Near-Earth Broadcast Network

Contract for Penetration Testing Services

1. Summary

Near-Earth Broadcast Network (NBN) has awarded a contract for qualified cybersecurity consultants ("Consultant") to perform penetration testing services ("Pen test") against a selection of 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.

2. 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").

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

NBN: We're always watching you.

3. Penetration Test Targets and Scope

NBN will provide two (2) system images ("Targets") to the Consultant at the start of the penetration test. These images represent the aggregation of the most common NBN applications and services. The scope of the test will entirely be only these two images. There will be no testing against any production NBN system.

The targets should be deployed and on Consultant-provided systems for testing. All testing should be done over the network, simulating an external adversary. There is no local access to the targets except for setting them up. Any report containing vulnerabilities discovered by having local access to the machines is a breach of this contract and the deliverables will not be accepted.

• Penetration Test Target Details

i. NBN Server ("6573FinalServer.ova")

The Server is a development build of a cloud image that will be deployed. It is used for customer online account access and employee customer service.

ii. NBN Client ("6573FinalClient.ova")

The Client is a development build of an employee workstation. They use this workstation to access the Server or perform other NBN customer service actions.

NBN Developers

- ### Detailed Scope of Work
  - Network Pen Testing
    - Enumerate and assess all external facing hosts and services.
  - Web App Pen Testing
    - Assess and test all external facing Web Apps.
  - Internal Pen Test
    - If internal network access is achieved, continue assessment to find more vulnerabilities and determine impacts.
  - Sensitive Data
    - These development images contain only unclassified test data. Enumerate anything sensitive that is insecure
    - Hidden “flags” are present and represent sensitive data. There eight (8) total. Enumerate any you find.
    - Crack any password hashes found
  - Out of Scope
    - Distributed Denial of Service attacks are out of scope.
    - Local access to the machines (Logging into the VM Console) or anything that would require physical access is strictly forbidden.
  - Severity
    - NBN is 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”.
  - Other Pen Testing
    - Besides what is specifically out of scope, assess and test anything else available for security impact.

4. 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. For each vulnerability, there should also be a methodology for recreating the same results and testing once remediations are implemented. Also provide best practices for software solutions to remediate the vulnerabilities identified.

- ### Deliverable Content and Format

Deliverables should be written as a penetration testing report (“Report”) and an Executive Summary.

Reports can take any format but should be thorough, well-written, and contain content that is useful to NBN. The following sections and content are recommendations but not strict requirements.

A. Executive Summary
   a. Explain purpose of the report
   b. Address major flaws

c. List immediate actions or fixes

d. Explain overall security rating or score

B. Preamble

a. Consultant name, title, and contact information

b. Subject

c. Date

d. Table of Contents

1. Introduction and Summary

a. Explain Test Goals and Objectives

b. Summarize your overall approach

c. Provide a schedule

d. Define the roles and responsibilities in your organization

e. Summarize your overall security rating or score

2. Methodology

a. Explain your high level testing methodology

b. Explain how you scored risk

c. List the tools you used

d. Provide a walkthrough of what you did and explain specific steps*

*This can be combined with the Findings section if you prefer

3. Findings*

a. List all findings. For each finding, include

i. How you found it

ii. How you exploited it

iii. What the score or risk is and why

iv. How to fix

*This section can utilize large tables, bullets, paragraphs. However you choose to organize and present the data.

4. Conclusion

a. Restate and summarize

i. test goals

ii. results

iii. targets

iv. risk

v. immediate fixes

Appendix – Some optional recommendations

b. Links, References, and Outside Resources

c. Glossary of terms

d. Ports, Protocols, and Services

e. Sensitive Data Enumeration (e.g. flags, passwords)

f. Tool output

g. Source code of exploits written

You are welcome to use any template as well. Offensive Security's Penetration Test Report has some nice features. There are other examples available on the following Github repo.

- https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf
- https://github.com/juliocesarfort/public-pentesting-reports

Simstim compatible reporting not required

5. Assessment and Grade

Deliverables will be assessed and scored ("Grade") based on several criteria. The most important part is to have a report that is useful to NBN. The Grade will be split into two equal parts: The quality of the report and the quality of the technical accomplishments.

- Report quality
  - It should have the major sections of a good pen test report
  - Each section should be well-written and organized
  - Ideas and explanations should be clear and concise
- Technical Accomplishments
  - Your ability to utilize the tools, techniques, and methods learned
  - There may be more than one way to accomplish an exploit, and more than one vulnerability to achieve a goal or an effect
- Demonstrate knowledge of the pen testing methodology
- Demonstrate excellent communication to explain vulnerabilities, their associated impact and risk to the target organization
- Demonstrate knowledge of identifying and exploiting vulnerabilities
  - Based on the number of significant vulnerabilities you identify and exploit
    - There are many and you don't need them all. If you're not sure, talk to the POC
  - Being able to explain why that vulnerability is impactful and how it can be fixed

Extra credit will be provided for flags if you explain where you found them and what you did to figure them out. There are eight flags total. Flags will always start off with the word 'flag' and have the following syntax: `flag{this_is_what_a_flag_will_look_like}`

6. Timeline

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

7. Contacts

Please direct questions to the Professor or TA.

All other NBN related questions
Bill Gibson, CISO
gibson@corp.nbn

NBN Corp
1800 Archer Street
New York, NY