Near-Earth Broadcast Network

Proposal for NBN
Penetration Testing Services

(Ref.: NYU “CS GY 6573” Fall 22)

AGYA Corporation is pleased to offer this Penetration Testing Services proposal, in order to help NBN securing its Valuable Assets. We have a team of experts with large international experience, which are committed to technical excellence with ethical behavior. The best-in-class approach we use to penetration tests and risk management has already been successfully tested in small, medium and large organizations. We are positive that our solution will greatly assist NBN in understanding the cybersecurity risks for outside threats, and will guide NBN on what can be done to minimize this risk.

Proposal:

Leandro R. Maciel, Pen Test Senior Consultant
leandro.maciel@agyacorp.com
5301 Technology Drive
Tampa, Florida, 33647

Subject: Penetration Tests and Risk Management Proposal, in reference to Near-Earth Broadcast Network (NBN) – Penetration Testing Services Request for Proposal (RFP)

Date: October 23rd, 2022

Table of Contents

NBN: We're here to assist you.

1. Introduction

AGYA Corporation started during 2005, with an original solution created for network packet visibility, applied to cybersecurity. A Deep Packet Inspection based technology was commercially implemented in 3 network operators throughout 2015, generating over 15M USD in revenues, providing IP traffic control (offloading congested networks), implementation of security policies (e.g., IPS/IDS), and the prevention of DDoS attacks, to list just a few applications. This success propelled the creation of a new cloud orchestration solution with Cybersecurity features, such as portal SSL encryption, OpenID Connect for secure login (via Office 365, G-Suite, Okta, etc.), Role Based Access Control (RBAC) and Ransomware protection. Following market needs, with cybersecurity as an inexorable building block in all networks, Penetration Testing and Risk Assessment was deeply studied, and incorporated as a key element in our portfolio. Equipped with best-in-class software tools, our solution is offered here as a critical service to many companies secure and prosper future.

a. Test Goals and Objectives

The objective of this Penetration Testing and Risk Assessment Service (Pen Test) is to perform a controlled cyber-attack helping to secure NBN's IT infrastructure. All security tests, internal and external, must be conducted in a way that simulates a malicious actor involved in a targeted attack against the NBN, with the objectives of:

- ✓ Identifying if a remote attacker could penetrate NBN's defenses
- ✓ Determining the impact of a security breach on:
  - Confidentiality of the company's private data
  - Internal infrastructure and availability of NBN's information systems

Our focus is on identifying and exploiting security weaknesses that could allow a remote attacker to gain unauthorized access to applications and organizational data. Attacks will be conducted with the level of access that a typical internet user would have. The evaluation will be carried out consistent with the recommendations outlined in NIST SP 800-115. Finally, all tests and actions will be conducted under controlled conditions.

b. AGYA Pen Test overall approach

Our overall approach is based on the following principles:

1. Data privacy is paramount. Your data is protected. We understand and respect "need-to-know" boundaries, we test legally and always with pre-authorization.
2. Technical Excellence. Only relying on best-in-class tools, extensively tested, and supported by reputable organizations (PTES, OSSTMM, NIST, OWASP, Metasploit, to name a few)
3. Stealth Mode. All tests are aimed to be unnoticed, with minimum impact to existing systems. No availability issues (Denial of Services) should be expected during our services intervention.

Given that, as listed in the RFP, 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 subscriber (subs), a Business Partner (BP), or a non-affiliate. So, from this requirement, we conclude that we should follow the approach of a RED TEAM (a.k.a., black box testing).

Following the Cyber Kill Chain Framework (CKCF), we believe that a substantial amount of time should be spent on the Reconnaissance phase (>50% of the Pen Test time). This approach is resulting from our experience, since only thoroughly understanding the environment will lead us to effective exploitation and a consequent security to a robust system.

