

# **Network Vulnerability Assessment**

## **Reports and Final Analysis using OpenVas Tool**

**Target : “192.168.1.56”**

**Tool Used : OpenVas**

**Initial Date : 10th January 2025**

**Final Date : 25th January 2025**

---

### **Assessment Overview:**

The Network Vulnerability Assessment involves a hands-on exercise and experiment for students, learners and especially for interns and IT Junior Professionals, where they are provided with a simulated network environment. This simulated environment has various benefits, which includes a practical lab, a virtual environment where the real time system or the host won't be affected if the target network is risky. They are tasked with conducting a thorough vulnerability assessment using tools such as Nessus or OpenVAS. This project is designed to build their skills in identifying, analyzing, and mitigating network vulnerabilities specialising the tool “OpenVas”.

---

### **Simulated Network Setup:**

#### **Environment Description:**

##### **1. Network Topology:**

- A virtual network, especially a WLAN is considered along with its physical components, such as routers, switches, etc.
- The Operating System (OS) : Windows 10

## 2. Components:

- **Servers:** A web server, a database server, and a file server connected to the connected network
- **Workstations:** Two client machines with outdated software.
- **Firewalls and Routers:** Configure the Scan and Prioritize the scan details based on the network details.

## 3. Predefined Vulnerabilities: (Presumptions)

- Unpatched software vulnerabilities.
- Open ports and unnecessary services.
- Weak passwords and misconfigured user permissions.
- Brute Force, CORS, SQL Injection on the possible connected networks.

### Tools Provided:

- OpenVas (Open Source, Github Reference).
  - Documentation for the tool.
- 

## Assessment Steps:

### 1. Vulnerability Scanning:

- I have conducted the scan on the target “192.168.1.56” using “OpenVas”.
- Objectives include:
  - Identifying vulnerabilities in the network.
  - Assessing the severity levels of each vulnerability.
  - Exporting detailed scan reports.

### 2. Analysis and Prioritization:

- I have keenly analysed and packed details based on the following factors and terms:
  - High-risk vulnerabilities that require immediate attention.
  - Medium and low-risk vulnerabilities for long-term planning.
  - False positives and validation of identified issues.

### 3. Mitigation Plan:

- Based on their findings, I have developed a remediation strategy, which should include:
  - Applying security patches.
  - Hardening configurations (e.g., disabling unnecessary ports/services).
  - Strengthening user access policies.
  - Addressing specific vulnerabilities (e.g., fixing SQL injection flaws).

### 4. Implementation:

- Interns may be asked to apply mitigation techniques in the simulated environment.
- Post-mitigation scans to verify the effectiveness of the implemented solutions.
- Any **HIGH** and **MEDIUM** severity vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be chained with other vulnerabilities to enable further attacks.

*A Detailed Report on the Host done along with Severity Level and Timings.*

#### Host Summary

Host	Start	End	High	Medium	Low	Log
192.168.1.56 (WIDGETServer)	Jan 15, 13:46	Jan 15, 14:13	1	6	1	0
Total: 1			1	6	1	0

*Severity Levels Found!*

#### Vulnerability Summary

Severity	Description	CVSS	Count
High	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3	1
Medium	DCE/RPC and MSRPC Services Enumeration Reporting	5.0	1
Medium	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	5.0	1
Medium	SSL/TLS: Report Weak Cipher Suites	4.3	4
Low	TCP timestamps	2.6	1

---

## **Deliverables:**

### **1. Vulnerability Assessment Report:**

- Comprehensive details on identified vulnerabilities from the OpenVAS scan of "192.168.1.56."
- Categorization by severity (critical, high, medium, low).
- Risk assessment and potential impacts.

### **2. Mitigation Plan:**

- Step-by-step recommendations for remediation.
- Justifications for proposed actions.
- Timeline for implementing fixes.

### **3. Post-Mitigation Report (if applicable):**

- Updated scan results showing resolved issues.
- Analysis of remaining vulnerabilities.

