# Dnevnik rada

## 1. tjedan (26.3-1.4.2018)

#### Dosadašnji rad

Reinstalacija virtualnog labaratorija, da se pobriše sve nepotrebne stvari nastale kod stvaranjal labaratorija na Projektu.
Dodan još jedan IDS/IPS sustav Surikata.

#### Daljnji koraci

Konfigurirati web application firewall Shadow Daemon. Sa asistentom dogovoriti detalje projekta.

---

## 2. tjedan (2.-8.4.2017)

Dosadašnji rad

Uspješna konfiguracija Shadow Daemona, dogovoreni daljnji koraci na projektu s asistentom.

Daljnji koraci

Proučiti web crawlere i generatore podataka pogodne za testiranje Waf-ova i IDS/IPS ova.

---

## 3. tjedan (9.-16.4.2018)

#### Dosadašnji rad

Prilagodba virtualnog sustava za instalaciju raznih sigurnosnih uređaja, također sam počeo pisati dokumentaciju/upute kako sigurnosne sustave instalirati na sustav. Informirao sam se o generatorima prometa i snimkama prometa te kako ih slati kroz mrežu, ali još nisam točno odlučio što koristiti.

#### Daljnji koraci

Pokušati konfigurirat neki generator prometa ili snimku prometa, te pisati dalje dokumentaciju.

## 4. tjedan (16.-23.4.2018)

**Dosadašnji rad**

Učenje za međuispite.

**Daljnji koraci**

Predati inicialni završni rad.

## 5. tjedan (23.4.-30.4.2018)

**Dosadašnji rad**

Podigao dvije nove Ubuntu virtualne mašine za IDS/IPS tester Pytbull, konfigurirana je napadačka i žrtvina strana. Sa asistentom treba dogovoriti kako alert.log dohvačati koji generira IDS/IPS.
Instaliran OWASP WebScarab za web crawlera, konfiguriran proxy, te sam se malo igrao sa spiderom i promjenom POST vrijednosti nakon što su poslane prema web aplikaciji.

**Daljnji koraci**

Dogovoriti sa asistentom dali će IDS/IPS ostati na pfSense routeru ili će se konfigurirati na žrtvnim računalima.

## 6. tjedan (30.-6.5.2018)

Pronađeno rješenje za testiranje IDS/IPS/a sa starim konfiguracijom snorta i suricate na pfsensu. Na pitbullu je izmjenjen source kode tako da čita IP adresu na kojoj se nalazi FTP server sa generiranim alert datotekama od strane snorta i suricate , te je u konfiguracijsku datoteku dodana linija u koju su upiše adresa FTP servera. Obavljena su prva testiranja sa pytbullom i dobiveni inicijalni rezultati. Dopisana izmjenjena konfiguracija u završni rad, te su dodane opisu konfiguracija Snorta i Suricate.

## Daljnji koraci

Provjeriti s asistentom slučaj oko licenci zbog izmjenje koda iako bi trebalo biti uredu jer je pytbull izdan pod General public licencom.
Konfigurirat ostale alate i započet testiranja.

## 8. tjedan (29.11.-5.12.2017)

**Dosadašnji rad**

Podizanje virtualnih mašina i pokušaji prvih testiranja WAF-ova.

**Daljnji koraci**

Nastaviti testiranje, i početi razmatrati kako testirat druge sigurnosne alate.

### 10. tjedan (12.12.-19.12.2017)

**Dosadašnji rad**
*Izabrano korištenje open source alata waf-testbed koji će služiti kao virtualni sustav za testiranje sigurnosnih alata.*
*Dolazi sa instaliranim Apache2 servisom i također WAF-om Mod Security koji je konfiguriran s verzijom 3.0.2 Owasp sigurnosnih pravila.*
*Za pokretanje skripti koje je će testirati Owasp pravila koristit će se open source alat Framework for Testing WAF-s (FTW) koji će primati*
*testove u YAML formatu. Svi alati su javno dostupni na gitu.*

*Pomoću alata Vagrant, waf-testbed je uspješno implementiran u virtualnoj mašini. Javljau se neki problemi s pokretanjem Apache2 servera.*

### *Daljnji koraci*

Uz navođenje asistena do kraja konfigurirat sustav i dobiti prve rezultate ispitivanje Mod Security pravila.

### 11 . tjedan ( 20 .12.- 26 .12.2017)

**Dosadanji rad**

*Uspješno pokrenut Apache2 server, problem je bio što je u konfiguracijskoj datoteci zadani port već bio korišten od strane operacijskog sustava. ModSecurity je uspješno pokrenuti ispred Apache2 servera sa Owasp sigurnosnim pravilima, te je postavljen u samo u detection*
*mode, a razlog je da Framework for Testing WAF-s može detektirati koja su sigurnosna pravila podignuta kod određenih napada, te time odrediti koji su napadi bili uspješni, a koji ne.*
*Uspio sam pokrenuti neke od testova sa FTW-om, ali se još javljaju neki errori za koje nisam siguran što znače.*

*Imperva je poslala svoj WAF testing framework nakon mjesec dana.*

### *Daljnji koraci*

Pokušati pokrenuti FTW sa cjelokupnim SQL injection i XSS scripting napadima, te također podignuti Impervin waf testing framework za koji
je potrebna Windows virtualna mašina, te na kraju odlučiti sa asistentom što koristiti.

### 12. tjedan (27.12.- 3.1.2018)

**Dosadanji rad**

Instalirao sam Windows na virtualnoj mašini, te uspješno instalirao Imperva WAF testing framework i pokrenuo webGoat na Tomcat serveru.
Pokrenuo sam napade na WebGoat i dobio izvještaj o uspješnosti napada na WebGoat aplikaciju, ali bez pokrenutog modSecurity-a da štiti aplikaciju. Nisam točno siguran kako instalirati modSecurity na Windowsima, pa sam napravio još virtualnu mašinu koja ima za operacijski sustav Security Onion koji je baziran na Ubutnu sustavu.

Uspio sam pokrenuti napade s Windows virtualne mašine na WebGoat aplikaciju koja je pokrenuta na Security Onion virtualnoj mašini, te sada još moram nekako instalirat modSecurity.

Također nisam uspio još natjerati framework for testing waf-s(FTW) da uspješno provede sve napade.

### *Daljnji koraci*

Konfigurirat modSecurity i SNORT na Security Onion-u, te dalje raditi na problemu sa FTW-om.

## 13. tjedan (3.1.- 10.1.2018)

### Dosadanji rad

Snort je konfiguriran i radi, sad još treba složiti virtualni labaratorij u virtualboxu. Snort da radi u IPS načinu mora biti postavljen između dvije mreže da može pregledavati pakete. Cilj je imati virtualnu mašinu sa ranjivom aplikacijom, te drugu sa koje se pokreću napadi, te između njih imati SNORT ili pfSense koji će provjeravati i prosljeđivati promet sa jedne na drugu mrežu. Neznam dali ću uspjeti složiti FTW.

### *Daljnji koraci*

Dovršiti virtualni labaratorij i generirati izvještaje o uspješnosti napada.

## 14. tjedan (10.1.- 17.1.2018)

### Dosadanji rad

Korištenjem mod_jk plugina uspješno sam uspio povezati Tomcat i Apache server. Ispred Apache servera je složen i konfiguriran modSecurity, a na Tomcatu je ranjiva web aplikacija WebGoat. Uz pomoć Imperve uspješno sam napao WebGoat na Tomcatu, te sam dobio rezultate napada.
Snort i virtualni labaratorij su uspješno konfigurirani.

### *Daljnji koraci*

Spojiti dvije interne mreže u virtualnom labaratoriju preko Snorta i pokrenuti napad.
Napraviti prezentaciju i dovršiti dokumentaciju.