Smlouva o realizaci expertního školení hackingu a jeho využití v praxi

Smluvní strany

Univerzita Hradec Králové, Fakulta informatiky a managementu (FIM)

Se sídlem: Rokitanského 62/26, 500 03, Hradec Králové

Zastoupená: prof. RNDr. Josef Hynek, MBA, Ph.D., děkanem

IČ: 62690094

DIČ: CZ62690094

Bankovní spojení: Česká spořitelna, a.s.

Číslo účtu: 2733582/0800

Kontakt: doc. Mgr. Josef Horálek, Ph.D., katedra informačních technologií; josef.horalek@uhk.cz

(dále jen „Objednatel")

a

TAYLLORCOX s.r.o.

se sídlem Na Florenci 1055/35, 110 00 Praha

zastoupená Aleš Pilný, jednatel

IČ: 27902587

DIČ: CZ27902587

bankovní spojení: RAIFFEISENBANK

číslo účtu: 4556253001/5500

(dále jen „Dodavatel ")

uzavírají podle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, následující **smlouvu.**

I. Předmět smlouvy

Dodavatel se zavazuje realizovat vzdělávací akce, konkrétně: 3 expertní školení v oblastech hakingu a jeho využitelnosti v praxi (dále též jen „Školení"), a to v souladu s Přílohou č. 1, v níž jsou identifikovány požadavky na jednotlivá Školení a Objednatel se zavazuje za tato Školení uhradit cenu sjednanou v čl. IV této Smlouvy.
Dodavatel prohlašuje, že má odbornou způsobilost pro splnění předmětu této Smlouvy a tato musí být platná po celou dobu trvání plnění dle této Smlouvy.

II. Místo plnění

Místem plnění je území České republiky, konkrétní místo plnění je u každého školení uvedeno v Příloze č. 1.

III. Doba plnění

1. Tato smlouva se uzavírá na dobu určitou; je splněna v souladu s harmonogramem (viz Příloha č. 1) realizací posledního Školení dle této smlouvy.

2. Konkrétní termín bude písemně dohodnut tak, že min. 4 týdny před konáním jednotlivého nebo více Školení dle Přílohy č. 1 zástupce Dodavatele a zástupce Objednatele dohodnou konkrétní den, čas a místnost konání jednotlivého nebo více Školení podle Přílohy č. 1.

IV. Cena

1. Cena za předmět plnění je sjednána dohodou smluvních stran a činí pro jednotlivá Školení dle přílohy:

   Školení 168.000 Kč bez DPH
   DPH 21 % 35.280 Kč
   Cena v Kč včetně DPH 203.280 Kč

2. Výše uvedené ceny pro jednotlivá školení je maximální a konečná. Cena zahrnuje veškeré náklady poskytovatele, a to zejména náklady spojené s realizací plnění, včetně ceny daní, inflačních vlivů, cestovného aj.

V. Platební podmínky

1. Objednatel se zavazuje uhradit cenu za předmět plnění na základě daňových dokladů- faktur vystavených poskytovatelem, který je oprávněn fakturovat cenu za plnění po nabytí účinnosti této smlouvy, a to vždy po bezvadné realizaci toho kterého Školení.

2. Dodavatel vystaví fakturu, které bude obsahovat a) označení zrealizovaného Školení s odkazem na přílohu s uvedením konkrétního data realizace, b) název projektu, z něhož je financováno, tj. „Rozvoj kapacit a adaptace na nové formy učení na UHK, NPO_UHK_MSMT-16601/2022". Faktura musí mít náležitosti daňového dokladu dle obecně závazných právních předpisů se dnem zdanitelného plnění určeným ke dni vydání faktury. Splatnost faktur činí 30 kalendářních dní od prokazatelného doručení Objednateli.

