Three Different Shades of Ethical Hacking: Black, White and Gray

GSEC Practical Assignment
Version 1.4b
Option 1

David M. Hafele
February 23, 2004

Abstract

Corporations and other entities are faced with the unenviable task of trying to defend their networks against various types of intrusive attacks. Although traditional methods of deterrence, (i.e. firewalls, intrusion detection devices, etc.) have their place in this battle, there has arisen the need to utilize specialists who are adept at exploiting both known and unknown vulnerabilities in networks in order to determine the security posture of an organization. These "Ethical Hackers" have created a niche for themselves in the "Defense in-Depth" spectrum. This paper seeks to investigate the rationale for using these penetration experts in order to determine the level of security in an organization. Additionally, it will examine the underlying philosophy behind choosing one of three possible attack models for the penetration tests: Black Box, White Box and Gray Box. Finally, each one of these ethical hacking approaches will be discussed.

The Rationale for the Ethical Hacker

Virtually everyday, one either reads in the newspaper or sees on the Internet some reference to a company or an organization suffering from the brunt of an overt attack against their networks. Hacking or cracking as it is known in some circles, has become synonymous with this new breed of criminal activity, hence to be labeled a "hacker" is understood in today's society as being a derisive term. However; this was not always the case, as it originally was understood to be a "badge of honor" bestowed to one who exhibited a high-level of expertise in knowledge about various computer-based subjects. Unfortunately, adverse media publicity skewed this view and blurred the distinction between one who was merely an intellectual seeker of computer knowledge and one who utilized this knowledge for criminal or selfish gains. [22]

Because of the explosive growth of the Internet and networks, there is a shortage of information technology security specialists. Now, a new breed of network defenders has arrived. Known as "Ethical Hackers", these individuals are viewed almost as an enigma. The marriage of the term ethical with hacking is understood as being an oxymoron, analogous to calling someone an "honest criminal." Nevertheless, it would appear as though Ethical Hackers may have found a place in our arsenal of defenses of network assets and that they are here to stay. Today, the stakes are much higher and the playing field encompasses every aspect of our society: business and industry, national security, educational enterprises and public/private organizations. The realm of the ethical hacker will expand into all these arenas and the insight derived from their expertise will have to be included in the body of statistical and empirical knowledge used to properly defend informational assets.

Business and industry face increasing scrutiny from regulatory constraints and from debacles like the Enron scandal. Corporations are forced to confront many factors that they have not had to face in the past. It is no longer acceptable to have a laissez-faire attitude towards protecting one's informational assets. Rather; as Gary Baker and Simon Tang of the Chartered Accountants of Canada Information Technology Committee indicate: successful businesses are challenged with pressures from a whole range of representatives including management, board of directors, customers and shareholders, in order to give an account for the information which they have been entrusted and how they are attempting to protect it. [3] These additional factors have contributed to the heightened sensitivity to maintaining the confidentiality, integrity and availability of network and financial resources.

Business is not the only entity that is a target in network attacks.
Our own national security is at risk by those who would seek to undermine our nation's stability. The U.S. General Accounting Office (GAO) indicated in 1996 these alarming statistics concerning attacks on Department of Defense (DOD) installations: the exact number of attacks against the DOD is unknown and is not properly reported, the Defense Information Systems Agency (DISA) feels that as many 250,000 attacks were attempted against the DOD that preceding year and finally as much as 65 percent of those attacks were successful. [13] In addition to these findings, the GAO anticipates the rate of growth of these attacks to be roughly doubling each year, making it very difficult for our nation to fend off these intrusions. [13]

Our educational enterprises also face the uncertainty of network compromises. As the bulwark of intellectual freedom and expression, many institutions, both public and private, fail to have adequate security measures in place. RedSiren IT Security Management Solutions says at their website: http://www.redsiren.com/education.htm that many academic institutions fail to protect their informational resources and network operations from all manner of unauthorized access and that the scholastic community has a responsibility to guard their students and their family members against "risky activities, identity theft, fraud or other malicious acts." [15] This places the impact of information security into the very heart of our society. Even our public and private organizations must be mindful of these warnings. There is no individual, group or organization, which is insulated from possible attacks, and each may offer something of intrinsic value to a determined criminal hacker.

Now, where does the Ethical Hacker fit into this scheme of things? Initially, it must be emphasized that the skills, which an Ethical Hacker may possess, could be utilized in any environment where information is housed, exchanged or disseminated. Penetration testing will become more commonplace in business, industry, government and in the public/private sector. The key factor is to realize that the Ethical Hacker may very well be instrumental in developing a more comprehensive panorama of the network and its vulnerabilities in any scenario. Much of what the Ethical Hacker does is done in "real-time", so this helps to clarify what issues a group or corporation may be facing presently. By being made aware of the current issues, the client of the Ethical Hacker can develop a plan for dealing with not only the existing problems, but also they can develop a plan of attack for addressing future ones. In addition, if the Ethical Hacker is truly "worth their salt", then they should be able to recommend security solutions that are viable and well suited to the customer's business needs.

