INTERNETOVÁ BEZPEČNOSŤ PRE LAIKOV

Autor	Vydavateľ	Licencia	Vydanie	Autor obálky
Peter Štec	Greenie knižnica	CC-BY-NC-ND	Prvé (2021)	Peter Štec

O knihe

Táto knižka je určená skôr laikom, ktorí už majú aké-také znalosti o internetovej bezpečnosti, ale potrebujú niečo vysvetliť, prípadne objasniť. Nástrahy Internetu číhajú na nás vždy, keď sme online a niektoré podvody a podvrhy sa môžu tváriť celkom nevinne. Niektoré je vidieť na prvý pohľad, iné sú sofistikovanejšie a ťažšie vystopovateľné. Neoplatí sa podceniť vlastnú bezpečnosť na Internete, hrozí veľké množstvo druhov kyberzločinov, ktoré sa stále len veľmi obtiažne dokazujú a tak sa stále podvodníkom oplatia. Nikto však nechce prísť o peniaze a už vôbec nie o svoju identitu, či osobné informácie.

V tejto knihe sa však pozrieme i na zálohovanie dát a zistíme, čo môžeme riskovať so zobrazovaním nelegálneho alebo nechceného softvéru alebo multimédií a koho najviac chrániť pred nástrahami súčasného virtuálneho sveta.

Obsah

Kapitola I: Moja známa písala diplomovku na 3x… (Zálohovanie)

Nikto také čosi nechce zažiť a predsa len zažil. Nie je potreba si zálohovať všetko, len to, čo považujeme za nutné a nevyhnutné. Nie je predsa príhodné, keď sa vrátite zo školy a po troch kávach s energeťákom dostanete nápad niečo napísať do diplomovej práce. Mať jedinú kópiu na svojom USB disku (nevyrobenom v USA), po tom, čo ste ju ukázali svojmu školiteľovi na jeho počítači, nie je dobrý nápad. Vedeli ste, že asi týždeň pred tým vás kolegovia z vašej triedy vystríhali, že po školskej sieti sa šíri vírus a vy tam nájdete len odkaz na ten samotný USB disk, ktorý ste práve strčili do portu počítača. Začudujete sa a chcete otvoriť ten odkaz. Ako to, že sa nedá otvoriť?

A panika začne. USB zálohy samy o sebe nestačia. Miniaturizácia pamäťových diskov spôsobila, že keď stratíte USB disk, nájdete ho o tri roky, keď ho už nepotrebujete, tak malý dokáže byť (aspoň čo sa týka fyzickej veľkosti). Môžete takisto využiť i služby internetových providerov ako Dropbox, Google Drive alebo MEGA. Ale pozor, odporúčame dôkladne prečítať si to, čo nečíta nikto: podmienky služby. Nezávislí provideri ako napr. MEGA ponúkajú veľa skvelých možností, ale ak váš cloud nepoužívate, provider ho môže po dlhšej aktivite deaktivovať, prípadne zmazať vaše dáta. A práva sa nedočkáte, pretože si neprečítate, že ste s tým súhlasili pri zriadení služby!

Zálohovanie dát je veľmi dôležitou súčasťou vašej obrany voči nepredvídateľným okolnostiam. Proti vírusom, proti poškodeniu hardvéru, softvéru a tiež proti nám samotným. Radi strácame USBčká, formátujeme SD karty, pričom zabudneme, že na nich máme tisíc fotiek z dovolenky v Tunisku, omylom potopíme notebook v súkromnom bazéne (alebo v chudobnejšej verzii – vo vani).

Existuje veľmi jednoduché pravidlo. **Lepšie zálohovať dáta na viac nosičov** (cloud, USB, SD karta) a stratiť s tým pár sekúnd života, **ako stráviť celé mesiace vytváraním toho istého od začiatku** alebo z veľmi starej zálohy. Existuje množstvo spôsobov, ako neprísť o dáta a niekedy stačí niečo úplne jednoduché, aby ste neboli v problémoch. Skôr, ako sa dnešná mládež stretla s Internetom, si staršia generácia posielala najdôležitejšie informácie mailom, pokojne aj samým sebe. Otvoriť totiž svoju mailovú schránku a v nej odoslanú poštu je rýchle a jednoduché a dá sa to dnes už na akomkoľvek zariadení. Neraz bola diplomovka zachránená tak, že sa v podstate hotová, len s chýbajúcimi zmenami v detailoch, poslala niektorej korektorke, ktorá si na to síce nenašla čas – ale mailovej adrese je to úplne jedno. **Urobiť si pokojne aj tisíc záloh dôležitého dokumentu nezaberie viac miesta na disku ako jediný diel obľúbeného seriálu**, tak prečo to nespraviť? Zároveň sa neraz zachránili dáta z notebooku, ktorý sa nedal spustiť. Pomôže pritom Linuxové LiveCD/LiveUSB, pripojenie disku do iného zariadenia či pravidelná záloha na Internet, ktorú niekto nastavil pred rokmi a stále funguje, ak používateľ dodržiaval základné pravidlá.

Kapitola II: Veľké písmená? Malé písmená? Čísla? To načo? (Heslá)

Pravdepodobne ste sa stretli s frázami „tých mladých by mal niekto otrieskať slovník o hlavu“ a „ja mám všade rovnaké heslo a mám tam meno dcéry, to aspoň nezabudnem“. Čuduj sa svete, tieto dve frázy súvisia oveľa viac, ako to vyzerá na prvý pohľad.

Dostať sa cez heslo nie je nikdy také, ako v známej scéne z českého seriálu Comeback (myslela som, že vieš, že Lexa sa píše s X!) alebo v rôznych amerických filmoch, kde ho hacker uhádne či prelomí za pol minúty, ani si poriadne nesadne k počítaču. Alebo áno? Na Slovensku bolo známe heslo nbusr123. Áno, bolo to reálne heslo pre Národný bezpečnostný úrad SR. Bezpečnosť na prvom mieste, či nie? Každopádne, zlých hesiel je naozaj veľmi veľa. Napríklad heslo 123456, password či totoniktoneuhadne sa dajú prekonať ľahko. Tak, ako meno dcérky, psíka či presná adresa aj s popisným číslom. Dobrý spôsob, ako napísať zlé heslo, je aj používanie úplne bežných slov. Keby mali stránky pivovaru heslo pivo, ako veľmi by to bolo bezpečné?

Ako vytvoriť dobré heslo? Prvým krokom je vedieť, ako útočník premýšľa. Povedzme, že sa chce dostať do mailov či Facebookovej stránky svojej bývalej, ktorá ho podvádzala s celou futbalovou reprezentáciou. Pravdepodobne by išiel podľa týchto krokov:

1. Rovnaké heslá ako inde. Ak vedel niektoré heslo z iného účtu, vyskúša ho aj tu. Ak má tá žena rovnaké heslo všade, môže si ho jednoducho zistiť a prečíta si čokoľvek. A je len na ňom, či ho okamžite zmení, alebo nie.
2. Databáza najčastejších hesiel. 123456 a podobné kombinácie, prípadne qwertz alebo qwerty, podľa klávesnice. Známych a častých hesiel je veľa.
3. Samozrejme názvy obcí a ulíc, kde sa daný človek nachádzal, nemôže chýbať. Ak ste napríklad každý deň v Nitre, tak by vaše heslo nemalo byť Nitra123 ani nič podobné.
4. Slovníkový útok! Všetko čo je v slovníku zaradom. Ak vie maximálnu a minimálnu dĺžku, vie si slovníkový útok prispôsobiť. Dovolenka, milenka, futbal… čokoľvek, čo je v slovníku.
5. Pomalé softvérové prelamovanie. Všetko, čo sa dá a inde sa nedostalo.

V praxi sa dá povedať, že **čo sa neprelomí do nejakého času, to sa neprelomí vôbec, jednoducho to útočníka prestane baviť**. Je teda dôležité mu túto prácu čo najviac skomplikovať, a to najlepšie dlhým, komplikovaným heslom, ktoré nie je v žiadnom slovníku. Dobré heslo môže byť napríklad Q11uTlwirTmt8u, ale… kto by si také pamätal? Tu je pár jednoduchých príkladov:

Chorvátsko 2018 letná dovolenka s Luckou a Jožkom => LuJoChor2018Let

Dcéra Iveta má rada ruže => ive456ruze789tka

Jano kúpil ukulele za 1000€ =1000_jnkplkll_1000

Ak neviete vymyslieť heslo ani za svet, pokojne vyskúšajte niektorý generátor a upravte si ho tak, aby sa vám lepšie pamätal, no dbajte na to, aby bolo heslo dosť silné podľa generátora.

