Mimikatz

Volodymyr Lisivka edited this page on Oct 12, 2013 · 3 revisions

Mimikatz is shell for various modules. Here is simple example how to export RDP and/or HyperV certificates with private keys for debugging of RDP session in Wireshark.

Run mimikatz alpha x64, then execute following commands:

```
mimikatz #
# Enable "debug" privilege to be able to patch CNG service
privilege::debug
# Patch CNG service, lasts until next reboot
crypto::cng
# Patch CAPI library in memory of this process
crypto::capi

# Export Remote Desktop certificate(s) without private keys, password is
"mimikatz"
crypto::certificates  -systemstore:CERT_SYSTEM_STORE_LOCAL_MACHINE -store:"Remote
Desktop" /export

# Export HyperV certificate(s) without private keys, password is "mimikatz"
crypto::certificates  -systemstore:CERT_SYSTEM_STORE_SERVICES -store:vmms\My
-export

# Export Remote Desktop certificate(s) with private keys, password is "mimikatz"
crypto::certificates  -systemstore:CERT_SYSTEM_STORE_LOCAL_MACHINE -store:"Remote
Desktop" /export

# Export HyperV certificate(s), password is "mimikatz"
crypto::certificates  -systemstore:CERT_SYSTEM_STORE_SERVICES -store:vmms\My
-export
```

Extract private key from .pfx files (pfx2pem):

```
#!/bin/bash
for I in "$@"
do
  openssl pkcs12 -in "$I" -nocerts -nodes -password pass:mimikatz -out "$I.pem"
|| echo "ERROR: A problem with certificate \"$I\": openssl returned non-zero exit
code: $?." >&2
done
```

Pages 48

Find a Page...

Home
BugReporting
Build on Windows Visual C 2012 (32 and 64 bit)
Build on Windows with Visual C 2010
Build Options
Certificate Export
Changelog
clang scan build
Coding Guidelines
CommandLineInterface
Compilation
Debug System
Doxygen
Eclipse
FAQ

Show 33 more pages...

Clone this wiki locally

https://github.com/FreeRI