HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Proactive Windows Security Explorer alata

CCERT-PUBDOC-2003-11-48

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Programi za ispitivanje sigurnosti zaporki vrlo su korisni alati za administratore sustava, tim više što iste te ili slične alate koriste i zlonamjerni korisnici u cilju probijanja zaštite sustava. Korištenjem tih alata administratori mogu na realan način sagledati jedan od ključnih sigurnosnih aspekata sustava.
Postoje mnogi alati namijenjeni raznim platformama, no zbog raširenosti Windows operacijskih sustava, najpopularniji su alati koji su namijenjeni upravo njima (npr. popularni L0phtcrack).
Korištenje alata za ispitivanje sigurnosti zaporki preporučljivo je za testiranje sigurnosti lokalnih korisničkih računa, no može imati i mnogo šire značenje. Tendencija Windows okruženja je integracija kroz *Active Directory* te korištenje istih autentikacijskih podataka za razne servise kao što su npr. WWW, POP3, IMAP, SMTP, *dial-in*, VPN itd. Vidljivo je da je većina ovih servisa dostupna i s Interneta, neovisno o tome štiti li se interna mreža vatrozidom. Zbog toga je sigurnost korisničkih računa mnogo osjetljivija nego što se to na prvi pogled čini, budući da potencijalni napadači mogu na raznim instancama pokušati razotkriti korisnička imena i zaporke.
Proactive Windows Security Explorer je alat za ispitivanje sigurnosti korisničkih zaporki namijenjen administratorima Windows NT/2000/XP/2003 sustava. Alat služi za identificiranje korisničkih računa s nesigurnim zaporkama, odnosno za podizanje razine sigurnosti na računalnoj i mrežnoj razini. Alat podržava nekoliko metoda dohvaćanja zaporki, a za ispitivanje sigurnosti može koristiti metode napada korištenjem sile (engl. *brute force*) ili korištenjem rječnika (engl. *dictionary attack*), te se može koristiti za napade na LM ili NTLM autentikacijske sheme.
Proactive Windows Security Explorer je trenutno u fazi beta testiranja, a važeća inačica u trenutku testiranja bila je 1.0 beta 2, koja je besplatna uz uvjete navedene u licenci distribuiranoj zajedno s paketom.

2. Metode napada na zaporke

Postoji nekoliko metoda napada na zaporke. Neke od njih su specifične obzirom na način pohrane i/ili generiranje zaporki kod određenih autentikacijskih shema, dok su druge metode univerzalne i mogu se primijeniti na sve sustave autentikacije. Najpopularnije metode napada na zaporke su:

- napad primjenom sile i
- napad korištenjem rječnika.

Napad primjenom sile predstavlja najprimitivniju metodu napada na sustave. Kod ovog napada za svaku moguću kombinacija slova, brojki i/ili specijalnih znakova, ovisno o autentikacijskoj shemi, provodi se šifriranje ili se računa *hash* vrijednost, te se tako dobiveni rezultat uspoređuje s originalnom šifriranom ili *hash* vrijednošću zaporke. Iako je provođenje ovih napada teoretski vrlo zahtjevno procesorski i vremenski, u praksi se pokazuje da se korištenjem ove metode mogu dobiti prilično dobri rezultati. Vrlo često korisnici odabiru kratke zaporke koje se sastoje uglavnom od slova i koje se na računalima veće procesorske moći vrlo lako mogu probiti u razumnom vremenskom periodu. Osim toga iskusni napadači mogu te napade prilagođavati; uključivati ili isključivati pojedine znakove ili skupove znakova ili definirati proizvoljne maske, te na taj način suziti ukupni broj kombinacija, direktno na taj način utječući na brzinu i efikasnost napada.
Napad korištenjem rječnika predstavlja sličnu metodu napada, samo se za usporedbu ne koriste sve moguće kombinacije znakova, već samo riječi iz pojedinog rječnika. Najčešće se pri tom koristi engleski rječnik, no vrlo lako je za napad iskoristiti i bilo koji drugi rječnik. Nadalje, obično se osim normalnih riječi govornog područja u takve rječnike ubacuju i specifične kombinacije znakova (npr. *qwerty*, *asdf* i sl.), koje korisnici vrlo često upotrebljavaju za generiranje zaporki. Ovakvi napadi također daju vrlo dobre rezultate, jer su korisničke zaporke vrlo često poznata imena ili riječi.
Opisane metode napada mogu se vrlo efikasno i kombinirati, a jedina zaštita od takvih napada jest odabir dovoljno složenih i dovoljno dugačkih zaporki.

