GoodSecurity Breech Report

RobertForee[@ScenarioLab.com](mailto:robforee@ScenarioLab.com)

11/01/2021

# High-Level Summary

GoodSecurity was tasked with auditing activity on GoodCorp’s network on March 25, 2020. The focus of this audit it to identify exploits and recommend mediation strategies.

When performing the audit, there were two sets of logs identified with traces of the attack, Microsoft Windows security auditing log, and the Apache web server log.

In the Windows logs, we see evidence the hacker initiated the following activities:

* High volume of attempts to login
* High volume of attempts to reset password

The results to this activity series was

* Legitimate users were unable to login

GoodSecurity recommends the following policies

* Strong password policies
* Two factor authentication on public facing servers.
* Disallow user creation and permission escalation on public facing servers.

Apache log analysis

In the Apache logs, we see evidence the hacker initiated two attacks:

* repeated GET requests for a non existent file from a single IP address (6pm peak)
* repeated login page POST requests from 3 IP addresses (8pm peak)

The result of this attack was

* loss of access to the web server
* unable to determine if any logins were successful
  + neither baseline or attack contains 401 responses
  + unable to examine POST contents

The recommendations to protect from these type of attacks are:

* alert on activity from a single IP address of greater than 5 per second
* black list any IP address that exceeds the alert threshold

# Question 1 ~

What mitigations would you recommend to protect each user account

# Question 2 ~

What sort of mitigation would you use to protect against “bad logins” lock out?