Final Engagement

Attack, Defense & Analysis of a Vulnerable System

Table of Contents

Overview

Cybersecurity is by no means solely a lateral issue. There is no sweeping statement, or solution, that can cover it all. However, this affords us the opportunity to invest time, enginuity, and resources into creating personalised outcomes for each digital hurdle we come across. Over the past week, we have employed strategies and techniques to hit the web server provided and see what shakes loose. The following is a condensed iteration of our two reports on both the findings and our proposed solutions in response to which security issues arose.

Don't Lack a Patch

Install and Maintain All Vendor Security and Integrity Patches

High Risk Vulnerabilities

1

Password Parameters :
Extremely weak password complexity
Insufficient Password Aging
Insufficiently Protected Credentials
Excessive Authentication Attempts

2

Network Vulnerabilities:
Weak or No Firewall
Exposed Ports 22 & 80
Weak SQL, Apache, and SSH security

3

User Accounts and Data:
High Volume of Data Accessible to External Actors
Private Information Exposed
Unsecured Databases
Shell Sessions Lacking Idle Timeouts
Improper Access Control
Insufficient Encryption


Risks Realised

Network Vulnerabilities

With the lack of Firewall, weak, off the shelf security measures on SSH, Apache and MySQL, and open SSH and HTTP/HTTPS ports, you're laying out the welcome mat for DDoS attacks, packet sniffing, HTTP request smuggling, and a wide array of other malicious attacks.

Implications:
Not only could you lose out on availability, but there's also the risk of allowing access to your databases, confidential information, and further ways to exploit your systems.

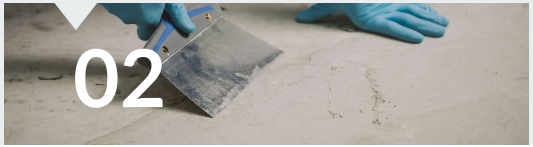
Network Solutions

Firewall

Firewalls are imperative for reducing unwanted and unauthorized network traffic. It will monitor all ingoing and outgoing traffic and work like a barrier for your internet-facing systems. Implementing further forms of monitoring like Fail2Ban is the next step in reinforcing that barrier.

SSH Hardening

Closing ports is not always the best way to protect your network from actors with ill-will. Often times hardening the service is a much more effective measure that will not hinder functionality. Implement SSH parameters such as disabling X11 forwarding, create idle timeout intervals, and removing dead passwords will make all the difference.



Retrofit MySQL

Running mysql_secure_install may seem like an extremely simple way to improve database security without having to put many recoursed into it, because it is! By using the secure install you are able to increase security without compromising on the speed and efficiency of SQL.

Password & Privacy Vulnerabilities

Something as small as a weak password can cause huge issues when it comes to information and database privacy. In 2019, 81% of hacking-related breaches were due to compromised passwords - this could be due to any number of weak permissions, however the most common are often the culprits.

Implications:
Lacking any rules regarding password complexity, aging, length, or failed login attempt restrictions leaves data and permissions open to being viewed and tampered with.

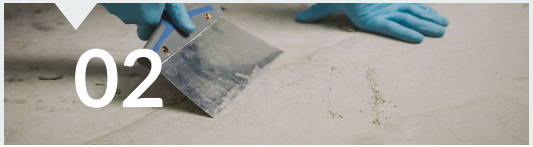
Password & Privacy Solutions

Harden Passwords

The most understated, but arguably the most important of maintaining data secrecy and system integrity. By increasing the parameters for password length and complexity, as well as implementing password aging, you can eliminate many of the opportunities for attackers to brute-force their way into your system.

Restricting Excessive Authentication Attempts

One of the best ways to defend against brute force attacks, either through password guessing or the use of John the Ripper, is to restrict excessive authentication attempts. Though it may seem like a miniscule addition, it is a must-have for any login credentials, especially those with sudo, administrative, or root access.



Role Based Authentication

Though it is more straightforward to deny access to certain files, databases and functions to everyone by default, the flexibility that role based authentication provides is much more impactful, especially for companies that have a large network. Though it can be laborious to implement, it is well worth the security it affords.

Thank you.