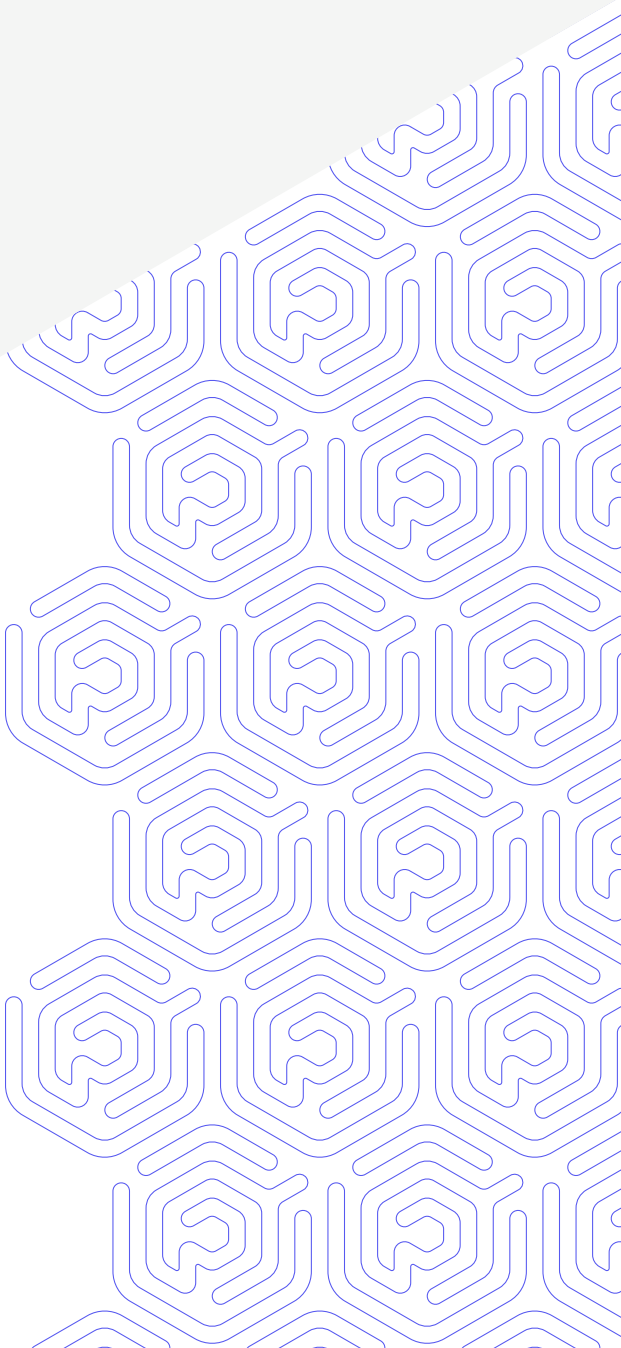
WHITE PAPER

How to Dramatically Improve Corporate IT Security without Spending Millions



praetorian

In 2016 Praetorian published a report detailing the top five attacks that we use to compromise clients during our security assessments. If you have not read that report, it is provided in the second part of this report, and we highly suggest starting there as almost all of the data and information contained therein is still fully valid five years later. Additionally, the attacks and their remediations are discussed in more detail there. This addendum will address only the updates and new trends we have seen since initial publication.

→

21 recent engagements ranging from enterprise to SMB clients including retail, technology, financial, manufacturing, and philanthropy sectors.

Sampling our most recent 21 assessments, we analyzed the results in a similar fashion to the original analysis. The summary of results below shows an interesting dynamic.

Attack	2016 Percent of Engagements	2021 Percent of Engagements
Weak Domain User Passwords	66%	67%
Broadcast Name Resolution Poisoning (BNRP)	64%	29%
Local Administrator Attacks (aka Pass-the-Hash)	61%	48%
Cleartext Passwords Found in Memory	59%	48%
Insufficient Network Access Controls	52%	76%

Weak domain user passwords remain a valid attack in 2/3 of our assessments but has lost the top spot to insufficient network access controls, which has shot up in the intervening years. This spike in insufficient network access controls stems largely from the rapid move of on-premises services (email, file storage, HRIS, etc.) to PaaS and SaaS platforms hosted externally in the cloud. With services exposed, the attack surface has grown dramatically. At the intersection of poor network access controls and weak user passwords is multi-factor authentication (MFA). Lack of MFA is the single most impactful issue that has driven these two attacks to the top of the prevalence list.

