

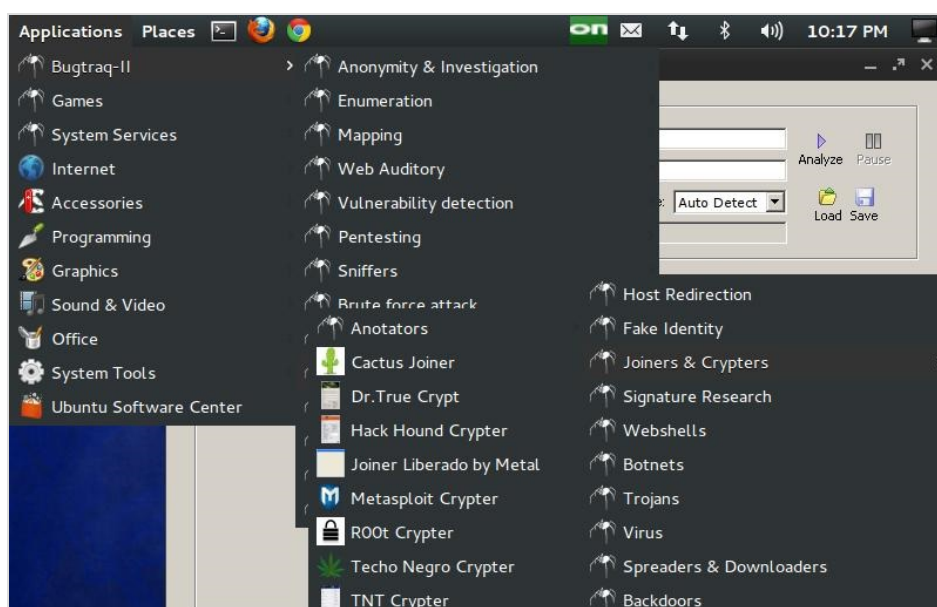
باگ ترک (Bugtrack) چیست؟ معرفی سیستم عامل هک و نفوذ BugTrack (نسخه چاپی)

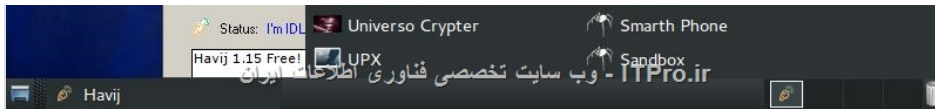
باگ ترک چیست؟ معرفی سیستم عامل هک و نفوذ Bugtrack به زبان ساده ، در قسمت های قبلی از این سری آموزشی ما در ITPRO با سیستم عامل های Kali Linux ، Parrot Security OS ، BackBox ، Samurai ، Pentoo ، DEFT ، CAINE ، NST ، BlackArch آشنا شدیم ، در انتهای این مجموعه آموزشی می خواهیم یک نسخه امنیتی جالب را به عنوان حسن ختام مجموعه مطالب این دسته معرفی کنیم و این لینوکس چیزی نیست جز Bugtraq ، سیستم عامل Bugtraq از جهاتی با سیستم عامل های امنیتی که تا به حال معرفی کردیم تفاوت دارد زیرا امکان استفاده و طراحی بر اساس چند سیستم عامل پایه لینوکس متفاوت را دارد. Bugtraq در مباحث کشف جرائم رایانه ای ، هک و تست نفوذ ، طراحی لابراتوارهای تجزیه و تحلیل بدافزار و کشف جرائم رایانه ای مرتبط با GSM ابزارهای بسیار کاربردی و بعضاً اختصاصی دارد.



Bugtraq هم مثل اندروید نسخه های متعددی دارد و هر کدام را به یک اسم معرفی می کند ، برای مثال آخرین توزیع از این سیستم عامل با عنوان بیوه سیاه (نوعی عنکبوت سیاه سمی) یا Black Widow معرفی شد که بر پایه و اساس سه سیستم عامل Ubuntu ، Debian و Open Suse کار می کند. با توجه به همین تنوع توزیع های استفاده شده ، دستکاپ های متفاوتی را می توان در Bugtraq مشاهده و استفاده کرد. نام سیستم عامل Bugtraq به معنی ردیابی حشره (البته اونجوری که از تفسیر ما برداشت میشه) است.

تعداد ابزارهایی که در Bugtraq وجود دارند واقعاً قابل توجه و زیاد هستند و مجموعه های متنوعی از ابزارهای کشف جرائم رایانه ای ، تست و تجزیه و تحلیل بدافزارها و ... برای آن وجود دارند ، Bugtraq جزو معدود سیستم عامل های امنیت و هک و نفوذ می باشد که Community آن ابزارهای اختصاصی برای آن ارائه می کنند. ابزارهای بازرسی از تکنولوژی های GSM ، ابزارهای تجزیه و تحلیل امنیت شبکه های وایرلس و بلوتوث و RFID ، ابزارهای هماهنگ با سیستم عامل ویندوز ، پشتیبانی از IPv6 و ... از جمله مواردی هستند که بصورت پیشفرض در Bugtraq وجود دارند.