3. Windows autentikacijske sheme

Na Windows NT/2000/XP/2003 sustavima svakom korisničkom računu dodijeljena je zaporka. Korištenjem zaporke provodi se autentikacija korisnika, te se odobrava pristup računalnim i mrežnim resursima. Zaporka je niz znakova i može sadržati brojke, slova i specijalne znakove. Isto tako zaporka

može biti i prazan niz znakova. Poželjno je da zaporka bude složena i dovoljno dugačka da bi napadi primjenom sile ili korištenjem rječnika bili neizvedivi u razumnom vremenskom periodu.
Windows sustavi korisničke zaporke ne pohranjuju kao otvoreni tekst, odnosno u originalnom obliku, već pohranjuju njihove *hash* vrijednosti. Te *hash* vrijednosti su pohranjene u SAM (engl. *Security Accounts Manager*) bazi ili unutar *Active Direcory*-ja. Postoje dvije metode za generiranje *hash* vrijednosti:

- LM (*LAN Manager*) i
- NTLM (*Windows NT LM*).

Kod LM metode maksimalna duljina zaporke je 14 znakova, dok NTLM podržava duljinu zaporke do maksimalno 128 znakova. Ukoliko je zaporka kraća od 15 znakova Windows operacijski sustavi generiraju i pohranjuju obje *hash* vrijednosti.

3.1. LM

LAN Manager zaporka služi za autentikaciju korisnika na DOS, Windows 3.1, Windows 95, Windows 98, Windows ME i Macintosh sustavima.
Kako je ranije rečeno, LAN Manager zaporka može biti maksimalne duljine 14 znakova, a također nije osjetljiva na velika i mala slova (nije *case-sensitive*). Duljina pohranjene *hash* vrijednosti zaporke iznosi 16 okteta. LM *hash* vrijednost se računa tako da se sva slova originalne zaporke pretvore u velika (engl. *uppercase*), zatim se tako dobivena vrijednost dijeli u dva dijela od 7 znakova koji predstavljaju dva 56-bitna ključa za DES algoritam i kojima se šifrira konstantna 8-oktetna vrijednost. Dobivene 8-oktetne vrijednosti se spajaju u 16-oktetni zapis.
Nedostaci LM autentikacije su to što podržava samo OEM skup znakova, te što maksimalna složenost zaporke nije 14 znakova već *de facto* 7 znakova, što čini ovu metodu izuzetno osjetljivom na napade primjenom sile. Sigurnost zaporke uvelike ovisi o korištenju brojki i specijalnih znakova, a zbog načina računanja *hash* vrijednosti može se i dogoditi da zaporka od 7 znakova bude sigurnija od zaporki koje su dulje.
Korištenje LM autentikacije može se onemogućiti na NT/2000/XP/2003 sustavima, no u tom slučaju neće biti moguća komunikacija sa Win9x/ME i starijim sustavima. Ukoliko se radi o isključivo NT okruženju onemogućavanje LM autentikacije je preporučeno.

3.2. NTLM

NTLM služi za autentikaciju korisnika na Windows NT obitelji sustava (NT/2000/XP/2003). Maksimalna duljina zaporke je 128 znakova, a velika i mala slova se razlikuju (*case-sensitive*). 16-oktetna NTLM *hash* vrijednost računa se korištenjem MD4 jednosmjerne funkcije nad zaporkom u Unicode reprezentaciji.
Iako je ova metoda mnogo sigurnija nego LM i ona ima neke implementacijske nedostatke. Kao prvo, sva postojeća korisnička sučelja ograničavaju duljinu zaporke na 14 znakova, a isto tako transformacija ASCII zaporke u Unicode reprezentaciju unosi određene pravilnosti u ulaznoj vrijednosti, no u ovom trenutku nisu poznate kriptografske metode koje bi mogle iskoristiti ovu mogućnost.
Sigurnost zaporke, odnosno osjetljivost na napade primjenom sile je veća u odnosu na LM autentikacijsku shemu, no slabe zaporke su i dalje ranjive na tu vrstu napada.

