Pre-Engagement Interactions

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?
4. During business hours?
5. After business hours?
6. On the weekends?
7. How many total IP addresses are being tested?
8. How many internal IP addresses, if applicable?

9. How many external IP addresses, if applicable?
10. 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?
11. In the case that a system is penetrated, how should the testing team proceed?
12. Perform a local vulnerability assessment on the compromised machine?
13. Attempt to gain the highest privileges (root on Unix machines, SYSTEM or Administrator on Windows machines) on the compromised machine?
14. 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?
7. If yes, what kind of documentation?
8. Will static analysis be performed on this application?
9. Does the client want fuzzing performed against this application?
10. Does the client want role-based testing performed against this application?
11. 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:
3. Does the guest network require authentication?
4. What type of encryption is used on the wireless networks?
5. What is the square footage of coverage?
6. Will enumeration of rogue devices be necessary?
7. Will the team be assessing wireless attacks against clients?
8. 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:
3. How many floors are in scope?
4. Which floors are in scope?
5. Are there any security guards that will need to be bypassed? If so:
6. Are the security guards employed through a 3rd party?
7. Are they armed?
8. Are they allowed to use force?
9. How many entrances are there into the building?
10. Is the use of lock picks or bump keys allowed? (also consider local laws)
11. Is the purpose of this test to verify compliance with existing policies and procedures or for performing an audit?
12. What is the square footage of the area in scope?
13. Are all physical security measures documented?
14. Are video cameras being used?

15. Are the cameras client-owned? If so:
16. Should the team attempt to gain access to where the video camera data is stored?
17. Is there an armed alarm system being used? If so:
18. Is the alarm a silent alarm?
19. Is the alarm triggered by motion?
20. 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:
4. 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.

Intelligence Garthering

General

This section defines the Intelligence Gathering activities of a penetration test. The purpose of this document is to provide a standard designed specifically for the pentester performing reconnaissance against a target (typically corporate, military, or related). The document details the thought process and goals of pentesting reconnaissance, and when used properly, helps the reader to produce a highly strategic plan for attacking a target.

Background Concepts

Levels are an important concept for this document and for PTES as a whole. It's a maturity model of sorts for pentesting. Defining levels allows us to clarify the expected output and activities within certain real-world constraints such as time, effort, access to information, etc.

The Intelligence Gathering levels are currently split into three categories, and a typical example is given for each one. These should guide the adding of techniques in the document below. For example, an intensive activity such as creating a facebook profile and analyzing the target's social network is appropriate in more advanced cases, and should be labeled with the appropriate level. See the mindmap below for examples.

Level 1 Information Gathering

(think: Compliance Driven) Mainly a click-button information gathering process. This level of information can be obtained almost entirely by automated tools. Bare minimum to say you did IG for a PT.

Acme Corporation is required to be compliant with PCI / FISMA / HIPAA. A Level 1 information gathering effort should be appropriate to meet the compliance requirement.

Level 2 Information Gathering

(think: Best Practice) This level can be created using automated tools from level 1 and some manual analysis. A good understanding of the business, including information such as physical location, business relationships, org chart, etc.

Widgets Inc is required to be in compliance with PCI, but is interested in their long term security strategy, and is acquiring several smaller widget manufacturers. A Level 2 information gathering effort should be appropriate to meet their needs.

Level 3 Information Gathering

(think: State Sponsored) More advanced pentest, Redteam, full-scope. All the info from level 1 and level 2 along with a lot of manual analysis. Think cultivating relationships on SocNet, heavy analysis, deep understanding of business relationships, most likely a large number of hours to accomplish the gathering and correlation.

An Army Red Team is tasked to analyze and attack a segment of the Army's network in a foreign country to find weaknesses that could be exploited by a foreign national. A level 3 information gathering effort would be appropriate in this case.

Intelligence Gathering

What it is

Intelligence Gathering is performing reconnaissance against a target to gather as much information as possible to be utilized when penetrating the target during the vulnerability assessment and exploitation phases. The more information you are able to gather during this phase, the more vectors of attack you may be able to use in the future.

Open source intelligence (OSINT) is a form of intelligence collection management that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence. [1]

Why do it

We perform Open Source Intelligence gathering to determine various entry points into an organization. These entry points can be physical, electronic, and/or human. Many companies fail to take into account what information about themselves they place in public and how this information can be used by a determined attacker. On top of that many employees fail to take into account what information they place about themselves in public and how that information can be used to to attack them or their employer.

What is it not

OSINT may not be accurate or timely. The information sources may be deliberately/accidentally manipulated to reflect erroneous data, information may become obsolete as time passes, or simply be incomplete.

It does not encompass dumpster-diving or any methods of retrieving company information off of physical items found on-premises.

Target Selection

Identification and Naming of Target

When approaching a target organization it is important to understand that a company may have a number of different Top Level Domains (TDLs) and auxiliary businesses. While this information should have been discovered during the scoping phase it is not all that unusual to identify additional servers domains and companies that may not have been part of the initial scope that was discussed in the pre-engagement phase. For example a company may have a TDL of .com. However, they may also have .net .co and .xxx. These may need to be part of the revised scope, or they may be off limits. Either way it needs to be cleared with the customer before testing begins. It is also not all that uncommon for a company to have a number of sub-companies underneath them. For example General Electric and Proctor and Gamble own a great deal of smaller companies.

Consider any Rules of Engagement limitations

At this point it is a good idea to review the Rules of Engagement. It is common for these to get forgotten during a test. Sometimes, as testers we get so wrapped up in what we find and the possibilities for attack that we forget which IP addresses, domains and networks we can attack. Always, be referencing the Rulles of Engagement to keep your tests focused. This is not just important from a legel perspective, it is also important from a scope creep perspective. Every time you get sidetracked from the core objectives of the test it costs you time. And in the long run that can cost your company money.

Consider time length for test

The amount of time for the total test will directly impact the amount of Intelligence Gathering that can be done. There are some tests where the total time is two to three months. In these engagements a testing company would spend a tremendous amount of time looking into each of the core business units and personal of the company. However, for shorter crystal-box style tests the objectives may be far more tactical. For example, testing a specific web application may not require you to research the financial records of the company CEO.

Consider end goal of the test

Every test has an end goal in mind - a particular asset or process that the organization considers critical. Having the end result in mind, the intelligence gathering phase should make sure to include all secondary and tertiary elements surrounding the end goal. Be it supporting technologies, 3rd parties, relevant personnel, etc... Making sure the focus is kept on the critical assets assures that lesser relevant intelligence elements are de-prioritized and categorized as such in order to not intervene with the analysis process.

OSINT

Open Source Intelligence (OSINT) takes three forms; Passive, Semi-passive, and Active.

- **Passive Information Gathering**: Passive Information Gathering is generally only useful if there is a very clear requirement that the information gathering activities never be detected by the target. This type of profiling is technically difficult to perform as we are never sending any traffic to the target organization neither from one of our hosts or “anonymous” hosts or services across the

Internet. This means we can only use and gather archived or stored information. As such this information can be out of date or incorrect as we are limited to results gathered from a third party.

- **Semi-passive Information Gathering**: The goal for semi-passive information gathering is to profile the target with methods that would appear like normal Internet traffic and behavior. We query only the published name servers for information, we aren't performing in-depth reverse lookups or brute force DNS requests, we aren't searching for "unpublished" servers or directories. We aren't running network level portscans or crawlers and we are only looking at metadata in published documents and files; not actively seeking hidden content. The key here is not to draw attention to our activities. Post mortem the target may be able to go back and discover the reconnaissance activities but they shouldn't be able to attribute the activity back to anyone.

- **Active Information Gathering**: Active information gathering should be detected by the target and suspicious or malicious behavior. During this stage we are actively mapping network infrastructure (think full port scans nmap –p1-65535), actively enumerating and/or vulnerability scanning the open services, we are actively searching for unpublished directories, files, and servers. Most of this activity falls into your typically "reconnaissance" or "scanning" activities for your standard pentest.

Corporate

Physical

Locations (L1)

Per location listing of full address, ownership, associated records (city, tax, legal, etc), Full listing of all physical security measures for the location (camera placements, sensors, fences, guard posts, entry control, gates, type of identification, supplier's entrance, physical locations based on IP blocks/geolocation services, etc… For Hosts/NOC: Full CIDR notation of hosts and networks, full DNS listing of all associated assets, Full mapping of AS, peering paths, CDN provisioning, netblock owners (whois data), email records (MX + mail address structure)

- Owner (L1/L2)
- Land/tax records (L1/L2)
- Shared/individual (L1/L2)
- Timezones (L1/L2)
- Hosts / NOC

Pervasiveness (L1)

It is not uncommon for a target organization to have multiple separate physical locations. For example, a bank will have central offices, but they will also have numerous remote branches as well. While physical and technical security may be very good at central locations, remote locations often have poor security controls.

Relationships (L1)

Business partners, customs, suppliers, analysis via whats openly shared on corporate web pages, rental companies, etc. This information can be used to better understand the business or organizational projects. For example, what products and services are critical to the target organization?

Also, this information can also be used to create successful social engineering scenarios.

- Relationships (L2/L3)
  - Manual analysis to vet information from level 1, plus dig deeper into possible relationships.
- Shared office space (L2/L3)
- Shared infrastructure (L2/L3)
- Rented / Leased Equipment (L2/L3)

Logical

Accumulated information for partners, clients and competitors: For each one, a full listing of the business name, business address, type of relationship, basic financial information, basic hosts/network information.

- Business Partners (L1/L2/L3)
  - Target's advertised business partners. Sometimes advertised on main www.
- Business Clients (L1/L2/L3)
  - Target's advertised business clients. Sometimes advertised on main www.
- Competitors (L1/L2/L3)
  - Who are the target's competitors. This may be simple, Ford vs Chevy, or may require much more analysis.
- Touchgraph (L1)
  - A touchgraph (visual representation of the social connections between people) will assist in mapping out the possible interactions between people in the organization, and how to access them from the outside (when a touchgraph includes external communities and is created with a depth level of above 2).
  - The basic touchgraph should reflect the organizational structure derived from the information gathered so far, and further expansion of the graph should be based on it (as it usually represents the focus on the organizational assets better, and make possible approach vectors clear.
- Hoovers profile (L1/L2)
  - What: a semi-open source intelligence resource (paid subscriptions usually). Such sources specialize in gathering business related information on companies, and providing a "normalized" view on the business.
  - Why: The information includes physical locations, competitive landscape, key personnel, financial information, and other business related data (depending on the source). This can be used to create a more accurate profile of the target, and identify additional personnel and 3rd parties which can be used in the test.

- How: Simple search on the site with the business name provide the entire profile of the company and all the information that is available on it. Its recommended to use a couple of sources in order to cross reference them and make sure you get the most up-to-date information. (paid for service).

- Product line (L2/L3)
  - Target's product offerings which may require additional analysis if the target does offer services as well this might require further analysis.
- Market Vertical (L1)
  - Which industry the target resides in. i.e. financial, defense, agriculture, government, etc
- Marketing accounts (L2/L3)
  - Marketing activities can provide a wealth of information on the marketing strategy of the target
  - Evaluate all the social media Networks for the target's social personas
  - Evaluate the target's past * marketing campaigns
- Meetings (L2/L3)
  - Meeting Minutes published?
  - Meetings open to public?
- Significant company dates (L1/L2/L3)
  - Board meetings
  - Holidays
  - Anniversaries
  - Product/service launch
- Job openings (L1/L2)
  - By viewing a list of job openings at an organization (usually found in a 'careers' section of their website), you can determine types of technologies used within the organization. One example would be if an organization has a job opening for a Senior Solaris Sysadmin then it is pretty obvious that the organization is using Solaris systems. Other positions may not be as obvious by the job title, but an open Junior Network Administrator position may say something to the effect of 'CCNA preferred' or 'JNCIA preferred' which tells you that they are either using Cisco or Juniper technologies.
- Charity affiliations (L1/L2/L3)
  - It is very common for executive members of a target organization to be associated with charitable organizations. This information can be used to develop solid social engineering scenarios for targeting executives.
- RFP, RFQ and other Public Bid Information (L1/L2)
  - RFPs and RFQs often reveal a lot of information about the types of systems used by a company, and potentially even gaps or issues with their infrastructure.

- Finding out who current bid winners are may reveal the types of systems being used or a location where company resources might be hosted off-site.

- Court records (L2/L3)
- Court records are usually available either free or sometimes at a fee.
- Contents of litigation can reveal information about past complainants including but not limited to former employee lawsuits
- Criminal records of current and past employees may provide a list of targets for social engineering efforts

- Political donations (L2/L3)
- Mapping out political donations or other financial interests is important in order to identify pivotal individuals who may not be in obvious power positions but have a vested interest (or there is a vested interes in them).
- Political donation mapping will change between countries based on the freedom of information, but often cases donations from other countries can be traced back using the data available there.

- Professional licenses or registries (L2/L3)
- Gathering a list of your targets professional licenses and registries may offer an insight into not only how the company operated, but also the guidelines and regulations that they follow in order to maintain those licenses. A prime example of this is a companies ISO standard certification can show that a company follows set guidelines and processes. It is important for a tester to be aware of these processes and how they could affect tests being performed on the organization.
- A company will often list these details on their website as a badge of honor. In other cases it may be necessary to search registries for the given vertical in order to see if an organization is a member. The information that is available is very dependent on the vertical market, as well as the geographical location of the company. It should also be noted that international companies may be licensed differently and be required to register with different standards or legal bodies dependent on the country.

Org Chart (L1)

- Position identification
- Important people in the organization
- Individuals to specifically target
- Transactions
- Mapping on changes within the organization (promotions, lateral movements)
- Affiliates
- Mapping of affiliate organizations that are tied to the business

Electronic

Document Metadata (L1/L2)

- What it is? Metadata or meta-content provides information about the data/document in scope. It can have information such as author/creator name, time and date, standards used/referred, location

in a computer network (printer/folder/directory path/etc. info), geo-tag etc. For an image its' metadata can contain color, depth, resolution, camera make/type and even the co-ordinates and location information.

- Why you would do it? Metadata is important because it contains information about the internal network, user-names, email addresses, printer locations etc. and will help to create a blueprint of the location. It also contains information about software used in creating the respective documents. This can enable an attacker to create a profile and/or perform targeted attacks with internal knowledge on the networks and users.
- How you would do it? There are tools available to extract the metadata from the file (pdf/word/image) like FOCA (GUI-based), metagoofil (python-based), meta-extractor, exiftool (perl-based). These tools are capable of extracting and displaying the results in different formats as HTML, XML, GUI, JSON etc. The input to these tools is mostly a document downloaded from the public presence of the 'client' and then analyzed to know more about it. Whereas FOCA helps you search documents, download and analyzes all through its GUI interface.

Marketing Communications (L1/L2)

- Past marketing campaigns provide information for projects which might of been retired that might still be accessible.
- Current marketing communications contain design components (Colors, Fonts, Graphics etc..) which are for the most part used internally as well.
- Additional contact information including external marketing organizations.

