SANS SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

(دوره پیشرفته تست نفوذ ، اکسپلویت نویسی و هک قانونمند)

طول دوره:"۶۰ ساعت"

پیشنیاز:

- SANS SEC560: Network Penetration Testing and Ethical Hacking
- مفاهیم پایه برنامه نویسی
- آشنایی با یک زبان برنامه نویسی مانند پایتون

توضیحات دوره: روز به روز حملات مهاجمان هوشمندانه تر و روش های آنها پیچیده تر میشود. شما برای همگام شدن با جدیدترین روش های حمله به یک میل شدید برای یادگیری ، پشتیبانی ، و فرصتی برای تمرین و ایجاد تجربه نیاز دارید. دوره SEC660 به عنوان ادامه مسیر و یک نقطه پیشرفت برای دانشجویانی که دوره SEC560 را گذرانده و یا تجربه عملی کافی در تست نفوذ دارند طراحی شده است. این دوره به شما دانش عمیق در مورد برجسته ترین و قدرتمند ترین محور های حمله میدهد. این دوره هم مانند دوره SEC560 دارای آزمایشگاه های عملی است. مفاهیم در اینجا فراتر از چندین اسکن ساده برای پیدا کردن آسیب پذیری های مختلف است و به شما نحوه استفاده از توانایی های یک مهاجم پیشرفته برای یافتن آسیب پذیری های قابل توجه آموزش داده میشود.

در هر جلسه ابتدا مفاهیم و توضیحات حمله گفته خواهد شد و سپس حمله به طور عملی انجام خواهد شد. پس از آن برای تثبیت مطالب در ذهن ، حمله توسط دانشجویان در یک محیط آزمایشگاهی انجام میشود. پس از پایان هر جلسه یک تمرین به همراه لابراتوار در اختیار دانشجویان قرار داده میشود. از موضوعات مورد بحث میتوان به استفاده از پایتون برای تست نفوذ ، حمله هایی به NAC (Network Access Control) ، حمله هایی به VLAN (Virtual Local Area Network) ، بیرون آمدن از محیط های محدود شده لینوکس و ویندوز ، IPv6 ، بالا بردن سطح دسترسی (Privilege Escalation) در لینوکس و ویندوز ، اکسپلویت نویسی لینوکس و ویندوز ، Fuzzing ، دور زدن کنترل های امنیتی مدرن سیستم عامل ها مانند ASLR ، DEP و بسیاری موارد دیگر اشاره کرد.

اهداف دوره: این دوره با معرفی مفاهیم پیشرفته تست نقوذ و ارائه یک نمای کلی برای آماده سازی دانشجویان در رابطه با آنچه در پیش است شروع میشود. در ابتدا تمرکز بر روی حملات شبکه است. عناوین این بخش شامل دسترسی ، دستکاری و اکسپلویت کردن آن است. حملات بر روی NAC ، VLANs ، OSPF ، 802.1x ، CDP ، IPv6 ، VOIP ، SSL ، ARP ، SNMP و ... انجام میشود. در ادامه نحوه انجام تست نفوذ بر روی پیاده سازی های مختلف رمزنگاری آموزش داده میشود. در ادامه زبان برنامه نویسی پایتون و کاربرد آن در تست نفوذ معرفی میشود. در نهایت حمله هایی که بر بستر سیستم عامل امکان پذیر است گفته خواهد شد. شما نحوه شناسایی Privileged Programs را یاد خواهید گرفت ، با مهندسی معکوس (Reverse Engineering) برای پیدا کردن کد های آسیب پذیر یک برنامه آشنا خواهید شد ، کنترل های امنیتی مدرن مانند ASLR ، DEP را دور خواهید زد.

به طور خلاصه:

- نحوه انجام تست نفوذ بر روی دیوایس های شبکه مانند روتر ها و سوییچ ها را یاد خواهید گرفت.
- تست نفوذ NAC (Network Access Control)
- تست نفوذ پیاده سازی های رمزنگاری (Cryptography Pentest)
- Fuzzing
- مهندسی معکوس (Reverse Engineering) کد های برنامه های ویندوزی و لینوکسی

- نحوه نوشتن اکسپلویت برای اپلیکیشن های ویندوزی و لینوکسی
- نحوه دور زدن (Bypass) ، DEP و ASLR

مخاطبین دوره:

- متخصصین تست نفوذ شبکه (Network and Systems Penetration Testers)
- کنترل و مدیریت کنندگان حادثه (Incident Handlers)
- توسعه دهندگان نرم افزار (Application Developers)
- متخصصین IDS (IDS Engineers)

سرفصل های دوره:

- **SEC660.1: Network Attacks for Penetration Testers**
  Topics:
  - Bypassing network access/admission control (NAC)
  - Impersonating devices with admission control policy exceptions
  - Exploiting EAP-MD5 authentication
  - Custom network protocol manipulation with Ettercap and custom filters
  - Multiple techniques for gaining man-in-the-middle network access
  - IPv6 for penetration testers
  - Exploiting OSPF authentication to inject malicious routing updates
  - Using Evilgrade to attack software updates
  - Overcoming SSL transport encryption security with SSLstrip
  - Remote Cisco router configuration file retrieval

- **SEC660.2: Crypto and Post-Exploitation**
  Topics:
  - Pen testing cryptographic implementations
  - Exploiting CBC bit flipping vulnerabilities
  - Exploiting hash length extension vulnerabilities
  - Delivering malicious operating systems to devices using network booting and PXE
  - PowerShell Essentials
  - Enterprise PowerShell
  - Post Exploitation with PowerShell and Metasploit
  - Escaping Software Restrictions
  - Two-hour evening Capture the Flag exercise against a modern network with hardened servers, desktops, and vApp targets

- **SEC660.3: Python, Scapy, and Fuzzing**
  Topics:
  - Becoming familiar with Python types
  - Leveraging Python modules for real-world pen tester tasks
  - Manipulating stateful protocols with Scapy
  - Using Scapy to create a custom wireless data leakage tool
  - Product security testing
  - Using Taof for quick protocol mutation fuzzing
  - Optimizing your fuzzing time with smart target selection
  - Automating target monitoring while fuzzing with Sulley
  - Leveraging Microsoft Word macros for fuzzing .docx files
  - Block-based code coverage techniques using Paimei

- **SEC660.4: Exploiting Linux for Penetration Testers**
  Topics:
  - Stack and dynamic memory management and allocation on the Linux OS
  - Disassembling a binary and analyzing x86 assembly code
  - Performing symbol resolution on the Linux OS
  - Identifying vulnerable programs
  - Code execution redirection and memory leaks
  - Identifying and analyzing stack-based overflows on the Linux OS
  - Performing return-to-libc (ret2libc) attacks on the stack
  - Return-oriented programming
  - Defeating stack protection on the Linux OS
  - Defeating ASLR on the Linux OS

- **SEC660.5: Exploiting Windows for Penetration Testers**
  Topics:
  - The state of Windows OS protections on Windows 7, 8, 10, Server 2008 and 2012
  - Understanding common Windows constructs
  - Stack exploitation on Windows
  - Defeating OS protections added to Windows
  - Creating a Metasploit module
  - Advanced stack-smashing on Windows
  - Using ROP
  - Building ROP chains to defeat DEP and bypass ASLR
  - Windows 7 and Windows 8 exploitation
  - Porting Metasploit modules
  - Client-side exploitation
  - Windows Shellcode

- **SEC660.6: Capture the Flag Challenge**