



UNIVERZITET U NOVOM SADU
FAKULTET TEHNIČKIH NAUKA
NOVI SAD



Grupa 13

Mario Klišanić PR15/2015

Dalibor Oletić PR39/2015

Mirko Milutin PR76/2015

Strahinja Šerbula PR138/2015

Zadatak 17

Sigurnost i bezbednost u elektroenergetskim
sistemima

- Primenjeno softversko inženjerstvo -

Novi Sad, 9.11.2018.

Sadržaj

1. OPIS REŠAVANOG PROBLEMA.....	3
2. TEORIJSKE OSNOVE.....	4
3. DIZAJN IMPLEMENTIRANOG SISTEMA.....	5
4. TESTIRANJE SISTEMA	6

1. OPIS REŠAVANOG PROBLEMA

Implementirati antivirus servisa koji za zadatak ima detekciju izvršavanja nedozvoljenih procesa. Antivirus ima listu zabranjenih procesa i periodično se pali i proverava da li u listi trenutno aktivnih procesa postoji nedozvoljeni proces. Nakon detekcije takvog procesa potrebno je da antivirus obavesti Intrusion Detection System. AV i IDS komuniciraju preko sertifikata.

Intrusion Detection System ima za zadatak da određuje nivo kritičnosti zabranjenog procesa. Nivo kritičnosti se određuje na osnovu broja detekcija. Tri nivoa kritičnosti koje je potrebno obezbediti su: Information (jedna ili dve detekcije), Warning (tri ili četiri detekcije) i Critical (pet ili više puta). Procene sa nivoom Critical, treba logovati.

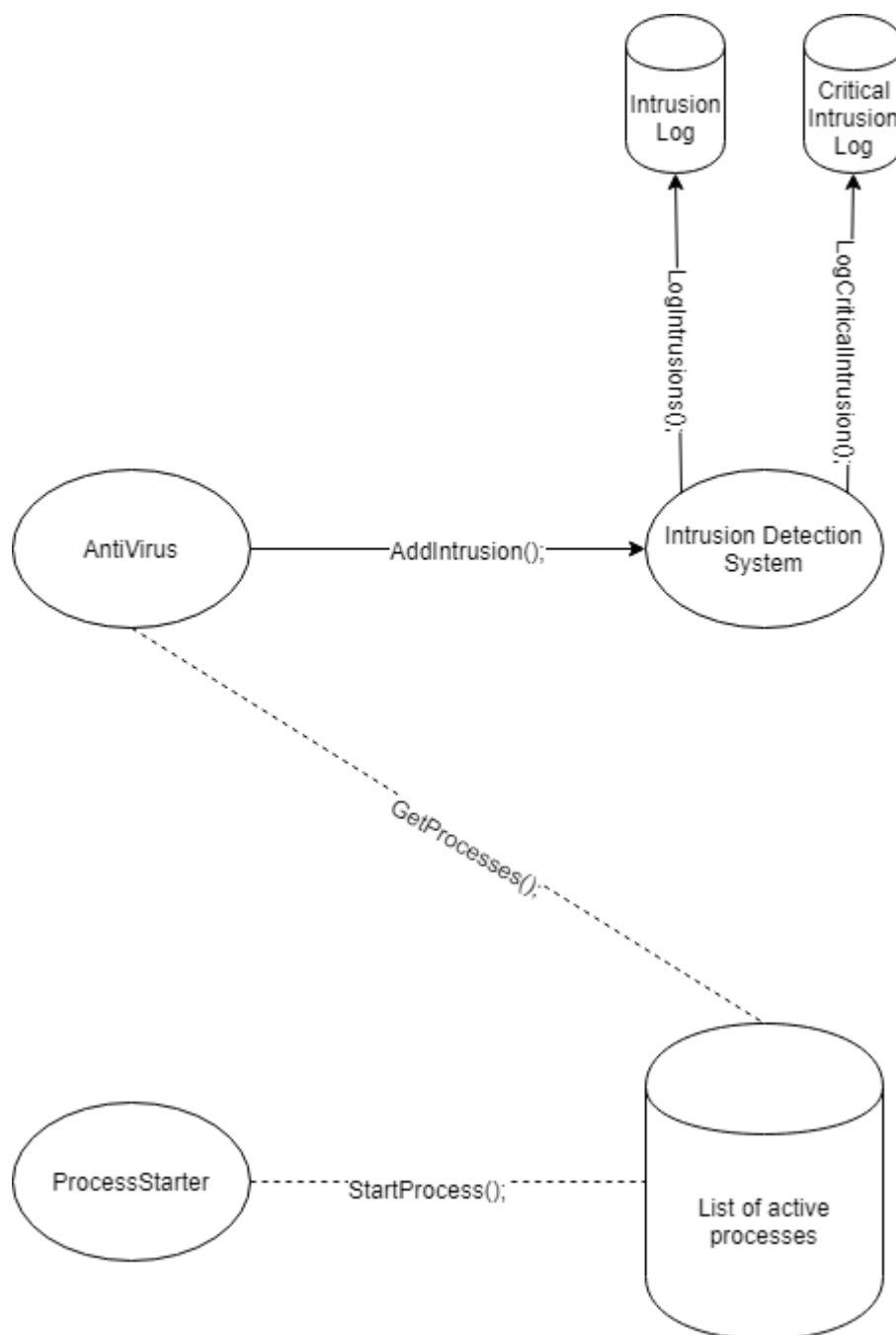
Konačno potrebno je obezbediti proveru integriteta antivirus konfiguracije na zahtev. Konfiguracioni fajl je dozvoljeno menjati isključivo pozivom odgovarajuće metode Antivirus Servisa. Ručne izmene fajla se smatraju neovlašćenim.