Infrastructure Assets

Network blocks owned (L1)

- Network Blocks owned by the organization can be passively obtained from performing whois searches. DNSStuff.com is a one stop shop for obtaining this type of information.
- Open Source searches for IP Addresses could yield information about the types of infrastructure at the target. Administrators often post ip address information in the context of help requests on various support sites.

Email addresses (L1)

- E-mail addresses provide a potential list of valid usernames and domain structure
- E-mail addresses can be gathered from multiple sources including the organizations website.

External infrastructure profile (L1)

- The target's external infrastructure profile can provide immense information about the technologies used internally.
- This information can be gathered from multiple sources both passively and actively.
- The profile should be utilized in assembling an attack scenario against the external infrastructure.

Technologies used (L1/L2)

- OSINT searches through support forums, mailing lists and other resources can gather information of technologies used at the target
- Use of Social engineering against the identified information technology organization
- Use of social engineering against product vendors

Purchase agreements (L1/L2/L3)

- Purchase agreements contain information about hardware, software, licenses and additional tangible asset in place at the target.

Remote access (L1/L2)

- Obtaining information on how employees and/or clients connect into the target for remote access provides a potential point of ingress.
- Often times link to remote access portal are available off of the target's home page
- How To documents reveal applications/procedures to connect for remote users

Application usage (L1/L2)

Gather a list of known application used by the target organization. This can often be achieved by extracting metadata from publicly accessible files (as discussed previously)

Defense technologies (L1/L2/L3)

Fingerprinting defensive technologies in use can be achieved in a number of ways depending on the defenses in use.

Passive fingerprinting

- Search forums and publicly accessible information where technicians of the target organisation may be discussing issues or asking for assistance on the technology in use
- Search marketing information for the target organisation as well as popular technology vendors
- Using Tin-eye (or another image matching tool) search for the target organisations logo to see if it is listed on vendor reference pages or marketing material

Active fingerprinting

- Send appropriate probe packets to the public facing systems to test patterns in blocking. Several tools exist for fingerprinting of specific WAF types.
- Header information both in responses from the target website and within emails often show information not only on the systems in use, but also the specific protection mechanisms enabled (e.g. Email gateway Anti-virus scanners)

Human capability (L1/L2/L3)

Discovering the defensive human capability of a target organization can be difficult. There are several key pieces of information that could assist in judging the security of the target organization.

- Check for the presence of a company-wide CERT/CSIRT/PSRT team
- Check for advertised jobs to see how often a security position is listed
- Check for advertised jobs to see if security is listed as a requirement for non-security jobs (e.g. developers)
- Check for out-sourcing agreements to see if the security of the target has been outsourced partially or in it's entirety
- Check for specific individuals working for the company that may be active in the security community

Financial

Reporting (L1/L2)

The targets financial reporting will depend heavily on the location of the organization. Reporting may also be made through the organizations head office and not for each branch office. In 2008 the SEC issued a proposed roadmap for adoption of the International Financial Reporting Standards (IFRS) in the US.

IFRS Adoption per country --> http://www.iasplus.com/en/resources/use-of-ifrs

Market analysis (L1/L2/L3)

- Obtain market analysis reports from analyst organizations (such as Gartner, IDC, Forrester, 541, etc...). This should include what the market definition is, market cap, competitors, and any major changes to the valuation, product, or company in general.

Trade capital

- Identify is the organization is allocating any trade capital, and in what percentage of the overall valuation and free capital it has. This will indicate how sensitive the organization is to market fluctuations, and whether it depends on external investment as part of it's valuation and cash flow.

Value history

- Charting of the valuation of the organization over time, in order to establish correlation between external and internal events, and their effect on the valuation.

EDGAR (SEC)

- What is it: EDGAR (the Electronic Data Gathering, Analysis, and Retrieval system) is a database of the U.S. Security and Exchanges Commission (SEC) that contains registration statements, periodic reports, and other information of all companies (both foreign and domestic) who are required by law to file.
- Why do it: EDGAR data is important because, in additional to financial information, it identifies key personnel within a company that may not be otherwise notable from a company's website or other public presence. It also includes statements of executive compensation, names and addresses of major common stock owners, a summary of legal proceedings against the company, economic risk factors, and other potentially interesting data.
- How to obtain: The information is available on the SEC's EDGAR website (http://www.sec.gov/edgar.shtml). Reports of particular interest include the 10-K (annual report) and 10-Q (quarterly report).

Individual

Employee

History

- Court Records (L2/L3)
- What is it: Court records are all the public records related to criminal and/or civil complaints, lawsuits, or other legal actions for or against a person or organization of interest.
- Why you would do it: Court records could potentially reveal sensitive information related to an individual employee or the company as a whole. This information could be useful by itself or may be the driver for gaining additional information. It could also be used for social engineering or other purposes later on in the penetration test.
- How you would do it: Much of this information is now available on the Internet via publicly available court websites and records databases. Some additional information may be available via pay services such as LEXIS/NEXIS. Some information may be available via records request or in person requests.
- Political Donations (L2/L3)
- What is it: Political donations are an individual's personal funds directed to specific political candidates, political parties, or special interest organizations.
- Why you would do it: Information about political donations could potentially reveal useful information related to an individual. This information could be used as a part of social network analysis to help draw connections between individuals and politicians, political candidates, or other

political organizations. It could also be used for social engineering or other purposes later on in the penetration test.

- How you would do it: Much of this information is now available on the Internet via publicly available websites (i.e., http://www.opensecrets.org/) that track political donations by individual. Depending upon the laws of a given state, donations over a certain amount are usually required to be recorded.
- Professional licenses or registries (L2/L3)
- What is it: Professional licenses or registries are repositories of information that contain lists of members and other related information for individuals who have attained a particular license or some measure of specific affiliation within a community.
- Why you would do it: Information about professional licenses could potentially reveal useful information related to an individual. This information could be used to validate an individual's trustworthiness (do they really have a particular certification as they claim) or as a part of social network analysisto help draw connections between individuals and other organizations. It could also be used for social engineering or other purposes later on in the penetration test.
- How you would do it: Much of this information is now available on the Internet via publicly available websites. Typically, each organization maintains their own registry of information that may be available online or may require additional steps to gather.

Social Network (SocNet) Profile

- Metadata Leakage (L2/L3)
- Location awareness via Photo Metadata
- Tone (L2/L3)
- Expected deliverable: subjective identification of the tone used in communications – aggressive, passive, appealing, sales, praising, dissing, condescending, arrogance, elitist, underdog, leader, follower, mimicking, etc…
- Frequency (L2/L3)
- Expected deliverable: Identification of the frequency of publications (once an hour/day/week, etc…). Additionally - time of day/week in which communications are prone to happen.
- Location awareness (L2/L3)

  - Map location history for the person profiled from various sources, whether through direct interaction with applications and social networks, or through passive participation through photo metadata.

- Bing Map Apps
- Foursquare
- Google Latitude
- Yelp
- Gowalla
- Social Media Presence (L1/L2/L3)

  - Verify target’s social media account/presence (L1). And provide detailed analysis (L2/L3)

Internet Presence

- Email Address (L1)
- What it is? Email addresses are the public mail box ids of the users.
- Why you would do it? Email address harvesting or searching is important because it serves multiple purposes - provides a probable user-id format which can later be brute-forced for access but more

importantly it helps sending targeted spams and even to automated bots. These spam emails can contain exploits, malware etc. and can be addressed with specific content particularly to a user.

- How you would do it? Email addresses can be searched and extracted from various websites, groups, blogs, forums, social networking portals etc. These email addresses are also available from various tech support websites. There are harvesting and spider tools to perform search for email addresses mapped to a certain domain (if needed).
- Personal Handles/Nicknames (L1)
- Personal Domain Names registered (L1/L2)
- Assigned Static IPs/Netblocks (L1/L2)

Physical Location

- Physical Location
- Can you derive the target's physical location

Mobile Footprint

- Phone number (L1/L2/L3)
- Device type (L1/L2/L3)
- Use (L1/L2/L3)
- Installed applications (L1/L2/L3)
- Owner/administrator (L1/L2/L3)

"For Pay" Information

- Background Checks
- For Pay Linked-In
- LEXIS/NEXIS

Covert Gathering

Corporate

On-Location Gathering

Selecting specific locations for onsite gathering, and then performing reconnaissance over time (usually at least 2-3 days in order to assure patterns). The following elements are sought after when performing onsite intelligence gathering:

- Physical security inspections
- Wireless scanning / RF frequency scanning
- Employee behavior training inspection
- Accessible/adjacent facilities (shared spaces)
- Dumpster diving
- Types of equipment in use

Offsite Gathering

Identifying offsite locations and their importance/relation to the organization. These are both logical as well as physical locations as per the below:

- Data center locations
- Network provisioning/provider

HUMINT

Human intelligence complements the more passive gathering on the asset as it provides information that could not have been obtained otherwise, as well as add more “personal” perspectives to the intelligence picture (feelings, history, relationships between key individuals, “atmosphere”, etc...)

The methodology of obtaining human intelligence always involves direct interaction - whether physical, or verbal. Gathering should be done under an assumed identity, that would be created specifically to achieve optimal information exposure and cooperation from the asset in question.

Additionally, intelligence gathering on more sensitive targets can be performed by utilizing observation only - again, either physically on location, or through electronic/remote means (CCTV, webcams, etc...). This is usually done in order to establish behavioral patterns (such as frequency of visitations, dress code, access paths, key locations that may provide additional access such as coffee shops).

Results

- Key Employees
- Partners/Suppliers
- Social Engineering

Footprinting

WHAT IT IS: External information gathering, also known as footprinting, is a phase of information gathering that consists of interaction with the target in order to gain information from a perspective external to the organization.

WHY: Much information can be gathered by interacting with targets. By probing a service or device, you can often create scenarios in which it can be fingerprinted, or even more simply, a banner can be procured which will identify the device. This step is necessary to gather more information about your targets. Your goal, after this section, is a prioritized list of targets.

External Footprinting

Identify Customer External Ranges

One of the major goals of intelligence gathering during a penetration test is to determine hosts which will be in scope. There are a number of techniques which can be used to identify systems, including using reverse DNS lookups, DNS bruting, WHOIS searches on the domains and the ranges. These techniques and others are documented below.

Passive Reconnaissance

WHOIS Lookups

For external footprinting, we first need to determine which one of the WHOIS servers contains the information we're after. Given that we should know the TLD for the target domain, we simply have to locate the Registrar that the target domain is registered with.

WHOIS information is based upon a tree hierarchy. ICANN (IANA) is the authoritative registry for all of the TLDs and is a great starting point for all manual WHOIS queries.

- ICANN - http://www.icann.org
- IANA - http://www.iana.com
- NRO - http://www.nro.net
- AFRINIC - http://www.afrinic.net

- APNIC - http://www.apnic.net
- ARIN - http://ws.arin.net
- LACNIC - http://www.lacnic.net
- RIPE - http://www.ripe.net

Once the appropriate Registrar was queried we can obtain the Registrant information. There are numerous sites that offer WHOIS information; however for accuracy in documentation, you need to use only the appropriate Registrar.

- InterNIC - http://www.internic.net/ http://www.internic.net]

Typically, a simple whois against ARIN will refer you to the correct registrar.

BGP looking glasses

It is possible to identify the Autonomous System Number (ASN) for networks that participate in Border Gateway Protocol (BGP). Since BGP route paths are advertised throughout the world we can find these by using a BGP4 and BGP6 looking glass.

- BGP4 - http://www.bgp4.as/looking-glasses
- BPG6 - http://lg.he.net/

Active Footprinting

Port Scanning

Port scanning techniques will vary based on the amount of time available for the test, and the need to be stealthy. If there is zero knowledge of the systems, a fast ping scan can be used to identify systems. In addition, a quick scan without ping verification (-PN in nmap) should be run to detect the most common ports avialable. Once this is complete, a more comprehensive scan can be run. Some testers check for only open TCP ports, make sure to check UDP as well. The http://nmap.org/nmap_doc.html document details port scan types. Nmap ("Network Mapper") is the de facto standard for network auditing/scanning. Nmap runs on both Linux and Windows.

You can find more information on the use of Nmap for this purpose in the PTES Technical Guideline

Nmap has dozens of options available. Since this section is dealing with port scanning, we will focus on the commands required to perform this task. It is important to note that the commands utilized depend mainly on the time and number of hosts being scanned. The more hosts or less time that you have to perform this tasks, the less that we will interrogate the host. This will become evident as we continue to discuss the options.

IPv6 should also be tested.

Banner Grabbing

Banner Grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports. Banner grabbing is used to identify network the version of applications and operating system that the target host are running.

Banner grabbing is usually performed on Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 respectively. Tools commonly used to perform banner grabbing are Telnet, nmap, and Netcat.

SNMP Sweeps

SNMP sweeps are performed too as they offer tons of information about a specific system. The SNMP protocol is a stateless, datagram oriented protocol. Unfortunately SNMP servers don't

respond to requests with invalid community strings and the underlying UDP protocol does not reliably report closed UDP ports. This means that "no response" from a probed IP address can mean either of the following:

- machine unreachable
- SNMP server not running
- invalid community string
- the response datagram has not yet arrived

Zone Transfers

DNS zone transfer, also known as AXFR, is a type of DNS transaction. It is a mechanism designed to replicate the databases containing the DNS data across a set of DNS servers. Zone transfer comes in two flavors, full (AXFR) and incremental (IXFR). There are numerous tools available to test the ability to perform a DNS zone transfer. Tools commonly used to perform zone transfers are host, dig and nmap.

SMTP Bounce Back

SMTP bounce back, also called a Non-Delivery Report/Receipt (NDR), a (failed) Delivery Status Notification (DSN) message, a Non-Delivery Notification (NDN) or simply a bounce, is an automated electronic mail message from a mail system informing the sender of another message about a delivery problem. This can be used to assist an attacker in fingerprint the SMTP server as SMTP server information, including software and versions, may be included in a bounce message.

This can be done by simply creating a bogus address within the target's domain. For instance, asDFADSF_garbage_address@target.com could be used to test target.com. Gmail provides full access to the headers, making it an easy choice for testers.

DNS Discovery

DNS discovery can be performed by looking at the WHOIS records for the domain's authoritative nameserver. Additionally, variations of the main domain name should be checked, and the website should be checked for references to other domains which could be under the target's control.

Forward/Reverse DNS

Reverse DNS can be used to obtain valid server names in use within an organizational. There is a caveat that it must have a PTR (reverse) DNS record for it to resolve a name from a provided IP address. If it does resolve then the results are returned. This is usually performed by testing the server with various IP addresses to see if it returns any results.

DNS Bruteforce

After identifying all the information that is associated with the client domain(s), it is now time to begin to query DNS. Since DNS is used to map IP addresses to hostnames, and vice versa we will want to see if it is insecurely configure. We will seek to use DNS to reveal additional information about the client. One of the most serious misconfigurations involving DNS is allowing Internet users to perform a DNS zone transfer. There are several tools that we can use to enumerate DNS to not only check for the ability to perform zone transfers, but to potentially discover additional host names that are not commonly known.

