ACCORIAN

Top 5 Red Team Scenarios To Understand True Security and Bolster Your Organization's Defenses

Cybersecurity is an ongoing battle and organizations need proactive measures to stay ahead of evolving threats.

While firewalls, antivirus software, IPS and other perimeter security tools act as the initial line of defense, a proactive approach to identify and address vulnerabilities is crucial before they're exploited in the wild. This is where red teaming comes in.

Imagine a team of seasoned security testers mimicking real-world attackers with a mission to infiltrate your organization's digital defenses, expose weaknesses, and test the effectiveness of your security controls. This simulated attack scenario is the essence of red teaming.

Traditional penetration testing (pentesting) identifies vulnerabilities in your systems. However, red teaming goes a step further by chaining different types of tests together. It simulates a real-world attacker's approach, complete with social engineering tactics and multi-stage attacks. This provides invaluable insights into your organization's preparedness against evolving cyber threats.

A security breach is CISO's nightmare. This could lead to financial losses, reputational damage, and even legal repercussions.

Red teaming helps CISOs and security teams proactively address these concerns by:

- **Identifying exploitable vulnerabilities:** Red teams uncover weaknesses in your security posture that traditional pentesting might miss. These could be technical vulnerabilities in systems or human vulnerabilities in security awareness training.
- **Testing security controls:** Red teaming puts your firewalls, intrusion detection systems, and other security controls to the test. This ensures they are functioning effectively and can identify and mitigate real-world attacks.
- **Evaluating incident response protocols:** Red teaming helps assess your team's ability to detect, contain, and remediate a cyberattack. While we are running a red team exercise, do your defenses alert and show the activity? This allows you to identify gaps in your incident response plan and make necessary improvements.
- **Empowering informed decision-making:** By providing a realistic picture of your security posture, red teaming empowers CISOs to make informed decisions regarding security strategy and helps gauge the true security of organizations.

During a red teaming engagement, you'll collaborate with the red team to define the scenarios they'll simulate. While scenarios can be customized to your specific needs, here are the top 5 red teaming scenarios that resonate with many organizations:

Scenario 1

Compromising Active Directory (AD)

Active Directory (AD) is the crown jewel of any organization's digital kingdom, making it a prime target for attackers. It stores user credentials and access controls. Red teams will employ various tactics to gain access to AD, such as exploiting overly permissive user accounts and attempting to exploit them through techniques like password spraying or brute-force attacks. The team would attempt to identify misconfigurations or launch social engineering attacks to trick users into revealing sensitive information. Once they gain access, they can potentially steal sensitive data, disrupt operations, or move laterally within your network to compromise other systems. Successfully compromising AD can grant attackers extensive control over an organization's resources and sensitive data.

Scenario 2

Targeting Business-Critical Machines/Servers

Imagine a specific machine or network segment housing your most sensitive data, like financial records or intellectual property. Red teams will meticulously craft an attack path, leveraging vulnerabilities in your network and systems, to reach and potentially compromise this critical target. This scenario is particularly relevant for organizations subject to regulations or compliance requirements that mandate stricter security measures for specific data types.

Scenario 3

C-Level Email Account Takeover

C-level executives often have access to highly sensitive information and could contain considerable decision-making power. A compromised C-level email account can be a goldmine for attackers. Red teams will attempt to gain access to C-level email accounts using sophisticated phishing techniques, similar to those used in real-world attacks like the infamous 2012 iCloud account hack. Once they gain access, they can steal sensitive information, impersonate executives to issue fraudulent instructions, or use the compromised account as a springboard to launch further attacks within your organization. The objective is not only to access sensitive information but also to gauge the potential for further compromise and lateral movement within the organization's infrastructure.

Scenario 4

Data Exfiltration

Gaining access to sensitive data is a victory for attackers, but the real damage comes when they can exfiltrate it. This scenario tests the effectiveness of your Data Loss Prevention (DLP) controls and other countermeasures designed to prevent unauthorized data movement. Red teams will attempt to exfiltrate data using various methods, potentially including seemingly harmless tools like Grammarly for example to sneak data out under the radar.

Scenario 5

Backdooring an Application

While compromising an application or server is a common goal for attackers, red teaming can also assess their ability to maintain persistent access. Imagine attackers implanting a hidden backdoor within an application, allowing them to regain access even after being detected. This scenario helps evaluate your blue team's (security operations) ability to detect and respond to such threats. Their response time and effectiveness in mitigating the backdoor can be crucial in preventing further damage.

Red team engagements can be simulated from both internal and external perspectives. It's often more valuable to start internally, mimicking an insider threat or an attacker with initial access within your network a.k.a, assumed breach. This allows red teams to focus on their objectives without needing to breach your external defenses first. Once internal security is strengthened, you can progress to scenarios mimicking an external attacker with no initial access. Ideally, a layered approach (inside-out) is recommended, prioritizing internal security while subsequently strengthening external perimeters.

The top 5 scenarios discussed earlier provide a strong foundation, but red teaming engagements should be tailored to address your specific needs and concerns. Remember, red teaming isn't about winning or losing; ***it's about continuous learning and fortifying your defenses against real-world threats.***

ACCORIAN

Focus On Your Business While We Focus On Your Security

info@accorian.com +1 732 443 3468 www.accorian.com