INGRAM MICRO
SECURITY

External Penetration Test

Sampledomain.com

20 May 2021

Document Management

Contact information

Name	Aswin Gopalakrishnan
Function	Cyber Security Consultant
E-mail address	cs-coe-weur@ingrammicro.com

Name	Hugo Inigo
Function	Cyber Security Consultant
E-mail address	cs-coe-weur@ingrammicro.com

Reviewers

Name	Function	Date	Version
Simeon Georgiev	Security Specialist	27-05-2021	0.1
Iulian Rotaru	Security Specialist	28-05-2021	1.0

Changes

Version	Date	Changes	Author Initial
0.1	03-01-2021	Initial Version	A.K
1.0	03-01-2021	Internally Reviewed Final Version	A.K

Disclaimer

Table of Contents

Management Summary

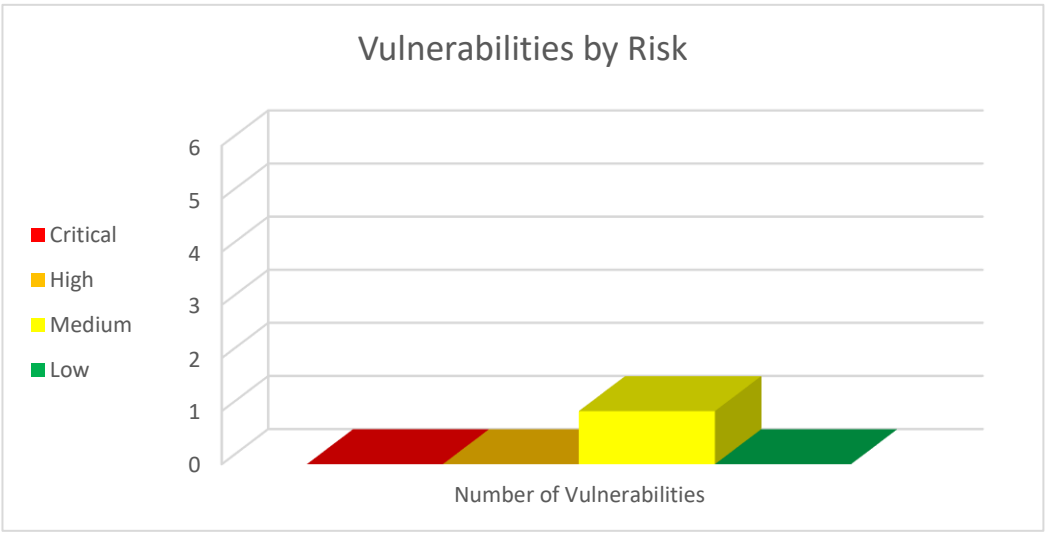
Ingram Cyber Security conducted a comprehensive security assessment of the external facing hosts of SAMPLEDOMAIN.COM from the 20th of May 2021 to the 22nd of May 2021. Throughout the goal-based engagement Ingram Micro Cyber Security performed activities to determine existing vulnerabilities, verify them, and establish the current level of security risk associated with the environment and its corresponding assets.

Objective

The external penetration test assessed the Company's externally facing systems from the perspective of an outside attacked sourced from the Internet. The goal was to discover an information disclosure and leverage potential vulnerabilities to gain access to the internal infrastructure.

Result

The following graph provide an overview of the findings identified during the engagement.



	Critical	High	Medium	Low	Total
Vulnerabilities	0	0	1	0	0

Since the business impact is hard to evaluate by us, all findings and their corresponding risks must be interpreted by Sampledomain.com in the context of the system.

At the time of testing, the consultant noted that the external perimeter was moderately hardened. The in-scope instances were not found vulnerable to any publicly available exploits. The only notable findings were related to the VPN gateway which utilised an outdated algorithm for cryptographic hashing operations. Such a risk could compromise integrity and availability of the application data.

Final Notes

if SAMPLEDOMAIN.COM has any questions with regards to the assessment or presented results, or requires further clarifications, please contact "Cyber Security Center of Excellence - WEUR" <cs-coe-weur@ingrammicro.com>.

Technical Summary

This chapter provides a technical overview of all findings in this report. More detailed information can be found in the actual findings later in this report.

Most Important Findings

- The *iker*[1] tool discovered that VPN gateway was using a weak hash algorithm. Using a weak hash algorithm such as MD5 could enable a rogue device to discover the authentication key enabling it to establish an Internet Key Exchange (IKE) Security Association with either of the VPN end points. Hence, Secure Hash Algorithm (SHA) must be used for IKE cryptographic hashing operations required for authentication and integrity verification.

Technical Recommendations

Ingram Micro Cyber Security recommends the following:

- Configure all ISAKMP policies to use SHA for IKE cryptographic hashing operations.

Operational Recommendations

- For a more thorough and conclusive investigation or retest of the identified threats, please reach out to your channel partner.

Strategic Recommendations

- There is no strategic recommendation for this assessment.

