QOS | Your key to Internet Security

Uncover Issues
before Real Attack

Hits Your Organization

Advanced Penetration Testing Services

Overview

Vulnerabilities on the Internet are being exploited in massive numbers every day. With the advancement of technology, what used to be a power reserved only for states and highly resourced organizations is now within reach of hackers and hacktivists. Moreover, the attack vectors are collaboratively crafted by the multiple attackers working in tandem to either exploit your organization's IT infrastructure for financial gains or targeting your assets & IT crown jewels for stealing specific business information or state sponsored cyber terrorism. The vectors are targeting the soft links like, human beings working or interacting with legitimate users of your IT infrastructure, and apart from this, they also exploit the vulnerabilities in the IT infrastructure & applications. Furthermore, they aim to discover the covert channels that exist owing to business interfaces within different units of the organization or its business associate companies.

In its preparedness to handle any such Advance Malware or Exploitation risk, the organizations have in-house Red Team functions (also referred to as penetration testing) or they outsource to organizations skilled with the Red Team functions. In a typical Red Team penetration services model, the objective is to discover the vulnerabilities, covert channels, unknown interfaces that exist in the IT infrastructure & applications and submit the report for the team to plug these gaps before a real hacker exploit any such gap.

Though the objective of Red Team is definitely a key function of IT Security & Risk management strategy of any IT-oriented business entity but the prevailing practice is not keeping the organizations ahead of the attack. The Red Team function of penetration testing on most occasions is shadowed with a mindset of discovering maximum vulnerabilities & produce a scary report. While discovering maximum gaps existing in the IT setup is a right thing, but the Red Team mindset creates a sense of insecurity in the Blue Team. The job of a Blue Team involves not only to prevent the attacks but also respond. The mindset of the Red Team function to defeat the Blue Team makes the Blue Team to provision the temporary controls for blocking the Red Team vectors or if Blue Team is caught unaware of the Red Team activities then they get into defensive adjustments. Either of the Blue Team responses is not inclusive in objective and despite investing resources in Red Team functions and also in the Security Controls & Blue Team operations, the organizations achieve results much less than desired to defeat the actual hackers proactively.

In order to bring a value and achieve the desired purpose, QOS Technology has adopted a Purple Team functions or the Advance Penetration Simulations. This is more like playing a Game with a sports spirit and evolve the security posture as a whole with every advance penetration simulation or assessment. The QOS Technology approach uses the combined skills of Red & Blue Teams with its consultant's assigned tasks of performing the Advance Penetration Simulations, hence at QOS Technology, we call it the Purple Team functions.

Advanced Attack Simulation Services

Advance Penetration Simulation Service (also referred to as Purple Team functions) will validate & fine-tune the Customers' IT infrastructure & security controls to prevent the advanced exploitation & intrusive attack vectors. Moreover, this exercise will provide a unique opportunity to your team to respond to a number of sophisticated exploitation attack scenarios by conducting a real-time attack simulations utilizing two distinct teams: "Red Team (Attack Team)" and a "Blue Team" in a real game format.

The attacks would be comprised of three scenarios:

1. Assessing the exploitation tactics against interacting network protocols (HTTP, SSL, SMTP, etc) and server operating systems used by Customer on the public facing infrastructure like email, web, portal, etc. for validating the external penetration testing or the end users in order to discover the lateral movement of attacks.

2. In this scenario, We assess the impact on the web & other application layer attacks, letting attack vectors to steal the data through SQL, XSS. Furthermore, other advanced attack vectors may be used to create the pivot hooks to laterally move inside the organization for more devastating attacks.

3. The third scenario aims at assessing the impact of a custom attack. This will replicate a sophisticated attack scenario where information on Customer Infrastructure has been gathered and intelligently analyzed to enable an attack team to target specific vulnerability within the Customer web platforms, such as login page, file uploads, data streaming, product brochures, etc. This may also be started or modulated to include the Phishing Attack and furthermore, bypass the AV controls installed.

Our Team emulates the real-world activities of advanced persistent threat actors and carries out different cyber attacks against your organization to identify vulnerabilities.

Methodology

Prior to the simulation, our Purple Team (Red Team plus Blue Team skills) conducts extensive research of the customer websites, customer information with OSINT (open source intelligence) and any associated business sites connected to this infrastructure where the exploits, or backdoors may sneak into customer infrastructure in order to collect valuable intelligence information. Based on the information gathered, QOS Purple Team will create different attack scenarios aimed to simulate real-world Advance Penetration or Intrusion attacks

Research engagement may be defined for 3 Days, One Week or Custom duration depending upon the scope of the infrastructure that needs to be tested for Advance Penetration Simulation services. Moreover, the Research engagement may be:

Black Box

No prior information about the infrastructure under testing, and no direct access or user credentials are given for the infrastructure access.

Grey Box

Basic information about the infrastructure, like IP Address (or URL, etc.) is shared by the customer for the infrastructure under scope, but no direct access or user credentials are shared by the customer with the Purple Team.

White Box

The complete information about the infrastructure (like IP address, URL, Server OS, Application type, platform details, etc.) is shared by the customer, and the direct access through LAN or WLAN is given to the purple team and authentication credentials to login into the systems/databases for the creation of advanced attack vectors.

Once the Purple Team completes the research for the attack simulations, the 6-7 scenarios are prepared that may include the SQL Injection, Cross Site Scripting (XSS), Privilege Escalation, Post Exploit lateral attacks, Data Exfiltration, Phishing Attacks, etc. Based on the scope of the customer infrastructure either the 5 days, 8 days or 10 days' simulation is planned. In the Attack Simulation phase, the Purple Team engineer of QOS will be on-site with the customer team(s) and the Purple Team attackers will launch the attacks in real time for the defined duration of the days. In the defined period of days, Purple Team will work to raise the security posture of the Customer Infrastructure & Services, etc. through 5, 8 or 10 days' simulations. On the completion of the Purple Team assessments, a report of the residual risk will be submitted.

Deliverables

The report delivered to the customer is called as "Advance Penetration Residual Risk Summary" Report. The report is based on the findings of the Research engagement and the subsequent revisions made to the security controls by the onsite QOS engineer. The report includes the following sections, enabling both management and the technical factors to clearly understand the key findings and required actions:

- Project Approach
- Scope of the Work
- Red Team Findings
- Blue Team review & revision to improvise security posture
- Residual Risk & Recommendations
- Technical Summary

The findings in the report will be comprised of insights furnished by the Red team, the data collected on-site by the Blue team and information received by the customer Team (such as server or network components logs). The report is delivered within ten business days after the simulation along with the recommendations.

Uncover hidden vulnerabilities of your infrastructure by emulating real-world attacks. Find ways to strengthen your defence and enhance your reputation by protecting your customer data and digital infrastructure.

For more information,

GET IN TOUCH

QOS Technology

Corporate Office
5th-Floor Navnit Motors Building, No 70, Millers Tank Bund Road,
Vasanth Nagar, Bengaluru, Karnataka 560052

Email: info@qostechnology.in
Website: www.qostechnology.in