Pokročilé (vy)užívání googlu část 2

Vložil/a czokl [1], 19 Březen, 2006 - 23:04

- Hacking [2]
- Security [3]

Pokračování minisérie, dokončíme vyhledávání souborů, podíváme se na systémy a zařízení a nebude chybět ani pár slov o obraně.

1) Hledání podle názvu

Zde zase využíváme už dříve vysvětlené vychytávky, např.: "intitle:Index of /pass + password.txt --html --htm --php --asp" touto query lze nalézt několik souborů s hesly, jak sami vidíte nejde o nic nového. Při tomto hledání se dá dobře využít toho, že na rozdíl od multimediálních souborů zde víte přesný název souboru, například velmi oblíbený totalcmd(souborový manažer) ukládá přihlašovací údaje na ftp servery do souboru wcx_ftp.ini, sice šifrované, ale toto šifrování už bylo prolomeno a navíc i kdyby nebylo stačí tento soubor nahradit vaším vlastním a máte přístup na všechny ftp účty své oběti. Pokud používáte třeba p2p síť dc++ zkuste na nějakým hubu vyhledat tento soubor, páč najdou se i ucha co sdílejí celý disk, a pokud ne, zkuste najít nějaký ten soubor přes google, například přes query jako "inurl:wcx_ftp filetype:ini" se dají získat zajímavé výsledky. Toto byl samozřejmě jen příklad, spousta webových i jiných aplikací ukládá citlivé informace do obyčejných textových souborů, kolikrát i nešifrované nebo velmi slabě šifrované.

2) Hledání podle obsahu

Druhou a v tomto materiálu poprvé použitou metodou je hledání podle obsahu souboru. Podle mých osobních zkušeností právě tento druhý typ vrací velice přesné a užitečné výsledky. Jak na to? Úplně jednoduše, do query napíšeme jedinečná slova struktury daného textového souboru, případně doplníme nějakým inurl nebo filetype parametrem a dáme vyhledat. Například chceme nějaký ten Mysql dump, tak sestavíme query nějak takto:""mysql dump" inurl:admin filetype:sql"(poznámka: někdy mysql dumpy mívají koncovku tar.gz). Nebo můžeme vylepšit query z minulého odstavce takto: " "[connections]" + inurl:wcx_ftp filetype:ini" a pak dokonce oddělat i celý název souboru, protože i když je to nepravděpodobné, tak se stane že název souboru je malinko(nebo i malinko více) pozměněn. Nakonec v kreativitě se meze nekladou.

No myslím, že k hledání dat by to mohlo být všechno, záměrně neuvádím hromady queries, protože to si můžete najít jinde a taky zastávám tne názor, že kopírováním cizích myšlenek ničeho nedosáhnete(haha, docela staromódní že? :)).

-[Vyhledávání systémů]-

Nyní se vrhneme na neméně zajímavou kapitolu a to je vyhledávání systému. V googlu se dá najít neskutečný počet různých verzí různých systémů, bohužel se musíme omezit na http a web aplikace (případně programy s web rozhranním).

1) Vyhledávání http serverů

Podle čeho určit verzi, typ, popřípadě os http serveru? Najít vylistovaný adresář, způsobit chybu nebo najít výchozí stránku webserveru, protože všude tady byste měli banner daného serveru. Nejdříve zkusíme nalézt vylistované adresáře. Jako příklad budu uvádět vyhledávání serveru Apache,

ale nic Vám nebrání v tom hledat jiný server. Zkusíme třeba nalézt nějaké Apache servery ve verzi 1.3.31 na české doméně. Query by mohla vypadat nějak takto: "intitle:index.of "Apache/1.3.31 Server at" site:cz". Nebo bysme mohli zkusit najít defaultní stránky webových serverů a to například zadáním této "The SSL/TLS-aware Apache webserver was successfully installed on this website" věty do googlu. Při tomto hledání jde (opět) o to, nalézt ve v textu (titulku, banneru, ...) jedinečnou část a podle ní vyhledávat. A s chybami se to má podobně, každý web server má svoje základní chybové stránky(404,..) a podle jejich obsahu lze najít i daný webový server, protože google indexuje i toto. Myslím, že nejlepší pro hledání určitého web servru pomocí googlu je mít tento webový server nainstalovaná na lokálním disku a hledat odlišnosti a podle nich sestavovat queries. Teady alespoň mě se tato metoda osvědčila.

