WHITE PAPER

eLearnSecurity
Forging security professionals

CHALLENGES

Protecting company systems and data from costly hacker intrusions

Finding tools and training to affordably and effectively enhance IT security

Building More Secure Companies (and Careers) with Penetration Testing Expertise

TAKEAWAYS

Why penetration testing is an extremely efficient way to improve your IT security

How hackers are damaging companies and what it could be costing you

What to look for in a penetration testing course

How Your Current IT Security System Might Be Leaving You Exposed

What's in this paper?

Introduction: The Need for Security

Security in cyberspace is a necessary fact of life. It's big news when a hacker attacks a notable target – TJX, Google, or a major bank or credit card company – but in the same way that a major bank robbery makes the news and a mugging doesn't, there are constant low-level attacks against smaller organizations that are very harmful.

Many low-level attacks go unreported, and a fair number of them go completely unnoticed. That doesn't mean they are any less damaging – in fact, the attack you don't know about will do more damage, over the long term, than the one you do know about.

Advanced Persistent Threats, a widely used term to describe these kinds of attacks, are attacks of varying degrees of sophistication that go unnoticed over a long time period.

The cost of these breaches tends to be higher than initial estimates. This is due to greater cleanup and remediation costs, and possibly the loss of confidential, proprietary information that occurs over the extended period of time that the hacker has access to the victim's network.

Estimates are that every record breached costs a company $40, a number that rises steeply when the records include credit card or social security numbers. And a single successful hacker attack might get thousands, or tens of thousands, of those records, potentially costing the company significant money, eroding customer trust and damaging brand equity.

Your organization spends a considerable amount to defend against these threats, but the only proven way to gauge your effectiveness, is to test or audit the security with a procedure known as penetration testing.

This whitepaper discusses the benefits of penetration testing and how developing a skill set in this critical and often-overlooked discipline will add value to your organization and enhance the effectiveness of your IT security spend. The best way to acquire that skill set — the types of courses available, and what to look for in a good one — will also be covered.

The Threat

Hackers attack in a number of ways for a number of reasons. Probably the most visible, and often the most harmless, hacker is simply in it for the notoriety – by defacing a web page, for example. However, contemporary incidents are becoming fewer and farther between.

Considerably more dangerous to your organization are thieves, who won't break a system if they can help it, but will quietly steal credit card records, identity data, and proprietary information. They can be hired by a competitor or be motivated by their own economic interest.

To break into systems, hackers employ a wide – and constantly evolving – range of approaches. Vulnerabilities are discovered every day, and most intrusion detection systems (IDS) or vulnerability scanners can keep up with that pace. However, techniques also evolve and attack trends change year over year.

Your organization needs to protect itself against:

- **Service detection and vulnerability scans**: The attacker rapidly checks computers on your corporate network for known weaknesses and vulnerabilities that can be exploited to gain unauthorized access.
- **Client side attacks**: These are attacks to your employees' workstations. Attacks like these are the rising trend of 2012, exploiting both human and software vulnerabilities.
- **Attacks to your website**: It is estimated that 70% of attacks begin with hacking attempts on the corporate website and its subdomains. SQL injection and similar vulnerabilities are still an easy way to retrieve data from corporate databases.
- **Worms and viruses**: Self-propagating programs that often create back-door access to servers and workstations within a network.

Countermeasures

Against these threats, your company employs a number of solutions. Some of these include:

- **Anti-virus and anti-malware software**, whose purpose is to detect (and remove) worms, viruses and trojan horses.
- **Access control**, which limits user privileges so that if a hacker gains access to a part of the system, their access is limited to only that part.
- **Firewalls**, which restrict the traffic that can pass through them, based on rule and permission sets.
- **Encryption**, to protect against packet-sniffing for passwords.

- **Intrusion detection systems**, which scan a network for users that shouldn't be there, or who are behaving suspiciously.

Although necessary, these systems are complex and expensive; according to Forrester Research, North American companies spent $31 billion on security in 2010. Hacking tools and techniques are constantly evolving, so security measures need to keep pace.

The Value of Penetration Testing

Data protection doesn't operate itself. System maintenance is necessary, to update patches and updates as new vulnerabilities are discovered. Incident response happens when an intruder does get in – locking out a presently-in-system intruder, or dealing with the aftermath.

A system looks different from the outside than it does from the inside. Considered much more thorough when compared to a security audit, penetration testing examines the system from the viewpoint of a potential attacker.

Essentially, penetration testing lets you know of weaknesses in advance, allowing you to find and fix them before a hacker discovers and exploits them. This ranges (depending on the level of testing desired) from the most obvious and common approaches, for example, passwords that have been left as the default are very easy to change to more difficult passwords – through complex attacks.

Moreover, penetration testing is the most efficient way to understand the real risk to which your data is exposed. There's no way to accurately gauge this risk without mimicking an attacker with sophisticated skills.

While a vulnerability scanner only scratches the surface, penetration testing is a methodical process of verifying actual exploitability of all weaknesses. The exploitation of each vulnerability will provide the penetration tester access to networks and computers to which a vulnerability scanner would never have access.

In short, penetration testing ensures that you're getting value from your security spend. It allows you to deny hackers the low- and medium-hanging fruit that can severely compromise your security and prepares you to mitigate and avoid even the most advanced attacks.

Pen Testing vs. Hacking

In years past, penetration testers were called “ethical hackers.” And on the surface, penetration testing does look a lot like hacking. However, the disciplines are distinct; much like a locksmith is from a lock-picking criminal. Penetration testers employ many of the same tools that a hacker does, but unlike hackers, penetration testers work under strict rules of engagement – they go into specific areas only, and have limits on their actions. The purpose is to discover weaknesses, not break into the system for its own sake.

