Clear Skies
SECURITY
Intelligence. Secured.

Assessment FAQ

Getting the most out of your security engagements

By:
Rick Belisle, COO Clear Skies Security, LLC

January 2010

Summary

Clear Skies Security, along with several of our competitors, offer a wide variety of assessments each with different methodologies, approaches, and outcomes. This set of Frequently Asked Questions (FAQ) walks through some of the common customer questions along with our perspective in detail. It is based on over 10 years experience in delivering security assessments to organizations of all sizes and types. Hopefully you will not only find this informative, but it will also give you the information you need to make the most informed decisions about security management processes.

Frequently Asked Questions (FAQ)

What is the difference between a Vulnerability Assessment, a Penetration Test, and a Web Application Assessment?

When it comes to the different kinds of assessments, the terms do tend to get either misused or misrepresented. The definitions commonly accepted within the industry differentiate the assessments by the amount of exploitation testing that is conducted during the testing.

A *Vulnerability Assessment* is typically conducted using automated vulnerability scanners such as Nessus, Qualys, ISS Internet Scanner, Rapid7, etc. This level of testing only attempts to identify if a particular vulnerability is present by relying on the parameters defined in the scanner. Accuracy of the findings depends on the accuracy of how the "check" is written within each of the tools. Therefore this level of testing tends to have the highest level of false positives. To counteract this, Clear Skies' methodology uses multiple tools and also does manual validation on checks with known high false positive rates. This makes our results more accurate and more beneficial to you.

A *Penetration Test*, commonly referred to as a "Pen Test, goes to the next level of testing and simulates real hacker techniques by exploiting the vulnerabilities identified through automated or manual vulnerability identification. The advantage to this testing over a Vulnerability Assessment is that the customer gains an understanding of what their real threat profile is by knowing what systems and data are truly at risk to compromise. Clear Skies' methodology puts a heavy focus on manual exploitation techniques during our Pen Testing. This simulates real world hacking attempts that examine both known technical vulnerabilities as well as configuration errors and logic errors. This is a big differentiator for Clear Skies as most competitors rely on exploitation tools like Metasploit to conduct their exploitation testing so the likelihood of a successful exploitation is much lower as each customer environment is unique and needs to be examined with specific testing parameters. ***The general rule of thumb is if there is no manual testing by a skilled human being then it is NOT a Pen Test.***

Defining a *Web Application Assessment,* however, is much more of a grey area. Most companies refer to a Pen Test against a web site as a Web Application

Assessment, but Clear Skies typically includes Web Application Pen Testing under our standard Pen Test service offering. However, to provide the focus needed on unique or highly customized application environments, we added a dedicated service for *Application Assessments. This offering* is the next level above our standard Pen Testing. Our Application Assessment usually has a smaller scope, being a specific application environment, and therefore testing can dive deeper into the details of the application. Application Assessments can also leverage multiple user account credentials so we can ensure all areas of the application are fully tested, and special testing can be conducted between user accounts and roles to simulate session hijacking attacks. Clear Skies' Application testing is suited to those that want to test the logic of the application more thoroughly then any tool will ever be able to provide.

What are the differences between a "black-box", "grey-box", and a "white-box" assessment?

These terms are typically used in conjunction with an assessment type, and refer to how much information is shared with the assessors prior to starting the assessment. A "black-box" test refers to the least amount of information being shared, and "white-box" is the opposite extreme where everything is shared up front with the assessor. "White-box" testing may also refer to when source code is provided for detailed analysis. Each kind of test has its pros and cons, and which one is the right one depends on what the individual goals are for that particular assessment. The main difference is that "black-box" testing best replicates the scenario of an unauthorized hacker coming from the Internet with limited knowledge of the environment. The down side is that the tester may have to spend a lot of the testing time acquiring the information needed to conduct a successful exploitation rather than conducting further testing. The different levels of information exchange help meet the assessment goals by balancing time versus effort as real hackers don't have the same limitations on the amount of time they spend against a target and can take as long as they want to develop a successful exploit if needed.

Why does your Pen Test service seem so much more expensive compared to an automated security assessment service?

As discussed above, Clear Skies' methodology relies heavily on manual testing techniques, which is extensively more time consuming when compared to a purely automated approach. We believe Clear Skies' approach provides a perfect balance between cost and quality findings. We feel that the added value that our security professionals can provide in doing the risk analysis far exceeds the perceived savings a solely automated approach provides. We can provide either approach based on each customer's needs and goals, but feel the additional manual testing provides significantly greater value to our customers.

What seems to be the biggest risk to organizations these days?

All of the current statistics show an overwhelming focus on application layer vulnerabilities. With the use of custom and Web 2.0 applications on the rise, the likelihood for insecure programming or faulty program logic is definitely high. Often the development team is focused on application functionality, compatibility, and ease of use and security tends to be an after thought. Hence applications that have not undergone specific security testing during development, QA, or beta testing are usually deployed straight to the Internet without a detailed understanding of what the real risks are. Clear Skies' Application Assessments can help identify these risks before they are put into a production environment, or a customer can leverage our Secure Code Training options to help train in-house developers to write more secure code during the development process.

Is the Clear Skies methodology based on any industry standards?

All of the assessment methodologies that Clear Skies utilizes have evolved over the last 15 years our assessors have focused in this arena. However, we understand that it is important to have a common framework that customers can leverage to ensure our approach meets their needs, and how it may differentiate from other vendors in the market place. Given that, Clear Skies methodologies are built around several industry standards to include:

- Open Web Applications Security Program (OWASP)
- Open Source Security Testing Methodology (OSSTM)
- Application Security Verification Standard (ASVS)
- NIST SP800-30

How could I use a Pen Test to evaluate the effectiveness of my staff?

