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 Widows NT 4.0 based Networks
Requirement for GTNT SANS Certification

The intent for this paper is to fulfill a SANS GIAC
certification requirement. These exercises have been
performed on a Windows NT Server V4.0 with SP 5 installed.
The server supports no clients.

Please note in some screen shots there are black out and
white spaces. This was for my protection. The black outs
are spaces where my computer name and IP address are listed
is synonymous with my Cable Internet Service Provider. As
you can imagine, having both my IP and computer name will
open my home network to potential hacks.

The aspect of actually securing a computer network is a bit
obscure. Being that the Internet is a public resource,
there is never a way to make any network completely hack-
proof. Administrators can only make it harder for a hacker
to actually gain access. Whether in limiting the amount of
server and network information available to the public or
utilizing a combination of the technical suggestions noted
in this practical.

This paper provides examples of how to enforce effective
Information Security in a network environment. This paper
reveals tips and suggestions to make this possible.
Warning, this is a small-scale guide to securing a network.

Social Engineering

The most dangerous threat to the integrity of the security
on any network is the users and support staff. If users are
not educated regarding the importance of network security,
all other efforts will eventually fail.

Users are deadly to the network. What can be done? There
are many ways of educating your user community ranging from
brochures in new employee packages to postings in commonly
traveled areas. But no one is there to make sure they are
actually performing what you suggest.

A great way to make sure the users in your community become
aware of the security risk they impose is to flash notes
upon logon that the users will tend to read. Other methods
include setting up mandatory security seminars explaining to
the users what risks are imposed by carelessness on the
network. But that can only be done with upper management's
agreement to host these events.

Some basic precautions users should be aware of include
never giving information like user names and passwords to
anyone, whether in person or over the phone. Not to reveal
any type of network information they may posses, domain
names and RAS dial in numbers. There are other good
suggestion regarding guidelines to pass on to users which
can be found at

<div align="center">www.microsoft.com\security.</div>

So what is Social Engineering or 'SI'? SI is manipulating
users into revealing network specific, i.e any information
that can lead a hacker to a successful breach.

The following dialogue notes an example of a potential means
of social engineering. It is a help desk call between the
president of the company (played by the hacker) and a Help
Desk Agent (HD)

HD - Helpdesk this is John Speaking.
Hacker - Hey John, I am having problems logging onto my
system.
HD - OK what is your user ID?
Hacker - I don't know? I can't remember. It is usually on

the screen when I log on. I never have to worry about that.
HD - OK What is you first and Last name?
Hacker - Steve Page (President of the company)
HD - Ohhh, Mr. Page, let me get you your User ID. I am
sorry to have kept you waiting.
Here it is.
Hacker – Great. Thanks. Do you mind staying on with me
while I try to get into it?
HD - Oh course, anything you need sir.
Hacker - Oh. I just typed in my password and it says it is
wrong. I dont think I have changed it anytime recently, nor
has my secretary.
HD - OK no problem sir. I will reset it to the word
password, and you will be prompted to change it when you
next log-in.
Hacker - Wow that is great. What is your name?
HD - John Doe.
Hacker - Well John thanks again, I will be sure to mention
how helpful you were next time I meet with your manager.
HD - Well thank you sir, and my pleasure.
Hacker - goodbye.

Now this hacker has the password to the president of the
companies' LAN account.

Helpdesk agents not aware that SI forms similar to this
example can and eventually will unknowingly undermining the
network. An undereducated support staff is the biggest hole
in any network. Informing agents of Social Engineering is
the key to stopping it.

In addition, policies should be set regarding resetting
passwords, access to network drive areas, revealing RAS dial
in numbers, and most importantly, working with your
companies' human resource department to obtain confidential
employee data for verification purposes.
Many companies find this data to be top secret, but there
are always alternatives. Request that HR releases the last
for digits of the Social Security numbers and the employees
home phone number. In-putting the data in the helpdesk
utility and enforcing policies stating this data must be
checked before any passwords or account information is
revealed.   This is a good start to preventing certain forms
of Social Engineering.

How to technically start

One option of the analysis and discovery portion of security
audit of a Windows NT network is to run a port scan on key
machines. Key machines are Primary Domain Controllers and
Backup Domain Controllers. Because the examples given in
the paper are from a mock network, the only node that exists
on the network is an NT 4.0 Server running service pack 5.

Port scanning is, in short, scanning through all 65000+
ports on your Server and detecting which ports are open. A
common way to explain it is going door to door in you
neighborhood, and turning each knob to see if you can
acquire access to the home, or port in our case.

Running port scanning software is fairly easy and there are
huge amounts of free utilities to use from the Internet. A
good overall site for utilities that deal with Network
Security is

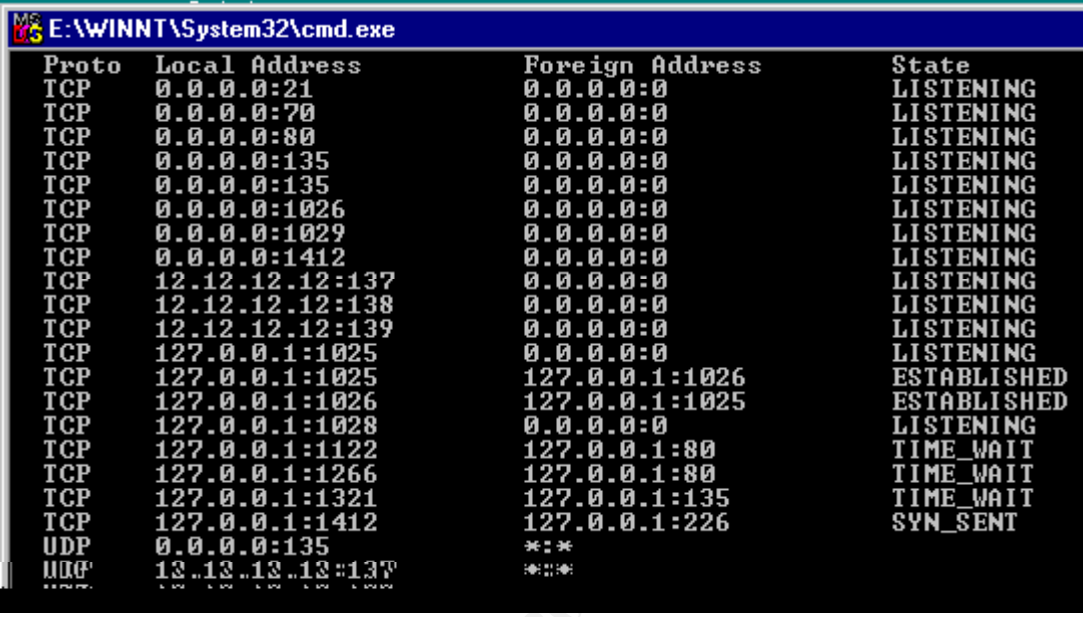   www.astalavista.box.sk.

