



National Cybersecurity Assessment and Technical Services: Capability Brief

Presented by: Sean McAfee

Updated: May 5, 2014



**Homeland
Security**



Program Overview

- Offer Full-Scope Red Team/Penetration Testing Capabilities
- Services are tailored to fit agency requirements
 - Risk and Vulnerability Assessments (RVA)
 - Cyber Hygiene (CH)
- Independent (third party) review; results of assessment will not be shared or disseminated
- Services provided at “No-Cost” to agencies



Objective and Benefits

- Proactive engagement to improve overall cyber security posture
- Identify risks, and provide risk mitigation and remediation strategies
- Provide access to high demand, limited supply expertise and resources – at no cost
- Complement an agency's existing security program and capabilities
- Provide an objective view of an agency's security posture



RVA Services and Capabilities

| Service | Description | Internal/ External to Customer Network |
|--------------------------------------|---|--|
| Vulnerability Scanning and Testing | Conduct Vulnerability Assessments | Both |
| Penetration Testing | Exploit weakness or test responses in systems, applications, network and security controls | Both |
| Social Engineering | Crafted e-mail at targeted audience to test Security Awareness / Used as an attack vector to internal network | External |
| Wireless Discovery & Identification | Identify wireless signals (to include identification of rogue wireless devices) and exploit access points | Internal |
| Web Application Scanning and Testing | Identify web application vulnerabilities | Both |
| Database Scanning | Security Scan of database settings and controls | Internal |
| Operating System Scanning | Security Scan of Operating System to do Compliance Checks (ex. FDCC/USGCB) | Internal |



RVA Process

Pre ROE

- Agency contacted
- Briefed on NCATS services
- Service is Requested
- Schedule Confirmed
- ROE Distributed/Agency signs ROE



Pre Assessment (Minimum) 2 weeks

- Pre-Assessment Package Distributed
- Receive Completed Pre-Assessment Package
- Conduct Pre-Assessment Teleconference
- Receive Pre-Assessment Artifacts (1 week)



Assessment 2 weeks

- Off-Site Assessment Activities
- On-Site Assessment Activities



Reporting 3 weeks

- Draft Report Started/Completed
- Submit Draft Report to Agency
- Receive Draft Report with Agency Comments
- Q&A Process Started/Completed



Post Assessment 1 week

- Final Draft Completed
- Final Report Delivered to Customer
- Assessment Out brief



RVA Report Snapshots

National Cybersecurity Assessment and Technical Services

Risk and Vulnerability Assessment

Prepared for {Agency Long Name}
{Long Date}

4. Detailed Assessment Findings

4.1 Overview

Within this report, findings and specific vulnerabilities are rated by severity, as shown in the table below, to assist management with prioritizing remediation and planning activities. The severity is an indication of the potential risk to an agency. {Agency Short Name} management and system owners should evaluate the actual business risk posed by these findings to the assessed applications. For a detailed description of the criteria used to apply severity ratings to identified risks, refer to [Appendix B](#).

The table below is a summary, separated by severity and system, of significant findings discovered during the assessment.

| Assessment | Critical | High | Medium | Low | Informational |
|----------------------------------|----------|----------|----------|----------|---------------|
| Network Mapping | | 1 | | | |
| Network Vulnerability Scan | 1 | 6 | 2 | 2 | |
| Wireless Network Scan | | | 1 | | |
| Web Application Scan | | | | | |
| Database Scan | | | 1 | | |
| Operating System Scan | | | | | |
| Network Penetration Test | | | 2 | 2 | |
| Web Application Penetration Test | | | | | |
| Wireless Penetration Test | | | | | |
| Phishing Click Rate | | | | | |
| Phishing Payload | | | | | |
| Total | 1 | 7 | 6 | 4 | |

Critical Vulnerabilities identified:

1. **Unrestricted Network File System (NFS) Shares** – Four hosts were identified within the internal network environment, which allowed access to the file system via unrestricted NFS shares. While analyzing the files available on the shares, credit card information, and customer personally identifiable information, application source code, transaction data and other sensitive information was discovered. An attacker could leverage this information to recover sensitive data about the users of the agency application.

All of the findings were mapped to applicable FISMA controls as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. The chart below illustrates the five most common control families cited based on the number of findings. The complete mapping is included in the detailed technical description for each finding. It should be noted that some findings mapped to multiple applicable FISMA controls.

