Trustwave®
Information Security & Compliance

Need a Hug? I'm Secure.

Steve Ocepek
Charles Henderson

July 1, 2010

A Whitepaper for Black Hat USA 2010

Table of Contents

1 Introduction

Earlier this year, at the end of a decade in which the information security industry grew at an unprecedented rate, many columnists and bloggers posed the question: are we really more secure? The answer, in a large majority of cases, was a resolute "no". Indeed, it was a decade that witnessed the exposure of countless cardholder numbers, the theft of thousands of identities, and the constant exploitation of critical software. It's hard not to agree.

At the same time, e-business continues to grow at a staggering rate, only adding to the problem. Fueled by these frightening headlines, despair infects security officers, often becoming marginalized in the face of business decisions that simultaneously increase profits while greatly increasing risk. This risk is unnecessary, usually fueled by imposed deadlines, but without a strong perception of the value of information security, its advocates are often forced to meet minimal goals imposed by compliance standards.

As with any discipline that is focused on prevention, Information Security's accomplishments are hard to list. We can point to the brilliant algorithms used to secure our data, the systems we've created to detect and fix software vulnerabilities, and a number of standards that we use to maintain secure systems. Without examples of actual thwarted attacks, however, it's hard to conceptualize just how effective these methods are.

Information Security, not without good reason, is an industry filled with pessimism, greeted with disdain, and often associated with hubris. As a practitioner, it is impossible to remain untouched by frustration, and even apathy, over the course of one's career. Ironically, the most creative and engaging portions of the security field involve creating exploits and tools to perform them. Indeed, many of us ended up in this field because of our own fascination with security flaws. It is this fascination that causes us to focus so heavily on new, 0-day attacks. These flaws, unpatched by the vendor, offer a tangible, demonstrable method for proving our value as security professionals. A double-edged sword, it is the sheer number of these exploits that highlight the failure of InfoSec to get ahead of the threat. These threats also have another, more subtle and damaging effect on the security field: they distract security professionals from older, sometimes more critical, vulnerabilities.

All of these problems culminate into the general disconnect between Information Security and the industries we are trying to protect. In this paper, we will discuss ideas to combat these problems using techniques that have proved successful during client engagements. The paper focuses on penetration testing, due to the authors' experience, and the highly customer-facing nature of this particular task.

2 Challenges

Penetration testing is an opportunity. As a response to the disparity between prevention and actual effectiveness, pentesters can show their clients hard evidence that supports common InfoSec guidelines. That being said, the act of penetration testing itself includes some common pitfalls that can make this task difficult. This section delves into a number of these pitfalls and offers insights about how to avoid them.

2.1 Experience vs. Payscale

There are many choices to be made when building a penetration testing team. A number of constraints factor in here, among them the choice of whether to hire relatively inexperienced staff and train them up, or hire experienced testers that can start working on day one. Even when deciding to hire experienced staff, the wide scope of penetration testing means that every new hire will be more experienced in some areas than others.

Both methods have benefits and drawbacks, and a combination is often the best approach for most organizations. That being said, penetration tests have more complete results when performed by staff with fairly deep general understanding of information systems. Context is key here, due to the large number of relatively unknown systems that are routinely encountered while performing this job. No matter the specific experience of the tester, it is inevitable that he or she will encounter a system that is completely foreign within the first couple tests.

It is at this point that a good tester will apply their general knowledge of information systems. Experienced testers understand how software is developed, common mistakes to look for, and importantly, which methods of attack have the best chance of success. The latter is arguably the most important skill of the penetration testing discipline: knowledgeable triage. Time constraints force pentesters to make gut decisions about which way to go during a test, and only experience can guide them here. Therefore, when building a team, it is important that inexperienced pentesters are paired with veterans in order to develop general test tactics in addition to specific skills.

2.2 Quality vs. Quantity

Having worked on a team that performs hundreds of penetration tests every year, the authors can vouch for this as one of the core struggles in our profession. Each test is unique, and must be treated as such. Cultures are different, implementations are different, and each organization has its own way of looking at security. For some, it is a core value, while others clearly show that security is an afterthought. Learning the organic component of each network is one of the most important differentiators between a penetration tester and an automated scan.

Nevertheless, good reconnaissance takes time, and automation of certain tasks is vital in order to perform the job within time constraints. Factor in the large quantity of tests that must be performed every quarter to meet compliance deadlines, and the temptation is there to reduce

pentesting to a series of shell scripts and packet captures. "Express" penetration testing is gaining popularity due this constraint.

In addition to these concerns, there's a difficult moment late in a no-finding penetration test where the tester has to walk away. The most difficult aspect of pentesting is ending the test, due to the large number of potential attack vectors that will undoubtedly remain unexplored. It is impossible to explore every possible avenue of attack – indeed, one of a pentester's worst fears is a missed finding, especially if it uncovered by another tester. This is why it is extremely important to document the attack vectors explored during a test so that the tester's methodology can be fully understood.

