Espada Tech Ltd
Plot 1829 Bukoto
Kampala, Uganda
P.O Box 3415

Contact
info@espadatech.io
www.espadatech.io
+256 703 768685

Espada Tech Security Services

Offensive Security Refined

Company Headquarters

Espada Tech Limted
Plot 1829 Bukoto, Kampala, Uganda
P: +256 703768685
E: info@espadatech.io

Last Update
May 10, 2016

Version 1.13

ESPADA TECH

Contents

1. Overview

The primary objective for a comprehensive penetration test is to identify exploitable vulnerabilities in networks, systems, applications, hosts and network devices (ie: routers, switches) before hackers are able to discover and exploit them. Comprehensive penetration testing will reveal real-world opportunities for hackers to be able to compromise systems and networks in such a way that allows for unauthorized access to sensitive data or even take-over systems for malicious/non-business purposes.

This type of assessment is an attack simulation carried out by our highly trained security consultants in an effort to:

- Identify security flaws present in the environment
- Understand the level of risk for your organization
- Help address and fix identified network security flaws

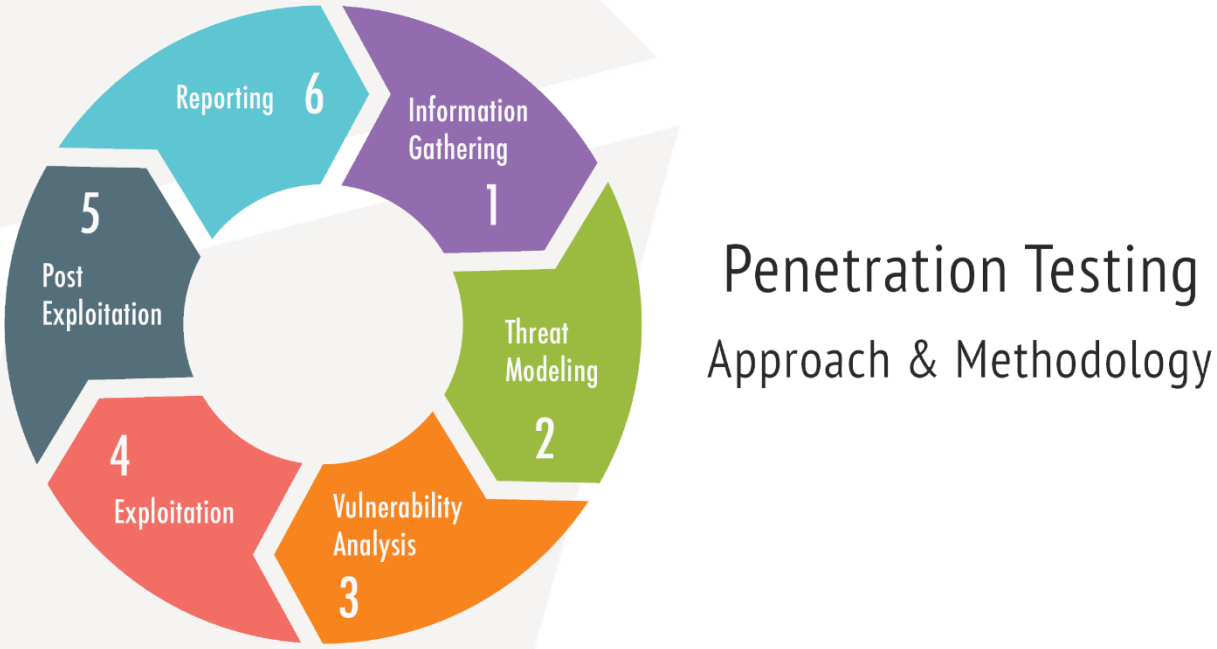
Espada Tech's expert penetration testers have had experience supporting network, applications, systems and hosts —not just trying to break them. They leverage this experience to zero in on critical issues and provide actionable remediation guidance.

As a result of our penetration tests, you'll be able to view your systems through the eyes of both a hacker and an experienced network security professional to discover where you can improve your security posture. Our consultants produce findings in written reports and provide your team with the guidance necessary to effectively remediate any issues we uncover.

Plot 1829 Bukoto. Kampala | P.O Box 3415 | +256 791494647 +256 703768685 | info@espadatech.io | www.espadatech.io

2. Approach

Espada Tech's penetration testing service utilizes a comprehensive, risk-based approach to manually identify critical application and network-centric vulnerabilities that exist on all in-scope networks, applications, systems and hosts.



