UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ

2026

Deception technológia

(technické stanovisko)

Projekt Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ (KCKB UPJŠ) financovaný Európskou úniou z prostriedkov Plánu obnovy a odolnosti Slovenskej republiky, kód projektu: 17R05-04-V01-00007.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

OBSAH

ÚVOD

Univerzita Pavla Jozefa Šafárika v Košiciach (ďalej len „UPJŠ“) prostredníctvom Kompetenčného centra kybernetickej bezpečnosti na UPJŠ (ďalej len „KC KB UPJŠ“) si dovoľuje reagovať na požiadavku o vypracovanie technických stanovísk zo strany Ministerstva investícií, regionálneho rozvoja a informatizácie SR (ďalej len „MIRRI“) zo dňa 2. 7. 2025 v časti **Technológia Deception**. Predmetom tohto materiálu je opis procesu a formulácia odporúčaní k nasadeniu tejto technológie, vrátane jej poskytovania vo forme služby, ako zdroja údajov pre potreby **spravodajstva o kybernetických hrozbách** v rámci bezpečnostného monitoringu. Téma zároveň môže zahŕňať aj využitie týchto prístupov vo vzťahu k službám podľa príslušnej legislatívy.

V prostredí súčasnej kybernetickej bezpečnosti rastie význam nástrojov, ktoré umožňujú nielen detegovať útoky, ale aj systematicky zhromažďovať poznatky o správaní útočníkov, ich technikách a používaných nástrojoch. Medzi takéto nástroje patria najmä honeypoty, honeynety a honeytokeny, ktoré predstavujú dôležitý prvok aktívnej obrany a zároveň cenný zdroj údajov pre bezpečnostnú analýzu a spravodajstvo o kybernetických hrozbách (threat intelligence). Ich prínos spočíva v schopnosti zachytávať pokusy o prieskum, prihlásenie, exploitáciu zraniteľností či šírenie malvéru bez priameho ovplyvnenia produkčných systémov organizácie.

Predkladaný text sa zameriava na základné východiská technológie deception, osobitne na problematiku honeypotov, ich klasifikáciu podľa účelu, úrovne interakcie, škálovateľnosti a modelu nasadenia, ako aj na spôsob zberu, správy a analytického spracovania údajov, ktoré z týchto systémov vznikajú. Osobitná pozornosť je venovaná aj honeytokenom ako pasívnemu doplnku detekčných mechanizmov, praktickým aspektom návrhu dôveryhodného a bezpečného honeypotu, jeho viditeľnosti a vhodnému umiestneniu v infraštruktúre. Súčasťou textu je tiež predstavenie vybraných honeypot platforiem, najmä T-Pot a Hugo, a možností využitia nástrojov, ako je Elasticsearch, pri analýze zachytených dát. Cieľom materiálu je poukázať na to, že technológia deception nepredstavuje len technický prostriedok na zachytávanie útokov, ale aj významný analytický nástroj na podporu situačného povedomia, posilnenie bezpečnostného monitoringu a zvyšovanie odolnosti organizácií voči kybernetickým hrozbám.

1 PREDSTAVENIE KC KB UPJŠ

Kompetenčné centrum kybernetickej bezpečnosti na Univerzite Pavla Jozefa Šafárika v Košiciach (KC KB UPJŠ) predstavuje kompetenčné centrum, v rámci ktorého sú realizované aktivity zamerané na vzdelávanie, výskum a expertnú činnosť v oblasti informačnej a kybernetickej bezpečnosti, ochrany dát, kyberkriminality a ochrany pred dezinformáciami. Súčasne KC KB UPJŠ realizuje medzinárodnú spoluprácu s akademickými partnermi zo zahraničia a poskytuje konzultácie pre možnosť prípravy a podania projektov v oblasti kybernetickej bezpečnosti.

Vytvorenie KC KB UPJŠ reflektuje viacero problémov, ktoré možno v súčasnosti identifikovať v oblasti informačnej a kybernetickej bezpečnosti (ďalej aj „KIB“):

- zvýšenie bezpečnostného povedomia relevantných subjektov zahŕňajúcich predovšetkým zamestnancov verejnej správy a študentov vysokoškolského a stredoškolského štúdia,
- vzdelávanie a výchova nových odborníkov pôsobiacich v tejto oblasti,
- výskum kybernetických hrozieb a identifikácia adekvátnych reakcií na tieto hrozby,
- zvýšenie operatívnej bezpečnosti v rámci verejnej správy poskytovaním expertných činností zo strany CSIRT tímu.

V rámci KC KB UPJŠ sa pripravoval študijný plán magisterského stupňa študijného programu aplikovaná informatika, ktorého jedna vetva sa zameriava na kybernetickú bezpečnosť. K tomuto študijnému plánu budú vytvorené, resp. modifikované viaceré predmety. Súčasne sa ako výstup kompetenčného centrá vytvára ponuka **vzdelávania** pre rôzne cieľové skupiny zamestnancov verejnej správy.

V kontexte projektu sa súčasne posilňuje **spolupráca so strednými školami**, najmä vo forme činnosti **KyberTímov**, ich vzdelávania a následného zapojenia do šírenia bezpečnostného povedomia medzi širokou verejnosťou.

V rámci vzdelávacích aktivít sa sumarizujú nové poznatky a skúsenosti z oblasti KIB, ale aj príbuzných oblastí. Tie sú aktuálne doplnené o rôzne formy zážitkového vzdelávania.

V rámci **výskumnej** činnosti dochádza v už existujúcich výskumných oblastiach k publikovaniu viacerých vedeckých výstupov a k vytvoreniu nových možných výskumných spoluprác na posilnenie výskumného a vývojového potenciálu KC KB UPJŠ.

Nemenej dôležitým výstupom projektu je doplnenie výbavy a vzdelávanie univerzitného CSIRT tímu a možnosť poskytovania **expertných činností** pre akreditované CSIRT tímy v SR za účelom rýchlejšej a adekvátnejšej reakcie na kybernetické bezpečnostné incidenty.

2 HONEYPOT

Honeypot je nástroj, ktorý slúži ako návnada na prilákanie útočníkov, resp. pasca za účelom získavania informácií o ich cieľoch, technikách ale aj nástrojoch. Základnou myšlienkou honeypotov je skutočnosť, že útočník nemá vedomosť o tom, že ide o honeypot [1].

Sieť, resp. spojenie dvoch alebo viacerých honeypotov označujeme ako **honeynet** [2], Takýto honeynet obsahuje tri základné prvky, a to kontrolu údajov (data control), zachytávanie údajov (data collection) a zber údajov [2].

Kontrola údajov zahŕňa kontrolu toku údajov tak, aby si útočníci neuvedomili, že sa nachádzajú v honeynete a zabezpečenie toho, aby sa v prípade kompromitácie honeynetu nepoužili na útok na iné systémy. Časť zachytávanie údajov zahŕňa zber všetkých údajov týkajúcich sa správania sa útočníka v rámci honeynetu. Zber údajov zahŕňa schopnosť bezpečne preniesť všetky zachytené údaje na centralizované miesto.

2.1 ROZDELENIE HONEYPOTOV

Honeypoty vieme klasifikovať do jednotlivých kategórii podľa módu interakcie, typov dát, ktoré zbierajú, podľa role v organizácii, resp. podľa jeho typu honeypotu a podľa mnoho ďalších kategórii.

Rozdelenie podľa účelu: Honeypoty možno rozdeliť do dvoch tried na základe účelu, na ktorý boli vytvorené: výskumné a produkčné honeypoty. Výskumné honeypoty sa používajú na zhromažďovanie a analýzu informácií o útokoch s cieľom vyvinúť lepšiu ochranu proti týmto útokom. Produkčné honeypoty sú viac zamerané na obranu. Zvyčajne sa implementujú s cieľom zabrániť útočníkovi v prístupe do skutočného systému organizácie, ktorá ho implementuje [2].