2. TEORIJSKE OSNOVE

Sertifikat predstavlja digitalni identitet korisnika izdat od strane sertifikacionih tela (certification authority, CA). Sertifikat sadrži različite podatke: podaci o vlasniku sertifikata (Subject), validnost odnosno period važenja sertifikata (ValidFrom, ValidTo), informacije o izdavaocu sertifikata (Issuer). U sertifikat se ugrađuje javni ključ korisnika (uz identifikator algoritma primenjenog za generisanje ključa, npr. RSA), dok se tajni ključ ne razmenjuje.

Svaki sertifikat je digitalno potpisan od strane sertifikacionog tela koje ga izdaje čime se potvrđuje da sertifikat zaista pripada podnosiocu zahteva. Na ovaj način je takođe moguće detektovati izmene u okviru samog sertifikata jer digitalni potpis obezbeđuje integritet podataka.

3. DIZAJN IMPLEMENTIRANOG SISTEMA



Implementacija se sastoji od tri konzolne aplikacije AntiVirus, IntrusionDetectionSystem i ProcessStarter.

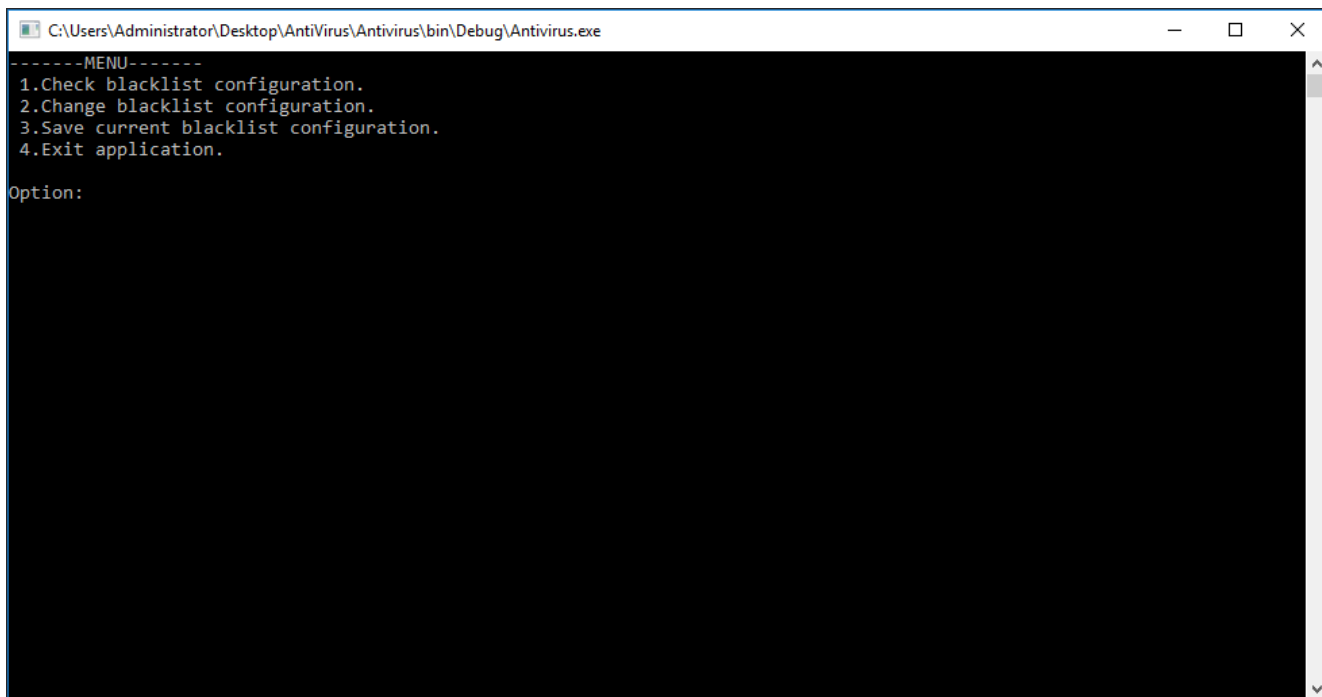
AntiVirus periodično proverava sve aktivne procese i upoređuje ih sa blacklist-om procesa. Ukoliko se proces nalazi na blacklist-i, intruzija se obrađuje i šalje se IntrusionDetectionSystem-u. Prilikom obrade intruzije AntiVirus proverava ime procesa, korisnika koji je započeo proces i vreme kada je proces aktivan. Takođe AV nudi proveru integriteta konfiguracionog fajla i izmenu konfiguracionog fajla. Integritet se proverava hash code-om.

IntrusionDetectionSystem prihvata intruzije od Antivirusa i svaku intruziju loguje. Pri svakom prihvatanju intruzije proverava se broj detekcije svake intruzije i menja se nivo kritičnosti. Ukoliko je nivo kritičnosti Critical, proces se loguje u CriticalIntrusionLog.

ProcessStarter aplikacija omogućava preko jednostavnog menija pokretanje nekoliko različitih procesa od strane nekoliko različitih korisnika. Pri pokretanju ProcessStarter-a pravimo četiri test user-a (Mario, Dalibor, Mirko i Strahinja). U toku gašenja aplikacije test korisnici se brišu. Pokretani procesi su jednosavni windows procesi (Notepad, Paint, Google Chrome, Mozilla Firefox).

