Pentest Pack (SANS 560 + SANS 542)

Network Penetration Testing & Ethical Hacking
WEB App PenTesting and Ethical Hacking

مدت(ساعت): ۷۰ | **پیش نیاز:** مبانی اولیه امنیت | **اعتبار دهنده:** SANS

معرفی دوره :

دوره آموزشی SANS 560 + SANS 542 در قالب یک بسته آموزشی توسط تیم اساتید کاریار ارقام طراحی شده است.

این بخش به منظور آشنایی کارشناسان شبکه و متخصصین امنیت شبکه با روش های کاربردی نفوذ به منظور استفاده از این دانش جهت امن سازی و دفاع در برابر حملات سایبری می باشد و برگرفته از 2 دوره SANS 560 و PWK میباشد و در حقیقت نگاه یک رویکرد آشنایی با مسائل کاربردی و سناریو محور دارد.

امروزه Web Application ها نقشی بسیار حیاتی برای سازمانها و شرکت های بزرگ و کوچک بازی می کنند. اگر مجموعه شما نتواند به درستی به تست و ایمن سازی Web Application های موجود بپردازد ، نفوذگران با انجام اقدامات بدخواهانه میتوانند به خرابکاریهای متفاوت، سرقت اطلاعات و در نتیجه ضربه زدن به کسب و کار شما اقدام نمایند.گروه امنیت یک مجموعه میبایست در حد امکان به صورت دوره اقدام به تست وضعیت امنیت سرویس ها و نرم افزارهای تحت وب نماید تا نقاط آسیب پذیر در اینگونه برنامه ها تا حد ممکن شناسایی و راه کارهای مناسب برای رفع عیوب آنها نیز توسط تیم امنیت ارائه گردد.

محتوای دوره SEC542 شرکت SANS این کمک را به متخصصان تست نفوذ در زمینه وب مینماید تا با گذراندن این دوره وارد دنیای حرفه ای تست نفوذ پذیری نرم افزارهای تحت وب شوند.

اهداف دوره :

- آشنایی با متدولوژی ۴ مرحله ای SANS به منظور انجام WEB Application Penetration Testing
- آشنایی با نحوه آنالیز اولیه ابزارهای Automated WEB Testing
- آشنایی با حملات XSS
- کار با Browser Exploitation Framework

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
  - مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
  - سازمان مدیریت و برنامه ریزی کشور (معاونت توسعه مدیریت و سرمایه انسانی رئیس جمهوری سابق)
  - شورای عالی انفورماتیک
  - قابلیت ترجمه وتایید قوه قضاییه وامور خارجه
- برگزاری لابراتوارهای دوره مبتنی بر Workshop رسمی دوره

مخاطبان دوره :

- مدیران، کارشناسان، دانشجویان فعال در حوزه فناوری اطلاعات

Accredited by CARRIER DIGIT Computer Software LLC
EC-Council
تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس: ۸۸۰۶۵۲۲۲

Course Outline :

SANS 560:
- Comprehensive Pen Test Planning, Scoping, and Recon
- In-Depth Scanning
- Exploitation & Post-Exploitation and Merciless Pivoting
- Password Attacks and Web App Pen Testing
- Bypassing Antivirus
- Malware (Worm, Virus, Trojan)

SANS 542:
Web Penetration Testing and Ethical Hacking: Introduction and Information Gathering
- Overview of the web from a penetration tester's perspective
- Exploring the various servers and clients
- Discussion of the various web architectures
- Discovering how session state works
- Discussion of the different types of vulnerabilities
- Defining a web application test scope and process
- Defining types of penetration testing
- Heartbleed exploitation
- Utilizing the Burp Suite in web app penetration testing

Web Penetration Testing and Ethical Hacking: Configuration, Identity, and Authentication Testing
- Discovering the infrastructure within the application
- Identifying the machines and operating systems
- Secure Sockets Layer (SSL) configurations and weaknesses
- Exploring virtual hosting and its impact on testing
- Learning methods to identify load balancers
- Software configuration discovery
- Exploring external information sources
- Learning tools to spider a website
- Scripting to automate web requests and spidering
- Brute forcing unlinked files and directories
- Discovering and exploiting Shellshock

Web Penetration Testing and Ethical Hacking: Injection
- Python for web app penetration testing
- Web app vulnerabilities and manual verification techniques
- Information leakage and directory browsing
- Username harvesting
- Interception proxies
- Zed Attack Proxy (ZAP)
- Burp Suite

- Command Injection
- Directory traversal
- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)
- SQL injection
- Blind SQL injection
- JavaScript for the attacker

Web Penetration Testing and Ethical Hacking: JavaScript and XSS
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Session flaws
- Session fixation
- AJAX
- XML and JSON
- Logic attacks
- Data binding attacks
- Automated web application scanners
- w3af

Web Penetration Testing and Ethical Hacking: CSRF, Logic Flaws and Advanced Tools
- The sqlmap tool
- Metasploit for web penetration testers
- Exploring methods to zombify browsers
- Browser Exploitation Framework (BeEF)
- Leveraging attacks to gain access to the system
- How to pivot our attacks through a web application
- Understanding methods of interacting with a server through SQL injection
- Exploiting applications to steal cookies
- Executing commands through web application vulnerabilities
- Walking through an entire attack scenario

محتوای دوره :

EC-Council

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی ، ساختمان فردوس ، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، ۸ فاکس :۸۸۰۶۵۲۲۲