Programy k lámání hesel pro Apple

Vložil/a el tenedor del ... [1], 10 Prosinec, 2006 - 22:43

- Apple [2]
- Cracking [3]
- Mac OS [4]

O trojských koních pro počítače Apple jsme se již jednou poučili. Dnes si uděláme malý průřez, obrázky i slovem, několika programy spojenými s louskáním hesel, tedy programy velmi atraktivními, jak nám může ukázat klasická apoteóza lamy s Widlemi v ruce jedné a Brutusem nebo wwwhackem v ruce druhé. Uživatelé jablek se vůbec nemusí bát, že by neměli k dispozici podobné nástroje, jaké můžeme najít na Windows.

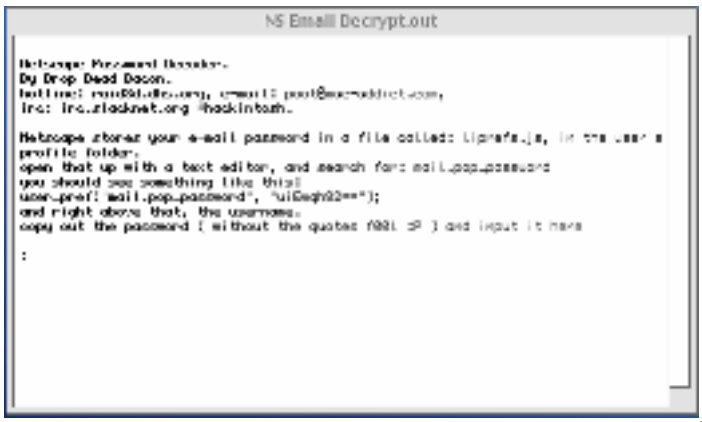
Rozdělme si programy podle dvou kriterií: jednak podle operačního systému - buď pro starý klasický MacOS, nebo moderní, na UNiXu (Darwin) založený OS X (některé programy využívající CarbonLib mohou běžet nativně na obou systémech), druhak podle toho, zda jde o programy pracující vzdáleně nebo off-line.

CLASSIC
Tak nejprve začneme programy pro klasický systém, to novější si necháme na později. A vezmeme si to hezky od největších kravin až po to nejzajímavější.

Classic - off-line:
Program, který se zcela vymyká louskání počítačových hesel je MasterLockSmith. Slouží k otevírání opravdových kódových zámků MasterLock (s kterými se ale u nás asi nesetkáte). Sám program obsahuje nápovědu, jak mechanickým trikem na různých verzích zámku najít jedno z čísel kódu, pak počítá kombinace těch ostatních, autor programu tvrdí, že vám umožní otevřít zámek do pěti minut. Neobvyklé, ale pěkné.
Dále jsem našel skupinu prográmků pro louskání hesla, lokálně uloženého, k nějakému programu, datovému souboru nebo dokonce systému.
Tady jsou:

OS9 Password Deleter - vyžaduje fyzický přístup k počítači, na kterém ho musíte spustit. Jde o instalátor, který do adresáře s nastaveními uloží soubor určující, že jsou použita prázdná hesla. Naštěstí nechává původní soubor, jen ho přejmenuje, takže pokud víte, že byl útok použit, můžete původní hesla, uživatelské účty a skupiny obnovit. Nemám ale vyzkoušeno, jestli program funguje i na systémech starších, než 9. V novějším OS X už pouhý fyzický přístup k počítači k přepisování souborů s účty a hesly nestačí.

Netscape e-mail decrypt - starší verze Netscape ukládaly mailová hesla do souboru liprefs.js, ve formě user_pref("mail.pop_password", "uiEwqh82=="); k rozkódování hesla slouží právě tento prográmek.



[5]

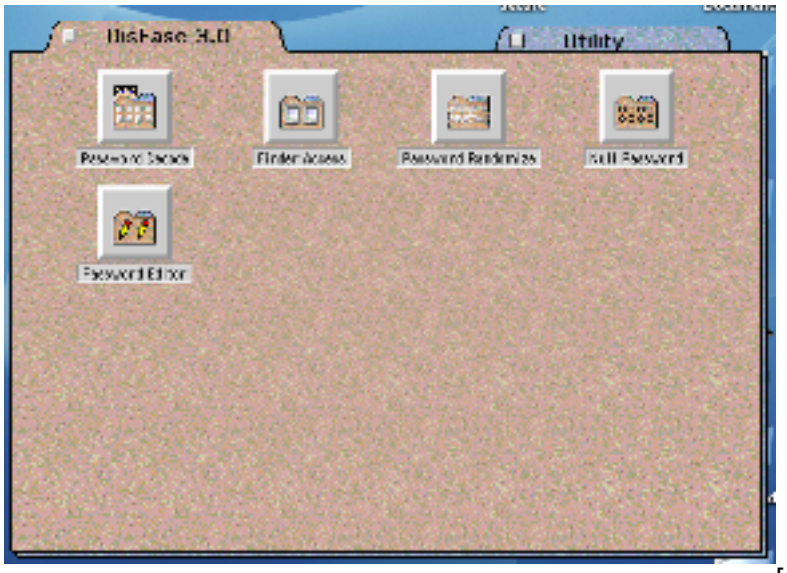
BigSecret Password Nabber - BigSecret je sharewarová aplikace, sloužící k utajování důvěrných souborů a složek, používá k tomu nastavování atributu Invisible. Aplikaci je možné chránit heslem, aby si jen tak někdo nemohl všechny vaše neviditelné soubory procházet. Heslo ale příliš dobře nechrání, pomocí tohoto prográmku ho vytáhnete. Jediná potíž, se kterou se můžete setkat, je skutečnost, že program může, pokud si uživatel změnil heslo za kratší, ukazovat za aktuálním heslem ještě zbývající znaky hesla původního. Pokud tohle ale víte, nebude už před vámi mít BigSecret už žádné tajemství.

