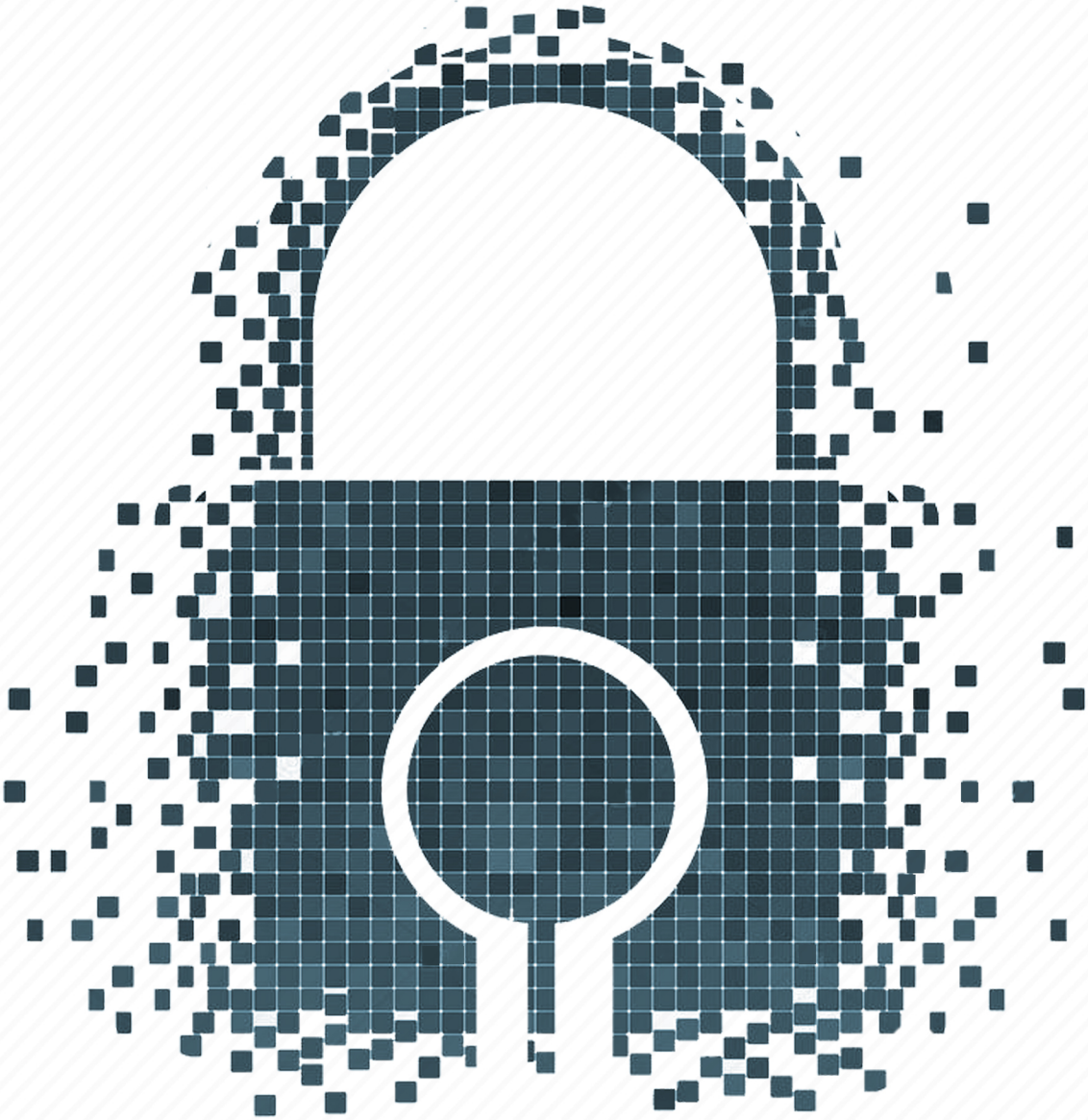
کایاد
مشاور برتر
امنیت اطلاعات



Homeland Security
kaipod

خدمات آزمون نفوذپذیری

Penetration Testing Services

Web App | Network | Mobile App | Softwares RE | Industrial Control Systems

www.kaipod.ir

خدمات آزمون نفوذپذیری شرکت پیشگامان کی‌پاد

- شرکت پیشگامان کی‌پاد در تاریخ ۱۳۸۴/۰۴/۰۵ با شماره ثبت ۷۴۸۰ فعالیت خود را تحت عضویت اتحادیه گروه تعاونی پیشگامان آغاز نمود. کی پاد با در اختیار داشتن کادری مجرب در تمامی حوزه‌های امنیت اطلاعات فعالیت می‌نماید. فعالیت‌های این شرکت در حوزه آزمون نفوذپذیری به شرح زیر است :
- تست نفوذپذیری (Pen-Test) با استفاده از ابزارهای تجاری (CANVAS, HP-Weblnspect, Burp Suite Pro, Metasploit Pro) کدهای مخرب محرمانه در سطح نرم افزارهای مدیریت محتوای وب (Joomla, WP, ...) و متدولوژی‌های ابداعی توسط تیم فنی.
- تولید محصولات امنیتی (UTM, ISMS Software, Anti Ransomware)
- تحلیل آسیب‌پذیری و توسعه PoC توسط (BA, WA PoC, Exploit) از انواع سرویس‌های رقابتی که تنها در صنعت توسعه IDS/IPS/AV نقش دارند.
- مقاوم‌سازی امنیتی (Special Hardening) در زمینه امن‌سازی ۹۹% تمامی سرویس‌ها و سیستم‌های عامل
- آموزش دوره‌های امنیت اطلاعات و شبکه (MicroTik, CCNA, MCSE, MCITP, CHFI, C|EH, CCNP, OWASP, ...)

پروانه فعالیت در حوزه خدمات عملیاتی افتا
شماره پروانه: ITO-NAMA-1110023
به استناد قوانین «برنامه‌های پنج‌ساله توسعه جمهوری اسلامی ایران»، «وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات»، «سند راهبردی امنیت فضای تولید و تبادل اطلاعات (افتا)» و در راستای اجرای «مصوبه مورخ ۱۳۸۸/۱۲/۲۴ هیات محترم دولت» و با توجه به احراز صلاحیت
به‌عمل آمده به:
شرکت پیشگامان کی پاد کویر یزد
اجازه داده می‌شود به مدت یک‌سال از تاریخ صدور پروانه تحت نظارت سازمان فناوری اطلاعات ایران با گرایش