Clear Skies' Pen Testing methodology, which mimics true hacker techniques, can be used to conduct a very controlled evaluation of how your staff might react to a real intrusion attempt. The key to doing this successfully is to limit the amount of people within the organization that know about the assessment project, so the staff reacts to it as if it were a real incident. Of course, the project sponsor should also be high enough in the reporting chain that they can effectively put a stop to any on-going investigation attempts before any authorities are notified. When executed properly under these conditions it can provide a great mechanism to help prepare your staff and exercise your Incident Response Plans so that when something does happen for real you will be prepared.

Does Clear Skies also do internal testing? If so, what kind?

Yes. Clear Skies can perform internal Pen or Application Testing to mimic a malicious insider. As an alternative, Clear Skies also offers our Internal Security Assessment (ISA) that provides an enterprise view of security throughout the organization. Given the large scope of an ISA, as compared to a Pen Test, the

methodology is slightly different and focuses more on vulnerability identification rather than exploitation. Our methodology, however, also incorporates extensive manual reviews of internal configurations of security devices to ensure that configuration errors that normal security testing may miss are still identified and rectified. Please refer to the ISA summary page on the website (www.clearskies.net/isa) for more information about this service.

Why should we conduct regular security assessments?

Regular security assessments are vital to any security management program. Vulnerabilities are continually being released at a record pace, and applications and infrastructure both constantly change and evolve. New findings combined with environmental changes often open up new security issues within organizations. Clear Skies recommends regular assessments to minimize the time that a potential vulnerability may be open before it is identified. In an effort to minimize costs, an assessment schedule that leverages multiple kinds of assessments can be very effective, for example, quarterly Vulnerability Scanning combined with semi-annual Pen Testing, and if needed annual Application Assessments. The kind of testing and the frequency should be set according to your overall risk level, and business goals.

How does Clear Skies evaluate a vulnerability's risk?

Clear Skies bases risk rankings on the metrics defined by NIST SP800-30. NIST categorizes risk based on the likelihood of the threat and the impact of the threat. The likelihood rating indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment. The following governing factors are considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

The impact a particular risk may have on an organization is based on the importance of:

- How critical the asset is to the organization
- The data that is stored on, or accessed via, that asset
- The sensitivity of the data stored on, or accessed via, that asset

The final determination of overall risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact.

What kind of information is included in the assessment deliverable?

The first section of the deliverable is a true executive level summary, which

provides a business risk analysis rather than just a summary of the technical details. The remainder of the deliverable provides the details on the findings to include both the vulnerability risk rating and the overall risk rating, as well as recommendations on how to correct the vulnerability or lower the overall risk. On assessments where exploitation is conducted, an entire section of the deliverable provides an "Attacker's Perspective" that walks through all of the exploits that were used, how they were executed, and screen shots of the results to fully detail what could be done if this were a malicious attack. All of these things combined, provide a complete picture of where an organization might be lacking security and what is truly at risk.

These assessments seem like overkill. I'm a small business, why would a hacker come after me?

In today's environment, targets are selected through a systematic process of scanning through the Internet in search of potential victims. As a result of this, every business, regardless of size or industry, must understand their true threat profile. Conducting regular assessments and minimizing your threat profile is the best way to protect yourself from becoming a target.

I've already invested heavily in security technologies like firewalls and antivirus…aren't I already protected from external attacks?

Firewalls and antivirus are solid security technologies that are essential for every organization, however, they are not capable of protecting a business from every possible avenue of attack. For example, firewalls allow or deny connections based on allowed behavior defined in the rule base. If a company has an external facing website, the firewall must allow Port 80 from the Internet, and if the web server or application has a known vulnerability, the firewall does nothing to protect that vulnerability from being exploited. By understanding what vulnerabilities are present and what data is at risk, an organization can make sure they are effectively spending their security budget in the areas that need it most. Technology purchases are only one piece of the overall puzzle.

What kinds of assessments are required for compliance purposes?

Unfortunately each regulatory compliance body defines their own set of assessment criteria based on what they feel is the highest risk for their particular vertical. Most of them, however, have used the international ISO 27002 standard as a baseline to build their requirements from. So, it is always recommended, at a minimum, to ensure you meet these high-level policy/procedure requirements and then follow the criteria for each individual regulation for the other technical requirements. It is also important to note that more and more of these regulations are requiring regular assessments, usually at least annually, for vulnerability scanning or Penetration Testing.

Let Clear Skies put YOU on the right path…

Clear Skies is a security consulting organization specializing in real world threat analysis through comprehensive security assessment services, specifically Penetration Testing and Application Assessments. Clear Skies focuses solely on services allowing our consultants to remain concentrated on providing the best vendor neutral advice to remediate the risks identified during the assessment process. Our primary goal is to become your Trusted Security Advisor. This allows us to work cooperatively to ensure the highest level of protection for the business and to provide some assurance in knowing that the true risks are being identified.

Clear Skies was founded by a team of elite security professionals, each bringing 10+ years of experience in the security industry, all with a specialty in security assessments. Our mission is to be a trusted name in the security industry, known for our technical knowledge, integrity, and business ethics. We do this by focusing on customer service and ensuring quality in everything we do.

In the end, our goal is to ensure that **our Intelligence Secures your Intelligence.**

Clear Skies
SECURITY
Intelligence. Secured.

12460 Crabapple Road Suite
202-253
Alpharetta, GA 30004
(772) 463-7525

sales@clearskies.net

www.clearskies.net