Sahin Security Institute

2022 Security Assessment Report Prepared For

ARTEMIS GAS, INC.

September 9, 2022

## Confidentiality Notice

*This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to Artemis Gas Inc. or facilitate attacks against Artemis Gas Inc. Sahin Security Institute shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.*

## Disclaimer

*Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on Artemis Gas Inc. ’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.*

**TABLE OF CONTENTS**

[Confidentiality Notice](#_heading=h.1fob9te) 2

[Disclaimer](#_heading=h.3znysh7) 2

[**EXECUTIVE SUMMARY**](#_heading=h.tyjcwt)4

[Oracle WebLogic and Microsoft Exchange Server Vulnerabilities Recommendation](#_heading=h.3dy6vkm) 4

[**HIGH LEVEL ASSESSMENT OVERVIEW**](#_heading=h.1t3h5sf)5

[Areas for Improvement](#_heading=h.17dp8vu) 5

[Recommendations](#_heading=h.3rdcrjn) 5

[**SCOPE**](#_heading=h.44sinio)7

[**TESTING METHODOLOGY**](#_heading=h.fdv58q820f68)7

[**CLASSIFICATION DEFINITIONS**](#_heading=h.1ci93xb)9

[Risk Classifications](#_heading=h.3whwml4) 9

[Exploitation Likelihood Classifications](#_heading=h.2bn6wsx) 9

[Business Impact Classifications](#_heading=h.qsh70q) 10

[Remediation Difficulty Classifications](#_heading=h.3as4poj) 10

[**ASSESSMENT FINDINGS**](#_heading=h.49x2ik5)11

[**TECHNICAL FINDINGS SUMMARY**](#_heading=h.bstd5volosz0)12

[**APPENDIX A - TOOLS USED**](#_heading=h.2p2csry)20

# 

# EXECUTIVE SUMMARY

Sahin Security Institute, performed a security assessment of the internal corporate network of Artemis Gas Inc. on September 9, 2022. Sahin Security Institute ’s penetration test simulated an attack from an external threat actor attempting to gain access to systems within the Artemis Gas Inc. corporate network. The purpose of this assessment was to discover and identify vulnerabilities in Artemis Gas Inc. ’s infrastructure and suggest methods to remediate the vulnerabilities. Sahin Security Institute identified a total of 2 Critical- and 7 High vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

| **CRITICAL** | **HIGH** | **MEDIUM** | **LOW** |
| --- | --- | --- | --- |
| **2** | **7** | **N/A** | **N/A** |

The highest severity vulnerabilities give potential attackers the opportunity to unauthenticated network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. The Microsoft Exchange server attack chain begins with the exploration of this flaw, also known as a server-side-request-forgery (SSRF) vulnerability. When exploited, HTTPS connections are established to authenticate user access. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

## Oracle WebLogic and Microsoft Exchange Server Vulnerabilities Recommendation

It is imperative that you update or mitigate your affected Exchange deployments immediately.

From Network layer:

* Segment remote resource access functionality in separate networks to reduce the impact of SSRF
* Enforce “deny by default” firewall policies or network access control rules to block all but essential intranet traffic.

~ Establish ownership and a lifecycle for firewall rules based on applications.

~ Log all accepted and blocked network flows on firewalls (see A09:2021-Security Logging and Monitoring Failures).

From Application layer:

* Sanitize and validate all client-supplied input data
* Enforce the URL schema, port, and destination with a positive allow list
* Do not send raw responses to clients
* Disable HTTP redirections
* Be aware of the URL consistency to avoid attacks such as DNS rebinding and “time of check, time of use” (TOCTOU) race conditions

Do not mitigate SSRF via the use of a deny list or regular expression. Attackers have payload lists, tools, and skills to bypass deny lists.

# HIGH LEVEL ASSESSMENT OVERVIEW

## Areas for Improvement

Sahin Security Institute recommends Artemis Gas Inc. takes the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack Artemis Gas Inc. ’s information systems and/or reduce the impact of a successful attack.

