshold_comparator	>
t	metadata.watcherui.time_field	event.start
#	metadata.watcherui.time_window_size	5
t	metadata.watcherui.time_window_unit	m
#	metadata.watcherui.trigger_interval_size	5
t	metadata.watcherui.trigger_interval_unit	m
t	metadata.xpack.type	threshold
t	node	FNfCktQkTMGDGHxIwpIOug
[⋯]	result.actions	⚠
#	result.execution_duration	3
📅	result.execution_time	May 25, 2022 @ 02:14:36.591

Hardening

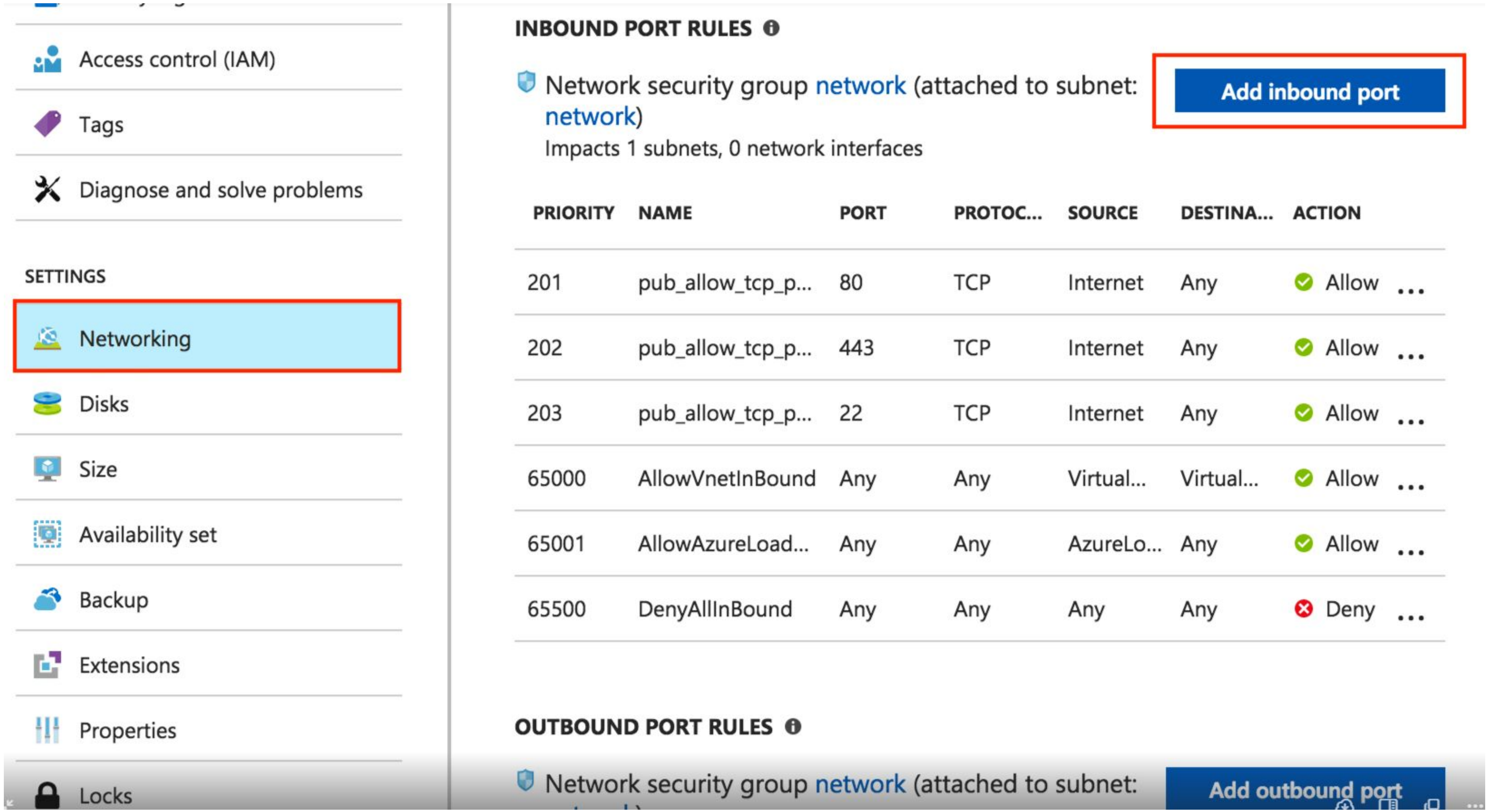
Hardening Against Open SSH on Target 1

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

Implement a firewall rule that only allows SSH access to specific IP Addresses

- Why the patch works.
    - Prevent outside of the IP range from being able to SSH
- How to install it (include commands)
    - Depends on the firewall rules

Example of Firewall ScreenShot



