GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Securing Windows and PowerShell Automation (Security 505)"
at http://www.giac.org/registration/gcwn

Securing NT – Practical Exercise

Submitted by:
Brendan Moon
bmoon@mail.com

August 14, 2000

© SANS Institute 2000 - 2002, Author retains full rights.

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Contents

INTRODUCTION **3**

THE BATCH FILES **4**

DOC.BAT 5
DOC-DOM.BAT 6
DOC-MEM.BAT 9

THE UTILITIES **10**

CHOICE.EXE 10
NLTEST.EXE 11
NTUSER.EXE 11
NETDOM.EXE 14
SHOWMBRS.EXE 16
AUDIT.EXE 16
SRVINFO.EXE 18
RMTSHARE.EXE 18
NBTSTAT.EXE 19
NMAPNT.EXE 19

REFERENCES **20**

APPENDIX – A REAL WORLD EXAMPLE..... ERROR! BOOKMARK NOT DEFINED.

DIRECTORY OF DOMAINS ..... **ERROR! BOOKMARK NOT DEFINED.**
DIRECTORY OF "PAX" DOMAIN DATA ..... **ERROR! BOOKMARK NOT DEFINED.**
!!PAX.TXT FILE ..... **ERROR! BOOKMARK NOT DEFINED.**
MOONB-DESKPRO.TXT FILE ..... **ERROR! BOOKMARK NOT DEFINED.**

© SANS Institute 2000 - 2002 - Author retains full rights.

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Introduction

To satisfy the Practical Assignment for SANS Security DC 2000, I have developed a tool that may be used to assist in auditing an existing Windows NT network. The tool is essentially a set of nested batch files that, when executed, will use various command line utilities to audit the configuration of an NT Domain, its servers, and member workstations.

This tool will assist in performing information gathering of a network prior to a detailed audit that would be much more time consuming. The tool may be used to quickly gather a great deal of information that may be later analyzed off-line. This may be appropriate for consulting engagements including, but not limited to, security assessments, or Windows 2000 migration planning.

© SANS Institute 2000 - 2002, Author retains full rights.

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The Batch Files

To use these files, you must do the following:

1) Copy the following files to a directory on your workstation:
   doc.bat
   doc-dom.bat
   doc-mem.bat
   NETDOM.CNT
   NETDOM.EXE
   NETDOM.HLP
   NLTEST.EXE
   nmapNT.exe
   nmap-os-fingerprints
   nmap-rpc
   nmap-services
   ntuser.exe
   RMTSHARE.EXE
   SHOWMBRS.EXE
   SRVINFO.EXE

2) Install the NmapNT packet drivers contained in the distribution. There is a WinNT and a Win2k version. These are required for nmapnt.exe. If these are not installed, you should "rem" out the appropriate lines in doc-mem.bat.

3) Line 31 of doc-mem.bat must be modified to include a name and password with full Domain Admin rights on each domain to be documented.

   I recommend creating temporary accounts in each domain with the same name and password for running these files. This temporary account should be deleted once the documentation is complete.

4) Create a domains.txt file so it contains the names of the domains you wish to document. Each domain should be on a separate line in the domains.txt file. There should be no extra lines at the beginning or end.

5) Execute the dom.bat file from the directory containing the files in step 1. You should be logged in as the user created in step 2.

NOTES:

1) This tool will skip member computers that do not respond to pings. You can simply re-execute the dom.bat file to rescan the same machines. Work already saved will not be redone, only missing data will be collected.

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2) I experienced occasional problems with the batch file hanging on some member computers. This was not always reproducible, so you need to keep an eye out for this. I have the current time displayed before each step starts. If any step takes more than a few minutes, issue a CTL-BREAK to stop that command. When asked if you want to "Terminate batch job" say No, then execution will continue with the next command.

Doc.bat

This file parses the domains.txt file to begin documentation for each domain.

```
@echo off

:: Domain Documentation Tool
:: Batch files written by Brendan Moon (bmoon@mail.com)
::
:: Modify these files at your own risk!!!  They have been tested by executing them
:: on an NT4 Workstation.  Executables called by these batch files should reside in
:: the default directory.
::
:: Times are periodically displayed during documentation to identify a hung process.
:: Execution may hang if a non-standard machine is queried.  If more than ten minutes
:: passes between a listed time and the current time, you should issue a CTL+BREAK
:: to terminate the existing command, but do not terminate batch file execution.

cls
echo Domain Documentation Tool
echo
echo Times are periodically displayed during documentation to identify a
echo hung process.  Execution may hang if a non-standard machine is
echo queried, if more than five minutes passes between a listed time and
echo the current time, you should issue a CTL+BREAK to terminate the current
echo command, but do not terminate batch file execution.
echo
choice /C:YN /T:Y,5 Do you wish to continue
IF ERRORLEVEL 2 goto end


:: Check for presence of domains.txt.  This file should contain a listing of each
:: NT Domain to be documented.  Each domain name must be on a seperate line of the file.
:: This "domains.txt" file will be used later in this batch file to document each
:: domain.


IF EXIST domains.txt goto step1
echo You must create a domains.txt file in the default directory
cd
echo
echo This file should contain a listing of each NT Domain to be documented.
echo Each domain name must be on a seperate line of the file.
echo
goto end

:step1

:: Clear the domcnt and memcnt variables.

set /a %domcnt=0
set /a %memcnt=0

:: Log the date and time when documentation of current domain starts.

echo Beginning Documentation
echo Beginning Documentation at >> log.txt
date /t >> log.txt
time /t >> log.txt
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
:: Execute the "doc-dom.bat" file for each domain listed in domains.txt  A subdirectory
:: will be created containing details collected for each domain.

FOR /F "eol=; tokens=1* delims=, " %%a in (domains.txt) do call doc-dom.bat %%a

echo Documentation Complete with %domcnt% domains and %memcnt% members documented. >>
log.txt
echo Documentation Complete with %domcnt% domains and %memcnt% members documented.

:end
```