Furthermore, leveraging DevOps culture and CI/CD methods, our methodology suggests many short cycles of "equivalent" CKCF, linked to a constant a Reconnaissance phase, supported by strong documentation steps. The next pictures describe our methodology.

i. Reference to our methodology (CKCF)

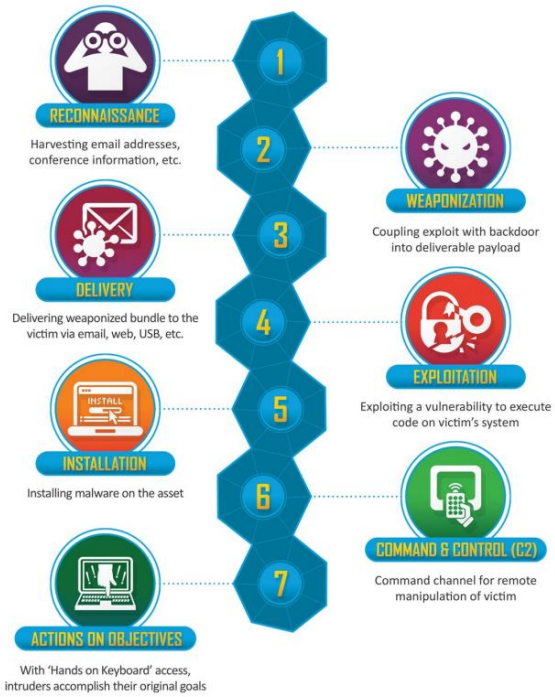

Figure 1: Lockheed Martin Cyber Kill Chain Framework (CKCF)

ii. Our Methodology

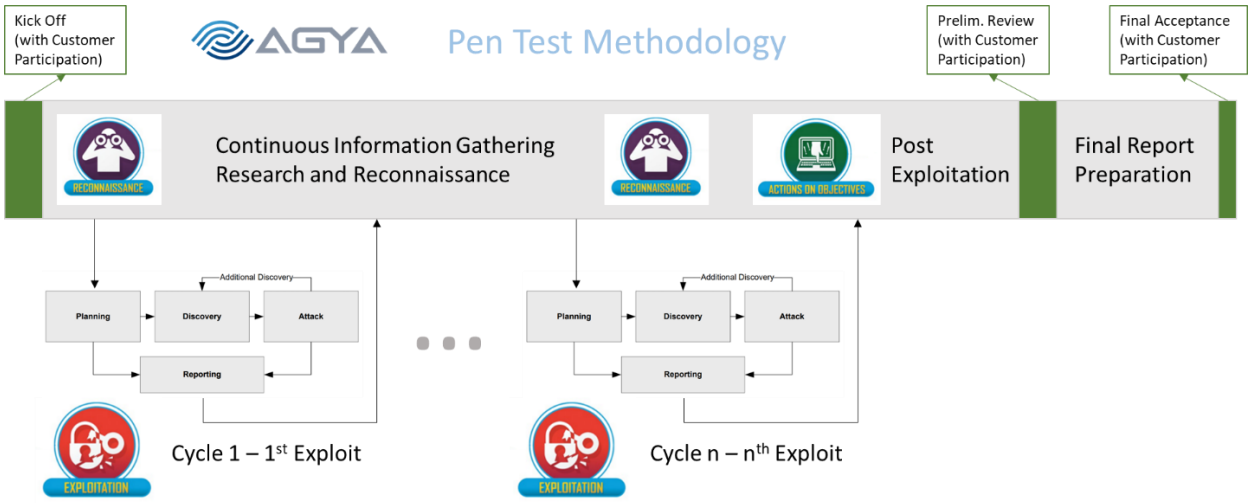

Figure 2: AGYA Pen Test Methodology based on DevOps and CI/CD Concepts.

c. Schedule of events

The engagement is planned for 3 weeks (15 days), with the following milestones:

Day 1: Contract Signature and Kick Off Meeting

- ✓ Customer Interview,
- ✓ Confirm or redefine testing scope and Rules of Engagement (RoE),
- ✓ Complete forms (Liability Waiver, NDA, Permission Memo – check Appendix),
- ✓ Confirm Test Team and review schedule / team needs.

