Osnove informacione bezbednosti u infrastrukturnim sistemima

Projektni zadatak 22

Članovi tima:

Luka Đelić PR60/2020

Stefan Malinović PR62/2020

Stefan Milovanović PR68/2020

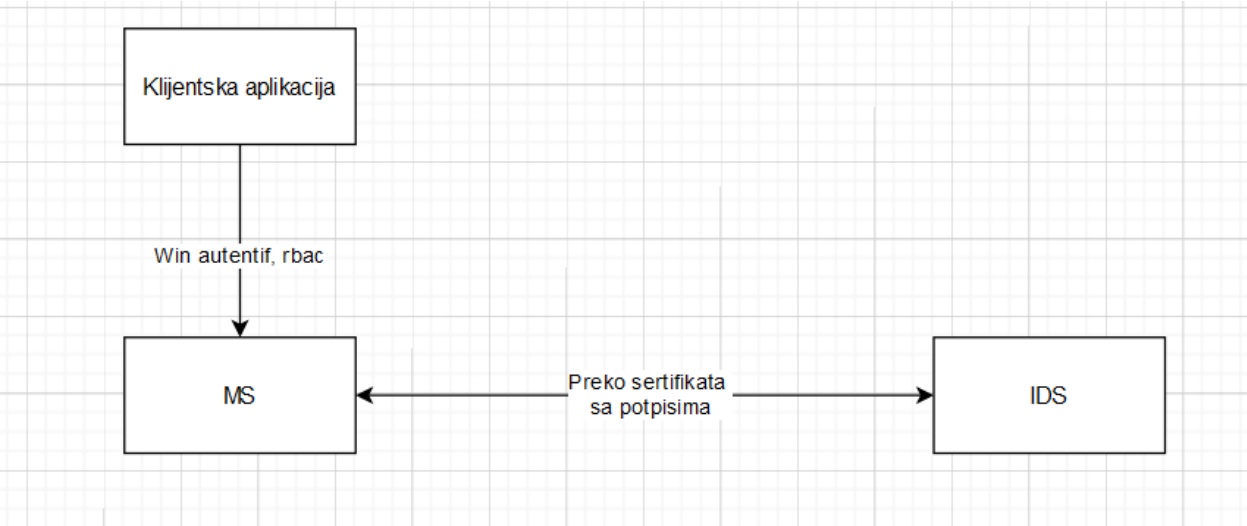
Srđan Mlađenović PR72/2020

Asistent:

Zorana Babić

Opis sistema

Malware Scanning alat je sistem koji služi za proveravanje dozvoljenih procesa među trenutno aktivnim. Aktivira se periodično i proverava procese na osnovu konfiguracije sa nedozvoljenim procesima. Ukoliko naiđe na takav proces šalje alarm Intrusion Detection System komponenti koja loguje kritične događaje. Postoji i posebna komponenta klijent koja služi za izmenu konfiguracije.

