

January 5, 2017

**Questions & Answers – Specification Clarification II**

**Request for Proposal #217-19**

Grand Valley State University (GVSU) has the following answers to questions that have been submitted for request for proposal #217-19. Note: GVSU’s responses have been noted in red.

PCI environment:

a.      How many devices are included in the Cardholder Data Environment?

Approximately 50 networking devices and 75 workstations and servers.

b.      Are there web applications included in the PCI environment for testing?

Yes, there are some smaller web applications that exist in the PCI environment and would be considered in scope.

2.      Housing:

a.      Would this include student housing workstations or just administrative workstations?

This RFP is only for faculty/staff workstations which we classify as “Office” machines. Lab and lab networks would be included. Student’s personnel machines would be out of scope.

3.      Campus:

a.      Does this pen test include locations outside of main campus?  Grand Rapids campus?  Remote campus locations?

Grand Valley’s main campus is located in Allendale, MI. This RFP includes Allendale and Grand Rapids. It does not include the Holland, Traverse City, or Detroit buildings.

1. Why is GVSU looking for security testing?

GVSU conducts penetration tests on a semi regular basis.

5. Is this the 1st time GVSU is security testing for applications?

GVSU has had several pen tests conducted historically and all of these applications have been included. Since most of these are third party purchased products the code review/code security would have been conducted by the specific vendor.

6. Can GVSU provide the detailed requirement of testing?

No. This is a pen test and we rely on the vendor to have a defined testing methodology which we will review.

7. Does GVSU expected duration of the project or timeline?

GVSU’s goal is to complete the pen test in one to two weeks.

8. Is GVSU looking for a Fixed Price quote?

Yes, we have a fixed budget for this project and we are not interested in a time and materials quote at this point.

9. IS GVSU expecting bidder to resell testing tool licenses to GVSU as part of the proposal. Or will GVSU purchase tools directly?

This is an RFP for a pen test. Tool recommendations would be welcome. We have the option to purchase direct or through reseller. The specific goal and budget for this RFP does not include the purchase of any tools.

10. Are there any project deliverables being requested other than a formal report?

Yes, beyond the formal report GVSU is looking for cross training of our internal security teams. While this deliverable is less tangible and harder to measure, it is expected that internal security team would be able to participate in the tests and would have access to all individual tool reports.

11. Is there a preferred approach for risk rating identified gaps for the engagement?

There is no preferred approach at this time.

12. Are there any internal security standards that devices, systems, processes or applications should be compared against for the report?

Not at this time.

13. Are the PCI environment systems included in the overall device count that was provided?

Yes, there are around 50 network devices and 75 workstations/servers that fall into our PCI environment.

14. Is the requested PCI penetration testing in support for PCI compliance?

That is not the only goal of this pen test but it may be used for PCI compliance as well. We have an additional PCI compliance advisor that handles PCI regulations.

15. Device count clarification/size clarification

a. GVSU servers have publically assigned IP addresses. GVSU owns the scope 148.61.0.0/16.

b. Size and scoping:

General office:

Approximately 850 servers

Approximately 1000 network devices

Approximately 100 security devices

PCI environment:

Approximately 50 network devices

Approximately 75 workstations

c. 802.1x is the authentication model and WPA2-AES is the encryption method.

d. Wireless equipment provider is Cisco

16. What level of training are you wanting?

We would like our internal security team (three people for the purposes of this training) to be able to participate in the process you are using, as well as training on the tools you are using, and the rationale behind the chosen methodology/path.

1. How many would be attending?

Three primary personnel but I am sure others will stop in from time-to-time if something interesting or relevant comes up.

1. Do you want the entire battery of testing to be done in front of this group?

Scanning and some of the full run tools take to long for the group to watch the scan. We would like to review the results of scans but to sit through an entire scan of our subnet is probably not appropriate.

1. Training – further clarification

GVSU is open to other training options other than purely onsite. We have Skype for Business / Lync as well as conference rooms equipped for virtual meetings.

17. Line item pricing

GVSU is requesting that each group of tests to be performed is listed as a separate line. An example of what we expect is:

PCI - External $$$$

PCI – Internal $$$$

Wireless $$$$

Etc.…

18. Testing systems

GVSU can supply a machine for testing on what is considered a non-privileged net. Also, if the vendor has a prebuilt system they would like to ship to GVSU we can place it on the same net. For testing inside the PCI environment, we can provide the tester with a standard PCI imaged machine.

