Penetration Testing - Report

Network Penetration Testing Standard

Mustermann GmbH

Herr Max Mustermann
Mustermann Str. 1
01234 Musterstadt

Author: Patrick Münch
SVA System Vertrieb Alexander GmbH
Borsigstraße 14
65205 Wiesbaden

Date: 27.02.2018
Version: 1.0Rel

Table of Contents

1 Document information

1.1 Distribution list

Name	Company / Department
Beispielmitarbeiter X	Beispielfirma, Einkauf
Beispielmitarbeiter Y	Beispielfirma, GL
Beispielmitarbeiter Z	Beispielfirma, IT-Produktion

Table 1: Distribution list

1.2 Document history

Version	Date	Author	Reason of modification	Status
1.0 WD	19.02.2018	P. Münch	Initial version	done
1.0 RC	23.02.2018	P. Münch	Addition	done
1.0 RV	26.02.2018	T. Löbner	Review	done
1.0 Rel	27.02.2018	P. Münch	Approval	done

Table 2: Document history

1.3 List of abbreviations

Abbreviation	Definition
AES	Advanced Encryption Standard
CA	Certification Authority
CBC	Cipher Block Chaining
CIFS	Common Internet File System
CIM	Common Information Model
CIS	Center for Internet Security
CN	Common Name
CTR	Counter Mode
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DES	Data Encryption Standard
DHE	Diffie-Hellman Exchange
DNS	Domain Name System

Abbreviation	Definition
DoS	Denial-of-Service
ECDHE	Elliptic Curve Diffie-Hellman Exchange
GCM	Galois/Counter Mode
HSTS	HTTP Strict Transport Security
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
MD5	Message-Digest Algorithm 5
MitM	Man-in-the-Middle
RC	Rivest Cipher
RFC	Requests for Comments
RSA	Rivest, Shamir und Adleman
SHA	Secure Hash Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UI	User Interface
XML	Extensible Markup Language
XSS	Cross-Site-Scripting

1.4 List of figures

1.5 List of tables

2 Introduction

2.1 Motivation

In recent years, the demands on IT security have grown significantly. It is important that IT operators know the IT security status of the company as well as of the products and applications offered by the company and ensure that the demands on IT security are effectively implemented.

IT networks and applications are constantly being adapted to new requirements and becoming more and more complex over time. The technology used provides a target for cybercriminals and insider threats. No matter how carefully the preventive building blocks of a security infrastructure are selected and implemented - proof for the effectiveness of these measures and the level of protection achieved can only be provided by a security assessment.

Companies and public-sector institutions must comply with laws, standards, and regulations and must therefore provide proof of an effective risk management, which also includes the operational areas with the technical protection measures. If these requirements are not taken seriously, a personal liability of those responsible cannot be ruled out.

Against this background, Mustermann GmbH (hereinafter referred to as the customer) contracted SVA System Vertrieb Alexander GmbH to verify the effectiveness of the implemented protective measures.

Main targets of the assessment were active IT systems accessible via Internet along with services connected to them.

2.2 Objectives

SVA conducted a coordinated penetration test for the test object described in Chapter 4, which identified possible weak points and assessed their technical risk.

The procedure complies with the specifications of the Bundesamt für Sicherheit in der Informationstechnik (BSI).

A proof of the current level of security is provided in the form of a comprehensive assessment report issued by an independent expertise. In order to remedy identified vulnerabilities, recommendations are given with prioritization so that they can be remedied by the customer according to their criticality.

3 Summary of the test results

The assessment took place on 2018-02-12 and was carried out by SVA GmbH. The following test objects of the customer where in scope:

- homamatic-ccu2.fritz.box

The target objects were specified by the customer before the Penetration test was carried out.

One target addresses were examined. In total, 1 hosts were identified as active. Active means that at least one service is publicly accessible via a port from the Internet. To this end, a TCP / IP and UDP / IP scan was performed in the first phase; regardless of whether the systems previously responded to an ICMP request (ping). A security scan was carried out for the systems recognized as active.

Figure 1 shows an overview of all findings grouped by its risk value:

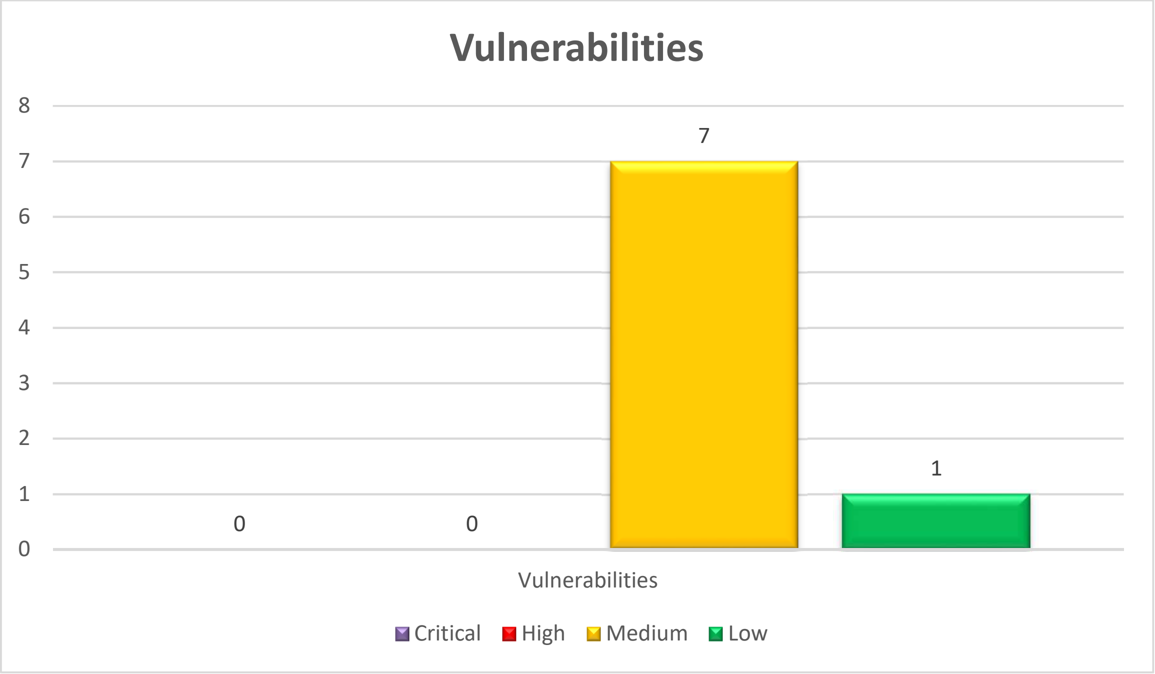

Figure 1: Findings grouped by risk value

0 vulnerabilities with the technical[1] risk value “critical” were identified by the examiner after evaluation of the results. Critical findings are weak points that can be exploited without or with little effort through tools or knowledge and can have a major impact. Vulnerabilities are classified as critical if they represent weaknesses in software where the manufacturer does no longer provide security updates and that could be exploited by existing malicious software like exploits for example. Critical vulnerabilities are a clear violation of statutory and regulatory requirements.

These vulnerabilities refer to:

0 findings were classified as a “high” technical risk. In case of a security breach, this may lead to a breach of the duty of care and may be a violation of legal and regulatory requirements or to an allegation of negligence.

These vulnerabilities refer to:

7 findings were classified by the examiner as "medium" technical risk. Exploiting these vulnerabilities requires high efforts while having little effects. These weak points could often only be used by an attacker in combination with other vulnerabilities found in the system or the environment. However, it may be possible to exploit these vulnerabilities in the future by using newer exploits. If economically justifiable measures are not implemented at this point in time and a damage occurs, a violation of statutory requirements could be assumed.

These vulnerabilities refer to:

- It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.
- The SSL certificate chain for this service ends in an unrecognized self-signed certificate.
- The SSL certificate for this service cannot be trusted.
- The remote service supports the use of medium strength SSL ciphers.
- An SSL certificate in the certificate chain has been signed using a weak hash algorithm.
- The remote service supports the use of weak SSL ciphers.
- The remote service encrypts traffic using a protocol with known weaknesses.

There were 1 vulnerabilities classified as “low” technical risk, because they do not imply direct harm to the examined systems. Exploitation of these weak points is not possible according to current knowledge. Normally there are no actions necessary to avoid exploitation of these vulnerabilities. In general a review on these findings and an evaluation whether additional security measures (e.g. implementation of a firewall or an intrusion detection system) to improve security are technically feasible and economically viable could be done. There is no threat and no violation of legal and regulatory requirements.

These vulnerabilities refer to:

- The remote service supports the use of the RC4 cipher.

Further details on the vulnerabilities and recommendations are given in chapter 7.

In summary, the assessment identifies 0 vulnerabilities with a critical or high technical risk. Security must be optimized at these points in a timely manner. Overall, the level of security can be improved by commercially reasonable efforts.

[1] A technical risk is the possibility of exploiting a weak point and causing damage. The amount of the possible damage or the business impact is not taken into account in the technical risk (no business impact analysis has been done)

General recommendations:

- Update systems and software in a timely manner and to review the patch management process.
- Open ports on all systems should be checked for their necessity and not necessary ports should be closed
- Connections used for authentication must be encrypted in all cases.
- Operating systems must be hardened (see: dev-sec.io)
- A system configuration review (system audit) of critical systems must be performed (regular compliance-checks of the environment).
- The introduction of a vulnerability management system for regular tests of the systems is recommended.
- Disable SSLv3.
  Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.
- Purchase or generate a proper certificate for this service.
- Purchase or generate a proper certificate for this service.
- Reconfigure the affected application if possible to avoid use of medium strength ciphers.
- Contact the Certificate Authority to have the certificate reissued.
- Reconfigure the affected application, if possible to avoid the use of weak ciphers.
- Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.1 (with approved cipher suites) or higher instead.
- Restrict access to your services to minimize attack surface.

4 Assessment definition

4.1 Assessment assignment

The aim of this network penetration test is a documented review of the current IT security level at the date of examination as well as the assessment of the existing security measures in the technical area through an independent review.

Amongst others the following information about the systems were gathered:

- open ports,
- running services,
- used software versions,
- weaknesses in network, systems and software.

4.2 Exclusions

Systems that could not be reached via Internet were not included in the assessment. This applies to all systems and services which were not active at the time of the assessment or which were switched off during the scans. All listed systems could be reached and were examined. Penetration tests that are known to lead to a failure situation in systems have not been performed in order not harm ongoing business operations. Therefore, the following tests were not part of the assessment:

- Destructive penetration test scenarios,
- Denial of Service attacks or
- Brute force attacks.

4.3 Scope

All information included in this document is based on the information provided by the examiner and the assessment results. The penetration testing results reflect the status of the systems at the date where the assessment was performed, i.e. 2018-02-12

5 Assessment methods

With Penetration Testing, SVA offers its customer a service for the identification of vulnerabilities or software and configuration errors in IT systems. SVA's IT security consultants draw on such strategies and tools that are also used by real attackers so that they can present a realistic and practically comprehensible picture of the security level to the customer. A penetration test consists of recurrent phases, which result in a comprehensive analysis of the target systems. These essentially include:

- Identification of systems and services
- Determination of software versions and (known) vulnerabilities
- Optional validation and exploitation of vulnerabilities

Depending on the depth of the audit, these steps include a variety of approaches, including automated identification of the systems and their vulnerabilities, manual vulnerability verification, or the manual development of proof-of-concepts or exploits.