Day 2: Information Gathering, Research and Reconnaissance (1/3)

- ✓ Learn about the targets / scope / roles and responsibilities
- ✓ Targets as organizations, people, applications, hosts, policies, networks, systems
- ✓ Passive information gathering
- ✓ Public facing targets (domains, DNS, IP's, etc.)

Day 3: Information Gathering, Research and Reconnaissance (2/3)

- ✓ Apply Reconnaissance tools such as Whois, Google search, OSINT, Shodan, Exiftool, FOCA, Recon-ng, Amass, etc.
- ✓ Inventory creation
- ✓ What was found, how was found, impact of findings

Day 4: Information Gathering, Research and Reconnaissance (3/3)

- ✓ Risk Scoring – prioritize, rank and score findings
- ✓ Use CVSS – Common Vulnerability Scoring System
- ✓ Set up environment and start scanning
- ✓ Vulnerability Enumeration

Day 5: Network Scanning

- ✓ Ping Sweep / Host Discovery
- ✓ Network Tracing
- ✓ Port Scanning - Identifying vulnerable servers and ports
- ✓ Version Scanning (OS finger printing)
- ✓ Vulnerability Enumeration Scanning
- ✓ Use tools such as TCPdump, nmap, ncat, OpenVAS, Scapy

End of First Week

Day 6: Exploitation Cycles (1/3)

- ✓ Run in parallel: Information Gathering, Research and Reconnaissance
- ✓ Service Side, Client Side, Applications, Web Applications, Background systems such as DB servers, and any other vulnerable element
- ✓ Use OWASP top 10 as reference, to protect against most common attacks
- ✓ Goal to achieve, at least, Shell access on remote system
- ✓ Tools used: Metasploit (including Meterpreter), Fuzzing, BOF, edb (Assembly), msfvenon, BURP, OWASP ZAP, C and Python programs

Day 7: Exploitation Cycles (2/3)

- ✓ Continuation from previous day

Day 8: Exploitation Cycles (3/3)

- ✓ Continuation from previous day

Day 9: Post-exploitation attacks (1/2)

- ✓ After previous exploits, having access to servers
- ✓ Local privileges escalation
- ✓ Relay creations, Transferring files, Remote file execution
- ✓ User credentials, passwords and authentications attacks
- ✓ Apply tools such as John the Ripper (JTR), THC-hydra, Hashcat, among others

Day 10: Post-exploitation attacks (2/2)

- ✓ Continuation from previous day

End of Second Week

Day 11: Customer Meeting – Preliminary Findings and Guidance on Final Report

- ✓ Final Report format, audience, any particular emphasis required
- ✓ Suggested topics:
  - Executive Summary
  - Introduction
  - Methodology
  - Findings
  - Conclusions
  - Next Steps / Future work
  - Appendix

Day 12: Final Report Preparation 1/3

- ✓ Review previous cycles / exploits, and act upon if needed

Day 13: Final Report Preparation 2/3

- ✓ War room, all hands on deck

Day 14: Final Report Preparation 3/3

- ✓ War room, all hands on deck

Day 15: Customer Meeting - Final Report Presentation and Suggested Next Steps

End of Engagement

d. Roles and responsibilities in NBN and AGYA organization

NBN (Customer) Team:

- NBN team is expected to participate on days 1, 11 and 15, guiding AGYA (Consultants) on questions, impediments and/or any variations from original scope of work (SOW)
- Any NBN system operational issue, or maintenance, that causes any impact on regular performance of the tested environment should be immediately informed to the Consultants
- Documents needed to be signed: Liability Waiver, NDA, Permission Memo – check Appendix
- Should provide a list of contacts and escalation path

AGYA (Consultants) Team:

- AGYA team is expected to provide all equipment, hardware and software, to carry out the work to be done, accordingly to the pre-approved SOW
- If by any chance a severe security breach (critical), or any service impacting event occur, Consultants should inform the Customer immediately, following the predefined escalation path
- Should provide a list of contacts and escalation path
- Daily 30 minutes report on project development presented via video call (tea time call – 5pm)

e. Cost

- The cost for this current engagement is US$ 41,400 (3 weeks minimum)
- Each additional week costs US$ 13,800
- Payment to be done in US currency and in US banks

2. Scope

From the RFP, we understand that 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.