### Recommendations

Sahin Security Institute recommends Artemis Gas Inc. take the following actions as soon as possible to minimize business risk.

Oracle WebLogic Server

Organizations running Oracle WebLogic Server should patch as quickly as possible. Those that are waiting for a yet-to-occur patch cycle to address CVE-2020-14882 would be well advised to break that cycle in favor of patching as soon as they can. Organizations that are unable to patch immediately should consider the following recommendations as partial mitigations, with the understanding that no mitigation is as effective as patching:

-Ensure the admin portal is not exposed to the public internet; blocking access to the admin portal (TCP port 7001 by default) may act as a partial mitigation until CVE-2020-14882 can be patched.

-Review application logs for HTTP requests that include the double-encoded path traversal %252E%252E%252F and the admin portal console.portal in the request URI.

-Monitor network traffic for suspicious HTTP requests if you have the ability to do so.

-Monitor for any suspicious processes created by the application, such as cmd.exe or /bin/sh.

Microsoft Exchange Server

This vulnerability is part of an attack chain. The initial attack requires the ability to make an untrusted connection to Exchange server port 443. This can be protected against by restricting untrusted connections, or by setting up a VPN to separate the Exchange server from external access. Using this mitigation will only protect against the initial portion of the attack. Other portions of the chain can be triggered if an attacker already has access or can convince an administrator to open a malicious file.

We recommend prioritizing installing updates on Exchange Servers that are externally facing.

# 

# SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

Assessment Scope

| **Target** | **Description** |
| --- | --- |
| Network | X |
| Servers | x |

# 

# TESTING METHODOLOGY

Sahin Security Institute’s testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about Artemis Gas Inc.’s network systems. Sahin Security Institute used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. Sahin Security Institute simulated an attacker exploiting vulnerabilities in the Artemis Gas Inc. network. Sahin Security Institute gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology.

# 

# CLASSIFICATION DEFINITIONS

## Risk Classifications

| **Level** | **Score** | **Description** |
| --- | --- | --- |
| **Critical** | **10** | The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed. |
| **High** | **7-9** | The vulnerability poses an urgent threat to the organization, and remediation should be prioritized. |
| **Medium** | **4-6** | Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible. |
| **Low** | **1-3** | The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible. |
| **Informational** | **0** | These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company. |

## Exploitation Likelihood Classifications

| **Likelihood** | **Description** |
| --- | --- |
| **Likely** | Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty. |
| **Possible** | Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation. |
| **Unlikely** | Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation. |

## Business Impact Classifications

| **Impact** | **Description** |
| --- | --- |
| **Major** | Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage. |
| **Moderate** | Successful exploitation may cause significant disruptions to non-critical business functions. |
| **Minor** | Successful exploitation may affect few users, without causing much disruption to routine business functions. |

## Remediation Difficulty Classifications

| **Difficulty** | **Description** |
| --- | --- |
| **Hard** | Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions. |
| **Moderate** | Remediation may require minor reconfigurations or additions that may be time-intensive or expensive. |
| **Easy** | Remediation can be accomplished in a short amount of time, with little difficulty. |

## 

# ASSESSMENT FINDINGS

| **Number** | **Finding** | **Risk Score** | **Risk** |
| --- | --- | --- | --- |
| 1 | Oracle WebLogic Server vulnerable to CVE-2020-14882 | **9.8** | **Critical** |
| 2 | Microsoft Exchange Server vulnerable to CVE-2021-26855 | **9.8** | **Critical** |
| 3 | Web application is vulnerable to SQL Injection | **8.8** | **High** |
| 4 | Default password on Cisco admin portal | **8.8** | **High** |
| 5 | Apache web server vulnerable to CVE-2019-0211 | **7.8** | **High** |
| 6 | Unpatched RDP is exposed to the internet | **7.5** | **High** |
| 7 | Web server is exposing sensitive data | **7.5** | **High** |
| 8 | Web application has broken access control | **7.5** | **High** |
| 9 | Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions) | **7.5** | **High** |

# TECHNICAL FINDINGS SUMMARY

**1 - Oracle WebLogic Server vulnerable to CVE-2020-14882**

| **Critical (9/10)** | |
| --- | --- |
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.