Ultimately, the ideal for the Ethical Hacker is to be a contributor to the body of knowledge of network security. With this in mind, it is imperative that these individuals follow a scientific methodology in approaching their respective network attacks. Further, the idea of breaking into a customer's network must be viewed in light of the final goal of mending it. This means that the Ethical Hacker is not one who is self-seeking, rather; they must view themselves as being another cog in the "Defense in-Depth strategy.

Philosophy of Attack Models: An Introduction to the Dilemmas, Which Face the Ethical Hacker and the Client

In virtually every aspect of life, there are different approaches to things. This is especially true when it comes to determining how to attempt to attack a client's network. Two factors which come into play are: what is the scope of the project and what is the amount of prior knowledge needed by the Ethical Hacker about their client and its resources in order to begin the mission? The criteria for determining these answers are largely founded upon what the customer desires, not necessarily what they need. As both Baker and Tang indicate, there is a large amount of negotiation done between the attack team and the customer prior to commencing with the project and that the final stated objectives will determine its scope. [3] These final objectives are going to be determined by the customer. That being the case, then the question that remains is this: does the client really desire to know the true level of security within their organization? This is obviously a loaded question since there are many different caveats concerning truth. What may be true in one situation may be false in another. Indeed, we are dealing with the problem of perception versus reality. Wojciech Dworakowski offers insight into this issue by saying that there is the common belief held by management that a firewall appliance is all that is needed to insure network safety. [6] In essence, this viewpoint may be summed up by saying that “I think my network is secure, therefore, it is secure, no matter what the security experts may say.”

Obviously, if the Ethical Hacker’s client feels this way, then one has to wonder whether they have an adequate understanding of what constitutes network security. RP Srikanth says that even though companies bring in outside security consultants, security breaches will still occur due to a lack of customer knowledge. [20] Moreover, there is more to it than mere lack of knowledge: business models and other constraints could be shaping what is going on. This is where the Ethical Hacker must be in tune with the pulse of the customer. Bill Coffin concurs when he says that the effectiveness of the ethical hack is largely determined by how well it coincides with the client’s business risks. [4] This observation implies that the Ethical Hacker must never be in the dark when it comes to assessing the business and political climate of the customer. If it is determined that no prior knowledge of the network resources is to be given to the Ethical Hacker, then it becomes all the more imperative for the Ethical Hacker to become intimately acquainted with the “corporate personality” of the client.

One thing that must be pointed out is that the Ethical Hacker must realize that providing education to the customer is paramount. Granted, one of the initial goals of the penetration tests may be to access the vulnerabilities of the network, but in the end, the customer must glean a larger understanding of the network as a whole. However, the customer’s predilections and agendas determine what they will choose to learn. Therefore, they must be made aware of what is truly at stake. If they misjudge their risk or liability, then it could be detrimental to themselves, to their customers or to others. This risk also extends to the testing process itself. Baker and Tang point out four caveats which must be made known to the customer prior to the tests commencing: first, it is possible that no significant vulnerabilities will be discovered, second, if the testing objectives are not met, then there could be conflict between the testing team and the client third, the testing itself could generate unexpected problems and fourth, it is conceivable that confidential or proprietary knowledge could be compromised. [3] In light of these issues, the Ethical Hacker must also exercise strident judgment in accomplishing the penetration test in order to mitigate possible risks or misunderstandings.

It should be readily apparent to the Ethical Hacker and his/her team that there is a great deal of psychodynamics going on in the clients’ world, whether it be business, government or education. For the business sector, the client is faced with pressure from shareholders, customers, competitors and regulatory agencies. However, when it comes to network security, pressure often comes from the fear of exposure. Ron Gula provides insight into the possible internal issues that the customer's network security team face when dealing with the unknown. The network team may have made unsubstantiated claims about the level of security that is found in the network. If the penetration team reveals hidden weaknesses in the clients' network security posture, then this could evoke animosity from the network staff towards the ethical hacking team. [8] This area of concern must be taken into consideration when determining whether or not to make the systems administration group privy to the penetration attacks. Therefore, to minimize the possible repercussions from this, both the customer and the ethical hacking team must be wise in determining who are to be included in the inner circle of knowledge.

