Microsoft Active Directory

A presentation to ISACA

Session S1

Monday, April 26, 10:20AM to 11:50 AM

Presenter:

Vincent LeVeque

With thanks to the United States government …..

Guide to Securing Microsoft Windows 2000® Active Directory

Operating Systems Division

of the

Systems and Network Attack Center (SNAC)

Author:
Mark J. Sanderson
David C. Rice

Updated: December 2000
Version 1.0

Active Directory

- Introduced with Windows 2000
- Enterprise wide directory services
  - Single locator for all objects
- Services, standards and protocols used to manage networked Domains.
- Similar to Novell NDS and other directory-based resource management systems

New features

- Integrates existing applications:
  - DNS
  - LDAP-based directory services
  - Kerberos (under the covers)
- Can model complex organization structures
- Trusts easier to implement than Win NT
- More scalable than Win NT

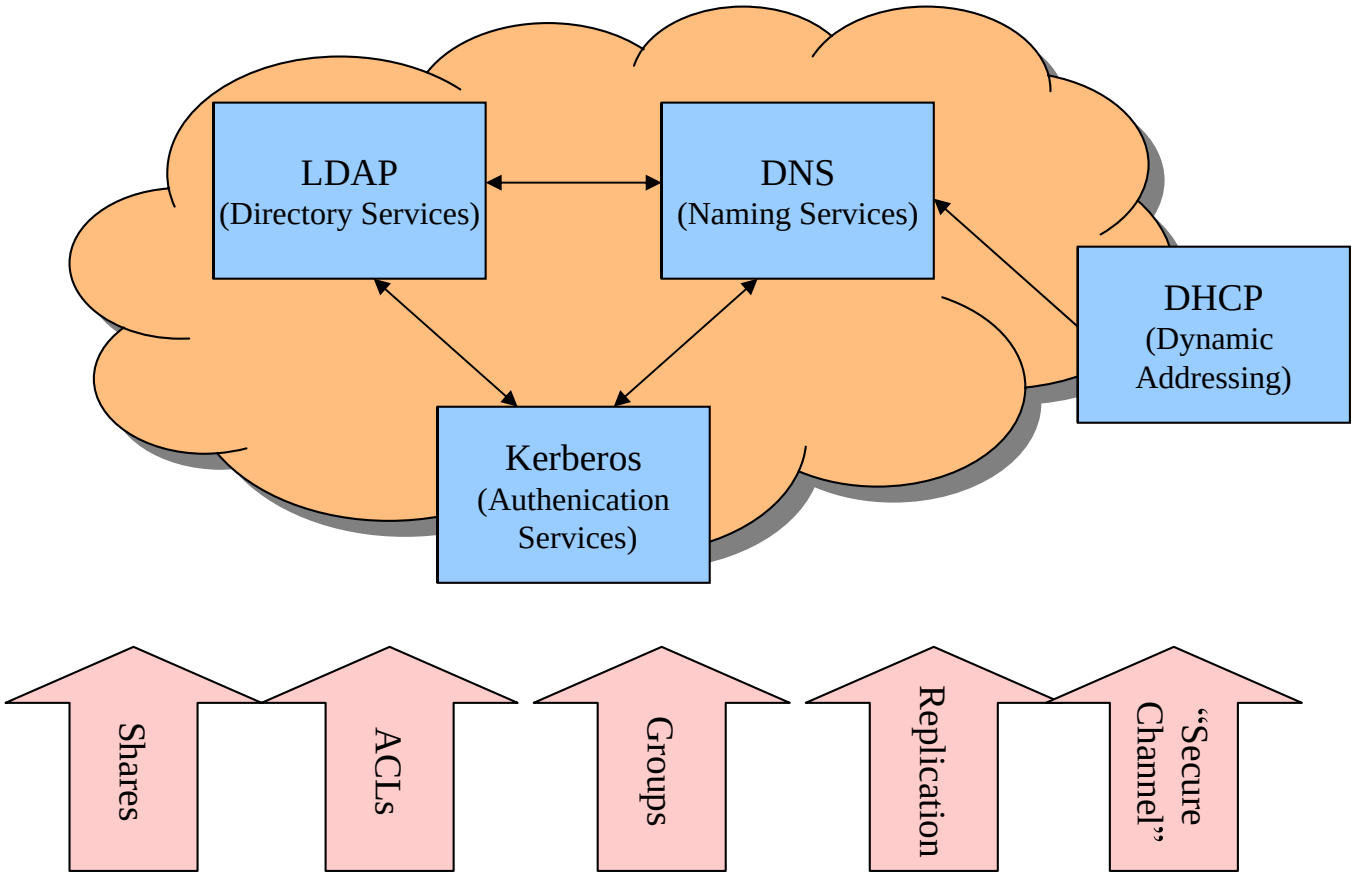
Compared to Win NT

- Multimaster
  - No PDC/BDC distinction
  - Better fault tolerance
- Kerberos authentication
  - More secure/powerful than NTLM
- DNS integrated
  - NetBIOS no longer necessary

Changes for .Net/Windows 2003

- Small improvements, not radical changes over Windows 2000
- 95% of basics still apply
- Major improvements:
  - Can now change domain name
  - Cross forest trusts supported
  - Application Data Partitions, LDAP-supported application software

Software Component View



What are these?

