فصل‌نامه تخصصی امنیت سایبری مرکز آپا دانشگاه کردستان
شماره دهم/ تابستان ۱۴۰۰

DIGITAL FORENSICS

- معرفی ابزار SN1PER
- مدیریت بحران بعد از حملات سایبری
- محافظت از فایل‌ها در برابر حملات باج افزاری
- ۲۵ پارامتر در بررسی آسیب‌پذیری‌های وب‌اپلیکیشن‌ها
- چک لیست بازبینی لاگ‌های حیاتی در رخدادهای امنیتی
- جرم‌شناسی USB - بازسازی شواهد دیجیتال از درایو USB

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
نویسندگان (به‌ترتیب مطالب):
علی کیائی‌فر/ محمد حبیبی/ هادی گلباغی
تینا احمدی/ نازیلا خسروی
+ با تشکر از علی کیائی‌فر (مدیر تحقیق و توسعه شرکت مدبران) و 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 QR کدها می‌توانید مستقیما به لینک‌ها منتقل شوید.

فهرست مطالب

مقاله‌های آموزشی

۰۲ مدیریت بحران بعد از حملات سایبری

۰۶ بررسی اکسپلویت‌های پرکاربرد سال ۲۰۲۰

۲۰ ۲۵ پارامتر در بررسی آسیب‌پذیری‌های وب‌اپلیکیشن‌ها

معرفی ابزار

۲۹ معرفی ابزار SN1PER

دفترچه تقلب

۴۳ چک لیست بازبینی لاگ‌های حیاتی در رخدادهای امنیتی

معرفی دوره

۴۸ معرفی دوره Complete Digital Forensics Masterclass

معرفی کتاب

۵۳ معرفی کتاب Network Forensics

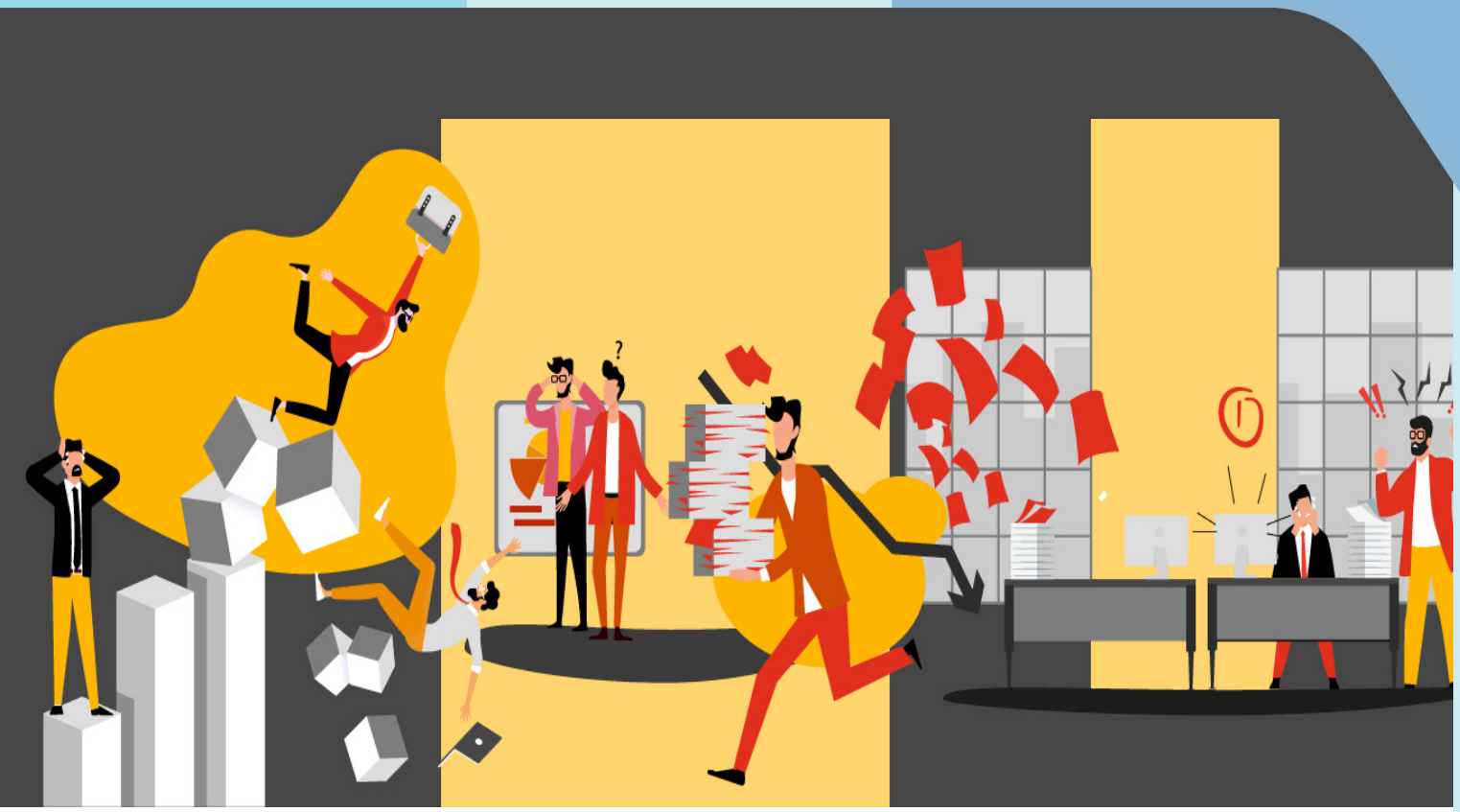
مقاله تحقیقاتی

۵۷ جرم‌شناسی USB - بازسازی شواهد دیجیتال از درایو USB

امنیت اطلاعات

۶۷ محافظت از فایل‌ها در برابر حملات باج افزاری

مقاله‌های آموزشی



مدیریت بحران بعد از حملات سایبری

علی کیائی‌فر

مقدمه

اخبار حملات سایبری به شرکت‌ها و سازمان‌ها به قدری زیاد شده که بخش ثابتی از اخبار روزانه را به خود اختصاص داده است. یکی از مهم‌ترین دلایل افزایش خبرهای هک و نفوذ به سازمان‌ها، این است که سرعت فرایند ارتقای امنیت سازمان‌ها بسیار کمتر از سرعت پیشرفت نفوذگران و هکرهاست.

در این نوشتار قصد نداریم در خصوص ارتقای امنیت سازمان‌ها بحث کنیم، بلکه می‌خواهیم با فرض بر اینکه هیچ سازمانی غیرقابل نفوذ و هک نیست به لحظات بحرانی یک سازمان بعد از وقوع نفوذ و دسترسی توجه کنیم.

همان‌قدر که داشتن استراتژی دفاعی برای هک نشدن یک سازمان مهم است، داشتن استراتژی بعد از وقوع حادثه نیز بسیار دارای اهمیت است.

اگر یک سازمان، استراتژی مناسبی برای بعد نفوذ نداشته باشد خسارات ناشی از وقوع حادثه در آن سازمان بسیار دامنه‌دارتر خواهد شد.

اجازه دهید با چند پرسش بحث را ادامه دهیم:

۱- اگر فردا راس ساعت ۱۰ صبح یک پیام تهدیدآمیز بر روی مانیتورهای کاربرانتان نقش ببندد اولین اقدام شما چیست؟

۲- اگر در اتاق سرور متوجه شوید که صدای فن‌های سرورها به طرز عجیب و غیرطبیعی زیاد شده است اولین اقدام شما چیست؟

۳- اگر متوجه شوید که یک کانال تلگرامی در حال آپلود کردن اسناد محرمانه سازمان شماست اولین اقدام شما چیست؟

٤- اگر متوجه شوید میزان آپلود در شبکه شما از یک پورت ناشناس به طرز عجیبی افزایش یافته است، اولین اقدام شما چیست؟

۵- اگر فردا به شما اطلاع دهند یک نفر در دارک‌وب ادعا کرده است که اطلاعات سازمان شما را برای فروش گذاشته است اولین اقدام شما چیست؟

٦- اگر متوجه شوید اصل داده‌ها و نسخه پشتیبان اطلاعات شما توسط یک باج‌افزار از بین رفته است، اولین اقدام شما چیست؟

۷- اگر فردا که به سازمان می‌روید متوجه شوید که تمام سیستم‌ها از دامنه سازمان جدا شده‌اند و اطلاعات سرورها هم به کلی پاک شده‌اند چه فرایندی را دنبال خواهید کرد؟

این اتفاق‌ها عجیب و غریب نیستند. برای خیلی از سازمان‌ها مشابه سازمان شما اتفاق افتاده است. از وزارتخانه گرفته تا یک شرکت خصوصی کوچک!

اگر سازمان شما استراتژی تعریف شده‌ای برای مدیریت بحران بعد از حملات سایبری را داشته باشد قطعا می‌تواند با مدیریت صحیح صحنه بحران از عواقب حملات بکاهد، اما تجربه نشان داده است که سیاست تدوین‌شده آنچنانی برای مدیریت بحران در حملات سایبری وجود ندارد. در هنگام بحران، مدیر شبکه بر اساس تشخیص خود عمل کرده و ممکن است سرورها را خاموش کرده و یا ارتباطات را قطع کند. از آن طرف هم چون مدیریت واحدی برای حل بحران وجود ندارد نهادهای بالادستی به موضوع ورود کرده و غالبا به بحران دامن می‌زنند.
درحالی‌که بعد از بحران، تمرکز تیم فنی باید به موضوعات فنی منعطف شود با ورود همزمان چندین نهاد بالادستی به ماجرا، مدیریت بحران پیچیده‌تر می‌شود. تیم فنی به‌جای تمرکز بر حل مشکلات، باید در لحظه پاسخگوی مدیران ارشد، حراست، افتا، پدافند غیرعامل و ... باشد.

لذا لازم است سازمان‌ها پیش از وقوع حوادث سایبری، این لحظات سخت را تمرین کنند و آماده باشند و استراتژی مدیریت صحنه بحران را برای سازمان‌شان تعریف و تدوین کنند.
استراتژی سازمان برای مدیریت صحنه بعد از هر نوع حمله باید مشخص باشد.
به‌عنوان‌مثال آن استراتژی که برای مدیریت صحنه بعد از حملات باج‌افزاری اتخاذ می‌شود برای حملات نشت اطلاعات، کاربردی ندارد. همچنین این استراتژی‌ها می‌توانند سازمان به سازمان متفاوت باشند.

مثال

در ادامه یک مثال از استراتژی‌های نمونه پیشنهادی را با هم مرور می‌کنیم.
این استراتژی‌ها باعث رفع خسارات حمله نمی‌شوند بلکه از ادامه حمله جلوگیری کرده و باعث مدیریت بحران می شوند.

نوع حادثه

نشت داده‌ها: اطلاعات محرمانه یکی از سرورها در یک کانال تلگرامی در حال انتشار است.

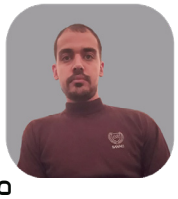
اقدامات لازم

- دسترسی به سروری که اطلاعاتش در حال انتشار است را از همه جا قطع کنید.
- با افراد متخصص و یا مشاوران امنیت سازمان تماس بگیرید.
- موضوع را به نهادهای متولی بالاسری اطلاع دهید. (افتا، پدافندغیرعامل، مرکز ماهر و ... . توجه به این نکته ضروری است که فقط به نهادی اطلاع دهید که متولی سازمان شماست. اطلاع به همه نهادها می‌تواند خود به چالشی پیچیده‌تر در صحنه بحران تبدیل شود!)
- تلفن‌های خود را قطع کنید و بر روی کار خود تمرکز کنید و به هیچ تماسی پاسخ ندهید. فقط یک نفر را به عنوان سخنگو، مسئول پاسخگویی به دیگران و نهادهای بالاسری در نظر بگیرید.
- به ذینفعان اطلاعات نشت شده یا لو رفته اطلاع دهید تا درصورت لزوم برای حفاظت از منافع خودشان اقدامات امنیتی را انجام دهند. (مثلاً حساب بانکی خود را مسدود کرده و یا برخی گذرواژه‌ها را تغییر دهند.)
- منشأ نفوذ را شناسایی کنید. (منشا نفوذ می‌تواند افراد یا آسیب‌پذیری‌ها باشند.)
- راهکارهای امنیتی خود را ارتقا دهید. این حمله و نفوذ نشان داده است که سیستم دفاعی شما ضعف‌هایی دارد.
- گزارش حمله را کامل کنید و آن را با دیگران به اشتراک بگذارید تا همه از این حمله درس بگیرند.

همان‌گونه که گفته شد این استراتژی‌ها می توانند در سازمان‌های مختلف متفاوت باشند. مهم این است که بعد از هر حادثه، دستورالعمل مشخص و تمرین شده‌ای داشته باشیم و در صحنه بحران غافلگیر نشویم.

هشدار AA21-209A

بررسی اکسپلویت‌های پرکاربرد سال ۲۰۲۰



محمد حبیبی

مقدمه

این مشاوره امنیت‌سایبری حاصل همکاری سازمان‌های FBI, ACSC, CISA و NCSC می‌باشد. در این مشاوره امنیتی جزئیات ۳۰ آسیب‌پذیری برتر از سال ۲۰۲۰ تا کنون که به صورت گسترده و مرتباً توسط مهاجمین مورد استفاده قرار گرفته است، آورده شده است.

مهاجمین سایبری همچنان آسیب‌پذیری‌های برنامه‌هایی که به صورت عمومی شناخته شده و اغلب تاریخ‌دار هستند را برای حمله به اهداف گسترده شامل سازمان‌های دولتی و خصوصی در سراسر جهان، استفاده می‌کنند. هرچند که کاربران در سراسر جهان می‌توانند با اعمال وصله‌های امنیتی منتشر شده بر روی سیستم خود یا استفاده از سیستم‌های مدیریت مرکزی وصله‌های امنیتی مانند Syxsense، NinjaRMM، Atera و ... آسیب‌پذیری‌های ذکر شده در این گزارش را به صورت خودکار وصله نمایند.

نکات کلیدی

در سال ۲۰۲۰ مهاجمان سایبری از آسیب‌پذیری‌هایی که اخیراً کشف شده بودند، برای حمله به سیستم‌هایی که به‌روزرسانی‌های امنیتی بر روی آن‌ها اعمال نشده بود، استفاده کردند. براساس داده‌های در دسترس دولت آمریکا اکثر آسیب‌پذیری‌هایی که در سال ۲۰۲۰ استفاده شده‌اند طی دو سال اخیر افشا گردیده‌اند.

بهره‌برداری مهاجمین سایبری از مشکلات نرم‌افزاریِ اخیراً افشا شده در سال ۲۰۲۰ احتمالاً ریشه در افزایش دورکاری مشاغل به دلیل پاندمی ویروس COVID-19 بوده است. تغییرات سریع و افزایش گزینه‌های دورکاری مانند استفاده از شبکه‌های خصوصی مجازی (VPN) و محیط‌های مبتنی بر اَبر احتمالاً بار اضافی را بر دوش مدافعان سایبری قرار می‌دهد که برای نگه‌داری و فرایندهای روتین مربوط به وصله امنیتی نرم‌افزارها در تلاشند.

چهار مورد از آسیب‌پذیری‌هایی که بیشترین استفاده را داشته‌اند مربوط به محیط‌های دورکاری، VPNها و تکنولوژی‌های مبتنی بر اَبر بوده است. بسیاری از دستگاه‌های gateway شبکه‌های VPN در طول سال ۲۰۲۰ وصله نشده باقی ماندند که این امر می‌تواند به دلیل افزایش گزینه‌های دورکاری برای سازمان‌ها باشد.

سازمان‌های NCSC، ACSC، CISA و FBI آسیب‌پذیری‌های جدول زیر را به‌عنوان پر استفاده‌ترین آسیب‌پذیری‌ها که توسط مهاجمین سایبری در سال ۲۰۲۰ استفاده شده‌اند، معرفی کرده‌اند.

Vendor	CVE	Type
Citrix	CVE-2019-19781	arbitrary code execution
Pulse	CVE 2019-11510	arbitrary file reading
Fortinet	CVE 2018-13379	path traversal
F5- Big IP	CVE 2020-5902	remote code execution (RCE)
MobileIron	CVE 2020-15505	RCE
Microsoft	CVE-2017-11882	RCE
Atlassian	CVE-2019-11580	RCE
Drupal	CVE-2018-7600	RCE
Telerik	CVE 2019-18935	RCE
Microsoft	CVE-2019-0604	RCE
Microsoft	CVE-2020-0787	elevation of privilege
Netlogon	CVE-2020-1472	elevation of privilege

آسیب‌پذیری‌های سال ۲۰۲۱

علاوه‌بر آسیب‌پذیری‌های سال ۲۰۲۰ که قبلاً اشاره شد، سازمان‌ها نیاز است اعمال وصله‌های امنیتی برای آسیب‌پذیری‌های زیر را نیز در اولویت قرار بدهند.

- Microsoft Exchange: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065
- Pulse Secure: CVE-2021-22893, CVE-2021-22894, CVE-2021-22899, and CVE-2021-22900
- Accellion: CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, CVE-2021-27104
- VMware: CVE-2021-21985
- Fortinet: CVE-2021-13379, CVE-2020-12812, and CVE-2019-5591

راهکارهای کاهش خطرات و شاخص‌گذاری آن‌ها

یکی از موثرترین اقداماتی که در زمینه کاهش خطر اغلب آسیب‌پذیری‌ها شناخته شده است، به‌روزرسانی نسخه‌ی نرم‌افزارها است زمانی که وصله‌ی آن‌ها منتشر می‌شود. اگر این فرایند امکان‌پذیر نیست، در صورت ارائه توسط ارائه دهنده (vendor)، راه‌حل‌های موقت استفاده شود. اگر یک سازمان نتواند تمامی برنامه‌ها را پس از انتشار وصله‌ها به‌روزرسانی نماید، می‌تواند اعمال وصله‌های امنیتی را برای CVE هایی که قبلاً از آن‌ها بهره‌برداری شده است، بر روی سرورهایی که برای تعداد بالایی از مهاجمین احتمالی قابل دسترس است، در اولویت قرار دهد.

این مشاوره امنیتی به آسیب‌پذیری‌هایی که نیاز است در اولویت قرار گیرد توجه بیشتری دارد. توصیه می‌شود در صورت امکان به‌روزرسانی خودکار نرم‌افزارها را فعال کنید. تمرکز بر منابع محدود دفاع سایبری در اعمال وصله‌های امنیتی برای آسیب‌پذیری‌هایی که مهاجمین سایبری بیشترین استفاده را از آن‌ها کرده‌اند، باعث تقویت پتانسیل امنیت شبکه شده و در عین حال مانع حملات مهاجمین می‌شود. برای مثال APT های دولتی در سال ۲۰۲۰ به‌صورت گسترده به یک آسیب‌پذیری اجرای کد از راه دور(RCE) کشف شده در Atlassian Crow با شناسه آسیب‌پذیری CVE-2019-11580 وابسته بودند. تمرکز بر روی اعمال وصله امنیتی برای این آسیب‌پذیری می‌تواند بسیار تاثیرگذار باشد و باعث شود مهاجمین به دنبال یک آسیب‌پذیری جایگزین باشند که ممکن است کاربرد گسترده‌ای برای مجموعه هدف خود نداشته باشد و در نتیجه سطح حمله محدودتر شود.

علاوه‌براین مهاجمین معمولاً از فرایندهای احراز هویت ضعیف به‌ویژه در دستگاه‌هایی که خارج از شبکه سازمان در دسترس هستند استفاده می‌کنند. سازمان‌ها نیاز است برای دسترسی به منابع و سرویس‌های داخلی، خارج از شبکه سازمان، خصوصاً برای دسترسی به حساب کاربری مدیر یا سایر حساب‌های کاربری با سطح دسترسی بالا از احراز هویت‌های چند مرحله‌ای استفاده کنند.

بررسی آسیب‌پذیری‌های ۲۰۲۰

در این بخش به بررسی آسیب‌پذیری‌هایی که بیشترین بهره‌برداری از آن‌ها در سال ۲۰۲۰ اتفاق افتاده است می‌پردازیم، همچنین خانواده بدافزارهایی که از این آسیب‌پذیری‌ها استفاده کرده‌اند، در بخش مربوطه آورده شده است.

عنوان و شناسه	Citrix Netscaler Directory Traversal (CVE-2019-19781)
توضیحات آسیب‌پذیری	Citrix Netscaler Application Delivery Control (ADC) به‌دلیل کنترل‌های دسترسی ضعیف نسبت به حملات اجرای RCE و Directory traversal آسیب‌پذیر است و می‌تواند باعث به خطر افتادن کل سیستم شود.
حساسیت	بحرانی (CVSS 3.0)
بررسی آسیب‌پذیری	نبود کنترل‌های دسترسی کافی، امکان مشاهده دایرکتوری‌های سیستم برای پیدا کردن کد آسیب‌پذیر (directory traversal) را به مهاجم می‌دهد، در این مثال Citrix ADC دارای یک اسکریپت پرل آسیب‌پذیر به‌نام newbm.pl است که وقتی برای آن درخواست HTTP با متد پست به URL زیر ارسال می‌شود: POST https://$TARGET/vpn/../vpn/portal/scripts/newbm.pl اجازه اجرای فرمان در سیستم‌عامل محلی را می‌دهد. مهاجم با استفاده از این عملکرد می‌تواند یک ابزار command and control (C2) یا reverse-shell را بر روی سیستم هدف آپلود و اجرا نماید با استفاده از دستورات تعبیه شده (e.g., curl, wget, Invoke-WebRequest) به دسترسی غیرمجاز به سیستم عامل برسد.

