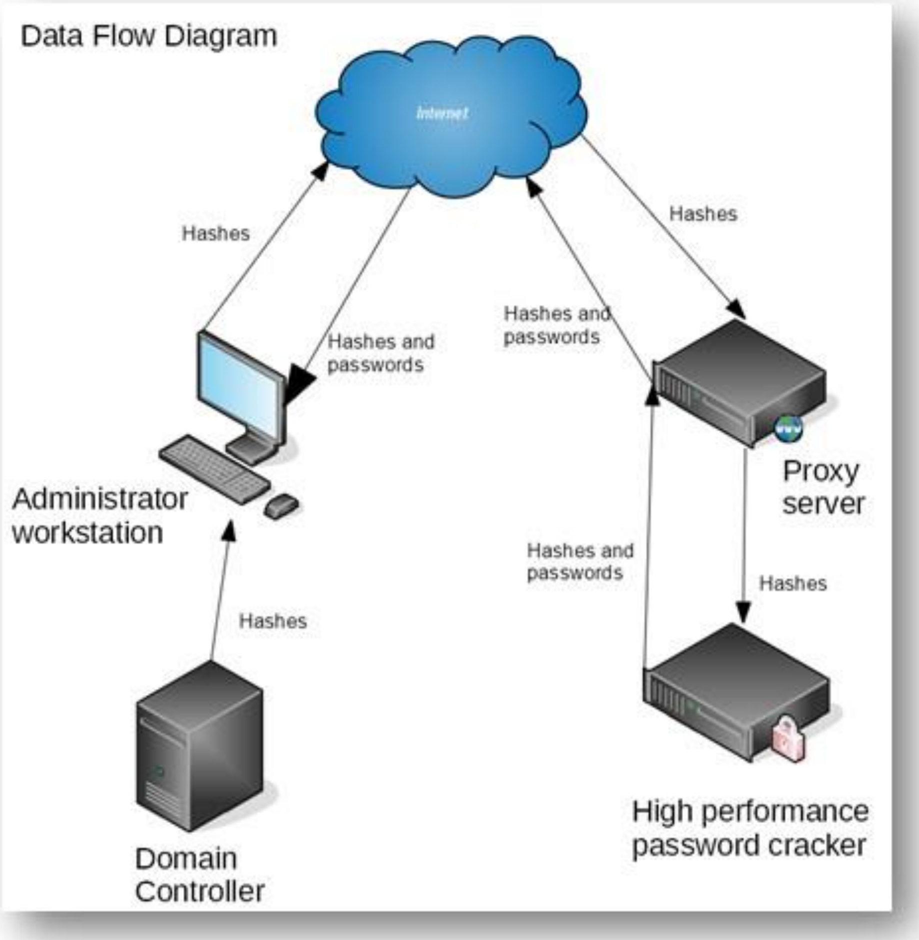
Email us today:
info@pentestpartners.com

