Capability Statement

Company Designations
CAGE CODE: 1PVX5
DUNS#: 132707923
EIN: 31-1699015
CCR Registered
8a/SDB Veteran Owned
ORCA REGISTRATION: COMPLETE

NAICS CODES
541690 Security Consulting Services
541512 Computer Related Services
541511 Software Related Services
517110 Telecommunications networks

Security Consulting Services- 541690

Outline of Services to be performed against machines with an Internet Presence:

Network Surveying
Identification of targets, DNS zone transfers, Search engine mining
Netblock identification, subnet sweeps.
Port Scanning
Nmap scan, Qualys scan, Nessus scan
Services Identification
Banner identification, identify known ports
System Identification
Nmap OS fingerprints, TCP windows size and sequence number checks, OS Banners
Vulnerability Research and Verification
Match identified ports and services with known vulnerabilities and exploits
Identify sources of rumored 0day. Exercise cold penetration if possible.
Rate level of risk associated with each vulnerability.
Internet Application Testing
Testing of home-grown Web Applications, SQL injection, XSS attempts,
general input validation testing.
Router Testing
Verification of Access Control Lists and rules
Trusted Systems Testing
Verification of Access from Trusted systems
Intrusion Detection System Testing
Validate effectiveness of IDS rules vs False positive generation (Stick)
Containment Measures Testing
Validate attempts to segregate the network, DMZ configuration, Make sure no dual-homed machines exist where they shouldn't, prevent distributed metastasis where possible.
Password Cracking
Attempt to crack passwords recovered during the pen test. Attempt to crack passwords of normal system users including end user and administrative support staff.
Denial of Service Testing
Attempt to trigger known denial of service conditions that may affect application stability.

Security Consulting Services- 541690

Forensic Analysis (Post-Incident)

Intrusion Prevention >VPN, Penetration Testing

Blind Testing

Cooperative Testing

Offensive Intrusion

a) Identify Target(s) and Types
b) Determine Region
c) Determine Class or National Origin
d) Software Intrusion or Operating System

Determine level of Offensive Intrusion Tool

Package and Provide the Exploit(Tool)

Provide Training and Documentation of Tools and Findings

Create Exploits for existing conditions

Provide Containment of Tools & Exploits

Customers

- City of Columbus, Ohio
- FBI> Infraguard
- idefense> Commercial Intelligence Gathering, Purchased Vulnerabilities
- H.B. Gary Distributed Various Security Products and Tools to Various Agencies
- Tipping Point> Zero Day Initiative Product