*Port Summary Done and Probable Weakness in the Google “192.168.1.56” Server.*

#### **Port Summary for Host 192.168.1.56**

---

Service (Port)	Severity
general/tcp	Low
3389/tcp	Medium
636/tcp	Medium
445/tcp	High
443/tcp	Medium
135/tcp	Medium
3269/tcp	Medium

The Reports Produced through the Scanners are considered voluminous. So as per my report, references from the internet and study, I will reduce the contents to as much short and precise as possible.

*We have considered some under different categories and some are shown under the scores:*

## 1) High Severity ( Above 8.0 Score)

### Security Issues for Host 192.168.1.56

<b>High</b> (CVSS: 9.3) NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)	445/tcp
<b>Summary</b> This host is missing a critical security update according to Microsoft Bulletin MS17-010.	
<b>Vulnerability Detection Result</b> Vulnerability was detected according to the Vulnerability Detection Method.	
<b>Impact</b> Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.	
<b>Solution</b> <b>Solution type:</b> VendorFix Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory	
<b>Affected Software/OS</b> Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016 Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2	
<b>Vulnerability Insight</b> Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.	
<b>Vulnerability Detection Method</b> Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.  Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID: 1.3.6.1.4.1.25623.1.0.810676)  Version used: \$Revision: 11874 \$	
<b>References</b>  CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148 BID: 96703, 96704, 96705, 96707, 96709, 96706 CERT: CB-K17/0435, DFN-CERT-2017-0448 Other: <a href="https://support.microsoft.com/en-in/kb/4013078">https://support.microsoft.com/en-in/kb/4013078</a> <a href="https://technet.microsoft.com/library/security/MS17-010">https://technet.microsoft.com/library/security/MS17-010</a> <a href="https://github.com/rapid7/metasploit-framework/pull/8167/files">https://github.com/rapid7/metasploit-framework/pull/8167/files</a>	

## 2) Medium (Around 5.0)

<b>Medium</b> (CVSS: 5.0) NVT: DCE/RPC and MSRPC Services Enumeration Reporting (OID: 1.3.6.1.4.1.25623.1.0.10736)	135/tcp
<b>Summary</b>  Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.	
<b>Vulnerability Detection Result</b>  Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:  Port: 49664/tcp  UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49664]  Port: 49665/tcp  UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49665] Annotation: DHCP Client LRPC Endpoint  UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49665] Annotation: DHCPv6 Client LRPC Endpoint  UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49665] Annotation: Event log TCPIP  Port: 49666/tcp  UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0 Endpoint: ncacn_ip_tcp:192.168.1.56[49666] Annotation: RemoteAccessCheck  UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49666] Named pipe : lsass Win32 service or process : Netlogon Description : Net Logon service  UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0 Endpoint: ncacn_ip_tcp:192.168.1.56[49666] Named pipe : lsass Win32 service or process : lsass.exe Description : LSA access  UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49666] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access  UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49666] Annotation: Ngc Pop Key Service  UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49666] Annotation: Ngc Pop Key Service  UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:192.168.1.56[49666] Annotation: KeyIso	

<p>Description : LSA access</p> <p>UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49674] Named pipe : lsass Win32 service or process : lsass.exe Description : SAM access</p> <p>UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49674] Annotation: Ngc Pop Key Service</p> <p>UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49674] Annotation: Ngc Pop Key Service</p> <p>UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2 Endpoint: ncacn_ip_tcp:192.168.1.56[49674] Annotation: KeyIso</p> <p>Port: 49675/tcp</p> <p>UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49675]</p> <p>UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49675] Named pipe : spoolss Win32 service or process : spoolsv.exe Description : Spooler service</p> <p>UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49675]</p> <p>UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49675]</p> <p>UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49675]</p> <p>Port: 49683/tcp</p> <p>UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2 Endpoint: ncacn_ip_tcp:192.168.1.56[49683]</p> <p>Port: 49728/tcp</p> <p>UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5 Endpoint: ncacn_ip_tcp:192.168.1.56[49728] Named pipe : dnsserver Win32 service or process : dns.exe Description : DNS Server</p> <p>Port: 49914/tcp</p> <p>UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1 Endpoint: ncacn_ip_tcp:192.168.1.56[49914] Annotation: Frs2 Service</p> <p>Port: 63520/tcp</p> <p>UUID: 91ae6020-9e3c-11cf-8d7c-00aa00c091be, version 0 Endpoint: ncacn_ip_tcp:192.168.1.56[63520] Named pipe : cert Win32 service or process : certsrv.exe Description : Certificate service</p>
---