19. What risks are of primary concern to GVSU?

The primary risks GVSU is investigating is the security of central IT, departmentally hosted servers, and IT security.

20. Will incident response testing be included?

Not for the purposes of this RFP.

21. Is remediation support desired? This includes validation of remediation and report regeneration.

Possibly, but please list as a separate line item so GVSU can choose rather the cost of this is within budget.

22. Are all assets to be tested located at GVSU?

All assets to be tested are located at GVSU. Assets will primarily be hosted in Allendale or Grand Rapids.

23. Would GVSU require any training documentation or additional classroom time beyond being present during the testing?

Training is an important part of this RFP. Simply being present while a Nessus (or similar) tool is run is of minimal value. GVSU is seeking knowledge transfer from tester to internal team members.

24. Is the purpose of testing to identify exploitable vulnerabilities in all hosts tested or is the purpose of testing to gain access to the hosts in scope?

The purpose is to gain access. We regularly scan our hosts with industry standard vulnerability scanners, primarily Nessus. While we do want to see some scanning to ensure we are not missing anything we want to test the resiliency of hosts beyond simply vulnerability scanning.

25. For PCI environment testing, is GVSU looking to use the results of this penetration test to satisfy PCI DSS requirements?

While that is not the primary focus of this RFP the pen test will be included in GVSU PCI environment reports and will be used to fix any issues identified by the test.

26. For each of the applications GVSU would like tested, please answer the following questions:

a. Are there any specific security concerns with this application?

Input validation, cross site scripting, privilege escalation, lateral host traversal, direct DB access, etc.

b. Will GSVU be providing credentials to perform authenticated testing?

We can setup temporary testing credentials to be used.

c. What type of application is it? (Web application, mobile application, application accessed via thick client)

All of the applications to be tested are primarily web applications. They may also have a mobile component and/or a thick client interface but the primary access point for most users is web based.

d. What is the software stack being used to run the application?

The stack varies depending on the application but is either nix running Apache and Oracle or Windows running IIS and SQL. A lot of the applications use ColdFusion but not all.

e. Will there be a load balancer or Web Application Firewall in front of the tested application?

Yes, there is a load balancer, IPS, and a minimally configured Web Application Firewall. We can provide a direct route to the application if required but the goal of the pen test is to ensure that the entire suite of products we have setup will protect the application.

f. Will documentation (including API documentation) be available to the testers?

Probably not but there may be some. All but one of the applications to be tested is a purchased third party system. We can provide what API documentation is given to us.

g. Will source code be available to the testers?

Source code for the web site or GVSU written applications can be shared with a proper NDA in place. Most products to be tested are third party purchased products that do not allow us to share the source code with another third party.

h. Describe the purpose and functionality of the application.

LMS – Learning management system

ERP

Website

Housing

27. Please describe briefly the purpose of each of the wireless networks that will be tested (for example, faculty only, student only, public use)

One Faculty/Staff network

One Student network

One Guest network

One networking that allows visiting individuals from other participating schools to login

28. For wireless networks that are using Pre-Shared Keys, once a handshake is captured, would GVSU provide us with the key for us to determine its strength in the interest of saving time that could be spent performing other tests?

GVSU does not use pre-shared keys. We use 802.1x, certificate, and MSCCHAPv2 tunnels.

29. Are internal Nessus scans being run by GVSU being done so authenticated or unauthenticated?

Unauthenticated or non-credentialed

30. Is DDoS testing an absolute requirement?

Actually performing a DDoS is not a requirement and is something that would have to be carefully scheduled and negotiated. Assessment for exposure to DDoS is a requirement.

31. Can testing be conducted during normal business hours?

Yes, most testing will be able to be done during business hours if it can be done on the week requested. That is spring break for our students. There are still probably a few systems where we may need to schedule a time that may be off hours.

32. Regarding the wireless penetration test dictated in section 4 of Scope of Work, MAD Security submits the following questions:

a. Will the testing be conducted at one location or will there be multiple locations?

