# GROUP 8

Dec 03, 2023

## PROJECT -TVRA REPORT

ISMAIL MAHAMED 125052191

JASKARAN SOHAL 150343218

RAYYAN KHAN 155534209

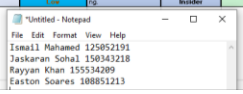
EASTON SOARES 108851213

# Table of Contents

# TVRA Report

## Introduction

Our network infrastructure is diligently segmented into zones that facilitate administrative efficiency, external web interaction, and overarching network management. In the face of persistent cyber threats, we continuously evaluate these zones to fortify our defenses. A prevalent concern is the vulnerability to SSH brute force attacks, a common yet critical security challenge that could compromise our network through widely utilized ports. The implications of such breaches are far-reaching, potentially causing operational interruptions, financial detriment, and reputational damage. This underscores the imperative for stringent security measures.



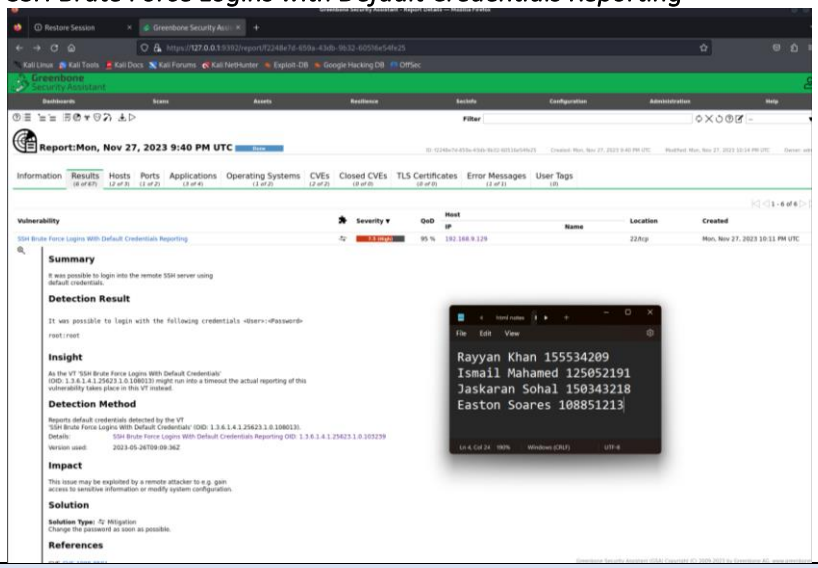
| Tool | Vulnerabilites | Vulnerability Descripti | Severity | Threat Event | Threat Sourc | Capability | Intent | Targeting | Relevance | elihood of Attack In | hood Initiated Attack | Overall Likelih | Impact | Risk |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| OpenVas | SSH Brute Force Logins With Default Credentials Reporting | It was possible to login into the remote SSH server using default credentials. | High | Conduct brute force login attempts/password guessing attacks | Insider | Low | Low | Very Low | Possible | High | High | High | High | High |
| OpenVas | SSH Brute Force Logins With Default Credentials Reporting | It was possible to login into the remote SSH server using default credentials. | High | login attempts/password guessing attacks | Insider | Low | Low | Very Low | Possible | High | High | High | High | High |
| OpenVas | SSH Brute Force Logins With Default Credentials Reporting | It was possible to login into the remote SSH server using default credentials. | High | login attempts/password guessing attacks | Insider | Low | Low | Very Low | Possible | High | High | High | High | High |
| OpenVas | SSH Brute Force Logins With Default Credentials Reporting | remote SSH server using default credentials. | High | login attempts/password guessing | Insider | Low | Low | Very Low | Possible | High | High | High | High | High |
| OpenVas | Missing Linux Kernel mitigations for 'MDS – Microarchitectural Data Sampling' hardware vulnerabilities | or more known mitigation(s) on Linux Kernel side for the referenced 'MDS - | Medium | or unauthorized information systems exposed to the Internet. | Insider | Low | Low | Very Low | Possible | Very Low | Low | Low | Low | Low |
| OpenVas | Missing Linux Kernel mitigations for 'MDS – Microarchitectural Data Sampling' hardware vulnerabilities | or more known mitigation(s) on Linux Kernel side for the | Medium | or unauthorized information systems | Insider | Low | Low | Very Low | Possible | Very Low | Low | Low | Low | Low |
| OpenVas | Missing Linux Kernel mitigations for 'MDS – Microarchitectural Data Sampling' hardware vulnerabilities | or more known mitigation(s) on Linux Kernel side for the | Medium | or unauthorized information systems | Insider | Low | Low | Very Low | Possible | Very Low | Low | Low | Low | Low |
| OpenVas | Missing Linux Kernel mitigations for 'MDS – Microarchitectural Data Sampling' hardware vulnerabilities | or more known mitigation(s) on Linux Kernel side for the referenced 'MDS - | Medium | or unauthorized information systems exposed to the Internet. | Insider | Low | Low | Very Low | Possible | Very Low | Low | Low | Low | Low |
| OpenVas | Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities | or more known mitigation(s) on | Medium | information via | Insider | Low | Low | Very Low | Possible | Very Low | Low | Low | Low | Low |
| OpenVas | Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities | or more known mitigation(s) on Linux Kernel side for the referenced 'Processor MMIO | Medium | Obtain sensitive information via exfiltration | Insider | Low | Low | Very Low | Possible | Very Low | Low | Low | Low | Low |
| OpenVas | Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities | or more known mitigation(s) on Linux Kernel side for the referenced 'Processor MMIO Stale Data' hardware | Medium | Conduct brute force login attempts/password guessing attacks | Insider | Low | Low | Very Low | Possible | Very Low | Low | Low | Low | Low |
| OpenVas | Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware vulnerabilities | or more known mitigation(s) on Linux Kernel side for the referenced 'Processor MMIO Stale Data' hardware vulnerabilities. | Medium | Obtain sensitive information via exfiltration | Insider | Low | Low | Very Low | Possible | Very Low | Low | Low | Low | Low |
| Nessus | HTTP TRACE / TRACK Methods Allowed | the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. | Low | Craft phishing attacks. | Insider | Low | Low | Very Low | Possible | Very Low | Low | Low | Low | Low |
| Nessus | SMB Signing not required | remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle | Medium | Craft phishing attacks. | Insider | Low | Low | Very Low | Possible | Very Low | Low | Low | Low | Low |
| Nessus | HTTP TRACE / TRACK Methods Allowed | The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. | Low | Perform perimeter network reconnaissance/scanning. | Insider | Low | Low | Very Low | Possible | Very Low | Low | Low | Low | Low |