خانواده بدافزاری	چندین کمپین بدافزاری شامل NOTROBIN از این آسیب‌پذیری استفاده کرده‌اند.
وصله امنیتی	در این لینک مشاهده شود.
راه حل کاهش تهدید	به‌روزرسانی‌ها و اقدامات لازم با توجه به جزئیات آسیب‌پذیری ارائه شده انجام شود. جستجو کنید: Citrix: Mitigation Steps for CVE-02019-19781
نحوه تشخیص	۱- CISA یک ابزار رایگان برای تشخیص این آسیب‌پذیری طراحی کرده که از لینک قابل دسترس است: https://github.com/cisagov/check-cve-2019-19781 ۲- Nmap یک اسکریپت برای تشخیص این آسیب‌پذیری طراحی کرده است که در لینک زیر قابل دسترس است: https://github.com/nmap/nmap/pull/1893/files ۳- Citrix نیز یک ابزار رایگان برای تشخیص این آسیب‌پذیری طراحی کرده است که از لینک زیر قابل دسترس می‌باشد: https://github.com/citrix/ioc-scanner-CVE-2019-19781
تکنولوژی و نسخه آسیب‌پذیر	Citrix ADC and Gateway 12.1 ,12.0 ,11.1 ,10.5, and 3.01
منابع	برای اطلاعات بیشتر به لینک‌های زیر مراجعه کنید:

عنوان و شناسه	Pulse Secure Connect VPN (CVE-2019-11510)
توضیحات آسیب‌پذیری	Pulse Secure Connect دارای آسیب‌پذیری arbitrary file disclosure می‌باشد و مهاجم با بهره‌برداری از این آسیب‌پذیری می‌تواند به اطلاعات حساس مدیر شامل نام‌کاربری، گذرواژه دسترسی پیدا کند.
حساسیت	بحرانی (CVSS 3.0)
بررسی آسیب‌پذیری	عدم وجود کنترل‌های سطح دسترسی مناسب، باعث به‌وجود آمدن آسیب‌پذیری directory traversal شده است که مهاجم می‌تواند با بهره‌برداری از آن محتویات فایل‌های سیستمی را بخواند. برای مثال مهاجم می‌تواند از درخواستی به شکل زیر برای خواندن فایل گذرواژه‌ها از سیستم استفاده کند: https://sslvpn.insecure-org.com/dana-na/../dana/html5/acc/guacmole/../../../../../../etc/passwd?/dana/html5/guacamole/
خانواده بدافزاری	چندین کمپین بدافزاری از این آسیب‌پذیری استفاده کرده‌اند که قابل‌توجه‌ترین آن‌ها باج‌افزار REvil/Sodinokibi بوده است.
وصله امنیتی	در این لینک مشاهده شود.
راه حل کاهش تهدید	۱- Pulse Secure VPN را به آخرین نسخه ارتقا دهید. ۲- مراقب scheduled tasks هایی که برای فایل/فایل اجرایی ناشناس تعریف شده‌اند،باشید. ۳-یک مکانیزم برای تشخیص یا جلوگیری از حملات directory traversal که سعی بر خواندن فایل‌های سیستمی می‌کند، تهیه و اجرا شود.
نحوه تشخیص	۱- CISA یک ابزار برای تشخیص این آسیب‌پذیری طراحی کرده که از مخزن زیر قابل دسترس است. https://github.com/cisagov/check-your-pulse ۲- Nmap نیز یک اسکریپت برای تشخیص این آسیب‌پذیری طراحی کرده است: https://github.com/nmap/nmap/pull/1708
تکنولوژی و نسخه آسیب‌پذیر	Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R8.3 ,12.1 before 8.3R7.1, and 9.0 before 9.0R3.4 are vulnerable.
منابع	برای اطلاعات بیشتر به لینک‌های زیر مراجعه شود:

عنوان و شناسه	F5 Big IP Traffic Management User Interface (CVE-2020-5902)
توضیحات آسیب‌پذیری	The Traffic Management User Interface (TMUI) یک آسیب‌پذیری اجرای کد از راه دور (RCE) در صفحات افشا نشده دارد.
حساسیت	بحرانی (CVSS 3.0)
بررسی آسیب‌پذیری	این آسیب‌پذیری به مهاجمی که احراز هویت نشده و به Configuration Utility دسترسی شبکه دارد، اجازه اجرای فرمان سیستمی دلخواه (execute arbitrary system commands)، ساخت یا حذف فایل، غیرفعال‌کردن سرویس‌ها و اجرای کد دلخواه جاوا را می‌دهد. این آسیب‌پذیری می‌تواند باعث به خطر افتادن کل سیستم شود. سیستم‌های BIG-IP در مد Appliance نیز آسیب‌پذیر هستند. این مشکل در data plane نمایش داده نمی‌شود و فقط control plane از آن تاثیر می‌گیرد.
خانواده بدافزاری	----
وصله امنیتی	در این لینک مشاهده شود.
راه حل کاهش تهدید	دانلود و نصب اخرین نسخه نرم‌افزاری اصلاح شده توسط ارائه دهنده
نحوه تشخیص	۱- F5 یک ابزار رایگان برای تشخیص این آسیب‌پذیری ارائه کرده است که از مخزن زیر قابل دسترس است. https://github.com/f5devcentral/cve-2020-5902-ioc-bigip-checker/ ۲- بررسی دستی نسخه نرم‌افزار برای بررسی اینکه آیا آسیب‌پذیر است یا خیر.
تکنولوژی و نسخه آسیب‌پذیر	BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO, CGNAT) ,15.0.1-15.0.0 ,15.1.0 12.1.5-12.1.0 ,13.1.3-13.1.0 ,14.1.2-14.1.0, and 11.6.5-11.6.1 are vulnerable.
منابع	برای اطلاعات بیشتر به منابع زیر مراجعه کنید:

عنوان و شناسه	Fortinet FortioOS Secure Socket Layer VPN (CVE-2018-13379)
توضیحات آسیب‌پذیری	Fortinet Secure Sockets Layer (SSL) VPN نسبت به حملات unauthenticated directory traversal آسیب‌پذیر است که به مهاجم اجازه می‌دهد به فایل sslvpn_ websession دسترسی پیدا کند. سپس مهاجم به نام‌کاربری و گذرواژه‌ها به‌صورت متن واضح و رمزگذاری نشده دسترسی پیدا می‌کند.
حساسیت	بحرانی (CVSS 3.0)
بررسی آسیب‌پذیری	ضعف در کنترل سطح دسترسی کاربر و ساختار دایرکتوری‌های برنامه کاربری وب، به مهاجم امکان خواندن یک فایل سیستمی بدون احراز هویت را می‌دهد. به‌عنوان مثال مهاجم می‌تواند در خواست HTTP زیر را با متد GET ارسال کند: http://$SSLVPNTARGET?lang=/../../../../////////dev/cmdb/sslvpn_ websession پاسخ سرور به این درخواست، نمایش credential (نام کاربری و گذرواژه) کاربران به صورت غیرقابل چاپ / فرمت Hex می‌باشد.
خانواده بدافزاری	چندین کمپین بدافزاری از این آسیب‌پذیری استفاده می‌کنند که قابل توجه‌ترین آن‌ها باج‌افزار Cring (شناخته شده با عناوین Crypt3، Vjszy1lo، Phantom، Ghost) می‌باشد.
وصله امنیتی	در این لینک مشاهده شود.
راه حل کاهش تهدید	۱- به‌روزرسانی به آخرین نسخه منتشر شده ۲- بررسی تمامی اخطارهایی که مربوط به یک unscheduled tasks یا یک فایل/ فایل اجرایی ناشناس می‌باشد. ۳- ساخت یک مکانیزم امنیتی برای تشخیص و جلوگیری از حملات directory traversal که سعی به خواندن فایل sslvpn_websessions می‌کنند.
نحوه تشخیص	اسکریپت‌های متفاوت تشخیص این آسیب‌پذیری برای Nmap طراحی شده است، مانند موارد زیر:
تکنولوژی و نسخه آسیب‌پذیر	Fortinet FortiOS 6.0.0 to 5.6.3 ,6.0.4 to 5.6.7, and 5.4.6 to 5.4.12 are vulnerable.
منابع	برای اطلاعات بیشتر به لینک‌های زیر مراجعه شود:

عنوان و شناسه	Microsoft Exchange Memory Corruption (CVE-2020-0688)
توضیحات آسیب‌پذیری	نرم‌افزار Microsoft Exchange به‌دلیل عدم مدیریت صحیح اشیاء در حافظه نسبت به حملات اجرای کد از راه دور آسیب‌پذیر است.
حساسیت	بحرانی (CVSS 3.0)
بررسی آسیب‌پذیری	این آسیب‌پذیری زمانی رخ می‌دهد که Microsoft Exchange Server در زمان نصب نمی‌تواند به درستی کلیدهای منحصر به‌فرد (unique keys) را ایجاد کند، یک کاربر احراز هویت شده که کلید اعتبارسازی (validation key) و یک mailbox را دارد، ممکن است یک شیء دستکاری شده برای deserialization به سمت برنامه‌کاربردی وب ارسال کند، برنامه ای که با سطح دسترسی SYSTEM در حال اجرا است و در نتیجه با بهره‌برداری موفق از این آسیب‌پذیری، مهاجم می‌تواند به سطح دسترسی SYSTEM در سرور دسترسی پیدا کند. به‌روزرسانی امنیتی منتشر شده برای این آسیب‌پذیری چگونگی ساخت unique keys در زمان نصب Microsoft Exchange را اصلاح می‌کند
خانواده بدافزاری	چندین APT حکومتی از این آسیب‌پذیری برای حمله به دولت‌ها و بخش‌های خصوصی در سرار جهان استفاده کرده‌اند.
وصله امنیتی	در این لینک مشاهده شود.
راه حل کاهش تهدید	دانلود و نصب نسخه نرم‌افزار اصلاح شده از طرف ارائه دهنده
نحوه تشخیص	۱- بررسی دستی نسخه نرم‌افزار نصب شده برای بررسی اینکه آیا آسیب‌پذیر است یا خیر ۲-این آسیب‌پذیری عموماً برای نصب WebShell ها استفاده شده است. پس توصیه می‌شود علاوه‌بر رفع آسیب‌پذیری موارد زیر مطالعه شود: https://media.defense.gov/2020/Jun/0/1-/1-/2002313081/09/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE20200422-.PDF https://github.com/nsacyber/Mitigating-Web-Shells
تکنولوژی و نسخه آسیب‌پذیر	Microsoft Exchange Server 2019 Cumulative Update 3 and 2016 ,4 Cumulative Update 14 and 2013 ,15 Cumulative Update 23, and 2010 Service Pack 3 Update Rollup 30 are vulnerable.
منابع	برای اطلاعات بیشتر به منابع زیر مراجعه کنید:

عنوان و شناسه	MobileIron Core & Connector (CVE-2020-15505)
توضیحات آسیب‌پذیری	محصولات MobileIron شامل Sentry، Core & Connector و Monitoring and Reporting Database (RDB) نسبت به حملات اجرای کد از راه دور (RCE) با بردارهای نامشخص آسیب‌پذیر هستند.
حساسیت	بحرانی (CVSS 3.0)
بررسی آسیب‌پذیری	آسیب‌پذیری با شناسه CVE-2020-15505، از نوع اجرای کد از راه دور می‌باشد که در MobileIron Core & Connector نسخه 10.3 به قبل وجود دارد. این آسیب‌پذیری به یک مهاجم خارجی اجازه می‌دهد بدون دسترسی، یک کد را بر روی سیستم آسیب‌پذیر اجرا کند. از آنجا که سیستم‌های mobile device management (MDM) برای مدیریت پیکربندی دستگاه‌های خارجی بسیار حیاتی هستند، یک هدف ارزشمند برای مهاجمین به حساب می‌آیند.
خانواده بدافزاری	چندین APT برای گرفتن دسترسی غیر مجاز از این آسیب‌پذیری استفاده کرده‌اند.
وصله امنیتی	در این لینک مشاهده شود.
راه حل کاهش تهدید	دانلود و نصب آخرین نسخه‌های اصلاح شده نرم‌افزار
نحوه تشخیص	ابزار خاصی در این زمینه طراحی نشده است، به‌صورت دستی نسخه نرم‌افزار استفاده شده خود را بررسی کنید تا مشخص شود آسیب‌پذیر است یا خیر.
تکنولوژی و نسخه آسیب‌پذیر	MobileIron Core & Connector versions 10.3.0.3 and earlier, ,10.4.0.0 10.5.2.0 ,10.5.1.0 ,10.4.0.3 ,10.4.0.2 ,10.4.0.1, and 10.6.0.0; Sentry versions 9.7.2 and earlier and 9.8.0; and Monitor and Reporting Database (RDB) version 2.0.0.1 and earlier are vulnerable.
منابع	برای اطلاعات بیشتر به لینک‌های زیر مراجعه کنید:

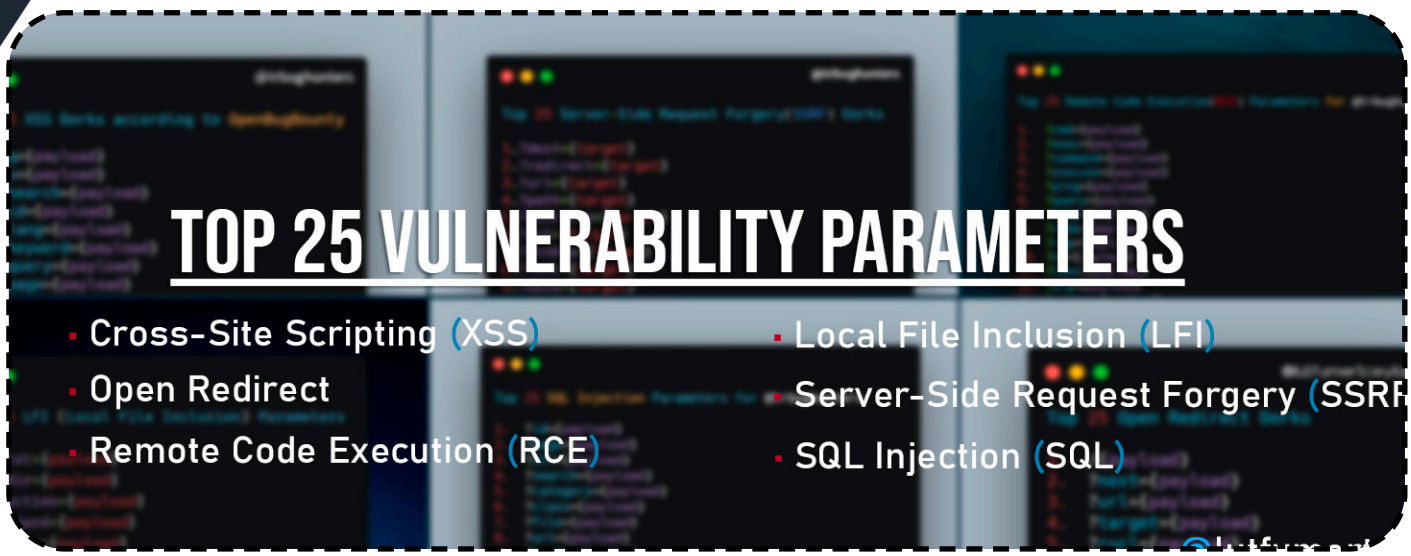
عنوان و شناسه	Microsoft Office Memory Corruption (CVE-2019-11882)
توضیحات آسیب‌پذیری	مایکروسافت آفیس مستعد به آسیب‌پذیری memory corruption است که به مهاجم اجازه اجرای کد دلخواه را می‌دهد. مهاجمین سایبری همچنان از این آسیب‌پذیری چهار ساله در مایکروسافت آفیس بهره‌برداری می‌کنند که در این میان دولت ایالات متحده مورد بیشترین حملات قرار گرفته است.
حساسیت	بحرانی (CVSS 3.0)
بررسی آسیب‌پذیری	Microsoft Equation Editor که یکی از کامپونت‌های مایکروسافت آفیس است، یک آسیب‌پذیری سر ریز بافر دارد که باعث اجرای کد از راه دور در سیستم آسیب‌پذیر می‌شود. این کامپونت در ۹ نوامبر سال ۲۰۰۰ کامپایل شده است. بدون هیچگونه ترکیب مجدد این کامپونت در تمامی نسخه‌های آفیس پشتیبانی می‌شود. Microsoft Equation Editor یک COM server خارج از پروسه است که توسط exe.eqnedt32 میزبانی می‌شود، به این معنی که به‌عنوان پروسه خود اجرا می‌شود و می‌تواند فرامینی را از سایر پروسه‌ها دریافت کند. مکانیزم‌های Data execution prevention و address space layout randomization (ASLR) می‌توانند در برابر این نوع حملات از سیستم آسیب‌پذیر محافظت نمایند.
خانواده بدافزاری	چندین کمپین جاسوسی سایبری از این آسیب‌پذیری استفاده کرده‌اند. CISA عنوان‌کرده است که بدافزار LokiBot نیز از این آسیب‌پذیری بهره‌برداری کرده است.
وصله امنیتی	در این لینک مشاهده شود.
راه حل کاهش تهدید	۱- برای رفع این مشکل، مدیران نیاز است وصله‌های امنیتی منتشر شده توسط مایکروسافت در این لینک را بر روی سیستم‌های خود اعمال نمایند. ۲- افرادی که نمی‌توانند این وصله‌های امنیتی را اعمال نمایند، می‌توانند Equation Editor را غیرفعال کنند. برای اطلاعات بیشتر به این لینک مراجعه شود.
نحوه تشخیص	ابزارهای امنیتی ویندوز شامل Windows Defender، Microsoft Defender Antivirus، Microsoft Security Essentials و Microsoft Safety Scanner همگی این آسیب‌پذیری را تشخیص و رفع می‌کنند.
تکنولوژی و نسخه آسیب‌پذیر	Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 are vulnerable.
منابع	برای اطلاعات بیشتر به منابع زیر مراجعه کنید:

عنوان و شناسه	WebDAV vulnerability (CVE-2019-3396)
توضیحات آسیب‌پذیری	Atlassian Confluence Server و Data Center Widget Connector نسبت به حمله سمت سرور template injection آسیب‌پذیر هستند.
حساسیت	بحرانی (CVSS 3.0)
بررسی آسیب‌پذیری	موارد عنوان شده یعنی Confluence Server و دیتاسنترهایی که قبل از تاریخ ۱۸ ژوئن ۲۰۱۸ عرضه شده‌اند نسبت به این مشکل آسیب‌پذیر هستند. مهاجم می‌تواند با بهره‌برداری از آسیب‌پذیری server-side request forgery یا به اختصار SSRF در پلاگین WebDAV یک درخواست HTTP دستکاری‌شده ارسال کند. حمله موفقیت آمیز این آسیب‌پذیری به مهاجم امکان انجام حملات side template injection، path traversal و اجرای کد از راه دور در سیستم آسیب‌پذیر را می‌دهد.
خانواده بدافزاری	چندین کمپین بدافزاری از این آسیب‌پذیری استفاده کرده‌اند که قابل توجه‌ترین آن‌ها باج‌افزار GandCrab بوده است.
وصله امنیتی	----
راه حل کاهش تهدید	دانلود و نصب آخرین نسخه نرم‌افزار اصلاح شده توسط ارائه دهنده
نحوه تشخیص	بررسی دستی نسخه نرم‌افزار استفاده شده برای اینکه آسیب‌پذیر بودن آن تشخیص داده شود.
تکنولوژی و نسخه آسیب‌پذیر	All versions of Confluence Server and Confluence Data Center before version 6.6.12, from version 6.7.0 before 6.12.3 (the fixed version for 6.12.x), from version 6.13.0 before 6.13.3 (the fixed version for 6.13.x), and from version 6.14.0 before 6.14.2 (the fixed version for 6.14.x) are vulnerable.
منابع	برای اطلاعات بیشتر به منابع زیر مراجعه کنید:

عنوان و شناسه	Telerik UI for ASP.NET AJAX Insecure Deserialization (CVE-2019-18935)
توضیحات آسیب‌پذیری	Telerik User Interface مربوط به ASP.NET به‌صورت صحیح ورودی‌های سریال‌سازی شده را برای موارد خطرناک فیلتر نمی‌کند. نسخه‌های قبل از ۲۰۲۰ R1 (۲۰۲۰٫۱٫۱۱٤) نسبت به حملات اجرای کد از راه دور در وب‌سرور مورد هدف، آسیب‌پذیر هستند.
حساسیت	بحرانی (CVSS 3.0)
بررسی آسیب‌پذیری	The Telerik UI به‌درستی ورودی‌های سریال‌سازی شده را فیلتر نمی‌کند. این آسیب‌پذیری می‌تواند باعث حملات اجرای کد از راه دور و به خطر افتادن کل سیستم شود. پارامتر آسیب‌پذیر rauPostData که از طریق متد HTTP POST به سمت سرور ارسال می‌شود از تابع آسیب‌پذیر AsyncUploadHandler استفاده می‌کند، این تابع یا شیء از متد JavaScriptSerializer.Deserialize() استفاده می‌کند و این متد به‌درستی مقدار ورودی سریال‌سازی شده را هنگام فرایند deserialization فیلتر و پاکسازی نمی‌کند.
خانواده بدافزاری	دو کمپین بدافزاری Netwalker Ransomware و Blue Mockbird Monero Cryptocurrency-mining از این آسیب‌پذیری استفاده کرده‌اند.
وصله امنیتی	در این لینک مشاهده شود.
راه حل کاهش تهدید	به‌روزرسانی Telerik UI به آخرین نسخه ارائه شده (حداقل 2020.1.114 و بالاتر)
نحوه تشخیص	۱- ACSC یک اسکریپت پاورشل برای تشخیص DLLs های آسیب‌پذیر Telerik UI در میزبان‌های ویندوز سرور دارد. ۲- میزبان‌های آسیب‌پذیر باید برای وجود شواهد بهره‌برداری از این آسیب‌پذیری بررسی شوند. شواهد بهره‌برداری از این آسیب‌پذیری ممکن است در لاگ درخواست‌های HTTP مربوط به IIS یا Application Windows event log پیدا شوند. ۳- بهره‌برداری از این آسیب‌پذیری و آسیب‌پذیری قبلی Telerik UI معمولاً منجر به بارگذاری web shell malware بر روی میزبان آسیب‌پذیر بوده است.
تکنولوژی و نسخه آسیب‌پذیر	Telerik UI for ASP.NET AJAX versions prior to 2020.1.14 R1 are affected.
منابع	برای اطلاعات بیشتر به منابع زیر مراجعه کنید:

عنوان و شناسه	Drupal Core Multiple Remote Code Execution (CVE-2018-7600)
توضیحات آسیب‌پذیری	نسخه‌های 7.58، 8.x، قبل از 8.3.9، قبل از 8.4.6 و قبل از 8.5.1 به مهاجم امکان اجرای کد دلخواه از راه دور را می‌دهد، زیرا که این مشکل بر روی چندین subsystems با پیکربندی‌های پیش‌فرض یا متداول تاثیرگذار است.
حساسیت	بحرانی (CVSS 3.0)
بررسی آسیب‌پذیری	آسیب‌پذیری اجرای کد از راه دور در چندین subsystems مربوط به Drupal نسخه 7.x و 8.x وجود دارد، این مسئله باعث می‌شود که مهاجم چندین بردار حمله برای سایت‌هایی که از سیستم مدیریت محتوای Drupal استفاده می‌کنند، داشته باشد که باعث به‌خطر افتادن کل سایت می‌شود. اکسپلویت ناموفق این آسیب‌پذیری ممکن است باعث از دسترس خارج شدن سرویس شود.
خانواده بدافزاری	کمپین‌های بدافزاری شامل Muhstik botnet و XMRig Monero Cryptocurrency mining از این آسیب‌پذیری استفاده کرده‌اند.
وصله امنیتی	در این لینک مشاهده شود.
راه حل کاهش تهدید	ارتقاء نسخه نرم‌افزار به آخرین نسخه ارائه شده Drupal7 یا core8
نحوه تشخیص	برای تشخیص این آسیب‌پذیری آقای Dan Sharvit یک ابزار طراحی که است که از طریق مخزن زیر قابل دسترس است. https://github.com/sl4cky/CVE-7600-2018-Masschecker/blob/master/Drupalgeddon-mass.py
تکنولوژی و نسخه آسیب‌پذیر	Drupal versions before 8 ,7.58.x before 8.4 ,8.3.9.x before 8.4.6, and 8.5.x before 8.5.1 are affected.
منابع	برای اطلاعات بیشتر به منابع زیر مراجعه کنید:

عنوان و شناسه	Microsoft SharePoint Remote Code Execution (CVE-2019-0604)
توضیحات آسیب‌پذیری	این آسیب‌پذیری در کامپونت XML deserialization در Microsoft SharePoint وجود دارد، که به مهاجم امکان اجرای کد دلخواه از راه دور در سرور Microsoft SharePoint را می‌دهد.
حساسیت	بحرانی (CVSS 3.0)
بررسی آسیب‌پذیری	بهره‌برداری از این آسیب‌پذیری معمولاً منجر به نصب وب‌شل بر روی میزبان آسیب‌پذیر می‌شود. وب‌شل می‌تواند در هر مسیر مرتبط با IIS قرار داده شود و نیازی به انجام احراز هویت ندارد. این وب‌شل‌ها معمولاً در دایرکتوری Layouts در مسیر زیر قرار میگیرند: C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\<version_number>\Template\Layouts متد xmlSerializer.Deserialize() به‌درستی ورودی‌های کاربر را که از تابع PickerEnitity/ValidateEnity (picker.aspx) دریافت شده است، فیلتر و پاکسازی نمی‌کند. زمانی که پیلود XML دریافت شده deserialized شود، کد XML برای دستورات و رشته‌های XML ارزیابی می‌شود. یک کاربر می‌تواند به یک برنامه مبتنی بر net. که فایل‌های XML را تجزیه و تحلیل می‌کند، با استفاده از تگ <system:string> و دستورات تعبیه شده سیستمی مخرب، حمله کند.
خانواده بدافزاری	این آسیب‌پذیری توسط بدافزارهای فیشینگ و باج افزار WickrMe/Hello استفاده شده است.
وصله امنیتی	در این لینک مشاهده شود.
راه حل کاهش تهدید	۱- ارتقاء نرم‌افزار به آخرین نسخه ارائه شده ۲-در صورت الزام دسترسی از راه دور به Microsoft SharePoint برای کاربران نیاز است از مکانیزم‌های احراز هویت مانند VPN استفاده شود.
نحوه تشخیص	۱- احتمال بهره‌برداری از این آسیب‌پذیری در سرورهای آسیب‌پذیر SharePoint نیاز است بررسی شود، برای اطلاعات بیشتر به این لینک مراجعه شود. ۲- NSA یک راهنمای جامع برای تشخیص و مقابله با وب‌شل‌ها ارائه کرده است که از طریق این لینک قابل دسترس است.
تکنولوژی و نسخه آسیب‌پذیر	At the time of the vulnerability release, the following Microsoft SharePoint versions were affected: Microsoft Sharepoint 2019, Microsoft SharePoint 2016, Microsoft SharePoint 2013 SP1, and Microsoft SharePoint 2010 SP2.
منابع	برای اطلاعات بیشتر به لینک‌های زیر مراجعه شود:

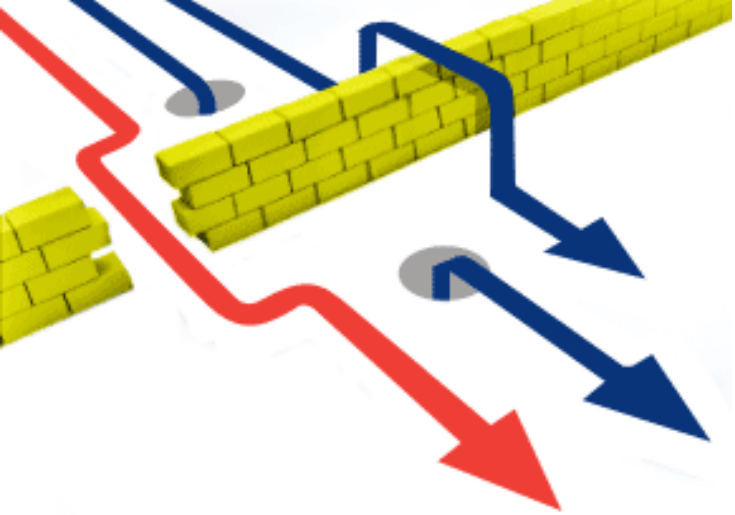


۲۵ پارامتر در بررسی آسیب‌پذیری‌های وب‌اپلیکیشن‌ها

هادی گلباغی

مقدمه

ارزیابی امنیتی جهت کشف آسیب‌پذیری و نقص‌ها و رفع آنها، یکی از فعالیت‌های مهم به منظور جلوگیری از نفوذ مهاجمین و ارتقاء امنیت سایبری است. یک متخصص حوزه ارزیابی امنیتی و تست نفوذ (Pentester) از روش‌ها و ابزارهای مختلفی در فرایند شناسایی آسیب‌پذیری‌ها و نقص‌ها بهره می‌برد، اساساً مراحل مختلفی برای تست نفوذ وجود دارد که این مراحل در شکل زیر نشان داده شده است.



محققین امنیتی چه در سطح مبتدی چه در سطح پیشرفته‌تر که در حوزه‌های مختلفی از قبیل ارزیابی امنیتی، باگ بانتی، شناسایی آسیب‌پذیری و تست نفوذ فعالیت دارند می‌توانند از چک‌لیست‌های بسیاری به منظور انجام فرایند شناسایی آسیب‌پذیری و نقص‌ها استفاده کنند.
در این مطلب لیستی از ۲۵ پارامتر مورد بررسی در چند آسیب‌پذیری شایع مورد بررسی خواهد بود. دلیل انتخاب این ۲۵ پارامتر نرخ استفاده از آن‌ها در مقاله‌ها و منابع مختلف بوده است و می‌توان از آن‌ها در ارزیابی‌های خودکار و ارزیابی دستی (Manual) استفاده کرد. بدیهی است متخصصین و منابع مختلف می‌توانند لیست یا پارامترهای متفاوتی را داشته باشند.

در لیست ۲۵ موردی مدنظر این مطلب، پارامترهای آسیب‌پذیری‌های زیر مورد بررسی قرار گرفته است:

- Cross-Site Scripting (XSS)
- Server-Side Request Forgery (SSRF)
- Local File Inclusion (LFI)
- SQL Injection (SQLi)
- Remote Code Execution (RCE) - [for GET and POST methods]
- Open Redirect

در ادامه پارامترهای مورد بررسی هر کدام از آسیب‌پذیری‌ها جداگانه ارائه می‌شوند. در این مطلب درخصوص آسیب‌پذیری‌ها توضیحاتی ارائه نشده است و صرفاً پارامترهای آسیب‌پذیر معرفی شده‌اند. درصورتی‌که نیاز به توضیحات تخصصی درخصوص هر کدام از آسیب‌پذیری‌ها بود، می‌توان به مطلب «۱۰ خطر امنیتی و آسیب‌پذیری مخرب OWASP» که در شماره نهم همین فصل‌نامه منتشر شده است، مراجعه کنید.

```
Top 25 XSS Dorks according to OpenBugBounty

1.  ?q={payload}
2.  ?s={payload}
3.  ?search={payload}
4.  ?id={payload}
5.  ?lang={payload}
6.  ?keyword={payload}
7.  ?query={payload}
8.  ?page={payload}
9.  ?keywords={payload}
10. ?year={payload}
11. ?view={payload}
12. ?email={payload}
13. ?type={payload}
14. ?name={payload}
15. ?p={payload}
16. ?month={payload}
17. ?immagine={payload}
18. ?list_type={payload}
19. ?url={payload}
20. ?terms={payload}
21. ?categoryid={payload}
22. ?key={payload}
23. ?l={payload}
24. ?begindate={payload}
25. ?enddate={payload}
```

```
Top 25 Server-Side Request Forgery(SSRF) Dorks

1.?dest={target}
2.?redirect={target}
3.?uri={target}
4.?path={target}
5.?continue={target}
6.?url={target}
7.?window={target}
8.?next={target}
9.?data={target}
10.?reference={target}
11.?site={target}
12.?html={target}
13.?val={target}
14.?validate={target}
15.?domain={target}
16.?callback={target}
17.?return={target}
18.?page={target}
19.?feed={target}
20.?host={target}
21.?port={target}
22.?to={target}
23.?out={target}
24.?view={target}
25.?dir={target}

Note: The popularity of dorks can vary.
```

```
Top 25 LFI (Local File Inclusion) Parameters

1.  ?cat={payload}
2.  ?dir={payload}
3.  ?action={payload}
4.  ?board={payload}
5.  ?date={payload}
6.  ?detail={payload}
7.  ?file={payload}
8.  ?download={payload}
9.  ?path={payload}
10. ?folder={payload}
11. ?prefix={payload}
12. ?include={payload}
13. ?page={payload}
14. ?inc={payload}
15. ?locate={payload}
16. ?show={payload}
17. ?doc={payload}
18. ?site={payload}
19. ?type={payload}
20. ?view={payload}
21. ?content={payload}
22. ?document={payload}
23. ?layout={payload}
24. ?mod={payload}
25. ?conf={payload}
```

```
Top 25 SQL Injection Parameters

1.  ?id={payload}
2.  ?page={payload}
3.  ?dir={payload}
4.  ?search={payload}
5.  ?category={payload}
6.  ?class={payload}
7.  ?file={payload}
8.  ?url={payload}
9.  ?news={payload}
10. ?item={payload}
11. ?menu={payload}
12. ?lang={payload}
13. ?name={payload}
14. ?ref={payload}
15. ?title={payload}
16. ?view={payload}
17. ?topic={payload}
18. ?thread={payload}
19. ?type={payload}
20. ?date={payload}
21. ?form={payload}
22. ?join={payload}
23. ?main={payload}
24. ?nav={payload}
25. ?region={payload}
```

```
Top 25 Remote Code Execution(RCE) Parameters

1.  ?cmd={payload}
2.  ?exec={payload}
3.  ?command={payload}
4.  ?execute={payload}
5.  ?ping={payload}
6.  ?query={payload}
7.  ?jump={payload}
8.  ?code={payload}
9.  ?reg={payload}
10. ?do={payload}
11. ?func={payload}
12. ?arg={payload}
13. ?option={payload}
14. ?load={payload}
15. ?process={payload}
16. ?step={payload}
17. ?read={payload}
18. ?function={payload}
19. ?req={payload}
20. ?feature={payload}
21. ?exe={payload}
22. ?module={payload}
23. ?payload={payload}
24. ?run={payload}
25. ?print={payload}
```

```
Top 25 Open Redirect Dorks

1.  /{payload}
2.  ?next={payload}
3.  ?url={payload}
4.  ?target={payload}
5.  ?rurl={payload}
6.  ?dest={payload}
7.  ?destination={payload}
8.  ?redir={payload}
9.  ?redirect_uri={payload}
10. ?redirect_url={payload}
11. ?redirect={payload}
12. /redirect/{payload}
13. /cgi-bin/redirect.cgi?{payload}
14. /out/{payload}
15. /out?{payload}
16. ?view={payload}
17. /login?to={payload}
18. ?image_url={payload}
19. ?go={payload}
20. ?return={payload}
21. ?returnTo={payload}
22. ?return_to={payload}
23. ?checkout_url={payload}
24. ?continue={payload}
25. ?return_path={payload}
```

معرفی ابزار

معرفی ابزار

SN1PER

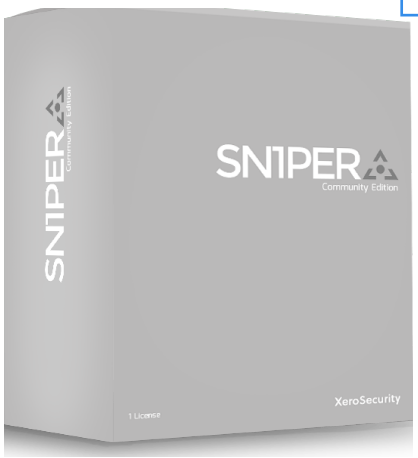
تینا احمدی

Automated pentest recon scanner

مقدمه

Sn1per یک اسکنر خودکار است که توسط XeroSecurity توسعه داده شده و می‌تواند فرآیند جمع آوری داده‌ها برای اکتشاف و تست نفوذ را به‌طور خودکار انجام دهد و از طریق سایت xerosecurity.com قابل دریافت است.
این شرکت سه نسخه از برنامه Sn1per را ارائه داده است که در ادامه جداگانه آورده شده‌اند.

Community
Scan Engine
$0



Community Updates

Command line (CLI)

scan engineScan

unlimited hostsUnlimited

workspacesCommunity

Github updatesCommunity

Github technical support

Professional
Sn1per Professional V9.0
Command Execution Add-On V2.0
$420

Sn1per SE v9.x scan engine updates
Self hosted solution
Full management and control via the web UIModular design to allow for add-on modules
2 weeks of email support
Single user license
Unlimited scans
Up to 50 workspaces
Up to 1000 hosts per workspace
Sn1per v9.x scan engine updates
Command Execution Add-on v2.0 included

Elite
Sn1per Professional V9.0
All Add-Ons
$570

Sn1per SE v9.x scan engine updates
Self hosted solution
Full management and control via the web UI
Modular design to allow for add-on modules
2 weeks of support
Single user license
Unlimited scans
Up to 50 workspaces
Up to 1000 hosts per workspace
Sn1per v9.x scan engine updates
All add-ons included

Sn1per شامل مجموعه‌ای از ابزارهای شناخته شده‌ی زیر است که در طی یک تست نفوذ برای شمارش و بررسی آسیب‌پذیری‌ها از آن‌ها استفاده می‌شود. با پلتفرم Sn1per Professional سطح حمله را کشف کرده و خطرات را اولویت‌بندی کنید.

- amap
- arachni
- cisco-torch
- dnsenum
- enum4linux
- golismero
- hydra
- metasploit
- nbtscan
- nmap
- smtp-user-enum
- sqlmap
- sslscan
- thevestvest
- w3af
- wapiti
- whatweb
- whois
- nikto
- wpscan
- theharvester

ویژگی‌ها

- جمع آوری اطلاعات (DNS، ping، whois و غیره)
- کوئری‌های Google Hacking را برای دامنه هدف اجرا می‌کند.
- پورت‌های باز را جمع آوری می‌کند.
- زیردامنه را brute force می‌کند و اطلاعات DNS را استخراج می‌کند.
- sub-domain hijacking را بررسی می‌کند.
- اسکریپت‌های Nmap هدفمند را برای پورت‌های باز اجرا می‌کند.
- ماژول‌های اسکن و بهره‌برداری Metasploit را اجرا می‌کند.
- تمام برنامه‌های وب را برای آسیب‌پذیری‌های رایج اسکن می‌کند.
- تمام سرویس‌های باز را brute force می‌کند.
- از راه دور از میزبان‌ها بهره‌برداری می‌کند تا به دسترسی shell برسد.
- Auto-pwn برای ShellShock، Metasploitable، MS08-067، Default Tomcat Creds اضافه شده است.
- برای گزارش‌گیری با MSFConsole، Metasploit Pro و Zenmap ادغام می‌شود.
- برای ذخیره کل خروجی اسکن‌ها، فضاهای کاری جداگانه ایجاد می‌کند.

ابزار Sn1per چه امکاناتی به شما می‌دهد؟

می‌توانید به راحتی سطح حمله (IP ها، نام دامنه‌ها، پورت‌های باز، هدرهای HTTP و غیره) را کشف کنید.

با استفاده از جدیدترین ابزارهای هکینگ و تست نفوذ فرایند بهره‌برداری را خودکار سازی می‌کند.

ایجاد یک visual recon برای همه میزبانان در فضای کاری شما با استفاده از نمایش اسلاید و تصاویر کوچک.

امکان جستجو، مرتب سازی و فیلترکردن بر اساس status، title، IP، DNS، هدرهای سرور، WAF و باز کردن پورت‌های TCP/UDP از کل سطح حمله.

تقویت توانایی پاسخ و تشخیص «تیم آبی» در برابر تکنیک‌های تست نفوذ خودکار

می‌توانید برای کمک به مدیریت داده‌های خود و سازماندهی امور، چندین یادداشت را در یک مکان واحد ذخیره کرده و به آن‌ها دسترسی داشته باشید.

با استفاده از جدیدترین اسکنرهای آسیب‌پذیری منبع باز و تجاری، به سرعت جدیدترین نقاط آسیب‌پذیر و CVE را اسکن کنید.

اسناد آنلاین، متا دیتا، آدرس‌های ایمیل و اطلاعات تماس را به‌صورت خودکار جمع می‌کند.

برنامه‌ریزی اسکن به‌صورت روزانه، هفتگی یا ماهانه برای پوشش مداوم تغییرات.

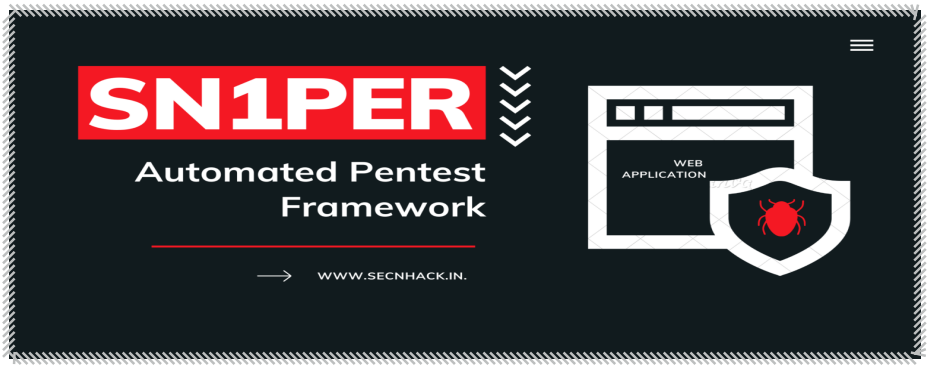
اسکن برنامه‌های وب از طریق Arachni، Burpsuite Professional و Nikto.

کل میزبان‌ها را لیست کرده و گزارش‌هاي آسیب‌پذیری را به‌صورت XLS، CSV یا فرمت PDF برای فیلتر کردن، مرتب سازی و مشاهده تمام داده‌های سطح حمله در اختیار ما قرار می‌دهد.

نمایش اعلان برای تغییرات وضعیت اسکن و میزبان، تغییرات URL و دامنه و آسیب‌پذیری‌های جدید کشف شده.

این ابزار می‌تواند به‌صورت خودکار سطح حمله را کشف و به راحتی جدیدترین آسیب‌پذیری‌ها و CVE را اسکن کند. مرتب سازی و مشاهده تمام داده‌های سطح حمله در اختیار ما قرار می‌دهد.

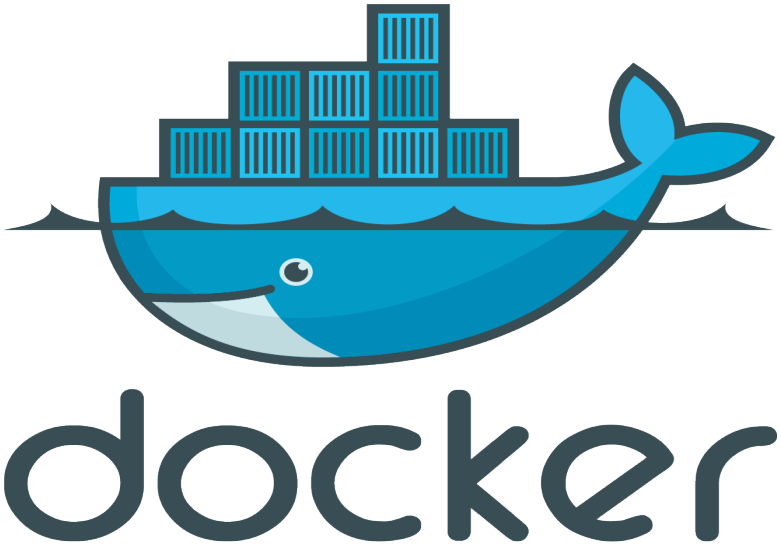
تمامی رکوردهای DNS را که در برابر حملات domain hijacking و domain takeover آسیب‌پذیر هستند، لیست می‌کند. مرتب سازی و مشاهده تمام داده‌های سطح حمله در اختیار ما قرار می‌دهد.



نصب

نصب ابزار Sn1per بر روی توزیع‌های مختلف LINUX مانند KALI/UBUNTU/DEBIAN/PARROT:

```
git clone https://github.com/1N3/Sn1per
cd Sn1per
bash install.sh
```



نصب DOCKER

از کنسول جدید Docker، دستورات زیر را اجرا کنید:

```
Download https://raw.githubusercontent.com/1N3/Sn1per/master/Dockerfile
docker build -t sn1per.
docker run -it sn1per /bin/bash

or

docker pull xerosecurity/sn1per
docker run -it xerosecurity/sn1per /bin/bash
```

USAGE

```
[*] NORMAL MODE
sniper -t <TARGET>

[*] NORMAL MODE + OSINT + RECON
sniper -t <TARGET> -o -re

[*] STEALTH MODE + OSINT + RECON
sniper -t <TARGET> -m stealth -o -re

[*] DISCOVER MODE
sniper -t <CIDR> -m discover -w
<WORSPACE_ALIAS>

[*] SCAN ONLY SPECIFIC PORT
sniper -t <TARGET> -m port -p
<portnum>

[*] FULLPORTONLY SCAN MODE
sniper -t <TARGET> -fp

[*] WEB MODE - PORT 443 + 80 ONLY!
sniper -t <TARGET> -m web

[*] HTTP WEB PORT MODE
sniper -t <TARGET> -m webporthttp -p
<port>

[*] HTTPS WEB PORT MODE
sniper -t <TARGET> -m webporthttps -p
<port>

[*] HTTP WEBSCAN MODE
sniper -t <TARGET> -m webscan

[*] ENABLE BRUTEFORCE
sniper -t <TARGET> -b

[*] AIRSTRIKE MODE
sniper -f targets.txt -m airstrike

[*] NUKE MODE WITH TARGET LIST,
BRUTEFORCE ENABLED, FULLPORTSCAN
ENABLED, OSINT ENABLED, RECON
ENABLED, WORKSPACE & LOOT ENABLED
sniper -f targets.txt -m nuke -w
<WORKSPACE_ALIAS>

[*] MASS PORT SCAN MODE
sniper -f targets.txt -m massportscan
```

```
[*] MASS WEB SCAN MODE
sniper -f targets.txt -m massweb

[*] MASS WEBSCAN SCAN MODE
sniper -f targets.txt -m masswebscan

[*] MASS VULN SCAN MODE
sniper -f targets.txt -m massvulnscan

[*] PORT SCAN MODE
sniper -t <TARGET> -m port -p <PORT_NUM>

[*] LIST WORKSPACES
sniper --list

[*] DELETE WORKSPACE
sniper -w <WORKSPACE_ALIAS> -d

[*] DELETE HOST FROM WORKSPACE
sniper -w <WORKSPACE_ALIAS> -t <TARGET> -dh

[*] GET SNIPER SCAN STATUS
sniper --status

[*] LOOT REIMPORT FUNCTION
sniper -w <WORKSPACE_ALIAS> --reimport

[*] LOOT REIMPORTALL FUNCTION
sniper -w <WORKSPACE_ALIAS> --reimportall

[*] LOOT REIMPORT FUNCTION
sniper -w <WORKSPACE_ALIAS> --reload

[*] LOOT EXPORT FUNCTION
sniper -w <WORKSPACE_ALIAS> --export

[*] SCHEDULED SCANS
sniper -w <WORKSPACE_ALIAS> -s
daily|weekly|monthly

[*] USE A CUSTOM CONFIG
sniper -c /path/to/sniper.conf -t <TARGET> -w
<WORKSPACE_ALIAS>

[*] UPDATE SNIPER
sniper -u|--update
```

MODE های ابزار Sn1per

REPORT	همه نتایج را به‌صورت متنی برای ارجاعات بعدی در دایرکتوری loot ایجاد می‌کند. برای فعال کردن گزارش‌گیری، «report» را به هر مد یا دستور sn1per اضافه کنید.
STEALTH	برای جلوگیری از شناسایی توسط WAF/IPS، اهداف واحد را سریعاً با استفاده از اسکن‌های non-intrusive جمع آوری کنید.
FLYOVER	اسکن سریع و چندگانه سطح بالا از چندین هدف (برای جمع آوری سریع داده‌های سطح بالا در بسیاری از میزبان‌ها مفید است)
DISCOVER	همه میزبان‌ها را در یک Subnet/CIDR تجزیه می‌کند (یعنی 192.168.0.0/16) و اسکن sn1per را برای هر میزبان شروع می‌کند. برای اسکن شبکه داخلی مفید است.
PORT	پورت مشخصی را برای آسیب‌پذیری اسکن می‌کند. گزارش‌گیری در حال حاضر در این مد در دسترس نیست.
FULLPORTONLY	اسکن کامل پورت را انجام می‌دهد و نتایج را با فرمت XML ذخیره می‌کند.
ASSPORTSCAN	اسکن «FULLPORTONLY» را روی اهداف مشخص شده چندگانه از طریق سوئیچ «-f» اجرا می‌کند.
WEB	اسکن کاملاً خودکار برنامه‌های وب را به نتایج اضافه می‌کند (فقط پورت tcp/80 و tcp/443). برای برنامه‌های وب مناسب است اما ممکن است زمان اسکن را به میزان قابل توجهی افزایش دهد.
NOBRUTE	اسکن کاملی را علیه میزبان/دامنه هدف بدون استفاده از brute force شروع می‌کند.
AIRSTRIKE	پورت‌ها/سرویس‌های باز را به سرعت از میزبان‌های چندگانه جمع‌آوری می‌کند و جمع‌آوری مقدماتی را انجام می‌دهد. برای استفاده، مکان کامل فایل را که شامل همه میزبان‌ها است،IP هایی که برای شروع اسکن نیاز به اسکن و دستور زیر را برای شروع پویش airstrike اجرا می‌کند. ./sn1per/full/path/to/targets.txt
NUKE	حسابرسی کامل میزبان‌های چندگانه مشخص شده در فایل متنی مشخص شده. مثال: ./sn1per/pentest/loot/targets.txt
LOOT	به‌صورت خودکار پوشه loot را در مرورگر شما سازماندهی کرده و نمایش می‌دهد و سپس ابزارهای Metasploit Pro و Zenmap GUI و خروجی تمام نتایج اسکن پورت باز را نمایش می‌دهد. برای اجرای این مد، دستور «sniper loot» را اجرا کنید.
MASSWEB	اسکن‌های مد «web» را روی چندین هدف مشخص شده از طریق سوئیچ «-f» اجرا می‌کند.

