Emulacija napadača na usluge u oblaku za potrebe penetracijskog testiranja

Raspudić, Luka

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 664

EMULACIJA NAPADAČA NA USLUGE U OBLAKU ZA POTREBE PENETRACIJSKOG TESTIRANJA

Luka Raspudić

Zagreb, lipanj 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 664

EMULACIJA NAPADAČA NA USLUGE U OBLAKU ZA POTREBE PENETRACIJSKOG TESTIRANJA

Luka Raspudić

Zagreb, lipanj 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 4. ožujka 2024.

DIPLOMSKI ZADATAK br. 664

Pristupnik:	**Luka Raspudić (0119044229)**
Studij:	Računarstvo
Profil:	Računarska znanost
Mentor:	izv. prof. dr. sc. Stjepan Groš

Zadatak: **Emulacija napadača na usluge u oblaku za potrebe penetracijskog testiranja**

Opis zadatka:

Sve više organizacija koristi usluge u oblaku koje se u određenoj mjeri razlikuju u odnosu na usluge koje se izvršavaju u samoj organizaciji. Posljedica je da se penetracijska ispitivanja moraju prilagoditi novoj situaciji i specifičnim karakteristikama usluga u oblaku. Za to je potrebno stvoriti katalog incidenata ih kojih se može učiti kako napadati usluge u oblaku te vježbe s kojima bi se stjecale odgovarajuće vještine. U diplomskom radu potrebno je pronaći i katalogizirati reprezentativni broj incidenata u oblaku. Na temelju tih incidenata potrebno je složiti kategorije napada te za svaku kategoriju opisati ključne karakteristike i taktičke korake korištenjem MITRE ATT&CK baze. Nadalje, potrebno je proučiti usluge koje pružatelji usluga u oblaku nude svojim korisnicima za zaštitu od napada te kakve tragove ostavlja svaka kategorija napada u tim sustavima. Opisati korake na obrambenoj strani uz pomoć kojih se mogu otkriti i spriječiti napadi u različitim fazama. U praktičnom dijelu potrebno je složiti zadatke uz pomoć kojih se mogu obučavati penetracijski testeri za ispitivanje sigurnosti usluga u oblaku.

Rok za predaju rada: 28. lipnja 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 664

EMULACIJA NAPADAČA NA USLUGE U OBLAKU ZA POTREBE PENETRACIJSKOG TESTIRANJA

Luka Raspudić

Zagreb, rujan, 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 4. ožujka 2024.

DIPLOMSKI ZADATAK br. 664

Pristupnik:	**Luka Raspudić (0119044229)**
Studij:	Računarstvo
Profil:	Računarska znanost
Mentor:	izv. prof. dr. sc. Stjepan Groš

Zadatak: **Emulacija napadača na usluge u oblaku za potrebe penetracijskog testiranja**

Opis zadatka:

Sve više organizacija koristi usluge u oblaku koje se u određenoj mjeri razlikuju u odnosu na usluge koje se izvršavaju u samoj organizaciji. Posljedica je da se penetracijska ispitivanja moraju prilagoditi novoj situaciji i specifičnim karakteristikama usluga u oblaku. Za to je potrebno stvoriti katalog incidenata ih kojih se može učiti kako napadati usluge u oblaku te vježbe s kojima bi se stjecale odgovarajuće vještine. U diplomskom radu potrebno je pronaći i katalogizirati reprezentativni broj incidenata u oblaku. Na temelju tih incidenata potrebno je složiti kategorije napada te za svaku kategoriju opisati ključne karakteristike i taktičke korake korištenjem MITRE ATT&CK baze. Nadalje, potrebno je proučiti usluge koje pružatelji usluga u oblaku nude svojim korisnicima za zaštitu od napada te kakve tragove ostavlja svaka kategorija napada u tim sustavima. Opisati korake na obrambenoj strani uz pomoć kojih se mogu otkriti i spriječiti napadi u različitim fazama. U praktičnom dijelu potrebno je složiti zadatke uz pomoć kojih se mogu obučavati penetracijski testeri za ispitivanje sigurnosti usluga u oblaku.

Rok za predaju rada: 28. lipnja 2024.

Sadržaj

1. Uvod

Današnje digitalne tehnologije se brzo razvijaju i svojim razvojem omogućavaju daljnji razvoj drugim tehnologijama. Jedna od takvih tehnologija koja je pridobila veliku pozornost je računalstvo u oblaku (eng. Cloud computing).

Glavni motivacijski razlozi za pridobivenu pažnju su smanjenje inicijalnih troškova infrastrukture, monetarnih i vremenskih, olakšan razvoj i proširivanje infrastrukture. Poslovni korisnici ne trebaju proširivati svoju hardversku infrastrukturu, što zahtijeva vrijeme, novac i ljudske resurse, kako bi podržala rast korisnika. Davatelj usluga (engl. Cloud provider) se brine o skaliranju korištenih resursa što znači da će davatelj usluga uvijek davati računalne snage koliko je potrebno. Poslovni korisnici trebaju samo platiti korištene resurse i u kraćem roku dobivaju sklopovlje nego što bi oni sami implementirali. Na taj način poslovni korisnici mogu davati najbolju uslugu, a korisnici imati najbolje korisničko iskustvo.

Jedno od često postavljanih pitanja je koliko je računalstvo u oblaku sigurno. Ovaj rad se bavi pronalaskom dosad zabilježenih napada na računalne usluge u oblaku, pokušava naći propuste u incidentu te klasificira greške na pružatelja ili razvojni tim korisnika.

Rad se sastoji od poglavlja: Incidenti, Cyber Conflict Simulator, Teorija, Praktični dio te Zaključak. U poglavlju Incidenti osvrćemo se na prijavljene ranjivosti (rezultat napada ili istraživanja), tijek događaja kao i greške pronađene u incidentima. U poglavlju Cyber Conflict Simulator se objašnjava platforma koja je korištena za simulaciju kao i neke osnovne mogućnosti za razumijevanje i korištenje. Poglavlje Teorija je zamišljenja kao objašnjavanje ideje iza implementacije. Sadrži potpoglavlja Idealni slučaj te potpoglavlje Implementacija gdje se objašnjavaju zaobilaznice koje su korištene u implementaciji idealnog slučaja gdje nemamo nikakva ograničenja. Poglavlje Praktični dio objašnjava

korake kojim se rješava zamišljena simulacija. Na kraju dolazi poglavlje Zaključak kojim zaokružujemo cijelu priču.

2. Incidenti

U ovom poglavlju se osvrćemo na pronađene propuste u aplikacijama koje se izvode u oblaku (engl. *Cloud*). Pronađeni propusti nisu nužno bili zabilježeni kao incidenti gdje su napadači iskoristili propuste u svoju korist te naštetili korisnicima ili kompanijama, već i kao rezultati istraživanja te nailaska na ranjive servise i njihovo dojavljivanje odgovornima.

Pošto nema svaki incident jasno okvirno vrijeme ili razdoblje događanja radi manjka zapisivanja u dnevnik događaja (engl. *event log*), napadačevoga brisanje tragova ili jednostavno odbijanja objavljivanja informacija) ići će se kronološki, primarno po znanju vremena incidenta, sekundarno po vremenu dojave. Vrijeme dojavljivanja je kada su odgovarajuće službe dobile saznanje za događanje.

2.1. Uber (2014)

Uber, američka multinacionalna transportna kompanija, pruža usluge prijevoza, kurirske usluge, dostavu hrane te prijevoz tereta [1].

Nepoznati napadač je iskoristio Uberov GitHub repozitorij gdje je kod bio javno dostupan [2, 3]. Unutar koda je bio AWS-ov (Amazon Web Services) pristupni ključ kojim je pristupio spremniku (eng. *bucket*). Podaci u spremniku su bili dostupni u nešifriranom obliku. Napadač je preuzeo datoteku s osjetljivim podacima koja sadrži preko 100 000 imena i podataka vozačkih dozvola te 215 korisničkih bankovnih računa. Napad se odvio 12.5.2014. te napadač nije otkriven.

Ovaj incident je primjer nesigurnih praksi razvojnog tima gdje je korišten jedan pristupni ključ za sve programe i zaposlenike koji je davao administrativne privilegije te tvrdo kodiranih (eng. *hard-coded*) osjetljivih podataka.

Ovaj incident je primjer nesigurne prakse razvojnog tima, korišten je jedan pristupni ključ [2] za sve programe i zaposlenike koji je davao administrativne privilegije. Drugi propust, tvrdo kodirani (eng. *hard-coded*) osjetljivi podaci.

2.2. Codespaces (2014)

Codespaces je usluga koja je pružala usluge hostinga koda i upravljanja projektima.

U opisu napada, niže, se spominje DDoS (*Distributed Denial of Service*) napad. Za početak, postoji i DoS (*Denial of Service*) napad gdje napadač šalje velike količine podataka putem interneta s namjerom da server ne stigne obraditi zahtjeve i ostali korisnici ne dobivaju tražene rezultate te nanijeti štetu kompaniji. Moguće je i da napadač koristi DoS napad kao ucjenu da traži od kompanije monetarna sredstva. DDoS je napredna verzija DoS napada, gdje ima više DoS napada odjednom, odnosno iz više izvora.

Također se spominje Amazonov EBS (*Elastic Block Store*). EBS je spremište podataka koji se priključuje za EC2 (*Elastic Compute Cloud*). EC2 je Amazonov servis koji omogućava korisnicima da pokreću svoje aplikacije, jednostavnije rečeno, EC2 je virtualni server, a EBS je njemu ono što je fizički disk računalu, pohrana podataka.

Spominje se i S3 spremnik (eng. *bucket*), S3 je sličan EBS-u u smislu da su oboje spremišta podataka, ali postoje razlike. EBS je brzo spremište koje se priključuje na samo jednu EC2 instancu i ima hijerarhijsku organizaciju (*file storage*) te je fiksne veličine. S3 je napravljeno više kao jezero podataka tako da se u svakom trenutku može spojiti više EC2 instanci i obrađivati podatke, S3 je *object storage service* te je napravljen za stvari koje se ne mijenjaju često, više kao sustav arhiviranja i skalabilan je.

Nepoznati napadač je 17.6.2014. izveo organizirani DDoS napad te pokušao ucijeniti kompaniju Codespaces [4, 5]. Kada je propao pokušaj ucjene, napadač je ostvario pristup do EC2 upravljačke ploče (eng. *control panel*), nije dodatno izjašnjeno kako je napadač došao do upravljačke ploče. Kada su zaposlenici Codespacea uspješno vratili kontrolu upravljačke ploče počeli su mijenjati sve zaporke, ali napadač je imao više novokreiranih stražnjih vrata te je izbrisao sve EBS sigurnosne pohrane, S3 spremnike, AMI (*Amazon Machine Images*) i nekolicinu mašina.

Ovaj incident je primjer da je potrebno imati kopije kritičnih podataka i infrastrukture te služiti korisničkom podrškom pružatelja jer bi Amazon lakše detektirao odstupanja [4].

