



DEMYSTIFYING PENETRATION TESTS

Copyright MIEL e-Security Pvt Ltd
Author: Rion Dutta

WHITEPAPER

Contents

1] Introduction	Pg - 2
2] Penetration Testing – What Value?	Pg - 3
3] Targeting the Right Assets	Pg - 4
4] Approach	Pg - 6
5] Hacking Skills Analysis	Pg - 8
6] The Cost Dimension	Pg - 8
7] After the Test	Pg - 8
8] Conclusion	Pg - 8

DEMYSTIFYING PENETRATION TESTS

Copyright MIEL e-Security Pvt Ltd

Author: Rion Dutta

Introduction:

Penetration testing, or 'ethical hacking' as it is commonly referred to, is the act of testing the security of your information assets by inviting a trusted third party to try and breach that security using the same techniques that an authentic hacker would use. The aim of this process is to ensure that potential weaknesses in your security are identified and can therefore be addressed before your security is compromised by attackers.

Whilst most organizations are reluctant to discuss the hard facts concerning security breaches by hackers, there is sufficient data available from government surveys, law enforcement agencies and anti fraud bodies for us to conclude that there has been a significant increase in hacking activity over the last two years.

Its not just 'script kiddies' that organizations have to worry about – there are several active criminal groups who have now come to the conclusion that 'you can steal more with a computer than you can with a weapon', and there have been several high profile instances of organized syndicates targeting a 'victim company' with skilled people and resources. Whilst traditionally attacks were randomly targeted, hacking is now far more likely to be specifically targeted at a particular organization.

'Ensuring that we are not hacked' is therefore a major priority these days for most CIO's and IT Managers. The truth is, however, that many perceive the value of penetration as highly questionable. In particular, a frequently recurring sentiment is summarized in the following statement:

'I've spent a lot of money on having a penetration test, and I've fixed the vulnerabilities that they found, but I still don't know whether my company is secure – and the vendor who did the test can't give me a guarantee...'

The statement raises several fundamental issues, and by analyzing those issues we will answer the following key questions:

- What value should a penetration test bring to the organization?
- What are the limitations of penetration testing?
- How do you maximize the probability that you will significantly increase the security of your company through penetration testing?

By and large, the information security industry has done a poor job in explaining what penetration testing is, how it works, and how the organization and the tester should best work together to ensure a variable result. It's time that these questions, and other relevant ones are addressed in the context of penetration testing.

Penetration Testing – What Value?

We all know the cliché 'security is never complete' and in today's operating environment, what with 'Zero day exploits' and human errors ensuring there will always be a possible security breach even in the best run organizations, businesses need to constantly reassess and evaluate their security posture so that they minimize the acceptable residual risk. Whilst no CIO or IT Manager can look their CEO in the eye and say 'I can guarantee you we are totally secure', they should be able to say 'we have taken the right steps to ensure that the probability of our organization being successfully hacked is very low, and we regard the residual risk level as acceptable'.

Penetration testing has a key role to play in minimizing the risk of an organization's online presence. However, in order to do so, it is necessary that:

- The penetration testing is risk focused, specifically targeting those assets that represent the greatest risk to an organization
- The penetration testing is conducted in the same manner that would be utilized by a would-be attacker.
- The penetration testing is carried out by an ethical hacker who is at least as skilled as a future would-be attacker.

If these three conditions are met, then once the testing has been completed and appropriate measures have been taken to deal with the weaknesses identified, the CIO or IT Manager should be able to feel a high level of confidence that:

- The likelihood of the organization being successfully hacked is sufficiently low that the risk is acceptable; and
- That if an attack is successful, the consequences of that attack will be sufficiently minor so as to render the risk acceptable.

Of course, there is an additional dimension that needs to be taken into account – costs. Properly conducted penetration tests requires the time and expertise of highly skilled professionals and can be costly as a result. The size (and therefore the cost) of the penetration test needs to be commensurate with the level of risk faced by the organization, and needs to be affordable. This in turn means that the money must be spent on the areas most at risk, and focused on testing the methods most likely to be used by today's hackers.

It is worth noting that poorly conducted penetration tests can in fact increase the levels of risk to organizations, as they can create a false sense of security.

