SANS PENETRATION TESTING

Use offense to inform defense.
Find flaws before the bad guys do.

Copyright SANS Institute
Author Retains Full Rights

This paper is from the SANS Penetration Testing site. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Techniques, Exploits & Incident Handling (SEC504)"
at https://pen-testing.sans.org/events/

Penetration Testing in the Financial Services Industry

GIAC (GPEN) Gold Certification

Author: Christopher Olson, cgolson@gmail.com
Advisor: Aman Hardikar

Accepted:

Abstract

The financial services industry has unique information security requirements. Frequently the target of attacks, banks have to perform a higher level of due diligence to ensure the confidentiality, integrity and availability of customer transactions. Penetration testing is one way to stress the attack surface that an organization presents to the outside world. The paper will propose a method by which senior management of financial organizations can prioritize a penetration test. By starting with a comprehensive vulnerability assessment it is possible to identify possible targets that may appeal to an attacker. Given that most financial institutions engage in some form of outsourcing we will also address whether it is better to source the test internally or to outsource.

© 2010 SANS Institute, Author retains full rights.

1. Introduction

The financial services industry is under attack from numerous and significant cybercriminal threats. Recent breach data numbers reveal that hackers have successfully compromised many financial institutions with the trend being that more records containing personally identifiable information (PII) are being stolen each year. In many cases where systems were breached the method of compromise was attributed to simple errors that gave rise to significant vulnerability. Given the ever present competitive pressure and the current economic strain to operate more efficiently banks are allocating resources with added care and may miss the opportunity to rally and mitigate existing deficiencies in basic operational and process controls. In lieu of allocating resources to implement appropriate preventative controls, penetration testing is one alternative detective control that can highlight areas of risk created when overburdened system administrators inadvertently create vulnerabilities.

When penetration testing is used in this manner the scope of the test must be carefully and clearly articulated. Before any work begins the scope may need to be narrowed to include a subset of business units or specific technology targets. For example, a business unit that has network connections to business partners may be given first priority, with the scope including a test of all Web applications, wired and wireless networks within that line of business. This paper will review the potential options by which an organization can execute penetration testing to identify vulnerabilities. There are three options: in-sourcing, out-sourcing and a hybrid approach by which a financial institution may develop some skills in-house and outsource those that require specialized skills.

2. General Considerations for Penetration Testing

Financial institutions must meet regulatory requirements, and this is frequently the driver for contracting a penetration test. Regardless of which organization does the penetration testing, there are some global issues that should be considered.

Author Name, email@address

© 2010 SANS Institute, Author retains full rights.

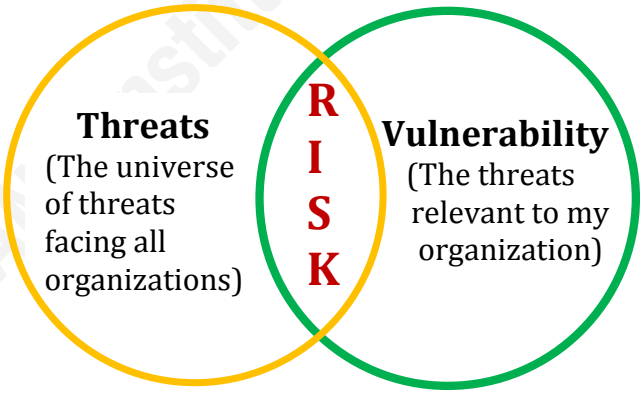
2.1. Penetration Testing Defined

Penetration testing is focused on finding security vulnerabilities in a target environment that could let an attacker penetrate the network or computer systems (Skoudis, 2008). The goal of penetration testing is to actually compromise a target system and ultimately steal information. This typically requires tools and techniques very similar to those that an attacker would use.

As a practical consideration the penetration test should not be done if the organization does not have the funds to remediate the findings. An iterative cycle of monitoring and testing should follow the remediation to ensure that changes to the information technology, business environment, or threat landscape do not introduce further vulnerability. A periodic vulnerability assessment is required to detect deviations from the security baseline.

