Pre-engagement

Contents

Overview

The aim of this section of the PTES is to present and explain the tools and techniques available which aid in a successful pre-engagement step of a penetration test. The information within this section is the result of the many years of combined experience of some of the most successful penetration testers in the world.

If you are a customer looking for penetration test we strongly recommend going to the General Questions section of this document. It covers the major questions that should be answered before a test begins. Remember, a penetration test should not be confrontational. It should not be an activity to see if the tester can "hack" you. It should be about identifying the business risk associated with and attack.

To get maximum value, make sure the questions in this document are covered. Further, as the Scoping activity progresses, a good testing firm will start to ask additional questions tailored to your organization.

Introduction to Scope

Defining scope is arguably one of the most important components of a penetration test, yet it is also one of the most overlooked. While many volumes have been written about the different tools and techniques which can be utilized to gain access to a network, very little has been written on the topic which precedes the penetration: preparation. Neglecting to properly complete pre-engagement activities has the potential to open the penetration tester (or his firm) to a number of headaches including scope creep, unsatisfied customers, and even legal troubles. The scope of a project specifically defines what is to be tested. How each aspect of the test will be conducted will be covered in the Rules of Engagement section.

One key component of scoping an engagement is outlining how the testers should spend their time. As an example, a customer requests that one hundred IP addresses be tested for the price of $100,000. This means that the customer is offering $1,000 per IP address tested. However, this cost structure only remains effective at that volume. A common trap some testers fall into is maintaining linear costs throughout the testing process. If the customer had only asked for one business-critical application to be tested at the same pricing structure ($1,000), while the tester will still be only attacking a single IP, the volume of work has increased dramatically. It is important to vary costs based on work done. Otherwise a firm can easily find themselves undercharging for their services, which motivates them to do a less than complete job.

Despite having a solid pricing structure, the process is not all black and white. It is not uncommon for a client to be completely unaware of exactly what it is they need tested. It is also possible the client will not know how to communicate effectively what they're expecting from the test. It is important in the Pre-Engagement phase that the tester is able to serve as a guide through what may be uncharted territory for a customer. The tester must understand the difference between a test which focuses on a single application with severe intensity and a test where the client provides a wide range of IP addresses to test and the goal is to simply find a way in.

Metrics for Time Estimation

Time estimations are directly tied to the experience of a tester in a certain area. If a tester has significant experience in a certain test, he will likely innately be able to determine how long a test will take. If the tester has less experience in the area, re-reading emails and scan logs from previous similar tests the firm has done is a great way to estimate the time requirement for the current engagement. Once the time to test is determined, it is a prudent practice to add 20% to the time.

The extra 20% on the back end of the time value is called padding. Outside of consultant circles, this is also referred to as consultant overhead. The padding is an absolute necessity for any test. It provides a cushion should any interruptions occur in the testing. There are many events which commonly occur and hinder the testing process. For example, a network segment may go down, or a significant vulnerability may be found which requires many meetings with many levels of management to address. Both of these events are time consuming and would significantly impact the original time estimate if the padding was not in place.

What happens if the 20% padding ends up not being necessary? Billing the client for time not worked would be extremely unethical, so it is up to the testers to provide additional value that may not normally have been provided if the engagement time limit had been hit. Examples include walking the company security team through the steps taken to exploit the vulnerability, provide an executive summary if it was not part of the original deliverable list, or spend some additional time trying to crack a vulnerability that was elusive during the initial testing.

Another component of the metrics of time and testing is that every project needs to have a definitive drop dead date. All good projects have a well-defined beginning and end. You will need to have a signed statement of work specifying the work and the hours required if you've reached the specific date the testing is to end, or if any additional testing or work is requested of you after that date. Some testers have a difficult time doing this because they feel they are being too much of a pain when it comes to cost and hours. However, it has been the experience of the author that if you provide exceptional value for the main test the customer will not balk at paying you for additional work.

Scoping Meeting

In many cases the scoping meeting will occur after the contract has been signed. Situations do occur wherein many of the scope-related topics can be discussed before contract signing, but they are few and far between. For those situations it is recommended that a non-disclosure agreement be signed before any in-depth scoping discussions occur.

