Ime in priimek: **Datum:**

Uvod v kibernetsko varnost

Namen vaje je:

- Spoznati črne luknje (primer: telescope.ltfe.org).
- Spoznati medene pasti (primer: cyber.ltfe.org).
- Se seznaniti z osnovami kibernetskega izvidništva.

Aktivne in pasivne tarče, kot so medene pasti (honeypots) in črne luknje (black holes) so ključnega pomena za spremljanje aktivnosti in strategij napadalcev, za oceno stopnje nevarnosti, ter za pripravo dobre obrambne strategije. Internetna črna luknja (ali internetni teleskop) je temno omrežje naslovov IP, ki še nikoli niso bili uporabljeni in na katere se ne sklicuje nobeno domensko ime. Vsaka dejavnost, ki jo je tam mogoče zaznati, je bodisi iskanje tarče s strani napadalca, bodisi odbit promet, ki je posledica večjih napadov drugje v internetu. Kibernetska past (honeypot) pa predstavlja aktivno storitev, ki zagotavlja dovolj interaktivnosti, da napadalca lahko preslepi, da gre za legitimno storitev, ki jo posledično lahko napade. Vzpostavitev učinkovitih in prilagodljivih pasti je še vedno velik izziv, vendar predstavlja osnovni mehanizem za spremljanje inicdentov z namenov izboljšanja ravni razumevanja napadalcev in njihovih tarč, ter prednostnih ranljivosti.

1. Naloga: omrežni teleskop

Uporabljenih 256 popolnoma svežih IP naslovov z enim samim namenom: pritegniti nepovabljen promet ter sistematično opazovati poskuse udorov.

Odpremo spletno stran: https://telescope.ltfe.org/

Vprašanja:

a) Koliko pregledov vrat je bilo v zadnjih 3h?

b) Katera vrata so bila največkrat podvržena pregledu?

c) Katere aplikacije privzeto uporabljajo ta vrata?

d) Kaj je smiselno storiti, če omrežje uporablja neko storitev (npr. SSH) in kaj če nekaterih vrat ne uporabljamo?

e) Komentirajte lokacije izvorov napadov.

2. Naloga: kibernetične pasti

Omrežje medenih pasti (angl. honeypots) z namenom izpostavitve aktivne storitve, ki zagotavlja dovolj interaktivnosti, da lahko napadalca preslepi, da gre za legitimno storitev, ki jo posledično lahko napade.

Odpremo spletno stran: https://cyber.ltfe.org/

Vprašanja:

a) Naštejte nekaj podatkovnih cetrov iz katerih izvira največ napadov?

b) Zapišite zadnjo sejo in komentirajte njen rezultat.

c) Koliko napadov v zadnjem mesecu je prišlo iz omrežja Telekoma Slovenije?

d) Koliko IP-jev Telekoma Slovenije smo detektirali in kolikšen procent to predstavlja?

e) Primerjajte aktivnosti IP-jev: 212.227.211.203 vs 217.160.9.187.

f) Katere zlonamerne datoteke je uporabil napadalec (IP: 74.208.69.80) in kaj počnejo?

g) Zapišite primer uporabe ene od datotek.

h) Na spletu obstaja več virov obveščevalnih podatkov o kibernetskih grožnjah, naštejte jih nekaj (vsaj 3).

i) Rezultate iz naloge 2.e primerjajte z informacijami na virih iz prejšnje naloge (2.h).

3. Naloga: kibernetsko izvidništvo (cyber passive reconnaissance)

Kibernetsko izvidništvo je prvi korak vsakega profesionalnega preizkusa penetracije. V tej fazi je cilj zbrati čim več informacij o cilju. To vključuje tehnične informacije o topologiji omrežja in sistemih. Vključuje pa tudi informacije o zaposlenih in samem podjetju, ki so lahko koristne v kasnejših fazah testa penetracije. Več informacij kot zberete med fazo izvidništva, večja je verjetnost, da boste uspeli v kasnejših fazah preizkusa penetracije.

a) S pomočjo spletnih iskalnikov izbrskajte čim več informacij o potencialni tarči IP: **212.101.174.100**.
   - Whois (who.is):
   - Shodan (www.shodan.io):
   - Zoomeye (https://www.zoomeye.org/):
   - Bing (www.bing.com)

b) Kateri server uporablja spletna stran?

c) Poiščite potencialne ranljivosti sistema (https://cve.mitre.org).

d) Poiščite potencialne avtorje spletne strani? Kako si lahko pomagamo s to informacijo?

4. Naloga: ali sem izpostavljen (haveibeenpwned)?

Haveibeenpwned.com je spletno mesto, ki uporabnikom interneta omogoča, da preverijo, ali so bili njihovi osebni podatki ogroženi zaradi zlorabe podatkov. Storitev zbira in analizira na stotine izpisov in lepljenja podatkovnih baz, ki vsebujejo informacije o milijardah razkritih računov.

a) Preverite ali se je vaš e-naslov pojavil zbirki.

b) Preverite ali se je vaša telefonska številka pojavila v zbirki.

c) Preverite ali se je katero od gesel, ki jih uporabljate. Se je kakšno pojavilo v zbirki? (Testirate lahko tudi kakšno staro geslo, ki ga sicer več ne uporabljate)

d) Podobno storitev ponuja chrome. Med shranjenimi gesli preverite katera so slaba? Koliko jih je?

5. Bonus: kanarček

V organiziranem kriminalu kanarček simbolizira obveščevalca, ki »poje policiji«.

Prodajalci varnostnih kopij svetujejo strankam, naj se odzovejo na izsiljevalsko programsko opremo, tako da se naj preprosto vrnejo nazaj na trenutek, preden je prišlo do okužbe, vendar določitev trenutka okužbe je vse prej kot trivialna. Vrzel je v poznavanju natančnega trenutka, ko je prišlo do okužbe, lahko zapolnijo kanarčki (angl. canary files).

a) Kaj so kanarske datoteke (angl. canary files)?

b) Kako jih uprabimo?

c) Ustvarite eno kanarsko datoteko (bodisi word, excel ali podobno) in preiskusite uporabo! Pomagajte si s storitvijo: https://www.stationx.net/canarytokens/. Datoteko si lahko naložite v Google Drive ali podobno stroritev.

Komentar, zapiski vaje: