بهره‌گیری رخنه‌گران از ویژگیهای ویندوز اکس‌پی

□ تورج صارمی راد

یکی از کارهایی که می‌توان برای پیشگیری از آلودگی رایانه به برخی از ویروسها و همچنین **رخنهٔ** رخنه‌گران انجام داد رسیدگی به وضع سیستم‌عامل است. برای انجام دادن این کار، لازم است به موردهای زیر توجه کرد:

۱- پوزیکس [1]

واژهٔ پوزیکس کوته‌نوشت گزارهٔ زیر، به معنای «رابط انتقال‌پذیر سیستم‌عامل به یونیکس» است:

Portable Operating System Interface for Unix

بدین‌گونه، دانسته می‌شود پوزیکس استانداردی را به سیستم‌عامل می‌شناساند که برنامه‌های تحت آن انتقال‌پذیر به سایر رایانه‌ها می‌شوند. این استاندارد بر پایهٔ یونیکس بنا نهاده شده است. برای همین، در انتهای گزاره، واژهٔ یونیکس آمده است؛ ولی این استاندارد به گونه‌ای طراحی شده است که امکان بهره‌گیری از آن در سایر سیستمهای‌عامل نیز وجود دارد. برای همین، آن را کوته‌نوشت گزاره‌های زیر نیز درنظر می‌گیرند:

Portable Operating System Interface

Portable Operating System Interface for Computer Environments

بدین‌گونه، می‌توان پوزیکس را مجموعه‌ای از استانداردهای سیستم‌عامل ویندوز دانست که امکان بهره‌گیری از فرمانهای یونیکس را میسر می‌کند. بنابراین، برای این که رخنه‌گران نتوانند از ویژگی پوزیکس برای رخنه به رایانه‌ها بهره گیرند، می‌توان این ویژگی را از کار انداخت. برای انجامیدن این کار، می‌توان کارهای زیر را به ترتیب در ویرایشگر رجیستری انجام داد:

HKEY_LOCAL_MACHINE/
SYSTEM/CurrentControlSet/
Control/Session Manager/ Sub Systems

آنگاه در پنجرهٔ سوی راست، کلید چپ ماوس را روی گزینهٔ زیر بفشرید:

Optional

در این صورت، می‌بینید این کلید دارای شمار پیش‌گزیدهٔ پوزیکس است. می‌توان آن را پاک کرد، ولی نباید خود کلید را پاک کرد. در ضمن باید توجه داشت این کلید به پروندهٔ زیر در پوشهٔ سیستم ۳۲ اشاره دارد؛ بنابراین، باید آن را نیز پاک کرد:

Psxss.exe

اکنون، می‌توان به ویرایشگر رجیستری برگشت و کلید مربوطه را نیز پاک کرد.

۲- نظام پرونده‌گردانی

بیشتر کاربران رایانه‌های شخصی از نظام پرونده‌گردانی «فت۳۲» [2] بهره می‌گیرند؛ ولی نظام پرونده‌گردانی «ان‌تی‌اف‌اس» [3] دارای ایمنی بیشتری است. افزون بر این، با آن می‌توان از نظام رمزنگاری پرونده‌ها، برای رمز کردن پرونده‌ها بهره گرفت. برای انجامیدن این دگرگونی، می‌توان در خط فرمان ویندوز از فرمان زیر بهره گرفت:

Convert

به همراه این فرمان، باید نام دیسک منطقی و گزینهٔ زیر را به کار برد:

/FS:NTFS

برای نمونه، می‌توان نوشت:

Convert C: /FS:NTFS

با بهره‌گیری از این فرمان، نظام پرونده‌گردانی نخستین دیسک منطقی از «فت۳۲» به «NTFS» دگرگون می‌شود. ولی باید توجه داشت برای برگشت به وضع پیشین، باید از نرم‌افزارهای ویژه‌ای بهره گرفت. بنابراین، پیشگیری کنید و پیش از این دگرگونی، **نسخهٔ پشتیبان** تهیه کنید و بدانید برگشت از «NTFS» به «فت۳۲»، توسط ویندوز امکان‌پذیر نیست. در ضمن گزینه‌های اختیاری زیر را نیز می‌توان به همراه این فرمان به کار برد:

[1] POSIX

[2] FAT32
[3] NTFS

۱- با بهره‌گیری از گزینهٔ زیر، می‌توان تنظیمهای ایمنی پوشه‌ها و پرونده‌های دگرگون‌شده را از کار انداخت و آنها را برای همهٔ کاربران دسترس‌پذیر کرد:

/No Security

۲- با بهره‌گیری از گزینهٔ زیر، می‌توان پرونده‌ای را در پوشهٔ ریشه برای نگهداری داده‌های نظام پرونده‌گردانی «ان‌تی‌اف‌اس»، به فرمان شناساند:

/Cvt Area: نام پرونده

۳- با بهره‌گیری از گزینهٔ زیر، دیسک منطقی این توانایی را می‌یابد که در صورت نیاز دسترس‌ناپذیر شود. بدین‌گونه، همهٔ دسترسیها به آن نامعتبر می‌شود:

/X

۴- با بهره‌گیری از گزینهٔ زیر، می‌توان فرمان را در حالتی به کار برد که دانستنیهای بیشتری بنمایاند:

/V

در ضمن، باید توجه داشت:

۱- این فرمان را نمی‌توان برای دیسک جاری به کار برد.

۲- با بهره‌گیری از این فرمان، می‌توان به توانایی‌های ایمنی سیستم‌عامل ویندوز افزود.

۳- با بهره‌گیری از نظام پرونده‌گردانی «ان‌تی‌اف‌اس»، فرمانهای دیگری را نیز می‌توان به کار گرفت. برای نمونه، فرمان زیر را می‌توان در ویندوز ۲۰۰۰ و اکس‌پی، برای فشرده‌سازی پرونده‌ها و پوشه‌ها به کار برد:

Compact

۳- اشتراک پرونده‌ها

برای بهره‌گیری اشتراکی از پرونده‌ها در شبکه، ویندوز اکس‌پی دارای برنامهٔ اشتراک سادهٔ پرونده‌هاست. وجود این برنامه، باعث دسترسی رخنه‌گران به داده‌های رایانه می‌شود. بنابراین، بهتر است اشتراک سادهٔ پرونده‌ها را در ویندوز از کار بیندازید. برای انجامیدن این کار، می‌توان کارهای زیر را به ترتیب انجام داد:

My Computer, Tools, Folder Options…, View

در پنجره‌ای که اجرای فرمان پایانی می‌نمایاند سراغ گزینهٔ زیر بروید و بهره‌گیری از آن را از کار بیندازید:

Use Simple File Sharing

٤-مجری نویسانهای ویندوز [4]

ویندوز برای اجرای پرونده‌های **اسکریپتی** از ویژگی **مجری نویسانهای** ویندوز، مشهور به «دبلیواس‌اچ» [5] بهره می‌گیرد. ویروس‌نویسان می‌توانند با بهره‌گیری از این ویژگی ویندوز، رایانه‌های دارای ویندوز را بیالایند.

مجری‌نویسانهای ویندوز را می‌توان مانند **پرونده‌های دسته‌ای** [6] داس دانست. برای همین، ویندوز با بهره‌گیری از این ویژگی می‌تواند کار پردازش دسته‌ای را انجام دهد. این پردازشگر دسته‌ای می‌تواند از هرگونه زبان اسکریپت‌نویسی پشتیبانی کند. برای انجامیدن این کار، مجری‌نویسانهای ویندوز دارای سه بخش اصلی زیر است:

۱- **هستهٔ مجری:** این بخش، بخشهای دیگر را به هم می‌پیونداند؛

۲- **زبان‌نویسایی:** این بخش، می‌تواند هر زبان اسکریپت‌نویسی مانند ویژوال‌بیسیک‌اسکریپت باشد. زبانهای اسکریپت‌نویس، زبانهایی گسترش‌پذیر هستند. برای همین، با آنها می‌توان کارهای گوناگونی انجام داد.

۳- **مجری‌نویسان:** این بخش، اجرای اسکریپتها را به عهده دارد. برای اجرای اسکریپتها، ویندوز از دو برنامهٔ زیر بهره می‌گیرد:

1) wscript.exe

2) cscript.exe

برای از کاراندازی این ویژگی در ویندوز ۲۰۰۰ و اکس‌پی، ویندوز اکسپلورر را باز کنید و کارهای زیر را انجام دهید:

Tools, Folder Options…

در پنجره‌ای که می‌بینید گزینهٔ زیر را برگزینید:

File Types

پس از آن، به بخش زیر بروید:

Registered file types

و گزینهٔ زیر را از کار بیندازید:

VBS

---

[4] Windows Script host
[5] WSH
[6] Batch files

۵-کاربر مهمان

یکی از کاربرانی که می‌تواند به رایانه‌های تحت ویندوز اکس‌پی دست یابد **کاربر مهمان** است. رخنه‌گران نیز می‌توانند از این دسترسی بهره گیرند و به رایانه‌ها دست یابند. بنابراین، اگر به آن نیاز ندارید، آن را به شیوهٔ زیر از کار بیندازید:

Control Panel, Administrative Tools, Computer Management

آنگاه، در فهرست درختی قاب سوی چپ پنجرهٔ مدیر رایانه، کارهای زیر را به ترتیب انجام دهید:

System Tools, Local Users and Groups, Users

اکنون، در قاب سوی راست، روی گزینهٔ مهمان، کلید چپ ماوس را بفشرید و گزینهٔ زیر را برگزینید:

Account is disabled

٦-پروندهٔ فراخوانی [7] (جابه‌جایی [8])

سیستم‌عاملهایی چون ویندوز از پروندهٔ پنهانی در دیسک سخت، برای نگهداری بخشهایی از برنامه‌ها و پرونده‌های داده‌ای که در حافظه جای نمی‌شوند بهره می‌گیرند. بدین‌گونه، داده‌ها هنگام نیاز از این پرونده به حافظه و برای آزادسازی حافظه برای داده‌های تازه، از حافظه به این پرونده می‌روند. در نتیجه، این پرونده و حافظهٔ فیزیکی، **حافظهٔ مجازی** را پدید می‌آورند.

می‌توان ویندوز را به گونه‌ای تنظیم کرد که هنگام پایان کار، محتوای پروندهٔ فراخوانی را پاک کند. برای انجامیدن این کار، ویرایشگر رجیستری را اجرا کنید و کارهای زیر را به ترتیب انجام دهید:

HKEY_LOCAL_MACHINE/ SYSTEM/ CurrentControlSet/ Control/ Session Manager/ Memory Management

در پایان، کلید زیر را بیابید:

ClearPageFileAtShutdom

اگر این کلید را دیدید به آن شمار «۱» را بدهید، ولی اگر آن را نیافتید آن را بسازید و سپس به آن شمار «۱» بدهید.

۷-پروندهٔ محتوابرداری [9]

ویندوز هنگام از کار افتادن رایانه، برای بازیابی آنچه در حافظه است از پرونده‌ای به نام پروندهٔ محتوابرداری بهره می‌گیرد. این پرونده می‌تواند مورد بهره‌برداری رخنه‌گران قرار گیرد. برای پیشگیری از دسترسی رخنه‌گران به این پرونده، ویندوز اکس‌پی گزینه‌های سامانش زیر را دسترس‌پذیر می‌کند:

1)None

2)Small memory dump (64 KB)

3)Kernel memory dump

4)Complete memory dump

برای دسترسی به این گزینه‌ها، می‌توان کارهای زیر را به ترتیب انجام داد:

Control Panel, System, Advanced

در پنجره‌ای که می‌بینید، به بخش زیر بروید:

Startup and Recovery

و کلید چپ ماوس را روی گزینهٔ زیر بفشرید:

Settings

اکنون در پنجره‌ای که می‌بینید، به بخش زیر بروید:

Write debugging information

و گزینهٔ زیر را برگزینید:

(none)

باید توجه داشت رایانه به هر دلیلی که قفل کند و بازراه‌اندازی شود، ویندوز محتوای بخشهای اصلی حافظه را در این پرونده می‌نویسد تا کاربرانی که با زبان ماشین آشنایی دارند بتوانند علت به وجود آمدن این دشواری را پی گیرند. بنابراین، کاربرانی که با زبان ماشین آشنایی ندارند، می‌توانند آن را از کار بیندازند.

