Netiq Technology, Inc

External Network Penetration Test Report

Version 1.0

October 24, 2022

Statement of Confidentiality

This Confidential Information is being provided to **Netiq Technology,Inc** 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 **Angu HariHara Prasad - Freelancer** for any purpose other than those stated.

Table of Contents

1 Results

1.1 Introduction

Angu HariHara Prasad - Freelancer was engaged by **Netiq Technology,Inc** (hereafter referred to as the **client**) to perform an External Network Penetration Test of their internet facing network segment. Throughout all testing, **Angu HariHara Prasad - Freelancer** did not perform any tests that would deliberately lead to system outages or affect application availability, such as denial-of-service tests.

The engagement began on October 19, 2022 which included multiple phases of testing, analysis and documentation. All testing was conducted on my lab. All testing was performed using a variety of industry leading security scanning tools.

This document summarizes the analysis, observations and recommendations for the assessment carried out by **Angu HariHara Prasad - Freelancer**.

1.2 Conclusion

Angu HariHara Prasad - Freelancer was able to penetrate into the **Netiq Technology,Inc** external network under scope using the identified vulnerabilities.

1.3 Goals & Objectives

The objective of this assessment on **the client's** external network was to detect vulnerabiltiies in the organization's IT System & Network which may lead to exploitation and for checking the effectiveness of the controls placed to prevent 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 being constant, information security management needs to regularly monitor, review and audit security controls and an ongoing process must be implemented for making improvements and taking corrective actions against these controls.

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, **the client** 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, Scope & Timeline

2.1 Methodology Description

Angu HariHara Prasad - Freelancer engineers follow the methodology mentioned below while 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 further analysis and exploitation.
- **A**nalysis - utilizes the list of assets from the discovery process and thoroughly examines them for potential vulnerabilities. The 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 investigation data. This 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 step may lead to unauthorized access of vulnerable systems which help an attacker gain a foothold in the target network or exfiltrate valuable data.
- **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.

Angu HariHara Prasad - Freelancer used this methodology to perform the vulnerability assessment and penetration testing and to assess the security posture of the **the client's** external network. Specifically, the following sections highlight the various tests that were used to complete each step of the methodology.

Discovery

The Client provided **four** IP addresses for the external network to be reviewed by **Angu HariHara Prasad – Freelancer.** The IP addresses which were provided for the assessment are:

External IP Address(es)/Domain(s):

- 205.155.58.132
- 205.155.48.2

Angu HariHara Prasad - Freelancer used the security tool NMAP to identify open ports and running services on the target IP addresses and domains. NMAP is designed to identify live systems, as well as services running on these systems.

Investigation

As a follow-up to the information gathered, Angu Harihara Prasad - Freelancer used the vulnerability scanning tool Nessus v6.4 to perform checks for known vulnerabilities on **the client's** external network. Nessus is a security-scanning tool that checks for over 100,000+ different known vulnerabilities on networked systems. Nessus performs extensive checks for vulnerabilities based upon predefined attack signatures. All tests were complemented with additional manual checks performed by assessors to ensure accuracy of the results.

Verification

Angu HariHara Prasad - Freelancer 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

Angu HariHara Prasad - Freelancer performs exploitation attempts against any external network host exhibiting vulnerability symptoms. These attempts include numerous manual exploitation attempts, information gathering and password guessing for well-known accounts using techniques developed and tested in our lab environment. All attacks are designed to limit the danger to services on the systems in order to prevent disruption of service during the testing. This phase is performed when exploitable vulnerabilities are observed, and due permission is provided by the client.

Reporting

The culmination of all observations is reported in this document using the **Angu HariHara Prasad - Freelancer** standard reporting template.

2.2 Testing Timeline

The following table outlines key milestones during the penetration test:

Timeline

Date	Milestone
October 19, 2022	Start of Project
October 24, 2022	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.

Angu HariHara Prasad - Freelancer 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)

Angu HariHara Prasad - Freelancer assessors observed that no CRITICAL information about the given IP addresses/domains of **Netiq Technology,Inc ’s** is available over internet which can be of any leverage to an external attacker. Furthermore, Angu HariHara Prasad - Freelancer assessor observed that target IP addresses/domains are not listed in well-known public databases as spamming hosts and are not blacklisted as known malicious IP addresses/domains either.

