COALFIRE LABS

PENETRATION TEST

RULES OF ENGAGEMENT

Prepared for:

Andrew Shirley
Information Security Officer
Iowa Judicial Branch
1111 East Court Avenue
Des Moines, IA. 50319
515-348-4773
Andrew.Shirley@IowaCourts.gov

Prepared by:

Dana Mortaro
Project Manager
Coalfire Systems, Inc.
11000 Westmoor Circle, Suite 450
Westminster, Colorado 80021

Date

7/30/2019

Version

1.0

Service Order

[redacted]CIS[redacted]

Disclosure Statement:

This document contains sensitive information about the computer security environment, practices, and current vulnerabilities and weaknesses for the client security infrastructure as well as proprietary tools and methodologies from Coalfire. Reproduction or distribution of this document must be approved by the client or Coalfire. This document is subject to the terms and conditions of a non-disclosure agreement between Coalfire and the Client.

TABLE OF CONTENTS

PROJECT DESCRIPTION AND OVERVIEW

Coalfire is under contract with Iowa Judicial Branch to deliver a penetration test ("the project") in accordance with Service Order [redacted]ICIS[redacted] This Rules of Engagement (ROE) document serves as a test plan and outlines the project activities from the Service Order, confirms project schedules, identifies project staff, and defines scope details and deliverable expectations. With this ROE, Coalfire's intent is to ensure a successful execution of all project activities.

PURPOSE

The penetration test and corresponding risk assessment will be performed by Coalfire to test the adequacy and effectiveness of security control measures in place to protect the security and integrity of sensitive information technology (IT) systems and data.

The test results from this engagement will be used to identify risks and vulnerabilities Iowa Judicial Branch systems, and evaluate the effectiveness of security configuration settings, policies and procedures, and existing technical controls in regards to the Iowa Judicial Branch's management of the components under its operation and control. This information will be provided to Iowa Judicial Branch's senior management and stakeholders, in the form of a Penetration Test Summary Report, to allow them to make an informed risk-based decision for the implementation of applicable applications, networks, and infrastructure. The report will also provide Iowa Judicial Branch with a list of identified risks and recommended remediation actions to help improve overall system security. Moreover, the report will provide valuable information on potential effects to the confidentiality, integrity, and availability of Iowa Judicial Branch data and system resources.

This ROE establishes the guidelines followed by Coalfire personnel during the assessment and defines the test plan, including methodology and testing activities. This allows Coalfire to perform testing in a manner that minimizes impact on operations while maximizing the usefulness of the results. This ROE is submitted for review and approval by Iowa Judicial Branch's management and stakeholders prior to execution of testing.

Specific project drivers include, among others:

- □ PCI DSS compliance (Report on Compliance, SAQ, etc.)
- □ Healthcare compliance (HIPAA/HITRUST)
- □ Financial Services compliance (FFIEC, GLBA, etc.)
- □ Federal/Public Sector compliance (FISMA, FedRAMP, etc.)
- □ SOC
- □ Utilities/SCADA/NERC/CIP
- ☒ Security Best Practices

SCOPE OF TESTING

The specific project activities defined in the Service Order and covered by this ROE include:

- External network penetration test (*see appendix 1.0*)
    - Up to 200 IP's
- Internal network penetration test (*see appendix 2.0*)
    - If no access can be gained during the external/social engineering activities after one week, we'll move to an assumed breach attack.
        - Drone, VM, payload?
- Application penetration test (*see appendix 3.0*)
    - Total of three (3) smaller internal web applications
    - Smaller to moderate complexity
- Social engineering activities: (*see appendix 4.0*)
    - Spear Phishing
        - Target ICIS employees
    - Pre-text phone calling
        - Target ICIS employees
    - Physical security assessment
        - Attempt to gain physical documentation at three locations
            - Polk County Courthouse
                - 500 Mulberry Street, Des Moines, IA. 50309
                - More security here
            - Judicial Branch Building
                - 1111 E. Court Ave, Des Moines, IA 50319
            - Dallas County Courthouse
                - 801 Court Street, Adel, IA. 50003
        - Can be during the day and evening
        - Talk your way into areas, limited physical bypass
        - Attempt to physically gain internal network access
        - Attempt to gain network access to facilitate persistent access
        - Coalfire will leave behind malicious devices, such as thumb drives, network devices
- Wireless vulnerability assessment (*see appendix 6.0*)
    - One (1) location, 500 Mulberry Street, Des Moines, IA. 50309
    - On-site
    - 2 SSID's

