Penetration Test Proposal and Plan

For Near-Earth Broadcast Network (NBN Corp)

Sky Security Company

yz5946@nyu.edu

Introduction

In this increasingly digitalized age, cyber threats have become more prevail, common, flexible, and dangerous. The Near-Earth Broadcast Network (NBN Corp), a leading telecommunications and media company, recognizes the critical importance of safeguarding its infrastructure and customer data against evolving cyber threats.

In response to the recent security incident that led to a significant exposure of customer data, this proposal outlines a comprehensive penetration test for Near-Earth Broadcast Network (NBN Corp) to identify potential vulnerabilities, which have not been detected from the previous attack, within NBN's digital infrastructure that may cause mass data loss in future attacks.

Particularly, the penetration test will evaluate the security of both external and internal network security, including the security of the customer-facing platform, internet-facing web server, internal database, and any other possible components that may participate in the interaction between NBN Corp and their customers. The style of these tests would be in a mixed strategy of Black Box, White Box, and Opaque Box testing to better simulate an outside attacker and carry out defensive strategies that neutralize potential vulnerabilities. The specific types of tests will be introduced in detail in the following sections.

Test Proposal

Types of Tests

- **Network Tests**

  Network tests include both external and internal tests. This set of tests targets NBN's internet-facing infrastructure, including web servers and online portals. The objective is to identify vulnerabilities that could be exploited from outside the network and to assess the network, protocols, hosts, and services available for vulnerabilities and weaknesses. This set of tests would be best to simulate an outside attacker. Therefore, Opaque-Box testing is

preferred given NBN is previously compromised, and the attacker already gained a certain extent of information of the security infrastructures. The scope of this set of tests will encompass all internet-facing services, internal networks, application systems, and support channels like online chat. Critical assets, including customer databases, billing systems, and media delivery networks, will be of particular focus. We intend to restrict our testing within the IP address that used in the company.

- **Application Security Testing**

  Given the breach involving access to NBN's internal database and sensitive customer information, a thorough security assessment of all customs and internal communication applications will be conducted. The goal of this set of tests is to prevent an attack from causing more damage to assets if one has already gained access from one of the components within the network. Also, a well-constructed network and internal application would give more time for NBN to react to the incoming attacks. Both White Box and Black Box testing will be employed in testing the security of the application. In particular, the tests include Static Code Analysis and Dynamic Code Analysis. Static Code Analysis aims to identify vulnerabilities by inspecting the code of the application in a White Box setting. Whereas Dynamic Code Analysis will debug the binary, fuzz memory, expose sensitive data, look for flaws and errors to exploit in a Black Box setting. The scope of application security testing encompasses various activities aimed at identifying and mitigating security vulnerabilities in software applications. This set of testing is crucial for ensuring that applications are secure by design, secure in deployment, and secure in maintenance.

Test Details

Network Services Testing

- **Port Vulnerability Scanning and Service Identification:** The purpose is to identify open ports and services running on those ports across networked devices, as well as to automatically scan network services for known vulnerabilities. This test helps in mapping the attack surface of the target network.
- **Protocol Analysis and Sniffing:** The purpose is to inspect network traffic for protocols in use, identifying potential misconfigurations or unencrypted data that could expose sensitive

information.

- **Firewall Configuration and Rule Testing:** The purpose is to evaluate the effectiveness of firewall configurations and rulesets in protecting network services from unauthorized access and other cyber threats.
- **DoS Protection Testing:** The purpose is to evaluate the network's resilience against denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks by testing rate limiting and DoS protection mechanisms.
- **SSL/TLS Configuration Testing:** The purpose is to assess the security of SSL/TLS configurations, including certificate validity, encryption algorithms, and protocol versions, to prevent man-in-the-middle (MitM) attacks and ensure secure data transmission.
- **Other tests:** Any other suitable tests may be performed after the team have a thorough scan of the system infrastructure.

Application Security Testing:

- **Static Application Security Testing (Source Code Analysis):** The purpose is to detect vulnerabilities such as buffer overflows, SQL injection, and other security flaws that can be identified by analyzing the code.
- **Dynamic Application Security Testing:** The purpose is to find issues like runtime SQL injection, cross-site scripting (XSS), authentication and session management flaws, and other vulnerabilities that only manifest when the application is executing.
- **Interactive Application Security Testing:** The purpose is to detect a wide range of issues, providing immediate feedback to developers, and to find vulnerabilities that are only detectable when the application is running with real-time data.
- **Configuration and Deployment Review:** The purpose is to identify misconfigurations, insecure deployment practices, and vulnerabilities related to how the application is set up and managed.

Timeline

The entire penetration test process is expected to be completed within 3 days. Our team intends to use a weekend and the following Monday. Ideally, each part of the penetration test should take 1 day. That is, Network Service Tests will be carried out on Saturday and

Application Security Testing will be carried out on Sunday. The following is used to test and validate the robustness and stability of updated and tested services under normal operating conditions.

Limitations

- **False Positives and False Negatives:** Automated tools can generate false positives and false negatives. Managing false positives can be time-consuming, while false negatives can leave vulnerabilities unaddressed.

- Coverage and Depth Limitations: No single testing method covers all possible security vulnerabilities. Therefore, despite the completeness and thoroughness of the penetration testing plan, there will always be vulnerabilities that remain undetected. To better protect against cyber threats, system security should be periodically analyzed and updated.

- Dynamic Environment Challenges: Applications that rely heavily on dynamic content, complex user interactions, or real-time data processing might not be thoroughly tested using automated tools. And it requires continuous investigation and surveillance over a period of time to better resolve any threats that cause by the change of environment.

Delivery

Upon conclusion of the testing phase, we will provide a detailed report and chart that includes the following: Executive summary of findings; Technical details of vulnerabilities discovered, including proof of concept; Prioritized recommendations for remediation. In addition, our team will hold a seminar with IT and Application Development departments to communicate the security of current system and future maintenance plan.

Extra

We may use the following resources and testing toolkits during our penetration test process: Kali Linux Machine will be used as testing machine. The following toolkits may be used: Nmap, Nessus, Netcat, OpenVAS, Telnet, Wireshark, tcpdump, Metasploit, John the Ripper, Hashcat, hping3, OWASP Threat Dragon, OWASP ZAP, SonarQube, Fortify.