2) Vyhledávání webových aplikací

Zde využíváme skutečnosti, že naprostá většina tvůrců webových aplikací je na svůj výtvor patřičně hrdá a takže pokud si jejich webovou aplikaci nainstalujete zpravidla úplně dole naleznete informace kdože za tím vlastně stojí. A některé webové aplikace mají dokonce ve svých licencích "podmínky" nebo doporučení, že pro používání těchto systémů musíte/měli byste nechávat tyto informace viditelné na stránce, což nám samozřejmě usnadňuje práci. Jako ukázkový cíl můžeme zvolit aplikaci vBulletin(fórum). Nejdříve si zjistíme banner. Napíšeme tedy do googlu obyčejné "vbulletin", obvykle nám google vrátí domovskou stránku na prvním místě (pokud hledáte jentak náhodný cíl, tak jsou domovské stránky nejen dobrým zdrojem bannerů, ale také informací o poslední verzi a hlavně o chybách ve verzích předchozích a ruku na srdce, kolik z nás každý den kontroluje domovské stránky všech svých produktů aby si ověřil, že se neobjevila žádná chyba a stane-li se tak ihned upgraduje). Banner máme (z hlavního indexu domovské stránky jsme se ovšem museli prokliknout na comunity forum), takže můžeme vesele hledat. Ještě ale jedna maličkost. Protože by se nám na prvních x stránkách vraceli odkazy hlavně na domovskou stránku vbulletinu, odstraníme jeho adresu z výsledků, výsledná query může vypadat takto: "Powered by vBulletin Version 3.5.2 -inurl:vbulletin". Podobným způsobem se dá nalézt snad prakticky každá webová aplikace nebo i její specifická část, třeba administrátorská část phpnuke se dá najít takto:"Website engine code is copyright by PHP-Nuke -inurl:phpnuke Administration System Login inurl:admin.php". A tak bysme mohli pokračovat dál a dál. Samozřejmě, toto samo o sobě moc užitečné není, ale myslím, že každého z Vás nyní napadá, jak se takto získané informace dají využít.

Ještě je tu druhý způsob vyhledávání a to podle url. Základní myšlenka je taková, že každý autor si pojmenování jednotlivých webových stránek, syntaxi zadávání parametrů apod. vymýšlí sám, protože neexistuje a ani nemůže existovat nějaký obecný formát. Toto vyhledávání se hodí hlavně v případě, že chcete prověřit bezpečnost nějakého určitého modulu web aplikace a tento modul není defautně s aplikací dodáván nebo zapnut. Asi nejvíce efektivní a nejpřesnější hledání lze zařídit kombinácí těchto dvou metod.