[6]

AfterDark Reader - AfterDark je velmi oblíbená kolekce screensaverů, ketré lze nechat chránit heslem, takže náhodný návštěvník vašeho opuštěného počítače se v něm nemůže hrabat. Přesněji řečeno, screensaver jde sice obejít (boot z jiného media), ale heslo tím nezjistíte - to vám musí prásknout tato utilita.
Remove Excel Password - název hovoří za vše, takže asi tušíte, že tato utilitka vám zjistí heslo k datovým souborům k microsoftímu Excelu. Výborná věc, pokud pomineme, že jde o Excel verze 2, který se už delší dobu nepoužívá a proprietární formát .xls souborů i způsob uložení hesla se za ty roky změnil.

[7]

DisEase 3.0 - tato utilita je perfektně zpracovaným manažerem hesel k velmi oblíbenému organizačnímu programu AtEase, svojí grafikou dokonce napodobuje vzhled originálního AtEase. A umí toho na tak malou utilitku docela dost. Zajímavou featurou je volba Nullify, která heslo vyplní znaky s kódem nula, takže nelze zadat z klávesnice.

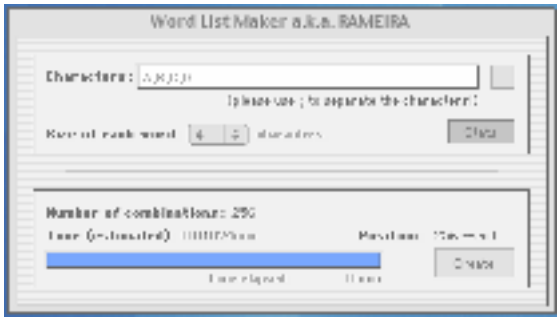


[8]

Password killer - kromě stolních Macintoshů se používaly i přenosné notebooku - PowerBooky. Přenosný počítač je pochopitelně v riziku, že ho někdo šlohne a dostane se k důvěrným datům. Je proto jasné, že výrobce umožnil chránit ho "biosovým" heslem, které je nutné zadat ještě dříve, než se zavede systém. Password killer je ovládací panel,který toto heslo vynuluje. Autor chtěl původně analyzovat rutiny v ROM, což se mu nepodařilo, tak jednoduše upravil ovládací panel "Password protection" tak, aby pro smazání nebo změnu hesla nevyžadoval znalost hesla starého, takže program funguje na všech modelech, ale bude vám k ničemu, pokud nemáte přístup na disk a ke spouštění programů.

Pokud chcete louskat hesla, potřebujete slovník. Buď ho můžete generovat klasickým bruteforcerem, který zkouší všemožné kombinace znaků, a pak bude obsahovat spoustu nesmyslných skupin znaků bez významu, nebo sebrat někde nějaký wordlist se smysluplnými slovy.

Rameira - wordlist generátor, kterému zadáte, jaké znaky chcete použít, a kolikaznaková mají být hesla, která se z nich budou generovat, program vám rovnou prozradí, kolik jich bude. Na mně utilitka zapůsobila dost rozpačitě - spousta bruteforcerů obsahuje nějaký wordlist lab,který i v té nejjednodušší podobě nabízí aspoň takové možnosti, jako tato rádoby specializovaná utilita. Navíc je problém s ovládáním, které napoprvé nepochopíte - tlačítko stats spočítá počet hesel, a povolí spuštění generování wordlistu, ale taky ho pak zakazuje.

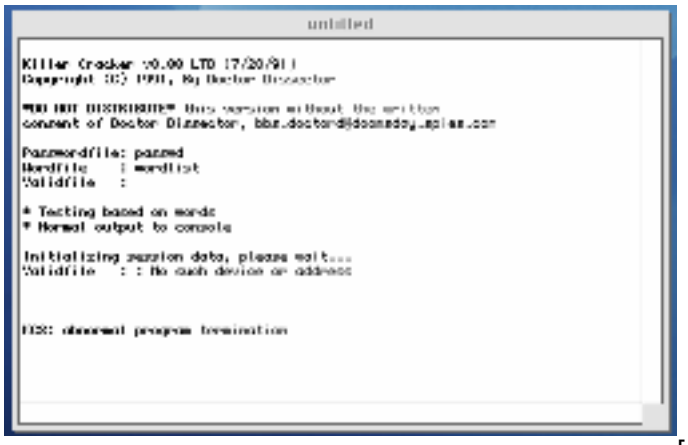


[9]

PassGuess - autor programu Password Guesser tvrdí, že narozdíl od jiných programů, které louskají například UNiXová hesla nebo hesla do Windows, jeho program hádá hesla pro libovolnou platformu. Trochu velkohubé. A co se pod tím skrývá?

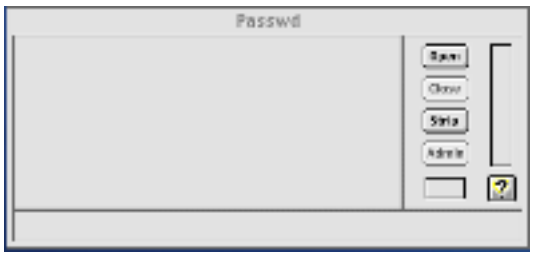
Je to spíše filtr wordlistů. Pomůže vám z nějakého existujícího wordlistu vytřídit pouze ta slova (potenciální hesla), která obsahují zadané znaky. Pokud jste zrovna ve fázi, kdy nechcete být script-kiddie a chcete si sami vytvořit nějaký jednoduchý program, zkuste si za domácí úkol napsat tohle. Raději bych ale tuhle možnost viděl jako přídavnou funkci v nějakém komplexnějším programu.
A teď už se dostáváme k dalším programovým produktům:

Killer Cracker - jde o port UNiXového programu pro wordlist útok na UNiXová hesla v souborech passwd, takže dnes už historická záležitost. Program byl psán v C pro příkazovou řádku, která v Classicu chybí, byl tedy trochu upraven pro macovské prostředí - obohacen o emulaci terminálu, a názvy souborů s hesly, wordlistem a soubor pro výstup se zadávají v dialogu a nikoliv v parametrech při spouštění. Nevím, jaké druhy kódování program zná - nikde se to neuvádí.



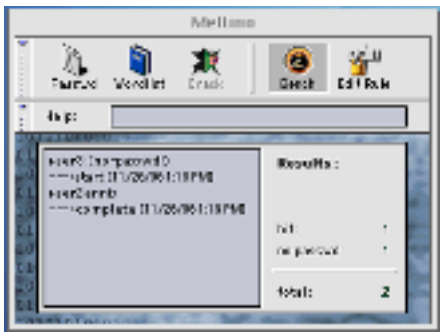
[10]

Pas - analyzuje UNiXové passwd soubory, v celkem ppříjemně navrženém GUI. Dnes už ale taky spíše historická záležitost.



[11]

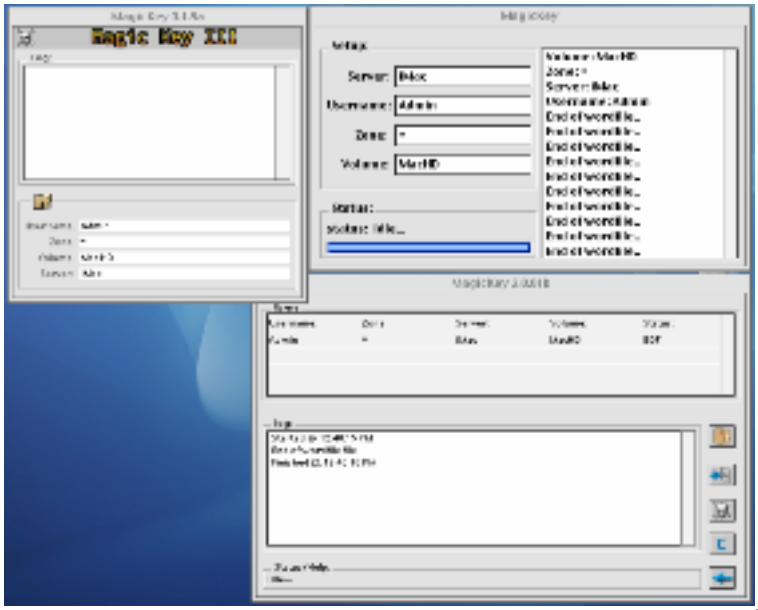
Meltino - perfektně provedený japonský program, opět pro louskání hesel z UNiXových passwd souborů. Zvládá hesla kódovaná pomocí DES nebo MD5 hashe. Dokonce si můžete před útokem naostro nechat odhadnout výkon programu na vašem počítači pro oba typy útoku. Jeho jedinou, ale zato výraznou nevýhodou je malá rychlost.



[12]

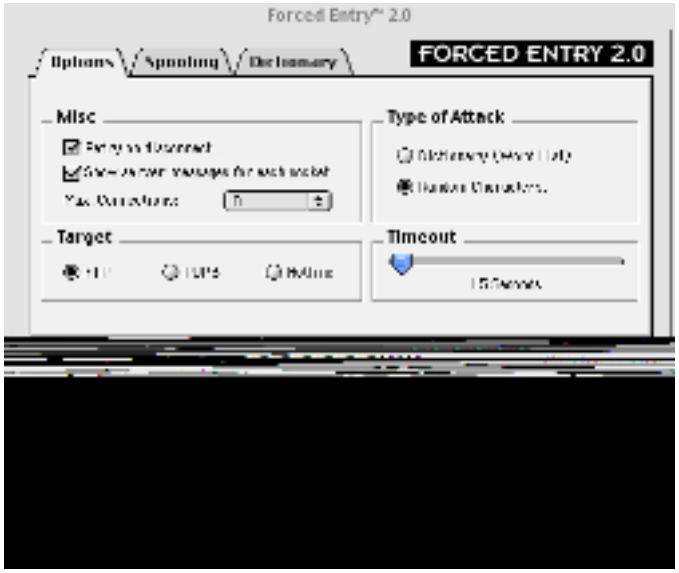
Classic - on-line:

MagicKey - zpočátku neměly počítače od Applu ethernet a do sítě se spojovaly pomocí sériové linky. Tato síť, která s příchodem ethernetu začala běhat i na něm, byla velmi důmyslně navržená. Tři verze programu MagicKey slouží k bruteforce útoku na uživatelské účty na sdílených discích. Prostě zadáte jméno uživatele (v druhé verzi programu jich můžete zadat až deset naráz), název počítače, název zóny (nebo hvězdičku), název disku, na který se chcete dostat, a pak už jen musíte mít ve stejném adresáři, kde se nachází program, i wordlist. Stisknete tlačítko a appletalkové účty se začnou louskat. Taková čistě applovská utilitka.



