

ATME COLLEGE OF ENGINEERING

13th KM Stone, Bannur Road, Mysore - 560 028



A T M E

College of Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
- CYBER SECURITY



LECTURE NOTES

COURSE: ETHICAL HACKING

COURSE CODE: BCY702

SEMESTER: VII

COURSE COORDINATOR: Mr. Chetan G

(ACADEMIC YEAR 2026-27)

CHAPTER-6

The Business Perspective

BUSINESS OBJECTIVES

- There are many characteristics of security and how security is realized in a company. The number of people responsible for security, their practices, and job pressures will have an impact on how the perception of security is materialized in the systems and applications.
- As with many things in business, there are always compromises, agreements, and politics that play into the mix.

SECURITY POLICY

- Security policies play a critical role in managing the organization's security by defining a desired posture that the organization strives to achieve and maintain. Policies set the bar for the organization's security, and information security management and operations personnel are tasked with driving the organization to that mark.
- A security policy is the foundation on which all security operations are built.
- Security policies come in many forms, from simple documents to policy applications that work within the environment to ensure they are communicated and applied.
- Policies are created to describe, detail, and communicate the expected security practices as well as the processes that are to be followed to protect, defend, and recover from attacks.
- The supporting material behind a policy statement consists of standards, guidelines, and procedures that outline specific processes to enforce the policy.
- *Policy Statement.* Policy statements should be clear statements on the particular aspect of security that provide no room for interpretation. They should provide generalized, yet pertinent information on what is expected to be practiced within the organization.
- *Standard.* A standard is the actual definition of the technical nature of the requirement communicated by the policy statement. Standards provide specific details that explain or quantify the policy statement with which they are associated.
- *Guideline.* A guideline is a collection of supporting activities to help associate everyday activities with the support of the policy statement. Guidelines provide general suggestions or recommendations that further clarify the policy with general details or suggestions for their implementation. Without guidelines, the policy statement and standard would have little meaningful impact on the typical user.
- *Procedure.* A procedure defines the tasks required to meet the requirements set forth in the policy. Procedures are step-by-step instructions detailing how a particular task is to be performed.

Following is a simple example of the policy structure.

- Policy Statement:

- Users shall use strong passwords on all network systems and elements.

- Standards:

- Passwords must be at least eight characters in length.

- Each password must contain alphabetic, numeric, and special characters.

- Guidelines:

- Users should avoid using personal information that can be easily guessed, such as a name or critical number as a password.

- Users should seek combinations of words that are easy to remember yet difficult to guess.

- Users should avoid the use of passwords that are commonly found in dictionaries.

- Users should avoid writing the password down.

- Procedures:

- Enforce password policy on NT Domains.

- Log on to domain controller as Administrator.

- Run the User Manager application.

- Select “Accounts...” from the Policies menu.

- Configure the system’s password policy to mirror the organization’s password policy.

- Click “OK” and close the User Manager application.

PREVIOUS TEST RESULTS

- There are many organizations that have tests performed regularly with their own set of results, recommendations, and implemented countermeasures.
- The deliverables from a previous test provide the opportunity to plan a new ethical hack in a manner that is complementary to previous investments.
- For example, a company may have identified specific vulnerabilities during the previous test resulting in the acceptance of that risk. To continue testing a risk that has been identified and absorbed into the client’s acknowledged exposure can be a waste of time. Nevertheless, vulnerabilities change with the ebb and flow of technology. Therefore, assumptions about identified weaknesses should not be made lightly.

BUSINESS CHALLENGES

Today companies are facing security threats that will turn into business risks that may include loss of productivity, financial and legal liabilities, loss of network availability, and corruption or theft of data.

In spite of the risks to achieve business goals companies understand the need to accomplish several fundamentals to ensuring the success for the overall business:

- Meeting financial and business objectives
- Maintaining and increasing corporate brand value and corporate reputation

- Protecting their network infrastructure investment
- Executing and protecting strategic initiatives (mergers, partner alliances, etc.)
- Providing a friendly and secure E-business environment
- Supporting a remote-based employee environment
- Reducing the time to market for providing new services to users and end clients

The security characteristics include:

- Access to security expertise to deal with rapidly evolving and complex issues associated with ensuring comprehensive network security
- Understanding network vulnerabilities and risks
- Protecting confidential corporate or client information
- Providing global and scalable security solutions due to the expanding network size, geography mandates, or corporate mergers
- Quickly deploying new security technology or upgrading existing security products
- Providing customized security solutions for their clients' specific needs
- Quickly identifying and resolving network intrusions and misuse of the network equipment (reducing downtime) maximizing uptime and availability
- Training personnel on security
- Meeting industry-specific security requirements or statutes

