INSOMNIA
SECURITY SPECIALISTS :: REST SECURED

INCREASING THE VALUE OF PENETRATION TESTING

PRESENTED BY BRETT MOORE

APRIL 2008, AUCKLAND, NEW ZEALAND

Table of Contents

About Your Speaker

Having conducted vulnerability assessments, network reviews, and penetration tests for the majority of the large companies in New Zealand, company founder Brett Moore brings with him over six years experience in information security.

Over the past six years, Brett has also worked with companies such as SUN Microsystems, Skype Limited and Microsoft Corporation by reporting and helping to fix security vulnerabilities in their products.

Brett has released numerous whitepapers and technical postings related to security issues and how companies can address these within their environment, and is considered a world expert on various aspects of computer security.

During this time he has also spoken at a number of security conferences both locally and overseas, including the invitation only Microsoft internal security conference called BlueHat. At this conference Brett addressed the executive members and the development teams on security vulnerabilities in their products and how they should be addressing these.

Prior to founding Insomnia, Brett held a position in another local security company where he managed the training, resourcing, and quality control of the consultancy team.

About Insomnia Security

Insomnia Security is a New Zealand based company dedicated to providing highly specialised information security consultancy services to our customers in the Asia-Pacific region.

Insomnia was founded in 2007 by security specialist Brett Moore with the aim of bringing together a team of highly skilled, technically focussed, and uncompromising security professionals.

Insomnia is a company whose services are based around information security; with a difference. We specialise in researching new and recently disclosed vulnerabilities, pushing the boundaries of modern day network and application security testing.

More that just using the publically available information related to security vulnerabilities, our team conducts independent research to discover new vulnerabilities that could affect our customers systems.

Contact

For sales enquires please contact sales@insomniasec.com

All other enquires should be directed to enquires@insomniasec.com

You may use this pgp key to encrypt communications sent to Insomnia Security

INSOMNIA
SECURITY SPECIALISTS :: REST SECURED

1.   What is penetration testing

When the industry was in its infancy, the term Penetration Testing was commonly used to describe a test whereby an authorised individual would attempt to break into a computer system. Supposably this would give a real life 'what a hacker could do' review of the security of a system.

Nowadays Penetration testing is widely used to describe a security review of IT Systems. This might include reviews of components such as;

- Network review
- Application review
- Source Code review
- Host hardening review
- Wireless network reviews
- etc

In its simplest form, a penetration test is an independent evaluation of how well, or how badly, an organisations security posture is.

Carrying out penetration testing allows you to confirm that the security processes that you have in place, are working as they should. Verification that your systems are patched, that your firewalls are configured properly, and that your application code, that was outsourced, is up to the standard that you expect.

And if issues are found during a test, these can be traced back to the processes that are either not working, or not there, to prevent occurrences in future projects.

Even with good process in place, and conducting penetration tests should be one of those processes, it is still likely that a penetration test will uncover security issues. This is because the person conducting the test is not biased or influenced in any way, from been part of the project team, or working in the organisation. And also because they spend their working hours doing security reviews, finding security vulnerabilities, and identifying issues that may not always be apparent to other people.

What it's not

Penetration testing makes my systems secure

Penetration testing is one of many parts of a systems total security, but can not guarantee the security of your systems. It's an ever changing landscape.

I've had Penetration testing done; I don't need to do it again

Penetration Testing provide a Snapshot in Time. Depending on the system requirements, testing in one form or another should be done on a regular basis

Penetration testing gives me a real life 'what a hacker could do' view of my systems.

If someone really wanted to compromise your systems, they would attack the weakest link. Your staff would be targeted before your servers. Social engineering attacks against staff occur over the phone, or through email Trojans, etc..

INSOMNIA
SECURITY SPECIALISTS :: REST SECURED

2.   Why carry out penetration testing

The statistical argument

The number of reported vulnerabilities, and system compromises, is increasing every year. This does not equate to a growing number of vulnerabilities in applications and systems though, as some of the reported vulnerabilities have been around for years.

Statistics can be interpreted in many ways, but one thing that can't be argued is that cybercrime is on the increase. Earlier this year IBM X-Force released their report for 2007, this can be found on the Internet http://www-935.ibm.com/services/us/iss/pdf/etr_xforce-2007-annual-report.pdf

It should be obvious that as there is more publicity around computer security vulnerabilities, there are more individuals learning the knowledge required to exploit such issues, and as such the number of attackers is rising.