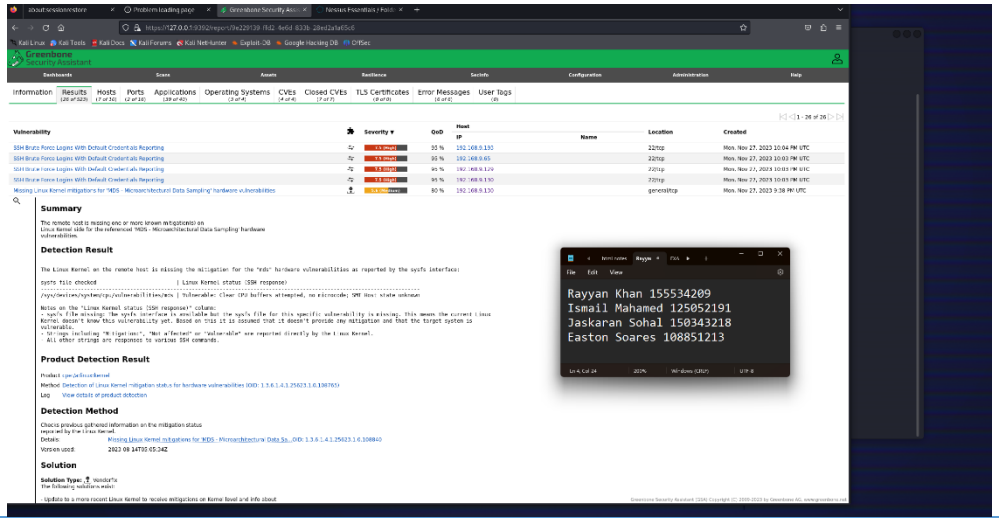
Ismail Mahamed 125052191
Jaskaran Sohal 150343218
Rayyan Khan 155534209
Easton Soares 108851213

This TVRA delves into the SSH vulnerability, among others, assessing not only the technical risks but also the associated business impacts. Should such vulnerabilities be exploited, the resulting damage could span from tangible operational halts to intangible losses of stakeholder trust. Our comprehensive analysis is designed to steer the development of a robust mitigation strategy to bolster network resilience and ensure business continuity.