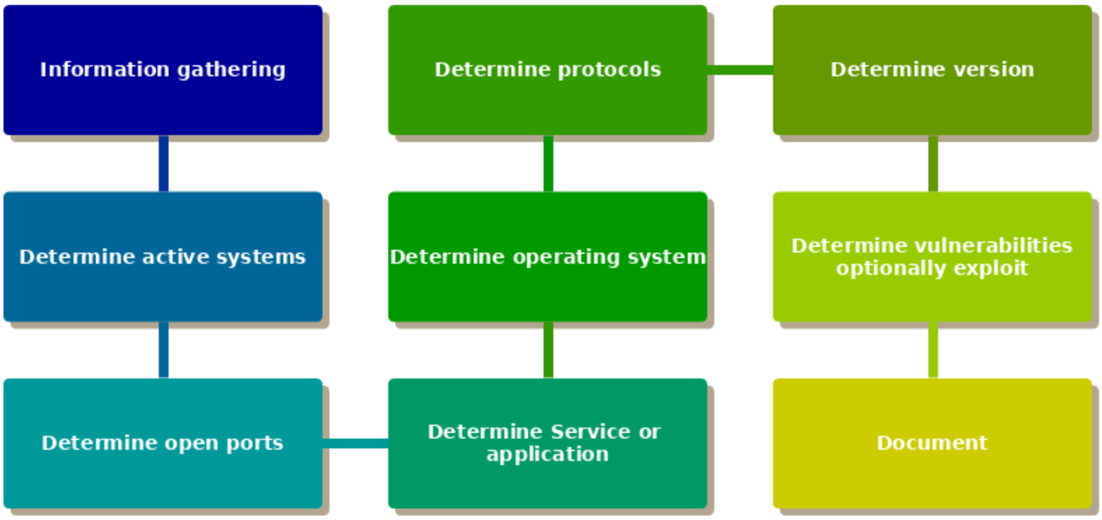

Figure 2: Penetration Testing process

5.1 Examiner

SVA employs experienced and qualified employees with several years of professional experience in penetration testing. Our employees hold the Offensive Security Certified Professional (OSCP) and Offensive Security Certified Expert (OSCE) certification.

Upon request, the employee will sign a privacy statement and a confidentiality agreement of the client before conducting the first audit.

5.2 External scan

Through an active Network Penetration Testing experienced IT security consultants from SVA identify typical vulnerabilities over the Internet. In this way our examiners simulate attacks by external parties over public network access. Objectives are all accessible IT systems and services from a previously agreed IP address range. This test is designed in such a way that a comprehensive overview of the current security level can be obtained in a comparatively short time. During this assessment information like the following is gathered:

- open ports,
- running services,
- software versions in use,

- missing security patches,
- shares and
- backdoors

More than 80,000 tests can be performed on Windows-, UNIX/Linux-, Firewall systems and active network components during a single penetration test.

5.3 Outside-In

An Outside-in test is performed from the outside; usually via the internet (see Figure 3). The investigation will be conducted over the Internet and all IT systems, services and applications accessible over the Internet will be audited. This test scenario simulates an attack of an external threat agent.

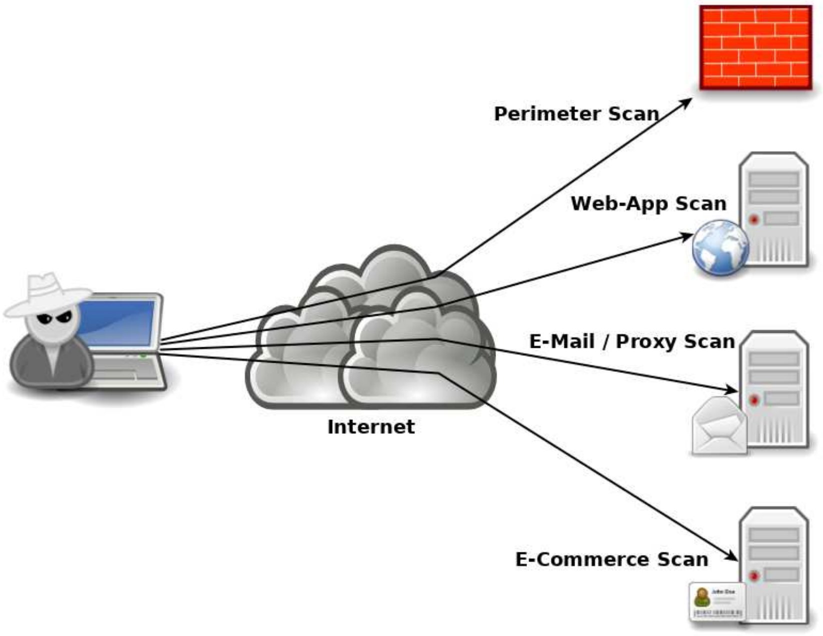

Figure 3: Outside-In

When testing via the Internet, it must be taken into consideration that there are various IT systems in the communication path between the tester and the test object (see Figure 4). Devices such as firewall systems, intrusion detection systems, web application firewalls, reverse proxy servers, SSL gateways or load balancers may corrupt the inspection results. This means that the target system or application is not checked directly, in fact also the communication path used. Therefore, this test is only partially suitable for a penetration test. The result does not reflect reality, but reflects the view from the outside. This check is useful to answer the question what information and vulnerabilities are "identifiable" over the Internet and whether the security measures implemented are effective.

