ControlCase
Compliance as a Service

Genpact

External Network Penetration Test Report

Version 1.0

February 23, 2021

Statement of Confidentiality

This Confidential Information is being provided to **Genpact** as a deliverable of this consulting engagement. The sole purpose of this document is to provide you with the results of, and recommendations derived from this consulting engagement. Each recipient agrees that, prior to reading this document, it shall not distribute or use the information contained herein and any other information regarding **ControlCase** for any purpose other than those stated.

Table of Contents

1 RESULTS 4

1.1 INTRODUCTION 4
1.2 CONCLUSION 4
1.3 GOALS & OBJECTIVES 4

2 METHODOLOGY 5

2.1 METHODOLOGY DESCRIPTION 5
2.2 PROJECT TEAM 7
2.3 PENETRATION TIMELINE 7

3 DETAILS OF WORK PERFORMED 8

3.1 PHASE 1– RECONNAISSANCE 8
3.2 PHASE 2 – PORT SCANNING 10
3.3 PHASE 3 – OBSERVATIONS 13
3.3.1 Deprecated SSH Cryptographic Settings 13
3.3.2 TLS Version 1.0 Protocol Detection 14
3.3.3 Network Time Protocol (NTP) Mode 6 Scanner 15
3.3.4 Closed Port Detection 16
3.4 PHASE 4 – EXPLOITATION 17
3.5 ASSESSOR’S NOTE 17

1 Results

1.1 Introduction

ControlCase was engaged by **Genpact** to perform an external network penetration testing of their internet facing network segment. Throughout all testing, **ControlCase** did not perform any tests that would deliberately lead to system outages or affect application availability, such as denial-of-service tests.

All network vulnerability testing was conducted from ControlCase testing networks from **February 20, 2021 to February 23, 2021.** All testing was performed using a variety of industry leading security scanning tools and applications.

The external network included twenty-nine (29) IP addresses on **Class-A, Class-B** and **Class-C** network provided to **ControlCase** by **Genpact.** A firewall or other network traffic-filtering device restricted access to these hosts.

1.2 Conclusion

ControlCase was unable to penetrate into the **Genpact's** external network under scope using the identified vulnerabilities. ControlCase concludes that **Genpact** has **PASSED** the External Network Penetration Test.

1.3 Goals & Objectives

The objective of this assessment on **Genpact's** external network was to detect any vulnerability in the organization's IT System & Network to exploit and for checking how effective the controls are in preventing any potential unauthorized information access.

Other Considerations:

As both the vulnerability assessment and the penetration test provide only a snapshot of the security posture, and with security exposure never a constant, information security management needs to be regularly monitored, reviewed and audited, and an ongoing process be implemented for making improvements and taking corrective actions.

We are of the opinion that even when all the identified vulnerabilities have eventually been addressed – in order to maintain on-going security posture of the network infrastructure, **Genpact** should consider the following:

To conduct periodic External and Internal Vulnerability Assessment and Penetration Testing as well as Security Audit Reviews especially after major changes in the systems and infrastructure.

2 Methodology

2.1 Methodology Description

ControlCase engineers follow the methodology below when performing External Network Penetration Testing. This methodology was created to promote a more consistent and thorough approach to vulnerability assessment and penetration testing. The methodology is broken down into these five components:

- **D**iscovery - aims at identifying all potential assets for investigation. The information gained through the discovery process creates a road map for the investigation module.
- **A**nalysis - utilizes the list of assets from the discovery process and thoroughly examines them for potential vulnerabilities. The raw data resulting from the investigation must be analyzed and verified.
- **V**alidation - tests vulnerabilities to ensure that all false positives and inaccuracies are removed from the raw investigation data. This often-neglected step ensures accuracy, painting a nearly complete picture of the security posture.
- **E**xploitation - involves the in-depth analysis and execution of advanced testing techniques against all verified vulnerabilities. This effort completes the security picture and provides the information necessary to fully mitigate the observations.
- **R**eporting - provides an overview of the assessment methodology, vulnerability and threat assessment observations, recommendations and corrective actions and a copy of all data collected.

