REIT4842 Project Proposal

Auditing The Auditor

Security Assessment of Detack EPAS – A Password Security Assessment System

Daniel Van Niekerk – 46413813

- 9-21-2023

Table of Contents

Introduction:

Password systems are a ubiquitous in tool in modern day privacy with the use of high quality being a requirement to make these systems effective and secure against cracking attacks [1]. Password policy enforcements and strength checkers attempt to ensure the use of secure passwords [2].

Detack EPAS introduces a new layer to password security assessment to further increase password quality and thereby resistance to attacks. This is done through an audit system that retroactively tests password strength by performing a password attack that goes beyond the scope a systems policy [3]. The password recovery is performed in a secure and privacy compliant manner, and ultimately reports summary statics of the audit to the system admin and notifies users who have been detected to have an insecure password [3].

With the introduction of new systems comes with it the potential for undiscovered vulnerabilities that could result in threats to the system if exploited by malware or other forms of cyber-attacks [4]. These vulnerabilities can be proactively managed in a controlled environment through the use of penetration testing [5] which seeks to discover and report vulnerabilities before they are exploited with ill intent.

That is why purpose one of this this project is to determine and detail the principles adopted by the Detack EPAS system. With purpose two being to find either an exploitable or theoretical vulnerability in the system. These goals will be accomplished through iterative tests that will follow a standardised framework in order to be focused in their scope, be repeatable in nature, have well defined results and critically thought-out outcomes from these results. With the final report being a meta review of the findings of these tests in order to summarise relevant findings and outcomes and use these high-level outcomes to make improvement recommendations.

Background & Literature Review:

System Context - Current Password Checkers

Password systems are the first layer defence in protecting users' private data making them a common target for hackers, for this reason it is import users use high quality passwords to reduce this risk. Password strength enforcement is commonly done in two forms, the first is policy enforcement [6], these are basic requirements that the password must follow in order to be accepted for example a minimum length or a requirement for use of multiple character sets [7], [8].The second is proactive password strength checkers, these may appear as a black box to users [9], are primarily functioning through performing a password attack. These are implemented at the time of password generation and often attempt to crack the user's password through a process of brute force and dictionary attacks [10].

Brute force attacks are done by checking all possible passwords allowable in the given system and as a result are often resource and time consuming. These can be made more efficient through the use of a rainbow table which is the precomputation of password hashes [11], meaning a lookup table can be used, this is however more memory intensive. Dictionary attacks function by limiting the password guessing space by skipping combinations a user is unlikely to use. Guesses are often based on discernible user attributes such as native language and the website being logged into [1] [12]. Often resulting in high coverage of passwords in a much smaller guessing space [13]. Dictionary attacks are also time restricted with strength being calculated at the time of password generation [14], with current password algorithms being imperfect allowing weak passwords to be accepted by the system [15].

System Context – The EPAS Password Auditing

The EPAS audit takes a unique perspective to password strength enforcement by simulating password attacks known as password recovery [3] this is done in a secure environment. The strength testing is done retroactively after the user password has already been set, this reduces time restrictions as a meaningful amount of time can be used to more accurately simulate password attacks [3]. If a user is found to be using an insecure password, they are emailed and are required to change their password [3]. This further filters weak and insecure passwords and overall increases password quality.