- LDAP – Lightweight Directory Access Protocol, the core of open directory access
- DNS – Domain Name Service, maps IP addresses to host names
  - In Windows AD, also allows service lookup
- Kerberos – A complex cryptographic authentication protocol, developed at MIT
  - Note: An AD “domain” is basically a Kerberos “realm”
- DHCP – Dynamic Host Configuration Protocol, assigns addresses dynamically to client hosts.

LDAP

- “Lightweight Directory Access Protocol”
- Standard method for accessing data in directory structures
- Defined in IETF RFC 2251 and others
- Standard interface to directory services
  - Directory organization
  - Naming conventions
  - APIs

LDAP Hacks

- NMRC Pandora attack for Novell NDS
- Some information available to unauthenticated users:

  In UNIX try:

  ```
  ldapsearch –v –H “ldap://serverip” –D “dc=name,dc=suffix”
  ```

- Access control to entities/attributes important
- Per SANS seminar, no AD “scanner” yet exists, but would be possible

DNS

- Domain Name Service
- Defined in IETF RFC 1035 and others
- Replaces WINS for name resolution
- Active Directory adds to classic DNS:
  - Entries for services as well as hosts (SRV records)
  - Dynamic update interfaced with DHCP
  - Integration with AD Domains, Trees, and Forests
  - No more zone files, DNS may be info kept in AD

AD DNS Issues

- Ensure dynamic update permissions locked down
- Set permissions! If “everyone” has “read” any hacker can read your DNS database

```
nslookup
 > set q=srv
 > _ldap._tcp.dc._msdcs.domainname
```

- Consider secure dynamic updates (requires Kerberos)
- Issues with installing DNS on AD DC.

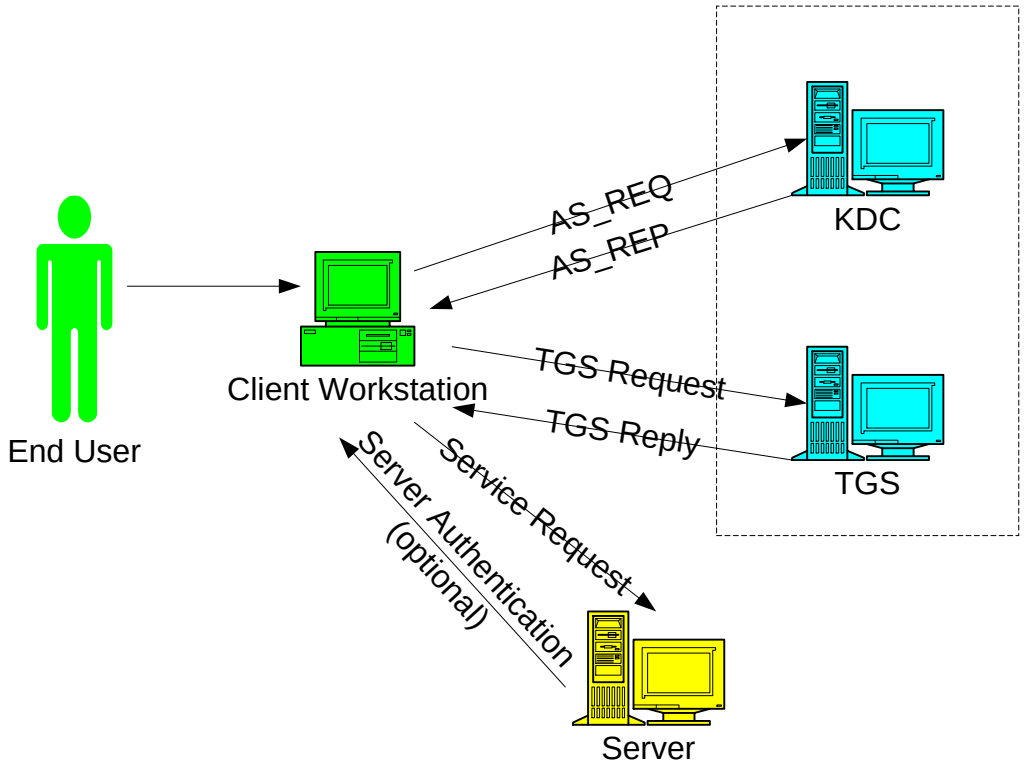
AD DNS Issues

- SRV records allow inquiry of services, not just hosts (as with classic DNS)
- DNS cache poisoning (as with any other DNS)
- Allow Zone Transfers?
- What if someone named their desktop computer “www”, and this name became registered with your dynamic DNS?

