۱۲:۶

فصل‌نامه تخصصی امنیت سایبری مرکز آپا دانشگاه کردستان
شماره یازدهم - پاییز ۱۴۰۰

- پیکربندی امن در سرور ایمیل
- راهنمای امنیتی هاست‌های اشتراکی
- رعایت نکات امنیتی در مرورگرهای وب
- کاربرد هوش مصنوعی در امنیت سایبری
- امنیت در VMware و بررسی آسیب‌پذیری‌های آن
- لیست ده آسیب‌پذیری مخرب OWASP در سال ۲۰۲۱

درباره

مرکز آپا دانشگاه کردستان

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
ویراستاری، طراحی و صفحه‌آرایی: نازیلا خسروی
(با تشکر از مونا علی‌اکبری)
نویسندگان (به‌ترتیب مطالب):
محمد فتحی/ محمد حبیبی/فائزه احمدبیگی/ هادی گلباغی/ امید حسینی/ ژینو سفاحی/ آرش بهرام‌زارعی/ نازیلا خسروی/ مونا علی‌اکبری

راه‌های ارتباطی:

تلفن مرکز: ۰۸۷۳۳۶۱۱۴۱۵
نشانی مجله: کردستان، سنندج، بلوار پاسداران، دانشگاه کردستان، دانشکده مهندسی، ساختمان شماره ۳، طبقه همکف، مرکز آپا
وب‌سایت: cert.uok.ac.ir
ایمیل: cert@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 لینک‌ها می‌توانید مستقیما به آدرس مورد نظر منتقل شوید.

فهرست

مطالب

۰۱
مقاله‌های آموزشی

۰۲ پیکربندی امن در سرور ایمیل
۰۷ معرفی سامانه پویش سرور ایمیل ویرا
۰۸ راهنمای امنیتی هاست‌های اشتراکی برای سال ۲۰۲۱
۱۲ OSINT (Open-source intelligence)

۱۹
آسیب‌پذیری

۲۰ امنیت در VMware و بررسی آسیب‌پذیری‌های بحرانی آن
۲۸ لیست آسیب‌پذیری‌های OWASP TOP 10 - 2021

۳۳
معرفی ابزار

۳۴ ابزار Qu1cksc0pe

۴۱
دفترچه تقلب

۴۲ دفترچه تقلب Burp Suite

۴۷
معرفی دوره

۴۸ دوره SEC579

۵۱
معرفی کتاب

۵۲ کتاب Cyber Security: A practitioner's guide

۵۴
مقاله تحقیقاتی

۵۵ کاربرد هوش مصنوعی در امنیت سایبری

۷۰
امنیت اطلاعات

۷۱ رعایت نکات امنیتی در مرورگرهای وب

مقاله‌های آموزشی

پیکربندی امن در سرور ایمیل

معرفی سامانه پویش سرور ایمیل ویرا

راهنمای امنیتی هاست‌های اشتراکی برای سال ۲۰۲۱

OSINT (Open-source intelligence)

محمد فتحی

پیکربندی امن سرور ایمیل

مقدمه

سرویس ایمیل یکی از سرویس‌های مهم در سازمان‌های بزرگ است که علاوه‌بر نقش حیاتی در ارسال و دریافت پیام، نشان‌دهنده درجه اعتبار و اهمیت سازمان است. در پیاده‌سازی این سرویس، امکان اعمال سیاست‌گذاری‌های مورد نظر سازمان وجود دارد، امنیت پیام‌ها و حریم خصوصی کاربران حفظ می‌شود و همچنین به سایر سرویس‌های ارتباطی وابستگی وجود ندارد. همچنین سازمان می‌تواند مدیریت بهتری بر روی کاربران و مشتریان انجام دهد و اگر میزبانی سرویس در داخل شبکه سازمان باشد پیام‌های بین کاربران داخلی از شبکه سازمان خارج نمی‌شود. به‌دلیل اهمیت موضوع، در این نوشتار پیکربندی امن سرویس‌های ایمیل بررسی می‌گردد.

پیکربندی امن

از نوع و بسترهای سخت‌افزاری و نرم‌افزاری سرویس ایمیل، نحوه پیکربندی آن از اهمیت بالایی برخوردار است. از نیازمندی‌های بارز سرویس ایمیل امنیت است که بسته به نوع سازمان اهمیت آن می‌تواند متغیر باشد. برای پیکربندی امن یک سرور ایمیل تنظیمات زیادی از جمله تنظیمات سیستم‌عامل، سرویس، شبکه و سرور DNS مورد نیاز است. به‌دلیل نقش بالای این تنظیمات در تامین امنیت سرویس ایمیل، نحوه انجام آن از اهمیت بالایی برخوردار است. سرور ایمیل برای پیدا کردن مشخصات سرورهای دریافت و ارسال ایمیل یک سازمان از رکوردهای DNS سازمان استفاده می‌کند. این رکوردها علاوه‌بر اینکه ابزار شناسایی سرویس ایمیل سازمانی هستند محافظی در برابر پیام‌های spam نیز هستند. در ادامه نحوه پیکربندی انواع رکوردهای DNS مرتبط با سرویس ایمیل و کاربردهای هر رکورد بیان می‌شود.

رکورد A

مشابه سرویس‌های دیگر شبکه، این رکورد نام دامنه سرویس ایمیل را به آدرس IP تبدیل می‌کند. علاوه‌بر این رکورد، سرورهای ایمیل برای شناسایی سرویس ایمیل سازمان نیازمند رکورد MX نیز هستند.

رکورد MX

رکورد MX یا Mail Exchanger نامه دامنه را به یک یا چند میزبان ایمیل نگاشت می‌کند. در واقع سرورهای ایمیل در یک سازمان توسط رکوردهای MX مشخص می شوند و این رکوردها تعیین می‌کنند که ایمیل‌های ورودی به سازمان به کدام آدرس ارسال شوند. در موارد متعددی ممکن است برای یک نام دامنه چندین سرور ایمیل موجود باشد، به طور مثال mail1.domain.ir، mail2.domain.ir و غیره. از این قابلیت برای load balancing در یک سازمان استفاده می‌شود و برای هر میزبان یک مقدار اولویت تعیین می‌شود. سرورهای با مقدار اولویت یکسان به‌طور تصادفی انتخاب می‌شوند.

رکورد PTR

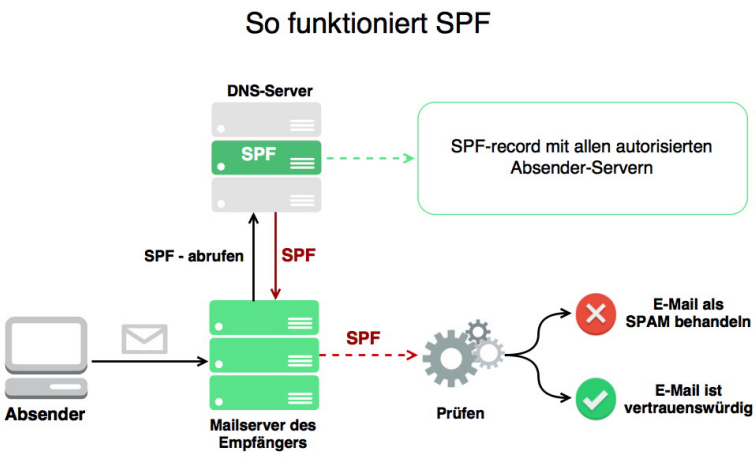
این رکورد که برعکس رکورد A عمل می‌کند آدرس IP را به نام دامنه تبدیل می‌کند و اصطلاحاً reverse lookup نامیده می‌شود. از این رکورد برای تشخیص منبع ارسال پیام استفاده می‌شود.

رکورد SPF

آدرس‌های IP مجاز برای ارسال ایمیل از طریق دامنه یک سازمان توسط رکورد SPF (Sender Policy Framework) مشخص می‌شوند. در هنگام دریافت یک ایمیل، سرورهای گیرنده ایمیل با چک کردن این رکورد از سرور DNS فرستنده اطمینان حاصل می‌کنند که ایمیل دریافتی از طرف دامنه واقعی سازمان ارسال شده است یا خیر. به‌همین دلیل این رکورد عامل مهمی در پیشگیری از جعل ایمیل است. مثلا در صورتی‌که آدرس IP ایمیل سرور یک سازمان 2.182.101.11 باشد رکورد SPF به‌صورت زیر می‌باشد:

“v=spf1 mx ip4:2.182.101.11 -all”

در شکل (۱) فرآیند چک‌کردن رکورد SPF نشان داده شده است. بعد از اینکه سرور گیرنده، ایمیلی را از دامنه یک سازمان دریافت می‌کند، رکورد SPF را از DNS سازمان فراخوانی می‌کند و مشخصات IP موجود در رکورد را با IP سرور فرستنده ایمیل مقایسه می‌کند. در صورت عدم تطبیق، ایمیل را به‌عنوان spam در نظر می‌گیرد [۱].



شکل (۱): فرآیند ارزیابی رکورد SPF

رکورد DKIM

رکورد DKIM (DomainKeys Identified Mail) روشی برای ارزیابی صحت هدر و محتوی پیام ارسالی با استفاده از رمزنگاری کلید نامتقارن است. در این روش، سرور فرستنده از محتوی پیام ارسالی و تعدادی از فیلدها در هدر ایمیل که در حین عملیات ارسال تغییر نمی‌کنند (مانند فیلدهای From و Subject) هش می‌گیرد و این هش را با استفاده از یک کلید خصوصی رمزنگاری می‌کند که به آن امضای دیجیتال می‌گویند. این امضا در یکی از تگ‌های هدر ایمیل ارسالی و در قسمتی تحت عنوان DKIM-Signature ارسال می‌شود [۲]. نمونه یک DKIM-Signature در زیر نشان داده می‌شود که در آن تگ h فیلدهای مورد استفاده در رمزنگاری را مشخص می‌کند و تگ b همان امضای دیجیتال یا رمزنگاری شده هش است.

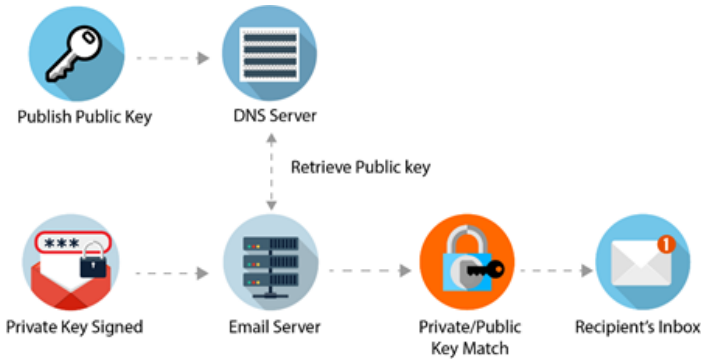
در تفاوت رکورد DKIM **با** SPF می‌توان گفت رکورد SPF تضمین کننده اصالت فرستنده پیام و عدم جعل آدرس است اما تضمین‌کننده صحت و یکپارچگی محتوی پیام نیست. به‌همین دلیل برای اطمینان از عدم تغییر محتوی پیام و فیلدها، باید از رکورد DKIM استفاده کرد.

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=brisbane;
     c=relaxed/simple; q=dns/txt; i=foo@eng.example.net;
     t=1117574938; x=1118006938; l=200;
     h=from:to:subject:date:keywords:keywords;
     z=From:foo@eng.example.net|To:joe@example.com|
     Subject:demo=20run|Date:July=205,=202005=203:44:08=20PM=20-0700;
     bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
     b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

در سرور گیرنده ایمیل، ابتدا کلید عمومی فرستنده ایمیل با استفاده از رکورد DKIM از سرور DNS فرستنده فراخوانی می‌شود و با استفاده از آن امضای دیجیتال ارسالی رمزگشایی و هش ارسالی استخراج می‌گردد. نمونه‌ای از رکورد DKIM در شکل زیر نشان داده می‌شود که در آن تگ p بیانگر کلید عمومی فرستنده است.

```
• k=rsa; t=s; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDGMjj8MVaESl30KSPYdLaEreSYzvOVh15u9
  YKAmTLgk1ecr4BCRq3Vkg3Xa2QrEQWbIvQj9FNqBYOr3XIczzU8gkK5Kh42P4C3DgNiBvlNNk2BlA5ITN/EvVAn
  /ImjoGq5IrcO+hAj2iSAozYTEpJAKe0NTrj49CIkj5JI6ibyJwIDAQAB
```

همچنین سرور گیرنده نیز از محتوی ایمیل و فیلدهای تعیین شده هش می‌گیرد. در صورت تطبیق این دو هش با همدیگر، مشخص می‌شود که محتوی و فیلدهای ایمیل مورد استفاده در امضا تغییر نیافته‌اند و امضا کننده ایمیل همان ارسال کننده ایمیل است. در صورت تغییر حتی یک کاراکتر، این تطابق فراهم نمی‌شود. این فرآیند در شکل (۲) نیز نشان داده شده است.



شکل (۲): فرآیند ارزیابی رکورد DKIM

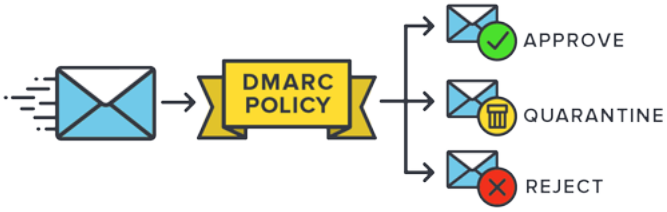
رکورد DMARC

رکورد DMARC برآورده شدن شرایط تعیین شده در رکوردهای SPF و DKIM را بررسی می‌کند. در صورت برآورده نشدن شرایط مذکور، DMARC سیاستی را در اختیار سرور دریافت کننده ایمیل قرار می‌دهد و با استفاده از این سیاست، سرور ایمیل گیرنده تصمیم می‌گیرد که ایمیل را دریافت، رد یا قرنطینه کند (شکل ۳).

رکورد DMARC یا Domain-based Message Authentication, Reporting and Conformance با ارزیابی‌هایی که بر روی احراز هویت فرستنده و صحت پیام انجام می‌دهد، فرستنده و گیرنده‌های ایمیل را در برابر اسپم، جعل ایمیل و فیشینگ محافظت می‌نماید. همچنین این رکورد قابلیت گزارش‌دهی اقدامات انجام شده توسط سایر سرورهای ایمیل بر روی ایمیل‌های ارسالی از یک دامنه مشخص را فراهم می‌آورد. نمونه یک رکورد DMARC در زیر نشان داده می شود.

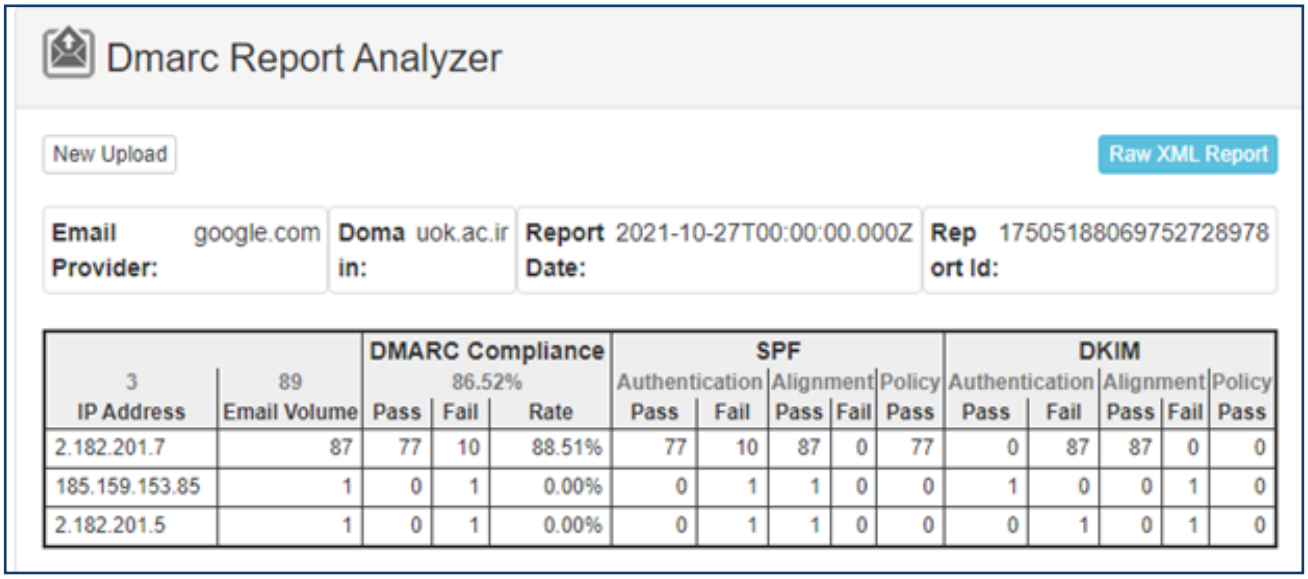
“ v=DMARC1; p=reject; rua=mailto:admin@uok.ac.ir;”

تگ p=reject در این رکورد به سایر سرورهای ایمیل اعلام می‌کند که در صورت عدم تطابق رکوردهای SPF و DKIM در هر ایمیل دریافتی، این ایمیل را reject کند و نتیجه را به آدرس admin@uok.ac.ir ارسال کند.



شکل (۳): سیاست‌های عملکردی DMARC

گزارش‌های DMARC را می توان با استفاده از ابزارهای آنلاین مانند MXtoolbox آنالیز کرد [۳]. در شکل (٤) یک نمونه از گزارش سرور ایمیل گوگل در مورد ایمیل‌های دریافت شده در یک بازه زمانی با دامنه uok.ac.ir و آدرس 2.182.201.7 نشان داده می‌شود. همچنان‌که ملاحظه می‌شود از ۸۹ ایمیل دریافتی با دامنه uok، فقط ۷۷ مورد توسط سرور گوگل تایید و دریافت شده‌اند. برای جزییات بیشتر در مورد ساختار DMARC به مرجع [٤] مراجعه نمایید.



Dmarc Report Analyzer

New Upload | Raw XML Report

Email Provider: google.com | Domain: uok.ac.ir | Report Date: 2021-10-27T00:00:00.000Z | Report Id: 1750518806975272897 8

		DMARC Compliance			SPF					DKIM				
3	89	86.52%			Authentication		Alignment		Policy	Authentication		Alignment		Policy
IP Address	Email Volume	Pass	Fail	Rate	Pass	Fail	Pass	Fail	Pass	Pass	Fail	Pass	Fail	Pass
2.182.201.7	87	77	10	88.51%	77	10	87	0	77	0	87	87	0	0
185.159.153.85	1	0	1	0.00%	0	1	1	0	0	1	0	0	1	0
2.182.201.5	1	0	1	0.00%	0	1	1	0	0	0	1	0	1	0

شکل (٤): گزارش تحلیلی DMARC

علاوه‌بر رکوردهای DNS که بر پیکربندی امن سرور ایمیل تاثیرگذار هستند در ادامه به دو آسیب‌پذیری مهم این سرورها می‌پردازیم.

Open Relay

اگر کاربری بدون احراز هویت، ایمیلی را از طریق یک سرور ایمیل برای یک سرور دیگر ارسال کند آسیب‌پذیری open relay وجود دارد. این آسیب‌پذیری که منشا آن پیکربندی ناامن پروتکل SMTP است موجب سوءاستفاده و ارسال ایمیل‌های با آدرس جعلی می‌شود. برای پیشگیری از این آسیب‌پذیری، پیکربندی امن SMTP جهت احراز هویت در هنگام ارسال ایمیل و یا بستن قابلیت relay در این پروتکل ضروری است. همچنان‌که در توضیح رکورد SPF ذکر شد یکی دیگر از روش‌های پیشگیری از ارسال ایمیل با آدرس جعلی استفاده از رکورد SPF در سرور DNS فرستنده است.

Email spoofing

در صورتی‌که بتوان از یک آدرس ایمیل جعلی به یک آدرس دیگر در همان دامنه ایمیل ارسال کرد، آسیب‌پذیری internal email spoofing وجود دارد. در حالت کلی ممکن است سایر فیلدهای هدر ایمیل نیز جعل شوند. از آنجا که رکورد SPF تاثیری در برطرف کردن این آسیب‌پذیری ندارد لذا وجود آن می‌تواند خطرناک باشد. برای پیشگیری از این آسیب‌پذیری، اعمال فرآیند احراز هویت در پروتکل SMTP ضروری است. در ادامه یک نمونه از کد ارسال ایمیل جعلی با پروتکل SMTP از طریق اتصال Telnet نشان داده می‌شود.

```
send: ‹telnet mail.test.ac.ir 25›
send: ‹ehlo mail.test.ac.ir›
send: ‹STARTTLS›
send: ‹ehlo mail.test.ac.ir›
send: ‹mail FROM:<author@test.ac.ir>›
send: ‹rcpt TO:<admin@test.ac.ir>›
send: ‹data›
send: ‹.›
send: ‹quit›
```

جمع‌بندی

در کنار همه مزایای سرویس ایمیل محلی، پیکربندی امن آن و پویش آسیب‌پذیری‌ها جهت پیشگیری از مشکلاتی مانند جعل ایمیل و فیشینگ از اهمیت بالایی برخوردار است. تنظیم رکوردهایی مانند DKIM، SPF، MX و DMARC در سرور DNS می‌تواند نقش تعیین‌کننده‌ای در پیشگیری از مشکلات داشته باشد. به همین منظور، مرکز آپا دانشگاه کردستان سامانه پویش سرور ایمیل ویرا را برای بررسی پیکربندی امن سرورهای ایمیل توسعه‌داده است که در این شماره فصل‌نامه این سامانه معرفی خواهد شد.

مراجع

[1] https://www.spf-record.com
[2] https://www.cloudflare.com/learning/dns/dns-records/dns-dkim-record/
[3] https://mxtoolbox.com/
[4] https://www.sparkpost.com/resources/email-explained/dmarc-explained/

سامانه پویش سرور ایمیل ویرا

https://msscanner.uok.ac.ir

معرفی سامانه

داشتن یک ایمیل سرور محلی امروزه از ملزومات تمامی سازمان‌ها، شرکت‌ها، موسسات و ادارات می‌باشد که پیکربندی صحیح و امن این ایمیل سرور باعث جلوگیری از برخی آسیب‌پذیری‌ها می‌شود که ممکن است صدمات جبران ناپذیری برای آن مجموعه به همراه داشته باشد. با توجه به اهمیت موضوع امنیت در این بستر، مرکز آپا دانشگاه کردستان در راستای رسالت خود اقدام به تولید سامانه پویشگر سرور ایمیل ویرا نموده که حسابرسی ایمیل‌سرورها و شناسایی نقص‌های موجود در پیکربندی آن‌ها را انجام می‌دهد. این سامانه به کاربران و کارشناسان این امکان را می‌دهد که به راحتی با استفاده از یک رابط گرافیکی اقدام به پویش سرور ایمیل خود نموده و خروجی پویش را دریافت کنند. همچنین نحوه رفع نقص و انجام پیکربندی امن در این سامانه در نظر گرفته شده است.

زبان‌ها، ابزارها و تکنولوژی‌های مورد استفاده

قابلیت‌ها

- پویش سرورهای ایمیل جهت شناسایی نقص‌ها در پیکربندی و تنظیمات نا امن
- انجام پویش‌ها به صورت موازی
- ثبت پویش‌های انجام شده در بانک اطلاعاتی
- ارائه راهکار جهت رفع نقص‌ها و ایجاد پیکربندی امن

ورودی ابزار

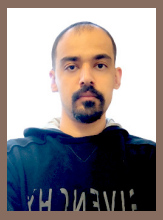
- آدرس دامنه
- آدرس سرور ایمیل
- پورت
- آدرس ایمیل معتبر بر روی سرور ایمیل (اختیاری)

پنل کاربری

- انجام پویش جدید
- مشاهده پویش‌های انجام شده
- چاپ اطلاعات پویش
- مشاهده راهکار رفع نقص و ایجاد پیکربندی امن
- جستجوی پویش‌های انجام شده
- ویرایش اطلاعات حساب کاربری

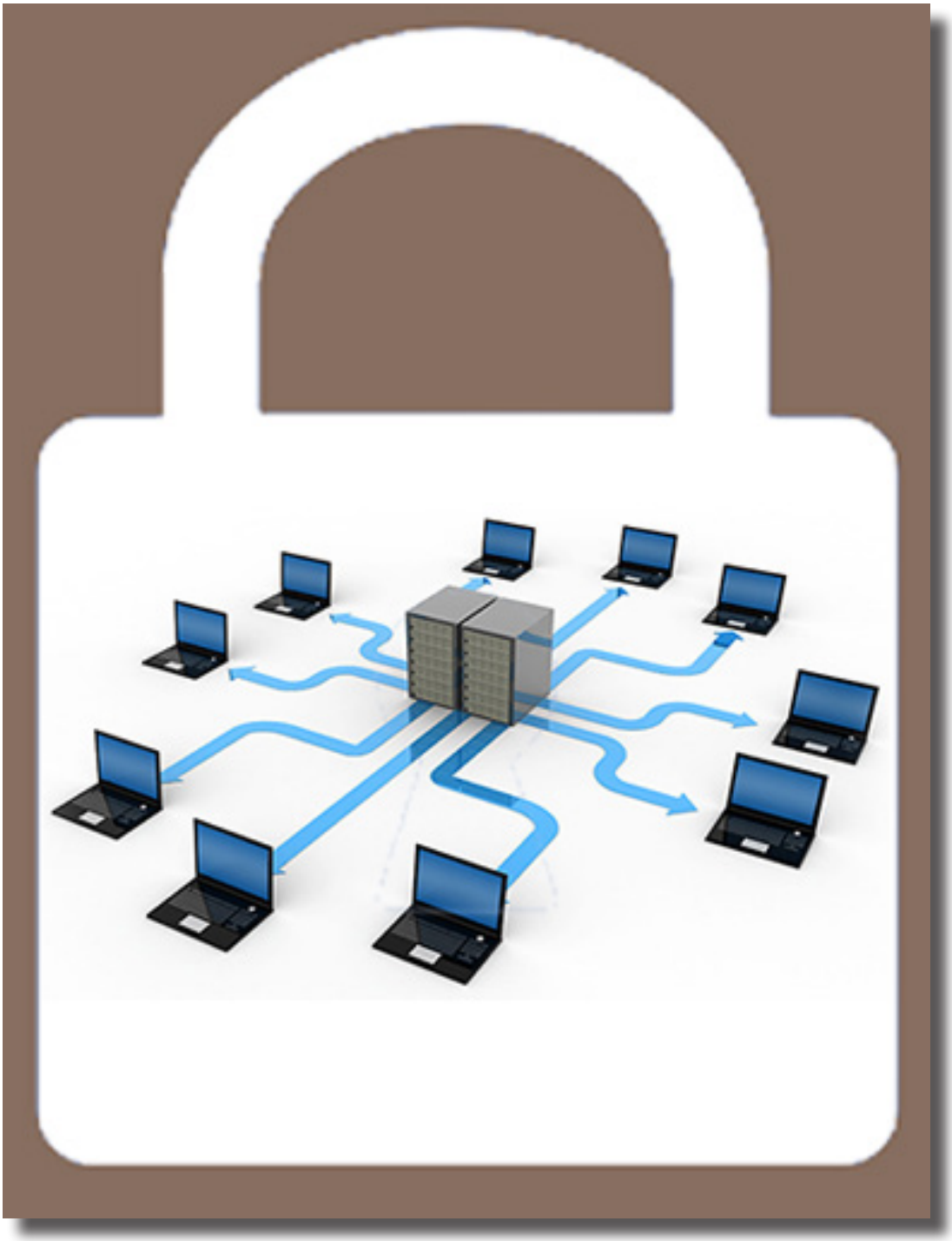
پنل مدیریت

- مدیریت، مشاهده و چاپ لیست کاربران
- مشاهده آمار مختلف از پویش‌ها
- انجام پویش جدید
- مشاهده و چاپ کل پویش‌های انجام شده
- چاپ اطلاعات پویش
- مشاهده راهکار رفع نقص و ایجاد پیکربندی امن
- جستجوی پویش‌های انجام شده
- ویرایش اطلاعات حساب کاربری



محمد حبیبی

راهنمای امنیتی
هاست‌های اشتراکی ۲.۲۱



مقدمه

معمولاً سایت‌های سرگرمی کوچک، کسب و کارهای نوپا یا وبلاگ‌های شخصی برای میزبانی خود از هاست‌هایی به‌عنوان هاست‌های اشتراکی (Shared hosting) استفاده می‌کنند. به‌ندرت ممکن است وب‌سایت‌های تجاری یا سازمانی از هاست‌های اشتراکی استفاده کنند، اگرچه بسیاری از مالکین وب‌سایت‌ها در ابتدا از هاست‌های اشتراکی استفاده می‌کنند تا زمانی که توانایی پرداخت هزینه سرورهای خصوصی مجازی (VPS) یا هاست‌های اختصاصی (dedicated hosting) را داشته باشند.
برای مالکین وب‌سایت‌ها اجرا شدن وب‌سایت‌ها با سرعت مطلوب و نبود بدافزار بر روی میزبان که از آن استفاده می‌کنند بسیار حائز اهمیت است. زمانی که صدها مالک وب‌سایت بدون داشتن کمترین دانشی در رابطه با امنیت سایبری یا تنظیمات مرتبط به کارایی و عملکرد، وب‌سایت خود را بر روی یک هاست اشتراکی راه‌اندازی می‌کنند، تامین امنیت این هاست اشتراکی برای مدیران هاست و همچنین کاربران بسیار دشوار و پیچیده می‌شود. با استفاده از یک ابزار مناسب مالکین وب‌سایت و مدیران هاست می‌توانند عملکرد وب‌سایت را در حد مطلوبی نگه داشته و آن را در مقابل اکسپلویت‌های (exploits) عمومی امن نگه دارند.

هاست‌های اشتراکی

پس از اینکه مالکین وب‌سایت دامنه مورد نظرشان را خریداری کردند نیاز است که فایل‌های مربوط به وب‌سایت را بر روی یک هاست قرار دهند و یکی از گزینه‌هایی که به‌دلیل هزینه پایین عموماً استفاده می‌شود هاست‌های اشتراکی است. هاست‌های اشتراکی برای سایت‌های کوچک با ترافیک پایین گزینه مناسبی است.

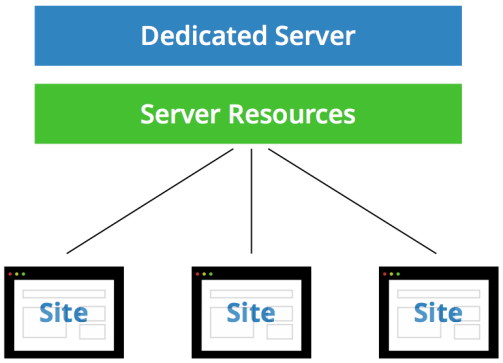
تفاوت هاست‌های اشتراکی و اختصاصی

برای سایت‌های سازمانی و تجاری معمولاً از هاست‌های اختصاصی استفاده می‌شد. سرورهای اختصاصی معمولاً یک سرور فیزیکی هستند که مشتریان از ارائه‌دهندگان خدمات هاستینگ اجاره می‌کنند. مشتری کنترل کاملی بر روی سرور دارد و معمولاً از آن به همراه سرورهای دیگری در شبکه کوچک مالکین سایت استفاده می‌کند. این سرورها را می‌توان در یک شبکه داخلی ادغام کرد یا در شبکه اینترنت در دسترس قرار داد.
شرکت‌ها ممکن است از هاست‌های اختصاصی برای برنامه‌های تجارت الکترونیک عمومی استفاده کنند.
مالکین وب‌سایت‌های کوچک ممکن است در ابتدا به‌دلیل هزینه بالا از هاست‌های اختصاصی استفاده نکنند، خصوصاً در ابتدا که از خدمات خود درآمد کمی به‌دست می‌آورند. هاست‌های اختصاصی برای شرکت‌هایی که نیاز به دسترسی کامل به سرور خود را دارند و نمی‌خواهند منابع سخت افزاری یا شبکه خود را با مشتریان دیگر ارائه دهنده، به اشتراک بگذارند عموماً گزینه مناسبی است.

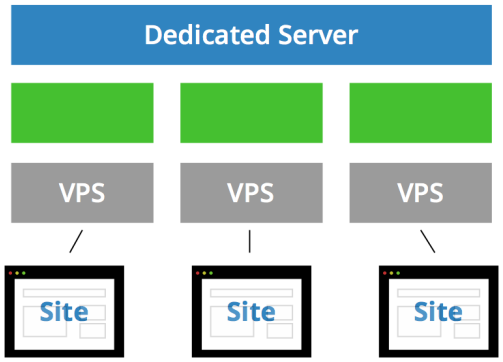
تفاوت هاست‌های اشتراکی و سرورهای خصوصی مجازی (VPS)

پس از هاست‌های اختصاصی، بهترین گزینه سرورهای خصوصی مجازی است. در سرورهای خصوصی مجازی مشتری به یک ماشین مجازی با منابع سخت‌افزاری مشخصی دسترسی پیدا می‌کند بدون اینکه به کل سرور فیزیکی دسترسی داشته باشد. سرورهای خصوصی مجازی شبیه به هاست‌های اختصاصی به نظر می‌رسند و عمل می‌کنند، البته هنوز مشتریان از منابع سخت‌افزاری و شبکه سرور فیزیکی به صورت اشتراکی استفاده می‌کنند. هزینه این سرورها چیزی مابین هاست‌های اشتراکی و اختصاصی است و برای اکثر کسب و کارهای کوچک قدمی مناسب بعد از هاست اشتراکی به حساب می‌آید.
میزبان می‌تواند یک ماشین مجازی برای مشتری راه‌اندازی کند یا اینکه مشتری به هر شکلی که می‌خواهد ماشین مجازی را از ارائه‌دهنده تحویل بگیرد و آن را پیکربندی کند.

Shared Hosting



VPS Hosting



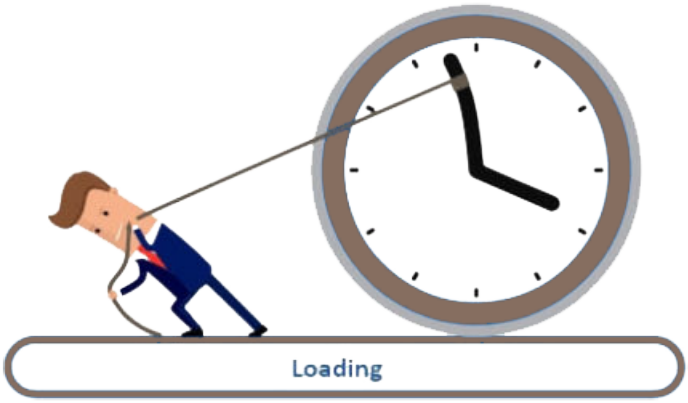
چه مشکلات امنیتی در هاست‌های اشتراکی وجود دارد؟

استفاده از هاست‌های اشتراکی مقرون‌به‌صرفه است اما ممکن است به قیمت از دست‌دادن امنیت وب‌سایت تمام شود. از آن‌جایی که شما کنترلی بر روی سایت سایر کاربران ندارید و نمی‌توانید تهدیداتی که برای سایر وب‌سایت‌ها رخ می‌دهد را مشاهده، کنترل و مدیریت کنید، هنگام استفاده از هاست‌های اشتراکی، وب‌سایت شما نیز ممکن است از حمله به سایر وب‌سایت‌ها صدمه ببیند. وقتی به دنبال هاست اشتراکی هستید باید این مسئله را در نظر بگیرید که هر میزبان روش خود را برای مدیریت وب‌سایت‌ها در سرور خود دارد.

دایرکتوری به اشتراک گذاشته شده با مالکین سایر وب‌سایت‌ها

در یک هاست اشتراکی ممکن است میزبان هاست یک فضای ذخیره‌سازی و یک دایرکتوری که فایل‌ها و داده‌های وب‌سایت خود را در آن ذخیره کنند، برای مشتریان ایجاد کند. اینکار باعث می‌شود که در صورت دسترسی مهاجم به این دایرکتوری، مهاجم به تمامی صفحات آپلود فایل، حتی آپلود فایل پیکربندی در وب‌سایت شما و سایر وب‌سایت‌ها دسترسی پیدا کند و در نتیجه امنیت تمامی وب‌سایت‌های میزبانی شده توسط این هاست به خطر بیافتند.

مشکل زمان بارگذاری (Load Time) وب‌سایت



عملکرد (Performance) یکی از مهم‌ترین مواردی است که باعث موفقیت یک وب‌سایت می‌شود. موتورهای جستجو از عملکرد وب‌سایت‌ها به عنوان یک فاکتور برای رتبه‌بندی وب‌سایت‌ها استفاده می‌کنند. مالکین وب‌سایت می‌توانند سایت خود را به شکلی طراحی و تنظیم کنند که عملکرد بهتری داشته باشد. در هاست‌های اشتراکی مالکین وب‌سایت نمی‌توانند منابع سرور میزبان را کنترل کنند و باید این منابع را به‌صورت اشتراکی با سایر مشتریان استفاده کنند، بنابراین هر وب‌سایت با کدنویسی ضعیف و ناامن می‌تواند عملکرد کلیه وب‌سایت‌های دیگر که در آن هاست میزبانی می‌شود را پایین بیاورد.

آیا هاست‌های اشتراکی قابل نفوذ هستند؟

به صورت کلی پاسخ به این سوال بله است و تقریباً هر بستری که در سطح اینترنت قابل دسترس است قابل نفوذ است. حتی منابعی که در شبکه‌های داخلی نیز وجود دارند پتانسیل حمله و افشای اطلاعات را دارند. اکثر اپلیکیشن‌ها دارای آسیب‌پذیری‌هایی هستند که از این آسیب‌پذیری‌ها می‌توان بهره‌برداری کرد و باعث سرقت اطلاعات یا نصب بدافزار بر روی وب‌سرور شود. هاست‌های اشتراکی به نسبت دیگر انواع هاست‌ها ریسک بالاتری دارند به این دلیل که ممکن است چند صد وب‌سایت بر روی آن‌ها راه‌اندازی شده باشد و طبعاً ریسک به‌خطر افتادن وب‌سرور نیز برای هاست‌های اشتراکی بالاتر است.

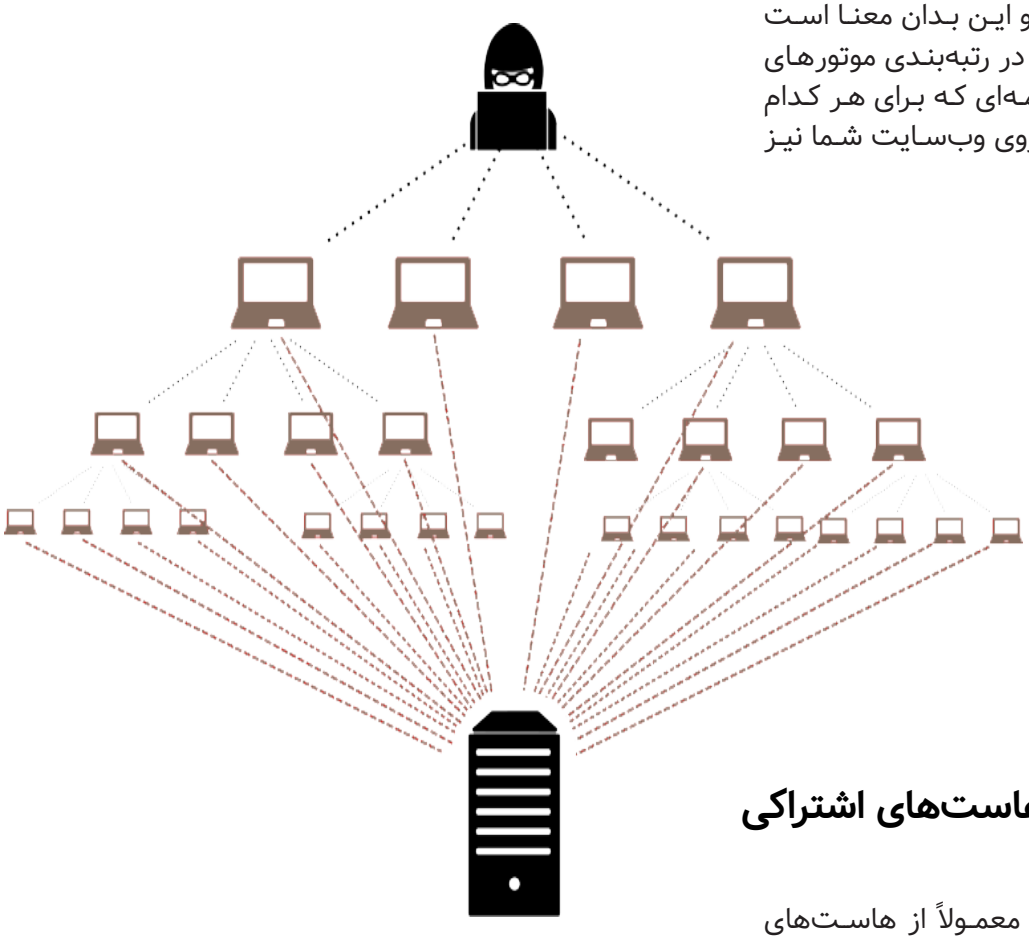
به‌طور معمول در هاست‌های اشتراکی از سیستم‌های مدیریت محتوا مانند وردپرس استفاده می‌شود. تفاوت اساسی هاست‌های اشتراکی، اختصاصی و سرورهای خصوصی مجازی در روش میزبانی وب‌سایت‌ها است. وقتی که یک مهاجم به یک هاست اختصاصی یا سرورهای خصوصی مجازی حمله می‌کند و به سرور دسترسی پیدا می‌کند، سایر مشتریان آن هاست تحت تاثیر قرار نمی‌گیرند، به‌عنوان‌مثال وقتی که یک بدافزار بر روی یک هاست اختصاصی آپلود شود تنها آن هاست و وب‌سایت تحت تاثیر قرار می‌گیرد اما اگر یک هاست اشتراکی مورد حمله قرار گیرد و مهاجم به سرور دسترسی داشته باشد و یک بدافزار بر روی آن آپلود کند، ممکن است چند صد وب‌سایت مرتبط با مشتریان آن میزبان تحت تاثیر قرار بگیرند و خسارت و خرابی وارد شده بسیار بالاتر باشد.

حملات منع سرویس توزیع شده (DDoS)

حملات DDoS با ارسال درخواست‌های بسیار زیاد به سمت یک هاست، عملکرد وب‌سرور را با مصرف بیش از حد منابع پایین می‌آورند. هنگامی که حملات DDoS بر روی یک هاست اشتراکی انجام شود، می‌تواند باعث اختلال یا قطع سرویس‌دهی تمامی وب‌سایت‌های موجود بر روی هاست شود. چون در هاست‌های اشتراکی مالکین وب‌سایت، دسترسی به وضعیت ترافیک و آمار مربوط به سایر وب‌سایت‌ها و همچنین خود هاست ندارند، نمی‌توانند دلیل کندشدن یا مختل‌شدن سرویس‌دهی وب‌سایت خود را تشخیص دهند.

آدرس IP مشترک

وب‌سایت‌های موجود برروی یک هاست اشتراکی از یک آدرس IP مشترک استفاده می‌کنند و این بدان معنا است که هر محتوایی که باعث اثر منفی در رتبه‌بندی موتورهای جستجو، لیست‌سیاه یا هرنوع جریمه‌ای که برای هر کدام از سایت‌های دیگر ایجاد شود، بر روی وب‌سایت شما نیز تاثیر بگذارد.



چگونه امنیت خود را در هاست‌های اشتراکی تامین کنیم؟

برای سایت‌های سازمانی و تجاری معمولاً از هاست‌های اختصاصی استفاده می‌شد. سرورهای اختصاصی معمولاً یک سرور فیزیکی هستند که مشتریان از ارائه‌دهندگان خدمات هاستینگ اجاره می‌کنند. مشتری کنترل کاملی بر روی سرور دارد و معمولاً از آن به همراه سرورهای دیگری در شبکه کوچک مالکین سایت استفاده می‌کند. این سرورها را می‌توان در یک شبکه داخلی ادغام کرد یا در شبکه اینترنت در دسترس قرار داد.

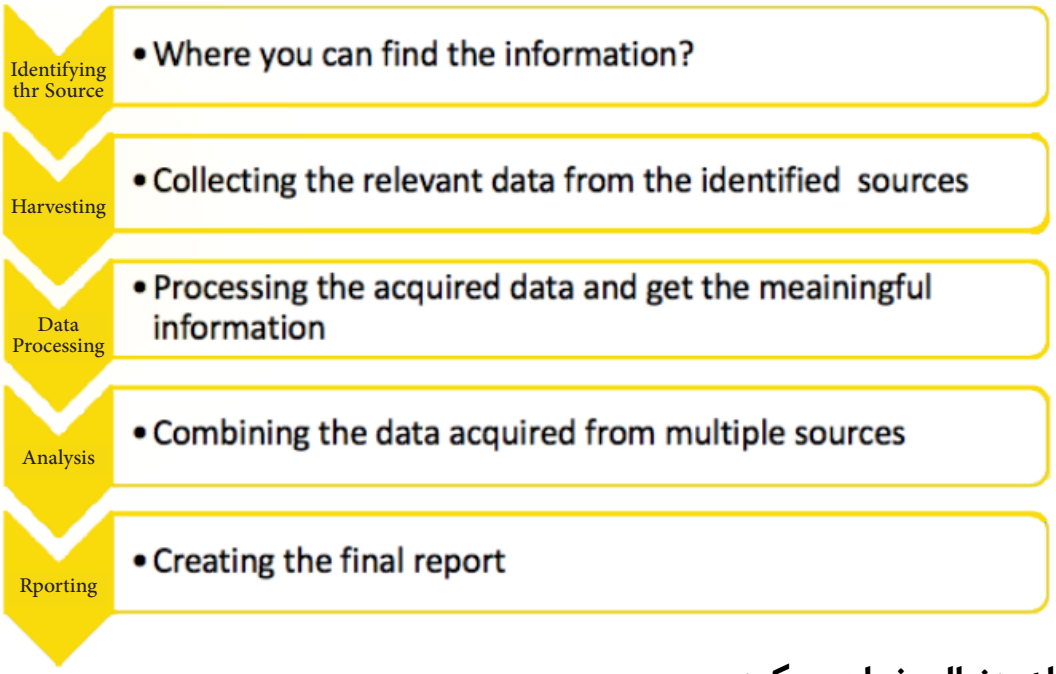
شرکت‌ها ممکن است از هاست‌های اختصاصی برای برنامه‌های تجارت الکترونیک عمومی استفاده کنند. مالکین وب‌سایت‌های کوچک ممکن است در ابتدا به‌دلیل هزینه بالا از هاست‌های اختصاصی استفاده نکنند، خصوصاً در ابتدا که از خدمات خود درآمد کمی به‌دست می‌آورند. هاست‌های اختصاصی برای شرکت‌هایی که نیاز به دسترسی کامل به سرور خود را دارند و نمی‌خواهند منابع سخت افزاری یا شبکه خود را با مشتریان دیگر ارائه دهنده، به اشتراک بگذارند عموماً گزینه مناسبی است.

فائزه احمدبیگی

OSINT
(Open-source intelligence)

مقدمه

OSINT به روشی برای جمع‌آوری اطلاعات از منابعی که در دسترس عموم است گفته می‌شود که از تجزیه‌وتحلیل آن برای تولید اطلاعات کاربردی استفاده می‌شود. OSINT فقط به امنیت سایبری محدود نمی‌شود، بلکه برای به‌دست آوردن اطلاعات شرکت‌های تجاری و نظامی یا سایر زمینه‌هایی که اطلاعات در آن‌ها اهمیت دارد، علم مهمی به شمار می‌آید.
یک محقق و تحلیلگر OSINT معمولاً فرآیند کار را مطابق شکل زیر دنبال می‌کند.



اهدافی که در این مقاله دنبال خواهیم کرد

چه شما یک استخدام‌کننده، مدیر بازاریابی، مهندس امنیت سایبری یا فقط یک فرد کنجکاو باشید که این مقاله را می‌خواند، مطمئن باشید نکات مفیدی برای خود پیدا خواهید کرد. شاید بخواهید بدانید چه اطلاعاتی از شما بر روی اینترنت برای دیگران وجود دارد یا فقط می‌خواهید ببینید آیا شخص یا سازمانی که به‌صورت آنلاین با شما تماس گرفته است قانونی است یا خیر. در این مقاله، نحوه کشف ردپای دیجیتالی یک فرد، انجام تحقیقات دیجیتال و جمع‌آوری اطلاعات برای تست امنیتی یا تست نفوذ را توضیح خواهیم داد.

بسیاری از ابزارهای OSINT امروزه در دسترس هستند و قصد نداریم به همه آن‌ها بپردازیم، فقط محبوب‌ترین آن‌ها و مواردی که توصیه شده و مفید هستند را بررسی می‌کنیم و در نهایت منابعی را برای مطالعه بیشتر علاقه‌مندان OSINT معرفی خواهیم کرد.

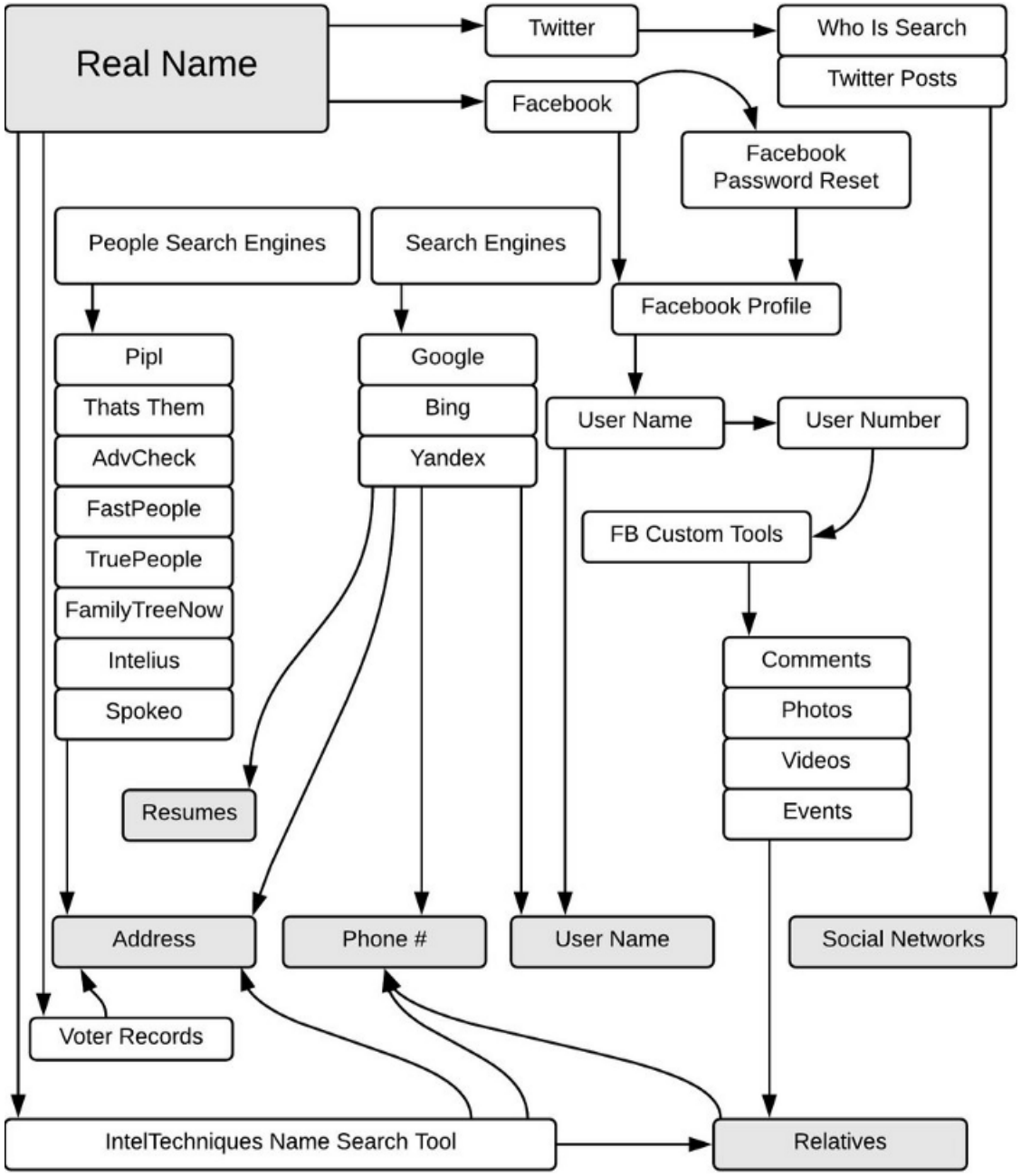
شناسایی فعال و غیرفعال (Active & Passive reconnaissance)

لازم است که قبل از کارکردن با ابزارهای OSINT حتما شناسایی فعال و غیرفعال را درک کرده باشیم. جمع‌آوری اطلاعات بدون برقراری ارتباط مستقیم با سایت را جمع‌آوری‌اطلاعات به‌صورت Passive یا غیرفعال می‌گویند که اطلاعاتی درباره هدف در اختیار ما می‌دهد. این فرایند را می‌توان از طریق نتایج موتور جستجو، اطلاعات whois و غیره به‌دست آورد.

اما شناسایی Active یا فعال نوعی حمله کامپیوتری است که در آن یک نفوذگر برای جمع‌آوری اطلاعات بیشتر مستقیماً با سیستم قربانی درگیر می‌شود. کلمه شناسایی یا reconnaissance از کاربرد نظامی آن وام گرفته شده است، جایی که به مأموریت در خاک دشمن برای به‌دست آوردن اطلاعات اشاره دارد. در زمینه امنیت سیستم، شناسایی معمولاً گامی مقدماتی به سوی حمله بیشتر برای سوءاستفاده از سیستم هدف است.

مراحل OSINT

۱. شروع با آنچه که می‌دانید (ایمیل، نام کاربری و غیره)
۲. تعریف الزامات (آنچه می خواهید به‌دست آورید)
۳. جمع‌آوری داده‌ها
٤. تجزیه‌وتحلیل داده‌های جمع‌آوری شده
۵. با استفاده از داده‌های جمع‌آوری‌شده جدید، برحسب نیاز، چرخه کلی فرایند را تکرار کنید.
٦. اعتبار سنجی مفروضات
۷. ایجاد گزارش



ابزارهای OSINT

با استفاده از ابزار OSINT، تحلیل‌گران می‌توانند سیل داده‌های در دسترس عموم را بهتر و راحت‌تر درک کرده و آن‌ها را به اطلاعات قابل استفاده تبدیل کنند. ابزارها نقش مهمی در جستجوی اطلاعات دارند، اما برای همه کاربران مفید نخواهند بود مگر اینکه بدانند استفاده از این ابزار تا چه حد اهمیت دارد. در ادامه این ابزارها توضیح داده می‌شوند.

Google Dorks

گوگل دورک، تکنیکی در حوزه امنیت سایبری است که از جستجوی گوگل برای یافتن حفره‌های امنیتی و اطلاعات حساس استفاده می‌کند که آن اطلاعات به‌راحتی در یک وب‌سایت در دسترس نیستند. این یکی از موثرترین تکنیک‌ها برای یافتن اطلاعات حساس هر وب‌سایتی است. گوگل دورک اطلاعاتی را در اختیار شما قرار می‌دهد که یافتن آن‌ها از طریق جستجوهای ساده دشوار است. یعنی اطلاعاتی که از گوگل دورک به‌دست می‌آوریم، برای مشاهده عمومی در نظر گرفته نشده است اما به اندازه کافی هم از آن محافظت نشده است. گوگل دورک می‌تواند نام‌های کاربری و رمزعبور، فهرست‌های ایمیل، اسناد حساس، کلیدهای API، اطلاعات شناسایی شخصی، آسیب‌پذیری‌های وب‌سایت و غیره را پیدا کند.

Google Dork

در لینک زیر می‌توان مجموعه‌ای از گوگل دورک‌ها را پیدا کرد:

https://www.exploit-db.com/google-hacking-database

همچنین در لینک زیر نیز مطالبی در مورد قابلیت‌های پنهان گوگل و نحوه جستجوی صحیح برای یافتن آسان اهدافتان را مشاهده خواهید کرد:

http://www.googleguide.com/advanced_operators_reference.html

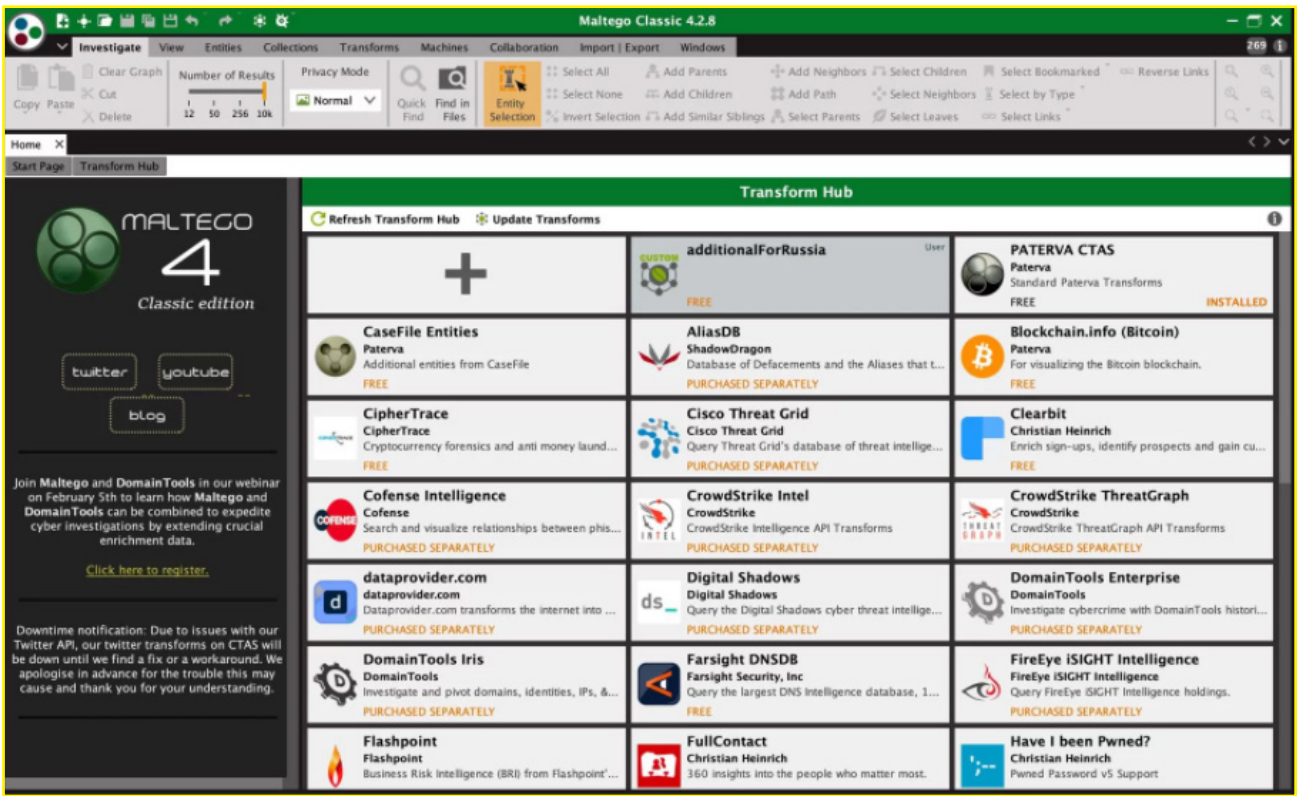
theHarvester

جمع‌آوری ایمیل‌ها یا در اصطلاح Email Harvesting شیوه‌ای موثر به منظور شناسایی ایمیل‌ها و نام‌های کاربری متعلق به سازمان هدف می‌باشد.
برای شناسایی غیرفعال، TheHarvester از منابع زیادی مانند موتورهای جستجوی بینگ، بایدو، یاهو و گوگل و همچنین شبکه‌های اجتماعی مانند لینکدین، توییتر و فیسبوک استفاده می‌کند. این ابزار برای شناسایی فعال از جستجوی معکوس DNS و DNS brute force استفاده می‌کند.

Maltego

ابزار Maltego یک پلت فرم پیشرفته برای تجزیه‌وتحلیل و جمع‌آوری اطلاعات است که پس از جمع‌آوری و تحلیل اطلاعات، آن‌ها را به گراف‌ها و نمایش بصری معناداری تبدیل می‌کند که به‌راحتی می‌توان اطلاعات را فهمید و درک کرد. این ابزار توسط Paterva توسعه‌یافته است و هم‌اکنون بخشی از توزیع لینوکس کالی نیز می‌باشد. یکی از بهترین قابلیت‌هایی که در این ابزار وجود دارد، مفهومی به نام «تبدیل» است. تبدیل در برخی موارد به صورت رایگان در دسترس است و در برخی دیگر فقط در نسخه‌های تجاری، آن را خواهید یافت. آن‌ها به شما کمک می‌کنند تا نوع متفاوتی از تست‌ها و ادغام داده‌ها را با برنامه‌های کاربردی خارجی اجرا کنید.

همچنین در وب‌سایت Maltego لیست عظیمی از وبلاگ‌ها، سایت‌ها، ابزارها، پادکست‌ها، کتاب‌ها و کانال‌ها وجود دارد که آن‌ها را به علاقه‌مندان به OSINT توصیه می‌کند.



Spiderfoot

Spiderfoot ابزاری است که به شما این امکان را می‌دهد تا اطلاعات زیادی در مورد هر سایت یا سروری جمع‌آوری کنید. اگر می‌خواهید OSINT را خودکار کنید، SpiderFoot یکی از بهترین ابزارهای شناسایی است زیرا می‌توان از آن برای پرس‌وجو در بیش از ۱۰۰ منبع داده عمومی به‌طور همزمان استفاده کرد و ماژولار بودن آن امکان تنظیم دقیق منابع موردنظر را فراهم می‌کند. اسکن با قابلیت‌های مختلف موضوع مورد علاقه بنده در خصوص این ابزار است. چهار مورد اسکن مختلف در این ابزار وجود دارد:

۱. دریافت همه چیز و همه چیز در مورد هدف.
۲. فهمیدن آنچه که هدف شما در اینترنت و در معرض دید همگان قرار می‌دهد (از طریق خزیدن وب یا web crawling و استفاده از موتور جستجو انجام می‌شود).
۳. جستجو در لیست سیاه و سایر منابع برای بررسی مخرب بودن هدف.
٤. جمع‌آوری اطلاعات از طریق منابع مختلف بدون اسکن مستقیم بر روی هدف که به آن اسکن passive گفته می‌شود.

Recon-ng

یکی دیگر از ابزارهای بسیار مفید Recon-ng بوده که به صورت خط فرمان است و برای جمع‌آوری اطلاعات به‌طور کامل و سریع استفاده می‌شود. این ابزار در کالی لینوکس همراه با ماژول‌های مستقل و تعامل با پایگاه داده، یک محیط قدرتمند را فراهم می‌کند که در آن می توان به شکل سریع و به‌طور کامل شناسایی مبتنی بر وب یا Web Reconnaissance را انجام داد.
برای کسانی که با Metasploit آشنا هستند، یادگیری Recon-ng آسان‌تر خواهد بود زیرا مدل استفاده مشابهی دارد.

shodan

Shodan سرورهایی در سرتاسر جهان دارد که برای ارائه جدیدترین اطلاعات اینترنتی و دستگاه‌های متصل در اینترنت می‌خزند و همین‌طور محبوب‌ترین اسکنر اینترنتی با API عمومی و قابل ادغام با بسیاری از ابزارهای امنیتی است. محققان امنیتی از آن برای کشف سیستم‌های آسیب‌پذیر و دسترسی به طیف گسترده‌ای از دستگاه‌های متصل و اینترنت اشیاء و ... استفاده می‌کنند، پس می‌توان از آن برای به خطر انداختن دستگاه یا یافتن اطلاعات مورد نیاز خود استفاده کرد. جایگزین‌های دیگری هم مانند Censys و مشابه چینی آن Fofa را می‌توان نام برد.

مقالات مفیدی در خصوص استفاده از Shodan در لینک‌های زیر قرار گرفته است.

- https://github.com/IFLinfosec/shodan-dorks
- https://github.com/humblelad/Shodan-Dorks
- https://github.com/jakejarvis/awesome-shodan-queries
- https://github.com/lothos612/shodan

سیستم عامل و ماشین مجازی برای OSINT

Tsurugi Linux

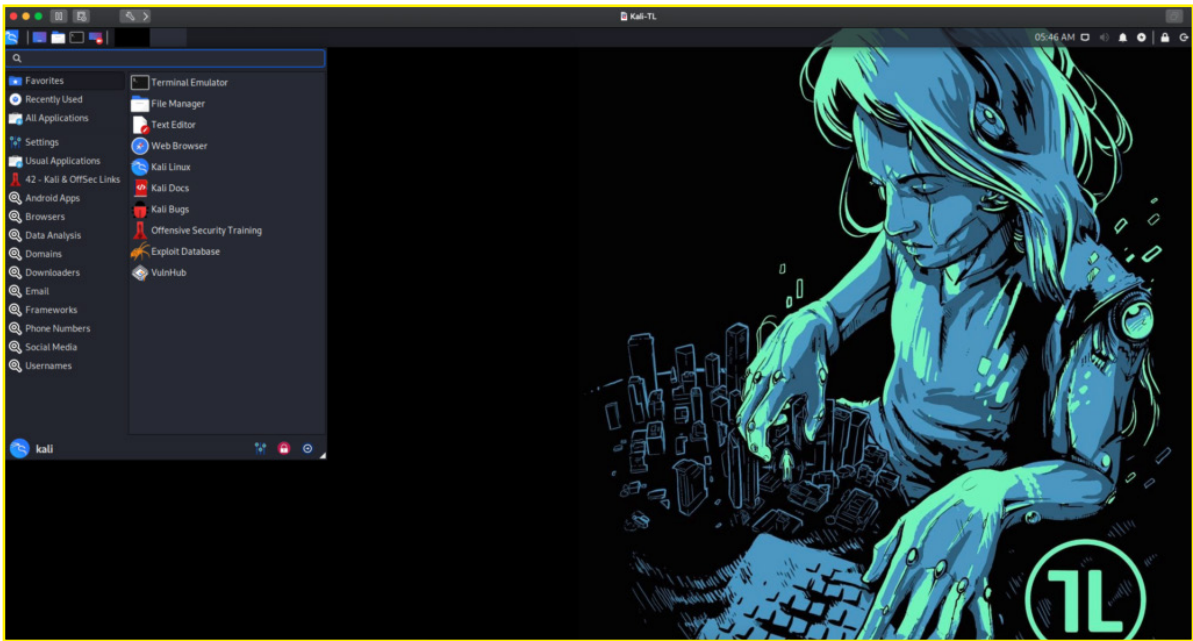
این توزیع از سازندگان DEFT و Kali است که بر اساس اوبونتو ساخته شده است. هدف از لینوکس Tsurugi جرم‌یابی و OSINT است، همچنین ابزارهایی برای تجزیه‌وتحلیل بدافزار، بازیابی اطلاعات و غیره نیز در آن وجود دارد.
هنگامی که سیستم‌عامل را راه‌اندازی می‌کنید، با محیط Mate و هنر جالب سامورایی روبرو خواهید شد که از قبل دارای یک دسکتاپ با پیکربندی حداقلی است که کار پردازنده‌ها، شبکه، هارد دیسک‌ها و تقویم را نمایش می‌دهد. اگر نمی‌خواهید از کالی استفاده کنید، Tsurugi یک جایگزین شایسته است.

می‌توان این توزیع لینوکسی را از وب‌سایت رسمی tsurugi linux در لینک زیر دانلود کرد.
https://tsurugi-linux.org/

Trace Labs OSINT VM

تیم Trace Labs یک OSINT VM ویژه ایجاد کرد تا مؤثرترین ابزارهای OSINT و اسکریپت‌های سفارشی‌شده را که در طول CTF ها مورد استفاده قرار می‌گیرند را یک‌جا جمع کند. این ماشین مجازی برای همه محققان OSINT قابل توجه و مفید خواهد بود.
توضیح بیشتر به صورت ویدیویی و همین‌طور فهرستی از ابزارها و دسته‌بندی‌های این ماشین مجازی را در لینک زیر می‌توان مشاهده کرد:

https://www.tracelabs.org/initiatives/osint-vm



جمع‌بندی

حفظ حریم خصوصی و کنترل اطلاعات که در این اقیانوس دیجیتال شناور است، دشوار است. در حالی که نمی‌توان همه اطلاعاتی را که در مورد ما وجود دارد کنترل کرد اما مهم است که حداقل در مورد آن آگاه بود!
ناگفته نماند که در عصر دیجیتال، اطلاعات نقش کلیدی را ایفا می‌کند، بنابراین کسانی که می‌دانند چگونه آن را پیدا کنند، همیشه یک قدم جلوتر خواهند بود. این مقاله تلاشی برای معرفی OSINT و نشان دادن دور نمای کلی از OSINT بود، بنابراین فقط نوک کوه یخ را توضیح داده شده است و اگرعلاقه‌مند به مطالعه بیشتر درخصوص OSINT هستید، منابع زیر را از دست ندهید:

- https://github.com/optiv/OSINT_Encyclopedia
- https://securitytrails.com/blog/osint-tools
- https://geekflare.com/osint-tools/
- https://github.com/cipher387/osint_stuff_tool_collection
- https://github.com/Dutchosintguy/OSINT-Discord-resources
- https://securitytrails.com/blog/top-osint-web-browser-extensions

آسیب‌پذیری

امنیت در VMware و بررسی آسیب‌پذیری‌های بحرانی آن

لیست آسیب‌پذیری‌های OWASP TOP 10 - 2021

هادی گلباغی

امنیت در VMware
و
بررسی آسیب پذیری های بحرانی آن

مقدمه

در شرایطهای مختلف در یک سازمان، تصمیمات مختلفی درخصوص استفاده از نرم‌افزارها، بسترهای ارتباطی و تجهیزات گرفته می‌شود. گاهاً ممکن است سازمان بخواهد برنامه یا سامانه جدیدی را راه‌اندازی کند و برای این کار نیاز به یک یا چند سرور جدید باشد. ممکن است شرکتی که این برنامه یا سامانه را برای سازمان شما توسعه می‌دهد، بخواهد یک سرور اختصاصی برایش فراهم کنید و یا سازمان شما به خاطر عدم تداخل با سایر سامانه‌ها و برنامه‌های خود بخواهد سرورهای آن‌ها از هم جدا باشند. قاعدتاً برای تهیه سرورهای جدید هزینه‌ای جداگانه لازم است و طبق روال معمول سازمان‌ها، مدتی باید برای تامین بودجه صبر کرد. یک سوال در این مورد مطرح می‌شود که آیا می‌دانید که شما سرورهایی دارید که در حال کارکردن با درصدی حداقلی از قدرت واقعی خود هستند؟ سوال دیگر این است که آیا می‌توان از این ظرفیت سرورهای موجود استفاده کرد و برای سامانه‌های جدید سرور جداگانه ایجاد کرد؟

در چند سال اخیر دنیای فناوری برای پاسخ به این سوال مجازی‌سازی را پیشنهاد کرده است که با استفاده از آن، می‌توان بدون خرید سخت‌افزار و سرور جدید، سامانه‌ها و برنامه‌های جدید خود را مورد بهره‌برداری قرار داد. به‌عنوان یک متخصص شبکه و امنیت حتماً با محصولات شرکت VMware و مجازی‌سازی تا حدی آشنا هستید و حتی برای این که بدانید مجازی‌سازی دقیقا چه کاری انجام می‌دهد، احتمالاً یک نسخه از VMware Workstation را بر روی سیستم‌عامل خود نصب کرده و با آن آشنایی پیدا کرده‌اید. اگر مقداری تخصصی‌تر به این موضوع نگاه کنیم درمی‌یابیم که جایی که تعداد سرورها بسیار زیاد است مواردی مانند سرعت، زمان در دسترس بودن یک سرور و سرویس‌های آن، زمان پشتیبان‌گیری و بازیابی، میزان مصرف برق، چگونگی خنک نگه داشتن سرورها، فضای لازم برای نگهداری سرورها، استفاده از حداکثر توانایی سرورها و بسیاری موارد دیگر برای مدیران شبکه و امنیت اهمیت پیدا می‌کند و در جای خود مدیریت این موارد چالش‌برانگیز نیز است. حال چه راهکاری برای داشتن سامانه‌ها و سرورهای متعدد و جداگانه اما با کاستن از میزان بارکاری که گفته شده می‌توان پیشنهاد داد؟ در ادامه پاسخ این سوال را بررسی خوهیم کرد.

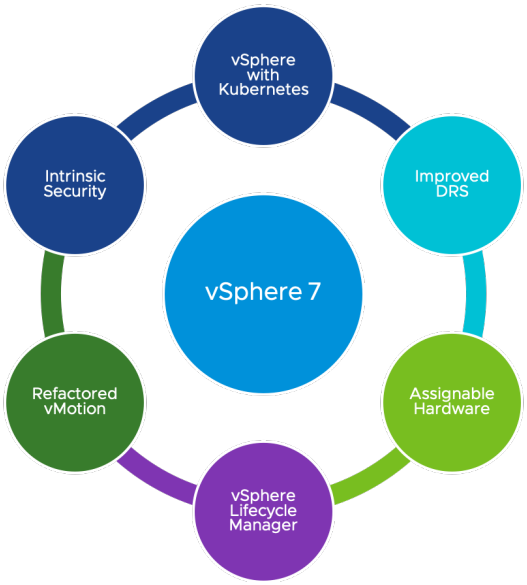
VMware

باتوجه به رشد روزافزون تکنولوژی‌های نوین و نفوذ بیش از پیش استفاده از نرم‌افزارها و سامانه‌های مختلف توسط مردم در زندگی روزمره، تیم‌های پشتیبانی از این بسترها نیز از روش‌های مختلف و بهتری برای مدیریت آن‌ها بهره می‌برند. مجازی‌سازی VMware مبتنی بر bare-metal hypervisor ESX/ESXi در معماری x86 است. با راه‌اندازی مجازی‌سازی سرور با VMware، هایپروایزر بر روی سرور فیزیکی نصب می‌شود و چندین ماشین مجازی (Virtual Machine) یا VM می‌سازد که بر روی این سرور اجرا می‌شوند. هر VM می‌تواند سیستم‌عامل خودش را داشته باشد و این یعنی چندین سیستم‌عامل بر روی یک سرور فیزیکی می‌تواند اجرا شود. منابع مختلف سرور مانند حافظه، شبکه و رم، بین تمامی VM های این سرور، به اشتراک گذاشته می‌شود.

شرکت VMware محصولات متفاوتی را در زمینه‌های مختلف دارد که شامل زمینه‌های مجازی‌سازی، شبکه و ابزارهای مدیریت امنیت، نرم‌افزار ذخیره‌سازی و نرم‌افزار دیتاسنتر نرم افزار محور (SDDC) است. اولین محصول VMware با نام VMware Workstation در سال ۱۹۹۹ ارائه شد و سپس در سال ۲۰۰۱، محصول دوم با نام VMware ESX عرضه شد. درصد زیادی از سازمان‌ها و شرکت‌های مختلف استفاده از محصولات شرکت VMware که آخرین و کامل‌ترین محصول آن vSphere است را انتخاب کرده‌اند. اولین تفاوتی که این نرم‌افزار ESX Server با نسخه Workstation خود دارد این است که به‌صورت مستقیم بر روی سخت‌افزار نصب می‌شود و دیگر نیازی به یک OS رابط نیست. این موضوع باعث افزایش ۷۰ درصدی سرعت کارکرد می‌شود. از سال ۲۰۰۹ محصول VMware vSphere با عنوان زیرساخت VMware شناخته می‌شد که شامل موارد زیر است:

- ESXi
- vCenter Server
- vSphere Client
- vMotion

آخرین نسخه این محصول، vSphere 7 بوده که در آوریل سال ۲۰۲۰ عرضه شده است که دارای قابلیت‌های زیر است.



مزایای مجازی‌سازی در VMware

- امنیت مبتنی بر مدل Zero Trust که در مقایسه با سیستم‌های Container مثل Kubernetes امنیت بهتری دارد.
- نظارت بهتر و سریع‌تر بر برنامه‌ها و منابع
- مدیریت ساده و راحت دیتاسنتر
- افزایش چابکی و کارایی در سیستم‌های دیتاسنتر
- حدف یا به حداقل رساندن Downtime
- افزایش پاسخ‌گویی و بهره‌وری سیستم
- تداوم کسب‌وکار و Disaster Recovery
- ایجاد SDDC یا دیتاسنتر نرم افزار محور با استانداردهای آن

معایب مجازی‌سازی در VMware

- هزینه بالای لایسنس
- در برخی موارد، Xen hypervisor و Hyper V جایگزین مناسبی برای آن هستند.
- هنگام کار با محصولات Oracle ممکن است برخی موارد پشتیبانی نشود و یا نقص‌هایی وجود داشته باشد.
- در صورت ناسازگاری سخت‌افزار ممکن است همه امکانات به شکلی که توقع داریم کار نکند.

امنیت در VMware

یک متخصص شبکه و امنیت سازمانی به‌منظور تامین امنیت VMware، باید امن‌سازی vCenter، ESXi، ماشین مجازی، vSwitch ها، امنیت در vSAN و بررسی لاگ‌های امنیتی را مدنظر داشته باشد. البته به‌صورت پیش‌فرض در بستر VMware ESXi ویژگی‌های متعددی وجود دارد که می‌توانند از نفوذ غیرمجاز و حملات مختلف جلوگیری کنند که برخی از این ویژگی‌ها به‌صورت پیش‌فرض یا پیکربندی نشده‌اند و یا به‌شکل صحیح پیکربندی نشده‌اند و یا به‌صورت کلی ما از آن‌ها بی‌اطلاع هستیم. از این بابت که VMware ESXi در اکثر سازمان‌های داخل کشور کاربرد بسیار زیادی دارد ما به‌عنوان یک ادمین شبکه یا متخصص امنیت وظیفه داریم که اقدامتی جهت امن‌سازی آن انجام دهیم.

برای امن‌سازی در ESXi، ماشین‌های مجازی و vCenter رعایت نکات مقابل ضروری است:

- فعال/غیرفعال و پیکربندی کردن سرویس‌دهنده‌ها در دیواره‌آتش ESXi
- فعال نمودن Lockdown Mode
- رعایت سیاست‌های امنیتی شبکه
- تغییر رمز عبور پیش‌فرض و استفاده از رمز عبور قوی و پیچیده
- اتصال میزبان ESXi به اکتیو دایرکتوری
- انتساب مجوزهای دسترسی به میزبان‌های ESXi به‌وسیله پروفایل‌ها (Host Profiles)
- پیکربندی سیاست‌های امنیتی ماشین مجازی
- ساخت/مدیریت گواهی‌نامه‌های امنیتی در vCenter Server
- وجود حداقل سرویس مورد نیاز برای اجرای بارهای کاری
- مسدود بودن Shell و SSH به‌صورت پیش‌فرض
- امکان استفاده از شبکه‌های اختصاصی براساس بارکاری (تفکیک بار)
- کنترل میزان استفاده از IO در سطح شبکه و فضای ذخیره‌سازی
- ایمن‌سازی ارتباط اجزای vSphere با پروتکل‌های امنیتی روز
- استفاده از UEFI Secure برای مقابله با نرم‌افزارها و بدافزارهایی که امضا دیجیتالی خاصی ندارند.
- محدودکردن استفاده از ESXi Shell به اموری مانند عیب‌یابی
- استفاده از vSphere Client برای مدیریت ESXi Host های مدیریت شده توسط vCenter
- غیرفعال‌سازی MOB یا همان Manged Object Browser
- تغییر تنظیمات ESXi Web Proxy

همچنین ESXi محافظت از VMkernel را به‌وسیله سه قابلیت زیر اعمال می‌کند:

Memory hardening

کرنل ESXi، برنامه‌های کاربران، کامپوننت‌های اجرایی مانند درایورها و کتابخانه‌ها را با استفاده از آدرس‌دهی تصادفی و غیرقابل پیش‌بینی حافظه، حفاظت می‌کند. Memory hardening همراه با ویژگی حفاظت از آدرس‌دهی‌های غیرقابل پیش‌بینی که توسط ریزپردازنده‌های امروزی تامین می‌شود، کار را برای کدهای مخرب که از این آسیب‌پذیری به‌منظور memory exploit سوءاستفاده می‌کنند، سخت می‌نماید.

Trusted Platform Module

TPM یک چیپ خاص است که بر روی بردهای سیستم نصب شده است و به‌منظور احراز هویت فرد استفاده کننده از دستگاه مورد استفاده قرار می‌گیرد. در این نوع از احراز هویت TPM دستگاه از کاربر سؤال پرسیده و اطلاعات خاصی مانند کلید رمزنگاری، گواهینامه‌های دیجیتال و مواردی از این دست را بر روی سیستم میزبان تعریف می‌نماید. VMware از قابلیت‌های TPM به منظور حفظ امنیت پشتیبانی می‌کند.

Kernel Module Integrity

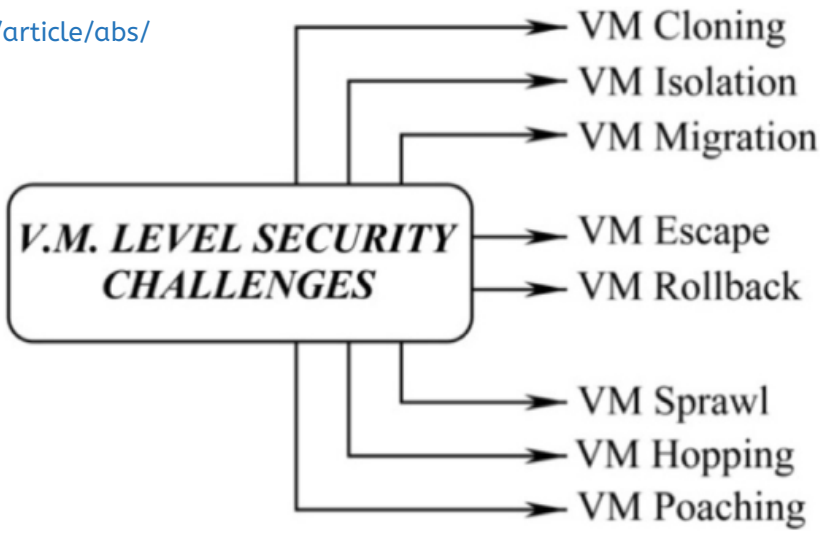
امضای دیجیتال باعث اطمینان از صحت و احراز هویت ماژول‌ها، درایورها و برنامه‌هایی که توسط VMkernel بار می‌شوند، می‌گردد. صحت عملکرد ماژول به ESXi این اجازه را می‌دهد که ماژول‌ها، درایورها، برنامه‌های کاربردی و گواهی‌نامه‌های امنیتی VMware را شناسایی کند.

لزوم به کارگیری امنیت در زیرساخت‌های مجازی‌سازی شبکه جهت بالاتر بردن ضریب امنیتی بسیار حائز اهمیت است. ماشین‌های مجازی شامل نرم‌افزارها و سیستم‌عامل‌های در حال اجرا هستند. به همین منظور حفظ امنیت آن‌ها از اهمیت خاصی برخوردار است. بر روی ماشین‌های مجازی سرویس‌های حساس و مهمی از قبیل Exchange Server, Active Directory, SQL Server, Firewall, Skype ها و بسیاری موارد دیگر وجود دارد، حتماً به‌عنوان یک کارشناس و ادمین شبکه بایستی بر سطح امنیتی موجود در ساختار مجازی‌سازی شبکه، نظارت دقیقی نمایید.

مخاطرات و چالش‌های امنیتی در ماشین مجازی در سطوح مختلفی قابل بررسی است که در عکس زیر مشاهده می‌شود.

برای بررسی دقیق‌تر هر یک از چالش‌ها به مقاله زیر مراجعه شود.

https://www.sciencedirect.com/science/article/abs/pii/S0045790617320724



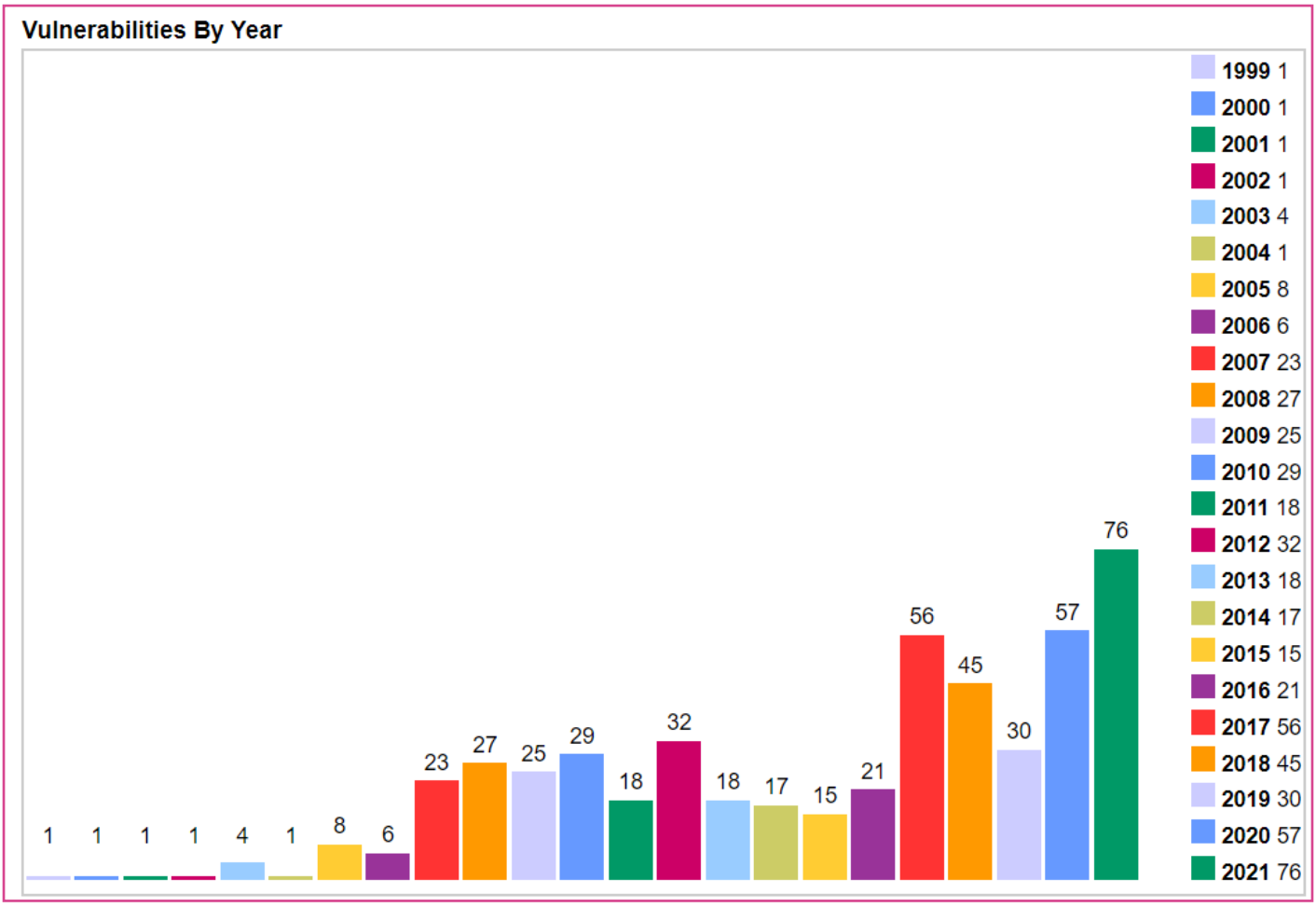
نکته حائز اهمیت این است که در حملاتی که در چند سال اخیر شاهد بودیم، مهاجمان به‌طور مستقیم اهداف خود را متمرکز بر دسترسی به ماشین‌های مجازی و حذف آن‌ها کرده‌اند که این می‌تواند چالشی جدی برای یک سازمان باشد. البته در بین ماشین‌های مجازی مختلف و متعددی که یک سازمان استفاده می‌کند، غالباً آسیب‌پذیرترین VM ها به‌عنوان نقطه شروع حملات مورد هدف قرار می‌گیرند. این نکته ضرورت توجه به امن‌سازی تمامی ماشین‌های مجازی مورد استفاده یک سازمان‌ها را بیش از پیش می‌کند. جدا از رعایت نکات ذکر شده درخصوص امن‌سازی و پیکربندی صحیح این بسترها، توجه به به‌روزرسانی‌ها و وصله‌های منتشر شده از طرف شرکت VMware برای محصولات تحت‌تاثیر نیز مهم و قابل توجه است.

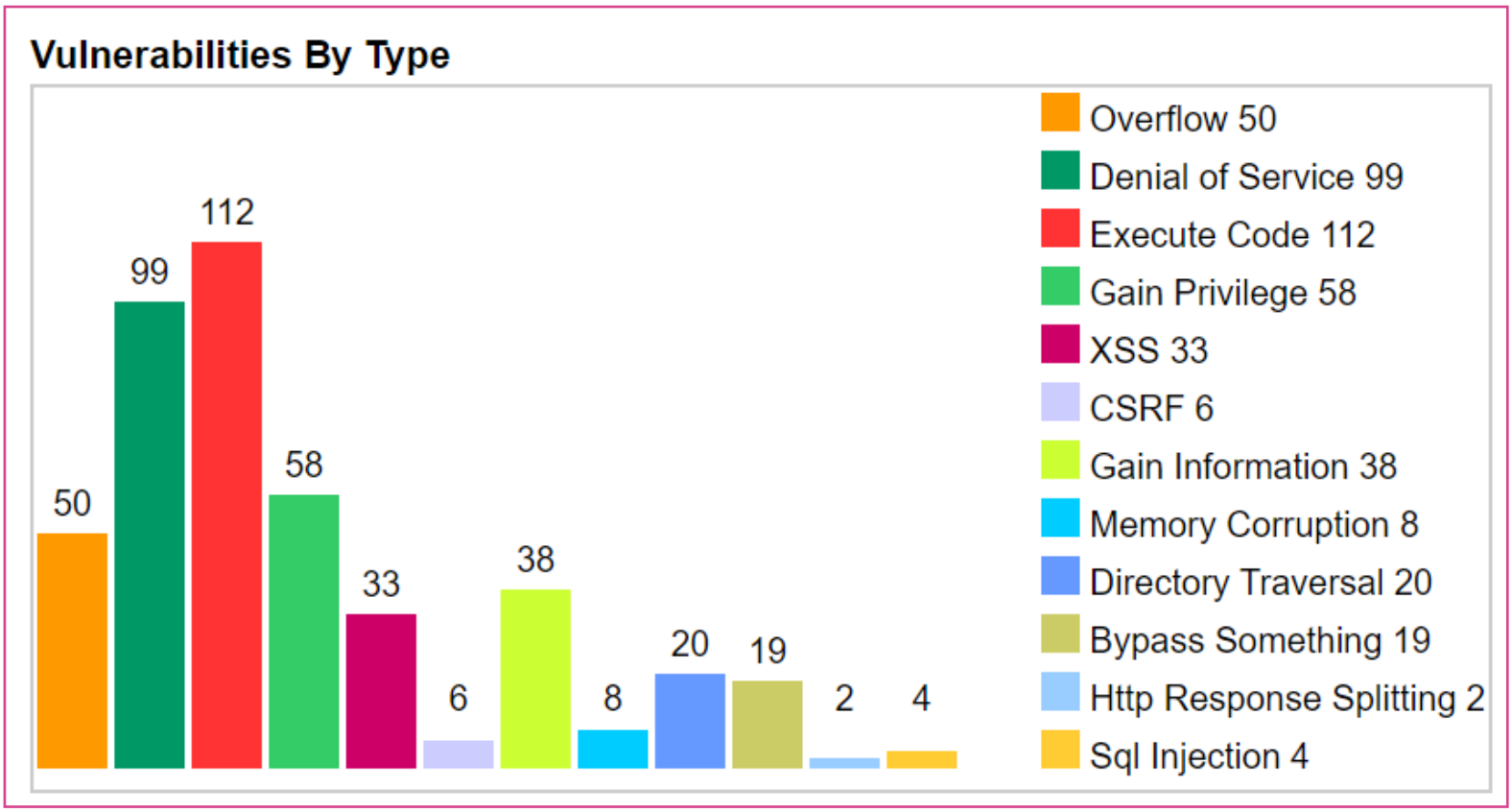
با دقت در آمار مربوط به تعداد آسیب‌پذیری‌های VMware که در بخش بعد نشان داده شده است، میبینم که در چند سال اخیر آمار آن رشد بالایی داشته است و مخصوصاً در یک سال اخیر در حدود ۲۰ درصد آسیب‌پذیری‌ها دارای حساسیت مهم و بحرانی بوده‌اند که بهره‌برداری از آن‌ها، منجر به چالش‌های جدی برای یک سازمان می‌شود. البته باید توجه داشت که برخی از آسیب‌پذیری‌ها دارای اکسپلویت هستند اما برای تمامی آن‌ها به‌صورت عمومی منتشر نشده است اما در لینک زیر می‌توان اکسپلویت‌هایی که به‌صورت عمومی برای محصولات VMware منتشر شده است را پیگیری و مشاهده کرد.

https://github.com/xairy/vmware-exploitation

در ادامه آمارهایی درخصوص آسیب‌پذیری‌های حساس و بحرانی محصولات VMware بررسی خواهند شد.

آسیب‌پذیری‌های VMware از سال ۱۹۹۹ تا دسامبر ۲۰۲۱



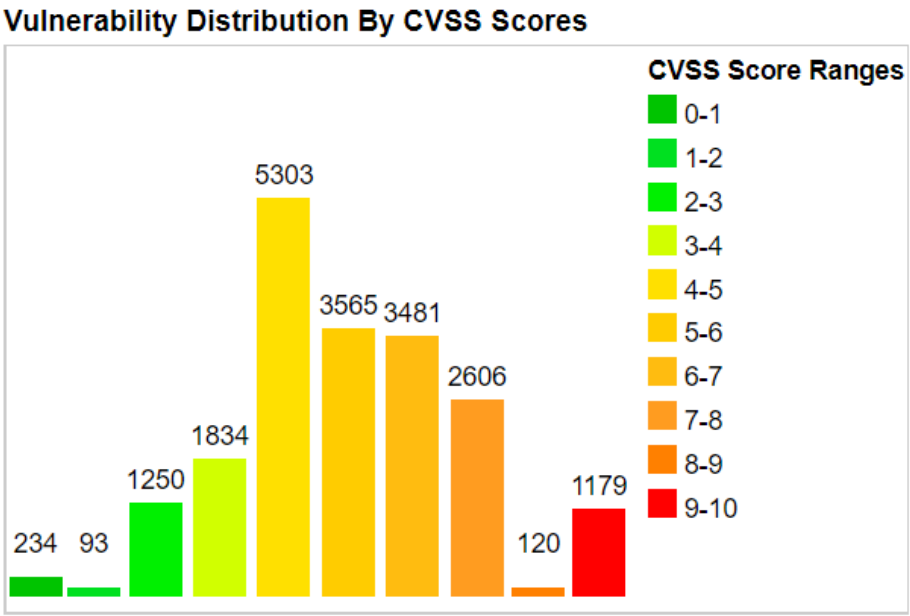


درجه حساسیت و تعداد آسیب‌پذیری‌های VMware از دسامبر ۲۰۲۰ تا دسامبر ۲۰۲۱

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	234	1.20
1-2	93	0.50
2-3	1250	6.40
3-4	1834	9.30
4-5	5303	27.00
5-6	3565	18.10
6-7	3481	17.70
7-8	2606	13.30
8-9	120	0.60
9-10	1179	6.00
Total	19665	

Weighted Average CVSS Score: **6**



در جدول زیر اطلاعات مربوط به آسیب‌پذیری‌های محصولات VMware از ابتدای سال ۲۰۲۰ تا دسامبر ۲۰۲۱ با درجه حساسیت‌های مهم و بحرانی نشان داده شده است.

شناسه آسیب‌پذیری	تاریخ انتشار	درجه حساسیت	نحوه دسترسی و نوع آسیب‌پذیری	محصولات تحت تاثیر آسیب‌پذیری
CVE-2021-22112	2021/02/23	9	بصورت Remote -	Spring by VMware
CVE-2021-22049	2021/11/24	7.5	بصورت Remote -	The vSphere Web Client (FLEX/Flash)
CVE-2021-22015	2021/9/23	7.2	بصورت Local -	VMware vCenter Server VMware Cloud Foundation
CVE-2021-22014	2021/9/23	9	بصورت Remote نوع Exec Code	VMware vCenter Server VMware Cloud Foundation
CVE-2021-22005	2021/9/23	7.5	بصورت Remote نوع Exec Code	VMware vCenter Server VMware Cloud Foundation
CVE-2021-22002	2021/8/31	7.5	بصورت Remote -	VMware Workspace ONE Access (Access) VMware Identity Manager (vIDM) VMware vRealize Automation (vRA) VMware Cloud Foundation vRealize Suite Lifecycle Manager
CVE-2021-21999	2021/6/23	7.2	بصورت Local نوع Exec Code	VMware Tools for Windows VMware Remote Console for Windows VMware App Volumes
CVE-2021-21998	2021/6/23	7.5	بصورت Remote نوع Bypass	VMware Carbon Black App Control (AppC)
CVE-2021-21986	2021/5/26	10	بصورت Remote -	VMware vCenter Server VMware Cloud Foundation
CVE-2021-21985	2021/5/26	10	بصورت Remote نوع Exec Code	VMware vCenter Server VMware Cloud Foundation
CVE-2021-21984	2021/5/26	7.5	بصورت Remote نوع Exec Code	VMware vRealize Business for Cloud
CVE-2021-21983	2021/3/31	8.5	بصورت Remote -	VMware vRealize Operations VMware Cloud Foundation vRealize Suite Lifecycle Manager
CVE-2021-21978	2021/3/3	7.5	بصورت Remote نوع Exec Code	VMware View Planner

محصولات تحت تاثیر آسیب‌پذیری	نحوه دسترسی و نوع آسیب‌پذیری	درجه حساسیت	تاریخ انتشار	شناسه آسیب‌پذیری
VMware ESXi VMware vCenter Server VMware Cloud Foundation	بصورت Remote نوع Exec Code	10	2021/2/24	CVE-2021-21972
Spring by VMware	بصورت Remote نوع Exec Code	7.5	2020/7/31	CVE-2020-5413
VMware Workspace One Access (Access) VMware Workspace One Access Connector (Access Connector) VMware Identity Manager (vIDM) VMware Identity Manager Connector (vIDM Connector) VMware Cloud Foundation vRealize Suite Lifecycle Manager	بصورت Remote -	9	2020/11/23	CVE-2020-4006
VMware ESXi VMware Workstation Pro / Player (Workstation) VMware Fusion Pro / Fusion (Fusion) VMware Cloud Foundation	بصورت Local -	7.2	2020/11/20	CVE-2020-4005
VMware SD-WAN Orchestrator (SD-WAN Orchestrator)	بصورت Remote -	7.5	2020/11/24	CVE-2020-4001
VMware ESXi VMware Workstation Pro / Player (Workstation) VMware Fusion Pro / Fusion (Fusion) NSX-T VMware Cloud Foundation VMware vCenter Server	بصورت Remote نوع Exec Code	10	2020/10/20	CVE-2020-3992
VMware Workstation Pro / Player (Workstation) VMware Fusion Pro / Fusion (Fusion) VMware Horizon Client for Windows VMware Remote Console for Windows	بصورت Local نوع Exec Code	7.2	2020/3/16	CVE-2020-3947

امید حسینی

لیست آسیب‌پذیری‌های
OWASP TOP 10-2021

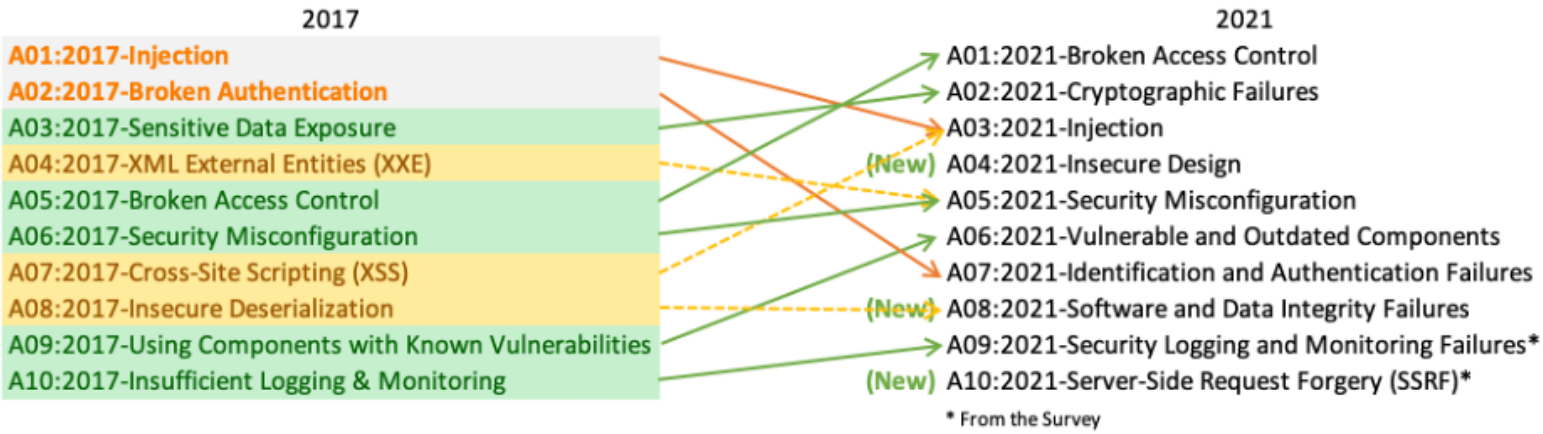
مقدمه

اگر یک طراح وب‌سایت هستید یا مدیریت یک وب‌سایت را به عهده دارید باید آگاهی کافی نسبت به خطرات احتمالی و آسیب‌پذیری‌هایی که وب‌سایت شما را تهدید می‌کنند داشته باشید.
در این مقاله می‌خواهیم آخرین به‌روزرسانی از ده آسیب‌پذیری مخرب که در در سال ۲۰۲۱ منتشرشده است را بررسی کنیم.

توجه:
تمرکز این مقاله بر روی تغییرات این لیست می‌باشد لذا برای دسترسی به توضیحاتی جامع در زمینه آسیب‌پذیری‌ها می‌توانید به فصل‌نامه شماره ۹ ویرا مراجعه کنید.

در لیست آسیب‌پذیری‌های OWASP TOP 10-2021 به نسبت سال ۲۰۱۷ چه تغییراتی ایجاد شده است؟

در لیست آسیب‌پذیری‌های مخرب ۲۰۲۱ سه دسته جدید insecure design, software and data integrity failures به لیست اضافه شده و عناوین چهار طبقه‌بندی نیز تغییر کرده است. همچنین تعدادی از دسته‌بندی‌ها با هم ادغام شده‌اند. دلیل تغییر نام بعضی از آسیب‌پذیری‌ها لزوم تمرکز بر علت اصلی به وجود آمدن آن‌ها است.



ده آسیب‌پذیری مخرب OWASP ۲۰۲۱ عبارتند از:

1. Broken Access Control
2. Cryptographic failures
3. Injection
4. Insecure design
5. Security Misconfiguration
6. Vulnerable and outdated components
7. Identification and authentication failures
8. Software and data Integrity failures
9. Security logging in monitoring failures
10. Server-side request forgery

Broken authentication

آسیب‌پذیری Broken authentication از جایگاه پنجم به جایگاه اول صعود کرده است و به جدی‌ترین خطر امنیتی برای وب اپلیکیشن‌ها تبدیل شده است.
داده‌های ارائه‌شده نشان می‌دهد که به‌طور متوسط، ۳٫۸۱٪ از برنامه‌های آزمایش‌شده دارای یک یا چند CWE هستند که از بین آن‌ها بیش از ۳۱۸ هزار مورد CWE در این دسته‌بندی قرار گرفته‌اند.

Cryptographic failures

نقص‌های رمزنگاری قبلا با نام sensitive data exposure شناخته می‌شد که به‌جای علت اصلی آسیب‌پذیری به یک موضوع کلی اشاره می‌کرد. نام گذاری جدید بر روی خطاهای مربوط به رمزنگاری تمرکز دارد. همچنین این آسیب‌پذیری از جایگاه سوم به جایگاه دوم صعود کرده است.
خطای رمزنگاری اغلب منجر به قرارگرفتن در معرض داده‌های حساس یا به خطر افتادن سیستم می‌شود.

injection

تزریق کد از جایگاه اول به جایگاه سوم نزول کرده است. ۹۴٪ از برنامه‌هایی که برای انواع تزریق کد آزمایش شدند حداکثر ۱۹٪ و میانگین ۳٫۳۷٪ شامل این آسیب‌پذیری بودند و ۳۳ CWE که در این دسته ثبت شده‌اند، با ۲۷۴ هزار مورد، بعد از Broken access control بیش‌ترین تعداد آسیب‌پذیری را در برنامه‌ها دارند.
همچنین در OWASP ۲۰۲۱، آسیب‌پذیری cross-site scripting در این دسته‌بندی قرارگرفته است و زیر مجموعه تزریق کد به حساب می‌آید.

Insecure sign

Insecure Design یک آسیب‌پذیری جدید است و این اولین بار است که ما در لیست آسیب‌پذیری‌های OWASP آن را مشاهده می‌کنیم.
طراحی ناامن، یک آسیب‌پذیری گسترده است که شامل نقاط ضعف مختلفی است که به‌عنوان «عدم کنترل طراحی یا ناکارآمدی کنترل طراحی» شناخته می‌شود. طراحی ناامن و پیاده‌سازی ناامن از هم متفاوت هستند. ما بین نقص‌های طراحی و نقص‌های پیاده‌سازی به دلایلی تفاوت قائل می‌شویم و دلایل ریشه‌ای به‌وجود آمدن آن‌ها و راهکارهای رفع آن‌ها متفاوت است. یک طراحی امن همچنان می‌تواند دارای نقص‌های پیاده‌سازی باشد که می‌تواند منجر به آسیب‌پذیری‌هایی شود که ممکن است مورد بهره‌برداری قرار بگیرند. یک طراحی ناامن را نمی‌توان با یک پیاده‌سازی بی‌نقص برطرف کرد، زیرا طبق تعریف، کنترل‌های امنیتی مورد نیاز که برای دفاع در برابر حملات خاص لازم هستند هرگز ایجاد نشده است. یکی از عواملی که به طراحی ناامن کمک می‌کند، فقدان رویکرد تشخیص و مدیریت ریسک در نرم افزار یا سیستم در حال توسعه است و در نتیجه نمی‌توان سطح طراحی امن مورد نیاز را تعیین کرد.

چگونه یک طراحی امن داشته باشیم؟

طراحی امن یک رویه و روش است که دائماً تهدیدات را ارزیابی می‌کند و تضمین می‌کند که کد به‌طور قوی و امن طراحی و آزمایش شده است تا از حملاتِ شناخته شده جلوگیری کند. شبیه‌سازی تهدید باید در جلسات اصلاح (یا فعالیت‌های مشابه) انجام شود. به دنبال تغییرات در گردش داده‌ها و کنترل دسترسی یا سایر کنترل‌های امنیتی باشید. در توسعه توضیحات ویژگی‌های اپلیکیشن، روند صحیح و شرایط خرابی را به درستی تعیین کنید، اطمینان حاصل کنید که آن‌ها به خوبی درک شده و افراد مسئول و صاحبان پروژه در آن به توافق رسیده‌اند. فرضیات و شرایطی را که در آن روند برنامه با شکست مواجه می‌شود را به خوبی تجزیه‌وتحلیل کنید، مطمئن شوید که دقیق و مطلوب هستند. نحوه تایید فرضیات و اجرای شرایط مورد نیاز برای رفتارهای مناسب را تعیین کنید. اطمینان حاصل کنید که نتایج در توضیحات ویژگی‌های برنامه مستند شده است.

جلوگیری از Insecure Design

- ایجاد و استفاده از چرخه توسعه امن (SDLC) با متخصصان امنیت نرم‌افزار برای کمک به ارزیابی و طراحی کنترل امنیت و حریم خصوصی
- استفاده از مدل‌سازی تهدید برای احراز هویت حیاتی، کنترل دسترسی، رد و بدل اطلاعات با کاربر و جریان‌های کلیدی
- ادغام تکنیک‌های امنیتی و کنترل‌ها در توضیحات ویژگی‌های اپلیکیشن
- بررسی دقت و کارایی برنامه خود در همه لایه‌ها (از فرانت اند تا بک اند)
- نوشتن تست‌های واحد و یکپارچه تا تأیید کنید که تمام فرآیندهای حیاتی در برابر مدل تهدید مقاوم هستند. اعمال مجاز و غیر مجاز را برای هر لایه از برنامه خود تعریف کنید.
- محدود کردن مصرف منابع توسط کاربر یا سرویس
- عدم دسترسی یکسان به کاربران و جدا کردن کاربران دارای سطوح مختلف دسترسی

Security Misconfiguration

این آسیب‌پذیری در نسخه پیشین این لیست در جایگاه ششم قرار داشت. ۹۰٪ از برنامه‌هایی که برای انواع پیکربندی نادرست آزمایش شدند میانگین ٤٫٥٪ شامل این آسیب‌پذیری بودند، و بیش از ۲۰۸ هزار مورد از CWEها در این دسته قرار دارند. با افزایش روز افزون نرم‌افزارها که نیاز به پیکربندی دارند ، تعجب‌آور نیست که ببینیم جایگاه این دسته به سمت بالاتر حرکت می‌کند.
آسیب‌پذیری XML External Entities که در نسخه قبل در جایگاه چهارم قرار داشت حالا بخشی از این دسته‌بندی است.

Vulnerable and Outdated Components

در نسخه قبلی به عنوان Using Components with Known Vulnerabilities شناخته می‌شد. این آسیب‌پذیری از جایگاه نهم به جایگاه ششم آمده است.

Identification and Authentication Failures

این آسیب‌پذیری قبلا با نام broken authentication شناخته می‌شد و در این نسخه در جایگاه هفتم قرار دارد درحالی‌که در نسخه پیشین در جایگاه دوم قرار داشت. درحال‌حاضر این آسیب‌پذیری شامل CWE هایی است که بیش‌تر به نقص شناسایی (Identification) مربوط می‌شوند. این دسته هنوز هم بخش جدایی‌ناپذیر از ۱۰ آسیب‌پذیری مخرب است، اما به نظر می‌رسد افزایش دسترسی به چارچوب‌های استاندارد در کمرنگ‌کردن آن کمک‌های زیادی کرده است.

Software and Data Integrity Failures

Software and Data Integrity Failures یک دسته‌بندی جدید برای سال OWASP ۲۰۲۱ است که برروی به‌روزرسانی نرم‌افزار، داده‌های حیاتی و روند CI/CD بدون تأیید صحت و امنیت داده تمرکز دارد. این آسیب‌پذیری یکی از بیش‌ترین سهم‌ها را در داده‌های آسیب‌پذیری رایج و سیستم امتیازدهی آسیب‌پذیری مشترک (CVE/CVSS) دارد. چند نقطه ضعف امنیتی رایج قابل توجه در این دسته در زیر آورده شده‌اند:

CWE-829: اضافه‌کردن کارایی از محیط کنترل غیرقابل اعتماد.

CWE-494: دانلود کد بدون بررسی امنیت و کیفیت آن.

CWE-502: deserialization داده‌های غیر قابل اعتماد.

برای کسب اطلاعات بیشتر در مورد deserialization به فصل‌نامه شماره ۹ ویرا مراجعه کنید.

جلوگیری Software and Data Integrity Failures

- از امضای دیجیتال یا مکانیسم‌های مشابه برای تأیید اینکه نرم افزار یا داده‌ها از منبع مورد انتظار هستند و تغییر نکرده‌اند، استفاده کنید.

- اطمینان حاصل کنید که کتابخانه‌ها و وابستگی‌ها، مانند npm یا Maven، از مخازن قابل اعتماد استفاده می‌کنند. همچنین برای اطمینان بیش‌تر، می‌توانید میزبانی یک مخزن داخلی شناخته شده را که امن است در نظر بگیرید.

- اطمینان حاصل کنید که یک ابزار امنیتی زنجیره تامین نرم‌افزار مانند OWASP Dependency Check یا OWASP CycloneDX، برای تأیید عدم وجود آسیب‌پذیری‌های شناخته شده در اجزا استفاده شود.

- اطمینان حاصل کنید که یک فرآیند بازبینی برای تغییرات کد و پیکربندی وجود دارد تا احتمال وارد شدن کد یا پیکربندی مخرب به کد نرم افزار شما به حداقل برسد.

- اطمینان حاصل کنید که شریان CI/CD شما دارای تفکیک، پیکربندی و کنترل دسترسی مناسب است تا از امنیت کدی که در فرآیندهای ساخت و عرضه جریان دارد اطمینان حاصل کنید.

- اطمینان حاصل کنید که داده‌های سریالی بدون امضای دیجیتال یا رمزگذاری به کاربران غیرقابل اعتماد، بدون بررسی صحت یا امضای دیجیتال ارسال نشوند تا از دستکاری و ارسال مجدد داده‌ها جلوگیری شود.

Security Logging and Monitoring Failures

این آسیب‌پذیری که قبلا با نام Insufficient Logging & Monitoring شناخته می‌شد در نسخه پیشین این لیست در جایگاه دهم قرار داشت. این دسته گسترش یافته است تا انواع بیش‌تری از خطاها را شامل شود. این آسیب‌پذیری مستقیما بر روی آمار بازدید وب‌سایت، سیستم هشدار رویدادها و روند تحقیقات روی خرابی‌ها و اعمال غیرقانونی کاربران تاثیر می‌گذارد.

Server-Side Request Forgery

جعل درخواست سمت سرور (همچنین به‌عنوان SSRF شناخته می‌شود) به مهاجم اجازه می‌دهد تا برنامه سمت سرور را وادار کند تا درخواست‌های HTTP را به دامنه دلخواه خود ارسال کند.

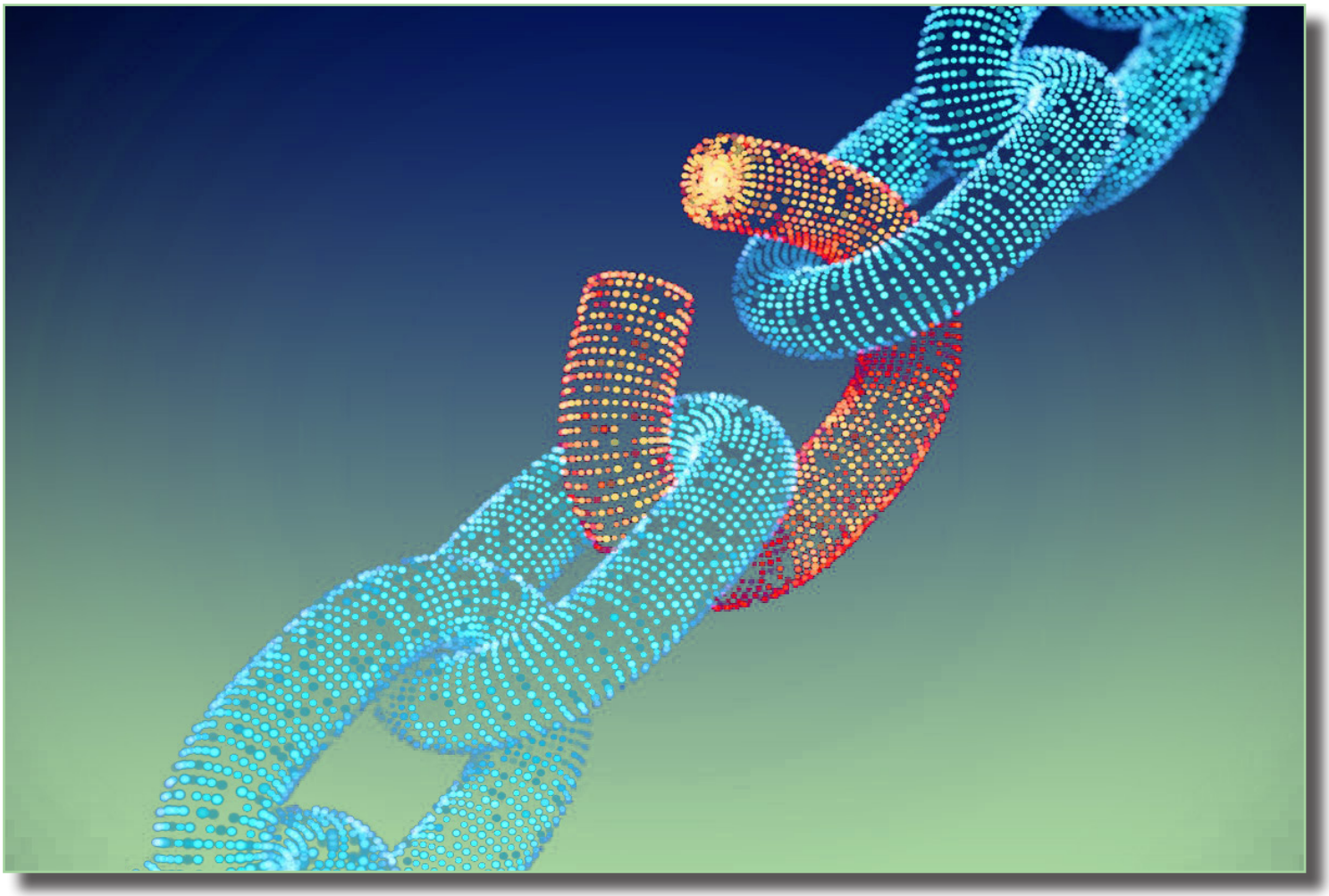
در یک حمله معمولی SSRF، مهاجم ممکن است باعث شود سرور به سرویس‌های داخلی در زیرساخت سازمان متصل شود. در موارد دیگر، آن‌ها ممکن است بتوانند سرور را مجبور به اتصال به سیستم‌های خارجی دلخواه کنند و به‌طور بالقوه داده‌های حساس مانند اعتبارنامه مجوز را نشت دهند.

