Sustavi za praćenje napadača

Sustavi za praćenje aktivnosti napadača po svojoj složenosti daleko nadilaze sustave za privlačenje i detekciju napadača, jer moraju uz kvantitativne podatke pružiti i iscrpne podatke o napadu (odnosno kvalitativne podatke), ali očigledno obuhvaćaju i privlačenje i detekciju napadača. U većini slučajeva to su stvarna računala (dakle govori se o fizičkom honeypotu) koja su posvećena samo i isključivo praćenju aktivnosti napadača na sustavu. Potrebno je posvetiti cijeli sustav (ili njih više) kako bi napadač stvarno stekao dojam da se nalazi u pravom sustavu ili mreži.

Ovakvi sustavi mogu pokazati razinu sposobnosti pojedinog napadača, jer će se, na primjer, iskusniji napadači "potiho" približiti i provaliti, a zatim se pokušati sakriti i proširiti svoj utjecaj po mreži, dok će velika većina script kiddiesa provaliti na prva slobodna vrata, nespretno se pokušati sakriti i najvjerojatnije instalirati IRC bot ili nešto slično. Visokointeraktivne (high-interaction) honeypotove je potrebno mnogo čvršće izolirati od ostatka mreže, jer se napadač doslovno nalazi na sustavu, te postoji rizik od proboja u ostatak mreže. Pri izgradnji sustava može se postupiti na dva načina – instalirati čisti sustav (bilo direktno na računalo ili pomoću slike sustava u nekom alatu za virtualizaciju) te ga ručno podešavati i postavljati zamke ili iskoristiti već gotovo programsko rješenje koje se instalira na čisti sustav, a već sadrži uprogramirane alate za praćenje kao i usluge koje se mogu omogućiti (npr. programski paket Argos o kojem će kasnije biti govora).

Ukoliko se želi postaviti cijeli sustav, tada treba paziti na nekoliko već navedenih stvari. Kao prvo, bitno je odabrati pogodan operacijski sustav – obično se odabere neka distribucija operacijskog sustava Linux jer je prilagodljiviji potrebama pojedinca nego operacijski sustav Windows. Nakon instalacije, prvo je potrebno izolirati honeypot tako da mu se može pristupiti samo iz lokalne mreže (za početak, u svrhe testiranja). Korištenjem alata VMWare za virtualizaciju to je moguće postići korištenjem NAT (engl. Network Address Translation) postavki mreže. Kada se honeypot konfigurira, tada se može otvoriti prema Internetu korištenjem bridged networkinga. Bridged networking omogućava da se sustav instaliran u alatu VMWare ponaša kao „zaseban" sustav, odnosno mrežni promet ne prolazi proces preslikavanja mrežnih adresa (ne stvara se nova lokalna „podmreža" na računalu, nego se dobije IP adresa lokalne mreže u kojoj se nalazi računalo na kojem je instaliran sustav u alatu VMWare). Kod izolacije sustava potrebno je omogućiti dolazne konekcije, ali onemogućiti izlazne (da se sa sustava ne može slati mrežni promet na druge sustave), jer bi u suprotnom napadač mogao pomoću honeypota dalje napadati potencijalne mete. No, mora se pažljivo ograničiti napadača, jer ukoliko mu se zabrane sve izlazne veze, mogao bi postati sumnjičav (pogotovo iskusniji napadači) i npr. obrisati čvrsti disk sa svim spremljenim podacima o napadima. Tako se mogu izgubiti podaci dugotrajnog istraživanja, a to nije u interesu. Nakon izolacije mreže, potrebno je prilagoditi sustav da izgleda "normalno" – dodati imena korisnika, postaviti neke skripte da se periodički izvršavaju, spremiti neke lažne podatke i slično. Uglavnom, bilo što samo da sustav izgleda što je autentičnije moguće. Zatim slijedi postavljanje alata za praćenje aktivnosti. Potrebno je omogućiti arhiviranje svih pokrenutih naredbi ili jednostavnije instalirati keylogger. Keylogger je program koji prati svaku pritisnutu tipku na sustavu. Osim praćenja pritisnutih tipki, potrebno je pratiti i sav mrežni promet i po mogućnosti, slati dnevničke datoteke prometa na neki drugi poslužitelj ili ih lokalno kriptirati, kako bi se kasnije mogli analizirati, ali da ne probude sumnju napadača. Jedan od primjera programa koji prati mrežni promet (engl. sniffer) jest tcpdump. Lako se instalira (dolazi instaliran skoro sa svakom distribucijom Linux operacijskog sustava), a ne opterećuje previše procesor. Potrebno je omogućiti praćenje izvođenja sistemskih poziva, u slučaju pokretanja programa koji lokalno iskorištavaju ranjivosti, ili za slučaj otkrivanja novih načina napada (0-day ranjivosti). Osim instalacije programa za praćenje, potrebno ih je i sakriti, jer se svi pokrenuti procesi na Linux operacijskom sustavu vide naredbom "ps". To se obično ostvaruje korištenjem sličnih principa kao što

su rootkitovi – uobičajene naredbe “ls”, “ps” i slično se zamjenjuju ekvivalentnim naredbama, koje ne ispisuju određene podatke. Time se može maskirati izvođenje prisluškivačkih programa na honeypotu. Slijedi instalacija zamki – to su najčešće ranjivi servisi, poput ranjivih FTP (engl. File Transfer Protocol) i Telnet programa, ranjivih aplikacija za elektroničku poštu, HTTP poslužitelja i slično. Potrebno je napraviti što “šareniji” sustav kako bi se privukli različiti napadači, jer ne raspolažu svi sa istim znanjem. Kad se sve postavi, potrebno je prvo iscrpno lokalno testirati honeypot na mogućnost probijanja u ostatak mreže, a zatim je potrebno omogućiti honeypotu izlazak na Internet i čekati rezultate.

Argos je virtualni visokointeraktivni honeypot razvijen na sveučilištu Vrije Universiteit u Amsterdamu. Ovaj alat prvenstveno služi za otkrivanje novih (0-day) ranjivosti. Način na koji se ostvaruje ta funkcionalnost jest da se prati sav mrežni promet, te se prati korištenje tog mrežnog prometa koji je spremljen u memoriji (npr. “čudne” JMP instrukcije, koje obično karakteriziraju buffer overflow napade), a zatim se na temelju izvršavanja generira “otisak memorije” (memory footprint) napada. Taj koncept se naziva dinamička analiza kvara (engl. dynamic taint analysis).

Sustavi za praćenje napadača se mogu ekvivalentno koristiti u svrhu podučavanja o računalnoj sigurnosti, jer su obično postavljeni isti zahtjevi na takvu vrstu sustava. Na takvim sustavima, korisnici mogu isprobavati i uvježbavati razne vrste napada bez pravnih posljedica, što inače mnoge odvrati od eksperimentiranja iako su željni znanja.