NO TESTING TO OCCUR ON 9/4 (Wednesday), 9/18 (Wednesday), or 9/19 (Thursday)

On 9/4, 9/18 and 9/19 the Supreme Court will be conducting business and we cannot interrupt it. The Appeals Court is conducting business on 9/3 - 9/5 and we cannot interrupt it either.

PROJECT SCHEDULE OF ACTIVITIES

Assessment activities will be conducted as described in Coalfire's Service Order. The following table serves to establish dates for key meetings, activities, and deliverables.

ACTIVITY		SCHEDULE*
Project Planning, ROE, and Test Plan ◦ Review documentation and align team to project scope and deliverables. Set a preliminary schedule and establish a communication plan. Confirm required document/information requests.		8/1/2019
RFI Due Date		8/12/2019
Pre-Project Checkpoint #1 ◦ Schedule re-confirmed. ◦ Communications plan re-confirmed. ◦ Discuss outstanding items related to connectivity, access, and execution logistics.		8/22/2019 (Target minimum 2 weeks prior to scheduled start.)
TESTING TIMELINE	**START DATE**	**EXPECTED CONCLUSION**
Application Penetration Test	8/19/2019	8/30/2019
External Network Penetration Test	8/26/2019	9/6/2019
Phishing	8/26/2019	9/6/2019
Pre-Text Calling	8/26/2019	9/6/2019
Social/Physical Assessment	9/9/2019	9/13/2019
Wireless Assessment	9/9/2019	9/13/2019
Internal Penetration Test ***No testing 9/18 or 9/19***	9/16/2019	9/27/2019
REPORTING		
Physical debrief in person		9/13/2019
Draft Report Available		10/11/2019
Final Deliverable		10/18/2019
Debrief Meeting		TBD
Remediation Check Point		TBD

NOTE: Once Coalfire and Iowa Judicial Branch agree on the schedule defined above and this ROE is signed, any changes to the schedule may result in additional fees per the terms of the Iowa Judicial Branch MSA. Please review your MSA to become familiar with the specific terms of your agreement with Coalfire.

PROJECT LOGISTICS

COALFIRE LABS TEAM			
Name	Email	Phone	Role
Joe Neumann	Joseph.Neumann@Coalfire.com	O: 703-429-2501 [redacted]	Project Director
Dana Mortaro	Dana.Mortaro@Coalfire.com	O: 720-251-4165 [redacted]	Project Manager
Gary De Mercurio	Gary.DeMercurio@Coalfire.com	O: 206-673-3043 [redacted]	Penetration Tester *Physical*
Justin Wynn	Justin.Wynn@Coalfire.com	O: 720-545-2424 [redacted]	Penetration Tester *Red Team*
Jake Nelson	Jakob.Nelson2@Coalfire.com	O: 303-872-8647 [redacted]	Penetration Tester *Wireless*

IOWA JUDICIAL BRANCH TEAM					
Name	Email	Phone	Role	Communication Level	
				Daily Emails	Report
Andrew Shirley **Error! Reference source not found.**	Andrew.Shirley@IowaCourts.gov	515-348-4773	Primary POC Info Sec Officer	☒	☒
Mark Headlee	Mark.Headlee@IowaCourts.gov	515-348-4823	Director/CIO	☐	☐
John Hoover	John.Hoover@IowaCourts.gov			☒	☒