آزمون و ارزیابی امنیتی
در کشور فعالیت نماید.

پروانه فعالیت در حوزه خدمات آموزشی افتا
شماره پروانه: ITO-NAMA- 1010045
به استناد قوانین «برنامه‌های پنج‌ساله توسعه جمهوری اسلامی ایران»، «وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات»، «سند راهبردی امنیت فضای تولید و تبادل اطلاعات (افتا)» و در راستای اجرای «مصوبه مورخ ۱۳۸۸/۱۲/۲۴ هیات محترم دولت» و با توجه به احراز صلاحیت
به‌عمل آمده به:
شرکت پیشگامان کی پاد کویر یزد
اجازه داده می‌شود به مدت یک‌سال از تاریخ صدور پروانه تحت نظارت سازمان فناوری اطلاعات ایران
در کشور فعالیت نماید.

پروانه فعالیت در حوزه خدمات مدیریتی افتا
شماره پروانه: ITO-NAMA- MC-0146
به استناد قوانین «برنامه‌های پنج‌ساله توسعه جمهوری اسلامی ایران»، «وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات»، «سند راهبردی امنیت فضای تولید و تبادل اطلاعات (افتا)» و در راستای اجرای «مصوبه مورخ ۱۳۸۸/۱۲/۲۴ هیات محترم دولت» و با توجه به احراز صلاحیت
به‌عمل آمده به:
شرکت پیشگامان کی پاد کویر یزد
اجازه داده می‌شود به مدت دوسال از تاریخ صدور پروانه تحت نظارت سازمان فناوری اطلاعات ایران با گرایش
مشاوره و استقرار استانداردهای امنیت اطلاعات و ارتباطات، پارتبه دو (۲)
در کشور فعالیت نماید.

پروانه فعالیت در حوزه خدمات عملیاتی افتا
شماره پروانه: ITO-NAMA-OS-0017
به استناد قوانین «برنامه‌های پنج‌ساله توسعه جمهوری اسلامی ایران»، «وظایف و اختیارات وزارت ارتباطات و فناوری اطلاعات»، «سند راهبردی امنیت فضای تولید و تبادل اطلاعات (افتا)» و در راستای اجرای «مصوبه مورخ ۱۳۸۸/۱۲/۲۴ هیات محترم دولت» و با توجه به احراز صلاحیت
به‌عمل آمده به:
شرکت پیشگامان کی پاد کویر یزد
اجازه داده می‌شود به مدت دوسال از تاریخ صدور پروانه تحت نظارت سازمان فناوری اطلاعات ایران با گرایش
امن سازی و مقاوم سازی سامانه‌ها، زیرساخت‌ها و سرویس‌ها
در کشور فعالیت نماید.

