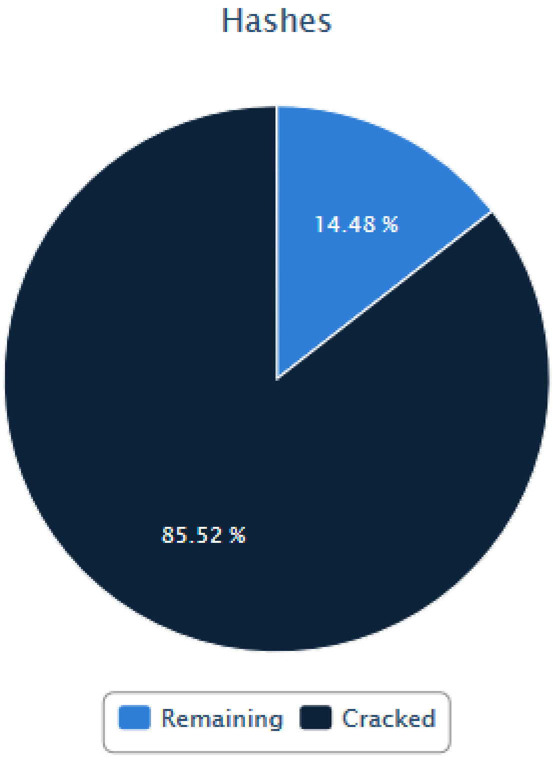
NetSPI’s Top Cracked Passwords for 2014

It’s been a big year for password cracking at NetSPI. We’ve spent a lot of time refining our dictionaries and processes to more efficiently crack passwords. This has been a huge help during our pentests, as the cracked passwords have been the starting point for gaining access to systems and applications. While this blog focuses on the Windows domain hashes (LM/NTLM) that we’ve cracked this year, these statistics also translate into the other hashes that we run into (MD5, NetNTLM, etc.) during penetration tests.

During many of our penetration tests, we gather domain password hashes (with permission of the client) for offline cracking and analysis. This blog is a summary of the hashes that we attempted to crack in 2014. Please keep in mind that this is not an all-encompassing sample. We do not collect domain hashes during every single penetration test, as some clients do not want us to. Additionally, these are Windows domain credentials. These are not web site or application passwords, which frequently have weaker password complexity requirements.

This year, we collected 90,977 domain hashes. On average, we still see about ten percent of domain hashes that are stored with their LM hashes. This is due to accounts that do not change their passwords after the NTLM-only group policy gets applied. The LM hashes definitely helped our password cracking numbers, but they were not crucial to the cracking success.

Of the collected hashes, 27,785 were duplicates, leaving 63,192 unique hashes. Of the total 90,977 hashes, we were able to crack 77,802 (85.52%). In terms of cracking effort, we typically put about a day’s worth of effort into the hashes when we initially get them. I did an additional five days of cracking time on these, once we hit the end of the year.



Here’s nine of the top passwords that we used for guessing during online brute-force attacks:

- Password1 – 1,446
- Spring2014 – 219
- Spring14 – 135
- Summer2014 – 474
- Summer14 – 221
- Fall2014 – 150
- Autumn14 – 15*
- Winter2014 – 87
- Winter14 – 63

