GREENVILLE UTILITIES COMMISSION

QUESTIONS AND ANSWERS FOR 23-59

RFP FOR IT PENETRATION TEST

12/19/2023 at 3:00PM

We appreciate the questions that many vendors have provided. In response we are providing the following Addendum to the RFP, followed by answers to the specific questions asked. Similar questions asked by multiple vendors but with wording variations have been consolidated into one response.

RFP Addendum I

The first goal of this pen test is to determine if an outsider can penetrate our network firewalls. For this external portion of the project, we will provide you with our external IP range that has a total of 38 IP addresses. You will then conduct reconnaissance and OSINT for up to 10 hours and then provide a preliminary report of findings for GUC to review.

Next, we will assume you have been able to gain access to our network and want to know if you can move laterally and escalate within our network. We will provide you with a generic AD user account with general user privileges for you to use to attempt to exploit and gain access to workstations, servers, or systems in a non-obtrusive and non-destructive manner. Our goal is for you to find and identify weaknesses in our environment that would allow gaining root access, access to PII or other high-value documents, etc., as well as the one identified application. If you wish to provide a VM or appliance that has needed tools for doing such reconnaissance, we will install it and provide you with secure remote access to it for this phase of the project.

Finally, from that same foothold in our network, you are to attempt to access our SCADA production networks with the goal of finding any weaknesses in the internal firewalls that separate the general network from our SCADA networks. Further, we will provide you with the IP address of 1 device (workstation, switch, or server) in each of the 4 SCADA networks for you to scan and try to gain control of. Since you will be in a SCADA production environment, you are NOT to do a general scan of the network or attempt any action on any other device except the 1 device of the IP address provided. Access to the PLC networks is not in scope for this project.

We further expect that a detailed Statement of Work (SOW) will be created with the selected vendor. That document will clearly lay out all the details of the engagement.

Answers to specific questions asked, grouped by type:

BUDGET

1. Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?
    a. Yes, according to Exhibit A which was included in the proposal documents, the budget for this project is $45,000.

REMOTE ACCESS

2. Will Vendors be permitted to use off-shore teams to perform and/or support any and all penetration testing and assessment activities?
    a. All remote workers and scans should originate from sites in the USA.

SCADA SYSTEMS

3. We have done similar work to big customers, is SCADA reference mandatory to bid?
    a. No, although this could result in a lower score during the evaluation process.

4. Page two of the RFP states "Attempt to compromise the one provided non-production SCADA HMI client or workstation" as part of the scope. Can you confirm that this is 1 HMI client/workstation, not 1 per network (for a total of 4)?
    a. There will be one HMI client per network for a total of 4.

5. Is there a firewall or airgap network to the SCADA Network? Answer: Yes

6. For the 5 networks (Corporate, Electric, Water, Wastewater and Natural Gas), how many physical locations are to be included in the scope for testing?
    a. All testing for the networks can be performed from one physical location.

7. Will Embedded / SCADA Testing be required? Answer: No

8. Regarding the technical testing of the SCADA networks, will we be placed inside the IT network attempting to attack the SCADA gateways? Answer: Yes Or will we be dropped into each SCADA network uniquely, assuming OT compromise and challenged to attack an EWS (Engineering Workstation)? Answer: No

9. The provided non-prod HMI client, will this be a unique test and representative of other HMI clients in the various SCADA networks? Yes, each device and each SCADA network is representative of other devices in that same network. Or can it be included in one of the production tests within scope of total targets? Answer: No

10. What information related to our prior SCADA engagement will be required for the proposal? Basically, we would like to understand some of the data points and criteria about our prior engagement that need to be highlighted in the proposal based on which our proposal would be evaluated.
    a. No Response

11. What vendors does GUC use for SCADA & ICS systems?
    a. This information will be provided to the selected vendor when developing the statement of work (SOW) for the project.

12. The # of internal IPs (endpoints) were listed in the RFP. Does that # include IPs for IT & SCADA networks or just SCADA?
    a. The number provided was for the IT corporate network only. Endpoints in the SCADA environments are not in scope for this project beyond the 1 device per SCADA network that an IP address will be provided for.

