Executive Summary

As of the termination of penetration testing activities, our investigation discovered 21 vulnerabilities of variable severity. We exploited 7 different hosts on 10 different ports, and discovered login credentials for multiple user accounts. Existing security measures were present, and often delayed the achievement of penetration testing goals, however all goals stated in the proposed objectives were ultimately achieved. The vulnerability summary below is organized by severity and will cover responsible disclosure of the vulnerabilities we found and the exploits leveraged against them. The executive summary will cover the broad strokes of our findings and will organize findings by target type (Web App, Linux host, Windows host).

The web application was the first target and was attacked on 05/20/2024. The web application contained 4 critical vulnerabilities, 3 high risk vulnerabilities, and 2 medium risk vulnerabilities. The web application can be summarized as needing to employ user-input sanitization across the board. Multiple vulnerabilities were exploited by inserting code that was not the intended usage at various inputs on different pages on the Total Rekall site. Rekall would also drastically improve their defense posture by implementing and enforcing a user password policy that requires unique and long passwords.

Multiple Linux machines were targeted and exploited on 05/22/2024. There were 3 critical vulnerabilities, 3 high risk vulnerabilities, and 1 medium risk vulnerability exploited on Linux machines. Broadly speaking, the Linux environment at Rekall is in need of software updates. Every critical vulnerability we discovered relied on exploits that have already been patched; furthermore, each of these exploits can be leveraged by novice hackers using the free and open-source Metasploit framework. All three of the high risk vulnerabilities pertain to poor file permissions/access controls and could be remediated by deploying Role Based Access Controls (RBAC) to categorize users and files based on the needs of the organization and user type. A password policy would also improve the defense posture of the Linux environment.

The Windows environment was attacked on 05/23/2024. We discovered 1 critical vulnerability, 1 high risk vulnerability, 1 medium risk vulnerability, and 2 low risk vulnerabilities. It should be noted that we only compromised one Windows machine, however we discovered a great deal of information regarding system info and username/password combinations that may have lead to further workstation compromise if that were in-scope. The critical vulnerability and the medium risk vulnerability can both be remediated by installing OS updates (and continuing to do so in the future). The high risk vulnerability and one of the low risk vulnerabilities are a product of poor access control policy and missing firewall rules. The other low risk vulnerability can be remediated by improving access controls and obfuscating certain administrative functions like task scheduling.

In summary, the Rekall corporation penetration test achieved all assessment objectives and has yielded 21 remediation recommendations. The White Hat Group would like to commend Rekall Corporation on their decision to seek out proactive penetration testing and would like to extend an offer to provide a follow up assessment at the leisure of Rekall Corporation.