**Analysis**

Vendor: Oracle Corporation

Product: WebLogic Server

Versions Affected:

=10.3.6.0.0: affects 10.3.6.0.0

=12.1.3.0.0: affects 12.1.3.0.0

=12.2.1.3.0: affects 12.2.1.3.0

=12.2.1.4.0: affects 12.2.1.4.0

=14.1.1.0.0: affects 14.1.1.0.0

**Recommendations**

Oracle strongly recommends that customers apply security patches as soon as possible.

**References**

* [**https://www.oracle.com/security-alerts/cpuoct2020.html**](https://www.oracle.com/security-alerts/cpuoct2020.html)
* [**http://packetstormsecurity.com/files/159769/Oracle-WebLogic-Server-Remote-Code-Execution.html**](http://packetstormsecurity.com/files/159769/Oracle-WebLogic-Server-Remote-Code-Execution.html)
* [**http://packetstormsecurity.com/files/160143/Oracle-WebLogic-Server-Administration-Console-Handle-Remote-Code-Execution.html**](http://packetstormsecurity.com/files/160143/Oracle-WebLogic-Server-Administration-Console-Handle-Remote-Code-Execution.html)
* [**http://packetstormsecurity.com/files/161128/Oracle-WebLogic-Server-12.2.1.0-Remote-Code-Execution.html**](http://packetstormsecurity.com/files/161128/Oracle-WebLogic-Server-12.2.1.0-Remote-Code-Execution.html)

**2 - Microsoft Exchange Server vulnerable to CVE-2021-26855**

| **Critical (9/10)** | |
| --- | --- |
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

Remote Code Execution

**Analysis**

Vendor: Microsoft

Product: Microsoft Exchange Server 2016 Cumulative Update 19

Product: Microsoft Exchange Server 2019 Cumulative Update 8

Product: Microsoft Exchange Server 2013

Versions Affected:

Cumulative Update 23

Product: Microsoft Exchange Server 2016 Cumulative Update 14

Product: Microsoft Exchange Server 2019 Cumulative Update 4

Product: Microsoft Exchange Server 2016 Cumulative Update 15

Product: Microsoft Exchange Server 2019 Cumulative Update 5

Product: Microsoft Exchange Server 2019 Cumulative Update 6

Product: Microsoft Exchange Server 2016 Cumulative Update 16

Product: Microsoft Exchange Server 2019 Cumulative Update 7

Product: Microsoft Exchange Server 2016 Cumulative Update 18

**Recommendations**

This vulnerability is part of an attack chain. The initial attack requires the ability to make an untrusted connection to Exchange server port 443. This can be protected against by restricting untrusted connections, or by setting up a VPN to separate the Exchange server from external access. Using this mitigation will only protect against the initial portion of the attack. Other portions of the chain can be triggered if an attacker already has access or can convince an administrator to open a malicious file.

We recommend prioritizing installing updates on Exchange Servers that are externally facing.

**References**

* [**https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855**](https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855)
* [**http://packetstormsecurity.com/files/161846/Microsoft-Exchange-2019-SSRF-Arbitrary-File-Write.html**](http://packetstormsecurity.com/files/161846/Microsoft-Exchange-2019-SSRF-Arbitrary-File-Write.html)
* [**http://packetstormsecurity.com/files/161938/Microsoft-Exchange-ProxyLogon-Remote-Code-Execution.html**](http://packetstormsecurity.com/files/161938/Microsoft-Exchange-ProxyLogon-Remote-Code-Execution.html)
* [**http://packetstormsecurity.com/files/162610/Microsoft-Exchange-2019-Unauthenticated-Email-Download.html**](http://packetstormsecurity.com/files/162610/Microsoft-Exchange-2019-Unauthenticated-Email-Download.html)
* [**http://packetstormsecurity.com/files/162736/Microsoft-Exchange-ProxyLogon-Collector.html**](http://packetstormsecurity.com/files/162736/Microsoft-Exchange-ProxyLogon-Collector.html)

**3 - Web application is vulnerable to SQL Injection**

| **HIGH RISK (7/9)** | |
| --- | --- |
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

**Analysis**

Vendor: Not Specified

Product: Forma

Versions Affected:

Forma LMS 2.2.1

**Recommendations**

If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.