<p>Note: DCE/RPC or MSRPC services running on this host locally were identified. Reporting this list is not enabled by default due to the possible large size of this list. See the script preferences to enable this reporting.</p>
<p><b>Impact</b></p> <p>An attacker may use this fact to gain more knowledge about the remote host.</p>
<p><b>Solution</b></p> <p><b>Solution type:</b> Mitigation</p> <p>Filter incoming traffic to this ports.</p>
<p><b>Vulnerability Detection Method</b></p> <p>Details: DCE/RPC and MSRPC Services Enumeration Reporting (OID: 1.3.6.1.4.1.25623.1.0.10736)</p> <p>Version used: \$Revision: 6319 \$</p>

<b>Medium</b> (CVSS: 5.0) NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (OID: 1.3.6.1.4.1.25623.1.0.108031)	443/tcp
<b>Summary</b>  This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.	
<b>Vulnerability Detection Result</b>  'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:  TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)  'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:  TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)  'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:  TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)	
<b>Solution</b>  <b>Solution type:</b> Mitigation  The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.	
<b>Affected Software/OS</b>  Services accepting vulnerable SSL/TLS cipher suites via HTTPS.	
<b>Vulnerability Insight</b>  These rules are applied for the evaluation of the vulnerable cipher suites:  - 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).	
<b>Vulnerability Detection Method</b>  Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS (OID: 1.3.6.1.4.1.25623.1.0.108031)  Version used: \$Revision: 5232 \$	
<b>References</b>  CVE: CVE-2016-2183, CVE-2016-6329 CERT: CB-K18/0296, CB-K17/1980, CB-K17/1871, CB-K17/1803, CB-K17/1753, CB-K17/1750, CB-K17/1709, CB-K17/1558, CB-K17/1273, CB-K17/1202, CB-K17/1196, CB-K17/1055, CB-K17/1026, CB-K17/0939, CB-K17/0917, CB-K17/0915, CB-K17/0877, CB-K17/0796, CB-K17/0724, CB-K17/0661, CB-K17/0657, CB-K17/0582, CB-K17/0581, CB-K17/0506, CB-K17/0504, CB-K17/0467, CB-K17/0345, CB-K17/0098, CB-K17/0089, CB-K17/0086, CB-K17/0082, CB-K16/1837, CB-K16/1830, CB-K16/1635, CB-K16/1630, CB-K16/1624, CB-K16/1622, CB-K16/1500, CB-K16/1465, CB-K16/1307, CB-K16/1296, DFN-CERT-2019-0068, DFN-CERT-2018-1296, DFN-CERT-2018-0323, DFN-CERT-2017-2070, DFN-CERT-2017-1954, DFN-CERT-2017-1885, DFN-CERT-2017-1831, DFN-CERT-2017-1821, DFN-CERT-2017-1785, DFN-CERT-2017-1626, DFN-CERT-2017-1326, DFN-CERT-2017-1239, DFN-CERT-2017-1238, DFN-CERT-2017-1090, DFN-CERT-2017-1060, DFN-CERT-2017-0968, DFN-CERT-2017-0947, DFN-CERT-2017-0946, DFN-CERT-2017-0904, DFN-CERT-2017-0816, DFN-CERT-2017-0746, DFN-CERT-2017-0677, DFN-CERT-2017-0675, DFN-CERT-2017-0611, DFN-CERT-2017-0609, DFN-CERT-2017-0522, DFN-CERT-2017-0519, DFN-CERT-2017-0482, DFN-CERT-2017-0351, DFN-CERT-2017-0090, DFN-CERT-2017-0089, DFN-CERT-2017-0088, DFN-CERT-2017-0086, DFN-CERT-2016-1943, DFN-CERT-2016-1937, DFN-CERT-2016-1732, DFN-CERT-2016-1726, DFN-CERT-2016-1715, DFN-CERT-2016-1714, DFN-CERT-2016-1588, DFN-CERT-2016-1555, DFN-CERT-2016-1391, DFN-CERT-2016-1378 Other: <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> <a href="https://mozilla.github.io/server-side-tls/ssl-config-generator/">https://mozilla.github.io/server-side-tls/ssl-config-generator/</a> <a href="https://sweet32.info/">https://sweet32.info/</a>	