The human factor

Ok, so you already scan your systems with automated tools and port scanners. Don't you? So why pay somebody else to do that?

Numerous tests of the popular vulnerability scanners, both network scanners and application scanners, have been conducted and always found the tools to fail in multiple areas. Perhaps if you ran all the available tools you could detect the majority of the issues in your environment, but it takes only one critical vulnerability to allow an attacker the ability to gain access to your infrastructure.

The ability of the human brain to make decisions and respond intelligently is the difference that can reduce that gap. The skills that an experienced penetration tester brings to the job go far an above the job that an automated tool can achieve. The testers should use tools of course, but an experienced tester also brings the ability to make decisions and interpret the results of tools as they apply to your environment. They can also test for things, and investigate attack paths that automated tools can not.

Key benefits

Penetration testing helps;

- Provide an independent evaluation of your security posture

- Prevent financial loss through fraud, information loss, or system downtime

- Provide due diligence and compliance to industry regulators, customers and shareholders

- Protect brand and reputational value

- Identifying real vulnerabilities and evaluating the impact likelihood within your environment

- Helps with risk analysis and management

- Provide justification for future security spending

INSOMNIA
SECURITY SPECIALISTS :: REST SECURED

3.   Measuring the value of penetration testing

Measuring the ROI

Determining the return on investment for security spending is a difficult task, and penetration testing work is no different. You know that you need firewalls to prevent access from the Internet. But how do you put a value on that?

Penetration testing can be thought of as similar to a health check-up. You may not know if anything is wrong until you go to the doctor's office and have an examination. You hope the doctor doesn't find anything wrong, but that's why you go get a check-up. If there is something wrong then you now have the information and advice to do something about it. If you get a clean bill of health you may wonder why you spent the money, but the fact that you now know you are healthy soon outweighs then concern about money.

You spend money hiring someone to carry out penetration testing, and you hope that they do not find any vulnerabilities. But until your security has been independently reviewed, you can not be certain of the security posture of your organisation.

Similar to insurance, you don't realise the value until you need to claim on it; yet you hope that you are never in the situation where you do need to make a claim.

Information Assets

It is better to think about what is the value of the information asset you are trying to protect. And that is one method of determining how much should be spent on security.

What would happen if that information was lost, or if the reputation of the company was affected in a negative way via a data disclosure breach?

> *"What would it cost our organisation if this data was leaked?"*

> *"Would we lose customers if there was a security breach?"*

Information data is the key asset within an organisation. This means that any system capable of accessing that data should have the requirements of been in the same security zone.

Different information data has different value, and your organisation should know that value. You should know what data is stored, where it is stored, how it is stored, and how it can be accessed. Without answering these questions how can you put a value on it? Ask yourself now "Which data is so important that a loss of it would be disastrous for our organisation?" and then answer the questions about where and how it is stored.

The value of the result

The value of the information gained through penetration testing goes beyond just securing a single entry point, or testing the security of a new project. As mentioned before most findings during a penetration test can be linked back to process, or the lack of adequate process. Addressing the problems at this root level can prevent the same problems occurring in the future.

Applying the results of a 'targeted' penetration test against the broader scope of the organisation is something that is not often done.

For example; if you are reviewing the findings from a web application test of your new online system, and the report states that there is a lack of patches to the server. Wouldn't it be a good idea to have one of the system administrations check the other servers for patch levels? Take this one step further and

review the internal patch management procedures, to determine why the servers were allowed to be deployed without proper security patching.

4.   When should it be done

Driven by value of information

The value of the information assets that you want to protect will drive the requirements of when penetration testing should be undertaken. Everything costs money, and this spend will need to be justified to upper levels of management, and since the ROI is difficult to quantify this can sometime be a difficult objective to achieve.

Some suggested for Penetration Testing are;

- Now – If you have never carried out external penetration testing of your entire environment

- Yearly – Internal critical asset testing and network segregation testing

- Yearly – Password and account auditing

- 6 Months – Full perimeter penetration test of all externally facing systems

- Monthly – Automated perimeter scanning and Vulnerability Assessment

- Project Based - penetration testing of new projects, including full application source code reviews, before they are allowed into the production environment

In the real world

This is never the case though, as cost and the intangible ROI of this sort of testing is the prohibiter. If you are in the position of trying to get this sort of work signed off. You will probably find that the best time is after a security compromise within your own organisation, or a highly public one in another. If the CEO reads that <insert company name here> was compromised and ten thousand customer records were stolen, and that 30% of the customer base has left because of that. Then he is highly likely to want answers to questions such as "Could this happen to us?" and will be much more likely to help push the sign off of penetration testing.