Kapitola III: Prečo mi nejde crackovať hry? (Multimédiá)

Od 90. rokov a začiatku storočia sa pár vecí zmenilo. Hry a podobné softvéry podivne podobného žánru už nie je potrebné crackovať, čiže oblbnúť protipirátsku ochranu. Jednak je to zakázané (ale kto ma pri tom vidí, že?) a na druhú stranu je to trošku nemorálne. Ak dvesto vývojárov pracovalo na hre tri roky a my im nezaplatíme, tak je vôbec dôvod robiť nové hry? Alebo udržiavať ich nažive cez pridávanie nového obsahu a vychytávanie chýb? A s príchodom streamovania a internetu je crackovanie o dosť náročnejšie a v podstate nepotrebné. Ak si cez webovú platformu kúpite nejakú hru, ktorá sa vám nepáči, nie je nič jednoduchšie, ako si vyžiadať vrátenie peňazí. Veľa ľudí totiž namietalo, že crackujú hry len preto, aby si ju len skúsili a keď sa im zapáči, tak si ju kúpia? Tak presne ten dôvod im odpadol.

Čo to ale je ten crack? Trochu si o tom povieme viac, urobme si malé okienko do histórie. Kedysi bolo bežné, že ste museli pri hraní hry mať vložené CD. Je to jednoduchá protipirátska ochrana. Samozrejme tí, ktorí nemali CD mechaniku, alebo im nefungovala správne, alebo jednoducho nevedeli nájsť CD, mali smolu. Vytvoril sa tak jednoduchý program, ktorý odstránil nutnosť mať vložené CD. Jednoduchý program, tzv. crack. Tých je viac druhov a často je to súbor, ktorým sa nahradí iný, nesprávne nainštalovaný súbor. Všetky súbory sú v poriadku, až na jeden. A ten stačí nahradiť dopredu pripraveným crackom. Problémov je s tým hneď niekoľko, okrem iného i to, že crack môže mať nielen to, čo chcete, ale veľmi často má pribalené aj niečo, o čom neviete nič. Môžete sa tak stretnúť s trójskym koňom alebo inou hrozbou.

Jožko napríklad vytvorí hru a dá do nej mechanizmus, ktorý bojuje proti piráteniu. Ferko urobí crack, aby si to mohol nelegálne zahrať ktokoľvek. Anička upraví Ferkov crack tak, aby jej umožnil vybieliť vaše bankové konto. Jednoduché, no nie? Antivírusy často vymazávajú cracky, a to práve preto, že sa tam nachádza bezpečnostná hrozba. Ak si máte vybrať medzi crackom aj s

hrozbou a medzi legálnou hrou, zistite si, koľko tá hra stojí a zvážte, či chcete autorov tej hry podporiť, alebo potopiť.

Zaujímavým príkladom ochrany pred kopírovaním mala najnovšia hra zo série Prince of Persia. Na nelegálnej (a niekedy i legálnej) verzii hry sa asi v tretine nedali otvoriť jedny dvere. Výsledok? Množstvo najrôznejších crackov, ktoré síce nepomôžu, ale majú pre vás nepríjemný obsah navyše. Taktiež sa ukázala vlna kritiky, ktorá označila hru za málo kvalitnú a plnú chýb. Hráč následne prestal mať chuť na kúpu tejto hry, pretože je jednoducho sklamaný.

Ľudia sa snažia brániť proti nelegálnemu obsahu rôzne. Napríklad v jednej počítačovej hre sa s tým popasovali svojsky. Cracknutá hra fungovala celkom normálne, iba vaša postava mala celý čas pásku cez oko, ktorú ste jej nemohli dať dole. Inde vám dali zbraň, ktorá strieľa kuratá a nespôsobujú žiadne poškodenie súperovi. Už dávno boli prekonané „kódové mriežky“, teda akoby kontrolné otázky. Ak ste si napríklad v roku 1991 kúpili hru na nejaký starý Commodore, tak sa hra opýtala napríklad: Aký znak je v riadku 5 a stĺpci 10? Ak ste si totiž hru poctivo kúpili, dostali ste i vytlačenú stranu s kódmi. Stlačili ste napríklad „p“ a hra sa spustila. Inak ste si totiž nezahrali.

S filmami je situácia horšia. Ľudia sťahujú horentné množstvá audiovizuálnej zábavy, napriek streamovacím službám, ktoré sa môžu rovnať virtuálnym knižniciam zábavy. To je práve spoločným menovateľom všetkého audiovizuálneho v dnešnej dobe. Niekomu k prospechu, iným nie. Veľa hudobníkov sa takto napríklad sťažuje, že len čo bežný poslucháč dostal príležitosť na jediné kliknutie dostať sa k databázam miliónov a miliónov skladieb, tak oni majú problém získavať nové a nové publikum. A keď stiahnete film, ktorý nejde ani za toho boha prehrať, tak buď ste sa nachytali nejakým šikovníkom, alebo ste stiahli po verzii, ktorú na lokálnych prehrávačoch nekúpite. Alebo vidíte príšerný obraz z kina, ktorý je každých 10 minút prerušovaný reklamou na stávkovú spoločnosť.

Vydavatelia filmov na DVDčkách boli nútení kódovať svoj obsah iba pre určitú časť sveta. Dokonca existoval zvláštny formát dátových diskových nosičov, ktorý sa mal po jedinom prezretí znefunkčniť. Mal to byť formát pre požičovne filmov, ale nepresadil sa. Ľudia sa však vždy vynájdu a napriek tomu si dávajú pásku cez oko, pretože vediac, že ešte nikoho za pirátske sťahovanie obsahu nevzali do Ilavy, si takto môžu užívať hodiny a hodiny zábavy zadarmo, miesto toho, aby svoj čas strávili nejak produktívne.

Do kategórie multimédiá už dávno patria i aplikácie na mobily a tablety. Často však nútia používateľa zapnúť internetové pripojenie, aby vôbec fungovali. Potom máte v rukách monštrum. O tom by mohla však byť nová knižka, ako s nami kvalitne vývojári appiek manipulujú. Kto by chcel aplikáciu, ktorá vás každú chvíľu pripája na Internet, aby vám pustila reklamu (samozrejme so zvukom na plné pecky) a vy mohli ďalej hrať? Nie je to ako televízia, len horšie?

Horšie na tom je vedomosť, že my to akceptujeme. A akceptujeme i ten fakt, že si kúpime pokoj – veď len za štyri doláre päťdesiat a reklám, škvŕn a špiny sa zbavíš! Akceptujeme i ten fakt, že toto monštrum dáme do ruky našim neplnoletým deťom, ktoré môžu na tomto „rodičovstve 21.storočia“ kvalitne doplatiť. **Práve deti sú tou najzraniteľnejšou skupinou online, a tak ich musíme viesť k čo najrozumnejšiemu používaniu Internetu!** Deti tak často dostávajú kvalitnú dávku hnusných reklám, návykových hier s pastelovými farbami a sociálnych sietí, dokonale ničiace ich detstvo a možno i ich budúcnosť, za ktorú sa budú o desať rokov hanbiť. Je však takmer nemožné dnes deťom čokoľvek zakázať, ale o tom, čo na deti dneška prostredníctvom modernej doby číha, je možné urobiť ďalšiu knižku.

K deťom jedna zaujímavosť dnešnej doby. Dieťa, ktoré má menej ako desať rokov, si vie vyhľadať a pozrieť rozprávku, pričom povypína vyskakujúce okná so sexuálnym obsahom a najrôznejšími kasínami, zatiaľ čo nejeden dospelý klikne na veci, na ktoré by nemal – a následne prosí svoje dieťa, aby skúsilo odstrániť škodu, čo on napáchal pár kliknutiami. A nie vždy sa to dá…

Kapitola IV: Tieto správy sú tak skvelé, až nie sú pravdivé (Hoaxy)

Čo je na tomto obrázku podozrivé ako prvé? Hlavne to, označené žltým zvýrazňovačom a čiernou šípkou. A prečo? Pretože táto stránka chce vyzerať ako oficiálna stránka Nového Času, až na to, že v adresnom riadku je readreadnews.com, ktorá je vymyslená.

Ak by sme sa po tejto stránke skúsili prejsť myšou a prezreli si, kde nás to chce presmerovať, zistíme, že každý jeden element – obrázok alebo preklik na ľubovoľnú sekciu, nás nasmerujú na jedinú adresu, odkiaľ od nás bude chcieť, aby sme naleteli trebárs na nejakú pyramídovú hru s vidinou rýchleho zárobku.

Možno si niekto všimne aj nevyskloňované meno v nadpise. Podvodníci sa často snažia preložiť svoje stránky do všemožných jazykov a pritom často používajú strojový preklad, ktorý ešte do dokonalosti musí dospieť. Je však pravdou, že v poslednom čase je takýchto stránok s lámanou slovenčinou už nižší, ako pred pár rokmi, a tak sofistikovanosť týchto podvodov len rastie.

Môžeme len odporúčať stránku hoax.sk, ktorá sa stala v podstate úplným základom pre širšie informácie o hoaxoch na Slovensku. Dozviete sa z nej nielen to, aké nepravdivé informácie alebo hoaxy teraz frčia a tiež i ako fungujú. Sú tam skvelé informácie i o Ponziho schéme, ktorá je určitým typom pyramídovej hry a tiež ako funguje. My môžeme len konštatovať, že **čokoľvek, čo vyzerá veľmi nerealisticky skvele na Internete, je takmer vždy podvod!**

Ak sa trochu zaujímate o takéto úžasné informácie, určite ste sa stretli aj s rovnakými článkami, kde je ale spomenutý iný človek. Je najľahšie hodiť tam niekoho veľmi známeho a je jedno koho. Hlavne, aby bol známy a kontroverzný. A hlavne, ak niečo vyľakalo odborníkov, tak to pravdepodobne je úplný nezmysel, ktorý vie ktorýkoľvek odborník ľahko vyvrátiť.

