SUSTAVI ZA DETEKCIJU NAPADA

Gregorek, Laura

SVEUČILIŠTE U SPLITU

SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Preddiplomski stručni studij Informacijske tehnologije

LAURA GREGOREK

Z A V R Š N I R A D

SUSTAVI ZA DETEKCIJU NAPADA

Split, rujan 2021.

SVEUČILIŠTE U SPLITU
SVEUČILIŠNI ODJEL ZA STRUČNE STUDIJE

Preddiplomski stručni studij Informacijske tehnologije

Predmet: Sigurnost računala i podataka

Z A V R Š N I R A D

Kandidat: Laura Gregorek

Naslov rada: Sustavi za detekciju napada

Mentor: Lada Sartori, v. pred.

Split, rujan 2021.

Sadržaj

Sažetak

U ovom završnom radu cilj je analizirati učinkovitosti i rad jednog od sustava za detekciju napada (engl. *intrusion detection system,* skraćeno IDS*)* na mreži.

Za simulaciju i primjer rada korišten je jedan od mnogih sustava za detekciju napada, pod imenom OSSEC. OSSEC je besplatni softver (engl. *software)*, koji će kao poslužitelj biti podignut preko VirtualBoxa na virtualnom stroju (engl. *virtual machine*) s Linux Mint operacijskim sustavom. Ovaj poslužitelj će nadzirati dolazi li do napada na ostalim nadgledanim računalima preko instaliranih agenata. Ostala računala će biti zasebni virtualni strojevi, na kojima su podignuti operacijski sustavi Linux Mint i Windows XP.

Kako bi se sama uloga OSSEC sustava bolje prikazala, simulirat će se namjerni napad na računala s agentima koji će se izvršiti s trećeg virtualnog računala s Kali Linux operacijskim sustavom. Prilikom napada, analizirat će se kako OSSEC javlja napade, koje vrste napada može prepoznati i je li ova vrsta detekcije napada dovoljna.

Ključne riječi: mreža, sustav, napad, zaštita, detekcija

Summary

Intrusion Detection Systems

The aim of this final paper is to analyze the efficiency and operation of one of the systems for intrusion detection system (IDS) on the network.

One of the many intrusion detection systems used for the simulation and example is OSSEC. OSSEC is a free software, which will act as a server on Linux Mint, built on a virtual machine via VirtualBox. This server will be able to monitor network attacks on other operating systems through the installed software called agents. The agents will be on separate virtual machines, using Linux Mint and Windows operating systems for them.

To better illustrate the role of the OSSEC system itself, a deliberate attack on the agents' system will be executed through the Kali Linux operating system. Data collected during the attack, will help to understand how OSSEC reports attacks, what types of attacks it can recognize, and whether this type of intrusion detection is sufficient.

Keywords: network, system, attack, protection, detection

1. Uvod

Razvojem tehnologije, osiguravanje pristupa mreži preko računala danas je ključno u radu svakog poslovanja i obrazovanja. Isto je dovelo do razvoja različitih načina napada na računala i samu mrežu što predstavlja svakodnevne rizike. Kako bi sav rad bio učinkovitiji i sigurniji, i kako bi se zaštitili svi potrebni podaci i informacije, mrežu i računalne sustave potrebno je zaštititi. Za zaštitu pojedinih računala koriste se vatrozidovi (engl. *firewall),* te razni antivirusni programi (engl. *antivirus software*). Olakšano nadziranje svih umreženih računala s ciljem prevencije neovlaštenih pristupa, omogućeno je preko sustava za detekciju napada.

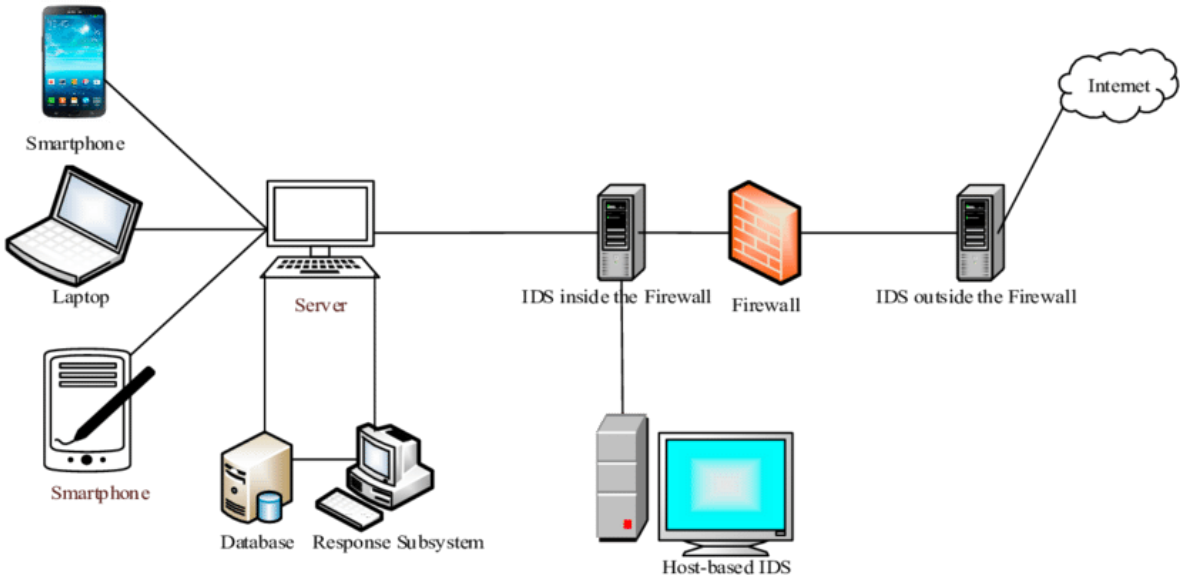
Cilj rada je prikazati kako instalirati i konfigurirati jedan sustav za detekciju napada, te prikazati kako sustav otkriva određene napade koje se u događaju na mreži ili na sustavu. U drugom poglavlju općenito su opisani takvi sustavi, što se pomoću njih točno može vidjeti, koliko su takvi sustavi učinkoviti i što sve takvi sustavi nadziru.

Kako bi se uloga takvih sustava bolje predočila, odabran je jedan besplatan IDS pomoću kojeg se nadzire mreža korisnika. Kako bi se osiguralo da sustav reagira i javi korisniku da je u tijeku pokušaj neovlaštenog upada u mrežu, simuliran je napad s trećeg računala. Sustavi za detekciju napada nemaju mogućnost spriječiti sam napad, već je to ostavljeno korisniku nakon što mu sustav dojavi da je napad u tijeku.

U trećem poglavlju detaljno je prikazan postupak instalacije i konfiguracije sustava za detekciju napada OSSEC, na kojeg se fokusiralo u ovom radu. Opisuje se postavljanje poslužitelja za nadzor, postavljanje agenata koji se nadgledaju, njihovo povezivanje te je dan prikaz onoga što poslužitelj pretražuje. Također su prikazani i svi problemi koji mogu nastati prilikom instalacija ili konfiguracija, samog sustava ili dodataka za sustav, te je opisano kako te probleme riješiti. Kako originalna web stranica OSSEC-a ima veoma ograničeno sučelje za prikaz događaja, instalirano je dodatno web sučelje koje je zahtijevalo migraciju cijelog sustava na noviju verziju.

2. Sustavi za detekciju napada

Kad je u pitanju nadziranje više računala odjednom, sve više se koriste sustavi za detekciju napada. Glavna uloga jednog takvog sustava je stalno praćenje onoga što se događa na mreži i računalima. Drugim riječima, IDS prati događaje koji se događaju u računalnom sustavu ili mreži, a bilježe se u zapisniku, tako što analizira znakove mogućih incidenata koji bi mogli dovesti do kršenja ili neposredne prijetnje kršenjem politike računalne sigurnosti. [1] Neki od najčešćih rizika koji se javljaju prilikom probijanja na mrežu su postavljanje zlonamjernog program (engl. *malware*) ili računalnog virusa, krađa tuđih osobnih informacija, pokušaj neovlaštenog pristupa sustavima i njihovog korištenja. Prikaz gdje se sve može nalaziti IDS vidi se na Slici 2.1 [2].



Slika 2.1.: IDS unutar sustava i mreže

2.1. Funkcije sustava i njihove metodologije

U praksi se koriste sustavi koji, uz sve funkcionalnosti koje imaju IDS-ovi, imaju mogućnost i sprječavanja napada, te se nazivaju IPS (engl. *intrusion prevention system*, skraćeno IPS). Postoje mnoge vrste IDS i IPS tehnologija koje se razlikuju po tome kakve događaje mogu prepoznati i pratiti, te metodologije koje koriste za identifikaciju incidenata. Sve vrste tih sustava izvode sljedeće funkcije: snimanje podataka vezanih uz promatrane

događaje, obavještavanje administratora sigurnosti o važnim zapaženim događajima i izrada izvještaja. [1] Može se razlikovati nekoliko metodologija koje ovi sustavi koriste za otkrivanje, a to su protokol za analizu zasnivan na potpisu (engl. *signature-based detection*), otkrivanje temeljeno na anomaliji (engl. *anomaly-based detection*) i analiza protokola stanja (engl. *stateful protocol analysis*). *Signature-based detection* se bazira na usporedbi potpisa (engl. *signature*) s promatranim događajima kako bi se otkrio potencijalni napad. Jedan od primjera potpisa je pokušaj upada na korisnikovo računalo s korisničkim imenom *root*. *Anomaly-based detection* funkcionira na način da uspoređuje aktivnosti koje se smatraju normalnim, s onim koje djeluju neuobičajenima kako bi se utvrdila odstupanja. Ova vrsta detekcije koristi račune (engl. *profiles*) koji predstavljaju normalne i svakodnevne aktivnosti korisnika, računala (engl. *host*), aplikacija (engl. *applications*) i mrežnih veza (engl. *network connections*). *Stateful protocol analysis* predstavlja proces usporedbe unaprijed određenih profila dobroćudne aktivnosti protokola za svako stanje protokola u odnosu na promatrane događaje kako bi se identificirala odstupanja. Ovaj protokol se oslanja na univerzalne profile koje su razvili proizvođači koji određuju kako bi određene protokole trebalo i ne bi trebalo koristiti. Riječ *stateful* u nazivu ovog protokola govori o tome kako je IDS sposoban razumjeti i pratiti stanje mreže, transporta i aplikacijskih protokola. [1]

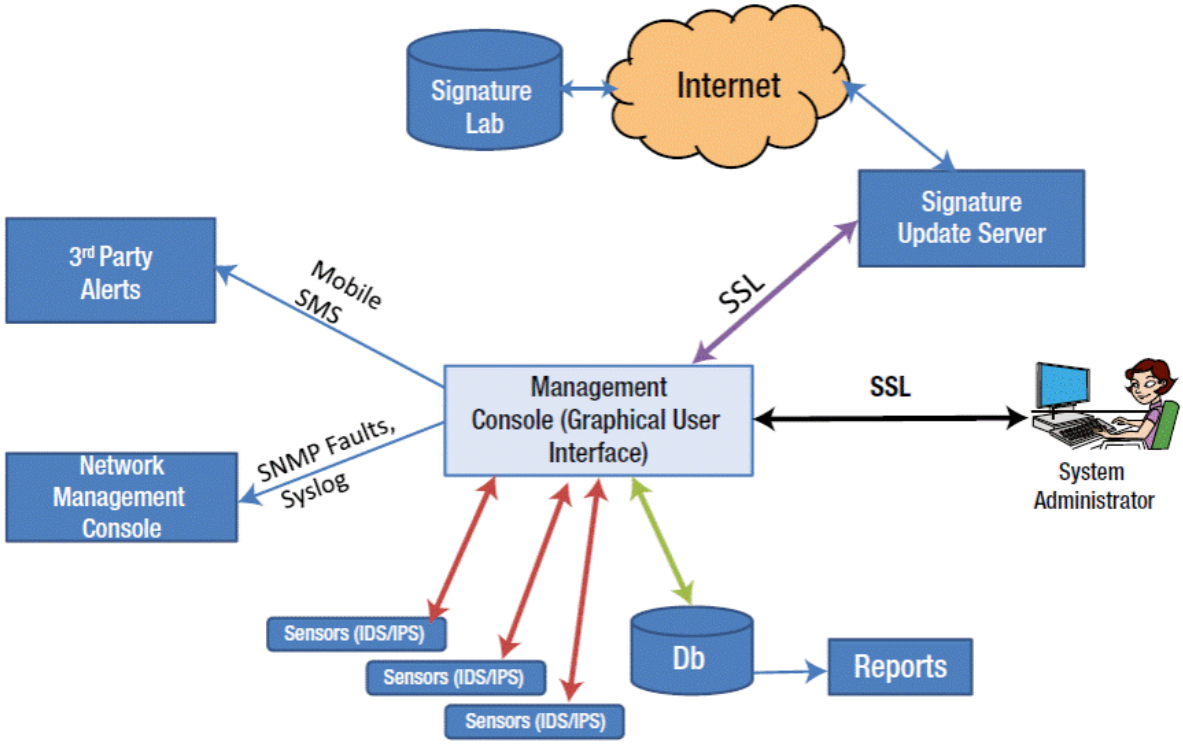
2.2. Vrste sustava za detekciju napada

Na osnovu toga kakve vrste događaja prate i kako su raspoređeni, sustavi za detekciju napada mogu se podijeliti u četiri skupine. Prva skupina su oni sustavi koji djeluju na mreži (engl. *network based*). Njihova uloga je praćenje mrežnog prometa određenih mrežnih segmenata ili uređaja, kao i analiza mreže i aktivnosti aplikacijskog protokola kako bi se utvrdila bilo kakva sumnjiva aktivnost. Najčešće se nalaze na vatrozidu ili usmjerivaču (engl. *router*), poslužitelju (engl. *server*) virtualne privatne mreže (engl. *Virtual Private Network*, skraćeno VPN), bežičnoj mreži (engl. *wireless network*) i poslužiteljima za udaljeni pristup (engl. *remote access server*). Druga skupina spada u bežične jer prati promet bežične mreže i analizira protokole bežičnog umrežavanja kako bi identificirao sumnjive aktivnosti koje se mogu dogoditi na bežičnoj mreži koja koristi npr. IP protokol. Najčešće se nalaze unutar bežične mreže neke organizacije, ali se mogu postaviti na lokacijama gdje se očekuje da bi napadač mogao neovlašteno podignuti bežičnu mrežu. Sustavi u trećoj skupini baziraju se na analizi ponašanja mreže (engl. *Network Behavior Analysis*, skraćeno NBA). Cilj analize

ponašanja mreže je identifikacija neželjenih prijetnji kao što su zlonamjerni programi, kršenje politike sigurnosti i distribuirano uskraćivanje usluge (engl. *Distributed Denial of Service*, skraćeno DDoS). NBA sustavi se koriste kako bi nadzirali tok prometa interne mreže neke organizacije, a nekad su raspoređeni kako bi mogli pratiti protok podataka između organizacijske mreže i vanjske mreže. U zadnjoj skupini nalaze se računalno orijentirani sustavi (engl. *host-based*) koji prate karakteristike i događaje na jednom računalu kako bi se otkrilo je li došlo do sumnjivih aktivnosti. Takvi sustavi se najčešće implementiraju na kritičnim računalima kao što su poslužitelji koji sadrže osjetljive podatke ili koji su javno dostupni. Karakteristike koje ovakav sustav prati su mrežni promet samog računala, sistemski zapisnici (engl. *system logs*), pokrenuti procesi (engl. *running processes*), aktivnosti aplikacije, pristup i izmjena datoteka (engl. *file access and modification*) i promjene konfiguracije sustava i aplikacija. [1]

2.3. Komponente sustava za detekciju napada

Postoje četiri osnovne komponente koje se nalaze unutar svakog sustava za detekciju i prevenciju napada. Agenti nadziru i analiziraju događaje i aktivnosti. Senzor je naziv koji se koristi za one IDPS (engl. *intrusion detection and prevention system,* skraćeno IDPS) koji prate sve vrste mreže, a agentima se nazivaju oni sustavi koji se koriste za IDPS tehnologije temeljene na računalu. Poslužitelj za upravljanje (engl. *management server*) je uređaj koji prima informacije od senzora ili agenata, te upravlja tim informacijama. Takav poslužitelj je centraliziran i on se bavi analizom događaja primljenih od senzora ili agenata s mogućnošću identificiranja događaja koje pojedini agenti ili senzori ne mogu. Poslužitelj baze podataka (engl. *database server*) je poslužitelj unutar kojeg se pohranjuju informacije o događajima dobivenih od senzora, agenata ili poslužitelja za upravljanje. Posljednja komponenta je konzola (engl. *console*). To je program koji pruža korisnicima i administratorima nekog IDPS-a prikaz sučelja. [1] Primjer arhitekture jednog takvog sustava može se vidjeti na slici 2.2 [3].



Slika 2.2.: Arhitektura IDS-a

2.4. OSSEC

U ovom završnom radu jedan od sustava za detekciju napada koji će se koristiti je OSSEC. OSSEC je sustav za otkrivanje napada koji je kompatibilan s više operacijskih sustava i platformi (engl. *multi-platform*). Njegove značajke su snažan mehanizam za analizu, analiza zapisnika integracije, nadzor integriteta datoteke, nadzor registra Windows operacijskog sustava, centralizirano provođenje pravila, otkrivanje *rootkita* i upozorenja koja se odvijaju u stvarnom vremenu. Moguće ga je koristiti na većini operativnih sustava kao što su Windows, Linux, MacOS, OpenBSD, FreeBSD i Solaris. OSSEC je besplatan softver koji je računalno orijentiran i ima mogućnost modificiranja. Osim za korištenje za zaštitu poslužitelja, često se koristi i kao alat za analizu zapisnika (engl. *log analysis tool*), za analizu vatrozida, web poslužitelja i zapisnika provjere autentičnosti (engl. *authentication logs*). [4]

Slika 2.3.: Logo OSSEC sustava

Na slici 2.3. [4] prikazan je logo OSSEC sustava.

2.5. OSSEC web poslužitelj

Osim što radi preko komandne linije, OSSEC poslužitelj ima mogućnost prikazivati zapisnike i uzbune preko web sučelja pod nazivom OSSEC *Web User Interface*. Kako bi se omogućila instalacija OSSEC web sučelja, potrebno je prvo instalirati i konfigurirati nekoliko programa, a to su Apache, PHP i MySQL.