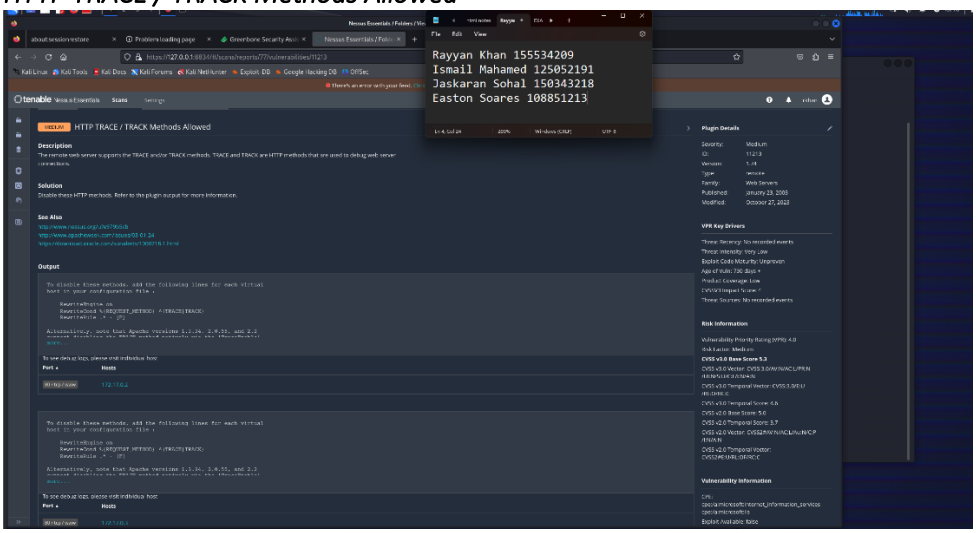
For a detailed account of our security posture, the vulnerabilities we face, and the strategies recommended to address these challenges, please refer to the full report below.

