PENETRATION TESTING

Today's evolving and sophisticated technologies have increased risks such as cyber-vandalism, intellectual piracy and hacking. Protecting your systems and data requires rigorous testing of security features.

Accume's security review identifies controls, sensitive resources and databases and vulnerabilities in your internal and extrernal networks. We then deploy a comprehensive methodology that is customized to your institution's specific needs and infrastructure.

Our Network Penetration Testing services include:

- Services & Databases Using Default Accounts
- Windows Enumeration
- SNMP Information Gathering
- Web Attacks/Session Hi-jacking
- DNS Attacks
- Denial of Service Attacks
- Buffer Overflow Attacks
- Password Cracking
- Gaining Access
- Escalating Privilege
- Advanced Browser Exploitation

PENETRATION TESTING OPTIONS

- **Black Box (Zero-Knowledge Based)**
  - Applies to external assessments only
  - Client provides their organization's name
  - Detailed footprinting phase
  - Target all hosts identified during footprinting
- **Grey Box (Minimal Knowledge)**
  - Applies to external and internal assessments
  - Description of infrastructure provided
  - Limited footprinting phase required
  - Client provides scoping of targets
- **White Box (Knowledge Based)**
  - Applies to external and internal assessments
  - Description of infrastructure provided
  - No footprinting phase necessary
  - Client provides a list of IP addresses to target

TO LEARN MORE, PLEASE CONTACT:
Michael Barrack, Managing Director
702.461.8682 or **mbarrack@accumepartners.com**