2.3. BrowserStack (2014)

BrowserStack je cloud platforma za testiranje više vrsta platformnih aplikacija (eng. *cross-platform applications*), omogućava korisnicima da testiraju rad internetskih aplikacija na više internetskih preglednika, rad mobilnih aplikacija na svim mobitelima bez ikakvih virtualnih mašina, uređaja i emulatora [6].

U studenom 2014. je napadač otkrio EC2 instancu koja se vrti od 2012. Nije bila više korištena, niti održavana te je bila podložna ranjivosti *Shellshock*, odnosno *Bashdoor* [6]. *Shellshock* ranjivost omogućava napadaču izvođenje proizvoljnih naredbi na uređaju koji ima pristup internetu [7]. Izvođenje proizvoljnih naredbi omogućava napadaču da izvrši naredbe kojima ne bi smio imati pristup, potencijalno može rezultirati napadačevim preuzimanjem potpune kontrole nad serverom te imati nesmetan pristup podacima. Zahvaća *Bash* ljusku na Unix obitelji operativnih sustava.

Zahvaćena mašina je na sebi imala AWS API pristupne ključeve (eng. *Application Programming Interface*) čime je napadač uspješno kreirao IAM (*Identity and Access Management*) korisnika i SSH ključ te tako otvorio trajna stražnja vrata (eng. *backdoor*). Zatim je napravio novu EC2 instancu koja je imala ulogu sigurnosne kopije podataka te je našao vjerodajnice za bazu podataka u kojoj su se nalazile vjerodajnice korisnika. Napadač je uspio napraviti sigurnosnu kopiju jedne baze podataka te je izvukao dio korisnika te njihove odgovarajuće informacije poput: šifriranih zaporki, zadnji testirani URL (*Uniform Resource Locator*) i adresa e-pošte (eng. *email address*).

Iz propusta je bilo utvrđeno da BrowserStack nije pratio sigurnosne procedure i preporuke. Kao prvo, pristupni ključevi nisu bili redovito mijenjani. Drugo, imali su nekorištene resurse koji su bili aktivni. Treće, aktivni resursi nisu bili ažurirani kako bi se ranjivosti zakrpale. Četvrto, nisu imali aktivne sustave koji su pratili promjene u administrativnim računima kako bi zabilježili promijene i obavijestili odgovarajuće osobe o potencijalnim sumnjivim aktivnostima.

2.4. Uber (2016)

Napadači su u listopadu 2016. pomoću ukradenih vjerodajnica te napadom grube sile (eng. *brute-force attack*) uspjeli ući korisnički račun programera Ubera na GitHubu [3, 2]. Kopanjem po GitHub repozitoriju su naišli na pristupni ključ za S3 spremnik. Taj spremnik je sadržavao indentificirajuće podatke za više od 57 milijuna korisnika.

Napadači su poslali e-poruku s obavijesti da su pronašli ranjivost i da su dobili pristup Uberovoj bazi podataka. Uberov CISO (*Chief Information Security Officer*) je pristao platiti $100,000 maskirajući iznos kao *bug-bounty* nagradu. Također, pristupni ključ u ovom incidentu je bio kreiran 2013. godine [2], što je godinu dana prije ranije spomenutog incidenta 2.1.

Ovaj incident je primjer nepoštivanja sigurnosnih preporuka. Pristupni ključ se nije rotirao. Drugo, ponovo su pronađeni osjetljivi podaci tvrdo kodirani u kodu. Treće, podaci se nisu sigurno skladištili i posljednje, nije bilo dvofaktorske autentifikacije.

2.5. Vitagene (2016)

Vitagene, kompanija koja se bavi sekvenciranjem DNA uzoraka te njihovog skladištenja, je imala javno dostupan S3 spremnik s 2,500 zdravstvenih podataka i genetskih sekvenci [8]. Vitagene je bio više puta upozoren da ima spremnik koji je javno dostupan, točnije 3 puta između srpnja 2017. godine i lipnja 2019. godine [9, 10]. Osoba koja je prijavila propust je bio sigurnosni istraživač, također je i Amazon dojavio Vitagenu da ima javno dostupan S3 spremnik, točnije 6 njih. Iako je bilo pokriveno na vijestima loša politika štićenja korisničkih DNA podataka, nije bilo nikakvih doznaka da se navedeni propust iskoristio. Unatoč brojnim upozorenjima kompanija nije duži period poduzela potrebne mjere da zaštiti svoje korisnike.

Ovaj incident je primjer loše postavljene konfiguracije servera.

2.6. DataDog (2016)

U 7. srpnja 2016. godine je SaaS (Software-as-a-Service) poslužitelj DataDog, kompanija koja se bavi davanjem usluga IT infrastrukture te usluga praćenja i analitike, imao

incident [11, 12]. Napadač nije otkriven, zna se da je dobio pristup produkcijskoj infrastrukturi na način da je postojalo curenje podataka (eng. *data leak*), točnije procurio je AWS pristupni ključ i SSH privatni ključ. Kombinacija ta dva ključa je omogućila da napadač dođe do tri EC2 instance i podskupa S3 spremnika. Unutar EC2 instanci i S3 spremnika napadač je uspio dodatno doći do korisničkih vjerodajnica, metapodataka usluga i vjerodajnica za integracije treće strane (eng. 3^{rd} *party integrations*).

Ovaj incident je primjer loše čuvanja pristupnih ključeva te SSH ključa.

2.7. Verizon (2017)

U lipnju 2017. UpGuard, kompanija za kibernetičku sigurnost, je naišla na S3 spremnik koji nije bio ni na koji način zaštićen u vlasništvu tvrtke Verizon [13, 14]. Podaci su bili nešifrirani i sadržavali su informacije o 200 milijuna američkih glasača. Svaki glasač je imao svoju decimalni broj između 0 i 1 za 46 kolona gdje je svaka kolona predstavljala glasačevu vjerojatnosnu pristranost politikama, političkim kandidatima i uvjerenju [15].

Ovaj incident je primjer pogrešne konfiguracije (eng. *misconfiguration*) spremnika.

2.8. Los Angeles Times (2018)

U veljači 2018. je sigurnosni istraživač Troy Mursch otkrio *crypto-jacking* skriptu [16, 17]. *Crypto-jacking* je vrsta napada u kojem napadač neautorizirano koristi tuđe uređaje kako bi rudarila kriptovalute. Napadač je otkrio nezaštićeni S3 spremnik na kojem se nalazila skripta koja se izvršavala svaki put kada bi netko otišao na poddomenu Homicide Los Angeles Times stranice. Napadač je izmijenio skriptu tako da se prilikom učitavanja stranice počela vrtiti i skripta za rudarenje kriptovalute, kako bi bila što manje uočljiva, je imala limitirao korištenje procesora na 80%.

Ovaj incident je primjer pogrešne konfiguracije.

2.9. Chegg

U travnju 2018. je edukacijska platforma Chegg imala incident. Edukacijska platforma je ostavila iste pristupne podatke s najvišim administratorskim (eng. *root*) ovlastima bez

višefaktorske autentifikacije svim svojim vanjskim izvođačima i zaposlenicima [18]. Saznalo se tek u rujnu 2018. kada je dobavljač obavještajnih podataka o prijetnjama otkrio internetski forum s 25 milijuna nešifriranih korisničkih zaporki.

Ovaj incident je primjer lošeg upravljanja pristupa.

2.10. Cisco (2018)

Cisco, američka multinacionalna kompanija koja se bavi digitalnim komunikacijama, je imala incident u rujnu 2018. Bivši zaposlenik je pomoću svojega pristupnoga ključa ušao u Ciscovu AWS-ovu upravljačku ploču te implementirao (eng. *deployed*) svoj kod s privatnog Google Cloud projekta čime je obrisao 456 virtualnih mašina koje su pružale usluge Ciscove *WebEx Teams* aplikacije za video sastanke, video poruke, prijenos datoteka i ostalih alata za suradnju (eng. *collaboration tools*) [19, 20, 21, 22].

Ovaj incident je primjer unutarnje prijetnje (eng. *insider threat*).

2.11. Imperva (2018)

U listopadu 2018. je napadač ušao u ranjivu EC2 instancu i na njoj našao AWS API ključeve [23, 24]. Ključevi su zatim korišteni da napadač dođe do Amazonove produkcijske RDS (*Relational Database Service*) snimke (eng. *snapshot*). RDS snimka je imala potrebne informacije o njihovom produktu *Incapsula WAF* (*Web Application Firewall*) i sadržavala je korisničke e-mail adrese, kriptografski heširane zaporke, API ključeve i korisničke SSL certifikate.

Ovaj incident je primjer lošeg upravljanja pristupa, točnije, EC2 instanca je trebala biti ugašena ako se više ne koristi. Pristupni ključevi su trebali biti rotirani te na kraju, EC2 instanca je imala pristup na internet iako nije trebala za svoju dužnost.

2.12. Attunity (2019)

Attunity, kompanija koja je pružatelj usluge za pola Fortune 100 kompanija, imala veliko curenje podataka (eng. *data leak*) [25]. U javno dostupnim spremnicima su sadržavali:

vjerodajnice, sistemske vjerodajnice (primjerice *connection string* za baze podataka), privatni ključevi, e-mail za resetiranje zaporke (cijeli e-mail bio nešifriran pa su se sve informacije vidjele), povijest lokalno spremljenih git verzija, produkcijski VLAN-ovi (Virtual Local Area Network), Excel tablica sa svim informacijama o zaposlenicima [25].

Ovaj incident je primjer pogrešno postavljene konfiguracije.

2.13. CAM4 (2020)

CAM4, platforma za odrasle koja prodaje odrasle snimljene usluge ili usluge uživo, je imala loše konfiguriranu bazu podataka te je bilo tko mogao vidjeti razne informacije [26]. Primjeri slika se mogu naći u izvještaju [27]. Baze podataka su pronašli istraživački tim kibernetičke sigurnosti kompanije SafetyDetectives. Među podacima su pronađeni identifikacijski podaci korisnika, e-mail adrese i odgovarajući kriptografski heš (eng. *hash*) zaporke, država rođenja, informacije uređaja, korisnička imena, privatni razgovori i sl. [28, 27, 26].

U ovom incidentu je krivica loše konfiguriranog servera.

2.14. First Republic Bank (2020)

U ožujku 2020. cloud inžinjer je dobio otkaz iz First Republic Bank banke [29]. Bivši zaposlenik je trebao predati svoje osobno računalo i prijenosno računalo. Predao je osobno računalo, ali je od doma pomoću prijenosnog računala koristeći svoje vjerodajnice ušao u sustav banke i lažno se predstavljao kao drugi zaposlenik. Tokom lažnog predstavljanja je pokrenuo skriptu koja je terminirala gotovo sve instance Amazon Web servisa, obrisao repozitorije kodova te ubacio podrugljive linije u kod [29, 30, 31].

Ovaj incident je primjer unutarnje prijetnje (eng. *insider threat*) kao i lošega upravljanja pristupa (eng *improper access management*). Bivšem zaposleniku su trebale biti ukinute vjerodajnice tako da nema pristup osjetljivim podacima.