Here, if you search for key words like 'Pots Scanner' you
will find hundreds of utilities.

I am using WS Ping Pack Pro. I scan the IP address
127.0.0.1 on ports 1 to 1000 for this example.
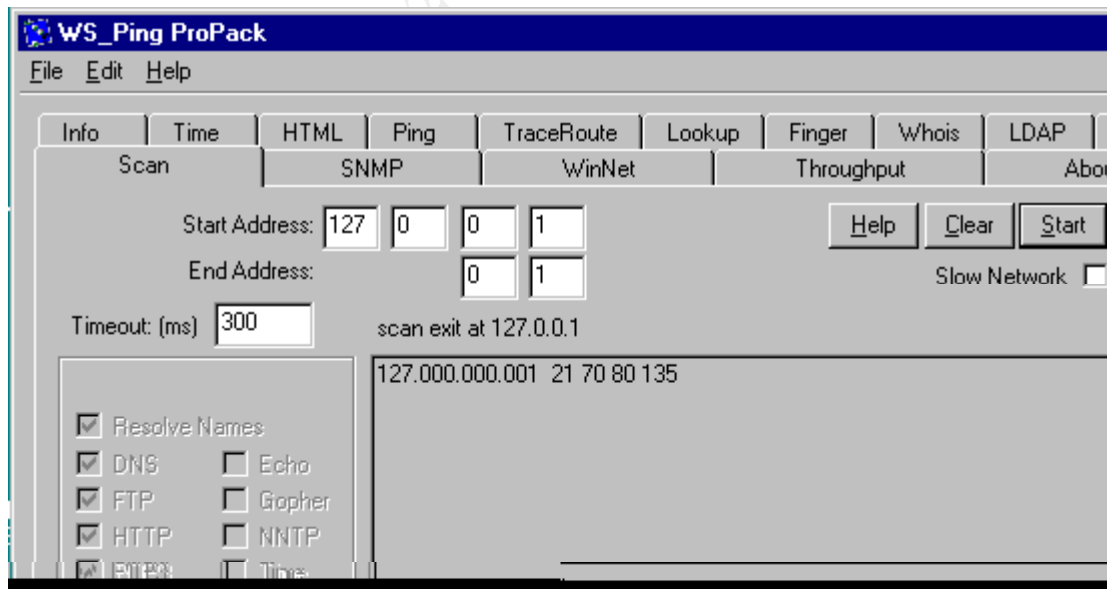
In the above screen shot, note the ports that are reported
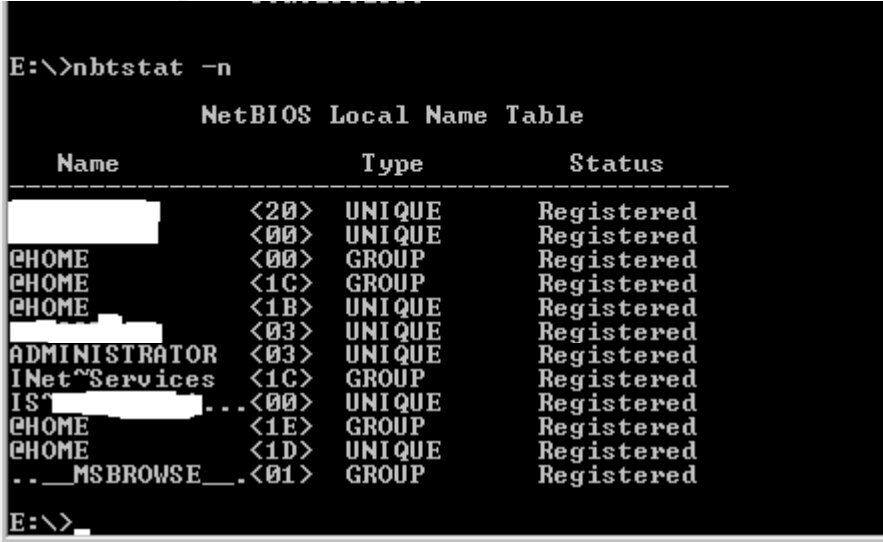as open when only scanning port numbers 1 to 1000.

A hacker or administrator may use a DOS command called netstat. Netstat works the same as a port scanner. The following is the result of using NETSTAT on the example server.

```
E:\WINNT\System32\cmd.exe
Proto  Local Address          Foreign Address         State
TCP    0.0.0.0:21             0.0.0.0:0               LISTENING
TCP    0.0.0.0:70             0.0.0.0:0               LISTENING
TCP    0.0.0.0:80             0.0.0.0:0               LISTENING
TCP    0.0.0.0:135            0.0.0.0:0               LISTENING
TCP    0.0.0.0:135            0.0.0.0:0               LISTENING
TCP    0.0.0.0:1026           0.0.0.0:0               LISTENING
TCP    0.0.0.0:1029           0.0.0.0:0               LISTENING
TCP    0.0.0.0:1412           0.0.0.0:0               LISTENING
TCP    12.12.12.12:137        0.0.0.0:0               LISTENING
TCP    12.12.12.12:138        0.0.0.0:0               LISTENING
TCP    12.12.12.12:139        0.0.0.0:0               LISTENING
TCP    127.0.0.1:1025         0.0.0.0:0               LISTENING
TCP    127.0.0.1:1025         127.0.0.1:1026          ESTABLISHED
TCP    127.0.0.1:1026         127.0.0.1:1025          ESTABLISHED
TCP    127.0.0.1:1028         0.0.0.0:0               LISTENING
TCP    127.0.0.1:1122         127.0.0.1:80            TIME_WAIT
TCP    127.0.0.1:1266         127.0.0.1:80            TIME_WAIT
TCP    127.0.0.1:1321         127.0.0.1:135           TIME_WAIT
TCP    127.0.0.1:1412         127.0.0.1:226           SYN_SENT
UDP    0.0.0.0:135            *:*
UDP    12.12.12.12:137        *:*
```

Using NETSTAT in DOS, you can see there is a difference in the reporting. This is because NETSTAT reports on all ports, not just a selected range.