Most Frequently Cited FISMA Controls:

| Initials | Control | Count |
|----------|----------------|-------|
| AC | Access Control | X |

For Official Use Only (FOUO)

Page | 14

INTERNAL Scan

| Port | Open on # of Hosts | Distinct Services (by Port) | Port | Open on # of Hosts | Distinct Services (by Port) | Port | Open on # of Hosts | Distinct Services (by Port) |
|---------|--------------------|-----------------------------|---------|--------------------|-----------------------------|----------|--------------------|-----------------------------|
| SMTP | 0 | | TCP 113 | 6,138 | 2 | TCP 995 | 0 | |
| SMTP | 189,903 | 4 | TCP 139 | 4,362 | 2 | TCP 1055 | 0 | |
| TCP 21 | 4,284 | 1 | TCP 139 | 4,377 | 2 | TCP 1720 | 2 | |
| TCP 22 | 4,284 | 1 | TCP 140 | 2 | 1 | TCP 1721 | 2 | |
| TCP 23 | 4,284 | 1 | TCP 140 | 2 | 1 | TCP 1936 | 2 | |
| TCP 24 | 4,284 | 1 | TCP 140 | 2 | 1 | TCP 1938 | 2 | |
| TCP 53 | 4,748 | 2 | TCP 445 | 9 | 1 | TCP 5800 | 2 | |
| TCP 80 | 180,178 | 0 | TCP 445 | 10 | 1 | TCP 5802 | 0 | |
| TCP 81 | 15,187 | 1 | TCP 548 | 2 | 1 | TCP 5808 | 0 | |
| TCP 138 | 13,288 | 0 | TCP 561 | 0 | 0 | TCP 5900 | 0 | |
| TCP 115 | 4,485 | 3 | TCP 995 | 8 | 1 | TCP 9900 | 0 | |

Geo-located Hosts:

Identified Operating Systems:

| OS | External | Internal |
|---------------------------|----------|----------|
| Microsoft Cable Modem | 83% | 83% |
| Microsoft Windows 2000/02 | 12% | 12% |
| Windows L2F Ear Switch | 3% | 3% |
| Other | 13% | 13% |

Identified Service Types:

| Service | External | Internal |
|------------|----------|----------|
| HTTP | 22% | 22% |
| HTTPS | 13% | 13% |
| HTTP Proxy | 17% | 17% |
| Other | 48% | 48% |

For Official Use Only (FOUO) Page | 17

Wireless Vulnerability Findings by Severity:

Scanned Network Findings:

Identified Vulnerabilities by Occurrence and Severity:

3.3.4 Phishing Click Rate

The Wireless Scan section contains statistics such as the number of hosts, types of operating systems and services running on the AGENCY's wireless network.

3.3.5 Phishing Payload

The Wireless Scan section contains statistics such as the number of hosts, types of operating systems and services running on the AGENCY's wireless network.

For Official Use Only (FOUO) Page | 13

3.2.2 Network Vulnerability Scan

The Network Vulnerability Scanning section contains information on the average Common Vulnerability Scoring System (CVSS), number of vulnerabilities by severity level, vulnerability counts by host, and the most at risk hosts. The closer a host's score is to zero, the less risk a system (CVE) or vulnerability (CVSS) holds. The closer to two a system is, the higher the risk.

CVSS Vulnerable Host Score Results:

Identified Vulnerabilities by Severity:

| Detect Vulnerabilities | EXTERNAL Vulnerabilities by Severity | | | | Total Findings |
|------------------------------|--------------------------------------|-----------|------------|-----------|----------------|
| | Critical | High | Medium | Low | |
| Detect Vulnerabilities | 4 | 12 | 30 | 10 | 56 |
| Total Vulnerabilities | 16 | 72 | 105 | 77 | 272 |

| Detect Vulnerabilities | INTERNAL Vulnerabilities by Severity | | | | Total Findings |
|------------------------------|--------------------------------------|-----------|------------|-----------|----------------|
| | Critical | High | Medium | Low | |
| Detect Vulnerabilities | 4 | 12 | 30 | 10 | 56 |
| Total Vulnerabilities | 16 | 72 | 105 | 77 | 272 |

Density of Vulnerabilities Found per Host:

For Official Use Only (FOUO) Page | 8



Cyber Hygiene (CH)

- Overview

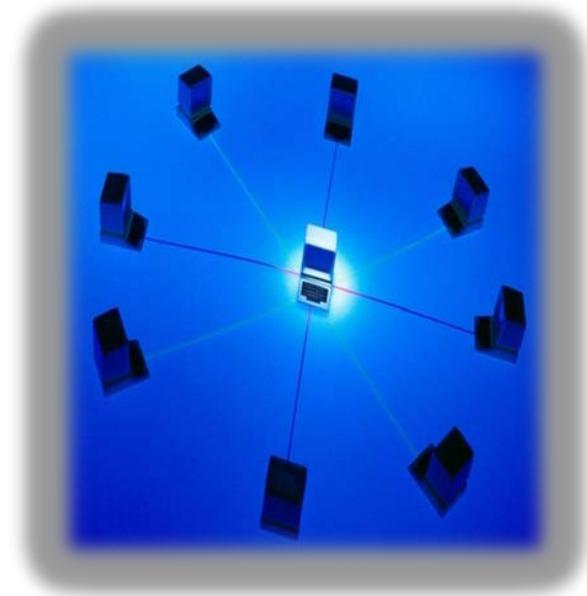
- Cyber Hygiene activities focus on increasing the general health and wellness of the cyber perimeter by broadly **assessing NCCIC stakeholders internet accessible systems for known vulnerabilities and configuration errors** on a **recurring** basis. As potential issues are identified the NCATS team will work with impacted agencies to **proactively mitigate threats and risks** to their systems prior to their exploitation by malicious third parties.
- Agency specific data is for the agency's eyes only

