

**TechnicalREPORT**

NETWORK VULNERABILITY ASSESSMENT

INTESA SAN PAOLO  
reportname

document SPECS

|  |  |  |  |
| --- | --- | --- | --- |
| **Activity ID** | Activity.Code | | |
| **Classification** | RESTRICTED | | |
| **Author** | Accenture | | |
| **File Name** | Activity.Code\_ReportName.docx | | |
| **Version** | 1.0 | **Status** | FINAL |
| **Creation Date** | Is.today | **Last Update** | Is.today |

N.B:

1) Documents classified as “Internal use only” must not be disclosed nor distributed outside of Intesa Sanpaolo.

2) In the event a person receives a document classified as "Restricted" and her name is not in the list of people who are authorized to use it, she has to give the document to one of the people named in the abovementioned list.

TABLE OF CONTENTS

1 Assessment Overview 5

1.1 Scope 5

1.2 Rules of Engagement (RoE) 6

1.3 Methodology 6

1.3.1 Information Gathering 6

1.3.2 Scanning & Vulnerability Analysis 7

1.3.3 Exploitation 7

1.3.4 Post Exploitation 8

1.3.5 Tools 8

1.4 Risk Evaluation Model 8

2 Executive Summary 10

3 Remediation Plan 11

4 Findings 14

4.1 OpenSSL Unsupported 14

4.2 ESXi 5.5 / 6.0 / 6.5 / 6.7 Multiple Vulnerabilities 16

4.3 Unsupported Web Server Detection 18

4.4 Microsoft RDP RCE (CVE-2019-0708) (uncredentialed check) 20

4.5 IBM WebSphere Java Object Deserialization RCE 22

4.6 IBM DB2 9.7 < Fix Pack Multiple Vulnerabilities 23

4.7 rexecd Service Detection 25

4.8 Apache 2.2.x < 2.2.34 Multiple Vulnerabilities 26

4.9 rlogin Service Detection 28

4.10 SAP Gateway 10Kblaze Remote Code Execution Vulnerability 29

4.11 OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities 30

4.12 Detected vulnerable Oracle TNS Listener 32

4.13 SSL Certificate Signed Using Weak Hashing Algorithm 34

4.14 TLS Session Renegotiation 41

4.15 NFS Share User Mountable / Information Disclosure 42

4.16 SSL Version 2 and 3 Protocol Detection 44

4.17 SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened Encryption) 50

4.18 RC4 Ciphers Supported 52

4.19 Unencrypted Telnet Server 56

4.20 SSL Medium Strength Cipher Suites Supported (SWEET32) 57

4.21 SSL Anonymous Cipher Suites Supported 64

4.22 OpenSSL AES-NI Padding Oracle MitM Information Disclosure 65

4.23 Network Time Protocol (NTP) Mode 6 Scanner 66

4.24 SMB Signing not required 68

4.25 Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness 70

4.26 User Enumeration via SMTP 72

4.27 HTTP TRACE / TRACK Enabled 73

4.28 DNS Server Cache Snooping Remote Information Disclosure 74

4.29 SSL Weak Cipher Suites Supported 76

4.30 Apache Tomcat Default Files 78

4.31 ETAG Header Information Disclosure 79

4.32 Apache mod\_status / mod\_info / server-status / server-info Information Disclosure 81

4.33 X Display Manager Control Protocol (XDMCP) Detection 82

4.34 SSL Certificate Chain Contains RSA Keys Less Than 2048 bits 83

4.35 SSH Weak Algorithms Supported 88

4.36 SSL Certificate Chain Contains Weak RSA Keys 90

4.37 Web Server Uses Basic Authentication Without HTTPS 91

4.38 Terminal Services doesn't use network level authentication (NLA) only 97

4.39 Terminal Services Encryption Level is Medium or Low 99

4.40 SSL/TLS EXPORT\_RSA <= 512-bit Cipher Suites Supported (FREAK) 101

4.41 Transport Layer Security (TLS) Protocol CRIME Vulnerability 102

4.42 PHP expose\_php Information Disclosure 103

4.43 SSL/TLS Diffie-Hellman Modulus with 1024 Bits (LogJam) 104

4.44 SSH Server CBC Mode Ciphers Enabled 107

4.45 SSH Weak MAC Algorithms Supported 109

4.46 TLSv1.0 Supported – BEAST Attack 111

4.47 HSTS Disabilitato 118

# Assessment Overview

In RP19\_49\_NVA\_OB\_Banca CIB Internal LAN Servers quarto trimestre Accenture Security verified the security posture of the targets in scope, part of the Intesa Sanpaolo internal hosts, through an Infrastructure Penetration Test activity.