ControlCase engineers used this methodology to perform the vulnerability assessment and penetration testing and to assess the security of the **Genpact's** external network. Specifically, the following sections highlight the various tests that were used to complete each step of the methodology.

Discovery

Genpact provided twenty-nine (29) IP addresses for the external network to be reviewed by **ControlCase.** The IP addresses which were provided for the assessment are shown below:

External IP Addresses:

- 3.209.54.246
- 3.93.227.220
- 4.59.196.78
- 12.125.232.106
- 12.87.39.214
- 32.6.166.114
- 32.6.166.118
- 32.6.185.174
- 32.6.185.182
- 32.6.185.186
- 38.142.188.30
- 50.207.117.50
- 59.160.97.246
- 67.154.112.26
- 69.174.28.138
- 115.114.73.26
- 121.241.55.129
- 121.241.98.81
- 122.15.135.129
- 122.55.2.142
- 125.21.0.182
- 125.21.44.66
- 136.232.138.70
- 157.130.132.82
- 182.19.62.165
- 202.54.240.182
- 216.195.64.30
- 216.195.64.34
- 222.127.146.122

ControlCase used the security tool NMAP to identify live services on the tested IP address. NMAP is designed to identify live systems, as well as services being offered by these systems.

Investigation

As a follow-up to the information gathered, ControlCase used the security tool Nexpose v6.6.58 to perform checks for known vulnerabilities on the **Genpact's** external network. Nexpose is a security-scanning tool that checks for over 150,000 different known vulnerabilities on networked systems. The Nexpose tool performs extensive checks for vulnerabilities based upon predefined attack signature criteria. All tests were complemented with additional manual checks performed by ControlCase engineers to ensure accuracy of the results.

Verification

ControlCase manually verified the outputs of all security tools to determine if any results were inconsistent and warranted additional examination and review. Outputs from the various tools used were compared and crosschecked for accuracy. False positives and duplicate entries were removed from the Investigation results. Vulnerabilities that could be neither confirmed nor disputed were categorized separately for follow-up checks and review. Those vulnerabilities that could not be tested and confirmed without endangering the systems on which they exist are noted as well.

Exploitation

ControlCase performed exploitation attempts against any external network host exhibiting vulnerability symptoms. These attempts included numerous manual exploitation attempts, information gathering and password guessing for well-known accounts using techniques developed and tested in our lab environment. All attacks were designed to limit the danger to services on the systems in order to prevent disruption of service during the testing.

Reporting

The culmination of all observations is reported in this document using the **ControlCase** standard reporting template.

2.2 Project Team

The engagement involved contributions from the following team members:

ControlCase Team	Genpact Team
Manali Brid	Ankur Shrivastava
Rajkumar Yadav	

2.3 Penetration Timeline

The following table outlines key milestones during the penetration test:

Penetration Timeline

Date	Milestone
February 20, 2021	Start of Project
February 23, 2021	Final Deliverable

3 Details of Work Performed

3.1 Phase 1– Reconnaissance

Reconnaissance is an information gathering phase for the target IP address or IP addresses range in the scope of penetration test.

