EITS
Enterprise IT Security

Penetration Testing

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

Process Overview

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 ingerprinting. The purpose of this step is to collectively map the in-scope environment and prepare for threat identification.

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.

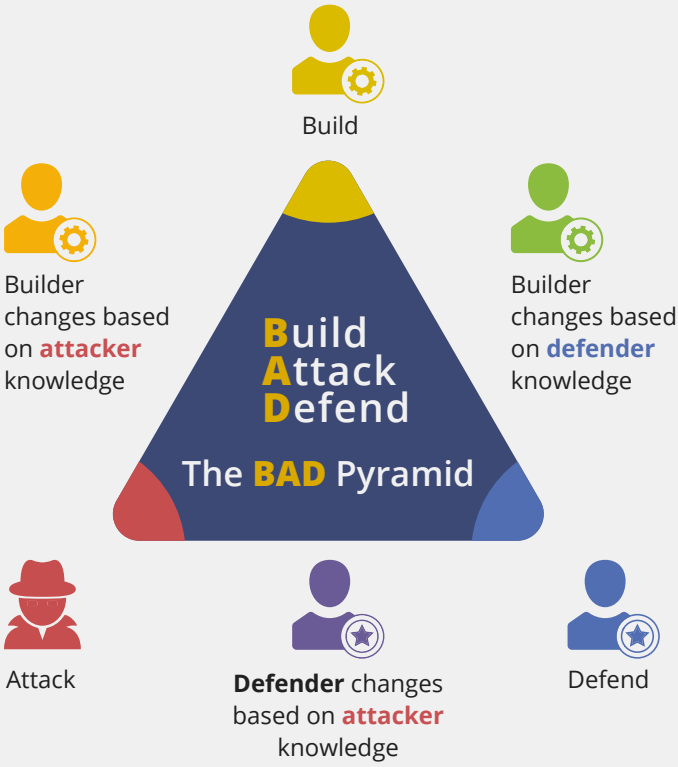
Exploitation

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.

Real World Testing Scenarios to Meet Your Organizations Needs



The EITS Difference

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.

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

Are you on the right track with your security posture?

Do you you want to know about your weaknesses before an attacker does?

- Penetration testing is a methodical assessment of your security controls that can help identify weakness and prioritize your organization's security plan for the future.
- Penetration testing is a methodical assessment of your security controls that can help identify weakness and prioritize your organization's security plan for the future.

Do you know you have weaknesses but are unable to quantify the risk?

- We will work with you to create tailored use cases and perform goal-oriented testing that can demonstrate the significance of being compromised.
- Many customers need an outside point of view to help justify security improvements.

Are you already laser focused on defending your network?

- If not, don't worry; It's our job to think like attackers.
- We draw from real-world incident response experience in addition to our pen test experience to emulate attacker methodologies and mindsets.

Are you confident your modern & legacy security mitigation technologies are optimized?

- Implementing a new security-in-a-box solution introduces more possibility for misconfiguration.
- We can help you evaluate the current return on your security investments.
- All of the NextGen products on the market won't save you from fundamental weaknesses in outdated protocols that aren't disabled by default.

Do you know how Ransomware would affect you?

- Most organizations do not realize that they have loose file permissions until it is too late.
- Let us show you the impact of allowing your users to run any program they want.
- We can validate whether backups are stored offline to protect data from ransomware encryption.

Would you know if the crown jewels left your network?

- We can demonstrate multiple ways to exfiltrate data out of your network and help you create alarms so you can respond quickly.

Do you want a REALISTIC table top scenario?

- Everybody has a plan on paper. Things happen quite differently in the heat of the incident.
- Let us perform a simulated attack and truly test your procedures and the humans behind them.

Would you like a second set of eyes on your Vulnerability Management, Patch Management, or Asset Management programs?

- It is common to inform customers of vulnerable systems that they did not know they had.
- Many times customers believe that remediation steps have been performed, only for us to discover that they were not adequate or complete.

Think you have enough monitoring or visibility?

- We will communicate to you exactly how we did it, and where you can look to find us in your network!
- We enjoy improving our customer's detection capabilities by working together in real time during engagements.

Verified skills produce real results.

GCED GDSA GCWN GSEC GCIH GWAPT GPEN GCFE MCFE CNDA Certified Network Defense Architect CEH Certified Ethical Hacker

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