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

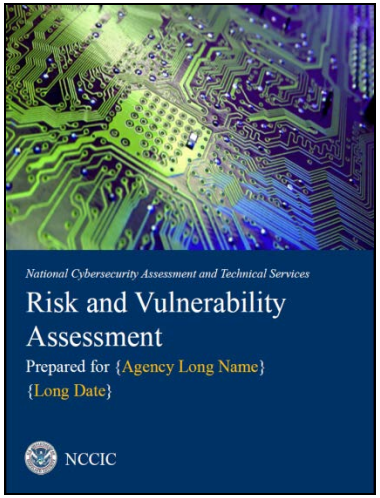
- Draft Report Started/Completed
- Submit Draft Report to Agency
- Receive Draft Report with Agency Comments
- Q&A Process Started/Completed

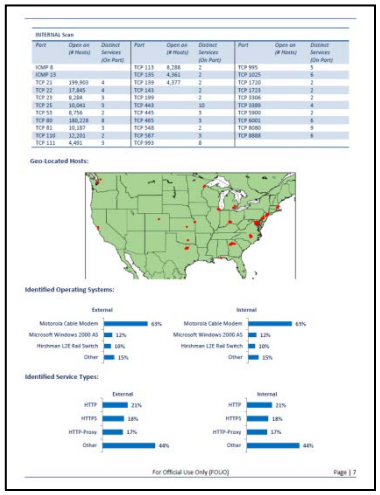
Post Assessment

1 week

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

RVA Report Snapshots





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:

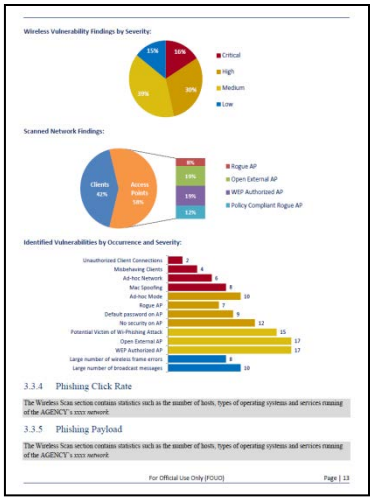
1. Unrestricted Network File System (NFS) Shares – *Four hosts were identified within the internal network environment, which allowed access to the file system via unrestricted NFS shares. While analyzing the files available on the shares, credit card information, and customer personally identifiable 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.*

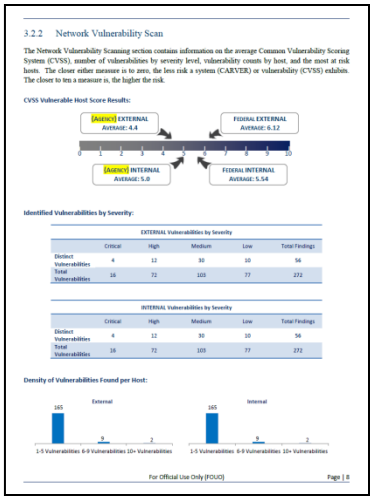
All of the findings were mapped to applicable FISMA controls as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. The chart below illustrates the five most common control families cited based on the number of findings. The complete mapping is included 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





