



IT Security Services

0xfb44f4f23139bb8a

Mateusz Kocielski

m.kocielski@logicaltrust.net

LogicalTrust

SecurityBsidess
Warszawa, 10 października 2015 r.

\$ whoami

- ▶ pentester w LogicalTrust
- ▶ open source:
 - ▶ PHP - bug fixing
 - ▶ NetBSD - libsasl(3), bozohttpd(8), losowe rzeczy & członek security-team@
- ▶ bezpieczeństwo:
 - ▶ PHP - CVE-2010-1868, CVE-2010-1917, CVE-2010-4150, CVE-2010-4156, CVE-2011-1938, ...
 - ▶ stunnel - CVE-2013-1762
 - ▶ OpenSSH - CVE-2011-0539
 - ▶ Apache - CVE-2014-0117, CVE-2014-0226
 - ▶ FreeBSD - CVE-2015-1414

0xfb44f4f23139bb8a?



CRYPTO/STEGANO 100000 pkt.

0xfb44f4f23139bb8a?

<https://www.youtube.com/watch?v=CgcorLQXsQQ>

O co chodzi?



- ▶ turecki rambo vs. księgowy
- ▶ weryfikacja faktów i mitów
- ▶ wskazówki jak zostać (dobrym) pentesterem
- ▶ doświadczenia innych

Ogłoszenie parafialne

- ▶ nie chcę definiować pojęć:
 - ▶ testów penetracyjnych
 - ▶ red team vs. blue team
 - ▶ audytów bezpieczeństwa
- ▶ pozostanmy na dużym stopniu ogólności

MIT - praca pentestera jest ULTRA ciekawa



- ▶ dokumentacja
- ▶ testy, które nie są interesujące
- ▶ testowanie technologii, które znasz na pamięć
- ▶ praca jest powtarzalna
- ▶ wskazanie wszystkich obszarów ryzyk, a nie jednej ścieżki jak zdobyć "roota"
- ▶ ale...

...dla tych (20-80)% warto być pentesterem



Źródło: http://img.fifa.com/mm/photo/tournament/competition/01/64/24/39/1642439_big-lnd.jpg

- ▶ Fakt: ok. (20-80)% pracy jest ciekawa
- ▶ ...każdy pentest zawiera jednak coś innego
- ▶ zrobienie "roota" zawsze jest przyjemne
- ▶ ciekawe projekty
- ▶ trafiają się błędy, które sprawiają, że serce bije szybciej:
 - ▶ wczytanie plików przez serię błędów w PHP (open source)
 - ▶ RCE w cache języków (open source)

MIT - praca pentestera jest tylko techniczna



Źródło: <http://3vxsjq3roj103wlhf71jhh7t.wpeengine.netdna-cdn.com/wp-content/uploads/2014/09/computer-nerd.jpeg>

- ▶ pentesterów, którzy wykonują tylko techniczną robotę nikt nie rozumie
- ▶ dokumentacja jest NIEZBĘDNA
- ▶ umiejętność napisania dwóch zdań jest NIEZBĘDNA
- ▶ potrzeba odtwarzania swoich kroków
- ▶ potrzeba edukacji klientów
- ▶ ...pamiętaj, że Twoja praca ma zostawić klienta w "bezpieczniejszym świecie"

MIT - pentesterzy są podziwiani



Źródło: <http://images.amcnetworks.com/ifc.com/wp-content/uploads/2014/02/nerd-dance.jpg>

- ▶ ...bo są "hakerami"
- ▶ postrzeganie pentestera jako intruza przez pracowników klienta:
 - ▶ jałowe dyskusje o krytyczności błędów
 - ▶ personalne odbieranie uwag
 - ▶ wyrywanie włosów
 - ▶ próby podważenia kompetencji i znalezisk
 - ▶ "Paaanie, to tylko na testówce!"
 - ▶ "Paaanie, to się nie wydarzy!"
 - ▶ "A nieprawda bo mamy HTTPS"
- ▶ jak czegoś nie znajdziesz, to dostaniesz po głowie

MIT - bezpieczeństwo jest najważniejsze



Źródło: <https://wombatsdojogle.files.wordpress.com/2012/01/search-results-cyclethere-i-fixed-it-redneck-repairs-page-3-1.jpg?w=560>

