DNEVNIK STRUČNE PRAKSE

Student: Jure Marinov
Mentor: Tea Kljajić
Poduzeće: OTP banka d.d.
Status dnevnika: Završen

Varaždin, 13.04.2026.

1. dan
10.03.2025.

Danas sam započeo praksu u OTP banci u Zadru, u odjelu za informacijsku sigurnost. Prvi dan bio je uvodni, a mentor mi je predstavio osnovne alate i sustave koji se koriste u svakodnevnom radu. Osnovna odgovornost ovog odjela je nadzor i zaštita IT sustava banke, detekcija prijetnji, provođenje sigurnosnih politika te osiguravanje usklađenosti s regulatornim zahtjevima. Tijekom dana dobio sam uvid u način rada tima, ključne procese i postupke koji se primjenjuju u slučaju sigurnosnih incidenata. Glavni alat za nadzor sigurnosnih događaja je IBM QRadar, koji služi kao SIEM (Security Information and Event Management) sustav. QRadar omogućuje prikupljanje, analizu i korelaciju sigurnosnih logova iz različitih izvora, što pomaže u detekciji potencijalnih incidenata i proaktivnoj zaštiti sustava. Osim njega, još je uvijek u upotrebi i McAfee SIEM, koji se i dalje koristi za određene zadatke, posebice za analizu povijesnih podataka i prepoznavanje obrazaca potencijalnih prijetnji. Ovi alati omogućuju brzu reakciju na sumnjive aktivnosti, što je ključno za sigurnost bankarskog sustava. Osim SIEM sustava, banka koristi i druge sigurnosne alate. FortiGate je napredni mrežni vatrozid koji omogućuje kontrolu prometa, inspekciju paketa i zaštitu od vanjskih prijetnji, uključujući DDoS napade, malware i neovlaštene pokušaje pristupa. Za upravljanje krajnjim uređajima zaposlenika koristi se VMware Workspace ONE UEM (ranije poznat kao AirWatch), koji omogućuje centralizirano upravljanje, implementaciju sigurnosnih politika i zaštitu osjetljivih podataka na mobilnim i desktop uređajima. Pored toga, koristi se i ObserveIT, softver koji omogućuje detaljan nadzor korisničkih aktivnosti na računalima, s posebnim fokusom na prevenciju insajderskih prijetnji i analizu sumnjivog ponašanja korisnika. Endpoint zaštita osigurana je putem Symantec rješenja, koje pruža zaštitu od virusa, ransomwarea i drugih vrsta zlonamjernog softvera. Za nadzor performansi i stabilnosti IT sustava koristi se Nagios, alat koji omogućuje praćenje mrežnih uređaja, poslužitelja i aplikacija u realnom vremenu te upozorava na potencijalne probleme prije nego što postanu kritični. Osim pregleda alata, razgovarali smo i o općim sigurnosnim politikama banke te važnosti pravilnog upravljanja incidentima. Poseban naglasak stavljen je na pravovremenu detekciju i prijavu sigurnosnih prijetnji, analizu uzroka incidenata te implementaciju sigurnosnih mjera kako bi se spriječilo njihovo ponavljanje. Također, istaknuta je važnost edukacije zaposlenika o sigurnosnim praksama i podizanju svijesti o potencijalnim prijetnjama, budući da ljudski faktor često predstavlja najslabiju kariku u sigurnosnom lancu. Prvi dan bio je vrlo informativan i omogućio mi je da steknem osnovni uvid u rad sigurnosnog tima. U narednim danima očekujem dublje upoznavanje s alatima kroz praktičan rad, analizu stvarnih sigurnosnih događaja i sudjelovanje u procesu rješavanja incidenata.

Screenshotovi nisu mogući.

2. dan
11.03.2025.

Drugi dan prakse bio je usmjeren na dublje upoznavanje s IBM QRadar SIEM sustavom. Mentor mi je detaljnije objasnio način na koji QRadar prikuplja i obrađuje logove te kako se konfiguriraju različiti izvori podataka. Učili smo o Log Source Identifier parametrima, koji su ključni za ispravno prepoznavanje logova unutar sustava. Tijekom dana smo riješili jedan manji problem gdje log source identifier nije bio pravilno imenovan, zbog čega ga QRadar nije ispravno prepoznavao i uključivao u logove. Nakon istrage problema, promijenili smo naziv u ispravan oblik, čime je problem riješen i logovi su počeli pristizati kako treba. Kasnije smo zaprimili alert, koji je bio generiran zbog instalacije WhatsApp.exe na poslovni laptop. Takva instalacija krši interne sigurnosne politike banke jer poslovni uređaji ne smiju imati neodobreni softver. Pregledali smo detalje alerta i analizirali kako je QRadar prepoznao ovaj incident, odnosno koje su pravila i uvjeti doveli do generiranja obavijesti. Ovaj slučaj bio je dobar primjer kako QRadar pravila i korelacijski mehanizmi rade u praksi te kako se sigurnosni tim treba nositi s potencijalnim prijetnjama ili nepravilnostima u sustavu. Napokon je danas stigao i moj službeni laptop, što mi je omogućilo da samostalno isprobam QRadar i istražim njegove funkcionalnosti. Također, dobio sam službeni korisnički račun, čime sam stekao pristup QRadaru. Zanimljivo je da svi ostali koriste laptop kao terminal za spajanje na virtualnu mašinu, s koje zatim rade unutar sigurnosnog okruženja. Moj način rada je drugačiji – nisam spojen na virtualnu mašinu, već direktno s laptopa pristupam QRadaru.

3. dan
12.03.2025.

