Using penetration testing to enhance your company’s security

John Yeo, Trustwave

Based on the fundamental principle that prevention is better than cure, penetration testing (pen-testing) is essentially an information assurance activity to determine if information is appropriately secured. Conducted by penetration testers, sometimes referred to as ‘white hats’ or ethical hackers, these tests use the same tools and techniques as the bad guys (‘black hat hackers’), but do so in a controlled manner with the express permission of the target organisation.

Depth of vulnerabilities

The aim of the exercise isn’t simply to determine whether it’s possible to break through an organisation’s defences, but about identifying the breadth and depth of vulnerabilities. Naturally a major focus is offering detailed and accessible recommendations to improve an organisation’s overall security posture. Aside from assessing the risk of the more technically oriented findings, typically root cause analysis will be provided as part of a report, and this has a tendency to be more business focused around shortcomings in the organisation’s overarching information security strategy. Examples include why a password policy is insufficient, or highlighting inconsistent patch management.

Any organisation with sensitive information, such as customer data, Personally Identifiable Information (PII), payroll data, payment card data, intellectual property or trade secrets should probably be incorporating penetration testing within their wider governance, risk and compliance activities. Specialist organisations conduct penetration tests against networks and applications for many different types of sensitive data using a primarily manual testing process (see Figure 1 for an outline of the process used).

One of the prominent drivers for conducting regular pen-testing is PCI-DSS compliance, which outlines requirements for penetration testing activities to validate the security controls in place. Other drivers include businesses wanting to validate the resilience of a new IT environment or perhaps following a major change. Fundamentally it’s driven by the desire to ensure the company’s assets and data are well protected from attack. We know that being the victim of data breach can impact a business’ top line revenue through negative press, and in some industries the risk of regulatory fines is also at play – no one wants to become the next data breach headline.

Those companies with more mature approaches to security will tend to have proactively incorporated the use of pen-tests into their strategy. At the beginning of each year, they’ll have a relatively clear roadmap including the network environments and most critical web applications that require pen-testing, how frequently they should be tested, and when. Others adopt an ad hoc approach, sometimes just before a new system goes live or as part of their annual PCI review. The latter frequently just focuses on the infrastructure associated with payment card data and may leave the remainder of the network untested.

Vulnerability scans versus pen-testing

A common area of confusion is the relationship between vulnerability scanning (automated) and pen-testing (expert-driven manual testing). Both involve a proactive and concerted attempt to identify vulnerabilities that could expose the organisation to a potential malevolent attack.

Vulnerability scanners are great at identifying ‘low-hanging’ vulnerabilities, such as common configuration mistakes or unpatched systems, that offer an easy target for attackers. What they are unable to determine is the context or nature of the asset or data at risk. They are also less able than humans to identify unknown-unknowns (things not already on the risk register, or which haven’t been theorised by the organisation as potential security issues). Good pen-testing teams, however, do this very well.

For instance, pen-testers can give countless examples of engagements where an environment was previously scanned only for vulnerabilities. When the same environment is subjected to a pen-test, the pen-testers manage to compromise a number of systems, gain unauthorised domain administrator or
root access to systems, and ultimately gain unauthorised access to sensitive data. One final distinction is that vulnerability scans are unable to process certain types of security issues, such as subtle business logic flaws that would require a human’s understanding of how a particular workflow or process is supposed to work in order to exploit it.

In truth, both are required – vulnerability scanning as a frequent (eg, monthly or quarterly) baseline activity and pen-testing as the more detailed exercise, perhaps once or twice per year, depending on the assurance objectives. The point is an experienced security tester, ethical or not, often finds critical and high-risk vulnerabilities in environments that regularly undergo automated vulnerability scanning.

**Different types of pen-tests**

The most common types of tests are either directed at network infrastructure or a specific application. A network pen-test typically includes entire networks and many hosts, sometimes crossing over geographical boundaries. This type of testing is usually conducted both externally, against Internet-facing servers and supporting infrastructure, and internally, against internal corporate information systems assets including servers, workstations and IP telephony systems.

