Analiza tehnika i alata ljubičastog tima u svrhu unaprjeđenja sigurnosti u organizacijama

Paun, Luka

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Luka Paun

ANALIZA TEHNIKA I ALATA LJUBIČASTOG TIMA U SVRHU UNAPRJEĐENJA SIGURNOSTI U ORGANIZACIJAMA

DIPLOMSKI RAD

Zagreb, 2023.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 21. lipnja 2023.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 7288

Pristupnik: **Luka Paun (0246071770)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Analiza tehnika i alata ljubičastog tima u svrhu unapređenja sigurnosti u organizacijama**

Opis zadatka:

U radu je potrebno istražiti teoretski okvir i pojmove iz područja digitalne sigurnosti. Opisati suvremene pristupe u unaprijeđenju sigurnostni rada neke organizacije. Opisati pojam i metodologuju rada tzv. ljubičastoga tima. Potrebno je detaljno istražiti tehnike i alate tzv. ljubičastog tima u svrhu unapređenja sigurnosti u organizacijama. Opisati studiju slučaja provedenoga istraživanja.

Mentor:

prof. dr. sc. Dragan Peraković

Predsjednik povjerenstva za diplomski ispit:

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

DIPLOMSKI RAD

ANALIZA TEHNIKA I ALATA LJUBIČASTOG TIMA U SVRHU UNAPRJEĐENJA SIGURNOSTI U ORGANIZACIJAMA

ANALYSIS OF PURPLE TEAM TECHNIQUES AND TOOLS FOR IMPROVING SECURITY IN ORGANIZATIONS

Mentor: prof. dr. sc. Dragan Peraković

Student: Luka Paun

JMBAG: 0246071770

Zagreb, svibanj 2023.

ANALIZA TEHNIKA I ALATA LJUBIČASTOG TIMA U SVRHU UNAPRJEĐENJA SIGURNOSTI U ORGANIZACIJAMA

SAŽETAK

Ovaj diplomski rad prikazuje tehnike i alate ljubičastog tima u svrhu unaprjeđenja sigurnosti u organizacijama. Ljubičasti tim je metodologija u informatičkoj sigurnosti u kojoj stručnjaci za ofenzivnu sigurnost, takozvani crveni tim, i stručnjaci za defenzivnu sigurnost, takozvani plavi tim, blisko surađuju kako bi poboljšali sigurnosni stav organizacije kroz kontinuirane povratne informacije i razmjenu znanja. Cilj rada je pojasniti pojam ljubičastog tima, njihovu metodologiju te alate i tehnike koje se koriste u svrhu unaprjeđenja sigurnosti u organizacijama. Praktični dio prikazati će proces postavljanja napadačke i ranjive virtualne mašine, iskorištavanja ranjivosti te korake otklanjanja i zakrpa ranjivosti uz pomoć informacija dobivenih iz raznih alata.

KLJUČNE RIJEČI: ljubičasti tim; poboljšanje sigurnosti; kibernetička sigurnost

SUMMARY

This master thesis presents techniques and tools of the Purple Team for the purpose of improving security in organizations. Purple Teaming is a methodology in IT security where offensive experts, the so-called red team, and defensive security experts, the so-called blue team, work closely together to improve the organization’s security posture through continuous feedback and knowledge sharing. The aim of this work is to explain the concept of the Purple Team, their methodology, as well as the tools and techniques used to improve security in organizations. The practical part will show the process of setting up the attacker and vulnerable virtual machines, vulnerability exploitation and finally, mitigation and patching with the help of information gained from security tools.

KEY WORDS: Purple Team; Improving security; Cybersecurity

Sadržaj

1. Uvod

Organizacije se često oslanjaju na defenzivne - plave i ofenzivne - crvene timove kako bi poboljšale svoju kibernetičku sigurnost. Ljubičasti tim je spoj crvenog i plavog tima kojemu je cilj koristiti ofenzivne i defenzivne vještine zaposlenika u svrhu procjene, analize i poboljšanja obrane od kibernetičkih napada. Ta poboljšanja mogu se odnositi na ljude, procese ili tehnologiju.

Ljubičasti tim može imati značajnu ulogu u poboljšanju sigurnosti organizacije zato što omogućava sigurnosnim timovima da unaprijede učinkovitost otkrivanja ranjivosti, traženja prijetnji i nadzora mreže. To se postiže točnim simuliranjem uobičajenih scenarija prijetnji i olakšavanjem stvaranja novih tehnika za sprječavanje i otkrivanje novih vrsta prijetnji. Bitno je razumjeti razliku između emulacije i simulacije u kibernetičkoj sigurnosti. Simulacija podrazumijeva korištenje unaprijed definiranih, automatiziranih napada koji oponašaju ponašanje potencijalnog zlonamjernog aktera. S druge strane, emulacija podrazumijeva dupliciranje identičnih taktika, tehnika i procedura koje bi zlonamjerni akter koristio te ih se testira u pravom okruženju.

Predmet analize ovog diplomskog rada su tehnike i alati ljubičastog tima u svrhu unaprjeđenja sigurnosti u organizacijama. Metodologija i primjena ljubičastog tima u praksi opisana je u trećem i četvrtom poglavlju, u petom poglavlju su navedeni i opisani alati i tehnike ljubičastog tim, a u šestom poglavlju napravljena je studija slučaja.

Cilj i svrha izrade ovog diplomskog rada je analiza mogućnosti tehnika i alata ljubičastog tima u svrhu unaprjeđenja sigurnosti u organizacijama te prikaz mogućnosti na konkretnom primjeru.

Diplomski rad sastoji se od 7 poglavlja:

1. Uvod
2. Teorijski okvir i definicija pojmova iz područja digitalne sigurnosti
3. Opis i metodologija ljubičastog tima
4. Primjena ljubičastog tima u praksi
5. Istraživanje alata i tehnika ljubičastog tima
6. Studija slučaja
7. Zaključak

U drugom poglavlju obrađen je teorijski okvir iz digitalne sigurnosti te su definirani najbitniji osnovni pojmovi vezani uz kibernetičku sigurnost. Potom je definiran termin ljubičastog tima, aktivnosti koje taj tim provodi te razlike između ljubičastog tima i ostalih pristupa.

U trećem poglavlju opisana je metodologija ljubičastog tima, PEIR model na kojem se ljubičasti tim zasniva te su opisane uloge plavog i crvenog tima unutar ljubičastog tima s primjerima.

Četvrto poglavlje obuhvaća primjenu ljubičastog tima u praksi kroz pet komponenti, objašnjene su razne metrike koje se mogu koristiti za evaluaciju učinkovitosti ljubičastog tima, zatim su predstavljene prednosti i izazovi kod primjene ljubičastog tima te neki primjeri izvođenja vježbi.

U petom poglavlju napravljeno je istraživanje alata i tehnika ljubičastog tima, te je opisana ideja kibernetičkog zavaravanja. Zatim su opisani pojmovi *honeypot* i *decoy* sustava te je prikazan i opisan lanac kibernetičkog zavaravanja koji će pomoći u razumijevanju životnog ciklusa ove operacije.

U šestom poglavlju napravljena je studija slučaja, gdje će se pokazati proces izrade virtualnih mašina, podizanje operativnih sustava, zatim instalacije potrebnih alata za izvođenje napada i ranjive aplikacije na ranjivoj virtualnoj mašini. Također popratit će se zapisi vatrozida, Docker spremnika, te će se opisati koraci otklanjanja i zakrpa ranjivosti.

2. Teorijski okvir i definicija pojmova iz područja digitalne sigurnosti

Tradicionalni pristup sigurnosnog testiranja kritični je aspekt koji provjerava sigurnost, pronalazi ranjivosti te provjerava usklađenost nekog sustava, aplikacije ili mreže sa standardima i regulacijama. Tradicionalni pristup sigurnosnog testiranja sastoji se od više elemenata, kao što su penetracijsko testiranje, procjena ranjivosti, testiranje otpornosti na zloupotrebe, provjera usklađenosti s regulacijama i standardima te testiranje na DDoS (engl. *Distributed Denial of Service*) napade.

Penetracijsko testiranje, također zvano i „*pen testing*“, je simulacija kibernetičkog napada na sustav, mrežu ili aplikaciju. Svrha te simulacije je otkrivanje slabih točaka i ranjivosti koje bi potencijalni zlonamjerni akter mogao iskoristiti. Penetracijsko testiranje sastoji se od raznih metoda, kao što su vanjsko testiranje, unutarnje testiranje, slijepo testiranje i ciljano testiranje. Vanjsko testiranje odnosi se na testiranje resursa organizacije koje su vidljive na internetu, npr. Web aplikaciju ili naziv domene. Unutarnje testiranje s druge strane, sadrži ispitivača s pristup aplikaciji iza vatrozida koji glumi *insider*-a. Najčešće se koriste napadi krađe identiteta u ovu svrhu testiranja. Slijepo testiranje podrazumijeva da ispitivač zna samo ime organizacije koju cilja, a defenzivnom timu ciljane organizacije daje pravovremen pogled na to kako izgleda stvarni napad. Ciljano testiranje podrazumijeva da ispitivač i defenzivni tim organizacije surađuju i razmjenjuju mišljena.

Procjena ranjivosti (engl. *vulnerability assessment*) je postupak prepoznavanja, klasificiranja i određivanja prioriteta sigurnosnih ranjivosti u IT infrastrukturi. Sveobuhvatnom procjenom ranjivosti određuje se izloženost IT sustava ranjivostima, te se zatim prema potrebi preporučuju koraci za otklanjanje ranjivosti ili ublažavanje. Procjene ranjivosti su standardni postupak jer pružaju detaljan pregled sigurnosnih rizika s kojima se organizacija može susresti, te tako omogućiti da organizacija bolje zaštiti svoje resurse i osjetljive podatke od kibernetičkih prijetnji. Proces procjene ranjivosti sastoji se od identifikacije i analize ranjivosti, procjene rizika, sanacije i na kraju otklanjanja ranjivosti. Jedan od čestih načina identifikacija ranjivosti je korištenje mrežnih skenera, koji mogu i ne moraju imati dozvoljen pristup mrežnim resursima.

Svrha testiranja otpornosti na zloupotrebe u domeni kibernetičke sigurnosti odnosi se na simulaciju zlonamjernog aktera u svrhu identifikacije i iskorištavanja ranjivosti u sustavu, mreži ili aplikaciji. Cilj ove vrste testiranja je pronalazak i identifikacija potencijalnih ranjivosti ili slabosti koje bi zlonamjerni akter mogao iskoristiti za dobivanje neovlaštenog pristupa.

Testiranje otpornosti na zloupotrebe može pomoći organizaciji identificirati slabosti i otkloniti ih prije nego li ih iskoristi zlonamjerni akter, te time prevenirati potencijalnu štetu.

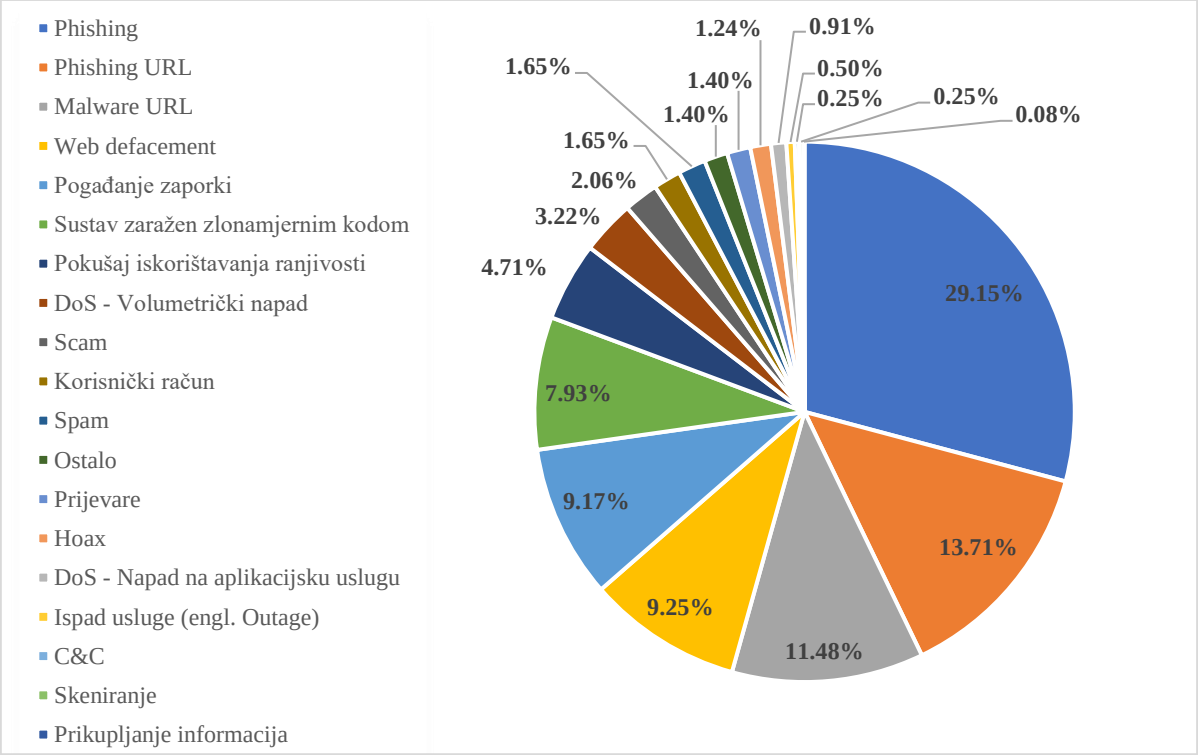
Testiranje usklađenosti (engl. *compliance testing*) je vrsta sigurnosnog testiranja koje provjerava usklađenost organizacije s regulacijama i standardima poput npr. standarda sigurnosti podataka industrije platnih kartica (engl. *Payment Card Industry Dana Security Standard,* PCI DSS), opće uredba o zaštiti podataka (engl. *General Data Protection Regulation,* GDPR) i sl. Testiranje usklađenosti pomaže organizacijama da njihove sigurnosne prakse zadovoljavaju zahtjeve regulatornih tijela i pomaže u sprječavanju financijskih i pravnih posljedica. Cilj PCI DSS-a je povećati kontrolu podataka o vlasnicima kartica kako bi se smanjile prijevare s kreditnim karticama. GDPR je regulacija Europske Unije kojoj je cilj zaštita osobnih podataka građana. Ta regulacija je obavezna za sve organizacije koje procesiraju podatke stanovnika EU, bez obzira gdje se organizacija nalazi, [1].

Ovi tradicionalni pristupi mogu biti korisni u procjeni sigurnosti sustava, aplikacija ili mreža, ali mogu biti ograničeni u otkrivanju novih prijetnji i napadačkih metoda. Stoga je cilj ovog diplomskog rada pokazati benefite ljubičastog tima u organizacijama.

U ovom diplomskom radu, često će se spominjati termini prijetnja, ranjivost i rizik, stoga ih je potrebno objasniti. Kada se govori o kibernetičkoj sigurnosti, prijetnja može biti sve što iskorištava neku ranjivost sustava, mreže ili aplikacije. Prijetnje ugrožavaju integritet, povjerljivost i sigurnost podataka i sustava. Prijetnja se također može opisati kao proces koji povećava vjerojatnost katastrofalnog događaja. Prijetnje se često klasificiraju na unutarnje i vanjske. Unutarnje su one koje nastaju ljudskom greškom i često su nenamjerne. Dobar primjer toga je kada zaposlenik otvori kompromitiranu datoteku koja omogućuje izvršavanje kibernetičkog napada. Vanjske prijetnje su one koje nastanu namjerno, gdje netko svjesno napada znajući da čini štetu. Često je cilj takvih napadača krađa osjetljivih podataka, novca ili narušavanje reputacije organizacije. Rizik je mogućnost nastanka katastrofalnog događaja ako prijetnja iskoristi ranjivost. Ranjivost se odnosi na nedostatke, slabosti i pogreške u kodu ili konfiguraciji koje mogu ugroziti resurse organizacije te ih izložiti unutarnjim ili vanjskim prijetnjama.

Prikaz prijavljenih kibernetičkih prijetnji prema vrsti napada najbolje je prikazan korištenjem grafičkog prikaza statistike o broju prijava i vrstama prijetnji, kao što je prikazano

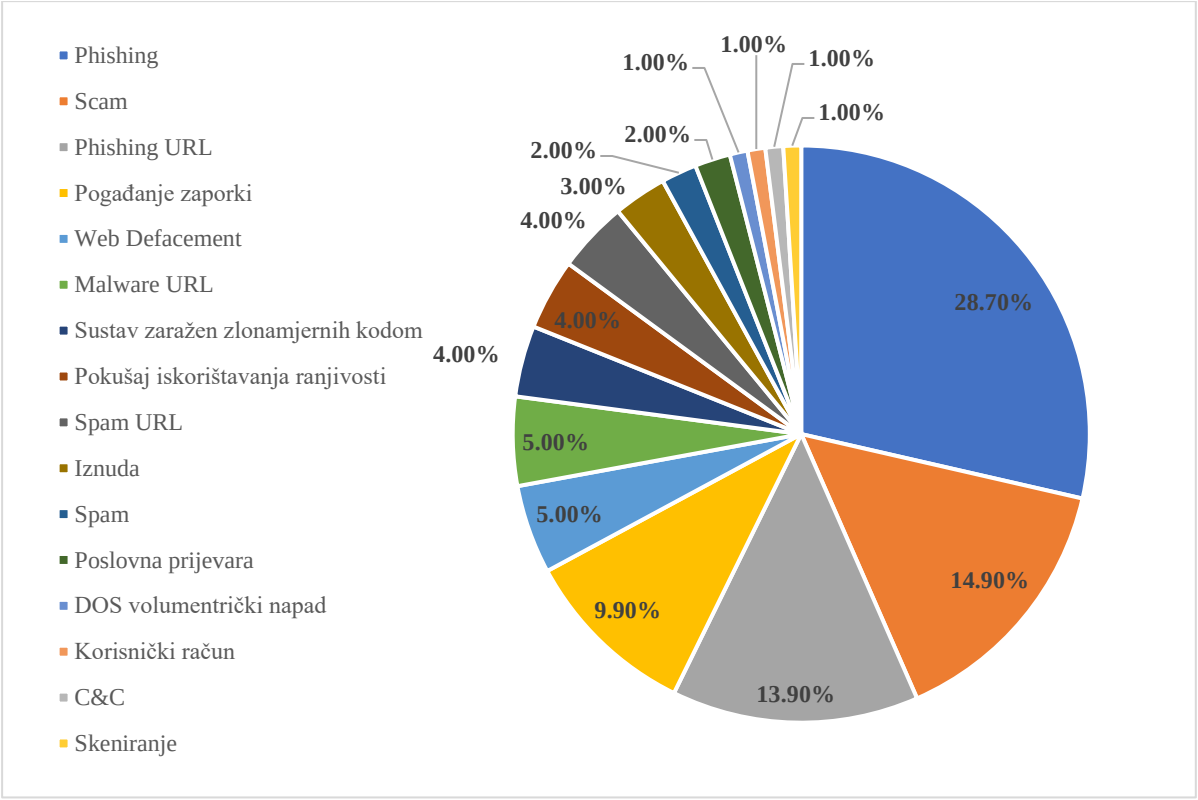
na slici 1 za podatke iz 2021. i na slici 2 za podatke iz 2022 godine. Podaci se odnose na prijavljene incidente u Hrvatskoj koje je zaprimio Nacionalni CERT.



Slika 1. Zastupljenost kibernetičkih napada po vrsti za 2021. godinu

Izvor: [2]

Na slici 1. može se primijetiti zastupljenost napada krađom identiteta od ukupno skoro 43% naspram ostalih vrsta kibernetičkih napada, nakon kojih slijede zlonamjerni softveri i *Web defacement* napadi (napad u kojem se mijenja izgled naslovne strane komprimirane *web*-stranice) te kibernetički napadi poput pogađanja zaporki, sustava zaraženih zlonamjernim kodom, pokušaji iskorištavanja ranjivosti i sl. Uspoređujući s godinom ranije, primijećen je manji broj korisničkih prijava računalno sigurnosnih incidenata za čak 29%, a broj otkrivenih kompromitiranih web sjedišta smanjio se za 23% u odnosu na godinu prije.