2.15. Drizly (2020)

U srpnju 2020. je Drizly, kompanija za dostavu alkohola na zahtjev, imala proboj podataka (eng. *data breach*) [32]. Unazad dvije godine, 2018., kompanija je napravila korisnički račun na GitHubu izvršnom direktoru za *hackathon* te dala dozvole pristupa kodu. Po završetku *hackathona* korisnički račun je ostao. Napadač je uspio ući u taj korisnički račun koristeći vjerodajnice iz nepovezanog proboja podataka (eng. *breach*). Korisnički račun je imao slabu zaporku, bez višefaktorske autentifikacije. Napadač je pomoću tog računa došao do svih GitHub repozitorija tvrtke. U jednom od repozitorija je našao pristupni ključ za AWS te je izvukao 2.5 milijuna korisničkih podataka. Ograničeni dio probijenih podataka su potvrdili, uz provjeru pomoću javnih zapisa, da sadrže broj mobitela korisnika, IP adrese i geolokacije uz korisnikovu adresu naplate [33].

Ovaj incident ima više propusta. Prvi je loše upravljanje pristupom (eng. *improper access management*), nepotreban korisnički račun je trebao biti onemogućen, potencijalno prevelika dopuštenja. Korisnik bi trebao imati onoliko dopuštenja kolika su mu potrebna da odradi posao. Drugi propust je loša *higijena* zaporki, 7 malih slova bez ikakvih specijalnih znakova bi se trebalo izbjegavati jer se probije momentalno[1]. Treći propust, osjetljivi podaci su tvrdo kodirani. Četvrti propust, nije korištena višefaktorska autentifikacija.

2.16. Ubiquiti (2020)

Početkom prosinca 2020. kompanija Ubiquiti je otpustila višeg (eng. *senior*) programera. Kasnije tokom prosinca, otpušteni programer je, uz pomoć VPN-a, iskoristio svoje vjerodajnice kako bi se prijavio u sustav [34]. Nakon uspješne prijave, počeo je skidati sav kod s GitHub repozitorija. Tokom skidanja informacija došlo je do prekida internetske veze, nakon uspostave veze se VPN nije ponovo povezao tako da je napadač pristupao podacima sa svojom IP adresom. Radi te greške je kasnije uhvaćen. Nakon skidanja većine repozitorija, napadač je otišao u AWS postavke kompanije, ali pod okriljem svojeg VPN-a promijenio postavke životnoga ciklusa S3 spremnika s zapisima pristupa (eng. *logs*) na jedan dan čime se svaki dan briše zapisnik. Kada se saznalo za napad, kompanija je kreirala istražni tim od viših programera i napadač, kao nedavni zaposlenik, se

[1] https://tech.co/password-managers/how-long-hacker-crack-password (pristupano 5.9.2024.)

bio pridružio. Nakon pridruživanja je napadač poslao ucjenjivačku poruku. Kompanija nije uplatila i tražila je pomoć od FBI-ja (*Federal Bureau of Investigation*). FBI je uhvatio napadača radi spomenute greške te ubrzo izgradio slučaj [35, 36].

Ovaj incident je primjer unutarnje prijetnje (eng. *insider threat*). Bivši zaposlenik koristi znanje rada kompanije kao i propuste, koje je on napravio ili barem znao, kako bi iskoristio u svoju korist. Naravno, drugi dio propusta je da kompanija ima loše upravljanje pristupa (eng. *improper access management*).

2.17. Adminer (2021)

Mandiant, podružnica Googla koja se bavi kibernetičkom sigurnosti, proučava često korištene taktike raznih hakerskih skupina te je uočila novu skupinu UNC2903 kako skenira infrastrukturu koja udomljava (eng. *hosting*) Adminer, alat otvorenog koda za održavanje baza podataka napisana u PHP-u [37]. Adminer, verzije između 4.0 i 4.7.9, imaju propust poznat kao *Server-Side Request Forgery* (SSRF). Napadači bi pomoću SSRF propusta došli do osjetljivih podataka poput pristupnog ključa i vjerodajnica.

Skupina UNC2903 je pokrenula svoj server koji na svaki zahtjev vraća odgovor *301 redirect* na adresu *http://169.254.169.254/latest/meta-data/*, ta adresa je namijenjena da korisnici AWS-a mogu dobiti metapodatke iz pokrenute instance. Prilikom prijavljivanja u Adminer, napadač bi unio IP adresu svojeg servera, poslao bi se zahtjev na napadačev server, dobio bi odgovor da pogleda na gore napisanu adresu. Amazon bi vratio metapodatke, a alat bi ih vratio napadaču uz grešku da se nije uspio spojiti [38].

Ovaj incident je primjer korištenja zastarjelog softvera.

2.18. LastPass (2022)

Kompanija LastPass je bila žrtva organiziranoga napada [39]. Prvi napad se dogodio u kolovozu 2022. gdje je napadač iskoristio ranjivost softvera za reprodukciju medija Plex [40, 41]. Plex je imao veliki propust jer je dozvoljavao napadaču da pokrene svoj kod, kroz njega je napadač instalirao svoj softver na zaposlenikovo računalo te pokrenuo softver za praćenje unosa s tipkovnice (eng. *keylogger*). Uspio je saznati zaporku i

višefaktorsku autentifikaciju potrebnu za infiltriranje u sustav kompanije. Napadač je ušao u neprodukcijski sadržaj i repozitorije kodova gdje je došao do tvrdo kodiranih vjerodajnica, digitalnih certifikata te enkriptiranih vjerodajnica [42]. Napadač je u drugom napadu uspio, na temelju podataka izvučenih iz prvog napada i glavne zaporke žrtve, ući u korporativni trezor i doći do ključeva za dešifriranje [43].

Ovaj incident je primjer korištenja zastarjelog/nezakrpanog (eng. *outdated* ili *obsolete*) sofvera. Kompanija je postavila *Cloud Security Posture Management* (CSPM), zaslužan za praćenje aktivnosti, otkrivanje prijetnji te pogrešnih konfiguracija, nakon prvoga napada što može implicirati da do tada nije bilo sigurnosnih sustava te vrste [39, 42].

2.19. CommuteAir (2023)

U siječnju 2023. napadač je, koristeći alat ZoomEye (kineska tražilica), skenirao internet za ranjive Jenkins servere [44, 45, 46]. Nađen je Jenkins server aviokompanije CommuteAir, unutar servera se nalazilo 70 repozitorija od kojih su dva sadržavala identificirajuće podatke o ljudima kojima je zabranjeno korištenje avioprijevoza. Napadač je, također, dobio pristup i *API* sučelju koje kontrolira punjenje aviona gorivom te ažuriranje i otkazivanje letova. Koristeći vjerodajnice u repozitoriju napadač je neometano pristupao AWS infrastrukturi aviokompanije.

Ovaj incident je primjer tvrdo kodiranih vjerodajnica, nešifriranja osjetljivih podataka te pogrešno konfiguriranoga servera.

2.20. Toyota (2023)

Toyota, japanski međunarodni proizvođač automobila, je imala javno dostupan Cloud server s informacijama o kupcima, e-mail adresama, punim imenima, vozilima, registarskim oznakama i identifikacijskim brojevima vozila te pretplatama na dodatne usluge [47, 48]. Toyota je priznala da je propust trajao 8 godina, od 2015. do 2023. godine. Nije bilo naznaka da su se procureni podaci iskoristili.

Ovaj incident je primjer loše konfiguriranog servera.

2.21. Microsoft (Storm-0558, 2023)

Microsoft je imao incident u svibnju 2023. gdje je počinitelj *Storm-0558*, kineska hakerska grupa koja je špijunažno motivirana, iskoristila propust u Microsoftovom kodu [49, 50]. Microsoftov izvještaj rezultata istraživanja [51] navodi da je korisnički sustav za potpisivanje ključa nakon pada sustava u travnju 2021. zabilježio sva stanja te zapisao i ključ, iako je trebao biti redaktiran/cenzuriran. Nakon pada je sustav bio prebačen u okruženje za otklanjanje pogrešaka koje je bilo povezano na korporativnu mrežu te nakon kompromitiranja računa Microsoftovog zaposlenika, Storm-0558 je uspio pronaći ključ u tom razvojnom okruženju. Microsoft navodi da zbog velike potražnje za aplikacije koje rade za privatne i poslovne korisnike je uveo krajnju točku (eng. *endpoint*) koja je povezivala poslovne i privatne servise. Servis je bio proširen i sa ograničenjima valjanosti ključa, ali radi loše implementacije servis nije provjeravao ograničenje ključa tako da je ključ za privatne korisnike mogao biti korišten za poslovne subjekte i podatke [51, 52]. Žrtve su bile odjeli ministarstva Amerike koji su ujedno i prijavili čudne pristupe e-mailovima.

Ovaj incident je primjer loše konfiguracije te lošega upravljanja pristupom.

2.22. Retool (2023)

Retool, softverska kompanija, je imala ciljanu krađu identiteta (eng. *spear phishing*) [53, 54, 55]. Napadač je koristio svoje znanje internog načina poslovanja, odveo je zaposlenika na lažnu *Okta* domenu pod krinkom problema otvorenog upisa (eng. *open enrollment*). Napadač se prezentirao kao zaposlenik unutar IT tima koristeći *deep-fake* glas te tražio žrtvu da napravi drugi token za višefaktorsku autentifikaciju. Pošto Googlove politike oko upravljanja višefaktorskim kodovima omogućava da napadač dobije sve kodove prilikom povezivanja s Cloud spremištem sjemena (eng. *seed*), napadač je uspio doći do svih kodova za resurse (VPN i interni administratorski sustav) te ukrao kriptovalute u vrijednosti od 15 milijuna američkih dolara.

Ovaj incident je primjer usmjerene krađe identiteta. Moglo bi se i reći da je ovo manjak sigurnosti s Cloudove strane jer Cloud ima nesigurnu politiku oko čuvanja sjemena višefaktorske autentifikacije [55].

2.23. Microsoft (Midnight Blizzard, 2023)

U studenom 2023. je ruski APT (Advanced Persistent Threat) Midnight Blizzard uspio ući u zastarjeli, neprodukcijski, testni račun [56]. Račun nije imao višefaktorsku autentifikaciju i imao je slabu zaporku. Kompromitirani račun je imao ovlasti pristupiti malom dijelu korporativnih e-mail adresa koji uključuju viši, rukovodeći tim, zaposlenike u kibernetičkoj sigurnosti i legalnom odjelu [57]. Napadači nisu uspjeli doći do korisničkih podataka i informacija.

Ovaj incident je primjer loše higijene zaštite sigurnosti računa.

2.24. Football Australia (2024)

Nacionalno upravno tijelo za sport, Football Australia, je imala javno dostupan S3 spremnik s nešifriranim, identificirajućim, osobnim podacima, informacije o kupcima karata, internom infrastrukturom, izvornim kodom digitalne infrastrukture te skriptama digitalne infrastrukture. Pristupni ključ za spremnike je bio tvrdo kodiran u službenu stranicu i dostupan svima [58, 59].

