Dnevnik rada

1. tjedan (26.3-1.4.2018)

Dosadašnji rad

Reinstalacija virtualnog labaratorija, da se pobriše sve nepotrebne stvari nastale kod stvara
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 pi
dokumentaciju/uputе kako sigurnosne sustave instalirati na sustav. Informirao sam se o genera
prometa i snimkama prometa te kako ih slati kroz mrežu, ali još nisam točno odlučio što koris

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 inicijalni završni rad.

5. tjedan (23.4.-30.4.2018)

Dosadašnji rad

Podigao dvije nove Ubuntu virtualne mašine za IDS/IPS tester Pytbull, konfigurirana je napadačk
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 spider
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 z
računalima.

6. tjedan (30.-6.5.2018)

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

Daljnji koraci

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

8. tjedan (6.5.-13.5.2018)

Dosadašnji rad

Prepravak završnog rada po uputama primljenih od asistenta. Daljnje izvođenje napada s pytbull

Daljnji koraci

Pisanje rada, početak prvih evaluacija.

10. tjedan (13.5.-21.5.2018)

Dosadašnji rad
Nadopunjen završni rad sa konfiguracijama ostalih alata. Traženje adekvatne snimke internetskog pro
Poslan mail Kanadskom institutu za CyberSecurity u nadi da pošalju vlastiti PCAP za testiranje IDS
koji bi se u mreži mogao pokrenuti preko pytbulla.

Daljnji koraci

Započeti evaluaciju sigurnosnih sustava i nastavit pisanje rada.

11. tjedan (21 - 28.5.12.2018)

Dosadanji rad

Instaliran SQLMap. Zbog nedostatka tutorija za korištenje SQLMapa sa WebGoat-om koji je pisan
i javascriptu instalirana je još jedna ranjiva web aplikacija bwapp koja je pisana u php-u. Za
instalirani i mySql baza podataka i php na žrtvinu Windows virtualnu mašinu.

Zbog novije verzije php-a aplikacija koristi puno metoda koja su sada depricated u php-u.
Uspješno je popravljen php kod za adekvatnu demonstraciju rada SQL-mapa.

Naučio sam kako koristiti neke postavke SQLMapa i izvoditi napade.

U pytbullu nisam siguran kako detektirati client side attacks.

Daljnji koraci
Iskoristiti SQLMap za adekvatnu evaluaciju WAF-ova, pokušat iskoristi SQLMap na WebGoatu jer j
konfiguracija bWappa sa preinakom izvornog koda dota teška. Pitati asistenta za savjet oko Pyt

12. tjedan (28.5.- 3.6.2018)

Dosadanji rad

Nakon učenja SQLMapa shvatio sam kako je uz pomoću BurpSuita moguće napadati WebGoat
stranice, tako da se bWapp odbacuje i testiranje SQLMapa će se odvijati uz dosadašnju konfigura

Daljnji koraci

Napisati rad i predati ga na recenziju.

13. tjedan (3.1.- 10.1.2018)

Dosadanji rad

Snort je konfiguriran i radi, sad još treba složiti virtualni labaratorij u virtualboxu. Snort
načinu mora biti postavljen između dvije mreže da može pregledavati pakete. Cilj je imati virt
mašinu sa ranjivom aplikacijom, te drugu sa koje se pokreću napadi, te između njih imati SNOR

pfSense koji će provjeravati i prosljeđivati promet sa jedne na drugu mrežu. Neznam dali ću us 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. 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.