Topics in Information Systems Security, 2003 January

Permissions in W2K

1. NTFS Inheritable permissions, allowing / not allowing for inheritance
2. Standard level permission and advanced permission
3. Mixing permission for a user with permission for a group
4. Moving and copying files within and between partitions
5. File compression
6. Quota management
7. Network permission for file sharing
8. Mixing network permissions with NTFS permissions

Vulnerability assessment

Security scanning tools e.g. Internet Security Scanner

Reconnaissance

- Obtaining information about domain name, IP addresses, server roles and names, telephone numbers of a chosen company
- Using DNS nslookup, whois, RIPE service, WWW pages, traceroute

Network scanning

- Finding out computers
- Scanning a computer to find out what services it is running (what ports are open)

Enumerating resources in a Windows network

- Listing active Windows computers and their types
- Enumerating shares, services etc using software tools

Enumerating accounts on a Windows machine

- Obtaining accounts lists
- Accounts names and SIDs

Breaking Windows security

- Obtaining password file
- Password breaking using different attack methods
- Significance of a physical access to a computer – booting from a removable media to change passwords

Monitoring network traffic

- What packets one can get from a wire using a network monitor
- Protocols using clear text to transfer data

Virtual private networks

- Securing network traffic using IPSec
- Differences between usual IP packets and IPSec packets
- VPN connections using PPTP and Remote Access

Personal Firewalls

- Rules – which program can perform what network operations (in/out, protocols, ports)
- Warnings and logs generated by a firewall
- MD5 file signatures
- Presenting which program uses what network resources

PGP and public key cryptography

- What keys are needed to send an encrypted message
- What keys are needed to send an signed message
- What is necessary to decrypt an encrypted message
- What is necessary to verify a digital signature
- What is the purpose to have one's public key signed by others
- How a private key is stored