### 3) Medium (Around 4.3)

<b>Medium</b> (CVSS: 4.3) NVT: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)		3389/tcp
<b>Summary</b>  This routine reports all Weak SSL/TLS cipher suites accepted by a service.  <b>NOTE:</b> No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.		
<b>Vulnerability Detection Result</b>  'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:  TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA  'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:  TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA  'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:  TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA		
<b>Solution</b>  <b>Solution type:</b> Mitigation  The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.  Please see the references for more resources supporting you with this task.		
<b>Vulnerability Insight</b>  These rules are applied for the evaluation of the cryptographic strength:  - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).  - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).  - 1024 bit RSA authentication is considered to be insecure and therefore as weak.  - Any cipher considered to be secure for only the next 10 years is considered as medium  - Any other cipher is considered as strong		
<b>Vulnerability Detection Method</b>  Details: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)  Version used: \$Revision: 11135 \$		
<b>References</b>  CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000		
  CERT: CB-K17/1750, CB-K16/1593, CB-K16/1552, CB-K16/1102, CB-K16/0617, CB-K16/0599, CB-K16/0168, CB-K16/0121, CB-K16/0090, CB-K16/0030, CB-K15/1751, CB-K15/1591, CB-K15/1550, CB-K15/1517, CB-K15/1514, CB-K15/1464, CB-K15/1442, CB-K15/1334, CB-K15/1269, CB-K15/1136, CB-K15/1090, CB-K15/1059, CB-K15/1022, CB-K15/1015, CB-K15/0986, CB-K15/0964, CB-K15/0962, CB-K15/0932, CB-K15/0927, CB-K15/0926, CB-K15/0907, CB-K15/0901, CB-K15/0896, CB-K15/0889, CB-K15/0877, CB-K15/0850, CB-K15/0849, CB-K15/0834, CB-K15/0827, CB-K15/0802, CB-K15/0764, CB-K15/0733, CB-K15/0667, CB-K14/0935, CB-K13/0942, DFN-CERT-2017-1821, DFN-CERT-2016-1692, DFN-CERT-2016-1648, DFN-CERT-2016-1168, DFN-CERT-2016-0665, DFN-CERT-2016-0642, DFN-CERT-2016-0184, DFN-CERT-2016-0135, DFN-CERT-2016-0101, DFN-CERT-2016-0035, DFN-CERT-2015-1853, DFN-CERT-2015-1679, DFN-CERT-2015-1632, DFN-CERT-2015-1608, DFN-CERT-2015-1542, DFN-CERT-2015-1518, DFN-CERT-2015-1406, DFN-CERT-2015-1341, DFN-CERT-2015-1194, DFN-CERT-2015-1144, DFN-CERT-2015-1113, DFN-CERT-2015-1078, DFN-CERT-2015-1067, DFN-CERT-2015-1038, DFN-CERT-2015-1016, DFN-CERT-2015-1012, DFN-CERT-2015-0980, DFN-CERT-2015-0977, DFN-CERT-2015-0976, DFN-CERT-2015-0960, DFN-CERT-2015-0956, DFN-CERT-2015-0944, DFN-CERT-2015-0937, DFN-CERT-2015-0925, DFN-CERT-2015-0884, DFN-CERT-2015-0881, DFN-CERT-2015-0879, DFN-CERT-2015-0866, DFN-CERT-2015-0844, DFN-CERT-2015-0800, DFN-CERT-2015-0737, DFN-CERT-2015-0696, DFN-CERT-2014-0977  Other: <a href="https://www.bsi.bund.de/SharedDocs/Warmmeldungen/DE/CB/warmmeldung_cb-k16-1465_update_6.html">https://www.bsi.bund.de/SharedDocs/Warmmeldungen/DE/CB/warmmeldung_cb-k16-1465_update_6.html</a> <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> <a href="https://mozilla.github.io/server-side-tls/ssl-config-generator/">https://mozilla.github.io/server-side-tls/ssl-config-generator/</a>		

