National CyberSecurity
& Communications
Integration Center

Department of Homeland Security

National Cybersecurity Assessments & Technical Services (NCATS)

Service Overview, Success and Challenges

3/18/2016

Agenda

- Discussion about NCATS
- Current Programs and Services
  - Cyber Hygiene
  - Risk and Vulnerability Assessments
    - High Value Asset (HVA) Scenarios
- Past Success Stories
- Pilot Services
  - Offensive Security Assessment
  - Phishing Campaign Service
- Current Challenges
- Questions

NCATS Overview

- Offer Full-Scope Red Team/Penetration Testing Capabilities through two primary programs: Risk and Vulnerability Assessment (RVA) and Cyber Hygiene
- Focus is on proactive engagements with stakeholders to improve their cybersecurity posture, limit exposure, reduce rates of exploitation
- Offers a full suite of tailored threat, vulnerability and risk assessment services and penetration testing capabilities to stakeholders
- Acts as a trusted advisor and provides independent review and recommendations for cybersecurity improvement

Stakeholder Groups

- Federal Civilian Executive Branch
- State, Local, Tribal, Territorial Governments (SLTT)
- Private Sector (PS)
- Unclassified / Business Networks
- Cyber Hygiene
  - Mandatory for Federal
  - Optional for SLTT and PS
- Risk and Vulnerability Assessments
  - Optional for Federal, SLTT and PS

FY16 Current Stakeholders

Service	Fed	SLTT	PS	Total
RVA	24	10	12	46
Cyber Hygiene	126	60	59	245

NCCIC

FOR OFFICIAL USE ONLY

RVA Services and Capabilities

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

HVA Testing Scenarios – FY15

- Derived from trending analysis data gathered through:
  - Previous Risk and Vulnerability Assessments
  - Emulation of Known Adversary Tactics, Techniques, and Procedures

Scenario #1: External Assessment (EA) - Determine what vulnerabilities exist in the agency's web presence and publically available hosts that an unauthorized, Internet-based attacker could discover and exploit.

Scenario #2: Phishing Campaign (PC) – Determine how effective a phishing campaign would be against agency employees by using enticing emails to convince users to click on malicious links.

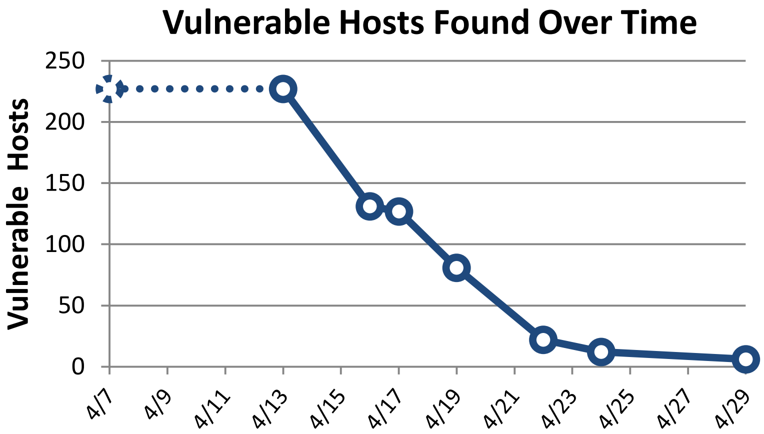
Scenario #3: Web Application Assessment (WAA) – Determine the accessibility of sensitive information through an agency web application by evaluating how the application processes, protects, and stores data submitted by application users.

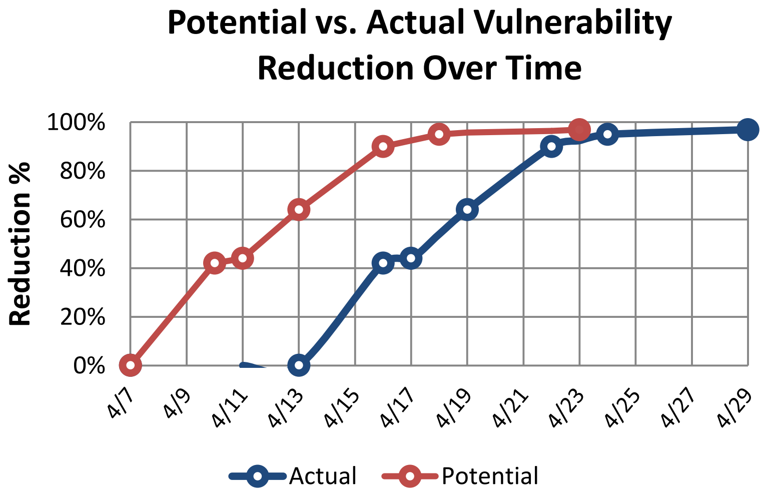
Scenario #4: Internal Assessment (IA) - Determine what vulnerabilities exist within the agency internal network that an attacker with physical access to the network could discover and exploit.