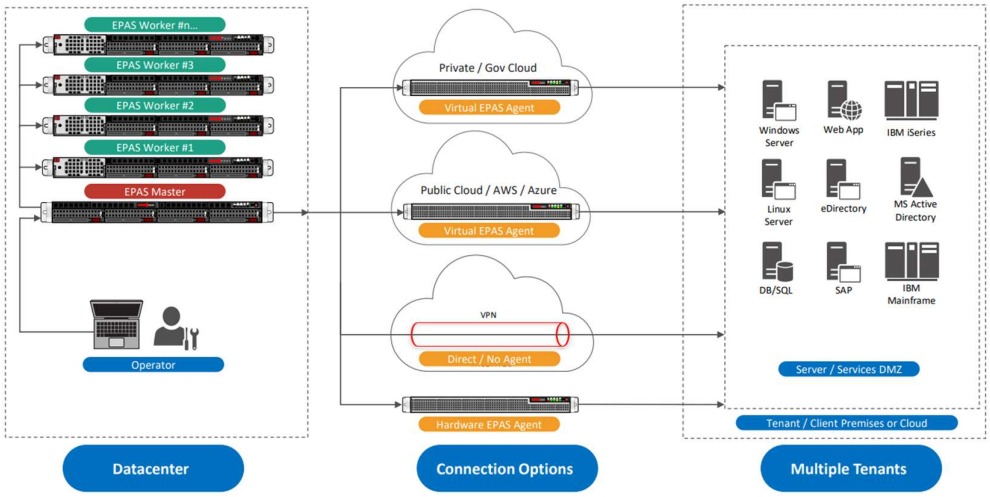


Figure 1:EPAS System Configuration [16]

The system operators in a datacentre as shown in Figure 1 making use of a master as a central point of contact for the system and a variable number of & Literature Review worker units to distribute work amongst during an audit. During an audit the system makes use of APIs to retrieve and send required data beyond the confines of the data centre [3]. The audit is performed through performing dictionary and brute force attacks [16]. This is a time-consuming process and if unoptimized may be ineffective at yielding meaningful results [14].

Although the system for the most part functions offline it is still connected to the internal network making it susceptible to cyber-attacks. The main functions of the system is to audit data and to report summary statics it is primarily susceptible to two types of cyber-attack, the first is data exfiltration attacks [17], this is the unauthorised access to data. And second false data injection attacks [18], this is false data injected by an attacker in an effort to mislead the system administrators about the status of the system.

Introduction to Penetration Testing

Penetration testing (Pen testing) is performed in a controlled circumstance to identify and exploit security vulnerabilities in a target system to test the effectiveness of the implemented security measures [5]. There are five main areas in penetration testing with the first being reconnaissance in which initial information is collected about the target organisation and systems. This is information from publicly available sources such as websites, social media but also extends to checking for leaked credentials [19] and often makes use of tools to aid this information gathering such as the Open-Source Intelligence Framework (OSINT) [20]. With the goal being to gather information that can be used to identify potential attack vectors.

The Second Phase is scanning and involves using network scanning tools such as Nmap [21] OpenVAS, Wireshark and nikto. These tools utilise ping sweeps along with TCP and UDP port scanning and make use of the resultant response or lack of response to identify discernible information. This can range from information on if a port is listening to more advanced information such as the ciphers being employed. Scanning gives further insight into the targets attack surfaces and can help to highlight particularly vulnerable surfaces.

The Third phase is enumeration and seeks to extend on information gathered in the first two phases often by interacting with the target systems by making use of tools such as the Metasploit framework [22], searchSploit along with known cybersecurity vulnerability databases such as CVE Mitre which quantitatively gauges the severity of vulnerabilities using a Common Vulnerability Scoring System (CVSS). With the goal of this phase being to identify weaknesses in attack surfaces.

The fourth phase exploitation aims to use gathered information on potential vulnerabilities in the system to gain some sort of unauthorised access to the system or data in the system. This can be done using the Metasploit exploit modules [23], along with custom scripts written in a scripting language to send data payloads in order to exploit a target system. This phase can also extend to human attack surfaces making use of social engineering tactics such as phasing emails [24].

The fifth main stage is post-exploitation which aims to extend upon the fourth phase by using the unauthorised accesses to maintain and extend the access to the compromised system. This often aims to establish persistence by using a backdoor or privilege escalation to gain higher-level access within the system.

Threat Landscape

Data exfiltration attacks is the attempt of an unauthorized entity to extract and obtain sensitive or private data. This can be perpetrated by external parties or from within an organisation [25], this can make them particular devesting if performed by an insider with comprehensive and in-depth knowledge of a system knowing where potential weaknesses may occur and the location of assets of higher sensitivity. This type of attack can result in devastating data breaches regarding user information. Data exfiltration attacks are particularly potent as they can be performed with little disruption and go unnoticed by investigative countermeasures, and if detected can be hard to respond to in real time [25].

