IT Professional Training Center

SANS SEC560: Network Penetration Testing and Ethical Hacking

(دوره تست نفوذ شبکه و هک قانونمند)

خلاصه دوره: دوره SANS SEC560 شما را برای انجام تست های نفوذ موفقیت آمیز آماده میکند. در این دوره شما نحوه شناسایی دقیق اهداف (Reconnaissance) و دسترسی از آنها را یاد خواهید گرفت ، با شیوه اسکن شبکه با استفاده از بهترین ابزار ها در آزمایشگاه ها و لابراتوار های عملی آشنا خواهید شد. علاوه بر ابزار های شناخته شده تست نفوذ ، شما با ابزار هایی که کمتر شناخته شده اند اما بسیار مفید هستند نیز کار خواهید کرد. در انتهای این دوره بین دانشجویان یک مسابقه فتح پرچم (CTF) برگزار خواهد شد.

شما به عنوان یک متخصص در حوزه امنیت سایبری (Cyber Security) و تست نفوذ (Pentest) ، وظیفه دارید آسیب پذیری های زیر ساخت های مختلف را شناسایی کرده و آنها را گزارش کنید. این کار باعث میشود که آسیب پذیری ها قبل از اینکه توسط هکر پیدا شده و استفاده شوند ، بر طرف شود. دوره SEC560 دوره ای ویژه برای یادگیری تست نفوذ (Penetration Testing) است.

دوره SEC560 با پوشش گسترده ای از ابزار های قدرتمند ، تکنیک ها و روش های تست نفوذ شبکه ، شما را برای انجام پروژه های تست نفوذ آماده میکند. هر شرکت یا سازمانی به پرسنلی نیاز دارد تا آسیب پذیری ها را بیابند و ریسک ها را کاهش دهند. این دوره برای آمادگی شما برای این نقش طراحی شده است. این دوره با برنامه ریزی صحیح شروع میشود و پس از آن ، شما نحوه مشخص کردن دامنه اهداف ، اسکن ، دسترسی و ... آشنا خواهید شد. تمامی مطالبی که در این دوره به شما آموخته میشود کاملا عملی بوده و لابراتوار های مختلفی برای تمرین در اختیار شما قرار میگیرد.

دوره SEC560 به منظور آماده سازی شما برای انجام یک تست نفوذ کامل و دقیق و با ارزش بالا طراحی شده است. پس از انجام تمرین ها و سناریو های مختلف ، این دوره با یک سناریو نهایی که شبیه سازی تست نفوذ در دنیای واقعی است به اتمام میرسد که برای انجام آن باید از دانش ، تجربه و ابزار هایی که در طول دوره یاد گرفتید استفاده کنید."

طول دوره:" ۴۰ ساعت

پیشنیاز: SANS SEC301: Introduction to Cyber Security

اهداف دوره: پس از اتمام این دوره شما میتوانید نحوه شناسایی دقیق (Reconnaissance) ، مطالعه زیر ساخت های هدف با استفاده از وبلاگ ها ، موتور های جست و جو ، شبکه های اجتماعی و سایر زیر ساخت های اینترنت را انجام دهید. در آزمایشگاه های عملی شما را قادر میسازیم تا با استفاده از بهترین ابزار ها ، شبکه های هدف را اسکن کنید. پس از آن روش های مختلف برای نفوذ به سیستم های مختلفی که در شبکه یک شرکت یا سازمان وجود دارند را یاد خواهید گرفت. حملات رمز عبور (Password Attacks) و اپلیکیشن های تحت وب دیگر اهداف این دوره خواهند بود. و در نهایت ما به قلب فناوری بیشتر سازمان ها یعنی سرویس Active Directory تمرکز خواهیم کرد. جزئیات فنی Kerberos و Windows Domain را پوشش خواهیم داد و از آنها برای نفوذ به Domain استفاده خواهیم کرد.

در انتهای این دوره دانشجویان موارد زیر را یا خواهند گرفت:

- برای اطمینان از متمرکز بودن و اجرای صحیح پروژه تست نفوذ محدوده و قوانین مختلفی ایجاد کنند.
- با استفاده از تکنیک های Reconnaissance ، موتور های جست و جو و سایر منابع اطلاعاتی که در دسترس عموم است ، شناسایی دقیقی (فنی و سازمانی) از هدف انجام دهند.

- با استفاده از ابزار Nmap ، شبکه و زیرساخت هدف را برای شناسایی پورت های باز ، سیستم عامل و ... اسکن کنند.
- اسکنر های امنیتی مختلف (Vulnerability Scanners) مانند Nessus ، Core Impact ، IBM Scanner و ... را کانفیگ کرده و نحوه کار با آنها برای شناسایی آسیب پذیری سیستم های مختلف را یاد بگیرند.
- از ابزار هایی مانند Netcat و Scapy برای کاهش False-Positive اسکن ، استفاده کنند.
- از ترمینال لینوکس و CMD ویندوز در جهت اهداف تست نفوذ استفاده کنند.
- از Metasploit استفاده و آن های برای مراحل مختلف تست نفوذ کانفیگ کنند.
- حملات مختلف رمز عبور (Password Attacks) را انجام دهند.
- با اسکنر های آسیب پذیری وب کار کرده و سپس به صورت دستی حملات CSRF ، XSS ، Command Injection و SQL Injection را انجام دهند.