Scenario #5: Internal Threat Emulation (ITE) – Simulate an attacker with assumed internal access, through phishing and other means, navigating the agency network to gain access to core servers, applications, and other sensitive information.

Scenario #6: Data Exfiltration (DE) – Simulate a malicious insider gathering sensitive information and transferring the data outside the internal network.

Success Story: HeartBleed





Notable Observations:

- DHS had the capability to initiate scanning immediately but was delayed due to a lack of authorization
- Observed 98% vulnerability reduction between first and last scan
- Had scanning started April 7th and achieved similar results the length of exposure could have been reduced by 29%

Offensive Security Assessment

- Currently Piloting the Service
  - Limited to Federal Stakeholders
- 90 Day Engagements
  - External Testing Only
    - All Testing Performed from NCCIC Lab
  - Allows for simultaneous engagements
- Goal is to train agencies to identify breaches
  - Monitor, train and track progress
  - True Red Team Capability
  - Measure response and sharing of Indicators of Compromise (IOCs)

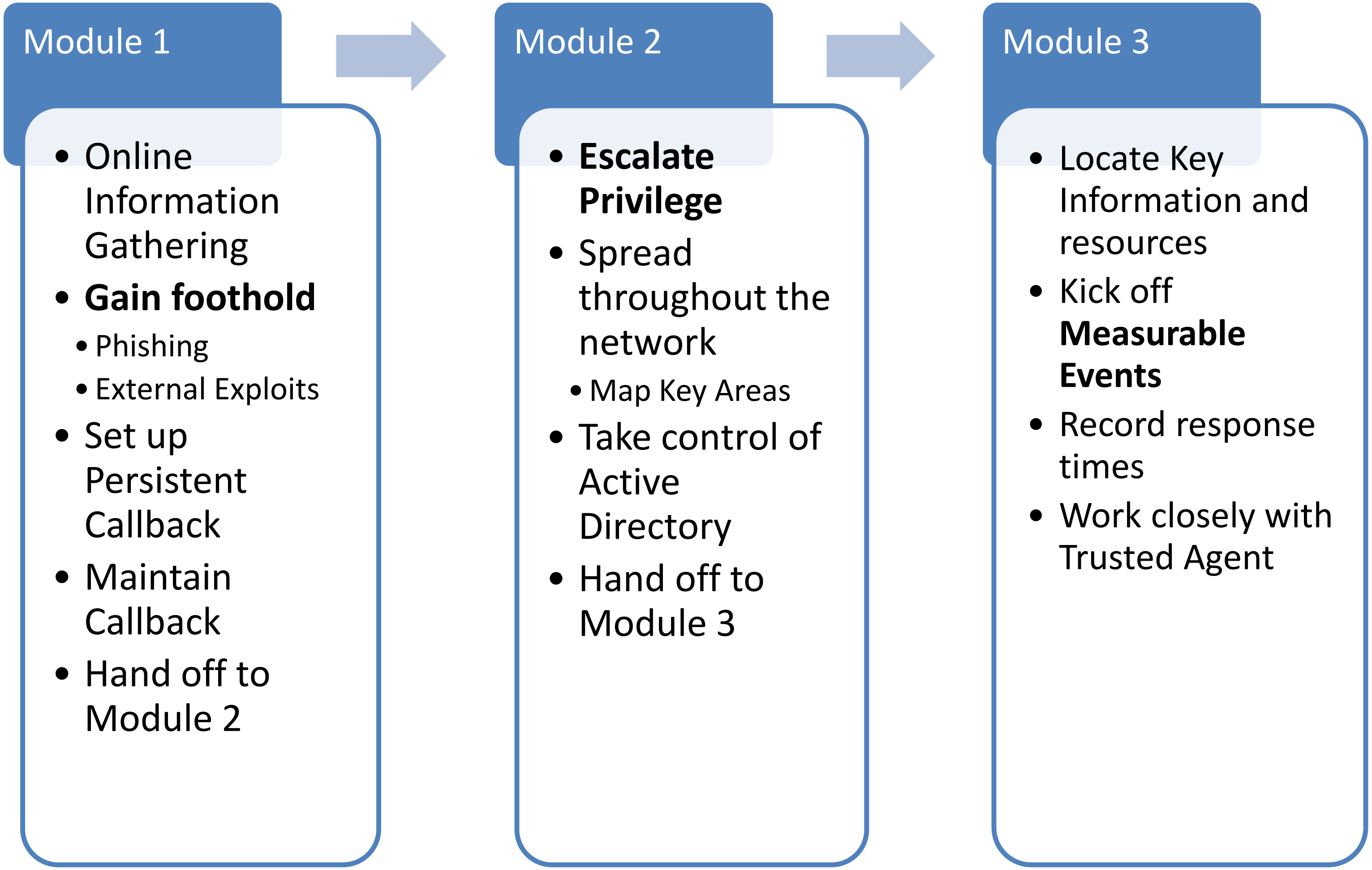
Why OSA?