Kerberos

- A complex authentication service using symmetric key crypto, timestamps, and various ticket granting servers
- Defined in IETF RFC 1510
- Name after the three-headed dog that guarded Hades
- Operates “behind the scenes” in Windows 2000

Kerberos


KDC
AS_REQ
AS_REP
End User
Client Workstation
TGS Request
TGS Reply
TGS
Service Request
Server Authentication
(optional)
Server

Kerberos

- A Windows 2000 domain is implemented as a Kerberos realm
- Explains why certain security parameters must be set at the domain level:
  - User logon restrictions (password and account lockout)
  - Maximum ticket lifetime
  - Clock synchronization tolerance
  - Accounts trusted for delegation
  - Secure channel options

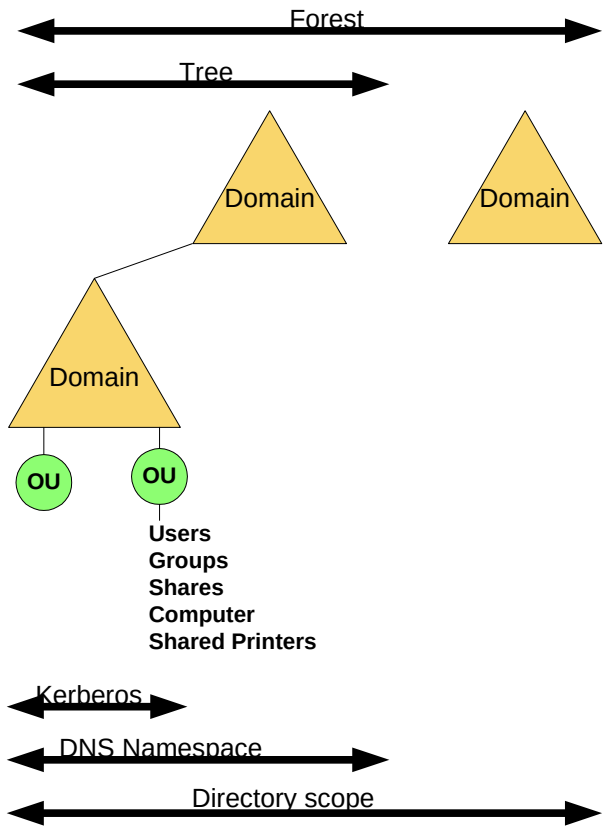
Kerberos not required but …

- Choices
  - NTLM v1 (very bad)
    - L0phtcrack, common utility can break ANY password
  - NTLM v2 (better)
  - Kerberos (best)
- Kerberos is default, but can fall back to NTLM

Kerberos Issues

- Ability to crack crypto?
  - See Arne Vidstrom's KerbCrack at http://ntsecurity.nu/toolbox/Kerbcrack
- Environment must be secure
  - Client system integrity (password grabbers)
  - Servers physically secured
- Requires network-wide time synchronization

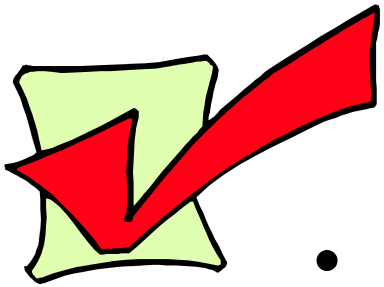
AD Logical/Functional Model



AD organization

- Logical
  - Forest – Different DNS name space, same directory database
  - Tree – Different domains, same DNS name space
  - Domain – Security perimeter, Kerberos entity
  - Organizational Unit – Organizes objects
- Physical
  - Sites and Site Links
  - Used to regulate replication traffic

AD organization



Audit Points

- Documented AD plan?
- Supports feasible business changes?
- Scales to anticipated growth?
- Supports appropriate authority delegation?

Group Policy

- Like NT system policies, but more powerful
- **Not** related to Security Groups
  - You cannot apply a group policy object to a group!
- Allows applying standard configuration options to collections of users and systems, based on:
  - Local Systems
  - Sites
  - Domains
  - Organizational Units

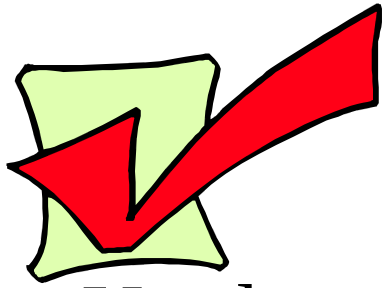
Group Policy

- Group policies can configure the following:
  - Set registry values
  - Install software
  - Assign scripts
  - Folder redirection
  - Set Internet Explorer options
  - Configure user desktop, menus, etc.
  - Set user rights and audit policies

Group Policy

- Applied in the order LSD-OU
- Last one in gets it!
- Inherited down the hierarchy
- Inheritance can be blocked
- But a higher level can override the block
- Resultant Set of Policies Tool facilitates analysis

Group Policy



Audit Points

- Used appropriately to control client and server machines?
- Effective policy is intended policy?
- Settings reflect organizational security policy?
- Settings documented?

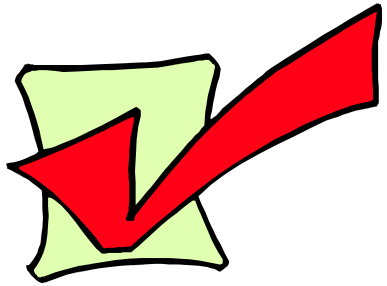
AD and Permission

- Security involves
  - Groups (of users)
  - Access Control Lists (ACLs) applied to objects
    - Made up of Access Control Entries (ACEs)
- Types of Groups
  - Domain Local
  - Domain
  - Universal (new to Windows 2003)

AD and Permissions

- Can set permissions to AD objects:
- Beware of the “everyone” group
  - Wherever possible, use the authenticated users group instead

AD Permissions



Audit Points

- Documented plan to grant/restrict access?
- Unauthenticated access appropriately restricted?
- AD changes restricted to authorized users?
- Sensitive attributes protected?
- Schema changes highly controlled?

