Masarykova univerzita v Brně
Filozofická fakulta
Ústav české literatury a knihovnictví
Kabinet informačních studií a knihovnictví

Závěrečný úkol do předmětu:

Informační bezpečnost

Autor: Bc. Lukáš Horák

UČO: 426740

Typ studia: kombinované magisterské navazující

Ročník: 1. ročník navazujícího magisterského studia

Brno
18. 3. 2014

Oběť: Martin Páč

Postup:

Výchozím bodem pro shromažďování informací bylo jméno osoby (dále jen subjektu). Pomocí Informačního systému MU (dále jen IS MU) jsem zjistil podobu subjektu, jaký obor subjekt studuje a v jakém ročníku se nachází. Na IS MU jsem objevil spoustu užitečných informací (viz níže v části Zjištěné informace – IS MU) včetně přezdívky subjektu. S těmito informacemi jsem zkusil štěstí na sociálních sítích – Facebooku (dále jen FB). Subjekt nebyl na FB pod svým jménem dohledatelný, a proto jsem zkusil přezdívku (Polki), uvedenou na IS MU. Pod přezdívkou jsem nakonec našel pravděpodobný profil, autentizaci subjektu jsem provedl pomocí komparace fotky v IS MU a úvodní fotky na FB. Na FB jsem shromáždil většinu informací, na základě kterých bych byl schopen utvořit si celkový profil o subjektu včetně jeho charakterových, morálně-volních a osobnostních kvalitách a vlastnostech. Dále jsem hledal v internetovém vyhledávači Google, díky kterému jsem byl schopen vyhledat, že subjekt byl členem Divadla na Pavlači. Na stránkách divadla jsem našel další fotky a informace o subjektu.

Zjištěné informace:

IS MU

- Studuje prezenčně, jednooborové studium na FF v programu „Informační studia a knihovnictví“ v oboru „Informační studia a knihovnictví“. V současné době je v druhém semestru.
- Přezdívka „Polki“
- K aktuálním pozicím a projektům uvádí „Flákač“ s odkazem na web www.polkisk.tk
- Profesní zkušenost uvádí „Správce webu - Eshopu“
- Informace o vzdělání: EZŠ Jazyková škola, SŠ Ekonomie – obchod
- Subjekt uvádí že je zdatný v práci na PC, současně že PC je jeho zájmem/koníčkem
- V IS je záznam že subjekt okomentoval osobu jménem Anežka Adamcová, ke které má pravděpodobně kladný vztah (pokud by bylo zjištěno více informací, lze dále využít)

Facebook

- Subjekt se přidal na FB 24.12.2004
- Subjekt vystupuje na FB pod přezdívkou „Polki Skiller King“
- Jeho profil je veřejně přístupný a jeho News feed se dá veřejně číst (pokud jste uživatelem služby FB)
- Subjekt pracoval v letech 2011 – 2012 v Divadle na Pavlači (www.divadlonapavlaci.cz)
- Na FB lze potvrdit že subjekt studuje MU ve zmíněném oboru a programu
- V informacích o sobě subjekt uvádí že je nutné se zaměřit na určitou činnost, abychom měli pro co žít, abychom se stále měli na co těšit. Dále subjekt uvádí, že se nebojí smrti a že jeho vzorem je Walter White.