[13]

Forced Entry™ 2.0 - program sloužící k útoku na FTP, POP3 nebo Hotline účty. Slušně provedený program, který se po odpojení umí znovu připojit a umí se schovat za SOCKS proxy.

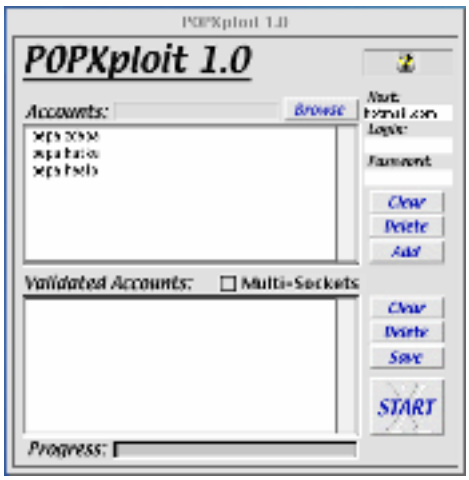


[14]

McAuthority - umožňuje útok na webové stránky. Ačkoliv autor tvrdí, že programuje hůř než opice a jen o něco líp než zelená améba, je opravdu výborný - můžete se schovat za proxy, nadefinovat si části hlavičky (X-forwarded, Via, User-Agent, ...), dokonce náhodně vybírané, které znesnadní vaši identifikaci, pochopitelně URL a wordlist.

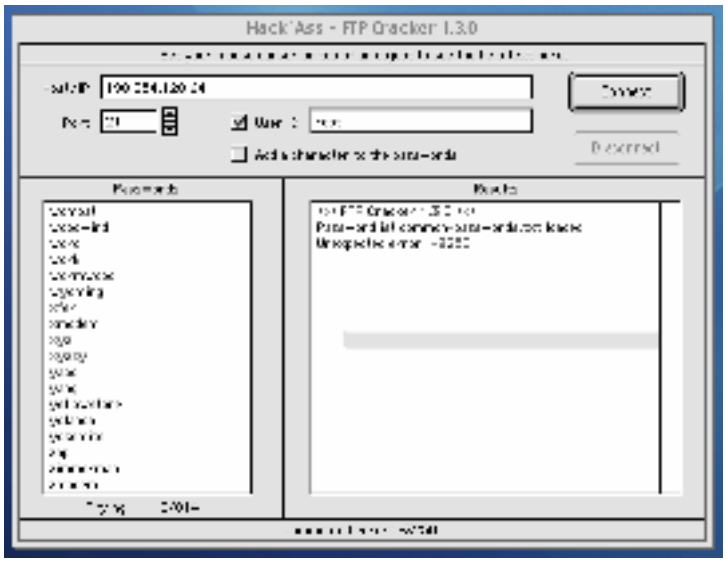
[15]

POPXploit - program, který bych označil za mizerný. Podniká útoky na e-mailové účty, jako vstup mu slouží dvojice názvu účtu a heslo - hesla jsou tak od začátku asociována s konkrétním účtem. Je tedy dobrý spíš na otestování toho, jestli se u některého z několika účtů nezměnilo heslo, než na útok nebo ověření síly hesla k účtu.



[16]

FTP Cracker - jednoúčelové FTP louskátko, kterému lze vytknout snad jen to, že se neumí schovat za proxy, takže Forced Entry nepřebije.



[17]

Mail Brute - jednoúčelové POP3 louskátko, u kterého se ale rovněž za proxy nechováte a tak Forced Entry i tentokrát vede.

[18]

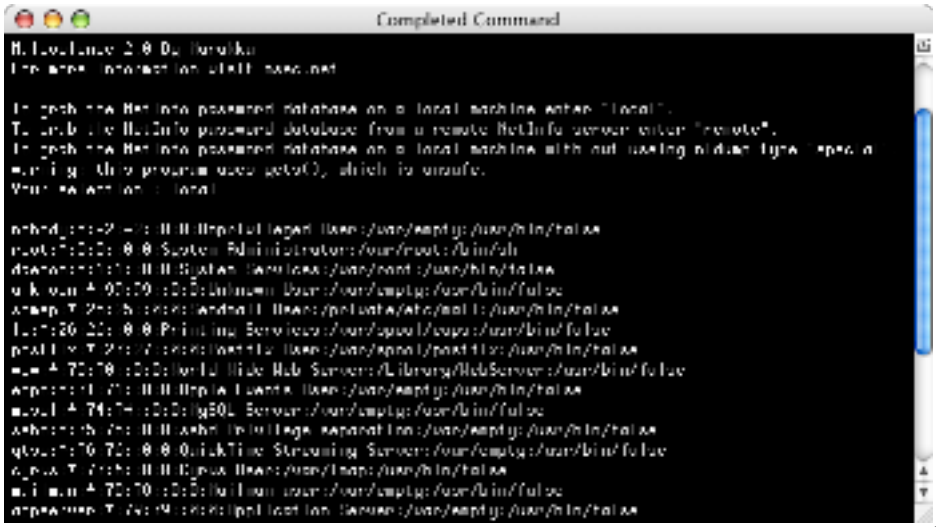
A tím máme starší systém odbytý a podíváme se, jak se změnily programy tohoto typu s příchodem

nového systému.

