تست نفوذ و ارزیابی امنیتی

Penetration Testing and Security Assessments

تست نفوذ خارجی

در این مرحله تمامی سرویس های در حال اجرا بر روی درگاه های باز شبکه پایش شده و بصورت BlackBox مورد شناسایی و ارزیابی امنیتی قرار میگیرند، این ارزیابی طیف گسترده ای از آسیب پذیری های منطقی و باینری را شامل می شود، طبق روش های NIST (انستیتوی ملی استاندارد و فناوری) و چارچوب PTES (استاندارد اجرای آزمایش های تست نفوذ)، ما تست نفوذ زیرساخت های شبکه (LAN / WAN / WLAN) را انجام می دهیم.

تست نفوذ داخلی

در این نوع ارزیابی کارشناسان می کوشند تا سیستم های داخلی را مورد نفوذ قرار دهند، این کوشش بر پایه تیکنیک هایی همچون نصب یک حافظه جانبی، مهندسی کارکنان مجموعه و از سوی دیگر فرایند شناسایی پیکربندی نادرست سیستم عامل ها و سرویس های فعال بر روی آنها هم مورد بررسی قرار خواهند گرفت، در این نقطه تمامی آسیب پذیری های سطح هسته سیستم عامل و Component های فعال و Active Directory را بررسی دقیق می شوند، همچنین نحوه عملکرد مکانیزم های شناسایی کننده و دفاعی که فرایند مقابله با حملات را دارا هستند.

تست نفوذ

سازمان ها تمام تلاش خود را برای محافظت از دارایی های مهم اینترنتی خود انجام می دهند، اما همیشه دفاع سیستم خود را به طور سیستماتیک آزمایش نمی کنند، تست نفوذ به شما کمک می کند با تعیین دقیق نقاط ضعف و تنظیمات نادرست در سیستم های امنیتی، امنیت خود را برای این دارایی ها تقویت کنید، انواع مختلف ارزیابی امنیتی مانند آزمایش زیرساخت داخلی / خارجی، بررسی امنیت برنامه که شامل محصولات وب، موبایل یا سرور مشتری را انجام می دهد.

راه ارتباطی

تلفن:
026 368 06249

وبسایت:
unk9vvn.com

ایمیل:
info@unk9vvn.com

برنامه های تحت وب

ما ارزیابی های امنیتی برنامه های وب را مطابق با رویه OWASP (پروژه امنیت برنامه متن باز) ارائه می دهیم، از جمله OWASP Top 10 و OWASP ASVS (استاندارد تأیید امنیت برنامه) که با تجربه ما ارائه شده است، ما فقط به آسیب پذیری های ذکر شده در OWASP محدود نمی شویم و هدف ما یافتن آسیب پذیری های خاص تجاری است که می تواند تهدیدی واقعی برای تجارت مشتری باشد و اغلب توسط اسکنرهای آسیب پذیری خودکار بدست نمی آیند.

برنامه های موبایلی

ما ارزیابی امنیت برنامه تلفن همراه را برای سیستم عامل های iOS و Android انجام می دهیم. ما روش خود را بر اساس OWASP Mobile (پروژه امنیت برنامه کاربردی متن باز) از جمله OWASP Mobile Top 10 و OWASP MASVS (استاندارد تأیید امنیت برنامه کاربردی تلفن همراه) که با تجربه خودمان در شناسایی آسیب پذیری در برنامه تلفن همراه افزایش یافته است، قرار داده ایم، مشاوران ما تجربه حسابرسی نرم افزارهای تلفن همراه از جمله مرورگرها، برنامه های مالی و بسیاری دیگر را دارند.

شبکه های بی سیم

تست نفوذ WiFi برای آزمایش امنیت شبکه های بی سیم مستقر در محل است، این هدف در راستای ورود به یک شبکه WiFi محافظت شده و همچنین افزایش امتیاز در شبکه مهمان بوده و نهایتا منجر به حمله کاربران شبکه بی سیم خواهد شد .امنیت بی سیم همچنین بخشی از خدمات تیم قرمز ما است که هدف آن انجام حملات مهندسی اجتماعی علیه کاربران بواسطه WiFi است، به عنوان مثال با اجرای یک Access Point جعلی.

فواید تست نفوذ

کارشناسان تیم، مهاجمان واقعی را که دارایی های سایبری پر خطر شما را هدف قرار می دهند، شبیه سازی می کنند .شناخت عمیق ما از رفتار مهاجم های پیشرفته (APT) می تواند به شما کمک کند.

کارشناسان برای شما تعیین میکنند که آیا داده های مهم شما واقعاً در معرض خطر است، قبل از سو استفاده مهاجمان از تنظیمات نادرست و آسیب پذیری های پیچیده امنیتی، آنها را شناسایی و شکار کنیم.

