

# **Final Engagement**

Attack, Defense & Analysis of a Vulnerable Network

# Start of Blue Team Presentation

# Table of Contents

---

This document contains the following resources:



**Alerts Implemented**



**Hardening**



**Implementing Patches**

# Alerts Implemented

# [HTTP Errors ]

- This metric alert monitors HTTP
- The threshold fires at 400
- Low reliability

Current status for 'Excessive HTTP Errors'

DeactivateDele

Execution history			Action statuses
Last one hour			
Trigger time	State <span>↑</span>	Comment	
2020-11-17T02:58:26+00:00	▶ Firing		
2020-11-17T02:43:26+00:00	▶ Firing		
2020-11-18T22:45:04+00:00	✓ OK		
2020-11-18T22:40:04+00:00	✓ OK		

# [HTTP Request Size Monitor]

- The metric alert monitors http.request.bytes
- The threshold fires at 3400
- Low Reliability

.

Current status for 'HTTP Request Size Monitor' [Deactivate](#) [Delete](#)

Execution history

Action statuses

Last 7 days

Trigger time	State <span>↑</span>	Comment
2020-11-18T22:48:04+00:00	<span>▶</span> Firing	
2020-11-18T22:47:04+00:00	<span>▶</span> Firing	
2020-11-18T22:46:04+00:00	<span>▶</span> Firing	
2020-11-18T22:45:04+00:00	<span>▶</span> Firing	
2020-11-18T22:44:04+00:00	<span>▶</span> Firing	
2020-11-18T22:43:04+00:00	<span>▶</span> Firing	
2020-11-18T22:38:04+00:00	<span>▶</span> Firing	
2020-11-18T22:37:04+00:00	<span>▶</span> Firing	
2020-11-18T22:36:04+00:00	<span>▶</span> Firing	
2020-11-18T22:34:04+00:00	<span>▶</span> Firing	
2020-11-18T22:33:04+00:00	<span>▶</span> Firing	
2020-11-18T22:32:04+00:00	<span>▶</span> Firing	
2020-11-18T22:31:04+00:00	<span>▶</span> Firing	
2020-11-18T22:30:04+00:00	<span>▶</span> Firing	
2020-11-18T22:29:04+00:00	<span>▶</span> Firing	
2020-11-18T22:24:04+00:00	<span>▶</span> Firing	
2020-11-18T22:23:04+00:00	<span>▶</span> Firing	
2020-11-18T22:22:04+00:00	<span>▶</span> Firing	

# [CPU Usage Monitor]

- The metric alert monitors `system.process.cpu.total.pct`
- The threshold it fires at 0.5

Current status for 'CPU Usage Monitor'

[Deactivate](#) [Delete](#)

[Execution history](#) [Action statuses](#)

Last one hour

Trigger time	State ↑	Comment
2020-11-17T03:28:02+00:00	▷ Firing	
2020-11-17T03:27:03+00:00	▷ Firing	
2020-11-17T03:26:03+00:00	▷ Firing	
2020-11-17T03:25:03+00:00	▷ Firing	
2020-11-17T03:24:03+00:00	▷ Firing	
2020-11-17T03:23:02+00:00	▷ Firing	
2020-11-18T22:45:04+00:00	✓ OK	
2020-11-18T22:40:04+00:00	✓ OK	
2020-11-18T22:35:04+00:00	✓ OK	

# Hardening



# Hardening Against [Open Ports] on Target 1

---

- Disable Root Logins
- Use Public/Private Keys for Authentication
- Assign Another port (Non standard port) for ssh, http etc
- Disable ICMP to prevent port scans

# Hardening Against [Excessive CPU Usage] on Target 1

---

- Load Balancer should be implemented prevent web-servers from overloading and to add redundancy.
  - Why It Works: Load balancers also add resiliency by rerouting live traffic from one server to another if a server falls prey to DDoS attacks or otherwise becomes unavailable.
- Set an alert that if a user exceeds the expected baseline traffic slow them down or block them temporarily and investigate their actions.
  - If a user was behaving maliciously you may quickly detect it or even prevent it.

# Hardening Against [Password Vulnerability] on Target 1

---

- Make a policy to require secure passwords
  - Guidelines: minimum 16 characters long
  - Must have a capital letter
  - Must have a lowercase letter
  - Must have a number
  - Must have a symbol
  - Lockout users after after multiple failed attempts
  - Maintain geolocation data of where a user logs in from and monitor for anomalies



# Implementing Patches

# Implementing Patches

```
1  README
2  Implementing Patches
3  Patches for Vulnerabilities on Target 1
4  Hardening against Open Ports [ssh port 22]
5      Disable root login
6          To do this: Go to /etc/ssh/sshd_config
7              set PermitRootLogin to no
8  Assign a Non Standard port for ssh to avoid casual scans
9      To do this: Open /etc/ssh/sshd_config file and look for line Port 22 and change line to port [Non Standard port]
10     Restart sshd server
11     Now ssh using ssh -p [non standard port choosen] user@your-ip
12  Disable ICMP to prevent results from port scanning
13     To do this: no ip icmp echo broadcast-request
14  Hardening against Password Vulnerabilities on Target 1
15  Steps to Enforcing password strenght and lenght
16     To do this:
17         1. Open Command prompt
18         2. Enter command net accounts
19         3. Enter command net accounts /minpwlen:NumberOfCharacters
20  Steps to force local account to change password as needed
21     To do this:
22         1. Click/tap on Users in the left pane of Local Users and Groups
23         2. Right click or press and hold on the name, then click on properties
24         3. In the General tab, check the User must change password at [Desired time]
25
26
```