OS X
Díky tomu, že v srdci OS X bije UNiXové jádro, mnohem snáze se na něm, vedle programů psaných pro jeho Applovské API, zprovozňuje software z jiných UNiXů, případně Linuxu. Chci se věnovat popisu programů specifických pro Apple, ale jednoho typicky UNiXového programu se stejně dotknu:

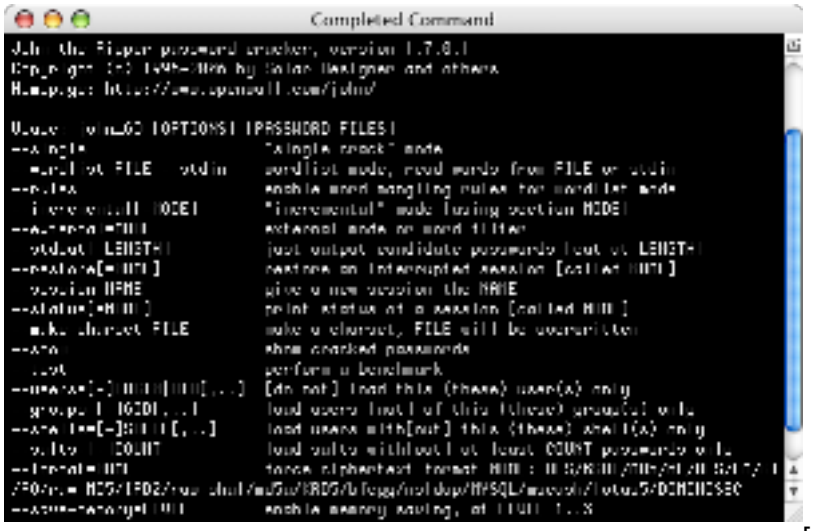
OS X off-line:

Malevolence - umožňuje získat soubor se seznamem uživatelských účtů, i když pro přístup k němu nemáte práva. V první verzi vytváří dokonce html stránku, kterou si můžete prohlédnout v browseru a použít tak Malevolence i k útoku na vzdálený OS X server. Program byl dokonce oceněn jako "exploit of the millenium". Pravděpodobně využívá chybu v getpwent(), ale kód nebyl uvolněn ani nikde publikován. OS X ale, jako většina moderních systémů, v etc/passwd neobsahuje hesla ani jejich hashe, narozdíl od Linuxu ale neobsahuje ani etc/shadow a hesla jsou ukryta v netinfo databázi. Z etc/passwd se ale stále můžete dozvědět jména uživatelů a další informace.



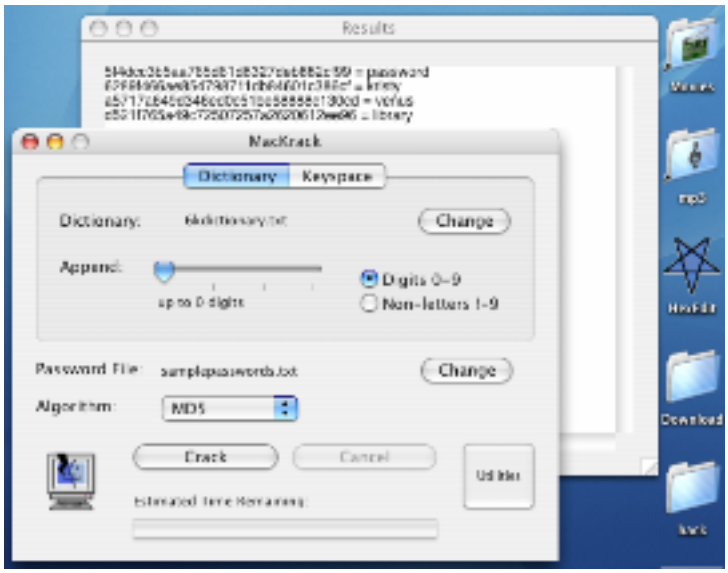
[19]

John the ripper - UNiXový program pro louskání UNiXových hesel. Ve verzi 1.7 zvládá DES, BSDI-DES, LM-DES, MD-4, MD-5, SHA-1, Blowfish a další. Verze 1.6 je ještě prostým portem programového kódu na OS X. Port verze 1.7 pak kromě jiných vylepšení přináší novinku - kód programu je k dispozici ve dvou verzích, jedna je univerzální pro všechny PPC procesory, druhá pak využívá k výpočtům vektorovou jednotku AltiVec, kterou obsahují procesory G4 a G5, což vede k mnohonásobnému urychlení běhu (asi dvacetkrát). Ovládá se normálně z příkazového řádku. I když už možná někdo pracuje na nějakém GUI, myslím si, že u tohohle kousku není ani potřeba. Pro šťouraly jsou dostupné zdrojové texty.



