woanware

APPLICATION SECURITY

ASP.Net Backdoors
filefolderenum
nnikto
SqlInjector
SqlServerDataExtractor
verbcheck
ViewStateHacker

FORENSICS

C4PReporter
ChromeForensics
EseDbViewer
FireFoxForensics
firefoxsessionstoreextractor
ForensicUserInfo
ForensicVideoTriage
FreeDownloadManagerForensics
gmailparser
JumpLister
lnkanalyser
OperaForensics
PrefetchForensics
RegExtract
USBDeviceForensics

NETWORK SECURITY

Arpey
bannergrab
bigfinger
ciscoioshttp
enumdotnet
ftpcheck
NetworkScanViewer
OracleEnumerator
ServiceEnum
smtpcheck
sslciphercheck

Info

After the previous post regarding Windows user passwords, I have now after quite a lot of work created ForensicUserInfo, which is a GUI tool that allows you to import registry files (requires the SAM, SOFTWARE and SYSTEM hives) and then extracts the user information from the various files and then decrypts the LM/NT hashes from the SAM file.The application can export the information to either CSV or HTML.

There is now a console version that generates text output.
This would not have been possible without the posting at the Push the Red Button blog regarding the SYSKEY and the SAM file. The process used to encrypt/obfuscate the password hashes is a joke, in that it is over the top, since once you have the files (SAM and SYSTEM) then you can get the hashes.

ForensicUserInfo will extract the following information:

- RID
- Login Name
- Name
- Description
- User Comment
- LM Hash
- NT Hash
- Last Login Date
- Password Reset Date
- Account Expiry Date
- Login Fail Date
- Login Count
- Failed Logins
- Profile Path
- Groups

Download

v1.0.1 Console
v.1.0.4 GUI

windemac
WinPentest
winserviceenum
winsnmp

UTILITIES

csv2html
Cvss2Calc
Encoder
hexlogparser
NetCalc

Set your Twitter account name in your settings to use the TwitterBar Section.

woanware

About RegExtract WinPentest SqlInjector ForensicUserInfo USBDeviceForensics Arpey ASP.Net Backdoors bannergrab bigfinger C4PReporter ChromeForensics ciscoioshttp csv2html Encoder enumdotnet EseDbViewer FireFoxForensics firefoxsessionstoreextractor ForensicVideoTriage FreeDownloadManagerForensics ftpcheck gmailparser hexlogparser lnkanalyser filefolderenum NetworkScanViewer NetCalc nnikto OperaForensics OracleEnumerator PrefetchForensics smtpcheck SqlServerDataExtractor sslciphercheck verbcheck ViewStateHacker windemac winsnmp winserviceenum JumpLister Cvss2Calc ServiceEnum

© 2011 woanware