HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza PsTools programskog paketa

CCERT-PUBDOC-2004-08-87

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 4

2. INSTALACIJA I POKRETANJE 4

3. ALATI 4

3.1. PsExec 4
3.2. PsFile 5
3.3. PsGetSid 6
3.4. PsInfo 6
3.5. PsKill 6
3.6. PsList 7
3.7. PsLoggedOn 7
3.8. PsLogList 8
3.9. PsPasswd 8
3.10. PsService 9
3.11. PsShutdown 9
3.12. PsSuspend 10

4. ZAKLJUČAK 10

1. Uvod

Windows NT/2000/XP operacijski sustavi pretežito su grafički orijentirani, te se većina administrativnih zadataka obavlja korištenjem grafičkih alata i aplikacija. U velikom broju slučajeva to pojednostavljuje poslove administracije sustava te olakšava rad sistem administratorima.
Unatoč tome, ponekad je obavljanje nekih specifičnih zadataka i/ili generiranje skripti za automatizirano izvođenje naredbi bez interakcije administratora mnogo jednostavnije i efikasnije korištenjem alata koji se mogu pokrenuti iz komandne linije (naredbenog retka).
Postoji određeni broj Windows aplikacija i programskih alata koji se mogu pokrenuti iz komande linije, a također postoje i Windows NT/2000/XP *Resource Kit* i *Support Tools* alati koji proširuju standardne mogućnosti administracije Windows operacijskih sustava. No i uz ovakve alate određeni broj funkcija i dalje nedostaje ili postoji mogućnost njihova unaprjeđenja i nadogradnje.
PsTools je *freeware* paket od 12 alata koje su razvili Mark Russinovich i Bryce Cogswell, odnosno tvrtka Sysinternals (http://www.sysinternals.com).
PsTools alati omogućavaju izvršavanje specifičnih administrativnih zadataka iz komandne linije. Samo ime PsTools vuče korijene od UNIX naredbe `ps`, dio čije funkcionalnosti je implementiran u prvom razvijenom alatu `PsList`, na temelju koje je i cijeli, kasnije razvijeni, paket alata dobio prefiks "Ps".
Ono po čemu se PsTools programi ponajviše razlikuju od standardnih Windows alata jest njihova mogućnost izvršavanja na udaljenim sustavima, što ih čini posebno korisnim za administratore sustava koji se sastoje od većeg broja dislociranih računala.

2. Instalacija i pokretanje

Instalacija pojedinih alata ili cijelog paketa u punom smislu riječi nije potrebna. Paket ili pojedine od alata iz paketa dovoljno je dohvatiti s referentne lokacije, odnosno službenih stranica Sysinternals-a (http://www.sysinternals.com/ntw2k/freeware/pstools.shtml), raspakirati u željeni direktorij te pokrenuti.

3. Alati

PsTools paket sastoji se od 12 alata navedenih u nastavku:
- PsExec – omogućava pokretanje procesa na udaljenim sustavima ,
- PsFile – prikazuje datoteke otvorene na udaljenim sustavima ,
- PsGetSid – prikazuje SID identifikator korisnika ili računala,
- PsKill – terminira procese prema imenu ili PID identifikatoru ,
- PsInfo – prikazuje informacije o sustavima,
- PsList – prikazuje informacije o procesima,
- PsLoggedOn – prikazuje popisnika prijavljenih lokalno ili preko dijeljenih resursa,
- PsLogList – prikazuje zapise *log* datoteka,
- PsPasswd – služi za promjenu zaporki,
- PsService – služi za pregled i kontrolu rada servisa,
- PsShutdown – služi za gašenje, restartanje i slične operacije,
- PsSuspend – suspendira procese.

Detaljna funkcionalnost i mogućnosti primjene svakog od spomenutih alata opisane su u nastavku dokumenta.

