

HAWK Network Defense, Inc.

Incorporating Advanced Penetration Testing for Your Security Response



Protection for the Enterprise

The HAWK Network Defense, Inc. (HAWK) penetration testing team uses security best practices to identify weaknesses in the client's internal and external infrastructure. By utilizing advanced methods, the HAWK penetration testing team helps You evaluate your externally facing security, as well as their internal security posture.

External Penetration Testing

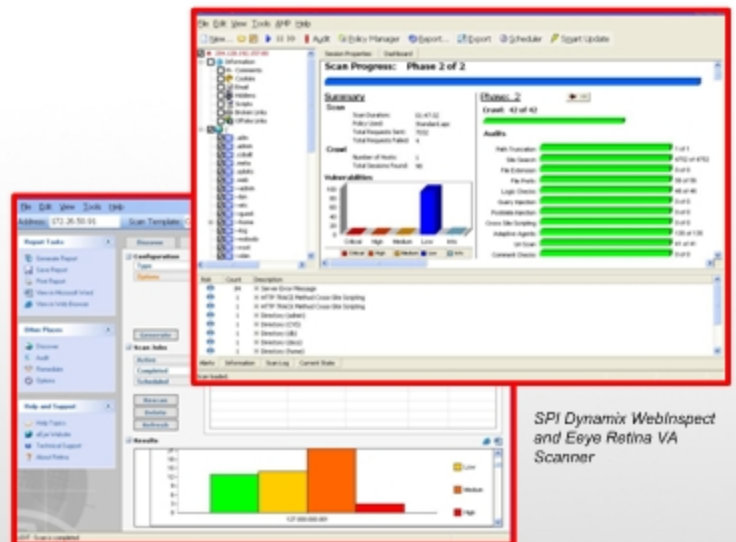
External Intrusion Testing and Analysis identifies security weaknesses and strengths of the client's systems and networks as they appear from outside the client's security perimeter, usually from the internet.

The goal of the External Intrusion Testing and Analysis is to demonstrate the existence of known vulnerabilities that could be exploited by an external attacker.

Internal Penetration Testing

Internal Intrusion Testing and Analysis identifies security weaknesses and strengths of the client's systems and networks as they appear to internal users, operating within the client's security perimeter. The goal of the Internal Intrusion Testing and Analysis is to demonstrate the existence or absence of known vulnerabilities that could be exploited by internal users.

Internal Intrusion Testing and Analysis mimics an attack on the internal network by a disgruntled employee or an authorized visitor having standard access privileges.



SPI Dynamix Webinspect and Eye Retina VA Scanner

Client Benefits

External and Internal Testing and Analysis allow the client to anticipate external/internal attacks that might cause security breaches and to proactively reduce risks to its information, systems and networks.

This will ensure that the client are able to conduct operations with increased confidence in their ability to protect valuable data, resources and reputation, as well as satisfy industry audit requirements.

Client Deliverable

The HAWK penetration team will deliver an advanced Analysis report containing an executive security overview, list of security threats, recommendations for risk mitigation, as well as our logs of compromised data obtained during the audit.

Software

Software

SPI Dynamix WebInspect
Eyee Retina VA Scanner
Immunity CANVAS
Metasploit
Advanced Software

Details

Web Application Scanner, currently the industry leader
System/Service Vulnerability Scanner
Exploitation Framework
Open Source Exploitation Framework
Internally developed software for exploitation and testing



OSSTMM is the industry standard for penetration testing

Methodologies

Methods

OSSTM
OWASP

Details

Open Source Security Testing Methodology (Industry Standard)
Open Web Application Security Project (Industry Standard Methodology)

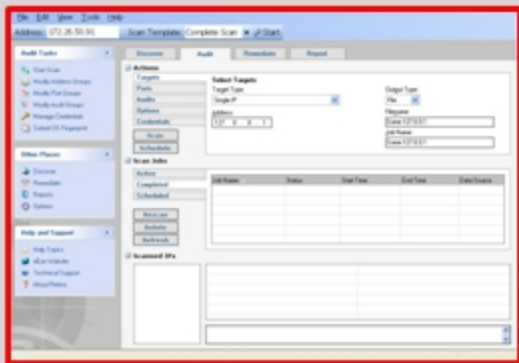
Service Methodology

HAWK's skilled security professionals will perform tests, analysis, scans and attack procedures from the Internet and internal networks against contracted client locations. All activities are conducted during client specified times over a predetermined evaluation period.

The HAWK Assessment team uses a testing methodology that mimics the process used by hackers to gain access to information and systems at the client's site. The methodology combines state-of-the-art testing techniques with unique security expertise to provide the client with an independent assessment of its security posture.

Our security professionals use a set of evaluation tools - public domain, commercial and others, to gather vulnerability information. Intrusion attempts are then performed using proprietary testing techniques. All known network-based attacks are employed in this process.

The HAWK Assessment team is dedicated to the use of the OSSTMM penetration testing methodology and use the OWASP standards for testing web applications. These are the industry-leading standards and practices.



Eyee Retina VA Scanner

Penetration Team Credentials

The HAWK penetration team has extensive experience in penetration testing, vulnerability discovery and creation of exploit proof of concept code, with over 20 years of combined experience in all facets of security exploitation and penetration testing.

All staff members of the HAWK penetration team have the following experience.

Coding – All HAWK team members have extensive experience in C, C++, Perl, Python, Assembly programming languages as well as expert knowledge in web application languages such as ASP, HTML, Java, PHP and more.

Vulnerability Discovery – HAWK team members are credited with the discovery of several previously unknown vulnerabilities, to include exploits of FTP servers, Email servers, Web servers, as well as local root exploits on several different operating systems such as Linux, FreeBSD and Windows OS systems.

Penetration Testing – All HAWK team members have conducted penetration testing and vulnerability testing on all types of network topologies. This include wireless security auditing and penetration, VPN audits, network equipment testing on switches and routers, firewall testing and internal/external black box methods.