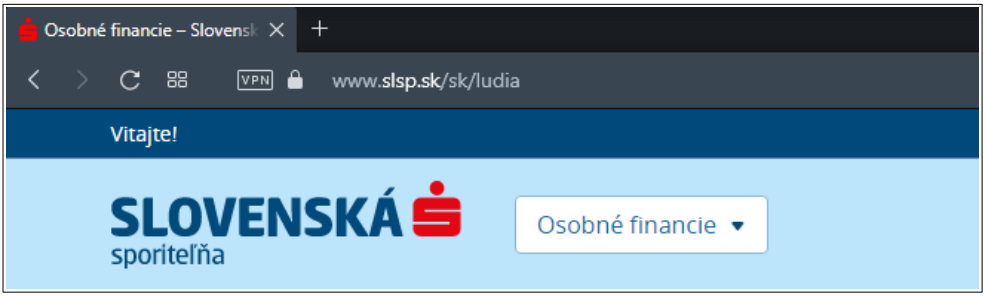
Kapitola V: Aký význam má jedno S? (HTTP a HTTPS komunikácia)

HTTPS (Hypertext Transfer Protocol Secure) je protokol, umožňujúci zabezpečenú komunikáciu v počítačovej sieti. Využíva protokol HTTP spolu s SSL a TLS (to je už zastaraný protokol). Zaisťuje autentifikáciu, dôveryhodnosť prenášaných dát a ich integritu. Všeobecne sa odporučuje používať HTTPS miesto HTTP.

Trend je taký, že všetky nové web servery už používajú HTTPS protokol prednostne. Umožnil to vývoj technológií a hlavne zistenie, že tajné služby často dokázali zachytávať nešifrovaný webový priestor. Komunikácia v HTTP je po ceste komukoľvek zachytiteľná, čitateľná a zmeniteľná, čím môže byť prenos dát pozmenený v okamihu, keď sa používateľ pripája napr. do internetového bankovníctva. Útočník môže získať prihlasovacie údaje a keksíky (cookies) a môže sa za používateľa vydávať (a vybieliť mu bankové konto). Preto sa využíva v emailovej komunikácii, online bankovníctve a všade tam, kde sa prenášajú osobné alebo citlivé informácie. Pre útočníka nie je problém vyskúšať vaše prihlasovanie aj na iných stránkach, ktoré navštevujete. Aj preto je dobré mať odlišné heslá.

V tomto prípade ide o stránku, ktorú sama spravuje a riadi malá skupina nadšencov do strategických hier. Stránka je dostupná i po zadaní HTTPS a

má platný certifikát. Je tu len na ukážku, ako vyzerá adresný riadok po vyhľadaní stránky s protokolom HTTP.



Použitie HTTPS sa indikuje v adresnom riadku, často i vizuálne (nejakou zámkou, kladkou alebo zelenou farbou).

Po kliknutí na kladku (visací zámok – veľmi zvláštne slovo) sa zobrazia informácie o certifikáte (možno ste niečo počuli o SSL certifikátoch – tak to je ono), vydanom pre danú doménu. Nie je potreba sa tak nejak zbytočne prehrabávať, pretože ak by certifikát vypršal alebo bol znehodnotený, prehliadač by nás na to upozornil, pretože tento SSL certifikát je dôležitý pri overení identity webu. Celá táto mašinéria je vybavená systémom pre vydávanie overených certifikátov, obmedzením ich časovej platnosti a podobne. Ani to však nie je na 100% blbuvzdorné a pre obyčajného používateľa je to často mätúce, no môže to dosť pomôcť pri odhalení phishingu a podobných útokoch.

Ak niekoho zaujíma pozadie: Na stránke je umiestnený skript, ktorý inak nie je viditeľný. Ak ideme na nejakú URL, tak je tam token, ktorý si web server kontroluje s CA (Certifikačná autorita). To je konkrétny server, ktorý spravuje certifikačná spoločnosť, pričom jedna spoločnosť môže mať i viac serverov. Ak sa tokeny nezhodujú, certifikát sa zneplatní. Ak teda chceme vydať certifikát pre stránku napr. https://blukote.sk, tak sa najprv rozhodneme, od koho chceme využívať túto službu (napr. DigiCert). Potom si vygenerujeme CSR (Certificate Sending Request) - určíme si, čo od neho vyžadujeme – autentifikáciu voči serveru, typ enkrypcie a metaúdaje (adresa, kontaktné osoby a pod.). Pošleme hotové CSR, DigiCert potom komunikuje s kontaktnou osobou, uvedenou v meta informáciách.

Ak prejde validácia, oni zoberú informácie z CSR a podpíšu ho verejným kľúčom a výsledkom je certifikát, kde je uvedené, pre koho je vydaný, sú tam metaúdaje z CSR, kým bol vydaný (DigiCert) a je tam pridaný i certifikačný chain – teda i metainfo o certifikáte Root CA, ktorá autorizovala Issuing CA (vo Windowse sa dá pozrieť, keď klikneme na ten zámok a dáme si zobraziť certifikáty a vyberieme Cesta k certifikátu).

V hotovom certifikáte ešte budú uvedené i vlastnosti samotného certifikátu – platnosť (validity – not before, not after) – a miesto, kde je CRL. CRL vydáva certifikačná autorita, je to verejne dostupný zoznam revokovaných certifikátov – Certificate Revocation List - (teda neplatných certifikátov pred dátumom skončenia platnosti). Revokácia (zneplatnenie certifikátu) môže nastať napríklad vtedy, keď ho niekto ukradne, alebo sa nájde iný dôvod, prečo by mal byť certifikát zrušený. Revokácia prebieha tak, že certifikačná autorita zaradí fingerprint (odtlačok, jeho jednoznačný identifikátor) certifikátu na CRL zoznam. Každý, kto overuje certifikáty, má možnosť overiť si CDP (CRL Distribution Point - je to internetová adresa, kde je CRL uvedená) a tak sa tento revoknutý certifikát neuzná.

Tedav krátkosti, ak pristupujeme prehliadačom na web server, ten sa nám predstaví certifikátom, napriek tomu, že mu prehliadač dôveruje, pred naviazaním spojenia sa ešte skontroluje CDP, či nie je náhodou zneplatnený. Ak je, tak prehliadač odmietne vytvoriť spojenie. V prípade, že je CDP nedostupné, tak sa to buď predvolene pustí, alebo sa zahodí.

Kapitola VI: Cukríky alebo ochranný mechanizmus? (Proxy)

Proxy (nie Doxy) je nástroj na kontrolovanie trafiky a skrývanie identity množstva používateľov, ktorí sa skryjú pod jedinú IP adresu. Často je jej súčasťou nejaká antivírusová zložka, kontrolujúca i dynamický obsah stránok. Proxy tiež dekryptuje HTTPS komunikáciu prostredníctvom SSL Interception. Tá sa môže vypínať, keďže podľa zákonov sa v určitých typoch inštitúcií nemá robiť kontrola šifrovanej trafiky. Ide predovšetkým o banky a finančné inštitúcie, keďže šifrovaná komunikácia musí byť podpísaná certifikačnou autoritou a vypína sa preto, aby neunikli citlivé alebo osobné údaje.

Proxy sa dá ešte použiť na okašľanie geolokácie, keď nás kvôli priradenej IP z rozsahu pre krajiny niekam nepustí. Proxy môže byť transparentná – trafika prechádza cez proxy, no nikto v sieti o nej nevie a ani ju nemá nastavenú v prehliadači. Tá sa môže napojiť ako fyzický stroj, alebo ako virtuálna mašina. Najčastejším typom je však explicitná proxy – všetci o nej v sieti vedia a je u nich nastavená.

Trafika prebieha od koncového požívateľa na proxy a odtiaľ už nová trafika s IP adresou proxy na web server, pričom proxy zisťuje, či je používateľ autentifikovaný, ak je pripojený i antivírusovému softvéru, tak ju rovno i skontroluje. Proxy sa dá predstaviť ako Black a Whitelisty pre dátové typy. Proxy sa díva len na frame – vidí proste len napríklad ZIP, nemôže sa už dívať do dokumentov. Až antivírový softvér sa podíva do súborov a je schopný zachytávať zakázané dátové typy.

Vykonáva i SSL Interception. Pri ňom je zrušené zabezpečené SSL spojenie (resp. je rozpojené), aby sa proxy dostala k nezabezpečeným údajom a tie mohla poslať na antivírus (AV). Aby sa nestalo, žeby sa zabezpečené informácie dostali na AV ako text, často proxy využívajú vlastné protokoly. Pokiaľ web stránka má certifikát podpísaný napr. spoločnosťou VeriSign, pre-

hliadač bude tomuto spojeniu dôverovať. Certifikát, ktorý je self-signed (podpísaným samým sebou) je primárne nedôveryhodný prehliadačom.