- Objectives

- Establish an enterprise view of the FCEB, SLTT, and critical infrastructure public cybersecurity posture
- Understand how we appear to an attacker

- Benefits

- **Complements** an agency's existing security program and capabilities
- Provides an **objective view** of an agency's public security posture
- **Reduced exposure** to known threats





Cyber Hygiene Activities

Network Mapping

- Identify a Department / Agency's public IP address space
- Identify hosts that are active on IP address space
 - Determine the O/S and Services running on the active hosts
 - Re-run scans to determine any changes on IP address space
- Graphically represent address space/system on geographical map

Network Vulnerability & Configuration Scanning

- Identify network vulnerabilities and weaknesses
- Identify common configuration errors in scanned assets such as
 - Improperly signed Domains (DNSSEC)



CH Sample Report Snapshots

Cyber Hygiene Assessment

Sample Organization
September 28, 2013

National Cybersecurity and Communications Integration Center

For Official Use Only (FOUO)

CYBER HYGIENE REPORT CARD

HIGH LEVEL FINDINGS

| ADDRESSES | HOSTS | SERVICES | VULNERABILITIES |
|-------------------|--------------------|--------------------|--------------------|
| 48 ↔ no change | 18 ↑ 8 increase | 18 ↑ 4 increase | 16 ↓ 8 decrease |

VULNERABILITIES

| CRITICAL | HIGH | MEDIUM | LOW |
|----------------------------|----------------------------|----------------------------|-----------------------------|
| 0 ↔ 0 resolved 0 new | 2 ↔ 0 resolved 0 new | 2 ↓ 8 resolved 0 new | 12 ↔ 2 resolved 2 new |

PREVIOUS REPORT ● resolved **CURRENT REPORT** ● new

ORGANIZATIONAL COMPARISONS

VULNERABLE HOST SCORE

4.0 ↓
1.6 better

OVERALL SCORE

2.2 ↓
2.8 better

For Official Use Only (FOUO)

For Official Use Only (FOUO)

Figure 4: Top Five Services Discovered

Figure 5: Top Five Vulnerabilities by Occurrence

NCAI recommends SAMPLE present the manifestation of the findings in Appendix B. The remainder of this report provides detailed findings, full scan data, agency history, and aggregate related comparisons. The CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. The overall CVSS score represents a calculated average of the CVSS scores for each host and the 'average' of those scores. CVSS scores represent a calculated average of the CVSS scores for each host as identified vulnerabilities. Both scores are reported to the CH Average 7 score. The CH Average scores were compiled using 20,725 data from 28 agency scans as of September 18, 2013 at 04:31 UTC.

Figure 6: CVSS Overall Score Results

Figure 7: CVSS Vulnerable Host Score Results

*Cyber Hygiene scores reported here by context (Cyber Hygiene Score NCAI) has not been validated.

For Official Use Only (FOUO)

For Official Use Only (FOUO)

2 Executive Summary

This report provides the results of a Department of Homeland Security (DHS) National Cybersecurity Assessment and Technical Services (NCAATS) and Cyber Hygiene (CH) assessment of Sample Organization (SAMPLE), conducted from September 18, 2013 at 04:31 UTC through September 18, 2013 at 04:31 UTC. The Cyber Hygiene assessment includes network scanning and vulnerability scanning for internet-accessible SAMPLE hosts. This report is intended to provide SAMPLE with enhanced understanding of their cyber posture and to promote a secure and resilient Information Technology (IT) infrastructure across the Federal government's internet-accessible networks and hosts. For this reporting period, a total of 18 hosts out of a possible 48 addresses were identified. The scan revealed 24 total potential vulnerabilities distributed across 10 (55.6%) of the hosts. A distinct open port, 4 distinct services, and 10 operating systems were observed.

5 distinct types of potential vulnerabilities (2 critical, 1 high, 2 medium, and 2 low) were discovered. SAMPLE should review the vulnerabilities detected and report any false positive back to the NCAATS so they can be excluded from future reports. Please refer to Appendix A for an illustration of the breakdown of vulnerability occurrences over time.

Figure 2: Top Five Risk Based Vulnerabilities

The top five operating systems, services, and vulnerabilities discovered are displayed in Figure 3, Figure 4, and Figure 5 respectively.

Figure 3: Top Five Operating Systems Detected

| Severity | Distinct Vulnerabilities | Total Vulnerabilities |
|----------|--------------------------|-----------------------|
| Critical | 0 | 0 |
| High | 1 | 2 |
| Medium | 2 | 2 |
| Low | 2 | 11 |
| Total | 5 | 16 |

Table 1: Number of Vulnerabilities by Severity Level

Additionally, the top five high-risk hosts and top five vulnerabilities are displayed in Figure 4.

Figure 4: Top Five High-Risk Hosts

For Official Use Only (FOUO)



Questions?

NCATS_INFO@hq.dhs.gov



Homeland Security