



“Partnership with Integrity”™

NETWORK SECURITY REVIEWS & VULNERABILITY ASSESSMENTS

Network Security Reviews, Penetration Tests, Intrusion Detection Routines and Vulnerability Assessments can identify areas within your organization’s IT infrastructure that are susceptible to security breaches and potential financial loss, regulatory fines and penalties, lost productivity, and/or embarrassing publicity.

ALP’s **Vulnerability Assessments and Security** reviews focus on nine key areas designed to expose the flaws of a network infrastructure:

- **Access Controls Systems & Methodology**
- **Security Management Practices**
- **Security Architecture**
- **Physical Security**
- **Operations Security**
- **Application Development Security**
- **Telecommunications, Network & Internet Security**
- **Cryptography**
- **Business Continuity Planning**

Our penetration testing services follow a three- tiered approach, consisting of **Discovery, Assessment and Exploitation**.

During the Discovery phase we attempt to discern as much information as we can about the topography of your network. One of the first steps we take is to do an external penetration test using commercial software and easily obtainable (public domain) information about your company. We determine whether or not you are paying attention to these attacks and reviewing the associated logs. All identified domain names and IP addresses are verified prior to moving on to the Assessment phase. We also complete “Whois” queries, zone transfers, ping sweeps, and traceroutes on several blocks of IP addresses. The traceroutes will help us identify routers, firewalls and gateways. We identify all connections to the Internet, some may be unknown to network managers.

The Assessment phase identifies all security holes and vulnerabilities of your network. We document all target hosts, along with Operating System, IP Addresses, Applications, Banner Information and Known

Vulnerabilities. This provides us with the amount of information a hacker can obtain about your company prior to compromising the network.

Once the Operating System is identified we tailor our list of port scans and develop a list of potential holes and vulnerabilities. Our port scanning is generally completed when your network is least busy to avoid disruption. Once we know the open ports, we connect to the ports and grab a banner to verify the applications that are running. Once a list of applications is developed, we determine which vulnerabilities exist, document them and download the exploit code (if applicable) for use in the next phase of our testing.

The Exploitation Phase may or may not be completed based on client objectives. We attempt to gain root or admin level access to the target systems. After we obtain unauthorized access to a remote system through the ability to execute a command on a target host or direct access to a user account, we document all relevant information and share it with the client so corrective action can be taken. At this point, depending on client concerns, we either install a tool kit and continue to exploit the system by acquiring UNIX password files or the Windows registry, or we stop the process. If we load our tool kit, we return the system to normal after testing is complete.

We have considerable experience and expertise completing NVA’s and penetration tests for the financial services, banking, manufacturing, higher education, medical, defense and transportation industries.

For more information on ALP’s IT and internal auditing capabilities, including our Network Security Review and Vulnerability Assessment services, please visit our website at www.alp-consulting.net, or contact:

Dave Laakso

Partner

877-312-6547

DLaakso@alp-consulting.net

“The IT Auditing and Security Professionals”™
www.alp-consulting.net