Co dokáží hackeři-amatéři

Poznejte, jak přesně se vám mohou nezvaní hosté nabourat do sítě či počítače (CD)

PATRIK MALINA

Při vyslovení pojmu hacker si uživatelé většinou představí někoho, kdo se pokouší za účelem dosažení nehynoucí slávy prolomit ochranu sítě co možná nejznámější instituce, či nepozorovaně přesunout zajímavé finanční částky z jednoho bankovního účtu na jiný. Realita je však ve srovnání s bájnými představami poněkud odlišná, a co více, drsná a neúprosná. Naprostá většina pokusů i úspěšných útoků proti privátním informacím probíhá v rámci vnitřní sítě, což jinými slovy znamená, že hackerem (byť jen amatérským) může být třeba někdo z vašich kolegů ve stejné kanceláři u protějšího stolu. Přemýšleli jste někdy o ceně a významu informací na vašem počítači, nebo o způsobu, jak přistupujete do své poštovní schránky? Máte představu, jak by mohli vaši „kolegové" či „spolupracovníci" naložit s daty, pokud by znali vaše přístupové heslo? Myslíte, že je to nesmysl? Pojďte se s námi podívat na několik možností a postupů, jež dávají jasně najevo, kde jsou slabá místa při běžném využití počítačové sítě. Možná budete překvapeni, jak neopatrně jste si dosud počínali. V tomto článku jsme se zaměřili na velmi běžně používané technologie a postupy, s nimiž většina uživatelů přichází do kontaktu mnohokrát denně. O to větší bude možná vaše překvapení.

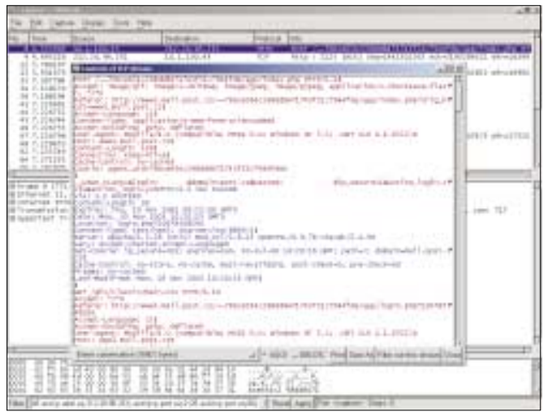
Upozornění: *V následujících odstavcích najdete poměrně podrobný popis postupů, jež mohou vést k narušení zabezpečení počítačů a počítačových sítí, jejich zneužití či zcizení důvěrných informací. Takto důkladně vám látku předkládáme proto, abyste si byli plně vědomi všech nebezpečí, jež vám hrozí. Uváděné návody by měly posloužit především k ověření „snadnosti", s jakou lze některé informaci získat, a tím k posílení snahy o zabezpečení komunikačních kanálů a odstranění případných slabin.*

Při experimentování buďte vždy opatrní a uvědomte si, že některými postupy je možné hrubě narušit jak etické, tak zákonné normy. Proto testování provádějte výhradně ve vlastní, nejlépe experimentální síti.

Typ útoku:

Nabourání do poštovní schránky freemailové služby

Používání veřejných, zdarma dostupných e-mailových služeb (tzv. freemailů) je dnes pro řadu uživatelů naprostou samozřejmostí. Ačkoliv na použití těchto systémů číhá z pohledu ohrožení privátnosti celá řada nebezpečí, svěřujeme jim dnes a denně svá tajemství, a to často velmi cenná. Pojďme se podívat na jednu z možností, jak lze zcizit obsah e-mailové komunikace či samotnou přihlašovací informaci.



◀ Program Ethereal je univerzálním síťových snifferem (analyzátorem). Dokáže nejen proniknout do hloubi paketů, ale i šikovně extrahovat TCP spojení do čitelné podoby. Jméno a heslo pro freemail bylo záměrně na konci prvního „hnědého" odstavce vymazáno, neboť bylo bez problémů čitelné.

Princip ohrožení:

Klíčem k potenciálně velmi vysoké míře ohrožení freemailové komunikace je několik okolností, jejichž součinnost dává obsah našich e-mailů či přihlašovací údaje všanc útočníkům. Prvním problémem je již samotný vstup do vaší osobní poštovní schránky prostřednictvím prohlížeče: v průběhu přihlašování typicky zadáváte prostřednictvím speciální stránky (formuláře) přihlašovací jméno a heslo.