SECURITY DRIVERS

The major drivers fueling the need for security include:

- Increasing network complexity
- Ensuring corporate value
- Lower management investment
- Business consolidation
- Mobile workforce
- Government regulations and standards

Increasing Network Complexity

- Networks today comprise a multitude of devices, technology, and applications that are continually being pushed onto the Internet and interacting with customers and partners.
- Business systems are more integrated and exchange information over complex networks such as the Internet.
- The increased complexities of an interconnected network and using the Internet have not only exposed businesses to the global online public, but have resulted in a composite of people, applications, and networks where any point within the system is intimately related to nearly every other point.

Ensuring Corporate Value

Today, many companies are publicly traded on the open market and maintaining shareholder value is significant in business success. In the event of a security breach, the perceived risk of

investing in the company will undoubtedly increase, possibly leading investors to look for other avenues to ensure personal gains. The result can be devastating to an organization's brand value, with measurable financial losses.

Lower Management Investment

In competitive markets and industries, the demand to reduce spending on perceived noncritical technology is becoming routine. For many companies, security is not a core business requirement and therefore security solutions usually meet only the observable demands.

Business Consolidation

- Organizations from all types of industries are seeking opportunities through mergers and acquisitions, and strategic partnerships. Because of the information exchange requirements and the consolidation of dissimilar network infrastructures, applications, and data, there is an increase in the opportunity for security-related issues.

Mobile Workforce

- As the demand for distributed operational models for companies increases to meet the demands of customers combined with cost-saving requirements, the result has been the continued evolution of a mobile workforce.
- A remote workforce needs access to corporate resources to accomplish tasks once provided only to on-site employees.

Government Regulations and Standards

In recent years, we have seen the explosion of government involvement in establishing requirements for the protection of information and privacy. The recent proliferation of regulations is mostly due to two factors:

1. Publication of internationally accepted security standards, and
2. Increase in cyber-related attacks on private and public entities.

The advent of security standards has been based on the demand for a doctrine defining the security "best practices" security practitioners have been employing for over a decade.

WHY HAVE THE TEST?

There are many reasons that drive a company to request a penetration test. More companies are seeking ethical hacking services today than ever before.

CHAPTER - 7

Planning for a Controlled Attack

INHERENT LIMITATIONS

Touched upon earlier, inherent limitations are boundaries that cannot be crossed in the realm of ethical hacking.

Following are some of the limitations that are intrinsic to the test:

- *Time.* The time a real hacker is afforded to collect information, gather tools, test the waters, get to know people, or any other aspect of hacking that can be used to obtain what is desired is arguably limited to only that person's life expectancy.
- *Money.* It should not be assumed that hackers don't have any money. In reality, depending on the role they may play in organized crime, substantial investments may be made in providing them all the necessary tools and technology to perform their deed. For organized crime, investing \$250,000 in a hacker is comparable to investing the same amount in guns or drug refinement equipment.
- *Determination.* Tenacity can play a significant role in how a hacker approaches a target. A disgruntled employee of a utilities company, Vitek Boden, took 48 attempts before he successfully accessed the SCADA system to release one million liters of sewage into the coastal waters off Queensland, Australia.
- *Legal Restrictions.* Regardless of a legal documentation put in place to protect the tester from typical activities that under normal circumstances would be considered illegal, a virtual line remains separating the typical attack strategy from an act of terrorism.
- *Ethics.* In every professional's career he is at one point faced with a dilemma that forces a decision based solely on his ethics.

IMPOSED LIMITATIONS

- The ability to realize the true value of a penetration test is proportionate to the client's interpretation of security and how those assumptions are translated into restrictions placed on the test.
- The point of the small list is to stimulate thought and introspection about your opinions of limitations that have the potential to affect value:
 - No dumpster diving.
 - Only test certain IP addresses.
 - Do not use ISS.
 - No Trojans.
 - No vulnerability can be exploited until permission is obtained.
 - Only wardial certain telephone numbers.
 - No e-mail-based social engineering.
 - No Web application-focused attacks.
 - Only attack Windows systems.
 - Do not use partner information to support an attack.
 - Do not attempt to avoid detection.
 - Only attack one site.

- Do not attack customer DNS systems.
- No user-focused attacks.
- No DoS attacks.
- No information shall be shared between testers on the engagement.
- No information is to be changed.
- No calling cards are to be left behind.
- Do not attempt to attack ports over 1024.
- Only test services running on specified ports.
- If a password file is obtained, the test must stop.

