

شناخت اجمالی فناوری های امنیت اطلاعات از دیدگاه های جرم شناسی رایانه ای و طبقه بندی آن ها

به بهانه مقدمه ای بر ارایه سلسله گزارشات فنی - تحلیلی اصول هک اخلاقی مدرن

مهندس علی کسرائی^(۱)

کلید واژه ها: فناوری امنیت داده، جرایم رایانه ای، طبقه بندی عملکردها، دانش علمی حفاظت از داده ها

مقدمه:

شکی نیست که پیرامون مباحث عمومی و مدیریتی امنیت اطلاعات، مقالات و سخنان بسیار رانده شده است. همچنین به این آمار، می توان، سمینارها و جلسات علمی برگزار شده در دانشگاه ها و مراکز پژوهشی - آموزشی کشور را نیز اضافه کرد. ولی کماکان، همه محققان را اتفاق نظر بر اینست که تمامی این تلاش ها، در نهایت به اصول تئوریک مسائل امنیتی اشاره دارد و تقریباً کمتر تلاشی برای ارائه موارد اجرایی و عملی آن، انجام شده است. اگر هم انجام شده، هیچ آماری از آن ها و نتایج کاریشان، در دسترس محققین نیست که بدان استناد شود. لذا بر آن شدیم تا این مهم را تا آنجا که توان امان اجازه دهد بر دیده ارائه گماریم؛ پس این سطور را به نوعی (گزارشی فنی - آماری) می کنیم؛ تا شاید خاتمه ای باشد بر سخنان قبلی و جمع بندی داده های عمومی - مدیریتی و مقدمه ای به نظر آید بر سرآغازی به سری جدید آگاهی ها و دستورالعمل های اجرایی کارآر. در این گزارش فنی اندیشه بر آن است که، لااقل چون معترفیم، بسیاری از مباحث اجرایی، احتیاج به لا براتوار دارد و... ولی نیز، معتقدیم که هنوز شماری از عزیزان، اصول اجرایی برقراری امنیت، در سطوح مختلف، بخصوص شبکه ها و همچنین هیچ گونه اطلاع صحیحی از این که: یک تیم امنیتی از لحاظ علمی و اجرایی، باید به چه ابزار و دانشی، مسلح باشند تا بتوانند، با انجام آزمون هایی از سیستم ها، نقاط آسیب پذیر آن را شناسایی، و به موقع، نسبت به مقابله با آن، عمل کنند را ندارند؛ بنابراین در نهایت خضوع اعلام می دارد، که با عنایت بر مطالبی که شرح آن ها گذشت، قصد بر آن شده که طی سلسله مقالاتی تحت عنوان (گزارشات فنی) به بهانه اطلاع رسانی علمی - اجرایی به خوانندگان، عزیزان را با اصول آکادمیک - اجرایی برقراری امنیت، آشنا ساخته و بتوانیم در عمل به ایجاد توانمندی بیشتری از امنیت در تحقیق و مطالعه نایل شویم. در خاتمه، معترفم این سلسله گزارشات فنی، به بررسی تحلیلی هک اخلاق مدارانه (Ethical Hacking)، خواهد پرداخت که در این وادی، خوانندگان گرامی را به آشنایی با دانش روز، در خصوص شناسایی و برخورد با جرائم کامپیوتری، رهنمون می سازد.

گر خطا گفتیم اصلاحش تو کن مصلحی تو ای تو سلطان سخن

به نظر نگارنده، شروع سخن، باید با ارائه تعریفی جامع، از (فناوری امنیت اطلاعات)، مناسب داشته باشد؛ چرا که تمامی اشارات مدیریتی و اجرایی به درک صحیح از این فناوری، بستگی مستقیم دارد.