3.1. PsExec

`PsExec` naredba služi za pokretanje aplikacija ili naredbi na udaljenim računalima. Aplikacije s dugačkim imenima potrebno je ograditi navodnicima (""), a mogu se izvoditi implicitno u kontekstu korisnika koji je pokrenuo `PsExec` naredbu, u kojem slučaju pristup mrežnim resursima nije moguć ili u eksplicitnom korisničkom kontekstu, kada je pristup mrežnim resursima moguć ovisno o ovlastima korištenog korisničkog računa. Naredba ne zahtijeva nikakvu instalaciju na udaljenim sustavima, a omogućava potpunu interaktivnost pri pokretanju alata iz komandne linije. Sigurnosni nedostatak u

ovom slučaju, kao i kod ostalih alata iz paketa, jest da se korisničko ime i zaporka navedeni u opcijama naredbe prenose preko mreže kao otvoreni tekst.
Sintaksa naredbe je sljedeća:

```
psexec [\\computer[,computer2[,...] | @file][-u user [-p psswd]]
[-n s][-s|-e][-i][-c [-f|-v]][-w directory][-d][-<priority>]
[-a n,n,...] cmd [arguments]
```

Pojedini parametri naredbe imaju sljedeća značenja:
- `-a` – služi za odjeljivanje procesora na kojima će aplikacija biti pokrenuta (separator je zarez ","),
- `-c` – kopira program koji je potrebno izvršiti na udaljeni sustav, ukoliko se ovaj parametar ispusti ciljna aplikacija mora biti u sistemskoj putanji na udaljenom sustavu,
- `-d` – ne čeka se terminacija procesa (ne-interaktivno),
- `-e` – učitava specificirani profil vezan uz korisnički račun,
- `-f` – kopira program koji je potrebno izvršiti na udaljeni sustav, bez obzira da li taj program već postoji na udaljenom sustavu,
- `-i` – pokreće program na udaljenom sustavu uz interakciju kroz radno područje (eng. *desktop*),
- `-n` – specificira vremensku zadršku (eng. *timeout*) prije spajanja na udaljena računala,
- `-p` – specificira opcionalnu zaporku za korisničko ime, ukoliko se ovaj parametar ispusti prilikom pokretanja naredbe biti će potrebno unijeti zaporku koja neće biti vidljiva na zaslonu,
- `-s` – pokreće udaljeni proces s ovlastima `System` korisničkog računa,
- `-u` – specificira opcionalno korisničko ime za izvršavanje naredbe,
- `-v` – kopira program koji je potrebno izvršiti na udaljeni sustav samo ukoliko je broj inačice veći ili je datoteka novija,
- `-w` – podešava radni direktorij procesa na udaljenom sustavu,
- `-priority` – specificira prioritet procesa koji se pokreće, dozvoljene vrijednosti su redom (od najmanjeg prioriteta): `-low`, `-belownormal`, `-abovenormal`, `-high`, `-realtime`,
- `computer` – pokreće specificiranu naredbu na računalu ili računalima, ukoliko je ovaj parametar ispušten naredba se izvršava na lokalnom sustavu, a ukoliko se koristi sintaksa `\\*`, naredba se izvršava na svim računalima koja se nalaze u domeni,
- `@file` – specificirana naredba se pokreće na svim računalima navedenim u datoteci,
- `program` – ime aplikacije ili naredbe ko ja se pokreće,
- `arguments` – specificira argumente koji se prosljeđuju naredbi (putanje datoteka moraju biti apsolutne na ciljnom sustavu ili sustavima).