TIMING IS EVERYTHING

- Security is constantly changing within an organization. Through the adoption and evolution of technology, practices, management, and the perception of security within the company, the security posture of a firm rises and falls frequently.
- Many characteristics of security increase, decrease, or simply fluctuate with time. As one characteristic gets more attention, others are certainly going to wane or grow stagnant.
- Security is the combination of technology, management, culture, and policy, and it is difficult to do all of them at the same time in the challenging environment of a typical company.

ATTACK TYPE

- Given the scope and scale of the Internet, it is easy to assume that there are huge numbers of hackers out there with varying degrees of intent and capability.
 1. *Opportunistic.* An opportunistic attack is the result of hackers looking for vulnerable systems rather than systems with specific information for the taking.
 2. *Targeted.* A targeted attack is the assumption that the hacker knows the target and knows what she wants to accomplish.

SOURCE POINT

- There are several types of attack that can be employed to help a company determine its exposure. Typically, these are broken into three major areas, each resulting in various conclusions about where the attack is launched.
 1. *Internet.* When you hear the term ethical hacking you immediately picture someone hacking into a network from the Internet. In most cases, this is a reality. The Internet is seen as the source for all the pains associated with hackers
 2. *Extranet.* To function in today's connected economy, most companies maintain some form of connectivity with partners, suppliers, and customers.
 3. *Intranet.* Arguably, one of the more complicated aspects of ethical hacking is the internal hack. Intranet-based attacks can be difficult to perform given the imposed limitations, but in practice it is like a playground for testers.

REQUIRED KNOWLEDGE

One of the first steps in establishing the rules of engagement is considering what information about the target should be provided to the tester.

Usually some form of information is provided by the target and only in the most extreme cases absolutely no information is offered.

Following are some basic definitions of information provisioning:

- *Zero Knowledge.* Zero knowledge is just that: the tester is provided nothing about the target's network or environment.
- *Limited Knowledge.* Something growing in popularity with companies seeking penetration testing is providing just enough information to get started.
- *Total Exposure.* Total exposure is when every possible piece of information about the environment is provided to the tester. Prior to the start of the engagement, a list of questions and required items is sent to the customer in preparation for the meeting.

MULTI-PHASED ATTACKS

- Many companies look to have several types of penetration testing performed in parallel or series in an attempt to gather as much insight into their security posture as possible.
- If a company is concerned about collusion between an employee and an outside hacker, then a parallel attack with sharing information between them is needed. On the other hand, if the client is worried about a hacker targeting her company, a serial attack should be used.

The following explanation should help in summarizing each of the four types:

1. Parallel shared
2. Parallel isolated
3. Series shared
4. Series isolated

PARALLEL SHARED

Multiple resources attacking the client network from the Internet, with limited access, and internal presence at the same time, and sharing information between them to gain added benefits, is an example of a parallel-shared attack structure.

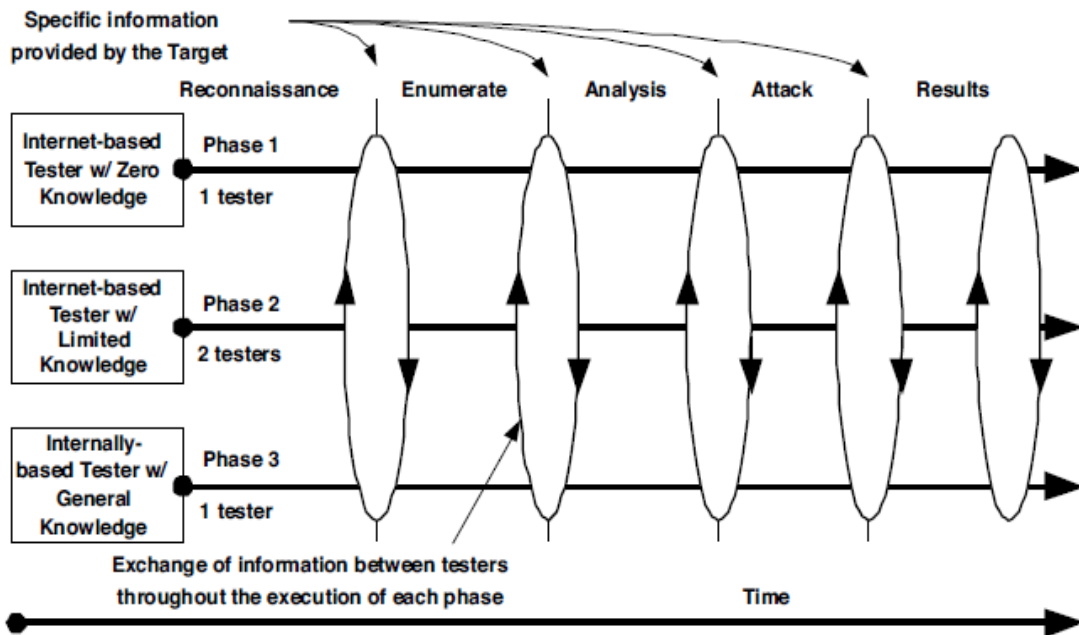


FIGURE 7.1 Impacts of Multiple Attackers Sharing Information Simultaneously

Companies should employ this type of attack when they are concerned about employees collaborating with hackers to obtain information or money.

