

# Windows NT Security

Windows NT is a 32 bit multitasking operating system from Microsoft for mostly Intel based computers

# Windows NT Security Areas

---

- Log on Security
- Password Storage
- File system security
- Process Security
- Directory Services
- Network Security
- System Logging and Auditing
- Security Protocol Support

# Log on Security

---

- Log on to Windows NT requires a valid username and password on the system
- Systems can have Trust Account on a Windows NT Domain and thus allow users with trust account on the domain to use the computers

# Password Storage

---

- Passwords are stored in MD5 hash format in registry
- Password creation and update policies can be defined
- The database of user, system and groups is called SAM - Security Accounts Manager

# File System Security

---

- NTFS is a secure file system
- Support ACLs
- Supports file system level Encryption (in Windows 2000)

# Process Security

---

- Preemptive multi-tasking
- Memory Protection

# Directory Services

---

- Windows NT 4.0 Directory Services use the Domain model with PDC and BDC's
- Concept of Trust Account
- Trusted Domains
- New directory services based on Active Directory Services - ADS to compete with NDS, StreetTalk, etc.
- ADS uses DNS Name Space and LDAP replication protocols

# Network Security

---

- Basic filters can be defined in Windows NT for TCP/IP traffic coming in and going out
- Add on products are available to implement more sophisticated firewalls using the Windows NT operating system

# System Logging and Auditing

---

- Event Log service logs critical events for troubleshooting and auditing

# Security Protocol Support

---

- All major network security protocols are supported:
- IPSec (Windows 2000)
- PPTP
- SSL-TLS
- Kerberos (Windows 2000)
- PGP
- etc.