Bugtraq را می توانید توسط یک DVD یا USB Drive بصورت Live نصب و استفاده کنید ، جالب اینجاست بدانید که در Bugtraq قابلیت های Packet Injection خاصی وجود دارد که در سایر توزیع های مشابه امنیتی برای هک وایرلس وجود ندارد و نوع Packet ای که این سیستم عامل می دهد برای آنها قابل فهم نیست.

یکی از قابلیت های جالب دیگر Bugtraq این است که امکان شناسایی مقدار RAM بیشتر از ۴ گیگابایت به سیستم عامل ۳۲ بیتی خودش را می دهد و همچنین فرآیند های نصب ابزارهایی مثل Hashcat ، Nod3۲ ، Nessus ، OpenVAS ، Greenbone ، بصورت خودکار توسط اسکریپ وجود دارد. تیم پشتیبانی سیستم عامل Bugtraq متشکل از مجموعه ای از هکرهاى خیره و برنامه نویس های قدر سیستمی می باشد که بصورت روزانه با پشتیبانی بسیار عالی این سیستم عامل را توسعه ، پشتیبانی و گسترش می دهند . شما می توانید نسخه اصلی Bugtraq را صرفا از طریق لینک معتبر زیر دانلود و استفاده کنید :

• [معتبرترین لینک دانلود Bugtraq](#)

نتیجه گیری از این مجموعه آموزشی

خوب این سری آموزشی از مجموعه ITPRO هم به پایان رسید ، ما در مجموع ده سیستم عامل تخصصی حوزه هک و امنیت اطلاعات را به شما معرفی کردیم ، همانطور که در ابتدای این سری آموزشی عنوان کردیم برای حوزه امنیت و نفوذ هیچوقت یک راهکار جامع یا Total Solution وجود ندارد و شما به عنوان یک کارشناس حرفه ای امنیت بایستی بتوانید از ابزارهای متنوع و سیستم عامل های متفاوت استفاده کنید. همانطور که مشاهده کردید برخی از سیستم عامل ها ابزارهای تخصصی یا نوع Packet های خاصی ارائه می کنند که فقط بر روی همان سیستم عامل قابل استفاده است و این قدرت همان سیستم عامل محسوب می شود.

شما باید بدانید در کجا از کدام ابزار و از چه سیستم عاملی استفاده کنید. چه زمانی ابزارهای Live را استفاده کنید و چه زمانی ابزارهای نصب شدنی را استفاده کنید. انتخاب بین سیستم عامل های امنیتی حق شماست و بعضا خیلی از این موارد بستگی به سلیقه کارشناس امنیت نیز دارد ، پیشنهاد می کنم که با توجه به رایگان بودن این سیستم عامل ها همه آنها را دانلود و نصب کنید و از محیط آنها استفاده کنید و بر اساس سلیقه ای که دارید و سهولت کاربری و ابزارهای متناسب با نیازتان چند عدد را به عنوان ابزار حرفه ای خودتان استفاده کنید ، به شخصه به عنوان یک کارشناس جرائم رایانه ای NST ، Kali و Bugtraq را به عنوان سیستم عامل های مورد علاقه خودم در هک و نفوذ استفاده می کنم اما اگر مواردی مجبور به تست نفوذ وب شویم از Samurai هم استفاده می کنم. امیدوارم این سری آموزشی مورد توجه شما قرار گرفته باشد. ITPRO باشید

نویسنده : محمد نصیری

منبع : [جزیره امنیت اطلاعات و ارتباطات وب سایت توسینسو](#)

هرگونه نشر و کپی برداری بدون ذکر منبع و نام نویسنده دارای اشکال اخلاقی می باشد

مسعود 

سلام مهندس جان ببخشید

میگم سیستم عاملی که تو دوره ی LPIC رو که آموزش میدین اسمش چیه و لینک دنالودش رو اگه زحمتی نیس بگین ممنون میشم !

محمد نصیری 

در دوره LPIC با توجه به شرایط مختلف من روی سیستم عامل های مختلفی درس میدم مهمترینشون اینها هستند :

۱. Debian

۲. Xubuntu

۳. Ubuntu

۴. Kali

۵. CentOS ۶

۶. CentOS ۷

فقط کافیست تو اینترنت واژه Download و بعدش اسم سیستم عامل مورد نظر رو بیاری و از وب سایت اصلیش دانلود کنی.


AZARAKHSH 

با سلام

ممنون از مهندس نصیری عزیز

اگر امکانش هست نحوه دریافت registration code مربوط به دانلود NST PRO رو هم یک راهنمایی بفرمایید.

با تشکر از زحماتتون

محمد نصیری 

کار سختی نیست فقط شما باید ترجیحا PayPal داشته باشید و برید داخل صفحه زیر و Version مورد نظرتون رو بصورت ماهیانه یا سالیانه انتخاب کنید و بعد پرداخت PayPal رو انجام بدید و بعد برای ایمیلتون ارسال میشه ، فقط باید ترجیحا آدرس IP ایتون ایرانی نباشه چون PayPal به شما Access Denied میده :

<http://www.networksecuritytoolkit.org/nstpro/>

مطلب اصلی