A DOS utility commonly used by hackers is NBTSTAT or NetBois Name Scanning. This utility is similar to NETSTAT, in that it is used to identify the services running on a particular machine.

```
E:\>nbtstat -n

          NetBIOS Local Name Table

   Name              Type         Status
---------------------------------------------------
                  <20>  UNIQUE     Registered
                  <00>  UNIQUE     Registered
@HOME             <00>  GROUP      Registered
@HOME             <1C>  GROUP      Registered
@HOME             <1B>  UNIQUE     Registered
                  <03>  UNIQUE     Registered
ADMINISTRATOR     <03>  UNIQUE     Registered
INet~Services     <1C>  GROUP      Registered
IS        ...<00>  UNIQUE     Registered
@HOME             <1E>  GROUP      Registered
@HOME             <1D>  UNIQUE     Registered
..__MSBROWSE__.<01>  GROUP      Registered

E:\>
```

Analyzing this report and comparing it with a list of
netbios names (found on MS Q163409) a hacker can determine
that on '1C' the domain controller is '@HOME' and on '20'
the File Server Service host is 'SERVERNAME'
For a list of port names to be identified by numbers, please
search on

                            www.microsoft.com,

With the utility 'NTSEC' a hacker using a ''NULL'' session
to connect has the ability to view the current registry
settings for passwords.

```
G:\SANS\ntsec>ntuser -s                policy
MIN PASSWORD LENGTH              0 characters
MAX PASSWORD AGE                 42d 22h 47m 31s
MIN PASSWORD AGE                 0d 0h 0m 0s
FORCE LOGOFF                     False
PASSWORD HISTORY                 0 changes
LOCKOUT DURATION                 0d 0h 30m 0s
LOCKOUT RESET                    0d 0h 30m 0s
LOCKOUT THRESHOLD                Disabled

G:\SANS\ntsec>_
```

With this information, hackers can restrict the large range
of possible password cracker dictionaries and routines to
the specific password characteristics of the target network.

Sound Decision Making while Setting Password Protection

Requiring users to have passwords and to have passwords with
strong requirements associated with their user accounts is
one of the most important keys to securing your network.
Generally speaking, users do not understand the concepts of
creating strong passwords, nor do they think there is a
valid reason. One suggestion is to set up an Information
Security Awareness Campaign at your company.

Standards set up on your network should be based on a few
key concepts. Ask yourself if the company you are securing
is a vendor for an organization that does contracting work
for the government, military, or other highly secure
organization. If so, they may require minimum password

standards in order to exchange data.

If this does not apply to you, you have the challenging job
of creating password requirements that are approved by
management, do not result in an influx of calls to the help
desk, and do not trigger threats of harm because of the new
crackdowns.

There are many utilities that exist to ensure users do
adhere to minimum password standards. PASSFLT is a registry
change found in Windows NT Server 4.0 SP 5 or greater, which
requires minimal password standards. These standards
include requirements for passwords containing three of the
following four options: uppercase, lowercase characters,
numbers, and non-alphanumeric symbols.

Please note the following registry path:

        Hive: HKEY_LOCAL_MACHINE
        Key: \System\CurrentControlSet\Control\LSA
        Calue Name   NotificationPackages
        ValueType: REG_MULIT_SZ
        Value Data: PASSFILT
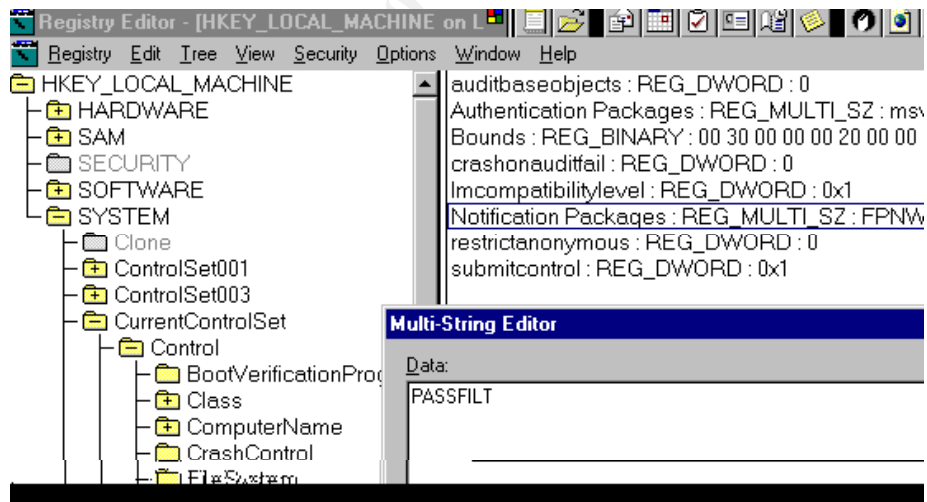
By making the change in the above screen shot, password
requirements are now activated.

In Service Pack 3 or higher, a utility found in the Resource
Kit called PassProp will enable the feature to lockout the
administer account when there are three or more unsuccessful

log-on attempts. In addition to enabling this feature, it
can also require password complexity for the administrator
account.

On the standard NT Server 4.0 install, the administrator
lockout feature is disabled, making it a target for hackers
to use a password guesser against it. With the account
lockout feature enabled on the administrator account, hacker
will only have three attempts to guess the password.

```
G:\reskit>passprop /adminlockout
Password must be complex
The Administrator account may be locked out except for interactive logon
on a domain controller.

G:\reskit>
```

The administrator account will only be locked out on remote
logons. The only way to log back on to the account is to
access it directly from the console of the server.

If registry setting changes are not permitable on the
network, or the ability to place different types of
restrictions on different types of accounts is necessary,
there are many third party utilities such as the GUI
interfaced Quakenbush Password Padlock. This utility can be
found at

www.quakenbush.com.