۸-دکتر واتسون

برنامهٔ دکتر واتسون یکی از برنامه‌های ویندوز است که گزارشهایی از کژکاری و دشواریهای برنامه‌ها تهیه می‌کند. بدین‌گونه، برنامهٔ دکتر واتسون هنگام از کار افتادن رایانه و برنامه‌های آن داده‌هایی را ذخیره می‌کند. این داده‌ها می‌تواند مورد بهره‌برداری رخنه‌گران قرار گیرد. برای از

---

[7] Page File
[8] Swap file
[9] Dump file

کار انداختن این برنامه، می‌توان در ویرایشگر رجیستری کارهای زیر را به ترتیب انجام داد:

HKEY_LOCAL_MACHINE/ SOFTWARE/ Microsoft/ Windows NT/CurrentVersion/ AeDebug

در این جا، به کلید زیر، شمار صفر را بدهید:

Auto

۹-اینترنت اکسپلورر

به شیوهٔ پیش‌گزیده، اینترنت‌اکسپلورر از ایمنی میانه بهره می‌گیرد، ولی شاید برخی از پلیدافزارها بتوانند آن را به کمترین میزان ایمنی دگرگون کنند. برای افزایش درجهٔ ایمنی و سنجش دگرگونی آن به وسیلهٔ پلیدافزارها، می‌توان در پنجرهٔ برنامهٔ اینترنت‌اکسپلورر، کارهای زیر را انجام داد:

Tools, Internet Options…, Security

۱۰-ماکروها

به شیوهٔ پیش‌گزیده، هنگام اجرای سندهای دارای ماکرو پیام هشداری به نمایش درمی‌آید. برخی از ویروس‌ها می‌توانند نمایش این هشدار را از کار بیندازند. بنابراین، لازم است گاهی وضع آن سنجیده شود. یعنی، نخستین سازوکار پدافندی آفیس در برابر ویروسهای ماکرو، پیام هشداری است که در صورت فعال بودن گزینهٔ «پاسداری در برابر ویروسهای ماکرو» می‌نمایاند. در این صورت، کاربر می‌تواند دربارهٔ بازکردن یا بازنکردن ماکروها بیندیشد. این ویژگی را می‌توان به صورتهای زیر به کار گرفت:

الف- در آفیس ۹۷، کارهای زیر را به ترتیب انجام دهید:

Tools, Options, General

در این جا، گزینهٔ زیر را برگزینید:

Macro Virus Protection

ب- در آفیس ۲۰۰۰ و ۲۰۰۳، کارهای زیر را به ترتیب انجام دهید:

Tools, Macro, Security…

در اینجا انتخابهای مندرج در جدول شماره ۱ دسترسی‌پذیرند.

جدول شمارهٔ «۱»

رویهٔ ایمنی نرم‌افزار	خیلی بالا	بالا	میانه	پایین
آفیس ۲۰۰۰	-	+	+	+
آفیس ۲۰۰۳	+	+	+	+

جدول ۱: رویه‌های ایمنی گوناگون ویروسهای ماکرو درآفیس

برای نمونه، با برگزیدن رویهٔ ایمنی خیلی بالا، در آفیس ۲۰۰۳ تنها ماکروهایی که از مکانهای امن دریافت و برپا شده باشند، پروانهٔ اجرا دارند. سایر ماکروهای دارای امضا یا بی‌امضا اجراناپذیر می‌شوند. یا با برگزیدن رویهٔ ایمنی بالا در آفیس ۲۰۰۳، تنها ماکروهایی که توسط فرستنده‌ها و منبعهای مورد اطمینان امضا شده باشند، پروانهٔ اجرا دارند. ماکروهای بدون امضا، به شیوهٔ خودکار اجراناپذیر می‌شوند.

۱۱-ویراستاریه

برای کاستهای ایمنی‌ای که در ویندوز یافت می‌شوند برنامه‌های اصلاحی ارایه می‌شود. به‌کارگیری بهنگام این گونه برنامه‌ها باعث می‌شود رخنه‌گران نتوانند از این کاستیها بهره بگیرند. بنابراین، باید از خبر عرضهٔ این گونه برنامه‌ها آگاه شد و در زمان مناسب از آنها بهره گرفت. با انجامش این گونه کارها، می‌توان از بسیاری از آلودگیها پیشگیری کرد.

۱۲-برنامه‌های کاری

بسیاری از برنامه‌های کاری در ویندوز وجود دارند که اغلب نیازی به آنها نیست. آنها را می‌توان از کار انداخت تا رخنه‌گران نتوانند از آنها بهره بگیرند. برای انجامیدن این کار، می‌توان یکی از شیوه‌های زیر را به کار برد:

۱-انجامش کارهای زیر به ترتیب:

Control Panel, Administartive Tools, Computer Management, Services and Applications, Services

در پنجره‌ای که می‌بینید، می‌توان برنامه‌های کاری را از کار انداخت یا به کار گرفت.