Slika 2. Zastupljenost kibernetičkih napada po vrsti za 2022. godinu

Izvor: [3]

U 2022. godini primijećeno je povećanje broja korisničkih prijava računalno-sigurnosnih incidenata od ukupno 7% u odnosu na godinu prije. Pretpostavlja se da je razlog tome generalno veća svijest građana i javne zauzetosti za teme iz područja kibernetičke sigurnosti. Uspoređujući ove dvije slike moguće je primijetiti porast incidenata klasificiranih kao prevara (engl. *scam*), a broj otkrivenih kompromitiranih web sjedišta smanjio se za 38,7% u odnosu na godinu prije. Napadi krađe identiteta (engl. *phishing*) su i dalje najzastupljeniji napadi.

2.1. Definiranje ljubičastog tima

Unatrag nekoliko godina, ljubičasti tim, relativno nova ideja u kibernetičkoj sigurnosti, privlači sve više pažnje. Kroz poboljšanu komunikaciju i timski rad između crvenog i plavog tima organizacije, ovaj suradnički pristup nastoji poboljšati sigurnosnu poziciju. Tim stručnjaka poznat kao „crveni tim“ simulira stvarne napade kako bi testirao obranu organizacije, dok je „plavi tim“ zadužen za odbijanje tih napada. Ljubičasti tim ima za cilj poticati suradnju između tih timova kako bi zajednički otkrivali i popravljali ranjivosti te stvoriti okruženje za testiranje koje je učinkovitije i točnije predstavlja trenutne prijetnje. Organizacije mogu bolje procijeniti

svoju sigurnosnu poziciju i poboljšati svoje postupke odgovora na incidente integrirajući ofenzivne i defenzivne vještine crvenog i plavog tima, [4].

Ljubičasti tim nije posvećeni tim, stoga nema potrebe za zapošljavanjem dodatnih sigurnosnih stručnjaka kako bi se izgradio novi tim. Međutim, primjena pristupa ljubičastog tima može biti izazovna, posebno za organizacije koje nemaju razvijen sigurnosni program. To zahtjeva resursa i vremena, kao i snažnu posvećenost suradnji i komunikaciji između crvenog i plavog tima. U nastavku će se prikazati i objasniti razne komponente koje zajedno čine ljubičasti tim.

2.2. Aktivnosti ljubičastog tima

Slika 3: Dijagram aktivnosti ljubičastog tima
Izvor: [5]

Kao što je vidljivo na dijagramu, aktivnosti ljubičastog tima nisu ograničene samo na interakcije između crvenih i plavih timova, već uključuju u sljedeće:

- Automatizacija: Prilagođeni razvoj kontinuiranih sigurnosnih kontrola na temelju poznatih prijašnjih napada.
- Procesi: Ova aktivnost uključuje razne procese kako bi se osigurao kontinuirani životni ciklus poboljšanja, uključujući zapise aktivnosti, izvještavanje i upravljanje promjenama.

- Emulacija zlonamjernog aktera: Identificiranje raznih tehnika koje koristi određeni zlonamjerni akter te izrada plana za njihovo ponovno izvođenje kako bi se mogla testirati obrana organizacije.
- Simulacija proboja sigurnosti (engl. *Breach Attack Simulation*, BAS): Postupak koji se sastoji od ponovnog izvođenja jedne ili više postojećih tehnika napada ručno ili uz pomoć postojećeg alata, [5].

Automatizacija igra veliku ulogu u ljubičastom timu. Ovaj pristup uključuje razvoj kontinuiranih sigurnosnih kontrola koje se temelje na temelju prethodnih napada i ranjivosti identificiranih tijekom prethodnih sigurnosnih testiranja. Ove sigurnosne kontrole mogu uključivati automatizirane postupke kao što su postavljanje upozorenja, blokiranje prometa ili slanje odgovarajućih upozorenja administratorima. Automatizacija se također može primijeniti na simulaciju napada proboja sigurnosti (engl. *Breach Attack Simulation*, BAS) i emulaciju zlonamjernog aktera. Automatizacija kod ove tehnike testiranja omogućuje bržu i učinkovitiju analizu sigurnosnih događaja, prepoznavanje ranjivosti i odgovor na napade. Uz automatizaciju, ljubičasti tim također koristi i alate za upravljanje incidentima i sigurnosnim informacijama i događajima (engl. *Security Information and Event Management*, SIEM) za automatizaciju procesa upravljanja incidentima i smanjenje vremena odgovora na sigurnosne incidente. Bitno je napomenuti da automatizacija ne može zamijeniti ljudske vještine analize rizika i procjene rizika. Iako automatizacija pomaže u otkrivanju sigurnosnih incidenata i odgovoru na njih, ljudi i dalje trebaju analizirati i razumjeti širi kontekst, identificirati nove prijetnje i izraditi strategiju za borbu protiv njih. Zato se automatizacija i ljudska analitika moraju kombinirati kako bi se organizacija zaštitila od kibernetičkih prijetnji, [6].

Procesi igraju važnu ulogu u osiguravanju kontinuiranom poboljšanju sigurnosnog životnog ciklusa organizacije. Ovi procesi uključuju sve od prikupljanje podataka, izvještavanje pa sve do upravljanja promjenama i sigurnosnih zakrpa (engl. *security patches*).

- Prikupljanje podataka je izuzetno važan proces tijekom kojeg se podaci prikupljaju iz raznih izvora poput izvješća o incidentima, zapisa aktivnosti, podataka o ranjivostima i obavještajnih podataka o prijetnjama. Ti podaci se zatim koriste za analizu i identifikaciju ranjivosti i razvoj sigurnosnih kontrola.
- Procesi izvještavanja su također bitni jer generiraju izvješća kako bi se pružio pregled cjelokupnog sigurnosnih stanja organizacije. Ta izvješća mogu sadržavati informacije o

ranjivostima, incidentima i drugim relevantnim sigurnosnim događajima, te također pružaju preporuke za poboljšanje.

- Upravljanje promjenama u kibernetičkoj sigurnosti podrazumijeva pronalazak potencijalnih problema u promjenama sustava. Svaka promjena može stvoriti nove ranjivosti ili smanjiti dostupnost sustava, Stoga organizacije moraju odrediti kako uravnotežiti potrebu za promjenom s minimiziranjem rizika.
- Proces upravljanja sigurnosnim zakrpama sastoji se od identificiranja i primjene ažuriranja, tj. zakrpa na razne krajnje točke sustava, uključujući računala, mobilne uređaje ili poslužitelje. Zakrpe su često samo kratkotrajno rješenje za otklanjanje ranjivosti, te dođe integrirana u sljedeću verziju softvera. [7].

Emulacija zlonamjernog aktera (engl. *Adversary emulation*) uključuje identificiranje različitih tehnika koje koristi određeni zlonamjerni akter, te prikupljanje saznanja o njihovim alatima, taktikama i postupcima (engl. *tools, tactics, and procedures,* TTPs) te razvoj plana za repliciranje tih tehnika za testiranje obrane organizacije. Emulacija zlonamjernog aktera ima za cilj testirati otpornost mreže na napredne zlonamjerne aktere i prijetnje. Organizacije često koriste emulaciju zlonamjernog aktera kao način da testiraju vlastitu sigurnost korištenjem tehnika, taktika i procedura koje koriste stvarni zlonamjerni akteri, ali u kontroliranom okruženju, [8].

Simulacija proboja sigurnosti je aktivnost usmjerena na testiranje obrambenih sposobnosti organizacije protiv različitih scenarija napada. Uključuje kontrolirano i sigurno ponavljanje poznatih napada kako bi se testirala učinkovitost sigurnosnih kontrola i sposobnosti odgovora organizacije. U kontekstu ljubičastog tima, simulaciju proboja sigurnosti izvodi crveni tim, koristeći razne alate i tehnike za simulaciju ponašanja zlonamjernog aktera. Može se izvoditi različitim metodama, od ručnog testiranja do potpuno automatiziranih alata koji simuliraju napade. Često se koriste kombinacije oba načina kako bi se postigli optimalni rezultati. Testove je moguće prilagoditi raznim scenarijima napada, kao što su mrežni napadi, infekcije zlonamjernim softverom ili društvenog inženjeringa. Plavi tim je odgovoran za praćenje i odgovaranje na simulirane napade, pružajući povratne informacije crvenom timu o učinkovitosti njihovih tehnika napada. Rezultati testiranja zatim se koriste za poboljšanje sigurnosne pozicije organizacije, identificiranjem područja slabosti i preporukom specifičnih radnji za jačanje obrane, [9].

2.3. Razlike ljubičastog tima u odnosu na druge pristupe

Ljubičasti tim razlikuje se od tradicionalnih pristupa testiranju i procjeni kibernetičke sigurnosti na nekoliko načina.

Prije svega, tradicionalan pristup obično koristi penetracijsko testiranje ili skeniranje ranjivosti kako bi se identificirale ranjivosti i slabosti u obrani organizacije. Prednost ljubičastog tima je suradnja crvenog i plavog tima, te usmjerenost na kontinuirano poboljšanje sigurnosnog stava organizacije.

Osim toga, tradicionalni pristupi često su reaktivne prirode i usmjereni na identificiranje i otklanjanje postojećih slabosti. Ljubičasti tim ima proaktivan pristup simuliranjem napada i testiranjem obrane u kontroliranom okruženju, omogućujući organizacijama da identificiraju i otklone potencijalne slabosti prije nego što ih stvarni zlonamjerni akteri mogu iskoristiti.

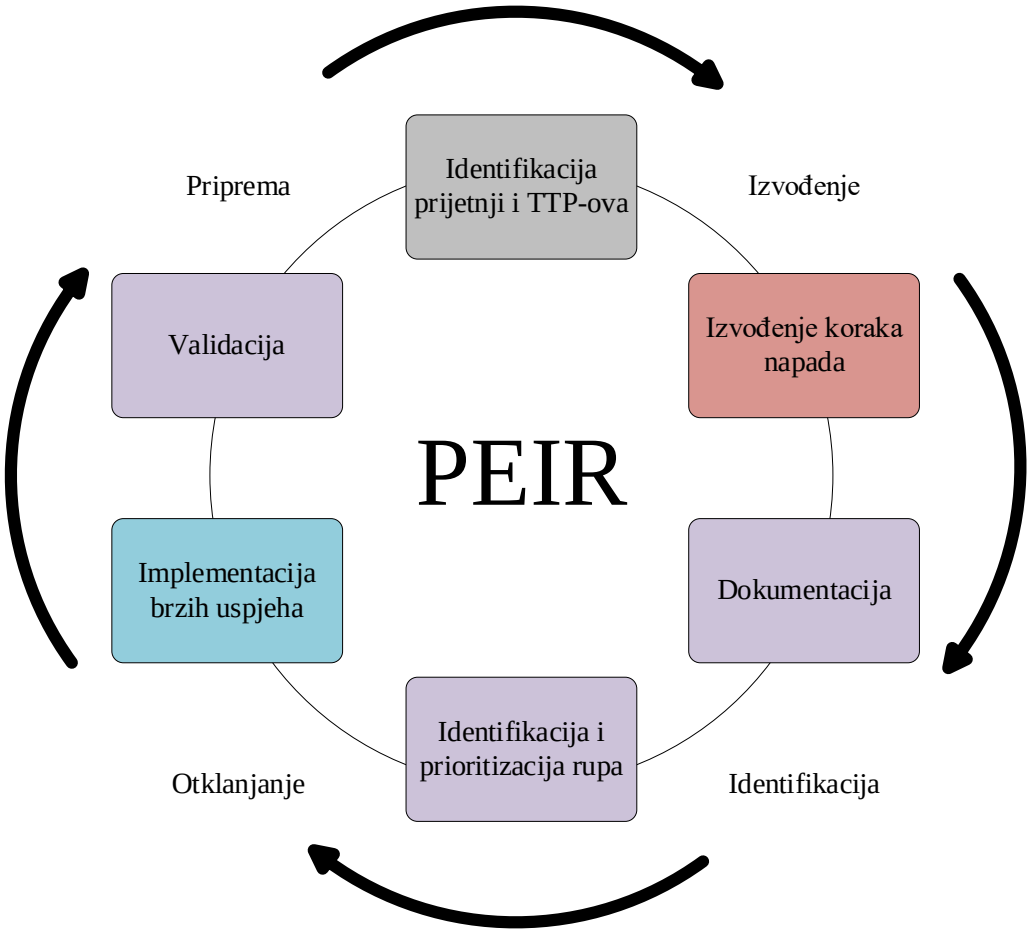
Također, tradicionalni pristupi često su odvojeni, s minimalno komunikacije i suradnje između različitih timova uključenih u testiranje i procjenu kibernetičke sigurnosti. Ljubičasti tim naglašava suradnju i komunikaciju između crvenog i plavog tima, omogućujući cjeloviti i integrirani pristup testiranju i procjeni sigurnosti.

Ukratko, glavna razlika između ljubičastog tima i tradicionalnih pristupa je ta što ljubičasti tim naglašava suradnju, proaktivno testiranje i cjeloviti pristup testiranju i procjeni sigurnosti organizacije, [10].

3. Opis i metodologija ljubičastog tima

Metodologija ljubičastog tima ima suradnički pristup testiranju i procjeni kibernetičke sigurnosti koji kombinira ofenzivne taktike crvenog tima s obrambenim tehnikama plavog tima. Cilj ljubičastog tima je poboljšati cjelokupni sigurnosni stav organizacije identificiranjem ranjivosti i slabosti u njenim sustavima i procesima te razvijanjem učinkovitih strategija za njihovo ublažavanje. PDCA (engl. *Plan-Do-Check-Act*) proces je široko je prepoznat model za kontinuirano poboljšanje u različitim industrijama, uključujući kibernetičku sigurnost. U kontekstu ljubičastog tima, PDCA proces može se primijeniti kako bi se vodilo stalno poboljšanje sigurnosnih mjera i sposobnosti odgovora na sigurnosne incidente. Taj model je kasnije prilagođen kako bi bolje odgovarao potrebama ljubičastog tima, iz čega je proizašao PEIR (engl. *Prepare-Execute-Identify-Remediate*) model.

3.1. PEIR model



Slika 4: PEIR dijagram
Izvor: [5]

Ovaj dijagram predstavlja pristup visoke razine ljubičastom timu u kojem su uključeni voditelji i ofenzivnog i defenzivnog sigurnosnog tima. Članovi plavog tima mogu i ne moraju biti obaviješteni o izvođenju vježbi. Cilj crvenog tima je neprimjetna procjena sposobnosti odgovora plavog tima na incident. Vježba ljubičastog tima ovdje je moguća bez informiranja većine plavog tima o vježbi, dok crveni tim koristi aktivnosti poput injektiranja log-ova i bezopasnih tehnika kako bi procijenili sposobnosti i kontrole plavog tima kao što su istraživanje, eskalacija i odgovor.

- Priprema – ova faza uključuje definiranje ciljeva opsega vježbe ljubičastog tima, uspostavljanje pravila angažmana i identifikaciju potrebnih resursa. Tijekom ove faze, plavi i crveni timovi također trebaju surađivati u planiranju vježbe, što uključuje stvaranje scenarija i odabir alata i tehnika koje će se koristiti.
- Izvođenje – u ovoj fazi provode se stvarne vježbe, u kojoj crveni tim simulira napade, a plavi tim se brani protiv njih. Ova se faza može ponoviti više puta , pri čemu se svako ponavljanje fokusira na određeni scenarij. Rezultati svakog ponavljanja su dokumentirani, te potom analizirani kako bi se identificirala područja koja je moguće poboljšati.
- Identifikacija – ova faza uključuje analizu rezultata vježbe kako bi se identificirale prednosti i nedostaci sigurnosnog stava organizacije. Plavi tim treba dokumentirati svoje obrambene taktike, dok bi crveni tim trebao dati povratne informacije o učinkovitosti tih taktika. Cilj ove faze je identificirati nedostatke u sigurnosnom stavu i dati prioritet rješavanju nedostataka na temelju razine rizika.
- Otklanjanje – ova faza uključuje provedbu promjena kako bi se riješili sigurnosni nedostaci. To uključuje poboljšanje sigurnosnih kontrola, ažuriranje politika i procedura te pružanje dodatne obuke osoblju. Također se treba obuhvatiti pregled napravljenih promjena i rezultata vježbe kako bi se osiguralo da se sigurnosni stav organizacije poboljšao, [5].

3.2. Uloga crvenog i plavog tima

Crveni tim, također zvan i ofenzivni tim, za svrhu ima oponašati taktike, tehnike i postupke zlonamjernog aktera iz stvarnog svijeta. Taj tim simulira zlonamjernog aktera, pokušavajući pronaći i iskoristiti ranjivosti u sigurnosnim obranama organizacije. Cilj crvenog tima je pomoći organizaciji da shvati gdje su njene obrane slabe i identificira područja za poboljšanje. Crveni tim obično ima opsežno znanje i iskustvo kod ofenzivnih sigurnosnih

tehnika i alata, poput penetracijskog testiranja, socijalnog inženjeringa i izviđanja. To znanje koriste za simulaciju realističnog napada na mreže, aplikacije i sustave organizacije. Neke od metoda napada koje crveni timovi koriste su iskorištavanje poznatih ranjivosti, korištenje taktika socijalnog inženjeringa i korištenje prilagođenog zlonamjernog softvera, [11].

Neki od primjera scenarija crvenog tima su:

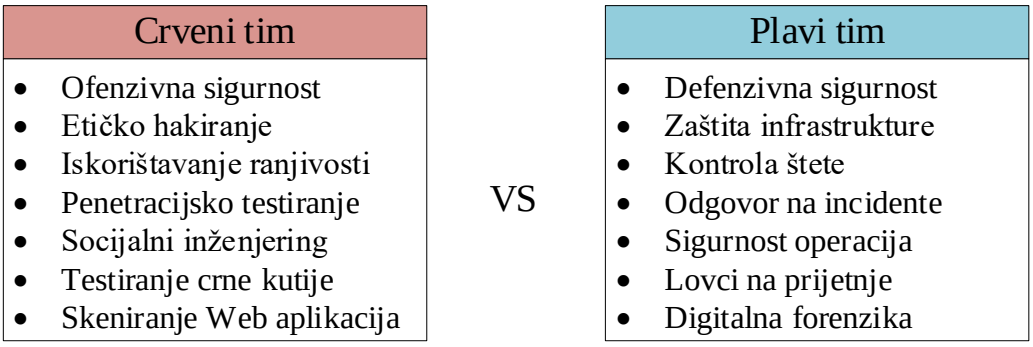
- Ostavljanje USB (engl. *Universal Serial Bus*) prijenosne memorije na ulazu organizacije, u nadi da će ga radnik uzeti i ukopčati u računalo
- Dolazak u organizaciju obučen kao serviser, pokušavajući dobiti fizički pristup LAN-u, ili serverskoj sobi, ili čak ukrasti tuđe računalo pod pričom „potreban je servis“ te tako zaobići restrikciju fizičkog pristupa
- Napredni socijalni inženjering, kao što je slanje elektroničke pošte zaposlenicima sa svrhom krađe identiteta ili dobivanja neovlaštenog pristupa (prijašnje spomenuti *phishing* napadi), telefonski pozivi, poštanski paketi i sl.

Plavi tim je skupina stručnjaka odgovorna za obranu organizacijskih informacijskih sustava održavanjem sigurnosnog stava. Glavni cilj plavog tima je analizirati trenutni sigurnosni stav organizacije i poduzimanje mjera za otklanjanje ranjivosti i nedostataka. Nadalje, plavi tim prati mrežu organizacije i reagira na sve sumnjive aktivnosti koje se događaju u njoj.

Za ostvarivanje željenih ciljeva plavi tim koristi razne elemente koji su podijeljeni u tri skupine:

- Ljudi: sigurnosna osviještenost, sigurnosni analitičari, forenzički specijalisti, analisti malicioznog softvera, SOC timovi, developeri, itd. U manjim organizacijama, često jedna osoba ima više takvih uloga.
- Procesi: Standardni NIST/SANS bazirani odgovori na incidente (priprema, identifikacija, karantena, eliminacija, oporavak, stečena iskustva), interne sigurnosne politike, standardne operativne procedure – SOP, itd.
- Proizvodi i tehnologije: SIEM kao jedan od glavnih alata koje koristi SOC, EDR (engl. *endpoint detection and response*), IDS (engl. *intrusion detection systems*), itd., [12].

