

Ethical Hacking

From start to success

By Rob Kraus – ISSA member, Alamo (San Antonio), USA Chapter

Ethical hacking services provide a unique solution to help IT practitioners secure their networks and other assets before malicious attackers gain a foothold on the secrets of the organization.

Ethical hacking is nothing new. The term has been used in the information security world and accepted by the security community for quite some time. Even though many have an understanding of the practical application of ethical hacking, organizations still fail to apply remediation recommendations based on assessment outcomes. This article does not identify innovative methods to put a new spin on an old concept, but instead focuses on where organizations fail to ensure success. For this reason, pre- and post-ethical hacking engagement activities are discussed rather than specific attacks or vendor selection criteria. Before exploring what organizations can do to maximize the ROI, consider the basic elements of ethical hacking and security principles.

Traditional ethical hacking

Let's face it, ethical hacking services are a part of the information security community and serve many purposes. In its most generic form, ethical hacking allows organizations to make use of professionals talented in the "black arts" of hacking and vulnerability identification. An ethical hacking engagement can be outsourced to a third party or can be conducted by an established internal team.

Ethical hacking engagements may include social engineering, wireless penetration testing, Web application reviews, and other consulting services in addition to the commonly associated external and internal penetration tests. The goal is to identify vulnerabilities in organizational

information technology (IT) assets and non-IT related assets. Of course, overlap is possible in some cases, and those instances should be addressed as necessary. Physical security and organizational practices, policies, and procedures must be addressed for a complete approach.

Management acceptance

As a general foundation for ethical hacking and other security-related initiatives, recall the most elemental of requirements: management acceptance and support. No security plan is guaranteed success. Additionally, no security plan lacking management support will succeed. Sometimes the most difficult part of embarking on a successful ethical hacking engagement is conveying to executive management the importance of the engagement in the overall security program.

This point may be common sense to most, but common sense is not always common. Ethical hacking should be a means to identify weaknesses in an organization's security posture. However, as a practitioner, I find a large number of organizations use ethical hacking engagements to measure the organization's implemented controls against Health Insurance Portability and Accountability Act (HIPAA),¹ Sarbanes-Oxley Act (SOX),² or Payment

1 <http://www.hhs.gov/ocr/privacy/index.html>.

2 http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf.

Card Industry (PCI)³ compliance directives, or simply to check-the-box. True management buy-in means supporting the assessment because the organization wants to be secure in addition to being compliant.

Getting back to basics

A “holistic approach” to security has been recommended by security practitioners for some time. Unfortunately, marketing and sales professionals may use this word in a different context than intended. In the eyes of the security professional, a holistic approach implies a comprehensive analysis of critical assets having a high risk that vulnerabilities may be leveraged or having an increased potential of loss. To the buzzword-enabled salesperson, it may sound like “holistic” means “kitchen sink.”

Rather than using holistic terminology, address organizational needs by evaluating existing controls against “best practices.” Following best practices means implementing controls and taking the course of a “prudent man.” A biblical reference to a prudent man states, “*A prudent man seeth the evil, and hideth himself; But the simple pass on, and suffer for it.*”⁴ In short, do not accept the deal of the week. Take a hard look at what is important, assess the risk, and engage in assessment activities that apply to your organization.

Defining a scope

One of the most important decisions an organization can make when preparing for ethical hacking engagements is to first conduct a risk assessment. Risk assessments allow organizations to review threat scenarios and quantify risks to which the organization may be vulnerable. Third-party risk assessments can prove to be valuable by allowing organizations to benefit from an experienced facilitator. If the organization has an internal risk assessment team, it may be a good idea to have a third party review prior assessment results, assist with verification, and aid in further risk identification.

Ensure a consistent and clear risk assessment methodology is followed. As an example, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®)⁵ methodology and tools provide a flexible approach to risk assessments. This methodology is currently maintained by the Software Engineering Institute at Carnegie Mellon University.

Once an initial risk assessment has been performed and the organization has an opportunity to review the risks, a plan should be developed to verify if vulnerabilities exist that can be leveraged to turn a risk into a reality. Where ethical hacking is concerned, a risk assessment provides the organization an educated view of required assessment services and extraneous services that may be draining the budget but providing little ROI. The organization may not require all the services

an ethical hacking provider offers. To put things into perspective, do not buy the buffet when à la carte will suffice. Use the risk assessment as a tool to save your organization money when deciding what services to purchase.

Thrifty...not cheap

Making the right choices can save the organization money, but be careful not to shortcut the quality and scope of the service. As ethical hacking services are selected and the scope is defined for the rules of engagement, consider the limitations your organization imposes on the services. Corporations today expect ethical hacking engagements to be quick, accurate, and cheap. These are basic requirements with which almost any project manager will agree. Facilitators should have a good idea of how the command and control of the engagements are handled but ensure it *does not hinder the ethical hackers from executing real world attack scenarios*. Most ethical hacking service providers understand project goals and are flexible to make clients happy.

