Masarykova univerzita v Brně

Filozofická fakulta

Ústav české literatury a knihovnictví

Kabinet informačních studií a knihovnictví

Závěrečný úkol do předmětu:

Informační bezpečnost

Autor: Michal Létal

UČO: 383687

Typ studia: prezenční

Ročník: druhý

Brno

8. 5. 2013

Oběť: Martin Horák

Postup:

Vycházel jsem z toho, že znám jméno kontaktu a jeho podobu. Následně jsem si vyhledal další informace na Informačním systému MU. Po té jsem se snažil zjistit nějaké informace pomocí Googlu. Tato metoda nebyl příliš úspěšná, protože jméno Martin Horák je v ČR velmi běžné. (Toto se ukázalo jako poměrně velká překážka.) Pomocí fiktivního účtu (hledání bez zaregistrování se do služby objevilo profil, nicméně nezobrazilo detaily) jsem našel jeho profil na LinkedIn, tato stopa však nevedla nikam dál. Po té jsem se snažil najít jeho profil na Facebooku. Hledání bez přihlášení nevedlo nikam, hledáním po přihlášení jsem byl schopen najít požadovaný profil. Z jeho profilu jsem vyvodil nějaké základní informace: Asi je z Dolních Bojanovic apod. S touto informací a s předpokladem, že v Bojanovicích chodil na ZŠ jsem dokázal na Spolužáci.cz identifikovat správného Martina Horáka. Posléze se mi podařilo prolomit heslo do jeho třídy na ZŠ. Tak jsem získal nějaké další informace. Když jsem se snažil ještě něco dalšího zjistit z jeho facebookového profilu zjistil jsem, že máme „společného známého“. Tuto osobu dále „kontakt“ jsem požádal, zda by mi byla ochotna, poskytnou nějaké informace o dotyčné osobě, kontakt souhlasil. Tak jsem se dostal k velmi detailnímu popisu cíle mých útoků. Mimo jiné jsem byl schopen najít další třídu na Spolužáci.cz, do které Martin chodil. Opět jsem měl štěstí při prolamování hesla a získal jsem tak další informace. Můj kontakt mi byl navíc ochoten pomoci s případným realizováním útoků.

Zjištěné informace:

IS MU

- studuje na PrF v programu: „Právní specializace“ obor: „Vyšší justiční úředník“. Ve druhém semestru
- na FF studuje v programu: „Obecná teorie a dějiny umění a kultury“, obor: „Estetika“ a obor: „Teorie interaktivních médií“

Facebook

- https://www.facebook.com/martin.horak.39 Autentizaci jsem provedl podle profilové fotografie a hlavně podle toho, že studuje na FF a PrF.
- profil má dostupný pouze pro přihlášené uživatele
- většinu informací sdílí pouze s přáteli
- Je členem skupin: Strategické plánování, studentoviny.cz, Debatní klub studentů MU (DK MU), FK Dolní Bojanovice, Policejní hlídky - Hodonínsko, eLAW.cz | právní portál, Hasičská noc 2012, Vinárna u Konšelů.
- Předpokládal jsem, že je z Dolních Bojanovic, a že tam nejspíše chodil na ZŠ.
- Hlavní poznatek byl, že znám osobu v blízkosti cíle, kterou jsem později kontaktoval pro sběr dalších informací.
- Získal jsem nějaké fotografie z jeho profilu.

Kontakt

- Vystudoval obor Technické lyceum na Střední škole průmyslové a umělecké v Hodoníně. Kde složil maturitní zkoušku, při níž ze všech předmětů dostal 1.
- Rok studoval na jazykové škole v Hodoníně. S největší pravděpodobností se jednala o školu IDEA (kontakt si nebyl zcela jistý).
- je věřící (římskokatolický křesťan)
- vytváří grafiky ve Photoshopu (získal jsem pár ukázek, které nemá na Facebooku uveřejněné)
- chodí v národním kroji
- je bývalý fotbalista
- posiluje, navštěvuje posilovnu v Dolních Bojanovicích
- má přítelkyni zjistil jsem i její jméno
- znám telefonní číslo
- věnuje se rychločtení, dělal kurzy na http://www.rozectise.cz
- oblíbená kniha: Cityboy
- oblíbené filmy: Forest Gump, Rio, 300, Saving Private Ryan, Výměna, Project X, RocknRolla, Seven pounds, Spartakus
- oblíbené tv pořady: Hyde park, Peklo na talíři, Tom a Jerry, Friends, Partička, Červený trpaslík, Futurama, The Big Bang Theory, How I Met Your Mother.
- Vyhraněný hudební styl nemá, poslouchá od roku až po hip-hop, přesto jsem dostal tip na skupiny jako Green Day, Simple Plan, Offspring, Linkin Park.
- Nemá rád tento druh emotikonů „ ;-) „.