- Subjekt uvádí 4 motta, která pravděpodobně odráží jeho názor na svět a životní filosofii. Př.: „I will always Stay at Last Stand“.
- Subjekt uvádí jako místo svého aktuálního pobytu Brno, Česká republika
- Subjekt uvádí jako místo svého narození Brunoy, Francie
- Subjekt uvádí, že hovoří jazyky Česky a Americká angličtina
- Subjekt uvádí odkaz na svůj web: http://polkiserver.wbs.cz
- Subjekt uvádí svou oblíbenou muziku, mezi kterou se řadí Kurt Cobain, AC-DC, Systém of a Down, Slipknot. Tedy obecně rock a tvrdší muzika.
- Subjekt uvádí knihy, které ho zajímají (zejména Star Wars a fantasy), dále filmy, které ho zajímají (opět série a filmy Star Wars, dále např South Park. Obecně filmy fantasy charakteru či animované seriály pro dospělé).
- Subjekt uvádí velké množství her, které hraje a má rád (Battlefield, Star Wars…) z čehož usuzuji, že hodně času stráví u PC
- Skupiny, ke kterým se subjekt hlásí: Bláznivé Odpoledne 23.11.2013, Prváci MUNI 2013/2014, Dřevomil.cz, Tréningy v Lužánkách ve městě Brno, Strojvedoucí, At si ženský vyskouší Erekci v Tramvaji , v létě a v kraťasech , Folklorní soubor POLAJKA.
- Na FB přidává subject příspěvky s frekvencí cca 1x za měsíc
- Přátele má subject zablokované zřejmě kvůli ochraně soukromí
- Hlavní fotka na FB profilu subjektu potvrzuje zálibu ve fantasy a Star Wars.

Webové stránky Divadla na Pavlači, sekce Spící členové

- Fotky subjektu
- Internetové stránky obsahují informace o osobnosti subjektu a o charakteru (temperamentní), dále pak i o původu (podle webu je subjekt potomkem kočovných Tatarů, kteří, procházejíc tehdejším územím Velké Moravy, zapustili kořeny na úrodných vinohradech, což vyvrací informaci z FB že subjekt pochází z Francie)
- Text na stránkách uvádí, že subjekt chodí ozbrojen (žádné další informace) a že pro ránu nechodí daleko

Další

- Účet na stream.cz pod přezdívkou Polk.i
- Přispěvatel do programu/databáze cheatů Scorpions Software
- Účet pod přezdívkou Polk.i na serveru www.lide.cz

Spolužáci

- Díky údajům o škole, přezdívce uvedené na IS a jménu subjektu jsem si byl schopen najít skupiny na serveru www.spoluzaci.cz ke kterým subjekt patří a současně jsem si potvrdil kam subjekt chodil do školy.
- 9.A, rok ukončení 2008
- EP 4.A, rok ukončení 2012
- xxx, rok ukončení 2008, ZŠ Evropská, Čejkovická 10

Další sociální sítě, instant messengery

- Zaregistrován pod přezdívkou Polki Polki s uvedením že je Profesionál v oboru počítačových her
- ICQ: 213144356, vystupuje pod jménem „Martin Polki“

Emaily

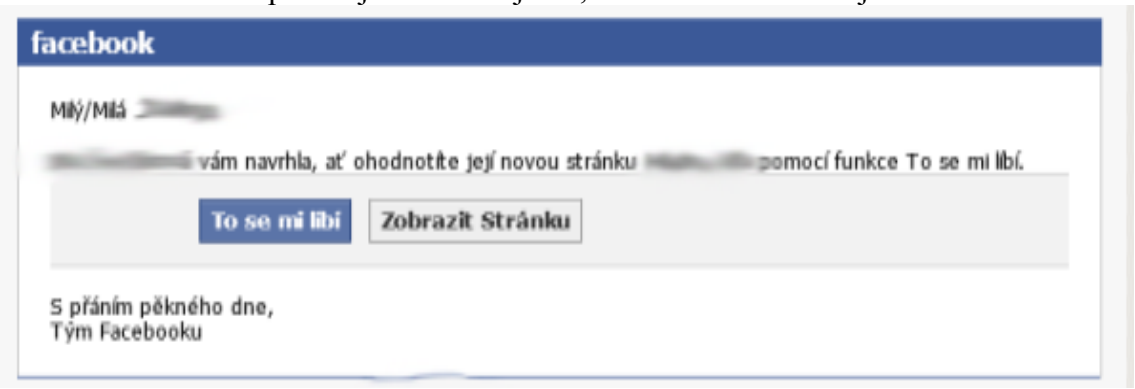
- polki@post.cz
- polk.i@seznam.cz

Web

- http://polkiserver.wbs.cz/
  Webové stránky o hře Star Wars: Jedi Outcast – Jedi Academy. Subjekt poskytuje server, kde s přáteli tuto hru hrají.
- IP adresa serveru (pravděpodobně i PC subjektu): 83.240.3.51.21000