Rather than have an adhoc approach to security testing, having the requirements written into procedural documentation can assist in the acceptance of the testing. Items such as requirements for Internet facing servers to be hardened to such standards, and reviewed independently, before accepting traffic from the Internet. Requirements for web applications to be developed to a set of standards (Secure Software Development standards), and to be independently reviewed before going live.

Cost is the prohibiter

Cost is still the prohibiter as requiring every project to go through security testing or penetration testing, will obviously increase the cost of the project.

The aim of this presentation is to help you gain more value from penetration testing, and one of the easiest ways to do that is to lower the overall cost.

Now I mentioned before to have projects independently reviewed. And what I mean by that is to be reviewed by somebody who was not associated with the host build, application development, or architecture design. A different set of eyes on a project often picks up things that those people involved with the project will not detect. This means that reviews can be undertaken by suitable skilled people within your own organisation.

If you have in place appropriate testing methodologies and check lists, peer reviews of developed solutions is an acceptable alternative to bring an outsider in every time. Even if this type of review is done as a precursor to bring in an external resource, it assists in cutting down the required time.

Different solutions have different risks associated with them, and it may be possible to implement a threshold level whereby it is accepted for those under the threshold to undergo a different level of testing than those above the threshold.

5. Steps to take before a penetration test

So you have decided that you need penetration testing done, and have got sign off for it to happen. Now what?

Identify The Outcome That You Require

Not all tests are the same, and different projects may require different results. Deciding what the outcome of the testing is to be, assists in quantifying how much time, effort and money should be spent on it.

Are you simply 'going through the motions' Are you after a PCI compliance tick in the box from a competent reviewer? Are you after a full low level source code review of a new web application? Is it time to get an understanding of the security posture of your external, or internal, environment. Are you really worried about what a targeted attack against your organisation could achieve?

Start thinking now about what is going to happen with the results. We will discuss reports in later slides, but think now. What sort of report and results do we want? Do we want the review team to sit down with the developers, and explain the findings and help them fix the problems? Do we want the review to fix the problems themselves?

Many automated tools produce good quality reports, and if this output of such a tool is adequate for your needs, then perhaps that is all you require. If the company that performs the penetration test is comfortable supplying reports in that way, then you could be in a position to cut down the length of the Penetration Test as reporting time will be reduced.

I will come back to this point.

Get Buy In From The Project Team

Quite often, system and network administrators consider auditors or penetration testers as the enemy, when in fact, they are allies. A good penetration test might prove your defences really do work. Or, that you have issues that need to be addressed that you can fix before you get attacked. It is much better to pay someone to discover your holes, than to have someone you don't know do it for you.

It is important to help the project team understand that 'the outsider' is a specialist in their field and will be coming in to assist with the overall security of the project. They should pay attention and they may find it interesting and learn something.

Reinforce that any findings from a review are not a slant against the project team, and will not be used to barrage them. Instead, raise the proposition that perhaps more training will be made available for those interested, or that the penetration testing report may be the leverage that is needed for management to finally take the issues about known problems seriously. It's amazing how the same comment from an outsider can get more momentum than when it is raised by somebody inside the organisation.

INSOMNIA
SECURITY SPECIALISTS :: REST SECURED

Do Some Internal Scoping

Here is where you start thinking about what it is that will actually be tested. Instead of ringing up your security provider and saying "We need another application test, what will it cost?" it is much better to be able to say "We have a 3 tier application that consists of a forward facing Apache server running mod_rewrite and mod_security. It communicates through XML/SOAP to a middle layer which is a C# .Net application running on an IIS6 web server. The middle layer uses a separate MS SQL instance for its data storage". "Our solution design documentation states that all database communications is done with stored procedures, and has separate SQL accounts for reading and writing data"

Instead of just saying "We have a Citrix implementation to review". You should say "We have a Citrix implementation to review that uses Citrix Ticket authority for single sign on authentication once a user has authenticated to our front end web server. The front end web server has been previously reviewed and we can make that information available, but the focus of the review will be Citrix. We are especially worried since our thick client application that we have made accessible does not work unless we give the Citrix user Desktop access"

If you don't know what you want tested, then how is your supplier able to scope it up appropriately. And if you don't know what the result is that you are looking for, then how do you know that at the end of the review you have what you need?