SCOPE

13. Will you require us to perform the external in a Red Team style attack or Black-box attempt?
    a. A black-box testing assignment is preferred for external testing.

14. Will a base user account be provided for access and attempt to escalate privileges? Or will we capture creds through traditional pen testing by putting in a field system?
    a. The selected vendor will be provided with a generic user account with basic privileges along with access to a device on the corporate network to attempt lateral movement and escalation from.

15. Will this be on Windows desktop system with access to AD? Answer: Yes

16. Internal Scope: Attempt to discover and identify Personally Identifiable Information (PII) or other high value documents of interest. This is not a service our company provides. Does this provision disqualify our company from the selection process?
    a. No, although this could result in a lower score during the evaluation process.

17. How many principal DNS domains are included?
    a. There are 4 domains.

18. How many sites are to be tested?
    a. Assuming that this is referring to physical sites, all testing for the networks can be performed from one physical location.

19. Has the Greenville Utilities Commission previously performed a penetration test? If yes, how many times and when? What were the previous scopes?

    a. Details of this nature will be discussed during the development of the Statement of Work (SOW) with the selected vendor and provided as appropriate.

20. Specify the VLAN details how many are included in the Scope?

    a. Details of this nature will be discussed during the development of the statement of work with the selected vendor and provided as appropriate.

21. Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?

    a. Please see page 2 in the RFP under the Scope of Services. Any further details will be provided to the selected vendor.

22. How much (%) of the infrastructure is in the cloud?

    a. For the scope of this project, we are focused on on-premise infrastructure applications only.

23. In the IT department/environment, how many employees work?

    a. No Response.

24. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

    a. We manage our own data center.

25. Is there any wireless testing in-scope? Answer: Yes.

    a. If wireless is in-scope, how many sites? There are 3 wireless networks that can be accessed all from one physical location.
    b. How large are the sites? NA. How far apart are the sites? NA.

26. For the 38 external IPs, we will prioritize all IPs equally and look for anomalies. However, it would be great to know specific IP/segments of the network that you want us to focus on.

    a. We agree and will provide that during the Statement of Work (SOW) development with the selected vendor.

27. Is there documentation on the 510 internal endpoints, along with the number of servers, clients, and log information?

    a. Details of this nature will be discussed during the development of the Statement of Work (SOW) with the selected vendor and provided as appropriate.

28. During the 10-hour reconnaissance and OSINT phase, are there particular areas or aspects of GUC's digital presence you are particularly concerned about (for instance, employee information leakage, exposed credentials)?

    a. No, there are no specific areas of concern currently.

29. Are there any specific limitations or restrictions on the methods or tools we can use during the OSINT phase?
    a. Yes, as listed on page 2 of Exhibit A which was included in the proposal documents. Any additional limitations will be specified during the development of the Statement of Work (SOW) with the selected vendor.

30. Can you provide information about the role categories of internal IT servers?
    a. Details of this nature will be discussed during the development of the Statement of Work (SOW) with the selected vendor and provided as appropriate.

31. What API, application, and network architecture documentation will GUC provide for commencing our assessment?
    a. None of this will be provided.

32. Are there any restrictions on the types of exploits or offensive tool sets that can be used to test the 5 applications?
    a. To clarify, only 1 application will be tested. Further, 1 HMI device from each of the 4 SCADA networks will be assessed. Any exploit that may be disrupted to our production or SCADA networks/applications is prohibited. Details of this will be worked out during the development of the Statement of Work (SOW) with the selected vendor.

APPLICATION TESTING

33. Page three of the RFP states "Perform application focused PEN test with a single application – ERP" as part of the scope. Is this a security assessment of the web portal for their enterprise application?
    a. We would consider the web portal as in scope for this engagement. The ERP has other components like servers, technology stacks, and databases as well.

    How Many User Roles?

    b. There are many responsibilities within the ERP. For this exercise we will assume there are five roles/responsibilities that will be considered in scope and shared with you at the time of engagement.

