شرکت مهندسی
اوژن تدبیر پارس

امنیت دستگاه‌های موبایل و نفوذ قانونمند
Mobile Device Security and Ethical Hacking

معرفی و کاربرد دوره

این دوره آموزشی SANs به منظور ارائه مهارت‌های موردنیاز برای شناخت نقاط قوت و ضعف امنیتی در iOS، اندروید و دستگاه‌های پوشیدنی مانند Apple Watch و Android Wear طراحی شده است. با استفاده از این مهارت‌ها می‌توان به ارزیابی نقاط ضعف امنیتی در برنامه‌های کاربردی پیش‌فرض کارخانه و جانبی پرداخت. در این دوره، فراگیران علاوه بر عبور از رمزنگاری پلتفورم چگونگی دستکاری برنامه‌های کاربردی تحت اندروید برای دور زدن تکنیک‌های درهم‌سازی را خواهند آموخت. همچنین به منظور شناسایی اشکالات در ترافیک شبکه برنامه‌های کاربردی موبایل، ذخیره‌سازی فایل سیستم و کانال‌های ارتباطی بین برنامه‌های کاربردی، از ابزارهای تحلیل خودکار و دستی برنامه‌های کاربردی استفاده خواهد شد. به علاوه، داوطلبان شرکت در این دوره با نمونه بدافزارهای موبایلی در شرایط ایمن کار خواهند کرد تا به آسیب‌پذیری داده‌ها و تهدیدات دسترسی اثرگذار بر دستگاه‌های تحت اندروید و iOS پی ببرند. همچنین به منظور به دست آوردن داده‌های حساس و مهم برنامه‌های کاربردی موبایلی از دستگاه‌های گمشده یا به سرقت رفته استفاده خواهد شد.

پیش نیازهای دوره

- آشنایی با مفاهیم تست نفوذپذیری شبکه
- دوره SEC504 ، کد SANSEC058
- دوره SEC560 ، کد SANSEC056

ابزار و منابع آموزشی

- لپ‌تاپ با سیستم عامل ویندوز یا macOS/ OSX

01 کد دوره: SANSEC072

02 مدت کل: ۴۸ ساعت

03 دسته بندی: Security

edu@clickpro.ir
www.clickpro.ir

اهـداف دوره

- توانایی استفاده از ابزارهای قفل‌شکن برای سیستم‌های تحت iOS و اندروید
- انجام تحلیل فایل سیستم iOS و اندروید برای سوءاستفاده از دستگاه‌های آسیب‌پذیر و استخراج اطلاعات کاربردی حساس دستگاه‌های موبایل
- تحلیل برنامه‌های کاربردی تحت iOS و اندروید با ابزارهای مهندسی معکوس
- تغییر قابلیت‌های برنامه‌های کاربردی تحت iOS و اندروید برای غلبه بر تکنیک‌های ضد قفل‌شکن یا دور زدن الزامات خرید درون‌برنامه‌ای
- ارزیابی امنیت خودکار برنامه‌های کاربردی موبایل
- استفاده از ابزارهای تحلیل شبکه‌های بی‌سیم برای شناسایی و سوءاستفاده از شبکه‌های بی‌سیم مورد استفاده در دستگاه‌های موبایل
- رهگیری و دستکاری فعالیت‌های شبکه در دستگاه‌های موبایل
- استفاده از چارچوب‌های اکسپلویت خاص دستگاه‌های موبایل به منظور دسترسی غیرمجاز به دستگاه‌های هدف
- دستکاری رفتار برنامه‌های کاربردی موبایل برای دور زدن محدودیت‌های امنیتی

مخاطبین دوره

- کارشناسان تست نفوذپذیری و نفوذگران قانونمند
- کـارشناسان ممیـزی با هـدف کسب مهـارت‌های فنـی عمیـق‌تـر
- کارکنان بخش امنیت کـه به واسطه شغل خود به ارزیابی، بکـارگیری و یا ایمن‌سازی موبایل و تبلت‌ها می‌پردازند.
- مدیران شبکه و سیستم‌ها که وظیفه پشتیبانی از تلفن‌های موبایل و تبلت‌ها را بر عهده دارند.

چرا به این دوره نیاز داریم

تصـور کنیـد کـه حملـه‌ای در سراسـر سـازمان شـما منتشـر شـود و ایـن کار بـه دسـت عواملـی انجـام گیـرد که بطـور مرتـب از جایی بـه جـای دیگـر می‌رونـد، داده‌هـای بـه شـدت حسـاس و مهـم را ذخیـره می‌کننـد و انـواع فناوری‌هـای بی‌سـیم مختلـف را، کـه همگـی مسـتعد حملـه هسـتند، مـورد اسـتفاده قـرار می‌دهنـد. امـروزه ایـن عوامـل بالقـوه همـان دسـتگاه‌های موبایـل هسـتند. ایـن دسـتگاه‌ها بزرگ‌تریـن سـطح حملـه در سـازمان‌های امـروزی را تشـکیل می‌دهنـد، امـا سـازمان‌ها اغلـب از مهارت‌هـای موردنیـاز بـرای ارزیابـی آنهـا برخـوردار نیسـتند. دسـتگاه‌های موبایـل دیگـر یـک فنـاوری رفاهـی محسـوب نمی‌شـوند، بلکـه ابزارهایـی ضـروری هسـتند کـه توسـط کاربـران در سراسـر جهـان حمـل شـده و اغلـب بـرای نیازهـای روزمـره سـازمان‌ها جایگزیـن رایانه‌هـای سـنتی می‌شـوند. ایـن رونـد در شـرکت‌ها، بیمارسـتان‌ها، بانک‌هـا، مـدارس و فروشـگاه‌های خرده‌فروشـی سراسـر جهـان دیـده می‌شـود. در واقـع کاربـران بیـش از هـر زمـان دیگـری بـه دسـتگاه‌های موبایـل اتـکا می‌کننـد، امـا آنچـه بایـد دانسـت ایـن اسـت که مهاجمان نیز رویکردی مشابه نسبت به این دستگاه‌ها دارند و این دوره دقیقا به حل‌وفصل همین مسئله می‌پردازد.

1 معماری دستگاه و تهدیدهای رایج موبایلی
Device Architecture and Common Mobile Threats

- چالش‌ها و فرصت‌های موبایل
  Mobile Problems and Opportunities
- تحلیل پلتفورم دستگاه‌های موبایل
  Mobile Device Platform Analysis
- پلتفورم‌های پوشیدنی
  Wearable Platforms
- ابزارهای تحلیل آزمایشگاهی دستگاه‌های موبایل
  Mobile Device Lab Analysis Tools
- تهدیدهای بدافزاری برای دستگاه‌های موبایل
  Mobile Device Malware Threats

2 دسترسی به پلتفورم‌های موبایل و تحلیل برنامه‌های کاربردی
Mobile Platform Access and Application Analysis

- رمزگشایی، دسترسی به بالاترین سطح کاربردی سیستم‌ها و قفل‌شکنی دستگاه‌های موبایل
  Unlocking, Rooting and Jailbreaking Mobile Devices
- ذخیره‌سازی داده‌های تلفن‌های موبایل و معماری فایل سیستم
  Mobile Phone Data Storage and File System Architecture
- پایش فعالیت‌های شبکه
  Network Activity Monitoring
- تحلیل ایستای برنامه‌های کاربردی
  Static Application Analysis

تهران، سعادت آباد، خ سرو غربی، خ بخشایش، کوچه هفدهم ساختمان اداری تجاری عرفان، پلاک ۵۴، طبقه سوم، واحد ۳۰۸
کد پستی: ۱۹۹۸۸۸۳۶۶۷
تلفن: ۲۲ - ۲۲۱۱۹۲۲۰ ۰۲۱
www.clickpro.ir edu@clickpro.ir

3 مهندسی معکوس برنامه‌های کاربردی موبایل
Mobile Application Reverse Engineering

- سیستم‌های تحلیل خودکار برنامه‌های کاربردی
  Automated Application Analysis Systems
- مهندسی معکوس برنامه‌های کاربردی درهم‌سازی شده
  Reverse Engineering Obfuscated Applications
- کارت‌های گزارش برنامه‌های کاربردی
  Application Report Cards

4 تست نفوذپذیری دستگاه‌های موبایل، بخش اول
Penetration Testing Mobile Devices, Part 1

- دستکاری رفتار برنامه‌های کاربردی
  Manipulating Application Behavior
- استفاده از تروجان‌های دسترسی از راه دور به دستگاه‌های موبایل
  Using Mobile Device Remote Access Trojans
- Probe Mapping شبکه‌های بی‌سیم
  Wireless Network Probe Mapping
- حملات ضعیف به شبکه‌های بی‌سیم
  Weak Wireless Attacks
- حملات امنیتی به شبکه‌های بی‌سیم سازمانی
  Enterprise Wireless Security Attacks
- حملات دستکاری شبکه
  Network Manipulation Attacks
- ربایش نشست‌ها در شبکه‌های بی‌سیم
  Sidejacking Attacks

5 تست نفوذپذیری دستگاه‌های موبایل، بخش اول
Penetration Testing Mobile Devices, Part 2

- حملات SSL/TLS
  SSL/TLS Attacks
- حملات تزریق سمت کاربر
  Client Side Injection (CSI) Attacks
- حملات فریم‌ورک مبتنی بر وب
  Web Framework Attacks
- حملات برنامه‌های کاربردی سمت سرور
  Back-end Application Support Attacks

6 برگزاری رویداد فتح پرچم
Capture the Flag