pellera

Red Team Report

2025 Penetration Testing Findings & 2026 Strategies

Pellera
Red Team Report

2025 Penetration Testing Findings & 2026 Strategies

CONTENTS

Prepared by: Pellera Cybersecurity Practice
pellera.com | 866.910.4425

INTRODUCTION

Threat actors don't rely on sophisticated exploits—they exploit opportunity. **Analysis from hundreds of real-world penetration tests** conducted by Pellera's Red Team in 2025 shows attackers continue to succeed through familiar weaknesses: compromised credentials, identity misconfigurations, and insecure default configurations. Despite increased investment in security controls, many organizations still struggle with these foundational risks.

The Pellera 2025 Red Team Report aggregates insights from more than 250 penetration tests across 150+ organizations, revealing trends that extend beyond individual assessments. **This data-driven analysis highlights the attack paths, technologies, and misconfigurations adversaries** most frequently abuse to gain initial access and escalate privileges.

As organizations harden traditional defenses, attackers adapt—pivoting toward identity infrastructure, internal authentication protocols, management platforms, and, increasingly, AI-enabled systems. Pellera's Red Team continuously mirrors this evolving threat behavior to identify weaknesses before they are exploited.

This report provides security leaders with clear insight into how modern attacks unfold, where defenses repeatedly fail, and why continuous, adversary-informed testing is essential. In an evolving threat landscape, regularly validating security posture against real attacker tactics is critical to reducing risk and improving resilience.

METHODOLOGY

This report is an analysis of the combined penetration testing results and statistics of the assessments that Pellera's 25+ penetration testers performed throughout 2025, leveraging data mined from the output of all these engagements. A key differentiator for our Penetration Testing practice is our people, their attention to detail, and their commitment to consistently performing thorough penetration tests. Pellera's consultants are all highly certified, possess a broad and deep level of knowledge in their craft, and continuously collaborate to improve each other, the team, and Pellera's service offerings.

The Pellera Red Team continuously reviews the tools, tactics, and techniques leveraged by real-world malicious actors, allowing Pellera to replicate those attack capabilities into our processes. Pellera's Red Team takes a comprehensive hacker mentality to identify our clients' weaknesses before they can be exploited by malicious adversaries. This dedication uncovers impactful findings that provide strong data points to use in this analysis.

150+
Clients

~250
Penetration Tests

~20,000
Vulnerabilities

~20,000
Assets

EXECUTIVE SUMMARY

The more things change, the more they stay the same. Credentials continue to be key targets of attack in a threat actor's attempt to obtain initial access. Organizations cannot simply rely on a Next-Generation Firewall and multi-factor authentication (MFA) at the perimeter. A strong identity and access management (IAM) program must be combined with just-in-time access, privileged access management solutions, password managers, stronger forms of authentication, segmentation between system components, and internal MFA to critical systems and jump boxes.

A review of the test cases and exploitable vulnerabilities that the Pellera Red Team most commonly abused illustrates how much organizations continue to struggle with the basics when it comes to good information security hygiene.

Top Test Cases

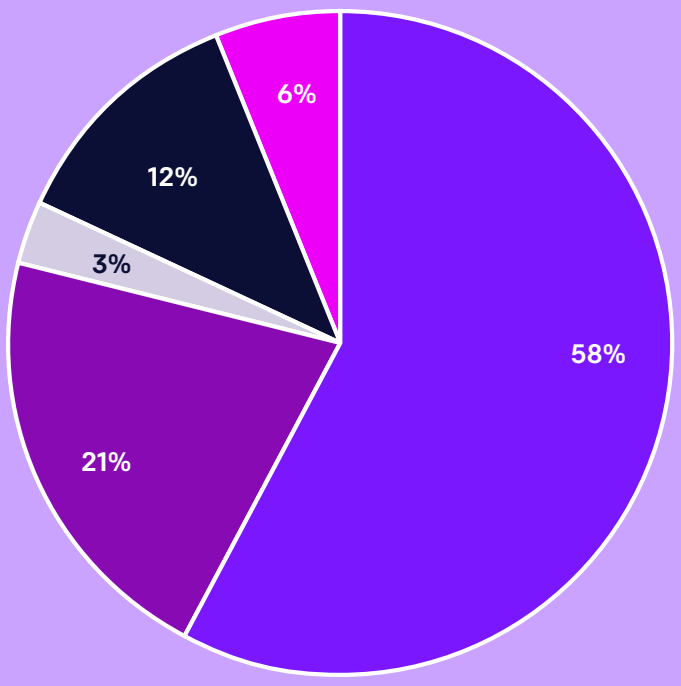
Pellera penetration testers found the most success in abusing these test cases to further their objectives:

1. Use of default credentials
2. Access and authorization bypass issues in applications
3. Weak or missing computer account passwords
4. Abuse of default Windows legacy network protocols and settings that enable poisoning and credential theft
5. Insecure or incorrect implementation of IPv6 traffic routing that enables poisoning and credential theft
6. Active Directory Certificate Services (ADCS) misconfigurations that enable privilege escalation
7. Use of weak and predictable passwords
8. Kerberoasting
9. System Center Configuration Manager (SCCM) and System Center Operations Manager misconfigurations that enable privilege escalation
10. Injection attacks in applications

Key Vulnerability Statistics

Top 10 Exploitable Vulnerabilities

1. SMB signing not required
2. Local administrator credential reuse
3. LDAP signing and channel binding not required
4. IPMI v2.0 password hash disclosure
5. Multicast name resolution poisoning
6. Default credentials
7. Kerberoasting
8. Service account credentials stored in plaintext
9. Computer accounts with weak or no password (Pre2k)
10. Cisco Smart Install Detection



Frequency of Vulnerability Classes

- Misconfiguration
- Patching
- Credential Abuse
- Unsupported Software
- Insecure Code

TRENDS BEYOND THE STATISTICS

While the top attack techniques and exploited vulnerabilities are relevant and useful metrics, trending attacker behavior, targets of opportunity, and applications of technology often provide a more complete picture of what organizations should focus on in terms of defensive security posture.

The trends that Pellera has observed are an outcome of defenders hardening their networks as a direct result of findings from regular penetration tests, forcing threat actors to change their tools, targets, and/or techniques to continue to be successful.

In addition, other observed trends are due to advances in technology that are being leveraged by defenders and attackers alike to attack and defend corporate environments.

To combat these trends and changes in the attack surface landscape, organizations are increasingly incorporating regular penetration testing and security assessments throughout the year, targeting application-layer, network-layer, people-layer, and physical-layer risks. The growth of the Cybersecurity-as-a-Service (CYSaaS) model that enables clients to perform testing and assessments on an as-needed basis throughout the year has compounded over time to meet this need. Pellera's CYSaaS model supports our clients' need to regularly assess their environments for threats and vulnerabilities in a cost-effective manner.

NTLM Reflection / Relay

Relay attacks against Windows-based systems leveraging New Technology LAN Manager (NTLM) for authentication have been successfully abused by attackers and penetration testers alike for a long time. However, the number of Microsoft Windows-based products for which adversaries target with relay attacks has expanded significantly since this vector of attack became popular. Internal attack surfaces have often been hardened against relaying to SMB services using configurations that require signing of the communications. This has forced malicious adversaries to pivot to targeting the Lightweight Directory Access Protocol (LDAP) on Active Directory (AD), Hypertext Transfer Protocol (HTTP) on endpoints such as ADCS and Internet Information Services (IIS), as well as Microsoft SQL SERVER (MSSQL) services. The number of services that are vulnerable to relay attacks has grown. In addition, there has been an increase in coercion-based vulnerabilities and techniques that enable a threat actor to force an authentication request that can then be relayed to these services. This has provided a rich internal attack surface for an attacker to obtain an initial foothold in an environment as well as escalating privileges.

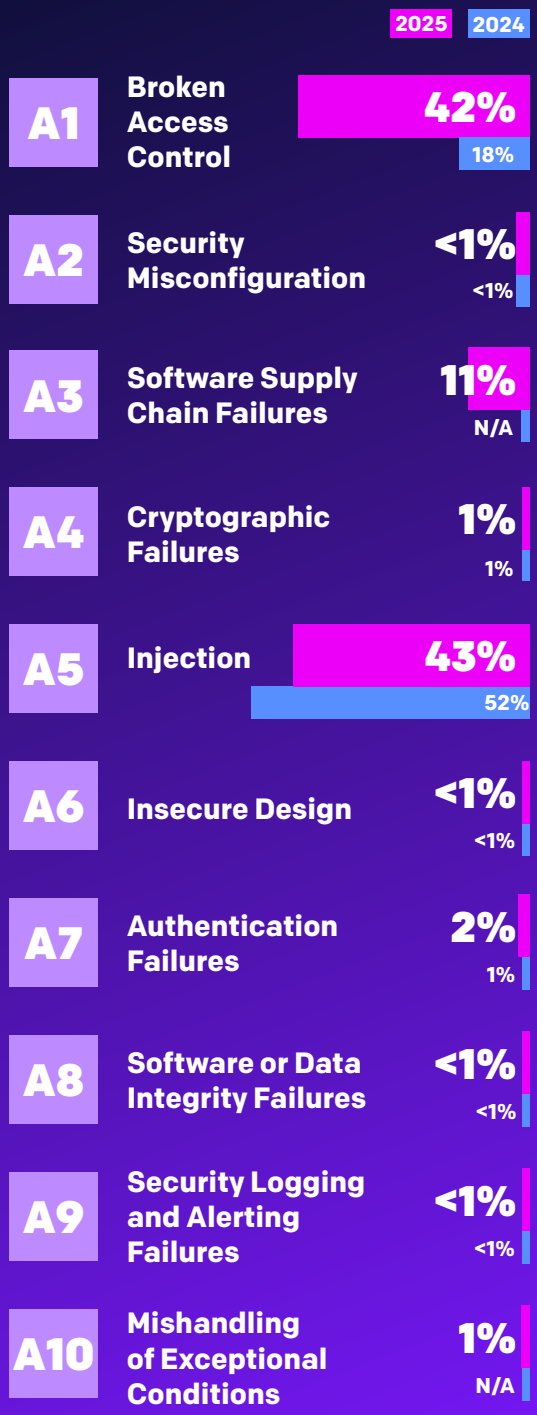
AD is often the target for relay attacks by malicious adversaries; however, AD's susceptibility to misconfigurations has resulted in an increase in privilege escalation vectors of attacks that are frequently targeted.

Active Directory (AD)

AD continues to be a common target of attack for misconfigurations that can lead to privilege escalation and full domain compromise. This is particularly true for Pellera's net-new penetration testing clients as well as organizations that are new to penetration testing in general. A wide variety of AD misconfigurations are common, but the most frequent paths to achieving adversarial goals tend to be:

- ADCS misconfigurations in newer client environments (known as the ESC class of attack techniques), enabling standard user accounts to escalate to domain administrator privileges

OWASP Top 10 Correlation



- Service accounts with associated Service Principal Names (SPN) and weak passwords are another common source of privilege escalation (Kerberoasting)
- Overprivileged accounts, overprivileged groups, and misconfigured AD access control lists (ACLs) often lead to privilege escalation
- Clear-text passwords in Group Policy Preference files and in description fields for user accounts

For clients in which Pellera's Red Team has performed penetration testing over the course of several years, it has been observed that these clients typically have more hardened AD configurations. For these organizations, another growing point of attack is Microsoft's Configuration Manager and Operations Manager products.

System Center Configuration Manager (SCCM, now Microsoft Configuration Manager (MCM)) & System Center Operations Manager (SCOM)

AD misconfigurations have become less prevalent over time for proactive organizations that perform routine, comprehensive, and thorough internal penetration tests. These improvements have led to offensive security professionals and malicious adversaries alike identifying new targets of opportunity. Microsoft's suite of management software has thus become a newer focus of attack. Like AD, SCCM / MCM / SCOM frequently provide a quick source of privilege escalation for environments in which they are insecurely deployed. Research is ongoing, and additional attack techniques will likely be identified, but the key misconfigurations that are commonly abused to achieve malicious objectives include:

- Preboot Execution Environment (PXE) misconfigurations and weak or missing passwords that enable access to the cleartext Network Access Account (NAA) credentials, combined with overprivileged access for the NAA account
- SCCM policy misconfigurations that enable automatic device registration and/or approval, which can be abused to escalate privileges
- Weak protocol configurations that enable coercion of an authentication request from the SCCM site server that is then relayed to the SCCM MSSQL database server to achieve privilege escalation

Artificial Intelligence (AI)

Surprising absolutely no one, AI usage to automate, enhance, and scale adversarial attack techniques has proliferated. Consulting agencies and malicious adversaries are leveraging AI to more efficiently enumerate and penetrate target networks and applications, as demonstrated by tools such as XBOW.

These tools are being used to augment, not replace, the human element, speeding up the pace of vulnerability identification and exploitation. The human element is still an essential component of a thorough penetration test, as reasoning through chains of attack, identifying logic flaws, and ensuring assessments stay within tightly-scoped parameters are capabilities where AI falls short. However, AI tools can enable human testers to more efficiently assess an environment. The acceleration of the capabilities of these tools will continue into the near future, enabling more efficient and thorough coverage of attack surface.

Another application of AI that is trending is voice cloning for malicious purposes. The technology is at a state in which open-source intelligence gathering (OSINT) to identify target audio on the web can be used to quickly clone a target employee's voice at a selected company and leverage that voice in vishing-based attacks against company personnel. The voice can be cloned and used in real-time to impersonate an employee over the phone. Pellera has expanded its social engineering services to include this capability, to better stress test our client's awareness training and phone-based security controls.

In addition, organizations continue to adopt and

implement AI technology into their own applications. This has increased the need for application penetration tests that target not only the attack surface of a typical application but include test cases specifically around AI related vulnerabilities. Pellera has developed a comprehensive approach around this need, combining comprehensive application penetration testing with consultative guidance from AI experts in architecture, design, and DevSecOps to provide an assessment outcome that identifies vulnerabilities at the application, design, architecture, and governance levels.

KEY TAKEAWAYS

Attackers continue to take the path of least resistance to achieve their objectives, illustrating that organizations still struggle with the basics when it comes to protecting credentials and configuring systems securely. Organizations should leverage the outcome of regular assessments to identify strategic solutions to more comprehensively address risk. Emerging technologies, such as passwordless authentication solutions, as well as more modern authentication protocols, should be evaluated for replacing existing services and protocols to more effectively protect credentials. Organizations should put greater emphasis and focus on IAM products and processes that can further reduce the risk to credentials and stolen identities.

Attackers Adapt Their Techniques

Attackers change tactics, techniques, and targets as the security of organizations improves, highlighting the need for more frequent testing to identify new targets of opportunity that represent risk. Previous technologies that have been ripe for exploitation are slowly hardened as organizations improve their security posture through regular testing. Pellera's Red Team has observed that the security posture of our clients improves over time against common threats and vulnerabilities, but that new paths to abuse pop up to replace the old techniques, creating avenues for threat actors to exploit.

New research routinely identifies systems prone to misconfigurations, which threat actors quickly pivot to explot. Regular testing reduces the time between vulnerability identification and remediation, enabling defenders to further harden their environments early and often. A continuous process of assessment and remediation shortens the window available to threat actors to exploit these targets of opportunity to achieve their objectives.

AI Continues To Dominate The Headlines

AI continues to be leveraged to augment human capabilities to more efficiently achieve outcomes. The technology is being implemented by threat actors and defenders alike to facilitate identification of vulnerabilities and bypassing security controls, as well as enable identification of potentially malicious behavior. Consulting organizations will need to embrace the technology in a responsible and ethical way to better enable their consultants to operate more effectively and efficiently. Additionally, consulting services will need to continue to evolve to include AI use cases within offensive security services. This adoption will identify areas of opportunity for clients to improve their resilience to attacks leveraging AI technologies, as well as potential use cases for defenders to implement AI for defensive purposes.

AI is also being adopted within custom applications at a rapid pace across all industry verticals, further increasing the attack surface of modern-day applications. Organizations will need to expand their application security programs to include evaluations of the design and architecture of AI-based systems, as well as assessments to identify AI-related vulnerabilities in applications prior to production rollout.

Top Five Actions to Do Now

1. Increase focus on identities and credentials, as these are the low-hanging fruit targets that threat actors take advantage of to achieve their objectives. Research passwordless authentication services, phishing-resistant MFA solutions, privileged access management (PAM) software, risk-based authentication features, behavioral authentication features augmented with AI, and processes such as just-in-time access to reduce the risk of a compromised credential.

2. Incorporate a continuous assessment approach into change management and secure development lifecycle processes to reduce the window of opportunity that malicious adversaries have to exploit vulnerabilities. The threat landscape evolves quickly and requires more frequent testing to ensure organizations can adequately respond to new threats.

3. As security programs improve, they need to evolve to address gaps in defenses. Organizations need to adapt their assessment programs to perform continuous penetration testing as a best practice, in addition to increasing their focus on the ability to detect and respond to common attack techniques as their security maturity improves. As well, organizations should enhance assessment programs to include testing for specific types of threats, such as ransomware threat actor groups, to identify gaps in defenses necessary to deter, prevent, and respond to these risks. Regular penetration tests help to significantly reduce vulnerabilities in patch management, configuration management, and credential management over time, but their value by themselves diminishes over time as organizations address identified threats and vulnerabilities. This can be addressed through layering on more advanced services with penetration testing, such as Purple Teaming and Ransomware Readiness Assessments.

4. Implement AI technologies to augment existing defensive capabilities. Perform social engineering assessments enhanced with AI to ensure security awareness training programs adequately address the risks of these attacks.

5. Update secure development lifecycle programs to include testing of AI-based use cases in all penetration tests of custom applications that leverage AI.

20%-30%
Savings Over Single Tests

84 NPS
Client Satisfaction Score

100%
Human Tested & Validated

100%
US-Based Testers Employed by Pellera

30
Certified Experts

15
Top-Secret Clearance

The Flexibility You Need for Cybersecurity Priorities That Can Change Overnight

Budgeting, staffing, and tooling for unknown needs make security complex. That's why our Security as a Service (SECaaS) uses a customized approach to provide consultation, solutions, and services that meet your varying security objectives with a single budget approval.

Your SECaaS team is US-based, with certified, specialized skills and up-to-date knowledge of leading technologies. Our proactive threat detection and response, data security, and compliance approach frees your team for other projects. The result is greater precision for your cybersecurity initiatives and an improved ROI.

Pellera SECaaS includes a wide range of cybersecurity services. You choose the ones you want, and only pay for the ones you choose. Budget protection is built in, with each service discounted **20 - 35%** off the cost of a single engagement.

One Budget Approval, Numerous Solutions

Customizable & Scaleable

Always Up-To-Date Expertise & Technologies

Keep your security options open and expand your purchasing power with Pellera SECaaS

Top-Level Certifications

AUTHOR

Josh Berry

Director of Advanced Testing & Governance, Risk & Compliance

josh.berry@pellera.com