Sustav za poučavanje i automatsku evaluaciju tehnika napada na informacijske sustave

Uvod

Računalna sigurnost je vrlo veliko i kritično područje u računarstvu. Kako ovo područje raste, postaje sve teže pratiti načine zaštite što povlači težu obranu računalnih sustava od neželjenih napada. Prije četrdesetak godina, na računalima su mogle raditi samo privilegirane osobe, dok danas skoro pa svatko bez problema koristi daleko naprednije sustave. Zbog velike dostupnosti informacija na Internetu, danas "hakerom" može postati svatko. No, taj naziv je preopćenit za današnju situaciju, pa tako na Internetu možemo pronaći finiju podjelu "hakera": script kiddies, blackhats, greyhats, whitehats i ostali. Podaci o zastupljenosti „naprednijih" korisnika na Internetu i njihovim motivima, dobivena je iz mjerenja aktivnosti napadača na posebno osmišljenim sustavima koji služe za otkrivanje tehnika i praćenje napada. Takvi sustavi su osmišljeni s jednom jedinom svrhom – da se izlože Internetu kako bi se olakšalo otkrivanje uobičajenih i potencijalno novih napada na sustave, te kako bi se whitehat skupini omogućio bolji uvid u način razmišljanja napadača u svrhu razvijanja novih i naprednijih načina obrane. Takvi sustavi zovu se honeypots. Također, postoje i slični sustavi koji su namjerno ranjivi, a služe za edukaciju pojedinaca u polju računalne sigurnosti, kako bi im se omogućio siguran (odnosno legalan) način vježbanja i isprobavanja tehnika napada. U ovom radu objašnjen je rad nekoliko vrsta sustava – sustava za privlačenje i detekciju napadača (engl. low-interaction honeypots), sustava za praćenje napadača (engl. high-interaction honeypots), te sustava za poučavanje. Osim toga, dan je i primjer dizajna i konfiguracije jednog takvog sustava koji bi se mogao u budućnosti implementirati.

Vrste sustava za automatsku evaluaciju tehnika napada na informacijske sustave

Kao što je spomenuto u uvodnom poglavlju, postoje dvije vrste sustava za evaluaciju. To su:

- Sustavi za privlačenje i detekciju napadača
- Sustavi za praćenje napadača

Dizajn i primjena sustava za poučavanje i automatsku evaluaciju tehnika napada na informacijske sustave

Sustavi za poučavanje i automatsku evaluaciju tehnika napada su vrlo korisni u mnogim situacijama – bilo da se želi voditi statistika pokušaja napada, ili da se želi podučiti korisnike naprednijim aspektima sigurnosti. Koliko god se Internet smatrao sigurnim mjestom, implementacija ovakvog sustava za praćenje i automatsku evaluaciju tehnika napada bi mogla otkriti uzbunjujuću realnost da to i nije u potpunosti istina. Testni sustavi postavljeni na Internet bili su kompromitirani u nekoliko minuta. Zasigurno bi svaki vlasnik nekakvog Internetskog biznisa htio otkriti kolika je vjerojatnost proboja u