1. Útok

Přestože subjekt nějakou dobu působil v Divadle na Pavlači, na FB do oficiální skupiny Divadla na Pavlači nepatří – neklikl na možnost „To se mi líbí“. Proto bych mu poslal z falešné emailové adresy v podobě notification@facebook.com email se subjektem „Divadlo Na Pavlači Vám doporučuje své stránky“.
Email by obsahoval standardní FB email (viz obrázek níže) s tlačítkem / odkazem na falešnou phishingovou URL adresu v podobě FB, kde by subjekt musel zadat své uživatelské jméno a heslo aby se na FB přihlásil. Jakmile by to udělal, získal bych jeho uživatelské jméno a heslo a to bych poté mohl využít např. ke kontaktování jeho přátel s cílem získat z nich peníze jménem subjektu, či zdiskreditovat subjekt.



2. Útok

Protože má subjekt kladný vztah osobě „Anežka Adamcová – spolužačka z MU, vytvořil bych si falešné ICQ na jméno Anežka Adamcová a snažil bych se hrát na subjekt na city, že se mi líbí a že je mi s ním dobře.
Poté co bych rozproudil konverzaci, snažil bych se využít výhody komunikace s opačným pohlavím a snažil bych se provádět sexting s cílem získat nějaké kompromitující fotky od subjektu (k navnazení bych mu nějaké fotografie ženy odpovídající Anežce ze serverů s pornografickou tématikou poslal jako první) s cílem subjekt diskreditovat. Poté bych mohl subjekt vydírat s tím, že jeho fotky uveřejním, pokud mi např. nezaplatí či neprovede nějaký skutek v mém zájmu.

3. Útok

Jelikož je subjekt fanda do ságy Star Wars, zejména pak do PC her série Jedi Outcast, vytvořil bych v Adobe Photoshopu profesionálně vypadající grafiku (něco ve stylu http://www.lucasarts.com/games/theforceunleashed2/game/index.html) a poslal bych přes falešný email vedoucího klanu FW (klan, kterého je subjekt součástí) – Thorna – email s textem přesvědčující subjekt o tom, že společnost LucasArts vyvíjí nové Jedi Academy II a kliknutím na odkaz se může subjekt podívat na více informací. Subjekt,

který by byl v úžasu a zároveň velice šťastný že se společnost LucasArts po deseti letech rozhodla udělat pokračování série by neváhal na odkaz kliknout. Odkaz by ale vedl na falešnou stránku, po jejíž nakliknutí by se stáhl a nainstaloval do PC subjektu malware. Tento malware by si nainstaloval backdoor, pomocí kterého bych poté mohl ovládnout PC subjektu.

Oběť: Václav Piták

Postup:

Výchozím bodem byl stejně jako u předchozí oběti IS MU, kde jsem našel fotku a obrázek subjektu. Jméno subjektu jsem vložil do vyhledávače Google a zkontroloval obrázky. Vyhledané obrázky pomocí služby Google jsem porovnal s fotkou na IS MU a pomocí Googlu jsem tak zjistil Facebook subjektu a následně několik dalších skutečností, jako např. že je redaktorem na serveru http://pasaz.abysszine.com/ a že pracuje pro společnost Kofi-Kofi. Subjekt byl velmi jednoduše dohledatelný, na sociálních sítích podle svého jména, a profil má nezabezpečený a otevřený, čili každý ho může na základě různých uvedených údajů identifikovat a zjistit podrobnosti o jeho životě, práci, zálibách i studiu. Díky profilu na různých internetových stránkách na základě emailu (bandzone.cz) lze dohledal další údaje jako například věk subjektu a místo narození (24 let, Otínoves).

Zjištěné informace:

IS MU

- Studuje prezenčně, jednooborové studium na FF v programu „Informační studia a knihovnictví“ v oboru „Informační studia a knihovnictví“. V současné době je ve čtvrtém semestru.
- Více informací na IS MU uvedených není, jedinými záchytnými body tu tedy byla fotka subjektu a jméno.