Internal Threat Modelling

Threat modelling should be used as part of any solution development. This is an easy way to determine what the risks are to the application/network, and therefore you can identify the core threats that you are wanting to protect against.

The people in the best position to perform threat modelling are your project team. There might be issues that they have thought of during the development cycle. There may be inter domain communications that have them worried. They are also in the best position to understand the business risks associated with the project, and how a failure of systems may affect the business.

The penetration testing team will ask these questions and you will have the material to answer them. If they don't ask, then use somebody that does.

Do Some Initial Testing

There are many automated tools available, some of these for free, that can be used for conducting security tests of your environment. The problem is that it takes time, and knowledge, to use these tools to their full potential. This is why you hire external resources to conduct penetration tests. As they do this type of work all the time, they have the ability to use these tools. And they also should have access to the specialised tools that do cost money.

There is however two tools that some of your network admin team probably already know how to use.

Nmap (http://nmap.org/) is a free port scanner, it checks out servers looking to which services are listening and is a quick way to determine if there is something listening that doesn't need to be.

Nessus (http://www.nessus.org) is a vulnerability scanner that has free version that checks out networks looking for known vulnerabilities.

You don't need to pay money to discover that "There are not appropriate firewall rules in place, and the server is accepting connections on ports that it should not be".

As far as patching goes, any system administrator is competent enough to discover that the service pack or security patches haven't been applied to a server.

Using these tools does not come close to replacing the expertise that you should receive from a specialised penetration tester, but they will help uncover some of the 'low hanging fruit' or common problems.

By doing so it allows (forces) the penetration tester to concentrate on the more subtle vulnerabilities that do require specialised knowledge and experience to uncover.

6.   Selecting your provider

Your security services provider should be a trusted adviser and a participant of project meetings at relevant times. Trust is the key point here, as you are going to accept what they say and the opinion that they have on security related matters that may be the difference between a data disclosure event, or not.

Following are some key points that you should consider when selecting a provider.

Everyone Is Not Equal

Different penetration testers have different fields of expertise. In this industry it is highly unlikely to find a person that is an expert in all fields. What this means is that the person who did the Host review on your SQL Server may not have the relevant experience to do the review of your critical Oracle server. The fact that they are both database servers, means nothing.

Qualifications should not be that important in your selection, you want people that have experience. Real world experience that is only gained from doing a lot of this type of work.

A company's work is only as good as the person on the ground doing the review. This goes for any industry. This can be compensated for by having a more experienced person overseeing the project, or having somebody do the initial data gathering before bringing in the Big Guns.

Either way, you want to meet the person who will be doing the work, and you want somebody from your project team to meet them as well, as they will be able to draw an opinion fairly quickly on whether the required skill sets are shown.

Don't expect the penetration tester to be an expert in the deployment and setup of your infrastructure, or to have the knowledge to code an application in your language of choice that integrates with all your components. That's not their job.

They should however have a base understanding of the infrastructure/language/components they will be testing and have knowledge of the security implication of such setups. Of course, you won't always find somebody that knows about the technology that you are using. So it might be a case of getting somebody in early, who has a good understanding of security, and having them become more deeply involved with the project to bring them up to speed.

A second opinion is something we often seek in the medical profession, and is something I recommend to organisations when dealing with security. Having the same person review the same application every year, is not as beneficial as getting a new set of eyes over the solution. Its not necessary to keep all your eggs in one basket either. It's more beneficial to have multiple trusted security providers that each offer their own areas of expertise.

This of course also helps when you can compare multiple quotes for various pieces of work.

Data Storage And Retention

Security reviews means dealing with sensitive information. Anyone conducting a penetration test will gain access to information, documentation, passwords, and otherwise confidential information that should not be disclosed to outside parties.

Of course Non Disclosure agreements are put in place, but data has a way of 'floating around'. Worst case scenario is that a consultants' laptop is stolen with the workings or results from a penetration test.

You need to ask your supplier what there data storage process is. Is it encrypted? All the time? Who within their organisation has access to the information?

And what happens to the information after the review is complete. Not only paper based material, but anything electronically stored needs to be handled in a secure manner. The supplier might have a process whereby they securely delete everything, or perhaps they keep it for later reference.

It's your information and you should know where it is located.