Ovaj incident je primjer tvrdo kodiranih osjetljivih podataka, loše konfiguriranoga servera te ne mijenjanje pristupnih ključeva.

3. Cyber Conflict Simulator

Cyber Conflict Simulator (CCS) je platforma koja je namijenjena uvježbavanju odgovora na kibernetičke napade. CCS razvija UTILIS d.o.o., u razvoju je pomogao Fakultet elektrotehnike i računalstva (FER) gdje je FER davao svoju istraživačku potporu u domeni kibernetičke sigurnosti. Odlika CCS-a je da radi na apstraktnijoj razini. Nema tehničkih detalja, odnosno ne implementira tehničke detalje. Svi "tehnički detalji" su apstraktirani na način da urednik scenarija (engl. *Scenario editor*) određuje što se može iskoristiti i što mu je potrebno prije toga, zatim rezultat ovisi o zadovoljenim preduvjetima. Neki od tehničkih detalja bi bili programi i njihove opcije, nema programa poput *nmap* sa svojim dodatnim opcijama za skeniranje - apstraktirano u radnju *Network Scan*, alata *John the Ripper* za testiranje i napadanje zaporki - apstraktirano u radnju *Crack Passwords*. Svi alati su zapravo apstraktirani u svoju namjenu, *Login Remote* može se spojiti na sve u simulacije ako ima zadovoljene preduvjete (nema različitih programa poput PuTTy, WinSCP, Xshell 7, itd.), *Exploit Software* je apstraktirano na način da ne trebamo tehnički napraviti da je program ranjiv na propuste u pravom svijetu (krađa kolačića sesije, slabe zaporke, itd.).

Također, sve radnje su opisane koliko vremenski traju ili brzina odvijanja (ili oboje) pa se brzina cijele simulacije može mijenjati. Ovo je korisno jer imaju poslovni objekti koji imaju fiksno radno vrijeme te se pomoć ne može pružiti van radnog vremena. Drugim riječima, bilo kakav pomak ili radnja se ne može ostvariti ako ne rade. Zatim, duge operacije poput forenzike računala, prijenos računala s jedne fizičke lokacije na drugu, ažuriranje programa i operativnih sustava, traženje pomoći od vanjskih suradnika i sl. se simulira te se može ubrzati kako bi se uštedilo vrijeme na efektivnim (poučnim) dijelovima scenarija.

Svi elementi u simulaciji su virtualni, točnije svaki element (računalo, ljudi, opera-

tivni sustav, programi, datoteke i ostalo) je simuliran. Svaki element ima svoj set oznaka koji ga opisuje, dodavanjem oznaka otvara nove opcije za element, od dodatnih radnji nad njim do novih načina eksploatacije.

Još jedna velika prednost CCS-a je što omogućava simulaciju zaposlenika. Ovo je velika stvar jer ako zaposlenici trebaju sudjelovati u simulaciji, onda kompanija ima dodatne izdatke jer zaposlenici ne zarađuju kompaniji sredstva u trenutku simulacije, a kompanija troši novce na njihovu obuku za simulaciju te vrijeme provedeno unutar simulacije. Zaposlenici bi trebali proći još obuku nakon simulacije da shvate gdje su pogriješili te kakve te pogreške imaju posljedice te gdje se još kriju opasnosti što je očekivani trošak nakon simulacije.

CCS se izvodi u internetskom pregledniku (engl. *internet browser*). Podijeljen je na dvije vrste izvođenja. Prva vrsta je *Editor*, u kojem se razvija okolina simulacije. Druga vrsta je *Simulator*, u kojem se izvodi napravljena simulacija. Prijavom u CCS, korisnik je automatski u pogledu Simulator te klikom na bilo koju simulaciju će se odvijati sljedeći niz opcija kao što je opisano niže u potpoglavlju 3.2. Gumb *Go to Editor* služi za prebacivanje u *Editor* način i nalazi se u gornjem desnom kutu, ispod gumba za odjavu.

3.1. Editor

Imamo 3 opcije stvaranja novog scenarija. Prva opcija je na temelju Excel datoteke, ali cloud opcije nisu još podržane u Excel načinu unosa te radi toga ne rade i neće se objašnjavati. Druga opcija je ako imamo zapakiranu zip datoteku simulacije. Treća opcija je kreiranje novog scenarija od početka. Kod treće opcija, trebamo unijeti naziv scenarija, vrijeme održavanja te opis. Vrijeme održavanja služi samo za početak odvijanja simulacije i nema razlike odabere li se neko vrijeme u prošlosti ili budućnosti.

Osnovni elementi *Editor*-a su podijeljeni u 4 područja. To su: *gornji panel*, *donji panel*, *lijevi panel* i *radna površina*.

Gornji panel sadrži gumb za mijenjanje pogleda, *Global landscape* je pogled koji ima voditelj scenarija i sadrži sve elemente, klikom na njega vidjet ćemo sve moguće poglede igrača koje smo kreirali. Promjenom pogleda, možemo dozvoliti igraču da ima početno znanje o tuđim elementima (zna da postoji web stranica organizacije, zna da organizacija

postoji i slično) na način da mu dodamo simulirani element, isto tako možemo micati početno znanje igrača (zna da postoji organizacija, ali ne zna još fizičku lokaciju organizacije) micanjem atributa elementa. Gumb do njega, *Edit player* služi za promjenu informacija o igraču, poput imena, organizacije, onemogućavanje pristupa (eng. *disabled*) te dodavanja svih elemenata igraču s odgovarajućom organizacijom. Sljedeći po redu element je *New player* kojim se dodaje igrač, preporučava se dodati igrača tek na kraju jer se neće automatski osvježiti stanje dodavanjem novih elemenata igraču. Nužan i najčešće korišten gumb je *New Item*, koristi se za stvaranje novog simuliranog objekta. Odabirom seta oznaka (eng. *Labels*) određujemo kakva će njegova uloga biti. Ako želimo dodati računalo, odabiremo oznaku *Machine*, automatski će se dodati i oznake *Operating System* i *Asset*. Oznaka *Asset* kaže da se simulirani element može prenijeti, radi toga ima fizičku lokaciju. Oznaka *Operating System* proširuje element atributima *Software patch date*, *Software version* i *Software info*. Kombinacija 3 navedena atributa se koristi za određivanje može li se operativni sustav iskoristiti prilikom pokretanja malicioznog programa. Zatim *New Label* i *New Attribute* su opcije za razvojne programere, preporučeno je ne koristiti ih te nije bila potrebna za ovu demonstraciju. *New Toolbox Item* je gumb koji će imati funkcionalnost u budućim verzijama programa, zasada je nepotreban. *New Shared Object* je gumb kojim omogućavamo kreiranje kopije grupacije elemenata koje možemo koristiti u svim ostalim simulacija po principu *povuci i ispusti* (eng. *drag and drop*). Ovo je napredna opcija, preporučena je iskusnim korisnicima CCS-a jer se lagano može dogoditi greška na način da propustimo kopirati element koji je nužan za rad drugom elementu. *New Trigger Expression* je skripta koja omogućava korisniku da na temelju preduvjeta objekata obavijesti igrača o određenim informacija, primjer bi bio antivirusni program je našao sumnjivu datoteku na računalu. *New Indicator* je funkcionalnost koja omogućava promatračima i voditelju scenarija (potencijalno i igračima) kako se kreću određeni indikatori performansi. To mogu biti u obliku numeričke vrijednosti, na primjer gubitak izražen u valuti; grafa, koliko je računala ili servisa raspoloživo, onesposobljeno ili slično. Zatim nam slijede gumbi za učitavanje simulacije na server, spremanje promjena te skidanje simulacije na naše računalo. *Action Localization* je za napredne korisnike i omogućava prijevod radnji na proizvoljan jezik. Zadnja dva gumba omogućavaju pregled i izmjenu informacija o scenariju.

Donji panel se sastoji od dvije kartice, *Errors* i *Warnings*. *Errors* kartica označava

probleme u kojima bi simulator mogao nepredvidljivo reagirati, obično na način da se simulacija zaustavi te ne može nastaviti dok se ne riješi problem. *Warnings* kartica označava potencijalne probleme na način da njihovo postojanje možda utječe na odvijanje simulacije na način da će simulacija nastaviti raditi, ali nećemo imati traženi utjecaj.

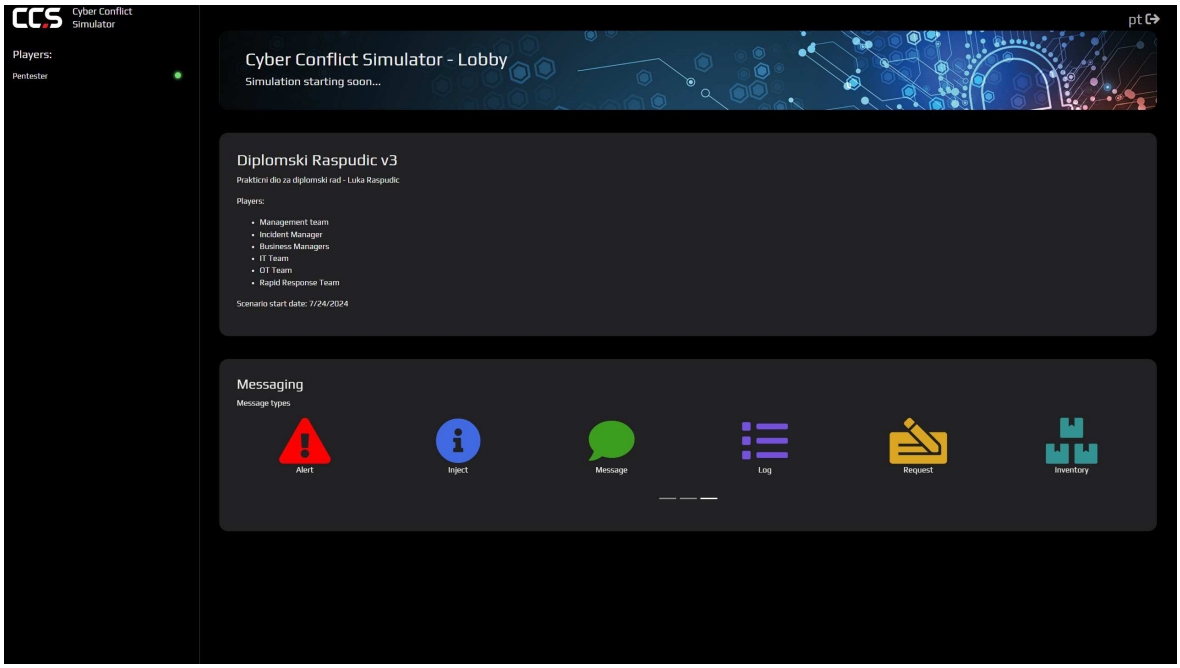
Lijevi panel sadrži sljedeće elemente: *Toolbox*, *Objects*, *Shared Objects*, *Labels*, *Attributes*, *Trigger Expressions* i *Indicators*. Postoji i dodatan element *Selected Objects* koji se prikaže kada se označi više elemenata, inače nije vidljiv. *Toolbox* sadrži grupacije elemenata koji su bili prethodno korišteni u drugim scenarijima i spremili smo ih pomoću opcije *New Shared Object*. Svi elementi sadrže spremljene atribute iz prethodnih scenarija, atributi se mogu mijenjati ako je potrebno. *Objects* sadrži sve simulirane elemente u scenariju, moguće je napraviti pretragu čime omogućava lakši pronalazak i izmjenu. *Shared Objects* se razvija i nije još za korištenje. *Labels* i *Attributes* su gumbi za razvojne programere i ne preporuča se njihovo korištenje. *Trigger Expressions* gumb omogućava prikaz svih skripti koje su kreirane u simulaciji i olakšava njihovu izmjenu. *Indicators* gumb prikazuje sve kreirane indikatore, također olakšava izmjenu.