This utility allows a Security Administrator to set
different types of password standards on three types of
users: Administrators, Standard Users, and Guests. The
screen shot below shows the administrator accounts standards
in a network considered having high password standards.
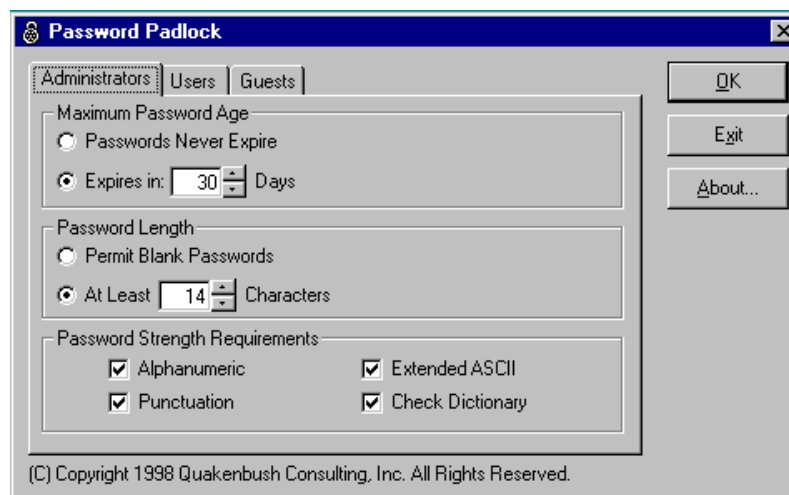
With this utility administrators will be set with strict
password standards. This includes a 30 day password
expiration period, 14 character passwords, and password that
include Alpha/Numeric, punctuation, and Extended ASCII
characters. Once the administrator successfully creates
their password, Quakenbush should be set to use a dictionary
scanner to ensure the password can not be easily guessed.

When a password cracker like 'l0pht' is used against the
'SAM' database (covered later in this paper), the high
security levels of the administrator accounts' passwords
would take months to crack. By requiring the passwords to
expire in 30 days, if the hacker cracks the password, the
administrator account password has already been changed and
the hacker has to start from scratch.

When the administrator tries to change the password to
'luckyduck', the following error occurs:
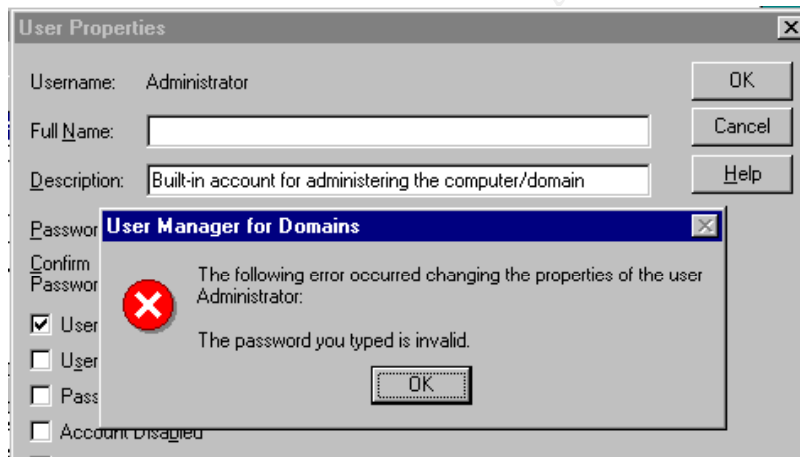
If the administrator uses the password <u>Th*$78luckyduck</u>,
where * equals the ASCII character 013 or 'Return Carriage'
it will be accepted.

Standard users have been set up through Quakenbush to have
passwords set with a minimum of 7 characters, which expire
every 60 days, and require a punctuation mark in the
password. They are also set to have their passwords checked
against a dictionary.
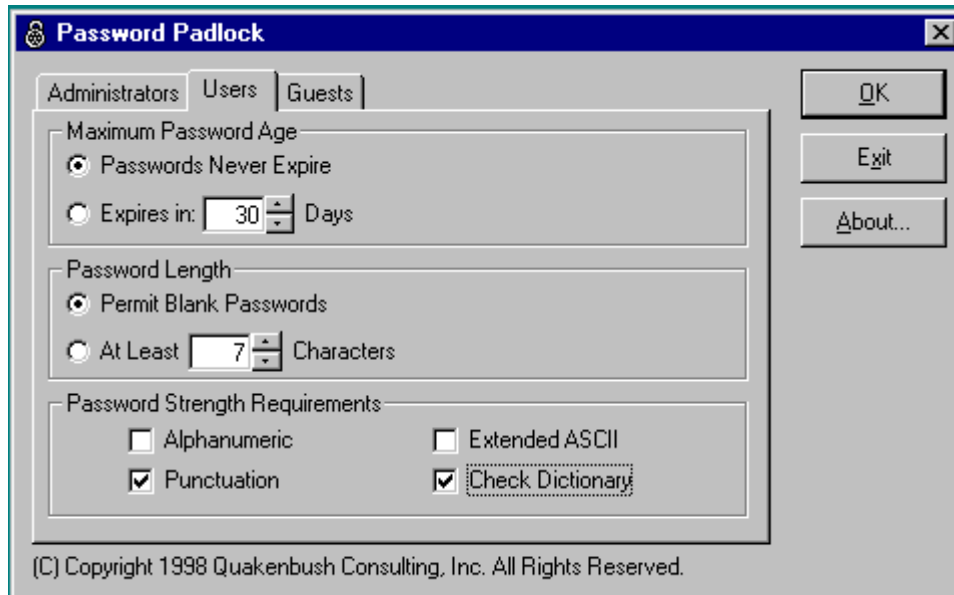
In the case of this network, I am using the Microsoft
Security Configuration Editor or SCE. This utility is
available for use with Windows NT 4.0 Server running SP4 or
later and Microsoft Internet Explorer 3.0 or later.

It serves three functions. The first is to define a
template of security configuration settings. The next is to
compare the local machine's settings against a template.
Third, it configures the local machine's settings to match a
template.

SCE provides features that allows for the configuration of
the password policy, account lockout policy, audit policy,
user rights assignments, event logs setting, group
membership, system services options, registry values,
registry permissions and auditing, and NTFS folder/file
permissions and auditing.

After running a Security Analysis on the current systems
settings and comparing it to a system template considered to
have high password settings, the SCE reported there existed
no password uniqueness, no minimum password age, no minimum
password length, and password complexity requirements were
disabled.

Note the screen shot below.

Settings on a network that are this weak can result in
breeches of the network. A hacker is able to create a
'NULL' session and easily download the following
information.

With this information a hacker can set their password
cracker to do its job based on the above settings.