WEBPORTHTTP	اسکن کامل برنامه وب HTTP را برای یک میزبان و پورت خاص راه اندازی می‌کند.
WEBPORTHTTPS	اسکن کامل برنامه وب HTTPS را برای یک میزبان و پورت خاص راه اندازی می‌کند.
WEBSCAN	اسکن کامل برنامه وب HTTP و HTTPS را از طریق Burpsuite و Arachni راه اندازی می‌کند.
MASSWEBSCAN	اسکن‌های مد «webscan» را برای چندین هدف مشخص شده از طریق سوئیچ «-f» اجرا می‌کند.
VULNSCAN	اسکن آسیب‌پذیری OpenVAS را راه اندازی می‌کند.
MASSVULNSCAN	اسکن‌های مد «vulnscan» را روی چندین هدف مشخص شده از طریق سوئیچ «-f» راه‌اندازی می‌کند.

نمایش (Demonstration) تفصیلی - Sn1per

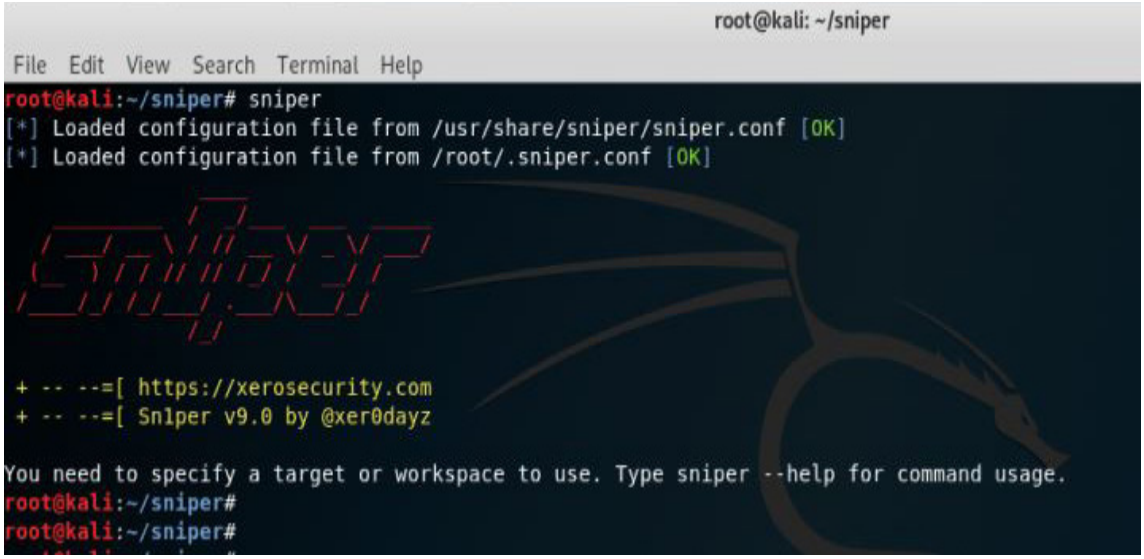
گام ۱

برای دانلود و نصب ابزار به ترتیب دستورات زیر را در ترمینال اجرا کنید:

```
#git clone https://github.com/1N3/Sn1per.git
#cd Sn1per
#chmod +x install.sh
#./install.sh
```

گام ۲

پس از نصب موفقیت آمیز Sn1per، آن را اجرا کنید.



گام ۳

پس از اجرای Sn1per، شروع به جمع آوری اطلاعات از هدف مورد نظر کنید.

```
#sniper  cert.uok.ac.ir
```

```
root@kali: ~/sniper
File  Edit  View  Search  Terminal  Help
root@kali:~/sniper# sniper -t cert.uok.ac.ir -o -re
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/ [OK]
[*] Scanning cert.uok.ac.ir [OK]
[*] Loaded configuration file from /usr/share/sniper/sniper.conf [OK]
[*] Loaded configuration file from /root/.sniper.conf [OK]
[*] Saving loot to /usr/share/sniper/loot/workspace/cert.uok.ac.ir [OK]
[*] Scanning cert.uok.ac.ir [OK]

 + -- --=[https://xerosecurity.com
 + -- --=[Sn1per v9.0 by @xer0dayz

=================================================================================•x[2021-07-27](02:26)x•
 GATHERING DNS INFO
=================================================================================•x[2021-07-27](02:26)x•
=================================================================================•x[2021-07-27](02:26)x•
 CHECKING FOR SUBDOMAIN HIJACKING
=================================================================================•x[2021-07-27](02:26)x•
=================================================================================•x[2021-07-27](02:26)x•
 GATHERING WHOIS INFO
=================================================================================•x[2021-07-27](02:26)x•
% This is the IRNIC Whois server v1.6.2.
% Available on web at http://whois.nic.ir/
% Find the terms and conditions of use on http://www.nic.ir/
%
```

بخشی از خروجی‌های این دستور در زیر آورده شده است:

```
root@kali: ~/sniper
File  Edit  View  Search  Terminal  Help
[*] Searching Bing email addresses from cert.uok.ac.ir
[*] Extracting emails from Bing search results...
[*] Searching Yahoo for email addresses from cert.uok.ac.ir
[*] Extracting emails from Yahoo search results...
[*] Located 0 email addresses for cert.uok.ac.ir
[*] Auxiliary module execution completed

CRTSH
=================================================================================•x[2021-07-27](02:27)x•
 GATHERING CERTIFICATE SUBDOMAINS
=================================================================================•x[2021-07-27](02:27)x•

0 /usr/share/sniper/loot/workspace/cert.uok.ac.ir/domains/domains-cert.uok.ac.ir-crt.txt

[+] Domains saved to: /usr/share/sniper/loot/workspace/cert.uok.ac.ir/domains/domains-cert.uok.ac.ir-crt.tx
t
=================================================================================•x[2021-07-27](02:27)x•
 GATHERING PROJECT SONAR SUBDOMAINS
=================================================================================•x[2021-07-27](02:27)x•
1 /usr/share/sniper/loot/workspace/cert.uok.ac.ir/domains/domains-cert.uok.ac.ir-projectsonar.txt
=================================================================================•x[2021-07-27](02:27)x•
 GATHERING RAPIDDNS SUBDOMAINS
=================================================================================•x[2021-07-27](02:27)x•
2 /usr/share/sniper/loot/workspace/cert.uok.ac.ir/domains/domains-cert.uok.ac.ir-full.txt
=================================================================================•x[2021-07-27](02:28)x•
 NEW SUBDOMAINS
=================================================================================•x[2021-07-27](02:28)x•
2 /usr/share/sniper/loot/workspace/cert.uok.ac.ir/domains/domains_new-cert.uok.ac.ir.txt
cert.uok.ac.ir
www.cert.uok.ac.ir
```

```
root@kali: ~/sniper
File  Edit  View  Search  Terminal  Help
rtt min/avg/max/mdev = 2.503/2.503/2.503/0.000 ms

=================================================================================•x[2021-07-27](02:28)x•
 RUNNING TCP PORT SCAN
=================================================================================•x[2021-07-27](02:28)x•
Starting Nmap 7.70 ( https://nmap.org ) at 2021-07-27 02:28 EDT
Nmap scan report for cert.uok.ac.ir (172.16.34.27)
Host is up (0.0013s latency).
Not shown: 62 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds

=================================================================================•x[2021-07-27](02:28)x•
 RUNNING INTRUSIVE SCANS
=================================================================================•x[2021-07-27](02:28)x•
 + -- --=[Port 21 closed... skipping.
 + -- --=[Port 22 closed... skipping.
 + -- --=[Port 23 closed... skipping.
 + -- --=[Port 25 closed... skipping.
 + -- --=[Port 53 closed... skipping.
 + -- --=[Port 67 closed... skipping.
 + -- --=[Port 68 closed... skipping.
 + -- --=[Port 69 closed... skipping.
 + -- --=[Port 79 closed... skipping.
 + -- --=[Port 110 closed... skipping.
 + -- --=[Port 111 closed... skipping.
 + -- --=[Port 123 closed... skipping.
 + -- --=[Port 135 closed... skipping.
 + -- --=[Port 137 closed... skipping.
```

```
root@kali: ~/sniper
File  Edit  View  Search  Terminal  Help
=================================================================================•x[2021-07-27](02:28)x•
 RUNNING TCP PORT SCAN
=================================================================================•x[2021-07-27](02:28)x•
 + -- --=[Port 443 opened... running tests...
=================================================================================•x[2021-07-27](02:28)x•
 CHECKING HTTP HEADERS AND METHODS
=================================================================================•x[2021-07-27](02:28)x•
HTTP/1.1 200 OK
Date: Tue, 27 Jul 2021 06:28:22 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN, SAMEORIGIN
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=remmct30mkodnrccih5cpoqr1k; path=/;HttpOnly;Secure
Set-Cookie: PHPSESSID=5bondikt2jq6u9o01nvm647psm; path=/;HttpOnly;Secure
Content-Type: text/html; charset=UTF-8

HTTP/1.1 200 OK
Date: Tue, 27 Jul 2021 06:28:23 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN, SAMEORIGIN
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=ebovqi2s56m0qq5u7kfh5m3c9u; path=/;HttpOnly;Secure
Set-Cookie: PHPSESSID=drg1k0ovi1s69te9k89nflj8lq; path=/;HttpOnly;Secure
Content-Type: text/html; charset=UTF-8
```

```
root@kali: ~/sniper
File  Edit  View  Search  Terminal  Help
[+] 1 actual URLs screenshot
[+] 0 error(s)
=================================================================================•x[2021-07-27](02:28)x•
 RUNNING NMAP SCRIPTS
=================================================================================•x[2021-07-27](02:28)x•
Starting Nmap 7.70 ( https://nmap.org ) at 2021-07-27 02:28 EDT
NSE: Loaded 48 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:28
Completed NSE at 02:28, 0.00s elapsed
Initiating NSE at 02:28
Completed NSE at 02:28, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 02:28
Completed Parallel DNS resolution of 1 host. at 02:28, 0.00s elapsed
Initiating SYN Stealth Scan at 02:28
Scanning cert.uok.ac.ir (172.16.34.27) [1 port]
Discovered open port 443/tcp on 172.16.34.27
Completed SYN Stealth Scan at 02:28, 0.03s elapsed (1 total ports)
Initiating Service scan at 02:28
Scanning 1 service on cert.uok.ac.ir (172.16.34.27)
Completed Service scan at 02:28, 12.05s elapsed (1 service on 1 host)
NSE: Script scanning 172.16.34.27.
Initiating NSE at 02:28
Completed NSE at 02:28, 2.62s elapsed
Initiating NSE at 02:28
Completed NSE at 02:28, 0.00s elapsed
Nmap scan report for cert.uok.ac.ir (172.16.34.27)
Host is up (0.0027s latency).
rDNS record for 172.16.34.27: www.cert.uok.ac.ir

PORT    STATE SERVICE VERSION
443/tcp open  ssl/ssl Apache httpd (SSL-only mode)
| http-brute:
```

برخی از ابزارهای موجود در Sn1per

THEHARVESTER

هدف این برنامه جمع آوری ایمیل‌ها، زیر دامنه‌ها، میزبان‌ها، نام کارمندان، پورت‌های باز و بنرها از منابع عمومی مختلف مانند موتورهای جستجو، سرورهای اصلی PGP و موتور جستجوی آسیب‌پذیری SHODAN است.

این ابزار برای کمک به متخصصین حوزه تست نفوذ در مراحل اولیه تست نفوذ به منظور فهمیدن ردپای مشتری در اینترنت است. همچنین برای هر کسی که می‌خواهد بداند یک مهاجم در مورد سازمان او چه چیزی را می‌بیند، می‌تواند مفید باشد.

Sublist3r

Sublist3r ابزار پایتونی است که برای شمارش زیر دامنه‌های وب سایت‌ها از طریق OSINT طراحی شده است. به متخصصین حوزه تست نفوذ و شکارچیان آسیب‌پذیری کمک می‌کند تا زیر دامنه‌هایی را برای دامنه مورد نظر خود جمع آوری کنند. Sublist3r با استفاده از بسیاری از موتورهای جستجو مانند Baidu، Bing، Google Yahoo و Ask زیر دامنه‌ها را جمع آوري می‌کند. Sublist3r همچنین با استفاده از DNSdumpster، ThreatCrowd، Virustotal، Netcraft و ReverseDNS زیر دامنه‌ها را جمع آوري می‌کند.

wafw00f

فایروال‌های برنامه وب معمولاً فایروال‌هایی هستند که روی لایه کاربرد کار می‌کنند و درخواست‌های HTTP را کنترل و اصلاح می‌کنند.
اساساً همه WAF ها از برنامه‌های کاربردی وب در برابر حملاتی مانند SQLi و XSS محافظت می‌کنند. Wafw00f در ساده‌ترین حالت یک ابزار پایتون است که به‌طور خودکار مجموعه‌ای از روش‌های مورد استفاده را برای یافتن WAF انجام می‌دهد. Wafw00f به سادگی از یک وب سرور با مجموعه‌ای از کوئري‌ها و متدهای HTTP پرس‌وجو می‌کند. پاسخ‌های دریافت‌شده از آن‌ها را تجزیه و تحلیل می‌کند و WAF مورد نظر را تشخیص می‌دهد.

XST

کلمه «XS» در XST شباهتی به کلمه XSS را تداعی می‌کند و ممکن است افراد آن را با روشی برای تزریق کدهای جاوا اسکریپت اشتباه بگیرند. درصورتی که کلمه XST مخفف Cross-Site Tracing می‌باشد. این حملات با ترکیبی از حملات XSS و استفاده از متد TRACE یا TRACK پروتکل HTTP انجام می‌شود و ممکن است باعث سرقت کوکی‌های کاربر شود.

Nikto

Nikto یکی از اسکنرهای قدرتمند و قدیمی برای پویش آسیب‌پذیری‌های وب‌سرور می‌باشد.

INURLBR

اسکنر INURLBR برای کمک به پنتسترها و افرادی که در زمینه امنیت سایبری وب کار می‌کنند، توسعه داده شده است. با این اسکنر می‌توان آسیب‌پذیری‌ها را در برنامه‌های تحت وب شناسایی کرد. این ابزار با زبان HP پیاده‌سازی شده و بر روی توزیع‌های مختلفی از لینوکس قابل دسترس است.

BruteX

به‌صورت خودکار تمام سرویس‌هایي را که بر روی یک هدف اجرا می‌شوند brute force می‌کند.

- پورت‌هاي باز
- دامنه‌های DNS
- نام‌های کاربری
- رمزهای عبور

MassBleed

MassBleed یک اسکنر آسیب‌پذیری SSL است. توابع اصلی با قابلیت پروکسی تمام اتصالات:

- برای اسکن گسترده هر محدوده CIDR برای آسیب‌پذیری‌های OpenSSL از طریق پورت tcp HTTPS /443
(مثال: sh massbleed.sh 192.168.0.0/16)
- برای اسکن هر محدوده CIDR برای آسیب‌پذیری‌های OpenSSL از طریق پورت سفارشی مشخص شده
(مثال: sh massbleed.sh 192.168.0.0/16 پورت 8443)
- برای اسکن کردن هر پورت (۱-۱۰۰۰۰) در یک سیستم واحد برای نسخه‌های آسیب‌پذیر OpenSSL
(مثال: sh massbleed.sh 127.0.0.1 single)
- اسکن هر پورت باز در هر میزبان در یک زیر شبکه کلاس C برای آسیب‌پذیری‌های OpenSSL
(مثال: sh massbleed.sh 192.168.0.0 subnet)

Yasuo

Yasuo یک اسکریپت ruby است که برنامه‌های وب آسیب‌پذیر 3rd-Party را اسکن می‌کند.

در حالی که روی ارزیابی امنیت شبکه کار می‌کنید (داخلی، خارجی، کنفرانس‌های Redteam و غیره)، ما اغلب با برنامه‌های تحت وب 3rd-party آسیب‌پذیر یا front-end وب مواجه می‌شویم که به مهاجم امکان می‌دهد با بهره‌برداری از آسیب‌پذیری‌های شناخته شده به سرور، از راه دور دسترسی پیدا کند.
برخی از برنامه‌های رایج و پرکاربرد واسط مدیریتی Hudson، JBoss jmx-console، Apache Tomcat Jenkins و غیره است.

بنابراین مجموعه‌ای از ابزارهای پیشرفته جمع‌آوری و اسکن اطلاعات، نقش خود را با Sn1per بازی می‌کنند و اطلاعات دقیق و نتیجه اسکن را با هدف خاص توزیع می‌کنند.

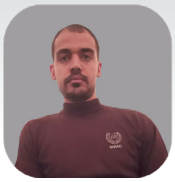
SN1PER

The ultimate "all-in-one"
offensive security framework

Xerosecurity

دفترچه تقلب

```
[root@localhost ~]# last reboot
reboot   system boot  3.10.0-1062.12.1 Wed Mar 11 05:28 - 05:45  (00:16)
reboot   system boot  3.10.0-1062.12.1 Thu Feb 27 05:22 - 05:45 (13+00:22)
reboot   system boot  3.10.0-1062.9.1. Tue Feb 25 06:25 - 05:45 (14+23:19)
reboot   system boot  3.10.0-1062.9.1. Mon Feb 24 05:52 - 05:45 (15+23:52)
reboot   system boot  3.10.0-1062.9.1. Tue Jan 28 08:47 - 05:45 (42+20:58)
reboot   system boot  3.10.0-1062.9.1. Mon Jan 27 08:18 - 05:45 (43+21:26)
reboot   system boot  3.10.0-1062.9.1. Wed Jan 15 05:24 - 05:45 (56+00:20)
reboot   system boot  3.10.0-1062.9.1. Wed Jan  8 05:18 - 05:45 (63+00:26)
reboot   system boot  3.10.0-1062.9.1. Wed Jan  8 03:20 - 05:45 (63+02:24)
```

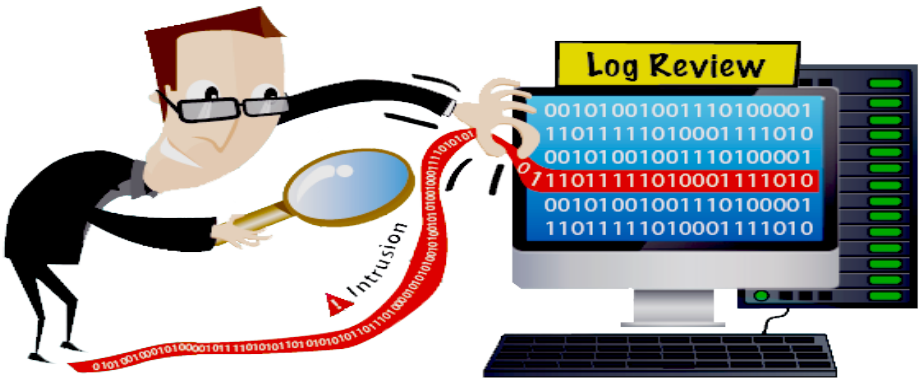


چک لیست بازبینی لاگ‌های حیاتی در رخدادهای امنیتی

محمد حبیبی

رویکرد کلی

- تشخیص این که کدام منابع و ابزارهای خودکار در طول فرایند بررسی لاگ‌ها می‌توانند استفاده شوند.
- کپی‌کردن رکوردهای لاگ به یک محل مشخص تا در صورت نیاز به‌سادگی بتوان آن‌ها را بازبینی کرد.
- کم‌کردن به اصطلاح «Noise» موجود در لاگ‌ها، با حذف موارد روتین و تکراری از موارد نمایش داده شده (view) بعد از اینکه کم‌خطر بودن آن‌ها مشخص شد.
- با درنظرگرفتن منطقه‌های زمانی متفاوت، تشخیص این‌که آیا می‌توانید به زمان ثبت‌شده (time stamps) در لاگ‌ها اعتماد کنید. به عنوان مثال فرض کنید که منطقه زمانی سرور بر روی UTC+۰ تنظیم شده و رایانه شخصی که لاگ‌ها را بررسی می‌کند در منطقه زمانی UTC+۳:۳۰ تهران تنظیم شده است.
- ابتدا نیاز است بر روی تغییرات انجام شده اخیر، تلاش‌هایی که با شکست مواجه شده‌اند، خطاها، تغییر وضعیت‌ها،رویدادهای دسترسی و مدیریتی و رویدادهای غیرمعمولی برای محیط شما، تمرکز کنید.
- بازسازی موارد، از حال حاضر تا قبل و بعد از تاریخ وقوع رخداد.
- بررسی فعالیت‌های متفاوت از طریق لاگ‌های مختلف، برای رسیدن به یک تصویر جامع از رخداد امنیتی.
- ایجاد تئوری‌هایی برای تشخیص این‌که چه اتفاقی رخداده است و تایید یا رد آن با بررسی لاگ‌ها.