On a good note, we have seen a dramatic decrease in the instances where BNRP was a successful attack. As networks move further away from legacy systems (perhaps due to shifts to the cloud) the prevalence of the legacy protocols required to execute a BNRP attack has decreased. Not to be outdone, new attack paths in a similar vein have joined the fray. Both IPv6 poisoning attacks and Kerberoasting are similar in nature to BNRP (capture hashes and crack offline). Factoring in these new attack paths, we see that access to credentials is still a significant problem. While there are mitigations that can be applied, strong passwords and password policies remain the most effective method to deter these types of attacks.

Small dips in prevalence of Local Administrator Attacks and Cleartext Credential in Memory indicate some progress but still point to a lack of general security hygiene that would prevent these types of attacks. Of these attacks, only one (Cleartext Passwords Found in Memory) is likely to set off alerts from endpoint security platforms and only a few platforms even do that.

> Sometimes this can be individual accounts or can be managed by SSO identity platforms such as Okta, Ping, or many others. Regardless, the growth of external logon portals means more opportunities for password spraying and credential dumping.

Weak Domain User Passwords

In 2016, we highlighted the prevalence of Active Directory-based identity platforms, and while Active Directory still maintains the top spot for networks, the move away from this network architecture is also gaining traction. With adoption of cloud, PaaS, and SaaS platforms, organizations are seeing a growing number of accounts being created for users outside (or in lieu of) Active Directory. Sometimes this can be individual accounts or can be managed by SSO identity platforms such as Okta, Ping, or many others. Regardless, the growth of external logon portals means more opportunities for password spraying and credential dumping. Attackers no longer need internal access to the network to test a large swath of accounts and passwords.

Regardless of the identity platform, the problem remains the same; accounts must be protected with strong passwords and multi-factor authentication. While a future of passwordless accounts is on the horizon with technologies such as Windows Hello, we simply are not there yet or in a place for most organizations to take advantage of these technologies.

Additional recommendations on top of what we recommended in 2016 that we have seen be successful for our clients are:

- **Adopt an SSO platform for use with identity and access management for accounts on systems managed by a third-party**
- **Ensure MFA uses strong factors (Hardware tokens or Yubikey type devices, app-based tokens, push, or biometrics). Do not use SMS or email based tokens.**
- **Implement an enterprise-grade password manager for employees and encourage use of long random passwords.**
- **Educate users on the use of "passphrases" instead of simple passwords.**

Broadcast Name Resolution Positioning

While the BNRP attack path itself has not changed much since 2016, a few key changes to the IT environment have driven the prevalence of these attacks down significantly.

- **Legacy systems are being phased out in greater numbers (the original report was only a year out from Windows Server 2003 end of life) and the newer systems do not require legacy name resolution protocols. Some newer systems also implement additional SMB protections (SMB signing) by default that prevent relay attacks.**
- **IPv6 has begun to take hold in some networks opening up a new attack path related to IPv6 poisoning of DHCP requests.**
- **Strong passwords are an effective mitigation that have begun to hamper this attack path.**

→

Check out the Praetorian Blog for for insights and research regarding Broadcast Name Resolution Poisoning and other topics :

SMB Relay

Implementing BNRP Protection

Strong passwords can help to mitigate this attack path but new "SMB Relay" style attacks are being discovered still today, so simply solving for password complexity will not solve the problem. The recommendations from 2016 still stand with full force with a few additions:

- **Enable SMB Signing wherever possible and definitely for critical servers/services to prevent relay attacks.**
- **If IPv6 is not actively being managed within the network, ensure it is disabled on all devices to prevent IPv6 poisoning attacks.**
- **If the organization has a strong threat hunting or detection/response capability, consider implementing BNRP detection. Even if all recommendations have been implemented and BNRP is no longer a threat, detection of poisoning attempts is useful to identify malicious activity.**

Local Administrator Attacks (AKA Pass the Hash)

The local administrator attack path is still alive and well, however, we did see a notable decrease in prevalence. Microsoft LAPS, our recommended mitigation for this attack, was release in mid-2015. The 5 years hence have seen broad adoption and therefore mitigation of these attacks. However, given that we still see this attack on almost half of our assessments, it is clear that not everyone has gotten the word yet.

If your organization has not yet implemented LAPS or another priviledged management solution, now is the time to do so. This should be done in conjunction with removal of local administrator privileges for most, if not all users.

If there is a strong use case for users to have local administrator access, a process should be implemented to provide time-scoped administrator credentials to users instead of providing full local administrator access.