Facebook

- Pracuje jako Fly-boy (servíruje kávu) ve společnosti Kofi-Kofi (od r. 2010)
- Volně dostupné fotky
- Žije v obci Otínoves
- Studuje na MU, předtím studoval na Střední průmyslové škole Prostějov
- Poslouchá tvrdou muziku, hlavně death metal a metal (kapely AHAB, Six degrees of separation, Insania apod.)
- Má rád seriály Dexter, Breaking Bad, Red Dwarf, Black Books, Partička
- Jako inspirativního člověka označil Tonyho Hortona – ikonu fitness
- Patří do šesti skupin: Filmy o kterých se nepíše., DJ Root, Nový Prostor a jeho přátelé, Knižní bazar, RC Brooklyn, motivačák- módní přehlídka
- Má rád fotbal, týmy které se mu pravděpodobně líbí jsou Juventus Southampton FC
- Příspěvky na FB přidává velmi sporadicky, cca 1-2x za měsíc

Server abysszine.com

- Subjekt zde působí na pozici redaktora, k autentizaci byl použit facebookový profil a fotka
- Díky serveru lze dohledat FB
- Díky serveru lze dohledat email: venca.pitak@gmail.com
- Články, které subjekt píše vypovídají o tom, co ho zajímá – nejen psaní, ale také poslech zejména death metalové hudby

Server bandzone.cz

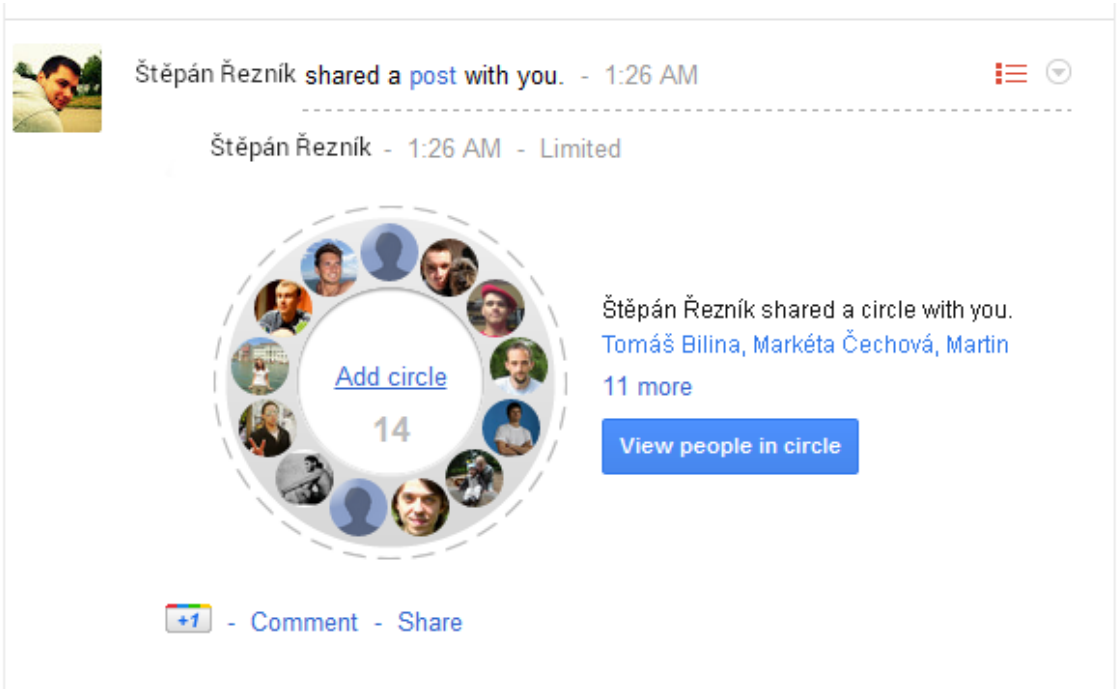
- Profil na serveru bandzone.cz. Zde uveden věk a místo narození. Také zde uvedena přezdívka Washek
- Dále je zde uveden email subjektu a ICQ (191229864)