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

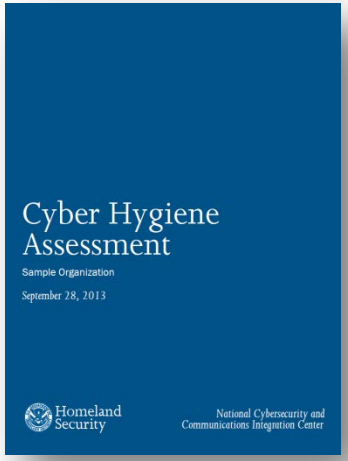
Network Mapping

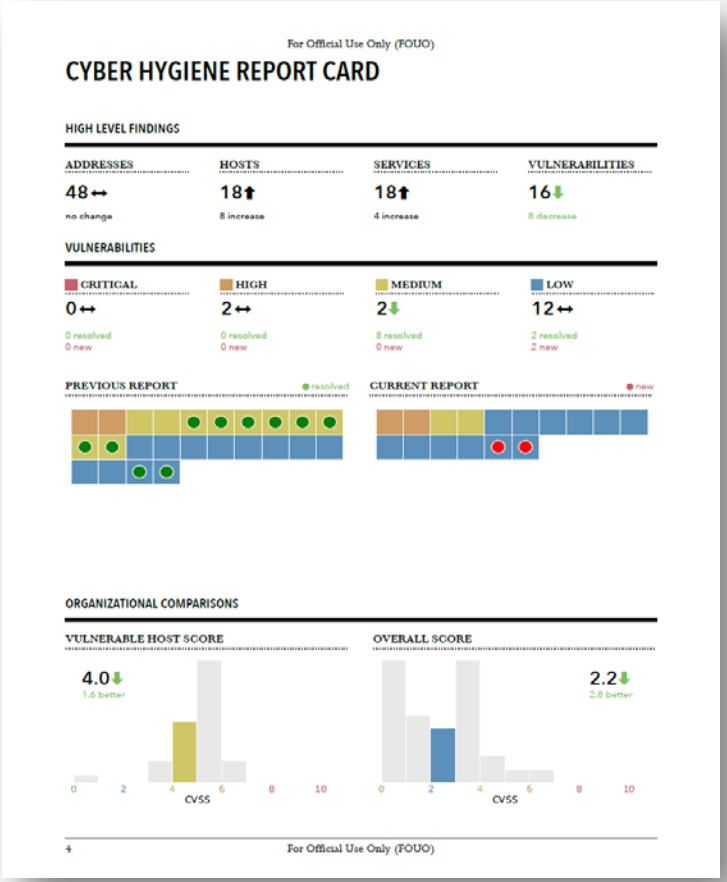
- Identify a Department / Agency's public IP address space
- Identify hosts that are active on IP address space
  - *Determine the O/S and Services running on the active hosts*
  - *Re-run scans to determine any changes on IP address space*
- Graphically represent address space/system on geographical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

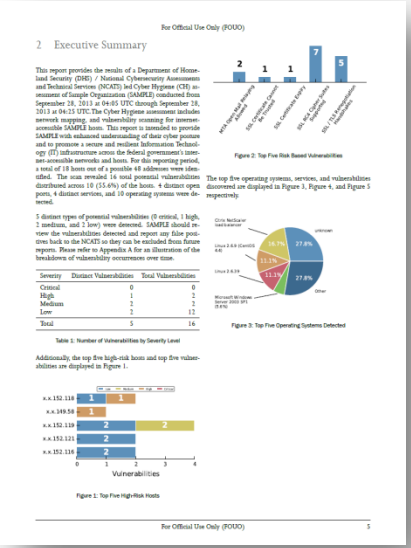
Network Vulnerability & Configuration Scanning

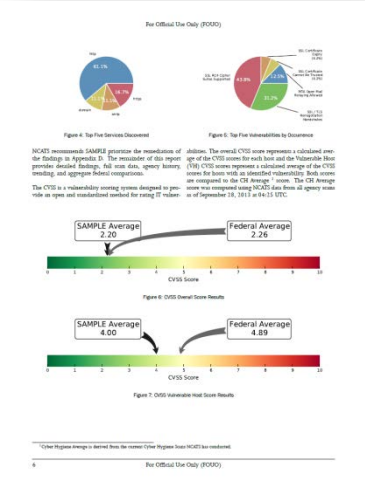
- Identify network vulnerabilities and weaknesses
- Identify common configuration errors in scanned assets such as
  - *Improperly signed Domains (DNSSEC)*

CH Sample Report Snapshots









Questions?

NCATS_INFO@hq.dhs.gov

Homeland Security