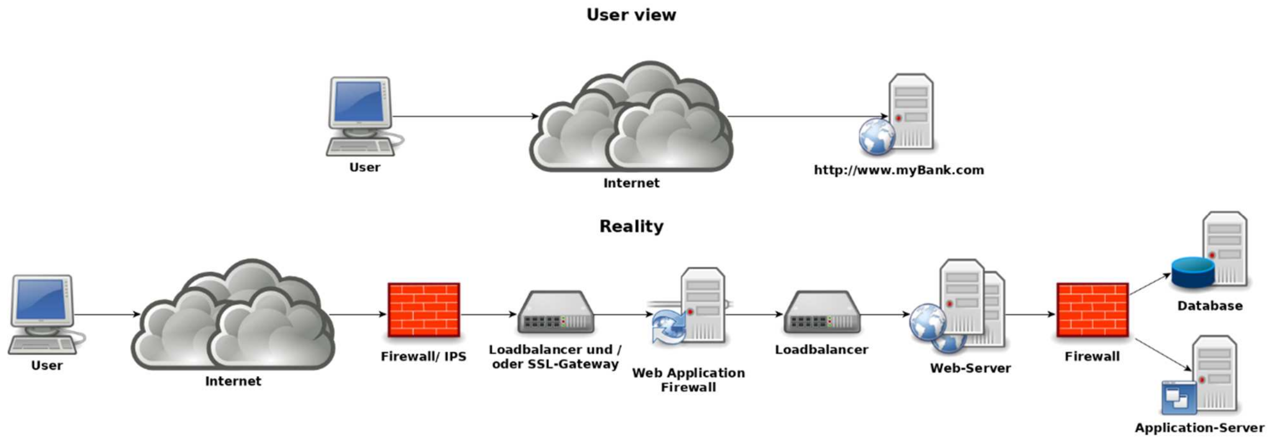

Figure 4: User view vs. reality

5.4 Test procedure

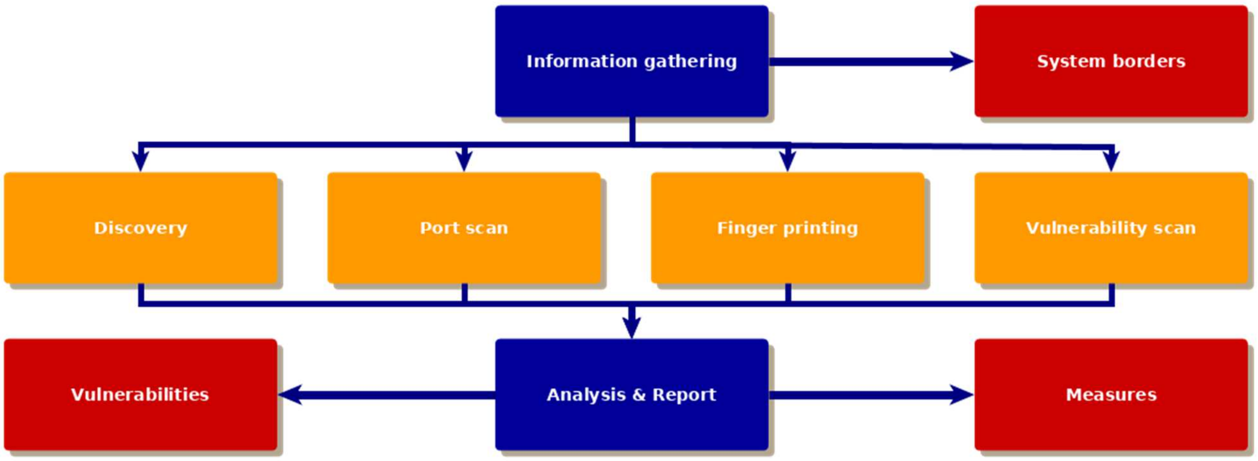

Figure 5: Procedure of Network Penetration Testing

The system borders were predefined together with the customer before the assessment started. For this purpose, the information provided by the customer or further information from public sources were used. At the beginning of the assessment the active systems (IP addresses) were identified using a method called host discovery. Afterwards, the services were identified through existing open network ports. This method is called fingerprinting. These results were the basis for the following vulnerability scan, which detects well-known vulnerabilities. The extensive results created by the vulnerability scanner were filtered and included into the test report for the customer. For all findings in this report suitable recommendations are given according to the risk value.

5.5 Services at a glance

The following services are included for the external Network Penetration Testing Standard (assessment over the Internet).

✓	Individual coordination and preliminary discussion of the assessment over the phone
✖	Individual coordination of the depth of the penetration test
✓	Service description including test agreement
✓	Host Discovery (determination of active systems)
✓	TCP/UDP port scan (65.535 ports each)
✓	Vulnerability scan
✖	Manual verification
✓	Performing the penetration test according to the BSI standard
✖	Exploitation of vulnerabilities, creation of proof-of-concepts
✓	Test report with the individual vulnerabilities (English) and management summary (German / English)
✖	Risk assessment by analysts and creation of a list of deficiencies with recommendations
✓	Discussion of the results over the phone
✖	Presentation of the results on site at the customer

✓ Included in the actual Scan ✖ Not included in the actual scan

Table 3: Service description of Network Penetration Testing Standard

6 Classification criteria

6.1 Explanation

This report identifies possible security weaknesses found during the security assessment. Identified vulnerabilities are presented in the form of a list for each test object.

A unique number in the test report identifies each vulnerability. This number is used to refer to a specific finding within the report.

