SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 000

Praćenje upotrebe računala radi detekcije neovlaštenog korištenja

Belma Gutlić

Zagreb, svibanj 2017.

Umjesto ove stranice umetnite izvornik Vašeg rada.
Da bi ste uklonili ovu stranicu obrišite naredbu `\izvornik`.

SADRŽAJ

1. Uvod

Sigurnost na internetu oduvijek je osjetljivo područje prvenstveno zbog velike i raznolike upotrebe širom svijeta. U 2017. godini zabilježeno je da blizu 50% svjetskog stanovništa koristi internet [1]. To je skoro 4 milijuna korisnika, što znači i 4 milijuna potencijalnih žrtvi cyber napada. Većina ih misli kako nisu ugroženi ili uopće ne razmišljaju da bi mogli postati žrtvom bilo kakvog napada. To često rezultira krađom podataka i korisničkih računa (uključujući i one za upravljanje financijama), krađom identiteta ili plaćanjem otkupnine zbog zaključavanja računala malicioznim programom ransomware. Napadi su najveći problem za tvrtke i organizacije zbog krađe osjetljivih podataka, narušavanja rada usluge ili rada zaposlenih, što dovodi do gubitka kredibiliteta odnosno povjerenja klijenata, ali i velikih financijskih gubitaka.

U zaštiti računala prvu liniju obrane čine antivirusne zaštite koje je potrebno redovito ažurirati. Kako napadači stalno razvijaju nove oblike prijetnji, neophodno je stalno ažuriranje i nadogradnja postojećih sigurnosnih sustava. Antivirusi i većina sličnih programa za otkrivanje prijetnji temelji se na tehnikama prepoznavanja uzorka (potpisa) za koji se već zna da je indikator zloupotrebe. Međutim, pomoću tehnika strojnog učenja moguće je na temelju podataka korisnika napraviti sustav za otkrivanje anomalija u korisnikovom ponašanju, odnosno detektiranje neovlaštenog korištenja računala. Izgradnja takvog sustava koji će pokušati detektirati prijetnje na Internetu ili lokalnoj mreži je cilj ovog rada.

U drugom poglavlju navedeni su postojeći radovi...

2. Postojeći radovi

3. Prijetnje na računalu

4. Prikupljanje podataka o korisnikovom ponašanju

4.1. Osquery

Tablica 4.1: Example of an table

Relacija	Opis sadržaja relacije	Upotreba relacije
chrome_extensions	Instalirani dodatci preglednika Google Chrome.	Novi dodatci mogu biti zloćudni ili utjecati na sigurnosni propust.
firefox_addons	Instalirani dodatci preglednika Mozilla Firefox.	Najčeće korišteni i najrazvnijeniji preglednici.
usb_devices	Aktivni USB uređaji.	USB uređaji su često korišteni sa neovlaštenim fizičkim pristupom.
deb_packages	Instalirani DEB paketi.	Instalacija nekih novih paketa može biti neuobičajena.
kernel_modules	Pokrenuti kernel moduli.	Korištenje kernel modula govori o upotrebi programa i sistemskih poziva.
iptables	Filteri vatrozida.	Uklanjanje pravila vatrozida može nagovijesiti neovlaštenu akciju.
etc_hosts	Identifikacija mrežne komunikacije koja se preusmjerava.	Preusmjeravanje odredišta često nije željeno ponašanje.
last	Sve prijave i odjave korisnika.	Detekcija neovlaštenih upada sa različitim korisničkim računima i virtualnim konzolama (tty).
open_sockets	Otvorene pristupne točke svakog procesa.	Procesi se mogu vezati na neuobičajena lokalna ili udaljena vrata.

Nastavak na idućoj stranici

Tablica 4.1 – *Nastavak*

Relacija	**Opis sadržaja relacije**	**Upotreba relacije**
open_files	Otvoreni dokumenti svakog procesa.	Identifikacija korištenih procesa koji otvaraju osjetljive dokumente.
shell_history	Povijest naredbene linije.	Korištenje naredbi je osnovno ponašanje kod Linux korisnika.
ramdisk[1]	Napadači često pokreću privremene memorije.	
listening_ports	Procesi sa otvorenim vratima.	Poznati procesi slušaju na određenim vratima, mogućnost pronalaska backdoora.
suid_bin	Datoteke koje imaju SUID (Set User ID) privilegije.	Mogućnost detekcije backdoor datoteka i potencijalnih ranjivosti.
arp_cache	Vrijednosti tablice Address resolution komunikacijskog protokola.	Protokol se koristi kod MITM napada.

[1] select * from block_devices where type = 'Virtual Interface';

5. Strojno i duboko učenje

5.1. LSTM

6. Sustav za predviđanje ponašanja korisnika

6.1. Upotreba neuronske mreže

6.2. Eksperimentalni rezultati

7. Zaključak

Zaključak.

8. Literatura

[1] Internet World Stats. http://www.internetworldstats.com/stats.htm. Accessed: 2017-05-02.

Praćenje upotrebe računala radi detekcije neovlaštenog korištenja

Sažetak

Sažetak na hrvatskom jeziku.

Ključne riječi: Ključne riječi, odvojene zarezima.

Monitoring user behavior on a computer system to detect unauthorized use

Abstract

Existing security solutions are mostly based on preventing known malicious threats or a defined set of rules and therefore most outside and inside threats end as successful attacks. In this paper, the proposed system is an adaptive user action identifier, which can predict and detect anomalous behavior in real time based on user and entity behavior analytics (UEBA). In this work an Osquery framework has been used to acquire user actions logs from Linux host and the implementation of machine learning algorithms to predict user's next step and identify it as malicious or not.

Keywords: UEBA, machine learning, neural network, anomaly detection