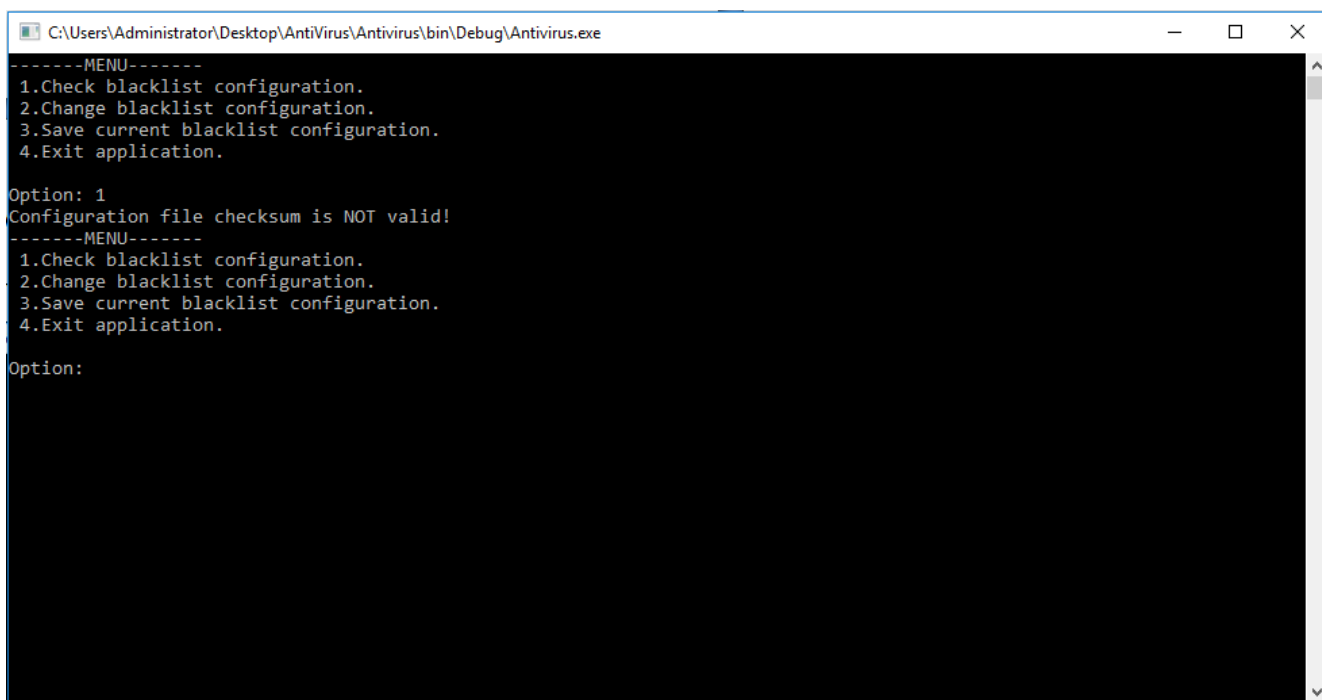
4. TESTIRANJE SISTEMA

Nakon pokretanja AntiVirus-a otvara se meni sa sledecim opcijama:

A screenshot of a Windows command prompt window titled "C:\Users\Administrator\Desktop\AntiVirus\Antivirus\bin\Debug\Antivirus.exe". The window displays a menu with four options: 1. Check blacklist configuration, 2. Change blacklist configuration, 3. Save current blacklist configuration, and 4. Exit application. Below the menu, the prompt "Option:" is visible, indicating the user is expected to enter a choice.