False data injection attacks are attacks that comprise the results of sensor readings and originated from attacks on modern power systems that target sensors [26]. In the cyber domain this can apply to the reported data from systems and is an increasing issuing as systems become more entangled [27]. In the context of the EPAS Audit reported results could be targeted and modified by adversaries, this would mislead system admins about the state of user password quality and make the system more vulnerable to data breaches.

Project Relevance & Purpose:

The Detack EPAS Audit implements retroactive password checking in a relatively new manner with limited research and analysis publicly available about the internal functioning of the system. That is why this project aims to document the core functionality of the Detack EPAS system and the principles adopted by the system in the way of password checking by the EPAS enforcer, along with details of the auditing process performed by the EPAS Audit.

Additionally given the brevity of the system it has had limited exposure as a potential attack surface for hackers. Cyber-attacks are commonplace in the modern era of online data being integral to everyday life and this data having substantial value it is natural groups seek out and exploit vulnerabilities of systems for personal gain. Given the EPAS system is already commercialised it is imminent that it will be used as an attack surface for hacker groups with undiscovered vulnerabilities proposing threats to the system. That is why this report also seeks to analyse the core function of the system and use this knowledge to find exploitable or theoretical vulnerabilities through employing penetration testing techniques and tactics. These findings will be used to make improvement recommendations of further measures that can be taken to safeguard the security of the system.

To summarise, purpose one is to: Document and outline the perceived internal functionality of the both the EPAS enforcer system and the EPAS audit system in the way of how these components are integrated into a larger system, under what circumstances data flows into and out of the system, what information this data is expected to contain and what form this data takes (method of encryption).

Purpose two will be to: Establish a repeatable framework of tests to systematically analyse and evaluate attack surfaces, vulnerabilities, and weaknesses that either directly or indirectly arise from the incorporation of the EPAS Audit and EPAS enforcer into a larger network.

Methodology & Milestones

The project will be undertaken in four main stages with overlap between stages. The first will be the preliminary information gathering and introduction to the problem, comprising of gaining a thorough understanding of the scope of the problem through speaking with a thesis supervisor, this stage will also include the completion of the UQ Academic integrity module due on the 17th of August. This stage will be completed by the 20th of August.

The second stage will be the formalisation of the problem, this will require a comprehensive background study and literature review to understand relevant information in the field. This has been narrowed down to the understanding of password systems, a core understanding of penetration testing along with the primary cyber attacks the system is susceptible to being data exfiltration and false data injection attacks. The result of this research will be used to complete a proposal report detailing the intended undertakings of the project. This stage will be summarised in the project proposal and will ideally be completed the same day the proposal is due on the 21st of September.

Additionally, as EPAS is a physical system it is to be installed into the UQ ASOC system during stage two. This will require the manual installation of the EPAS Master and worker units into the ASOC server rack which will first require the physical system. It will also require the initial software setup and configuration of the system with the appropriate network routing in order to have the system functional. This is prone to delay as it requires the cooperation of external parties being Detack to

provide the system and virtual help with setup if required. An individual qualified to interact with the ASOC server rack and set up the network routing. Along with UQIT for required software licencing and permissions.

The third stage will be to iteratively implement and test solutions. Initially tests will be implemented to uncover and demonstrate the internal functionality of the system fulfilling purpose one of the projects. Secondly tests will be implemented and performed to expose vulnerabilities in the system fulfilling purpose two of this project. The results of these tests will be used to understand the inner workings of the systems and the principles it adopts as seen from an outside perspective. The first iteration of tests and progress will be presented in a seminar progress report in Week 12 of semester 2 2023. This stage will then continue until week 7 semester 1 2024 as more tests are implemented and executed. It is noted that stage 3 is subject to change and further specification as work progresses and more avenues of progress are discovered. Stage three is partially bottlenecked by stage two as the system is required to be installed and configured before testing can begin, however tests can be planned and theorised if delays are present in this bottleneck.