Process SQL queries using prepared statements, parameterized queries, or stored procedures. These features should accept parameters or variables and support strong typing. Do not dynamically construct and execute query strings within these features using "exec" or similar functionality, since this may re-introduce the possibility of SQL injection. [REF-867]

**References**

* [**https://talosintelligence.com/vulnerability\_reports/TALOS-2019-0903**](https://talosintelligence.com/vulnerability_reports/TALOS-2019-0903)

**4 - Default password on Cisco admin portal**

| **HIGH RISK (7/9)** | |
| --- | --- |
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

Insecure Default Password Vulnerability

**Analysis**

Vendor: Not Specified

Product: Cisco Ultra Services Framework Element Manager

Versions Affected:

Cisco Ultra Services Framework Element Manager

**Recommendations**

We recommend to change the default password on all devices.

**References**

* [**http://www.securityfocus.com/bid/98981**](http://www.securityfocus.com/bid/98981)
* [**https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usf5**](https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-usf5)

**5 - Apache web server vulnerable to CVE-2019-0211**

| **HIGH RISK (7/9)** | |
| --- | --- |
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

Apache HTTP Server privilege escalation from modules' scripts

**Analysis**

Vendor: Apache

Product: Apache HTTP Server

Versions Affected:

2.4.17 to 2.4.38

**Recommendations**

All http users running MPM event, worker or prefork should upgrade to

2.4.39 or later.

**References**

* [**http://www.openwall.com/lists/oss-security/2019/04/02/3**](http://www.openwall.com/lists/oss-security/2019/04/02/3)
* [**http://www.securityfocus.com/bid/107666**](http://www.securityfocus.com/bid/107666)
* [**https://seclists.org/bugtraq/2019/Apr/5**](https://seclists.org/bugtraq/2019/Apr/5)
* [**https://www.synology.com/security/advisory/Synology\_SA\_19\_14**](https://www.synology.com/security/advisory/Synology_SA_19_14)
* [**http://packetstormsecurity.com/files/152386/Apache-2.4.38-Root-Privilege-Escalation.html**](http://packetstormsecurity.com/files/152386/Apache-2.4.38-Root-Privilege-Escalation.html)
* [**https://usn.ubuntu.com/3937-1/**](https://usn.ubuntu.com/3937-1/)
* [**https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WETXNQWNQLWHV6XNW6YTO5UGDTIWAQGT/**](https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WETXNQWNQLWHV6XNW6YTO5UGDTIWAQGT/)

**6 - Unpatched RDP is exposed to the internet**

| **HIGH RISK (7/9)** | |
| --- | --- |
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

CWE-287: Improper Authentication

**Analysis**

Vendor: FreeRDP

Product: FreeRDP

Versions Affected:

< 2.7.0

**Recommendations**

Update to 2.7.0.

**References**

* [**https://github.com/FreeRDP/FreeRDP/releases/tag/2.7.0**](https://github.com/FreeRDP/FreeRDP/releases/tag/2.7.0)
* [**https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6x5p-gp49-3jhh**](https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-6x5p-gp49-3jhh)
* [**https://github.com/FreeRDP/FreeRDP/pull/7750**](https://github.com/FreeRDP/FreeRDP/pull/7750)
* [**https://gitlab.gnome.org/GNOME/gnome-remote-desktop/-/issues/95**](https://gitlab.gnome.org/GNOME/gnome-remote-desktop/-/issues/95)
* [**https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AELSWWBAM2YONRPGLWVDY6UNTLJERJYL/**](https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/AELSWWBAM2YONRPGLWVDY6UNTLJERJYL/)
* [**https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/DOYKBQOHSRM7JQYUIYUWFOXI2JZ2J5RD/**](https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/DOYKBQOHSRM7JQYUIYUWFOXI2JZ2J5RD/)
* [**https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/PZWR6KSIKXO4B2TXBB3WH6YTNYHN46OY/**](https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/PZWR6KSIKXO4B2TXBB3WH6YTNYHN46OY/)

**7 - Web server is exposing sensitive data**

| **HIGH RISK (7/9)** | |
| --- | --- |
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

Intuit Lacerte 2017 for Windows in a client/server environment transfers the entire customer list in cleartext over SMB, which allows attackers to (1) obtain sensitive information by sniffing the network or (2) conduct man-in-the-middle (MITM) attacks via unspecified vectors.