3.2. PsFile

`PsFile` naredba služi za pregled ili zatvaranje datoteka otvorenih s udaljenih sustava na lokalnom sustavu ili na udaljenom računalu. Prikazuje se direktorij koji je otvoren s udaljenog sustava, korisnički račun koji se koristi za pristup, te efektivna prava pristupa. Za razliku od `net file` naredbe, `PsFile` ne skraćuje imena dugačkih datoteka.
Sintaksa naredbe je sljedeća:

```
psfile [\\RemoteComputer [-u Username [-p Password]]] [[Id | path]
[-c]]
```

Pojedini parametri naredbe imaju sljedeća značenja:
- `-c` – zatvara datoteku s identifikatorom "Id",
- `-p` – specificira opcionalnu zaporku za korisničko ime, ukoliko se ovaj parametar ispusti prilikom pokretanja naredbe biti će potrebno unijeti zaporku koja neće biti vidljiva na zaslonu,
- `-u` – specificira opcionalno korisničko ime za izvršavanje naredbe,
- `Id` – identifikator datoteke za pregled ili zatvaranje, ukoliko se ovaj parametar ispusti ispisuju (ili zatvaraju) se sve datoteke na ciljnom sustavu,
- `Path` – puna ili djelomična putanja datoteka za pregled ili zatvaranje.

3.3. PsGetSid

`PsGetSid` naredba služi za dohvaćanje SID-a (eng. *Security Identifier*) pojedinog računala ili korisničkog računa, što je inače moguće jedino pregledavanjem *registry* datoteke. Ova naredba je vrlo korisna prilikom pojave dupliciranih SID identifikatora na računalnoj mreži.
Sintaksa naredbe je sljedeća:

```
psgetsid [\\computer[,computer[,...] [-u Username [-p Password]]]
[account | SID]
```

Pojedini parametri naredbe imaju sljedeća značenja:
- `-p` – specificira opcionalnu zaporku za korisničko ime, ukoliko se ovaj parametar ispusti prilikom pokretanja naredbe biti će potrebno unijeti zaporku koja neće biti vidljiva na zaslonu,
- `-u` – specificira opcionalno korisničko ime za izvršavanje naredbe,
- `computer` – udaljeno računalo ili računala, ukoliko je ovaj parametar ispušten naredba se izvršava na lokalnom sustavu,
- `account` – korisnički račun za koji se želi dohvatiti SID oznaka (ukoliko se želi dohvatiti isti umjesto SID oznake računala),
- `SID` – inverzna operacija, dohvaćanje korisničkog računa prema specificiranom SID broju.

3.4. PsInfo

`PsInfo` naredba služi za ispis sistemskih informacija o lokalnom ili udaljenom Windows NT/2000/XP operacijskom sustavu. Ispisuju se standardne informacije kao što su operacijski sustav, inačica jezgre sustava (engl. *kernel*), *uptime*, inačica Internet Explorer Web preglednika, radna memorija, procesor(i) i sl. Također je moguć ispis informacija o instaliranim programskim paketima i/ili zakrpama (eng. *hotfixes*). Za ispravan rad, psinfo naredba mora imati ovlasti za pristup `HKLM\System` grani *registy* datoteke.
Sintaksa naredbe je sljedeća:

```
psinfo [-h] [-s] [-d] [-c [-t delimiter]] [filter]
[\\computer[,computer[,..]]|@file [-u Username [-p Password]]]
```

Pojedini parametri naredbe imaju sljedeća značenja:
- `-c` – ispis u CSV (eng. *comma separated values*) formatu,
- `-d` – prikaz informacija o tvrdim diskovima sustava (*disk volume information*),
- `-h` – prikazuje instalirane zakrpe,
- `-p` – specificira opcionalnu zaporku za korisničko ime, ukoliko se ovaj parametar ispusti prilikom pokretanja naredbe biti će potrebno unijeti zaporku koja neće biti vidljiva na zaslonu,
- `-s` – prikazuje instalirane programske pakete,
- `-t` – specificira separator u CSV formatu (predefinirana vrijednost je zarez ","),
- `-u` – `specificira` opcionalno korisničko ime za izvršavanje naredbe,
- `filter` – specificira filtar za prikaz sistemskih informacija (u tekstualnom obliku),
- `computer` – ispisuje sistemske informacije o udaljenom računalu ili računalima, ukoliko je ovaj parametar ispušten naredba se izvršava na lokalnom sustavu, a ukoliko se koristi sintaksa `\\*`, naredba se izvršava na svim računalima koja se nalaze u domeni,
- `@file` – ispisuje sistemske informacije o svim računalima navedenim u datoteci.

3.5. PsKill

`PsKill` naredba služi za terminiranje procesa na lokalnom ili udaljenom sustavu prema imenu procesa ili njegovom idententifikatoru. Slična naredba (`kill`) dio je i npr. *Resource Kit* paketa za Windows 2000 sustave, no korištenjem te naredbe nije moguće terminirati procese na udaljenim računalima. Sintaksa naredbe je sljedeća:

```
pskill [\\computer [-u username [-p password]]] <process Id or
name>
```

Pojedini parametri naredbe imaju sljedeća značenja:

- `-p` – specificira opcionalnu zaporku za korisničko ime, ukoliko se ovaj parametar ispusti prilikom pokretanja naredbe biti će potrebno unijeti zaporku koja neće biti vidljiva na zaslonu,
- `-u` – specificira opcionalno korisničko ime za izvršavanje naredbe,
- `computer` – udaljeno računalo ili računala, ukoliko je ovaj parametar ispušten naredba se izvršava na lokalnom sustavu.

3.6. PsList

`PsList` naredba daje popis procesa na lokalnom ili udaljenom sustavu s pripadajućim informacijama. Rezultat ove naredbe u velikoj mjeri je sličan sa standardnom Windows GUI aplikacijom *Task Manager*, odnosno s `pstat` and `pmon` alatima komandne linije iz *Resource Kit* paketa. `PsList` u sebi sadrži mogućnosti oba spomenuta alata, a za razliku od njih, omogućava pregledavanje procesa i na udaljenim sustavima.
Sintaksa naredbe je sljedeća:

```
pslist [-d][-m][-x][-t][-s [n] [-r n] [\\computer [-u username][-p password][name|pid]
```

Pojedini parametri naredbe imaju sljedeća značenja:
- `-d` – prikazuje informacije o programskim nitima (eng. *thread*),
- `-e` – zahtijeva točno ime definirano `name` parametrom,
- `-m` – prikazuje informacije memoriji,
- `-p` – specificira opcionalnu zaporku za korisničko ime, ukoliko se ovaj parametar ispusti prilikom pokretanja naredbe biti će potrebno unijeti zaporku koja neće biti vidljiva na zaslonu,
- `-r n` – kontinuirani (*task manager*) način rada, period osvježavanja se definira u sekundama, a izlazak iz ovog načina rada provodi se pritiskom na tipku ESC,
- `-t` – prikazuje se stablo procesa,
- `-u` – specificira opcionalno korisničko ime za izvršavanje naredbe,
- `-x` – prikazuje procese, informacije o memoriji i programskim nitima
- `computer` – udaljeno računalo ili računala, ukoliko je ovaj parametar ispušten naredba se izvršava na lokalnom sustavu,
- `name` – prikazuje informacije o procesu čije ime počinje s navedenim imenom (može se koristiti i s `-e` parametrom)
- `PID` – prikazuje informacija o procesu sa specificiranim PID-om (eng. *process ID*).

U tekstualnom prikazu sve memorijske vrijednosti prikazane su u KB (kilobajtima), a imena stupaca označavaju sljedeće:
- `Pri` – prioritet,
- `Thd` – broj programskih niti,
- `Hnd` – broj rukovatelja (eng. *handles*),
- `VM` – virtualna memorija,
- `WS` – radni skup (eng. *working set*),
- `Priv` – privatna virtualna memorija,
- `Priv` Pk – maksimalna vrijednost (eng. *peak*) privatne virtualne memorije,
- `Faults` – broj promašaja virtualnih stranica,
- `NonP` – skup koji nije indeksiran u priručnoj memoriji (eng. *non-paged pool*),
- `Page` – skup koji je indeksiran u priručnoj memoriji (eng. *paged pool*),
- `Cswthc` – kontekstni prekidači (eng. *context switches*).