Additionally, the testing team may be facing two mutually exclusive perspectives as to how security measures are to be implemented: the view of the business world versus the view of the ethical hacking community. Max Smetannikov feels that the business community likes security solutions to be "straightforward and ubiquitous." [19] Conversely, Smetannikov states that the ethical hacking community views security as being organic and under a state of constant change so that simplistic one-and-for-all security solutions are destined to failure. [19] What the ethical hacker must impress upon the client is the fact that we live in a dynamic, not a static world. Attacks change, networks change and businesses change so our defenses against network attacks must be fluid and dynamic as well. Therefore, it is to be expected that multiple attack models are to be part of the ethical hackers' arsenal.

Philosophy of Attack Models: Three Methodologies Defined

Three basic models are utilized by the Ethical Hacker in order to attack the network. These models are the Black Box Model, the White Box Model and the Gray Box Model. Concerning the Black Box model, Ron Gula states that this penetration test is only revealed to a very few members of the network security team in order to ascertain their response to the attack. [8] However, it must also be mentioned that the Black Box model also presupposes that the Ethical Hacker has limited knowledge of the network. This forces the ethical hacking team to gather a lot of information about the company from various sources prior to launching the penetration attack. With respect to the White Box approach, Gula indicates that this model presupposes an expansive amount of knowledge about the company and its network. Furthermore, he indicates that the scope of the pre-attack information gathering might include interviews, access to internal network assets, physical security inspections and security policy evaluations. [8] The last category of attack models is the Gray Box model. This model combines elements of both the Black Box model and the White Box model providing a hybrid method of attack. [8] In other words, knowledge concerning some areas will be clearly defined, whereas, other areas will require detective work by the ethical hacking team.

Since each model approaches the attack from a different vantage point, all will have a different focus and therefore, a unique perspective that will be derived from the attack. This being the case, it is conceivable to conclude that all of the methods are valuable to the Ethical Hacker and the client. However, none of these methods exhausts the range of possibilities when it comes to hacking into the network. Therefore, both the client and the hacking team must understand this and come to their own conclusions which model or combination of models is best suited for their individual network security assessment.

The Black Box Approach

The Black Box model follows a stochastic approach to the attack. [26] This signifies that there are many more unknowns or variables to be learned when utilizing this modus operandi of attack than when one uses other approaches. However, this does not mean that this method is anarcharistic or without bounds. The static portion of this attack centers on the operational constraints that are placed upon the hacking team. These limiting parameters may be quite extensive and detailed based on the levels of risk that the client is willing to assume. Consequently, the hacking team must know the “rules of engagement” beforehand.

Andrew T. Robinson views the perspective of the Black Box hacker as one who is a distrusted outsider with little or no knowledge concerning either the network or any security policies in effect. [16] Therefore, this model assumes that the network attackers proceed from the unknown to the known much as a criminal hacker would in real life during the initial phases of the attack. However, one must also differentiate between the various kinds of criminal hackers in order to determine which categories of attackers will be used during the Black Box test. There are four basic competencies or types of criminal hackers: script kiddies or novices, technically astute hackers, sophisticated “Ueberhackers”, and disgruntled insider attackers.

Webopedia.com at http://www.webopedia.com/TERM/s/script_kiddie.html gives the following definition of script kiddie:

> A person, normally someone who is not technically sophisticated, who randomly seeks out a specific weakness over the Internet in order to gain root access to a system without really understanding what it is s/he is exploiting because the weakness was discovered by someone else. A script kiddie is not looking to target specific information or a specific company but rather uses knowledge of a

> vulnerability to scan the entire Internet for a victim that possesses that vulnerability. [23]

This level of attacker tends to approach hacking from a more-or-less “helter- skelter” form point of view where they run roughshod over any target that they may find using any sort of attack tool that works. This being the case, it is especially important that the penetration team clear this approach with the client in order to determine the appropriateness of this “shotgun” technique.

Technically astute hackers represent a higher caliber of threat than the script kiddies do. Typically, they have obtained quite a high level of understanding and experience with operating systems, programming or network theory. This variety of intruder is one who can serve as an excellent attacker model for the hacking team since their skill level would very likely be encountered in a real hacker attack.

The most menacing class of attacker is the so-called “Ueberhacker”. Both Dan Farmer and Wietse Venema categorize this individual as being one who has extensive knowledge and experience about a myriad of computing subjects, ranging from developing their own vulnerability programs to erasing any evidence of their attacks. [7] This villain is most insidious about how they go about their assault. They are extremely methodical and tend to be very particular about their targets. For the ethical hacking team to emulate this attacker requires a great deal of resourcefulness and patience. This patience may not translate well into the time framework allocated for the penetration attack, so it is conceivable that the “Ueberhacker" approach may be outside the scope of the Black Box or any model of penetration tests.