Spolužáci

- Martin navštěvoval ZŠ Dolní Bojanovice, ročník ukončení 2006, třídu 9. A. Poté studoval na SŠPU a VOŠ v Hodoníně, třídu 4. A, rok ukončení 2010. Podařilo se mi prolomit heslo na otázku: „Co máme napsané na tričkách z devítky? (dohromady)“. (Předpoklad- nebude to moc dlouhé a asi bez diakritiky, nejméně dvě slova) a také na otázku: „Třídní učitel?...“ (jméno získáno z webu školy). Stačilo něco kolem dvaceti pokusů u obou otázek. To, že se jedná o relevantní osobu, jsem poznal z fotek ve fotogaleriích.
- Zjistil jsem datum narození
- ICQ
- 2 emailové adresy.
- Přezdívku (tu mi pak potvrdil i kontakt)
- Jména a kontakty spolužáků Martina
- Několik fotografií, na kterých Martin je

LinkedIn

- Autentizaci jsem provedl díky informacím z ISu. V profilu je uvedeno, že studuje PrF. na Masarykově univerzitě od roku 2012 do roku 2018. Podle ISu momentálně

žádný jiný Martin Horák na PrF MU nestuduje. Kromě výše uvedeného profil obsahuje pouze hlášku: „I law you“.

1. Útok

Díky spoustě informací a komunikačním kanálům, které se mi podařilo získat, bych se snažil oslovit Martinovy přátele a jeho jménem z nich vymámit peníze. Spolupracoval bych na tom s mým kontaktem, který by potvrdil mou totožnost. Mohl bych je kontaktovat s tím, že se Martinovy naskytla nějaká mimořádná příležitost například na extrémně výhodnou koupi auta a potřebuje půjčit peníze, které momentálně nemá, ale v blízké době je sežene a vrátí je ještě s nějakým bonusem. Peníze by potřeboval půjčit velmi rychle, jinak by auto koupil někdo jiný. Také bych se zaštítil tím, že můj kontakt mu již peníze poskytl (toto by kontakt potvrdil), takto bych se snažil oslovit co nejvíce jeho přátel v co nejkratší době s použitím co nejvíce možných komunikačních kanálů. Peníze by chodily na číslo účtu, které bych jim sdělil.

2. Útok

Zde bych využil znalosti toho, že se Martin věnuje učení se rychločtení na portálu Rozectise.cz. Kde bych mu v den jeho narozenin poslal spoofingový email z falešné adresy, který by se vydával za dárkový poukaz koupený jeho přítelkyní jemu k narozeninám. E-mail by obsahoval odkaz, který by po kliknutí na něj nainstaloval do počítače backdoor, který by později ovládl Martinův počítač.

3. Útok

Díky tomu, že vím, že má Martin málo vyplněný a téměř nevyužívaný profil na síti LinkedIn bych mu poslal e-mail ve kterém bych ho vyzval k tomu, aby si propojil tento účet se svým účtem na Facebooku. Součástí tohoto e-mailu by byl odkaz na phishingovou stránku. Tato stránka by ho vyzvala k zadání jak jeho hesla k profilu na LinkedIn tak Facebook. Tím bych získal obě hesla a mohl bych ovládnout oba jeho účty. S takto ukradenou identitou bych mohl páchat další trestnou činnost, např. šířit malware a nelegální obsah. Nebo se vydávat za Martina a poškodit jeho vztahy s okolím anebo to použít k něčemu podobnému jako v případě prvního útoku.

Oběť: Petr Šmíd

Postup:

Nejdříve jsem si v Informačním systému Masarykovy univerzity našel nějaké základní informace. Po té jsem se snažil pomocí Googlu vyhledat něco dalšího. Bohužel jméno Petr Šmíd je v ČR opět velmi běžné a nepodařilo se mi najít žádné profily, u kterých bych mohl s jistotou říci, že patří „mému“ Petru Šmídovi. Našel jsem spoustu profilů na Facebooku, LinkedIn, Spolužácích, Twitteru ale žádný jsem nemohl vyhodnotit jako relevantní. Zkoušel

jsem i další služby např. Foursquare, Lidé, Líbímseti, vše bez úspěchu. Nakonec jsem alespoň podle znalosti UČO a toho, že vím, že navštěvoval předměty Informační bezpečnost a Účast na konferencích, zjistil jeho přihlašovací jméno do WikiKnihovny, které je s UČO shodné.