If these principles were universally understood and acted upon, penetration testing would undoubtedly be an effective weapon in the fight

against the hacker, and would be regarded as an essential cornerstone of every organization's security strategy.

In the next sections of this white paper, we will explain how to apply the principles identified above.

Targeting the Right Assets:

The first step in scoping a penetration test must be to determine which information assets are most at risk. This can be viewed from two different perspectives:

- Which information assets, if compromised, would cause greatest loss or damage to the organization?; and
- Which information assets are hackers most likely to attack?

In the vast majority of cases, these two questions will yield the same answers, but this may not always hold true. From a prioritization (and cost management) perspective, it is important to focus primarily on the assets which, if compromised, would cause greatest damage to the organization.

This need not involve a complex risk management exercise. In most cases, it is obvious what the biggest risk areas are and most CIOs and IT managers would be able to state this information quite easily.

For example, consider the following types of businesses:

Online Financial Services Brokerage:

If the web applications which enable an online share trading company's clients to transact were compromised (ex. a hacker succeeding in taking over clients' trading accounts to commit fraudulent transactions) then the entire business would be in jeopardy due to the loss of trust in the market about the security of the company.

The impact of such an incident would be far greater than an incident where a hacker managed to break into the back office systems and compromise the payroll. Of course, any breach is of concern, but the overall risk to the business (and therefore the risk of weighting of such an incident) would be significantly less than an incident with the online applications.

Therefore the first priority for such an organization in terms of penetration testing would be rigorous probing of the web applications where the clients' financial transactions occurred, because that is where the greatest business risk exists.

Coincidentally, this would also be the point where the greatest risk occurs in terms of where a hacker is most likely to attack, as it is widely recognized amongst hackers that web applications are often the Achilles heel of an organization's security, and by definition will be exposed to the Internet.

Even if the organization (share brokerage) does not have a large security budget, it should focus their penetration testing on their web applications to obtain the greatest 'security payoffs' from their investment.

Pharmaceutical Company:

Unlike the online share brokerage, the pharmaceutical company will probably have a relatively 'inert' web site used primarily for providing information about the company and its products. Whilst it would be embarrassing if the website were to be defaced by activists or malicious attackers, it is unlikely that such an incident would pose a major threat to the company.

However, if the confidential plans and test data for the next generation products (stored in the systems on the company network) were to be accessed by a hacker, this would have a serious negative impact on the pharmaceutical company's business.

Therefore, following our rules of prioritization, this company should take measures to protect the confidentiality of data stored on its internal network. Penetration testing would be best focused on preventing unauthorized access to internal systems both via the Internet gateway and also from within.

Approach – Using the same Attack Signatures as a Black Hat

Penetration testing is only valuable to a company if the tester uses the same types of techniques that a real ‘black hat’ hacker is likely to use on your organization. Like in similar real world instances of break in and theft, hackers are in a hurry and look for the points of least resistance. Once they decide to target an organization, they will rapidly look for any obvious potential ‘soft spots’ that the organization may have, and devise a way of exploiting that weakness.

In particular, they will not necessarily limit their activities to network based techniques. If the most efficient entry method is via weaknesses in physical security or social engineering, then that is exactly what a determined hacker will do.

Here is a typical process flow of a Penetration Test (which shows the outputs of each stage):

- 1. Scope -> *Scope Document***
- 2. Information Gathering -> *Network Diagram***
- 3. Attack Planning -> *Attack Plan***
- 4. Attack Attempt -> *Attack List***
- 5. Reporting -> *Final Report***
- 6. Review -> *Change Document***

Depending on what they are attempting to achieve and the characteristics of your organization, hackers are likely to attempt one or more of the following ways of breaching your security:

Network Attacks:

Identifying ways to penetrate the network through Internet facing hosts is a natural starting point for most hackers. The range of methods employed is considerable. These can include:

- Scanning for known vulnerabilities
- Password cracking brute force attacks
- Attempts to bypass access control lists
- Network eavesdropping
- Trojan attacks
- Exploitation of buffer overflows

Information
Gathering Tools/
Activities

**White & Yellow
Pages
Whois
DNS
Newsgroups
Web Search
Ping &
Traceroute
Firewalk
NMAP
Cheops**

Web Application Attacks:

It is increasingly recognized that web applications are often an 'open window' into the IT infrastructure of many organizations. This is because few web applications are developed with security in mind, and very few developers understand web application security techniques. Hackers will therefore attack these applications as an end in itself (ex. to perpetrate fraud via an insecure financial service application) or to seek to use the web application as a soft entry point into the other internal systems.