Papa – Security Model

PTP Advanced Password Auditor

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

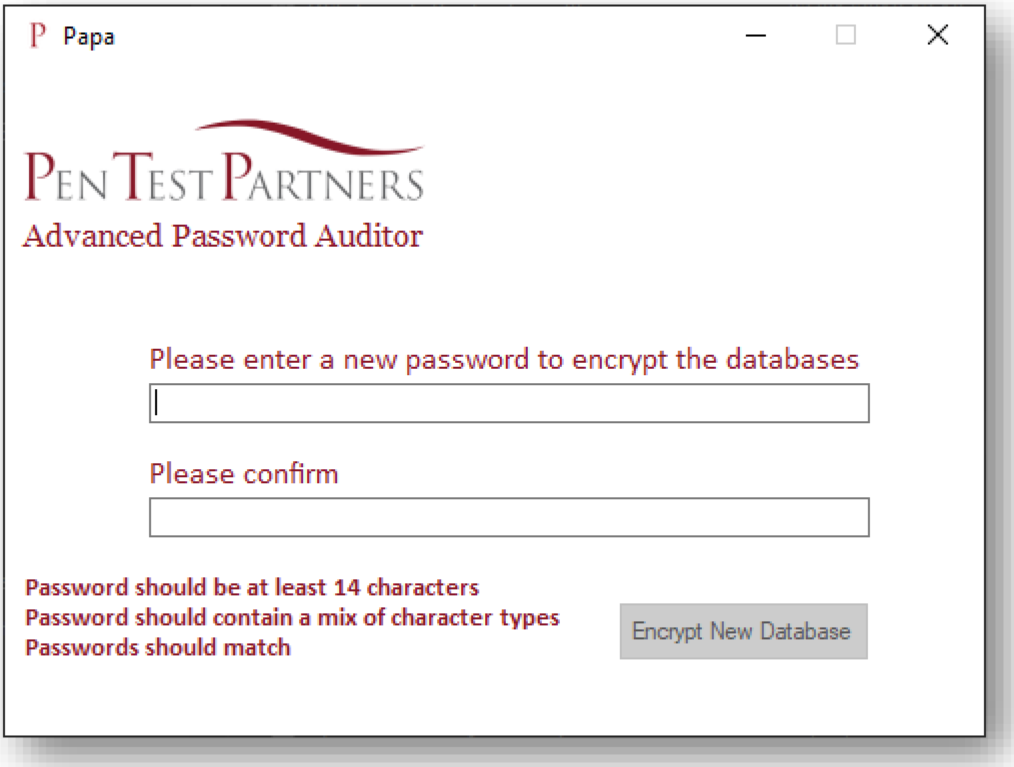
Data Flow Diagram



The following security controls are in place at each layer of the data flow:

Administrator Workstation

The Papa client uses a separate authentication model before access to the main view is permitted. The password is subject to a strong password policy and is used to generate an AES key with which the local database is encrypted. All locally-sored hashes are stored in this encrypted database and never written to disk in cleartext.



Please enter a new password to encrypt the databases

Please confirm

Password should be at least 14 characters
Password should contain a mix of character types
Passwords should match

Internet Transfer

The hashes are transmitted to the PTP Proxy server using AES cyphers with TLS version 1.2. Other cyphers and protocols are not supported or enabled on the PTP servers. The Papa client checks the server certificate, and the server checks the client certificate before any data is transmitted. It's not possible to Man-in-the-Middle the connection on either network or on the internet. Data is returned via client-initiated API calls and is encrypted to the same standard.

Hash Transfer within the PTP Network

The hashes are transferred from the proxy server to a password cracking server via a locked-down SSH protocol. The hashes are 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 ideally, it would not be in use.

Hash Storage

The hashes are stored on an encrypted disk and the entire database is sorted by NTLM hash to randomise the most recent cracked hashes. We do not store any hashes that we cannot crack, so the passwords that are marked as secure, or uncracked, are not stored anywhere on PTP infrastructure.

PTP Servers

As you would expect, the PTP servers are not cloud-hosted. They are physical devices that we own and manage. They are under change control, regularly patched, and penetration tested. We use full disk encryption, and use active monitoring.

Papa Source Code

Papa was designed and written by a penetration tester with security primarily in mind. It was subject to peer review, and source code audit.

Anonymity and Password Security

The PTP servers does not log the IP address of any host connecting to it, so even PTP does not know who's NTLM hashes are being cracked. The cracked hashes are mixed into a huge database containing real and generated passwords. In the event of a compromise, an attacker would not know which customer each password belonged to or whether they are still in use, changed, or even a valid password at all.

Client-Side Extra Protections

If you do not want a particular hash to be sent to PTP, the user and hash can be simply removed from the database before being sent for cracking. In addition, banned password lists can be added to the Papa client and these would be flagged as cracked. This would prevent a corresponding hash being sent to PTP servers.