

Trusting a Pen Tester/Pen Testing Client

By Robert E. Johnston

Penetration testing is a process intended to expose the soft underbelly of a client and determine how it can be compromised. As a consumer, you engage a pen tester to evaluate the resilience of your web-facing environment. A pen tester examines that soft underbelly. What provides you with the confidence that the other party will not use the results to exploit the web-facing environment being evaluated?

Let us first clarify the matter of “penetration testing”...a term commonly misused. I have responded to many RFPs specifying a “pen test” be performed and even demanded that the individual performing the evaluation have extensive experience penetrating networks. However, upon reviewing the details of the RFP it becomes clear that the title and summary/overview is designed to impress someone, but I am never sure whom. What they are really looking for is a network security evaluation, often limited to the web-facing environment. Thus, hereon out I will refer to such activities as an evaluation and the vendor as an NSE (network security evaluator). As an aside, I have never found a client that wanted true penetration testing. The few that have wanted penetration testing, normally following an evaluation, all placed a couple of criteria on the penetration testing:

- ▲ Conduct the pen test during non-critical service hours at pre-agreed times.
- ▲ Once the pen test reaches the point of risking a server crash or other interruption in service, the test must stop.

Enough already, what about determining that the client or NSE is trustworthy? Amongst NSEs it is common to trust the client without conducting an adequate client assessment before commencing the evaluation. Heck, conducting a client assessment, never mind adequate, increases the cost/price and the NSE may not win the contract...its all about revenue. Most clients trust the selected NSE without conducting an adequate assessment of the NSE; after all that’s a task for purchasing, the CFO and corporate attorneys, but not in this case. There is too much room for error that could result in liability to either or both parties to make such assumptions.

What if a Fortune 50 company engaged a premier consulting firm to conduct an evaluation? Why shouldn’t they trust each other? Simply stated, a couple of common errors could result in the wrong web-facing environment being evaluated, possibly compromised or even damaged. How? Fortune 50 company provides NSE with a number of Class C address ranges and makes a mistake, a typing error. The trusting NSE conducts the evaluation without properly evaluating the information provided. While I am not aware of this ever happening, I can state unequivocally that

notable clients have provided me with invalid IP address ranges, I believe the result of keystroke errors. Prior to initiating my evaluation I then took the time to validate the information provided and returned to the client for confirmation.

Thus, potentially significant errors were avoided. In addition, while conducting my client validation I frequently uncover relative IP addresses/ranges that were not provided. Clearly an evaluation cannot be complete unless all addresses are identified. Thus, the NSE’s client validation is as valuable to the client as it is to the NSE. Engaging an NSE that does not conduct a thorough client validation places not only the NSE but also the client at risk. Simply stated we are speaking of “Due Diligence” on the part of both the client and the NSE. The client by insisting that the NSE conduct a thorough client validation and then presenting the result prior to initiating the evaluation provides the client with the assurance that the NSE has a proper understanding of the task at hand and that all IP addresses to be evaluated are accurate and complete. These results are of equal value to the NSE with one other benefit...that the client is not requesting an IP address be evaluated that is not their own.

Illustration A, Prior to Client Scanning/Penetration Testing Due Diligence Issues, contains elements that should be included in the NSE’s Client Validation process. The NSE should have some form of a standard Client Validation Report (CVR) that presents this information plus all of the contact information for the staff member(s) that will be performing the evaluation as well as one or more of management. The CVR should be delivered to the client and approved before the evaluation commences.

The client should carefully review the CVR delivered by the NSE validating all information contained therein including testing the NSE contact information. Should activities raise questions regarding whether there is an active attempt in progress to compromise client resources, it is important that the NSE can be reached to determine whether their evaluation is active at that time. Should the NSE be actively evaluating client resources, the NSE should be prepared to immediately stop until it is ascertained that the only activity is that of the NSE. It is possible for a potential intruder to veil penetration activity by conducting activity during the time that a legitimate evaluation is being conducted.

