DIRECTDEFENSE

CASE STUDY

GAINING UNDETECTED ACCESS AND ESCALATING PRIVILEGES AT A MAJOR ORGANIZATION

How a Red Team Assessment Uncovered Hidden Security Vulnerabilities

One of our clients, a major organization that manages large amounts of critical data, prioritizes internal and external security to protect that data. As their MSSP, we staff a 24/7/365 SOC, perform penetration testing, and make continuous recommendations for added security solutions – and we recently conducted a red team assessment to put their security up against the real-world tactics and procedures of determined attackers.

A red team assessment is useful for organizations with security maturity that need a more comprehensive analysis of their security posture. This in-depth assessment can go a long way in validating existing security measures and identifying gaps. All organizations – especially those housing critical data – should conduct penetration test assessments annually to keep up with ever-evolving threats and attack tactics.

Organizations like our client that handle large amounts of personally identifiable information (PII) and protected health information (PHI) are targets for attackers looking to score data they can sell on the dark web. A large-scale breach involving compromise of significant amounts of PII and PHI can cripple an organization both reputationally and financially, and the best defense is to test your security against even the most deceptive attack vectors.

While we identified many strengths during the red team assessment that validated the organization's security posture, numerous weaknesses left data open to compromise.

Observed Strengths:

01. **Internal Network Security Monitoring and Alerting:**
A drop box our consultants connected to the internal network during the physical penetration test was quickly discovered and was disconnected by security personnel within 30 minutes of detection.

02. **Multi-Factor Authentication (MFA) Enabled for VPN Access:**
The organization successfully deployed MFA for external access to the VPN, requiring users to authenticate from a device with the organization's certificate installed. Without the certificate, no connection can be established, representing a strong control to prevent external compromise even if an attacker has account information.

03. **Separation of Duties:**
Personnel with privileged access have separate accounts for privileged and daily use. These role-based accounts reduce the probability of privileged accounts being compromised through excessive use.

04. **Azure Ingress Controls:**
Despite our modifications of security rules, inbound SSH connections were blocked from reaching Azure VMs. While we were eventually able to bypass these controls, the restrictions demonstrate strong defense-in-depth control.

05. **Active Directory (AD) Computer Account Creation Restrictions:**
Controls related to the creation of computer accounts prevented our consultants from leveraging compromised user accounts to create new computer accounts.

06. **AD Certificate Services (AD CS) Vulnerability Remediation:**
We observed that an AD CS vulnerability uncovered during a previous penetration test had since been remediated.

Observed Vulnerabilities:

01. **MFA Deficiencies:**
Despite being required for VPN access, MFA was not found to be required for external logins; protection was limited to Microsoft 365, leaving other Internet-facing services, including those handling sensitive data, without MFA defenses.

02. **Help Desk Security Practice Deficiencies:**
The help desk lacked verification procedures, password reset policies, and post-reset password management, allowing our consultants to socially engineer help desk staff into performing resets of passwords and MFA devices for targeted employee accounts. In addition, the use of common passwords as part of the reset process allowed our red team to compromise many employee accounts via password spraying attacks.

03. **Azure Security Monitoring and Alerting:**
We identified deficiencies within Azure security monitoring and alerting mechanisms, allowing us to perform unauthorized user additions and modifications within Azure without detection. This lack of monitoring and alerting indicates substantial gaps in the organization's ability to detect and respond to potential threats within the Azure environment.

04. **Security Awareness:**
Personnel lacked security awareness, allowing us to effectively execute caller ID spoofing to facilitate password and MFA device resets for impersonated employees. Targeted IT administrators were consequently deceived into clicking malicious links from a compromised HR administrator's account, resulting in the submission of credentials to a phishing site and indicating an urgent need for security awareness training.

05. **Sensitive Data Privacy Concerns:**
We discovered critical exposures of PII and PHI on Internet-facing platforms not protected by MFA and in email communications, posing a significant threat to privacy, data security, and potentially regulatory compliance.

06. **Excessive Azure Privileges:**
We identified a lapse in the organization's approach to Azure access control wherein standard user accounts were found to be provisioned with elevated privileges, which deviates from the principle of least privilege (PoLP), in which users and applications should only have access to the data and resources they need to do their jobs.

07. **Network Access Controls (NAC):**
Due to a lack of NAC, our consultants connected an unauthorized device to the internal network and obtained an internal IP address via Dynamic Host Configuration Protocol (DHCP).

08. **Wireless Network Attacks:**
We determined that the organization's wireless infrastructure is susceptible to unauthorized access points mimicking legitimate service set identifiers (SSIDs), and these remained operational over several days without detection. Coupled with our exploitation of the GTC downgrade attack technique against mobile devices on the network, we gained an initial foothold during this assessment through cleartext credentials submitted to our evil twin access point.

Preparation

Having a Run at the Physical and Networked Environments

Our initial conversations with our client established the types of attacks we would execute and what the goals for the assessment would be. This red team assessment was intended to help the organization prepare for a situation in which they would be handling more critical data than usual, so it was important to conduct attacks that would help them get the most out of the assessment.

The series of attacks we executed during the red team assessment considered different types of vulnerabilities and what a threat actor might do in different attack scenarios:

- Physical penetration testing
- Wireless network attacks
- Email and voice phishing
- Exploiting Microsoft Azure and internal network vulnerabilities

We established three objectives with our client for the red team assessment, all to be attempted without detection:

1. Gain access to a specific type of confidential report
2. Gain access to PHI and/or PII for the organization's members
3. Compromise administrator accounts

DirectDefense consultants leveraged advanced social engineering tactics, technical exploitation, and thorough reconnaissance to gain access to sensitive data and critical systems.

