# VAJA: Pasivni napadi poizvedovanja (ang. Reconnaissance) - OSINT

**Namen**

Namen te vaje OSINT je usposobiti udeležence za identifikacijo in analizo javno dostopnih informacij, s ciljem izboljšanja varnostnih strategij organizacije. Osredotoča se na razvoj veščin za prepoznavanje potencialnih ranljivosti in groženj z etično uporabo zbranih podatkov. Vaja poudarja pomen kritične analize in etičnih smernic v procesu zbiranja obveščevalnih informacij iz odprtih virov.

**Uvod**

Kratica OSINT označuje "Open Source Intelligence" (odprti viri obveščevalnih informacij). Namen OSINT je zbiranje, analiziranje in interpretacija informacij, ki so javno dostopne, kot so podatki na internetu, v javnih dokumentih, družbenih omrežjih, novicah itd. OSINT se uporablja v različnih kontekstih, vključno z varnostjo, obveščevalno dejavnostjo, poslovno analitiko, novinarstvom in raziskovalnim delom. Glavni cilj OSINT je pridobivanje koristnih informacij za podporo odločitvam, analizo tveganj, prepoznavanje trendov ali identifikacijo potencialnih groženj. Ker se osredotoča na javno dostopne vire, se šteje za etično in legalno metodo zbiranja informacij. Seveda pa potencialni napadalci to lahko s pridom izkoriščajo za pridobivanje informacij o podjetju, osebah zaposlenih v podjetju ter tehničnih vidikih omrežja.

- OSINT Framework (https://osintframework.com/): Strukturiran vodič po orodjih in virih za OSINT, ki ponuja organiziran pristop k iskanju javno dostopnih informacij.
- WhatsMyName (https://github.com/WebBreacher/WhatsMyName): Orodje za iskanje uporabniških imen preko različnih spletnih platform, ki pomaga pri identifikaciji digitalnih sledi oseb ali organizacij.odja in spletna mesta:
- Certificate Transparency logs (https://certificate.transparency.dev/): Ponuja vpogled v SSL/TLS certifikate, ki so javno objavljeni, pomagajoč pri identifikaciji in analizi spletnih strani.
- crt.sh (https://crt.sh/): Orodje za iskanje SSL/TLS certifikatov, ki omogoča pregled nad šifriranjem in varnostjo spletnih strani.

**Naloge:**

1. Zbiranje informacij na družbenih omrežjih.

Družbena omrežja so lahka tarča za pridobivanje informacij o posameznikih, ki so zaposleni v podjetjih. Podatki, ki jih pridobimo se lahko nanašajo na osebne podatke posameznika lahko pa tudi pridobimo tehnične podatke o sistemu katerega želimo napasti.

Kakšne informacije bi lahko pridobili na družbenih omrežjih?

Katera družbena omrežja lahko vsebujejo tehnične podatke?

Ali je teža pridobljenih podatkov odvisna od funkcije?

2. Orodje whois

Whois je orodje, ki nam omogoča pridobivanje informacij o domenskih imenih. Orodje lahko zaženemo iz ukazne vrstice Windowsa ali pa uporabimo spletno inačico.

V cmd-ju zaženite ukaz whois <ime_domene>. Preverite naslednje domene:

- www.ltfe.org
- www.google.com
- www.gov.si

Nato za iste domene preverite še podatke na spletni različici whois.

Kateri vsi podatki so vidni za posamezne domene?

Podatke o slovenski domenah preverite tudi na spletni strni register.si.

Ali register Slovenskih domen razpolaga z informacijami, ki so lahko škodljive?

3. Orodje Shodan

Spletna stran Shodan (https://www.shodan.io/) je specializirano orodje za iskanje in analizo naprav, povezanih v internet. Njen glavni namen je omogočiti uporabnikom, da poiščejo različne naprave, kot so strežniki, usmerjevalniki, kamere, pametne naprave in drugo, ki so povezane v svetovni splet. Shodan zbira in indeksira informacije o teh napravah ter omogoča uporabnikom iskanje po različnih parametrih, kot so vrsta naprave, odprti vrata, uporabljene protokole, geografska lokacija itd.

Poiščite kamero, ki se nahaja v Sloveniji in naredite analizo podatkov, ki jih Shodan vrača.

Poizkusite najti naprave, ki imajo privzeta gesla.

4. Orodje AbuseIPdb

AbuseIPdb (https://www.abuseipdb.com/) je spletno orodje, ki omogoča uporabnikom, da prijavijo zlonamerne IP naslove. Na spletni strni si lahko ogledamo statistiko za vse prijavljene IP naslove: kolikokrat so bili prijavljeni, kaj te IP naslovi izvajajo ter kje se nahajajo.

Oglejte si podatke za nekaj IP naslovov.

5. Orodje Mitre-CVE

https://www.cve.org/

6. Praktičen primer DNS rerouta

DNS reroute predstavlja napad kjer zakupljena domena kaže na drugo domeno. Ta domena je lahko zlonamerna lahko pa predstavlja izključno reroute na drugo domeno. Obiščite spletno strani aliexpress ter vtipkajte ključno besedno »laptop backpack«. Poiščite artikel, ki ima »ime« in ta artikel najdite v Sloveniji. S pomočjo whois ter register.si poiščite podatke o domenah.