KAPITOLA 3

Interní penetrační testy firemních sítí

V této kapitole se dozvíte:
- Úvod
- Případová studie
- Fáze 1: Cíl a rozsah penetračního testu
- Fáze 2: Sběr dat
- Fáze 3: Skenování a exploatace
- Fáze 4: Report
- Závěr
- Reference

Úvod

Třetí kapitola této knihy navazuje na předchozí kapitolu a bude věnována penetračním testům firemních sítí z vnitřní strany. Z vnitřní strany mohou ohrožovat firemní síť a firemní data vlastní zaměstnanci, zejména ti, kteří mají nekalé úmysly.

Podle průzkumu, který v březnu 2011 provedla společnost GFI software mezi bezpečnostními experty, IT manažery a administrátory, se podniky v České republice zaměřují zejména na sledování stavu serverů a síťových prvků a detekci útoků z vnější strany sítě. Riziku, které přichází z vnitřní strany, z řad vlastních zaměstnanců, se taková pozornost nevěnuje.

Výše uvedené tvrzení dokládají výsledky, které vyplynuly z průzkumu. Podle nich:

- 43 % podniků využívá pro log management specializované nástroje,
- 42 % podniků provádí pouze manuální kontrolu,
- 7 % dotázaných oba výše uvedené přístupy kombinuje,
- 8 % podniků neprovádí log management vůbec.

V rámci log managementu společnosti nejvíce sledují:

- provozní stav své sítě a jejích prvků – 65 %,
- detekci nestandardních aktivit uživatelů – 65 %,
- rozpoznání útoku z vnější sítě – 60 %.

Naopak jen 45 % firem kontroluje riziko zneužití dat v síti vlastními zaměstnanci a pouze 27 % využívá tyto nástroje k dosažení shody s průmyslovými a právními normami. [1]

Jak vyplývá ze studie s názvem 2011 Cost of Data Breach Study, která byla prezentována v první kapitole této knihy, kriminální útoky, krádeže a nedbalost zaměstnanců a dodavatelů tvoří majoritní podíl na příčinách firemních ztrát.

Právě z toho důvodu byla problematika vnitřní bezpečnosti zařazena do této knihy. V následujícím textu bude možné najít mezi probíranými oblastmi například:

- ukázku zdrojů informací, které mohou posloužit při návrhu testů zaměřených na otestování vnitřní bezpečnosti,
- ukázky práce s některými zdroji těchto informací,
- tipy pro filtrování informací z logovacích souborů,
- ukázky testovacích nástrojů od společnosti Microsoft,
- testování síťových zařízení Cisco,
- offline a online prolamování hesla.

Případová studie

Zájem firmy o vnitřní bezpečnost by měl pramenit z vlastní iniciativy, a nikoliv až z objevení prvního problému. Následující krátký příklad ukazuje, jak by mohl vypadat požadavek společnosti na otestování vnitřní bezpečnosti.

Společnost chce otestovat firemní síť z vnitřní strany a najít potenciální slabiny, které by mohly být zneužity. Firma se pro testování rozhodla z vlastní iniciativy, jelikož konkurenční firma v oboru se objevila v médiích, kde došlo k úniku privátních dat na veřejnost.

Firmu zajímají odpovědi na otázky:

- Co by mohlo způsobit společnosti problém?
- Jak velká škoda by vznikla v případě, že by se potenciální problém stal skutečností?
- Jak velké je riziko, že skutečně dojde k těmto problémům?
- Kde jsou inkriminovaná data nebo informace uloženy?
- V jaké formě jsou soubory/data/informace uloženy?
- Jak se může útočník dostat k uvedeným souborům/datům/informacím?
- Jsou tyto soubory/data/informace nějak chráněny?

Firma v závěrečné zprávě požaduje identifikaci rizik a určení cílů potenciálních útoků, jež by mohly být provedeny ze strany zaměstnanců, kteří mají v úmyslu poškodit firmu způsobením škody, odcizením dat nebo poškozením firemních zařízení.

Fáze 1: Cíl a rozsah penetračního testu

V následujícím textu bude popisován další možný pohled na bezpečnost firemní sítě. V této fázi 1 budou představeny body, odkud je možné čerpat inspiraci při návrhu cílů jednotlivých testů. Testy by měly být zaměřeny na místa, která mohou představovat slabinu ve firemní síti. Fáze 2 navazuje na první fázi. V ní budou detailněji představeny jednotlivé body, nástroje a postupy pro získávání detailnějších informací o firemní infrastruktuře.