The classification reflects the risk classification from the analysts' point of view. Depending on the estimate, the analyst assigns a risk level to each finding. These risk levels are based on an evaluation procedure defined for this report and therefore do not need to be consistent with other definitions of risk assessment used within the company.

A brief description is given for each finding. The finding is explained in more detail in its description. The description also shows the reason why the specific finding has been classified accordingly. The analyst gives a recommendation for each finding. This can also be a recommendation to retrieve further information or to carry out further tests. Specific details on sources for security updates are listed, if any are available. If a finding gets explained in more detail or the demonstration of the vulnerability has been documented, a reference is made to further information in the report or to a data source accessible to the reader.

6.2 Assessment levels

This section explains the risk assessment levels in the context of penetration testing in more detail.

low risk

The analyst estimates the risk of a vulnerability as low if there are only indications and assumptions that a finding could be exploited. As a rule, no action has to be taken. In general, it can be checked whether it is technically feasible and economically justifiable to protect an IT system or an application with additional security measures (e.g. a firewall or an intrusion detection system). There is no threat or violation of statutory and regulatory requirements.

medium risk

The analyst estimates the risk of a vulnerability as medium if the effort to take advantage of the finding is not in a reasonable ratio to the effect achieved. These are often vulnerabilities which can only be exploited in combination with other information or vulnerabilities.

If there are economically justifiable measures to eliminate a vulnerability with a medium risk or at least reduce the risk potential, these measures should be implemented within 6 months. If economically justifiable measures are not implemented and there is a damage, a breach of the obligation to take precautions could be assumed.

high risk

In the view of the analyst, a finding represents a high risk if there are concrete indications that the vulnerability could be exploited by an attacker (for example, there are corresponding exploits, or the risk could be clearly demonstrated by exploitation). As a rule, vulnerabilities found, which can be fixed with an available security update, are also classified as high risk, since this could lead to a proof of a breach of the precautionary obligation.

Vulnerabilities representing a high risk should be eliminated by appropriate measures within 3 months after the finding. To implement the measures resources are required, which are not always immediately available.

In case of a security incident, this may result in a breach of the precautionary obligation or a breach of statutory and regulatory requirements as well as negligence.

critical Risk

From the perspective of the analyst, a vulnerability represents a critical risk if the security of an application or of the IT infrastructure is at imminent risk. Measures must be initiated immediately. Resources must be made available immediately, and the vulnerability is usually reported as soon as it is detected (e.g. during a vulnerability scan) and could be escalated in time if necessary. These are vulnerabilities, which can be exploited without or with little help / knowledge. Example: Log on to a server as a privileged user without entering a password. This may present a clear violation of statutory and regulatory requirements, and gross negligence or even intent may be assumed.

6.3 Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) is an industry standard for evaluating the severity of possible or actual security gaps in computer systems. In the CVSS, security vulnerabilities are evaluated according to different criteria and compared with one another, so that a list of priorities for counter-measures can be established. If present, a CVSS value is included. Table 4 shows the CVSS Score Rating lists for each CVSS score.

Rating	CVSS Score
None	0
Low	0,1 – 3,9
Medium	4,0 – 6,9
High	7,0 – 8,9
Critical	9,0 – 10,0

Table 4: CVSS Score Rating

7 Test report

The test report documents which specific assessments were performed and whether there were any inconsistencies. Only systems are listed which were identified as active during the whole test and from which information could be gathered. A network security scan of the following IP addresses and IP address ranges was performed from the outside via the Internet:

192.168.2.65

Several hundred individual tests were done during that assessment.

7.1 System overview

Host-IP	Host- FQDN	Port / Protocol / Service	Operating system
192.168.2.65	homematic-ccu2.fritz.box	22 / tcp / ssh 80 / tcp / www 443 / tcp / www 1999 / tcp / tcp-id-port? 2001 / tcp / dc? 2010 / tcp / www 8181 / tcp / www 9292 / tcp / www	

7.2 Findings

Finding no. 11

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Risk

medium risk

CVSS-Score: 4.3

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.
As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.
The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.
This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Objectives / Hosts

192.168.2.65

Recommended solution

Disable SSLv3.
Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Finding no. 16

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Risk

medium risk

CVSS-Score: 6.4

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Objectives / Hosts

192.168.2.65

Recommended solution

Purchase or generate a proper certificate for this service.

Finding no. 20

The SSL certificate for this service cannot be trusted.

Risk

medium risk
CVSS-Score: 6.4

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Objectives / Hosts

192.168.2.65

Recommended solution

Purchase or generate a proper certificate for this service.

Finding no. 34

The remote service supports the use of medium strength SSL ciphers.

Risk

medium risk

CVSS-Score: 5

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.
Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Objectives / Hosts

192.168.2.65

Recommended solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Finding no. 36

An SSL certificate in the certificate chain has been signed using a weak hash algorithm.

Risk

medium risk

CVSS-Score: 4

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

Objectives / Hosts

192.168.2.65

Recommended solution

Contact the Certificate Authority to have the certificate reissued.

Finding no. 38

The remote service supports the use of weak SSL ciphers.

Risk

medium risk

CVSS-Score: 4.3

Description

The remote host supports the use of SSL ciphers that offer weak encryption.
Note: This is considerably easier to exploit if the attacker is on the same physical network.

Objectives / Hosts

192.168.2.65

Recommended solution

Reconfigure the affected application, if possible to avoid the use of weak ciphers.

Finding no. 51

The remote service encrypts traffic using a protocol with known weaknesses.

Risk

medium risk

CVSS-Score: 5

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:
- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.
An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.
Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.
NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Objectives / Hosts

192.168.2.65

Recommended solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

Finding no. 15

The remote service supports the use of the RC4 cipher.