2.3 Job Scoping

Considering the fact that many penetration tests discover assets that were previously unknown to the client, best-guess scoping methods often fall short. Most firms incorporate some sort of logic to account for a certain percentage of unknown devices, but most of these methods still rely on the number of devices as a metric. Depending on the type of applications in use, a small number of hosts can offer a fairly large attack surface.

2.4 Disruption

Of course no one likes the idea of an outsider hacking his or her network. Proving security flaws can often require the interruption of the organization's workflow. This is one of the main counter-arguments to penetration testing as a form of security assessment. To the inexperienced, pentesting can appear as egregious, unnecessarily going beyond what a vulnerability scanner can present. When the results are presented, however, it is often clear how manual processes find things that cannot be detected automatically.

The manual nature of penetration testing actually has an advantage over the vulnerability scanner in terms of disruption. This is because the tester is acutely aware of where he or she is in the testing process, and what the next test involves. Successful penetration testers involve their clients in the process throughout the engagement to ensure that production systems remain unharmed.

2.5 Communication

Indeed a good portion of this white paper focuses on better ways of communicating with the client – and "no finding" tests are a great example of how we can benefit from this approach. By gathering ample notes during the process and presenting all of the attack vectors investigated, the thoughts behind each, and what was learned during the test, the client can get a very detailed picture of their security posture. This is, in a way, the ultimate return on investment for their security discipline – they are able to see the prevention of a real attack.

This very thing, the realization that attacks can indeed be defeated, this is the bridge between where we are at as an industry, and where we want to be. Taking this a step farther, even when an attack is successful, we need to spend equal time stressing that they made an

attacker's job harder. Simply pointing at the flaw and leaving out information about all other attempts only creates more frustration and despair, missing a great opportunity to show how far they have come.

Admittedly, this doesn't apply in every case. There are many ridiculously insecure networks and applications in the world, created with little or no security discipline whatsoever. It is important to stress that this is not about making all of our clients "feel better" – instead it is about giving credit where credit is due, and not simply highlighting the exploit. The following passages, taken from actual penetration tests, help to illustrate this point.

This passage summarizes the results of a test in which a database was compromised but contained tokenized data.

Trustwave feels that, based on the results of this penetration test, the client has taken care to protect their PCI assets. Compromise of database credentials did not result in compromise of cardholder data, which demonstrates the value of well-implemented tokenization controls. Moving forward, security controls around point-of-sale databases should be further scrutinized to prevent breach by an attacker without time constraints. Special attention should be paid to any devices that handle cardholder data directly.

Another test resulted in root access inside the target network, however the path followed by the attacker was convoluted and difficult to execute.

Based on the results of this penetration test, Trustwave feels that the servers in the provided list are vulnerable to system-level compromise. While the attack itself requires a number of steps to execute, this test proves the importance of layered security. With less access at any stage of the exploit, the attack may not have been successful. As it stands, there is just enough access to gain root privileges to systems in this configuration.

Each of these challenges represents a specific area that successful penetration testers focus on during each engagement. While ignoring these challenges can lead to missed opportunities and rocky engagements, the opposite is also true. Paying special attention to these items allows a penetration team to excel in ways that will create fans out of clients, simply because they feel that they are a part of the project.

3 The Need to go in Both Directions

The threat landscape presents an endless chase: 0-day attack vectors change the game on a daily basis, while old attacks remain valid in many environments. Despite our fascination with 0-day attacks, few of these become "weaponized" in a way that makes them valuable to attackers. Real attackers look at the world in a way similar to pentesters - they go with what works. This parallel is completely intentional: good pentesting emulates the attacker's tactics and outlook as closely as possible.

It is difficult to discern the exact formula that individual attackers use when considering whether to incorporate an exploit into their own arsenals, but the decision process is generally composed of one or more of the following elements:

- Ease of exploit
- Likelihood of counter-measures
- Speed of exploit
- Detection risk
- Target prevalence

Some 0-day attacks are indeed better than others, according to this formula. Those of us who subscribe to security mailing lists have learned to quickly triage each new vulnerability according to this methodology, also taking into account our own roles. For example, an exploit against Windows desktops that requires man-in-the-middle privileges is much more interesting on an internal or wireless penetration test. Conversely, a 0-day against a popular shopping cart system is much more interesting to external penetration testers.

This brings us to the essential difference between pentesters and real attackers: scope. Where a new vulnerability is added to a tester's "backpack" for use when the opportunity presents itself, attackers can begin testing immediately. Not constrained to a particular client, attackers can sweep large swaths of address space and perform wide-spread queries for specific filenames to exploit these vulnerabilities. In this way, the readily exploitable 0-day simply becomes another hunting tool. Casting as wide of a net as possible, their reconnaissance can include any number of attacks, of any vintage, in order to locate and reliably exploit targets. Attackers, in some ways, are skeptical of 0-day exploits until they have been validated on an actual system. Compared to the tried-and-true, which can include exploits of any age, these new attacks have to prove themselves as uniquely useful before they will supplant other vectors.

