Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Bezpečnost operačního systému Windows

Marek Pohl

Bakalářská práce

2008

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Katedra informačních technologií
Akademický rok: **2007/2008**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Marek POHL**

Studijní program: **B2646 Informační technologie**

Studijní obor: **Informační technologie**

Název tématu: **Bezpečnost operačního systému Windows**

Zásady pro vypracování:

Teoretická část:
* Zhodnocení bezpečnosti OS Windows verze NT následujících.
* Možné techniky napadení OS, jejich detekce a prevence.

Implementační část:
* Použití škodlivého kódu, který využívá bezpečnostní mezeru OS k jeho napadení.
* Vytvoření kódu, který bude umožňovat monitorování aktivit uživatele na počítači.
* Zabezpečení OS před obdobným útokem.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

Endrof, Carl. Hacking - detekce a prevence počítačového útoku

Vedoucí bakalářské práce: **Ing. Lukáš Slánský**
Ústav elektrotechniky a informatiky

Datum zadání bakalářské práce: **30. listopadu 2007**

Termín odevzdání bakalářské práce: **16. května 2008**

Univerzita Pardubice Česká republika

L.S.

doc. Ing. Simeon Karamazov, Dr.

děkan

V Pardubicích dne 29. dubna 2008

SOUHRN

Tato práce se zabývá problematikou bezpečnosti operačních systémů Windows. Cílem této práce je poukázat na hrozby skrývající se ve škodlivých programech a ukázat základní metody jak se proti těmto programům bránit. Popsáno je několik nejrozšířenějších metod počítačových útoků na operační systém Windows a jejich následky. Součástí jsou také doporučení bezpečné konfigurace systému a základní bezpečnostní pravidla. Výsledkem této práce je zhodnocení bezpečnosti operačních systémů Windows.

KLÍČOVÁ SLOVA

bezpečnost, windows, cracking, exploit

TITLE

Security of Operating System Windows

ABSTRACT

This paper deals with problem of security of Windows operating system. The main objective of this work is to show danger hidden in malicious programs and to show the basic methods how to defend the computer against it. This paper describes the most common methods used to attack the Widows operating system and shows impacts of these attacks.
The recommendation of safe configuration and the basic security rules are given. The results of this paper is evaluation of the security of Windows operating systems.

KEYWORDS

security, windows, cracking, exploit

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

Název zkratky	Anglický význam	Český význam
AGP	Accelerated Graphics Port	AGP je vysokorychlostní sběrnice pro připojení grafické karty k základní desce počítače.
Assembler	Assembler	Assembler je programovací jazyk velice blízký strojovému kódu.
DoS	Denial of Service	Odmítnutí služby, nedostupnost služby jejím běžným uživatelům.
Exploit	Exploit	Exploit je kousek kódu který umožňuje díky chybě v běžící aplikaci spustit vlastní kód, což by za standardní situace nebylo možné.
FTP	File Transfer Protocol	Technologie pro přenos souborů mezi počítači.
LPS	Low Privilege Service	Nízkoprivilegovaný mód, aplikace ve Windows Vista je spuštěna s nižšími uživatelskými právy.
MFC	Microsoft Foundation Class	MFC je knihovna zaobalující části Windows API do tříd.
TFTP	Trivial File Transfer Protocol	Zjednodušená implementace protokolu FTP.
UAC	User Account Control	UAC slouží k přiřazování práv spouštějící se aplikaci nebo programu.

1 ÚVOD

Se stále se rozvíjejícím světem počítačů a počítačových sítí a internetu se rozvíjí také jeho „podsvětí“. Na škodlivý programový kód je dnes možné narazit na každém kroku.

Od dob kdy se využívají počítače téměř všude a ke všemu, narůstá i počet počítačových útočníků. Počítačové útoky se stále častěji stávají noční můrou správců podnikových i malých sítí, administrátorů malých stanic i domácích uživatelů. Počítačoví útočníci chtějí nad počítačem získat kontrolu, získat z něj informace a později jej využít ke svému účelu. Útočníci zkouší stále nové fígle jak počítač ovládnout. Nezabezpečený a zastaralý systém pro ně bývá snadnou kořistí.

V operačních systémech se často objevují chyby, které je třeba záplatovat dříve než jsou zneužity. Záplaty vydává vydavatel operačního systému, aplikuje je správce operačního systému. Programové chyby se vyskytují také v nainstalovaných programech a službách a tyto chyby je také možné zneužít.

Dobrá bezpečnost operačního systému je podmínkou pro to, aby se systém nestal nebezpečný pro samotné uživatele počítače. Dobře zabezpečený systém vyžaduje pravidelnou a důkladnou údržbu. Operační systém vyžaduje péči administrátora, potřebuje být aktualizovaný, záplatovaný a v neposlední řadě také správně zkonfigurovaný. Patřičnou pozornost a péči vyžadují taktéž v systému nainstalované programy a služby.

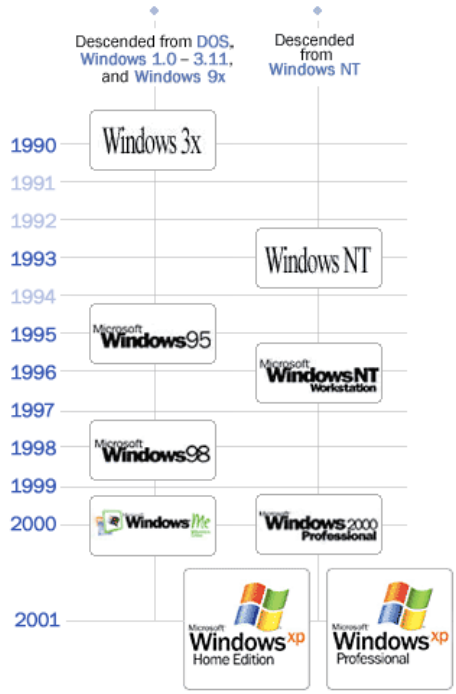
2 HISTORIE WINDOWS

Microsoft Windows je řada grafických víceúlohových operačních systémů společnosti Microsoft. První operační systém firmy Microsoft se objevil na trhu v roce 1981 a od těch dob jsou operační systémy této firmy neoddělitelnou součástí počítačového světa.

2.1 Rozdělení Windows podle technologie

Podle prostředí ve kterém umožňují spouštět aplikace je možné je rozdělit do tří skupin, na 16bitové, 32bitové a 64bitové. Obrázek 2.1.1 ukazuje operační systémy Windows na časové ose.

Obr. 2.1.1: Časová osa Windows (1)



2.1.1 16bitové operační systémy

Společnost Microsoft uvedla první verzi Windows na trh v roce 1985. Tehdy se jednalo pouze o nadstavbové grafické uživatelské prostředí nad tehdejším 16bitovým operačním systémem MS-DOS. Mezi uživateli byla velice oblíbena verze Windows 3.1, která spatřila světlo světa v roce 1992. Další verze Windows 3.11 for Workgroups pak přinesla sdílení souborů v síti.

Ve Windows 95 v roce 1995 byl zásadně změněn grafický vzhled, v systému bylo integrováno dříve samostatně dostupné rozšíření Win32s pro podporu 32bitových aplikací v 16 bitovém systému. Integrována byla také podpora protokolu TCP/IP, což znamenalo umožnění přímého přístupu k Internetu bez instalace doplňků od jiných dodavatelů.

Další vylepšení přinesla verze Windows 98 v roce 1998 a posléze Windows ME (Millennium Edition), vydaná k příležitosti nového tisíciletí v roce 2000, což byla i poslední verze této řady.

I přes podporu 32bitových aplikací zůstaly některé části operačního systému 16bitové, což vedlo k nestabilitě systému, který mohl být snadno ohrožen nesprávně fungujícím programem.

2.1.2 32bitové operační systémy

V roce 1993 byla představena nová řada operačních systémů firmy Microsoft, která byla založena na plně 32bitovém jádře NT (New Technology). Tato architektura je založena na architektuře OS/2. Prvním zástupcem byla Windows NT 3.1. Windows NT převzala úspěch nového grafického vzhledu z Windows 95. Dále následovala Windows 2000 vydaná v roce 2000, Windows XP vydaná roku 2001, Windows Server 2003 vydaná v roce 2003 a Windows Vista pro výrobce vydaná na konci roku 2006, pro uživatele až v roce 2007.

2.1.3 64bitové operační systémy

První 64bitovou verzí pro procesory Intel byla po dlouhých odkladech Windows XP vydaná v roce 2005. Windows NT existovala také ve verzi určené pro procesory Alpha, ale tyto 64bitové procesory byly přepnuty do 32bitového režimu, což vedlo k degradaci výkonu.

Windows Vista jsou v dnešní době dostupná v 32bitových i v 64bitových verzích.

2.2 Rozdělení operačních systémů Windows podle verzí

Následně je možné operační systémy firmy Microsoft rozčlenit podle časového hlediska na jednotlivé verze systému Windows.

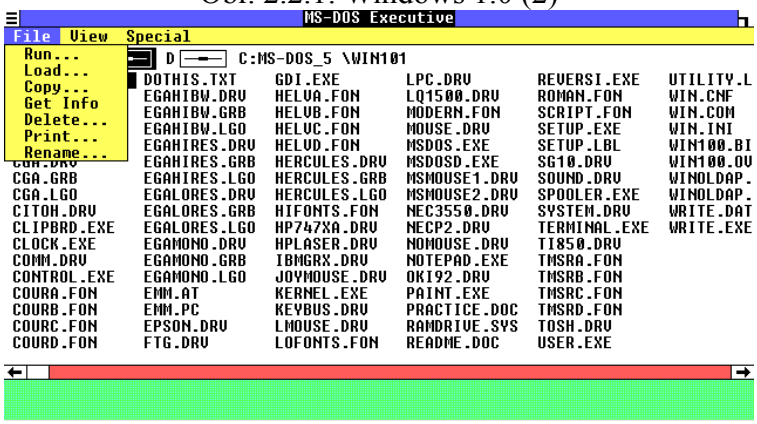
2.2.1 MS-DOS

Prvním operačním systémem firmy Microsoft byl MS-DOS. Tento operační systém byl uveden společně s osobními počítači firmy IBM v roce 1981. Tento systém umožňoval pracovat pouze jednomu uživateli, který mohl v mít současně spuštěn pouze jeden program. MS-DOS byl 16 bitový, podporoval maximálně 640 kB paměti a dovedl pracovat s pevnými disky do kapacity 30 MB. Práce v tomto systému nebyla příliš pohodlná.

2.2.2 Windows 1.0

První verze Windows spatřila světlo světa v roce 1985. Tehdy se jednalo o verzi 1.0. Operační systém Windows napravil většinu nedostatků systému MS-DOS. Windows zavedl multitasking, bylo umožněno uživateli přepínat se mezi běžícími úlohami (v systému MS-DOS bylo nutné pro spuštění jiného programu ukončit běžící program). Okna však nebylo možné překrývat. Na obrázku 2.2.1 je zachyceno pracovní prostředí operačního systému Windows 1.0.

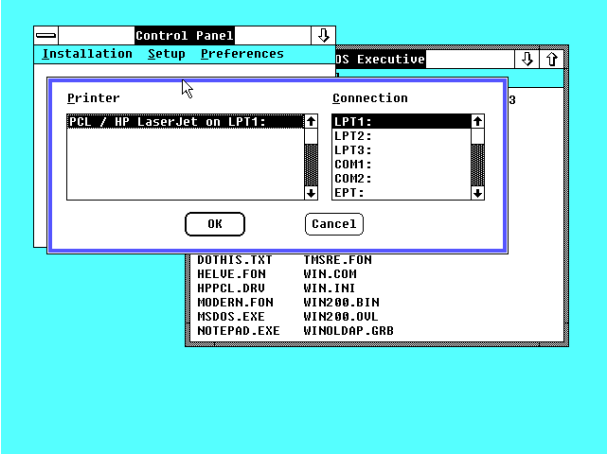
Obr. 2.2.1: Windows 1.0 (2)



2.2.3 Windows 2.0

Windows verze 2.0 byla vydaná v roce 1987. V těchto Windows již bylo možné překrývat okna a nebylo nutné je mozaikově skládat vedle sebe, jak tomu bylo ve verzi 1.0. V prosinci roku 1987 pak byla uvedena Windows 2.0 verze 386, která byla optimalizována tehdy pro nejnovější čip firmy Intel. Na obrázku 2.2.2 je zachyceno pracovní prostředí operačního systému Windows 2.0.

Obr. 2.2.2: Windows 1.0 (2)

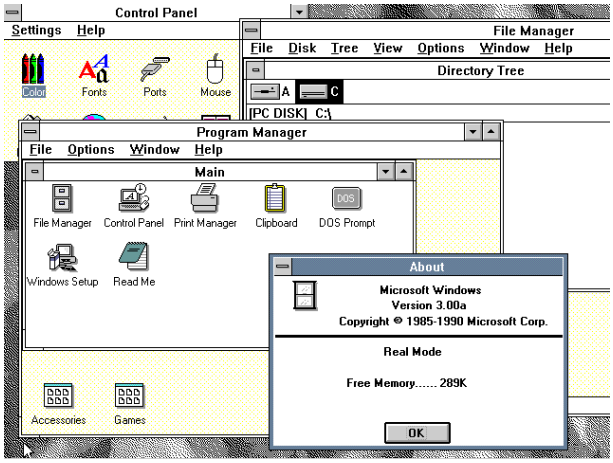


2.2.4 Windows verze 3.0

Windows verze 3.0 se v roce 1990 velmi rychle rozšířila především díky předinstalovávání na nová PC. Tato Windows s sebou přinesla novinky jako je vylepšené grafické prostředí (16ti bitové barevné prostředí), virtuální paměť, tři módy operací (real, standard, 386 enhanced), stromový správce souborů, nebo běh Windows v chráněném módu 386.

O rok později byla vydána rozšířená verze Multimedia Extension, která vylepšila práci systému s multimédii. Tato Windows vyžadovala instalaci na počítač, ve kterém byla nainstalována VGA karta, CD-ROM, 2tlačítková myš a zvuková karta. Na obrázku 2.2.3 je zachyceno pracovní prostředí operačního systému Windows 3.0.

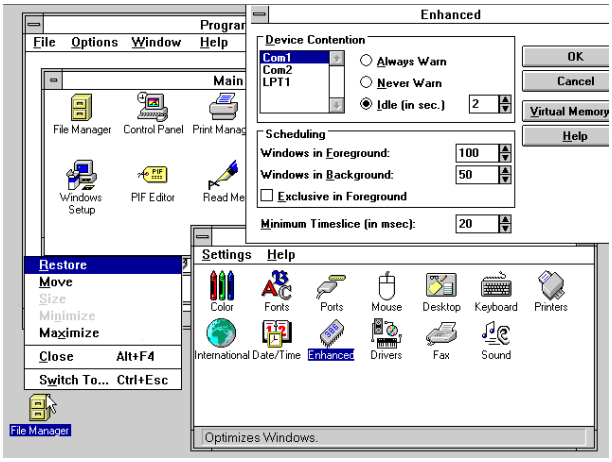
Obr. 2.2.3: Windows 3.0 (2)



2.2.5 Windows 3.11 for Workgroups

Verze 3.11 for Workgroups byla vydána v roce 1993 a byla první verzí Windows s podporou Peer-to-Peer sítě. Tato Windows umožňovala snadné sdílení souborů v síti a obsahovala první program Microsoft Mail, díky čemuž bylo možné používat elektronickou poštu. Tuto verzi již firma Microsoft kompletně lokalizovala do češtiny. Na obrázku 2.2.4 je zachyceno pracovní prostředí operačního systému Windows 3.11.

Obr. 2.2.4: Windows 3.11 (2)



2.2.6 Windows NT 3.1

V roce 1993 přichází také první plně 32bitový systém, který na vnější pohled vypadá stejně jako Windows 3.1. Windows NT vznikla ze systému OS/2, který původně Microsoft vyvíjel společně s firmou IBM. Později však spolupráce obou firem zkrachovala a obě firmy začaly vyvíjet svůj systém zvlášť.

Windows NT 3.1 byla prvním operačním systémem, který byl vyvíjen ve dvou verzích, ve verzi pro pracovní stanice (verze Workstation) a ve verzi pro servery (Advanced Server). Tato verze Windows přinesla podporu více procesorů, integrovanou podporu sítě a souborový systém NTFS. Na obrázku 2.2.5 je zachyceno pracovní prostředí operačního systému Windows NT 3.1.

Obr. 2.2.5: Windows NT 3.1 (2)

2.2.7 Windows 95

Roku 1995 byla na trh uvedena Windows 95. Windows 95 je první systém firmy Microsoft, který nevyžadoval předchozí instalaci systému MS-DOS. Tento systém byl opatřen řadou vylepšení jakými byly například částečně 32-bitové jádro, podpora dlouhých názvů souborů, vylepšená podpora sítě a zcela nové grafické rozhraní. Objevila se také podpora technologie Plug & Play.

V roce 1996 přichází firma Microsoft s novou verzí operačního systému Windows 95. Tato verze nese označení Windows 95 OSR2 a přidává ke své předchozí verzi podporu nového souborového systému FAT 32.

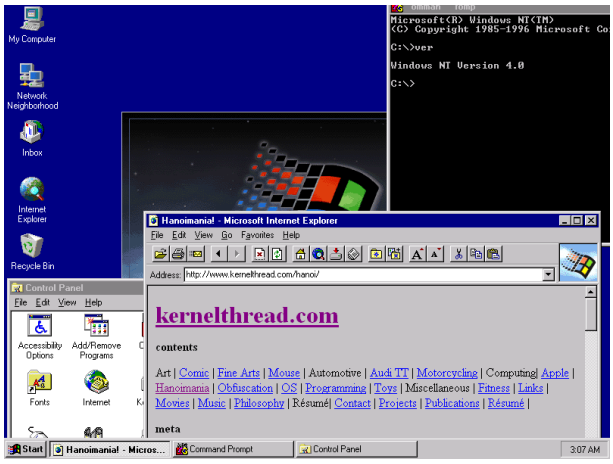
Windows 95 se ve své době začala používat jako herní platforma především díky rozhraní DirectX. Na obrázku 2.2.6 je zachyceno pracovní prostředí operačního systému Windows 98.

Obr. 2.2.6: Windows 98 (2)

2.2.8 Windows NT 4.0

Grafické uživatelské rozhraní Windows 95 bylo tak úspěšné, že se jej Microsoft rozhodl využít i v nové verzi Windows NT 4.0, která přišla na trh v roce 1996. Grafické rozhraní však bylo jediné co měly tyto operační systémy společné. Windows NT se prosadil především v podnikovém prostředí díky své robustnosti oproti Windows 95 a zejména pro své bohaté síťové služby. Na obrázku 2.2.7 je zachyceno pracovní prostředí operačního systému Windows NT 4.0.

Obr. 2.2.7: Windows NT 4.0 (2)



2.2.9 Windows 98

Roku 1998 byla na trh uvedena nová verze Windows s označením Windows 98. Tato Windows vycházela z operačního systému Windows 95. Tato Windows, oproti dřívějším verzím, podporují DVD mechaniky, USB zařízení, rozhraní AGP, rozhraní FireWire a práci s více monitory. Přímo v systému je zahrnut Internet Explorer 4.0.

V roce 1999 byla vydána vylepšená verze operačního systému Windows 98 s názvem Windows 98 Second Edition. Vylepšen byl především Internet Explorer, který byl aktualizován na verzi 5.0, do systému bylo začleněno rozhraní DirectX 6.1 a přibyla možnost sdílení připojení k internetu. Integrovány byly taktéž opravy pro přechod na rok 2000. Na obrázku 2.2.8 je zachyceno pracovní prostředí operačního systému Windows 98.

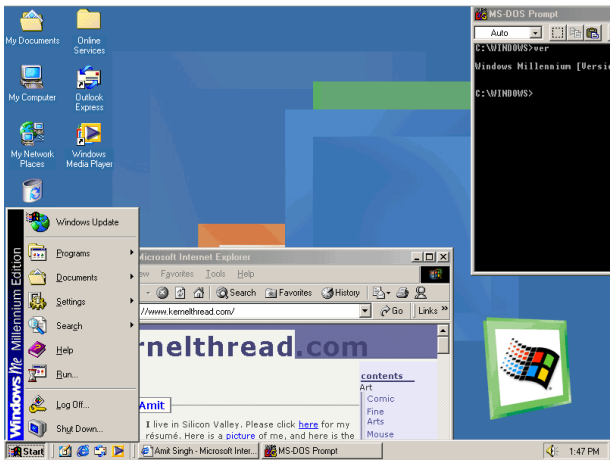
Obr. 2.2.8: Windows 98 (2)

2.2.10 Windows ME

V roce 2000 Microsoft nabídl poslední operační systém vycházející z Windows 95 pod označením Windows Millennium Edition (Windows ME). Ke změnám patřilo zamaskování MS-DOSu a System Restore pro obnovu poškozených systémových souborů. Nově byl do systému začleněn Movie Maker a Media Player 7.

Verze Windows ME se setkala se značnou kritikou uživatelů pro svou nespolehlivost. Přestože jsou Windows ME vydaná později než Windows 98 SE, obecně se doporučuje využití spíše verze Windows 98 SE. Windows ME již dalšího nástupce nemají. Na obrázku 2.2.9 je zachyceno pracovní prostředí operačního systému Windows ME.

Obr. 2.2.9: Windows ME (2)



2.2.11 Windows 2000

Windows 2000 byla uvedena v roce 2000. Tato Windows jsou nástupcem Windows NT 4.0. Tento operační systém je založen na jádru Windows NT, obohaceném uživatelským rozhraním z Windows 9x. Jádro typu NT je obecně stabilnější než jádro, které používala Windows 98, protože je založeno na architektuře OS/2, které je plně 32bitové.

Ve Windows 2000 jsou také mnohé úspěšné nástroje, které se objevily již ve Windows 98 a ME. Jedná se například o nástroj Automatické Aktualizace, Outlook Express, sdílení internetových připojení, Windows Media Player a další. V tomto operačním systému je zahrnut Internet Explorer 5. V grafickém prostředí přibylo dynamické skrývání méně často používaných položek menu pod šipku v jeho spodní části.