#### 4) Medium Range Continued for different range

Medium (CVSS: 4.3) NVT: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)		3269/tcp
<b>Summary</b>  This routine reports all Weak SSL/TLS cipher suites accepted by a service.  NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.		
<b>Vulnerability Detection Result</b>  'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:  TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA  'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:  TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA  'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:  TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA		
<b>Solution</b>  <b>Solution type:</b> Mitigation  The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.  Please see the references for more resources supporting you with this task.		
<b>Vulnerability Insight</b>  These rules are applied for the evaluation of the cryptographic strength:  - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).  - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).  - 1024 bit RSA authentication is considered to be insecure and therefore as weak.  - Any cipher considered to be secure for only the next 10 years is considered as medium  - Any other cipher is considered as strong		
<b>Vulnerability Detection Method</b>  Details: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)  Version used: \$Revision: 11135 \$		
<b>References</b>  CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000		
  CERT: CB-K17/1750, CB-K16/1593, CB-K16/1552, CB-K16/1102, CB-K16/0617, CB-K16/0599, CB-K16/0168, CB-K16/0121, CB-K16/0090, CB-K16/0030, CB-K15/1751, CB-K15/1591, CB-K15/1550, CB-K15/1517, CB-K15/1514, CB-K15/1464, CB-K15/1442, CB-K15/1334, CB-K15/1269, CB-K15/1136, CB-K15/1090, CB-K15/1059, CB-K15/1022, CB-K15/1015, CB-K15/0986, CB-K15/0964, CB-K15/0962, CB-K15/0932, CB-K15/0927, CB-K15/0926, CB-K15/0907, CB-K15/0901, CB-K15/0896, CB-K15/0889, CB-K15/0877, CB-K15/0850, CB-K15/0849, CB-K15/0834, CB-K15/0827, CB-K15/0802, CB-K15/0764, CB-K15/0733, CB-K15/0667, CB-K14/0935, CB-K13/0942, DFN-CERT-2017-1821, DFN-CERT-2016-1692, DFN-CERT-2016-1648, DFN-CERT-2016-1168, DFN-CERT-2016-0665, DFN-CERT-2016-0642, DFN-CERT-2016-0184, DFN-CERT-2016-0135, DFN-CERT-2016-0101, DFN-CERT-2016-0035, DFN-CERT-2015-1853, DFN-CERT-2015-1679, DFN-CERT-2015-1632, DFN-CERT-2015-1608, DFN-CERT-2015-1542, DFN-CERT-2015-1518, DFN-CERT-2015-1406, DFN-CERT-2015-1341, DFN-CERT-2015-1194, DFN-CERT-2015-1144, DFN-CERT-2015-1113, DFN-CERT-2015-1078, DFN-CERT-2015-1067, DFN-CERT-2015-1038, DFN-CERT-2015-1016, DFN-CERT-2015-1012, DFN-CERT-2015-0980, DFN-CERT-2015-0977, DFN-CERT-2015-0976, DFN-CERT-2015-0960, DFN-CERT-2015-0956, DFN-CERT-2015-0944, DFN-CERT-2015-0937, DFN-CERT-2015-0925, DFN-CERT-2015-0884, DFN-CERT-2015-0881, DFN-CERT-2015-0879, DFN-CERT-2015-0866, DFN-CERT-2015-0844, DFN-CERT-2015-0800, DFN-CERT-2015-0737, DFN-CERT-2015-0696, DFN-CERT-2014-0977  Other: <a href="https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warmmeldungen_cb-k16-1465_update_6.html">https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warmmeldungen_cb-k16-1465_update_6.html</a> <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> <a href="https://mozilla.github.io/server-side-tls/ssl-config-generator/">https://mozilla.github.io/server-side-tls/ssl-config-generator/</a>		