- Black Box Assessment – Mirrors APT
- Provide security personnel real world examples of being attacked
    - Trains Security Operations Center (SOC) personnel to recognize and respond to threat indicators
- Help identify security holes within an organization
- Track response times of security events across government agencies
    - Master Scenario Event List (MSEL) used to measure response

Team (Module) Concept

- Assembly line like concept
- Breaks up methodology into manageable pieces
- Clear lines of responsibility
- Modular
  - Easy to substitute testers/team members
  - Focused operations

Modules



Module 1

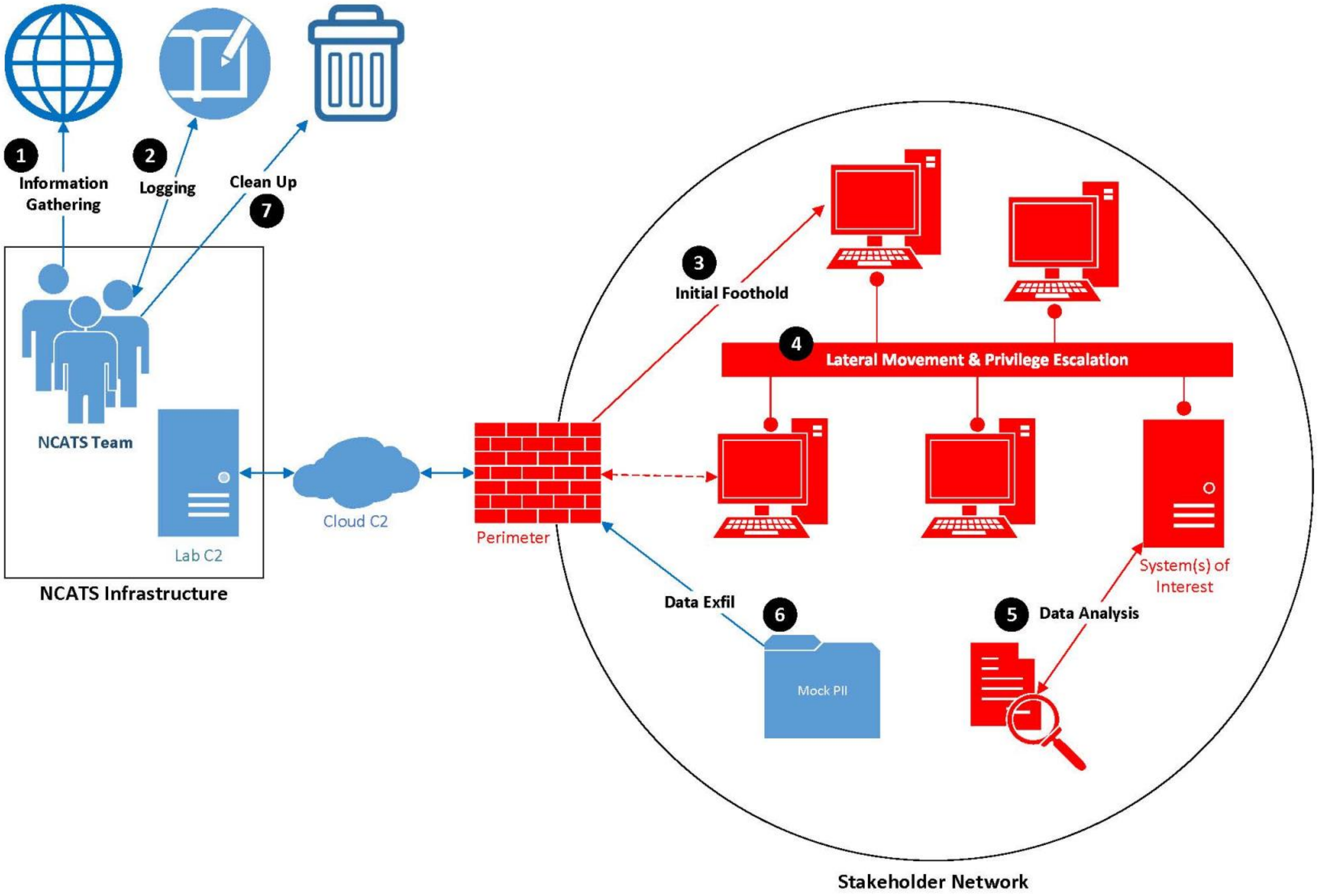
- Online Information Gathering
- **Gain foothold**
  - Phishing
  - External Exploits
- Set up Persistent Callback
- Maintain Callback
- Hand off to Module 2

