Feb 2014

Guide to Creating an RFP for Vulnerability Assessment/ Penetration Test

Version 1.0

Introduction

The California Community Colleges Technology Center and the Information Security Advisory Committee has created this document to assist Colleges to create a Request for Proposal Document for an Information Technology Vulnerability Assessment or Penetration Test.

Define Scope

1. External Servers/Devices only (those assessable from outside the campus)
2. Internal Server/ Devices only (those assessable only on campus)
3. External and internal
4. Any specific exclusions (any devices or server that shouldn't be examined)
5. Priority of targets (You will likely have a fixed number of hours, more important devices/ servers should be examined first)
6. Order of testing (will tie into priority, what order do you want the network examined)
7. In a penetration test it should be determined whether the tester should look for PII after exploiting vulnerabilities.
8. Determine if Denial of Service (DOS) attacks should be tested.
9. Determine if social engineering of staff is in scope
    a. Should it be limited to electronic phishing (email, IM, etc.)
    b. Should phone calls be in scope (Calling help desk pretending to be an employee)
10. Define if physical assessment is wanted.
    a. Want means can be used (lock picking, social engineering, etc.)

   b. Determine any out of scope tactics (physical destruction of any kind, no compromising professors offices, other things that may break union contract rules)
   c. Determine what building/offices are not in scope (president's office, etc.)
11. Define the time limitation.
   a. Limit the number of days and time of days the tests are able to be run on important network segments and servers to prevent the tests from impacting business processes.

Determine type of test

1. Vulnerability assessment – Only looks at potential vulnerabilities, does not validate vulnerabilities by exploiting them.
   a. Determine what type of test you want, white box or black box.
   b. In a white box vulnerability assessment you work with the consultants, providing network diagrams or other information to help them determine where vulnerabilities are. You may also provide them with valid credentials to scan inside your servers/ devices to determine if there are missing patches or out of date firmware. Consultants may also interview IT staff to determine potential vulnerabilities. This type of test more closely simulates an insider threat with advanced knowledge. This type of test is more likely to result in the consultants finding vulnerabilities as they spend less time on reconnaissance.
   c. In a black box vulnerability assessment you only give the consultants the scope and let them test the devices/ servers. You may or may not inform all of the IT staff of the test that a test is taking place to determine if potential attacks are detected by IT staff. This more closely

simulates an outside attacker. This type of vulnerability assessment is less likely to find vulnerabilities as it is very limited to what can be found without exploitation and inside knowledge of the services and applications on the network.

2. Penetration test – Identifies potential vulnerabilities and exploits them to validate that they are really vulnerable. May also use exploited device/ computer to launch more attacks.
    a. Determine what type of test you want, white box or black box.
    b. In a white box penetration test you work with the consultants, providing them information such as network diagrams and documentation of what services are running, and where. You may provide them credentials to determine of your devices/computers may be vulnerable to privilege escalation vulnerabilities and to test the internal applications. In a penetration test the consultant will attempt to compromise the devices/computers once vulnerability is found. An important part of the contract should be that the consultant removes all backdoors that may have been installed as part of the test. Consultants may also interview IT staff to determine potential vulnerabilities. This type of test more closely simulates an insider threat with advanced knowledge. This type of test is more likely to result in the consultants finding vulnerabilities as they spend less time on reconnaissance.
    c. In a black box penetration test you only give the consultants the scope and let them test the devices/ servers. You may or may not inform all of the IT staff of the test that a test is taking place to determine if potential attacks are detected by IT staff. This more closely simulates an outside attacker. This type of attack is less likely to have as many findings as they consultant will spend more time on reconnaissance, and not knowing what other services they may be able to compromise from the vulnerable computers.

Final Report

1. Report – The report should include the following at a minimum]
    a. Purpose of the vulnerability assessment/Penetration test (Compliance with regulations (PCI, FERP, etc.), best practices, etc.
    b. The name of the company and the names of the testers
    c. An executive summary, which should be fairly non-technical that can be shared with constituents on campus such as the President, Vice Presidents, Chancellor, etc.
    d. It should detail the vulnerabilities that were found, and in the case of a penetration test should include wither the consultants were able to exploit the vulnerably.
    e. Remediation steps should be included for each of the vulnerabilities found. If there is no remediation available (for example end of life devices or software) that should also be noted.
    f. The report should include a risk rating for each vulnerability found to aid in your priority of remediation.
    g. If the scope included finding sensitive information (PII, SSN, etc.)
    h. It a vulnerability was exploited the report should detail the steps to reproduce the exploit (for example Metasloit module foo)
    i. The report should include what tools were used to perform the test.
    j. The report should detail the start time(s) and end time(s) of the test.

Expectations

1. For a standard vulnerability test/Penetration test typically the testers will not have the time and expertise to examine custom web application. They should be able to find if standard application such as WordPress or Joomla is out of date and vulnerable. Consider having a separate web application penetration

test done for custom applications that have access to data such as SSN, addresses, grades, etc.

2. Consultants probably won't be familiar with custom applications used at the community college systems such as Banner, PeopleSoft, Datatel , SARS, degree works, etc. Consultants will be able to find implementation flaws such as server misconfigurations, but likely won't know if the current version you are running may have known flaws. It is important to keep up to date with these products yourself, and install critical updates as they are released by the vendors.

Caveats

a. A non-discloser agreement should be required for all consultants performing test for the college.
b. DOS attacks can have a serious impact on your network and should only be performed after normal school hours.
c. Some test can be destructive; you should have the consultant do testing in your test environment if available before attempting in your production environment. A full and verified backup should be completed before any penetration test is performed.