Application testing on the other hand involves a targeted assessment of an individual, usually web-based, application. The application may be accessible just to the company’s own employees, third parties or partners, or it could be facing the Internet and available to all, such as an e-commerce website. Conducting this type of testing will require the authentication credentials so that each role or privilege level within the application can be tested. This will enable the tester to ensure that, for any given user role, that role cannot create, read, delete or update data in an unauthorised manner. Most organisations possess numerous web-based applications, not just the corporate website, that could be potential entry points for attackers.

The recently published Trustwave Global Security Report, which gleaned results from 2,000 manual pen-tests globally, revealed that SQL injection and business logic flaws are the most common web-based vulnerabilities that testers regularly identify.

“Some 5% of all passwords involved some variation of the word ‘password’ – ‘Password1’ was the most commonly used because it satisfies the complexity rules for many systems”

On top of this, as more and more organisations begin to implement Bring Your Own Device (BYOD) policies, pen-testers are increasingly required to conduct Mobile Application Penetration Testing. This would involve the testing of Android, iOS and BlackBerry applications that can help organisations pinpoint and correct flaws in their mobile applications as well as understand the risks posed by new mobile platforms.

There are numerous other types of penetration testing that include social engineering, physical security testing and password security testing. In 2012,
Trustwave did over two million network vulnerability scans and found that some 5% of all passwords involved some variation of the word ‘password’ – ‘Password1’ was the most commonly used because it satisfies the complexity rules for many systems including the default settings for Microsoft’s widely used Active Directory identity management software.

What makes a good pen-tester?

Defining the required body of knowledge that a penetration tester needs to know is quite difficult to describe succinctly. Certainly some typical traits are a strong theoretical computer science background and an extensive and broad foundation of practical knowledge with respect to operating systems and software used within the enterprise. Naturally on top of this needs to be layered an in-depth knowledge of attack and penetration techniques that don’t always lend themselves well to being assessed through typical interview scenarios. Therefore many hiring managers will look for candidates with a minimum level of experience working in a full-time penetration-testing role with companies the manager holds in a high regard. Also it is not unusual to have an ‘assault course’ type of practical assessment as part of the interview process to determine whether a candidate can ‘walk the walk’.

One very important aspect is mindset; it’s not uncommon for a particular security control to require a level of creativity and persistence in order to circumvent or bypass; or to have to think outside the box to exploit a seemingly unconnected set of vulnerabilities together in order to gain the most privileged levels of access to systems and data.

What happens in a pen-test

Due to the many laws and regulations that address hacking, very specific discussions happen between a penetration tester and an organisation. Before any engagement starts, both the tester and the organisation clearly define what systems or targets they are trying to access. There must also be in-depth discussions of the risks involved in a penetration test, and one of the key questions to be asked is whether there are any highly sensitive systems that could be impacted. Although the penetration tester is essentially trying to mimic a real-world attack, they do not want to disrupt any business processes; however, due to the nature of the work this sometimes cannot be guaranteed.

Once the target systems have been agreed upon, the first step in a penetration test is reconnaissance or asset gathering, which is the process of identifying visible assets that the penetration tester can access. The aim of the recon is to go from knowing nothing about the target network to possessing a detailed inventory of its systems and services. No attempt to gain access is performed at this stage.

Once the recon phase has been completed the results are used to identify potential weak points within the network and prioritise the next step – vulnerability identification. This is the complex part, where the lists of potential targets are examined to find vulnerabilities. The techniques involved with finding vulnerabilities can be very diverse and some are more accurate or more passive than others, but this is the stage where the penetration tester becomes more interrogative. One such method is through packet sniffing, which is the process of capturing packets of data flowing across a computer network to gather information about that network. Packet sniffing can potentially capture data such as passwords or re-playable password hashes (often these would require cracking), IP address and protocols being used on a network as well as other information that can help the penetration tester infiltrate the network.