Windows 2000 podporují souborový systém NTFS ve verzi 3.0, který je vylepšen, oproti starší verzi, o podporu kvót. Kvótu je možné aplikovat na diskový oddíl, nelze aplikovat na složku, ale i přesto je možné systémovými prostředky vymezit uživateli maximální využitelné místo na disku. Představena byla také funkce spánku.

Stabilita systému se zvýšila používáním pouze ovladačů schválených laboratořemi firmy Microsoft. Havárii systému totiž ve starších verzích Windows často způsobil právě chybný ovladač. Microsoft zavedl novou metodu Windows File Protection k ochránění kriticky důležitých systémových souborů proti smazání a tím zabraňuje závažnému poškození celého systému.

Windows 2000 obsahují podporu pro moderní hardware jako jsou rozhraní Firewire, IrDa porty, porty USB, bezdrátové sítě a další, nabízejí lepší integraci do podnikových sítí, Vzdálenou Plochu, podporu VPN a řadu dalších vylepšení.

Windows 2000 byla vydávána ve čtyřech verzích a to Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server a Windows 2000 Datacenter Server.

Windows 2000 Professional je nástupcem Windows NT 4.0 workstation. Tento systém je určený pro pracovní stanice, podporuje 2 procesory a dokáže využít 4 GB operační paměti.

Windows 2000 Server je nástupcem Windows NT 4.0 Server a podporuje maximálně 2 procesory a 4 GB paměti. Operační systém Windows NT 4.0 Server však podporoval maxi-

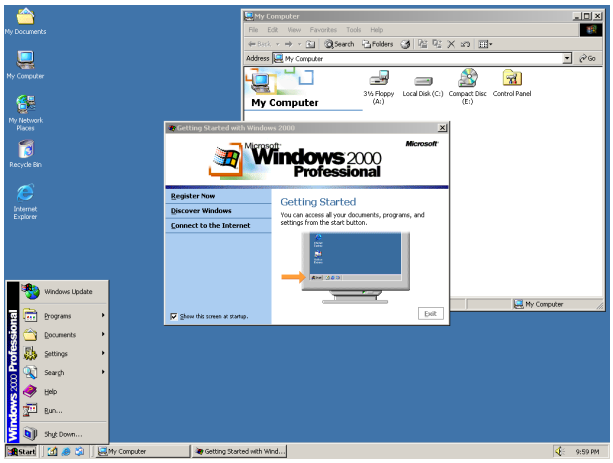
málně 4 procesory a proto je k dispozici upgrade, který do systému přidá podporu pro využívání 4 procesorů. Na tomto systému je možné zprovoznit službu Terminal Services, která dokáže zpřístupnit aplikace Windows formou „tenkých klientů“ ostatním počítačům.

Windows 2000 Advanced Server je serverem pro kritické aplikace. Na rozdíl od Windows 2000 Serveru podporuje 4 procesory a až 64 GB operační paměti. Disponuje navíc skupinou aplikačních služeb zajišťujících dostupnost serveru a vyvažování zátěže.

Windows 2000 Datacenter Server je vyspělejší verzí Windows 2000 Advanced Serveru a je určen především pro velmi velké společnosti. Oproti Advanced Serveru nabízí navíc dvě věci: podporu až pro 32 procesorů a dokonalejší klastrování.

Windows 2000 jsou i v dnešní době používána nezanedbatelným počtem uživatelů i přesto, že podpora tohoto systému ze strany firmy Microsoft byla ukončena v roce 2005 a od té doby běží již pouze prodloužená doba podpory do roku 2010, ve které bude Microsoft vydávat pouze kritické bezpečnostní záplaty a ostatní chyby zůstanou nepokryté. Na obrázku 2.2.10 je zachyceno pracovní prostředí operačního systému Windows 2000.

Obr. 2.2.10 Windows 2000 (3)



2.2.12 Windows XP

Windows XP je rodina operačních systémů firmy Microsoft vyvinutá pro použití na osobních počítačích, pro domácnosti a pro použití ve firmách. Vydána byla také edice se zaměřením na multimédia. Zkratka XP znamená eXPerience, což v češtině znamená zážitek. Windows XP jsou nástupcem Windows 2000 a zároveň Windows ME a tím se staly prvním operačním systémem firmy Microsoft založené na jádře NT určené pro použití na osobních počítačích. Windows XP byla vydána v roce 2001 a okamžitě se rozšířila mezi uživatele.

Nejrozšířenější varianta Windows XP je Windows XP Home Edition, která je určena uživatelům v domácnostech a Windows XP Professional, která je obohacena o funkce Windows Server Domain, podporuje dva fyzické procesory a je určena pro použití ve firmách.

Windows XP Media Center Edition má navíc funkce zaměřená na multimédia jako je podpora pro sledování televize na počítači a nahrávání filmů, sledování DVD filmů a poslech hudby.

Windows XP vyšla také ve dvou oddělených 64bitových verzích a to Windows XP 64-bit Edition pro procesory Itanium IA-64 a Windows XP Professional x64 Edition pro procesory architektury x86-64.

Windows XP mají zlepšenou stabilitu a grafické uživatelské prostředí. Zlepšena byla práce s DLL knihovnami a jejich rozmístění na pevném disku počítače. V dřívějších verzích Windows byl tento nedostatek znám pod názvem „DLL hell“ v češtině peklo dynamických knihoven.

Windows XP představila několik nových funkcí, které se ve dřívějších verzích operačního systému Windows neobjevily. Mezi ty nejvýznamnější patří rychlejší start a hibernace systému, vylepšená práce s ovladači, nové, uživatelsky příjemnější grafické rozhraní s podporou motivů, rychlé přepínání uživatelů, které umožňuje uživatelům uložit rozpracovaný stav a umožňuje přihlášení jiného uživatele bez nutnosti ukončit své běžící aplikace, vyhlazování písma, které zlepšuje čitelnost textů na LCD monitorech, vzdálená plocha, která umožňuje uživatelům se přihlásit přes síť, nebo přes internet a používat své aplikace, soubory, tiskárny a jiná zařízení, podpora pro většinu DSL modemů, bezdrátových karet a také možnosti vytvořit síť pomocí rozhraní FireWire nebo Bluetooth.

Servisní balíček **Service pack 1** pro Windows XP byl vydán v roce 2002. Obsahuje opravy bezpečnostních chyb, aktualizace a volitelnou podporu pro nové rozhraní .NET Framework. Nejvýznamnější vylepšení je zavedení podpory pro USB 2.0. Uživatelé systému si také mohou zvolit výchozí aplikaci pro prohlížení internetu, instantní messaging, výchozí klient pro elektronickou poštu a podobně.

Servisní balíček **Service pack 2** byl vydán v roce 2004. Na rozdíl od předchozích servisních balíčků přidal do Windows XP zásadně nové funkce. Mezi nejvýznamnější patří Windows Firewall, zlepšená podpora Wifi karet, možnost použití šifrování bezdrátové sítě po-

mocí WPA, možnost blokovat vyskakovací Pop-up okna v Internet Exploreru 6 a podporu pro rozhraní Bluetooth. Service Pack 2 také viditelně zrychlil start systému a zavedl do Windows XP podporu NX bitu, který je využíván moderními procesory k ochraně paměti proti přetečení zásobníku. Service Pack 2 přidal do systému Windows XP nástroj Centrum Zabezpečení, díky kterému je možné centrálně řídit bezpečnost systému. Centrum Zabezpečení dovede řídit antivirový program, Windows Firewall a nástroj Automatické aktualizace.

Windows XP jsou často kritizována pro výskyt chyb a také pro integraci Microsoft Internet Exploreru 6 a Windows Media Playeru.

Windows XP je v současnosti mezi uživateli velmi oblíbeným operačním systémem a je mezi nimi hojně rozšířen. Společnost Microsoft se však chystá ukončit podporu tohoto operačního systému díky jeho následníku Windows Vista. Na obrázku 2.2.11 je zachyceno pracovní prostředí operačního systému Windows XP.

Obr. 2.2.11: Windows XP (4)

2.2.13 Windows Server 2003

V roce 2003 byl představený operační systém Windows Server 2003. Jedná se o čistě serverový produkt, který není dostupný ve verzi pro osobní počítače a k jeho vlastnostem patří zejména propracovanější bezpečnost, lepší robustnost a správa systémů. Windows Server 2003 je základem pro celou další rodinu serverových produktů Microsoftu.

2.2.14 Windows Vista

V letošním roce, v roce 2008 byla vydána zatím poslední verze operačního systému Windows, Windows Vista.

K nejvýznamnějším vylepšením proti předchozím verzím systému je přechod k modularitě. Windows Vista nyní používají architekturu která k jádru připojuje moduly. Taková architektura je velmi výhodná protože umožňuje snadno vytvořit několik různě vybavených verzí systému. Tato architektura má také vliv na výkon, protože v momentu kdy není nějaký modul potřeba, je možné jej odpojit a tím šetřit systémovými prostředky.

Dalším příkladem kdy může být tato vlastnost s výhodou použita je práce s aktualizacemi. V dobách Windows XP byly vydávány záplaty v anglické verzi a lokalizované verze bývaly vydávány později. Ve Windows Vista jsou záplaty nezávislé na lokalizaci, lokalizace je také ve zvláštním modulu, tudíž je vydána pouze jedna verze záplaty a celý proces opravení kritické chyby je tím podstatně zrychlen.

Dalším vylepšením je Platforma WinFX, neboli .NET Framework 3.0, která je novější verzí .NET Framework 2.0. Jedná se o rozhraní pro podporu aplikací.

Windows Vista mají některé nové bezpečnostní metody. První z nich je UAC[1]. UAC slouží k přiřazování práv spouštějící se aplikaci nebo programu. Každá aplikace je standardně spouštěna v módu LPS[2], kdy smí pracovat pouze s uživatelem dříve definovanými částmi systému. Pokud chce zasáhnout do části systému, do které v rámci LPS módu nemá přístup, je nutné aby jí uživatel přidělil práva. Pokud se tak stane v účtu běžného uživatele, je pouze informován o tom že k úkonu nemá dostatečná práva[3], pokud se tak stane v účtu administrátora, je uživatel dotázán, zda dovolí aplikaci přepnout do privilegovaného režimu, ve kterém má přístup do celého systému.

Další dvě, ve Windows zcela nové, technologie Compatibility Redirector a Virtual Store slouží také ke zlepšení bezpečnosti celého operačního systému. Technologie Virtual Store představuje virtuální adresářovou strukturu, do kterého jsou ukládány soubory, které by měly být zapsány do systémových adresářů jako jsou Program Files nebo adresář Windows. Pokud se program pokouší zapsat data do registrů, do složek Program Files, nebo do složky

1 UAC (User Account Controll).
2 LPS (Low Privilege Service, nízkoprivilegovaný mód).
3 Typickým příkladem je instalace programu.

Windows, má v režimu Low Privilege Service přístup pouze k Virtual Store. Technologie Compatibility Redirector zajistí to že program o tomto přesměrování neví. Každý uživatel má v rámci svého účtu vlastní Virtual Store.

Významné zlepšení bezpečnosti ve Windows Vista bylo dosaženo technologií Protected Mode v Internet Explorer 7. Toto zlepšení spočívá především v zákazu zápisu do důležitých systémových struktur pro webové stránky. toto omezení se týká v první řadě prvků ActiveX, které doposud měly přístup v podstatě k celému systému. Internet Explorer má v protected mode omezená práva, nezávisle na tom, zda je Internet Explorer povýšen do privilegovaného módu, či nikoli a může zapisovat pouze do definovaných bezpečných částí disku.

Mezi další nové možnosti systému Windows Vista patří například technologie Bit Locker sloužící k šifrovaní dat na pevném disku, zlepšený Windows Firewall, který již monitoruje a filtruje také příchozí pokusy o připojení, Windows Vista taktéž dokáže podle práv uživatele zacházet s výměnnými paměťovými médii, jako jsou flash disky.

Ve Windows Vista se objevuje zcela přepracované grafické rozhraní, označované názvem Aero. Toto grafické prostředí obsahuje některá grafická lákadla jako průhlednost oken a nabídek, trojrozměrné animace, hezčí ikonky přizpůsobené i vyšším rozlišením apod.

Nevýhodou tohoto nového systému může být vyšší spotřeba elektrické energie, což má na noteboocích za následek kratší dobu výdrže baterie.

Bohužel, ve Windows Vista chybí několik stěžejních technologií, které byly slíbeny firmou Microsoft, například systém souborů WinFS, který by zefektivnil vyhledávání.

Windows Vista má velmi líbivé uživatelské rozhraní, které si jistě i v budoucnu oblíbí mnoho uživatelů počítače. Kromě pěkného vzhledu je ze strany firmy Microsoft kladen důraz na bezpečnost a Windows Vista mají díky své přepracované architektuře nadějné vyhlídky být bezpečnější než sví předchůdci. Na obrázku 2.2.12 je zachyceno pracovní prostředí operačního systému Windows Vista.

Obr. 2.2.12: Windows Vista (5)

2.2.15 Windows Server 2008

Windows Server 2008 vyl vydán v roce 2008 a je nejnovějším zástupcem operačních systému pro servery společnosti Microsoft. Windows Server 2008 je nástupcem operačního systému Windows Server 2003, který vyšel před pěti lety. Tento operační systém je založen na stejném jádru jako Windows Vista, na jádru využívajícím technologii NT.

Windows Server 2008 umožňuje práci bez grafického uživatelského rozhraní, umožňuje být konfigurován a spravován přes příkazovou řádku PowerShell, zlepšena byla také bezpečnost systému.

3 ŠKODLIVÉ PROGRAMY

Se stále se rozvíjejícím světem počítačů, počítačových sítí a internetu se rozvíjí i jeho „podsvětí“. Na škodlivý programový kód dnes můžeme narazit na každém kroku.

Podle typu můžeme škodlivé počítačové programy rozdělit do několika skupin.

3.1 Malware

Jako Malware bývají souhrnně označovány škodlivé programy jako jsou například počítačové viry, trojské koně, spyware a adware. Výraz malware vznikl složením anglických

slov „malicious“, s českým významem „zákeřný“ a „software“. Malware je někdy nazýván jako počítačová nečistota.

3.2 Počítačový virus

Jako virus se v oblasti počítačové bezpečnosti označuje program, který se dokáže sám šířit bez vědomí uživatele. Pro své množení se samovolně vkládá do jiných spustitelných souborů či dokumentů. Jeho chování je podobné chování biologického viru, který se šíří vkládáním svého kódu do živých buněk hostitelského organismu. Pro tuto podobnost se někdy procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel.

Vir se šíří přenosem hostitele (například infikovaného dokumentu, nebo spustitelného souboru) na jiný počítač.

3.3 Počítačový červ

Počítačový červ je zvláštním typem počítačového viru. Šíří se v podobě infikovaných souborů nebo paketů počítačové sítě. Infikovaný systém červ využije k odeslání své kopie na další systémy v síti Internet a velmi rychle se tak rozšiřuje. Na rozdíl od počítačového viru se počítačový červ šíří i prostřednictvím sítě.

Zajímavostí je že původně byly vyvíjeny užitečné počítačové červy. Například rodina červů Nachi zkoušela stáhnout a instalovat záplaty z webu Microsoftu. V dnešní době však páchají počítačoví červi převážně škodlivou činnost.

3.4 Trojský kůň

Trojský kůň je skrytá součást užitečného programu. Název Trojský kůň pochází z antického příběhu o dobytí Tróje. Program na pozadí tajně provádí kromě užitečné činnosti další činnost a pravidlem bývá, že je tato činnost uživateli škodlivá.

Trojský kůň může být samostatný program – například hra, spořič obrazovky nebo nějaký jednoduchý nástroj. Někdy se trojský kůň vydává za program k odstraňování malware (dokonce jako takový může fungovat a odstraňovat konkurenční malware). Tato funkčnost slouží ale pouze jako maskování záškodnické činnosti, kterou v sobě trojský kůň ukrývá.

Trojské koně se často vyskytují v software staženém z nedůvěryhodného zdroje. Uživatel tak může získat pozměněnou kopii aplikace obsahující část programového kódu trojského koně dodaného třetí stranou.

Trojský kůň sice nedokáže sám infikovat další počítače nebo programy svojí kopií, ale existují však počítačoví červi, kteří na napadeném počítači instalují trojské koně nebo vytvářejí trojské koně z programů, které se v napadeném systému nacházejí.

3.5 Spyware

Spyware je program, který využívá internetu k odesílání dat z počítače bez vědomí uživatele. Velmi často jsou takovýmto způsobem odesílány informace o internetových stránkách, které uživatel navštívil a o programech, které má v počítači nainstalované.

Takto získané informace jsou často využity pro cílenou reklamu. Spyware ale dokáže odeslat i hesla a přihlašovací údaje k nejrůznějším službám jako je například emailový účtet, nebo čísla kreditních karet.

Přítomnost spyware v počítači můžeme poznat například změněnou domovskou stránkou. Velice často spyware zpomalí start počítače a nabíhání internetu. Při surfování na internetu se mohou ve zvýšené míře zobrazovat reklamy.

3.6 Adware

Adware je program zobrazující reklamu na napadeném počítači. Nejčastěji je reklama zobrazována ve formě banerů, vyskakujících Pop-up oken nebo ikon v oznamovací oblasti. Adware také mění domovskou stránku webového prohlížeče aniž by si to uživatel přál.

Adware bývá šířen jako součást freewarových a sharewarových programů. Adware, na rozdíl od spyware, se do počítače instaluje se souhlasem uživatele.

3.7 Rootkit

Rootkit je program, který se snaží zamaskovat vlastní přítomnost, nebo přítomnost jiných programů, v počítači. Rootkity slouží především k ukrývání souborů, maskování změn v registrech, v procesech, nebo k maskování zvýšené síťové aktivity.

Následkem jejich působení v systému není přítomnost zákeřného software odhalitelná běžně dostupnými systémovými prostředky.

3.8 Škodlivý počítačový program budoucnosti

Škodlivé počítačové programy procházejí stálým vývojem. Jejich tvůrci bývají o krok před autory antivirových programů a záplat závažných programových chyb.

Škodlivé počítačové programy budoucnosti budou muset být jiné, než ty dnešní. Hlavní odlišnost bude spočívat ve schopnosti přežít v různorodém prostředí. V dnešním světě počítačů převládají počítače s jedním operačním systémem, ale s rostoucím počtem mobilních zařízení bude tohoto faktu ubývat. Škodlivé počítačové programy se budou muset s tímto faktem vypořádat. Nebudou se již moci šířit jednoduchou cestou jako doposud.

Nejdříve se nejspíše setkáme se škodlivým programem zaměřeným na jeden konkrétní druh zařízení. Dopad takového druhu viru bude jen omezený.

Další možnou formou může být škodlivý program s centralizovanou databází. Takový program si stáhne odpovídající kód pro cílovou platformu, ovšem centralizovaná databáze představuje zranitelné místo škodlivého programu tohoto typu.

Velký potenciál s sebou nesou Peer-to-peer sítě a proto můžou být dalším krokem ve vývoji škodlivých počítačových programů komplexní programy s chováním Peer-to-peer sítí. Program vybere oběť a podle konfigurace cílového systému najde v síti svou kopii pro tuto platformu.

Vyloučit nemůžeme ani použití umělé inteligence a využití obrovského výpočetního potenciálu distribuované sítě.

4 NEJBĚŽNĚJŠÍ METODY A DOPADY POČÍTAČOVÝCH ÚTOKŮ

Počítačové útoky se stále častěji stávají noční můrou správců podnikových i malých sítí, administrátorů malých stanic i domácích uživatelů. Od dob kdy se využívají počítače téměř všude a ke všemu, narůstá i počet počítačových útočníků. Počítačoví útočníci chtějí nad počítačem získat kontrolu, získat z něj informace a později jej využít ke svému účelu. Ne-

zabezpečený a zastaralý systém pro ně bývá snadnou kořistí. Především je třeba brát na vědomí že útočníci zkouší stále nové fígle, jak počítač ovládnout.

4.1 Využití bezpečnostní mezery operačního systému díky špatné konfiguraci

Špatně nakonfigurovaný systém se špatně zabezpečenými službami může být velmi snadno úspěšně napaden nejběžnějšími metodami počítačových útoků. Jedná se především o konfiguraci v oblasti správy uživatelů a správy zón, ze kterých bude služba dostupná.

4.1.1 Uhodnutí slabého hesla

Protože pro vstup do systému a pro přístup ke službám mnohdy stačí znalost uživatelského jména a hesla, je nutností volit heslo v souladu se zásadami tvorby bezpečného hesla a uchovávat jej v tajnosti. Zásady tvorby bezpečného a silného hesla jsou popsány v kapitole 5.1.3.

Kvalitu hesla je možné ověřit například na internetové adrese: http://securitystats.com/tools/password.php. Po zadání hesla je ohodnocena jeho bezpečnost.

Nyní bude poukázáno na nutnost volit silné heslo pomocí slovníkového útoku na FTP server. K útoku bude použit program Brutus, který je možné stáhnout na internetové adrese: http://www.hoobie.net/brutus/brutus-download.html.

Specializované slovníky pro použití k útoku jsou k dispozici ke stažení na internetu. Jako slovník je také možné použít například soubor slov překladového slovníku, nebo slovník sloužící ke kontrole pravopisu v textovém editoru, či v emailovém klientu.

Program Brutus byl nastaven tak aby načetl soubor s uživatelskými jmény, kterými se bude snažit přihlásit a také soubor s hesly, která bude zadávat. Na FTP serveru je vytvořen uživatel „user“ a má nastaveno heslo „princess“.