Apache, pod nazivom Apache HTTP *Server Project*, je projekt čiji je cilj bio realizacija HTTP (engl. *Hypertext Transfer Protocol*) poslužitelja koji je komercijalan, robustan, karakterističan i čiji je izvorni kôd dostupan i besplatan. Preteča Apache web poslužitelju bio je HTTP *daemon*, također besplatan i javno dostupan softver čiji je naziv još bio httpd. Nakon odlaska glavnog programera koji je razvio HTTP *daemon*, grupa programera je samostalno razvila vlastita proširenja i unijela potrebne ispravke grešaka. Ista grupa programera, koristeći NCSA (skraćeno *National Center for Supercomputing Applications*) httpd 1.3 verziju kao bazu, uz dodatak svih objavljenih ispravaka i poboljšanja, napravila je prvi Apache poslužitelj 1995. godine. I danas Apache ostaje platforma na kojoj su institucije i pojedinci u mogućnosti graditi pouzdane sustave, kako u eksperimentalne svrhe, tako i u kritične svrhe. [6]

PHP, koji dolazi od akronima *Hypertext Preprocessor*, je široko korišteni skriptni jezik, otvorenog kôda, koji je pogodan za razvoj web sučelja i može biti ugrađen u HTML (skraćeno *Hypertext Markup Language*). On spada u grupu jezika za skriptiranje, koji su podskup jezika za kodiranje koji se koriste za automatizaciju procesa. Skriptni jezici se koriste kako bi se izbjeglo izvršavanje kôda web lokacije korak po korak. PHP se kao jezik obično koristi na poslužitelju. Funkcionira na način da web preglednik upućuje zahtjev web poslužitelju, koji zatim odgovara na zahtjeve uz slanjem HTML kôda u kojem može biti integriran PHP dio kojeg web preglednik može obraditi, prikazati i pretvoriti u određeni sadržaj koji će biti prikazan na zaslonu korisnika. Skriptni jezik kao što je PHP, koristi se za pretraživanje sadržaja s poslužitelja ili baze podataka nekog web mjesta, kako bi mogao taj sadržaj učiniti dostupnim i vidljivim za klijenta. [7] Osim za prikazivanje sadržaja na web stranici, PHP također može obavljati druge funkcije kao što su prikupljanje podataka obrazaca, generiranje dinamičnog sadržaja stranice ili primanje i slanje kolačića (engl. *cookies*). PHP skripte se mogu koristiti i preko sučelja naredbenog retka (engl. *command line interface*) gdje se mogu pokrenuti bez poslužitelja ili preglednika, ali i za pisanje aplikacija za radnu površinu. Prednost je što se može

koristiti na svim značajnim operacijskim sustavim poput Linuxa, puno Unix varijanti kao Solaris i OpenBSD, Microsoft Windows, MacOS, i RISC OS. Ima podršku i za većinu današnjih web poslužitelja, među kojima su Apache i IIS i mnogi drugi. S PHP-om nema ograničenja vezano za izlazni HTML jer njegove mogućnosti uključuju izbacivanje slika, PDF datoteka i Flash filmova generiranih u hodu. Moguće je lako ispisati bilo koji tekst kao što je XHTML i bilo koja druga XML datoteka jer PHP može automatski generirati te datoteke i spremiti ih u datotečni sustav. Jedna od njegovih najboljih značajki je podrška širokom spektru raznih baza podataka. Zbog te podrške, pisanje web stranica koje sadrže neku bazu podataka, jako je jednostavno koristeći specifična proširenja koje nudi PHP, kao na primjer za MySQL. Također ima korisne značajke koje se koriste za obradu teksta, što uključuje Perl kompatibilne regularne izraze (engl. *Perl compatible regular expressions*) i mnogo alata i proširenja za raščlanjivanje i pristup XML dokumentima. [8]

2.6. MySQL

MySQL spada među najpopularnije sustave za upravljanje bazom podataka otvorenog SQL kôda. SQL dio unutar naziva MySQL znači strukturirani jezik upita (engl. *Structured Query Language*), a to je najčešći standardizirani programski jezik koji se koristi za pristup bazama podataka. Baza podataka je strukturirana zbirka podataka koja može sadržavati bilo koje podatke poput galerije slika, popisa za kupovinu ili velike količine informacija u nekoj korporacijskoj mreži. Kako bi bilo moguće dodavati, pristupati i obrađivati podatke koji su pohranjeni u računalnoj bazi podataka, potreban je sustav za upravljanje tim bazama kao što je MySQL poslužitelj. Sustavi za upravljanjem bazama podataka mogu djelovati kao samostalni uslužni programi ili kao dijelovi nekih drugih aplikacija. MySQL baze podataka su relacijske, što znači da takva baza podataka pohranjuje podatke u zasebne tablice, umjesto da sve podatke sprema u jedno veliko spremište. Strukture baze podataka ovog poslužitelja su organizirane u fizičke datoteke koje su optimizirane za brzinu. Logički model s objektima poput baze podataka, tablica, redaka i stupaca nudi fleksibilno programsko okruženje. Kod ovog poslužitelja postoji mogućnost postavljanja pravila koja reguliraju odnose između različitih podatkovnih polja, kao što su jedan na jedan, jedan na više, jedinstveni, obavezni ili neobavezni i pokazivači između različitih tablica. Baza podataka zatim primjenjuje postavljena pravila, tako da aplikacija nikada neće vidjeti nedosljedne, dvostruke, zastarjele ili podatke koji nedostaju. MySQL je softver otvorenog izvora i kôda, što znači da svatko može koristiti i mijenjati njegov izvorni kôd prema vlastitim potrebama. Također je besplatan i dostupan za

preuzimanje svima na internetu. Značajke ovog poslužitelja su velika brzina, pouzdanost, skalabilnost i jednostavnost upotrebe. Može se bez problema pokretati na prijenosnom računalu ili radnoj površini zajedno s ostalim aplikacijama, web poslužiteljima i ostalim, zahtijevajući malo ili nimalo pažnje. MySQL baza podataka i softver je klijent/poslužiteljski sustav koji se sastoji od višenitnog (engl. *multithreaded*) SQL poslužitelja koji podržava različite pozadine (engl. *backend*), nekoliko različitih klijentskih programa, administrativnih alata i širokog spektra sučelja za aplikacijsko programiranje. [9]

2.7. Wazuh

Wazuh je sustav koji je besplatno rješenje za sigurnosni nadzor za otkrivanje prijetnji, nadzor integriteta i odgovaranje na incidente koji je otvorenog kôda. Sustav se može koristiti za provođenje sigurnosne analitike kombinacijom implementiranog softvera, algoritama i analitičkih procesa koji se koriste za otkrivanje potencijalnih prijetnji i nesigurnosti. [10] Wazuh ima mogućnost prikupljanja, indeksiranja i analize sigurnosnih podataka, pomažući organizacijama u otkrivanju napada, prijetnji ili anomalija.

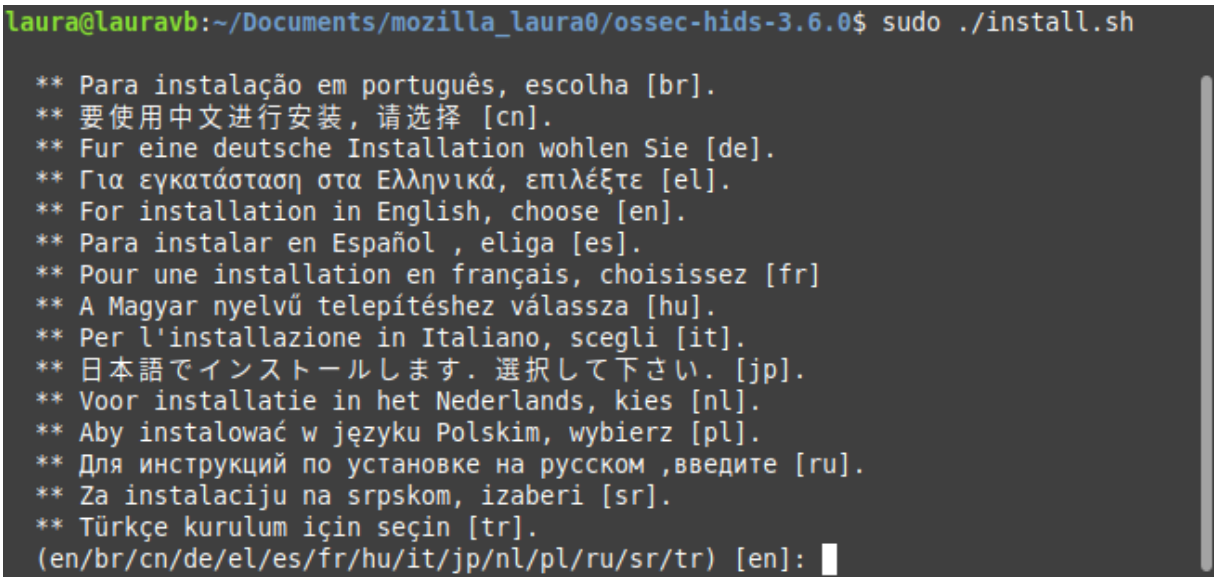
Pošto su računalne prijetnje sve sofisticiranije, za brzo otkrivanje i otklanjanje opasnosti potrebni su nadzor i sigurnosna analiza u stvarnom vremenu. Zbog toga su Wazuh agenti lagani, i pružaju potrebne mogućnosti praćenja i reagiranja na prijetnje, dok njegova poslužiteljska komponenta pruža sigurnosnu inteligenciju i obavlja analizu podataka. Drugi način uporabe ovog sustava je samo otkrivanje napada i upada. Wazuh agenti skeniraju sustave koje nadgledaju u potrazi za zlonamjernim softverom ili sumnjivim anomalijama. Imaju mogućnost otkrivanja skrivenih procesa, skrivenih datoteka ili alata za neregistrirano praćenje prometa na mreži, kao i nedosljednosti u odgovorima na sistemske pozive. Uz navedene mogućnosti agenata, poslužitelj koristi pristup otkrivanju napada zasnovan na potpisu (engl. *signature-based*), koristeći svoj mehanizam regularnih izraza za analizu prikupljenih podataka zapisnika. Sljedeća funkcija je analiza podataka zapisnika. Wazuhovi agenti čitaju zapisnike aplikacija i operacijskog sustava i sigurno ih prosljeđuju poslužitelju za analizu i pohranu temeljenu na pravilima. Ta pravila pomažu upoznavanju korisnika s pogreškama aplikacija ili sustava, pogrešnim konfiguracijama, pokušajima zlonamjernih aktivnostima, kršenjem pravila i nizom drugih sigurnosnih i operativnih problema. Praćenje integriteta datoteke također je jedna od funkcija Wazuha. On nadgleda datotečni sustav tako što prepoznaje promjene u sadržaju datoteka, promjene u dozvolama nad datotekama i vlasništvu. Uz to, izvorno identificira programe i korisnike koji se koriste za izmjenu ili stvaranje datoteka. Jedna od funkcija Wazuha

je otkrivanja ranjivosti, pri čemu Wazuh agenti izvlače podatke iz softverskog inventara i šalju ih poslužitelju, gdje su povezani s kontinuirano ažuriranim bazama podataka CVE (engl. *Common Vulnerabilities and Exposure*), kako bi se identificirao dobro poznati ranjivi softver. Procjena konfiguracije, također bitna funkcija ovog sustava, gdje Wazuh nadgleda postavke konfiguracije aplikacija i sustava. Zbog toga agenti vrše povremena skeniranja sustava kako bi otkrili postoje li aplikacije koje su ranjive ili nesigurno konfigurirane. Funkcija odgovora na incident omogućava da Wazuh pruža aktivne odgovore za provođenje različitih protumjera za rješavanje aktivnih prijetnji i to van mreže.

Ostale dostupne funkcije ovog sustava su sigurnost oblaka (engl. *cloud*) i sigurnost spremnika (engl. *containers*). Kod sigurnosti oblaka, ovaj sustav nadzire infrastrukturu i sigurnost oblaka koristeći integracijske module koji su u mogućnosti izvući sigurnosne podatke od poznatih pružatelja usluga oblaka, kao što su Amazon AWS, Azure ili Google Cloud. Wazuh kod sigurnosti spremnika pruža sigurnosnu preglednost Docker kontejnerima, nadgleda njihovo ponašanje i otkriva prijetnje, ranjivosti i anomalije. [11] Osim svih funkcija koje ovaj sustav čine pogodnim za korištenje, razlog odabira baš njega je to što je Wazuh migrirao iz OSSEC-a. Pošto dugo vremena na OSSEC-u nije bilo nikakvih promjena, popravaka niti ažuriranja, Wazuh tim je odlučio preuzeti projekt i stvoriti novi sustav koji sadrži sve funkcije koje ima OSSEC, ali i mnogo više. Ovaj sustav također sadrži nekoliko bitnih dodataka za još bolje nadziranje i upravljanje. Osim samog Wazuha, uz njega se koriste Elasticsearch, Filebeat i Kibana. Elasticsearch je distribuirani i besplatni program za pretraživanje i analizu svih vrsta podataka, uključujući tekstualne, numeričke i ostale, te je poznat po svojoj brzini i skalabilnosti. On pohranjuje podatke kako bi se mogli vrlo brzo pretraživati, ima moćnu analitiku koja se lako prilagođava i precizno podešenu relevantnost. Filebeat se isporučuje s modulima za promatranje i izvorima sigurnosnih podataka koji pojednostavljuju prikupljanje, raščlanjivanje i vizualizaciju zapisnika. Glavna uloga Filebeta je da nadzire zapisnike ili specificirane lokacije na računalu i sustavu, prikuplja događaje zapisnika, te ih prosljeđuje Elasticsearchu. Kibana je besplatno i otvoreno korisničko sučelje koje omogućava vizualizaciju podataka prikupljenih s Elasticsearcha. [12]

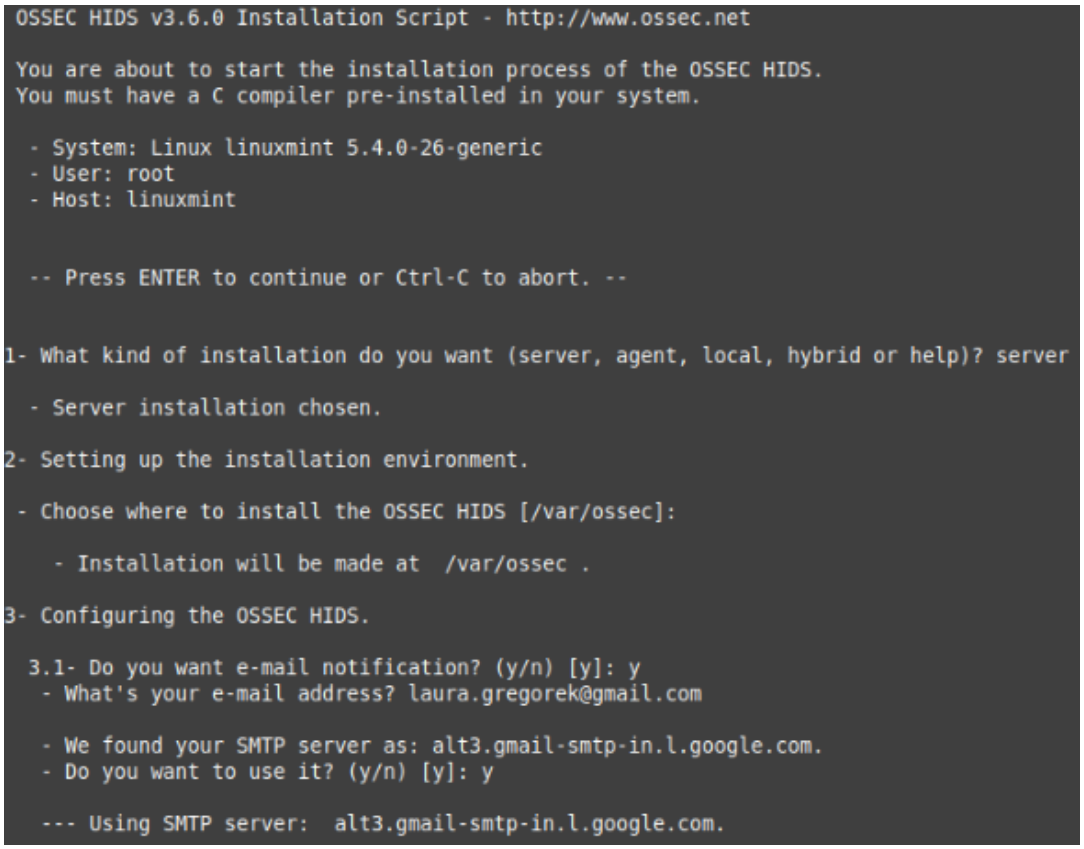
3. Postavljanje sustava OSSEC

OSSEC kao poslužitelj može se instalirati isključivo na operacijskom sustavu Linux. Ista instalacija može se koristiti i kao agent, odnosno, poslužitelj može nadzirati i samog sebe. Kao prvi korak instalacije, sa službene web stranice OSSEC sustava, preuzme se datoteka s potrebnim dokumentima za instalaciju. Nakon preuzimanja, datoteka se mora raspakirati. Iz komandne linije, uđe se u direktorij u koji se arhiva raspakirala naredbom `cd ossec-hids-3.6.0`. Pokretanjem skripte za instalaciju naredbom `sudo ./install.sh`, započinje instalacija koja se provodi kroz nekoliko koraka.



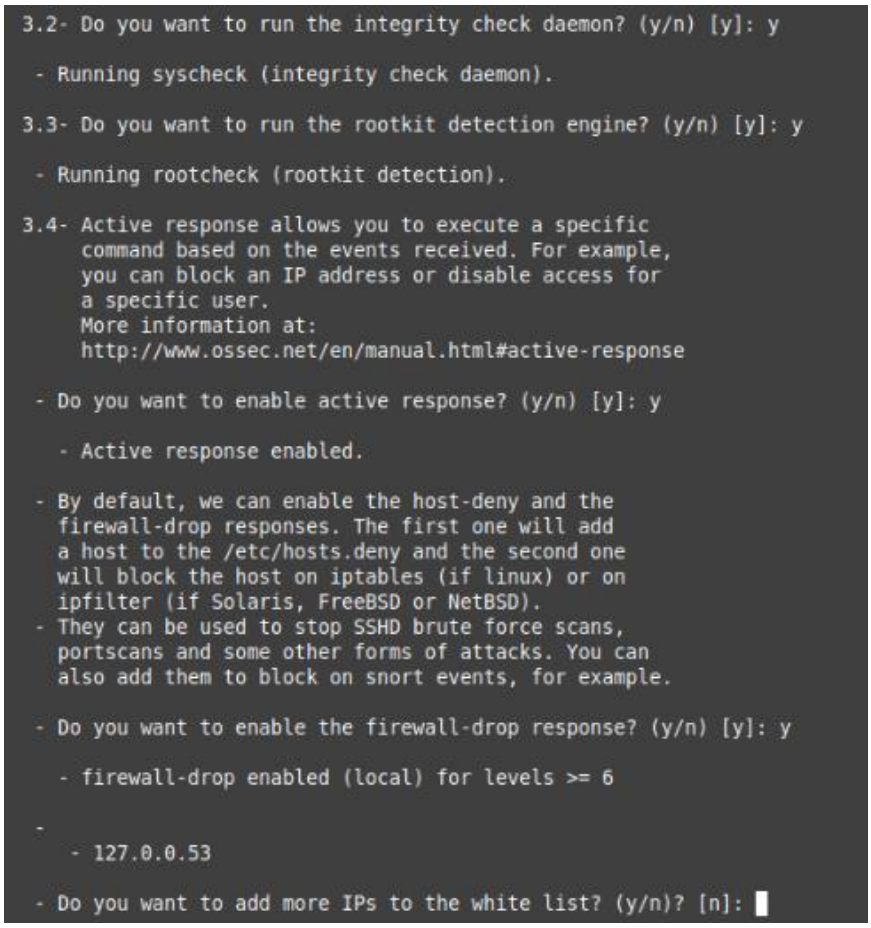
Slika 3.1.: Odabir jezika za OSSEC

Nakon odabira jezika koji će se koristiti (slika 3.1.) prikazani su podaci o sustavu korisnika. Pritiskom tipke *ENTER*, postavlja se pitanje o tipu instalacije i odabire direktorij u kojem će se izvršiti instalacija. OSSEC ima mogućnost slati notifikacije putem elektroničke pošte, pa je prilikom instalacije omogućeno postaviti informacije o željenoj adresi kao što je prikazano na slici 3.2.



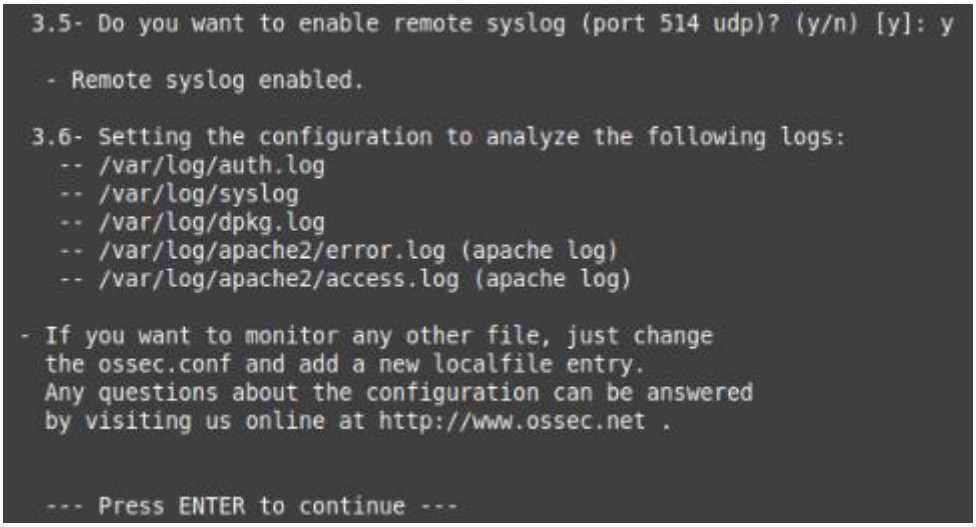
Slika 3.2.: Osnovne postavke OSSEC sustava

Na slici 3.3. prikazan je odabir provjera koje OSSEC može izvršavati kao što su provjera integriteta, mehanizam za otkrivanje zbirke zlođudnog softvera (engl. *rootkit detection engine*), aktivni odgovor, mogućnost blokiranja pristupa računalu, opcija kojom se određene IP-adrese mogu dodati na bijelu listu, te definira koji se sustav zapisnika koristi, što se može vidjeti na slici 3.4.



Slika 3.3.: Odabir provjera

Pri samom kraju instalacije, postavlja se konfiguracija koja će analizirati određene zapisnike i u kojim putanjama se mogu naći. Dostupna je i opcija nadziranja dodatnih datoteka koja se može postaviti mijenjanjem konfiguracijske datoteke ossec.conf.