Report Type And Follow up

The report is the deliverable that you will get after the security review has been completed. It is this document that will be used to drive changes in your organisation, if required, or used as the security verification document for project sign-off.

A typical report will include the analyses of any vulnerabilities discovered during the review. The penetration testers must not only document what they found, but also the significance of their findings. Where appropriate, the penetration testers can also suggest methods for remediation, for example, updating a server, disabling network services, changing firewall rules, etc.

I mentioned before about obtaining the raw output of automated tools, as the deliverable. While this may appear to cut down on reporting time, and therefore costs, one of the most valuable aspects of a Penetration Test is the analyses of the findings. An experienced Penetration Tester is capable of making decisions around what are false positives and what is really a critical vulnerability in the target infrastructure. They should also be able to recognise that while a particular piece of information may not mean much by itself, if it is combined with other issues then it can cause a completely different effect that might have consequences that would otherwise not have been known.

Earlier on I mentioned that you should start thinking about what you will use the results for, and therefore in what format are they required. Is the report for the penetration test going to be used to increase project funding, and therefore needs to include a section for upper management. Or is it a mid project review that will be viewed only by technical staff, and therefore only needs technical level details.

Your supplier should be flexible in the content of the report, but don't expect them to change their format too much. Doing so has the potential to increase the reporting time, as the person writing the report will be accustomed to doing so in the vendors' format.

Ask your supplier for a sample report.

Methodology Used

Asking your supplier to explain the methodology they use during a security review. They should be able to give you a basic overview of the approach they take, without having to divulge the exact details. Every review is different, especially for application reviews, but there should still be a standard approach taken that covers of the basic areas, at least. Two of the commonly referred to methodologies are OWASP and OSSTMM.

The methodology below is probably as simple as it can get. It shows the different segments of a penetration test, but doesn't provide any detail as to what is happening.
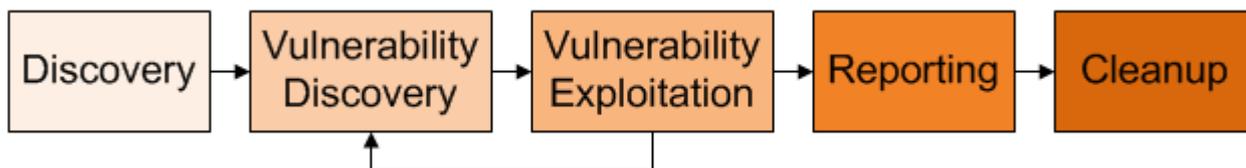
A better example provides more details about the activity, still without releasing the suppliers' complete methodology, which of course is highly sensitive.
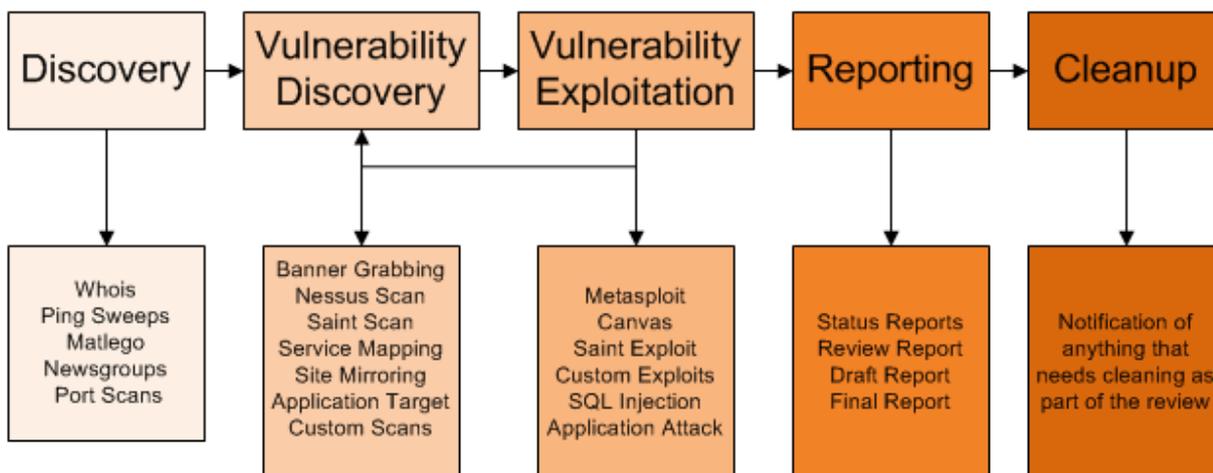
Tools

Commercial tools used to test for and exploit vulnerabilities can cost a lot of money. Your supplier should use tools, but definitely not rely on them and must validate the findings. Otherwise the report will come back with a lot of false positives and otherwise useless information. Your supplier should be able to tell you the names of at least some of the tools that they will use on the job.