Web application attacks will typically involve one or more of the following:

- SQL injection
- Cross site scripting attacks
- Exploitation of authentication, access control and authorization issues
- Exploitation of session management problems
- Exploitation of web server configuration issues

Wireless Attacks:

A large number of companies who have been diligent in establishing a secure traditional wireline infrastructure suddenly throw caution to the wind when they roll out wireless networks. If a hacker knows that your company uses wireless technology, the hacker will almost certainly attempt to break your security through the wireless network, using techniques such as:

- Locating or establishing an unauthorized wireless access point
- Eavesdropping and exploiting weaknesses in network encryption
- Exploiting weaknesses in network access control

Social Engineering:

Hackers use a wide variety of social engineering techniques in an attempt to elicit passwords and other information that may assist an attack from staff by covert means.

The methods used are many and various, but frequently involve telephoning a junior employee, posing as a member of the IT department and requesting that person's user ID and password so as to perform some remote diagnostic tests.

Physical Security Attacks:

Hackers are aware that whilst most organizations have invested heavily in logical security infrastructure, this is frequently undermined by holes in physical security. Hackers will therefore often attempt to breach the physical security of a site through a number of techniques, which can include:

- Stealing laptops
- Obtaining access to a building through false pretenses (posing as maintenance staff, etc) and
 - stealing assets containing confidential data; or
 - furtively setting up a rogue wireless access point; or

- looking out for passwords and user names written down on pieces of paper
- Exploiting weakness in building access control devices to gain after hours access or access to data centers.

Telephony Systems Attacks

Telephonic communication systems and computer systems are highly integrated these days, and in many companies, practically indistinguishable from one another. Not surprisingly, hackers can and do use weaknesses in telephony systems to break into company networks. Techniques used by hackers include:

- War dialing (for the identification of remote access points)
- Attacking remote access port vulnerabilities
- Brute force attacks (for gaining access to remote access ports)
- PABX attacks (modifying PABX settings to re route calls)

The Compromise

In an ideal world, any penetration test would include all these attacks since a real hacker is likely to try all of them (depending on what they are trying to achieve). However, this would make the cost of a penetration test prohibitive. An intelligent compromise must be reached when defining the scope of penetration testing. This is considered further in *The Cost Dimension* below.

The important thing to note at this stage is that a penetration test will only make your organization more secure if the tester uses the same techniques that a black hat hacker is likely to use on your organization.

Hacking Skills Analysis:

Any organization is likely to be attacked by 'script kiddies', since their attacks are typically random and targeted at known vulnerabilities. Script kiddies typically have no idea who they are targeting – and generally,

they don't care. The only thing they are interested in is that you are vulnerable, and therefore potentially open to exploitation by them.

The skills of the penetration tester should therefore be at least on par with the average script kiddy.

At the other end of the spectrum are the sophisticated hackers (increasingly being used by organized crime syndicates) who usually target government, large enterprises such as financial institutions. At this level, the hacker may spend months crafting strategies and gathering intelligence before launching an esoteric and original attack. Although these organizations are often in an almost constant state of penetration testing with different aspects of their systems being tested by experienced 'white hat' hackers, the result is often a battle of wits between security departments and top level hackers.

Companies at risk need to invest in the services of the best penetration testers as the stakes at this level are very high.