Web Application Discovery

Identifying weak web applications can be a particularly fruitful activity during a penetration test. Things to look for include OTS applications that have been misconfigured, OTS application which have plugin functionality (plugins often contain more vulnerable code than the base application),

and custom applications. Web application fingerprinters such as WAFP can be used here to great effect.

Virtual Host Detection & Enumeration

Web servers often host multiple "virtual" hosts to consolidate functionality on a single server. If multiple servers point to the same DNS address, they may be hosted on the same server. Tools such as MSN search can be used to map an ip address to a set of virtual hosts.

Establish External Target List

Once the activities above have been completed, a list of users, emails, domains, applications, hosts and services should be compiled.

Mapping versions

Version checking is a quick way to identify application information. To some extent, versions of services can be fingerprinted using nmap, and versions of web applications can often be gathered by looking at the source of an arbitrary page.

Identifying patch levels

To identify the patch level of services internally, consider using software which will interrogate the system for differences between versions. Credentials may be used for this phase of the penetration test, provided the client has acquiesced. Vulnerability scanners are particularly effective at identifying patch levels remotely, without credentials.

Looking for weak web applications

Identifying weak web applications can be a particularly fruitful activity during a penetration test. Things to look for include OTS applications that have been misconfigured, OTS application which have plugin functionality (plugins often contain more vulnerable code than the base application), and custom applications. Web application fingerprinters such as WAFP can be used here to great effect.

Identify lockout threshold

Identifying the lockout threshold of an authentication service will allow you to ensure that your bruteforce attacks do not intentionally lock out valid users during your testing. Identify all disparate authentication services in the environment, and test a single, innocuous account for lockout. Often 5 - 10 tries of a valid account is enough to determine if the service will lock users out.

Internal Footprinting

Passive Reconnaissance

If the tester has access to the internal network, packet sniffing can provide a great deal of information. Use techniques like those implemented in p0f to identify systems.

Identify Customer Internal Ranges

When performing internal testing, first enumerate your local subnet, and you can often extrapolate from there to other subnets by modifying the address slightly. Also, a look a the routing table of an internal host can be particularly telling. Below are a number of techniques which can be used.

DHCP servers can be a potential source of not just local information, but also remote IP range and details of important hosts. Most DHCP servers will provide a local IP gateway address as well as the

address of DNS and WINS servers. In Windows based networks, DNS servers tend to be Active Directory domain controllers, and thus targets of interest.

Active Reconnaissance

Internal active reconnaissance should contain all the elements of an external one, and in addition should focus on intranet functionality such as:

- Directory services (Active Directory, Novell, Sun, etc...)
- Intranet sites providing business functionality
- Enterprise applications (ERP, CRM, Accounting, etc...)
- Identification of sensitive network segments (accounting, R&D, marketing, etc...)
- Access mapping to production networks (datacenters)
- VoIP infrastructure
- Authentication provisioning (kerberos, cookie tokens, etc...)
- Proxying and internet access management

Identify Protection Mechanisms

The following elements should be identified and mapped according to the relevant location/group/persons in scope. This will enable correct application of the vulnerability research and exploitation to be used when performing the actual attack - thus maximizing the efficiency of the attack, and minimizing the detection ratio.

Network Based Protections

- "Simple" Packet Filters
- Traffic Shaping Devices
- DLP Systems
- Encryption/Tunneling

Host Based Protections

- Stack/Heap Protections
- Application Whitelisting
- AV/Filtering/Behavioral Analysis
- DLP Systems

Application Level Protections

- Identify Application Protections
- Encoding Options
- Potential Bypass Avenues
- Whitelisted Pages

Storage Protections

- HBA - Host Level
- LUN Masking
- Storage Controller
- iSCSI CHAP Secret

User Protections

- AV/Spam Filtering Software
  - SW Configuration which limit exploitability can be considered antispam / antiAV

Threat Modeling

General

This section defines a threat modeling approach as required for a correct execution of a penetration testing. The standard does not use a specific model, but instead requires that the model used be consistent in terms of its representation of threats, their capabilities, their qualifications as per the organization being tested, and the ability to repeatedly be applied to future tests with the same results.

The standard focuses on two key elements of traditional threat modeling - assets and attacker (threat community/agent). Each one is respectively broken down into business assets and business processes and the threat communities and their capabilities.

As a minimum, all four elements should be clearly identified and documented in every penetration test.

When modeling the attacker side, on top of the threat community (which is mostly semantic and can be tied back to the organization's business SWOT analysis), and the capabilities (which is mostly technical), additional aspects of motivation modeling should also be provided. These additional points essentially take into account the value of the different assets available at the target and are combined with the cost of acquiring it. As a complementary model, impact modeling should also be performed for the organization in order to provide a more accurate view of the "what-if?" scenario surrounding the loss event of each of the identified assets. This should take into account the assets "net" value, its intrinsic value, and other indirectly incurred costs associated with a loss event.

The threat modeling phase of any penetration testing engagement is critical for both the testers, as well as the organization. It provides clarity as far as the organization's risk appetite and prioritization (which assets are more important than others? what threat communities are more relevant than others?). Additionally, it enables the tester to focus on delivering an engagement that closely emulates the tools, techniques, capabilities, accessibility and general profile of the attacker, while keeping in mind what are the actual targets inside the organization such that the more relevant controls, processes, and infrastructure are put to the test rather than an inventory list of IT elements. The threat model should be constructed in coordination with the organization being tested whenever possible, and even in a complete black-box situation where the tester does not

have any prior information on the organization, the tester should create a threat model based on the attacker's view in combination with OSINT related to the target organization.

The model should be clearly documented, and be delivered as part of the final report as the findings in the report will reference the threat model in order to create a more accurate relevance and risk score that is specific to the organization (rather than a generic technical one).

High level threat modeling process

1. Gather relevant documentation
2. Identify and categorize primary and secondary assets
3. Identify and categorize threats and threat communities
4. Map threat communities against primary and secondary assets

Example

In the light of a PTES assessment the internally hosted CRM application may be in scope. The customer information stored in the back-end database is an easily identifiable primary asset as it is directly linked to the application in scope. However, by reviewing the technical design of the database server, it can also be identified that the HR database stored on the same back-end database server is a secondary asset. An attacker can use the CRM application as a stepping stone to obtain employee information. In a basic threat modeling exercise, certain threat communities may be identified as not relevant when mapped to the CRM application, but by identifying the secondary assets the threat landscape suddenly changes.

High level modeling tools

There are a variety of tools available to identify targets and map attack vectors. These normally focus on the business assets (what systems to target) and business processes (how to attack them.) Depending on the engagement, the penetration testing team may perform these exercises with no input from the customer; or they may spend a lot of time with customer stakeholders identifying targets of interest. Tools with a business asset focus usually require a quantitative input to describe how important each potential target is to test. The inputs may also be qualitative, such as a description by the customer's CIO that a system is mission-critical. Tools focused on business processes, information flows and technical architecture are used to identify potential attack vectors and choose which are mostly likely to succed or most likely to be used by a certain class of adversary.

Business Asset Analysis

During the business asset analysis part of the threat modeling exercise an asset-centric view is taken on all assets, and business processes they support them, included in the scope. By analyzing the gathered documentation and interviewing relevant personnel within the organization, the pentester is able to identify the assets that are most likely to be targeted by an attacker, what their value is and what the impact of their (partial) loss would be.

Organizational Data

Policies, Plans, and Procedures

Internal policies, plans, and procedures define how the organization does business. These documents are of particular interest as they can help identify key roles within an organization and critical business processes that keep a company running.

Product Information (e.g. trade secrets, R&D data)

Product related information includes any patents, trade secrets, future plans, source code, supporting systems that directly affect the product market value, algorithms, and any other information that the organization regards as a key factor to the business success of such product.

Marketing Information (plans, roadmaps, etc.)

Marketing plans for promotions, launches, product changes, positioning, partnerships, 3rd party providers, business plans related to activities inside or outside the organization. Additionally, PR related data such as details of partners, reporters, consulting firm, and any correspondence with such entities is also considered a highly sought after target.

Financial Information (e.g. bank, credit, equity accounts)

Financial information is often some of the most guarded information an organization possesses. This information can include bank account information, credit card account information and/or credit card numbers, and investment accounts, among others.

Technical Information

Technical information about the organization, and the organization's operations, is of unique interest to the penetration tester. Such information is often not the expected deliverable of a penetration test, however, it facilitates the testing process by feeding valuable information to other areas; infrastructure design information may provide valuable data to the Intelligence Gathering process.

- Infrastructure Design Information

  Infrastructure design related information pertains to all the core technologies and facilities used to run the organization. Building blueprints, technical wiring and connectivity diagrams, computing equipment/networking designs, and application level data processing are all considered infrastructure design information.

- System Configuration Information

  System configuration information includes configuration baseline documentation, configuration checklists and hardening procedures, group policy information, operating system images, software inventories, etc. This information could aid the discovery of vulnerabilities (such as through the knowledge of configuration errors or outdated software installations).

- User Account Credentials

  User account credentials help facilitate access to the information system, at a non-privileged level, as long as a means to authenticate exists (e.g. VPN, web portal, etc.).

- Privileged User Account Credentials

  Privileged user account credentials help facilitate access to the information system, at an elevated level of access, as long as a means to authenticate exists (e.g. VPN, web portal, etc.). Obtaining privileged user account credentials often leads to compromise of the information system being tested.

Employee Data

Here employee data is being analyzed as any data that can have a DIRECT affect on the organization is obtained or compromised by an attacker. Organizations that have to adhere to some compliance which places fines on the loss or exposure of such data are obvious candidates for such a direct loss

effect. Also, organizations who's employees may be considered critical assets may also be subjected to such scrutiny (specific government bodies, specialized trade secret related employees/departments, etc…). The following list provides examples to information realms of personal data that may be considered business assets for the threat modeling.

- National Identification Numbers (SSNs, etc.)
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Financial Information (e.g. bank, credit accounts)

Customer Data

Much like employee data, customer data is considered a business asset in the threat modeling process when such information will incur a direct/indirect loss to the organization. On top of regulatory/compliance need (based on fines), an additional factor comes into play here when such data can be used to conduct fraud, where the organization may be held liable or sued for the losses related to the fraud (based on losing the customer information that enabled the fraud to take place). The following list provides examples of such information realms that may hold relevant customer data and should be considered business assets for the sake of the threat modeling

- National Identification Numbers (SSN's, etc.)
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Financial Accounts (e.g. bank, credit, equity accounts)
- Supplier Data

Information related to suppliers that is considered critical to the organization (such as critical component manufacturers, agreements with suppliers that may be part of a trade secret, cost analysis of supplied components), as well as any data that may be used to affect the business operations of the organization through its suppliers is considered a business asset.

- Partner Data
- "Cloud" Service Account Information

Human Assets

When identifying human assets in an organization, we have to remember that the context is having such assets part of a greater effort to compromise the organization. As such, human assets that are identified as business assets are those that could be leveraged to divulge information, manipulated to make decisions or actions that would adversely affect the organization or enable an attacker to further compromise it. Human assets are not necessarily the highest up within the corporate hierarchy, but are more often key personnel that are related to previously identified business assets, or are in positions to enable access to such assets. This list can also include employees that normally would not be associated with access to restricted company assets, but may be in a position to grant physical access to a company that facilitates a breach of security or procedure. The following list provides some examples of such assets, and should be adapted to the organization being tested.

- Executive Management
- Executive Assistants
- Middle Management
- Administrative Assistants
- Technical/Team Leads

- Engineers
- Technicians
- Human Resources

Business Process Analysis

A business isn't a business if it doesn't make money. The way this happens is by having either raw goods or knowledge run through various processes to enhance them and create added value. This generates revenue. Business processes and the assets (people, technology, money) supporting them form value chains. By mapping these processes, identifying the critical vs. non-critical processes and eventually finding flaws in them we are able to understand how the business works, what makes them money and eventually how specific threat communities can make them lose money.

In the business process analysis we differentiate between critical business processes, and non-critical processes. For each category the analysis is the same, and takes into account the same elements. The main difference is in the weighting that the threat from a critical business process is assigned with as opposed to a non-critical one. Nevertheless, it's imperative to remember that an aggregation of a few non-critical business processes can be combined into a scenario that essentially forms a critical flaw within an element/process. Such threat scenarios should also be identified within this phase and mapped out for later use in the penetration test.

Technical infrastructure supporting process

As business processes are usually supported by IT infrastructure (such as computer networks, processing power, PCs for entering information and managing the business process, etc...), all those elements must be identified and mapped. Such mapping should be clear enough to be used later on in the process when translating the threat model to the vulnerability mapping and exploitation.

Information assets supporting process

Contrary to technical infrastructure, information assets are existing knowledge bases in the organization that are used as either a reference, or as support material (decision making, legal, marketing, etc...). Such assets are usually identified in the business process already, and should be mapped alongside the technical infrastructure, as well as any additional technical infrastructure that supports the information assets themselves.

Human assets supporting process

Identification of the HR that are involved in the business process should be made in conjunction with the process analysis itself (whether documented or not), and every person that has any kind of involvement (even if it does not relate to a specific information asset or a technical infrastructure element) should be documented and mapped in the process. Such HR assets are usually part of an approval sub-process, a verification sub-process, or even a reference (such as legal advice). These kinds of assets (especially ones that have no relation to information assets or technical infrastructure) would be later mapped to attack vectors that are more social than technical in nature.

3rd party integration and/or usage of/by process

Similar to human assets supporting the process, any 3rd party that has any involvement with the business process should be mapped as well. This category can be tricky to map out, as it could contain both human assets, as well as information/technical ones (such as a SaaS provider).

Threat Agents/Community Analysis

When defining the relevant threat communities and agents, a clear identification of the threat should be provided in terms of location (internal / external to the organization), the specific community within the location, and any additional relevant information that would assist in establishing a capabilities/motivation profile for the specific agent/community. Where possible, specific agents should be identified. Otherwise, a more general community should be outlined, along-with any supporting material and intelligence. Some examples of threat agent/community classifications are:

Internal	External
Employees	Business Partners
Management (executive, middle)	Competitors
Administrators (network, system, server)	Contractors
Developers	Suppliers
Engineers	Nation States
Technicians	Organized Crime
Contractors (with their external users)	Hacktivists
General user community	Script Kiddies (recreational/random hacking)
Remote Support	

Employees

Persons working directly for the company under a part-time or full-time contract. In general they are not regarded as posing a severe threat as most of them are relying on the company to make a living and, assuming they are treated well, are inclined to protect the company rather than to hurt it. Oftentimes involved in data loss incidents or accidental compromise. In rare cases they may be motivated by outsiders to assist in intrusions or they may engage in malicious acts on their own (e.g. rogue traders). While the skill level may vary, it is usually low to medium.