- ▶ nikt nie ma potrójnej ściany ognia i sendmaila
- ▶ bezpieczeństwo jest dla biznesu, a nie odwrotnie!
- ▶ często trzeba zwrócić
- ▶ Klient optimalizuje po wielu zmiennych, nie tylko po bezpieczeństwie
 - ▶ pani Zosia w kiosku nie ma sejfu
 - ▶ a pan Antoni obsługuje metodę TRACE na swoim hostingu

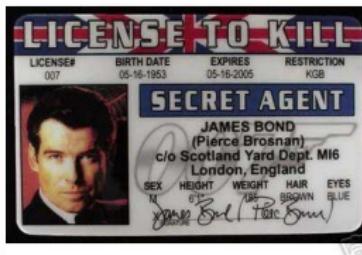
MIT - będziesz szukał 0-dayów



Źródło: <http://thewindowsclub.thewindowsclubco.netdna-cdn.com/wp-content/uploads/2015/02/zero-day-attack.png>

- ▶ ...nie będziesz
- ▶ ...nie będziesz ich używał
- ▶ ...ale sporadycznie coś samo się trafi!
- ▶ ...ale czasem są misje specjalne

MIT - pentester podczas pentestu może wszystko!



Źródło:

http://cdn.okcimg.com/php/load_okc_image.php/images/0x0/0x0/0/8954805073882791803.jpeg___1_500_1_500_cb94de6a..png

- ▶ niestety w praktyce nie można wejść do dyskoteki i bić kogo popadnie
- ▶ często narzucone są sztywne ramy (czasowe, wpływu ataków na biznes etc.)
- ▶ często trzeba zwrócić i pozostawić rzeczy niedopowiedziane

MIT - firmy pentesterskie są cool



Źródło: https://imagoinc.files.wordpress.com/2010/04/dreamstime_corporate.jpg

- ▶ te większe, nie różnią się NICZYM od typowego korpo
 - ▶ timesheets, raporty, ...
- ▶ te mniejsze, nie różnią się NICZYM od typowej mniejszej firmy
- ▶ praca pentestera wymaga profesjonalizmu

FAKT - poznasz wiele technologii



Źródło: <http://i.ytimg.com/vi/McaV4Ua-QMA/maxresdefault.jpg>

- ▶ ...o ile pracujesz w firmie, która wykonuje testy "na zewnątrz"
- ▶ styczność z Luą, Scalą, Pythonem, PHP, Javą, Cobolem, APL i **milionami** innych technologii
- ▶ musisz się szybko uczyć
- ▶ większość z nich tylko "liźniesz"

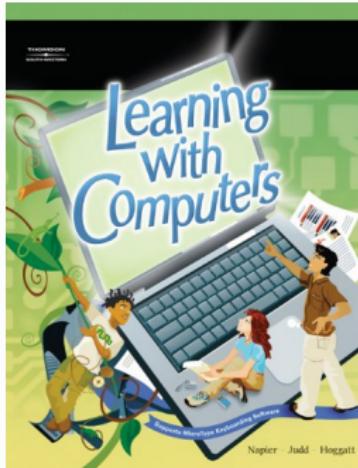
FAKT - zobaczysz wiele!



Źródło: http://memestorage.com/_nw/23/87899101.jpg

- ▶ styczność z systemami niedostępnymi dla "szaraka"
- ▶ styczność z usługami/aplikacjami przed "premierą"
- ▶ możliwość spotkania ekspertów w wielu dziedzinach
- ▶ zobaczysz ...za wiele

FAKT - pentester się ciągle uczy



Źródło: http://computers.childrens-library.com/images/Learning_With_Computers_0.large.jpg

- ▶ wiedza z 2014...
 - ▶ ...to nieaktualna wiedza!
- ▶ trzeba się uczyć, STALE
- ▶ trzeba się uczyć nowych technologii



FAKT - pentester robi to czego wymaga rynek



Źródło: https://c2.staticflickr.com/4/3118/2398651856_022030f3e4.jpg

- ▶ ...urządzenia mobilne
- ▶ ...aplikacje www
- ▶ Java (tm) i inne straszne technologie