Na sljedećoj slici prikazati će se usporedba između klasičnog crvenog i plavog tima:



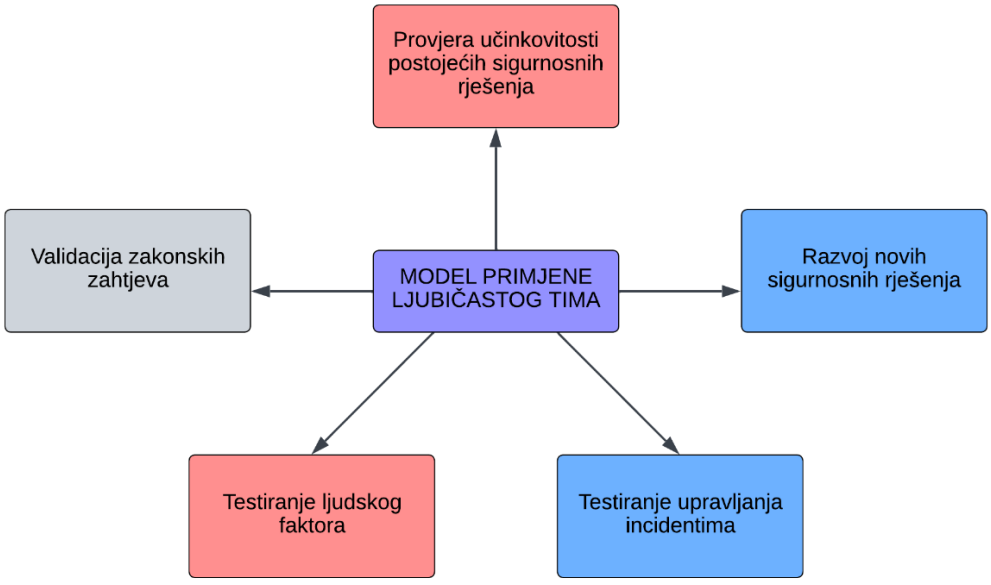
Slika 5: Usporedba klasičnog crvenog i plavog tima

Ukratko, crveni tim sastoji se od stručnjaka za ofenzivnu sigurnost koji se specijaliziraju za proboj obrane i ciljanje sustava. S druge strance, plavi tim sastoji se od stručnjaka za defenzivnu sigurnost koji su zaduženi za održavanje unutarnje mrežne obrane protiv kibernetičkih prijetnji i opasnosti. Crveni timovi često oponašaju napade kako bi testirali plavi tim i istovremeno učinkovitost sigurnosti mreže.

4. Primjena ljubičastog tima u praksi

Implementacija ljubičastog tima u organizacijama ovisi o njenim potrebama i ciljevima. Autor ovdje predstavlja vlastiti model koji predstavlja univerzalan način primjenjivanja ljubičastog tima u organizacijama. Sastoji se od 5 komponenti:

1. Provjera učinkovitosti postojećih sigurnosnih rješenja: Timovi simuliraju napade kako bi provjerili koliko su dobro sigurnosna rješenja pripremljena za takve scenarije. Timovi isprobavaju razna sigurnosna rješenja za detekciju, sprječavanje i reagiranje na kibernetičke napade.
2. Razvoj novih sigurnosnih rješenja: Zajednički rad crvenog i plavog tima omogućuje „*outside the box*“ način razmišljanja i razvijanja inovativnih rješenja. Te nove perspektive donose kreativnost i zaokruženije razumijevanje kibernetičke sigurnosti.
3. Testiranje upravljanja incidentima: Podrazumijeva simulaciju napada u svrhu testiranja sposobnosti organizacije da odgovori na njih. Rezultat toga je identifikacija slabosti u postojećim procesima organizacije, nakon čega slijedi izrađivanje planova za poboljšanje.
4. Testiranje ljudskog faktora: Timovi mogu simulirati napade kako bi vidjeli koliko dobro zaposlenici reagiraju na takve scenarije. Mogu se identificirati područja za poboljšanje u obuci i svijesti o digitalnoj sigurnosti.
5. Validacija zakonskih zahtjeva: Timovi provjeravaju usklađenost organizacije sa zakonima i propisima u području kibernetičke sigurnosti.



Slika 6: Model primjene ljubičastog tima u organizacijama

Neke od organizacija koje koriste ljubičasti tim u stvarnom svijetu su: Microsoft, Packetlabs, Nettitude, međutim s obzirom na to da je ljubičasti tim još uvijek novi pojam koji nije službeno definiran i dokumentiran, svaka organizacija ima svoju ideju što točno ljubičasti tim treba predstavljati i kako treba funkcionirati.

4.1. Evaluacija učinkovitosti ljubičastog tima

Autor još jednom naglašava kako je pojam ljubičastog tima relativno nov i ne postoji puno materijala za istraživanje, međutim, po njegovom istraživanju i mišljenju, postoji nekoliko načina na koji se može napraviti evaluacija učinkovitosti ljubičastog tima:

- Mjerenjem vremena potrebnog za detekciju i odgovor na sigurnosne incidente
- Analiza poboljšanja sposobnosti organizacije da spriječi sigurnosne incidente
- Analiza povećanja otpornosti organizacije na kibernetičke napade
- Mjerenje poboljšanja sigurnosnog stava organizacije
- Analiza razine suradnje i komunikacije između crvenog i plavog tima

Bitno je napomenuti kako učinkovitost ljubičastog tima može ovisiti o specifičnim ciljevima vježbe, kao i o sigurnosnom stavu organizacije.

Također, postoje i standardne, dobro poznate metrike koje se koriste za evaluaciju sigurnosnog stava organizacije:

Prosječno vrijeme otkrivanja (engl. *Mean time to detect*, MTTD): prosječno vrijeme potrebno da sigurnosni tim detektira sigurnosni incident. Mjeri se kao ukupno vrijeme potrebno da tim detektira incidente u danom vremenskom periodu podijeljen s brojem incidenata. Ova metrika koristi se za evaluaciju učinkovitosti između timova ili za mjerenje trenutnih nadzornih kontrola. Na primjer, ako neki tim prijavi 10 incidenata u mjesecu, a vrijeme detekcije 1000 minuta, MTTD računa se po formuli (1):

$$MTTD = \frac{10}{1000} = 100\ minuta\ za\ detekciju \quad (1)$$

Korištenjem ove metrike, mogu se pronaći načini kako bi se smanjilo vrijeme koje maliciozni akteri provode u sustavu organizacije.

Prosječno vrijeme reakcije (engl. *Mean time to acknowledge*, MTTA): prosječno vrijeme između trenutka kada sustav generira obavijest i trenutka kada zaposlenik reagira na

obavijest. Dok MTTD mjeri vrijeme potrebno za detekciju ili obavještavanje incidenta, MTTA mjeri vrijeme potrebno do započinjanja rješavanja problema.

Prosječno vrijeme oporavka (engl. *Mean time to recovery*, MTTR): prosječno vrijeme potrebno da se zaposlenici ili sustav vrati u normalno radno stanje. Ova metrika daje uvid u to koliko brzo tim odgovora na incidente može vratiti radno stanje organizacije u normalu. Dakle, može se reći da je MTTR sveukupno vrijeme koje je sustav ili organizacija nije funkcionirala zbog nekog sigurnosnog incidenta kroz određen broj incidenata. Na primjer, ako je sveukupno vrijeme nedostupnosti bio 20 minuta, a broj incidenata koji su prouzrokovali tu nedostupnost 2, znači da se MTTR može izračunati prema formuli (2):

$$MTTR = \frac{20}{2} = 10\ minuta \tag{2}$$

Ova metrika daje uvid jeli neki sustav predugo bio nedostupan. Ako je, znači postoji neki problem i organizacija zna gdje treba staviti fokus na daljnje istraživanje.

Prosječno vrijeme za suzbijanje (engl. *Mean time to contain*, MTTC): daje holistički pogled na koliko dobro organizacija odgovara na incidente spajanjem prijašnje tri metrike. Da bi se MTTC izračunao, uzima se suma sati potrošenih na otkrivanje, reagiranje i oporavak, tj. efektivno vrijeme potrebno za prevenciju dodane štete načinjenu od zlonamjernog aktera. Na primjer, ako je organizacija imala 2 incidenta gdje je bilo potrebno 3 sata za detekciju svakog, 2 sata za reagiranje na pojedini incident, te 5 sati pojedinačno na oporavak, tada se MTTC računa se prema formuli (3):

$$MTTC = \frac{2 + 2 + 3 + 3 + 5 + 5}{2} = 10\ sati \tag{3}$$

Dostupnost sustava: metrika koja pokazuje koliko je sustav vremena radio ispravno u nekom vremenskom periodu, najčešće u jednoj godini, iskazuje se u postocima, npr. 90%. Što je postotak veći, to bolje, jer ako je postotak dostupnosti sustava veći naspram prijašnjih godina, to znači da su mjere poduzete u međuvremenu kako bi se ta metrika poboljšala efektivne.

Sporazum o razini usluge (engl. *Service level agreement*, SLA): ugovor koji sadržava npr. ugovorenu razinu dostupnosti sustava kroz godinu i vrijeme oporavka. Služi kako bi se ugovorene vrijednosti usporedile s onima iz stvarnosti te procijenio rad treće stranke s kojom je napravljen ugovor. Ako treća strana ne zadovoljava standarde, potrebno je naći drugog partnera.

Prosječno vrijeme između kvarova (engl. *Mean time between failures,* MTBF): mjereno vrijeme između kvarova sustava, može se mjeriti kao ukupan broj sati tijekom kojeg je sustav radio u nekom periodu podijeljen s brojem kvarova u tom istom periodu. Npr. ako je sustav radio 5000 sati tijekom jednog mjeseca, a bilo je 3 kvara, MTBF se računa po formuli (4):

$$MTBF = \frac{5000}{3} = 1667\ sati\ između\ kvarova \quad (4)$$

U kontekstu kibernetičke sigurnosti, MTBF može biti pokazatelj da je sustav pri kraju svog radnog života te da je stoga i najslabija karika u sigurnosti organizacije, [13].

4.2. Prednosti i izazovi u primjeni ljubičastog tima

Ljubičasti tim ima nekoliko prednosti. Prije svega, poboljšava sigurnosni položaj organizacije redovnim provjerama. Omogućava pregled trenutne strategije kibernetičke sigurnosti organizacije kako bi se provjerila reakcija plavog tima na napade. Crveni tim provodi različite aktivnosti kako bi vidjeli sigurnosni stav organizacije. Zatim, ljubičasti tim omogućava voditeljima da vide kakav povrat ulaganja (engl. *Return on Investment,* ROI) organizacija dobiva za svoje troškove kibernetičke sigurnosti. Ljubičasti tim omogućava organizacijama da se fokusiraju na prijetnje s kojima će se suočiti i kako će upravljati tim prijetnjama.

Glavni cilj ljubičastog tima je pružiti sveobuhvatan, koordiniran pristup sigurnosti koji kombinira napadačke i obrambene strategije. Nastoji se kontinuirano poboljšavati sigurnosni stav organizacije identificiranjem slabosti i praznina u obrani kroz vježbe ljubičastog tima, te nakon toga razvojem i implementacijom planova za njihovo rješenje. Neki od benefita implementacije ljubičastog tima u organizacijama su:

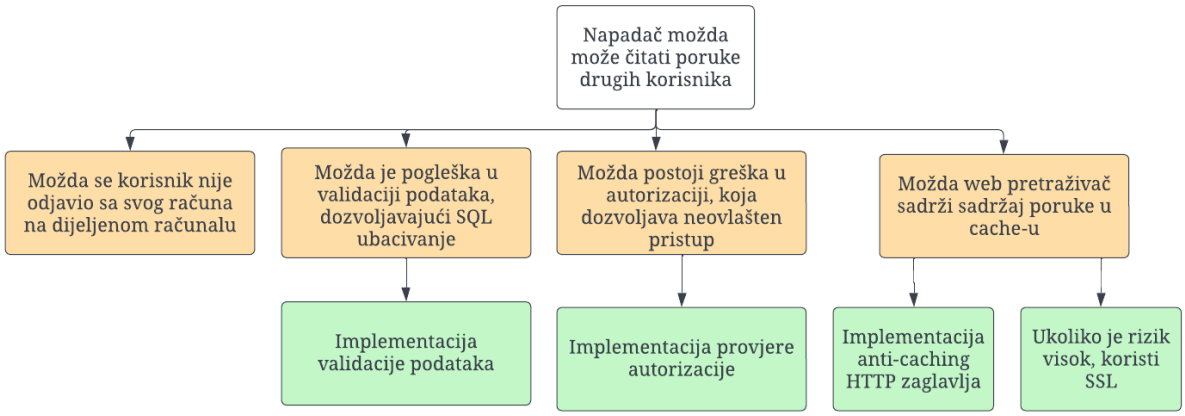
- Brže jačanje ukupne kibernetičke sigurnosti: Ljubičasti tim može pomoći u prepoznavanju ranjivosti i slabosti sigurnosnog stava organizacije. Organizacija može riješiti ove probleme implementacijom boljih politika, procedura i tehnologija.
- Poboljšanje sposobnosti otkrivanja ranjivosti: Ljubičasti tim može pomoći sigurnosnim stručnjacima da bolje razumiju kako napadači razmišljaju i djeluju, olakšavajući prepoznavanje potencijalnih ranjivosti prije nego što ih se iskoristi.
- Stalne povratne informacije: Ljubičasti tim pruža stalnu petlju povratnih informacija između plavih i crvenih timova, što može pomoći u prepoznavanju područja za poboljšanje, [14].

4.3. Primjeri izvođenja vježbi ljubičastog tima u organizacijama

Po mišljenju autora, neki od najboljih načina izvođenja vježbi ljubičastog tima u organizacijama su sljedeći:

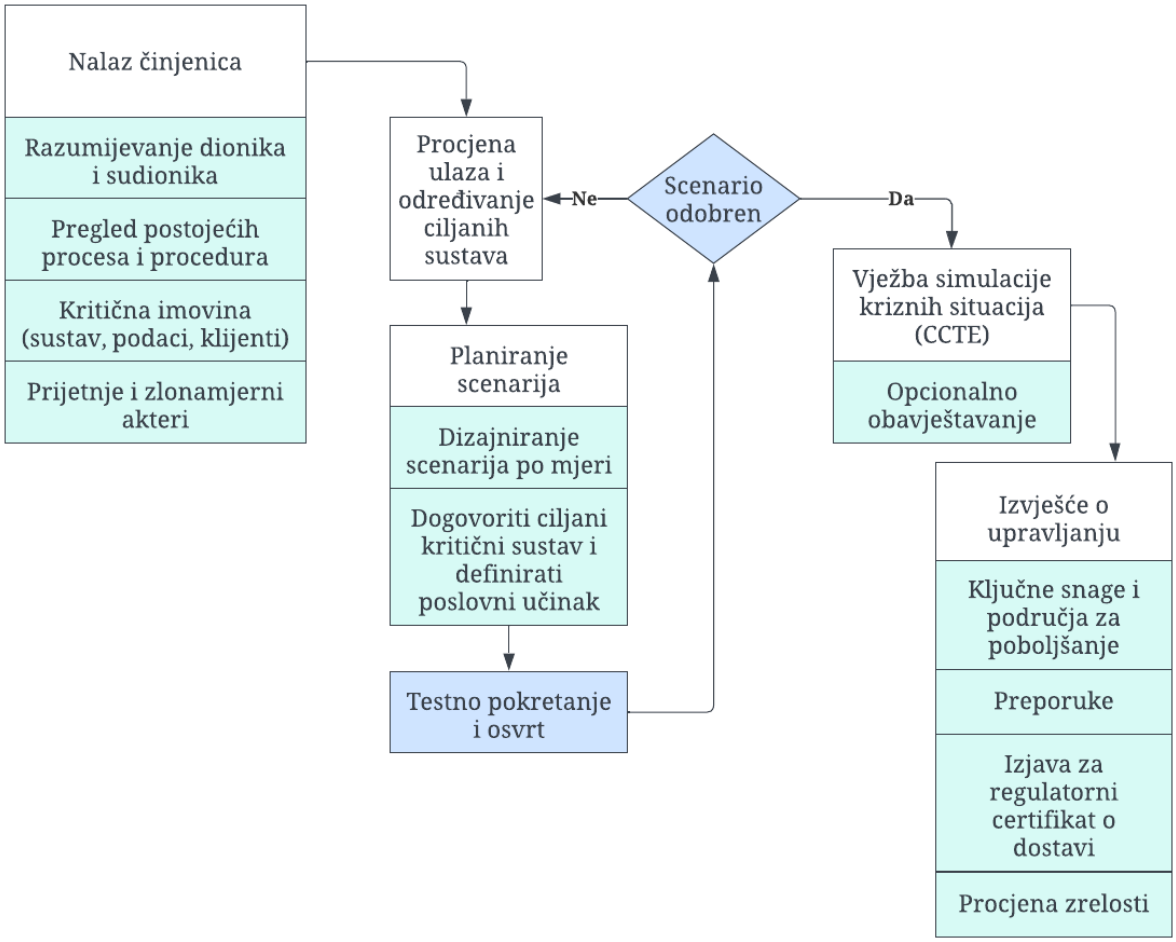
- Baziran na scenarijima (engl. *Scenario-based*): vježbe uključuju simulaciju stvarnih prijetnji ili scenarija napada, koji se temelje na poznatim i stvarnim događajima iz prošlosti, [15].
- U stvarnom okruženju (engl. *Live-fire*): vježbe uključuju korištenje stvarnih napadačkih tehnika na stvarnim sustavima u kontroliranom okruženju, u svrhu testiranja reakcije organizacije na stvarni napad. S obzirom na to da je ovo vrlo realistična metoda, zahtjeva veliku količinu planiranja i koordinacije, a može otkriti stvarne slabosti u sustavu. [16].
- Modeliranje prijetnji (engl. *Threat modeling*): vježbe uključuju izradu modela prijetnji koji predstavljaju stvarne prijetnje organizaciji. Timovi za sigurnost i razvoj rade zajedno kako bi se identificirale slabosti u sustavu i razvile nove sigurnosne mjere kako bi se organizacija bolje zaštitila, [17].

  Analiza prijetnje može se prikazati sljedećim dijagramom:



Slika 7: Stablo prijetnje za slučaj neovlaštenog pristupa poruka zaposlenika
Izvor: [18]

- Vježba „za stolom“ (engl. *Tabletop*): vježbe uključuju simulaciju različitih scenarija prijetnji u kontroliranom okruženju, ali bez korištenja stvarnih sustava. Timovi za sigurnost i razvoj zajedno rade na identifikaciji sigurnosnih problema i razvijaju nove strategije kako bi se organizacija bolje zaštitila u slučaju napada, [19].



Slika 8: Dijagram pristupa vježbi „za stolom“
Izvor: [20]

5. Istraživanje alata i tehnika ljubičastog tima

Alati koji je koriste u vježbama ljubičastog tima kombinacija su alata koje danas koriste crveni i plavi timovi. Međutim, postoji nekoliko alata koji su napravljeni s ljubičastim timom na umu. Neki alati su više fokusirani na tehničke aspekte ljubičastog tima, a neki su napravljeni imajući kolaboraciju i dokumentaciju na umu. U ovom poglavlju proći će se kroz razne alate otvorenog koda, koji su također besplatni i najbliže predstavljaju ideju ljubičastog tima.

Autor još jednom podsjeća na razliku između emulacije zlonamjernog aktera i simulacije zlonamjernog aktera, ali ovaj put u pogledu ljubičastog tima. Važno je razumjeti razliku, posebno činjenicu da je CTI (engl. *Cyber Threat Intelligence*) upravo ulaz koji će učiniti simulaciju realističnijom i stoga ju čini emulacijom.

Atomski crveni tim (engl. *Atomic Red Team*, ART) kolekcija je jednostavnih i modularnih testova koje organizacije mogu koristiti za provjeru svojih sigurnosnih kontrola i osiguravanje da njihove sposobnosti otkrivanja i odgovora djeluju učinkovito. U kontekstu ljubičastog tima, ART se može koristiti kao alat za podršku u procesu stvaranja i izvođenja scenarija crvenog tima. ART testovi mogu se koristiti za simuliranje specifičnih tehnika i taktika napada koje su poznate da ih koriste stvarne prijetnje. Crveni tim može koristiti te testove za procjenu učinkovitosti sposobnosti otkrivanja i odgovora organizacije na te tehnike. Nakon što se završe ART testovi, rezultati se dijele sa sigurnosnim timom. Tada se te informacije mogu koristiti kako bi se identificirala područja gdje se sigurnosne kontrole organizacije mogu poboljšati. ART testovi također se mogu koristiti za potvrdu promjena napravljenih na sigurnosnim kontrolama, kao dokaz učinkovitosti, [21].