Treći dan prakse započeo je pregledavanjem logova i offenses unutar IBM QRadar sustava. Kroz analizu sam bolje razumio način na koji QRadar detektira potencijalne sigurnosne incidente te kako ih kategorizira prema razini prijetnje. Offenses predstavljaju grupirane sigurnosne događaje koji upućuju na moguću prijetnju te su ključni za pravovremenu reakciju i istraživanje incidenata. Svaka offense analiza uključuje provjeru povezanih logova, korisničkih aktivnosti i mrežnog prometa, kako bi se utvrdilo radi li se o stvarnoj prijetnji ili lažnom pozitivnom upozorenju. Nakon toga, radio sam na identificiranju svih IP adresa povezanih s jednim korisničkim imenom. Cilj je bio pronaći sve povezane IP adrese kako bismo mogli isključiti nepotrebna obavještavanja vezana uz njih i smanjiti broj lažnih alarma. Pretragu sam obavio unutar QRadar konzole, analizirajući povijesne logove i filtrirajući ih prema korisničkom imenu. Ovaj zadatak mi je pomogao da bolje razumijem način na koji QRadar obrađuje logove i kako pravilno koristiti query-je za filtriranje podataka. Sljedeći zadatak bio je pronaći sve podatke vezane za IP adresu x.x.x.x. Međutim, unatoč detaljnoj pretrazi, nisam pronašao nikakve konkretne informacije povezane s njom. Nakon konzultacije s mentorom, zaključili smo da QRadar, na temelju određenog parent pravila, randomizira IP adrese unutar tog raspona, što je dovelo do toga da se tražena IP adresa ne pojavljuje u logovima na očekivani način. Ovo mi je pružilo uvid u to kako QRadar obrađuje IP adrese unutar određenih pravila i kako ih može modificirati prije nego što se prikažu u logovima. Na kraju dana, prilagodio sam pravilo unutar QRadara koje se odnosi na blokiranje određenih URL stranica. Ova promjena omogućila je preciznije filtriranje nepoželjnih web stranica, čime se dodatno poboljšala sigurnosna politika pristupa internetu unutar banke. Također, prilagodba pravila smanjila je broj nepotrebnih upozorenja (tzv. šuma), čime je omogućena bolja fokusiranost na stvarne sigurnosne prijetnje.

4. dan
13.03.2025.

Danas smo radili na kreiranju novog pravila unutar IBM QRadar sustava koje će slati e-mail alert svaki put kada dođe do promjene bilo kojeg sigurnosnog pravila. Cilj ovog pravila je osigurati praćenje svih izmjena u sigurnosnim postavkama te omogućiti pravovremenu reakciju na neovlaštene ili nenamjerne promjene. Konfiguracija je uključivala definiranje uvjeta za detekciju promjena, kao i postavljanje automatizirane notifikacije sigurnosnom timu, čime se osigurava bolja kontrola nad sigurnosnim politikama sustava. Zatim sam dobio zadatak analizirati sve evente vezane uz nekoliko specifičnih korisničkih imena i pronaći poveznice među njima. Pregledao sam logove i uspješno identificirao većinu podataka koji su ukazivali na moguće obrasce povezanosti između korisnika. Međutim, primijetio sam da određeni eventi dolaze na McAfee SIEM, ali se ne prikazuju unutar QRadar-a. Zajedno s mentorom pokušao sam istražiti uzrok problema, no unatoč detaljnoj analizi i testiranju različitih mogućnosti, do kraja radnog dana nismo uspjeli pronaći konačno rješenje. Dugo smo razmatrali potencijalne uzroke, uključujući probleme u konfiguraciji log forwardinga i postavke unutar SIEM-a, ali problem je ostao neriješen, te ćemo nastaviti istragu idući dan. Na kraju dana, za potrebe sigurnosnog izvještavanja, napravili smo quick search unutar QRadar-a kako bismo dobili popis svih zaključanih korisničkih računa. Ova pretraga omogućila nam je brz i točan pregled svih trenutno blokiranih korisnika, što je bilo ključno za pripremu izvještaja sigurnosnom timu i daljnju analizu. Na temelju dobivenih podataka, osigurali smo pravovremenu identifikaciju korisnika kojima je potreban dodatni nadzor ili resetiranje pristupa, čime smo poboljšali efikasnost sigurnosnog procesa.

5. dan
14.03.2025.

Na početku dana, poslao sam e-mail voditelju tima s obavijesti da od idućeg tjedna prelazim u Split, budući da moj mentor u Zadru odlazi na edukaciju. Peti dan prakse bio je fokusiran na rješavanje problema s kašnjenjem logova i njihovim izostankom unutar QRadar-a. Nakon što prethodnog dana nismo uspjeli pronaći konačno rješenje, danas smo nastavili istraživanje i kroz detaljnu analizu zajedno s kolegom iz drugog odjela došli do odgovora. Problem je bio u tome što su određeni logovi dolazili na McAfee SIEM, ali nisu bili vidljivi unutar QRadar-a, a istovremeno je kašnjenje logova bilo neprihvatljivo veliko – preko 30 minuta. Nakon više pokušaja, zaključili smo da problem leži u načinu na koji su agenti za prikupljanje logova bili konfigurirani putem GP. Naime, logovi su bili slani kroz posredne postavke, što je uzrokovalo gubitke i dodatna kašnjenja u obradi. Kako bismo potvrdili pretpostavku, u suradnji s kolegom iz drugog odjela odlučili smo na najmanje korištenom serveru ukloniti GP postavke i ručno instalirati Agenta. Nakon što smo to implementirali i testirali, primijetili smo da logovi s tog servera dolaze u realnom vremenu i bez gubitaka. Ova promjena pokazala se kao ispravan smjer, pa smo postupno implementirali isto rješenje i na kritičnijim serverima. Nakon primjene ovog rješenja, logovi su konačno počeli pravilno pristizati u QRadar, a kašnjenje je svedeno ispod jedne minute, što je sada u skladu s regulatornim zahtjevima. Ovaj proces mi je omogućio bolje razumijevanje kako funkcionira prikupljanje logova, kao i važnost ispravne konfiguracije agenta i optimizacije sustava kako bi se spriječili gubici podataka. Osim toga, isprobavali smo opciju Generative AI za Pulse dashboard unutar QRadar-a. Cilj je bio testirati kako AI analizira podatke i može li otkriti dodatne sigurnosne prijetnje. Međutim, kroz testiranje smo ustanovili da nije dao nikakve nove informacije koje već nismo znali standardnim metodama. Iako tehnologija može biti korisna za buduće analize, u ovom trenutku nije pokazala značajnu dodatnu vrijednost u našem radu. Kasnije tijekom dana, pregledao sam logove povezane s upozorenjima na SQL injection napade. Analizirajući događaje, mentor i ja smo zaključili da su svi pokušaji napada uspješno blokirani, a detaljnijom inspekcijom logova došli smo do zaključka da se najvjerojatnije radi o automatiziranom skeniranju ranjivosti od strane botova, kroz tehniku Host Port Scan. Takvi pokušaji su česti, ali zahvaljujući postojećim sigurnosnim mjerama nisu predstavljali stvarnu prijetnju.