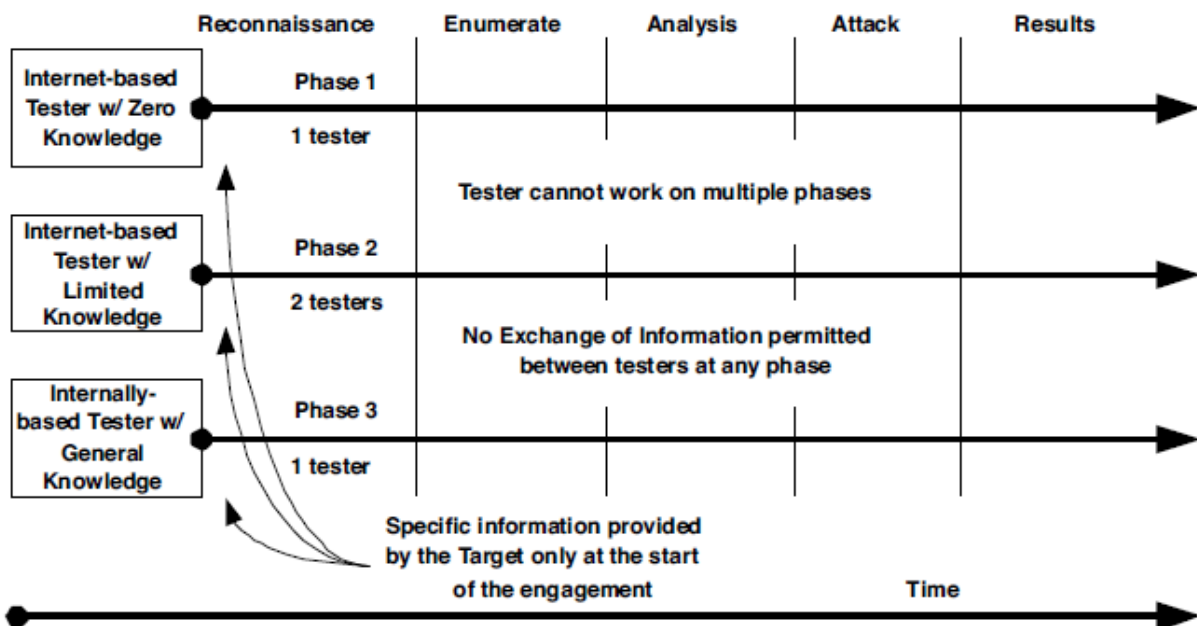


FIGURE 7.2 Multiple Simultaneous Tests without Sharing Information

PARALLEL ISOLATED

There are occasions where the multi-phased test is performed in parallel, but no information is exchanged between the consultants performing the tests.

There are few security reasons to perform a test of this type to mimic a real assault. In nearly all cases, the driving factors are money and time.

SERIES SHARED

There is always the potential for an attacker to move from a digital attack to a physical one. This is especially true in comprehensive and well-funded attacks, such as espionage or terrorism.