Cleartext Passwords Found in Memory (Mimikatz)

Similar to Local Administrator Attacks, we have also seen a downward trend in the cleartext credential in memory attack path. Similar to BNRP, adoption of modern operating systems is a strong reason for this decline. However, this is still a major method used in our campaigns to escalate access and pivot throughout the network.

Some endpoint detection and response tools do a good job of detecting this attack but many still do not. Additionally, detection and alerting is a lagging indicator. By the time defenders have triaged the alert, the attacker may already be much deeper into the network. This is why prevention is key here. The WDigest recommendation from our original report is still valid, but additional protections have been implemented in modern versions of Windows.

The Protected Users Group in active directory implements additional mandatory protections to prevent credential exposure within the domain. This coupled with Mircosofts recommended Tiered approach to account management and use is an extremely strong protection against cleartext credentials ending up in memory. The following are useful resources for more information:

Microsoft - Applying the Principle of Least Privilege to User Accounts on Windows

Microsoft TechNet - Protected Users Security Group

SANS - Protecting Privileged Domain Accounts: Restricted Admin and Protected Users

Authentication Policies and Authentication Policy Silos

Implementing Least-Privilege Administrative Models

SANS Digital Forensics and Incident Response Blog | Protecting Privileged Domain Accounts: Restricted Admin and Protected Users | SANS Institute

→

Since its release in 2011, Mimikatz has had a decade's worth of use and updates and is still a primary tool in any attackers arsenal…while mitigations exist, we are still fighting against it

Source: https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/

Insufficient Network Access Controls

Going hand-in-hand with weak passwords, Insufficient Network Access Controls is one of the easiest ways for our teams to gain an initial foothold and pivot through a network. There is not much to update here from 2016, save for one aspect; network segmentation alone is not enough. When determining network classification levels and segmentation, additional protections such as MFA should also be considered. While segmentation can thwart attacks, in some cases, it just becomes an annoyance to an attacker who can pivot through the network to find appropriate ingress and egress points. As such, organizations should never consider network segmentation to be a single defensive measure and should always consider it as a part of a broader defense in depth strategy.

→

You don't need AI, machine learning, or blockchain. You need hygiene, administrative tools, and strong processes and standards.

"Without Millions" but you just Recommended a Bunch of Tools ..

Yes we did, but we intend to focus on the most high leverage preventative controls and tools rather than spending millions on detective capabilities of unknown efficacy. Protection and prevention are proactive in nature instead of reactive. As such, money spent in these areas has a much greater impact. From the original report and this update, here are the commercial tools we have recommended:

- **SSO and/or Identity Management Platform**
  Strong chance your organization already has this or has considered it
- **Password Manager**
  Generally a small cost for SIGNIFICANT improvement in password security
- **Microsoft LAPS**
  Free, but with a non-trivial implementation resource cost

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.

How to Dramatically Improve Corporate IT Security Without Spending Millions

Now enterprise IT leaders can maximize budgets and outcomes by focusing on 5 key data-driven strategies for information security success

Table of Contents

AUTHORED BY

Josh Abraham, Practice Manager, Praetorian
josh.abraham@praetorian.com

There is too much noise in the IT and security communities. Focus is critical.

75
Unique organizations involved in the study

100
Internal penetration test reports analyzed

450
Attack vectors instances identified and exploited

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.

Most organizations never see or understand a real attacker's playbook. They have assumptions of how an attack might occur, but these assumptions are often based on a lack of understanding or include many false assumptions. We decided to change this. Organizations should not need to go through a penetration test (pentest) to gain an understanding of the most common internal attack vectors used to cause a security breach.

We go on the offensive to help defenders address the most common internal attack vectors. Achieving all of our engagement objectives within minutes generally isn't sophisticated, hard, or fun for us, and it isn't cost-effective for our clients. Organizations could save time and effort if they focus on the primary attack vectors we use every day. Our top attack vectors are not new zero-day vulnerabilities. They are methods that have been around for years. Until organizations cover the basics, they won't be ready for more advanced adversaries.

In sports, great coaches study the opposition's favorite strategies and build in defensive strategies to take them off the table. That's exactly what defenders need to do to raise their level of play. Study our playbook. Focus on our most effective methods for breaching systems. Do everything you can to take our primary kill chains off the table. You will make our job, and the attackers' jobs we simulate, much harder. You will increase the energy we must expend to achieve our desired level of compromise and increase our likelihood of being discovered.