6. dan
17.03.2025.

Danas sam proveo dan u Splitu s voditeljem tima, koji me upoznao s ključnim sigurnosnim sustavima koje banka koristi za zaštitu e-mail komunikacije i fizičke medije za prijenos podataka. Fokus je bio na Symantec Mail Security Gateway sustavu koji se koristi za filtriranje i propuštanje e-mailova te na kontroli USB uređaja, kako bi se spriječila neovlaštena upotreba vanjskih medija. Symantec Mail Gateway je alat koji omogućava detaljno skeniranje svih e-mailova koji ulaze i izlaze iz sustava banke. Glavna svrha ovog alata je zaštita zaposlenika i sustava od malicioznih napada putem e-maila, kao i prevencija curenja podataka. Prvo mi je objašnjeno kako funkcionira mehanizam filtriranja e-mailova. Svaka dolazna i odlazna e-mail poruka prolazi kroz višestruke slojeve analize, uključujući: Antivirusnu analizu koja provjerava privitke i sadržaj na poznate malware prijetnje, antispam filtere koji prepoznaju neželjene e-mailove i premještaju ih u karantenu, DLP (Data Loss Prevention) pravila koja sprječavaju neovlašteno slanje osjetljivih podataka van sustava banke, analizu reputacije pošiljatelja – ako je domena ili IP adresa s koje dolazi e-mail označena kao sumnjiva, e-mail se automatski odbacuje ili šalje na dodatnu provjeru. Voditelj mi je pokazao administratorsko sučelje Symantec Mail Gatewaya, gdje se može ručno intervenirati u slučaju da neki e-mail bude pogrešno blokiran. U ovim situacijama, security tim može provjeriti e-mail u karanteni, analizirati sadržaj i odlučiti hoće li ga propustiti ili trajno odbaciti. Zanimljivo mi je bilo vidjeti kako sustav prepoznaje phishing e-mailove. Npr., ako zaposlenik dobije e-mail u kojem se tvrdi da je od nadređenog ili iz IT odjela, Symantec može prepoznati neslaganje u adresi pošiljatelja i označiti ga kao sumnjiv. Ako e-mail sadrži poveznicu na lažnu stranicu za prijavu, Symantec je može blokirati prije nego korisnik uopće klikne na nju. Također, vidjeli smo kako banka koristi whitelist i blacklist pravila. Npr., postoji lista provjerenih partnera i klijenata čiji se e-mailovi automatski propuštaju, dok se e-mailovi s određenih domena, kao što su besplatne e-mail usluge (gmail.com, yahoo.com, itd.), dodatno provjeravaju prije nego što ih sustav propusti do primatelja. Drugi dio dana bio je posvećen politici sigurnosti USB uređaja. Voditelj mi je objasnio kako je u banci sustavno blokiran pristup USB portovima, osim za uređaje koji su prethodno autorizirani. Cilj ove sigurnosne mjere je spriječiti curenje povjerljivih podataka i onemogućiti unos malicioznog softvera putem vanjskih medija. Svaki pokušaj umetanja USB uređaja u računalo unutar banke se bilježi i prijavljuje sigurnosnom sustavu. Ako korisnik pokuša koristiti USB koji nije odobren, sustav ga automatski blokira, a incident se može pratiti u logovima.

7. dan
18.03.2025.

