Hlídejte si svá data

JAK NA BEZPEČNOST WINDOWS 2000

MARTIN IGNJATOVIĆ

Windows se stala rozšířeným systémem nejen pro pracovní stanice uživatelů, ale v poslední době i v oblasti serverů. To s sebou samozřejmě přináší rizika i co se týče bezpečnosti. A právě na to, jak je to s (ne)bezpečností systému Windows nasazeného jako serveru, se podíváme v dnešním článku. Článek je určen zejména pro začínající správce a má jim poskytnout úvod do bezpečnosti Windows jako serveru.

WINDOWS JAKO SERVER

Jak již bylo řečeno v úvodu, začínají se systémy Windows prosazovat i v oblasti serverů. To má několik příčin, ale tou hlavní je samozřejmě uživatelská přítulnost. Server Windows dokáže nakonfigurovat prakticky každý pokročilý uživatel systému Windows, který má alespoň základní znalosti o službách a sítích. Stačí několik kliknutí, a vše funguje. To s sebou však nese i značná bezpečnostní rizika. Stejně jako i u jakéhokoliv jiného systému platí, že bezpečnost nedělá systém, ale člověk a většina bezpečnostních incidentů je způsobena právě lidskými chybami.

IDENTIFIKACE A ANALÝZA

Pro útočníka je životně důležité zjistit, na co vlastně útočí. Proto musí mít detailní informace o svém potenciálním cíli. Naneštěstí jsou systémy Windows poměrně sdílné, co se týká poskytování informací. Chce-li útočník napadnout nějaký firemní server, jeho první kroky nejspíše povedou na webové stránky příslušné firmy, pokud existují. Z nich lze vyčíst mnoho informací. Pokud jsou například stránky psány v asp, je jasné, že firemní web běží pod systémem Windows a pravděpodobně i pod http serverem o společnosti Microsoft. Dále, pokud stránky poskytují nějakou službu, u níž se předpokládá ukládání údajů, je pravděpodobné, že na serveru poběží i nějaký databázový server. Ze stránek lze získat rovněž mnoho užitečných informací, jako například kontakty na správce sítě, webu atd. Další krok povede téměř jistě na některý vyhledávač. Vyhledávač, ač se to zdá na první pohled nepravděpodobné, je skvělým prostředkem v rukou zkušeného útočníka. Lze hledat na stránkách různých firem, prohledávat diskusní fóra a jinak zjišťovat informace o potenciálním cíli. Pokud útočník ze zjištěných informací usoudí, že mu cíl stojí za námahu, bude pokračovat ve sbírání dalších informací. Jeho kroky velmi pravděpodobně povedou do databáze whois, aby zjistil, jaké IP adresy, doménové servery a jací lidé mají něco společného s vybraným cílem. Po získání těchto informací přijdou na řadu aktivní kroky, a těmi jsou skenování systému a identifikace služeb. Je však třeba upozornit, že všechny tyto kroky útočník dělat vůbec nemusí, pokud se snaží útočit zevnitř sítě. Všechny tyto informace mu budou zajisté známy a navíc bude vědět, jak systém pracuje, jaké služby se používají. Útočníci z vlastních řad jsou tudíž daleko nebezpečnější než ti zvenku a mohou způsobit mnohem víc škod. Cílem útočníka zvenku je právě přístup do vnitřní sítě, a tak se zaměříme na kroky, které k tomu musí udělat.

Nyní tedy k aktivním krokům průzkumu, jimiž jsou skenování a identifikace služeb. Pro tento účel existuje spousta nástrojů. Jelikož se pohybujeme na platformě Windows, ukážeme si nástroje určené právě pro tyto systémy. Zřejmě jedničkou v oboru je nástroj NetScanTools Pro (zkušební verze je k dispozici na stránkách *www.netscantools.com*). Možnosti, které nám tento nástroj dává k dispozici, jsou opravdu široké, jak vidíte na obrázku. Nevýhodou tohoto produktu však je, že není k dispozici zdarma.