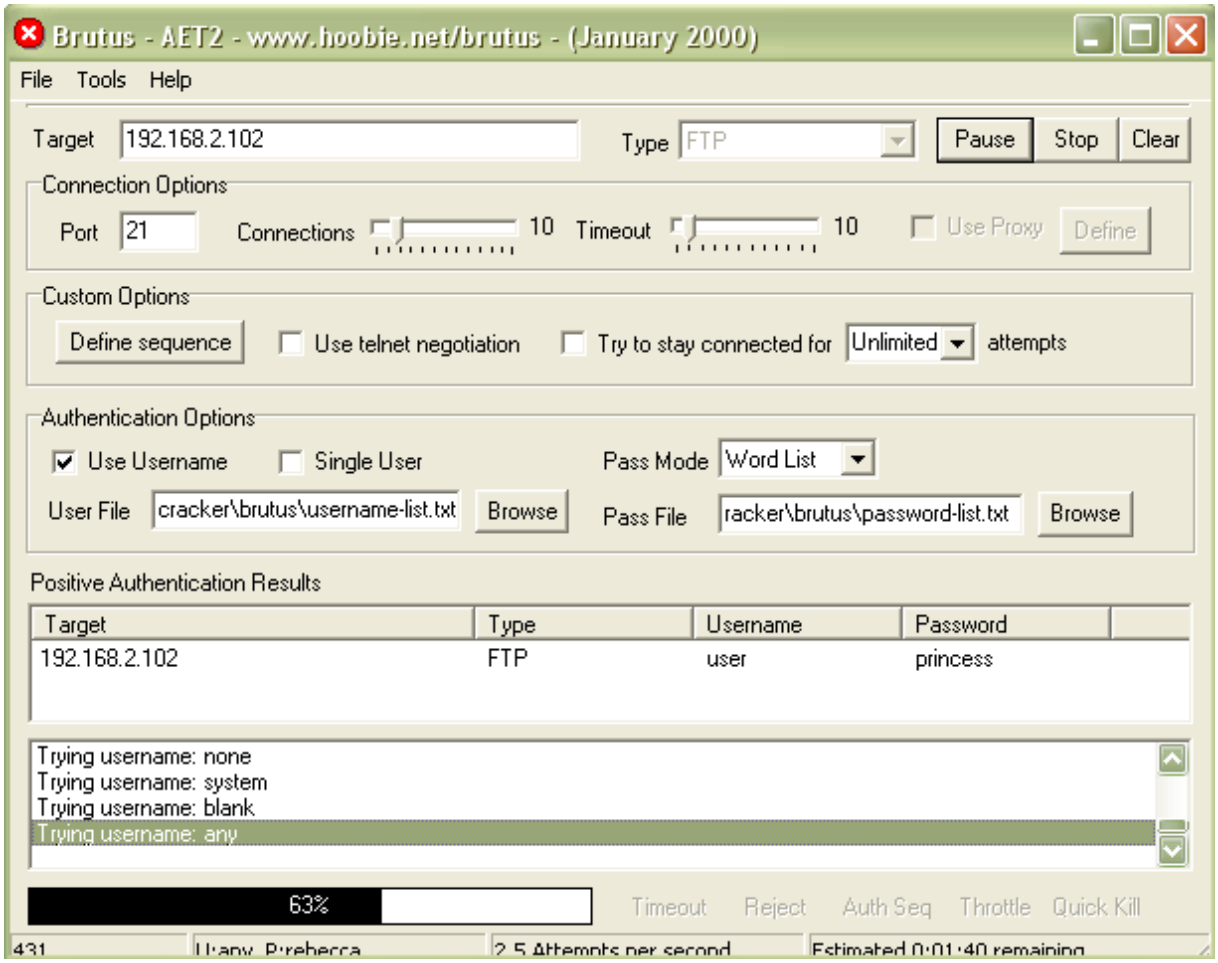
V konfiguraci FTP serveru byl úmyslně vytvořen uživatel user, který se přihlašuje heslem princess, protože takové uživatelské jméno s jednoslovným heslem v angličtině se často ve slovnících vyskytuje. Pokud by bylo zvoleno složitější heslo, které se ve slovnících nevyskytuje, bylo by k jeho uhodnutí nutné použít útoku hrubou silou, nebo alespoň kombinaci útoků hrubou silou a slovníkového útoku.

Nevýhodou metod hádání hesla hrubou silou a slovníkovým útokem je fakt že přihlašování uživatelů je ve většině případů logováno a tento útok je v logu patrný na první pohled. Druhou nevýhodou je dlouhá doba trvání tohoto útoku, která může být o to větší když se server před tímto útokem chrání tím že po určitém počtu neúspěšných pokusů o přihlášení na nějakou dobu zablokuje přihlašování uživatele. Další pokusy je možné zkusit po uplynutí této doby.

Používáním kvalitního hesla nelze zabránit jeho uhodnutí, ale silné heslo může proces hádání ztížit tak, že je prakticky nemožné jej uhodnout.

Na obrázku 4.1.1 je zobrazen program Brutus, který již uhodl uživatelské jméno a jemu odpovídající heslo.

Obr. 4.1.1: Program Brutus



4.1.2 Ledabyle ponechaný nezabezpečený účet, spuštěná nezabezpečená služba

Protože uživatel s uživatelským účtem typu administrátor má přístup ke všem systémovým prostředkům, může spravovat systém, smí přistupovat do registrů, libovolně zapisovat a mazat data z disku a odesílat a přijímat data přes internet, je velmi důležité, aby byl opatřen bezpečným heslem. Pokud je heslo snadno uhodnutelné, nebo dokonce prázdné, je možné že se běžný uživatel přihlásí na počítač pomocí tohoto účtu a bude moci spravovat systém.

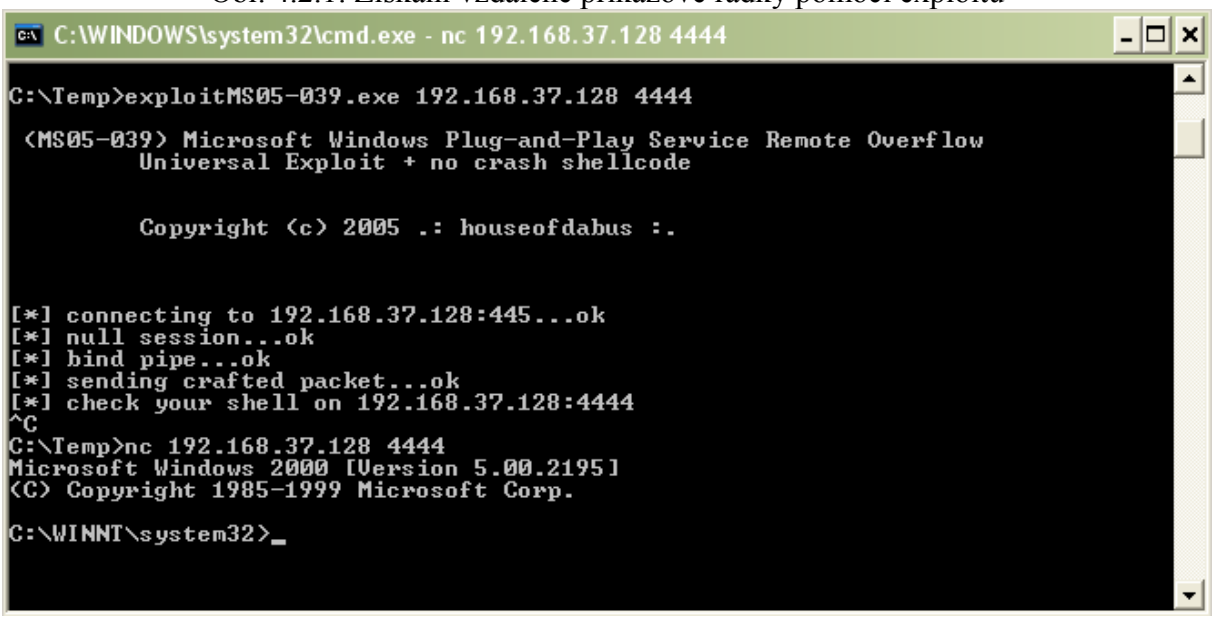
4.2 Využití programové chyby

V operačních systémech se často objevují programové chyby, které je třeba záplatovat dříve, než jsou zneužity. Záplaty vydává vydavatel operačního systému, aplikuje je správce operačního systému. Programové chyby se vyskytují také v nainstalovaných programech a službách a tyto chyby je také možné zneužít.

Jako demonstrace nutnosti včas systém a programy záplatovat, bude předveden ukázkový útok na operační systém Windows 2000 SP4 ve výchozím nastavení pomocí exploitu. Exploit je krátký program který využívá chyby programu. Tento exploit využívá přetečení zásobníku ve službě Plug and Play. Tato chyba je označena kódem MS05-039 a její zneužití umožňuje vykonání jakéhokoliv kódu, v tomto případě získání vzdáleného příkazového řádku s právy administrátora. Podrobný popis chyby je zveřejněn v článku (14), zdrojový kód exploitu pochází z článku (13).

Zdrojový kód exploitu lze zkompilovat do spustitelné podoby v Microsoft Visual Studiu ve Windows. Exploit vyžaduje jako parametr IP adresu počítače, na kterém běží operační systém Windows 2000 SP4 a číslo portu, na který je nutné se připojit k získání vzdáleného příkazového řádku.

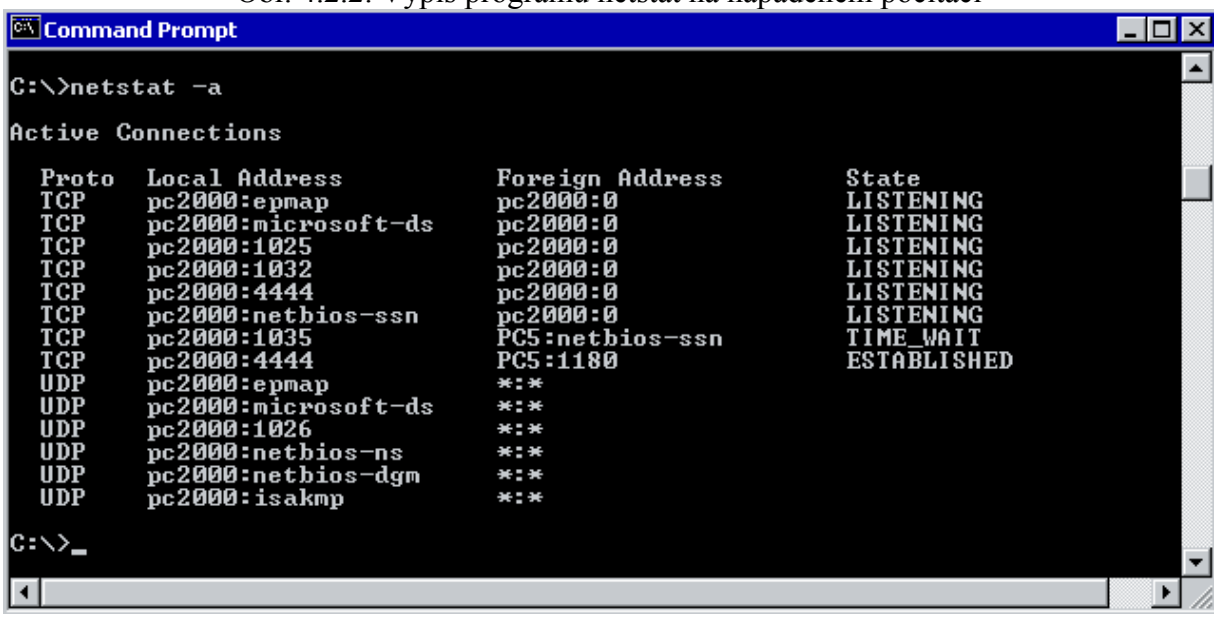
Obr. 4.2.1: Získání vzdálené příkazové řádky pomocí exploitu



Na obrázku 4.2.1 je příkazová řádka spuštěná na počítači, ze kterého je ověřována náchylnost systému Windows 2000 SP4 na chybu MS05-039. Počítač, na kterém je spuštěn operační systém Windows 2000 SP4 má IP adresu 192.168.37.128. Programem exploitMS05-039.exe byla využita bezpečnostní chyba a napadený systém naslouchá na portu 4444 a čeká na připojení na tento port aby navázal spojení. K tomuto účelu byl použit program NetCat. Stejně tak mohl být použit například program Telnet, který je běžnou součástí Windows.

Na napadeném počítači se ve Správci programů Windows objevil nový proces cmd.exe reprezentující vzdálenou příkazovou řádku. Dále, jak je vidět na obrázku 4.2.2, ve výpise programu NetStat se objevilo navázané spojení s počítačem útočníka pc5 na portu 4444.

Obr. 4.2.2: Výpis programu netstat na napadeném počítači



Nyní má útočník k dispozici vzdálený příkazový řádek s administrátorskými právy a tím získal neomezenou moc nad napadeným počítačem. Do počítače je přenesen program NetCat a jsou jím vytvořena zadní vrátka do systému. K přenesení je použito protokolu TFTP[4]. Pomocí TFTP protokolu je možné přenášet soubory mezi počítači pomocí počítačové sítě. Jedná se v podstatě o odlehčenou variantu protokolu FTP obsahující pouze jeho nejnutnější části. TFTP klient je standardní součástí Windows.

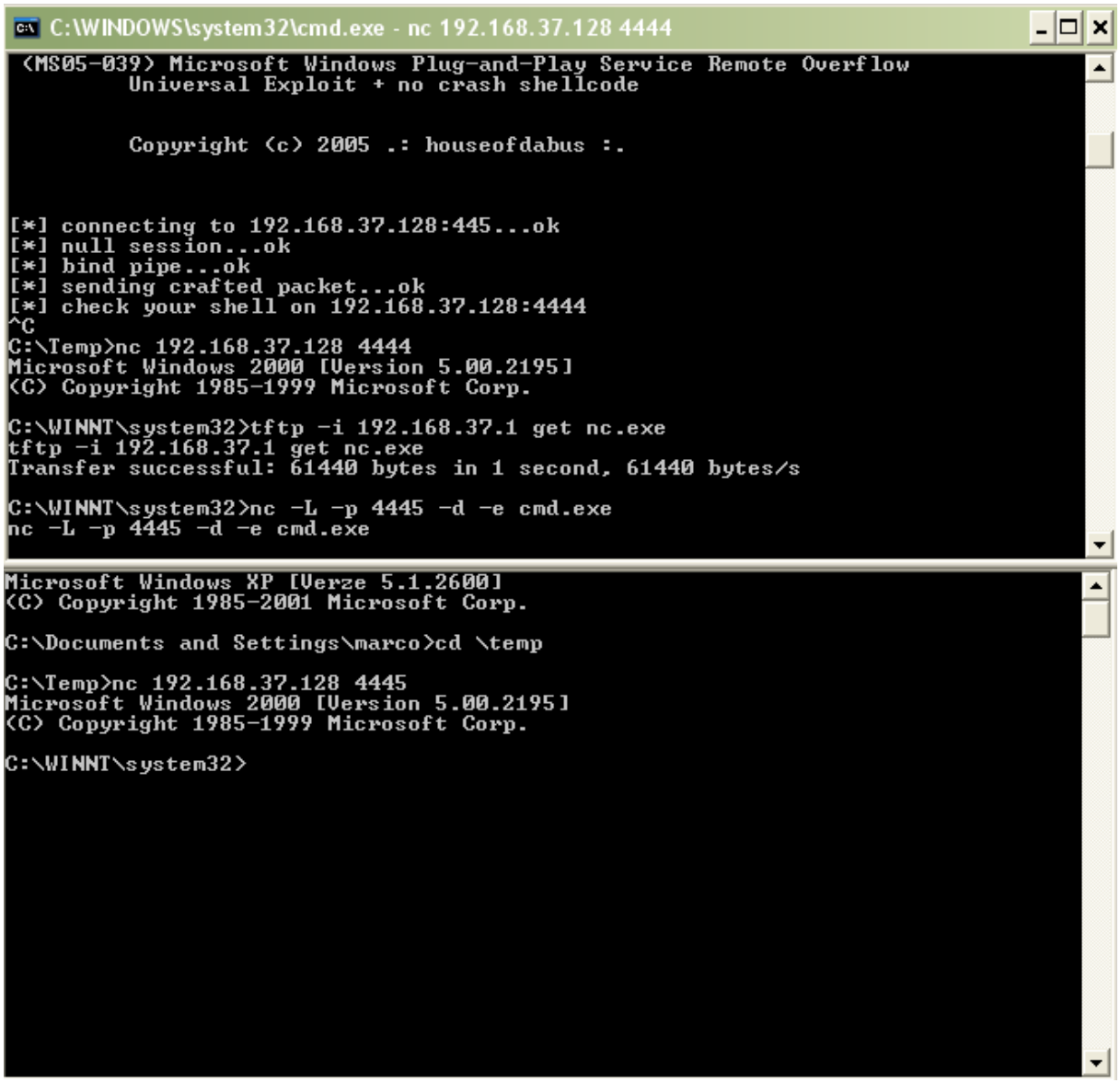
Na počítači útočníka je spuštěn jednoduchý TFTP server pomocí programu SolarWinds TFTP Server. Tento TFTP server je freeware a lze jej získat na internetové adrese http://www.solarwinds.com/downloads/.

Pomocí vzdálené příkazové řádky je spuštěn TFTP klient na napadeném počítači a s pomocí tohoto klientu je napadený počítač připojen k počítači útočníka, aby bylo možné přenést potřebné soubory z útočícího počítače na napadený. Na obrázku 4.2.3 je možné vidět přenos souboru na napadený počítač. V témže obrázku je na dalším řádku program NetCat spuštěn na napadeném počítači v režimu zadních vrátek.

Podobným způsobem by bylo možné na napadeném počítači například vytvářet a mazat uživatelské účty, měnit uživatelská hesla, přidávat, odebírat a konfigurovat služby, nebo mazat soubory.

4 TFTP (Trivial File Transfer Protocol).

Obr. 4.2.3: Přenos programu na napadený počítač pomocí protokolu TFTP



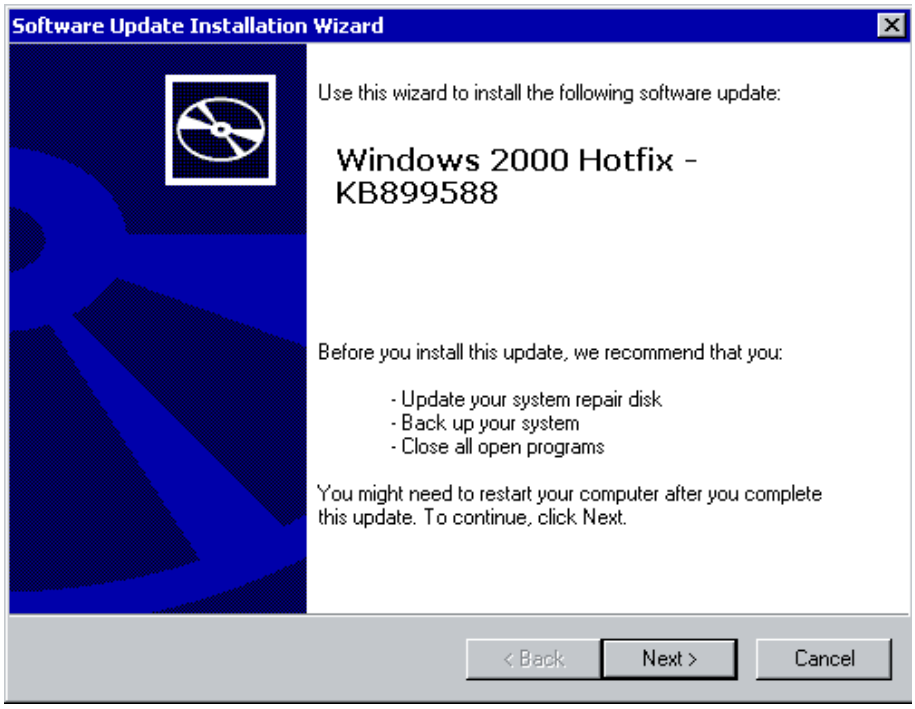
Předvedeno bylo jak je nesmírně důležité udržovat operační systém aktuální a jak katastrofální důsledky může mít zanedbání péče o operační systém.

Podobných exploitů je na internetu mnoho. Psaní exploitů je velmi důležité pro upozornění na možné zneužití závažných bezpečnostních mezer v operačních systémech a pro uspíšení jejich nápravy. Včasnou aplikací záplat je možné podobným útokům předejít.

Na systém bude aplikována záplata Windows2000-KB899588-x86-ENU.EXE, která byla vydaná pro opravu bezpečnostní chyby MS05-039. Záplata je pro Windows 2000 SP4 k dispozici ke stažení na internetové adrese: http://www.Microsoft.com/downloads/details.aspx?

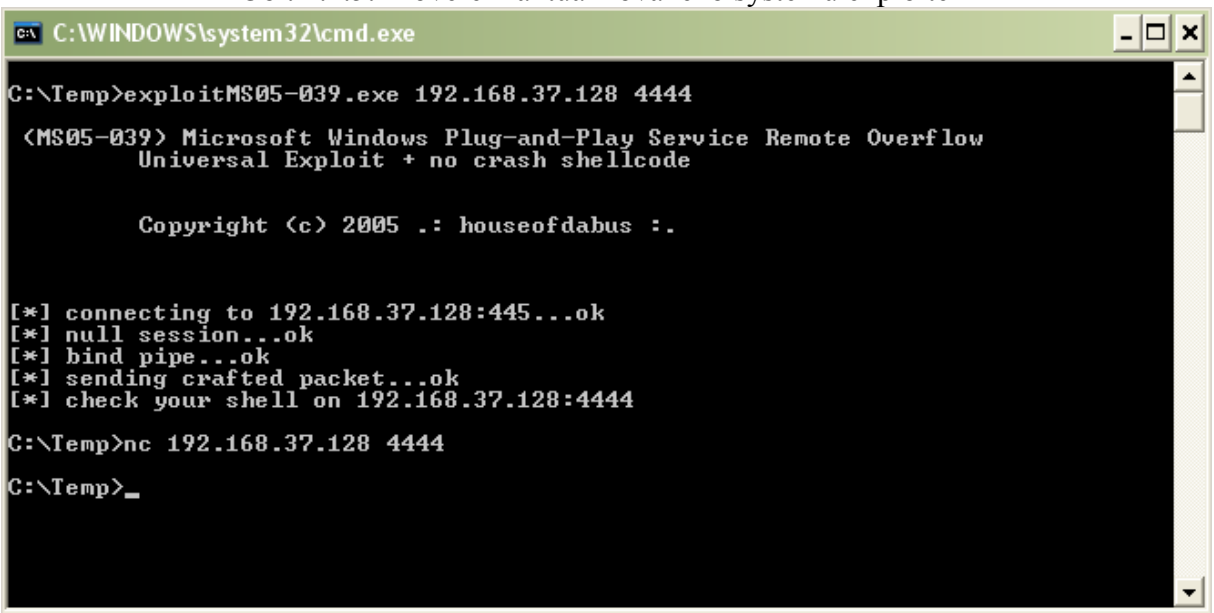
FamilyId=E39A3D96-1C37-47D2-82EF-0AC89905C88F&displaylang=en. Na obrázku 4.2.4 je zobrazena instalace záplaty.

