



“The Internal Audit Professionals”™

NETWORK SECURITY REVIEWS & IDENTIFICATION OF VULNERABILITIES

Network Security Reviews, Penetration Testing, Intrusion Detection and Vulnerability Assessments can identify areas within your organization that are susceptible to security breaches and potential financial loss, regulatory fines and penalties, lost productivity, and/or potentially embarrassing publicity. PRI Audit & Control utilizes the latest software tools as well as custom-designed hacking routines to replicate attacks your systems might be subjected to in order to identify any vulnerabilities you might have.

Our Network Vulnerability Assessments and Security Reviews focus on nine key areas:

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

Our Penetration Testing Services include the evaluation of methods available to gain access to your internal network from the outside. Much like an Attorney prosecuting a case or a General preparing for battle, we follow a three step methodology which includes 1) Discovery, 2) Assessment and 3) Exploitation.

During the Discovery phase we attempt to uncover as much information as we can about the topography of your network. One of the first things we do is an external penetration test using commercial software and easily obtainable (public domain) information about your company. We'll want to find out if 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'll identify all connections to the Internet - some which may be unknown to the network managers, leading to potential network breaches.

The Assessment Phase will identify all security holes and vulnerabilities of your network. We will document all target

hosts along with Operating System, IP Addresses, Applications, Banner Information Available and Known Vulnerabilities. This identifies 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 based on expected applications running on the network and begin to develop a list of potential holes and vulnerabilities. We do both comprehensive port scans and scans of the lower port numbers depending on client requirements. 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 available) for use in the next phase of our test.

The Exploitation Phase may or may not be completed, based on client objectives. If we are asked to exploit the system, our primary targets are open ports not tied to specific applications and potentially vulnerable applications. We are attempting 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 we can install a tool kit and continue to exploit the system by acquiring Unix password files or the Windows registry, or we stop the process – again this is dependent on client wishes. If we load our tool kit and continue to exploit the system, we ensure that we can return the system to normal after our testing is complete.

We Have Significant experience and expertise completing NVA's for the financial services, banking, manufacturing, medical, defense and transportation industries.

For more information on PRI's IT and internal auditing capabilities, including our Network Security Review services, please visit our website at www.priauditandcontrol.com or contact:

PRI Audit & Control
317-573-1600

Indianapolis@priauditandcontrol.com
www.priaudit.com