Zásadní potíž spočívá v tom, že ve výchozí podobě, kterou řada freemailů využívá, se tyto údaje přenášejí pomocí základní HTTP komunikace v nezašifrované podobě. Bez větších obtíží lze tedy potřebná data v lokální síti odchytit (vyčenichat – sniffovat), takže například kolegové v práci mohou při vaší neopatrnosti získat plnohodnotné přihlašovací údaje do vaší schránky.

Velmi podobným způsobem – opět na principu sniffování – lze snadno odchytit i samotný obsah e-mailových zpráv, neboť ten je doručován z poštovního serveru do prohlížeče uživatele v typicky nijak nešifrované, textové podobě. Útočník tedy v případě, že do pošty přistupujete např. z pracovního počítače ve firemní síti, nemusí nijak složitě vaše heslo hádat, neboť si je prostě odchytí a přečte.

Postup útoku:

Pro odchycení komunikace s webovou freemailovou schránkou může velmi dobře posloužit jakýkoliv kvalitní sniffer (analyzátor síťových paketů), jako např. zdarma dostupný Ethereal. Tento nástroj může zachytit veškerý síťový provoz v „okolí" vašeho počítače – tedy např. u kolegy u vedlejšího stolu – a poskytnout pohled do nitra přenášených paketů.

Zmíněný program naleznete na stránkách ***www.ethereal.com*** nebo na našem CD. Při jeho instalaci je potřeba dodržet následující sled: nejdříve spusťte zavedení speciálního ovladače s názvem WinPcap, jenž zajistí odchytávání vlastního síťového provozu, a poslé-ze instalujte samotný Ethereal. Po spuštění samotné aplikace, jež pracuje s dobře ovladatelným grafickým rozhraním, spustíte vlastní odchytávání síťové komunikace pomocí povelu Start v menu Capture – v bezprostředně zobrazeném dialogu si nezapomeňte ověřit, že program pracuje v tzv. promiskuitním modu, což jinými slovy znamená zachycování kompletního provozu v síti kolem vás.

Po spuštění provádí Ethereal načítání obsahu paketů do hlavního okna, a práce útočníka tím teprve začíná. V získané záplavě informací je potřeba se nejdříve zorientovat – pomocí klepnutí na záhlaví ve sloupci Source doporučujeme seřadit pakety dle odesílatele, což vám velmi usnadní nalezení konkrétního provozu z inkriminovaného počítače. Pokud hledáte přístup uživatele do webové pošty, měli byste se zaměřit na protokol HTTP a adresu některého z freemailových serverů. Po nalezení alespoň jednoho z paketů odpovídajícího typu lze využít výbornou schopnost Etherealu: použijte na vybrané položce pravé tlačítko myši a zvolte možnost Follow TCP Stream, díky čemuž dojde k zobrazení obsahu komunikace ve speciálním okně. V tomto rozhraní snáze dohledáte přihlašovací údaje, a pokud uživatel nesáhl po šifrovací technologii, vše pravděpodobně bude čitelné.

Jak se bránit:

Samotnému čenichání (sniffování) se lze bránit jen stěží, neboť tato možnost je dána samotným principem používané síťové technologie (ethernet), a proto si musíme pomoci dodatečnými mechanismy. Poměrně účinným postupem je využívání zabezpečovacích technologií pro přenos šifrovaného webového obsahu, jímž vévodí protokolová sada SSL. Pokud si chcete být zabezpečením alespoň trochu jisti, vyberte si freemailovou službu, jež přenos pomocí SSL podporuje. Docílíte toho, že veškerý přenos je kryptován, a útočník v odchycených paketech není schopen nic zjistit.

Důležitým druhotným krokem je též striktní používání odlišného hesla u freemailů a ostatních systémů – pokud by přeci jen potenciální útočník přihlašovací údaje získal, neměly by se shodovat třeba s přihlašováním do firemní sítě, neboť to by pro vás mohlo znamenat velké nebezpečí.

Najděte informace, které opravdu potřebujete!

MARTIN IGNJATOVIĆ

Každý, kdo to myslí s bezpečností vážně, musí mít své zdroje informací. Pokud chcete o bezpečnosti vědět více, případně si udržet aktuální přehled, jste na tom podobně. Tento článek by měl být jemným úvodem do této problematiky a ukázat základní směr, kudy se vydat. Míst, kde naleznete informace o bezpečnosti jsou tisíce, liší se však svou aktuálností, rozsahem a kvalitou.

