Security - od czego zacząć

Autor

Rafał Dobrosielski

PUSHSEC.PL

1. Zdobądź fundamenty

Wiem, że wszędzie jest to powtarzane i sam pewnie już nie raz to słyszałeś, ale powtórzę to jeszcze raz: zdobądź dobre fundamenty, a dalej będzie Ci łatwiej. Największe budynki zbudowane są na najsolidniejszych podstawach.

To jasne, że osobom posiadającym doświadczenie w innych dziedzinach IT łatwiej jest się dostać na stanowiska bezpieczeństwa.

A spowodowane jest to faktem, że miały one czas i możliwości, by uczyć się i praktykować dużo dłużej, niż osoby zaczynające dopiero przygodę z IT od bezpieczeństwa. Ale jeśli nie masz jeszcze doświadczenia, nie martw się — możesz osiągnąć nawet więcej, niż osoby, które mają doświadczenie w IT. Dlaczego? Ponieważ często zdarza się tak, że osoby te nabrały złych praktyk lub nauczyły się czegoś błędnie, a być może ktoś bez doświadczenia uczy się od początku w sposób poprawny.

Tak więc zacznij od pierwszej chwili uczyć się solidnie fundamentów: nie pobieżnie, spędź nad tym odpowiednią ilość czasu, by czuć się tutaj pewnie, tak, abyś w nocy o północy wiedział, co jest czym. A żeby osiągnąć taki poziom, należy zrozumieć dane zagadnienie i je przetestować w praktyce. Tylko te dwie rzeczy dadzą Ci pewność, że znasz coś od podszewki. Zatem zdobądź jak najlepsze fundamenty — później będzie tylko trudniej i ciekawiej, ale będziesz w stanie przez to przejść ;)

2. Wybór materiałów do nauki

Sam musisz wybrać formę nauki, z której będziesz korzystać na drodze do rozwoju w kierunku mida (nie juniora). Tak, jak wspomniałem w wywiadzie u Rafała, łatwiej jest celować od razu na stanowisko mida, a nie juniora, ponieważ stanowisk juniorskich jest mało. Poniżej przedstawię Ci kilka sposobów, w jakie możesz się uczyć: poprzez lekturę, pisanie oraz praktykę online. Kombinacja wszystkich tych form pomoże Ci w szybszym rozwoju.

Zacznijmy od książek, ponieważ ja najwięcej wiedzy czerpię właśnie z nich i tak jest mi ją najłatwiej przyswoić. Poniżej przedstawie Ci listę książek w kolejności z materiałami, jakie trzeba by przyswoić.

Zanim jeszcze zaczniemy, wspomnę, że znajomość języka angielskiego będzie Ci potrzebna, ponieważ większość firm, w których wprowadzane jest bezpieczeństwo, to firmy, które mają jakieś kontrakty międzynarodowe bądź są filią jakiejś globalnej korporacji.

Dodatkowo angielski pomoże Ci w rozwoju, ponieważ zdecydowanie więcej materiałów jest po angielsku niż po polsku. Chociaż ostatnio powstaje coraz więcej polskojęzycznych źródeł na temat bezpieczeństwa, to jednak zdecydowana większość i tak będzie po angielsku, więc warto się go nauczyć.

3. Książki

Kolejność	Co Ci da dana książka	Książka\Link
1.	Dzięki tej książce poznasz podstawy działania systemów operacyjnych. I dowiesz się, jak wyglądają one od środka.	Systemy operacyjne. Architektura, funkcjonowanie i projektowanie. Wydanie IX
2.	Dzięki tej książce zdobędziesz większą wiedzę na temat systemów Linux, co przyda Ci się w bezpieczeństwie — wiele narzędzi jest właśnie na ten system.	Linux. Biblia. Wydanie X
3.	Sieci są podstawą funkcjonowania w dzisiejszym świecie. Dzięki tej książce będziesz miał okazję w praktyce sprawdzić, jak działają.	CCNA 200-301. Zostań administratorem sieci komputerowych Cisco
4.	Dzięki tej książce poznasz podstawowe zagadnienia z dziedziny bezpieczeństwa.	CompTIA Security+: SY0-601 Certification Guide

PUSHSEC.PL

Chronię cenne informacje przed wszechobecnym zagrożeniem.
Pomagam małym i dużym firmom w przejściu na wyższy poziom profesjonalizmu.