Pokud se vám nechce platit, můžete sáhnout po jiném nástroji, jímž je SuperScan od společnosti Foundstone, Inc. *(www.foundstone.com)*. Tento program nemá tak široké možnosti jako NetScanTools, je však rychlejší a je zdarma. Ideální kombinací obou dvou je nástroj CyberKit *(www.networkingfiles.com/PingFinger/CyberKit.htm)*, který je rovněž k dispozici zdarma a obsahuje základní nástroje pro diagnostiku sítě.

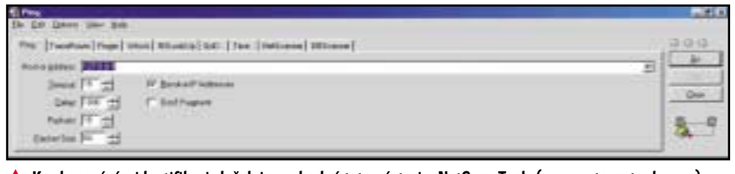
Nyní tedy již k samotnému skenování. Pro útočníka je důležité vědět, jaké služby na serveru běží. Proto bude pravděpodobně začínat skenováním portů. K tomu může použít jeden z výše uvedených nástrojů. Systémy Windows standardně poslouchají na několika portech, a podle toho jsou také snadno identifikovatelné. Pokud tedy budou otevřené porty 135 až 139 nebo 445, jde téměř jistě o systém Windows. Tyto porty používá protokol NetBIOS, který je v systémech Windows využíván nejčastěji. Systémy Windows lze podle těchto portů identifikovat i podle jejich verze. Např. Windows 9x nenaslouchají na portu 135, naopak Windows 2000 jako jediná naslouchají na portu 445. Dále existuje několik standardně využívaných služeb, které běží na známých portech. Mezi tyto služby patří např. http server na portu 80, SMTP server na portu 25, DNS server na portu 53, FTP server na portu 21, MSSQL na portu 1433 až 1434 a Windows terminal server na portu 3389. Pokud se podaří útočníkovi zjistit služby, které na serveru běží, dost možná bude chtít zjistit i jejich verzi a další informace, jež o sobě tyto služby poskytují. Ideálním nástrojem pro tuto činnost je Netcat *(www.atstake.com/research/tools/index.html#network_utilities)*.

Tento nástroj je k dispozici pro systémy Windows i pro UNIX. Nástroj je řádkově orientovaný a dá se přirovnat k švýcarskému noži, který by měl patřit do výbavy každého, kdo se zajímá o bezpečnost IS. Řada služeb, jako například IIS server, o sobě poskytuje mnoho informací, které mohou útočníkovi velmi pomoci. Obrana proti poskytování těchto informací není vůbec snadná, jako je tomu např. u systému UNIX, kde můžeme tyto informace libovolně modifikovat. Nyní se tedy podíváme na protokol, který je v systémech Windows využíván nejčastěji, a tím je SMB/CIFS.

PROTOKOL SMB/CIFS

Jak již bylo řečeno, je protokol SMB/CIFS nejčastěji využívaným protokolem v sítích Windows. Tento protokol je relativně starý, ale prošel řadou inovací a změn. Přesto je zmíněný protokol stále velmi nebezpečný a při špatném nastavení poskytuje o systému velmi mnoho informací. Cílem útočníka bude zjistit, jak jsou počítače logicky uspořádány a pojmenovány. Máme tím na mysli zejména pracovní skupiny, domény, doménové stromy a doménové lesy. K tomuto průzkumu útočník nebude potřebovat žádné speciální nástroje, vystačí si s nástroji dodávanými standardně se systémem Windows. Mezi tyto nástroje patří například program NetView. Tento nástroj je velmi jednoduchý, znakově orientovaný, avšak velmi účinný. Pomocí příkazu netview /domain lze zjistit všechny domény v síti. Pokud bude chtít útočník získat výpis z počítačů náležejících do jedné z domén, použije příkaz netview /domain:název_domény. Stejnou práci vykoná i nástroj Okolní počítače, avšak není tak rychlý a jeho výstup nelze dále zpracovávat (skripty atd.). Cílem každého útočníka bude pravděpodobně řadič primární domény. Tento počítač shromažďuje informace o všech počítačích v doméně, může řídit jejich činnost a většinou obsahuje údaje, které se snaží útočník získat.

