HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza Core Force alata

CCERT-PUBDOC-2005-12-144

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

CORE FORCE alat služi zaštiti osobnih računala s Windows 2000 ili Windows XP inačicom operacijskih sustava. Ovaj besplatan alat istovremeno je sustav za prevenciju incidenata (engl. *host-based Intrusion Prevention System*, *H-IPS*) i osobni vatrozid.
Ovaj se alat može koristiti za:

1. zaštitu računala od crva, virusa i zlonamjernog koda,
2. sprečavanje napada na računalo,
3. sprečavanje iskorištavanja rupa u operacijskom sustavu i ostalim aplikacijama koje su instalirane na računalu,
4. sprečavanje iskorištavanja nepoznatih rupa u operacijskom sustavu i ostalim aplikacijama koje su instalirane na računalu (eng. *zero-days*),
5. otkrivanje i sprečavanje izvršavanja *adware*, *spyware* programa, trojanskih konja i ostalog zlonamjernog koda na računalu.

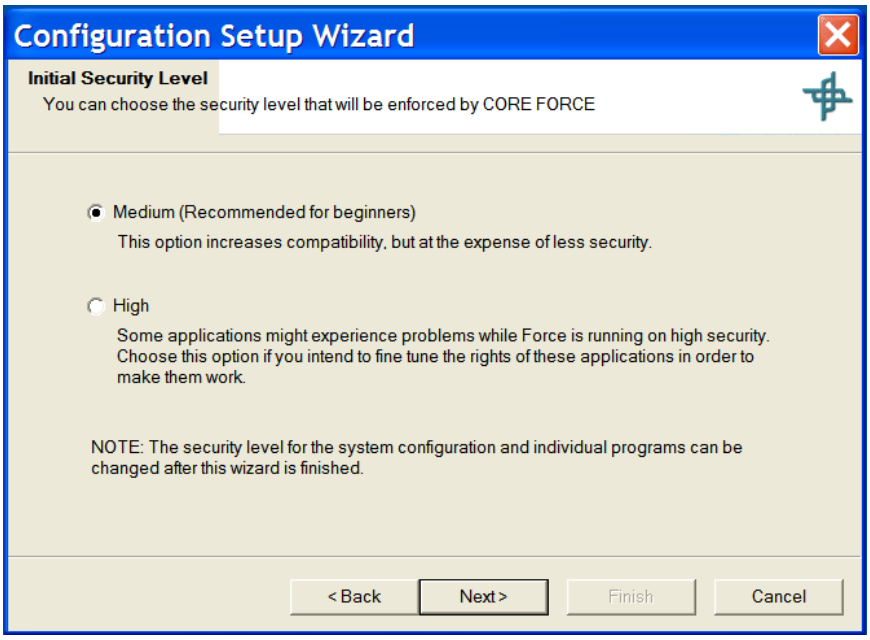
Alat omogućuje ulazno i izlazno filtriranje paketa TCP/IP protokola, granularnu kontrolu pristupa datotečnom sustavu i postavkama *registry-a* te provjeru integriteta programskih proizvoda. Alat se može podesiti da štiti sustav ili/i pojedinačnu aplikaciju ili/i skupine aplikacija kao što su npr. web pretraživači, klijenti za elektroničku poštu, i sl.
Daljnji opis alata i njegova podešavanja služe upravo za navedene aktivnosti.

2. Instalacija i pokretanje

Za instalaciju alata *Core Force* potrebno je dohvatiti izvršnu datoteku s adrese http://force.coresecurity.com/index.php?module=base&page=download i spremiti ju unutar proizvoljne mape na računalu. Datoteka je dostupna u `.exe` formatu pod imenom `CoreForceSetup0.80.120.exe` i veličine je 10,156 MB. Posljednja dostupna verzija alata je iz siječnja 2006. godine. Pokretanjem izvršne datoteke započinje instalacijski postupak koji će instalirati program unutar mape `Program Files` na računalu.
Kod instalacije na računalima s Windows XP inačicom operacijskog sustava korisnik treba dozvoliti instalaciju novih nepotpisanih upravljačkih programa (engl. *new unsigned drivers*). Tijekom instalacije, privremeno će doći do prekida mrežne povezanosti računala pa se preporuča zatvaranje svih mrežnih aplikacija, a po završetku instalacije, računalo treba ponovno pokrenuti (eng. *restart*). *Core Force* će biti aktivan tek nakon ponovnog pokretanja operacijskog sustava.

3. Početno podešavanje alata

Prilikom prvog pokretanja, alat treba podesiti. Podešavanje se izvodi neovisno o konfiguracijskim postavkama operacijskog sustava. Za podešavanje koristi se sučelje koje omogućuje spremanje postavki u datoteku, u `.xml` obliku . Korisnici mogu razmjenjivati datoteke s postavkama. Podešavati se može na dva načina. Prvi način jest podešavanje na razini sustava (engl. *system permissions*) koje sadrži postavke unutar operacijskog sustava. Drugi način je podešavanje za aplikacije koje mogu biti grupirane prema profilima (engl. *program permissions*).
Početno podešavanje odnosi se na postavljanje željene sigurnosne razine. Prva kartica čarobnjaka za podešavanje alata nudi izbor između srednje (engl. *medium*) i visoke (engl. *high*) razine sigurnosti.
Odabirom razine sigurnosti korisnik definira skupinu dozvola koje će se primjenjivati tijekom aktivnog djelovanja alata. Preporučena razina za početnike je srednja razina sigurnosti koja se kasnije može promijeniti i na visoku razinu. Izbor razina prikazan je na slici Slika 1.