The goal of the scoping meeting is to discuss what will be tested. Rules of engagement and costs will not be covered in this meeting. Each of these subjects should be handled in meetings where each piece is the focus of that meeting. This is done because discussions can easily become confused and muddled if focus is not explicitly stated. It is important to act as moderator and keep the discussions on-topic, preventing tangents and declaring certain topics more suited for off-line discussion when necessary.

Now that a Rough Order of Magnitude (ROM) value has been established for the project it is time to have a meeting with the customer to validate assumptions. First, it needs to be established explicitly what IP ranges are in scope for the engagement. It is not uncommon for a client to be resistant and assume that it is the prerogative of the tester to identify their network and attack it, to make the test as realistic as possible. This would indeed be an ideal circumstance, however, possible legal ramifications must be considered above all else. Because of this, it is the responsibility of the tester to convey to a client these concerns and to impart upon them the importance of implicit scoping. For example, in the meeting, it should be verified that the customer owns all of the target environments including: the DNS server, the email server, the actual hardware their web servers run on and their firewall/IDS/IPS solution. There are a number of companies which will outsource the management of these devices to third parties.

Additionally, the countries, provinces, and states in which the target environments operate in must be identified. Laws vary from region to region and the testing may very well be impacted by these laws. For instance, countries belonging to the European Union are well known to have very stringent laws surrounding the privacy of individuals, which can significantly change the manner in which a social engineering engagement would be executed.

Additional Support Based on Hourly Rate

Anything that is not explicitly covered within the scope of the engagement should be handled very carefully. The first reason for this is scope creep. As the scope expands, resources are consumed, cutting into the profits for the tester and may even create confusion and anger on the part of the customer. There is another issue that many testers do not think of when taking on additional work on an ad-hoc basis: legal ramifications. Many ad-hoc requests are not properly documented so it can be difficult to determine who said what in the event of a dispute or legal action. Further, the contract is a legal document specifying the work that is to be done. It should be tightly tied to the permission to test memo.

Any requests outside of the original scope should be documented in the form of a statement of work that clearly identifies the work to be done. We also recommend that it be clearly stated in the contract that additional work will be done for a flat fee per hour and explicitly state that additional work can not be completed until a signed and counter-signed SOW is in place.

Questionnaires

During initial communications with the customer there are several questions which the client will have to answer in order for the engagement scope can be properly estimated. These questions are designed to provide a better understanding of what the client is looking to gain out of the penetration test, why the client is looking to have a penetration test performed against their environment, and whether or not they want certain types of tests performed during the penetration test. The following are sample questions which may be asked during this phase.

General Questions

Network Penetration Test

1. Why is the customer having the penetration test performed against their environment?
2. Is the penetration test required for a specific compliance requirement?
3. When does the customer want the active portions (scanning, enumeration, exploitation, etc...) of the penetration test conducted?
    1. During business hours?
    2. After business hours?
    3. On the weekends?
4. How many total IP addresses are being tested?
    1. How many internal IP addresses, if applicable?
    2. How many external IP addresses, if applicable?
5. Are there any devices in place that may impact the results of a penetration test such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?
6. In the case that a system is penetrated, how should the testing team proceed?
    1. Perform a local vulnerability assessment on the compromised machine?
    2. Attempt to gain the highest privileges (root on Unix machines, SYSTEM or Administrator on Windows machines) on the compromised machine?
    3. Perform no, minimal, dictionary, or exhaustive password attacks against local password hashes obtained (for example, /etc/shadow on Unix machines)?

Web Application Penetration Test

1. How many web applications are being assessed?
2. How many login systems are being assessed?
3. How many static pages are being assessed? (approximate)
4. How many dynamic pages are being assessed? (approximate)
5. Will the source code be made readily available?
6. Will there be any kind of documentation?
    1. If yes, what kind of documentation?
7. Will static analysis be performed on this application?
8. Does the client want fuzzing performed against this application?
9. Does the client want role-based testing performed against this application?
10. Does the client want credentialed scans of web applications performed?