3. V případě, že faktura nebude mít stanovené náležitosti (příp. bude obsahovat chybné údaje), je objednatel oprávněn tuto fakturu vrátit ve lhůtě splatnosti poskytovateli, jenž je povinen vystavit novou fakturu se správnými náležitostmi. Do doby, než je vystavena nová faktura, není objednatel v prodlení se zaplacením ceny za plnění. Lhůta splatnosti nově vystavené faktury je rovněž 30 dní ode dne jejího doručení.

4. Stane-li se Dodavatel nespolehlivým plátcem ve smyslu § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (zákon o DPH), je povinen neprodleně o tomto informovat Objednatele.

5. Bude-li Dodavatel ke dni poskytnutí zdanitelného plnění veden jako nespolehlivý plátce ve smyslu § 106a zákona o DPH, je Objednatel oprávněn část ceny odpovídající dani z přidané hodnoty uhradit přímo na účet správce daně v souladu s ust. § 109a zákona o DPH. O tuto část bude ponížena fakturovaná cena a poskytovatel obdrží pouze cenu za plnění bez DPH.

7. Dojde-li po uzavření smlouvy ke změně účtu Dodavatele, který je zveřejněn na stránkách České daňové správy, je poskytovatel povinen o tom neprodleně informovat Objednatele. Smluvní strany se dohodly, že v takovém případě není nutné uzavírat dodatek ke smlouvě.

VI. Práva a povinnosti smluvních stran

1. Objednatel má právo na informace o průběhu vzdělávací akce, a to v kterékoliv fázi se právě nachází. Informace si může vyžádat telefonicky, e-mailem, písemně.

2. Objednatel má právo obdržet výsledky testování, pokud toto proběhlo.

3. Objednatel má právo znát jména lektorů na konkrétní vzdělávací akci. Má právo vyžádat si profil lektora. Rovněž má právo vyžádat si změnu lektora, pakliže má k tomu závažný důvod.

4. Dodavatel předá po skončení každého školení každému účastníkovi osvědčení o absolvování Školení, kde bude uveden název a číslo projektu, z něhož je Školení hrazena, tedy „Rozvoj kapacit a adaptace na nové formy učení na UHK, NPO_UHK_MSMT-16601/2022".

5. Dodavatel se zavazuje realizovat Školení dle svého nejlepšího vědomí s patřičnou odbornou způsobilostí, v požadovaném rozsahu a termínu.

6. Dodavatel zaručuje a odpovídá za to, že předané plnění odpovídá sjednané specifikaci, je bez faktických vad a právních vad i za to, že plněním této Smlouvy nebude zasaženo do práv třetích osob, a to včetně práv k předmětům duševního vlastnictví. Uplatněním nároku z odpovědnosti za vady není dotčen nárok Objednatele na náhradu újmy.

VII. Smluvní sankce

Smluvní strany se dohodly na následujících sankcích za porušení smluvních povinností:
a) v případě, že Dodavatel nezrealizuje Školení v den, který byl předem písemně odsouhlasen, má Objednatel právo na zaplacení smluvní pokuty ve výši 0,1 % z celkové dohodnuté ceny v Kč s DPH za toto Školení a současně má nárok na odstoupení od smlouvy bez náhrady za již uskutečněná školení, pokud se smluvní strany nedohodnou jinak

b) smluvní strany mají v případě nedodržení sjednaného termínu splatnosti kteréhokoliv peněžitého závazku nárok na zaplacení úroku z prodlení ve výši 0,05 % z neuhrazené částky do jejího zaplacení.

VIII. Závěrečná ustanovení

1. Smluvní strany shodně prohlašují, že si tuto smlouvu před jejím podpisem přečetly, že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle, určitě, vážně a srozumitelně.

2. Dodavatel bere na vědomí, že je osobou povinou spolupůsobit při výkonu finanční kontroly dle § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, v platném znění. Prodávající se zavazuje, že umožní všem subjektům oprávněným k výkonu kontroly projektu, z jehož prostředků je dodávka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu danou právními předpisy ČR k jejich archivaci (zákon č. 563/1991 Sb., o účetnictví, a zákon č. 235/2004 Sb., o dani z přidané hodnoty).