Web

Nejrozsáhlejším místem, kde lze hledat informace o bezpečnosti, je samozřejmě prostředí webu. Ovšem v tomto rozsáhlém prostoru potřebujeme najít to, co hledáme. Můžeme se proto spolehnout buď na informace od lidí z oboru, nebo na svůj vyhledávač. Vyhledávač vám však nepodá informace o tom, jak je stránka kvalitní nebo aktualizovaná. Je proto lepší dát na rady lidí z oboru a navštěvovat známé a ověřené servery. Výčet serverů však není tím jediným, co budete potřebovat. Především si budete muset uvědomit, jaký je váš konkrétní cíl a požadavky. Od těchto jasně stanovených priorit se odvíjí vše. Nelze zbytečně bloudit po stránkách zabývajících se bezpečností operačních systémů Windows, pokud chceme nastavit přístupová práva pod Linuxem, nebo hledat na stránkách, zabývajících se zabezpečením poštovního serveru, informace o bezpečném programování v Perlu. Rozdělíme si tedy následující přehled serverů podle okruhu našeho zájmu.

Aktuality

Pokud nemáte vyhrazený směr a požadavky na konkrétní věc, můžete čerpat z níže uvedených serverů. Tyto servery poskytují aktuality v oblasti počítačové bezpečnosti. Chcete-li být tedy v obraze a vědět, co právě hýbe světem bezpečnosti, navštivte následující stránky.

Kvalitních serverů poskytujících takovéto informace mnoho není, a v českých zemích je to ještě podstatně horší. Zaměříme se tedy na dva nejvýznamnější anglické servery, kterými jsou:

● ***www.securityfocus.com***

Patrně nejvýznamnější server co se týče aktuálnosti a rozsahu. Najdete tu téměř vše, co chcete o bezpečnosti vědět. Stránky jsou neustále aktualizovány. Najdete zde sekce věnované produktům od Microsoftu, systémům UNIX, systémům odhalení průniku, penetračním testům či firewallům. Každá ze sekcí je aktualizovaná a obsahuje mnoho informací o bezpečnosti. Stačí si vybrat. Nejdůležitější částí stránek však je sekce, která obsahuje seznam a popis aktuálních chyb různých produktů. Jde o takzvaný BugTraq. Tato databáze je velmi kvalitní a rozsáhlá. Můžete zde najít seznam chyb téměř libovolného produktu. V informaci naleznete přesný popis chyby, za jakých podmínek může být chyba zneužita, kterého konkrétního systému (programu) a verze se chyba týká, jak může být chyba odstraněna, jak může být zabráněno zneužití. Často je přiložen i takzvaný exploit, což je část kódu, která ukazuje, jak může být chyba zneužita. Ke sledování chyb v jednotlivých produktech se můžete přihlásit i pomocí e-mailové konference. O tom však až za chvíli.

● ***www.cert.org***

Jde o projekt pod záštitou univerzity Carnegie. Stránky jsou zaměřeny na sledování bezpečnosti jednotlivých systémů a na hledání chyb v těchto systémech. Tento projekt běží již od roku 1988 a je stále jedním z nejlepších. Informace o aktuálních chybách jsou podobné jako na webu securityfocus, avšak jejich popis není tak konkrétní ani obsáhlý. Na konci každé stránky s informacemi o chybě však naleznete refe-

rence na stránky, kde se můžete o programu či chybě dozvědět mnohem více, což je velmi cenný zdroj informací.

Linux

Pokud provozujete na svém systému, ať již jde o server nebo pracovní stanici, operační systém Linux(UNIX), a chcete znát několik zdrojů o bezpečnosti, můžete navštívit následující webová sídla:

● ***www.redhat.com***

Stránky nejrozšířenější distribuce Linuxu. Najdete zde opravy pro několik verzí. U každé opravy je uvedeno, i čeho se oprava přesně týká, jak funguje a na co si je třeba dávat pozor. Opravy jsou distribuovány pomocí rpm balíčků, takže aktualizace je téměř triviální a zvládne ji každý běžný uživatel linuxového systému. Pokud provozujete jinou distribuci, než je redhat, navštivte webové sídlo své distribuce a naleznete zde podobné informace a aktualizace. Každá distribuce je pravidelně aktualizována a je na vás, zda tyto změny sledujete či nikoliv. Na většině stránek je rovněž možné přihlásit se do konference, pomocí které jste automaticky informování, pokud je nalezena nějaká bezpečnostní chyba nebo je vydána nová záplata.