تعاریف اولیه:

- (۱) فناوری به مجموعه دانش یا علمی اطلاق می گردد، که برای تولید و ساخت یک محصول، مورد مکاشفه و در نهایت، مورد استفاده قرار می گیرد.
 - (۲) امنیت اطلاعات نیز به نگهداری از داده ها و به حداقل رساندن خطر افشای آن ها، در بخش های بدون مجوز و غیر مجاز، اشاره دارد.
- بنابراین، فناوری امنیت اطلاعات، به استفاده مناسب از تمام فناوری های امنیتی به روز و پیشرفته به جهت

نگهداری و حفاظت از تمامیت اطلاعات، در شبکه‌ها (به عنوان مثال، اینترنت) اشاره دارد. اینترنت، یک شبکه عظیم اطلاع‌رسانی است که اهمیت بهره‌مندی از آن، در عصر حاضر، بر همگان مشهود است. این شبکه جهانی، حاصل اتصال هزاران شبکه کوچکتر است و در کمترین حد آن، ۶۰ میلیون رایانه، در عضویت شبانه‌روزی آن، ثبت شده است و می‌تواند انسان را در خصوص هدف اصلی شبکه، یعنی به اشتراک گذاشتن داده‌ها، کمک کند.

طبق آمار، بیش از ۲ میلیارد صفحه اینترنتی وجود دارد که همه آن‌ها، در این شبکه به ارائه اطلاعات حقیقی و حقوقی می‌پردازند. کارشناسان معتقدند که حمایت از جریان آزاد اطلاعات و بستر سازی مناسب برای این برقراری اتصال، شعار روز دولت‌ها در جهان است و این در حالیست که گستردگی و تنوع داده‌های مخرب و آلوده، روز به روز، بر نگرانی دولت‌ها و کشورها، می‌افزاید.

آری، بیم آن می‌رود که صدمات ناشی از هجوم این داده‌های مخرب، به تخریب مبانی اخلاقی و اجتماعی مردمان بیانجامد، که واکنش دولت‌ها نیز به این امر مهم اجتماعی، کاملاً منطقی و ضروری بنظر می‌رسد؛ چرا که هر جامعه‌ای مبانی اعتقادی و اجتماعی خود را داراست و عدم تفکر به این امر، سلامت روحی و امنیت جوامع را به خطر می‌اندازد.

هشدار به مسئولین کشور اعم از امنیتی - حراستی و IT:

امروزه، دستکاری‌های داده‌ها به عنوان طرحی عمیق و مهم از طرف سازمان‌های خرابکار بین‌المللی به منظور مختل کردن ساختار امنیت ملی، علیه دولت‌ها و ملت‌هایی چون ایران، روی کار است و حمایت می‌شود. کشور ما، نرم‌افزارهای اصلی از قبیل، سیستم‌های عامل و... مورد استفاده‌اش را از طریق واسطه‌های خارجی تهیه می‌کند. نگارنده به دفعات، در تحقیقات خود به حفره‌های امنیتی پرخطر در این محصولات، برخورد داشته است. در این محصولات، راه‌های ناامن بسیاری وجود دارد و بیم آن می‌رود، که به عنوان مثال، اگر از این محصولات در شبکه‌های (Online) بانکی و بسیاری از نهادها، استفاده شود، چه کسی و چگونه از نفوذ عوامل مخرب در این شبکه‌ها، جلوگیری خواهد کرد؟!

نفوذ و راه‌های مقابله با آن، در کشورها به مسئله‌ای استراتژیک، تبدیل شده و عدم توجه به آن، به دولت‌ها، خساراتی چشمگیر وارد می‌سازد. فرض اگر از طرف شرکت مایکروسافت، داده یا بسته امنیتی به سیستم‌ها، وارد شده و عملکرد کلیه سیستم‌ها را مختل نماید، آیا می‌دانید که چه خسارتی به امنیت ملی و اقتصاد ایران، وارد خواهد آمد؟ نکته پر اهمیت این‌که، همه کارشناسان نیک می‌دانند که شرکت (چک پوینت)، بزرگترین تولیدکننده ادوات امنیتی در جهان می‌باشد که شعبه اصلی آن در اسرائیل است، که متأسفانه از این محصولات به لحاظ کارایی بالای‌شان، در همه دستگاه‌های از امنیتی گرفته تا سازمانی، استفاده مزید بعمل می‌آید. البته، تاکنون گزارشی مبنی بر سوء استفاده‌های عوامل مخرب از این نرم‌افزارها، در جامعه علمی ارائه نشده است ولی بیم آن می‌رود که چون برخی از این فناوری‌ها، به صورت نرم‌افزاری، قابل خریداری نیستند، روزی کشورها را دچار خطر سازند. پس باید با حمایت از محققین فرزانه کشورمان، نسبت به ورود به درک، تحقیق و در نهایت تولید محصولات مشابه برای آینده کشورمان اهتمام ورزیده و اقدامات ملی صورت گیرد.