We have spent countless hours poring through the data from previous engagements so that defenders can learn from the pain that others have gone through. This is one of the best strategies for organizations to improve their security maturity. Before making your next security investment into technology with more blinking lights, make sure the basics are covered. That is the key to dramatically improving corporate IT security without spending millions.

No more excuses. The ball is in your court.

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. Credential theft is highly reliable, repeatable, and has a low likelihood of negative impact for an attacker.

The last finding in our list is insufficient network segmentation. Attackers can use credentials wherever they are allowed, even in places the users might not need or know about. This is why it is important to restrict access at the network level based on business requirements.

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 (e.g. cardholder data, PII, and PHI).

97%

had two or more root-cause findings

82%

had three or more root-cause findings

4.47

was the average number of root-cause findings

The average internal engagement length was

ONE WEEK

0 of the top 5 internal attack vectors required exploitation of unpatched software

Top Internal Attack Vectors

The following table represents the top five attack vectors used by Praetorian between 2013 and 2016 as part of a complete corporate network compromise kill chain. This list was last updated in June 2016 and is based on a review 100 reports.

RANK	FINDING	PERCENTAGE
1	Weak Domain User Passwords	66%
2	Broadcast Name Resolution Poisoning (aka WPAD)	64%
3	Local Administrator Attacks (aka Pass the Hash)	61%
4	Cleartext Passwords Stored in Memory (aka Mimikatz)	59%
5	Insufficient Network Filtering	52%

Table 1: Praetorian's top internal findings based on frequency of occurence in kill chain

We compiled this paper to detail the top internal attacks we used over the past three years that resulted in Praetorian achieving its objectives. Common objectives include achieving a sitewide compromise and/or access to sensitive information the client requested we gain access to. During the course of this research, we identified and selected 100 assessments. These assessments included 75 unique organizations. The focus of this research was to identify the most common, recurring security weaknesses that led to compromise so that organizations can focus efforts on closing the gaps actually used by malicious actors.

We reviewed internal pentest reports compiled between 2013 - 2016. This report only considered attack vectors ("findings") that were part of a "kill chain" leading to compromise or access to sensitive information. Therefore this document excludes many common findings from internal penetration tests, as they did not directly contribute to compromise.

To be clear, two or more vulnerabilities may be chained together to take control of the network. If a finding was included in the chain and resulted in a network compromise, it was counted. Also, if a single finding was used to compromise an environment but was not chained together with other findings, it was still included as a root-cause finding. Each finding in the chain was counted as a single instance.

We considered any method that resulted in access to sensitive data information or network compromise to be a "root-cause" finding.

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 against an organization's network. As a refresher nd as a reminder, the goal of a penetration test is to showcase the same standard operating procedures of an actual attacker. Penetration testing evaluates the effectiveness of security controls by simulating a real-world attack that mimics current adversary techniques. Unfortunately, most security firms are incapable of truly executing this kind of advanced attack. Instead, unqualified firms fall back on activity that is easily detected and thwarted due their reliance on unskilled and unseasoned consulting labor. **Running a vulnerability scan is noisy and — the most salient point of all — not required to identify organizational weaknesses that could allow a site-wide compromise or access to sensitive data.** Fortunately, Praetorian's core team includes former NSA operators and CIA clandestine service officers who are able to mimic the kill chains that are outlined in Verizon, Mandiant, and CrowdStrike's annual breach reports.

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 chief information security officer (CISO) unless all of these weaknesses would cause a going-out-of-business event. Any going-out-of-business event, and the attack vectors that caused it, MUST be the focus for all security teams. The top attack vectors discussed in this document should help security teams focus their efforts on issues that have the highest impact. 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.