منابع لاگ که پتانسیل امنیتی دارند:

لاگ‌های مربوط به سیستم عامل سرورها و ایستگاه‌های کاری.
لاگ‌های مربوط به برنامه‌های کاربردی (وب‌سرویس، پایگاه‌داده و...)
لاگ‌های مربوط به ابزارهای امنیتی (آنتی‌ویروس، فایروال، IPS، IDS و...)
لاگ پروکسی‌های خروجی و برنامه‌های سمت کاربر نهایی (End-User application)

به‌خاطر داشته باشید بجز منابع لاگ‌ها سایر منابع را برای رویدادهای امنیتی بررسی کنید.

مسیرهای پیش‌فرض برای ذخیره‌سازی لاگ‌ها:

برای سیستم‌عامل لینوکس و برنامه‌های پایه نصب شده: /var/log
برای سیستم عامل ویندوز و برنامه‌های پایه: Windows Event Log
تجهیزات شبکه: معمولاً لاگ‌ها با استفاده از پروتکل Syslog ذخیره می‌شوند، برخی از آن‌ها نیز در مسیرها و فرمت‌های اختصاصی خود ذخیره می‌شوند.

در لاگ‌ها به دنبال چه باید گشت؟

در جداول صفحه بعد برخی از مواردی که در منابع لاگ‌ها نیاز است بررسی شوند آورده شده است. لازم به ذکر است که این موارد خلاصه شده‌اند و ممکن است در رخدادی های امنیتی موارد بیشتری نیاز به بررسی داشته باشند.

بررسی لاگ‌های لینوکس

ورود موفقیت آمیز کاربر	Accepted password", "Accepted publickey","session" "opened
ورود به سیستم‌های ناموفق کاربر	"authentication failure", "failed password"
خروج از سیستم کاربر	"session closed"
تغییرات در اکانت کاربر یا حذف آن	"password changed", "new user", "delete user"
دستوراتی که با sudo اجرا شده‌اند	"sudo: ... COMMAND=..." "FAILED su"
خرابی یا مشکل سرویس‌ها	"failed" or "failure"

بررسی لاگ‌های ویندوز

Event ID هایی که در زیر لیست شده‌اند برای ویندوز XP/2000 هستند، برای ویندوز 7/Vista نیاز است Event ID با شماره ٤٠٩٦ در بخش موردنظر اضافه شود. قابل ذکر است که موارد گفته شده به‌عنوان مثال آورده شده است و باید این لیست‌ها توسط فردی که لاگ‌ها را بررسی می‌کند مرتب به‌روزرسانی و ارتقا یابد.

رویدادهای مربوط به ورود و خروج کاربر	ورود موفقیت آمیز: ٥٢٨ , ٥٤٠ ورود ناموفق: ٥٢٩-٥٣٧ , ٥٣٩ خروج از سیستم: ٥٣٨ , ٥٥١
تغییرات حساب کاربری	ساخت اکانت: ٦٢٤ فعال‌سازی:٦٢٦ ایجاد تغییرات:٦٤٢ غیرفعال‌سازی: ٦٢٩ حذف شدن:٦٣٠
تغییر گذرواژه	برای خود:٦٢٨ برای دیگران:٦٢٧
شروع به کارکردن یا متوقف‌کردن یک سرویس	٧٠٣٥ , ٧٠٣٦
رد شدن دسترسی به یک شیء (اگر حسابرسی فعال باشد)	٥٦٠,٥٦٧

لاگ‌های دستگاه‌های شبکه

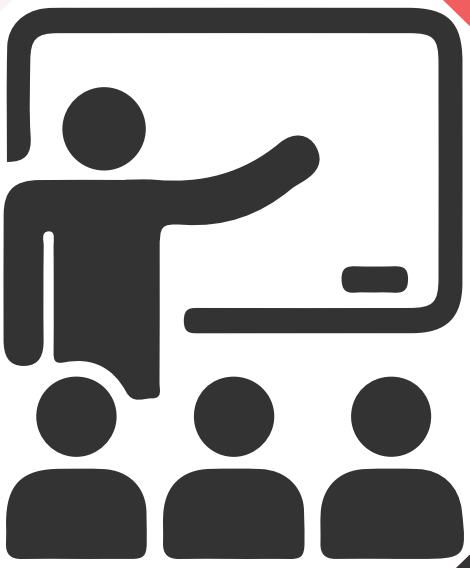
بررسی ترافیک فعالیت‌های ورودی و خروجی:
مثال‌های زیر از Cisco ASA logs آورده شده است. سایر دستگاه‌ها نیز عملکرد مشابهی دارند.

ترافیکی که در دیواره‌آتش اجازه عبور گرفته است	“Built ... connection”, “access-list ... permitted”
ترافیکی که در دیواره‌آتش مسدود شده است	“access-list ... denied”, “deny inbound”; “Deny ... by
بایت‌های انتقال یافته (آیا فایل حجیمی ارسال شده؟!)	“Teardown TCP connection ... duration ... bytes ...”
پهنای باند و پروتکل‌های استفاده شده	“limit ... exceeded”, “CPU utilization”
فعالیت‌های مربوط به حملات تشخیص داده شده	“attack from”
تغییرات در حساب کاربری	“user added”, “user deleted” “User priv level changed”
دسترسی مدیریتی	“AAA user ...”, “User ... locked out”,“login failed”

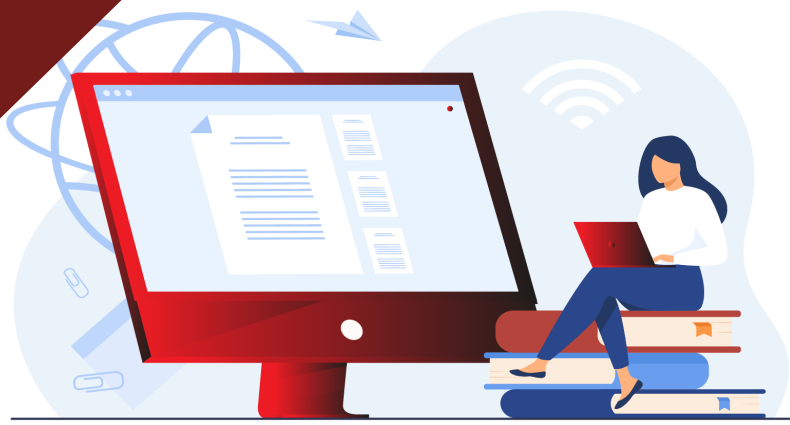
لاگ‌های وب‌سروها

درخواست دسترسی بیش از حد معمول به فایلی که وجود ندارد.
مشاهده کدهای متفاوت (HTML یا SQL) به‌عنوان بخشی از URL
درخواست دسترسی به پسوندهایی که توسط شما تعریف نشده است.
توقف، شروع به کار یا با خطا مواجه‌شدن یک وب‌سرویس.
دسترسی پیداکردن به یک صفحه خطرناک که از کاربر ورودی قبول می‌کند.
بررسی لاگ تمامی سرورهای موجود در استخر مربوط به load balancer
پاسخ با کد ۲۰۰ برای فایلی که متعلق به شما نیست.

احراز هویت ناموفق کاربر	Error code:401-403
درخواست اشتباه	Error code:400
خطای داخلی سرور	Error code:500



معرفی دوره



معرفی دوره Complete Digital Forensics Masterclass

هادی گلباغی

مقدمه

مرکز Udemy به‌عنوان یکی از پیشروترین سازمان‌ها در امر ارائه آموزش‌های گسترده و جامع در زمینه‌های مختلف از جمله امنیت اطلاعات در دنیا شناخته می‌شود و دارای ده‌ها هزار آموزش و دوره آنلاین است. این مرکز در بسیاری از حوزه‌ها، دوره‌هایی با هدف مهارت‌آموزی برای کاربران برگزار کرده است. Udemy تا آوریل ۲۰۲۱ دارای ۴۰ میلیون دانش‌آموز، ۱۵۵ هزار دوره، ۷۰ هزار مدرس و بیش از ۴۸۰ میلیون دوره ثبت‌نام شده، بوده است. این مرکز در سال‌های اخیر دوره‌های بسیار خوبی در حوزه امنیت‌سایبری برگزار کرده است که در این مطلب، دوره جرم‌شناسی دیجیتال Complete Digital Forensics Masterclass را معرفی خواهیم کرد.

مشخصات دوره آموزشی

ناشر: Udemy
مدرس: TechBinz Academy
سطح: پیشرفته
مدت زمان: ٦ ساعت و ۳۵ دقیقه
تعداد دروس: ۱۱ بخش، ۳۰ درس
زبان: انگلیسی

این دوره یکی از جامع‌ترین دوره‌ها در زمینه جرم‌شناسی دیجیتال است که در آن نگاه عمیقی درخصوص این‌که سیستم‌های کامپیوتری چگونه کار می‌کنند و به چه شکل می‌توان جرم‌شناسی دیجیتال را در آن انجام داد، ایجاد می‌شود. سرفصل‌های این دوره به‌صورت مداوم در حال ارتقاء بوده و سرفصل حاضر نیز در ماه جولای ۲۰۲۱ به‌روزرسانی شده است.

می‌توان از جرم‌شناسی دیجیتال به‌عنوان فرایندی به منظور شناسایی، استخراج شواهد و مستندسازی در رخدادها، حملات سایبری و پرونده‌های قضایی و جنایی استفاده کرد. این مهارت برای شناسایی شواهد مختلف در انواع سیستم‌ها، بسترهای ارتباطی و حافظه‌های ذخیره‌سازی مانند کامپیوتر، تلفن همراه، سیستم‌عامل، حافظه موقت و ثانویه، سرور و یا شبکه کاربرد دارد. این دوره سعی دارد بهترین مهارت‌ها، ابزارها و تکنیک‌ها را برای حل موارد پیچیده در اختیار مهارت‌آموزان قرار دهد. دوره Digital Forensics به تیم جرم‌شناسی کمک می‌کند تا شواهد دیجیتال را از سیستم‌ها، بسترهای ارتباطی و رسانه‌های مختلف ذخیره‌سازی استخراج کرده تا بر روی آن‌ها شناسایی، تجزیه و تحلیل و مستندسازی لازم صورت گیرد.

جرم‌شناسی دیجیتال کاربردهای گوناگونی دارد. رایج‌ترین کاربردهای آن مربوط به حملات و رخدادهای سایبری، امور جنایی و قضایی و کلاهبرداری‌ها است. هدف از جرم‌شناسی دیجیتال جستجو، کشف و تحلیل اطلاعات و شواهد احتمالی در حملات، رخدادها و پرونده‌های قضایی است. معمولاً در چنین مواردی، منابع بسیاری برای تیم جرم‌شناسی به‌منظور بررسی و تحلیل وجود دارد که گاه این منابع مختلف با حجم بالا سردرگم‌کننده بوده و روال شناسایی و تحلیل شواهد احتمالی را بسیار کند می‌کند. با این حال در این دوره، موارد اساسی درخصوص جرم‌شناسی دیجیتال و چک‌لیست‌های لازم به منظور بررسی و تحلیل در بسترهای مختلف مدنظر قرار می‌گیرد که تا حد زیادی می‌تواند مسیر انجام این فرایند را برای تیم جرم‌شناسی روشن سازد. در این دوره که با روش‌ها و تکنیک‌های جرم‌شناسی بر روی سیستم‌عامل‌های ویندوز و اندروید آشنا خواهید شد، دسته‌بندی‌های مختلفی از جرم‌شناسی دیجیتال ارائه خواهد گردید. انواع مختلف حافظه و ویژگی‌های آن‌ها معرفی می‌شوند و روش‌ها و تکنیک‌های پیشرفته تحلیل و بررسی حافظه موقت و ثانویه برای فرآیند جرم‌شناسی را فرا خواهید گرفت. برای انجام جرم‌شناسی یک آزمایشگاه با Caine OS راه‌اندازی می‌شود و راهکارهای شناسایی و تحلیل شواهد دیجیتال بیان خواهد شد. یکی دیگر از بخش‌های این دوره مربوط به جرم‌شناسی از مرورگرهای وب است و در بخشی دیگر جرم‌شناسی تلفن‌همراه بررسی شده است.

به‌دلیل اینکه حوزه تکنولوژی‌های نوین به شدت در حال پیشرفت بوده و روز به روز تغییرات را در این عرصه شاهد هستیم، مهارت‌ها و تکنیک‌های حوزه جرم‌شناسی دیجیتال نیز سریع‌تر از سایر زمینه‌ها در حال تکامل و تغییر است، یک متخصص حوزه جرم‌شناسی نیز باید همگام با این تغییرات، دانش و مهارت خود را به‌روز کرده و با تکنیک‌ها و ابزارهای جدید آشنا باشد. یکی از دلایلی که سرفصل‌های این دوره نیز به صورت مداوم بازنگری شده و به‌روزرسانی می‌شود، همین مسئله است.

- Introduction
  - Digital Forensics Categories
  - Cybercrime Types
- Memory Types
  - Volatile Memory
  - Non-Volatile Memory
  - Memory Types Practice Test
- Preparing Lab
  - Installing FTK Imager
  - Installing Caine OS
- Storage Acquisition
  - Storage Acquistion Tutorial
  - Hashing Evidence
  - Storage Acquistion Example
  - Cyber Crime
- Memory Acquisition
  - Windows RAM Acquisition with FTK Imager
  - Windows RAM Acquisition with Magnet
- Evidence Analysis
  - Windows RAM Analysis - Volatility Part 1
  - Cridex Malware Analysis - Volatility Part 2
  - Metadata Fundamentals
- Autospy
  - Autopsy Storage Evidence Analysis
- Web Browser Forensics
  - Chrome, Opera, Yandex Browser Forensics
- Mobile Forensics
  - Mobile Forensics Potential Evidence
  - Mobile Forensics Fundamentals
  - Lockscreen Cracking without Data Loss
- Android Forensics
  - Installing and Configuring Emulator
  - Android Architecture
  - Android Security
  - Android File Structure
  - Installing TWRP Android
  - Root in Theory
- Additional Lectures
  - Digital Forensics Patterns
  - Digital Forensics 2

آنچه خواهید آموخت:

مقدمات جرم‌شناسی دیجیتال
دسته‌بندی‌های مختلف جرم‌شناسی دیجیتال
جرم‌شناسی سیستم کامپیوتری
جرم‌شناسی تلفن همراه
جرم‌شناسی ایمیل
جرم‌شناسی مرورگر وب
انواع بازرسی در جرم‌شناسی دیجیتال
جمع‌آوری و تحلیل شواهد جرم‌شناسی در تلفن همراه
جمع‌آوری و تحلیل شواهد جرم‌شناسی در سیستم کامپیوتری
چگونگی بررسی حافظه ذخیره‌سازی
چگونگی بررسی حافظه موقت
نصب آزمایشگاه جرم‌شناسی (Caine OS)

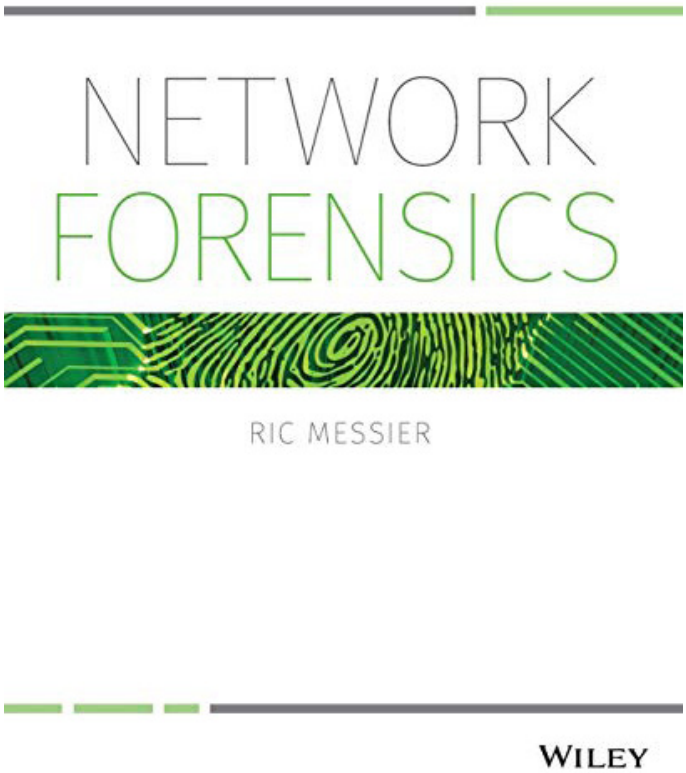
مخاطبان دوره:

کارشناسان شبکه
کارشناسان جرم‌شناسی
کارشناسان امنیت سایبری
علاقمندان به حوزه جرم‌شناسی دیجیتال

لینک دوره

معرفی کتاب

معرفی کتاب



نازیلا خسروی

تعاریف

Forensic در لغت به معنی جرم‌شناسی است و به روش‌های علمی اشاره دارد که برای کشف جرم استفاده می‌شود. در واقع Forensic جمع‌آوری و تجزیه‌وتحلیل تمام شواهد فیزیکی مرتبط با جرم است تا بتواند در مورد مظنون نتیجه‌گیری کند.

Network Forensics یکی از زیرشاخه‌های جرم‌شناسی دیجیتال است.
این امر برای جمع‌آوری اطلاعات مهم و شواهد قانونی مربوط به نظارت و تجزیه‌وتحلیل ترافیک شبکه‌های رایانه‌ای می‌باشد.

درباره‌ی نویسنده

Ric Messier نویسنده، مشاور و مربی امنیتی است که گواهینامه‌های CEH، GSEC، GCIH، CCSP و CISSP را دارا می‌باشد، همچنین چندین کتاب در زمینه‌ی امنیت اطلاعات و Digital Forensics منتشر کرده است.
او با چندین دهه تجربه در زمینه فناوری اطلاعات و امنیت اطلاعات، مسئولیت‌های متنوعی همچون برنامه نویس، مدیر سیستم، مهندس شبکه، مدیر مهندسی امنیت، مشاور و استاد را برعهده داشته است. او در حال حاضر مشاور امنیت اصلی FireEye Mandiant است.

درباره‌ی کتاب

کتاب Network Forensics یک راهنمای کاربردی منحصربه‌فرد برای متخصصان فناوری اطلاعات و جرم شناسان دیجیتال است که به دنبال درک عمیق‌تری از امنیت سایبری هستند. این کتاب در همه‌ی زمینه‌های جرم‌شناسی دیجیتال کاربردی است و دانش اساسی که فقط از تجربه حاصل می شود را در اختیار شما قرار می‌دهد. در بخش‌هایی از این کتاب، برای انجام جرم‌شناسی بررسی بسته‌ها در ترافیک شبکه و فایل‌های لاگ مدنظر است و به روش‌های یادگیری با انجام مهارت‌هایی اساسی که ممکن است جرم‌شناسان سنتی نداشته باشند، تاکید دارد. این کتاب تکنیک‌های مهمی را اساس کار قرار می‌دهد که شواهدی عینی را به معرض نمایش می‌گذارد، از تجزیه‌وتحلیل بسته‌های شبکه گرفته تا دستگاه‌های ارتباطی میزبان و تجزیه‌وتحلیل ورود به سیستم و فراتر از آن.

داده‌های شبکه همیشه در حال تغییر هستند و هرگز در یک مکان ذخیره نمی‌شوند. یک محقق باید نحوه بررسی داده‌ها که شامل مهارت‌هایی تخصصی فراتر از حافظه، تلفن همراه یا جرم‌شناسی داده است را در طول زمان درک کند.

این مسئله که آیا شما برای دریافت یک گواهینامه امنیتی آماده می‌شوید یا فقط به دنبال آموزش‌های عمیق‌تر برای اجرای قانون یا یک مسئولیت در شغل فناوری اطلاعات هستید، فقط منجر به یادگیری موارد زیادی از مفهوم می‌شود درحالی‌که برای درک کامل یک موضوع، باید آن را به صورت عملی انجام دهید. کتاب Network Forensics تمرینات عملی فشرده‌ای را در ارتباط با رخدادهای واقعی ارائه می‌دهد.

جرم‌شناسی شبکه، یک زمینه رو به رشد است که با پیچیده‌تر شدن جرایم رایانه‌ای به‌طور فزاینده‌ای در اجرای قانون مورد توجه قرار گرفته است. این کتاب سطح بی‌سابقه‌ای از آموزش‌های عملی را از مهارت‌های مورد نیاز به محققان ارائه می‌دهد. این آموزش‌ها شامل:

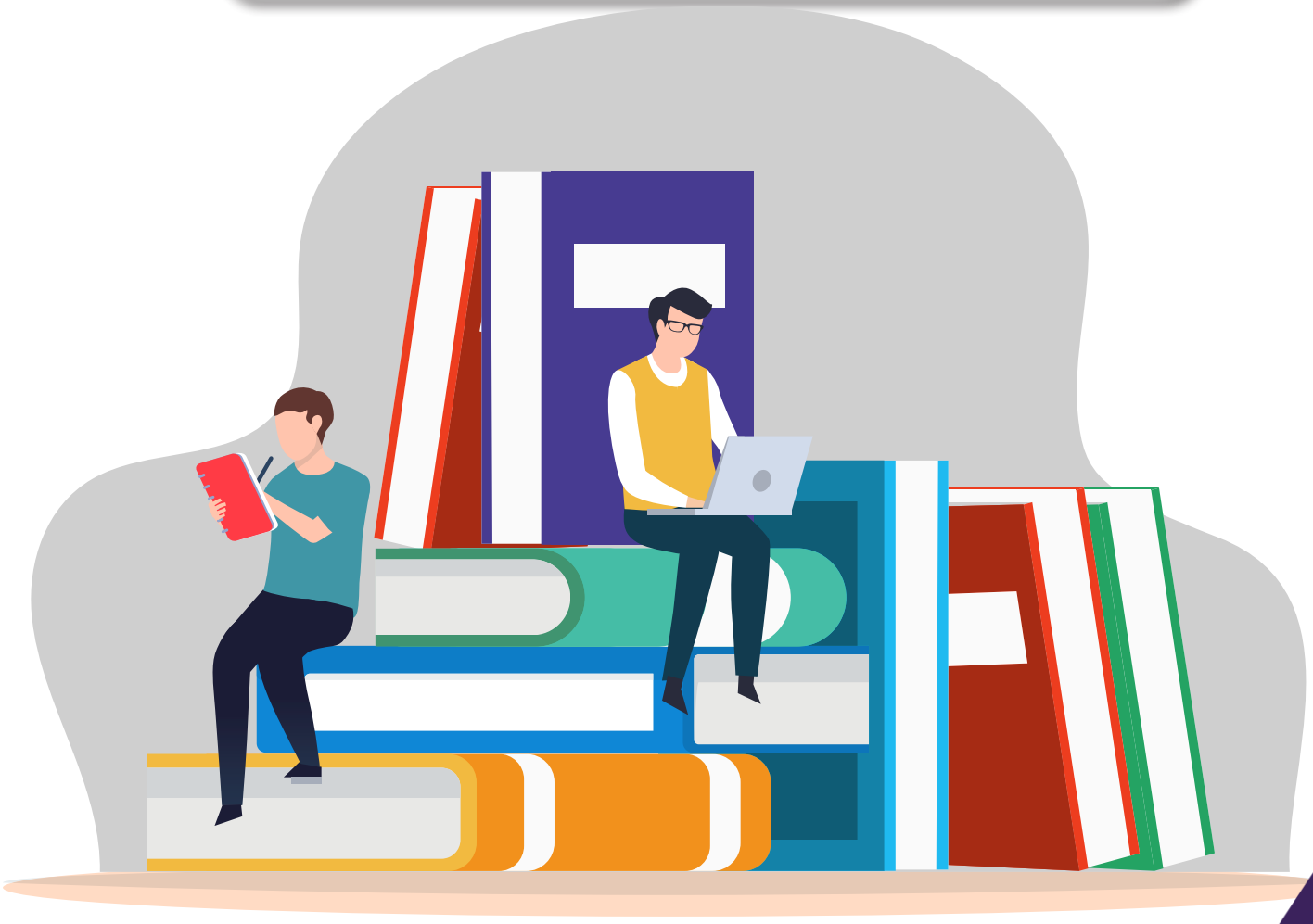
- وارسی بسته‌های رکورد شده جهت بررسی ارتباطات شبکه
- تعیین تجهیزات میزبان و تجزیه‌وتحلیل گزارش‌های شبکه
- شناسایی سیستم‌های تشخیص نفوذ
- داشتن معماری و سیستم‌های مناسب پیش از وقوع حادثه

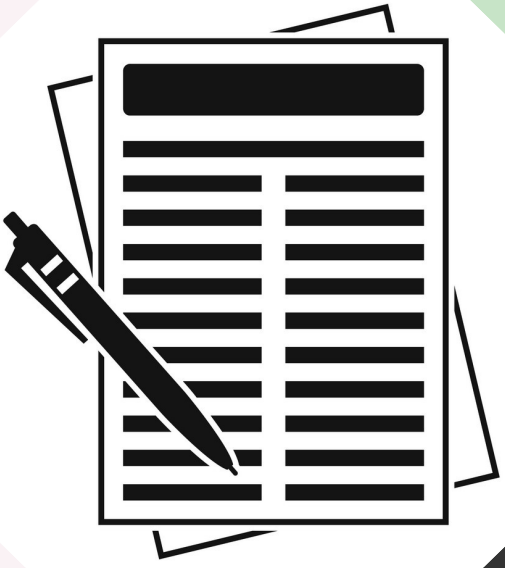
مشخصات کتاب

نام کتاب	Network Forensics
نویسنده	Ric Messier
زبان	English
تعداد صفحات	360
ناشر و سال انتشار	Wiley; 1st edition (August 2017 ,7)

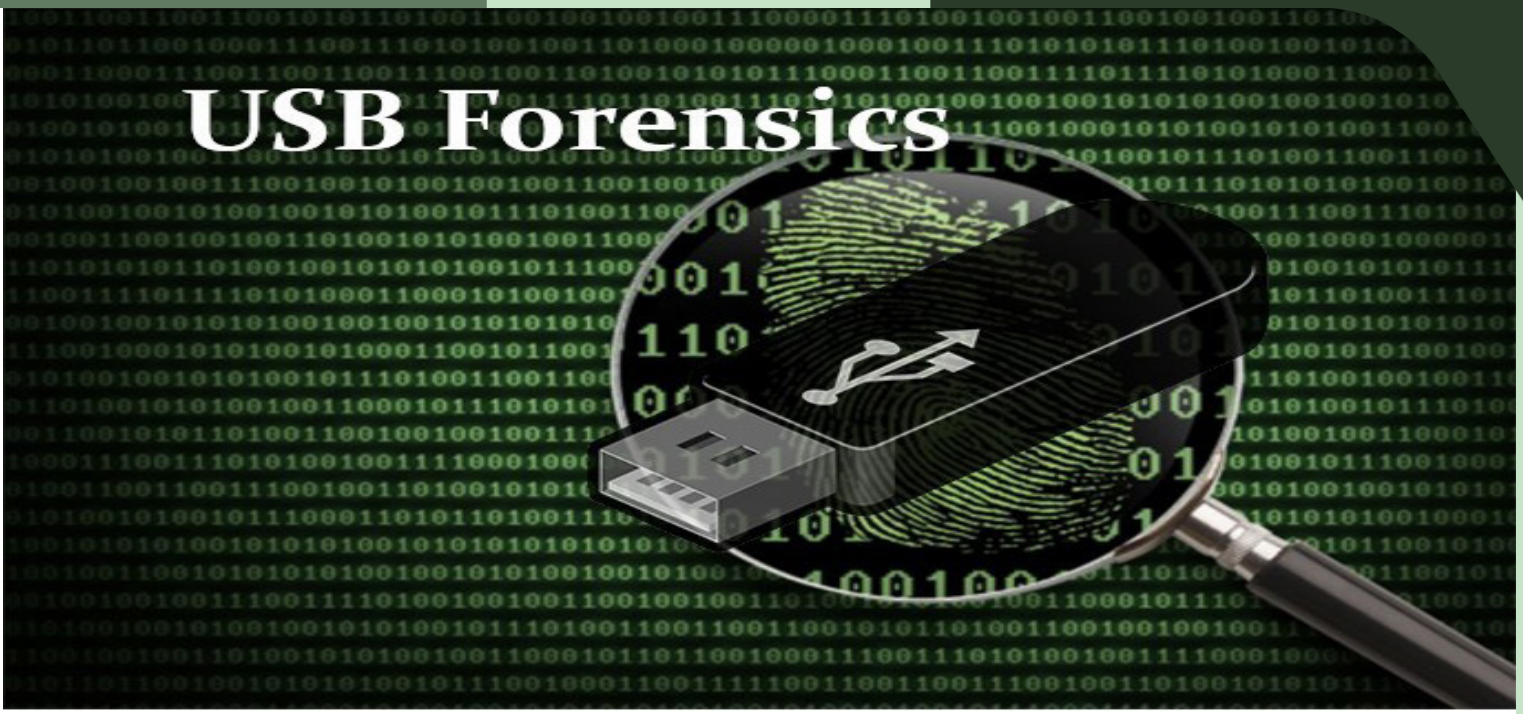
لینک کتاب

- 1 Introduction to Network Forensics
- 2 Networking Basics
- 3 Host-Side Artifacts
- 4 Packet Capture and Analysis
- 5 Attack Types
- 6 Location Awareness
- 7 Preparing for Attacks
- 8 Intrusion Detection Systems
- 9 Using Firewall and Application Logs
- 10 Correlating Attacks
- 11 Network Scanning
- 12 Final Considerations





مقاله تحقیقاتی



جرم‌شناسی USB - بازسازی شواهد دیجیتال از درایو USB

تینا احمدی

مقدمه

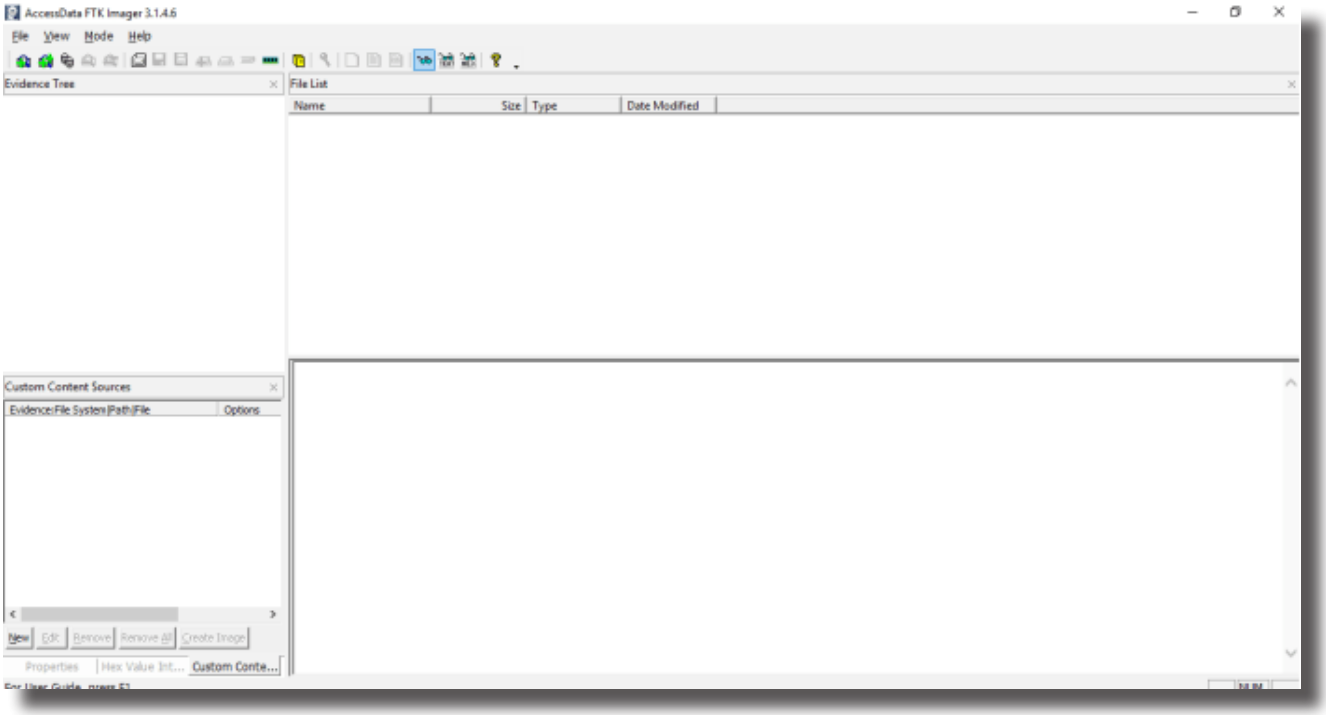
آنالیز جرم‌شناسی دیجیتال حافظه USB شامل حفظ، جمع‌آوری، اعتبارسنجی، شناسایی، تجزیه و تحلیل، تفسیر مستندات و ارائه شواهد دیجیتال مشتق‌شده از منابع دیجیتال به‌منظور تسهیل یا پیش‌برد بازسازی وقایع مجرمانه، شناخته شده است.

Disk Image - جرم‌شناسی USB

- Disk Image به‌عنوان یک فایل رایانه‌ای تعریف می‌شود که شامل محتویات و ساختار یک دستگاه ذخیره اطلاعات مانند هارد دیسک، درایو CD، تلفن، رایانه لوحی، RAM یا USB است.
- Disk Image شامل محتوای واقعی دستگاه ذخیره اطلاعات و همچنین اطلاعات لازم برای شبیه‌سازی ساختار و طرح محتوای دستگاه است.
- با این وجود طبق محکمه قضایی برای انجام تجزیه و تحلیل از طیف گسترده‌ای از ابزارهای شناخته‌شده استفاده می‌شود.
- طبق قانون صرفاً استفاده از ابزارهای استاندارد مجاز است و بازرسان جرم‌شناسی برای ایجاد Disk Image نباید از ابزارهای ناشناخته‌ی جدید استفاده کنند.
- **ابزارهای استاندارد:** ابزار Encase Forensic Imager و پسوند آن (Imagename.E01) که یک جعبه ابزار جرم‌شناسی برای ایجاد Image و آنالیز آن است. فرایند کار با استفاده از نرم افزار FTK Forensic ساخته شده توسط AccessData انجام می‌شود.
- FTK یک ابزار ساده و مختصر مستقل برای ایجاد Image است.

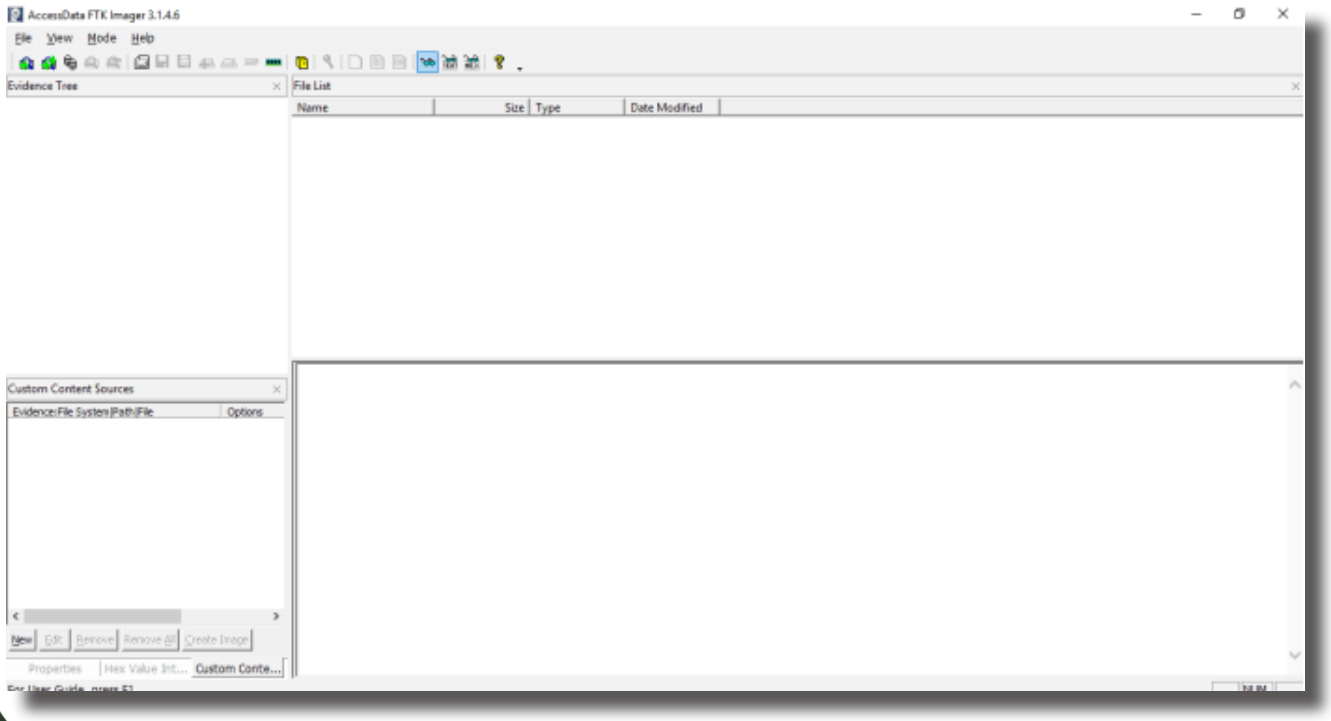
FTK Imager

در شکل زیر پنل Access data FTK Imager نمایش داده شده است.

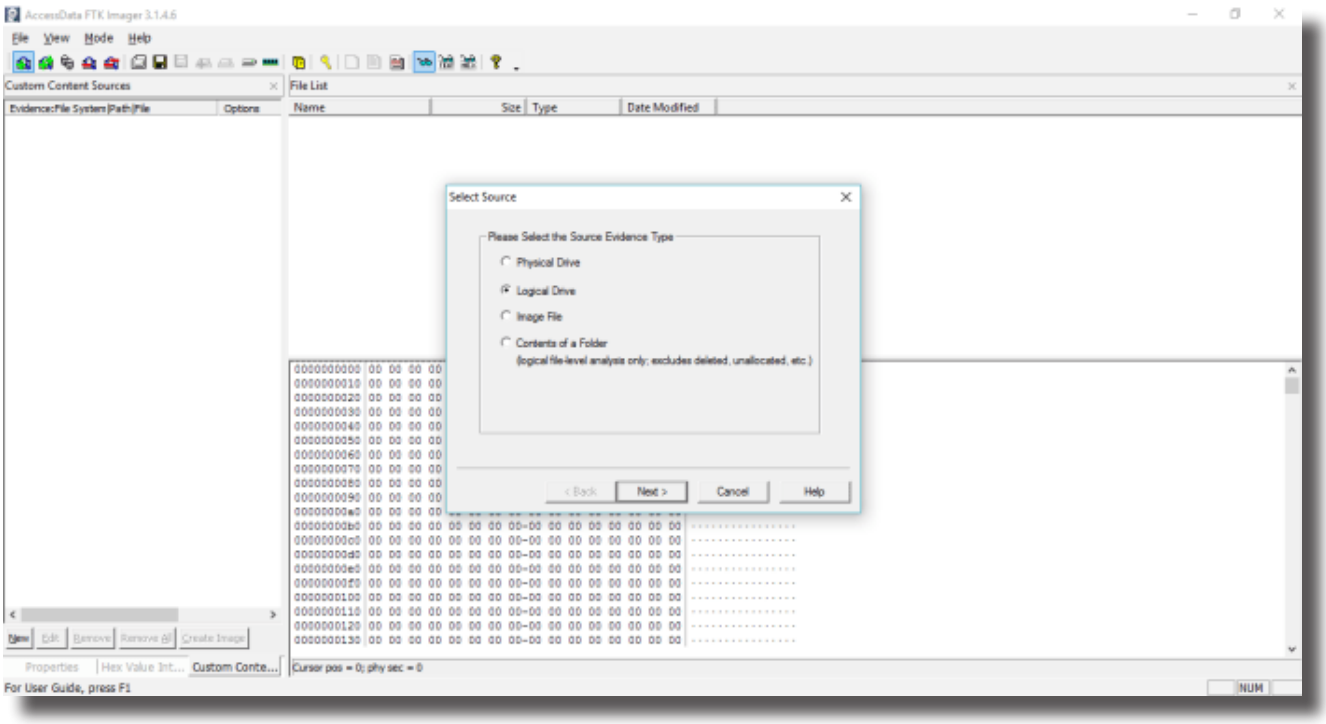


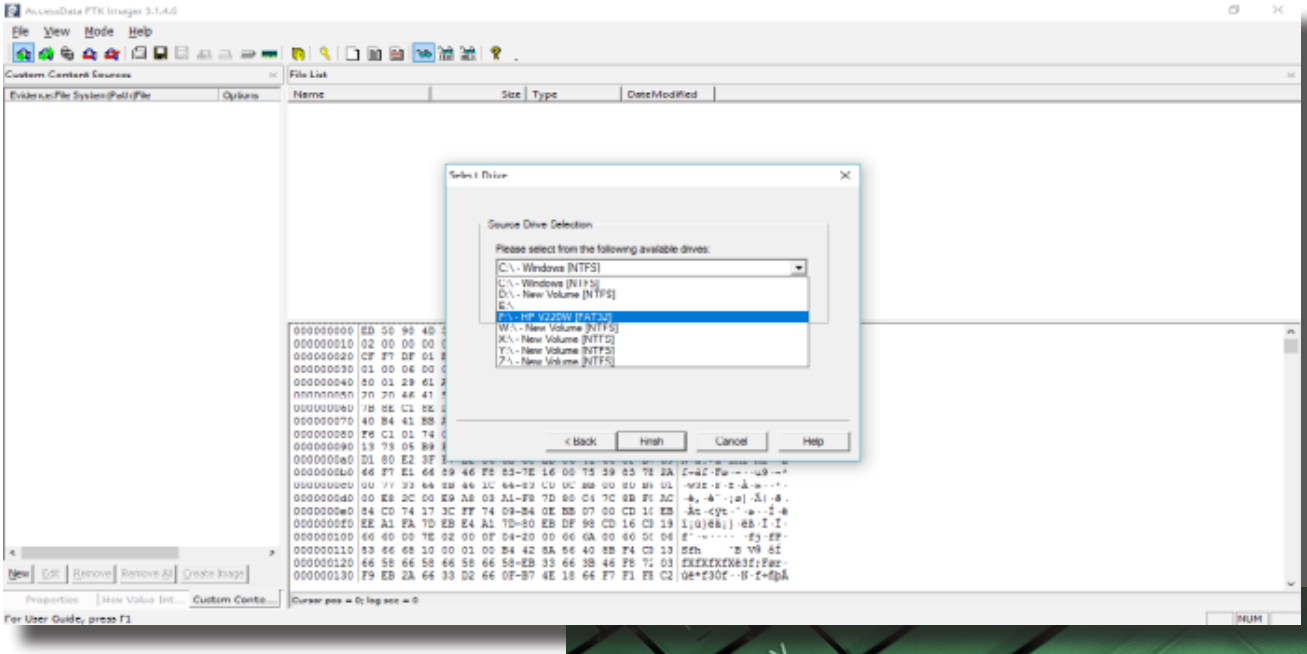
درخت شواهد (Evidence)

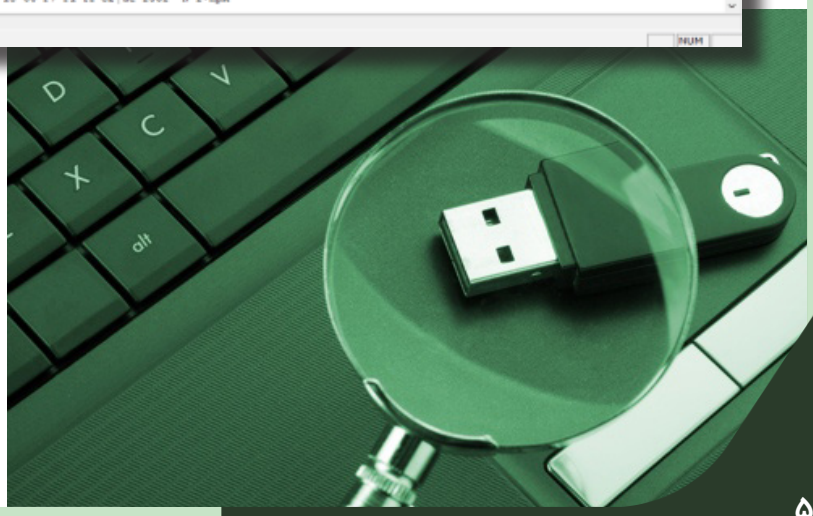
برای افزودن شواهد به پنل، روی دکمه سبز رنگ بالا سمت چپ کلیک کرده و نوع منبع شواهد را انتخاب کنید. منبع انتخاب شده درایو منطقی (USB) است.



همانند تصاویر زیر در Wizard ابتدا Logical Drive سپس USB درایو HP را برای آنالیز انتخاب کنید.

