



Fall 2005

Remote Dictionary Attack Against Terminal Services

What is a dictionary attack?

Passwords are the weakest link in the security chain. People have a very difficult time remembering strong passwords. Often times, they will choose a word, or a derivation of a word as their password. This can make the job of an attacker much easier than if the user had chosen a secure password using numbers and symbols.

If an attacker is trying to guess a users password, he can use the dictionary as a list of passwords to try. Electronic versions of English dictionaries contain thousands of words. Many of these dictionaries have duplicate entries for each word, where certain letters have been replaced with symbols that resemble them. (mary, m@ry, nnary, nn@ry, ...) Attempting to guess a user's password by *throwing a dictionary* is known as a dictionary attack.

What is Terminal Services (Remote Desktop Connection) ?

Remote Desktop Connection is a service built into many editions of Microsoft Windows that allows a user to connect to their computer remotely. Once connected, the remote computer takes up the whole screen, as if the user was sitting right behind the remote computer. All key-strokes and mouse-movements are sent to the remote computer. Terminal Services is another name for Remote Desktop Connection.

What is TSCrack 2.1?

TSCrack 2.1 is an application that was written to run on Microsoft Windows 2000 and *throw a dictionary* at a computer which accepts remote connections to the Remote Desktop service. By default, it will try to login using the "Administrator" account. This is because other accounts will lock themselves up if they receive too many incorrect login attempts. However, the Administrator account never locks-out. TSCrack was the first program that was written to throw a dictionary at the Remote Desktop service. There is another application now available called TSGrinder that is similar, but newer.

What are some of the drawbacks of TSCrack 2.1?

Both TSCrack and TSGrinder were written as proof-of-concept applications. They both have serious drawbacks that can make them difficult to use effectively. TSCrack will only work from Microsoft Windows 2000. It will not work properly on Windows XP.

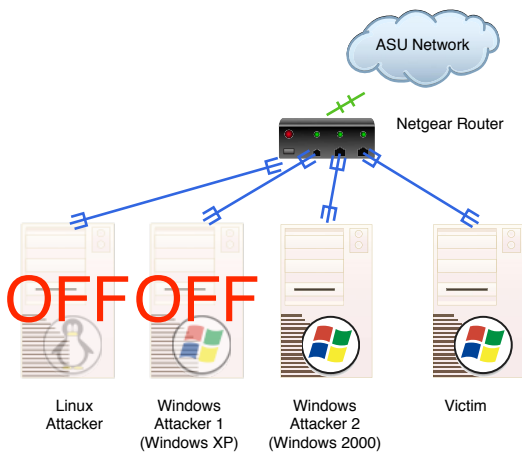
Both of these applications share a very serious drawback. When connecting to a remote computer with the login "Bob", if a user "Sarah" is already on the remote computer, then RDP will show a message saying that someone else is already using the computer. (By this point, you know your password is correct. A well written application would save this password and then try to login again later when Sarah was gone.) However, both of these applications misinterpret this error message as a failed login, and move onto the next password in the dictionary.

Because of this drawback, these applications only work when

- a) the remote computer is already at the login screen with no one currently using it, or
- b) when the Administrator is currently using the machine, since the Administrator account is the one for which you successfully 'guessed' the password.

TSCrack takes a screen shot of the Remote Desktop window, and uses neural networks to interpret it's meaning. It is somewhat slow, only trying three passwords a second. TSGrinder uses a more efficient method which allows it to try passwords at a faster rate. TSGrinder is not limited to Windows 2000.

How was our attack setup ?



Network Setup: The Netgear router is setup as a DHCP server. It assigns IP addresses in the range 192.168.0.2 - 192.168.0.5. The router's DMZ and it's Port forwarding are disabled. Computers are allowed to connect outwardly to the ASU network (and to the internet) but inward connections are not allowed.

Computer Setup: Our victim computer is a Windows XP machine. Our attacker machine is a Windows 2000 machine.

The Windows XP (victim) machine is setup to allow remote desktop connections for the Administrator account. Because of the limitations described above, the user must log into the victim machine locally as the Administrator. (Normally, the user logs in via the "Admin" account. However if the local user is logged into

the "Admin" account and the attacker successfully chooses the "Administrator" account password, TSCrack will not realize that it has found the correct password, as described above.)

To commence the attack, the attacker machine starts running TSCrack against the victim. TSCrack comes with a very basic dictionary, so that it was replaced with a more complete dictionary. The correct password was placed in the middle of the dictionary file so that it would be reached after about 10 minutes of incorrect attempts.

	A	B	C
4	Operating System	Windows 2000 5.00.2195	Windows XP
5	Service Pack	4	2
6	Processor	Pentium 4 3.00GHz	Pentium 4 3.00GHz
7	RAM	1 GB	3.00 GB
8	Login Type	Professional	Professional
9	Username	Administrator	admin for most attacks, "Administrator" for tscrack
10	Centurion	none	Hardware Centurion
11	Software Setup		
12	Automatic Updates	Disabled	Disabled
13	Microsoft Office	2003	2002
14	Adobe Acrobat	yes	
15	RSA Authentication Manager		
16	Solar Winds Engineering Edition		
17	others	tscrack	Allows Remote Desktop Connections to the Administrator's account.
18	Startup Software		
19	NvCpl (Nvidia Display)	yes	yes
20	censtat (Centurion)		yes
21	Microsoft Office		yes
22	netcat (bindhsell for automation)		installed for all attacks except FU rootkit
23	gcasServ (Anti-spyware)	yes	
24	cftmon (speech input for Office)	yes	
25	VpnTool (RSA software)		
26	Anti-virus	McAfee	