March 1, 2018

Questions and Answers #1 Related to the RFP for External and Internal Penetration Testing Services

EXTERNAL NETWORK PENETRATION TESTING QUESTIONS

1. How many Internet accessible servers/services are present? **Less than 5.**
2. How many of these services are web servers (HTTP and HTTPS)? **Less than 5.**
3. How many interactive web applications are in scope for the assessment? **Less than 5.**
4. How many firewalls would you like reviewed? **Less than 5.**
5. Approximately how many active IPs (i.e., in use IPs) are exposed on the external perimeter and would be considered in scope? **Less than 10.**
6. For the Firewall Assessment, would this be black box testing to determine which ports/protocols are accessible from external networks or a review of configuration files and rulesets? **Black box.**
7. Are there any third party hosted services (i.e., AWS, Azure, Digital Ocean)? **Yes.**
8. Firewall Assessment: number of firewalls, model and brand, and any total rules per device over 200? **Cisco ASA, No. It is in scope to include the firewall in the penetration test, attempt to circumvent/bypass it's ruleset and/or compromise the device, and review the firewall configuration settings and rules.**
9. Number of live or active external IPs to be tested. **Less than 15.**
10. Number of hosts (IPs)? **255.**
11. How many external IP addresses should be tested? **All.**
12. How many of the above IP addresses host a web application? **Less than 5.**
13. External IP Address Ranges. **1.**
14. Domain Names. **1.**
15. Any additional information. **We would like to utilize more than one type of simulation for the testing. We will provide input into the development of the scenarios.**
16. Is target of opportunity an acceptable methodology or is every IP needing to be tested? **All.**

INTERNAL NETWORK PENETRATION TESTING QUESTIONS

1. How many total devices (servers, workstations, network infrastructure, etc.) are in scope for the internal penetration assessment? **All, approx. 330.**
2. How many different network segments are implicated in the internal penetration assessment? Is there a single location from which all segments are accessible? **14 Class C subnets, sparsely populated. No.**

3. Is the Internal network penetration testing dependent on breaching the external network? **No.**
4. Number of internal hosts to be tested? **All, approximately 330.**
5. Approximately how many assets are in scope for the internal penetration test? (Approximate number of servers and workstations). **Approx. 288.**
6. Are there any third party Active Directory trust relationships that would be considered out of scope for the penetration testing? **No.**
7. What is the predominant operating system in use throughout the internal environment (i.e., Windows, Mac OS, Linux/Unix)? **Windows.**
8. What scenarios should be simulated during the internal testing (e.g., malicious insider, unauthorized visitor)? **Multiple plausible scenarios.**
9. How many endpoints in scope? **328.**
10. How many of the above IP addresses host a web application? **Less than 5.**
11. Number of Workstations. **223.**
12. Number of Servers. **65.**
13. Domain Names. **1.**
14. Total Number of Internal Hosts. **1.**
15. Any additional information. **We would like to utilize more than one type of simulation for the testing. We will provide input into the development of the scenarios.**

CTPF WEBSITES PENETRATION TESTING QUESTIONS

1. How many web applications is CPTF having tested? **Less than 5.**
2. Can you provide guidance as to the type of web applications in use? IE Home grown, Third party, etc. **All.**
3. Is Credentialed and/or Non-Credentialed testing required/preferred? **Both required.**
4. On average how many Static Pages do these web applications have? **To be provided to the selected vendor.**
5. On average how many user levels will be tested? **To be provided to the selected vendor.**
6. What types of Databases are in use for the backend of these web applications? **To be provided to the selected vendor.**
7. What platform is/are the app(s) built on? **To be provided to the selected vendor.**
8. Are there any directly connected APIs for the app(s)? If so, is CTPF looking for API penetration testing pricing and on average how many methods would be testing for each API? **Yes to both.**
9. For CTPF Website, please answer yes or no as to whether the application includes one or more of the following: **In regards to the following list, this information is to be provided to the selected vendor.**
    a. Static Content. -
    b. Dynamic pages. -
    c. Database backend. -
    d. Login/accounts. -
    e. Search function. -
    f. HTML forms. -
    g. File upload/download. -
    h. Forums. -
    i. Credit card payments. -
    j. Shopping cart. -
    k. Content Management (CMS). -
    l. AJAX. -
    m. JSON. -
    n. Flash. -
    o. Silverlight. -