“The testing often creates an ‘attack sequence’ where stepping stones of chained weaknesses are combined to prove the cumulative resultant risk is real”

Following this, there should be a list of probable ways in to the target network, and the next step is to begin exploiting vulnerabilities within systems. In internal penetration tests this does not necessarily mean directly attacking the target – it could involve finding ways in through other connected services, systems or networks that weren’t necessarily the primary target. This simulates the actions a real-world attacker could take, although this similarity is limited by the professional nature of the service which requires that any ‘no go’ areas are agreed beforehand. Again, there are numerous

Continued on page 20...
ways that a system can be exploited, whether it is through vulnerable services, weak password policies or a multitude of possible control weaknesses and failures.

Ultimate goal

The ultimate goal of the penetration tester is to identify gaps in security posture, and use exploits to get in to the target network and gain access to sensitive data. The definition of sensitive data clearly depends upon the client organisation requesting the penetration test. Because the route taken to achieve this goal may not have been direct, the testing often creates an ‘attack sequence’ where stepping stones of chained weaknesses are combined to prove the cumulative resultant risk is real.

“By incorporating pen-testing activities as part of a wider information security strategy, organisations can validate the robustness of their security controls and identify as yet unknown risks to their business”

In the process of exploiting systems, it is possible the penetration tester’s view of the network will be different to when the engagement began. When this happens, a second phase of reconnaissance is started. If this second (or third or fourth, ad infinitum) phase of recon identifies new systems to exploit, then the process of the test will continue, with the iterative progression focusing upon gaining access to the targets or, in some scenarios, establishing how deep the rabbit hole goes.

Choosing a pen-tester

Clearly, choosing a trusted partner to conduct pen-testing is itself a sensitive matter and the area of professional penetration testing is still relatively new and somewhat unregulated. For instance, it lacks a central governing body on professional standards when compared with more established professions, such as financial auditing. Some accreditations do exist, such as those offered by CREST (Council of Registered Ethical Security Testers), however it is a chiefly UK-centric accreditation at both company and individual level.

Given the relatively low barrier to entry for organisations claiming to be expert penetration testers, reputation and industry standing is of utmost importance when selecting a provider. And while there are a number of high-calibre individuals working for boutique security consultancies, organisations should seek well established penetration testing providers with well documented methodologies, careful recruitment policies, established references and track record for delivering the full spectrum of advanced technical security services.

By incorporating pen-testing activities as part of a wider information security strategy, organisations can validate the robustness of their security controls and identify as yet unknown risks to their business. The results of a pen-test and guidance provided, helps organisations better protect sensitive data from falling into the wrong hands.

About the author

John Yeo is EMEA director at Trustwave, a cloud-based compliance and information security solutions provider. He has extensive professional information security expertise with a particular focus on large application security programmes and enterprise-class penetration testing service delivery. He has run and managed multiple outsourced global security assessment programmes for large corporations. Prior to his management roles, Yeo has delivered technical security consultancy and led security testing assessments for major IT programmes within both government and the private sector.

2–4 May 2013
Hackito Ergo Sum
Paris, France
hackitoergosum.org

23–24 May 2013
Source Dublin
Dublin, Ireland
https://www.sourceconference.com/dublin

25–26 May 2013
LayerOne
Los Angeles, US
www.layerone.org

4–7 June 2013
CyCon: International Conference on Cyber Conflict
Tallinn, Estonia
http://ccdcoe.org/cycon/

10–12 June 2013
ISACA Insights 2013
Berlin, Germany
www.isaca.org/insights2013

27 July–1 August 2013
Black Hat USA
Las Vegas, US
www.blackhat.com/us-13/

29–31 July 2013
Secrypt – International Conference on Security and Cryptography
Reykjavik, Iceland
www.secrypt.icete.org

1 August 2013
DefCon 21
Las Vegas, US
www.defcon.org

20–23 August 2013
OWASP AppSec EU Research 2013
Hamburg, Germany