As value-added resellers (VARs) diversify from pure product resales to professional services, they begin to navigate new waters. One common service offering is security assessment, such as network penetration testing, or pen testing. Pen testing involves exploiting holes in a customer's network to determine its absolute level of security. This Channel Checklist provides five steps to help VARs prepare to offer penetration testing services. For a portable copy, download the .pdf and print it out.

✔ Develop a Statement of Work

Typically, penetration testing and other assessment services are based upon a Statement of Work (SOW) created by the VAR for the customer. This becomes a contractual document signed by the customer that authorizes the work to be performed. An SOW must define the test's objectives, the work to be performed and how the VAR and its representatives will interact with the customer. The SOW also defines deliverables and sets limitation on the VAR's liability. The VAR should understand that there is significant risk to the customer's network and should delineate that risk within the SOW. In short, the SOW provides rules of engagement for the penetration testing service.

✔ Create a "get out of jail free" card

Before beginning any pen test, it's important to have what is commonly called the "get out of jail free" card. Jail for the pen tester would be something going wrong during the test. It's not unheard of for corporate CIRT teams to alert their ISP and law enforcement authorities upon evidence of a pen test. This can create a significant mess for the testers. In this case, some type of electronic version of a signed authorization can be helpful.

More information

Learn more about how to offer network penetration testing services in our guide for security resellers and consultants.

This "card" is often part of the SOW, but should also include a streamlined incident response plan and a call tree so the appropriate customer contact can be alerted if there is an issue.

✔ Determine the testing objectives

There are numerous ways to perform a network penetration test, so it's important to determine the objectives of the test prior to beginning the testing process. Back in the day, it was common to just start poking around a customer's network. Today, objectives must be clearly defined. Which systems will be tested? How will they be tested? What pen testing tools will be used? Will the test take place from inside or outside the customer's network? What does the customer want from the test? These and other objectives must be defined prior to testing so there are no surprises and the customer receives the expected services.

✔ Measure twice, cut once

In carpentry, there is an old saying: "Measure twice, cut once." This saying also holds true in the world of pen testing. If you screw up your customer's network, you won't get a second chance to do it right so be careful before beginning the test. Verify all information you have been given. For example, it's common to receive a list of IP addresses to scan as part of an external pen test. Unfortunately, it's also common for there to be errors in that list of addresses. In this case, make sure that those addresses are registered to your customer. The last thing you want to do is run a pen test against some other company's network.

✔ Begin thinking about the report now

The ability to communicate findings is just as valuable as the ability to hack a network. While you may have uber-hackers on staff, your customer cannot know that unless they see results in the report. Bad reporting is a common issue with security assessments, often because the report isn't considered beforehand. Prepare a template well in advance of the testing so that it can be double-checked prior to the end of the engagement. Be sure to check spelling and grammar. It's not uncommon for clients to receive network penetration testing reports with an abundance of typos, which reduces your service's value in their eyes.