Evropská unie
Evropský sociální fond
Operační program Zaměstnanost

Úřad práce ČR

příloha č. 6 dohody č.:		POVEZ II (CZ.03.1.52/0.0/0.0/15_021/0000053)		Vzdělávací zařízení:	HACKER Consulting s.r.o.
Plán výuky				Lektor:	Roman Kümmel
Zaměstnavatel:	Adbros s.r.o.	IČO:	27677338	Místo výuky:	Charvatská 1838/21, 612 00 Brno-Královo Pole
Název vzdělávací aktivity:	Etický hacking v praxi a testování webových aplikací				

	Datum*	Počet vyučovacích hodin	Od-do	Okruhy plánovaných témat
1	9.10.2017	8	8:00-17:00	příkazy ve Windows pro práci s uživateli, procesy, sítí, službami a registrem; analýza provozu příkazem netstat; popis konfiguračních souborů a registrů souvisejících se síťovými službami; základy použití analyzátoru sítí Ethereal/Wireshark a Network Monitor; analýza protokolů TCP, UDP a IP.
2	10.10.2017	8	8:00-17:00	zachycení hesla v síti; zachycení a ukázka analýzy protokolů ARP,http, FTP, DNS a DHCP.RDP, IPSec, Skype a dalších; použití filtrů ve Wireshark; základy unix příkazů pro práci v síti; změna MAC adresy ve Windows a v Linuxu. Úvod do etického hackingu; dělení útočníků a jejich motivace; možnosti získávání zpráv o cíli; nástroje hackerů pro Linux a Windows; základy inventarizace a použití skenerů na síťové vrstvě; ukázka různých druhů skenerů.
3	11.10.2017	8	8:00-17:00	specializované skenery a jejich použití pro kontrolu WWW serverů; odhalování snifferů pomocí specializovaných nástrojů – PromiScan nebo sentinel. Použití nezávislých databází slabin a zranitelností. Možnosti inventarizace pomocí protokolů vyšších vrstev např. přes LDAP, SNMP a další.
4	16.10.2017	8	8:00-17:00	základy virů, jejich dělení a postup odstranění virové nákazy spojený s praktickou ukázkou; použití nástrojů od sysinternals; ověření a odstranění nákazy pomocí specializovaných antivirových nástrojů. Způsoby manipulace jádra a paměti škodlivým kódem a rootkity. Seznámení s rootkity a postupy pro jejich identifikaci a odstranění. Použití trojanů pro ovládnutí systému. Praktické odstranění trojanů z operačního systému. Popis útoků na síťové vrstvě. Použití programu Cain & Abel pro odchytávání hesel a demonstraci útoku „Man in the middle“. Ukázka použití programu ettercap pro zachytávání hesel. Formy útoků na protokoly a služby konkrétně DNS, ARP, http a další.
5	17.10.2017	8	8:00-17:00	obcházení firewallů, IDS a honeypotů; ukázka monitorovacích a detekčních nástrojů. Demonstrace útoků na WWW a proxy servery. Kontrola zabezpečení Web serveru MS IIS 6 a 7. Slabiny webovských prohlížečů. Ochrana vzdálených přístupů pomocí VPN a možné potenciální útoky. Možnosti zvýšení privilegií na vzdáleném systému. Možnosti obrany proti technikám hackerů pomocí šifrování – SSL a IPSec a dalších speciálních technik – port cnocking. Činnosti prováděné po zjištění napadení počítače. Dohledávání aktivity útočníka. Skrývání stop nelegální aktivity. Možnosti standardních prostředků bezpečnostního auditu.

Vyplňte pouze bílá pole

* V případě, že vzdělávací aktivita bude probíhat v určitém termínu denně, vypište do prvního sloupce datum od-do (např. 1.8.2016-20.8.2016).
V případě, že vzdělávací aktivita bude probíhat nepravidelně nebo pouze v určitý den v týdnu, vypište jednotlivé dny do připravených sloupců.

Datum:	26.7.2017
Vyřizuje:	X
Číslo telefonu:	X
Email:	X

jméno, příjmení, funkce a podpis oprávněné osoby (razítko)	Mgr. Jan Ptáčník, jednatel