HTB Assessment Report: The Credential Theft Shuffle

# Executive Summary

This red team engagement simulated an internal compromise of Nexura LLC. The goal was to gain command execution on the domain controller (DC01). Initial access was gained using reused credentials. From there, pivoting, BloodHound enumeration, and credential dumping led to domain administrator access.

# Engagement Scope

|  |  |
| --- | --- |
| Host | IP Address |
| DMZ01 | 172.16.119.13 |
| JUMP01 | 172.16.119.7 |
| FILE01 | 172.16.119.10 |
| DC01 | 172.16.119.11 |

# Attack Path Summary

1. Initial access via jbetty:Texas123!@#  
2. SSH history revealed William's internal creds  
3. Chisel pivot enabled internal network access  
4. BloodHound revealed bdavid is admin on JUMP01  
5. Legacy Password Safe vault cracked  
6. Mimikatz used to dump stom (Domain Admin) hash  
7. Pass-the-Hash used to gain shell on DC01

# Credentials Discovered

|  |  |
| --- | --- |
| Username | Password / Hash |
| jbetty | Texas123!@# |
| hwilliam | dealer-screwed-gym1 |
| bdavid | caramel-cigars-reply1 |
| stom | NTLM: 21ea958524cfd9a7791737f8d2f764fa |

# Domain Controller Compromise

Using Mimikatz on JUMP01, the NTLM hash for the domain admin account 'stom' was extracted. This was leveraged via wmiexec and evil-winrm to gain code execution and full access to DC01.

# Recommendations

• Enforce password reuse policies and monitor for vault leaks.  
• Rotate credentials and enforce aging/complexity.  
• Protect LSASS from memory dumping.  
• Audit local admin group memberships.  
• Enable account lockout thresholds.

Report generated on 2025-06-06 21:32:59