Risk

low risk

CVSS-Score: 2.6

Description

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.
If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Objectives / Hosts

192.168.2.65

Recommended solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Finding no. 1

The remote service encrypts traffic using an older version of TLS.

Risk

Information

CVSS-Score: 0

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.
PCI DSS v3.1 requires that TLS 1.0 be disabled entirely by June 2018, except for point-of-sale terminals and their termination points.

Objectives / Hosts

192.168.2.65

Recommended solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Finding no. 2

The remote web server hosts linkable content that can be crawled by Nessus.

Risk

Information
CVSS-Score: 0

Description

The remote web server contains linkable content that can be used to gather information about a target.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 3

The remote web server hosts linkable content that can be crawled by Nessus.

Risk

Information
CVSS-Score: 0

Description

The remote web server contains linkable content that can be used to gather information about a target.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 4

The remote web server hosts linkable content that can be crawled by Nessus.

Risk

Information
CVSS-Score: 0

Description

The remote web server contains linkable content that can be used to gather information about a target.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 5

The remote web server hosts linkable content that can be crawled by Nessus.

Risk

Information
CVSS-Score: 0

Description

The remote web server contains linkable content that can be used to gather information about a target.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 6

The remote web server redirects requests to the root directory.

Risk

Information
CVSS-Score: 0

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server. This plugin is informational only and does not denote a security problem.

Objectives / Hosts

192.168.2.65

Recommended solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Finding no. 7

An HTTP/2 server is listening on the remote host.

Risk

Information
CVSS-Score: 0

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

Objectives / Hosts

192.168.2.65

Recommended solution

Limit incoming traffic to this port if desired.

Finding no. 8

An HTTP/2 server is listening on the remote host.

Risk

Information
CVSS-Score: 0

Description

The remote host is running an HTTP server that supports HTTP/2 running over cleartext TCP (h2c).

Objectives / Hosts

192.168.2.65

Recommended solution

Limit incoming traffic to this port if desired.

Finding no. 9

The remote web server is not enforcing HSTS.

Risk

Information
CVSS-Score: 0

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Objectives / Hosts

192.168.2.65

Recommended solution

Configure the remote web server to use HSTS.

Finding no. 10

This plugin gathers the logs written by other plugins and reports them.

Risk

Information
CVSS-Score: 0

Description

Logs generated by other plugins are reported by this plugin. Plugin debugging must be enabled in the policy in order for this plugin to run.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 12

An SSH server is listening on this port.

Risk

Information
CVSS-Score: 0

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 13

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Risk

Information
CVSS-Score: 0

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 14

The remote host is missing several patches.

Risk

Information
CVSS-Score: 0

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Objectives / Hosts

192.168.2.65

Recommended solution

Install the patches listed below.

Finding no. 17

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Risk

Information
CVSS-Score: 0

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 18

The remote service encrypts communications.

Risk

Information
CVSS-Score: 0

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 19

The remote host allows resuming SSL sessions.

Risk

Information
CVSS-Score: 0

Description

This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID. If the server accepts the session ID in the second connection, the server maintains a cache of sessions that can be resumed.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 21

The remote service appears to use OpenSSL to encrypt traffic.

Risk

Information
CVSS-Score: 0

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.
Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 22

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Risk

Information
CVSS-Score: 0

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.
The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

Objectives / Hosts

192.168.2.65

Recommended solution

Set a properly configured X-Frame-Options header for all requested resources.

Finding no. 23

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Risk

Information
CVSS-Score: 0

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.
The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

Objectives / Hosts

192.168.2.65

Recommended solution

Set a properly configured X-Frame-Options header for all requested resources.

Finding no. 24

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Risk

Information
CVSS-Score: 0

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.
The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

Objectives / Hosts

192.168.2.65

Recommended solution

Set a properly configured X-Frame-Options header for all requested resources.

Finding no. 25

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Risk

Information
CVSS-Score: 0

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.
The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

Objectives / Hosts

192.168.2.65

Recommended solution

Set a properly configured Content-Security-Policy header for all requested resources.

Finding no. 26

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Risk

Information
CVSS-Score: 0

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.
The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

Objectives / Hosts

192.168.2.65

Recommended solution

Set a properly configured Content-Security-Policy header for all requested resources.

Finding no. 27

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Risk

Information
CVSS-Score: 0

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.
The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

Objectives / Hosts

192.168.2.65

Recommended solution

Set a properly configured Content-Security-Policy header for all requested resources.

Finding no. 28

It was possible to enumerate CPE names that matched on the remote system.

Risk

Information
CVSS-Score: 0

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.
Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 29

This plugin determines which HTTP methods are allowed on various CGI directories.

Risk

Information
CVSS-Score: 0

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 30

This plugin determines which HTTP methods are allowed on various CGI directories.

Risk

Information
CVSS-Score: 0

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 31

This plugin determines which HTTP methods are allowed on various CGI directories.

Risk

Information
CVSS-Score: 0

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 32

This plugin determines which HTTP methods are allowed on various CGI directories.

Risk

Information
CVSS-Score: 0

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 33

This plugin determines which HTTP methods are allowed on various CGI directories.

Risk

Information
CVSS-Score: 0

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.
As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.
Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 35

Security patches are backported.

Risk

Information
CVSS-Score: 0

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.
Banner-based checks have been disabled to avoid false positives.
Note that this test is informational only and does not denote any security problem.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 37

Load estimation for web application tests.

Risk

Information
CVSS-Score: 0

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.
The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.
Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 39

Some information about the remote HTTP configuration can be extracted.

Risk

Information
CVSS-Score: 0

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 40

Some information about the remote HTTP configuration can be extracted.