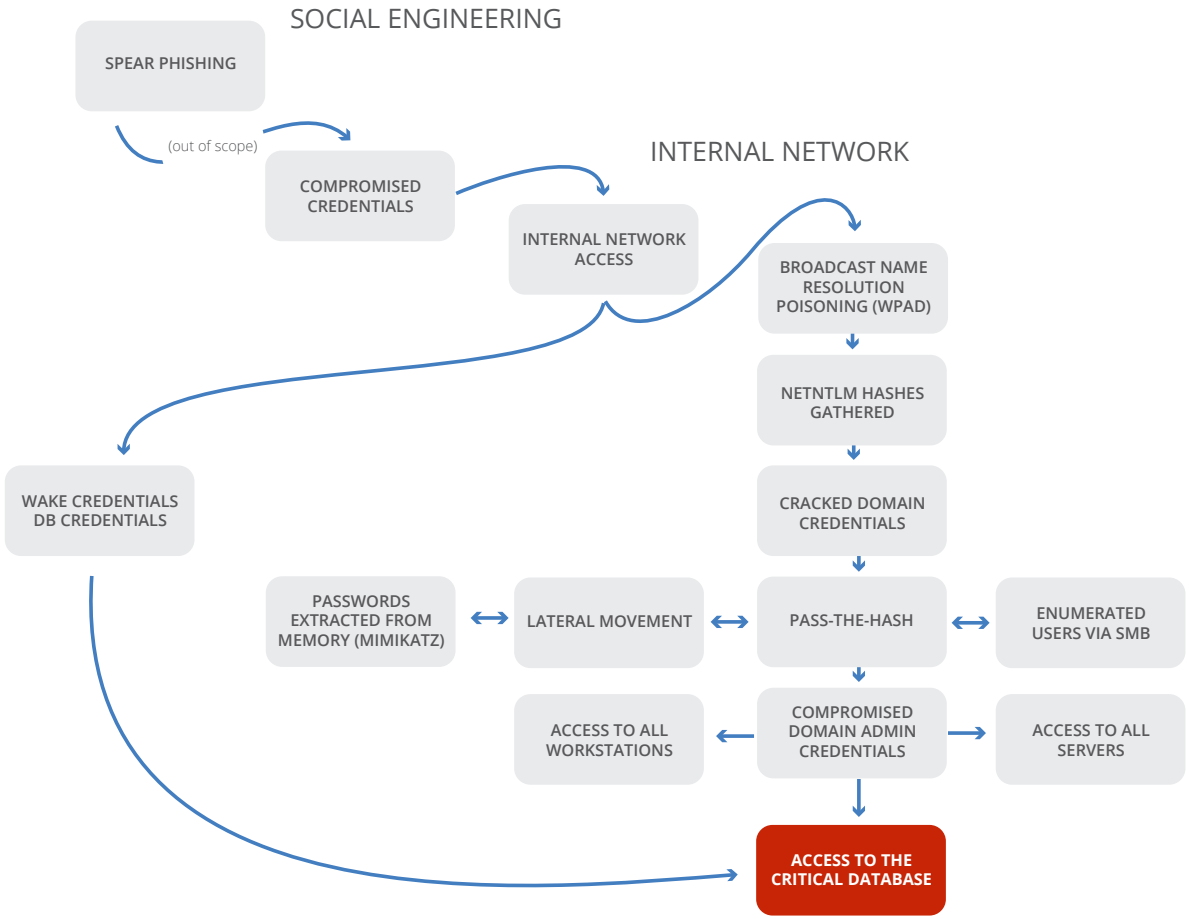
The reason why attackers focus on exploiting design weaknesses is because they more prevalent and reliable vectors. Design weaknesses will be present in the environment until the design changes. They also have a longer shelf life, which makes them very attractive since they won't be fixed in a short period of time (monthly or quarterly patch cycle).

Why only the top 5? Why not more?

When we started this research, our plan was to release a list of the top 10 internal attack vectors. However, when we reviewed the results of our research, we found a significant percentage drop (14%) after the fifth attack vector. Therefore, we decided to release the top five.

The rest of this paper is devoted to describing the top security weaknesses Praetorian has seen in organizations.

Sample Anatomy of Attack



The main attack vectors used were Pass the Hash, WPAD poisoning, Weak Domain Credentials, and Cleartext Passwords Stored in Memory.

> *...attackers don't rely on zero-day exploits extensively—unique attacks that take advantage of previously unknown software holes to get into systems. That's because they don't have to.*
>
> *"[With] any large network, I will tell you that persistence and focus will get you in, will achieve that exploitation without the zero days," he says.* ***"There's so many more vectors that are easier, less risky and quite often more productive than going down that route."*** *This includes, of course, known vulnerabilities for which a patch is available but the owner hasn't installed it.*

Rob Joyce
Chief, Tailored Access Operations
National Security Agency (NSA)

Wired - NSA Hacker Chief Explains How to Keep Him Out of Your System

The Top Attack Vectors

ATTACK ONE
WEAK DOMAIN USER PASSWORDS

ATTACK TWO
BROADCAST NAME RESOLUTION POISONING

ATTACK THREE
LOCAL ADMINISTRATOR ATTACKS - AKA PASS THE HASH

ATTACK FOUR
CLEARTEXT PASSWORDS FOUND IN MEMORY - MIMIKATZ

ATTACK FIVE
INSUFFICIENT NETWORK FILTERING

To effectively mitigate the attack vectors above, it is strongly recommended that organizations break down the mitigations into smaller, more manageable chunks. Verify remediation on these smaller elements before pushing out changes to all systems in the environment. For example, to deploy Pass-the-Hash mitigations, consider splitting this into two mitigations: one for workstations and one for servers. The following section contains strategic guidance for addressing each of the attack vectors to make the remediation process easier to manage.