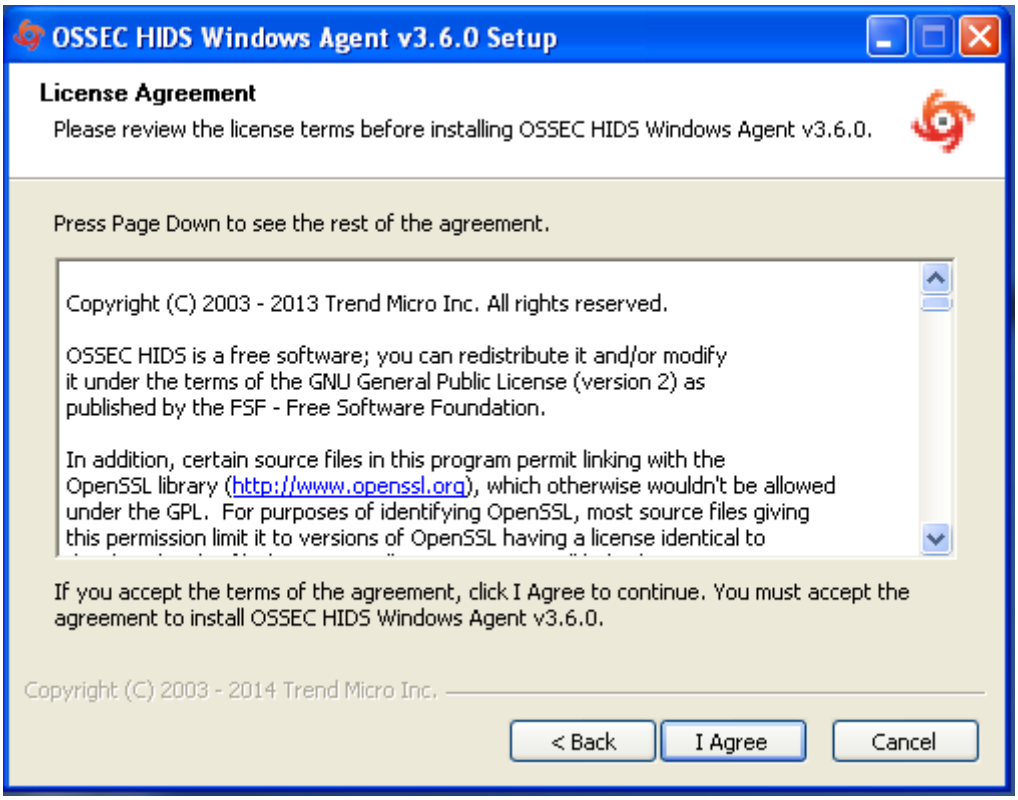


Slika 3.4.: Podaci o pokretanju, zaustavljanju i konfiguraciji OSSEC-a

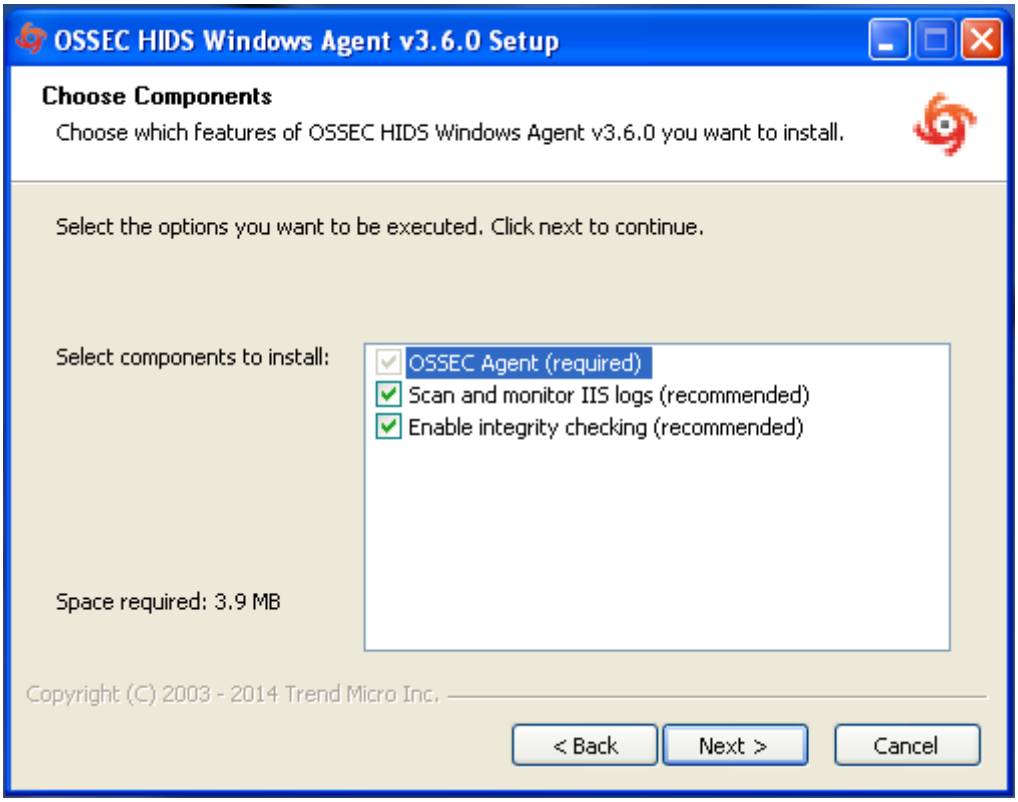
U ovom radu osim Linux operacijskog sustava, nadgleda se i Windows XP operacijski sustav. Instalacija agenta na Windows sustavu izgleda kao instalacija bilo kojeg programa. Kao i kod Linuxa, prvi korak je preuzeti datoteku sa službene OSSEC web stranice koja je namijenjena za Windows sustave. Kada se preuzimanje završi, otvori se preuzeta datoteka i s time se započinje proces instalacije i postavljanja OSSEC-a kao što je prikazano na slici 3.5.

Slika 3.5.: Postavljanje Windows agenta

Nakon pritiska na tipku *Next*, otvara se prozor sa svim podacima o uvjetima licence što se može vidjeti na slici 3.6. Pritiskom na tipku *I Agree*, potrebno se složiti se sa svima uvjetima, nakon čega se otvara sljedeći prozor u kojem se odabiru komponente koje se žele instalirati. Na slici 3.7. vidljive su sve ponuđene komponente, i odabrano je skeniranje i nadzor IIS (engl. *Internet Information Services*) zapisnika. Datoteke IIS zapisnika su po zadanim postavkama pohranjene u mapi na IIS poslužitelju koja se nalazi na putanji `%SystemDrive%\inetpub\logs\LogFiles`. Zapisnici pružaju informacije o web stranicama i podatke o njima kao što su IP-adrese, informacije o korisniku i kada je stranica bila posjećena, u koje vrijeme i datum. IIS zapisnici također pružaju informacije o podacima i korištenju IIS web poslužitelja. [5] Osim toga, odabrano je i omogućavanje provjere integriteta.



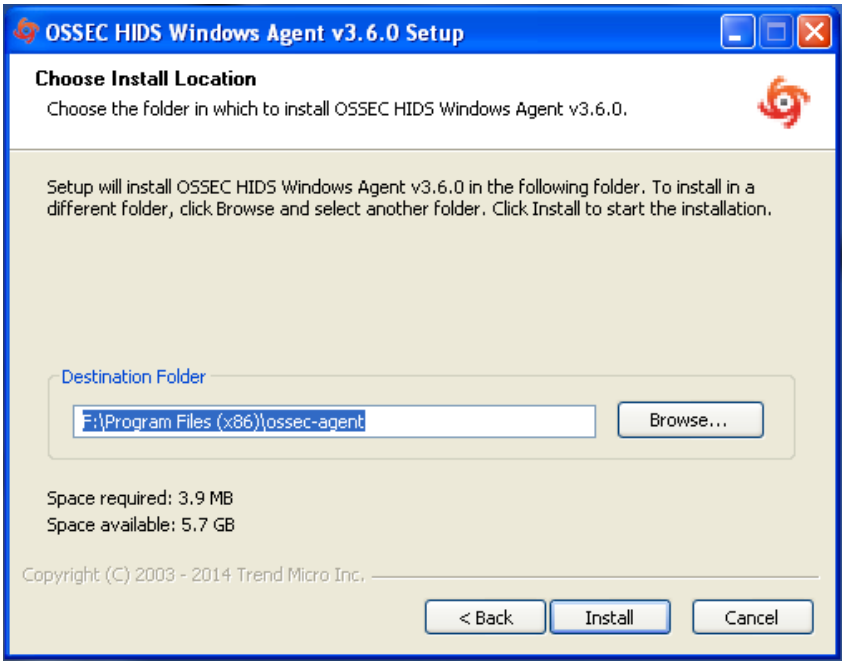
Slika 3.6.: Uvjeti licence



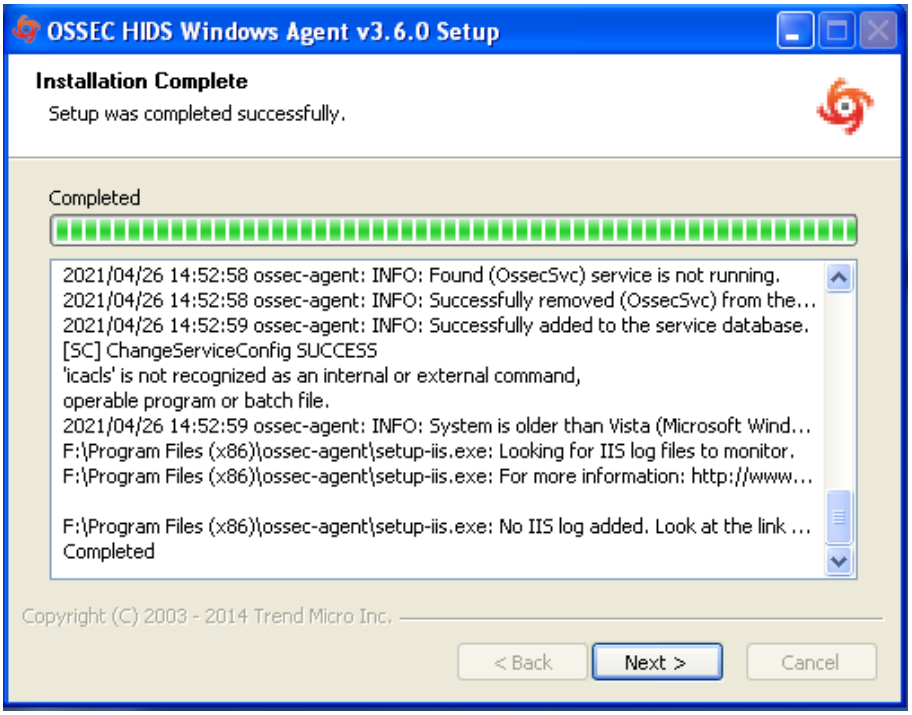
Slika 3.7.: Odabir komponenti za instalaciju

Odabiranjem željenih komponenti i pritiskom na tipku *Next*, pojavljuje se prozor na kojem se postavlja lokacija i direktorij unutar kojeg će se izvršiti instalacija kako je prikazano

na slici 3.8. Nakon što se odabere destinacijski direktorij, pritiskom na *Install* otvara se prozor koji je vidljiv na slici 3.9. i obavlja se proces instalacije.



Slika 3.8.: Odabir datoteke za instalaciju



Slika 3.9.: Proces instalacije

Slika 3.10. pokazuje da je sa završetkom instalacije, omogućen odabir pokretanja OSSEC-a odmah ili kasnije.

Slika 3.10.: Pokretanje OSSEC-a

3.1. Povezivanje agenata s poslužiteljem

Kako bi poslužitelj bio u mogućnosti nadzirati sve agente, potrebno ih je povezati. Za proces povezivanja, prvo je potrebno pokrenuti OSSEC na poslužitelju. Naredbom `sudo /var/ossec/bin/ossec-control start` pokreće se OSSEC. Posebnom naredbom `sudo /var/ossec/bin/manage_agents` otvara se OSSEC-ov upravitelj agentima koji nudi nekoliko opcija vezanih za rad s agentima. Dostupne opcije su dodavanje agenta, generiranje ključa za agenta, prikaz liste dodanih agenata, uklanjanje agenta i izlazak iz izbornika. Slika 3.11. pokazuje pokretanje OSSEC-a i upravitelja agentima, kao i sve opcije koje se nalaze unutar upravitelja.

```
linuxmint@linuxmint201:~$ sudo /linuxmint/ossec/bin/ossec-control start
Starting OSSEC HIDS v3.6.0...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
linuxmint@linuxmint201:~$ sudo /linuxmint/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v3.6.0 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

Slika 3.11.: Pokretanje OSSEC-a upravitelja agentima

Dodavanje agenta poslužitelju je prvi korak u povezivanju. Odabirom slova A, potrebne su određene informacije o agentu kao što su njegov naziv koji se bira dobrovoljno, agentova IP-adresa i identifikacijski broj agenta. Za završetak dodavanja potrebna je potvrda upisivanjem slova y, nakon čega se dobije informacija da je agent dodan. Primjer dodavanja agenta poslužitelju vidljivo je na slici 3.12.

```
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: LinuxAgent
   * The IP Address of the new agent: 192.168.126.89
   * An ID for the new agent[005]: 005
Agent information:
   ID:005
   Name:LinuxAgent
   IP Address:192.168.126.89

Confirm adding it?(y/n): y
Agent added with ID 005.
```

Slika 3.12.: Dodavanje agenta

Drugi korak povezivanja uključuje generiranje ključa potrebnog za agenta. Poslužitelj generira jedinstveni niz slučajnih brojeva, slova i znakova koje može upotrijebiti samo jedan agent. Za generiranje tog ključa, potrebno je na poslužitelju pri konfiguraciji upravitelja agenata

odabrati slovo E. Zatim se prikaže lista svih dostupnih agenata i traži se identifikacijski broj agenta. Upisivanjem identifikacije, poslužitelj generira ključ koji je potrebno kopirati. Proces generiranja ključa vidi se na slici 3.13.

```
****************************************
* OSSEC HIDS v3.6.0 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 005, Name: LinuxAgent, IP: 192.168.126.89
Provide the ID of the agent to extract the key (or '\q' to quit): 005

Agent key information for '005' is:
MDA1IExpbnV4QWdlbnQgMTkyLjE2OC4xMjYuODkgZjE0ZWYwN2JiODE1YzdmNGM4NTc3ZTk1MzA5OTBhOWM1ZmMzNmJmYjI4MzMxNDlkM2FlZjA2ZDk4MDBmNGQ1Ng==

** Press ENTER to return to the main menu.
```

Slika 3.13.: Generiranje ključa

U isto vrijeme, s agentove strane također je potrebno ući u agent upravitelja. Naredbom `sudo /var/ossec/bin/manage_agents` na agentu se ulazi u spomenuti upravitelj. Za razliku od poslužitelja, agent ima ponuđene samo dvije opcije koje uključuju uvoz ključa i izlazak iz izbornika. Na slici 3.14. vidi se da je upisivanjem velikoga slova I, moguće zalijepiti prije kopirani ključ, što rezultira ispisivanjem informacija o agentu na kojemu se radi. Za završetak povezivanja, upisuje se slovo y kao konačna potvrda.

```
agent@agent-VirtualBox:~/ossec/ossec-hids-3.6.0$ sudo /var/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v3.6.0 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDA1IExpbnV4QWdlbnQgMTkyLjE2OC4xMjYuODkgZjE0ZWYwN2JiODE1YzdmNGM4NTc3ZTk1MzA5OTBhOWM1ZmMzNmJmYjI4MzMxNDlkM2FlZjA2ZDk4MDBmNGQ1Ng==

Agent information:
   ID:005
   Name:LinuxAgent
   IP Address:192.168.126.89

Confirm adding it?(y/n): y
2021/04/26 14:48:03 manage_agents: ERROR: Cannot unlink /queue/rids/sender: No such file or directory
Added.
** Press ENTER to return to the main menu.
```

Slika 3.14.: Povezivanje agenta s poslužiteljem

Za spajanje agenta na Windows operacijskom sustavu, postupak je skoro isti. Ponovno je potrebno prvo na poslužitelju dodati agenta, ali ovaj put s informacijama za Windows sustav. Kada je taj agent dodan, generira se njegov ključ na poslužitelju. Sa strane agenta, potrebno je ući u OSSEC agent upravitelja. Na otvorenom prozoru prikazan je status agenta, a na slici 3.15.

može se vidjeti kako se traži ključ potreban za autentičnost i IP-adresa poslužitelja. Na odgovarajuća mjesta unose se IP-adresa OSSEC poslužitelja i ključ. Pritiskom na *Save*, otvara se novi prozor za potvrdu uvezenog ključa koji sadrži informacije o trenutnom agentu što je prikazano na slici 3.16. Završetak dodavanja agenta postiže se tipkom OK. Sada su podaci o agentu osvježeni, pa se može vidjeti njegovo ime, IP-adresa i status koji sada može biti samo upaljen ili ugašen. Također ostaju spremljeni podaci o poslužitelju i ključ koji se koristio ranije za autentikaciju. Primjer osvježenih podataka vidi se na slici 3.17.

Slika 3.15.: Podaci o Windows agentu

Slika 3.16.: Potvrda ključa autentikacije

Slika 3.17.: Nove informacije o agentu

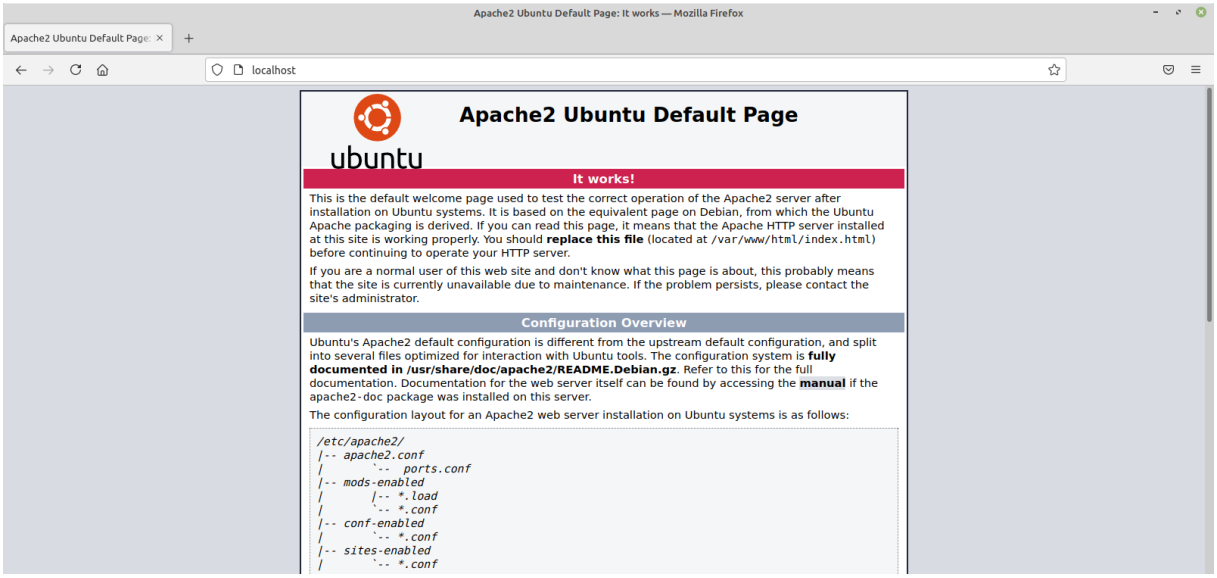
3.2. Instalacija i konfiguracija OSSEC web poslužitelja

U ovom radu koristi se PHP verzija 7.4, Apache verzija 2.4 i MySQL verzija 8.0. Za instalaciju i konfiguraciju koristi se komandna linija na virtualnom stroju na kojem je podignut Linux Mint. Na istom virtualnom stroju podignut je OSSEC poslužitelj. Kako bi se osiguralo da je sve na operacijskom sustavu ažurirano, u komandnoj liniji pokreće se naredba `sudo apt update`. Ova naredba preuzima nove podatke o svim paketima iz konfiguriranih izvora. U slučaju da neki paketi moraju biti nadograđeni, u komandnoj liniji će biti ispisano koji su to paketi. Nadogradnja paketa obavlja se naredbom `sudo apt upgrade`. Nakon što su svi paketi na sustavu ažurirani, prvi korak je instalacija Apache poslužitelja koja se pokreće naredbom `sudo apt install apache2`. Naredba `apt`, koja je uslužni program naredbenog retka za instaliranje, uklanjanje i ažuriranje unaprijed pripremljenih paketa, u komandnoj liniji će ispisati koji paketi će biti instalirani i koliko će se dodatnog prostora zauzeti na disku. Prema zadanim postavkama, Apache poslužitelj je odmah nakon instalacije aktivan, a njegov status može se provjeriti naredbom `systemctl status apache2` ili `service apache2 status` što je prikazano na slici 3.18.