Při určování hlavních cílů testů zabezpečení sítě je možné použít přístup, který byl představen ve druhé kapitole v sekci **Případová studie**. Jiným možným pohledem na situaci bezpečnosti je zaměření se na tyto základní části [5]:

- Zabezpečení IT infrastruktury
- hardwarové zabezpečení
- softwarová ochrana
- Ochrana před selháním lidského faktoru

Zabezpečení IT infrastruktury

Zabezpečení firemní síťové infrastruktury je možné dále rozdělit na hardwarovou a softwarovou část.

Hardwarovou částí zabezpečení je myšlena fyzická ochrana firemních zařízení. Ochrana má za úkol zamezit nežádoucím změnám na zařízeních ze strany cizích osob – zaměstnanců, klientů nebo například studentů. Podrobnější informace jsou probírány v testu 1 ve fázi 3 této kapitoly.

Druhou částí je softwarové zabezpečení, čímž je myšlena ochrana na abstraktní vrstvě. Ochrana je většinou zajišťována pomocí restriktivního nastavení systému, systémových politik nebo aplikací třetích stran. Detaily jsou popisovány v testu 2 ve fázi 3 této kapitoly.

Ochrana před selháním lidského faktoru:

Do této kategorie spadají opatření a testy, které mají zamezit lidským chybám, způsobeným nedbalostí nebo záměrně s cílem poškodit firmu. Detaily k této kategorii je možné najít například v testech 3, 12 a 13 ve fázi 3 této kapitoly.

Riziko úniku dat

Jak již bylo zmíněno v první kapitole, pro firmy představuje odcizení interních dát ztrátu. Pro vytvoření prvotní představy o míře rizika ztráty interních dat ve vlastní firmě je možné vypočítat hodnotu přibližně podle *kalkulátoru míry rizika úniku firemních dat*, který byl vytvořen společností Symantec. Dotazníkový kalkulátor je dostupný na webových stránkách:

Web: `www.databreachcalculator.com/Default.aspx`

Dotazník se v třinácti krocích dotazuje například otázky týkající se oblasti působení firmy, počtu zaměstnanců, typu záznamů, které firma uchovává, firemní politiky nebo používání šifrování.

Po dokončení průzkumu je zobrazen stručný výsledek. Příklad výstupu kalkulátoru ukazuje následující výstup:

```
Results

Based on your inputs and our trend data, your risk exposure is:

Companies in your industry with your risk profile have a likelihood of
experiencing a data breach in the next 12 months of  9.3%

Your average cost per record is  € 124

Your average cost per breach is  € 930,833
```

Inspirace pro volbu cílů

Návrh cílů může vycházet z informací, které může o firemní síti shromáždit administrátor. Pro sběr potřebných informací je možné použít například tyto zdroje:

- Mapu firemní sítě – analýzou mapy sítě je možné určit kritická místa sítě, která mohou obsahovat důležité informace. Například přes hraniční firewall nebo směrovač prochází veškerá síťová komunikace – proto by měl být v centru pozornosti.
- Typy síťových zařízení a jejich konfigurace – tento návrh vychází z předchozího bodu a nabízí možnosti, kam je také vhodné zaměřit pozornost. Určíme-li, jaké zařízení se v síti nachází, je možné dále určit, jaké informace lze ze sítě získat. V případě, že se v síti nachází IDS zařízení, je z pohledu administrátora možné získat jiné informace než z přepínače, tiskového nebo proxy serveru.
- Záznamové soubory – s pomocí záznamových souborů (logů) lze odhalit celou řadu aktivit, například zjistit, kdo a z kterého počítače se ve sledovaný okamžik přihlásil do sítě, kdo tiskl na tiskárně, kdo v daný okamžik otevřel dané dveře svou čipovou kartou, kdo a kdy přistoupil k danému souboru a mnoho dalších informací.
- Firemní bezpečnostní politiky, interní směrnice – tyto politiky a směrnice určují (svým způsobem nařizují) postupy, jak se mají zaměstnanci chovat a postupovat v určitých situacích. V některých případech může být v těchto firemních nařízeních nalezena chyba, nesrovnalost nebo mezera, která může být zneužita pro nekalou aktivitu.

V tomto případě se jedná o testování white-box metodou. Jde o cílenou analýzu firemní sítě a vyhledávání potenciálně rizikových míst s tím, že objevené body budou následně otestovány podrobněji.