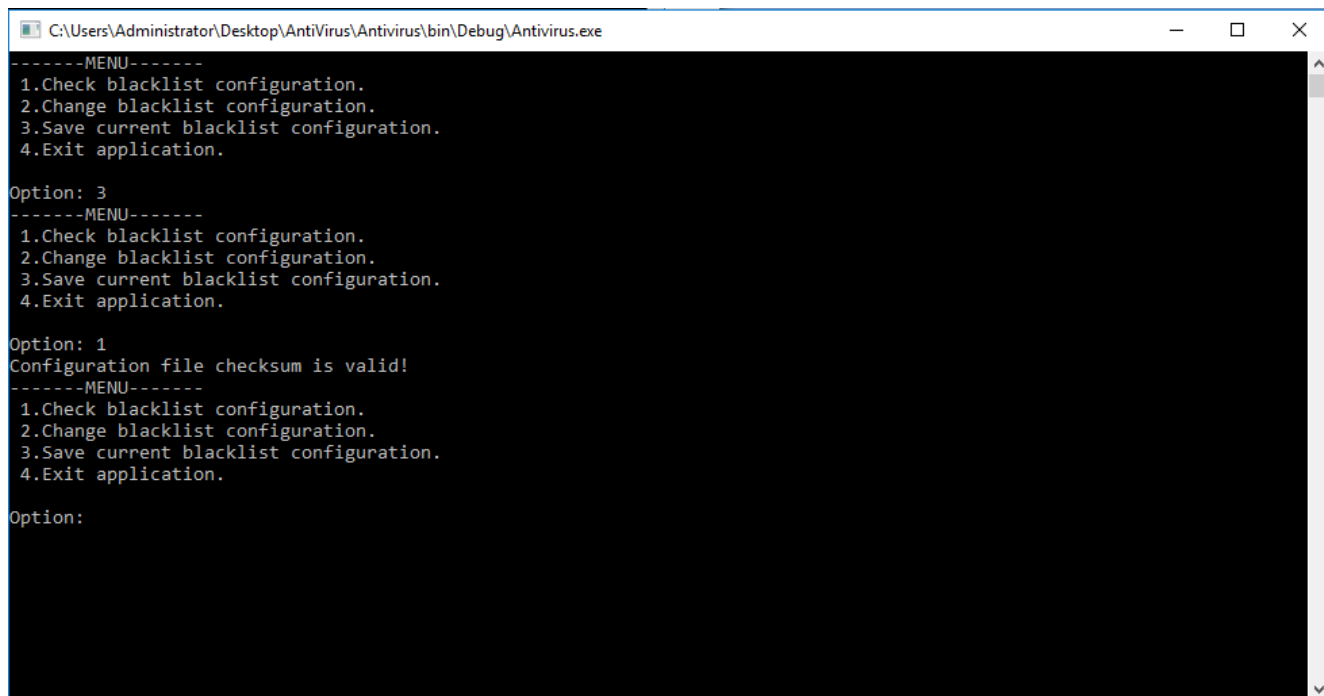
```
C:\Users\Administrator\Desktop\AntiVirus\Antivirus\bin\Debug\Antivirus.exe
-----MENU-----
1.Check blacklist configuration.
2.Change blacklist configuration.
3.Save current blacklist configuration.
4.Exit application.
Option:
```

Ukoliko proverimo konfiguraciju pre prvog čuvanja konfiguracije program javlja da nije validna.

A screenshot of the same AntiVirus application window. This time, option 1 has been selected, and the program has displayed an error message: "Configuration file checksum is NOT valid!". The menu is shown again, and the "Option:" prompt is at the bottom, ready for the next input.

```
C:\Users\Administrator\Desktop\AntiVirus\Antivirus\bin\Debug\Antivirus.exe
-----MENU-----
1.Check blacklist configuration.
2.Change blacklist configuration.
3.Save current blacklist configuration.
4.Exit application.
Option: 1
Configuration file checksum is NOT valid!
-----MENU-----
1.Check blacklist configuration.
2.Change blacklist configuration.
3.Save current blacklist configuration.
4.Exit application.
Option:
```

