Footprinting & Reconnaissance

Kaj je Reconnaissance?

Izvidništvo – zbiranje informacij o tarči, kar je prvi korak pri vsakem napadu na sistem

Svoje korenine ima v vojaških operacijah, kjer se izraz nanaša na cilj zbiranja informacij o sovražniku

Napadalcem pomaga zožiti obseg njihovih naporov in pomaga pri izbiri napadalnega orožja

Napadalci zbrane podatke uporabijo za izdelavo načrta (footprint) organizacije, ki jim pomaga izbrati najučinkovitejšo strategijo za ogrožanje varnosti sistema in omrežja

Izvidništvo pri etičnem hekanju

Podobno se ocena varnosti določenega sistema ali omrežja začne z izvidništvom

Etični hekerji in preizkuševalci penetracije (pen testers) morajo pred začetkom ocenjevanja zbrati dovolj informacij o cilju, ki ga ocenjujejo

Etični hekerji in pen testerji naj bi simulirali vse korake, ki jih napadalec običajno sledi, da dobijo boljšo predstavo o varnosti ciljne organizacije

Footprinting

Footprinting se nanaša na postopek zbiranja informacij o ciljnem omrežju in njegovem okolju, ki pomaga pri ocenjevanju varnostne drže informacijske infrastrukture ciljne organizacije

Pomaga tudi pri prepoznavanju stopnje tveganja, povezanega z javno dostopnimi informacijami organizacije

Tipi:

- Pasivno
- Aktivno

Footprinting - tipi

Pasivno

- Napadalec uporablja pasivne izvidniške tehnike, ne sodeluje neposredno s tarčo
- Namesto tega se napadalec zanaša na javno dostopne informacije, objave novic itd.
- Ta način se uporablja, kadar cilj ne sme zaznati zbiranja informacij

Footprinting - tipi

Aktivno

- Vključuje neposredne interakcije s ciljnim sistemom z uporabo orodij za odkrivanje odprtih vrat, dostopnih gostiteljev, lokacij usmerjevalnikov, kartiranje omrežja, podrobnosti operacijskih sistemov in aplikacij
- Pri tem načinu obstaja možnost, da se tarča zaveda zbiranja informacij

Cilji

Naučiti se varnostne „drže“ (security posture) – Analizirati varnostno držo cilja, poiskati luknje in ustvariti načrt napada

Določiti območje fokusa (focus area) – Z različnimi orodji in tehnikami zožiti obseg naslovov IP

Poiskati ranljivosti (vulnerabilities) – Zbrane informacije uporabiti za prepoznavanje pomanjkljivosti v varnosti ciljne organizacije

Zemljevid omrežja (network map) – Grafično predstaviti ciljno omrežje in ga uporabiti kot vodilo med napadom

Zbrane informacije

Informacije o organizaciji

- Informacije o zaposlenih
- Ozadje organizacije
- Telefonske številke
- Lokacije

Zbrane informacije

Informacije o sistemih

- Operacijski sistemi spletnih strežnikov
- Lokacije strežnikov
- Uporabniki
- Gesla

Zbrane informacije

Informacije o omrežju

- Domene
- Poddomene
- Naslovi IP
- Zapisi Whois in DNS

Kako pridobiti informacije?

Iskalniki in spletni viri

Whois, IP Geolocation, in DNS Interrogation

Email footprinting

Website footprinting

Kloniranje spletnih strani

Network footprinting

Iskalniki in spletni viri

Iskalniki se lahko uporabljajo za pridobivanje informacij o ciljni organizaciji

Rezultati iskanja lahko vključujejo informacije o zaposlenih v ciljni organizaciji, intranet, strani za prijavo in druge informacije, ki bi lahko bile koristne napadalcem

Eden od načinov zbiranja informacij s pomočjo iskalnikov je uporaba Google hacking techniques

Google hacking je tehnika, ki jo napadalci uporabljajo za zapleteno iskanje in pridobivanje pomembnih informacij o svojih ciljih

- Vključuje uporabo nabora iskalnih operatorjev in ustvarjanje zapletenih poizvedb
- Operaterji, ki se uporabljajo pri Google hacking, se imenujejo **dorks**

Whois, IP Geolocation, in DNS Interrogation

Whois - se nanaša na protokol za poizvedbe in odzive, ki se uporabljajo za pridobivanje informacij o dodeljenih internetnih virih

- Podatkovne baze Whois vsebujejo osebne podatke lastnikov domen in jih vzdržujejo regionalni spletni registri (Regional Internet Registers)

IP Geolocation – pomaga najti informacije o lokaciji cilja, kot so država, mesto, poštna številka, ponudnik internetnih storitev itd.

