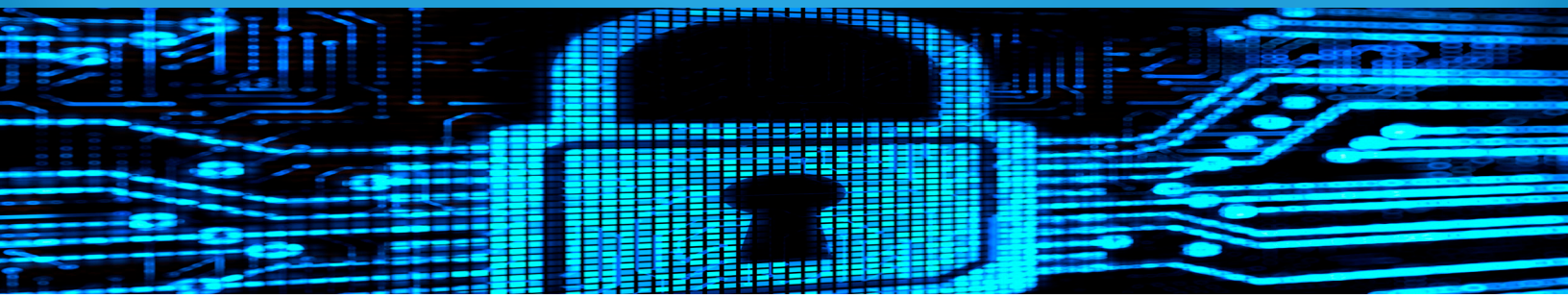
HoganTaylor LLP
CPAs + ADVISORS



RISK ASSURANCE: NETWORK ATTACK & PENETRATION SERVICES

Network pentests attack the actual network devices such as firewalls, routers, printers, servers and workstations as well as users. In a network pentest, the objective for the HoganTaylor team is to break into a network and determine the amount of damage possible with the weaknesses found. Once an external device is compromised and gives access to the internal network, the HoganTaylor team will continue probing the internal network to determine just how far an intrusion can go.

HoganTaylor has a signature Three Phase Pentest. The three-phased test takes three to four weeks to complete and includes the following testing activities.

PHASE I

During phase 1, the HoganTaylor team is given the name of the company and an emergency contact. A HoganTaylor employee separate from the testing team will be the gatekeeper during phase 1. As the testing team identifies possible external devices within the scope of the attack, they are validated to ensure the device is owned by the target and within the scope of the audit. This phase emulates a true external hacker.

PHASE II

During phase 2, the HoganTaylor team is given a list of target IP addresses and a brute force attack is started. This phase is a gray box test and more closely emulates an attack from someone who has a relationship with the target network, such as a vendor or customer.

During phase 2, social engineering testing is also started. This is designed to test the human component and awareness of security. An attempt to gain access to the target network will be made by sending realistic looking emails to employees to trick someone into revealing information that can be used to attack systems or networks. This type of attack will put your employee's information security training to the test. When a social engineering element is added to a pentest, it provides a look into how your staff will respond that can't be foreseen with a survey or training quiz. More importantly, it gives the organization a better understanding of what could happen if they are not careful and guarded with the access with which they have been entrusted. There is a saying in the Navy that goes back to World War II: "Loose lips sink ships.", but until it is made real to people they will not understand the saying and its consequences.

PHASE III

During phase 3, the HoganTaylor team is allowed to see any required platform/configuration documentation necessary and ask relevant questions of the network administrators or management to complete the engagement. This phase is important to ensure all of the devices within the scope of the engagement have been tested.

THE BENEFITS OF OUR THREE-PHASE METHODOLOGY

By using the three-phased methodology, HoganTaylor can show what level of compromise could be achieved by each of the vantage points discussed above.

In the final report, HoganTaylor will list and discuss all vulnerabilities found, the extent to which those vulnerabilities were exploited, and the extent to which those vulnerabilities can be expected to be exploited in the real world. In the report, a complete list of methods and tools used for the test will be provided, as well as discussion about each method or tool's usefulness and functionality as it pertains to weakening or defeating your network defenses.

NETWORK ATTACK & PENETRATION SERVICES LEADERSHIP

Cody Griffin,
CPA, CITP, CISA

Cody Griffin leads HoganTaylor's Attack & Penetration services team. Mr. Griffin has more than 14 years of experience in both public and private industry.

Mr. Griffin began his career in PriceWaterhouseCooper's risk assurance and advisory practice. In the years since, he has gained industry experience in information technology, telecommunications, retail, financial institutions, energy, higher education and transportation.

As a member of the firm's Risk Assurance practice group, Mr. Griffin also practices Sarbanes-Oxley (SOX) Section 404, IT audit, business process reviews, service organization control (SOC) reports, fraud reviews, agreed upon procedures, internal audit assurance services and compliance audits.

YOUR ATTACK & PENETRATION SERVICES TEAM

The Network Attack and Penetration team consists of certified professionals with extensive experience with TCP/IP, networking, and OS knowledge; advanced knowledge of network and system vulnerabilities and exploits; knowledge of techniques to evade security detection. Our personnel have backgrounds in conducting assessments for the Department of Defense, law enforcement, and the private sector.

ABOUT HOGANTAYLOR

HoganTaylor is one of the largest public accounting firms in Oklahoma and Arkansas. In addition to Risk Assurance services, HoganTaylor has many other practice groups made up of knowledge experts in important, highly specialized areas of accounting.

SERVICES

- Accounting Solutions
- Advisory
- Assurance
- Business Valuation
- Employee Benefit Plans
- Human Capital
- Information Technology
- Litigation Support
- Outsourced CFO Services
- Risk Assurance
- Tax
- Wealth Management

INDUSTRIES

- Collective Investment Funds
- Construction
- Energy
- Financial Institutions
- Insurance
- Manufacturing & Distribution
- Nonprofit
- Retail
- Transportation

BDO ALLIANCE USA

HoganTaylor is an independent member of the BDO Alliance USA and is able to access the resources of BDO USA, LLP and its trusted network throughout the world.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA

CONTACT INFORMATION

For additional information about HoganTaylor's Network Attack & Penetration services, please contact Cody Griffin at cgriffin@hogantaylor.com or 501.227.4343.

HoganTaylor LLP
CPAs + ADVISORS

hogantaylor.com

TULSA

2222 South Utica Pl., Ste. 200
Tulsa, OK 74114
Phone: 918.745.2333

OKLAHOMA CITY

11600 Broadway Ext., Ste. 300
Oklahoma City, OK 73114
Phone: 405.848.2020

FAYETTEVILLE

688 East Millsap Rd., Ste. 203
Fayetteville, AR 72703
Phone: 479.521.9191

LITTLE ROCK

11300 Cantrell Road, Suite 301
Little Rock, AR 72212
Phone: 501.227.5800