Doc-dom.bat

This file documents the domain specific information. Then executes dom-mem.bat for each domain server and member.

```
@echo off

echo Documentation continues with %domcnt% domains and %memcnt% members documented. >>
log.txt
echo Documentation continues with %domcnt% domains and %memcnt% members documented.

choice /C:YN /T:Y,5 Do you wish to continue with documentation of the %1 Domain
IF ERRORLEVEL 2 goto end2

:: Log the date and time when documentation of current domain starts.

echo Beginning %1 Documentation at >> log.txt
date /t >> log.txt
time /t >> log.txt

:: Set domcnt variable for stats.

set /a %domcnt=domcnt+1

:: Check for existing Domain data from a previous run

IF NOT EXIST %1\!PDC.txt goto md
choice /C:YN /T:N,5 Old %1 Domain data exists.  Should it be erased
IF ERRORLEVEL 2 goto pdc

:md
:: A seperate subdirectory is made for each Domain.  Any existing files in this directory
:: will be deleted.

echo Creating %1 Directory
md %1
echo y | del %1\*.*

:pdc
:: Create a file identifying the PDC of the current domain.

IF EXIST %1\!PDC.txt goto dc
echo Listing %1 PDC
time /t
nltest /dcname:%1 > tmp.txt
FOR /F "eol=T tokens=6* delims=\, " %%p in (tmp.txt) do echo %%p > %1\!PDC.txt
del tmp.txt

:dc
:: Create a file identifying all of the Domain Controllers in the current domain.
:: This "!DC.txt" file will be used later in this batch file to document each
:: domain controller.

IF EXIST %1\!DC.txt goto mem
echo Listing %1 Domain Controllers
time /t
nltest /dclist:%1 > tmp.txt
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
del %1\!dc.txt
FOR /F "eol=T skip=1 tokens=1* delims=\, " %%a in (tmp.txt) do echo %%a >> %1\!DC.txt
del tmp.txt

:mem
:: Create a file identifying Domain Member (workstation) accounts that HAVE
:: changed their password in the past 15 days.Workstation accounts are changed by default
:: every 10 days.  Any account with a password age of over 15 days should be expired.
:: This "!Members.txt" file will be used later in this batch file to document each
:: active member workstation.

IF EXIST %1\!Members.txt goto expmem
echo Listing %1 Active Members (This may take a while in a large domain.)
time /t
FOR /F "eol=T tokens=1* delims=\, " %%a in (%1\!PDC.txt) do ntuser -s %%a show * -where
"hasflag(UF_WORKSTATION_TRUST_ACCOUNT) AND password_age<1296000" > %1\!Members.txt

:expmem
:: Create a file identifying Domain Member (workstation) accounts that HAVE NOT
:: changed their password in the past 15 days.Workstation accounts are changed by default
:: every 10 days.  Any account with a password age of over 15 days should be expired.

IF EXIST %1\!ExpMembers.txt goto trusts
echo Listing %1 Expired Members (This may take a while in a large domain.)
time /t
FOR /F "eol=T tokens=1* delims=\, " %%a in (%1\!PDC.txt) do ntuser -s %%a show * -where
"hasflag(UF_WORKSTATION_TRUST_ACCOUNT) AND password_age>1296000" > %1\!ExpMembers.txt

:trusts
:: Create a file identifying trusts of the current domain.

IF EXIST %1\!Trusts.txt goto admin
echo Listing %1 Trusting Domains
time /t
netdom /D:%1 RESOURCE >> %1\!Trusts.txt
echo Listing %1 Trusted Domains
time /t
netdom /D:%1 MASTER >> %1\!Trusts.txt

:admin
:: Create a file identifying members of the Local and Domain Administrator groups.

IF EXIST %1\!Administrators.txt goto audit
echo Listing Contents of %1 Administrative Groups
time /t
showmbrs %1\Administrators > %1\!Administrators.txt
showmbrs %1\Domain Admins >> %1\!Administrators.txt

:audit
:: Identifies the Domain audit policies
IF EXIST %1\!AuditPol.txt goto users
echo Listing Domain Audit Policy
time /t
audit policy -s %PDC% show > %1\!AuditPol.txt

:users
:: Create a file identifying domain user accounts.

IF EXIST %1\!Users.txt goto disusr
echo Listing Users of %1 (This may take a while in a large domain.)
time /t
ntuser show %1\* | FIND /V "$" > %1\!Users.txt

:disusr
:: Create a file identifying domain user accounts that are disabled.

IF EXIST %1\!DisUsers.txt goto expusr
echo Listing Disabled Users of %1 (This may take a while in a large domain.)
time /t
FOR /F "eol=T tokens=1* delims=\, " %%a in (%1\!PDC.txt) do ntuser -s %%a show * -where
"hasflag(UF_ACCOUNTDISABLE)" >> %1\!DisUsers.txt
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
:expusr
:: Create a file identifying domain user accounts whose last logon date is earlier than
:: April 1, 2000.  (This should be updated to a proper date prior to execution)

::IF EXIST %1\!ExpUsers.txt goto docdc
::echo Listing Expired Users of %1 (This may take a while in a large domain.)
::time /t
::FOR /F "eol=T tokens=1* delims=\, " %%a in (%1\!PDC.txt) do ntuser -s %%a show * -where
"logon<='20000401'" >> %1\!ExpUsers.txt

:combine
:: Combine multiple text files into a single report file

echo Creating Combined %1 Report...
echo Combined %1 Report > %1\!!%1.txt
date /t >> %1\!!%1.txt
time /t >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo Primary %1 Domain Controller >> %1\!!%1.txt
type %1\!PDC.txt >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo ----------- >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo Complete %1 Domain Controller List >> %1\!!%1.txt
type %1\!DC.txt >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo ----------- >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo Trust Report for %1 >> %1\!!%1.txt
type %1\!Trusts.txt >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo ----------- >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo Audit Policy for %1 >> %1\!!%1.txt
type %1\!AuditPol.txt >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo ----------- >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo User List for %1 >> %1\!!%1.txt
type %1\!Users.txt >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo ----------- >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo Disabled User List for %1 >> %1\!!%1.txt
type %1\!DisUsers.txt >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo ----------- >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo Administrator Group Memberships for %1 >> %1\!!%1.txt
type %1\!Administrators.txt >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo ----------- >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo Member Computer Accounts for %1 >> %1\!!%1.txt
type %1\!Members.txt >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo ----------- >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo Expired Computer Accounts for %1 >> %1\!!%1.txt
type %1\!ExpMembers.txt >> %1\!!%1.txt


:docdc
:: Execute the "doc-mem.bat" file for each domain controller.  A file will be created
:: for each one containing details collected for each macine.

echo Documenting Domain Controllers
time /t
FOR /F "eol=; tokens=1* delims=\, " %%a in (%1\!DC.txt) do @call doc-mem.bat %1 %%a
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
:noping
:: Check for existance of a !NoPing.txt file, indicating a previous run on this domain.
IF NOT EXIST %1\!NoPing.txt goto docmem
copy %1\!NoPing.txt !NoPing.old
del %1\!NoPing.txt

:docmem
:: Execute the "doc-mem.bat" file for each domain member.  A file will be created
:: for each one containing details collected for each macine.

echo Documenting Members
time /t
FOR /F "eol=; tokens=1* delims=$, " %%a in (%1\!Members.txt) do @call doc-mem.bat %1 %%a

:combine2
:: Add Non-Responsive Members to combined report.
echo   >> %1\!!%1.txt
echo ----------- >> %1\!!%1.txt
echo   >> %1\!!%1.txt
echo Non-Responding Computers with Member Accounts for %1 >> %1\!!%1.txt
type %1\!NoPing.txt >> %1\!!%1.txt

:end2
```