3.2. Simulator

Prilikom pokretanja simulatora, voditelj simulacije (engl. *Game master*) će odrediti korisnička imena i lozinke za igrače. Pokretanjem simulacije će se igrači moći prijaviti s odgovarajućim vjedajnicama. Zatim će se svi igrači staviti u predsoblje (eng. *lobby*) dok simulacija ne počne. Izgled predsoblja se može vidjeti na slici 3.1. Simulacija kreće kada voditelj simulacije klikne na start čime počinje teći vrijeme.

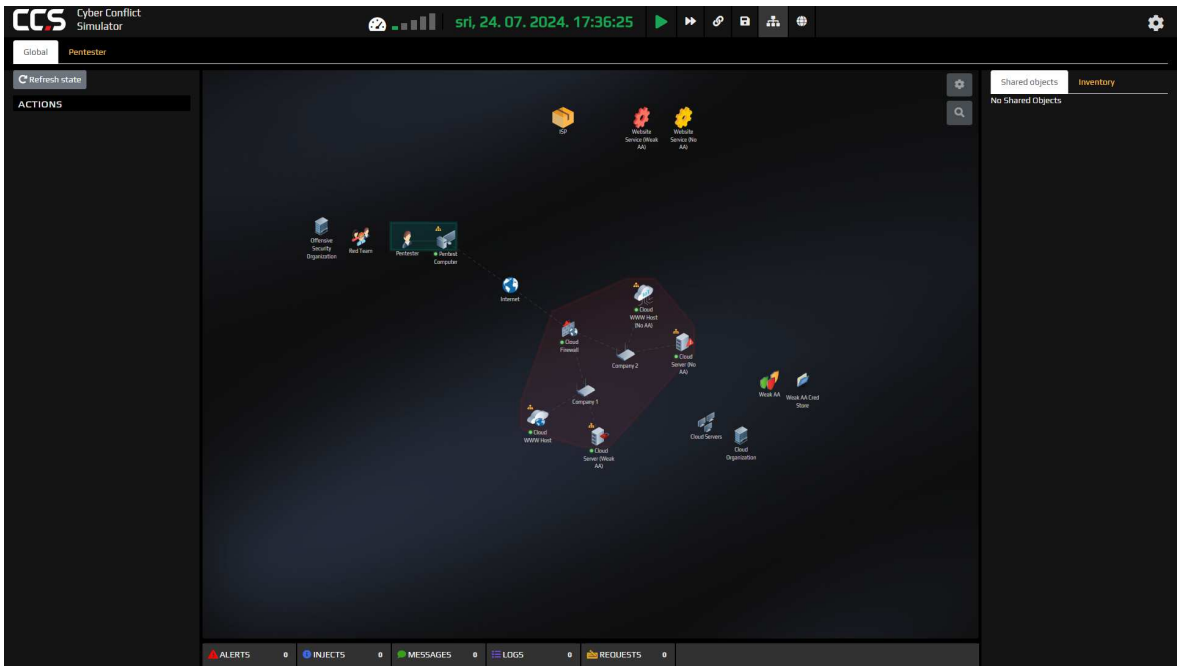
Na početku simulacije, svaki igrač vidi svoju "stranu" simulacije. To su elementi poput računala, mreža, lokacija, simuliranih zaposlenika, organizacije i slično. S lijeve strane ima popis mogućih opcija. S napadačke strane, neke od mogućih radnji su: *Blackmail*, *Exploit Software*, *Network Scan*, *Recon*. Važno je napomenuti da se u *Editoru* indirektno daju igraču radnje preko znanja (eng. *skills*). U ovom slučaju, igrač ima znanja o administraciji računala (eng. *System administration*), ofenzivi (eng. *Offensive*) i skupljanju informacija (eng. *Intelligence gathering*).

Izgled simulacije s voditeljeve strane se može vidjeti na slici 3.2. Za početak, voditelj

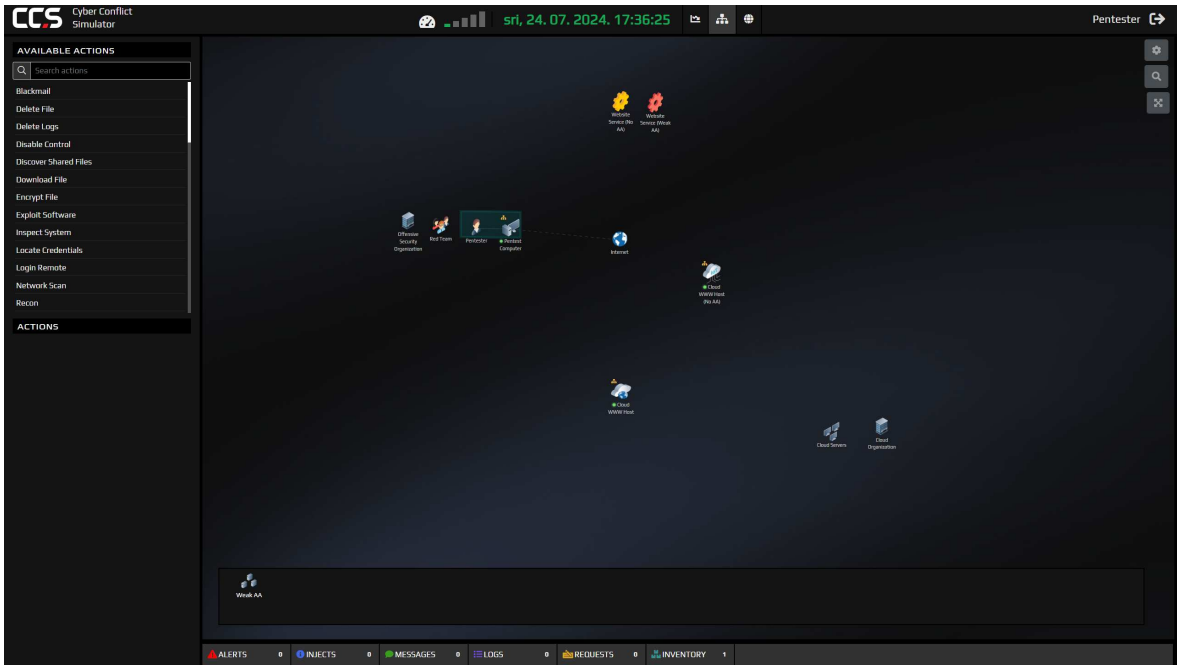


Slika 3.1. Predsoblje u CCS-u

simulacije vidi cjelokupnu sliku simulacije, odnosno sve elemente. Ima opciju promijeniti perspektivu klikom na igrača (poveznica *Pentester*) u gornjem lijevom kutu. Nema dozvoljenih radnji, ali vidi sve radnje koje su odradili svi igrači. U gornjem panelu mogu se vidjeti opcije upravljanja simulacije, prva opcija je upravljanje brzinom vremena (pravokutnici nalik na jačinu signala pored vremena). Najmanji pravokutnik je 1 sekunda u pravom svijetu je 1 sekunda simuliranog vremena. Drugi pravokutnik je 1 sekunda u pravom svijetu je 1 minuta simuliranog vremena, treći pravokutnik je 1 sekunda u pravom svijetu je 10 minuta simuliranog vremena, zatim 1 sekunda u pravom svijetu je 30 minuta simuliranog vremena i posljenja opcija je 1 sekunda u pravom svijetu je 1 sat u simuliranom vremenu. S desne strane vremena se mogu vidjeti opcije redom: pokretanje/zaustavljanje toka vremena, preskakanje simulacije na proizvoljni datum i vrijeme, dijalog za nastavak od spremljenih trenutaka tokom prošlih simulacija, spremanje trenutnog stanja simulacije, pregled grafa simulacije (trenutni pogled) te otvaranje mapu planet Zemlje kako bi mogli vidjeti gdje se nalaze svi simulirani elementi i igrači.



Slika 3.2. Voditeljeva perspektiva tokom simulacije



Slika 3.3. Igračeva (pentester) perspektiva tokom simulacije

4. Teorija

U ovom poglavlju se razrađuje ideja za praktični dio. U praktičnom dijelu je zamisao bila prikazati pronađene incidente iz pravog svijeta, radi ograničenja platforme CCS, ovo poglavlje je podijeljeno u dva potpoglavlja. Radi jednostavnosti, incidenti su se sveli na 2 situacije opisane u potpoglavljima. Prvo potpoglavlje je idealni scenarij, drugo potpoglavlje je implementacija idealnog scenarija te načini zaobilaska ograničenja.

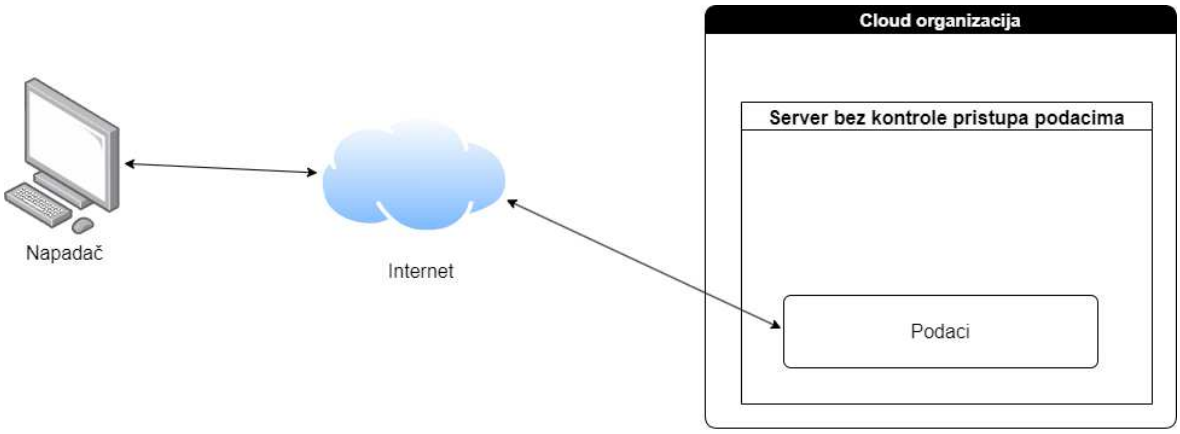
4.1. Idealni scenarij

Zamišljena su dva praktična primjera. Prvi primjer je napravljen tako da obuhvaća pogrešno konfigurirane servere. Primarno servere koji su bili javno dostupni bez ikakve autorizacije, na primjer curenje podataka (eng. *data leak*). Ideja je poprilično jednostavna, imamo server koji se nalazi unutar Cloud servisa i nema nikakvu zaštitu. Napadač koji ne bi smio moći pristupiti podacima, nalazi server na internetu te ulazi bez poteškoća. Shema se može vidjeti sa slike 4.1.