3. Dodavatel potvrzuje, že se na zpracování jeho nabídky nepodílel zaměstnanec Objednatele či člen statutárního orgánu Objednatele, statutární orgán Objednatele, člen řídicího orgánu Objednatele, člen realizačního týmu projektu či osoba, která se na základě smluvního vztahu podílela na zadání předmětné zakázky; prodávající rovněž prohlašuje, že s ohledem na plnění na základě své nabídky není ve střetu zájmu (viz ustanovení § 44 zák. č. 134/2016 Sb. ve znění novel).

4. Dodavatel prohlašuje, že veškeré práce na plnění této smlouvy budou prováděny v souladu s pracovněprávními předpisy (zejména při odměňování, organizaci pracovní doby, doby odpočinku, pravidel bezpečnosti a ochrany zdraví při práci), že všichni cizí státní příslušníci, kteří se budou podílet na plnění smlouvy, splňují podmínky pobytu a výkonu příslušné výdělečné činnosti cizinců (tedy zejm. mají potřebná povolení k pobytu na území České republiky, pracovní povolení, atp.) a všechny osoby podílející se na plnění smlouvy jsou řádně vedeny v příslušných registrech (vztahujících se zejm. k agendě daně z příjmů fyzických osob, veřejného zdravotního pojištění a sociálního zabezpečení); rovněž

prodávající prohlašuje, že jako poddodavatelé budou k plnění smlouvy využívány výhradně právnické či fyzické osoby s příslušným oprávněním k podnikání. Poskytovatel podpisem této Smlouvy též čestně prohlašuje, že vůči němu není orgánem veřejné moci zahájeno řízení pro porušení pracovněprávních předpisů a/nebo zákona č. 198/2009 Sb., antidiskriminační zákon, ve znění pozdějších předpisů a že řádně a včas splní finanční závazky vůči svým poddodavatelům, přičemž za řádné a včasné plnění se považuje plné uhrazení poddodavatelem vystavených faktur za plnění poskytnutá k plnění veřejné zakázky v souladu se Smlouvou uzavřenou s poddodavatelem. Porušení povinnosti uvedené v tomto článku je porušením Smlouvy se všemi z toho plynoucími důsledky.

5. Dodavatel prohlašuje, že se na nabízené plnění nevztahují sankce EU a rovněž že on sám, jeho poddodavatel, nebo dodavatel, se kterým podává společnou nabídku, není osobou, subjektem či orgánem uvedeným na sankčním seznamu EU, nebo jinak sankcionovanou osobou, subjektem či orgánem, na které se vztahuje zákaz zadat nebo dále plnit veřejnou zakázku podle evropské legislativy s ohledem na opatření vzhledem k činnostem Ruska destabilizující situaci na Ukrajině, tj. vůči mezinárodním sankcím (např. nařízení Rady č. 269/2014 či 208/2014 či 765/2014, 576/2022). Rovněž prohlašuje, že není veřejným funkcionářem dle § 4b) zákona č. 159/2006 Sb. ve znění novel.

6. Smlouva bude uzavírána elektronicky - smlouva bude uzavřena připojením elektronických podpisů obou Smluvních stran. V případě listinné verze je vyhotovena ve dvou stejnopisech s platností originálu, z nichž jedno vyhotovení obdrží Dodavatel a jedno vyhotovení obdrží Objednatel.

7. Tuto smlouvu lze měnit a doplňovat pouze písemnými dodatky podepsanými oběma stranami.

8. Smlouva nabývá platnosti dnem podpisu smluvních stran.

IX. POVINNOSTI DLE ZÁKONA Č. 340/2015 Sb.

v platném znění (dále jako „zákon o registru smluv")

1. Tato smlouva bude zveřejněna ve veřejně dostupném registru smluv a nabývá účinnosti tímto dnem zveřejnění, s nímž obě smluvní strany svým podpisem souhlasí.