Weak Domain User Passwords

66%

Attack Vector #1: Out of 100 internal pentests, Weak Domain User Passwords were used to compromise the environment 66% of the time.

Summary of the Attack

Most corporate environments use Microsoft's Active Directory to manage employee accounts and access. One problem with Active Directory is that it does not allow for comprehensive password complexity requirements. In essence, it does not restrict users from choosing bad passwords, because it only requires passwords to meet a specific length and contain specific characters sets. Therefore, passwords like "Password1!" and "Summer2016" are acceptable by Microsoft's built-in Active Directory policy unless third-party software is used to enhance these requirements.

Many organizations also provide users with Administrator access to their system. This is done to make it easy to install software, add print drivers and help with troubleshooting problems. The problem with this approach is that it allows users, or attackers who have compromised a user account, to install software could be malware or a virus that traverses the network.

If employees have Local Administrator rights to more than their own system, then malware is able to spread to those systems more easily. There are many ways to do this. One technique that has become popular for attackers recently is to use a compromised account to execute Powershell and WMI commands on remote systems. Most users do not require this ability to execute remote commands, but have received the permissions anyway. Instead, these capabilities should be restricted to only certain IT users who legitimately need them.

Recommendations

- Increase Active Directory password requirements to at least 15 characters in length, and implement an enhanced password policy enforcement solution.
- Implement two-factor authentication for all administrative access.
- Implement two-factor authentication for all remote access (VPN/Citrix).

Strategic Guidance

- Focus on implementing two-factor authentication externally first (VPN/Citrix).
- Next, expand the password length requirements to 16 characters. Start with users who have access to critical data. Educate end users about the value of using passphrases instead of passwords. Consider changing the rotation requirement from 90 days to 180 days to allow for greater acceptance due to the increased length.
- Once this is done, implement a "blacklist-based" enhanced password policy enforcement solution to prevent common passwords such as "Password1!," "$CompanyName16," "Summer16" and "August16."

References

Praetorian - Blog - Statistic Based Password Cracking Rules
Praetorian - Blog - Statistics Will Crack Your Password Mask Structure

Broadcast Name Resolution Poisoning

Summary of the Attack

This attack can be used when an attacker is on the corporate network. The attacker configures its system to respond to broadcast requests such as LLMNR, NetBIOS, or MDNS by providing its own IP. When a user tries to access network resources, such as websites that require authentication internally or an SMB share, the user's credentials can be transmitted to the attacker's system instead. The attacker is then able to replay the authentication attempt or crack the credentials offline (depending on the specific protocol). In certain situations, cleartext credentials may also be captured.

Strategic Guidance

- Populate DNS servers with entries for all known valid resources.
- Disable LLMNR and NetBios on a sample of end-user workstations.
- Based on the test sample, expand this to a wider test group and continue to iterate until all employee workstations are updated.
- Update the laptop/workstation gold image and/or build process.
- Test and deploy the updates to servers.
- Update the server gold image and/or build process.
- Throughout this process, monitor the network for broadcast queries to determine the effectiveness of these steps, while also monitoring for attacks.

References

Praetorian - Blog - Broadcast Name Resolution Poisoning / WPAD Attack Vector Turn off Multicast Name Resolution
US-Cert - Alert (TA16-144A) WPAD Name Collision Vulnerability

64%

Attack Vector #2: Out of 100 internal pentests, Broadcast Name Resolution Poisoning was used to compromise the environment 64% of the time.

Recommendations

To fully mitigate this attack, it's recommended that organizations take a defense-in-depth approach. This includes implementing the following protections.

- Create a WPAD entry that points to the corporate proxy server, or disable proxy auto-detection in Internet Explorer.
- Disable NBNS and LLMNR (test in a lab before deploying to all systems).
- Set valid DNS entries for all internal and external resources.
- Monitor the network for broadcast poisoning attacks.
- Restrict outbound 53/tcp and 445/tcp for all internal systems.

US-CERT encourages users and network admins to implement the following recommendations to provide a more secure and efficient network infrastructure:

- Consider disabling automatic proxy discovery/configuration in browsers and operating systems during device setup if it will not be used for internal networks.
- Consider using a fully qualified domain name (FQDN) from global DNS as the root for enterprise and other internal namespace.
- Configure internal DNS servers to respond authoritatively to internal TLD queries.
- Configure firewalls/proxies to log/block outbound requests for wpad.dat files.
- Identify expected WPAD network traffic and monitor the public namespace, or consider registering domains defensively to avoid future name collisions.
- File a report with ICANN by visiting https://forms.icann.org/en/help/name-collision/report-problems if your system is suffering demonstrably severe harm as a consequence of name collision.

Local Administrator Attacks (aka Pass the Hash)

Summary of the Attack

Organizations often configure all systems with the same Local Admin password. If an attacker is able to compromise the LM/NT hash representation of the password, then the attacker can use the hash to authenticate and execute commands on other systems that have the same password. This is exacerbated by the fact the attacker only needs the LM/NT hashes; the attacker doesn't need to crack the password at all. Having a very good understanding of this attack, how it works and what it looks like from a defensive perspective is the best way to be able to properly mitigate it.

If workstations and servers share a common Local Admin password, then all systems with this configuration can be compromised easily.

Recommendations

To address this attack, Microsoft has released a free tool, called LAPS. With this tool, all credentials are stored in Active Directory, which makes it easy to implement unique passwords for all Local Admin accounts. This protection should be implemented for all workstations and servers. Also, the organization should implement several defense-in-depth strategies, which are documented in the Microsoft Pass-the-Hash whitepaper, version 2 (included in the references below).

61%

Attack Vector #3: Out of 100 internal pentests, Pass the Hash was used to compromise the environment 61% of the time.

Strategic Guidance

- Work with IT department personnel to revise processes around utilizing local administrative privileges.
- Deploy LAPS on IT user workstations.
- Deploy LAPS on a sample of end-user workstations.
- Deploy LAPS on all remaining end-user workstations.
- Deploy LAPS on a sample of servers.
- Deploy LAPS on all servers.
- Update the workstation/laptop gold image or build process.
- Update the server gold image or build process.

References

Praetorian - Blog - Microsoft's Local Administrator Password Solution (LAPS)
Microsoft - Local Administrator Password Solution (LAPS)

Cleartext Passwords Found in Memory (Mimikatz)

59%

Attack Vector #4: Out of 100 internal pentests, we used cleartext passwords found in memory to compromise the environment 59% of the time.

Summary of the Attack

Modern versions of the Microsoft Windows operating system store domain credentials in cleartext within memory of the LSASS process. An attacker that is able to read memory is able to extract the cleartext domain credentials. This weakness requires an attacker to have Local Admin or SYSTEM-level access.

There are several popular free tools that can be used to execute this attack, but the most popular is called Mimikatz. This weakness has been addressed in Windows 2012R2+ and Windows 8.1+. To secure older systems, organizations need to install a KB article and implement a registry change. Once both have been implemented, credentials will no longer be stored in memory.

Recommendations

The Microsoft Security Advisory 2871997 should be installed and the following registry change should be implemented:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control SecurityProviders\WDigest
UseLogonCredential: Value 0 (REG_DWORD)

After the change has been implemented, credentials will no longer be stored in memory. Attackers also know about this fix, however, and if they have SYSTEM access, they can revert the registry change. Therefore, this registry key should continue to be monitored for unauthorized changes.

Strategic Guidance

- Deploy and test this mitigation on all domain Admin workstations.
- Deploy and test this mitigation on all IT workstations.
- Deploy this mitigation on all workstations.
- Deploy and test this mitigation on a sample of critical servers.
- Deploy and test this mitigation on a larger sample of servers.
- Deploy this mitigation on all servers.
- Update the workstation/laptop gold image or build process.
- Update the server gold image or build process.
- Monitor for unauthorized registry changes that revert this setting.

References

Praetorian - Blog - How to Mitigate Mimikatz WDigest Cleartext Credential Theft
Microsoft - Microsoft Security Advisory 2871997
Microsoft - KB2871997 and Wdigest – Part 1
Microsoft - KB2871997 and Wdigest – Part 2

Insufficient Network Filtering

Summary of the Attack

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. This means that after a single system on the internal network is compromised, an attacker can use this access to directly communicate with critical systems.