۲-اگر بخواهید بدانید کدام برنامهٔ کاری مایکروسافتی است و کدام برنامهٔ کاری مایکروسافتی نیست، می‌توان از فرمانmsconfig بهره گرفت.

در این صورت، پنجره‌ای با گزارهٔ آغازین زیر به نمایش درمی‌آید:

System Configuration Utility

در این پنجره، گزینهٔ زیر را برگزینید تا پنجرهٔ آن را ببینید:

Services

اکنون، می‌توان برنامه‌های کاری مایکروسافتی را با بهره‌گیری از گزینهٔ زیر پنهان کرد:

Hide All Microsoft Services

باید توجه داشت، اگر از رایانه در شبکه بهره نمی‌گیرید، می‌توان برخی از برنامه‌های کاری، مانند برنامه‌های کاری زیر را از کار انداخت:

Alerter – Clip Book – Computer Browser - …

۱۳-دسترسی محدود

اگر از نظام پرونده‌گردانی «NTFS» بهره می‌گیرید، می‌توان دسترسی به پرونده‌ها و پوشه‌ها را محدود کرد. برای انجامش این کار، روی پرونده یا پوشه‌ای که می‌خواهید دسترسی دیگران به آن امکان‌پذیر نباشد کلید راست ماوس را بفشرید و کارهای زیر را به ترتیب انجام دهید:

Properties, Advanced

اکنون پنجره‌ای با گزارهٔ آغازین زیر به نمایش درمی‌آید:

Advanced Attributes

در این پنجره، گزینهٔ زیر را برگزینید:

Encrypt Centents for secure data

و پایان کار را تأیید کنید. پس از آن، شاید پنجره‌ای با گزارهٔ آغازین زیر ببینید:

Confirm Attribute Change

در این پنجره، دو گزینهٔ زیر وجود دارند:

Apply changes to this folder only

Apply changes to this folder, subfolders and files

گزینهٔ دوم، گزینهٔ پیش‌گزیده است. با برگزیدن آن، می‌توان دسترسی به پوشه‌ها و پرونده‌های پوشه‌ها را برای دیگران امکان‌ناپذیر کرد. اکنون، اگر با نام کاربری دیگری بخواهید به این پوشه و پرونده‌های آن دسترسی یابید، پیامی می‌بینید که می‌گوید: نمی‌توان به آن دسترسی یافت.

۱۴-شماره‌گیری خودکار

برخی از برنامه‌ها از جمله برنامه‌های **هرزه‌نگار** می‌کوشند به اینترنت وصل شوند. برای رهایی از شماره‌گیری خودکار این گونه برنامه‌ها، می‌توان کارهای زیر را به ترتیب انجام داد:

Control Panel, Administrative Tools, Services

در پنجرهٔ سوی راست روی گزینهٔ زیر، کلید چپ ماوس را دوبار بفشرید:

Remote Access Auto Connection Manager

به بخش زیر بروید:

Startup type

و گزینهٔ زیر را برگزینید:

Disabled

۱۵-پیش‌واکشی [10]

ویندوز برای بازاجرای سریع برنامه‌ها، کارهای زیر را انجام می‌دهد:

الف- شیوهٔ بازاجرا: دانستنیهای لازم برای بازاجرای برنامه‌ها را در پرونده‌ای با پسوند «پی اف»، در پوشهٔ «پری‌فچ» [11] از پوشهٔ ویندوز می نویسد.

ب- شیوهٔ بازراه‌اندازی: دانستنیهای لازم برای بازراه‌اندازی برنامه‌ها، هنگام راه‌اندازی ویندوز را در پرونده‌ای با نام زیر، در پوشهٔ «پری‌فچ» از پوشهٔ ویندوز می‌نویسد:

NTOSBOOT-B00DFAAD.pf

چیدمان برنامه‌ها: دانستنیهای لازم برای فراخوانی شیوهٔ اجرا و شیوهٔ بازراه‌اندازی برنامه‌ها را در پرونده‌ی نوشتاری زیر، در پوشهٔ «پری‌فچ» از پوشهٔ ویندوز می‌نویسد:

Layout.ini

ت- لوفو [12]: ویندوز بر پایهٔ الگوریتم لوفو، پرونده‌های پوشهٔ «پری‌فچ» را نگه‌داری می‌کند.نام این الگوریتم، سرواژهٔ گزارهٔ زیر، به معنای «کمترین کاربرد، نخستین خروج» است:

---

[10] prefetch
[11] prefetch
[12] LUFO

Least Used First Out

این گزاره می‌نمایاند کم‌کاربردترین برنامه از فهرست «پری‌فچ» پاک می‌شود تا جا برای نوشتن پیشینهٔ برنامه‌های پرکاربرد و تازه باز شود؛ زیرا گنجایش پوشهٔ «پری‌فچ» از چند مگابایت بیشتر نیست.