2.2. Vulnerability Assessment

The financial institution should have the ability to assess the vulnerabilities associated with their infrastructure (what hardware and software they own and maintain) and network architecture (how that hardware and software is arranged to affect data transmission).



The diagram is useful to provide a visual perspective of how the assets in the financial institution are linked to risk. The left circle represents the universe of threats facing the organization. For example, on any given day a number of new threats are identified by research organizations that collect vulnerability information; e.g. the Mitre organization (http://www.mitre.org/cve) and there are many others. The right circle

© 2010 The SANS Institute Author retains full rights.

represents the vulnerabilities that have to be managed by virtue of the financial institution's infrastructure and network architecture configuration. There may only be a fraction of threats in the universe that present risk to the organization—as depicted by the intersection in this Venn diagram—and this is the set of threats in the local universe that we must manage.

Penetration testing should identify vulnerabilities that arise from improper configuration and patch management processes. This is not an indictment that corporations cannot manage their infrastructure, but a testament to the reality that attackers only need to be right one time to exploit a vulnerability, whereas the IT organization needs to be right 100% percent of the time when managing vulnerabilities. Penetration testing is a tool in the vulnerability management arsenal that helps bridge the gap between human fallibility and the need to be right 100% percent of the time.

Most organizations are managing the risk to the enterprise—that is the intersection between threats and vulnerabilities—with some level of proficiency. The organization with a mature vulnerability management process will significantly reduce the need for penetration testing. Unfortunately, a mature vulnerability management process does not eliminate the need for penetration testing. If fact, most organizations that have highly effective vulnerability management programs are likely to be the targets of hacker attention. However, regardless of the size of the financial institution or maturity of the vulnerability management program, penetration testing is required to reduce the residual risk.

To make the most of a penetration test it is necessary to prioritize the engagement. There are six major areas to which penetration testing applies: (i.) the network is typically scanned to identify the network addresses of all target hosts (firewalls, servers, routers, essentially all live devices) connected to the network. Vulnerability scanning precedes the penetration test and will determine the network topology of the target environment, type of operating systems discovered, open ports and services, and list of potential vulnerabilities. (ii.) The network perimeter devices like the border router are continually scanned by attackers looking to exploit a new vulnerability. (iii.) Wireless devices also present a potential entry point. Penetration testing will reveal any configuration or

Author Name, email@address

© 2010 The SANS Institute Author retains full rights.

implementation errors. (iv.) Web-based applications should be penetration tested as they represent a high risk attack surface that attackers are continuously probing. (v.) Commercial-Off-The-Shelf (COTS) software should also be penetration tested as this represents a risk of exploit by insiders. (vi.) In-house developed applications should be tested as they can also provide an entry point for an attacker. All six of these areas must be considered within scope for the penetration test.

The following table depicts an example set of applications by platform and is included to represent one possible means by which penetration testing can be prioritized.

Platform	OS	Version	Example Applications						Risk Rating	Vuln. Status	Vuln. Rating	Pen-Test Priority
			e-Mail	*Wireless*	*VoIP*	*G/L*	*Citrix*	*SSH*				
Unix/Linux	AIX	5.6						yes	4	patched 13-02-10	2	**8**
	SuSE	5.5				yes		yes	5	patched 06-27-09	4	**20**
Midrange	iSeries	v6r1				yes			3	patched 06-27-09	4	**12**
	iSeries	v5r4				yes			3	patched 13-02-10	3	**9**
Mainframe	OS/390	R6				yes			2	patched 13-02-10	3	**6**
	z/OS	V1.9				yes			2	patched 13-02-10	3	**6**
Windows	Win 2008		yes		yes				4	patched 13-02-10	2	**8**
	Win 7						yes		3	patched 13-02-10	2	**6**
Network	IOS	12.4		yes				yes	3	patched 13-02-10	3	**9**
	IOS	12.3			yes			yes	4	patched 06-20-09	4	**16**

In its simplest form this is a way of identifying the universe of threats facing the organization by enumerating all software and hardware that can be exploited by an attacker. The risk rating is a qualitative assessment of risk based on knowledge of the environment. For example, the SuSE version of the ***ssh*** application may have more vulnerabilities than the AIX version, so we assign it a value of five (5)—the highest rating given this one to five scale, one being least, five being greatest. Similarly the vulnerability rating is a qualitative assessment of vulnerability given that we may have

© 2010 The SANS Institute Author retains full rights.

mitigated the weakness by applying the vendors latest recommended patches. The penetration testing score is then the product of the risk rating and vulnerability rating columns.