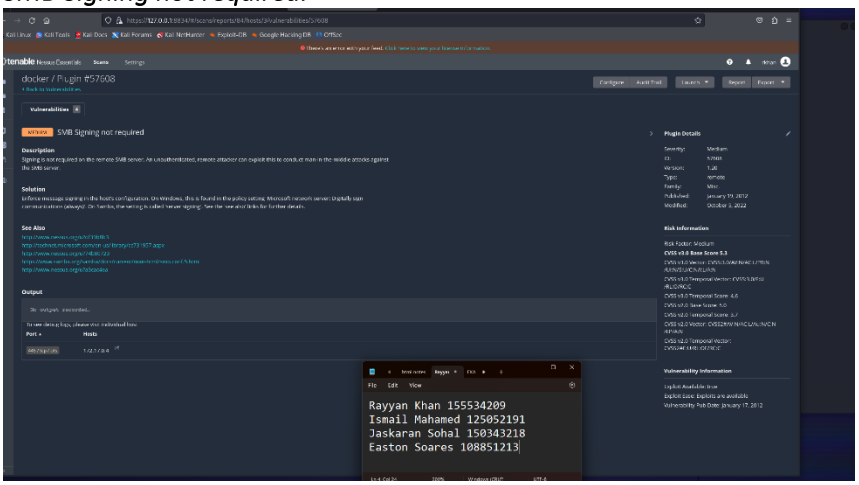
## Vulnerabilities

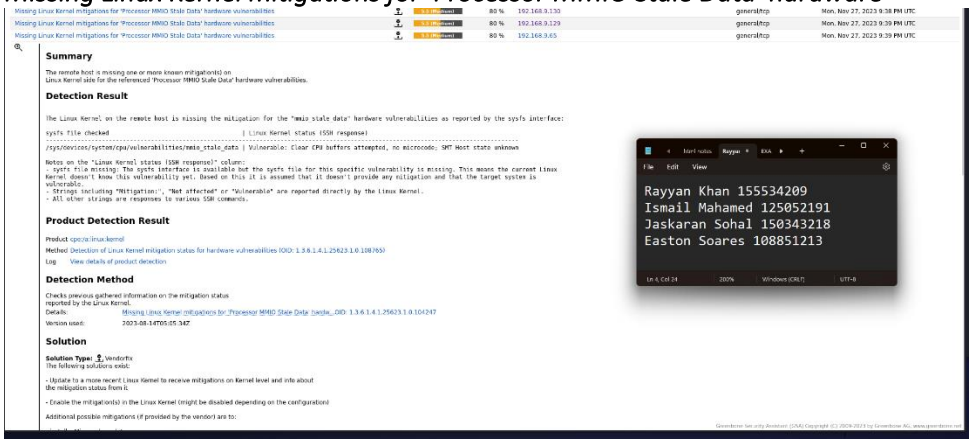
| | |
|---|---|
| Vulnerability | *SSH Brute Force Logins with Default Credentials Reporting*   |
| Vulnerability Description | It was possible to login into the remote SSH server using default credentials. |
| *Vulnerability Severity* | High |
| Level of Impact | High |
| Overall Likelihood | High |
| Risk | High |
| Business Impact | A successful attack could lead to operational disruptions and financial losses due to data breaches or system outages. Reputation damage and legal penalties due to non-compliance with regulations could also occur. |
| Mitigation | Implement strong, unique passwords, disable default accounts, and enforce account lockout policies. Regularly audit and monitor SSH logs. |

| | |
|---|---|
| *Vulnerability* | Missing Linux Kernel mitigations for 'MDS- Microarchitectural Data Sampling' hardware vulnerabilities   |

| | |
|---|---|
| *Vulnerability Description* | The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'MDS - Microarchitectural Data Sampling' hardware vulnerabilities. |
| *Vulnerability Severity* | Medium |
| *Level of Impact* | Low |
| *Overall Likelihood* | Low |
| *Risk* | Low |
| *Business Impact* | Exposure of sensitive data could result in intellectual property theft, customer trust erosion, and legal ramifications. |
| *Mitigation* | Apply the latest kernel patches and updates and check for microcode updates from hardware vendors. |

| | |
|---|---|
| *Vulnerability* | ***HTTP TRACE / TRACK Methods Allowed***   |
| *Vulnerability Description* | The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. |
| *Vulnerability Severity* | Low |
| *Level of Impact* | Low |
| *Overall Likelihood* | Low |
| *Risk* | Low |
| *Business Impact* | Disclosure of internal network details could aid further attacks, leading to website compromise and undermining customer confidence in web services security. |
| *Mitigation* | Disable HTTP TRACE and TRACK methods on web servers and configure them to reject such requests. |

| | |
|---|---|
| *Vulnerability* | ***SMB Signing not required.***   |
| *Vulnerability Description* | The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. |
| *Vulnerability Severity* | Medium |
| *Level of Impact* | Low |
| *Overall Likelihood* | Low |
| *Risk* | Low |
| *Business Impact* | Compromise of data integrity and potential operational sabotage could cause critical business processes to cease, incurring financial and operational losses. |
| *Mitigation* | Enforce SMB signing on all devices to ensure data integrity and prevent unauthorized access. |

| | |
|---|---|
| *Vulnerability* | ***Missing Linux Kernel mitigations for 'Processor MMIO Stale Data' hardware***   |
| *Vulnerability Description* | is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'Processor MMIO Stale Data' hardware vulnerabilities. |
| *Vulnerability Severity* | Medium |

| | |
|---|---|
| *Level of Impact* | Low |
| *Overall Likelihood* | Low |
| *Risk* | Low |
| *Business Impact* | This vulnerability could result in unauthorized access to critical data, leading to operational disruptions, financial losses, and reputational damage. |
| *Mitigation* | Apply the latest kernel patches and updates addressing 'Processor MMIO Stale Data' vulnerabilities. Regularly check for and apply microcode updates provided by hardware vendors. |

## Mitigation Strategies

This section is an overview of mitigations required to mitigate the vulnerabilities listed above.

- Strengthen passwords and disable default accounts.
- Enforce account lockout policies and monitor SSH logs.
- Apply kernel patches and hardware microcode updates.
- Disable HTTP TRACE and TRACK methods on web servers.
- Enforce SMB signing to ensure data integrity and security of SMB traffic.
- Apply kernel patches addressing 'Processor MMIO Stale Data' vulnerabilities.

## Conclusion

Addressing the identified vulnerabilities is imperative for maintaining network integrity and security. The business impacts highlight the necessity for a proactive security approach and continuous adaptation to evolving threats. Implementing regular updates, monitoring, and adhering to security best practices is crucial for a robust defense mechanism. We recommend prioritizing mitigations based on the severity of business impacts and updating business continuity plans to manage these risks effectively.