Caldera je platforma koja se može koristiti u vježbama ljubičastog tima za simulaciju napada i testiranje učinkovitosti organizacije da se obrani. Nudi raspon alata koji omogućavaju ljubičastom timu izvođene raznih simulacija i scenarija napada u svrhu identifikacije potencijalne slabosti i ranjivosti u sigurnosnom stavu organizacije. Simulacijom scenarija napada iz stvarnog svijeta, sigurnosni analitičari mogu testirati i potvrditi svoje sigurnosne kontrole i sposobnosti odgovora na incidente. Neki od primjera napade koje Caldera može simulirati su napad zlonamjernim softverom, napad krađe identiteta, [22].

VECTR je platforma koja se koristi u ljubičastom timu za vizualizaciju i analizu *cyber kill chain*-a. Pruža okvir za organiziranje podataka o različitim fazama napada i analizu uzoraka napada. VECTR se često koristi za podršku stvaranju modela prijetnji i simuliranje napada na

te modele. VECTR je osmišljen za promicanje transparentnosti između napada i obrane, poticanje obuke između članova tima i poboljšanje stope uspješnosti otkrivanja i prevencije kibernetičkih napada u cijelom okruženju organizacije, [23].

Picus Security je platforma koja se koristi u ljubičastom timu za kontinuiranu validaciju sigurnosti. Omogućava sigurnosnim timovima da provjere svoje obrane protiv stvarnih prijetnji te otkriju i odrede prioritete ranjivosti prije nego što one mogu biti iskorištene. Kod ljubičastog tima, Picus security može se koristiti za simuliranje napada i procjenu učinkovitosti defenzivnih kontrola. Rezultati tih simulacija se zatim mogu koristiti za poboljšanje sigurnosnog stava organizacije i optimizaciju raspodjele resursa za bolje sigurnosne rezultate, [24].

Ovo su bili neki od alata koji su korisni kako bi se poboljšala sigurnost organizacije, ali se skoro nikad ne koriste samostalno, nego u sklopu paketa alata. Sada će se predstaviti relativno nova ideja u kibernetičkoj sigurnosti, kibernetičko zavaravanje (engl. *Cyber deception*). Nije pitanje hoće li neki zlonamjerni akter pokušati kompromitirati resurse organizacije, nego kada. Stoga, autor ovog rada smatra da je kibernetičko zavaravanje puno realističnija strategija obrane nego klasični pristup plavog tima, gdje je cilj u potpunosti zaustaviti scenarij kompromitiranja organizacije na prvom mjestu.

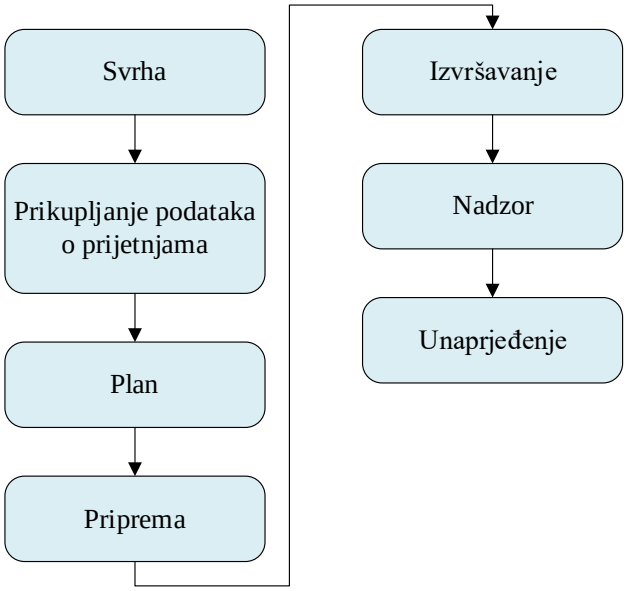
Kibernetičko zavaravanje defenzivna je strategija koja uključuje namjerno postavljanje i raspoređivanje zavaravajućih elemenata unutar mreže organizacije kako bi se otkrili, odvratili i prevarili potencijalni zlonamjerni akteri. Cilj ove strategije je povećati troškove resursa i vremena zlonamjernog aktera tako što ih se vodi u zamke i zavaravanje, dok istovremeno pruža rane znakove neovlaštene aktivnosti.

Koncept je jednostavan: kibernetičko zavaravanje djeluje na principu obmanjivanja zlonamjernog aktera tako što im se predstavljaju lažne informacije, te ih se potiče da stupaju u interakciju s mamcem sustava, mreže ili podataka. Glavni ciljevi su rano otkrivanje napada, prikupljanje prijetnji, odgađanje napada, odvraćanje njihove pažnje i dobivanje uvida u njihove taktike, tehnike i motivacije. Obmanjujući elementi (lažne informacije) mogu poprimiti različite oblike, poput lažnih računa, izmišljenih podataka, lažnih vjerodajnica, *honey* tokena, *honeypot*-ova i krušnih mrvica (engl. *breadcrumbs*). Ti elementi su dizajnirani da oponašaju stvarnu imovinu i potiču zlonamjerne aktere da se s njom angažiranju.

Honeypots su izolirani sustavi ili mreže namjerno stvoreni kako bi privukli zlonamjerne aktere. Izgledaju ranjivo kako bi odvratili zlonamjerne aktere od kritične imovine, kupujući vrijeme za defenzivni tim da promatraju njihovo ponašanje i prikupljaju obavještajne podatke.

Decoy sustavi, s druge strane, mogu se rasporediti uz stvarne sustave kako bi se zlonamjerni akteri zbunili i tako otežali razlikovanje stvarne i lažne imovine.

Na sljedećoj slici prikazan je lanac kibernetičkog zavaravanja koji će pomoći u razumijevanju životnog ciklusa ove operacije. Opisuje različite faze uključene u provedbu uspješne strategije kibernetičkog zavaravanja.



Slika 9: Lanac kibernetičkog zavaravanja
Izvor: [25]

1) Svrha: Početna faza gdje se definiraju strateški, operativni i taktički cilj za operacije zavaravanja, tj. svrha zavaravanja, te kriteriji koji bi ukazivali na uspjeh zavaravanja.
2) Prikupljanje podataka o prijetnjama: Definira se očekivano ponašanje zlonamjernih aktera. Pomaže utvrditi uspješnost zavaravanja.
3) Plan: Analizira karakteristika stvarnog događaja, identifikacija odgovarajućih potpisa (engl. *signatures*) zlonamjernog aktera, te planiranje taktika zavaravanja (maskiranje, prepakiranje, označavanje itd.). Također se analiziraju obilježja zamišljenih događaja i aktivnosti koje se moraju prikazati i promatrati.

4) Priprema: Dizajniraju se željeni perceptivni i kognitivni učinci na zlonamjernog aktera i istraživanje dostupnih sredstva i resursa za stvaranje tih učinaka.
5) Izvršavanje: Koordinacija i kontrola svih relevantnih operacija kako bi se dosljedno, vjerodostojno i učinkovito izvršila strategija zavaravanja.
6) Nadzor: Planeri surađuju s analitičarima obavještajnih podataka o kibernetičkim prijetnjama. To podrazumijeva praćenje defenzivnih i neprijateljskih operativnih priprema, izvore odabrane za prenošenje zavaravanja zlonamjernog aktera itd.
7) Unaprjeđenje: Ako se ukazuje na to da trenutne taktike zavaravanja nemaju željeni učinak na zlonamjernog aktera, potrebno je unaprijediti taktike i ponovno razmotriti prvu fazu lanca zavaravanja, izvršavanje sigurnosnog zavaravanja ili plan, [25].

6. Studija slučaja

U ovoj cjelini proveden je praktični dio diplomskog rada u kojem je postavljeno virtualno okruženje koje se sastoji od dvije virtualne mašine, gdje jedna predstavlja crveni tim, a druga plavi tim. Crveni tim simulira zlonamjernog aktera, a u ovom slučaju, plavi tim simulira žrtvu kibernetičkog napada – organizaciju, tj. njene resurse. Za potrebe izvođenja praktičnog dijela korištena su saznanja iz prijašnjih poglavlja. Cilj praktičnog dijela je prikazati iskorištavanje vrlo poznate ranjivosti Log4j koja se dogodila krajem 2021. godine. Ranjivost Log4j predstavlja ozbiljnu kritičnu ranjivost daljinskog izvršavanja koda (engl. *Remote code execution,* RCE). Log4j može utjecati na bilo koju Java aplikaciju koja uključuje biblioteku Log4j verziju 2.15 ili stariju. Ovaj softver koristi se za snimanje raznih vrsta aktivnosti koje se odvijaju ispod haube u širokom rasponu računalnih sustava. Upravo ova studija slučaja pokazuje zašto je bitno ažurirati sustave s najnovijim sigurnosnim zakrpama i najnovijim verzijama softvera.

U nastavku će se opisati proces podizanja virtualnih mašina, instalaciju i postavljanje ranjive aplikacije te sami proces iskorištavanja ranjivosti.

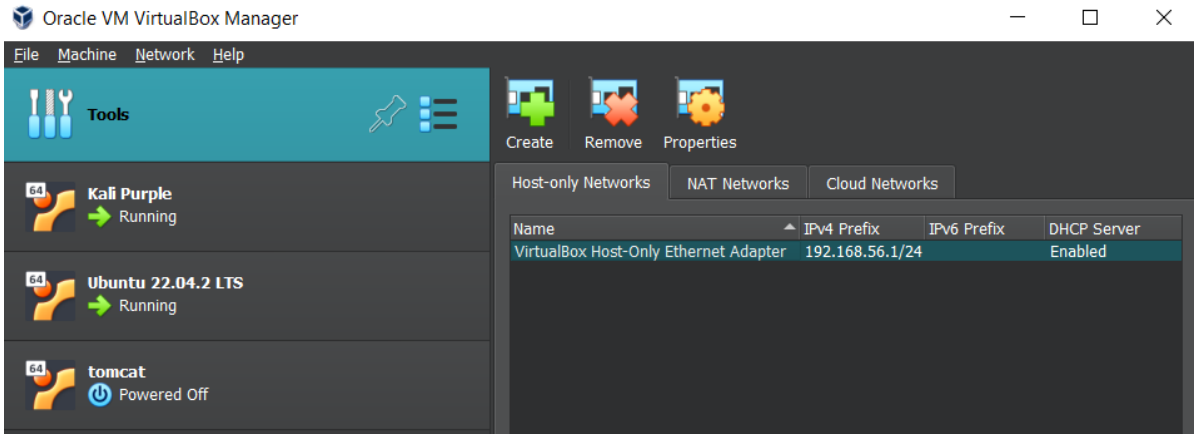
6.1. Napadačka virtualna mašina

U svrhu izvođenja ove vježbe, koristit će se Kali Purple distribucija Linuxa za napadačku mašinu. Za potrebe virtualizacije koristit će se Oracle VM VirtualBox Manager koji omogućuje stvaranje i korištenje virtualnih mašina. Instalacija samog programa je standardna i neće se opisati. Kreirane virtualne mašine su u izoliranom okruženju i mogu sadržavati različite operativne sustave. Neke od značajka ovog alata su:

- Mogućnost podizanja različitih operativnih sustava kao što su Windows, Linux ili MacOS na svaku pojedinu virtualnu mašinu, gdje sve mogu istovremeno raditi
- S obzirom na to da su mašine u izoliranom okruženju često se koriste za potrebe razvoja i testiranja aplikacija kroz razne operativne sustave. Još jedan benefit izoliranog okruženja je mogućnost testiranja potencijalno zlonamjernog softvera bez utjecaja na ostatak računala
- Mogućnost korištenja zastarjelih aplikacija kroz zastarjele operativne sustave, npr. u slučaju testiranja aplikacije koja radi isključivo na Windows XP operativnom sustavu
- Korištenje u edukacijske svrhe

- Sigurnosne kopije - u slučaju da virtualna mašina prestane raditi iz bilo kojeg razloga, moguće ju je vratiti u prijašnje stanje izradom sigurnosnih kopija. Sigurnosne kopije poželjno je kreirati redovito kako bi se izgubilo što manje podataka
- Simulacija mreža - Oracle VM ima mogućnost kreiranja virtualnih mreža, što je prikladno za testiranje raznih mrežnih topologija

Prije postavljanja virtualnih mašina, potrebno je kreirati i postaviti VLAN (engl. *Virtual Local Area Network*).



Slika 10: Kreiranje novog VLAN-a

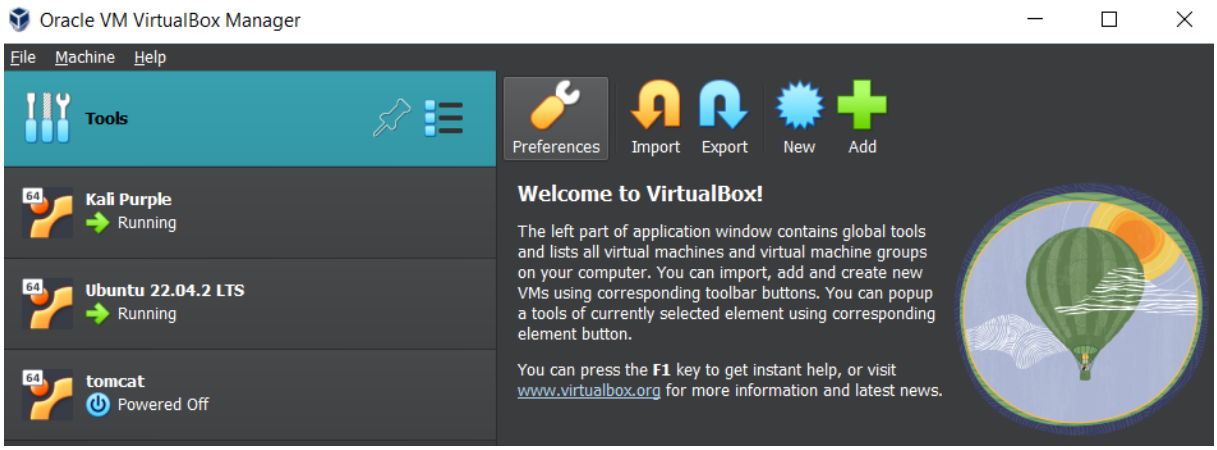
Ako ne postoji već kreiran VLAN, potrebno ga je kreirati i pravilno postaviti, kao što je vidljivo na slici 10. Virtualna lokalna mreža je potrebna kako bi se virtualne mašine mogle „vidjeti“, tj. kako bi napadačka mašina mogla izvršavati napade na ranjivu mašinu. Nakon toga, potrebno je kreirati napadačku mašinu.

Kali Linux jedan je od najpopularnijih distribucija Linux-a za potrebe raznih operacija kibernetičke sigurnosti, poput forenzičke analize, penetracijskog testiranja, analize mrežnih podataka, testiranje sigurnosti bežičnih mreža i web aplikacija, probijanja lozinki itd.

Kali Linux moguće je koristiti na raznim uređajima kao što su radne stanice, poslužitelji, osobna računala, mobilni uređaji itd. Alati koji su dostupni na ovoj distribuciji Linuxa su mnogobrojni te ih se može podijeliti na sljedeće grupe alata:

- Digitalna forenzika - alati za analizu sistemskih log-ova, proučavanje digitalnih dokaza, povratak izgubljenih podataka te odgovora na incidente.

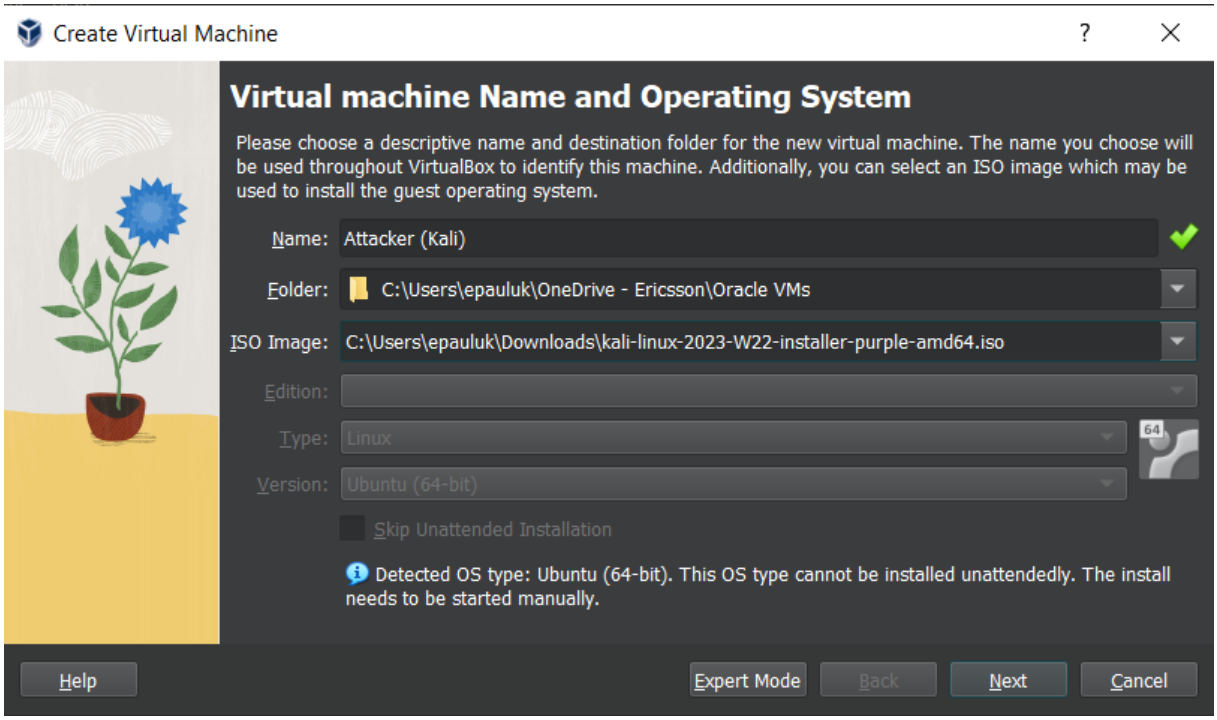
- Iskorištavanje ranjivosti - alati koji pomažu u procesu preuzimanja kontrole nad ranjivim uređajem, sustavom ili aplikacijom. Najčešće se to postiže podizanjem razine pristupa.
- Socijalni inženjering - alati koji omogućuju razne vektore napada s ciljem krađe identiteta ili dobivanja informacija.
- Izvješćivanje - prikupljanje svih relevantnih informacija potrebnih za izradu dokumentacije i izvještaja.
- Obrnuti inženjering - alati koji pomažu u simulaciji zlonamjernog aktera ili za identifikaciju ranjivosti sustava, a za defenzivne svrhe koriste se za analizu zlonamjernog softvera
- Probijanje lozinki - alati koji se koriste za probijanje korisničke lozinke, poput napada grubom silom ili napada pomoću rječnika, [26].