Danas sam se prvi put upoznao s Qualys platformom, alatom koji se koristi za skeniranje ranjivosti i praćenje sigurnosnog stanja IT sustava unutar banke. Mentor mi je objasnio osnovne koncepte Qualysa i kako se koristi u svakodnevnom radu. Također mi je dao dva jednostavna zadatka kako bih se upoznao s osnovnim funkcionalnostima sustava i načinom na koji se analiziraju ranjivosti. Prvi zadatak bio je istražiti Qualys Cloud Platform sučelje i glavne module. Fokus je bio na Vulnerability Management (VM), koji služi za otkrivanje i kategorizaciju ranjivosti na IT resursima, Asset Management, gdje se nalazi popis svih uređaja uključenih u skeniranja, te Reports, gdje se generiraju izvještaji o pronađenim ranjivostima i njihovoj ozbiljnosti. Na početnom dashboardu vidio sam sažeti prikaz sigurnosnog stanja, s naglaskom na trenutno otkrivene ranjivosti, koje su bile podijeljene prema ozbiljnosti (Critical, High, Medium, Low). Ova podjela pomaže timu da prioritizira rješavanje problema i usmjeri resurse na najvažnije sigurnosne propuste. Moj prvi konkretan zadatak bio je istražiti različite dijelove sučelja, upoznati se s pretragom uređaja i naučiti kako se pregledavaju ranjivosti za određeni IP ili hostname. Kroz ovaj zadatak shvatio sam kako Qualys omogućava brzo pretraživanje IT imovine i identificiranje uređaja koji su podložni sigurnosnim prijetnjama. Mentor mi je pokazao kako Qualys automatski ažurira bazu poznatih ranjivosti i kako nove sigurnosne prijetnje postaju vidljive unutar sustava. Drugi zadatak bio je analiza rezultata jednog od prethodno provedenih skeniranja. U sekciji Scans otvorio sam detaljan Scan Report, gdje sam mogao vidjeti popis pronađenih ranjivosti, njihovu CVSS ocjenu i preporučene mjere za sanaciju. Mentor mi je objasnio kako Qualys procjenjuje ozbiljnost ranjivosti, uzimajući u obzir više faktora, uključujući postojanje javnih exploita, složenost iskorištavanja i potencijalni utjecaj na sustav. Vidio sam i kako se ranjivosti označavaju kao False Positive ako su prethodno provjerene i ocijenjene kao nevažeće, što smanjuje nepotrebne alarme i omogućava fokusiranje na stvarne prijetnje. Kroz ovaj zadatak stekao sam bolji uvid u način rada Qualysa i kako se banka koristi ovim alatom za kontinuirano praćenje sigurnosti svojih sustava.

8. dan
20.03.2025.

Danas smo na praksi nastavili s nizom operativnih zadataka u sklopu redovitog održavanja sigurnosnih sustava banke. Jedan od prvih zadataka bio je dodavanje dodatnih krajnjih uređaja, konkretno USB uređaja, u sustav nadzora. Cilj je bio omogućiti praćenje svih pokušaja korištenja vanjskih medija na poslovnim računalima, budući da neautorizirani USB uređaji predstavljaju potencijalni sigurnosni rizik, osobito u kontekstu insajderskih prijetnji i mogućnosti curenja podataka. Paralelno s tim, bavili smo se i analizom prometa elektroničke pošte, gdje smo ručno propuštali određene e-mailove koje je sustav greškom označio kao prijetnju. Takvi slučajevi zahtijevaju dodatnu pažnju jer postoji fina granica između lažnog pozitivnog rezultata i stvarne prijetnje – zbog čega smo prije svakog propuštanja temeljito pregledavali zaglavlja, privitke i tijelo poruke. Također mi je danas pokazan alat Symantec Content Analysis, koji služi za analizu privitaka i sadržaja unutar mrežnog prometa. Radi se o sigurnosnoj komponenti koja koristi statičke i dinamičke metode kako bi otkrila zlonamjerni softver, analizirajući sve ulazne datoteke prije nego što dođu do korisnika. U radu s Content Analysis sustavom posebno su mi bili zanimljivi mehanizmi integracije s drugim alatima poput proxy sustava, jer omogućuju automatsku detekciju i blokiranje sumnjivog sadržaja u stvarnom vremenu. Uz pomoć sandbox tehnologije alat može pokretati sumnjive datoteke u izoliranom okruženju kako bi se otkrilo ponašanje koje ukazuje na malware – npr. pokušaje pisanja u registar, mrežnu komunikaciju prema sumnjivim domenama ili slične aktivnosti. Mentor mi je pojasnio razliku između lokalne i cloud verzije sustava, kao i način na koji se Content Analysis koristi za donošenje odluka unutar email i web prometa. Danas smo ga koristili u kontekstu praćenja sumnjivih privitaka unutar nekoliko e-mail poruka koje su bile blokirane radi heurističke detekcije, no ispostavilo se da su lažno pozitivne.

9. dan
19.03.2025.

Danas sam zajedno s mentorom proveo testiranje ranjivosti unutar interne mreže (Internal Scan) te smo generirali izvještaj u kojem je evidentirano ukupno 270 ranjivosti, od kojih se većina odnosi na Information Gathering, što znači da ne predstavljaju izravnu prijetnju, ali mogu poslužiti kao osnova za daljnje napade. Među ozbiljnijim ranjivostima izdvojili smo 22 ranjivosti razine 2 te 4 ranjivosti razine 3. Neke od ključnih ranjivosti uključuju SMB Signing Not Required Vulnerability, što znači da SMB protokol ne zahtijeva digitalno potpisivanje poruka, čime je omogućeno presretanje i manipulacija podacima u MITM napadima, zatim HTTP Security Header Not Detected, što ukazuje na nedostatak ključnih sigurnosnih zaglavlja poput X-Frame-Options, X-Content-Type-Options i Strict-Transport-Security, čime aplikacija postaje podložna napadima poput Clickjackinga, MIME sniffinga i drugih prijetnji povezanih s neadekvatnim HTTP zaglavljima. Također smo uočili SSL Certificate - Self-Signed Certificate, što znači da je korišten certifikat koji nije izdan od pouzdanog autoriteta, što kompromitira sigurnost jer korisnici ne mogu biti sigurni u autentičnost poslužitelja, kao i SSL Certificate - Invalid Maximum Validity Date Detected, što može uzrokovati sigurnosne i kompatibilne probleme s modernim preglednicima i klijentima koji odbacuju certifikate s nepravilnim datumima isteka. Osim internog skeniranja, proveli smo i testiranje ranjivosti web aplikacije, pri čemu su identificirane sljedeće ranjivosti: CWE-451: User Interface (UI) Misrepresentation of Critical Information (Clickjacking), koja se pojavljuje zbog nedostatka X-Frame-Options zaglavlja, što omogućava napadačima umetanje aplikacije unutar iframe elemenata na zlonamjernim stranicama, pri čemu korisnik može nenamjerno izvršiti radnje koje omogućuju napadačima krađu podataka ili izvođenje neautoriziranih akcija u korisničkom kontekstu. Također smo otkrili CWE-319: Cleartext Transmission of Sensitive Information, što znači da web aplikacija ne preusmjerava HTTP promet na HTTPS, čime omogućava MITM napade jer se osjetljivi podaci šalju u nešifriranom obliku, što je ozbiljan sigurnosni propust. Nadalje, identificirana je ranjivost CWE-200: Exposure of Sensitive Information to an Unauthorized Actor, gdje su verzije softvera na poslužitelju javno vidljive u HTTP odgovorima ili kroz druge tehničke informacije dostupne napadačima, čime se omogućava iskorištavanje poznatih ranjivosti specifičnih verzija softvera. U izvještaju smo evidentirali 24 ranjivosti kategorije Information Gathering, 1 ranjivost na razini 2, te 2 ranjivosti na razini 3.

10. dan
21.03.2025.

Danas smo se na praksi bavili temom DMZ-a (Demilitarized Zone), jednim od ključnih koncepata u mrežnoj sigurnosti. Tijekom dana mentor mi je objasnio osnovnu svrhu i strukturu DMZ-a, a i sam sam dodatno istraživao ovu temu kako bih bolje razumio njezinu ulogu u zaštiti informatičkih sustava. DMZ je posebna mrežna zona koja se koristi za smještaj javno dostupnih servisa, poput web poslužitelja, mail servera ili DNS servisa, koji moraju biti dostupni iz vanjskog (npr. internetskog) svijeta. Osnovna ideja iza DMZ-a je odvajanje tih javnih servisa od unutarnje mreže, kako bi se spriječilo da eventualni kompromis javno dostupnog servisa omogući napadaču direktan pristup osjetljivim resursima unutar interne mreže. Drugim riječima, DMZ djeluje kao sigurnosni tampon između vanjskog internetskog prometa i unutarnjih sustava banke. U praksi, DMZ se obično implementira pomoću dvaju ili više vatrozida – jedan filtrira promet između interneta i DMZ-a, a drugi između DMZ-a i unutarnje mreže. Tako se postiže granularna kontrola nad time tko može pristupiti čemu i iz kojeg smjera. Danas smo gledali konkretne primjere servisa koji su smješteni unutar bankinog DMZ-a, poput web aplikacija koje komuniciraju s korisnicima, a pri tome su strogo izolirane od ostatka interne infrastrukture. Također sam naučio da se sav promet prema i iz DMZ-a strogo nadzire i logira, te da se koriste različite sigurnosne politike kako bi se smanjio rizik od neovlaštenih pristupa ili lateralnog kretanja unutar mreže.

11. dan
24.03.2025.

Tijekom današnje prakse bila su zakazana dva važna sastanka koji su praktički oblikovali cijeli dan. Prvi je bio interni, u okviru odjela za informacijsku sigurnost, gdje smo raspravljali o izazovima u vezi s upravljanjem privilegiranim pristupima i mogućnostima kako dodatno pojačati nadzor nad osjetljivim dijelovima sustava. Ekipa je podijelila konkretna iskustva iz prakse, uključujući situacije gdje su postojale rupe u kontroli pristupa, a spomenuti su i pojedini alati koji više ne zadovoljavaju moderne sigurnosne zahtjeve. U tom kontekstu je i drugi sastanak dobio na težini – održan je s tvrtkom Infigo, koja je prezentirala svoje rješenje za upravljanje privilegiranim pristupima: Wallix PAM. Prodajna prezentacija bila je temeljita i vrlo tehnički usmjerena, s ciljem demonstriranja kako Wallix rješava probleme koji nas muče – od nevidljivih lozinki do detaljnog nadzora nad administratorskim aktivnostima. Wallix PAM omogućuje centralizirano upravljanje privilegiranim računima, bez da korisnik ikad ima direktan pristup lozinkama – umjesto toga, pristup ide kroz proxy koji snima cijelu sesiju i bilježi svaku akciju. To omogućuje potpunu sljedivost, mogućnost revizije i brzo reagiranje ako se nešto krene odvijati sumnjivo. Ono što je posebno korisno je mogućnost definiranja detaljnih pravila pristupa – tko može pristupiti kojem sustavu, kada, preko kojeg uređaja i u kojem kontekstu. Uz to, sustav podržava integraciju s Active Directoryjem i drugim autentikacijskim servisima, te se može skalirati prema potrebama organizacije. Prikazali su i uživo kako administrator ulazi u sustav preko Wallixa, kako se sesija snima i kako se u slučaju nepravilnosti može odmah prekinuti.

12. dan
25.03.2025.

