AGC
Accelerating Business

AGC Networks Consulting Offer

Vulnerability Assessment & Penetration Testing

An ESSAR Enterprise

OBJECTIVE

- Comprehensive testing for IT infrastructure including Applications, Servers and Network components
- Discover vulnerabilities in IT infrastructure at OS, Applications and Network Level
- Assist in meeting compliance requirements of PCI, SOX, ISO 27001 & HIPAA standards

DESCRIPTION

Vulnerability Assessments and Penetration Testing meet two distinct objectives, usually with different results, within the same area of focus. Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between exploitable flaws and innocuous ones. Penetration tests attempt to utilize the vulnerabilities in a system to determine if any unauthorized access or other malicious activity is possible and identify the threats. AGC's VAPT practice meets various security assessment needs ranging from awareness to extensive penetration and ethical hacking by iteratively identifying the weakest link in the chain and prioritizing real threats.

METHODOLOGY

Terms of Reference

01 Pre Assessment
- Define objectives & Scope of Assessment
- Establish Information Protection Procedures
- Identify and Rank Critical assets

02 Assessment
- Conduct Vulnerability Assessment
- Conduct Penetration Testing

Findings & Recommendations

03 Post-Assessment
- Report
- Priorities Recommendations

Assessment Process

Vulnerability Assessment Phase

Information Gathering

We use OSINT (Open Source Intelligence)
- Enumerate info using search engines/social media
- Network recom using who is rewards, DNS queries etc

Network Mapping
- Scanning
- OS Finger printing
- Enumeration

Vulnerability Identification
- Misconfiguration detection
- Detect vulnerabilities
- Missing patches
- Default password & password guessing
- Unwanted ports (possible threats)
- Network devices and server weakness

Penetration Testing Phase

Testing Process
- Gaining access & privilege evaluation
- Manual pentesting
- Automated tool based pentest
- Exploitation or vulnerabilities in VA
- Privilege escalation
- Post exploitation task (pivoting, gathering more information)
- Exploit further into network (server & devices)
- Clean up activity (post expectation phase)
- Compromise Remote users / sites
- Maintaining access
- Auditing

1. VA ASSESSMENT PHASES

- Discovery
- Exploitation/Analysis
- Reporting

2. VA ASSESSMENT PHASES IN DETAIL

- Discovery
  - Identification of all hosts in the client's network that are visible from the internet
  - Following that, there is the discovery of the services that each machine offers
- Exploitation/Analysis
  - Each service and application discovers a cross-reference to an extensive database to generate a list of potential vulnerabilities
- Reporting
  - Detailed and easy-to-read reports containing High Risk, Medium Risk and Low Risk will be provided along with the remediation recommendations
  - For High Risk Vulnerabilities identified by AGC consulting team, client may opt to install a comprehensive security solution or other services in areas of Policy and Implementation

3. PENETRATION TESTING PHASES

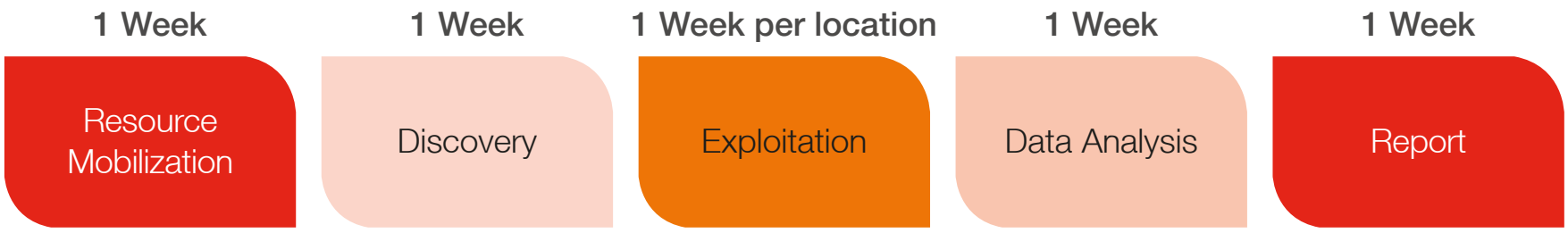
- Discover/Map
- Penetrate Perimeter
- Attack Resources

4. PENETRATION TESTING PHASES IN DETAIL

- Reconnaissance
- Discovery
- Public Domain Sources
- Port Scanning
- Identification of Services
- Short Listing of Crucial IPs
- Identification of Operating System
- Identification of Vulnerabilities
- Exploitation of Vulnerabilities
- Other Attacks

TIMELINES

The following is an indicative timeline for an IT infrastructure to be assessed having **50 IP addresses** for VA/PT (Blackbox Testing). The timelines for exploitation and data analysis may vary depending on the complexity of operations.