ASSUMPTIONS AND LIMITATIONS

Project Planning

- Coalfire and Iowa Judicial Branch will confirm that the agreed-upon schedule outlined in this ROE works for both parties. Iowa Judicial Branch must complete the necessary sections required for testing and Coalfire will adhere to the outlined schedule. Client delays and/or inaccurate information can lead to delays in testing execution and final report delivery.
- The request for information (RFI) section of this ROE must be completed in full and returned on or prior to the date listed in the defined schedule below. Non-compliance may adversely affect scheduling of project activities.
- This ROE, which includes the test plan, must be signed and approved prior to the execution of the penetration test and by the agreed-upon due date.
- During execution, status calls will be conducted and/or emails exchanged with the Iowa Judicial Branch stakeholders to provide a summary of the activities to occur for the testing period or as needed.
- An agreed-upon timeframe is required to allow the test team to complete the report prior to the first draft submission to Iowa Judicial Branch stakeholders.
- Once the schedule defined above is confirmed, any changes to it may result in additional fees per the terms of the Iowa Judicial Branch Master Services Agreement (MSA). Iowa Judicial Branch is expected to review and be familiar with the terms of the MSA with Coalfire.

Project Schedule

- All penetration testing is expected to be conducted:
  - During normal business hours: Monday through Friday between the hours of 6AM and 6PM Mountain time. **NOTE: Requests for testing outside of the above approved time periods may result in additional charges per the terms of the MSA.**

Scope Assumptions and Test Process

- A preliminary vetting process will be conducted with Iowa Judicial Branch prior to test plan execution to ensure that the necessary preparation has been made and to ensure that the client is ready for the penetration test. All access and logistical issues will be addressed and planned for accordingly.
- Coalfire Labs has worked closely with the Coalfire sales team to gather specific scope information for this project. If significant differences in the scope of testing are identified either in the completed RFI or during testing, a change order may be required to cover the level of effort required for testing the scope delta.

Reporting

- Coalfire will provide one (1) comprehensive report at the end of this engagement. Please include an Executive Summary.
- The report deliverable will include the following high-level information in a format suitable for management:
  - Purpose of the engagement including project's scope and approach/methodology.
  - Positive security controls that were identified, as appropriate.
  - Tactical recommendations to reduce the risk in the environment in the immediate term, including technical descriptions for mitigating specific vulnerabilities.

- Strategic recommendations for preventing similar issues from recurring and for improving the client's overall security posture.
- Technical description and classification of each significant vulnerability.
- Anatomy of exploitation (i.e., "kill chain") including steps taken and evidence in support of exploitation (i.e., screenshots, etc.).
- Vulnerability classification that describes the severity ranking as a function of vulnerability impact and ease of exploitation.

- The report must describe a threat scenario, likelihood, and impact for each vulnerability discovered.

  Once the draft report is submitted and reviewed, Iowa Judicial Branch can begin the remediation process.

SECURE DOCUMENT SHARING – PROJECT PORTAL

Project team members recognize that assessment activities and communications, including notes, draft documents, email, and other forms of communication are sensitive and should be treated accordingly under a need-to-know concept. To facilitate project management activities and communications, including document retention and destruction, project team members will use the CoalfireOne project portal accessible at:

https://one.coalfire.com/

Portal access rights are developed based on authority granted by Iowa Judicial Branch**Error! Reference source not found.**. Project documents should not be exchanged via email, but rather uploaded/retrieved through the portal. Care should be taken to protect sensitive information when using email.

If a team member does not have an account created for the portal, please have the Project POC contact the Coalfire project manager and they will assist with setting up an account.