The last form of attacker is the insider. We are all familiar with this type of individual: the disgruntled worker who has an “axe to grind” with either their current or past employer. Paul Midian points out that this kind of hacker is not necessarily technically astute; however, they either have or have had access to information about the network that makes them potentially dangerous to the client. [10] Insider attacks are well known and very effective, but the Black Box model usually does not use this sort of category for hacking since it is an attack that begins externally, not internally. One is more likely to see this category utilized in either the White Box or the Gray Box methods where either internal information is provided to the hacking team or where one of the attack members is surreptitiously placed on the customer’s staff.

The Five Phases of the Black Box Approach

Although there are numerous ways of delineating the breakdown of the Black Box methodology (note: some aspects of this breakdown are also applicable to the White Box and Gray Box models as well), one very useful framework developed for this attack method is described by Paul Midian. There are five basic phases to the Black Box test: the initial reconnaissance, service determination, enumeration, gaining access, and privilege escalation. [11]

The initial reconnaissance phase is an extremely important facet of the attack. Gabriel Serafini states that this phase centers on investigating the target organization by means of readily available public information. [18] A great deal of insight can be gained concerning the objective just by accessing the client's own web page. Often, important information concerning key personnel is listed here as well as other information that can be utilized when attempting to use social engineering tactics. Other sources of useful public information include using the various WHOIS databases, (i.e. ARIN, InterNIC, RIPE etc.), to glean important insights concerning a company's network and personnel. For example, the ARIN WHOIS database provides the following information about establishments, which utilize its services at http://ww1.arin.net/whois:

> ARIN's WHOIS service provides a mechanism for finding contact and registration information for resources registered with ARIN. ARIN's database contains IP addresses, autonomous system (AS) numbers, organizations or customers that are associated with these resources, and related points of contact. [1]

As anyone can see, a great deal of information about a company can be gathered just by using this one resource. There are many other valuable sources of information that may be utilized: trade magazines, web search engines, newspaper articles, advertisements, and even such mundane items as the telephone directory. Information that may seem to be innocuous in and of itself, can be particularly valuable in combination with other seemingly harmless data. Through this aggregation of public domain information, the Black Box team can begin to paint a vivid picture of the target establishment.

The next stage of the Black Box approach is called the service determination or scanning phase. Namji describes this phase as one that attempts to derive information about the various listening services and ports that are currently operational on the client's network. From this information, the penetration team should be able to determine the type of operating system that the client is using. [12] Different operating systems have unique characteristics in that they will listen on specific TCP ports for service traffic which is particular to that OS. For example, Microsoft's operating systems are famous for their utilization of such well-known ports as TCP-UDP137, 138, 139 and 445. [14] When a port scanner indicates that these ports are listening, then it is a good bet that that organization is running on a Microsoft platform. Among the various tools that the team may utilize to gather this data are the well-known NMap and others. The testing team will also use this time to scrutinize the network for various vulnerabilities. They may utilize "war dialing" techniques to determine if there are any errant dial-in modems existing on the network. Modems often provide the Ethical Hacker with a means to bypass the perimeter defenses of a network, (i.e. firewalls and routers), thus giving the attack team direct access to the internal protected network. The penetration team will also utilize vulnerability scanners, (i.e. ISS, Nessus, SARA, SATAN, SAINT etc,), in order to automate the process of determining possible weaknesses in the companies network.

Webopedia.com provides a useful definition of vulnerability scanning at http://www.webopedia.com/TERM/v/vulnerability_scanning.html, which states that it is:

> The automated process of proactively identifying vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. [24]

Every application and operating system has built-in flaws. The automated vulnerability scanners enable the hacking team to be able to document these defects in a quick and effective manner. With this vital information, they can research not only what methods can be used to capitalize on these vulnerabilities, but also they can determine what avenues are available for mitigating the risks associated with them.

The third element in the Black Box attack is the enumeration phase. Ida Mae Boyd breaks the objectives of the enumeration attack into three distinct focal points: "network resources and shares, users and groups, and applications and banners." [2] If any of these items have not been properly guarded, then this provides the hacking team with an avenue for gaining initial access to the network system.

The Black Box attackers will look to see if there are any open network services available for possible exploit. It is often observed that network operating system vendors usually ship their systems with most or all of their network services running. Some services, such as Telnet and FTP provide a direct link to the customer's most critical resources. Since neither one of these TCP services require strong encryption and since information and authentication is sent in clear-text, they are both vulnerable to numerous types of attacks. Sharon Ruckman of Symantec Security response sums it up by saying either close or deletes any services that are not needed. [17]

Users and groups have their own special issues. The enumeration phase will attempt to determine whether or not there are default user or administrator accounts operating on the network. Najmi states that network administrators often fail to delete guest user accounts. [12] This is but the tip of the iceberg since it is often observed that even the administrator or root accounts may have either weak or no passwords at all. Another issue that plagues system administrators is their failure to delete old user accounts. This lack of follow-through in combination with possible weak password policy is the perfect launching point for further escalation of privilege attacks later on.

