PRAETORIAN

WHITE PAPER

How to Dramatically Improve Corporate IT Security Without Spending Millions

Focus on 5 key data-driven strategies for information security success

INSIDE THIS REPORT

Based on 100+ internal penetration test engagements

INTRODUCTION

The IT Security Community is Noisy. Focus is Critical.

Narrow your focus, concentrating on the most important elements, and leave the rest for later. We want to reduce the noise to help organizations focus on what is important based on data, not our opinions.

This research presents a list of vectors commonly used by attackers to compromise internal networks after achieving initial access. It delivers recommendations on how to best address the issues. The goal is to help defenders focus efforts on the most important issues by understanding the attacker's playbook, and thereby maximize results.

As a security services organization, we simulate high-impact network and application security breaches to help organizations understand real security risks in their environments. The goal is for the organization to use our findings and recommendations to prevent future breaches.

75

UNIQUE ORGANIZATIONS INVOLVED IN THE STUDY

100

INTERNAL PENETRATION TEST REPORTS ANALYZED

450

ATTACK VECTOR INSTANCES IDENTIFIED AND EXPLOITED

2021 UPDATE

New Trends from Recent Engagements

In 2016 Praetorian published a report detailing the top five attacks used to compromise clients during security assessments. Almost all of the data and information contained therein is still fully valid five years later. This addendum addresses the updates and new trends we have seen since initial publication.

Sampling our most recent 21 assessments across enterprise to SMB clients including retail, technology, financial, manufacturing, and philanthropy sectors, we analyzed the results in a similar fashion to the original analysis.

Attack	2016 %	2021 %
Weak Domain User Passwords	66%	67%
Broadcast Name Resolution Poisoning	64%	29%
Local Administrator Attacks	61%	48%
Cleartext Passwords in Memory	59%	48%
Insufficient Network Access Controls	52%	76%

> **Key Insight:** Weak domain user passwords remain valid in 2/3 of assessments but has lost the top spot to insufficient network access controls, which has shot up due to the rapid move of on-premises services to cloud platforms. At the intersection of poor network access controls and weak passwords is multi-factor authentication (MFA). Lack of MFA is the single most impactful issue.

ANALYSIS

Summary of Results

The data set includes 100 separate internal penetration test engagements spanning 75 unique organizations. The top four attack vectors are based on utilizing stolen credentials. This is a serious problem because credential theft will always work as long as the credentials are valid.

97%
HAD TWO OR MORE ROOT-CAUSE FINDINGS

82%
HAD THREE OR MORE ROOT-CAUSE FINDINGS

4.47
AVERAGE NUMBER OF ROOT-CAUSE FINDINGS PER ENGAGEMENT

The five identified issues are "root causes" of a compromise, which we define as security weaknesses that were used to achieve a network compromise or engagement objective, such as access to sensitive information.

> **The average internal engagement length was ONE WEEK. 0 of the top 5 internal attack vectors required exploitation of unpatched software.**

METHODOLOGY

Hacking Without Exploits

Many organizations use vulnerability scanning software to identify weaknesses in their environment. This is an important element of a security program; however, organizations can become fixated on these issues at the expense of elements of risk that are often more important.

The fixation on patch management is compounded by professional service firms who equate a penetration test to little more than running a vulnerability scan. As a refresher and reminder, the goal of a penetration test is to showcase the same standard operating procedures of an actual attacker.

> *"[With] any large network, I will tell you that persistence and focus will get you in, will achieve that exploitation without the zero days. There's so many more vectors that are easier, less risky and quite often more productive than going down that route."*
>
> *— Rob Joyce, Chief, Tailored Access Operations, NSA*

A vulnerability scanner can identify significant weaknesses, but it can lead to a focus on symptoms over identifying core issues. Having a list of 100,000 vulnerabilities probably won't mean anything to a CISO unless all of these weaknesses would cause a going-out-of-business event.

> **It is important to note that none of the top internal attack vectors were based on a missing security patch; rather, they are weaknesses in the design of the environment.**

ATTACK VECTORS

66%

Attack One: Weak Domain User Passwords

Out of 100 internal pentests, weak domain user passwords were used to compromise the environment 66% of the time.

Most corporate environments use Microsoft's Active Directory to manage employee accounts. One problem is that Active Directory does not allow for comprehensive password complexity requirements. Passwords like "Password1!" and "Summer2016" are acceptable unless third-party software is used.

Recommendations

- Increase Active Directory password requirements to at least 15 characters
- Implement two-factor authentication for all administrative and remote access
- Implement an enterprise-grade password manager for employees
- Educate users on using "passphrases" instead of simple passwords

64%

Attack Two: Broadcast Name Resolution Poisoning (WPAD)

Out of 100 internal pentests, BNRP was used to compromise the environment 64% of the time.

This attack can be used when an attacker is on the corporate network. The attacker configures their system to respond to broadcast requests such as LLMNR, NetBIOS, or mDNS. When a user tries to access network resources, their credentials can be transmitted to the attacker's system.

ATTACK VECTORS

61%

Attack Three: Local Administrator Attacks (Pass-the-Hash)

Out of 100 internal pentests, Pass-the-Hash was used to compromise the environment 61% of the time.

Organizations often configure all systems with the same Local Admin password. If an attacker compromises the LM/NT hash, they can use the hash to authenticate and execute commands on other systems with the same password. The attacker doesn't need to crack the password at all.

Recommendations

- Deploy Microsoft LAPS (Local Administrator Password Solution) for all workstations and servers
- Implement defense-in-depth strategies from Microsoft's Pass-the-Hash whitepaper
- Remove local administrator privileges for most users

59%

Attack Four: Cleartext Passwords Found in Memory (Mimikatz)

Out of 100 internal pentests, cleartext passwords in memory were used to compromise the environment 59% of the time.

Modern Windows versions store domain credentials in cleartext within memory of the LSASS process. An attacker with Local Admin or SYSTEM-level access can extract these credentials using tools like Mimikatz.

Recommendations

- Install Microsoft Security Advisory 2871997
- Implement registry change: UseLogonCredential: Value 0 (REG_DWORD)
- Use Protected Users Group in Active Directory

ATTACK VECTORS

52%

Attack Five: Insufficient Network Filtering

Out of 100 internal pentests, insufficient network filtering was used to compromise the environment 52% of the time.

Lateral movement throughout the environment can only be achieved if network-level access to systems is not properly restricted. Most organizations do not have tight access control lists that restrict access based on business requirements. After a single system is compromised, an attacker can use this access to directly communicate with critical systems.

Recommendations

- Review all critical systems and the data that resides in them
- Gather feedback from business owners regarding access requirements
- Enforce network ACLs so only authorized systems have access to critical systems
- Consider using jump boxes with MFA for accessing critical server VLANs

> **You don't need AI, machine learning, or blockchain. You need hygiene, administrative tools, and strong processes and standards.** These things will significantly improve your security, all without having to buy the latest wares.

Ready to Improve Your Security?

Partner with Praetorian to assess your security posture and implement effective defenses.

Contact Us