SSL Interception funguje nasledovne: Prehliadač kontaktuje proxy server a získa informácie o obsahu web stránky. Proxy vytvorí zabezpečenú HTTPS komunikáciu s web stránkou. Web server dodá ešte SSL certifikát, ktorý bol vydaný pre danú web stránku. Ak proxy spozná Root (hlavný) certifikát, označí ho ako dôveryhodný. Ak však neverí serverovému certifikátu, nemôže vytvoriť HTTPS komunikáciu a používateľ dostane chybovú hlášku, že je serverový certifikát nedôveryhodný. Ak je však potrebné, aby proxy dôverovala tomuto certifikátu, musí byť manuálne pridaná na proxy. Ak je už certifikát nainštalovaný ako dôveryhodný a proxy mu dôveruje, vytvorí nový certifikát s rovnakým obsahom, keďže certifikát nebol vydaný a podpísaným dôveryhodným CA, ale samotnou proxy. Nakoniec tento certifikát je samopodpísaný a pošle ho prehliadaču. Proxy však nie je dôveryhodná CA, preto by sa používateľovi mala tiež zobraziť chybová hláška. Aby sa tomuto problému predišlo, vykoná sa SSL Interception. Tak prehliadač dôveruje i proxine.

Často sa využíva vo firmách a korporáciách. Zamestnanci napríklad vďaka nej nie sú sledovateľní pomocou IP adresy.

Kapitola VII: Attacke! (Typy útokov)

DoS alebo DDoS útoky – (Denial of Service alebo Distributed Denial of Service) – tento typ útoku je pomerne častý vo väčších korporáciách a jeho cieľom je znemožniť prístup na web stránku, prípadne inú službu zahltením internetovej linky. Web stránka sa bude zvonku javiť ako nedostupná. Pri DDoS útoku sa používajú často viaceré počítače z rôznych IP adries.

Útočník väčšinou akýmkoľvek spôsobom zahtlí linku záplavou žiadostí, napríklad klasickým PINGom (ICMP floods). Útočník teda toľko ráz a tak často kontaktuje danú službu, až ju vyťaží. A to tak, akoby z jednej haly plnej ľudí vypustíte naraz všetkých a tí sa ponáhľajú, prechádzajúc jedinými maličkými dvermi. Skúste im ísť oproti. Tento typ útoku môže zasiahnuť web stránky i emailové schránky. Niekto totiž môže zahltiť mailovú schránku opakujúcimi sa mailami až natoľko, že sa nebudeme môcť vôbec do nej dostať.

Čo sa týka emailov, môžeme sa stretnúť i s tzv. Outbreak Attackom. Je to taký útok, pri ktorom sa útočí na Address book (Zoznam adries) a posiela zavírenú správu všetkým v zozname. Phishing Attack na druhej strane nemá prílohy, ale nejakú zavírenú adresu a snaží sa nachytať ľahkomyseľných používateľov, že zdedili milióny po nigérijskom princovi.

Jedna z menej príjemných vecí, ktoré môžeme dostať kliknutím napríklad na exe súbor (i keď to dnes väčšina mailových riešení blokuje), je tzv. trójsky kôň, alebo skrátene trojan. Tie sú nebezpečné, síce sa nešíria ako vírusy, ale môžu otvoriť váš počítač pre útočníka a pravidelne môžu odosielať vaše údaje útočníkovi, alebo umožní nahrať skutočne nebezpečný kód do počítača. Dobrým príkladom je tzv. keylogger, ktorý môže odoslať útočníkovi napríklad vaše meno a heslo napísané na počítačovej klávesnici. Pomocou umelej inteligencie je relatívne ľahké zistiť, ktorá časť vami zadaných znakov je skutočne meno a heslo. Preto je dobrý nápad neotvárať prílohy.

Škodlivý kód sa môže dostať do počítača taktiež cez reklamu. Chcete vypnúť otravnú reklamu, no pri jej vypínaní sa dostanete na stránku, ktorá vám začne niečo sťahovať do počítača a v horšom prípade tento kód aj spustí. Aj preto je dobrý nápad mať blokovač reklám v internetovom prehliadači.

Historicky sa stále zaznamenáva nárast útokov, pri ktorých je potreba sa ochrániť podľa hesla: „Mysli ako útočník“.

Typy sieťových útočníkov:

White hat - hľadá slabiny zabezpečenia systému. Jeho úmysel je však upozorniť providerov na chyby v zabezpečení siete. Dá sa tak povedať, že ide o človeka, ktorý hľadá chyby v nových projektoch a stará sa o to, aby boli zabezpečené.

Hacker - historicky sa ním označovali programátori – experti, dnes sú to skôr ľudia, ktorí sa snažia získať neautorizovaný prístup k sieťovým zdrojom a údajom (často i súkromným)

Black hat – človek, ktorý zneužíva svoje IT vedomosti k prielomu do siete neautorizovane. Cieľom je často osobný alebo finančný zisk.

Phreaker – je útočník, ktorý sa neautorizovane snaží dostať do telefónnej siete (napríklad za účelom volaní zadarmo)

Phisher - využíva maškarádu za niekoho za účelom získania citlivých informácii.

Kapitola VIII: A čo si mám z toho odniesť ja? (Zraniteľnosť siete)

Každá sieťová a počítačová technológia sama o sebe obsahuje určité bezpečnostné problémy. Veľkú úlohu pri bezpečnosti sietí zohráva ľudský faktor. Pri zlom zaobchádzaní alebo konfigurovaní i tej najbezpečnejšej technológie vzniká veľké riziko ohrozenia bezpečnosti (nezabezpečené účty, zlé a chybné konfigurácie a pod.)

Nielen aktívny hacking je problém, ale aj riešenie fyzickej bezpečnosti zariadení. Hrozby týkajúce sa hardvéru - fyzické poškodenie serverov, smerovačov (príliš teplo, zima, vlhkosť, prašnosť, napäťové špičky, prepätia, prepady, šum, rušenie, interferencie, strata napájania)

No a čo my s tým? Ako môžeme zmierňovať následky útokov?

- odstránením výrobných nastavení po inštalácií alebo umiestnení na sieti
- pravidelnou aktualizáciou antivírusu
- vlastnením osobného firewallu
- inštalovaním zariadení, zvyšujúcich úroveň zabezpečenia siete
- zakázaním nechcených alebo nepotrebných služieb
- zabezpečením konektivity pomocou VPN, Web SSL
- zabezpečiť autentifikáciu (autorizovanie)
- dodržiavaním bezpečnosti pravidelnou zmenou hesiel každé 3 mesiace
- pozorovaním a detekciou nechcených aktivít
- neotvárať prílohy v mailoch, ktoré vyzerajú podozrivo a používať blokovač reklám

Vlastnením osobného firewallu. Hm, dve brány firewall sú lepšie ako jedna, však? Ak ich človek nevie nastaviť, tak sú samozrejme celkom nanič. V sieťovej komunikácii, pokiaľ sa bavíme o firewalloch, sú to presne tým, čomu hovorím "omen nomen". Teda horiaca stena. V prenesenom význame teda protipožiarna stena. Dokáže zablokovať veľa nechcenej trafiky z Internetu, hoci veľmi často sa používajú i v interných sieťach spoločností a korporácií. Tam je prúd dát tak spletitý a zložitý, že vždy potrebujú niekoľko párov firewallov.

Prečo hovoríme o pároch? Nie preto, že v dvojici sa lepšie kráča životom, ale preto, že vždy sa musí myslieť na zadné vrátka. Čo ak náhodou vypadne elektrina a po jej nahodení zrazu jeden z nich zlyhá? Alebo ak náhodou zlyhá jeho nejaká vnútorná súčiastka? Vtedy by sme boli na holej, ak by sme nemali druhý firewall, ktorý jeho funkciu rád zastúpi. Dve firewally sa používajú i v prípade, že cez ne majú tiecť obrovské množstvá dát. Každý jeden z nich je koncipovaný na určitú záťaž. Čo ak ju jeden proste nepotiahne? Preto sa môžu použiť i na tzv. load balancing, teda na balansovanie záťaže na sieti.

A čo tie naše nechválne známe aktualizácie Windowsu, ktoré majú schopnosť objaviť sa v najnevhodnejšej chvíli? Áno, človeka dokážu poriadne rozčúliť, pretože len a jedine na Windowsoch je potrebný reštart pri nich. Aktualizácie riešia zraniteľnosti, ktoré so sebou prinášajú nové verzie operačných systémov. Preto skáčeme z Windows XP do Windows 7, cez 8, 8.1. až k súčasnej desiatke a jedenástke (nikdy nenechajte, aby vaše dieťa učiť Bill Gates počítať, prosím). Ešte i v januárovej verzii sa môže objaviť nejaká zraniteľnosť, ktorá je ošetrená vo februárovej verzii a tak podobne. Teda nezabúdajme, že kým je operačný systém plne Microsoftom podporovaný (narozdiel od XP, 7 a o chvíľu to čaká i osmičky a desiatky) a **kým máme aktualizácie zapnuté, znižujeme šancu na akýkoľvek útok.** Príchodom SSD diskov sa ale bootovanie do operačného systému skrátilo na pár sekúnd a to platí i o reštartoch.

