Whitepaper: Penetration Testing

Penetration Testing -
A Guide to Achieving Better Outcomes

Date: March 2016

Doc Ref: SOS-WP-PTG-1631

Author: Murray Goldschmidt

Author Title: Chief Operating Officer

Table of Contents

1 Overview

Our reliance on information technology has been increasing over time. The market is demanding instant access to data and the ability to interact. As supply must meet demand, organisations that wish to participate with market dynamics have seen rapid changes to the profile of their networks and applications (systems). Cloud computing, Voice over IP (VoIP), wireless networking and mobility solutions are now standard business requirements. Emerging technologies such as the Internet of Things (IoT)[1] will see further transformation of our personal and corporate networks to accommodate our appetite for data-on-demand. For many years already, the perimeter of the network is no longer defined. The internal network is not secure. What was once an internal application, and thought to be secured from harm by perimeter security controls, is now likely to be exposed to the internet and accessible online. Even industrial control systems (ICS), that were once operating in air-gapped networks due to their importance for the continued operation of our critical infrastructure, are now increasingly more connected. The adoption of mobility solutions and the applications developed for them are compelling for convenience and remote access.

Along with great benefits associated with developments in technology, risks follow because complex environments are never immune to security flaws. As the Internet population and the availability of online content grow at an exponential rate, there is also an increasingly large pool of (miscreant) talent looking for opportunities to identify vulnerabilities to exploit.

The cyber threat landscape is certainly changing at high frequency. Attackers are devising new and novel approaches to circumvent the controls that we put in place to protect and our systems. As we bolster our perimeter defences making it harder to penetrate our systems from the outside, attackers will focus on an easier path to the data that they want to compromise. Increasingly our people, trusted employees, subcontractors and suppliers are targeted. Their inherent higher privileged access to critical systems, and human nature to be inquisitive or trusting, make people highly susceptible to social engineering. This is likely to be the initial attack vector to a more sophisticated cyber-attack that can then be leveraged to penetrate deeper into networks.

Accordingly, organisations are faced with the task of ensuring that their information security management capability is robust, comprehensive and able to meet the ongoing demands of compliance and regulation. And to do this, organisations need to adopt a risk and data centric approach to security rather than looking at systems in isolation. In particular, it should be clear what is being protected, and the business implication of a security breach. Many organisations struggle, or fail, to identify what there sensitive data is, where it is and who has access to it. This in turn can lead to ill-informed investment in security controls and assessment activities of which, penetration testing plays a vital role.

[1] The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data

2 Penetration Testing - What is it?

Penetration Testing includes a series of activities (see Methodology in Section 9.1) with the objective of determining the current technical security posture.

The effectiveness of protective controls is evaluated, which can in turn be used to deduce the effectiveness of detective and responsive controls. Furthermore, this testing can identify opportunities for improvement in information security governance.

For example, the findings may identify areas in application development where security was lacking or possibly where inadequate diligence in change management has resulted in insecure settings being enabled on systems which may have resulted in, or contributed to, a compromise.

3 Why do it?

"Foolproof systems don't take into account the ingenuity of fools." — Gene Brown.

Systems in general are recognised to comprise a combination of People, Process and Technology. Failings in any of these can lead to weaker systems with the possibility that the weakness may be exploited. Since systems are complex, technology is buggy and people are fallible, insecure deployments abound. Public facing systems are subject to the scrutiny of an almost unlimited pool of evaluators, many with a lot of time on their hands, and some with dubious motives, stealth, persistence and financial resources.

