

Евалуација на можностите на T-Pot Honeypot

Габриела Гаврилова 191182

Бојана Димитријевска 193128

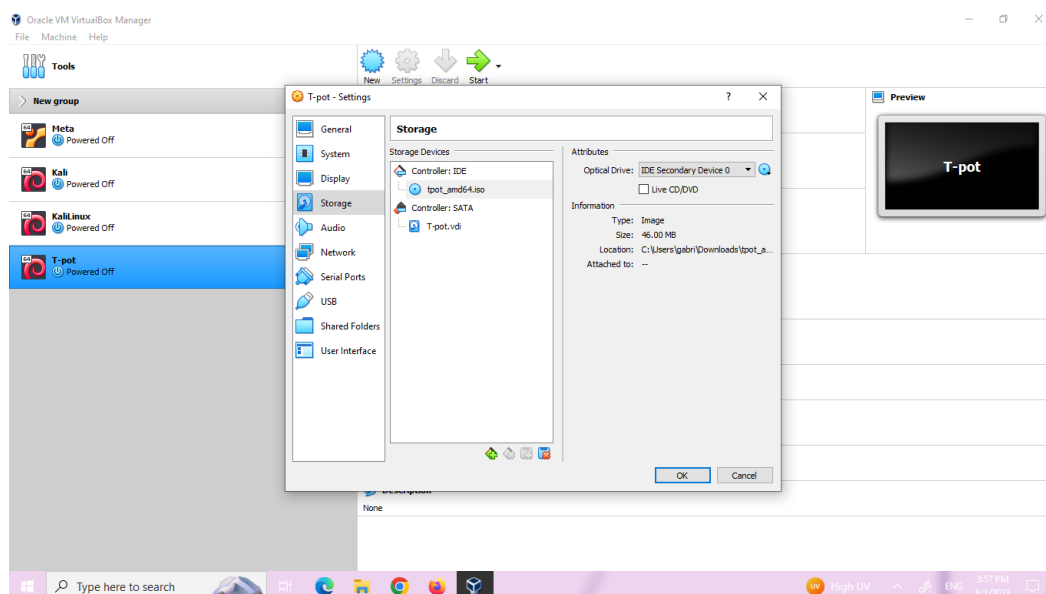
1. Што е Honeypot?

Honeypot е систем кој се користи како мамка за привлекување потенцијални напаѓачи и собирање информации за нивните активности. Honeypot, исто така често може да се користи за да се одвлече вниманието на напаѓачите подалеку од критични системи. Како резултат, Honeypot системите може да играат важна улога во заштитата на мрежата од софистицирани и аматерски напади. Има многу видови на Honeypot, оној што го истражувавме ние е Tpot Honeypot.

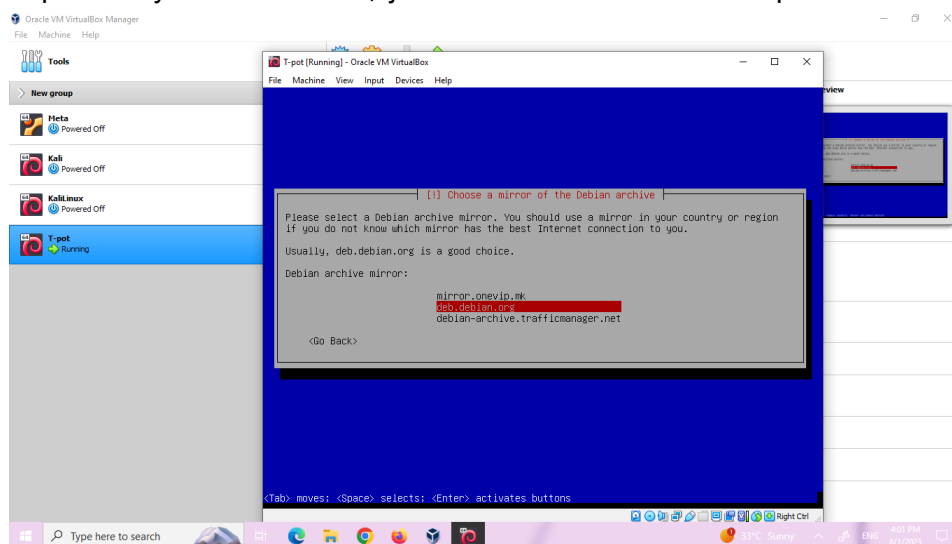
1.1 Tpot Honeypot

T-pot е open source проект кој е започнат од луѓе во Телеком. Комбира одлични технологии како што се Docker и Elasticsearch. T-pot може да функционира во виртуелна машина, на оперативен систем или како посебна виртуелна машина. Ние го инсталиравме како посебна виртуелна машина.