Klasifikácia podľa úlohy: Úloha označuje, či honeypot aktívne detekuje alebo pasívne zachytáva prevádzku. Klientský honeypot môže aktívne iniciovať požiadavku na server na preskúmanie škodlivého programu, zatiaľ čo serverový honeypot čaká na útoky. Veľká väčšina honeypotov sú serverové honeypoty.

Klasifikácia podľa škálovateľnosti: Škálovateľnosť sa vzťahuje na schopnosť honeypotu rásť a poskytovať viac návnad. Neškálovateľný honeypot má len určitý počet návnad a nedá sa meniť. Škálovateľný honeypot môže rozšíriť počet návnad, ktoré nasadzuje a monitoruje [2].

Klasifikácia podľa úrovne interakcie: Honeypoty možno klasifikovať podľa úrovne interakcie, ktorú umožňujú útočníkovi, a to na honeypoty s nízkou interakciou, strednou interakciou a vysokou interakciou a hybridná interakcia. Nízko interakčné honeypoty napodobňujú jednu alebo viacero služieb s jednoduchými funkciami a neposkytujú prístup k operačnému systému [2]. Výhodami honeypotov s nízkou interakciou sú jednoduchá inštalácia, nízke riziko, nízke náklady a nenáročná

údržba. Útočníci však honeypoty s nízkou interakciou oveľa ľahšie identifikujú, pretože dané honeypoty sú obmedzené a informácie, ktoré zhromažďujú, majú nízku vernosť.

Honeypoty s vysokou úrovňou interakcie poskytujú oveľa viac funkcií, nielen emulujú služby, ale umožňujú aj prístup k samotnému operačnému systému. Tento typ honeypotu zhromažďuje informácie o všetkých aktivitách útočníka, čo je výhodou oproti honeypotom s nízkou, alebo strednou úrovňou interakcie, pretože zhromaždené informácie majú vysokú mieru vernosti [3]. Ako už názov napovedá, honeypoty so strednou úrovňou interakcie poskytujú úroveň interakcie medzi honeypotmi s nízkou a vysokou úrovňou interakcie. Hoci existujú rôzne pohľady na to, či majú skutočný operačný systém alebo emulovaný operačný systém, je isté, že poskytujú viac funkcionalít ako nízko úrovňové honeypoty, týmto sťažujú útočníkom ich odhalenie. Honeypoty s nízkou úrovňou interakcie sa hodia najmä na hromadný zber informácií o skenovaní a automatizovaných útokoch. Slúžia na rýchlu detekciu základných hrozieb pri nízkom riziku a minimálnych nárokoch na prevádzku. Naopak, honeypoty s vysokou úrovňou interakcie umožňujú detailnú analýzu správania útočníka po úspešnom prieniku, no ich nasadenie vyžaduje prísne bezpečnostné opatrenia.

Platforma T-Pot nepredstavuje jeden konkrétny typ honeypotu, ale spája viacero honeypotov s rôznou úrovňou interakcie. Väčšina honeypotov v rámci T-Pot patrí do kategórie nízko až stredne interaktívnych riešení. Tento prístup zodpovedá hlavnému cieľu platformy, ktorým je zber dát pre účely threat intelligence. Umožňuje zachytávať široké spektrum útokov pri zachovaní primeranej úrovne bezpečnosti a jednoduchej správy. Honeypoty s vysokou úrovňou interakcie nie sú v základnom nasadení T-Pot dominantné, pretože by výrazne zvýšili riziko kompromitácie aj nároky na správu prostredia. T-Pot je preto vhodné vnímať najmä ako nástroj na systematický zber a analýzu v prvotných fázach útoku, nie ako platformu určenú na detailnú forenznú analýzu po úplnom prieniku do systému.

Klasifikácia podľa modelu vývoja: Dostupné honeypoty a deception riešenia sa líšia mierou interakcie, účelom použitia, atď. Open-source nástroje sa využívajú najmä na výskum a zber pre účely threat intelligence, zatiaľ čo komerčné platformy sú navrhnuté predovšetkým na detekciu útokov v organizácii.

Open-source honeypoty sú spravidla zamerané na konkrétnu službu alebo protokol. Používajú sa najmä na zachytávanie skenovania portov, pokusov o prihlásenie a zneužívanie známych zraniteľností. Medzi bežne používané riešenia patrí napríklad už spomínané Cowrie, ktorý zaznamenáva SSH a Telnet, alebo Dionaea, zameraný na zachytávanie malvéru a exploitov. Tieto nástroje sa často nasadzujú samostatne a ich hlavnou výhodou je nízka vstupná bariéra a možnosť prispôsobenia. Nevýhodou je obmedzená schopnosť simulovať komplexné produkčné prostredia a vyššia náročnosť správy.

Komerčné deception platformy poskytujú komplexnejší prístup a sú určené najmä na ochranu interných sietí. Typicky kombinujú honeypoty z vysokou mierou interakcie, honeytokeny a centralizovanú správu falošných systémov a účtov. Medzi známe riešenia patria platformy od SecurityHive alebo napríklad Thinkst Canary. Tieto nástroje ponúkajú integráciu so SIEM systémami a

podporu incident response, no vyžadujú vyššie finančné náklady a poskytujú menšiu transparentnosť vnútorného fungovania.

2.2 ZBER A SPRÁVA ÚDAJOV Z HONEYPOTOV

Honeypoty zbierajú údaje pasívnym alebo aktívnym spôsobom v závislosti od úrovne interakcie, ktorú poskytujú útočníkovi. Pasívny zber sa zameriava na zachytávanie sieťovej aktivity bez výraznej komunikácie so službou, zatiaľ čo aktívny zber umožňuje útočníkovi pracovať s reálnym alebo simulovaným systémom. V oboch prípadoch ide o úmyselne vystavené systémy, ktorých cieľom je zaznamenať správanie útočníkov bez ovplyvnenia produkčného prostredia.

Medzi základné údaje, ktoré honeypoty štandardne zbierajú, patria zdrojové IP adresy, časové pečiatky, cieľové porty, použité protokoly a typy požiadaviek. Tieto informácie umožňujú identifikovať skenovanie portov, automatizované útoky a časové vzory aktivity. Honeypoty s nízkou úrovňou interakcie sa spravidla obmedzujú na tento typ zberu dát, keďže neposkytujú plnohodnotnú interakciu so službami. Príkladom je Honeytrap, ktorý zaznamenáva pokusy o spojenie na rôzne porty a poskytuje prehľad o cieľoch a intenzite útokov na sieťovej úrovni.

Honeypoty so strednou a vysokou úrovňou interakcie umožňujú zber detailnejších informácií o správaní útočníkov. Napríklad honeypot Cowrie [4] zaznamenáva celé SSH a Telnet relácie vrátane použitých prihlasovacích údajov, vykonaných príkazov a prenesených súborov. Takéto údaje poskytujú pohľad na používané nástroje, skripty a techniky po úspešnom prihlásení a umožňujú rozlišovať medzi plne automatizovanými útokmi a manuálnou aktivitou útočníka. Osobitnú kategóriu tvoria honeypoty zamerané na zachytávanie malvéru. Honeypot Dionaea [5] simuluje zraniteľné služby a protokoly s cieľom zachytiť exploit kód a binárne súbory, ktoré sa útočníci pokúšajú do systému nahrať. Výsledkom sú vzorky malvéru spolu s informáciami o použitých zraniteľnostiach a spôsoboch šírenia.

Správa threat intelligence informácií získaných z honeypotov si vyžaduje priebežné spracovanie a hodnotenie dát v čase. Surové údaje, ako sú IP adresy, cieľové porty alebo prihlasovacie údaje, majú obmedzenú platnosť a ich hodnota rýchlo klesá, najmä pri automatizovaných útokoch využívajúcich dynamickú infraštruktúru. Z tohto dôvodu je vhodné pracovať s časovými oknami a pravidelne prehodnocovať relevanciu indikátorov na základe ich opakovania a kontextu výskytu. Praktickým prístupom k správe dát je časové obmedzenie platnosti indikátorov, napríklad formou automatizovaného vyradenia údajov, ktoré sa v definovanom období znovu neobjavili. IP adresy a sieťové rozsahy používané pri masovom skenovaní môžu byť relevantné len niekoľko dní až týždňov, zatiaľ čo informácie o používaných nástrojoch, exploitoch alebo malvéri majú dlhšiu analytickú hodnotu, rádovo niekoľko týždnou až pár mesiacov. Tieto údaje je vhodné uchovávať dlhodobo, keďže umožňujú sledovať vývoj útočných techník a opakované vzory správania.