Module 2

- **Escalate Privilege**
- Spread throughout the network
  - Map Key Areas
- Take control of Active Directory
- Hand off to Module 3

Module 3

- Locate Key Information and resources
- Kick off **Measurable Events**
- Record response times
- Work closely with Trusted Agent


1
Information Gathering
2
Logging
Clean Up
7
NCATS Team
Lab C2
NCATS Infrastructure
Cloud C2
Perimeter
3
Initial Foothold
4
Lateral Movement & Privilege Escalation
System(s) of Interest
Data Exfil
6
Mock PII
5
Data Analysis
Stakeholder Network

Rapid Response

- Test of external system(s) within two (2) business days of request
- Limited scope to include no more than:
  - 5 IP addresses
  - 1 Web Application
- Communications
  - Daily Briefing
  - Draft Report delivered Next Business Day
- Successful Pilot with CFO Act Agency 1st Qtr, FY16

Phishing Campaign Service

- Purpose
  - Most common attack vector used to breach a stakeholder’s environment
- Scope
  - 13-week (90 Day) engagement period
  - Stakeholder provides a reasonable list of target users
  - Phishing emails capture click-rate only, NO payloads
- Objectives
  - Increase security awareness
  - Decrease potential threat of successful attacks
  - Provide meaningful and actionable metrics

PCS Methodology

- **Complexity Levels**: Method for calculating the difficulty to identify indicators of a crafted phishing email
  - Levels 0-10+ (Easy to Difficult)
  - Calculation based on four categories of indicators:
    1. Appearance
    2. Sender
    3. Relevancy
    4. Behavior/Emotion
- **Time Windows**: Varied periods during the day to send crafted phishing emails
  - Monday morning (just before business hours)
  - Tuesday afternoon (lunch hour)
  - Wednesday evening (after business hours)
  - Thursday late (middle of the night)
  - Friday afternoon (just before business hours end)

PCS Complexity Calculator

Phishing E-mail Template Complexity Rating Calculator			
Category	**Indicator**	**Ranking Scale**	**Ranking**
Appearance	Grammar	0=Poor, 1=Decent, 2=Good	
	Link Domain	0=Fake, 1=Impersonated	
	Logo/Graphics	0=Fake, 1=Impersonated	
Sender	External	0=Fake, 1=Impersonated	
	Internal	0=Fake, 1=Impersonated	
	Authoritative	0=Fake, 1=Corporate, 2=Federal	
Relevancy	Organization	0=No, 1=Yes	
	Public News	0=No, 1=Yes	
Behavior (Optional)	Fear	0=No, 1=Yes	
	Pride or Shame	0=No, 1=Yes	
	Greed	0=No, 1=Yes	
		Total	

Sample Phishing Email

To: <Stakeholder List>
From: Apples Customer Relations <freeapplesforyou@gmail.com>
Subject: Free iPad – Just Complete a Survey!

Want the new iPad or iPad Mini? I got mine free from this site: <newtechnologyforfree.apples.biz> !!!!!