2. Zápis do Registru smluv bude dále obsahovat údaje v souladu se zákonem o registru smluv.

3. Zveřejnění smlouvy provede smluvní strana Objednatele v souladu se zákonem o registru; až bude registrace provedena, Objednatel bude Dodavatele informovat.

Příloha

V Hradci Králové dne: 23.10.2023

(Objednatel)

V Praze dne 31.8.2023

TAYLLORCOX s.r.o.
Na Florenci 1055/35
110 00 Praha 1
IČO: 27902587
DIČ: CZ27902587

(Poskytovatel)

Příloha 1:

H. Principy a využití hackingu II

Seznámení se základními nástroji a principy v oblasti hackingu, které se používají pro útoky a penetrační testování patří mezi znalosti, jež umožňují zvýšení efektivity řešení informační a síťové bezpečnosti.

Počet účastníků: 2
Místo školení: prostory dodavatele
Typ školení: online
Ukončení kurzu: Certifikát o absolvování
Časová dotace: 40 hodin (8výukových hodin/den)
Pozn. Výuková hodina = 45 min.

Cíle školení:

Cílem školení je poskytnout seznámí se základními nástroji a principy, které se používají pro útoky a penetrační testování a umožní do detailu pochopit i vyzkoušet metody, pomocí kterých se provádí útoky na počítačové sítě a serverové systémy z vnitřní části sítě a při útocích Man-in-the-Middle proti klientům mimo vnitřní síť.

Minimální obsah kurzu:

- Analýza prostředí náchylných k sociálnímu inženýrství
- Skenování síťových služeb pomocí skenování otevřených portů a bannerů
- Analýza používaných operačních systémů
- Princip a aplikování ARP poisioningu pomocí nástrojů pro Microsoft Windows i Linux
- Principy ukládání hesel v operačních systémech
- Přenos hesel při síťovém ověřování
- Downgrade ověřovacích metod
- Útoky na hesla hrubou silou pomocí CPU, grafických karet a distribuovaného útoku
- Rainbow Tables - principy vyhledávání, způsob generování pro konkrétní prostředí a druhy útoků, analýza time/memory tradeoff efektu
- Analýza bezdrátových sítí v dosahu
- Zneužití neautorizovaných rámců
- WiFi Injection a monitor mód WiFi karet
- Útoky na WEP sítě
- Útoky na WPA1 PSK a WPA2 PSK sítě
- Prolamování EAPOL rámců pomocí grafických karet
- Vetřelecká AP
- WPS
- Zasílání falešných certifikátů, importování kořenových certifikačních autorit a vytváření legitimních falešných certifikátů obcházení HTTPS zabezpečení
- Využití Metasploit Frameworku pro exploitaci síťových služeb
- Skrývání prostředků pomocí rootkitů

H. Principy a využití hackingu II
Seznámení se základními nástroji a principy v oblasti hackingu, které se používají pro útoky a penetrační testování patří mezi znalosti, jež umožňují zvýšení efektivity řešení informační a síťové bezpečnosti.

Počet účastníků: 2
Místo školení: prostory dodavatele
Typ školení: online
Ukončení kurzu: Certifikát o absolvování
Časová dotace: 40 hodin (8výukových hodin/den)
Pozn. Výuková hodina = 45 min.

Cíle školení:

Cílem školení je naučit odhalovat a pro penetračního testování využívat nejzávažnější chyby, v bezpečnosti firem. Kurz naučí eticky zneužívat nejčastější chyby IT pracovníků, vytvářet malware pro vzdálené převzetí kontroly nad počítači, sledování aktivit uživatelů, získávání uložených tajemství, skrývání komunikace při ovládání obětí. Dále seznámí s útoky realizovanými pomocí USB zařízení a vytvářením kódu pro ovládání mobilních zařízení.