Odstraňovanie alebo archivácia neaktuálnych údajov je dôležité nielen z pohľadu kvality threat intelligence, ale aj z hľadiska efektívnej správy dát. Oddelenie aktuálnych dát od historických dát zjednodušuje ich spracovanie a podporuje celkové hodnotenie hrozieb. Dĺžka uchovávania zozbieraných údajov teda závisí od cieľov a potrieb bezpečnostného tímu. Údaje určené na operatívne sledovanie hrozieb majú význam len v kratšom časovom horizonte, zatiaľ čo pri analytických alebo výskumných aktivitách je vhodné uchovávať historické dáta dlhšie. Honeypoty tak neposkytujú len

krátkodobé indikátory kompromitácie, ale aj vstupy pre dlhodobé sledovanie trendov a vývoja hrozieb v prostredí internetu.

3 HONEYTOKEN

Honeytokeny predstavujú pasívny doplnok k honeypotom, ktorý umožňuje detekovať neoprávnený prístup bez potreby interakcie so službami. Ide o zámerne umiestnené falošné artefakty, ako sú prihlasovacie údaje, konfiguračné súbory, dokumenty alebo databázové záznamy. Každý honeytoken má jednoznačný identifikátor, ktorý umožňuje presne určiť miesto jeho úniku alebo použitia. Ak sa honeytoken objaví mimo očakávaného prostredia, ide o silný indikátor kompromitácie [6].

V praxi sa honeytokeny používajú na monitorovanie prístupov k súborovým systémom, databázam, cloudovým službám alebo zdrojovým kódom. Typickým príkladom je falošný konfiguračný súbor s prihlasovacími údajmi uložený v systéme, ku ktorému by legitímny používateľ nemal dôvod pristupovať. Pokus o jeho použitie je jednoznačný signál bezpečnostného incidentu. Výhodou honeytokenov je nízka prevádzková náročnosť a minimálne riziko zneužitia, keďže samy o sebe neposkytujú útočníkovi žiadnu reálnu hodnotu. Honeytokeny je možné využiť aj na vytvorenie logického honeynetu bez potreby nasadenia viacerých aktívnych honeypotov. Strategickým rozmiestnením honeytokenov naprieč systémami, sieťovými segmentmi a aplikáciami vzniká sieť pasívnych senzorov, ktorá mapuje pohyb útočníka v prostredí. Takýto prístup je vhodný najmä na detekciu samotného prieniku, zneužitia privilegovaných účtov alebo exfiltrácie dát, kde klasické honeypoty nemusia zachytiť samotnú aktivitu [6].

Platforma T-Pot neposkytuje natívnu podporu pre správu honeytokenov, keďže sa zameriava na sieťovo orientované honeypoty a zber dát o externých útokoch. Existujú samostatné riešenia, ktoré podporujú generovanie a správu honeytokenov, napríklad platformy založené na falošných prihlasovacích údajoch, dokumentoch alebo cloudových kľúčoch. Kombinácia T-Pot a honeytokenov tak umožňuje pokryť viaceré fázy útoku bez veľkého zvýšenia nákladov na údržbu [6].

4 ODPORÚČANIA A PRAKTICKÉ ASPEKTY

Medzi najčastejšie zaznamenané útoky v honeypotoch a honeynetoch patria skenovacie útoky. Tie slúžia útočníkom na mapovanie siete, zisťovanie otvorených portov a dostupných služieb, ktoré môžu byť potenciálne zraniteľné. Často sa vyskytujú aj útoky typu DoS/DDoS, ktorých cieľom je narušiť dostupnosť cieľového systému alebo služby. Bežné sú aj útoky cez SSH pomocou brute-force, prípadne Man-in-the-Middle zamerané na odpočúvanie komunikácie. Menej často sa objavujú ransomvér, cryptojacking či malvér, ktoré spravidla nasledujú po úspešnom preniknutí do systému.

4.1 POKUSY O PRIHLÁSENIE A SPRÁVANIE ÚTOČNÍKOV

Pripojenie bez následnej aktivity sa vo väčšine prípadov považuje za pokus o útok. Na druhej strane, aj takéto pokusy môžu byť pre správcu honeypotu užitočné. Na základe frekvencie odmietnutých pokusov o prihlásenie je možné identifikovať a obmedziť prístupy z IP adries, ktoré sa

neprihlásili opakovane. Tieto jednorazové pokusy môžu naznačiť špecifickú aktivitu jednotlivých útočníkov alebo skenovacích nástrojov, najmä ak sa analyzujú v kontexte IP rozsahov [3].

Údaje o cieľových portoch a používaných systémoch majú taktiež určitú hodnotu. Môžu napríklad pomôcť odhaliť, či je dané zariadenie súčasťou botnetu. Typickým príkladom je komunikácia na port 445, ktorá sa často spája s určitými typmi operačných systémov. Takéto spojenia môžu signalizovať automatizované útoky alebo zapojenie zariadenia do rozsiahlejšej útočnej infraštruktúry [3].

Cielený útok na konkrétny port sa prejavuje opakovanými pokusmi o interakciu s tou istou službou, často s rôznymi vstupnými parametrami alebo prihlasovacími údajmi. Na rozdiel od toho je skenovanie portov charakteristické krátkodobou aktivitou zameranou na veľký počet portov bez hlbšej interakcie so službami. Tieto dva typy správania je možné v praxi rozlíšiť analýzou aktivity zdrojovej IP adresy v definovanom časovom intervale, napríklad 1 až 2 hodín. Udalosti sa agregujú podľa IP adresy a honeypotu, pričom sa sleduje počet unikátnych cieľových portov a rozsah interakcie. Ak sa aktivita sústreďuje na jeden honeypot a jeden alebo úzky rozsah portov, ide o cielený útok na konkrétnu službu. Naopak, výskyt tej istej IP adresy na viacerých honeypotoch alebo vysoký počet rôznych portov poukazuje na automatizované skenovanie.

Na rozlíšenie IP adresy útočníka cieliaceho priamo na honeypot organizácie od automatizovaných skenovacích nástrojov je možné využiť kombináciu viacerych faktorov. Automatizované nástroje a boty sa spravidla prejavujú krátkodobou aktivitou zameranou na veľký počet portov alebo služieb bez výraznej snahy o interakciu. Ich správanie je často konzistentné, opakovateľné a nezohľadňuje odpovede cieľového systému. Naopak, IP adresy cieliace na konkrétny honeypot vykazujú zvýšenú aktivitu na danom honeypote, napríklad opakované pokusy o prístup k rovnakej službe, zmenu prihlasovacích údajov alebo návrat v rôznych časových intervaloch. Dôležitým indikátorom je aj rozsah interakcie po úspešnom pripojení. Zatiaľ čo skenovacie nástroje sa po nadviazaní spojenia často okamžite odpoja alebo vykonajú len základný test služby, cielený útočník má tendenciu pokračovať v aktivite, skúšať ďalšie príkazy alebo overovať dostupné funkcie systému, atď. Opakovaný výskyt tej istej IP adresy v kombinácii s konkrétnou službou zvyšuje pravdepodobnosť, že ide o cielenie na honeypot danej organizácie.Ďalšie faktory ovplyvnujúce rozhodovanie sú IP rozsahy známe pre masové skenovanie, typ použitého klienta alebo časovanie aktivity, reputácia IP adresy, atď. IP adresy, ktoré sa objavujú naprieč viacerými honeypotmi alebo v krátkom čase generujú veľké množstvo spojení, je možné s vysokou pravdepodobnosťou považovať za súčasť automatizovanej infraštruktúry. Naopak, aktivita obmedzená na jeden honeypot a úzky rozsah služieb naznačuje cielený prieskum alebo pokus o kompromitáciu.