To secure these features, a new template was created, set
with the following requirements, and compared to the setting
of a high security network:

With the proper control of the 'NULL' session this data will
not be able to be accessed, but if it is, the network is now
securing with a high password security standard:

'NULL' USERS AND HOW TO PREVENT THEM
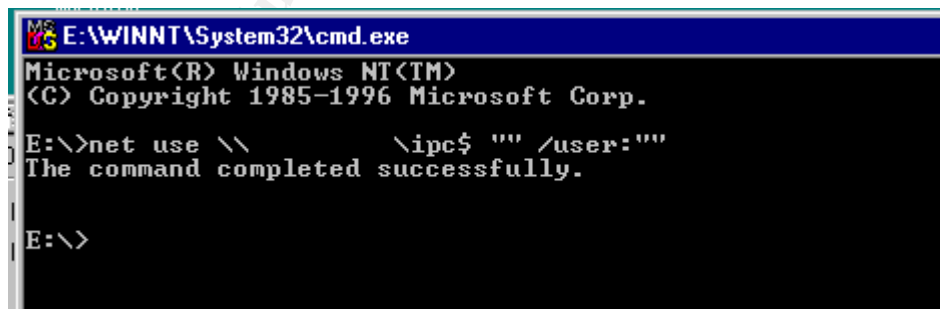
When securing your network, a System Administrator needs to
consider the existence of a 'NULL' Session. Before defining
the vulnerabilities and ways of correcting this threat, a
full understanding of 'NULL' session is necessary.

A 'NULL' session is not a guest or anonymous account. Users do not enter any characters for a password or user ID when logging into the 'NULL' session. Simply, if the proper precautions are not taken, it is a universal path into any network by connecting through DOS commands.

They exist for multiple reasons. The major reason is for administrative purposes for IS support staff. It is also built into some programming applications for various data uploading. Mostly, it is there to open a giant gaping whole into the networks of companies using the wonderful NOS called Windows NT.
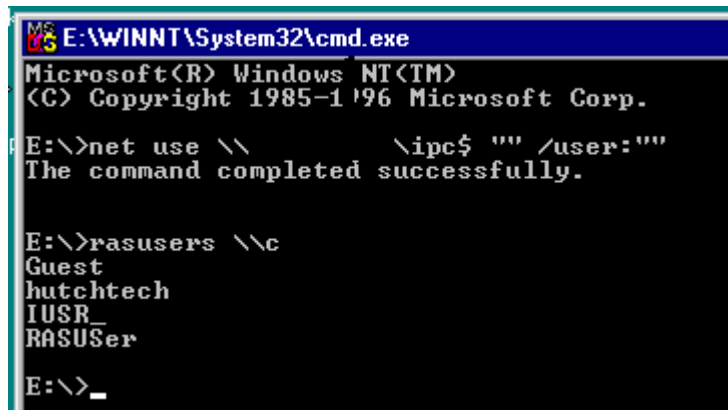
Once a 'NULL' session is established, a hacker has complete access to any shared folders with the NTFS permissions set to everyone. In addition and most importantly, this session, by default can gain access to the %systemroot\system32\repair\SAM._ which houses the Security Administration Management or SAM database file.   The SAM database is a file created, in short, to backup User ID's and their password hashes, for all users on the network.

The following Screen Shot depicts gaining access to a 'NULL' session.


```
E:\WINNT\System32\cmd.exe
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

E:\>net use \\          \ipc$ "" /user:""
The command completed successfully.


E:\>
```

Once a 'NULL' session is opened, a hacker can run a utility called 'RASUSERS' to determine which user accounts on the network have dial-in access to the network.
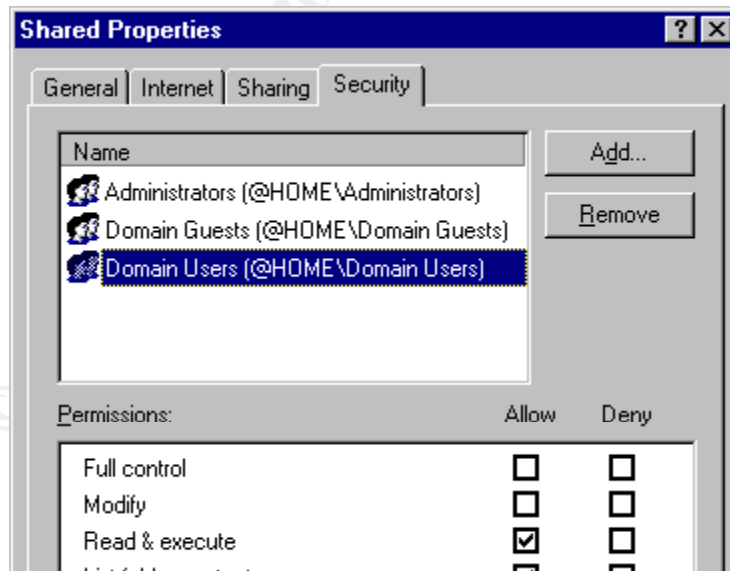
```
E:\WINNT\System32\cmd.exe
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1'96 Microsoft Corp.

E:\>net use \\           \ipc$ "" /user:""
The command completed successfully.


E:\>rasusers \\c
Guest
hutchtech
IUSR_
RASUSer

E:\>_
```

Note that the account guest, hutchtech, iusr_Computer Name, and RASuser have dial in access to the network. All a hacker needs to gain access to the network is the Dial in number and a good password guessing program.

By default, 'NULL' sessions have access to all file and folders belonging to the Everyone Group and the Network Group. To prevent a 'NULL' session from accessing the date in these groups, the NTFS permission on shared drives should be set up with groups that only include the Authenticated users.

```
Shared Properties                                    ? X
 General | Internet | Sharing | Security |

  Name                                          Add...
   Administrators (@HOME\Administrators)
   Domain Guests (@HOME\Domain Guests)         Remove
   Domain Users (@HOME\Domain Users)



 Permissions:                          Allow    Deny
   Full control                          □       □
   Modify                                □       □
   Read & execute                        ☑       □
   List folder contents                  ☑       □
```

Groups including Domain Users and Domain Guests only allow
users that have authenticated to the network to access the
data in this folder.

Other possibilities of a 'NULL' session are the potential of
gaining registry information, permission settings, and other
information about your network. One such utility to obtain
this information is called DumpSEC from

www.Somersoft.com.

