Digital Boundary Group

NETWORK SECURITY ASSESSMENT

A Network Security Assessment combines penetration testing, vulnerability assessment, and security architecture review into a single onsite engagement. It provides independent verification of the operational security status of the internal network infrastructure and the physical environment.

HIGHLIGHTS

- Comprehensive review of security posture from an internal perspective
- Determines whether identified technical vulnerabilities may be exploited
- Determines the extent to which internal users may represent a risk to the organization's security

INCLUSIONS

1. Physical Security
2. Network Management and Monitoring
3. Firewall Security
4. Authentication and Authorization
5. File System Security
6. Remote Access / VPN
7. Network Security
8. Host Security
9. Content Inspection
10. Wireless Networks
11. Antivirus and Malicious Code
12. Intrusion Detection and Prevention
13. Vulnerability Assessment
14. Wide Area Network (WAN) Infrastructure
15. Internet Traffic Analysis
16. Policies, Procedures, and Documentation

REPORTING

The final report includes a summary of findings, prioritized recommendations, and detailed observations, implications, and recommendations for each discovered vulnerability.

COST

Based on factors including the number of servers (both physical and virtual), workstations, and physical locations (unless all are centrally managed).

1-800-747-3557 | sales@digitalboundary.net

Digital Boundary Group

REMOTE NETWORK SECURITY ASSESSMENT

A Remote Network Security Assessment combines penetration testing and a vulnerability assessment into a single offsite (remote) engagement. It provides independent verification of the operation security status of the internal network infrastructure.

Scanning of the internal network is performed using a small appliance that contains all the tools necessary to carry out the engagement.

HIGHLIGHTS

- Comprehensive review of security posture from an internal perspective
- Determines whether identified technical vulnerabilities may be exploited
- Determines the extent to which internal users may represent a risk to the organization's security

INCLUSIONS

1. Network Management and Monitoring
2. Firewall Security
3. Authentication and Authorization
4. File System Security
5. Remote Access / VPN
6. Network Security
7. Host Security
8. Content Inspection
9. Antivirus and Malicious Code
10. Intrusion Detection and Prevention
11. Vulnerability Assessment
12. Wide Area Network Infrastructure

REPORTING

The final report includes a summary of findings, prioritized recommendations, and detailed observations, implications, and recommendations for each discovered vulnerability.

COST

Based on the number of servers (both physical and virtual) and workstations.

1-800-747-3557 | sales@digitalboundary.net