Pri emulácii služby vzdialeného prístupu, ako je napríklad SSH, majú pokusy o prihlásenie vyššiu výpovednú hodnotu v porovnaní s bežnými pripojeniami na iné sieťové porty. V prípade emulácie iných protokolov môže ísť o neúmyselné prístupy, spôsobené napríklad chybami v smerovaní alebo legitímnymi požiadavkami používateľov, napríklad pri prezeraní obsahu webových stránok, požiadavkách DNS, IRC alebo FTP prístupoch. V takýchto prípadoch nie je vždy možné pripojenie jednoznačne považovať za útok. Služby ako SSH však spravidla neslúžia na všeobecný prístup, ale primárne na správu systémov alebo prenos súborov, a preto sa v honeypotoch nepredpokladá legitímne využitie. Administrátori pritom na správu samotného honeypotu nepoužívajú rovnaký port ani rovnaký prístupový kanál, čím sa minimalizuje riziko falošnej identifikácie. Z toho vyplýva, že akýkoľvek pokus o prístup prostredníctvom SSH možno považovať za pokus o útok alebo prieskum [3].

Takéto pokusy môžu naznačovať konkrétny záujem útočníkov o vzdialený prístup a o vyhľadávanie zraniteľných systémov. Zároveň ponúkajú možnosť sledovať používané kombinácie prihlasovacích údajov, IP adresy útočníkov či verziu ich klientskych nástrojov, čo môže byť cenné pre ďalšiu analýzu.

Neúspešný pokus o prihlásenie (napríklad pri použití nesprávnej kombinácie mena a hesla) nemá výraznú informačnú hodnotu pre ďalšiu analýzu, okrem základných štatistických údajov. Takéto prístupy je možné využiť najmä na tvorbu prehľadov o frekvencii pokusov a používaných prihlasovacích údajoch. Z tohto dôvodu sa neúspešné prihlásenie do honeypotu obvykle považuje za pokus o útok. Naopak, úspešné prihlásenie má oveľa vyššiu výpovednú hodnotu. Okrem zaznamenania kombinácie mena a hesla je možné analyzovať aj IP adresu útočníka, verziu klienta či ďalšie metadáta spojené s prístupom. Ak však po prihlásení nenastane žiadna ďalšia aktivita, správca honeypotu často na základe objektívnych kritérií vyhodnotí, či išlo o útok. Toto hodnotenie zohľadňuje napríklad to, či útočník použil bežné alebo silné heslo a aká je pravdepodobnosť, že sa na systém vráti [3].

4.2 Zložitosť systému

Zložitosť honeypotu alebo honeynetu priamo závisí od úrovne interakcie, ktorú systém poskytuje, a od počtu podporovaných služieb a protokolov. Čím vyššia je táto interaktivita a čím viac služieb je emulovaných, tým rozsiahlejšie a kvalitnejšie údaje možno zozbierať. Simulácia reálnych systémov pomocou honeypotov umožňuje vytvoriť dôveryhodné návnady, ktoré napodobňujú bežnú infraštruktúru organizácií prístupnú z internetu. Takéto systémy môžu reprezentovať aplikačné servery, databázové služby, sieťové prvky alebo prvky identity infraštruktúry. Na druhej strane si to vyžaduje väčšie množstvo výpočtových zdrojov na spracovanie a ukladanie týchto dát. Jednou z hlavných výziev pri nasadzovaní honeypotov je vytvoriť čo najrealistickejšie prostredie, ktoré nebude ľahko identifikovateľné ako falošné, ani pre útočníkov, ani pre automatizované nástroje. Je to kľúčové pre to, aby honeypot skutočne prilákal útoky a umožnil sledovanie správania útočníkov v reálnom čase.

Aby sa zvýšila dôveryhodnosť a minimalizovalo riziko odhalenia, pričom zložitosť systému ostala manažovateľná sa odporúča napríklad používať obmedzený počet služieb, ktoré zodpovedajú typickému správaniu bežného systému, pričom je potrebné zabezpečiť, aby príkazy systému vrátili zmysluplné a realistické výstupy (napr. bežiace procesy). Taktiež za zmienku stojí vyhnutie sa používaniu statických, vopred definovaných hodnôt. Takéto opatrenia zvyšujú efektivitu honeypotu pri získavaní relevantných dát bez toho, aby pôsobil podozrivo alebo bol rýchlo odhalený. Funkcionalita systémových nástrojov by mala byť úplná a prirodzená, aby prostredie pôsobilo autenticky. Požiadavky útočníkov, napríklad na sťahovanie súborov, by mali byť najskôr presmerované do izolovaného prostredia (sandboxu) a až po určitom oneskorení analyzované pomocou externých služieb, ako je napríklad VirusTotal [2].

Pri simulácii aplikačných serverov sa honeypoty zameriavajú najmä na služby ako HTTP a HTTPS, ktoré patria medzi najčastejšie ciele útokov. Podobne je možné simulovať aj databázové a aplikačné služby dostupné z internetu, napríklad prostredníctvom protokolov používaných databázovými servermi. V takom prípade honeypot reaguje na základné požiadavky, aby sa dal zachytiť prieskum a pokusy o kompromitáciu. Samostatnú kategóriu tvoria služby vzdialeného prístupu, hlavne SSH, ktoré útočníci často využívajú pri automatizovaných aj cielenejších útokoch. V týchto prípadoch má zmysel zachytávať pokusy o prihlásenie a následnú interakciu, keďže ide o typ služby, pri ktorej sa v honeypote nepredpokladá legitímne používanie. Simulovať je možné aj sieťové prvky, ako sú VPN brány alebo

administračné rozhrania zariadení, ak sa takéto typy služieb bežne vyskytujú medzi verejne dostupnými cieľmi. Pri simulácii komplexnejších systémov, ako sú prvky identity infraštruktúry, sa honeypoty spravidla obmedzujú na emuláciu vybraných rozhraní vystavených do internetu. V praxi sa preto takéto prvky často nasadzujú ako súčasť širšieho honeynetu, kde viaceré IP adresy a služby vytvárajú ucelený obraz infraštruktúry, ktorý pôsobí dôveryhodnejšie než izolované návnady.

4.3 VIDITEĽNOSŤ HONEYPOTU

Nemenej dôležitým faktorom je aj to, ako systém pôsobí navonok najmä vo vyhľadávačoch zariadení. Ak je honeypot zobrazený ako dôveryhodný a reálny systém, zvyšuje to šancu, že sa stane cieľom útoku. Zároveň je však dôležité minimalizovať jeho identifikovateľnosť ako falošného cieľa, aby sa predišlo jeho rýchlemu odhaleniu. Jedným z dôležitých aspektov pri prevádzke honeypotu alebo honeynetu je dosiahnuť, aby sa systém objavil vo vyhľadávačoch zariadení na internete, no zároveň nepôsobil podozrivo alebo nebol identifikovaný ako falošný. Z tohto dôvodu je potrebné priebežne sledovať špecializované vyhľadávače ako Shodan, ktoré mapujú a kategorizujú zariadenia pripojené na internet – vrátane honeypotov.

Tieto služby síce môžu pomôcť overiť, že honeypot je z internetu viditeľný a dostupný, no zároveň uľahčujú prácu útočníkom, keďže im poskytujú zoznam potenciálnych cieľov. Ak je však honeypot vo vyhľadávači zobrazený ako bežné zariadenie a nie ako návnada, ide o výhodu a teda, zvyšuje to jeho dôveryhodnosť a pravdepodobnosť, že sa stane cieľom útoku. Takéto zaradenie napomáha naplniť hlavný cieľ honeypotu: prilákať útočníkov a získať informácie o ich správaní. Dôveryhodnosť honeypotu je možné ďalej zvýšiť nasadením plnohodnotnej simulácie prostredia, kde operačný systém a aplikácie reagujú konzistentne. Kľúčovým prvkom je dynamická interakcia, ktorá umožňuje útočníkovi vykonávať príkazy a pozorovať realistické správanie systému, namiesto vopred definovaných odpovedí. K tomu je vhodné doplniť simulovanú legitímnu prevádzku, ako sú prihlasovania cez SSH alebo bežná webová aktivita, aby honeypot nepôsobil nečinne alebo opustene.