INBOUND PORT RULES

Network security group network (attached to subnet: network)

Impacts 1 subnets, 0 network interfaces

PRIORITY	NAME	PORT	PROTOC...	SOURCE	DESTINA...	ACTION
201	pub_allow_tcp_p...	80	TCP	Internet	Any	✓ Allow ...
202	pub_allow_tcp_p...	443	TCP	Internet	Any	✓ Allow ...
203	pub_allow_tcp_p...	22	TCP	Internet	Any	✓ Allow ...
65000	AllowVnetInBound	Any	Any	Virtual...	Virtual...	✓ Allow ...
65001	AllowAzureLoad...	Any	Any	AzureLo...	Any	✓ Allow ...
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny ...

OUTBOUND PORT RULES

Network security group network (attached to subnet:

source: Microsoft, retrieved from: https://docs.bitnami.com/azure/faq/administration/use-firewall/

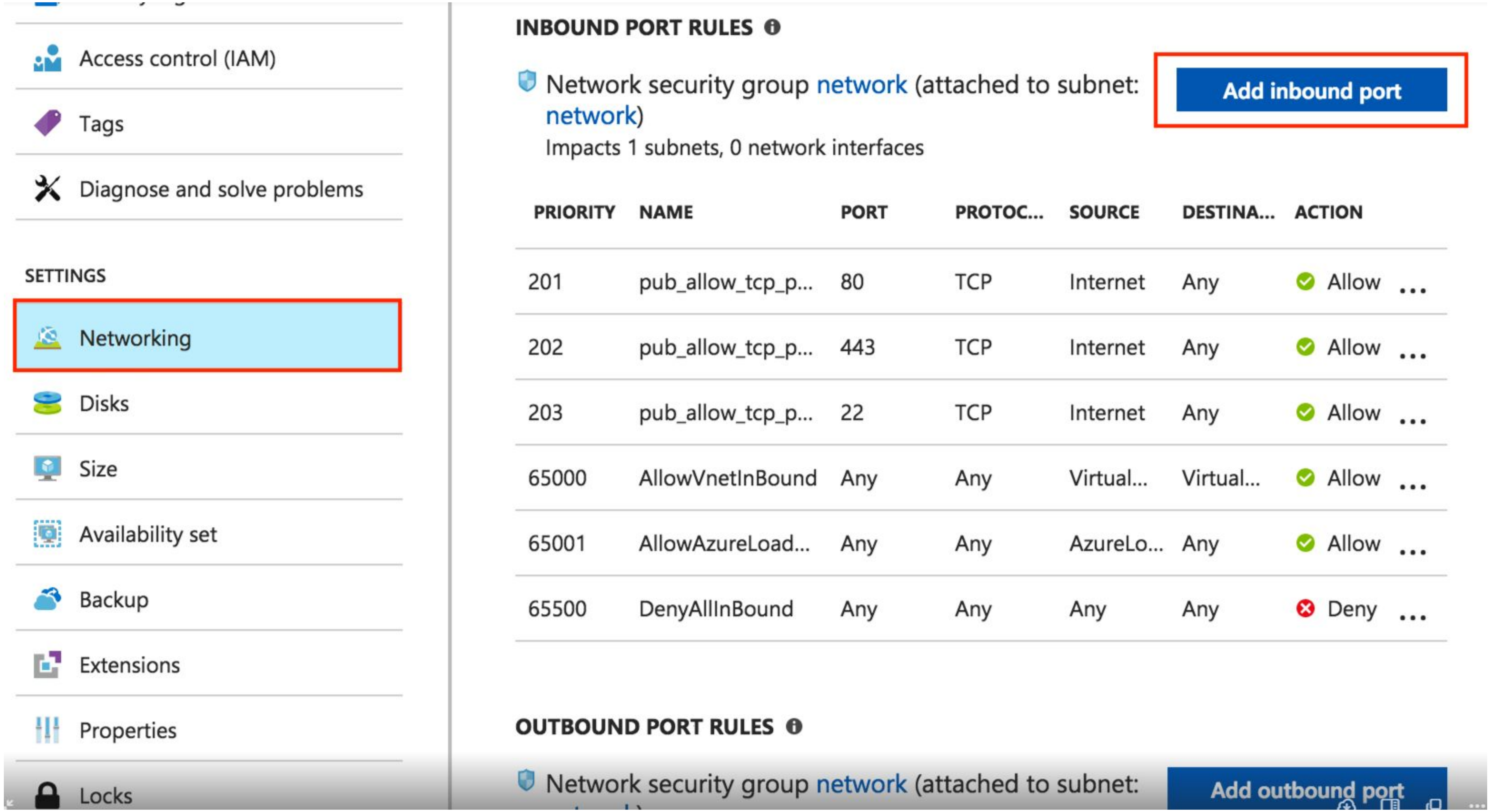
Hardening Against Open Port 80 on Target 1

