



ILLUSTRATIVE SAMPLE REPORT

External Penetration Test

Executive Summary

Sample Environment

Original sample assessment: August 4, 2025

Illustrative findings supplied for demonstration only.

Not a Massive IT client assessment or evidence of client outcomes.

Branding and vendor-specific technical labels have been adapted;
sample findings, dates, and page numbering have been retained.

Massive IT

www.massiveit.com | sales@massiveit.com

(813) 518-5454 | Tampa, Florida | Nationwide service

SAMPLE ONLY - Not a security assessment of your organization.

Summary

Started	Aug 04, 2025, 1:14 PM UTC	Initiated by	Massive IT	Scanner IP	104.236.72.193
Completed	Aug 04, 2025, 4:53 PM UTC	For client	Sample Account	Hosts Assessed	15
Duration	3h 39m				

**111**
Attack Paths Exploited

**157**
Weaknesses Found

**64**
Credentials Compromised

**10**
Hosts Compromised

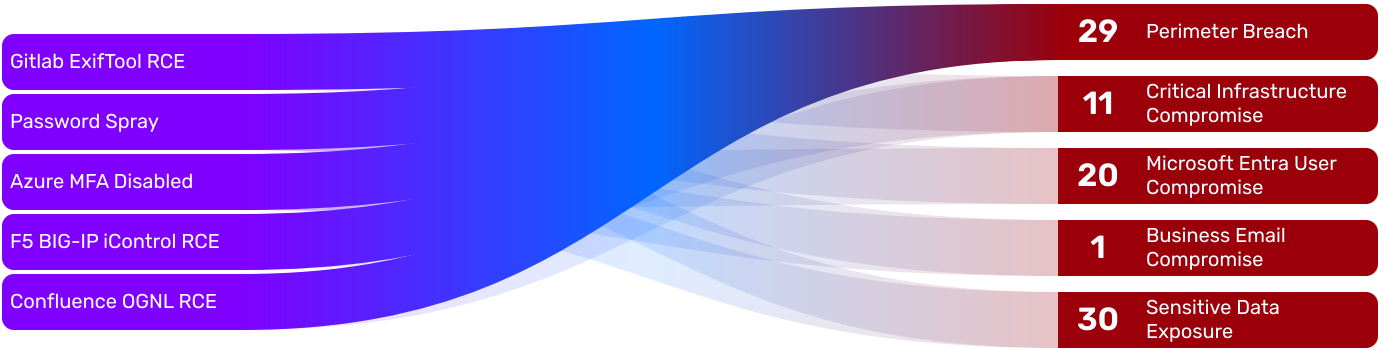
Overall Exposure Level: Critical

This exposure level stems from finding and exploiting **critical weaknesses** affecting external assets, leading to **Perimeter Breach, Critical Infrastructure Compromise, and Business Email Compromise**.

To reduce the exposure level, remediate the weaknesses that led to the greatest impacts. To further improve cyber resilience, implement the security policy recommendations provided to address any systemic issues affecting the external assets as a whole.



Top Business Risks and Impacts

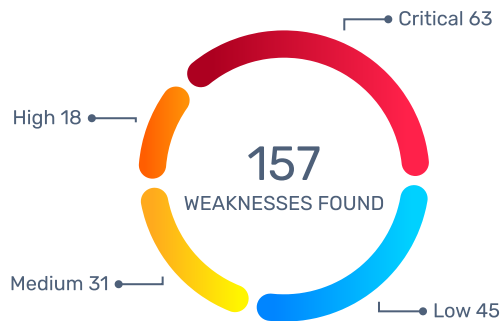


Perimeter breach can lead to attackers gaining access to your internal network from the public internet.

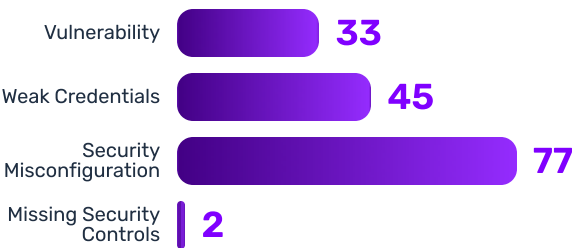
Top impacts found along the 111 attack paths exploited during the pentest:

- Critical Infrastructure Compromise:** Discovered and exploited vulnerabilities affecting GitLab on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) port 8080, Atlassian Confluence on 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com) port 8090, and 5 other critical assets. These assets are critical infrastructure that provide attackers with a privileged position in the network from which they can access a wealth of sensitive data and launch further attacks.
- Perimeter Breach:** Discovered and exploited critical vulnerabilities that could allow attackers to breach the perimeter of your network on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com), 3.91.156.158 (ec2-3-91-156-158.compute-1.amazonaws.com), and 12 other hosts. Perimeter breach can lead to attackers gaining access to your internal network from the public internet.
- Business Email Compromise:** Compromised the email account 79c1f87so8@pod02.example.com. Business email compromise enables attackers to send and receive emails under the guise of that user. Attackers commonly leverage email access to conduct business accounting fraud, conduct highly targeted phishing attacks, gain access to sensitive information, and elicit trusting coworkers to perform actions on their behalf.