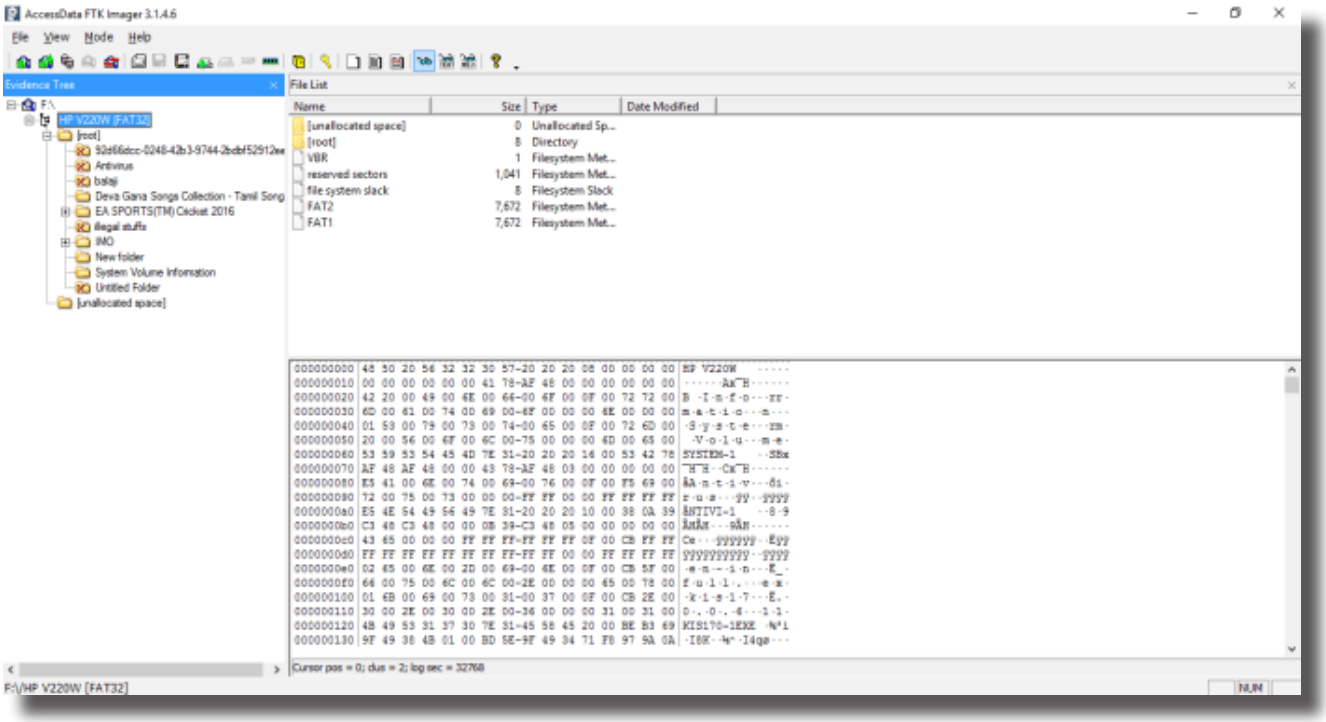






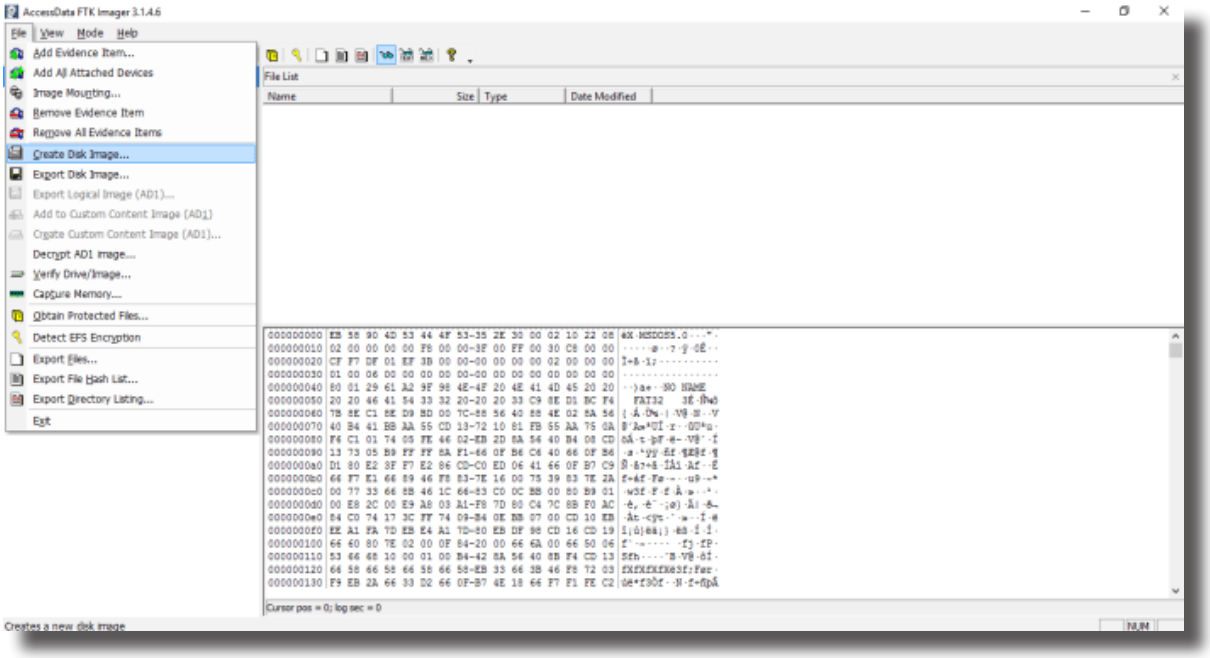
در بخش درخت شواهد درایو USB نمای کلی از داده‌های پاک شده در گذشته، نمایش داده شده است. می‌توان با بررسی‌های بیشتر نوع شواهد حذف شده را مشخص کرد.

توصیه می‌شود در تحقیقات، با شواهد اصلی کار نکنید زیرا کپی‌کردن تصادفی داده‌های جدید در USB، پرونده‌های پاک‌شده قبلی را در USB رونویسی می‌کند و یکپارچگی شواهد از بین می‌رود، بنابراین همیشه با کپی Image جرم‌شناسی کار کنید.



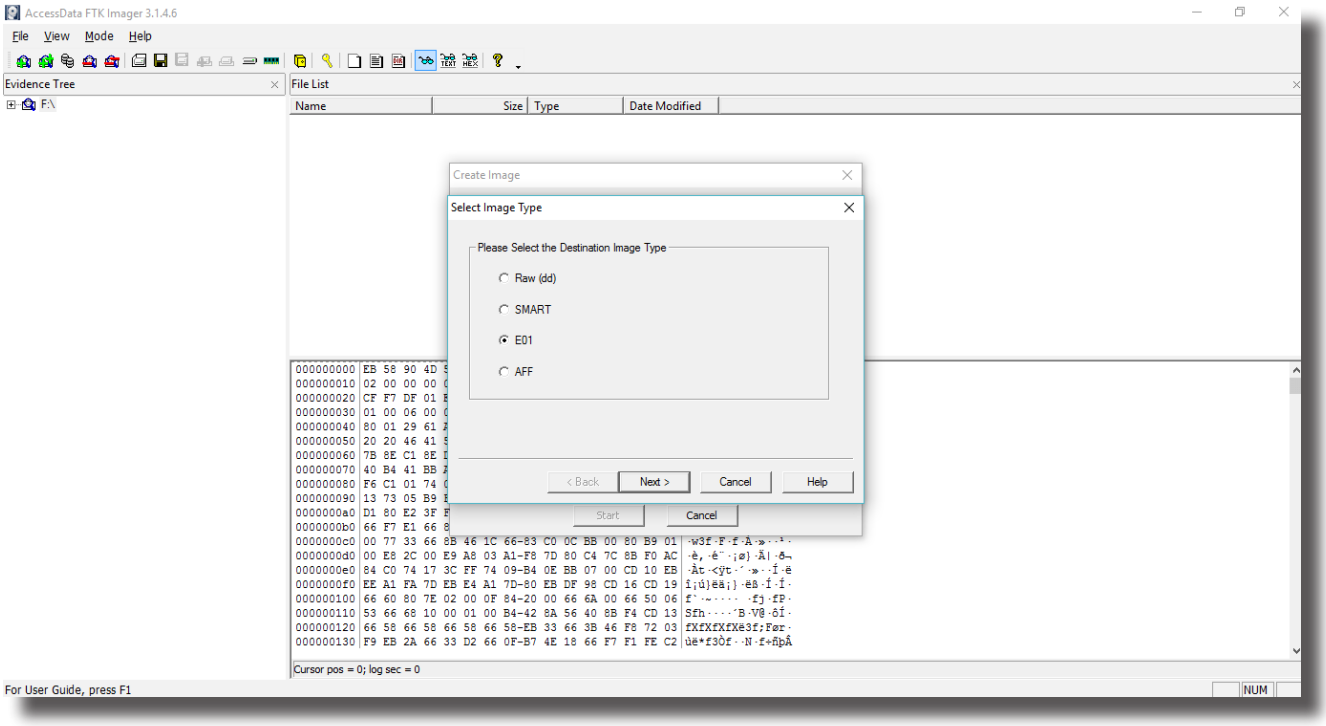
ایجاد Image از USB

از منوی File، گزینه Create Disk Image را انتخاب کنید.



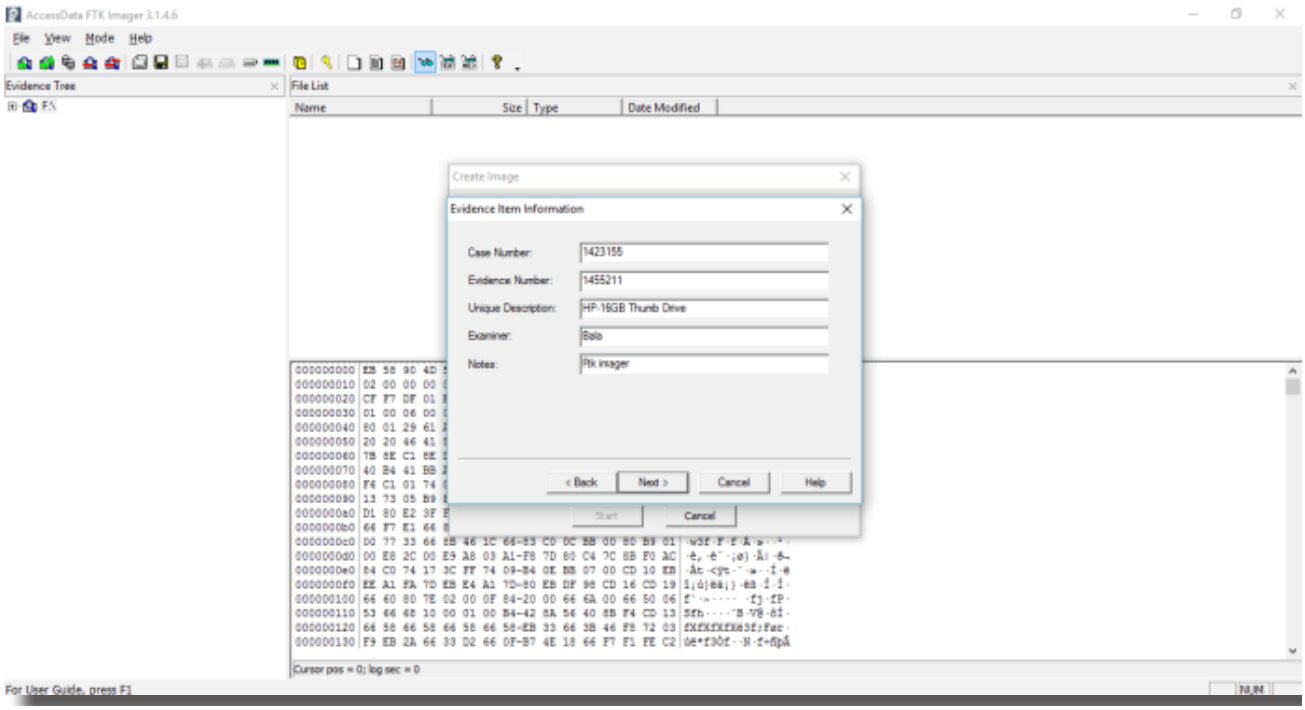
فرمت Image دیسک

برای انتخاب فرمت Image همانند تصویر زیر روی دکمه افزودن، کلیک کنید و نوع مناسب فرمت Image گزینه E01 را انتخاب کنید.



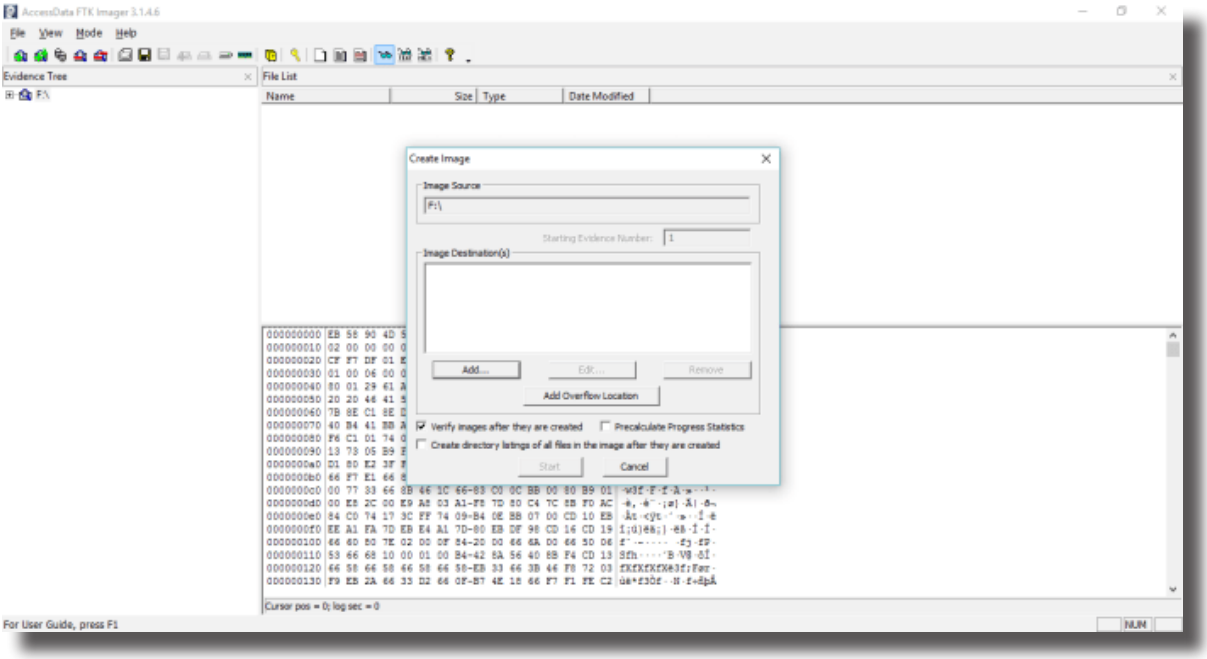
اطلاعات شواهد

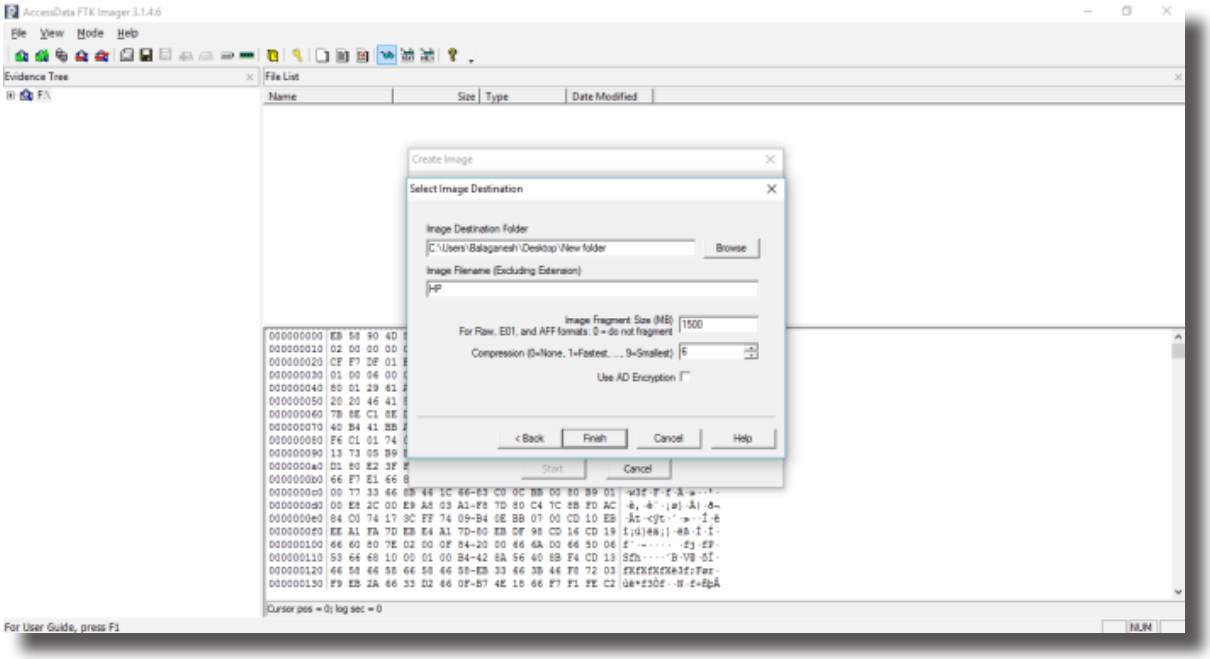
الزامی است که اطلاعات بیشتری در مورد نوع درایو USB، حجم، رنگ و اطلاعات هویتی بیشتر در مورد شواهد اضافه کنید.



مقصد Image

مسیر مقصد محل ذخیره‌سازی فایل Image از درایو USB آدرس C:\Users\Balaganesh\Desktop\Newfolder و نام فایل Image نیز HP Thumb Drive است.





شکل زیر نشان می‌دهد که فرایند ساخت image با فرمت USB.E01 در حال انجام است. ایجاد فایل Image چند دقیقه تا چند ساعت طول خواهد کشید.

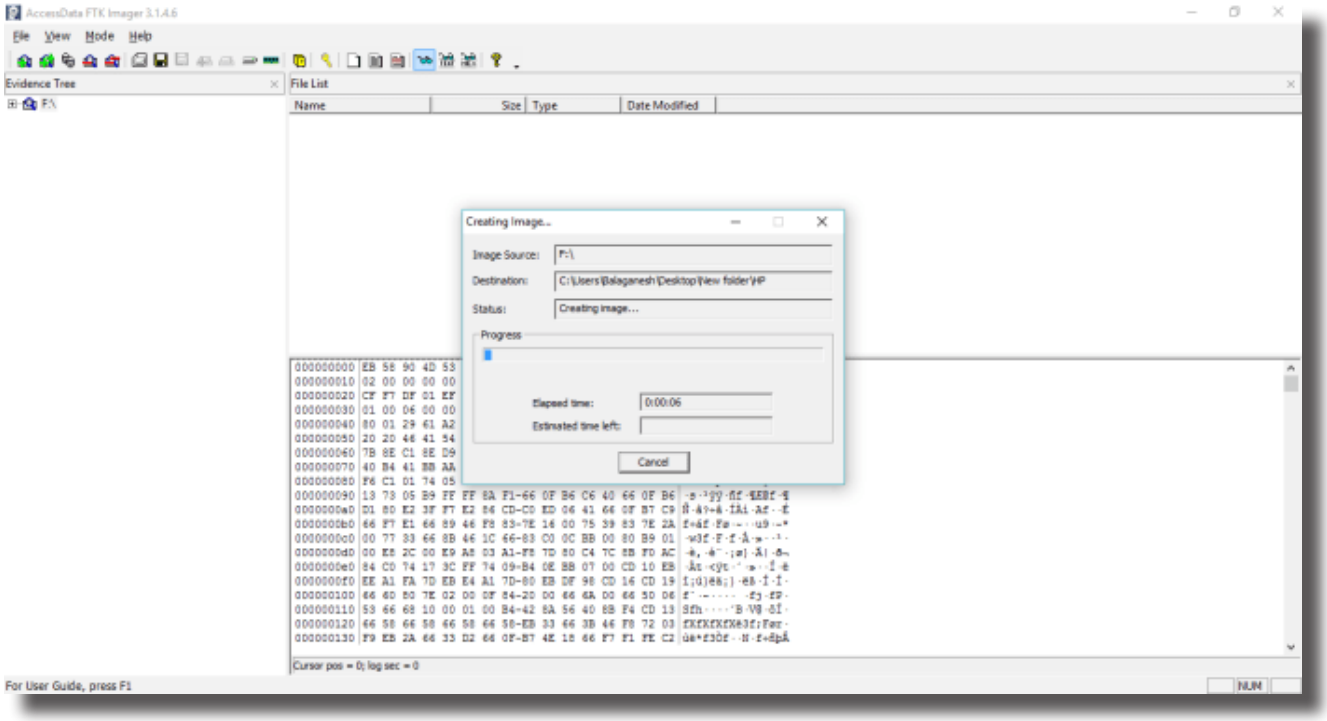
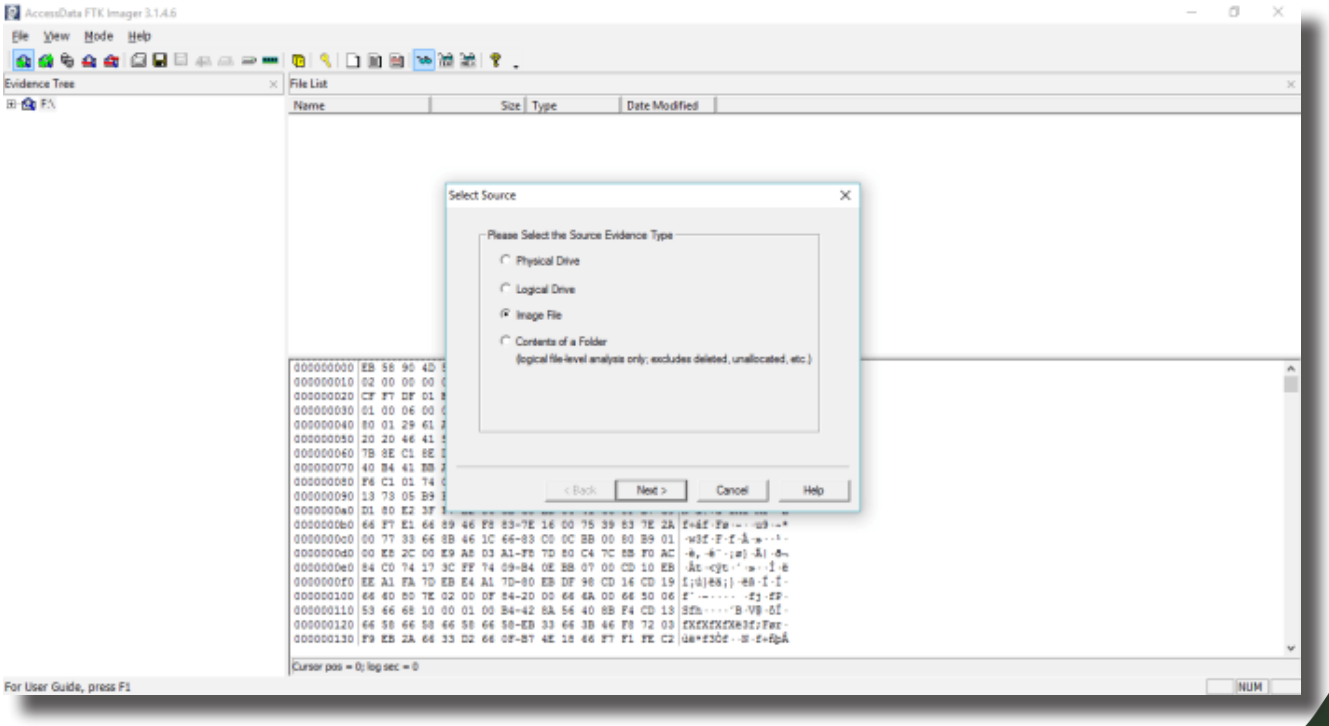


Image - جرم‌شناسی

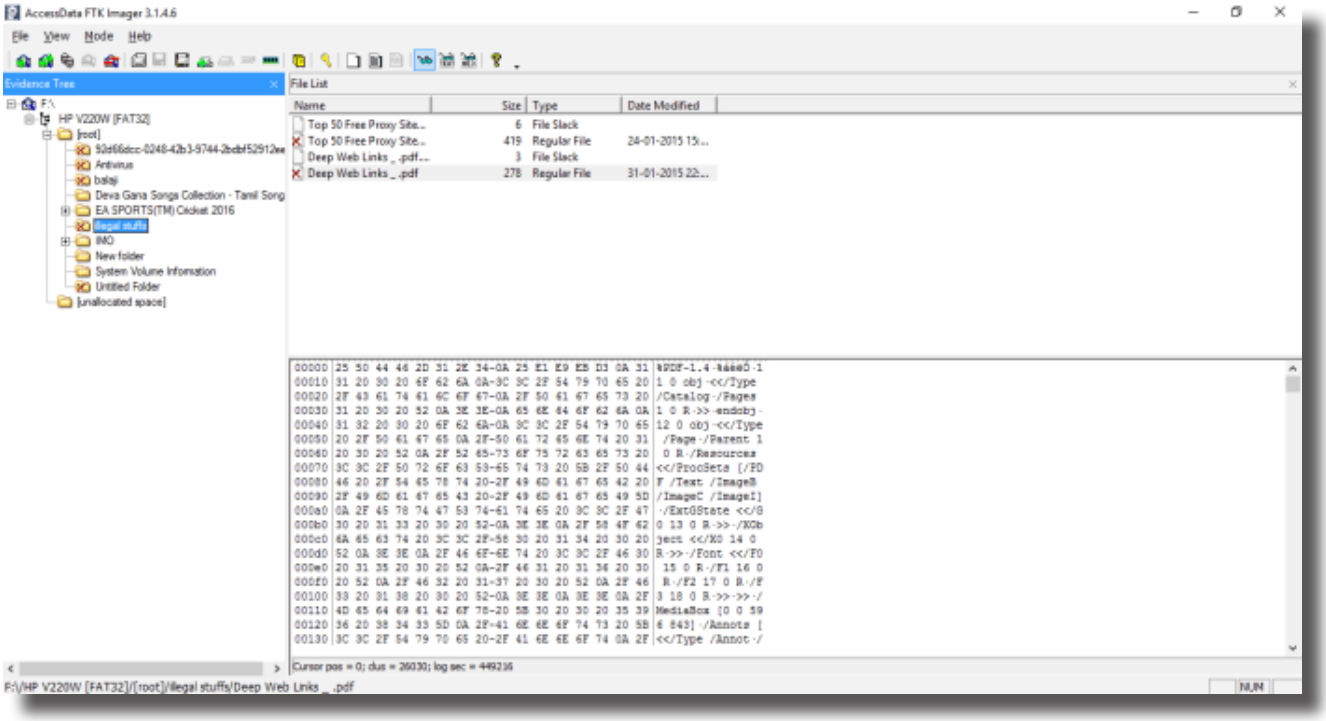
درایو USB را جدا کنید و شواهد اصلی را ایمن نگه دارید و همیشه با Image جرم‌شناسی کار کنید.