The column for "vulnerability status" contains a description to provide context about the vulnerability. This is helpful when trying to assign a numerical score to a subjective parameter. Ideally the values for the risk rating and the vulnerability rating should be quantified using a scoring approach. It is left to the reader to adopt a framework by which to assign the impact of a given hardware and software combination. One possible framework is the Common Vulnerability Scoring System, which at the time of this paper is version 2.0 (http://www.first.org/cvss/cvss-guide.html). An organization with few IT resources may rely on a qualitative prioritization as shown here, whereas an organization with a complex set of hardware and software may need to quantify the vulnerability assessment in a more rigorous manner. The important take away is that some process for reviewing vulnerability should be adopted so that penetration testing can be appropriately prioritized. With targeted results from a penetration test in hand, it is possible to focus remediation efforts on the highest priority risks.

Note that the table does not include databases or applications as these warrant special consideration. Databases are the logical repository for all corporate information and as such they are the ultimate destination for attackers. Applications are the source of data for databases and are also subject to attack. We can divide applications into two categories: (1.) Web-based banking applications; and, (2.) internal banking applications.

The premise of building security into software applications started taking hold in 2000. Static and dynamic testing tools were adopted as a part of the software development life-cycle (SDLC), and genuine consideration was given to include security into the SDLC (McGraw, Pohlmann, Reimer, & Schneider, 2009). Prior to this epiphany, however, corporations realized that fixing the code was hard. This gave rise to putting security layers around applications and databases. Web application firewalls, network segmentation and other means have always been a cheaper mitigation that fixing the code. The problem is that poor coding practices have lead to vulnerabilities that continue to be exploited by attackers because they provide a means of bypassing the current

© 2010 The SANS Institute Author retains full rights.

mitigations—like Web-application firewalls—and allow direct access to databases, privilege escalation, access to memory, or other means that can be used to gain entry.

Current threats in 2010 include the Zeus Trojan Botnet. This malicious software has the ability to bypass many conventional security controls. Once a client PC inside the organization is infected an attacker can pivot and compromise other hosts. Penetration testing is one means to discover the latest threats.

2.2.1. Web-based Banking Applications

Web-based applications should be coded using secure coding practices and should be tested using automated code scanners that can identify vulnerabilities. There are a number of vendors that provide automated web-application testing suites, as characterized by the growing maturity and functionality of tools in this space. Also, to compliment the efficiency of automated scanners, manual code review of high risk Web based banking applications is a necessity. Automated scanners should be used to test code in the development phase, manual code review and penetration testing should be done before deployment.

The strength of automated scanners is their ability to identify simple coding errors. Human code review is the only way to find complex coding errors. Testing and eliminating vulnerabilities brought about by poor coding will significantly reduce the risk, but there will always be some level of residual risk. The only way to reduce residual risk is to perform penetration testing of the Web-based banking application to first find and then fix the vulnerability.

A zero-day exploit requires special consideration, for which the financial institution should have access to reliable information from peers or law enforcement agencies that can provide tips to manage and mitigate associated risk. It is also important for the financial organization to have an incident response plan to handle those contingencies where an attacker does bypass controls and compromise the organization.

Just as developing a zero-day exploit is valuable in the hacker community, so too is protecting and minimizing the impact of a zero-day exploit essential to the financial organization. However, timing is of the essence in protecting from zero-day exploits.

Author Name, email@address

© 2010 The SANS Institute Author retains full rights.

Penetration testing is not a strategy to protect against zero-day vulnerabilities. In this context it is more effective to obtain the latest signatures and then tune monitoring devices to shun malicious traffic.

2.2.2. Internal Banking Applications

Internal banking applications can be compromised in the same fashion as Web-base banking applications. Secure coding practices, application testing and the use of strong authentication mechanisms are methods to minimize the risk of running internal banking applications. In this case we also have to consider enforcing segregation of duties as a vital control necessary to protect the financial institution.