Metoda napada bi bila da napadač skenira servis, pronađe bazu podataka koja ima pristup internetu, pokuša pristupiti, uspije te preuzme podatke.

Drugi scenarij je zamišljen kao primjer gdje su kompanije imale loše prakse upravljanja sigurnosti. To mogu biti: jednostavne zaporke bez višefaktorske autentifikacije, tvrdo kodirani osjetljivi podaci u javno dostupnim kodovima/informacijama, trajni pristupni ključevi, korišten nezakrpani, zastarjeli kod ili proboj podataka (eng. *data breach*). Uglavnom, scenariji u kojima su napadači uložili trud da iskoriste propuste.

Metoda napada bi bila da napadač nađe ranjivost u internetskom servisu (aplikaciji), otkrije pristup serveru, pokuša pristupiti serveru, ne uspije jer nema vjerodajnice, izvrši napad grubom silom, uspije te dođe do podataka. Shema za drugi scenarij je prikazana



Slika 4.1. Prvi idealni scenarij

na slici 4.2.

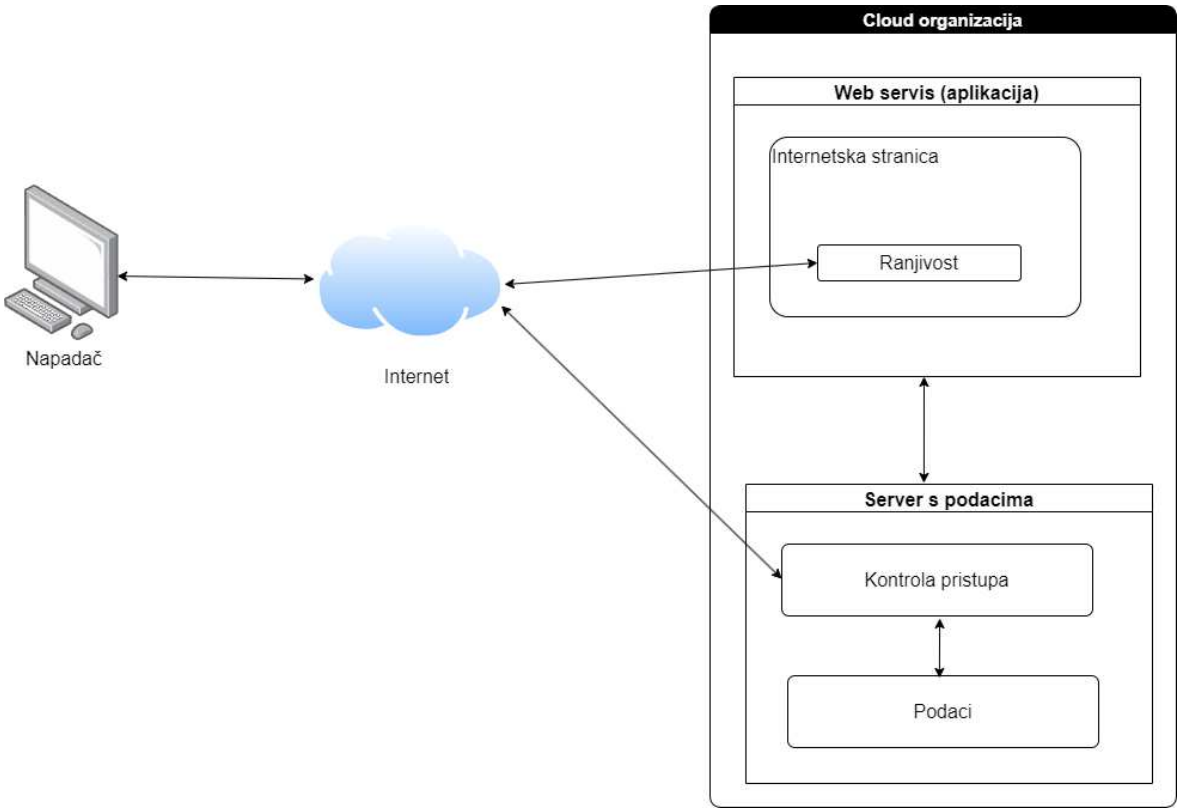
4.2. Implementacija

U ovom poglavlju objašnjavamo kako smo došli do praktičnog scenarija na temelju idealnog scenarija. Prvo, CCS je napravljen za kompanije i vojsku, nije imao na umu proširenje za Cloud servise, tako da već u startu nismo mogli imati jednostavnu topologiju na koju samo dodajemo opcije koje trebamo. Za početak, topologija se može vidjeti na slici 4.3.

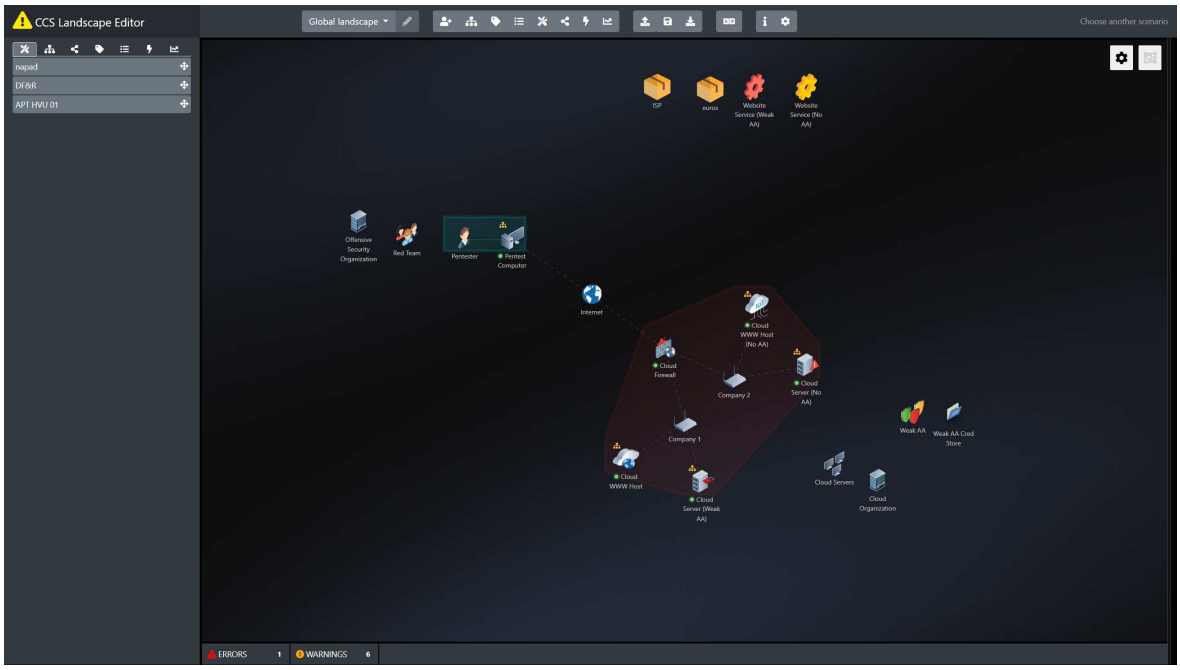
Igrač se nalazi u zelenom području, a kompanije koje treba testirati unutar crvenog područja. Scenarij je napravljen tako da u jednom scenariju obuhvaća obje teorijske simulacije. Ovdje su 3 organizacije, prva organizacija je kompanija koja nudi penetracijska testiranja aplikacija, druga organizacija je Cloud i treća je internet. Internet je treća organizacija jer treba biti neutralna, ako je na nečijoj strani onda mijenja pogled koji ta organizacija ima. Neutralnim načinom sve organizacija imaju dozu neznanja protivnika.

Unutar Clouda se mogu vidjeti zone povjerenja (eng. *trust zones*). Zona povjerenja se može smatrati kao podmreža (eng. *subnet*), fizička uloga bi bila preklopnik (eng. *switch*). Vatrozid (eng. *Firewall*) je nužan kao prvi kontakt s internetom, druga namjena je kontrolirat tok podataka. U vatrozidu su napravljena pravila tako da nema razmjene podataka između zona povjerenja *Comapany 1* i *Company 2*. To je napravljeno da napad na jedan scenarij ne utječe na drugi scenarij.

Može se vidjeti da obje kompanije imaju različita računala za internetsku aplikaciju i



Slika 4.2. Drugi idealni scenarij



Slika 4.3. Topologija implementacije

bazu podataka. Razlog je kontroliran način testiranja i provođenja. Također, u trenutku pravljenja scenarija, nije bilo dovoljno materijala za opis rada sustava, upute su objašnjavale što testni scenarij (nije povezan s ovim radom) ima te kako ga napraviti. Nije bilo dodatnih informacija poput kakve rezultate možemo dobiti promjenom testnih postavki tako da sve ideje su trebale biti testirane metodom pokušaja i pogrešaka. U početku nije bila jasna ideja oznake *File System*, nije ni bilo poznato može li računalo imati više atributa *File System* što je po prvotnoj pretpostavci bilo da ne može, prekasno se saznalo da može. Nakon toga se nije htjelo pokušavati jer bi se stvarali novi, nepotrebni problemi kao i cijela promjena scenarija.

Company 1 ima sigurnost, ali loše postavljenu. Ima internetsku aplikaciju nazvanu *DogLovers* koja ima ranjivost. Ranjivost je namjerno apstraktna jer možemo reći da ima bilo koju od navedenih u potpoglavlju 4.1. za Scenarij 2. Ima i grupu za vjerodajnice koja se nalazi na računalu na kojem se nalazi internetska aplikacija. CCS sve elemente fizički simulira te se one moraju negdje nalaziti. CCS ne dozvoljava da mi imamo napad na zaporke direktno na server, nego je to napad na simulirani fizički element. Bila je odluka staviti grupu za vjerodajnice na servera s podacima ili na server s aplikacijom. Odlučeno je na server s aplikacijom jer bi teže omotali glavu oko napada na zaporke kada smo već kompromitirali server s podacima.

Company 2 je prvi scenarij u idealnom scenariju 4.1. *Company 2* nema nikakve autorizacije, bazi podataka svi mogu pristupiti i pročitati podatke. Iako je baza podataka javno dostupna, napadaču je malo otežano, ne vidi ju odmah te se treba potruditi naći ju da bi joj pristupio.

