From Passwords to Pass-the-Hash: Why Credentials Are Still the #1 Attack Vector

By Lucio Rodrigues

🔐 Introduction

In the ever-evolving threat landscape, one thing remains shockingly consistent: **compromised credentials** are still the leading cause of data breaches.

Despite advancements in **EDR**, **XDR**, and **Zero Trust** models, attackers continue to exploit poor password hygiene, misconfigured authentication mechanisms, and legacy protocols to breach even the most "secure" infrastructures.

This post explores the evolution of credential attacks, with a focus on **Pass-the-Hash (PtH)**, why it remains effective, and how organizations can remediate this persistent threat.

🧾 Abbreviation Summary

MFA - **M**ulti-**F**actor **A**uthentication
PtH - **P**ass-**t**he-**H**ash
NTLM - **N**etwork **T**rust **L**evel **M**anager (Legacy authentication protocol)
AD - **A**ctive **D**irectory
RDP - **R**emote **D**esktop **P**rotocol
EDR - **E**ndpoint **D**etection and **R**esponse
SIEM - **S**ecurity **I**nformation and **E**vent **M**anagement
LAPS - **L**ocal **A**dministrator **P**assword **S**olution
LSA - **L**ocal **S**ecurity **A**uthority
LSASS - **L**ocal **S**ecurity **A**uthority **S**ubsystem **S**ervice
PPL - **P**rotected **P**rocess **L**ight
Sysmon - **Sys**tem **Mon**itor (Windows logging tool)
ACL - **A**ccess **C**ontrol **L**ist
C2 - **C**ommand and **C**ontrol
SMB - **S**erver **M**essage **B**lock
PsExec - **P**rocess **Exec**ution

📊 Real-World Impact: The Credential Crisis

According to **Verizon's 2024 Data Breach Investigations Report (DBIR)**:

- **86% of web application breaches** involved stolen credentials.
- **74% of all breaches** involved the human element, primarily weak passwords and phishing.
- Only **28% of organizations** enforce Multi-Factor Authentication (MFA) enterprise-wide.
- **Over 80% of ransomware attacks** started with credential access (via brute force or phishing).
- **More than 40 million passwords** were found exposed on the dark web in 2024 alone (Digital Shadows report).

These statistics make it clear: passwords are no longer just a user issue, they're a **security architecture issue**.

🧬 From Passwords to Pass-the-Hash (PtH)

Credential attacks have matured beyond brute-force logins. Today, adversaries often leverage **post-exploitation credential theft techniques**, such as **Pass-the-Hash**, which exploit flaws in Windows authentication.

📌 What is Pass-the-Hash?

Pass-the-Hash is a technique where an attacker, having obtained a **hashed version of a user's NTLM password**, can authenticate to other systems **without knowing the actual password**. It abuses the fact that NTLM authentication only requires the hash itself.

⚠️ *This technique is still effective in many enterprise environments running Active Directory with default configurations.*

🛠️ Typical Workflow:

1. **Initial Access:** Via phishing, RDP brute force, or exploiting a service.
2. **Privilege Escalation:** The attacker elevates privileges using exploits or misconfigurations.
3. **Credential Dumping:** Tools like Mimikatz or LSASS memory scraping reveal NTLM hashes.
4. **Lateral Movement:** The hash is reused on other systems to move laterally using PsExec, WMI, or SMB.

⚙️ Tools Commonly Used

Tool	***Purpose***
Mimikatz	Extracts plaintext creds, hashes, tickets
Impacket	Performs SMB relay, PtH attacks
Evil-WinRM	Remote PowerShell with PtH support
CrackMapExec	Automates lateral movement and PtH
Rubeus	Kerberos ticket manipulation (used in conjunction with PtH)

🔎 Why PtH Still Works

Despite being documented since 1997, PtH remains effective due to:

- Overuse of **NTLM** (instead of Kerberos)
- Lack of Credential Guard or **LSA** protection
- Local Admin reuse across machines
- No network segmentation
- Plaintext hashes in memory (if WDigest is enabled or memory is unprotected)

Organisations failing to properly secure their **authentication infrastructure** are vulnerable to **entire domain** compromise from a single foothold.

🔧 Remediation Strategies

✅ 1. Enforce Strong Authentication

- Implement **Multi-Factor Authentication (MFA)** across *all* access points.
- Disable **NTLM** where possible; **enforce Kerberos** for internal auth.
- Use certificate-based logins or smart cards where feasible.

✅ 2. Harden Local Accounts

- Use **LAPS** to rotate local admin passwords uniquely across endpoints.
- Avoid account reuse across the domain, especially privileged accounts.

✅ 3. Enable Credential Guard

- Deploy **Windows Defender Credential Guard** to block access to **LSASS** memory.
- Set RunAs**PPL** to protect **LSASS** at boot time.

✅ 4. Monitor and Detect

- Use **Sysmon** and **Windows Event Logs** to detect credential dumping attempts.
- Monitor for anomalous lateral movement behavior: **PsExec**, **RDP** logons, **SMB** connections.
- Use **SIEM rules** to alert on:
  - Multiple failed logons from a single IP
  - **NTLM** authentication in Kerberos-preferred networks
  - Mimikatz signatures or PowerShell obfuscation

✅ 5. Network Segmentation and Least Privilege

- Use **firewall rules and VLANs** to limit lateral movement.
- Apply **principle of least privilege**: users should not have local admin unless strictly necessary.
- Remove unnecessary **SMB** shares or disable administrative shares.

✅ 6. Regular Credential Hygiene Audits

- Periodically check for stale accounts, shared accounts, and accounts with no **MFA**.
- Audit passwords against known breach dumps using tools like **HaveIBeenPwned** or **pwdump-checkers**.

👨‍💻 Pentesting Reflection

During my pentesting labs and red team simulations, **credential access is often the first and most reliable path to full domain compromise**. Combined with improper privilege management can allow **domain admin access in under 30 minutes**.

Simulating **PtH** and credential theft scenarios allows me to demonstrate how easily attackers can escalate privileges and move laterally in under-secured environments. It also showcases my ability to provide **defensive recommendations** that align with real-world risks and architecture.

Lucio Rodrigues - Cybersecurity Portfolio

Final Thoughts

Credential theft isn’t going away, it’s evolving. As long as organisations rely on outdated protocols and ignore identity-centric threats, techniques like Pass-the-Hash will continue to be exploited.

The solution lies not only in **strong passwords**, but in building a **resilient identity infrastructure**, one where authentication is layered, monitored, and hardened against misuse.