KNOWING YOUR ENEMY:

HOW PENETRATION TESTING CAN AID IN UNDERSTANDING YOUR THREAT ACTORS

subrosa

FOREWORD

The existential expansion of technology and ever-expanding use of computers has led to the emergence of new types of risk, which the use of standard security testing methods cannot prevent. The number of incidents is growing year over year, along with the impacts of these incidents.

This has forced organization's to prepare themselves for the ever expanded dangers posed by real attacks. Assessments, training and risk management are all useful solutions, but require additional, technical experitse to underpin them.

CONTENTS

THINK LIKE YOUR ENEMY

Penetration testing involves simulating cyberattacks on an organization. It’s one of the most important aspects of ensuring effective cybersecurity in today’s digital landscape. Vulnerability assessments and penetration testing can help expose potential weaknesses in an organization's defense that might have otherwise gone unnoticed. Unnoticed and unpatched, these weaknesses can serve as potential attack vectors for cyber threats.

Traditionally, cybersecurity has been about employing defensive measures to thwart any potential threats. These measures however comprehensive they may be are certainly not adequate to deal with rapidly changing digital landscapes and evolving threat actors. Passive defenses alone cannot ensure effective cybersecurity on all fronts.

Penetration testing forces you to think like your enemy. How would you infiltrate the digital infrastructure of this organization? Which vulnerabilities would you try and exploit? How would you scope the defenses? Which attack vector would provide you with the best chance of success?

Thinking like your enemy helps simulate the entire attack-response chain. First, an attack is simulated on the existing systems and measures. Then, actionable data and input of the attack attempt is received. A thorough analysis of the obtained information is used to formulate protective measures to patch up the said vulnerabilities. Penetration testing thus ensures that clear and actionable steps can be undertaken to remediate vulnerabilities and mitigate the overall risk factor.

Thinking like your enemy helps simulate the entire attack-response chain.

THE RANGE OF TESTING THAT IT ALLOWS FOR

Addressing findings resulting from penetration testing allows for businesses to ensure safety and protection on multiple fronts.

STEPS IN A PENETRATION TEST

PLANNING PHASE.
The first step of a penetration test is to know the scope and extent of the required test. Risk analysis and threat modeling are also used to determine the area of focus for the test and the potential threats that are likely to arise. Key test factors such as tools and methodologies to be used, level of sophistication, response measures, etc are also discussed in this phase.

SCOPING PHASE.
The scoping phase of a penetration test involves gathering intelligence on the target firm's systems and networks. Following a vulnerability assessment, the penetration tester undertakes further reconnaissance to assess and target specific vulnerabilities.

ATTACK PHASE.
This phase involves the actual attempt to exploit the vulnerabilities that were exposed during the scoping phase. During the attack, penetration testers often use a combination of multiple tools and methods to try and gain a persistent presence in the target systems.

ANALYSIS PHASE.
All the observable and actionable data resulting from the attack are compiled and formulated into a report. Risk analysis of the affected data sections and the impact of every key action is analyzed to present a clear picture of what the penetration test achieved.

REMEDIATION PHASE.
Based on the analysis obtained from the penetration test, remediation measures are taken to patch the exposed vulnerabilities and to minimize the impact of any potential attacks in the future.

THE ADAPTABILITY FACTOR

Each security audit has specific goals and requirements. Penetration testing is highly adaptable to test for vulnerabilities in various domains of an organization’s digital systems.

Be it probing for internal or external points of entry. A penetration tester can replicate multiple scenarios where weaknesses within the organization’s internal systems and/or external systems can be exposed. Social engineering attacks, phishing attacks and malicious insider acts are a few examples where the damage inflicted from the threat actor can be pinpointed to an internal point of origin. External threat sources can range from DDoS attacks to SQL injection to DNS tunneling and many more. In today’s business environment, ransomware attacks are also proving to be increasingly debilitating. Considering all the potential sources of entry that a threat actor can utilize, penetration testing is paramount to proactively address any potential weaknesses before they can be exploited.

Depending on the organizational motivation behind the penetration test, various approaches can be taken to best suit the test requirements. In a black box penetration test, the penetration tester is given little or no information about the target firm’s infrastructure.

Each type of test brings with it a certain edge. The higher the level of information provided to the tester, the more focused and targeted is the penetration test.

Whereas the opposite ensures a more real-life attack and response scenario. The double blind testing replicates a real-life cyber attack in all manner and form, from the simulated threat actor not having any internal information to the firm’s very own cybersecurity team also being kept in the dark to best adjudge their real-world response capabilities. Depending on the needs, testing can range from both the parties i.e the penetration tester and the target firm’s cybersecurity firm being informed to none of the parties being informed to either one of the parties being informed.

INDUSTRY 4.0

With this level of flexibility and adaptability, companies can tweak the parameters and the focus of their penetration tests to gauge and remediate the areas of greatest risk. Complex interwoven digital infrastructure is the backbone of modern businesses. With Industry 4.0, this is only bound to accelerate in the near future. There is no doubt that penetration testing is and will continue to be a crucial part of organizational cybersecurity.

HIGHLIGHTING THE THREAT LANDSCAPE

Following every penetration test, an impact report is prepared based on the tools and methodologies used to exploit specific vulnerabilities, this includes the outcome of the said actions and also the duration and extent to which the attacker was able to maintain access. This report provides a clear picture of the level of risk and the potential fallout that could arise from a threat actor utilizing a certain point of entry. Effective penetration testing combined with vulnerability scanning models a comprehensive picture of a firm's cyber threat landscape.

It also helps in identifying and categorizing an organization's data records and digital assets. This includes identifying highly-sensitive intellectual and technical property, sensitive personnel information, client data as well as third-party vendor data. A clear view of the threat landscape helps organizations prioritize security investments to best ensure the safety and security of high-value data.

IMPORTANT COMPLIANCE CONSIDERATIONS

With regulations such as the European Union's GDPR and Singapore's PDPA, managing and protecting client data is an absolute necessity for all businesses. This will not only help organizations adhere to the regulations but also help them achieve and maintain customer trust. With proprietary technology, corporate data, core business operations and supply chain functions all at severe risk to cyber threats increased vigilance is integral to every firm. With increased vigilance, undertaking frequent penetration testing too gains a higher level of importance. Understanding the threat landscape empowers organizations with the knowledge and data required to take the necessary steps in the right direction.

THE VALUE THAT IT BRINGS TO THE TABLE

Penetration testing enables a realistic examination of a company's capability to deal with cyber threats. Tools and techniques that are used by threat actors are replicated in real-time, due to which penetration testing paints a better, more accurate picture of a firm's cybersecurity preparedness.

Furthermore, it helps in framing security policies and procedures in line with regulations and the company's organizational goals. Ensuring cybersecurity is not a one-time done and dusted process. New software updates, changing third-party vendors and evolving data processing systems mean that no system is the same for an extended period of time. With every change, the threat and risk factors too change.

Cybersecurity procedures and methodologies need to be regularly tested and updated to ensure all-round protection to business critical equipment and systems. And, penetration testing is one of the most effective ways to iron out the kinks in your organization's cybersecurity defenses. To stay ahead of your enemy, you need to think like your enemy.

Our Company

We deliver cutting edge security technology solutions and services to our Clients so that they are prepared to tackle the ever growing cyber threat. Through the SubRosa Unified Risk Platform, we deliver threat intelligence, security controls validation and incident alerting and response. We employ and partner with some of the leading risk and security experts in the industry, enabling us to deliver effective services and software solutions to our clients of all sizes, across the globe.

More resources available at: https://subrosacyber.com

SUBROSA
2000 Auburn Dr
Ste 200 #366
Beachwood OH
44122
888.893.1983
info@subrosacyber.com

Since 2017 SubRosa proudly delivers cyber risk advisory and related services to public, private and government clients.

This brochure is to be used as a reference for general information only, and no content contained herein is designed to provide cyber risk professional advice or services.