Dnevnik rada

1. tjedan (10.-17.10.2017)

Dosadašnji rad

Sastanak s mentorom i asistentima i generalni dogovor oko tema za projekt.
Informiranje o potencijalnim temama na internetu i kroz wiki bazu podataka.

Daljnji koraci

Dogovor s asistentom kako najbolje implementirati temu.
Krenut s radom na dokumentu plan projekta.

---

2. tjedan (18.-24.10.2017)

Dosadašnji rad

Postignut je dogovor s asistentom oko teme i koje stvari bi se trebale implementirati na projektu. Otvorena je Zotero baza i stavljeni su prvi pročitani dokumenti. Trenutno sam u procesu upoznavanja s različitim tehnologijama i programima koje se koriste za obrane informatičkih sustava. Na kompjuter sam instalirao IDS/IPS program SNORT, te se upoznavao s njegovim mogućnostima.

Daljnji koraci

U bazi znanstvenih radova pronaći radove koji odgovaraju mojim potrebama, staviti ih u Zotero bazu i tagirati. Napisati plan projekta i predati ga do nedjelje asistentu na pregled.

---

3. tjedan (25.-31.10.2017)

Dosadašnji rad

Predao sam plan projekta asistentu na inicialno razmatranje. Trenutno sam u procesu pisanja dokumenta u kojem će biti kategorizirani i opisani razni informacijski sustava koji planiram predati asistentu 2.11, te onda u dogovoru s njime odrediti koje sigurnosne alate ćemo testirati.

Daljnji koraci

Nakon dogovora o alatima koje ćemo testirati, do 7.2 napisati i predati asistentu dokument u kojem će biti opisani načini na koji su već provedena testiranja sigurnosnih sustava, te inicijalna razmatranja

kako bi to mi mogli implementirati.

4. tjedan (1.-7.11.2017)

Dosadašnji rad

Asistentu Žadu sam predao dokument o kategorizaciji mrežnih sigurnosnih alata. Dokument o koje funkcionalnostima alata koje bi trebalo testirati je skoro gotov. Također smo započeli razgovor o načinu implementacije virtualne mreže.

Daljnji koraci

Predati kroz koji dan dokument o testiranju funkcionalnosti sigurnosnih alata, te nakon pregleda dokumenta od strane asistenta nastaviti planiranje kako izvesti testiranje u virtualnoj mreži.

5. tjedan (8.-14.11.2017)

Dosadašnji rad

Asistentu Žadu predan je dokument o testiranju funkcionalnosti sigurnosnih sustava i plan projekta na službeni forum FER-a.

Daljnji koraci

Dogovoriti način implementacije virtualne mreže, da nakon međuispita mogu početi testiranja.

6/7. tjedan (15.-28.11.2017)

Međuispiti

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) **CKGE_TMP_i Dosadašnjirad** ***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. CKGE_TMP_i Daljnji koraci Uz navođenje asistena do kraja konfigurirat sustav i dobiti prve rezultate ispitivanje Mod Security pravila.

1 1 . tjedan (20 .12.- 26 .12.2017) CKGE_TMP_i Dosadanji rad CKGE_TMP_i 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 određenog 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 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.