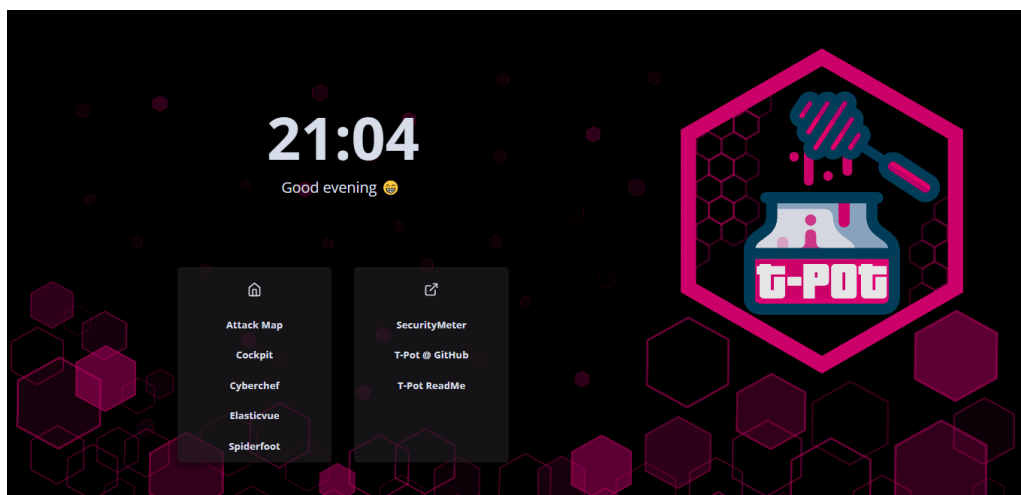
За да се инсталира правилно при креирање на виртуелната машина треба да се постават потребните барања и откако ќе се креира виртуелната машина треба да добие storage диск, .iso датотека која може да се преземе од Github.



Откако ќе се постават потребните барања за виртуелната машина, таа треба да се стартува и T-pot почнува со инсталација на сличен начин како Оперативен Систем.



Откако ќе се инсталира Tpot во веб пребарувач е достапен Dashboard-от на <https://localhost:64297>.



2. Алатки

При работа со T-pot Honeypot имаме голема варијација на сценарија и потсценарија кои можат да се изведат. По инсталација и конфигурацијата на T-pot имаме неколку основни алатки кои се користат. Во продолжение ќе ги опфатиме сите во неколку сценарија.

2.1 Прво сценарио: Работа со Cockpit

По покревање на апликацијата во VirtualBox ја пишуваме ip адресата, дадена за admin , во полето за адреси на вашиот browser , заедно со портата пишана до адресата. При првото вклучување во browser од вас се бара да внесете Username и Password кои при инсталација ги внесуваш како Username/Password за admin.

На тој начин влегуваме во серверот кој не поврзува со T-pot, и преку кој се прават некои клучни измени за негова ефикасна работа. Овој дел исто така се нарекува Cockpit и се вклучува пред главната страна на T-pot. Cockpit се користи во главно за активација на некои сегменти и карактеристики кои ги има вклучено T-pot во својата конфигурација.

Во овој дел ние ќе се фокусираме на некои полиња во главно, и тоа делот системот. Тој е одговорен да перцепира кој дел од нашата машина како работи и колкава им е преоптеретеноста. Пример CPU cores, memory, I/O disk, Network Traffic и тн. Потоа го имаме делот за сервиси, и овој дел ни кажува дали системот е правилно update-иран и дали е во добра состојба. И секако терминало кој најмногу се користи.