Nakon čuvanja trenutne konfiguracije, proverom dobijamo obaveštenje da je konfiguracija validna.



```
C:\Users\Administrator\Desktop\AntiVirus\Antivirus\bin\Debug\Antivirus.exe
-----MENU-----
1.Check blacklist configuration.
2.Change blacklist configuration.
3.Save current blacklist configuration.
4.Exit application.

Option: 3
-----MENU-----
1.Check blacklist configuration.
2.Change blacklist configuration.
3.Save current blacklist configuration.
4.Exit application.

Option: 1
Configuration file checksum is valid!
-----MENU-----
1.Check blacklist configuration.
2.Change blacklist configuration.
3.Save current blacklist configuration.
4.Exit application.

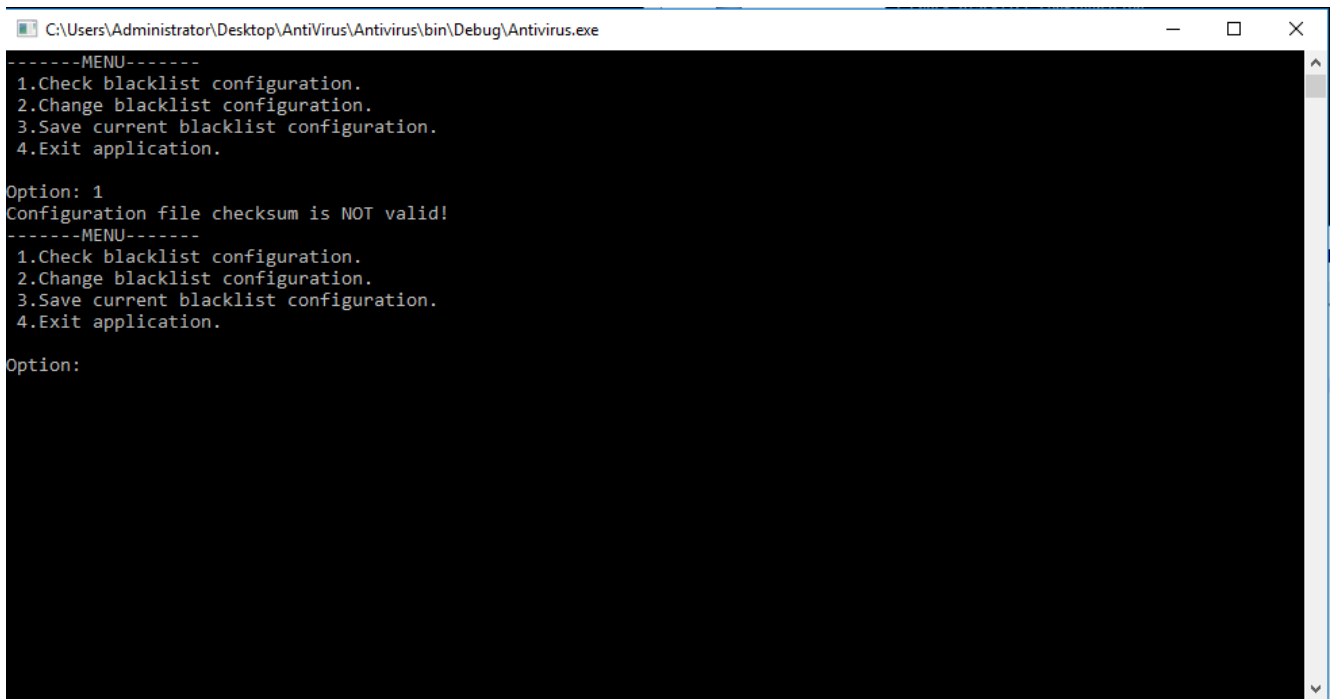
Option:
```

Ukoliko ručno izmenimo konfiguraciju:



```
1 {
2   {
3     "name": "Shavast",
4     "user": "Strahinja",
5     "startHours": "10",
6     "startMinutes": "30",
7     "endHours": "4",
8     "endMinutes": "23"
9   },
10 },
11 {
12   "name": "DhotoShop",
13   "user": "Dalibor",
14   "startHours": "3",
15   "startMinutes": "30",
16   "endHours": "20",
17   "endMinutes": "23"
18 },
19 },
20 {
21   "name": "notepad",
22   "user": "Mario",
23   "startHours": "13",
24   "startMinutes": "0",
25   "endHours": "19",
26   "endMinutes": "0"
27 }
28 ,{"user": "Mario", "name": "Mario", "startHours": 13, "startMinutes": 13, "endHours": 18, "endMinutes": 18}, {"user": "asfsa", "name": "asfsa"
```

Program javlja nevalidnu konfiguraciju.