Obr. 4.2.4: Aplikace záplaty



Po úspěšné aplikaci záplaty je znovu ověřena bezpečnost systému Windows 2000 SP4 shodným postupem jako před aplikací záplaty. Protože po vykonání exploitu na portu 4444 systém nenaslouchá, program NetCat se na tento port nedovedl připojit a ukončil se, jak je vidět na obrázku 4.2.5.

Obr. 4.2.5: Prověření aktualizovaného systému exploitem



Důsledky zneužití programové chyby můžou být různé, nemusí se bezpodmínečně jednat o ideální získání vzdáleného příkazového řádku. Takové důsledky mohou být například získání práv administrátora nestandardní cestou, přístup k citlivým datům, vyřazení služby mimo provoz a podobně.

4.2.1 Princip exploitu přetečením zásobníku

Exploit je program, který využije chybu programu ke změně chování tohoto programu. Výsledkem je že se program začne chovat jinak než by se choval, kdyby k programové chybě nedošlo. Exploit je typicky zaměřen na vykonání cizího kódu, který do původního programu vůbec nepatří. Může se jednat například o spuštění příkazové řádky. Taková varianta je velmi výhodná, protože příkazový řádek umožňuje zadávání dalších příkazů.

Zásobník je struktura programu nacházející se v operační paměti a je využívána při volání funkcí. Přetečení zásobníku je chyba programu. Typickým příkladem této chyby může být například zápis do bufferu o pevně definované velikosti. Pokud při tomto zápisu nejsou kontrolovány hranice bufferu, může tato chyba nastat pokud je objem zapisovaných dat větší, než je kapacita bufferu.

Pokud je v programu volána funkce, na zásobník jsou uloženy její parametry, návratová adresa funkce a její lokální proměnné. Pokud jsou uvnitř funkce například kopírovány řetězce, nebo načítán řetězec z uživatelského vstupu, nebo ze souboru, načítaný řetězec může přetéct a přepsat tak data následující na zásobníku, nejprve všechny lokální proměnné funkce a potom i návratovou adresu funkce. Po ukončení funkce program pokračuje programovým kódem právě na této adrese. Tím je možné docílit vykonání jiného programového kódu než by se vykonal kdyby k přetečení řetězce nedošlo.

Pokud jsou na zásobník cíleně zapsána data, která způsobí smysluplné přepsání hodnoty adresy návratové funkce, je možné s jistotou určit kam se program po opuštění funkce vrátí a kde bude ve své činnosti pokračovat.

Hodnoty, které je třeba na zásobník zapsat jsou do jisté míry velmi blízké nízkoúrovňovému programování v assembleru. Proto je funkčnost exploitu často velmi závislá na operačním systému a na architektuře procesoru. To dává exploitům charakter jednoúčelovosti.

4.3 DoS – odmítnutí služby

Specifickým důsledkem, kterého může útočník chtít dosáhnout, je takzvaný DoS[5]. Následkem úspěšného útoku je nedostupnost služby jejím běžným uživatelům. DoS je někdy nekalou praktikou konkurenčního boje mezi společnostmi, kdy může například vyřazení internetového obchodu z funkce být velkou ztrátou.

Odmítnutí služby lze dosáhnout několika způsoby – vyčerpáním kapacity linky, vyčerpáním systémových zdrojů, nebo zneužitím chyby v programu (28).

Útok, který má za následek vyčerpání kapacity linky je možné uskutečnit takovým množstvím požadavků, na které již průchodnost linky nestačí a žádné další požadavky již nemohou být zpracovávány. Pro tento typ útoku se hojně používá DDoS[6], který bývá silnější než DoS, protože na systém útočí několik různých ovládnutých počítačů naráz.

Útok metodou vyčerpání systémových zdrojů může obsazovat například procesorový čas, operační paměť, nebo diskový prostor. Následek tohoto útoku je ten že napadenému systému chybí systémové zdroje k tomu, aby mohl uspokojivě obsluhovat své běžné uživatele.

Útok metodou zneužití chyby programu způsobí že se služba zhroutí a přestane být dostupná svým běžným uživatelům.

5 BEZPEČNOST OPERAČNÍHO SYSTÉMU

Dobrá bezpečnost operačního systému je podmínkou pro to aby se systém nestal nebezpečný pro samotné uživatele počítače. Dobře zabezpečený systém vyžaduje pravidelnou a důkladnou údržbu. Operační systém vyžaduje péči administrátora, potřebuje být záplatovaný, aktualizovaný a v neposlední řadě také správně zkonfigurovaný. Patřičnou pozornost a péči vyžadují taktéž v systému nainstalované programy a služby.

Největší péči však vyžadují uživatelé počítače. Počítač by měli užívat poučení uživatelé, protože největší hrozbou každého operačního systému bývají právě oni samotní. Uživatele je třeba pravidelně školit o dodržování alespoň těch nejzákladnějších bezpečnostních zásad.

Deset univerzálně použitelných bezpečnostních pravidel doporučených firmou Microsoft při příležitosti akce Štít bezpečí (15):

5 DoS (Denial of Service, Odmítnutí služby).
6 DDoS (Distributed DoS, Distribuovaný DoS).

1. pravidelně aktualizujte operační systém,
2. používejte antivirový program a pravidelně jej aktualizujte,
3. chraňte své připojení firewallem,
4. nesnižujte základní bezpečnostní nastavení systému Windows,
5. přistupujte pouze k důvěryhodným webovým stránkám,
6. neinstalujte neověřené nebo nevyzkoušené aplikace,
7. před potvrzením volby prostudujte, co potvrzujete,
8. nereagujte na nevyžádané emailové zprávy,
9. neotevírejte nevyžádané nebo neznámé přílohy e-mailů,
10. v případě potíží kontaktujte odbornou pomoc.

5.1 Konfigurace systému

Po instalaci systému Windows je systém nakonfigurován tak, aby vyhovoval co největšímu počtu zákazníků a proto jsou spuštěny některé služby které v té dané situaci nebudou používány a některé jiné potřebné spuštěné nejsou.

5.1.1 Eliminace spuštěných procesů a služeb

Každý spuštěný program a služba je potenciálním rizikem k tomu aby byl zneužit, nebo v něm byla objevena nějaká závažná chyba, pomocí které může útočník získat systém pod svou kontrolu, proto je velice výhodné spouštět pouze potřebné a ověřené programy a služby.

Správce úloh systému Windows umí zobrazit mimo jiné seznam spuštěných procesů a je standardní součástí systému. Lze jej vyvolat stiskem klávesové zkraty CTRL+ALT+DELETE a po přepnutí na záložku procesy se objeví zmiňovaný seznam běžících procesů. Ve standardním nastavení zobrazuje o každém spuštěném procesu název procesu, uživatelské jméno uživatele, který jej spustil, množství procesorového času, který aktuálně využívá v procentech a množství paměti, které mu bylo přiděleno. Tímto nástrojem je možné měnit prioritu běžících procesů, ukončovat je a spouštět nové procesy.

Alternativou k rozšířeným funkcím Správce úloh systému Windows může být například program Process Explorer. Process Explorer zobrazuje procesy ve stromové struktuře a ve vlastnostech každého procesu dokáže zobrazit velmi podrobné informace o běžícím procesu, například umístění exe souboru na pevném disku, seznam DLL knihoven které proces

používá a programová vlákna, která proces vytvořil. Program Process Explorer lze stáhnout na internetové adrese http://technet.Microsoft.com/cs-cz/sysinternals/bb896653(en-us).aspx.

Nebezpečnost podezřelých procesů lze ověřit například na internetové adrese http://www.processlibrary.com/directory/. Jedná se o internetovou stránku tématicky zaměřenou na informace o procesech systému Windows.

Služby systému Windows lze spravovat pomocí nástroje s názvem Služby, který je standardní součástí Windows. Lze jej spustit kliknutím na tlačítko Start, dále na položku Spustit a do okénka napsat příkaz „services.msc“. Služby je možné spouštět, restartovat, pozastavovat a ukončovat. Lze také nastavit kdy se má služba spustit. Možná nastavení jsou spustit službu automaticky při startu systému, spustit ručně a zákaz spouštění služby.

Program X-RayPc umí zobrazit jak seznam běžících procesů, tak seznam spuštěných služeb. Procesy dokáže spouštět i zastavovat a při zastavení procesu nabídne taktéž možnost vymazat exe soubor procesu z pevného disku. Tento program lze stáhnout na internetové adrese http://www.x-raypc.com/download.php.

5.1.2 Analýza otevřených portů

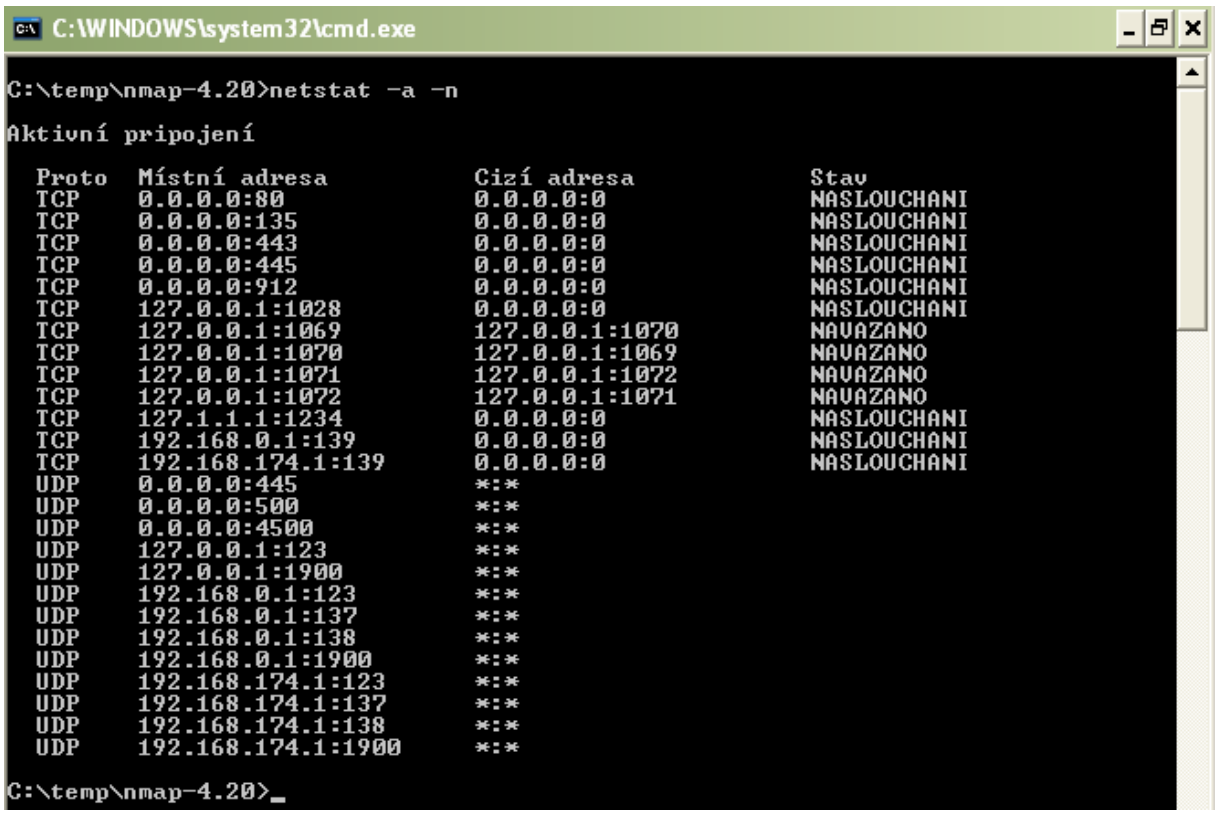
Počítače mezi sebou komunikují pomocí síťových protokolů TCP a UDP. Na těchto protokolech jsou definovány porty. Číslo portu slouží k identifikaci aplikace spuštěné na počítači. Čísla portů mohou být v rozsahu čísel 0 až 65535, z toho je interval 0 až 1023 vyhrazen pro standardní porty (well-known ports), tyto porty jsou většinou pojmenovány podle síťového protokolu, kterým jsou využívána.

Na počítači mohou být porty otevřené například v případě že program port otevřel a právě jej používá k přenosu, nebo na něm naslouchá a čeká na příchozí spojení. Příklad takového programu může být například webový server, který naslouchá na portu http číslo 80. Dalším příkladem je například FTP server, který naslouchá na portu číslo 21. Na portech ale také naslouchají programy backdoor, které tak vytvoří zadní vrátka do systému.

Zadní vrátka je možné odhalit ve výpise otevřených portů systému. K výpisu otevřených portů slouží například program NetStat, který je standardní součástí Windows.

Další metodou sloužící k odhalení programů komunikujících přes síť je skenováním portů. Port scannery dokážou zjistit na kterých portech systém naslouchá. Na základě tohoto výpisu je možné podle čísla portu a povahy odpovědi při připojení na daný port odhadnout jaký program je za naslouchání zodpovědný. Parametr programu NetStat -n zajistí to že ve výpisu se budou čísla portů zobrazovat numericky, a parametr -a zajistí že se ve výpisu objeví všechny otevřené porty.

Obr. 5.1.1: Výpis otevřených portů programem NetStat

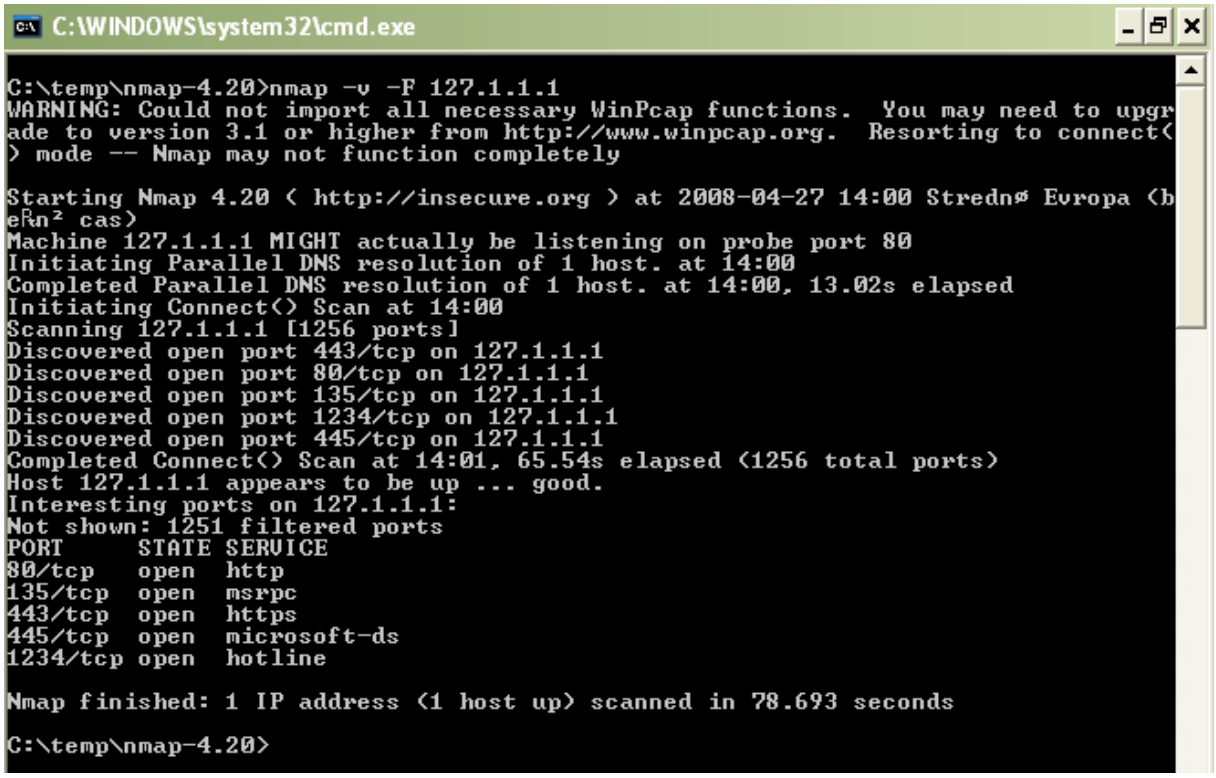


Ve výpise programu NetStat na obrázku 5.1.1 je možné si všimnout otevřeného portu TCP 1234, který je svým číslem více než podezřelý. Tento port nenáleží žádnému názvu z Well Known Names. Navíc je tento port ve stavu naslouchání. Program NetStat je spuštěn ještě jednou, tentokrát navíc s parametrem -k, který ke každému portu zobrazí také jméno exe souboru programu, který port otevřel. Z tohoto výpisu je možné zjistit že port 1234 otevřel program s názvem nc.exe.

Dále je proveden scan portů programem NMap. Přepínač programu NMap -v má vliv na intenzitu skenování a přepínač -F omezí rozsah skenovaných portů pouze na čísla portů, která má NMap nastavená ve svém konfiguračním souboru. Tento přepínač se používá kvůli

urychlení skenovacího testu. Ve výpise na obrázku 5.1.2 je možné vidět že systém naslouchá na portech 80, 135, 443, 445 a 1234.

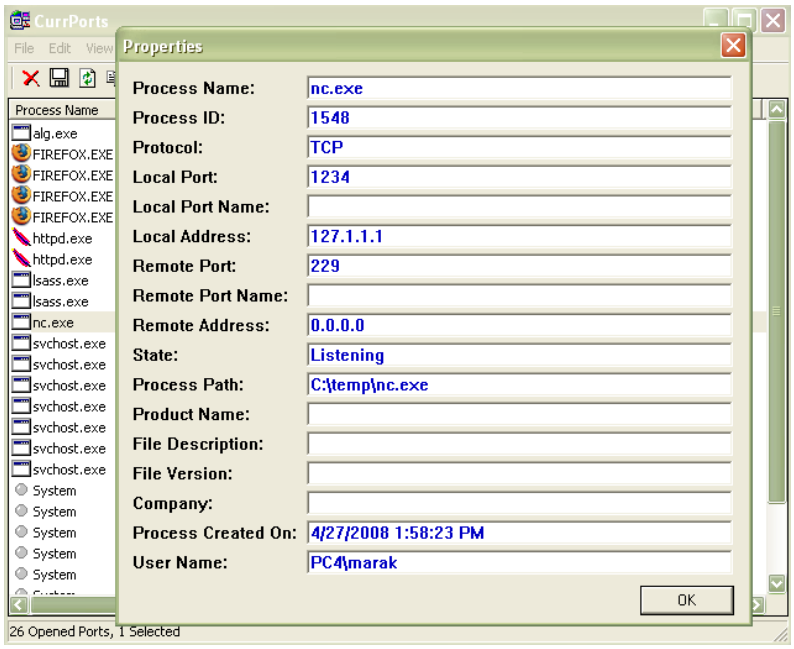
Obr. 5.1.2: Sken portů programem NMap



Je provedeno připojení programem NetCat na port 1234 a tím je získána vzdálená příkazová řádka testovaného systému. Nyní je jisté že v počítači je nainstalován program zprostředkující zadní vrátka do systému.

Nyní je vhodné tento závažný bezpečnostní nedostatek odstranit. Za tímto účelem je možné použít program CurrPorts, který umí zobrazit podrobnější informace o otevřených portech. Program již není konzolovým nástrojem, nýbrž má grafickou nadstavbu v podobě grafického uživatelského rozhraní. Informace o otevřeném portu 1234 je možné vidět na obrázku 5.1.3. Z tohoto výpisu je možné zjistit který program je za otevřený port zodpovědný a navíc také vím ve kterém souboru je tento program uložený.

Obr. 5.1.3: Informace o vybraném otevřeném portu programem CurrPorts



Za tato zadní vrátka je zodpovědný program NetCat v režimu poskytujícím zadní vrátka do systému. Pomocí Správce úloh systému Windows je ukončen proces nc.exe a poté smazán soubor c:\temp\nc.exe. Program CurrPorts je možné stáhnout na internetové adrese http://www.nirsoft.net/utils/cports.html

5.1.3 Zásady tvorby bezpečného hesla

Protože pro přístup ke službám, nebo k systému mnohdy stačí znalost uživatelského jména a hesla, je nutností volit heslo v souladu se zásadami tvorby bezpečného hesla a uchovávat jej v tajnosti.

Zásady tvorby bezpečného hesla:

- Heslo by mělo být co nejdelší.
- Heslo by se mělo skládat z velkých i malých písmen a číslic a by mělo obsahovat i jiné než alfanumerické znaky (` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /).
- Heslo by nemělo být odvoditelné z uživatelského jména.
- Za heslo by nemělo být voleno běžné slovo, jméno, osobní údaje, názvy a varianty těchto slov.

- Heslo by nemělo být tvořeno sekvencí například 123456, nebo abcdef, nebo i například qwerty.

- Za heslo je vhodné zvolit kombinaci více slov, například větu, která je lehce zapamatovatelná, například „raduji-se-z-malickosti“

Kvalitu hesla je možné ověřit například na internetové adrese: http://securitystats.com/tools/password.php. Po zadání hesla je ohodnocena jeho bezpečnost.