Dalším krokem útočníka bude inventarizace sdílených prostředků. Systémy Windows



▲ Ke skenování a identifikaci služeb jsou vhodné tyto nástroje: NetScan Tools (www.netscantools.com), SuperScan (www.foundstone.com) a CyberKit (www.networkingfiles.com/PingFinger/CyberKit.htm)

standardně nabízejí několik položek, na které může směřovat útok. Těmito položkami jsou IPC$, Netlogon, Admin$, C$. Ideálním nástrojem pro průzkum sdílených prostředků je DumpSec od firmy Somarsoft *(www.somarsoft.com)*. Tento nástroj využívá k průzkumu tzv. prázdnou relaci. Jistě si říkáte, že tyto informace by neměly být volně k dispozici. Nyní si tedy řekneme, jak tomuto úniku informací zabránit. Nejsnazší je vypnutí protokolu SMB/CIFS. Tento protokol lze blokovat na hraničním firewallu, pokud chcete omezit přístup k těmto službám zvenčí. Nechcete-li tyto služby používat ve vnitřní síti, budete je muset vypnout na všech strojích. Pokud se těchto služeb nechcete vzdát, ale zároveň chcete zabránit inventarizaci, pozměňte v registrech klíč HKLM\SYSTÉM\CurrentControlset\Control\LSA\Restrictanonymous a jeho hodnotu změňte na dva. Pokud používáte Windows 2000, můžete pomocí modulu Bezpečnostní zásady aplikovat toto nastavení na všechny podřízené objekty Active Directory.

Poté, co útočník zjistí všechny údaje, které jsou mu k dispozici, má na výběr několik věcí. Pravděpodobně se však bude snažit získat uživatelský účet na některém systému. Může k tomu použít více nástrojů, lze ovšem předpokládat, že nejdříve vyzkouší známé účty a známá hesla. Mezi tyto účty patří účty vestavěné do systému Windows, jako například účet Guest, Administrator atd. Známá hesla jsou taková, která se například shodují s názvem účtu, s něčím jménem, nebo heslo není vyžadováno vůbec. Situace častější, než se může zdát. Kolik z vás se přihlašuje do systému Windows bez hesla a má práva administrátora? Kolik lidí má na svém systému vypnut účet Guest nebo má jiné heslo u toho účtu, než je prázdné heslo nebo heslo guest? To zkušenému útočníkovi může stačit na to, aby do systému vstrčil pomyslné dva prstíky a později jej celý zdiskreditoval. Pokud však na žádná taková hesla nepřijde, bude zřejmě následovat slovníkový nebo podobný útok. Databázi často používaných hesel lze na internetu celkem snadno získat. Následná aplikace je velmi prostá. Lze k tomu použít spoustu speciálních nástrojů, jako např. NAT nebo SMBGRind.