DELIVERABLES

Post completion of the activity, a detailed report will be submitted to the client. The report format will be as under:

A. Introduction

- Objectives of the assignment
- Scope of the assignment
- Standards followed
- Duration of the assignment

B. Management Summary

- High-level findings
- High-level recommendations
- Graphical summary

C. Technical Report

- This report will contain the vulnerabilities discovered with CVE ratings and the mitigation recommendations

D. Conclusion

CASE STUDIES

1. Large BPO based out of Philippines

Problem Statement

1. Non-compliance with PCI-DSS standards
2. Lack of visibility of top management into IT Security layers
3. Customer acquisition – Security and Compliance as necessary enablers for top management

Program Intervention

- Information gathering through OSINT
- Network mapping using scanning and enumeration techniques
- Scan of unwanted ports
- Detection of vulnerabilities and exploitation
- Auditing

- **Compliance levels upgraded to PCI-DSS for handling banking data**
- **Improved customer acquisition capabilities**

2. Large BFSI Organization

Problem Statement

1. Compliance mandate for ISO 27001
2. Entrustment of financial information, intellectual property,and employee details by third parties
3. Business alignment with industry best practices

Program Intervention

- Information gathering through OSINT
- Network mapping using enumeration techniques
- Vulnerability identification through multiple methods
- Ethical hacking to identify and prioritize flaws into high, medium and low risk

- **ISO 27001 compliance achieved for business with a much better alignment to business strategy**

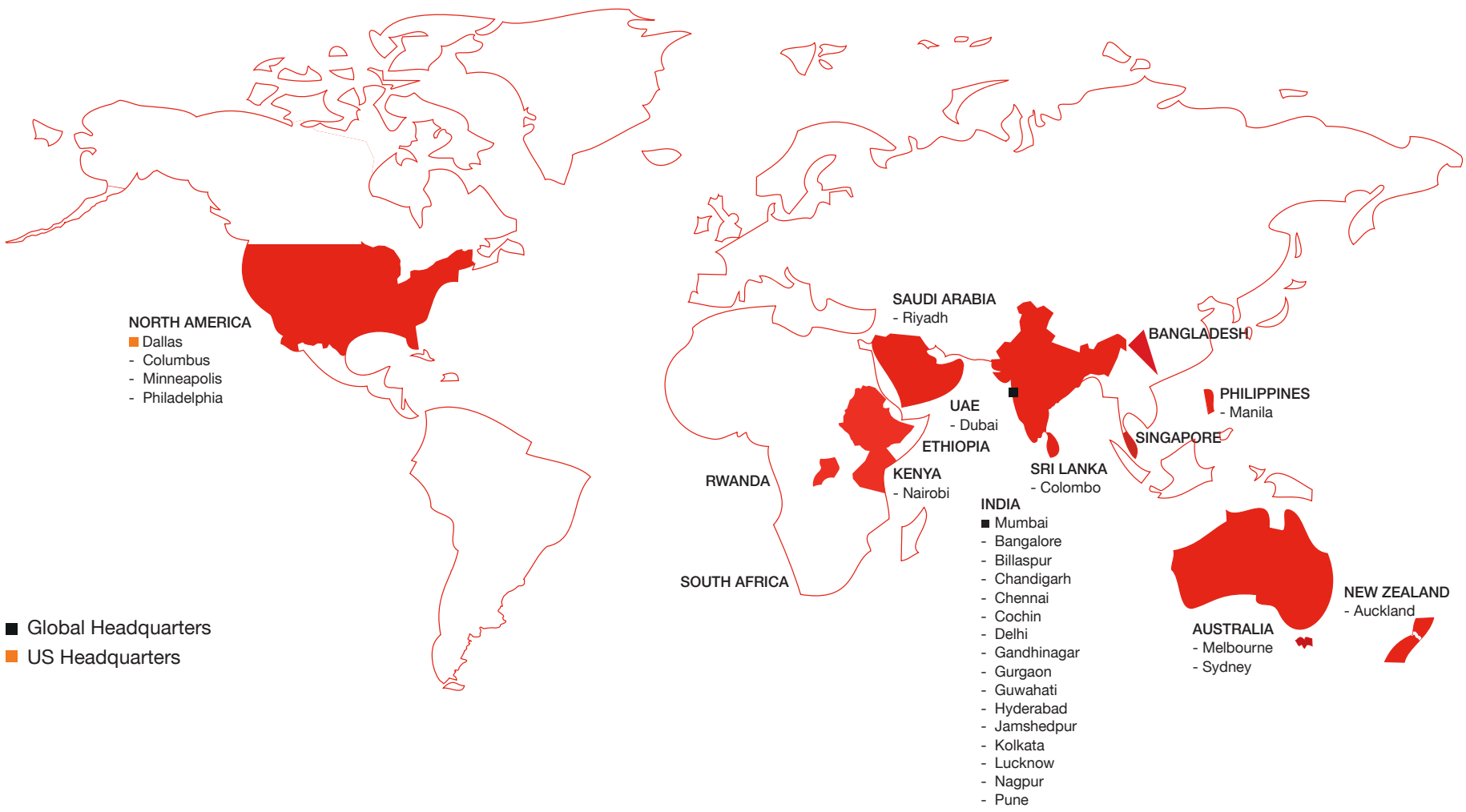
ABOUT AGC

AGC Networks (AGC) is a Global Solution Integrator delivering technology solutions in Unified Communications, Network Infrastructure & Data Center, Cyber Security and Enterprise Applications. AGC is a leader in Enterprise Communications in India and has a significant presence in the Middle East / Africa, North America, Philippines and Australia / New Zealand.

In collaboration with global technology partners like Avaya, Cisco, HP, Juniper, Netapp and Polycom among others, AGC delivers domain-focused, flexible and customized technology solutions and seamless services to accelerate our customer's business. AGC Networks is an Essar Enterprise.

For more information, log on to www.agcnetworks.com

GLOBAL FOOTPRINT



Contact Us

Registered Office

AGC Networks Limited, Equinox Business Park, Tower A (Peninsula Techno Park),
Off. BKC, LBS Marg, Kurla West, Mumbai 400070, India. | T: + 91 22 66617272

E: info@agcnetworks.com | W: www.agcnetworks.com