<b>Medium</b> (CVSS: 4.3) NVT: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)	443/tcp
<b>Summary</b> This routine reports all Weak SSL/TLS cipher suites accepted by a service. <b>NOTE:</b> No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.	
<b>Vulnerability Detection Result</b> 'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:  TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA  'Weak' cipher suites accepted by this service via the TLSv1.1 protocol:  TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA  'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:  TLS_RSA_WITH_RC4_128_MD5 TLS_RSA_WITH_RC4_128_SHA	
<b>Solution</b> <b>Solution type:</b> Mitigation The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore. Please see the references for more resources supporting you with this task.	
<b>Vulnerability Insight</b> These rules are applied for the evaluation of the cryptographic strength: - RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808). - Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000). - 1024 bit RSA authentication is considered to be insecure and therefore as weak. - Any cipher considered to be secure for only the next 10 years is considered as medium - Any other cipher is considered as strong	
<b>Vulnerability Detection Method</b> Details: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440) Version used: \$Revision: 11135 \$	
<b>References</b>  CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000	
 CERT: CB-K17/1750, CB-K16/1593, CB-K16/1552, CB-K16/1102, CB-K16/0617, CB-K16/0599, CB-K16/0168, CB-K16/0121, CB-K16/0090, CB-K16/0030, CB-K15/1751, CB-K15/1591, CB-K15/1550, CB-K15/1517, CB-K15/1514, CB-K15/1464, CB-K15/1442, CB-K15/1334, CB-K15/1269, CB-K15/1136, CB-K15/1090, CB-K15/1059, CB-K15/1022, CB-K15/1015, CB-K15/0986, CB-K15/0964, CB-K15/0962, CB-K15/0932, CB-K15/0927, CB-K15/0926, CB-K15/0907, CB-K15/0901, CB-K15/0896, CB-K15/0889, CB-K15/0877, CB-K15/0850, CB-K15/0849, CB-K15/0834, CB-K15/0827, CB-K15/0802, CB-K15/0764, CB-K15/0733, CB-K15/0667, CB-K14/0935, CB-K13/0942, DFN-CERT-2017-1821, DFN-CERT-2016-1692, DFN-CERT-2016-1648, DFN-CERT-2016-1168, DFN-CERT-2016-0665, DFN-CERT-2016-0642, DFN-CERT-2016-0184, DFN-CERT-2016-0135, DFN-CERT-2016-0101, DFN-CERT-2016-0035, DFN-CERT-2015-1853, DFN-CERT-2015-1679, DFN-CERT-2015-1632, DFN-CERT-2015-1608, DFN-CERT-2015-1542, DFN-CERT-2015-1518, DFN-CERT-2015-1406, DFN-CERT-2015-1341, DFN-CERT-2015-1194, DFN-CERT-2015-1144, DFN-CERT-2015-1113, DFN-CERT-2015-1078, DFN-CERT-2015-1067, DFN-CERT-2015-1038, DFN-CERT-2015-1016, DFN-CERT-2015-1012, DFN-CERT-2015-0980, DFN-CERT-2015-0977, DFN-CERT-2015-0976, DFN-CERT-2015-0960, DFN-CERT-2015-0956, DFN-CERT-2015-0944, DFN-CERT-2015-0937, DFN-CERT-2015-0925, DFN-CERT-2015-0884, DFN-CERT-2015-0881, DFN-CERT-2015-0879, DFN-CERT-2015-0866, DFN-CERT-2015-0844, DFN-CERT-2015-0800, DFN-CERT-2015-0737, DFN-CERT-2015-0696, DFN-CERT-2014-0977 Other: <a href="https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warmmeldung_cb-k16-1465_update_6.html">https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warmmeldung_cb-k16-1465_update_6.html</a> <a href="https://bettercrypto.org/">https://bettercrypto.org/</a> <a href="https://mozilla.github.io/server-side-tls/ssl-config-generator/">https://mozilla.github.io/server-side-tls/ssl-config-generator/</a>	

