EITS
Enterprise IT Security

Penetration Testing as a Service

A managed service that identifies your network access vulnerabilities to address the ever-evolving threat landscape.

The Value of Managed Services

Many customers desire to offload the responsibility of certain tasks to an external entity which will provide a higher level of expertise than the job market can afford them. **This shift to "everything as a service" has resulted in significant cost savings in many IT areas, and remedies the following:**

- Difficulties around procurement speed
- Remediation efforts
- Validation
- Training
- Risk guidance

Our customers benefit from the skillsets and contactable resources without the expense of hiring and training new staff.

How Does Our Service Differ From Typical Penetration Testing?

Legacy Penetration Tests had the potential to leave organizations in a frustrating cycle of point-in-time assessments and hurried remediations. Receiving reports with findings was only half of the battle, as even following through on remediation efforts could not guarantee that an organization would be adequately prepared for next year's test - resulting in another round of time consuming work without any real progress being made. ***EITS' Penetration Testing as a Service provides a comprehensive solution which break this cycle and allows businesses to make lasting security improvements over time.***

Continuous Testing Without the Burden of Added Resources

Organizations with extensive resources can employ internal offensive and defensive penetration testing teams that work year-round to detect new attack types. This effective combination of offensive knowledge, represented by "Continuous Testing," and defensive capabilities such as monitoring their environment for attackers right away - termed "Continuous Monitoring" – is critical to identify malicious threats rapidly. ***EITS offers an offensive approach to Continuous Testing tailored explicitly towards these needs, combining security-forward procedures into one seamless package guarantee to increase long-term protection from potential danger.***

(704) 900-8042 www.eits.com info@eits.com

Are You Comfortable with Your

Current Security Posture?

Does your security team have questions?

Though it may not take an entire year to remediate your penetration test findings, the security team probably has questions about the latest exploits and could use help determining the organizations risk exposure. Maybe your security team would like to understand how the exploit takes advantage of a vulnerability that the organization cannot patch so that it can be properly mitigated. It would probably be beneficial to validate that mitigation is working as intended by attempting the exploit in production.

Do you perform Incident Response Tabletop exercises?

If not, you should be. But even if you already are, how applicable are the scenarios to your business? Most times these exercises are purely on paper and give the benefit of doubt to your staff that they will follow the procedures that were meticulously labored over before adoption. A more beneficial approach to these exercises would be to use real compromise scenarios performed during a penetration test to see where the processes broke down in a non-hypothetical way. The lessons learned from that type of effort will be exponentially more helpful than an "on rails" scenario where everything is assumed to have gone perfectly.

What size organization will benefit from this service?

It is EITS' goal to provide the benefits of internal penetration testing teams of larger organizations, to businesses of any size. Customers will be able to reach out to a penetration tester at any time throughout the year – a phone call away. Instead of waiting a full year to identify remaining items to remediate, old findings can be validated immediately upon being addressed. Additionally, testers can learn more about your environment over longer periods of time, which will result in identifying deeper issues and assist in developing a long-term plan to protect your most sensitive information, ensuring that no matter that attack vector, the organizations risk is as low as possible.

When new vulnerabilities are discovered, an exploitation expert is at your disposal to explain the difficulty to execute that attack and even more importantly, how that new vulnerability can be leveraged with older ones to achieve compromise in a way not being reported in the media. This will also remove guesswork in determining impact, as your testing team will perform the exploitation to prove effectiveness.

What kind of budget will this service consume?

For less than the cost of employing a qualified security professional, our customers receive the benefits of an internal testing team. We are offering the capability to perform "Continuous Testing", thereby reducing time to detection of exploitable vulnerabilities, and hopefully beating the attacker to the hole.

What types of tasks can customers leverage with this service?

As customer needs evolve, our service offerings will continue to grow each year. Currently, customers will be able to request the below tasks as a part of this service offering:

- **Table Top IR with scenarios customized for the specific customers environment**
- **Remediation guidance and validation**
- **Purple Team Exercises**
- **Consulting for new technology deployment or network design as it relates to security**
- **Additional highly scoped testing**
- **Training**
- **Prioritization of remediation activities**
- **Applicability assessment for headline snatching vulnerabilities**

(704) 900-8042 www.eits.com info@eits.com

Our white hat hackers target your environment to identify vulnerabilities and fix them before a problem becomes a disaster.

Process Overview

We'll put your security to the test before the hacker does.

Intelligence Gathering

The information-gathering phase of EITS's infrastructure pen testing methodology consists of service enumeration, network mapping, banner reconnaissance, and more. Host and service discovery includes initial domain foot printing, live host detection, service enumeration, and operating system & application fingerprinting.

Threat Modeling

With the information collected previously, security testing transitions to identifying vulnerabilities within systems. During the threat-modeling step, assets are identified and organized into threat categories.

Vulnerability Analysis

The vulnerability analysis phase involves the documenting and analysis of vulnerabilities discovered as a result of the previous infrastructure pen testing steps. At this point, a list of attractive vulnerabilities, suspicious services, and items worth researching further is created and weighted for further analysis.

Exploitation

Exploitation involves actually carrying out the vulnerability's exploit (i.e. buffer overflow) in an effort to determine if the vulnerability is truly exploitable. Exploitation may include, but is not limited to, buffer overflow, SQL injection, OS commanding, etc.

Reporting

The reporting step is intended to deliver, rank, and prioritize findings as well as generate a clear and actionable report, complete with evidence and remediation guidance, to project stakeholders. EITS considers this phase to be the most important, and we take great care to thoroughly communicate the value of our service and findings.

We focus on tailor-fitting the test to each customer's unique needs. Whether you are looking for a white box, black box, or grey box test, EITS will meet you where you are today. We will customize our offering for purple team, red team, or blue team to ensure successful testing.

GDSA · GCED · GICSP · GCUX · GCFE · GCIH · GPEN · GWAPT · GSEC · GCWN · MCFE · CNDA (Certified Network Defense Architect) · CEH (Certified Ethical Hacker)

(704) 900-8042 www.eits.com info@eits.com