

Forum: [Hack Forums](#)

Thread: [\[service\] Free NTLM cracking \(US95 Len 8\)](#)

Frosteh - January 13, 2015, 12:48 am

Since I've been a member of these forums for a little while now I thought I'd give back a little bit where I can.

I have rainbow tables for NTLM up to and including length 8 for the entire US95 character set (you can get these from [Cryptohaze.com](#) but they're about 1.5Tb)

If you dump me any NTLM hashes you want checking against this set then leave them in this thread, since it doesn't take much longer to batch check multiple hashes but a single run is about 3-4 hours anyway, it's best to wait a while and do them in batches.

State whether you want any results posted or PM'd to you (for privacy) when they're found.

For anyone interested 95 characters at length 8 is 95^8 which is 6,634,204,312,890,625 combinations of letters, checked in approximately 4 hours is about 460,000,000,000 per second, this is limited by HDD read speed primarily, cracking on a GTX 980 and i7 2600k with 16Gb RAM.

Hope some of you can find this helpful! :)

chick3nman - January 13, 2015, 12:50 am

(Jan 13, 2015 01:48 AM)Frosteh Wrote: [\[CITE\]](#) Since I've been a member of these forums for a little while now I thought I'd give back a little bit where I can.

I have rainbow tables for NTLM up to and including length 8 for the entire US95 character set (you can get these from [Cryptohaze.com](#) but they're about 1.5Tb)

If you dump me any NTLM hashes you want checking against this set then leave them in this thread, since it doesn't take much longer to batch check multiple hashes but a single run is about 3-4 hours anyway, it's best to wait a while and do them in batches.

State whether you want any results posted or PM'd to you (for privacy) when they're found.

For anyone interested 95 characters at length 8 is 95^8 which is 6,634,204,312,890,625 combinations of letters, checked in approximately 4 hours is about 460,000,000,000 per second, this is limited by HDD read speed primarily, cracking on a GTX 980 and i7 2600k with 16Gb RAM.

Hope some of you can find this helpful! :)

Any you can't get pass to me and I'll run them with >8 restrictions through hashcat. Makes cracking them a little easier.

Frosteh - January 13, 2015, 12:53 am

(Jan 13, 2015 01:50 AM)chick3nman Wrote: [\[CITE\]](#) Any you can't get pass to me and I'll run them with >8 restrictions through hashcat. Makes cracking them a little easier.

Ok cool.

What are you doing there, are they dictionary attacks or brute force? What character set are you

using?

I think there's rainbow tables for >8 char's but they're for much smaller character sets like alpha only, be interested to hear what you have set up.

chick3nman - January 13, 2015, 1:19 am

(Jan 13, 2015 01:53 AM)Frosteh Wrote: [\[CITE\]](#) Ok cool.

What are you doing there, are they dictionary attacks or brute force? What character set are you using?

I think there's rainbow tables for >8 char's but they're for much smaller character sets like alpha only, be interested to hear what you have set up.

I'm doing dictionary+rules. Full keyspace brute force past 8 takes too long for it to be useful to anyone.

Frosteh - January 13, 2015, 1:30 am

Cool, yeah I figured. Brute forcing Length 8 at full US95 charset is a crazy number of calculations, I actually just tested the raw cracking power of my GTX 980 at stock speeds and it's 4500MH/sec or 4,500,000,000

So to cover the length 9 keyspace (95^9 or 630,249,409,724,609,375) without rainbow tables would take 1,621 days LOL, even Len 8 brute force is 17 days which is why the Rainbow tables that can do it in under 4 hours are so good.

chick3nman - January 13, 2015, 1:39 am

(Jan 13, 2015 02:30 AM)Frosteh Wrote: [\[CITE\]](#) Cool, yeah I figured. Brute forcing Length 8 at full US95 charset is a crazy number of calculations, I actually just tested the raw cracking power of my GTX 980 at stock speeds and it's 4500MH/sec or 4,500,000,000

So to cover the length 9 keyspace (95^9 or 630,249,409,724,609,375) without rainbow tables would take 1,621 days LOL, even Len 8 brute force is 17 days which is why the Rainbow tables that can do it in under 4 hours are so good.

I have a 7970 that will do about 18,000 MH/s or 18 GH/s and it would still take me forever to brute the 8 and 9 keyspaces. It's just not efficient to brute force anything past there.

Frosteh - January 15, 2015, 10:15 am

I just wanted to this in case anyone is interested.