Near-Earth Broadcast Network



Request for Proposal

Penetration Testing Services

# Summary

Near-Earth Broadcast Network (NBN) is issuing this Request For Proposal (RFP) for qualified cybersecurity consultants (“Consultant”) to perform penetration testing services (“Pen test”) against our IT infrastructure. The Pen test should focus on NBN’s cybersecurity risk for outside threats, and what NBN can do to minimize this risk.

# Background

NBN is an advertising and media company that creates, licenses, and provides content for its paying residential subscribers (“Sub”). In addition to serving content to subscribers, NBN also sells access to our advertising network where subscriber data is used to intelligently provide targeted text, images, video, or interactive media advertisements by business partners (“BP”) to NBN’s Subscribers.

NBN operates out of the US but subscribers may be any household with internet access.



*NBN: We're always watching you.*

# NBN Details

NBN operates public web applications (“Apps”) used by their subscribers and business partners. These web apps and APIs communicate with internal application servers and databases. Both Subs and BPs create accounts for specific public web apps. Everything is hosted by NBN in their own network and on premises.

The Sub web app (“NBN TVee”) is the streaming media app. This app has two clients: a web version and a mobile version. Both operate using the same back-end APIs and architecture. Subs can use the app to search for and stream media.

The BP web app (“NBN ADs”) is the advertising app. This app only has a web client. BPs can create and manage ads, configure targeted Subs, and measure engagement.

There is also a support app (“NBNHelp”) which only has a web client. It is used by both Subs and BPs for making account changes and chatting with customer support.

NBN offers no email or phone support.

# Pen Test Details

NBN is seeking to reduce its overall risk by using the results of a Pen test to help secure their IT infrastructure. The Pen test should include both external and internal security testing.

Consultants will not be provided any network access, system access, physical access, or IT infrastructure details. Consultants are expected to perform the pen test from the perspective of an outsider: A Sub, a BP, or a non-affiliate.

# Scope of Work

1. External Network Pen Testing
   * Enumerate and assess all external facing hosts and services.
2. External Web App Pen Testing
   * Assess and exploit all external facing Web Apps.
3. Internal Network Pen Test
   * If internal network access is achieved, continue assessment to find more vulnerabilities and determine impacts.
4. Out of Scope
   * NBN employees use a vendor-hosted VPN provider which is not in scope.
   * NBN offices are all leased spaces that include physical security which is not in scope.
   * Existing NBN Subs and BP accounts are outside scope.
   * Distributed Denial of Service attacks are out of scope.
5. Severity
   * NBN is only interested in security flaws that have “medium” security impact or higher but will still accept any vulnerability or weakness.
   * Attacks that compromise a single account are considered “low”.
   * Information-only, suggested best practices, and theoretical-only exploits are considered “low”.
6. Other Pen Testing
   * Besides what is specifically out of scope, assess and test anything else available for security impact.

# Final Pen Test Deliverable

Based on the Pen Test results, provide a comprehensive technical, detailed, Executive Summary and Report. They should contain vulnerabilities, by level of risk, with recommended correlated remediation. Also provide best practices for software solutions to remediate the vulnerabilities identified.

# Proposal Content and Format

Proposals should be written as a penetration testing plan (“Plan”). The Plan will be used to assess the value of the consultant’s approach. In addition, the Plan could also expect to be used by the Consultant during the test as a guide.

Proposals should the following sections with recommended content of each section:

**Preamble**

* 1. Consultant name, title, and contact information
  2. Subject
  3. Date
  4. Table of Contents

1. **Introduction**
   1. Explain Test Goals and Objectives
   2. Summarize your overall approach
      1. Reference your methodology
   3. Provide a schedule of events
   4. Define the roles and responsibilities in your organization
   5. Cost
2. **Scope**
   1. Targets
      1. Explain what is in/out of scope
      2. Enumerate the assets which will be tested
   2. Limitations
      1. What will not be done
   3. Rules of Engagement
   4. Assumptions
3. **Methodology**
   1. Testing
      1. Explain the types of tests that will be performed
   2. Steps
      1. List and explain the steps to take based on the pen testing framework or methodology
   3. Risk Scoring Methodology
4. **Deliverables**
   1. Explain what will happen at the conclusion of the test
   2. Explain what will be delivered in the final Pen Test Report
   3. Explain the report format
      1. Provide a template as an example

**Appendix**

* 1. Links and References
  2. Glossary of terms
  3. Tools expected to use
  4. Outside Resources that may be used
  5. Additional Interview Questions for Bill Gibson/NBN

# Timeline

Proposals (“Midterm”) should be submitted by the date on the course assignment page.

The Penetration Test will take place during the second half of the course (“CS GY 6573”).

Penetration Test Deliverable (“Final Project”) must be submitted by the date on the course assignment page.

# Contacts

Bill Gibson, CISO  
[gibson@corp.nbn](mailto:gibson@corp.nbn)

NBN Corp  
1800 Archer Street  
New York, NY