بررسی تیتروار سابقه امنیت شبکه:

- (۱) اینترنت در سال (۱۹۶۹) تحت عنوان شبکه‌های آرپانت، توسط وزارت دفاع آمریکا، پایه‌گذاری شد.
- (۲) با توجه به اشتراک گذاری داده‌ها، از همان ابتدا، به منظور جلوگیری از اثرات مخرب حملات اطلاعاتی، تدابیری اندیشیده شد.
- (۳) در سال (۱۹۷۱) تعداد زیادی از کامپیوترهای دانشگاه‌ها و مراکز دولتی به این شبکه، متصل شدند.
- (۴) یک حادثه غیرمنتظره در سال (۱۹۸۸)، آرپانت را لرزاند. رابرت مورس، دانشجویی در نیویورک بود؛ برنامه‌ای را نوشت که می‌توانست خود را در کامپیوترهای دیگر، تکثیر کند و بعدها به (کرم مورس) مشهور شد.
- (۵) حادثه مورس، (۸۸۰۰۰) رایانه را به خطر انداخت، بطوریکه در مدت کوتاهی، ۱۰٪ از رایانه‌های دولتی آمریکا، از کار افتادند.

(۶) به دنبال این حادثه، سازمان مقابله با مشکلات امنیت داده‌ها، تحت نام (IRST) شکل گرفت.

(۷) مهم‌ترین حوادث اختلال در امنیت آن روز عبارت بودند از:

- کرم WINK / OILS در سال (۱۹۸۹)
- (Sniff Packet) سال (۱۹۹۴) که با پست الکترونیک منتشر می‌شد و باعث افشای اطلاعات کاربران سیستم‌ها، می‌شد.
- و...

۸) سالها گذشت و اکنون هیچکس، بر تاثیر اینترنت را به عنوان برجسته‌ترین ویژگی فناوری اطلاعات و ارتباطات، منکر نیست.

به عنوان مثال پست الکترونیک و استفاده وسیع از آن، نمونه‌ای از لبه مثبت آن پیشرفت به شمار می‌آید. در این بین، سهولت دسترسی به اسناد و جستجوی نامحدود اطلاعات در اینترنت، بدون توجه به مرزهای جغرافیایی، خود یکی دیگر از دستاوردهای شبکه است. اما پیشرفت‌های فوق، لبه خطرناکی نیز دارد که خود از بزرگ‌ترین عوامل پیدایش عناوینی چون (جرائم رایانه‌ای) است که حاصل استفاده ناصحیح، از فناوری‌های جدید، در ارتکاب به جرم، به شمار می‌آید. بطوری‌که سرانجام، در سال (۲۰۰۱) با امضای مصوبات کنوانسیون بین‌المللی رایانه‌ای که به امضای (۳۰) کشور جهان رسید، دولت‌ها به قانونگذاری پیرامون مقابله با این جرائم پرداختند.

تعریف جرم رایانه‌ای:

با مراجعه به این منابع و مواخذ، به تعاریف متفاوتی از جرم در حیطه رایانه، مواجه شدیم که گاهی اوقات خیلی از آن‌ها را کامل نیافتیم، لذا نگارنده خود به ارائه تعریفی می‌پردازد تا جمیع جهات مطلب را در بر گیرد.

«هر نوع عملکردی در اینترنت، شبکه‌ها و... با استفاده از رایانه، مستقیماً یا بطور غیر مستقیم، منجر به نقض قوانین گردد و برای آن عمل در قانون، مجازات تعیین شده باشد (البته با توجه به نیازهای روز)، (جرم رایانه‌ای) نامیده می‌شود.