Je potrebný antivírus keď chodím len na Internet? A kde inde by si prehliadal? Ak je počítač mimo Internetu a siete, pričom vskutku pri ňom nestojí niekto s flash diskom a na ňom nahratým vírusom, čo už taký počítač môže dostať? Ale v opačnom prípade, čo taký antivírus robí? Je to zoznam všetkých známych vírusov, ktoré existujú. A vedzte, že málo ich nie je. Je to v podstate databáza, na základe ktorej sa antivírus rozhoduje, ktoré súbory, programy a aplikácie sú neškodné a ktoré dokážu narobiť šarapatu. Preto **je dôležité mať antivírus zapnutý a nechať ho aktualizovať si databázy**. Čo spraví antivírus, keď nemá nejaký potenciálne škodlivý vírus v databáze? Já jsem všude zdejší, já jsem všude zdejší, u mně nejsi zdejší...já tě tady nemám! Pustí ho priamo do počítača ako neškodný súbor, pričom on si už môže kradnúť informácie z vášho počítača.

Kapitola IX: Aj rúter toho dokáže veľa (Blokovanie URL)

Administrátori používajú ACL (access listy) na zakázanie prevádzky alebo na povolenie iba špecifickej časti prevádzky. Používajú bezpečnostné brány (ďalej len firewally) na to, aby ochránili sieť pred neoprávneným vstupom. Filtrujú neautorizovaný alebo potenciálne nebezpečný paket (balíček s dátami) ešte predtým ako vstúpi do siete.

ACL je sekvenčný zoznam povolení a zákazov, ktorý sa aplikuje na adresy alebo protokoly vyšších vrstiev. ACL poskytuje účinný spôsob ako kontrolovať prevádzku, ktorá vstupuje alebo vychádza zo siete. Je schopný vybrať informácie z hlavičky paketu, otestovať ich a rozhodnúť o jeho osude na základe zdrojovej IP adresy, cieľovej IP adresy a typu ICMP správy.

ACL je kontrolované od hora smerom dole, každý riadok samostatne, hľadajúc zhodu v prichádzajúcom pakete. Smerovač (router, ten prístroj na vašom stole, vďaka ktorému ide doma Internet) nemá štandardne žiadne predkonfigurované ACL, teda nefiltruje prevádzku. Pakety, ktoré prijme sieťové rozhranie sú priamo smerované do smerovacej tabuľky. Všeobecným pravidlom pri aplikovaní ACL je konfigurácia jedného ACL pre protokol, pre smer a pre rozhranie.

Jednoducho definuje súbor pravidiel, ktoré kontrolujú pakety, vstupujúce na vstupné rozhrania, prechádzajú cez smerovač, odchádzajú cez výstupné rozhrania. Neaplikujú sa na pakety, ktoré vzišli zo smerovača. Aplikujú sa však na vstupné a výstupné rozhrania.

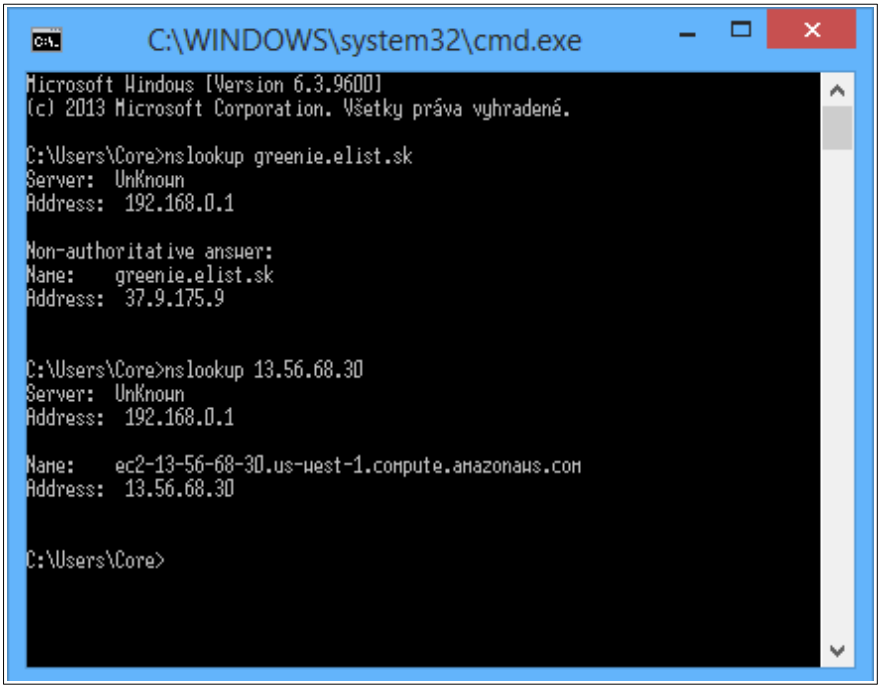
A úplne jednoducho: Do samotného rozhrania routera viete napísať zoznam web stránok či už s podozrivým, nebezpečným alebo pornografickým materiálom. Bežne si môžete stiahnuť i rôzne iné softvéry, ktoré to dokážu blokovať i bez nutnosti inštalovať tieto pravidlá na router. Mávajú i kategorizácie web stránok podľa obsahu, aby sa dali ľahšie identifikovať. Vy teda zablokujete pornografický obsah a aplikácia má už v sebe zabudovanú databázu web stránok tejto kategórie a vy teda nemusíte do zoznamu manuálne pridávať jednu po druhej. Teda môžete, ak sa náhodou omylom prekliknete na podobne hnusnú stránku, ktorá v tejto databáze chýba. V rozhraní aplikácie si jej adresu hodíte do chlievika tej kategórie, do ktorej zapadá. Môžete takto ochrániť seba a deti pred nástrahami čoraz bláznivejšieho Internetu. I hnusný obsah je totiž ľahšie prístupný.

Kapitola X: Aby sme sa nenachytali (IP adresy)

Podvodníci radi využívajú technologickú bublinu a keď sa snažia získať peniaze, povymýšľajú si kopec volovín. A podvodníci nie sú tí, ktorí chodia pod vodou, ale to sú tí, ktorí podvádzajú. Používajú rôzne metódy na získanie peňazí od svojich obetí. A jednou z týchto metód je i technologická bublina – podvodník si môže vymýšľať klamstvá a nepravdivo svoju obeť informovať o skutočnostiach, o ktorých obeť nemá dostatok informácií. Ak obeť napríklad nevie podrobnosti o IP adresách a podvodník jej povie, že jeho IP adresa je ukradnutá, tak obeť zareaguje zhrozene môže povedať: „Preboha a viete mi to opraviť?“ A to je presne to, kam sa každý podvodník chce dostať. Chce si získať dôveru svojej obete a tak tára dve na tri.

Preto je dobré vedieť aspoň základy. V takomto prípade, keď podvodník ohlási, že vaša IP adresa je kompromitovaná (alebo poškodená – nech to znamená čokoľvek) a že hackeri ju využívajú na svoje nekalé účely, cielene klame (sám to ale dobre vie). Vystríha vás, že keď „sa niečo stane“, tak to bude na vás. Určite. Neverte im to. IP adresa sa nedá nijak poškodiť ani ukradnúť, dá sa poškodiť zariadenie alebo počítač, ale nie IP adresa. Dokonca povedia, že sa dá brániť „IP maskovaním“. To je blud na druhú. Takže si to preberme postupne.

IP adresa rozhrania je adresa samotného rozhrania (sieťovej karty). Slovo „adresa“ má dokonca v mene! Je to ako adresa bydliska. Každý niekde bývame a tak i počítače a všetky zariadenia v sieti tiež niekde bývajú. A napríklad 37.9.175.9 môže byť adresa nejakého servera v sieti. A to je adresa web stránky Greenie knižnice. Ako to viem? Keď je počítač pripojený do Internetu, môžete si vyvolaním cmd (príkazového riadku) a príkazom nslookup skontrolovať akúkoľvek adresu či web server.



Ako to funguje? Všade po Internete existujú špeciálne servery, majúce skratku DNS (Domain Name System). Keď vy zadávate do adresného riadka napríklad greenie.elist.sk, tak zjednodušene sa vždy po stlačení klávesy Enter prehliadač opýta DNS servera: „Prosím ťa, akú IP adresu má táto web stránka? Používateľ ju zadal do adresného riadka a potrebujem ju kontaktovať.“ A ten mu odpovie: „Jasné kámo, mám tu záznam vo svojej tabuľke, že tejto web stránke je pridelená adresa 37.9.175.9.“

Učenými slovami ide o 4 skupiny dekadických čísiel, oddelených bodkami, v každej skupine sú čísla v intervale od 0 po 255 (8 bitov umožňuje generovať max. 28 , t.j. 256 kombinácií). Okrem verejných, „bežných“ adresných rozsahov sú k dispozícii i tri tzv. „súkromné“ adresné rozsahy, ktoré sa používajú rozsahy:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

pre tzv. „nepripojené“ siete. Adresy z týchto rozsahov nesmú byť použité na „verejnom“ internete! Súkromné IP adresy slúžia v sieťach, ktoré buď vôbec nie sú pripojené ku Internetu (izolované lokálne siete) alebo sú ku Internetu pripojené prostredníctvom proxy serverov, firewallov či NAT serverov, teda zariadení, ktoré zabezpečia preklad „súkromnej“ adresy na reálnu „verejnú“ IP adresu. Vezmime si teda to, čo mám vyhodil príkaz nslookup pri druhom pokuse s 13.xx.xx.xx adresou (niekedy sa dá takto označiť adresný rozsah sietí.) Všimli sme si, že nám ukázalo 2 výsledky a teda i túto adresu 192.168.0.1. Možno je vám povedomá.