```
linuxvb@lauraVB:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2021-06-26 15:34:53 CEST; 18min ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 634 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 749 (apache2)
      Tasks: 11 (limit: 4613)
     Memory: 55.4M
     CGroup: /system.slice/apache2.service
             ├─ 749 /usr/sbin/apache2 -k start
             ├─ 796 /usr/sbin/apache2 -k start
             ├─ 801 /usr/sbin/apache2 -k start
             ├─ 818 /usr/sbin/apache2 -k start
             ├─2056 /usr/sbin/apache2 -k start
             ├─2100 /usr/sbin/apache2 -k start
             ├─2105 /usr/sbin/apache2 -k start
             ├─2106 /usr/sbin/apache2 -k start
             ├─2299 /usr/sbin/apache2 -k start
             ├─2305 /usr/sbin/apache2 -k start
             └─2310 /usr/sbin/apache2 -k start
```

Slika 3.18.: Status Apache poslužitelja

Prema zadanim postavkama, Apache poslužitelj je već konfiguriran za obradu zahtjeva na lokalnom računalu (engl. *localhost*). Za pristup poslužitelju, potrebno je otvoriti bilo koji web preglednik, i upisati `http://localhost/`, što će nakon pretraživanja dovesti do zadane web stranice Apache poslužitelja. Zadana web stranica prikazana je na slici 3.19.



Slika 3.19.: Zadana web stranica Apache poslužitelja

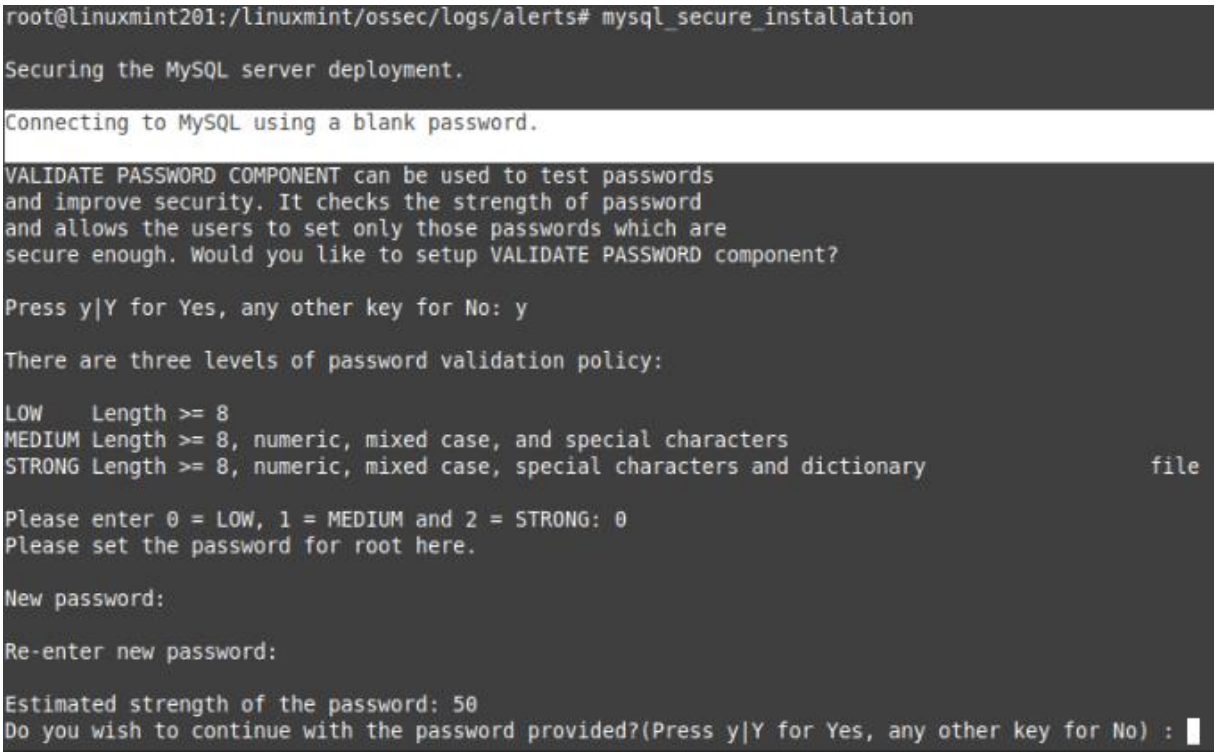
Osim upisivanja `http://localhost/`, moguće je i upisati `http://127.0.0.1/` što također označava lokalno računalo. Konfiguracija lokalnog računala može se vidjeti upisivanjem naredbe `cat /ect/hosts` u komandnoj liniji gdje je prikazana njegova IP-adresa 127.0.0.1 kao što je vidljivo na slici 3.20.

```
linuxvb@lauraVB:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       lauraVB

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

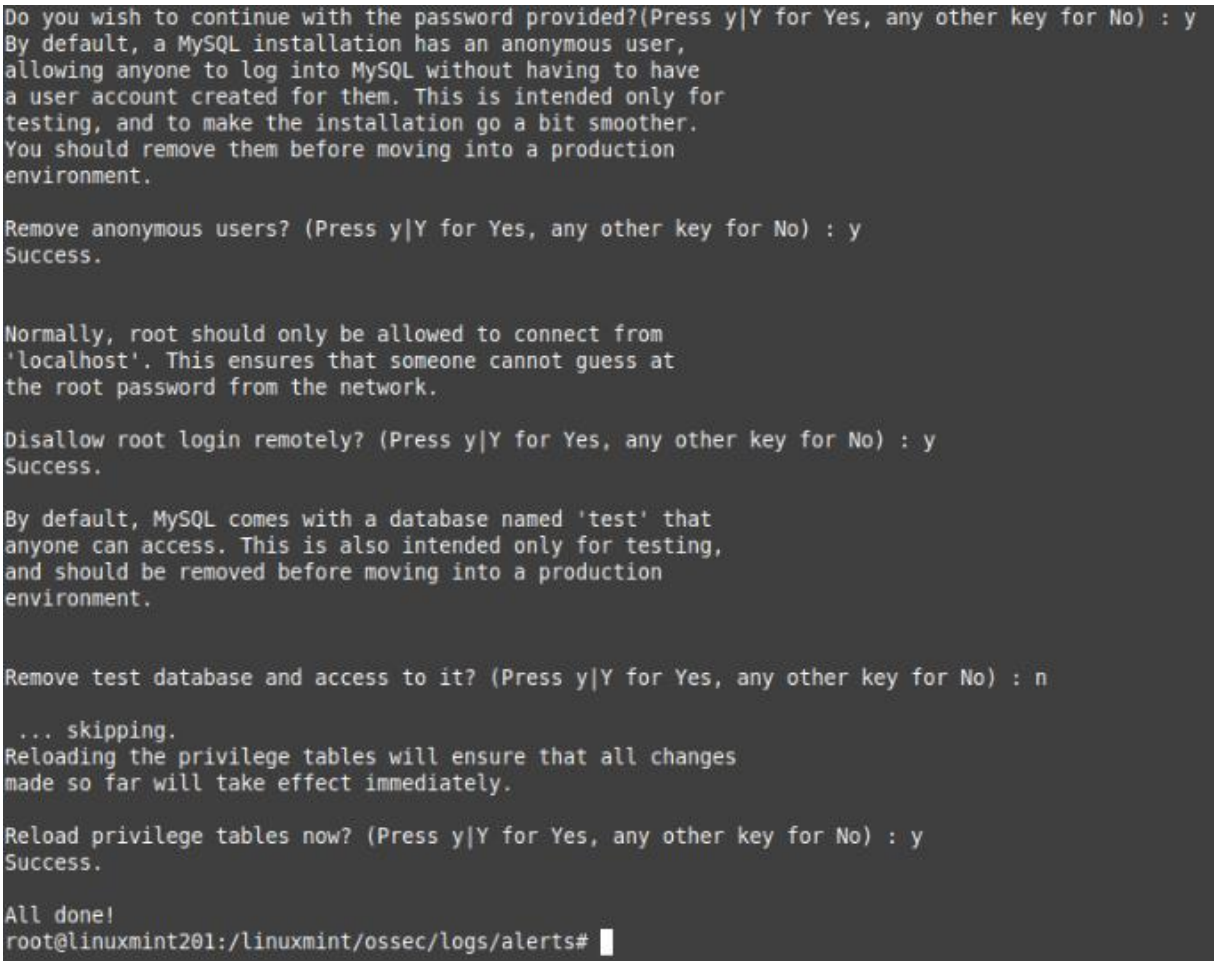
Slika 3.20.: IP postavke lokalnog računala u datoteci `/etc/hosts`

Zadana Apache web stranica može se pronaći u direktoriju `/var/www/html`, a datoteka je nazvana `index.html`. Prema zadanim postavkama, Apache poslužitelj poslužuje datoteke u tom direktoriju i u njemu se može unijeti dodatan put do lokalne mrežne adrese.

Nakon instalacije Apachea, slijedi instalacija MySQL baze podataka. Za pokretanje instalacije MySQL poslužitelja, u komandnoj liniji se koristi naredba `sudo apt install mysql-server`. Naredba `apt` će u komandnoj liniji ispisati pakete koji će biti instalirani i veličinu diska koju će zauzeti. Kada se instalacija završi, potrebno je pokrenuti sigurnosnu skriptu koja dolazi unaprijed instalirana s MySQL-om. Ta skripta se koristi kako bi se baza podataka na sustavu mogla zaključati i osigurati od vanjskih prijetnji. Za pokretanje skripte za sigurnost potrebno je u komandnu liniju upisati `sudo mysql_secure_installation`. Glavna svrha ove skripte je mogućnost osiguravanja baze, i u ovom slučaju to se postiže potvrdom dodatka za lozinku što je prikazano na slici 3.21. Na istoj slici su također prikazana tri nivoa politike provjere lozinke koja definiraju kako bi lozinka trebala izgledati. Niski nivo zahtijeva lozinku koja je duga osam ili više znakova, srednji nivo prema kojemu lozinka od osam ili više znakova mora sadržavati numeričke znakove, velika i mala slova, i specijalne znakove poput točke, upitnika, uskličnika i slično. Jaki nivo zahtijeva isti broj znakova kao i prethodna dva, te da lozinka sadržava numeričke znakove, velika i mala slova, specijalne znakove i riječi. Kada se nivo lozinke odabere, slijedi upisivanje željene lozinke za *root* korisnika koja mora biti napisana prema spomenutim pravilima.

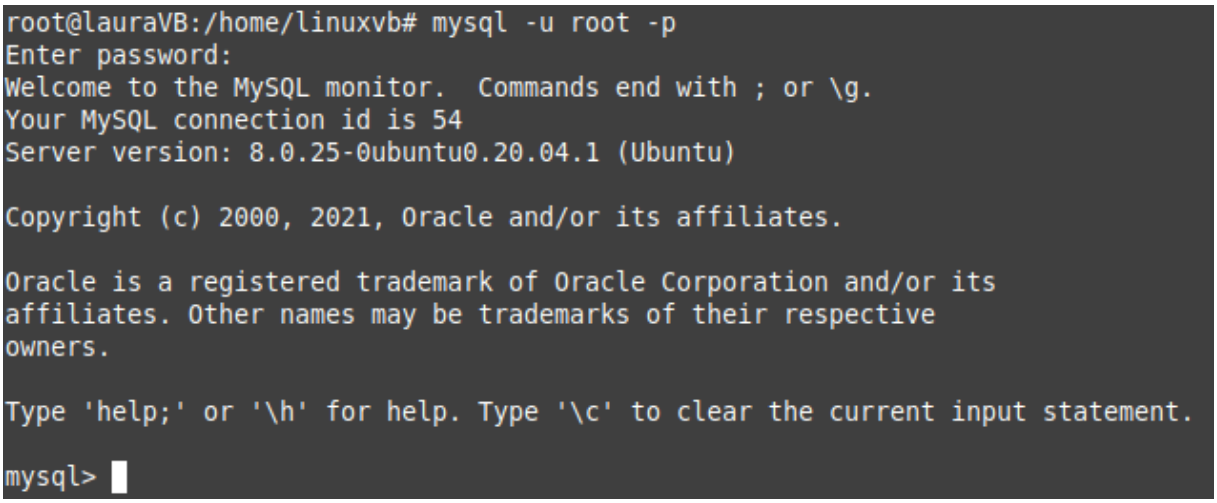


Slika 3.21.: Pokretanje sigurnosne skripte i nivoi lozinke

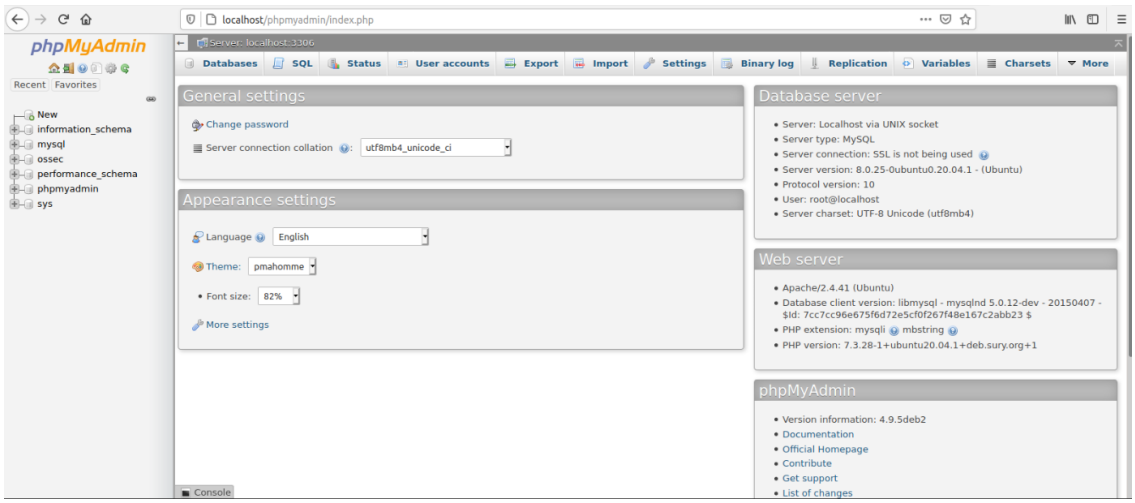


Slika 3.22.: Dodatni upiti

Postavljeni su dodatni upiti i objašnjenja o konfiguraciji MySQL-a nakon što je lozinka unesena. Prema zadanim postavkama, MySQL dolazi s anonimnim korisnikom koji se može maknuti zbog toga što omogućava pristup bilo kome u MySQL bazu čak i ako profil za tog korisnika ne postoji. Sljedeća opcija kaže kako bi *root* korisniku trebalo biti dopušteno povezivanje preko lokalnog računala, kako bi se osiguralo da netko ne može pogoditi lozinku *root* korisnika s mreže. Zatim opcija koja kaže da MySQL prema zadanim postavkama dolazi s testnom bazom podataka kojoj bilo tko može pristupiti i hoće li biti uklonjena. Sve navedeno vidljivo je na slici 3.22. Ulazak u sučelje ove baze podataka vrši se putem naredbe `mysql -u root -p`. Parametar `-u` označava koji korisnik će pristupiti bazi podataka, u ovom slučaju *root* korisnik, dok parametar `-p` zahtijeva unos lozinke za korisnika. Kako izgleda sučelje MySQL-a na operacijskom sustavu Linux vidi se na slici 3.23. Za lakše korištenje baze podataka, instalirano je web sučelje pod nazivom phpMyAdmin. phpMyAdmin je besplatni softverski alat napisan u PHP-u, te je namijenjen upravljanju MySQL-a putem weba. Instalacija ovog sučelja moguća je preko komandne linije naredbom `sudo apt install phpmyadmin`. Prilikom instalacije unose se korisničko ime i lozinka koji se koriste za pristup ovom sučelju. Nakon što je instalacija završena, pristup ovoj web stranici moguć je putem adrese `http://localhost/phpmyadmin/index.php`. Slika 3.24. prikazuje kako izgleda phpMyAdmin sučelje.



Slika 3.23.: Sučelje MySQL-a



Slika 3.24.: Web sučelje phpMyAdmin

Za instalaciju PHP-a, koristi se naredba `sudo apt install php libapache2-mod-php php-mysql php-curl php-gd php-intl php-pear php-imagick php-imap php-memcache php-ps php-pspell php-snmp php-tidy php-xmlrpc php-xsl`. Ova naredba, osim što instalira sam PHP, također uključuje dodatne pomoćne pakete kao podrška za MySQL, biblioteku jedinstvenog lokatora resursa (engl. *Uniform Resource Locator*, skraćeno URL) klijenata, obrada slika i grafička biblioteka, spremište proširenja i aplikacija pod nazivom PEAR, protokol za pristup internetskim porukama, sustav predmemoriranja i drugi. Nakon što se instalacija završi, potrebno je ponovno pokrenuti Apache poslužitelja kako bi prepoznao PHP i pravilno konfigurirao potrebne datoteke. Naredba za ponovno pokretanje Apachea je `sudo systemctl restart apache2`.

Završetkom instalacija svih potrebnih programa, slijedi instalacija OSSEC web sučelja koji se nalazi na službenoj OSSEC stranici. Može se pronaći na djelu gdje se nalaze svi paketi za instalaciju, pod nazivom *Web UI*. Nakon preuzimanja, kôd se mora izdvojiti (engl. *extract*). Pošto će web sučelje koristiti ranije postavljen Apache i PHP, potrebno je izdvojeni kôd premjestiti u direktorij koji se nalazi na putanji `/var/www/html` u kojem se nalaze same web stranice. Prema zadanim postavkama unutar direktorija nalazi se skripta index.html koja sadrži PHP kôd za web stranicu koja se dobiva upisivanjem adrese `http://localhost/` u web preglednik, kao što je ranije prikazano na slici 3.19. Zbog lakšeg rukovanja web stranicom i njenom konfiguracijom, preuzeti kôd će se premjestiti u poddirektorij. Prvi korak je iz terminala napraviti zadani direktorij naredbom `mkdir /var/www/html/ossec`. Preuzeti kôd nalazit će se u direktoriju pod nazivom ossec-wui-0.9, i sadržaj tog direktorija se mora premjestiti u

Apacheov direktorij kako bi ga mogao čitati. To se postiže naredbom `mv ossec-wui-0.9/* /var/www/html/ossec`.

Sljedeći korak je pokretanje skripte za postavljanje OSSEC web sučelja. Skripta se pokreće iz direktorija `/var/www/html/ossec` naredbom `./setup.sh` kao *root* korisnik. Konfiguracija traži da se unese korisničko ime i lozinka kojim će se sigurno pristupati OSSEC web sučelju. Potrebno je još unijeti ime korisnika pod kojim se pokreće web poslužitelj, u ovom slučaju je to korisnik www-data i time se završava konfiguracija web sučelja kao što se vidi na slici 3.25.

```
root@lauraVB:/etc/apache2# cd /var/www/html/ossec
root@lauraVB:/var/www/html/ossec# ./setup.sh
trap: SIGHUP: bad trap
Setting up ossec ui...

Username: laura
New password:
Re-type new password:
Adding password for user laura
Enter your web server user name (e.g. apache, www, nobody, www-data, ...)
www-data

Setup completed successfully.
```

Slika 3.25.: Konfiguracija OSSEC web sučelja

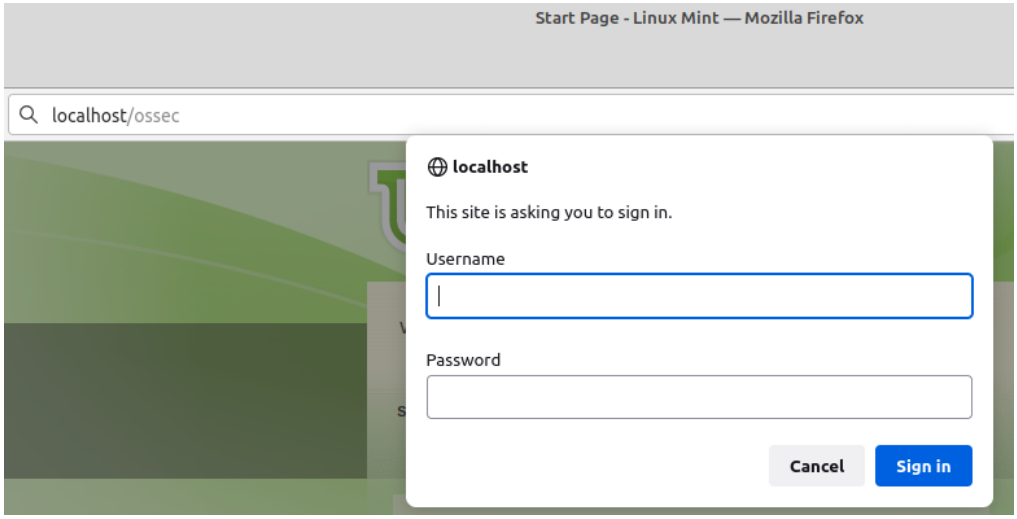
Pristupanje OSSEC webu preko web preglednika moguće je putem adrese `http://localhost/ossec`, što direktno dovodi do željene stranice bez ikakvih sigurnosti i pitanja o korisničkom imenu i lozinki. Ovaj problem nastaje jer je konfiguracija Apachea ostala prema zadanim postavkama koje ne uključuju .htaccess. Postavljanjem datoteke .htaccess omogućuje se korištenje korisničkog imena i lozinke postavljene prilikom pokretanja skripte setup.sh. .htaccess je konfiguracijska datoteka koju koristi Apache web poslužitelj ako je pri pokretanju pronađe. Datoteka se može koristiti kako bi se uključile ili isključile dodatne funkcije od kojih je jedna zaštita web stranice lozinkom. [13] Za omogućavanje dodatne funkcije zaštite lozinkom, potrebno se prebaciti u direktorij `/etc/apache2`. U tom direktoriju nalazi se konfiguracija samog Apachea, pod nazivom apache2.conf. Otvaranjem te datoteke programom za uređivanje teksta, potrebno je promijeniti dio koji se odnosi na direktorij `/var/www`, u kojem se nalaze sve web stranice kojima se pristupa preko Apache poslužitelja. Unutar dijela kôda označenog s `/var/www`, nalazi se opcija *AllowOverride* koja je prema zadanim postavkama postavljena u vrijednost *None* (nitko). Promjenom *None* u *All*, .htaccess

je uključen i Apache će pri svakom pristupu sadržaju tog direktorija tražiti korisničko ime i lozinku. Pravilno napisan kôd prikazan je na slici 3.26.

```
# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
</Directory>
```

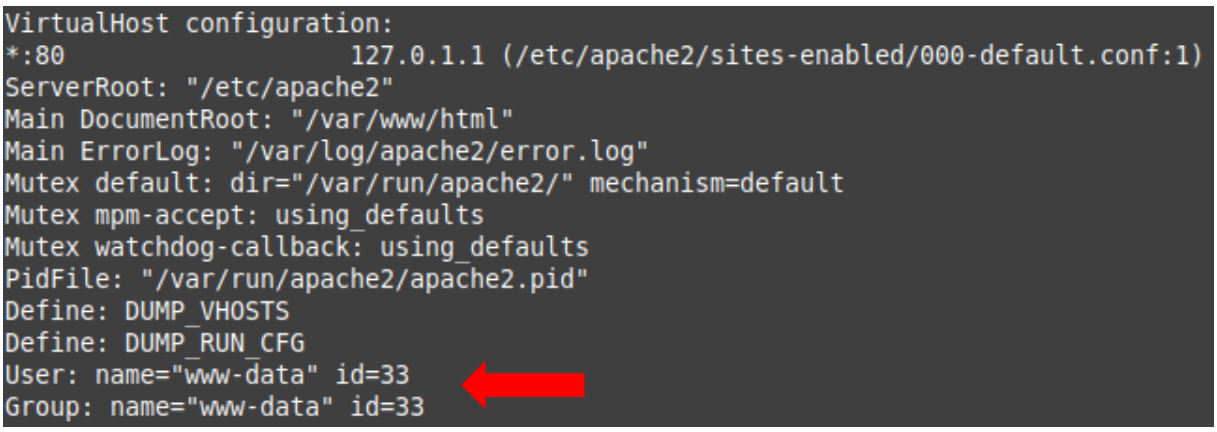
Slika 3.26.: Ispravno napisan kôd za .htaccess

Kako bi .htaccess mogao utjecati na OSSEC web stranicu, potrebno je ponovno pokrenuti skriptu setup.sh čime se u direktoriju `/var/www/html/ossec` postavljene nove datoteke .htaccess i .htpasswd jer je sada Apache omogućio funkciju traženja lozinke za OSSEC web. Slika 3.27. pokazuje da se prilikom upisivanja adrese `http://localhost/ossec`, zatražilo korisničko ime i lozinka.