4. Instalacija

Instalacija Proactive Windows Security Explorer-a je jednostavna i intuitivna. Paket je moguće skinuti u obliku `.zip` datoteke s Web stranica proizvođača (http://www.elcomsoft.com/pwsex.html). Komprimiranu datoteku potrebno je raspakirati te pokrenuti `Setup.exe`. Nakon toga *Installer* vodi korisnika kroz korake instalacije u kojima je moguće podesiti ciljni direktorij, te *backup* opciju starih datoteka, što može biti korisno prilikom mogućih nadgradnji paketa.

5. Korištenje

5.1. Upravljanje

Paket je još u beta inačici, pa je njegovo korištenje dozvoljeno samo za ispitivanje, uz uvjete navedene u licenci za korištenje. Sama aplikacija posjeduje standardno Windows GUI sučelje (Slika 1) podijeljeno na:

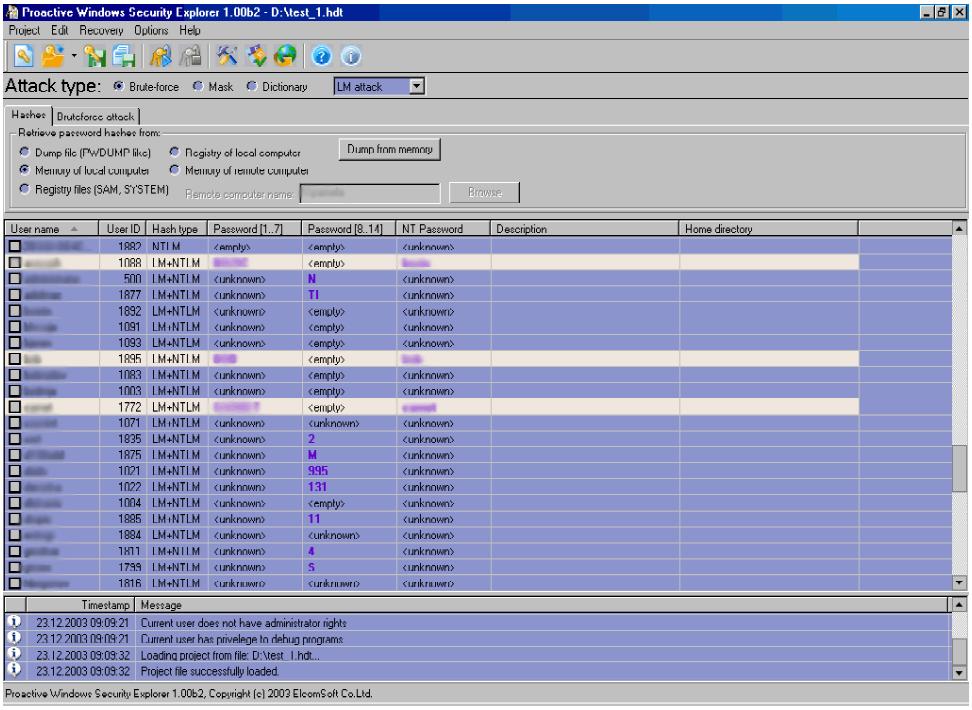
- traku s izbornicima,
- traku s alatima,
- radno područje.

Traka s izbornicima sastoji se od pet izbornika (*Project*, *Edit*, *Recovery*, *Options*, *Help*), kroz koje je moguće podešavanje parametara aplikacije, dok traka s alatima, uobičajeno, sadrži ikone pritiskom na koje je moguć odabir jednog dijela opcija iz izbornika.

Radno područje aplikacije podijeljeno je u tri dijela. U gornjem dijelu moguće je odabrati vrstu ispitivanja sigurnosti, odnosno napada, te podesiti specifične parametre vezane uz svaku vrstu ispitivanja sigurnosti. Središnji dio radnog područja sadrži listu korisničkih računa s pripadajućim atributima nad kojima se provodi testiranje, dok se u donjem dijelu radnog područja nalazi statusni prozor za poruke koje generira aplikacija.