The enumerating phase will also attempt to determine vital information about the types of web servers, e-mail servers, routers and other key components on the network. Banner grabbing is one technique the team may use where they query a network resource to determine what type of device it is or what type of software is running on it. If the queried item is not configured properly, it will often provide a detailed fingerprint of its internal information that can be used to search for vulnerabilities that are indicative of that particular device running that version of software. An example of this type of attack would be determining that a web server is running a specific version of either IIS or Apache software, then looking up the looking up the vulnerabilities of either on the Internet to determine what exploits to use against that server.

Gaining access to the network is a high point for the infiltration team. Nevertheless, this is where the work really begins. They will attempt to compromise and take over the system by using various forms of attacks such as password cracking programs, buffer overflow attacks, and possibly denial of service attacks. The use of denial of service attacks is unlikely to be used against the whole client organization since it will be extremely disruptive of their services. However, there is a possibility that it could be used against specific target items in the network if the senior management agrees to it. The key here for the penetration team is to have explicit details of this agreement clearly spelled out in the services contract prior to the attack. Remember, the goal of the gaining access phase is to establish a foothold into the target network so that the final phase, escalation of privileges, may be placed into effect.

Now that the Black Box team is in the network, the next phase will be to attempt to gain administrative or root level privileges on the customer's system. The goal of this phase ranges from owning a specific item on the network to complete control of it. Obviously, these goals are pre-determined by the customer and they will reflect to a large degree the size and type of the network attacked. Privilege escalation may be accomplished by using such powerful password cracking tools as L0phtcrack for Windows based systems and John the Ripper for UNIX and other platforms. It must be stated that even if the team is able to gain administrative level access on one area of the network, it does not mean that they will be able to on others. If the client does not have a uniform security policy that is in place everywhere, then it is conceivable that the there would be varying levels of security measures in place in different parts or divisions of the organization. Conversely, if the penetration team is not able to effectively penetrate their target network, this does not mean there are no vulnerabilities, it only signifies that none were found during the current testing phase.

If the organization were dealing with a real hacker, then the hacker would probably attempt to keep his/her stranglehold on the network by installing backdoors in the network. In addition, criminal attackers usually attempt to cover up their tracks by auditing and deleting various security logs on the network. These additional phases of attack may or may not be used by the hacking team, but if they are, usually it is to determine how strong of an audit trail the client network has and to see if the network security staff is following up on any audit anomalies.

The White Box Approach

The White Box approach is another attack method that may be used by the Ethical Hacker. This is a more deterministic plan of attack than the Black Box one. [26] What is meant by this is that the White Box ethical hacking team will have much more information divulged to them prior to the penetration test, so there will be fewer unknowns or variables. Since the variables are limited, the methods utilized in the attack will probably be more controlled, hence more deterministic.

The rationale behind using the White Box mode versus the Black Box mode is twofold: time and money. The ethical hacking team only has a limited amount of time in order to access the network and the longer it takes them, the more resources they will have to utilize and ultimately the more it will cost the customer. By giving the ethical hacker the information about the network and its security posture in advance, the White Box method can reduce the amount of investment required to accomplish this task significantly. However, there are those who feel that the Black Box approach is a more accurate way to access the strength of a network's defense because it illustrates how a criminal hacker might attempt to attack the network. Corsaire Limited Corporation, an information assurance corporation, feels that this is not necessarily the case. They argue that the criminal hacker may have extensive knowledge of the target organization since the hacker might have been an previous employee or because hackers have a great amount of time to gather intelligence. [5] Paul Midian agrees with Corsaire and says that since the criminal hacker has had so much time to gather information about the network, it would be wise to allow the penetration testers to have access to the internal networks' configuration. [10] While there are pros and cons to any method of penetration testing, it must be reiterated there is a time and place for each one.

Andrew T. Robinson states that the White Box model takes the approach that the penetration team functions as "trusted insiders" who have access to the complete details of the internal network. [16] This is not to say that there will not be any need of reconnaissance done against the company, rather there may be a real need to do so. As Marcia J. Wilson so aptly points out there is the distinct possibility that the customer is very unaware of the boundaries of their network. If the organization is large, then there is the likelihood that they are connected to other partners or different divisions within the same organization that have different levels of security protections and policies in place. [25] If this is in fact the case, then it would be a grave disservice to the client for the ethical hacking team to fail to explore this. In addition, it must be stated that the White Box team will use the same tools and similar methods as the Black Box team. The difference between the two approaches is more in terms of the degree of usage and the amount time needed to utilize them in the attack.