ControlCase team examined the target by passive techniques such as

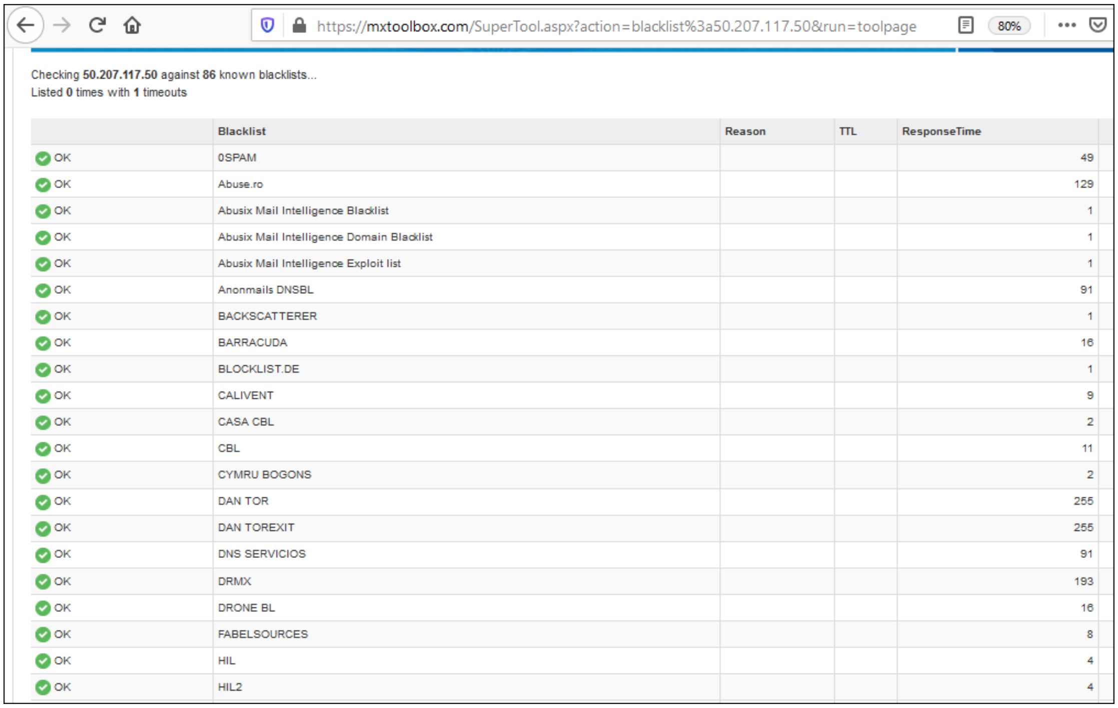
- **Internet Service Registration** – The global registration and maintenance of IP address information.
- **Domain Name System** – Local and global registration and maintenance of host naming.
- **Search Engines** – Specialist retrieval of distributed material relating to an organization or their employees.
- **Email Systems** – Information contained within and related to emails and email deliver processes. Mainly information disclosed via “Contact Us” features.
- **Website Analysis** – The information intentionally made public, that may pose a risk to security.

Observations of reconnaissance whether technical or non-technical in nature, can be used against target IP address to plan further attack scenarios. This phase uses various search engines, mailing groups, online forums, collaboration sites etc. for collecting information. A subset of the same is –

1. Search engines such as Google, Yahoo, Bing etc.
2. GHDB (Google Hacking Database leverage to an external attacker)

ControlCase assessors observed that no CRITICAL information about the given IP addresses of **Genpact** is available over internet which can be of any leverage to an external attacker. Furthermore, ControlCase assessor observed that target IP addresses are not listed in well-known public databases as spamming hosts and are not blacklisted as known malicious IP addresses either.