Upravljanje radom aplikacije moguće je kroz izbornike. Korisniku je na raspolaganju pet izbornika:

- *Project*,
- *Edit*,
- *Recovery*,
- *Options* i
- *Help*.



Slika 1: Izgled aplikacije

Izbornik *Project* sadrži naredbe kojima se može upravljati projektima odnosno radnom okolinom (ekstenzija Security Explorer projects datoteka je `.hdt`). Istovremeno nije moguće imati otvoreno više radnih okolina no, ukoliko je to potrebno, aplikaciju je moguće pokrenuti u više instanci. Naredbe izbornika *Project* su sljedeće:

- *New* – otvara novu radnu okolinu,

- *Open* – otvara postojeću radnu okolinu,
- *Save*, *Save as* – pohranjuje trenutno otvoreni projekt,
- *Save report* – pohranjuje izvješće o otkrivenim zaporkama unutar trenutno otvorene radne okoline,
- *Exit* – izlaz iz aplikacije.

Izbornik *Edit* sadrži naredbe kojima je moguće podešavati odabir korisničkih računa nad kojima će se provoditi ispitivanje sigurnosti. Na raspolaganju su sljedeće naredbe:

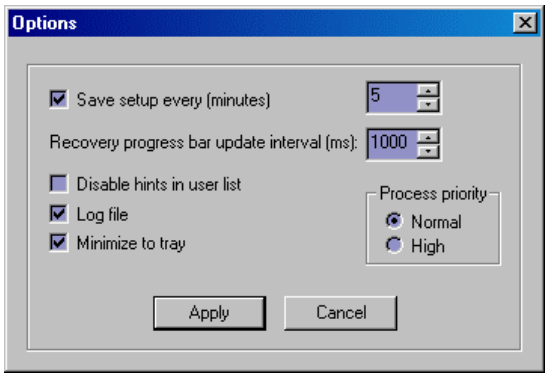
- *Select all* – odabir svih korisničkih računa,
- *Select highlited* – odabir označenih korisničkih računa,
- *Unselect all* – uklanjanje svih označenih korisničkih račina,
- *Reverse selection* – odabir neoznačenih korisničkih računa (inverzija).

Izbornik *Recovery* sadrži samo dvije naredbe za pokretanje i zaustavljanje ispitivanja sigurnosti:

- *Start recovery* – pokreće ispitivanje sigurnosti,
- *Stop recovery* – zaustavlja ispitivanje sigurnosti.

Kroz izbornik *Options* (Slika 2) odabirom naredbe *General* moguće je podesiti sljedeće parametre rada aplikacije:

- *Save setup every (minutes)* – omogućava automatsko pohranjivanje trenutnog stanja radne okoline (*backup*); čak i ukoliko projekt nije bio pohranjen, ukoliko je ova opcija uključena, stanje radne okoline se pohranjuje u `untitled.hdt` datoteku,
- *Progress bar update interval (ms)* – omogućava podešavanje osvježavanja vizualnog indikatora i statusnog prozora; povećavanjem ove vrijednosti moguće je postići nešto veću brzinu samog ispitivanja sigurnosti,
- *Disable hints in user list* – ova opcija se ne koristi u beta inačici,
- *Minimize to tray* – minimizira prozor u *Tray*, a ne u traku s aplikacijama,
- *Log file* – zapisuje sve informacije iz statusnog prozora u log datoteku `pwsex.log`,
- *Priority* – podešavanje prioriteta aplikacije; ukoliko se prioritet postavi na vrijednost *Normal* aplikacija koristi samo slobodno procesorsko vrijeme ne utječući na performanse ostalih aplikacija; ukoliko se pak prioritet postavi na vrijednost *High*, ispitivanje sigurnosti se odvija osjetno brže, no istovremeno se narušavaju performanse izvođenja drugih aplikacija na sustavu.