Slika 11: Oracle VM VirtualBox

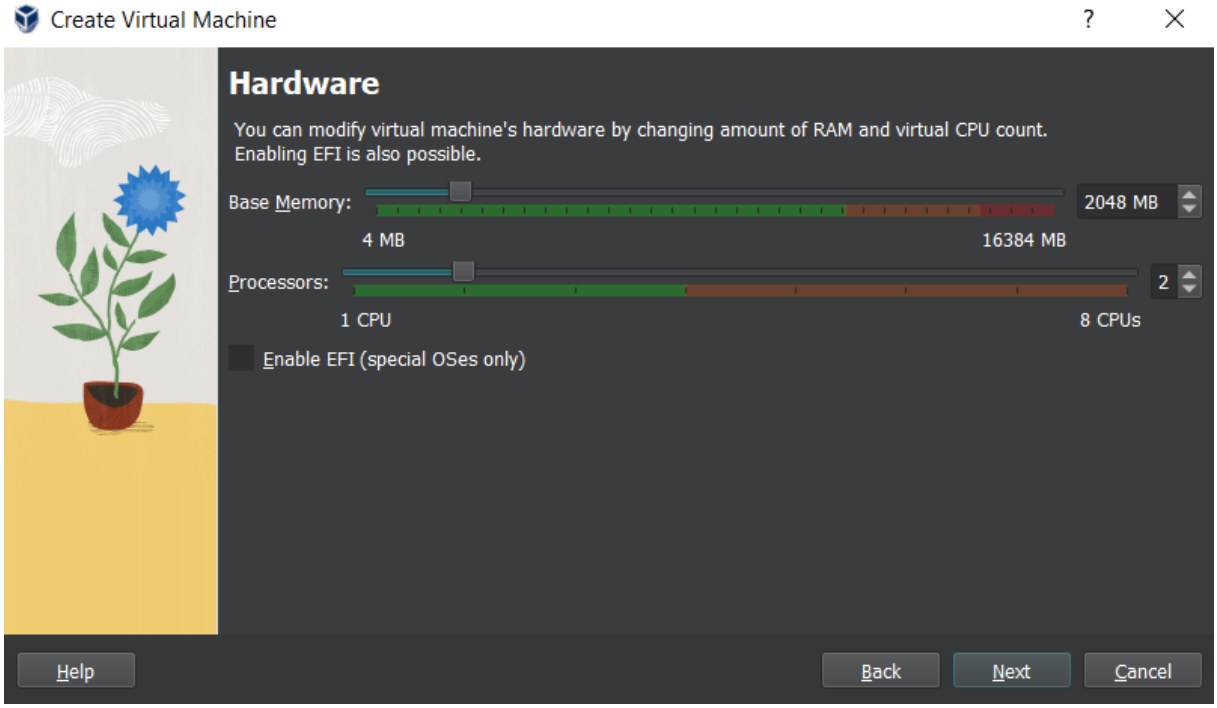
Kao što je i ranije spomenuto, za napadačku mašinu koristi se Kali Linux. Razlog zašto se koristi je zbog unaprijed instaliranih alata koji će se koristiti u ovoj studiji slučaja. Kali Linux je distribucija otvorenog koda, te je popularan izbor za svrhe kibernetičke sigurnosti.

Na slici 11 vidljiv je izbornik kreiranih virtualnih mašina unutar Oracle VM Virtualbox softvera. Osim što je virtualne mašine moguće kreirati, moguće ih je u uvesti, tj. određene distribucije moguće je direktno uvesti u Oracle VM Virtualbox jer su specifično kreirane za taj softver. To značajno olakšava proces kreiranja, jer ga se ustvari kompletno preskače. U ovom izborniku je također moguće urediti postavke pojedine virtualne mašine, kao što su dodijeljeno ime, računalni resursi, virtualna sučelja itd.



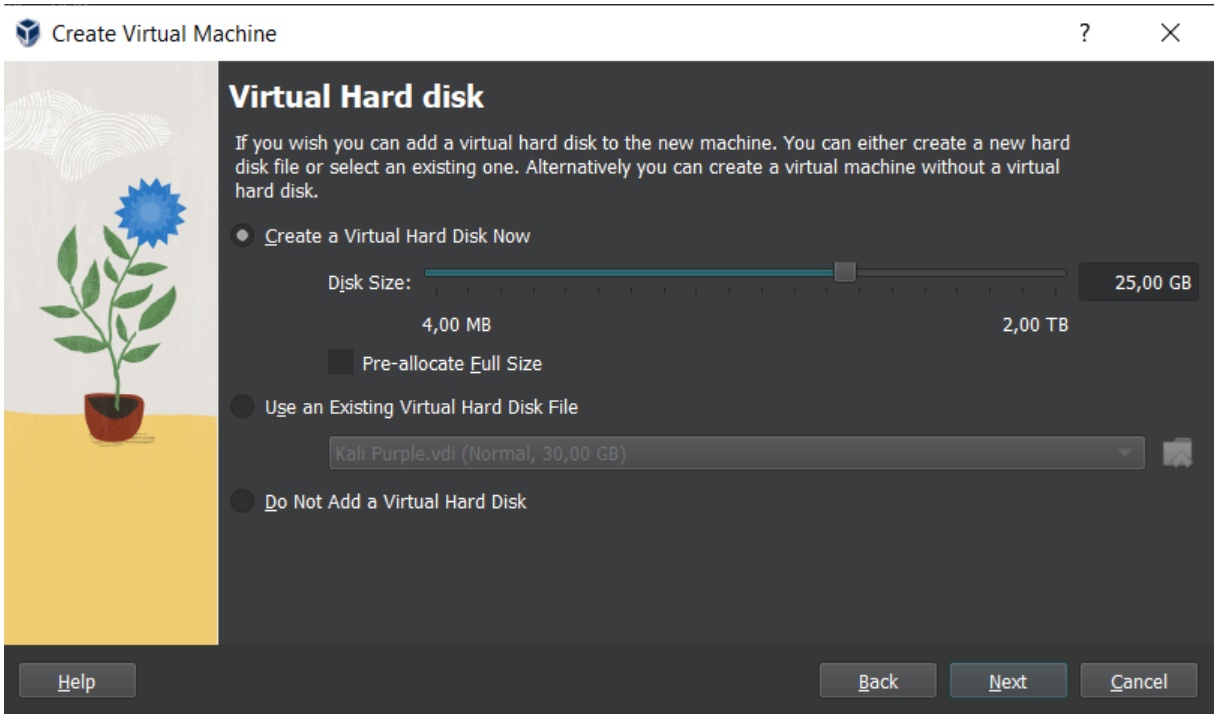
Slika 12: Imenovanje virtualne mašine

Na slici 12 vidljiv je prozor u procesu kreiranja napadačke virtualne mašine, gdje je potrebno unijeti naziv, direktorij u kojem će se nalaziti virtualna mašina, koja ISO slika (operativni sustav) će se instalirati na mašinu itd.



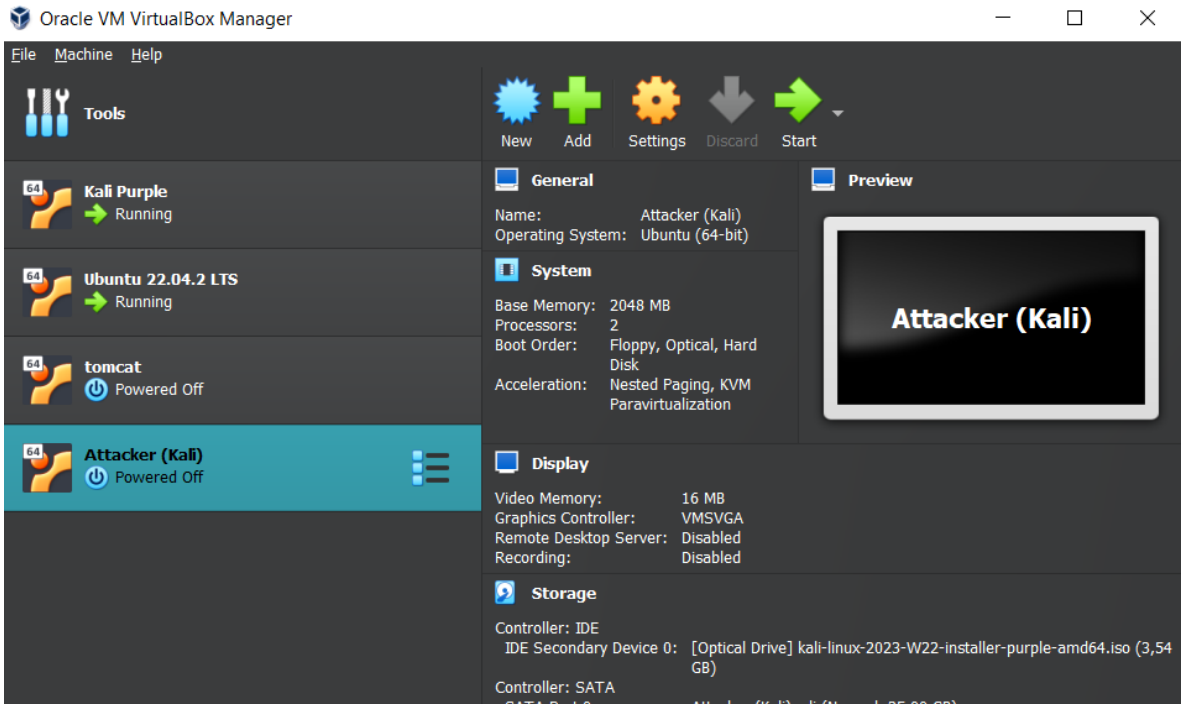
Slika 13: Dodjeljivanje količine RAM-a i procesorskih jezgri

Na slici 13 vidljiv je prozor postavljanja virtualnog hardvera, tj. resursa kojima će virtualna mašina pristupati. Potrebno je dodijeliti dovoljno računalnih resursa za gladak rad.

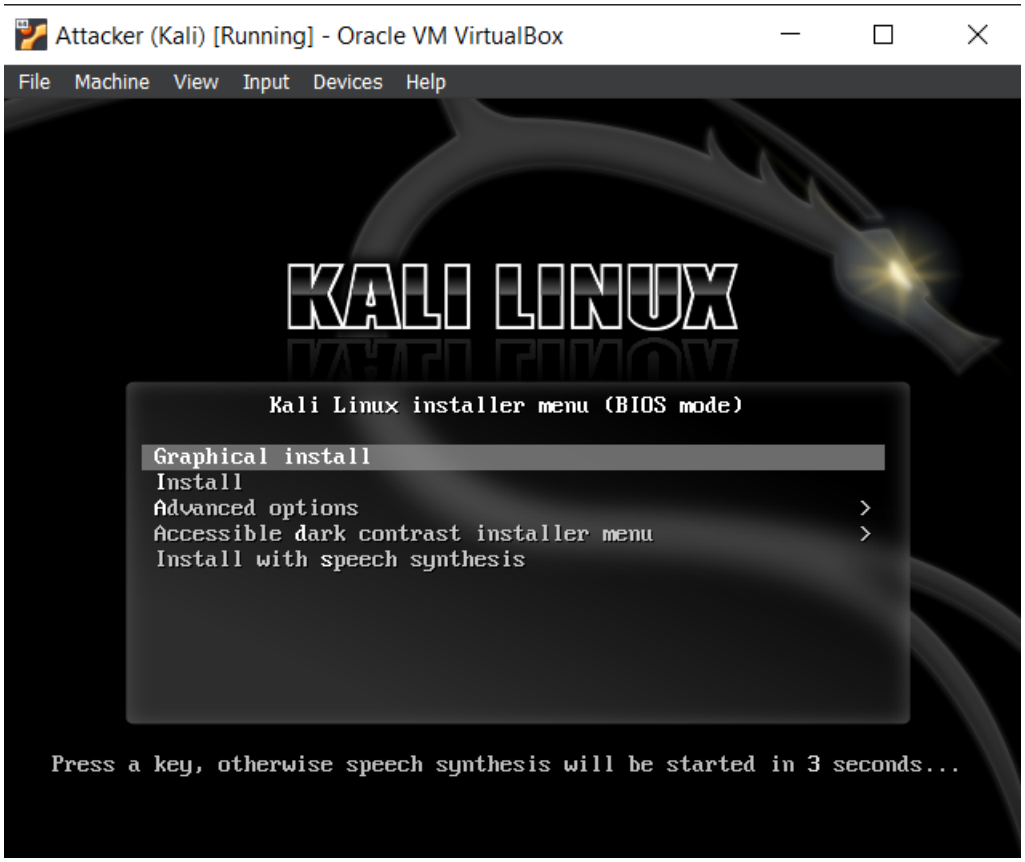


Slika 14: Dodjeljivanje količine prostora tvrdog diska

Na slici 14 vidljiv je još jedan bitan korak, a to je kreiranje virtualnog tvrdog diska koji će virtualna mašina koristiti. Potrebno je postaviti dovoljno velik virtualni disk kako bi se operativni sustav mogao ispravno instalirati, te da ima mjesta i za očekivane programe koji će se naknadno instalirati. Na slici 15. može se primijetiti kako je kreirana nova virtualna mašina i sve njene specifikacije.



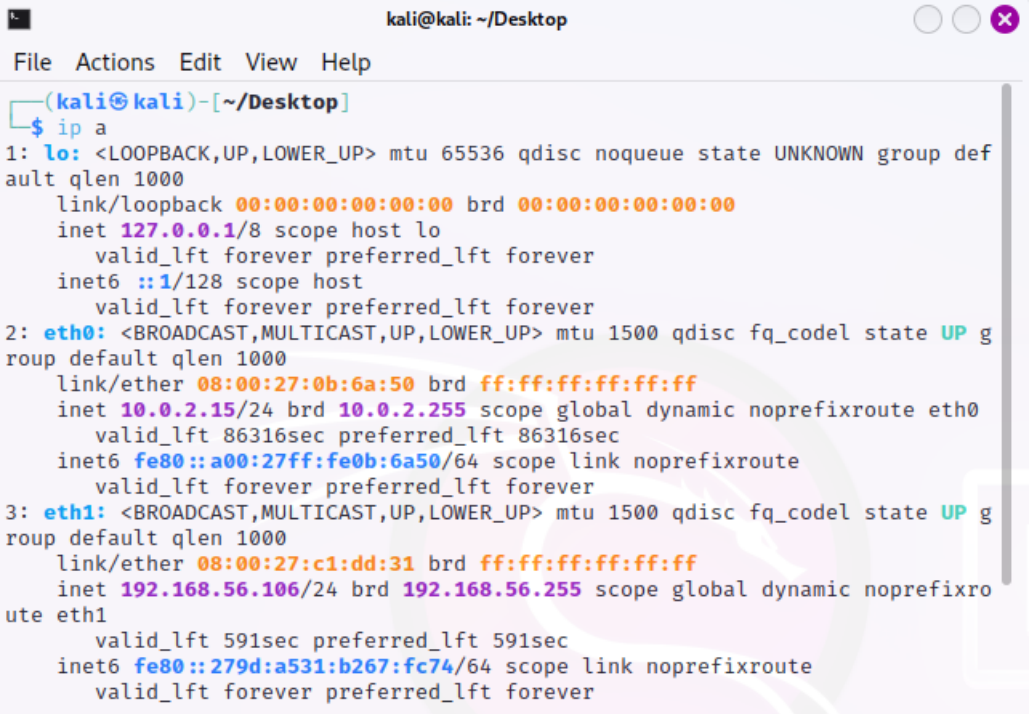
Slika 15: Pregled nove virtualne mašine



Slika 16: Instalacija Kali Linux-a

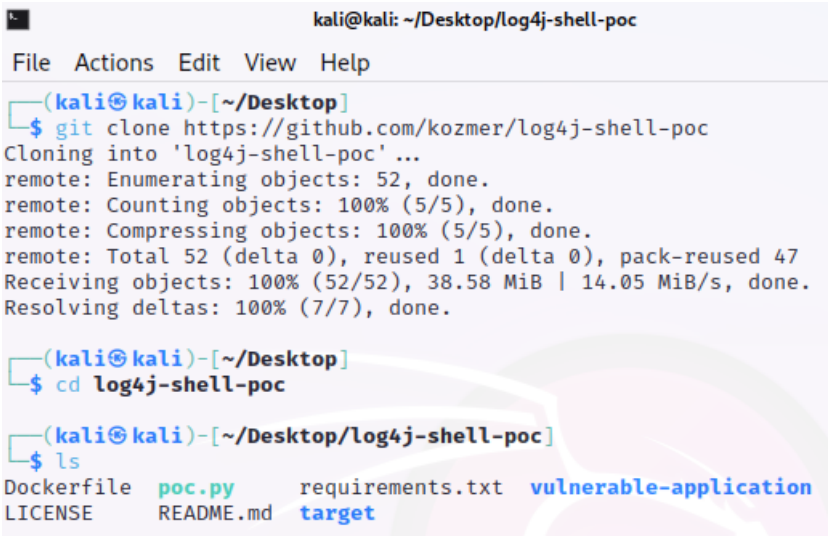
Slika 16 prikazuje prvi korak kod podizanja operativnog sustava. Nakon toga potrebno je odabrati jezik koji će operativni sustav koristiti, te je potrebno odabrati regiju, lokaciju, jezični paket i jezik tipkovnice.

Također je potrebno odabrati primarno mrežno sučelje koji će se koristiti prilikom instalacije, u ovom slučaju odabran je eth0 jer on nije u virtualnoj mreži i dozvoljava pristup internetu, a eth1 je mrežno sučelje unutar VLAN-a koje je prethodno postavljeno. Zatim se postavljaju korisničko ime i lozinka.



Slika 17: Pregled mrežnih sučelja unutar Kali Linux-a

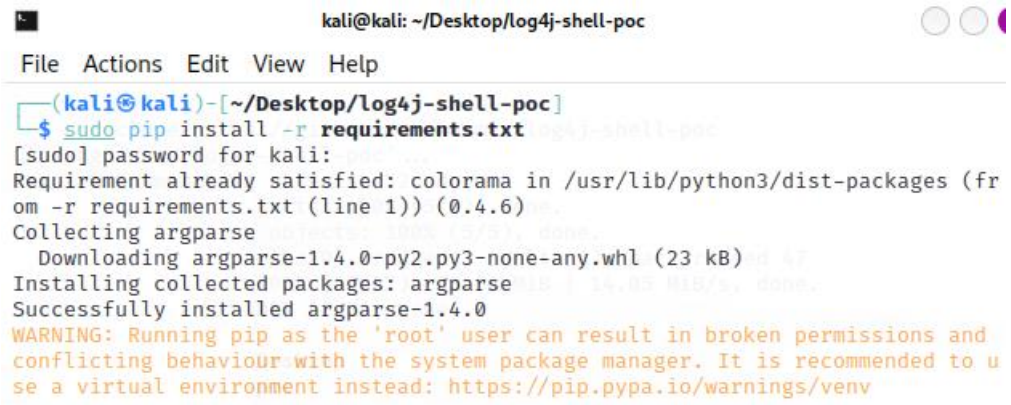
Na slici 17 može se primijetiti kako virtualna mašina ima dva mrežna sučelja, a mrežno sučelje unutar VLAN mreže lako je upečatljivo zbog dodijeljene IP adrese. Ključna riječ *UP* pokazuje da je mrežno sučelje aktivno. Sada je moguće preuzeti GitHub repozitorij koji sadrži ranjivu web aplikaciju, kao što je vidljivo na slici 18. Ime preuzetog direktorija je „log4j-shell-poc“.



Slika 18: Preuzimanje repozitorija za studiju slučaja

Nakon pozicioniranja u preuzeti direktorij, naredbom „ls“ mogu se prikazati datoteke i pod-direktoriji. Tekstualna datoteka „requirements.txt“ sadrži popis potrebnih biblioteka kako bi se ova vježba uspješno izvela, a otvaranjem te datoteke može se vidjeti da su to biblioteke

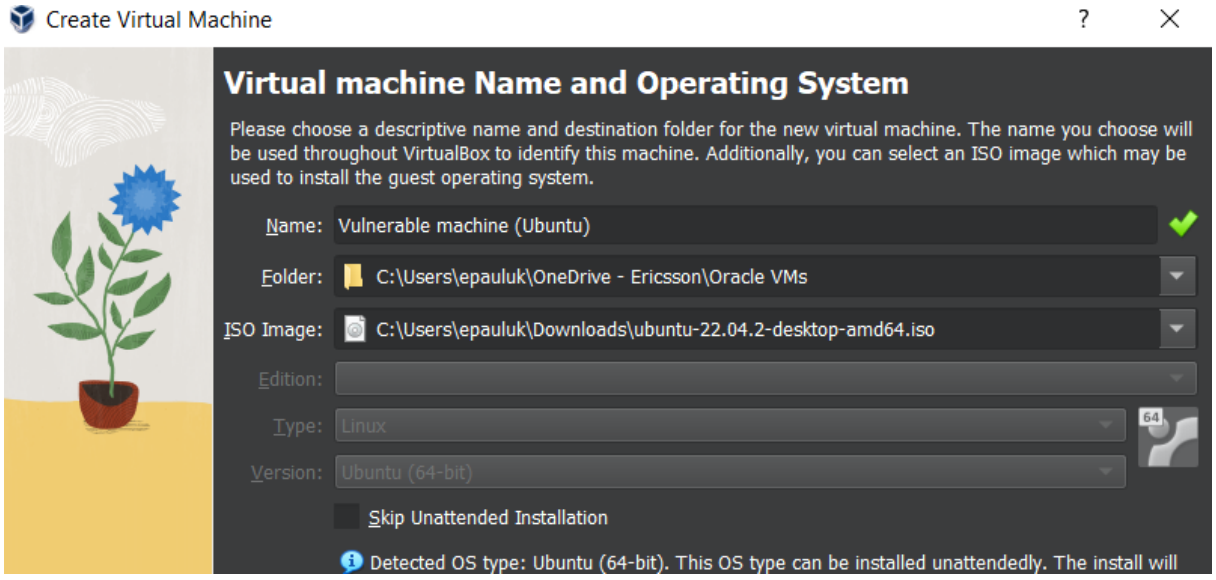
Colorama i Argparse. Colorama je biblioteka koja olakšava stvaranje i upravljanje bojama i stilovima ispisa u konzolnim aplikacijama. Argparse je biblioteka za analizu argumenata naredbenog retka. Koristi se za olakšavanje obrade i upravljanja argumentima koje korisnik unosi prilikom pokretanja Python skripte putem naredbenog retka. Ova biblioteka pojednostavljuje upotrebu i upravljanje naredbenim argumentima u Python skriptama. Stoga je potrebno instalirati spomenute biblioteke, kao što je prikazano na slici 19.