Hackers operate with a view to getting into the system at all costs; a pen tester’s role is to probe for correctible weaknesses in the system and improve its overall security.

A penetration tester is a professional who can also suggest and advise the most appropriate and cost-effective countermeasures for each discovered vulnerability. A penetration testing report is the confidential document delivered to the corporation, showing executives as well as IT departments what needs to be done to solve the discovered security issues.

In-house vs. Outsourced Penetration Testing

There is ongoing a debate about whether a company should hire an external company over using internal staff to perform penetration testing. Both approaches have their pros and cons.

An external company whose core business is penetration testing is surely specialized and can deliver a much better result if you don’t have a trained staff.

However, many privacy and data access issues arise from this approach.

A security audit that simulates a hacking attack is likely to come across sensitive data. It could be customer records, credit card numbers or competitive information, but it’s going to be data that hackers would seek. Because the outside penetration tester is under a contract doesn’t mean you want them to have access to the information any more than you’d want a trusted, but not cleared, internal employee to have that information.

There are also political reasons - a security audit is going to bypass the protected elements of your security and discover those that aren’t. Most security systems contain a hole or two, but it’s going to be less embarrassing to have those revealed by an insider.

Finally, there's the element of cost. An externally run security audit will cost you anywhere from thousands to tens of thousands of dollars – even for very small engagements. And audits will need to be performed regularly, as new capabilities (thus, potential security weaknesses) and upgrades are added to your network. In the long run, if you want to perform periodical penetration tests, the costs of external penetration testing can be difficult to justify.

Having an in-house employee or a team of employees run the penetration testing will save the company a lot of money over the long run. Being an in-house employee who can run penetration testing will add meaningful value to your organization, as well as to your value within the company. Additionally, building in-house competencies can be cost-effective if properly done.

Becoming a Pen Tester

So how do you acquire the skills needed to become a penetration tester for your organization? Like any skill set, there are a number of ways:

- Books have been written on the subject.
- You can take courses at your local college.
- You can find an existing mentor and learn as an apprentice.
- You can take a specialized course in the subject.

For a busy professional with other responsibilities, finding a mentor may be difficult and a college class isn't likely to be specific or action-oriented enough. Books are updated every two or three years, and are therefore often obsolete and missing any practical training. Your best approach is to go through a specialized course and earn a penetration testing certification.

What to Look for in a Course

Penetration testing is a hands-on skill set; you can't learn all of it, or even most of it, from a book. A competent pen tester uses a number of tools, techniques and skills in the course of his work.

A good penetration testing course will give you the subject matter, but it will also allow you to apply that knowledge, turning academic understanding into hands-on expertise. Active exercises and sandboxed environments are important – you want to

be able to test your skills with real tools, in a realistic virtual environment, before applying them in practice.

But that expertise is only one element. You also need to gain a broader understanding of how hackers think; information security is about protecting assets from threats, and that's hard to do when you don't comprehend the threat in the first place.

Also, computer security is a rapidly moving field. You'll need to stay ahead of the latest threats and defensive measures; a good penetration testing course will keep you engaged and updated even after completion, allowing its value to you and your organization to carry on well into the future.

Finally, you want a comprehensive course. The actual penetration testing is an information-gathering exercise, and information is only actionable when it's reported usefully. Your course should teach you how to accurately and constructively report your findings – "I got in through a loose port" is much more relevant and actionable when you can advise on how to tighten that port. A good penetration testing course provides a full end-to-end grounding in all aspects of a security audit.

New and Old Methodologies

A course that teaches only the latest approaches is good, but it's not sufficient. Hackers don't just use the latest approaches; they consistently breach networks and inflict damage through techniques that date back a decade or more.

One of the most popular methods of the infamous hacker group Anonymous, for example, is called a SQL injection. That's been known since 1998, but modern networks are still falling victim to it.

Don't make the mistake of learning to defend your systems against the equivalent of artillery and nuclear weapons while ignoring older and more primitive weapons. There are hackers out there still using the equivalent of catapults, and those people can cause as much damage to your system as someone using a more modern approach.

An effective penetration testing course also needs to be comprehensive. You want to take a course that trains you to secure your organization against any threat, whether it's brand new or a decade and a half old. Your course should cover everything from SQL injection to the latest Wi-Fi cracking technologies.

Summary

It's a dangerous world out there, and IT security is critical. Your organization spends a lot of money and time on IT security, and for good reason.

But that spend may deliver value – or it may not. You don't want to find out that your network is insecure only once you've been hacked. Regular security audits and penetration testing are a necessary part of your defensive IT strategy, and it behooves you for a number of reasons to handle them in-house.

Learning penetration testing can be done via coursework, and will enhance your value to the organization. But you need to choose the right course; you want one that gives you hands-on experience and a thorough understanding of where threats originate. You also want one that delivers a solid grounding in all the ways an attacker might breach your security, from the newest to oldest — but still harmful — techniques.

About eLearnSecurity

Based in Pisa, Italy, eLearnSecurity is a leading provider of IT security and penetration testing courses for IT professionals. eLearnSecurity advances the career of the IT security professional by providing affordable top-level instruction. We use engaging eLearning and the most effective mix of theory, practice and methodology in IT security — all with real-world lessons that students can immediately apply to build relevant skills and keep their companies' data and systems safe. For more information, visit http://www.elearnsecurity.com.

© 2012 eLearnSecurity S.R.L
Via Carnelutti 11
56124 Pisa, Italy

For more information, please visit http://www.elearnsecurity.com.