MIT - gracze CTF to świetni pentesterzy



Źródło:

http://www.seguridadaldia.net/wp-content/uploads/imgcache/0335da827f_Capture-the-Flag-Graphic.jpg.jpg

- ▶ nie każdy kto dobrze biega przez płotki będzie dobrym piłkarzem
- ▶ $\forall_{x,y}$ nie każdy x będzie dobrym y - truizm
- ▶ CTFy często są DIAMENTRALNIE RÓŻNE od pentestów
 - ▶ są ograniczenia, jest Klient, jest inny cel

MIT - będziesz ciągle siedział w majtach i zapoconej koszulce przed komputerem...



LOLhome.com

Źródło: http://www.lolhome.com/img_big/home-office.jpg

www.logicaltrust.net

MIT - pentesterzy milionerzy



Źródło: <http://i.wp.pl/a/f/jpeg/27303/sknerus.jpeg>

- ▶ jeżeli chcesz zjeźdzać na nartach z góry hajsu, to zostań:
 - ▶ blackhatem
 - ▶ programistą Javy w banku
 - ▶ tańcz z gwiazdami

MIT - pentester od 8 do 16



Źródło:

<http://1.bp.blogspot.com/-EdLID12IJEk/UM7z9t3CPpl/AAAAAAAAbk/1dLLuZz1cO4/s1600/Gamer-Meme.jpg>

- ▶ bycie pentesterem to styl życia
- ▶ będziesz ciągle myślał o tym jak coś obejść lub zepsuć
- ▶ stały rozwój

FAKT: dyskrecja jest ważną częścią pracy



Źródło: <http://esklep-sportowy.pl/grafiki-allegro/pliki/pku1.jpg>

- ▶ zaufanie jest podstawą współpracy z klientem
- ▶ jeżeli zawiedziesz je chociaż raz, to wybrany klient (i inni) uciekną
- ▶ "nie paplaj w słuchawę"

FAKT: wiedza praktyczna jest nie do przecenienia



Źródło: <http://cdn.thedailybeast.com/content/dailybeast/articles/2014/08/14/rambo-hates-guns-how-sylvester-stallone-became-the-most-anti-gun-celeb-in-hollywood/jcr:content/image.crop.800.500.jpg/47401550.cached.jpg>

- ▶ ...większość dobrych pentesterów (których znam) najpierw było programistami/administratorami
- ▶ jeżeli nie rozumiesz jak coś działa, to nie przetestujesz tego od "a do z"
- ▶ w praktyce pentester to często człowiek orkiestra

FAKT: CTFy, Bug Bounty i WARGAMEy są bardzo przydatne



Źródło: <http://www.sw.gov.pl/Data/Files/pzaranek/poezja-006.jpg>

- ▶ można poćwiczyć bez obawy o bilet do ZK Wronki
- ▶ ciemne strony bug bounty
- ▶ często zadania na CTF/wargame są WYDUMANE

FAKT: umiejętność programowania jest przydatna



Źródło: <http://i.ytimg.com/vi/utTclg8vDis/hqdefault.jpg>

- ▶ ...do automatyzacji różnych rzeczy
- ▶ ...do zrozumienia jak działa aplikacja
- ▶ ...do popełniania błędów

FAKT: bardzo ważne są umiejętności miękkie



Źródło: <http://www.kindofcreepy.com/wp-content/uploads/2011/02/super-nerds02.jpg>

- ▶ rozmowy z osobami nietechnicznymi
- ▶ praca w grupie
- ▶ samodzielność
- ▶ rozmowy/negocjacje z klientem

Moar?



Źródło: <http://i0.kym-cdn.com/entries/icons/original/000/000/574/moar-cat.jpg>

inne fakty/mity?

Czas na pytania (i odpowiedzi)

Q&A



LOGICALTRUST

IT Security Services

Dąbrowskiego 23/9 50-457 Wrocław, PL

T. +48 71 738 24 35 K. +48 601 86 14 85
F. +48 71 738 25 52 E. biuro@logicaltrust.net

NIP: 899-237-42-67 REGON: 021227658

www.logicaltrust.net