Security Test Report

ACME Example

Confidential

SKOPOS
SECURITY LABS

Table of contents

Summary

Introduction

This document is a summary of the findings from a penetration test performed for client. The pentest commenced the 2nd of December 2019 and concluded the 4th of December 2019. The scope included 65 IP-addresses belonging to client: this is the publicly reachable infrastructure of ACME Example. The scope of this test was a blackbox test on a number of IP-addresses.

This report contains issues found during the pen-test. A severity 1 vulnerability that offered root access on one machine has been reported directly via telephone.

The initial stage was done via automated scanning tools: Nmap, Zap and Arachni. The second stage testing was performed manually to validate issues found based on the tooling. In the third stage the team performed more complex tests.

To score issues we report in two ways: using the classic CVSS scoring and the SKES (Skopos Exploit Score). The CVSS method is used, using this calculator: https://first.org/cvss/calculator/3.0

The Skopos Exploit Score (SKES) indicates the probability of exploitation of a vulnerability in the next 12 months from 0 – 100%. This score is based on historical attacks, availability of exploits and the amount of references found in the public domain. The SKES helps to understand the real world risk of vulnerabilities.

Assessment level of security measures

Based on the test results the level of the security measures at client is **critical**:

	Informational	*Low*	*Medium*	*High*	*Critical*
Test result	2	0	4	2	1

The relation between the level of security measures and the amount of issues is depicted in the following table.

	Strong	*Good*	*Unsafe*	*Very unsafe*	*Critical*
Informational	1 or more	Up to 4	5 and more	5 and more	5 and more
Low			Up to 4	Up to 4	1 or more
Middle					
High					
Critical					

A security test can not definitively conclude that a network, system or application is completely safe. A security test can only show that security measures are not effective and whether there are any vulnerabilities at the moment of testing.

Overview of findings

The following positive points were found:

- The servers on Amazon AWS did not reveal any vulnerabilities
- Standardized product, for example Cisco, are used
- Cloudfront is used as a security measure

The following issues were found, sorted on CVSS impact:

#	Issue	SKES(%)	CVSS	Details CVSS
1	Datalogger has TCP server with root privileges and default username and password	98.7	9.8	AV:N/AC:L/ PR:N/UI:N/S:U/ C:H/I:H/A:H/ E:H/RL:O/ RC:C/CR:L/ IR:M/AR:M
2	Cisco SSH 1.25 (protocol 1.99) has multiple known vulnerabilities	12,3	7.5	AV:N/AC:L/ PR:N/UI:N/S:U/ C:N/I:N/A:H/ E:P
3	HTTP Trace vulnerable to Cross Site Tracing (XST)	9,6	7.5	AV:N/AC:L/ PR:N/UI:N/S:U/ C:N/I:N/A:H/ E:P
4	Untrusted issues of wildcard certificate	5,6	6.1	AV:N/AC:L/ PR:N/UI:R/S:C/ C:L/I:L/A:N
5	VPN server can be brute forced	45	5.9	AV:N/AC:L/ PR:N/UI:N/S:U/ C:L/I:L/A:N/ E:P/RC:R
6	MQTT broker can be subscribed to without authentication	32	5.2	AV:N/AC:L/ PR:N/UI:N/S:U/ C:L/I:N/A:N/ E:F/RC:C
7	VPN server offers old and low grade TLS	29,5	4.2	AV:N/AC:H/ PR:N/UI:R/S:U/ C:L/I:L/A:N

- Cisco and VMWare admin console publicly exposed - CVSS: None – Informational
- Overall hardening of systems - CVSS: None – Informational

Summary and advice

The scope for the pen-test was quite broad. Using tools and open source information (OSINT) a global picture was created and from there on the pen-test was performed manually, supported here and there by specific tools.

A couple of vulnerabilities with a high and one critical were found. The critical vulnerability was communicated directly after it was verified by the tester. At the moment of finishing this report the vulnerability is not yet solved.