● ***www.seifried.org***

Pokud jste v bezpečnosti Linuxu nováček a chcete nějaký komplexní zdroj informací o zabezpečení svého systému, navštivte stránky *www.seifried.org*. Naleznete zde proslulou Linux Administrator's Security Guide. Je to velmi dobrý první krok k zabezpečení vašeho systému. Na těchto stránkách však naleznete mnohem více. Najdete zde i OpenBSD Administration Guide. Obě publikace jsou velmi dobře napsané a začátečníkům v *nixové bezpečnosti jsou většinou vřele doporučovány. Pro někoho však může být mírně handicapující, že jsou oba dokumenty v angličtině. Ti, kteří nevládnou anglicky, však ještě nemusí věšet hlavu. Existují i české zdroje.

● ***www.root.cz***

Patrně nejčtenější a obsahově nejkvalitnější český server, zabývající se Linuxem. Server je rozdělen do několika sekcí, z nichž je jedna věnována bezpečnosti. Naleznete zde spoustu praktických informací a návodů. Spousta návodů je typu „step by step", takže podle nich může postupovat i začátečník v této oblasti. Problém je zde zpravidla velmi dobře popsán a jsou vysvětleny i některé důležité momenty, které by mohly dělat začínajícím uživatelům potíže.

Ke každému článku lze přidat vlastní komentář, a právě tyto komentáře jsou velmi často také velmi dobrým zdrojem informací. Jsou pomocí nich zodpovězeny některé nejasné momenty, případně jsou uvedena a diskutována jiná možná, často i lepší řešení. Server je aktualizován velmi často, nové články přibývají denně.

● ***www.linuxzone.cz***

Další známý server, zabývající se Linuxem. Podobně jako na rootu zde naleznete spoustu zajímavých informací, recenzí, ale i praktických návodů. Sekce serveru jsou rozděleny podle tématu a vybere si zde každý, od programátora přes správce systému až po běžného uživatele. Velmi zajímavou a dobrou částí projektu jsou takzvané Secuity Digest. V nich naleznete typy na zajímavé programy, přehled chyb v programech současných, ale i odkazy na zajímavé články a témata, jež souvisejí s bezpečností.

Typ útoku:

Prolomení a ukradení bezdrátové Wi-Fi komunikace

Bezdrátové síťové připojení pomocí technologie Wi-Fi (též dle normy 802.11b) je stále populárnější metodou přístupu k jiným počítačům, a to jak v lokálních sítích, tak k poskytovatelům internetových služeb. Uživatelé běžně spoléhají při zabezpečení na volbu SSID identifikátoru a v lepším případě ještě na šifrovací technologii WEP, přestože existuje způsob, jak tyto mechanismy prolomit a utajené údaje následně zneužít. Útočník navíc nemusí sedět u vedlejšího stolu, ale např. v sousední místnosti či na lavičce před budovou. Komunikujeme přeci vzduchem, ne?

Princip ohrožení:

Použití bezdrátové síťové technologie Wi-Fi nabízí v současné době několik mechanismů zabezpečení provozu, jejichž cílem je eliminovat neautorizované uživatele při snaze o „parazitování" na cizí síti. Protože samotná podstata přenosu – rádiové vysílání – nijak nemůže zabránit odposlechu (sniffování), je obsah přenášených dat vydán napospas potenciálním útočníkům. Přestože Wi-Fi implementuje jako jeden z ochranných postupů šifrování, označované jako WEP, tato metoda bohužel není dostatečně odolná. Jedním z problémů je samotná implementace šifrovacího postupu, jenž není z nejkvalitnějších, a do hry vstupuje další klíčový faktor: pro šifru je zadáván statický klíč k opakovanému, dlouhodobému použití. A právě tento postup umožňuje existenci nástrojů, s jejichž pomocí lze při určitém úsilí rozlomit i přenos chránění šifrou WEP. Stejně tak druhý základní mechanismus ochrany bezdrátové komunikace, kterým je přidělení a následné použití identifikátoru SSID, je možno obejít a přípojné body tak zneužít.