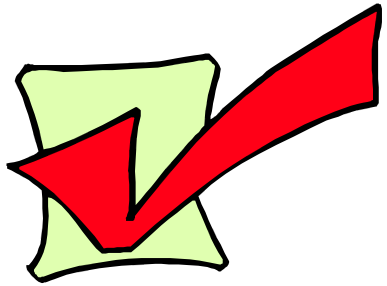
Multimaster

- No more PDC/BDC
- All Domain Controllers are equal!
- All Domain Controllers must be protected
  - Physical and administrative security
  - Beware if you have promoted old Win NT BDCs to AD DCs!
- But some Domain Controllers are more equal than others

Single Master – More Equal than others

- Single Master Operations – privileged Domain Controllers
- Types:
  - PDC Emulator
  - RID Master
  - Infrastructure Master
  - Schema Master
  - Domain Naming Master
- Special recovery procedures required for these

Backup and Recovery



Audit Points

- Documented and tested recovery plan for AD?
- Takes into account AD operations and functioning:
  - Authoritative vs. non-authoritative restores
  - Schema recovery

Secure Channel

- How does security information get to the security service?
- NetLogon Secure Channel!
- Group Policy options to configure:
  - Encrypt (always, when possible)
  - Digitally sign (always, when possible)
  - Require “strong” session key

New ports to block

- With the new services, AD presents new ports to block at firewall:
  - LDAP (389, 636)
  - Kerberos (464, 88, 544)
  - Global Catalog (3268, 3269)

Audit Tools

- Security Templates
- Microsoft Baseline Security Analyzer
- Command line tools
- Third Party
  - CISecurity
  - Bindview, “the usual suspects”

Security Templates

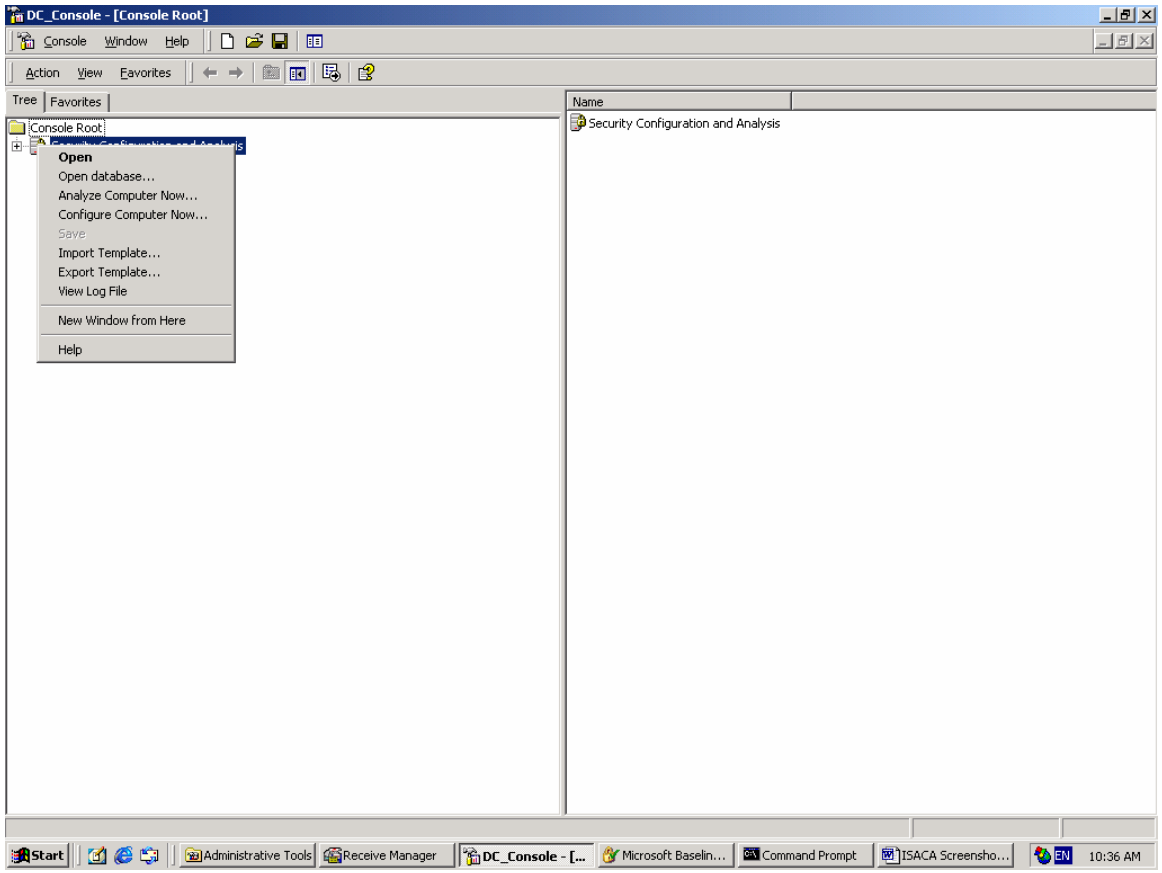
- Kind-of-sort-of like Group Policy Objects
- Can only be applied to local machine
- Can be used in analysis mode
- A great tool for configuration audits!
- Many standard templates available
  - Microsoft (look in %SystemRoot%\Security\Templates)
  - NSA (for Common Criteria evaluation)

Security Templates

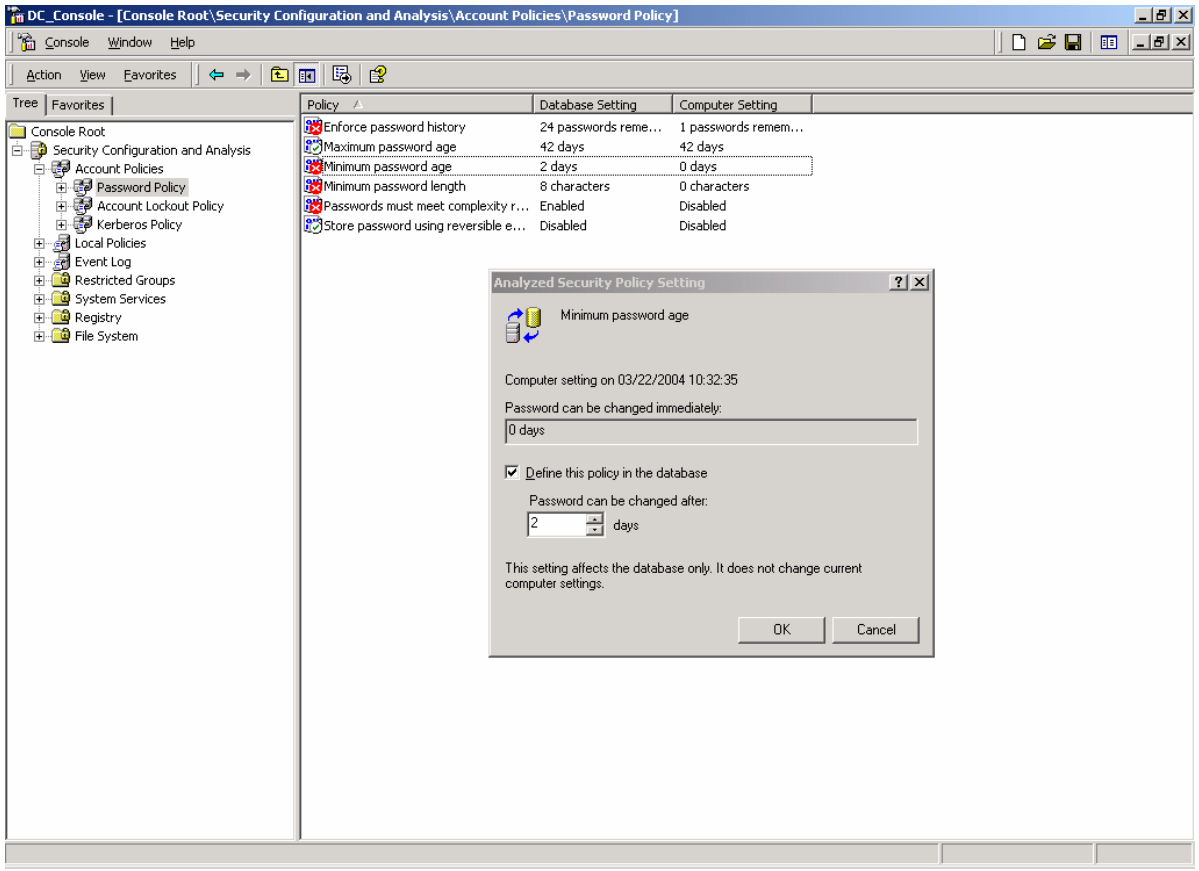
From Microsoft:

Basicwk.inf	Basic Security - Windows 2000 Professional
Basicsv.inf	Basic security - Windows 2000 Server
Basicdc.inf	Basic security - Domain Controller
Securews.inf	Secure - Windows 2000 Professional
Securedc.inf	Secure – Domain Controller

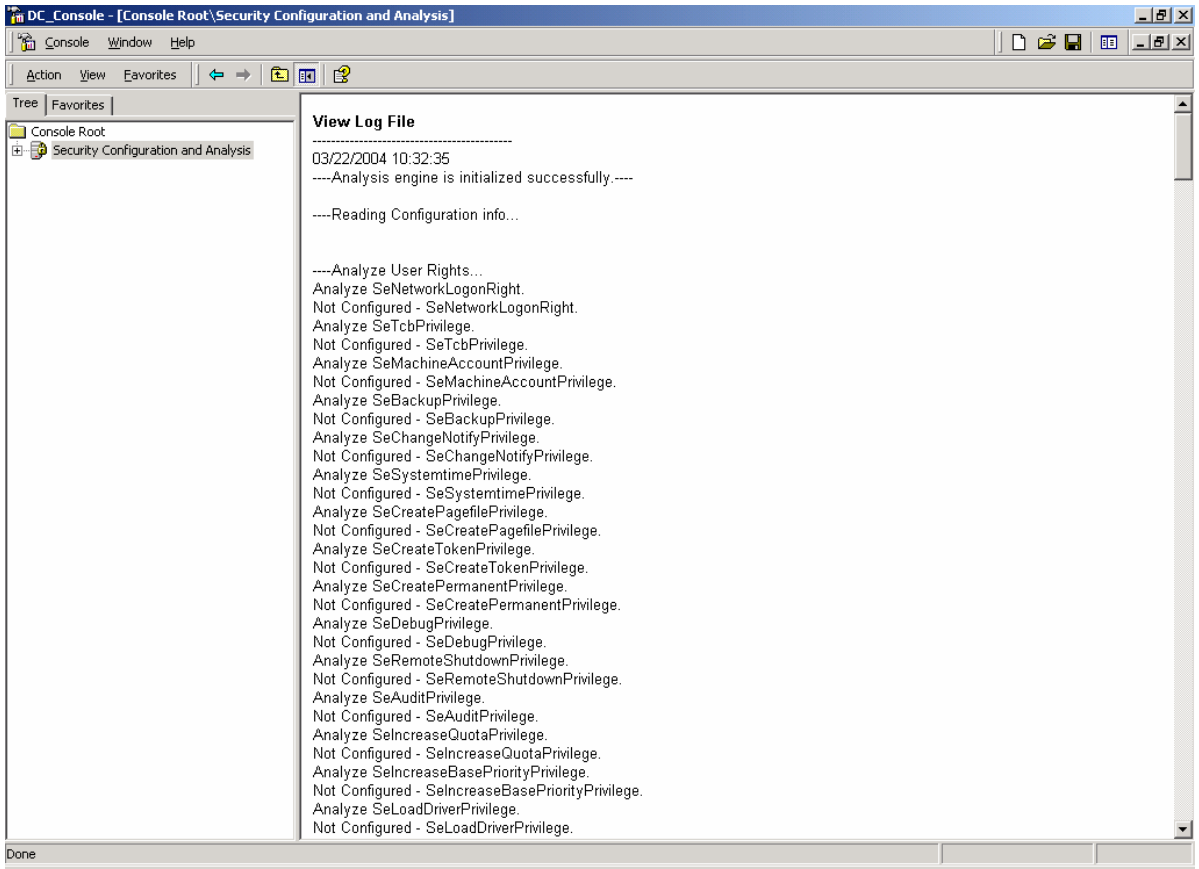
Security Templates



Security Templates

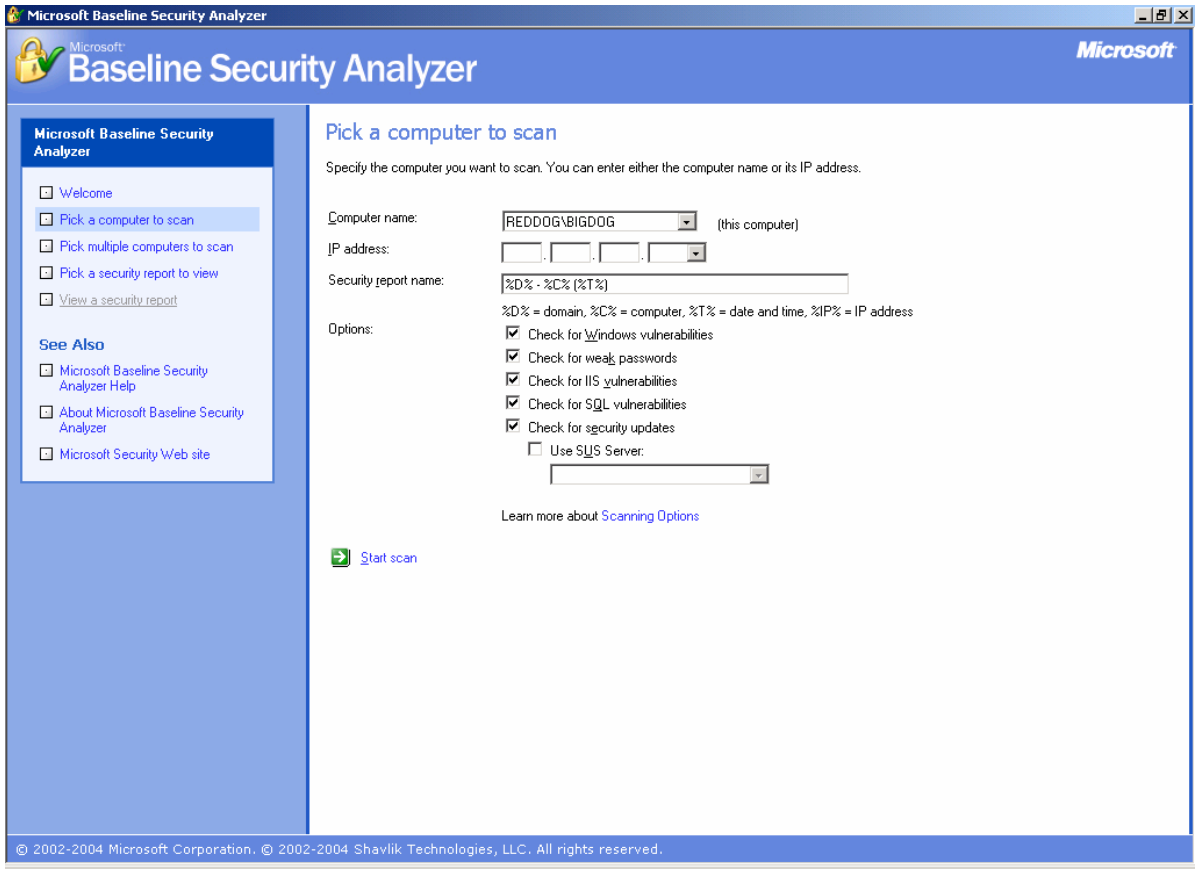


Security Templates

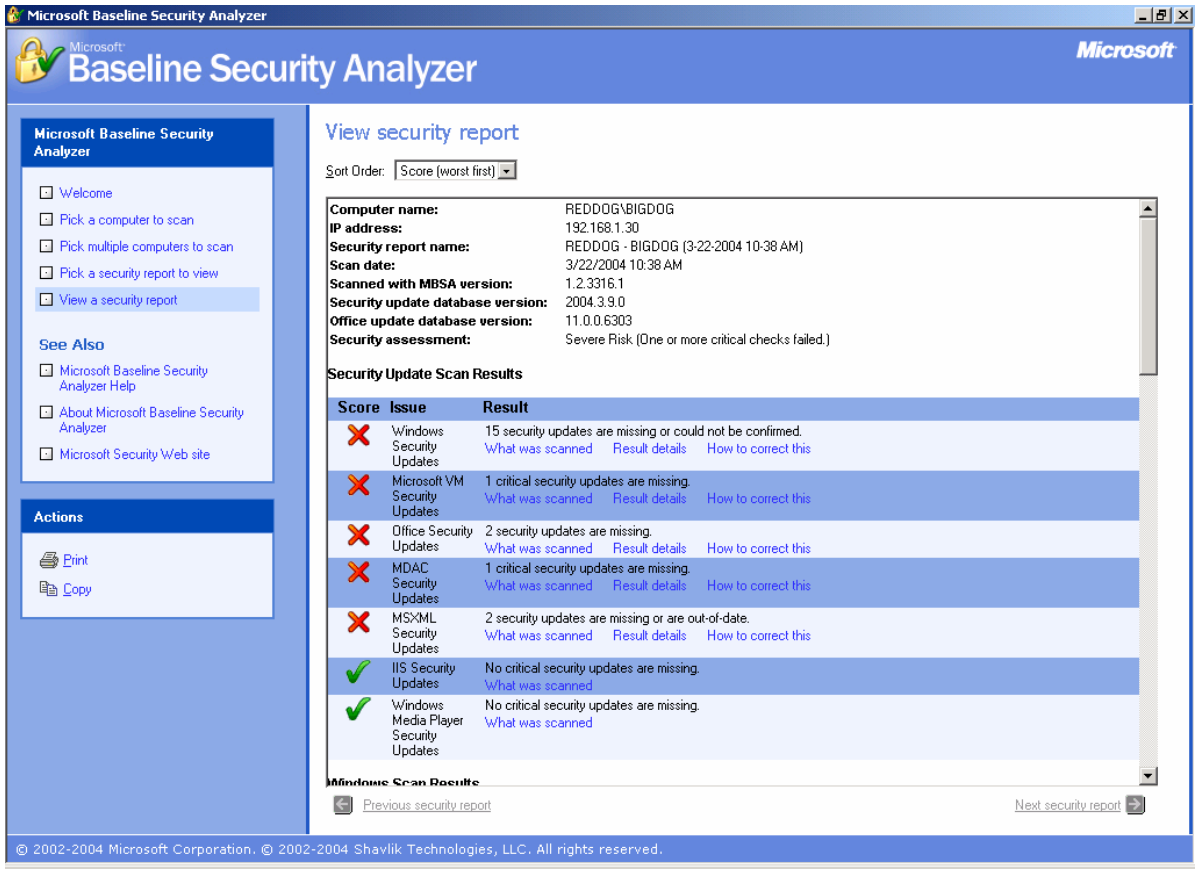


Microsoft Baseline Security Analyzer

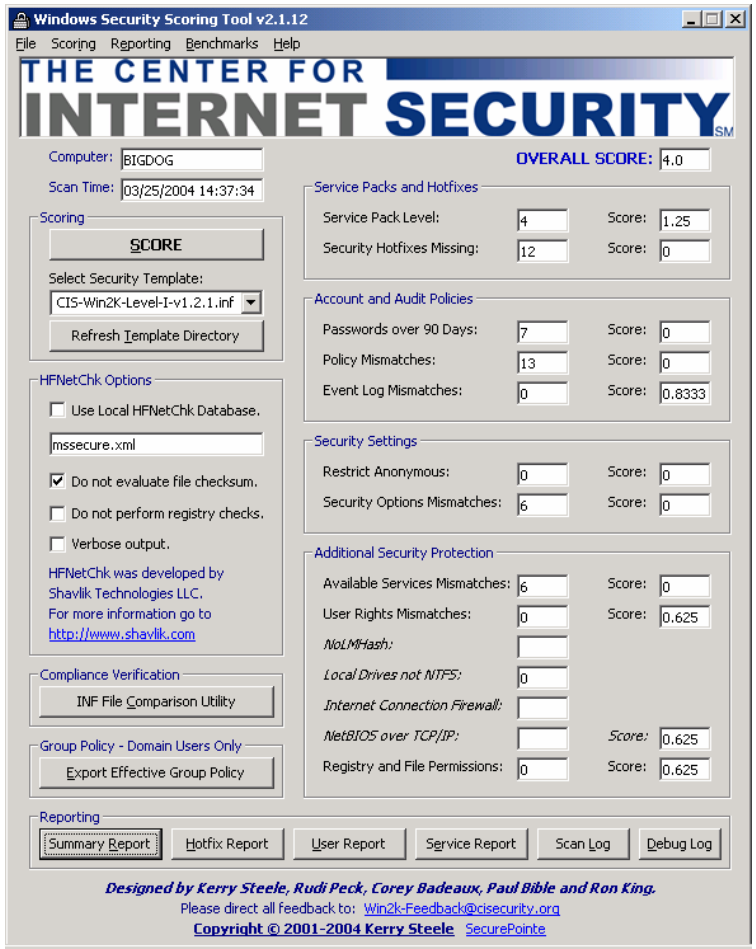
Microsoft Baseline Security Analyzer



Microsoft Baseline Security Analyzer



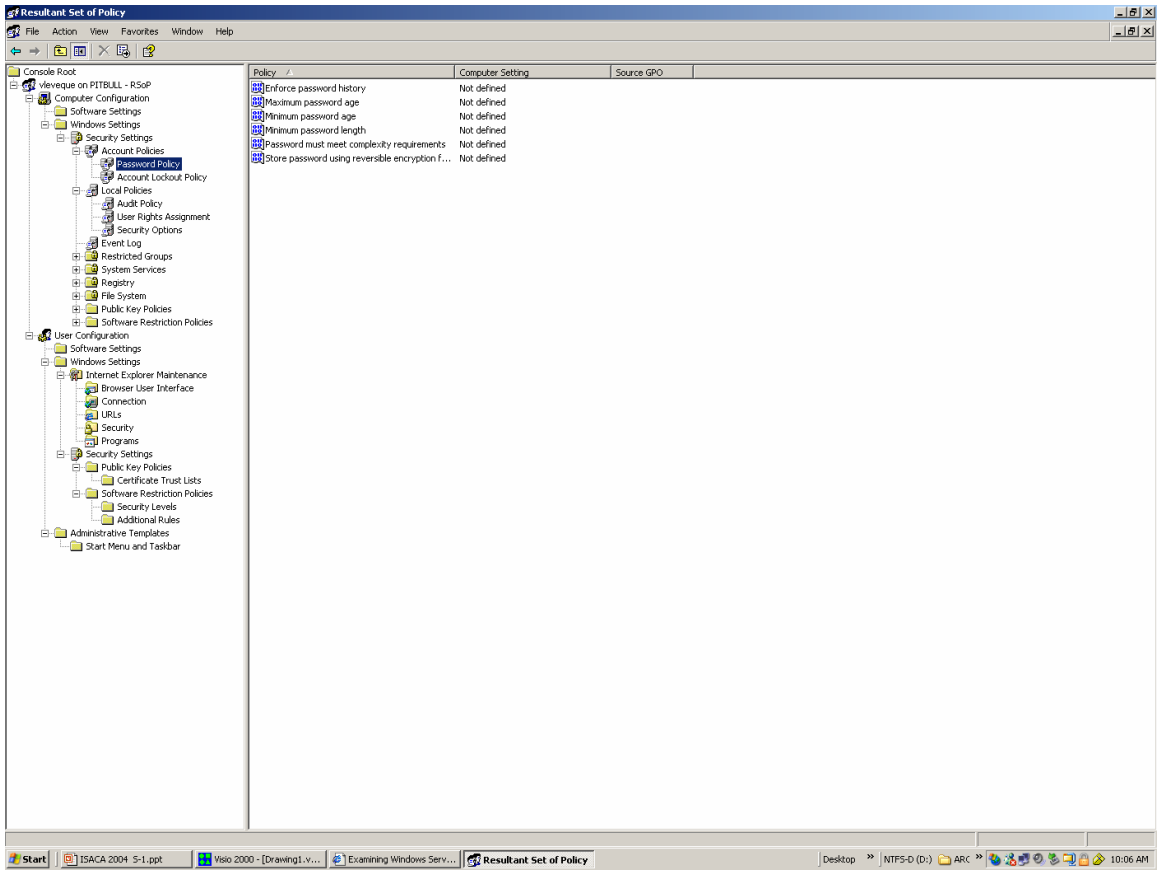
Center for Internet Security Tool



Command Line Tools

- Resource Kit and the Support Tools
- ACLDIAG.EXE
- Resultant Set of Policies
  - GPResult.exe
  - RSOP.MSC

Resultant Set of Polices



More info

- **http://www.cisecurity.org** – Center for Internet Security, scripted security benchmarks
- **http://www.www.isi.edu/~brian/security/kerberos.html -** Moron's Guide to Kerberos
- **http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp** - Windows 2000 tool downloads, a subset of the Resource Kit
- **http://support.microsoft.com/default.aspx?scid=kb;en-us;q313203&sd=tech** – Using security templates for security analysis
- **http://www.sans.org/resources/auto_audit.php** - Automated auditing in a Windows 2000 environment.
- **http://www.microsoft.com/technet/security/tools/mbsahome.mspx -** Intro page for the Microsoft Baseline Security Analyzer
- **http://nsa2.www.conxion.com/win2k/download.htm -** NSA security guides and templates (*.inf files)