Veru tak. Možno je to adresa i vášho routera, ktorým sa pripájate na Internet vy. Prečo je tomu tak? Ak si vezmeme všetky možné kombinácie, (pozor na vyhradené adresné priestory – môžu byť vyhradené pre testovacie účely a pod.) tak môžeme vytvoriť 232 adries, teda celkovo 4 294 967 296 adries. Veľa, nie? No už nie. V dnešnom svete sa tieto adresy pomaly vyčerpávajú. Preto sa zaviedli „súkromné“ adresné bloky, pre súkromné siete, ako je tá vaša. Skrátene, adresa 192.168.0.1 sa môže na svete vyskytovať miliónkrát, zatiaľ čo 13.56.68.30 len raz. Súkromné adresy z izolovaných sietí však nemôžu byť vysielané, preto sú preložené na jedinú verejnú.

Predtým, než si povieme, niečo o maske, možno si lámete hlavu nad tým, prečo také čísla. Prečo od 0 do 255, prečo nie do 800? Prakticky sa stretneme s IP adresou najčastejšie v dekadickom tvare, napr.: 94.160.100.211. Ale prečítali ste si i to v zátvorke? Myslím to, že 8 bitov umožňuje generovať max. 28 , t.j. 256 kombinácií. Takže sa mrknime na túto adresu.

Toto je dekadický zápis:	94.160.100.211
Toto je binárny zápis:	01011110.10100000.01100100.11010011

Každé číslo v tejto štvorici je teda osemmiestne binárne číslo. Maximum je binárne číslo 11111111, teda dekadické 255.

A načo je nám maskovanie IP adries? Možno to nie je šťastné pomenovanie, pretože to práve týmto podvodníkom nahráva na smeč. My si však zapamätajme to, že maska siete udáva, ktorá časť IP adresy predstavuje adresu siete a ktorá adresu samotného rozhrania v rámci siete. Jednoducho povedané, maska predstavuje objekt s veľkosťou 32 bitov (pozícií) a je zložená zo súvislej oblasti samých jednotiek, na ktoré nadväzuje súvislá oblasť núl.

Príklad:

MASKA 11111111.11111111.11111111.11000000

v dekadickom zápise je to 255.255.255.192 a určuje pre adresu siete 26 bitov (z tých 32 bitov je jednotiek práve 26).

Namiesto dekadického zápisu sa môže použiť i zjednodušený zápis prefixom a to takto:

IP 94.160.100.0 MASK 255.255.255.192

je možné nahradiť úspornejším zápisom

IP 94.160.100.0 /26

Aby sme tomu pochopili, ako maska delí siete, dáme si príklad:

Príklad: Sieť 94.160.100.0 rozdelíme maskou 255.255.255.128 na dve podsiete.

Sieť 1:

adresa siete: 94.160.100.0

brána: 94.160.100.1- tu môže ísť router

broadcast: 94.160.100.127 – volanie siete

Sieť 2:

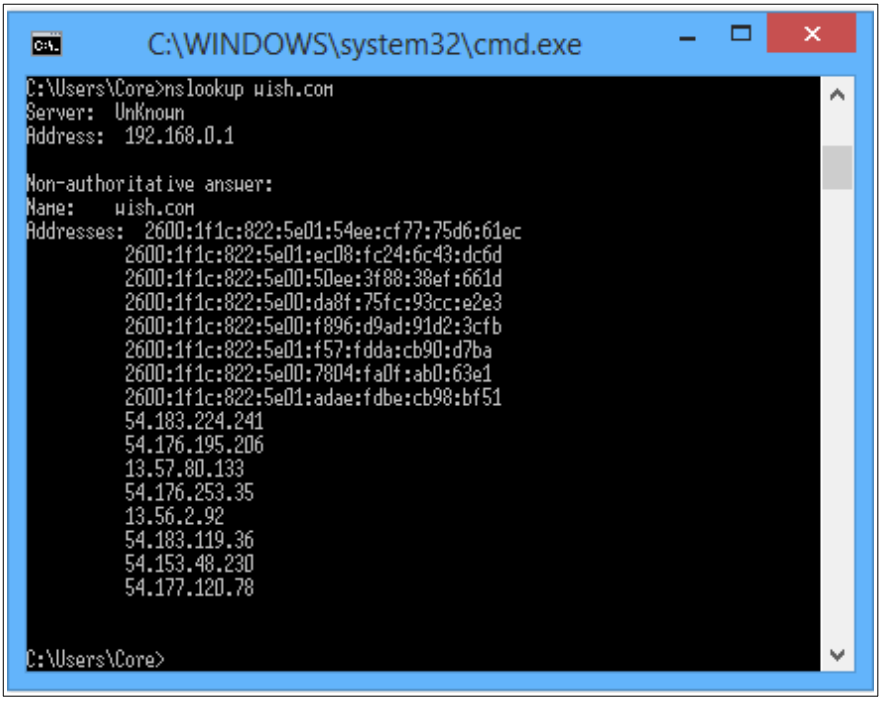
adresa siete: 94.160.100.128

brána: 94.160.100.129 – tu môže ísť router

broadcast: 94.160.100.255 – volanie siete

V každej sieti môže byť 125 počítačov (spolu s bránou to je 126 rozhraní v každej sieti). Každá podsieť môže byť samostatne smerovaná.

Vráťme sa na chvíľu ešte k starému dobrému nslookup a skúsme ešte jednu vecičku. Vyhľadajme si adresu napríklad známej nákupnej platformy wish.com. Čo tak pozeráte, s amazonom alebo ebayom sa také niečo neukáže:



Z tohto zápisu vieme, že adresa má viacero serverov s rôznymi adresami, ale čo zač sú tie, ktoré začínajú na 2600? Zmätení? Posledných 9 adries, ktoré už poznáme, sú typu IPv4 (verzie 4) a tie vrchné sú IPv6 (verzie 6). Prečo teda celkom iný zápis?

Vieme, že veľkosť dostupného IPv4 adresného priestoru klesá, pretože je zaznamenaný nárast populácie pripojenej na internet (najmä Ázia) a nárast zariadení s IP prístupom. Preto sa zadefinovala nová forma IP adries. Tieto „šestky“ majú väčší adresový priestor, sú lepšie globálne dosiahnuteľné, konfigurujú sa samy, nemusia sa prekladať (nejestvujú žiadne „súkromné“ siete) a tiež to pomáha i sieťarom, keďže nie je potrebná ani maska.

IPv4 má 32 bitov (znakov) a celkovo asi 4 294 967 296 adresovateľných uzlov.

IPv6 má 128 bitov (16 bajtov) - štvornásobná dĺžka oproti IPv4- teda $3{,}4x10^{38}$ adresovateľných uzlov (340 282 366 920 938 463 374 607 432 768 211 456) - $5x10^{28}$ adries na osobu. To už je riadne množstvo!

Zatiaľ čo IPv4 sú binárne, IPv6 sú 16-bitové (hexadecimálne)! Preto môžu vyzerať napríklad i takto:

2031:0:130F:0:0:9C0:876A:130B

Kapitola XI: Aké taktiky používajú podvodníci? (Telefonické podvody)

Aj vám volali nejakí týpci, hovoriaci angličtinou s divným prízvukom a povedali vám, že máte niečo s počítačom? Alebo zase iní (pokojne i v češtine alebo slovenčine), že ste vyhrali nejakú voňavku? Tak v prvom rade, ak ste sa nezúčastnili žiadnej súťaže, nemáte ako vyhrať. Chcú od vás vylákať osobné informácie a hlavne peniaze. Toľké prekvapenie.

