VAJA: Eksfiltracija podatkov z DNS

Namen

Demonstracija vaje eksfiltracije podatkov prek DNS temelji na analizi zajetih DNS zahtevkov. Cilj je prepoznati, kateri podatki so bili nepooblaščeno izneseni iz omrežja. DNS eksfiltracija je metoda, kjer napadalec kodira podatke v DNS poizvedbe, ki se nato pošljejo na zlonamerni strežnik. Kot analitik pregledujemo vzorce v zajetih poizvedbah, preverjamo neobičajne domene, dolge nize ali sumljivo frekvenco zahtevkov, da ugotovimo, kateri podatki so bili eksfiltrirani. Vaja ponuja vpogled v zaznavanje tovrstnih tehnik in krepitev varnostnih ukrepov.

Uvod

Eksfiltracija podatkov preko DNS je tehnika, pri kateri napadalci izkoriščajo DNS protokol za nepooblaščen prenos podatkov iz omrežja. DNS poizvedbe, ki so običajno namenjene prevajanju domenskih imen v IP naslove, omogočajo vključevanje poljubnih podatkov v poddomenah. S tem lahko napadalci kodirajo občutljive informacije, kot so gesla, ključi ali drugi podatki, in jih pošljejo na oddaljen strežnik, ki ga nadzorujejo.

Primer takšne tehnike je orodje **iodine**, dostopno na GitHubu, ki omogoča prenos podatkov preko DNS tuneliranja. Orodje deluje tako, da kodira podatke v DNS poizvedbe (npr. v poddomene), ki se nato pošiljajo na DNS strežnik, nastavljen s strani napadalca. Strežnik sprejme poizvedbe, dekodira podatke in omogoča njihovo rekonstrukcijo. Zaradi narave DNS prometa, ki je običajno dovoljeno v večini omrežij, je ta metoda težko zaznavna brez napredne analize.

V tej nalogi boste analizirali priloženo datoteko z zajetimi DNS zahtevki, da bi ugotovili, ali vsebujejo znake potencialne eksfiltracije podatkov, in identificirali, kateri podatki bi lahko bili preneseni. Naloga bo zahtevala pozornost do neobičajnih vzorcev v DNS poizvedbah, kot so dolge, nenavadne poddomene ali poizvedbe na sumljive domene.

Naloge:

V tej nalogi boste analizirali priloženo datoteko z zajetimi DNS zahtevki, pri čemer se sumi, da so napadalci s pomočjo DNS protokola eksfiltrirali datoteko. Vaša naloga je rekonstruirati končno datoteko, ki je bila prenesena iz omrežja.

cybersec.ltfe.org/vaje2/dns_requests.txt

1. **Razumevanje podatkov:**
    - Preglejte strukturo DNS poizvedb v priloženi datoteki.
    - Pozorni bodite na nenavadne poddomene, dolžine imen in frekvenco poizvedb, saj so to lahko znaki kodiranih podatkov.
2. **Identifikacija eksfiltriranih podatkov:**
    - S pomočjo vzorcev analizirajte, kako so lahko napadalci kodirali podatke v DNS poizvedbe (npr. base64, hex, binarni podatki).
    - Ugotovite, katere domene so bile uporabljene za eksfiltracijo.

3. **Rekonstrukcija datoteke:**
    - Iz pridobljenih informacij rekonstruirajte podatke, ki so bili preneseni.
    - Uporabite ustrezna orodja za dekodiranje in združevanje podatkov v celotno datoteko.
4. **Orodja za pomoč:**
    - Za analizo DNS poizvedb lahko uporabite orodja, kot so **Wireshark**, **tshark**, ali skripte v **Python-u** z uporabo knjižnic, kot so dnslib ali scapy.
    - Za dekodiranje podatkov uporabite orodja, kot so base64, xxd, ali binwalk.
5. **Končni rezultat:**
    - Ob zaključku naloge boste morali predložiti rekonstruirano datoteko in opisati korake, ki ste jih uporabili za identifikacijo in rekonstrukcijo.

Skozi nalogo upoštevajte metodologijo forenzične analize in poskrbite, da bo vaša dokumentacija omogočila ponovitev vaših korakov. Srečno pri analizi!