SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

SEMINAR

Pregled svjetskih edukacija za penetracijsko testiranje

Luka Soklić

Voditelj: doc.dr.sc.Predrag Pale

Zagreb, svibanj, 2019.

Sadržaj

1. Uvod

Penetracijsko testiranje je provjera sigurnosti informacijskog sustava u kojoj se ispitivač stavlja u ulogu napadača nekog sustava kako bi uočio ranjivosti tog sustava.

Ono pokazuje koje su mogućnosti iskorištavanja ranjivosti informacijskog sustava te otkriva razmjere štete koje potencijalni napadač može počiniti.

S obzirom na porast prijetnji s kojima se suočavaju pojedinci, razne organzacije pa i države, mnoga sveučilišta i fakulteti diljem svijeta stvorili su programe većinom diplomskih studija vezano za područje računalne sigurnosti.

Stručnjaci koji se bave penetracijskim testiranjem ne moraju imati formalno obrazovanje u računalnoj sigurnosti već je bitnije znanje i odgovarajuće radno iskustvo u tome.

2. Pregled svjetskih edukacija za penetracijsko testiranje

2.1. Edukacije u okviru studija

Tijekom proučavanja ove teme zaključio sam da ne postoji studij penetracijskog testiranja već se o penetracijskom testiranju uči u sklopu kolegija o računalnoj sigurnosti.

Jako je zahtjevno doći do detaljnijih informacija o sadržaju kolegija na većini fakulteta te sam odlučio samo navesti neke fakultete koji se bave računalnim znanostima.

Neki od najboljih sveučilišta koji imaju studij računalnih znanosti i u sklopu njega obrazovanje o penetracijskom testiranju su

1. Imperial Collage London (UK)

- U sklopu kolegija: Networks and Communications uče sadržaj: Penetration testing.

- U sklopu kolegija: Network and Web Security preporučena literatura je: Professional penetration testing : creating and learning in a hacking lab / Wilhelm, Thomas.

2. Vienna University of Technology (Austrija)

- U sklopu kolegija:Internet Security uči se sadržaj:Network discovery/vulnerability scanning,techniques and tools.
- U sklopu kolegija:Network Security uči se sadržaj: Security objectives in communication networks, threats and attack techniques.

3. Delft University of Technology (Nizozemska)

- U sklopu kolegija:Software Security uči se sadržaj:Static Analysis Techniq

4. Harvard University (SAD)

- U sklopu kolegija: Systems and Security uči se općenito o raznim tehnikama za napad i obranu računalnih sustava.

2.2. Komercijalne edukacije

Većinom se koriste za poboljšanje već stečenog znanja, ali ima i nekih koji nude tečajeve u osnovama za početnike.

1. Offensive Security

Offensive Security tečajevi su dizajnirani za profesionalce koji se bave informatičkom sigurnosti koji žele napredovati u području penetracijskog testiranja te steći certifikat.

Na navedenom tečaju fokus je na radu sa Kali Linuxom.Cijena tečaja se kreće od 800 do 1200 dolara.Polaznici dobivaju materijale za vježbu online kao i pristup virtualnom laboratoriju te se predavanja organizraju u vidu konferencija.Po završetku tečaja, nakon položenog ispita koji traje 24 sata i u obliku je “real world“ scenarija , polaznici dobivaju jedan od najcjenjenijih certifikata: OSCP-Offensive Security Certified Professional.

2. EC-Council

EC-Council nastao je kao International Council of E-Commerce Consultants nakon terorističkih napada na Ameriku 11.9.2001. kako bi se pokušalo spriječiti buduće terorističke Cyber napade.

Programi koje EC-Council nudi vezano za penetracijsko testiranje su namijenjeni stručnjacima u području računalne sigurnosti:

-program za stjecanje CEH certifikata

-program za stjecanje LPT Master certifikata

Cijene programa se kreću od $850 za CEH program do $900 za LPT Master program. Licenca LPT Master se obnavlja svake dvije godine po cijeni od $250.

Nakon petodnevnog tečaja za CEH certifikat slijedi ispit u trajanju od 4 sata u kojem polaznici odgovaraju na 125 pitanja.Ispit se polaže u formatu po izboru polaznika.

Nakon završenog programa za LPT Master certifikat slijedi ispit u trajanju od 18 sati. Ispit se polaže online i podijeljen je u tri etape po 6 sati. Ispitivači nadgledaju uživo cijeli proces ispita.

3. London South Bank University

London South Bank University je jedno od najstarijih i najvećih londonskih sveučilišta osnovano 1892.

Edukacija za penetracijsko testiranje na ovom sveučilištu nudi se u vidu preddiplomskog modula:Systems and cyber security koji je namijenjen studentima zainteresiranim za ovo područje.Program traje jednu godinu, njegova cijena je od 7500 funti do 12000 funti. Predavanja se održavaju u prostoru sveučilišta. U programu sudjeluju i gostujući predavači, poput stručnjaka iz kompanija kao što su VISA, HP,IBM.

Po završetku programa dobiva se diploma prvostupnika inženjera računarstva koja je certificirana od strane GCHQ-a (“Government Communications Headquarters“ -državna organizacija zadužena za sigurnost Velike Britanije).

4. SANS

SANS institut je utemeljen 1989. godine kao znanstvena i obrazovna institucija i jedan je od najvećih centara u svijetu za edukaciju u području računalne sigurnosti.

SANS-ovi programi edukacije za penetracijsko testiranje i etičko hakiranje namjenjeni su stručnjacima u računalnoj sigurnosti,ali i početnicima koji su zainteresirani za to područje.

Po mom mišljenju ovo je najopširnija edukacija za penetracijsko testiranje u ovoj kategoriji s obzirom da polaznici mogu birati 17 programa koji su podijeljeni u 6 razina zavisno o predznanju polaznika.

Svaki polaznik može po svom nahođenju složiti redoslijed polaganja programa.

Cijena programa kreće se od 6000USD na više, opet zavisno o odabranom programu. Svaki ima svoj oblik provjere znanja nakon čega se dobiva jedan od 8 certifikata:

- GISF (GIAC* Information Security Fundamentals)
- GCIH (GIAC Certified Incident Handler)
- GWAPT (GIAC Web Application Penetration Tester)
- GPEN (GIAC Penetration Tester)
- GPYC (GIAC Python Coder)
- GMOB (GIAC Mobile Device Security Analyst)
- GAWN (GIAC Assessing and Auditing Wireless Networks)
- GXPN (GIAC Exploit Researcher and Advanced Penetration Tester)

*GIAC – Global Information Assurance Certification

5. eLearnSecurity

eLearnSecurity je tvrtka koja se bavi edukacijom u području računalne sigurnosti. Svi njihovi programi dostupni su online, a podučavanje se odvija online uživo.

Njihovi programi variraju od osnovnih do naprednih tečajeva u pen testingu, također imaju specijalizirane programe koji se bave penetracijskim testiranjem unutar uskog područja kao što su web aplikacije i pen testing u mobilnim aplikacijama.

Certifikati (eJPT,eCPPT,eCPTX,eMAPT,eWPT,eWPTX) se dobivaju nakon uspješno položene provjere znanja u kojoj se ispituje praktična primjena stečenog

znanja u sklopu penetracijskog testa prave mreže koja je simulirana sa Hera Labom .

Cijena programa od 1000 do 2000USD.

2.3. Besplatne edukacije

Istražujući na internetu naišao sam na nekoliko stranica koje nude besplatnu edukaciju. Ovdje bih naveo dvije najzanimljivije:

1. Cybrary

   Cybrary je najveća online platforma namijenjena svima koje zanima računalna sigurnost, profesionalno ili amaterski. Nudi razne materijale i tečajeve od početničkih do naprednih kao i mogućnost kontaktiranja profesionalaca i tvrtki koje se bave područjem računalne sigurnosti.

2. Coursera

   Coursera je online platforma za učenje koju su osnovali profesori sa američkog sveučilišta Stanford. Nudi razne online tečajeve i specijalizacije u suradnji sa sveučilištima i drugim organizacijama.

Za entuzijaste i one koji se zanimaju za ovo područje ima dosta praktičnih primjera i videa i na Youtubeu.

3. Pregled tema koje čine edukaciju za penetracijsko testiranje

Na temelju svega proučenog teme koje ulaze u okvir edukacije za penetracijsko testiranje su:

- Metode sakupljanje informacija o sustavu
- Identifikacija ranjivosti sustava
- Metode exploita
- Post exploit

3.1. Metode sakupljanja informacija o sustavu

Prvi važan korak u penetracijskom testiranju je sakupljanje informacija o sustavu.

Pentesteri moraju sakupiti što više podataka o sustavu i potencijalnim mjestima sustava koji su ranjivi. Ovo se može odvijati pasivno ili aktivno.

Pasivno skupljanje informacija podrazumjeva sakupljanje informacija bez uspostavljanja kontakta između pen testera i mete dok aktivno skupljanje informacija uključuje kontakt između pentestera i mete.