Whilst not many organizations are operating at this level of threat, a large number of businesses are at risk from hackers whose skills are beyond those of script kiddies. If your organization meets any of the following criteria, then there is a strong likelihood that you will attract the attention of a real hacker:

- Engaged in the financial services industry at any level
- Offering online credit card transactions with you customers
- Federal, state or local government agency
- Telecommunications company
- Defense sector organization
- Healthcare company and likely to store and access patient records
- Publicly listed on any stock exchange
- Internet Service Provider (ISP)

- High profile organization of any type (perceived as open to extortion in return for not launching denial of service attack or public defacement of website)
- Engaged in design and manufacturing of leading edge products in any sector (particularly pharmaceutical, IT, electronics, defense, etc)
- Part of the 'extended enterprise' with a direct link into the trusted networks of any of the above

This is not an exhaustive list, given the widely differing agendas of hackers. However, for any organization fitting into the profiles listed above, using simple network scanning tools to identify known vulnerabilities is an approach fraught with risk and will not make your organization more secure.

The Cost Dimension:

The cost of a penetration test is generally a function of the time taken to do it and the skill level of the tester (just as a senior counsel costs more than a rookie lawyer, the same applies with penetration testers). So how long should a test take, and who should you employ to do it?

Diminishing Returns:

Most people are familiar with what economists term as 'the law of diminishing returns' – i.e. there comes a point when the value add of additional activity is insufficient to justify the additional investment. In everyday speak, we refer to the 80 / 20 concept which is based on similar principles.

These concepts are relevant and applicable to penetration testing. Provided your penetration tester is skilled, there is a direct correlation between the amount of time allocated to testing and the increased level of security you should achieve. As a penetration test progresses, the rate at which security is being improved slows, and there comes a point in a penetration test where it is no longer efficient to continue the test.

The objective is to test to the point where the level of residual risk is considered acceptable (i.e. it is recognized that the risk of attacks still exists, but estimated that the likelihood and consequence of an attack is acceptable to your business).

Identifying the Acceptable Risk Point:

In the previous sections of this paper, we discussed the main principles to be applied in ensuring that a penetration test really made you more secure. These were:

- The penetration test is risk focused, specifically targeting those assets that represent the greatest risk to an organization
- The penetration testing is conducted in the same manner that would be utilized by a would be attacker
- The penetration test is carried out by an ethical hacker who is at least as skilled as a future would be hacker

Applying these principles to your organization will enable you to quickly determine the scope of the penetration test (what aspects of the IT infrastructure should be tested, what kinds of tests should be carried out) and also define an acceptable risk point. Quotations can then be obtained from suitably qualified testers to test to this point.

It is possible that the costs of testing as far as the 'acceptable risk point' will exceed your budget. Then, you will have to scale back the scope of the penetration test accordingly – with a clear set of priorities so that even with the increased level of risk, you remain in control and decide how to play the odds.

Estimating Time Frames for Penetration Tests:

The cost of a penetration test depends on the time a tester will require to complete the testing – we have stated this in this paper. Based on the experience of conducting numerous penetration tests for a wide variety of companies, we offer the following table as a guide to typical time frames for a penetration test. Of course, these are approximations only,

and will vary from case to case, depending on the complexity of the IT infrastructure, size of the organization, etc. However, they should provide a helpful ball part indication:

Activity	Timeframe
On Site Scoping Activities	1 – 2 days
Information Gathering	1 – 2 days
Network Enumeration & Fingerprinting	1 – 2 days
Mail Server Testing	½ day (per server)
Name Server Testing	½ day (per server)
Firewall Testing	1 day (per gateway)
Remote Access Testing	1 day (per device)
Web Server Testing	1 day (per server)
Web Application Testing (Smaller Sites)	1 – 2 days (per application)
Web Application Testing (Medium Sites)	2 – 4 days (per application)
Web Application Testing (Large Sites)	4 – 7 days (per web application)
Physical Security Testing	1 – 2 days (per site to be tested)
Social Engineering Exercises	1 – 2 days
Report Writing	1 day
Management Presentation	1 day

Educated Attacks and Blind Attacks:

From the table above, it may be noted that some time is allocated to information gathering, network enumeration and fingerprinting. This raises the question of whether a 'blind' or 'educated attack' is more appropriate for your organization. A black hat attacker will gather as much intelligence as possible about the intended target prior to conducting an attack, and this is reflected in the preparatory intelligence gathering activity above. However, in order to save time and money, some organizations provide the tester with significant amounts of information at the outset of the test, enabling the tester to then focus on developing and executing the 'educated' attack. Other organizations prefer to be more realistic by providing the tester with no information at all, effectively putting the tester in the same situation as a real attacker – this is called the 'blind attack'.