INTERNAL TESTING - CONNECTIVITY OPTIONS

There are a few different options we can pursue to perform the internal network testing. Remote solutions help save costs and allow for quicker connectivity, assuming the appropriate setup. Potential solutions include:

1. Coalfire Drone Appliance ***(Coalfire preferred method)***
   - Physical device available to be shipped to the client site
   - Egress 443 required for connectivity
2. Virtual Machine (VM)
   - Virtual drone available to be built for client virtual environment
   - See the RFI section below for additional RFI items related to virtual drone configuration
   - Final download instructions for VM will be provided once the ROE is finalized

NOTE: Hardware drone must be returned to Coalfire within four (4) weeks of completion of testing. Exceptions may be made if remediation activities are completed within one (1) week of testing completion and remediation testing is required. The hardware drone must be returned to Coalfire if remediation testing is expected to occur greater than four (4) weeks following the completion of testing. ***Hardware drones not returned to Coalfire are subject to a $1,500 hardware/service charge.***

REQUEST FOR INFORMATION (RFI)

RFI Due Date: 8/12/2019

NOTE: Not completing by due date above may impact the overall timeline of this engagement.

EMERGENCY CONTACT INFORMATION	
Provide contact and escalation information for communications during testing, including names, titles, phone numbers, and email addresses.	Andrew Shirley, ISO Office: 515-3484773 [redacted] Andrew.shirley@iowacourts.gov Mark Headlee, CIO/Director Office: 515-348-4823 [redacted] Mark.headlee@iowacourts.gov John Hoover, IT Management – Infractructure Office: 515-348-4777 [redacted] John.hoover@iowacourts.gov

INFORMATION REQUIRED FOR THE APPLICATION PENETRATION TEST	
What is the application name?	
What is the application URL?	
What language is the application written in (ASP, PHP, Java, etc.)?	
Is this a Cloud Hosted Site?	
Cloud Provider?	
Have you submitted a Testing Request with the Provider?	
Is a web application firewall (WAF) being utilized?	
If "YES", will the WAF be disabled during testing or will you whitelist our IP's?	
What is the backend database, if applicable (MySQL, Microsoft SQL, Oracle, etc.)?	
Are you using Cloud Service Provided Databases (Azure SQL, AWS Database)?	
Is the application static or dynamic?	
What are the application login credentials, if required?	
Does the application have multiple Roles (unauthenticated, user, admin, manager)?	
Is the site hosted on a shared platform with other sites?	
Is the site load balanced?	
Roughly how many pages and parameters are employed within the site?	
Are Administrators or Developers notified of errors via email?	

INFORMATION REQUIRED FOR THE APPLICATION PENETRATION TEST
What is the application name?
What is the application URL?
What language is the application written in (ASP, PHP, Java, etc.)?
Is this a Cloud Hosted Site?
Cloud Provider?
Have you submitted a Testing Request with the Provider?
Is a web application firewall (WAF) being utilized?
If "YES", will the WAF be disabled during testing or will you whitelist our IP's?
What is the backend database, if applicable (MySQL, Microsoft SQL, Oracle, etc.)?
Are you using Cloud Service Provided Databases (Azure SQL, AWS Database)?
Is the application static or dynamic?
What are the application login credentials, if required?
Does the application have multiple Roles (unauthenticated, user, admin, manager)?
Is the site hosted on a shared platform with other sites?
Is the site load balanced?
Roughly how many pages and parameters are employed within the site?
Are Administrators or Developers notified of errors via email?

INFORMATION REQUIRED FOR THE APPLICATION PENETRATION TEST	
What is the application name?	
What is the application URL?	
What language is the application written in (ASP, PHP, Java, etc.)?	
Is this a Cloud Hosted Site?	
Cloud Provider?	
Have you submitted a Testing Request with the Provider?	
Is a web application firewall (WAF) being utilized?	
If "YES", will the WAF be disabled during testing or will you whitelist our IP's?	
What is the backend database, if applicable (MySQL, Microsoft SQL, Oracle, etc.)?	
Are you using Cloud Service Provided Databases (Azure SQL, AWS Database)?	
Is the application static or dynamic?	
What are the application login credentials, if required?	
Does the application have multiple Roles (unauthenticated, user, admin, manager)?	
Is the site hosted on a shared platform with other sites?	
Is the site load balanced?	
Roughly how many pages and parameters are employed within the site?	
Are Administrators or Developers notified of errors via email?	