Overall, the potential attack surface for client is very big. This means that potential attackers have many options at their disposal to break in. We recommend two actions: make the attack surface as small as possible and implement a hardening policy. It would also be wise to look at the security architecture and the information security policies. Maturing towards an architecture that follows Defense in Depth, Least Privilege and Need to Know privileges will greatly improve the safety of the company.

Report classification: Confidential

Report date: 04-12-2019

Report signed by:

ing. Bas van den Berg MA CEH AT CISSP CISM S-EHP S-ITSE S-CSPL S-CT

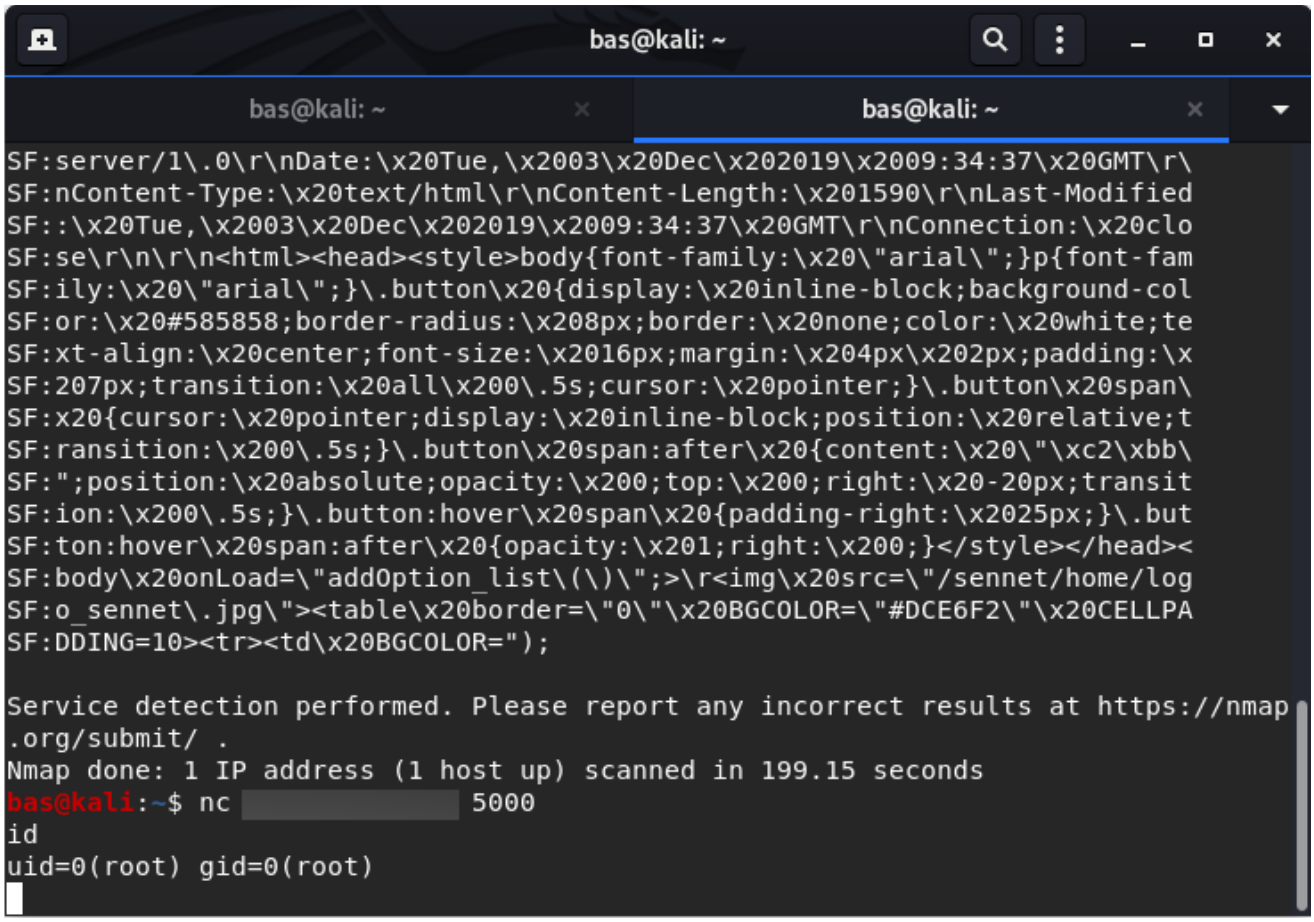
(Ethical hacker)

Issues

This chapter will cover issues that were discovered found during the test.