They are after all, going to be a trusted supplier of security services to your organisation.

One important thing to query is the use of exploit scripts that are publically available on the Internet. What is the suppliers' policy on using such scripts, and what testing regime do they put the script through before using them against your organisation.

References

It is usually difficult to get references, largely due to the fact that NDA agreements are put in place and because of the nature of the work people are not that willing to divulge information about their security review partners.

And with just cause. If a real attacker wanted to break into a company, part of the information they would look for is "Who supplies security services to this organisation?"

We are lucky in New Zealand though, as the IT industry is relatively small and references or commendations can often be gained through talking to your peers. Places such as this conference are good for such communications with others in the industry.

Searching on the Internet is another good source of information around a company and its individuals.

7. Before The Review

Scoping Is Not A Sales Exercise

The sales guy has done his job already. He has sold the Penetration Tester to you, you are happy to go ahead and use them, but you probably want to know how much it will cost.

Costing without proper scoping is like putting a finger in the air.

Hopefully you have already created a detailed scope of the work that you want undertaken, based on what you want to secure, and the internal threat modelling that you have done. Sit down with the supplier and the person who will be doing the work to go over the scope and get their input.

They may suggest that "Reviewing that server is not as important as reviewing this one", or they may have input into tasks that they think should be carried out that you may not have thought of.

The scope should be clearly defined, and include not only the components that are to be tested, but also those that are not. Any restrictions on time or attacks not to be performed should also be included.

Costing is difficult for this type of work, but working from experience and backed by a proper methodology a reasonably accurate estimate of time should be able to be achieved. Remembering that you have a trusted relationship with your supplier and you expect them to be acting in a manner that is best for your organisation.

Time And Project Slippages

Have a set timeframe for when the testing is going to happen, and stay in touch with your supplier to keep them informed of slippages. Once an assessment is booked in, the person doing the Penetration Test can not be booked for other jobs during that time. If the time comes to carry out the security review, and the project is not ready, there could be charges for downtime or you could be paying to have a Penetration Tester waiting around for things to happen.

Get The Security Review Team In Early

The need for security within the Software Development Lifecycle is widely accepted, but still the call for Penetration Testing is left to get that final Security Tick before a project is pushed into production. Worse still, sometimes due to project slippages, it's left till a project is already publically accessible.

If you decide early enough during a project that you will be using an external resource to perform Penetration Testing, get the reviewer involved with the project first.

It's a proven fact that fixing a security vulnerability early in a project costs less than having to fix it once in production. And if the results of the security review prevent the project from going live, then the repercussions can have more than just financial loss.

Bring The Review Team Up To Speed

The person who is going to do the Penetration Test not only needs to know about the technical aspects of the components involved in the review, but also how they are used within your environment. They need to spend time understanding what the project or application does, and how it fits into your organisations business.

The best way to do this is to have a meeting with the appropriate people, and bring the tester up to speed. They need to understand what your business is, what the risks associated with the business are and get an overall understanding of the system they are going to review.

Even if they are not reviewing the architecture of a system, they might be doing a web application test, it may still be appropriate for them to see the network design documentation. This allows them to view the big picture of the target they are reviewing. They may also have some comments about the network design, that they will pass on without 'officially' been part of the review.

8. During The Review

Give Them What They Need

As I mentioned back at the beginning, there used to be this fascination with the 'hacker view' or "black box" testing. With black box testing, the penetration testers are told nothing about the target, under the assumption that real attackers will work under similar conditions.

Not only is this a good way to waste your organization's money, it is also not true. A real attacker does not abide by any rules and will attempt to compromise your organisation through means that a typical Penetration Tester won't attempt. An attacker may try to gain access through social engineering, theft, bribery, infiltrating your Network communications at the ISP, or even trying to compromise our security supplier.

You want the best result that you can get and to do so you should provide as much information as possible to the testing organization. We are talking about your trusted security provider, and as mentioned before, NDA documents should be already in place so you should feel comfortable with sharing information about your network and critical systems.