At the start of the engagement, the NSE should submit to the client a Release Form that contains all of the information detailed in item 1, illustration A. Upon receipt from the client the NSE should ensure that the Release Form is clear and complete. At this point the information contained in the Release Form is transferred to the Client Validation Report and validation of URL ownership and external IP addresses begins. With the advent of private domain registrations, on occasion, and likely more frequent in the future the NSE will not be able to validate ownership of the URL. Since private registration is relatively new and the process for

obtaining the ownership information varies from one domain registrar to another, this is simply another hurdle to overcome. When URL ownership has been ascertained, a discovery scan should be conducted of the URL to validate all associated IP addresses. It is likely that the NSE will discover numerous addresses associated with a URL that are not owned by the client. When this occurs, it is necessary for the client to ensure that the ISP hosting the client's web server is aware of the planned evaluation and a chain of communication established should it not be present. Not planning for notifying the ISP and establishing/verifying the chain of communication is likely to delay a schedule for weeks.


Prior to Client Scanning/Penetration Testing

Due Diligence Issues

1. Proper release form including:
 - a. Firm name and address
 - b. Detail identification of Contact Person
 - c. Detail identification of Person in Authority to authorize
 - d. Proper authentication
 - e. URLs
 - f. IP addresses to be scanned
 - g. External IP address range owned or leased from ISP
 - h. If the number of IP addresses specified in f. is less than those specified in g. (commonly the situation), why are those not included in f. excluded?
 - i. If any of the addresses in f. are not within g., determine why. A likely error or missing details.
 - j. If external IP address range is leased, clear identification of the ISP.
 - k. Initial scheduling
2. Validate release form for clarity and being complete.
3. Validate ownership of URL:
 - a. @ <http://www.internic.com/whois.html> or http://www.networksolutions.com/en_US/whois/index.jhtml. I prefer the latter as it provides detailed information from other registrars whereas Internic does not.
 - b. If ownership information is incomplete, determine the registrar and go to the registrar's web site for details.
 - c. Ownership information @ registrar should be consistent with the information collected in step one.
4. Validate external IP address range:
 - a. @ <http://www.arin.net/whois/index.html>
 - b. The ownership information should correspond to the information collected in step one.
 - c. If the address range is owned by and ISP, contact the ISP and verify that the client in fact does have the lease for the IP address range specified.
5. Document all validation steps as executed with notes. Both the form and all validation notes are to be placed on file. There really should be an accompanying checklist with space for notes and dates of completion.

Confirm the results with the client.

It is not uncommon to encounter resistance by the ISP. However, the client should insist. Vulnerabilities within a web server environment can be exploited to compromise the web server. It is essential that all components within the direct chain be evaluated. Once the evaluation is completed, the client will be in a stronger position to demand corrections to vulnerabilities that threaten their web server. When validating external IP addresses, it is not uncommon to learn that the addresses are leased rather than owned. Validation with the lessor is necessary.

Failing to perform an adequate client evaluation prior to conducting a network security assessment of a client's web-facing environment presents significant risks to both the client and NSE. It is essential that the client ensure a client evaluation is specified within the contract and that the appropriate parties within the corporation are aware of the need. Further, when evaluating potential vendors, those that do not include the client evaluation within their offering should be considered suspect. After all, it is much like getting ready to take a family outing in a motorboat. You always check to ensure that you have adequate gas, life preservers, food, water, etc. To do otherwise is very risky. Take due care going into uncharted waters when engaging a vendor to perform a network security evaluation of your web-facing environment. 

Bob Johnston has been a CISSP for more than ten years and an active member of ISSA since 1991. He has been a full-time information security practitioner for more than 30 years having spent a significant portion of that time as the senior information security practitioner in the financial services world. He has also spent more than 10 years as an information security consultant with emphasis upon policy, procedures, organization and network security.