1. Data logger has TCP server with root privileges and default username and password

On IP-address *{Redacted}* a data logger was found posing a shell through port 5000. Connecting to the shell using NetCat (nc) resulted in a shell with high privileges.



This is a known vulnerability with a fix released in 2017. There are also multiple exploits available.

The website on the data logger did provide a login, but a quick search resulted in the default username and password (https://manualzz.com/doc/10477030/datalogger-sennet-dl160, page 28):

Username: user

Password: logger

SenNet Datalogger Web Interface

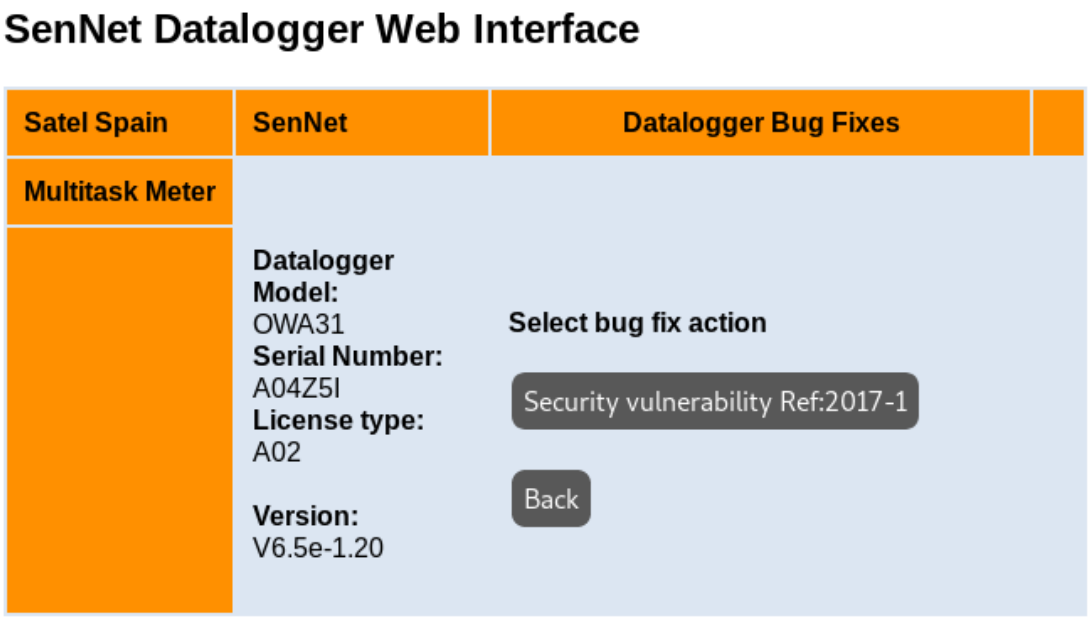
Although this user doesn't have administrator privileges, the login page is easily brute forced to find the admin password (the username is fixed).

Besides that, the admin username and password also can be found in the documentation (https://www.satel-iberia.com/wp-content/uploads/2018/04/manual_hardware_datalogger_owa31ieth_v1.01.pdf, page 12):

Username: admin

Password: owasat

Note: The password can be changed through the webinterface.



The root password was easily retrieved based on the hash (salted MD5) in the shadow file:

root:1O7tDWPOZ$497dh2xRuhjXWyda9cYa9.:13852:0:99999:7:::

Resulted within 2 hours of bruteforcing to the password “owasys”.

