Light years beyond the Penetration Test.
Enter the Cyber Risk Assessment.

by Lauro Chavez, Master Security Architect

Penetration testing is now a permanent requirement in most governance frameworks from NIST to PCI DSS, making it a mandatory step in the annual budgets and operations. While most understand a penetration test is necessary in order to meet their client and regulatory requirements for the year, there is little knowledge on what these tests actually accomplish for the organization and how they are conducted. In addition, an industry-wide consensus of what defines a true penetration test does not exist, creating further confusion.

The results many receive from their organization's penetration tests are often not meaningful and insufficient to minimize cyber risk. Companies often receive a basic vulnerability scan that was sold to them as being a penetration test, or overly simplified penetration test with results showing a pie chart with OWASP (Open Source Web Application Security Project) vulnerabilities.

Some may think these limited approaches are acceptable and some were acceptable years ago, but we operate in modern times with a heightened level of cyber risk. A modern and effective risk identification approach is now required for a penetration test to be valid.

Enter the Cyber Risk Assessment – A comprehensive and tailored approach to defining cyber risk, which includes penetration testing.

An organization that does even a small part of its business over the World Wide Web or Internet of Things (or however you prefer to refer to "public fabric"), incurs a specific amount of risk due to their dependence on technologies and public interconnected infrastructure. The excuse of "I don't have anything cyber-criminals want" is over. If you have computing power even in the form of a home grade laptop or personal smart phone be assured, you are most wanted by cyber-criminals. Your risk exposure is dependent on several factors of your technology-based activities as a business and an individual user.

Silent Sector has designed its Cyber Risk Assessment around the key areas of risk to an organization based on their dependency on technologies and the public and private networks that assist them. This way we can strategically assist the organization with the areas and activities pose the most significant risk, providing a strategic pathway to resolve the most critical vulnerabilities and risks. This makes the best use of time and budget while ensuring the attack surface is reduced and blocked. Handing over a vulnerability scan with remediation assistance or pie charts is unfortunately a backward method to present risk to an organization. It often leads to either a false sense of security or more remediation work than necessary.

Let's get into the components of the Cyber Risk Assessment and how they provide the foundation of understanding your company's cyber risk. Considering the purpose, there is a formality that should be kept around penetration testing, which is why we utilize a comprehensive approached split into three-phases.

1 - Analysis and Scoping

During the initial steps we refer to as "Analysis and Scoping," we interview the business to define the scope that needs to be included in the testing. This is done via a conference call. Depending on the company size, several teams may be involved or one individual who really understands the company's technical dependencies. Once we understand the fundamental operations of the business, its compliance requirements, and its staff's technical capacity, we can recommend a plan and scope for the Cyber Risk Assessment or take the data and work it into a larger cyber risk management plan.

2 - Engagement Activities

During this phase of the Cyber Risk Assessment Silent Sector will provide the timelines and confirm the scope/targets for the testing. Organizations with high-volumes of web or network traffic are typically tested during off-peak hours so operations are not hindered. We will also establish a campaign name that can be referred to in email for quick discovery of events.

Unless testing is meant to assess the in-house technical team's monitoring and response capabilities, an email is sent to the client's technical team to alert them that testing will begin. This provides an opportunity for an optional "purple-team" exercise which allows the client's team to see the outcomes of our testing activities in real time. We also use the campaign name to alert the organization of any critical items that are discovered, as they are discovered. That's correct, Silent Sector doesn't wait until the testing is finalized to tell you that you are hackable, "pwnable" or simply put, misconfigured in a way that a 10-year-old can break in. We can halt testing and work with your technical team to validate the critical issue and remediate as quickly and securely as possible. Then we can re-test during the active campaign to confirm successful remediation.

This phase ranges from 40 hours to 300 hours or more of testing and assessment time, depending on the needs and complexity of the organization. All of our electronic espionage activities and cyber-attack testing will be performed during this phase, along with any location specific physical perimeter or wireless testing.

3 - Replay and Report

When the campaign is finalized and the hours have been utilized, the pen-tester will formally turn down the pen-testing activities by alerting technical teams and leadership. The report will be written, reviewed and presented formally to the organization with a walk through from the pen-tester. During this time any activities that resulted in any exploitation can be replayed for the audience if requested and retesting activities that were not able to be accomplished during the engagement can be scheduled. This is also provides and opportunity to discuss any remediation tactics or future testing activities.

Our common testing tools and how we use them:
Metasploit Professional is where the majority of our exploitation activities are rooted. We deploy this industry recognized tool onto Kali Linux so that we can also take advantage of some of the more common web application penetration testing tools like Hydra Brute Force software and WordPress Scanner. Silent Sector leverages an enterprise version of Qualys for external 'cloud' based and internal 'virtual' vulnerability scanning. We can import .xml into the Metasploit framework for quick and accurate exploit matching. Zed Attack Proxy provides a very clean method to interrupt the post and get responses in order to manipulate Java Script and other queries.

For SaaS companies and others with proprietary applications, there are many free tools that we can show your team how to install and leverage for the software delivery processes. We believe highly in the "train the trainer approach."

Finally, we head into the research and partial/working exploit modifications. We search the dark-web and other locations for working and partially working exploits. Depending on the time allotted for the campaign, we can demonstrate a proof of concept turning new partially working exploits into fully functional take-down scripts, preparing the client for some of the future cyber-criminal attack methods.

We will work directly with your team to validate each exploit's accuracy and validity. This means Silent Sector will not knowingly and purposefully take down your systems without careful and strategic assistance from your team, unless destructive demonstration is the intent of the test and is conducted in a test environment.

When wireless networks for security and proper segmentation, we leverage the latest industry testing tools like the WiFi Pineapple. We can even test the awareness of your physical security staff with social engineering and physical breach incident reaction assessments.

Proactive companies are discovering that the cybersecurity industry is selling "penetration tests" that turn out to be nothing more than vulnerability scans and automated reports, which are insufficient in mitigating risk on their own.

With the absence of a widely accepted standard of what makes a true penetration test, the Silent Sector team supports clients by defining the activities that must occur in their Cyber Risk Assessment to truly identify and minimize current cyber risks. Working within your organization's needs, capabilities, budget, and timeline, our tailored testing and assessment services do more than just "check the block."

To meet the demands of today's cyber risk environment, Silent Sector takes a consultative and customized approach. Contact us to learn more about protecting your company's brand reputation, wellbeing, and continued success.