Doc-mem.bat

This file documents each domain server and member.

```
@echo off
IF EXIST %1\%2.txt goto end3
echo Checking %1 %2

:: Verify the presence of the current member via the PING command.  If there is no
:: reply, add this memeber's name to the "!NoPing" file and return to "doc-dom.bat"

::ping -a -n 1 -w 500 %2 > %1\%2.png
::FOR /F "eol=; skip=3 tokens=1* delims=\, " %%a in (%1\%2.png) do @IF %%a==Reply goto
skip1
FOR /F "eol=; skip=3 tokens=1* delims=\, " %%a in ('ping -a -n 1 -w 500 %2') do @IF
%%a==Reply goto skip1
echo %2 Not Found
::del %1\%2.png
echo %1\%2 >> %1\!NoPing.txt
goto end3

:skip1
::del %1\%2.png
echo %2 Found

:: Set memcnt variable for stats.

set /a %memcnt=memcnt+1

:: Establish an SMB session with the member using the specified user account.  This
:: account must have administrator privileges to complete all documentation successfully.

echo Establishing SMB Connection
time /t
net use \\%2 /user:%1\{username} {password}

:: Create a file for the current machine which will contain details about the OS
:: currently installed.

echo Listing Computer Details
time /t
srvinfo -v \\%2 > %1\%2.txt

:: Identify possible service accounts and append the list to two files.  One is specific
:: to the current machine, the other contains service accounts for all machines in the
:: domain.
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
echo Listing Service Accounts
time /t
ntuser -s %2 rights show seservicelogonright | find "\" >> %1\%2.txt
time /t
ntuser -s %2 rights show seservicelogonright | find "\" >> %1\!SvcAcct.txt

:: Identify members of the current machine's local Administrator group.

echo Listing Contents of Administrative Group
time /t
showmbrs \\%2\Administrators >> %1\%2.txt

:: Identify details about the local Administrator account if it has not been renamed.

echo Listing Administrator Details
time /t
nltest /user:Administrator /server:%2 >> %1\%2.txt

:: Identify details about existing shares on the current machine.

echo Listing Shares
time /t
rmtshare \\%2 >> %1\%2.txt

:: Close the SMB session to the current machine.

echo Terminating SMB Connection
time /t
net use \\%2 /d

:: Perform a NETBIOS scan of the current machine.

echo Performing NBTSTAT scan
time /t
nbtstat -a %2 >> %1\%2.txt

:: Perform an nmap scan of the current machine.

echo Performing nmapNT scan
time /t
FOR /F "eol=; skip=3 tokens=3* delims=\:, " %%a in ('ping -a -n 1 -w 500 %2') do nmapnt -
O -sS %%a >> %1\%2.txt

:end3
```