When we are able to clearly separate the mentality of the career hacker from the career attacker, we realize that their ultimate goals are very different. While the hacker is interested in new attacks, solving puzzles and trying to gain access where it should be impossible, the attacker focuses on actual results. This drives the attacker to consider reliability above all else, regardless of the age of each individual vector. Certainly there are many types of attackers – some that target individual organizations – but the prevalence of phishing scams, botnets, and mass-targeted malware clearly demonstrates that the majority of attackers focus on reliable, time-tested methods.

4 Real-world Application

If we are going to build a better bridge between InfoSec and our clients, much of this work will undoubtedly be placed on the shoulders of penetration testers. As stated earlier, the act of proving actual vulnerabilities in an environment greatly increases the organization's impetus to fix these problems. That being said, we believe a number of issues, based on material presented here, are preventing penetration testing from realizing its full potential.

4.1 Strong Reconnaissance

One of the most valuable deliverables of a good penetration test is the recon sheet. A spreadsheet or diagram of the environment, this document shows what is visible from the outside looking in, and provides a great deal of insight into the information that a potential attacker is working with. Strong recon also allows the tester to create a priority list of attack vectors. Equipped with a better understanding of what is there, the tester can try specific tests rather than relying on blind methods.

Successful penetration testers are very aware of their time limitations, and therefore take this step very seriously. Failure to properly recon an environment and apply appropriate tests can result in random results, since no test can blindly test every possible attack vector. The most dangerous result of a random test is an easy miss: a glaring flaw that is not exploited due to lack of visibility. This is akin to failing to enter a building through a locked second story window, while the front door remains unlocked.

4.2 Balance between Manual and Automated Methods

Lack of visibility often stems from over-reliance on automation. Scanners are very useful time-savers in any test, though the informational findings should be considered in addition to any exploit messages these programs generate. Using a scanner to better understand the environment is a vital part of reconnaissance, but when they are used for their vulnerability testing abilities only, they tend to fall short. Like any scanner, false positives and negatives must be taken into consideration: the job of a pentester is to serve as a buffer between these results and the client. Any positive results should be distrusted until the tester can successfully exploit the finding. This is our job.

4.3 Controlled Exploit Testing

Alongside scanners, automated systems exist that attempt to exploit each discovered host with every possible vulnerability, based on a built-in decision-tree. "Autopwn" scripts that do this are not inherently bad things, but can easily run amok in production environments. Attackers don't have to care about this, but it reflects poorly on penetration testing as a discipline when we don't have control of our own tests. It's important that we maintain control of our tests, and schedule this type of testing on a subset of clients beforehand.

4.4 Client Visibility

This brings us to one of the most important aspects of penetration testing: the client's visibility. There is definitely a fine line here. Say too little, and the client doesn't see the value of the test, but checking in at every possible opportunity will quickly become excessive and drag the test on. Knowing when to contact the client is a skill that experienced pentesters stress as one of the most important, and each pentester will handle this a little differently depending on their style.

To set expectations, a set of guidelines should be agreed upon at the beginning of the test, and the tester should have a strong say here. After all, the pentester knows better than anyone that "call me before you do anything," while it looks good on paper, is setting the client up for a long, difficult test. Any test with this hard requirement (such as government work) is usually best-performed onsite with a representative setting next to the tester. These are rare situations however, and often the client just wants to ensure that their network won't suffer an outage during the test.

Getting this right means that the client representative feels involved, and will feel like a part of the test. Indeed, this is where most tests fail to capitalize on the opportunity – this is likely the most engaged in information security that the client has ever been. This means reporting failures and successes equally. The most valuable tests are able to express the following:

1. This is what we saw
2. This made us decide to test for vulnerability "x"
3. We met resistance from counter-measure "y" during the exploitation phase
4. We did/did not circumvent this counter-measure

Not only does this methodology show a return-on-investment for each counter-measure, but also it gives a full picture of how the pentester viewed the network as an outsider.

5 Conclusion

As stated earlier, it is impossible to test every possible attack vector. Indeed, all penetration test contracts include this clause – which causes some detractors to ask, "What is the value?" A penetration test is not, cannot, be a guarantee against compromise – nothing can guarantee that. Pentesting provides a window into how vulnerable the environment is from the perspective of a skilled attacker. Thus it is critical that this window is as transparent as possible – it is, in a very real way, the entire value proposition.

The value of penetration testing is not a Boolean – it can't solve all of our problems, nor is it without value. From personal experience, we know of specific security flaws that once existed and are now resolved thanks to our ability to test these environments and present our findings. Over the course of the authors' career, neither has found a more effective way of solving security issues than what penetration testing offers.

That being said, our profession is at a critical point in its development. Automated systems are becoming smarter and more effective at discovering flaws, and some are turning away from patching in favor of cloud computing in the misguided hope that giving away ownership means increased security. The only ones who aren't changing their methods are real attackers, who have long had a culture of innovation, incorporating the best new attacks alongside legacy vectors that just work. Penetration testing offers a way for clients to tap into this successful methodology as well, with one important distinction: it gives them the final word.