CVSS: 9.8 - Critical (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:L/IR:M/AR:M), SKES 98,7%

2. Cisco SSH 1.25 (protocol 1.99) has multiple known vulnerabilities

Version 1.25 and protocol version 1.99 are used in multiple publicly exposed Cisco products. This version has multiple known vulnerabilities that can be exploited by unauthenticated attackers. It would be very wise to update these products and keep them updated.

https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20080521-ssh.html

CVSS: 7.5 – High (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P), SKES 12,3%

3. HTTP Trace vulnerable to Cross Site Tracing (XST)

The web server *{Redacted}* allows HTTP Trace requests. A Trace request is used for debugging purposes and can be abused to mislead employees, customers or others. However modern browsers provide more protection against this attack nowadays. Since it serves no purpose on production system, it can easily be disabled.

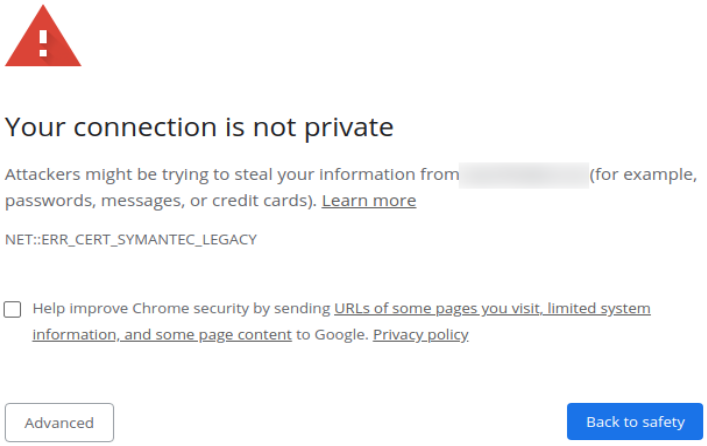
https://www.owasp.org/index.php/Cross_Site_Tracing

CVSS: 7.5 – High (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P), SKES 9,6%

4. Untrusted issues of wildcard certificate

For all subdomains of client a wildcard certificate is used. Inherently a wildcard certificate is less secure, since it isn't domain specific. But the ease of use for administrators often compensates for this low risk. In this case the certificate is signed by “GeoTrust SSL CA - G3 (GeoTrust Inc. from US)”, which is a label of Symantec. Among others, Google and Mozilla stopped trusting certificates from Symantec in 2017 because they had lost confidence about Symantec’s certificate issuance policies and practices of recent years.

This means that the end user in Chrome and Firefox will receive this warning:



This is itself isn’t a security problem, but since it is a wildcard certificate (which can be abused to seem an untrusted server like a trusted one) and the error is already given (user get the error already and might be ignoring it) it will be far easier for attackers to abuse this and perform a successful social engineering attack.

CVSS: 6.1 - Medium (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N), SKES 5,6%