While there are arguments either way as to which model works better, our recommendation is that if you can afford it, there is significant value in getting the penetration tester to gather his own intelligence. It can also be an eye opener experience for many businesses to learn just how much information they thought was 'internal' or 'company confidential' can actually be gathered in the public domain simply by using search engines and basic hacking tools and techniques.

Differential Tests:

Another cost related issue is the frequency with which tests should be conducted. The IT infrastructures of most organizations are dynamic and in a constant state of change. Therefore, the results of a Penetration Test have limited validity and relevance – but, apart from the most secure operating environments, it would clearly be inappropriate to be in a constant state of Penetration Testing. Increasingly, organizations have a rolling program of testing based around a 'full' Penetration Test at quarterly intervals, coupled with monthly 'differential' tests. The results of the most recent 'full tests' are used as a baseline to measure the state of security, and deviations from the baseline are identified in the 'differential' tests. This kind of program is more cost effective for the business, whilst still ensuring that key threats are constantly monitored and it is a model that is likely to be adopted by more organizations.

After the Test

So far we have focused on how to ensure that real value is obtained from a penetration test by looking at how (and by whom) the test should be conducted. However, an equally critical issue is what happens after the testing has been completed.

The output from a penetration test should be a written report documenting the following:

- Executive Summary
- Description of testing methodology

- Detailed findings including an evaluation of risk
- Recommendations for risk mitigation

Executive Summary:

It is particularly important that the report contains an Executive Summary aimed at non technical senior management. In our experience, a typical penetration test will identify several high risk categories where action is required. So it is important that the findings are presented from a risk perspective, using a grading convention (high / medium / low) based on likelihood and consequence. This will enable company managers to allocate resources and budget (if necessary) to ensure that appropriate remediation treatments are implemented.

Remediation Treatments:

A penetration test will make your organization more secure if the risks are subjected to remediation treatment. That may sound like an obvious statement, but many organizations routinely commission a penetration test, receive a report detailing several major risks, and then fail to do anything about them. Failure to respond to security issues identified in a penetration test would well result in legal implications for the organization, if the weaknesses are subsequently exploited by the hacker. When companies are hacked, the fall out will often adversely affect third parties (customers, suppliers, business partners, etc) – who may, and often will initiate legal proceedings alleging negligence. If the claimant can show that the loss they suffered arose from a security weakness that had been pointed out, then there is a greatly increased chance that the claim for negligence will succeed. In addition, many organizations face stringent disclosure and corporate governance norms – which will affect their standing in the industry, public bourses and even result in a loss of operating licenses.

Conclusion

Penetration testing should be a central plan of the information security strategy of any organization that is at risk from attack as a result of having Internet facing information assets. However, penetration testing will yield significant benefits if:

- The testing is risk focused
- The testing is conducted using the same comprehensive range of techniques that a real attacker would use
- The tester has skills at least equal to those of probable attackers
- The results are presented in a way that enables senior management to truly understand the business risks that they are currently facing
- The organization has the will to implement the remediation strategies necessary to deal with the risks that are identified.

A suitably qualified organization should be appointed to conduct the penetration testing. That organization needs to be able to demonstrate a sound understanding of the principles set out in this White Paper, whilst simultaneously providing value for money.

About MIEL e-Security

MIEL e-Security is a specialist in information security services and consulting. MIEL has performed extensive penetration tests for a wide variety of businesses, including large multinational corporations and government agencies. MIEL is widely recognized as a leader in penetration tests and can be contacted at any time.



Reach us at:

MIEL e-Security Pvt. Ltd.: C – 611 / 612, Floral Deck Plaza
MIDC Central Road, Andheri (East), Mumbai 400 093. INDIA
Tel # General: +91 22 28215050 | Tel # Training: +91 22 39560003 / 04 | Fax#: +91 22 28215838
Email – General: feelsecure@mielesecurity.com | Email – Training: isti@mielesecurity.com
Website: www.mielesecurity.com