5. Praktični dio

Praktični dio je zamišljen kao *Capture the Flag* (CTF) vježba. Na serverima *Cloud Server (No AA)* i *Cloud Server (Weak AA)* se nalaze datoteke koje imaju ulogu osjetljivih podataka pod nazivima *CTF on Cloud Server (No AA)*, odnosno *CTF on Cloud Server (Weak AA)*. Igrač pobjeđuje kada dođe do obje datoteke.

5.1. Scenarij bez autorizacije

Prvi napad možemo podijeliti u više faza. Podjelom na faze će biti lakše shvatiti napad u CCS-u jer da bi dobili jedan rezultat, u CCS-u ćemo trebati napraviti više akcija.

Prva faza je otkrivanje ranjivosti, odnosno pronalazak servera. Server ćemo pronaći tako da ćemo naći propust u internetskoj stranici kompanije *Company 2*. Radnjom *Exploit Software* s opcijama *Pentest Computer* za izvorište (eng. *Source*), opcijom *Exploit* s vrijednosti *Apache Exploit v2 (Pentest Computer)* i opcijom meta (eng. *Target*) s vrijednosti *Cloud WWW Host (No AA)* se možemo praviti da smo pronašli vjerodajnice.

Druga faza je otkrivanje lokacije servera, to možemo odraditi radnjom *Login Remote*, *Source* je *Pentest Computer*, *Target* je *Cloud WWW (No AA)*, *Account* je *default Admin acc* i *Protocol* je *http:80* te radnjom *Login Remote*, *Source* s vrijednosti *Pentest Computer*, *Target* s vrijenosti *Cloud WWW (No AA)*, *Account* s vrijednosti *default Admin acc* i *Protocol* s vrijednosti *http:80* te radnjom *Network Scan* s opcijama: *Source - Cloud WWW Host (No AA)*, *Target - Cloud Organization*, *Speed - Insane*, *Port - all* te *Level of details - L3*. Ovime sada znamo lokaciju servera. Preostaje nam ući u server.

Posljednja faza je pokušaj ulaska u server. Pošto *Cloud Server (No AA)* nema nikakvu autorizaciju svatko tko može pristupiti serveru, može pristupiti i podacima. Pokrećemo akciju *Login Remote* s opcijama *Source - Pentest Computer*, *Target - Cloud Server (No AA)*,

Account - default Admin acc te *Protocol - http:80*. Sada trebamo saznati ima li išta važno na serveru, to radimo opcijom *Inspect System* s opcijom *Machine - Cloud Server (No AA)*. Na kraju radnje ćemo saznati da ima neka datoteka, točnije *CTF on Cloud Server (No AA)*. Sada preostaje da skinemo datoteku, to radimo opcijom *Download File* s opcijama: *Source - Cloud Server (No AA)*, *Target - Pentest Computer*, *File - CTF on Cloud Server (No AA) (Cloud Server (No AA))*, *Speed - 10* (proizvoljna brzina), *Protocol - http:80*.

Gornjim scenarijem u tri faze i puno više koraka (radnji) smo uspjeli ući u nezaštićeni server i dohvatili podatke što označava kraj scenarija.

5.2. Scenarij s autorizacijom

Drugi napad ćemo isto podijeliti u više faza. Kompanija *Company 2* ima bolji sigurnosni sustav te prethodni princip neće proći i morat ćemo utrošit više truda i akcija.

U prvoj fazi ćemo figurativno pronaći ranjivost u internetskoj stranici. To ćemo napraviti radnjom *Exploit Software*, ali ovaj put je drugi zlućudni kod. Opcije su: *Source - Pentest Computer*, *Exploit - WP exploit (Pentest Computer)*, *Target - Cloud WWW Host*. Radi jednostavnosti, u CCS-u je zlućudnom kodu *WP exploit (Pentest Computer)* dano više funkcija. Jedna od funkcija je preuzimanje računala, odnosno automtski se radi *Login Remote* radnja.

Druga faza nam započinje traženjem servera radnjom *Network Scan* sa servera internetske stranice te možemo zamisliti da u ranjivosti ima, opet, mrežna adresa servera s podacima. Radnju *Network Scan* pokrećemo s opcijama: *Source - Cloud WWW Host (Weak AA)*, *Target - Cloud Organization*, *Speed - Insane*, *Port - all* te *Level of details - L3*. Sada smo dobili informacije o serveru kompanije *Company 1*.

Treća faza je pokušaj prijavljivanja u server s podacima, isto kao i u prethodnom scenariju. Prijavljivanje radimo radnjom *Login Remote* s opcijama *Source - Pentest Computer*, *Target - Cloud Server (Weak AA)*, *Account - default Admin acc* te *Protocol - http:80*. Ovdje ćemo dobiti negativan rezultat, odnosno neuspješnu prijavu.

Četvrta faza je pokušaj napada grubom silom. Pošto CCS ne omogućava da direktno napadnemo računalo, moramo napasti simuliranu grupu korisničkih računa. Njih ćemo

tražiti radnjom *Locate Credentials* s opcijama *Machine - Cloud WWW Host*. Po završetku ćemo dobiti informaciju da je pronađen *Credential Store*. Sada preostaje namjera prvotna namjera ove faze, napad grubom silom radnjom *Crack Passwords* s opcijama *Machine - Cloud WWW Host* i *Data - Weak AA Cred Store (Cloud WWW Host)*.

Peta faza je uspješan napad grubom silom što simuliramo radnjom *Login Remote* s opcijama: *Source - Pentest Computer Target - Cloud Server (Weak AA) Account - admin@cloud Protocol - http:80*.

Šesta faza je skidanje podataka što simuliramo radnjama *Inspect System* s opcijom *Machine - Cloud Server (Weak AA)* kojom saznajemo da ima datoteka i radnjom *Download File* s opcijama: *Source - Cloud Server (Weak AA)*, *Target - Pentest Computer*, *File - CTF on Cloud Server (Weak AA) (Cloud Server (Weak AA))*, *Speed - 10* (proizvoljna brzina) i *Protocol - http:80*.

Dohvaćanje datoteke označava kraj drugog scenarija.

6. Zaključak

Ovim radom smo proučavali sigurnost Cloud usluga. Iz navedenih incidenata smo mogli vidjeti da su gotovo svi incident rezultati pogrešaka razvojnih timova kompanija. Cloud pruža dobru zaštitu ako se implementiraju sigurnosne preporuke, ali isto stoji i za servere koje kompanija udomljava i servisira kada se poštuju sigurnosne preporuke. Čini se da je najveći problem manjak znanja novih tehnologija.

Gledajući trend, Cloud usluge postaju sve zastupljenije čime će se povećati broj ranjivih servisa ako razvojni timovi ne nauče na tuđim greškama ili počnu učiti iz dobrih izvora [60]. Cloud tehnologija ima velika očekivanja, prema istom izvoru 94% kompanija u svijetu koristi na neki način Cloud usluge, a prema izvoru [61], 60% svih korporativnih podataka se nalazi u Cloudu.

Iz incidenata se može vidjeti da ranjivosti Cloud usluga malo proširuje set ranjivosti aplikacija. Cloud je dodao još mogućnost napada pristupnim ključem što je vjerodajnica u suštini. Drugi primjer je problem čuvanja sjemena višefaktorske autentifikacije.

Iz praktičnog dijela se može vidjeti da je CCS moćna platforma za uvježbavanje odgovora na kibernetičke napade. Ima više pozitivnih strana nego negativnih i još kada se uzme u obzir da se konstantno nadograđuje, moglo bi se reći da bi CCS trebao postati standard uvježbavanja. Naravno, CCS ima još dosta opcija koje nisu dotaknute u ovom radu te koliko se brzo napravi vježba uz Excel datoteku za kompaniju koja ima stotine, tisuće računala i zaposlenika, može se reći da CCS ima svijetlu budućnost.

Literatura

[1] W. Contributors, “Uber”, Wikipedia, pristupano 4.9.2024.

[2] M. Gaddy, “Uber breaches (2014 & 2016)”, Breaches.cloud, pristupano 4.9.2024. URL: https://www.breaches.cloud/incidents/uber/

[3] M. Dinzeo, “Hacker details plot to breach Uber’s data servers”, Courthousenews.com, pristupano 4.9.2024. URL: https://www.courthousenews.com/hacker-details-plot-to-breach-ubers-data-servers-at-trial/

[4] “Codespaces (2014)”, Breaches.cloud, 2023., pristupano 4.9.2024. URL: https://www.breaches.cloud/incidents/codespaces/

[5] “Hacker puts ’full redundancy’ code-hosting firm out of business”, Computerworld, 2014., pristupano 4.9.2024. URL: https://www.computerworld.com/article/1394982/hacker-puts-full-redundancy-code-hosting-firm-out-of-business.html

[6] M. Gaddy, “BrowserStack”, Breaches.cloud, pristupano 4.9.2024. URL: https://www.breaches.cloud/incidents/browserstack/

[7] Wikipedia Contributors, “Shellshock (software bug)”, Wikipedia, 2024., pristupano 4.9.2024. URL: https://en.wikipedia.org/wiki/Shellshock_%28software_bug%29

[8] “Vitagene”, 2023., pristupano 4.9.2024. URL: https://www.breaches.cloud/incidents/vitagene/

[9] L. M. Khan-Chair, R. K. Slaughter, i A. M. Bedoya, “Complaint”, pristupano 4.9.2024. URL: https://www.breaches.cloud/incidents/vitagene/complaint.pdf

[10] ——, “Complaint”, pristupano 4.9.2024. URL: https://www.breaches.cloud/incidents/vitagene/complaint.pdf

[11] “DataDog (2016)”, Breaches.cloud, 2023., pristupano 5.9.2024. URL: https://www.breaches.cloud/incidents/datadog-2016/

[12] “Datadog forces password reset following breach”, Threatpost.com, 2016., pristupano 5.9.2024. URL: https://threatpost.com/datadog-forces-password-reset-following-breach/119179/

[13] “Tested techniques for preventing cloud attacks on your system”, 2023., pristupano 5.9.2024. URL: https://www.hornetsecurity.com/en/blog/cloud-attacks/

[14] “Data of almost 200 million voters leaked online by GOP analytics firm”, 2017., pristupano 5.9.2024. URL: https://money.cnn.com/2017/06/19/technology/voter-data-leaked-online-gop/index.html?iid=EL

[15] “The RNC Files: Inside the Largest US Voter Data Leak | UpGuard”, 2017., pristupano 5.9.2024. URL: https://www.upguard.com/breaches/the-rnc-files

[16] “LA Times Cryptomining”, 2023., pristupano 5.9.2024. URL: https://www.breaches.cloud/incidents/latimes/

[17] “Cryptojacking Attack Found on Los Angeles Times Website”, 2018., pristupano 5.9.2024. URL: https://threatpost.com/cryptojacking-attack-found-on-los-angeles-times-website/130041/

[18] “Chegg (2018)”, 2023., pristupano 6.9.2024. URL: https://www.breaches.cloud/incidents/chegg/

[19] “Cisco webex”, 2023., pristupano 5.9.2024. URL: https://www.breaches.cloud/incidents/cisco-2020/