A graphical representation of the environment is presented to better assist our teams. This could be referred as the Solution Architecture:

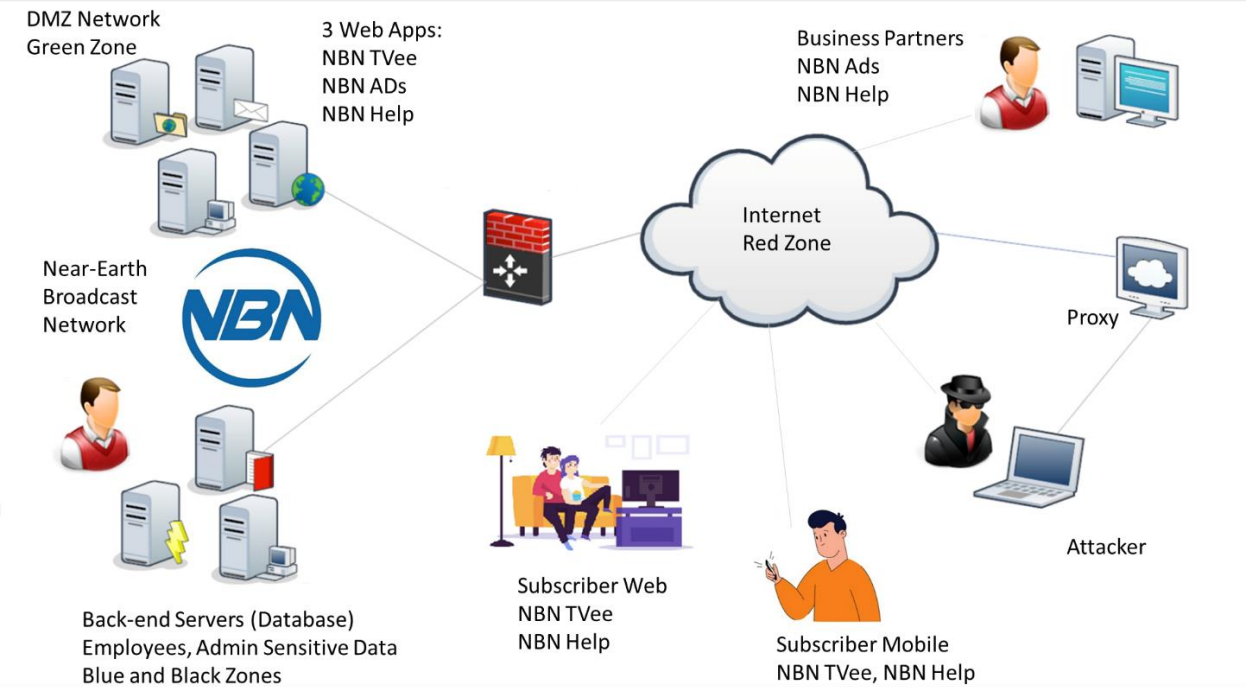

Figure 3: NBN Architecture

a. Targets
    i. What is in scope
    - External Network Pen Testing
        Enumeration and assessment of all external facing hosts and services.
    - External Web App Pen Testing
        Assessment and exploitation of all external facing Web Apps.
    - Internal Network Pen Test
        If an internal network access is achieved, continue assessment to find more vulnerabilities and determine impacts.
    - Severity
        This offer is only interested in security flaws that have "medium" security impact or higher (i.e., "high" and "critical") but this offer will still report any vulnerability or weakness.
        Attacks that compromise a single account are considered "low" security impact.
        Information-only, suggested best practices, and theoretical-only exploits are considered "low" security impact.
    - Other Pen Testing
        Besides what is specifically out of scope, namely, third parties applications other than NBN's, industry software and OS's (Windows, Linux, and commercial available applications), this offer will assess and test anything else available for security impact.

    ii. Enumerate the assets which will be tested
    - 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 ("NBN Help") which only has a web client. It is used by both Subs and BPs for making account changes and chatting with customer support.

b. Limitations
    i. What will not be done
    - Anything illegal in reference to the current law of the land.
    - 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.

c. Rules of Engagement

The document NIST SP 800-115, Appendix B, provides a detailed template for the Rules of Engagement (RoE). The link for such document is provided at the end (below) of this Pen Test Service offer. Here we will present only the key points for the RoE. Upon contract signature, a joint team NBN + AGYA could delve into a detailed RoE document creation.

The final RoE should include name of participants, detailed schedule, equipment identified by respective MAC's, incident handling and response, targeted system / network (domain names or IP addresses), data handling (storage, privacy), etc.

For now, previous and subsequent sections in this current document describes the critical information pertained in the RoE, i.e., the SoW, the Test Schedule, the Tools suggested for use, the Communication strategy (30 minutes calls, and the escalation path for both companies, for incident handling), and the preliminary and final reporting.

d. Assumptions

The assumptions made by our Pen Test Team is very basic, that the 3 applications to be tested, likewise all network supporting NBN infrastructure, WILL be available during all test period. If any outage is experienced, there will be consequences in the proper development of this Pen Test service. We also assume that NBN will be available for the predefined meetings and for the 30 minutes "tea time" project status reporting.

3. Methodology

a. Testing

i. Types of tests that will be performed

Network Scanning Tests

Ping Sweep / Host Discovery
Network Tracing
Port Scanning - Identifying vulnerable servers and ports
Version Scanning (OS finger printing)
Vulnerability Enumeration Scanning
Use tools such as TCPdump, nmap, ncat, OpenVAS, Scapy

Exploitation Tests

Run in parallel: Information Gathering, Research and Reconnaissance

Test vulnerability on Service Side, Client Side, Applications, Web Applications, Background systems such as DB servers, and any other possible element vulnerability

Test using OWASP top 10 as reference, to protect against most common attacks

Goal to achieve, at least, Shell access on remote system

Tools used: Metasploit (including Meterpreter), Fuzzing, BOF, edb (Assembly), msfvenon, BURP, OWASP ZAP, C and Python programs

Post-exploitation Tests

After previous exploits, having access to servers, test how one can navigate internally at NBN

Test if it is possible to have Local privileges escalation

Test for Relay creations, Transferring files, Remote file execution

Test vulnerability for User credentials, passwords and authentications attacks

Apply tools such as John the Ripper (JTR), THC-hydra, Hashcat, among others

Customer Tests

Review Preliminary Findings and Provide Guidance on Final Report

Test Final Report format, audience, and if any particular emphasis required

It is expected a Test Pass validation in order to progress to Final Report

b. Steps

i. List and explain the steps to take based on the pen testing framework or methodology

Step number 1:

Information Gathering, Research and Reconnaissance

Learn about the targets / scope / roles and responsibilities

Targets as organizations, people, applications, hosts, policies, networks, systems

Passive information gathering

Public facing targets (domains, DNS, IP's, etc.)

Apply Reconnaissance tools such as Whois, Google search, OSINT, Shodan, Exiftool, FOCA, Recon-ng, Amass, etc.