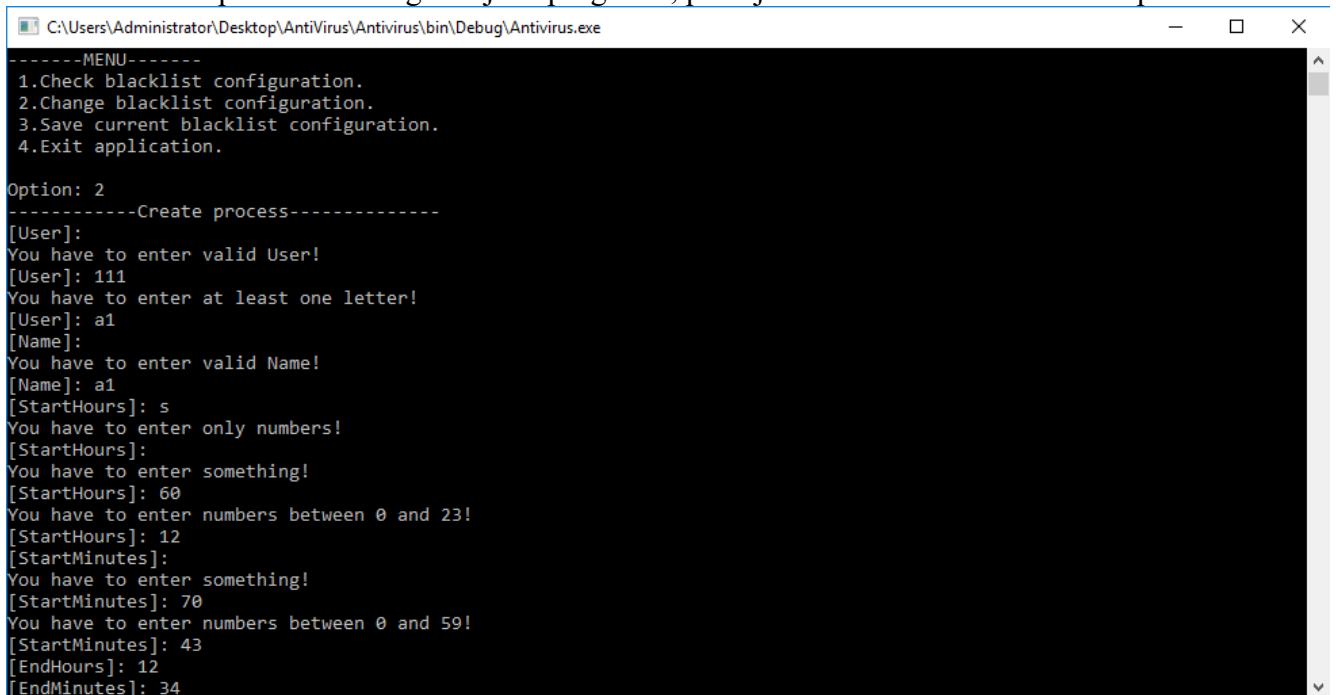
The screenshot shows a Windows application window titled "C:\Users\Administrator\Desktop\AntiVirus\Antivirus\bin\Debug\Antivirus.exe". The application displays a menu with four options: 1. Check blacklist configuration, 2. Change blacklist configuration, 3. Save current blacklist configuration, and 4. Exit application. The user has selected option 1, and the application displays the message "Configuration file checksum is NOT valid!". The menu is repeated below the message.

```
-----MENU-----
1.Check blacklist configuration.
2.Change blacklist configuration.
3.Save current blacklist configuration.
4.Exit application.

Option: 1
Configuration file checksum is NOT valid!
-----MENU-----
1.Check blacklist configuration.
2.Change blacklist configuration.
3.Save current blacklist configuration.
4.Exit application.

Option:
```

Prilikom promene konfiguracije iz programa, postoji zaštita od unosa nevalidnih podataka.



The screenshot shows the same application window, but now the user has selected option 2, "Change blacklist configuration". The application prompts the user to enter a valid User, Name, StartHours, StartMinutes, and EndHours. Each input is validated, and the user is prompted to enter a valid value if the current input is invalid. The user enters "111" for User, "a1" for Name, "s" for StartHours, "60" for StartMinutes, "12" for EndHours, and "34" for EndMinutes.

```
-----MENU-----
1.Check blacklist configuration.
2.Change blacklist configuration.
3.Save current blacklist configuration.
4.Exit application.

Option: 2
-----Create process-----
[User]:
You have to enter valid User!
[User]: 111
You have to enter at least one letter!
[User]: a1
[Name]:
You have to enter valid Name!
[Name]: a1
[StartHours]: s
You have to enter only numbers!
[StartHours]:
You have to enter something!
[StartHours]: 60
You have to enter numbers between 0 and 23!
[StartHours]: 12
[StartMinutes]:
You have to enter something!
[StartMinutes]: 70
You have to enter numbers between 0 and 59!
[StartMinutes]: 43
[EndHours]: 12
[EndMinutes]: 34
```

AntiVirus u pozadini pronalazi i šalje nevalidne procese.

Pri pokretanju IntrusionDetectionSystema program javlja da je pokrenuo servis.

```
C:\Users\Administrator\Desktop\AntiVirus\MDMS.IntrusionDetectionSystem\bin\Debug\MDMS.IntrusionDetectionSystem.exe
IntrusionService service is started.
Press <enter> to stop service...
```

IDS od AV-a prima intruzije i loguje ih.

```
C:\Users\Administrator\Desktop\AntiVirus\MDMS.IntrusionDetectionSystem\bin\Debug\MDMS.IntrusionDetectionSystem.exe
IntrusionService service is started.
Press <enter> to stop service...
2018-11-08 17:06:31,070 INFO [5] IntrusionService P05-03\Dalibor - Adding intrusions to file.
2018-11-08 17:06:31,180 INFO [5] IntrusionService P05-03\Dalibor - Logging critical intrusions.
2018-11-08 17:06:31,226 INFO [5] IEnumerableExtensions P05-03\Dalibor - No critical intrusions.
2018-11-08 17:06:34,258 INFO [6] IntrusionService P05-03\Dalibor - Adding intrusions to file.
2018-11-08 17:06:34,274 INFO [6] IntrusionService P05-03\Dalibor - Logging critical intrusions.
2018-11-08 17:06:34,274 INFO [6] IEnumerableExtensions P05-03\Dalibor - No critical intrusions.
2018-11-08 17:06:37,299 INFO [5] IntrusionService P05-03\Dalibor - Adding intrusions to file.
2018-11-08 17:06:37,299 INFO [5] IntrusionService P05-03\Dalibor - Logging critical intrusions.
2018-11-08 17:06:37,299 INFO [5] IEnumerableExtensions P05-03\Dalibor - No critical intrusions.
2018-11-08 17:06:40,333 INFO [6] IntrusionService P05-03\Dalibor - Adding intrusions to file.
2018-11-08 17:06:40,365 INFO [6] IntrusionService P05-03\Dalibor - Logging critical intrusions.
2018-11-08 17:06:40,380 INFO [6] IEnumerableExtensions P05-03\Dalibor - No critical intrusions.
2018-11-08 17:06:43,389 INFO [7] IntrusionService P05-03\Dalibor - Adding intrusions to file.
2018-11-08 17:06:43,404 INFO [7] IntrusionService P05-03\Dalibor - Logging critical intrusions.
2018-11-08 17:06:43,404 INFO [7] IEnumerableExtensions P05-03\Dalibor - Critical: Name:notepad, User:Mario, Count:5
2018-11-08 17:06:46,426 INFO [6] IntrusionService P05-03\Dalibor - Adding intrusions to file.
2018-11-08 17:06:46,442 INFO [6] IntrusionService P05-03\Dalibor - Logging critical intrusions.
2018-11-08 17:06:46,442 INFO [6] IEnumerableExtensions P05-03\Dalibor - Critical: Name:notepad, User:Mario, Count:6
2018-11-08 17:06:49,461 INFO [6] IntrusionService P05-03\Dalibor - Adding intrusions to file.
2018-11-08 17:06:49,477 INFO [6] IntrusionService P05-03\Dalibor - Logging critical intrusions.
2018-11-08 17:06:49,477 INFO [6] IEnumerableExtensions P05-03\Dalibor - Critical: Name:notepad, User:Mario, Count:7
```