There are three main groups of personnel in the organization for the penetration team to bring into play in order to obtain the information they need for the White Box attack: upper management, technical support management and human resources working in conjunction with the legal department. Each group will provide a different expertise and viewpoint for the penetration team. Collectively employed, these three groups will provide the framework for the attack process.

Upper Management

It must be stated that everything begins with upper management. They are not only the ones who create policy, but also they are the ones who have the vision for the organization. Thus, it is extremely important that the White Box hacking team "be on the same sheet of music" with them.

If the penetration team fails to win the trust and cooperation of these individuals, then the penetration attack is doomed to failure.

Upper management should provide to the penetration team a clear understanding of the current security policies that under gird their business. If upper management has not seen fit to establish a credible security policy or if the current one is not enforced or up-to-date, then the organization has unwittingly conceded defeat to any future attacks on their network assets. With this knowledge available to the hacking team, they can strongly urge upper management to develop a plan of attack for instituting a strong security policy.

In addition to having an understanding of the security policy of an organization, the penetration specialists may also need upper management to provide insight into their overall corporate structure and their current business models. Many times a company's network structure will mirror (at least functionally) its corporate formation. This information is particularly helpful in assessing where the most sensitive and valuable network assets are located. Knowing a business' current business model is advantageous to the hacking team because it may direct them in determining where their security plans need to focus in the future.

The White Box penetration team will probably need to know something about the types of customers an organization has. Every organization and business has customers since both render either some sort of service or product to someone. Upper management will also be primary resource for this information as well. By being aware of the customer base of the client, the penetration team will know why certain administrative and regulatory constraints are in place in order to protect the privacy and integrity of the customer.

Upper management knows their competitors. The ethical hacking team needs to know them as well since competitors; vendors, and partners may occasionally decide to use unethical means to gather information about a company. Knowing what the competition is after is a good way to determine whether the business is adequately defending these targets. This forces upper management to know what assets they are seeking to protect and knowing what measures they are willing to take to defend them. Once again, the specter of perception versus reality may come into play especially if the upper management is unaware of the true value of their informational assets.

Finally, upper management will have to delineate the parameters of the attack. They must determine what is suitable for exploitation and to what extent it may be exploited. They cannot expect the ethical hackers to be able to make an assessment here, since the hackers are not really insiders in the strictest sense. In addition, upper management has a right to be made aware of just how these vulnerabilities will be tested so that they may seek the appropriate intervention should something go awry. [9] Upper management will also be responsible for notifying the appropriate personnel of the ethical hackers' agenda. It would prove to be very embarrassing to both the management and to the ethical hacking team if the organization's security forces brought law enforcement into the picture. In addition, it would be advantageous for the team if management introduced the team to key players in the organization. Knowing who to contact and who to interview for information will help expedite the process of beginning the full phased attack

.

Technical Support Management

It is obvious that one of the key players in the penetration attack will be the technical support management group. They will be the primary source of information for the team in order to enumerate and map the network. Also, technical support will be the "watchdogs" for the testing process since they may have to intervene during the testing process should the need arise.

The hacking team will enlist the help of the technical support team for several key areas:

- Physical topology and key access points to the network
- Logical topology and the protocols used on the network
- Major applications and the network operating systems
- Firewalls, Routers, Switches, IDS and other devices and their configurations
- RAS and VPN services
- Modems
- Wireless networks
- Telecommunications devices: PBXs etc.
- Intranet and extranet services
- Web and e-mail servers
- DNS and DHCP servers
- Other specialty servers
- Authentication methods
- Patch management
- Antivirus software

Hopefully, the technical support group will be conscious of possible downstream liability issues should one of the attacks result in a denial of service against some other organization. This is imperative if the company has intranet or extranet services utilized with partners or other company divisions. If in doubt, then corporate legal will have to be consulted in order to determine the extent of the corporate accountability.

One final area where the technical support management will be providing input is for the security procedures of the network. This information is essential in determining whether or not their security lists and guidelines need to be revised in light of the results of the penetration test. The client needs to know if their security countermeasures have enough thoroughness and depth so that their network administrators will be able to adjust to varying types and degrees of attack with a high level of proficiency.

Human Resources and Legal

The Human Resources department can provide useful insight about the company's organization. They are a good source for revealing decision makers and they may know the leaders who are "in the trenches". This type of knowledge is valuable to the ethical hacking team because it may help them to determine the frontline personnel who will put up roadblocks or other objections to their penetration analysis. In addition, Human Resources' understanding of the personnel roster is usually more granular than that of the upper management. Furthermore, they will be able to fill in the gaps of knowledge concerning corporate policy which should minimize the amount of personnel interviewing the attack team may have to do.

