سامانه تله‌عسل بومی

مرکز آپا دانشگاه صنعتی شریف
https://cert.sharif.edu

جمهوری اسلامی ایران
شورای عالی علوم، تحقیقات و فناوری

ستاد ملی هفته پژوهش و فناوری

سرآغاز

با ورود فضای سایبری به عرصه‌های گوناگون زندگی امروزی، جذابیت این فضا به‌عنوان محلی برای پیگیری اهداف خرابکارانه و ضربه زدن به قربانیان توسط مهاجمان افزایش چشمگیری داشته است. همه‌روزه حملات پرشمار و گوناگونی در سطح اینترنت گزارش می‌شود که در برخی موارد این حملات حتی از سوی دولت‌ها یا نهادها بر علیه یکدیگر صورت می‌پذیرد. در چنین فضایی، توانایی تشخیص حملات و شناسایی روش‌های مورد استفاده مهاجمان در اجرای حملات، به یک توانائی کلیدی برای صاحبان شبکه و متخصصان امنیت سایبری بدل می‌گردد.

دستیابی به چنین توانی، علاوه بر کسب مهارت‌های فنی از سوی متخصصان، مستلزم به‌کارگیری ابزارهای مناسب جهت تشخیص نفوذ و شناسایی روش‌های بکار رفته از سوی مهاجمان در اجرای حملات است. سامانه‌های امنیتی بسیاری با هدف شناسایی حملات سایبری طراحی و ساخته شده‌اند، اما بیشتر آنها در برابر حملات ناشناخته و جدید (روز صفر) از کارآئی لازم برخوردار نیستند. یکی از تکنیک‌های شناخته‌شده برای دستیابی به اطلاعات مرتبط با حملات روز صفر، بهره‌گیری از سامانه‌های تله‌عسل است.

تله‌عسل یک منبع محاسباتی است که از دو ویژگی کلیدی

۱. نظارت کامل بر کلیه فعالیت‌ها و
۲. عدم ارائه خدمات تولیدی

برخوردار است. این دو ویژگی در کنار عدم تبلیغ سرویس ارائه شده توسط این سامانه باعث می‌گردد تا کلیه مراجعات به آن

۱. مظنون به خرابکارانه بودن و
۲. همچنین تحت نظارت کامل

باشد. همین ویژگی‌ها، کلید شناسائی حملات نو و روش‌های به‌کار رفته در اجرای آنها خواهد بود.

به صورت کلی کارکرد اصلی تله‌عسل در شبیه‌سازی محیط ارائه خدمات برای مهاجمان و گرفتار کردن آنها در دام خدمات غیرتولیدی است. از دیدگاه سطح تعامل با مهاجم، سامانه‌های تله‌عسل به دو دسته کلی کم‌تعامل (شبیه‌سازی محدود خدمات و تعامل حداقلی با مهاجم) و پرتعامل (ارائه سرویس آسیب‌پذیر واقعی و نه شبیه‌سازی شده و تعامل کامل با مهاجم) تقسیم می‌شود. سامانه تله‌عسل بومی تولید شده در مرکز آپا دانشگاه صنعتی شریف به صورت تلفیقی (Hybrid) (کم‌تعامل و پر تعامل) است.

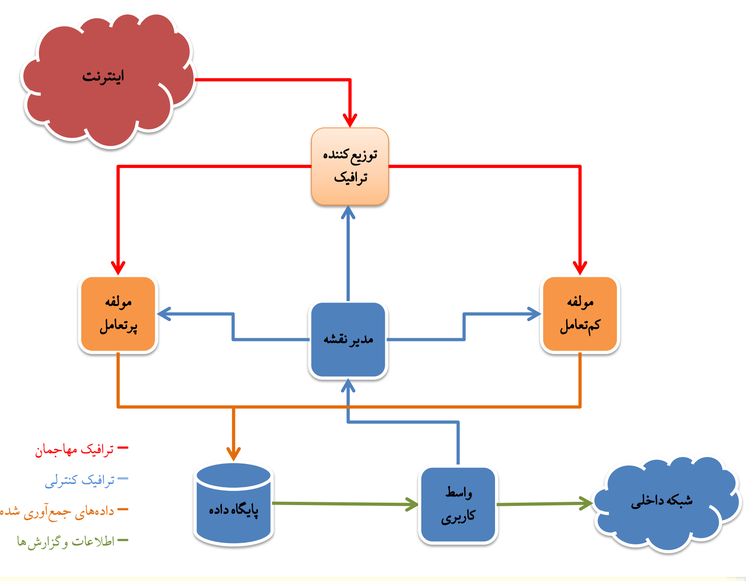
ویژگی‌های اساسی سامانه

برخی از ویژگی‌های اساسی سامانه تله‌عسل بومی در زیر فهرست شده‌اند:

- ✓ معماری نیمه‌متمرکز با هدف گسترش شبکه تله‌عسل در سطح جغرافیائی وسیع
- ✓ قابلیت گسترش‌پذیری بالا از طریق توسعه افزونه‌های لایه کاربرد با هدف پوشش دادن خدمات گوناگون قابل ارائه در این لایه
- ✓ امکان افزودن گزارش‌های متناسب با افزونه جدید
- ✓ عدم نیاز به تغییر در هسته و یا واسط کاربری سامانه در هنگام به‌کارگیری افزونه‌های جدید
- ✓ فضای توسعه افزونه‌ای نزدیک به توسعه ابزار در پلتفرم لینوکس
- ✓ شبیه‌سازی کامل پشته قرارداد TCP/IP در مولفه کم‌تعامل

معماری کلی

شمای کلی سامانه تله‌عسل.



سامانه از چهار مولفه اصلی تشکیل شده است:

- ✓ مولفه کم‌تعامل
- ✓ مولفه پرتعامل
- ✓ مولفه پایگاه‌داده
- ✓ مولفه مدیر نقشه و توزیع‌کننده ترافیک

مولفه‌های سامانه

۱ـ مولفه توزیع‌کننده ترافیک

- ✓ ایجاد و ثبت میزبان‌های کم‌تعامل و پرتعامل
- ✓ تعیین دامنه‌های آدرس تخصیص یافته به هر یک از مولفه‌ها
- ✓ اعمال پیکربندی‌های مرتبط با مسیردهی و کنترل ترافیک

۲ـ مولفه مدیر نقشه

- ✓ ایجاد و ثبت میزبان‌های کم‌تعامل و پرتعامل
- ✓ تعیین دامنه‌های آدرس تخصیص یافته به هر یک از مولفه‌ها
- ✓ اعمال پیکربندی‌های مرتبط با مسیردهی و کنترل ترافیک