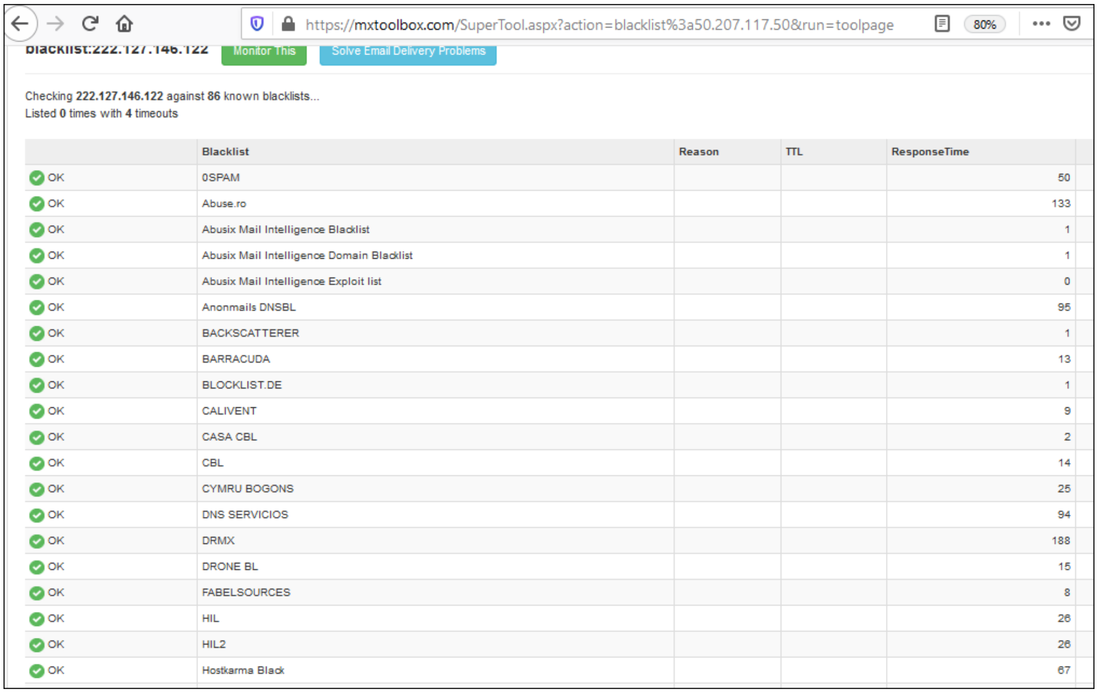
Followings are the subset of POCs for performed reconnaissance:



https://mxtoolbox.com/SuperTool.aspx?action=blacklist%3a50.207.117.50&run=toolpage

Checking **50.207.117.50** against **86** known blacklists...
Listed **0** times with **1** timeouts

	Blacklist	Reason	TTL	ResponseTime
✓ OK	0SPAM			49
✓ OK	Abuse.ro			129
✓ OK	Abusix Mail Intelligence Blacklist			1
✓ OK	Abusix Mail Intelligence Domain Blacklist			1
✓ OK	Abusix Mail Intelligence Exploit list			1
✓ OK	Anonmails DNSBL			91
✓ OK	BACKSCATTERER			1
✓ OK	BARRACUDA			16
✓ OK	BLOCKLIST.DE			1
✓ OK	CALIVENT			9
✓ OK	CASA CBL			2
✓ OK	CBL			11
✓ OK	CYMRU BOGONS			2
✓ OK	DAN TOR			255
✓ OK	DAN TOREXIT			255
✓ OK	DNS SERVICIOS			91
✓ OK	DRMX			193
✓ OK	DRONE BL			16
✓ OK	FABELSOURCES			8
✓ OK	HIL			4
✓ OK	HIL2			4



https://mxtoolbox.com/SuperTool.aspx?action=blacklist%3a50.207.117.50&run=toolpage
80%
Monitor This
Solve Email Delivery Problems

blacklist:222.127.146.122

Checking **222.127.146.122** against **86** known blacklists...
Listed **0** times with **4** timeouts

	Blacklist	Reason	TTL	ResponseTime
✓ OK	0SPAM			50
✓ OK	Abuse.ro			133
✓ OK	Abusix Mail Intelligence Blacklist			1
✓ OK	Abusix Mail Intelligence Domain Blacklist			1
✓ OK	Abusix Mail Intelligence Exploit list			0
✓ OK	Anonmails DNSBL			95
✓ OK	BACKSCATTERER			1
✓ OK	BARRACUDA			13
✓ OK	BLOCKLIST.DE			1
✓ OK	CALIVENT			9
✓ OK	CASA CBL			2
✓ OK	CBL			14
✓ OK	CYMRU BOGONS			25
✓ OK	DNS SERVICIOS			94
✓ OK	DRMX			188
✓ OK	DRONE BL			15
✓ OK	FABELSOURCES			8
✓ OK	HIL			26
✓ OK	HIL2			26
✓ OK	Hostkarma Black			67

3.2 Phase 2 – Port Scanning

Port Scans are attempts to connect to ports corresponding to services on the assessed hosts. By scanning ports which are available on the hosts, potential weaknesses on them can be further exploited.