مخاطبین دوره:

- تمامی علاقه مندان به تست نفوذ و هک
- پرسنل امنیتی که کار آنها ارزیابی شبکه و سیستم ها برای پیدا کردن و رفع آسیب پذیری های مختلف است.
- متخصصان تست نفوذ (Penetration testers)
- هکر های اخلاقی و قانونمند
- متخصصان امنیتی و فعالین شاخه های (Defensive) که میخواهد روش ها ، ابزار ها و تکنیک های تهاجمی (Offensive) را بهتر درک کنند.
- اعضای تیم قرمز (Red Team)
- اعضای تیم آبی (Blue Team)
- متخصصان فارنزیک – جرم شناسی دیجیتال (Digital Forensics) که میخواهند تاکتیک های تهاجمی (Offensive) را بهتر درک کنند.

سرفصل های دوره:

- SEC560.1: Comprehensive Pen Test Planning, Scoping, and Recon
  Exercises:
  - Tour of the SANS Slingshot Penetration Testing Virtual Machine
  - Formulating an Effective Scope and Rules of Engagement
  - Document Metadata Treasure Hunt
  - Utilizing Recon-ng to Plunder DNS for Useful Information

  Topics:
  - The Mindset of the Professional Pen Tester
  - Building a World-Class Pen Test Infrastructure
  - Creating Effective Pen Test Scopes and Rules of Engagement
  - Detailed Recon Using the Latest Tools
  - Effective Pen Test Reporting to Maximize Impact
  - Mining Search Engine Results
  - Document Metadata Extraction and Analysis

- SEC560.2: In-Depth Scanning
  Exercises:
  - Getting the Most Out of Nmap
  - OS Fingerprinting and Version Scanning In-Depth
  - The Nmap Scripting Engine
  - The Nessus Vulnerability Scanner
  - Netcat for the Pen Tester
  - PowerShell for the Pen Tester

Topics:

- Tips for Awesome Scanning
- Tcpdump for the Pen Tester
- Nmap In-Depth: The Nmap Scripting Engine
- Version Scanning with Nmap
- Vulnerability Scanning with Nessus
- False-Positive Reduction
- Enumerating Users
- Netcat for the Pen Tester
- Monitoring Services during a Scan

- SEC560.3: Exploitation

Exercises:

- Client-Side Attacks with Metasploit
- Exploiting Network Services and Leveraging the Meterpreter
- Evading Anti-Virus Tools with the Veil Framework
- Metasploit Databases and Tool Integration
- Port Pivoting Relays
- Leveraging PowerShell Empire for Post Exploitation
- Creating Malicious Services and Leveraging the Wonderful WMIC Toolset

Topics:

- Comprehensive Metasploit Coverage with Exploits, Stagers, and Stages
- Strategies and Tactics for Anti-Virus Evasion
- In-Depth Meterpreter Analysis, Hands-On
- Implementing Port Forwarding Relays for Merciless Pivots
- How to Leverage PowerShell Empire to Plunder a Target Environment

- SEC560.4: Password Attacks and Merciless Pivoting

Exercises:

- Password Guessing and Spraying with THC-Hydra
- Metasploit Psexec, Hash Dumping and Mimikatz Kiwi Credential Harvesting
- Pivoting with Metasploit and SSH
- Password Cracking with John the Ripper and Hashcat
- Sniffing and Cracking Windows Authentication Exchanges
- Metasploit Pivoting and Mimikatz Kiwi for Credential Harvesting

Topics:

- Windows Command Line Kung Fu for Penetration Testers
- PowerShell's Amazing Post-Exploitation Capabilities
- Password Attack Tips
- Account Lockout and Strategies for Avoiding It
- Automated Password Guessing with THC-Hydra
- Retrieving and Manipulating Hashes from Windows, Linux, and Other Systems
- Pivoting through Target Environments
- Extracting Hashes and Passwords from Memory with Mimikatz Kiwi

- SEC560.5: Domain Domination and Web App Pen Testing

Exercises:

- Kerberos Attacks
- Attacking Nearby Clients with Responder
- Domain Mapping and Exploitation with Bloodhound
- Effective Domain Privilege Escalation
- Domain Dominance
- Using the ZAP Proxy to Manipulate Custom Web Applications
- Leveraging Command Injection Flaws
- Exploiting SQL Injection Flaws to Gain Shell Access of Web Targets

Topics:

- Kerberos authentication protocol
- Poisoning multicast name resolution with Responder
- Domain Mapping and Exploitation with Bloodhound

- Effective Domain Privilege Escalation
- Persisting administrative domain access
- Using the ZAP Proxy to Manipulate Custom Web Applications
- Maximizing Effectiveness of Command Injection Testing
- Data Plundering with SQL Injection
- Leveraging SQL Injection to Perform Command Injection

- SEC560.6: Penetration Testing Workshop

  Exercises:
  - A Comprehensive Lab Applying What You Have Learned Throughout the Course
  - Modeling a Penetration Test Against a Target Environment

  Topics:
  - Applying Penetration Testing and Ethical Hacking Practices End-to-End
  - Detailed Scanning to find Vulnerabilities and Avenues to Entry
  - Exploitation to Gain Control of Target Systems
  - Post-Exploitation to Determine Business Risk
  - Merciless Pivoting
  - Analyzing Results to Understand Business Risk and Devise Corrective Actions