واژه‌نامه امنیت سایبر

Iranian Council For Defending The Truth

درباره واژه‌نامه

این واژه نامه به عنوان مقدمه‌ای بر آشنایی با اصطلاحات و مفاهیم استراتژیک، عملیاتی و تاکتیکی مورد استفاده در شاخه علمی امنیت سایبر تهیه و تنظیم شده است. این واژه‌نامه به هیچ وجه کامل نبوده و تنها بخش اندکی از پرکاربردترین اصطلاحاتی را در بر می‌گیرد که هر پژوهشگر آکادمیک و مخاطب این حوزه احتیاج دارد تا از آنها شناخت اولیه‌ای داشته باشد.

از آن جایی که حوزه امنیت سایبر پیوندی میان‌رشته‌ای با دو حوزه فنی و نظری برقرار می‌کند، مفاهیم آن نیز ترکیبی از علوم کامپیوتر و علوم اجتماعی (امنیت‌پژوهی) است؛ فلذا حداکثر تلاش خود را نموده‌ایم تا مفاهیم و عبارات گردآوری شده بر اساس همین نظم، عمده نیاز پژوهشگران و مخاطبان را بر طرف سازد.

نویسنده: محمدجواد یزدانی

ICDT.iR

مفاهیم و اصطلاحات فنی

علوم رایانه

مکانیسم کنترل دسترسی (Access Control Mechanism)

پادمان‌های امنیتی (یعنی ویژگی‌های سخت‌افزاری و نرم‌افزاری، کنترل‌های فیزیکی، رویه‌های عملیاتی، رویه‌های مدیریت، و ترکیب‌های گوناگونی از این موارد) که برای شناسایی اجازه دسترسی مجاز و رد دسترسی غیرمجاز به یک سیستم اطلاعاتی طراحی شده‌اند.

شبکه تک‌کاره (Ad Hoc)

یک شبکه بی سیم که به صورت پویا دستگاه های سرویس گیرنده بی سیم را بدون استفاده از دستگاه زیرساختی مانند یک نقطه دسترسی (Access Point) یا یک ایستگاه پایه به یکدیگر متصل می‌کند.

افزونه امنیتی (Add-on Security)

ادغام پادمان‌های جدید سخت افزاری، نرم افزاری، یا سفت‌افزار (Firmware) در یک سیستم اطلاعات عملیاتی.

حمله روز صفر (Zero-day attack)

یک حمله یا تهدید رایانه‌ای است که از یک آسیب‌پذیری در یک نرم‌افزار کاربردی که تا پیش از آن ناشناخته بوده‌است بهره‌جویی می‌کند. این بدان معناست که توسعه‌دهندگان برای رفع آسیب‌پذیری صفر روز فرصت داشته‌اند.

پشتیبان (Backup)

تهیه یک نسخه تکراری از داده ها بر روی یک دستگاه ذخیره سازی فیزیکی اختصاصی یا ذخیره سازی در فضای آنلاین/ابری. نسخه پشتیبان در برابر از دست دادن اطلاعات کاربران را بیمه می‌کند. با یک نسخه پشتیبان می توان فایل های داده های آسیب دیده یا از دست رفته را بازیابی کرد. پشتیبان گیری باید به طور منظم و دوره ای مانند روزانه ایجاد شود.

درِ پشتی یا بَک‌دُر (Backdoor)

در علوم رایانه به راهی گفته می‌شود که بتوان از آن بدونِ اجازه به قسمت/قسمت‌های مشخصی از یک سامانهٔ دیگر مانند رایانه، دیوار آتش، یا افزاره‌های دیگر دست پیدا کرد. درهای پشتی ممکن است از قبل در سامانه وجود داشته باشند یا اینکه فرد نفوذگر با فریب کاربر، او را نسبت به نصب در پشتی ترغیب کند (مانند ارسال پیوست‌های آلوده در رایانامه).

رمزنگاری قالبی (Block Cipher)

نوعی الگوریتم رمزگذاری متقارن که داده ها را به بخش هایی با طول ثابت تقسیم می کند و سپس عملیات رمزگذاری یا رمزگشایی را در هر بلوک انجام می دهد. عمل تقسیم یک مجموعه داده به بلوک ها، الگوریتم را قادر می سازد تا داده ها را با هر اندازه ای رمزگذاری کند.

مفاهیم و اصطلاحات فنی

علوم رایانه

باتنت (Botnet)

اصطلاحی که از «robot network» گرفته شده است. یک شبکه بزرگ و خودکار از رایانه‌های پخش‌شده می‌باشد که قبلاً در معرض خطر قرار گرفته‌اند و می‌توان به طور همزمان برای انجام حملات در مقیاس بزرگ به قربانیان تحت کنترل گرفت.

باگ یا اشکال (Bug)

یک خطا یا اشتباه در کدنویسی نرم افزار یا طراحی یا ساخت سخت افزار. یک باگ نشان دهنده یک نقص یا آسیب پذیری در یک سیستم است که توسط مهاجمان قابل کشف می‌باشد

Clickjacking

تکنیک مخربی که توسط آن قربانی فریب داده می شود تا روی یک URL، دکمه یا شیئی از صفحه نمایش غیر از آنچه که کاربر در نظر گرفته یا ملاحظه می کند، کلیک نماید. این عمل را می توان به روش های مختلفی انجام داد. یکی از آنها این است که یک صفحه وب را بدون آگاهی کاربر پشت صفحه قابل مشاهده اصلی بارگذاری کنید، به گونه ای که لینک ها و اشیاء مشهود قبال انتخاب، نمای ظاهری هستند؛ بنابراین کلیک بر روی یک پیوند مشهود در واقع باعث می شود که پیوندِ صفحهٔ پنهان انتخاب شود.

کراکر (Cracker)

اصطلاح مناسب برای اشاره به مهاجم غیرمجاز به رایانه ها و شبکه ها به جای اصطلاح نادرست "هکر".

نقض داده (Data Breach)

افشای اطلاعات محرمانه، دسترسی به اطلاعات محرمانه، تخریب داده‌های باارزش یا استفاده سوء از یک محیط IT خصوصی. به طور کلی، نقض داده منجر به ایجاد دسترسی غیرمجاز به داده‌های داخلی برای نهادهای بیگانه می‌شود.

صحت داده (Data Integrity)

یک ویژگی امنیتی است که تأیید می کند داده ها اصلاح نشده و به عبارتی اصیل، کامل و دست نخورده هستند. صحت سنجی داده با استفاده از هش رمزنگاری انجام می شود.

داده کاوی (Data Mining)

فعالیت تجزیه و تحلیل و/یا جستجو در میان داده ها به منظور یافتن موارد مرتبط، با اهمیت یا ارزشمند. نتایج داده کاوی با نام متا داده شناخته می شود.

حملهٔ محروم‌سازی از سرویس یا حملهٔ بندآوری خدمات (DDoS)

حمله ای که تلاش می کند دسترسی و استفاده از یک منبع را مسدود کند. در واقع نوعی اختلال در دسترسی به شبکه است. DDOS گونه‌ای از حمله DoS است و شامل سیل حملات و فرسوده نمودن اتصال(کانکشن) می‌باشد. وجه

مفاهیم و اصطلاحات فنی

علوم رایانه

تمایز DDOS از DOS در این است که ترافیک حمله ممکن است از منابع متعددی منشا گرفته یا در سیستم‌های واسطه‌ای متعدد منعکس شود.

اکسپلویت (Exploit)

استفاده کامل از یک آسیب پذیری به نفع یک مهاجم. اکسپلویت، یا همان کدهای مخرب، برنامه‌ها و کدهایی هستند که توسط یک یا چند هکر یا محقق امنیتی برای اثبات یا استفاده از آسیب‌پذیری امنیتی خاصی در یک نرم‌افزار، سیستم‌عامل یا سخت‌افزار خاص نوشته می‌شوند. این برنامه‌ها لزوما برای خرابکاری نوشته و منتشر نمی‌شوند، اهداف تحقیقاتی و آموزشی را نیز دنبال می‌نمایند.

IDS (سیستم تشخیص نفوذ)

یک ابزار امنیتی است که فعالیت‌های امنیتی شبکه و میزبان (هاست) را برای شناسایی الگوهای مشکوک بازرسی می‌کند تا حمله به شبکه یا سیستم را نمایان سازد. IDS یک ابزار امنیتی منفعل می‌باشد.

IPS (سیستم جلوگیری از نفوذ)

یک ابزار امنیتی است که تلاش می کند مهاجمین به شبکه را شناسایی کند و سپس از موفقیت آمیز شدن آن حمله جلوگیری کند. IPS یک ابزار امنیتی کنشگر می‌باشد زیرا تلاش می کند به طور فعال به تهدیدات بالقوه پاسخ دهد. یک IPS می تواند آدرس های IP و پورت‌ها را مسدود ، خدمات را قطع، و همچنین به مدیران (اَدمین‌ها) اطلاع‌رسانی کند.

آدرس آی پی (IP address)

یک عدد باینری منحصربفرد که برای شناسایی دستگاه‌ها در شبکه TCP/IP استفاده می‌شود.

پارازیت (۱ – (Jamming)

حمله‌ای که در آن از یک دستگاه برای انتشار انرژی الکترومغناطیسی در فرکانس شبکه بی سیم استفاده می شود تا آن را غیرقابل استفاده کند. ۲) حمله ای که سعی در تداخل در دریافت ارتباطات رادیویی دارد.

کی لاگر (Keylogger)

هر ابزاری که به وسیله آن ضربات صفحه کلید قربانی در هنگام تایپ ثبت و ذخیره می شود. کی لاگر می‌تواند یک نرم‌افزار یا یک دستگاه سخت‌افزاری باشد که برای ضبط هر چیزی که کاربر ممکن است تایپ کند، از جمله رمز عبور، پاسخ به سؤالات مخفی یا جزئیات و اطلاعات مربوط به ایمیل‌ها، چت‌ها و اسناد استفاده می‌شود.

بد افزار (Malware)

از ترکیب دو کلمه malicious و software به‌دست آمده است. بدافزار، نرم‌افزاری است که معمولاً با نیت سوء به قصد ایجاد اختلال در عملیاتهای رایانه‌ای یا به دست آوردن بدون رضایت اطلاعات محرمانه توسط هکرها ایجاد و استفاده می‌شود.

مفاهیم و اصطلاحات فنی

علوم رایانه

پچ (وصله) (Patch)

یک به روز رسانی برای یک سیستم عامل، اپلیکیشن، یا سایر نرم افزارها که به منظور اصلاح مشکلات خاص نرم افزاری منتشر شده است. گاهی اوقات در برخی از نسخه‌های پچ‌ها، ویژگی‌ها و قابلیت‌های جدید نیز معرفی می‌شوند.

تست نفوذپذیری (Penetration testing)

یک روش ارزیابی میزان اثربخشی اقدامات دفاعی-امنیتی که در آن ارزیابان تلاش می کنند تا ویژگی های امنیتی یک سیستم اطلاعاتی را به تقلید از مهاجمان واقعی دور بزنند یا شکست دهند.

باج افزار (Ransomware)

نوعی بدافزار که معمولاً از طریق رمزگذاری قوی، داده های قربانی را در رایانه خودشان گروگان نگه می دارد. پس از آن، از کاربر تقاضا پرداخت باج به شکل بیت کوین (یک ارز دیجیتال غیرقابل ردیابی) به منظور آزاد کردن کنترل داده های غنیمت گرفته شده انجام می‌شود.

جاسوس‌افزار (Spyware)

نوعی بدافزار که فعالیت های کاربر را رصد می کند و آنها را به یک شخص ثالث خارجی گزارش می دهد. نرم افزارهای جاسوسی می توانند قانونی و مشروع باشند برای مثال در صورتی که توسط یک آژانس تبلیغاتی و بازاریابی با هدف جمع آوری اطلاعات جمعیتی مشتریان به کار گرفته شود. با این حال، جاسوس‌افزارها می‌توانند توسط مهاجمان به واسطه جمع‌آوری داده‌ها به منظور سرقت هویت یا اطلاعات کافی در مورد قربانی برای آسیب رساندن به آنها از راه‌های دیگر مورد استفاده قرار گیرند.

اسب تروا (تروجان) (Trojan Horse)

نوعی بدافزار که یک محموله آسیب‌زننده در داخل یک فایل میزبان بی‌خطر جاسازی شده است. قربانی فریب خورده و باور می‌کند که فایل مذکور، میزبانی بی‌خطر و قابل مشاهده است. با این حال، زمانی که قربانی از فایل میزبان استفاده می کند، محموله مخرب به طور خودکار بر روی سیستم کامپیوتری او بارگذاری می شود. برخلاف ویروس ها، آنها خودشان را تکثیر نمی کنند، اما می توانند به همان اندازه برای یک کامپیوتر مخرب باشند.

مفاهیم و اصطلاحات فنی

علوم پدافندی

حمله فعال (Active Attack)

حمله ای که یک سیستم یا داده را تغییر می دهد.

جنگ سایبری (Cyber warfare)

فعالیت‌هایی که توسط سازمان‌های نظامی با هدف تهدید بقا و رفاه جامعه/نهادهای خارجی پشتیبانی می‌شوند.

هانی‌پات (گلدان عسل- Honeypot)

یک تله برای مهاجمان است. هانی‌پات با نیت گیج نمودن مهاجمان به منظور جلوگیری از حمله آنها به سیستم‌های تولید واقعی استفاده می شود. هانی‌پات یک سیستم کاذب است که به گونه‌ای پیکربندی شده است که به عنوان یک سیستم تولیدی به نظر برسد و عمل کند و در جایی قرار می گیرد که مهاجم با آن مواجه شود. یک هانی‌پات ممکن است حاوی داده های نادرست باشد تا مهاجمان را فریب دهد و زمان و تلاش قابل توجهی را برای حمله و بهره برداری از سیستم جعلی صرف کنند. هانی‌پات همچنین بعضی مواقع می‌تواند حملات جدید یا هویت مهاجمان را نیز کشف کند.

شبیه‌سازی هویت (Identity Cloning)

شکلی از سرقت هویت که در آن مهاجم، هویت یک قربانی را می گیرد و سپس سعی می کند به عنوان هویت دزدیده شده زندگی و عمل کند. شبیه سازی هویت اغلب به منظور پنهان کردن کشور مبدأ یا سابقه کیفری مهاجم انجام می شود.

کلاهبرداری (جعل) هویت (Identity Fraud)

شکلی از سرقت هویت که در آن یک معامله، معمولاً مالی، با استفاده از هویت دزدیده شده یک فرد دیگر انجام می شود. در این کلاهبرداری مهاجم وانمود می‌کند شخص دیگری است.

حملهٔ شخص میانی (یا حملهٔ ژانوس) (Man-in-the-middle attack)

حمله‌ای که به پروتکل احراز هویت انجام می‌شود به این نحو که مهاجم خود را بین کلایمنت (ادعاکننده) و تأییدکننده قرار می‌دهد تا بتواند داده‌هایی را که بین آنها جایه‌جا می‌شود، رهگیری و تغییر دهد. به عبارتی دیگر یک راهبرد تهاجمی (و نوعی شنود فعال) است که در آن مهاجم جریان ارتباطی بین دو جزء (عضو) از سیستم هدف را رهگیری می‌کند و سپس نفوذگر را در ترافیک بین دو جزء جایگذاری می‌کند و در نهایت کنترل ارتباطات را به دست می‌گیرد.

فیشینگ (Phishing)

یک حمله دسته جمعی است که سعی در جمع آوری اطلاعات از قربانیان دارد. حملات فیشینگ می‌تواند از طریق ایمیل، پیام‌های متنی، شبکه‌های اجتماعی یا به واسطه اپلیکیشن‌های گوشی هوشمند انجام شود. هدف حمله فیشینگ دانستن اطلاعات ورود به سیستم، اطلاعات کارت اعتباری، جزئیات پیکربندی سیستم یا سایر اطلاعات مربوط به شرکت، شبکه، کامپیوتر یا هویت شخصی می‌باشد. حملات فیشینگ اغلب موفقیت آمیز هستند، زیرا نحوه

مفاهیم و اصطلاحات فنی

علوم پدافندی

مکاتبات نهادها یا گروه های مورد اعتماد را تقلید می کنند مانند ارسال ایمیل های جعلی از یک بانک یا یک وب سایت خرده فروشی.

اسنیفینگ (حمله بویش یا حمله بویشگر – Sniffing)

فرآیندی که طی آن داده‌های عبوری از یک شبکه ضبط یا نظارت می شوند. وقتی داده ها در بین شبکه ها انتقال می یابند، اگر بسته های داده رمزگذاری نباشند، داده های درون بستهٔ شبکه می توانند با استفاده از sniffer (برنامه‌ای با هدف ضبط بسته های شبکه) خوانده شوند.

مفاهیم و اصطلاحات نظری

تست امنیتی فعال (Active Security Testing)

تست امنیتی است که شامل تعامل مستقیم با یک هدف می‌باشد.

امنیت بسنده (Adequate Security)

امنیت متناسب با خطر و میزان آسیب ناشی از فقدان، سوء استفاده، یا دسترسی غیرمجاز یا تغییر اطلاعات.

استاندارد رمزنگاری پیشرفته (AES)

"استاندارد رمزنگاری پیشرفته" یک الگوریتم رمزگذاری مورد تایید دولت ایالات متحده می‌باشد که برای محافظت از داده های الکترونیکی استفاده می‌شود. الگوریتم AES یک رمزنگاری قالبی متقارن است که می تواند اطلاعات را رمزگذاری و رمزگشایی کند.

تهدیدات پایدار پیشرفته (APT)

یک رخنه امنیتی که مهاجم را قادر می‌سازد تا برای مدت طولانی به سیستم دسترسی یا بر آن کنترل داشته باشد؛ معمولاً بدون اینکه صاحب سیستم از تعدی به آن آگاه باشد. یک APT اغلب از آسیب‌پذیری‌های ناشناخته متعدد یا حملات روز صفر استفاده می‌کند، که به مهاجم اجازه می‌دهد حتی با مسدود شدن برخی از مسیرهای حمله، دسترسی به هدف را حفظ کند.

احراز هویت (Authentication)

عمل تأیید هویت یک کاربر و واجد شرایط بودن کاربر برای دسترسی به اطلاعات رایانه ای

* **توجه:** احراز هویت برای محافظت در برابر ورود تقلبی به سیستم طراحی شده است. همچنین می تواند به تأیید صحت داده اشاره کند.

مدارک قانونی کامپیوتری

به کارگیری روش علمی در رسانه های دیجیتال به منظور فراهم کردن اطلاعات واقعی برای بررسی قضایی

* **نکته:** این فرآیند اغلب شامل بررسی سیستم‌های رایانه‌ای به قصد تشخیص اینکه آیا آنها برای فعالیت‌های غیرقانونی یا غیرمجاز استفاده شده‌اند یا خیر. به عنوان یک رشته علمی، اصول قضائی و علوم رایانه را جهت جمع‌آوری و تجزیه و تحلیل داده‌ها از سیستم‌های اطلاعاتی (مانند رایانه‌های شخصی، شبکه‌ها، ارتباطات بی‌سیم و دستگاه‌های ذخیره‌سازی دیجیتال) به گونه‌ای ترکیب می‌کند که به عنوان مدرک در دادگاه قابل قبول باشد.

رمزنگاری (Cryptography)

هنر یا علم مربوط به اصول، ابزارها و روش‌های غیرقابل فهم کردن اطلاعات ساده و بازگرداندن اطلاعات رمزگذاری شده به شکل قابل فهم. رمزنگاری شامل سه جزء اصلی است: رمزگذاری متقارن، رمزگذاری نامتقارن و هَشینگ.

مفاهیم و اصطلاحات نظری

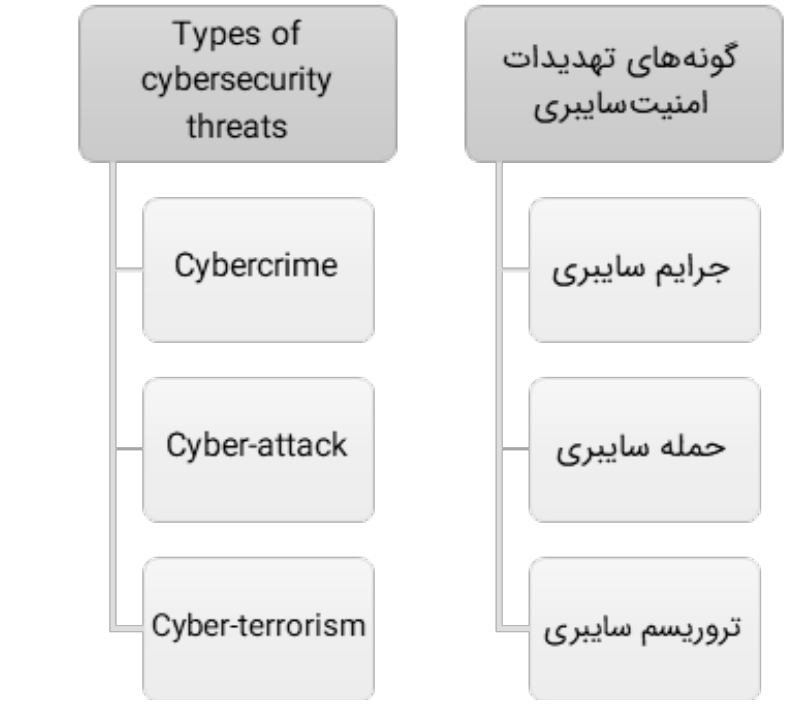
هکر (Hacker)

شخصی که دانش و مهارت در تجزیه و تحلیل کد برنامه یا یک سیستم کامپیوتری، تغییر عملکردها یا اعمال آن و تغییر توانایی ها و قابلیت های آن دارد. یک هکر ممکن است اخلاقی و مجاز باشد (تعریف اصلی) یا ممکن است مخرب و غیرمجاز باشد (استفاده تغییر یافته اما فعلی از این اصطلاح).

هکتویسم (Hacktivism)

مهاجمانی که به خاطر یک جنبش یا باور به جای برخی از اشکال منافع شخصی هک می کنند. هکتیویسم اغلب توسط مهاجمان به عنوان نوعی اعتراض یا مبارزه برای "حق" یا "عدالت" خود در نظر گرفته می شود. با این حال، این یک اقدام غیرقانونی است.

مفاهیم و اصطلاحات نظری



کتابشناسی

the Common Language Initiative Team, a subcommittee of the Transportation Systems Sector Cyber . (n.d.). Common Cyber Security Language. Retrieved from https://transops.s۳.amazonaws.com/uploaded_files/Common%۲۰Cyber%۲۰Language.pdf

ISACA. (۲۰۱۶). Cybersecurity Fundamentals Glossary. Retrieved from ISACA: https://www.isaca.org/resources/glossary

Paulsen, C., & Byers, R. (May ۲۰۱۳). Glossary of Key Information Security Terms. US Department of Commerce : National Institute of Standards and Technology.

Singh, N. (۲۰۲۰, October). Cyber Security Terminology. Retrieved from ResearchGate: https://www.researchgate.net/publication/۳۴۴۷۸۳۲۹۷_Cyber_Security_Terminology

The A to Z of Cybersecurity glossary. (n.d.). Retrieved from Simplicity VoIP: https://www.simplicityvoip.net/hubfs/glossary.pdf