[20]

macKrack - program louská UNiXová hesla krytá pomocí MD-5, SHA-1, Crypt a pak hesla k .dmg souborům s image disku (.dmg je formát typický pro použití v OS X, dřívější systémy používaly .smi - self mounting image). Program umí i spočítat MD-5 a SHA-1 hashe heslům, která mu zadáte, a encodovat base64 encodovaná hesla. Pěkná featurka je, že ke slovům ve wordlistu umí vytvářet permutace (přeskupením písmen) a zvyšuje tak mnohonásobně počet zkoušených kombinací, dále k heslům ve wordlistu přidávat číselné nebo i jiné kombinace nastavených délek (což umožní objevit i hashe hesel typu "Karolina123"). Umí vytáhnout heslo k formwaru a číst hesla z passwd souboru, ale ani jedno z toho na mém počítači neproběhlo úspěšně. I přesto je to pěkný, povedený a užitečný program.



[21]

MHW 1.1 - Macintosh hackers workshop. Vlastně bych ho neměl řadit striktně k programům pro OS X, protože využívá CarbonLib a měl by tedy běžet i na OS 9, navíc je spolu s ním v archivu i starší verze, která chodí i na systémech ještě starších. Zdrojáky jsou přiloženy. Samostatně jsou přibaleny prográmky pro příkazovou řádku OS X pro konverzi wordlistů z Maca do UNiXu a obráceně (jde o konce řádků), nastavování parametrů souboru (atributy, tvůrce, datum, typ souboru) a program, který dělá v podstatě to samé co Malevolence (a možná i stejným způsobem), ty ale ve starších systémech nejde použít. Teď ale k vlastnímu programu. Můžete použít wordlist nebo bruteforce. Obsahuje jeden z nejlepších generátorů wordlistů, s jakým jsem se setkal, funguje do osmimístných hesel. Umí číst gecos a získaná slova zahrnout do wordlistu (kdyby někdo jako heslo použil své příjmení, ulici nebo tak). Filrtr pro odstraňování duplicit z wordlistu - tak to se opravdu nikde jinde

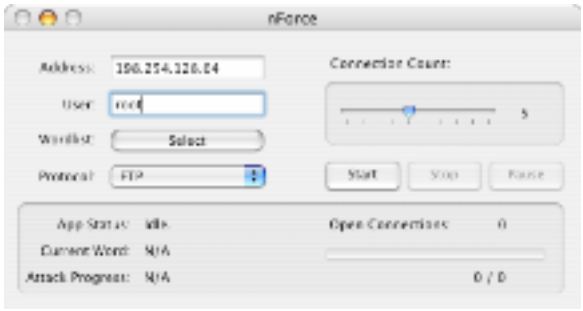
nevidí. Dokumentace bohužel neuvádí, jaká kódování podporuje, vyrozuměl jsem jen, že MD-5 asi nepodporuje.

OS X on-line:

AFPBrute - Zkratka AFP označuje AppleTalk filling protocol, slouží k přenosu protokolu AppleTalk po TCP/IP. Podobně jako MagicKey, i AFPBrute slouží k útoku na disky sdílené v tomto protokolu. Zadáte prostě jen IP adresu, jméno účtu (jména uživatelů se vám může podařit získat při pokusu o přihlášení) a wordlist. Jediným nedostatkem, na který jsem narazil, je vyskakující okno s hlášením o neúspěšném přihlášení, se kterým se někdy potkáte. To použití programu znemožňuje (při vyzkoušení tisíce hesel by na vás vybaflo tisíc oken). Nezjistil jsem ještě, na čem je vyskakování okna závislé, jestli na verzi atakovaného serveru, nebo jestli se mi do systému dostalo při některém z updatů. Rozhodně vím, že jsem dříve program používal a okno mi nevyskakovalo.

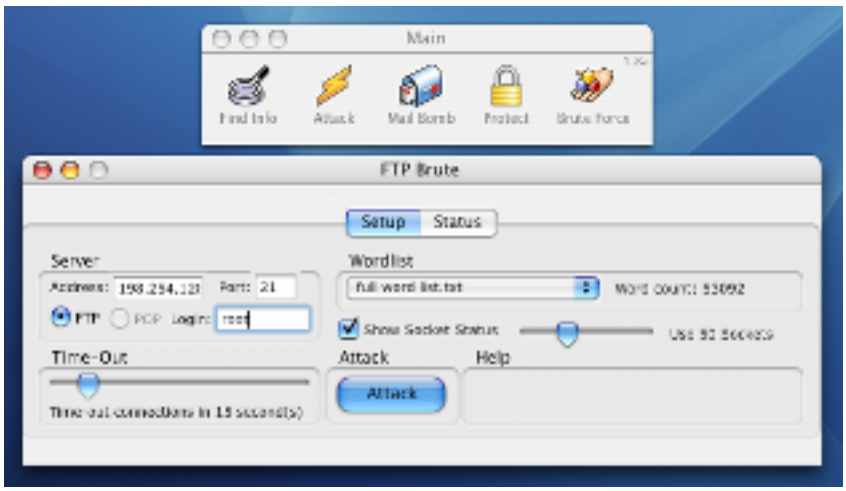
[7]

nForce - přívětivé, ale jednoduché louskátko FTP a POP3 účtů, bez podpory proxy, vyniká ale rychlostí, kterou využijete hlavně při nastavení vyššího počtu připojení.