The Utilities

Both Microsoft and third parties have developed a number of command-line utilities that perform a variety of functions. The Domain Documentation tool (DomDoc) uses a combination of these utilities to collect a wealth of information about an existing NT network.

Choice.exe

Choice prompts the user to make a choice in a batch program by displaying a prompt and pausing for the user to choose from among a set of keys. It can be found in Windows NT or Windows 2000 Resource Kits.

```
CHOICE [/C[:]choices] [/N] [/S] [/T[:]c,nn] [text]

/C[:]choices Specifies allowable keys. Default is YN
/N           Do not display choices and ? at end of prompt string.
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
/S           Treat choice keys as case sensitive.
/T[:]c,nn    Default choice to c after nn seconds
text         Prompt string to display

ERRORLEVEL is set to offset of key user presses in choices.
```

Nltest.exe

Administers and tests domains and user accounts. It can be found in Windows NT or Windows 2000 Resource Kits.

```
Usage: nltest [/OPTIONS]


    /SERVER:<ServerName> - Specify <ServerName>

    /QUERY - Query <ServerName> netlogon service
    /REPL - Force replication on <ServerName> BDC
    /SYNC - Force SYNC on <ServerName> BDC
    /PDC_REPL - Force UAS change message from <ServerName> PDC

    /SC_QUERY:<DomainName> - Query secure channel for <Domain> on <ServerName>
    /SC_RESET:<DomainName> - Reset secure channel for <Domain> on <ServerName>
    /DCLIST:<DomainName> - Get list of DC's for <DomainName>
    /DCNAME:<DomainName> - Get the PDC name for <DomainName>
    /DCTRUST:<DomainName> - Get name of DC is used for  trust of <DomainName>
    /WHOWILL:<Domain>* <User> [<Iteration>] - See if <Domain> will log on <User>

    /FINDUSER:<User> - See which trusted <Domain> will log on <User>
    /TRANSPORT_NOTIFY - Notify of netlogon of new transport


    /RID:<HexRid> - RID to encrypt Password with
    /USER:<UserName> - Query User info on <ServerName>

    /TIME:<Hex LSL> <Hex MSL> - Convert NT GMT time to ascii
    /LOGON_QUERY - Query number of cumulative logon attempts
    /TRUSTED_DOMAINS - Query names of domains trusted by workstation

    /BDC_QUERY:<DomainName> - Query replication status of BDCs for <DomainName>
    /SIM_SYNC:<DomainName> <MachineName> - Simulate full sync replication

    /LIST_DELTAS:<FileName> - display the content of given change log file
    /LIST_REDO:<FileName> - display the content of given redo log file
```

