ACCORIAN

CASE STUDY

RED TEAM MULTI-LAYERED ASSESSMENT

Here's how the client assessed their overall security posture through a multi-layered security approach engaging in a Red Team Assessment.

THE CLIENT: An established digital marketing platform that empowers businesses with comprehensive tools to thrive in today's digital landscape.

LOCATION: USA

INDUSTRY: Digital Marketing

SERVICE BRIEF: Our client has an established digital marketing platform.

Our client is a well-established digital marketing platform, boasting a global network of offices and a team of 1,500 employees. They empower businesses of all sizes to thrive in the ever-evolving digital landscape by providing a comprehensive suite of tools for online marketing success.

1 THE CHALLENGE FOR THE CLIENT

The client sought a comprehensive evaluation of their security posture. They possess a robust vulnerability management program and have always prioritized employee security awareness. However, understanding the ever-changing threat landscape, the client desired to test both the effectiveness of their external defenses and their internal network preparedness against simulated real-world attacks by engaging in a red team assessment.

While a robust vulnerability management program is essential, cyberattacks are becoming increasingly sophisticated. Basic malware is no longer the main concern. Attackers are employing advanced techniques that target specific organizations. These targeted attacks are designed to bypass traditional security controls. According to cybersecurity ventures, global cybercrime costs are projected to reach $10.5 trillion annually by 2025 (up from $6 trillion in 2021). This staggering increase underscores the growing threat landscape and hence our client approached Accorian to assess their readiness for their cyber defenses.

2 THE SOLUTION

Despite robust external defenses evident in Phase 1 (External Defence Mechanisms Evaluation), the Phase 2 (Internal Network Preparedness Assessment) revealed significant vulnerabilities within the internal network. Weak password hygiene practices and inadequate access controls presented substantial security risks. This assessment highlighted the importance of prioritizing internal network security alongside external perimeter defenses.

3 OUR SCOPE

We were asked to identify different methods of compromising internal accounts & systems to assess internal teams' exposure to an attack and assess the implications of this exposure on the Client’s IP and customer data.

4 OUR APPROACH

We proposed a Multi-Layered Assessment (two phased), which presented a dynamic and goal-oriented testing approach. Phase 1 focused on evaluating external defenses with minimal initial information, starting only with the company name, while Phase 2 targeted internal network preparedness with limited domain user credentials provided by the client.

PHASE 1: EXTERNAL DEFENSE MECHANISMS EVALUATION

By employing open-source intelligence (OSINT) techniques, the Red Team conducted extensive reconnaissance. This included:

1. **Enumeration:** Identifying numerous subdomains and confirming newly acquired ones.
2. **Service Identification:** Enumerating exposed services and determining the technology stack utilized.
3. **Information Gathering:** Collecting employee, partner, and client information for potential social engineering attempts.

Despite encountering HTTP services secured by Cloudflare, the Red Team successfully:

1. **Extracted Valid Email Addresses:** This information could be used for future phishing campaigns.
2. **Identified Kubernetes Clusters and ArgoCD Services:** While beneficial for development and deployment, the awareness of usage of these technologies could help attackers tailor their attack.
3. **Uncovered Sensitive Information in Personal Repositories:** Leaked credentials and API tokens exposed in employee repositories could be exploited by attackers.
4. **Identified Leaked Credentials:** Credentials compromised in third-party breaches could be leveraged if reused across multiple platforms.
5. **Social Engineering Attempt:** The Red Team successfully conducted a social engineering attempt (spear phishing) on an employee. However, the swift reporting demonstrated commendable awareness and response capabilities within the client's organization.

PHASE 2: INTERNAL NETWORK PREPAREDNESS ASSESSMENT

With limited domain user credentials, the Red Team delved deeper into the internal network:

- The team, using network mapping techniques, meticulously mapped the Active Directory (AD) network, identifying potential high-value targets.
- Service accounts susceptible to kerberoasting were discovered. While cracking the tickets wasn't possible in the limited time, the team adapted their approach.
- Attempts were made to capture network hashes through LLMNR/NBT-NS poisoning. The lack of captured hashes suggested potential mitigation strategies employed by the client.
- The Red Team gained access to Network Shares with excessive permissions. These shares contained sensitive files, source code, configuration files, etc., allowing the team to compromise privileged user accounts.
- By exploiting misconfigured access controls, the Red Team escalated privileges and ultimately achieved domain administrator access, surpassing the initial flags for assessment purposes.

5 THE RESULT

While Phase 1 did not completely breach the external perimeter, it revealed valuable insights. The client learned about potential social engineering vulnerabilities and the types of information exposed through side channels. This knowledge allows them to implement targeted measures to strengthen their external defenses. The assessment's true impact lied in Phase 2's identification of significant vulnerabilities within the internal network. This highlighted the critical need for a multi-layered security approach that prioritizes both external and internal controls.

KEY TAKEAWAYS:

- Implement stringent access controls and regular audits to mitigate risks associated with vulnerable service accounts.
- Enforce encryption protocols and conduct periodic reviews to ensure the integrity of network communications.
- Enhance employee training programs to foster a culture of cybersecurity awareness and vigilance.
- Continuously monitor and update security measures to adapt to emerging threats and evolving attack vectors.

6 SURPRISE IN THE JOURNEY

The most surprising aspect for the client was the Red Team's complete takeover, achieving external defenses and the Red Team started with limited access. The other surprise points were the vulnerabilities within the internal network, such as weak passwords and poorly configured access controls.

7 WHY ACCORIAN?

Accorian is a leading cybersecurity firm, distinguished by its CREST accreditation, renowned for unparalleled expertise. Our team comprises technology and cybersecurity leaders, ensuring proficiency that exceeds industry standards. What truly distinguishes us is our commitment to tailor-made solutions. Each red team assessment, backed by our remarkable 100% success rate, is meticulously customized to meet an organization’s unique needs, ensuring relevance and effectiveness in today’s business landscape.

Source: Cybersecurity Research: All In One Place (cybersecurityventures.com)

ACCORIAN

Focus On Your Business While We Focus On Your Security

✉ info@accorian.com ☎ +1 732 443 3468 🌐 www.accorian.com