با استفاده به همان منابع که شرح‌شان گذشت، تاریخچه جرائم کامپیوتری را به ۳ دسته، می‌توان تقسیم کرد:

۱) نسل اول (Computer Crime) جرائم رایانه‌ای تا اواخر دهه (۱۹۸۰) که به جرائمی اطلاق می‌شدند که حیطه جرم، در رایانه و تجهیزات جانبی آن‌ها باشد. مانند: سرقت و کپی برداری از برنامه‌ها و در نهایت، سوء استفاده از حریم خصوصی افراد مثل سرقت آثار و تحقیقات آنان.

۲) نسل دوم (Crime Against Data) که تا اواخر دهه (۱۹۹۰) ادامه داشت. در این دسته از جرائم، از رایانه، به عنوان ابزار، جهت ارتکاب به جرم، استفاده می‌شد. مانند جرائمی علیه فناوری اطلاعاتی، ارتباطاتی، ماهواره‌ای و شبکه‌های بین‌المللی.

۳) نسل سوم (Cyber Crime) یا جرائم سایبر که از اواسط دهه (۱۹۹۰) شروع می‌شود که در متون علمی به (جرائم رایانه‌ای محض) نیز شهرت دارند. این گونه جرائم در دنیای مجازی به وقوع می‌پیوندند ولی آثار این ارتکاب، در دنیای واقعی مشهود می‌شود. مانند دسترسی غیر مجاز به سیستم‌های رایانه‌ای.

پیدایش جرائم رایانه‌ای:

هیچ دلیلی مبنی بر زمان دقیق پیدایش جرائم رایانه‌ای در دست نیست، چرا که این مورد خود به رشد و کاربرد فناوری‌های رایانه‌ای در کشورها، بستگی دارد و به دلیل این که این کاربردها، ابتدا به ساکن، در چند کشور در جهان مطرح است، امر تحقیق پیرامون این مطلب را سبب می‌کند. ولی طبق اطلاعات، در جامعه آمریکا، ماجرای رویس بود که برای اولین بار، اذهان عمومی را به جرائم کامپیوتری به شکل حقوقی، متوجه ساخت.

داستان رویس (بصورت تیتروار):

۱) آلدون رویس، حسابدار شرکتی بود که چون بنا به نظر شخصی، شرکت مزبور را در پرداخت حقوق و مزایا، به خود خائن می‌پنداشت، برنامه رایانه‌ای تهیه کرد که با انگیزه انتقام، منجر به اختلاس از پول‌های آن شرکت گردید.

۲) کلیه امور حسابداری شرکت مزبور به گونه ذخیره داده‌ها، بر روی نوارهای الکترونیکی بود. رویس با اضافه سازی دستورالعمل‌هایی به برنامه اصلی، قیمت‌های کالاها را تغییر می‌داد و مبالغ حاصل را به حساب‌های خصوصی واریز می‌کرد.

۳) وی در مدت ۶ سال، مبلغ یک میلیون دلار برداشت کرد.

۴) در نهایت چون نمی‌توانست مکانیزم این اختلال را متوقف نماید، خود را به مراجع قانونی، معرفی کرد.

۵) رویس به ۱۰ سال زندان محکوم شد و از این پس، در قوانین حقوقی، مباحثی چون تعریف جرائم رایانه‌ای، آغاز شد.

اشاره:

این‌که، در کنار بررسی مواردی چون جرائم رایانه‌ای و تاریخچه پیدایش آن، خالی از لطف نیست که بر پیامدهای

سازمانی فناوری اطلاعات نیز نظر افکنیم. چراکه بهره‌وری از این دانش در جهان، منجر به پیدایش دولت‌های الکترونیک، تجارت الکترونیک، بانکداری الکترونیک، آموزش الکترونیک، درمان الکترونیک و... شده است. ذکر این مطلب، نمای جامع تری از تقسیم‌بندی جرائم رایانه‌ای را ارائه می‌دهد که عبارتند از:

- الف) جرائم رایانه‌ای علیه اشخاص
 ب) جرائم رایانه‌ای علیه اموال و دارائی اشخاص یا جرائم اقتصادی
 ج) جرائم رایانه‌ای علیه دولت‌ها

در این جاست که ناخودآگاه، مسئله تهدیدات این فناوری نمایان می‌شود که به اختصار به ذکر عناوین آن می‌پردازیم.