INFORMATION REQUIRED FOR THE PHYSICAL SECURITY ASSESSMENT	
How many target locations are in scope for the physical security assessment?	3
In a prioritized listing, please provide the physical addresses of the facilities where physical security assessment is to be performed.	JB Building 1111 E. Court Ave Des Moines, IA 50319 Polk County 500 Mulberry St Des Moines, IA 50309 Dallas County 801 Court St Adel, IA 50003 Juvenile Justice 222 5th Avenue 50309 Criminal Court Area 206 6th Avenue 50309
Does Coalfire have permission to tail-gate, that is, attempt to gain physical access to your facilities by following employees into the building?	Yes
Does Coalfire have permission to dumpster dive, that is, search through garbage cans and/or dumpsters on your property for sensitive information?	Yes
Does Coalfire have permission to access all areas inside the building(s)? If not, please list areas where access in not permitted.	JB Building, floors 3 & 4 no access **3 & 4 are out of scope period. May show proof of concept to access it.**
If physical access is gained to your facility, does Coalfire have permission to attempt logical access to the network, including plugging into a conference room or office Ethernet jack, attempting to join the network, and then attempting further reconnaissance (ping sweep) activities?	Yes
Does Coalfire have permission to perform lock-picking activities to attempt to gain access to locked areas?	Yes
Does Coalfire have permission to strategically place hardware (USB drives, mice, keyboards, netbooks) around the building?	Yes
Does your company use proximity readers with access cards, badges or key fobs? If so, can you specify the technology? (Vendor make and model and card type?)	[redacted]
Does your network use DHCP or static IP addressing?	DHCP
Is egress filtering employed on the network? If so, please provide allowed outbound ports. 80,443,53 etc.	[redacted]
Do you employ any physically armed personnel at the location(s) that will be tested?	[redacted]

INFORMATION REQUIRED FOR THE PHYSICAL SECURITY ASSESSMENT	
	[redacted]
Do you have 24/7 surveillance monitoring in place at the locations to be tested?	[redacted]
Are any facilities or areas of buildings or the office complex to be excluded? If so, please list here and provide reasoning for exclusion.	[redacted]
Will local law enforcement or security personnel be notified that a penetration test is taking place on the specified dates?	No
What assets or areas inside the target location are of most concern in regard to physical access?	Computer Room Switch Closets

INFORMATION REQUIRED FOR THE EXTERNAL NETWORK PENETRATION TEST	
If systems are hosted outside the client managed network, please specify which hosting/cloud provider hosts these systems.	
Have you received authorization for testing from the provider?	Yes
How many external IP addresses are in scope for testing?	
List the external IP ranges in scope for testing.	[redacted]
Are all systems being tested located within a client managed network?	
Are perimeter/edge security controls configured to block known scans and attacks?	[redacted]
If "YES" to the above, will these controls be temporarily altered to fully test the target systems?	
Are any targets to be excluded? If so, please list targets and provide reasoning for exclusion.	None

INFORMATION REQUIRED FOR THE INTERNAL NETWORK PENETRATION TEST	
List the internal network subnets in scope for testing.	
If systems are hosted outside the client managed network, please specify which hosting/cloud provider hosts these systems.	
Have you received authorization for testing from the provider?	
How many internal IP addresses are in scope for testing?	
List the internal IP addresses in scope for testing.	
Can a hardware or virtual drone be utilized to access the internal network? See "Drone/VM Info Required" below.	
Are internal network security controls configured to block known scans and attacks?	
If "YES" to the above, will these controls be temporarily altered to fully test the target systems? Note: It is recommended to fully test in scope systems on the internal network(s).	
Are any targets to be excluded? If so, please list targets and provide reasoning for exclusion.	None