3.7. PsLoggedOn

`PsLoggedOn` naredba prikazuje popis korisnika trenutno prijavljenih za rad na lokalnom sustavu, udaljenom sustavu ili unutar domene. Naredba je funkcionalno slična `net session` naredbi, no za razliku od `net session` koja radi isključivo lokalno, `PsLoggedOn` omogućava pregled prijavljenih korisnika i na udaljenim sustavima. Za ispravan rad naredba mora imati odgovarajuće ovlasti za pristup `HKEY_USERS` grani *registry* datoteke.
Sintaksa naredbe je sljedeća:

```
psloggedon [-l] [-d domain] [-x] [\\computername]
```

Pojedini parametri naredbe imaju sljedeća značenja:
- `-d` – pretražuje specificiranu domenu,
- `-l` – prikazuje samo lokalne prijave za rad,
- `-x` – isključuje prikaz vremena prijave za rad.

3.8. PsLogList

`PsLogList` naredba služi za prikaz informacija iz *log* datoteka u tekstualnom obliku, za razliku od standardne Windows aplikacije *Event Viewer* koja slične informacije prikazuje u grafičkom obliku. Prikaz u tekstualnom obliku može biti vrlo koristan za administratore, jer primjenom pojedinih filtara i/ili teksutalnim pretraživanjem mogu doći do korisnih informacija. Funkcionalno naredba je ista kao i `elogdump` naredba *Resource Kit* paketa, ali za razliku od nje omogućava unos korisničkog imena i zaporke ukoliko ovlasti trenutno prijavljenog korisnika nisu dovoljne za pregled udaljenih ili lokalnih *log* datoteka.
Sintaksa naredbe je sljedeća:

```
psloglist [\\computer[,computer2[,...] | @file] [-u username
[-p password]]] [-s [-t delimiter]] [-n # | -d # | -h #][-c][-x]
[-r][-a mm/dd/yy][-b mm/dd/yy] [-f filter] [-i ID,[ID,...]]
[-o event source] [-l event log file] <event log>
```

Pojedini parametri naredbe imaju sljedeća značenja:
- `-a` – prikazuje zapise s vremenskom značkom novijom od specificiranog datuma,
- `-b` – prikazuje zapise s vremenskom značkom starijom od specificiranog datuma,
- `-c` – briše event *log* nakon prikaza,
- `-d` – prikazuje samo zapise iz prethodnih `n` dana,
- `-f` – filtrira događaje prema vrsti, kao filtar služi početno slovo npr. "-f we" filtrira upozorenja (eng. *warnings*) i pogreške (eng. *errors*),
- `-h` – prikazuje samo zapise prethodnih `n` sati,
- `-i` – prikazuje samo događaje sa specificiranim ID-om ili ID-ovima (maksimalno 10),
- `-l` –prikazuje sadržaj specificirane *event log* datoteke,
- `-n` – prikazuje samo posljednjih `n` zapisa,
- `-o` – prikazuje samo zapise od specificiranog izvora
- `-p` – specificira opcionalnu zaporku za korisničko ime, ukoliko se ovaj parametar ispusti prilikom pokretanja naredbe biti će potrebno unijeti zaporku koja neće biti vidljiva na zaslonu,
- `-r` – prikazuje *log* zapise obrnutim redoslijedom, od najstarijeg do najnovijeg,
- `-s` – zapisi se prikazuju u jednom retku, odvojeni separatorom
- `-t` – specificira separator (predefinirani separator je zarez ","), a koristi se u kombinaciji s `-s` parametrom
- `-u` – specificira opcionalno korisničko ime za izvršavanje naredbe,
- `-x` – prikazuje proširene informacije,
- `computer` – udaljeno računalo ili računala, ukoliko je ovaj parametar ispušten naredba se izvršava na lokalnom sustavu,
- `@file` – naredba se izvodi na svim računalima navedenim u datoteci,
- `eventlog` – specificira koji *log* se prikazuje (predefinirano je *system*), a ukoliko se koristi `-l` parametar, služi za određivanje načina interpretacije *log* datoteke.