ث- ویندوز هنگام کم‌کاری یا بی‌کاری محتوای این پوشه را بر پایهٔ داده‌های پروندهٔ چیدمان برنامه‌ها جابه‌جا می‌کند. بدین‌گونه، کاری مانند یک‌پارچه‌سازی[13] برنامه‌ها انجام می‌دهد.

بر پایهٔ آن‌چه گذشت، شماری معتقدند باید محتوای این پوشه را در بازه‌های زمانی پاک کرد، تا کارایی ویندوز افزایش یابد و بتوان برنامه را مناسبتر سامان داد؛ ولی برخی دیگر معتقدند تا زمانی رویداد ناگواری روی نداده است نباید محتوای این پوشه را پاک کرد. به هر حال، اگر بخواهید پرونده‌های این فهرست را پاک کنید، باید کارهای زیر را انجام دهید:

۱-در ویرایشگر رجیستری کارهای زیر را به ترتیب انجام دهید:

HKEY_LOCAL_MACHINE/
SYSTEM/ Current Control Set/ Control/
Session Management/ Prefetch Parameters

۲-در این جا، می‌توان شمار «واژهٔ دوگانه»[14] را بر پایهٔ جدول شمارهٔ «۲» نوشت.

بدین‌گونه، دانسته می‌شود:

۱-با دادن شمار صفر به واژهٔ دوگانه، می‌توان این ویژگی ویندوز را از کار انداخت؛

شمار	بازاجرا	بازراه‌اندازی
۰	–	–
۱	+	–
۲	–	+
۳	+	+

جدول ۲: فعال و نافعال‌سازی ویژگی پیش‌واکشی

۲-با دادن شمار «۱» به واژهٔ دوگانه، می‌توان این ویژگی را برای بازاجرای برنامه‌ها از کار انداخت؛

۳-با دادن شمار «۲» به واژهٔ دوگانه، می‌توان این ویژگی را برای بازراه‌اندازی برنامه‌ها از کار انداخت؛

۴- با دادن شمار «۳» به واژهٔ دوگانه، می‌توان این ویژگی را برای بازاجرا و بازراه‌اندازی برنامه‌ها به کار گرفت.

۱۶-پاکسازی گذرا

می‌توان پرونده‌های گذرای اینترنت اکسپلورر را پاک کرد و به ایمنی رایانه افزود. برای انجامیدن این کار، می‌توان کارهای زیر را به ترتیب انجام داد:

HKEY_LOCAL_MACHINE/
SOFTWARE/ Microsoft/ Windows/
CurrentVersion/ Internet Settings/ Cache

در پنجرهٔ سوی راست، دنبال واژهٔ زیر بگردید و به آن شمار صفر بدهید:

Persistent

ولی اگر آن را نیافتید آن را از گونه‌ی دودویی بسازید و به آن شمار صفر بدهید.

۱۷-برنامهٔ کاری پیام‌رسان

رخنه‌گران از برنامهٔ کاری پیام‌رسان ویندوز برای فرستادن پیامهای ناخواسته، مشهور به هرزنامه بهره می‌گیرند. برای رویارویی با این شیوهٔ کاری رخنه‌گران، می‌توان کارهای زیر را به ترتیب در ویرایشگر رجیستری ویندوز انجام داد:

HKEY_LOCAL_MACHINE/
SYSTEM/ CurrentControlSet/ Services/
Messenger

در این جا، از پنجرهٔ سوی راست دادهٔ زیر را بیابید و به آن شمار «۴» بدهید:

Start

۱۸-کاربر سرپرست[15]

رخنه‌گران می‌توانند با بهره‌گیری از توانایی کاربر سرپرست به آن یورش برند. برای پیشگیری از انجامیدن این کار، می‌توان از نام دیگری برای این کاربر بهره گرفت، بدون این که از توانایی‌های این کاربر کاسته شود. یعنی، به جای نام Administrator، می‌توان از نام دیگری بهره گرفت.□

[13] defragmentation
[14] DWORD
[15] administrator