Each iterative test performed in stage three will be conducted according to a standardised framework that will require for each test to encompass the following three phases:

- Planning Phase
    - Have a specific and well-defined scope of focus. This will also outline which purpose (one or two) the test is intended to cover.
    - A date of commencement set on the day the scope of focus is initially understood.
    - A prior motive for the test and why it should it commended along with any background research to substantiate this motivation.
    - Qualitative and/or quantitative expected outcomes of the test.
- Implementation Phase
    - An overview of the implementation along with research into any supporting material required for its implementation.
    - A set of procedures in which the test can be carried out that are well defined and repeatable.
- Evaluation Phase
    - The results of the test either quantitative or qualitative
    - A CVSS score to quantitively score a vulnerability and zero if none is found.
    - Research into future directions that can be taken to extend upon the outcomes.

Refer to Appendix 2 for testing procedure template documentation. Each test will be kept small in scope ideally taking no more than two weeks to complete. Tests that are seen to be going out of scope will be reviewed and be separated into smaller tests with a narrower scope or dropped if the hurdles are seen as insurmountable in a reasonable time period, this will be to prevent over extending resources and help to prevent delays in progress. These will still be documented and included in the final report as partially completed with an outline of the hurdles. This stage will be completed on the 3rd of May 2024.

The fourth stage will heavily overlap with stage 3 and will be the summarising result outcomes of tests that is discovered during stage 3, this will be information about system vulnerabilities and core functions. This information along with the initial thesis proposal with be used to lay a foundation of background knowledge that will be used to construct a thesis report being a comprehensive detailing of the project and its findings. This final thesis report will be compressed into a Poster to be presented as a demonstration.

Page 7 Is a full Gantt Chart timeline outlining specific timeframes for each process.

REIT4842 GanTT Chart

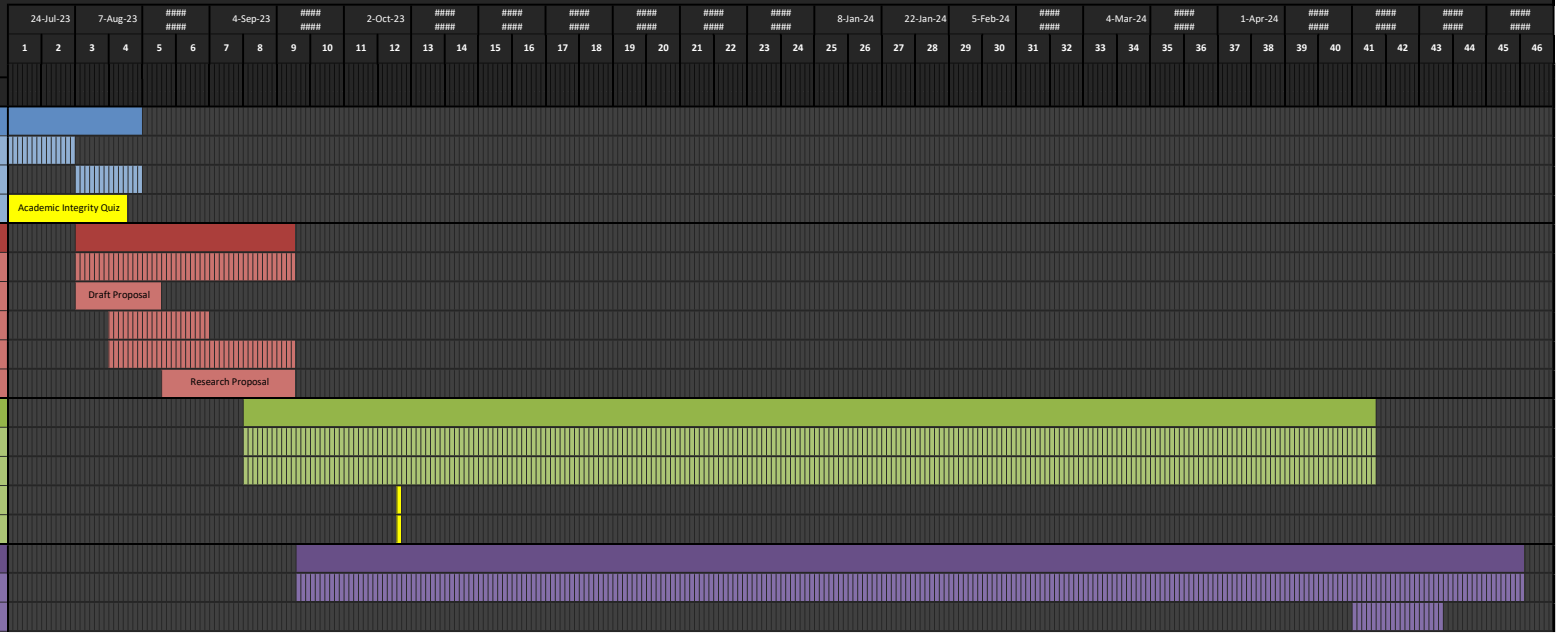
SIMPLE GANTT CHART by Vertex42.com
https://www.vertex42.com/ExcelTemplates/simple-gantt-chart.html