Using this industry-standard approach, Espada Tech's comprehensive method covers the classes of vulnerabilities in the Penetration Testing Execution Standard (PTES) and the Information Systems Security Assessment Framework (ISSAF) including, but not limited to: CDP attacks, MIME testing, DNS enumeration/AXFR, SMTP relay, SNMP recon, port security, brute force, encryption testing and more.

Manual Testing Vs Automated Testing

Espada Tech's approach consists of about 80% manual testing and about 20% automated testing – actual results may vary slightly. While automated testing enables efficiency, it is effective in providing efficiency only during the initial phases of a penetration test. At Espada Tech, it is our belief that an effective and comprehensive penetration test can only be realized through rigorous manual testing techniques.

Plot 1829 Bukoto. Kampala | P.O Box 3415 | +256 791494647 +256 703768685 | info@espadatech.io | www.espadatech.io

Tools

In order to perform a comprehensive real-world assessment, Espada Tech utilizes commercial tools, internally developed tools and the same tools that hacker use on each and every assessment. Once again, our intent is to assess systems by simulating a real-world attack and we leverage the many tools at our disposal to effectively carry out that task.

Reporting

We consider the reporting phase to mark the beginning of our relationship. Espada Tech strives to provide the best possible customer experience and service. As a result, our report makes up only a small part of our deliverable. We provide clients with an online remediation knowledge base, dedicated remediation staff and ticketing system to close the ever important gap in the remediation process following the reporting phase.

We exist to not only find vulnerabilities, but also to fix them.

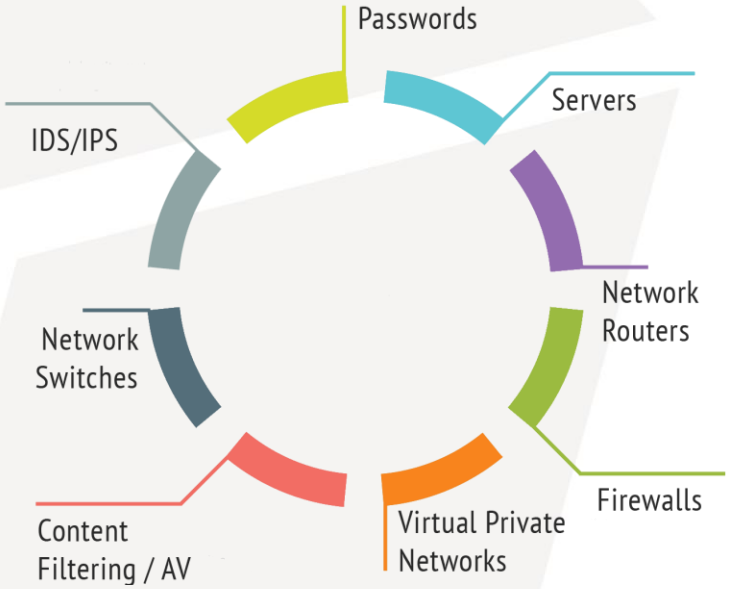
Remediation & Re-testing

Simply put, our objective is to help fix vulnerabilities, not just find them. As a result, remediation re-testing is always provided at no additional cost.

Plot 1829 Bukoto. Kampala | P.O Box 3415 | +256 791494647 +256 703768685 | info@espadatech.io | www.espadatech.io

3. Methodology

Each and every network penetration test is conducted consistently using globally accepted and industry standard frameworks. In order to ensure a sound and comprehensive penetration test, Espada Tech leverages industry standard frameworks as a foundation for carrying out penetration tests. At a minimum, the underlying framework is based on the **Penetration Testing Execution Standard (PTES)** but goes beyond the initial framework itself.



Intelligence Gathering

The information-gathering phase consists of service enumeration, network mapping, banner reconnaissance and more. Host and service discovery efforts results in a compiled list of all accessible systems and their respective services with the goal of obtaining as much information about the systems as possible. Host and service discovery includes initial domain foot printing, live host detection, service enumeration and operating system and application fingerprinting. The purpose of this step is to collectively map the in-scope environment and prepare for threat identification.

Threat Modelling

With the information collected from the previous step, security testing transitions to identifying vulnerabilities within systems. This begins with automated scans initially but quickly develops into deep-dive manual testing techniques. During the threat-modelling step, assets are identified and categorized into threat categories. These may involve: sensitive documents, trade secrets, financial information but more commonly consist of technical information found during the previous phase.