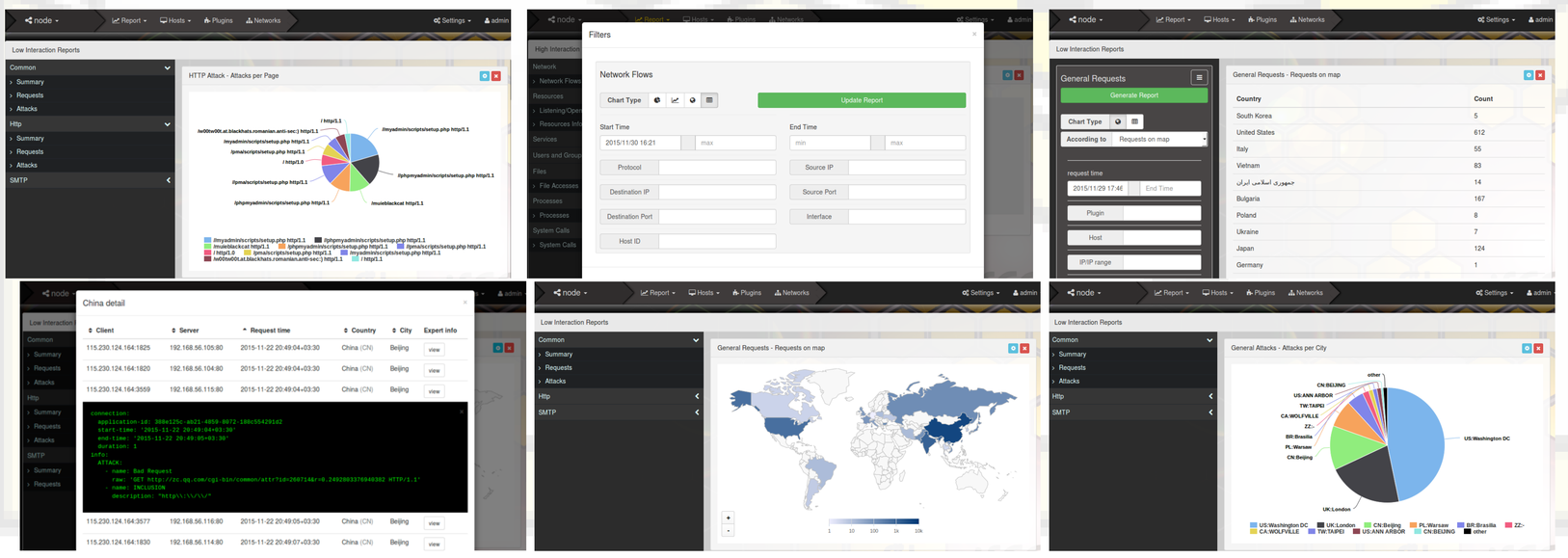
۳ـ مولفه کم‌تعامل

- ✓ شبیه‌سازی شبکه و میزبان‌های کم‌تعامل
- ✓ مقابله با حملات خودکار (برنامه‌های خودکار و کرم‌های اینترنتی)
- ✓ اقدام به شبیه‌سازی خدمات با بهره‌گیری از افزونه‌های لایه کاربرد
- ✓ ثبت و ضبط کلیه تعاملات صورت گرفته در لایه‌های گوناگون پشته قرارداد در طی مدت زمان تعامل مهاجم با سامانه
- ✓ تعیین میزان تعامل و سطح رویدادنگاری در لایه کاربرد از سوی توسعه‌دهنده افزونه لایه کاربرد

۴ـ مولفه پرتعامل

- ✓ یک کارگزار لینوکس مجهز به ابزارهای پایشی پیشرفته
- ✓ کمترین سربار ممکن در عین جمع‌آوری حداکثری اطلاعات
- ✓ ناممکن بودن شناسائی و از کار انداختن ابزارهای پایشگر برای مهاجم
- ✓ قابلیت پیکربندی سطح پایش برای مدیر سامانه
- ✓ ثبت رویدادهای مرتبط با:
  - پردازه‌ها
  - دسترسی‌های فایلی
  - ورود و خروج کاربر
  - تغییر در اطلاعات هویت‌سنجی
  - جریان‌های شبکه
  - دیگر رویدادهای سیستم.

چند نما از رابط کاربری سامانه



درباره آپا دانشگاه صنعتی شریف

آپا شریف
آگاهی‌رسانی، پشتیبانی، امداد

مرکز آگاهی‌رسانی، پشتیبانی و امداد در حوزه افتا (آپا) دانشگاه صنعتی شریف، با رویکرد استفاده از نیروهای دانشگاهی در سال ۱۳۸۶ جهت خدمت به صنعت کشور و تقویت پیوند دانشگاه و صنعت، در دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف راه‌اندازی گردید. آپا یک تیم خدماتی است که هدف اصلی آن ارائه خدمات امنیتی، با محور مدیریت و تحلیل حوادث، و آسیب‌پذیری‌ها در فضای تبادل اطلاعات به سازمان‌ها و کاربران است. مرکز آپا دانشگاه صنعتی شریف به عنوان مکمل مرکز امنیت داده و شبکه شریف فعالیت‌های خود را در جهت ارائه خدمات امنیتی به کاربران و سازمان‌ها دنبال نموده است.

در طی ۱۴ سال فعالیت مرکز آپا دانشگاه صنعتی شریف پروژه‌های مشاوره و تحقیقاتی متعددی به اجرا رسیده و یا در حال اجرا است که از اهم آن‌ها می‌توان به طراحی و پیاده‌سازی سامانه‌های:
تلسکوپ آی‌پی برای شبکه؛ کشف شبکه‌های بات؛ فروچاله نام دامنه؛ تحلیل بدافزارهای جمع‌آوری‌شده از شبکه تله‌عسل؛ کنترل دسترسی چندسطحی سمپاد بومی؛ و کشف شواهد جرائم رایانه‌ای مبتنی بر ترافیک شبکه اشاره کرد.

همچنین این مرکز، فعالیت به‌سزائی در آگاهی‌رسانی، پشتیبانی و امداد در خصوص امنیت انواع سمپادها در سطح کشور و ارائه خدمات رسیدگی رخداد و حملات امنیتی به سازمان‌ها و شرکت‌های مختلف داشته است.

آدرس مرکز: تهران، خیابان آزادی، دانشگاه صنعتی شریف، دانشکده مهندسی کامپیوتر، طبقه ۵، مرکز آپا دانشگاه صنعتی شریف
تلفن و نمابر: ۷ـ ۶۶۱۶۶۶۷۵
وب‌سایت: https://cert.sharif.edu