Not all of the flaws found in software will be related to security, but attackers will continue to stress test applications looking for that chink in the armor. Until bug-free applications—both Web-based and internal—can can be developed consistently, there will continue to be a need to engage penetration testing of code.

2.3. Core Processing

Core processing is a financial industry term used to represent those applications that are essential to the business. These applications are fundamental to operations, like a general ledger application that keeps a record of all financial transactions within an entity. There are many technology service providers (TSPs) that offer a general ledger and other applications as a service to banks. These software-as-a-service (SaaS) offerings are tested by the vendors, but the financial institution does not know the extent of diligence in this testing.

If core processing is done by an external entity in a true SaaS configuration, then the client should request an attestation indicating that the application has been penetration tested. This will become more relevant as TSPs move parts of their processing into both private and public clouds where the attack surface may be dramatically different.

If the financial institution is running a commercial-off-the-shelf (COTS) general ledger application in-house it is worthwhile to run a penetration test against the application to test that the code is not vulnerable. Outsourcing the penetration testing of COTS applications and hardware for vulnerabilities is generally more productive as an

© 2010 The SANS Institute Author retains full rights.

experienced penetration testing team will have more exposure to the breadth of this type of software. A third-party will also be more familiar with any potential vulnerabilities associated with hardware, which should also be considered part of the testing scope when appropriate.

Attackers are targeting weaknesses in the application layer so it is important to mitigate this risk for both COTS and in-house developed code. Unlike security functional testing, which demonstrates that software behaves per the product's advertised security controls, penetration testing is a form of stress testing which demonstrates flaws that could be exploited by an attacker. Penetration testing is the only way to unequivocally identify application vulnerabilities that can be exploited by the stress that an attacker creates. Fewer application vulnerabilities will likely exist in a mature organization, however all organizations will need to consider the following questions to mitigate the risk associated with running applications that have not been fully stress tested for vulnerabilities:

- Are the version control and configuration management policies consistent throughout the organization for all applications?
- How is the configuration management policy enforced?
- Are third party developers contractually required to follow these policies and procedures?
- Are test reports available under a non-disclosure agreement?
- Have all applications undergone penetration testing?
- How have the findings been mitigated?

Special consideration must be given to running penetration tests of core processing systems. As these applications are typically mission-critical, testing should be conducted in a non-production environment that closely mirrors production. If the decision is made to test production systems it is crucial to set guidelines—regarding which services are tested and the technical means employed—in the rules of engagement. Planning the test in this manner will require more effort, but it will provide the peace of mind that live systems will not be impacted.

Author Name, email@address

© 2010 SANS Institute, Author retains full rights.

© 2010 The SANS Institute Author retains full rights.

If core processing is outsourced, the financial institution will want to ensure that the TSP is exercising appropriate due diligence and provide an attestation that professional penetration testing is done with a specified frequency. Reports from third-party penetration tests of TSPs should be made available to all clients.

2.4. Development Environments

Penetration testing during the Software Development Life Cycle should focus on separation of duties to ensure that developers do not have access to production data. In lieu of penetration testing, configuration reviews, architectural reviews, interviews and audits are appropriate in this environment. Network monitoring could be adopted to identify PII traversing a development network. The testing organization could attest that no PII is traversing the development network and thus ensure that no real customer data is being used in the test environment.

2.5. Virtualization

Virtual environments should be given special consideration given that many financial institutions have adopted virtualization without regard for control integration. This is partially due to the fact that vendors use virtual machine point solutions to mimic firewall, anti-virus, and IDPS functionality that are present in the physical data center. In some cases these virtual machines (VMs) may be deployed without regard to centralized logging or other security controls may be bypassed because of the ease of VM creation.

Penetration testing of virtual environments should be treated the same as physical data centers. Scope should be set by the risk assessment and asset inventory, priority should be given to remediation of high-risk systems and applications, and monitoring and testing should be done to ensure systems stay secure. Various financial industry regulations will dictate the frequency with which penetration testing should be done and these are being updated to address the use of virtualization.

2.6. Frequency and Reporting

Testing is costly, so companies may perform a thorough penetration test once a year and then rotate between other firms for the remaining quarters of the year. This allows the hiring financial institution to compare results between vendors, and to confirm

© 2010 The SANS Institute Author retains full rights.

previous results by doing a retest to ensure that new faults have not been introduced or uncovered as a result of changes to the environment. All penetration testing artifacts should be stored securely and encrypted, including hard-copies that should be shredded after a period of time. Hard copies are helpful when making comparisons from quarter to quarter when regression testing is done.

3. Regulatory Drivers for Penetration Testing

Various regulatory bodies require penetration testing. Network Frontiers, LLC, has created the Unified Compliance Framework (UCF), which is a Web-based spread-sheet to identify all regulatory guidance by topic. By using the UCF, it is possible to identify all regulation that contains a reference to penetration testing. Controls are organized by UCF identifier, and in the case of penetration testing the control id is 00654. This can be cross referenced by searching the Unified Controls Framework Web-site at the URL: http://www.unifiedcompliance.com/matrices/live/00655.html.

Financial regulatory documents that include a reference to penetration testing include the following:

- FFIEC IT Examination Handbook, Pg. 89, Exam Tier II Obj M.12
- PCI DSS Security Scanning Procedures, v1.1

The Unified Compliance framework contains the following general reference to penetration testing (UnifiedCompliance, 2010):

"The organization will perform penetration testing on all defined major, general support, and key minor application systems at least yearly or after any material changes."

There is also specific industry guidance. For example, the Payment Card Industry Data Security Standard contains the following reference to penetration testing (PCI, 2008):

"Once the threats and vulnerabilities have been evaluated, design the testing to address the risks identified throughout the environment. The penetration test should be appropriate for the complexity and size of an organization".

© 2010 The SANS Institute Author retains full rights.

Another section of the Payment Card Industry standard references that the goal of the penetration test is to gain access (PCI, 2008):
"The goal of penetration testing is to determine if unauthorized access to key systems and files can be achieved."

The Information Systems Audit and Control Association (ISACA) also provide guidance on penetration testing (ISACA, 2004). ISACA acknowledges the continual refinement of attacker methods and cites that tools should be adapted to the environment being tested:
"Since methods used for unauthorized access vary greatly and are becoming more sophisticated, the procedures defined are general in nature and should be supplemented, whenever possible, with techniques and tools specific to the environment(s) under examination."

The continually evolving threat landscape brought about by ever increasing complexity of attack techniques underscores the need for the financial services industry to continually monitor and manage vulnerabilities. The PCI guidance on penetration testing also suggests that penetration testing will differ based on size and complexity of an organization. All of the available regulatory guidance indicates that penetration testing is necessary to determine whether identified vulnerabilities pose a genuine risk to the organization.

4. Sourcing the Penetration Test

Penetration testing requires specialized skills. If the financial institution is outsourcing vulnerability assessments then it should consider outsourcing of penetration testing as these skills are likely not available in-house. Furthermore, even if some technical staff members are familiar with penetration testing, it is unlikely that they will have the experience that a seasoned penetration testing firm can bring to the table. Good penetration testing skills consist of more than running a vulnerability scanner against a defined set of targets. The best penetration testing companies have experience gained over a number of client engagements that involve unique hardware and software configurations.

© 2010 The SANS Institute Author retains full rights.

4.1. Scope

Before the organization can determine whether to in-source or outsource a penetration test, the scope should be defined. Ideally this will be done collaboratively by working with all business units to identify a comprehensive list of hardware and software assets. There are many tools that can be used to generate an inventory, and although this takes more time it will result in better value for the organization. The table in section 2.2 is an example of one result.

Scope should be carefully defined to specify which networks, devices and services should be included to avoid scope creep. There are cases when the tools used might find a vulnerability on an out-of-scope system, and this fact should be included in the report. Regardless of how the financial institution identifies all assets, this exercise should obviate whether the penetration test should be in-sourced or outsourced.

4.2. In-Sourcing the Penetration Test

Finding and exploiting flaws in an actual penetration test often offers more real-world proof of the need for action than other methods of vulnerability discovery (Skoudis, 2008). The problem is that finding and exploiting flaws is not something that in-house technical staff may be capable of. The most valued intellectual property that a penetration testing company has is expertise and effective exploits. This is precisely why it is very difficult for in-house staff to successfully complete penetration testing. Furthermore, when a vulnerability is identified, it is important to verify the validity using multiple sources.

There are public testing methodologies that are available. Various organizations have published free frameworks that will facilitate successful in-house penetration testing:

- The Open Source Security Testing Methodology Manual (OSSTMM), currently version 2.2 and version 3 Lite are free
- Open Web Application Security Project (OWASP) Testing Guide
- NIST Special Publication 800-42: Guideline to Network Security Testing

© 2010 The SANS Institute Author retains full rights.

When comparing methodologies, the financial institution should strive for repeatability, consistency, and high quality in the kinds of tests that are conducted. One advantage of running penetration testing in-house is that it will validate that the network design reflects what has been implemented.

It is possible to in-source a penetration test, but this decision should not be taken lightly as the cost of retaining this expertise on staff is frequently the deciding factor to pursue outsourcing. Successful penetration testing requires meticulous attention to detail and careful record keeping. Make sure that the in-house team has both the technical capability to identify vulnerabilities and that someone in the organization will be given the autonomy to ensure that any identified issues will be fixed with appropriate priority.

4.3. Outsourcing the Penetration Test

Once the organization decides that outsourcing is the right strategy under which to conduct penetration tests, there are some key characteristics that should be considered when picking a company. Reputation is certainly a good start, but there are number of subtle elements that will distinguish the excellent organization. Interview potential penetration testing companies to determine how they will set scope, how they will prioritize the testing, and the mechanics of the testing. It is also essential that the firm be diligent about handling of sensitive data, and that they be beyond reproach in how they address questions regarding the high-level technical approach. In some cases the penetration testing company will use customized exploits that will generally not be shared due to their proprietary nature.

The penetration testing firm should engage the customer to carefully identify the scope of the test. The client financial institution must disclose those areas that are of greatest concern. Only by disclosing this information can the efforts of the test be focused on finding the most significant vulnerabilities. If the penetration test results in a map of the infrastructure gained by spending thousands of dollars to scan all subnets, then this is money poorly spent. It is better to provide a map of the network architecture to the penetration testing firm and scope the test to focus on the high-risk systems and applications in that environment. Follow-up testing should then be driven by changes in information technology, the business environment, or the threat landscape.

Author Name, email@address

© 2010 The SANS Institute Author retains full rights.

The threat landscape is in part determined by what hardware and software is running in the client environment. Therefore, when setting the scope it is important for the financial services organization to have an updated comprehensive asset inventory. This will minimize the probability of bringing down systems that are being run by a third-party on behalf of the financial institution. Domain Name System (DNS) is a great example of such a system that is often outsourced. A good penetration testing firm will guide the client organization to adopt rules of engagement that protects both the client and the provider organization doing the testing. The rules of engagement will include getting permission to test systems owned or managed by a third-party. The rules of engagement are the essential list of rules that both the penetration testing firm and the hiring financial services firm will adopt for mutual protection. A good penetration testing firm will be insistent about creating a clear set of rules around what should be tested and what is out of scope and should be avoided. The scope should clearly define what systems will be tested.

Testing of production environments is generally dangerous because some penetration tests have the ability to bring down systems. The rules of engagement will clearly spell out whether test or development systems are in scope. In the planning phase before conducting the test, consideration should be given to staging the test from internal to the corporate network or from outside. Conducting penetration testing from outside the network is intended to mimic the conditions that an attacker will see, whereas testing from inside the network mimics what a malicious insider or a hacker that makes it through perimeter defenses will see.

4.4. Hybrid Approach

The hybrid approach will require collaboration between the penetration testing company and the financial services institution. Such a partnership will utilize both parties' strengths in a manner that maximizes the value of the penetration test. Value in this case means identifying as many risks as possible, and this can only be done when both organizations embrace a spirit of full disclosure.

The financial institution should be able to identify all of the assets within the enterprise. This list should be comprehensive and include those items recently added to

© 2010 The SANS Institute Author retains full rights.

the network, for example a new wireless access point that was put into the executive boardroom last week, or a new Web application firewall that is being tested. Ongoing vulnerability management results, like scans that have been run, should be shared with the penetration testing company if White-box testing is being done. When the financial institution is giving the penetration testing company complete knowledge of the infrastructure, the information should include the technical and security staff perspective on their areas of greatest exposure. Such disclosure can focus the test on those areas to probe the validity of the concern. It is important to leverage the experience of the operations, security and other staff since they often have the greatest familiarity with the degree of exposure within the infrastructure. This information is learned over the duration of their employment with the financial services organization and is crucial to help identify potential exposures. The penetration testing company can do that much better when working with the client organization collaboratively.

The penetration testing company must also step up and bring their best people to the penetration testing engagement. C. Warren Axelrod, in his book Outsourcing Information Security says, "Customers should be forewarned that, while a service provider may have presented staff with exemplary credentials, it may not be planning to assign those particular individuals to your account. It is important that customers understand exactly who is to be assigned to their project and in what roles. Specific staff assignments should be included in the service agreement." (Axelrod, 2004) Experienced staff will be able to develop scripts and use custom exploits that make the most sense for a given network configuration. They will have exposure to a larger number and variety of client engagements. This experience will enable them to review the vulnerability scanning results and other information to suggest a prioritization that yields the quickest reduction in risk to the environment.

When the resources of the penetration testing company and the financial industry client are combined to focus on identifying risk, the results of the penetration test are dramatically better. A collaborative effort will help to determine scope and leverage each parties experience to prioritize remediation.

Author Name, email@address

© 2010 The SANS Institute Author retains full rights.

5. Conclusion

Penetration testing is essential given the context of high operational risk in the financial services industry. Web-based and internal applications should be fully tested to ensure they do not provide an avenue of entry for attackers. Vulnerability management should be considered a priority given the sophisticated malware targeting client PCs inside the organization. Wireless vulnerabilities also add to the attack surface that can be exploited.

Penetration testing is the only legitimate means to identify residual risk that remains after code has been tested and operational and other threats have been minimized. To make the most of penetration testing it is necessary to prioritize the effort. The penetration test should be scoped properly and should take advantage of the knowledge that the client organization has regarding exposures within their enterprise. And this information should be combined with the experience and insight of the penetration testing company.

As stated initially, the goal of penetration testing is to compromise a target system and ultimately steal information. Penetration testing is focused on finding security vulnerabilities in a target environment that could let an attacker penetrate the network or computer systems (Skoudis, 2008). A collaborative approach is recommended whereby the financial services organization and the penetration testing organization work together to more efficiently identify which exploits can be leveraged to steal information.

6. References

Arce, I., & McGraw, G. (2004, July). Why Attacking systems is a good idea. *IEEE Security & Privacy*, *1504-7993*(04), 17-19.

Axelrod, C. W. (2004). *Outsourcing information security*. Norwood, MA: Artech House.

ISACA. (2004). Security assessment-penetration testing and vulnerability analysis. *IS Auditing Procedure*, (P8), Retrieved from http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=31608

Author Name, email@address

© 2010 SANS Institute, Author retains full rights.

McGraw, G. (2006). *Software security: building security in*. Boston, MA: Pearson Education, Inc. McGraw, G. (2006). *Software security: building security in*. Boston, MA: Pearson Education, Inc.

PCI. (2008). Information supplement: requirement 11.3 penetration testing. *PCI Security Standards Council*, *11.3*. Retrieved from https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf

Skoudis, E. (2008). Planning, scoping and recon. *Proceedings of the Network penetration testing and ethical hacking course* (pp. 12-16). The SANS Institute. V120708

Unifiedcompliance. (2010). *Penetration testing and vulnerability scanning*. Retrieved February 21, 2010, from Unified Compliance Web site: http://www.unifiedcompliance.com/matrices/live/00655.html

Whitaker, Andrew, & Newman, Daniel. (2005). *Penetration testing and network defense*. Cisco Systems.

