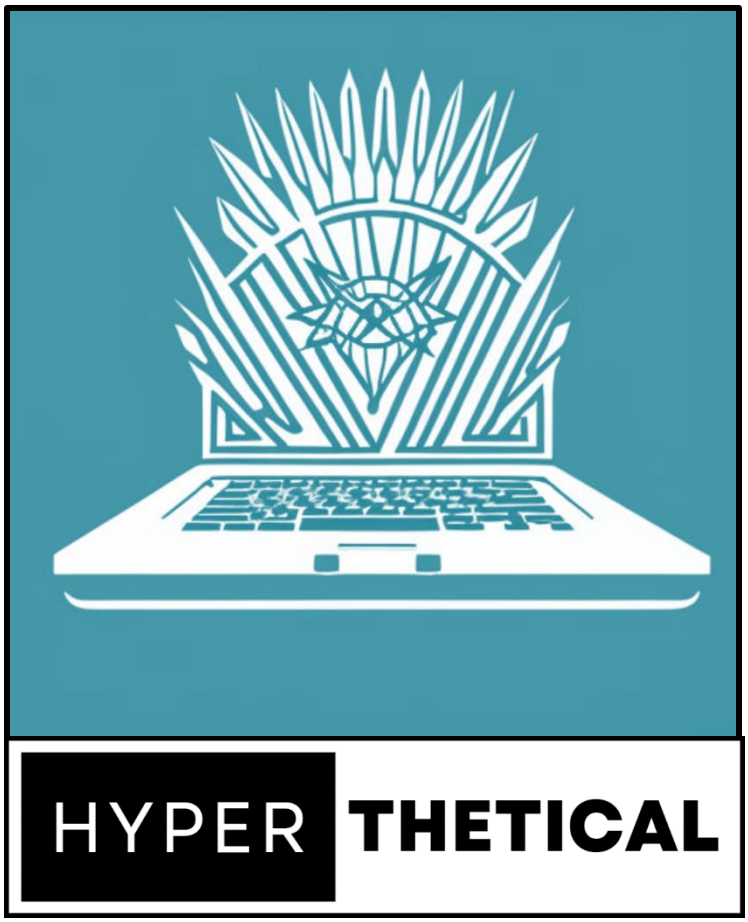
Penetration Test Proposal

Near-Earth Broadcast Network

03/10/2023



Hyperthetical Security Consulting

6 MetroTech Center,
Brooklyn, NY
11201

https://hyperthetical.com

HYPER THETICAL

Table of Contents

Executive Summary

The proposed penetration test offers a thorough and all-encompassing approach to assess the security of the Near-Earth Broadcast Network ("NBN") IT infrastructure. Hyperthetical Security Consulting ("Hyperthetical"), with their extensive experience and expertise, will conduct a comprehensive penetration test to identify vulnerabilities and potential security risks, recommend remediation measures, and suggest software solutions best suited for NBN's needs.

The Hyperthetical team will assess NBN's ability to defend against direct and indirect attacks by enumerating and then performing attacks against external facing hosts and services, external web apps, and the internal network while avoiding disrupting NBN's daily operations. This penetration test proposal provides an exceptional opportunity for NBN to assess its security posture comprehensively and obtain actionable insights into improving its IT infrastructure's security.

Goals and Objectives

The goal of this penetration test is to evaluate NBN's cybersecurity risk for outside threats and recommend actions to minimize this risk. Specifically, our objectives are to:

- Identify potential vulnerabilities and weaknesses in the IT infrastructure, web applications, and APIs.
- Test the effectiveness of existing security controls.
- Provide recommendations for improving the security posture of NBN's IT infrastructure.
- Produce a comprehensive report that outlines all findings, recommendations, and best practices for remediation.

Scope Overview

In Scope

- NBN public web applications.
- Externally facing hosts and services
- Internally facing hosts and services

Out of Scope

- NBN Employee VPN
- NBN Office Spaces
- Existing NBN subscriber (“Sub”) and business partner (“BP”) accounts

Introduction

This Penetration Testing Proposal aims to provide a comprehensive approach to performing a penetration test against the Near-Earth Broadcast Network ("NBN") IT infrastructure. This proposal outlines the scope, methodology, and deliverables for the proposed penetration test ("pentest"). Using our methods, the pentest team will identify vulnerabilities and potential security risks, provide recommended remediation, and suggest best practices for software solutions. The Hyperthetical Security Consulting ("Hyperthetical") team has the necessary experience and expertise to perform a comprehensive and detailed pen test of NBN's IT infrastructure, identify vulnerabilities and recommend remediation measures.