*Fall14 is too short for most complexity requirements

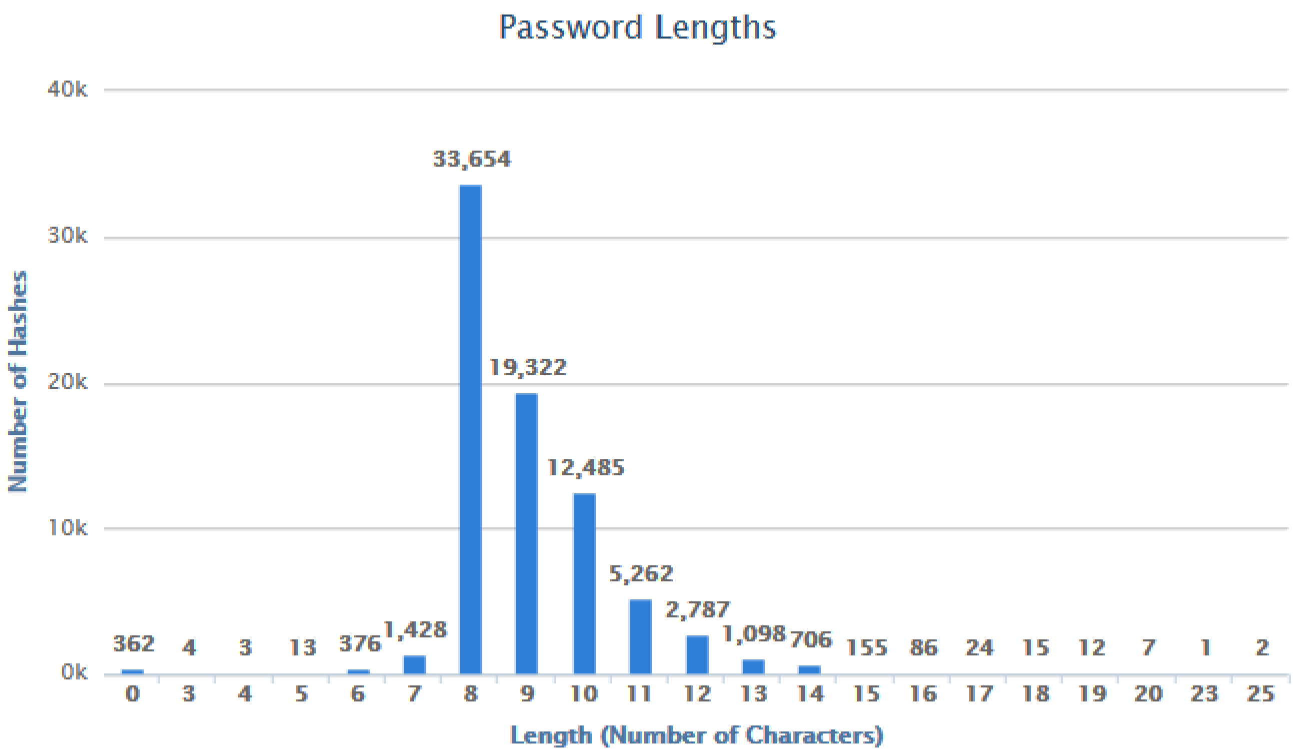
Combined, these account for 3.6% of all accounts. These are typically used for password guessing attacks, as they meet password complexity requirements and they’re easy to remember. This may not seem like a large number, but once we have access to one account, lots of options open up for escalation.

Other notable reused passwords:

- Changem3 – 820
- Work1234 – 283
- Password2 – 142
- Company Name followed by a one (Netspi1)

Cracked Password Length Breakdown:

As you can see below, the cracked passwords peak at the eight character length. This is a pretty common requirement for minimum password length, so it’s not a big surprise that this is the most common length cracked. It should also be noted that since we’re able to get through the entire eight character key space in about two days. This means any password that was eight characters or less was cracked within two days.



Some interesting finds:

- Most Common Password (3,003 instances): [REDACTED] (This one was very specific to a client)
- Longest Password: **UniversityofNorthwestern1** (25 characters)
- Most Common Length (33,654 instances – 43.2%): **8 characters**
- Instances of "password" (full word, case-insensitive): 3,266 (4.4%)
- Blank passwords: 362
- Ends with a "1": 10,025 (12.9%)
- Ends with "14": 4,617 (6%)
- Ends with "2014": 2645 (3.4%)
- Passwords containing profanity ("7 dirty words" – full words, no variants): 48
- Top mask pattern: **?u?l?l?l?l?l?d?d** (3,439 instances – 4.4%)
  - Matches Spring14
  - 8 Characters
  - Upper, lower, and number
- The top 10 mask patterns account for 37% of the cracked passwords
  - The top 10 masks took 25 minutes for us to run on our GPU cracking system
- One of our base dictionaries with the d3ad0ne rule cracked **52.7% of the hashes in 56 seconds**

Note: I used Pipal to help generate some of these stats.

I put together an hcmask file (to use with oclHashcat) of our top forty password patterns that were identified for this year. You can download them here

Additionally, I put together one for every quarter. These can be found in the previous quarter blogs:

- Q1 – https://blog.netspi.com/cracking-stats-for-q1-2014/
- Q2 – https://blog.netspi.com/cracking-stats-for-q2-2014/

- Q3 – https://blog.netspi.com/cracking-stats-q3-2014/

For more information on how we built our GPU-enhanced password cracking box, check out our slides

For a general outline of our password cracking methodology check out this post