5.	Dzięki tej książce poznasz podstawy bezpieczeństwa informacji.	Podstawy bezpieczeństwa informacji. Praktyczne wprowadzenie
6.	Przeczytaj tę książkę, by jeszcze zwiększyć praktykę w analizie pakietów.	Praktyczna analiza pakietów. Wykorzystanie narzędzia Wireshark do rozwiązywania problemów związanych z siecią. Wydanie III
7.	Dzięki tej książce dowiesz się, jak oceniać podatności w sieci.	Network Vulnerability Assessment
8.	Skryptowanie jest bardzo ważnym aspektem bezpieczeństwa. Dzięki tym książkom poznasz podstawy PowerShella.	• PowerShell dla administratorów systemów. Prosta automatyzacja zadań. • PowerShell Cookbook. 4th Edition

9.	Dzięki tej książce dowiesz się jak skryptować, ale tym razem nie w Windows, ale w Linux.	Learn Linux Shell Scripting Fundamentals of Bash 4.4
10.	Warto też poznać język programowania, by np. tworzyć swoje programy czy reverse shelle itd. Dzięki tej książce nauczysz się podstaw programowania w Python.	Automate the Boring Stuff with Python
11.	Dzięki tej książce zwiększysz swoją wiedzę na temat tworzenia oprogramowania.	Building Secure and Reliable Systems. Best Practices for Designing
12.	Dzięki tej książce poznasz podstawy standardu, jakim jest ITIL. Pomoże Ci to w tworzeniu dokumentacji i będzie podwaliną pod naukę innych, bardziej skomplikowanych standardów.	ITIL(R) 4 Foundation Courseware - English

13.	Tutaj z gwiazdką, bo to już naprawdę trudny temat, czyli Threat Modeling. Z książki dowiesz się naprawdę dużo o tym temacie.	Threat Modeling

Oczywiście zawartość książek trzeba praktykować, więc nie liczy się samo przeczytanie, ale również przerobienie materiałów i przetrenowanie ich. To dopiero da Ci odpowiednią wiedzę :)

4. Platformy

Niektórzy łatwiej łapią wiedzę z video, więc i takie platformy przygotowałem, byś miał wybór i dobrał materiały jak najbardziej pod swoje preferencje. Poniżej stronki godne polecenia, z których możesz czerpać masę wiedzy. Nie wszystkie materiały są super aktualne, ale dalej uważam, że warto.

- https://www.cybrary.it/
  - Dla cybrary szczególnie polecam dwie poniższe ścieżki na początek:
    - https://www.cybrary.it/catalog/career-path/soc-analyst-level-1/
    - https://www.cybrary.it/catalog/career-path/information-security-fundamentals/
- https://www.pluralsight.com/
  - Dla pluralsight szczególnie polecam dwie poniższe ścieżki na początek:
    - https://www.pluralsight.com/paths/ethical-hacking-ceh-v11-prep
    - https://www.pluralsight.com/paths/comptia-security-sy0-601

- https://www.youtube.com/c/Freecodecamp
  - https://www.youtube.com/playlist-Ethical Haking
  - https://www.youtube.com/playlist-Python
- https://www.youtube.com/
  - https://www.youtube.com/c/JohnHammond010
  - https://www.youtube.com/user/Computerphile
  - https://www.youtube.com/c/ippsec/videos
  - https://www.youtube.com/c/HackerSploit/videos

Praktykę można też zdobyć dzięki CTF. Poniżej dowiesz się, czym są CTF, a na kolejnej stronie znajdziesz linki do CTF dla początkujących.

"CTF (ang. Capture The Flag) to drużynowy turniej, podczas którego drużyny starają się rozwiązać jak najwięcej zadań z kategorii powiązanych z security/hackingiem, takich jak: web (bezpieczeństwo aplikacji webowych), pwn (exploitacja low-level / bezpieczeństwo aplikacji natywnych), RE (crackme / ogólno pojęty reverse engineering), crypto (kryptoanaliza), forensics (informatyka śledcza), stegano (steganografia), ppc/programming (programowanie/algorytmika), itp." - gynvael

Pamiętaj też, że do wykonywania CTF z poniższych stron nie potrzebujesz zespołu. Zarejestruj się, a na platformie dowiesz się, jak rozwiązywać zadania.

