Slika, ki vsebuje besede steklenica, oblikovanje, cerkev

Opis je samodejno ustvarjen

Projekt

**ThreatInsight**

**Povzetek**

**projekta**

Naredil:

**Aljaž Bračko**

22. April, 2024

Vsebina

[1. OZADJE PROJEKTA 1](#_Toc164717039)

[1.1. Opis Projekta 1](#_Toc164717040)

[1.2. Cilji projekta 1](#_Toc164717041)

[1.3. Namen 1](#_Toc164717042)

[2. PODROČJE PROJEKTA 2](#_Toc164717043)

[2.1. Kibernetska Varnost in Faza Izvidništva (Footprinting & Reconnaissance) 2](#_Toc164717044)

[2.2. Aktivnosti v Fazi Izvidništva 2](#_Toc164717045)

[2.3. Namen Izvidništva v etičnem hekanju 3](#_Toc164717046)

[3. Obseg projekta in omejitve projekta 4](#_Toc164717047)

[4. Izdelki projekta 5](#_Toc164717048)

[4.1. Končna Android aplikacija: 5](#_Toc164717049)

[4.2. Uporabniška dokumentacija: 5](#_Toc164717050)

[4.3. Baza podatkov: 6](#_Toc164717051)

[4.4. Tehnična dokumentacija in navodila: 6](#_Toc164717052)

[5. Pričakovana kakovost projektnih rezultatov 7](#_Toc164717053)

[6. Identificirana prva prepoznana tveganja za izvajanje projekta 8](#_Toc164717054)

[7. Okvirno določen časovni vidik projekta 9](#_Toc164717055)

# OZADJE PROJEKTA

## Opis Projekta

Ta projekt bo spletna aplikacija, ki integrira več orodij in storitev za kibernetsko varnost, z namenom zagotavljanja celovitega pregleda nad kibernetskimi "tarčami" kot so Google, UM, ciljna podjetja itd. Aplikacija omogoča uporabnikom, da zberejo, shranijo in analizirajo podatke o različnih entitetah za boljše razumevanje potencialnih ranljivosti in izboljšanje etičnih hekerskih praks.

## Cilji projekta

Glavni cilj projekta je ustvariti uporabniku prijazno platformo, ki združuje različna orodja za zbiranje informacij in analizo podatkov o določenih tarčah v kibernetskem prostoru.

**Ta integrirana rešitev bo uporabnikom omogočila:**

* Učinkovitejše izvidništvo in skeniranje omrežij.
* Boljšo pripravljenost na obrambo pred potencialnimi kibernetskimi grožnjami.
* Spremljanje in analizo stanja tarč skozi enotno in intuitivno uporabniško vmesnik.

## Namen

Projekt se izvaja z namenom, da se zmanjša kompleksnost procesov in orodij, potrebnih za kibernetsko varnost, ter da se uporabnikom omogoči lažji dostop do ključnih informacij, ki lahko pripomorejo k boljši pripravljenosti in odzivnosti na kibernetske incidente. Cilj je, da aplikacija postane centralno središče za etične hekerje, penetracijske testerje in IT administratorje za izvajanje različnih varnostnih preverjanj in analiza. Ob enem pa bi tudi radi zmanjšali časovne stroške pri fazi izvidništva etičnega hekanja.

# PODROČJE PROJEKTA

## Kibernetska Varnost in Faza Izvidništva (Footprinting & Reconnaissance)

Kibernetska varnost je široko področje, ki se ukvarja z zaščito sistemov, omrežij in programov pred digitalnimi napadi. Ti napadi so običajno namenjeni (nedovoljenemu) dostopu, spreminjanju ali uničevanju/kraji občutljivih informacij. Implementacija učinkovitih kibernetskih varnostnih rešitev je zato ključna za preprečevanje izgub informacij, denarja in ugleda.

**Faza Izvidništva**

Ena izmed ključnih začetnih faz v kibernetski varnosti, še posebej v etičnem hekanju, je faza izvidništva, znana tudi kot footprinting ali reconnaissance. To je prva faza vsakega etičnega hekerskega dela, kjer se zbira čim več informacij o tarči pred dejanskim napadom. Ta faza je pomembna za uspešno načrtovanje in izvedbo varnostnih ukrepov, saj pomaga identificirati možne vhodne točke in ranljivosti v sistemu tarče.