Čo sa týka tých bláznov s údajne pokazeným počítačom, tí budú chcieť, aby ste im umožnili remote session, teda vzdialené pripojenie. **Nikdy nikomu cudziemu nedávajte remote access!** Môže od vás vylákať osobné heslá, ktoré máte uložené v prehliadači. **Neukladajte si heslá do browseru (prehliadača)!** Robte to mimo neho. Existuje kopec organizérov, ktoré vám umožnia si bezpečne ukladať svoje heslá v jednej databáze, ktorá je zaheslovaná. Principiálne, stačí si pamätať jedno heslo, ktorým otvoríte databázu. V týchto organizéroch vidíte svoje prihlasovacie údaje iba ako hviezdičky, po dvojkliku vám umožnia skopírovať heslo iba na pár sekúnd, kým ho zadáte do okna prehliadača, čím obchádzajú softvéry na sledovanie klávesnice. A hlavne, vyberajte si offline password organizéry. Nie zriedka sa totiž stane, že databázy veľkých korporácií a firiem sa leaknú (to je anglický výraz pre ukradnutie údajov hackerom) a na svetlo sveta ujde veľké množstvo personálnych informácií. **Určite si skontrolujte svoj email cez stránku https://haveibeenpwned.com**. Tá vám dá informáciu o tom, či niekto ukradol heslá k prepojeným službám k vášmu emailu.

V tom horšom prípade môže od vás získať citlivé údaje. Ani za čokoládu im **nevyplňujte formuláre, obsahujúce osobné či bankové údaje!** A čo je dôležitejšie **nikdy tým trollom neplaťte!** Prečo? No pretože platiť sa má za službu. A títo podvodníci vám ukradnú dáta, osobné údaje, zhoršia bezpečnosť počítača a oklamú vás. Stojí vám to za tie peniaze? A ak sa im to vyplatí, idú do toho znovu a znovu a znovu.

Často sa stane, že zle zadáte adresu do adresného riadka, napríklad gooogle.com (a nie že to budete skúšať, vy nezbedníci). I na to čakajú podvodníci. Presmeruje vás to na akúsi ohyzdne vyzerajúcu stránku, ktorá vám oznamuje, že v PC máte vírus a že sa vám Windows zmaže od 300 sekúnd. Prečo to nie je pravda? Je to len skript na tej stránke, prehliadač nikdy nevie siahať do antivírusového softvéru. A ak je na stránke uvedené i telefónne číslo na to, aby ste im zavolali, je to podvod ako vyšitý. Vyšívaný podvod.

Ich klasické taktiky:

- Otvoria Event Viewer a snažia sa vás presvedčiť, že to množstvo chybových hlášok je nejaký vírus alebo hoccčo, pričom tieto nemajú s vírusmi vôbec nič spoločné, na každom normálnom počítači to bude ukazovať rovnako.

- V Správcovi úloh vám ukážu Stopped Services. Na normálnom PC majú byť niektoré služby zapnuté a iné vypnuté, to neznamená žiaden problém.

- Nainštalujú scareware – softvér, ktorý má pôsobiť ako legitímny program, ale jeho úlohou je vystrašiť používateľa falošnými hláseniami o údajných vírusoch a samozrejme, núti vás kúpiť si plnú verziu toho softvéru, napr ReimagePlus.

- Nainštalujú tzv. Registry Cleaners. Ale tie nerobia nič! Skôr môžu ešte poškodiť PC.

- Snažia sa vás presvedčiť, že chodíte na stránky HTTP miesto HTTPS – pozor, to len znamená, že trafika (nie tá na rohu ulice, ale internetový tok údajov) nie je v HTTP nijak zabezpečená, teda ak zadáte prihlasovacie údaje, idú ako plain text (prostý, nijak nešifrovaný text), neznamená to ale, že je stránka nejak škodlivá.

– Aj keď máte všetky položky vo Windows Updates zelené, tak on si bude mlieť svoje, že updates padajú, vyhľadá si len tie, ktoré spadli – ale to je normálne a väčšinou sa tie nedokončené i tak po čase spustia znova. S tým súvisí i ďalšia lož, ktorá spočíva v tom, že tie aktualizácie, ktoré z nejakého dôvodu spadli, označí ako nevyhnutné, ale tie sa temer vždy nainštalujú bez problémov, občas ide o zlyhanie inštalácie balíčka, ktorý je už nainštalovaný. Aktualizácie sa navyše dejú ticho na pozadí a len málokedy upozornia užívateľa, pričom tento človek povie: „A prečo ste si to nevšimli?“

– Ak nemáte iný antivírusový softvér, iba Windows Defender (nie je to nič zlé, ten je v podstate veľmi dobrý! Bez irónie) a podvodník, pozrúc do nainštalovaných programov povie: „Hmm, vidím, že vy nepoužívate žiaden antivírusový program.“, tak znova klame. Windows Defender sa nikdy v nainštalovaných programoch neukáže, pretože v Ovládacom paneli má svoju vlastnú sekciu.

– Vírus sa nechytí tým, že kliknete na množstvo reklám. Vírus sa dostane do PC len aktívnym nainštalovaním alebo na počítači, ktorý nie je aktualizovaný a ktorý nie je inak chránený. Áno, reklamy nás istým spôsobom sledujú, pomocou keksíkov (cookies), ale tie iba navrhujú reklamy a žiadne údaje nikomu nepodstrkujú. Problém je v tom, že veľmi často pri kliknutí na web, ktorý sa tvári ako originálna stránka napríklad kozmetiky, sa presuniete na úplne iné miesto. Prípadne je reklama, ktorá imituje klasické tlačidlo na sťahovanie, ale namiesto vytúženého softvéru získate niekým upravenú verziu.

– Ukazujúc výstupnú tabuľku z netstat sa vám snažia povedať, že máte toľko a toľko cudzích ľudí, ktorí sú na vás pripojení. Nebaštite im to. Väčšina záznamov v tabuľke vzniká tým, že máte otvorené nejaké web stránky, mail klienta alebo pripojenie práve prostredníctvom remote session, takže ak je niekto cudzí na vás pripojený, tak je to on sám! Tu by bolo dobré doplniť si info o internetových protokoloch, ktoré sa zobrazujú v samotnom výpise.

Našťastie napríklad taká aplikácia ako TeamViewer rozpozná konekcie, prichádzajúce z Indie (odkiaľ 90% týchto podvodníkov pracuje). Aplikácia vás upozorní, že sa k vám pripája niekto cudzí a vystríha vás pred možnými útokmi podobného razenia. Títo špekulanti to však obišli tým, že chcú, aby ste sa vy pripojili na nich ako prvý. Už to je ale indikátor toho, že jeho úmysly sú nekalé.

Kapitola XII: Ale ja v tom počítači predsa nič nemám! (Spambot)

Nejeden človek, bez ohľadu na vek, je presvedčený, že v počítači nič dôležité nemá. Pár fotiek, pár hier, nič zaujímavé pre útočníka. Preto ani nie je potrebné riešiť bezpečnosť a všímať si možné riziká. Je to podobné ako s medicínou, kde sa nedá očkovať niekto, kto je presvedčený, že jeho telo je z titánu a nič sa mu nestane a tak si na neho nikto ani žiadny vírus netrúfne.

Výsledok? **Ohromné množstvo spamu šíria počítače, o ktorých to ich majitelia vôbec netušia.** Známy bol prípad z Nemecka, kde sa akosi náhodne objavilo ohromné množstvo detskej pornografie v počítačoch domova dôchodcov. Ľudia, ktorí to tam dostali cez diery v zabezpečení, tak len posielali IP adresy ďalším ľuďom s podobnou záľubou. Prišlo sa na to jednoducho, keď nový počítač s veľkým diskom, na ktorý neboli doinštalované žiadne programy a na ktorom si občas dôchodcovia pozerali fotky z dovoleniek, začal hlásiť nedostatok voľného miesta.

Šikovný a zlomyselný človek môže dostať niektorou cestou svoj softvér do vzdialeného, nezabezpečeného počítača, kde môže monitorovať aktivitu a kde môže daný počítač využívať pre svoje ciele. Občas sa tak stane, že počítače, ktoré skoro nikto nepoužíva a nič zaujímavé tam na prvý pohľad nie je, môžu spôsobiť problémy tak majiteľovi, ako i ostatným. Ak sa napríklad vytvorí spambot, začne z tohto počítača šírenie nebezpečných súborov k ľuďom, ktorých poznáte a máte v adresároch. Vaša mamička si od vás prevezme vírus a už je zle. Prípadne sa cez vašu mailovú schránku dostane k heslám, ktoré doteraz možno niekde používate vy alebo napríklad spomínaná mamička. Niektoré útoky môžu byť naozaj nenápadné a medzi tie zákernejšie patrí pripojenie sa do internetbankingu a presmerovanie pravidelných platieb na iný účet. Vy si to nevšimnete, adresát spočiatku tiež nie a útočník je šťastný. Čím dlhšie sa to nebude kontrolovať, tým bude bohatší a bude rovnaký postup skúšať na ďalších počítačoch a je úplne jedno v akej krajine.

Najväčší problém je s nezabezpečenými počítačmi, ktorý ovláda viac používateľov, vždy len na pár minút, napríklad v knižnici či kaviarni. Nikto tam počas krátkeho času nebude kontrolovať antivírus, firewall či aktualizácie, ale každý tam rýchlo naťuká svoje prihlasovanie do internetbankingu, sociálnych sietí či firemného projektu. Stačí, ak si tam dá niekto chtiac alebo nechtiac uložiť informácie a už sa k tomu dostane ktokoľvek. A hlavne, len úplné minimum ľudí na spoločných, zdieľaných počítačoch, používa tzv. inkognito mód. Len čo otvoríte Facebook, už vás víta správa od milenky toho kolegu, ktorý bol na počítači pred vami. Úsmevné, alebo ani nie?