The series of attacks we executed during the red team assessment considered different types of vulnerabilities and what a threat actor might do in different attack scenarios.

Execution

Identifying the Biggest Threats to Sensitive Data

Because of the nature of this organization's business, our access for the physical breach was limited; their team simulated what would happen if someone tried to break into the facility and place a device on the internal network.

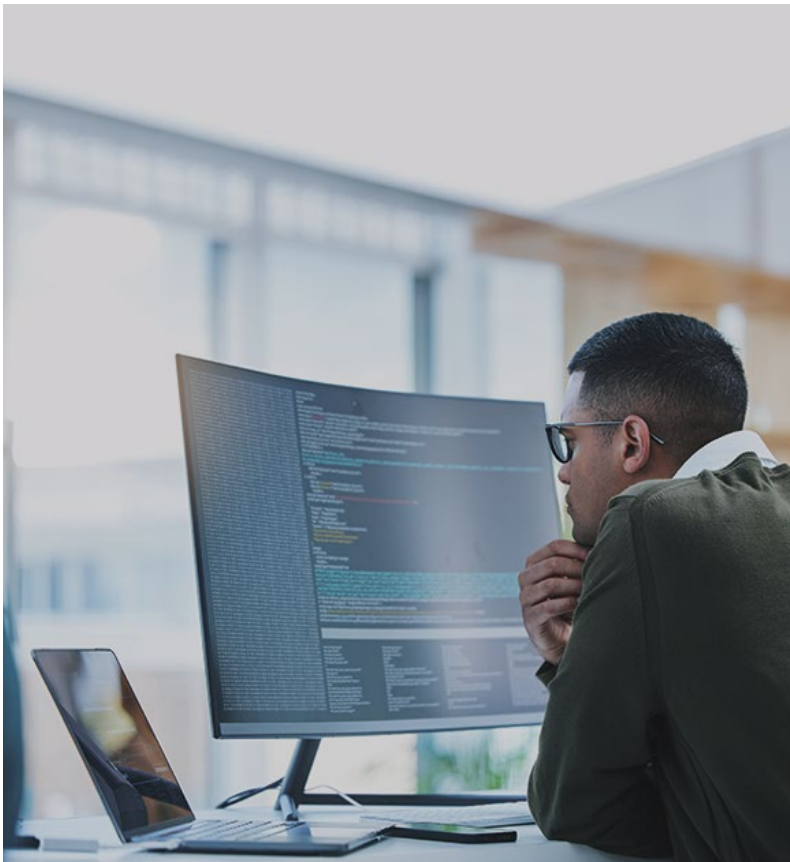
While our device was recognized almost immediately, demonstrating strong physical security, the other types of access we gained into the networked environment raised security concerns.

MFA Can't Be Selective

While MFA was enforced for VPN access, which is highly recommended given today's widespread remote work environment, it was not enforced for many internal and Internet-facing applications. This lack of MFA was one of our top concerns as it demonstrates incomplete application coverage for a range of users, including privileged users.

We gained access to several applications using stolen usernames and passwords, which gave us access to highly sensitive data.

We also easily accessed the organization's Azure environment and performed undetected attacks. Many organizations face a similar challenge where their on-prem network is secure but cloud environments like Azure aren't set up with the same precautions and have security vulnerabilities.



Getting a Little Too Much Help from the Help Desk

Another top concern for the organization's security posture was the lack of security training and awareness at its help desk. Once we had accessed several user accounts through other means, we attempted to escalate privileges through social engineering tactics.

Attackers frequently use social engineering tactics to expand their access once they have gained a foothold in an organization, and we mimicked these tactics by calling the help desk using spoofed numbers. Because the help desk relies on caller ID, we convinced help desk personnel to reset passwords for two accounts, granting our consultants access to administrator controls.

We have significantly higher success when spoofing caller ID because you can show up on the ID as any employee, adding credibility to the request and lowering the level of skepticism that the request is legitimate. We recommend help desk personnel do a call back to a known number on file, request a video call, or utilize an app-based MFA challenge that the user must respond to during the call. Relying on caller ID or security questions aren't reliable security measures.

For this red team assessment, we leveraged a lot of new attack tactics to ensure we were mimicking what an attacker would really be doing to gain access to this critical data. Our approach is never "cookie cutter" – we continually learn what real adversaries are doing today and learn quickly so we can be flexible rather than relying on a single or dated approach.

Maintenance

Relying on the "Same Old" Testing Approach is Risky Business

Continued security testing is a must – but more than that, it's important to improve the assessments year after year. If your organization is performing the exact same testing and assessments each year, you'll get to a point where the reporting looks solid but your organization will be vulnerable to the different tactics and threat models that are always developing.

You should be doing continuous and evolving testing to make sure you're addressing new vulnerabilities and new attack behaviors.

Key Achievements & Takeaways

Our expertise in "being the attacker" ensured we could really put our client's networked environment to a real-world test based on the attack vectors and tactics bad actors are using today.

For this organization, our MSSP partnership enabled our recommendation for a red team assessment at the perfect time to enhance their security posture. This kind of involved partnership puts DirectDefense and our clients in the ideal position to stay on top of threats with the most current and sophisticated testing.

As a result of our red team assessment, we helped our client:

- Improve its security posture ahead of a situation that would have put their critical data at greater risk of a breach
- Identify gaps within its security posture despite having tight security in certain areas
- Understand the best next steps to close security gaps and eliminate vulnerabilities
- Refine their security training and awareness for a complete approach to security

DirectDefense information security and managed services experts bring years of industry experience to our clients and we deliver solutions that are critical for companies of all sizes and in multiple industries.

Contact Us Today!

If your organization is looking for MSSP services, or if you want a routine security assessment, we're ready to help.
Visit directdefense.com or call 1 888 720 4633.