Slika 2: Podešavanje radnih parametara

Izbornik *Help* sadrži standardne naredbe vezane uz pomoć pri radu (*Contents*, *Tip of the day*, *About*), informacije o registriranju (*Registration information*), te potencijalno vrlo korisnu naredbu za *online* provjeru raspoloživosti novijih inačica aplikacije (*Check for updates*). U ispitanoj beta inačici ova naredba nije bila funkcionalna.

5.2. Ispitivanje sigurnosti

5.2.1. Dohvaćanje autentikacijskih podataka

Dohvaćanje autentikacijskih podataka nad kojima će se provoditi ispitivanje sigurnosti moguće je provesti na više načina, a odabire se unutar kartice *Hashes* u radnom području aplikacije (Slika 3). Podržane su sljedeće metode:

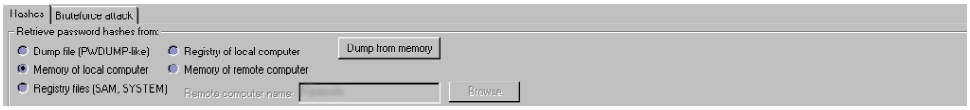
- korištenje datoteke (*Dump file*),
- korištenje lokalne *registry* datoteke (*Registry of local computer*),
- korištenje *registry* datoteka na disku (*Registry files*),
- korištenje memorije lokalnog računala (*Memory of local computer*) i
- korištenje memorije udaljenog računala (*Memory of remote computer*).

Za korištenje podataka iz datoteke potrebno je navesti izvor, odnosno *dump* datoteku za zapisima u sljedećem obliku:

```
korisničko_ime:korisnički_ID:LM_hash:NTLM_hash:komentar:HOME_directorij:
```

Ovako oblikovanu dump datoteku moguće je dobiti korištenjem drugih aplikacija (npr. PWDump ili Samdump).

Na sustavima koji ne koriste *Active Directory* autentikacijske podatke je moguće dohvatiti iz lokalne *registry* datoteke. Za dohvaćanje podataka na ovaj način potrebne su lokalne administrativne ovlasti. Također, moguće je dohvaćanje autentikacijskih podataka iz SAM i SYSTEM *registry* datoteka na disku. Pri tome treba imati na umu da su te datoteke pri radu sustava zaključane od strane operacijskog sustava, pa im direktan pristup nije moguć.



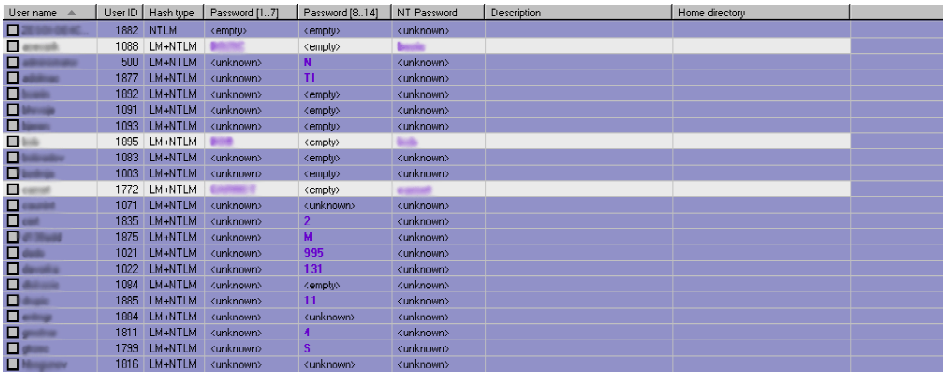
Slika 3: Odabir metode dohvaćanja autentikacijskih podataka

Podatke je također moguće dohvatiti iz memorije lokalnog ili udaljenog računala, za što su također potrebne administrativne ovlasti na sustavu s kojeg se podaci žele dohvatiti. Pri tome nije važno da li na sustavu postoji *Active Directory* ili ne. Podaci s udaljenog računala dohvaćaju se unošenjem UNC putanje (`\\server`).