Any ports that are found visible on the hosts should be verified if they are supposed to be opened there. Unexpected open ports should be closed. The firewall should also be checked if the listening ports on the hosts should expose to the internet or to the internal networks. It is recommended to remove any unnecessary services and implement firewall rules to prevent exposure of any legitimate services that are not meant for the internet.

Ports on which the connection attempts were made are shown below. The table consists of host IP address, protocol types, port numbers and the probable services. It is recommended to remove any unnecessary ports/services as identified below.

Following table shows the Port Scan Results:

Address of Host (Hostname)	Protocol / Port / Service / Status	Comments
115.114.73.26	UDP / 161 / SNMP / OPEN	All TCP/UDP ports on the target host which are not listed here were observed to be in state as FILTERED.
136.232.138.70	UDP / 161 / SNMP / OPEN	All TCP/UDP ports on the target host which are not listed here were observed to be in state as FILTERED.
38.142.188.30	UDP / 123 / NTP / OPEN UDP / 161 / SNMP / OPEN UDP / 500 / ISAKMP / OPEN	All TCP/UDP ports on the target host which are not listed here were observed to be in state as FILTERED.
122.55.2.142	TCP / 53 / DOMAIN / OPEN UDP / 53 / DOMAIN / OPEN UDP / 123 / NTP / OPEN UDP / 161 / SNMP / OPEN	All TCP/UDP ports on the target host which are not listed here were observed to be in state as FILTERED.
3.209.54.246	TCP / 443 / HTTPS / OPEN	All TCP/UDP ports on the target host which are not listed here were observed to be in state as FILTERED.
3.93.227.220	TCP / 443 / HTTPS / OPEN	All TCP/UDP ports on the target host which are not listed here were observed to be in state as FILTERED.
12.87.39.214	TCP / 22 / SSH / OPEN TCP / 830 / SSH / OPEN	All TCP/UDP ports on the target host which are not listed here were observed to be in state as FILTERED.
125.21.0.182	TCP / 179 / BGP / CLOSED	All TCP/UDP ports on the target host which are not listed here were observed to be in state as FILTERED.
125.21.44.66	TCP / 179 / BGP / CLOSED	All TCP/UDP ports on the target host which are not listed here were observed to be in state as FILTERED.

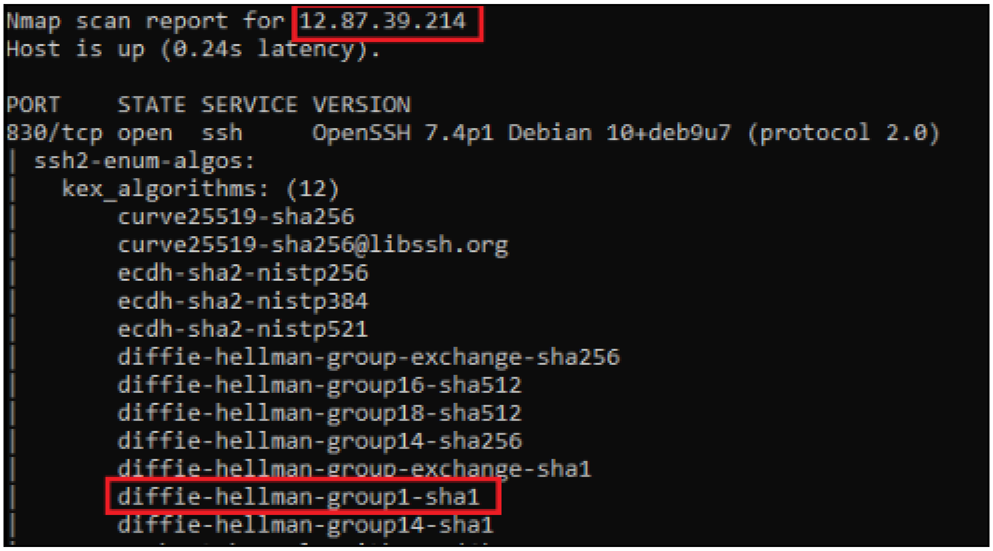
Address of Host (Hostname)	Protocol / Port / Service / Status	Comments
4.59.196.78	TCP / 179 / BGP / CLOSED	All TCP/UDP ports on the target host which are not listed here were observed to be in state as FILTERED.
50.207.117.50	TCP / 113 / IDENT / CLOSED TCP / 179 / TCPWRAPPED / OPEN TCP / 541 / REVERSE-SSL / OPEN	All TCP/UDP ports on the target host which are not listed here were observed to be in state as FILTERED.
12.125.232.106	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
121.241.55.129	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
121.241.98.81	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
122.15.135.129	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
157.130.132.82	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
182.19.62.165	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
202.54.240.182	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
216.195.64.30	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
216.195.64.34	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
222.127.146.122	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
32.6.166.114	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
32.6.166.118	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
32.6.185.174	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
32.6.185.182	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.