Risk

Information
CVSS-Score: 0

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 41

Some information about the remote HTTP configuration can be extracted.

Risk

Information
CVSS-Score: 0

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 42

Some information about the remote HTTP configuration can be extracted.

Risk

Information
CVSS-Score: 0

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 43

Some information about the remote HTTP configuration can be extracted.

Risk

Information
CVSS-Score: 0

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...
This test is informational only and does not denote any security problem.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 44

The remote service could be identified.

Risk

Information
CVSS-Score: 0

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 45

The remote service could be identified.

Risk

Information
CVSS-Score: 0

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 46

The remote service could be identified.

Risk

Information
CVSS-Score: 0

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 47

The remote service could be identified.

Risk

Information
CVSS-Score: 0

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 48

The remote service could be identified.

Risk

Information
CVSS-Score: 0

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 49

The remote service could be identified.

Risk

Information
CVSS-Score: 0

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 50

The remote service encrypts communications using SSL.

Risk

Information
CVSS-Score: 0

Description

This plugin detects which SSL ciphers are supported by the remote service for encrypting communications.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 52

This plugin displays information about the Nessus scan.

Risk

Information
CVSS-Score: 0

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 53

It was possible to resolve the name of the remote host.

Risk

Information
CVSS-Score: 0

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 54

It is possible to determine which TCP ports are open.

Risk

Information
CVSS-Score: 0

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Objectives / Hosts

192.168.2.65

Recommended solution

Protect your target with an IP filter.

Finding no. 55

It is possible to determine which TCP ports are open.

Risk

Information
CVSS-Score: 0

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Objectives / Hosts

192.168.2.65

Recommended solution

Protect your target with an IP filter.

Finding no. 56

It is possible to determine which TCP ports are open.

Risk

Information
CVSS-Score: 0

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Objectives / Hosts

192.168.2.65

Recommended solution

Protect your target with an IP filter.

Finding no. 57

It is possible to determine which TCP ports are open.

Risk

Information
CVSS-Score: 0

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Objectives / Hosts

192.168.2.65

Recommended solution

Protect your target with an IP filter.

Finding no. 58

It is possible to determine which TCP ports are open.

Risk

Information
CVSS-Score: 0

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Objectives / Hosts

192.168.2.65

Recommended solution

Protect your target with an IP filter.

Finding no. 59

It is possible to determine which TCP ports are open.

Risk

Information
CVSS-Score: 0

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Objectives / Hosts

192.168.2.65

Recommended solution

Protect your target with an IP filter.

Finding no. 60

It is possible to determine which TCP ports are open.

Risk

Information
CVSS-Score: 0

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Objectives / Hosts

192.168.2.65

Recommended solution

Protect your target with an IP filter.

Finding no. 61

It is possible to determine which TCP ports are open.

Risk

Information
CVSS-Score: 0

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Objectives / Hosts

192.168.2.65

Recommended solution

Protect your target with an IP filter.

Finding no. 62

HTTP form based authentication.

Risk

Information
CVSS-Score: 0

Description

This script logs onto a web server through a login page and stores the authentication / session cookie.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 63

HTTP form based authentication.

Risk

Information
CVSS-Score: 0

Description

This script logs onto a web server through a login page and stores the authentication / session cookie.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 64

HTTP form based authentication.

Risk

Information
CVSS-Score: 0

Description

This script logs onto a web server through a login page and stores the authentication / session cookie.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 65

HTTP form based authentication.

Risk

Information
CVSS-Score: 0

Description

This script logs onto a web server through a login page and stores the authentication / session cookie.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 66

HTTP form based authentication.

Risk

Information
CVSS-Score: 0

Description

This script logs onto a web server through a login page and stores the authentication / session cookie.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 67

It is possible to enumerate directories on the web server.

Risk

Information
CVSS-Score: 0

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 68

It is possible to enumerate directories on the web server.

Risk

Information
CVSS-Score: 0

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 69

It is possible to enumerate directories on the web server.

Risk

Information
CVSS-Score: 0

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 70

A SSH server is running on the remote host.

Risk

Information
CVSS-Score: 0

Description

This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 71

This plugin displays the SSL certificate.

Risk

Information
CVSS-Score: 0

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 72

Nessus can crawl the remote website.

Risk

Information
CVSS-Score: 0

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.
It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 73

The remote web server does not return 404 error codes.

Risk

Information
CVSS-Score: 0

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page. Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 74

It was possible to obtain traceroute information.

Risk

Information
CVSS-Score: 0

Description

Makes a traceroute to the remote host.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 75

An SSH server is listening on this port.

Risk

Information
CVSS-Score: 0

Description

It is possible to obtain information about the remote SSH server by sending an empty authentication request.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 76

It is possible to determine the exact time set on the remote host.

Risk

Information
CVSS-Score: 0

Description

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Objectives / Hosts

192.168.2.65

Recommended solution

Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Finding no. 77

A web server is running on the remote host.

Risk

Information
CVSS-Score: 0

Description

This plugin attempts to determine the type and the version of the   remote web server.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 78

A web server is running on the remote host.

Risk

Information
CVSS-Score: 0

Description

This plugin attempts to determine the type and the version of the remote web server.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

Finding no. 79

A web server is running on the remote host.

Risk

Information
CVSS-Score: 0

Description

This plugin attempts to determine the type and the version of the remote web server.

Objectives / Hosts

192.168.2.65

Recommended solution

n/a

8 Annex

8.1 Tools used for assessment

8.1.1 Network vulnerability scanner

Nessus is a licensed vulnerability scanner designed to identify vulnerabilities, configuration problems, and malware in physical, virtual, and cloud environments. Nessus runs on all popular computer operating systems and provides official binary packages for Linux, Windows and Mac OS X.