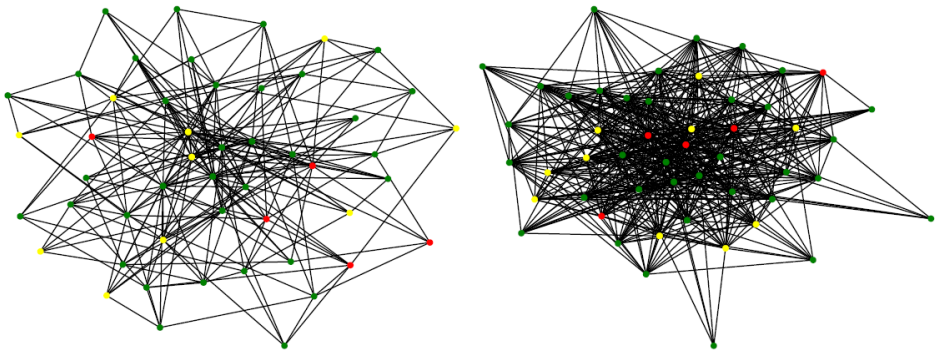
Zníženie pravdepodobnosti identifikácie honeypotu si vyžaduje aj úpravu predvolených nastavení. Patria sem zmeny bannerov služieb, prezentovaných verzií softvéru, štruktúry súborového systému a odstránenie typických znakov štandardných inštalácií honeypotov. Rovnako dôležité je napodobňovanie správania sieťových protokolov tak, aby odpovede zodpovedali reálnym implementáciám a neobsahovali zjednodušené alebo generické reakcie. Útočníci často využívajú práve tieto odchýlky na odhalenie falošných systémov. Samostatnú pozornosť si vyžaduje časovanie a latencia odpovedí. Honeypoty môžu reagovať inak než bežné produkčné systémy, čo umožňuje ich identifikáciu pomocou časovej analýzy. Zavedenie realistických oneskorení a konzistentných fingerprintov operačného systému a služieb pomáha eliminovať nezrovnalosti, ktoré dokážu nástroje na skenovanie odhaliť. Zachovanie konzistencie naprieč sieťovou vrstvou, službami a operačným systémom je základným predpokladom na to, aby sa honeypot neobjavil v databázach označených falošných cieľov a zároveň zostal atraktívny pre útočníkov.

Aby jednotlivé honeypoty a IP adresy pôsobili navonok legitímne, je potrebné vytvoriť jednotný profil služieb naprieč celým prostredím. Profil by mal zohľadňovať, ktoré služby sú bežne dostupné z internetu a ako sa typicky správajú. Nezladené kombinácie služieb, nelogické porty alebo nekonzistentné odpovede môžu útočníkom aj automatizovaným nástrojom signalizovať umelé prostredie. Dôveryhodný profil obsahuje konzistentné informácie naprieč službami, napríklad zladené

bannery, verzie a typické reakcie protokolov. Pri webových službách je dôležitá konzistencia HTTP odpovedí a hlavičiek, primeraná štruktúra URL a obsah, ktorý nepôsobí prázdno. Pri službách vzdialeného prístupu je dôležité, aby prihlasovacie dopyty a následné odpovede zodpovedali očakávaniam útočníka a nevykazovali typické znaky emulácie. Súčasťou profilu je aj realistické časovanie odpovedí a konzistentný fingerprint operačného systému a služieb. Ak sieťová vrstva, bannery a správanie protokolov pôsobia umelo, zvyšuje sa riziko, že systém bude v databázach označený ako honeypot. Simulácia viacerých služieb preto zvyšuje viditeľnosť honeypotu ako bežného cieľa a zároveň znižuje pravdepodobnosť jeho rýchleho odhalenia.

4.4 UMIESTNENIE HONEYPOTOV

Okrem samotného počtu honeypotov hrá dôležitú úlohu aj ich strategické umiestnenie. Správne rozmiestnenie pomáha oklamať útočníka, zdržovať ho a odvádzať od skutočných cieľov. Dve infraštruktúry honeynetov s rovnakým počtom honeypotov môžu mať odlišnú efektivitu práve v závislosti od toho, kde sú tieto prvky umiestnené. Na určenie vhodného umiestnenia možno využiť tzv. **graf útoku** – orientovaný graf, ktorý znázorňuje možné cesty, akými môže útočník postupovať pri zneužívaní zraniteľností v sieti. Uzly v grafe predstavujú jednotlivé systémy alebo stavy v sieti a hrany medzi nimi znázorňujú závislosti medzi zneužitiami. Napríklad, ak útočník môže kompromitovať systém *h1* až po tom, čo získa kontrolu nad *h2*, v grafe bude medzi *h2* a *h1* hrana [7] (Obr. č. 1).



(e) N_5 (f) N_6

Obr. č. 1: Ukážka topológie vybraných sietí [7].

Honeypoty by mali byť umiestnené medzi takýmito prepojenými bodmi, kde pre útočníka pôsobí interakcia s honeypotom ako logická súčasť cesty útoku. Tým sa zvýši pravdepodobnosť, že sa do honeypotu zapojí, čo ho odvedie od reálneho cieľa. Zároveň tým možno vytvoriť dojem, že je sieť zraniteľnejšia, než v skutočnosti je. Okrem toho vhodne umiestnené honeypoty umožňujú sledovanie postupu útočníka. Ak sa dostane do kontaktu s honeypotom, znamená to, že už prekonal určité predchádzajúce kroky útoku, čo poskytuje cenné informácie o jeho správaní a stratégii.

Topológia honeynetu je ďalším dôležitým faktorom, ktorý ovplyvňuje jeho účinnosť. Spôsob, akým sú jednotlivé systémy navzájom prepojené, môže mať výrazný vplyv na schopnosť odhaliť správanie útočníka. Napríklad v sieti s plne prepojenou (full mesh) topológiou sú všetky systémy navzájom