## Aktivnosti v Fazi Izvidništva

1. **Zbiranje Informacij:** Zbiranje javno dostopnih informacij o tarči. Tukaj govorimo o informacijah o domeni, IP naslovih, informacijah o zaposlenih, lokaciji podjetja in drugih javno dostopnih podatkih.
2. **Skeniranje Omrežja:** Uporaba orodij kot je nmap za določanje aktivnih naprav na omrežij, identifikacija operacijskih sistemov, uporabljenih programskih paketov in konfiguracij vrat.
3. **Podrobnejše informacije:** Po skeniranju sledi zbiranje podrobnejših informacij o posameznih napravah, kot so uporabniška imena, skupine, role in druge specifike sistema.
4. **Izkoriščanje javnih virov:** Iskanje informacij v podatkovnih bazah kot so WhoIs, HaveIBeenPwned in druge spletne storitve, ki lahko razkrijejo informacije o preteklih varnostnih incidentih, registraciji domen in podobno.
5. **Geolokacijska Analiza:** Določitev geografske lokacije tarče na podlagi IP naslovov za dodatno identificiranje možnih fizičnih varnostnih tveganj.
6. **Varnostni Pregledi:** Preverjanje konfiguracije TLS/SSL certifikatov in DNSSec postavitev za oceno transportne in domenske varnosti.

## Namen Izvidništva v etičnem hekanju

Namen izvidništva v etičnem hekanju je identificirati in dokumentirati potencialne vhodne točke in ranljivosti, ki jih lahko kasneje varnostne ekipe odpravijo. Pripraviti podlago za nadaljnje faze testiranja penetracij, ki bodo sledile. Z zbiranjem podatkov o tarči, etični hekerji pomagajo organizacijam razumeti njihove varnostne luknje in pripraviti boljše obrambne strategije.

# Obseg projekta in omejitve projekta

Projekt "ThreatInsight" je zasnovan kot rešitev, ki bo na voljo kot spletna aplikacija. Aplikacija bo v (prijaznem za uporabo) uporabniškem vmesniku vsebovala nabor orodij in storitev za izvidništvo, ki uporabnikom omogočajo zbiranje, shranjevanje in analizo podatkov o izbranih tarčah.

**Omejitve:**

* **Uvoz/Izvoz Podatkov:** Projekt ne bo omogočal uvoza in izvoza datotek, ki bi vsebovale zgodovinske podatke o varnostnih pregledih ali izvidniških aktivnostih, kot so logi nmap skeniranja ali izvoz analiz WhoIs. Ta omejitev je postavljena za zagotovitev, da se uporabniki osredotočajo na trenutne informacije in zmanjšanje tveganj povezanih z zlorabo podatkov.
* **Funkcionalnosti Napadov:** V skladu z etičnimi normami in pravnimi zahtevami, projekt ne bo vključeval orodij ali funkcionalnosti, ki bi omogočale izvedbo dejanskih kibernetskih napadov, kot so DDoS napadi, izkoriščanje ranljivosti ali infiltracija zlonamerne programske opreme. Vsa orodja in funkcionalnosti bodo omejene na pasivno zbiranje podatkov in analizo.
* **Promocija Rešitve:** Projekt ne vključuje aktivnosti povezanih s trženjem ali promocijo aplikacije, saj je fokus izključno na razvoju in izboljšanju tehničnih funkcionalnosti.

# Izdelki projekta

## Končna spletna aplikacija:

Končna spletna aplikacija bo spletna verzija "ThreatInsight", ki bo omogočala uporabnikom dostop do vseh funkcionalnosti projektne rešitve. Aplikacija bo vključevala:

* **Moduli za Skeniranje, Analizo in Poročanje:** Uporabniki bodo lahko izvajali skeniranje omrežij, iskanje podatkov z orodji, preverjanje izpostavljenosti, shranjevanje izvidništva, ustvarjanje zaznamkov.
* **Interaktivni Vmesnik:** Uporabniški vmesnik, ki omogoča enostavno navigacijo med različnimi funkcionalnostmi.
* **Varnostne Funkcije:** Vključene bodo varnostne funkcije za zaščito uporabniških podatkov in integritete aplikacije.

## Uporabniška dokumentacija:

Uporabniška dokumentacija bo set dokumentov, ki bodo uporabnikom pomagali razumeti in učinkovito uporabljati aplikacijo.

Vključevala bo:

* **Navodila in pogoje za začetek pporabe:** Korak-po-korak vodiči za uporabo aplikacije in začetne nastavitve.
* **Opisi Funkcionalnosti:** Podrobni opisi vseh funkcij aplikacije s primeri uporabe za boljše razumevanje.
* **FAQ in Odpravljanje Težav:** Seznam pogostih vprašanj in težav z rešitvami, ki uporabnikom pomagajo pri morebitnih problemih.

## Baza podatkov:

Projekt bo razvit z bazo podatkov, ki bo hranila vse zbrane in obdelane podatke. Baza podatkov bo vključevala:

* **Učinkovito Shranjevanje Podatkov:** Struktura za hitro shranjevanje in dostop do informacij.
* **Varnost:** Uporaba tehnik šifriranja in varnostnih protokolov za zaščito podatkov pred nepooblaščenim dostopom.

## Tehnična dokumentacija in navodila:

Projekt bo vseboval sledeče tehnične dokumente:

* **Specifikacije Zahtev Programske Opreme (SZPO):** Podroben dokument, ki opisuje tehnične zahteve in specifikacije za razvoj in delovanje aplikacije.
* **Diagram Primerov Uporabe (DPU):** Vizualni prikazi arhitekture aplikacije, funkcionalnosti in interakcij med uporabniki in sistemom, ki pomoč pri razumevanju delovanja aplikacije.
* **Dodatni Vizualni Pripomočki:** Različni diagrami in skice, ki pomagajo pri razvoju in razumevanju projekta.

# Pričakovana kakovost projektnih rezultatov

**Kakovostne Zahteve in Standardi:**

1. **Funkcionalnost Aplikacije:**

* Aplikacija mora brezhibno izvajati vse načrtovane funkcionalnosti, kot so opisane v dokumentaciji za funkcionalne zahteve (SZPO).
* Vse funkcionalnosti morajo biti preverjene z testiranjem. (testiranje enote, integracijski testi in sistemski testi)

1. **Uporabniški Vmesnik:**

* Uporabniški vmesnik mora biti enostaven za uporabo za vse ciljne skupine uporabnikov.
* Design in navigacija aplikacije morata omogočati uporabnikom, da z minimalnim usposabljanjem dostopajo do vseh funkcionalnosti.

1. **Varnost:**

* Aplikacija mora upoštevati varnostne standarde, kamor spada uporaba tehnik šifriranja in varnostnih protokolov za zaščito uporabniških podatkov.

1. **Zmogljivost:**

* Aplikacija mora biti optimizirana za hitro delovanje, tudi ko obravnava velike količine podatkov ali veliko število sočasnih uporabnikov.
* Čas odziva aplikacije ne sme presegati določenih mejnih vrednosti, ki bodo določene in testirane.

1. **Dokumentacija in podpora:**

* Pričakuje se, da bo na voljo ustrezna dokumentacija za uporabo aplikacije.
* Zagotovitev tehnične podpore v primeru težav ali vprašanj s strani uporabnikov.

1. **Skladnost s Pravilniki in Zakonodajo:**

* Vsi projektni izdelki morajo biti v skladu z relevantnimi lokalnimi, nacionalnimi in mednarodnimi pravnimi zahtevami, vključno z zakonodajo o zasebnosti podatkov.

# Identificirana prva prepoznana tveganja za izvajanje projekta

Identificiranje in upravljanje tveganj je pomembnega pomena za uspešen potek projekta. Prva prepoznana tveganja so:

* **Bolezni/odsotnost:** Odsotnost vodilnih akterjev pri razvoju, lahko vpliva na časovni okvir dostave izdelka ali dostavo izdelka onemogoči.
* **Varovanje Podatkov in Zasebnost:** Možnost varnostnih groženj in tveganj za varovanje osebnih podatkov uporabnikov. Potreba po skladnosti z zakonodajo o varstvu podatkov in zahtevami glede zasebnosti.
* **Primanjkljaj sredstev:** Pomankanje časa ali kvalitete, povečanje stroškov razvoja, neomogočen dostop do orodij.
* **Zunanji Vplivi:**Naravne nesreče, politični dogodki ali drugi zunanji dejavniki, ki bi lahko vplivali na razvoj ali dostopnost aplikacije.
* **Tehnična tveganja:** Nepričakovane tehnične ovire ali težave pri programiranju, ki bi lahko privedle do zamud v razvojnem procesu.

# Okvirno določen časovni vidik projekta

Projekt "ThreatInsight" bo sledil določenemu časovnemu načrtu za zagotavljanje, da so vse faze projekta zaključene pravočasno. Celotna dolžina razvoja projekta bo 7 tednov, pri čemer se pričakuje, da bo vsak član projektnega tima delal po 5 ur na dan, od ponedeljka do petka.

**Podrobni Časovni Načrt:**

* **Teden 1-2:** Planiranje in definicija projekta, začetno zbiranje zahtev in izdelava začetnih specifikacij.
* **Teden 3-4:** Razvoj osnovne funkcionalnosti in prvih testiranj.
* **Teden 5:** Integracija dodatnih funkcionalnosti in začetek obsežnejših testiranj.
* **Teden 6:** Dokončanje funkcionalnih testov, priprava na začetek produkcije.
* **Teden 7:** Finalizacija projekta, priprava uporabniške in tehnične dokumentacije, zaključna predaja in pregled projektne rešitve.