Ntuser.exe

NTUSER is used to manipulate users, groups, rights and account policies. It is part of Pedestal Software's NTSEC Security Utilities. (www.pedestalsoftware.com)

```
NTUSER [parms] NEW <user> [options]
                      CHANGE <user> [options]
                      DELETE <user>
                      SHOW <user | *>
                      RENAME <old_user> <new_user>
                      COPY <orig_user> <new_user> [new_server]
                      GROUPS <user>
                      DUPLICATE DOMAIN <old_domain> <new_domain>
                      DUPLICATE SERVER <old_server> <new_server>
                      [L]GROUP NEW <group> [options]
                      [L]GROUP CHANGE <group> [options]
                      [L]GROUP DELETE <group>
                      [L]GROUP SHOW <group | *>
                      [L]GROUP RENAME <old_group> <new_group>
                      [L]GROUP APPEND <group> <users...>
                      [L]GROUP REMOVE <group> <users...>
                      [L]GROUP DUPLICATE DOMAIN <old_domain> <new_domain>
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
                      [L]GROUP DUPLICATE SERVER <old_server> <new_server>
                      RIGHTS SHOW <right | *>
                      RIGHTS ADD <right> <user(s) | group(s)>
                      RIGHTS REMOVE <right> <user(s) | group(s)>
                      POLICY [options]
                      HELP OPTIONS
                      HELP FLAGS     (used by -set and -unset)
                      HELP RIGHTS    (used by RIGHTS, -addright and -remright)
                      HELP POLICY    (used by POLICY)

Use parms: -s <server> : use as default server.
           -sr <server>: user server to evaluate rights (default same as -s).
           -35         : using NT 3.5 features only
           -ras        : Enable ras features
           -wts        : Enable terminal server features
           -userrights : Show user rights when displaying
           -sam        : get permissions to read the password field
           -nocreate   : don't create missing groups when copying users
           -nogroup    : don't copy group memberships
           -nolocalgroup : don't copy local group memberships
           -details    : display details in wildcard matches
           -csv        : display output in comma-separated-values format
           -std        : redirect stderr to stdout
           -b          : return 0 if no errors or 1 if errors occurred
                         (default is to return number of errors)
           -bw         : return 0 if no matches in where expression or 1 if at least one
match was made

[L]GROUP means to use GROUP for global groups and LGROUP for local groups


NTUSER OPTIONS:

-full_name <name>
-comment <comment_text>
-usr_comment <comment>
-country_code <number>
-code_page <number>
-primary_group <group_name>
-primary_group_id <group_number>
-home_dir <directory>
-home_dir_drive <drive:>
-script_path <path>
-profile <direcotory>
-workstations <computer_name>
-logon_server <computer_name>
-password <new_password>
-random_password <number of character>
-random_password_show <number of character>
-password_expired <yes|no>
-acct_expires <mm/dd/yyyy [hh:mm]>
-max_storage <amt_disk>
-addright <userright>
-remright <userright>
-rasphone <phone>
-wts_initial_program <path>
-wts_working_directory <dir>
-wts_inherit_initial_program <true-or-false>
-wts_allow_logon <true-or-false>
-wts_timeout_connections <milliseconds>
-wts_timeout_disconnections <milliseconds>
-wts_timeout_idle <milliseconds>
-wts_client_drives <true-or-false>
-wts_client_printers <true-or-false>
-wts_client_default_printer <true-or-false>
-wts_broken_timeout_settings <0 or 1>
-wts_reconnect_settings <0 or 1>
-wts_modemcb_settings <0,1, or 2>
-wts_modemcb_phone <phone-number>
-wts_shadowing_settings <0,1,2,3 or 4>
-wts_profile_path <directory>
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
-wts_home_dir <directory>
-wts_home_dir_drive <drive:>
-wts_remote_home_dir <true-or-false>
-set <flag>     * -set item can be repeated
-unset <flag>   * -unset item can be repeated


NTUSER FLAGS:

Note: UF_SCRIPT and UF_NORMAL_ACCOUNT are always set if no other flags are specified when
adding new accounts.
UF_SCRIPT : The logon script executed. This value must be set for LAN Manager 2.0 or
Windows NT.
UF_ACCOUNTDISABLE : The user's account is disabled.
UF_HOMEDIR_REQUIRED : The home directory is required. This value is ignored in Windows
NT.
UF_PASSWD_NOTREQD : No password is required.
UF_PASSWD_CANT_CHANGE : The user cannot change the password
UF_LOCKOUT : The account is currently locked out. When changing a user, this value can be
cleared to unlock a previously locked account. This value cannot be used to lock a
previously unlocked account.
UF_DONT_EXPIRE_PASSWD : Represents the password, which should never expire on the
account. This value is valid only for Windows NT.
UF_MNS_LOGON_ACCOUNT : No known description
UF_ENCRYPTED_TEXT_PASSWORD_ALLOWED : Windows 2000. The user's password is stored under
reversible encryption in the Active Directory
UF_NOT_DELEGATED : Windows 2000. This account is marked as 'sensitive'; other users
cannot act as delegates of this user account.
UF_SMARTCARD_REQUIRED : Windows 2000. This user must logon using a smart card.
UF_TRUSTED_FOR_DELEGATION : Windows 2000. The account is enabled for delegation. This is
a security-sensitive setting; accounts with this option enabled should be tightly
controlled. This setting allows a service running under the account to assume a client's
identity and authenticate as that user to other remote servers on the network.
UF_USE_DES_KEY_ONLY : Windows 2000. Restrict this principal to use only Data Encryption
Standard (DES) encryption types for keys.
UF_DONT_REQUIRE_PREAUTH : Windows 2000. This account does not require Kerberos
preauthentication for logon.
UF_NORMAL_ACCOUNT : This is a default account type that represents a typical user.
UF_TEMP_DUPLICATE_ACCOUNT : This is an account for users whose primary account is in
another domain. This account provides user access to this domain, but not to any domain
that trusts this domain. The User Manager refers to this account type as a local user
account.
UF_WORKSTATION_TRUST_ACCOUNT : This is a computer account for an Windows NT Workstation
or Windows NT Server that is a member of this domain.
UF_SERVER_TRUST_ACCOUNT : This is a computer account for an Windows NT Backup Domain
Controller that is a member of this domain.
UF_INTERDOMAIN_TRUST_ACCOUNT : This is a permit to trust account for a Windows NT domain
that trusts other domains.
RASPRIV_NoCallback : The user has no call-back privilege.
RASPRIV_AdminSetCallback : The user account is configured to have the administrator set
the call-back number.
RASPRIV_CallerSetCallback : The remote user can specify a call-back phone number when
dialing in.
RASPRIV_DialinPrivilege : The user has permission to dial in to this server.


NTUSER RIGHTS:

SeInteractiveLogonRight              "Log on locally"
SeNetworkLogonRight                  "Access this computer from network"
SeBatchLogonRight                    "Log on as a batch job"
SeServiceLogonRight                  "Log on as a service"
SeCreateTokenPrivilege               "Create a token object"
SeAssignPrimaryTokenPrivilege        "Replace a process level token"
SeLockMemoryPrivilege                "Lock pages in memory"
SeIncreaseQuotaPrivilege             "Increase quotas"
SeMachineAccountPrivilege            "Add workstations to domain"
SeTcbPrivilege                       "Act as part of the operating system"
SeSecurityPrivilege                  "Manage auditing and security log"
SeTakeOwnershipPrivilege             "Take ownership of files or other objects"
SeLoadDriverPrivilege                "Load and unload device drivers"
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
SeSystemProfilePrivilege              "Profile system performance"
SeSystemtimePrivilege                 "Change the system time"
SeProfileSingleProcessPrivilege       "Profile a single process"
SeIncreaseBasePriorityPrivilege       "Increase scheduling priority"
SeCreatePagefilePrivilege             "Create a pagefile"
SeCreatePermanentPrivilege            "Create permanent shared objects"
SeBackupPrivilege                     "Back up files and directories"
SeRestorePrivilege                    "Restore files and directories"
SeShutdownPrivilege                   "Shut down the system"
SeDebugPrivilege                      "Debug programs"
SeAuditPrivilege                      "Generate security audits"
SeSystemEnvironmentPrivilege          "Modify firmware environment values"
SeChangeNotifyPrivilege               "Bypass traverse checking"
SeRemoteShutdownPrivilege             "Force shutdown from a remote system"


NTUSER POLICY:

-min_password_len <characters>
-max_password_age <seconds>
-min_password_age <seconds>
-force_logoff <yes|no>
-password_hist_len <times>
-lockout_duration <seconds>
-lockout_reset <seconds>
-lockout_threshold <seconds>
```