## Scope

The following table summarizes the Target of Evaluation (ToE), the timeframe in which the activity was executed and the IP addresses from which the assessment was performed (attack point).

|  |  |  |  |
| --- | --- | --- | --- |
| **ToE** |  | | |
| **Data Inizio** |  | **Data Fine** |  |
| **Inizio Finestra Temporale** | 9:00 - CEST | **Fine Finestra Temporale** | 17:00 - CEST |
| **Attack Point** |  | | |
| **Modalità Operativa** | Black-box. Sono stati forniti solo indirizzi IP in-scope. | | |

## Rules of Engagement (RoE)

The Rules of Engagement (RoE) establish what is and what is not possible to do during a security testing activity. In this specific case, the Rules of Engagement forbid any kind of activity that can result in service unavailability.

## Methodology

The methodology adopted by Accenture Security comes from the best-of-breed of the following methodologies and from many years of international experience in the Ethical Hacking field:

* OWASP
* SANS
* EC-Council
* NIST
* OSSTMM
* PTES

The Security Testing service for Infrastructure Penetration Testing include 4 macro-steps:

1. Information Gathering
2. Scanning & Vulnerability Analysis
3. Exploitation
4. Post Exploitation

### Information Gathering

Many companies do not know how much information regarding them are public and how these could be used by an attacker. In the same way, many employees do not take into consideration the amount of information they publicly share and how these could be exploited by an attacker to attack them or the company they work for.

The Intelligence Gathering is a reconnaissance task (Recon) with the objective of gaining as much information as possible about a target and to reuse these in the next attack phases. The more information is obtained the more attack vectors can be used.

The information gathered in this activity includes technical details of the hosts in the target perimeter and details about services exposed by the host.

### Scanning & Vulnerability Analysis

The Vulnerability Analysis phase is strictly bound to the vulnerability testing concept, that is the process of finding vulnerabilities that can be exploited by an attacker. These vulnerabilities depend on various factors such as misconfigurations of the services, obsolete software, etc.

The Scanning phase is related to identifying open TCP/UDP ports on the targets. Then, service fingerprinting is executed to further identity specific service and version running on the targets.

The approach used for the Vulnerability Analysis is based on the OSSTMM (<http://www.isecom.org/research/osstmm.html>) methodology that includes the following test categories:

* Operative Systems (Windows, Linux, Unix, MacOs, Solaris, BSD, AIX, z/OS, HP/UX, etc.)
* Hypervisor (Xen, Oracle VM Server, Citrix XenServer, VmWare ESX/i, etc.)
* Services (Active Directory, LDAP, Mail, Database, DNS, Web Server, FTP, LDAP, VPN, etc.)
* Protocols (CIFS, SSL, SSH, RDP, Telnet, HTTP, SMTP, SNMP, ZigBee, LoRa, Z-Wave, 802.x, SCTP, SIGTRAN, SS7, ISO 1800, etc.)

The Vulnerability Analysis phase includes two kind of analysis: Passive and Active. The Passive mode consist in the passive interception of the traffic generated during a normal and legit interaction with the service and the analysis of the requests and responses looking for detectable vulnerabilities. Since not every vulnerability is detectable in passive mode, it is also necessary to perform Active mode analysis, which includes direct interaction with the component subject of the test. In detail, this mode includes the generation of artifacts requests that fall outside the normal use cases of the service, and consequently could alter the behavior of this if those requests are not handled properly.

### Exploitation

The Exploitation phase focuses on gaining access to a system or a resource bypassing the in-place security measures. The main objective is to identify the fundamental access points that an attacker could exploit to penetrate the defenses of the target company, and therefore its most valuable assets.

If the Vulnerability Analysis phase was properly done, the attacker should have a list of high sensitivity targets and a list of potential exploitable access points, therefore this phase will be extremely precise and planned to reduce the potential risks originated by this kind of activity (potential system reboot and service unavailability).