یک سوءاستفاده SSRF که باعث اتصال به سیستم‌های شخص ثالث خارجی می‌شود ممکن است منجر به حملات مخرب بعدی شود که به نظر می‌رسد از سازمان میزبان منشأ می‌گیرند.

جلوگیری از Server-Side Request Forgery

در سطح برنامه:

- تمام داده‌های ورودی کاربران را فیلتر و اعتبارسنجی کنید.
- پاسخ‌های خام را برای مشتریان ارسال نکنید.
- تغییر مسیرهای HTTP را غیرفعال کنید.
- برای جلوگیری از حملاتی مانند DNS rebinding و «Time-of-check-to-time-of-use» از ثبات URL آگاه باشید.



معرفی ابزار

محمد حبیبی

معرفی ابزار Qu1cksc0pe

مقدمه

ابزار Qu1cksc0pe که با زبان پایتون توسعه داده شده است، قابلیت نصب بر روی سیستم‌عامل‌های لینوکسی را دارد. همچنین می‌توان این ابزار را با استفاده از Windows Subsystem Linux موجود در ویندوز ۱۰ اجرا کرد. این ابزار برای آنالیز استاتیک فایل‌های اجرایی ویندوز، لینوکس، مک و همچنین اپلیکیشن‌های اندرویدی طراحی شده است. با استفاده از این ابزار کاربر می‌تواند اطلاعات بیشتری در رابطه با فایل‌های مشکوک بدست بیاورد.

با استفاده از این ابزار می‌توان موارد زیر را بررسی کرد:

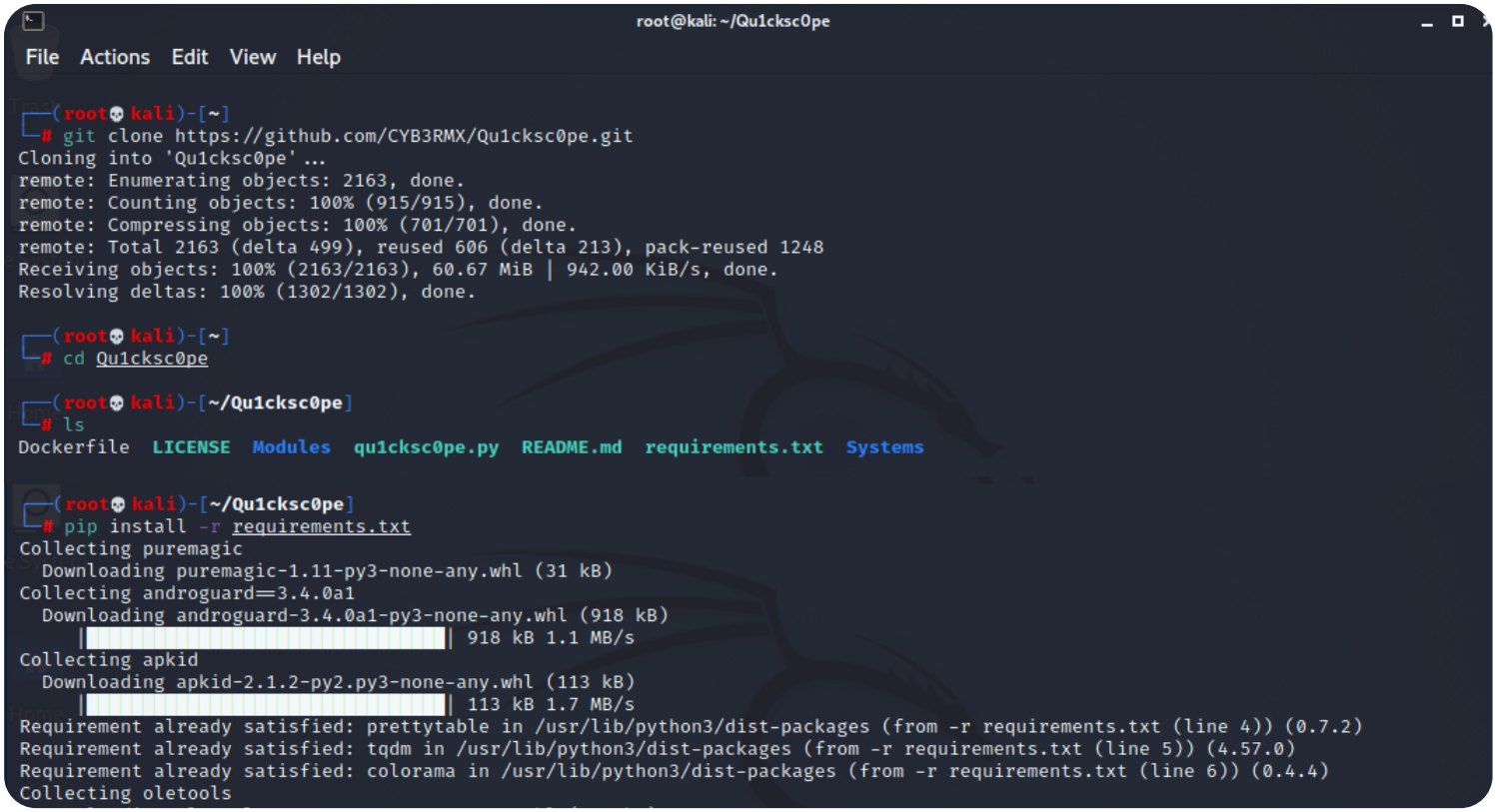
- فایل‌های DLL
- توابع و API ها
- بخش‌ها و سگمنت‌ها
- آدرس‌های URL، آدرس‌های IP و ایمیل‌ها
- مجوزهای مورد استفاده اپلیکیشن‌های اندرویدی
- افزونه‌های فایل‌ها

و مواردی دیگر

راه اندازی

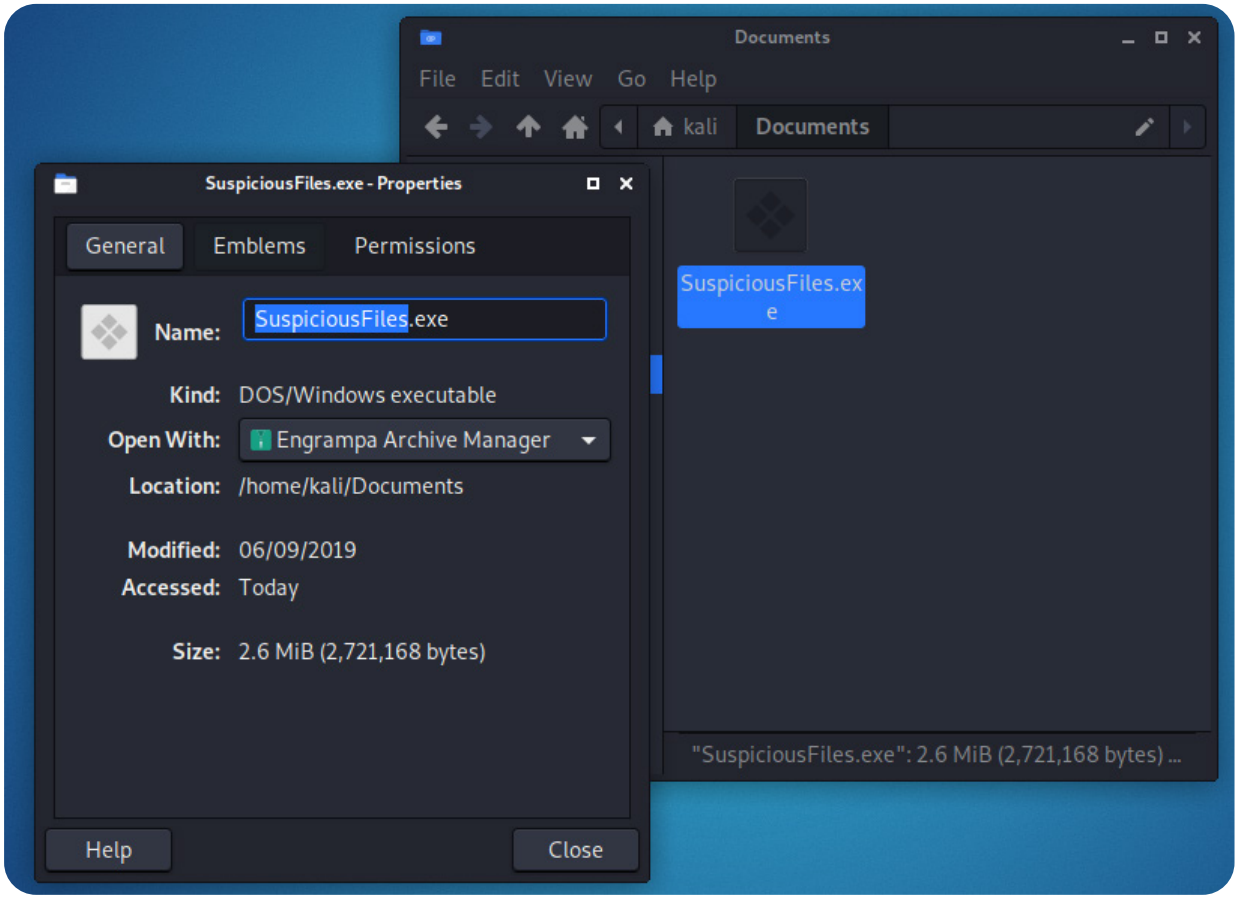
برای نصب ابزار نیاز است که پروژه را از مخزن گیت‌هاب به شکل زیر دانلود کرد، سپس ماژول‌های پایتون مورد نیاز آن را نصب کرد.

```
git clone https://github.com/CYB3RMX/Qu1cksc0pe.git
cd Qu1cksc0pe
pip install -r requirements.txt
```



اجرا

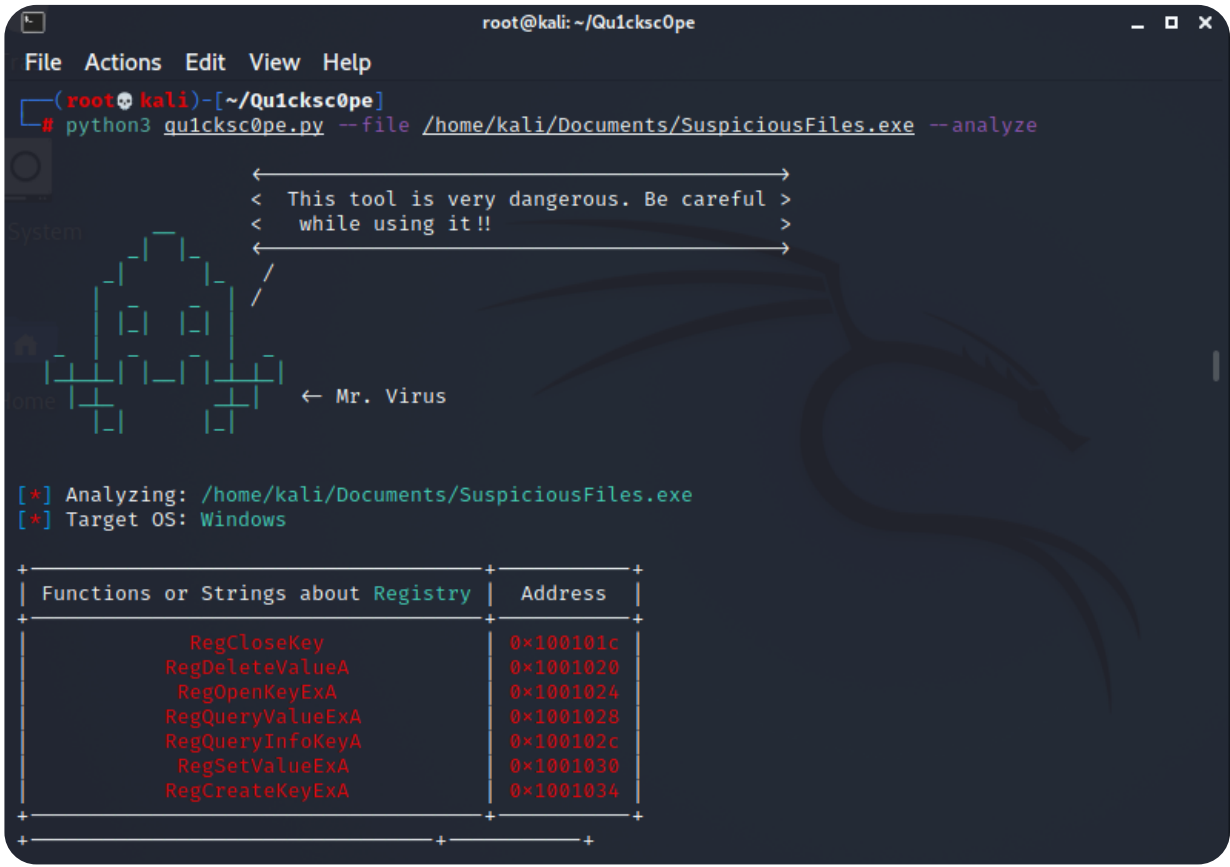
ابتدا یک فایل اجرایی ویندوزی را بر روی آزمایشگاه خود کپی می‌کنیم.



برای اجرای ابزار و بررسی فایل مورد نظر می‌توان دستور زیر را اجرا کرد:

```
python3 qu1cksc0pe.py --file /home/kali/Documents/SuspiciousFiles.exe --analyze
```

بخشی از خروجی دستورات را می‌توان در تصاویر زیر(این صفحه و صفحه بعد) مشاهده کرد.



```
root@kali: ~/Qu1cksc0pe
File  Actions  Edit  View  Help
|          RegSetValueExA          | 0x1001030 |
|          RegCreateKeyExA         | 0x1001034 |
+----------------------------------+-----------+

+----------------------------------+-----------+
| Functions or Strings about File  |  Address  |
+----------------------------------+-----------+
|       GetWindowsDirectoryA       | 0x1001070 |
|         CreateDirectoryA         | 0x1001074 |
|        GetFileAttributesA        | 0x1001078 |
|        GetModuleFileNameA        | 0x100107c |
|       GetSystemDirectoryA        | 0x1001080 |
|         RemoveDirectoryA         | 0x1001084 |
|             FindClose            | 0x1001088 |
|          FindNextFileA           | 0x100108c |
|           DeleteFileA            | 0x1001090 |
|        SetFileAttributesA        | 0x1001094 |
|          FindFirstFileA          | 0x100109c |
|        GetShortPathNameA         | 0x10010b8 |
|          LoadResource            | 0x10010d8 |
|             ReadFile             | 0x10010e4 |
|            WriteFile             | 0x10010e8 |
|         SetFilePointer           | 0x10010ec |
|          SetFileTime             | 0x10010f0 |
|     LocalFileTimeToFileTime      | 0x10010f4 |
|          CreateFileA             | 0x10010fc |
|       SetCurrentDirectoryA       | 0x1001100 |
|          GetTempPathA            | 0x100112c |
|     GetSystemTimeAsFileTime      | 0x1001188 |
+----------------------------------+-----------+

+------------------------------------+-----------+
| Functions or Strings about Process |  Address  |
```

```
root@kali: ~/Qu1cksc0pe
File  Actions  Edit  View  Help
|     GetSystemTimeAsFileTime      | 0x1001188 |
+----------------------------------+-----------+

+------------------------------------+-----------+
| Functions or Strings about Process |  Address  |
+------------------------------------+-----------+
|          OpenProcessToken          | 0x1001010 |
|       AdjustTokenPrivileges        | 0x1001014 |
|        GetCurrentProcess           | 0x1001058 |
|           CloseHandle              | 0x10010e0 |
|           ExitProcess              | 0x1001114 |
|          CreateProcessA            | 0x1001128 |
|           CreateMutexA             | 0x1001134 |
|           CreateThread             | 0x1001140 |
|          TerminateThread           | 0x1001148 |
|       GetCurrentProcessId          | 0x1001184 |
|         TerminateProcess           | 0x100118c |
|       WaitForSingleObject          | 0x10011a0 |
+------------------------------------+-----------+

+--------------------------------------------+-----------+
| Functions or Strings about Memory Management |  Address  |
+--------------------------------------------+-----------+
|                  LocalFree                 | 0x100104c |
|                  LocalAlloc                | 0x1001050 |
|                  GlobalFree                | 0x10010a4 |
|                 GlobalUnlock               | 0x10010a8 |
|                  GlobalLock                | 0x10010ac |
|                 GlobalAlloc                | 0x10010b0 |
|                    memcpy                  | 0x1001270 |
|                    memset                  | 0x1001274 |
+--------------------------------------------+-----------+

+--------------------------------------------------+-----------+
```

```
root@kali: ~/Qu1cksc0pe
File  Actions  Edit  View  Help
>> Time Date Stamp: Mon Jul 13 23:42:43 2009 UTC
+---------------+---------------+-----------------+-----------------+-----------------+-------
---+
| Section Name | Virtual Size | Virtual Address | Size Of Raw Data | Pointer to Raw Data |
   |
+---------------+---------------+-----------------+-----------------+-----------------+-------
---+
|    .text      |    0×aae4     |     0×1000      |     0×ac00      |      0×400      |
   |
|    .data      |    0×225c     |     0×c000      |     0×600       |      0×b000     |
   |
|    .rsrc      |   0×28b000    |     0×f000      |    0×28aa00     |      0×b600     | 7.990
!) |
|    .reloc     |    0×d98      |    0×29a000     |     0×e00       |     0×296000    |
   |
+---------------+---------------+-----------------+-----------------+-----------------+-------
---+

→ Statistics for: /home/kali/Documents/SuspiciousFiles.exe
+----------------------+-----------------------------+
|      Categories      | Number of Functions or Strings |
+----------------------+-----------------------------+
|    All Functions     |              93             |
|       Registry       |              7              |
|        File          |              22             |
|      Process         |              12             |
|   Memory Management  |              8              |
| Dll/Resource Handling |             8              |
|   Evasion/Bypassing  |              3              |
|   System/Persistence |              2              |
| Information Gathering |             18             |
|    Other/Unknown     |              13             |
+----------------------+-----------------------------+
```

برای آنالیز چند فایل می‌توان به شکل زیر عمل کرد:

```
python3 qu1cksc0pe.py --multiple FILE1 FILE2 FILE3
```

بررسی Hash مرتبط با فایل:

```
python3 qu1cksc0pe.py --file suspicious_file --hashscan
```

در این نوع بررسی ابزار هش بدست آمده از فایل مشکوک را در پایگاه داده خود جستجو می‌کند و تطابق هش با بدافزارهای ثبت شده را بررسی می‌کند.

```
root@kali: ~/Qu1cksc0pe
File  Actions  Edit  View  Help
1.64kKB [00:01, 996KB/s]

┌──(root💀 kali)-[~/Qu1cksc0pe]
└─# sudo python3 qu1cksc0pe.py --file /home/kali/Documents/SuspiciousFiles.exe --hashscan

                                .oodMMMM
                            .oodMMMMMMMMMMMMM
                 .. oodMMM  MMMMMMMMMMMMMMMMMMMM
          oodMMMMMMMMMMMM   MMMMMMMMMMMMMMMMMMMM
           MMMMMMMMMMMMMMM  MMMMMMMMMMMMMMMMMMMM
           MMMMMMMMMMMMMMM  MMMMMMMMMMMMMMMMMMMM
           MMMMMMMMMMMMMMM  MMMMMMMMMMMMMMMMMMMM
           MMMMMMMMMMMMMMM  MMMMMMMMMMMMMMMMMMMM
           MMMMMMMMMMMMMMM  MMMMMMMMMMMMMMMMMMMM

           MMMMMMMMMMMMMMM  MMMMMMMMMMMMMMMMMMMM
           MMMMMMMMMMMMMMM  MMMMMMMMMMMMMMMMMMMM
           MMMMMMMMMMMMMMM  MMMMMMMMMMMMMMMMMMMM
           MMMMMMMMMMMMMMM  MMMMMMMMMMMMMMMMMMMM
           MMMMMMMMMMMMMMM  MMMMMMMMMMMMMMMMMMMM
           ^^^^^^^MMMMMMM   MMMMMMMMMMMMMMMMMMMM
                  ^^^^^^^   ^^MMMMMMMMMMMMMMMMMMM
                                ^^^^^^^^^^^^MMMM

[*] Total Hashes: 47650
[*] File Name: /home/kali/Documents/SuspiciousFiles.exe
[*] Target Hash: 2a63268a0350709048278cd0914efe413439392a

[!] Target hash is not in our database.
[*] Try --analyze and --vtFile instead.
```

One day Windows will be MALWAREPROOF ...

Just kidding XDD

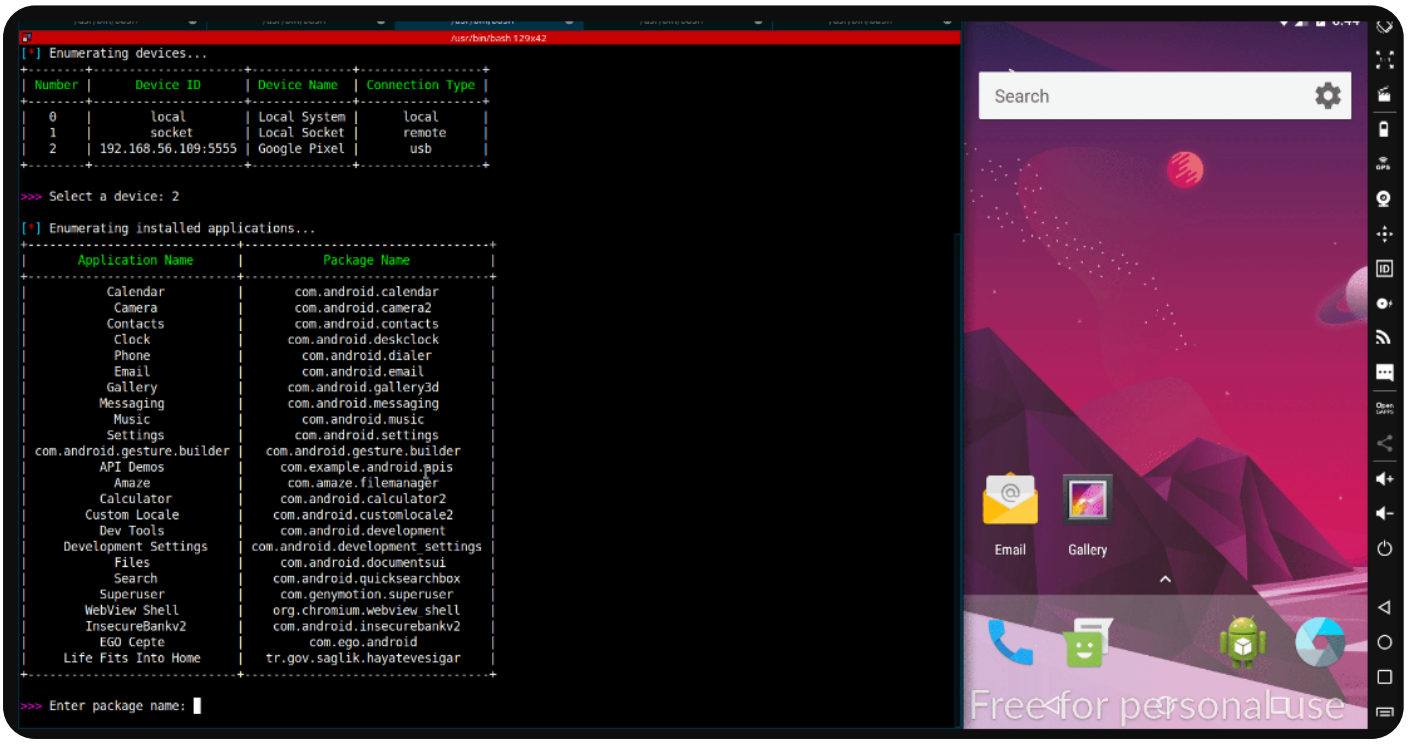
در صورتی که از نسخه‌های جدید کالی لینوکس استفاده می‌کنید یا به هر دلیلی دسترسی به حساب کاربری root برای شما محدود شده است، ممکن است اجرای این دستور با خطایی به شکل زیر مواجه شود:

```
root@kali: ~/Qu1cksc0pe
File  Actions  Edit  View  Help
[*] Downloading signature database please wait ...

┌──(root💀 kali)-[~/Qu1cksc0pe]
└─# sudo python3 qu1cksc0pe.py --file /home/kali/Documents/SuspiciousFiles.exe --hashscan

                 <  This tool is very dangerous. Be careful >
                 <   while using it !!                      >

                                    ← Mr. Virus

mkdir: cannot create directory '/home/root/sc0pe_Base/': No such file or directory
[!] Local signature database not found.
⇒ Would you like to download it [Y/n]?: y

[*] Downloading signature database please wait ...
```

برای حل این مشکل می‌توان فایل hashScanner.py را در دایرکتوری Modules مانند تصویر زیر تغییر داد. یعنی مقدار {username} به نام کاربری دلخواه که در اینجا kali است تغییر پیدا کند.

```
root@kali: ~/Qu1cksc0pe/Modules
File  Actions  Edit  View  Help
  GNU nano 5.4                    hashScanner.py
sc0pe_path = open(".path_handler", "r").read()

# User home detection
homeD = "/home"
if sys.platform == "darwin":
    homeD = "/Users"

# Directory checking
if os.path.exists(f"{homeD}/kali/sc0pe_Base/"):
    pass
else:
    os.system(f"mkdir {homeD}/kali/sc0pe_Base/")

# Configurating installation directory
install_dir = f"{homeD}/kali/sc0pe_Base"

def DatabaseCheck():
    if os.path.isfile(f"{install_dir}/HashDB.json") == False:
        print(f"{errorS} Local signature database not found.")
        choose = str(input(f"{green}⇒{white} Would you like to download it [Y/n]?: "))
        if choose == "Y" or choose == "y":
            local_database = f"{install_dir}/HashDB.json"
            dbUrl = "https://raw.githubusercontent.com/CYB3RMX/MalwareHashDB/main/HashDB.json"
            req = requests.get(dbUrl, stream=True)
            total_size = int(req.headers.get('content-length', 0))
            block_size = 1024
            wrote = 0
            print(f"\n{infoS} Downloading signature database please wait ...")
            try:
                with open(local_database, 'wb') as ff:
                    for data in tqdm(req.iter_content(block_size), total=math.ceil(total_size//bl>
                        wrote = wrote + len(data)
```

در به‌روزرسانی ماه اکتبر ۲۰۲۱ نیز ماژول AndroidRuntime به این ابزار اضافه شد که قابلیت تحلیل داینامیک اپلیکیشن‌های اندرویدی را فراهم می‌کند.



پویش‌های کاربردی ابزار Qu1cksc0pe

کاربرد	دستور
بررسی هش فایل‌های موجود در یک دایرکتوری	python3 qu1cksc0pe.py --folder FOLDER --hashscan
بررسی فایل با استفاده از موتورهای سایت VirusTotal	python3 qu1cksc0pe.py --file suspicious_file --vtFile
بررسی اسناد	python3 qu1cksc0pe.py --file suspicious_document --docs
تشخیص زبان برنامه‌نویسی استفاده شده	python3 qu1cksc0pe.py --file suspicious_executable --lang
استخراج دامنه‌ها از فایل اجرایی	python3 qu1cksc0pe.py --file suspicious_file --domain

دسته‌بندی‌های موجود در این ابزار

- Registry
- File
- Networking/Web
- Process
- Dll/Resource Handling
- Evasion/Bypassing
- System/Persistence
- COMObject
- Cryptography
- Information Gathering
- Keyboard/Keylogging
- Memory Management

دفترچه تقلب

ژینو سفاحی

دفترچه تقلب ابزار

BURPSUITE

مقدمه

Burp یا Burp Suite مجموعه‌ای از چندین ابزار توسعه‌داده شده در جاوا است که بیشتر برای تست‌نفوذ در وب‌اپلیکیشن‌ها استفاده می‌شود. Burp Suite توسط شرکت امنیت وب Portswigger توسعه‌یافته است. Burp Suite یک ابزار GUI بوده که هدف آن اجرای مجموعه‌ای از ابزارها است و قابلیت‌های آن را می‌توان با نصب افزونه‌هایی به نام BApps افزایش داد. این ابزار باتوجه به امکانات و قابلیت‌هایی که در اختیار کاربر قرار می‌دهد، یکی از مجموعه ابزارهای پراستفاده و محبوب بین متخصصین حوزه تست نفوذ و باگ‌بانتی است.
این برنامه تا حد زیادی به متخصصین حوزه تست نفوذ کنترل کامل داده و اجازه می‌دهد تکنیک‌های مختلف و پیشرفته‌ای را با یکدیگر ترکیب نموده و به این ترتیب سریع‌تر، موثرتر و به‌صورت خودکار امور ارزیابی امنیتی را انجام دهند. در اصل یکی از کارکردهای اصلی این ابزار این است که به‌صورت یک پروکسی عمل کرده و با کمک آن می‌توان درخواست و پاسخ‌های HTTP/S را در بین مرورگر محلی و وب‌سایت هدف تحلیل کرده و در صورت لزوم آن را ویرایش کرد.
در ادامه دفترچه تقلب یا Cheat Sheet از قابلیت‌های این ابزار ارائه می‌شود.

Burp suite در کالی لینوکس

Spider

ابزار Spider یک spider/crawler وب است که برای تهیه نقشه از وب‌سایت یا وب‌اپلیکیشن مورد نظر استفاده می‌شود. در فرایند نگاشت لیستی از endpoints را به ما ارائه می‌دهد تا بتوان عملکرد آن‌ها را مشاهده و آسیب‌پذیری‌های احتمالی را شناسایی کنیم. Spidering یا crawling به این دلیل انجام می‌شود که هرچه endpoints بیشتری در طی فرآیند شناسایی جمع‌آوری کنیم، سطوح حمله بیشتری را در طی تست واقعی خود داریم.

Proxy

Burp Suite دارای یک پروکسی است که به کاربر اجازه می‌دهد محتوای درخواست‌ها و پاسخ‌ها را در حین انتقال ببیند و تصحیح کند. همچنین به کاربر کمک می‌کند تا درخواست یا پاسخ را تحت نظارت ابزار دیگری در Burp Suite پایان دهد. پروکسی در Burp Suite همچنین می‌تواند برای فیلتر کردن انواع خاصی از درخواست-پاسخ‌ها تنظیم شود.

Intruder

Intruder ابزاری است که به ما این امکان را می‌دهد انواع مختلفی از حملات را انجام دهیم که از آن‌ها برای یافتن انواع آسیب‌پذیری‌ها می‌توان استفاده کرد.
برخی از رایج‌ترین حملاتی که می‌توان با استفاده از Intruder انجام داد Brute-forcing، Enumeration، Fuzzing و Application layer DoS می‌باشد.

Repeater

این یک ابزار بسیار ساده برای دستکاری و انتشار مجدد پیام‌های HTTP و WebSocket به‌صورت دستی و تجزیه و تحلیل پاسخ‌های وب‌اپلیکیشن است.

Sequencer

Burp Sequencer ابزاری است که برای تجزیه‌وتحلیل کیفیت تصادفی بودن توکن‌های application session و سایر موارد داده مهم استفاده می‌شود. این توکن‌ها عموماً برای احراز هویت در عملیات‌های حساس مثل کوکی‌ها و توکن‌های anti-CSRF استفاده می‌شوند.

Decoder

Decoder (رمزگشا) متدهای رمزگذاری رایج مانند Base64، HTML، URL، Hex و غیره را فهرست می‌کند. رمزگشا هنگام جستجوی بخش زیادی از داده در مقادیر پارامترها می‌تواند به کار آید.

Extender

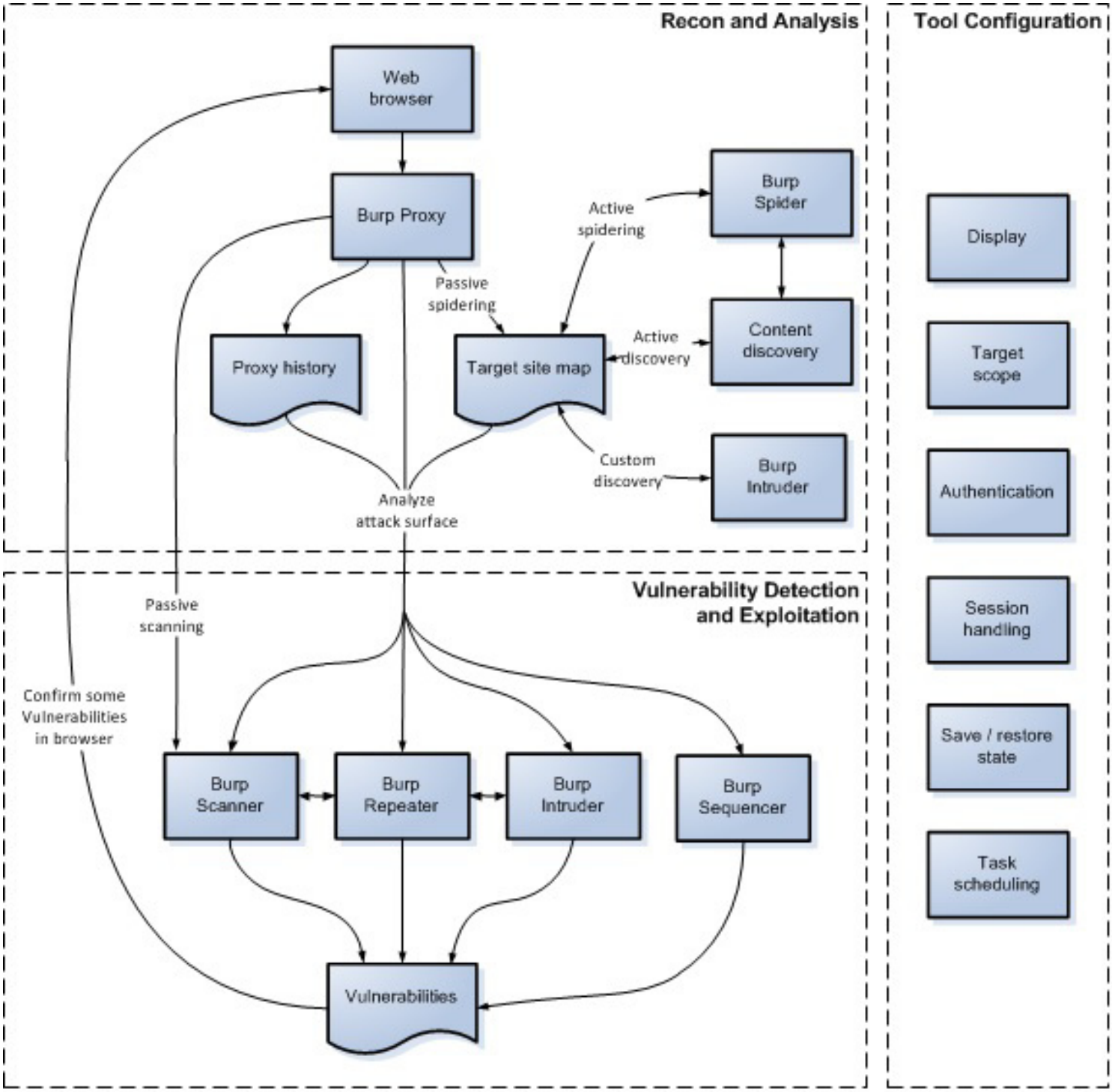
Extender به ما اجازه می‌دهد تا برنامه‌های افزودنی مختلفی را بارگذاری کنیم که می‌توان از آن‌ها برای کارآمدتر کردن تست نفوذ استفاده کرد. این افزونه‌ها BApps نامیده می‌شوند که دقیقاً مانند افزونه‌های مرورگر کار می‌کنند. این افزونه‌ها قابل مشاهده، تغییر، نصب و حذف نصب در تب Extender هستند.

Scanner

اسکنر به‌طور خودکار بسیاری از آسیب‌پذیری‌های رایج در وب اپلیکیشن مورد نظر را پویش می‌کند. به‌طور مکرر به‌روزرسانی می‌شود و آسیب‌پذیری‌های کمتر شناخته‌شده زیادی را که با به‌روزرسانی‌ها به‌دست‌آمده، به پایگاه داده‌اش اضافه می‌کند.

Comparer

این بخش برای انجام مقایسه داده‌های اپلیکیشن برای یافتن تفاوت‌های ساختاری استفاده می‌شود و به‌عنوان‌مثال دو پاسخ دریافتی از وب‌سایت را با هم مقایسه می‌کند.



Proxy > Intercept tab And click Open Browser

برای استفاده از Burp Suite در تست نفوذ، می‌توانید از مرورگر تعبیه‌شده (این بخش از نسخه 2020.7 به بعد موجود است) در Burp استفاده‌کنید یا مرورگر خارجی خود را بر روی پروکسی پیش‌فرض Burp با آدرس 127.0.0.1 و پورت 8080 تنظیم کنید.

Proxy > Intercept tab

اطمینان از این که شنود روشن است.

Intercept tab

هر درخواست HTTP که توسط مرورگر شما ارسال می‌شود در صورت فعال بودن حالت شنود قبل از ارسال به سمت وب‌سرور مقصد، در این تب نمایش داده می‌شود.

Forward button

درصورت انجام تغییرات بر روی پیام، با این دکمه می‌توان درخواست را به وب‌سرور مقصد ارسال کرد.

Intercept is on/off button

امکان فعال یا غیرفعال کردن حالت شنود را فراهم می‌کند.

Proxy > HTTP history tab

رکوردی از تمام درخواست‌ها و پاسخ‌ها، حتی زمانی که شنود خاموش است، نگه می‌دارد. از این برگه می‌توانید گزارشی از درخواست‌هایتان را تهیه و بررسی کنید.

Inspector panel

یک پنل است که ویژگی‌های کلیدی زیر را ارائه می‌دهد:

- بدون نیاز به جابه‌جایی بین تب‌های مختلف، ویژگی پیام‌های HTTP و WebSocket را به سرعت مشاهده و ویرایش کنید.
- مقادیر کاملاً رمزگشایی شده پارامترها، کوکی‌ها یا زیر رشته‌ای را که در ویرایشگر انتخاب کرده‌اید، مشاهده کنید.
- به جای کار با دستورات خام HTTP، با کلیک بر روی یک دکمه موارد را اضافه، حذف و مجدداً تنظیم کنید.
- داده‌ها را به شکل رمزگشایی شده ویرایش کنید. دنباله‌ای که مربوط به رمزگذاری به‌طور خودکار است هنگام به‌روزرسانی درخواست دوباره اعمال می‌شود.
- پروتکل مورد استفاده برای ارسال درخواست‌های فردی را تغییر دهید. Burp به طور خودکار تبدیل‌های لازم را برای ایجاد یک درخواست معادل برای پروتکل جدید انجام می‌دهد.
- با (header) سرایندهای HTTP و شبه سرایندها بدون وابستگی به گرامر HTTP/1 ویرایشگر پیام کار کنید. این کار تعدادی از تکنیک‌های پیشرفته را برای آزمایش اختصاصی HTTP/2 ساده می‌کند.

Target > Site map tab

به‌طور پیش‌فرض یک نقشه سایت از اپلیکیشن مورد نظر ایجاد می‌کند.

Target tool

یک نمای کلی از محتوا و عملکرد برنامه مورد نظر ارائه می‌دهد و بعد از نقشه‌برداری کامل اپلیکیشن و ارزیابی سطح حمله آن، به شما این امکان را می‌دهد که تست workflow را هدایت کنید.

Proxy > Intercept, HTTP history or Site map tabs

امکان ارسال پیام در هر جایی از Burp که پیام‌های HTTP را می‌بینید را دارید.

تنظیمات ابزار

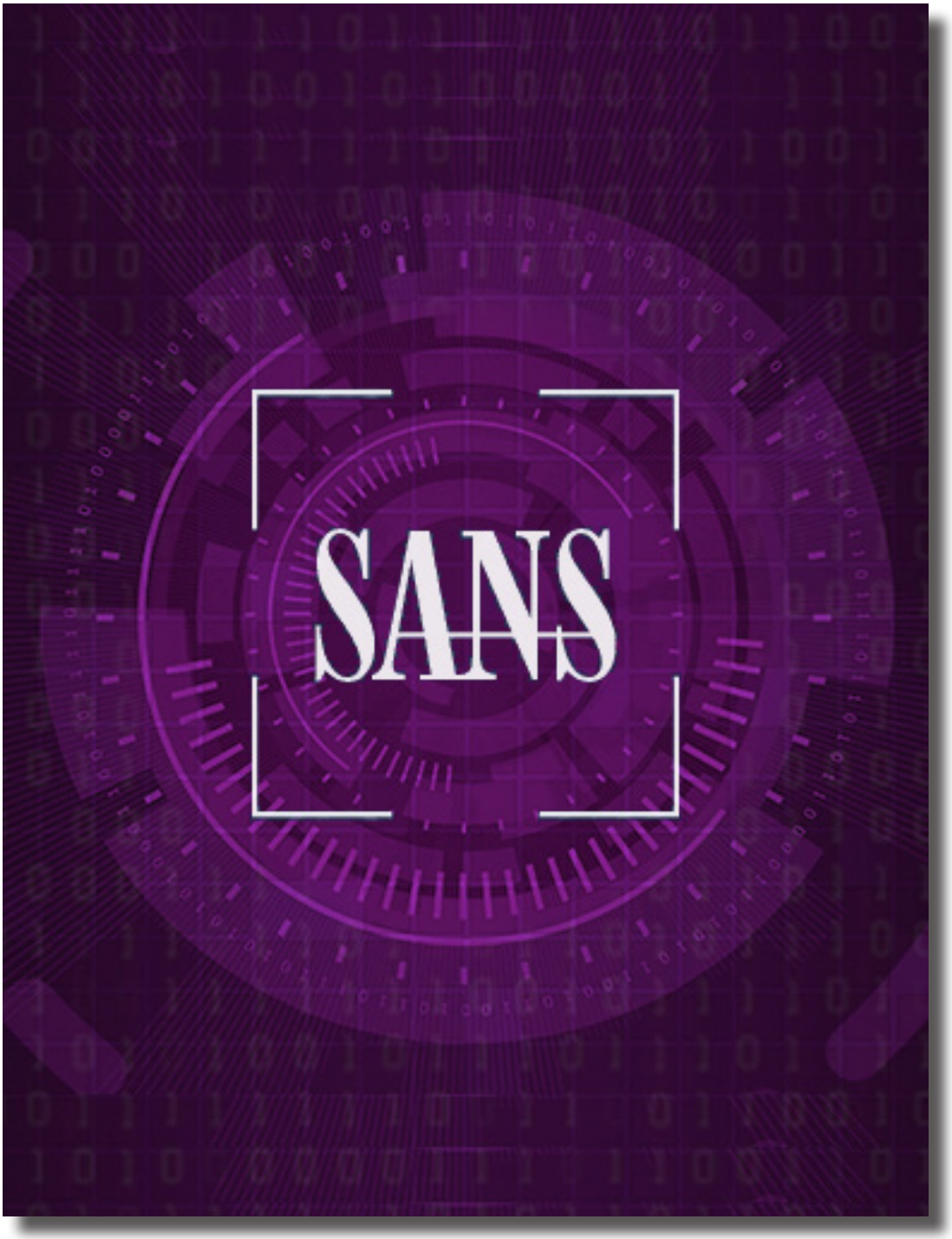
Display	می‌توانید مجموعه فونت و کاراکتر مورد استفاده برای نمایش پیام‌های HTTP و همچنین فونت را در رابط کاربری خود Burp تنظیم کنید.
Target scope	پیکربندی محدوده هدف به Burp مواردی را انتقال می‌دهد که می‌خواهید به آن‌ها حمله کنید. باید این پیکربندی را در اوایل تست انجام دهید، زیرا می‌تواند مواردی را که نمایش داده می‌شود در تاریخچه پروکسی، نقشه سایت هدف، پیام‌هایی شنود شده در پروکسی و هر موردی که ممکن است اسکن شوند، کنترل کند.
Platform authentication	اگر سرور اپلیکیشن از هر نوع احراز هویت سطح پلت فرم (HTTP) استفاده می‌کند، Burp را برای کنترل خودکار احراز هویت می‌توان پیکربندی کرد.
Session handling	بسیاری از اپلیکیشن‌ها دارای ویژگی‌هایی هستند که می‌توانند از تست خودکار یا دستی جلوگیری‌کنند.
Task scheduling	می‌توانید Burp را برای برنامه‌ریزی وظایف در زمان‌ها یا فواصل زمانی معین، پیکربندی کنید تا به شما امکان دهد در پنجره‌های آزمایشی مشخص کار کنید.

معرفی دوره

آرش بهرام‌زارعی

معرفی دوره SEC579

Virtualization And Software-Defined Security



مقدمه

دوره آموزشی SEC579 با موضوع مجازی‌سازی و امنیتِ تعریف‌شده نرم‌افزاری توسط موسسه SANS ارائه شده است. موسسه آموزشی SANS با نام کامل Information Security Training Cyber Certification and Research در سال ۱۹۸۹ به‌عنوان یک مجموعه آموزشی و تحقیقاتی ایجاد گردید. طبق گفته کارشناسان، SANS در حال حاضر یکی از مهم‌ترین، معتبرترین و بزرگ‌ترین مراکز آموزشی دوره‌های امنیت سایبری در دنیا می‌باشد.
در این موسسه دوره‌های مختلفی با موضوعاتی گسترده در حوزه امنیت سایبری ارائه می‌شود که موضوعات این دوره‌ها شامل تست نفوذ، جرائم رایانه‌ای، امنیت شبکه و حسابرسی سیستم‌ها می‌باشد. مدارک برخی از دوره‌های این موسسه را GIAC صادر و تایید می‌کند. مجله معتبر SC Magazine به‌صورت مستمر برنامه‌های آموزش امنیت اطلاعات موسسه SANS را به‌عنوان بهترین موسسه آموزشی به رسمیت شناخته است. دوره‌های ارائه شده توسط SANS به فراگیران خود خواهد آموخت که چگونه از سیستم‌ها و شبکه‌های خود در برابر خطرات بالقوه امنیتی این حوزه دفاع کنند. ارائه دوره‌های SANS به کمک متخصصان و محققانی در سراسر دنیا انجام می‌شود که هر کدام در زمینه‌های مختلف امنیت اطلاعات در سازمان‌های دولتی، شرکت‌ها و دانشگاه‌ها همه ساله زمان بسیاری را به تحقیق در این زمینه‌ها اختصاص می‌دهند. دوره آموزشی SEC579 به‌عنوان یکی از دوره‌های آموزشی این مرکز پیرامون مبحث مجازی‌سازی و امنیتِ تعریف‌شده نرم‌افزاری است که در ادامه توضیحاتی در این‌خصوص ارائه می‌شود.

معرفی دوره

یکی از مطرح‌ترین و گسترده‌ترین فناوری‌های امروزی مخصوصاً در سازمان‌ها و شرکت‌های بزرگ، استفاده از مجازی‌سازی است. اگر بخواهیم تعریفی از مجازی‌سازی ارائه کنیم، می‌توان گفت استفاده از سخت‌افزار و منابع سخت‌افزاری شامل حافظه، پردازنده، دیسک، کارت شبکه و غیره در یک سیستم کامپیوتری برای راه‌اندازی و استفاده (میزبانی) بیش از یک سیستم عامل به‌صورت همزمان را مجازی‌سازی می‌گوییم.

بسیاری از سازمان‌ها در حال حاضر متوجه صرفه‌جویی در هزینه‌های پیاده‌سازی سرورهای مجازی شده‌اند و مدیران سیستم‌ها، سهولت و مدیریت کار با سیستم‌های مجازی‌سازی شده را دوست دارند. از جمله مزایای مجازی‌سازی می‌توان به موارد زیر اشاره کرد:

- کاهش هزینه خرید تجهیزات سخت‌افزاری
- متمرکز سازی
- کاهش هزینه‌های جاری نظیر برق، نگهداری، تعمیرات
- کاهش گرمای تولیدی توسط دستگاه‌ها
- عدم نیاز به فضای زیاد نسبت به حالت سنتی
- استفاده از بیش‌ترین ظرفیت تجهیزات سخت‌افزاری
- جابجایی راحت
- پشتیبان‌گیری ساده از اطلاعات
- تسریع امور به خاطر وجود بالقوه دستگاه‌ها و عدم نیاز به صرف زمان برای خرید، نصب و آماده‌سازی
- امکان تنظیم و نصب سرورها و تجهیزات مجازی با استفاده از الگو و کپی برداری
- ریکاوری یا بازیابی‌کردن راحت‌تر تجهیزات مجازی

با وجود این مزایا چالش‌هایی نیز در این حوزه وجود دارد. مجازی‌سازی به‌صورت بالقوه مورد توجه تهدیدات و بهره‌برداری‌ها در حوزه امنیت سایبری نیز می‌باشد و می‌بایستی تهدیدات و آسیب‌پذیری‌های آن مدیریت شود. برای مجازی‌سازی تنظیمات و پیکربندی‌های مختلفی در زمینه رعایت نکات امنیتی وجود دارد که ادمین‌های سیستم می‌بایستی در کنار راه‌اندازی لایه‌های مختلف آن، به تنظیمات امنیتی و پیکربندی امن آن نیز توجه داشته باشند. تکنولوژی مجازی‌سازی به بسترهای شبکه و ذخیره‌سازی نیز مرتبط است و نیازمند دقت در نقشه‌ها و تکنیک‌های مورد استفاده در کنترل دسترسی‌ها، مجوزهای کاربران و کنترل‌های اساسی امنیتی است.
علاوه‌بر این، بسیاری از سازمان‌ها مجازی‌سازی خود را با دیگر زیرساخت‌ها مانند ابرهای خصوصی با استفاده از نرم‌افزارهای تعریف‌شده و لایه‌های قابل برنامه‌ریزی پشته به منظور کنترل مراکز داده بزرگ و پیچیده، همگرا می‌کنند. زیرساخت‌های امنیتی، سیاست‌ها و فرایندها می‌بایستی با این زیرساخت‌های همگرا شده، منطبق باشند و تغییرات زیادی باید توسط تیم‌های امنیتی برای اطمینان از محافظت از منابع و دارایی‌ها در سازمان صورت گیرد.

مشخصات دوره

ناشر: SANS
مدرس: TechBinz Academy
سطح: پیشرفته
مدت زمان: ۴۰ ساعت
تعداد دروس: ٤ فصل، ٤٥ درس
زبان: انگلیسی

آموزش‌های عملی

- قفل و از کار افتادن ESXi
- حملات vMotion بر روی محرمانگی داده‌ها
- Netflow بر روی زیرساخت‌های مجازی

سرفصل دوره

1: Core Concepts of Virtualization Security
2: Virtualization and Software-Defined Security Architecture and Design
3: Virtualization Threats, Vulnerabilities, and Attacks
4: Defending Virtualization and Software-Defined Technologies

لینک

آنچه خواهید آموخت

- معنا و مفهوم اصلی امنیت مجازی‌سازی ودسته‌بندی‌های مختلف برای مجازی‌سازی
- معماری مجازی‌سازی و طراحی و امنیت تعریف شده توسط نرم افزار
- تهدیدات، آسیب پذیری‌ها و حملات احتمالی مجازی‌سازی
- دفاع از مجازی‌سازی و فناوری‌های تعریف‌شده توسط نرم افزار

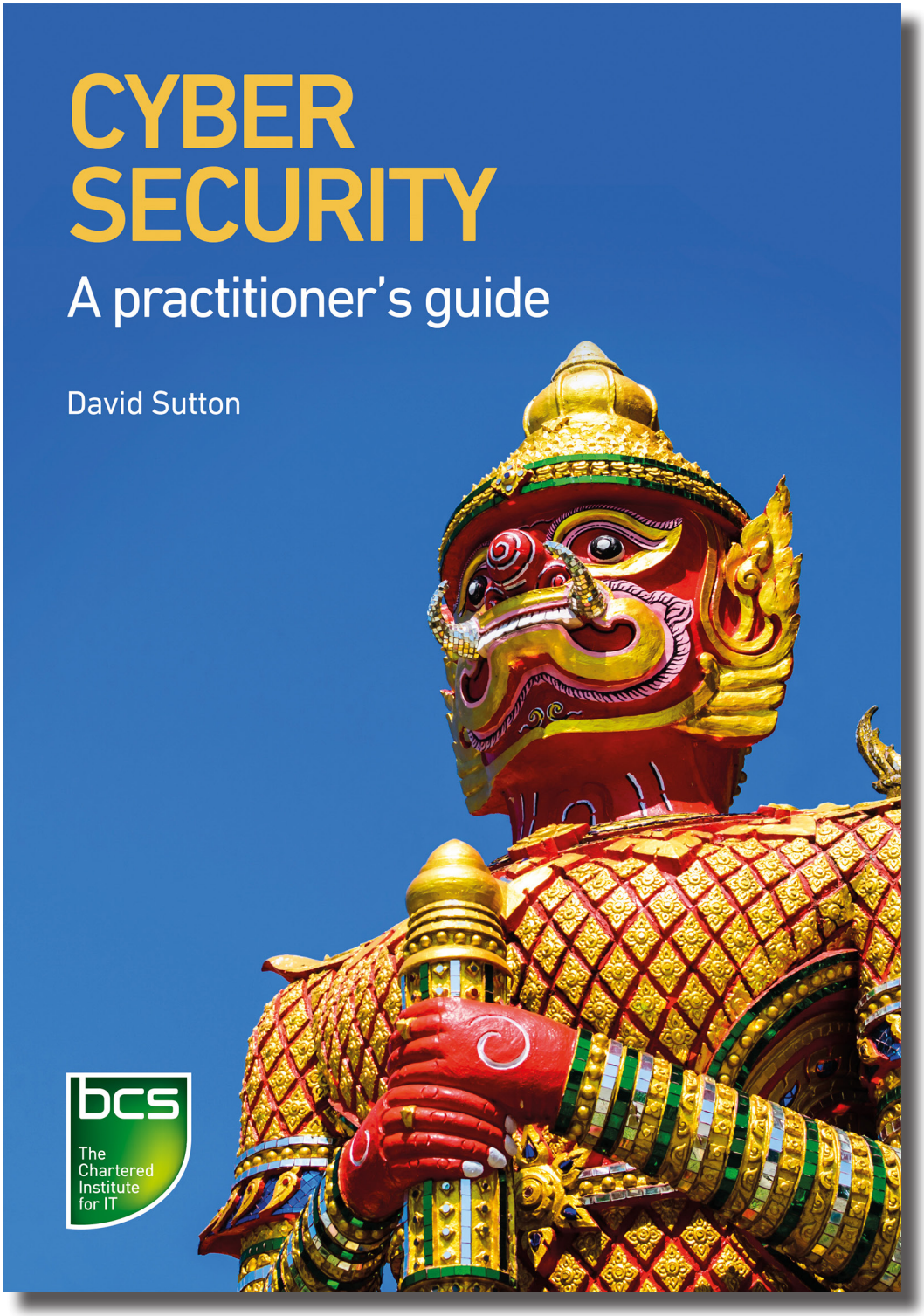
مخاطبان دوره

- پرسنل امنیتی که وظیفه ایمن‌سازی، مجازی‌سازی و زیرساخت‌ها را بر عهده دارند.
- مدیران شبکه و سیستم‌ها که نیاز به درک معماری، ایمن‌سازی و سعی در حفظ فناوری‌های مجازی دارند.
- حسابرسان و مشاوران فنی که نیاز به درک عمیق‌تری از مجازی‌سازی VMware از نظر امنیت انطباق دارند.

معرفی کتاب

نازیلا خسروی

معرفی کتاب



مشخصات

نام کتاب	Cyber Security: A practitioner's guide
نویسنده	David Sutton
زبان	English
تعداد صفحات	222
ناشر و سال انتشار	Wiley; 1st edition (August 2017 ,7)

معرفی

تقریبا هر روز اخبار مبنی بر به خطر افتادن اطلاعات کاربران و یا کشف آسیب‌پذیری‌های جدید، منتشر می‌شود. این اتفاقات می‌تواند منجر به در معرض خطر افتادن اطلاعات شخصی و دسترسی افراد سودجو به آن گردد. امروزه امنیت سایبری بیش از هر زمان دیگری نه تنها در محل کار بلکه در خانه‌ها نیز اهمیت پیدا کرده و امری ضروری تلقی می‌شود. در این کتاب انواع تهدیدات مختلف سایبری و اقدامات لازم برای کاهش مخاطرات و ایمن نگه‌داشتن داده‌ها توضیح داده شده است.
کتاب توسط یک متخصص و نویسنده مجرب امنیت اطلاعات، نوشته شده است و برای افرادی که مایل به درک بهتر خطرات امنیتی و اطمینان از امنیت داده‌های خود هستند، بسیار با ارزش می‌باشد اما برای کسانی که شغل آن‌ها با حفاظت از داده‌ها و امنیت اطلاعات ارتباط دارد و ممکن است در معرض تهدیدات جدی سایبری قرار گیرند، لازم و ضروری است.

نویسنده

سابقه دیوید ساتون در زمینه فناوری اطلاعات چیزی نزدیک به ۵۰ سال می‌باشد و فعالیت او در حوزه‌های شبکه‌های صدا و داده، امنیت اطلاعات و حفاظت از زیرساخت‌های حیاتی اطلاعات بوده است. وی سخنرانی‌هایی در زمینه مدیریت ریسک اطلاعات و تداوم کسب‌وکار در دانشگاه رویال هالووی لندن برگزار کرده و مدرک کارشناسی ارشد در رشته امنیت اطلاعات را نیز از آنجا اخذ کرده است.

لینک

فهرست مطالب

PART I: CYBER SECURITY PROBLEMS
1. INTRODUCTION
2. THE BIG ISSUES
3. CYBER TARGETS
4. CYBER VULNERABILITIES AND IMPACTS
5. CYBER THREATS

PART II: IMPROVING CYBER SECURITY
6. RISK MANAGEMENT OVERVIEW
7. BUSINESS CONTINUITY AND DISASTER RECOVERY
8. BASIC CYBER SECURITY STEPS
9. ORGANISATIONAL SECURITY STEPS
10. AWARENESS AND TRAINING
11. INFORMATION SHARING

PART III: APPENDICES
APPENDIX A – STANDARDS
APPENDIX B – GOOD PRACTICE GUIDELINES
APPENDIX C – CYBER SECURITY LAW
APPENDIX D – CYBER SECURITY TRAINING
APPENDIX E – LINKS TO OTHER USEFUL ORGANISATIONS

مقاله تحقیقاتی

ژینو سفاحی

کاربرد هوش مصنوعی در امنیت سایبری

هوش مصنوعی در امنیت سایبری

تکنولوژی‌های حال حاضر، امنیت سایبری هر سازمانی را به خطر می‌اندازند، هرچند که با پیشرفت استراتژی‌های دفاعی، متخصصان امنیتی در مقاطعی در حفظ امنیت سازمان‌ها ممکن است شکست بخورند اما ترکیب توانایی‌های هوش مصنوعی (AI) در امنیت سایبری با مهارت متخصصان امنیتی از مرحله بررسی آسیب‌پذیری تا دفاع در برابر حملات بسیار موثر است. استفاده هوش مصنوعی در حوزه امنیت سایبری تحولی جدید و پرکاربرد در این حوزه محسوب می‌شود.
در ادامه انواع حملاتی که در حال حاضر شاهد آن هستیم بیان خواهند شد.

- بدافزارهای پیشرفته
- تهدیدهای داخلی
- تقلب در معاملات
- حملات رمزگذاری شده
- استخراج داده‌ها
- بهره‌برداری از آسیب‌پذیری‌های برنامه‌ها در زمان اجرا
- تملک و مالکیت حساب‌ها

فهرست اهداف اولیه مهاجمان یا تهدیدهای سایبری شامل شرکت‌ها، دولت‌ها، ارتش یا سایر دارایی‌های ساختاری یا شهروندان یک ملت است. همان‌طور که قبلا ذکر شد، حجم و حملات سایبری پیشرفته افزایش یافته است. به‌همین دلیل به ترکیب هوش مصنوعی با روش‌های موجود در امنیت سایبری برای تجزیه‌وتحلیل مناسب و کاهش وقوع حملات سایبری نیازمندیم.

راه‌حل‌های تجزیه‌وتحلیل امنیت سایبری برای شرکت‌ها

تعریف پیشرفته کاربرد هوش مصنوعی در امنیت سایبری برای سازمان‌ها و شرکت‌ها در زیرآمده است:
۱. آنالیز Perspective: تعیین اقدامات مورد نیاز برای تجزیه‌وتحلیل یا پاسخ
۲. آنالیز Diagnostic: ارزیابی علت اصلی تجزیه‌وتحلیل و نحوه عملکرد حوادث و حملات
۳. آنالیز Predictive: تعیین کاربران و دارایی‌های پر ریسک در آینده و احتمال تهدیدات آینده
٤. آنالیز Detective: شناسایی تهدیدات پنهان، ناشناخته، تهدیدات دور زدن امنیت، بدافزار پیشرفته و حرکت جانبی
۵. آنالیز Descriptive: به‌دست آوردن وضعیت و عملکرد فعلی معیارها و روندها

چرایی نیازمندی به سیستم‌های مبتنی بر هوش مصنوعی در حوزه امنیت سایبری

- شکار موثر تهدیدات
- تجزیه‌وتحلیل کامل حوادث و بررسی تهدیدات
- پیش‌بینی تهدیدات
- بازیابی سیستم‌های آسیب‌دیده، بررسی علل اصلی حملات و بهبود امنیت سیستم
- نظارت بر امنیت

قابلیت‌های اصلی سیستم امنیت سایبری مبتنی بر هوش مصنوعی چیست؟

امنیت سیستم

- امنیت شبکه
- امنیت بستر ابری
- امنیت اینترنت اشیاء
- بدافزار
- امنیت خودکار

امنیت داده‌ها

- تجزیه‌وتحلیل امنیت
- پیش‌بینی تهدید
- یادگیری ماشین در محیط سایبری
- امنیت شبکه‌های اجتماعی
- تشخیص حملات داخلی

کاربرد امنیت

- تکنولوژی مالی و بلاکچین
- ریسک و تصمیم‌گیری
- امنیت داده‌ها
- تشخیص هرزنامه‌ها

قدرت هوش مصنوعی در رویکرد مدیریت ریسک برای امنیت سایبری

- مجموعه درست داده‌ها
- نمایش برنامه یادگیری
- فرایند اصلاح و انجام تغییرات در یادگیری ماشین بنا به درخواست متقاضی
- تجزیه‌وتحلیل تهدیدات سایبری
- مدل‌سازی از مشکلات امنیتی

چگونه یادگیری ماشین و یادگیری عمیق در امنیت سایبری کمک می‌کنند؟

تکنولوژی‌های مرتبط با AI به‌صورت هوشمند بوده و از توانایی‌های خود برای بهبود امنیت شبکه در طول زمان می‌توان مورد استفاده قرار گیرند. از یادگیری ماشین و یادگیری عمیق برای یادگیری رفتار در شبکه که الگوها را در شبکه شناسایی و تکنیک‌های زیر را بر روی آن پیاده‌سازی می‌کند.

تکنیک: طبقه‌بندی

توصیف: برای تعیین اینکه آیا رویداد امنیتی قابل اعتماد است یا نه و متعلق به یک گروه یا دسته است یا نه.

الگوریتم: الگوریتم‌های احتمالی مثل شبکه بیزین و الگوریتم‌های مبتنی بر نمونه مثل KNN,SVM,SOM و درخت تصمیم و همچنین شبکه‌های عصبی.

تکنیک: تطبیق الگو

توصیف: تشخیص الگو و شاخص‌های مخرب در مجموعه داده‌های بزرگ.

الگوریتم: تابع آنتروپی KMP بویر مور.

تکنیک: رگرسیون

توصیف: تعیین روند رویدادهای امنیتی پیش‌بینی رفتار ماشین‌ها و کاربران.

الگوریتم: رگرسیون خطی، رگرسیون لاجستیک و رگرسیون چند متغیره.

تکنیک: یادگیری عمیق

توصیف: ایجاد شیوه‌نامه خودکار بر پایه اقدامات گذشته برای شکار حملات

الگوریتم: شبکه‌های عمیق Boltzmann

تکنیک: رابطه ضابطه‌ها

توصیف: هشدار بعد از تشخیص حملات و مهاجمان مشابه

الگوریتم: قانون وابستگی (Apriori Eclat)

تکنیک: خوشه‌بندی

توصیف: تعیین موارد پرت و ناهنجاری. ایجاد گروه‌های همتا از ماشین‌ها و کاربران.

الگوریتم: خوشه‌بندی K-means، خوشه‌بندی سلسله مراتبی

تکنیک: هوش مصنوعی با استفاده از نوروساینس

توصیف: تقویت هوش انسانی، یادگیری با هر تعامل برای تشخیص فعال، تجزیه‌وتحلیل و ارائه بینش‌های کاربردی درمورد تهدیدات.

الگوریتم: امنیت شناختی.

الگوریتم‌های ذکر شده در بالا دارای محدودیت‌هایی هستند، درنتیجه نمی‌توانند به خوبی در تجزیه‌وتحلیل‌های امنیتی عمل کنند. بنابراین، برخی از تکنیک‌های اولیه برای انجام این تحلیل‌های امنیتی باید پیاده‌سازی شوند.

شفافیت

زیربنای هر تکنیک و دلایل انتخاب یک تکنولوژی خاص نسبت به سایر آن‌ها آمار، یادگیری ماشین و ریاضیات است که به محض انتخاب از بین می‌روند یا فراموش می‌شوند. با سیستم‌های مبتنی بر قوانین، تعداد زیادی از قوانین، بار شناختی ایجاد می‌کنند که باعث می‌شود از بلوک‌ها درک جامعی داشته باشند و در نهایت، در سیستم این خروجی‌ها به سختی به‌دست می‌آیند و تنها به‌صورت تدریجی در طول زمان بهبود می‌یابند.

دانش تخصصی

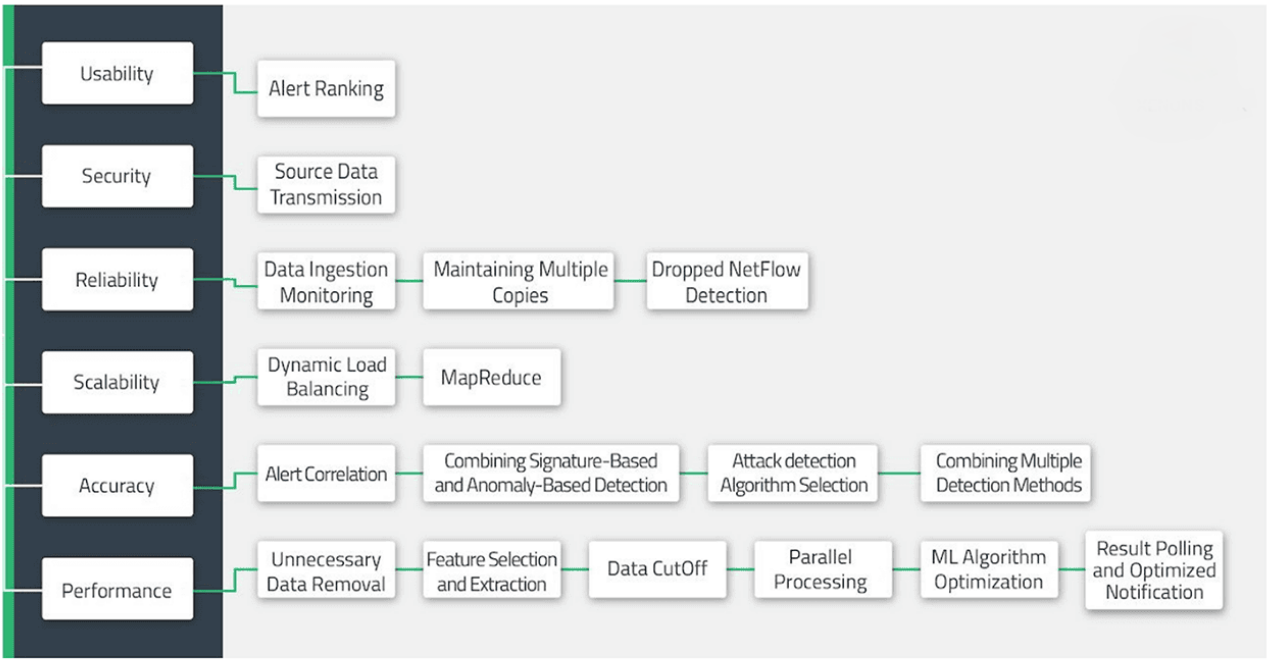
تجزیه‌وتحلیل در امنیت، یک فعالیت پیچیده است که به دانش تخصصی در مورد سیستم‌های مدیریت ریسک، فایل‌های لاگ، بسترهای شبکه و تکنیک‌های تجزیه‌وتحلیل نیاز دارد.

چگونه تجزیه‌وتحلیل با هوش مصنوعی از امنیت سایبری پشتیبانی می‌کند؟

هر نوع تجزیه‌وتحلیل با جمع‌آوری داده‌ها شروع می‌شود. در جدول زیر منابع مختلف داده‌ها از جایی که داده‌ها جمع‌آوری و سپس تجزیه‌وتحلیل می‌شوند، آمده است.

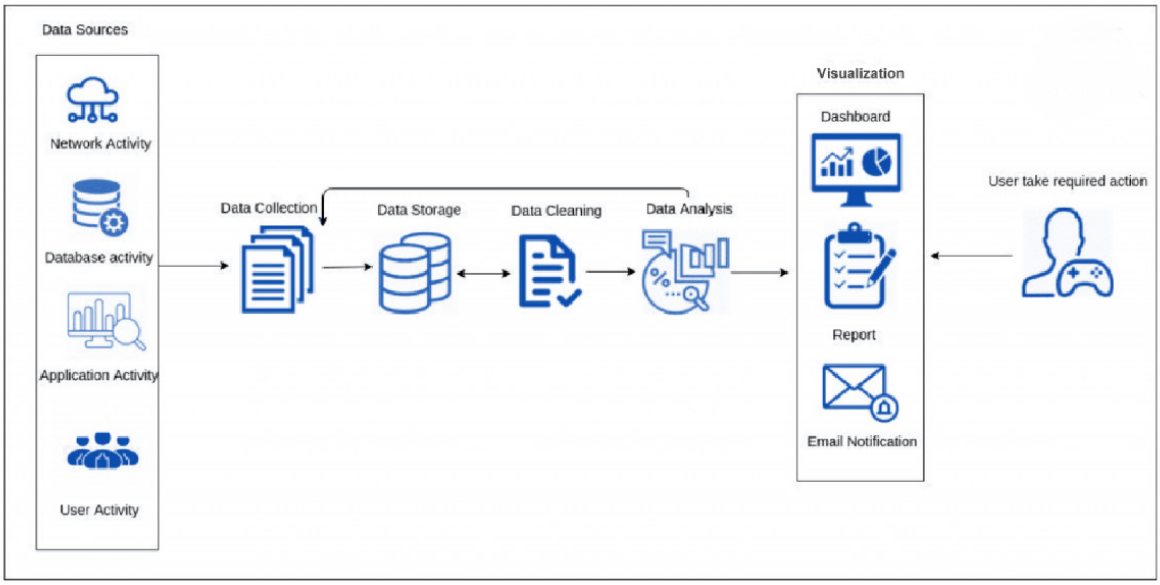
نوع داده: داده‌های کاربر **دسته بندی:** محصولات UBA **توصیف:** جمع‌آوری و تجزیه‌وتحلیل دسترسی و فعالیت کاربر از VPN، Proxy، AD و برنامه‌ها	**نوع داده:** داده‌های برنامه **دسته بندی:** محصولات RASP **توصیف:** جمع‌آوری و تجزیه وتحلیل درخواست‌ها، تبادل داده‌ها، دستورات همراه داده‌های WAF برای نصب عوامل روی برنامه
نوع داده: داده‌های نقطه پایانی **دسته بندی:** محصولات EDR **توصیف:** تجزیه‌وتحلیل نقاط پایانی داخلی مانند فایل‌ها، پردازش‌ها، حافظه، رجیستری، اتصالات و بسیاری موارد دیگر با نصب Agent ها.	**نوع داده:** داده‌های شبکه **دسته بندی:** محصولات شبکه کشف (جرم کاوی) جرم‌ها و تجزیه‌وتحلیل **توصیف:** جمع‌آوری و تجزیه‌وتحلیل packet ها، net flow ها، DNS، داده‌ها IPS با نصب دستگاه‌هایی در شبکه

جنبه‌های عملکرد راه‌حل‌ها در امنیت سایبری



حذف داده‌های غیر ضروری

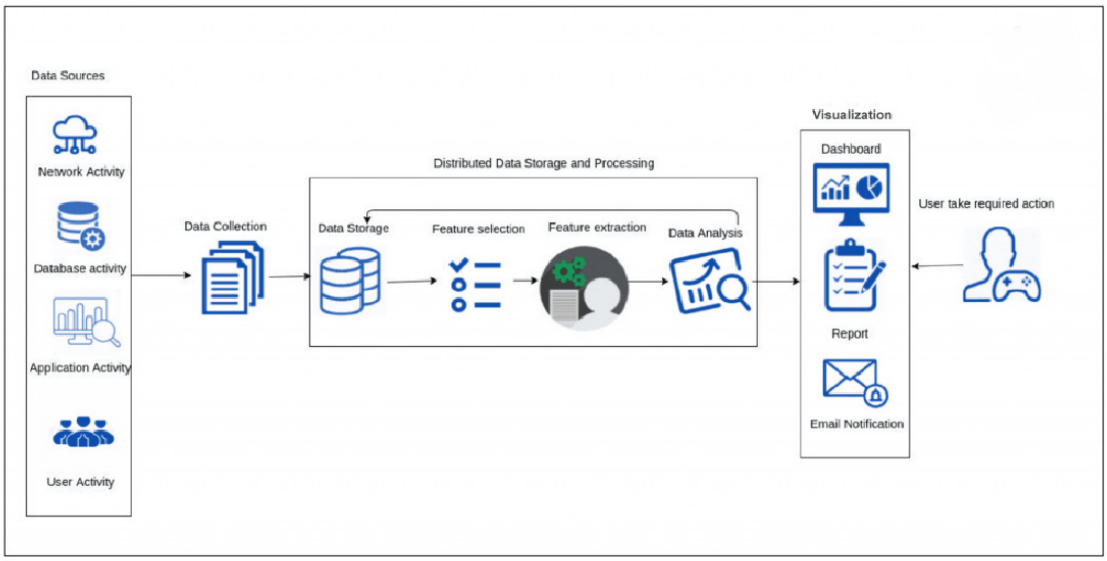
زیرمجموعه‌ای از داده‌های مربوط به رویدادها که در فرایند تشخیص مفید نیستند، به‌عنوان داده‌های اضافی در نظر گرفته و برای افزایش عملکرد حذف می‌شوند.



همان‌طور که در شکل نشان داده شده است، پس از حذف داده‌های غیر ضروری، داده‌ها برای شناسایی حملات سایبری به بخش تجزیه‌وتحلیل ارسال می‌شوند. در نهایت، نتایج با استفاده از ماژول تجسم یا Visualization Module نشان داده می‌شوند.

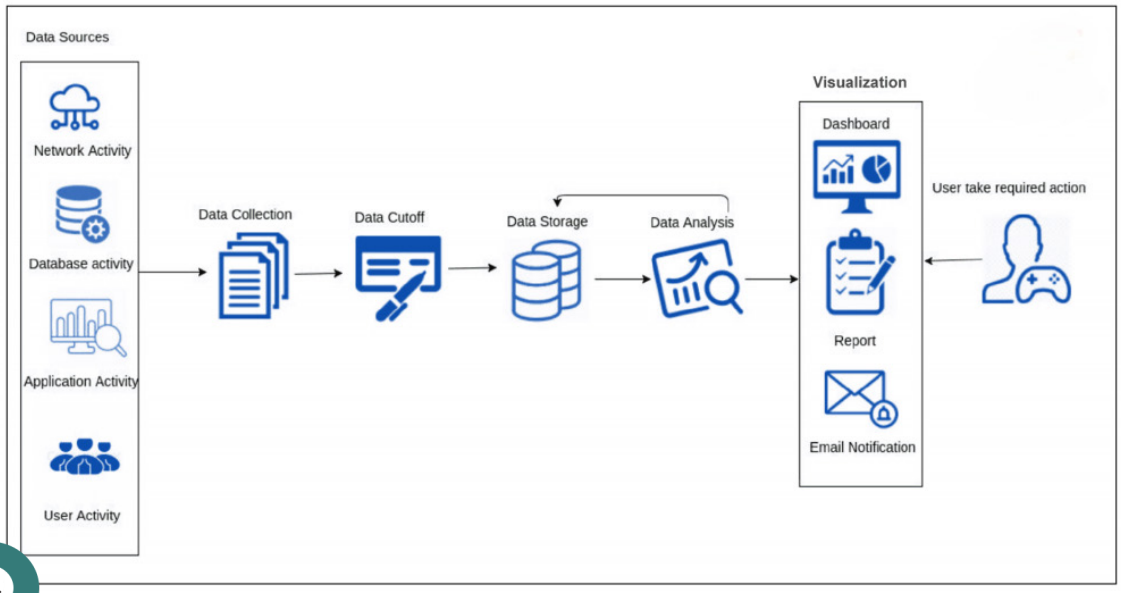
استخراج و انتخاب ویژگی

فرآیندهای استخراج و انتخاب ویژگی به پردازش موازی داده‌ها این قابلیت را می‌دهد تا سرعت فرایند انتخاب و استخراج را افزایش دهند. سپس مجموعه داده ویژگی استخراج شده به ماژول تجزیه‌وتحلیل داده‌ها ارسال می‌شود که عملیات تجزیه‌وتحلیل متفاوتی را در کاهش اندازه مجموعه داده برای شناسایی حملات سایبری انجام می‌دهد. در موقعیت حمله، هشدارهایی که توسط مدیر شبکه یا کارشناس امنیت ایجاد می‌شوند با استفاده از مولفه تجسمی قابل مشاهده است. هنگامی که این هشدارهای حمله مورد توجه قرار گیرد، یک شرکت یا کاربر می‌تواند اقدامات مهمی را برای کاهش یا جلوگیری از اثرات حمله انجام دهد.



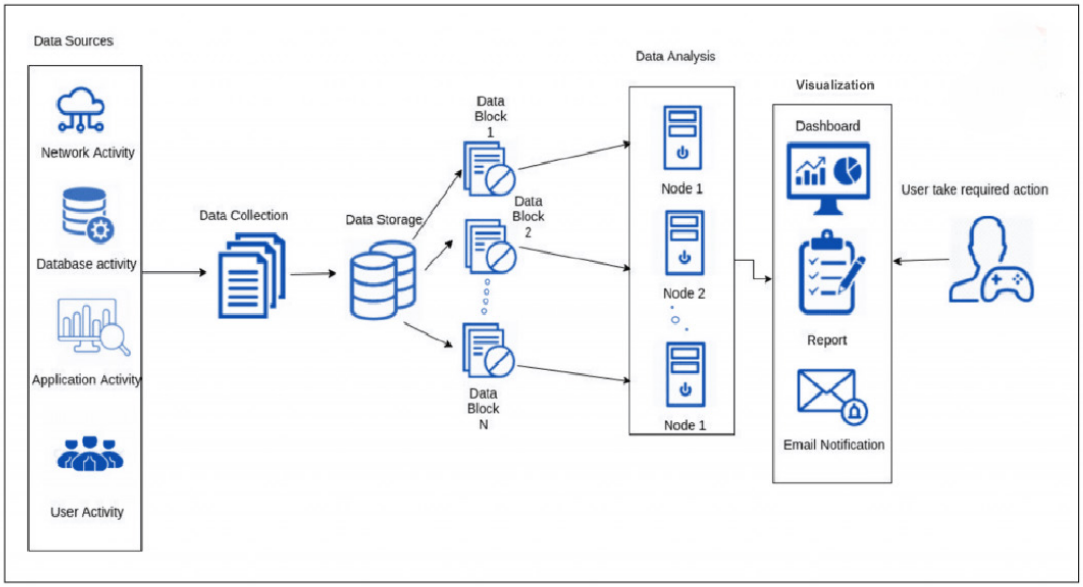
متوقف کردن داده‌ها!

مؤلفه قطع داده یا Data Cutoff با نادیده‌گرفتن رویدادهای امنیتی که پس از اتصال به یک شبکه یا پردازش حاصل می‌شود و برای آن مرزی تعریف شده است، قطع داده را اعمال می‌کند. هر رویداد امنیتی که بالاتر از مرز تعریف شده باشد، به فرآیند تشخیص حمله کمک نمی‌کند، بنابراین تجزیه‌وتحلیل مستلزم این نوع رویدادهای امنیتی است که همانند یک بار اضافی بر روی منابع پردازش داده هستند و هیچ دستاورد قابل تشخیصی ندارند. ماهیت ذخیره‌سازی داده‌ها ممکن است داده‌های رویداد امنیتی باقی مانده را پس از قطع، ذخیره کنند. ماژول تجزیه‌وتحلیل داده برای تشخیص حملات سایبری داده‌های ذخیره شده را می‌خواند. در پایان، نتایج تجزیه‌وتحلیل از طریق یک نهاد یا ماهیت نمایان، برای کاربر قابل مشاهده است که به کاربر اجازه می‌دهد بعد از رسیدن هر هشدار مهم، اقدامی ضروری انجام دهد.



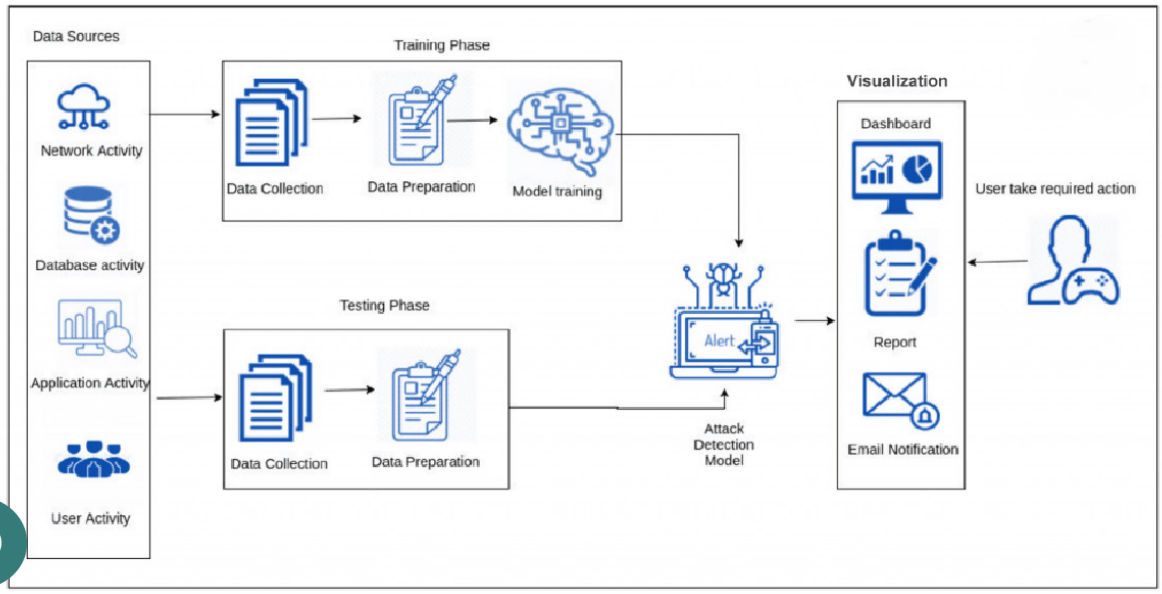
پردازش موازی

جمع‌آورنده داده‌ها یا Data Collectorها داده‌های رویداد امنیتی را از منابع مختلف بسته به انواع تجزیه‌وتحلیل‌های امنیتی و الزامات امنیتی یک شرکت خاص دریافت می‌کنند. جمع‌آورنده داده، داده‌های گرفته شده را به یک نهاد ذخیره‌سازی داده تحویل می‌دهد. روش‌های زیادی برای ذخیره‌سازی داده‌ها وجود دارد مانند Hadoop Distributed File System یا HDFS و Relational Database Management System یا RDBMS و HBase. برای اعمال پردازش موازی، داده‌های ذخیره شده باید در بلوک‌هایی با اندازه ثابت (۱۲۸ مگابایت یا ٦٤ مگابایت) توزیع شوند. داده‌ها پس از قسمت‌بندی کردن، در مولفه تجزیه‌وتحلیل داده‌ها از طریق گره‌های مختلف که به طور موازی بر اساس دستورالعمل‌های یک چارچوب توزیع شده مانند Spark یا Hadoop کار می‌کنند نتیجه‌ای که توسط تجزیه‌وتحلیل دریافت شده، از طریق مولفه تجسمی با کاربر به اشتراک گذاشته می‌شود.



الگوریتم‌های یادگیری ماشین و یادگیری عمیق برای فعال‌سازی امنیت سایبری با بهره از هوش مصنوعی

ماهیت یا نهاد Data Collector، داده‌های رویداد امنیتی را برای فرایند آموزش یک سیستم تجزیه‌وتحلیل امنیتی ضبط می‌کند. داده‌های آموزشی را می‌توان از منابع درون شرکتی که قرار است عملیات در آن اجرا شود، دریافت کرد. پس از جمع‌آوری داده‌ها برای آموزش، مؤلفه آماده‌سازی داده‌ها (Data Preparation)، فرآیند آماده‌سازی داده‌ها را برای آموزش مدل با اعمال فیلترهای مختلف آغاز می‌کند. بعد از آن، الگوریتم یادگیری ماشین انتخاب شده بر روی داده‌های آموزشی آماده شده برای آموزش مدل تشخیص حمله، پیاده‌سازی می‌شود. زمانی که الگوریتم برای آموزش یک مدل در نظر می‌گیرد (زمان آموزش) برای هر الگوریتم متفاوت است.



پس از آموزش مدل، برای بررسی اینکه آیا مدل می‌تواند حملات سایبری را تشخیص دهد، آزمایش می‌شود. برای آزمایش مدل، داده‌ها از شرکت جمع‌آوری می‌شوند. داده‌هایی که برای آزمایش هستند از طریق ماژول آماده‌سازی داده‌ها فیلتر شده و به مدل تشخیص حمله وارد می‌شوند که برای تجزیه‌وتحلیل داده‌ها برای تشخیص حملات بر اساس قوانینی که در مرحله آموزش آموخته می‌شوند، استفاده می‌شود. زمان گرفته شده در مدل تشخیص حمله برای نتیجه‌گیری اینکه آیا جریان خاصی از داده‌ها که مربوط به حمله است (زمان تصمیم‌گیری) بستگی به الگوریتم تکمیل شده دارد یا خیر. نتیجه دریافت شده توسط تجزیه‌وتحلیل داده‌ها ازطریق مولفه تجسمی برای کاربر نمایان می‌شود.

- **درجه دقت در مدل‌های امنیتی**

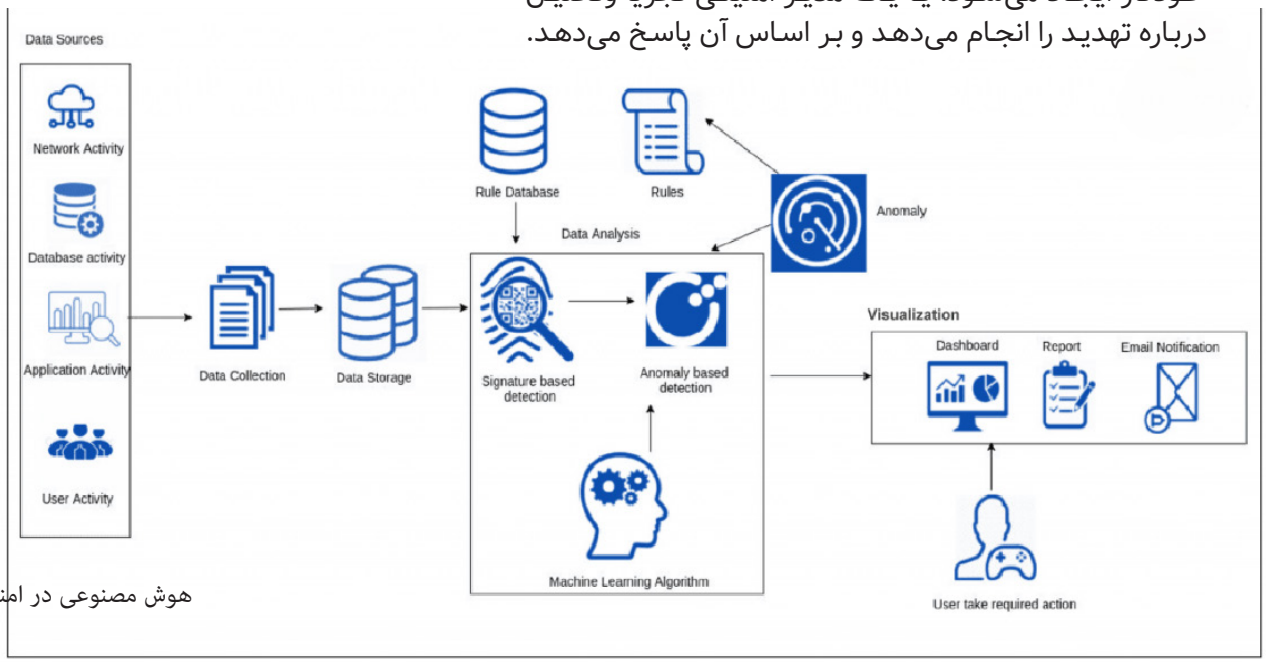
این بخش شامل ویژگی کیفیت دقت است.

هشدار همبستگی(Correlation)

ماژول مجموعه داده یا Data Collection، داده‌های رویداد امنیتی را از منابع مختلف می‌گیرد، سپس داده‌های جمع‌آوری‌شده در محل ذخیره‌سازی داده، ذخیره می‌شوند و برای اعمال تکنیک‌های پیش پردازش بر روی داده‌های خام در ماژول Data Per-Processor کپی می‌شود. داده‌هایی که از قبل پردازش شده‌اند وارد ماژول آنالیز هشدار می‌شوند که داده‌ها را برای شناسایی حملات تجزیه‌وتحلیل کنند. در اینجا لازم است اشاره شود که ماژول آنالیز هشدار داده‌ها را به شیوه‌ای رها شده (بدون مشاهده هیچ گونه اطلاعات زمینه‌ای) مبتنی بر ناهنجاری یا مبتنی بر سوءاستفاده یا هر دو، مورد تجزیه‌وتحلیل قرار می‌دهد. هشدارهای تولید شده به ماژول تأیید هشدار ارسال می‌شوند که از تکنیک‌های مختلف برای تشخیص اشتباه بودن هشدار استفاده می‌کند. هشدارهای شناسایی شده به‌عنوان تشخیص‌های اشتباه در این سطح نادیده گرفته می‌شوند. سپس هشدارهای واضح و مرتب‌شده برای تجزیه‌وتحلیل بیشتر به ماژول همبستگی هشدار ارسال می‌شود. پس از آن، هشدارها با استفاده از تکنیک‌ها و الگوریتم‌های مختلف مانند همبستگی مبتنی بر قاعده، همبستگی مبتنی بر سناریو، همبستگی زمانی و همبستگی آماری، همبستگی (به‌طور منطقی مرتبط) می‌شوند. ماژول همبستگی هشدار با ذخیره‌سازی داده‌ها برای گرفتن اطلاعات متنی مورد نیاز در مورد هشدارها هماهنگ می‌شود. نتایج همبستگی از طریق ماژول تجسم آزاد می‌شود. در نهایت، یا یک پاسخ خودکار ایجاد می‌شود، یا یک مدیر امنیتی تجزیه‌وتحلیل درباره تهدید را انجام می‌دهد و بر اساس آن پاسخ می‌دهد.

تشخیص ناهنجاری مبتنی بر امضاء

مولفه جمع‌آوری داده‌ها، داده‌های مربوط به امنیت را از منابع مختلف جمع‌آوری می‌کند. بعد از آن، داده‌های جمع‌آوری شده توسط ماژول ذخیره‌سازی داده‌ها، ذخیره می‌شود. سپس داده‌ها به مؤلفه تشخیص مبتنی بر امضا وارد می‌شوند که تجزیه‌وتحلیل داده‌ها را برای شناسایی الگوی حمله انجام می‌دهد. در چنین تحلیلی، نقطه قوت این مؤلفه این است که قوانین از پیش طراحی شده را از پایگاه داده کشورها فراهم می‌کند که الگوی حمله را شناسایی می‌کنند. اگر مطابقت تشخیص داده شود، یک هشدار مستقیماً از طریق یک ماژول تجسم ایجاد می‌شود.

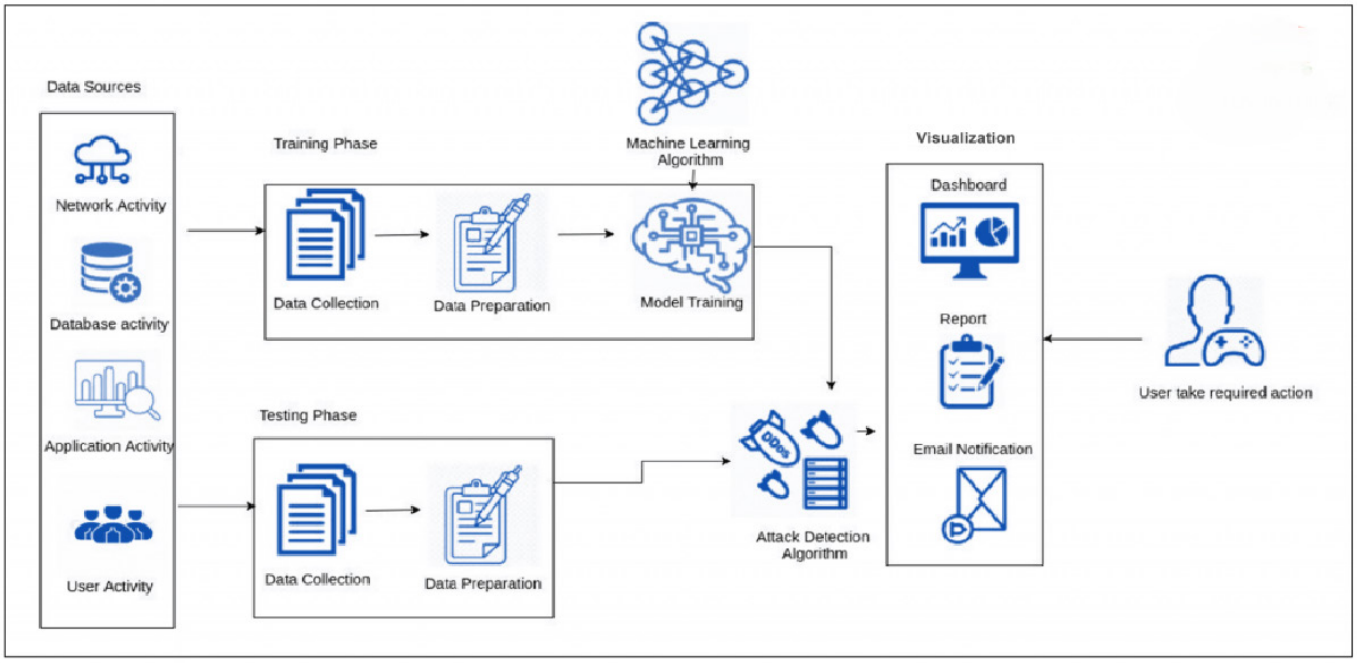


اگر مؤلفه تشخیص مبتنی بر امضا هیچ الگوی حمله‌ای را در داده‌ها شناسایی نکند، داده‌ها برای شناسایی حملات ناشناخته‌ای که توسط مؤلفه تشخیص مبتنی بر امضا قابل شناسایی نیستند به مؤلفه تشخیص مبتنی بر ناهنجاری منتقل می‌شوند. ناهنجاری به‌عنوان رفتار یا الگوی غیرعادی داده‌ها تعریف می‌شود که این به خصوص نشان دهنده وجود خطا یا نقصی در سیستم است.

ماژول تشخیص مبتنی بر ناهنجاری، داده‌ها را با استفاده از الگوریتم‌های یادگیری ماشین برای شناسایی انحرافات از رفتار عادی تجزیه‌وتحلیل می‌کند. هنگامی که یک ناهنجاری (انحراف) شناسایی می‌شود، یک هشدار از طریق ماژول تجسم تولید می‌شود. در همان زمان، ناهنجاری در قالب یک الگوی حمله یا قانون تعریف شده و به پایگاه داده قوانین ارسال می‌شود. با استفاده از این روش، پایگاه داده قوانین، به طور مداوم به‌روز می‌شود تا مؤلفه تشخیص مبتنی بر امضا بتواند انواع حملات را شناسایی کند.

الگوریتم تشخیص حمله

ماژول مجموعه داده، داده‌های رویداد امنیتی را برای آموزش سیستم تجریه وتحلیل امنیتی در شناسایی حملات سایبری دریافت می‌کند. پس از انجام فرآیند جمع‌آوری داده مربوط به داده‌های آموزشی، ماژول Data Preparation داده را با استفاده از فیلترها و تکنیک‌های مختلف استخراج ویژگی، برای آموزش مدل آماده می‌کند.



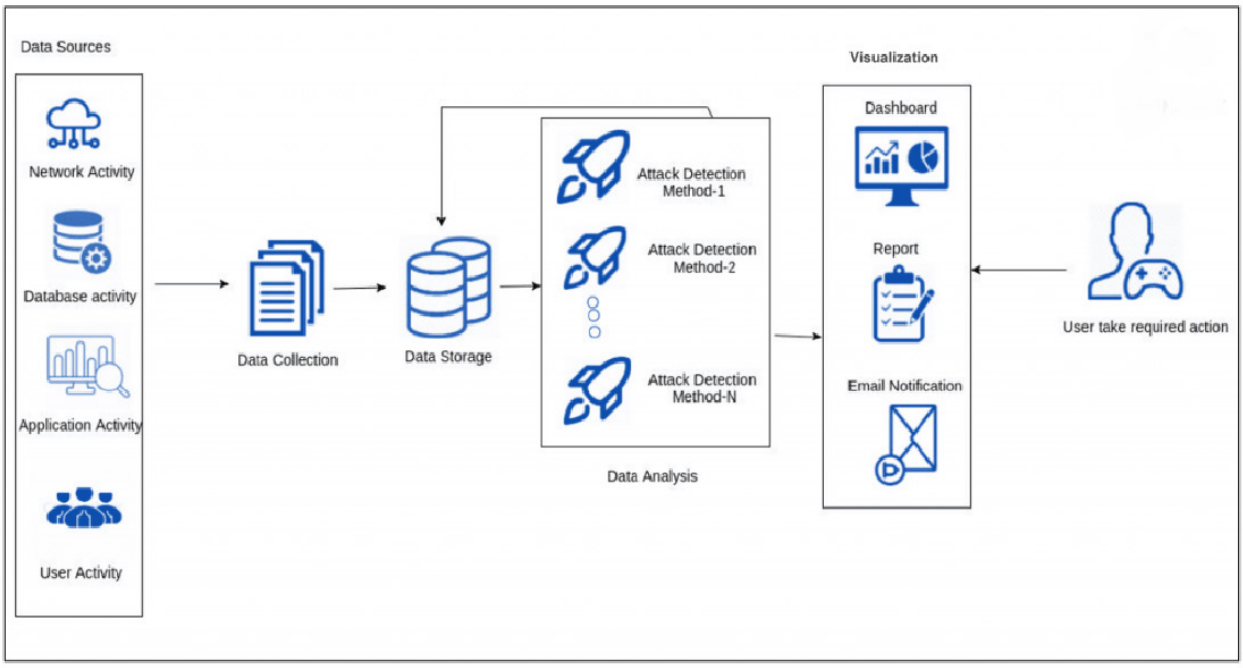
بعد از آن داده‌های آموزشی آماده شده، شروع به آموزش ماژول attack detection می‌کند. هنگامی که ماژول آماده شد، برای بررسی اینکه آیا مدل می‌تواند حملات سایبری را شناسایی کند، اعتبارسنجی می‌شود. برای اعتبارسنجی مدل، داده‌ها از یک شرکت را جمع‌آوری می‌کنند. training data برای ارسال به ماژول تشخیص حمله آماده می‌شوند و به مدل تشخیص حمله وارد می‌شوند که تجزیه‌وتحلیل را بر اساس قوانین آموخته‌شده در مرحله آموزش انجام می‌دهد. در اینجا، نمونه داده‌های آزمایشی به‌عنوان سالم یا مخرب طبقه‌بندی می‌شوند. نتایج تجزیه‌وتحلیل از طریق ماژول تجسم برای کاربر نمایش داده می‌شود. در موقعیت‌های مخرب یا حمله، کاربر می‌تواند اقدامات مورد نیاز فوری را انجام دهد که ممکن است شامل مسدودکردن چند پورت یا جداکردن اجزای آسیب‌دیده از شبکه، تا از آسیب بیشتر جلوگیری کند.

ترکیب چندین روش تشخیص

داده‌های رویداد امنیتی از منابع مختلف گرفته می‌شود. توجه به این نکته حائز اهمیت است، منابعی که از آنجا می‌توان داده‌های رویداد امنیتی را گرفت به آنچه در تصویر نشان داده شده است محدود نمی‌شود.

انتخاب منابع داده از سازمانی به سازمان دیگر متمایز است و به الزامات امنیتی دقیق آن‌ها بستگی دارد. پس از تکمیل فرآیند جمع‌آوری، داده‌های حاصل در مولفه ذخیره‌سازی داده، ذخیره می‌شود. سپس داده‌ها به مولفه تجزیه‌وتحلیل داده‌ها منتقل می‌شوند که در آن روش‌ها و تکنیک‌های مختلف تشخیص حمله در تجزیه‌وتحلیل داده‌ها پیاده‌سازی می‌شود. انتخاب‌ها و تعداد روش‌ها و تکنیک‌های تشخیص حمله به عواملی بستگی دارد.

این عوامل شامل توانایی پردازش یک سازمان، منابع داده، الزامات امنیتی و در نهایت تخصص امنیتی تیم‌های سازمان است. به‌عنوان‌مثال، یک سازمان بسیار حساس به امنیت،به‌عنوان مثال آژانس امنیت ملی، بودجه زیاد و همچنین ابزارهایی با قدرت محاسباتی بالایی دارد که ممکن است برای ایمن‌سازی داده‌ها و زیرساخت‌های خود در برابر حملات مربوط به تکنولوژی‌های سایبری چندین روش و تکنیک تشخیص حمله را ترکیب کند. روش‌ها و تکنیک‌های تشخیص حمله به‌صورت موازی بر کل مجموعه داده اعمال می‌شوند. ماژول تجسم بلافاصله در مورد هر گونه ناهنجاری برجسته به کاربران یا مدیرانی که انتظار می‌رود به هشدارهای امنیتی پاسخ دهند، اطلاع می‌دهد.

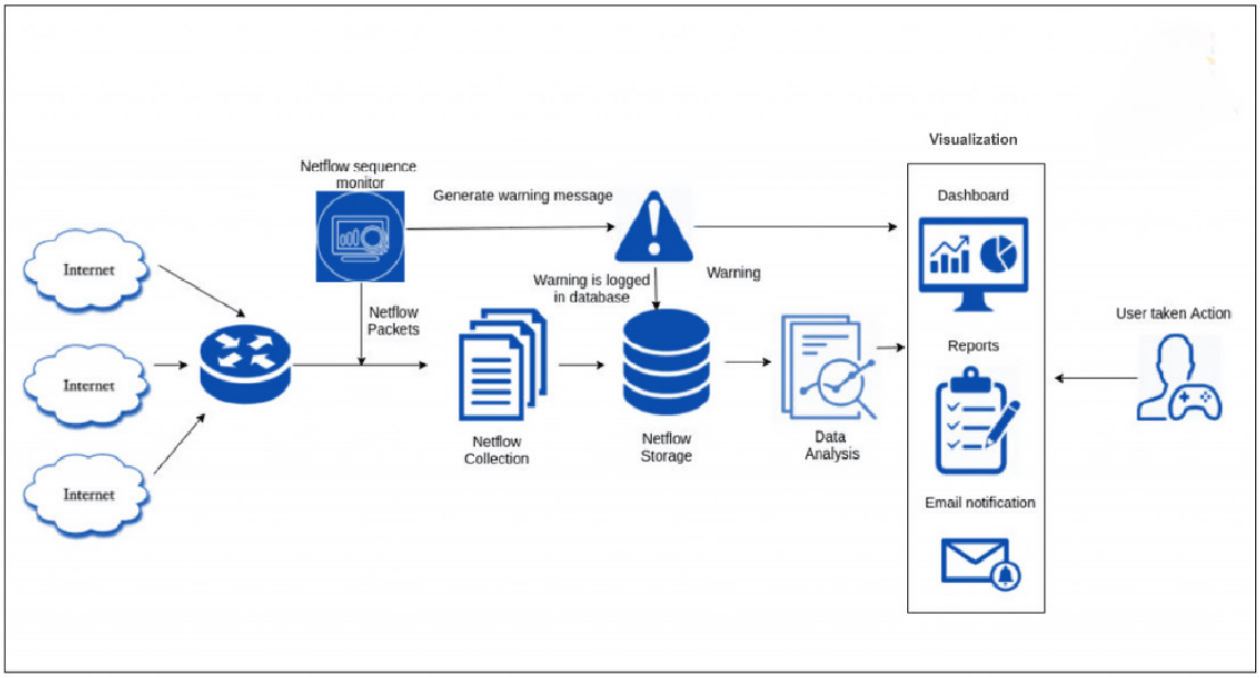


راهکارهای امنیت سایبری هوش مصنوعی برای مقیاس‌پذیری

این بخش به ویژگی کیفیت قابلیت اطمینان مربوط می‌شود.

تشخیص Netflow کاهش یافته

ترافیک شبکه از طریق روتر نشان داده شده در شکل زیر عبور می‌کند. یک گیرنده NetFlow به روتر متصل است که NetFlow را گرفته و در حافظه خود ذخیره می‌کند. در طول فرآیند جمع‌آوری NetFlow، ماژول نظارت زنجیره‌ای NetFlow در حال نظارت بر دنباله‌ای از اعداد است که بر اساس طراحی در NetFlow تعبیه شده‌اند.



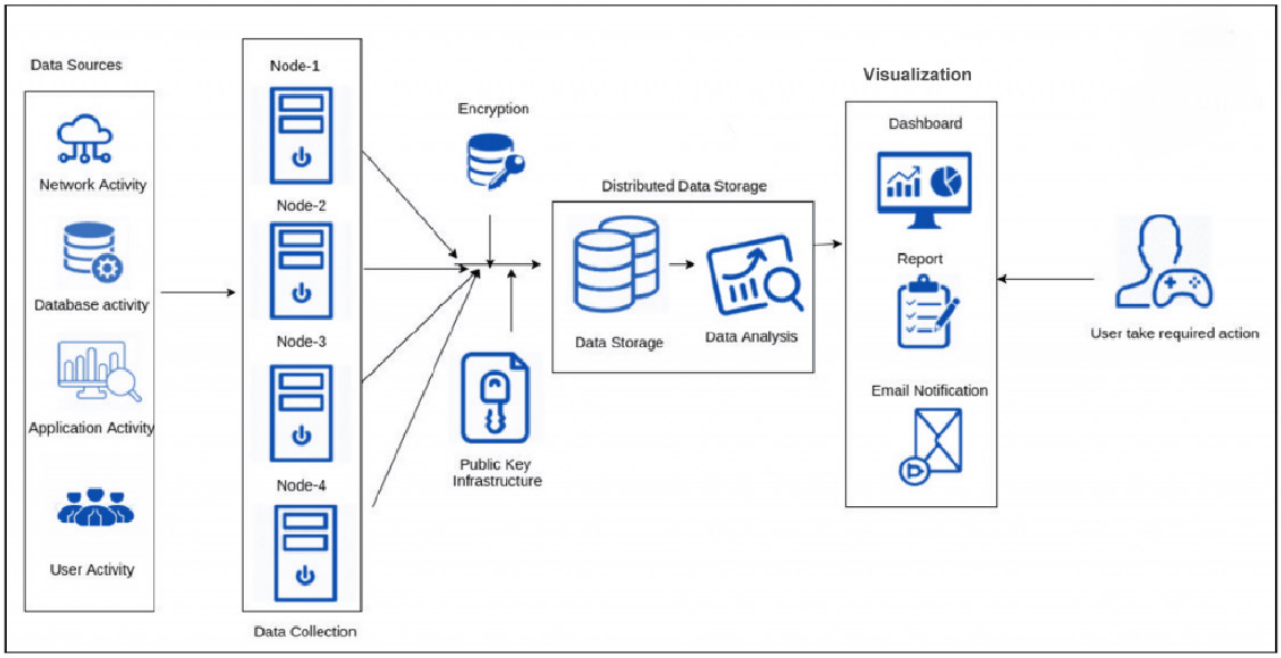
در شرایطی که دنباله‌ای از اعداد در هر مرحله نامرتب هستند، نظارت دنباله‌ای NetFlow یک پیام هشدار ارسال می‌کند که نشان‌دهنده Flow گم شده در NetFlow است. سپس پیام هشدار در کنار جریان دقیق در ماژول ذخیره‌سازی NetFlow ثبت می‌شود تا به این نکته اشاره شود که جریان NetFlow دارای برخی جریانات گم شده است که ممکن است برای شناسایی یک حمله بسیار مهم باشد. در همان زمان، یک اخطار از طریق ماژول تجسم برای یک مدیر امنیتی نمایش داده می‌شود. سپس یک مدیر امنیتی می‌تواند اقدامات فوری را برای حل این مشکل انجام دهد و ممکن است برخی از NetFlow ها حذف شوند.

توانایی رسیدگی به حجم زیادی از داده‌ها

فعالیت‌های زیادی در شبکه یک شرکت اتفاق می‌افتد و به‌طور متوسط ترافیک زیادی دارد. این بدان معناست که روزانه داده‌های زیادی بین مشتریان و شرکت منتقل می‌شود. این داده‌ها نیاز به محافظت در برابر افراد و نرم‌افزارهای مخرب دارند اما تیم امنیت سایبری یک شرکت بدون استفاده از ابزار و تکنولوژی‌های مرتبط نمی‌تواند تمام ترافیک را برای تهدیدات احتمالی بررسی کند.
هوش مصنوعی بهترین راه‌حلی است که به شما کمک می‌کند هرگونه تهدیدی که به‌عنوان فعالیت عادی پنهان شده است را شناسایی کنید. ماهیت خودکار هوش مصنوعی این قابلیت را به آن می‌دهد تا ترافیک زیاد داده‌ها برایش چالش نباشد. تکنولوژی‌هایی که از هوش مصنوعی استفاده می‌کنند، مانند یک residential-proxy، می‌توانند به شما در تحلیل ترافیک و انتقال داده‌ها کمک کنند. همچنین می‌تواند با توجه به حجم بالای ترافیک، هر تهدیدی را که پنهان شده باشد، شناسایی کند.

معیارهای هوش مصنوعی در امنیت سایبری چیست؟

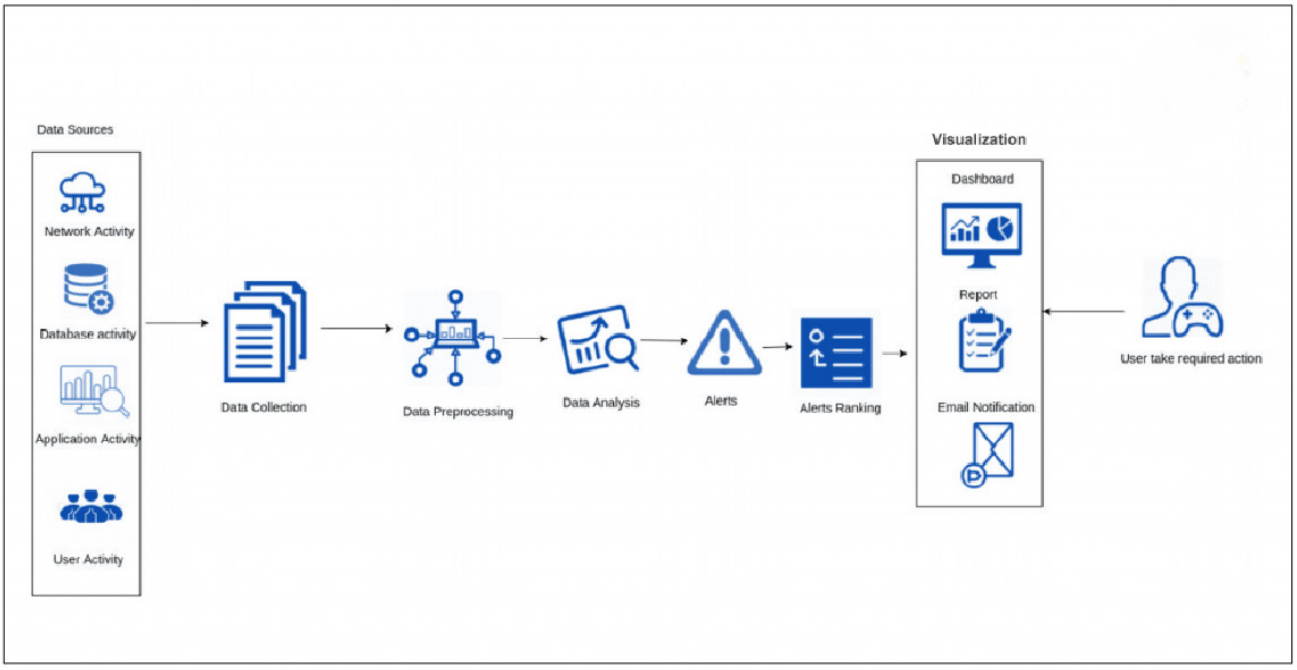
گره‌ها برای جمع‌آوری داده‌های رویداد امنیتی استفاده می‌شوند و در بخش‌های مختلف برای جمع‌آوری انواع مختلف داده‌ها قرار می‌گیرند. برخی داده‌های مربوط به ترافیک شبکه را جمع‌آوری می‌کنند و برخی دیگر اطلاعات دسترسی به پایگاه‌داده و غیره را جمع‌آوری می‌کنند. اقدامات امنیتی برروی داده‌هایی که جمع‌آوری می‌شوند اجرا شده تا از فرآیند انتقال امن آن از ماژول جمع‌آوری داده‌ها به ماژول ذخیره‌سازی و تجزیه‌وتحلیل داده‌ها اطمینان داشته باشند. اقدامات امنیتی گنجانده شده از سیستمی به سیستم دیگر متفاوت است.



برخی از سیستم‌ها ترجیح می‌دهند داده‌های جمع‌آوری شده را رمزگذاری کنند و سپس فرآیند انتقال داده‌ها را به‌صورت رمزگذاری‌شده انجام دهند. سیستم‌های دیگر ترجیح می‌دهند از زیرساخت کلید عمومی (PKI) برای اطمینان از فرآیند انتقال امن داده‌ها و تأیید گروه انتقال دهنده داده استفاده کنند. به محض اینکه داده‌ها توسط ماژول ذخیره‌سازی دریافت شد و ماژول تجزیه‌وتحلیل در یک حالت امن قرارگرفت، عملیات تجزیه‌وتحلیل داده‌ها برای شناسایی حملات اعمال می‌شود. نتایج حاصل از تجزیه‌وتحلیل از طریق ماژول تجسم به کاربران ارائه می‌شود.

ماژول‌های رتبه‌بندی هشدار امنیت سایبری هوش مصنوعی

ماژول جمع‌آوری داده، داده‌های رویداد امنیتی را از منابع مختلف دریافت می‌کند که سپس توسط ماژول pre-processing data، پیش‌پردازش می‌شود. داده‌های پیش‌پردازش‌شده رویداد امنیتی به مؤلفه تجزیه‌وتحلیل داده‌ها منتقل می‌شوند که شیوه‌های تحلیلی مختلفی را بر روی داده‌ها برای شناسایی حملات سایبری انجام می‌دهند. نتایج صادر شده از تجزیه‌وتحلیل (هشدارها) به ماژول رتبه‌بندی هشدار ارسال می‌شود که هشدارها را بر اساس قوانین از پیش‌تعریف‌شده رتبه‌بندی می‌کند تا تأثیر هشدار را بر کل زیرساخت سازمان ارزیابی کند. معیارهای رتبه‌بندی هشدارها به سازمان بستگی دارد.



برای مثال، قوانین رتبه‌بندی برای سازمان‌هایی که در برابر حملات DoS آسیب‌پذیر هستند، با سازمانی که در برابر حملات brute force آسیب‌پذیر است، متفاوت است. در نهایت، فهرست رتبه‌بندی هشدارهای ساده برای تفسیر و با استفاده از ماژول تجسم با مدیران امنیتی به اشتراک گذاشته می‌شود،که کار یک مدیر امنیتی را آسان می‌کند تا ابتدا به هشدارهای موجود در لیست رتبه‌بندی پاسخ دهد زیرا پیش‌بینی می‌شود این هشدارها پیامدهای خطرناک‌تری دارند.

بهترین ابزار برای استفاده هوش مصنوعی در امنیت سایبری چیست؟

در ادامه برخی از ابزارهایی که از الگوریتم‌های مختلف هوش مصنوعی برای رسیدن به امنیت بهتر و کاهش خطر در سازمان‌ها استفاده می‌کنند، معرفی می‌شوند.

Symantec Targeted Attack Analytics

این ابزار برای کشف حملات خصوصی و هدفمند استفاده می‌شود. هوش مصنوعی و یادگیری ماشین را در فرآیندها، دانش و قابلیت‌های کارشناسان و محققان امنیتی Symantec به کار می‌برد. ابزار تجزیه‌وتحلیل Targeted Attack توسط هوش مصنوعی برای مقابله با حمله Dragonfly2.0 استفاده شد. این حمله چندین شرکت فعال در حوزه انرژی را در ایالات متحده هدف قرار داد و سعی کرد به شبکه‌های عملیاتی دسترسی پیدا کند.

Sophos Intercept X tool

Sophos یک شرکت انگلیسی نرم افزار و سخت افزار امنیتی است. Intercept X از یک شبکه‌عصبی یادگیری عمیق که مانند مغز انسان عمل می‌کند، استفاده می‌کند. قبل از اجرای یک فایل، Intercept X میلیون‌ها ویژگی را از یک فایل بازیابی می‌کند، یک بررسی عمیق انجام می‌دهد و در عرض ۲۰ میلی‌ثانیه تصمیم می‌گیرد که آیا یک فایل سالم است یا فعالیت مخربی را انجام می‌دهد.

IBM QRadar Advisor

مشاور QRadar IBM از تکنولوژی‌های IBM Watson برای مقابله با حملات سایبری استفاده می‌کند. این مشاور از هوش مصنوعی برای بررسی خودکار نشانه‌های هر گونه آسیب‌پذیری یا بهره‌برداری استفاده می‌کند. مشاور QRadar از استدلال شناختی برای ارائه بازخورد ارزشمند و سرعت بخشیدن به فرآیند پاسخ استفاده می‌کند.

Vectra Cognito

مهاجمان را در زمان واقعی با استفاده از هوش مصنوعی شناسایی می‌کند. تشخیص تهدید و شناسایی مهاجمان در این ابزار به‌صورت خودکار انجام می‌شود. Cognito گزارش‌ها، رویدادهای ابری، داده‌های استفاده از شبکه و الگوریتم‌های تشخیص رفتار را جمع‌آوری می‌کند تا مهاجمان پنهان را در حجم‌های کاری و دستگاه‌های IOT آشکار کند.

Darktrace Antigena

روشی موثر برای دفاع از سیستم خود است. Antigena عملکرد فوری و ضروری Darktrace را گسترش می‌دهد تا نقش پادتن‌های دیجیتالی را که تهدیدها و ویروس‌ها را شناسایی و خنثی می‌کنند، شناسایی و تکرار کند. Antigena از سیستم ایمنی Enterprise Darktrace برای شناسایی و واکنش به رفتار مخرب در زمان واقعی، بر اساس ماهیت خطر، استفاده می‌کند.

جمع‌بندی

هوش مصنوعی (AI) به سرعت در حال تبدیل‌شدن به یک ابزار ضروری برای بهبود اثربخشی تیم‌های امنیت سایبری و فناوری‌اطلاعات (IT) است. ایمن نگه‌داشتن داده‌ها و شبکه در محیط کسب‌وکار امروزی بسیار پیچیده و مشکل شده است. با استفاده از هوش مصنوعی می‌توان برای تقویت زیرساخت امنیتی خود گامی در جهت ایمن‌تر شدن سیستم خود برداشت که در این مقاله برخی تکنیک‌ها و ابزارهای مورد استفاده در این راستا معرفی شد.

امنیت اطلاعات

منا علی‌اکبری

رعایت نکات امنیتی در مرورگرهای وب

مقدمه

مرورگر وب یک برنامه کاربردی است که به کاربران اجازه می‌دهد، اطلاعات را از شبکه جهانی وب، مشاهده و دریافت کنند. این اطلاعات می‌تواند شامل متن، تصویر، ویدئو و هر نوع اطلاعات دیگری باشد. نحوه کارکرد مرورگرهای وب، تحلیل و تفسیر کدهای HTML و تبدیل آن‌ها به عناصر و المان‌های قابل مشاهده است. بسیاری از مرورگرها افزونه‌هایی نیز ارائه می‌دهند که قابلیت‌های مرورگر را افزایش می‌دهند، به عنوان مثال این افزونه‌ها می‌توانند به کاربران اجازه دهند از اقداماتی مانند افزودن ویژگی‌های امنیتی استفاده کنند.

برخی از مرورگرهای وب عبارتند از:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Opera
- Safari

محبوب‌ترین مرورگرهای وب طبق سه ویژگی زیر، امتیاز بندی می‌شوند:

- فاصله زمانی بین هر به‌روزرسانی
- ویژگی‌های امنیتی مرورگر موردنظر
- ابزارهای رعایت حریم شخصی

به موازات رشد روزافزون کارکردهای مرورگرها هیچ یک از مرورگرهای وب از تهدیدهای امنیتی در امان نیستند، هرچند توسعه‌دهندگان مرورگرها همواره در تلاش هستند که بالاترین ضریب امنیتی را برای کاربران خود فراهم کنند اما هنگامی‌که کاربران با وب‌سایت‌ها تعامل می‌کنند، احتمال وجود لینک‌ها و فایل‌های مخرب، عدم آگاهی کاربران از امکاناتی که به مرورگرها اضافه می‌شود و سایر تهدیدات را در پیش‌روی خود دارند.

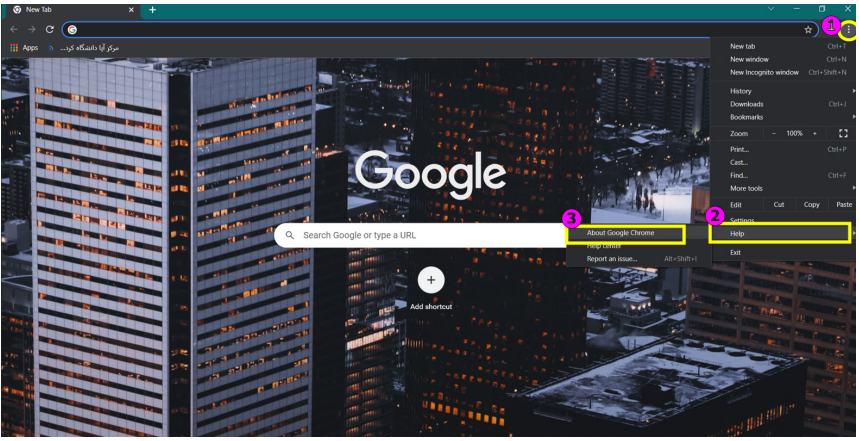
طبق بررسی‌های انجام شده، هم در داخل ایران و هم به‌صورت جهانی، دو مرورگر **گوگل کروم** و **موزیلا فایرفاکس** دارای بیش‌ترین درصد استفاده و به نسبت دیگر مرورگرها محبوب‌تر نیز هستند و در ادامه درخصوص رعایت نکات امنیتی در این دو مرورگر نکاتی بیان خواهد شد.

به‌روزرسانی مرورگرها

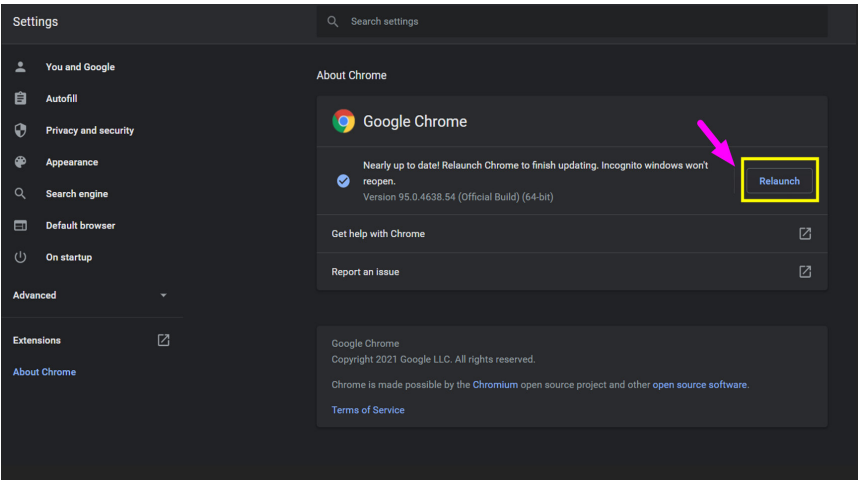
به‌روز نگه‌داشتن مرورگرها به این‌دلیل‌که بیشترین نقطه اتصال بین سیستم و دنیای خارج از آن هستند، بسیار حائز اهمیت است. مرورگرهای قدیمی می‌توانند مشکلات امنیتی جدی داشته باشند و با اجرای مرورگرهای قدیمی‌تر، احتمالاً قابلیت‌های مفید و جدیدی را که مرورگرها در نسخه‌های جدیدتر پشتیبانی می‌کنند از دست خواهید داد.

به‌روزرسانی مرورگر گوگل کروم

۱. گوگل کروم را باز کنید.
۲. بر روی منوی به شکل سه نقطه افقی در سمت راست بالا کلیک کنید.
۳. در منوی باز شده، از زیرمنوی Help گزینه About google chrome را انتخاب کنید.



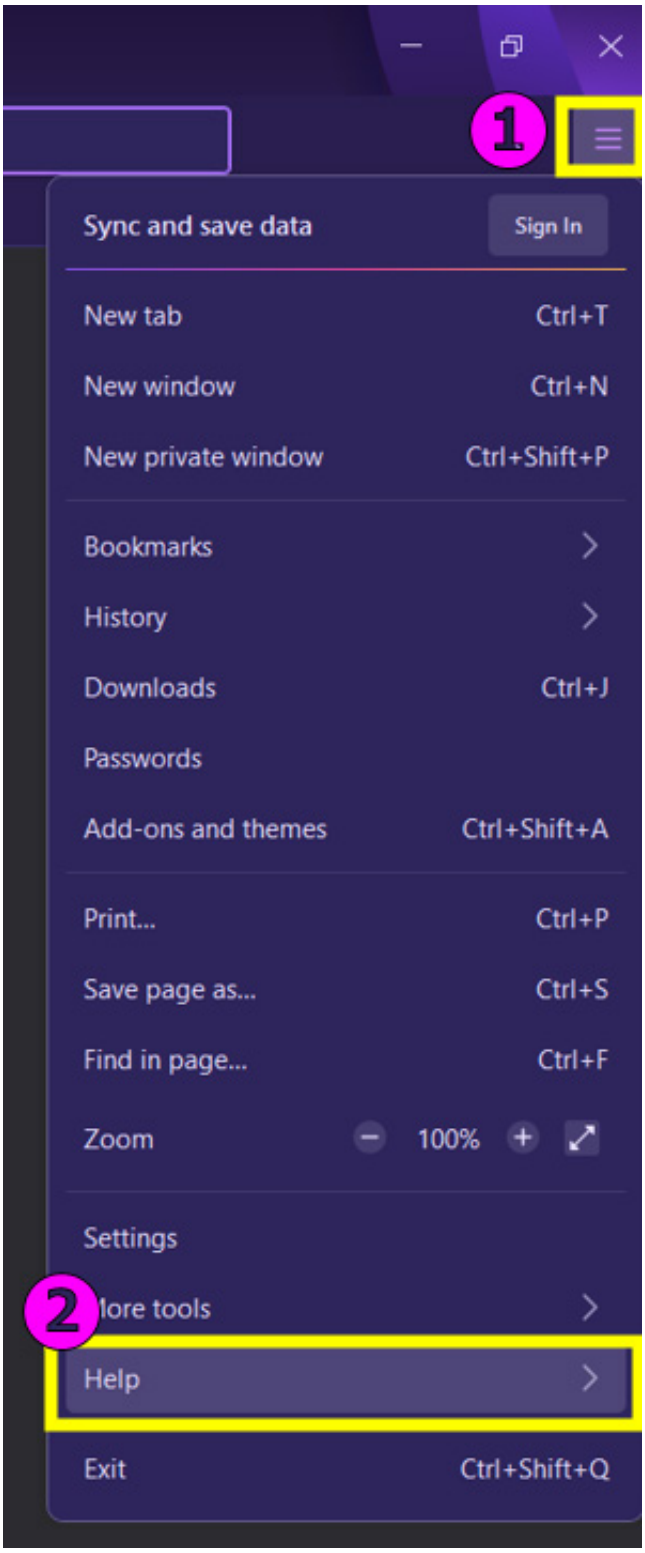
۴. وقتی پنجره About google chrome باز شد، به‌صورت خودکار به‌روزرسانی‌ها را بررسی می‌کند، اگر به‌روزرسانی جدیدی در دسترس باشد، آن را دانلود می‌کند.
۵. بعد از انجام به‌روزرسانی، بر روی گزینه Relaunch کلیک کنید تا مرورگر راه‌اندازی مجدد شده و به‌روزرسانی اعمال شود.

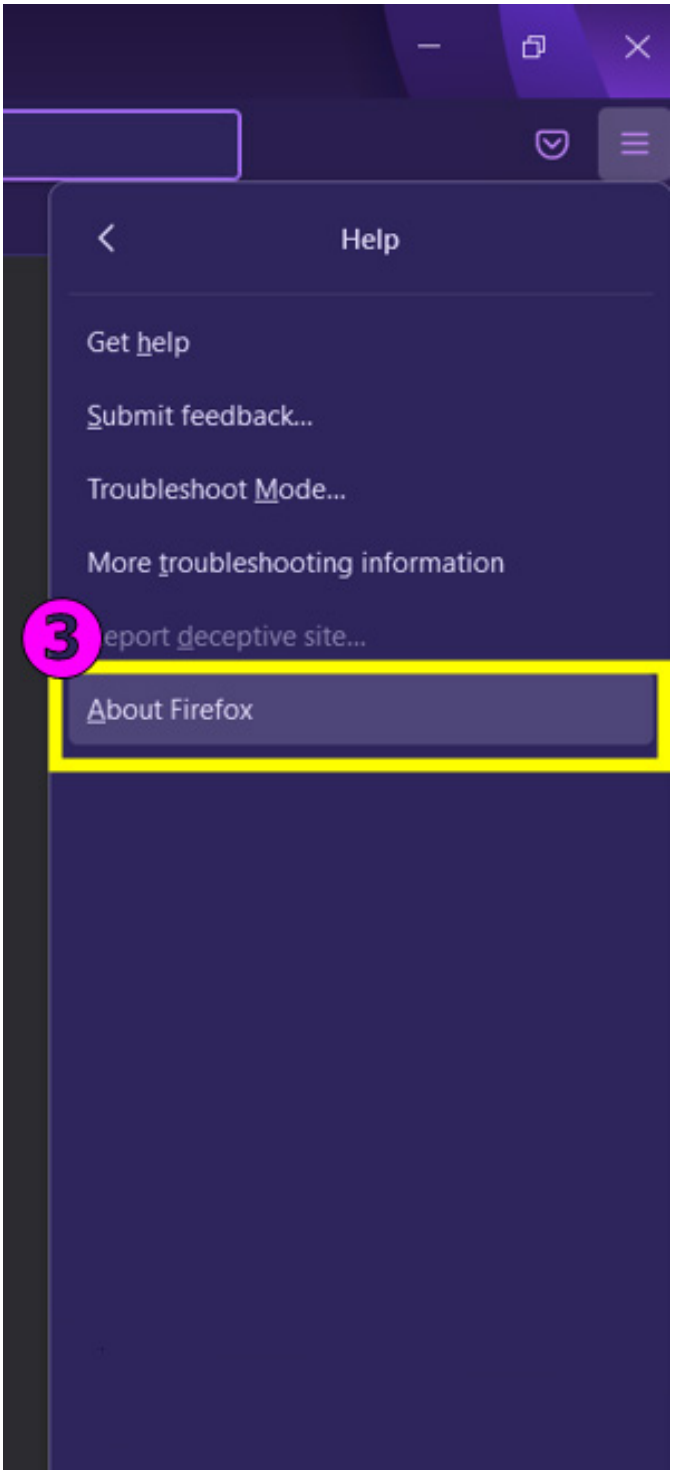


به‌روزرسانی مرورگر موزیلا فایرفاکس

به‌صورت پیش‌فرض، در این مرورگر به‌طور خودکار به‌روزرسانی انجام می‌شود اما کاربر نیز هر زمان بخواهد می‌تواند به‌روزرسانی دستی هم انجام دهد. در ادامه این فرایند بیان شده است.

۱. فایرفاکس را باز کنید.
۲. بر روی منو به شکل سه خط افقی در سمت راست بالا کلیک کنید.
۳. در منوی باز شده، از زیر منوی Help گزینه About firefox را انتخاب کنید.
٤. وقتی پنجره About firefox باز شد، به‌صورت خودکار به‌روزرسانی‌ها را بررسی می‌کند، اگر به‌روزرسانی جدیدی در دسترس باشد، آن را دانلود و نصب می‌کند.
۵. بعد از انجام به‌روزرسانی فایرفاکس Restart شود.



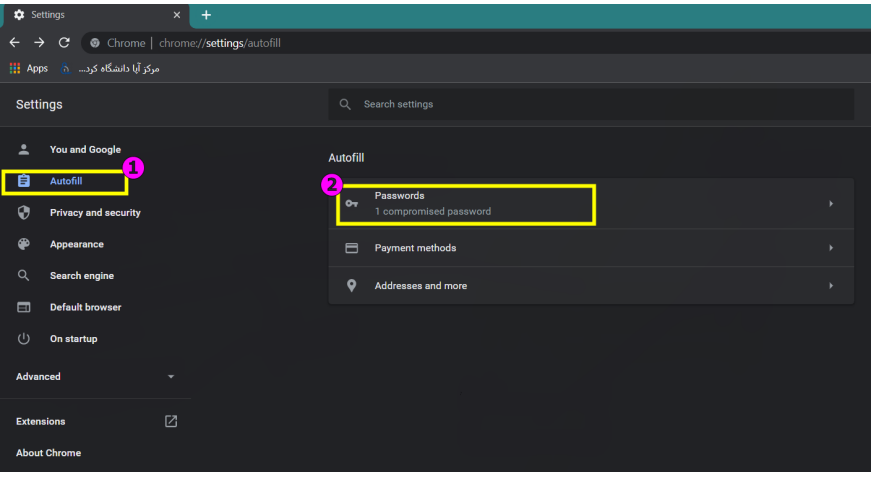


حذف گذرواژه‌های ذخیره شده در مرورگر

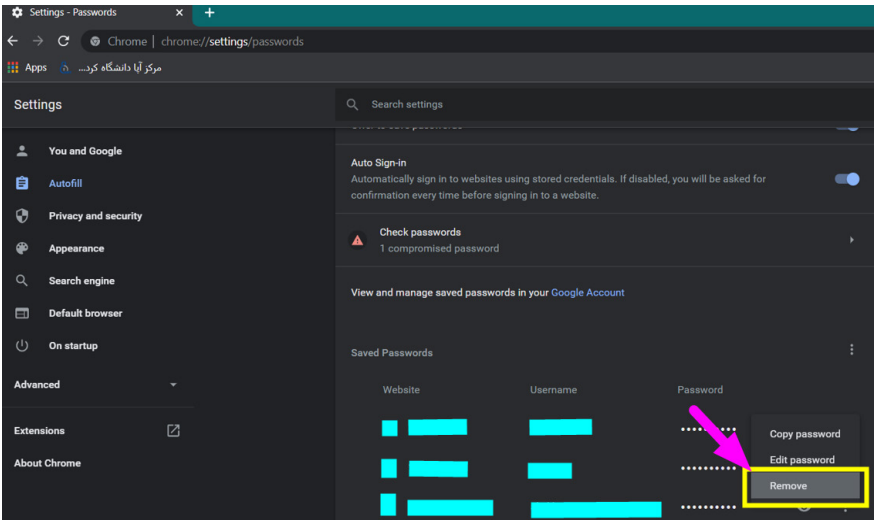
گذرواژه‌های ذخیره شده در مرورگرها یک تهدید امنیتی برای کاربران به حساب می‌آیند. هکرها به راحتی می‌توانند به گذرواژه‌های ذخیره شده در مرورگر کاربران دست پیدا کنند و امنیت حساب‌های کاربری آن‌ها را دچار چالش کنند. برای جلوگیری از این کار لازم است، گذرواژه‌های ذخیره شده در مرورگر را حذف کرد. همچنین پیشنهاد می‌شود گزینه ذخیره گذرواژه در مرورگر غیرفعال شود.

نحوه حذف گذرواژه‌های ذخیره شده در کروم

۱. گوگل کروم را باز کنید.
۲. بر روی منوی به شکل سه نقطه افقی در سمت راست بالا کلیک کنید.
۳. در منوی باز شده، گزینه Setting و سپس گزینه Autofill و در آخر گزینه Passwords را انتخاب کنید.

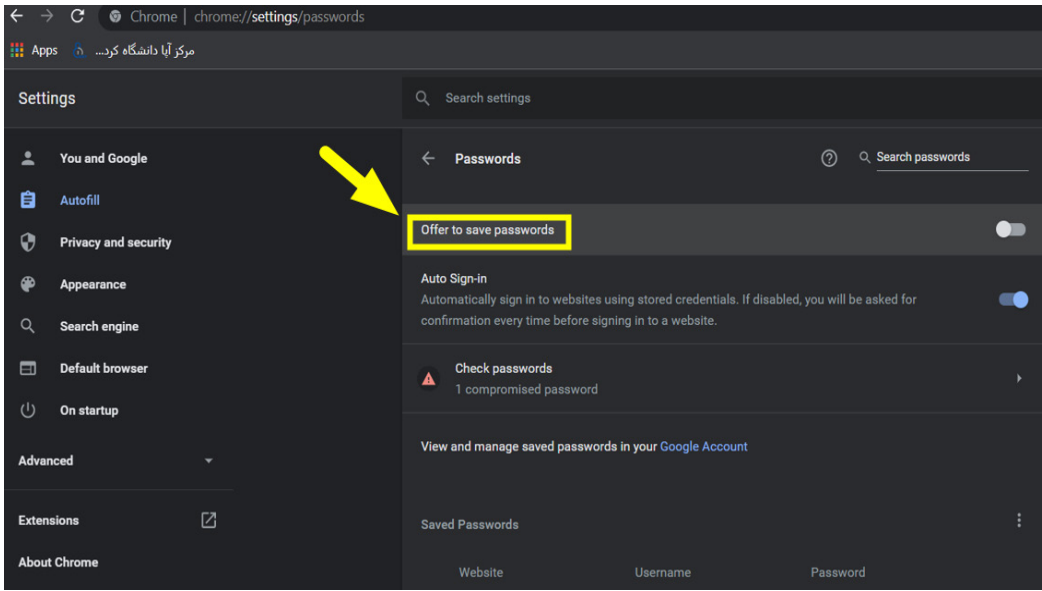


٤. سپس گذرواژه‌های ذخیره شده شما نمایش داده می‌شوند و با کلیک بر روی سه نقطه افقی کنار گذرواژه‌های و انتخاب گزینه Remove موارد ذخیره شده، حذف می‌شوند.

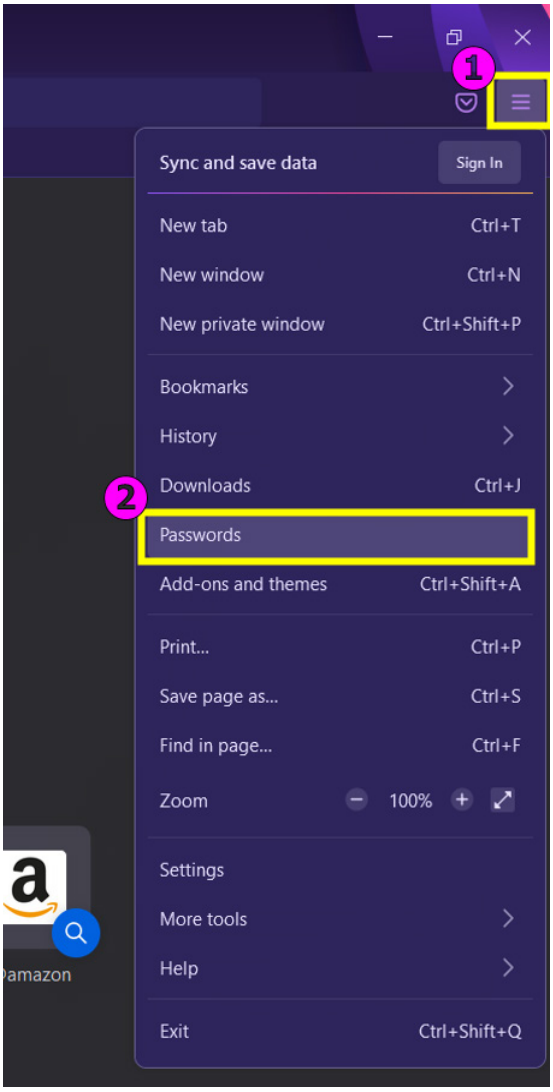


همچنین برای عدم نمایش پیشنهاد ذخیره گذرواژه‌ها گزینه Offer to save passwords را طبق مسیر زیر غیرفعال کنید.

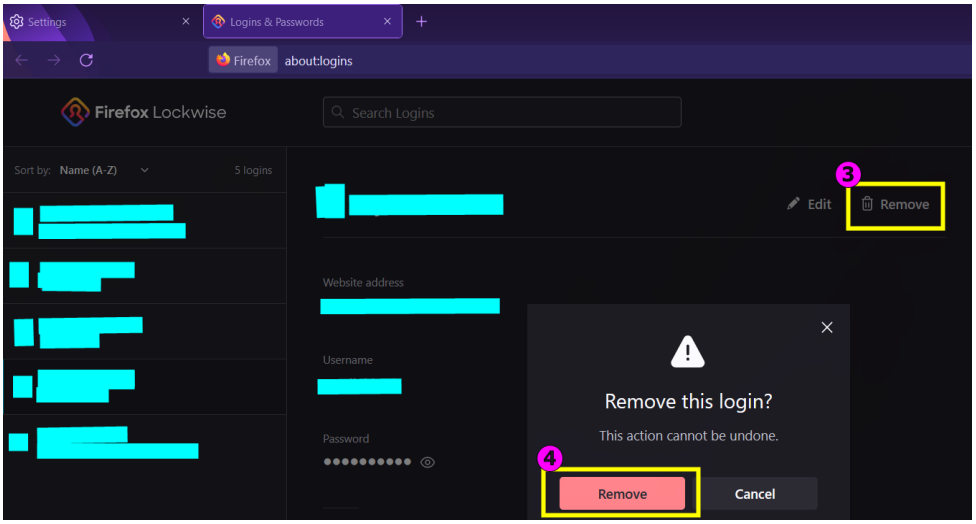
Chrome://Setting/Autofill/Passwords/Offer to save passwords



نحوه حذف گذرواژه‌های ذخیره شده در فایرفاکس

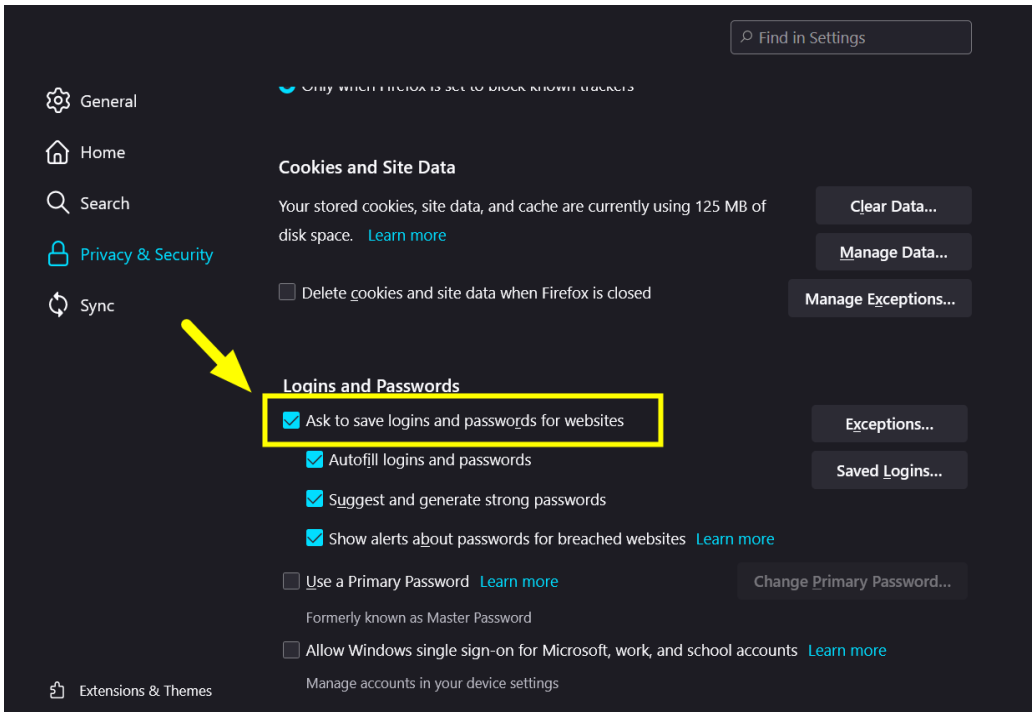


۱. فایرفاکس را باز کنید.
۲. بر روی منوی به شکل سه خط افقی در سمت راست بالا کلیک کنید.
۳. در منوی باز شده بر روی Passwords کلیک کنید.
٤. در این مرحله گذرواژه‌های ذخیره شده نمایش داده می‌شوند و با انتخاب هر کدام و کلیک بر روی Remove می‌توان آن را حذف کرد.



همچنین برای عدم نمایش پیشنهاد ذخیره گذرواژه‌ها گزینه Ask to save logins and passwords for websites را طبق مسیر زیر غیرفعال کنید.

Firefox://Setting/Privacy and security/Logins and Passwords/Ask to save logins and passwords for websites



غیرفعال کردن گزینه Third-Party Cookies

کوکی چیست؟

کوکی‌ها فایل‌های متنی با داده‌های کوچک هستند که بر روی سیستم کاربر ذخیره می‌شوند، در کوکی‌ها اطلاعاتی برای شناسایی کاربر و علاقه‌مندی‌هایش ذخیره می‌شود. وب‌سایت‌ها از کوکی‌ها برای ساده‌سازی تجربیات وب شما استفاده می‌کنند، مثلا اگر تنظیمات بخصوصی را که برای سایتی انتخاب کرده‌اید و به‌طور تصادفی صفحه را بستید یا صفحه را بازسازی کردید، به‌جای اینکه مجدداً وارد سیستم شوید و تغییرات را دوباره اعمال کنید، کوکی‌ها اطلاعات ورود شما را ذخیره دارند و از اعمال مجدد آن‌ها جلوگیری می‌کنند.

آیا کوکی‌ها می‌توانند خطرناک باشند؟

به‌دلیل ماهیت ساختاری و محدودیت‌هایی که کوکی‌ها دارند، مضر نیستند و قادر به انتقال فایل‌های مخرب یا بدافزار به داخل سیستم کاربر نیستند اما توانایی آن‌ها در ردیابی سابقه مرور افراد، خطرساز است.

کوکی‌های اول شخص و شخص ثالث

کوکی‌ها به دسته‌های مختلفی تقسیم‌بندی می‌شوند اما به‌صورت کلی دو نوع کوکی مرورگر وجود دارد، کوکی اول شخص و شخص ثالث.

از لحاظ فنی بین کوکی اول شخص و شخص ثالث هیچ تفاوت اساسی وجود ندارد. هر کوکی مالکی دارد که همین موضوع باعث نامگذاری آن شده است.

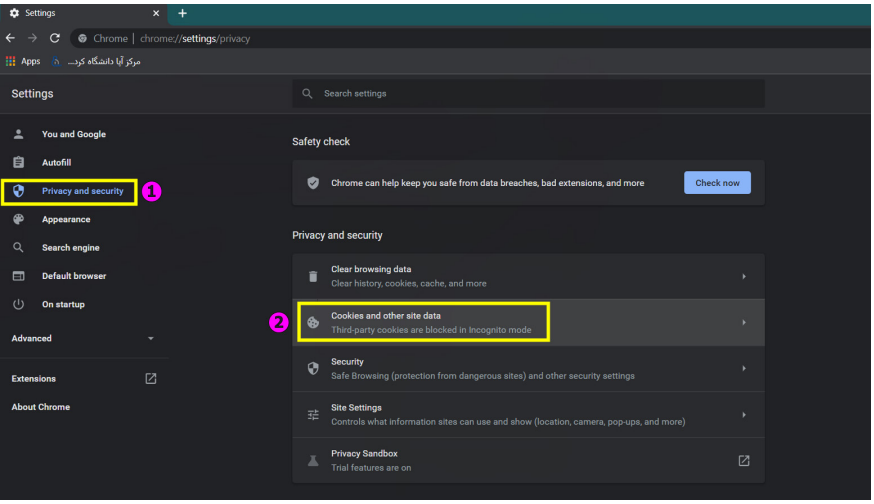
کوکی اول شخص «First-Party Cookie» مستقیما توسط همان سایتی که در حال بازدید از آن هستید ایجاد می‌شود.

همه کوکی‌هایی که توسط دامنه دیگری به‌جز دامنه‌ای که در حال بازدید از آن هستید ایجاد می‌شوند، کوکی شخص ثالث «Third-Party Cookie» می‌باشند.

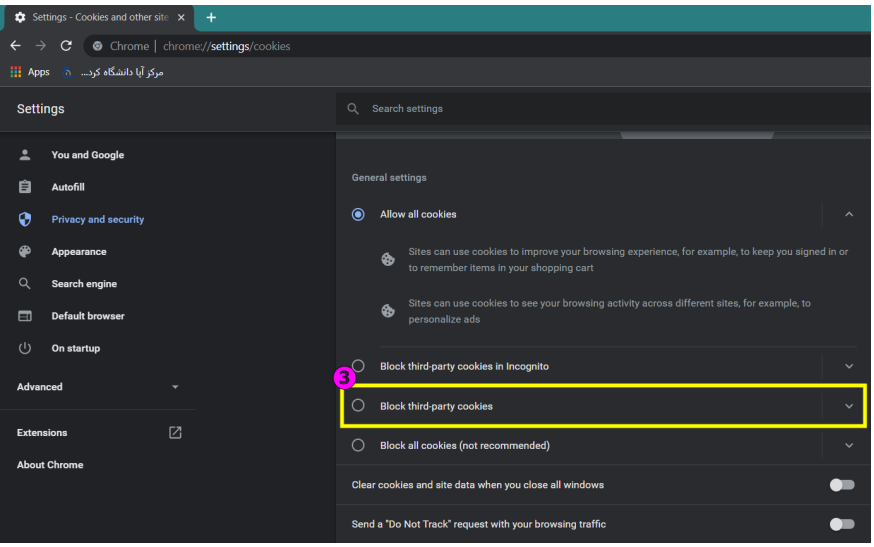
کوکی‌های شبکه‌های اجتماعی و سایت‌های تبلیغاتی و فروش از نوع شخص ثالث هستند و با ردیابی فعالیت‌های کاربر می‌توانند تبلیغات هدفمند را برایش ارسال کنند. می‌توان به‌صورت کلی کوکی‌های شخص ثالث را مسدود کرد. فرآیند انجام این کار در مرورگرهای مختلف متفاوت است.

نحوه فعال کردن گزینه Block third-party cookies در مرورگر گوگل کروم

۱. گوگل کروم را باز کنید.
۲. بر روی منوی به شکل سه نقطه افقی ⋮ در سمت راست بالا کلیک کنید.
۳. در منوی باز شده، گزینه Setting و بعد از آن گزینه Privacy and security را انتخاب کنید.

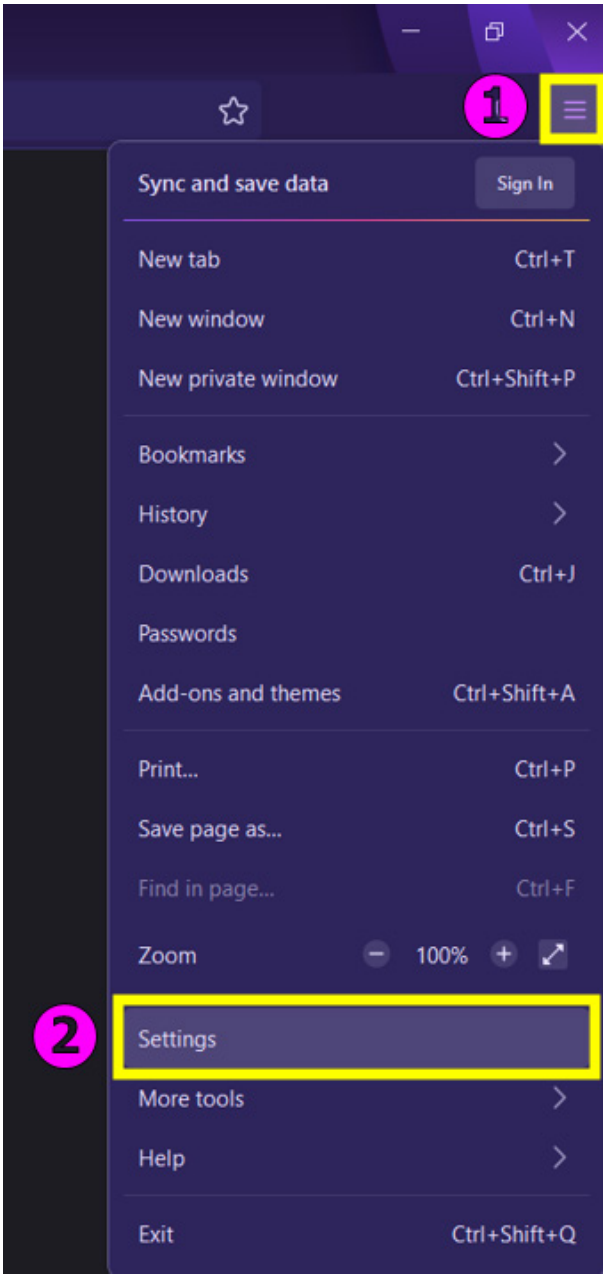


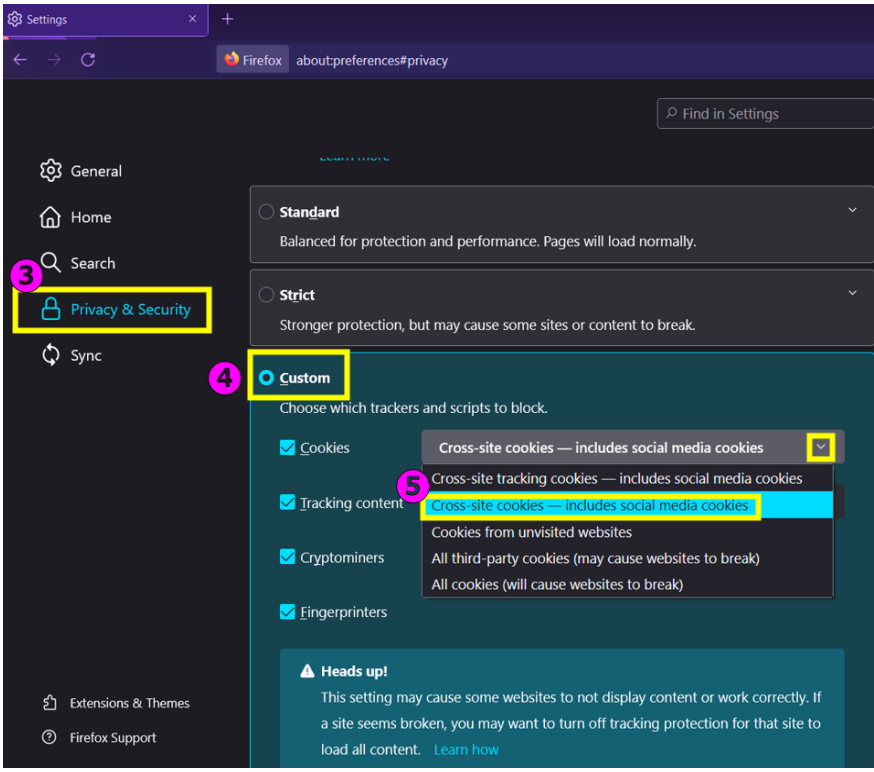
٤. سپس گزینه Cookies and other site data را انتخاب کرده، در این بخش گزینه Block third-party cookies را فعال کنید.



نحوه فعال کردن گزینه Block third-party cookies در مرورگر موزیلا فایرفاکس

۱. فایرفاکس را باز کنید.
۲. بر روی منو به شکل سه خط افقی در سمت راست بالا کلیک کنید.
۳. در منوی باز شده، ابتدا بر روی گزینه Setting کلیک کنید.
٤. سپس بر روی گزینه Privacy and security کلیک کنید. حال در پنجره باز شده به پایین اسکرول کرده و در قسمت Custom طبق عکس زیر بخش Cross-site–includes social media cookies را انتخاب کنید.

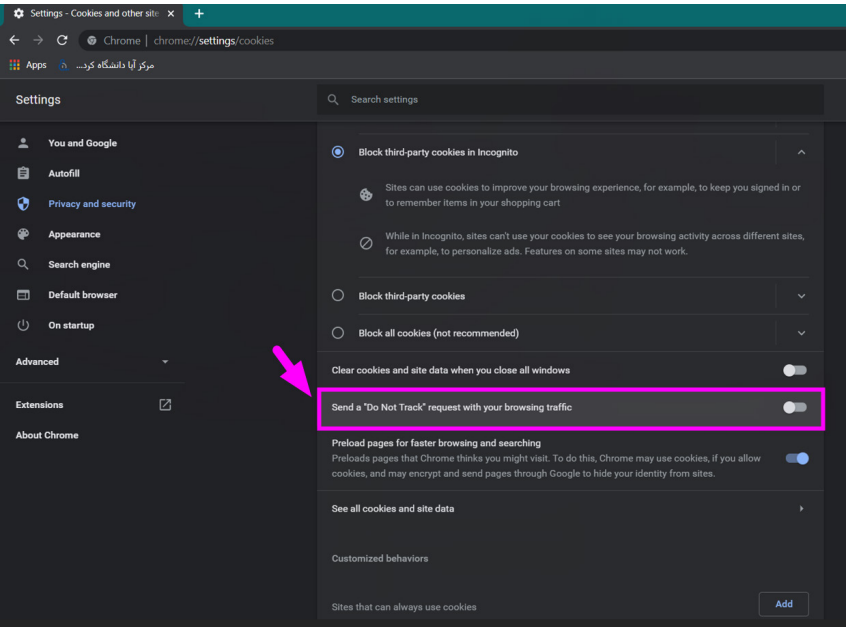




غیرفعال‌کردن ویژگی Tracking در مرورگرها

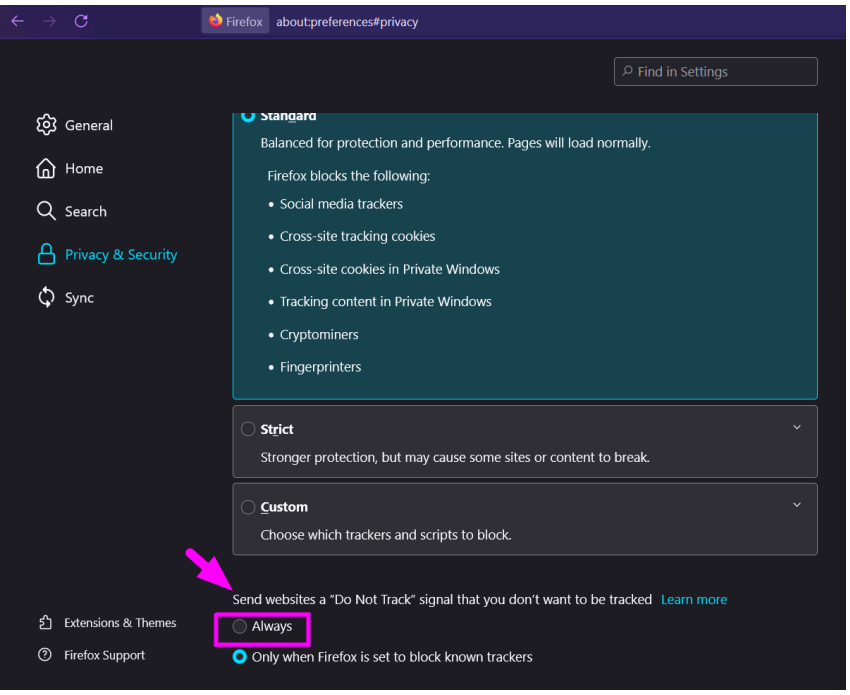
Tracking یا ردیابی وب‌سایت روشی برای تجزیه‌وتحلیل و ثبت رفتار آنلاین کاربران، جهت تبلیغات هدفمند در وب‌سایت است. ردیاب‌ها اطلاعاتی مانند تجزیه‌وتحلیل ترافیک مرورگرها، جزئیات خرید، تعامل با رسانه‌های اجتماعی، سیستم‌های نظردهی تعبیه شده در سایت‌ها و مکان را جمع‌آوری می‌کنند. کاربران اغلب از ردیابی در حال انجام بی‌اطلاع هستند که این امر، ردیابی را به یکی از دغدغه‌های مهم حفظ حریم خصوصی کاربران تبدیل می‌کند.
قابلیت Do Not Track یا DNT به معنای ردیابی نکردن است و به سایت‌ها نشان می‌دهد که کاربر مایل نیست فعالیت‌های او مورد ردیابی و پیگیری قرار گیرد و به‌وسیله روش‌های زیر در مرورگرهای کروم و فایرفاکس فعال می‌شود:

نحوه فعال سازی Do Not Track در مرورگر کروم



۱. گوگل کروم را باز کنید.
۲. بر روی منوی به شکل سه نقطه افقی در سمت راست بالا کلیک کنید.
۳. در منوی باز شده، گزینه Setting و بعد از آن گزینه Privacy and security و سپس گزینه Cookies and other site data را انتخاب کنید.
٤. در منوی باز شده به پایین اسکرول کرده و تیک گزینه Send a “Do Not Track”request with your browsing traffic را فعال کنید.

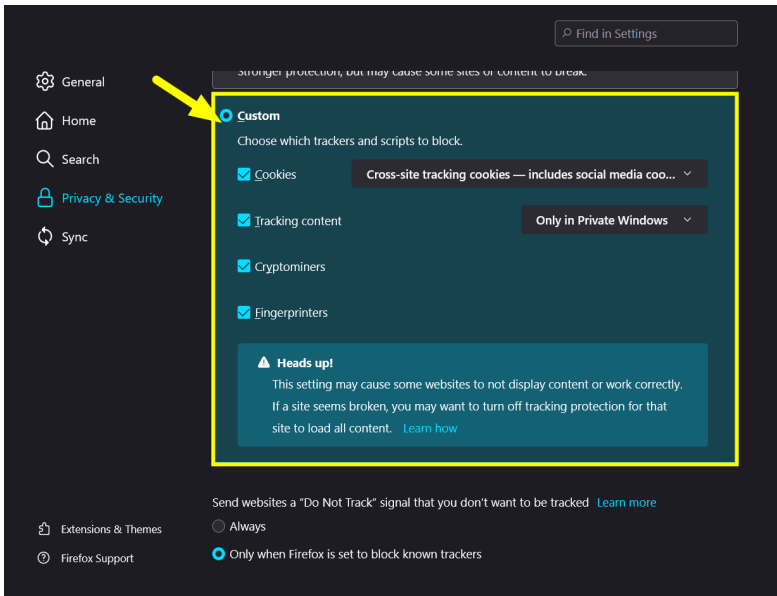
نحوه فعال سازی Do Not Track در مرورگر فایرفاکس



۱. فایرفاکس را باز کنید.
۲. بر روی منو به شکل سه خط افقی در سمت راست بالا کلیک کنید.
۳. در منوی باز شده بر روی Setting و بعد بر روی Privacy and security کلیک کنید.
٤. به پایین اسکرول کرده و در بخش Send websites a “Do Not Track” signal that you don’t want to be tracked گزینه Always را فعال کنید

نحوه قرار دادن تنظیمات Do Not Track به‌صورت سفارشی:

Firefox://Setting/Privacy and security/Enhanced Tracking Protection/Custom

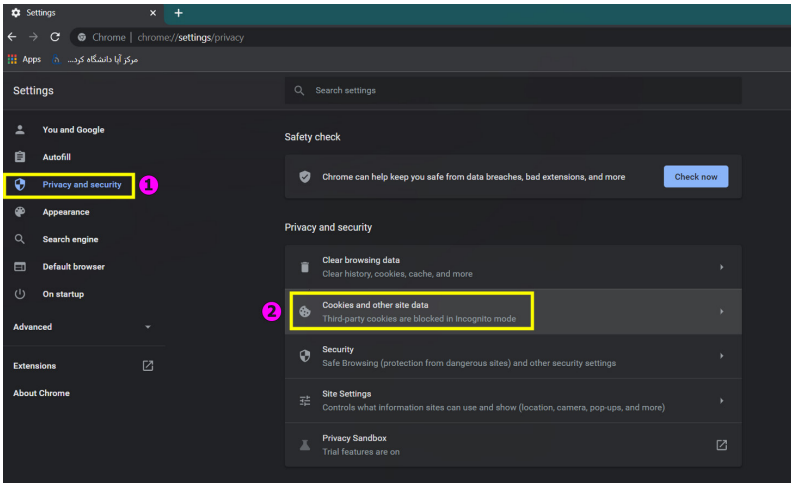


حالت ناشناس در مرورگرها

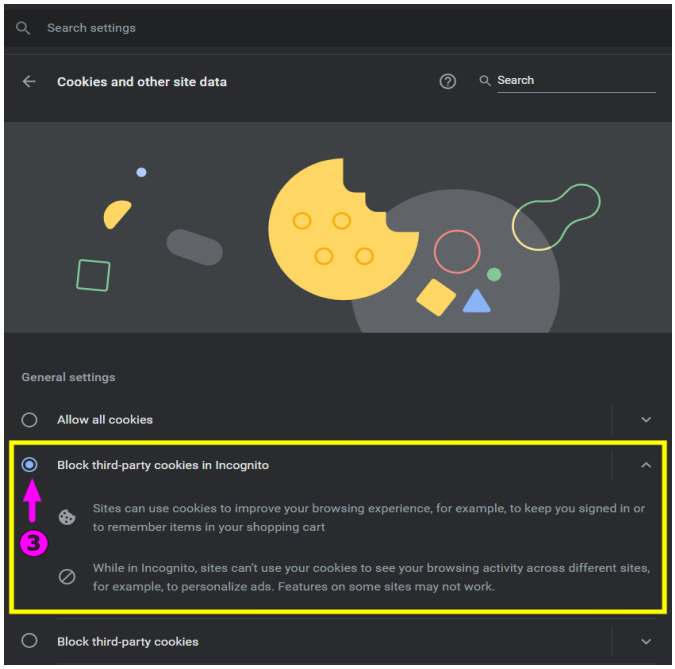
حالت ناشناس به معنای پنهان کردن هویت کاربر بوده که این حالت در مرورگر گوگل کروم با نام Incognito و در مرورگر موزیلا فایرفاکس با نام InPrivate شناخته می‌شود. حالت ناشناس این امکان را فراهم می‌کند که شما بتوانید با خیال راحت‌تری بدون اینکه اطرافیان بتوانند سابقه فعالیت شما در وب را زیر نظر بگیرند، وب‌گردی کنید. به‌عبارت دیگر در حالت ناشناس، مرورگر هرگز پیشینه وب‌گردی، کوکی‌ها و تاریخچه دانلودهای شما را ذخیره نخواهد کرد.

نحوه فعال کردن حالت Incognito در مرورگر گوگل کروم

۱. گوگل کروم را باز کنید.
۲. بر روی منوی به شکل سه نقطه افقی در سمت راست بالا کلیک کنید.
۳. در منوی باز شده، گزینه Setting و بعد از آن گزینه Privacy and security را انتخاب کنید، بعد وارد بخش Cookies and other site data شوید.

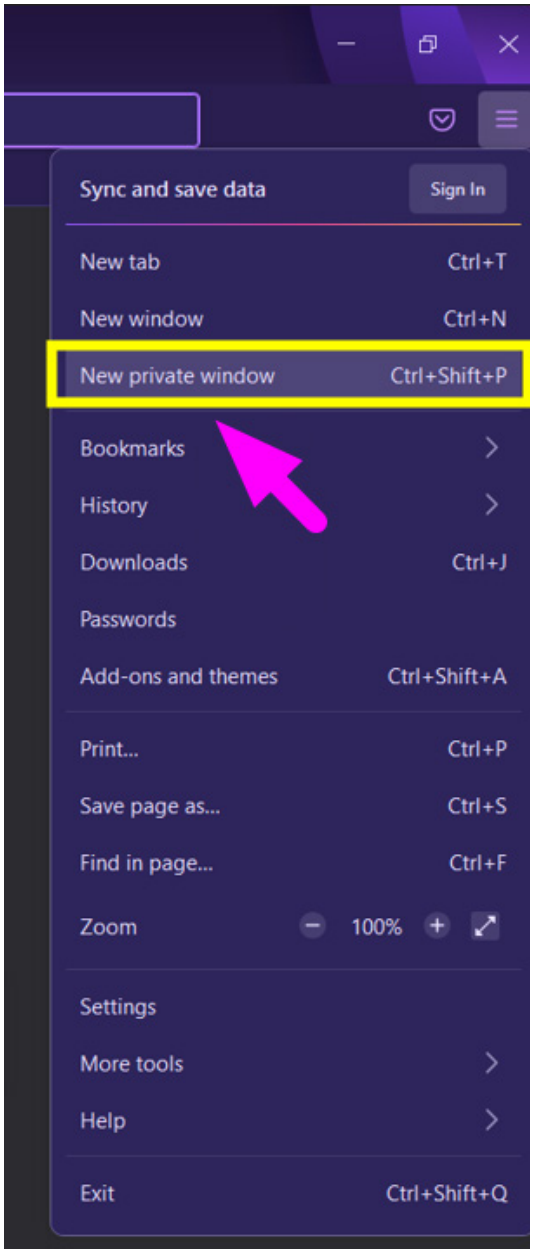


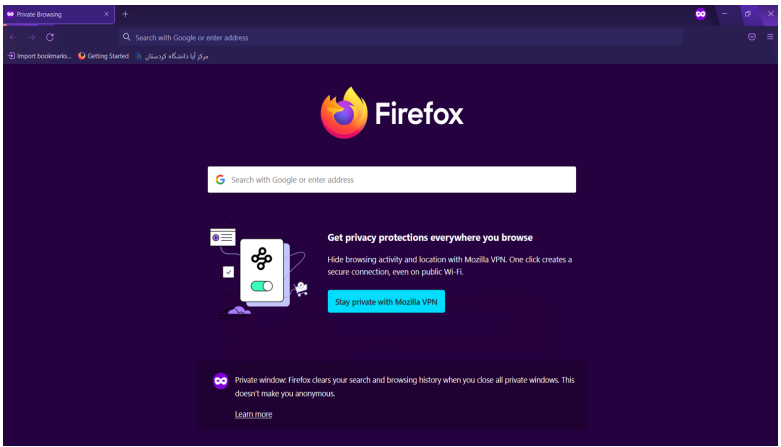
٤. در این بخش گزینه Block third-party cookies in Incognito را فعال کنید.



نحوه فعال کردن حالت In-Private در مرورگر موزیلا فایرفاکس

۱. فایرفاکس را باز کنید.
۲. بر روی منوی به شکل سه خط افقی در سمت راست بالا کلیک کنید.
۳. در منوی باز شده بر روی New private window کلیک کنید.



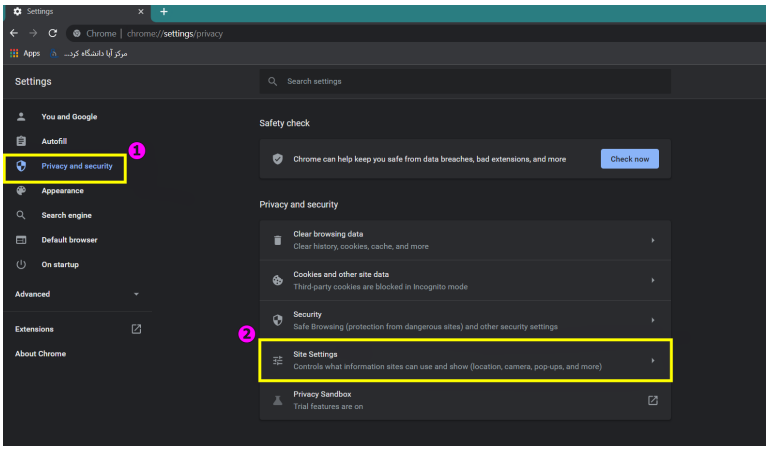


فعال کردن گزینه‌های block pop-up

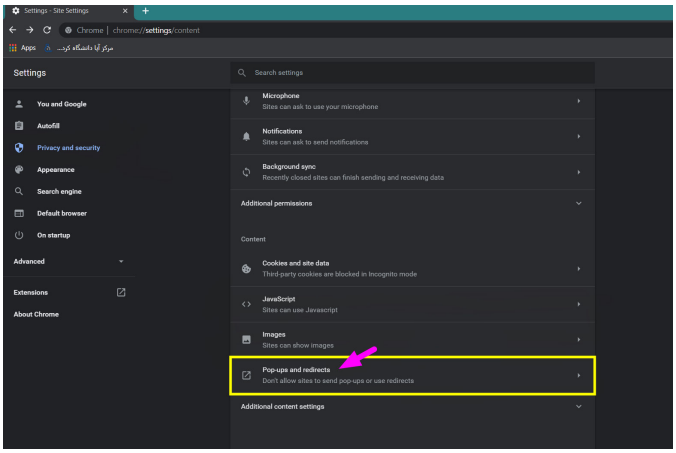
پاپ آپ (Pop-Up)ها تبلیغاتی هستند که بدون اجازه کاربر باز می‌شوند و در اکثر موارد آزار دهنده بوده و ممکن است حاوی لینک‌های آلوده و مخرب برای کاربران باشند. نحوه مسدود کردن آن‌ها در ادامه بیان می‌شوند

نحوه فعال سازی Block pop-ups در مرورگر کروم

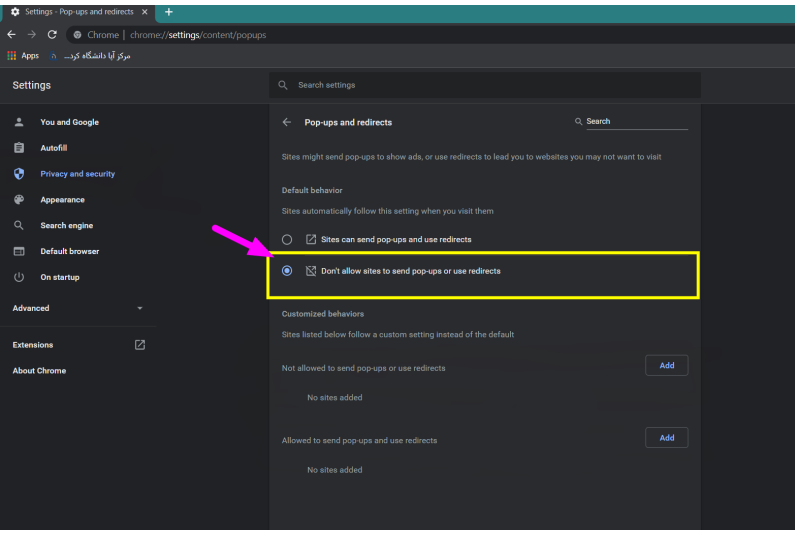
۱. گوگل کروم را باز کنید.
۲. بر روی منوی به شکل سه نقطه افقی در سمت راست بالا کلیک کنید.
۳. در منوی باز شده بر روی Setting و سپس بر روی Privacy and security و بعد بر روی Site setting کلیک کنید.



۴. به پایین اسکرول کرده و بر روی Pop-ups and redirects کلیک کنید.

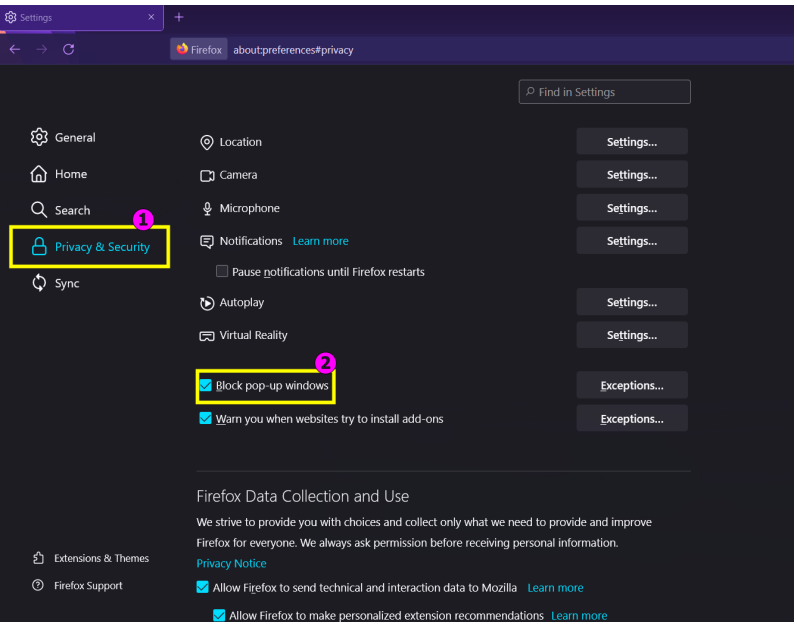


۵. در بخش Sites automatically follow this setting when you visit them بر روی گزینه Don't allow sites to send pop-ups or use redirects کلیک کنید.



نحوه فعال‌سازی Block pop-ups در مرورگر فایرفاکس

۱. فایرفاکس را باز کنید.
۲. بر روی منو به شکل سه خط افقی در سمت راست بالا کلیک کنید.
۳. در منوی باز شده بر روی Setting و بعد بر روی Privacy and security کلیک کنید.
۴. به پایین اسکرول کرده و تیک گزینه Block pop-up windows را فعال کنید.

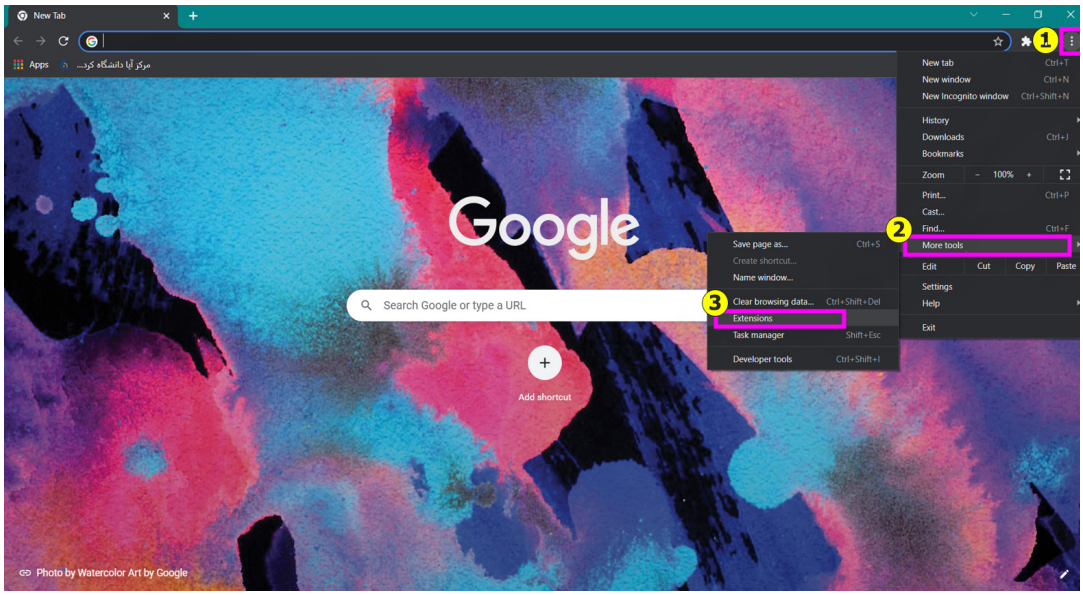


استفاده از افزونه‌ها

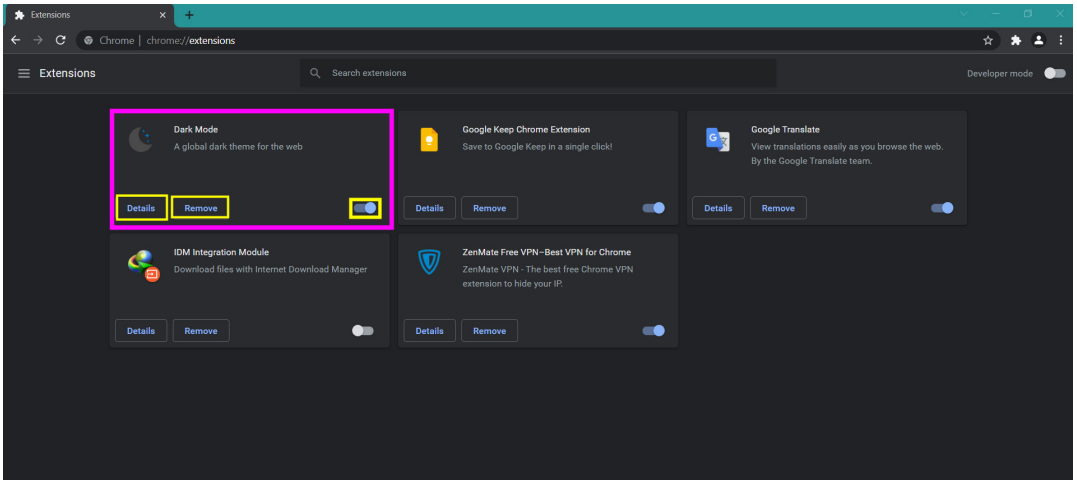
افزونه‌ها با اضافه‌کردن قابلیت‌هایی به مرورگر می‌توانند عملکرد آن‌ها را افزایش دهند یا ویژگی‌های جدیدی به آن‌ها اضافه کنند. در مرورگرهای مختلف سه واژه Extension و Add-on و Plug-in را می‌توان مترادف درنظر گرفت. به این صورت که مرورگر Firefox از اصطلاح Add-on و مرورگر کروم از اصطلاح Extension و پلتفرم مدیریت محتوای وردپرس (WordPress) و نرم افزارهای Adobe Photoshop و Adobe Audition از همان اصطلاح Plug-in استفاده می‌کنند که در زبان فارسی، همگی افزونه ترجمه شده‌اند.

افزونه‌ها در انواع رایگان و تجاری وجود دارند و برای دانلود و نصب باید به فروشگاه رسمی افزونه هر مرورگر مراجعه کنید. توسعه‌دهندگان مرورگر قبل از اینکه افزونه‌ها را برای دانلود در دسترس قرار دهند، مورد بررسی و ارزیابی قرار داده و پس از تأیید، اقدام به انتشار می‌کنند. بعد از نصب هر افزونه، لیستی از آنها برای مرورگر کروم و فایرفاکس به‌صورت زیر نشان داده می‌شود. البته می‌توان آیکون مربوط به هر افزونه در گوشه‌ی بالا، سمت راست مرورگر نمایش داده شود.

بخش افزونه‌ها در مرورگر کروم chrome://extensions



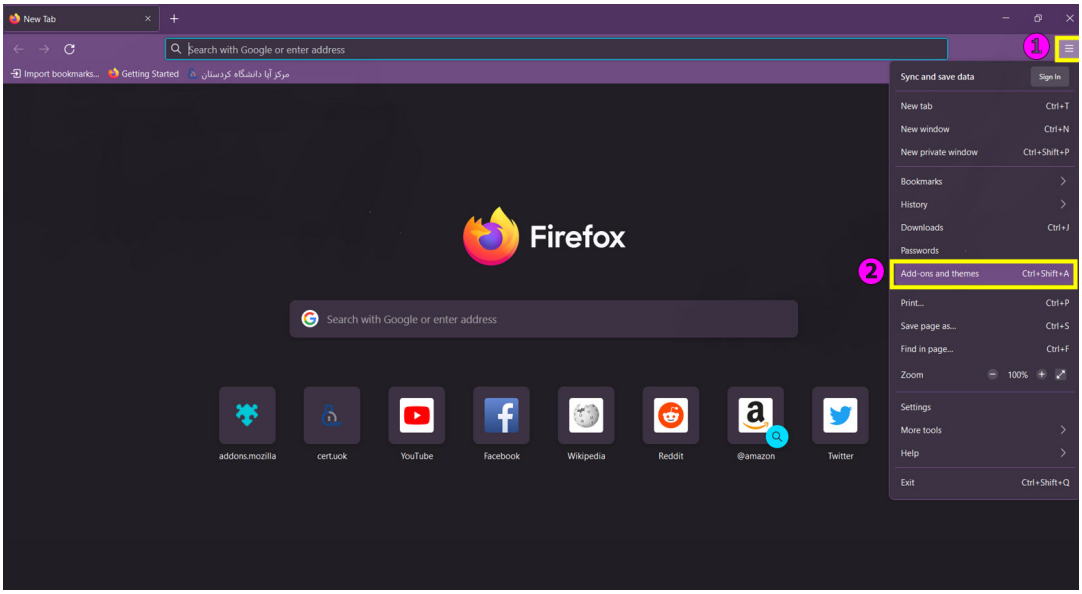
در بخش مربوط به Extension می‌توان لیستی از افزونه‌هایی که در مرورگر نصب شده را مشاهده کرد.



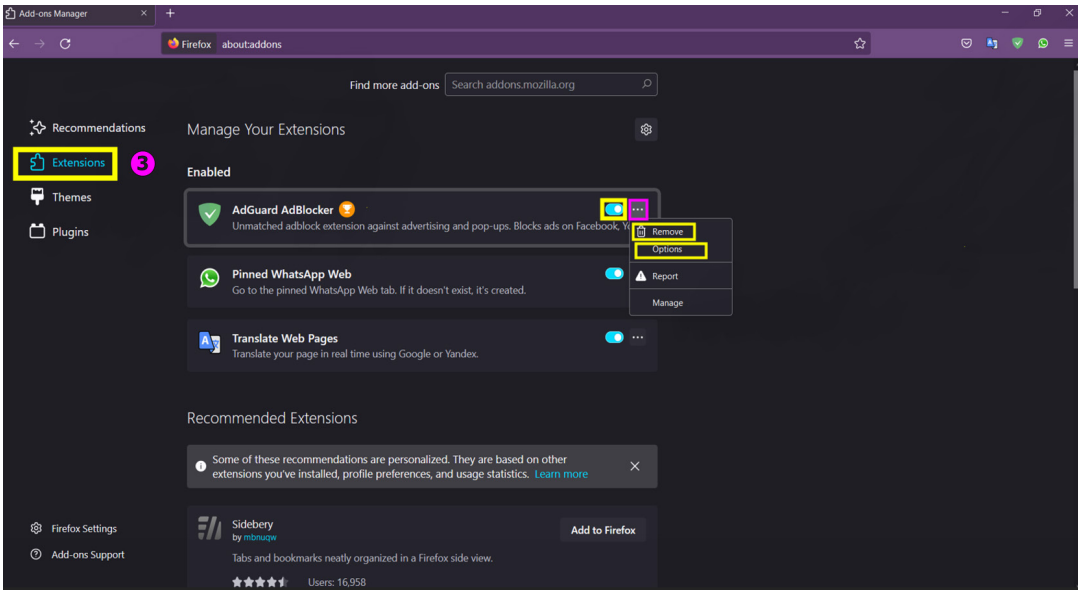
همان‌طور که در عکس روبرو مشخص است، می‌توان هر کدام از افزونه‌های مورد نظر را انتخاب کرد. برای فعال/غیرفعال‌کردن آن از دستگیره پایین سمت راست استفاده کرد. با استفاده از گزینه Details می‌توان جزئیات بیش‌تری را در خصوص افزونه مشاهده کرد و یا از نظر امنیتی آن را بررسی کرد. همچنین با استفاده از گزینه Remove می‌توان افزونه را حذف کرد.

بخش افزونه‌ها در مرورگر فایرفاکس

Firefox://Add-on and themes/Extensions



در بخش مربوط به Extension می‌توان لیستی از افزونه‌هایی
که در مرورگر نصب شده را مشاهده کرد.



در ادامه شش افزونه که در حوزه امنیت و فناوری اطلاعات استفاده می‌شوند مورد بررسی قرار گرفته‌اند.

Avast Online Security

این افزونه باعث افزایش کلی سطح امنیت مرورگر شما می‌شود، به‌علاوه اینکه با اسکن کامل صفحاتی که باز کرده‌اید و تشخیص اصل یا تقلبی بودن آن‌ها، به خوبی از حملات فیشینگ در امان خواهید بود. همچنین این افزونه به‌صورت خودکار آدرس URL وب‌سایت‌هایی که قصد بازدید از آن‌ها را دارید تصحیح می‌کند تا ناخواسته وارد وب‌سایت‌های اشتباه نشوید.
Avast Online Security از یک سیستم آزاد نظرسنجی برای وب‌سایت‌ها استفاده می‌کند تا وب‌سایت‌های اصلی و جعلی را به خوبی تفکیک کند؛ همچنین کوکی‌هایی که قصد ردیابی کاربر را دارند مسدود می‌کند تا کسی از محتوایی که شما در وب به دنبالش هستید، باخبر نشود.

WOT

با نصب این افزونه در مرورگر خود پس از مراجعه به هر وب‌سایتی نظر دیگر کاربران و توسعه‌دهندگان این سرویس را درباره آن سایت خواهید دید و درصورتی‌که در گذشته کد مخرب و یا تهدید دیگری گزارش شده باشد، شما نیز از این امر با خبر می‌شوید.

Click & Clean

این افزونه که وظیفهٔ اصلی آن پاکسازی است، تمام اطلاعات و آثار فعالیت‌های اینترنتی کاربر را تنها با یک کلیک پاک می‌کند که از آن جمله می‌توان به تاریخچه، کَش، کوکی‌ها، فلش کوکی‌ها، URL های ذخیره‌شده، فایل‌های موقت و غیره اشاره کرد. این افزونه یک برنامه‌ی ضد بدافزار نیز در خود گنجانده است که توسط BitDefender طراحی شده و سیستم شما را اسکن می‌کند تا شما را از حضور احتمالی بدافزارهای گوناگون در سیستم‌تان آگاه کند. خوبی دیگر این افرونه که تیر خلاصی برای رقبا می‌باشد این است که تا حد زیادی قابل شخصی‌سازی است. به‌طوری‌که می‌توانید تعیین کنید می‌خواهید چه فایل‌ها یا اطلاعاتی پاک شوند.

AdBlock Plus

AdBlock Plus یا ABP، افزونه‌ای است که می‌تواند به اکثر مرورگرهای وب اضافه شود. همان‌طور که از اسم این افزونه مشخص است، هدف آن مسدود کردن تبلیغات بوده و به‌طور موثری از نمایش آن‌ها در وب‌سایت‌هایی که کاربران بازدید می‌کنند جلوگیری می‌کند. برخلاف AdBlock سابق، ABP به‌صورت پیش‌فرض، فقط تبلیغات نفوذی و مزاحم را مسدود می‌کند، که این کار به سایت‌هایی که از طریق تبلیغات کسب درآمد می‌کنند، کمک می‌کند.

No-Script

افزونه No-Script امنیت بیشتری را برای مرورگر شما فراهم می‌کند. این افزونه اجازه می‌دهد تا کدهای جاوا اسکریپت (داخلی و خارجی) فقط توسط وب‌سایت‌های مورد اعتماد انتخابی شما اجرا شود. برخی از وب‌سایت‌ها به‌طور پیش‌فرض به لیست سفید اضافه می‌شوند، اما شما می‌توانید در هر زمان مواردی را اضافه یا حذف کنید.

Costomize google

این افزونه به شما اجازه می‌دهد تا ظاهر قسمت سرچ گوگل (google search) خود را با راه‌های مختلف مثل افزودن لینک‌هایی به دیگر ماشین‌های جستجو و محدودکردن تبلیغات، اصلاح کنید. همچنین از طریق این افزونه‌ها، پنهان کردن ID گوگل و پنهان‌کردن نتایج جستجو در گوگل نیز برای شما امکان‌پذیر است.

KURD
SIRT
مرکز آپا دانشگاه کردستان

مرکز آپا دانشگاه کردستان
cert.uok.ac.ir