# Assignment 1: Penetration Test Proposal

February 9, 2020

## Introduction

The objective of this vulnerability assessment and penetration test is to identify vulnerabilities in the information systems and networks of the Near-Earth Broadcast Corporation, or NBN Corp. Findings will be used to develop and present a set of recommendations to improve NBN Corp's information security posture, particularly with regard to preventing mass exfiltration of customer data by unauthorized persons. This proposal was requested by Bill Gibson, the Chief Information Security Officer, or CISO, of NBN Corp following a recent incident in which one or more individuals external to NBN Corp gained unauthorized access to customer data. The individuals broke into an Internet-facing server, which they used as a foothold to penetrate into NBN Corp's internal systems, including database servers containing customer data. Although NBN Corp's IT infrastructure and application teams have already identified and remediated several vulnerabilities, NBN Corp has requested a comprehensive vulnerability assessment of its information systems and networks.

## Test Proposal

The recent incident experienced by NBN Corp demonstrates that its information systems, network, and business data are vulnerable to unauthorized access by external adversaries. As the potential for new incidents of similar or greater magnitude is concerning to NBN Corp's management, our work will be guided in part by the following three questions:

- How could external parties gain unauthorized access to NBN Corp's information systems, network, and business data?
- How effective are existing systems, processes, and controls at protecting NBN Corp's information systems, network, and business data from unauthorized access and distribution?
- What steps can be taken to improve NBN Corp's security posture with the objective of meeting or exceeding industry standard best practices for information security?

Our team's vulnerability assessment and penetration test will focus on a Red Team approach, including phases for conducting reconnaissance on NBN Corp's network, identifying targets of interest, attempting to obtain access to the network, and attempting to maintain a persistent foothold within NBN Corp's IT environment. Initially, the team should operate with little to no information on NBN Corp's network (black box testing), although successive tests should include progressively greater amounts of information. We will separately audit and assess the security posture of NBN Corp's network to uncover gaps between the current configuration and industry standard best practices for information security. These results will enable us to develop and to present a set of recommendations to NBN Corp's management for improving NBN Corp's overall security posture.

At every stage of our work, we will communicate with NBN Corp's management to maintain transparency and insight into this vulnerability assessment and penetration test.

## Test Details

**Scope.** The scope of this assessment includes the entirety of NBN Corp's IT environment, including its network, servers, applications, and existing security measures.

**Limitations.** The physical security of NBN Corp's network is outside the scope of this assessment. Also, because NBN Corp does not use wireless or mobile networks, we will not be focusing on those attack vectors.

**Duration of Assessment.** The following table gives our initial estimate of the duration of this assessment, broken down into four phases. This estimate is for a team of three people and is subject to adjustment.

| Phase | Days | | | |
|---|---|---|---|---|
| **Intelligence Gathering** | 0-3 | | | |
| **Infrastructure Assessment** | | 3-12 | | |
| **Application Assessment** | | | 6-15 | |
| **People, Policies, and Procedures** | | | 6-15 | |

**Assessment Methodology.** The following table gives an overview of the methodologies that we will be using for this assessment, grouped into three categories (people, applications, infrastructure).

| | |
|---|---|
| People | ▪ **Gather information:** Perform background checks; conduct periodic audits of employee activities and correspondence.<br>▪ **Examine human vulnerabilities:** Use a variety of social engineering strategies against NBN Corp resources to obtain privileged access to systems and data.<br>▪ **Audit and improve organizational policy:** Review and audit organizational policies, including security awareness training. |
| Applications | ▪ **Identify applications**: Understand range of business applications in use by NBN Corp, including the chat service.<br>▪ **Discover vulnerabilities**: Test for common vulnerabilities in applications, including such as those in the OWASP Top 10. Initial tests will be black box tests.<br>▪ **Audit**: Evaluate application code and the configuration of its underlying servers and determine the level of compliance with industry standard best practices. |
| Infrastructure | ▪ **Discover vulnerabilities:** Use network scanner software such as nmap to gather information about targets, including:<br>— IP addresses of hosts<br>— Protocols and port numbers<br>— Versions of network services (such as web servers, application servers, and database servers)<br>▪ **Exploit vulnerabilities:** Use existing public databases such as the MITRE CVE to determine what vulnerabilities are present in the targets. Use industry standard tools such as Kali and Metasploit to attempt to exploit vulnerabilities.<br>▪ **Gain access:** Once access is gained, gather information, including the configurations of accessible devices, including servers, firewalls, and routers. Examine and retain business and other interesting data on accessible systems. |