Each entity’s cyber threat profile will differ, depending on the industry you operate in, the type of data you process or store, the secrecy of your operations, your affiliations and political status. This profile will be relevant to the class of threat actors that you need to defend yourself against. Well known cyber threat actors include:

- Cyber terrorist – An actor that carries out an attack designed to cause alarm or panic with ideological or political goals.
- Hacktivist - An actor that performs attacks in order to draw attention to a cause (such as free speech, human rights or the environment), or hinder the support of a cause.
- Identity Unknown - Actor is not identified either by handle or affiliation.
- Individual - A specific person or group acting on their own, and not a member of any other Actor threat category.
- Information Security - Includes organisations or persons from, or whose actions affect, the Information Security sector. These are security researchers, computer scientists, antivirus vendors, CERTs, threat intelligence (non-state-sponsored).
- Law Enforcement/Authority - Will include anyone involved in law enforcement (police, police cyber-crime units, courts, judges) as well as lawyers.
- Organisation - Organisations not specifically associated with information security but having some effect over the information security space.
- Organised Crime - Groups of criminals that intend to engage in illegal

activity, most commonly for monetary profit. Attacks are designed to either extort money from the target, or the actors are funded to carry out an attack. Attacks to undermine a competitors capability to operate or outright theft of intellectual property and now rife.

- State-sponsored - The Actor or group is employed by the government of a nation-state with motives for political or economic gain.

Depending on the effectives of your current capability, your organisation could succumb to a relatively unsophisticated cyber-attack if your systems are vulnerable to a well-publicised issue for which exploit kits are readily available for download. However, while sophistication of attacks in general is increasing, sophistication and funding are not requirements to cause cyber damage. Botnets can be hired to deliver distributed damage, exploit code is freely available and there are many soft targets.

In the alternative, even heavily fortified environments may be compromised because cyber threat actors including nation states and organised crime can pose a significant threat considering the resources they can muster.

Internal systems may also be manipulated by trusted employees or subject to abuse of disgruntled staff, or possibly even be compromised through malicious software inadvertently introduced into the environment through poor controls. Compromised internal computers are likely to be remote controlled and the point through which sensitive data is exfiltrated to attackers on the outside. The internal network is not secure. There is no perimeter. This is the issue of cyber security.

The growth of cyber-attacks on private and public sector organisations, locally and globally, is very real and reported to continue. A security breach could have broad-ranging negative consequences for an organisation including disruption to business, reputational risk, revenue loss, and potential regulatory implications. For example, in 2015 there were five healthcare mega-breach disclosures, which together exposed nearly 100 million records of Personally Identifiable Information (PII) patient data [2].

Over the years, the sophistication of attacks has increased. And as systems are increasingly interconnected, the exposure to the threat has increased accordingly. Attackers are using advanced persistent methods with a bevy of tools, not only automated and technical, but they are also targeting the element of human weakness through conniving tricks to gain the confidence of a victim and to socially engineer their way to success.

Organisations, government and commercial alike, have a duty of care to protect sensitive information. But organisations need not leave themselves in an exposed position. According to one law enforcement body, “Some 90 percent of data breaches could have been avoided if organisations conducted penetration tests” [3].

Certainly all these items, notwithstanding any one of them in isolation, warrants the security capabilities of systems to be tested, in a controlled manner, under contract, and by suitably qualified and independent personnel/companies.

[2] Michelle Alvarez, “The Year of the Health Care Industry Security Breach,” *Security Intelligence*, 01 December 2015. https://securityintelligence.com/the-year-of-the-health-care-industry-security-breach/

[3] http://www.crn.com.au/News/278512,police-pen-tests-could-thwart-90-percent-of-breaches.aspx?eid=4&edate=20111101&utm_source=20111101&utm_medium=newsletter&utm_campaign=daily_newsletter

4 Effectiveness of Outcomes

In order to achieve the best outcome one has to understand the four dependencies: Limitations, Constraints, Deliverables and Capability.

4.1 Limitations

Penetration Testing is conducted as a point-in-time exercise. Accordingly, the results will only reflect the status of the system at the point it was evaluated. Therefore, the testing of dynamic systems needs to be carefully considered and planned.

Penetration Testing is in the category of negative testing, because it only proves the presence of a flaw. It will not prove that some other flaw doesn't exist. Of course the number of flaws detected is also limited by the time spent evaluating the system and the capability of the assessor which are classified as constraints (see time and capability sections further on).

Funding is also recognised to be finite. While cyber criminals may have substantial resources backing them, organisations across the spectrum of government and commercial sectors have defined IT Budgets from which a further pool may be assigned to testing or consulting services in general. We will refer to funding as a limitation in this section as it denotes limited funding at the global level of the organisation (the IT Budget) whereas the project budget will be considered a constraint.