We would like to invite you to be part of a brand new pilot program to get our new product in the hands of users before official release. This assures that any issues or errors are mitigated before the release. If you are accept to participate in this program all we ask is that you submit a survey at the end of the Pilot. You be able to keep iPad at the end for free!

Apples Customer Relationships Office
Apples Campus, Cupertino, California 95114

1

PCS Metrics

- User Based
  - %Clicked – Are employees falling for the phishing email?
  - %Reported – Are employees alerting security regarding suspicious emails?
- System Based
  - %Browser – What browser software and version are employees using by default?
  - %Mobile – Are employees opening email on their mobile devices?
- Time Based
  - Time until first click
  - Time until first user reporting and/or security response
- Training and Awareness Effectiveness
  - %Clicked delta between Round 1 and Round 2
  - %Complete - Are employees acknowledging and completing security awareness training?

Current Challenges

Questions?

For more information:
NCATS_info@hq.dhs.gov

Backup Slides

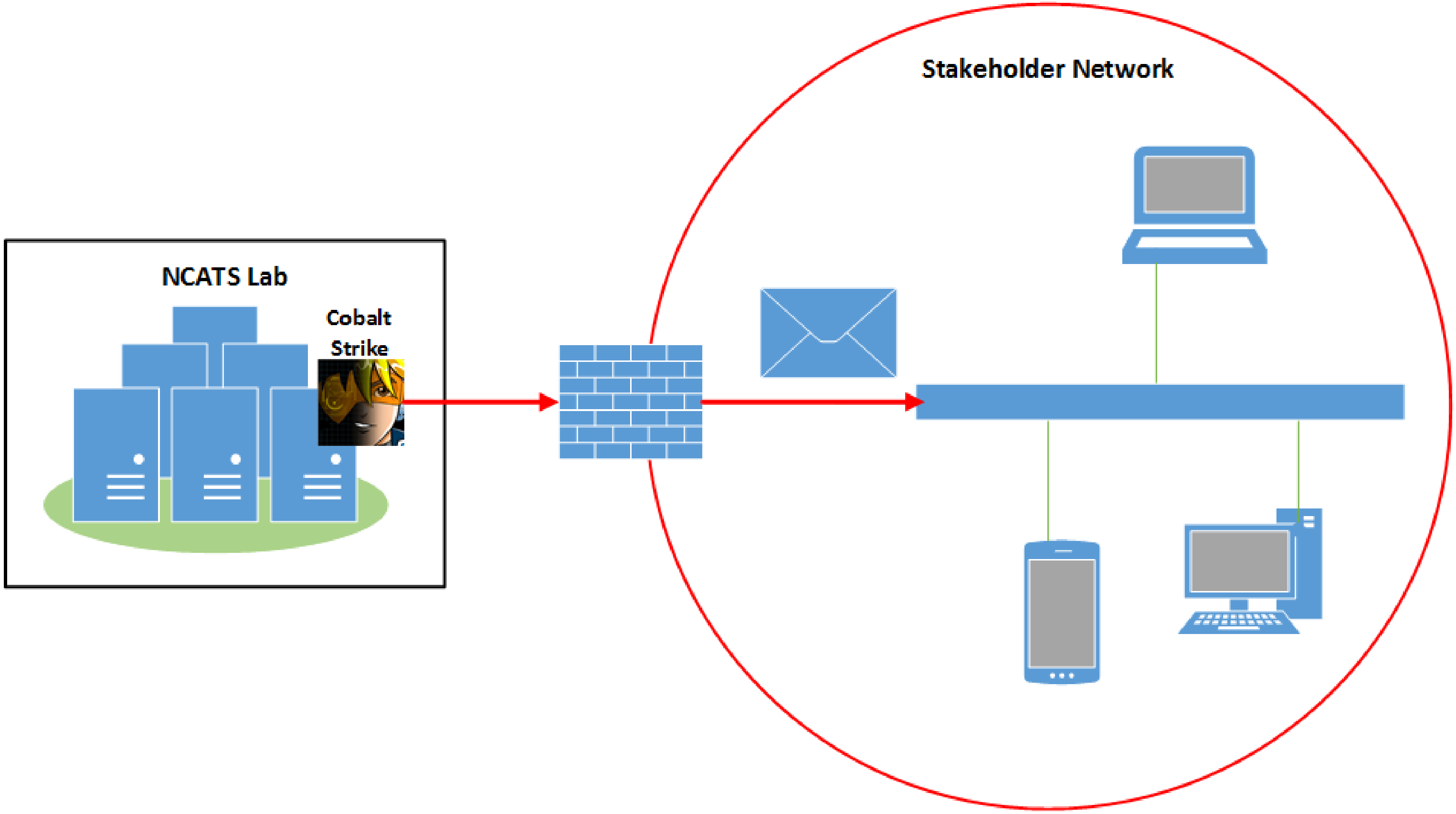
RVA Service Examples

Service	Example	Impact	Mitigation
Network Scanning	Stakeholder believed they had 800 hosts, scan revealed over 7,000	Flat network, person in region 1 can access all machines in region 8	Segment network with router or firewall rules
Penetration Test	Discovered over 200 security cameras accessible with default credentials	Physical security, theft, watching key strokes of users	Change default credentials and add network level filters
Application Test	SQL Injection- successfully crafted and input a data string that enumerated web application usernames and passwords. Used credentials to log into web application and other devices	Unauthorized user access was achieved from the internet	Sanitize all input provided by an untrusted source. Implement server-side controls of white-listed character sets. Encrypt data stored on the database
Penetration Test	Discovered an application that had login credentials for user 'admin' cached. This allowed for administrative access on the active directory.	Loss of confidentiality. Anyone on the network could potentially become the Domain Admin	Restrict Access to the application and if possible turn off caching on the application
Wireless Test	Discovered WAP buried underneath paper/trash/debris and plugged into the Local Area Network	Security controls implemented to connected to the LAN are bypassed. Anyone at Starbucks next door could have access	Monitor network for rogue devices, conduct periodic walk-throughs to identify rogue devices