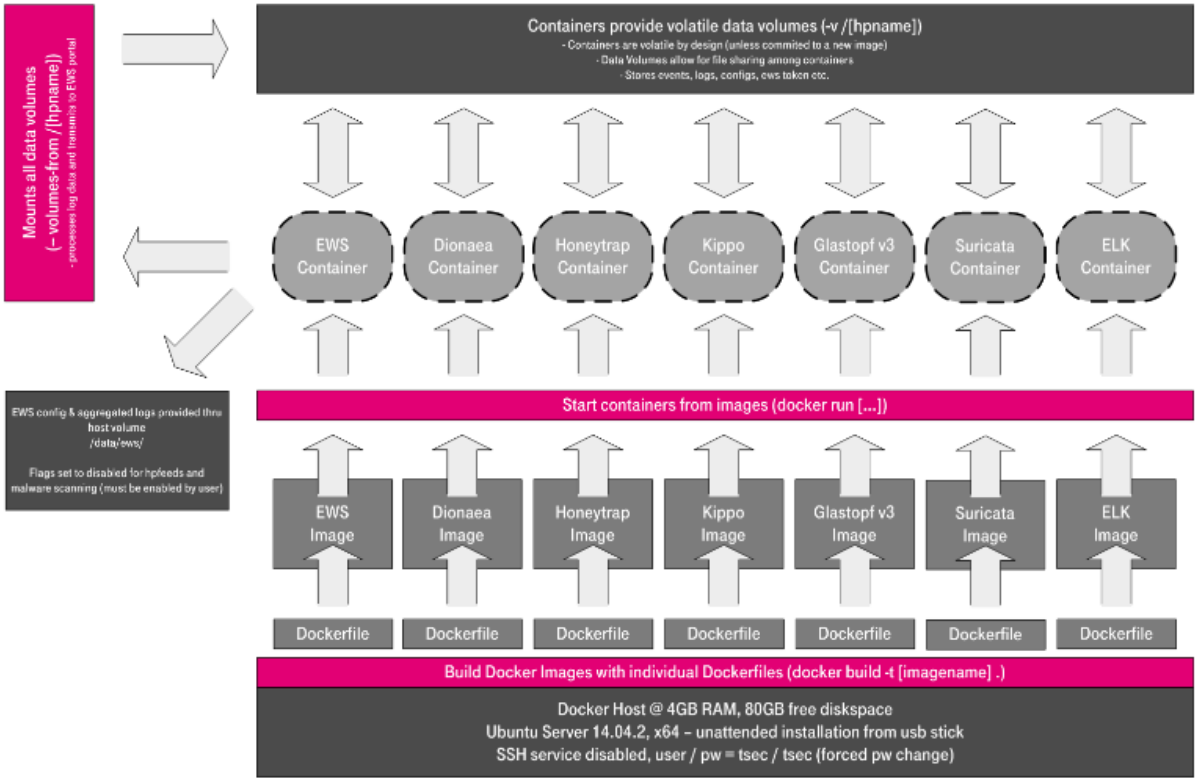
priamo prepojené, čo umožňuje rýchle šírenie škodlivého kódu (malvéru) medzi nimi. Takáto štruktúra môže byť pre útočníka atraktívna, no zároveň predstavuje vyššie bezpečnostné riziko a vyžaduje väčšiu pozornosť zo strany obrancu pri kontrole šírenia a izolácie incidentov. Z tohto dôvodu je dôležité starostlivo zvoliť topológiu honeynetu tak, aby bola v súlade s cieľmi systému – či už ide o zber informácií, oneskorenie útočníka, alebo minimalizáciu rizík. Správne navrhnutá sieťová štruktúra môže výrazne zlepšiť celkový výkon honeynetu [7].

5 HONEYPOT PLATFORMY

Honeypot platformy predstavujú komplexné riešenia, ktoré integrujú viacero honeypotov do jedného nasaditeľného celku. Na rozdiel od samostatných honeypotov poskytujú centralizovanú správu, jednotné logovanie a nástroje na vizualizáciu a analýzu zachytených dát. Vďaka tomu je možné súčasne monitorovať väčšie množstvo služieb a protokolov, pričom všetky získané informácie sú analyzované na jednom mieste. Takéto platformy sú nasadzované najmä v akademickom a výskumnom prostredí, ale aj v komerčnej sfére, kde slúžia ako zdroj informácií o aktuálnych hrozbách v rámci threat intelligence. Medzi najznámejšie a najrozšírenejšie honeypot platformy patrí T-Pot, pričom v stredoeurópskom kontexte je relevantnou alternatívou aj projekt Hugo vyvíjaný združením CESNET.

5.1 T-POT PLATFORMA

T-Pot je honeypot platforma, cez ktorú vieme monitorovať a analyzovať útoky na infraštruktúru (Obr. č. 2). Využíva pri tom viacero honeypotov, ktoré sú určené na simuláciu zraniteľného prostredia snažiace sa prilákať útočníkov. Cieľom T-Pot je zachytávať metódy útokov, správanie útočníkov a zároveň poskytovať cenné dáta pre ďalšiu analýzu a zlepšenie bezpečnosti. V rámci typického nasadenia je T-Pot vystavený priamo do internetu a simuluje zraniteľné alebo nesprávne zabezpečené služby, ktoré sú bežným cieľom automatizovaných aj cielenejších útokov. Platforma týmto spôsobom zachytáva skenovanie portov, pokusy o prihlásenie, exploitáciu známych zraniteľností a pokusy o šírenie malvéru. Získané údaje poskytujú prehľad o aktuálnych hrozbách a umožňujú sledovať zmeny v správaní útočníkov v čase [8].



Obr. č. 2: Ukážka vybranej časti T-Pot architektúry [9].

T-Pot využíva široké spektrum honeypotov, z ktorých každý je navrhnutý na simuláciu konkrétneho typu služby alebo prostredia:

- **Cowrie** je zo skupiny honeypotov so strednou až vysokou úrovňou interakcie zameraný na služby SSH a Telnet. Zaznamenáva útoky hrubou silou na tieto služby. Vďaka nemu vieme analyzovať správanie útočníka, keďže zachytáva pokusy o vykonanie príkazov, vykonané príkazy aj logy o nahraných a stiahnutých súboroch.
- **Dionaea** emuluje Windows prostredie a služby so zraniteľnosťami a odchytáva malvér, ktorý ich zneužíva.
- **Heralding** je určený na zbieranie prihlasovacích údajov. Registruje pokusy o prihlásenie a teda deteguje brute-force útoky, zaznamenáva aj použité používateľské mená a heslá, čo sa dá využiť v prehľadoch o najčastejšie používaných heslách.
- **Mailoney** je SMTP honeypot s nízkou interakciou špecializovaný na mailové služby. Emuluje rôzne typy zraniteľností.
- **Tanner** sleduje útoky na službu RDP.
- **Adbhoney** je honeypot s nízkou úrovňou interakcie, špecificky navrhnutý na detekciu útokov zameraných na zariadenia s otvoreným portom 5555. Tento port je štandardne využívaný pre Android Debug Bridge (ADB)
- **Honeytrap** pôsobí ako bežiaca TCP alebo UDP služba. Je to honeypot s nízkou interakciou, ktorý bol vytvorený s myšlienkou odchytávania útokov na TCP a UDP služby.

- **ConPot** je ICS/SCADA honeypot, ktorý simuluje zraniteľné ICS/SCADA protokoly, a tak zhromažďuje informácie o motívoch a metódach útočníkov zameraných na priemyselné riadiace systémy.
- **CitrixHoneypot** je honeypot špecificky navrhnutý na emuláciu Citrix Gateway VPN, aby detegoval útoky na Citrix remote access.
- **ElasticPot** simuluje zraniteľný Elasticsearch server zverejnený na internete.
- **RedisHoneypot** simuluje zraniteľný Redis databázový server s neautorizovaným prístupom.
- **CiscoASA** honeypot je navrhnutý na detegovanie CVE-2018-0101, čo je zraniteľnosť týkajúca sa DoS a remote code execution.
- **DDoSPot** monitoruje Distributed Denial of Service (DDoS) útoky založené na UDP.

T-Pot využíva široké spektrum honeypotov, z ktorých každý sa zameriava na konkrétny typ služby alebo prostredia. Honeypoty orientované na vzdialený prístup, ako Cowrie, zachytávajú pokusy o prihlásenie cez SSH a Telnet a umožňujú analyzovať vykonané príkazy a prenášané súbory. Honeypoty zamerané na zber malvéru, ako Dionaea, simulujú zraniteľné služby a zaznamenávajú exploit kód a binárne súbory používané pri útokoch. Ďalšie komponenty platformy pokrývajú databázové služby, webové aplikácie, VPN brány, priemyselné riadiace systémy alebo sieťové protokoly používané pri DDoS útokoch.

Takéto rozdelenie umožňuje získať údaje o tom, ktoré služby sú zo strany útočníkov najčastejšie cieľom, aké porty sú skenované a aké techniky sa používajú pri pokusoch o kompromitáciu. Kombináciou dát z viacerých honeypotov je možné rozlišovať medzi plošným skenovaním, automatizovanými útokmi a cielenejšou aktivitou zameranou na konkrétny typ služby alebo prostredia. Získané údaje sú v T-Pot centralizované a časovo korelované, čo umožňuje ich ďalšiu analýzu. Dáta môžu slúžiť na tvorbu prehľadov o zdrojových IP adresách, používaných prihlasovacích údajoch, cieľových portoch alebo typov útokov. V dlhšom časovom horizonte je možné sledovať trendy, opakujúce sa vzory správania a porovnávať aktuálnu aktivitu s historickými dátami. Z pohľadu threat intelligence je T-Pot vhodný najmä ako zdroj informácií o aktualnych hrozbách. Neposkytuje detailný pohľad na správanie útočníka po prieniku do systému, no efektívne pokrýva fázu prieskumu a počiatočného prístupu.

5.2 HUGO PLATFORMA

Hugo je honeypot platforma vyvíjaná českým združením CESNET, ktorá je postavená na koncepte „Honeypot as a Service". Jej hlavným cieľom je poskytnúť inštitúciám jednoducho nasaditeľné honeypoty vo forme virtuálnych strojov, ktoré po nasadení v sieti členov CESNET automaticky reportujú zachytenú aktivitu do centrálneho systému. Zachytené udalosti sú odosielané prostredníctvom systému Warden, ktorý slúži na efektívne zdieľanie informácií o detegovaných hrozbách medzi CERT/CSIRT tímami a bezpečnostnými zložkami. Udalosti je možné následne monitorovať cez SIEM systém Mentat prevádzkovaný v rámci e-infraštruktúry CESNET. Každý honeypot po registrácii a schválení sa stáva klientom Warden servera a začína automaticky zasielať udalosti. Systém je navrhnutý tak, aby po úvodnej konfigurácii nevyžadoval ďalší zásah správcu. Prípadná obnova klientských certifikátov aj prípadné aktualizácie sú automatizované [10].

Hugo využíva honeypoty pokrývajúce rôzne typy služieb a protokolov:

- **Cowrie** emuluje SSH a Telnet servery, zaznamenáva príkazy, stiahnuté súbory a použité prihlasovacie údaje.
- **Dionaea** je modulárny honeypot pokrývajúci protokoly ako SMB/CIFS, FTP, HTTP(S) či MS-SQL, zachytáva exploit kód a škodlivé binárne súbory.
- **Heralding** zbiera prihlasovacie údaje a deteguje brute-force útoky.
- **ADBHoney** deteguje útoky na rozhranie Android Debug Bridge.
- **ElasticPot** simuluje zraniteľný Elasticsearch server.
- **Conpot** emuluje priemyselné riadiace systémy (ICS/OT).
- **SNARE** a **TANNER** zabezpečujú simuláciu webových aplikácií.

Platforma tak spája decentralizované nasadenie u členských organizácií s centralizovaným dohľadom a zdieľaním dát, čo z nej robí vhodný nástroj pre kolaboratívny threat intelligence v akademickom a výskumnom prostredí.

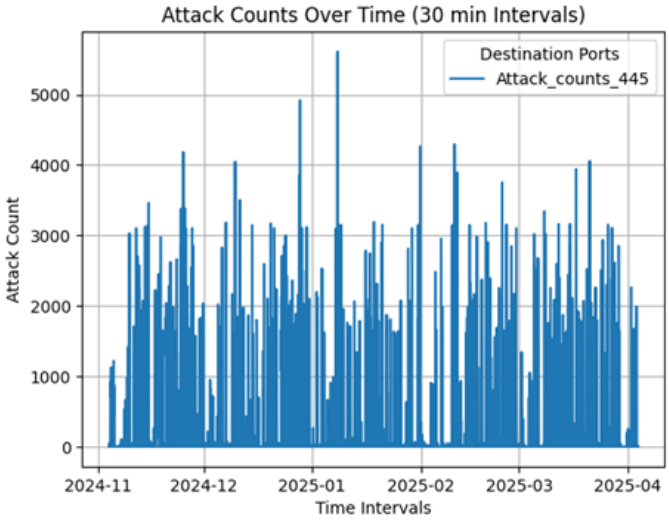
6 ANALÝZA DÁT

Analýza dát umožňuje identifikovať vzorce v správaní útočníkov, sledovať vývoj hrozieb v čase a odhaliť potenciálne slabiny v monitorovanom prostredí. Zistenia z tejto analýzy môžu slúžiť ako podklad pre návrh efektívnejších obranných opatrení v reálnych systémoch.

6.1 ANALÝZA ÚTOKOV NA SLUŽBY PODĽA PORTOV

Pri prevádzke honeypotov, ako aj pri zabezpečovaní reálnych systémov, je dôležité monitorovať, ktoré sieťové porty sú najčastejšie cieľom útokov. Vizualizácia týchto portov, napríklad pomocou histogramov, poskytuje cenný prehľad o tom, aké služby a protokoly sú zo strany útočníkov najviac vyhľadávané a zneužívané. Z praxe vyplýva, že niektoré porty predstavujú výrazne vyššie riziko ako iné. Napríklad port 445, ktorý je tradične spojený so službou SMB, sa často zneužíva v rámci ransomvérových kampaní, a preto by mal byť v prostredí, kde nie je nevyhnutný, úplne zablokovaný na úrovni firewallu (Obr. č. 3).

Dáta z honeypotov je možné exportovať do analytických nástrojov, ako sú Jupyter Notebooky, kde sa vykonávajú pokročilé analýzy. Tok dát typicky prebieha cez Elasticsearch API, pričom existujú aj notebooky s otvoreným kódom s preddefinovanými metrikami pre analýzu spravodajských hrozieb. Príkladom je verejne dostupný notebook publikovaný na platforme Kaggle [11], ktorý sa zameriava na identifikáciu vzorcov kybernetických hrozieb v dátach z honeypotov, ako aj notebook určený na analýzu logov Cowrie honeypotu, dostupný v repozitári GitHub [12].

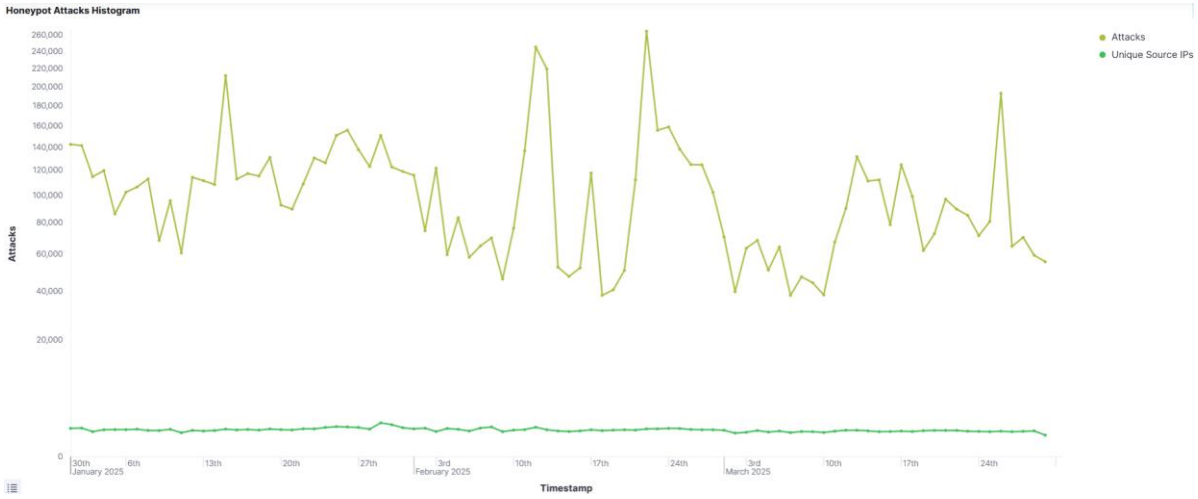


Obr. č. 3: Ukážka časového radu útokov na port 445.

Podobne port 5900, používaný na vzdialený prístup k ploche cez protokol VNC, býva často vystavený bez dostatočnej autentifikácie a predstavuje bezpečnostnú slabinu. Port 1433, slúžiaci na komunikáciu s databázovým serverom SQL, by nemal byť verejne dostupný bez adekvátneho zabezpečenia. Port 23, spojený so službou Telnet, je považovaný za zastaraný a nebezpečný najmä pre absenciu šifrovania, a jeho používanie by malo byť nahradené modernými alternatívami. Napokon, port 22, typický pre službu SSH, síce poskytuje šifrovanú komunikáciu, no pre svoju širokú dostupnosť je častým cieľom brute-force útokov. Preto sa odporúča implementovať viacfaktorovú autentifikáciu, prípadne zmeniť predvolený port a dôsledne sledovať prihlasovacie pokusy. Dôkladná analýza a ochrana najčastejšie zneužívaných portov predstavuje základný krok pri znižovaní rizika prieniku a zvyšovaní celkovej odolnosti systému voči útokom.