The environment against which the test is conducted is also important. Frequently, organisations elect tests to be run against testing environments rather than the production environment for fear of disrupting normal business processes. However, any inconsistencies between the environments may result in certain issues going unnoticed when the system is ultimately in production.

In many circumstances, certain systems are excluded from testing, due to concerns about their sensitivity or availability. For example, "we can't test the ERP or Payroll systems in-case you bring it down". But because of concerns of sensitivity or availability, is that not more of a reason to evaluate the security of the system? Organisations with a Business Continuity Plan (BCP) or a Major Incident Process should be able to conduct more thorough testing knowing they have the capability to deal with any issues that may result.

Once testing is completed and a report is issued, the true value of the testing can only be realised if the issues are remediated. While it may be difficult to know how much time and money to allow for remedial activities before the test, there certainly should be an allocation made and provision to seek further resources (personnel and monetary) as warranted.

One of the most significant limitations of penetration testing occurs when a test was simply run to address an audit or compliance requirement. This is normally associated with a compromised procurement process, selection of a low cost (less comprehensive) supplier/resource, and lack of interest in the result other than a pass mark for an audit check box. This is an abuse of the true intention of a penetration test, which is to identify the very issues that expose an organisation to risk including those that should be addressed for regulation and compliance. This is commonly called “check box testing” or “security for compliance sake”.

4.2 Constraints

There are three constraints that will be discussed in further detail in this paper: scope, time and project budget.

4.3 Capability

The following attributes of capability will be discussed in further detail in this paper: methodology (approach), experience, skill and tools.

4.4 Deliverables

The report is the tangible product of a penetration test and therefore the ultimate result of the project will rely heavily on the quality of the report and the ability to act on it. The following attributes should be sought in the deliverable:

- Ease of use: Simply put, reports must be easy to use. Otherwise they become paperweights or put in the too-hard basket.
- Accuracy of findings: All findings must be validated; accordingly there should be no false positives reported.
- Action for remediation: Technical findings should be concise but precise. There should be adequate detail for the recipient to remediate the issue with no further research. This really comes down to the capability of the supplier to produce a quality deliverable.
- Technical & Business risk: The report must articulate both technical and business risk. This requires a deeper understanding of the organisation, the market and compliance and regulatory requirements. The executive summary must have adequate information so that it can be used as a business case for further investment (e.g. funding for remedial efforts, hardware, software etc.). In general, the report must provide information that can be communicated upwards in an organisation so that business executives can digest the contents and understand the implications of technical risks.
- Anatomy of attack: Where a system is compromised, the exact steps, replete with screen shots, should be provided to allow the organisation to reproduce the exploit. This will allow the organisation to ascertain the implication of the compromise if the testing was time constrained and no further analysis conducted.
- Root cause analysis: If a recommendation is limited to cosmetically addressing an issue, it is likely the issue will re-emerge some time later (probably with greater significance and impact). Accordingly, the root cause of the issue needs to be identified. This takes further time in research and analysis but certainly provides better value in the outcome.

5 Know Your Data

Before any testing is commenced the organisation should determine what is being protected. This requires a risk based approach whereby the information assets are identified and the implication of a breach of those assets is ascertained.

Unfortunately, many organisations don't know what their sensitive data is, where it is, who has access to it and how many interfaces or access points there are to it.

6 The Squeeze

As it has been acknowledged that resources are finite, every project is going to experience pressure (the squeeze) on one of the following inputs: scope, time, budget and capability.

As the squeeze weighs down on the inputs, the effectiveness of the outcome will be reduced to the point at which it is rendered ineffective. Effective outcomes can only be realised through achieving a balance on these inputs. Getting the balance right will be discussed further in this paper.

So this raises the question – What defines a good outcome?

7 A Good Outcome?

Could a good outcome of a penetration test be a report that didn't identify any security issues? At least the system manager could get a report validating competence and diligence in security management.

Another possible outcome is a report that has identified a spattering of findings.

Or consider a very lengthy report with a raft of findings detailing how an organisation was compromised through every vector attacked. At least with this report perhaps the organisation could secure some funding to resolve the issues and improve their security posture.

The answer is that any one of these outcomes could be a good outcome. It depends on quality of the inputs into the test. As a procurer of penetration testing services, you can only be confident of the outcome knowing that informed decisions were made on the inputs.

Certainly a report with no findings is not a good outcome if there were security issues, but they were not identified due to lack of time to find them or lack of competence in reviewing the system. For example, relying just on a scanner to identify the issues is highly limiting, given that certain vulnerabilities are undetectable through automated scanning and really require an expert to correlate the trace data to ascertain the presence of a more complicated vulnerability and then the capability to effect and attack on it.

A report with no findings is highly unlikely in our experience, even if a system is not compromised. There is always room for improvement and actions that can be made to make a system more secure.

Consider the importance of the inputs that will enable you to make informed decisions. Get the balance right in terms of scope, capability, time and budget.

8 Breadth & Depth of Scope

A risk based approach will identify the scope of testing in breadth and depth. The breadth of scope will determine the number of systems, technologies or techniques to be assessed. The depth of scope will determine the number of attributes or complexity to review.

For example, in breadth you may consider testing at the network layer, application layer and also social engineering. In depth you may consider testing external and internal networks, only web applications (but all interfaces including administration, web services and content management for all roles and pages) and a single element of social engineering (e.g. client side attacks).

More time will be required to review the systems as breadth and depth is increased.

The problem with selecting a very narrow scope for the test is that there are very likely to be other attack vectors, potentially more relevant, that are likely to be the focus of a targeted real life attack.

An alternative approach to conducting testing on large environments is through a red teaming approach. Red team exercises are bespoke, intelligence-led security tests designed to replicate as closely as possible the evolving threat landscape. For example, cyber-attackers are likely to carefully profile your organisation before launching an attack so that they can select the easiest attack vector that is least likely to be detected. Therefore performing an isolated penetration test on a single network or application will not provide the true visibility you require to understand your exposure.

There are many variations on red team exercises. Comprehensive approaches should include an initial consultation with stakeholders (who have a need-to-know), a risk assessment workshop to identify and agree critical assets/targets, threat actors, and attack scenarios. This should then evolve into a testing program that encompasses digital attacks, social engineering, and physical security assessments.

Frequently we find that organisations compromise the integrity of the testing by being too narrow in both breadth and depth. While a narrow scope is itself likely not representative of your threat profile, even if a single review type is considered (for example application penetration testing), the scope seldom addresses all aspects of the application. Either there is a lack of awareness of the components of the system; or the scope is cut for procurement due to budgetary constraints. Either way, the result is that interfaces of system that increase exposure, and could lead to a compromise, are frequently left out of reviews. Examples of this include neglecting to review the web services component of a web application [4], or the administration interface which is frequently a separate application.

[4] Web services are typically application programming interfaces (API) or Web APIs that are accessed via Hypertext Transfer Protocol (HTTP) and executed on a remote system hosting the requested services.

9 Capability

Selection of an appropriate service provider to conduct testing is essential to an effective outcome.

Capability should be assessed with respect to the following attributes: methodology, experience, skill and tools.

9.1 Methodology

Testing can only be considered to be comprehensive if conducted in accordance with an appropriate methodology. Testing across the breadth and depth of scope will require expertise in all the domains, because each domain is considered a distinct discipline. Just because a company performed a network penetration test doesn’t mean they can deliver wireless or mobile application assessments.

Similarly, red team exercises require a highly orchestrated, systematic, repeatable and reproducible methodology. This can only be delivered effectively through a specialised service provider with experience in current and emerging threats, the ability to develop simulation tools, benign exploit code, and adopt the tools, tactics and procedures of real-world attackers that target your environment.

The red team needs to have the capability to breach your current controls, embed themselves in your environment, maintain persistence, escalate privileges, obtain access to key systems through direct and lateral attacks, and actively demonstrate how access to defined resources has been achieved. Such an assessment must focus on non-disruptive, non-damaging tactics to achieve its objectives

Service providers should not only have defined methodologies for each testing service offered, but they should also be able to demonstrate the substance behind this. Summaries of commonly accepted methodologies are freely available and generally included in proposals. However, the procurer should discern lip service from substance and validate the provider’s capability in the disciplines.