The complexity of this phase is bound to the protection systems in place like Intrusion Prevention System, Antivirus, Web Application Firewall, or other attack mitigation mechanisms.

To bypass the security mechanism in place it might be necessary to use evasion techniques like payload obfuscation to evade Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) and encoding of requests/responses to deceive the web application firewalls (WAF), etc.

### Post Exploitation

The Post Exploitation phase allows to determine the value of the exploited system and to maintain access on such system for the next interactions. The value of the system depends on the level of Confidentiality of the data that the system contains and on the possibility to use such system to attack other systems on the same or adjacent network. All the operating modes used in this phase are defined according to the Rules of Engagement.

### Tools

Tools used in Penetration Testing activity include:

* Port and Service Scanners (e.g. nmap, netcat, amap, etc.)
* Vulnerability Scanner (e.g. Tenable Nessus, OpenVAS, etc.);
* Interception Proxy (e.g. Portswigger Burp, OWASP Zap, etc.);
* Ad-hoc Service Assessment Tools (e.g. sslscan, sslyze, etc.)
* Exploitation tools (Metasploit/Armitage, BEeF, sqlmap, etc.)

## Risk Evaluation Model

The risk evaluation model is based on international standards, defined by FIRST, and measurable concept defined by MITRE. These are mandatory to have a unique dictionary to define vulnerabilities (CVE), weaknesses (CWE), attack patterns (CAPEC), configurations (CCE) and platforms (CPE) and a single way to evaluate all vulnerabilities. This allow to define a model that is the most possible objective and compatible with the most used standards and platforms.

The risk associated to a vulnerability is evaluated through the Common Vulnerability Scoring System (CVSS) version 3 and depends to several objective parameters like the attack vector, the attack complexity, the need of authentication and user interaction, the impacts of the vulnerabilities exploitation to other assets and the impacts in terms of confidentiality, integrity and availability, etc.

The evaluation process of a single vulnerability is divided into four phases:

1. Identification of the public score (CVSS) associated to the vulnerability based on the maximum value among those linked to the CVEs related to the vulnerability, if available;
2. Contextualization of the score based on the actual environment, modifying, if necessary, the values related to the access vector (Attack Vector AV) and the values of Confidentiality (Confidentiality C), Integrity (Integrity I) and Availability (Availability A) of the data contained in the asset;
3. Recalculation of the score based on the result of the exploitation phase going to re-evaluate the true complexity of the attack (Attack Complexity AC), which depend on the protective measures in place, and inserting, in the calculation, the level of maturity of the exploit used (exploit Code Maturity E), the complexity of the remediation (remediation level RL) and the confidence value on the obtained result (Report confidence RC)
4. Conversion of the score, expressed on a scale 0 - 10, in a level of risk according to the following scheme.

|  |  |
| --- | --- |
| **Level** | **Description** |
| **Critical** | The vulnerability allows the attacker to completely compromise the target application. (CVSS score: 9.0-10.0) |
| **High** | The vulnerability allows executing malicious code, not authorized access to administrative sections of the application, to access data stored on databases. (CVSS score: 7.0-8.9) |
| **Medium** | The vulnerability allows you to acquire sensitive information or at least important that can be used in subsequent attacks. The vulnerability could allow an attacker to modify the normal operation of the application. (CVSS score: 4.0-6.9) |
| **Low** | The vulnerability allows you to acquire information on the configuration (CVSS score: 0.0) or allows you to permit an attack with limited impact on the business of the client. (CVSS score: 0.1-3.9) |

# Executive Summary

The activity Activity.Code\_ReportName included hosts.

The testing activity found a lot of open ports, there was a great heterogeneity of services exposed.

Considering the results of the activity, it is suggested to concentrate the remediation phase on the following points:

* To remedy the misconfiguration
* Purchase or generate a proper certificate for this service.
* Upgrade the services
* Apply the patches

# Remediation Plan

Ad To fix the found vulnerabilities it is recommended to apply the suggested remediation plan.

The order by which the remediation should be applied reflects the severity associated to the respective vulnerability. For all those not verified vulnerabilities, the associated remediation should be checked if already applied first.

remed.plan

Copyright © 2018 Accenture

All rights reserved.

Accenture, its logo, and

High Performance Delivered

are trademarks of Accenture.

# Findings

{List}

Tech.Report