بیش از شش منطقه عملیاتی در تست نفوذ مورد آزمون قرار میگیرند که هر یک از این مناطق طیف وسیعی از آسیب پذیری ها را ارزیابی می کنیم، هر کدام از موارد تست نفوذ طبق استانداردهای جهانی انجام می شود

.

چرا تیم ما؟

همه گزارش ها توسط مشاوران ما نوشته شده اند و بدون اسکنرهای امنیتی اتوماتیک تهیه شده اند. علاوه بر این، کارشناسان ما به عنوان شکارچی چندین آسیب پذیری در نرم افزار های محبوب شناسایی کرده و با موفقیت در برنامه های Bug Bounty ثبت کرده اند.

اسناد فنی که به شما امکان می دهد یافته های ما را تجزیه و تحلیل و رفع آسیب پذیری کنید، همچنین ریسک مبتنی بر واقعیت که مشخص می شود ممکن است در سیاست های سرویس دهی شما هم تاثیر گذار باشد.

کارشناسان ما محصولات نرم افزاری شکارچی آسیب پذیری خود را بومی سازی کرده اند و با استفاده از اتوماسیون های خود فرایند ارزیابی آسیب پذیری ها را انجام میدهد.

اینترنت اشیاء

ارزیابی امنیت دستگاه خود با تلاش برای سو استفاده از آسیب پذیری ها و بهره برداری از سیستم عامل تعبیه شده، کنترل دستگاه با عبور یا تزریق دستورات مخرب ناخواسته یا تغییر داده های ارسالی از دستگاه، این آزمون ها شامل ارتباطات بی سیم مانند استفاده از بلوتوث ارتباطات شبکه ای است، همچنین فرایند Debug Programming مستقیم بواسطه زدن JTAG بر روی MCU دستگاه.

فضای ابری

ورود به محیط های ابری اغلب با نتیجه پیکربندی نامناسب سرویس همراه است. در هنگام ارزیابی امنیت ابری، همه تهدیدهای احتمالی برای کاربران نهایی و دارندگان زیرساخت های ابر را شناسایی می کنیم. ارزیابی امنیت ابر به منظور تشخیص نقص امنیتی و تنظیمات نادرست، که می تواند یک نقطه ورود جذاب برای یک مهاجم باشد همچنین مدل سازی تهدید از پروژه های ابری برای اینکه شما بتوانید یک مرور سریع از تهدیدات احتمالی در معماری خود داشته باشید.

اطلاعات متن باز

پایش اطلاعات متن بازه در سطح اینترنت میتواند اطلاعات حساسی که از سرویس های مشتری ضبط شده است را نمایان سازد، موتورهای جستجوگر متعددی در راستای جمع آوری اطلاعات لحظه ای از سرویس و سامانه های سطح اینترنت وجود دارد و همین امر موجب میشود تا آدرس IP های واقعی یک سرور پیش از قرار گرفتن در لیست سرویس های CDN ضبط و لو برود.

تست جعبه سیاه

تست نفوذ و ارزیابی زیرساخت ها و نرم افزارها را می توان از دید مهاجم خارجی انجام داد، به این معنی که آزمایش کننده هیچ اطلاعاتی در مورد سیستم مورد نظر به غیر از آنهایی که به صورت عمومی در دسترس است، ندارد.

هیچ اطلاعاتی در مورد معماری و سیستم های مشتری تحویل داده نمی شود، هیچ حساب کاربری به جز مواردی که توسط مهاجم می تواند ایجاد شود (به عنوان مثال با ثبت نام در برنامه).

به جز ارزیابی امنیت برنامه های وب و تلفن همراه، ما قدرت آزمایش برنامه های Desktop و Server را هم دارا هستیم . ما می توانیم تست امنیتی برنامه های نوشته شده با C / C ++ / Java C # ورود دیگر را برای سیستم عامل های Linux Windows و OS X ارائه دهیم.

تست جعبه سفید

این نوع ممیزی امنیتی نسخه گسترده ای از محرمانگی جعبه خاکستری است که در آن آزمایش کنندگان دانش کاملی از داده های مورد نظر دارند. در صورت استفاده از یک برنامه وب، به هر گونه کد منبع علاوه بر آنچه در یک تست جعبه خاکستری اعطا می شود، به ما داده می شود.

معمولاً هنگام انجام ارزیابی امنیتی وب رویکرد جعبه خاکستری توصیه می شود زیرا ممکن است رویکرد جعبه سیاه پوشش کافی را فراهم نکند، به عنوان مثال وقتی بیشتر ویژگی ها پشت صفحه ورود به سیستم هستند و برنامه اجازه ثبت نام را نمی دهد.

تجربه گسترده ما در شناسایی آسیب پذیری های امنیتی در برنامه های تحت وب، موجب میشود تا آسیب پذیری های سطح Critical براحتی شناسایی و شکار کنیم.