3.9. PsPasswd

`PsPasswd` naredba služi za promjenu zaporke ili zaporki na lokalnom sustavu, udaljenim sustavima ili na domeni. Korištenje ove naredbe korisno je prilikom izvršavanja *batch* procesa ili promjene sistemskih i/ili administratorskih zaporki na udaljenim sustavima.
Sintaksa naredbe je sljedeća:

```
pspasswd [\\[computer[,computer,[,...]|Domain]|@file] [-u Username
[-p Password]]] Username [NewPassword]
```

Pojedini parametri naredbe imaju sljedeća značenja:

- `-p` – specificira opcionalnu zaporku za korisničko ime, ukoliko se ovaj parametar ispusti prilikom pokretanja naredbe biti će potrebno unijeti zaporku koja neće biti vidljiva na zaslonu,
- `-u` – specificira opcionalno korisničko ime za izvršavanje naredbe,
- `computer` – udaljeno računalo ili računala, ukoliko je ovaj parametar ispušten naredba se izvršava na lokalnom sustavu, a ukoliko se koristi sintaksa `\\*`, naredba se izvršava na svim računalima koja se nalaze u domeni,
- `@file` – naredba se izvodi na svim računalima navedenim u datoteci,
- `Username` – specificira korisnički račun kojem se mijenja zaporka,
- `NewPassword` – specificira novu zaporku, ukoliko se ovaj parametar ispusti nova zaporka ima `NULL` vrijednost.

3.10. PsService

`PsService` naredba služi za kontrolu servisa na udaljenim sustavima ili lokalnom računalu. Korištenjem ove naredbe moguće je pokretati i zaustavljati pojedine servise, ispitivati njihov status, konfiguraciju, te ispitati međusobnu ovisnost servisa.
Za razliku od `sc` alata iz *Resource Kit* paketa, `PsService` omogućava prijavu na udaljene sustave korištenjem alternativnog korisničkog imena i zaporke, a također omogućava i automatsku identifikaciju specifičnih servisa na mreži (npr. DNS, DHCP i sl.).
Sintaksa naredbe je sljedeća:

```
psservice.exe [\\Computer [-u Username [-p Password]]] <cmd>
<optns>
```

Pojedini parametri naredbe imaju sljedeća značenja:

- `-p` – specificira opcionalnu zaporku za korisničko ime, ukoliko se ovaj parametar ispusti prilikom pokretanja naredbe biti će potrebno unijeti zaporku koja neće biti vidljiva na zaslonu,
- `-u` – specificira opcionalno korisničko ime za izvršavanje naredbe,
- `cmd` – naredba koja se izvršava, moguće je koristiti sljedeće naredbe:
    - `query` – ispituje status servisa,
    - `config` – ispituje konfiguraciju,
    - `start` – pokreće servis
    - `stop` – zaustavlja servis
    - `restart` – zaustavlja i zatim ponovno pokreće servis
    - `pause` – pauzira rad servisa
    - `cont` – pokreće pauzirani servis
    - `depend` – ispisuje servise koji su ovisni o specificiranom servisu
    - `find` – traži instance servisa na mreži
- `computer` – udaljeno računalo na kojem se kontrolira rad servisa, ukoliko se ovaj parametar ispusti kontroliraju se lokalni servisi.