Address of Host (Hostname)	Protocol / Port / Service / Status	Comments
32.6.185.186	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
59.160.97.246	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
67.154.112.26	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.
69.174.28.138	NO OPEN PORTS OBSERVED	All TCP/UDP ports on the target host were observed to be in state as FILTERED.

3.3 Phase 3 – Observations

This phase has been completed successfully and following are the observations which were noted during the External Network Penetration Test:

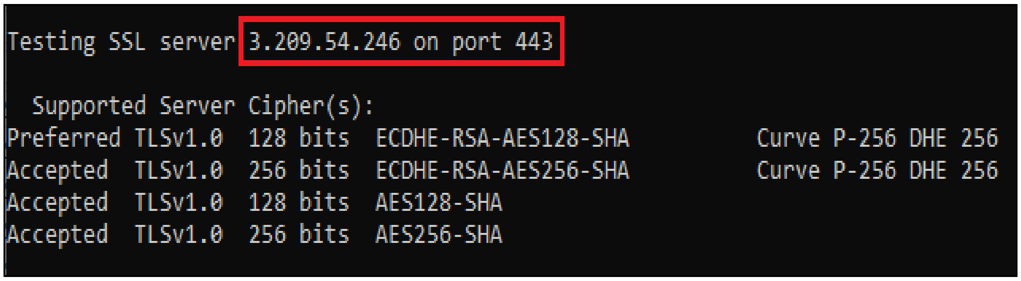
<table>
<tr><th colspan="2">3.3.1 Deprecated SSH Cryptographic Settings</th></tr>
<tr><td><b>Ports</b></td><td>TCP 22, 830</td></tr>
<tr><td><b>Observation</b></td><td>Assessor observed that the target host is using deprecated SSH cryptographic settings to communicate.</td></tr>
<tr><td><b>Affected Resource</b></td><td>12.87.39.214</td></tr>
<tr><td><b>POC</b></td><td>