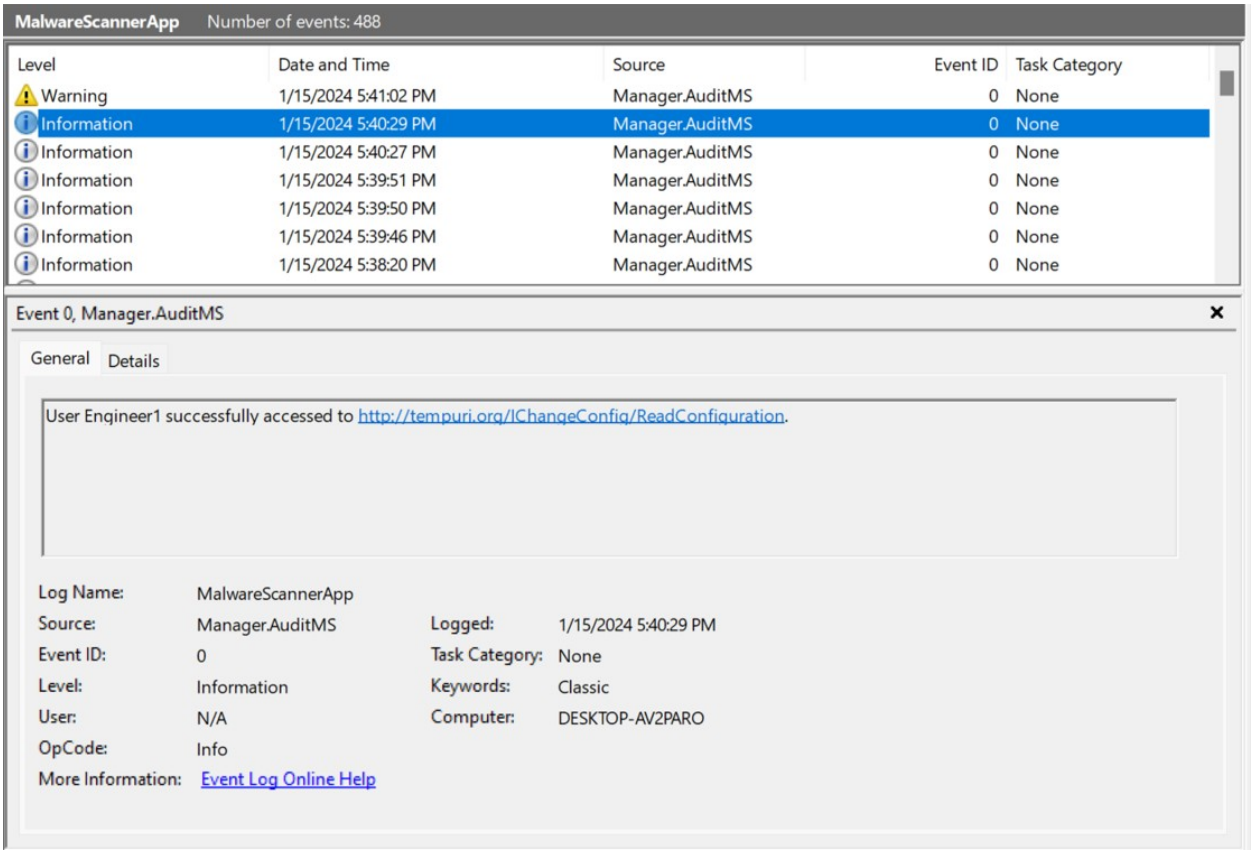


Opis komponenti

Malware scanning

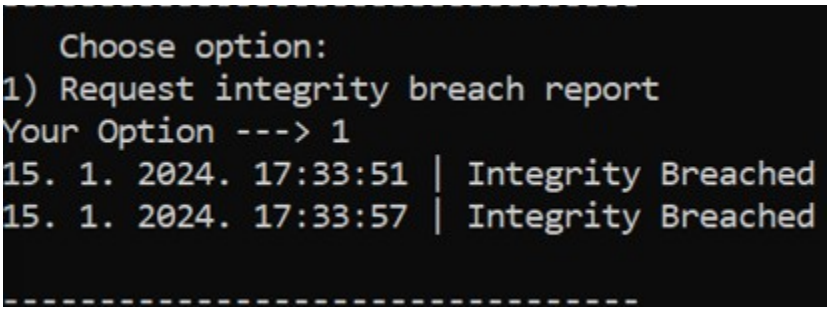
Malware Scanning (MS) servis je glavna komponenta sistema. Komunicira sa klijentskom aplikacijom kao server i sa IDS komponentom kao klijent. Služi za praćenje procesa aktiviranjem na svakih N sekundi. Ukoliko naiđe na nedozvoljeni proces automatski šalje alarm IDS-u. Da bi se za početak započela komunikacija između ove dve komponente potrebno je da imaju instalirane sertifikate, konkretno "wcfclient" i "wcfservice" sertifikate.

MS je zadužen da i sam loguje kritične događaje u svojoj log datoteci u Windows Event Log.



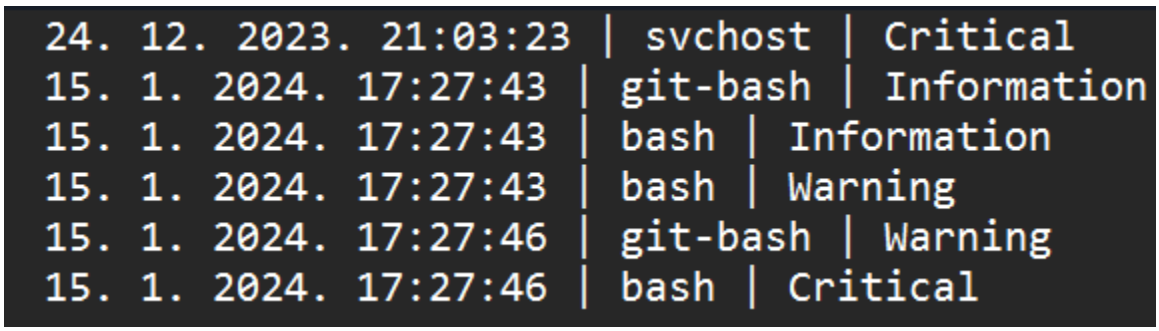
Dodatno, da bi IDS prihvatio poruku potrebno je da on sadrži i digitalni potpis kojim se obezbeđuje integritet i autentičnost poruke, kao i neporecivost od strane pošiljaoca da je upravo on poslao poruku. Naime, digitalni potpis predstavlja hash vrednost izračunatu nad sadržajem poruke koja se zatim kriptuje privatnim ključem pošiljaoca. Primalac poruke, dekriptovanjem digitalnog potpisa javnim ključem pošiljaoca potvrđuje autentičnost poruke, jer samo pošiljalac ima odgovarajući privatni ključ. Ovim je istovremeno omogućeno da pošiljalac neće moći da porekne da je on poslao poruku.