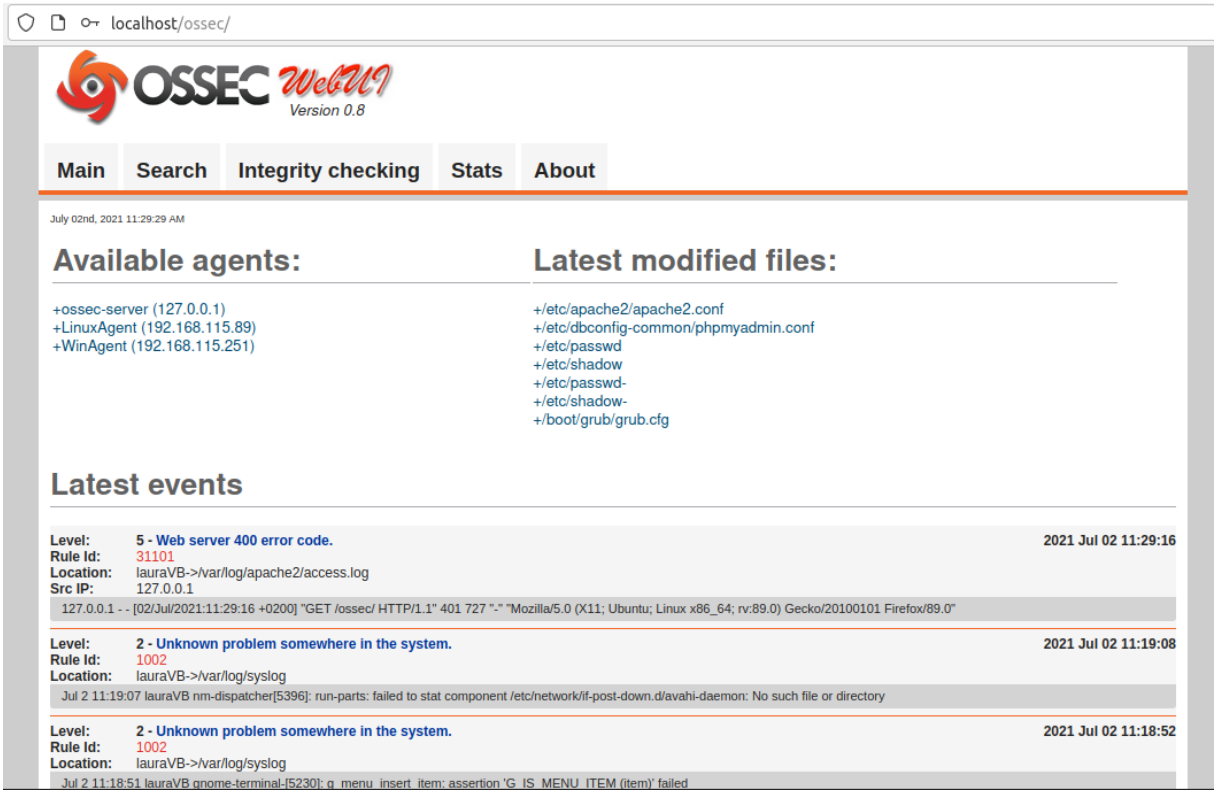
Slika 3.27.: Traženje lozinke i korisničkog imena

Pristupom na web stranicu sustava za detekciju napada, jedino vidljivo su naslov i različite kategorije koje se mogu pogledati, ostatak stranice je prazan. Jedna od uloga ovog sustava za detekciju je pregledavanje zapisnika, pa je potrebno omogućiti da Apache poslužitelj ima pristup zapisnicima koje OSSEC provjerava. Kako bi se to omogućilo, prvi korak je ustanoviti pod kojim korisnikom i kojom grupom se pokreće Apache. To se postiže upisivanjem naredbe `apache2ctl -S` u komandnu liniju. Naredba `apache2ctl` je *front end* Apache poslužitelja koja je dizajnirana da pomogne administratoru upravljanje Apache uslugom. [14] Opcija `-S` je sinonim dviju naredbi u jednoj, `-t -D DUMB_VHOSTS` koja izlista informacije o raščlanjenim postavkama virtualnog računala, i `-D DUMP_RUN_CFG` koja prikaže raščlanjene postavke pokretanja. Potrebne informacije vide se na slici 3.28.



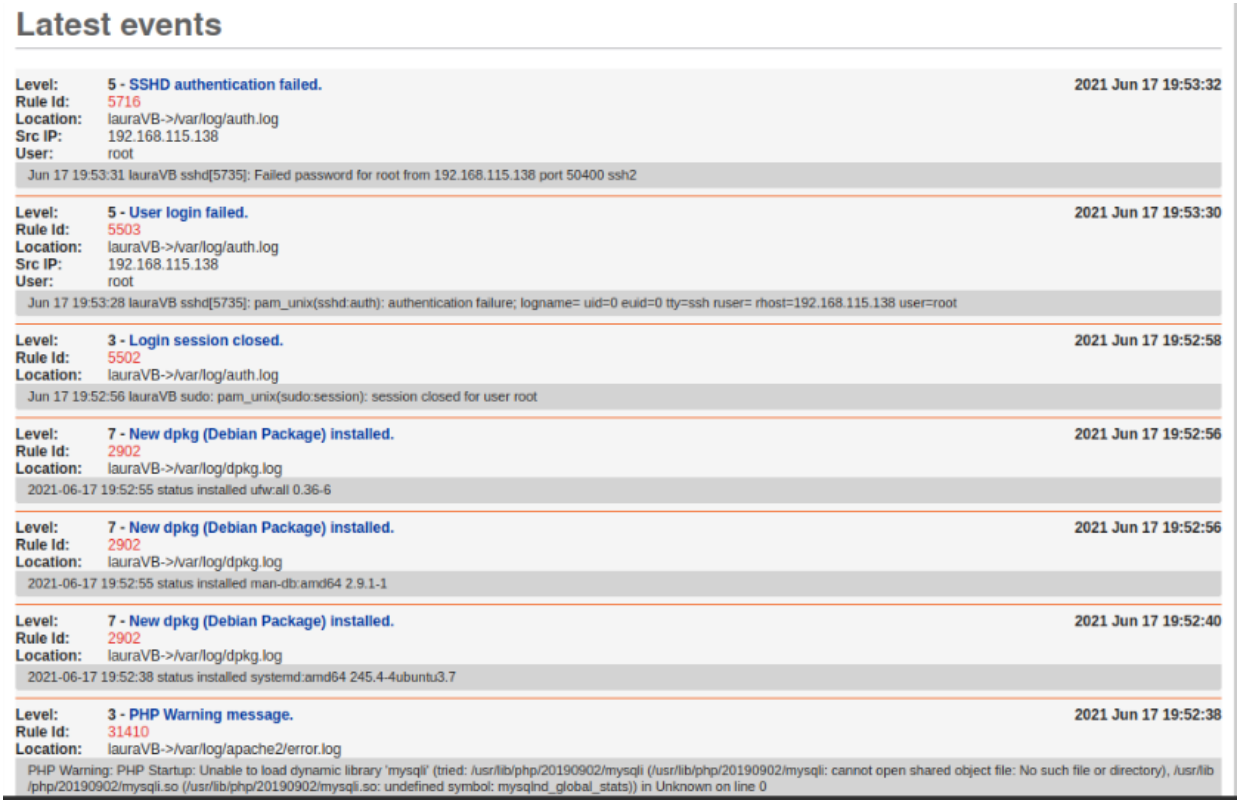
Slika 3.28.: Informacije o postavkama virtualnog računalima i pokretanja

Svi zapisnici koje OSSEC prikuplja, nalaze se u direktoriju `/var/ossec/logs`. Kako bi web sučelje moglo čitati i prikazivati zapise, Apache mora imati pristup tim podacima. Pomicanjem u direktorij `/var/ossec`, putem komandne linije pokreće se naredba `chgrp -R www-data logs`. Naredba `chgrp` mijenja grupu koja je vlasnik direktorija *logs* na www-data čime se omogućuje web poslužitelju pristup podacima u njemu, dok opcija `-R` radi rekurzivne promjene na cijelu strukturu direktorija. Potrebno je također omogućiti da grupa www-data ima pristup OSSEC-ovom web sajtu kako bi Apache mogao čitati konfiguraciju ovog sajta. Naredbom `chown :www-data /var/www/html/ossec`, grupa www-data sada uz *root* korisnika ima pristup svim podacima unutar `/var/www/html/ossec`. Nakon što je konfiguracija OSSEC-a i Apachea gotova, sada je moguće sigurno pristupiti web stranici koji će prikazivati zapisnike različitih razina i sadržaja. Na slici 3.29. može se vidjeti da su sada vidljivi agenti povezani s poslužiteljem koje on nadgleda, datoteke koju su nedavno modificirane, razne kategorije koje se mogu odabrati te nedavne aktivnosti iz zapisnika.



Slika 3.29.: OSSEC web sučelje

Zapisnici koje OSSEC prikazuje mogu biti različiti. Mogu se odnositi na nove pakete koji su instalirani na operacijskom sustavu, otvorene ili zatvorene sesije za *root* korisnika, mogu prikazivati PHP pogreške, poznate ili nepoznate pogreške unutar sustava, nepravilne konfiguracije i unutar koje datoteke se nalaze, ali najbitnije od svega što prikazuju kada je netko drugi pokušao pristupiti kao *root*, odnosno pokušaj neovlaštenog pristupa sustavu. Kako neki od tih upozorenja izgledaju, prikazano je na slici 3.30. Na istoj slici, prvo i drugo upozorenje se pojavljuju jer je s operacijskog sustava Kali Linux namjerno simuliran pokušaj upada kao *root* korisnik na samog poslužitelja, pri čemu sustav za detekciju napada javlja s koje IP-adrese dolazi pokušaj napada i s kojeg mrežnog priključka.



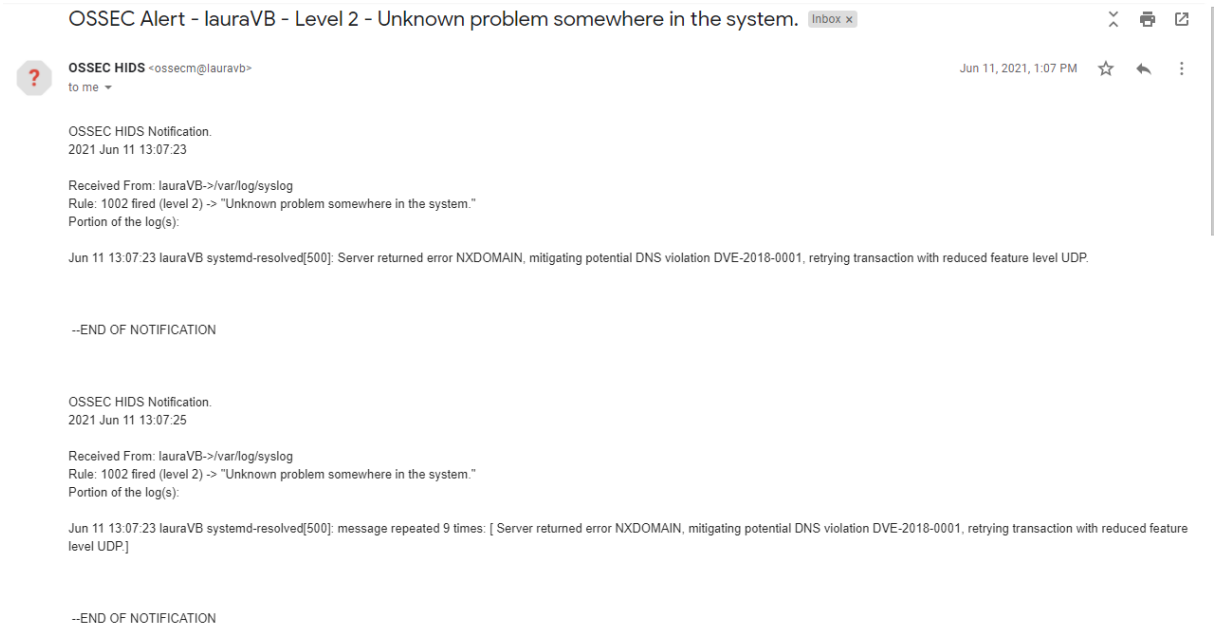
Slika 3.30.: Razni zapisnici i upozorenja

Kao što je ranije spomenuto, OSSEC ima mogućnost slati upozorenja putem elektroničke pošte za što je potrebno instalirati odgovarajući poslužitelj. Odabran je *sendmail* poslužitelj. Ako već ranije nije prisutan na sustavu, instalacija je moguća preko komandne linije, naredbom `apt install sendmail`. Ukoliko je odabrano slanje elektroničke pošte tokom instalacije, u OSSEC-ovoj konfiguracijskoj datoteci mogu se provjeriti detalji, ili, ukoliko je potrebno, promijeniti ih. Ta konfiguracijska datoteka se nalazi na putanji `/var/etc/ossec/`, a naziv joj je ossec.conf. Otvaranjem datoteke u nekom od uređivača teksta kao što je Vim, odmah na početku je vidljiva konfiguracija za elektroničku poštu, kao na slici 3.31.

```
<ossec_config>
  <database_output>
        <hostname>localhost</hostname>
        <username>user</username>
        <password>ZaRa2021!</password>
        <database>ossec</database>
        <type>mysql</type>
   </database_output>

  <global>
    <email_notification>yes</email_notification>
    <email_to>laura.gregorek@gmail.com</email_to>
    <smtp_server>alt1.gmail-smtp-in.l.google.com.</smtp_server>
    <email_from>ossecm@lauraVB</email_from>
  </global>
```

Slika 3.31.: OSSEC konfiguracija za *e-mail*

Za vrijeme konfiguracije i postavljanja potrebnih stvari za ovaj rad, niti jedno upozorenje putem elektroničke pošte nije poslano sa strane OSSEC-a. Dolaskom na fakultet i promjenom IP-adrese i DNS-a samog virtualnog stroja na kojem se nalazi OSSEC poslužitelj, *e-mail* o upozorenjima dolazi. Razlog tomu je što spomenuti fakultet koristi obrnuto DNS pretraživanje (engl. *reverse DNS lookup*). S uobičajenim DNS pretraživanjem, postavlja se upit DNS-u kako bi se na osnovu imena računala dobila IP-adresa. Obrnutim DNS pretraživanjem postavlja se upit koji na osnovu IP-adrese vraća ime računala. Iz sigurnosnih razloga OSSEC može slati upozorenja putem *e-maila* samo ako je IP-adresa poslužitelja unesena u datoteku koja omogućava obrnuto pretraživanje. Primjer upozorenja primljenog putem pošte vidljivo je na slici 3.32.



Slika 3.32.: Upozorenje na elektroničkoj pošti

3.3. Instalacija i konfiguracija sustava AnaLogi

Vlastito OSSEC web sučelje (Web UI) prilično je oskudno, te je tim programera razvio grafički bogatije sučelje pod nazivom AnaLogi. Naziv dolazi od skraćenice za *Analytical Log Interface*. Ovo grafičko sučelje dizajnirano je da se pokreće i funkcionira na OSSEC poslužitelju i pruža više vizualnih informacija od standardnog web sučelja. OSSEC u svojoj konfiguraciji dolazi s potrebnom shemom koju AnaLogi treba za pristup bazi podataka. AnaLogi za svoj rad zahtijeva da su na sustavu instalirani MySQL i web poslužitelj koji podržava PHP. Dosad u ovom radu, sve potrebno za AnaLogi je instalirano, pa je sljedeći korak potrebna konfiguracija programa kako bi ovo grafičko sučelje moglo pravilno raditi. Prvi korak

je konfiguracija MySQL-a, jer kako bi ovo grafičko sučelje moglo pristupati podacima, potrebno je kreirati u MySQL-u bazu podataka pod imenom ossec i novog korisnika koji može pristupati toj bazi. Iz komandne linije je potrebno ući u MySQL sučelje kao *root* korisnik, upisivanjem naredbe `mysql -u root -p`. Sada se iz sučelja MySQL-a, kreira nova baza podataka pod imenom ossec, koristeći naredbu `create database ossec;`. Zatim je potrebno kreirati korisnika koji će moći pristupati ovoj bazi i čitati potrebne podatke iz nje, dodavati, brisati, kreirati i drugo. Kreiranje korisnika na MySQL-u moguće je naredbom `CREATE USER 'username'@'localhost' IDENTIFIED BY 'password';`. Da bi novokreirani korisnik mogao izvršavati određene funkcije nad bazom, potrebno mu je dodijeliti prava. Ponovno unutar MySQL sučelja, upisuje se naredba `grant INSERT,SELECT,UPDATE,CREATE,DELETE,EXECUTE on ossec.* to username;`. Kako bi se određene dozvole i promjene primijenile na korisnika, potrebno je resetirati privilegije naredbom `FLUSH PRIVILEGES;`. Sada korisnik može slobodno odrađivati sve funkcije koje su mu dozvoljene nad bazom ossec. Ranije spomenuta shema koja dolazi s OSSEC-om, sada se treba prebaciti u novu bazu podataka ossec, a putanja na kojoj se nalazi je `/home/linuxvb/ossec-hids-3.6.0/src/os_dbd`. Unutar direktorija os_dbd nalazi se potrebna shema pod nazivom mysql-schema. Kako bi se ta shema prebacila unutar ossec baze podataka, potrebno je ući u direktorij os_dbd. Preko komandne linije kao *root* korisnik, moguće je premjestiti tu shemu jednom naredbom koja glasi `mysql -u root -p ossec < mysql.schema`. Konfiguracija baze ossec s novim korisnikom, treba se dodati u samu konfiguraciju OSSEC poslužitelja kako bi se OSSEC mogao pravilno povezati s MySQL-om. OSSEC-ova konfiguracija nalazi se u datoteci pod nazivom ossec.conf, na putanji `/var/ossec/etc/ossec.conf`. Ulaskom u konfiguracijsku datoteku preko uređivača teksta, na samom početku potrebno je dodati dio kôda koji će omogućiti povezivanje s ossec bazom podataka koja se nalazi unutar MySQL-a i korisnikom koji joj može pristupiti. Potrebni kôd koji se mora dodati prikazan je na slici 3.33.

```
<ossec_config>
  <database_output>
        <hostname>localhost</hostname>
        <username>user</username>
        <password>ZaRa2021!</password>
        <database>ossec</database>
        <type>mysql</type>
   </database_output>
```