Во терминалот пишуваме команда `sudo su` за да пишуваме команди во root папката. Од тука ги внесуваме следните команди(една по друга, секако откако завршува предходната команда со извршување):

```
$systemctl stop tpot
```

```
$cd /opt/tpot/etc/
```

```
$curl -o tpot.yml https://raw.githubusercontent.com/munozrc/t-pot/main/compose/conpot.yml
```

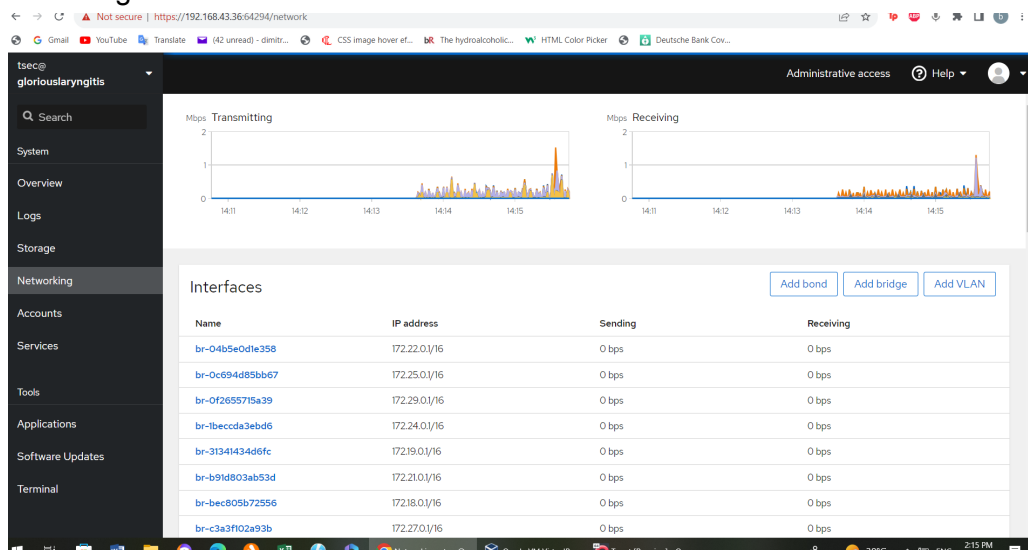
```
$systemctl start tpot
```

```
$dps.sh 1
```

Последната команда ги активира сите алатки на T-pot и може да потрае околу 5-10 минути, се со цел да се вклучат сите алатки правилно.

Оваа е неопходна постапка без која не можеме да ја вклучиме главната страна или корисничката страна на T-pot, без која не може да се користат главните функции на T-pot. Освен ова во терминалот можеме да направиме update за да се вклучат сите нови карактеристики и предности на алатката.

Можеме и да ја следиме работата на мрежата и колкава е оптеретеноста на истата, во делот Networking.



2.2 Второ сценарио: Работа со Kibana

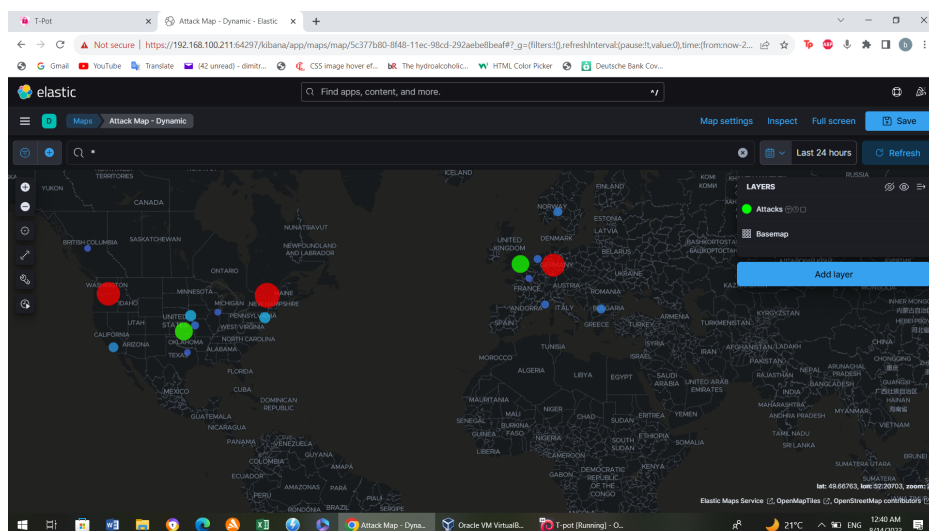
Наредното сценарио кое ќе го разгледаме е сценарио во кое ќе ја разгледаме алатката Kibana. Таа е алатка на која и треба одредено време да се стави во акција, по вклучување на T-pot.