Phishing Campaign	Phishing email sent to a limited number of employees. One employee, forward to the entire agency	All machines were potentially compromised or had to be cleaned. IT resources allocated to mitigation and clean up	Train users to identify malicious email, implement technical controls.
Application Testing	Password reset function allowed the reset password to be mailed to any email address	Anyone could reset an account and log into the application. This logic flaw impacted Confidentiality, Availability and Integrity	Ensure passwords can only be reset by the actual account owner and sent to the email address on record for the account owner

Cyber Hygiene Activities

Scanning	Past and Present Use
• Identify • *Active hosts, Operating System and Services* • *Vulnerabilities and weaknesses* • *Common configuration errors* • *Improperly signed Domains* • *Expired SSL Certificates* • Understand how external systems and infrastructure appear to potential attackers	• Federal Response to Heartbleed • OMB: M-15-01 • *Identification of publicly available vulnerabilities* • DHS Binding Operational Directive • Individual Stakeholder persistent scans and exposure status • *2800+ Reports delivered this Fiscal Year* • *185 Stakeholders and growing*

Initial PCS Infrastructure



PCS Timeline

Week	Action	Dependency
-2	Initial coordinate of scope, plan, pre-assessment information gathering, template creation, and rules of engagement	Stakeholder agrees to service activities
-1	Test templates created and tweak for use in campaign	Feedback from stakeholder POCs
1	Launch Level 0-1 phishing	Complete pre-assessment
2	Launch Level 2-3 phishing	Complete previous phishing
3	Launch Level 4-5 phishing	Complete previous phishing
4	Launch Level 6-7 phishing	Complete previous phishing
5	Launch Level 8-9 phishing	Complete previous phishing
6	Launch Level 10+ phishing	Complete previous phishing
7	Stakeholder Phishing Awareness Action Briefing of initial Round 1 findings and assistance with awareness action	Development of stakeholder specific materials or implementation of default materials
8	Launch Level 0-1 phishing	Complete awareness action
9	Launch Level 2-3 phishing	Complete previous phishing
10	Launch Level 4-5 phishing	Complete previous phishing
11	Launch Level 6-7 phishing	Complete previous phishing
12	Launch Level 8-9 phishing	Complete previous phishing
13	Launch Level 10+ phishing	Complete previous phishing
+1	Closing brief of initial Round 2 findings compared to Round 1 pre-awareness action	Completion of all phishing and collection of all metrics
+2	Completed report of findings, and recommendations for awareness and security best practices	Stakeholder satisfaction with campaign and metrics discussed in closing brief