Zkušenější útočník si vystačí i s příkazovou řádkou a jejími vestavěnými funkcemi. Útočník má však ještě další možnost, a tou je sledování síťového provozu. Síťový provoz v rámci protokolu SMB/CIFS může být velice účinným zdrojem informací, zejména pro útočníka. Nejzajímavější budou pro útočníka jistě ověřovací údaje. K tomu lze použít nástroje L0phtcrack *(www.atstake.com/research/lc/)*. Nástroj by měl mít, stejně jako netcat, ve výbavě každý, kdo se zabývá bezpečností systémů Windows. Tento nástroj sloužil primárně ke crackování systémových hesel systému Windows, umí však crackovat i hashe, které slouží k ověřování v sítích Windows. Tyto hashe lze zachytávat pomocí libovolného snifferu, lze však použít i vestavěný modul L0phtcracku, jímž je SMBCapture. Tento modul sleduje síťový provoz a zachycené údaje předává přímo crackovacímu nástroji, takže máte tzv. vše v jednom. Crackování hashů je pak podle složitosti hesla otázkou času. Nejlepší obrana je tedy protokol SMB/CIFS nepoužívat, což není vždy možné, proto se podíváme, jak se takovým útokům bránit.

První zásada je používat složitá hesla. Jak však to však vynutit i u ostatních uživatelů? S pomocí systému Windows celkem lehce. Otevřete si v *Ovládacích panelech* položku *Místní nastavení zabezpečení* a zde přejděte na položku Zásady účtu. Zde pak povolte, aby heslo splňovalo požadavky na složitost. Rovněž se můžete bránit tak, že nastavíte, aby se heslo po zvoleném počtu špatných pokusů o přihlášení automaticky zamknulo. U této direktivy však buďte opatrní, neboť může velice snadno dojít k uzamčení všech účtů a vlastně tak dojít k útoku typu DoS (odmítnutí služby), protože útočník, jenž zná jména uživatelských účtů, může všechny účty snadno zamknout a rovněž uživatel, který si splete heslo, může svůj účet zamknout. Vy pak budete mít plné ruce práce s opětovným odemknutím všech účtů. Lze rovněž nastavit, po jaké době se heslo odemkne, což ale není příliš šťastné řešení, protože to útočníka nezastaví, nanejvýše zpomalí. Proto je lépe vynutit používání silných hesel, která nebudou snadno uhodnutelná. To docílíte již zmiňovaným způsobem, ale můžete rovněž udělat osvětu mezi uživateli a vysvětlit jim, jak vypadá správné heslo. Stejně tak je dobré chybné pokusy o přihlášení logovat a logy pravidelně kontrolovat a analyzovat. Pokusy o průlom odhalíte snadno a lehce je rozeznáte od špatných přihlášení legitimních uživatelů. Je rovněž dobré vypnout účty, které nejsou používané.

▲ **Pokud máte kapesní počítač, navštivte stránku www.memoware.com a stáhněte si odtud užitečné příručky o bezpečnosti**

ÚČET ADMINISTRÁTORA

Pokud se i přesto podaří útočníkovi nějakým způsobem proniknout do vašeho systému nebo sítě, lze předpokládat, že se nesmíří jen s uživatelským účtem. Určitě bude chtít svá privilegia rozšířit, nejlépe rovnou na úroveň administrátora. V sítích, kde jsou k dispozici domény Windows, jsou doufám tato rizika všem jasná. Jak se ovšem může útočník stát administrátorem? Má k dispozici několik nástrojů. Mezi oblíbené patří například PipeUpAdmin *(http://content.443.ch/pub/security/blackhat/WinNT%20and%202K/pipeup/)*. Ten po spuštění přidá zvolený účet do skupiny Administrators. Naštěstí tuto chybu řeší záplata od Microsoftu, ale ne každý má systém aktualizovaný. Podobné chyby se však objevují poměrně často, a tudíž si nemůžete být nikdy jisti tím, že se někomu nepodaří eskalovat svá privilegia. Proto bedlivě sledujte bezpečnostní věstníky Microsoftu a včas aplikujte příslušné záplaty. Nejlepší obranou je samozřejmě útočníka do systému vůbec nepouštět.