Fáze 2: Sběr dat

Pro získávání informací o firemní síti a vyhledávání slabin a potenciálních cílů pro útok je nezbytný sběr informací. Návrhy na několik zdrojů, z nichž mohou být tyto informace získány, byly představeny na předchozích stránkách. V dalším textu následuje několik tipů, jak tyto informace sbírat, a pár ukázek, jak mohou tyto informace vypadat.

Architektura sítě

Mapa sítě může být zaznamenána v různých podobách, v různých aplikacích. Příkladem aplikace, která umožňuje zaznamenávat a sledovat počet a aktivitu (zapnuté/vypnuté) zařízení v síti, je Friendly pinger. Aplikace tohoto druhu mohou být využity při analýze síťové topologie a architektury.

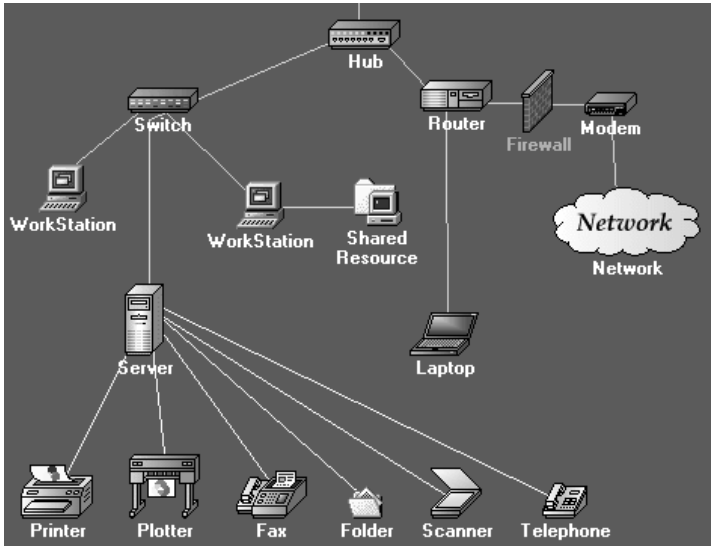
Instalační balík aplikace je dostupný na webových stránkách:

Web: `www.kilievich.com/fpinger`

Popisovaná aplikace je volně dostupná a nabízí poměrně rozsáhlou funkcionalitu. Nástroj umožňuje automaticky mapovat zařízení v síti a v zakreslované mapě vytvářet jejich přepojení. U jednotlivých zařízení a stanic je možné:

- přikládat detailní textové záznamy,
- sledovat jejich hardwarovou konfiguraci,
- kontrolovat nainstalované aplikace.

Prostřednictvím kontextového menu je možné provádět základní testy dostupnosti. Obrázek 3.1 demonstruje mapu, která je vytvořena v této volně dostupné aplikaci.



Obrázek 3.1 Friendly_pinger

Prohledávání logů

Logy neboli záznamové soubory obsahují záznamy o událostech, které proběhly v aplikacích, systémech a sítích. Informace, které jsou v těchto souborech, lze využít pro jakoukoliv analýzu chyb, optimalizaci, záznam akcí a chování aplikací a uživatelů.

Existuje několik úrovní těchto záznamů od relativně informativních, kde jsou zaznamenány jenom základní informace a nejdůležitější proběhlé události a akce, až po velice detailní záznamy, které popisují téměř každý krok a akci, jež byla vykonána. Se zvyšující se úrovní logování rostou nároky na systémové prostředky a diskový prostor. V některých případech je téměř nereálné používat plné logování.

Typickým příkladem může být zaznamenávání u mobilních operátorů. V případě hlasových služeb zaznamenává operátor o každém proběhlém hovoru pouze identifikátor volajícího a volaného, místo, čas hovoru, dobu hovoru a ostatní detaily. Obsah hovoru není v podstatě reálné zaznamenávat, jelikož na denní množství provedených hovorů by se jednalo o obrovské množství dat, která by bylo potřeba zpracovávat v reálnem čase a ukládat na datová úložiště.

S pomocí aplikačních logů vytvořených bezpečnostními aplikacemi, které běží na koncové stanici, jako například antivirusový software, softwarový firewall, lze objevit infekce a útoky šířené v síti.