njegov sustav – a to se vrlo lako može postići stvaranjem “duplikata” sustava, samo s omogućenim dodatnim praćenjem. To je dugoročno vrlo pametna investicija, jer time osim što se pojedinac štiti, aktivnim sudjelovanjem u zajednici (HoneyNet project) može pridonijeti dodatne statističke podatke. Također, u znanstvenim krugovima, pogotovo vezanim za sigurnost, uvijek se istražuju novi načini obrane sustava od napadača. To predstavlja vrlo velik problem, jer se za “velike rupe” zna samo u određenim krugovima. Krugovi u kojima takvi podaci kolaju su najčešće zatvoreni, pa je time teže dobiti uvid na moguće propuste u sustavima. Propust se u nekom trenutku mora iskoristiti, pa je moguće uhvatiti otisak napada (engl. footprint) na određenu uslugu ili sustav, koji se kasnije podvrgava detaljnoj analizi. Osim praćenja i evaluacija tehnika napada, vrlo česta primjena ovakvih sustava je u edukaciji (budućih) sigurnosnih stručnjaka. Ovakvi sustavi se mogu koristiti na barem tri načina: kao sustave za prikupljanje materijala za forenzičku analizu (npr. za buduće računalne forenzičare), kao sustave za isprobavanje tehnika napada s kakvima se možemo susresti u stvarnom svijetu (npr. za buduće stručnjake sigurnosnih proboja), ili kao sustave za analizu zloćudnih programa (npr. analiza virusa, crva, trojanskih konja i sličnih programa). Krajnji cilj je u konačnici isti – pružiti sigurno okruženje budućim stručnjacima (ili zainteresiranima) za isprobavanje različitih tehnika napada i obrade podataka nepoznatog podrijetla, te vježbanje odziva na incidente (engl. incident response). Razmotreni su mogući pristupi dizajnu dvaju sustava:

- Sustav za automatsku evaluaciju tehnika napada
- Sustav za poučavanje

Prijedlog praktične implementacije

Zbog istraživanja uobičajenih načina ponašanja napadača, potrebno je implementirati sustav za praćenje napadača i automatsku evaluaciju tehnika napada. Budući je odlučeno da se želi napraviti sustav za praćenje napadača, to za sobom povlači da je potrebno implementirati visokointeraktivni honeypot. Preporuča se odvojiti zasebno računalo za implementaciju sustava, kako bi se mrežni promet mogao izolirati i fizičkim komponentama, čime se smanjuje rizik za ostatak mreže. Sustav bi bio pokretan nekom distribucijom operacijskog sustava Linux. Prijedlog nekih osnovnih sigurnosnih propusta bio bi ranjiv SMTP servis, kako bi se privuklo spammere, te ranjiv ftp servis i HTTP servis (npr. neka starija verzija Apache HTTP poslužitelja), kako bi se privukli ostali napadači. Na sustavu je potrebno omogućiti praćenje i filtriranje mrežnog prometa pomoću programa tcpdump (filtriranje se može naknadno napraviti korištenjem skripti), ali je potrebno prikriti izvođenje programa mijenjanjem naredbi (npr. izmijeniti naredbu ps da se ne prikazuju određeni procesi). Osim toga, potrebno je instalirati i keylogger (npr. LKL Keylogger), čije je izvođenje također potrebno sakriti kako napadač ne bi posumnjao. Potreba za instalacijom ovog tipa programa je što je mehanizam arhiviranja naredbi bash ljuske lako zaobići pokretanjem neke druge ljuske. Također, bilo bi korisno implementirati i periodičko uzimanje “slike” sustava (odnosno ključnih datoteka, dnevničkih datoteka i sl.) te njihovo kriptiranje i slanje na neki drugi sustav kojem nije moguće pristupiti nekim drugim načinom, kako bi se podaci očuvali u slučaju da napadač otkrije zamku, a i kako bi se mogle pratiti izmjene i napadačevi pokušaji prikrivanja svoje aktivnosti. Potrebno je izolirati i sav izlazni mrežni promet pomoću alata iptables (ili nekom sličnom varijantom programskog vatrozida), ali omogućiti ulazni promet na mrežnim priključcima za zadane servise. Osim svih postavljenih alata za praćenje, postoji i mogućnost stavljanja nekih nasumičnih podataka na sustav kako bi se napadaču činilo kako se sustav i inače koristi za neku svrhu (preočito je da na sustavu nema nikoga osim njega). Po završetku istraživanja, moguće je napraviti ekstrakciju značajki iz dnevničkih datoteka, na temelju čega bi se moglo naučiti modele koji bi automatski mogli profilirati napadača, i olakšati prepoznavanje istog ako ponovno napadne.