Slika 19: Instalacija biblioteka

6.2. Ranjiva virtualna mašina

Postupak postavljanja ranjive virtualne mašine puno je lakši zato što postoji mogućnost automatiziranog podizanja operativnog sustava, kao što je vidljivo na slici 20. Za ovu svrhu koristi se Ubuntu operativni sustav. Ubuntu je operativni sustav otvorenog koda, baziran je na Debianu, isto kao i Kali Linux, te je solidan izbor za operativni sustav ranjive virtualne mašine.

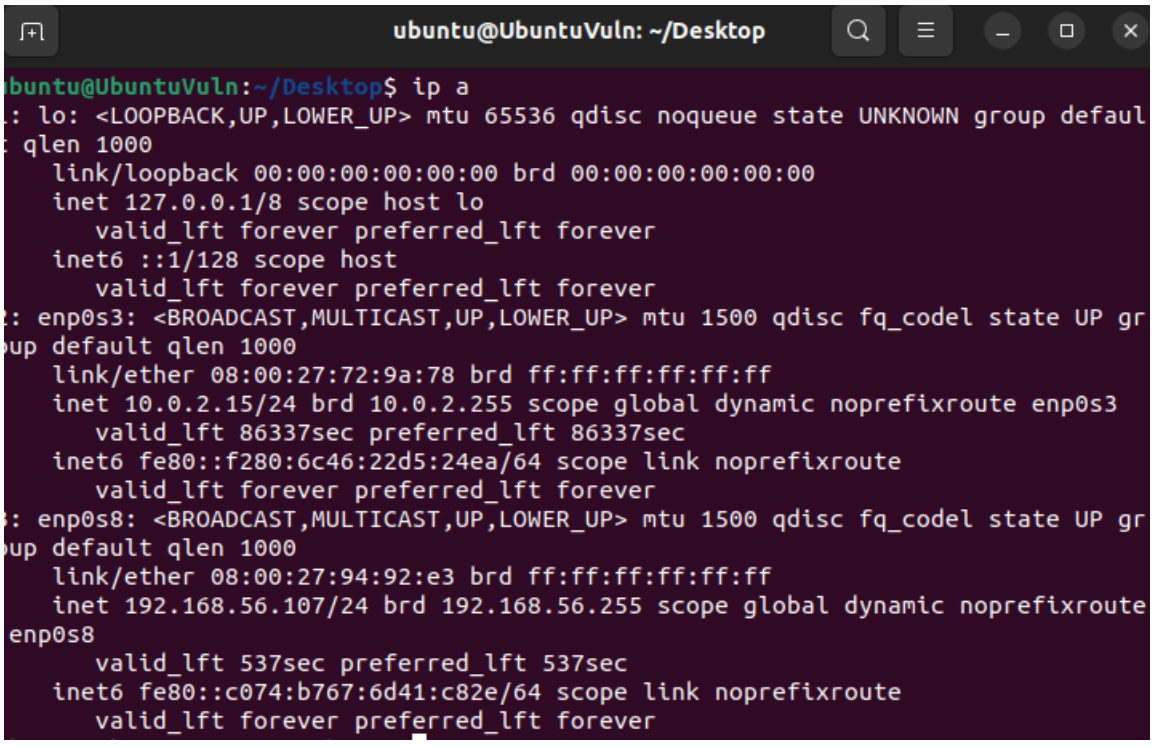


Slika 20: Imenovanje Ubuntu virtualne mašine

Zatim je potrebno dodijeliti količinu RAM memorije i procesorskih jezgri koje će virtualna mašina imati na raspolaganju, te korisničko ime i lozinku. Ostatak izrade virtualne mašine identičan je kao i kod postavljanja napadačke mašine. Kao što je već spomenuto, podizanje Ubuntu operativnog sustava je u potpunosti automatiziran proces, što znatno ubrzava cijeli proces.

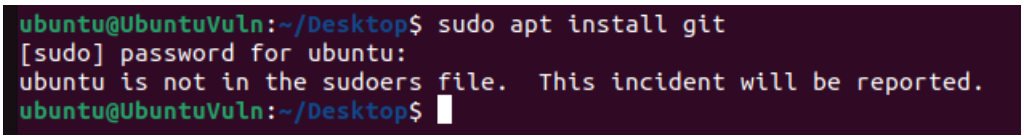
Nakon uspješnog podizanja operativnog sustava, može se primijetiti kako je operativni sustav na engleskom jeziku, ali tipkovnica je na poljskom jeziku. To je glavni nedostatak automatiziranog postavljana Ubuntu operativnog sustava, problem se rješava preuzimanjem hrvatskog jezika te postavljenjem istog kao zadanog, uključujući i tipkovnicu.

Ranjivu virtualnu mašinu također je potrebno staviti u VLAN koji je prethodno kreiran, na isti način kako je postavljena i napadačka virtualna mašina. Upisivanjem naredbe „ip a“ u terminal dobiva se pregled svih mrežnih sučelja i njima dodijeljenih IP adresa. Ako je sve postavljeno kako treba, bit će vidljiva 2 mrežna sučelja, od kojih će jedan od njih imati IP adresu u rasponu VLAN-a, kao što je vidljivo na slici 21.



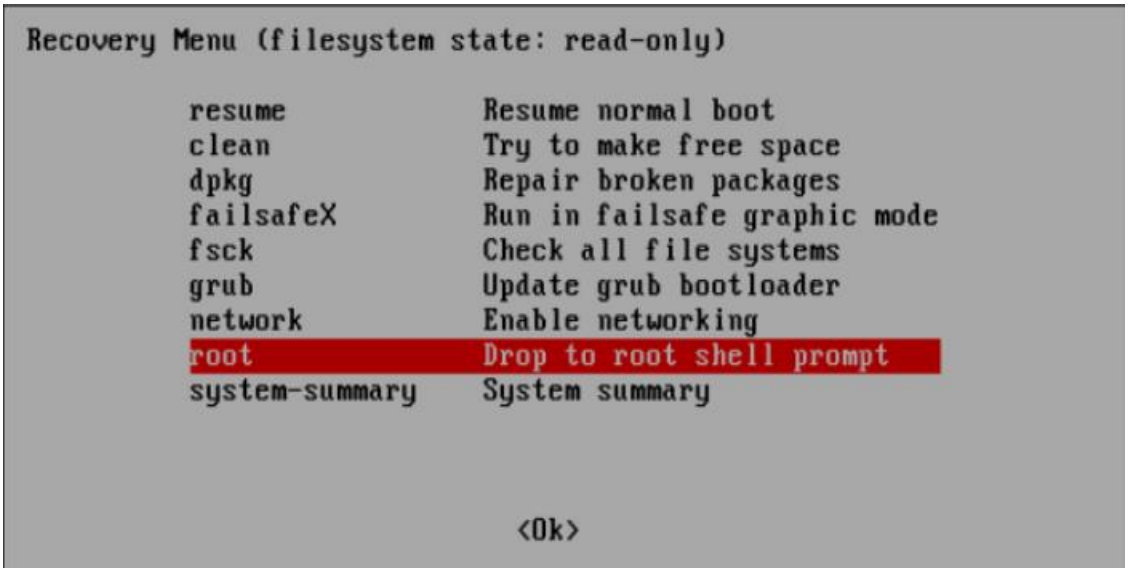
Slika 21: Mrežna sučelja Ubuntu virtualne mašine

Na slici 22 vidljivo je kako korisnik nema administratorska prava, te zbog toga nije moguće instalirati Git paket.



Slika 22: Korisnički račun nema administratorska prava

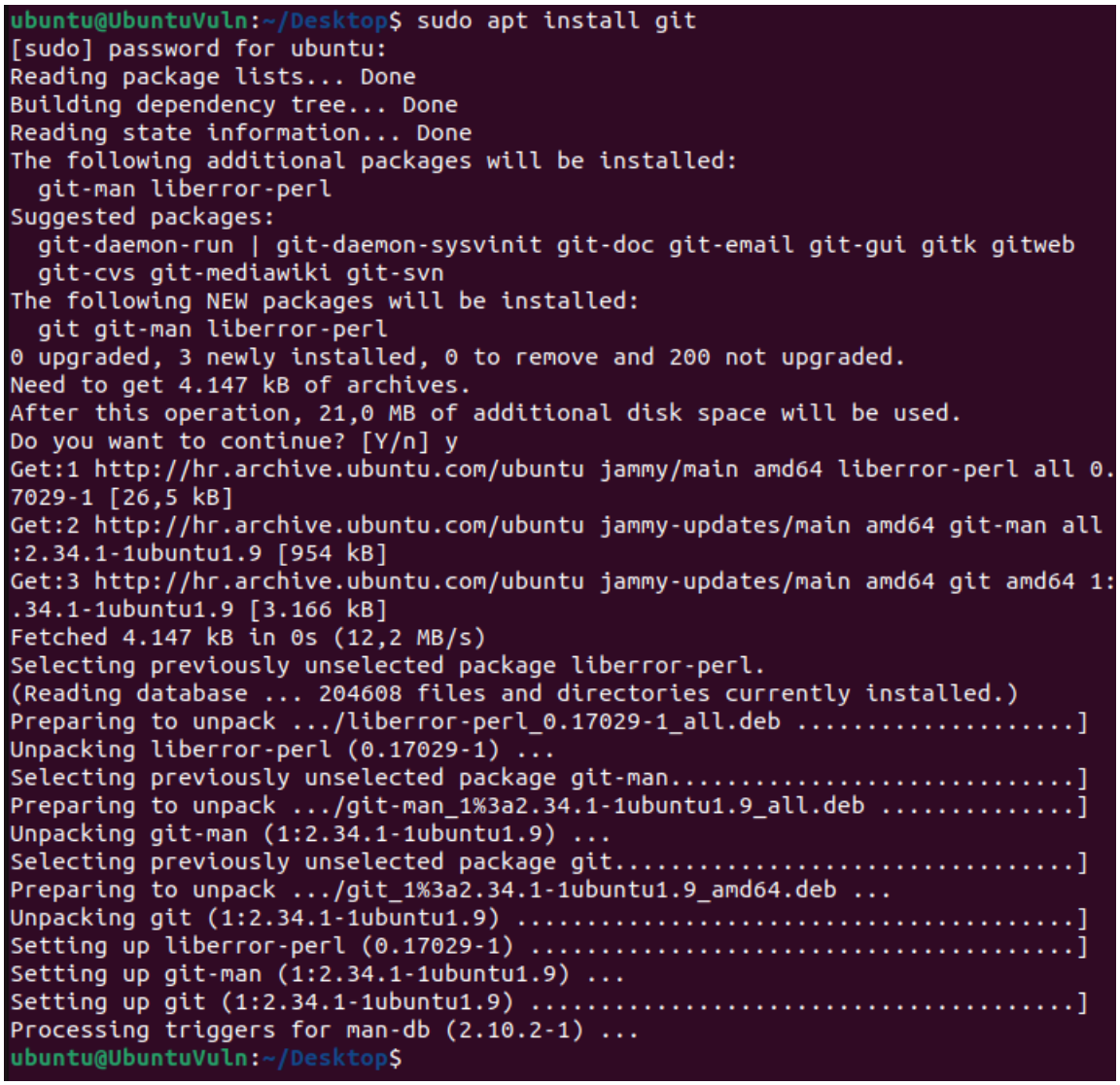
Kako bi se taj problem riješio, potrebno je korisniku dati administratorska prava, kao što je prikazano na slici 23. Administratorska prava korisniku su dodijeljena pomoću izbornika oporavka kojem se može pristupiti prilikom pokretanja virtualne mašine.



Slika 23: Izbornik oporavka

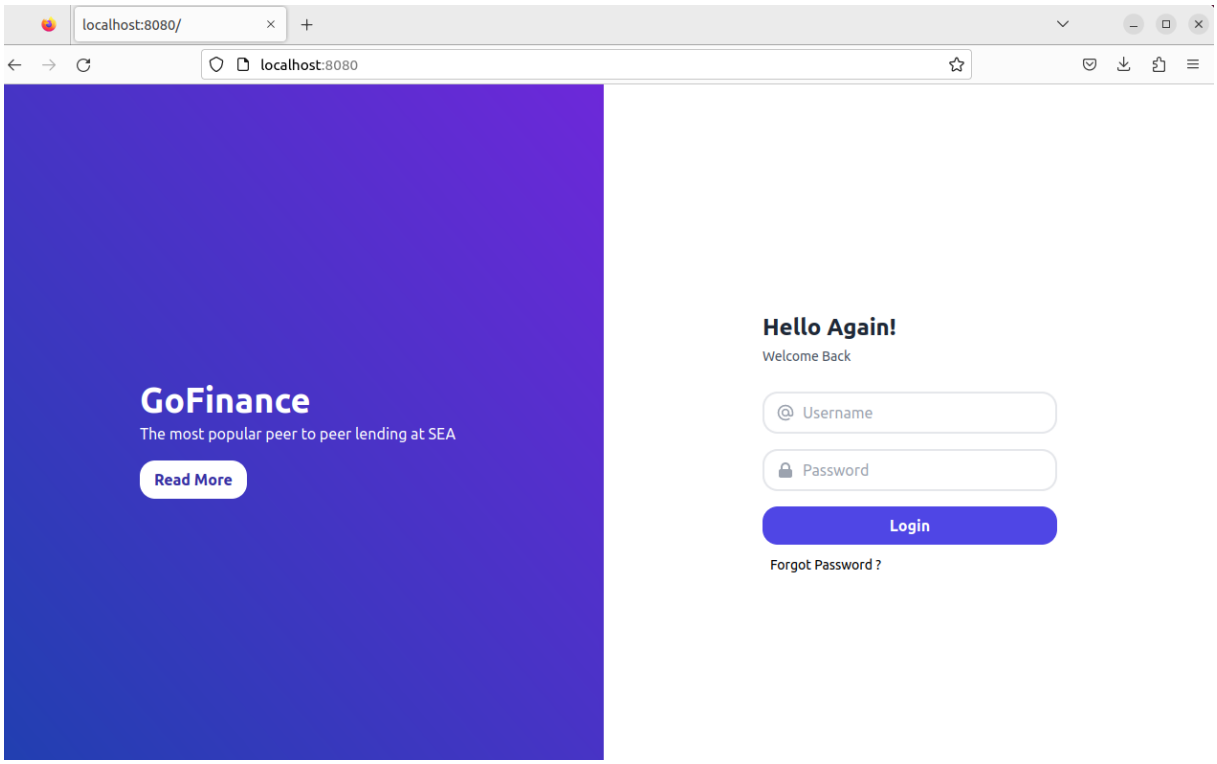
Korisnika je potrebno dodati u „sudo“ grupu i dodijeliti mu administratorska prava. Zatim je potrebno na datoteku „sudoers.d“ postaviti prava 0440, tako da korisnik može njoj pristupiti u budućnosti unutar operativnog sustava.

Za kraj je potrebno postaviti ranjivu aplikaciju, međutim Ubuntu nema unaprijed instaliran git paket, stoga ga je potrebno preuzeti prije nego što je moguće preuzeti repozitorij.



Slika 24: Instalacija git paketa

Kako bi se instalirale potrebne biblioteke potrebno je instalirati python programski jezik, a nakon toga moguće je instalirati i Docker paket. Prije nego li se može pokrenuti Docker spremnik (ranjiva aplikacija), potrebno je u preuzeti staviti Java verziju koja je ranjiva u git repozitorij, a ona se može skinuti sa službene stranice. Potrebno ju je staviti i u ranjivu mašinu i u napadačku mašinu. Za kraj potrebno je izgraditi i pokrenuti Docker ranjivu aplikaciju. Ako je sve ispravno napravljeno, moguće je provjeriti postoji li web aplikacija na localhost:8080 u Internet pregledniku. Ako postoji, treba izgledati ovako:



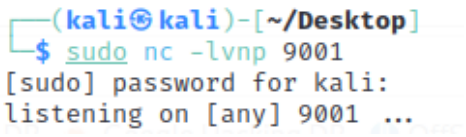
Slika 25: Ranjiva web aplikacija

6.3. Proces iskorištavanja ranjivosti

Ranjivost se bazira na mogućnosti izvršavanja udaljenog napada putem zlouporabe funkcionalnosti za obradu log zapisa. Konkretno, ranjivost se odnosi na neispravnu obradu log poruka koje sadrže određene ulazne podatke koji se mogu kontrolirati od strane zlonamjernog aktera. Iskorištavanje ove ranjivosti može omogućiti zlonamjernom akteru izvršavanje zlonamjernog koda na ranjivom sustavu koji koristi Log4j biblioteku. Zlonamjerni akter može iskoristiti ranjivost putem manipulacije log porukama koje se šalju aplikaciji koja koristi Log4j. Ova ranjivost je posebno opasna jer zlonamjerni akter može izvršiti udaljene napade bez potrebe za autentifikacijom, [27].

Najveći problem ove ranjivosti je što ju je izuzetno lagano iskoristiti u zlonamjerne svrhe. Postoji mnogo sličnih načina na koje se ova specifična ranjivost može iskoristiti, a za konkretan primjer prikazat će se samo jedan primjer.

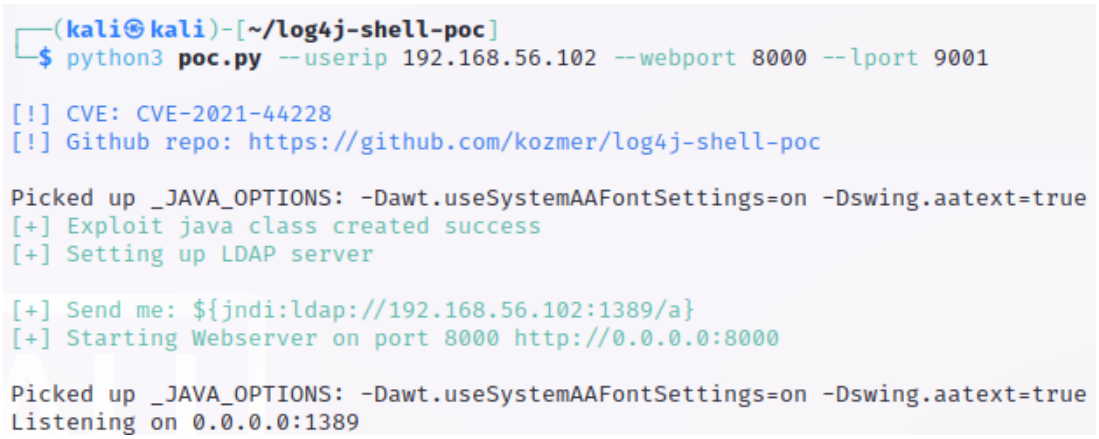
Do neovlaštenog pristupa moguće je doći u samo tri koraka. Prvi korak je pokretanje netcat alata koji sluša i čeka na određenom portu, u ovom slučaju odabran je port 9001, kao što je prikazano na slici 26:



Slika 26: Netcat alat

Ova naredba pokreće netcat s određenim opcijama i postavkama. Opcija „-l“ označava na netcat treba biti u „*listen*“ modu, tj. priprema se za primanje dolaznih veza. Opcija „-v“ omogućuje "*verbose*" način rada, što znači da će netcat ispisivati detaljnije informacije o aktivnostima. Opcija „-n“ onemogućuje rezoluciju DNS-a (engl. *Domain Name System*), čime se osigurava brže pokretanje netcat-a. Opcija „-p“ postavlja odabrani broj porta na 9001.