Malicious attackers have a major advantage over typical business culture when it comes to time, planning, and execution of attacks. A well-planned attack can cause havoc for even the largest of corporations. For this reason, proper funding should be secured to ensure the assessments conducted resemble authentic attack scenarios.

Variety is important

Organizations should embrace the knowledge ethical hackers have and entertain different attack scenarios where possible. Avoid conducting the same scenarios repeatedly as it provides a false sense of security. For instance, if your organization determines it has a high risk of falling victim to social engineering attacks, a variety of attack types should be used during ethical hacking exercises.

I have found that diversity during assessments helps organizations prepare for a variety of attack types rather than a single threat. Most organizations I have engaged were very comfortable about not falling for phone-based social engineering attacks, but after a little variety was introduced, the comfort level had dropped. Experience has shown that most employees will be more skeptical when asked to provide a password over the phone, but when an official phishing email is used in conjunction with the phone-based attack, the ethical hacking team often has a higher level of success with obtaining user credentials. These threats need to be tested to validate the actual exposure to the organization and how training employees in proper email and password policies can really help. The variety will also promote employee awareness and help employees identify activities that may seem out of the norm.

Making it legal...and safe

Legal binding contracts should identify the terms of the delivery and execution of services provided to ensure service details are clearly understood by all parties involved. Contracts apply to not only the direct relationship between the

3 <https://www.pcisecuritystandards.org>.

4 *American Standard Version*, Proverbs 22:3. <http://asvbible.com/proverbs/22.htm>.

5 <http://www.cert.org/octave>.

organization and the vendor but also any third-party consultants enlisted by the vendor to assist with the delivery of services. Qualified legal council should review contracts to ensure the interests of the organization are protected.

Although I discussed the importance of real world attacks, it is equally important to ensure the organization is not jeopardizing existing client service level agreements (SLAs). Interruption of services to legitimate customers during engagements is always a possibility that should be taken into consideration. Although the intent of ethical hacking is not to disrupt service, the nature of the testing always provides that risk. Most vendors understand this and will be willing to accommodate testing during off-peak production times. As mentioned previously, organizations should ensure these types of details and options are addressed in formal contracts.

Results and remediation

After organizations have identified risks, enlisted services, and digested the results of ethical hacking activities, remediation efforts must be planned and engaged. The results of ethical hacking assessments may be one of the first ROIs for an organization's investment in security. However, a word of caution: the results may not always be as attractive as anticipated. The skilled professionals who perform ethical hacking services are usually highly trained and want to show you the value of their services as well as ensure you receive a good ROI. Good or bad, the results of ethical hacking engagements are an important part of verifying the risks discussed earlier.

Comprehensive reporting and results

Depending on report formats and the skill level of the individual responsible for reviewing the assessment results, understanding the results can be confusing. Report delivery and format should be discussed with the vendor prior to finalizing service contracts to ensure it will provide the appropriate level of detail. This detail will help your organization identify the root cause of the issues and help define possible remediation paths. At a minimum, organizations should be aware of the following:

- The report generation and delivery time line
- The report format (CSV, PDF, Microsoft Word, Web-based)
- If remediation recommendations are available for identified vulnerabilities
- The report retention policies of the provider to ensure reports are available in the future if needed

Take immediate action

Many organizations fail due to the lack of planning for remediation efforts, and misunderstanding of how to address the identified issues with proper, industry-recommended solutions. One of the worst things an organization can do is to conduct a risk assessment, identify required ethical hacking services, select a vendor, conduct the assessment, and then

Qualified legal council should review contracts to ensure the interests of the organization are protected.

read the report without taking action. However, many organizations do just that, stuffing the final assessment reports in between policy manuals to collect dust.

Having conducted hundreds of exit briefings, I have experienced situations where C-level executives can become angry after learning no remediation efforts have taken place since the previous assessments. It makes it a bad day for those who are responsible for remediation, and it makes it hard to convince executives that the appropriate budget for future assessments is important.

Time is a commodity many organizations are short on; the lack of time allocated to perform remediation tasks and poor time management are significant contributors to the failure of the remediation process. In modern business, the drive to become the leader in the market and push products to customers in the most efficient manner possible is often the overriding goal. Something important to remember is vulnerabilities do not sleep, do not have deadlines, and could care less about market share. In many cases, vulnerabilities can be remediated by providing the appropriate resources with the time required to execute a well-thought-out remediation plan.

Sometimes it can be a tough decision to make for organizations that need to protect assets and deliver products while maintaining a competitive advantage. Making decisions based on gaining competitive advantage can cause organizations to neglect security initiatives. As mentioned earlier, it is vital to the success of any security initiative to have upper management support and ensure that the delicate balance between functionality and security is maintained.