Project Conducted by:
Daniel van Niekerk

Project Start: 24/07/2023

Week:

TASK	START	END
Preliminary Information Gathering	**24-Jul**	**20-Aug**
Topic Selection	9-Aug	15-Aug
Problem Scoping	7-Aug	20-Aug
Online Academic Integrity Quiz	24-Jul	17-Aug
Formalisation of Problem	**7-Aug**	**25-Aug**
Literature Review of existing solutions	7-Aug	16-Aug
Proposal Draft Report	7-Aug	16-Aug
Implementation of System	14-Aug	21-Aug
Primary System Analysis	14-Aug	21-Aug
Research Proposal Report	25-Aug	25-Aug
First Iteration of Problem solutions	**11-Sep**	**3-May**
Iterative System analysis	11-Sep	3-May
Implementation and testing of solutions	11-Sep	3-May
Progress Seminar Presentation	26-Aug	13-Oct
Progress Seminar Participation	29-Aug	13-Oct
Summarisation of Findings	**31-Aug**	**11-Oct**
Thesis Report Submission	31-Aug	3-Jun
Poster and Demonstration	31-Aug	17-May



Risk Assessment

The project requires some physical installation along with interacting with existing network devices both physically and virtually there are different types of potential risks that can result during different stages of the project.

Risk	Potential Outcome	Severity	Mitigation
Damage to EPAS or existing equipment during installation	Physical systems are physically damage and rendered Unusable	Medium	Ensure the installation is done only by an authorised induvial who is familiar with the installation
Mishandling of EPAS during moving of system.	Injury to operator or damage to equipment	Low	Ensure the use of multiple individuals when required during handling of equipment
Corruption of existing network infrastructure during testing	Existing network infrastructure is corrupted and or compromised.	Medium	Ensure the EPAS is installed on a separate LAN network that is physically or virtually isolated from other networks

Ethics Assessment

As the project attempts to compromise a commercialised system it poses several ethical risks.

Risk	Potential Outcome	Severity	Mitigation
The copywrite and patent owner of the system Detack does not agree to the hacking performed.	An infringement of the law and infringing parties are held liable.	High	Seek Written approval for tests performed on system and work within the agreed upon scope of the project to ensure all hacking is done ethically.
System Vulnerabilities are made known to untrusted entities before preventions and fixes are put in place.	Companies that employ the system are made readily vulnerable to malicious cyber attacks	Medium	Ensure all findings are not leaked to untrusted entitles before system mitigations are put in place.

References

[1] D. V. a. C. E. V. Madhavan, “Efficient dictionary for salted password analysis,,” *IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT),* vol. 1, no. 1, pp. 1-6, 2014.

[2] M. M. a. H. G. a. J. S. Algharibeh, “A Data-Driven Password Strength Meter for Cybersecurity Assessment and Enhancement,” *2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys),* pp. 1980-1987, 2021.

[3] L. (. Costin Enache, “PASSWORD AUDIT SYSTEM”. US Patent 9,292,681 B2 , 22 March 2016.

[4] M. N. M. J. N. Humayun, “Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study.,” *Arab J Sci Eng,* vol. 45, no. 4, p. 3171–3189, 2020.

