Cyber Vulnerability Assessment

Network Vulnerability Analysis and Penetration Testing

Penrose Security, is pleased to offer network vulnerability analysis and penetration testing.

The world and the devices we use are more and more connected every day, and while this enhances our lives and businesses, there are significant risks to our data and business security. We no longer live in a compartmentalized network model; we live in a borderless network where servers, storage, desktops, printers, phones, and security systems—and even lighting, HVAC systems, and coffeemakers—are all interconnected. This integration improves the quality of our lives and enables great success in our businesses but also introduces increased risk of business interruption, network breaches, service outages, and loss of valuable confidential data. Additionally, you may be subject to federally mandated industry security regulations.

Penrose Security's Networking Security Engineers combine top-tier network assessment methodology, custom coding, and in-depth testing tools with years of security, testing, and remediation experience. We filter out the noise, identify real-world threats, and provide recommendations for protecting your valuable data and your business.

Approach and Methodology

Assessments and penetration tests—tests to gain unauthorized access to a network—can be performed on-site or remotely, depending on your organizational policies and requirements. Penrose can provide both white-box and black-box security services. White-box services, which are recommended, involve the organization giving full access of its network to Penrose while black-box services entail Penrose receiving no knowledge or assistance from the organization.

- Network scanning and discovery: A basic network scan will be conducted to identify devices related to infrastructure and assess vulnerable attack targets
- Wireless injection attacks: Passive password sniffing, PAN ("blue-jacking"), and brute force are used to crack wireless encryption keys and passwords to gain unauthorized access
- Network vulnerability analysis: An inventory of equipment on the network is collected to create a catalog, which we attempt to exploit
- Cross-site scripting: The network web browser is attacked in an attempt to interrupt service, exploit applications, and gather user cookies, passwords, etc.
- Database injection: The network database's security policies are tested for unauthorized commands, e.g. a "DROP TABLE" command that could destroy the database
- Physical environment assessment: The main distribution frame, independent distribution frame, and telecommunications, including power feeds, HVAC feeds, and humidity levels, are reviewed to attempt to identify any abnormalities or risks
- Social engineering: Attempts are made to access the network by targeting and tricking users into giving their passwords, "following" users into secure areas on the network, duplicating websites as well as other information-gathering techniques
- Summary report: Findings will be noted in a report with remediation recommendations and a visual diagram representing the physical topology of the network, noting IP addresses; subnet schemes; and, if desired, administrator credentials

Help protect your business: Call Penrose at (505) 386-0123 or email compliance@penrosesecurity.com

Penrose Security, LLC
320 Gold Ave SW Suite 1131
Albuquerque, NM 87102

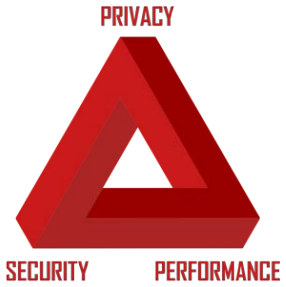
(505) 386-0123 - penrosesecurity.com
compliance@penrosesecurity.com

What is Penetration Testing?

Penetration testing is a way for IT professionals to test your network's security for vulnerabilities, including its operating system, service and application flaws, improper configurations, and end-user behavior. This helps Penrose Security validate the efficacy of your security system and for you to monitor end-users with security policies.

Penetration tests are performed by IT professionals using manual or automatic technologies that safely and systematically put in danger:

- Servers
- Endpoints
- Web applications
- Wireless networks
- Network devices
- Mobile devices
- Other access points of exposure



Once Penrose Security professionals have successfully detected weaknesses, they can begin to create strategic conclusions and prioritize related interventions.

Why Penetration Testing Helps

Penetration testing is an important tool used to detect weaknesses within your network so your business' data is not compromised. In addition to detecting threats, penetration testing offers:

- Early detection: Penetration testing saves on costs related to security breaches by detecting them before they become larger issues
- Safeguarding of information: Technology is growing and changing every day, meaning we need to be able to consistently look for new vulnerabilities and attacks that are evolving technically
- Identification and prioritization of risks: With penetration testing, Ardham Technologies is able to evaluate your organization's ability to protect its networks, applications, endpoints, and internal/external attempts for unauthorized access

Penrose Security performs penetration testing for its clients on a regular basis to create more consistent network security management. This helps us detect new threats, emerging vulnerabilities, and create regularly scheduled analysis and assessments as required by regulatory mandates.

About Penrose Security

Penrose Security has experienced IT professionals you can trust. Penrose Security technicians have extensive knowledge and experience in information technology (IT) or management information systems (MIS) and serves many industries across the board and in real time ensuring they are up to date on the latest developments in the networking and security fields. With more than 80 years of combined IT experience, Penrose Security's expertise is highly sought after.

Help protect your business: Call Penrose at (505) 386-0123 or email compliance@penrosesecurity.com

Penrose Security, LLC
320 Gold Ave SW Suite 1131
Albuquerque, NM 87102

(505) 386-0123 - penrosesecurity.com
compliance@penrosesecurity.com