[1] https://github.com/Zamanry/iker

Engagement Description

The engagement is based on TAL (Test Authorisation letter) “TAL_ -Sampledomain.com.pdf.”

Scope

The following assets were in scope for the investigation.

Asset	External IP address
Customer Main Firewall	xxx.xxx.xxx.xxx

Table 1: Target Systems and applications

Information and Documents Provided

Sampledomain.com did not provide Ingram Micro with additional information to perform this investigation. The design and architecture documentation were provided in the following repositories:

Goal of the assessment

The goal of this assignment was to independently determine the effectiveness of the security measures implemented to protect the customers' application and network, by identifying potential vulnerabilities and to suggest improvements to its security.

Limitations

The investigation was conducted with several limitations, these are discussed below:

1. The methodologies used during the assessment include both automated scans and manual verification of the security flaws in a time-boxed manner. Malicious user may discover and exploit additional vulnerability over an extended period or use social engineering techniques.
2. Certain security issues that might disrupt and influence the normal system operations such as Denial of Service (DoS) or buffer overflow attempts were not attempted as part of the assessment.
3. Social Engineering or Client-Side attacks are not in scope of this assessment.
4. The assessment was conducted without security system whitelisting, which had considerable effect on the investigation. IDS and IPS systems attempt to prevent attacks and falsify results which may be gained from the tests. This may lead to inaccurate results. The customer was made aware of the risks and the investigation was continued.

Assessment

The investigation was commenced by first identifying the targets hosts for this assessment.

Discovering hosts

The following table summarises the active machine in the network.

Asset	IP address	Host Name	Alive	Ports Filtered
VPN Server	xxx.xxx.xxx.xxx	cli-5b7e2252.wholesale.sample.es.	Yes	Yes

Table 2: Discovered Targets in the network

Note that the IP address was accessible from the public internet.

IKE Service with Aggressive Mode

The exploration phase on the UDP ports identified the IKE negotiation running on port 500 of the host 51.140.95.220. The protocol ensures security for SA (Security Association) communication without pre-configuration that would otherwise be required.

The *ike-scan* tool was executed to identify valid transformations. A transformation is a combination of values where each value referred to attributes like encryption algorithm, integrity algorithm, authentication type and key distribution algorithm. The following is the result of the tool:

```
$ sudo ike-scan -M xxx.xxx.xxx.xxx
Starting ike-scan 1.9.4 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
xxx.xxx.xxx.xxx     Main Mode Handshake returned
        HDR=(CKY-R=91aa14b1f00ccea8)
        SA=(Enc=3DES Hash=SHA1 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)
        VID=5b362bc820f60007 (SonicWall-7)
```

Table 3: Ike-scan tool with transformation values

Note that the above negotiations were performed using "Main Mode Handshake." The AUTH returned with value PSK (Pre-Shared Key) which confirms that VPN is using a pre-Shared key. Also, the value of the last line "1 returned handshake; 0 returned notify" confirms that target is configured for IPsec (Internet Protocol Security) and is willing to perform IKE negotiations.

Tests were conducted using *ike-scan* tool to discover the vendor of the device. Based on the time difference between the received messages from the server and the matching response pattern, the tool would successfully fingerprint the VPN gateway vendor. The following was the output from tools:

```
IKE Backoff Patterns:

IP Address          No.     Recv time               Delta Time
xxx.xxx.xxx.xxx     1       1622059092.316077       0.000000
xxx.xxx.xxx.xxx     2       1622059096.637492       4.321415
xxx.xxx.xxx.xxx     3       1622059106.637655       10.000163
xxx.xxx.xxx.xxx     4       1622059126.637725       20.000070
xxx.xxx.xxx.xxx     Implementation guess: UNKNOWN

Some IKE implementations found have unknown backoff fingerprints
If you know the implementation name, and the pattern is reproducible, you
are encouraged to submit the pattern and implementation details for
inclusion in future versions of ike-scan.  See:
http://www.nta-monitor.com/tools/ike-scan/submit-patterns.html
Ending ike-scan 1.9.4: 1 hosts scanned in 94.457 seconds (0.01 hosts/sec).  1 returned handshake; 0 returned
notify
```

Table 4: Ike-scan tool with Vendor Name (Unknown)

The above test was inconclusive as vendor could not be fingerprinted.