Matematika nepustí. Stačí prístup k jednému napadnutému počítaču a desať či dvadsať ľudí, čo ho používa, vie poskytnúť šikovnému útočníkovi všetky prístupy ku všetkým kontaktom, správam či napríklad k fotografiám, ktoré by sa nemali dostať na Internet. A niekto, kto bude mať najviac smolu, svoje fotky na Internete uvidí, ak nezaplatí mastnú sumu na modernom výpalnom.

Kapitola XIII: Nástrahy reálneho sveta (Overovanie)

Internet je a vždy bude o výmene informácii. Kedysi bol problém získať nové informácie, no dnes sa dá dostať k takmer čomukoľvek bez námahy. O to ťažšie je overiť si pravosť informácii, keď je ich všade záplava. Hovorí sa, že všetko je na nete, vrátane nástrah pre reálny svet. Tých je, samozrejme, veľa – a najlepšou obranou je zdravý rozum.

Dnes je bežné, že na rôznych zoznamkách je oveľa viac mužov ako žien. A tak mužovi väčšinou nikto nenapíše, zatiaľ čo ženy dostávajú množstvo správ, vrátane najrôznejších netypických požiadaviek. Ak však príde mužovi správa o ženy, vo väčšine prípadov ide o niečo nekalé. Či už reklamu, nejaký podvod alebo celkovo niečo, čo si normálny muž nepraje. Správa od ženy, že muž vyzerá sympaticky a chce s ním sex a ešte sa to doplní o fotografiu intímnych partií je s najväčšou pravdepodobnosťou podvodom. Je to veľmi jednoduchý spôsob, ako bez námahy a na základe vytvorenia ženského profilu (2 minúty) a fotografie z akéhokoľvek videa (1 minúta) dostať človeka na opustené miesto, kde je ľahké zobrať peňaženku či vyžiadať si výkupné od rodiny. Postoj typu „pôjdem sa a keby nič nebolo tak sa vrátim“ môže byť nebezpečný, ale i smrteľný.

Podobne je to s prácou. Bežnou praxou je núkanie jednoduchej praxe v Nemecku či Rakúsku za oveľa vyšší plat ako tu, na Slovensku. Niekto, kto vie o bezpečnosti na Internete i mimo neho len minimum, tam môže ísť aj bez akéhokoľvek overovania. Overiť si pritom telefónne číslo (stačí hodiť do Google), meno a všetko ostatné je pritom pomerne jednoduché. V každom prípade je dobrý nápad dať vedieť viac ľuďom, ak sa niekde chystáte – a ideálne osloviť nikoho, kto sa vyzná do Internetu a má dosť zdravého rozumu, aby to urobil za vás. Aby sa nestalo, že namiesto opatrovania starších ľudí bude nútené ponúkanie sexuálnych služieb, alebo napríklad ťažká práca za minimálnu mzdu alebo za jedlo niekde v podzemí.

Môžete tiež spolupracovať s políciou, ktorá overuje najrôznejšie ponuky. **Nahlásením niečoho, čo nemusí byť v poriadku, môžete zachrániť životy ostatným ľuďom.** V každom prípade je vždy lepšie ísť spoznávať svet cez uznávanú agentúru než cez niekoho úplne neznámeho.

Kapitola XIV: Som lepší, lebo som viac závislý! (Freemium hry)

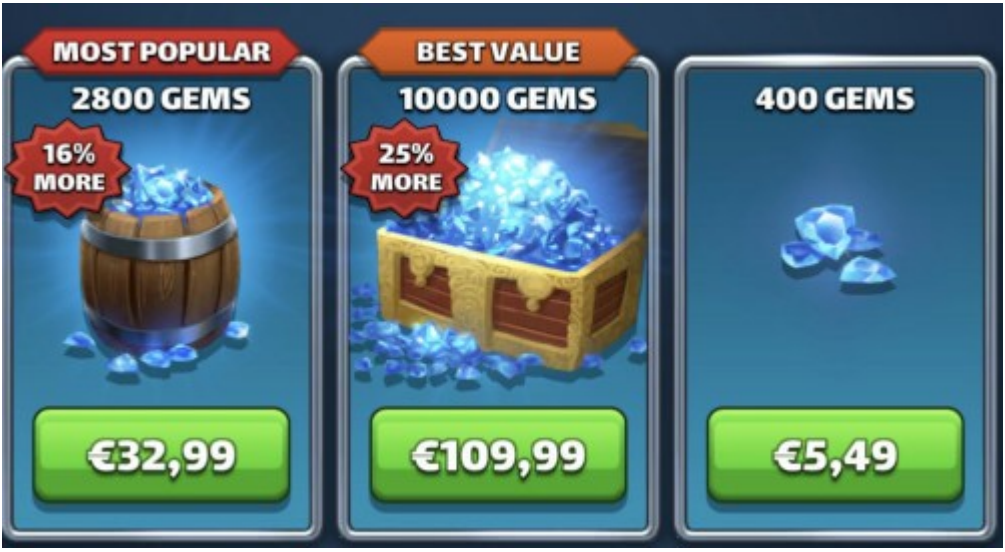
Internet je plný nebezpečenstiev, no nie všetko je o internetovom bankovníctve, ukradnutých heslách či rôznych neznámych hrozbách. Niekedy patrí medzi najväčšie hrozby to, čo je krásne, farebné a vyzerá tak bezpečne a bezproblémovo. Ozaj, už máte svoje mesto?

Freemium hry sú zaujímavé v tom, že ich môže zadarmo hrať ktokoľvek. Dostanete svoje mestečko a ako správny architekt, Boh alebo čokoľvek iné si robíte čo chcete. Teda, často aj to čo nechcete. Kto chce byť prvý v rebríčkoch, odkryť všetky špeciálne stavby a mať lepšiu armádu ako ostatní? Pravdepodobne všetci. A je to logické. Pekne vybudované mestečko je krásne a čoraz krajšie, tak… prečo s tým prestať?

Nebezpečenstvo je úplne jednoduché. Závislosť. Pocit, keď potrebujete prekonať toho otravného hráča, ktorý rýchlo buduje svoje mesto z rovnakého dôvodu ako vy. Závislosť je zo začiatku len ťažko pozorovateľná, ale ak chce-

te postupovať v rebríčku, rýchlo sa chytíte do pasce. Nový mlyn sa bude stavať ešte 15 minút. Počkáte 15 minút, aby ste ho mohli znovu vylepšiť? Ak áno, budete mať viac pšenice. Ak nie, ten druhý hráč bude produkovať viac a bude mať výhodu.

Tvorcovia hier to dobre vedia. Náklady na údržbu hier sú malé, no kto si kúpi hru, ktorú predtým nehrali? A zvlášť hru, ktorá nemá koniec? Asi nikto. Preto je registrácia rýchla a bezplatná. Čo však, ak si to niekto po vyskúšaní zamiluje? Stačí ponúknuť pár balíčkov, kde si môžete zakúpiť diamanty a za diamanty zlato. Prečo dve meny? Je to preto, aby bežný hráč nemal presný prehľad, čo si vlastne kupuje. Balíčky mincí, drahokamov a v podstate akejkoľvek hernej meny si môže kúpiť za reálne peniaze, pričom nikdy nevie presne ani akú hodnotu vlastne kupuje.



No a teraz babo, raď! Naschvál si vymyslia divné hodnoty (2800, na to ako prišli?) len preto, aby vám sťažili počítanie. Nie zriedka je nejaká ponuka označená ako Best Value, aby vám to „uľahčili“. V zmysle skôr sťažili, pretože občas sú ponuky časovo obmedzené a ak rýchlo nekúpite, zdražejú! To podmieňuje len efekt nedostupnosti, výnimočnosti a to sa ľuďom páči. Na druhej strane ale nedáva hráčom čas na premyslenie si svojich krokov. Zároveň ten, kto má diamanty, môže napredovať rýchlejšie. A čo je lepšie, dať pár eur za rýchle vypracovanie projektu alebo čakať dva mesiace, kým sa to postaví?

Freemium hry tak prinášajú pocit, že niečo dokážete, ale musíte pracovať na svojej dedinke deň i noc. Vstať skoro, aby sa dal povel na poslanie armády, stavanie nového levelu múru a tak podobne. Ale čo ak treba ísť do práce, do postele alebo čokoľvek podobné? Čo ak ma niekto prepadne, keď tu nebudem? Čo ak prídem o 1000 jednotiek, ktoré som budoval dva mesiace? Najlepším spôsobom je vykašľať sa na tieto hry. Už deň či dva po tomto rozhodnutí sa človek cíti ľahšie, viac uvoľnene a menej podráždene. Žiť v strachu, že sa niečo stane vašej dedinke, je príšerné a zväzujúce. Veľmi rýchlo to prestane byť potešenie a začne to byť potreba, podobne ako spánok, ktorá nedokáže byť naplnená, pretože vždy príde nová a nová výzva, ktorá hráčovi prinesie malý bonus, ale človeku vôbec nič.