**Effective penetration testing involves modeling the activities of real-world attackers with the goal of better understanding and managing business risk to improve an organization's security stance.**

Real-world attackers undermine modern organizations in a variety of ways, so penetration testers need to be prepared to draw from a variety of different attack types, tools, and techniques to simulate the activities of real-world attackers. Skilled penetration testers are familiar with numerous different attack types, and strive to build and reinforce their capabilities in each of these areas. Each diagram on this poster shows how different penetration testing techniques and tools can be applied to assessing the security stance of the same organization's infrastructure.

---

**Related SANS Courses:**
- **SEC560**
- **SEC561**
- **SEC562**
- **SEC563**
- **SEC575**
- **SEC617**
- **SEC618**
- **SEC632**
- **SEC660**
- **SEC680**
- **SEC700**

---

**Tools and Techniques Applied:**
- **Hashcat, Asleap & Pass the Hash (Step 8)**
- **Mimikatz (Step 6)**
- **HostAP-WPE (Step 7)**
- **Ruby, Metasploit & Meterpreter (6)**
- **AIreplay-ng (Step 2)**
- **cpscam (Step 2)**
- **WinDbg & Fuzzing (Step 1)**
- **Elcomsoft Phone Password Recovery for iOS (Step 9)**
- **Configuration Utility (Step 9)**

---

**Related Websites:**
- [Free Pen Testing Resources](https://www.sans.org/blog)
- [Pen-testing.sans.org/blog](https://www.pentesting.sans.org/blog)

---

**Twitter:** @SANSPenTest