COURT INFORMATION TECHNOLOGY OFFICERS CONSORTIUM

Helping Judicial Stakeholders Understand Penetration Testing

Technology Experience Bulletin, TEB: 2007-01

Understanding Penetration Testing

Penetration testing can be understood as the proactive use of *friendly* hackers to identify what vulnerabilities have inadvertently been left for *unfriendly* hackers to exploit. But for judicial stakeholders to make an informed choice to accept the good that can come of the penetration testing exercise, we may need to help them come to terms with the balance of pros and cons of doing penetration testing.

Court Environment

Texas has a decentralized court system, with trial court funding almost entirely provided by the counties, with the exception of the salaries of district judges. In this framework, the Texas Office of Court Administration (OCA) provides support to courts in Texas, with emphasis on certain special areas of centralized statistical reporting and technical consulting. Information technology (IT) resources are provided locally to trial courts, creating great diversity in IT infrastructures. OCA receives a state appropriation to provide IT support to the fourteen mid-level appellate courts and the two high courts (the Supreme Court and the Court of Criminal Appeals), but half of the mid-level courts also have a source of additional funding in their districts, which each chief justice may use for supplemental IT resources. This article is written from the perspective of a state-level courts' IT manager where the state's judicial structure implies local judicial independence as including administrative independence as well as adjudicatory independence. The intended audience for this article is IT directors within a judicial system.

Tips for Implementation

Tip 1: Explain penetration testing to your stakeholders.
Tip 2: Use an independent tester.
Tip 3: List other respected organizations that use penetration testing.
Tip 4: Know what penetration testers are looking for, including accidentally-discovered illegal materials.
Tip 5: Explain the risks
Tip 6: Determine the scope of the test.
Tip 7: Respect stakeholder limitations.
Tip 8: Commit to reporting to your stakeholders.
Tip 9: Know how the results will be provided.
Tip 10: Hold provider to confidentiality.

Tip 1: Explain penetration testing to your stakeholders. Explain to the judges and clerks whom you serve what you plan to achieve through penetration testing. Emphasize the value of detecting vulnerabilities and getting them fixed before the bad guys find them.

Tip 2: Use an independent tester. If your staff knew all of the network's vulnerabilities, they would have fixed them already, right? Using an external entity to do the penetration testing helps eliminate bias, so you can really find the vulnerabilities. Internal testers may have mixed incentives when testing their own network. And totally automated testing tools may not go as far or bring the creativity to the penetration test that human testers can. For example, an automated testing tool can do very little social engineering.

Tip 3: List other respected organizations that use penetration testing. Find out about other organizations—especially other courts—who have used penetration testing. This carries great credibility, as well as "cover," to any stakeholder group to give their endorsement of the penetration test.

Tip 4: Know what penetration testers are looking for, including accidentally-discovered illegal materials. Penetration tests disclose software that is not patched to current revisions, overly-revealing system responses, weak passwords, application programming flaws, faulty firewall settings, etc. Optional levels of testing include searches for covert modems and wireless access points.

Though a penetration test doesn't look for such materials, testers have the potential to incidentally find illegal materials—if they exist—such as child pornography on their customers' systems, obliging them to report to law enforcement.

Tip 5: Explain the risks. Penetration testing creates a risk for the IT director that shortcomings of the IT shop will be exposed. Additionally, your stakeholders may be concerned that penetration testing may lead to the discovery of embarrassing materials on court computers. Explain that to your stakeholders and ask them to take the message back to the users that inappropriate computer usage could be discovered if it continues.

Penetration testing does create some risk of degraded system performance or even complete denial of service during automated scans of your infrastructure. Make plans for quick response if this happens; including an urgent desist message to the testers. Explain this plan to your stakeholders.

Further, testers have the potential to access confidential legal work product or work in progress, such as information on sealed cases, legal research opinions in progress, and random e-mail contents. You will want to note that it's better for the good guys to find this and tell you about it than for the bad guys to find it and not tell you.

Tip 6: Determine the scope of the test. Your contract with the external tester should define the boundaries of the testing. Will it be through Internet access only? Will it include searches for modems through "war dialing" to

extensions in your PBX? Will it include a search for rogue wireless access points or open network ports in court buildings? Will it include attempts at social engineering? If so, information obtained from the court's point of contact should be designated as off-limits.

At a minimum, your testing provider will need to know the IP address ranges and domain names to test within. This information doesn't particularly help the tester with discovering the network, but keeps the tester from testing more broadly than required.

To test for internal vulnerabilities which cannot be reached through your firewall but could be exploited by internal users, your tester may need for you to lower some of your defenses temporarily, so that a specified IP address can probe through your firewall. If so, this should be prearranged and documented, so that it will not become an item of contention during testing.

Finally, determine general parameters for the timing of the testing. If certain parts of the test have the potential to impact system performance, get contractual commitments that these are done during off-hours.

Tip 7: Respect stakeholder limitations. You should leave plenty of time in the project schedule for explaining the penetration testing to your stakeholders and answering their questions before having a contract to sign. Through this open dialog, you will work through many of the concerns they may have. In the end, they may have certain areas that they will not allow you to test. Gather those exceptions, and write them into the contract, and let the stakeholders know that you are respecting their limitations. But if you agree to a limited test, you should explain if the results will be devalued because of it.

Tip 8: Commit to reporting to your stakeholders. Be accountable. Commit to sharing the final report—or at least an executive summary of it—with your stakeholders. You may want to provide telephone or personal briefings to avoid creating documents that could fall into the hands of hackers. This is part of the way you show confidence in your IT organization generally and in the penetration testing process specifically.

Tell your stakeholders that you will also report to them your actions to fix the discovered problems within a short period of time after receipt of the report. Pledge to continue reporting until each vulnerability has been addressed. (This could include a well-informed and well-documented decision to tolerate certain vulnerabilities.) Consider in advance and notify your stakeholders how much of this will be in writing or if you have determined that it is better for such sensitive information to not be written.

Tip 9: Know how the results will be provided. Get contractual commitments for how the results are delivered. Those commitments should include immediate notification of critical vulnerabilities, so that they can be remedied immediately. Also, if any illegal materials are discovered, requiring notification to law enforcement, you should have a written commitment to simultaneous notification to you.

Before the testing, you should make yourself aware of statutes or rules of judicial administration that legally bar the public release of such information. Knowing this will also prepare you to defend the process, because you will be able to state unequivocally whether you would have to release the information into the hands of potential hackers. If your statutes or rules of judicial administration would require release, you may need to reconsider your approach so that you can fully protect your network security.

Tip 10: Hold provider to confidentiality. Your contract language with your tester should require that the tester and all of its staff will hold in confidence all discoveries to the extent legally permissible.

Summary

In summary, use your communication skills to help judicial stakeholders to make an informed choice to accept the good that can come of the penetration testing exercise.

Author: Bruce Hermes, Director of Information Services, [Texas] Office of Court Administration, bruce.hermes@courts.state.tx.us, 512.463.1625.

Resource and Jurisdiction Contacts

Bruce Hermes, Director of Information Services, [Texas] Office of Court Administration, bruce.hermes@courts.state.tx.us, 512.463.1625.

Approved by the CITOC Editorial Board on March 15, 2007.