Provide them access to application source code, even if they are not doing a code review. Provide host level access to the web servers, or database servers, or any other server within the review. Allow them access to any and all technical and design documentation that is relevant to the project, regardless if they are doing a document review.

Not only does this increase the speed in which a review is done, but also it also obtains a more complete and accurate review of the security of a project. A good example would be when attacking a web application one of the tests is to attempt to find files that reveal sensitive information. If the person doing the review manually or automatically checks for all the files they check for, they may miss one that another person or attacker may find. And it may be this one missed file that allows an attacker further access to the environment.

Supply them with passwords. At least two sets of credentials for each authenticated level within the project. This allows them to test for things such as cross account vulnerabilities, and authorisation issues. Not checking for vulnerabilities at an administrative level within an application, just because normal users won't have that access, doesn't help if the administrators credentials are obtained by an attacker through information leaks, traffic sniffing, or just reading that post it note on the side of the screen.

If you do want to have an idea about what an individual could do without any prior knowledge or authentication, then write that into the scope. Assign a number of hours or days for that type of testing, but don't limit the entire Penetration Test to that restricted type of testing. It's not cost effective.

Be Ready For Them

Have all the information ready for them before the job is due to start. If possible send it through to them beforehand so they can check, and if necessary they can make requests for further information. This prevents the review from been held up.

Have adequate access available for them. If the testing will be done from an onsite location, then ensure that staff knows they are coming and that there is suitable working space for them.

Understand that they will most likely want to connect their laptops or other devices into your network and you need to be prepared for this. If there is security vetting that needs to be done on any devices to be connected, then this requirement needs to be communicated with the supplier prior to the consultant turning up for the job, so that the appropriate steps can be carried out.

The penetration tester will not be able to perform as good a job if they are not able to use their own tools for testing and data gathering, and therefore the security review will take longer and not be as comprehensive as could be.

Freeze The Project

Put a hold on changes to the project, or at least communicate changes with the person doing the testing so they can schedule testing times around any outages. You don't want to be paying for a tester to sit there for half a day because an upgrade caused the main servers to drop, and they won't be up for a while.

Another issue that arises is when the Penetration Tester has found a vulnerability, which the project team fixes in the background. The tester will spend time trying to reproduce the issue, time that could be spent on other things.

Become Involved With The Testing

Somebody from the project team should be in contact with the penetration tester everyday or two. Communication should be open between the two parties, so that the tester is able to ask questions or request further details on a particular area.

Other members of the project team could treat this as a learning exercise, and if approached in the proper way the Penetration Testing team could be a valuable resource for picking up tricks and techniques.

This is made easier if the tester has been involved with the project and met with the project team forming an open relationship.

INSOMNIA
SECURITY SPECIALISTS :: REST SECURED

9.   After The Review

Review The Report

You have paid for the review, and you have received the report. So is that the end of it. Now is the time to review the report and make comments back to the Penetration Testing team. If you need clarification on any points, it is best to do so now, while everything is still fresh in their mind, before they start working on another job.

Understand the root causes

As mentioned previously, most security vulnerabilities can be traced back to a lack of procedures, or process documentation. So one of the valuable pieces of information that can be extracted from the report might not even be mentioned in the report.

Understanding the root cause of vulnerabilities allows you to ensure, or attempt to at least, that they are not reproduced in other projects and can be identified and mitigated in projects that are already in production.

Meet With The Project Team

After the review is complete, and the report is in delivered, hold a meeting with the relevant members of the review team. This gives them an opportunity to discuss the findings, validate them, and come up with actions to mitigate any risk or to fix the vulnerabilities.

After this initial team meeting, arrange for the Penetration Testing to meet with the project team. Sometimes issues raised in the report are not valid within the environment of the business and a little discussion between the two parties can quickly evaluate any findings that are not relevant.

It is also worthwhile noting any that may be beneficial to other members of the organisation such as other development group. An email or monthly group meeting could be the opportune time to raise and discuss the current Penetration Test.

Consider Security Training

You already have competent staff members that are skilled in the areas that they work. Security training is an option that has far reaching benefits. If a large number of application vulnerabilities is discovered in a review, rather than just fixing them for the project, consider sending some of your lead developers for secure coding training. Network administrators and project managers can also benefit from security training in a range of areas.

Take Action

Make use of the information in the report. It is after all what you paid for. If you feel that you are overwhelmed by the number of issues that need fixing, seek help from your supplier. Start with the most critical of issues that affect your core information assets, and then work down to the lower ones.