5.1.4 Uživatelská práva

Pokud se již nějaký škodlivý program do systému dostane například nepozorností uživatele, je možné eliminovat následky jeho působení alespoň částečně. Pokud se takový program spustí s právy přihlášeného uživatele, jak tomu ve standardních situacích je, je nanejvýš vhodné uživatelská práva omezit na minimum.

Velké škody může v systému způsobit program spuštěný s právy administrátora, protože administrátor má přístup ke všem systémovým prostředkům, může konfigurovat systém, smí přistupovat do registrů, libovolně zapisovat a mazat data z disku a odesílat a přijímat data přes internet.

Windows XP podporují dva základní typy účtů, účet typu běžný uživatel a účet typu administrátor. Oba tyto účty se od sebe liší uživatelskými právy. Mezi nejvýznamnější odlišnosti patří odlišná práva v přístupu k registrům, k souborům, k systémové konfiguraci apod. Uvažujme situaci že neopatrný uživatel stáhne z internetu spustitelný soubor se škodlivým programem a spustí jej.

Pokud takto učiní s právy správce operačního systému, tento program může vykonat svou činnost a není vůbec ničím omezován. Může neomezeně mazat data z disku, může odeslat vybrané soubory pomocí FTP[7], nebo SMTP[8] protokolu, vytvořit zadní vrátka do systému, a do registrů nastavit, aby se program spouštěl se startem systému, může deaktivovat antivirový program a upravit nastavení firewallu apod.

Pokud se však spustí tento program běžný uživatel, nemá přístup k soukromým složkám ostatních uživatelů, nemůže měnit nastavení systému, antivirového programu a fi-

7 FTP (File Transfer Protocol, protokol pro přenos souborů mezi počítač).
8 SMTP (Simple Mail Transfer Protocol, protokol pro odesílání pošty).

rewallu (pokud to antivirový software a firewall nepodporuje). Při správně nakonfigurovaném firewallu nebude neznámému programu povolen přístup na internet.

Uživatelská práva je možné nastavit a později upravovat, přidávat a odebírat jednotlivým uživatelům systému nástrojem Místní uživatelé a skupiny. Tento nástroj je standardní součástí Windows a lze jej spustit kliknutím na tlačítko start, vybrat volbu spustit a do okénka napsat příkaz „lusrmgr.msc“.

Velkým krokem vpřed v zacházení s uživatelskými právy je metoda UAC představená ve Windows Vista. UAC slouží k přiřazování práv spouštějící se aplikaci nebo programu. Metoda UAC je podrobněji popsána v kapitole 2.2.14.

5.2 Prohlížeč událostí Windows

Systém Windows zaznamenává informace o prováděných činnostech do logů. Tyto logy jsou velmi sdílný zdroj informací o dění v systému. Prohlížeč událostí Windows dokáže tyto logy zobrazit.

Prohlížeč událostí Windows lze najít na ploše v kontextovém menu položky Tento počítač. Z místní nabídky je nutné vybrat volbu Spravovat a ve stromové struktuře přejít k prohlížeči událostí. Jiná možnost jak tento nástroj spustit je stiskem tlačítka Start a přejít k příkazu Spustit, v okénku je nutné zadat název příkazu „eventvwr.msc“.

Prohlížeč událostí Windows člení události podle původce události do tří skupin na události týkající se aplikací, události týkající se zabezpečení a systémové události. Ve všech těchto podkategoriích jsou informace o událostech znovu členěny a to podle typu události na informaci, upozornění a chybu.

Protokol aplikací je uložen v souboru AppEvent.Evt. Uchovává události zaznamenané při spouštění, běhu nebo ukončení aplikací. Typ zaznamenávaných událostí určuje vývojář dané aplikace a mohou se u různých aplikací lišit. **Protokol zabezpečení** je uložen v souboru SecEvent.Evt. Uchovává informace o bezpečnostních událostech jako je úspěšné nebo neúspěšné přihlášení k počítači, události při práci se soubory, úspěšný pokus o smazání, či čtení souboru. Výchozí nastavení je takové že systém Windows tento typ událostí nezaznamenává. **Systémový protokol** je uložen v souboru SysEvent.Evt. Tento log je vyhrazen pro

systémové události jakými můžou být například úspěšné i neúspěšné zavedení ovladačů a také systémové chyby.

Informační zpráva informuje o úspěšné události, například při zavedení ovladače, spuštění služby a podobně. **Varování** má funkci upozornění na možný problém. Varování může vyvolat například málo volného místa na pevném disku, nebo změna v konfiguraci. **Hlášení o chybě** vznikne při kritické události v systému. Může být vyvoláno selháním ovladače, hardware, nebo při závažné chybě části systému.

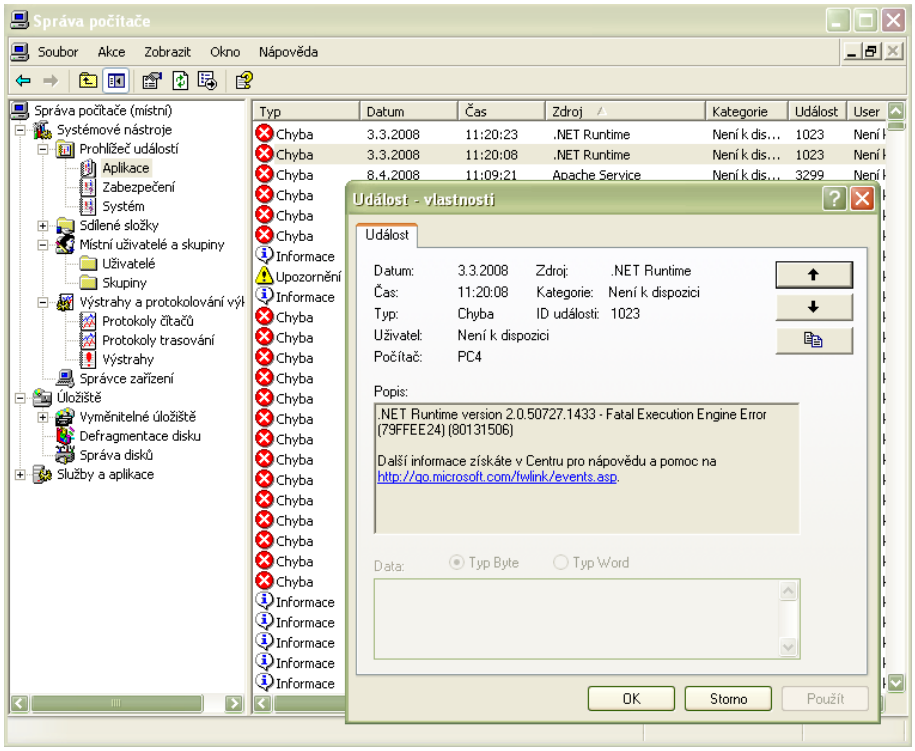
Poklepáním myší na jednotlivé položky lze zobrazit jejich detailnější popis. V nově otevřeném okně se zobrazí datum, čas a typ události, jméno uživatele, který zapříčinil vznik události, název počítače na kterém k události došlo a popis události. V některých případech jsou zobrazena také binární data, které pomáhající vývojářům blíže určit příčinu události.

V Prohlížeči událostí Windows můžeme nastavit logování do jednotlivých souborů. Kliknutím pravého tlačítka myši na protokol lze zvolit z místní nabídky „Vlastnosti“ a objeví se nové okno. V tomto okně je možné zjistit podrobné informace o protokolu a upravovat velikost a způsob záznamu. Maximální velikost protokolu umožňuje určit velikost protokolu souboru. Práce s menšími protokoly je mnohem snadnější a rychlejší (povolené hodnoty jsou od 64kB do 4 194 240 kB). Položka Přepisovat události dle potřeby má za funkci to že při překročení maximální velikosti protokolu budou nejstarší události smazány. Přepisovat události starší x dnů má za funkci to že události starší x dnů budou automaticky mazány. Bohužel při dosažení maximální velikosti protokolu během menšího počtu dní se nezapisují nové události. Volba nepřepisovat události znamená že události nebudou přepisovány a při zobrazení upozornění je administrátor povinen obsah protokolu smazat. Při dosažení maximální hranice nebudou zapisována nová data. Zde je taktéž možné všechny události smazat.

Na další záložce s nápisem „Filtr“ lze filtrovat události zobrazované v hlavním okně. Prohlížeč událostí Windows umožňuje také jednoduché vyhledávání podle identifikátoru události, podle uživatelského jména, nebo podle popisu. Události lze podle těchto polí také třídit. Toto vyhledávání lze nalézt v menu zobrazit, položka najít.

Volbou exportovat seznam lze obsah exportovat do textového souboru a následně například zazálohovat, nebo analyzovat některým automatizovaným nástrojem. Nevýhodou však je ztráta binárních informací u některých zpráv. Na obrázku 5.2.1 je prohlížeč událostí Windows se zobrazeným detailem události.

Obr. 5.2.1: Prohlížeč událostí Windows



Je možné prohlížet log systému Windows také jinými nástroji než Prohlížečem událostí Windows. Příkladem může být například program Event Log Explorer. Funkčnost tohoto programu je možné zdarma zkoušet po dobu 30 dní, poté je potřeba vložit registrační kód. Internetové stránky programu jsou na internetové adrese http://www.eventlogxp.com a program lze zdarma stáhnout na internetové adrese http://www.eventlogxp.com/download/elex.zip.

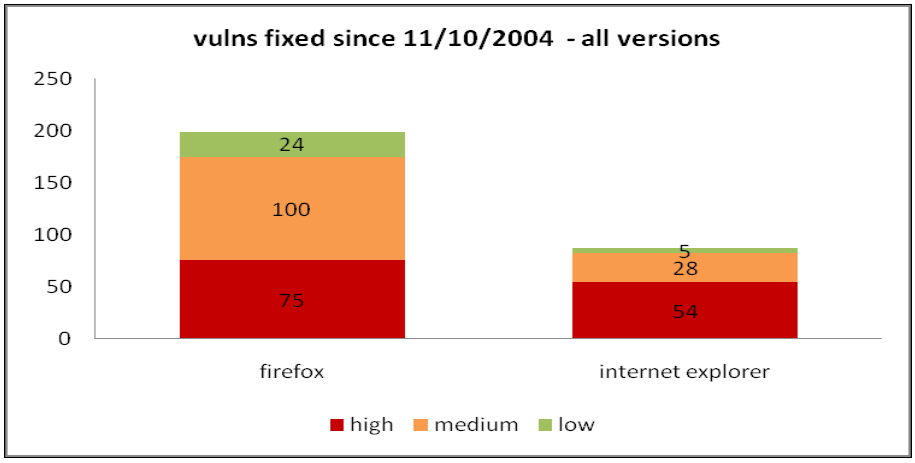
5.3 Výběr bezpečných aplikací

Stejně jako operační systémy obsahují programové chyby, je možné chyby nalézt také v aplikacích. Tyto chyby mohou být zneužity například exploitem. Protože bezpečnost systému není pouze bezpečnost operačního systému, ale závisí taktéž na bezpečnosti aplikací které jsou v tomto operačním systému spouštěny, je výběr aplikací velice důležitá otázka.

Jako příklad uvedu dva nejpopulárnější webové prohlížeče Microsoft Internet Explorer a Mozilla Firefox. Oba tyto prohlížeče mají své zastánce i odpůrce. Prohlížeče se liší ve svých funkcích, rozšiřitelností pomocí pluginů a v neposlední řadě také uživatelským rozhraním. Avšak oba tyto prohlížeče umožňují pohodlně prohlížet web, stahovat obrázky a například sledovat video. Podívejme se na ně nyní z bezpečnostního hlediska.

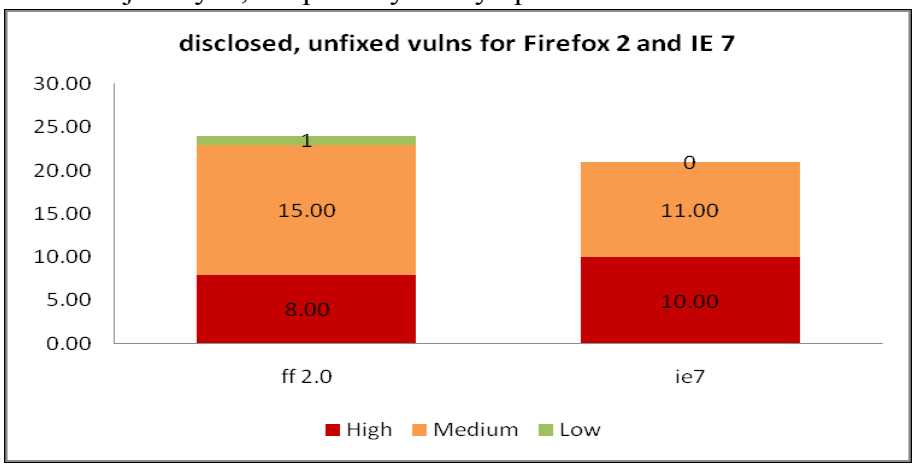
Grafy se týkají období od roku 2004, kdy vyšla první verze prohlížeče Mozilla Firefox 1.0 do roku 2007, kdy byly tyto grafy publikovány.

Obr. 5.3.1: Počet opravených chyb prohlížečů Firefox a Internet Explorer (6)



Na obrázku 5.3.1 je graf. Graf vyjadřuje počet vydaných záplat na bezpečnostní mezery prohlížečů. Pro internetový prohlížeč Firefox bylo celkově vydáno podstatně více záplat než pro Internet Explorer. Ovšem počet záplat na velmi závažné chyby je u obou prohlížečů podobný. Při pohledu na tento graf je třeba brát v úvahu že obě společnosti mohou opravit více chyb v rámci jedné záplaty a Microsoft navíc záplatuje Internet Explorer také v rámci servisních balíčků pro své operační systémy.

Obr. 5.3.2: Počet objevených, neopravených chyb prohlížečů Firefox a Internet Explorer (6)



Na obrázku 5.3.2 je graf. Tento graf pak ukazuje počet objevených chyb, které v době publikace grafu, v roce 2007, nebyly opraveny. Tento graf pro oba prohlížeče ukazuje podobné výsledky.

Podobné šetření je možné provést při výběru emailového klientu, FTP serveru a mnohých dalších programů.

5.4 Programy používané pro zvýšení bezpečnosti

Protože počty škodlivých programů rostou a objevují se stále nové, je třeba vybavit operační systém obrannými programy. Mezi tyto programy patří firewall, antivirový program a program proti spyware.

5.4.1 Firewall

Firewall je prvek, který odděluje sítě za účelem zvýšení bezpečnosti sítě chráněné tímto firewallem. Firewall může být realizován samostatně jako síťový prvek nebo může být nainstalován na počítači firewall softwarový ve formě programu. Hlavní funkcí firewallu je možnost filtrovat síťový provoz. Firewall vyhodnotí zda je síťová komunikace žádoucí či není a na základě pravidel tuto síťovou komunikaci propustí nebo zadrží. Pravidla je možné upravovat, přidávat nová a odebírat ta současná.

V operačním systému Windows XP SP2 a ve Windows Vista je jednoduchý firewall standardní součástí. Tento firewall se jmenuje Brána firewall systému Windows. Mnozí uživatelé si jej oblíbili právě pro jeho jednoduchost. Jeho nedostatkem však je že neumožňuje filtrovat odchozí provoz. Zapnout, vypnout a nastavit tento firewall lze v panelu nástrojů.

Kompletním firewallem může být program ZoneAlarm. Tento program umožňuje filtrovat příchozí i odchozí spojení, ve svém nitru má integrován také antivirový software, antispywarový program a program pro filtrování pošty pro ochranu proti spamu. Tento firewall má také užitečnou funkci filtrování obsahu webu nevhodného pro děti. Sleduje také změny exe souborů, čímž upozorňuje uživatele na skutečnost že v programu může být virus. Samozřejmostí je tvorba logů. Program může automaticky aktualizovat svou virovou databázi přes internet.

ZoneAlarm ve verzi free je k dispozici zdarma pro domácí uživatele a neziskové organizace a je možné jej stáhnout na internetové adrese http://www.zonealarm.com

Dalšími kvalitními firewally jsou například Outpost Firewall Pro, Norman Personal Firewall a za firewally zdarma například Sygate Personal Firewall nebo Sunbelt Kerio Personal Firewall.

5.4.2 Antivirový program

Primární funkce antivirového programu je odhalení a odstranění virů z operačního systému a ochrana před dalšími viry. U programů tohoto typu je důležitá aktuálnost. Tyto programy velmi často mívají také další funkce například pro detekci spyware, rootkitů a ostatních škodlivých programů. Jejich výrobci často nabízejí kompletní řešení, ve kterém jsou zahrnuté programy typu antivir, antispyware a firewall.

Antivirový software BitDefender nabízí automatickou aktualizaci virové databáze z internetu, spolehlivě odhaluje viry, spyware a rootkity. Při hraní her je možné jej přepnout do režimu, který sníží nároky na systém a sníží jeho zatížení. Tento program se také vyskytuje ve variantě kompletního řešení společně s firewallem, ochranou proti spammu, rodičovskou kontrolou pro filtrování obsahu webu nevhodného pro děti, zálohovacím programem a optimalizátorem registrů Windows. Tento program je možné stáhnout na internetové adrese http://www.bitdefender.com/site/Downloads/.

Jiná varianta antivirového řešení je například program AVG. Tento program je z dílny českého výrobce a nabízí rezidentní ochranu před viry, trojskými koni, spyware, nevyžádanou poštou, hackery, rootkity a programy typu exploit. Tento antivirový program je k dispozici také ve variantě kompletního řešení společně s firewallem. Tento program je možné stáhnout na internetové adrese http://www.grisoft.cz.

Další antivirové programy jsou například ESET Nod32, Kapersky, F-Secure, nebo Norton.

5.4.3 Antispywarový program

Hlavní funkcí antispywarových programů je ochrana proti spyware. Většina antivirových programů má v sobě zabudovanou funkci pro detekci a odstranění a prevenci spyware, ale existují i programy zabývající se pouze tímto typem škodlivých programů. Na programy typu antispyware je, stejně jako u programů proti virům, kladen požadavek aktuálnosti.

Prvním z řad těchto programů může být například Spyware Doctor. Je možné jej stáhnout na internetové adrese http://www.pctools.com/spyware-doctor/.

Dalším příkladem může být Windows Defender který pochází z dílny firmy Microsoft a je možné jej používat zdarma. Program je možné stáhnout na internetové adrese http://www.Microsoft.com/cze/athome/security/spyware/software/default.mspx.

Dalšími programy zabývající se touto problematikou můžou být Spy Sweeper, CounterSpy a Ad-Ware Pro.

5.5 Tvorba záloh

Zálohování je činnost jejíž výsledky jsou doceněny teprve v případě, kdy dojde ke ztrátě důležitých dat. Možností, jak přijít o cenná data, je celá řada. Nemusí jít pouze o napadení počítače škodlivým programem, živelnou katastrofu nebo fyzické selhání pevného disku. K poškození dat může vést i obyčejná a všudypřítomná neopatrnost uživatele vlivem lidského faktoru. Pokud se tak stane, je dobré mít možnost obnovit data ze zálohy.

K dispozici je hned celá řada metod tvorby záloh.

Prvním typem zálohování je záloha plná. Plná záloha spočívá v přesné kopii zálohovaných dat, takže pokud je třeba z této zálohy data obnovit, stačí pouze tato záloha. Tento typ záloh bývá předstupněm zálohy inkrementální a diferenciální.

Dalším typem je Inkrementální (přírustková) záloha, která zaznamenává změny vzhledem k nejpozději zálohovanému stavu. Důvodem k použití tohoto typu zálohy může být šetření času a místa potřebné k vytvoření zálohy. Pokud dojde ke ztrátě nebo poškození dat, je třeba nejprve obnovit nejnovější plnou zálohu a poté postupně aplikovat všecky předchozí inkrementální zálohy od nejstarší po nejnovější.

Posledním nejběžnějším typem zálohy je záloha diferenciální. Při tomto typu zálohování jsou vždy zaznamenány změny vzhledem poslední plné záloze. Tento typ záloh je kompromisem mezi plnou a inkrementální zálohou. Pokud dojde k havárii zálohovaných dat, je k jejich úspěšnému obnovení potřeba mít k dispozici nejnovější plnou zálohu a nejnovější diferenciální zálohu.

Čas potřebný k provedení diferenciální zálohy dat je v průměru srovnatelný s časem potřebným k vytvoření zálohy diferenciální (s přihlédnutím k charakteru dat), doba potřebná k obnovení dat však bývá kratší při použití diferenciálního zálohování, protože doba obnovení

dat z inkrementálních záloh narůstá s počtem těchto záloh. Plná záloha bývá nejnáročnější z časového hlediska i z pohledu objemu dat, který je třeba uchovat.

Tyto metody je možné kombinovat v závislosti na charakteru a důležitosti dat. Klasický postup je například každý týden vytvořit plnou zálohu a tu každý den doplnit o zálohu inkrementální.

Některé zálohovací programy pro zálohování využívají příznak archivovat ve vlastnostech souborů a složek. Význam tohoto příznaku je takový že při vytvoření zálohy je tento příznak vymazán. Pokud dojde v souboru ke změně je při příštím zálohovacím procesu znovu zazálohován.

Pro zaručení bezpečnosti dat je nutné vzít v úvahu také fyzické uložení zálohovaných dat a to jak z hlediska čitelnosti média a jeho spolehlivosti, tak z hlediska možného poškození v případě uložení ve stejném prostoru s osobním počítačem například v případě požáru nebo krádeže.

Problematikou zálohování se věnuje mnoho kvalitních specializovaných programů. Mezi možnosti těchto programů patří například podpora základních metod zálohování, možnost ukládat zálohy na pevný disk, na síťové disky, podpora protokolu FTP a SMTP a možnost plánovat čas kdy se proces zálohování spustí. Většina těchto programů podporuje také kompresi a šifrování záloh, které nabývá na důležitosti při zálohování na vzdálený počítač v internetu.

Mezi nejznámější programy pro tvorbu záloh patří Genie Backup Manager 8, který lze stáhnout na internetové stránce http://www.genie-soft.com, nebo program Acronis True Image Home který lze stáhnout na internetové stránce http://www.acronis.com. Dalším příkladem může být program NTI Backup NOW, který je možné stáhnout na internetové adrese http://www.ntius.com.