This application has the ability to gain a large range of
account information. Refer to this software for greater
examples.
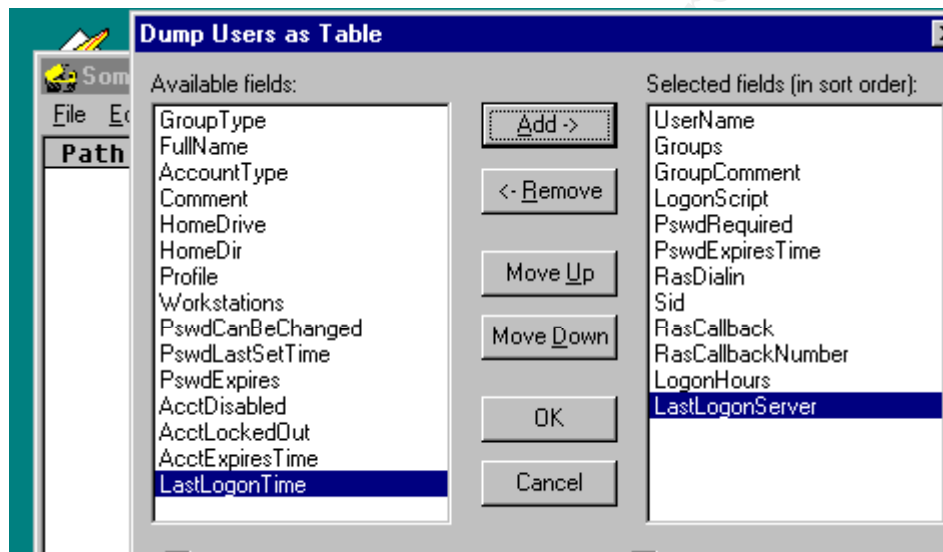
Having this information readily available to anyone
interested in finding it raises the question of 'How to
prevent it'?

A simple registry change removes the ability for a 'NULL'
session to access User Names and other such information
about one's network.

Hive: HKEY_LOCAL_MACHING
Key: \System\CurrentControlSet\Control\LSA
Value Name: RestrictAnonymous
Value Type: REG_DWORLD
Value Data: 1

After making this registry change, 'NULL' sessions will not

be able to list this type of data.

Preventing access to the SAM Database

Security Account Manager or 'SAM' database contains the
LanManager and MD$ hashes of users' passwords. Basically
this is the database where all the users on your network
specific User ID and the associated password hash is stored.

A password hash is the breakdown of your password into an
encrypted challenge/response authentication code. This hash
can be translated into the actual password using the utility
'L0pht'.

Note the screen shot below of a crack of the SAM database in
progress. Total time left to the crack is almost 20 hours
but you can see in the LANMan Password column some passwords
have already been cracked.

Some hackers will break into your system just to perform a
DOS or Denial of Service attack. A DOS attack is stopping
any services your network provides. There are numerous ways
of executing a DOS attack from the BSOD or Blue Screen of
Death caused by a lack of free hard drive space to SYN
flooding.

Prevent Denial of Service

Hackers will try to fill up all available hard drive space
on your network to cause a BSODDOS. A hacker may connect to
a network drive of a user and if restrictions are not set, a
hacker can upload data to this folder or any folder, and
utilize all remaining hard disk space.

There are tips and suggestions on how to prevent this from
happening. In this network plenty of RAM has been
installed, and the NOS is loaded on a separate partition.
If the hacker decides to cause a DOS using this rout, they
still will be able to utilize all free disk space but they
will not cause a DOS because the NOS is running on another
partition. In prevention, limits have been placed on the
maximum size a user's home drive can grow.

Setting Permissions on Files and Folders

Deciding the levels of security needed on a network depends
on what type of data you are protecting. If you are trying
to protect data that is freely viewable for everyone in the
company, the NTFS permission can be set up loosely.
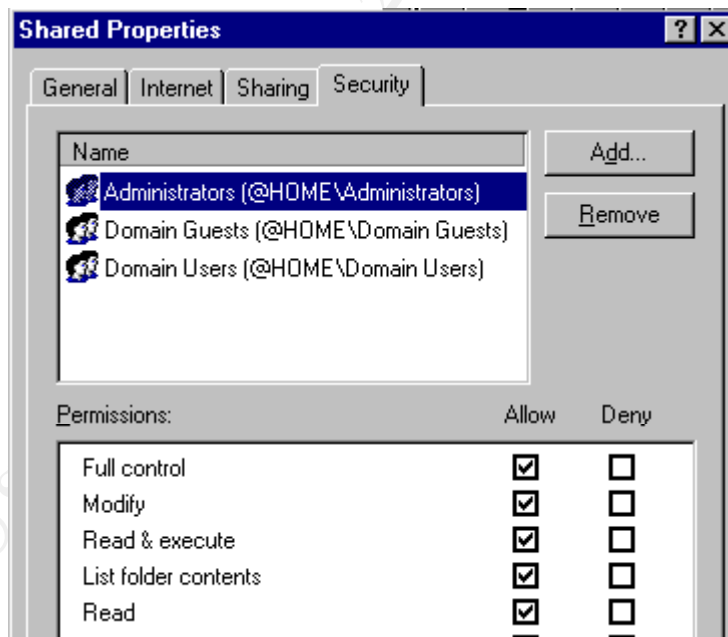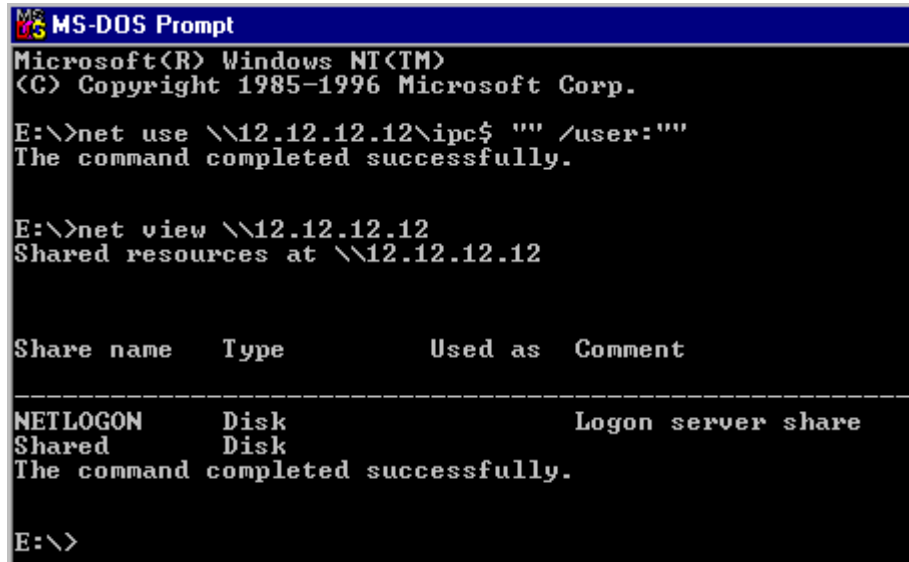
The folder named shared has been set up for Administrators
to have full control of the folder, Domain Guests to only
have read and execute, and for Domain Users to have change

