PEN TEST PARTNERS

Email us today:
info@pentestpartners.com

Papa - FAQ

PTP Advanced Password Auditor

What is Papa?
The PTP Advanced Password Auditor, Papa, is a password cracking and auditing service from PTP Labs.

How does it work?
Papa extracts all user's password hashes from the domain, and securely transmits them to our high-performance password cracking servers. Any hashes that represent weak passwords are cracked, and the results are sent back to the Papa client. The weak passwords are matched against your domain users, and you can identify users with weak passwords, and perform trend, and attack analysis.

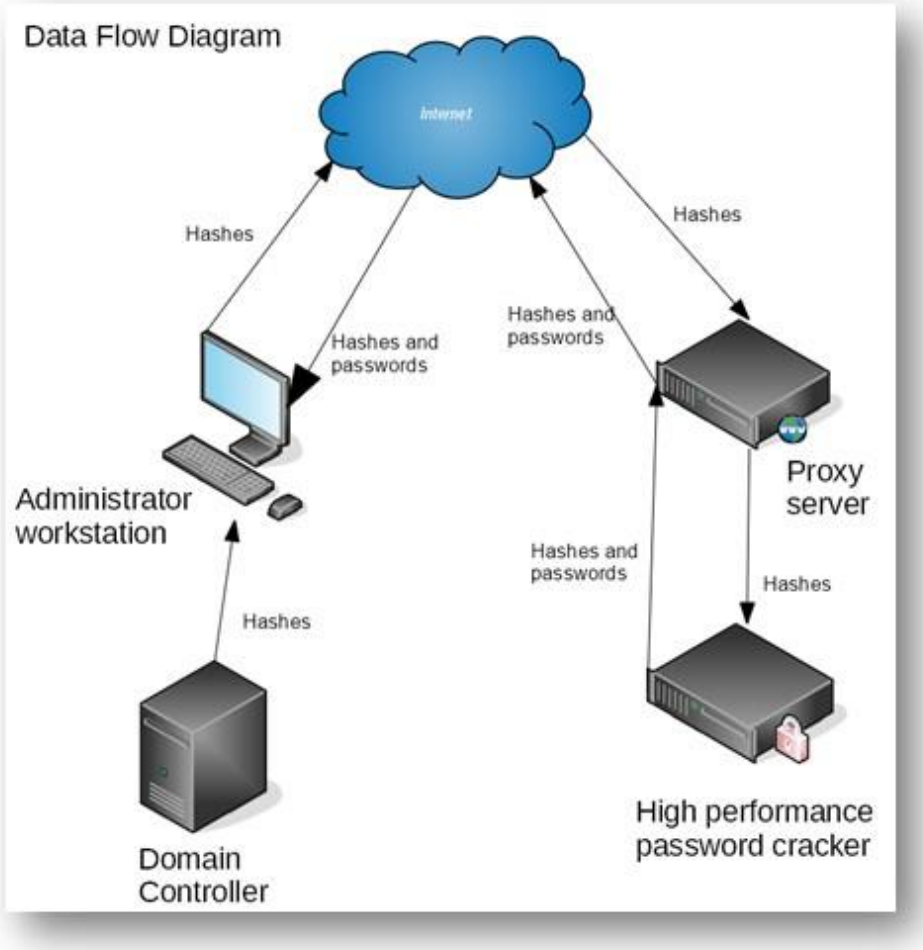
How secure is sending our hashes to you?
It's literally just the NTLM password hashes that are sent to our servers - we do not get the username, domain, or company information, and only weak passwords that we've cracked are sent encrypted back across the Internet to the client. The cracked hashes are mixed with the 100's of thousands of hashes that we already have and are sorted. We have no way of identifying which hashes are yours, and in the event of a compromise, neither does an attacker. We've even been careful not to store IP connection information in our logs. If the hash is not cracked, it's not stored on our servers, because it's of no use to us. The hashes corresponding to weak passwords are the accounts that you'd want to change the passwords on anyway. So, if your domain admin accounts are not cracked, we don't keep the hashes or passwords, and even if we did, we wouldn't know which of the thousands of passwords belonged to your domain or matching user account.

Who has access to the hashes?
Our IT support staff and development team have access to the cache of cracked hashes. No one knows which hashes belong to which customer, or even if they are used on customer domains at all. Many passwords were generated from common dictionaries.

Is it possible to use Papa with an air-gapped system?
Yes, you can simply have a Papa install on the domain, and copy the database files in the Documents/PTP-Labs/Papa folder to an Internet-connected PC with the client certificate installed. You can then copy the database files back, or perform the analysis on the Internet PC.

PEN TEST PARTNERS

Do you have a Data Flow Diagram?
Funny you should ask:



What connections are required from my network?
Papa needs to establish a connection to proxy.ptp-labs.com on port 443/TCP. We need a clean uninterrupted connection. If you use an SSL proxy of some kind, Papa won't connect. We don't want the hashes being intercepted by anyone.

Does Papa run in a browser?
There is no browser. It's a thick client tool written in C#.

What is downloaded from PTP?
The only data back from PTP is hashes and corresponding cracked passwords.

PEN TEST PARTNERS

How are the hashes stored and transmitted from my Papa client?
The hashes are stored in an AES encrypted database. The key for the database is generated from the password that you choose. That's why we insist on a long and complex password on first use. The hashes and cracked passwords are transmitted via AES with TLS 1.2 or 1.3. The Papa client checks our server certificate, and we check your client certificate before any data is transmitted. It's not possible to Man-in-the-Middle the connection on the network.

How are the hashes stored and transmitted within the PTP network?
The hashes are stored on an encrypted disk, and are transferred from the proxy server to a password cracking server via encrypted transport protocols. The file is backed up, again to encrypted storage via IT support. We don't intend to ever delete any of the cracked hashes, but if you'd like us to remove a particular hash, we'd be happy to. If we can crack the hash, then it's a weak password, and not something that you'd want to make use of, so you shouldn't really be using it anyway.

What happens when we submit a hash?
If you upload a hash and we've already cracked it, the hash you uploaded is not written to disk and it's all performed from memory.
If we've not cracked it, then it is written to an encrypted disk and send to a password cracker. It's merged with any other cracking tasks that are queued, and the file is simply a list of NTLM hashes. Nothing else. It runs on hardware all owned by PTP and no one outside of IT support and the development team have access to it. No backup is made of the individual hash submissions. Internally a random session ID is generated and returned to the Papa client. Papa then submits that session ID to check on the cracking status of the submitted hashes.

What happens if PTP gets hacked?
We thought about the possibility of compromise. The only data stored on PTP servers is a list of hashes and matching passwords. This has, currently, more than 600,000 NTLM hashes and matching passwords. This is from all customers currently using the Papa service, as well as, common words and obfuscations. This is then sorted alphabetically, so there is no way of knowing what hash belongs to what customer, or even if it's a password that's actually in use anywhere. The list would be interesting, but useless to an attacker. Even if they had all the passwords, they would need to try 600,000 attempts on every user account before they were able to gain access. They would quickly hit your account lockout policy. It would be a pointless attack, and the password list is useless. In addition, any password we have, would be one that Papa has highlighted as being weak. The idea is that the users will have changed that password to something more secure, and we wouldn't store the hash of that new strong password that we've not been able to crack.

Can we request new features for Papa?
Of course. We're always happy to add new features that our customers might find useful. We'll always try our best to implement them for you, or give you a good reason why it might not be possible.