5.2.2. Pregled podataka radne okoline

Svi autentikacijski podaci koji su dohvaćeni korištenjem neke od metoda opisanih u prethodnom poglavlju prikazuju se u radnom području aplikacije kao niz zapisa sa sljedećim atributima (Slika 4):

- korisničko ime (*User name*),
- korisnički ID broj (*User ID*),
- vrsta *hash* podataka (*Hash type*) – LM i/ili NTLM,
- prvi dio LM zaporke (*Password [1.7]*),
- drugi dio LM zaporke *(Password [8..14]*),
- NT zaporka (*NT Password*),
- opis (*Description*) i
- *home* direktorij (*Home directory*).



Slika 4: Izgled radnog područja

Osim korištenja metoda za dohvaćanje podataka, autentikacijske podatke moguće je dobiti i otvaranjem neke od postojećih datoteka radne okoline (`.hdt` datoteka).

Između svih zapisa koji se nalaze u radnom području aplikacije moguće je odabrati proizvoljni broj zapisa nad kojima će se provoditi ispitivanje. To se postiže korištenjem izbornika *Edit* ili kontekstnog izbornika (pritiskom na desni gumb miša iznad radnog područja aplikacije).

5.2.3. Odabir načina ispitivanja

Ispitivanje sigurnosti, obzirom na raspoložive *hash* vrijednosti zaporki, odnosno obzirom na metodu autentikacije, moguće je provesti nad LM ili NTLM vrijednostima. Ukoliko su na raspolaganju LM i NTLM *hash* vrijednosti preporuča se korištenje LM vrijednosti, pošto se kod LM autentikacijske sheme koriste jednostavniji algoritmi, pa je i vremenska složenost manja.
Ispitivanje sigurnosti moguće je provesti na tri načina:

- napad primjenom sile (engl. *brute force*),
- napad korištenjem maske (engl. *mask*) i
- napad korištenjem rječnika (engl. *dictionary attack*).

Napad primjenom sile predstavlja napad u kojem se ispituju sve moguće kombinacije iz odabranog skupa znakova u cilju pronalaženja originalne zaporke. Ova vrsta napada je relativno najsporija, no kod kratkih i jednostavnih zaporki postiže izuzetno dobre rezultate.
Napad korištenjem maske jest ustvari varijacija napada primjenom sile, u kojem je moguće odabrati proizvoljnu masku i na taj način efektivno smanjiti broj kombinacija, odnosno ukupno vrijeme potrebno da bi se napad proveo. Npr., ukoliko je poznato da su prva dva znaka zaporke "AB", a sedmi znak "0", moguće je postaviti sljedeću masku:

```
AB####0
```

Ukoliko se provodi ispitivanje korištenjem napada primjenom sile ili korištenjem maske moguće je podesiti dodatne parametre. Podešavanje se provodi u radnom području aplikacije unutar kartica *Bruteforce attack* (Slika 5) ili *Mask attack*. Parametri koji se mogu podešavati su sljedeći:

- Skup znakova – moguće je uključivati slova (*All latin*), brojke (*All digits*) i specijalne znakove (*Special*) u bilo kojoj kombinaciji, a također je moguće uključiti i specifične skupove znakova (*Custom charset*). Ako se koristi napad na NTLM zaporke moguće je definirati da li će se u ispitivanju koristiti velika i/ili mala slova (*Uppercase*, *Lowercase*, *Both cases*).
- Duljina zaporke (*Password length*) – moguće je podesiti minimalnu i maksimalnu duljinu zaporki koje će se ispitivati. Iako Windows operacijski sustav podržava duljine zaporki veće od 14 znakova, u aplikaciji je maksimalna duljina ograničena na 14 znakova, budući da napad primjenom sile nad duljim nizovima znakova nije moguće provesti u vremenski razumnom periodu. Ovaj parametar moguće je podesiti samo za napad primjenom sile.
- Proizvoljni početak zaporke (*Start from password*) – ova opcija omogućava pokretanje ispitivanja od neke specifične zaporke na dalje. U načelu ovo polje je potrebno ostaviti praznim. Ukoliko se ispitivanje prekine u tom polju će ostati zapisana posljednja ispitana zaporka, te se u tom slučaju ispitivanje može naknadno nastaviti od te točke na dalje.
- Maska (*Password mask*) – ovom opcijom moguće je podesiti proizvoljnu masku kako je ranije opisano, s time da je znak maskiranje također moguće odabrati proizvoljno (*Mask char*). Ovaj parametar moguće je podesiti samo za napad korištenjem maske.