Wireless Network Penetration Test

1. How many wireless networks are in place?
2. Is a guest wireless network used? If so:

   1. Does the guest network require authentication?
   2. What type of encryption is used on the wireless networks?
   3. What is the square footage of coverage?
   4. Will enumeration of rogue devices be necessary?
   5. Will the team be assessing wireless attacks against clients?
   6. Approximately how many clients will be using the wireless network?

Physical Penetration Test

1. How many locations are being assessed?
2. Is this physical location a shared facility? If so:
   1. How many floors are in scope?
   2. Which floors are in scope?
3. Are there any security guards that will need to be bypassed? If so:
   1. Are the security guards employed through a 3rd party?
   2. Are they armed?
   3. Are they allowed to use force?
4. How many entrances are there into the building?
5. Is the use of lock picks or bump keys allowed? (also consider local laws)
6. Is the purpose of this test to verify compliance with existing policies and procedures or for performing an audit?
7. What is the square footage of the area in scope?
8. Are all physical security measures documented?
9. Are video cameras being used?
   1. Are the cameras client-owned? If so:
      1. Should the team attempt to gain access to where the video camera data is stored?
10. Is there an armed alarm system being used? If so:
    1. Is the alarm a silent alarm?
    2. Is the alarm triggered by motion?
    3. Is the alarm triggered by opening of doors and windows?

Social Engineering

1. Does the client have a list of email addresses they would like a Social Engineering attack to be performed against?
2. Does the client have a list of phone numbers they would like a Social Engineering attack to be performed against?
3. Is Social Engineering for the purpose of gaining unauthorized physical access approved? If so:
   1. How many people will be targeted?

It should be noted that as part of different levels of testing, the questions for Business Unit Managers, Systems Administrators, and Help Desk Personnel may not be required. However, in the case these questions are necessary, some sample questions can be found below.

Questions for Business Unit Managers

1. Is the manager aware that a test is about to be performed?
2. What is the main datum that would create the greatest risk to the organization if exposed, corrupted, or deleted?
3. Are testing and validation procedures to verify that business applications are functioning properly in place?
4. Will the testers have access to the Quality Assurance testing procedures from when the application was first developed?
5. Are Disaster Recovery Procedures in place for the application data?

Questions for Systems Administrators

1. Are there any systems which could be characterized as fragile? (systems with tendencies to crash, older operating systems, or which are unpatched)
2. Are there systems on the network which the client does not own, that may require additional approval to test?
3. Are Change Management procedures in place?
4. What is the mean time to repair systems outages?
5. Is any system monitoring software in place?
6. What are the most critical servers and applications?
7. Are backups tested on a regular basis?
8. When was the last time the backups were restored?

Scope Creep

Scope creep is one of the most efficient ways to put a penetration testing firm out of business. The issue is that many companies and managers have little to no idea how to identify it, or how to react to it when it happens.

There are a couple of things to remember when battling scope creep. First, if a customer is pleased with the work done on a particular engagement, it is very common for them to request additional work. Take this as a compliment, and do not hesitate to ask for additional funding to compensate for the extra time spent. If a customer refuses to pay for the extra work, it is almost never worth staying on to do that work.

The second point is even more critical. When dealing with existing customers, take care to keep the prices lower. Taking advantage of a good situation by price gouging is a sure way to drive away repeat business. Take into consideration that prices can be lowered since the firm avoided the costs of acquiring the customer such as the formal RFP process and hunting for the customer itself. Further, the best source for future work is through existing customers. Treat them well and they will return.

Specify Start and End Dates

Another key component defeating scope creep is explicitly stating start and end dates. This allows the project to have definite end. One of the most common areas in which scope creep occurs is during retesting. Retesting always sounds like a good idea when going after a contract. It shows that the firm is caring and diligent, trying to make ensure that the customer is secure as possible. The problem begins when it is forgotten that the work is not paid for until it is completed. This includes retesting.

To mitigate this risk, add a simple statement to the contract which mentions that all retesting must be done within a certain timeframe after the final report delivery. It then becomes the responsibility of the testers to spearhead the retesting effort. If the customer requests an extension, always allow this with the condition that payment be fulfilled at the originally specified date. Finally, and most importantly, perform a quality retest. Remember, the best source for future work is your existing customer base.