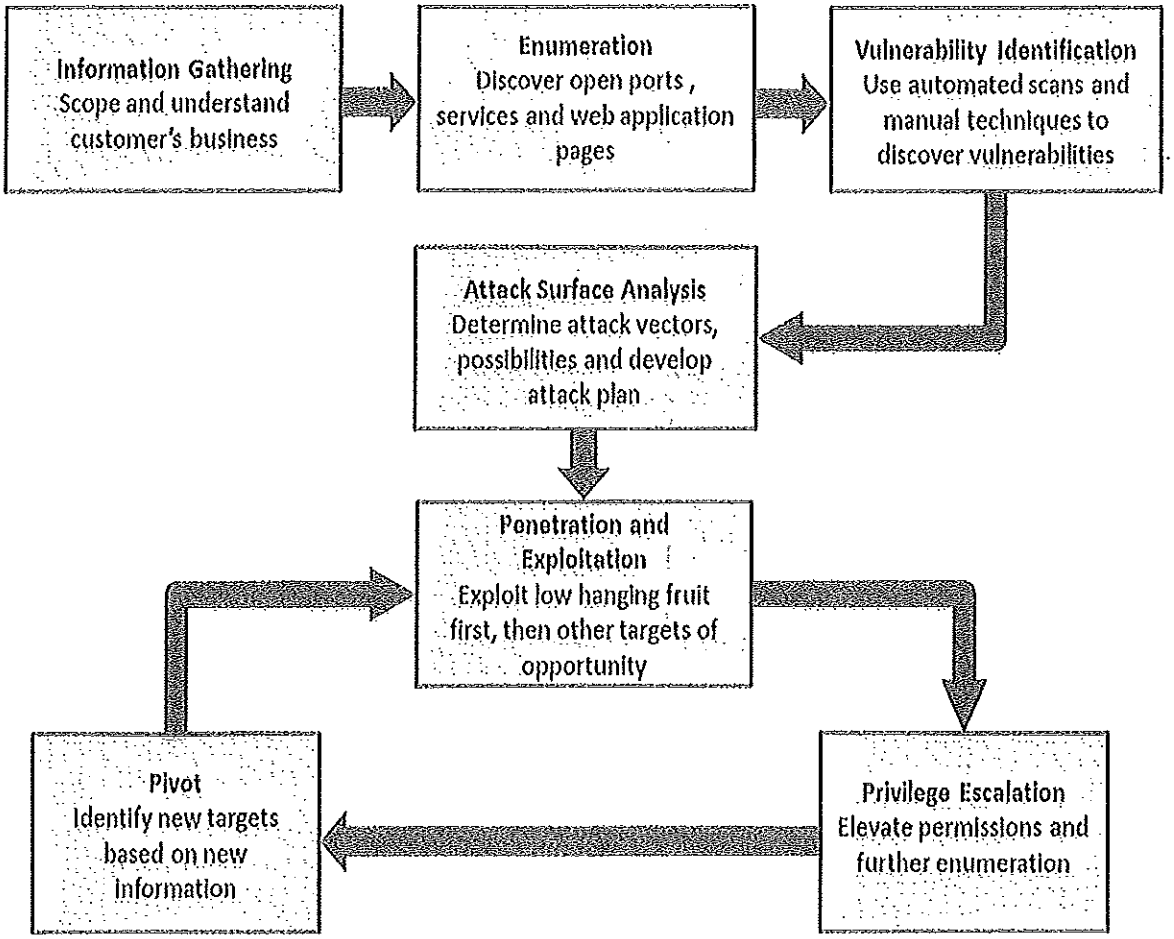
INFORMATION REQUIRED FOR THE WIRELESS ASSESSMENT	
At how many locations is wireless testing be performed?	
Please provide the physical addresses of the facilities in scope for wireless security testing.	
Please provide the approved SSIDs for the company's wireless access points.	
Technologies in use? WPA, WPA2 – PSK or EAP? Are all accessible over 2.4GHz or some exclusive to 5GHz?	
Is there any Wireless Intrusion Prevention Systems, Network Access Control (NAC) or Rogue AP detection in use?	