34. Where is the application hosted?
    a. In our on-premises data center.

35. Is the ERP 3rd Party SaaS or Custom in House Hosted in AWS or Azure?
    a. It is internally hosted.

36. Can you give a better description of the ERP?
    a. Our ERP is a purchased system from Oracle. It serves to help us manage financial operations, human capital, and inventory.

37. Will this be required to be done onsite?   Answer: No.

38. If we gain access, DO WE STOP or continue to exploitation?
    a. We would have preference to not damage our system. The goal is for you to provide feedback on what you assess is in fact possible for a would-be attacker on our system.

39. Is this a web application or internal? If a web application, how many pages does the application have?
    a. This is an application in which the main entry point is via a web browser. Java is also part of the equation. There are too many possible pages to list a number.

40. Regarding the application (ERP) test, what language is this written in?
    a. This is a purchased application. We believe the base of the application is built with Java, however, there are other technologies involved from a stack perspective.

41. For the single business application and its five supporting servers, can you describe the languages used for the codebase (for frontend, middleware, and backend) and any known security mechanisms in place?
    a. This is a purchased application. We believe the base of the application is built with Java, however there are other technologies involved from a stack perspective. Weblogic and Oracle databases are known critical parts.

42. Is account management or a profile system part of the application, or is it separated into a module? Are there APIs to authenticate and authorize in place?
    a. We don't currently use any web-based APIs with this system. Exposing them and describing why in their current configuration they are an issue could be part of your effort. Authentication and authorization are part of the application.

43. Will we be given specific credentials to access this application, or are we expected to test as an unauthorized user initially?
    a. At the beginning we would expect unauthorized unless you gain a credential on your own. Later if you determine you are unable to gain entry, we may give you a credential with limited access to see if you can escalate.

44. For the external perspective of the ERP application penetration test, are there specific interfaces or services (like APIs or web portals) that should be the focus of the testing?
    a. Part of the application is exposed to the public internet. You should consider those in scope.

45. Which ERP application are we testing? Is it an open-source platform?
    a. Our ERP is a purchased system from Oracle. It serves to help us manage financial operations, human capital, and inventory.

46. Is GUC able to provide details about the type and size of the ERP system, or is it custom?
    a. Our ERP is a purchased system from Oracle. It serves to help us manage financial operations, human capital, and inventory.

47. If possible, we would need to know the number of dynamic pages in the business applications as well as the number of roles to be tested.
    a. There are many responsibilities within the ERP. For this exercise we will assume there are five roles/responsibilities that will be considered in scope and shared with you at the time of engagement. We cannot say how many screens and/or pages are in the application.

GENERAL & Miscellaneous

48. Regarding Section 1.6 on Page 9 of the RFP, which mandates a security assessment of vendor systems, we have queries concerning the alternative GUC-provided security assessment.
    a. For organizations not typically subjected to a SOC 2 audit due to industry specifics, we seek clarity on the contents and process of the GUC security assessment. Specifically, if this involves document completion, we would like to know if these documents can be accessed before RFP submission.
    b. Understanding the requirements of the GUC-provided security assessment beforehand would greatly aid our compliance with the RFP guidelines. Could you provide clarification on these points?

    ANSWER: After further review, section 1.6 of the original RFP does not apply and can be disregarded for the proposal response.

49. Because the requested services are strictly professional services and there is no delivery of an information system or application, we would like to request consideration that the SOC 2 audit be removed as a requirement because a SOC 2 audit does not apply to network and application security penetration tests.
    a. ANSWER: After further review, we agree. Section 1.6 of the original RFP does not apply and can be disregarded for the proposal response.

50. Will a list of personnel and certifications suffice or are resumes required?
    a. Full resumes are not required, although providing on a list of staff and their certifications could result in a lower score during the evaluation process. We are looking for all relevant information to rate the quality of personnel, so the more information that is provided, the better.

51. Proposal Requirements: Schedule of Rates. – As pricing for the project is fixed per the requirements, what is the purpose of this section?
    a. While engagements like this are typically a fixed fee project, vendor can choose to submit a time and materials proposal with a maximum “not to exceed” amount. In that case, a schedule of rates would be required.