- شکل زیر نسخه Image جرم‌شناسی را نشان می‌دهد که باید انتخاب شود. در اینجا تصویر جرم‌شناسی HP.E01 است.



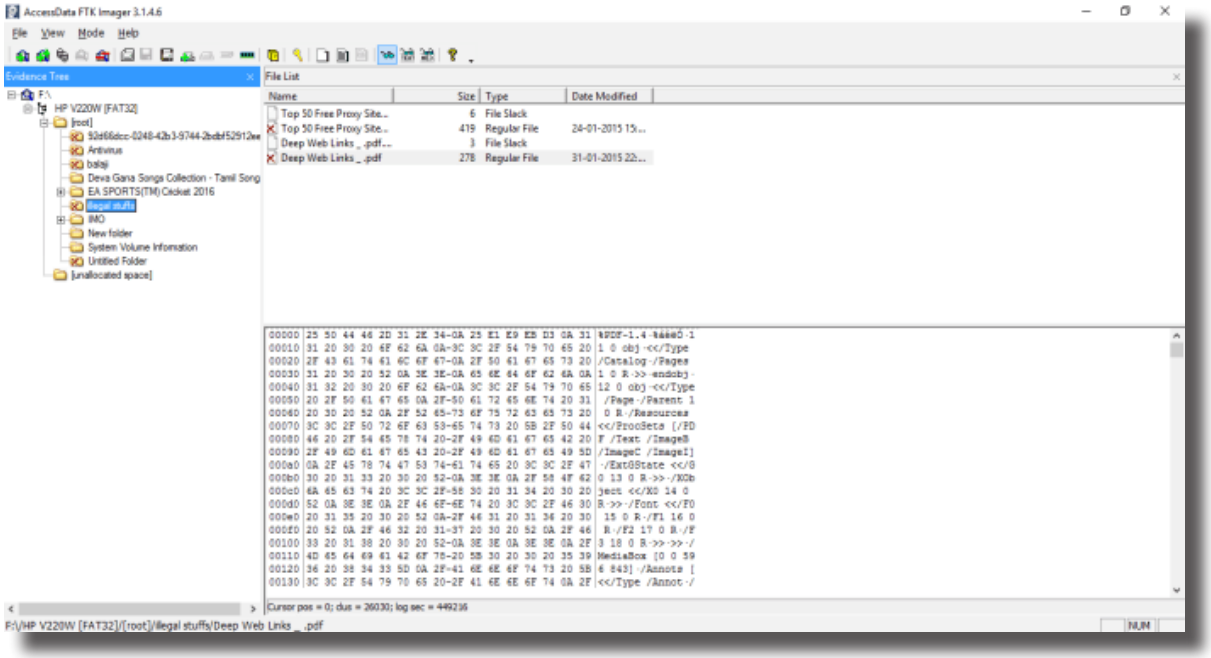
تجزیه و تحلیل شواهد دیجیتال

عکس زیر برخی از فعالیت‌های مشکوک را نشان می‌دهد که احتمالاً در درایو USB پیدا می‌شود که شامل انتی ویروس، موارد غیرقانونی و بیشتر پوشه‌های دیگری که حذف شده‌اند می‌باشد.



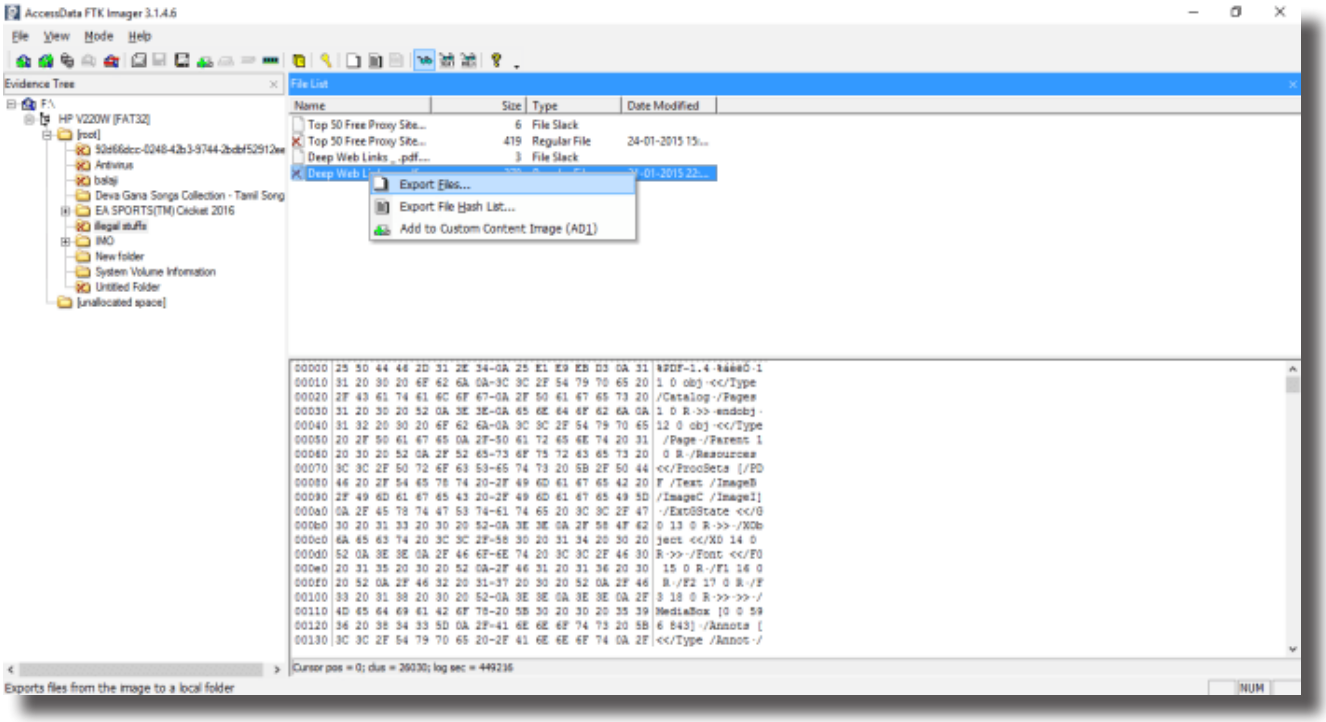
بازیابی فایل‌ها و پوشه‌های حذف شده

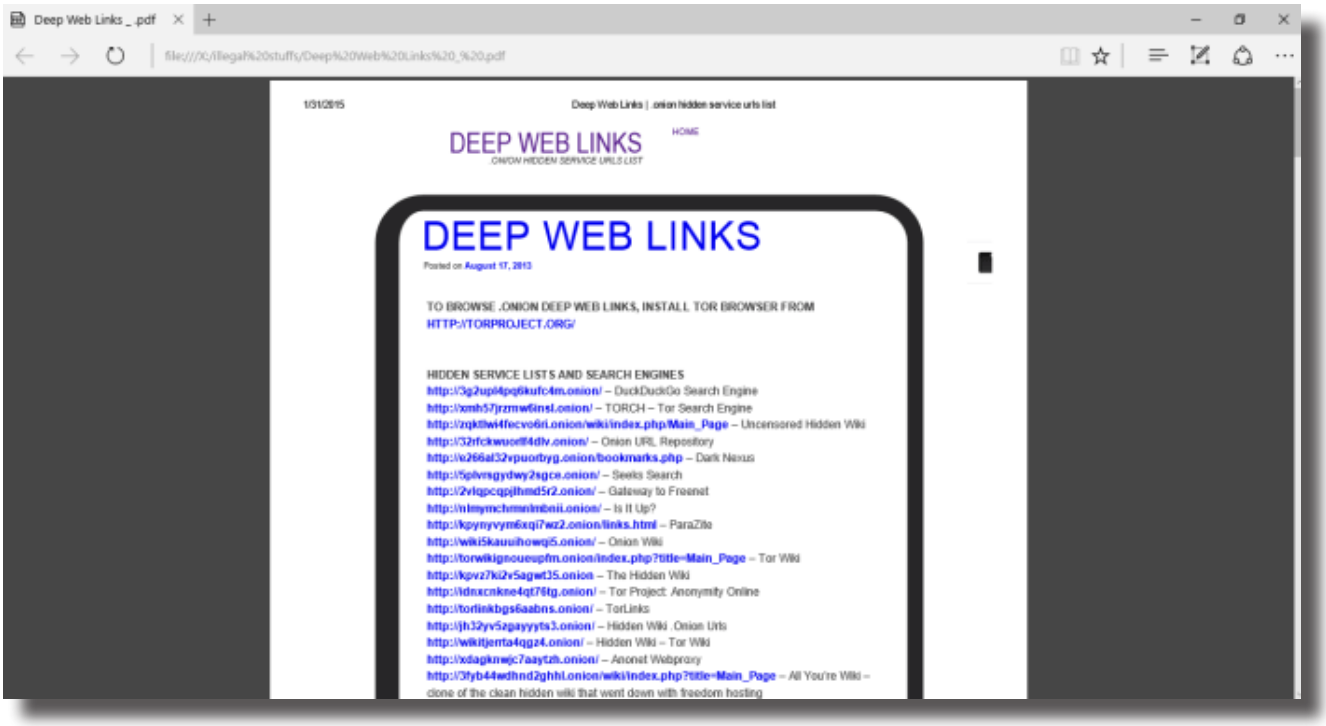
در اینجا متوجه شدیم، USB شامل برخی از نام فایل‌های مشکوک در قالب pdf است.



استخراج شواهد

سرانجام، ما لینک‌های مخرب Tor را با فرمت onion. ، با فرمت pdf به‌عنوان مدرک بازیابی کردیم.

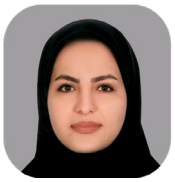




در برخی موارد فایل‌های استخراج شده ممکن است محتوایی نداشته باشند و این نشان می‌دهد که فایل‌های جدید به جای آن‌ها بازنویسی شده‌اند. در این حالت ویژگی‌های فایل به‌عنوان شواهد به‌حساب می‌آیند.

امنیت اطلاعات

محافظت از فایل‌ها در برابر حملات باج افزاری



نازیلا خسروی

مقدمه

پیشگیری و مقابله با باج‌افزارها یکی از مهم‌ترین مباحث امنیت‌سایبری در سال ۲۰۲۱ می‌باشد.
پیش از پرداختن به این موضوع نیاز است بررسی کنیم که باج‌افزار چیست، باج افزار یکی از انواع بدافزارها می‌باشد، اگر باج‌افزار یا یک تروجان رمزگذار وارد سیستم شما بشود شروع به رمزگذاری داده‌ها یا قفل کردن سیستم‌عامل شما می‌کند سپس با داشتن یک گروگان دیجیتالی (داده‌ها، فایل‌ها و...) برای آزادسازی آن از شما درخواست **باج** می‌کند.
بهتر است شما برای مقابله با این نوع خطر آماده باشید، به‌عنوان‌مثال با استفاده از ابزار ضد باج‌افزار از قرارگرفتن در چنین موقعیتی و مجبورشدن به پرداخت هزینه‌های بسیار بالا برای بازیابی فایل‌ها و داده‌هایتان جلوگیری کنید.

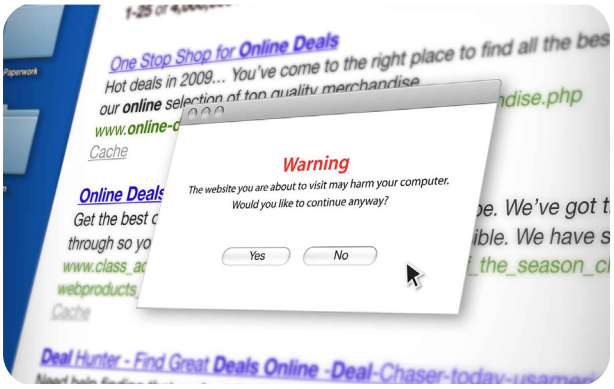
آیا شما پتانسیل مورد حمله قرارگرفتن باج‌افزارها را دارید؟

فاکتورهایی که باعث می‌شود شما مورد حمله باج‌افزارها قرار بگیرید شامل موارد زیر است:

- دستگاه شما از تکنولوژی‌های به‌روز استفاده نمی‌کند.
- دستگاه شما از نرم‌افزارهای به‌روزرسانی نشده استفاده می‌کند.
- مرورگر یا سیستم‌عامل شما به‌روزرسانی و وصله نشده‌اند.
- یک برنامه مناسب برای پشتیبان‌گیری از فایل‌های خود ندارید.
- به امنیت‌سایبری توجه نشده و برنامه مشخصی برای آن تعریف نشده است.

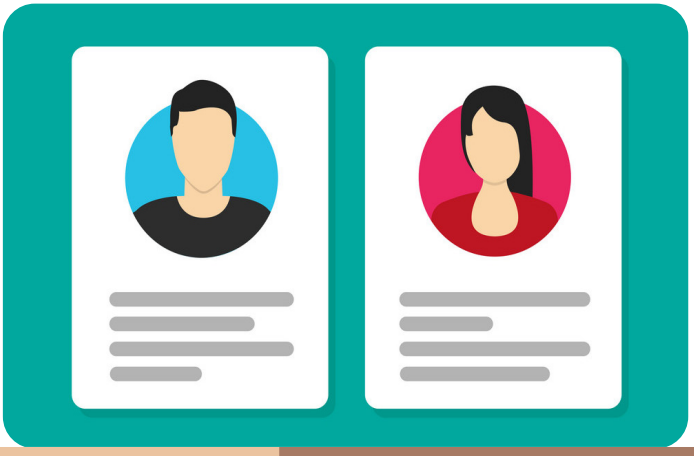
محافظت در برابر باج افزارها - جلوگیری از آلوده شدن

هرگز بر روی لینک‌های ناامن و مشکوک کلیک نکنید.



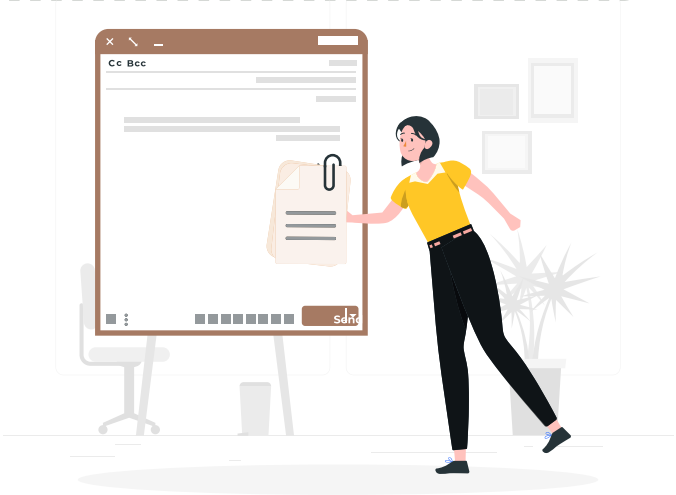
از کلیک‌کردن بر روی لینک‌های موجود در هرزنامه‌ها یا وب‌سایت‌های ناشناس خودداری کنید. اگر بر روی لینک‌های مخرب کلیک کنید ممکن است یک دانلود خودکار آغاز شود و منجر به آلوده شدن سیستم شما شود.

خودداری از افشای اطلاعات شخصی



اگر شما یک تماس، پیام، ایمیل و ... از طرف یک منبع ناشناس دریافت کردید که در آن از شما درخواست ارسال اطلاعات شخصی شده بود، به آن پاسخ ندهید. مجرمین سایبری که قصد اجرای حملات باج افزاری را دارند ممکن است بخواهند اطلاعات شخصی از شما را به‌دست آورند که در آینده در حملات فیشینگ مخصوص به شما از این اطلاعات در جهت سوء بهره‌برداری کنند.

پیوست‌های مشکوک ایمیل‌ها را اجرا نکنید.



باج‌افزارها ممکن است از طریق پیوست‌های ایمیل به سیستم شما وارد شوند. هرگز پیوست‌های ایمیلی که مشکوک هستند را باز نکنید، برای اینکه از قابل اعتماد بودن ایمیل اطمینان حاصل کنید، ارسال کننده ایمیل و صحت آدرس را بررسی کنید. هرگز پیوست‌هایی که از شما میخواهد برای مشاهده آن‌ها یک ماکرو اجرا کنید را باز نکنید. اگر پیوست‌ها آلوده باشند، مشاهده آن‌ها یک ماکروی مخرب را ایجاد می‌کند که به بدافزار، کنترل سیستم شما را می‌دهد.

نرم‌افزارها و سیستم‌عامل خود را به‌روزرسانی کرده و آخرین وصله‌های امنیتی را بر روی آن‌ها اعمال کنید.

به‌طور معمول به‌روزرسانی نرم‌افزارها و سیستم‌عامل شما را در برابر بدافزارها محافظت می‌کند. وقتی به‌روزرسانی‌ها را اعمال می‌کنید اطمینان حاصل کنید که آخرین وصله‌های امنیتی را بر روی سیستم خود اعمال کرده‌اید و این باعث می‌شود بهره‌برداری از آسیب‌پذیری‌های موجود در برنامه‌های شما برای مهاجم بسیار مشکل باشد.

استفاده از مراجع معتبر برای دانلود

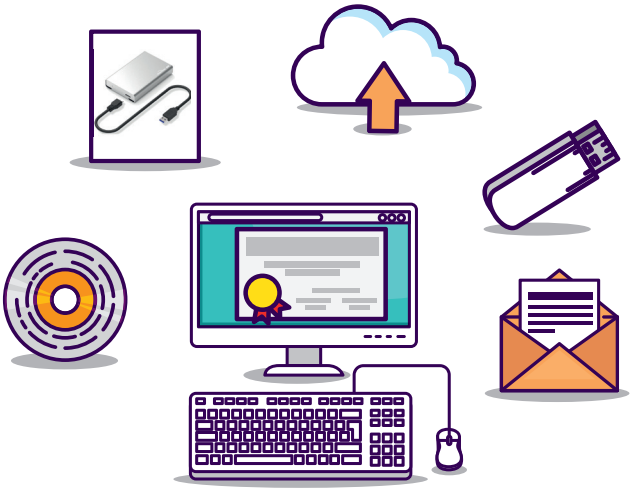
برای حداقل کردن ریسک دانلود باج‌افزار، سعی کنید هرگز برنامه‌ها یا سایر محتواها را از سایت‌های ناشناس دانلود نکنید و تنها از سایت‌های تایید شده و قابل اعتماد برای دانلود محتوای مورد نظر خود استفاده کنید. اطمینان حاصل کنید که سایتی که قصد دانلود محتوا از آن را دارید از «HTTPS» بجای «HTTP» استفاده می‌کند. برای دانلود اپلیکیشن‌های موبایل می‌توانید از Google Play Store یا Apple App Store استفاده کنید.

استفاده از سرویس VPN در شبکه‌های Wi-fi عمومی

STOP, think twice!

زمانی که از یک شبکه Wi-Fi عمومی استفاده می‌کنید، سیستم شما بیشتر در مقابل حملات آسیب‌پذیر است، پس برای محافظت از خود تا حد امکان از شبکه‌های Wi-Fi عمومی استفاده نکنید و در صورت استفاده، از یک سرویس VPN امن استفاده کنید.

تهیه نسخه پشتیبان از اطلاعات مهم و کاربردی خود به صورت مرتب و روزانه



از فایل‌ها و داده‌های خود سعی کنید به‌صورت مرتب نسخه پشتیبان تهیه کنید، در نظر داشته‌باشید بسته به حساسیت و اهمیت داده‌ها ممکن است این فرایند به صورت ماهانه، هفتگی، روزانه، ساعتی و ... انجام پذیرد تا در صورت آلوده‌شدن سیستمِ شما به باج افزار و رمزگذاری شدن فایل‌ها امکان بازگردانی آن‌ها وجود داشته‌باشد.

نصب نرم‌افزارهای امنیتی مانند انتی‌ویروس، فایروال و ضد باج‌افزار

نرم‌افزارهای امنیتی مانند انتی ویروس‌ها نقش بسیار مهمی در تشخیص، جلوگیری از فعالیت و متوقف‌کردن فعالیت باج‌افزارها به‌عهده دارند و استفاده از یک نرم‌افزار امنیتی قدرتمند و به‌روزرسانی شده نقش به‌سزایی در جلوگیری از این نوع حملات دارد. هرچند لازم به ذکر است در صورتی که خود کاربر فایل آلوده به باج‌افزار را اجرا کند و هشدارهای آنتی‌ویروس و ... را نادیده بگیرد و فایل را به‌عنوان یک فایل قابل اعتماد بر روی سیستم خود اجرا کند، بازهم سیستم او آلوده به باج‌افزار می‌شود و فایل‌های خود را از دست می‌دهد، به‌عنوان‌مثال اکثر کرک‌های ارائه شده برای نرم‌افزارهای مختلف توسط آنتی‌ویروس‌ها به عنوان بدافزار شناخته می‌شود ولی کاربر برای اجرای این کرک از طریق آنتی‌ویروس مجوز اجرای این فایل را می‌دهد یا حتی انتی‌ویروس خود را موقتاً غیرفعال می‌کند.

KURD SIRT

مرکز آپا دانشگاه کردستان

مرکز آپا دانشگاه کردستان

cert.uok.ac.ir