Your Partner For Success

Securing Your Business for the Future

COMPREHENSIVE, FLEXIBLE VULNERABILITY MANAGEMENT

Client's Challenge

As the largest integrated healthcare network in the northeast United States, this company which includes numerous major hospitals and employs more than 4,000 physicians with annual revenues in excess of $5 billion. The management team recently turned its attention on determining how to perform comprehensive vulnerability management given the size of their Internet facing infrastructure. Meeting industry and regulatory compliance requirements was a top priority.

With over 200,000 IPs in their network, scope management presented its own set of challenges. In addition to the scope challenges, there were several other constraints:

- ICMP echos ("pings") would not be allowed, making it difficult to identify which of the 200,000 IPs were actually hosting live systems.
- Full port scan would be required,
- Vulnerability scans must be performed within the guidelines of the PCI board, a time consuming process considering the network size.
- Firewall configurations would prove to render standard UDP scanning useless, so an alternative method would be required.
- Reporting would prove to be cumbersome. Reports must comply with PCI standards, yet still had to be disseminated in such a way that remediation could be carried out in a cohesive, expeditious manner.

TBG Security Solution

The challenges posed by the project forced TBG Security to rethink the typical vulnerability management solution. We instituted an assessment methodology that met all of the requirements posed by the client by creating a flexible vulnerability management approach including:

- Instituting a process of host identification through TCP port pinging.
- Once our target list had been identified, stateless TCP scanning of the entire 65535 port range was performed on each identified host. This technique allowed us to scan a very large number hosts/ports using a very small source foot print.
- To perform UDP port scanning, we utilized a UDP scanner capable of communicating with UDP services using their native protocols, eliminating numerous false positives caused by firewalls.
- By pre-populating the list of ports the vulnerability scanner was to scan, we were able assure that lengthy vulnerability scanning would be contained within a manageable timeframe.
- Once all scanning has been performed, PCI reports are generated separated by Class B network range.

Impact on client's business

TBG's methodology for performing large scale enterprise scans has proved a manageable approach which fits nicely into the clients broader vulnerability and risk management initiatives. TBG Security is able to produce customized, reports which meet the requirements of both internal and external consumers. By implementing this flexible approach to vulnerability management, our client now far exceeds the requirements of the PCI Standard. Commoditized scanning and management solutions, which are prevalent in the industry today, do not allow for this level of customization.