Kibana е моќна алатка која содржи голем број на honeypots, чија улога е да детектираат, фаќаат и анализираат напади и напаѓачи од различен вид. На оваа алатка се вклучуваме преку главната страна на T-pot. По вклучување ни се покажува посебен

Dashboard на кој се дадени сите аналитички алатки кои можеме да ги користиме за анализа на напади. Ние имаме пристапено и примено напади на неколку различни honeypot алатки, но ќе опфатиме само неколку во овој дел.

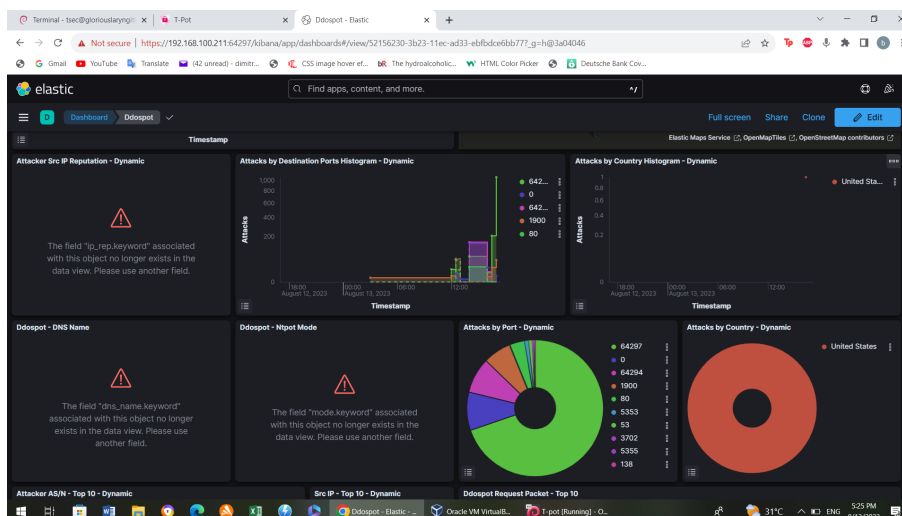
Прво ќе ја разгледаме cowrie алатката. Cowrie е honeypot со висока интеракција, дизајнирана да ги евидентира сесиите на SSH и Telnet од напаѓачите. Може да снима активности на командната линија, да собира интеракција со школка, па дури и да презема примероци од малициозен софтвер. По отварање на новит прозорец со Cowrie, можеме да видиме мапа на сесиите од десната страна кои биле детектирани од страна на оваа алатка.

Прикажани се неколку хистограми кои прикажуваат разни настани како напади прикажани според држава, според дестинациските порти, исто така има најдолу кои IP адреси ги имаат напаѓачите.



Втора алатка која ќе ја анализираме е Suricata. Suricata е софтвер со високи перформанси, со отворен код за анализа на мрежата и откривање закани, што е користена од повеќето приватни и јавни организации, а вградена од големите продавачи за заштита на нивните средства. Таа има некои слични аналитички способности како и сите останати алатки, има хистограми, пита, графови кои ги детектираат и покажуваат напаѓачите и познати детали за истите.

Трета алатка која ќе ја разгледаме е T-pot attack map dynamic. Оваа алатка е мапа на сите напади кои се насочени кон нашата мрежа. Можеме самите да одредиме колкав временски период да биде опфатен, почнувајќи од 1 секунда до неколку месеци. Таа прикажува напаѓачи во форма на кругови во разни големини и бои зависно од големината и бројот на напади кои се насочени кон нас. На десната страна каде што е прикажан делот за промена на временскиот период кој е опфатен, имаме и мала легенда која кажува која боја што означува.