**Assumptions.** For this assessment, we will make the following assumptions:

- All relevant NBN Corp stakeholders, including NBN Corp's Internet Service Provider, will be given advance notice of this assessment, as well as timely and complete updates during the assessment.
- The targets in this proposal are owned or controlled by NBN Corp; we will only attempt to access targets that NBN Corp has explicitly permitted us to test.
- NBN Corp's IT teams have functioning disaster recovery and business continuity systems in place, including backups of business data that can be restored by NBN Corp's IT teams if necessary.
- Business data that our team may access during this assessment will be treated as proprietary and confidential to NBN Corp. No business data will be retained following the conclusion of the test.

**Rules of Engagement.** Prior to beginning this assessment, we will provide a written document to NBN Corp management containing the rules of engagement, including the following rules:

- NBN Corp explicitly consents to our services and grants us permission to conduct this assessment.
- NBN Corp indemnifies us and our team from any liability that may arise during this assessment.
- The assessment will be conducted during a mutually agreed upon range of hours over the course of approximately ten to fifteen business days.
- We will provide information on the members of the team conducting the assessment, locations from which the assessment's activities are performed, and IP addresses and other technological details about the hardware and software being used to perform the assessment.
- Evidence and business data that may be produced or discovered during this assessment will be treated as proprietary and confidential to NBN Corp.

## Deliverables

Following the conclusion of this assessment, we will provide a comprehensive report on our work to NBN Corp's management, including the following artifacts:

- Executive summary with a high-level overview of this vulnerability assessment and penetration test, including the rationale for this assessment.
- Overview of the assessment's activities, including scope and methodologies.
- Explanations of the tests that our team conducted, including written steps for reproducibility, screen captures, command scripts, and pertinent data produced by our tests.
- Our evaluation of NBN Corp's present security measures, policies, and controls, including a set of recommendations for improving NBN Corp's overall security posture to meet or exceed industry standard best practices.
- Appendices containing test results, as well as the final version of this proposal document as agreed upon by our team and by NBN Corp's management.

## Questions for NBN Corp Management

The following table gives a list of some of the questions that we have for NBN Corp's management.

| | |
|---|---|
| **Technology** | ▪ What public IP address blocks and domain names are in active use by NBN Corp?<br>▪ What is the contact information for NBN Corp's Internet Service Providers?<br>▪ Does NBN Corp leverage any third-party public cloud computing resources, including resources from service providers such as Amazon Web Services or Microsoft?<br>▪ Does NBN Corp use Virtual Private Networking (VPN) technology to enable its resources to remotely access the enterprise network?<br>▪ Does NBN Corp use Voice over Internet Protocol (VoIP) technology as part of its voice and video infrastructure? |
| **Employees** | ▪ How many employees and contractors does NBN Corp have?<br>▪ At what locations or offices do NBN Corp employees typically work? Are any NBN Corp employees working remotely?<br>▪ What is NBN Corp's existing background check policy?<br>▪ What is NBN Corp's existing security awareness training program?<br>▪ What monitoring and logging systems for employee and contractor activities does NBN Corp presently use? |
| **Customers** | ▪ Where are NBN Corp customers physically located?<br>▪ What laws and regulations regarding data privacy are applicable to NBN Corp customers?<br>▪ Is NBN Corp presently compliant with Payment Card Industry, or PCI, standards? |
| **Policies and Procedures** | ▪ What are NBN Corp's existing security policies?<br>▪ How does NBN Corp manage access control to its environment?<br>▪ What is NBN Corp's incident response policy? |

# References

[1] http://www.pentest-standard.org/

[2] https://www.oaklawn-il.gov/home/showdocument?id=10954

[3] https://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343