Top Weaknesses



WEAKNESSES BY CATEGORY



Fix the weaknesses from the most impactful weakness types found during the pentest:

- 1. **CVE-2021-22205: Gitlab ExifTool RCE** affecting application GitLab on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) port 8080 and application GitLab on 184.73.131.205 (ec2-184-73-131-205.compute-1.amazonaws.com) port 8080. Unauthenticated attackers can exploit this vulnerability to run arbitrary commands as the git user on the Gitlab host. The weakness was leveraged in **2 attack paths** leading to **Critical Infrastructure Compromise and Perimeter Breach**.
- 2. **PT-2021-0019: Password Spray** affecting the credential for Microsoft Entra user kionbobwe2@pod16.example.com in Microsoft Entra tenant d6e507ea-d3cb-442f-8c56-94142f3ddd15 and 54 other credentials. An attacker can openly maneuver throughout an environment and access information if a password is compromised. The weakness was leveraged in **25 attack paths** leading to **Business Email Compromise, Microsoft Entra User Compromise, Perimeter Breach, and Sensitive Data Exposure**.
- 3. **PT-2022-0002: Azure MFA Disabled** affecting the credential for Microsoft Entra user kionbobwe2@pod16.example.com in Microsoft Entra tenant d6e507ea-d3cb-442f-8c56-94142f3ddd15 and 53 other credentials. This misconfiguration permits remote attackers to conduct credential attacks like password spraying to compromise an account and using it to further compromise an organization. The weakness was leveraged in **25 attack paths** leading to **Business Email Compromise, Microsoft Entra User Compromise, Perimeter Breach, and Sensitive Data Exposure**.

Systemic Issues

Issue	Policy Recommendation
Critical Vulnerabilities 10 Hosts that the test compromised via CISA known exploited vulnerabilities.	Improve Vulnerability Management Known exploited vulnerabilities should be patched or mitigated in an efficient manner to make it harder for attackers to achieve initial access or move laterally through an environment.
Inadequate Endpoint Security Controls 4 Credentials that the test acquired from OS credential dumping	Tune Endpoint Security Controls An Endpoint Detection and Reponse (EDR) solution should be deployed to every endpoint and tuned to prevent common attacker methods for harvesting credentials such as dumping LSASS, LSA, and SAM.

Issue	Policy Recommendation
Missing Multi-Factor Authentication (MFA) 1 User(s) whose Microsoft365 e-mail inboxes were compromised by The test	Enable MFA for Microsoft365 Multi-Factor Authentication (MFA) should be enabled for all Microsoft365 users to make it difficult for attackers to take over accounts, compromise business email, access sensitive data, and conduct lateral phishing attacks.

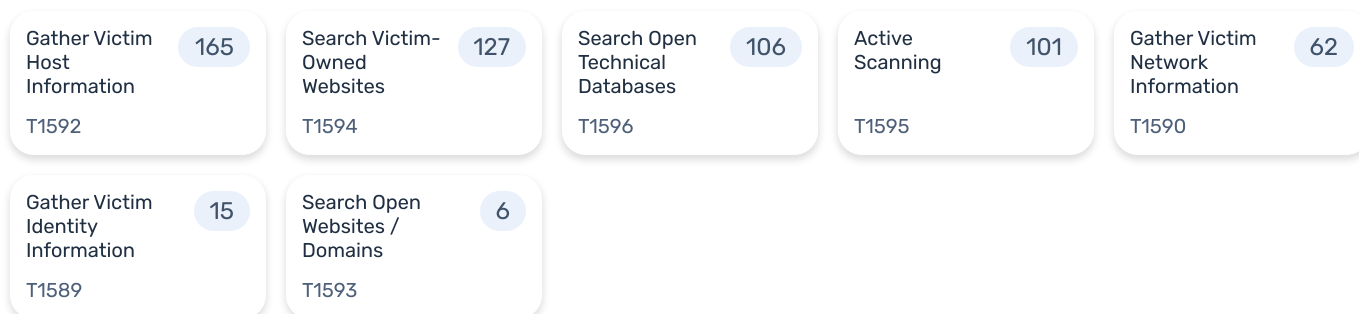
The test identified important systemic issues affecting the overall environment. Addressing these issues will improve the environment's resilience to future cyber attacks.

