Policy_VA_Q3
Rules For Vulnerability Assessment (Partial)

Testing Infrastructure

- Target Machine – 10.10.10.10
- Analyst Machine – 10.10.10.7

Folder Contents - /root/Desktop/Q3

- Q3_Phishing_Results.zip – Users & Passwords for Brute forcing
- Q3_OSINT_Data.zip – Screenshots for OSINT Assessment
- backdoor.php – A PHP Based Web Shell

Trusted Sources

- Research – CVE Details, MITRE, NVD, Google, YouTube
- Exploits/PoC – GitHub
- Scoring & Rating - CVSS 3.0
    - Confidentiality Requirements - Medium
    - Integrity Requirements - Medium
    - Availability Requirements – Low
    -

Tools & Programs Allowed

- Nessus Essentials
- Faraday CE
- NMap
- BurpSuite
- Wpscan
- Netcat
- Curl
- Google Docs or Similar Office Suites

Testing Requirements

- Automated Scan as Per Policy_NS_Q3
  - Use Nessus to scan
  - Upload results to Faraday
- Manual Network Vulnerability Assessment
  - Testing to be done for services marked High or Critical in Automated Scan
  - Only Test CVE's With Exec Code
- Web Vulnerability Assessment
  - No Report Needed
  - If exploited successfully, Post screenshot in Appendix D

Report Structure

- Document Control
- Legal Disclaimer
- Table of Contents
- Executive Summary
- A Glance Through Target Security Posture
- Testing Methodology
- Tools & Websites Used
- Detailed Technical Reports (Scope Limited)
  - [infra.example.com]
    - Finding X: Description – Rating
    - Steps to Reproduce
- Appendixes
  - Appendix A: Vulnerability Score Analysis – CVSS 3.0
  - Appendix B: Modified Exploit Code For CVE-XXXX-XXXXX
  - Appendix C: Screenshots For Nessus & Faraday
  - Appendix D: Screenshots Of Exploited Web App
  - Appendix E: OSINT / Phishing Results Data Used