تست نفوذ نرم‌افزارهای کاربردی تحت وب (Web Application Pentest)

به دلیل سهولت در دسترسی نرم‌افزارهای کاربردی تحت وب، این سامانه‌ها یکی از اهداف نفوذگرها می‌باشند. متخصصین این شرکت بر اساس مراحل زیر با اتکا به نرم‌افزارهای تجاری و دانش تیم ارزیاب اقدام به تست و تحلیل اهداف مذکور می‌نماید.

01 تست نفوذ خودکار وب‌سایت و سامانه‌های تحت وب

02 آزمون نفوذپذیری به صورت دستی

03 نفوذ و بهره‌برداری از آسیب‌پذیری‌های کشف‌شده و تست مجدد

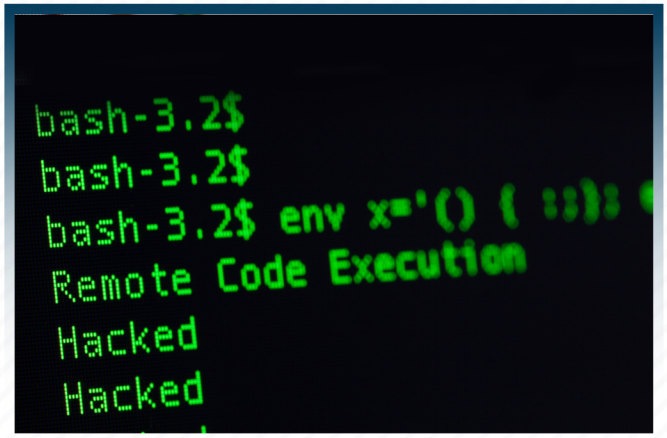
04 ارائه گزارش از آسیب‌پذیری‌ها و دسترسی‌ها

05 ارائه راه‌کارهای امنیتی

تست نرم‌افزارهای کاربردی و مهندسی معکوس (Software Pentest & Reverse Engineering)

نرم‌افزارهای سیستمی و رومیزی نیز از حوزه امنیت منفک نبوده و نیستند، حتی نرم‌افزارهایی که به صورت کامپایل شده و یا بر بستر پلتفرم‌های ویندوزی بر روی سیستم عامل ارائه خدمت می‌نمایند دارای آسیب‌پذیری‌های بسیاری می‌باشند. متخصصین ما با سنجش پیچیدگی، سطح مبهم‌سازی و سختی در دسترسی به سورس نرم‌افزار، بررسی استخراج اطلاعات حیاتی در جهت استفاده مستقل و نیز کشف آسیب‌پذیری‌هایی که منجر به سوء استفاده از سیستم‌عامل کاربر نهایی می‌گردد، ارزیابی نرم‌افزارهای کاربردی را انجام می‌دهند.

- اعمال تکنیک‌های Hard-Core و Protocol Fuzzing
- پایش رفتار نرم‌افزار در مواقع خاص
- انجام Fuzzing و تخمین میزان پایداری نرم‌افزار
- بررسی سورس کد (Source Code Auditing)
- اعمال تکنیک‌های مهندسی معکوس در توابع و ماژول‌های مشکوک
- تست و بررسی توابع سیستمی و روش‌های کاربردی در نرم‌افزار



تست نرم‌افزار موبایل (Android Mobile App Pentest)

با توجه به گستردگی استفاده از دستگاه‌های تلفن همراه و تبلت که قابلیت اجرای برنامه‌ی کاربردی موبایل را دارند، موضوع امنیت این دسته از نرم‌افزارها باید بیشتر مورد توجه قرار گیرد. معماری اکثر برنامه‌های موبایل به صورت سرویس‌دهنده و کلاینت می‌باشد. کلاینت‌های موبایل علاوه بر آسیب‌پذیری‌هایی که برنامه‌های کاربردی تحت وب را تهدید می‌کند، در معرض مفقودشدن یا سرقت نیز می‌باشند. ازاین‌رو، امنیت سرور نیز بر روی دستگاه کاربران اهمیت ویژه‌ای یافته است. بنابراین این سطح از امنیت باید به‌گونه‌ای تأمین گردد تا در صورت مفقود یا سرقت و یا نفوذ دستگاه کاربر، مخاطره‌ای از جانب این برنامه‌ها، اطلاعات محرمانه‌ی کاربران را تهدید نکند.