Inventory creation

What was found, how was found, impact of findings

Risk Scoring – prioritize, rank and score findings. Use CVSS – Common Vulnerability Scoring System

Set up environment and start scanning

Create table with Vulnerability Enumeration

Step number 2:

Network Scanning

Ping Sweep / Host Discovery

Network Tracing

Port Scanning - Identifying vulnerable servers and ports
Version Scanning (OS finger printing)
Vulnerability Enumeration Scanning
Use tools such as TCPdump, nmap, ncat, OpenVAS, Scapy

Step number 3:
Exploitation Cycles
As described in the Methodology – recurrent - repeat as many times as needed
Run in parallel: Information Gathering, Research and Reconnaissance
Test vulnerability on Service Side, Client Side, Applications, Web Applications, Background systems such as DB servers, and any other possible element vulnerability
Use OWASP top 10 as reference, to protect against most common attacks
Goal to achieve, at least, Shell access on remote system
Tools used: Metasploit (including Meterpreter), Fuzzing, BOF, edb (Assembly), msfvenon, BURP, OWASP ZAP, C and Python programs

Step number 4:
Post-exploitation attacks
After previous exploits, having access to servers
Local privileges escalation
Relay creations, Transferring files, Remote file execution
User credentials, passwords and authentications attacks
Apply tools such as John the Ripper (JTR), THC-hydra, Hashcat, among others

Step number 5:
Customer Meeting – Preliminary Findings and Guidance on Final Report
Final Report format, audience, any particular emphasis required
Suggested topics:
- Executive Summary
- Introduction
- Methodology
- Findings
- Conclusions
- Next Steps / Future work
- Appendix

Step number 6:
Final Report Presentation and Suggested Next Steps

Step number 7:
Signature of Term of Acceptance for the service rendered

c. Risk Scoring Methodology

i. Use CVSS – Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity (form 1 to 10, 10 being the highest vulnerability). The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

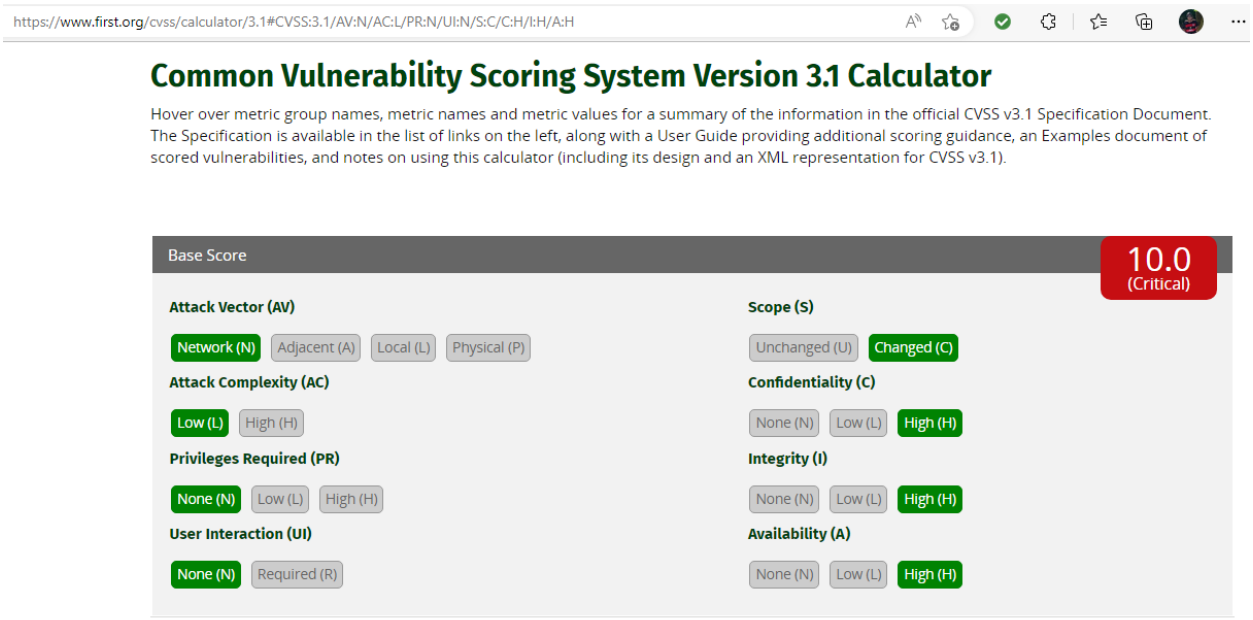

Figure 4: Common Vulnerability Scoring System (CVSS) Version 3.1 Calculator

CVSS is a published standard used by organizations worldwide. The Calculator can be found in the Appendix below.