- (۱) عوامل خارجی: مانند جنگ و عملیات نظامی، جاسوسی ملی، جاسوسی صنعتی و...
- (۲) تروریست‌ها و گروه‌های افراطی
- (۳) گروهک‌های جنایتکار سازمان یافته
- (۴) مجرمین عادی

بررسی عمده جرائم رایانه‌ای در ایران:

این بخش خود به ۲ دسته تقسیم می‌شود:

الف) کامپیوتر به عنوان ابزار ارتکاب

ب) جرائم سایبر یا محض که به اختصار به توضیح آنان می‌پردازیم:

• در خصوص بخش اول:

(۱) (جعل اسناد با استفاده از رایانه):

شامل استفاده از نرم افزارهای طراحی دیجیتال مانند فتوشاپ و غیره و بکارگیری چاپگرهای رنگی و اسکنرهای پیشرفته است که توسط مجرمین برای جعل اسکناس، مدارک اسناد تجاری و... مورد استفاده قرار می‌گیرد.

(۲) (کلاهبرداری از طریق شبکه‌های رایانه‌ای):

مانند برداشت مبلغ (۳۸۵) میلیون تومان از حساب‌های عابر بانک ملت توسط ۳ نفر در اهواز و همچنین فعالیت‌های موسسات مالی و اعتباری اعم از (Prime bank itd)، (My7 diamonds (Gold quest)، نیز، نمونه‌ای از این کلاهبرداری‌ها می‌باشد.

(۳) (آزار واذیت):

شامل دزدیدن نام‌های کاربری و کلمات عبور پست الکترونیک کاربران و ارسال نامه‌های تهدیدآمیز به دیگران، نسبت دادن فحشا و ارائه عکس‌های تلفیقی مستهجن به خانواده‌های افراد از این قبیل جرائم می‌باشند.

(۴) (اهانت به مقدسات دینی و اشاعه فحشا):

شامل راه‌اندازی سایتهای اینترنتی رواج فحشا و اهانت آمیز به مقدسات دینی و نظام جمهوری اسلامی ایران توسط مخالفین داخلی، خارجی یا افراد نا آگاه و منحرف است که به شدت در حال افزایش است.

• (در خصوص بخش ب)

(۱) (نقض حقوق تولیدکنندگان نرم افزارها):

بر طبق قانون، هر گونه تکثیر غیر مجاز نرم افزارهای ایرانی ثبت شده، جرم محسوب می‌شود. این در حالی است که با توجه به نقایص موجود در قوانین و همچنین عدم آشنایی قضات محترم و ضابطین ارجمند با مقوله فناوری اطلاعات، در حد یک متخصص در شاخه نرم افزار، موجبات دل‌سردی سرمایه‌گذاران داخلی را بوجود آورده است.

(۲) (نفوذ غیر مجاز به رایانه‌ها):

کارشناسان امر می‌دانند که سرورهای ایرانی مستقر در کشورهایی چون کانادا و آمریکا، قدر تاکنون، مورد حمله قرار گرفته‌ند. یکی از دلایل این امر را می‌توان، وجود سی‌دی‌های آموزشی فارسی زبانی دانست که مورد سوء استفاده بسیاری از جوانان نا آگاه جویای علم رایانه، قرار گرفته است. در مقاله‌ای، ارائه شده است که در آذرماه (۱۳۸۱)، بیش

از ۲۰۰ سایت ایرانی توسط هکری به نام (اسپایدرمن) و در دی ماه سال (۱۳۸۱) حدود ۱۸۰ سایت ایرانی توسط هکری به نام (مش قاسم) مورد حمله قرار گرفته و تخریب شده‌اند و در ادامه اشاره می‌کنند که در سال (۱۳۸۲) تعداد ۳۵۰ سایت ایرانی توسط هکری به نام (Defender man) هک شده که توسط مامورین معاونت آگاهی ناجا، شناسایی و دستگیر شد؛ همچنین هک شدن سیستم سیبای بانک ملی و برداشت غیر قانونی حدود ۶۰ میلیون تومان از حساب‌های مشتریان، یکی دیگر از آثار مخرب لبه ترسناک فناوری اطلاعات است که توسط نیروهای انتظامی کشف و شناسایی شد.