Recommendations

- Review the list of all critical systems and the data that resides in these systems.
- Gather feedback from business owners regarding which users need access to which systems and data.
- Enforce network Access Control Lists (ACLs) so that only authorized systems have access to critical systems. This can be done on a machine basis, by VLAN, or per user with certain "Next Gen" firewalls.
- Update network architecture and network diagrams to reflect the new ACLs.

52%

Attack Vector #5: Out of 100 internal penetration tests, insufficient network filtering was used to compromise the environment 52% of the time. Although not the main cause of breach, insufficient network filtering significantly expand the blast radius.

Strategic Guidance

When determining how to segment the network, consider what access a user would need. If network connectivity can be restricted to the local VLAN, then that is the best approach. In general, access from low-security into higher-security network segments should be tightly restricted. Forcing an attacker to be on a specific VLAN in order to access specific resources is a strong approach.

If several VLANs can communicate with a critical server VLAN, consider creating a boundary by requiring the use of a jump box before users access critical servers. Jump boxes should require two-factor authentication to prevent attackers from crossing this trust boundary.

Group systems based on data categories, applications, business units, or some other method. Include all related applications and databases and all back-end functionality. Put these types into a logical grouping. Think of it as a virtual private network. Access into and out of this network segment can be heavily monitored using an IDS/IPS device.

References

InfoSec Institute - VLAN Network Segmentation and Security- Chapter 5

PRAETORIAN

Want to learn how you compare against industry peers?

Qualified organizations are invited to schedule a free 30-minute strategy session with a Praetorian security engineer to answer questions about addressing the top 5 attack vectors.

Schedule Free Strategy Session

or visit http://www3.praetorian.com/connect.html

85% ALL-TIME NPS
Services Excellence

Find out why 97% of our clients are highly likely to recommend Praetorian.

Based on all-time Net Promoter Score (NPS) of 85.52%

"Very skilled, professional, and detail oriented. Did a great job explaining results and the process to create the results which was extremely helpful."

Director, Information Security
at one of the top-5 largest global media organizations

"Praetorian always considers the broader set of enterprise services we have here at Qualcomm so reports and recommendations can be actionable."

Senior IT Security Engineer
at Global Fortune 500 American multinational semiconductor

"Praetorian was fantastic to work with, and we really appreciate your professionalism and capabilities."

Chief Security Officer (CSO)
at major technology software/hardware vendor serving Fortune 100

"Praetorian has been flexible, fast, and easy to work with."

VP, Application Management
at top global investment management firms

"Team was highly skilled, professional and the reports were well written."

Director of Information Security
at one of the world's leading publishing companies

Find out why 97% of our clients are highly likely to recommend Praetorian.

Based on Net Promoter Score (NPS) of 85.52%

About Praetorian

Praetorian is a cyber security company that solves our client's biggest security challenges. Through offensive and defensive services and solutions, Praetorian provides tactical ground support and strategic guidance that meaningfully improves an organization's security posture.

Praetorian is a collective of highly technical engineers and developers with decades of industry experience. Our singular focus on information security consulting delivers unbiased expertise. The value we provide stems directly from our engineering culture – a continuous pursuit of efficiency and improvement in all operations. From proprietary methodologies and toolsets to project management and back office operations, we deliver quality results while decreasing your costs.

Headquarters
401 Congress Ave.
Suite 1540
Austin, TX 78701
P (800) 675-5152

info@praetorian.com
www.praetorian.com

How to Dramatically Improve Corporate IT Security Without Spending Millions

Now enterprise IT leaders can maximize budgets and outcomes by focusing on 5 key data-driven strategies for information security success

Scope

- Only security weaknesses that were used to obtain a full network compromise were included in this research.
- This report includes internal pentesting results.
- This report does not cover compliance requirements.
- This report does not cover all risks to an organization.

Bias

Not all attackers are motivated by the same end goals. For all of our internal engagements, one of the primary objectives was to achieve a full compromise of the environments tested.

This research was based on security testing for Praetorian's clients. Many of these organizations consider security mission critical and, therefore, the state of security in these internal environments may not be representative of all organizations.

Limitations

- Our results are limited by the findings we identified during selected security assessments between 2013 and 2016.
- Our results are limited by the time frame of the engagements.
- Our results are limited to the clients for which we performed the engagements.
- Our results are limited by the skills, tools and process of the penetration tester.
- Our results are limited to the scope of the engagements.
- Our results are limited by the details captured in our previous reports.