Minimální obsah kurzu:

- Zneužívání nejčastejších chyb v administraci ke kompletní kompromitaci sítě
- RDP MitM a session recording aneb vzdálený záznam klávesnice a obrazovky admina
- Chybné používání identit pro administraci, spuštění úloh a služeb
- Offline útoky pro ovládnutí domény
- Hesla a vykrádání tajemství z počítačů
- Zneužívání shadowcopy pro vykrádání databází, Active Directory a file serverů
- Zneužívání lokálních účtů ve výchozím nastavení
- Vykrádání paměti počítače, profilů a šifrovacích tajemství
- Pass The Hash aneb jak s údaji z paměti ovládnout vzdálené systémy a proč není třeba lámat hesla
- NTLM Relay aneb jak položit zcela vzdálené systémy, kam nikdo nechtěl přistupovat jen během útoků MitM
- Responder a podvrh legitimních cílů aneb jak snadno nalákat oběť a zneužít její výchozí nastavení
- Pass The Ticket aneb vykrádání Kerberosu
- Kerb roasting aneb kompromitace účtů služeb
- Golden Ticket prakticky - průstřel celého AD forestu pomocí jediné domény
- DMA útoky aneb jak obejít ochranu BitLocker
- Malware a vše na co jste se báli zeptat aneb jak ovládnout firmu na dálku a proč je většina firem prostřelená zevnitř
- Možnosti ovládání a sledování obětí
- Skrývání malware
- Opomíjená nastavení office
- Skrývání v registrech
- Šifrování
- Neobvyklé metody spouštění kódu
- Využívání skrytých kanálů a tuneling v jiných protokolech
- Pivoting aneb jak prostoupit z napadeného počítače dál do nepřístupného prostředí

I. Principy a využití hackingu III
Pokročilé techniky v oblasti hackingu zaměřené na pokročilé síťovéútoky pro detailní průzkum síťového prostředí a následné zneužívat slabiny v chybné implementaci zabezpečení ethernet i WiFi sítí je nedílnou součástí znalostí, které jsou nutné pro efektivní výuku bezpečnosti počítačových sítí.

Počet účastníků: 2
Místo školení: prostory dodavatele
Typ školení: online
Ukončení kurzu: Certifikát o absolvování
Časová dotace: 40 hodin (8výukových hodin/den)
Pozn. Výuková hodina = 45 min.

Cíle školení:

Cílem školení je naučit se pokročilé techniky napadání sítí, obcházet zabezpečení segmentace sítí do VLAN, prostřelit routery oddělující síťové segmenty. Dále je cílem naučit se testovat bezpečnost podnikových WiFi klientů a infrastruktury a seznámit se s principy SDR hackingu a útoky na BluetoothLE.

Minimální obsah kurzu:

- SPAN a RSPAN
- Vlan Hopping
- Útoky na 802.1x
- Man in the Middle i bez APR
- Statické zásahy do cache
- Statické zásahy do routingu
- Podvrhávání DHCP serveru
- DHCP Starvation attacks
- DNS spoofing a poisoning
- DNS typy záznamů a chyby v zabezpečení
- Probourávání identit pomocí falešných AP
- Zneužívání falešných AP pro otrávení klientů
- Zneužívání Hosted Networks jako backdoor do podnikového prostředí
- Skenování živých cílů i bez nmapu
- Skenování cílů, se kterými nejde komunikovat
- Enumerace aneb zjišťování detailů o napadeném prostředí
- SNMP aneb Security Not My Problem a jak může vést až k podrobení sítě
- Síťové útoky
- Instalace backdoorů do firmware
- Praktické otevření administrace pomocí CSRF útoků
- Přetečení paměti
- Session Hijacking
- Cross Site Request Forgery
- Cross Site Scripting
- Error Based SQL Injection vs. blind SQL injection
- Command injection
- Click jacking
- Princip SDR útoků
- Praktické testování SDR
- Útoky na BLE
- Statická analýza firmware
- Credential bruteforcing
- Napadání síťové komunikace
- Command injection