INFORMATION REQUIRED FOR THE WIRELESS ASSESSMENT	
Are any SSIDs/wireless access points to be excluded? If so, please list here and provide reasoning for exclusion.	County Wi-Fi

INFORMATION REQUIRED FOR SPEAR PHISHING	
Provide the date and time to send spear phishing emails.	
What is the duration of the campaign (i.e., 72 hours)?	
List the email addresses in scope for this assessment. (These may be provided separately.)	Will provide
Coalfire can craft the email and corresponding linked website to appear as if it was originated from an HR department or IT department. Is there a preference for either scenario?	
Based upon the source described above (i.e., HR or IT), please describe that department, including how it is staffed and how communication between these departments and your employees typically occurs.	
Please describe, at a high-level, your network infrastructure (e.g. We are a Windows shop and use Active Directory for authentication. We have X workstations on the network that run Windows XP and 7. We have a web server in a DMZ that hosts our website.).	
Are any spear phishing targets to be excluded? If so, please list here and provide reasoning for exclusion.	None

INFORMATION REQUIRED FOR THE PRE-TEXT PHONE CALLING	
How many target employees are in scope for the pre-texting exercise?	20 to 25, different departments
What is the preferred date and time to place phone calls? (You may provide a date range.)	Okay to do during blackout dates
Please provide the first and last name, title, role, and phone number to call for each employee in scope to receive a pre-text phone call.	
We will create a "back-story" for the pre-text calling and confirm this with you before engaging. However, if you have a specific scenario that you would like us to include in our pre-text to make it more believable, please provide a description of that here.	[redacted]
Are any pre-text calling targets to be excluded? If so, please list targets and provide reasoning for exclusion.	None

PENETRATION TESTING METHODOLOGY



Information Gathering
Scope and understand customer's business

Enumeration
Discover open ports , services and web application pages

Vulnerability Identification
Use automated scans and manual techniques to discover vulnerabilities

Attack Surface Analysis
Determine attack vectors, possibilities and develop attack plan

Penetration and Exploitation
Exploit low hanging fruit first, then other targets of opportunity

Privilege Escalation
Elevate permissions and further enumeration

Pivot
Identify new targets based on new information

CUSTOMER SATISFACTION AND REFERENCES

Coalfire is committed to meeting the objectives of the project and ensuring Iowa Judicial Branch's satisfaction throughout the engagement. At the completion of the project, we will ask you for feedback on the engagement and for Iowa Judicial Branch to be a reference for our future customers.

To ensure that your review of this engagement with Coalfire meets our high standard, we ask that you let us know if, during the engagement, we do not meet your expectations, so we can address any concerns immediately. All members of our project team are happy to address any issues that may arise and route them appropriately for resolution. Additionally, you can contact Mike Weber, Coalfire Labs Vice President, at mike.weber@coalfire.com or 303.554.6333 x7052.

After this Project, our Quality Assurance team will be reaching out via email to request the completion of a satisfaction survey. Client satisfaction is a critical measure of quality and we prefer to receive this feedback directly from Coalfire clients. We regularly analyze all client feedback and report results to the delivery personnel for corrective actions and/or process improvements. Please take a minute to review and complete the survey once it is sent.

ROE AND TEST PLAN APPROVAL AND SIGNATURE

Iowa Judicial Branch accepts all risk and liability for all actions taken as part of the penetration testing activities performed and will ensure all precautions are taken prior to and during vulnerability scanning activities to prevent connectivity issues which could result in project slippage are taken prior to and during vulnerability scanning activities. The below signatory is authorized to approve this ROE and the included test plan.

Andrew Shirley

8/21/2019

Andrew Shirley

Date

Information Security Officer

Iowa Judicial Branch

Dana M. Mortaro

8/21/2019

Dana Mortaro

Date

Project Manager

Coalfire Labs

APPENDICES

1.0 External Network Penetration Testing – Meets PCI 11.3

2.0 Internal Network Penetration Test

3.0 Web Application Penetration Test

4.0 Social Engineering

5.0 Mobile Device Application Security Analysis

6.0 Wireless Vulnerability Assessment