Sa MS-a se može tražiti i provera integriteta log fajla koju proverava IDS:



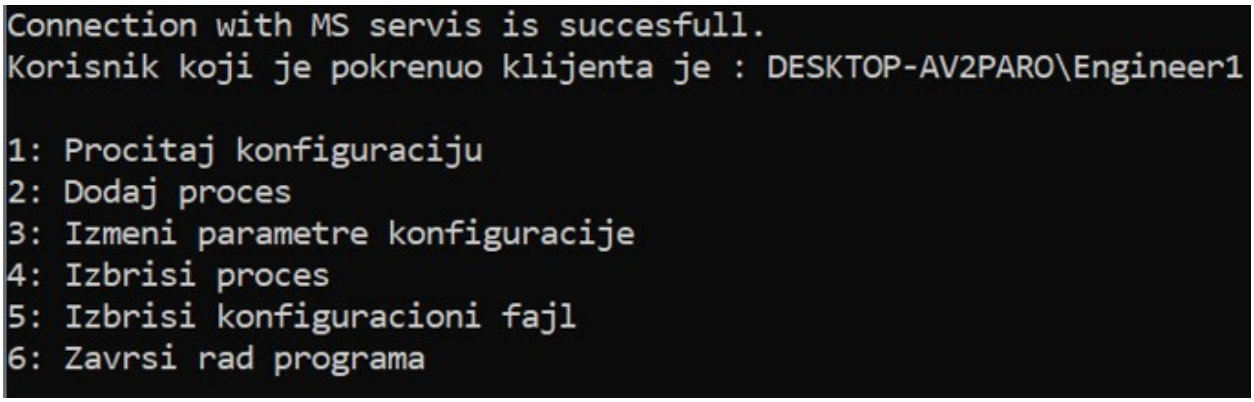
Intrusion Detection System

Intrusion Detection System (IDS) je komponenta sistema koja loguje alarme koje dobija od MS-a na ranije objašnjen način. Log sadrži datum i vreme detekcije, naziv procesa i jedan od 3 nivoa kritičnosti - Information (proces detektovan prvi put), Warning (proces detektovan drugi put) ili Critical (proces detektovan više puta).



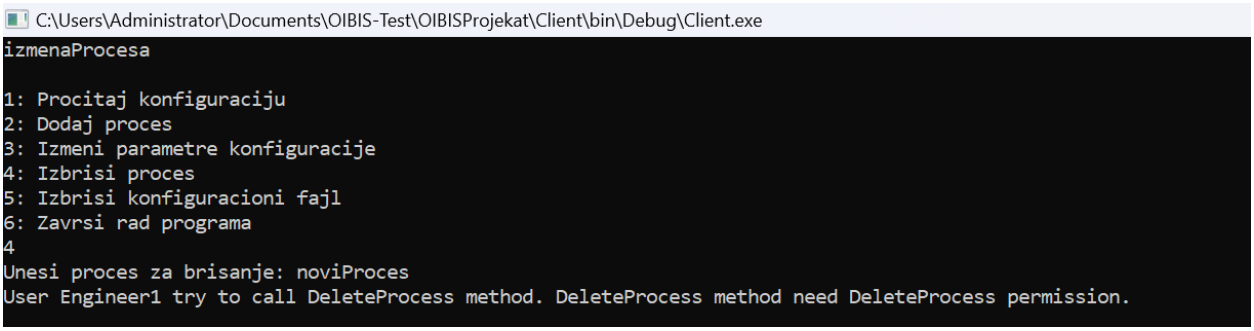
Klijent

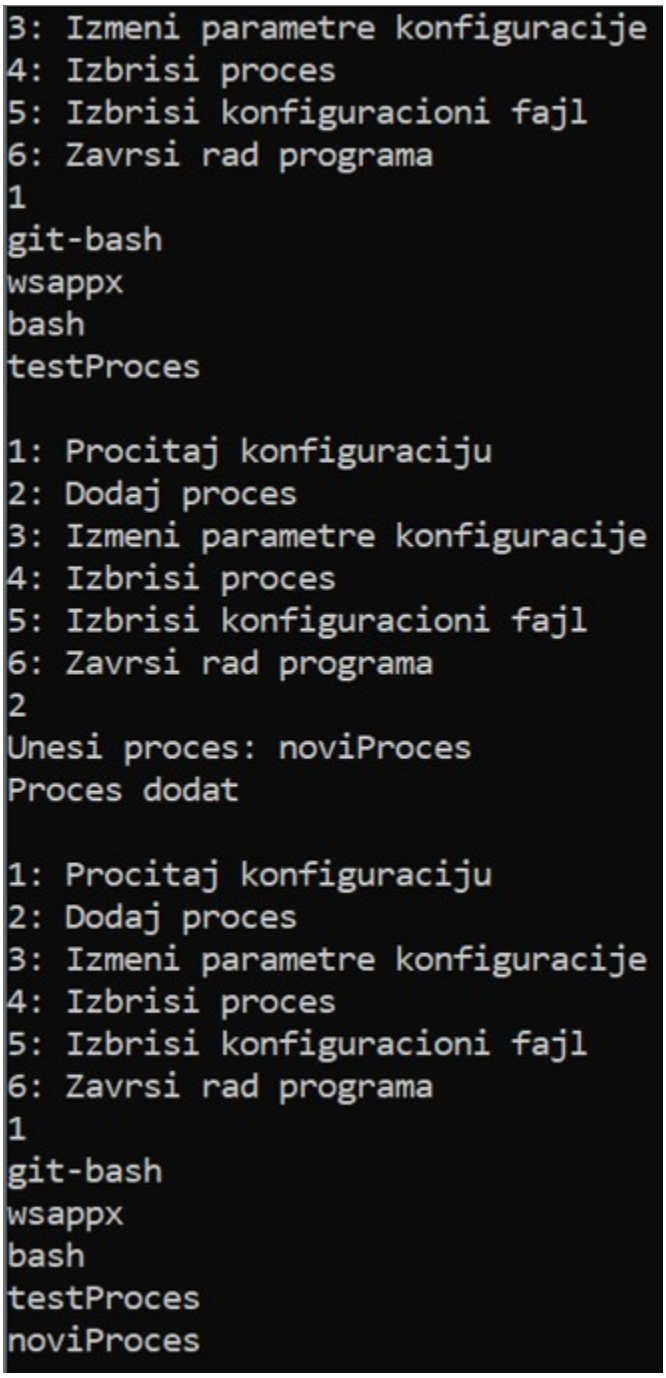
Klijentska aplikacija ima ulogu samo u izmeni blacklist malware konfiguracije. Klijenta pokreću korisnici koji, da bi uopšte mogli da pristupe MS-u, moraju da bude autentifikovani. Autentifikacija se vrši preko Windows autentifikacionog protokola. Između njih se otvara siguran komunikacioni kanal, tako da treća strana neće moći da pristupi podacima koji se šalju.



Da bi mogao da izmeni konfiguraciju klijent prvo mora biti autorizovan za to radnju i to se postiže RBAC modelom. RBAC (Role-Based Access Control) je tip autorizacije kojim se svakom korisniku dodeljuje jedna od definisanih uloga, a svakoj ulozi jedna ili više dozvola. Na taj način MS proverava kojoj ulozi pripada klijent i da li ta uloga ima dozvolu za traženu radnju.

Postoje 4 uloge i ukupno 5 radnji nad konfiguracijom: Manager može da pročita konfiguraciju ali nema pravo da napravi izmenu; Engineer ima pravo da izmeni postojeće parametre u konfiguraciji, kao i da dodaje nove procese, ali nema pravo da briše postojeće procese; Support Member ima pravo da izmeni postojeće parametre u konfiguraciji, da dodaje nove procese kao i da briše postojeće; Chief Officier jedina grupa korisnika koja ima pravo da obriše konfiguracioni fajl.





Zaključak

Malware Scanning system bi se mogao koristiti bi se mogao koristiti kao zaštita od zlonamernog softvera. Potencijalno značajno unapređenje bilo bi sakupljanje veće baze nedozvoljenih procesa koji bi se na primer dobavljali iz neke poznatije baze sličnih sistema.