Příklad záznamu v logu:

Antivirový program (detekce testovacího viru Eicar):

```
  [RS] DEBUG 2012-04-13 05:54:32,276 PID:3264 THID:4004 MSG:OnScanResult():
obname 'eicar.com', objtype=0, detname '@EID_Id_vir|%name%=EICAR_
Test|%idn%=07616d9a80000000|', dettype=4, curtype=2, flags=262400

  [RS] DEBUG 2012-04-13 05:54:32,276 PID:3264 THID:3984 MSG:Scanned 68 bytes in
188 ms @ 0 kBps

  [RS] INFO 2012-04-13 05:54:32,276 PID:3264 THID:3984 MSG:Infection '@EID_Id_
vir|%name%=EICAR_Test|%idn%=07616d9a80000000|' found!

  [RS] DEBUG 2012-04-13 05:54:32,276 PID:3264 THID:3984 MSG:Native file name: '\
Device\HarddiskVolume1\Users\tester\Downloads\eicar_com\eicar.com'
```

Dalším ze záznamových souborů, které stojí za pozornost, jsou logy vytvořené zařízeními, jež zabezpečují sledování komunikace v síti nebo se na něj specializují. Příkladem může být záznam:

- relací vzdáleného přístupu, kde jsou zaznamenávány informace o uživateli, čase a době vzdáleného připojení. Záznam je možný i o relacích VPN připojení.
- webové proxy, která zaznamenává navštívené webové stránky.
- IDP/IPS systémů, které sledují chování aplikací a uživatelů v síti a reportují o každém chování mimo standardně nastavená pravidla.

- směrovačů a firewallů; prostřednictvím záznamů vytvořených na těchto zařízeních lze sledovat například typy síťového provozu, který prochází sítí, pokusy o připojení do podsítí, kde je omezený přístup. Záznamy firewallů umožňují získávat detailnější informace než logy z routerů. Tato zařízení bývají vstupní bránou do firemní sítě z vnějšího světa. Proto by jim měla být věnována pozornost také při prevenci a případné analýze útoků na síť z vnějšího světa.

Příklady záznamů v logu:

Vzdálený přístup (vzdálený přístup na stanici):

```
Dec  9 19:45:37 teststation NetworkManager: <info>  Starting VPN service 'org.
freedesktop.NetworkManager.pptp'...

Dec  9 19:36:37 teststation NetworkManager: <info>  VPN service 'org.
freedesktop.NetworkManager.pptp' started (org.freedesktop.NetworkManager.pptp),
PID 7371

Dec  9 19:36:37 teststation pptp[7376]: nm-pptp-service-7371
log[main:pptp.c:314]: The synchronous pptp option is NOT activated

Dec  9 19:36:37 teststation NetworkManager: <info>  VPN connection 'Shinjiru 1'
(Connect) reply received.

Dec  9 19:36:37 teststation pptp[7476]: nm-pptp-service-7371
log[ctrlp_rep:pptp_ctrl.c:251]: Sent control packet type is 1
'Start-Control-Connection-Request'

Dec  9 19:36:37 teststation pptp[7476]: nm-pptp-service-7371 log[ctrlp_
disp:pptp_ctrl.c:739]: Received Start Control Connection Reply

Dec  9 19:36:37 teststation pptp[7476]: nm-pptp-service-7371 log[ctrlp_
disp:pptp_ctrl.c:773]: Client connection established.

Dec  9 19:36:38 teststation pptp[7476]: nm-pptp-service-7371 log[ctrlp_
rep:pptp_ctrl.c:251]: Sent control packet type is 7 'Outgoing-Call-Request'
```

Webová proxy (připojování přes webovou proxy):

```
12-04-2012 10:19:21 -  INFO - URL is: https://testovaciweb.cz:10000

12-04-2012 10:19:21 - DEBUG - Base URL is: testovaciweb.cz:10000

12-04-2012 10:19:21 - DEBUG - Sanitized 'testovaciweb.cz:10000' to
'testovaciweb_cz_10000'

12-04-2012 10:19:21 - DEBUG - No auth data

12-04-2012 10:19:21 - DEBUG - Setting referer to: http://novyweb.co.uk/proxy/
```

Směrovač (přihlašování do konfigurace zařízení):

```
%SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: test] [Source: 172.16.1.1]
[localport: 23] at 19:10:27 UTC Sat Dec 2 2006

1d04h: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: a] [Source: 192.168.0.10]
[localport: 80] [Reason: Login Authentication Failed - BadPassword] at 19:35:53
UTC Sat Dec 2 2006
```

Hlavní nevýhodou prohledávání těchto záznamových souborů je jeho obrovská časová náročnost. Záznamy obsahují obrovské množství dat a informací, může se jednat o objemy řádově ve stovkách megabajtů. Při analýze je tedy třeba vědět, co hledáme.

