Redpoint CYBERSECURITY

USE CASE

PENETRATION TEST

THE CHALLENGE:

A global organization faced a large- scale ransomware attack. We provided emergency response coupled with remediation and rebuild services. Following the rebuild we performed a penetration test (pentest) to identify vulnerabilities on the network. We found that the network was severely vulnerable to additional attacks:

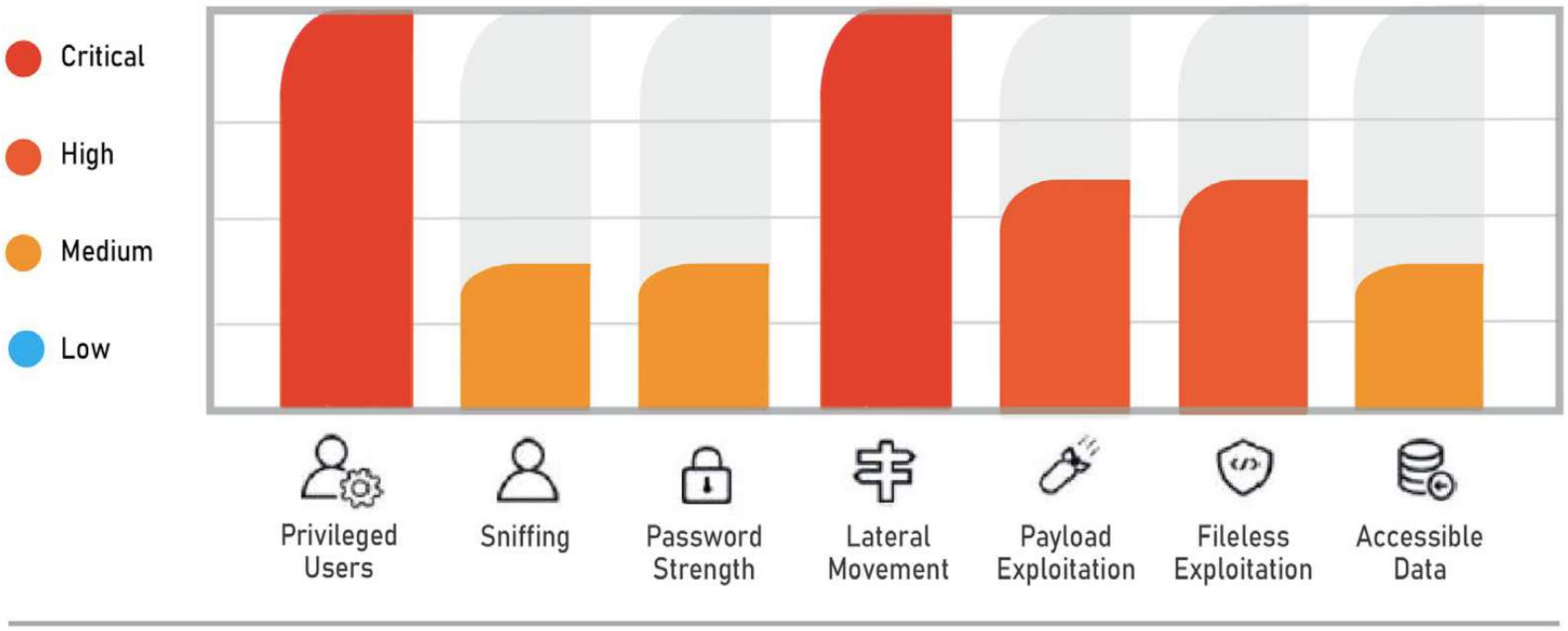
- The client had 5 hosts vulnerable to Blue Keep, allowing us to quickly exploit the network
- The client purchased antivirus (AV) software; however, we were able to successfully bypass their AV and download 62 malicious files
- The client did not enforce strong password policy or patch legacy systems allowing us to crack passwords and elevate privileges to Domain Admin, effectively taking ownership of the entire network.

TOOLS & TECHNIQUES:

Software Pentest:

- Extremely fast and thorough
- Continuously testing and identifying vulnerabilities and exploits not found by a human ethical hacker
- Tested 196 endpoints with over 12,757 exploits leveraged against the network in under 36 hours
- MITRE ATT&CK: The pentest follows the MITRE ATT&CK Matrix, exploiting the network to the fullest extent possible to mimic a malicious actor.

Resilience Score Card



422
Vulnerabilities

85 Critical	15 High	23 Medium	299 Low

OUTCOMES:

- Rapid identification of 422 vulnerabilities along with remediation for the top 10 most critical vulnerabilities.
- An in-depth report highlighting vulnerabilities and attack vectors and providing insight to support a holistic cyber security approach
- Implementation of new policies and procedures, enforcing least privilege and applying stronger password policy
- Leadership across the organization now has a better understanding of cyber security and how to better secure their network from future attacks.

Redpoint CYBERSECURITY

Book a Free Consultation

888 523 2604

redpointcyber.com