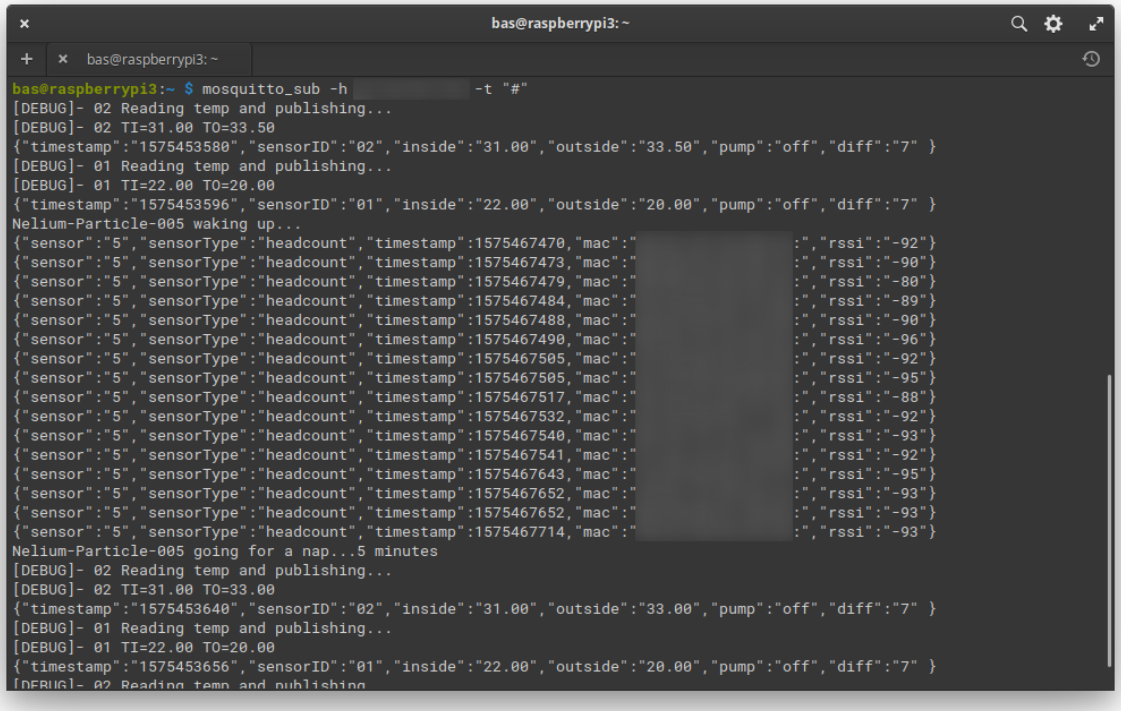
5. VPN server can be brute forced

The Cisco VPN server (*{Redacted}*) doesn't provide any mitigation for brute forcing the login functionality. Through an easy script it is possible to continuously try username and password without any time penalty or IP-address blocking.

CVSS: 5.9 - Medium (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RC:R), SKES 45%

6. MQTT broker can be subscribed to without authentication

There is a MQTT broker running on *{Redacted}* which can be subscribed to without any authentication or validation. Therefore anyone on the internet is able to collect all sensor data and other communication that goes through this broker.



CVSS: 5.2 - Medium (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RC:C), SKES 32%

7. VPN server offers old and low grade TLS

The Cisco VPN server (*{Redacted}*) offers only older encryption mechanisms and DH params that are too short. The server only offers TLS 1.0 without the option for upgrading to newer and stronger protocols (TLS 1.0 with DHE-RSA-AES256-SHA, 1024 bit DH (CBC) is used). Further more the TLS 1.0 implementation on this machine is vulnerable to Secure Renegotiation attacks, BEAST (CVE-2011-3389) and potentially to

LUCKY13 (CVE-2013-0169), since it uses CBC. Combined with the issue of less trusted or untrusted wildcard certificates will leave users vulnerable to social engineering and man in the middle attacks.

CVSS: 4.2 - Medium (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N), SKES 29,5%

8. Cisco and VMWare admin console publicly exposed

The Cisco and VMWare admin consoles are publicly exposed (among others):

{Redacted}

Both Cisco and VMWare are well-known to secure their products, but even in those cases there is always a possibility for the existence of zero day vulnerabilities. Therefore if credentials are uncovered (for example through social engineering) there is no other security measure between an attacker and the administration of the servers. Better would be to keep the admin consoles only accessible from the internal network and let server administrators use a VPN to first login and then use the consoles if necessary, e.g. implement a layered security model. Since the consoles couldn't be exploited during the test, this is informational.

CVSS: None – Informational

9. Overall hardening of systems

What generally stands out is that systems aren't sufficiently hardened. Details like older encryption protocols on SSL/TLS connection, older SSH versions (for example 1.0), default passwords, TCP timestamps (allows to compute the up-time) are found on most servers not hosted by a cloud provider. There is no specific risk attached to this, but every bit helps potential attackers build an attack strategy and successfully executing such an attack. Our advice would be to review the information security policies and validate how they work, validate and improve security awareness, look at the security architecture and implementation and start improving from that point on.

An first step could be to follow hardening guides from suppliers, like this one:

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/hardening_guide/b_dnac_security_best_practices_guide.html

CVSS: None – Informational