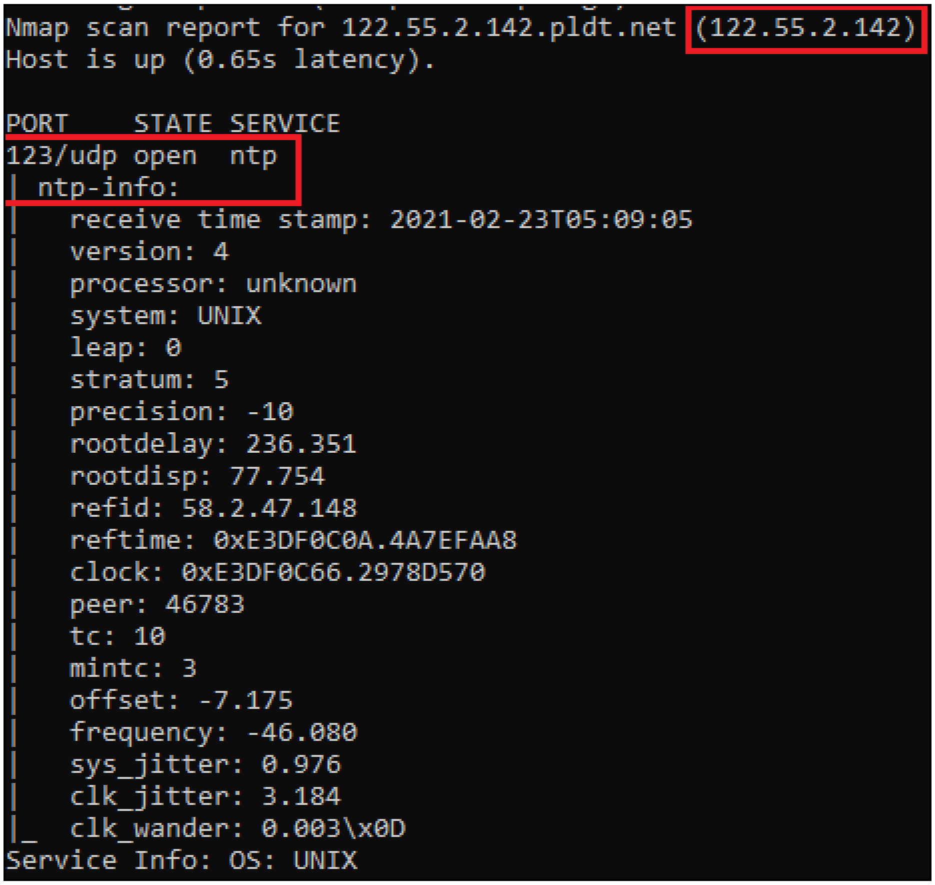
```
Nmap scan report for 12.87.39.214
Host is up (0.24s latency).

PORT    STATE SERVICE VERSION
830/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh2-enum-algos:
|   kex_algorithms: (12)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|       diffie-hellman-group-exchange-sha1
|       diffie-hellman-group1-sha1
|       diffie-hellman-group14-sha1
```

</td></tr>
<tr><td><b>Results</b></td><td>The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another. The target host is using deprecated SSH cryptographic settings (key exchange algorithm: diffie-hellman-group1-sha1).
A man-in-the-middle attacker may be able to exploit this vulnerability to record the communication to decrypt the session key and even the messages.</td></tr>
<tr><td><b>Risk Mitigation</b></td><td>It is recommended to avoid using deprecated cryptographic settings.
Use best practices when configuring SSH.
Refer to Security of Interactive and Automated Access Management Using Secure Shell (SSH) (https://csrc.nist.gov/publications/detail/nistir/7966/final) .</td></tr>
<tr><td><b>CVE</b></td><td>NA</td></tr>
<tr><td><b>CVSS Base Score</b></td><td>6.4</td></tr>
</table>

3.3.2 TLS Version 1.0 Protocol Detection

Port	TCP 443
Observation	Assessor observed that the remote service encrypts traffic using an older version of TLS.
Affected Resources	3.93.227.220, 3.209.54.246
POC	 Testing SSL server 3.209.54.246 on port 443 Supported Server Cipher(s): Preferred TLSv1.0 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256 Accepted TLSv1.0 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256 Accepted TLSv1.0 128 bits AES128-SHA Accepted TLSv1.0 256 bits AES256-SHA
Results	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 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.
Risk Mitigation	It is recommended to enable support for TLS 1.2 and 1.3 and disable support for TLS 1.0.
CVE	NA
CVSS Base Score	6.1