Netdom.exe

Enables administrators to manage domains. It can be found in Windows NT or Windows 2000 Resource Kits.

```
NetDom 1.7 @1997. Written by Christophe Robert (chrisrob@microsoft.com).

The syntax of this command is:


NETDOM [/Options] command
- or -
NETDOM HELP command

Commands available are:

   NETDOM BDC         NETDOM HELP       NETDOM MASTER
   NETDOM MEMBER      NETDOM QUERY      NETDOM RESOURCE


Options are as follows:

   Options                    Description
   ---------------------------------------------------------------------
   /D[OMAIN]:DOMAINNAME       Performs the operation on the primary domain
                              controller of the domain DOMAINNAME.
                              If this option is not used then the domain
                              is the one of which the workstation or the
                              server is a server. If the computer is a
                              domain controller, the operation takes place
                              on the current domain.

   /U[SER]:DOMAIN\USER        User account used to make the connection with
                              the primary domain controller on which the
                              action is to be performed.
                              If this option is not used, the current user
                              account is used.

   /P[ASSWORD]:password       Password of the user account defined along with
                              the option /USER.

   /NOVERBOSE                 Not verbose. Displays only the results of the
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
                              performed operation.

NETDOM [/Options] RESOURCE [ResourceDomain] [password] [/Command]

Options are as follows:

   Options                    Description
   ---------------------------------------------------------------------
   /D[OMAIN]:DOMAINNAME       Performs the operation on the primary domain
                              controller of the domain DOMAINNAME.
                              If this option is not used then the domain
                              is the one of which the workstation or the
                              server is a server. If the computer is a
                              domain controller, the operation takes place
                              on the current domain.

   /U[SER]:DOMAIN\USER        User account used to make the connection with
                              the primary domain controller on which the
                              action is to be performed.
                              If this option is not used, the current user
                              account is used.

   /P[ASSWORD]:password       Password of the user account defined along with
                              the option /USER.

   /NOVERBOSE                 Not verbose. Displays only the results of the
                              performed operation.

Commands are as follows:

   Command                    Description
   ---------------------------------------------------------------------
   No command                 Lists the resource domains of the master domain.
                              Must be used without any domain resource name.

   /ADD                       Adds an account for the resource domain.

                              A password can be specified in the command line.
                              If no password is defined then a default password
                              is used (eg, the resource domain name in lower
                              case and limited to 14 characters).

   /DELETE                    Removes the account for the resource domain.

   /QUERY                     Queries the resource domain account. Checks the
                              secure channel between the resource domain and
                              the master domain.

Samples are as follows:

   NETDOM /Domain:MyMasterDomain /User:MyMasterDomain\AUser /Password:apassword
          RESOURCE MyResourceDomain MyPassword /ADD

   NETDOM /Domain:MyMasterDomain RESOURCE MyResourceDomain MyPassword /ADD
   NETDOM /Domain:MyMasterDomain RESOURCE MyResourceDomain /DELETE
   NETDOM /Domain:MyMasterDomain RESOURCE MyResourceDomain /QUERY

NETDOM [/Options] MASTER [MasterDomain] [password] [/Command]

Options are as follows:

   Options                    Description
   ---------------------------------------------------------------------
   /D[OMAIN]:DOMAINNAME       Performs the operation on the primary domain
                              controller of the domain DOMAINNAME.
                              If this option is not used then the domain
                              is the one of which the workstation or the
                              server is a server. If the computer is a
                              domain controller, the operation takes place
                              on the current domain.
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
   /U[SER]:DOMAIN\USER        User account used to make the connection with
                              the primary domain controller on which the
                              action is to be performed.
                              If this option is not used, the current user
                              account is used.

   /P[ASSWORD]:password       Password of the user account defined along with
                              the option /USER.

   /NOVERBOSE                 Not verbose. Displays only the results of the
                              performed operation.

Commands are as follows:

   Command                    Description
   ---------------------------------------------------------------------
   No command                 Lists the resource domains of the master domain.
                              Must be used without any master domain name.

   /TRUST                     Establish a trust relationship between the
                              resource domain and the master domain.
                              The resource domain is the current domain or the
                              domain specified along with the option /DOMAIN.
                              Resets the secure channel if the trust
                              relationship was previously existing.

                              A password can be specified in the command line.
                              If no password is defined then a default password
                              is used (eg, the resource domain name in lower
                              case and limited to 14 characters).

   /DELETE                    Removes the Master Domain.

   /QUERY                     Queries the master domain information on the
                              resource domain PDC and checks the secure channel.


Samples are as follows:

   NETDOM /Domain:MyResourceDomain /User:MyResourceDomain\AUser
          /Password:apassword MASTER MyMasterDomain MyPassword /TRUST

   NETDOM /Domain:MyResourceDomain MASTER MyMasterDomain MyPassword /TRUST
   NETDOM /Domain:MyResourceDomain MASTER MyMasterDomain /TRUST
   NETDOM /Domain:MyResourceDomain MASTER MyMasterDomain /DELETE
   NETDOM /Domain:MyResourceDomain MASTER MyMasterDomain /QUERY
```