سخن آخر:

جمع بندی و نتیجه گیری تیتروار از عناوین، همچنین اشارتی کوتاه به اصول اولیه طبقه بندی در فناوری اطلاعات:

- مهم ترین مزیت و رسالت شبکه های رایانه ای، اشتراک منابع سخت افزاری و نرم افزاری و دستیابی سریع و آسان به داده ها است.

- کنترل دسترسی و نحوه استفاده از منابع اشتراکی، مهم ترین هدف یک نظام امنیتی عمیق در شبکه ها است.
- هر سازمان، به جهت حفاظت در داده هایش باید به یک راهبرد خاص پایبند باشد و بر اساس آن نظام امنیتی را اعمال کند.

- بدین دلایل از سرویس های امنیتی استفاده می شود.
- سرویس های امنیتی، باید پتانسیل لازم در خصوص ایجاد یک نظام امنیتی مناسب به جهت تشخیص به موقع حملات و ارائه واکنش سریع را دارا باشد.

- بنابراین، محورهای راهبری در این مقوله را به ۳ مولفه می توان استوار دانست:

(۱) حفاظت

(۲) تشخیص

(۳) واکنش

- با استناد بر تعریف ارائه شده از فناوری امنیت اطلاعات، در ابتدای این گزارش، عملکرد قبل یا بعد از وقوع تهدیدات را به ۲ دسته می توان طبقه بندی کرد:

الف) کنشی: به اعمال پیشگیرانه قبل از وقوع یک مشکل امنیتی خاص، اشاره دارد.

ب) واکنشی: که به عکس العمل های لازم پس از وقوع یک مشکل خاص امنیتی اشاره دارد.

اقدامات کنشی به اختصار به بررسی، کنترل و انتخاب راهبردهای مناسب امنیتی، پیرامون مباحث ذیل اشاره دارد:

(۱) رمز نگاری

(۲) امضای دیجیتالی

(۳) گواهی نامه های دیجیتالی

(۴) شبکه های مجازی

(۵) نرم افزارهای آسیب نما

(۶) آنتی ویروس ها

(۷) پروتکل های امنیتی

(۸) سخت افزارهای امنیتی

(۹) Box های توسعه نرم افزارهای امنیتی

× اقدامات واکنشی نیز به بررسی و کنترل های راهبردی امنیتی، پیرامون مباحث ذیل اشاره دارد:

(۱) دیوار آتش یا فایروال ها

(۲) کنترل دسترسی ها

(۳) بررسی کلمات عبور

(۴) زیست سنجی (شامل فناوری هایی جهت سنجش و تحلیل ویژگی های بدن انسان مانند اثر انگشت، قرنيه و شبکیه چشم و...)

(۵) نظام های آشکار ساز نفوذ در شبکه ها

(۶) مستند سازی

(۷) کنترل دسترسی از راه دور

- با عنایت بر مطالبی که شرح‌شان گذشت، سیستم‌های کاربردی، علمی، اجرایی و امنیتی تحت عناوین مختلف و توسط شرکت‌های امنیتی تولیدی مختلفی، ارائه شده است.
 - نگارنده این سطور، یکی از طرح درس‌های امنیتی ارائه شده توسط شرکت (Ec-Council) را انتخاب کرده است که در گزارشات فنی بعدی، به شرح مفصل، اما کاربردی همه آن موارد می‌پردازد.
 - در آن سلسله گزارشات فنی مورد بحث، بطور کلی به بررسی توانمندی‌های علمی یک تیم امنیتی اشاره می‌شود که در عمل، جهت مقابله با تهدیدات مذکور، بدان نیازمند است.
- موارد مذکور عبارتند از:

- (۱) شناسایی علمی مباحث هک و انواع حملات
- (۲) شناسایی رایانه‌ها
- (۳) توانایی اسکن شبکه‌ها در موارد مختلف و شناخت انواع حملات مبتنی بر اسکن
- (۴) مستندسازی پیشرفته
- (۵) شناسایی انواع هک کردن سیستم‌ها
- (۶) شناخت تروژن‌ها و بک‌دورها
- (۷) شناسایی اسنifferها
- (۸) درک مکانیزم سرویس‌های عدم انکار
- (۹) درک مفاهیم مهندسی اجتماعی
- (۱۰) درک لایه‌های دزدی رایانه‌ای
- (۱۱) درک مفاهیم هک وب سرورها
- (۱۲) درک آسیب پذیری برنامه‌های تحت وب
- (۱۳) درک تکنیک‌های پایه مبتنی بر کراک پسوردهای وب
- (۱۴) درک مفاهیم بنیادی (SQL Injection)
- (۱۵) درک هک کردن شبکه‌های بی سیم
- (۱۶) شناسایی ویروس‌ها و آشنایی با مکانیزم اثرات آن‌ها
- (۱۷) امنیت فیزیکی
- (۱۸) آشنایی با حملات مبتنی بر هک لینوکس
- (۱۹) گریز از فایروال‌ها، IDSها و Hony Pots
- (۲۰) شناسایی با مکانیزم هک‌های مبتنی بر سرریزی بافرها
- (۲۱) آشنایی با اصول رمزنگاری
- (۲۲) توانایی اجرای تست‌های نفوذ (Penetration testing)

در پایان اعتقاد بر آنست که خوانندگان گرامی می‌بایست از اصول شناخت و برپاسازی شبکه‌ها، همچنین نظام علمی حاکم بر آنان، از اطلاعات وافی برخوردار باشند. چراکه در گزارشات فنی آینده کمتر به مباحث عمومی می‌پردازیم و تمرکز سطور ارائه شده، بر مباحث فنی خواهد بود.

منابع:

- باستانی، برومند. جرائم کامپیوتری و اینترنتی، چاپ بهنامی، سال ۱۳۸۳ ص ۲۷
- بابازاده، قاسم. پیرامون کنوانسیون اروپائی جرائم کامپیوتری، شورای عالی انفورماتیک شماره ۸۱
- سازمان ملل. نشریه بین‌المللی سیاست جنائی، ترجمه دبیرخانه شورای عالی انفورماتیک، ۱۳۷۶
- پرویزی، رضا (۱۳۸۱) جرائم کامپیوتری و اینترنتی، نشریه آسیا
- دانش‌کیا، ماهرخ (۱۳۸۳) گسترش جرائم اینترنتی و رایانه‌ای، نشریه صدای عدالت
- حاتمی، سوگل (۱۳۸۵) اجرای طرح ویژه مبارزه با جرایم رایانه‌ای، روزنامه جهان اقتصاد
- دنیای اقتصاد (دی ۸۱) پیشگیری یا برخورد گفتگو با رضا پرویزی دبیر کمیته مبارزه با جرائم رایانه‌ای و اینترنتی
- دیداری، اکرم (۱۳۸۱) جنگ آخر، جرائم رایانه‌ای ۶۴ در صد رشد سالانه، نشریه دنیای اقتصاد

• پیش نویس طرح قانونی جرم کامپیوتری، مقررات

Director, Computer Security Institute

• به منظور نگارش سلسله گزارشات فنی آینده، برای تبادل اطلاعات و اخذ مآخذ به روز امنیتی، با موسسات، محققان و سازمان‌های بسیاری مکاتبه شده است که جهت آشنایی و اطلاع محققان گرامی، به ذکر نامشان اکتفا می‌گردد:

" Frank Abagnale - Abagnale and Associates
Author of 'Catch Me if You Can', Lecturer, Consultant,
National Cyber Security Alliance spokesman

" Prof. Matt Bishop - University of California Davis
Computer Security Professor, Author of 'Computer Security:
Art and Science'

" LTC Dr. Andrew Glen - United States Military Academy
Associate Professor, Department of Mathematical Sciences

" Dr. Simon Jackman - Stanford University
Political Science and Statistics Professor

" Dr. Nimrod Kozlovski - Yale University,
Computer Science Department, Adjunct Professor of Law at
New York Law School,
Author of 'The Computer and the Legal Process'

" Kevin Mitnick - Mitnick Security Consulting
Author, Public Speaker, Consultant, and Former Computer
Hacker

" Dr. Tom Piazza - University of California Berkeley
Senior Sampling Statistician, Survey Research Center