PUSHSEC.PL

Chronię cenne informacje przed wszechobecnym zagrożeniem.
Pomagam małym i dużym firmom w przejściu na wyższy poziom profesjonalizmu.

	Beginner CTF Sites	
Strona CTF	Description	Start PWNing
linuxpwndiary	Discord-based wargame, that offers fun linux challenges!	Click To Start
picoCTF	The best beginner's level CTF site, highly recommended!	Click To Start
OverTheWire	Collection of wargames, start with Bandit.	Click To Start
TryHackMe	Platform for learning and teaching cybersecurity.	Click To Start
Backdoor	CTF platform, there is a beginners area.	Click To Start
cmdchallenge	Linux commands challenges, its fun!	Click To Start
hpandro1337	Android CTF for beginners.	Click To Start

Lista jest autorstwa sh3llm4g1ck więcej CTF możecie znaleźć w tym linku jest ich tam jeszcze sporo :).

5. Konferencje bezpieczeństwa

Poniżej wrzucam Ci 12 konferencji — nie tylko polskich — na które możesz zajrzeć i dowiedzieć się co nieco o bezpieczeństwie.

- Microsoft Ignite
- Nullcon
- Semafor
- InfoSecurityEurope
- Black Hat USA
- Atsummit
- Oh My H@ck
- x33fcon
- Semafor
- DEF CON 29
- GrrCON
- Sekurak Mega Hacking Party