Last, but certainly not least is the legal department. They will help to insure that the hacking team doesn't "step on the wrong toes" and end up creating a legal quagmire that nobody wishes to occur. They will be involved in the contractual agreement phase prior to the commencement of any type of ethical hack, so their importance is not to be underestimated. They will be aware of any kind of network boundary sharing with other groups or organizations. This will help the ethical hacking team to avoid any areas ambiguity when it comes to the demarcation point of the network. In addition, they will be partner to the agreement of limitations of legal liability for the penetration team. Furthermore, the legal department will provide detailed regulatory and administrative information to the attack group. If an organization is bound by certain security rules and regulations, then the ethical hackers should have this knowledge so that they may determine whether the target organization is in compliance. Once the level of compliance is determined, then this information will be brought to both upper management and to the legal department for their perusal.

The Gray Box Approach

The Gray Box approach is essentially a hybrid attack model. It incorporates elements of both the Black Box and the White Box methods. Andrew T. Robinson says that there are two players in this scenario: the untrusted outsider who is working with the trusted insider to compromise the network.[16] Basically, this attack model allows for many interesting possibilities. The outsider may be in the process of initiating Black Box reconnaissance attacks while the insider is feeding important information to him or her. Now the external hacker will be able to tailor the scope of these attacks to the areas of true vulnerability.

As with any attack model, the ultimate focus and direction comes from the clients' management team. They will determine the criteria for specifying the rules of engagement and will dictate what levels of knowledge will be revealed to the hacking team. Therefore, the ethical hacking members may have to play different roles for this approach, some acting as insiders while others are acting as outsiders. This will posit some interesting problems for the team. First, the management will have to determine what sort of communications channels will be allowed between the insiders and the outsiders. If the rules of engagement presuppose that the external attackers are thousands of miles away, then it would not be appropriate for the Black Box team to get with the White Box team at the end of the day to compare notes. Second, the ethical attack team must have a contingency plan in place should it just so happen that the communication link between insider and the outsider becomes broken, (remember, there may be various scenarios acted out during the attack). The team must be ready to revert to a pure Black Box approach if this transpires. Since it may not be possible to regain insider access again, they must use any insider information previously obtained in a judicious fashion.

One possible drawback to using the Gray Box approach is one that may also be seen in the White Box approach. When resources are revealed to the attack team, there is the tendency to overlook vulnerabilities that aren't readily apparent. The attack team has the information that it is looking for, but they aren't forced to scrutinize the network, so things are overlooked. The way to avoid this issue is to ensure that the test team has a definitive methodology to their attack models. By following checklists and using established procedures, this is less likely to happen.

Conclusion

This paper addressed ethical hacking from several perspectives. First, the need for ethical hacking was proposed. Ethical Hacking is a tool, which if properly utilized, can prove useful for understanding the weaknesses of a network and how they might be exploited. Ethical Hacking is not a panacea for all network security problems, but it is a fascinating craft that can be used to bolster the Defense in-Depth principle. Each attack model had a different perspective or underlying philosophy. The Black Box model operated from the known to the unknown, using covert methods to gain access to the network. The White Box model allowed the attackers an abundance of information concerning the configuration and structure of the network. It provided a solid foundation for the hacking team to explore the customer's information assets. The Gray Box model was a hybrid between the Black Box and the Gray Box that allowed the attack team to exploit the network from two different perspectives. The outsider acted as a Black Box attacker and the insider was a White Box attacker.

In conclusion, it must be reiterated that the ethical hacker is an educator who seeks to enlighten not only the customer, but also the security industry as a whole. By thinking like the enemy, the ethical hacker is able to ferret out issues in security which others may not even be aware of. Since few will walk down the Ethical Hacker's path, we must pay attention to the nuggets of wisdom that they will present us. SUN TZU in the Art of War at http://www.kimsoft.com/polwar3.htm so aptly summed up the battle that the White Hat must fight:

> Hence the saying: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat . . . If you know neither the enemy nor yourself, you will succumb in every battle. [21]

Thus, the security community must consolidate their efforts to thwart the adversaries of our networks. In an effort to accomplish this, let us welcome the Ethical Hacker into our ranks as a partner in this quest.

