EPAS and Password Cracking Tools: A Comparative Analysis

Tri Nhan Pham – Supervised by Prof Ryan Ko, Daniel van Niekerk and Taejun Choi

[1] Detack, “EPAS STORY V0”.
[2] Detack, “EPAS - PoC Audit 2023,” 2023

Introduction

Passwords are still the most common authentication method in the world nowadays, despite being introduced a long time ago. They are protecting about 60% of all digital logins around the world. On the downside, weak passwords are the leading cause in data breaches.

This project evaluates the usage of Enterprise Password Analytics System (EPAS) from Detack. This is a password auditing platform which is designed to flag and report weak passwords to businesses so they can protect themselves from adversarial hackers.

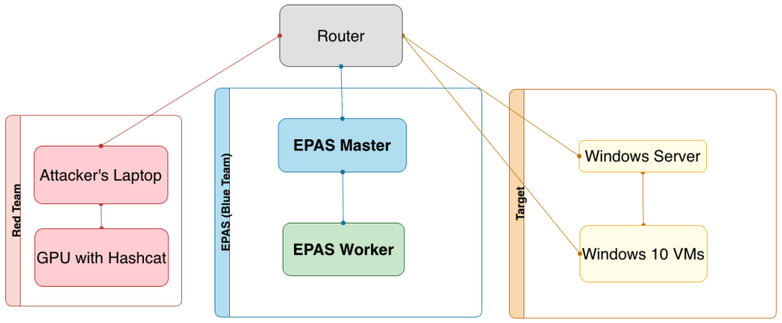

Figure 1: Diagram of network setup

Methodology

Setup:
- 50 Windows accounts on a Windows Server domain as the victims
- EPAS installed
- Hashcat installed on a RTX A4000 GPU

Process:
- Perform a password extraction: SAM Dumbing, Privilege Escalation, Responder
- Collect all the hashes and feed into Hashcat for cracking, using RockYou dictionary and Best66 rule
- Connect the virtual machine to EPAS and run an audit session
- Collect the result and perform comparative analysis with Hashcat

Figure 2: Workflow for comparing EPAS (Blue Team) with a traditional cracking tool (Red Team).

trinhan.pham@student.uq.edu.au
Tri Nhan Pham

School of Electrical Engineering and Computer Science

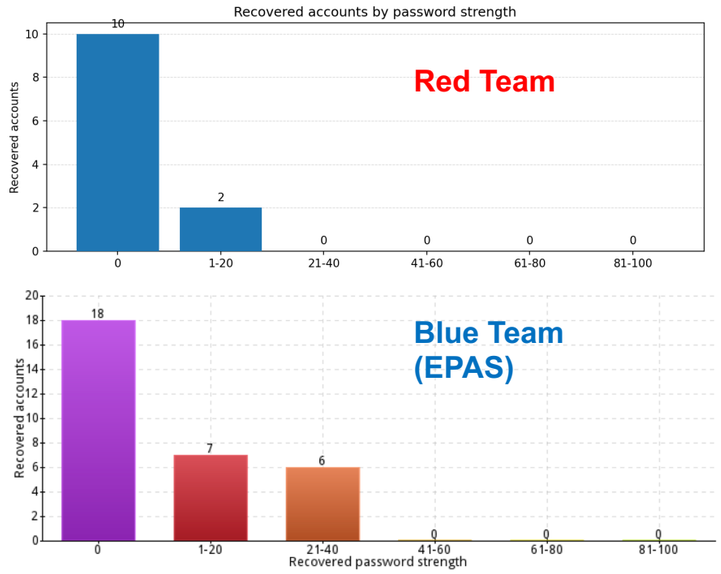

Figure 3: Zxcvbn password-strength scores for Blue Team vs. Red Team.

Results

Cracked password strengths

The number of passwords cracked by EPAS was about 150% more than Hashcat’s. Each password was assigned a score for their strength (using the password strength estimation tool provided by EPAS based on zxcvbn). The total score of passwords EPAS cracked was about 500% higher than Hashcat’s (average on 5 runs, each tested with 50 passwords with maximum 16 characters, generated by PassGPT).

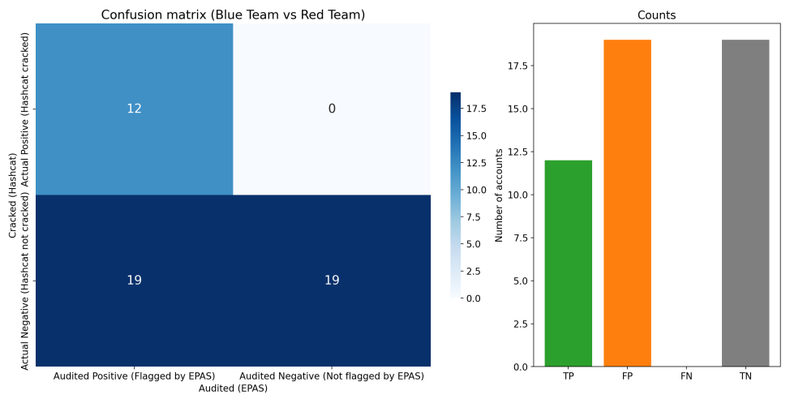

Figure 4: Confusion matrix of cracked passwords by Red Team vs. EPAS audit results.

Acknowledgements

I want to send special thanks to Prof. Ryan Ko, Taejun Choi, and Daniel van Niekerk (Detack) for their guidance and infrastructure access.

Cracked password coverage

Results showed that EPAS audited a wider set of weak passwords than those cracked by the Red Team.

The confusion matrix in figure 4 illustrates that EPAS flagged every password cracked by the Red Team (FN = 0). The additional flag from EPAS that Hashcat did not crack reflect weaknesses in password policies as some were found in compromised databases and some were found by the AI feature. This is desirable for business, which minimises undetected compromises.

The Venn diagram below shows more details on which passwords were cracked by both teams.

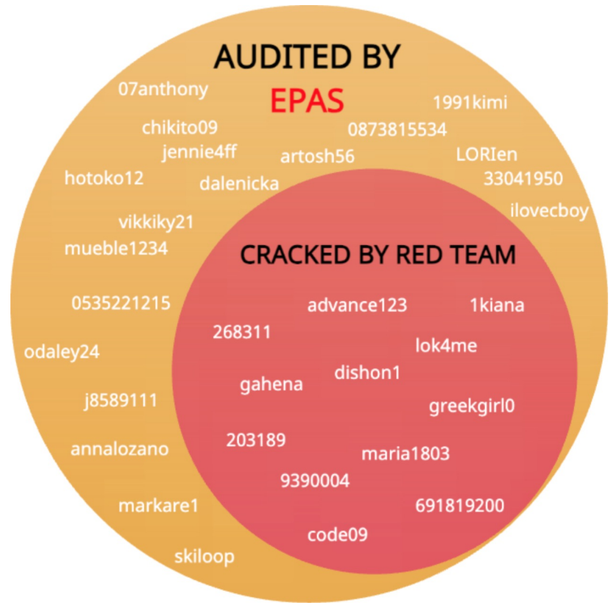

Figure 5: Venn diagram of password coverage.

Conclusion

This study showed that **EPAS can detect weak enterprise passwords with a high accuracy** compared to those traditional cracking tools were able to crack, while being easier to use and more scalable for large organizations.

Future work will expand testing to larger datasets and evaluate performance on different hash types and password policies.