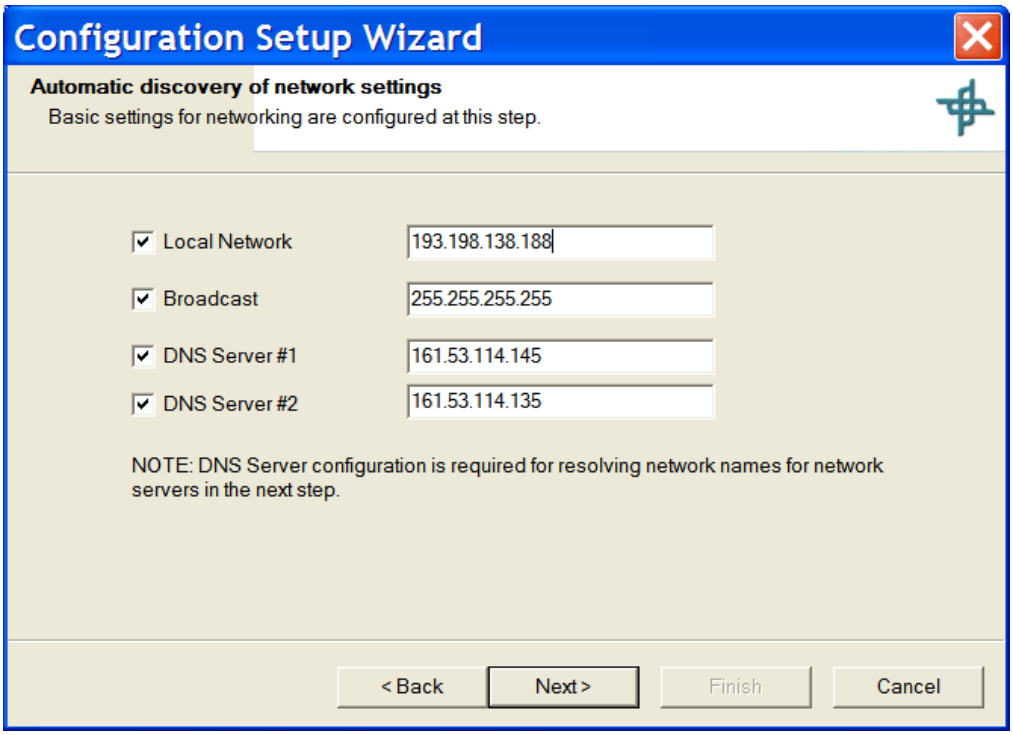


Slika 1: Podešavanje inicijalne razine sigurnosti alata

Na slijedećim karticama nazvanima *Automatic Discovery of Network Settings on the Setup Wizard (Basic settings)* i *Automatic Discovery of Network Settings on the Setup Wizard (Common servers)* podešavaju se mrežne postavke računala (Slika 2 i Slika 3). Alat će pretražiti mrežne postavke računala i prikupiti potrebne podatke. Ukoliko alat ne pronađe potrebne vrijednosti automatski, mora ih unijeti korisnik.

Na prvoj kartici upisuju se vrijednosti:

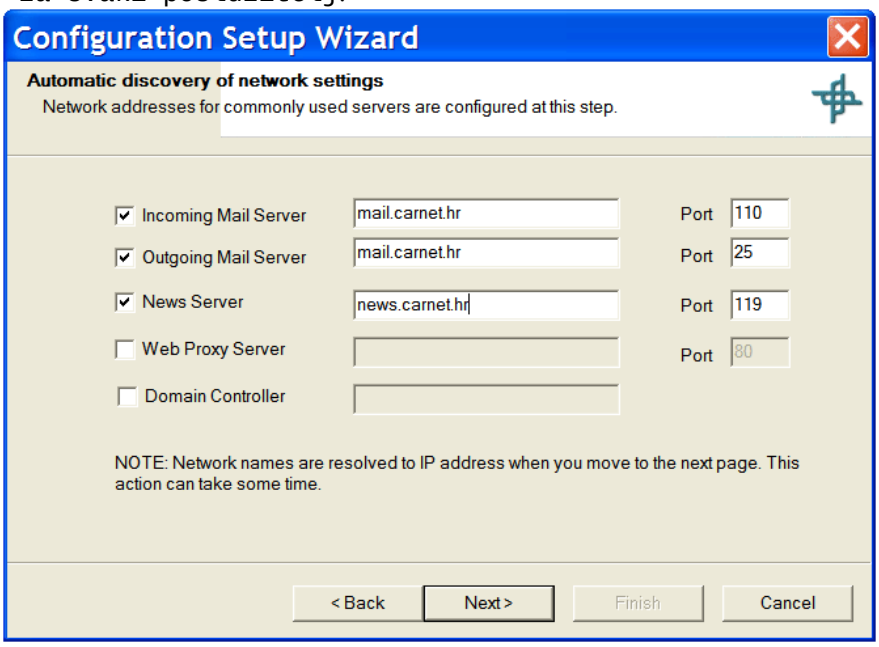
- `local network`,
- `broadcast`,
- `DNS Server #1`,
- `DNS Server #2`.



Slika 2: Automatsko otkrivanje mrežnih postavki (osnovno podešavanje)

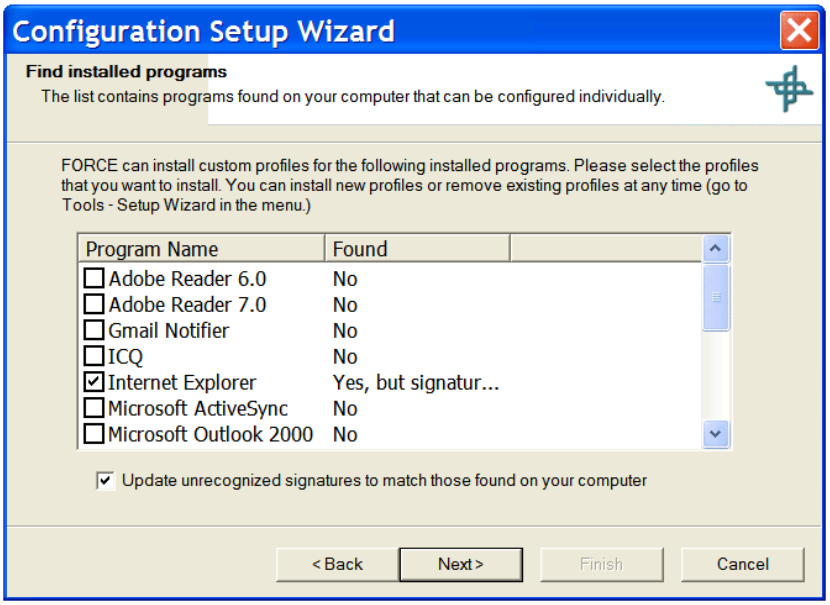
Na drugoj kartici upisuju se vrijednosti za najčešće korištene poslužitelje:

- `Incoming Mail Server`,
- `Outgoing Mail Server`,
- `News Server`,
- `Web Proxy Server`,
- `Domain Controller`,
- `port za svaki poslužitelj`.