52. 8.0 Insurance: 8.1.3 … including 3rd party coverage …. – Is the 3rd party coverage referring to coverage for GUC?
    a. This section refers to coverage for any sub-contractors or sub-vendors that you may engage to provide the requested services to GUC.

53. Is there an incumbent providing similar services to the Greenville Utilities Commission? If yes, is the incumbent performing to the satisfaction of the Greenville Utilities Commission, and the Director of Information Technology? Is the incumbent eligible to bid on this contract?
    a. We did a RFP for similar services 2 years ago, and the provider who was awarded is eligible to submit again. They did provide satisfactory services at that time, but all proposals will be judged on the requirements of the current RFP.

54. Is there currently an incumbent company or previous incumbent, who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number, dollar value, and period of performance?
    a. See answer for question number 53. Go to: www.guc.com

       About Us, Doing Business With Us, Past bids, Scroll down and find the RFP #21-65

55. Will the Greenville Utilities Commission be permitting penetration testing to be performed by existing or previous IT or Managed Service Providers? Or will the Greenville Utilities Commission be requiring third party independence to reduce the risks of conflicts of interest or the optics of "grading one's work"?
    a. Current or previous IT service or Managed service providers are not prohibited from responding to this the RFP if they believe they can meet the specifications therein.

56. Is there an up to date and current asset inventory, and network topologies available for both IT and OT networks? Upon contract award and execution, will these documents be made available to the penetration testing team?
    a. These items are available but will only be shared with the selected vendor if it is deemed necessary during the development of the Statement of Work (SOW).

57. Are IT and OT devices on physically separated and different networks? Or are IT and OT systems co-mingled together on the same network?
    a. They are both physically and logically separated.

58. We would like to confirm that our understanding statement on 1 of Exhibit A is accurate: "Any work that has any potential of negative impact should be performed from 6 a.m. to 6 p.m. Monday-Friday, Eastern Standard Time." - Work that has potential negative impact should be performed during business hours where there is reasonable support to support the effort. However, work can be performed around the clock provided that it does not have any potential negative impact.
    a. Your understanding is correct. Further, the times listed in Exhibit A should have been “7 a.m. to 5:30 p.m. Monday-Friday Eastern Standard Time”. These are the times that any work that may have negative impact should be conducted since we will have staff working to address any issues.

59. Page 5, first bullet point. It is stated that "All firms submitting proposals must be duly licensed to practice business in the state of North Carolina." What license are we expected to have? Can this be obtained post award?
    a. License to practice business in the State of North Carolina. No.

60. The requirement states: "8.1.3 Network security & Privacy Liability - The VENDOR shall provide and maintain Commercial Network Security & Privacy Liability insurance, including 3rd party coverage in the minimum amount of $5,000,000 per occurrence." Would Greenville Utilities Commission accept limits of $2,000,000 per occurrence?
    a. No Response.

61. How do you want us to report our findings while testing, especially the critical ones? Is there an Incident Response Team that we need to get in touch with?
    a. Yes, we have a security team that any critical findings will need to be reported to during testing. This will be discussed further with the selected vendor when developing the Statement of Work (SOW) with the selected vendor.

62. Are there any specific standards followed for assessing the quality of the pentest proposal? Answer: No. Are there any quality attributes that you want us to focus on? Answer: No.

63. Does GUC have any specific expectations regarding the skill level, certifications, or experience of the engineers? Answer: No.

64. Due to the confidential nature of our security business as well as existing NDAs, we would like to provide anonymized references at this RFP stage, i.e., we would provide project implementation details, but the client would be described, not named, and specific contact information would be withheld for now. Reference calls would be coordinated upon request at down-select. Would this approach be acceptable to GUC for this RFP response?
    a. Yes. We will accept anonymized references for this stage if they indicate the size of the company, the industry they are in, and the scope of security work provided to them. After review of all proposals, we will narrow the list to the top 2-4 vendors and will require full contact info for references at that time.

65. Could a company's headquarter status outside North Carolina potentially impact our chances of being down selected? Answer: No.

66. We are a small business based in California, Is North Carolina business license mandatory? Can we apply for that after the award?
    a. Yes. Per RFP, see Page 5 first bullet point.