Postup útoku:

Prvním předpokladem pro úspěšné odchycení Wi-Fi komunikace je hardwarové vybavení v podobě odpovídající síťové karty, neboť zdaleka ne všechny typy poskytují potřebnou funkcionalitu. Vhodné jsou například adaptéry s čipovými sadami Orinoco, nicméně před koupí je potřeba komponentu vyzkoušet. Druhou nezbytnou součástí je anténa s kvalitním příjmem, resp. s tzv. vysokým ziskem, jež dovoluje z éteru „vylovit" hledaný signál. Právě s kvalitním přijímačem lze odchytit komunikaci i na desítky či několik stovek metrů daleko.

Potřebnou hardwarovou výbavu je rovněž dobré porovnat s nároky softwaru, jejž budete pro útok využívat. Jedním z vhodných programů, po němž je potřeba sáhnout v první řadě, je NetStumbler. Aplikace slouží k „pátrání" v rádiových pásmech a vyhledávání existujících komunikačních kanálů. Na stránkách ***www.stumbler.net*** najdete mimo jiné i popis kompatibilních síťových karet, a aplikaci samotnou též naleznete na našem CD. Pomocí této aplikace učiní útočník první krok: prozkoumá své okolí a nalezne existující sítě a jejich konfiguraci, např. v podobě identifikátoru SSID, jehož hodnotu musí znát pro „napíchnutí" do existující infrastruktury.

Samotná aplikace NetStumbler již může být pro prolomení existující bezdrátové sítě dostačující. Po prozkoumání jednotlivých frekvenčních pásem, na nichž Wi-Fi komunikuje, lze v přehledném zobrazení zjistit, které sítě nejsou chráněny šifrou, a lze za pomoci zobrazeného SSID okamžitě podniknout pokus o připojení. Pokud tato snaha nevede k cíli, je možné, že cílová síť provádí kontrolu MAC (hardwarových) adres síťové karty klienta. V tomto případě přichází na řadu použití nástroje typu sniffer, tedy např. již výše zmíněného Etherealu. Cílem je zachytit probíhající komunikaci a vysledovat MAC adresy počítačů, jež do sítě mají oprávněný přístup. Následně tuto informaci využijeme a změníme MAC adresu svého fyzického adaptéru na onu oprávněnou – toho lze dosáhnout třeba pomocí oblíbeného programku SMAC, jejž naleznete na adrese ***www.klcconsulting.net/smac*** nebo na našem CD. Předstíráním oprávněné fyzické adresy tedy můžete překonat další obrannou bariéru.

▲ **Měli jste až dosud dojem, že MAC (hardwarová) adresa síťové karty je parametr neměnný a spolehlivý? Třeba tento prográmek SMAC názorně předvede, že vše je jinak!**

Posledním oříškem na cestě do cizí bezdrátové sítě může být šifrování zkoumaného provozu pomocí mechanismu WEP. I když překonání této překážky není nijak snadné, existují určité možnosti, například v podobě nástroje AirSnort. Tato utilita je dostupná pro operační systém Linux (či příbuzné) a pro její použití ve Windows je nutná alespoň kompilace v prostředí Cygwin. Program dokáže vyhodnocením dostatečného množství paketů s určitou pravděpodobností odhalit klíč k šifře WEP, a tím překonat často poslední obranu, která navíc bývá považována za spolehlivou. Tento krok však většinou vyžaduje dlouhodobější úsilí, neboť počet potřebných paketů jde řádově do stovek tisíc až milionů, což často odpovídá mnohahodinové komunikaci.

Windows

Pokud pracujete s operačními systémy z rodiny Windows, budou vás pravděpodobně zajímat stránky, které se bezpečnosti Windows věnují. Takových stránek je opět mnoho, a je jen na vás, které z nich si vyberete. Majitele operačních systémů Windows však netrápí jen bezpečnost systému samotného, ale všechny s bezpečností související věci. Dalším velmi důležitým prvkem a problémem v oblasti zabezpečení systémů Windows jsou viry a červy. Informace o nich a ochranná opatření proti nim jsou nedílnou součástí bezpečnosti Windows. Virové problematice se věnují následující servery.

● ***www.microsoft.com/security***

Zde by měl začít asi každý uživatel systémů Windows. Naleznete zde přehled všeho důležitého, co se týká bezpečnosti Windows. Nejde tedy jen o Security Bulletins, které popisují odhalené chyby Windows, ale i o informace o právě „řádících" virech, červech atd. Pokud toužíte po praktických informacích, jak zabezpečit váš systém Windows, budete se muset podívat někde jinde. Například na již zmíněném securityfocusu najdete spoustu užitečných článků.

Ostatní

Bez ohledu na to, jaký operační systém provozujete, existují věci, které jsou společné téměř všem operačním systémům. Jde o obecné postupy nebo konkrétní problémy společné více operačním systémům. Stránek, zabývajících se takovouto problematikou, je opět mnoho. Zde je příklad několika z nich:

● ***www.krypta.cz***

Jde o český projekt. Naleznete zde spoustu užitečných informací, jako jsou návody, přehled aktuálních událostí, ale i články, které se zabývají teoretickou stránkou některých bezpečnostních aspektů. Velmi dobře a důkladně je zde zpracováno téma kryptografie.

Dokumentace

Klíčem k zabezpečení systému je jeho velmi dobrá znalost. Pokud svůj systém dobře znáte a rozumíte jeho vnitřním mechanismům, nebude pro vás takový problém jej zabezpečit, na rozdíl od systému, který znáte jen povrchně. Proto je studium a poznávání systému stejně důležité, jako shánění informací o jeho zabezpečení. Dokumentace k jednotlivým operačním systémům je velmi mnoho, dokonce i v elektronické podobě.

● ***www.linuxdocs.org***

Jak již to u Linuxu bývá, je možné sehnat vše co s ním souvisí přímo v prostředí internetu. Nejinak je tomu i u dokumentace. Na těchto stránkách naleznete dokumenty opravdu o všem, co souvisí s Linuxem. Počínaje programováním a informacemi o hardwaru, přes síťování a konfiguraci systému až po dokumentaci k jednotlivým aplikacím. Jsou zde i všechna HOWTO, což je nesmírně cenný zdroj informací.

● ***www.memoware.com***

Pokud vlastníte PDA zařízení a chcete si dokumentaci číst i jinde než u svého PC, navštivte tyto stránky. V sekci Computers naleznete nepřeberné množství dokumentů týkajících se více či méně výpočetní techniky. Výběr je opravdu obrovský, a záleží jen na vašich požadavcích.

● ***docs.linux.cz***

Ani české servery nezůstávají pozadu a nabízejí informace o produktech. Vedle již výše zmíněných praktických návodů na jednotlivých serverech, můžete i na těchto stránkách nalézt informace z mnoha oblastí.

Software

V mnoha návodech na zabezpečení systému se dozvíte, že pomocí příslušných nástrojů můžete bezpečnost svého systému otestovat. Kde však všechny tyto nástroje získat? Spousty bezpečnostních nástrojů naleznete na následující webové stránce.

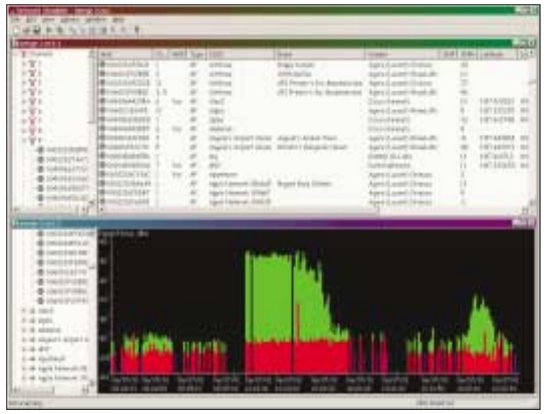
● ***www.packetstormsecurity.org***

Patrně nejrozsáhlejší archiv bezpečnostních nástrojů. Naleznete zde nástroje pro všechny současně používané operační systémy a plnící nejrůznější funkce. Každý měsíc zde najdete i soubor obsahující všechny exploity (programy využívající bezpečnostní chyby) vydané v uplynulém měsíci. S nimi však raději neexperimentujte, pokud přesně nevíte, co dělají a jak fungují. Jsou však dobrým zdrojem informací o tom, jak která konkrétní chyba funguje a k otestování bezpečnosti vašeho systému.

Konference

Sledovat dění v oblasti bezpečnosti není jednoduché. Vyžaduje to spoustu času a zdrojů. Naštěstí existují nástroje, pomocí kterých si můžete celou situaci velice usnadnit. Takovými nástroji jsou například i e-mailové konference a souhrny zpráv. Stačí se do příslušné konference přihlásit, a budete všechny požadované zprávy dostávat pohodlně na svou e-mailovou adresu. Nejkvalitnější konference naleznete na již několikrát zmíněných stránkách securityfocusu. Zde v sekci mailing lists naleznete konference zaměřené prakticky na všechny oblasti bezpečnosti. Namátkou jmenujme například: BugTraq, firewally, Linux, Microsoft, viry a další.

3 0666/FEL ❑



▶ Utajení jakékoli provozované bezdrátové sítě standardu Wi-Fi je opravdu iluzorní. První pomůckou při průzkumu je Network Stumbler, jenž dokáže pročesat éter a poskytnout potenciální cíle.

Jak se bránit:

Z výše uvedeného postupu je patrné, že stoprocentně spolehlivá ochrana bezdrátového připojení je v praxi spíše iluzí, a závěr je takový, že na samotnou konfiguraci Wi-Fi nelze spoléhat. Při přenosu dat po síti tedy musíte důsledně využívat dodatečné ochranné postupy a příslušné technologie: při přístupu na citlivé webové stránky nezapomínejte na SSL komunikaci, e-mailové zásilky šifrujte např. pomocí PGP či S/MIME (obě varianty mohou fungovat např. v Outlooku) a případně ochraňte celý síťový provoz pomocí šifrovaného tunelu (např. IPSec). Pokud využíváte Wi-Fi pro přístup k internetu, ujistěte se, zda váš poskytovatel podporuje ověřování přihlášení pomocí normy 802.1x, aby na vaší přípojce nepozorovaně neparazitoval někdo jiný.

Samotné šifrování WEP má sice výše zmíněné nedostatky, avšak jeho použití přeci jen může výrazně napomoci k zabezpečení – jak jsme uvedli, prolomení vyžaduje dlouhodobé sledování a slabinou je právě statický, dlouhodobě používaný klíč. Pokud jej budete často obměňovat, bude to sice mírně nepohodlné, avšak o mnoho bezpečnější.

Typ útoku:

Hacknutí přihlašování do instant messaging programu

Aplikace pro „instant messaging“, tedy jakousi jednoduchou, přístupnou komunikaci patří v současné době k nejběžnějším, a proto není třeba představovat programy jako ICQ či MS Messenger. Při každodenním používání těchto nástrojů drtivá většina uživatelů ani nepřemýšlí o tom, že jimi přenášená data jsou velmi náchylná na odchycení. Falešný pocit bezpečí rovněž vyvolává možnost přihlašování pomocí hesla, což je opět zásadní nedorozumění. Přihlašovací informaci lze totiž u výše uvedených programů poměrně jednoduše odhalit, a váš účet tak může být snadno použit někým jiným.

Princip ohrožení:

Možnost ohrožení či zcizení komunikace programů uvedeného typu je založeno na stejném principu, jako výše uvedené hledání přihlašovacích informací k freemailovým službám. V roli útočníka můžete průběžně monitorovat komunikaci okolních počítačů a využít zásadní slabiny programů jako např. ICQ, neboť v průběhu přihlašování jsou kritické informace zasílány bez dostatečného zabezpečení.

Pokud použijete výchozí instalaci programu ICQ, ICQ Lite či MSN Messenger (starší varianty), bez jakéhokoliv varování jste vystaveni riziku, že zasílané přihlašovací heslo bude v lokální síti, tedy např. kolegou u vedlejšího stolu, odchyceno. Velmi alarmující je fakt, že pro tuto proceduru není potřeba žádných mimořádných znalostí.

Postup útoku:

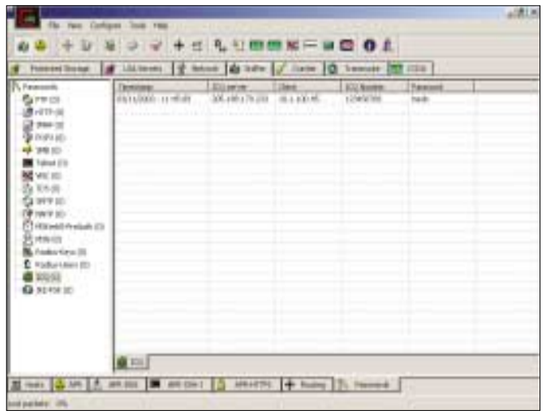
Pro realizování tohoto typu útoku budete v případě dobré volby potřebovat jediný program, jenž zajistí vše potřebné. Velmi vhodným nástrojem je nesmírně všestranná utilita Cain & Abel, kterou najdete na stránkách ***www.oxid.it/cain. html*** nebo na našem CD. Jednou z mnoha jejích možností je právě průběžné sledování síťové komunikace a „vysávání“ hesel či jiných přihlašovacích údajů do velmi přehledné podoby.

Po běžné instalaci vám program nabídne grafické uživatelské rozhraní, v němž přejděte na kartu pojmenovanou Sniffer. Právě tato část aplikace řeší odchytávání síťových paketů a jejich průzkum. Přejděte do spodní části okna a zvolte záložku Hosts, jež slouží k sestavení seznamu počítačů – cílů vašich útoků. Pomocí pravého tlačítka myši vyberte volbu Scan MAC Addresses a zvolte rozsah síťových IP adres, jejichž držitelé vás zajímají.

Pokud adresu cíle neznáte, zadejte určitý rozsah a program prozkoumá a vyhledá dostupné počítače, z nichž si můžete vybrat, neboť jejich jména budou rovněž přeložena. Poté v tabulce zanechte pouze cílový stroj (či více sledovaných počítačů), a zahajte samotné odchytávání pomocí tlačítka při levém okraji horní lišty nástrojů (se symbolem síťové karty). Poté, co

program po určitou dobu poběží, zkuste se podívat na záložku Passwords (při spodním okraji okna) a očekávejte žádoucí údaje. Při bližším ohledání sami zjistíte, že aplikace toho dokáže „nasát" opravdu hodně, tedy nejen hesla pro ICQ.

Takto jednoduše může útočná akce proběhnout v případě, že cílový počítač se nachází v lokální síti na stejném ethernetovém segmentu, tedy typicky ve společném rozbočovači (hubu). Avšak ani v případě, že využíváte moderní infrastruktury a jednotlivé stanice jsou připojeny do přepínače (switche), není nic ztraceno, neboť Cain & Abel nabízí možnost v podobě speciální techniky, jež dovoluje tento *„nedostatek"* obejít. Postup bývá nazýván jako ARP Poissoning či ARP Spoofing, a protože jeho následky mohou být i při pouhém experimentování dosti nevyzpytatelné, před jeho použitím důrazně varujeme. I ve výše uvedené základní podobě program dokáže hodně a jeho sílu si takto můžete ověřit.



▶ Nástroj Cain&Abel patří mezi velmi všestranné a zdatné pomocníky při odchytávání informací v lokální síti a jejich dešifrování. Zde je na ukázku zachycena komunikace klienta ICQ, a to včetně jeho přihlašovacího hesla.

Jak se bránit:

Možnosti zabezpečení instant messaging komunikace jsou velmi problematické, případně často téměř nemožné. Tvůrci těchto programů se primárně přeci jen zaměřují na jiné vymoženosti svých výtvorů, než je kvalitně zabezpečený přenos. Pokud chcete s vysokou pravděpodobností eliminovat pokusy o sniffování hesla v lokální síti, je vhodné použít univerzální řešení, např. v podobě technologie IPSec, jež šifruje síťovou komunikaci již na úrovni IP paketů bez ohledu na aplikační data. Tato možnost je plně dostupná v operačních systémech Windows 2000, XP a 2003 Server, a to bez nutnosti používat jakýkoliv další software.

Další možností je přinutit komunikační program používat v lokální síti přenos pomocí aplikačního šifrovaného kanálu SSL, k čemuž je ovšem zapotřebí na hranici sítě umístit odpovídající proxy službu. Např. ICQ umožňuje zapouzdřit svůj přenos právě do podoby tohoto odolného protokolu, čímž je možno eliminovat lokální odposlech.

Pochopitelně nejspolehlivější metodou ochrany je zmíněný software nepoužívat. Protože to však často není možné, dávejte si pozor alespoň na to, abyste používali k přihlašování v těchto systémech zcela odlišná hesla od těch, jež slouží pro přístup do firemní sítě. Prozrazení vašeho „univerzálního" hesla by mohlo mít katastrofální následky. 3 0669/FEL ❑