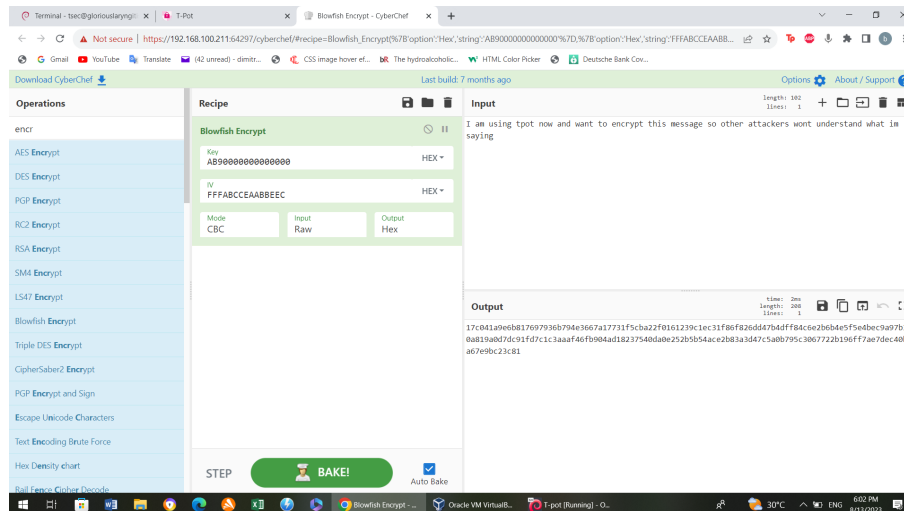
Покрај овие Kibana има и многу други можности и карактеристики но овие се главните кои најчесто се користат при вклучување на оваа алатка во вашата мрежа. Има делови за менаџмент и адаптирање на другите податоци зависно од барањето на корисникот итн.

2.3 Трето сценарио: Работа со CyberChef

CyberChef е бесплатна, веб-базирана алатка за безбедносна анализа, која има отворен-код и развиена од GCHQ (Штабот за комуникации на Владата на Обединетото Кралство), која е владина разузнавачка агенција. Во оваа алатка може да компресирате податоци, извлечете податоци, изведувате аритметички функции во однос на податоците и многу други функции.

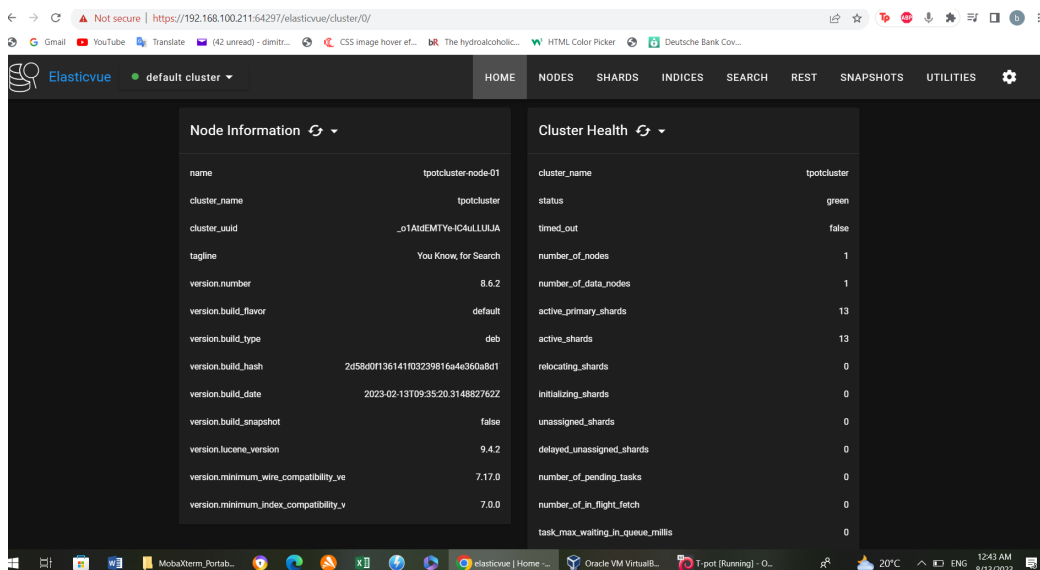
Се користи така што ја вклучуваме преку T-pot главната страна. По нејзино отварање, на екранот имаме четири прозорци, најлево на екранот се сите можности за кодирање и декодирање на текст, кои ги содржи оваа алатка. Во прозорецот веднаш до овој се наоѓа прозорецот во кој стои алгоритмот кој сме го избрале за енкриптирање на нашиот текст. Во него доколку се бара се додаваат клучеви за енкрипција или иницијализирачки вектор. Исто така може да се додаде во кој формат да биде дали хексадецимален дали децимален или слично.

Во двата прозорци од десната страна имаме прикажано дел за влезни единици и дел за излезни. Во горниот прозорец кој прима излезни единици внесуваме текст, кој сакаме да се шифрира и по кликање на големото зелено копче BAKE!, излезниот резултат односно енкриптираниот код е прикажан во прозорецот за output.



