**Windows Checklist**

1. Firewall
   1. Exceptions
   2. Advanced (ICMP, Security Logging, Network Connection Settings, Default Settings)
2. Automatic Updates
3. Local Security Policy
   1. Password Policy
      1. Password History: 5
      2. Maximum Password age
         1. **90** for **users**
         2. **30** for **administrators**
      3. Minimum password length : **8**
      4. Password must meet complexity requirements : **Enabled**
      5. Store password using reversible encryption for all users in the domain : **Disabled**
   2. Account Lockout Policy
      1. Account lockout duration
      2. Account lockout threshold
      3. Reset account lockout after counter
   3. Audit Policies
      1. Audit account logon events
      2. Audit object access
      3. Process Tracking
      4. Account management
      5. Directory service access
      6. Logon events
      7. Privilege use
      8. Policy change
      9. System events
   4. Remove everyone access to your computer
4. Event Viewer
5. Services
   1. Turn off unnecessary services
      1. IIS
      2. NetMeeting Remote Desktop Sharing
      3. Remote Desktop Help Session Manager
      4. Remote Registry
      5. Routing and Remote Access
      6. Simple File Sharing
      7. SSDP Discovery Service
      8. Telnet
      9. Universal Plug and Play Device Host
      10. Windows Messenger Service
      11. *SNMP Service*
6. Task Manager (performance monitoring)
   1. Applications
   2. Processes
   3. Performance
   4. Users
7. User Accounts settings
   1. Limit Privileges
   2. Make sure all accounts have passwords
   3. Disable Guest Account
8. Administrator Account
   1. Change password!
   2. Obfuscate the account (Change the name)
   3. Don’t use the account
9. Install and Maintain Malware protection software
   1. Keep signatures up to date
10. Patch more than just the OS
11. Look for alternative to default applications
12. Run Vulnerability scanners on a regular basis
    1. MBSA
    2. Superscan (Port Scanner)
    3. Nessus
    4. Internet Security Scanner (ISS)
    5. Security Auditor’s Research Assistant (SARA)
13. Check File System
    1. Check startup to examine .exe files
    2. Monitor .dll changes
14. Monitor open ports

Examples of Protective security Measures per SANS

1. Access controls

User IDs and passwords, appropriate password and security policies, separation of duties

User authentication, with appropriate use of controls, where possible (e.g. ,smart cards), biometrics, etc.

2. Workstation lock screens

3. Encryption

4. Proper registry permissions

5. Proper directory and file permissions

6. Properly defined user rights

7. Social engineering prevention

8. Applying patches/updates

9. Firewalls

10. VPN tunneling

11. Screening routers

12. Anti-virus software

13. Prompt removal of terminated/transferred employee accounts, default passwords, and unnecessary services running on the system

14. Implementing and enforcing change control policy to limit activity to authorized users only

15. Review and management signoffs of user authorizations

16. Use of checksums with attendant software to report file modifications

17. Enable audit logging and perform log reviews

18. Review of open ports and services

19. Properly configured routers

20. Searching for and disconnecting unauthorized or poorly configured modem services