Management (Executive, middle)

Employees working directly for the company as described above. Given their position and function within the company they oftentimes have access to privileged information and may

Threat Capability Analysis

Once a threat community has been identified, the capabilities of said community must also be analyzed in order to build an accurate threat model that reflects the actual probability of such a community/agent to successfully act upon the organization and compromise it. This analysis requires both a technical analysis as well as an opportunity analysis (where applicable).

Analysis of tools in use

Any tools that are known to be available to the threat community/agent are to be included here. Additionally, tools that may be freely available should be analyzed for the required skill level needed to be able to utilize them to their potential, and mapped in the threat capability.

Availability to relevant exploits/payloads

The threat community/agent should be analyzed in terms of its capability to either obtain or develop exploits for the environment relevant to the organization. Additionally, accessibility to such exploits/payloads through 3rd parties, business partners, or underground communities should also be to taken into account in this analysis.

Communication mechanisms

An analysis of communication mechanisms available to the threat agent/community should be made to evaluate the complexity of attacks against an organization. These communication mechanisms range from simple and openly available technologies such as encryption, through to specialist tools and services such as bulletproof hosting, use of drop-sites, and the use of known or unknown botnets to perform attacks or mask source information. For example, as part of testing we test to see what the overall attack surface for an organization is from the outside. However, there is another whole component that is often times missed. What types of threats can exist post exploitation? This falls under the context of detecting exfiltration channels. Coincidentally, penetration testers are uniquely situated to test an organizations capability to detect command and control channels of today's modern malware. When this is in scope, we recommend the tester create a series of malware specimens that increase the level of obfuscation used to hide C2. The goal is to create malware that is easily detected, then increase the obfuscation to the point where detection no longer occurs.

Accessibility

The final element in the threat actor capability analysis is their accessibility to the organization and/or the specific assets in question. Completing the profile depicted above while factoring in accessibility analysis would enable the penetration test to create clear scenarios that are relevant to the organization’s risk.

Motivation Modeling

The possible motivation of threat agents/communities should be noted for further analysis. Motivations of attackers are constantly changing, as can be seen by the increase in hacktivism branded attacks by groups such as Anonymous and Antisec. There will be subtle differences in unique motivations based on each organization and/or vertical market, some common motivations include :

- Profit (direct or indirect)
- Hacktivism
- Direct grudge
- Fun / Reputation
- Further access to partner/connected systems

Finding relevant news of comparable Organizations being compromised

In order to provide a complete threat model, a comparison to other organizations within the same industry vertical should be provided. This comparison should include any relevant incidents or news related to such organizations and the challenges they face. Such a comparison is used to validate the threat model and offer a baseline for the organization to compare itself to (taking into account that this publicly available information only represents a portion of the actual threats and incidents the compared organization actually face).

Vulnerability Analysis

Testing

Vulnerability testing is the process of discovering flaws in systems and applications which can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration, or insecure application design. Although the process used to look for flaws varies and is highly dependent on the particular component being tested, some key principals apply to the process.

When conducting vulnerability analysis of any type the tester should properly scope the testing for applicable depth and breadth to meet the goals and/or requirements of the desired outcome. Depth values can include such things as the location of an assessment tool, authentication requirements, etc. For example; in some cases it maybe the goal of the test to validate mitigation is in place and working and the vulnerability is not accessible; while in other instances the goal maybe to test every applicable variable with authenticated access in an effort to discover all applicable vulnerabilities. Whatever your scope, the testing should be tailored to meet the depth requirements to reach your goals. Depth of testing should always be validated to ensure the results of the assessment meet the expectation (i.e. did all the machines authenticate, etc.). In addition to depth, breadth must also be taken into consideration when conducting vulnerability testing. Breadth values can include things such as target networks, segments, hosts, application, inventories, etc. At its simplest element, your testing may be to find all the vulnerabilities on a host system; while in other instances you may need to find all the vulnerabilities on hosts with in a given inventory or boundary. Additionally breadth of testing should always be validated to ensure you have met your testing scope (i.e. was every machine in the inventory alive at the time of scanning? If not, why).

Active

Active testing involves direct interaction with the component being tested for security vulnerabilities. This could be low level components such as the TCP stack on a network device, or it could be components higher up on the stack such as the web based interface used to administer such a device. There are two distinct ways to interact with the target component: automated, and manual.

Automated

Automated testing utilizes software to interact with a target, examine responses, and determine whether a vulnerability exists based on those responses. An automated process can help reduce time and labor requirements. For example, while it is simple to connect to a single TCP port on a system to determine whether it is open to receive incoming data, performing this step once for each of the available 65,535 possible ports requires a significant amount of time if done manually. When such a test must be repeated on multiple network addresses, the time required may simply be too great to allow testing to be completed without some form of automation. Using software to perform these functions allows the tester to accomplish the task at hand, and focus their attention on processing data and performing tasks which are better suited to manual testing.

Network/General Vulnerability Scanners

Port Based

An automated port based scan is generally one of the first steps in a traditional penetration test because it helps obtain a basic overview of what may be available on the target network or host. Port based scanners check to determine whether a port on a remote host is able to receive a connection. Generally, this will involve the protocols which utilize IP (such as TCP, UDP, ICMP, etc.), However, ports on other network protocols could be present as well dependent on the environment (for example, it's quite common in large mainframe environments for SNA to be in use). Typically, a port can have one of two possible states:

```
   Open - the port is able to receive data    Closed - the port is not
able to receive data
```

A scanner may list other states, such as “filtered”, if it is unable to accurately determine whether a given port is open or closed.

When the scanner determines that a port is open, a presumption is made by the scanner as to whether a vulnerability is present or not. For example, if a port based scanner connects to TCP port 23, and that port is listening, the scanner is likely to report that the telnet service is available on the remote host, and flag it as having a clear text authentication protocol enabled.

Service Based

A service based vulnerability scanner is one which utilizes specific protocols to communicate with open ports on a remote host, to determine more about the service that is running on that port. This is more precise than a port scan, because it does not rely on the port alone to determine what service is running. For example, a port scan may be able to identify that TCP port 8000 is open on a host, but it will not know based on that information alone what service is running there. A service scanner would attempt to communicate with the port using different protocols. If the service running on port 8000 is able to correctly communicate using HTTP, then it will be identified as a web server.

Banner Grabbing

Banner grabbing is the process of connecting to a specific port and examining data returned from the remote host to identify the service/application bound to that port. Often in the connection process, software will provide an identification string which may include information such as the name of the application, or information about which specific version of the software is running.

Web Application Scanners

General application flaw scanners

Most web application scans start with the address of a website, web application, or web service. The scanner then crawls the site by following links and directory structures. After compiling a list of webpages, resources, services and/or other media offered, the scanner will perform tests, or audits against the results of the crawl. For example, if a webpage discovered in the crawl has form fields, the scanner might attempt SQL injection or cross-site scripting. If the crawled page contained errors, the scanner might look for sensitive information displayed in the error detail, and so on.

It should be noted that crawling and testing phases can be staggered and performed at the same time to reduce overall scanning time. This is the default behavior for many web application scanners.

Directory Listing/Brute Forcing

Suppose there are directories available on the website that the crawler won’t find by following links. Without prior knowledge of these directories, provided by the user, the scanner has at least two additional options.

The scanner/crawler can search for “common” directories. These are directories with names and variants of names that are commonly found, and are included in a list that has been compiled as the result of years of experience and scanning. Most web applications have a “built-in” list of this sort, while some penetration testers maintain their own custom lists. Sometimes directory names are unique enough that they can be used to identify a 3rd party web application with reasonably high

accuracy. An accurate directory list can often be the key to finding the “administrative” portion of a website - a portion most penetration testers should be highly interested in discovering.

Brute forcing directories is a similar approach, though instead of using a static list, a tool is used to enumerate every possibility a directory name could have. The downside of using this approach is that it has the potential to crash or inundate the web server with requests and thus cause a denial-of-service condition. Care should be taken to perform directory brute forcing while someone is keeping a close watch on the condition of the web server, especially in a production setting.

The reason you as the penetration tester would want to perform directory listing is to extend your attack field or to find directories that could contain sensitive information (which depending on the goal of the penetration test, may lead to a major finding within it).

Web Server Version/Vulnerability Identification

Many web application scanners will attempt to compare the version of the web server with known vulnerable versions in security advisories. This approach can sometimes lead to false positives; as there are some cases where open-source web servers are forked or copied and given new names, banners, and assigned different version numbers. Additional steps should be taken to verify that the web server is, in fact, running what the banner, or web scanner reports.

Methods

Several web server methods are considered insecure, and can allow attackers to gain varying levels of access to web server content. The fact that these methods are part of the web server software, and not web site content differentiates it from other vulnerabilities discussed thus far. Some insecure methods include:

OPTIONS

While the HTTP OPTIONS method is not insecure by itself, it can allow an attacker to easily enumerate the kinds of HTTP methods accepted by the target server. Note, the OPTIONS method is not always accurate and each of the methods below should be validated individually.

PUT/DELETE

Using the PUT method, an attacker can upload malicious content such as HTML pages that could be used to transfer information, alter web content or install malicious software on the web server. Using the DELETE method an attacker could remove content or deface a site causing a disruption of service.

Additionally, modern REST applications use PUT in a different manner:

Create->POST Read->GET Update->PUT Delete->DELETE

WebDAV

WebDAV is a component of the Microsoft Internet Information Server (IIS). WebDAV stands for “Web-based Distributed Authoring and Versioning” and is used for editing and file management. WebDAV extensions are used by administrators to manage and edit Web content remotely on IIS Web servers and can include PROPFIND, COPY, MOVE, PROPPATCH, MKCOL, LOCK, and UNLOCK .WebDAV interacts with core operating system components, which can expose a system to several possible vulnerabilities. Some of these potential risks include:

Buffer overflow conditions due to improper handling of user requests Denial-of-service conditions from malformed requests Domain based scripting attacks Privilege escalation Execution of arbitrary code

TRACE/TRACK

Modern web servers support the TRACE HTTP method, which contains a flaw that can lead to unauthorized information disclosure. The TRACE method is used to debug web server connections and can allow the client to see what is being received at the other end of the request chain. Enabled by default in all major web servers, a remote attacker may abuse the HTTP TRACE functionality to disclose sensitive information resulting in a loss of confidentiality.

Network Vulnerability Scanners/Specific Protocols

VPN

Conventional vulnerability assessment tools are not capable of performing the correct protocol negotiations with VPN devices that service Internet Key Exchange (IKE). In situations where IKE is in use, it will be necessary to use additional toolkits that can perform functions such as accurate fingerprinting, back off patterns and identify authentication mechanisms that are in use. By identifying these attributes of a VPN device, weaknesses can be identified in running code versions as well as authentication types such as static preshared keys.

Voice Network Scanners

War Dialing

Many organizations still utilize out of band access over telephone lines. Using vulnerability assessment tools that are designed to conduct war-dialing can determine weaknesses in authentication and network architecture.

VoIP

Voice over IP technologies are now abundant within most organizations. Many tools have been developed to conduct vulnerability analysis of VoIP infrastructures. Using these tools, one can identify if VoIP networks are properly segmented and potentials for leveraging these networks to access core infrastructure systems or record phone conversations on a target network may exist.

Manual Direct Connections

As with any automated process or technology, the margin for error always exists. Instabilities in systems, network devices and network connectivity may introduce inaccurate results during testing. It is always recommended to execute manual direct connections to each protocol or service available on a target system to validate the results of automated testing as well as identifying all potential attack vectors and previously unidentified weaknesses.

Obfuscated

Multiple Exit Nodes

Security monitoring and defense systems operate under the pretense of identifying malicious activity from a specific IP address. In situations where Intrusion Detection systems are deployed and monitoring activity, sourcing assessment and attack activities from multiple IP addresses provide more accurate results and lessen the opportunity for a monitoring device on a target network to

identify and respond. Technologies such as TOR proxies can provide a means to conduct assessment activities without sourcing from a single IP address.

IDS Evasion

When conducting assessment activities against a target environment where IDS technologies are deployed, it may be necessary to perform evasion. Using methods such as string manipulation, polymorphism, session splicing, and fragmentation can provide more accurate results while bypassing signature matching patterns implemented in IDS devices.

Passive

Metadata Analysis

Metadata analysis involves looking at data that describes a file, as opposed to the file data itself. A Microsoft Office document for example, might list the document author, company, when the document was last saved, when the document was created, and so on. Many documents even allow for the entry of custom metadata. This could potentially contain internal addresses and paths to servers, internal IP addresses, and other information a penetration tester could use to gain additional access or information.

Though metadata is quite common on documents located on a company's internal network, companies should take care to purge metadata before making documents available to the public, or on the public Internet. For this reason, any metadata an attacker could gain access to passively (without directly attacking the target) should be considered a security issue.

Traffic Monitoring

Traffic monitoring is the concept of connecting to an internal network and capturing data for offline analysis. Route poisoning is excluded from this phase as these create "noise" on the network and can easily be detected. It is often surprising how much sensitive data can be gleaned from a "switched" network. This "leaking of data" onto a switched network can be categorized as follows:

ARP/MAC cache overflow, causing switched packets to be broadcast - this is common on Cisco switches that have improper ARP/MAC cache timing configurations.

Etherleak - some older network drivers and some embedded drivers will use data from system memory to pad ARP packets. If enough ARP packets can be collected, sensitive information from internal memory can be captured

Misconfigured clusters or load balancers

Hubs plugged into the network Note that some of these categories only result in data leakage to a single subnet, while others can result in leakage to much larger network segments.

Validation

Correlation between Tools

When working with multiple tools the need for correlation of findings can become complicated. Correlation can be broken down into two distinct styles, specific and categorical correlation of items, both are useful based on the type of information, metrics and statistics you are trying to gather on a given target.

Specific correlation relates to a specific definable issue such as vulnerability ID, CVE, OSVDB, vendor indexing numbers, known issue with a software product, etc. and can be grouped with micro factors such as hostname, IP, FQDN, MAC Address etc. An example of this would be grouping the findings for host x by CVE number as they would index the same issue in multiple tools.

Categorical correlation relates to a categorical structure for issues such as in compliance frameworks (i.e. NIST SP 800-53, DoD 5300 Series, PCI, HIPPA, OWASP List, etc.) that allow you to group items by macro factors such as vulnerability types, configuration issues, etc. An example of this would be grouping all the findings for hosts with default passwords into a group for password complexity within NIST 800-53 (IA-5).

In most cases penetration testers are going to focus on the micro issues of specific vulnerabilities found in redundancy between multiple tools on the same host. This redundancy can skew the statistical results in the test output leading to a false increased risk profile.

The inverse of this is with an over reduction or simplification in macro correlation (i.e. top 10/20 lists) as the results can skew the output resulting in a false reduced risk profile.

Manual Testing/Protocol Specific

VPN

Fingerprinting

Fingerprinting is useful to determine the type of VPN device and correct version of code released installed. By accurately fingerprinting the device, proper research and analysis can then be conducted against the target system.

Authentication

VPN devices can operate with various forms of authentication. Using VPN toolkits that are not part of conventional vulnerability assessment tools allow for proper identification of the authentication mechanisms and determine weaknesses that may exist such as pre-shared keys or default group IDs.