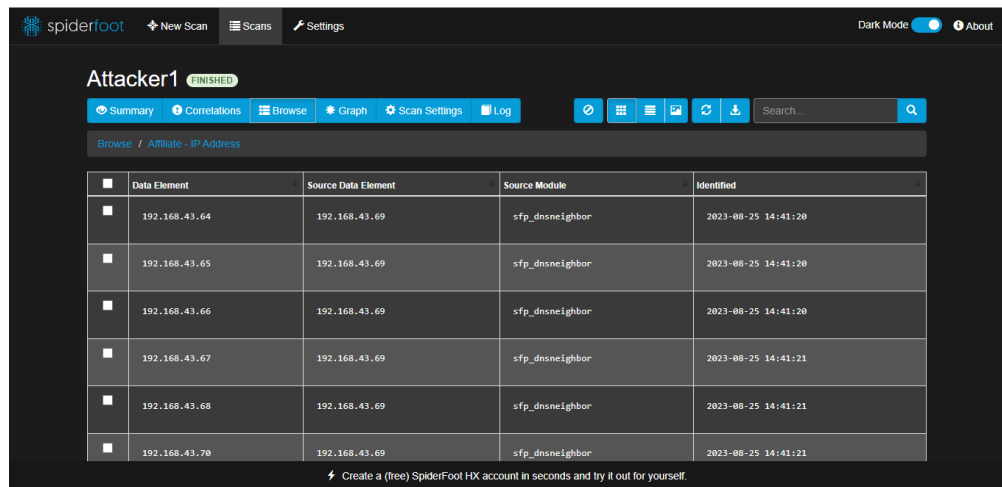
2.4 Четврто сценарио: Работа со Elasticvue

Во ова сценарио ќе ви отсликаме кои податоци ги чува Elasticvue односно веб-фронд за прелистување на податоците во вашиот кластер elasticsearch. Накратко кажано Elasticvue се користи за да се чуваат скриптите и сите log фајлови кои им се потребни на honeypots-от за да работат коректно . Таа ги чува ресурсите и новите ажурирања на апликацијата. Чува кластери и информации за секој индекс и секое id на добиените податоци. На некој начин служи како дата база. Освен овие карактеристики, Elasticvue не извржува никакви напади, анализи или пак визуелизации за разлика од предходните алатки на T-pot.



2.5 Петто сценарио: Работа со Spiderfoot

Откако откривме напади, истите може да ги истражваме со Spiderfoot. Spiderfoot е OSINT алатка дизајнирана да го автоматизира процесот на собирање информации за различни цели од јавно достапни извори на интернет. Наша цел беше да го откриеме дигиталниот footprint на напаѓачот и да откриеме со кои IP адреси е поврзан. За време на истрагата откривме список на придружни IP адреси поврзани со почетниот напаѓач. Сите адреси започнуваа со 192.168.43 што значи овие адреси припаѓаа на локална мрежа на корисници.