## 6) Low Severity (Around 2.6)

<b>Low</b> (CVSS: 2.6) NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)		general/tcp
<b>Summary</b> The remote host implements TCP timestamps and therefore allows to compute the uptime.		
<b>Vulnerability Detection Result</b> It was detected that the host implements RFC1323.  The following timestamps were retrieved with a delay of 1 seconds in-between: Packet 1: 623055 Packet 2: 624131		
<b>Impact</b> A side effect of this feature is that the uptime of the remote host can sometimes be computed.		
<b>Solution</b> <b>Solution type:</b> Mitigation  To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.  To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'  Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.  The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.  See also: <a href="http://www.microsoft.com/en-us/download/details.aspx?id=9152">http://www.microsoft.com/en-us/download/details.aspx?id=9152</a>		
<b>Affected Software/OS</b> TCP/IPv4 implementations that implement RFC1323.		
<b>Vulnerability Insight</b> The remote host implements TCP timestamps, as defined by RFC1323.		
<b>Vulnerability Detection Method</b>  Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.  Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091) Version used: \$Revision: 10411 \$		
<b>References</b>  Other: <a href="http://www.ietf.org/rfc/rfc1323.txt">http://www.ietf.org/rfc/rfc1323.txt</a>		

## **Evaluation Criteria:**

### **1. Technical Proficiency:**

- Accuracy and thoroughness of the vulnerability assessment.
- Effective use of OpenVAS tools.

### **2. Analytical Skills:**

- Ability to prioritize vulnerabilities based on risk and impact.
- Logical and practical approach to remediation.

### **3. Report Quality:**

- Clarity, organization, and professionalism of the report.
- Inclusion of all required details and actionable recommendations.

### **4. Problem-Solving:**

- Creativity and effectiveness in proposing mitigation strategies.
- Success in resolving vulnerabilities during implementation which has been explained using the fetchings we had done through the automated open source scanning.

---

## **Remedies Based on Severity:**

### **● Critical:**

- Apply security patches immediately to vulnerable systems.
- Disable or restrict access to critical services running on open ports.
- Implement network segmentation to isolate affected components.
- Strengthen authentication mechanisms (e.g., enforce strong passwords, enable multi-factor authentication).

For the above target “192.168.1.56”, there seems to be less critical issues, but for overall security standards, a centralized security mechanism will be held for the working for the corporation’s smooth flow and continuity. Here, the corporation is “Google” with its server localised in “192.168.1.56”.

- **High:**

- Update software and operating systems to their latest versions.
- Remove or disable unused services and ports.
- Reconfigure firewalls to block unauthorized access attempts.
- Conduct regular penetration tests to validate fixes.

- **Medium:**

- Review and update access controls and permissions.
- Harden system configurations (e.g., disable default accounts, enforce secure protocols like HTTPS and SSH).
- Educate users about phishing and social engineering risks.

- **Low:**

- Address minor misconfigurations and cosmetic vulnerabilities.
- Ensure proper documentation and monitoring for potential future escalation.
- Schedule periodic vulnerability assessments to maintain security.

---

## **Conclusion on the Report:**

From a overlook from this project, we can decipher that, even when an organization is big and highly structural, like “Google”, we can have certain errors and risks, which might risk the users and clients, who use such services, at a greater risk. Through this project, I have gained hands-on experience with OpenVAS, developed critical thinking in analyzing and prioritizing risks, and learned practical approaches to mitigating real-world network vulnerabilities. This foundational knowledge will prepare them for future roles in cybersecurity.