**Učna enota Projekt**

ITK / IPT UNI 3. Letnik

**Ekipa, ki predlaga projekt**

Ekipa praviloma šteje 3 člane/ice, izjemoma 2 ali 4.

|  |  |  |
| --- | --- | --- |
|  | **Naziv ekipe: ThreatInsight** | |
| **Član/ica** | **Ime in priimek** | **E-poštni naslov** |
| 1. | Aljaž Bračko | [aljaz.bracko@student.um.si](mailto:aljaz.bracko@student.um.si) |
| 2. | Teodor Verhovnik | [teodor.verhovnik@student.um.si](mailto:teodor.verhovnik@student.um.si) |
| 3. | Matevž Nerat | [matevz.nerat@student.um.si](mailto:matevz.nerat@student.um.si) |

**Projekt bo :**

* nadaljevanje našega projekta pri predmetu Praktikum II
* narejen na osnovi lastnega predloga
* rešitev na osnovi predlogov koordinatorjev (št. predloga: \_\_\_\_\_ )

|  |
| --- |
| Spletna aplikacija, ki bo na enem mestu ponujala več orodij/storitev kibernetske varnosti za zbiranje podatkov o »tarči«(Google, UM, ciljno podjetje,…), katere bo potem uporabnik shranil in o njih pridobil nasvete o stanju »tarče« oz. o možnih ranljivostih.  Uporabnik bo lahko ustvaril novo entiteto »podatki o tarči«, kjer bo izbiral med ponujenimi funkcionalnostmi orodij/storitev. Vsaka entiteta »podatki o tarči«, bi imela eno tarčo, kar bi predstavljalo lahek in skupen pregled informacij o »tarči« na enem mestu.  Orodja, ki jih bo rešitev ponujala so:   * nmap(skeniranje omrežnega stanja tarče –gostitelji, stanja gostiteljev, stanja vrat gostiteljev, OS,…), * WhoIs(pridobivanje podatkov o domeni/IP – datum ustvarjanja, imenski strežniki, registrar,…), * HaveIBeenPwned(vpogled ali so podatki tarče bili že kdaj izpostavljeni v vdoru in v katerem) * IpGeolocation(z vnosom IP naslova tarče, bo uporabnik dobil približno lokacijo tarče) * TLS/DNSSec scan(TLS informacije, DNSSec aktiviranost) * E-mail verifier(potrjevanje obstoja mailov oziroma iskanje mailov glede na domeno ali celoten naslov) * E-mail permutator(generiranje možnih phishing e-mail računov, glede na neke vnesene smernice)   Ob koncu zbiranja informacij o tarči, bo uporabnik lahko shranil pridobljene informacije, katere bo kasneje tudi dostopal ali spreminjal. Prav tako bo lahko pregledal/spreminjal vsa pretekla shranjena iskanja za tarče, ki jih je preiskoval v preteklosti(npr. informacije o Google-u, informacije o UM,…). Pridobljene pomembne informacije bodo vizualno predstavljene in podprte z jasnimi kratkimi razlagami. Ob pregledu »podatki o tarči«, bo lahko iz pridobljenih informacij o tisti tarči, dobil pregled možnih ranljivosti oziroma napotke o pristopu penetracijskega testiranja.  Cilj: Ustvariti spletno aplikacijo, ki združuje več orodij za kibernetsko varnost na enem mestu, omogočajoč uporabniku celovit pregled informacij o določeni tarči. S poudarkom na zbiranju, shranjevanju in analizi podatkov, bo naša rešitev omogočila uporabnikom učinkovito ocenjevanje stanja tarče iz pridobljenih informacij. Olajšanje dela uporabnikom v fazah etičnega hekanja: izvidništvo in skeniranje omrežja. |

**Vizija izdelka / storitve:**

**Podatki o izdelku / storitve**

|  |  |
| --- | --- |
| **Ključni uporabniki** | Penetracijski testerji, etični hekerji, administratorji |
| **Glavne funkcionalnosti**  (omejite se na funkcionalne zahteve, opremite s prioritetami) | Ustvarjanje profila, ustvarjanje/pregledovanje/urejanje/brisanje entitete »podatki o tarči«, uporaba orodij za pridobivanje podatkov entitete »podatki o tarči«:   * Uporaba nmap in prikaz/pregled rezultatov(možnost prilagajanja skeniranja(TCP skeni, OS zaznavanje, agresivnost,…) * Uporaba storitve WhoIs in prikaz/pregled (domena/ip, lastnik, gostovanje,…) * Uporaba orodja HaveIBeenPwned(vnos maila oz. gesla) in prikaz/pregled rezultatov * Uporaba storitve IpGeolocation(vnos IP/domene) in prikaz/pregled države, mesta, časovne cone, ISP ponudnika,.. * Uporaba storitve TLS/DNSSec in prikaz/pregled verzije šifriranja, certifikat, aktiviranost DNSSec * Uporaba storitve E-mail verifier in prikaz/pregled zaznanih e-mail naslovov oz. domen * Uporaba storitve E-mail permutator in prikaz/pregled generiranih e-mail naslovov   selekcija bistvenih podatkov, predvidevanje ranljivosti tarče iz izbranih bistvenih podatkov |
| **Glavne omejitve**  (npr. varnostne, performančne, omejitve okolja ipd.) | Pridobivanje podatkov nekaterih orodij je težavno in časovno potratno |
| **Meje izdelka / storitve**  (česar NE boste vključili) | Ne bomo vključili celotne varnostne analize aplikacije, razbijanja gesel, napadov na tarčo, podrobnih navodil izkoriščanja ranljivosti |
| **Uporabniški vmesnik(i)**  (npr. mobilni, spletni, namizni, API, konzolni ipd.) | Spletni uporabniški vmesnik |
| **Zahteve rešitve / storitve**  (npr. posebna strojna ali programska oprema, veljavna naročnina na storitve ipd. ) | Pridobivanje dostopa do API-jev(naročnine), odprtokodne rešitve |
| **Alternativne rešitve / storitve na trgu** | nmap.online, hackertarget.com, shodan.io, domsignal.com |
| **Konkurenčna prednost**  Zakaj bo predlagan izdelek /storitev za uporabnika boljši od obstoječih? | Na trgu so rešitve, ki omogočajo uporabo orodij, ampak brez možnosti ustvarjanja nekega stanja o tarči z pridobljenimi informacijami. |
| **Planirane integracije**  (npr. sistemi za overjanje, sistemi za shranjevanje vsebin na oblaku, napovednimi modeli v oblaku, zunanjimi viri podatkov ipd.) | Sistem za overjanje, API-ji orodij, model predvidevanja |
| **Zagotavljanje trajnosti podatkom**  (npr. relacijska baza podatkov, NoSql baza, blockchain platforma, PB v oblaku, trajnosti podatkov ne bo ipd.) | NoSQL baza |
| **Namestitev zaledja izdelka / storitve**  (npr. oblak - zabojniki, oblak - serverless, lasten strežnik, zalednega sistema ne bo.) | Oblak - serverless |
| **Plan organizacijskega vidik razvoja**  (uporabljena razvojna metoda – npr. Scrum, Kanban…; Uporabljeni standardi dokumentiranja – npr. UML ipd...) | Scrum, Jira, Github, SonarQube,…  UML(diagram primerov uporabe, komponentni diagram, flowchart, diagram varnosti aplikacijske arhitekture,…) |