příloha č. 6 dohody č.:	JEA-MN-8/2018	POVEZ II (CZ.03.1.52/0.0/0.0/15_021/0000053)		Čas výuky od - do:	8:00-16:30
Plán výuky				Lektor:	xxx
Zaměstnavatel:	Euro Enterprise Development	IČO:	27773728	Místo výuky:	Šumperk, Langrova 25
Název vzdělávací aktivity:	**odborné vzdělávání deployment+security**				

PČ	Datum	Počet vyučovacích hodin	od - do	Okruhy plánovaných témat
1	12.2.2018	8	8:00-16:30	Problematika bezpečnosti, historie, charakteristika prostředí, cíle útoků, typy útočníků, základní příkazy používané v operačních systémech Windows, Protokol TCP/IP, sada protokolů a adresování v sítích TCP/IP, protokol TCP, protokol IP, protokol http, ftp, DNS a další, Typy útoků, Sběr informací o systému - skenování stanic a portů, sběr informací o OS a aplikacích, odposlech síťového provozu, získání informací od personálu, Zablokování služeb (Útoky typu DoS), Získání přístupu do systému: útoky na hesla, útoky na TCP spojení, útok na spojení Telnet/FTP, podvržení IP-adresy (IP-spoofing), útok pomocí paketů směrovaných zdrojem, Získání přístupu do systému: útoky na webové servery, útoky na klienty webových serverů, útoky v prostředí e-mailů, útoky na databáze, problematika obchodování na Internetu, Charakteristika základních operačních systémů a útoků na ně, Windows 7/8 - Windows Server 2008/2012, Linux – ukázka linuxové distribuce, Obrana proti útokům, Obecné zásady obrany, Bezpečnostní politika - obsah bezpečnostní politiky, třídy zabezpečení,
2	13.2.2018	8	8:00-16:30	Zálohování, Autentizace, Sledování událostí (Auditing), Firewally - problematika připojování k Internetu, firewally a jejich typy, začlenění firewallu do sítě, Šifrování a bezpečné protokoly - bezpečnostní služby v počítačových sítích, SSL a IPSec, Používané prostředky a aplikace - síťové analyzátory, prostředky pro scanování, prostředky pro detekci napadení a reakci, Doporučená opatření, Nasazení šifrování na serverech, Nasazení síťových filtrů ve Windows serverech, Nasazení VPN a NAT technologie pro ochranu Windows serveru v Internetu, Základní příkazy ve Windows 7 pro práci s uživateli, procesy, sítí, službami a registrem, Analýza provozu příkazem netstat a jeho parametrů, Popis konfiguračních souborů a registrů souvisejících se síťovými službami, Základy použití analyzátoru sítí Ethereal/Wireshark a Network Monitor v prostředí windows, Analýza protokolů TCP, UDP a IP, Zachycení hesla v síti, Analýza protokolů na linkové vrstvě např. CDP,
3	14.2.2018	8	8:00-16:30	Model klient-server v sítíc, 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, Ukázka snifování v Linuxu, Změna MAC adresy ve Windows, 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. Použití skenerů pro ohledání vyšších vrstev – amap, dsniff, Skenování netbiosu, Použití nástroje Cain&Abel pro detekci zařízení, Specializované skenery a jejich použití pro kontrolu WWW serverů, Odhalování snifferů pomocí specializovaných nástrojů, Použití nezávislých databází slabin a zranitelností, Možnosti inventarizace pomocí protokolů vyšších vrstev např. přes LDAP, SNMP a další,
4	15.2.2018	8	8:00-16:30	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, Možnosti přímých útoků na síťová zařízení primárně s Cisco IOS, Ukázka DoS útoků, vyhladovění tabulky MAC adres atd., Obcházení firewallů, IDS a honeypotů, Možnosti logování běžné a nestandardní aktivity, Zajištění odezvy na nestandardní aktivitu v síti, Ukázka monitorovacích a detekčních nástrojů,
5	16.2.2018	8	8:00-16:30	Demonstrace útoků na WWW a proxy servery, Útoky na IPv6 např. pomocí nástroje EvilFOCA, Kontrola zabezpečení Web serveru MS IIS 7, Možnosti narušení bezpečnosti serverů přes dynamický kód – ActiveX, Chyby v implementaci Java Virtual Machine. Slabiny webovských prohlížečů, Ochrana vzdálených přístupů pomocí VPN a možné potenciální útoky, Možnosti zvýšení privilegií na vzdáleném systému a ukázka ovládnutí vzdáleného systému, Možnosti obrany proti technikám hackerů pomocí šifrování – SSL a IPSec a dalších speciálních technik, Činnosti prováděné po zjištění napadení počítače, Dohledávání aktivity útočníka, Skrývání stop nelegální aktivity, Možnosti standardních prostředků bezpečnostního auditu, Podporované souborové systémy, Vztah s klasickým UNIX modelem přístupových práv, Efektivní využití SSH, Konfigurace síťového přístupu pomocí klíčů, Doporučované postupy pro zabezpečení,
6	19.2.2018	8	8:00-16:30	Použití SSH pro vzdálený přenos souborů, Zabezpečení síťových služeb, Možnosti zabezpečení na aplikační úrovni (SSL), Možnosti a výhody zabezpečení na síťové úrovni, Zabezpečení přenosu na síťové úrovni, Koncept VPN, OpenVPN, Výhody a nevýhody, Konfigurace přístupového bodu, Nastavení klientů, Ipsec, Výhody a nevýhody, Možnosti využití Ipsec v tunelovacím a transportním režimu, Podpora IPSec na Linuxu, možnosti konfigurace, různé implementace Ipsec na Linuxu, Koncept PSK a certifikátů, Konfigurace IPSec tunelu mezi dvěma body, Efektivní tvorba firewallů, Blokování klientů, Omezení počtu, Šifrování souborů,
7	20.2.2018	8	8:00-16:30	Možnost využití PGP / GPG pro šifrování souborů, Podpora šifrování disků, Výhody a nevýhody SW a HW řešení šifrování, Koncept dmcrypt, Koncept encfs, výhody a nevýhody, Vytvoření zašifrovaného disku, Konfigurace SSL v webovém serveru Apache, Vytvoření certifikátů, Instalace certifikátů, Ověření funkčnosti, Preface: Security Administration, Introduction to Check Point Technology, Deployment Platforms, Lab: Branch Office Security Gateway Installation, Lab: CLI Tools, Introduction to the Security Policy, Lab: Building a Security Policy, Lab: Configure the DMZ, Monitoring Traffic and Connections, Lab: Monitoring Traffic with SmartView Tracker and SmartView Monitor
8	21.2.2018	5	8:00-14:00	Network Address Translation, Lab: Configuring NAT, Using SmartUpdate, User Management and Authentication, Identity Awareness, Introduction to Check Point VPNs, Lab: Site-to-Site VPN Between Corporate and Branch Office, SmartLog Lab: Using SmartLog to Review Off-line Logs, Security Engineering, Upgrading, Advanced Firewall, Clustering and Acceleration, Advanced User Management, Advanced IPsec VPN and Check Point Capsule, Threat Prevention, Intrusion Prevention Systém, Auditing and Reporting
9	22.2.2018	2	8:00-10:00	Závěrečná zkouška

Vyplňte pouze bílá pole

Datum:	30.1.2018
Vyřizuje:	XXX
Číslo telefonu:	XXX
Email:	XXX

jméno, příjmení, funkce a podpis oprávněné osoby (razítko)	Ing. Roman Kratochvíl, jednatel	
	v zastoupení Bc. Helešic	