Zjištěné informace:

IS MU

- Studuje obor: „Informační studia a knihovnictví“ ve čtvrtém semestru.
- Publikoval tři články na Inflow:
  1. ICT ve vzdělávání
  2. Jak vyzrát na sebezdokonalování v komunikačních a prezentačních dovednostech
  3. Seminář NAKLIV: Základy lektorské práce
- Školní e-mail
- UČO

Články na Inflow

- Účastnil se 7. – 8. listopadu 2012 konference ICT ve vzdělávání.
- 8. listopadu 2011 se zúčastnil semináře prezentačních a komunikačních dovedností.
- 5. Prosince 2011 se zúčastnil semináře základů lektorské práce.

WikiKnihovna

- Přihlašovací jméno na WikiKnihovnu

1. Útok

Na školní e-mail bych poslal Petrovi pozvánku na účast na konferenci ICT ve vzdělávání 2013, s odkazem na spoofingově upravené stránky, podobné těm z konference z minulého roku. (http://www.kurzyict.upol.cz/konference/) S tím, že letos je registrace zpoplatněna a cena je 1500 Kč. Přičemž registrace bude potvrzena až po zaplacení této částky na příslušný účet. Snažil bych se o to, aby fiktivní program byl co nejlákavější. Také bych využil technik sociálního inženýrství. Snažil bych se předstírat, že o konferenci je velký zájem a že zbývá posledních pár míst, abych Petra dostal pod tlak. E-mail bych pochopitelně poslal z falešného účtu, vydával bych se za Mgr. Zuzanu Pustinovou, která byla v loňském roce koordinátorkou konference. E-mail bych poslal z adresy podobné této: „ zuzana.pustinova@upol.cz“ což je adresa výše zmiňované koordinátorky.

2. Útok

K dalšímu útoku bych využil znalost přihlašovacího jména na WikiKnihovnu a školní e-mail. Přičemž, bych se vydával za člena týmu Knihovna.cz. Ke kontaktu bych se snažil použít adresu podobné této: „*kisk@phil.muni.cz*“ což je adresa uvedená v kontaktech projektu knihovna.cz. Na Petrův školní e-mail bych zaslal e-mail podobný tomuto:

„Dobrý den,

právě převádíme projekt WikiKnihovna na novou platformu a proto pokud chcete dále na Wikiknihovnu přispívat, prosíme, abyste se přihlásil svým přihlašovacím jménem (které je: „zjištěné přihlašovací jméno“) a heslem na této stránce *odkaz na falešnou phishingovou stránku*. Zde udělíte souhlas s převodem na novou platformu. Budete si moci také zvolit nové přihlašovací jméno a heslo (toto není povinné). V případě že neudělíte souhlas s převodem, bude celý obsah vytvořený Vámi na staré verzi do čtrnácti dní ztracen. (stará verze WikiKnihovny již nebude dále dostupná.) Celá operace vám nezaber více než 2 minuty.

S pozdravem

Technický tým projektu Knihovna.cz“

Ukradenou identitu bych použil k šíření zmatku na WikiKnihovně, nahrávání nelegálního obsahu a podobně. Také bych Petrovi mohl způsobit problémy s tím, že bych se za něj na Wikiknihovně vydával, odevzdal bych špatné úkoly apod.

3. Útok

Pod nějakou „důvěryhodně“ falešnou identitou např. PhDr. Petra Škyřika nebo Marie Dorazilové bych mému cíli poslal nějaký dotazník, který by byl určen pouze studentům 2. ročníku a vyžadoval by rychlé vyplnění (takové dotazníky studentům KISKu chodí poměrně často). V tomto dotazníku bych se snažil zjistit o Petrovi nějaké bližší informace, např. odkud je, co studoval za předešlou školu, jaké používá sociální sítě, jaké využívá online nástroje a služby. Celé bych se to snažil provést pod záštitou např. nějakého evropského výzkumu. Za vyplnění bych slíbil odměnu. Získané informace bych použil k naplánování dalších útoků.

Hodnocení úkolu

Úkol akceptuji, moc se mi líbil, jen bych uvítala, kdyby byly uvedeny formulace útočných zpráv. Protože ale vyly popsány charakteristiky obsahu pro důvěryhodnost, akceptuji znění.

Otázka pro kolokvium vychází z té drobnosti, co mi chyběla - Jak by zněla zpráva, která by přišla známým M. Horáka při prvním popsaném útoku?