4. Deliverables

a. What will happen at the conclusion of the test

The Final Report will present our findings after 3 weeks of thorough system penetration testing, enumerating the vulnerabilities found, while attempting to breach NBN systems. Our final goal is to greatly assist NBN in understanding the cybersecurity risks for outside threats, and guide NBN on what can be done to minimize this risk.

A list of cybersecurity risks will be presented, and for each one there will be four categories to proper describe their relevance:

- Rating (Low, Medium, High and Critical)
- Description
- Impact
- Remediation

Also, the report will present details on how each cybersecurity risk was found, the software tools that were used during the process, and the methodology applied. Finally, a set of recommendation will be provided based on our previous experience, with additional information, suggested best practices, and theoretical exploits, so prevention could be considered as the best "remediation" (crisis avoidance) to protect NBN's valuable assets.

b. What will be delivered in the final Pen Test Report

We are committed to provide a comprehensive technical, detailed, Executive Summary and Report, based on our Pen Test results obtained. They will contain vulnerabilities, by level of risk, with recommended correlated remediation. For each vulnerability, there will also be a step-by-step approach for recreating the same results and testing once remediations are implemented. Also, the report will provide best practices for software solutions to remediate the vulnerabilities identified.

c. The report format

Deliverables will be written as a penetration testing Report and an Executive Summary. Reports that we typically deliver are thorough, well-written, and contains content that is useful to our customers. The following section has the typical template used in our Pen Test reports.

i. Example of a Final Pen Test Report Template

A. Executive Summary

a. The purpose of the report

b. Major flaws encountered

c. Immediate actions or fixes

d. The overall security rating / score

B. Preamble

a. Consultant name, title, and contact information

b. Subject

c. Date

d. Table of Contents

1. Introduction and Summary

a. Test Goals and Objectives

b. Our overall approach

c. Test schedule

d. Roles and responsibilities in our organization

e. Our overall security rating / score

2. Methodology

a. Our high-level testing methodology

b. How the risk was scored

c. Tools used

d. Walkthrough of what we did and the specific steps

3. Findings

a. List of all findings. For each finding:

i. How it was found

ii. How it was exploited

iii. The score risk and why such score

iv. How to fix

4. Conclusion

a. Summary of

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

Appendix

a. Links and References

https://csrc.nist.gov/publications/detail/sp/800-115/final
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
https://www.nist.gov/privacy-framework/nist-sp-800-30
https://www.first.org/cvss/
https://github.com/juliocesarfort/public-pentesting-reports

b. Glossary of terms

https://csrc.nist.gov/glossary

c. Tools expected to use

Whois, Google search, OSINT, Shodan, Exiftool, FOCA, Recon-ng, Amass
TCPdump, nmap, ncat, OpenVAS, Scapy
Metasploit (including Meterpreter), Fuzzing, BOF, edb (Assembly), msfvenon, BURP, OWASP ZAP, C and Python programs
John the Ripper (JTR), THC-hydra, Hashcat, among others

d. Outside Resources that may be used

Permission Memo: Legal Docs\Permission Memo v 1.0.docx
Liability Waiver: Legal Docs\Liability Waiver v 1.0.docx
NDA (Non-Disclosure Agreement): Legal Docs\2022 Mutual NDA AGYA v 1.0.doc

e. Additional Interview Questions for Bill Gibson/NBN

None, so far. Thanks!