p. COTS (SP, SAP, Lotus, etc.).-

10. Applications: Number of applications & are they internal or external (or both) – and complexity (dynamic pages?) **Line of business and ERP applications.**
11. What is the level of rigor required for the web app testing? **Level to be provided in SOW.**
12. Unauth testing is covered in the External Pentest, is a deeper assessment required? If so, please provide user roles to be tested, number of API's, size of code base, language application is written (Java, etc.). **Some user roles may be provided in SOW.**
13. Will code be provided for review? **Not provided.**
14. How many applications are in scope? **Less than 5.**
15. Should both authenticated and unauthenticated testing be performed? **Yes.**
16. Can testing be performed remotely? **Yes.**
17. Number of pages (include sub modules if any). **TBD.**
18. Number of privilege levels (include sub modules if any). **TBD.**
19. Application available on Internet or Intranet? **Both.**
20. Do you require OWASP Top 10 for website testing? **Yes, but not limited to OWASP Top 10.**
21. Application Name. **Test line of business and ERP applications.**
22. Application Description. **To be provided to the selected vendor.**
23. Application URL(s). **To be provided to the selected vendor.**
24. Is the application Internet Accessible? **Yes.**
25. Number of Dynamic Pages. **To be provided to the selected vendor.**
26. Number of Static Pages. **To be provided to the selected vendor.**
27. Number of Parameters. **To be provided to the selected vendor.**
28. Number of Authenticated User Roles (Admin, User, etc.) **To be provided to the selected vendor.**
29. Describe Authenticated User Roles. **To be provided to the selected vendor.**
30. Application Technologies / Platform. (Indicate: ASP.net, PHP, Java, Ruby on Rails, or Other). **To be provided to the selected vendor.**
31. Are there any Web Services that need to be tested? If yes, describe. **Yes.**
32. Are there Mobile Applications to be tested? If yes to the above question, what type? (Indicate: browser, IOS/iPad, IOS/Watch, IOS/iPhone, Android, or Windows Mobile). **Yes, various.**
33. Testing time requirements? (Indicate: anytime, non-business hours, business hours, or other). **All times.**
34. Testing environment? (Indicate: production, development, QA, staging, or other). **All environments.**
35. Requested testing start date. **TBD.**
36. Requested completion date. **TBD.**
37. Describe any pages or functionality that should be excluded from testing. **None.**

WIRELESS SECURITY SCANNING QUESTIONS

1. How many wireless networks are in scope for the wireless penetration assessment? Across how many facilities? **3.**
2. How many locations are in scope for the Wireless Penetration Testing? **1.**
3. On average how many APs are at each location? **8.**
4. Does CTPF utilize guest networks at the above locations? **Yes.**
5. How many SSID's? **3.**
6. Are they centrally managed? **Yes.**
7. Will you provide configuration files for review? **No.**
8. Are attacks against clients joined to the wireless networks considered in-scope for this assessment (e.g. Evil Twin Attack)? **Yes.**
9. Number of wireless devices. **40.**
10. Number of separate facilities/buildings that have separate wireless network. **0.**

11. Physical Locations for On-site Wireless Assessment (Site Names and Addresses). **203 N LaSalle St, Ste 2600, Chicago, IL, 60601.**
12. List SSIDs and Purpose. **3 for staff, devices, and guests.**
13. Is Guest Access Provided for Non-Corporate Devices? **Yes.**
14. Any additional information. **We would like to utilize more than one type of simulation for the testing. We will provide input into the development of the scenarios.**

SOCIAL ENGINEERING QUESTIONS

1. How many employees would be targeted for the Social Engineering Phishing testing? **All.**
2. Will CTPF provide the email addresses for the Social Engineering Phishing testing? **Yes.**
3. Number of unique email address for phishing. **270.**
4. This includes physical – do you want onsite SE, or perhaps Overt/Covert Physical also? **Yes, this includes onsite SE and Covert Physical.**
5. How many locations in scope for the physical security assessment? Will this assessment be guided by a CTPF employee? **1 and Yes.**
6. What is the objective of the phishing exercise? Does CTPF expect the vendor to execute a mass campaign with the goal of collecting security metrics (e.g., % clicked, % opened, etc.) or does the CTPF want the vendor to gain a foothold from over the Internet and pivot to the internal network? **Yes, metrics required.**
7. Is CTPF interested in doing a targeted spear phishing assessment of a smaller sample size of employees? **Yes.**
8. In regards to a social engineering – email phishing simulation, we request the following information:
    a. Email Provided by Customer or Harvested by Vendor? **Provided by Customer.**
    b. Any additional information. **We would like to utilize more than one type of simulation for the testing. We will provide input into the development of the scenarios.**
9. Physical Security Testing:
    a. How many physical locations are in scope for Physical Social Engineering testing? **1.**
    b. Are all the locations in Illinois? **Yes.**
    c. Has CTPF ever conducted a physical security risk assessment? **Yes.**
    d. How many facilities are part of your organization that would be considered in scope for the Physical Security testing? **1.**
    e. On average how many employees & contractors work at each facility that are deemed in scope? **Less than 200.**
    f. On average what is the approximate size of each facility that are deemed in scope? **28,000 sq ft.**
10. Does the social engineering/phishing include email and telephone? If so, do you have a number in mind for how many emails and phone calls you would like for this testing? **Both email and phone. Approximately 200.**

GENERAL QUESTIONS

1. Is one of the goals of this assessment to test the detection and response capabilities of the CTPF security team? Specifically, is there an expectation to perform stealth testing? **Yes.**
2. Are there any compliance requirements that we should be aware of, IE PCI-DSS, HIPAA? **HIPAA.**
3. Will testing be conducted during business hours, after hours, or weekends? **All.**
4. In regards to billing, only hourly rates or are you willing to accept project based pricing? **Project-based pricing is acceptable.**

5. In regards to mode of execution, can the testing be done remotely? If yes, will CTPF be able to provide necessary connections for bidder to conduct activities remotely? **Yes.**
6. Please specify the type of special request that might come up. **Special requests may include testing new applications that may be implemented.**
7. How frequently do you perform Pen Tests? **The tests are performed at least twice per year.**
8. Do you want a Pen Test performed for compliance? If so, which compliance requirement do you want to meet? **The tests are performed as a self-assessment best practice.**
9. 58. Can a current IT service provider of CTPF submit a proposal? **Since the penetration testing will be of all IT functions, any vendor who is a current IT service provider to CTPF is precluded from consideration to avoid any conflicts or lack of independence.**