Slika 3.33.: Dio OSSEC konfiguracije za povezivanje s bazom podataka

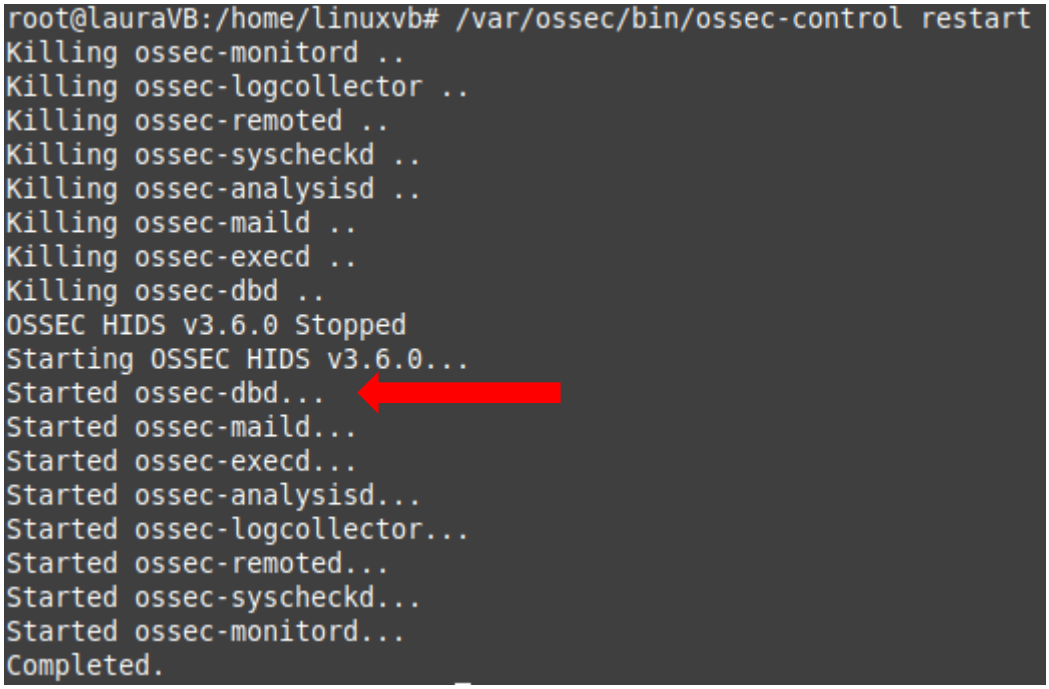
Nakon dodavanja dijela konfiguracije za ossec bazu, konfiguracijsku datoteku potrebno je spremiti, a novu bazu podataka omogućiti. Baza se omogućuje naredbom pokrenutom iz terminala koja glasi `sudo /var/ossec/bin/ossec-control enable database`. Kako bi OSSEC primijenio nove promjene, potrebno ga je ponovno pokrenuti naredbom `sudo /var/ossec/bin/ossec-control restart`. Nakon ponovnog pokretanja, OSSEC javlja grešku vezanu za novo konfiguriranu i pokrenutu bazu podataka, vidljivo na slici 3.34.

```
root@linuxmint201:/home/linuxmint# /linuxmint/ossec/bin/ossec-control restart
Killing ossec-monitord ..
Killing ossec-logcollector ..
Killing ossec-remoted ..
Killing ossec-syscheckd ..
Killing ossec-analysisd ..
Killing ossec-maild ..
Killing ossec-execd ..
ossec-dbd not running ..
OSSEC HIDS v3.6.0 Stopped
Starting OSSEC HIDS v3.6.0...
2021/07/03 18:50:03 ossec-dbd(5207): ERROR: OSSEC not compiled with support for 'mysql'.
2021/07/03 18:50:03 ossec-dbd(1202): ERROR: Configuration error at '/linuxmint/ossec/etc/ossec.conf'. Exiting.
ossec-dbd did not start correctly.
```

Slika 3.34.: Greška o pokretanju baze podataka

Greška koja se pojavila govori kako OSSEC nije sastavljen s podrškom za MySQL, i da je unutar konfiguracijskog kôda došlo do greške zbog dodanog kôda koji podržava novu bazu podataka. Za rješenje ovog problema prilikom izrade praktičnog dijela, bilo je potrebno naći izvor i uzrok ovih grešaka. Nakon istraživanja, ispostavilo se kako se podrška MySQL-a mora omogućiti prije same instalacije OSSEC poslužitelja kroz nekoliko koraka. Prvo je potrebno osigurati da su na sustavu prisutni svi potrebni paketi naredbom `sudo apt-get install build-essentials libmysqlclient-dev`. Nakon instalacije paketa, sa službene web stranice OSSEC-a treba preuzeti OSSEC dokumentaciju. Unutar dokumentacije nalazi se skripta koja kada se pokrene, omogući podršku za MySQL. Za ovu verziju OSSEC-a potrebna skripta nalazi se na putanji `/home/linuxvb/ossec-hids-3.6.0/src/os_dbd`. Ulaskom u direktorij os_dbd, i izlistom njenog sadržaja, vidljiva je skripta pod nazivom dbmake.sh. Pokretanjem te skripte kao *root* korisnik, OSSEC se kompilirao na način da sada ima podršku za MySQL bazu podataka. Prije instalacije OSSEC-a, uz pretpostavku da se MySQL već nalazi na sustavu, potrebno je ponoviti korake konfiguracije nove baze podataka i korisnika koji će moći obavljati funkcije nad njom. Postupak je isti, iz MySQL ljuske kreiranje baze podataka pod nazivom ossec, `create database ossec;`, kreiranje korisnika `CREATE USER 'username'@'localhost' IDENTIFIED BY 'password';`, i dodjeljivanje prava i dozvole tom korisniku `grant INSERT,SELECT,UPDATE,CREATE,DELETE,EXECUTE on ossec.* to username;`. Kad je baza podataka konfigurirana, potrebno je prebaciti shemu

mysql.schema iz OSSEC direktorija os_dbd u ossec bazu podataka koja se nalazi unutar MySQL-a. Tek kada je osigurano da su ove stvari prvo konfigurirane, OSSEC poslužitelj se može instalirati. Nakon završene instalacije potrebno je u konfiguracijsku datoteku ossec.conf ubaciti kôd koji će unutar ovog poslužitelja povući potrebne podatke o bazi podataka s kojom onda može rukovati. Kôd je isti, prikazan na slici 3.34. Zatim sa strane poslužitelja treba omogućiti bazu podataka, naredbom `sudo /var/ossec/bin/ossec-control enable database`. Ponovnim pokretanjem OSSEC-a, sada je vidljivo da se podrška za bazu podataka pravilno konfigurirala kao što se vidi na slici 3.35.



Slika 3.35.: Pravilno pokrenuta baza podataka

Pravilnom konfiguracijom svih potrebnih programa i samog sustava za detekciju napada, moguće je na kraju instalirati dodatno grafičko web sučelje poslužitelja korištenog u ovom radu. Instalacija AnaLogija se sastoji od kloniranja Github spremišta u potrebni direktorij i uređivanja datoteke postavki grafičkog sučelja. Kao *root* korisnik u komandnoj liniji, potrebno se prebaciti u direktorij `/var/www/html` naredbom `cd /var/www/html`. Unutar tog direktorija sa stranice Github, klonirati će se spremište sa svim AnaLogi datotekama naredbom `git clone https://github.com/ECSC/analogi.git`. Nakon što se preuzimanje završi, zbog potrebe promjene određenih parametara u konfiguracijskoj datoteci, prvo će se napraviti njena kopija. Naredbom `cp analogi/db_ossec.php.new analogi/db_ossec.php` kao *root* korisnik, datoteka za konfiguraciju ossec baze podataka je kopirana. Ulaskom u datoteku db_ossec.php, parametri koji se odnose na ime baze, ime

korisnika, lozinku korisnika i računala su isti koji su bili kreirani unutar MySQL-a. Definirani parametri unutar datoteke db_ossec.php mogu se vidjeti na slici 3.36.

```php
<?php
/*
 * Copyright (c) 2012 Andy 'Rimmer' Shepherd <andrew.shepherd@ecsc.co.uk> (ECSC Ltd).
 * This program is free software; Distributed under the terms of the GNU GPL v3.
 */

define ('DB_USER_O', 'user');
define ('DB_PASSWORD_O', 'ZaRa2021!');
define ('DB_HOST_O', 'localhost');
define ('DB_NAME_O', 'ossec');
```

Slika 3.36.: Konfiguracija AnaLogija

Unošenjem podataka u ovu konfiguracijsku datoteku, sve potrebno za rad OSSEC-a je ispravno konfigurirano. Pristup grafičkom sučelju AnaLogi moguć je putem bilo kojeg web preglednika, na adresi `http://localhost/analogi`. Odlaskom na tu web stranicu, ništa nije prikazano i web stranica je u potpunosti prazna. Kako bi se otkrio uzrok zašto na stranici ništa nije prikazano, potrebno je naći datoteku u kojoj se spremaju zapisnici o greškama. U ovom slučaju, pretpostavlja se da je problem u Apacheu ili PHP-u pošto je sva ostala dokumentacija do sada pravilno konfigurirana. Direktorij unutar kojeg će se pronaći bilo kakve vrste zapisnika, nalazi se na putanji `/var/log`. Tamo je smješten i direktorij s raznim zapisnicima o Apacheu, pod nazivom apache2. Ulaskom u direktorij apache2, vidljiva je datoteka pod imenom error.log. Kako bi se greške mogle pročitati, potrebno je tu datoteku otvoriti u jednom od uređivača teksta. Prikazane greške na slici 3.37. javljaju PHP upozorenja u nekoliko datoteka.

```
[Mon Jun 07 13:52:29.538849 2021] [core:notice] [pid 11776] AH00094: Command line: '/usr/sbin/apache2'
[Mon Jun 07 13:52:31.795327 2021] [php7:warn] [pid 11778] [client 127.0.0.1:52240] PHP Warning:  mysqli_query() expects parameter
1 to be mysqli, string given in /var/www/html/analogi/index.php on line 18, referer: http://localhost/analogi/
[Mon Jun 07 13:52:31.795424 2021] [php7:warn] [pid 11778] [client 127.0.0.1:52240] PHP Warning:  mysqli_query() expects parameter
1 to be mysqli, string given in /var/www/html/analogi/index.php on line 47, referer: http://localhost/analogi/
[Mon Jun 07 13:52:31.803188 2021] [php7:warn] [pid 11778] [client 127.0.0.1:52240] PHP Warning:  mysqli_query() expects parameter
1 to be mysqli, string given in /var/www/html/analogi/php/index_graph.php on line 109, referer: http://localhost/analogi/
[Mon Jun 07 13:52:31.809045 2021] [php7:warn] [pid 11778] [client 127.0.0.1:52240] PHP Warning:  mysqli_query() expects parameter
1 to be mysqli, string given in /var/www/html/analogi/php/index_graph.php on line 250, referer: http://localhost/analogi/
[Mon Jun 07 13:52:31.809096 2021] [php7:warn] [pid 11778] [client 127.0.0.1:52240] PHP Warning:  mysqli_query() expects at least 2
 parameters, 1 given in /var/www/html/analogi/php/index_graph.php on line 294, referer: http://localhost/analogi/
[Mon Jun 07 13:52:31.815288 2021] [php7:warn] [pid 11778] [client 127.0.0.1:52240] PHP Warning:  mysqli_query() expects parameter
1 to be mysqli, string given in /var/www/html/analogi/php/topid.php on line 41, referer: http://localhost/analogi/
[Mon Jun 07 13:52:31.817519 2021] [php7:warn] [pid 11778] [client 127.0.0.1:52240] PHP Warning:  mysqli_query() expects parameter
1 to be mysqli, string given in /var/www/html/analogi/php/toplocation.php on line 43, referer: http://localhost/analogi/
[Mon Jun 07 13:52:31.820911 2021] [php7:warn] [pid 11778] [client 127.0.0.1:52240] PHP Warning:  mysqli_query() expects parameter
1 to be mysqli, string given in /var/www/html/analogi/php/toprare.php on line 31, referer: http://localhost/analogi/
```

Slika 3.37.: PHP upozorenja vezana za AnaLogi

Lako se uočava upozorenje koje se javlja za isti problem na nekoliko različitih mjesta. U pet različitih datoteka, indeks.php, index_graph.php, topid.php, toplocation.php i toprare.php, greška javlja kako se očekuje parametar pod nazivom mysqli. Razlog tomu je što je sučelje AnaLogi dizajnirano za starije verzije PHP-a i MySQL-a, a u ovom radu korištene su najnovije

verzije tih programa. Za verzije PHP-a iznad 5.0, uvedene su promjene poput ovog parametra kako bi PHP mogao pristupati novijim verzijama MySQL-a, verzije 4.1 ili novije. Pošto je PHP skritpni jezik, rješenje ovog problema je zamjena potrebnih parametara unutar kôda, kako bi verzija PHP-a bila kompatibilna s verzijom MySQL-a. Ukoliko mysqli ekstenzija ne postoji za PHP koji se nalazi na sustavu, može se instalirati naredbom `sudo apt-get install php7.4-mysqli`. Otvaranjem u nekom od uređivača teksta sve ranije navedene datoteke koje se nalaze na putanji `/var/www/html/analogi`, mogu se ispraviti sve varijable koje se nalaze na određenim linijama u kôdu. Greška se također javila u samoj konfiguracijskoj datoteci za AnaLogi, db_ossec.php. Nakon korekcije kôda, konačan izgled ove datoteke vidljiv je na slici 3.38.

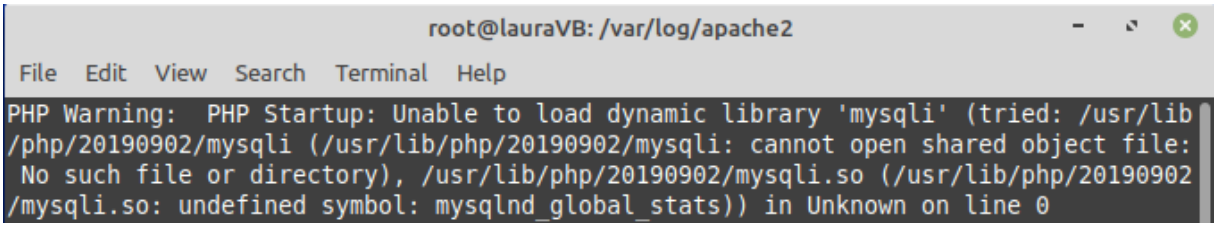
```php
<?php
/*
 * Copyright (c) 2012 Andy 'Rimmer' Shepherd <andrew.shepherd@ecsc.co.uk> (ECSC
 Ltd).
 * This program is free software; Distributed under the terms of the GNU GPL v3
.
 */

define ('DB_USER_O', 'user');
define ('DB_PASSWORD_O', 'ZaRa2021!');
define ('DB_HOST_O', 'localhost');
define ('DB_NAME_O', 'ossec');

$db_ossec = mysqli_connect (DB_HOST_O, DB_USER_O, DB_PASSWORD_O) OR die ('Could
 not connect to SQL : ' . mysqli_error() . "<br/>Click <a href='' onclick='docu
ment.cookie=\"ossecdbjs=;expires=Thu, 01 Jan 1970 00:00:00 GMT\"' >HERE</a> to
select your main OSSEC DB");

mysqli_select_db ($db_ossec, DB_NAME_O) OR die ('Could not select the database
: ' . mysqli_error() . "<br/>Click <a href='' onclick='document.cookie=\"ossecd
bjs=;expires=Thu, 01 Jan 1970 00:00:00 GMT\"' >HERE</a> to select your main OSS
EC DB");

?>
```

Slika 3.38.: Konačna konfiguracija AnaLogija

Završetkom svih potrebnih promjena koje su javljale greške, na stranici grafičkog sučelja prikazuje se tekst vidljiv na slici 3.39.

Slika 3.39.: Web sučelje AnaLogija

Prvo je prikazano kako nema dostupnih podataka za ovaj upit i kako je pokrenuta dijagnostika. Dijagnostika pokazuje 4 testa. Prvi test kaže kako PHP ne može otkriti MySQL modul mysql_connect koji za potrebe novijih verzija ovih programa mora biti noviji modul mysqli_connect. Drugi test potvrđuje da su PHP i MySQL povezani. Treći test se odnosi na MySQL shemu koju je prije same instalacije OSSEC-a bilo potrebno prebaciti u MySQL. Iz nepoznatih razloga, shemu nije bilo moguće prebaciti u bazu podataka, bez obzira na koji način se pokušalo i koliko puta. Zadnji test govori kako nema nikakvih podataka u bazi, te kako se treba osigurati da agenti zapisuju podatke. U ovom slučaju agenti nisu bili povezani s poslužiteljem, pa iz tog razloga sustav nije mogao prikupljati njihove zapisnike ni podatke. Istraživanje kako omogućiti novi mysqli modul za AnaLogi bilo je bezuspješno. Nakon pokušavanja na sve načine, također nije bilo moguće naći nikakvo rješenje za uvoz sheme u bazu podataka. Ponovnim odlaskom u zapisnik s greškama vezanih za PHP, može se vidjeti greška na slici 3.40.



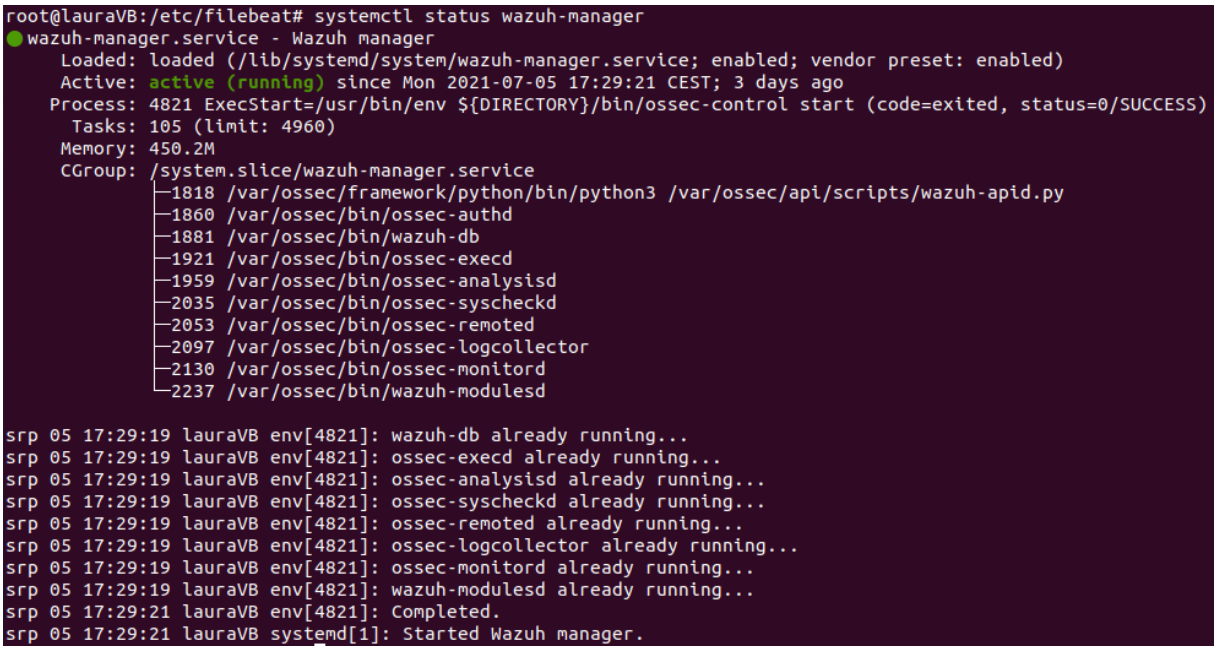
Slika 3.40.: Greška za mysqli

Zapisnik prikazuje kako prilikom PHP pokretanja, nije moguće učitati dinamičnu mysqli biblioteku. Daljnjim istraživanjem i pokušavanjem, otkriva se kako je AnaLogi dizajniran samo

za verzije OSSEC-a 2.6 i 2.7, iako se OSSEC kasnije razvijao i u radu je korištena najnovija verzija 3.6. Nove verzije OSSEC-a koje koriste nove verzije PHP-a, Apachea i MySQL, nisu kompatibilne s verzijom AnaLogija jer on podržava samo stare verzije tih programa. Primjer toga je što AnaLogi zahtijeva mysql_connect modul, ali u novim verzijama dostupan je samo mysqli_connect modul. Iako je AnaLogi samo dodatak OSSEC-u za preglednije nadziranje zapisnika, puno je praktičnije koristiti sustav za detekciju napada koji vizualno može prikazati što se događa u sustavu ili s povezanim agentima. Ovaj problem bilo je moguće riješiti samo potragom za novim sustavom za detekciju, koji će pregledavati zapisnike, upozoravati o potencijalnim napadima, prikazivati što se sve događa na sustavu i agentima, ali koji će moći prikazivati većinu tih stvari vizualno. Idealan sustav koji će pokrivati sve traženo naziva se Wazuh. U sljedećem poglavlju opisan je proces njegove instalacije i prikazane njegove funkcije.