6.2 Analýza časových radov a histogramov

Analýza časových radov a histogramov nám pomáha určiť, aké trendy sa v ich aktivitách objavujú. Časové rady umožňujú sledovať, ako sa útoky vyvíjajú v čase, pričom môžeme vidieť, kedy aktivita stúpa a kedy klesá. Vďaka nim dokážeme rozpoznať dlhodobé trendy či opakujúce sa vzorce, ako sú napríklad denné alebo týždenné cykly útokov. No rovnako si vďaka nim môžeme všimnúť aj náhle výkyvy, ktoré často signalizujú prebiehajúce kampane alebo nové formy útokov. Na vizualizáciu týchto dát sa často používajú nástroje ako heatmapy alebo časové grafy. Tie pekne ukážu, v ktorých časoch je aktivita najvyššia.



Obr. č. 4: Ukážka histogramu z počtom útokov a unikátnych zdrojových adries za vybrané časové obdobie.

Histogram na Obr. č. 4 nám ukazuje, koľko útokov zachytili honeypoty v priebehu určitého časového obdobia. Sledujeme nielen samotný počet útokov, ale aj to, koľko unikátnych zdrojových IP adries za nimi stálo. Inak povedané, vieme rozlíšiť, či ide o nové zariadenia, ktoré sa do útokov zapájajú po prvý raz, alebo skôr o opakované pokusy známych aktérov. Z histogramu sa tiež dá vyčítať, či útoky prichádzajú v pravidelných vlnách, alebo či ide o nepretržitú, konštantnú aktivitu. Dôležitý moment nastáva, keď náhle stúpne počet unikátnych IP adries. Takýto nárast často naznačuje, že existujúce bezpečnostné opatrenia možno prestávajú byť účinné, alebo že došlo k ich narušeniu.

Pri samotnej interpretácii údajov je preto dôležité nepozerať sa len na to, koľko útokov prebehlo, ale rovnako podstatné je sledovať, z koľkých unikátnych IP adries pochádzajú. Ak vidíme prudký nárast nových adries, môže to byť znak toho, že sa šíri botnet alebo že ide o masívnu automatizovanú kampaň. Na druhej strane ak sa opakovane objavujú tie isté adresy, môže to naznačovať perzistentnú hrozbu z konkrétnych, známych zdrojov. Práve prepojenie týchto údajov, počtu útokov, jedinečných adries a časových vzorcov nám umožňuje lepšie porozumieť, čím daná činnosť je len bežný skript, koordinovaný útok, alebo niečo cielené.

6.3 ELASTICSEARCH

Medzi hlavne úlohy honeypotu/honeynetu je aj zber dát a údajov zo samotných systémov, ktoré simulujú zraniteľné služby. Jedným z hlavných cieľov je, aby tieto údaje mali praktickú hodnotu pre našu organizáciu, aby sme ich vedeli rýchlo a prehľadne monitorovať a analyzovať za cieľom získania lepšieho prehľadu o hrozbách pre prijatie efektívnejších opatrení a zvýšenia odolnosti našej organizácie. Pre tento krok využijeme Elasticsearch, ktorý využijeme na prácu s veľkým objemom záznamov. Elasticsearch je výkonný nástroj na zhromažďovanie a prácu z množstvom dát z rôznych senzorov. Dáta sa ukladajú vo forme dokumentov najčastejšie vo formáte JSON. To umožňuje ukladať rôznorodé údaje, od jednoduchých textových logov až po komplexne záznamy so sieťovými parametrami a časovými pečiatkami. Priložené skripty slúžia ako ukážka práce a spracovania údajov z Elasticsearch a následnej analytickej práce nad danými datami. Tieto skripty sú navrhnuté tak aby jednoducho demonštrovali rýchly spôsob analýzy nad základnými dopytmi.

ZÁVER

Honeypoty, honeynety a honeytokeny predstavujú v súčasnosti dôležitý doplnok bezpečnostných mechanizmov organizácie, najmä v oblasti monitorovania hrozieb, zberu indikátorov kompromitácie a budovania spravodajstve o kybernetických hrozbách (threat intelligence). Ich hlavnou hodnotou nie je len schopnosť zachytiť pokusy o útok, ale predovšetkým možnosť analyzovať správanie útočníkov, identifikovať trendy v cieľoch a technikách útokov a získať podklady pre prijímanie efektívnejších bezpečnostných opatrení. Správne navrhnutý a umiestnený honeypot dokáže poskytnúť relevantné údaje o prieskume, počiatočnom prístupe aj automatizovaných útokoch, pričom pri vhodnej kombinácii s honeytokenmi možno rozšíriť detekčné schopnosti aj na interné prostredie a laterálny pohyb útočníka.

Zároveň však platí, že efektivita týchto riešení závisí od realistickosti simulovaného prostredia, kvality správy zozbieraných údajov, primeranej miery izolácie a bezpečnostných opatrení, ako aj od schopnosti organizácie tieto dáta priebežne vyhodnocovať. Platformy ako T-Pot alebo Hugo ukazujú, že moderné honeypot riešenia dokážu výrazne zjednodušiť nasadenie, centralizovať zber dát a podporiť ich ďalšie zdieľanie a koreláciu. Analýza údajov z honeypotov, napríklad podľa portov, časových radov alebo unikátnych zdrojových adries, následne umožňuje lepšie porozumieť aktuálnej situácii o kybernetických hrozbách. Z pohľadu praxe preto honeypoty nemožno vnímať len ako pascu na útočníka, ale ako súčasť širšej stratégie obrany, ktorá prispieva k posilneniu bezpečnostného povedomia, k včasnej detekcii hrozieb a k dlhodobému zvyšovaniu kybernetickej odolnosti organizácie.

POUŽITÉ ZDROJE

[1] Spitzner, Lance. *Honeypots: tracking hackers*. Addison-Wesley Longman Publishing Co., Inc., 2002.

[2] Franco, Javier, Ahmet Aris, Berk Canberk, and A. Selcuk Uluagac. "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems." *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2351-2383.

[3] Sokol, Pavol, Ján Host, and Michal Vasko. "Data control in virtual honeynets based on operating system-level virtualization." *International Journal of Advanced Studies in Computers, Science and Engineering* 4, no. 9 (2015): 14.

[4] Cowrie Honeypot. [online] Dostupné z: https://github.com/cowrie/cowrie

[5] Dionaea Honeypot. [online] Dostupné z: https://github.com/dinotools/dionaea

[6] Honeytokens as active defense [online] Dostupné z: https://ieeexplore.ieee.org/abstract/document/7160478

[7] Javadpour, Amir, Forough Ja'fari, Tarik Taleb, Mohammad Shojafar, and Chafika Benzaïd. "A comprehensive survey on cyber deception techniques to improve honeypot performance." *Computers & Security* 140 (2024): 103792.

[8] Oficiálna príručka T-Pot. [online] Dostupné z: https://github.com/telekom-security/tpotce?tab=readme-ov-file#installation

[9] Repozitár projektu T-Pot. [online] Dostupné z: https://github.com/telekom-security/tpotce

[10] Hugo Platforma. [online] Dostupné z: https://hugo.cesnet.cz/en/index

[11] Honeypot Data: Insights into Cyber Threat Patterns. [online] Dosupné z: https://www.kaggle.com/code/hackandtoss/honeypot-data-insights-into-cyber-threat-patterns

[12] Cowrie Honeypot Log Analysis [online] Dostupné z: https://github.com/marcopedrinazzi/cowrie-honeypot-log-analysis/blob/main/cowrie_log_analysis.ipynb

PRÍLOHY

[1] attacks_ips.ipynb

[2] hps.ipynb

[3] time_series_analysis.ipynb