Showmbrs.exe

This command-line tool shows the user names of members of a given group, even within a given network domain. It can be found in Windows NT or Windows 2000 Resource Kits.

```
Usage:

showmbrs domain\group or
showmbrs \\domain\group or
showmbrs group
```

Audit.exe

AUDIT serves two functions. First, it manipulates the auditing settings of files and directories. Second, it manipulates the auditing policies of the machine. It is part of Pedestal Software's NTSEC Security Utilities. (www.pedestalsoftware.com)

```
AUDIT add [options] user:Perms,FileInherit,DirInherit
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
             user:... file file ... [-x file file ...]
       AUDIT del [options] user:Perms,FileInherit,DirInherit
             user:... file file ... [-x file file ...]
       AUDIT clear [-b] [-r] [-usepriv] file file ... [-x file file ...]
       AUDIT protect [options] file ... [-x ...]
       AUDIT autoi[nherit] [options] file ... [-x ...]
       AUDIT propagate dir dir ...
       AUDIT policy [-s server] show
       AUDIT policy [-s server] (enable|disable) (+-)event-name ...

Options:
       Perms       Series of audit types (listed below) to add or del.
                   Each type must have a + and/or - suffix. eg:
                      [r(+-)][w(+-)][x(+-)][d(+-)][p(+-)][o(+-)]
       FileInherit Windows 2000 File Inherited audit permissions
       DirInherit  Windows 2000 Directory Inherited audit permissions
       add         Add auditing flags
       del         Remove auditing flags
       clear       Remove all auditing flags
       policy      Change system auditing policy
       protect     Windows 2000. Enable auditing descriptor protection.
       autoinherit Windows 2000. Inherit ACLs from parent and mark as auto-inherited
       -r          Recurse into subdirectories.
       -noprop     Don't automatically propagate.
       -replace    Replace existing user's audit triggers with ones specified.
       -clear      Clear all auditing before adding.
       -usepriv    Allow audit to temporarily take ownership in order to
                   set permissions. Backup files privilege required.
       -autoprotect Windows 2000. If necessary, automatically turn on
                   descriptor PROTECTION to achieve desired access. Inherited
                   ACEs are copied.
       -hideprop   Don't show propagation output.
       -ru         Remove 'account unknown' access control entries
       -rd         Remove deleted and invalid entries
       -std        Redirect stderr to stdout
       -b          Return 0 if no errors or 1 if at least one error occured.
                   (Default is to return the number of errors encountered.)
       -x          Exclude these files from the list (may use wilcards).


  Audit types ---------------------------------------------
  NT 4.0                 Windows 2000 (case sensitive)
  R  READ                c READ DATA
  W  WRITE               t READ ATTRIBUTES
  X  EXECUTE             e READ EXTENDED ATTRIBUTES
  D  DELETE              a READ PERMISSIONS
  P  CHANGE-PERMISSIONS  A APPEND DATA
  O  TAKE-OWNERSHIP      C WRITE DATA
                         T WRITE ATTRIBUTES
                         E WRITE EXTENDED ATTRIBUTES
                         u FILE EXECUTE
                         b DELETE CHILD OBJECTS
                         y ACCESS_SYSTEM_SECURITY
                         D DELETE
                         P CHANGE-PERMISSIONS
                         O TAKE-OWNERSHIP
                         # New access control entries will apply to objects
                           and/or containers within this container only

  +     Audit successful operation event
  -     Audit failure operation event
  +-    Audit both success and failure
  user  A valid user or group name. You may specify up to 30 users.

Example: audit add user:r-w+- file

Global system auditing policy parameters:
   EVENT-NAME  DESCRIPTION
   logonoff    Logon and logoff
   objects     File and Object Access
   userrights  Use of User Rights
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
   usersgroups User and Group Management
   policies    Security Policy Changes
   restart     Restart, Shutdown, and System
   process     Process tracking
   diraccess   Directory service access
   logon       Account logon
```