1. **Critical Vulnerabilities:** the test compromised 10 hosts via CISA known exploited vulnerabilities. Known exploited vulnerabilities should be patched or mitigated in an efficient manner to make it harder for attackers to achieve initial access or move laterally through an environment.
2. **Inadequate Endpoint Security Controls:** the test acquired 4 credentials from OS credential dumping. An Endpoint Detection and Reponse (EDR) solution should be deployed to every endpoint and tuned to prevent common attacker methods for harvesting credentials such as dumping LSASS, LSA, and SAM.
3. **Missing Multi-Factor Authentication (MFA):** the test compromised the Microsoft365 e-mail inboxes of 1 user(s). Multi-Factor Authentication (MFA) should be enabled for all Microsoft365 users to make it difficult for attackers to take over accounts, compromise business email, access sensitive data, and conduct lateral phishing attacks.

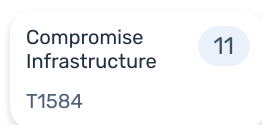
MITRE

This diagram illustrates the actions of the test, as they pertain to MITRE tactics and techniques. Each tile indicates how many attack modules were used for a given technique during the pentest. A total of **3,210 attack modules** employed **51 techniques** across **11 MITRE tactics**.

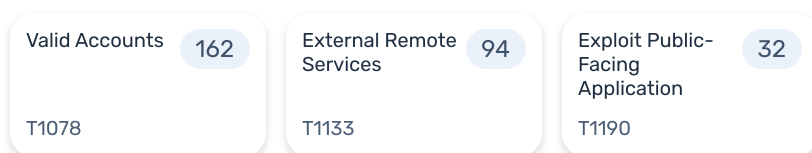
Reconnaissance



Resource Development



Initial Access



Execution

Command and Scripting Interpreter

30

T1059

Privilege Escalation

Exploitation for Privilege Escalation

1

T1068

Abuse Elevation Control Mechanism

1

T1548

Credential Access

Unsecured Credentials

564

T1552

Brute Force

103

T1110

OS Credential Dumping

12

T1003

Exploitation for Credential Access

8

T1212

Credentials from Password Stores

2

T1555

Steal Application Access Token

1

T1528

Discovery

Account Discovery

377

T1087

Network Service Scanning

201

T1046

Permission Groups Discovery

193

T1069

Software Discovery

125

T1518

Container and Resource Discovery

102

T1613

Cloud Infrastructure Discovery

91

T1580

Cloud Service Discovery

22

T1526

System Information Discovery

15

T1082

Remote System Discovery

14

T1018

Cloud Storage Object Discovery

4

T1619

System Network Connections Discovery

2

T1049

System Owner / User Discovery

2

T1033

File and Directory Discovery

1

T1083

System Service Discovery

1

T1007

System Network Configuration Discovery

1

T1016

Process Discovery

1

T1057

Lateral Movement

Remote Services

115

T1021

Exploitation of Remote Services

31

T1210

Use Alternate Authentication Material

6

T1550

Collection

Data from
Cloud Storage
Object

152

T1530

Screen Capture

111

T1113

Data from
Information
Repositories

16

T1213

Data from
Configuration
Repository

2

T1602

Data from Local
System

1

T1005

Data from
Network Shared
Drive

1

T1039

Email Collection

1

T1114

Command and Control

Non-Application
Layer Protocol

7

T1095

Application Layer
Protocol

6

T1071

Impact

Data Manipulation

3

T1565

Account Access
Removal

2

T1531

Defacement

1

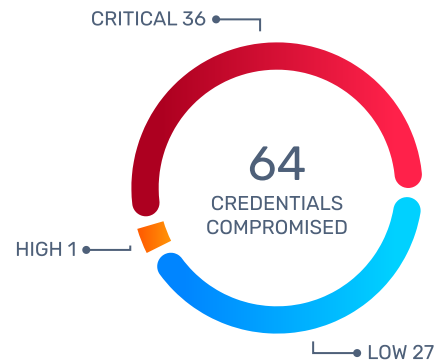
T1491

Top Credentials

9.8
CRITICAL **79c1f87so81262**
ENTRA USER

9.8
CRITICAL **kionbobwe2**
ENTRA USER

9.8
CRITICAL **79c1f87so8**
ENTRA USER



As illustrated by severity, the pentest discovered **64 credentials** in total, with **36 CRITICAL credentials**. The most impactful credentials likely contribute to the most critical attack paths.