Speciální nástroj pro zálohování operačního systému Windows se jmenuje **Obnovení systému**. Tento nástroj je standardní součástí Windows Millennium, Windows 2000, Windows XP a Windows Vista. Obnovení systému vytváří takzvané body obnovy, které je možné vytvářet ručně. Tento nástroj je k nalezení v nabídce Start, v položce Všechny programy, pod položkou Příslušenství a dále pod položkou Systémové nástroje a konečně položka Obnovení systému. Toto zdlouhavé hledání lze urychlit stiskem tlačítka Start,

položka Spustit a do okénka napsat příkaz „%systemroot%\system32\restore\rstrui.exe“. K těmto bodům obnovy je možné se později vrátit a obnovit uložený stav systému. Tento nástroj je užitečný v případě že se v systému objeví komplikace.

V operačním systému Windows je zálohovací nástroj pod názvem Zálohování zahrnut jako standardní součást. Tento nástroj umožňuje automatické zálohování vybraných souborů a složek v určený čas. Program dokáže provádět běžné typy záloh a dovede je kopírovat v rámci počítače na pevné disky, ale podporuje taktéž disky síťové.

Zálohování systému obrazem disku se hodí pro zálohu celého systému včetně systémové konfigurace a nainstalovaných programů. To může být potřeba například pro zálohu „čistého“ systému, což v budoucnu usnadní a urychlí reinstalaci systému nebo jako záloha před instalací potenciálně nebezpečného software nebo před závažnou změnou konfigurace. V případě neúspěšné instalace tohoto software stačí obnovit stav systému před instalací.

K takovému účelu existují specializované programy jakým je například Acronis True Image. Tento program umožňuje vytvářet obrazy celých disků, nebo diskových oddílů a uložit je na pevném disku, na síťový disk nebo v podobě fragmentů optimalizovaných pro výměnná média jakým jsou například CD, nebo DVD a tato média ukládat. Program je možné stáhnout na internetové adrese http://www.acronis.com. Dalším programem je Drive Image který je možné stáhnout na internetové adrese http://www.drive-image.com. Problematice vytváření diskových obrazů se věnuje mnoho dalších programů.

5.6 Použití virtuálního počítače

Jedním z mnoha doporučení jak zmírnit dopad napadení počítače škodlivým programem je používat k práci takzvaného virtuálního počítače. Virtuální počítač je program, který umožní spustit na hostitelském operačním systému druhý operační systém. Na virtuální počítač je možné nainstalovat jakýkoliv podporovaný operační systém.

S virtuálním počítačem je možné provádět všechny běžné činnosti jako se skutečným počítačem. S výhodou je možné virtuální počítač použít k běžným činnostem jako je například přístup na internet, nebo pro testování neověřených programů.

Virtuální počítač lze snadno zálohovat a v případě napadení virtualizovaného operačního systému nepřátelským programem lze předchozí stav zpět snadno obnovit ze zálohy.

Výhoda spočívá v tom že hostitelský operační systém, ve kterém je virtuální počítač spuštěn, se vlivem činností prováděných v počítači virtuálním nemůže poškodit.

Mezi nejvýznamnější programy které virtualizaci umožňují patří například VMware s internetovými stránkami na adrese: http://www.vmware.com.

6 ZHODNOCENÍ BEZPEČNOSTI OPERAČNÍCH SYSTÉMŮ

Jedním z hlavních kritérií pro posouzení kvality operačních systémů je jejich bezpečnost. Hlavními hledisky jejího posuzování může být počet odhalených chyb, závažnost odhalených chyb a čas potřebný k vydání záplaty.

6.1 Výskyt chyb ve Windows v časovém horizontu

V příloze A je přiložena skupina šesti grafů. Tyto grafy vyjadřují histogramy výskytu chyb v operačních systémech Windows v období od roku 2003 do roku 2008 s měsíční periodou. Zkoumanými operačními systémy jsou Windows NT 4.0, Windows 98 Second Edition, Windows Millennium, Windows 2000, Windows XP a Windows Vista.

Z grafů vyplývá že ve zkoumaném období byl objeven největší počet chyb v operačních systémech Windows 2000 a Windows XP. Za tyto výsledky může být do jisté míry zodpovědný fakt, že ve zkoumaném období byly nejvíce používané právě tyto dva operační systémy. Z grafů je také patrné v jakém období byla na trh uvedena Windows Vista. Od toho okamžiku se začaly objevovat chyby v tomto operačním systému. Stejně tak s klesající popularitou starších operačních systémů, jakými v těchto grafech jsou Windows NT 4.0 Workstation, Windows 98 Second Edition a Windows ME, klesá v těchto systémech také počet nově objevených chyb.

6.2 Ošetřenost objevených chyb

Protože opravená chyba není již zneužitelná, je důležité chyby opravovat. V příloze B je přiložena další skupina šesti grafů, grafy vyjadřuje do jaké míry byly opraveny chyby operačních systémů firmy Microsoft.

Míra opravenosti je vyjádřena hodnotami pojmenovanými „Unpatched“, což znamená že chyba nebyla ani částečně opravena, „Partial Fixed“, která vyjadřuje že chyba byla

částečně opravena, „Vendor Patch“ což znamená že společnost Microsoft chybu již kompletně záplatovala a hodnota „Vendor Workaround“ znamená že chyba je ošetřena metodou, která chybu sice neodstraní, ale tato chyba již dále není zneužitelná.

Zkoumanými operačními systémy jsou Windows NT 4.0, Windows 98 Second Edition, Windows Millennium, Windows 2000, Windows XP a Windows Vista. A zkoumané období je, stejně jako u předchozí skupiny grafů, období od roku 2003 do roku 2008.

Z grafů vyplývá že systém s největším procentním podílem neopravených chyb je systém Windows NT Workstation 4.0 s hodnotou 20 %. Zbývající operační systémy mají procentuální hodnotu neopravených chyb velmi podobnou a tato hodnota se pohybuje okolo 12 %. Zkoumané operační systémy mají záplatováno přibližně 85 % objevených chyb. Výjimku opět tvoří Windows NT 4.0, která jsou záplatovaná pouze ze 77 %.

6.3 Možný dopad chyb

Protože různé objevené chyby jsou různě závažné, je také jejich dopad na napadený operační systém různý. V příloze C je přiložena další skupina šesti grafů, které vyjadřují možný dopad objevených programových chyb zkoumaných operačních systémů.

Zkoumanými operačními systémy jsou Windows NT 4.0, Windows 98 Second Edition, Windows Millennium, Windows 2000, Windows XP a Windows Vista. A zkoumané období je, stejně jako u předchozí skupiny grafů, období od roku 2003 do roku 2008.

Nejběžnější hodnota vyskytující se v grafech je hodnota „System access“ a tato hodnota znamená že po úspěšném zneužití chyby je možné získat přístup do systému. Tato hodnota je zvýšená u operačních systémů Windows 98 Second Edition a Windows Millennium a dosahuje 60 %. Ostatní operační systémy mají tuto hodnotu přibližně 50 %. Ve Windows Vista je však tato hodnota nižší a klesla na 40 %.

Druhým nejběžnějším dopadem je takzvané odmítnutí služby a v grafech je označen jako „DoS“. Zneužitím chyby s tímto dopadem přestane systém poskytovat danou službu. Tato hodnota se ve všech zkoumaných systémech pohybuje okolo 20 %, ve Windows Vista je však opět nižší a je 13 %.

Další častou hodnotou je zvýšení uživatelských práv označené jako „Privilege escalation“. Tato hodnota se různí, ale nejvyšší je ve Windows NT 4.0 Workstation a ve

Windows Vista. Ve tato hodnota ve Windows Vista může být za toho navýšení zodpovědná nově zavedená funkce přidělování uživatelských práv UAC.

6.4 Místo odkud je možné chyby zneužít

Zajímavou statistikou může být statistika toho, odkud je možné objevenou chybu zneužít. V příloze D je přiložena další skupina šesti grafů, které právě takovou statistiku vyjadřují.

Zkoumanými operačními systémy jsou Windows NT 4.0, Windows 98 Second Edition, Windows Millennium, Windows 2000, Windows XP a Windows Vista. A zkoumané období je, stejně jako u předchozí skupiny grafů, období od roku 2003 do roku 2008.

Hodnoty vyskytující se v grafech jsou „From remote“ což znamená že chyba může být zneužitá ze vzdáleného počítače, „From local network“ což znamená že chyba může být zneužitá z počítače připojeného k místní síti a poslední hodnotou je hodnota „Local system“ což znamená že chybu je možné zneužít zevnitř systému.

Nejvíce chyb lze podle grafů ve všech zkoumaných operačních systémech zneužít ze vzdáleného počítače. Jedná se o množství více než poloviny objevených chyb. Tato část je velmi vysoká ve Windows 98 Second Edition a ve Windows Millennium a podle grafů dosahuje přes 80%.

6.5 Závažnost objevených se chyb

Protože následky zneužití objevených chyb se mohou lišit, je zajímavé zkoumat v jakém počtu a do jaké míry jsou objevené chyby závažné. V příloze E je přiložena další skupina šesti grafů, které vyjadřují závažnost objevených chyb v procentech.

Zkoumanými operačními systémy jsou Windows NT 4.0, Windows 98 Second Edition, Windows Millennium, Windows 2000, Windows XP a Windows Vista. A zkoumané období je, stejně jako u předchozí skupiny grafů, období od roku 2003 do roku 2008.

Hodnoty v grafech jsou podle závažnosti seřazeny od nejzávažnější po nejméně závažnou a jejich hodnoty jsou Extremely, Highly, Moderately, Less, Not.

Z grafů vyplývá skutečnost že ve Windows NT 4.0 Workstation nebyla ve zkoumaném období objevena žádná extrémně závažná chyba. U ostatních zkoumaných operačních systé-

mů se tato hodnota pohybuje mezi třemi a čtyřmi procenty. Největší podíl pak ve všech zkoumaných operačních systémech pokrývají středně závažné chyby.

6.6 Počet exploitů vybraných produktů Firmy Microsoft

Tabulka 6.6.1 ukazuje počet oznámených chyb a počet exploitů vybraných produktů firmy Microsoft v letech 2006 a 2007. Vybrány byly různé verze webového prohlížeče Internet Exploreru, kancelářského balíku Microsoft Office a také operačních systémů Windows. Z tabulky vyplývá že přibližně na polovinu oznámených chyb zmíněných programů již byl nalezen způsob jak je zneužít.

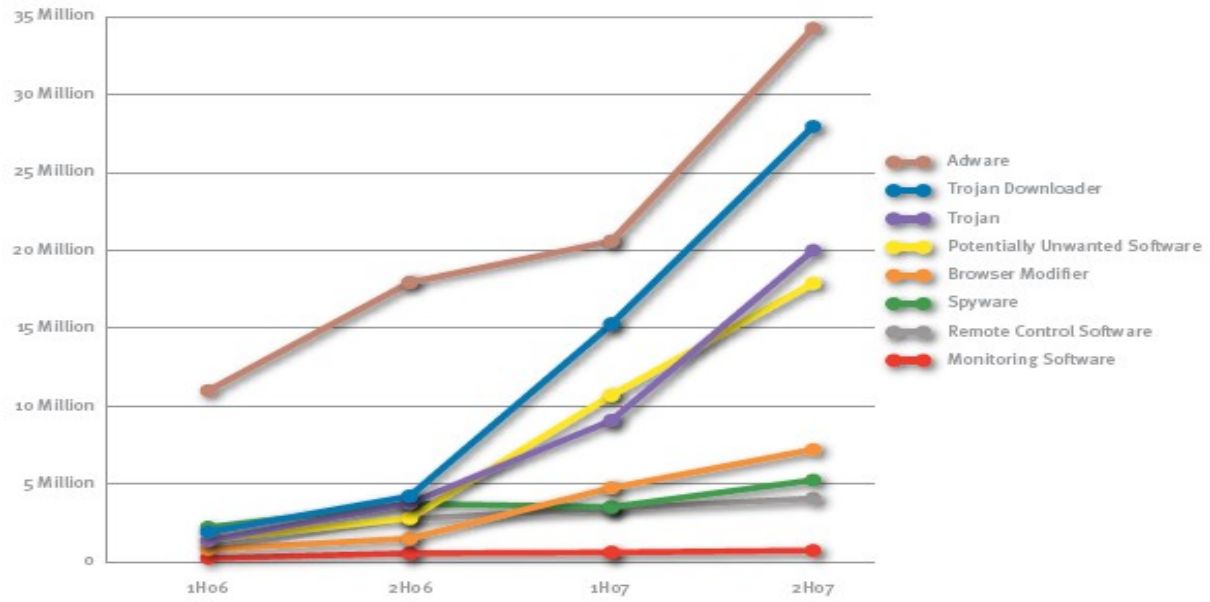
Jaké mohou být důsledky úspěšného exploitování chyby programu jsem předvedl na příkladu exploitu chyby ve službě Plug & Play operačního systému Windows 2000.

Tab. 6.6.1: Počet exploitů za rok 2006 a 2007 (7)

By Microsoft Security Bulletin		2006			2007			
Product	Version	Microsoft Security Bulletin Count	Exploits	Percentage	Microsoft Security Bulletin Count	Exploits	Percentage	Delta Microsoft Security Bulletin
Internet Explorer®								
	5	8	4	50.0%	8	3	37.5%	-12.5%
	6	7	3	42.9%	8	3	37.5%	-5.4%
	7	0	0	—	8	3	37.5%	—
Microsoft Office								
	2000	13	7	53.9%	11	6	60.0%	6.2%
	XP	13	5	38.5%	12	6	54.6%	16.1%
	2003	12	5	41.7%	13	6	46.2%	4.5%
	X-Mac	7	2	28.6%	1	1	100.0%	71.4%
	2004-Mac	7	3	42.9%	11	5	45.5%	2.6%
	2007	0	0	—	5	1	20.0%	—
Windows®								
	98	13	5	38.5%	0	0	—	—
	ME	13	4	30.8%	0	0	—	—
	2000	46	14	30.4%	36	5	13.9%	-16.5%
	XP	53	27	51.9%	39	5	12.8%	-39.1%
	2003	49	26	53.1%	39	18	46.2%	-6.9%
	Windows Vista	0	0	—	22	9	40.9%	—

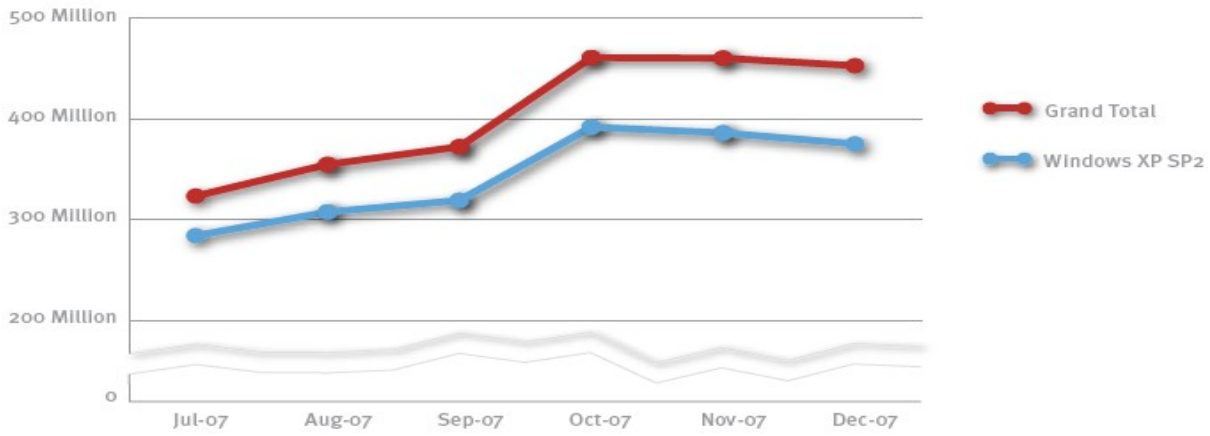
6.7 Množství detekovaných škodlivých programů

Nárůst počtu škodlivých programů je patrný z dalšího grafu, který je na obrázku 6.7.1. Graf znázorňuje počet detekovaných škodlivých programů v období let 2006 až 2007. V největší míře jsou podle grafu škodlivé programy zastoupeny adwarem. Hlavní činnost adware je zobrazovat nevyžádanou reklamu. Další nejhojnější jsou škodlivé programy typu trojan downloader, které mají za úkol instalovat další škodlivé programy za zády uživatele. Třetí největší výskyt patří programům typu trojský kůň.



6.8 Napadnutelnost Windows XP v porovnání s ostatními verzemi Windows

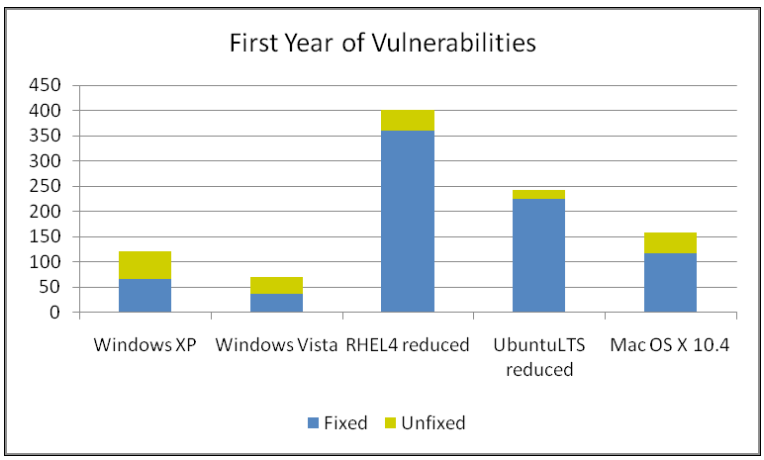
Graf na obrázku 6.8.1 vyjadřuje počet škodlivých programů detekovaných v operačním systému Windows. Červenou barvou je vykreslen celkový počet škodlivých programů detekovaných v operačních systémech Windows, modrou barvou je vykreslen počet výskytů pouze ve Windows XP SP2. Vysoký podíl výskytu škodlivých programů právě ve Windows XP může být zdůvodněn jeho převahou v použití pro přístup na internet.



6.9 Porovnání množství bezpečnostních chyb různých platforem

Zajímavé je také srovnání zranitelnosti různých operačních systémů v porovnání s operačními systémy firmy Microsoft. Graf na obrázku 6.9.1 vyjadřuje množství opravených a neopravených programových chyb v jednotlivých zkoumaných operačních systémech. Z grafu vyplývá že systém s nejmenším počtem chyb za poslední rok je operační systém Windows Vista. Systém s druhým nejmenším počtem chyb je dle grafu Windows XP a největší počet programových chyb dle grafu obsahuje operační systém Red Hat rhel4ws. Vysoký počet programových chyb obsažených v linuxových systémech může být do jisté míry zapříčiněn tím, že linuxové systémy v sobě obsahují velmi mnoho programů, které rozšiřují funkčnost tohoto operačního systému.

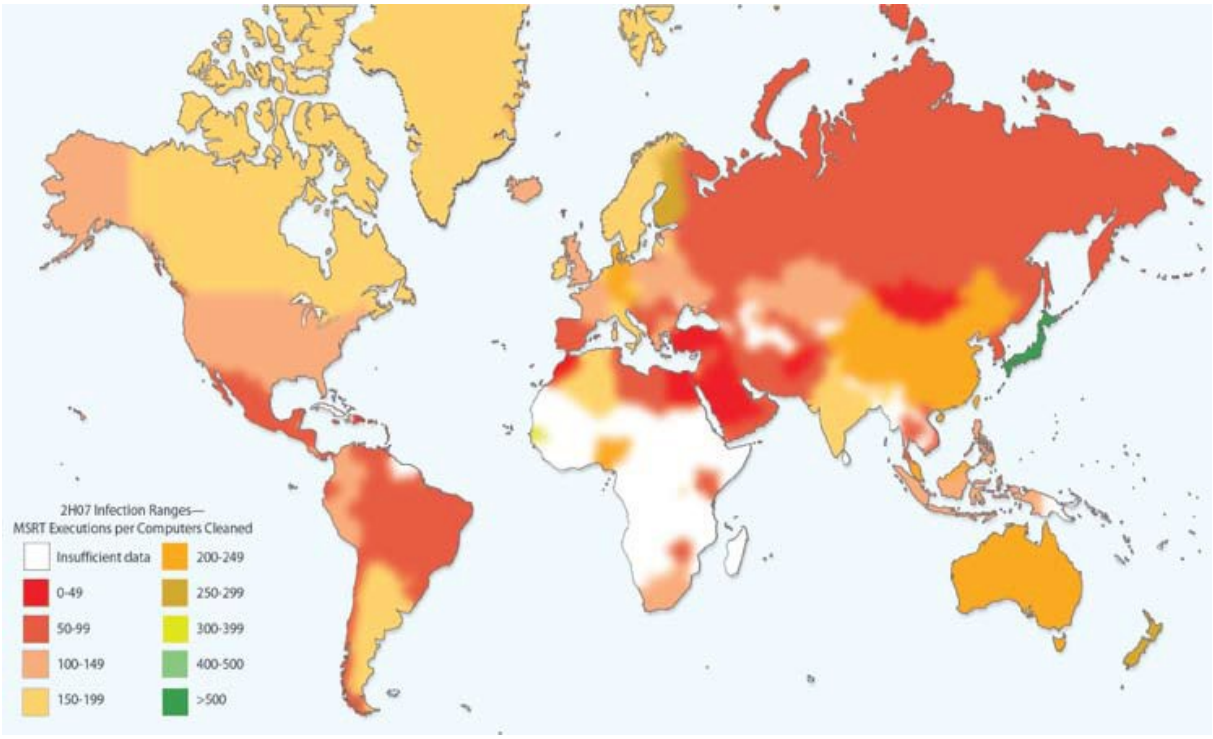
Pokud se ovšem zaměříme na počet neopravených chyb, jsou Windows XP operačním systémem s největším počtem neopravených chyb.



