CYBERTECH360
SECURITY · MONITORING · MANAGEMENT

Penetration Testing

Find Any Holes in Your Cyber Security?

Our Pen Testing will!

Overview: The benefits of risk mitigation, compliance, business reputation, cost saving, and competitive advantage make penetration testing a worthwhile investment.

Features: Penetration testing, also known as "pen-testing," is a method of evaluating the security of a computer system or network by simulating an attack on known software vulnerabilities.

As technology continues to evolve, new vulnerabilities will arise that can be exploited by bad actors or simply by Sam in the warehouse.

By regularly conducting pen testing, your organization can stay ahead of these threats and ensure the ongoing security of critical systems.

Once the testing is complete, we then provide a report that outlines the vulnerabilities found, along with recommendations on how to address them. This information can then be used to plan and improve the security of the systems and reduce the risk of a cyber attack.

Alleviate Your Aggravations

1-833-362-9237

CYBERTECH360

What Are the Different Types of Reports Available?

Executive Reports

- The executive summary serves as a high-level view of both risk and business impact in plain English. This report helps non-technical business leaders gain insight into the security concerns highlighted in the report. The consolidated report combines the Executive Summary, Technical and Vulnerability reports into one PDF.

Technical Reports

- The technical reports will identify risks and their potential impact. These reports will give you multiple remediation options that are detailed enough to prepare an IT team for a swift resolution.
- Supporting Evidence
- These are reports that provide additional evidence to the testing results and activities. You can use the raw data provided in these deliverables to conduct further investigation or validate findings.

Overview

- In vPenTest, we try to present as many reports as possible to help our partners dissect the information that's necessary for them to take action. The deliverables that are available depend on the type of assessment you've run.

Consolidated Report

- The consolidated report is essentially all the reports combined into one. Rather than downloading separate PDF documents, it may be more useful for your team to review the report in one single consolidated report.
- One thing that you should note, however, is that when using the consolidated report, the number of pages can grow significantly due to the vulnerability assessment results.

Executive Summary

- The executive summary report is more of a high-level report that talks about the penetration test findings without getting too technical. Using the executive summary, you can find information about the following:

Overall scope of work

- Engagement statistics (e.g. number of compromised users, overall severity rating, number of activities, etc.)
- Overall number of penetration test and vulnerability assessment findings by severity rating
- Summaries of the penetration test findings
- A remediation roadmap

Technical Report

- The technical report contains a significant amount of more details than the executive summary. The technical report is broken up into the following components:
- Penetration Test Narrative: Details about each step of the penetration test, from start to finish.
- MITRE ATT&CK: A list of cross-referenced MITRE TTPs that were executed as part of the penetration test.
- Findings: A break down of each finding, including their description, recommendations, references, supporting evidence, etc.
- Activity Log: A detailed breakdown of each single activity performed on the penetration test, organized by time stamp.

Vulnerability Assessment

- The vulnerability assessment report is basically a branded report that contains all of the vulnerability assessment results. These reports are going to usually be a lot more detailed in terms of findings, due to just the nature of vulnerability assessments.

Supporting Evidence

- We try to include as much supporting evidence as possible along with all the assessments that we deliver. This includes vulnerability output files, any outputs from all the tools that we've discovered, and more. This is significantly helpful for teams that are interested in diving deeper into the results to understand how we were able to discover some of the findings that we identified.

Contact us today