Specify IP Ranges and Domains

Before starting a penetration test, all targets must be identified. These targets should be obtained from the customer during the initial questionnaire phase. Targets can be given in the form of specific IP addresses, network ranges, or domain names by the customer. In some instances, the only target the customer provides is the name of the organization and expects the testers be able to identify the rest on their own. It is important to define if systems like firewalls and IDS/IPS or networking equipment that are between the tester and the final target are also part of the scope. Additional elements such as upstream providers, and other 3rd party providers should be identified and defined whether they are in scope or not.

Validate Ranges

It is imperative that before you start to attack the targets you validate that they are in fact owned by the customer you are performing the test against. Think of the legal consequences you may run into if you start attacking a machine and successfully penetrate it only to find out later down the line that the machine actually belongs to another organization (such as a hospital or government agency).

Dealing with Third Parties

There are a number of situations where an engagement will include testing a service or an application that is being hosted by a third party. This has become more prevalent in recent years as “cloud” services have become more popular. The most important thing to remember is that while permission may have been granted by the client, they do not speak for their third party providers. Thus, permission must be obtained from them as well in order to test the hosted systems. Failing to obtain the proper permissions brings with it, as always, the possibility of violating the law, which can cause endless headaches.

Cloud Services

The single biggest issue with testing cloud service is there is data from multiple different organizations stored on one physical medium. Often the security between these different data domains is very lax. The cloud services provider needs to be alerted to the testing and needs to acknowledge that the test is occurring and grant the testing organization permission to test. Further, there needs to be a direct security contact within the cloud service provider that can be contacted in the event that a security vulnerability is discovered which may impact the other cloud customers. Some cloud providers have specific procedures for penetration testers to follow, and may require request forms, scheduling or explicit permission from them before testing can begin.

ISP

Verify the ISP terms of service with the customer. In many commercial situations the ISP will have specific provisions for testing. Review these terms carefully before launching an attack. There are situations where ISPs will shun and block certain traffic which is considered malicious. The customer may approve this risk, but it must always be clearly communicated before beginning. Web Hosting As with all other third parties, the scope and timing of the test needs to be clearly communicated with the web hosting provider. Also, when communicating with the client, be sure to clearly articulate the test will only be in search of web vulnerabilities. The test will not uncover vulnerabilities in the underlying infrastructure which may still provide an avenue to compromise the application.

MSSPs

Managed Security Service Providers also may need to be notified of testing. Specifically, they will need to be notified when the systems and services that they own are to be tested. However, there are circumstances under which the MSSP would not be notified. If determining the actual response time of the MSSP is part of the test, it is certainly not in the best interest of the integrity of the test for the MSSP to be notified. As a general rule of thumb, any time a device or service explicitly owned by the MSSP is being tested they will need to be notified.

Countries Where Servers are Hosted

It is also in the best interests of the tester to verify the countries where servers are being housed. After you have validated the country, review the laws of the specific country before beginning testing. It should not be assumed that the firm’s legal team will provide a complete synopsis of local laws for the testers. It should also not be assumed that the firm will take legal responsibility for any laws violated by its testers. It is the responsibility of each tester to verify the laws for each region they are testing in before they begin testing because it will be the tester who ultimately will have to answer for any transgressions.

Define Acceptable Social Engineering Pretexts

Many organizations will want their security posture tested in a way which is aligned with current attacks. Social engineering and spear-phishing attacks are currently widely used by many attackers today. While most of the successful attacks use pretexts like sex, drugs, and rock and roll (porn, Viagra, and free iPods respectively) some of these pretexts may not be acceptable in a corporate environment. Be sure that any pretexts chosen for the test are approved in writing before testing is to begin.

DoS Testing

Stress testing or Denial of Service testing should be discussed before the engagement begins. It can be a topic that many organizations are uncomfortable with due to the potentially damaging nature of the testing. If an organization is only worried about the confidentiality or integrity of their data, stress testing may not be necessary; however, if the organization is also worried about the availability of their services, then the stress testing should be conducted in a non-production environment which is identical to the production environment.