Next, tests were conducted to identify whether the IKE VPN allow Aggressive Mode negotiations. Aggressive mode is often considered as an exploitable vulnerability as it is less secure. Aggressive modes use three-way handshake where the VPN sends the hashed PSK to the client in a **single unencrypted message**. This mode often used in situations where both peers have dynamic external IP addresses. Aggressive mode is still commonly used due to its speed during

handshake (three rounds when compared to six in Main Mode). A tool called *iker* was used to discover this vulnerability, the following is the output:

```
iker v. 1.1

The ike-scan based script that checks for security flaws in IPsec-based VPNs.

                    by Julio Gomez ( jgo@portcullis-security.com )

Starting iker (http://labs.portcullis.co.uk/tools/iker) at Wed, 26 May 2021 22:11:59 +0000
[*] Discovering IKE services, please wait...
[92m[*][0m IKE service identified at: xxx.xxx.xxx.xxx
[*] Checking for IKE version 2 support...
[92m[*][0m IKE version 2 is supported by xxx.xxx.xxx.xxx
to take a while (1-5 minutes per IP). Be patient...
[91m[*][0m The device xxx.xxx.xxx.xxx could not been fingerprinted. It will not be retrying again.
[====.................] 21% - Current transform: 5,1,1,2
[92m[*][0m Transform found: Enc=AES KeyLength=192 Hash=MD5 Group=2:modp1024 Auth=PSK
LifeType=Seconds LifeDuration=28800
[92m[*][0m Transform found: Enc=AES KeyLength=256 Hash=SHA1 Group=2:modp1024 Auth=PSK
LifeType=Seconds LifeDuration=28800
```

Table 5: Iker tool with Aggressive Mode output

The following results were returned by the scan:

1. IKE service could be discovered;
2. IKE v2 is supported;
3. The IKE service could be fingerprinted by analysing the responses received: Linksys Etherfast.
4. Weak hash algorithm was supported: MD5

Aggressive mode was not being used; however the VPN gateway was using a weak hash algorithm. Using a weak hash algorithm such as MD5 could enable a rogue device to discover the authentication key enabling it to establish an Internet Key Exchange (IKE) Security Association with either of the VPN end points. Hence, Secure Hash Algorithm (SHA) must be used for IKE cryptographic hashing operations required for authentication and integrity verification[2]. A finding is reported below:

Name	Weak Hash Algorithm		H001
Severity	CVSS 3.0 Score (4.8)	MEDIUM RISK 1	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:N
Category	Vulnerability		
Location	UDP Port 500		
Applies To	xxx.xxx.xxx.xxx (cli-5b7e2252.wholesale.sample.es.)		
Description	The iker tool discovered that VPN gateway was using a weak hash algorithm.		
Risk	Using a weak hash algorithm such as MD5 could enable a rogue device to discover the authentication key enabling it to establish an Internet Key Exchange (IKE) Security Association with either of the VPN end points. Hence, Secure Hash Algorithm (SHA) must be used for IKE cryptographic hashing operations required for authentication and integrity verification.		
Recommendation	Configure all ISAKMP policies to use SHA for IKE cryptographic hashing operations.		

[2] https://www.stigviewer.com/stig/ipsec_vpn_gateway/2017-03-02/finding/V-30950

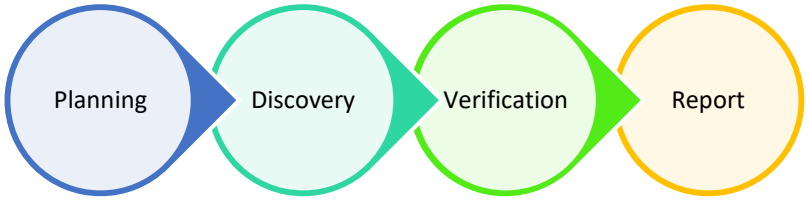
Appendix: Assessment Approach

External penetration test targets external target hosts or domains where the consultant reviews the security posture and report the plausible vulnerabilities that affects the organisation.

Overview

The testing is performed in several related phases:

1. In the planning phase, the rules of engagement are identified, scope of the test and time were finalized, and testing goals were set.
2. The discovery phase included automated vulnerability scanning during industry standard tools.
3. The vulnerabilities identified during the discovery phase is verified and rated based on likelihood and impact of the exploitation.
4. The final phase recorded all findings in a manner that supports risk assessment and remediation by the customer. This included the writing of this report.



Discovery and Reconnaissance

As the first step of this engagement, Ingram Micro Cybersecurity performed discovery and reconnaissance of the web application. This includes performing scans and reviewing of the web application or walking through a typical use case scenario for the application.

Validation and Reporting

The finding reported from the discovery phase are further review and validated by the consultant. At this stage of the assessment, the consultant would identify the risks that compromise the Confidentiality, Integrity and Availability (CIA) of the data in the system.

The sections below describe the results of the exploitation, the validation tests, and necessary steps to mitigate each of them.

Appendix: Risk Rating Scale

The risk rating score assigned to each exploitable vulnerability finding is then translated into a CRITICAL, HIGH, MEDIUM, LOW Risk Rating to simplify reporting, analysis, and remediation planning.

Risk Rating	Description
CRITICAL	High Severity issues that can be exploited in isolation, with no additional steps necessary, that may provide total compromise of the system.
HIGH	Severe issues that can easily be exploited to immediately impact the environment
MEDIUM	Moderate security issues that require some effort to successfully influence the environment.
LOW	Security issues that have a limited or trivial impact to the environment.
INFORMATIONAL	These vulnerabilities represent significantly less risk and are informational in nature. These items can be remediated to increase security.