Slika 5: Parametri napada primjenom sile

Napad korištenjem rječnika jest specifična vrsta napada koja koristi ulaznu datoteku s popisom riječi koje se upotrebljavaju prilikom iskušavanja potencijalnih zaporki. Aplikacija podržava ulazne datoteke u `.txt` ili `.dic` formatu. Kod ovog napada moguće je podesiti samo početak od proizvoljnog retka datoteke (*Start from line*).

6. Mogućnosti i primjena

Ispitana aplikacija, iako u beta inačici, pokazala se vrlo dobrom i stabilnom. Prilikom rada nisu uočeni nikakvi nedostaci niti nelogičnosti u korisničkom sučelju.

Testna platforma je bio Celeron 500 s 512MB radne memorije. Za potrebe testiranja provedena su ispitivanja korištenjem napada primjenom sile, dok su svi testovi provedeni s normalnim prioritetom procesa. Pokazalo se da je i na platformama koje u današnje vrijeme ne predstavljaju sam vrh po računalnim resursima moguće vrlo efikasno provoditi ovakvu vrstu testiranja/napada. U najkraćem vremenskom periodu (nekoliko sekundi) probijene su slabe zaporke <6 znakova, dok je za dulje zaporke bilo potrebno nekoliko sati; no većina zaporki (>80%) probijena je u roku kraćem od jednog dana.
Testni sustav predstavljao je sliku uobičajenog produkcijskog sustava za naše prilike (~100 korisnika, *Active Directory* servis, LM+NTLM autentikacija). Na temelju dobivenih rezultata pokazuje se da je vrlo velik broj korisničkih računa podložan napadima korištenjem rječnika ili primjenom sile, pošto korisnici vrlo često odabiru zaporke čija složenost nije zadovoljavajuća.
Zbog toga je korištenje aplikacija ovog tipa, u periodičkim vremenskim razdobljima, vrlo korisno za administratore sustava, budući da se na temelju dobivenih rezultata mogu uočiti potencijalno ranjive korisničke zaporke, a samim time i potencijalne penetracijske točke za lokalne ili udaljene zlonamjerne korisnike.

7. Zaključak

Kompromitiranje zaporki je jedan je od najčešćih i najefikasnijih napada na računalne i mrežne resurse. Korisnici vrlo često upotrebljavaju jednostavne kombinacije znakova, fraze, imena itd. Isto tako, mrežni administratori vrlo često zaboravljaju ukloniti predefinirane korisničke račune, račune korisnika koji više nisu zaposleni i sl. Takvi korisnički računi najčešće su meta napada.
Zbog sve češće integracije servisa isti korisnički računi upotrebljavaju se za razne namjene i kao takvi mogu biti meta napada na raznim instancama, kao što su npr. WWW, FTP, VPN, *dial-in*, POP3, IMAP, SMTP i drugi servisi koji zahtijevaju autentikaciju.
Ispitivanje sigurnosti zaporki jedna je od osnovnih metoda ispitivanja sigurnosti kojoj se svakako mora pridijeliti odgovarajuća pažnja, pošto je poznato da korisnici vrlo često ne obraćaju pozornost na sigurnost svojih zaporki, što se pokazalo i prilikom eksperimentalnog ispitivanja sigurnosti gdje je korištenjem ispitanog alata unutar 24 sata otkriveno više od 80% zaporki na ispitanom sustavu, što predstavlja poražavajući rezultat.
Proactive Windows Security Explorer, iako u beta inačici, pokazao se kao vrlo efikasno i pouzdano rješenje za ispitivanje sigurnosti zaporki. Sve opcije alata funkcioniraju u skladu s očekivanjima, a korisničko sučelje je pregledno i intuitivno. Neke od opcija koje nisu dostupne u ovom alatu, a bile bi vrlo korisne, jesu mogućnost dohvaćanja i ispitivanja sigurnosti zaporki pregledavanjem mrežnog prometa, no i bez toga alat se svakako može preporučiti mrežnim administratorima za redovito provođenje ispitivanja sigurnosti njihovih sustava.