Citrix

Enumeration

Many default installations and poorly configured Citrix appliances provide a means to enumerate published applications and determine valid usernames that are configured to authenticate to the device. This information becomes crucial during brute force attacks and attempts to break out of predefined profiles for authorized users.

DNS

Domain Name Systems can offer an abundance of information to an attacker when they are not properly hardened. Version information allow for proper identification and accurate research analysis. Weaknesses such as zone transfers provide an exhaustive list of additional targets for

attack as well as information leakage of potentially sensitive data pertaining to the target organization.

Web

Web services provide a large landscape for an attacker. Unlike most other protocols and services, web services are often found running on multiple ports of a single system. Administrators may focus their hardening on the common ports for web services or published directories and neglect to properly harden additional attributes. Web services should always be reviewed in a manual fashion as automated assessment tools are not capable of identifying most weaknesses in their services.

Mail

Mail servers can provide an abundance of information about a target organization. Using inherent functions in the target device, confirmation of valid accounts can be conducted as well as developing a list of potential usernames for additional attacks on other systems. Vulnerabilities such as mail relaying can be leveraged for additional attacks on the organization such as phishing. Often, mail servers will provide a web interface for remote access that can be targeted in brute force campaigns.

Attack Avenues

Creation of attack trees

During a security assessment, it is crucial to the accuracy of the final report to develop an attack tree as testing progresses throughout the engagement. As new systems, services and potential vulnerabilities are identified; an attack tree should be developed and regularly updated. This is especially important during the exploitation phases of the engagement as one point of entry that materializes could be repeated across other vectors mapped out during the development of the attack tree.

Isolated Lab Testing

The accuracy of vulnerability analysis and exploitation is substantially greater when replicated environments are setup in an isolated lab. Often times, systems may be hardened with specific control sets or additional protection mechanisms. By designing a lab that mimics that of the target organization, the consultant can ensure that the vulnerabilities identified and exploits attempted against the desired targets are reliable and lessen the opportunity for inaccurate results or system inoperability.

Visual Confirmation

Manual Connection with Review

While proper correlation can help reduce false findings and increase overall accuracy, there is no substitute for visually inspecting a target system. Assessment tools are designed to review the results of a protocol/service connection or the response and compare to known signatures of vulnerabilities. However, tools are not always accurate in identifying services on uncommon ports or custom logic that may be built into an application. By manually assessing a target system, its services available and the applications that provide functionality for those services, a tester can ensure that proper validation and vulnerability identification have been completed.

Research

Public Research

Once a vulnerability has been reported in a target system, it is necessary to determine the accuracy of the identification of the issue, and to research the potential exploitability of the vulnerability within the scope of the penetration test. In many cases, the vulnerability will be a reported software vulnerability in a commercial or open source software package, and in other cases the vulnerability can be a flaw in a business process, or a common administrative error like misconfiguration or default password usage.

Vulnerability Databases

Vulnerability databases can be used to verify an issue reported by an automated tool, or to manually review the vulnerability of a target application. Most tools will use the CVE identifier for a given vulnerability, which can be used to access the summary information and links to other sources in the CVE database. The CVE can also be used to search for the issue in vulnerability databases like OSVDB and Bugtraq, or in exploit databases and frameworks.

Vulnerability databases should be used to verify the accuracy of a reported issue. For example, an Apache web server flaw can exist on Windows, but not on Linux, which may not be taken into account by an automated scanner.

Vendor Advisories

Vendor-issued security advisories and change logs can provide pointers to vulnerability information that may not be reported by any automated tools. Many major software vendors report limited details on internally discovered issues and issues where an independent researcher coordinates the disclosure of a vulnerability. If the researcher chooses to remain silent on the details of the vulnerability, the vendor advisory is frequently the only data available. In these cases, other researchers may discover more details independently, and add the details to vulnerability databases. Searching for the CVE used in a vendor advisory may turn up more detail on a potentially exploitable issue.

Change logs can provide guidance for additional research, especially in open source products, where a diff between versions can reveal a vulnerability which was fixed but not widely known, and perhaps not prioritized for upgrade or installation as a result.

Exploit Databases and Framework Modules

Many exploit databases are actively maintained and publicly accessible on the Internet. Security researchers and exploit writers do not always submit their exploit code to multiple sites, so it is advisable to become familiar with several sites, and check each one for exploit code to use against potentially vulnerable applications. While some vulnerability databases track exploit availability, their coverage is usually incomplete and should not be considered exhaustive.

Commercial and open source exploit frameworks can also prove useful in researching vulnerabilities. In most cases, available exploit modules are listed on their public web sites, and can be a valuable indication of the exploitability of an issue.

Common/default Passwords

Frequently, administrators and technicians choose weak passwords, never change the default or do not set any password at all. Manuals for most software and hardware can be easily found online,

and will provide the default credentials. Internet forums and official vendor mailing lists can provide information on undocumented accounts, commonly-used passwords and frequently misconfigured accounts. Finally, many web sites document default/backdoor passwords and should be checked for every identified system.

Hardening Guides/Common Misconfigurations

One of the primary goals of penetration testing is to simulate the tactics and behavior of an actual attacker. While automated scanning can reduce the time window of a test, no scanner can behave like a human being. Hardening guides can be an invaluable reference for a penetration tester. They not only highlight the weakest parts of a system, but you can gain a sense of the diligence of an administrator by validating how many recommendations have been implemented. During every penetration test, time should be taken to review every major system and its recommended hardening settings, in order to discover vulnerabilities left in place by the administrator.

User forums and mailing lists can provide valuable information about systems and the various issues administrators have in configuring and securing them. A tester should research target systems as if he were installing one himself, and discover where the pain points and probable configuration errors will lie.

Private Research

Setting up a replica environment

Virtualization technologies allow a security researcher to run a wide variety of operating systems and applications, without requiring dedicated hardware. When a target operating system or application has been identified, a virtual machine (VM) environment can be quickly created to mimic the target. The tester can use this VM to explore to configuration parameters and behaviors of the application, without directly connecting to the target.

Testing Configurations

A testing VM lab should contain base images for all common operating systems, including Windows XP, Vista, 7, Server 2003 and Server 2008, Debian, Ubuntu, Red Hat and Mac OS X, where possible. Maintaining separate images for each service pack level will streamline the process of recreating the target's environment. A complete VM library in combination with a VM environment that supports cloning will allow a tester to bring up a new target VM in minutes. Additionally, using a snapshot feature will allow to work more efficiently and to reproduce bugs.

Fuzzing

Fuzzing, or fault injection, is a brute-force technique for finding application flaws by programmatically submitting valid, random or unexpected input to the application. The basic process involves attaching a debugger to the target application, and then running the fuzzing routine against specific areas of input and then analyzing the program state following any crashes. Many fuzzing applications are available, although some testers write their own fuzzers for specific targets.

Identifying potential avenues/vectors

Log in or connect to a target network application to identify commands and other areas of input. If the target is a desktop application that reads files and/or web pages, analyze the accepted file formats for avenues of data input. Some simple tests involve submitting invalid characters, or very

long strings of characters to cause a crash. Attach a debugger to analyze the program state in the event of a successful crash.

Disassembly and code analysis

Some programming languages allow for decompilation, and some specific applications are compiled with symbols for debugging. A tester can take advantage of these features to analyze program flow and identify potential vulnerabilities. Source code for open source applications should be analyzed for flaws. Web applications written in PHP share many of the same vulnerabilities, and their source code should be examined as part of any test.

Exploitation

Purpose

The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions. If the prior phase, vulnerability analysis was performed properly, this phase should be well planned and a precision strike.. The main focus is to identify the main entry point into the organization and to identify high value target assets.

If the vulnerability analysis phase was properly completed, a high value target list should have been complied. Ultimately the attack vector should take into consideration the success probability and highest impact on the organization.

Countermeasures

Countermeasures are defined as preventative technology or controls that hinder the ability to successfully complete an exploit avenue. This technology could be a Host Based Intrusion Prevention System, Security Guard, Web Application Firewall, or other preventative methods. When performing an exploit, several factors should be taken into consideration. In the event of a preventative technology, a circumvention technique should be considered. In circumstances when this is not possible, alternative exploit methods should be considered.

Overall, the purpose is to remain stealth when attacking the organization, if alarms are tripped the level of the assessment could be diminished. If at all possible, the countermeasures should be enumerated prior to triggering the exploit. This could be done through doing dry runs of the attack or enumerating the technology.

Anti-Virus

Anti-virus is a technology aimed at preventing malicious software from being deployed on the system. As a penetration tester we should be able to identify these types of anti-virus technologies and be able to protect against them. Anti-virus is a small subset of all of the different preventative measures that can be in place, for example host-based intrusion prevention systems, web application firewalls, and other preventative technologies.

Encoding

Encoding is the method of obfuscating data in a way that makes the deployed piece of code not appear the same. With encoding, the obfuscation occurs usually by scrambling the information and re-arranging in order to hide the fact of what the application is actually doing.

Packing

Packing is similar to encoding in a sense in that it attempts to re-arrange data to compress the application or "pack" it. The hopes of this is that the executable or piece of code being delivered is obfuscated in a manner that it won't be picked up by anti-virus technologies.

Encrypting

Encrypting, like Encoding and Packing is another method of manipulating the intended runnable code such that it is not recognizable or available for inspection. Only after decrypting in in-memory (with methods similar to packing) the actual code is exposed for the first time - hopefully after security mechanisms have allowed it through and it is executed immediately after it is decrypted.

Whitelist Bypass

Whitelisting technologies leveraged a trusted model for applications that have been seen on a given system at a time. The technology takes a baseline of the system and identifies what is normal to be run on the system versus what is something foreign. The penetration tester should be able to circumvent whitelist technologies. One of the most common methods is through direct memory access. Whitelisting does not have the capbility of monitoring memory real time and if a memory resident program is running and not touching disk, it can run without being detect by the given technology.

Process Injection

Process injection is simply the method to inject into an already running process. By injecting into a process, the information of the application can be hidden within a process that would normally be trusted in nature. It's very difficult for preventative measure technology to inspect running processes and can almost always hide in a different process that the application would think is a trusted one.

Purely Memory Resident

Memory resident attacks are generally the most preferred as most technologies do not inspect memory. As an attacker, finding a way to live in memory purely would be most desirable. When writing to disk, most applications will conduct scans, baselines, and other identifications of potentially maliicous software. The ability to be detected when writing to disk becomes significantly greater.

Human

When performing exploitation, it is not always the best route to go through a direct exploit or through an application flaw. Sometimes the human element may be a better way to attack an organization. It's important to understand the right attack avenue and make sure that the method we are leveraging is the best route to take.

Data Execution Prevention (DEP)

When performing exploitation, many preventative measures canc ome into play. Data Execution Prevention is a defensive measure implemented into most operating systems and prevents execute permission when an overwrite in memory has occurred. The thought process behind DEP is to stop an attacker in rewriting memory and then executing that code. There are mulitple methods to bypass data execution prevention and discussed later in the the exploitation phase of PTES.

Address Space Layout Randomization

During a buffer overflow vulnerability (or that of anything where we control memory), memory addresses are hardcoded in order redirect execution flow to our shellcode. In the event of ASLR, certain bytes are randomized in order to prevent an attacker from predicting where he/she can always go to in order to execute shellcode.

Web Application Firewall (WAF)

Web application firewalls are a technology that sits inline with an application in order to protect against web-based application attacks. Web application firewalls attempt to identify potentially dangerous or malforms attacked towards a given web applciation and prevent them. There are a number of bypass techniques for web application firewalls and should be tested during the penetration test.

Evasion

Evasion is the technique used in order to escape detection during a penetration test. This could be circumventing a camera system as to not be seen by a guard, obfuscating your payloads to evade Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) or encoding requests/responses to circumvent web application firewalls. Overall, the need to identify a low risk scenario for evading a technology or person should be formulated prior to the exploit.

Precision Strike

The main focus of a penetration test is to simulate an attacker in order to represent a simulated attack against the organization. The value brought through a penetration test is generally not through smash and grab techniques where the attacks are noisy in nature and in an attempt to try every exploit. This approach may be particularly useful at the end of a penetration test to gauge the level of incident response from the organization, but in most cases the exploitation phase is a accumulation of specific research on the target.

Customized Exploitation Avenue

Every attack will typically not be the same in how the exploitation avenue occurs. In order to be successful in this phase, the attack should be tailored and customized based on the scenario. For example, if a wireless penetration test is occurred, and a specific technology is in use, these need to be identified and attacked based on what technologies are in place. Having a clear understanding of each scenario and the applicability of an exploit is one of the most important aspects of this phase of the penetration test.

Tailored Exploits

In a number of occasions the exploits that are public on the Internet may need some work in order to successfully complete. In most cases, if an exploit is designed for Windows XP SP2, specific modifications to the exploit will be required in order for the attack to be successful via Windows XP SP3. The penetration tester should have the knowledge in place to be able to customize an exploit and the ability to change on the fly in order to successfully complete the attack.

Exploit Customization

In the event of an attack, it is often required to simulate the victims infrastructure in order to ensure that the exploitation phase will be successful. The techniques leveraged in the information gathering phase can always help assist in that however, having a working infrastructure and systems in place will make the expliotation phase much easier. In the event of a tailored exploit, the penetration tester should be able to customize already public exploits in order to successfully attack a system. A common theme for exploits is to target specific versions of operating systems or applications. The reason for this is due to memory addresses changing based on service packs, and/or new versions of the operating system. The tester should be able to customize these exploits to successfully deploy to different operating systems and successfully compromise the system.

Zero-Day Angle

In most cases, the zero-day angle is often a last resort for most penetration testers. This type of attack often represents a highly advanced organization that can handle a focused attack against the organization through normal attack methods. In certain scenarios research may be conducted in order to reverse engineer, fuzz, or perform advanced discovery of vulnerabilities that have not been discovered. In the event this type of attack is applicable, ensure that the environment to the best of the attackers knowledge is reproduced to include countermeasure technology.

In order for zero-day exploits to be successful (or any exploit for that matter), having the same operating system, patches, and countermeasures is highly important on success. Sometimes this information may not be available based on the level of access or enumeration that has occurred.

Fuzzing

Fuzzing is the ability to recreate a protocol or application and attempt to send data at the application in hopes of identification of a vulnerability. Often times the hopes of a fuzzer is to identify a crash in an application and craft a specific exploit out of it. In the case of fuzzing, the attacker is attempting to create a specific vulnerability out of something that hasn't been discovered before. As part of a penetration test, if no avenues are identified during the engagement, or the engagement calls for zero-day research; fuzzing techniques should be leveraged in order to identify potentially vulnerable exposures.

Source Code Analysis

Other avenues that a penetration tester has available is if the source code is available or open-source. If the tester has the ability to look at the source code and identify flaws within the application, zero day exposures can also be identified through these methods.

Types of Exploits

There are several types of exploits that can be identified during a penetration test that could be classified as a zero-day. Some are listed in this section.

