SEC573: Automating Information Security with Python *NEW!*

Mon, 3 July - Sat, 8 July | Laptop Required | GIAC Cert: GPYC | Instructor: Jonathan Thyer

Writing a tool is easier said than done, right? Not really. Python is a simple, user-friendly language that is designed to make automating tasks that security professionals perform quick and easy. Whether you are new to coding or have been coding for years, **SEC573 Automating Information Security** with Python will have you creating programs to make your job easier and make you more efficient. This self-paced class starts from the very beginning assuming you have no prior experience or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced material in the class. The self-paced style of the class will meet you where you are to let you get the most out of the class you can. Beyond the essentials we discuss file analysis, packet analysis, forensics artifact carving, networking, database access, website access, process execution, exception handling, object oriented coding and more.

This course is designed to give you the skills you need for tweaking, customizing, or outright developing your own tools. We put you on the path of creating your own tools, empowering you in automating the daily routine of today's information security professional, achieving more value in less time. Again and again, organisations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it. Join us and learn Python in-depth and fully weaponized.

CORE NETWARS EXPERIENCE

29-30 June | Pieter Danhieux

The Core NetWars Experience is a computer and network security challenge designed to test a participant's experience and skills in a safe, controlled environment while having a little fun with your fellow IT security professionals. Many enterprises, government agencies, and military bases are using NetWars to help identify skilled personnel and as part of extensive hands-on training. With Core NetWars, you'll build a wide variety of skills while having a great time.

Who Should Attend

- Security professionals
- System administrators
- Network administrators
- Ethical hackers
- Penetration testers
- Incident handlers
- Security auditors
- Vulnerability assessment personnel
- Security Operations Center staff

www.sans.org/cyber-defence-canberra-2017

SANS Instructors

SANS instructors are real-world practitioners who specialise in the subjects they teach. All instructors undergo rigorous training and testing in order to teach SANS courses. This guarantees that what you learn in class will be up to date and relevant to your job. The SANS Cyber Defence Canberra 2017 lineup of instructors includes:

Pieter Danhieux
Principal Instructor
@PieterDanhieux

Mick Douglas
Instructor
@BetterSafetyNet

Jess Garcia
Principal Instructor
@j3ssgarcia

Tim Garcia
Certified Instructor
@tbg911

Bryan Simon
Certified Instructor
@BryanOnSecurity

Jonathan Thyer
Instructor
@joff_thyer

Training Campus

Canberra Rex Hotel

150 Northbourne Avenue | Canberra, 2612 AU
+61 (0)2 6248 5311 | www.canberrarexhotel.com

Save $350 USD when you register and pay by 3 May

Contact Information

For further information, please contact:

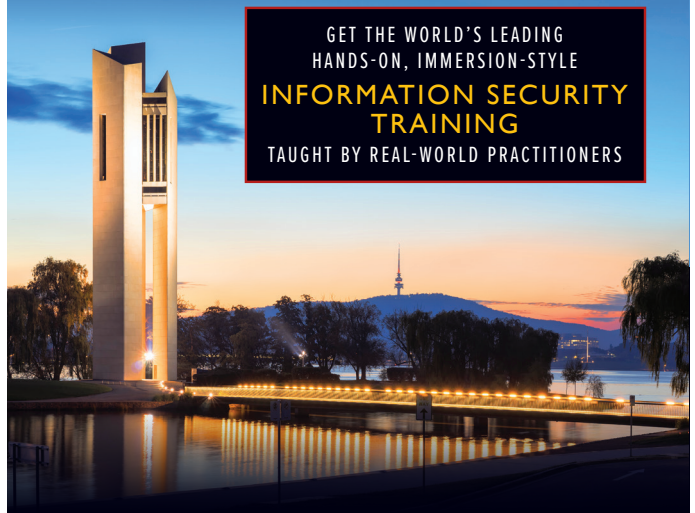
Email: **asiapacific@sans.org** | Call: **(02) 6198 3352**

REGISTER AT
www.sans.org/cyber-defence-canberra-2017

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS CYBER DEFENCE Canberra 2017

26 June – 8 July | Venue: Canberra Rex Hotel



GET THE WORLD'S LEADING
HANDS-ON, IMMERSION-STYLE
INFORMATION SECURITY TRAINING
TAUGHT BY REAL-WORLD PRACTITIONERS

Seven courses in:

- CYBER DEFENCE
- PENETRATION TESTING
- INCIDENT RESPONSE
- CYBER THREAT INTELLIGENCE
- ETHICAL HACKING
- PYTHON SECURITY

GIAC CERTIFICATIONS
GIAC-Approved Training

And featuring

CORE NETWARS EXPERIENCE

SAVE $350 USD
for any 5-6 day course paid for by 3 May 2017

REGISTER AT
www.sans.org/cyber-defence-canberra-2017

SEC301: Intro to Information Security

Mon, 26 June - Fri, 30 June | Laptop Required | GIAC Cert: GISF | Instructor: Tim Garcia

To determine if the SANS SEC301 course is right for you, ask yourself five simple questions:

- Do you have basic computer knowledge, but are new to information security and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Are you a non-IT security manager (with some technical knowledge) who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?
- Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?