[20] “San Jose Man Sentenced To Two Years Imprisonment For Damaging Cisco’s Network”, 2020., pristupano 5.9.2024. URL: https://www.justice.gov/usao-ndca/pr/san-jose-man-sentenced-two-years-imprisonment-damaging-cisco-s-network

[21] “UNITED STATES’ SENTENCING MEMORANDUM”, 2020., pristupano 5.9.2024. URL: https://www.breaches.cloud/incidents/cisco-2020/ramesh-sentencing.pdf

[22] “Ex-Cisco Employee Pleads Guilty to Deleting 16K Webex Teams Accounts”, 2020., pristupano 5.9.2024. URL: https://threatpost.com/ex-cisco-employee-pleads-guilty-to-deleting-16k-webex-teams-accounts/158748/

[23] “Imperva RDS Snapshot”, 2023., pristupano 5.9.2024. URL: https://www.breaches.cloud/incidents/imperva-rds-snapshot/

[24] “Cybersecurity Firm Imperva Discloses Breach”, 2019., pristupano 5.9.2024. URL: https://krebsonsecurity.com/2019/08/cybersecurity-firm-imperva-discloses-breach/

[25] “Data Warehouse: How a Vendor for Half the Fortune 100 Exposed a Terabyte of Backups”, 2019., pristupano 5.9.2024. URL: https://www.upguard.com/breaches/attunity-data-leak

[26] “What happened with the CAM4 Data Leak?” 2020., pristupano 5.9.2024. URL: https://teampassword.com/blog/what-happened-with-the-cam4-data-leak

[27] “CAM4 adult cam site leaked 11B database records including emails, private chats”, 2020., pristupano 5.9.2024. URL: https://securityaffairs.com/102776/data-breach/cam4-data-leak.html

[28] “CAM4 Data Leak Exposes Personal Data of Millions of Users”, 2020., pristupano 5.9.2024. URL: https://www.bitdefender.com/blog/hotforsecurity/cam4-data-leak-exposes-personal-data-of-millions-of-users/

[29] “First republic bank”, 2023., pristupano 5.9.2024. URL: https://www.breaches.cloud/incidents/first-republic/

[30] “Cloud engineer gets 2 years for wiping ex-employer’s code repos”, 2023., pristupano 5.9.2024. URL: https://www.bleepingcomputer.com/news/security/cloud-engineer-gets-2-years-for-wiping-ex-employers-code-repos/

[31] “Criminal complaint”, 2021., pristupano 5.9.2024. URL: https://www.breaches.cloud/incidents/first-republic/gov.uscourts.cand.375169.1.0_1.pdf

[32] “Drizly (2020)”, 2023., pristupano 5.9.2024. URL: https://www.breaches.cloud/incidents/drizly/

[33] “Alcohol delivery service drizly hit by data breach”, 2020., pristupano 5.9.2024. URL: https://techcrunch.com/2020/07/28/drizly-data-breach/

[34] “Ubiquiti (2020)”, 2023., pristupano 5.9.2024. URL: https://www.breaches.cloud/incidents/ubiquiti/

[35] “Ex-Ubiquiti engineer behind ’breathtaking’ data theft gets 6-year prison term”, 2023., pristupano 5.9.2024. URL: https://arstechnica.com/tech-policy/2023/05/ex-ubiquiti-engineer-behind-breathtaking-data-theft-gets-6-year-prison-term/

[36] “GOVERNMENT’S SENTENCING MEMORANDUM REGARDING DEFENDANT NICKOLAS SHARP”, 2023., pristupano 5.9.2024. URL: https://cdn.arstechnica.net/wp-content/uploads/2023/05/US-v-Sharp-Sentencing-5-11-2023.pdf

[37] “UNC2903”, 2023., pristupano 5.9.2024. URL: https://www.breaches.cloud/incidents/unc2903/

[38] “Old Services, New Tricks: Cloud Metadata Abuse by UNC2903”, Google Cloud Blog, 2022., pristupano 6.9.2024. URL: https://cloud.google.com/blog/topics/threat-intelligence/cloud-metadata-abuse-unc2903/

[39] “LA Times Cryptomining”, 2023., pristupano 5.9.2024. URL: https://www.breaches.cloud/incidents/lastpass/

[40] “LastPass says employee’s home computer was hacked and corporate vault taken”, 2023., pristupano 5.9.2024. URL: https://arstechnica.com/information-technology/2023/02/lastpass-hackers-infected-employees-home-computer-and-stole-corporate-vault/

[41] “Experts Fear Crooks are Cracking Keys Stolen in LastPass Breach – Krebs on Security”, 2023., pristupano 5.9.2024. URL: https://krebsonsecurity.com/2023/09/experts-fear-crooks-are-cracking-keys-stolen-in-lastpass-breach/

[42] “Incident 1 – Additional details of the attack”, 2023., pristupano 6.9.2024. URL: https://support.lastpass.com/s/document-item?language=en_US&bundleId=lastpass&topicId=LastPass/incident-1-details.html&_LANG=enus

[43] “Incident 2 – Additional details of the attack”, 2023., pristupano 6.9.2024. URL: https://support.lastpass.com/s/document-item?language=en_US&bundleId=lastpass&topicId=LastPass/incident-2-details.html&_LANG=enus

[44] “CommuteAir”, 2023., pristupano 6.9.2024. URL: https://www.breaches.cloud/incidents/commuteair/

[45] “U.S. No Fly list shared on a hacking forum, government investigating”, 2023., pristupano 6.9.2024. URL: https://www.bleepingcomputer.com/news/security/us-no-fly-list-shared-on-a-hacking-forum-government-investigating/

[46] “EXCLUSIVE: U.S. airline accidentally exposes ‘No Fly List’ on unsecured server”, 2023., pristupano 6.9.2024. URL: https://www.dailydot.com/debug/no-fly-list-us-tsa-unprotected-server-commuteair/

[47] “Cloud misconfiguration causes massive data breach at Toyota Motor”, 2023., pristupano 6.9.2024. URL: https://www.csoonline.com/article/575483/cloud-misconfiguration-causes-massive-data-breach-at-toyota-motor.html

[48] “Apology and Notice Concerning Newly Discovered Potential Data Leakage of Customer Information Due to Cloud Settings | Corporate | Global Newsroom | Toyota Motor Corporation Official Global Website”, 2023., pristupano 6.9.2024. URL: https://global.toyota/en/newsroom/corporate/39241625.html

[49] “Microsoft (Storm-0558)”, Breaches.cloud, 2023., pristupano 6.9.2024. URL: https://www.breaches.cloud/incidents/o365-2023/

[50] “Compromised Microsoft Key: More Impactful Than We Thought”, wiz.io, 2023., pristupano 6.9.2024. URL: https://www.wiz.io/blog/storm-0558-compromised-

microsoft-key-enables-authentication-of-countless-micr

[51] “Results of Major Technical Investigations for Storm-0558 Key Acquisition | MSRC Blog | Microsoft Security Response Center.” Microsoft.com, 2023., pristupano 6.9.2024. URL: https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

[52] “Compromised Microsoft Key: More Impactful Than We Thought”, wiz.io, 2023., pristupano 6.9.2024. URL: https://www.wiz.io/blog/storm-0558-compromised-microsoft-key-enables-authentication-of-countless-micr

[53] “Retool MFA”, Breaches.cloud, 2023., pristupano 6.9.2024. URL: https://www.breaches.cloud/incidents/retool-mfa/

[54] “Retool blames breach on Google Authenticator MFA cloud sync feature”, BleepingComputer, 2023., pristupano 6.9.2024. URL: https://www.bleepingcomputer.com/news/security/retool-blames-breach-on-google-authenticator-mfa-cloud-sync-feature/

[55] “When MFA isn’t actually MFA | Retool Blog | Cache”, retool.com, 2023., pristupano 6.9.2024. URL: https://retool.com/blog/mfa-isnt-mfa

[56] “When MFA isn’t actually MFA | Retool Blog | Cache”, Breaches.cloud, 2024., pristupano 6.9.2024. URL: https://www.breaches.cloud/incidents/o365-2024/

[57] “Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard | MSRC Blog | Microsoft Security Response Center”, Microsoft.com, 2024., pristupano 6.9.2024. URL: https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

[58] “Football Australia leak exposes players’ details”, Cybernews, 2024., pristupano 6.9.2024. URL: https://cybernews.com/security/football-australia-leak-expose-players/

[59] “Football Australia”, Breaches.cloud, 2024., pristupano 6.9.2024. URL: https://www.breaches.cloud/incidents/footballaustralia/

[60] “The Future is Now: How Companies are Using Cloud Computing in 2024”, Edge Delta, 2024., pristupano 7.9.2024. URL: https://edgedelta.com/company/blog/how-many-companies-use-cloud-computing-in-2024

[61] “25 Amazing Cloud Adoption Statistics [2023]: Cloud Migration, Computing, And More”, Zippia, 2023., pristupano 8.9.2024. URL: https://www.zippia.com/advice/cloud-adoption-statistics/

Sažetak

Emulacija napadača na usluge u oblaku za potrebe penetracijskog testiranja

Luka Raspudić

Ovaj rad se bavio sigurnosti Cloud usluga, na temelju incidenata zabilježenih na internetu te njihovih zapisa o propustima, shvatiti koliki opseg ranjivosti je s pružateljeve strane, a koliki opseg s krivoga korisničkoga korištenja. Na temelju pronađenih incidenata napravljene su simulacije pomoću platforme Cyber Conflict Simulator (CCS). Apstraktniji način rada CCS-a omogućava da se incidenti prokuhaju na dva slučaja. Prvi scenarij je napad na server bez autentifikacije i autorizacije, a drugi scenarij je napad na server sa slabom autentifikacijom. Rezultati su pokazali da je Cloud usluga sigurna, a najslabija točka je razvojni tim s prečacima koji se suprostavljaju sigurnosnim preporukama. Mogući razlog je neznanje tehnologije (važnost pristupnog ključa, javno dostupna postavka) što je veliki propust za bilo koju tehnologiju.

Ključne riječi: emulacija; napadanje; penetracijsko testiranje; CCS; Cyber Conflict Simulator; oblak;

Abstract

Emulating attackers on cloud services for penetration testing

Luka Raspudić

This paper's purpose was to address security of Cloud services by analyzing incidents found on the internet, to understand the magnitude of flaws from provider's side to client's wrongful use. Based on the incidents found, simulations were made with the help of Cyber Conflict Simulator (CCS) platform. By functioning on the more abstract level, CCS allows the inscidents to boil down into two scenarios. The first scenario is an attack on a server without authentication and authorization, and a second scenario is an attack on a server with weak authentication. The results showed that Cloud services are secure, the weakest link is the development team with cutting corners that are against safety recommendations. A possible reason is a lack of understanding how Cloud technology operates (importance of access keys, publicly available setting) which is a significant flaw for any technology.

Keywords: emulating; attack; penetration testing; CCS; Cyber Conflict Simulator; Cloud;