The Art of Compromising Passwords

Lessons Learned from Security Assessments

>whoami

Senior Offensive Security Consultant at Depth Security

Former Attorney

Recently finished my first marathon

First try guessed a valid password on first ever pentest

>why

Lack of resources on how passwords are actually compromised beyond the basics

Explain the preparation behind the luck of password compromises on assessments

Provide some practical insights and examples to help improve footholds and lateral movement

(My) Shame

>grep -v

Summer2025! or Company2025! or Password123!(For the most part)

The very important step of user enumeration

The process of secrets hunting/where to find cleartext passwords

Password Cracking (but lessons can be learned from them)

“Thank you for contacting the Microsoft Security Response Center (MSRC). Upon investigation we have determined that these do not meet the bar for security servicing. In general, username enumeration does not meet the bar as there are many ways to do this and on its own it does not allow an attacker access or control in any way, as the attacker would still need to bypass login.”

>Passwords --help

Variations of common words are still viable

Deny lists can be very brittle

Evaluate against Entra Password Protection Global Banned List and Rules

Use age of when accounts are created (if known) to inform year selection

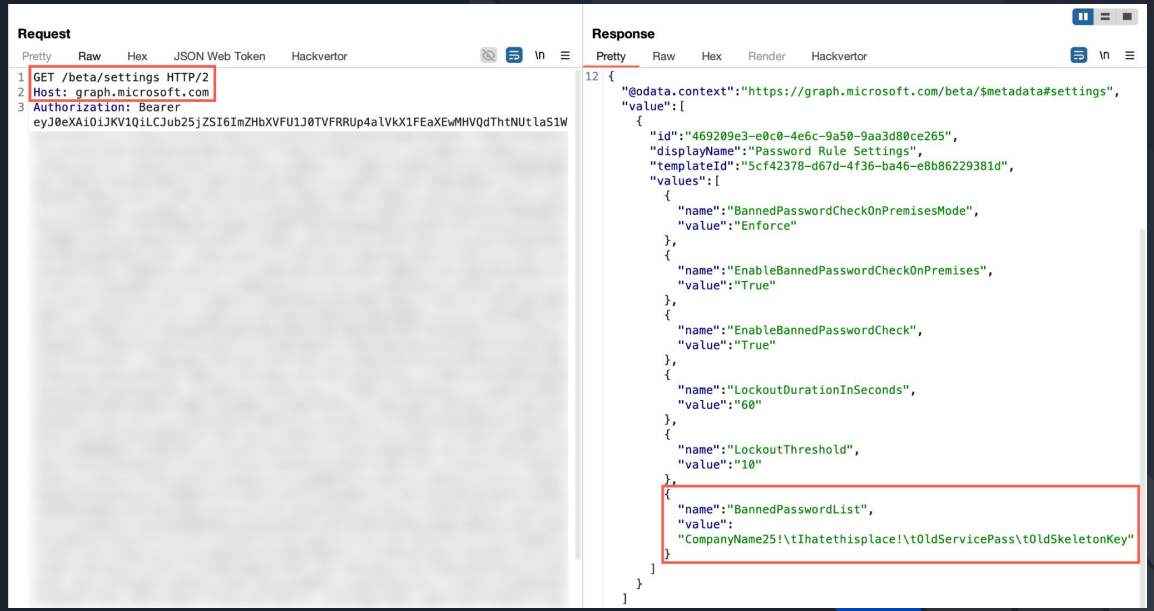
>Passwords --help cont.

Custom banned lists can provide targets

GET /beta/settings on graph.microsoft.com as authenticated user

Still might be in use by service and/or local accounts

Iterate Iterate Iterate



>Passwords --help cont.

Breach Credentials

Onboarding/Reset Password Schemes (FirstDay!, Welcome2company! etc…)

If authenticated, crawl through emails and documentation for commonly used organizational passwords and/or schemes

Iterate Iterate Iterate

>Passwords --help cont.

Password Reuse

Iterate Iterate Iterate

(Lack) of Separation of Privilege:
user:Retirement2025!
adminuser:Retirement2025@

Stale passwords can reveal old or current password schemes

Iterate Iterate Iterate

>Passwords --help cont.

Target the weak links

Focus on accounts without password expiration

Service accounts more likely to have non-conforming passwords and have insecure MFA

Don’t forget to target .onmicrosoft.com accounts if you have them

If targeting all accounts, don’t overthink and don’t take password policy at face value

>Final Thoughts

Not one size fits all

Context is key (cloud or on prem, unauthenticated versus foothold, users versus service accounts, adjust as needed)

Conduct target research (industry, location, street, phone extensions, address, etc…)

Complexity and character minimums rarely matter when it comes to weak passwords