References:

1. American Registry for Internet Numbers, “ARIN Whois Database Search, 22 February 2004. URL: http://www.arin.net.whois

2. Boyd, Ida Mae, “The Fundamentals of Computer Hacking”, December 2000. URL: http://www.giac.org/practical/GSEC/Ida_Boyd_GSEC.pdf

3. Chartered Accountants of Canada Information Technology Committee, “Using Hacking Techniques to Access Information Security Risk”, principle authors: Baker, Gary and Tang, Simm, June 2003. URL: http:/www.cica.ca/multimedia/Download_Library/Standards/Studies/English/ITAC_-_ethical_hacking -_e.pdf

4. Coffin, Bill, “It Takes a Thief: Ethical Hackers Test Your Defenses”, Risk Management Magazine, 1 July 2003. URL: http://www.ins.com/Downloads/publications/risk_management_0703cover.pdf

5. Corsair Limited, “Penetration Testing Guide”, 2003. URL: http://www penetration-testing.com

6. Dworakowski, Wojciech, “Why a firewall alone is not enough? What Are IDSes and why are they worth having?” 22 August 2002. URL: http://windowsecurity.com/articles/Why_is_a_firewall_alone_not_enough_What_are_IDSes_and_why_ are_they_worth_having.html

7. Farmer, Dan and Venema, Wietse, “Improving the Security of Your Site by Breaking into It”, 1993. http://www.fish.com/security/admin-guide-to-cracking.html

8. Gula, Ron, “Broadening the Scope of Penetration Testing Techniques: The Top 14 Things Your Ethical Hackers-for-Hire Didn’t Test”, copyright 2001, Enterasys Networks Inc, paper originally Published in 1999 prior to the acquisition of Network Security Wizards By Enterasys Networks. URL: http://www.enterasys.com/products/Whitepapers/security/9012542.pdf

9. Herzog, Peter Vincent, “OSSTMM 2.1. Open-Source Security Testing Methodology Manual”, 23 August 2003. URL: http://isecon.securnetltd.com/OSSTMM.en.2.1.pdf

10. Midian, Peter, “Penetration Testing”, February 2004, URL: http://www insight.co.uk/downloads/whitepapers/Penetration%20Testing%20(White%20Paper).pdf

11. Midian, Peter, “Perspectives on Penetration Testing – Black Box vs. White Box, First published in Elsevier Network Security 13 November 2002. URL: http://www.insight.co.uk/downloads/presscoverage/Black%20Box%20versus%20White%20Box%20(Network%20Security).pdf

12. Najmi, “How Hackers/Crackers Break Into Your System?” 13 May 2002. URL: http://techniwarehouse.com/Articles/2002-05-13.html

13. Public Broadcasting Service, “computer attacks at department of defense pose increasing risks” May 1996, US General Accounting Office, GAO/AIMD -96-84 Defense Information Security 1996. URL: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/risks/dodattacks.html

14. PC Flank Website, “Quick reference to Windows Ports”, February 2004. URL: http://www.pcflank.com

15 Redsiren Inc, “Education Marketing Services” February 2004. URL: http://www.redsiren.com/education.htm

16. Robinson, Andrew T. “Validating Your Security Plan Using Penetration Testing: An Executive Summary”, February 2004. URL: http://www.nmi.net/pages/pentest.html

17. Ruckman, Sharon, “Blended Threats: New Recipes for IT Disaster”, 2 December 2003, interview with Ziff Davis Channel Zone writer Joel Shore. URL: http://www.channelzone.ziffdavis.com/article2/0,3973,1401426,00.asp

18. Serafini, Gabriel CISSP, “An Introduction to Ethical Hacking” February 2004. URL: http://www.midwesttechjournal.com/modules/.php?name=news&file=article&sid=172

19. Smetannikov, Max, “If Firewalls are Folly, Are Homegrown Hackers the Answer?”, June 2003. URL: http://www.webhostingmonthly.thewhir.com/archives/june2003.pdf

20. Srikanth RP, “Should Ethical Hacking Be Taught as a Career Course?” 22 April 2002. URL: http://www.expressitpeople.com/20020422/cover1.shtml

21. Sun Tzu, The Art of War, translated by Lionel Giles, first published in 1910 as part of the Project Gutenberg. URL: http://www.kimsoft.com/polwar3.htm

22. Webopedia.com, “Hacker”, a definition, February 2004. URL: http://www.webopedia.com/TERM/h/hacker.html

23. Webopedia.com, “Script Kiddie”, a definition, February 2004. URL: www.webopedia.com/TERM/s/script_kiddie

24. Webopedia.com, “Vulnerability Scanning” a definition, February 2004, URL: http://www.webopedia.com/TERM/v/vulnerability_scanning

25. Wilson, Marcia J. CISSP, “Demonstrating ROI for Penetration Testing (Part Four), 7 October 2003. URL: http://www.securityfocus.com/infocus/1736

26. Zak, M and Park H. “The Gray Box Approach to Sensor Data Analysis”, 15 February 2001. URL: http://tmo.jpl.nasa.gov/tmo/progress_report/42-144/144B.pdf

Note: All URL listings have been verified as being active as of February 22, 2004