Slika 3: Automatsko otkrivanje mrežnih postavki (uobičajeni poslužitelji)

Kartica *Find Installed Programs* prikazuje listu svih programskih proizvoda čije su sigurnosne postavke već predviđene u *Core Force*. Svaku od tih aplikacija, alat pokušava naći na računalu. Ako je nađe, u stupcu *Found* bit će označena. U slučaju da je program pronađen, ali njegov digitalni potpis nije u skladu s potpisom spremljenim u profilu, u stupcu *Found* javit će se poruka „*Yes, but signature is invalid*“. To znači da je instalirana drugačija inačica programa od navedene, da je instalirana sigurnosna zakrpa ili je neki zlonamjerni program modificirao aplikaciju. Popis pronađenih aplikacija prikazan je na slici Slika 4.

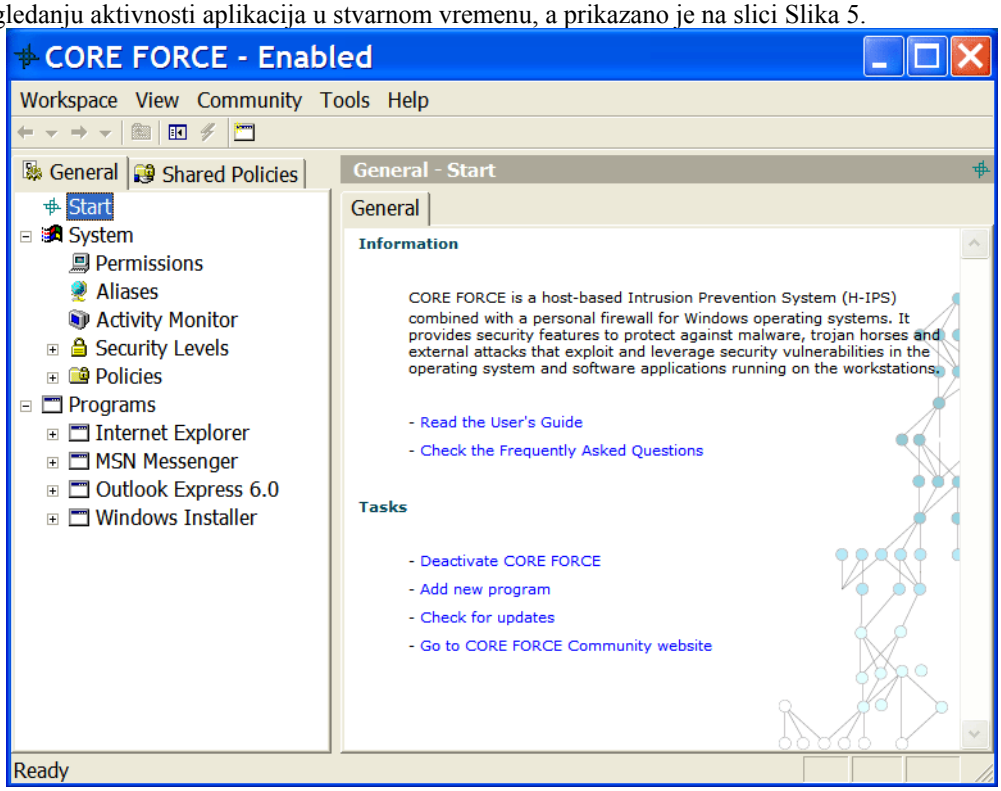


Slika 4: Popis programskih proizvoda sukladnih s alatom Core Force

Samo označene aplikacije su sukladne s podacima o njima koje ima alat. Međutim, naknadno se mogu dodati te ukloniti aplikacije po želji korisnika.
Nakon pritiska na gumb *Next*, profili će biti instalirani što može potrajati dulje vrijeme. Po završetku ovog procesa, završeno je i početno podešavanje alata.

4. Sučelje

Sučelje alata *Core Force* služi daljnjem podešavanju alata, promjeni postavki, pregledu zapisa i nadgledanju aktivnosti aplikacija u stvarnom vremenu, a prikazano je na slici Slika 5.



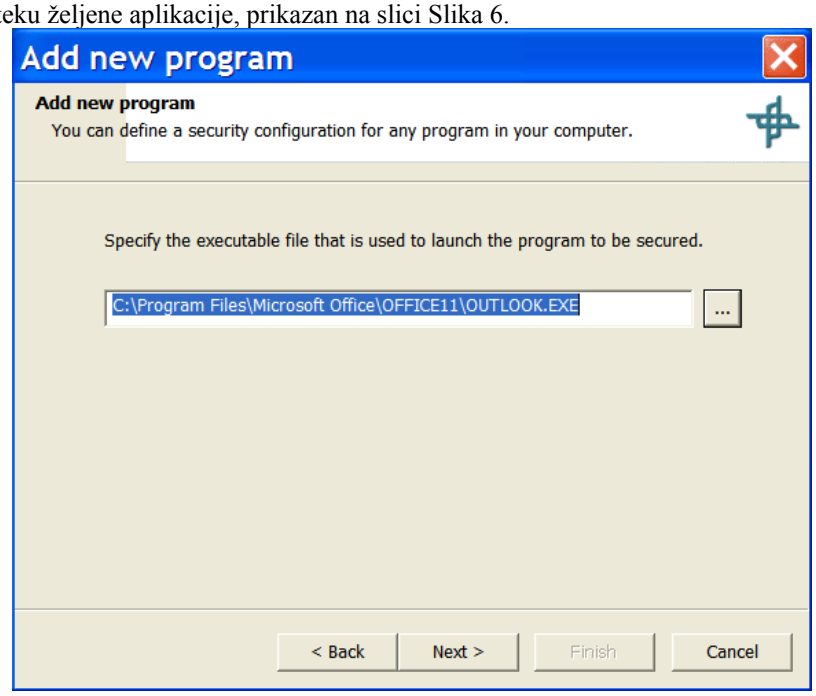
Slika 5: Sučelje alata Core Force

Na kartici *General* nalazi se radno sučelje koje omogućuje pristup sistemskom profilu te globalnim postavkama alata. Na kartici *Shared Policies* nalaze se grupirane dozvole pristupa koje omogućavaju konstrukciju profila za aplikacije.
Za podešavanje profila sustava i pojedinačnih aplikacija postoje definirani elementi koji su prikazani na slici Slika 5:

- `Launch control` – element je dostupan samo za pojedinačne aplikacije, a omogućuje određivanje lokacije izvršne datoteke aplikacije i dodavanje digitalnog potpisa,
- `Permissions` – prikazuje skup pravila definiranih za aplikaciju, uključujući sustav datoteka i pravila vatrozida,
- `Aliases` – element u kojem se definiraju mrežne postavke koje se koriste pri podešavanju pravila,
- `Activity Monitor` – omogućava praćenje aplikacija u realnom vremenu,
- `Security Levels` – prikazuje politike, lokalne i dijeljene, raspodijeljene po svakoj sigurnosnoj razini,
- `Security leves` – sadrži podelemente koji predstavljaju razine sigurnosti. Trenutno odabrana razina označena je ikonom kvačice, dok su ostale razine osjenčane.
- `Policies` – omogućava promjene pravila pristupa definiranih za svaku lokalnu politiku te kreiranje novih.

5. Korisničko podešavanje alata

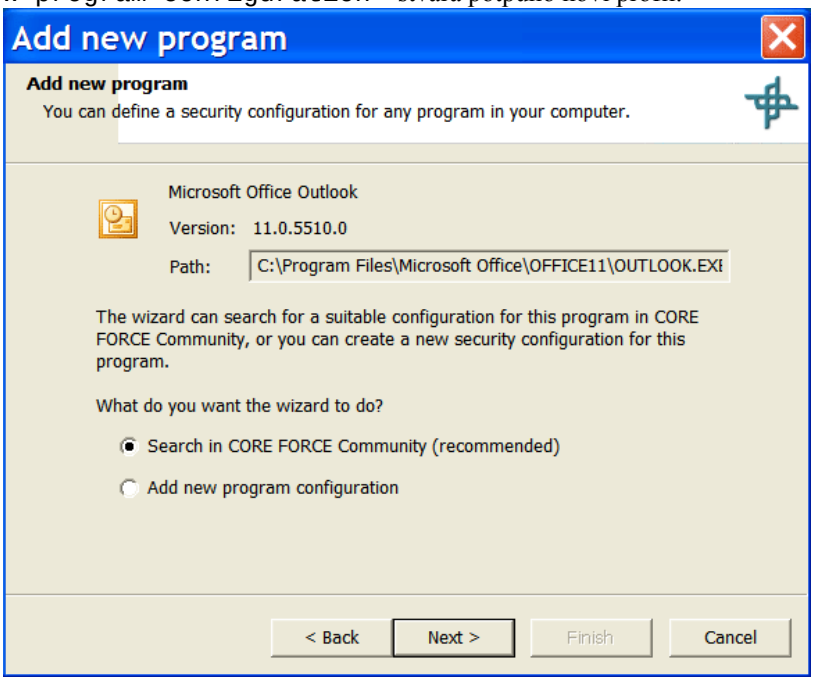
Osnovu rada ovog alata čini dodavanje novih aplikacija, odnosno stvaranje novog sigurnosnog profila. Postupak započinje desnim klikom na element *Programs* te odabirom naredbe `Add new program`. Odabirom navedene naredbe otvara se dijaloški okvir *Add new program* u kojem treba odabrati izvršnu datoteku željene aplikacije, prikazan na slici Slika 6.



Slika 6: Izbor izvršne datoteke nove aplikacije

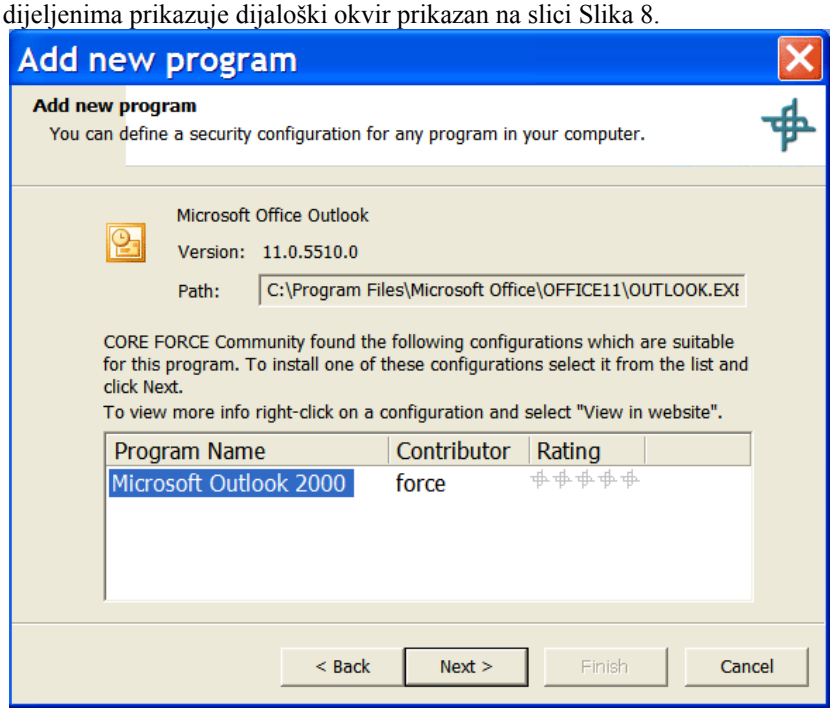
Slijedećim korakom korisnik odabire način stvaranja profila aplikacije između dvije ponuđene mogućnosti (Slika 7):

- `Search in Core Force Community (recommended)` – traži aplikaciju unutar postojećih profila alata koje su stvorili i pregledali ostali korisnici alata, a koje se mogu preuzeti s adrese http://force.coresecurity.com/index.php?module=forcecommunity.
- `Add new program configuration` – stvara potpuno novi profil.