- Nessus version : 7.0.1
- Plugin feed version : 201802021815

8.2 Explanations of the individual tests performed

This section describes the individual tests in more detail.

Name resolution

In most cases, the Domain Name System (DNS) is used to determine the associated IP address for a domain name. However, there is also the reverse situation where the name is required for a given IP address. If this resolution is enabled, a reverse DNS lookup is used.

Reachability

It is checked whether a host with an IP address is active in the network at the time of the test.

Open ports and services enumeration

A port is the part of a network address that causes the allocation of TCP and UDP connections and data packets to server and client programs through operating systems. Ports can also identify network protocols and network services.

Operating system enumeration

With a combination of remote probes (SMB, NTP, HTTP, TCP / IP, SNMP, etc.), it is often possible to determine the remote operating system. This makes it possible to determine whether a current operating system is used. If an operating system cannot be determined, this does not constitute a vulnerability.

Version and patch level enumeration

Various requests are used to determine from the outside which versions and updates are installed on the system. This test merely provides an indication of what information can be easily retrieved by an external party. Only with a privileged access to the system such information can be reliably determined.

SSL certificate verification

Transport Layer Security (TLS), more commonly known as the Secure Sockets Layer (SSL), is a hybrid encryption protocol for secure data transmission over the Internet. TLS encryption is now used mainly with HTTPS. Typically, the server first authenticates against the client with a certificate. The certificate is issued by a certification authority (CA) and a publicly available signature verification key is assigned to a specific person or organization. This certification is confirmed by the certification body by providing the digital signature for the certificate. If a browser does not know a CA, a user cannot directly ensure that the communication between the right instances takes place.

Information on Encryption

The use of current encryption algorithms is verified. Used encryption protocols are validated against their level of security. The algorithms used for encryption are checked for security. It is checked whether the key length is sufficiently long in the used encryption.

Backdoor check

A backdoor (also a trapdoor) is a part of a software that allows users to gain access to the IT system or to an otherwise protected function of an application by bypassing normal access security. One example is universal passwords or a special software (usually secretly installed by a Trojan), which allows remote access on the IT system.

Check for usage of standard accounts

Often, the initial configuration of an application or an IT system consists of standard access data, which is-given by the manufacturer and is often the same for all such systems. If such standard access data is not changed, there is a risk of unauthorized access.

Remote shell access

Many IT systems offer the possibility to access the command plane via a connection. This access is not always disabled.

Exploitable vulnerabilities in the operating system

If operating systems are configured incorrectly or are not up-to-date, the system could be vulnerable. An attacker may exploit these vulnerabilities.

Exploitable vulnerabilities in services / applications

If services or applications are configured incorrectly or are not up-to-date, the system could be vulnerable. An attacker could exploit these vulnerabilities.

Identify web server

Often banners or other parameters can be used to determine which web server is used in which version. This can be used to determine whether a web server is up-to-date.

HTTP Header examination

HTTP header fields (often inaccurate HTTP headers) are components of the Hypertext Transfer Protocol (HTTP) protocol header and transmit the parameters and arguments important for the transmission of files via HTTP.

Depending on the web page, possible security options should be used in the http header. This improves the security on the client side and contributes to the protection of the users.

HTTP OPTIONS identification

It is checked whether http request methods can be used that could pose a threat to the application or to the user.

8.3 Glossary

(IT-) Assessment

The term is understood as an evaluation of an IT environment.

Audit

The aim of an audit is to provide a documented status of the level of safety, the detection of deficiencies and security gaps as well as the assessment by means of an independent review of the existing technical and organizational security measures.

Depending on the area, the actual state is analyzed during an audit or a comparison of the original objective with the actually achieved goals is determined. Often an audit is also intended to identify general problems or an needed improvements.

Black-Box-Test

Designates a test method from software development in which the tests are developed without knowledge of the internal functioning of the IT system to be tested. This term is often used synonymously with the term "zero knowledge test" in IT vulnerability analysis.

Code Review

Code Review refers to the review of source texts (source recension) by another person. The method of code review is used to improve and assure the quality of computer programs.

Dynamic Application Security Testing (DAST)

Main focus of the DAST is the detection of errors and security gaps in a web application itself and a verification of the webserver on the operating system level.

Gray-Box-Test

Designates a test method from the software development, in which the tests are only developed with a partial knowledge about the internal functioning of the IT system to be tested. This term is often used synonymously with the term "half knowledge test" in IT vulnerability analysis.

Network Security Scan (NSS)

An NSS is a vulnerability scan using a vulnerability scanner. The results are being prepared and recommendations are made to eliminate weaknesses.

Penetration test

Penetration test is the technical language for a comprehensive security test of individual computers or networks of any size. However, the aim of such a test is not only to uncover a possible weakness but also to prove its existence by actually exploiting the weakness point and penetrating an IT system.

Vulnaribility

Vulnerabilities are the cause of security breaches.

Security vulnaribility

A security vulnerability is an error in a software, in the logic, or in a configuration that can be used for manipulation or intrusion by malicious code or an attacker. Problems in the organization of a company or in the processes used can also lead to security vulnerabilities.

System Security Check (SSC)

An SSC is performed by accessing a system with privileged rights for a direct system examination.

Vulnerability Scanner

A software tool that automatically or semi-automatically performs security tests and reports vulnerable points.

White-Box-Test

Describes a test method from the software development, in which the tests are developed with knowledge about the internal functioning of the IT system to be tested. This term is often used synonymously with the term "full knowledge test" in IT vulnerability analysis