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

Implement a firewall rule that only allows specific IP Addresses to access the company website

- Why the patch works.
  - Prevent outside IP addresses to access the company website
- How to install it (include commands)
  - Depends on the firewall rules

Example of Firewall ScreenShot



INBOUND PORT RULES

Network security group network (attached to subnet: network)
Impacts 1 subnets, 0 network interfaces

PRIORITY	NAME	PORT	PROTOC...	SOURCE	DESTINA...	ACTION	
201	pub_allow_tcp_p...	80	TCP	Internet	Any	✓ Allow	...
202	pub_allow_tcp_p...	443	TCP	Internet	Any	✓ Allow	...
203	pub_allow_tcp_p...	22	TCP	Internet	Any	✓ Allow	...
65000	AllowVnetInBound	Any	Any	Virtual...	Virtual...	✓ Allow	...
65001	AllowAzureLoad...	Any	Any	AzureLo...	Any	✓ Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny	...

OUTBOUND PORT RULES

Network security group network (attached to subnet:

source: Microsoft, retrieved from: https://docs.bitnami.com/azure/faq/administration/use-firewall/

Hardening Against Password Complexity on Target 1

Explain how to patch Target 1 against Vulnerability 3. Include:

Train employees how to create difficult passwords and use two-factor authentication, implement password complexity requirements

- Why the patch works.
  - Complex passwords make it harder for hackers to gain access
- How to install it
  - Administrative policies to include complexity requirements, employee training
  - Mandatory password changes every quarter
  - Mandatory training on cybersecurity - password practices every 6 months
  - Implement Password Manager like LastPass

Hardening Against Administration Access on Target 1

Explain how to patch Target 1 against Vulnerability 4. Include:

Do not allow employees to have root access

- Why the patch works.
  - Giving employees root access risks the chance of a hacker gaining access to company or sensitive data and information.
- How to install it (include commands).
  - sudo deluser steven sudo
  - sudo deluser (insert name) sudo

Implementing Patches

Implementing Patches with Ansible

Playbook Overview

Explain which vulnerability each task in the playbook patches.

The vulnerabilities that were identified are: Open SSH, Open Port 80, Open Port 111, Open Port 139/445. In order to fix these vulnerabilities, the organization would have to implement configuration files for each firewall rule where the firewall rule limits IP Addresses from accessing certain ports. This would then be pushed out to all systems that host WordPress in order to avoid unwanted exploitations.