control.   The difference between Full Control and Change
control is Full control has the ability to add Users and
Groups to the folder or file, and change can not.
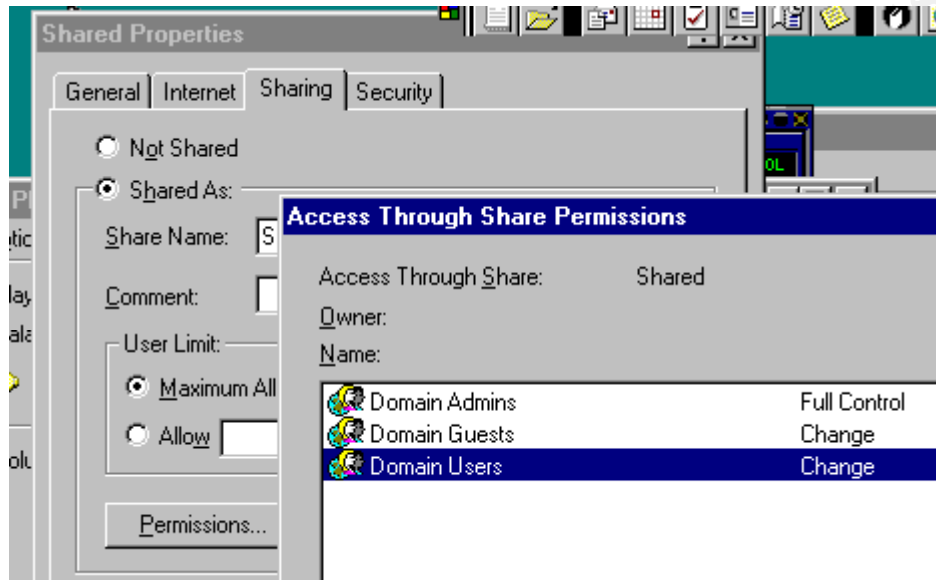
Viewing the folder share permissions, note that the only
difference between the NTFS setting and the Share setting is
Domain Guests have Change Control.   In the current setting,
Domain users will have change control even though the NTFS
permission are set for Read and Execute only.

Hackers will use 'NULL' sessions to try to list share names.
If the shares are set to allow the Everyone Group to access
the data, then the hacker can map to the drive he or she has
discovered.   By default in Windows NT 4.0 Server, 'NULL'
sessions are able to list shared names,

A registry change will stop 'NULL' sessions from accessing
share folder listing:

```
Hive:           HKEY_LOCAL_MACHINE
Key:            \System\CurrentControlSet\Control\LSA
Value Name:     RestrictAnonymous
Value Type:     REG_DWORLS
Value Data:     1
```
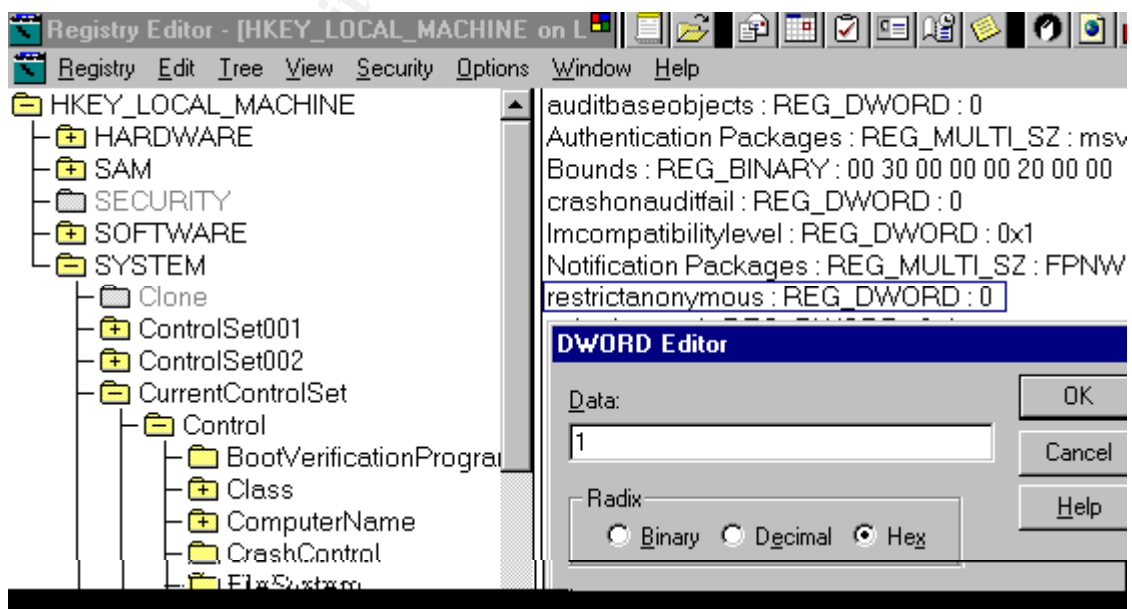
With this change made, a hacker will no longer be able to access shared name listing with a 'NULL' session.