[22]

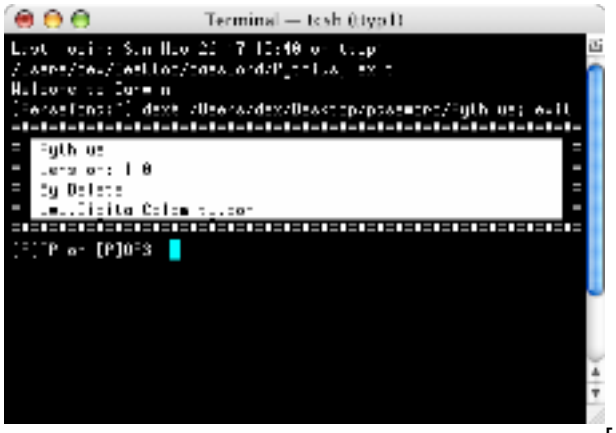
Cyanide - to je jedna z těch utilitek, kterým by se dalo říkat "hackerský švýcarský nožík". Obsahuje v jediné aplikaci všechno možné - portscanner, ping, lookup, traceroute, whois s volbou několika databází, port flooder, mass connect, mail bomber s anonymizérem, jednoduchý hlídač zvolených portů a pochopitelně bruteforcer FTP a POP3, srovnatelný zhruba s nForce (rychlost jsem netestoval). Celkem pěkný kousek. Pokud chcete, můžete si vybrat, jestli budete chtít používat jeden Cyanide, nebo několik specializovaných aplikací. Je to na vás.



[23]

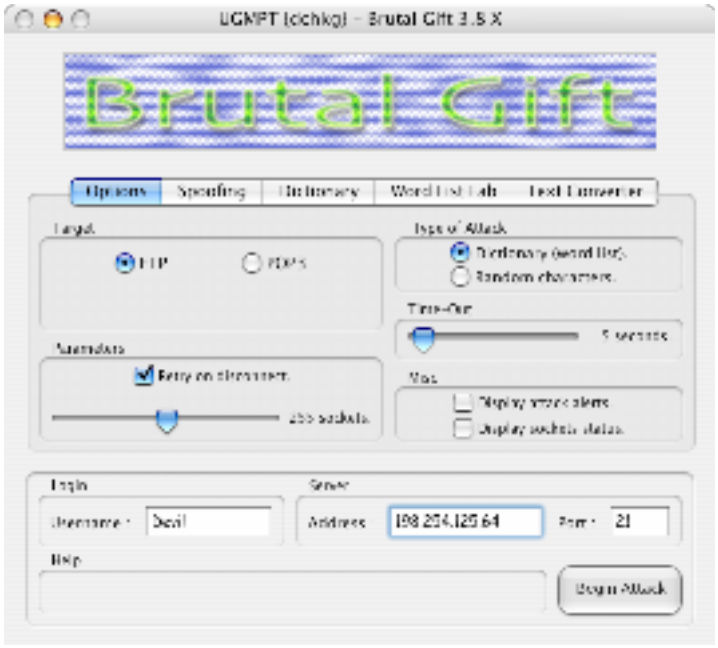
Noxious - čtenáři fóra Security-portalu se s tímhle programem, přesněji jeho zdrojákem, už setkali. Jde opět o bruteforce na FTP a POP3, program z dílny skupiny Nexus9 se spouští a ovládá z příkazového řádku v terminálu.

Pythius - další bruteforce na FTP a POP3, tentokrát od Digital Calamity, spouštěný v příkazové řádce terminálu, zdrojový kód ale nebyl uvolněn.

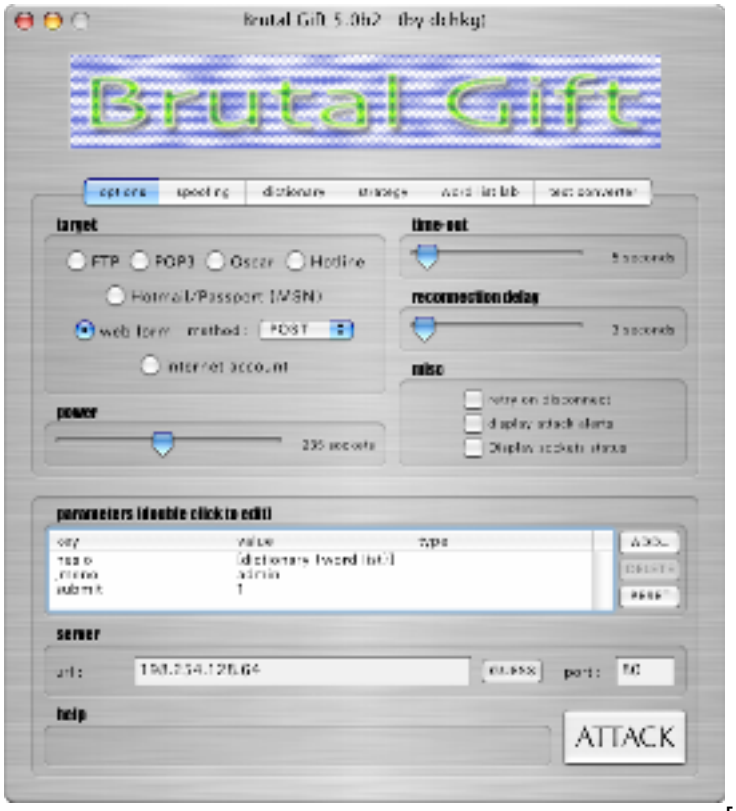


[24]

