Penetration Testing a Cloud Environment

Digital Marketing Firm

TESTING SECURITY CONTROLS INSIDE AND OUT

CUSTOMER PROFILE

A Digital Marketing Technology startup headquartered in the Northeast and focused on content personalization and consumer data onboarding.

CHALLENGES:

✓ Uncover vulnerabilities in applications and network perimeters.

✓ Discover weaknesses in process or technical countermeasures.

✓ Identify potential vulnerabilities from system misconfigurations.

✓ Actively exploit those vulnerabilities found in order to prove or disprove them.

RESULTS:

✓ Identified unpatched administrative interfaces, administrator authentication bypass.

✓ External webserver leaking internal IP address.

✓ Services found running insecure SSL modes Were immediately disabled.

✓ Leaked password hash information

✓ Default credentials eliminated.

620 Newport Center Drive, Suite 1100 | Newport Beach, CA 92660

THE PROBLEM

The investors of a well-funded startup required the company to test their security controls in real-world attack vectors against the organization, their assets, data, and employees. The purpose of this project was to perform that testing.

The objective was to identify vulnerabilities and potential weaknesses in the identified client network perimeter and web applications. The test was conducted as a "**black box**" test with limited information, such as target IP/URLs, provided by the client. iPRESIDIUM'S Security Team then performed digital reconnaissance in order to determine the client's publicly accessible IP addresses and applications being used.

SCOPE & CRITERIA

The startup's environment involved numerous IT stakeholders. The client required an outside consultant to complete a security assessment of production web applications and the servers that the applications are hosted on.

The critical success factors for this project included:

- Understanding of the objectives of the project in detail, how the testing would be performed and how the findings would be reported to the company.

- Communication throughout the project would be required with both IT and IS teams to keep them informed of progress, issues that arose and interim results, especially as they related to the need to adjust the approach to maximize the benefit of the engagement.

- Demonstrate sensitivity to the security team so as to maintain a balance between their need to perform their duties while testing the ability of their network defenders to successfully detect and respond to the attacks.

ENGAGEMENT

iPRESIDIUM performed a vulnerability assessment and penetration test against the list of public IPs and web applications, confirmed by the client, using both automated commercial and open source tools.
The results were then verified by performing manual testing of each reported exploit in order to rule out any false positive results.

iPRESIDIUM assessment was conducted with the use of both non-intrusive and robust commercial scanning tools and manual testing to deliver comprehensive infrastructure reports of active IP systems. Open-source tools were also used to validate certain checks to remove any false positives.

METHODOLOGY

THE SOLUTION

The entire project took 4 weeks to complete providing the startup and their investors with the comprehensive evaluation of their cyber security posture and a detailed report of our findings presented to the company, including:

- Background Information.

- Description of methodology used.

- List of discovered vulnerabilities found.

- Details of exploited vulnerabilities and steps describing how to reproduce the exploit.

- Conclusions.

- Recommendations.

Following iPRESIDIUM'S engagement, the startup was able to quickly remediate the vulnerabilities found, mitigate their risks and show both their investors and customers their commitment and dedication to security.

About iPRESIDIUM

iPRESIDIUM is a cyber security and risk advisory firm. We provide end-to-end enterprise security services for private and public entities of all sizes. iPRESIDIUM helps customers protect their business, employees, data, and their reputations. We succeed by offering our clients cutting edge technologies with best-in-class security solutions, experienced industry professionals proficient in cyber security and managed service platforms. Our goal, to deliver our clients' the peace of mind they need so that they can focus on their business.

Since its inception in 2002, iPRESIDIUM has successfully exceeded the security needs of numerous organizations, across the following sectors: Healthcare, Retail, Education, Government and Public Sector, Financial, Technology, Hospitality, Insurance, Transportation and Manufacturing as well as over 50 US federal agencies and the intelligence communities.

www.ipresidium.com | info@ipresidium.com | 949-721-6612