ژوان عبدمؤخر

مرکز آپا دانشگاه کردستان

معرفی دوره

PEN-210

Offensive Security Wireless Attacks

KURD SIRT

مقدمه

Offensive Security یک شرکت در حوزه امنیت اطلاعات، تست نفوذ و جرم‌شناسی دیجیتال بوده که توسط Mati Aharoni در سال ۲۰۰۷ تاسیس شد. این شرکت دارای پروژه‌های متن‌باز، دوره‌های امنیتی پیشرفته، بانک اطلاعاتی آسیب‌پذیری ExploitD و توزیع کالی لینوکس است و متخصصان امنیتی با تجربه در تست نفوذ و ارزیابی امنیتی سیستم‌ها را استخدام می‌کند. همچنین به بسیاری از شرکت‌های فناوری مشاوره امنیتی داده و دوره‌های مختلف و تخصصی در این زمینه ارائه می‌کند. در این مطلب دوره PEN-210: Offensive Security Wireless Attacks از Offensive Security توضیح داده خواهد شد.

سرفصل‌ها

PEN-210 مانند سایر دوره‌های آموزشی Offensive در حوزه امنیت، مفاهیم تئوری را با تمرین عملی در محیط آزمایشگاه مجازی ترکیب می‌کند. این دوره سرفصل‌های زیر را پوشش می‌دهد:

- IEEE 802.11
- شبکه‌های بی‌سیم
- رمزگذاری Wi-Fi
- ابزارها، درایورها و پشته‌ها
- کار با Wireshark
- تعامل شبکه
- کار با Aircrack-ng
- کرک‌کردن هش‌های مربوط به احراز هویت
- حمله به WPS
- بررسی نقاط دسترسی
- حمله به WPA
- کار با bettercap
- کار با Kismet
- بررسی چیپست‌ها و درایورها
- اتصالات دستی شبکه

مخاطبان

- مدیران شبکه
- کارشناسان امنیت سایبری
- علاقه‌مندان به شبکه و امنیت سایبری

توضیح در خصوص دوره

دوره PEN-210 فراگیران را با مهارت‌های مورد نیاز برای ارزیابی و ایمن‌سازی دستگاه‌های بی‌سیم آشنا می‌کند. این دوره، یک دوره آموزشی پایه در کنار PEN-200 است و برای کسانی که می‌خواهند مهارت بیشتری در امنیت شبکه کسب کنند مفید خواهد بود. درPEN-210، به فراگیران این آموزش داده خواهد شد که آسیب‌پذیری‌ها را در شبکه‌های 802.11 شناسایی کرده و حملات سازمان‌یافته را اجرا کنند. هر یک از فراگیران برای انجام آموزه‌های عملی این دوره یک آزمایشگاه راه‌اندازی خواهند کرد تا تکنیک‌های این دوره آنلاین را تمرین کنند. پس از تکمیل موفقیت آمیز دوره و امتحان، گواهینامه Offensive Security Wireless Professional یعنی OSWP به فراگیران اعطا می‌شود.

مشخصات

- آماده‌سازی برای گواهینامه OSWP
- زمان امتحان: ٤ ساعت
- ۳٫۵ ساعت فیلم دوره آموزشی
- ۳۸۰ صفحه راهنمای دوره
- دارای انجمن‌های دانشجویی فعال
- دسترسی به تنظیمات آزمایشگاه

پیش‌نیازها

- درک کامل از TCP/IP و مدل OSI و همچنین آشنایی با لینوکس.
- یک لپ‌تاپ یا سیستم که می‌تواند کالی لینوکس را بوت و اجرا کند.
- برای تکمیل تمرینات دوره به سخت‌افزارهای خاصی نیاز است؛

روترهای شبکه بی‌سیم توصیه شده:
NETGEAR AC1000 (R6080)
Linksys WiFi 5 Router Dual-Band AC1200 (E5400)
کارت بی‌سیم توصیه شده :
AWUS036NHA Alfa

آنچه خواهید آموخت

- قادر به شناسایی رمزگذاری‌ها و آسیب‌پذیری‌های موجود در شبکه های 802.11
- دورزدن محدودیت‌های امنیتی شبکه و بازیابی کلیدهای رمزگذاری در حال استفاده
- بینش بیشتر در مورد امنیت تهاجمی بی‌سیم و آگاهی گسترده از نیاز به راه‌حل‌های امنیتی در دنیای واقعی
- استفاده از ابزارهای مختلف شناسایی شبکه‌های بی‌سیم
- اجرای حملات علیه شبکه‌های رمزگذاری شده WPA Personal و Enterprise
- درک نحوه اجرای حملات مختلف rogue access point
- اجرای حملات علیه WPS
- استفاده از ابزارهای مختلف برای شکستن هش‌های مربوط به احراز هویت
- اجرای حملات علیه Captive Portals

لینک