S pomocí filtračních pravidel nebo skriptů lze vyfiltrovat jenom chybové záznamy a následně se zaměřit na konkrétní záznam na stanici nebo na záznamy v určitém časovém rozpětí.

V souvislosti s prohledáváním záznamových souborů může vzniknout otázka, kde se tyto soubory nacházejí. Na operačním systému Linux lze systémové a aplikační logy najít na adrese:

/var/logs

V případě operačního systému Windows však není odpověď jednoznačná. Některé aplikace mají logy uloženy v adresáři, kde je aplikace nainstalována, některé využívají úložiště **ProgramData**, v jiných případech se využívá systémový adresář **Windows**, kde bývají také uloženy systémové logy. Místo uložení záleží na operačním systému a aplikaci.

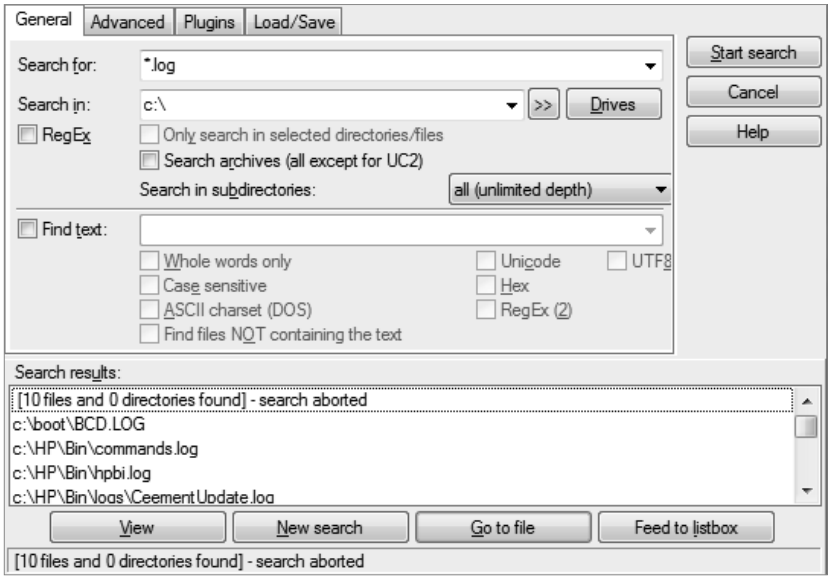
Jeden ze způsobů, jak najít požadovaný log soubor (nebo úložiště log souborů), je například s pomocí souborového manažeru Total Commander, který je dostupný na webových stránkách:

Web: `www.ghisler.com`

Po instalaci aplikace je možné spustit funkci vyhledávání klávesovou zkratkou **ALT+F7**, přičemž do prvního pole je třeba zadat název vyhledávaného souboru. V tomto případě to bude výraz:

```
*.log
```

Uvedený výraz zabezpečí, že se budou vyhledávat všechny soubory (zástupný znak hvězdička) s příponou `log`.



Obrázek 3.2 TotalCMD vyhledávání

Očekávaný výsledek:

V případě práce se záznamovými soubory je očekávaným výsledkem získání informací o činnosti ve firemní síti nebo konkrétně na koncové stanici. Například v případě proxy serveru to může být seznam navštívených stránek, IP adresy koncových stanic, které uvedenou proxy používají.

Filtrování záznamů

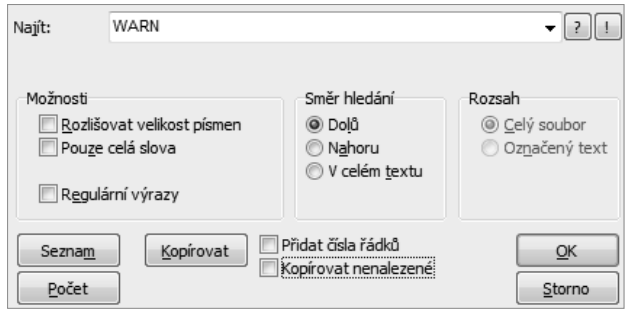
Při filtrování a vyhledávání chybových záznamů může být nápomocná aplikace PSPad od českého autora, která je dostupná na webových stránkách:

Web: `www.pspad.com`

Jedná se volně šiřitelný editor, který je určen pro práci v prostředí systému Windows. S pomocí této aplikace lze například z textového souboru s 30 000 řádků záznamů vyfiltrovat záznamy, kterým je přiřazena závažnost [`Warning`]. Jednou z velkých výhod této aplikace je, že umožňuje otevírat i poměrně velké textové a datové soubory, které ostatní textové editory nezvládají tak snadno.