3.4. Instalacija i konfiguracija sustava Wazuh

Instalacija Wazuha moguća je odjednom na način da se svi paketi i sve komponente instaliraju uz pomoć jedne naredbe. U ovom radu koristio se drugi način instalacije, korak po korak, gdje se svaka komponenta instalira zasebno kako bi se osigurala što točnija instalacija i potrebna konfiguracija. Za ovaj sustav koristio se novi virtualni stroj na kojem je podignut operacijski sustav Ubuntu. Prvi korak je instalacija samog Wazuh poslužitelja. Za to je potrebno preuzeti preko komandne linije sve potrebne pakete naredbom `apt install curl apt-transport-https unzip wget libcap2-bin software-properties-common lsb-release gnupg2`. Zatim se instalira GNU *Privacy Guard* ključ, `curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -`. Sljedeći korak je dodavanje spremišta naredbom `echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list` i ažuriranje informacija o novim paketima s naredbom `apt-get update`. Nakon preuzetih svih potrebnih paketa, pokretanjem naredbe `apt-get install wazuh-manager` započinje instalacija Wazuh poslužitelja. Kada se instalacija završi, Wazuh poslužitelj se treba omogućiti uz `systemctl enable wazuh-manager`. Pokretanjem `systemctl status wazuh-manager` vidjeti će se status ovog poslužitelja kao na slici 3.41.



Slika 3.41.: Status Wazuh poslužitelja

Iz ovog statusa može se vidjeti dokaz kako je Wazuh migrirao iz OSSEC-a jer se skoro sve funkcije koje koristi nalaze u direktoriju pod nazivom ossec, na putanji `/var/ossec/bin`, isto kao što je kod samog OSSEC-a. Sljedeća je instalacija Elasticsearcha naredbom `sudo apt install elasticsearch-oss opendistroforelasticsearch`. Posebno se mora preuzeti konfiguracijska datoteka za Elasticsearch komandom `sudo curl -so /etc/elasticsearch/elasticsearch.yml https://documentation.wazuh.com/4.1/resources/open-distro/elasticsearch/7.x/elasticsearch_all_in_one.yml`.

Kako bi se Kibana mogla pravilno koristiti, potrebno je dodati korisnike i pravila. Za dodavanje pravila i korisnika, potrebno je pokrenuti tri naredbe:

`curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles.yml https://documentation.wazuh.com/4.1/resources/open-distro/elasticsearch/roles/roles.yml,`

`curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles_mapping.yml https://documentation.wazuh.com/4.1/resources/open-distro/elasticsearch/roles/roles_mapping.yml,`

`curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/internal_users.yml https://documentation.wazuh.com/4.1/resources/open-distro/elasticsearch/roles/internal_users.yml.`

Dodani su korisnici wazuh_user i wazuh_manager, a njihove uloge su zaštićene i ne mogu se mijenjati iz Kibaninog sučelja. Pošto Elasticsearch koristi certifikate kako bi komunikacija u Elasticsearch klasteru bila šifrirana, sljedeći korak je generiranje i implementiranje potrebnih certifikata. Prvi korak je njihovo preuzimanje, naredbama `curl -so ~/wazuh-cert-tool.sh https://documentation.wazuh.com/4.1/resources/open-distro/tools/certificate-utility/wazuh-cert-tool.sh` i

`curl -so ~/instances.yml https://documentation.wazuh.com/4.1/resources/open-distro/tools/certificate-utility/instances_aio.yml`.

Zatim se mora pokrenuti Wazuh skripta koji kreira preuzete certifikate uz `bash ~/wazuh-cert-tool.sh`. Kako su certifikati namijenjeni za Elasticsearch, potrebno ih je premjestiti na odgovarajuću lokaciju, unutar elasticsearch direktorija. Kreirati će se novi direktorij na potrebnoj lokaciji s `mkdir /etc/elasticsearch/certs/`, premjestiti u novokreiranu datoteku s `mv ~/certs/elasticsearch* /etc/elasticsearch/certs/` i `mv ~/certs/admin* /etc/elasticsearch/certs/` i na kraju kopirati certifikati za *root* korisnika uz `cp ~/certs/root-ca* /etc/elasticsearch/certs/`. Elasticsearch dolazi sa skriptom pod nazivom *securityadmin* koja omogućava dodavanje ili modificiranje novih korisnika ili uloga. Za učitavanje svih informacija o ranije preuzetim certifikatima, potrebno je pokrenuti skriptu `export JAVA_HOME=/usr/share/elasticsearch/jdk/ && /usr/share/elasticsearch/plugins/opendistro_security/tools/securityadmin.sh -cd /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/ -nhnv -cacert /etc/elasticsearch/certs/root-ca.pem -cert /etc/elasticsearch/certs/admin.pem -key /etc/elasticsearch/certs/admin-key.pem`.

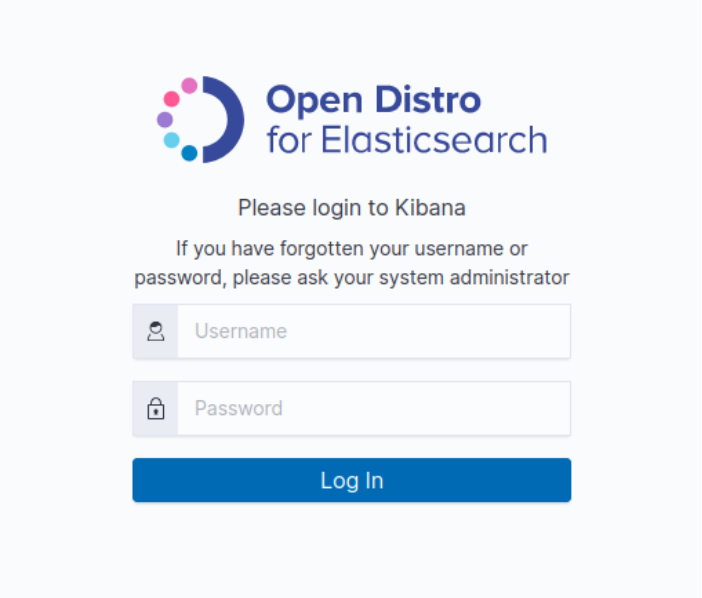
Sada su svi certifikati omogućeni i uz to su dodane sve potrebne uloge za korisnika administrator. Sljedeća je instalacija Filebeta, koja se pokreće naredbom `apt-get install filebeat`. Kad se instalacija završi, preuzet će se Filebeat konfiguracijska datoteka koja je već konfigurirana kako bi Filebeat mogao proslijediti Wazuh uzbune Elasticsearchu. Preuzimanje te datoteke moguće je uz pomoć naredbe `curl -so /etc/filebeat/filebeat.yml https://documentation.wazuh.com/4.1/resources/open-distro/filebeat/7.x/filebeat_all_in_one.yml`.

Zatim je potrebno preuzeti predložak u kojem se nalaze uzbune za Elasticsearch naredbom `curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/4.1/extensions/elasticsearch/7.x/wazuh-template.json` i dati im prava nad tim predloškom s `chmod go+r /etc/filebeat/wazuh-template.json`. Kako bi se Filebeat i Wazuh pravilno povezali, mora se preuzeti Wazuh modul za Filebeat uz pomoć naredbe `curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.1.tar.gz | tar -xvz -C /usr/share/filebeat/module`.

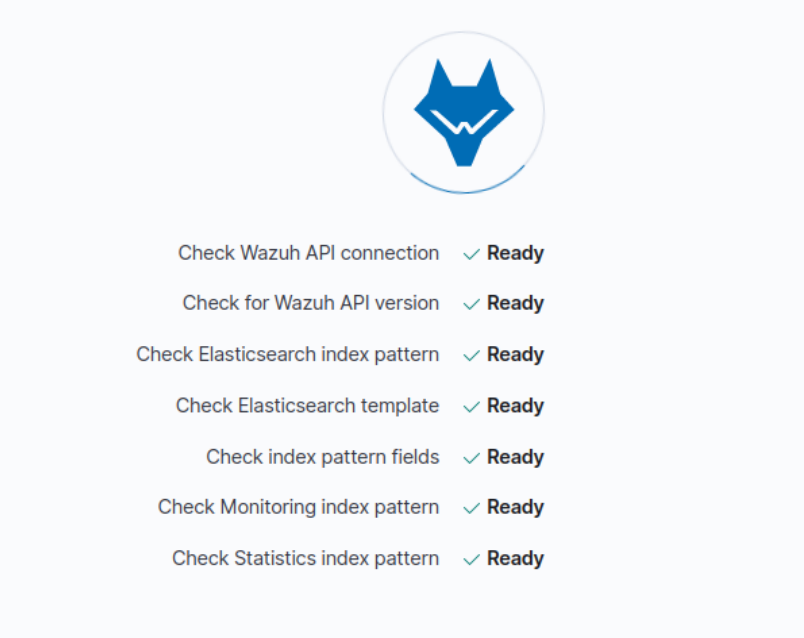
Na kraju se Elasticsearch certifikati trebaju premjestiti u direktorij na putanji `/etc/filebeat` uz isti postupak koji je opisan ranije na putanji /etc/elasticsearch. Na samom kraju dolazi instalacija Kibane pokretanjem naredbe `apt-get install opendistroforelasticsearch-kibana`. Konfiguracijska datoteka se mora zasebno preuzeti i to je moguće uz naredbu `curl -so /etc/kibana/kibana.yml https://documentation.wazuh.com/4.1/resources/open-distro/kibana/7.x/kibana_all_in_one.yml`. Kao i ranije, da bi se pravilno povezali, potrebno je instalirati Kibana dodatak za Wazuh. Za to, prvo se mora kreirati potrebna datoteka na putanji `/usr/share/kibana/data` i staviti vlasništvo nad tim direktorijima Kibani s naredbom `chown -R kibana:kibana /usr/share/kibana/data`. Iz glavnog direktorija Kibane se sada može preuzeti potrebni dodatak, pokretanjem naredbe `sudo -u kibana /usr/share/kibana/bin/kibana-plugin install https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4.1.5_7.10.2-1.zip`.

Nakon toga, ponavlja se isti postupak kopiranja Elasticsearch certifikata, ali sada u glavni direktorij Kibane. Zadnji korak je povezivanje Kibane na privilegirani mrežni priključak 443 korištenjem naredbe `setcap 'cap_net_bind_service=+ep' /usr/share/kibana/node/bin/node`.

S ovim je završena instalacija i konfiguracija Wazuh poslužitelja i svih njegovih dodatnih programa. Dodatne servise prije korištenja treba omogućiti pokretanjem `systemctl enable` pa upisivanjem imena programa. Kada su svi servisi omogućeni, ovom poslužitelju se pristupa preko bilo kojeg web preglednika, upisivanjem adrese `https://IP-adresa` računala. Učitana stranica prvo zahtjeva prijavu na Kibanu, prikazano na slici 3.42. Zatim Wazuh provjerava jesu li sve potrebne komponente za rad spremne, a one se vide na slici 3.43.

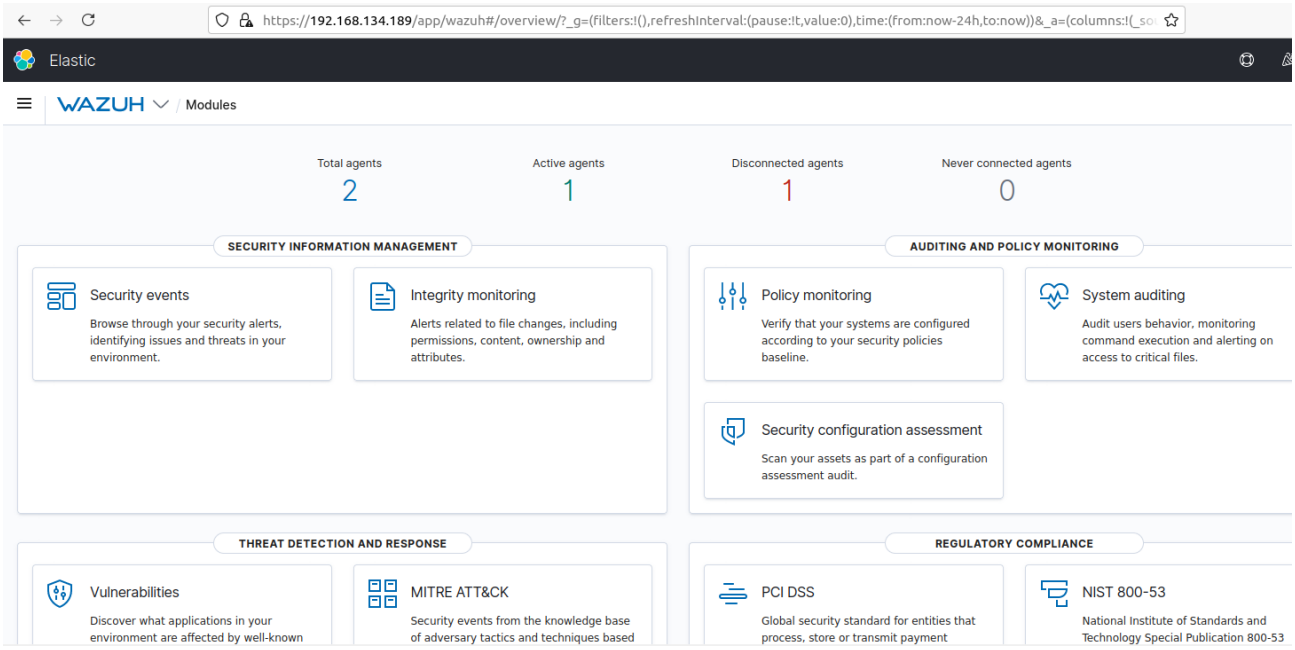


Slika 3.42.: Prijava na Kibanu



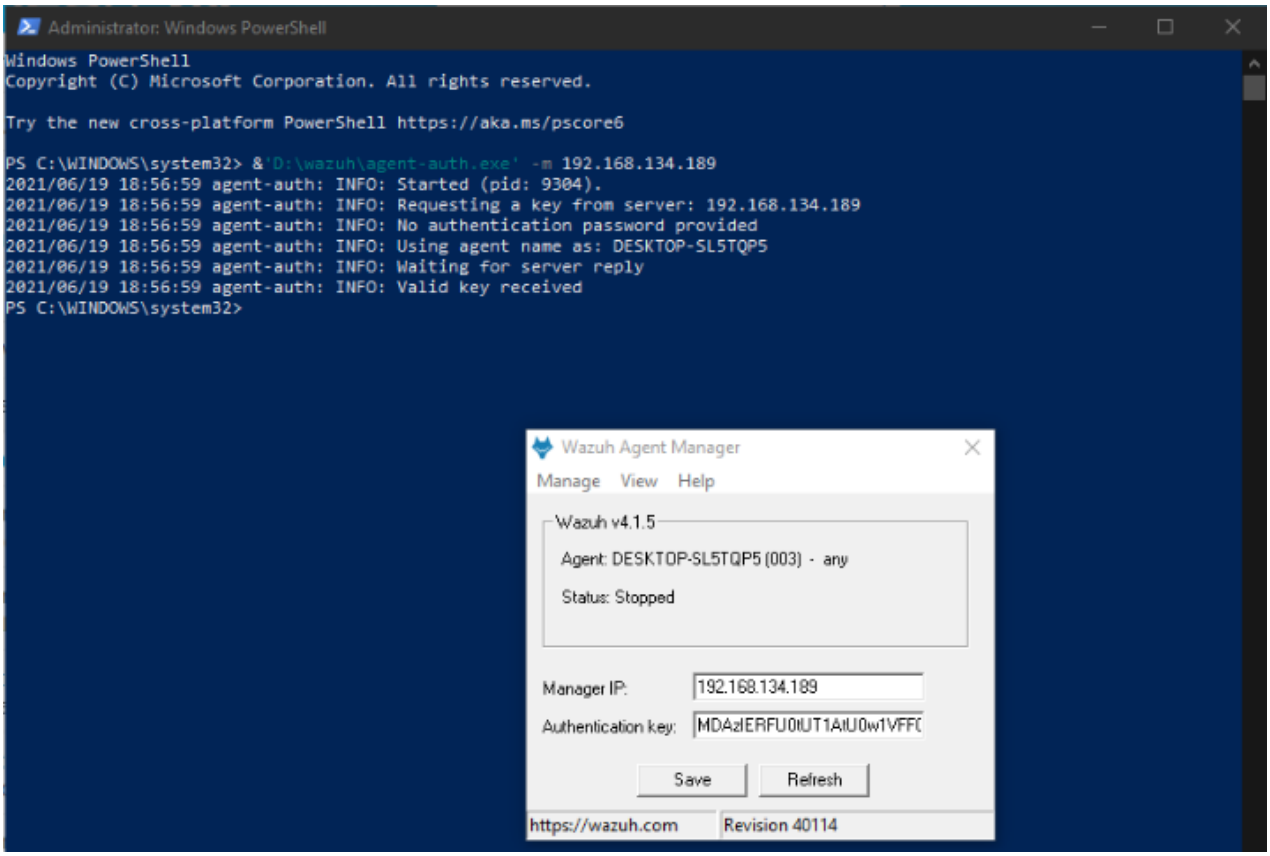
Slika 3.43.: Provjera potrebnih komponenti

Kada se obavi prijava i provjera, sljedeće što je otvoreno je početna stranica Wazuha. Na njoj je prikazan ukupan broj agenata, broj aktivnih i neaktivnih agenata, agenata koji nikada nisu spojeni s Wazuhom. Ispod toga nalaze se sve funkcije koje su bile ranije opisane u teoretskom dijelu o Wazuhu. Na svaku od tih funkcija moguće je kliknuti kako bi se prikazalo ono što je prikupljeno od podataka iz zapisnika. Kako izgleda Wazuh početna stranica, može se vidjeti na slici 3.44.



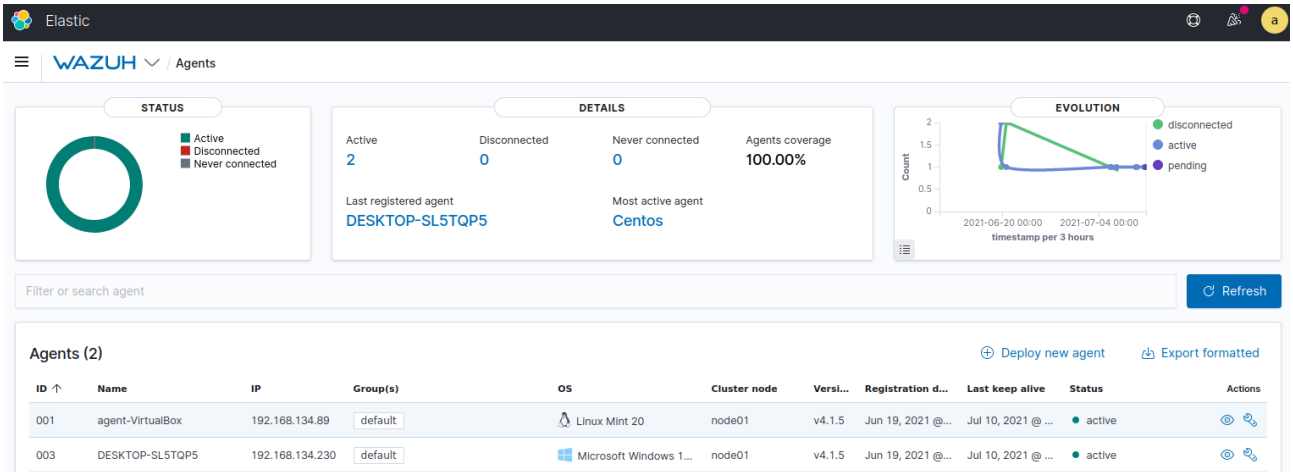
Slika 3.44.: Početna Wazuh stranica

Povezivanje agenata s poslužiteljem jako je slično povezivanju kod OSSEC-a. Pošto su OSSEC agenti kompatibilni s Wazuh poslužiteljem, u ovom radu nije obavljena instalacija novog agenta, nego je korišten isti kao i za OSSEC. Ono što se mora promijeniti konfiguracijskoj datoteci ossec.conf kako bi se agent spojio s Wazuh poslužiteljem, je IP-adresa koja se odnosi na poslužitelj, odnosno lokalnog računala. Instalacija za Windows agenta obavljena je na prijenosnom računalu koje je fizičko računalo, a ne na virtualnom stroju. Proces i za ovaj operacijski sustav je isti kao kod OSSEC-a, preuzimanjem potrebne datoteke sa službene web stranice, pa pokretanjem preko grafičkog sučelja. Kada je instalacija agenta gotova, mora se registrirati i povezati s poslužiteljem. To je moguće preko komandne linije agenta, upisivanjem naredbe `&'C:\Program Files (x86)\ossec-agent\agent-auth.exe' -m <manager_IP>` gdje se umjesto zadanih parametara upisuju stvarni. Kako to izgleda s pravilnim podacima prikazano je na slici 3.45., ujedno sa sučeljem agenta koje izgleda isto kao i kod OSSEC-a.