" Dr. Sam Sander - Clemson University
Computer Engineering Professor

" Dr. Eugene Spafford - Purdue University
Computer Security Professor, CISSP, ISSA Hall of Fame,
security advisor to Presidents Bill Clinton and George W Bush

" Paul Williams - Gray Hat Research
Chief Technology Officer, MCSE, NSA IAM and IEM

" Ray Yepes - Computer Security Consultant
CISSP, MCSE, MCP, NSA IAM and IEM, Homeland Security
level 5, CCNP, CCSP

نرم افزار جامع

دبیرخانه ایمگانی

سیستم مکانیزه ثبت نامه،
آرشیو پرونده، اسناد، عکس،
صدا، فیلم، کتاب، مجله، سی دی، نوار و ...
دارای تقویم شمسی و امکانات فارسی
برای ویندوزهای ۹۵، ۹۸، XP و ۲۰۰۰

www.sinapardazeshsoft.com

- ثبت نامه های وارده و صادره - وارده از صادره و صادره از وارده
- امکان تفکیک نامه های پستی - فکسی - دستی و پست الکترونیکی
- ورود اطلاعات نامه ها در کمترین زمان و بدون نیاز به استفاده از ماوس
- جستجوی سریع در میان نامه های ثبت شده به دو صورت ساده و کامل
- گزارش گیری متنوع از مطالب ثبت شده
- امکان گروه بندی نامه ها و شماره سریال مختص به هر گروه
- امکان ثبت رونوشت نامه ها به هر تعداد
- ثبت ارجاعات نامه ها به تعداد دلخواه با ساعت و تاریخ ارجاع همراه با ثبت اقدامات انجام شده
- دارای کار تابل خاص برای هر کاربر (در نسخه شبکه)
- امکان ثبت نامه توسط دو یا چند کاربر به طور همزمان (در نسخه شبکه)
- دارای امکان اسکن نامه ها به هر تعداد صفحه و بدون نیاز به اختصاص نام به فایل های اسکن شده
- دسترسی به برنامه word جهت تایپ نامه ها بدون نیاز به اختصاص نام به فایل های ایجاد شده
- ارسال یک نامه به دسته ای از مخاطبین همراه با سابقه ارسال
- چاپ فرم ادغام پستی با درج تاریخ، شماره ثبت، پیوست، فرستنده، گیرنده و عنوان نامه به صورت خودکار
- چاپ آدرس و مشخصات مخاطبین بر روی پاکت از روی فرم ادغام پستی
- ایجاد پرونده به تعداد نامحدود و ارتباط خودکار با قسمت های مختلف برنامه
- دارای دفتر تلفن گسترده همراه با جستجوی آسان
- نمایش محتویات پرونده و دسته بندی موضوعات و اختصاص شماره برگه به هر کدام
- استفاده گسترده از صفحه کلید و بدون نیاز از ماوس
- ثبت و دسته بندی موضوعات مختلف شامل مخاطبین، پرونده های کامپیوتری، کتاب، مجله، نوار و
- دسترسی به سیستم درس طرح مختلف امنیتی (مدیر، کاربر و گزارش گیر و
- دارای سیستم پشتیبان گیری دستی و خودکار بر روی هارد یا کارت های حافظه
- محیط کاملاً فارسی و دارای نمایش راهنمای استفاده از بخش ها
- امکان نصب بر روی ویندوزهای ۲۰۰۰ - ایکس پی و ۲۰۰۳
- و امکانات ویژه دیگر

تهیه شده جهت سازمانها،

ادارات دولتی، شرکتها، موسسات خصوصی

www.sinapardazeshsoft.com



نرم افزار سیپاردازش

صندوق پستی: ۱۵۸۷۵/۹۶۶۳
واحد پشتیبانی: ۸۸۴۲۳۵۷۲ (خط ۵)
دفتر فروش: ۸۸۴۳۹۰۲۶ (خط ۵)
روابط عمومی: ۸۸۴۵۲۷۳۵
فکس: ۸۸۴۳۵۷۰۶

info@sinapardazeshsoft.com

پخش کننده های فعال از تهران
تهرانستان ها و بخش های فارسی زبان