Další

- ICQ pod přezdívkou „Pitva“. ICQ: 191229864
- Skype pod přezdívkou “abigar90”. Dohledatelné pod jménem “Václav Piták”. Dohledatelné pomocí emailu.
- Dále používaná přezdívka “Satyr”
- Účet na stránkách online hry “Chmatákov online” dostupné na http://www.chmatakov.cz/uzivatele/3654. Zde mj. Uveden email I ICQ subjektu.
- Spolužáci.cz:
  Subjekt se objevuje v těchto skupinách: E1-4A, rok ukončení 2010, SOŠ průmyslová a SOU strojírenské, Lidická 1686/4 (dříve SPŠ a SPŠ strojní), Prostějov
- Na Youtube má profil https://www.youtube.com/user/Abigar666
- Na Google plus má profil https://plus.google.com/u/0/104248777728517517695/about

1. Útok

Na účtu Google Plus je uvedeno, že subjekt má v kruzích osobu jménem Štěpán Řezník – následně jsem zjistil, že je to spolužák subjektu. Využil bych tedy informaci že subjekt má tuto osobu v kruzích a poslal bych mu falešný email z adresy googleplus@google.com pobízející k potvrzení kruhu. Email by vyzýval subjekt standardním způsobem, aby se přidal do dalšího kruhu, ve kterém by byli lidé z jeho okolí/kruhu (lidé studující jeho obor KISK – okruh lidí se dá získat přes kruhy na IS MU: https://is.muni.cz/auth/lide/lide_kruhy.pl?lang=cs;uco=413505). Poté, co by subjekt klikl na odkaz, musel by se standardně přihlásit přes falešnou phishingovou adresu do svého účtu google plus. Tímto bych získal heslo k emailu subjektu. Náhled (vytvořeno jednoduše pomocí Photoshopu) emailu níže:



2. Útok

Jelikož má subjekt na výše zmíněných serverech o své osobě velké množství volně šiřitelných informací, včetně fotek, nebyl by problém provést krádež identity. Realizaci bych provedl tím způsobem, že bych založil nový profil na jméno a přezdívku subjektu, s podobnými či stejnými zájmy a propojil bych tento profil pro zvýšení kredibility s účty jakými je Google plus, Youtube a ostatní. Přátelům subjektu (jsou volně viditelní) bych napsal, že jsem si vytvořil nový profil, protože na ten starý mi někdo zjistil a změnil heslo: „Ahoj, starý profil už nepoužívám, protože mi někdo vzal heslo, přidej si mě prosím tě pod tímto profilem a ten starý z přátel vymaž.“. Následně bych na profilu mohl psát velmi negativní příspěvky na adresu společnosti Kofi-Kofi, týkající se nekvalitních surovin, odporných praktik při servírování a šikanování podřízených. Tímto bych pravděpodobně brzy docílil toho, že subjekt přijde o zaměstnání. Dále bych mohl psát erotické zprávy známým subjektu s cílem diskreditovat jej.

3. Útok

Třetím útokem by byly nevyžádané emaily (SPAM). Jednoduše co bych udělal je registrace subjektu pomocí jeho emailové adresy do co největšího množství databází newsletterů a na co největší množství serverů. Jelikož programuji webové stránky tak vím, že některé formuláře newsletteru fungují tak, že po registraci do newsletteru pošlou potvrzení uživateli na registrovaný email, ale některé (a to většina) tuto proceduru nevykoná (protože se jedná o velmi jednoduchý script). Registrace do několika desítek různých newsletterů různých firem povede k tomu, že v delším časovém horizontu bude subjektu chodit spoustu obchodních sdělení a emailů. Každý tento email standardně obsahuje odkaz na deaktivaci, současně ale každá mnou provedená registrace do newsletteru na serverech vede k tomu, že se emailové adresa subjektu šíří internetem, sdílí, multiplikuje a kopíruje a je dále využívána v databázích. Je to tedy celkem rafinovaný útok na dlouhou trať, který ale vždy povede k úspěchu (systém tak prostě funguje). Proto tomuto bohužel není jiné obrany, než nakonec emailovou adresu zrušit.