Plot 1829 Bukoto. Kampala | P.O Box 3415 | +256 791494647 +256 703768685 | info@espadatech.io | www.espadatech.io

Vulnerability Analysis

The vulnerability analysis phase involves the documenting and analysis of vulnerabilities discovered as a result of the previous steps. This includes the analysis of out from the various security tools and manual testing techniques. At this point, a list of attractive vulnerabilities, suspicious services and items worth researching further has been created and weighted for further analysis. In essence, the plan of attack is developed here.

Exploitation

Unlike a vulnerability assessment, a penetration test takes such a test quite a bit further specifically by way of exploitation. Exploitation involves actually carrying out the vulnerability's exploit (ie: buffer overflow) in an effort to be certain if the vulnerability is truly exploitable. During an Espada Tech penetration test, this phase consists of employing heavy manual testing tactics and is often quite time-intensive.

Exploitation may include, but is not limited to: buffer overflow, SQL injection, OS commanding and more…

Reporting

The reporting step is intended to deliver, rank and prioritize findings and generate a clear and actionable report, complete with evidence, to the project stakeholders. The presentation of findings can occur via Skype or in-person – whichever format is most conducive for communicating results. At Espada Tech, we consider this phase to be the most important and we take great care to ensure we've communicated the value of our service and findings thoroughly.

We're not done yet…

We consider the reporting phase to mark the beginning of our relationship. Espada Tech strives to provide the best possible customer experience and service. As a result, our report makes up only a small part of our deliverable. We provide clients with an online remediation knowledge base, dedicated remediation staff and ticketing system to close the ever important gap in the remediation process following the reporting phase.

We exist to not only find vulnerabilities, but also to fix them.

Plot 1829 Bukoto. Kampala | P.O Box 3415 | +256 791494647 +256 703768685 | info@espadatech.io | www.espadatech.io

4. Deliverable

At Espada Tech, we consider the Delivery / Reporting phase to be the most important and we take great care to ensure we've communicated the value of our service and findings thoroughly. The deliverable consists of an electronic report that includes several key components including, but not limited to: Executive Summary, Scope, Findings, Evidence, Tools and Methodology. In addition to the report, a raw file in comma-separated value (CSV) format is also provided in an effort to optimize the remediation and management of any identified findings.

Findings are communicated in a stakeholder meeting and typically presented in-person or virtually via Skype — whichever medium is most conducive for communicating results effectively. During this time, Espada Tech consultants will walk through the report, in detail, to ensure all findings and their corresponding description, risk rating, impact, likelihood, evidence and remediation steps are thoroughly understood. While this typically involves a single meeting, there is no limitation to that number. The key underlying message is that all information is clearly understood and that a roadmap toward remediation / mitigation is crystal clear.

Components

Some of the key components to our network penetration test deliverable include, but are not limited to:

- Scope
- Control Framework (i.e: OWASP, PCI, PTES, OSSTMM)
- Timeline
- Executive Summary Narrative
- Technical Summary Narrative
- Report Summary Graphs
- Summary of Findings
- Findings (Description, Business Impact, Recommendation, Evidence, References, CVSS, Risk Rating Calculation)
- Methodology and Approach
- Risk Rating Factors
- Tools

Plot 1829 Bukoto. Kampala | P.O Box 3415 | +256 791494647 +256 703768685 | info@espadatech.io | www.espadatech.io

5. Frequently Asked Questions

Why should I conduct a penetration test?

A penetration test is a simulated attack from the perspective of a bad actor, such as a malicious hacker. The objective is to simulate a cyber security attack and attempt to uncover security vulnerabilities that might otherwise be discovered by hackers. In doing so, you would gain valuable insight into the security posture of the in-scope assets and be able to fix them before hackers are able cause serious damage by exploiting them.

How long does it take to conduct a penetration test?

The overall time depends on the size and complexity of the in-scope network(s) and application(s). That said, most tests take anywhere from one week to four weeks, start to finish.

How much does a network penetration test cost?

We get this question a lot and it's not easy to answer until some level of scoping has been performed. Our scoping process is quick and painless. But overall, the complexity of the application(s), network(s), or both will ultimately determine its cost. For example, when determining the work effort, we take the following into account: number of live IP addresses, etc.

What's the difference between a Penetration Test and a Vulnerability Assessment?

We get this question a lot as well. Short answer: Exploitation and Post-Exploitation. Vulnerability assessments do not involve Exploitation while penetration testing goes well beyond a vulnerability assessment and into Exploitation and Post-Exploitation phases.

Request a free penetration test scope assessment today by sending an email to security@espadatech.io

Plot 1829 Bukoto. Kampala | P.O Box 3415 | +256 791494647 +256 703768685 | info@espadatech.io | www.espadatech.io