6.10 Rozšířenost malware ve světě

Na obrázku 6.10.1 je mapa, která zobrazuje výskyt škodlivých programů na planetě Zemi v roce 2007. Největšímu výskytu odpovídá zelená barva a nejnižšímu odpovídá bílá barva.

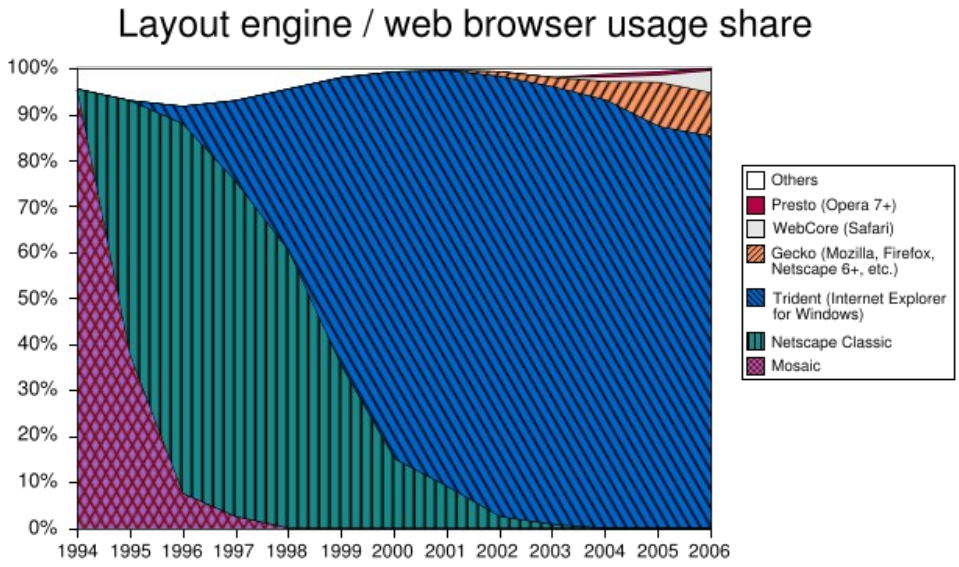
Největší výskyt malware byl zaznamenán v oblasti Japonska, může to být způsobeno vysokou hustotou zalidnění a vysokou technickou vyspělostí civilizace v této oblasti. V menší míře se malware objevoval v oblasti Austrálie, Číny, a severní Evropy. Nepatrný výskyt byl zaznamenán v oblasti Afriky.



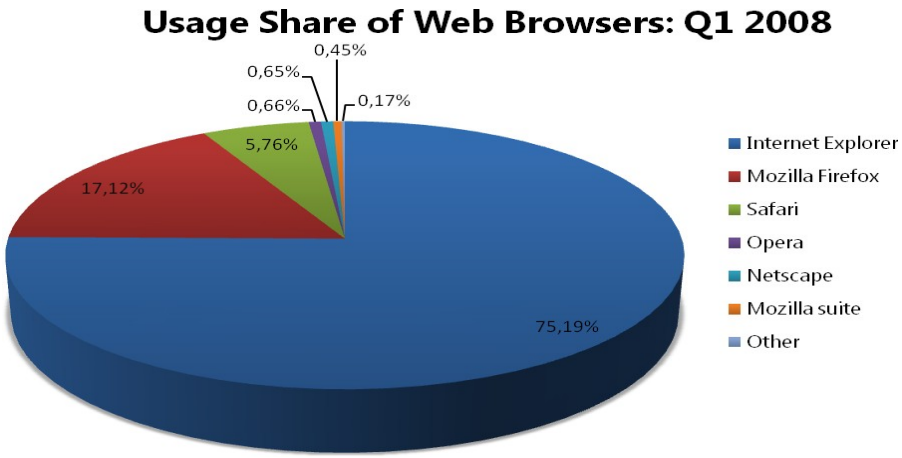
6.11 Používanost OS k přístupům na web

První graf na obrázku 6.11.1 ukazuje vývoj používanosti internetových prohlížečů od roku 1994 do roku 2006. Z grafu je vidět že webový prohlížeč Mosaic se z internetu vytratil přibližně do roku 1998, naproti tomu se velmi rozšířil webový prohlížeč Internet Explorer firmy Microsoft především díky tomu že je distribuován společně s operačními systémy Windows. Prohlížeč Internet Explorer je v dnešní době majoritním internetovým prohlížečem.

Druhým nejpoužívanějším prohlížečem současnosti je internetový prohlížeč Firefox. Ten se na pole webových prohlížečů probojoval přibližně v roce 2003.



Druhý graf na obrázku 6.11.2 ukazuje používanost internetových prohlížečů v prvním čtvrtletí roku 2008. Celé tři čtvrtiny uživatelů používá pro přístup na internet prohlížeč Internet Explorer z dílny firmy Microsoft. Druhým nejpopulárnějším prohlížečem je Firefox, který si oblíbila téměř pětina uživatelů. Třetím nejúspěšnějším prohlížečem je prohlížeč Safari od firmy Apple. Tento prohlížeč se těší velké oblibě u uživatelů operačního systému Mac OS X.



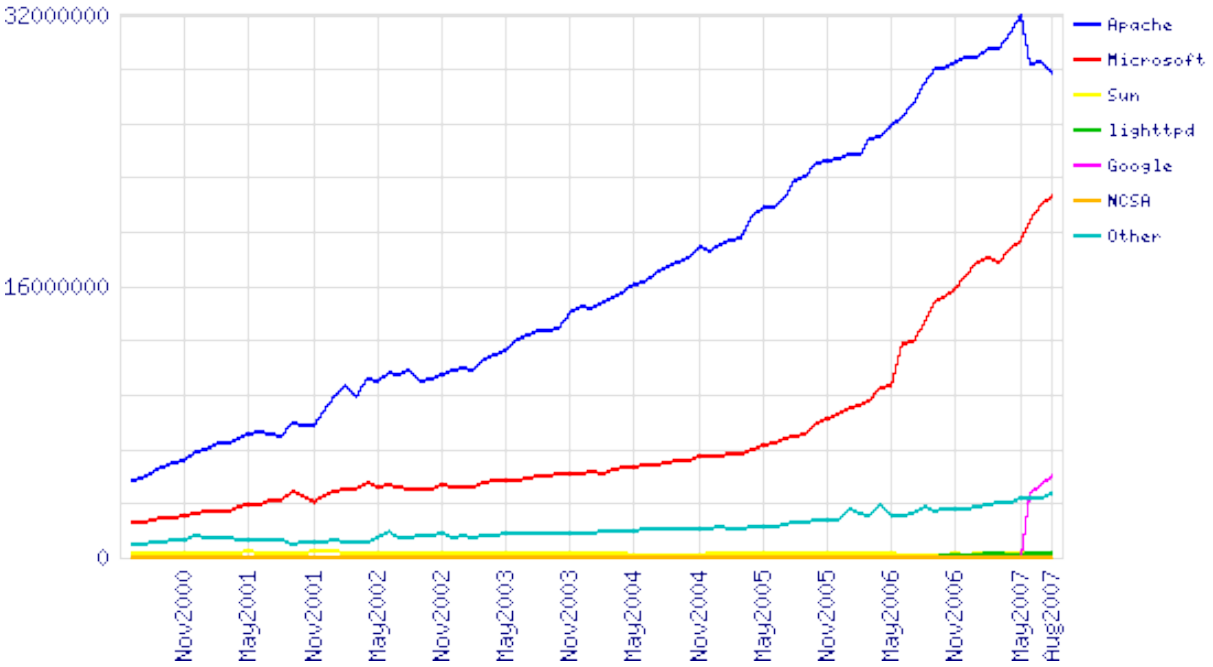
Z těchto statistik je možné odhadnout do jaké míry je používán systém Windows k přístupu k internetu. Microsoft Internet Explorer lze spustit pouze z operačního systému

Windows, tudíž všichni uživatelé kteří prohlíží web s Internet Explorerem pravděpodobně Windows používají. K tomu je možné připočíst také určitou část uživatelů, kteří upřednostňují prohlížeč Firefox, protože tento prohlížeč je určen jak pro Linux, tak pro Windows. Z tohoto úsudku vyplývá že více než 75 % uživatelů internetu používá operační systém Windows.

6.12 Používanost os k provozování serveru

Grafy vyjadřují používanost software k provozování webových serverů. Již dlouhou dobu mezi sebou vedou souboj dva nejoblíbenější produkty, jeden je z dílny Microsoftu jménem IIS[9], druhý se jmenuje Apache a je možné jej provozovat na dvou nejvýznamnějších platformách, platformách Linux a Windows. Grafy se opírají o výsledky ankety, kterou pravidelně provádí společnost Netcraft, jejíž internetové stránky jsou k nalezení na internetové adrese http://news.netcraft.com/.

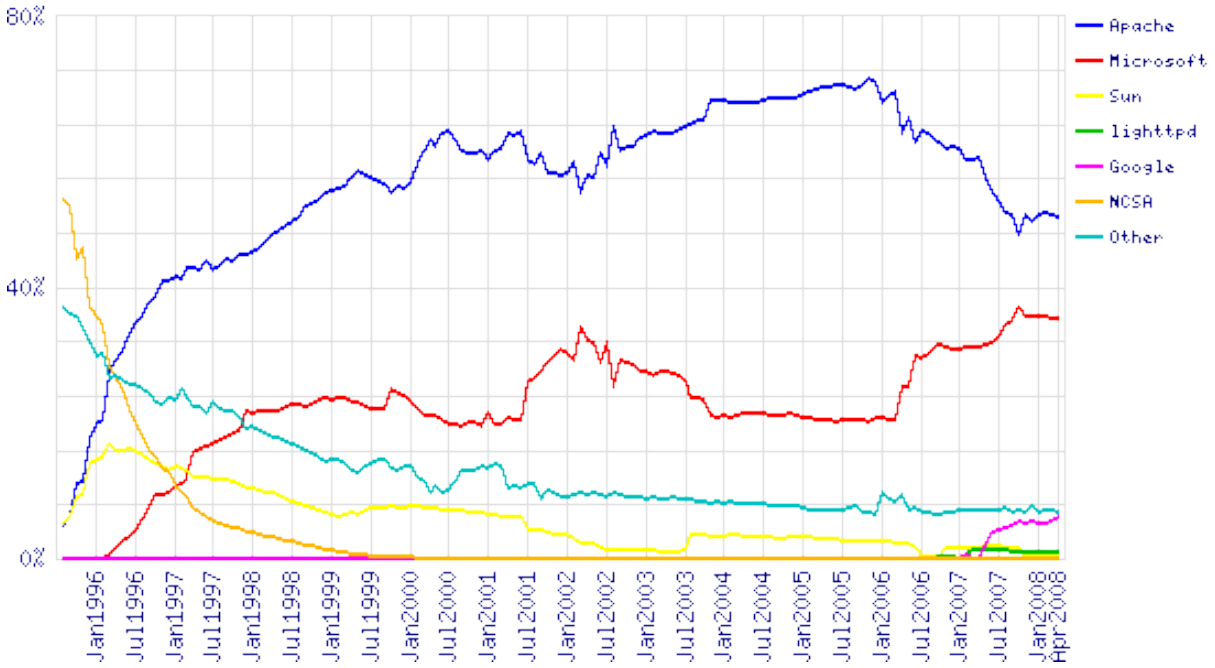
První graf na obrázku 6.12.1 zkoumá období let 2001 až 2007. Z grafu je patrné že počet serverů se rok od roku zvyšuje. V roce 2006 a 2007 byl zaznamenán prudký nárůst počtu serverových systémů firmy Microsoft.



Druhý graf na obrázku 6.12.2 vyjadřuje počty webových serverů mezi roky 1996 a 2008 v procentech. Od roku 2006 začíná nárůst počtu nasazení produktů firmy Microsoft. Při

9 IIS (Internet Information Server).

zkoumání grafu je třeba přihlédnout k faktu že webový server Apache lze provozovat na platformě Linux, ale také na platformě Windows.



Obě technologie provozování serveru jak IIS, tak Apache jsou hojně rozšířeny a prověřeny časem. Server Apache je k dispozici zdarma a je možné jej provozovat pod Linuxem, ale taktéž pod Windows, což mu dává jistou výhodu.

7 ZÁVĚREČNÉ ZHODNOCENÍ BEZPEČNOSTI WINDOWS

Operační systém Windows je již dlouho velmi oblíbeným a rozšířeným operačním systémem. Stejně jako všecky programy a operační systémy, také operační systémy Windows obsahuje programové chyby. Tyto chyby lze různým způsobem zneužít a docílit tak nestandardního chování systému.

Správnou konfigurací, dodržováním bezpečnostních zásad a pravidelnými a častými aktualizacemi lze minimalizovat počet zneužitelných chyb a zvýšit bezpečnost tohoto operačního systému.

Na rozdíl o dob počítačových začátků, kdy tvůrci operačních systémů příliš nepředpokládali možnost napadení jejich systému, se postupně přikládal větší důraz na bezpečnost a v dnešní době se stal důležitým hlediskem v hodnocení kvality operačního systému.

Windows Vista obsahuje mnohá vylepšení oproti svým předchůdcům. V oblasti bezpečnosti urazila velký kus cesty Windows Vista novými technologiemi, které s sebou přináší, a může se tak stát nadějí bezpečnějších zítřků.

8 PROGRAM SEARCH & UPLOAD

Search & Upload je konzolový zálohovací nástroj. Program po spuštění vyhledá soubory podle vyhledávacích masek zadaných v konfiguračním souboru, následně je zkomprimuje metodou zip do archivu a nakonec odešle na FTP server, který je taktéž zadaný v konfiguračním souboru. Program podporuje plné zálohování.

V současné době existuje nepřeberné množství programů, které vykonají nějakou činnost a její výsledky ukládají do souborů. Může se jednat například o textové, tabulkové, nebo grafické editory, programovací nástroje, nebo soubory, do kterých poštovní klient ukládá poštu. Mnohdy jsou pro nás tyto soubory velice důležité a proto chceme mít jejich kopii zálohovanou na jiném počítači pro případ že o primární kopii přijdeme.

Protože tyto programy v sobě nemají zabudovány automatizované zálohovací nástroje, je nutné využít nástroje vyvinuté speciálně pro tvorbu záloh. Program Search & Upload je konzolový program a slouží k automatickému zálohování libovolných souborů na FTP server. Zálohovací proces proběhne bezprostředně po startu programu. Program Search & Upload může však být zneužit pro odesílání souborů vygenerovaných spywarem, nebo keyloggery, nebo jinými programy sloužícími ke sledování aktivit uživatele, jakými jsou například programy typu watchdog.

8.1 Popis funkce

Program po svém spuštění vyhledá a načte hlavní konfigurační soubor, ve kterém jsou uloženy hodnoty které ovlivňují chování programu. Druhým konfiguračním souborem je soubor, který definuje které soubory budou zálohovány. V hlavním konfiguračním souboru lze nastavit zda se má program spouštět automaticky po přihlášení uživatele (položka autostart), zda se má spustit ve skrytém režimu (položka stealth), interval opakování zálohovacího procesu v minutách (položka periodasearch, periodaupload) a údaje FTP serveru, na který se má záloha přenést (položka ftpserver, ftpuser, ftppass). Pro možnost použití zálohování více počítači na jeden společný FTP sever je v hlavním konfiguračním souboru definována ještě jedna hodnota (položka machineprefix), která určuje ze kterého počítače záloha pochází. Tato

hodnota je přidána na začátek každého souboru před odesláním na FTP server. Ve druhém konfiguračním souboru jsou uloženy údaje o zálohovaných souborech. Pro každou zálohovanou složku lze nastavit filtr pro soubory, které budou do zálohy zahrnuty. Používat lze zástupné znaky otazník a hvězdičku. Určit lze také hloubku, do které se bude adresářová struktura prohledávat. Jednotlivá pole jsou oddělena speciálním znakem svislou čarou. Jméno konfiguračního souboru je data\settings.txt a jméno druhého konfiguračního souboru je data\search.txt

8.2 Programátorská dokumentace

Program je psán z části objektově, z části funkcionálně. Funkcí bylo použito zejména z nedostatku času. V průběhu psaní programu byl kladen důraz znovupoužitelnost kódu a snadnou rozšiřitelnost programu.

8.2.1 Nejzajímavější funkce a třídy

Jednou z nejzajímavějších tříd programu je třída CFileUNICODE, která umožňuje pohodlně načítat a zapisovat textové řetězce ve formátu UNICODE (včetně diakritiky a národních znaků) do souboru.

Další velmi užitečná třída se nazývá CSettings a využívá třídu CFileUNICODE. Tato třída umožňuje velmi snadno přidávat, odebírat a modifikovat položky konfiguračních souborů. V její členské metodě getSettings je ošetřena inicializace proměnných implicitními hodnotami, pokud hledaná položka není v konfiguračním souboru definována.

Funkce s názvem compressFilesToFile slouží ke komprimaci souborů metodou zip. Ke své činnosti využívá třídu jménem HZIP, která představuje elegantní způsob komprimace souborů. Tato třída podporuje vytváření šifrovaných zip archivů. Zdrojový kód této třídy je dostupný na internetové adrese [27].

Ve funkci genSoubFileList je implementováno rekurzivní vyhledávání souborů na pevném disku. Tato funkce je implementována pomocí standardních algoritmů.

Pomocí funkce fileUpload je možné ukládat soubory na FTP server. Tato funkce využívá funkci CftpConnection z knihovny MFC[10]. Spojení je implementováno synchronním způsobem. Tato funkce je využívána funkcí fileUpload_withRetry. Tato zdokonalená verze

10 MFC (Microsoft Foundation Class).

funkce řeší dočasnou nedostupnost FTP serveru. Funkce opakuje pokus o připojení k FTP serveru v pravidelných intervalech, dokud není tento pokus úspěšný. Tato funkce je opět volána synchronně.

Prováděné operace jsou zaznamenávány pomocí funkcí log a logTF do log souborů. Druhá zmíněná funkce může být s výhodou využita pokud je třeba do logu zapsat různé hodnoty v závislosti na výsledku sledované operace. Výhoda spočívá ve zjednodušení zdrojového kódu.

8.2.2 Plánovaná vylepšení programu

Stávající verze programu je plně funkční a představuje jedno z možných řešení zálohování souborů na FTP server.

Program by mohl být rozšířen o další metody zálohování. K jejich implementaci by mohlo být využito kontrolního součtu zálohovaných souborů pro detekci změny v obsahu souborů. Takový způsob by byl výhodný zejména při současném používání programu Search & Upload a jiného zálohovacího software, který využívá ke své záloze atribut souborů archivovat.

Dalším vylepšením programu by mohlo být zlepšení bezpečnosti zálohovaných souborů pomocí šifrovaného archivu. Tato vlastnost je důležitá zejména při zálohování na nedůvěryhodný FTP server.

Protože většina komplikací je vyřešena po analýza logu, další vylepšení by mohla být provedena v oblasti zaznamenávání informací do logů. Zaznamenávané informace by mohly být podrobnější.

9 SHRNUTÍ

Cílem této práce bylo poukázat na hrozby skrývající se ve škodlivých programech a ukázat základní metody jak se proti těmto programům bránit.

Práce obsahuje základní metody útoků na operační systém Windows, ukazuje následky zneužití chyb tohoto operačního systému a vyzdvihuje nutnost aktuálnosti systému a správné systémové konfigurace a konfigurace služeb v systému spuštěných. Součástí jsou doporučení bezpečné konfigurace systému a základní bezpečnostní pravidla.

V rámci práce byl proveden úspěšný pokus zneužití chyby v operačním systému Windows 2000. Výsledkem tohoto pokusu bylo získání vzdáleného příkazového řádku s právy správce systému.

Jako součást této práce byl vytvořen počítačový program Search & Upload, který je primárně určen k zálohování souborů na FTP server, ale může být taktéž zneužit k přenosu citlivých souborů z napadeného systému do rukou útočníka.

Výsledkem této práce je zhodnocení bezpečnosti operačních systémů Windows.