3.11. PsShutdown

`PsShutdown` naredba služi za upravljanje radom lokalnog i udaljenih sustava. Upravljanje radom podrazumijeva mogućnosti gašenja, ponovnog pokretanja (engl. *restart*), isključivanja, hibernacije i slične opcije.
Sintaksa naredbe je sljedeća:

```
psshutdown -s|-r|-h|-d|-k|-a|-l|-o [-f] [-c] [-t [nn|h:m]]
[-m "message"] [-u Username [-p password]] [-n s]
[\\computer[,computer[,...]|@file]
```

Pojedini parametri naredbe imaju sljedeća značenja:
- `-a` – prekida postupak gašenja (moguće jedino ukoliko je pokrenuto gašenje s odbrojavanjem),
- `-c` – omogućava da interaktivno prijavljeni korisnik može prekinuti postupak gašenja
- `-d` – suspendira računalo,
- `-f` – prisiljava pokrenute aplikacije da se zatvore,
- `-h` – hibernira računalo,
- `-k` – isključuje računalo (restarta ukoliko isključivanje nije podržano),
- `-l` – zaključava (eng. *lock*) računalo,
- `-m` – šalje poruku na zaslon prijavljenih korisnika,
- `-n` – specificira vremenski period u sekundama prije spajanja na udaljena računala,
- `-o` – odjavljuje trenutno prijavljenog korisnika,
- `-p` – specificira opcionalnu zaporku za korisničko ime, ukoliko se ovaj parametar ispusti prilikom pokretanja naredbe biti će potrebno unijeti zaporku koja neće biti vidljiva na zaslonu,
- `-r` – restarta računalo nakon gašenja,
- `-s` – gasi računalo bez isključivanja,
- `-t` – specificira odbrojavanje u sekundama prije gašenja (predefinirana vrijednost je 20 sekundi) ili vrijeme gašenja (u 24-satnoj notaciji),
- `-u` – specificira opcionalno korisničko ime za izvršavanje naredbe,
- `computer` – udaljeno računalo ili računala, ukoliko je ovaj parametar ispušten naredba se izvršava na lokalnom sustavu,
- `@file` – naredba se izvodi na svim računalima navedenim u datoteci.

3.12. PsSuspend

`PsSuspend` naredba služi za suspendiranje i ponovno pokretanje procesa na lokalnom ili udaljenim sustavima, što je praktično prilikom vršnih opterećenja sustava, ukoliko se žele osloboditi resursi bez da se pojedini procesi terminiraju, što ostavlja mogućnost njihovog kasnijeg pokretanja.
Sintaksa naredbe je sljedeća:

```
pssuspend [-r] [\\RemoteComputer [-u Username [-p Password]]]
<process Id or name>
```

Pojedini parametri naredbe imaju sljedeća značenja:
- `-p` – specificira opcionalnu zaporku za korisničko ime, ukoliko se ovaj parametar ispusti prilikom pokretanja naredbe biti će potrebno unijeti zaporku koja neće biti vidljiva na zaslonu,
- `-r` – ponovno aktivira (eng. *resume*) suspendirani proces,
- `-u` – specificira opcionalno korisničko ime za izvršavanje naredbe,

4. Zaključak

PsTools alati predstavljaju skup iznimno korisnih i praktičnih alata koji proširuju standardne mogućnosti administracije Windows operacijskih sustava. Najveća specifičnost, a ujedno i najveće unaprjeđenje u odnosu na standardne Windows alate komandne linije jest mogućnost jednostavne administracije udaljenih računala. Svi alati su stabilni i rade u skladu s očekivanjima i specifikacijama. Jedini nedostatak cijelog paketa nije funkcionalni nego sigurnosni, naime korisnička imena i zaporke koje se unose kao opcionalni parametri naredbi preko mreže se prenose kao otvoreni tekst. Ovakav način prijenosa sa sigurnosnog stajališta nije prihvatljiv, pogotovo na nepreklapanim mrežama.
Sve u svemu, PsTools je funkcionalno besprijekorni paket, izuzetno koristan za mrežnu administraciju Windows operacijskih sustava, no sa sigurnosnog stajališta potrebna su određena unaprjeđenja.