9.2 Experience

Experience comes from maturity. Capability in penetration testing cannot be developed overnight. Companies with a heritage, and specialisation, in Penetration Testing are likely to be able to demonstrate a successful track record. Experience across a broad range of industries and sectors is desirable which would include an exposure to various technologies, regulatory and compliance requirements.

Service providers that are committed to maintaining and expanding their knowledge in their penetration testing capability should be expected to demonstrate their commitment through investment in their own research facilities. Publication of whitepapers, security advisories and contribution to the community can measure the depth of research commitment.

A capable service provider should also demonstrate how their approaches have maintained pace with evolving threats and techniques adopted by the various classes of cyber threat actors. The ability to orchestrate an effective red team exercise through a well-managed and sound approach are key markers of an experienced specialist.

9.3 Skill

Good penetration testers hone their skills over time, all having strong fundamentals in their discipline of speciality. Expert network penetration testers will understand networking concepts; expert application penetration testers will understand the language the application is written in and how application components connect and interact. A penetration tester needs to know how the system was constructed in order to systematically deconstruct it. This ability is innate and part of a good penetration tester’s intuition. However, native capability isn’t where it ends. The tester needs to deliver with flair but follow the process of the methodology to confirm the comprehensiveness of the coverage.

Another important attribute is that of finesse and accuracy. Spraying a network with a myriad of noisy scanning tools is the brute force approach to testing (hoping that the tool will do the job for you). A far more professional approach is to demonstrate skills by interpreting scan results, and accurately exploiting vulnerabilities with finesse. Tools may provide insight into technical flaws but cannot identify logic flaws. A technical flaw could be identifying a system is vulnerable to a buffer overflow attack; a logic flaw may be determining if an application can be tricked into executing something outside of its intended business purpose - such as refunding a transaction twice which could be used to defraud a business. It takes intellect and finesse to identify logic flaws.

9.4 Tools

Modern systems are complex, networks are large and applications are multi-functional. Tools assist testers through automation, using the processing power of the computer combined with purpose written software to systematically probe systems to identify points of weakness or exposure to known vulnerabilities. However, not all tools are created equally. Some studies have demonstrated that tools missed nearly half of the vulnerabilities on systems -- even when they were fully "trained," or tuned, rather than set to point and scan the sites. Sometimes vulnerabilities are inherent in particular products and remain “undetected” until effectively demonstrated to exist. For example, the Heartbleed vulnerability in OpenSSL affected systems globally but was only detected in 2014 although understood to be vulnerable since 2011. The Unix Bash shell has been extensively deployed from 1989 but the Shellshock vulnerability was only discovered in 2014.

Therefore, a tester needs to have at their disposal a suite of tools so that the outputs can be reviewed across the spectrum to ensure good coverage of automation. A suite of tools should comprise a variety of open source, commercial and custom written tools.

A capable service provider should also demonstrate how their approaches have maintained pace with evolving threats and techniques adopted by the various classes of cyber threat actors. The ability to orchestrate an effective red team exercise through a well-managed and sound approach are key markers of an experienced specialist.

All of these attributes need to be present in a service provider to deliver effective outcomes to a penetration testing project. The true capability of a service provider can be assessed by their ability to deliver the chemistry of these attributes through project and quality management and through personnel with the skill.

10 Time & Budget

Unfortunately time and budget are frequently underestimated for penetration testing projects which ultimately leads to a compromised outcome.

A risk assessment should identify the scope (breadth and depth) of the test. The time to conduct the test will be directly proportional to the scope (clearly the more there is to test the longer it will take). However, it is also a function of capability. One may expect to yield time savings through economies of scale; and certain tests may be run in parallel if the provider has the resources and capability across the disciplines.

In general budget will buy you time. But if the budget is underestimated, the time allocation or scope is likely to be retrospectively revised downwards. The result is squeezing a test to fit into an ill-defined budget, the outcome is certainly affected.