VZDÁLENÁ SPRÁVA

Pokud se útočníkovi podaří do systému proniknout a zvýšit svá práva na úroveň administrátora, pravděpodobně si bude chtít nad systémem udržet kontrolu a vzdálený přístup. Ten může realizovat pomocí různých programů a služeb. Jednoduchou možnost, jak přistupovat do systému, nabízí například služba Telnet. Ta je součástí systému Windows a na mnoha systémech je zapnutá, čímž si správci zjednodušují život. Bohužel ho zjednodušují i útočníkovi, protože Telnet je služba, která by již v dnešní době neměla mít na systému co dělat. Bohužel Windows nenabízejí standardně šifrovaný nástroj, jako například ve světě UNIXu běžně používaný SSH. Proto Telnet vypněte a sledujte, zda není aktivní. To by mohlo znamenat, že si někdo udělal zadní vrátka do vašeho systému. Dalším nástrojem je *remote.exe,* který je součástí Ressource kitu. Jiným ideálním nástrojem pro správu z příkazového řádku je například i nástroj netcat. Ideálním a jistě pohodlnějším je však pro útočníka ovládání systému z grafického uživatelského rozhraní (GUI). K tomuto účelu se ideálně hodí například VNC nebo nástroj podobného typu. Ten umožňuje útočníkovi pracovat v grafickém rozhraní přesně tak, jako kdyby seděl přímo před monitorem počítače. Může tak systém s Windows ovládat z grafického prostředí UNIXu, neboť VNC je k dispozici i pro tuto platformu.

Jaká je tedy nejlepší obrana proti vzdálené správě a vzdálenému ovládání systému? Stejně jako v předchozích případech, i zde platí, že nejlepší obranou je útočníka do systému vůbec nepouštět. Pokud si chcete ověřit, zda na vašem systému neběží nějaká služba, která by umožňovala vzdálený přístup, proskenujte svůj počítač a všechny nestandardní porty, o kterých víte, že by se ve výpisu objevovat neměly, důkladně analyzujte a později zakažte.

IIS5

Http server společnosti Microsoft je jednou z nejvíce napadaných aplikací na platformě Windows. Přesto jej používá stále víc lidí. Existují stovky možností, jak využít konkrétních chyb daného produktu. Nemá cenu zde všechny chyby a útoky podrobně vysvětlovat. Povíme si čeho se mohou chyby týkat, jaké mohou mít důsledky, jak se proti nim bránit. První skupina útoků může směřovat na vyřazení serveru z provozu. To lze učinit například špatným požadavkem URL. Takových chyb již bylo objeveno mnoho a jistě není příjemné, když vám každých pět minut někdo shodí váš systém. Druhá skupina útoků směřuje k odhalení zdrojového kódu aplikací napsaných například v asp.net nebo asp. Tyto zdrojové kódy mohou obsahovat spoustu důležitých informací, jako například hesla k databázovému serveru, uživatelská jména a hesla nebo poznámky programátorů, jež mohou být pro útočníka velice cenné. Třetí skupina útoků se zaměřuje na souborový systém, který je na systému, kde server IIS běží. Bylo rovněž odhaleno několik chyb, jež umožňovaly procházet souborovým systémem. Nyní si tedy povíme, jak se v obecné rovině bránit útokům na IIS. Tyto rady jsou univerzální a měly by velmi výrazně přispět k bezpečnosti systému. Velmi dobrým nápadem je umístit složku, kde jsou vaše skripty, na jednotku jinou, než na jaké se nachází váš systém. Většina známých chyb, které umožňovaly procházet souborovým systémem nebo spouštět systémové příkazy, neumožňovala přeskakovat z jedné jednotky na druhou. Nikdo vám sice nezaručí, že příští chyba toto umožní, nicméně je to lepší opatření než žádné. Na jednotce, kde budou umístěny vaše skripty, nepoužívejte systémový soubor FAT a práva nastavte velmi restriktivně, což znamená, že by nikdo krom uživatele, pod kterým běží IIS, neměl mít právo na spuštění nebo zápis. Všechny události pečlivě protokolujte a analyzujte. Rovněž sledujte všechny bezpečnostní opravy, a záplaty neprodleně aplikujte. Známý červ Code-Red se šířil v době, kdy se již měsíc vědělo o chybě v IIS. Jeho šíření tedy v podstatě umožnili neschopní a nezodpovědní administrátoři.

