Info@Risk via David Trepp

*Table of Services*

**Comprehensive Penetration Test** – Penetration

**Implement Risk Assessment Methodology** – Risks

**Information Security Program Review -** Secure Data

**Information System Controls Audit –** Audits

**Device/System Configuration Review** – Installation and Testing

**Application Penetration Test –** Vulnerabilities

**Wireless Network Topography Assessment** – Network Maps and Frequencies

Compliances

NIST, HIPAA, PCI, GLBA, SOX,

CIA

Confidentiality – Data that is kept secret

Integrity – Data that is kept the same

Availability – Data that is quick to use

(Red Team Field Manual)

Application or Infrastructure Experience

Infrastructure Testing vs Application Testing

Application testing examples – Banking website or UI, Healthcare utilities, POS systems, CMS applications

BlackHat (Mandalay Bay hotel in Las Vegas, 2015 – August 1st – 4th)

https://www.blackhat.com/us-15/ - Black Hat USA 2015

https://www.blackhat.com/us-15/briefings.html - Briefing

DEFCON (Paris and Bally’s in Las Vegas, 2015 – August 6th – 9th)

https://media.defcon.org/ - Old conferences

https://forum.defcon.org/ - Forums

https://www.defcon.org/html/links/dc-goons.html - DEFCON Goons

https://www.defcon.org/html/links/dc-faq/dc-faq.html - DEFCON FAQ

https://www.defcon.org/html/links/dc-torrent.html - All DEFCONS

https://www.defcon.org/html/links/dc\_press/dc\_press.html - 2015 DEFCON Subjects

https://www.defcon.org/html/links/mailing-lists.html - DEFCON Mailing List

The Five Stages of Ethical Hacking

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Covering Tracks

Other Resources

*CEH Certified Ethical Hacker PFD Kimberly Graves PDF*  
Ethics, Reconnaissance and Fingerprinting, Network Information and Scanning, Password Cracking and Privilege escalating, Malware and Backdoors, Additional Sniffing, Denial of Service and Session Hijacking, Google Hacking and Web Vulnerabilities, SQL Injection and Buffer Overflows, Wireless Network Hacking, Physical Security, Hacking Linux, Honeypots and Firewalls, The Penetration Test

*Spy Kit*

Cain – ARP poisoning, enumeration (WindowS), sniffing, password cracking

Tcpdump – Sniffing

Hunt – Session hijacking

Sam Spade – WHOIS, Traceroute

Netstat – Trojans

Splunk – Audit logs

Windows Live CD

Laptop with Kali Linux and Putty/Telnet

Wifite/Aircrack-ng

?: Helix, Kleopatra, TFTP32, IZarc