If you answer yes to any of these questions, the **SEC301: Intro to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cyber security. The hands-on, step-by-step teaching approach will enable you to grasp all the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

SEC401: Security Essentials Bootcamp Style

Mon, 3 July - Sat, 8 July | Laptop Required | GIAC Cert: GSEC | Instructor: Bryan Simon

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment. SEC401 is focused on teaching you the essential information security skills and techniques you need to protect and secure your organisation's critical information assets and business systems. Our course will show you how to prevent your organisation's security problems from being headline news!

PREVENTION IS IDEAL BUT DETECTION IS A MUST

Security is all about making sure you focus on the right areas of defence. In SEC401 you will learn the language and underlying theory of computer and information security. You will gain the essential and effective security knowledge you will need if you are given the responsibility for securing systems and/or organisations. This course meets both of the key promises SANS makes to our students: (1) You will learn up-to-the-minute skills you can put into practice immediately upon returning to work; and (2) You will be taught by the best security instructors in the industry.

SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling

Mon, 3 July - Sat, 8 July | Laptop Required | GIAC Cert: GCIH | Instructor: Mick Douglas

The Internet is full of powerful hacking tools and bad guys using them extensively. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

This course enables you to turn the tables on computer attackers by helping you to understand their tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare for, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

SEC505: Securing Windows and PowerShell Automation

Mon, 26 June - Sat, 1 July | Laptop Required | GIAC Cert: GCWN | Instructor: Bryan Simon

Hackers know how to use PowerShell for evil, do you know how to use it for good? In SEC505 you will learn PowerShell and Windows security hardening at the same time. SecOps requires automation, and Windows automation means PowerShell.

You've run a vulnerability scanner and applied patches – now what? A major theme of this course is defensible design: we have to assume that there will be a breach, so we need to build in damage control from the beginning. Whack-a-mole incident response cannot be our only defensive strategy – we'll never win, and we'll never get ahead of the game. By the time your monitoring system tells you a Domain Admin account has been compromised, it's TOO LATE.

For the assume breach mindset, we must carefully delegate limited administrative powers so that the compromise of one administrator account is not a total catastrophe. Managing administrative privileges is a tough problem, so this course devotes an entire day to just this one critical task.

Learning PowerShell is also useful for another kind of security: job security. Employers are looking for people with these skills. You don't have to know any PowerShell to attend the course, we will learn it together. About half the labs during the week are PowerShell, while the rest use graphical security tools. PowerShell is free and open source on GitHub for Linux and Mac OS too.

SEC560: Network Penetration Testing and Ethical Hacking

Mon, 26 June - Sat, 1 July | Laptop Required | GIAC Cert: GPEN | Instructor: Pieter Danhieux

SEC560 is designed to get you ready to conduct a full-scale, high-value penetration test - and on the last day of the course you'll do just that. After building your skills in comprehensive and challenging labs over five days, the course culminates with a final full-day, real-world penetration test scenario. You'll conduct an end-to-end pen test, applying knowledge, tools, and principles from throughout the course as you discover and exploit vulnerabilities in a realistic sample target organisation, demonstrating the knowledge you've mastered in this course.

You will learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Our hands-on labs will equip you to scan target networks using best-of-breed tools. We won't just cover run-of-the-mill options and configurations, we'll also go over the lesser known but super-useful capabilities of the best pen test toolsets available today. After scanning, you'll learn dozens of methods for exploiting target systems to gain access and measure real business risk. You'll dive deep into post-exploitation, password attacks, and web apps, pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defence in depth.

FOR578: Cyber Threat Intelligence

Mon, 26 June - Fri, 30 June | Laptop Required | Instructor: Jess Garcia

Make no mistake: current network defence, threat hunting, and incident response practices contain a strong element of intelligence and counterintelligence that cyber analysts must understand and leverage in order to defend their networks, proprietary data, and organisations.

FOR578 will help network defenders, threat hunting teams, and incident responders to:

- Understand and develop skills in tactical, operational, and strategic level threat intelligence
- Generate threat intelligence to detect, respond to, and defeat advanced persistent threats (APTs)
- Validate information received from other organisations to minimize resource expenditures on bad intelligence
- Leverage open-source intelligence to complement a security team of any size
- Create Indicators of Compromise (IOCs) in formats such as YARA, OpenIOC, and STIX.

The collection, classification, and exploitation of knowledge about adversaries - collectively known as cyber threat intelligence - gives network defenders information superiority that is used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture.

FOR578: Cyber Threat Intelligence will train you and your team in the tactical, operational, and strategic level cyber threat intelligence skills and tradecraft required to make security teams better, threat hunting more accurate, incident response more effective, and organisations more aware of the evolving threat landscape.