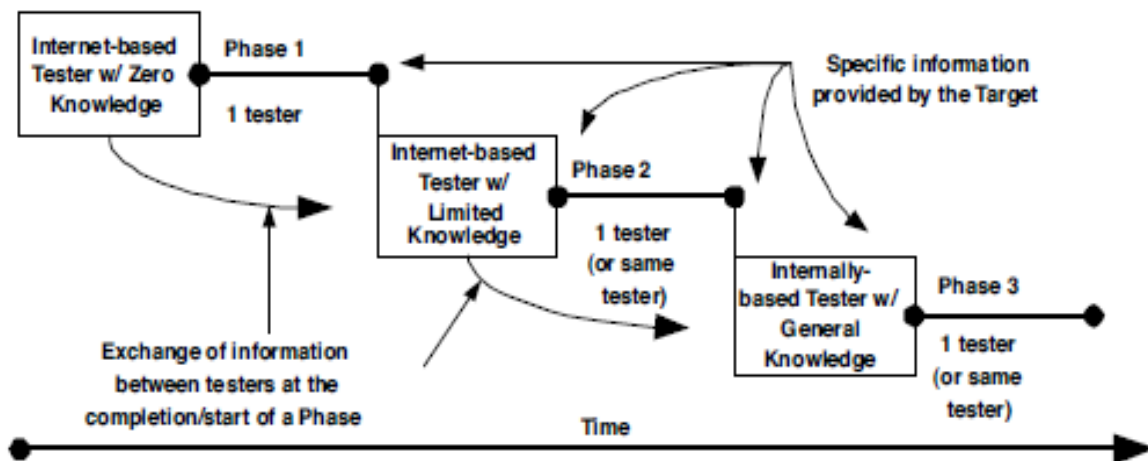


FIGURE 7.3 Sequential Testing Permitting Information to Flow from One Phase to the Next

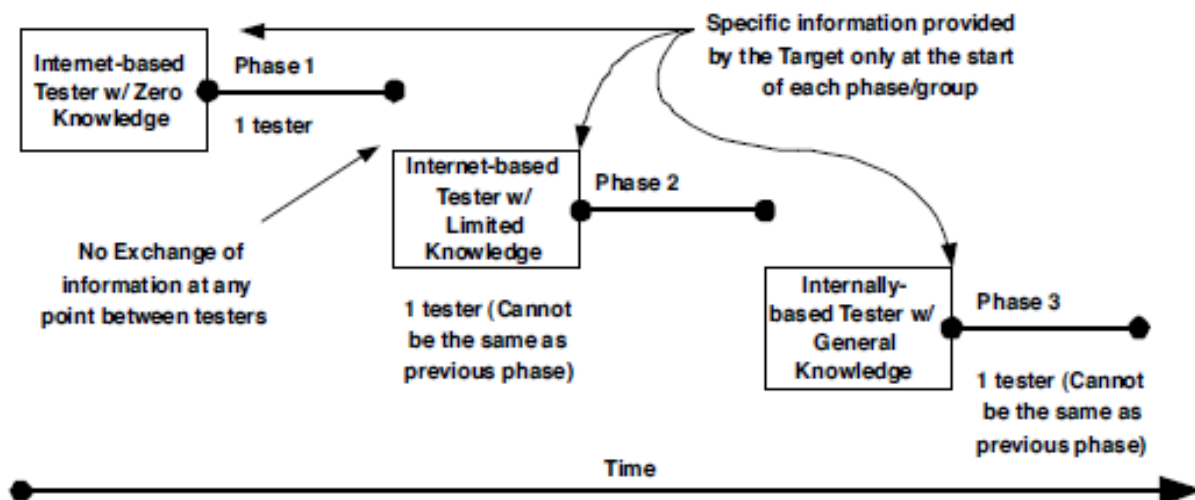


FIGURE 7.4 Sequential Testing without Permitting Information to Flow from One Phase to Another

SERIES ISOLATED

Series multi-phased penetration tests where information is not transferred from one phase to another is typically practiced when each phase is considered unique, unrelated, and there is ample time allotted to the engagement. This technique is also leveraged when there is a great deal of management associated with each phase.

VALUE OF MULTI-PHASE TESTING

It is safe to assume that information is the key to a successful test, or a real attack for that matter, and managing information in a multi-phased, or even a straightforward, penetration test can directly affect the true value of the test being performed.

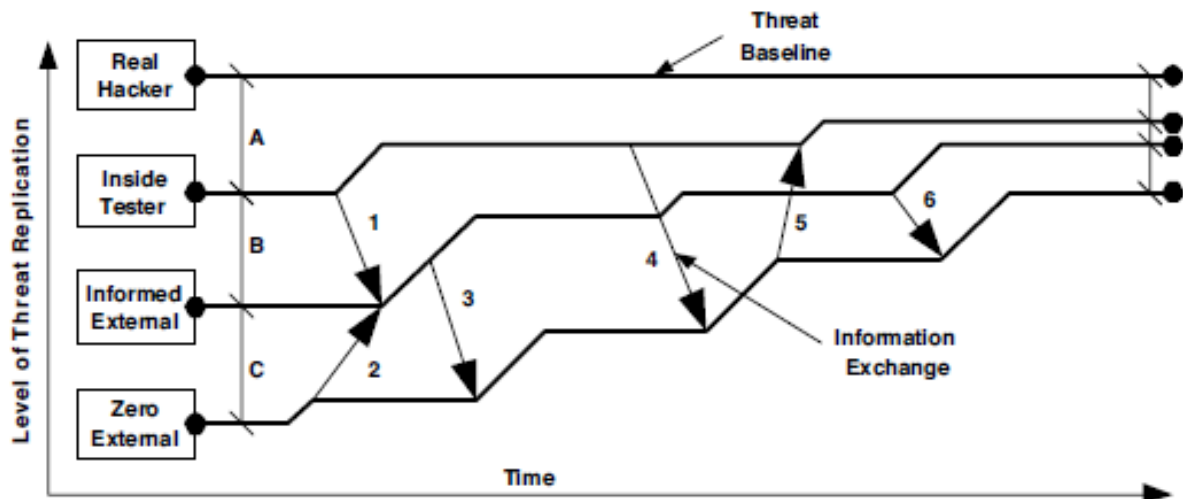


FIGURE 7.5 Impact of Overlapping Information in a Multi-Phased Approach

EMPLOYING MULTI-PHASED TESTS

- Employing a multi-phase attack has the potential to introduce several types of complexities and costs to the target. Nevertheless, many of these challenges are greatly outweighed by the potential for considerable value of the test.
- Companies looking to have tests performed usually have a predefined perception of what they want, leading to a conclusion on the scope and methodology of the test they expect.
- Vendors of ethical hacking services are more than capable of performing complex tests, but comprehensive testing scares many of their customers.

TEAMING AND ATTACK STRUCTURE

As with any test there must exist procedures outside the direct experiment to ensure stability, safety, and accuracy of the results.

Following is a very simple teaming framework for establishing a project management protocol, which assists in dealing with unexpected events in the engagement—Red, White, and Blue—external, control, and internal, respectively.

RED TEAM

The Red Team performs the test. Based on the type of test and the level of knowledge their client is willing to provide, they may be involved in the establishment of the engagement with the White Team to make certain expectations, guidelines, and procedures are well communicated. The goal of the Red Team is relatively simple: to attack the target firm within the established scope of the engagement and communicate to the White Team any critical issues that may represent a risk to the target organization.

It is necessary for the Red Team to provide the following information: vulnerability explanation, testing focus, and mitigation.

- *Vulnerability Explanation.* Detail the vulnerability and the impact that could result from exploitation. This can include characteristics such as downtime, exposure of critical business systems such as billing or transaction systems, customer impact, partner exposure, or the inadvertent disclosure of private or proprietary information previously defined as beyond the scope of the engagement.
- *Testing Focus.* Beyond detailing the extent the proposed attack could have, it is necessary to explain what would be the disadvantages of not performing the test.
- *Mitigation.* Finally, for the client to fully weigh the options compared to risk and cost, the Red Team should provide a collection of high-level recommendations for repairing the hole.

WHITE TEAM

The White Team is a mixture of customer representatives and the managing staff of the consulting firm. The White Team is the liaison between the attackers and the target providing control over the attack and monitoring the reaction of internal staff to the test.

Following are some examples of specific issues where the White Team can become very helpful: piggyback attacks, reverse impact, and detection.

- *Piggyback Attacks.* Some organizations are constantly under attack from real hackers because of their size or what they represent. It is not uncommon for hackers to monitor a target's network, waiting for the opportunity to gain access.
- *Reverse Impact.* Stated earlier, the Red Team should notify the White Team if a critical vulnerability is identified and report on the various risks associated with the weakness.
- *Detection.* Although some tests are performed surreptitiously to avoid detection there are cases where this is not critical to the success of the engagement.

BLUE TEAM

The Blue Team is the internal employees who, traditionally, are not aware the test is taking place. If someone knows the test is being performed, it is best to make her part of the White Team.

There are three primary objectives for establishing a Blue Team: incident response, vulnerability impact, and counterattack.

1. *Incident Response.* Organizations have different methods for dealing with attacks and responding to incidents. In some cases, firms seeking penetration-testing services are more interested in measuring the ability of their security team to react to a threat than the actual attack itself.

2. *Vulnerability Impact.* As with the other two teams, the ability to determine how badly a vulnerability can affect the network's operations falls within the role of the Blue Team.
3. *Counterattack.* A hugely debated concept is counterattacking. When under attack, a company can attempt to stop it by instituting updated controls, but, in the case of a counterattack, will attempt to inflict damage on the hacker.

TEAM COMMUNICATIONS

Creating a communication plan for the White and Red Teams is essential to making sure the groups can communicate in a secure and timely fashion. There is little that can be prepared for the Blue Team because they are simply unaware of the entire process. However, the White Team should present a plan, or an existing communication process at the beginning of the project so the Red and White Teams are assured there is a mechanism for the Blue team to provide information to the White Team. There are several components to the communication plan beyond membership and contact information.

- *Communication Platforms.* Define the types of acceptable communications that can be utilized by the team members.
- *Criticality Matrix.* Defining a minimum of three classifications of information will help determine what should be shared with whom, how that information is to be communicated, and the timing.
- *Materials and Format.* Based on the type of communication and the platform, there must exist acceptable supporting materials and format of the communication.

ENGAGEMENT PLANNER

A great number of details have been introduced: subjects ranging from multi-phased attacks to information flow from the target to the testers, as well as between the testers on an engagement.

When all these components of the test are considered, the planning of the engagement can become overwhelming. As stated above, many organizations have an ethical hack performed with very little planning.

Guidelines:

- Perform a self-evaluation of your goals and objectives. Ask yourself what you expect to gain from the test and how you plan to use the results.
- Consider the scope of the attack and what is "in bounds."
- Ensure all the appropriate people are involved. On paper this appears obvious and simple, but internal politics and departmental rivalries introduce interesting results.
- Commit to having a technical expert involved in the process in addition to business managers or executives.
- During the planning session, ask a lot of questions. However, one must keep an open mind and expect answers that conflict with personal perceptions of security.

THE RIGHT SECURITY CONSULTANT

Security consultants come in many forms with different abilities and conclusions about security. Much of this is based on their exposure and experience in the security industry and where they have realized successes and failures.

TECHNOLOGISTS

- A natural progression for many in the security field came from their experience with technology and implementing solutions in a secure manner. For some, this started early with their first installation of Windows, UNIX, or a router and they gravitated to securing that system. Firewalls are a good example where some evolved from installing routers or system gateways to integrating complex firewalls.

ARCHITECTS

- There are security consultants who have moved away from technology, or never fully immersed themselves in technology, and focus on the business of security.
- Many architects may have begun their careers with technology, but were immediately drawn to the operational aspects of security.

ETHICS

- An understanding of ethics involves learned behavior, problem solving, creativity, invention, awareness, and social structures, among other life attributes. In virtually every event in our lives—in our problems, opportunities, decisions, actions, reactions—ethics make a difference.
- Information security requires a substantial amount of trust, an attribute based on a foundation of ethics. Security professionals are constantly provided sensitive information about a company and their systems to accomplish their task.

The following list is a good basis for understanding what is and should be expected from people performing security services.

1. *Perform Services in Accordance with the Law.* There may be situations where a consultant is asked to perform or made aware of something illegal.
2. *Maintain Confidentiality.* As alluded to above, security consultants are regularly exposed to proprietary information and ethically bound to protect that information.
3. *Honesty.* In addition to simple professionalism, given the sensitivity of interacting with proprietary information and all that it implies, honesty must be practiced to ensure continued trust.
4. *Conflict of Interest.* Everyone during some point in his or her career has been faced with professional conflict.
5. *Intentional Acts.* Clearly associated with ethics, intentionally harming or damaging the reputation of clients, employers, or colleagues is unacceptable behavior.

THE TESTER

- It is clear that ethical hacking can provide value to the overall assessment of an organization's security posture and assist in developing solutions that better meet the types of vulnerabilities and threats.
- The practice of hiring hackers was commonplace during the early years of ethical hacking when the skills of a traditional security consultant were in defending rather than attacking a customer's network.
- In addition, for hackers it is an opportunity to meet their personal hunger for illicit activities, but in a legitimized format while getting paid handsomely. People choose various paths in life and the argument for reformed hackers for hire is you cannot hold someone accountable for their historical activities.
- Hacking for money is also a fertile territory for training people how to hack.

LOGISTICS

There is another side to planning: logistics. Logistics are the nuts and bolts of an engagement and are a necessary evil to ensure the total operation is a success.

AGREEMENTS

An agreement between the service provider and the customer is a must.

It is doubtful that standing agreements cover areas directly associated with the risks of hacking a network.

There are several key characteristics of penetration testing that should be evaluated by both parties. Of course, the granularity and the context of the agreement are up to the customer and the provider, but should cover the following in some manner: downtime issues, system and data integrity, get out of jail free card, intermediates, and law enforcement.

By and Between "Client" and ACME Services Inc.

- Client has requested the services of an ACME Project Team ("ACME Team") for a security assessment of Client's network environment.
- The undersigned has the authority to permit, as further signified by a letter to be supplied to ACME in a form as attached in Exhibit A, and by this signature authorizes the ACME Team to attempt to compromise the devices on the Client network during the proposed security assessment.
- ACME warrants that all security services shall be performed in a professional and workmanlike manner in accordance with this agreement. ACME makes no warranties of merchantability and fitness for a particular purpose.

Accepted and Agreed to by:

ACME Services Inc.:

Client:

Signature

Signature

Print Name

Print Name

Title

Title

Date

Date

DOWNTIME ISSUES

- Even if a DoS attack is part of the engagement, the intentional or accidental shutdown of a system must be addressed.
- Many companies maintain service-level agreements with their customers (internal and external), and when data or services are not available it not only costs the company money to rectify the problem, but there are frequently fines associated with the downtime.
- Given the risk associated with a penetration test, both organizations have to come to some form of understanding before starting the engagement.
- Without an agreement defining the responsibilities of both parties to address risks associated with the test, the relationship between provider and client can grow very bad, very quickly.

System and Data Integrity

- Exploiting a vulnerability is one of several steps in performing a test.
- The major difference is that the tester must notify the client that the backdoor was installed and how to remove it.
- As you can see, implanting backdoors moves well beyond known or discovered vulnerabilities associated with poor security practices of the client and actually introduces security holes based on the actions of the tester.
- It should be noted that in an attack scenario, modifying data from a remote system with stolen privileges could cause problems. It is necessary for the organizations to discuss preparing, detecting changes, and recovering data in the event of an adverse event.

Get Out of Jail Free Card

- One of the more humorous aspects of penetration testing is the “Get Out of Jail Free Card.”
- Hacking can attract the attention of many people and organizations not aware the hack is a test, such as the FBI.

- The “Get Out of Jail Free Card” is an important document to ensure the tester has some form of protection. Of course, the document has to be very clear, dated, and signed with several pieces of contact information; otherwise, it could be used by a real hacker.

INTERMEDIATES

- During a test, many networks and organizations can be caught in the wake of an attack and possibly be affected by a test to which they did not agree.
- It may be necessary to notify the owners of networks that have the potential of being inadvertently included in the attack.

Partners

- As networks have evolved, companies have leveraged them to exchange information with other firms to promote more effective business models and growth through alliances.
- Depending on the type of relationship a client has with its partners, it is usually rare for the targeted company to allow or sanction any type of attack on a partner’s network.
- If a customer wants the greatest value, the opportunity to test all systems on their network, an ethical hack regardless of owner should be considered.
- The obvious workaround is to collaborate with the partner and see if it is willing to permit a test against its system.
- In the event the partner does not permit the test and all other avenues have been exhausted, the client should ask them to sign some form of agreement binding them to the potential risks.
- Partner networks, systems, and applications pose a challenge to the tester in addition to presenting a potential obstacle for the customer to realize the full value of the exercise.

Customers

- Businesses offer a wide range of products and services to customers that may be based on technical integration to provide the product.
- In general, businesses supply several different types of network connectivity for their customers, such as frame relay, remote dial-in access, and VPN on a segmented network, much the way they support partners.
- Conversely, many companies such as Amazon.com and Yahoo! offer products and services simply over the Internet that are accessed via a traditional Web browser.
- There are several types of attacks that can leverage customer connectivity or privileged access allowing the tester to penetrate the target network.
- For clients who want to understand the exposure if a customer were to attempt an attack or a hacker were to somehow obtain the credentials of a paying customer, they should provide the necessary information to the tester. This is a prime example of a multi-phase, shared attack strategy.

Service Providers

It is common for a company to use a service provider to support various IT services internally or for external customer support. Services can range from simple Internet connections and collaboration tools to applications and managed security services.

the best method is to establish a basic approach that can be applied to all types of services, if for no other reason than to build a starting point. This can include:

- *Communication.* Apprise the service provider that the test is being performed and create a communication protocol to support emergencies.
- *Details.* The source IP addresses of the tester, timing of the test, and what falls within the scope of the test are all important elements to share with any provider.
- *Support.* More often than not, service providers can help with collecting information about the test. This is especially true with managed security service providers. They can passively collect information about the test and provide a report on activity.

Without a foundation of understanding the test will have the potential to cause problems.

LAW ENFORCEMENT

- As mentioned earlier, law enforcement, specifically the FBI, is getting more and more involved with Internet-related attacks. Usually, the FBI only becomes involved after the attack to help investigate the crime in support of the victim.
- However, more time is being invested by the FBI and other law enforcement agencies in looking for malicious activities on the Internet.
- When planning an attack against a company, especially large ones that have historically attracted hackers and may have asked the FBI for support, it is important to make them aware of the test.
- Notifying law enforcement is not necessary in most engagements, but it should be considered as a gesture of professionalism and awareness that the test could affect others inadvertently involved.