3.2. Identifikacija ranjivosti sustava

Tijekom identifikacija ranjivosti sustava, student se obučava kako obraditi sakupljene podatke o sustavu, uočiti i kategorizirati ranjive točke sustava te napraviti plan napada.

3.3. Exploit

Cilj teme je obučiti buduće pen testere načinima exploita kojima se nastoji testirati ciljani sustav.Studenti moraju exploitirati ranjive točke sustava, doći do najbitnijih informacija i izbjeći svaku vrstu detekcije.

3.4. Post exploit

Nakon izvršavanja exploita, student mora znati napraviti detaljan pregled metoda koje je koristio za pristup informacijama sustava. Također, pen tester mora procijeniti kvalitetu informacija do kojih je bio u stanju doći te napraviti prijedloge vezane za poboljšanje sigurnosti sustava.

Jednom kada je izvještaj o exploitaciji sustava završen, tester mora počistiti sve exploite koji su izvršeni na sustavu.

4. Metode podučavanja

Penetracijsko testiranje podučava se putem predavanja koja zavisno od vrste edukacije dolaze u raznim oblicima.Također, u sklopu te edukacije jako je bitan rad u laboratoriju. Na laboratoriju studenti imaju priliku u virtualnom okruženju koja simuliraju rad realnih sistema i strojeva isprobati tehnike pen testinga u praksi.

Predavanja uživo su na svim fakultetima te na ovim tečajevima: Ec Council, SANS.

Svi ostali imaju predavanja u obliku video materijala gdje je gradivo pregledno sastavljeno na slajdove u ppt-u dok profesor objašnjava pojedine slajdove i ulazi u detalje vezano uz gradivo koje trenutni slajd prikazuje na ekranu.Postoje i predavanja u kojima predavač demonstrira na zaslonu ekrana korak po korak sadržaje koje budući pentesteri moraju znati.

Odlični primjeri su na Cybraryu ili Courseri gdje su sva predavanja objavljena besplatno.

Snimke predavanja nisu dostupna na službenim stranicama sveučilišta, ali neka predavanja pojedinih sveučilišta mogu se naći i na nekim stranicama besplatnih edukacija. Neki fakulteti imaju čak svoje vlastitie web stranice na kojima dijele besplatna predavanja raznog sadržaja. Neka predavanja su čak vezan za ovu temu, ali većina toga je dosta šturo i pokriva samo osnovne pojmove

5. Metode provjere znanja

Metoda provjere znanja za penetracijsko testiranje može biti praktična, što znači da polaznik na kraju edukacije polaže praktični dio ispita u vidu identifikacije ranjivosti i izvršavanja napada na sustav.Ovo obično uključuje izradu exploita sa ciljem kompromitiranja sistema. Na kraju predaje izvještaj o penetracijskom testiranju koji sadrži detaljne zapise o postupku napada na sustav.

Metoda provjere znanja može biti i pisana, što znači da na kraju nekih edukacija student mora riješiti pisani test koji se sastoji od postavljenih pitanja i više ponuđenih odgovora.Ispit ovog tipa traje u prosjeku 2 sata.

Obje metode provjere znanja mogu se polagati i od kuće.

Ec Council i Offensive Security imaju provjere znanja u praktičnom obliku gdje student polaže ispit koji se sastoji od simuliranog virtualnog okruženja o kojem student unaprijed ništa ne zna. Student mora uspješno izvršiti napad na sustav unutar danog vremenskog intervala i obrazložiti svoje pronalaske i postupke u izvještaju. Ispit je u suštini simulacija realnog okruženja s kojim će se student susresti u svojoj radnoj karijeri kao pen tester. Ispit traje od 6 sati na više.

6. Zaključak

Edukacija o penetracijskom testiranju u svijetu namijenjena je stručnjacima u računalnoj sigurnosti, početnicima i svim entuzijastima koji žele naučiti više o toj temi.

Bazira se na ovim sadržajima: metode sakupljanja informacija o sustavu, identifikacija ranjivosti sustava, metode exploita te post exploit.

Po završetku edukacije slijedi provjera znanja u vidu praktičnog rada nakon čega se može dobiti certifikat.

Mislim da je šteta što je penetracijsko testiranje u okviru formalnog obrazovanja obrađeno u okviru većih cjelina jer smatram da se puno više može naučiti iz proučavanja samo te teme.

7. Literatura

https://www.offensive-security.com/

https://www.eccouncil.org/

https://www.lsbu.ac.uk/

https://www.elearnsecurity.com/

https://www.sans.org/

https://www.tuwien.at/en/

https://www.tudelft.nl/en/

https://www.imperial.ac.uk/

https://www.giac.org/

https://www.coursera.org/

https://www.cybrary.it/