**Recommendations**

Configure servers to use encrypted channels for communication, which may include SSL or other secure protocols.

**References**

* [**https://corporateblue.com/your-taxes-are-being-leaked/**](https://corporateblue.com/your-taxes-are-being-leaked/)
* [**https://www.themikewylie.com/intuit-lacerte-vulnerability-and-data-exposure-cve-2018-11338-cve-2018-14833/**](https://www.themikewylie.com/intuit-lacerte-vulnerability-and-data-exposure-cve-2018-11338-cve-2018-14833/)

**8 - Web application has broken access control**

| **HIGH RISK (7/9)** | |
| --- | --- |
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources.

**Recommendations**

Divide the software into anonymous, normal, privileged, and administrative areas. Identify which of these areas require a proven user identity, and use a centralized authentication capability.

**References**

* [**https://www.ftc.gov/system/files/documents/cases/dlink\_proposed\_order\_and\_judgment\_7-2-19.pdf**](https://www.ftc.gov/system/files/documents/cases/dlink_proposed_order_and_judgment_7-2-19.pdf)
* [**https://www.dlink.com/en/security-bulletin**](https://www.dlink.com/en/security-bulletin)
* [**https://github.com/0x8b30cc/DSL-2680-Multiple-Vulnerabilities**](https://github.com/0x8b30cc/DSL-2680-Multiple-Vulnerabilities)
* [**https://github.com/0x8b30cc/DSL-2680-Multiple-Vulnerabilities/blob/master/CVE-2019-19225.md**](https://github.com/0x8b30cc/DSL-2680-Multiple-Vulnerabilities/blob/master/CVE-2019-19225.md)

**9 - Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)**

| **HIGH RISK (7/9)** | |
| --- | --- |
| **Exploitation Likelihood** | **Possible** |
| **Business Impact** | **Severe** |
| **Remediation Difficulty** | **Easy** |

**Security Implications**

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

**Analysis**

Vendor: shopware

Product: platform

Versions Affected:

< 6.4.1.1

**Recommendations**

We recommend updating to the current version 6.4.1.1.

**References**

* [**https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-06-2021**](https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-06-2021)
* [**https://github.com/shopware/platform/security/advisories/GHSA-vrf2-xghr-j52v**](https://github.com/shopware/platform/security/advisories/GHSA-vrf2-xghr-j52v)
* [**https://github.com/shopware/platform/commit/ba52f683372b8417a00e9014f481ed3d539f34b3**](https://github.com/shopware/platform/commit/ba52f683372b8417a00e9014f481ed3d539f34b3)

# APPENDIX A - TOOLS USED

| **TOOL** | **DESCRIPTION** |
| --- | --- |
| **BurpSuite Community Edition** | Used for testing of web applications. |
| **Metasploit** | Used for exploitation of vulnerable services and vulnerability scanning. |
| **Nmap** | Used for scanning ports on hosts. |
| **OpenVAS** | Used to scan the networks for vulnerabilities. |
| **PostgreSQL Client Tools** | Used to connect to the PostgreSQL server. |
| **Nessus** | Used for vulnerability scanning. |
| **Acunetix** | Used for web vulnerability scanning. |
| **GFI Languard** | Used for network and web application vulnerability scanning. |
| **SolarWinds Port Scanner** | Used for scanning the available IP addresses and their corresponding TCP and UDP ports. |
| **Maltego** | Used for Reconnaissance |

***Table A.1:*** *Tools used during assessment*