Author Name, email@address

© 2010 SANS Institute, Author retains full rights.

Last Updated: March 10th, 2014

Upcoming SANS Penetration Testing

SANS PENETRATION TESTING

Click Here to {Get Registered!}

Mentor Session - AW - SEC 504	Atlanta, GA	Mar 13, 2014 - May 15, 2014	Mentor
SANS Northern Virginia 2014	Reston, VA	Mar 17, 2014 - Mar 22, 2014	Live Event
Community SANS Paris @ HSC - SEC560 (in French)	Paris, France	Mar 24, 2014 - Mar 28, 2014	Community SANS
SANS vLive - SEC504: Hacker Techniques, Exploits & Incident Handling	SEC504 - 201403,	Mar 25, 2014 - May 01, 2014	vLive
Mentor Session - SEC 560	Annapolis Junction, MD	Mar 26, 2014 - May 28, 2014	Mentor
Mentor Session - SEC 504	Regina, SK	Apr 02, 2014 - Jun 04, 2014	Mentor
Mentor Session - SEC504	Boston, MA	Apr 02, 2014 - Jun 04, 2014	Mentor
Mentor Session - SEC 560	Augusta, GA	Apr 03, 2014 - Jun 05, 2014	Mentor
Mentor Session - SEC 560	brentwood, CA	Apr 03, 2014 - Jun 05, 2014	Mentor
SANS 2014	Orlando, FL	Apr 05, 2014 - Apr 14, 2014	Live Event
Community SANS Cupertino	Cupertino, CA	Apr 07, 2014 - Apr 12, 2014	Community SANS
SANS 2014 - SEC560: Network Penetration Testing and Ethical Hacking	Orlando, FL	Apr 07, 2014 - Apr 12, 2014	vLive
Mentor Session - SEC 504	Cleveland, OH	Apr 09, 2014 - Jun 11, 2014	Mentor
Community SANS Colorado Springs	Colorado Springs, CO	Apr 21, 2014 - Apr 26, 2014	Community SANS
Community SANS Montreal	Montreal, QC	Apr 23, 2014 - Apr 24, 2014	Community SANS
Mentor Session - SEC 560	Fredericksburg, VA	Apr 24, 2014 - Jun 26, 2014	Mentor
Mentor Session - SEC560	Toronto,	Apr 24, 2014 - Jun 26, 2014	Mentor
SANS Austin 2014	Austin, TX	Apr 28, 2014 - May 03, 2014	Live Event
SANS vLive - SEC542: Web App Penetration Testing and Ethical Hacking	SEC542 - 201404,	Apr 28, 2014 - Jun 04, 2014	vLive
SANS Security West 2014	San Diego, CA	May 08, 2014 - May 17, 2014	Live Event
SANS Security West 2014 - SEC504: Hacker Techniques, Exploits & Incident Handling	San Diego, CA	May 10, 2014 - May 15, 2014	vLive
SANS Secure Europe 2014	Amsterdam, Netherlands	May 10, 2014 - May 24, 2014	Live Event
Community SANS Columbus	Columbus, OH	May 12, 2014 - May 17, 2014	Community SANS
SANS Malaysia @MCMC 2014	Cyberjaya, Malaysia	May 12, 2014 - May 24, 2014	Live Event
SANS vLive - SEC560: Network Penetration Testing and Ethical Hacking	SEC560 - 201405,	May 12, 2014 - Jun 18, 2014	vLive
Mentor Session - SEC 504	Raleigh, NC	May 12, 2014 - Jun 19, 2014	Mentor
SANS Melbourne 2014	Melbourne, Australia	May 12, 2014 - May 17, 2014	Live Event
Mentor Session - SEC 504	San Diego, CA	May 15, 2014 - Jul 24, 2014	Mentor
Community SANS Paris @ HSC - SEC542 (in French)	Paris, France	May 19, 2014 - May 23, 2014	Community SANS
SANS Secure Thailand	Bangkok, Thailand	May 26, 2014 - May 31, 2014	Live Event
Community SANS Minneapolis	Minneapolis, MN	Jun 02, 2014 - Jun 07, 2014	Community SANS