To test NBN's ability to defend against direct and indirect attacks, the Hyperthetical team will perform a comprehensive penetration test of NBN's external facing hosts and services, external web apps, and internal network. The team will begin the assessment from outside of the network and perform discovery and enumeration of the NBN external network. After verifying the discovered scope with the NBN security team, they will move on to vulnerability discovery and exploitation against the NBN external network and web applications. If the assessment team gains access to the NBN internal network, they will continue the assessment to find more vulnerabilities in the internal network. The team will perform testing with a focus on identifying medium to critical severity security vulnerabilities.

The Hyperthetical team will conduct the Penetration Test to avoid disrupting NBN's day-to-day operations. The assessment team will not perform Denial of Service (DoS) testing and will provide NBN with a schedule of events outlining the planned testing activities.

Methods and Scope

Detailed Scope

All testing will be conducted within a stringently adhered-to scope. All findings and analyses are limited to this scope.

External Network Pentest

In Scope

The assessment team will enumerate all external-facing hosts and services. After performing enumeration, the team will verify the discovered scope with the NBN security team.

Out of Scope

Name	IP Address/URL	Description
NBN VPN	Not Provided	Vendor-hosted VPN for NBN employees.
Physical Office	N/A	NBN Office locations.

External Web Application Pentest

In Scope

The assessment team will enumerate all external-facing web applications. After performing enumeration, the team will verify the discovered scope with the NBN security team.

Name	IP Address/URL	Description
NBN TVee Web	Not Provided	Media streaming application web version.
NBN TVee Mobile	Not Provided	Media streaming application mobile version.
NBN Ads	Not Provided	Business partner advertisement web application.
NBN Help	Not Provided	Support app for subscriber and business partner accounts.

Out of Scope

Name	IP Address/URL	Description
NBN Accounts	N/A	Existing NBN subscribers (SUB) and Business Partners (BP)

Internal Network Pentest

In Scope

If the assessment team gains access to the internal network, they will continue the assessment to find internal vulnerabilities and determine impacts.

Out of Scope

Name	IP Address/URL	Description
NBN VPN	Not Provided	Vendor-hosted VPN for NBN employees.
Physical Office	N/A	NBN Office locations.

Rules of Engagement

All technical testing will be conducted using proven methodologies to avoid disruption of services.

- The assessment team will not perform denial-of-service testing or utilize techniques deemed likely to cause a system outage or service disruption.
- The assessment team will not attack trusted third-party entities.

Methodology

The assessment team will conduct testing from both an internal and external standpoint using only proven methodologies. Because the Hyperthetical team will have no prior knowledge of, or access to, the NBN networks or systems, the testing team will conduct a "black box penetration test."

The penetration testing framework will include the following steps.

1. Reconnaissance
    a. Collect publicly available information about the target organization.
    b. Search for known vulnerabilities in the target network using publicly available information.
    c. Scan the target network to identify live hosts, ports, and services.
    d. Identify the operating systems, applications, and their versions running on the target network.
2. Vulnerability Discovery
    a. Conduct vulnerability scanning and testing to identify potential vulnerabilities in the target network.
    b. Use manual and automated techniques like fuzzing to identify vulnerabilities that automated scanners may miss.
    c. Prioritize the vulnerabilities based on their severity and likelihood of exploitation.
    d. Verify the identified vulnerabilities and ensure that they are exploitable.
3. Exploitation and Escalation
    a. Exploit any discovered vulnerabilities to gain unauthorized access to the target network.
    b. Use privilege escalation techniques to elevate the privileges of any compromised accounts.
    c. Conduct lateral movement to expand the compromise to other systems on the network or gain access to the internal network.
    d. Maintain persistence on the compromised systems to ensure continued access.
    e. Cover tracks to avoid detection by the target organization.

Deliverables

At the conclusion of the penetration test, Hyperthetical Consulting will deliver the following:

1. Comprehensive Executive Summary
    a. Separate executive report.
    b. The executive summary will be delivered in PDF format.
2. Penetration Test Report
    a. Executive Summary
    b. Narrative attack walkthrough
    c. Vulnerabilities are arranged by level of risk.
    d. Recommendations and proposed remediation steps, including software solutions and best practices.
    e. The report will be delivered in PDF format.

Roles and Responsibilities

The Hyperthetical team consists of experienced penetration testers who will work closely with NBN's IT staff throughout the testing process. We will assign a project manager to oversee testing and ensure that clear lines of communication are maintained throughout the engagement.

Hyperthetical Consulting

Hyperthetical Security Consulting ("Hyperthetical")	
Business Address	6 MetroTech Center, Brooklyn, NY 11201
Website	https://hyperthetical.com
Lead/Technical Consultant	
Assessor Name	Lindsay Von Tish
Title	CEO, Senior Security Consultant
Email	lmv9443@nyu.edu
Telephone	(646) 997-3600
Engagement Manager	
Name	Lindsay Von Tish
Title	CEO, Senior Security Consultant
Email	lmv9443@nyu.edu
Telephone	(646) 997-3600

Near-Earth Broadcast Network

Near-Earth Broadcast Network ("NBN")	
Business Address	1800 Archer St. The Bronx, NY 10460
Website	https://corp.nbn
Point of Contact	
Name	Bill Gibson
Title	CISO
Email	gibson@corp.nbn

Appendix A: Glossary and Definitions

Asset: Something that holds value, whether it's a system or data, that a threat may be trying to access or compromise.

Attack Vector: The path or means by which an attacker can access a system or network.

Authentication: The process of verifying the identity of a user or device before granting access to a computer system or network.

Authorization: The process of granting or denying access to a specific resource or system based on a user's identity and permissions.

Denial of Service (DoS): An attack meant to make a system unavailable to legitimate users.

Encryption: The process of converting sensitive data into an unreadable format to protect it from unauthorized access.

Ethical Hacking: Authorized behavior and actions to identify vulnerabilities of a system to help improve its security posture.

Exploit: A threat event that weaponizes code or an application, to take advantage of a weakness for the purpose of having an intended effect to a target that would otherwise be impossible, unintended by the target owner, or unauthorized.

Firewall: A network security system that monitors and controls incoming and outgoing network traffic.

Hacking: Using something in a deliberate way to create effects that is against the original intention or design.

LoLBins ("Living off the Land Binaries"): Legitimate binaries or executables included with operating systems or other software that an attacker can use to perform malicious activities, often to evade detection by security software.

Mitigation: A measure taken to reduce the risk of a successful attack or to minimize the harm caused by an attack.

Patch: A software update that fixes a computer system or network vulnerability.

Penetration testing: A method of testing a computer system, network, or web application to identify vulnerabilities and exploit them to gain unauthorized access to sensitive data.

Phishing: A social engineering attack that uses email or other messaging platforms to trick users into revealing sensitive information or clicking on malicious links or attachments.

Risk: The potential for damage or harm resulting from a successful attack.

Security Audit: A thorough checklist of security controls are measured against both technical implementations, policies, and procedures.

Severity: The degree of harm that could result from a successful attack, often measured on a scale from low to critical.

Social engineering: Using psychological manipulation to trick users into divulging sensitive information or performing actions that could compromise security.

Threat: Something that can cause the system harm, either adversarial, environmental, or accidental.

Threat Event: The event that is doing some harm against a target. Adversarial could take the form of recon, creating weapons (exploits), attacking, exfiltrating data, or other malicious actions against a target. Non-adversarial examples might be disk failure, employee negligence, or natural disaster.

Vulnerability: A weakness in a business process, configuration, operating system, or application that can be used to create unintended and undesired scenarios or opportunities for threat events.

Appendix B: Tools

Reconnaissance

Name	URL
BuiltWith	https://builtwith.com/
Get All URLs (GAU)	https://github.com/lc/gau
GoWitness	https://github.com/sensepost/gowitness
Massscan	https://github.com/robertdavidgraham/masscan
Nmap	https://nmap.org/
Recon-ng	https://www.kali.org/tools/recon-ng/
Shodan	https://www.shodan.io/
TheHarvester	https://www.kali.org/tools/theharvester/

Vulnerability Discovery

Name	URL
FFUF	https://github.com/ffuf/ffuf
Gobuster	https://github.com/OJ/gobuster
Nikto	
Nmap Scripting Engine (NSE)	https://nmap.org/book/nse.html
OpenVAS	https://github.com/sullo/nikto

Exploitation and Escalation

Name	URL
CrackMapExec	https://www.kali.org/tools/crackmapexec/
Metasploit	https://www.metasploit.com/
Mimikatz	https://github.com/ParrotSec/mimikatz
PowerSploit	https://github.com/PowerShellMafia/PowerSploit
Responder	https://github.com/SpiderLabs/Responder