Payment Terms

Another aspect of preparing for a test that many testers completely forget about is how they should be paid. Just like contract dates there should be specific dates and terms for payments. It is not uncommon for larger organizations to delay payment for as long as possible. Below are a few common payment methods. These are simply examples. It is definitely recommended that each organization create and tweak their own pricing structure to more aptly suit the needs of their clients and themselves. The important thing is that some sort of structure be in place before testing begins.

Net 30

The total amount is due within 30 days of the delivery of the final report. This is usually associated with a per month percentage penalty for non-payment. This can be any number of days you wish to grant your customers (i.e. 45, or 60).

Half Upfront

It is not uncommon to require half of the total bill upfront before testing begins. This is very common for longer-term engagements.

Recurring

A recurring payment schedule is more commonly used for long-term engagements. For example, some engagements may span as far as a year or two. It is not at all uncommon to have the customer pay in regular installments throughout the year.

Goals

Every penetration test should be goal-oriented. This is to say that the purpose of the test is to identify specific vulnerabilities that lead to a compromise of the business or mission objectives of the customer. It is not about finding un-patched systems. It is about identifying risk that will adversely impact the organization.

Primary

The primary goal of a test should not be driven by compliance. There are a number of different justifications for this reasoning. First, compliance does not equal security. While it should be understood that many organizations undergo testing because of compliance it should not be the main goal of the test. For example, a firm may be hired to complete a penetration test as part of PCI-DSS requirements.

There is no shortage of companies which process credit card information. However, the traits which make the target organization unique and viable in a competitive market will have the greatest impact if compromised. Credit card systems being compromised would certainly be a serious issue, but credit cards numbers, along with all of the associated customer data being leaked would be catastrophic.

Secondary

The secondary goals are directly related to compliance. It is not uncommon for primary and secondary goals to be very closely related. For example, in the example of the PCI-DSS driven test, getting the credit cards is the secondary goal. Tying that breach of data to the business or mission drivers of the organization is the primary goal. Secondary goals mean something for compliance and/or IT. Primary goals get the attention of upper management.

Business Analysis

Before performing a penetration test it is beneficial to determine the maturity level of the client's security posture. There are a number of organizations which choose to jump directly into a penetration test first assessing this maturity level. For customers with a very immature security program, it is often a good idea to perform a vulnerability analysis first.

Some testers believe there is a stigma surrounding Vulnerability Analysis (VA) work. Those testers have forgotten that the goal is to identify risks in the target organization, not about pursuing the so-called "rockstar" lifestyle. If a company is not ready for a full penetration test, they will get far more value out of a good VA than a penetration test.

Establish with the customer in advance what information about the systems they will be providing. It may also be helpful to ask for information about vulnerabilities which are already documented. This will save the testers time and save the client money by not overlapping testing discoveries with known issues. Likewise, a full or partial white-box test may bring the customer more value than a black-box test, if it isn't absolutely required by compliance.

Establish Lines of Communication

One of the most important aspects of any penetration test is communication with the customer. How often you interact with the customer, and the manner in which you approach them, can make a huge difference in their feeling of satisfaction. Below is a communication framework that will aid in making the customer feel comfortable about the test activities.

Emergency Contact Information

Obviously, being able to get in touch with the customer or target organization in an emergency is vital. Emergencies may arise, and a point of contact must have been established in order to handle them. Create an emergency contact list. This list should include contact information for all parties in the scope of testing. Once created, the emergency contact list should be shared with all those on the list. Keep in mind, the target organization may not be the customer.