Nakon toga pokreće se poc.py skripta s određenim parametrima koji se očekuju za postavljanje LDAP i HTTP servera. Opcija „--webport 8000“ indicira port koji će se koristiti za pokretanje HTTP servera, a opcija „--lport 9001“ indicira port koji će se koristiti za pokretanje LDAP servera. Opcija „--userip“ određuje koja će se IP adresa koristiti.



Slika 27: Izvršavanje python skripte za postavljanje LDAP i HTTP servera

U početku, skripta uvozu različite module koji će se koristiti za svoje funkcionalnosti, kao što su „argparse“ za parsiranje argumenata s terminala, „colorama“ za obojenu uzlaznu poruku, „subprocess“ za izvršavanje sistemskih naredbi, „threading“ za korištenje više procesorskih jezgri, „pathlib“ za ras s putanjama datoteka, „os“ za funkcionalnosti vezane uz operacijski sustav, te „http.server“ za pokretanje HTTP poslužitelja.

Skripta zatim definira konstantu koja predstavlja putanju do trenutne mape u kojoj se skripta izvršava. Nakon toga slijedi funkcija „generate_payload“, koja generira Java program koji sadrži kod za iskorištavanje Log4j ranjivosti. Ovaj program se koristi za uspostavljanje veze s određenim poslužiteljem, izvršavanje naredbi na tom poslužitelju i prenošenje podataka

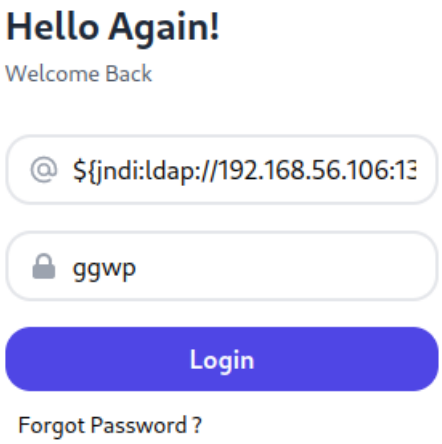
između napadača i žrtve napada. Nakon toga definira se funkcija „payload“. Ova funkcija koristi „generate_payload“ kako bi generirala Java *payload* i zatim pokreće LDAP poslužitelj na novoj jezgri. Također postavlja HTTP poslužitelj za obradu web zahtjeva.

Nakon toga, skripta definira funkciju „ldap_server“ koja generira URL za LDAP poslužitelj koristeći IP adresu korisnika i odabrani lokalni priključak. Zatim izvršava Java naredbu pomoću specifične JAR datoteke kako bi pokrenula LDAP poslužitelj. Glavna funkcija „*main*“ upravlja glavnim tijekom izvršavanja skripte. Ona pokreće sve prethodno definirane funkcije i provjerava je li Java platforma instalirana prije iskorištavanja Log4j ranjivosti. Na kraju, skripta izvršava funkciju „*main*“ kako bi iskoristila Log4j ranjivost.

Autor napominje kako ova skripta služi samo za edukacijske svrhe te da je korištenje ove ranjivosti u druge svrhe bez odgovarajućih dozvola neetično i protuzakonito.

Sve što je ostalo je izvršiti sami napad iskorištavanja ranjivosti na ranjivoj aplikaciji koja je postavljena na ranjivoj virtualnoj mašini. U ovom primjeru to se postiže pristupanju ranjivoj aplikaciji preko internetskog pretraživača kao što su Google Chrome, Mozilla Firefox i sl. Nakon što je pristupljeno toj aplikaciji, vidljiva su polja za upisivanje korisničkog imena i lozinke. Za dobivanje neovlaštenog pristupa potrebno je u polje korisničkog imena upisati određenu sintaksu, kao što je vidljivo na slici 28:

${jndi:ldap://192.168.56.106:1389/a}



Slika 28: Iskorištavanje ranjivosti web aplikacije

Ova sintaksa radi na način da pokrene JNDI pretraživanje na temelju navedene URL adrese „ldap://192.168.56.106:1389/a“, zatim se kontaktira taj zlonamjerni LDAP poslužitelj koji vraća odgovor. Taj odgovor može sadržavati Java kod. Log4j zatim izvršava taj kod, te se na taj način postiže neovlašten pristup.

Nakon toga, u terminalu gdje je pokrenut netcat, može se vidjeti kako je dobiven neovlašteni pristup svim podacima pohranjenim na tom poslužitelju, kao što je vidljivo na slici 29.

Slika 29: Neovlašteni pristup web aplikaciji

6.4. Analiza prikupljenih podataka

Nakon provođenja napada iskorištavanja ranjivosti Log4j potrebno je složiti strukturiranu dokumentaciju koja sadrži sve važne informacije o napadu, te se tako mogu odrediti prioriteti za zakrpu sigurnosnih rupa i poboljšanja. Ta analiza treba obuhvatiti sljedeće elemente:

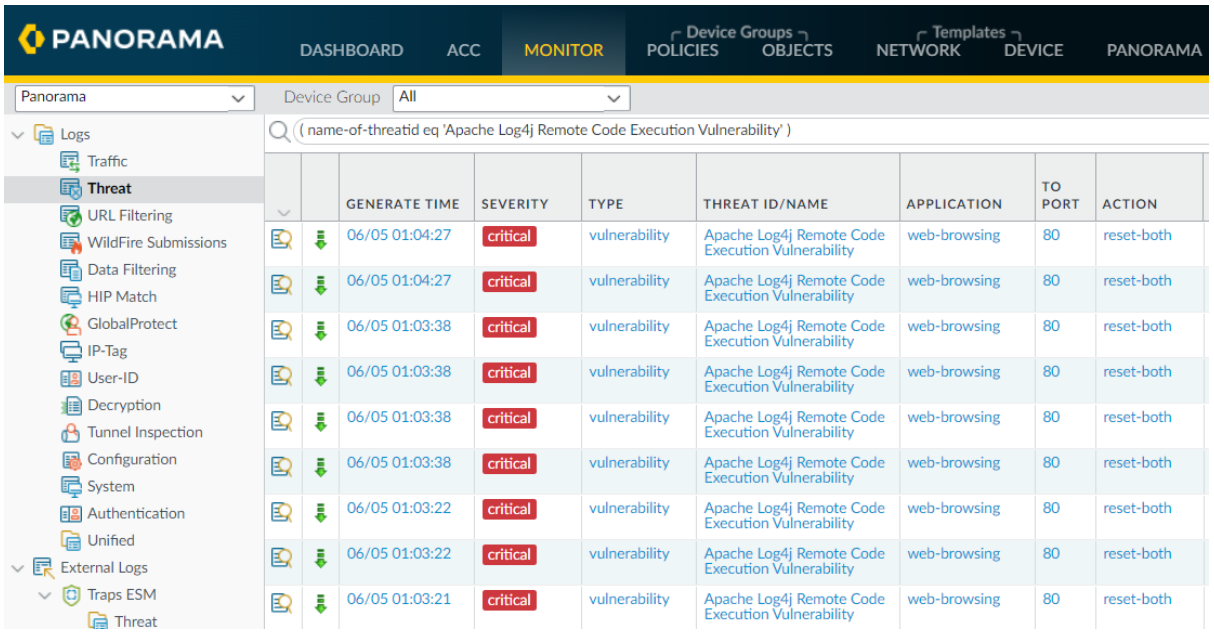
1. Identifikacija ranjivosti: identifikacija svih ranjivosti koje su otkrivene tijekom izvršavanja vježbe ljubičastog tima. Uključuje identifikaciju ranjivih točaka, sigurnosnih propusta ili slabih karika u aplikaciji ili sustavu.
2. Utjecaj ranjivosti: Analiza treba procijeniti potencijalni utjecaj svake ranjivosti na sigurnost aplikacije ili sustava. Ovo uključuje razumijevanje mogućnosti zloupotrebe ranjivosti, potencijalnog oštećenja ili gubitka podataka, prekid rada ili mogućeg utjecaja na korisnike.
3. Razlozi i uzorci ranjivosti: Potrebno je istražiti razloge postojanja ranjivosti, a to može uključivati loš dizajn, greške u kodu, neispravne konfiguracije ili propuste u sigurnosnom procesu.

4. Procjena rizika: Potrebno je procijeniti rizik koji svaka ranjivost predstavlja za organizaciju. To uključuje vrednovanje vjerojatnosti iskorištavanja ranjivosti i mogućeg utjecaja na poslovanje, povjerljivost, integritet i dostupnost sustava.
5. Naučene pouke (engl. *lessons learned*): Analiza treba sadržavati pouke naučene iz provedenih vježbi. Uključuje identifikaciju najvažnijih sigurnosnih lekcija, nedostataka u postupcima ili praksama te preporuke za poboljšanje budućih vježbi i sigurnosnih postupaka.
6. Izvješće o zaključcima: Analiza treba rezimirati sve zaključke i nalaze u obliku pisanih izvješća. To izvješće mora biti jasno i sažeto, ali istovremeno informativno i detaljno, kako bi moglo služiti kao referenca za donošenje odluka i planiranje sigurnosnih aktivnosti u budućnosti.
7. Komunikacija i suradnja: Analiza bi trebala biti temelj za komunikaciju između crvenog i plavog tima, jer bez razmjene informacija između timova ljubičasti tim ne postoji, [27].

U nastavku su podaci prikupljeni na resursima organizacije, koji predstavljaju što plavi tim vidi tijekom izvođenja napada crvenog tima u vježbi ljubičastog tima, a u ovoj studiji slučaja to su podaci prikupljeni od strane raznih alata koji se koriste u organizacijama.

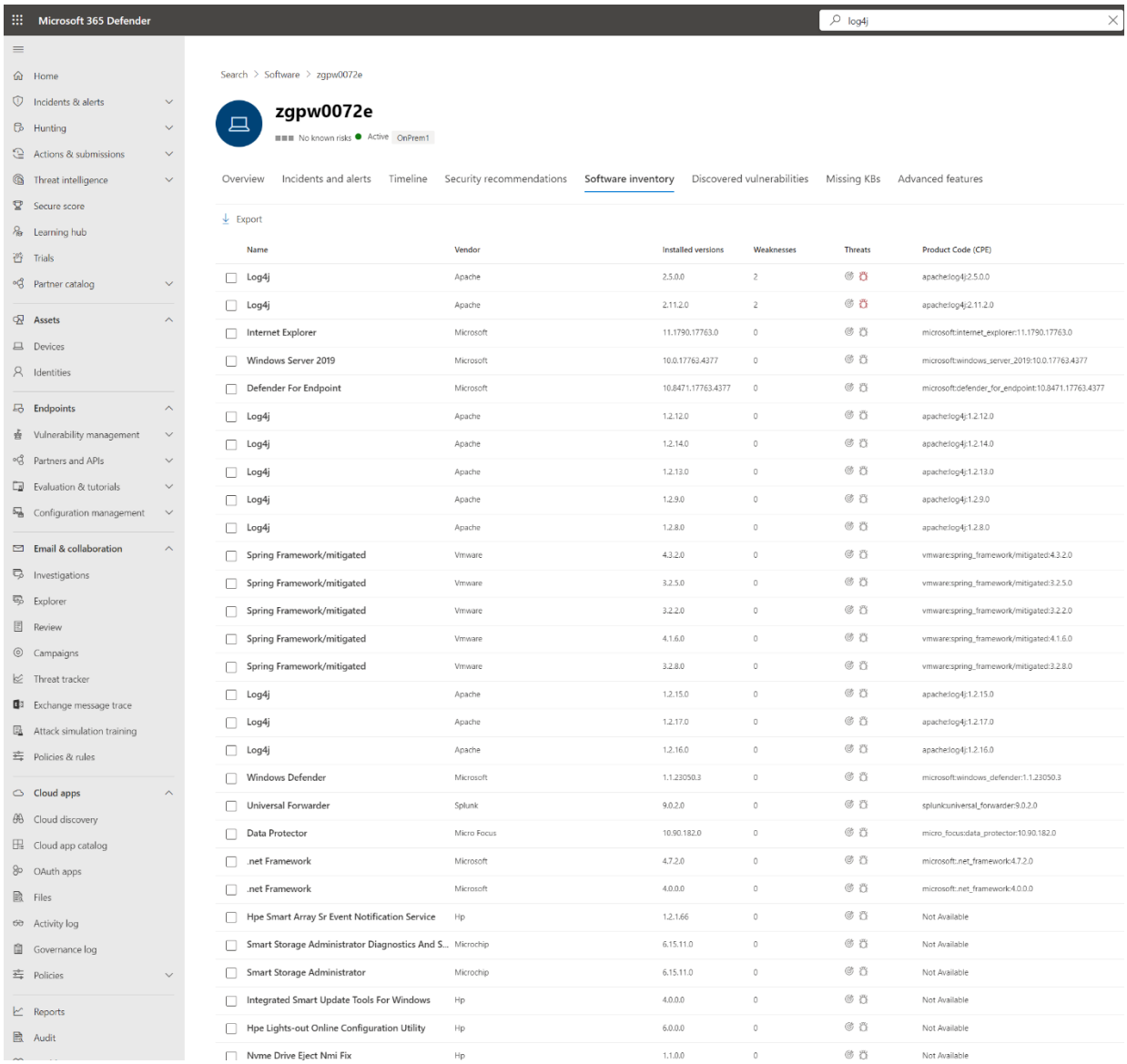
6.5. Izvještaj vatrozida

Ponavljanjem studije slučaja na resursima organizacije, dobiveni su razni izvještajni podaci. Za početak prikazati će se podaci koje su prikupili vatrozid Palo Alto Panorama i Windows 365 Defender.



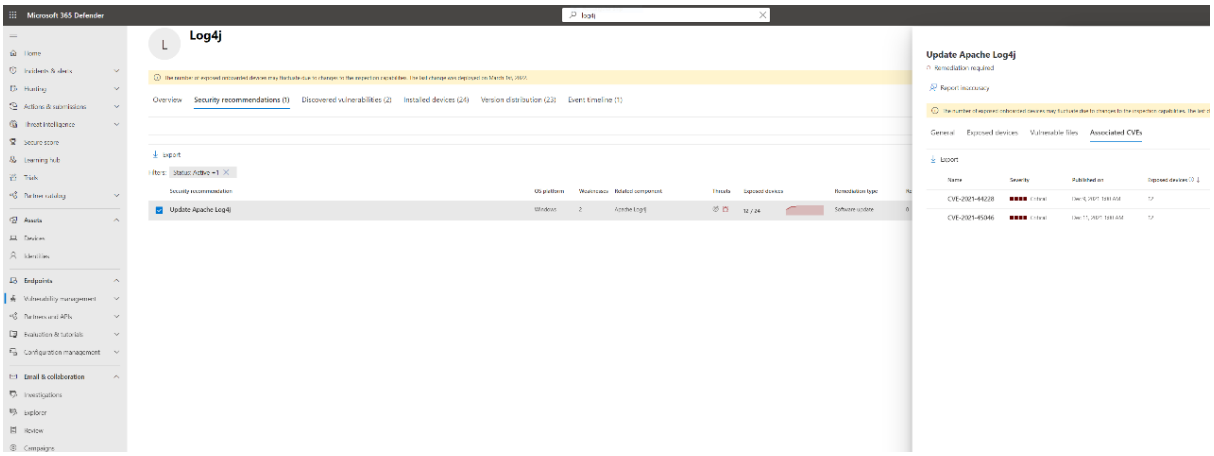
Slika 30: Palo Alto Panorama vatrozid

Palo Alto je centralizirani upravljački sustav koji omogućuje upravljanje i nadzor Palo Alto Networks sigurnosnih rješenja, uključujući vatrozide. Palto Alto Networks je poznat po naprednim vatrozidovima koji pružaju zaštitu mreže i kontrole prometa. Panorama pruža središnje mjesto za konfiguriranje, upravljanje i nadgledavanje Palo Alto vatrozida, uključujući postavljanje sigurnosnih pravila, praćenje događaja i upravljanje sigurnosnim politikama. Na slici 32 vidljivo je kako je Palo Alto vatrozid primijetio pokušaj iskorištavanja ranjivosti. Osjetljive informacije su cenzurirane, ali vidljivi su imena stupaca. Mogu se vidjeti vrsta i ime pojedine prijetnje, iz koje zone dolazi napad, u kojoj se zoni napada uređaj s navedenom ranjivosti, IP adresa izvornog uređaja i žrtve napada, ozbiljnost ranjivosti itd. Prepoznavanje napada moguće je samo zašto to u ovom slučaju promet nije kriptiran. Ako je promet kriptiran, vatrozid ne bi mogao napraviti depaketizaciju i provjeriti sadržaj paketa, te ne bi mogao prepoznati pokušaj iskorištavanja ranjivosti.



Slika 31: Microsoft 365 Defender

Microsoft 365 Defender integrirano je sigurnosno rješenje koje pruža zaštitu na različitim razinama, uključujući zaštitu na razini mreže i aplikacija. Iako Microsoft 465 Defender nije specifično vatrozid rješenje, Microsoft pruža vatrozid funkcionalnosti putem drugog proizvoda po nazivom „Microsoft Defender Firewall“, koji je ugrađen u Windows operativne sustave te pruža zaštitu na razini računala i mreže. Na slici 33. jasno je vidljivo kako je vatrozid prepoznao koje su verzije Log4j instalirane na računalo te ih je uspješno prepoznao kao ranjivosti. A na slici 34. vidi se predloženi postupak za otklanjanje ranjivosti, u ovom slučaju rješenje bi bilo ili nadogradnja Apache Log4j na noviju verziju ili korištenje drugog alata s istom funkcionalnosti koji nema tu ranjivost.