SEZNAM LITERATURY

[1] Windows History. [cit. 2008], [ONLINE]. <http://www.Microsoft.com/Windows/WinHistoryProGraphic.mspx>

[2] HOLČÍK, Tomáš. Stručná historie Windows. [cit. 2008], [ONLINE]. <http://www.zive.cz/default.aspx?article=115491>

[3] Windows 2000. [cit. 2008], [ONLINE]. <http://en.wikipedia.org/wiki/Windows_2000>

[4] Windows XP. [cit. 2008], [ONLINE]. <http://en.wikipedia.org/wiki/Windows_XP>

[5] Windows Vista. [cit. 2008], [ONLINE]. <http://en.wikipedia.org/wiki/Windows_Vista>

[6] JONES, Jeff. Browser Vulnerability Analysis. [cit. 2008], [ONLINE]. <http://blogs.technet.com/security/attachment/2594822.ashx>

[7] CRANTON, Tim, GULLOTTO, Vinny, JONES, Jeff. Microsoft Security Intelligence Report (July - December 2007). [cit. 2008], [ONLINE]. <http://www.Microsoft.com/downloads/details.aspx?FamilyId=BCC879DB-9FE6-4331-B231-E274EA8FC804&displaylang=en>

[8] JONES, Jeff. Windows Vista. [cit. 2008], [ONLINE]. <http://blogs.technet.com/security/attachment/2772991.ashx>

[9] Comparison of web browsers. [cit. 2008], [ONLINE]. <http://en.wikipedia.org/wiki/Comparison_of_web_browsers>

[10] Usage share of web browsers. [cit. 2008], [ONLINE]. <http://en.wikipedia.org/wiki/Usage_share_of_web_browsers>

[11] August 2007 Web Server Survey. [cit. 2008], [ONLINE]. <http://news.netcraft.com/archives/2007/08/06/august_2007_web_server_survey.html>

[12] Market Share for Top Servers Across All Domains August 1995 - April 2008. [cit. 2008], [ONLINE]. <http://news.netcraft.com/archives/2008/04/index.html>

[13] Vulnerability in Plug and Play Allows Remote Code Execution and Elevation of Privilege (MS05-039, Exploit_). [cit. 2008], [ONLINE]. <http://www.securiteam.com/exploits/5TP0C1FGKY.html>

[14] Microsoft Security Bulletin MS05-039. [cit. 2008], [ONLINE]. <http://www.Microsoft.com/technet/security/Bulletin/MS05-039.mspx>

[15] SCHÖN, Otakar. Microsoft se snaží v oblasti bezpečnosti. [cit. 2008], [ONLINE]. <http://www.zive.cz/default.aspx?section=21&server=1&article=123926>

[16] Vulnerability Report: Microsoft Windows NT 4.0 Workstation. [cit. 2008], [ONLINE]. <http://secunia.com/product/15/?task=statistics>

[17] Vulnerability Report: Microsoft Windows 98 Second Edition. [cit. 2008], [ONLINE]. <http://secunia.com/product/13/?task=statistics>

[18] Vulnerability Report: Microsoft Windows Millenium. [cit. 2008], [ONLINE]. <http://secunia.com/product/14/?task=statistics>

[19] Vulnerability Report: Microsoft Windows 2000 Professional. [cit. 2008], [ONLINE]. <http://secunia.com/product/1/?task=statistics>

[20] Vulnerability Report: Microsoft Windows XP Professional. [cit. 2008], [ONLINE]. <http://secunia.com/product/22/?task=statistics>

[21] Vulnerability Report: Microsoft Windows Vista. [cit. 2008], [ONLINE]. <http://secunia.-com/product/13223/?task=statistics>

[22] NOVÁK, Jiří. Definice a rotace záloh. [cit. 2008], [ONLINE]. <http://www.storage.cz/index.php?option=com_content&task=view&id=47&Itemid=39>

[23] Linux Security: How Not to Get Hacked. [cit. 2008], [ONLINE]. <http://www.linux.uc-la.edu/guides/security.php3>

[24] HELMICH, Jiří. Windows Vista - Co v sobě ukrývají? [cit. 2008], [ONLINE]. <http://pctuning.tyden.cz/index.php?option=com_content&task=view&id=7269&Itemid=89&limit=1&limitstart=3>

[25] Prohlížeč událostí (Event Viewer). [cit. 2008], [ONLINE]. <http://www.adminxp.cz/windows2000/index.php?aid=35>

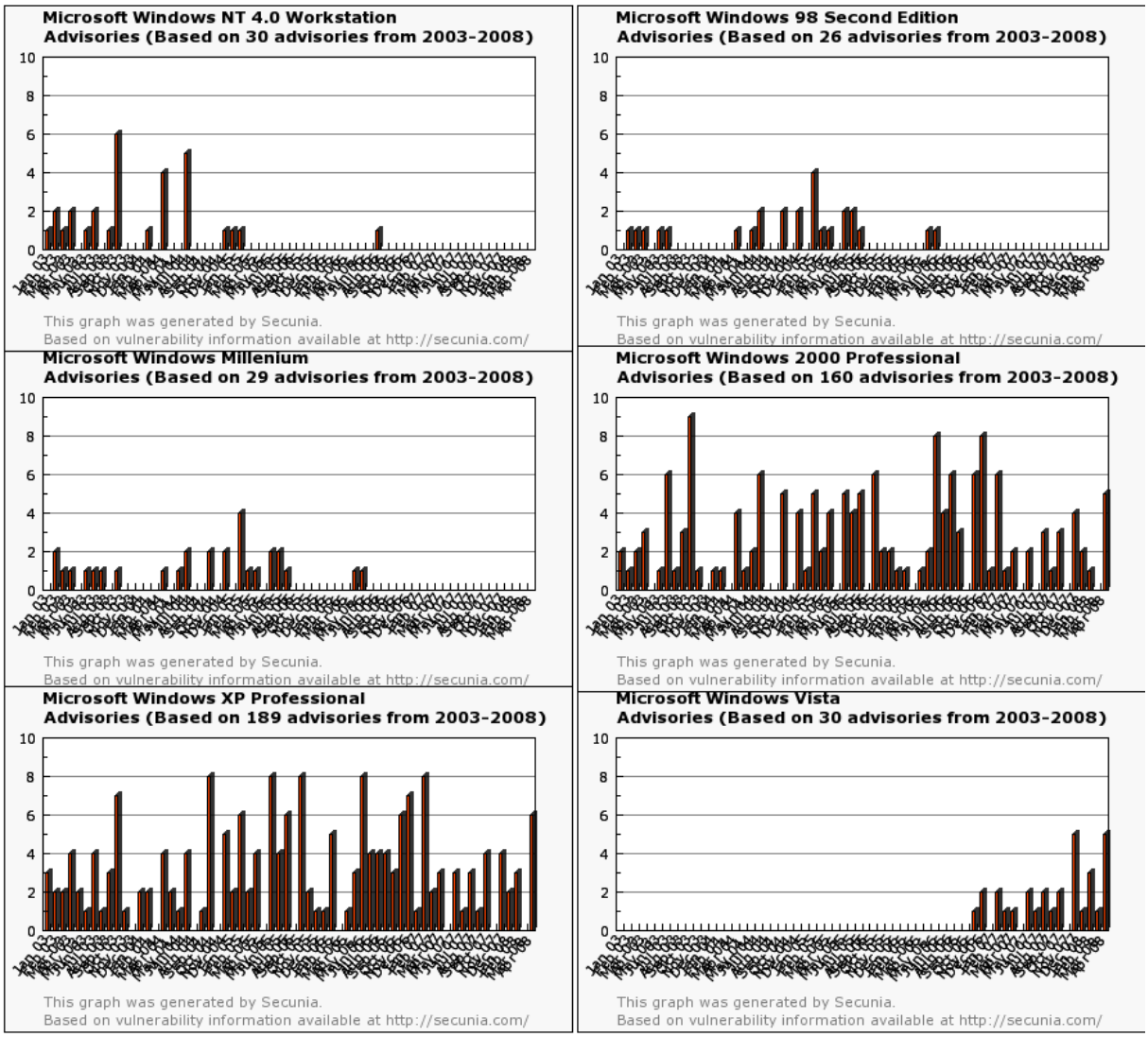
[26] JANÁK, David. Historie operačních systémů Windows a Unix. [cit. 2008], [ONLINE]. <http://www.fi.muni.cz/usr/jkucera/pv109/2002/xjanak.html>

[27] Zip Utils - clean, elegant, simple, C++/Win32. [cit. 2008], [ONLINE]. <http://www.-codeproject.com/KB/files/zip_utils.aspx>

[28] MCLURE, Struart, SCRAMBRAY, Joel, KUTZ, George. *Hacking bez tajemství : 3. aktualizované vydání*. Petr Břehovský, Josef Pojsl, Radek Čevela. Brno : Computer Press, 2003. 632 s. ISBN 80-722-6948-8.

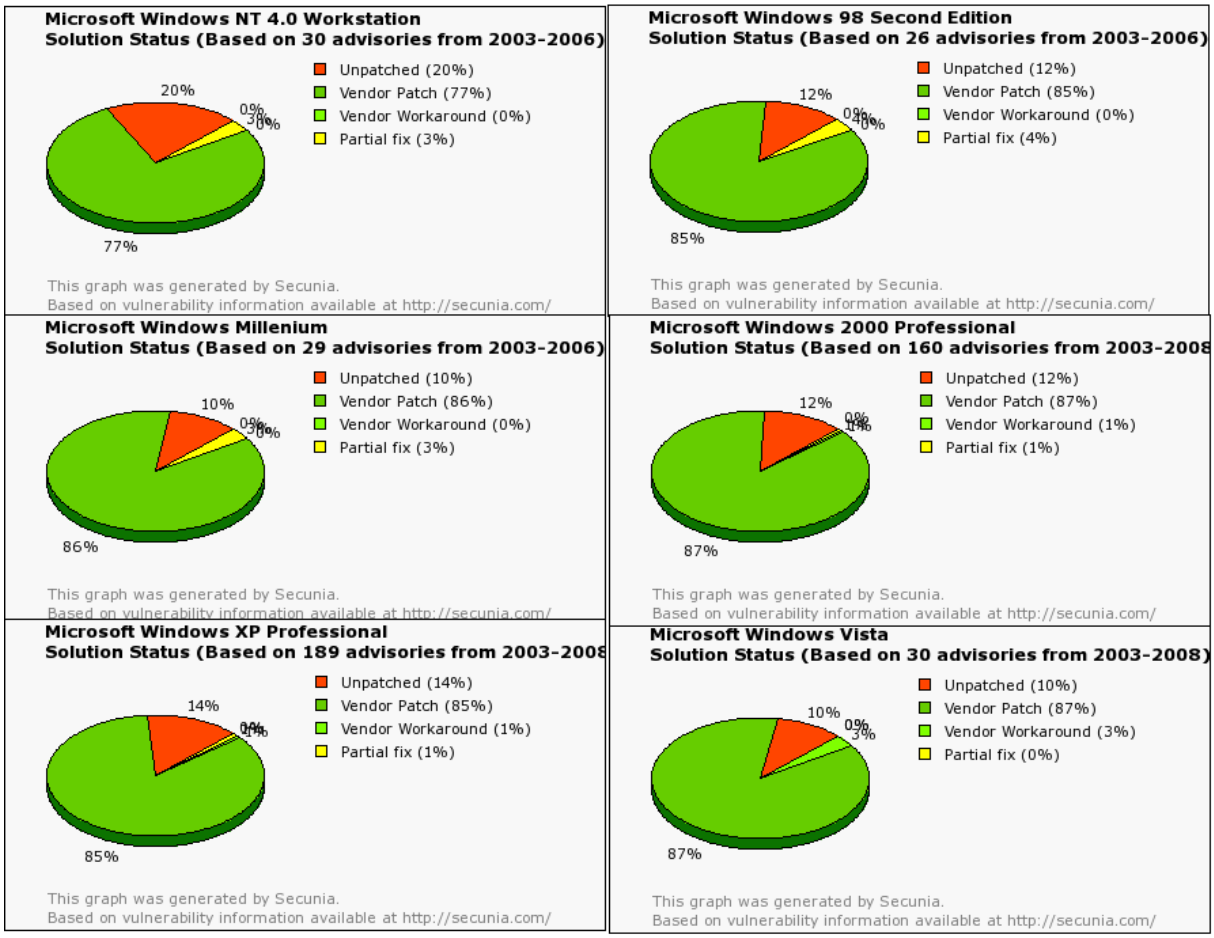
SEZNAM PŘÍLOH

Výskyt chyb ve Windows v časovém horizontu



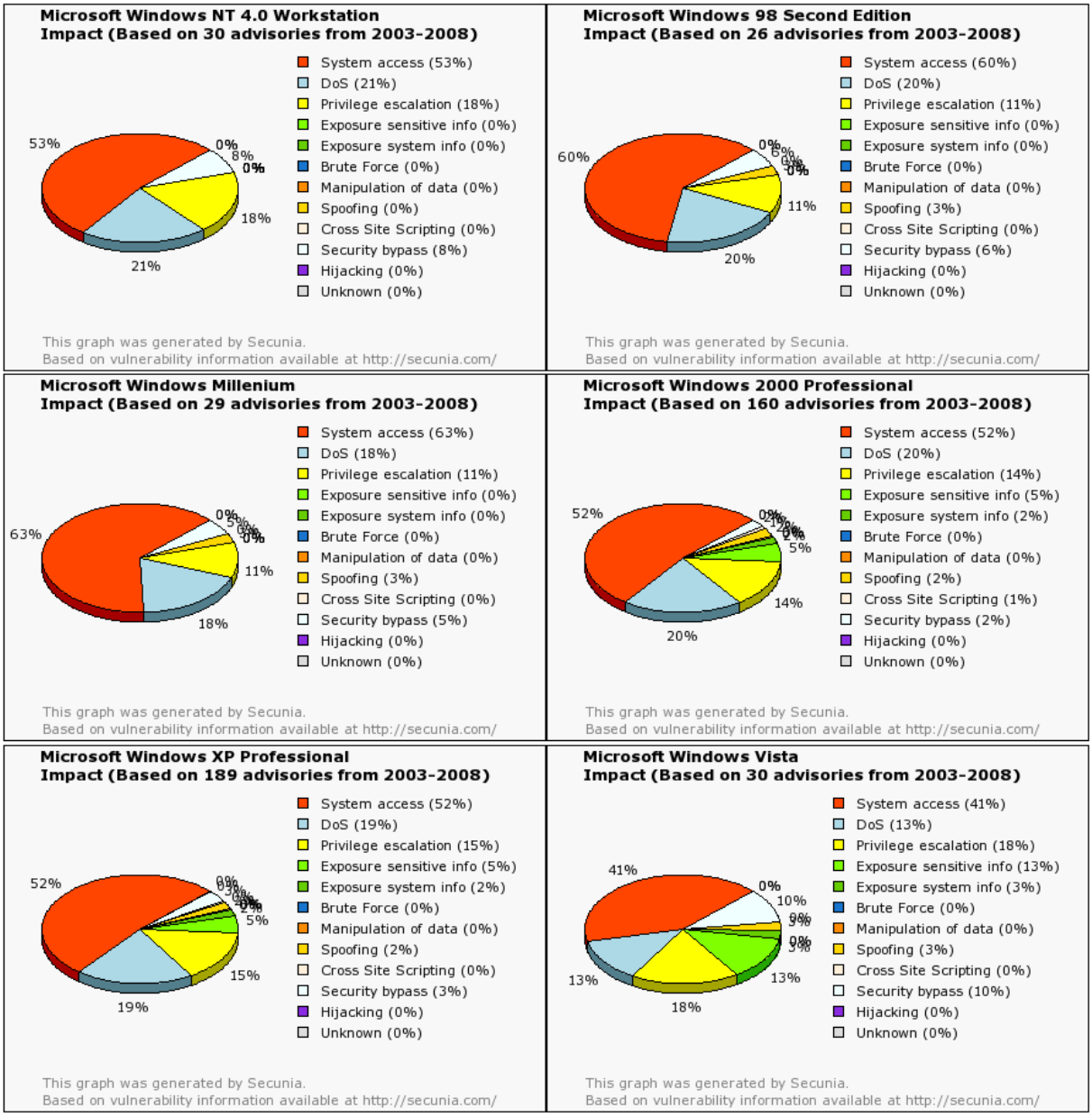
ZDROJ: [16], [17], [18], [19], [20], [21]

Ošetřenost objevených chyb



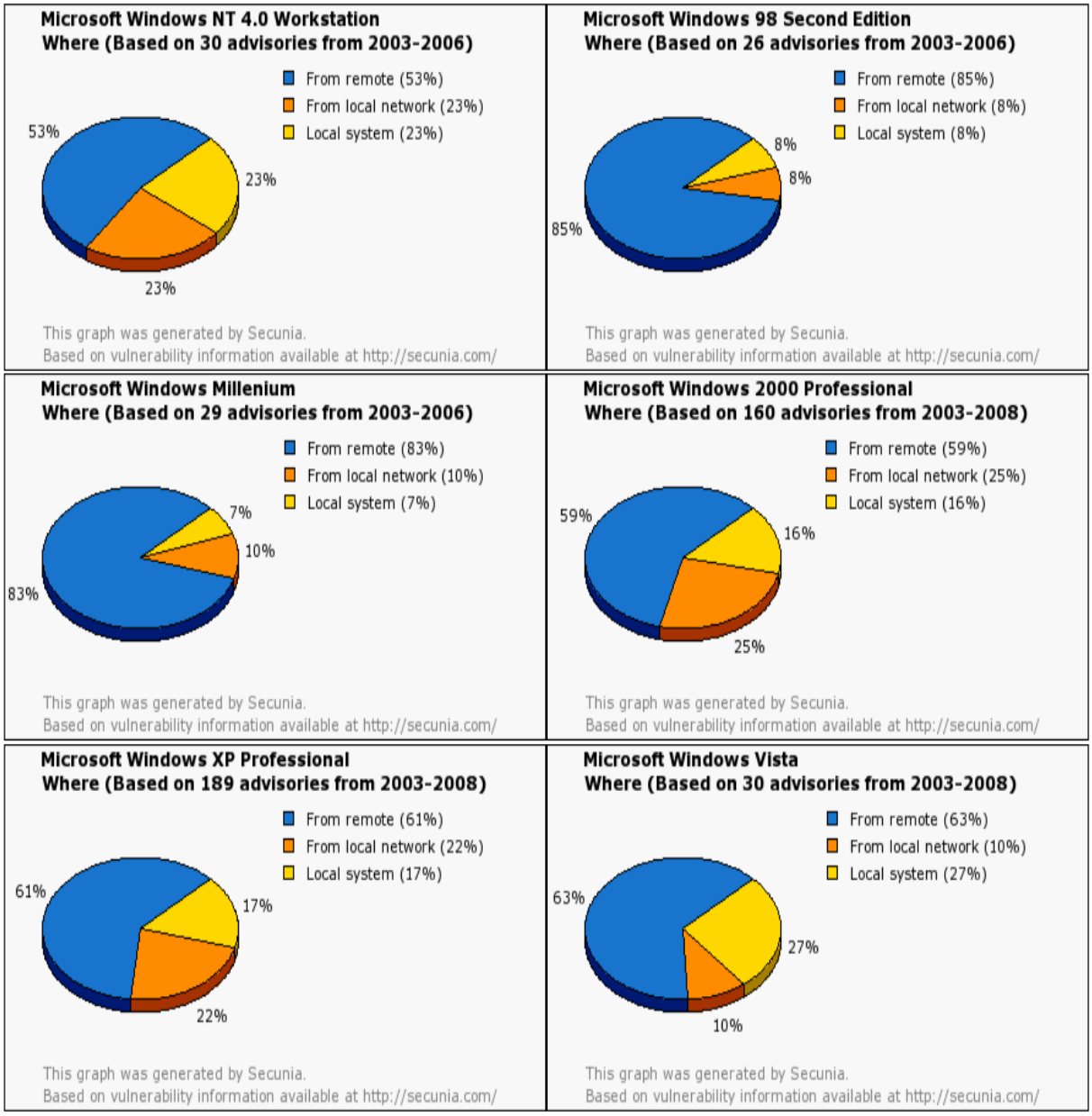
ZDROJ: [16], [17], [18], [19], [20], [21]

Možný dopad chyb



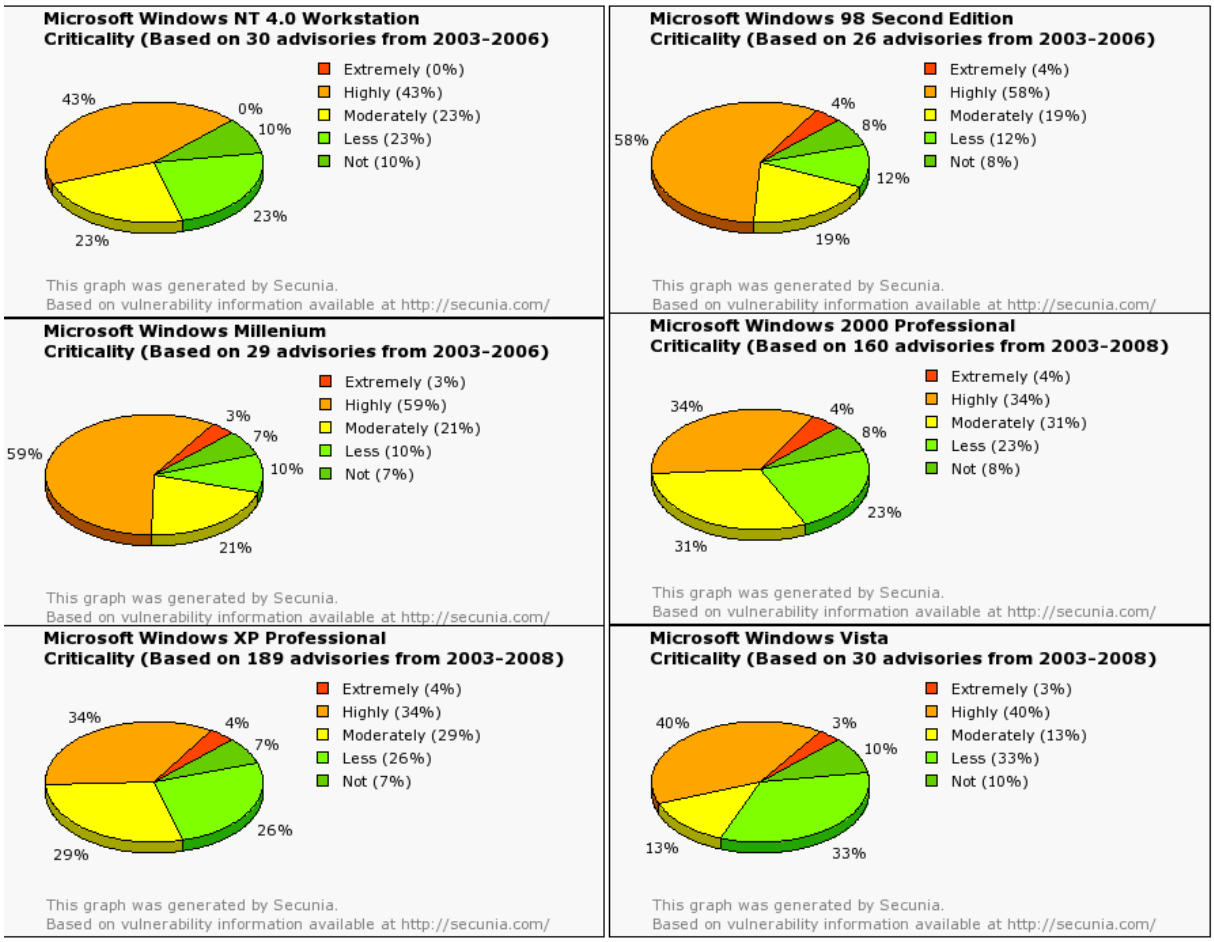
ZDROJ: [16], [17], [18], [19], [20], [21]

Místo odkud je možné chyby zneužít



ZDROJ: [16], [17], [18], [19], [20], [21]

Závažnost objevených se chyb



ZDROJ: [16], [17], [18], [19], [20], [21]