Testing could be accomplished in one location.

b. Are any of the wireless networks located in a multitenant facility where you may be sharing a building with other companies that could be affected by this testing? If yes what locations? 0 Yes 0 No

No, GVSU is the sole occupier for buildings where tests would happen.

c. How many SSIDs are in scope?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SSID | Total Number of Access Points | Physical Location | Approx. Sq. Footage | Additional Notes |
| GV-Faculty-Staff | 2800 | All locations | Most of campus |  |
| GV-Student | \* | \* | \* |  |
| GV-Guest | \* | \* | \* |  |
| eduroam | \* | \* | \* |  |

33. In Section 4.0 Scope of Work GVSU lists systems it would like tested (Banner, Blackboard, Campus Loan Management, Housing, and GVSU’s primary website).

A. Are these systems listed all web applications?

Yes, the primary interface is web based or Java based. There are often secondary access methods like thick clients for administrative work.

B. Will the consultant be testing them with credentials, or unauthenticated?

We can accommodate either. We would prefer both. A test without credentials to check if access can be obtained without proper credentials and then a credentialed test to see if other exposures exist once authenticated. Please note the cost for each as a separate line item in the pricing section.

34. In Section 4.0 Scope or Work GVSU requests: Test Client hardening actions to ensure endpoint clients have been reasonably locked down.

a. Does GVSU need hardening assessed against a specific industry standard (i.e. CIS benchmarks?)

There is no specific industry stand standard at this time.

35. In section 4.1 Overview of technical environment to be tested, GVSU provides a table of Device Types, Quantity and Platforms.

a. Can GVSU describe what network structure looks like (i.e. do these systems live on 4 class b (/16) networks or 10 class c (/24) networks, etc.)?

The devices will primarily exist on 16 separate class C networks. That is not to say that all class C subnets are fully populated with hosts but there are 16 primaries subnets.

b. Can all of these networks and devices be assessed from one location or will be need to move from location to location to perform the assessment?

All assessments should be reachable from one location.

36. In Section 4.2, #9, GVSU requests DDoS of selected systems.

a. Has GVSU undergone DDoS testing in the past?

GVSU is requesting DDoS evaluation and limited testing. An actual full scale DDoS is not desired. GVSU may ask the bidder to attempt to DDoS a specific system if the risk is believed to be high enough. If that is requested, it would need to be carefully scheduled and negotiated.

b. Is GVSU aware that the risk of DDoS (Distributed Denial of Service) testing even on targeted systems/services, may cause disruption to the entire network and in many instances, can cause unforeseen outages?

Refer to the above. We are seeking to asses our risk to DDoS not specifically carry one out. If a system is deemed vulnerable GVSU may ask the bidder to run a limited DDoS against a test version of the application.

37. Is there are standard operating system imaging and patch management processes in place, would a sampling approach of systems be considered for the penetration testing?

There is a standard image in place and patch management is in place as well. While some sampling is expected, IE if you can exploit any windows box we only need you to prove it on a small subsection. But, the hope is that the pen test will check for systems that have been missed by the standard image and patch management systems.

38. Would GVSU consider a targeted penetration testing approach (on the internal environment) where we attempts to gain access to specific targeted information or systems, instead of looking across all hosts in the environment?

We would consider a targeted test but would prefer a broader approach. I would encourage you to submit a price for both.

39. We offer a service for testing at the start of the engagement to help validate that IDS / IPS systems are detecting malicious activities known as an External Evasive Pre-test. Would GVSU consider using the External Evasive Pre-test to determine the effectiveness of existing detective and responsive network controls?

Yes, we would be open to doing some form of a pre-test. Please include this a separate line item in the quote so that we can accurately determine rather the cost of the test fits within our goals.

40. For internal testing, can all IP addresses being tested be reached from a single internal network port?

The port provided will allow access to all applications but it is not unrestricted. Example, if it is a web port you may only have TCP/80 to the application. Part of the pen test is to test that we have restricted enough ports to applications to prevent unwanted access like SSH or RDP.

a. If not, how many unique VLANS will we need to connect to in order to perform testing?

There would be roughly 50 VLANS that would be in scope.

Bid Opening: Monday, January 13, 2017 @ 10:00 AM

Thank you for your participation,

Valerie Rhodes-Sorrelle, C.P.M.

Sr. Strategic Sourcing Specialist

***Procurement Services - 2033 Zumberge Hall - Allendale, MI 49401***

***Phone – 616/331-2283 – Fax 616/331-3287***