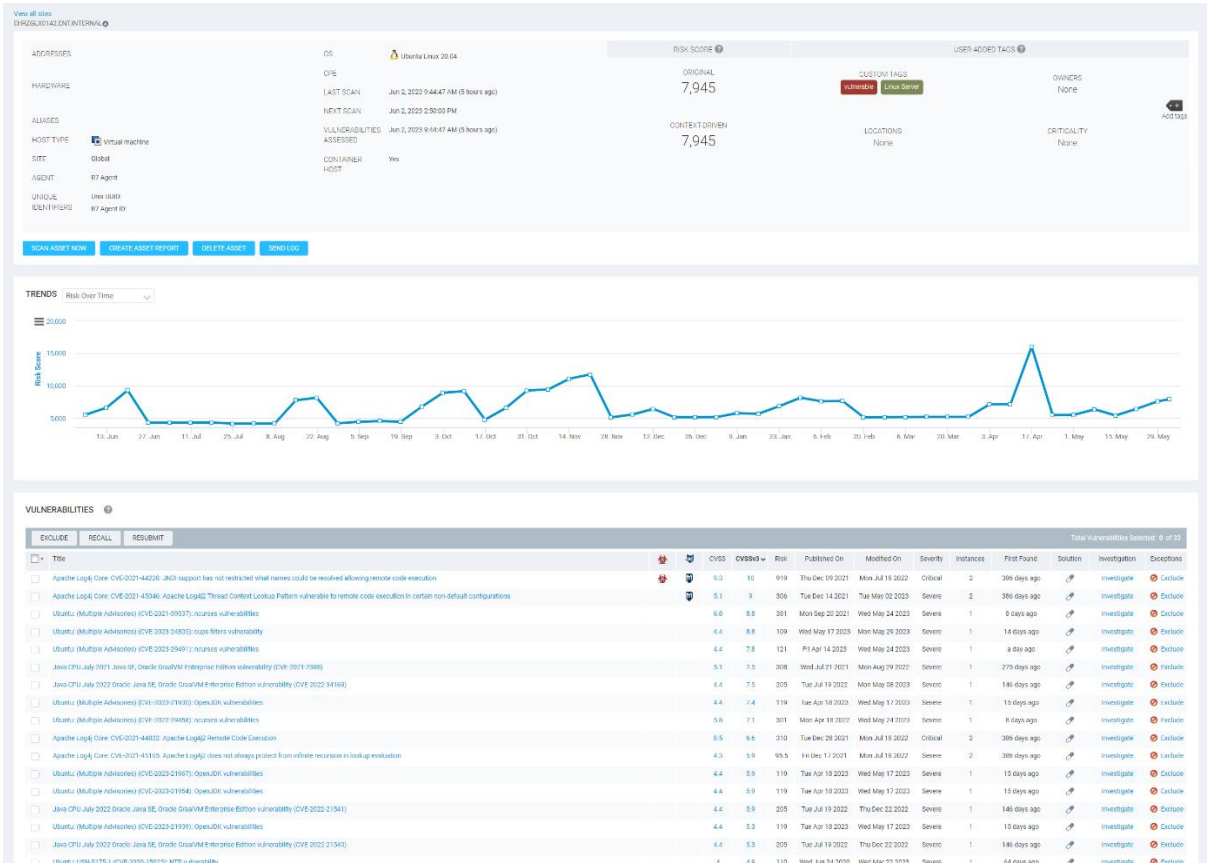


Slika 32: Predloženi koraci za otklanjanje ranjivosti unutar Microsoft 365 Defendera

6.6. Izvještaj mrežnog i lokalnog skenera

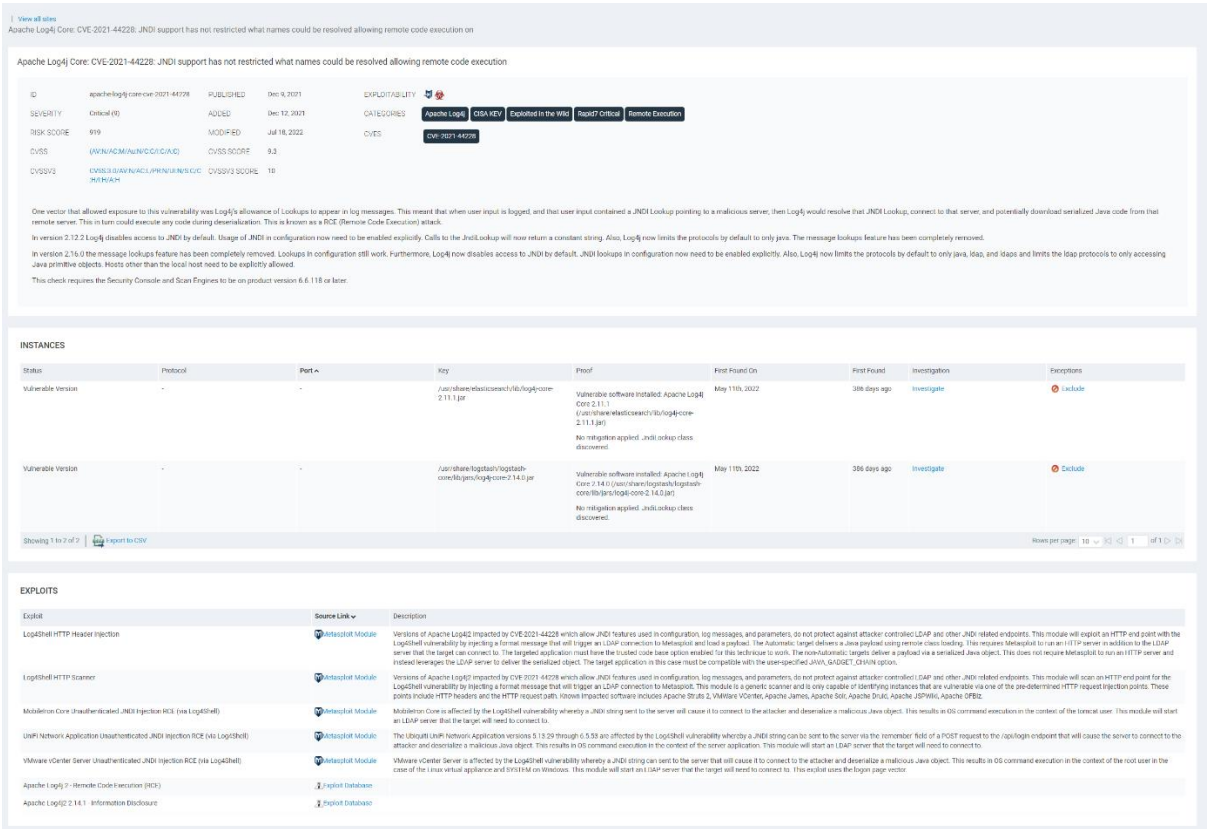
InsightVM je rješenje za upravljanje ranjivostima (engl. *Vulnerability Management Solution*) koje pruža tvrtka Rapid7. To je alat koji pruža zajedničko gledište i zajednički jezik potreban za usklađivanje tradicionalno izoliranih timova. Također potiče proaktivan pristup upravljanju ranjivostima s praćenjem i metrikom. Neke funkcije koje InsightVM nudi su *lightweight* agent krajnjih točaka, *real-time* nadzorna ploča, određivanje prioriteta rizika, integrirani agenti za simulaciju prijetnji i izvršavanje simulacije iskorištavanja ranjivosti itd.

Općenito, lokalni skener je alat koji se koristi za pronalaženje i upravljanje uređajima na mreži. Lokalni skener skenira lokalnu mrežu, tražeći spojene uređaje unutar nje, dok mrežni skener ima mogućnost skeniranja šire mreže, uključujući udaljenje mreže. Informacije koje ti skeneri mogu pružiti o pronađenim uređajima su njima dodijeljene IP adrese, *hostname* i MAC adrese, operativne sustave itd.



Slika 33: InsightVM tvrtke Rapid7

Na slici 35. vidljiv je mrežni i lokalni skener InsightVM, koji ima sposobnost provjere ranjivosti koje se mogu iskoristiti preko mreže - RCE. Osjetljive informacije su cenzurirane. Na donjoj polovici slike 35. jasno su vidljive ranjivosti koje su pronađene, na nekima postoje i ikone ispred stupca CVSS koje pokazuju kako je InsightVM uspješno replicirao iskorištavanje ranjivosti koristeći MetaSploit ili neki drugi alat. Također pokazuje ozbiljnost (engl. *severity*), broj instanci, kada je prvi put ta ranjivost publicirana itd. Graf trendova prikazuje promjenu u sigurnosnom stanju organizacijskih resursa tijekom vremena. Na vodoravnoj osi nalazi se vremenska os, a na vertikalnoj osi prikazuje se neki relevantni pokazatelj sigurnosti. Na grafu su vidljiva povećanja i smanjenja broja ranjivosti, trendovi u riziku i učinkovitost organizacije u rješavanju otkrivenih ranjivosti.



Slika 34: InsightVM detalji o Log4j ranjivosti

Na slici 36. prikazani su detalji o ranjivosti Log4j. Može se primijetiti kako je ranjivosti dodijeljen unikatan ID (engl. *Identifier*), njegova ozbiljnost, ocjena rizičnosti, te sažetak načina na koji funkcionira iskorištavanje ranjivosti. Zatim, pod sekcijom „*Instances*“ mogu se točno vidjeti koje su zahvaćene datoteke i koja verzija Apache Log4j je instalirana na mašini. Na dnu slike detaljno su opisani načini iskorištavanja te ranjivosti.

6.7. Popis komponenti softvera Dockera ranjive aplikacije

Popis komponenti softvera (engl. *Software Bill of Materials*, SBOM), je datoteka koja sadrži popis svih komponenti softvera koje su korištene unutar Docker spremnika. Za generiranje ove datoteke koristio se API (engl. *Application Programming Interface*) otvorenog koda zvan Anchore, te alati Syft i Grype. Naredba koja se koristila za dobivanje ovog popisa komponenti, vidljivih na slikama 35 i 36 je:

```
$ sudo syft packages docker:log4j-shell-poc -o json | grype
```

589	log4j-core	2.14.1	2.16.0	GHSA-7rjr-3q55-vv33	Critical
590	log4j-core	2.14.1	2.17.1	GHSA-8489-44mv-ggj8	Medium
591	log4j-core	2.14.1	2.15.0	GHSA-jfh8-c2jp-5v3q	Critical
592	log4j-core	2.14.1	2.17.0	GHSA-p6xc-xr62-6r2g	High
593	log4j-core	2.14.1		CVE-2021-44228	Critical
594	log4j-core	2.14.1		CVE-2021-44832	Medium
595	log4j-core	2.14.1		CVE-2021-45046	Critical
596	log4j-core	2.14.1		CVE-2021-45105	Medium

Slika 35: Popis komponenti softvera za Log4j

tomcat-jdbc	8.0.36	CVE-2016-0762	Medium
tomcat-jdbc	8.0.36	CVE-2016-5018	Critical
tomcat-jdbc	8.0.36	CVE-2016-5388	High
tomcat-jdbc	8.0.36	CVE-2016-5425	High
tomcat-jdbc	8.0.36	CVE-2016-6325	High
tomcat-jdbc	8.0.36	CVE-2016-6794	Medium
tomcat-jdbc	8.0.36	CVE-2016-6796	High
tomcat-jdbc	8.0.36	CVE-2016-6797	High
tomcat-jdbc	8.0.36	CVE-2016-6816	High
tomcat-jdbc	8.0.36	CVE-2016-8735	Critical
tomcat-jdbc	8.0.36	CVE-2016-8745	High
tomcat-jdbc	8.0.36	CVE-2017-12617	High
tomcat-jdbc	8.0.36	CVE-2017-5647	High
tomcat-jdbc	8.0.36	CVE-2017-5648	Critical
tomcat-jdbc	8.0.36	CVE-2017-5664	High
tomcat-jdbc	8.0.36	CVE-2017-7674	Medium
tomcat-jdbc	8.0.36	CVE-2018-1304	Medium
tomcat-jdbc	8.0.36	CVE-2018-1305	Medium
tomcat-jdbc	8.0.36	CVE-2018-1336	High
tomcat-jdbc	8.0.36	CVE-2018-8014	Critical
tomcat-jdbc	8.0.36	CVE-2018-8034	High
tomcat-jdbc	8.0.36	CVE-2020-8022	High

Slika 36: Popis komponenti softvera za tomcat

Generirana datoteka u sebi sadrži 5 stupaca: Ime paketa, instalirana verzija, u kojoj verziji je popravljena ranjivost, unikatan ID ranjivosti, te njezina ozbiljnost.

6.8. Otklanjanje ranjivosti

Log4j ranjivost može se otkloniti na nekoliko načina. Jedan način je ažuriranje ranjive aplikacije ili biblioteke na noviju verziju koja sadrži zakrpu te specifične ranjivosti. Potrebno je provjeriti koji sve sustavi i aplikacije koriste tu biblioteku i jesu li one osjetljive na tu ranjivost. Ako jesu, potrebno ih je ažurirati na noviju verziju. Zatim, moguće je isključiti JNDI (engl. Java Naming and Directory Interface) *lookup* u Log4j konfiguraciji, kako bi se smanjio rizik od ranjivosti. Također je moguće korištenje vatrozida i sustava za detekciju/upade (IDS i IPS) kako bi se ograničio pristup prema Log4j serverima i blokirao potencijalno zlonamjerne upite koji pokušavaju iskoristiti ranjivost. Na kraju, može se poboljšati nadzor mrežnog prometa kako bi se otkrile sumnjive aktivnosti. Nadzor i analiza mrežnog prometa može pomoći u otkrivanju pokušaja iskorištavanja ranjivosti, [27].

7. Zaključak

Analiza tehnika i alata ljubičastog tima u svrhu unaprjeđenja sigurnosti u organizacijama pokazuje značajnu vrijednost i potencijal ovog suradničkog pristupa u borbi protiv kibernetičkih prijetnji. Ljubičasti tim, koji se sastoji od crvenog i plavog, tj. ofenzivnog i defenzivnog tima, kombinira taktike i tehnike oba tima kako bi identificirao ranjivosti i slabosti u sustavima organizacije. Kroz emulaciju zlonamjernih aktera, ljubičasti tim kreira realistične scenarije napada i testira obranu resursa organizacije. Korištenje metodologije emulacije zlonamjernih aktera omogućuje ljubičastom timu da stekne bolje razumijevanje tehnika i taktika koje zlonamjerni akteri koriste te pronalazak ranjivosti koje bi se uobičajeno mogle previdjeti. Kroz primjenu prilagođenog PDCA procesa, tj. PEIR modela, ljubičasti tim usmjerava se na kontinuirano poboljšanje sigurnosnih mjera i sposobnosti odgovora na sigurnosne incidente. Ovaj ciklus osigurava da se organizacija brzo prilagođava promjenjivom krajoliku sigurnosti. Evaluacija učinkovitosti ljubičastog tima moguća je kroz razne metrike kao što su prosječno vrijeme otkrivanja, prosječno vrijeme reakcije, prosječno vrijeme oporavka, prosječno vrijeme za suzbijanje, dostupnost sustava itd.

Korištenjem alata poput vatrozida, mrežnog i lokalnog skenera, te raznih platformi za upravljanjem sigurnosti resursa organizacije, omogućuje se cjelovit uvid u sigurnosno stanje organizacijskih resursa, omogućuje se aktivno skeniranje, nadzor u oblaku itd. Takvi alati pomažu ljubičastom timu u identificiranju ranjivosti, smanjenju rizika od potencijalnih napada te osigurava organizacijama adekvatan odgovor na sigurnosne incidente. Tijekom izvršavanja vježba ljubičastog tima, izuzetno je bitno dokumentirati cijeli proces i napraviti analizu prikupljenih podataka. Ta analiza treba obuhvatiti sljedeće elemente: identifikacija ranjivosti, utjecaj ranjivosti, razlozi i uzorci ranjivosti, procjena rizika, naučene pouke, izvješće o zaključcima, komunikacija i suradnja. Provođenjem studije slučaja prikazano je kako izvršiti jednu jednostavnu vježbu ljubičastog tima, gdje je izvršen proces iskorištavanja ranjivosti te analiza prikupljenih podataka, a dodatno je i prikazan rad raznih alata koji se koriste za zaštitu od kibernetičkih napada. Analiza tehnika i alata ljubičastog tima ukazuje na njihovu važnost u unaprjeđenju sigurnosti organizacija, a strategije koje koristi ljubičasti tim postaje ključni element u borbi protiv sve sofisticiranijih napada i osigurava održivu digitalnu sigurnost organizacija.

Literatura

[1] D. Peraković, I. Cvitić: Separati sa predavanja iz kolegija Sigurnost i zaštita informacijsko komunikacijskog sustava, Fakultet prometnih znanosti, Zagreb, 2020

[2] Nacionalni CERT. Godišnji izvještaj rada nacionalnog CERT-a za 2021. godinu, Preuzeto sa: https://www.cert.hr/wp-content/uploads/2022/03/CERT-godisnje-izvjesce-2021.pdf [Pristupljeno: travanj 2023.]

[3] Nacionalni CERT. Godišnji izvještaj rada nacionalnog CERT-a za 2022. godinu, preuzeto sa: https://www.cert.hr/wp-content/uploads/2023/02/CERT-G.I.-2022..pdf [Pristupljeno: travanj 2023.]

[4] Hickey M., Arcuri J. Hands on Hacking, 2020.

[5] Routin D., Thoores S., Rossier S. Purple Team Strategies, 2022.

[6] Iansresearch. Strategies for Building an Effective Purple Team. Preuzeto sa: https://www.iansresearch.com/resources/all-blogs/post/security-blog/2022/04/26/strategies-for-building-an-effective-purple-team [Pristupljeno: svibanj 2023.]

[7] Coursera. What Is the Purpose of the Purple Team? Preuzeto sa: https://www.coursera.org/articles/purple-team [Pristupljeno: svibanj 2023.]

[8] PlexTrac. What is Adversary Emulation? Preuzeto sa: https://plextrac.com/what-is-adversary-emulation-adversary-simulation/ [Pristupljeno: svibanj 2023.]

[9] Picussecurity. Purple Team Automation with Breach and Attack Simulation. Preuzeto sa: https://www.picussecurity.com/purple-team-automation-with-breach-and-attack-simulation-bas [Pristupljeno: svibanj 2023.]

[10] Danielmiessler. The Difference Between Red, Blue, and Purple Teams. Preuzeto sa: https://danielmiessler.com/study/red-blue-purple-teams/ [Pristupljeno: svibanj 2023.]

[11] Oakley, J.G., Professional Red Teaming, 2019.

[12] Sehgal K., Thymianis N., Cybersecurity Blue Team Strategies 2023.

[13] SecurityScorecard. 7 Incident Response Metrics and How to Use Them. Preuzeto sa: https://securityscorecard.com/blog/how-to-use-incident-response-metrics/ [Pristupljeno: svibanj 2023.]

[14] Techtarget. Understanding purple teaming benefits and challenges. Preuzeto sa: https://www.techtarget.com/searchsecurity/feature/Understanding-purple-teaming-benefits-and-challenges [Pristupljeno: svibanj 2023.]

[15] Nettitude. Purple teaming. Preuzeto sa: https://www.nettitude.com/uk/penetration-testing/purple-

teaming/#:~:text=By%20creating%20a%20scenario%20where%20the%20Red%20Team,is%20much%20more%20closely%20aligned%20with%20real-world%20threats. [Pristupljeno: svibanj 2023.]
[16] Cybexer. What is a Live Fire Exercise and How is it Conducted?. Preuzeto sa: https://cybexer.com/resource-center/what-is-a-live-fire-exercise-and-how-is-it-conducted/ [Pristupljeno: svibanj 2023.]
[17] Crowdstrike. What is a threat model?. Preuzeto sa: https://www.crowdstrike.com/cybersecurity-101/threat-modeling/ [Pristupljeno: svibanj 2023.]
[18] Owasp. Threat modeling process. Preuzeto sa: https://owasp.org/www-community/Threat_Modeling_Process [Pristupljeno: svibanj 2023.]
[19] Redlegg. Tabletop exercise: pretty much everything you need to know. Preuzeto sa: https://www.redlegg.com/solutions/advisory-services/tabletop-exercise-pretty-much-everything-you-need-to-know [Pristupljeno: svibanj 2023.]
[20] CM-Alliance. Cyber Crisis Tabletop Exercises. Preuzeto sa: https://www.cm-alliance.com/cyber-crisis-tabletop-exercise [Pristupljeno: svibanj 2023.]
[21] Explore Atomic Red Team. Preuzeto sa: https://atomicredteam.io/ [Pristupljeno: svibanj 2023.]
[22] Caldera. Preuzeto sa: https://caldera.mitre.org/ [Pristupljeno: svibanj 2023.]
[23] VECTR. Preuzeto sa: https://docs.vectr.io/ [Pristupljeno: svibanj 2023.]
[24] Picus security. Preuzeto sa: https://www.picussecurity.com/ [Pristupljeno: svibanj 2023.]
[25] ResearchGate. Integrating Cyber-D&D into Adversary Modeling for Active Cyber Defense. Preuzeto sa: https://www.researchgate.net/publication/305365880_Integrating_Cyber-DD_into_Adversary_Modeling_for_Active_Cyber_Defense [Pristupljeno: svibanj 2023.]
[26] Microsoft. What is a Virtual Machine. Preuzeto sa: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-virtual-machine/ [Pristupljeno: lipanj 2023.]
[27] CISA. Apache Log4j Vulnerability Guidance. Preuzeto sa: https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance [Pristupljeno: lipanj 2023.]

Popis kratica

API	Application Programming Interface
ART	Atomic Red Team
BAS	Breach Attack Simulation
CERT	Computer Emergency Response Team
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial of Services
DNS	Domain Name System
EDR	Endpoint Detection and Response
GDPR	General Data Protection Regulation
ID	Identifier
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
ISO	Identical Storage Image
JNDI	Java Naming and Directory Interface
LAN	Local Area Network
MTBF	Mean Time Between Failures
MTTA	Mean Time To Acknowledge
MTTC	Mean Time To Contain
MTTD	Mean Time To Detect
MTTR	Mean Time To Recovery
NIST/SANS	National Institute of Standards and Technolog/SysAdmin, Audit, Network and Security
PCI DSS	Payment Card Industry Data Security Standard
PDCA	Plan-Do-Check-Act
PEIR	Prepare-Execute-Identify-Remediate
RAM	Random Access Memory
RCE	Remote Code Execution
ROI	Return on Investment

SBOM	Software Bill of Materials
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SOC	Security Operations Center
SOP	Standard Operating Procedures
TTP	Tactics, Techniques, and Procedures
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VM	Virtual Machine

Popis slika

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom Analiza tehnika i alata ljubičastog tima u svrhu unaprjeđenja sigurnosti u organizacijama, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

U Zagrebu, 05.06.2023

Student/ica:

Luka Pavić

(ime i prezime, *potpis*)