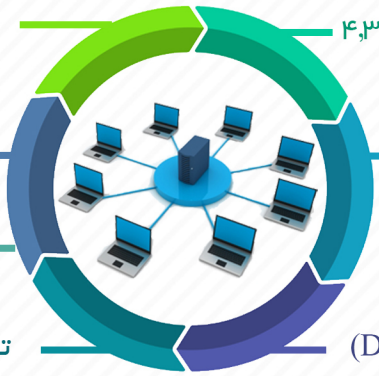
01 عدم نشست اطلاعات
02 کلاس اصالت‌سنجی امن کاربر
03 بررسی مجوز دسترسی از سمت سرور
04 جلوگیری از جستجوی فراگیر
05 جلوگیری از حملات تزریق در سمت سرور
06 جلوگیری از آسیب‌پذیری XSS
07 خط‌مشی مناسب برای انتخاب گذرواژه
08 عدم وجود آسیب‌پذیری DoS
09 مدیریت مناسب نشست

01 بررسی مجوز دسترسی در برنامه کاربردی
02 کلاس اصالت‌سنجی امن کاربر
03 بررسی مجوزهای داده شده به برنامه
04 ذخیره‌سازی امن داده‌ها در سمت کاربر
05 عدم افشای اطلاعات حساس در سمت کاربر
06 محافظت برای کدهای اجرایی

تست نفوذ شبکه و تجهیزات اکتیو (Wired & Wireless Networking Pentest)

شبکه‌ها جزو لاینفک زندگی و چرخه حیات یک سازمان می‌باشند. تداوم کسب و کارها ملزم به پایداری و امنیت زیر ساخت‌های ارتباطی هستند. متخصصین این شرکت با انجام حملاتی در لایه‌ها و پروتکل‌ها و نیز به تجهیزات ارتباطی و امنیتی شبکه تلاش می‌کنند تا علاوه بر کشف و ارائه آسیب‌پذیری‌ها در حفظ و پایداری آن‌ها به مدیران فناوری اطلاعات یاری بخشند.

- نفوذ و بهره‌برداری از آسیب‌پذیری‌های کشف‌شده در زیرساخت‌های مجازی‌سازی و سرویس‌دهنده
- تست امنیت فیزیکی سامانه‌ها و مراکز داده
- تست لایه‌های Access, Distribution, Core و WAN-Edge
- تست و ارزیابی شبکه‌های بی‌سیم پروتکل‌های (WEP, WPA, WPA2, LEAP)



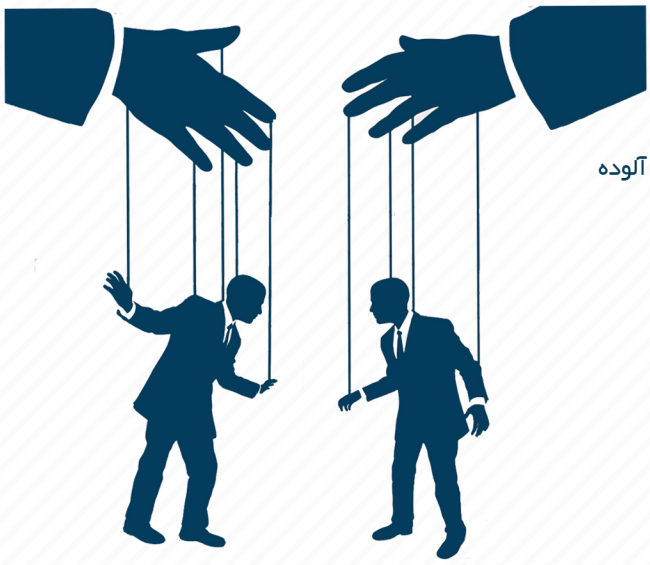
- تست آسیب‌پذیری پروتکل‌های لایه های ۲,۳,۴
- تست بستر Active Directory و ضعف‌های پیکربندی
- تست شبکه‌های صنعتی (DCS, SCADA) و میزان Isolation

مهندسی اجتماعی (Social Engineering Techniques)

شبکه‌های ما هیچ‌گاه صد در صد امن نخواهند بود، چرا که حتی اگر به آخرین تمهیدات امنیتی دسترسی داشته باشیم نهایتاً کنترل همه‌ی این موارد بر عهده‌ی یک یا چند انسان است. انسان ذاتاً موجودی احساساتی و اجتماعی است و همین دو خصیصه پتانسیلی برای آسیب‌پذیری خواهد بود. در دنیایی که رقابت‌های کاری و تجاری بر روابط انسانی ارجحیت دارد از هر تکنیکی برای پیشی گرفتن از رقبا و سرقت اطلاعات آنان استفاده می‌شود. یکی از این تکنیک‌ها، هنر مهندسی اجتماعی است. متخصصین ما، ضمن حضور در محل سازمان جهت انجام مراحل فنی آزمون‌ها، شرایط را برای مهندسی اجتماعی و تکنیک و تهدیدات خارج سازمان آماده می‌سازند. آزمون‌های این حوزه مبتنی بر تکنیک‌های کامپیوتر و انسان می‌باشد:

مبتنی بر انسان

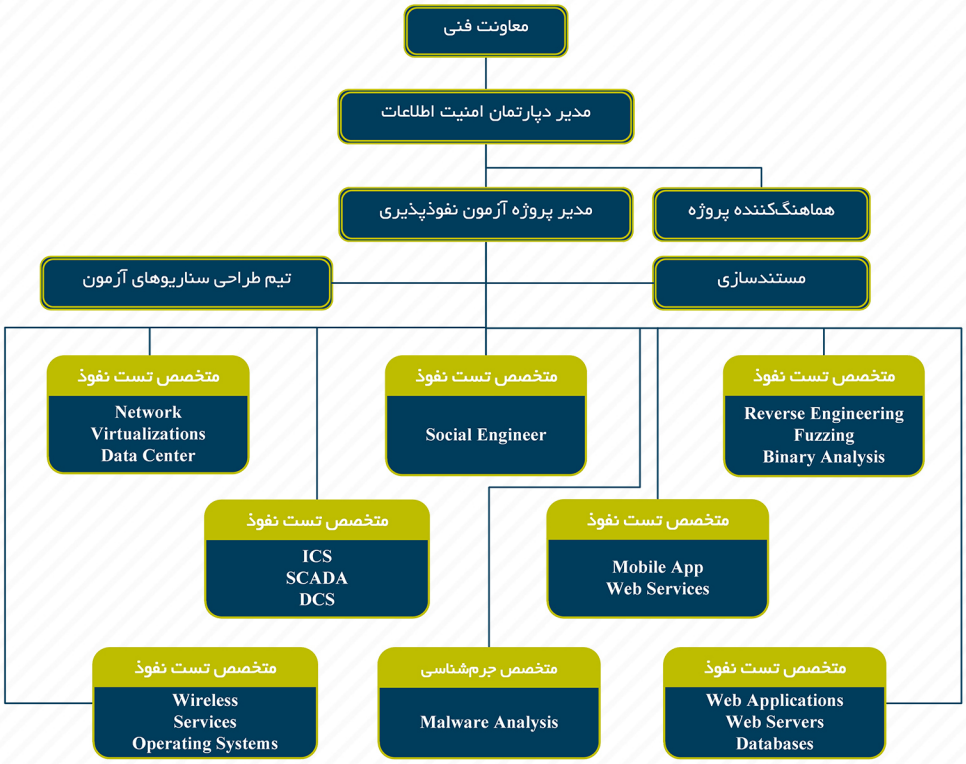
- جعل ایمیل سازمانی و پیوست‌های آلوده
- انجام حملات جعل منابع سازمانی
- تکنیک‌های Spear-Phishing
- انجام حملات Baiting



مبتنی بر کامپیوتر

- تحریک حس پذیرش اعتماد
- کشف پرسنل ناراضی
- تحریک حس انطباق‌پذیری
- تحریک حس عاطفی
- تحریک حس کمک به هم‌نوع
- استفاده از منابع دور ریخته‌شده

چارت سازمانی دپارتمان آزمون نفوذپذیری



kaipod.ir

گروه پیشگامان

کی‌پاد، کیان امنیت

یزد، خیابان کاشانی
روبروی هلال احمر
کوچه ۴۳، ساختمان
پیشگامان کی‌پاد
کدپستی: ۸۹۱۵۶۱۳۳۸۹
تلفن: ۰۳۵۳۶۲۹۴۳۵۳
فکس: ۰۳۵۳۶۲۴۶۳۶۰

تهران، ستاری شمالی
پیامبر مرکزی، ۲۰ متری
مطهری، پلاک ۵
طبقه ۵، واحد ۱۸
کدپستی: ۱۴۷۱۸۵۳۶۴۷
تلفن: ۰۲۱ ۴۴۹۵۵۵۶۷
فکس: ۰۲۱ ۴۳۸۵۱۳۷۹

مشهد، بلوار خیام
نبش خیابان خیام جنوبی
شماره ۲۸، پلاک ۲، ساختمان
پیشگامان، طبقه دوم
کدپستی: ۹۱۸۷۶۹۳۶۳۴
تلفن: ۰۵۱۳۷۶۵۵۵۵۹
تلفکس: ۰۵۱۳۷۶۷۹۷۷۲

www.kaipod.ir info@kaipod.ir