11 Cloud & Regulation

No information technology discussion is complete without a discussion on cloud computing. The flexibility and opportunities offered through cloud computing are very compelling. Demand has been established in both the commercial and public sector. For example, the Australian Government has provided a Whole of Government (WoG) policy position on Cloud Computing. “Agencies may choose cloud-based service where they demonstrate value for money and adequate security” [5]. Adequate security requires meeting the mandatory requirements outlined in Protective Security Policy Framework (PSPF), the Australian Government Information Security Manual (ISM) and the Privacy Act.

As cloud offerings mature, the regulations to control and protect use of such services will mature as well. Regulations are already in place across a number of jurisdictions, and also for specific industry sectors (e.g. PCI DSS applies to organisations dealing with credit card data). Organisations are expected reasonable steps to monitor, review and audit information security effectiveness of cloud providers, which would include engaging internal and/or external auditors and specialist organisations where required to deliver penetration testing. End users of cloud services are entitled to expect their personal information is protected from loss or misuse and unauthorised access, modification or disclosure [6].

Security requirements must be clearly defined and managed through contract. A cloud vendor’s commitments to important security considerations must be captured in a contract, otherwise the customer only has vendor promises and marketing claims to rely on that can be hard to verify and may be unenforceable. Penetration testing is a good technical measure of evaluating the effectiveness of a cloud offering and

[5] Australian Government Cloud Computing Strategic Direction Paper, Dept of Finance, April 2013 Version 1.1. http://www.finance.gov.au/files/2013/04/final-_cloud_computing_strategy_version_1.1.pdf

[6] Guide to securing personal information. ‘Reasonable steps’ to protect personal information (Jan 2015). https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

should be included as part of an overall capability review of the vendor. Scope could include network and application testing against the public facing and internal systems as well as a review of the ability of the provider to maintain isolation in a multi-tenanted deployment.

12 Where does Penetration Testing Fit In?

Penetration testing will not be effective if considered an exercise in isolation. Testing should be part of the ongoing information security management lifecycle (Plan, Do, Check, Act). Testing should be conducted in the Plan and Check phases and issues remediated in the Do and Act phases.

Industry standards define the testing requirements (e.g. OWASP). Testing will verify the implementation of security requirements (e.g. the organisation’s development, configuration or deployment standards). Governance Standards (ISM, ISO 27001) will include the organisation’s security requirements and require regular testing to validate the security of the process. Outcomes of the tests will identify risks that must be addressed through the organisation’s Risk Management capability.

13 Conclusion

Don’t think of your organisation as silos of systems. Adopt a risk based approach and understand what it is that you wish to protect and the implication of a security breach. Know your data, determine where it is, who has access to it and how many systems or interfaces there are to it. Scope should be determined through risk assessment and the testing approach should simulate current and emerging trends that are already adopted by the various threat actors targeting entities in your sector.

Due to the increased sophistication of attacks there is an increased requirement for expertise. Organisations will need to rely less on tools and more on expertise to interpret and evaluate their security posture.

Assessing the capability of a service provider is essential in making an informed decision in selecting the party to deliver a penetration test. Capability is a function of methodology, skill, heritage and reporting.

Penetration testing in isolation is of limited value. Testing must be part of a broader vulnerability management program. You then need to be able to act on the recommendations which will require planning, resources and budget.

Price is always important. However, consideration should be applied that comprehensive testing will cost more than check box testing and testing in breadth and depth will incur higher costs too – but deliver more value in the results.

Cloud is an extension of your organisation and the risks must be evaluated and treated accordingly.

About Sense of Security

Sense of Security Pty Ltd is an Australian based information security and risk management consulting practice delivering industry leading services and research to organisations throughout Australia and abroad. Our strategic approach to security provides you with a capability to assess your risk and deliver qualified guidance on how to protect your information assets. We provide expertise in governance & compliance, strategy & architecture through to risk assessment, assurance & technical security testing.

For more information please contact us:

Web: www.senseofsecurity.com.au

Email: info@senseofsecurity.com.au

Phone: 1300 922 923

Sense of Security - Compliance, Protection and Business Confidence