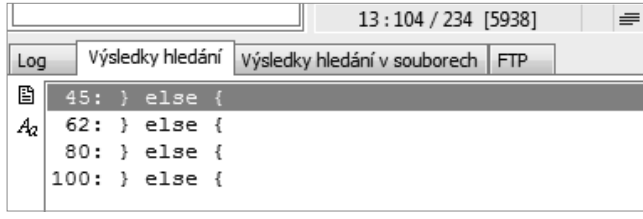
Postup filtrace řádků obsahujících označení [`Warning`] je následující:

1. Po otevření souboru v aplikaci PSPad je potřeba použít klávesovou zkratku **CTRL+F**, která otevře dialogové okno pro vyhledávání v souboru (viz obrázek 3.3).



Obrázek 3.3 PSPad vyhledávací dialog

2. Do vyhledávacího pole zadáte výraz, který má být vyfiltrován, a potom:
   - kliknete na tlačítko **Kopírovat,**
   - nebo spustíte akci prostřednictvím klávesové zkratky **ALT+K**,
   - případně kliknete na tlačítko **Seznam.**
3. Následně dojde k vyfiltrování všech řádků, které obsahují zadaný výraz. Akce provedené podle prvních dvou odrážek v předchozím bodě zobrazí výsledek na nové záložce. Akce provedená podle poslední odrážky předchozího bodu zobrazí seznam v dolní části pracovního okna. Dvojklikem na jednotlivé položky seznamu bude označen řádek, kde se výsledek nachází. Tato druhá volba umožňuje efektivnější orientaci a nalezení jednotlivých položek z vrácených výsledků v původnímu souboru.



Obrázek 3.4 PSPad – seznam výsledků

Tímto postupem je možné značně urychlit a zpřehlednit práci se soubory, které obsahují ohromné množství záznamů síťového provozu a akcí, jež se udály v síti.

Alternativou k aplikaci PSPad je Notepad++, který je dostupný na webových stránkách:

Web: `http://notepad-plus-plus.org`

Regulární výrazy

Aplikace PSPad a Notepad++ nabízejí také další možnosti pro filtrování výrazů, a to pomocí regulárních výrazů. Regulární výrazy jsou v podstatě masky pro textové řetězce. Využívají se při kontrolách dat zadávaných do formulářů, parsování (rozdělování, přípravě obsahu sou-

boru pro další zpracování) kódu nebo také při vyhledávání informací v textových souborech, které obsahují velké množství dat.

Následující tabulka 3.1 ukazuje několik základních metaznaků, které je možné využít při tvorbě regulárních výrazů.

Tabulka 3.1 Základní metaznaky regulárních výrazů a jejich význam

Metaznak	Význam znaku
`^`	začátek řetězce (textu, v němž se vyhledává)
`$`	konec řetězce (textu, v němž se vyhledává)
`?`	0 nebo 1 výskytů předcházejícího znaku
`.`	Zástupný symbol pro 1 libovolný znak
`+`	1 a více výskytů předcházejícího znaku
`*`	0 a více výskytů předcházejícího znaku
`( )`	Vyhledání skupiny znaků
`{n}`	Přesně n opakování předcházejícího znaku
`{n,}`	n a více opakování předcházejícího znaku
`{n,m}`	Nejméně n a nejvíce m opakování předcházejícího znaku
`\`	Následující znak není metaznak
`\d`	Vyhledání číslic v rozsahu 0–9
`\D`	Vyhledání jakéhokoliv znaku kromě číslic
`\w`	Vyhledání alfanumerických znaků [0–9A–Za–z].
`\W`	Všechno kromě alfanumerických znaků [0–9A–Za–z].
`A|B`	Výraz A, nebo výraz B

Vyhledávání pomocí regulárních výrazů se nijak výrazně neodlišuje o normálního vyhledávání, jak bylo představeno v předchozím textu. Jediným rozdílem je, že se mění význam některých znaků a posloupnosti znaků a pro aplikaci výrazu je potřeba zaškrtnout volbu „**regulární výrazy**“.

Následující výrazy prezentují příklad regulárních výrazů vytvořených z výše uvedených metaznaků.

Příklad 1:

```
Andr.id
```

Zadaný regulární výraz při vyhledávání vrátí všechny výsledky, které obsahují dané slovo, přičemž místo pátého znaku (tečka) může být jakýkoliv jiný znak, a to v počtu právě jeden. Vrácené výsledky by tudíž mohly být například: `Android, Andruid, Andreid, Andr8id` apod.