Buffer Overflows

Buffer overflows occur due to improper coding techniques. Specifically this usually occurs when a program writes data to a buffer and then overruns the buffer's boundary and begins to overwrite portions of memory. In buffer overflow exploits the attackers goal is to control a crash and gain code execution on the given system. In a buffer overflow exploit, one of the more common techniques is to overwrite a given register and "jump" to the shellcode.

SEH Overwrites

SEH overwrites occur when the structured exception handler begins to gracefully close an application. The attacker can manipulate how SEH works, overwrite the base address of the SEH handler and gain control of execution flow through the SEH. This is a common attack leveraged with buffer overflow vulnerability and applications that have been complied with SEH.

Return Oriented Programming

Return Oriented Programming (ROP) is a technique used during a portion where the user has control of execution flow however data execution prevention (DEP) or other precluding defense mechanisms may be in place. In the situation where DEP is enabled, the attacker does not have direct access to execute specific assembly instructions, therefor the attacker buildsa ROP gadget in order to prep certain Windows API calls or techniques to disable DEP or circumvent DEP. A common

method is leveraging the WriteProcessMemory call to copy data from the stack into a writable memory space that can then be executed.

Traffic Analysis

Traffic analysis is the technique of identifying what type of information is being sent and the ability to understand and manipulate that traffic. A penetration tester should be able to understand how a protocol works and how it can be manipulated in order to leverage an attack.

Physical Access

Physical access during a penetration test can be a viable attack method for attempting to circumvent physical security controls and gain unauthorized access. During a penetration test, the assessor should be able to identify potentially flawed physical security controls and attempt to gain access to the facility if within scope.

Human Angle

During a physical penetration test, some of the most obvious ways would be to social-engineer your way into the facility and gain access. This requires significant knowledge of how the organization performs business, and everything you learned from the intelligence gathering phase.

PC Access

If physical access is granted to a PC, the penetration tester should be able to attack the PC and gain access through multiple methods that would allow access to the system.

Proximity Access (WiFi)

Wireless communications are an avenue for attacks to gain access through RF type communications. The penetration tester should view the FCC radio frequency list to see if the target has registered spectrum frequencies in use.

WiFi Attacks

Regardless of protocol, there are a number of attacks available for WEP, WPA, WPA2, EAP-FAST, EAP-LEAP, and other avenues. The attacker should be familiar with the various encryption protocols and standards and be able to effectively test the implementation around the controls put in place.

Attacking the User

Leveraging rogue access points in order to attack the victim is often a beneficial and a viable attack method. Leveraging a rogue access point to entice victims in order to leverage exploits or steal sensitive information should be performed during a wireless assessment. There are several common techniques in use of this, but most commonly the attacker would setup a wireless access point with the same name or an enticing name in order for the victim to connect.

Example Avenues of Attack

In any scenario, the attacks should consist based on the scenario that is within scope of the engagement. Below is a list of several attack avenues to consider based on scenario but is by no means a comprehensive list.

Web Application Attacks Social-Engineering Physical Attack Avenues Memory Based Exploits (i.e. buffer/heap overflows, memory corruptions, use-after-free). Man in the Middle VLAN Hopping USB/Flash Drive deployment Reverse Engineering Zero-Day Angle Attacking the user Encryption Cracking Graphics Processing Unit (GPU) Cracking Traffic Analysis Firewire Routing protocols Phishing with Pretexting Employee Impersonation

Again, these examples are only basic avenues for attack based on the scenario you are performing for the organization. The value from a penetration test comes from creativity and the ability to identify exposures and exploit them in a precise manner.

Overall Objective

In the pre-engagement interaction phase with the customer, a clear definition of the overall objectives of the penetration test should have been communicated. In the case of the exploitation phase, the biggest challenge is identifying the least path of resistance into the organization without detection and having the most impact on the organizations ability to generate revenue.

By performing the prior phases properly, a clear understanding of how the organization functions and makes money should be relatively understood. From the exploitation phase and into the post-exploitation phase, the attack vectors should rely solely on the mission of circumventing security controls in order to represent how the organization can suffer substantial losses through a targeted attack against the organization.

Post Exploitation

Purpose

The purpose of the Post-Exploitation phase is to determine the value of the machine compromised and to maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machines usefulness in further compromising the network. The methods described in this phase are meant to help the tester identify and document sensitive data, identify configuration settings, communication channels, and relationships with other network devices that can be used to gain further access to the network, and setup one or more methods of accessing the machine at a later time. In cases where these methods differ from the agreed upon Rules of Engagement, the Rules of Engagement must be followed.

Rules of Engagement

The following Rules of Engagement are specific to the Post-Exploitation phase of a penetration test and are intended to ensure that the client's systems are not subjected to unnecessary risk by the (direct or indirect) actions of the testers and to ensure a mutually agreed procedure to follow during the post-exploitation phase of the project.

Protect the Client

The following rules are to be used as a guideline of rules to establish with a client to ensure that the day to day operations and data of the client are not exposed to risk:

- Unless previously agreed upon, there will be no modification of services which the client deems "critical" to their infrastructure. The purpose of modifying such services would be to demonstrate to the client how an attacker may:
- Escalate privileges
- Gain access to specific data
- Cause denial of service
- All modifications, including configuration changes, executed against a system must be documented. After finishing the intended purpose of the modification, all settings should be returned to their original positions if possible. The list of changes should be given to the client after the engagement

to allow them to ensure all changes were properly undone. Changes that could not be returned to their original positions should be clearly differentiated from changes that were successfully reversed.

- A detailed list of actions taken against compromised systems must be kept. The list should include the action taken and the time period in which it occurred. Upon completion, this list should be included as an appendix to the final report.
- Any and all private and/or personal user data (including passwords and system history) uncovered during the course of the penetration test may be used as leverage to gain further permissions or to execute other actions related to the test only if the following conditions are met:
- The client's Acceptable Use Policy states all systems are owned by the client and all data stored on those systems are the property of the client.
- The Acceptable Use Policy states connection to the client's network is considered consent for the connected machine to be searched and analyzed (including all present data and configurations).
- The client has confirmation that all employees have read and understand the Acceptable Use Policy.
- Passwords (including those in encrypted form) will not be included in the final report, or must be masked enough to ensure recipients of the report cannot recreate or guess the password. This is done to safeguard the confidentiality of the users the passwords belong to, as well as to maintain the integrity of the systems they protect.
- Any method or device used to maintain access to compromised systems and that could affect the proper operation of the system or whose removal may cause downtime may not be implemented without the prior written consent of the client.
- Any method or device which is used to maintain access to compromised systems must employ some form of user authentication such as digital certificates or login prompts. A reverse connection to a known controlled system is also acceptable.
- All data gathered by the testers must be encrypted on the systems used by the testers.
- Any information included in the report that could contain sensitive data (screenshots, tables, figures) must be sanitized or masked using techniques that render the data permanently unrecoverable by recipients of the report.
- All data gathered will be destroyed once the client has accepted the final report. Method used and proof of destruction will be provided to the client.
- If data gathered is regulated by any law, the systems used and their locations will be provided by the client to ensure that the data collected and processed does not violate any applicable laws. If the systems will be those of the penetration testing team the data may not be downloaded and stored on to their systems and only proof of access will be shown (File Permissions, Record Count, file names..etc).
- Third party services for password cracking will not be used, nor will there be sharing of any other type of data with third parties without the clients prior consent.
- If evidence of a prior compromise if found in the assessed environment all logs with actions and times recorded during the assessment by the penetration team will be saved, hashed and provided to the client. The client can then determine how best to respond to and handle the incident response.
- No logs should be removed, cleared or modified unless specifically authorized to do so by the client in the engagement contract/statement of work. If authorized, the logs must be backed up prior to any changes.

Protecting Yourself

Due to the nature of a penetration test, you must ensure that you cover all your bases when dealing with the client and the tasks you will be performing. Discuss the following with the client to ensure a clear understanding of the roles and responsibilities of both client and provider prior to beginning any work.

- Ensure that the contract and/or statement of work signed by both the client and provider that the actions taken on the systems being tested are on behalf and in representation of the client.
- Obtain a copy of the security policies that govern user use of company systems and infrastructure (often referred to as "Acceptable Use" policies) prior to starting the engagement. Verify that policy covers:
- Personal use of equipment and storage of personal employee data on the client systems and ownership and rights on that data.
- Ownership of data stored on company equipment.
- Confirm regulations and laws that govern the data that is managed and used by the client on their systems and the restrictions imposed on such data.
- Use full drive encryption for those systems and removable media that will receive and store client data.
- Discuss and establish with the client the procedures to follow in the case that a compromise from a third party is found.
- Check for laws concerning the capture and/or storage of audio and video since the use of this methods in post-exploitation may be considered a violation of local or country wiretap laws.

Infrastructure Analysis

Network Configuration

The network configuration of a compromised machine can be used to identify additional subnets, network routers, critical servers, name servers and relationships between machine. This information can be used to identify additional targets to further penetrate the client's network.

Interfaces

Identify all of the network interfaces on the machine along with their IP addresses, subnet masks, and gateways. By identifying the interfaces and settings, networks and services can be prioritized for targeting.

Routing

Knowledge of other subnets, filtering or addressing schemes could be leveraged to escape a segmented network, leading to additional hosts and/or networks to probe and enumerate. This data could come from a variety of sources on a particluar host or network including:

- Interfaces
- Routing tables, including static and dynamic routes
- ARP Tables, NetBios or other network protocols used for service and host discovery.
- For multi-homed hosts, determine if they are acting as a router.

DNS Servers

Identify all DNS servers in use, by assessing host settings. DNS servers and information could then be used to develop and execute a plan for discovering additional hosts and services on the target network. In the case that a DNS Server is compromised, the DNS database will provide valueable information about hosts and services that can be used to prioritize targets for the remainder of the

assessment. The modification and addition of new records could be used to intercept the data of services depending on DNS.

Cached DNS Entries

Identify high value DNS entries in the cache, which may include login pages for Intranet sites, management interfaces, or external sites. Cached interfaces provide information of the most recent and most used host used by the compromised host providing a view of the relations and interactions of the hosts providing information that could be used to prioritization of targets for further penetration of the target network and infrastructure. Modification of cached entries if permitted can be used to capture authentication credential, authentication tokens or to gain further information on services used by the compromised hosts leading to further penetration of the target network.

Proxy Servers

Identify network and application level proxy servers. Proxy servers make good targets when in enterprise-wide use by the client. In the case of application proxies, it may be possible to identify, modify and/or monitor the flow of traffic, or the traffic itself. Proxy attacks are often an effective means to show impact and risk to the customer.

ARP Entries

Enumerate cached and static ARP table entries, which can reveal other hosts that interact with the compromised machine. Static ARP entries may represent critical machines. If the scope of the assessment allows for intercepting and modifying ARP entries, it is simple to show the possibility of disrupting, monitoring, or compromising a service in a manner that is usually not detected or protected against.

Network Services

Listening Services

Identify all the network services offered by the target machine. This may lead to the discovery of services not identified by initial scanning as well as the discovery of other machines and networks. The identification of services not shown in scanning can also provide information on possible filtering and control systems implemented in the network and/or host. In addition, the tester may be able to leverage these services to compromise other machines. Most operating system include a method of identifying TCP and UDP connections made to and from the machine. By checking both connections to and from a compromised machine it is possible to find relationships that were previously unknown. As well as the host the service should also be considered, this may reveal services listening on non-standard ports and indicate trust relationships such as keyless authentication for SSH.

VPN Connections

All VPN connections into and out of the target machine or network should be identified. Outbound connections can provide paths into new systems which may have not previously been identified. Both inbound and outbound can identify new systems and possible business relationships. VPN connections often bypass firewalls and intrusion detection/prevention systems due to their inability to decrypt or inspect encrypted traffic. This fact makes VPNs ideal to launch attacks through. Any new targets should be verified as in scope before launching attacks against them. The presence of VPN client or server connections on the target host may also provide access to credentials previously not known that could be used to target other hosts and services.

Directory Services

A targeted host running directory services may provide an opportunity to enumerate user accounts, hosts and/or services that can be used in additional attacks or provide additional targets that may not have been previously discovered in the vulnerability analysis phase. Additionally, the details of users found in directory services could be used for Social Engineering and phishing campaign attacks, thus providing a possible higher success rate.

Neighbors

In todays network many services and operating systems use a number of protocols for neighbor discovery in an effort make the access of services, troubleshooting and configuration more convenient. Protocols vary depending on the type of target host. Networking equipment may use protocols like CDP (Cisco Discovery Protocol) and LLDP (Link Layer Discovery Protocol) to identify systems, configurations and other details to hosts directly connected to them or present in the same subnet. Similarly, desktop and server operating systems may use protocols like mDNS (Multicast Domain Name Service) and NetBios to find details of hosts and services in the same subnet.

Pillaging

Pillaging refers to obtaining information (i.e. files containing personal information, credit card information, passwords, etc.) from targeted hosts relevant to the goals defined in the pre-assessment phase. This information could be obtained for the purpose of satisfying goals or as part of the pivoting process to gain further access to the network. The location of this data will vary depending on the type of data, role of the host and other circumstances. Knowledge and basic familiarity with commonly used applications, server software and middleware is very important, as most applications store their data in many different formats and locations. Special tools may be necessary to obtain, extract or read the targeted data from some systems.

Installed Programs

Startup Items

Most systems will have applications that can run at system startup or at user logon that can provide information about the purpose of the system, software and services it interacts with. This information may reveal potential countermeasures that could be in place that may hinder further exploitation of a target network and it's systems (e.g. HIDS/HIPS, Application Whitelisting, FIM). Information that should be gathered includes:

- List of the applications and their associated versions installed on the system.
- List of operating system updates applied to the system.

Installed Services

Services on a particular host may serve the host itself, or other hosts in the target network. It is necessary to create a profile of each targeted host, noting the configuration of these services, their purpose, and how they may potentially be used to achieve assessment goals or further penetrate the network.

Security Services

Security services comprise the software designed to keep an attacker out of systems, and keep data safe. These include, but are not limited to network firewalls, host-based firewalls, IDS/IPS, HIDS/HIPS and anti-virus. Identifying any security services on a single targeted host gives an idea of what to expect when targeting other machines in the network. It also gives an idea of what alerts may have been triggered during the test, which can be discussed with the client during the project debrief, and

may result in updates to Security Policies, UAC, SELinux, IPSec, windows security templates, or other security rulesets/configurations.

File/Printer Shares

File and print servers often contain targeted data or provide an opportunity to further penetrate the target network and hosts. The information that should be targeted includes:

- Shares offered by File Servers - Any file shares offered by target systems should be examined. Even just the names and comments of shares can leak important information about the names of internal applications or projects (i.e. if only "Fred" and "Christine" have access to the "Accounting" folder, perhaps they are both accounting employees).
- Access Control Lists and permissions for shares. - From the client side, if it is possible to connect to the share, then it should be checked to see if the connection is read/only or read/write. Remember that if a share contains directories then different permissions may apply to different directories. From the server side both server configuration and file/directory permissions should be examined.
- File share file and content listings
- Identify files of interest from the file share listings. Look for interesting or targeted items such as:
- Source Code
- Backups
- Installation Files
- Confidential Data (financial data in spreadsheets, bank reports in TXT/PDF, password files, etc.)
- Place trojans or autorun files - Using clever naming, or by mimicking naming conventions already in use, users can be encouraged to execute these payloads, allowing the tester to further penetrate the network. If file server logs can be obtained, specific users may even be targeted.

Database Servers

Databases contain a wealth of information that may be targeted in an assessment.

- Databases - A list of database names can help the assessor to determine the purpose of the database and the types of data the database may contain. In an environment with many databases, this will help in prioritizing targets.
- Tables - Table names and metadata, such as comments, column names and types can also help the assessor choose targets and find targeted data.
- Table Content, row count for regulated content
- Columns - It is possible in many databases to search all column names of all tables with a single command. This can be leveraged to find targeted data (e.g. If credit card data is targeted on an Oracle database, try executing *select * from all_tab_columns where name = '%CCN%';*.
- Database and Table Permissions
- Database Users, Passwords, Groups and Roles

The information hosted on databases can be also be used to show risk, achieve assessment goals, determine configuration and function of services or to further penetrate a client network and hosts.

Directory Servers

The main goals of a directory service is to provide information to services and hosts for reference or/and authentication. The compromise of this service can allow the control of all hosts that depend on the service and well as provide information that could be used to further an attack. Information to look for in a directory service are:

- List of objects (Users, passwords, Machines..etc)

- Connections to the system
- Identification of protocols and security level

Name Servers

Name server provide resolution to host and services depending on the types of records it servers. Enumeration of records and controls can provide a list of targets and services to prioritize and attack to further penetrate a clients network and hosts. The ability to modify and add records can be use to show risk of denial of services as well as aid in the interception of traffic and information on a customer network.

Deployment Services

Identification of deployment services allows for the access and enumeration of:

- Unattended answer files
- Permission on files
- Updates included
- Applications and versions

This information can be used to further penetrate a client network and hosts. The ability to modify the repositories and configuration of the service allows for

- Backdoor installation
- Modification of services to make them vulnerable to attack

Certificate Authority

Identification of Certificate Authority services on a compromised client host will allow for the access to

- Root CA
- Code Signing Certificates
- Encryption and Signing Certificates

Control of the service will also allow for the

- Creation of new certificates for several tasks
- Revocation of certificates
- Modification of the Certificate Revocation List
- Insertion of Root CA Certificate

The control of the services shows risk and allows for the compromise of data and services on a client's network and hosts.

Source Code Management Server

Identification of source code management systems via by the service running on the compromised host or the client part of the service provides the opportunity for:

- Enumerate projects - The project names can give away sensitive information on company projects.
- Verify access to source code files
- Modify source code files - If it is allowed in scope then modifying source code proves that an attacker could make changes that would affect the system
- Enumerate developers - Developers details can be use for social engineering attacks as well as as inputs for attacking other areas of the system

- Enumerate configuration

Dynamic Host Configuration Server

Identification of dynamic host configuration service or use of the service by the compromised host allows for:

- Enumeration leases given
- Enumeration configuration
- Enumeration Options
- Modification of configuration
- Consumption of all leases

The control of the service can be used to show risk of denial of service and for use in man in the middle attacks of hosts and services on the compromised network.

Virtualization

Identification virtualization services or client software allow for:

- Enumerate Virtual Machines (name, configurations, OS)
- Enumerate passwords and digital certificates for administration systems.
- Enumerate virtualization software configuration
- Configuration of Hosts
- Show risk of denial of service with control of VM state
- Access to data hosted on VM's
- Interception of traffic of virtual hosts or services hosted on the compromised host

Messaging

Identification of services or client software for messaging provides the opportunity to

- Identify Directory Services
- Compromise of credentials
- Access to confidential information
- Identification of hosts on the network
- System and business relationships

All of this information and actions can be used to show risk and to further penetrate a client's network and hosts.

Monitoring and Management

Identification of services or client software for the purpose of monitoring and/or management may provide identification of additional servers and services on the target network, in addition the configuration parameters gained may provide access to other targets host and to determine what actions performed by the tester can be detected by the client. Some services to look for:

- SNMP (Simple Network Management Protocol)
- Syslog

Some Management Services and Software to look for to gain credentials, identify host and gain access to other services may be:

- SSH Server/Client
- Telnet Server/Client

- RDP (Remote Desktop Protocol) Client
- Terminal Server
- Virtual Environment Management Software

Backup Systems

Identification of services or client software for the purpose of backing up data provide a great opportunity to an attacker since these system require access to the data and systems they need to backup providing an attacker:

- Enumeration of hosts and systems
- Enumeration of services
- Credentials to host and/or services
- Access to backup data

The information gained from the service can be used to show risk to the confidentiality, integrity and access tot he system and their information. Access to the backups can also provide opportunity to introduce miss configuration, vulnerable software or backdoors in to the clients systems.

Networking Services (RADIUS,TACACS..etc)

Identification of services or use of networking services allows for the:

- Enumeration of users
- Enumeration of hosts and systems
- Compromise of credentials
- Show risk of denial of service if alternate methods are not present

Sensitive Data

Key-logging

By monitoring key strokes it is possible to detect sensitive information including passwords and PII - Don't know what the legality of this is if the user is say chatting on private IM while also using company software, anyone know? If the company says that all data on the network can be monitored then this should be ok. If the second bullet point in Protect Yourself is present and it states that use of equipment can be monitored and no personal use is permitted yes, if policy does not cover personal user or ownership of data, no. It should be extended to cover Network also.

Screen capture

Screen capture can be use to show evidence of compromise as well as access to information that can shown on the screen and access thru other means is not possible. Great care should be taken with the data collected thru screen capture so as to nor show private data of employees of customers of the client.

Network traffic capture

Network traffic capture can be used depending on the controls on the network and medium used for capture can be used to:

- Identify hosts on the network
- Intercept data
- Identify services
- Identify relations between hosts in the network
- Capture of credentials

Care should be taken to only capture traffic covered under the scope of the engagement and that the information captured does not fall under the control of local laws like the capture of Voice Over IP calls. Information retained and shown should be filtered so as to protect client's customer and/or employee personal and confidential data.

Previous Audit reports

User Information

In this section the main focus is on the information present on the target system related to user accounts either present on the system or that have connected remotely and have left some trace that the personnel performing the assessment can gather and analyze for further penetration or provide the desired goal of the assessment.

On System

General information that can be gather on a compromised system are:

- History files - History files store recent commands the user has executed. Reading through these can reveal system configuration information, important applications, data locations and other system *sensitive information.
- Encryption Keys (SSH, PGP/GPG)
- Interesting Documents (.doc/x, .xls/x , password.*) - Users often store passwords and other sensitive information in clear text documents. These can be located in two ways, either searching through file names for interesting words, such as password.txt, or searching through the documents themselves. Indexing services can help with this, for example the Linux locate database.
- User specific application configuration parameters
- Individual Application History (MRU Windows only, history files..etc)
- Enumerate removable media
- Enumerate network shares / domain permission (gpresult)

Web Browsers

Information that can be gathered from web browsers that can be use to identify other hosts and systems as well as provide information to further penetrate a client's network and hosts are:

- Browser History
- Bookmarks
- Download History
- Credentials
- Proxies
- Plugins/Extensions

Great care should be taken that only data in scope for the engagement is capture since the information from a web browser may contain client's employee confidential and private data. This data should be filtered from the data returned and report.

IM Clients

Information that can be gathered from IM Clients on a compromised system is:

- Enumerate Account Configuration (User, Password, Server, Proxy)
- Chat Logs

Great care should be taken that only data in scope for the engagement is capture since the information from a web browser may contain client's employee confidential and private data. This data should be filtered from the data returned and report.

System Configuration

Password Policy

By enumerating the systems password policy the ability to brute force and crack passwords becomes much more efficient, for example knowing that the minimum password length is 8 characters you can remove any word less than 8 characters from a dictionary.

Security Policies

Configured Wireless Networks and Keys

By finding the targets wireless information it becomes possible to launch physical attacks through the companies wifi when on site. It can also allow a fake AP to be set up to lure targets to connect when away from site.

High Value/Profile Targets

High value/profile targets can be identified and further expanded from the targets identified in the pre-engagement meetings thru the analysis of the data gathered from the compromised systems and the interactions of those systems and the services that run on them This view of the the operation and interactions of these high value/profile targets helps in the identification and measurement of of impact that can be gained to the business do to the data and processes and to the overall integrity of the client's infrastructure and services.

Data Exfiltration

Mapping of all possible exfiltration paths

from each of the areas where access has been achieved, a full exfiltration paths should be created. This includes secondary and tertiary means of getting to the outside world (through different accessible subnetc, etc). Once the mapping is provided, the actual exfiltration testing should be commenced.

Testing exfiltration paths

Per exfiltration paths mapping, data should be exfiltrated from the organization being tested. This should already be covered in the Pre-engagement scoping and adequate infrastructure should have been setup which adheres to the customer's acceptable engagement policy (i.e. data being exfiltrated is usually exfiltrated to a server in the full control of the tester, and will access and ownership right to the tested organization). The exfiltration itself should simulate real-world exfiltration strategies used by the threat actors that correspond to the Threat Modeling Standard relevant for the organization (i.e. if criminal mostly then "standard" exfiltration using a staging area inside the network where data is archived inside zip/7z encrypted files and then sent to FTP/HTTP servers on the Internet, if a more sophisticated threat actor then using means that simulate such strategies and tactics used for exfiltration).

Measuring control strengths

When performing exfiltration testing, the main goal of the test is to see whether the current controls for detecting and blocking sensitive information from leaving the organization actually work, as well as exercise the response teams if anything has been detected in terms of how they react to such alerts and how are the events being investigated and mitigated.

Persistence

- Installation of backdoor that requires authentication.
- Installation and/or modification of services to connect back to system. User and complex password should be used as a minimum; use of certificates or cryptographic keys is preferred where possible. (SSH, ncat, RDP). Reverse connections limited to a single IP may be used.
- Creation of alternate accounts with complex passwords.
- When possible backdoor must survive reboots.

Further Penetration Into Infrastructure

Pivoting is the action in which the tester will use his presence of on the compromised system to further enumerate and gain access to other systems on the client's infrastructure. This action can be executed from the compromised host it self using local resourced or tools uploaded to the compromised system.

From Compromised System

Actions that can be taken from a compromised system:

- Upload tools
- Use local system tools
- ARP Scan
- Ping Sweep
- DNS Enumeration of internal network
- Directory Services Enumeration
- Brute force attacks
- Enumeration and Management thru Management Protocols and compromised credentials (WinRM, WMI, SMB, SNMP..etc)
- Abuse of compromised credentials and keys (Webpages, Databases..etc)
- Execute Remote Exploits

The action that will be executed will depend on the information needed to show specific risk and/or further penetrating the client's network and hosts. Regular planning sessions are recommended to re-evaluate the information gather and decide the best approach to continue the post exploitation until the set goals are meet.

Thru Compromised System

Actions that can be taken thru a compromised system:

- Port Forwarding
- Proxy to internal network (SSH)
- VPN to internal network
- Execute Remote Exploit
- Abuse of compromised credentials and keys (Webpages, Databases..etc)

The action that will be executed will depend on the information needed to show specific risk and/or further penetrating the client's network and hosts. Regular planning sessions are recommended to re-evaluate the information gather and decide the best approach to continue the post exploitation until the set goals are meet.

Cleanup

The cleanup process covers the requirements for cleaning up systems once the penetration test has been completed. This will include all user accounts and binaries used during the test.

- Remove all executable, scripts and temporary file from a compromised system. If possible use secure delete method for removing the files and folders.
- Return to original values system settings and application configuration parameters if they where modified during the assessment.
- Remove all backdoors and/or rootkits installed.
- Remove any user accounts created for connecting back to compromise systems.

Reporting

Overview

This document is intended to define the base criteria for penetration testing reporting. While it is highly encouraged to use your own customized and branded format, the following should provide a high level understanding of the items required within a report as well as a structure for the report to provide value to the reader.

Report Structure

The report is broken down into two (2) major sections in order to communicate the objectives, methods, and results of the testing conducted to various audiences.

The Executive Summary

This section will communicate to the reader the specific goals of the Penetration Test and the high level findings of the testing exercise. The intended audience will be those who are in charge of the oversight and strategic vision of the security program as well as any members of the organization which may be impacted by the identified/confirmed threats. The executive summary should contain most if not all of the following sections:

Background:

The background section should explain to the reader the overall purpose of the test. Details on the terms identified within the Pre Engagement section relating to risk, countermeasures, and testing goals should be present to connect the reader to the overall test objectives and the relative results.

(Example: (CLIENT) tasked <Pentester> with performing an internal/external vulnerability assessment and penetration testing of specific systems located in (logical area or physical location). These systems have been identified as (risk ranking) and contain (data classification level) data which, if accessed inappropriately, could cause material harm to (Client). In an effort to test (CLIENT's) ability to defend against direct and indirect attack, <Pentester> executed a comprehensive network vulnerability scan, Vulnerability conformation(<-insert attack types agreed upon->) exploitation of weakened services, client side attacks, browser side attacks (etc) The purpose of this assessment was to verify the effectiveness of the security controls put in place by (CLIENT) to secure business-critical information. This report represents the findings from the assessment and the associated remediation recommendations to help CLIENT strengthen its security posture.

