Welcome to BlackHat!

Black Hat USA 2003 Briefings and Training

Las Vegas July 28-31, 2003

Timothy M. Mullen
AnchorIS.Com, Inc.

Ryan L Russell

TSGrinder

Terminal Server brute force password guessing tool

Black Hat Las Vegas – July 2003; Timothy M. Mullen, AnchorIS.Com; thor@hammerofgod.com

Need

- Penetration testers do not have a good automated tool for testing Terminal Services authentication
- Should work with a variety of RDP versions
- Should allow password permutations
- Should use as many simultaneous channels as the server allows
- Every authentication protocol should have a brute force guessing tool

Possible ways to accomplish

- Reverse engineer the RDP protocol from scratch
- Use rdesktop from rdesktop.org
- Use smclient from Win2K Server Resource Kit
- Hook mstsc.exe

Reversing engineering the RDP protocol

- Yeah, right. (but see next slide)

rdesktop.org

- Portable, independently-created RDP client implementation.
- Fairly functional
- Closest thing to public documentation of the RDP protocol
- Doesn’t deal with text, it deals with glyphs (D’oh!)

Smclient

- Looks almost exactly like what we want
- Allows limited scripting of input and output
- Allows multiple simultaneous clients
- Always tries each (bad) password 6 times. Why would it do that?

Hooking mstsc.exe

- Turns out, that’s exactly how smclient works.
- At least back to Win2K, mstsc.exe has an *undocumented API*.
- Yes, we were as shocked as you are.

/clxdll

- Mstsc.exe has a command-line option to use a dll with callback functions to hook the client.
- Command-line looks like:

```
mstsc.exe /CLXDLL=CLXTSHAR.DLL
  /CLXCMDLINE=hSMC=(hWnd)
  smclient_(procid)_(threadid)
```

tclient.dll

- Smclient.exe is a simple front-end to tclient.dll
- Tclient.dll appears to expose enough public functions to do what we want
- Problem is, the SCConnect function has a hard-coded 6 attempts per password. This also limits it to one password per connection.

Some notes on logging

- You get 5 bad password attempts, and the sixth attempt cuts your connection
- A log entry is created only if you make 6 bad attempts *on the same connection*
- If you make 5 attempts, and then disconnect, no log.
- That's why tclient.dll does 6 tries.

Performance

- We want to try multiple passwords per connection (up to 5)
- We want to have multiple clients attempting simultaneously, with coordination about who is doing which passwords.

Solution

- Write our own connect function
- Can use the rest of the function in tclient.dll as-is (some of which are not exported)
- Allows us to have the degree of control we need

Amusements

- Smclient is only half-done, doesn't actually work like the docs say
- Smclient is compiled in debug mode
- Turns out, tsgrinder crashes if in release (non-debug) mode. It crashes in tclient.dll
- I know why smclient.exe was shipped in debug mode.

Future enhancements

- Need help testing with non-English versions of terminal server
- Tell us what you'd like to see it do that it doesn't do now
- Mail ryan@thievco.com with requests

Demo