Danas smo, u sklopu edukacije i praktičnog rada pod mentorstvom, radili na zadatku iz područja informacijske sigurnosti koji je bio podijeljen u dva međusobno povezana dijela. Prvi cilj bio je pronaći administratorsku lozinku kroz mrežno istraživanje, dok se drugi nadovezivao na to i uključivao pristup bazi podataka s ciljem pronalaska broja kreditne kartice određene osobe. Zadatak smo započeli analizom mreže 10.0.1.0/24, nakon čega smo skenirali otvorene portove pomoću alata nmap. Otkrili smo dva aktivna HTTP servisa – jedan nije imao login formu, dok se na drugome nalazila. Daljnjom enumeracijom pomoću alata Dirb i Nikto pronašli smo korisnička imena te nastavili istraživati ostale servise. Identificirali smo NFS servis koji je bio loše konfiguriran i omogućavao pristup bez autentikacije. Korištenjem naredbi showmount i mount uspjeli smo pristupiti dijeljenom direktoriju, unutar kojega smo pronašli korisničke podatke i privatne SSH ključeve. Nakon što smo postavili odgovarajuće dozvole na ključevima, uspjeli smo se putem SSH-a spojiti na sustav kao jedan od korisnika. Daljnjom analizom sustava pronašli smo i administratorsku lozinku, čime smo uspješno riješili prvi dio zadatka. U drugom dijelu zadatka bilo je potrebno pronaći broj kartice unutar baze podataka. Budući da nismo imali pristupne podatke za bazu, odlučili smo dodatno istražiti ostale mrežne servise. Otkrili smo FTP servis, na kojem smo pronašli backup konfiguracijskih datoteka. Unutar njih nalazila se .env datoteka koja je sadržavala korisničko ime i lozinku za bazu. Nakon uspješne autentikacije pristupili smo bazi i kroz jednostavne SQL upite došli do traženih podataka, odnosno broja kartice. Ova vježba pokazala nam je koliko je važno detaljno proučiti sve dostupne servise u mreži, iskoristiti loše konfiguracije poput anonimnog NFS pristupa i nezaštićenih FTP servisa, te kako povezivanjem informacija iz različitih izvora možemo doći do krajnjeg cilja. Kroz zadatak smo koristili niz alata kao što su nmap, dirb, nikto, showmount, mount, ssh, ftp, te alate za pristup bazama podataka, što nam je pomoglo da u praksi primijenimo znanja stečena tijekom edukacije.

13. dan
26.03.2025.

Na današnjoj praksi nastavili smo s vježbama iz edukacije vezane uz sigurnosne zadatke, s naglaskom na prepoznavanje i iskorištavanje ranjivosti unutar zadane mreže. Dobili smo samo osnovne informacije o mrežnoj strukturi, bez konkretnih podataka o cilju, što je značilo da prvo moramo provesti detaljnu rekognoscenciju kako bismo identificirali potencijalne mete. Krenuli smo standardno s alatom Nmap, koristeći različite vrste skeniranja, uključujući nmap -sS, -sV i -p-, kako bismo dobili što potpuniji pregled svih aktivnih hostova i njihovih otvorenih portova. Ubrzo smo otkrili jedan uređaj s otvorenim portom 445, koji je ukazivao na SMB servis. Detaljnijim skeniranjem verzije usluge ustanovili smo da je na tom hostu aktivna Samba verzija 3.5.0, što nam je odmah bilo zanimljivo jer smo se ranije kroz teoriju upoznali s poznatom ranjivošću vezanom uz funkciju is_known_pipename(). Riječ je o ranjivosti CVE-2017-7494, koja omogućuje udaljeno izvršavanje koda (RCE) ukoliko su ispunjeni određeni uvjeti. Prebacili smo se u Metasploit Framework pomoću msfconsole i pronašli odgovarajući modul za iskorištavanje ove ranjivosti (exploit/linux/samba/is_known_pipename). Konfigurirali smo ciljne parametre, uključujući IP adresu mete, port te korisnika i lozinku (u ovom slučaju guest pristup bez lozinke), i zatim postavili Meterpreter payload s reverse TCP konekcijom prema našoj Kali mašini. Nakon pokretanja exploita, uspješno smo uspostavili Meterpreter sesiju, čime smo dobili pristup ciljnom sustavu.

14. dan
27.03.2025.

Danas na praksi odrađena su dva zanimljiva i edukativna zadatka vezana uz sigurnost mreža i analizu prometa. Prvi zadatak bio je simulacija password guessing napada na login stranicu. Na početku smo pomoću alata Nmap skenirali mrežu i pronašli port na kojem se nalazila login forma. Dobili smo informaciju da je korisničko ime “admin”, dok je lozinka neki broj između 00 i 99, što nam je dalo 100 mogućih kombinacija. Problem je bio što sustav nakon 10 neuspješnih pokušaja blokira IP adresu na 5 minuta, što onemogućava klasični brute force napad unutar vremenskog ograničenja od 30 minuta. Rješenje je bilo korištenje alata proxychains i Tor mreže, čime smo mogli mijenjati svoju javnu IP adresu nakon svakih 10 pokušaja, čime smo zaobišli sigurnosnu zaštitu. Nakon što smo potvrdili da rotacija IP adresa funkcionira, napisali smo jednostavan brute force skriptu koja je testirala sve lozinke od 00 do 99 i uspješno se ulogirali unutar zadanog vremena. Drugi zadatak odnosio se na mrežnu analizu sumnjivog prometa. Analizirali smo IP adresu 172.x.x.x koja je imala velik broj konekcija putem porta 137 prema eksternim IP adresama. Port 137 koristi NetBIOS Name Service (NBNS), protokol koji omogućuje razrješavanje NetBIOS imena u IP adrese unutar lokalne mreže. Uobičajeno je da se takav promet odvija unutar LAN-a, pa komunikacija prema vanjskim adresama može ukazivati na pogrešnu konfiguraciju. U ovom slučaju, eksterni IP-ovi nisu se činili maliciozni, već su izgledali kao nasumične adrese bez jasnog obrasca, što upućuje na to da se vjerojatno radi o nekoj aplikaciji ili uređaju koji je greškom slao NBNS zahtjeve izvan mreže.

15. dan
28.03.2025.