Gather the following information about each emergency contact:

1. Full name
2. Title and operational responsibility
3. Authorization to discuss details of the testing activities, if not already specified
4. Two forms of 24/7 immediate contact, such as cell phone, pager, or home phone, if possible
5. One form of secure bulk data transfer, such as SFTP or encrypted email

Note: The number for a group such as the help desk or operations center can replace one emergency contact, but only if it is staffed 24/7. The nature of each penetration test influences who should be on the emergency contact list. Not only will contact information for the customer and targets need to be made available, but they may also need to contact the testers in an emergency. The list should preferably include the following people:

1. All penetration testers in the test group for the engagement
2. The manager of the test group
3. Two technical contacts at each target organization
4. Two technical contacts at the customer
5. One upper management or business contact at the customer

It is possible that there will be some overlap in the above list. For instance, the target organization may be the customer, the test group's manager may also be performing the penetration test, or a customer's technical contact may be in upper management. It is also recommended to define a single contact person per involved party who leads it and takes responsibility on behalf of it.

Incident Reporting Process

Discussing the organization's current incident response capabilities is important to do before an engagement for several reasons. Part of a penetration test is not only testing the security an organization has in place, but also their incident response capabilities.

If an entire engagement can be completed without the target's internal security teams ever noticing, a major gap in security posture has been identified. It is also important to ensure that before testing begins, someone at the target organization is aware of when the tests are being conducted so the incident response team does not start to call every member of upper management in the middle of the night because they thought they were under attack or compromised.

Incident Definition

The National Institute of Standards and Technology (NIST) defines an incident as follows: "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." (Computer Security Incident Handling Guide - Special Publication 800-61 Rev 1). An incident can also occur on a physical level, wherein a person gain unauthorized physical access to an area by any means. The target organization should have different categories and levels for different types of incidents.

Status Report Frequency

The frequency of status reporting can vary widely. Some factors which influence the reporting schedule include the overall length of the test, the test scope, and the target's security maturity. An effective schedule allows the customer to feel engaged. An ignored customer is a former customer.

Once frequency and schedule of status reports has been set, it must be fulfilled. Postponing or delaying a status report may be necessary, but it should not become chronic. The client may be asked to agree to a new schedule if necessary. Skipping a status report altogether is unprofessional and should be avoided if at all possible.

PGP and Other Alternatives

Encryption is not optional. Communication with the customer is an absolutely necessary part of any penetration testing engagement and due to the sensitive nature of the engagement, communications of sensitive information must be encrypted, especially the final report. Before the testing begins, a means of secure communication must be established with the client. Several common means of encryption are as follows:

1. PGP/GPG can be used to both communicate over e-mail and to encrypt the final report (remember that subject lines are passed through in plaintext)
2. A secure mailbox hosted on the customer's network
3. Telephone
4. Face to face meetings
5. To deliver the final report, you can also store the report in an AES encrypted archive file, but make sure that your archive utility supports AES encryption using CBC.

Also ask what kinds of information can be put in writing and which should be communicated only verbally. Some organizations have very good reasons for limiting what security information is transmitted to them in writing.

Rules of Engagement

While the scope defines what will be tested, the rules of engagement defines how that testing is to occur. These are two different aspects which need to be handled independently from each other.

Timeline

A clear timeline should be established for the engagement. While scope defines the start and the end of an engagement, the rules of engagement define everything in between. It should be understood that the timeline will change as the test progresses. However, having a rigid timeline is not the goal of creating one. Rather, having a timeline in place at the beginning of a test will allow everyone involved to more clearly identify the work that is to be done and the people who will be responsible for said work. GANTT Charts and Work Breakdown Structures are often used to define the work and the amount of time that each specific piece of the work will take. Seeing the schedule broken down in this manner aids those involved in identifying where resources need to be applied and it helps the customer identify possible roadblocks which many be encountered during testing.

There are a number of free GANTT Chart tools available on the Internet. Many mangers identify closely with these tools. Because of this, they are an excellent medium for communicating with the upper management of a target organization.

Locations

Another parameter of any given engagement which is important to establish with the customer ahead of time is any destinations to which the testers will need to travel during the test. This could be as simple as identifying local hotels, or complex as identifying the applicable laws of a specific target country.