[5] A. a. Y. X. a. C. B. a. J. M. Bacudio, “An Overview of Penetration Testing,” *International Journal of Network Security & Its Applications,* vol. 3, pp. 19-38, 2011.

[6] D. V. K. Matt Bishop, “Improving system security via proactive password checking,,” *Computers & Security,,* pp. Pages 233-249, 1995.

[7] T. N. M. G. B. C. a. S. F. A. S. K. Pushpa, “An Empirical Analysis of Passwords,,” *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT),* pp. 89-92, 2018.

[8] G. H. a. S. J. M. M. Algharibeh, “A Data-Driven Password Strength Meter for Cybersecurity Assessment and Enhancement,” *2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys),* pp. 1980-1987, 2021.

[9] X. D. C. D. a. M. M. Carnavalet, “A Large-Scale Evaluation of High-Impact Password Strength Meters,” *Association for Computing Machinery,* vol. 18, no. 1, pp. 1-32, 2015.

[10] J. J. Yan, “A Note on Proactive Password Checking,” *Proceedings of the 2001 Workshop on New Security Paradigm,* vol. 1, no. 1, p. 127–135, 2001.

[11] G. a. C. X. a. L.-A. D. Avoine, “Stairway To Rainbow,” *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security,* vol. 1, no. 1, p. 286–299, 2023.

[12] H. J. L. M. E. L. F. a. J. P. A. A. H. R. G. Cacacho, “Breaking the Password Security Standards Using Offline Attacks and Public User Attributes,” *IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM),* pp. 1-5, 2019.

[13] A. a. S. V. Narayanan, “Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff,” *Proceedings of the 12th ACM Conference on Computer and Communications Security,* vol. 1, no. 1, p. 364–372, 2005.

[14] E. Stavrou, “Enhancing Cyber Situational Awareness: A New Perspective of Password Auditing Tools,,” *International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA),* pp. 1-4, 2018.

[15] J. J. Yan, “A Note on Proactive Password Checking,” *Proceedings of the 2001 Workshop on New Security Paradigms,* vol. 1, no. 1, p. 127–135, 2001.

[16] DETACK, “EPAS – Audit & Enforce Secure Passwords, On-Premises and in the Cloud,” DETACK, Ludwigsburg, 2022.

[17] Z. Tari, N. Sohrabi, Y. Samadi and J. Suaboot, “Data Security Threats,” *Data Exfiltration Threats and Prevention Techniques: Machine Learning and Memory-Based Data Security , IEEE,* vol. 1, no. 1, pp. 31-61, 2023.

[18] G. B. a. D. B. Rawat, “Security Analysis in Context-Aware Distributed Storage and Query Processing in Hybrid Cloud Framework,” *IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC),* pp. 0177-0183, 2019.

[19] philipperemy, “1.4 Billion Text Credentials Analysis (NLP),” [Online]. Available: https://github.com/philipperemy/tensorflow-1.4-billion-password-analysis. [Accessed 18 9 2023].

[20] M. a. J. D. R. a. S. A. E. a. K. V. D, “Information Retrieval using OSINT and GHDB,” *2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI),* pp. 1-7, 2023.

[21] P. Calderon, “Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips,” *IEEE,* 2021.

[22] R. Messier, “Enumeration,” in *CEH v11 Certified Ethical Hacker Study Guide*, 2021, pp. 221-262.

[23] metasploit, “metasploit,” [Online]. Available: https://www.metasploit.com/. [Accessed 18 9 2023].

[24] J. a. H. T. a. C. R. a. V. A. a. R. H. R. Wang, “Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email,” *IEEE Transactions on Professional Communication,* vol. 55, pp. 345-362, 2012.

[25] M. E. R. R. R. C. M. A. B. A. R. Faheem Ullah, “Data exfiltration: A review of external attack vectors and countermeasures,,” *Journal of Network and Computer Applications,* vol. 101, pp. 18-54, 2018.

[26] S. Sengupta, “What is False Data Injection?,” *crashtest-security,* 18 8 2022.