Današnji dan na praksi bio je zanimljiv i raznolik, s kombinacijom tehničkog uvida i praktičnih zadataka. Na početku dana, zajedno s mentorom i još jednim kolegom iz našeg odjela otišli smo u sistemsku salu s kolegom iz drugog odjela kako bismo obišli prostor u kojem se nalaze serveri ključni za infrastrukturu i sigurnost sustava. Tamo su mi pokazani fizički serveri povezani sa sigurnosnim komponentama kao što su IBM QRadar, Fortinet, Check Point i ostali sustavi koji služe za detekciju, prevenciju i upravljanje sigurnosnim događajima u mreži. Bilo je vrlo korisno vidjeti fizički aspekt svega o čemu dosad učim u softverskom kontekstu – kako ti serveri izgledaju, kako su raspoređeni i kako se održavaju. Posebno mi je pažnju privukla sigurnosna oprema u prostoriji, poput boca plina koje se automatski aktiviraju u slučaju požara kako bi se spriječilo oštećenje opreme klasičnim gašenjem vodom, zatim sustavi za napajanje koji osiguravaju neprekidan rad servera čak i u slučaju nestanka struje, kao i sustavi hlađenja koji održavaju optimalnu temperaturu za rad opreme. Povratkom u ured, posvetio sam se edukacijskom zadatku vezanom uz SQL injection, gdje sam trebao iskoristiti ranjivost web aplikacije kako bih dobio pristup podacima u bazi. Prvi pokušaj nije bio uspješan jer sam pogrešno interpretirao odgovor aplikacije, no u drugom pokušaju bio sam blizu rješenja, ali mi je ipak nedostajalo malo znanja i iskustva da točno složim ispravan upit. Iako zadatak nisam potpuno riješio, bio je odlična prilika za učenje i bolje razumijevanje SQL ranjivosti te načina na koji aplikacije komuniciraju s bazama podataka. Na kraju dana pozdravio sam se s kolegama iz Zadra jer mi ostaje još samo jedan tjedan prakse u Splitu, nakon čega završava moj angažman. Ovaj dan bio je odličan spoj teorije i prakse, te mi je dao dodatnu motivaciju da nastavim učiti i istraživati područje informacijske sigurnosti.

16. dan
31.03.2025.

Danas na praksi dan je prošao prilično opušteno. Napravili smo par puta dodavanje i uklanjanje dozvola za USB uređaje putem Symanteca, temeljem zahtjeva koje zaposlenici šalju mailom. Proces je jednostavan – otvori se Symantec konzola, pronađe se korisnik koji je poslao zahtjev, provjeri se razlog i zatim se uređaju dodaju ili uklone dozvole za USB pristup, ovisno o potrebi. Nekoliko takvih zahtjeva stiglo je ujutro, pa smo to odradili bez problema, sve rutinski. Nakon toga više nije bilo nikakvih zadataka, pa sam odlučio iskoristiti vrijeme za rad na diplomskom radu. Smjestio sam se za svoj stol, otvorio dokument i nastavio pisati bez ometanja. Iskoristio sam mirnu atmosferu da se koncentriram i napravim veći dio posla nego što bih možda stigao kod kuće. Bio sam fokusiran i radio u kontinuitetu, što mi je stvarno dobro došlo. Danas sam u kod dodao i novu funkciju koja omogućuje automatsko pokretanje alata Sherlock prilikom pokretanja skripte, što će olakšati rad jer više nije potrebno ručno unositi svaki put korisničko ime i pokretati alat posebno. Sherlock je inače alat koji služi za pronalazak korisničkih imena na raznim web platformama, pa mi ta funkcionalnost puno znači u kontekstu rada koji obrađujem. Uz to sam još malo doradio komentare u kodu kako bi sve bilo jasnije za kasniju dokumentaciju. Ostatak dana prošao je u tišini, bez dodatnih zadataka ili ikakvih promjena, pa sam jednostavno nastavio pisati sve do kraja radnog vremena.

17. dan
01.04.2025.

Danas na praksi nije bilo klasičnih aktivnosti jer je mentor radio od kuće, pa nisam imao nikakve konkretne taskove ni zadatke za odraditi. U uredu je bilo prilično mirno, bez posebnih uputa ili stvari koje bih mogao samoinicijativno preuzeo s obzirom na ograničenja pristupa određenim sustavima. Iskoristio sam zato slobodno vrijeme da nastavim rad na diplomskom radu. Danas sam se fokusirao na tehnički dio vezan uz integraciju alata za prikupljanje podataka. Djelomično sam implementirao alat Harvester, koji se koristi za prikupljanje informacija o domenama i emailovima putem OSINT metoda. Uz to, doradio sam i dio koji se odnosi na Sherlock – alat za traženje korisničkih imena na različitim platformama. Nakon što sam ih pokrenuo i testirao, krenuo sam s implementacijom zapisivanja podataka koje Sherlock i Harvester pronađu direktno u bazu podataka. Napravio sam osnovnu strukturu tablica, sredio povezivanje s bazom i testirao unos rezultata s oba alata. Sve zasad funkcionira kako treba, ali još ima posla oko validacije podataka i kasnijeg prikaza. Dodatno sam proveo neko vrijeme testirajući kako se ponašaju upiti iz oba alata na različite primjere korisničkih imena i domena, kako bih kasnije mogao automatski filtrirati rezultate koji su korisni za analizu. Razmišljam i o dodavanju vremenske oznake za svaki unos u bazu, kako bi se moglo pratiti kad je koji podatak dohvaćen, što bi moglo biti korisno za kasniju obradu.

18. dan
02.04.2025.