3.3.3 Network Time Protocol (NTP) Mode 6 Scanner

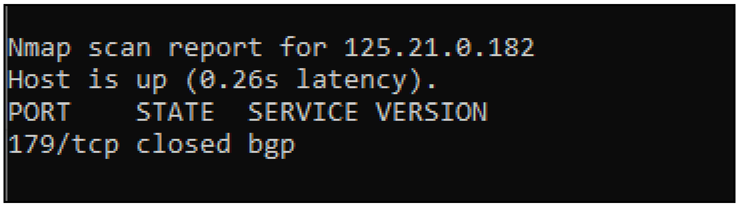
Port	UDP 123
Observation	Assessor observed that the remote NTP server responds to mode 6 queries.
Affected Resources	38.142.188.30, 122.55.2.142
POC	

```
Nmap scan report for 122.55.2.142.pldt.net (122.55.2.142)
Host is up (0.65s latency).

PORT    STATE SERVICE
123/udp open  ntp
| ntp-info:
|   receive time stamp: 2021-02-23T05:09:05
|   version: 4
|   processor: unknown
|   system: UNIX
|   leap: 0
|   stratum: 5
|   precision: -10
|   rootdelay: 236.351
|   rootdisp: 77.754
|   refid: 58.2.47.148
|   reftime: 0xE3DF0C0A.4A7EFAA8
|   clock: 0xE3DF0C66.2978D570
|   peer: 46783
|   tc: 10
|   mintc: 3
|   offset: -7.175
|   frequency: -46.080
|   sys_jitter: 0.976
|   clk_jitter: 3.184
|_  clk_wander: 0.003\x0D
Service Info: OS: UNIX
```

Results	The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.
Risk Mitigation	It is recommended to restrict NTP mode 6 queries.
CVE	NA
CVSS Base Score	5.0

3.3.4 Closed Port Detection

Ports	For detailed Port Scanning results please refer to section 3.2 Phase 1 – Port Scanning
Observation	Assessor observed that few TCP ports on the affected resources are not being filtered by any filtering device like firewall, Router, IPS or IDS. Thus, the port scanning attempts successfully discovered the exact state of ports as being closed. It seems that the firewall/filtering device allows traffic to pass affected resources which send RESET packet as a response to SYN request. Another possibility is that the firewall / filtering device itself sends the RESET response for such requests
Affected Resources	Please refer to section 3.2 Phase 1 – Port Scanning

POC	
	`Nmap scan report for 125.21.0.182`
	`Host is up (0.26s latency).`
	`PORT    STATE  SERVICE VERSION`
	`179/tcp closed bgp`

Results	Port scanning attempts on affected resources are showing few tcp ports as closed. Revealing the correct states of the port to any user results into information discloser. An attacker can leverage the information about closed ports to deduce what other ports may be open / filtered. This also shows that the ports are not being filtered by firewall and thus an attacker can use those for installing backdoors as part of post-exploitation.
Risk Mitigation	Network and security devices shall be configured in a way that they won't reveal the status of closed ports to port scan attempts. Also, mentioned affected devices shall follow the configuration which detects and filters port scanning attempts. This kind of attack can be prevented on router by using TCP Intercept which can be configured to intercept all incoming SYN packets, or an ACL can be written to identify the source and destination for packets that should be intercepted. It can also be run in watch mode, a more passive mode than intercept mode. In watch mode, the router does not intercept the SYN packets, but passes them through to the TCP server.
CVE	NA
CVSS Base Score	2.2

3.4 Phase 4 – Exploitation

ControlCase assessor did not observe any vulnerability which can be exploited within a given period and based on that determined that the identified vulnerabilities cannot affect confidentiality or integrity of critical information. The necessary information was gathered for the identified observations and provided in the “POC” section of the vulnerability table.

3.5 Assessor’s Note

Assessor attempted to discover vulnerabilities at network layer using automated as well as manual techniques. The vulnerability scanning and penetration testing of the target systems included, but was not limited to, following attack vectors:

Sr. No.	Attack Vector	No. of Observations
1.	Operating System Vulnerabilities	No Vulnerabilities Observed
2.	Service Misconfiguration	Three Vulnerabilities Observed
3.	Network Misconfiguration	One Vulnerability Observed
4.	Web Interfaces Discovery	No Vulnerabilities Observed
5.	Common Ports used by Backdoors / Viruses / Worms	No Vulnerabilities Observed
6.	DNS Recursion / Zone Transfer / Poisoning	No Vulnerabilities Observed