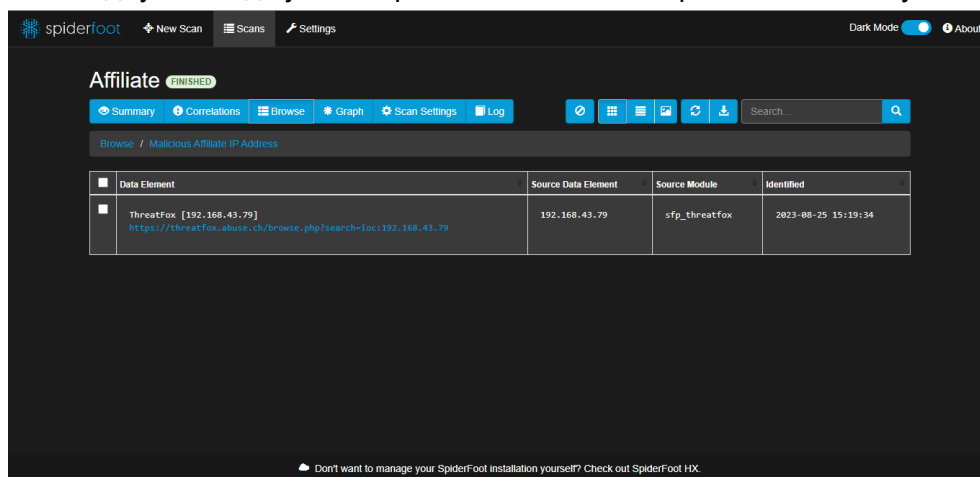


The screenshot shows the Spiderfoot web interface. At the top, there's a navigation bar with 'New Scan', 'Scans', and 'Settings'. The main header shows 'Attacker1' with a 'FINISHED' status. Below the header, there's a toolbar with buttons for 'Summary', 'Correlations', 'Browse', 'Graph', 'Scan Settings', and 'Log'. A search bar is also present. The 'Browse' button is active, and the breadcrumb trail shows 'Browse / Affiliate - IP Address'. The main content area displays a table with the following data:

	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	192.168.43.64	192.168.43.69	sfp_dnsneighbor	2023-08-25 14:41:20
<input type="checkbox"/>	192.168.43.65	192.168.43.69	sfp_dnsneighbor	2023-08-25 14:41:20
<input type="checkbox"/>	192.168.43.66	192.168.43.69	sfp_dnsneighbor	2023-08-25 14:41:20
<input type="checkbox"/>	192.168.43.67	192.168.43.69	sfp_dnsneighbor	2023-08-25 14:41:21
<input type="checkbox"/>	192.168.43.68	192.168.43.69	sfp_dnsneighbor	2023-08-25 14:41:21
<input type="checkbox"/>	192.168.43.70	192.168.43.69	sfp_dnsneighbor	2023-08-25 14:41:21

At the bottom, there's a prompt: 'Create a (free) SpiderFoot HX account in seconds and try it out for yourself'.

За подобра да ја разбереме ситуацијата, го искористивме Spiderfoot за да ги скенираме добиените адреси. За една од нив добивме IP адреса која Spiderfoot ја сметаше за малициозна па одлучивме да ја скенираме и неа, но скенирањето беше неуспешно.



The screenshot shows the Spiderfoot web interface. At the top, there's a navigation bar with 'New Scan', 'Scans', and 'Settings'. The main header shows 'Affiliate' with a 'FINISHED' status. Below the header, there's a toolbar with buttons for 'Summary', 'Correlations', 'Browse', 'Graph', 'Scan Settings', and 'Log'. A search bar is also present. The 'Browse' button is active, and the breadcrumb trail shows 'Browse / Malicious Affiliate IP Address'. The main content area displays a table with the following data:

	Data Element	Source Data Element	Source Module	Identified
<input type="checkbox"/>	ThreatFox [192.168.43.79] https://threatfox.abuse.ch/browse.php?search=loc:192.168.43.79	192.168.43.79	sfp_threatfox	2023-08-25 15:19:34

At the bottom, there's a prompt: 'Don't want to manage your SpiderFoot installation yourself? Check out SpiderFoot HX'.

3. Заклучок

T-Pot нуди сеопфатна и корисничка платформа која комбинира повеќе технологии на honeypot, обезбедувајќи интегрирана средина за следење, откривање и анализа на потенцијалните закани. Една од најистакнатите придобивки на T-Pot е неговата способност да фаќа податоци за напади во реално време, обезбедувајќи богатство од разузнавачки информации за закани што може да се преземат. Со привлекување на напаѓачите во контролирана средина, T-Pot им дава овластување на организациите да ги разберат техниките на напад, да ги идентификуваат ранливостите и да ги подобрат нивните одбранбени стратегии.

Со помош на алатките добивме сеопфатна и повеќеслојна перспектива за сложеноста на нападите со Honeypot. Во текот на процесот, стекнавме подлабоко разбирање за тоа како honeypots ефикасно ги имитираат вистинските системи, привлекувајќи потенцијални напаѓачи и овозможувајќи ни да ги набљудуваме нивните тактики и техники во контролирана средина. Од ова истражување научивме дека honeypots се системи за навремено предупредување, обезбедувајќи ни можност да откриеме, анализираме и разбереме закани пред тие да влијаат на нашите живи системи.

Дополнително, откривме дека honeypots може да играат клучна улога во собирањето информации за потенцијални напади. Со фаќање и анализа на шеми на напади, можеме да го подобриме нашето разбирање за заканите кои се појавуваат, да ги усовршиме нашите безбедносни мерки и да придонесеме за поширокото знаење на заедницата за сајбер безбедност.