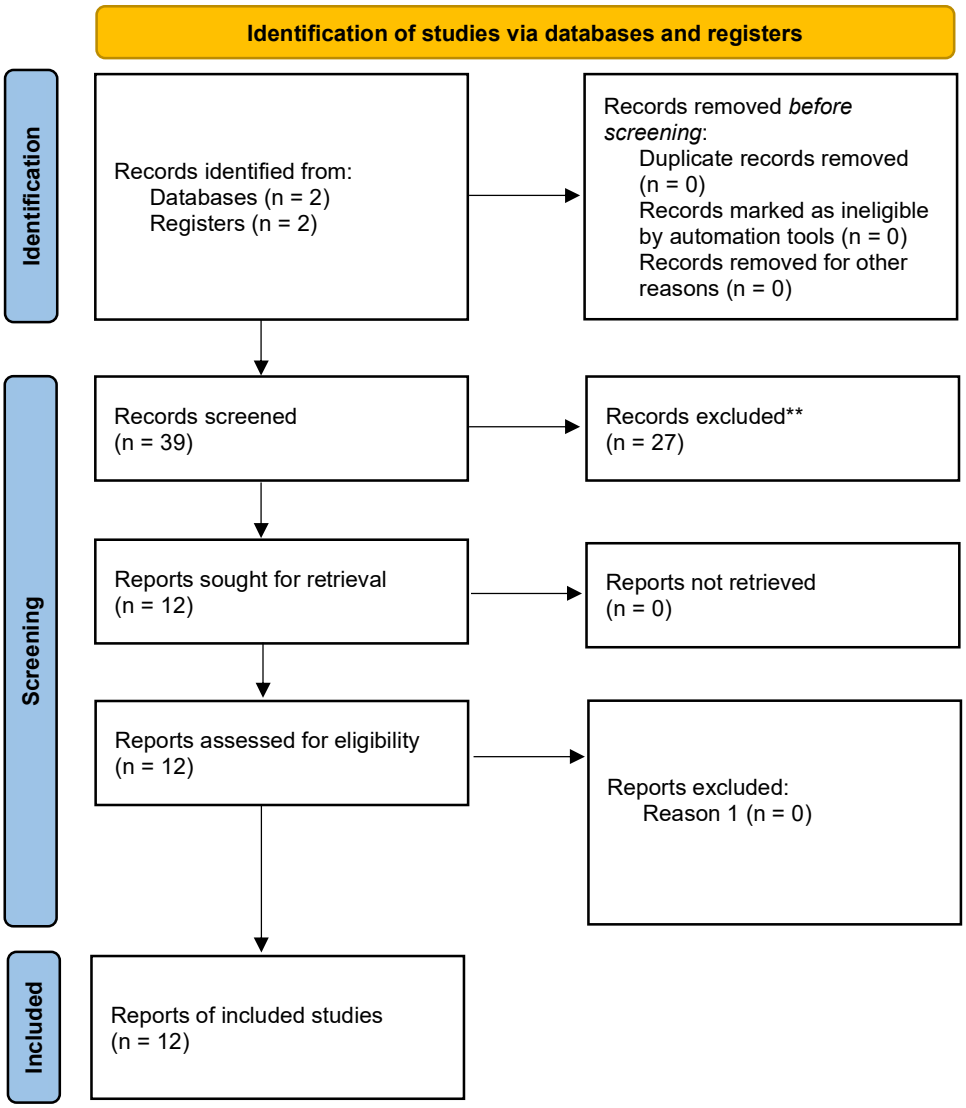
[27] M. P. A. Ahmed, “False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure.,” *Complex Adaptive Systems Modeling,* vol. 8, no. 1, p. 4, 2020.

Appendix)

Appendix 1) Prisma Review

Appendix 1.1) Prisma Review for Password Systems & Vulnerabilities:

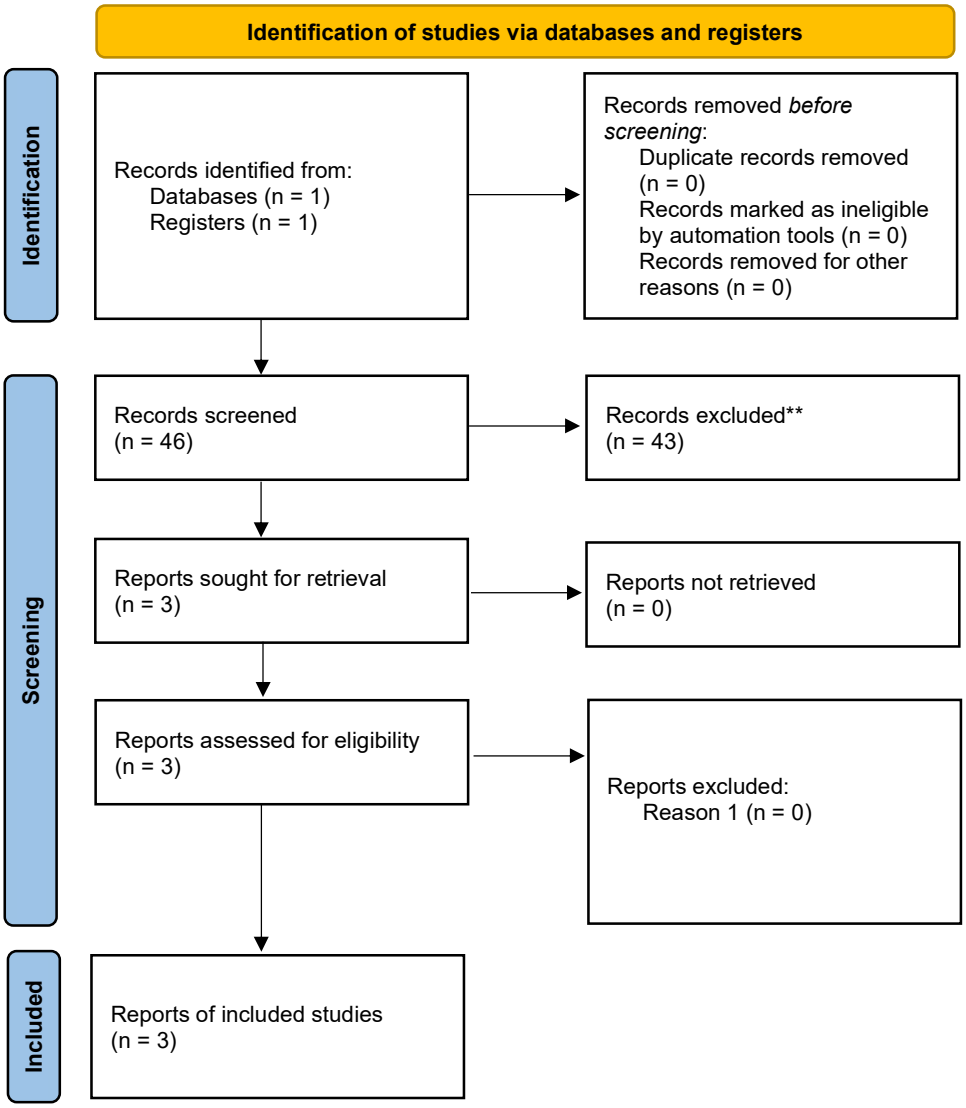
Performed using conditional keyword search with ACM and IEEE registries.
(("Abstract":"password") AND (("Abstract":"strength") OR ("Abstract":"checker")) AND (("Abstract":"weak") OR ("Abstract":"vunerability")))



Appendix 1.2) Vulnerability Assessment:

Performed using two key word searches in IEEE register.

1) ("Abstract":Vulnerability) AND ("Abstract":Assessment) AND ("Abstract":Password) AND ("Abstract":System) (11)
2) ("Abstract":Vulnerability) AND ("Abstract":Assessment) AND ("Abstract":Audit) (35)



Appendix 2) Testing Procedure Template:

Title:	**Number: #**	**Date Commenced:** dd/mm/yy
Planning Phase		
Scope:		
Motivation: Reference to relevant Resources:		
Expected Outcome/s:		
Implementation Phase:		
Test Overview:		
Initial Setup of Test: (Device and network configurations) Execution of Test: 1. … 2. …		
Evaluation Phase:		
Results:		
Calculated CVSS Score: Justification for Score:		
Future Directions:		