In many cases, I discover IT and security administrators are at a disadvantage when answering to upper management and board members, especially when security evaluations do not provide positive findings. Ultimately, the finger is pointed at IT and security administrators for not doing the job. However, in some cases, the friction between administrators and management may be due to lack of understanding, funding issues, or lack of resources being properly allocated to ensure a properly secured organization. Take a moment to review the concept of ownership and maintenance roles within an organization and how those roles may contribute to the overall information security program.

Data Ownership

One common misconception is that the data stored within the organization is owned by the IT department. To the layman the rational may sound similar to "Of course, they perform backups and ensure availability, so that must be the correct answer." This actually cannot be further from the truth.

Data belongs to “data owners,” and the data maintenance functions belong to “data custodians.”

Data owners may include the frontline manager all the way up to the CEO. A data owner is an individual or group responsible for the identification and protection of a data set. This includes deciding who is granted appropriate access, determining sensitivity classification, and the frequency of backing up the data. Additionally, the data owner is responsible for the due care of the data and will be held accountable for any loss of integrity and confidentiality.

| Data Owner | Data Custodian |
|------------------------------|-----------------------------------|
| Disclosure approvals | Integrity verification |
| Violation investigations | Data backup |
| Data classification | Restoring data |
| Define security requirements | Enforcing standards of protection |

A data custodian is responsible for the care and feeding of the data that needs to be protected. This includes your IT and security administrators who will perform integrity tests, backups, test restores, and implement technologies to help ensure the overall availability of the data.

The roles of owner and custodian responsibilities can indeed overlap in some cases. However, the data owner is the one who ultimately has to answer for mishaps and losses. The distinction is important, as it can often be a struggle to remember the overall goal of ensuring confidentiality, integrity, and availability of data.

The strong finish

Maintaining a secure environment is one of the most difficult organizational challenges. A delicate balance exists between costs, functionality, and prudence in security decisions. Sometimes it may be difficult to identify the appropriate level of security simply because as technology advances, so do the attack vectors. No organization can be prepared for one hundred percent of the possibilities *and* stay vigilant. The common administrator is focused primarily on the availability of services and ensuring SLAs are met. Even organizations with dedicated staff responsible for security cannot keep up with the vulnerabilities published on a daily basis.

Planning for success

Much of this article has discussed concepts important to understand when attempting to maximize an ethical hacking engagement. As security practitioners the goal is to ensure a plan is in place, appropriate parties are included in the process, and execution yields results your organization can use.

It is important to remember plans change! As you travel down the road of outlining your ethical hacking engagement, do not be surprised if you find the path taking you in an unexpected direction. During engagements high-level vulnerabilities may be identified, requiring immediate remediation. The severity of the vulnerabilities may warrant halting as-

essment activities. While the organization may experience a slight delay to the progress of the engagement, it may be better to take the immediate action rather than allowing the vulnerability to remain. Flexibility needs to be considered while ensuring the core goals of the project are not compromised.

Peer support

Over the last ten years, there has been tremendous growth in the security community. Conferences and training are excellent places to meet peers, discuss security, and share experiences. Some of the greatest things I have learned about ethical hacking engagements have come from listening to the success and failure of others' experiences. Ensure your IT and security administrators have the opportunity to attend these priceless events. Organizations such as the ISSA provide access to many resources through publications and local chapters.

Security ambassadors

Trick Question: Who is responsible for the security of your organization? Answer: **Everyone**. Security is not a one-man or one-woman show. It takes effort for any security program to be successful, and this alone is a large burden to carry without help. Empowering the organization's employees at all levels increases the overall success of the program.

In the past, I have advised organizations to implement a “security ambassador program,”⁶ which makes it fun for employees to engage in thinking and acting securely. Simple security awareness programs can have a significant impact on the overall security. Implement awareness and be open with your employees about ways they can help protect the organization.

Conclusion

Preparing your organization for an ethical hacking engagement and trying to maximize its effectiveness can be a challenge. Ensuring proper planning is in place for both pre- and post-engagement activities can be the ultimate test of maximizing your ROI. Ensuring the proper support channels are in place will help guide your organization to success. Use your resources and do not be afraid to ask questions of your peers, vendors, and stakeholders. Lastly, security is dynamic, be flexible.

About the Author

Rob Kraus of Digital Defense, Inc. conducts internal and external penetration tests and social engineering engagements. He serves as the program director for the ISSA Alamo (San Antonio) Chapter and is a regular presenter at TRISC. You can contact Rob at rob.kraus@ddifrontline.com.



⁶ A security ambassador is how I refer to the individuals who are regular employees, but have the capability of helping ensure security practices are being followed. Think of them as the equivalent to your local community safety watch programs found in many residential neighborhoods today.