It is not uncommon for an organization to operate in multiple locations and regions and a few select sites will need to be chosen for testing. In these situations, travel to every customer location should be avoided, instead, it should be determined if VPN connections to the sites are available for remote testing. Disclosure of Sensitive Information

While one of the goals of a given engagement may be to gain access to sensitive information, certain information should not actually be viewed or downloaded. This seems odd to newer testers, however, there are a number of situations where the testers should not have the target data in their possession. For example Personal Health Information (PHI), under the Health Insurance Portability and Accountability Act (HIPAA), this data must be protected. In some situations, the target system may not have a firewall or anti-virus (AV) protecting it. In this sort of situation, the testers being in possession of any and all Personally Identifiable Information (PII) should be absolutely avoided.

However, if the data cannot be physically or virtually obtained, how can it be proved that the testers indeed obtained access to the information? This problem has been solved in a number of ways. There are ways to prove that the vault door was opened without taking any of the money. For instance, a screenshot of database schema and file permissions can be taken, or the files themselves can be displayed without opening them to displaying the content, as long as no PII is visible in the filenames themselves.

How cautious the testers should be on a given engagement is a parameter which needs to be discussed with the client, but the firm doing the testing should always be sure to protect themselves in a legal sense regardless of client opinion. Regardless of supposed exposure to sensitive data, all report templates and tester machines should be sufficiently scrubbed following each engagement. As a special side note, if illegal data (i.e. child pornography) is discovered by the testers, proper law enforcement officials should be notified immediately, followed by the customer. Do not take direction from the customer.

Evidence Handling

When handling evidence of a test and the differing stages of the report it is incredibly important to take extreme care with the data. Always use encryption and sanitize your test machine between tests. Never hand out USB sticks with test reports out at security conferences. And whatever you do, don't re-use a report from another customer engagement as a template! It's very unprofessional to leave references to another organization in your document.

Regular Status Meetings

Throughout the testing process it is critical to have regular meetings with the customer informing them of the overall progress of the test. These meetings should be held daily and should be as short as possible. Meetings should be kept to three concepts: plans, progress and problems.

Plans are generally discussed so that testing is not conducted during a major unscheduled change or an outage. Progress is simply an update to the customer on what has been completed so far. Problems should also be discussed in this meeting, but in the interest of brevity, conversations concerning solutions should almost always be taken offline.

Time of the Day to Test

Certain customers require all testing to be done outside of business hours. This can mean late nights for most testers. The time of day requirements should be well established with the customer before testing begins.

Dealing with Shunning

There are times where shunning is perfectly acceptable and there are times where it may not fit the spirit of the test. For example, if your test is to be a full black-box test where you are testing not only the technology, but the capabilities of the target organization's security team, shunning would be perfectly fine. However, when you are testing a large number of systems in coordination with the target organization's security team it may not be in the best interests of the test to shun your attacks.

Permission to Test

One of the most important documents which need to be obtained for a penetration test is the Permission to Test document. This document states the scope and contains a signature which acknowledges awareness of the activities of the testers. Further, it should clearly state that testing can lead to system instability and all due care will be given by the tester to not crash systems in the process. However, because testing can lead to instability the customer shall not hold the tester liable for any system instability or crashes. It is critical that testing does not begin until this document is signed by the customer.

In addition, some service providers require advance notice and/or separate permission prior to testing their systems. For example, Amazon has an online request form that must be completed, and the request must be approved before scanning any hosts on their cloud. If this is required, it should be part of the document.

Legal Considerations

Some activities common in penetration tests may violate local laws. For this reason, it is advised to check the legality of common pentest tasks in the location where the work is to be performed. For example,any VOIP calls captured in the course of the penetration test may be considered wiretapping in some areas.

Capabilities and Technology in Place

Good penetration tests do not simply check for un-patched systems. They also test the capabilities of the target organization. To that end, below is a list of things that you can benchmark while testing.

1. Ability to detect and respond to information gathering
2. Ability to detect and respond to foot printing
3. Ability to detect and respond to scanning and vuln analysis
4. Ability to detect and respond to infiltration (attacks)
5. Ability to detect and respond to data aggregation
6. Ability to detect and respond to data ex-filtration

When tracking this information be sure to collect time information. For example, if a scan is detected you should be notified and note what level of scan you were preforming at the time.

Retrieved from "http://www.pentest-standard.org/index.php?title=Pre-engagement&oldid=940"