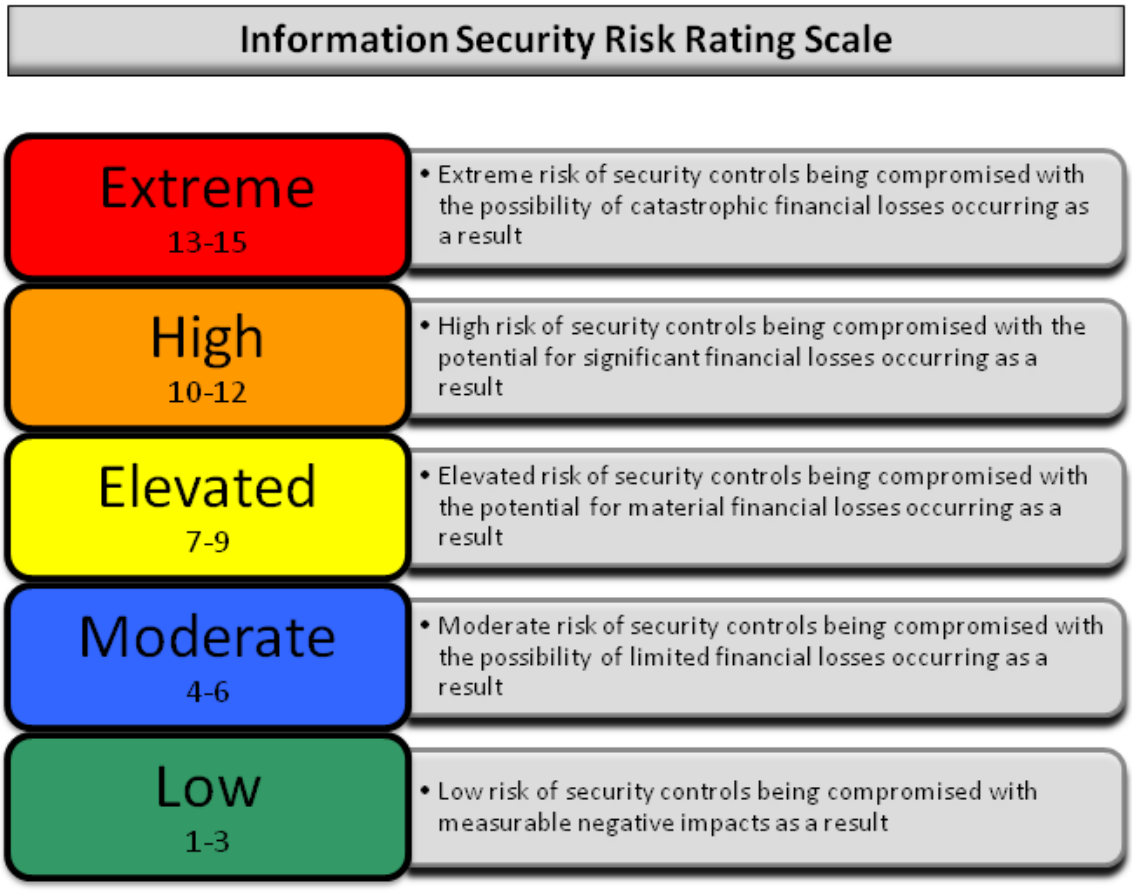
- If objectives were changed during the course of the testing then all changes must be listed in this section of the report. Additionally, the letter of amendment should be included in the appendix of the report and linked to from this section.

Overall Posture:

This area will be a narrative of the overall effectiveness of the test and the pentesters ability to achieve the goals set forth within the pre engagement sessions. A brief description of the Systemic (ex. Systemic issue= Lacking Effective Patch Management Process vs. Symptomatic= Found MS08-067 missing on xyz box) issues identified through the testing process as well as the ability to achieve access to the goal information and identify a potential impact to the business.

Risk Ranking/Profile:

The overall risk ranking/profile/score will be identified and explained in this area. In the pre engagement section the Pentester will identify the scoring mechanism and the individual mechanism for tracking/grading risk. Various methods from FAIR, DREAD, and other custom rankings will be consolidated into environmental scores and defined.

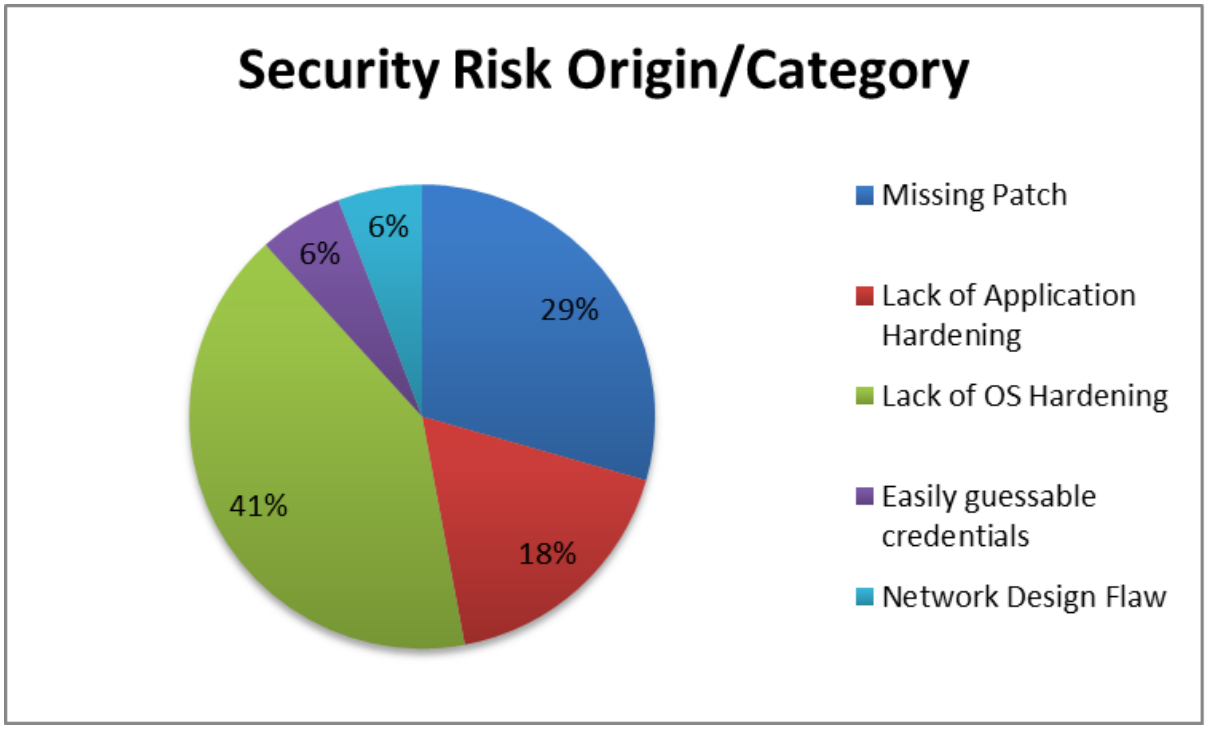


The “Overall Risk Score” for the (CLIENT) is currently a Seven (7). This rating implies an ELEVATED risk of security controls being compromised with the potential for material financial losses. The consultant determined this risk score based on one high risk and several medium risk vulnerabilities, along with the success of directed attack. The most severe vulnerability identified was the presence of default passwords in the corporate public facing website which allowed access to a number of sensitive documents and the ability to control content on the device. This vulnerability could lead to

theft of user accounts, leakage of sensitive information, or full system compromise. Several lesser severe vulnerabilities could lead to theft of valid account credentials and leakage of information.

General Findings:

The general findings will provide a synopsis of the issues found during the penetration test in a basic and statistical format. Graphic representations of the targets tested, testing results, processes, attack scenarios, success rates, and other trendable metrics as defined within the pre engagement meeting should be present. In addition, the cause of the issues should be presented in an easy to read format. (ex. A graph showing the root cause of issues exploited)



If defined within the Pre engagement exercise, this area should also include metrics which depict the effectiveness of the countermeasures within the environment. (ex.. we ran x attacks and IPS blocked y. Other countermeasures should also have similar metrics of design vs. effectiveness.)

Recommendation Summary:

The recommendation section of the report should provide the reader with a high level understanding of the tasks needed to resolve the risks identified and the general level of effort required to implement the resolution path suggested. This section will also identify the weighting mechanisms used to prioritize the order of the road map following.

Strategic Roadmap:

Roadmaps should include a prioritized plan for remediation of the insecure items found and should be weighed against the business objectives/ level of potential impact. This section should map directly to the goals identified as well as the threat matrix created in the PTES-Threat modeling section. By breaking up into predefined time/objective based goals, this section will create a path of action to follow in various increments. Example:

Completed at the time of this assessment

Tasks

Identify internal security point of contact

- Identify current resources to dedicate the task of resolving security concerns within the environment. The remediation process should be owned and supported by senior staff in order to effectively manage its completion.
- Secure appropriate funding for initial program review and 3rd party assessment

Identify Current Security State of security

- This task will be performed at an executive level. CLIENT will identify the proper ownership and executive support channel to champion this effort. In addition, CLIENT will need to take inventory of the "Security Management Chain of Command", Policy, Procedure, and Compliance tracking sophistication.

One (1) to Three (3) Months

Tasks

Create Remediation Strategy

- Leverage results found within the Penetration Test to create a full remediation strategy
- This assessment report will provide the basis for this action. It must now be formalized and approved by the CLIENT Security Team.

Create Information Security Council/Task Force

- To gain better traction in the remediation and security onboarding process, CLIENT should create a specific ISEC council to aid in remediation and adequately involve each individual team.
- The council should consist of Management of each individual business unit
- ....

Begin Security Project planning

- Assign Executive owners of security for CLIENT
- **...**

Prioritize Remediation Events

- Leverage results found within Penetration Test to gain understanding of the tasks needed to be performed in order to resolve the risks identified.
- Assign priority listing to remediation tasks that will provide the highest level of impact and largest reduction of identified risk.
- Start process with server patching to gain quick increases in environment security.

Patch Services

- **Specific things to be fixed/how...**
- **...**

Harden Servers

- ...
- ...

Three (3) to Twelve (12) Months

Tasks

Security Self Assessment

Adequate security of information and the systems that process it is a fundamental management responsibility. CLIENT officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. Self-assessments provide a method for CLIENT officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. A good guide for this is **NIST SP 800-53a**: found at http://csrc.nist.gov/publications/PubsDrafts.html. Another approach would be to run the **Microsoft Security Assessment Tool** : found at http://www.microsoft.com/technet/security/tools/msat/default.mspx

Twelve (12) Months+

Tasks

Perform 3rd Party Assessment of Information Security and Compliance with 27001/2 (or any other compliance control set chosen).

- Perform a Corporate wide assessment of CLIENT's ability to defend against targeted & generic attacks
- Identify the root cause of compliance gaps
- Identify strategy for using the output of the assessment to facilitate a security baseline

Begin remediation planning/budgeting

Technical Report

This section will communicate to the reader the technical details of the test and all of the aspects/components agreed upon as key success indicators within the pre engagement exercise. The technical report section will describe in detail the scope, information, attack path, impact and remediation suggestions of the test.

Introduction:

The introduction section of the technical report is intended to be an initial inventory of:

- Personnel involved in the testing from both the Client and Penetration Testing Team
- Contact information
- Assets involved in testing
- Objectives of Test
- Scope of Test
- Strength of Test
- Approach
- Threat/Grading Structure

This section should be a reference for the specific resources involved in the testing and the overall technical scope of the test.

Information Gathering:

Intelligence gathering and information assessment are the foundations of a good penetration test. The more informed the tester is about the environment, the better the results of the test will be. In this section, a number of items should be written up to show the CLIENT the extent of public and private information available through the execution of the Intelligence gathering phase of PTES. At a minimum, the results identified should be presented in 4 basic categories:

Passive Intelligence:

Intelligence gathered from indirect analysis such as DNS,Google dorking for IP/infrastructure related information. This section will focus on the techniques used to profile the technology in the CLIENT environment WITHOUT sending any traffic directly to the assets.

Active Intelligence:

This section will show the methods and results of tasks such as infrastructure mapping, port scanning, and architecture assessment and other foot printing activities. This section will focus on the techniques used to profile the technology in the CLIENT environment by sending traffic DIRECTLY to the assets.

Corporate Intelligence:

Information about the structure of the organization, business units, market share, vertical, and other corporate functions should be mapped to both business process and the previously identified physical assets being tested.

Personnel Intelligence:

Any and all information found during the intelligence collection phase which maps users to the CLIENT organization. This section should show the techniques used to harvest intelligence such as

public/private employee depots, mail repositories, org charts and other items leading to the connection of employee/company.

Vulnerability Assessment:

Vulnerability assessment is the act of identifying the POTENTIAL vulnerabilities which exist in a TEST and the threat classification of each threat. In this section, a definition of the methods used to identify the vulnerability as well as the evidence/classification of the vulnerability should be present. In addition this section should include:

- Vulnerability Classification Levels
- Technical Vulnerabilities
- OSI Layer Vulns
- Scanner Found
- Manually identified
- Overall Exposure
- Logical Vulnerabilities
- NON OSI Vuln
- Type of vuln
- How/Where it is found
- Exposure
- Summary of Results

Exploitation/ Vulnerability Confirmation:

Exploitation or Vulnerability confirmation is the act of triggering the vulnerabilities identified in the previous sections to gain a specified level of access to the target asset. This section should review, in detail, all of the steps taken to confirm the defined vulnerability as well as the following:

- Exploitation Timeline
- Targets selected for Exploitation
- Exploitation Activities
- Directed Attack
- Target Hosts unable to be Exploited
- Target Hosts able to be Exploited
- Individual Host Information
- Attacks conducted
- Attacks Successful
- Level of access Granted +escalation path
- Remediation
- Link to Vuln section reference
- Additional Mitigating technique
- Compensating control suggestion
- Indirect Attack
- Phishing
- Timeline/details of attack
- Targets identified
- Success/Fail ratio
- Level of access granted

- Clientside
- Timeline/details of attack
- Targets identified
- Success/Fail ratio
- Level of access granted
- Browser Side
- Timeline/details of attack
- Targets identified
- Success/Fail ratio
- Level of access granted

Post Exploitation:

One of the most critical items in all testing is the connection to ACTUAL impact on the CLIENT being tested. While the sections above relay the technical nature of the vulnerability and the ability to successfully take advantage of the flaw, the Post Exploitation section should tie the ability of exploitation to the actual risk to the business. In this area the following items should be evidenced through the use of screenshots, rich content retrieval, and examples of real world privileged user access:

- Privilege Escalation path
- Technique used
- Acquisition of Critical Information Defined by client
- Value of information
- Access to core business systems
- Access to compliance protected data sets
- Additional Information/Systems Accessed
- Ability of persistence
- Ability for exfiltration
- Countermeasure Effectiveness

- This section should cover the effectiveness of countermeasures that are in place on the systems in scope. It should include sections on both active (proactive) and passive (reactive) countermeasures, as well as detailed information on any incident response activities triggered during the testing phase. A listing of countermeasures that were effective in resisting assessment activities will help the CLIENT better tune detection systems and processes to handle future intrusion attempts.

- Detection Capability
- FW/WAF/IDS/IPS
- Human
- DLP
- Log
- Response & effectiveness

Risk/Exposure:

Once the direct impact to the business is qualified through the evidence existing in the vulnerability, exploitation and post exploitation sections, the risk quantification can be conducted. In this section the results above are combined with the risk values, information criticality, corporate valuation, and derived business impact from the pre engagement section. This will give the CLIENT the ability to

identify, visualize and monetize the vulnerabilities found throughout the testing and effectively weight their resolution against the CLIENTS business objectives. This section will cover the business risk in the following subsections:

- Evaluate incident frequency
- probable event frequency
- estimate threat capability (from 3 - threat modeling)
- Estimate controls strength (6)
- Compound vulnerability (5)
- Level of skill required
- Level of access required
- Estimate loss magnitude per incident
- Primary loss
- Secondary loss
- Identify risk root cause analysis
- Root Cause is never a patch
- Identify Failed Processes
- Derive Risk
- Threat
- Vulnerability
- Overlap

Conclusion:

Final overview of the test. It is suggested that this section echo portions of the overall test as well as support the growth of the CLIENT security posture. It should end on a positive note with the support and guidance to enable progress in the security program and a regimen of testing/security activity in the future to come.