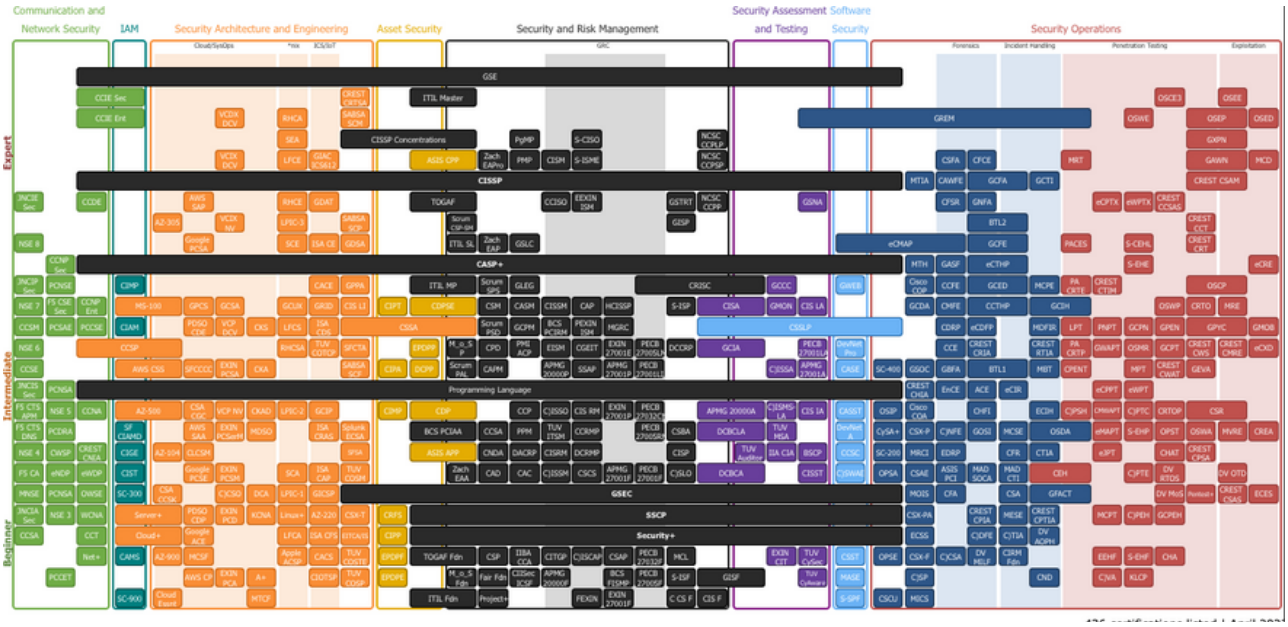
6. Certyfikaty

- Comptia Security + — Jest to ogólny certyfikat dotyczący bezpieczeństwa. Uczyć się do niego można z książki podanej powyżej jak i z mojego bloga pushsec.pl. Dużo materiałów na moim blogu z działu Podstawy pokrywa wymagania Comptii Sec +, więc zajrzyj, bo warto ;) Wybrałem ten certyfikat zamiast SSCP, ponieważ SSCP jest certyfikatem prostszym z punktu widzenia nowej osoby w bezpieczeństwie — ale przez to niestety nie przynosi on takiego efektu u potencjalnego pracodawcy co Comptia Sec +.
- CEH — Certified Ethical Hacker. Dzięki temu certyfikatowi dowiesz się, jak wykorzystuje się narzędzia i umiejętności hackerskie w sposób legalny i na zlecenie firm. Bardziej dla początkującego pentestera.

Certyfikaty chmurowe dotyczące bezpieczeństwa to na przykład:

- Ścieżka Azure — Należy wybrać ścieżkę "Cybersecurity Architect". przed tą ścieżką należy zrobić jeszcze certyfikację SC-400.
- Ścieżka AWS
- Ścieżka GCP
- Certyfikat CCSP

Pozostała certyfikacja zależy od wyboru specjalizacji. Tabele z certyfikatami autorstwa Paula Jerimy znajdziesz poniżej, a jeśli chcesz przejść do wersji klikalnej, to przejdź tam poprzez ten link.



7. Blogi

Również z blogów możesz czerpać dużo wiedzy. Jak już wspomniałem powyżej, sam prowadzę takiego bloga i zapraszam cię serdecznie na niego: www.pushsec.pl. Ale jest też masa innych blogów, do których możesz zajrzeć i zdobyć masę wiedzy. Poniżej zamieszczam dwie listy polecanych blogów, pierwsza jest moja, a druga jest od Adama Haertle z Zaufanej Trzeciej Strony.

- https://pushsec.pl/top-7-blogow-o-bezpieczenstwie-w-2022/
- https://zaufanatrzeciastrona.pl/post/25-miejsc-gdzie-warto-czytac-po-polsku-o-bezpieczenstwie/

8. Rozwój i rozpoczęcie kariery w bezpieczeństwie

Cała powyższa wiedza powinna być Ci pomocna niezależnie od tego, jaką ostatecznie wybierzesz specjalizację. Jeśli jeszcze nie wiesz, jakie są specjalizacje w bezpieczeństwie, możesz się z nimi zapoznać w niniejszym artykule. Jeśli wybrałeś już specjalizację, powyższych też możesz się nauczyć, ale wtedy ścieżkę układałbym już konkretnie pod daną specjalizację.

Pamiętaj, by nie spoczywać na laurach. Wiem, że wszystkie powyższe tematy to naprawdę dużo spędzonych godzin na nauce, ale w bezpieczeństwie musisz się cały czas rozwijać i przeć do przodu, ponieważ napastnicy robią dokładnie to samo i Ty musisz ich gonić, a masz dużo więcej do zrobienia. Jest tak dlatego, ponieważ, zabezpieczając system jako defensywa, musisz zabezpieczyć więcej niż tylko jedną podatność, którą wykorzystasz. A jako pentester nie masz do znalezienia jednej podatności, tylko musisz przeszukać całą aplikację czy sieć itd. i znaleźć wszystkie możliwe, a nie tylko tą, która da Ci dostęp.

Tak że z mojej strony życzę Ci powodzenia, wytrwałości, chęci rozwoju, dyscypliny i abyś osiągnął swój cel.

Koniec

Mam nadzieje, że powyższe materiały były Ci pomocne i że dzięki nim osiągniesz zamierzony cel, czyli zdobędziesz pracę marzeń !!!

pozdrawiam Pusz

Rafał Dobrosielski

PUSHSEC.PL