Setting up auditing

Certain types of auditing should to be set up to have a secure network. But auditing is restricted to how much disk space you want to utilize. You can manually regulate how much disk space you want to use for your log files and determine whether or not the files should be overwritten or manually deleted. The screen shot below identifies the setting on this network for Security logs. Note that System and Application logs have been set the same.
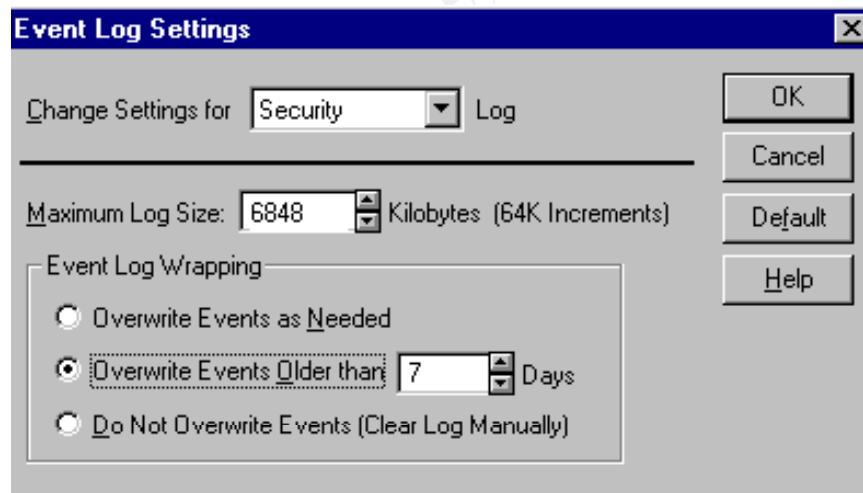
With the setting in place for the log files, it now should be determined what types of auditing will be reported in the logs on a system wide and folder by folder basis. The following screen shot is the settings for the systems wide auditing trail:
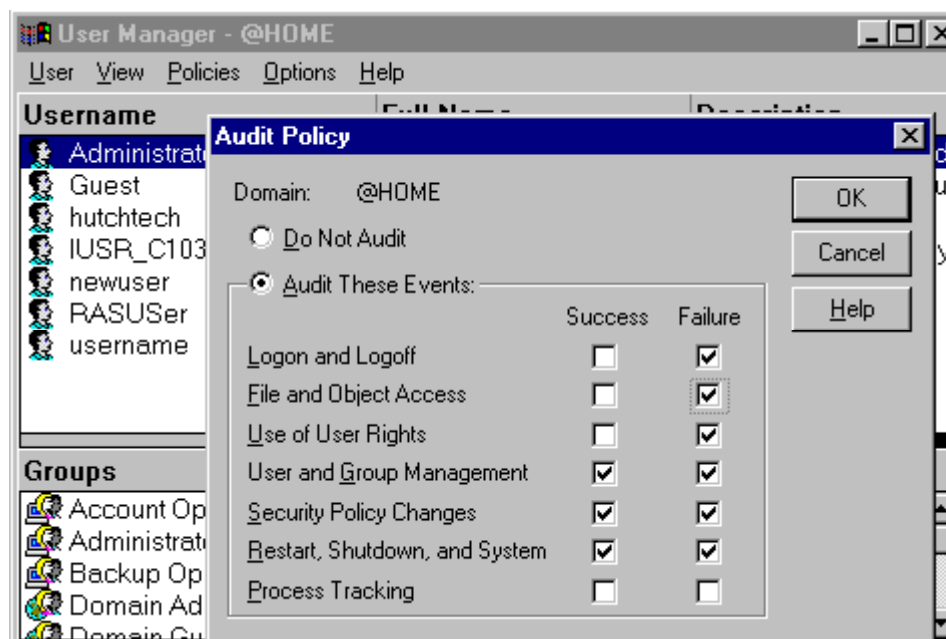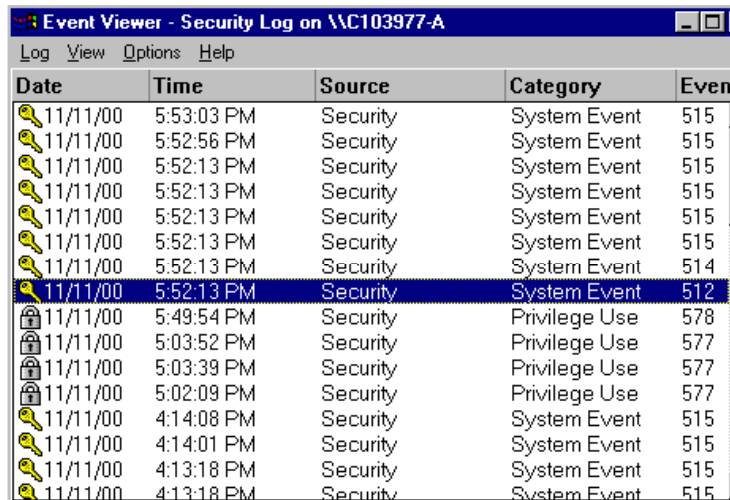
Auditing is also set up on specific folders, in order to
monitor what data is being accessed and by whom. The screen
shot below depicts the setting of the auditing for the
folder called Shared:
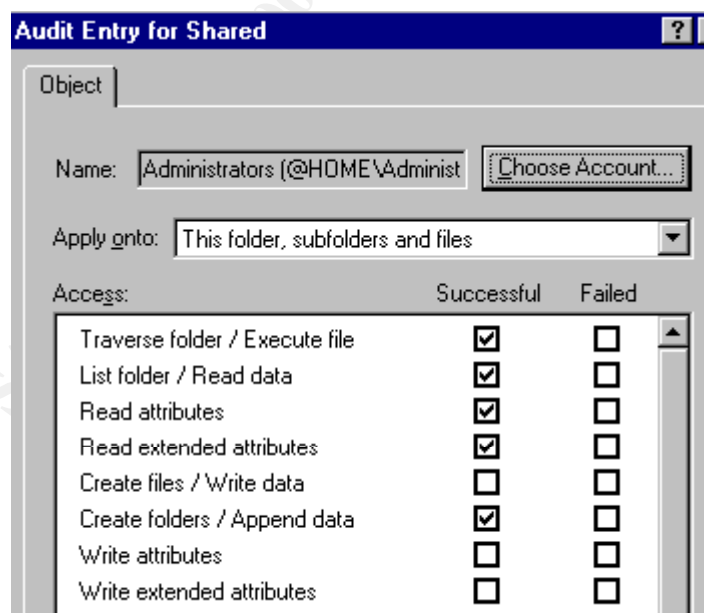
Using the Event Viewer and selecting the Security Log, I can
see all events that were selected to be audited in a row by

column basis:

Securing a network must be thought of as more then what is
covered in this paper. Many considerations need to be
reviewed and discussed before identifying a plan of attack
when securing a network. Some basic ideas and concepts
should be practiced for all networks including minimal
password standards and 'SAM' database encryption. Some more
advanced networks may need greater security imposed like
Intrusion Detection Software and Firewalls.

In either case there is always a threat when your network is
attached to the Internet or is just set up for internal use.
Sometimes the greatest threat to a network is the users
themselves.

In network setting, company employees often install modems
on computer that are logged on to a network. Then these
employees use software like 'PC ANYWHERE' to connect to
their work computers from home. When running a 'War Dialer'
a hacker can identify where these modems exist and connect
to a network without having to avoid detection or spend time
trying to hack through firewalls and passwords. There are
endless concepts that have been looked over for reasons of
time limitations (and my sanity). Virus Protection should
always be set up on both network clients and network

servers. Changing the name of the administrator account and setting up a 'Honey Pot' to lure hackers into a trap you set for them.

Intrusion Detection and Firewall software is also very important for a network to be secure. This software can be quite expensive and difficult to grasp the concepts of. Both have such intricate details that can't be covered in this paper.

One of the most important and easiest forms of securing a network is tape backup. Even if a network administrator takes the proper precautions to secure the network, there are always ways around the prevention. Being that the Internet is a public resource, there is never a way to make any network completely hack-proof. Administrators can only make it harder for a hacker to actually gain access.

Credits:

SANS NETWORK SECURITY 2000
Securing Windows NT, Step by Step, Parts 1-3
Jason Fosssen
Jennifer Kolde