Brutal Gift - to nejlepší nakonec. Brutal Gift je postupně vyvíjený a neustále zdokonalovaný program, ve verzi 3.8 uměl sice jen FTP a POP3, zato s velkou podporou dobře udělaného wordlist labu ke generování wordlistů (v Advanced mode od verze 3.2 si dokonce můžete nadefinovat vlastní strukturu generovaných hesel), podporuje SOCKS proxy, obnovu spojení po odpojení, zvládá až 500 spojení, a vůbec. Jeho vývoj je ale rychlý, verze 5.0 už umí FTP, POP3, Oscar (AIM / ICQ2000), Hotline, Hotmail/MSN passport, internet account a webové formuláře (POST i GET, názvy jednotlivých parametrů si umí vyčíst sám). Další novinkou je definování strategie, Brutal Gift totiž může z odděleného seznamu brát i názvy účtů a v takovém případě může zkoušet buď postupně po jednom účtu různá hesla, nebo po hesla po jednom zkoušet na různé účty, nebo přiřadit podle pořadí jednomu účtu jedno heslo. Zajímavé je, že aplikace ProxyM8, která testuje, které protokoly přes sebe SOCKS proxy propustí, byla původně součástí Brutal Giftu.



[25]



[26]

Tento krátký článek kromě výčtu programů nepřináší příliš nového, a pro ty, kdo nepřijdou s jablečnými počítači do styku, není asi zajímavý vůbec ničím. Těm, kterým doma nebo ve škole či práci na stole nějaký ten Apple sedí, by ale mohl přinést aspoň základní orientaci v tom, jaké asi programy pro jejich stroj existují a ušetří jim hledání a tápání, kterému jsou jako příslušníci menšiny při shánění programového vybavení vystaveni.

A co nějaké shrnutí?
Pro bruteforce na FTP nebo POP3 na starých systémech použijete as Forced Entry.
Offline crackování UNiXových hesel asi použijete buď Meltino (vzhledem k tomu, že umí i MD-5), nebo starší verzi MHW.
Pokud byste náhodou byli v appletalkové síti, bude se vám (kromě jiných nástrojů - existuje například

program, který váš stroj v síti zneviditelní, takže vás případní hackeři nechají na pokoji) hodit MagicKey.
Mnohem spíš ale budete v dnešní době používat OS X.

Ti, co nemají rádi příkazovou řádku, mohou pro off-line útok na hesla používat MHW, případně macKrak, ale nejlepší bude nechuť překonat a přidat se k těm, kteří používají osvědčeného Johna.

AFP serverů je ve světě dost a tak se AFPbrute jako jediný program svého druhu taky šikne.
Pak záleží asi spíš na tom, na co jste zvyklí a co vám bude vyhovovat - jestli univerzální Cyanide, nebo nForce (případně zda se budete držet příkazové řádky a programů Noxious či Pythius), největší možnosti ale nabízí Brutal Gift a využijete ho určitě aspoň na přípravu wordlistů (pokud si neoblíbíte za tímto účelem MHW), podle mého Brutal Gift všechny ostatní programy své kategorie velmi dobře zastoupí.

A příště?
Příště bych rád vyjmenoval a popsal pár programů pro zabezpečení a šifrování. Snad to vyjde.

URL článku:
https://security-portal.cz/clanky/programy-k-l%C3%A1m%C3%A1n%C3%AD-hesel-pro-apple

Odkazy:
[1] https://security-portal.cz/users/el-tenedor-del-diablo
[2] https://security-portal.cz/category/tagy/apple
[3] https://security-portal.cz/category/tagy/cracking
[4] https://security-portal.cz/category/tagy/mac-os
[5] http://www.security-portal.cz/img/clanky/103/nsemaildecrypt.png
[6] http://www.security-portal.cz/img/clanky/103/bigsecretpasswordnabber.png
[7] http://www.security-portal.cz/img/clanky/103/afpbrute.png
[8] http://www.security-portal.cz/img/clanky/103/disease.png
[9] http://www.security-portal.cz/img/clanky/103/rameira.png
[10] http://www.security-portal.cz/img/clanky/103/killercracker.png
[11] http://www.security-portal.cz/img/clanky/103/pas.png
[12] http://www.security-portal.cz/img/clanky/103/meltino.png
[13] http://www.security-portal.cz/img/clanky/103/magickey.png
[14] http://www.security-portal.cz/img/clanky/103/forcedentry.png
[15] http://www.security-portal.cz/img/clanky/103/mcauth.png
[16] http://www.security-portal.cz/img/clanky/103/popxploit.png
[17] http://www.security-portal.cz/img/clanky/103/ftpcracker.png
[18] http://www.security-portal.cz/img/clanky/103/mailbrute.png
[19] http://www.security-portal.cz/img/clanky/103/malevolence.png
[20] http://www.security-portal.cz/img/clanky/103/john.png
[21] http://www.security-portal.cz/img/clanky/103/mackrak.png
[22] http://www.security-portal.cz/img/clanky/103/nforce.png
[23] http://www.security-portal.cz/img/clanky/103/cyanide.png
[24] http://www.security-portal.cz/img/clanky/103/pythius.png
[25] http://www.security-portal.cz/img/clanky/103/brutalgift38.png
[26] http://www.security-portal.cz/img/clanky/103/brutalgift50.png