Srvinfo.exe

This command-line tool displays information about a remote server, including available disk space, partition types, and status of services. It can be found in Windows NT or Windows 2000 Resource Kits.

```
srvinfo [-d] [-ns] [-s] [-v] [\\computer_name] [-?]

Where:

-d
shows service drivers and services.
-ns
does not show any service information.
-s
shows shares.
-v
gets version information for Exchange Server, Internet Information Services, and SQL
Server.
\\computer_name
specifies the name of a remote server. If omitted, information on the local computer is
displayed.
-?
displays a syntax screen at the command prompt.
```

Rmtshare.exe

Remote Share is a command-line utility that allows you to set up or delete shares remotely. It can be found in the Windows NT Resource Kit.

In order to run Remote Share, even to just view shares, you must have share changing permissions on the remote computers.

```
RMTSHARE  \\server
          \\server\sharename
          \\server\sharename=drive:path [/USERS:number | /UNLIMITED]
                               [/REMARK:"text"]
                               [/GRANT [user[:perm][ /GRANT user[:perm]]]]
                               [/REMOVE user]
          \\server\sharename=printername /PRINTER [/USERS:number | /UNLIMITED]
                               [/REMARK:"text"]
                               [/GRANT [user[:perm][ /GRANT user[:perm]]]]
                               [/REMOVE user]
          \\server\sharename [/USERS:number | /UNLIMITED]
                               [/REMARK:"text"]
                               [/GRANT [user[:perm][ /GRANT user[:perm]]]]
                               [/REMOVE user]
          \\server\sharename /DELETE

NOTE: if a sharename or path contains spaces, it should be enclosed
          in quotes:
            \\server\"with space"="c:\with space"

      perm can be Read, Change, or Full Control

EXAMPLE: RMTSHARE \Computer1Share1 /GRANT YourDomainYou:Read
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Nbtstat.exe

```
Displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over
TCP/IP).  Nbtstat.exe is included in Windows NT and Windows 2000.

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP
addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINs and then, starts Refresh
  RemoteName   Remote host machine name.
  IP address   Dotted decimal representation of the IP address.
  interval     Redisplays selected statistics, pausing interval seconds
               between each display. Press Ctrl+C to stop redisplaying
               statistics.
```

NmapNT.exe

nmap is a the most customizable network scanner ever. It has various options to perform stealth scans, ping scans, UDP scans, as well as a handful of other scan types. It can be obtained from eEye Digital Security. (http://www.eeye.com/)

nmap also has the ability to remotely fingerprint an IP address. In other words, by sending various queries to a remote IP address and reading the responses, nmap can determine which operating system the remote IP address is running or whether it is a router, a network printer, etc. In all, nmap's database contains over 500 unique fingerprints.

```
nmapNT V. 2.53 by ryan@eEye.com
eEye Digital Security ( http://www.eEye.com )
based on nmap by fyodor@insecure.org  ( www.insecure.org/nmap/ )

nmap V. 2.53 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
* -sS TCP SYN stealth port scan (best all-around TCP scan)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oM <logfile> Output normal/machine parsable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
```

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

Securing Windows NT: Step by Step. Fossen, Jason. The SANS Institute.

"Windows NT Security Guidelines, Considerations and Guidelines for Securely Configuring Windows NT in Multiple Environments." A Study for NSA Research. Sutton, Steve. Trusted Systems Services, Inc.

Windows NT Resource Kit Tools, Microsoft

Effects of Machine Account Replication on a Domain [Q175468], Microsoft

NMAP -- The Network Mapper, http://www.insecure.org/nmap/

© SANS Institute 2000 - 2002, Author retains full rights.

© Copyright 2000, Brendan Moon (bmoon@mail.com) – All rights reserved, duplication without permission is prohibited.
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: April 25th, 2017

Upcoming Training

SANS Security West 2017	**San Diego, CA**	**May 09, 2017 - May 18, 2017**	**Live Event**
SANS Northern Virginia - Reston 2017	**Reston, VA**	**May 21, 2017 - May 26, 2017**	**Live Event**
SANS Cyber Defence Canberra 2017	**Canberra, Australia**	**Jun 26, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**