



What do you think of when you hear the word “hacker?” For most, the word congers up images of someone breaking into a computer system or network with malicious intent. However, not all hackers are bad. “Good” hackers are professionals that identify and report computer network security vulnerabilities to management, hopefully *before* weaknesses are exploited and bad hackers can do harm.

The procedures used by “good” hackers attempting to successfully break into computer systems are called penetration tests (PenTests). A PenTest is the authorized, scheduled and systematic process of identifying and exploiting known security vulnerabilities with the primary objective of gaining access to a computer host, network or application.

Under the current regulatory environment, periodic PenTests are an integral part of an organization’s information security program. Penetration testing plays an essential role in mitigating risks associated with network and systems vulnerabilities and demonstrating due diligence in the area of information technology governance.

Penetration Testing



Let good hackers
test your network
before bad hackers
can do harm



Penetration Testing

A penetration test (PenTest) is the authorized, scheduled and systematic process of identifying and exploiting known security vulnerabilities with the primary objective of gaining access to a computer host, network or application. The following procedures comprise the main steps of a PenTest:

- ▲ Footprinting: to identify public IP addresses that may be targeted by hackers
- ▲ Subnet Scanning: to identify systems within those IP addresses that may be potential targets for hackers
- ▲ Enumeration: to gather information about the available attack routes
- ▲ Vulnerability Scan: to audit discovered systems for known vulnerabilities
- ▲ Gaining Access: to penetrate systems and define potential attack impact
- ▲ Collecting Evidence: to document a successful unauthorized access or attack
- ▲ Recommendations: to educate on how to eliminate, mitigate or minimize impact of exploits for detected vulnerabilities

Periodic PenTests are an integral part of an organization's information security program. Penetration testing plays an essential role in mitigating risks associated with network and systems vulnerabilities and demonstrating due diligence in the area of information technology governance.



Let good hackers
test your network
before bad hackers
can do harm



Penetration Testing

Can individuals outside your organization gain access to confidential customer and company data? Is your organization at risk of unauthorized access of this critical data for malicious intent by hackers? A penetration test (PenTest) by PKM creates a profile of your organization's systems that can be "seen" from the Internet. This profile is an important indicator of your organization's vulnerability to hacker attack. A PenTest will not only enlighten you on the systems that can be attacked, but also the information potential hackers can gain from these systems.

A PenTest is the authorized, scheduled and systematic process of identifying and exploiting known security vulnerabilities with the primary objective of gaining access to a computer host, network or application. Periodic PenTests are an integral part of an organization's information security program. Penetration testing plays an essential role in mitigating risks associated with network and systems vulnerabilities and demonstrating due diligence in the area of information technology governance.



Let good hackers
test your network
before bad hackers
can do harm

Porter Keadle Moore, LLP (PKM) is a full-service accounting and consulting firm that provides accounting, auditing, tax, information technology, risk advisory and management consulting services to clients throughout the country. PKM's Risk Advisory group is committed to information technology integrity and offers a number of attest and consulting services for financial service firms, such as banks, insurance companies and broker-dealers, and to companies that provide outsourced services to financial service firms.

Specializing in Penetration Testing, TG-3 ATM audits, Network Vulnerability Assessments, Information Technology General Control reviews, Management Information Systems reviews, SAS 70 reports and e-commerce/Internet banking reviews, PKM's experienced technology professionals provide clients with the expertise and skills necessary to comprehend current regulatory and technology environments while helping them maximize resources, enhance operating efficiency and improve the bottom line.

For more information contact:

Warren Puy Arena
Porter Keadle Moore, LLP
wpuyarena@pkm.com
404-420-5684

Visit www.pkm.com to learn more.



Porter Keadle Moore, LLP
235 Peachtree Street, NE
Suite 1800
Atlanta, GA 30303