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 to be open on the target hosts should be verified if they are supposed to be opened there. Unexpected or unwanted open ports should be closed by shutting down the corresponding services. It is recommended to remove any unnecessary services and implement firewall rules to prevent external exposure of any legitimate services that are not meant for the internet.

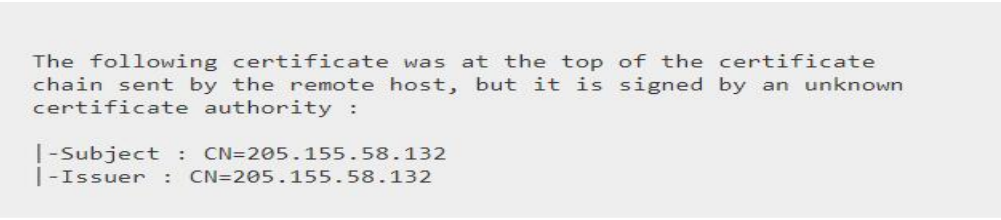
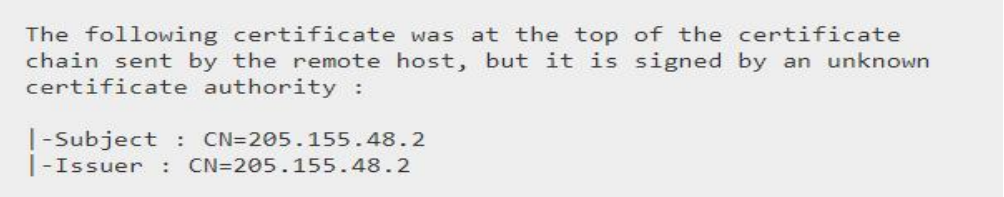
Angu HariHara Prasad - Freelancer attempted to connect to all 65535 TCP and well-known UDP ports in order to determine the services running on the target hosts. The following table consists of host IP address, protocol types, port numbers and the probable services that were discovered.

Address of Host (Hostname)	Protocol/Port/Service/Status
205.155.58.132	PORT **TCP** 80,443 AND **UDP** 53
205.155.48.2	PORT **TCP** 80,443 AND **UDP** 53

3.3 Phase 3 – Exploitation

This During the assessment multiple vulnerabilities were observed for which exploits are publically available. **Angu Hari** has prepared summary report titled "Netiq_Technology_External_NPT_Exploitable_Vulnerabilities_v1.0_24_Oct_2022.pdf" containing all the exploitable vulnerabilities with their impact upon exploitation on **the client's** production network and provided to **the client** for review.
The client has not approved to proceed with the exploitation considering the impact on the production network. The exploitation phase was carried out till certain level where no impact will happen on the production network.

3.3.1 SSL Certificate Cannot Be Trusted

Port	TCP 443
Observation	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.
Affected Resources	205.155.58.132 , 205.155.48.2
POC	 1) **205.155.48.2**: 

Reference	https://www.itu.int/rec/T-REC-X.509/en
Risk Mitigation	Purchase or generate a proper SSL certificate for this service.
CVE	CVE-2011-3389
CVSS Base Score	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

3.3.2 Self-Signed TLS/SSL Certificate Detected

Port	TCP 443
Observation	Assessor observed that the affected resource is running with TLS/SSL certificate which is self-signed.
Affected Resource	205.155.58.132, 205.155.48.2

POC	1) **205.155.58.132**:
	`The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :`
	`|-Subject : CN=205.155.58.132`
	2) **205.155.48.2**:
	`The following certificate was found at the top of the certificate chain sent by the remote host, but is self-signed and was not found in the list of known certificate authorities :`
	`|-Subject : CN=205.155.48.2`

Results	Self-signed certificates cannot be trusted by default, especially because TLS/SSL man in-the-middle attacks typically use self-signed certificates to eavesdrop on TLS/SSL connections.
Risk Mitigation	It is recommended that a new TLS/SSL server certificate that is NOT self-signed shall be obtained and installed on the server. The exact instructions for obtaining a new certificate depend on your organization's requirements. Generally, it is needed to generate a certificate request and save it as a file. This file is then can be sent to a Certificate Authority (CA) for processing. The requesting organization may have its own internal Certificate Authority. If not, it may have to pay for a certificate from a trusted external Certificate Authority, such as Thawte or VeriSign.
CVE	N/A
CVSS Base Score	3.4

3.4 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 Mis-configuration	Two Vulnerabilities Observed
3.	Network Mis-configuration	No Vulnerabilities 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