Slika 7: Izbor kreiranja sigurnosnog profila

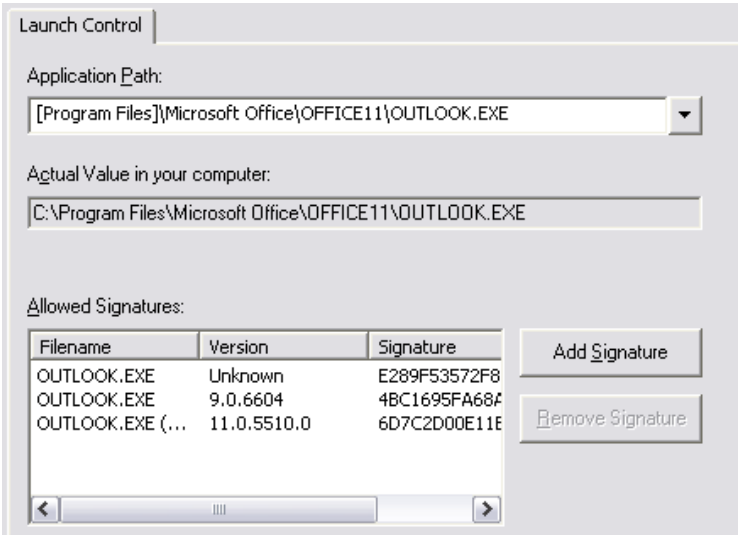
Ako je izabran prvi način stvaranja profila, alat pretražuje dijeljene profile. Ukoliko alat pronađe profil među dijeljenima prikazuje dijaloški okvir prikazan na slici Slika 8.



Slika 8: Prijedlog profila koji odgovara aplikaciji

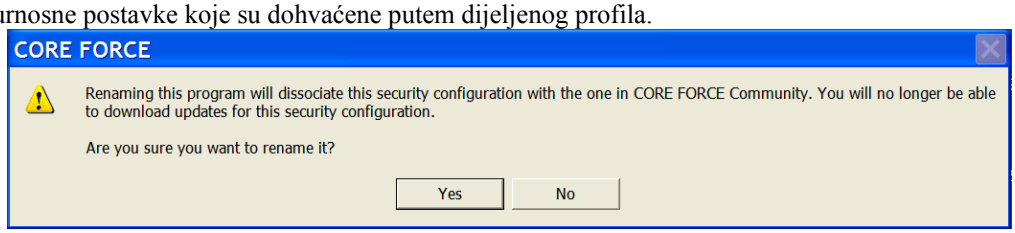
Odabrani profil, koji ne mora biti potpuno odgovarajući, se instalira nakon čega je omogućena daljna prilagodba profila. U gore ilustriranom primjeru dodavanja nove aplikacije, dodavao se Microsoft Outlook 2003, a predložen je profil za Microsoft Outlook 2000. Završetkom postupka dodavanja, pod elementom *Program* pojavljuje se nova stavka Microsoft Outlook 2000.
Za dodatno podešavanje novog profila treba podesiti njegove podelemente.
Opcija `Launch Control`, prikazana na slikama Slika 9 i Slika 10, omogućava pronalaženje putanje na računalu do željene aplikacije i omogućava dodavanje digitalnog potpisa te izvršne datoteke. Putanja se bira izborom naredbe `Browse` u polju `Application Path`. Digitalni potpis dodaje se naredbom `Add Signature` te izborom iste izvršne datoteke kao i kod izbora putanje.

Slika 9: *Launch Control* opcija novo dodane aplikacije



Slika 10: Detalji *Launch Control* kartice

Za preimenovanje aplikacije potrebno je desnom tipkom miša odabrati trenutni naziv aplikacije i naredbu *Rename*. Upozorenje prikazano na slici Slika 11 upozorava korisnika da će se poništiti sigurnosne postavke koje su dohvaćene putem dijeljenog profila.



Slika 11: Upozorenje prilikom preimenovanja profila preuzetog s Interneta

Prikazani način preuzimanja gotovog profila koji ne zadovoljava potrebe aplikacije koju korisnik želi dodati nije preporučljiv upravo zbog toga što prilikom promjena profila može doći do poništenja sigurnosnih mjera koje je postavio izvorni tvorac profila.
U slučaju da se među dijeljenim profilima ne nalazi identičan profil onome koji korisnik želi primijeniti, preporučuje se drugi način izrade profila.
Ako se odabere `Add new program configuration`, na slijedećem dijaloškom okviru treba upisati naziv aplikacije koji će se prikazivati u elementu `Programs`. Time dodavanje nove aplikacije završava, a započinje podešavanje pravila tj. sigurnosnog profila.

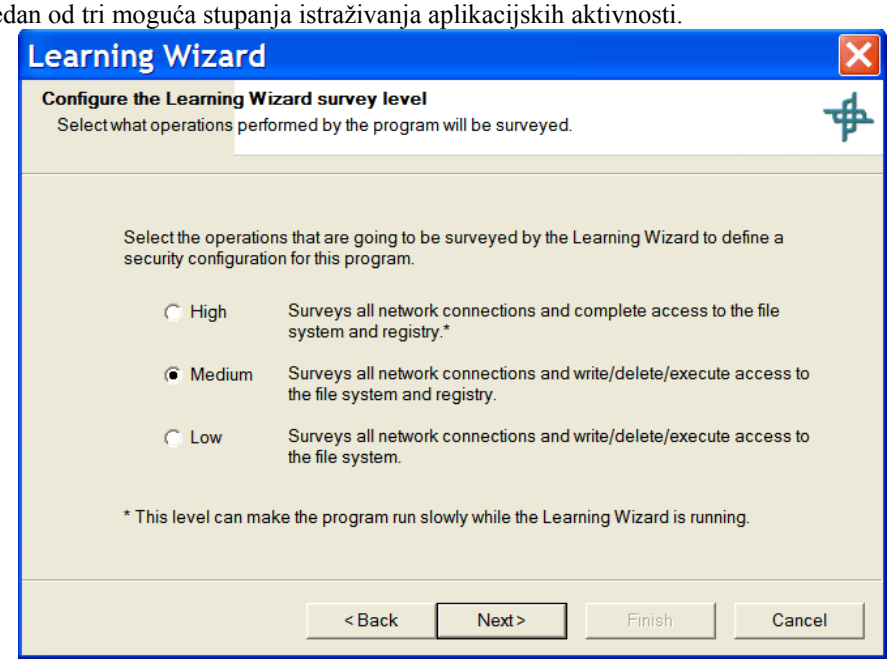
6. Podešavanje korisničkog sigurnosnog profila

Core Force alat ima dvije skupine pravila koja se primjenjuju na aplikacije koje štiti. Prvu skupinu čine sistemska predefinirana sigurnosna pravila (engl. *system default security permissions*) koja se primjenjuju ukoliko aplikacija nema posebno definirana pravila. Drugu skupinu čine upravo specifična sigurnosna pravila primjenjiva na određenu aplikaciju, pa se ona primjenjuju jer imaju višu razinu od sistemskih pravila (engl. *configuration for specific programs*).
Za podešavanje profila korisničke aplikacije (u ovom primjeru Microsoft Outlook 2003) poželjno je da korisnik dobro poznaje namjenu aplikacije i resurse koje aplikacija koristi pri svome radu.

6.1. Čarobnjak za snimanje aktivnosti aplikacije

Prije definiranja dozvola za korisničku aplikaciju, preporučljivo je ući u trag aktivnostima aplikacije. Za to se koristi čarobnjak ovog alata, jednostavnog imena *Learning Wizard*, koji će pomoći korisniku da snimi aktivnosti aplikacije u dnevnik (engl.*log files*) i na temelju tih aktivnosti postavi sigurnosna pravila za aplikaciju.
Čarobnjak se pokreće odabirom desne tipke miša na nazivu korisničke aplikacije koja se želi snimati te odabirom naredbe `Learning Wizard`. Prije pokretanja snimanja aktivnosti, aplikacija koja se

snima mora biti zatvorena. Korisniku se otvara dijaloški okvir, prikazan na slici Slika 12, u kojem se izabire jedan od tri moguća stupanja istraživanja aplikacijskih aktivnosti.

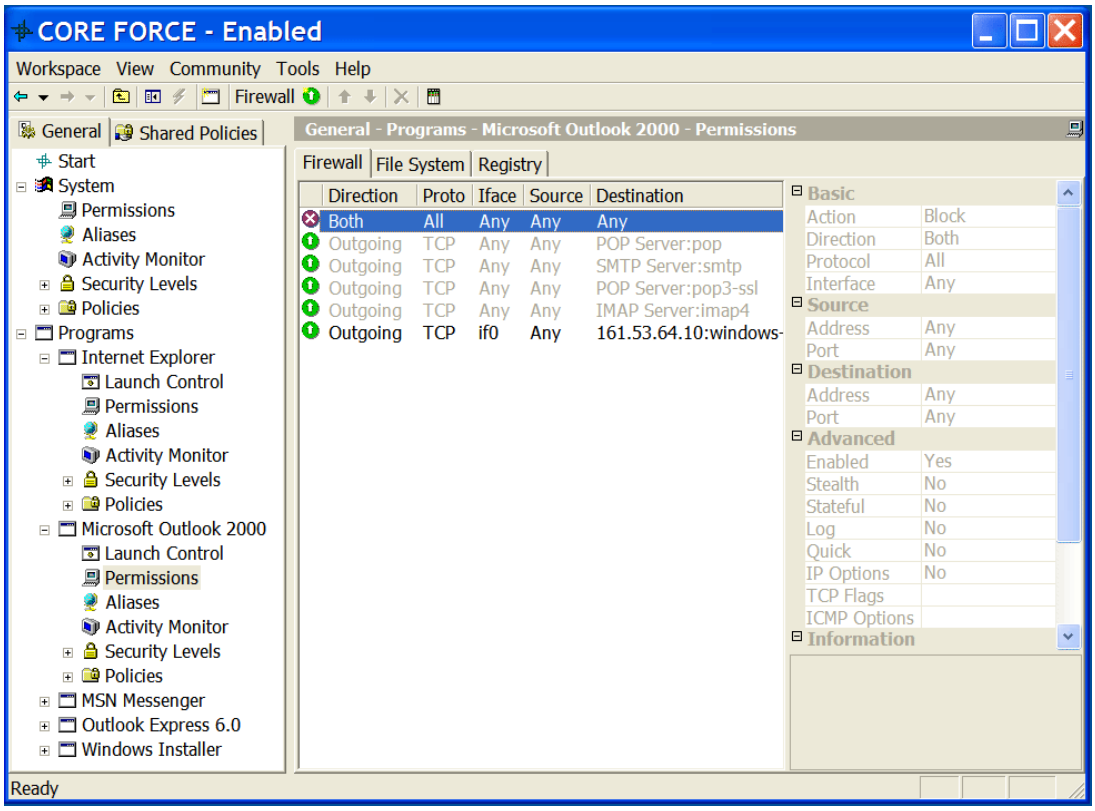


Slika 12: Izbor razine ispitivanja aplikacijskih aktivnosti

U slijedećem koraku pokreće se program čije će se aktivnosti pratiti. To je najjednostavnije pokrenuti odabirom na gumb `Run,` jer je izvršna datoteka aplikacije već ponuđena. Nakon pokretanja aplikacije korisnik treba što raznovrsnije koristiti razne mogućnosti aplikacije kako bi se snimilo što je moguće više aktivnosti. Međutim, treba se zadržati na standardnim mogućnostima alata, a ne provoditi akcije koje nisu svakodnevne ili uobičajene (npr. instalacija dodatnih mogućnosti aplikacije). Nakon nekoliko provedenih akcija, korisnik se vraća alatu *Core Force*, odnosno dijaloškom okviru *Learning Wizard* i pritiskom na gumbe `Next` i `Finish` završava proces snimanja aktivnosti.

Završavanjem procesa aktivnosti na kartici *Firewall* vidljiva su pravila koja su kreirana za one aktivnosti koje je korisnik izvodio tijekom snimanja. Pravila inače čine osnovu podešavanja ovog alata. Ona su osnovna konfiguracijska jedinica i mogu se definirati za mrežni resurs, datoteku ili objekt u *registry* datoteci.

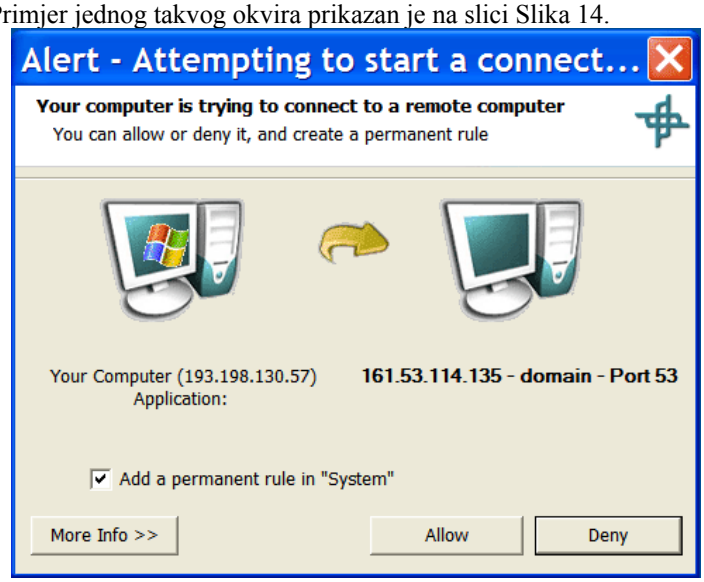
Rezultat snimanja pravila za Microsoft Outook 2003 aplikaciju prikazan je na slici Slika 13.



Slika 13: Kreirana pravila aplikacije nakon snimanja stanja

6.2. Dodavanje aktivnosti tijekom rada aplikacije

Ukoliko korisnik ne želi koristiti čarobnjak za snimanje aktivnosti aplikacije, drugi način dodavanja pravila jest dozvoljavanje aktivnosti u vrijeme njihova izvršavanja. Prilikom pokretanja korisničke aplikacije, a uz uvjet da je alat *Core Force* aktivan, javljaju se dijaloški okviri koji traže odobrenje za svaku aktivnost. Primjer jednog takvog okvira prikazan je na slici Slika 14.



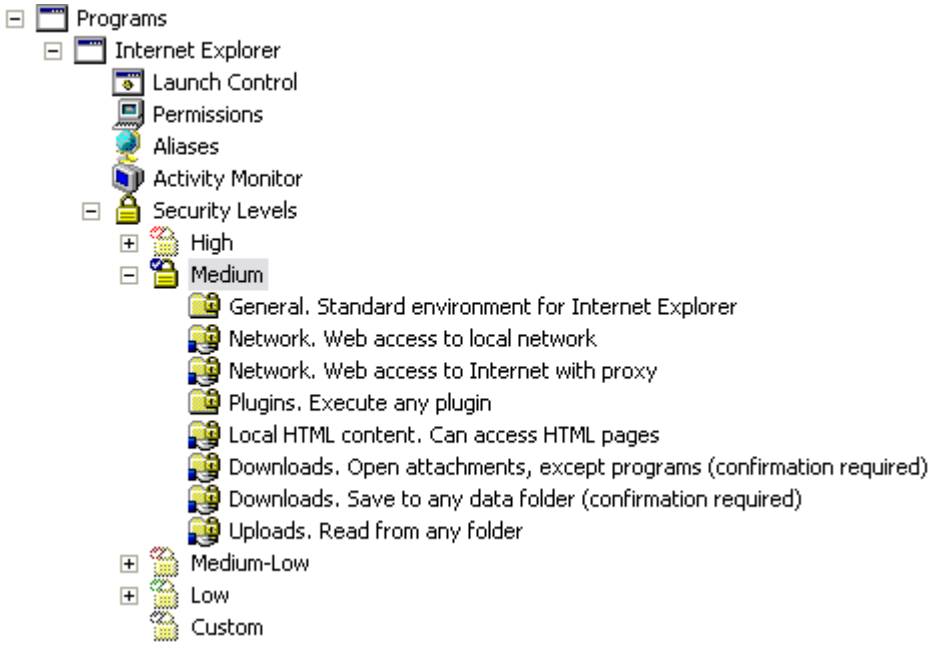
Slika 14: Dijaloški okvir za odobrenje aktivnosti u realnom vremenu

Da bi se pravilo dodalo u profil ove aplikacije potrebno je uključiti opciju *Add a permanent rule in „Microsoft Office Outlook 2003“* te kliknuti gumb `Allow`.

7. Definiranje sigurnosnih razina i politika

7.1. Predefinirane politike

Već je spomenuto da osnovu podešavanja alata čini pravilo koje se može definirati za mrežni resurs, datoteku ili objekt u *registry* datoteci. Ova razina definiranja pravila omogućuje vrlo detaljan okvir ostvarivanja sigurnosti aplikacija. Međutim, detaljno podešavanje pravila nije uvijek pogodno. Iz tog razloga moguće je definirati skupinu pravila koji se nazivaju politike (engl. *policies*).
Svaki sigurnosni profil može imati vlastitu kolekciju definiranih politika. Slika 15 prikazuje politike za aplikaciju Internet Explorer, a koje dolaze s alatom.



Slika 15: Politike definirane za aplikaciju Internet Explorer

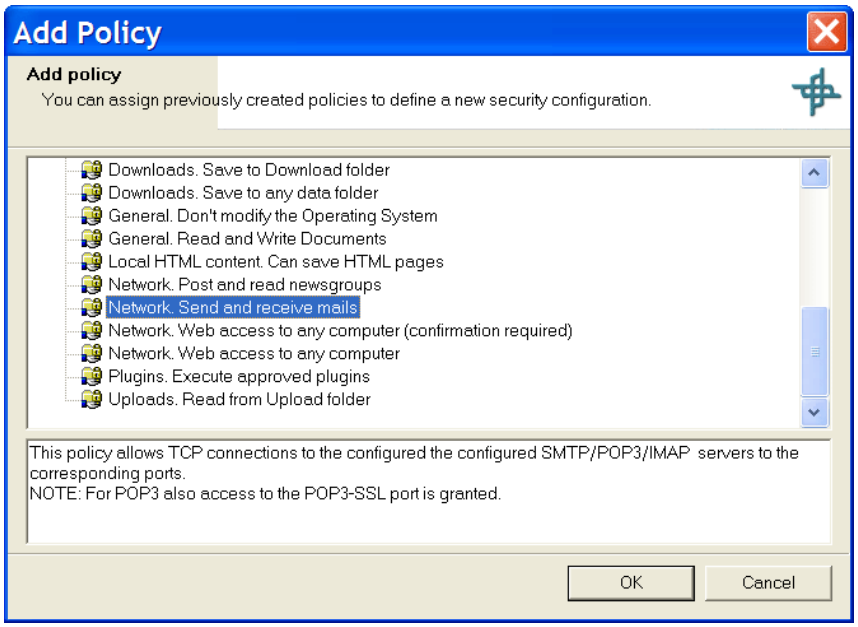
7.2. Sigurnosne razine

Za svaku aplikacija određuje se sigurnosna razina. To može biti:

- `High`,
- `Medium`,
- `Medium-low`,
- `Low` i
- `Custom`.

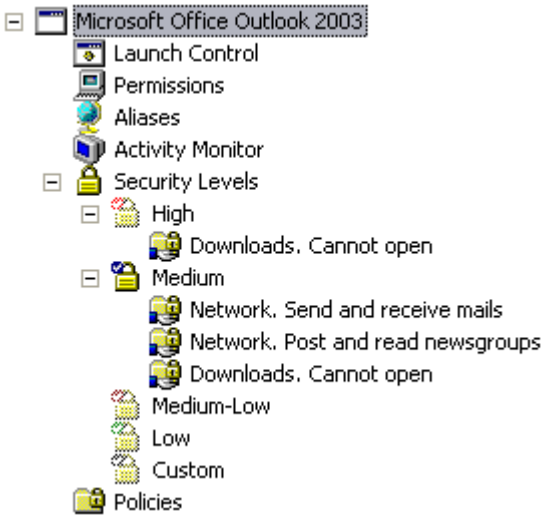
Kod korisničkog dodavanja aplikacija sigurnosne razine nisu korisnički definirane. Pregledom bilo koje od navedenih sigurnosnih razina, vidljivo je da nisu definirana pravila.
Prilagođavanje sigurnosnih razina odvija se u slijedećim koracima:

1. Odabrati aplikaciju za koju se žele definirati sigurnosne razine.
2. Odabrati podelement `Security Levels` te odabrati sigurnosnu razinu koja se želi modificirati.
3. Odabrati naredbu `Add policy` kako bi se dodala nova politika pri čemu će se pojaviti dijaloški okvir *Add policies* Wizard.
4. U okviru je potrebno odabrati dijeljene politike (engl. *shared policies*) kako bi se politike dodale pripadajućoj razini sigurnosti.



Slika 16: Dodavanje politika sigurnosnoj razini korisničke aplikacije

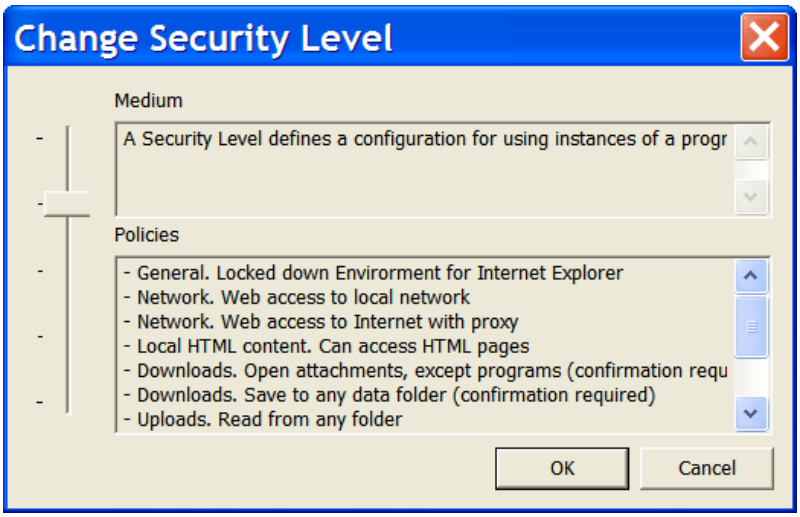
Rezultat dodanih politika vidljiv je na slici Slika 17.



Slika 17: Novo dodane politike za aplikaciju Microsoft Outlook 2003

Trenutno aktivna sigurnosna razina aplikacije vidljiva je u podelementu *Security Levels*. Kvačicom označena razina je aktivna, a ostale razine su zasjenčane. Promjena sigurnosne razine provodi se u slijedećim koracima:

1. Odabrati desnom tipkom miša aplikaciju kojoj se mijenja aktivna sigurnosna razina te odabrati naredbu `Change Security Level`. Otvara se dijaloški okvir prikazan na slici Slika 18.
2. Pomoću klizne trake odabrati željenu razinu i pritisnuti gumb `OK`.



Slika 18: Promjena sigurnosne razine

U primjeru su dodana pravila za sigurnosnu razinu *Medium* u kojem su definirane politike za primanje i slanje poruka elektroničke pošte, čitanje i slanje poruka na grupe te zabrana otvaranja priloženih datoteka.

Svaka od dodanih politika može se jednostavno obrisati tako da se desnom tipkom miša odabere politika, a zatim naredba `Remove Policy`. Ukoliko se politika želi zadržati u sigurnosnoj razini, ali se privremeno želi deaktivirati tada je potrebno desnom tipkom miša odabrati politiku i zatim naredbu `Disable`. Ponovno aktiviranje provodi se na identičan način, ali korištenjem naredbe `Enable`.

8. Zaključak

Alat Core Force izuzetno je dobar za primjenu na osobnim računalima. Iako je podešavanje alata dugotrajno te iziskuje srednje ili napredno poznavanje korisničkih aplikacija, nakon završetka tog postupka korisnik ima alat koji mu omogućava odgovarajuću razinu zaštite. U ovom dokumentu opisane su osnovne mogućnosti programa. Korisnicima je na raspolaganju i korisnički priručnik koji vrlo detaljno opisuje i ostale mogućnosti alata.

9. Reference

1. Core Force alat
   http://force.coresecurity.com/index.php?module=base&page=download
2. Upute za korisnike
   http://force.coresecurity.com/download/CoreForceUserGuide.pdf
3. Postojeći profili aplikacija
   http://force.coresecurity.com/index.php?module=forcecommunity