3) obecné zjišťování

Nakonec si ukážeme, že se dá zjistit pomocí googlu o systému strašně moc věcí. I když zde není google úplně dominantní, ale jeho pomoc nám výrazně usnadní práci. K prvnímu triku potřebujeme aby na serveru běželo php a aby správce nechal někde na viditelném místě na serveru soubor s funkcí phpinfo(). Tato funkce totiž popisuje jednak nastavení jazyka php (což nás zase tak moc nezajímá) a také docela detailní popis systému, na kterém běží (a to už nás zajímá hodně). Query může pak vypadat nějako takto: "phpinfo filetype:php site:cz". Druhý trik spočívá v zneužití monitorovacího systému big brother (ano přesně jak ta reality show). Vtip je v tom, že bb generuje vlastní webové rozhranní, které je velice často přístupné z vnější sítě (internet) a i když je možné tento systém zaheslovat, velká část jeho uživatelů tak nedělá. Pro nalezení aktivních serverů s bb stačí zadat: " intitle:green:Big Brother " a máte před sebou hromadu kompletních sítí, o kterých se můžete pomocí big brotheru dozvědět opravdu mnoho. Další podobnou web aplikací je phpsysinfo, která taktéž získává se systému všemožné informace a z těch potom generuje web. Ve verzí 2.3 jí lze najít například: "Created by phpSysInfo-2.3". Poslední věcí, o které se zmíním je využití souborů robots.txt. V robots.txt mohou webový roboti(spideři), kteří prohledávají webové stránky ukládájí jejich obsah do své databáze, seznam adresářů, do jejichž adresářů se nemají pouštět. Tento systém je založen na důvěře, protože robot může klidně tento soubor ignorovat a i když to googlebot nedělá,

soubory robots.txt už do své db nahrává. A jelikož jsou někteří administrátoři moc moc neopatrní a dají do robots.txt nějaký "důležitý" adresář, kteří navíc nijak nezaheslují a ještě povolí výpis obsahu, můžete s trochou štěstí (nebo pomocí silné neomezené linky a krátkého skriptu) nalézt zajímavé informace. Minimálně zjistíte, které adresáře se na daném ftp mohou vyskytovat, což se někdy docela hodí.

-[Vyhledávání zařízení]-

Třetí, asi nejméně užitečnou a zároveň nejvíce zarážející skupinou je vyhledávání zařízení. Najdeme zde různé tiskárny, webkamery nebo dokonce i routery. Aby se dalo zařízení nelézt musí se splnit několik podmínek: zařízení musí mít webovou administraci, administrace nesmí být zaheslovaná a musí být přístupná z vnější sítě. Navíc, tato informace se musí do google nějako dostat, to mě na celé věci nejvíce zaráží, v tomto případě se jendá vyloženě o velkou neopatrnost a nepozornost majitelů (správců) těchto zařízení. Princip je stejný jako v ostatních typech hledání, protože se jedná o zařízení, ve většině queries by se mohlo objevit něco jako "device status". Například : "intitle:device status "LAN MAC" -manual -guide -support" by mohlo najít nějaký ten router. Ovšem pozor, ne všechny Vámi nalezené stránky budou ostré verze, velká část z nich budou akorát ukazkové demoverze a jiné budou pro změnu jakéhokoli nastavení vyžadovat heslo. Takové tiskárny dají najít dle mého názoru mnohem snáze, protože jich bez ochrany existuje více a je i větší pravděpodobnost úniku informací o tiskárně. Query můžeme sestavit třeba takhle: "intitle:status "Print Server Status" device". Myslím si, že by to na ukázku mohlo stačit.

-[Obrana]-

Teď když víte vše potřebné o tom, jak pomocí google útočit, ještě zbývá pár slov o tom, jak se poti těmto útokům bránit. Myslím si, že většinu z Vás jistě napadají postupy, jak tyto metody eliminovat, protože nejde ve své podstatě o nic jiného než o nepozornost nebo přílišnou neopatrnost. Shrňmě si to tedy do několika bodů:
- dodržujte základní bezpečnostní pravidlo: defaultně všechno zakázat a povolit jen to nezbytně nutné (ať už se to týká výpisů adresářů, přístupu k "citlivým" nezaheslovaným adresářům, přístup k zařízením s web administrací apod., doporučuji tyto věci zakazovat přímo http serverem)
- mějte ve svém webovém prostoru pořádek(to znamená neskladovat na webu nepotřebné věci, vylistovat opravdu jen 100% nutné a nedůležité adresáře, ...)
- mařit práci robotům (souborem robots.txt, pomocí javascriptů a jiných interaktivních mechanismů), zde bych také rád upozornil na http://www.google.com/webmasters/remove.html [4], kde samotný google radí, jak na to.
- nezobrazování bannerů, pokud útočník neví přesnou verzi vašeho systému tak ve většině případů zkusí štěstí jinde,tam , kde zobrazené bannery mají (autor článku si rozhodně neělá iluze, že by všichni lidé prezentující na internetu začali myslet na bezpečnost).
- nenabízet veřejně přes http a ftp chráněné soubory mp3, avi apod. Nejenže je to trestné, ale nikdy nevíte, kdo si ten Váš warez server přes google najde a bude Vaší "dobrotivosti" zneužívat.
- myslet hlavou a být opatrný při práci s citlivými daty.