- S temi informacijami lahko hekerji izvajajo napade socialnega inženiringa

DNS Interrogation – se nanaša na zbiranje informacij o podatkih o območju DNS, kar vključuje informacije o ključnih gostiteljih v omrežju

- Orodja za DNS interrogation pomagajo napadalcem pri izvedbi DNS footprintinga
- Z uporabo teh orodij lahko napadalci pridobijo informacije o vrstah strežnikov in njihovih lokacijah

Email footprinting

Email footprinting se nanaša na zbiranje informacij iz e-pošte s spremljanjem dostave e-pošte ter ustreznih headerjev

Informacije, zbrane prek odtisa email footprinting, vključujejo:

- Naslov IP prejemnika
- Geolokacija prejemnika
- Podatki o dostavi
- Obiskane povezave
- Informacije o brskalniku in OS
- Čas branja

Prav tako je mogoče slediti elektronski pošti z različnimi orodji za sledenje. Orodja za sledenje e-pošte imajo možnost sledenja e-poštnim sporočilom in pregledovanja njihovih headerjev za pridobivanje koristnih informacij. Pošiljatelj je obveščen o prejetem in odprtem e-poštnem sporočilu.

Website footprinting

Tehnika, pri kateri se informacije o cilju zbirajo s spremljanjem ciljne spletne strani

Hekerji lahko preslikajo celotno spletno stran cilja, ne da bi bili opaženi

Website footprinting nam lahko da informacije o:

- Programski opremi
- Operacijskem sistemu
- Podimeniki (Subdirectories)
- Kontaktnih podatkih
- Skriptni platformi
- Podrobnosti poizvedbe (Query details)

Website footprinting

Dodatni načini za zbiranje informacij:

- Izvorna koda HTML – s preučitvijo izvorne kode HTML lahko iz komentarjev v kodi izvlečemo informacije in pridobimo vpogled v strukturo datotečnega sistema z opazovanjem povezav in slikovnih oznak
- Piškotki – lahko razkrijejo pomembne informacije o programski opremi, ki se izvaja na strežniku, in njenem vedenju
- Tudi z pregledovanjem sej je mogoče prepoznati skriptne platforme

Obstajajo programi, namenjeni pomoči pri odtisu spletnih strani. Ti programi se imenujejo spletni pajki in sistematično brskajo po spletnem mestu v iskanju določenih informacij. Tako zbrani podatki lahko napadalcem pomagajo pri socialnem inženiringu.

Kloniranje spletnih strani

Zrcaljenje ali kloniranje spletnih strani se nanaša na postopek podvajanja spletnega mesta

Zrcaljenje spletnega mesta pomaga pri brskanju določenega spletnega mesta brez povezave (offline), iskanju ranljivosti na spletnem mestu in odkrivanju dragocenih informacij

Spletna mesta lahko shranjujejo dokumente drugačne oblike, ki lahko vsebujejo skrite informacije in metapodatke, ki jih je mogoče analizirati in uporabiti pri napadu

Te metapodatke je mogoče pridobiti z različnimi orodji za pridobivanje metapodatkov in pomagajo napadalcem pri izvajanju napadov socialnega inženiringa

Network footprinting

Nanaša se na postopek zbiranja informacij o ciljnem omrežju

Med tem postopkom napadalci zbirajo informacije o območju omrežja in jih uporabljajo za preslikavo ciljnega omrežja

Obseg omrežja daje napadalcem vpogled v to, kako je omrežje strukturirano in kateri stroji pripadajo omrežju.

Orodja

Iskalniki in spletni viri

- OSINT framework - zbiranje informacij iz brezplačnih orodij ali virov
  - Vključuje preprost spletni vmesnik, ki vsebuje različna orodja OSINT, razporejena po kategorijah, in je prikazan kot drevesna struktura OSINT na spletnem vmesniku
- Google dorks – osnovni (težje dostopni) podatki
- Shodan – IoT naprave, OS
- HaveIbeenPwned – preverimo ali je določeno geslo ali uporabniško ime ogroženo
- PeekYou – podrobnejši podatki o osebi
- Netcraft – OS
- Censys – OS

Whois, IP Geolocation, in DNS Interrogation

- DomainTools (Whois Lookup)
- NSLOOKUP – DNS

Orodja

Email footprinting
- EmailTrackerPro – 15 dni trial
- Infoga – open source
- theHarvester – seznam emailov

Website footprinting
- Website informer – odkriva glavne konkurente spletnega mesta, razkrije strežnike DNS, pridobi Whois…
- Web Data Extractor – kontaktni podatki, URLji, meta tags…

Kloniranje spletnih strani
- HTTrack Web Site Copier

Network footprinting
- ARIN Whois database – Network range
- Network Tracerooting

Dodatno

Recon-ng – je spletno izvidniško ogrodje z neodvisnimi moduli in interakcijo z bazami podatkov, ki zagotavlja okolje, v katerem je mogoče izvajati odprtokodno spletno izvidništvo.

Maltego – orodje, ki se uporablja za zbiranje čim več informacij za namene etičnega vdiranja, računalniške forenzike in testiranja. Ponuja knjižnico transformacij za odkrivanje podatkov iz odprtih virov in jih vizualizira v obliki grafa, primerno za analizo povezav in rudarjenje podatkov. Ponuja grafični vmesnik, ki omogoča takojšen in natančen ogled teh odnosov in celo omogoča prikaz skritih povezav.

BillCipher - je orodje za zbiranje informacij za spletno mesto ali naslov IP. S tem orodjem lahko zbirate informacije, kot so iskanje DNS, iskanje Whois, iskanje GeoIP, iskanje podomrežja, Port Scanner, Page Links, HTTP header itd.