Tijekom današnje prakse fokusirao sam se na analizu problema prekida veze između jednog routera i SIEM sustava (IBM QRadar). Identificiran je problem u kojem uređaj u određeno vrijeme svakog dana prestaje slati logove prema QRadar-u, što potencijalno znači da dolazi do privremenog gašenja ili restarta routera. Korištenjem IP SLA mehanizma potvrđeno je da se u tom periodu router nakratko gasi – prestaje odgovarati na pingove, što se vremenski poklapa s nestankom logova u SIEM-u. Analizirani su potencijalni uzroci tog ponašanja, uključujući mogućnost zakazanog restarta, problema s napajanjem (npr. nestabilan adapter ili PoE prekid), automatskog firmware ažuriranja, ali i internih sigurnosnih mehanizama kao što su zaštita od pregrijavanja ili pad sustava zbog bugova u firmwareu. Preporučeno je dodatno analizirati logove na samom uređaju (npr. syslog, uptime, crash logovi), kao i moguće zadane rasporede restarta (scheduler ili cron, ovisno o proizvođaču routera), kako bi se utvrdio konkretan uzrok ponašanja. Također, tijekom dana bio je održan sastanak na kojem su predstavnici tvrtke Darktrace predstavili funkcionalnosti njihovog sigurnosnog rješenja koje se odnedavno koristi u OTP banci. Budući da je sustav još u fazi uvođenja, sastanak je bio fokusiran na osnovne značajke platforme, uključujući način na koji koristi umjetnu inteligenciju za prepoznavanje anomalija i prijetnji unutar mrežnog prometa. Demonstrirane su mogućnosti vizualizacije mrežnih tokova, automatske reakcije na sumnjive aktivnosti te integracija s drugim sigurnosnim alatima poput SIEM-a. Ova prezentacija bila je korisna za razumijevanje kako se Darktrace može koristiti u svakodnevnom operativnom radu sigurnosnog tima i kako doprinosi bržoj detekciji prijetnji u realnom vremenu. Osim rada na praktičnim zadacima i sudjelovanja na sastanku, danas sam također posvetio dio vremena svom diplomskom radu. Konkretno, proučavao sam alat SpiderFoot, koji je namijenjen za automatsko prikupljanje OSINT (Open Source Intelligence) podataka. SpiderFoot nudi velik broj modula za prikupljanje informacija o ciljevima iz javno dostupnih izvora – uključujući domene, IP adrese, email adrese i ostale oblike identiteta. Alat može poslužiti u sklopu diplomskog rada kao snažan dodatak za automatizaciju phishing kampanja, što je glavni fokus mog rada. Danas sam se detaljno upoznao s načinom na koji SpiderFoot funkcionira, kako se konfiguriraju moduli te koje sve izvore koristi, no implementacija u vlastiti kod još nije izvršena.

19. dan
03.04.2025.

Danas sam na praksi započeo sudjelovanjem u online prezentaciji održanoj putem Webex platforme, koju je organizirala SWIFT Learning Services, edukacijska jedinica unutar organizacije SWIFT (Society for Worldwide Interbank Financial Telecommunication). Prezentacija je bila usmjerena na detaljno razumijevanje uloge SWIFT mreže u međunarodnim financijskim transakcijama, pri čemu je objašnjeno da SWIFT sam po sebi ne prenosi novac, već služi kao globalna mreža za sigurnu i standardiziranu razmjenu financijskih poruka između banaka i drugih financijskih institucija. Kroz konkretne primjere poruka poput MT103, sudionicima je prikazano kako se komuniciraju nalozi za plaćanje i kako sustav osigurava točnost, sigurnost i brzinu prijenosa tih informacija. Poseban naglasak bio je na sigurnosnim aspektima, uključujući enkripciju, digitalno potpisivanje poruka, autentifikaciju korisnika, kao i na mjerama iz Customer Security Programme (CSP) – inicijative koja ima za cilj podići razinu sigurnosti svih sudionika unutar SWIFT mreže. Također se govorilo o budućem prelasku na standard ISO 20022, koji donosi bogatiju strukturu podataka i veću interoperabilnost među sustavima. Nakon završetka prezentacije, nastavio sam s radom na svom diplomskom radu. Danas sam implementirao funkcionalnost koja omogućuje da se svi relevantni podaci prikupljeni preko OSINT alata automatski pohranjuju u bazu podataka.

20. dan
04.04.2025.

Danas sam nastavio s radom na diplomskom radu, fokusirajući se na operativni dio koji uključuje obradu i organizaciju podataka prikupljenih putem Google dorkanja. Glavnina aktivnosti bila je usmjerena na filtriranje i pripremu linkova za daljnji scraping, kao i na tehničku prilagodbu alata kako bi se osigurala stabilnost i pouzdanost procesa. Uz pomoć dorkanja, točnije korištenja naprednih Google pretraživačkih operatora (Google dorkova), uspio sam pronaći značajan broj linkova koji vode do javno dostupnih podataka o firmama koje koriste određene banke. Dorkovi koje sam koristio bili su orijentirani na pronalazak e-mail adresa, kontakt stranica, popisa zaposlenika i povezanih PDF ili Excel dokumenata. Na temelju tih rezultata, sada imam kolekciju linkova koju je potrebno obraditi tehnikom web scrapinga. Tijekom rada razvio sam funkcionalnosti za dohvat sadržaja stranica, no kako bi proces bio što učinkovitiji i izbjegao probleme s ograničenjima (npr. greška 429 – Too Many Requests), razmatram i dodatne mjere zaštite. Trenutno radim na implementaciji rotacije User-Agent zaglavlja kako bi scraper imitirao različite preglednike i uređaje. Osim toga, potrebno je uvesti rotaciju proxy IP adresa, kako bi se izbjeglo da više zahtjeva dolazi s iste IP adrese u kratkom vremenu, što lako može dovesti do privremenih ili trajnih blokada pristupa određenim stranicama. Također, počeo sam razmatrati promjenu trenutnog Google Custom Search Engine (CSE) API-ja. Iako daje solidne rezultate, u nekim slučajevima API vraća previše irelevantnih rezultata ili preskače korisne linkove koje bih dorkanjem mogao pronaći ručno. Istražujem mogućnosti boljeg podešavanja trenutnog CSE-a, ali i opciju kreiranja više CSE instanci s različitim konfiguracijama kako bih dobio širi spektar podataka za analizu.