SQL SERVER

Přestože existují i jiné databázové produkty, je SQL server od společnosti Microsoft stále velmi využívaným nástrojem pro ukládání dat. Oblíbený je zejména ve spolupráci s IIS v prostředí WWW. Bohužel i SQL server s sebou nese bezpečnostní rizika, která je třeba mít na zřeteli a dávat si na ně pozor. Jeden okruh problémů tvoří uživatelská jména a konta. Na ty si je třeba dávat pozor zejména. Většina vývojářů se totiž nějakou autentizací neobtěžuje a používá prázdná hesla. Tato prázdná hesla používá zpravidla i pro účet správce serveru SQL (sa). Tato hesla zůstanou bohužel často zachována i při přechodu aplikace do ostrého provozu. Útočníkovi pak stačí napsat libovolný skript v jeho oblíbeném jazyce ASP, VB, PHP, Perl... a může se pustit do pátrání po serverech, které mají prázdné heslo. Takových serverů je v sítí víc, než by se dalo čekat. Proto vždy dobře zabezpečte uživatelské účty a pravidelně je kontrolujte. Dalším rovněž hluboce rozšířeným zlozvykem je poskytnout plný přístup k databázi všem uživatelům a neobtěžovat se zřízením uživatelských účtů s jasně vymezeným přístupem k jednotlivým datům. To může být v prostředí WWW velmi nebezpečné. Posuďte sami, co způsobí více škod, pokud se útočníkovi podaří získat zdrojový kód stránky a bude zde uvedeno jméno a heslo uživatele s plným přístupem k databázi, nebo pokud zjistí jméno a heslo uživatele, který má přístup pouze k datům, jež jsou zobrazena na stránce WWW, a má přístup jen pod heslem. Dobrým nápadem je rovněž nespouštět SQL server pod účtem administrátora. Sice je to docela pracné, ale určitě se vám to vyplatí. Důležité je rovněž to, jak SQL server po síti komunikuje. Standardně používá šifrovací mechanismus XOR, který, jak jistě sami uznáte, není pro prostředí sítě tím ideálním. Proto uvažujte o zavedení SSL modulu, jenž bude veškerou komunikaci šifrovat, nebo o nasazení IPSecu. Oboje není snadné, ale pokud to s bezpečností myslíte vážně, nic jiného vám nezbude. Důležitá je rovněž pravidelná aplikace záplat, stejně jako u jakéhokoliv jiného produktu.

OBECNÉ RADY PRO ZABEZPEČENÍ

Neexistuje žádná obecná rada, jak zabezpečit systém Windows. To vždy záleží na podmínkách, možnostech a požadavcích. Existuje však několik obecných kroků, které k bezpečnosti systému výrazně přispějí. V úvodu bylo řečeno, že bezpečnost systému dělají lidé. Proto jsou nejúčinnější zbraní v boji proti útočníkům znalosti. Sledujte proto konference o bezpečnosti a čtěte literaturu na toto téma. Pokud máte například kapesní počítač, navštivte stránku *www.memoware.com* a stáhněte si příručky o bezpečnosti. Nelze však studovat pouze bezpečnost. Abyste zabezpečili svůj systém, musíte mu dobře rozumět a chápat všechny jeho vlastnosti a schopnosti. Je-li počítač v síti, je rozumět i síťové komunikaci a chápat její principy.

Dalším krokem je sledovat současné dění v oblasti a být včas informován o všech incidentech a chybách, které se objeví. Poté logicky vyvstává nutnost včas a správně aplikovat všechny bezpečnostní záplaty a opravy.

Nápady, dotazy, návrhy témat, jež vás zajímají zasílejte na adresu igm@centrum.cz. Na vaše dotazy k této problematice se pokusíme najít odpovědi. 3 0325/FEL ❑