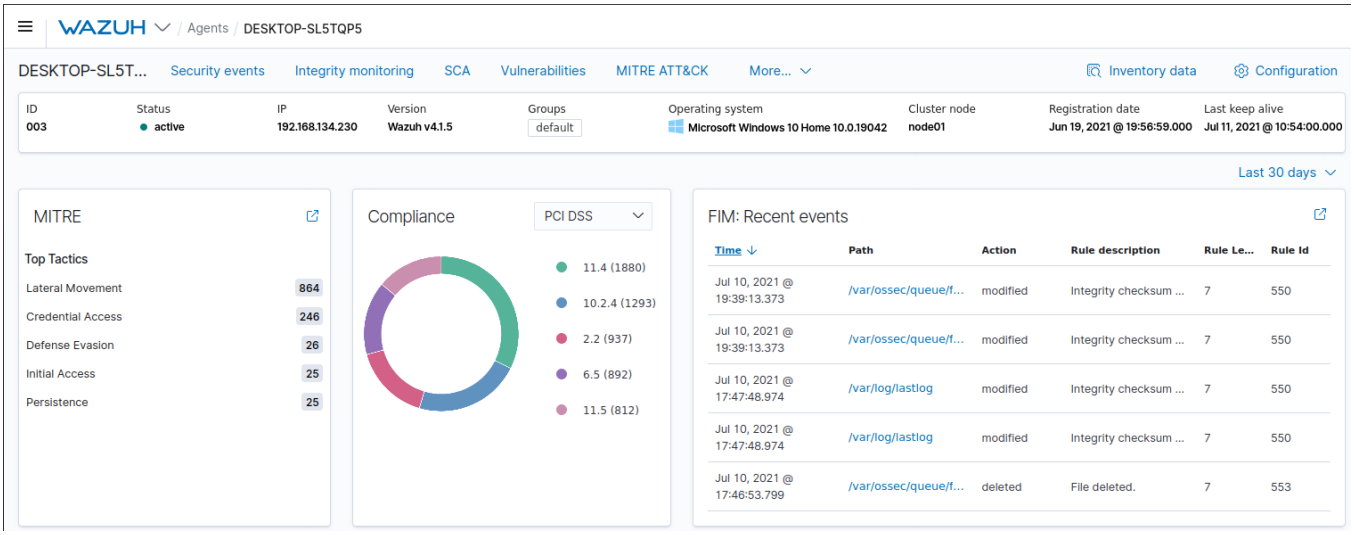
Slika 3.45.: Povezivanje Wazuh agenta s poslužiteljem i sučelje agenta

Klikom na Aktivni agenti (engl. *Active agents*) sa slike 3.44., prikazat će se informacije o spojenim agentima, njihov status, detalji o aktivnosti, neaktivnosti, najčešće aktivnom agentu i ostalo. Kako to sve skupa izgleda vidi se na slici 3.46. Klikom na red u kojem se nalaze identifikacijski broj, ime, IP-adresa, grupa, operacijski sustav i ostalo, u tablici pod nazivom Agenti (engl. *Agents*), bit će moguće vidjeti puno više detalja i podataka prikupljenih o određenom agentu.

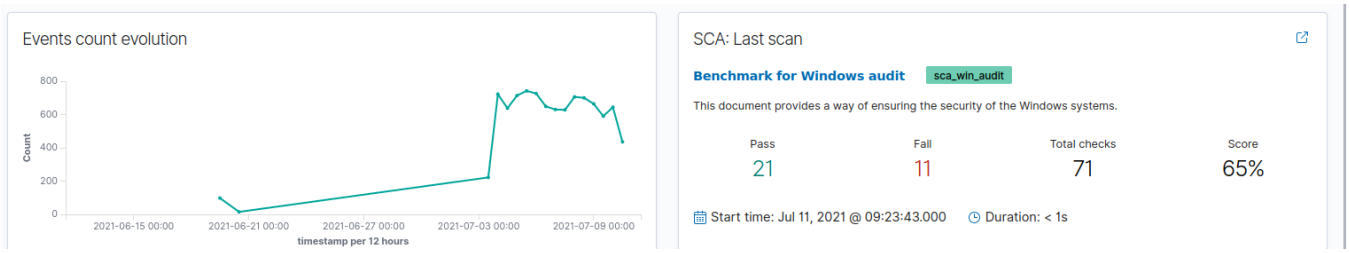


Slika 3.46.: Detalji o Wazuh agentima

Na slikama 3.47. i 3.48. vidi se prikaz početne stranice agenta prijenosnog računala. Ono što se može vidjeti na toj stranici je sažetak određenih prikupljenih podataka. MITRE pokazuje podatke pohranjene o svim mogućim napadima koji se mogu dogoditi. Standard zaštite podataka industrije platnih kartica (engl. *Payment Card Industry Data Security Standard*, skraćeno PCI DSS) koji je vlasnički standard za zaštitu informacija. [15] Također se vide nedavni događaji vezani za datoteke, na kojoj putanji se nalaze, akcija provedena nad njima i kada, graf koji prikazuje brojanje evolucije događaja i kada se izvršilo zadnje skeniranje sustava.



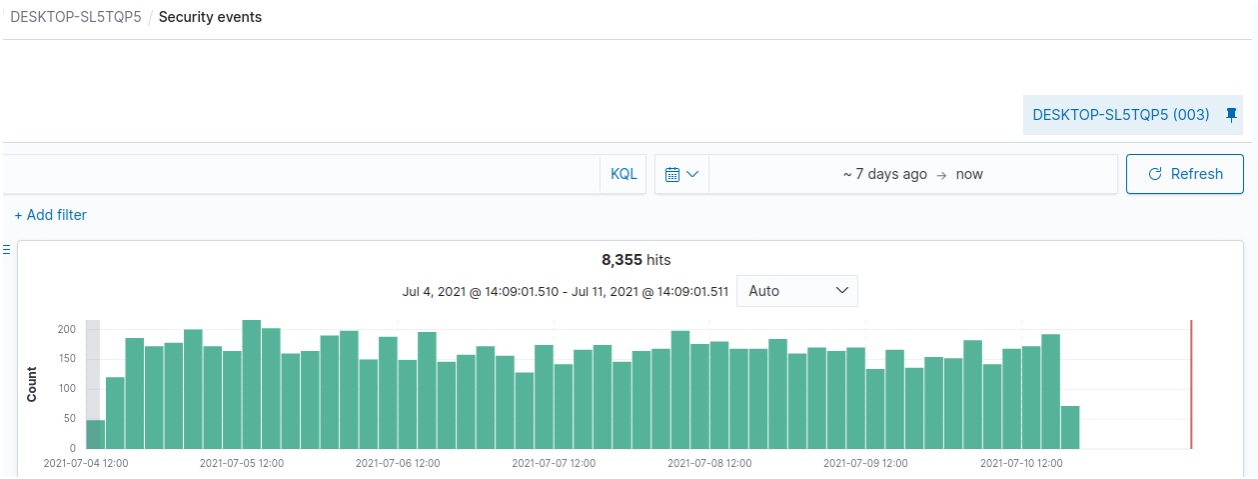
Slika 3.47.: Podaci po mogućim napadima, zaštiti i događajima vezanim za datoteke



Slika 3.48.: Prikaz zadnjeg skeniranja i evolucija događaja

Pritiskom na sigurnosni događaji, bit će vidljiv graf s brojem vremenskih oznaka svaka 3 sata. Može se prikazati sadržaj prikupljen u posljednjih dvadeset četiri sata, tjedan dana, mjesec dana, godina, ali čak i posljednjih petnaest ili trideset minuta. Ispod grafa nalaze se razni sigurnosni događaji na sustavu, vrijeme kada su se dogodili, njihov opis i razina uzbune. Neke od uzbuna koje se mogu naći su vezane za grešku na web poslužitelju, mogući napad na protokol sigurne ljuske (engl. *Secure Shell Protocol*, skraćeno SSH) poslužitelja, neuspješna autentifikacija,

pogreška obrnutog pretraživanja i mnoge druge. Kako izgleda graf s prikupljenim podacima u posljednjih sedam dana, i primjeri uzbuna vidljivi su na slikama 3.49. i 3.50.

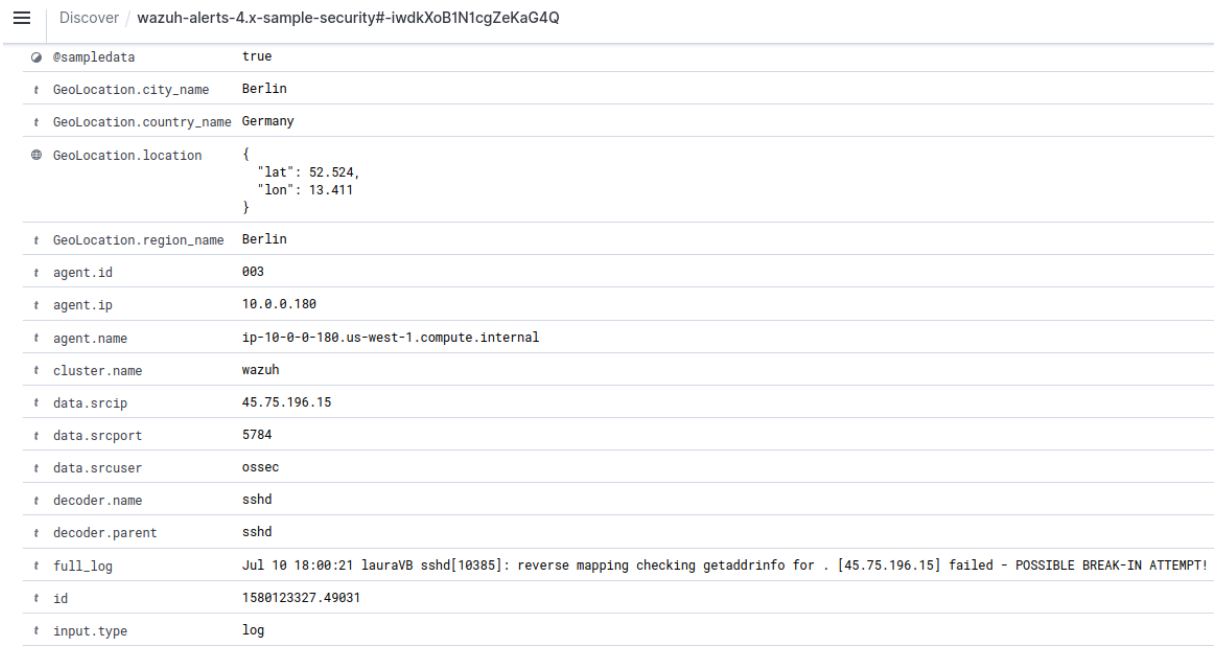


Slika 3.49.: Graf s brojem vremenskih oznaka

›	Jul 10, 2021 @ 19:09:21.707	Multiple web server 400 error codes from same source ip.	10	31151
›	Jul 10, 2021 @ 19:06:09.818	sshd: Attempt to login using a non-existent user	5	5710
›	Jul 10, 2021 @ 19:06:09.818	sshd: Attempt to login using a non-existent user	5	5710
›	Jul 10, 2021 @ 19:06:04.726	GCP alert event from VM 531339229531.instance-1 with source IP 83.32.0.0 from europe-west1	11	65037
›	Jul 10, 2021 @ 19:06:04.726	GCP alert event from VM 531339229531.instance-1 with source IP 83.32.0.0 from europe-west1	11	65037
›	Jul 10, 2021 @ 19:04:19.163	Sample alert 2	5	3981
›	Jul 10, 2021 @ 19:04:19.163	Sample alert 2	5	3981
›	Jul 10, 2021 @ 19:02:23.723	Audit: Command: /usr/sbin/bash	3	80781
›	Jul 10, 2021 @ 19:02:23.723	Audit: Command: /usr/sbin/bash	3	80781
›	Jul 10, 2021 @ 19:00:13.304	sshd: Possible attack on the ssh server (or version gathering).	8	5701
›	Jul 10, 2021 @ 19:00:13.304	sshd: Possible attack on the ssh server (or version gathering).	8	5701
›	Jul 10, 2021 @ 18:59:16.402	sshd: authentication failed.	5	5716

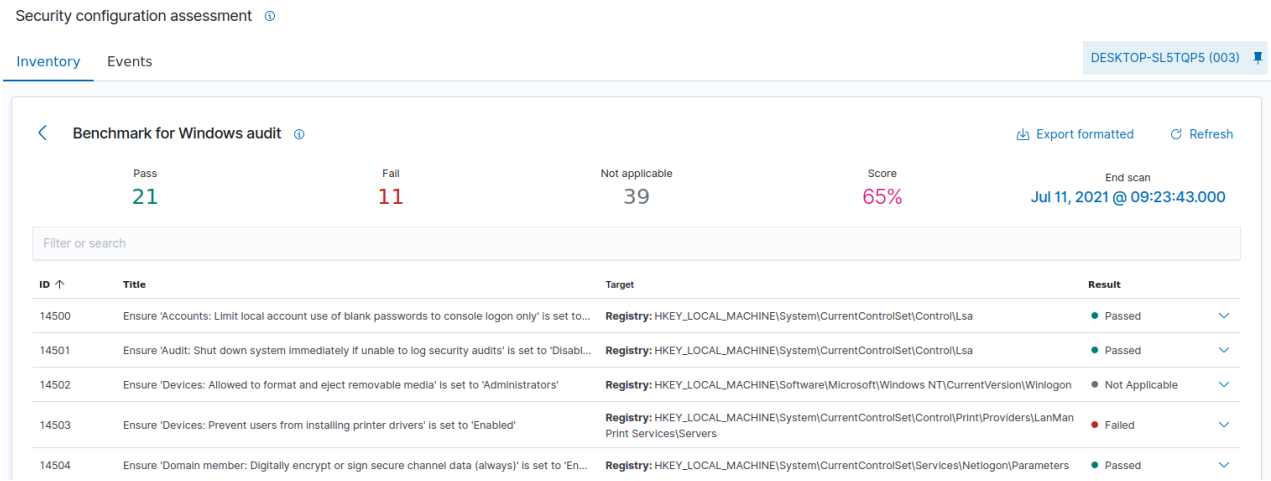
Slika 3.50.: Primjer sigurnosnih uzbuna

Dodatna mogućnost ovog sustava za detekciju napada je što omogućava da klikom na svaku od ovih uzbuna, prikaže detalje koje je uspio prikupiti. Primjer će se pokazati na uzbuni koja je vezana za mogući pokušaj provale u sustav. Wazuh iz zapisnika prikupi podatke o lokaciji s koje dolazi mogući napad, agentov identifikacijski broj i IP-adresa i mnogi druge podatke. Detaljan prikaz podataka o mogućem napadu prikazan je na slici 3.51.



Slika 3.51.: Detalji o mogućem napadu

Nakon sigurnosnih događaja (engl. *security events*), praćenje integriteta (engl. *integrity monitoring*) na isti način prikazuje podatke, ali o raznim datotekama i direktorijima. Također prikazuje graf s brojem vremenskih oznaka kao kod sigurnosnih događaja, a ispod njega se nalaze informacije o putanji na kojoj je došlo do neke promjene, kada je došlo do promjene, je li nešto brisano, modificirano ili dodano na sustav. Sljedeći modul je provjera sigurnosne konfiguracije (engl. *Security Configuration Assessment*, skraćeno SCA), koji prikazuje mjerilo za provjeru Windows sustava. Tamo se može vidjeti broj uspješnih i neuspješnih provjera, onih koji nisu primjenjivi, ukupan postotak pogodaka i kada je završeno skeniranje. Također su vidljivi opisi i putanje onoga što se provjeravalo. Izgled prikupljenih podataka o provjerama i skeniranjima sustava je na slici 3.52.



Slika 3.52.: Provjera sigurnosne konfiguracije

Nakon provjere sigurnosne konfiguracije, moduli koji su još prisutni su ranjivosti i MITRE ATT&CK. Oba modula odnose se na sigurnost sustava, te pokazuju potencijalne rizike na sustavu ili uzbune. MITRE ATT&CK prikazuje iste uzbune kao i sigurnosni događaji, uz mogućnost detaljnog prikaza informacija. Ovaj program je baza znanja i model za ponašanje cyber protivnika, koji odražava različite faze životnog ciklusa napadačevog napada i platforme koje su poznate po čestim napadima. [16] Osim ovih modula, Wazuh nudi provjeru i pregled mnogih drugih stvari koje pokriva, za razliku od OSSEC-a koji je samo prolazio kroz zapisnike.

4. Zaključak

Povećanjem broja napada na računala koji su umreženi, računala i mrežu je potrebno zaštititi. Uz osnovne alate koji se dobiju na samom računalu, dodatnu zaštitu moguće je postići podizanjem poslužitelja koji će nadzirati događanja na mreži.

Cilj ovog rada bio je prikazati kako se jedan takav sustav može koristiti. Detaljno je razrađena instalacija sustava na poslužitelj i agente, te njihovo povezivanje i konfiguracija. Kao i kod svakog programa ili softvera, moguća je pojava problema pri postavljanju, pa je i ovdje to bio slučaj. Zato su razrađeni i problemi koji su se javili, te kako ih riješiti da bi sustav bio pravilno konfiguriran za sigurno nadziranje.

U prvom poglavlju ukratko je objašnjeno što će pokrivati ovaj završni rad i koji su ciljevi. U drugom poglavlju detaljno je objašnjen prvi sustav za detekciju napada koji se koristi i svi potrebni programi za pravilan rad tog sustava. Kako je prvi sustav zastario, te nema novih ažuriranja ni dodataka, prelazi se na noviji i bolji sustav za detekciju. Drugo poglavlje također sadrži detaljan opis novog sustava za detekciju i svih njegovih komponenti. U trećem poglavlju razrađen je postupak instalacije i konfiguracije svih potrebnih programa i samog sustava, i povezivanje agenata s poslužiteljem. Također je prikazano kako sustav djeluje, sve njegove mogućnosti, problemi koji se mogu pojaviti prilikom postavljanja sustava i kako ih riješiti. Isto je u trećem poglavlju prikazano i objašnjeno za novi sustav za detekciju koji se koristio.

Osim glavne funkcije otkrivanja potencijalnih napada, ovakvi sustavi prolaze kroz zapisnike operacijskog sustava i računala, prikupljajući podatke o promjenama. Te promjene su vidljive na web poslužiteljima sustava koje je bilo potrebno posebno instalirati. Nakon instalacije, svi podaci koje je sustav prikupio bili su prikazani i ažurirani na jednom mjestu.

Novi sustav koji se koristi odabran je namjerno jer je migrirao iz sustava na kojem se ranije radilo. Uz sve komponente i funkcije koje su preuzete prilikom migracije, dodano je još mnogo više modula i funkcija kako bi se sustav što bolje osigurao. Osim samog pregledavanja zapisnika poslužitelja i agenata, dostupne su mogućnosti detaljnog pregledavanja sigurnosnih događaja i potencijalnih napada. Takve detaljne informacije o napadu na starom sustavu nisu bile vidljive, s čime se vidi veliki pomak i napredak u novom sustavu.

Jednom pravilno konfiguriran i postavljen sustav omogućava korisnicima siguran i zaštićen rad, a prednosti su što takav sustav ne zahtjeva puno pažnje i jednostavno ga je koristiti. Uz njega biti će moguće obavljati svakodnevne poslove mnogo sigurnije i preciznije, uz činjenicu da se ne treba svako računalo posebno paziti, već ih je moguće pratiti sve odjednom.

5. Literatura

[1] NIST, „Guide to Intrusion Detection and Prevention Systems (IDPS)“ https://web.archive.org/web/20100601171625/http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf (zadnje posjećeno 10.8.2021.)

[2] ResearchGate, „Intrusion detection system architecture“ https://www.researchgate.net/figure/Intrusion-detection-system-architecture-37_fig2_315662151 (zadnje posjećeno 2.9.2021.)

[3] Ebrary.net, „IDS/IPS System Architecture and Framework“ https://ebrary.net/26724/computer_science/idsips_system_architecture_framework (zadnje posjećeno 2.9.2021.)

[4] OSSEC, https://www.ossec.net/about/ (zadnje posjećeno 22.6.2021.)

[5] Techwalla, „How to Delete the Proxy Cache on IE“ https://www.techwalla.com/articles/how-to-delete-the-proxy-cache-on-ie (zadnje posjećeno 15.6.2021.)

[6] APACHE HTTP SERVER PROJECT, http://httpd.apache.org/ABOUT_APACHE.html (zadnje posjećeno 2.7.2021.)

[7] Skillcrush, „Everything You Need To Know About PHP“ https://skillcrush.com/blog/php/ (zadnje posjećeno 2.7.2021.)

[8] php, „What can PHP do?“ https://www.php.net/manual/en/intro-whatcando.php (zadnje posjećeno 2.7.2021.)

[9] MySQL, „What is MySQL?“ https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html (zadnje posjećeno 2.7.2021.)

[10] McAfee, „What Is Security Analytics?“ https://www.mcafee.com/enterprise/en-us/security-awareness/operations/what-is-security-analytics.html (zadnje posjećeno 10.8.2021.)

[11] WAZUH, „A Comprehensive Open Source Security Platform“ https://wazuh.com/product/#usecases (zadnje posjećeno 10.8.2021.)

[12] elastic, https://www.elastic.co/ (zadnje posjećeno 10.8.2021.)

[13] .htaccess – Guide, „What is .htaccess?“ http://www.htaccess-guide.com/ (zadnje posjećeno 6.7.2021.)

[14] APACHE HTTP SERVER PROJECT, „apachectl - Apache HTTP Server Control Interface“ https://httpd.apache.org/docs/2.4/programs/apachectl.html (zadnje posjećeno 6.7.2021.)

[15] WAZUH Docs, https://documentation.wazuh.com/current/pci-dss/ (zadnje posjećeno 11.7.2021.)

[16] McAfee, „What Is the MITRE ATT&CK Framework?“ https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html (zadnje posjećeno 11.7.2021.)