-[Ukázkové queries]-

Následující queries jsem vymýšlel sám (snad teda, vybírám je z paměti svého prohlížeče), takže mají k dokonalosti daleko, ale můžete si udělat představu:

data :`index of backup`
```
mysql dump inurl:sql.gz
index of /mp3 name last modified size
inurl:ftp mp3 -www "parent directory"
--www hudebni_skupina size "Last modified" mp3
inurl:ftp mp3 -www "parent directory"
"[connections]" + inurl:wcx_ftp filetype:ini
intitle:Index of /pass + password.txt --html --htm --php --asp
```

```
systémy:phpinfo filetype:php site:cz
"Created by phpSysInfo-2.3"
index.of Apache/1.3.31 Server at
"Microsoft IIS server at" "dir" "parent directory"


zařízení :query: intitle:status "Print Server Status" device
inurl:status device status "print"
intitle:device status "LAN MAC"
```

-[Závěr]-

Tak a to je všechno. Ještě bych se měl zmínit o legálnosti celé věci, samotné vyhledávání je samozřejmě legální, další činnosti už být nemusejí, ale s tím už nemá google co dělat. Navíc i kdyby nebylo, tak samotný google nemá při jeho zatížení šanci sledovat svoje uživatele a i když informace o hledání logují ze statistických důvodů, je velmi pravděpodobné, že se do cizích rukou nedostanou. Viz nedávný případ, kdy americká vláda chtěla určité informace od třech největších vyhledávačů (google, yahoo, msn), ale google jim, na rozdíl od zbytku, nic neposkytl. Na úplný závěr bych Vám chtěl popřát hodně trpělivosti a štěstí při sestavování queries, minimálně ze začátku budete obojí potřebovat :)

-[Reference]-

Původně sem chtěl vycházet z různých anglických textů od různých autorů, kteří se již touto témou zabývali a umístit odkazy na tyto dokumenty, ale protože jsem celou svojí práci pojal trošku jinak než oni, nevycházel jsem úbec z ničeho, pouze z myšlenek v mé hlavě. I přesto bych ale chtěl pro anglicky hovořící část čtenářů uvést několik zajímavých odkazů pro rozšíření obzoru:

[1] http://johnny.ihackstuff.com/index.php?module=prodreviews [5] - taková mekka všech google hackerů, databáze všemožných queries, na stránkách lze nalézt další informace o google hackingu, prezentace a research papery, všechno ve vysoké kvalitě.

[2] http://www.hackingspirits.com/eth-hac/papers/Demystifying%20Google%20Hac... [6] - zajímavý whitepaper, který zasvěcuje do tajů google hackingu

URL článku:
https://security-portal.cz/clanky/pokro%C4%8Dil%C3%A9-vyu%C5%BE%C3%ADv%C3%A1n%C3%AD-googlu-%C4%8D%C3%A1st-2

Odkazy:
[1] https://security-portal.cz/users/czokl
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/security
[4] http://www.google.com/webmasters/remove.html
[5] http://johnny.ihackstuff.com/index.php?module=prodreviews
[6] http://www.hackingspirits.com/eth-hac/papers/Demystifying%20Google%20Hacks.pdf

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn