

ASSESSING VULNERABILITIES

Data breaches dominate the headlines, so it is no wonder organizations turn to encryption and other sophisticated solutions to protect sensitive assets. But we must not forget that a secure network is the first line of defense in data protection.

Even the smallest organizations have sophisticated network architectures and numerous outward-facing server systems and IP addresses. Combined with an increasing number of physical devices and mobile networks – and exploding growth of software vulnerabilities and exploits – maintaining a secure network has become a near-impossible task for today's understaffed IT departments.

A Network Vulnerability Assessment from the certified professionals at infoLock Technologies can arm your organization with the information required to identify vulnerabilities before they become incidents, develop and enforce security policies, and create an effective remediation plan for a more stable and secure network.

Network Mapping/Port Scanning

Using automated scanning tools to conduct active and passive port scanning, infoLock will perform a series of tests to accurately identify open ports and active services accessible from the Internet. Through the use of tools such as SAINT, nmap, traceroute, tcptraceroute, hping, and scanrand, we will be able to obtain information such as the following:

- IP addresses and open ports of live systems
- Map of internal system network as seen from the Internet
- Filtered or closed ports
- List of discovered tunneled, encapsulated, and routing protocols
- Active services by type
- System type (hardware)

NETWORKS IN DISTRESS

THE 2009 VERIZON BUSINESS DATA BREACH REPORT STATES THAT **99.9% OF RECORDS COMPROMISED** IN DATA BREACHES WERE FROM SERVERS AND APPLICATIONS



infoLock
TECHNOLOGIES

DATA SHEET: NETWORK VULNERABILITY ASSESSMENT

FIREWALL RULE MAPPING

Engineers from infoLock will test firewall, web proxy, and configurations of any perimeter security controls by using network scanning tools and packet analyzers. We will collect the following information regarding the network traffic allowed/permitted through the perimeter:

- List of packet types which may enter the network
- List of protocol types with network access
- List of live systems found
- List of packets which entered the network by port number
- List of unmonitored paths into the network

REGULATORY COMPLIANCE

A Network Vulnerability Assessment from infoLock Technologies can help demonstrate compliance with current government and industry regulations, such as:

- FISMA
- SOX
- GLBA
- HIPAA
- HITECH ACT
- PCI DSS

CREATING THE SOLUTION

The Network Vulnerability Assessment from infoLock Technologies culminates in an exhaustive report providing an overview of – as well as detailing specific findings and recommendations from – our scanning, testing, and assessment activities. The findings are broken out based on severity and indicate whether a vulnerability could be exploited, the degree of access that might be gained, and an estimation of the level of damage that could have been done. Remediation recommendations are made in order of security priority, and provide actionable and detailed information. The report can be presented in person or in a Webbased meeting, and includes an in-depth question and answer session.

VULNERABILITY TESTING OF DMZ AND OTHER ACCESSIBLE HOSTS

Once we have conducted port scanning and firewall mapping activities, we will turn to testing identified systems and devices. Through the use of the various automated vulnerability scanning tools, infoLock engineers will enumerate the following information on live hosts:

- Potentially vulnerable services
- Potentially exploitable vulnerabilities
- Out-dated software, services, and operating systems
- Un-patched or out-of-date security updates on hosts

We will also attempt different connection types to and through firewalls or filtering routers that are protecting internal resources, and attempt to gain an understanding of any rules and filters in place by sending various forms of correctly formed, malformed, unfragmented, and fragmented packets to and through the perimeter security devices and analyzing the results.



infoLock
TECHNOLOGIES