SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling

10-15 July | GIAC Cert: GCIH | George Bakos & Zach Matthis

By helping you understand attackers' 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, this course helps you turn the tables on computer attackers. 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, detect, and respond to them.

Taught in Japanese Language

SEC401
Security Essentials Bootcamp Style

5-7 & 12-14 July | GIAC Cert: GSEC | Satoshi Hayashi & Masafumi Negishi

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 organization's critical information assets and business systems. Our course will show you how to prevent your organization's security problems from being headline news!

"This course is an eye opener for anyone who cares about securing their information today!"

-Don Cervone, Bridgewater Associates

SEC575
Mobile Device Security and Ethical Hacking

10-15 July | GIAC Cert: GMOB | Tim Medin

This course is designed to give you the skills you need to understand the security strengths and weaknesses in Apple iOS, Android, and wearable devices including Apple Watch and Android Wear. With these skills, you will evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption, and how to manipulate Android apps to circumvent obfuscation techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you'll exploit lost or stolen devices to harvest sensitive mobile application data.

SEC660
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

10-15 July | GIAC Cert: GXPN | Stephen Sims

This course is designed as a logical progression point for those who have completed SANS SEC560, or for those with existing penetration testing experience. Students with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a real-world lab environment to solidify advanced concepts and allow for the immediate application of techniques in the workplace. Each day includes a two-hour evening bootcamp to allow for additional mastery of the techniques discussed and even more hands-on exercises. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and VLAN manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as ASLR and DEP, return-oriented programming (ROP), Windows exploit-writing, and much more!

SANS

Training Roadmap | Choose Your Path

Please join us for the first Core NetWars Experience in Japan!

CORE NETWARS EXPERIENCE

13-14 July, 18:00 - 21:00

Led by Tim Medin

Core NetWars is a computer and network security challenge designed to test a participant's experience and skills in a safe 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.

NetWars Coin for Winners!

Baseline Skills

1 **You are** experienced in technology, but need to learn hands-on, essential security skills and techniques

Core Security Techniques
Defend & Maintain

Every security professional should know the defense-in-depth techniques taught in SEC401, and SEC504 completes the "offense informs defense" preparation that teaches defense specialists how attacks occur and how to respond. If you've got the core defense skills, start with SEC504.

- **SEC401** Security Essentials Bootcamp Style — **GSEC** Certification Security Essentials
- **SEC504** Hacker Tools, Techniques, Exploits, and Incident Handling — **GCIH** Certification Certified Incident Handler

1b **You** will be responsible for managing security teams or implementations, but you do not require hands-on skills

Security Management

- **MGT512** SANS Security Leadership Essentials for Managers with Knowledge Compression™ — **GSLC** Certification Security Leadership
- **SEC566** Implementing and Auditing the Critical Security Controls – In-Depth — **GCCC** Certification Critical Security Controls

New to Cybersecurity?

- **SEC301** Intro to Information Security — **GISF** Certification Information Security Fundamentals

Intermediate Job Roles

2 **You are** experienced in security, preparing for a specialized job role or focus

Security Monitoring & Detection

- **SEC503** Intrusion Detection In-Depth — **GCIA** Certification Certified Intrusion Analyst
- **SEC511** Continuous Monitoring and Security Operations — **GMON** Certification Continuous Monitoring

Penetration Testing & Vulnerability Analysis

- **SEC560** Network Penetration Testing and Ethical Hacking — **GPEN** Certification Penetration Tester
- **SEC542** Web App Penetration Testing and Ethical Hacking — **GWAPT** Certification Web Application Penetration Tester

Incident Response and Enterprise Forensics

- **FOR508** Advanced Digital Forensics, Incident Response, and Threat Hunting — **GCFA** Certification Forensic Analyst
- **FOR572** Advanced Network Forensics and Analysis — **GNFA** Certification Network Forensic Analyst

- **MGT414** SANS Training Program for CISSP® Certification — **GISP** Certification Information Security Professional

Crucial Skills, Specialized Roles

SANS' comprehensive course offerings enable professionals to deepen their technical skills in key practice areas. The courses also address other topics and audiences, such as security training for software developers, industrial control engineers, and non-technical personnel in management, legal, and audit.

3 **You are** a candidate for specialized or advanced training

Cyber Defense Operations

- SEC501 Advanced Security Essentials – Enterprise Defender **GCED**
- SEC505 Securing Windows and PowerShell Automation **GCWN**
- SEC506 Securing Linux/Unix | **GCUX**
- SEC566 Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC**
- SEC579 Virtualization and Software-Defined Security

Industrial Control Systems Security

- ICS410 ICS/SCADA Security Essentials | **GICSP**
- ICS456 Essentials for NERC Critical Infrastructure Protection
- ICS515 ICS Active Defense and Incident Response | **GRID**

Penetration Testing & Ethical Hacking

- SEC550 Active Defense, Offensive Countermeasures and Cyber Deception
- SEC561 Immersive Hands-On Hacking Techniques
- SEC562 CyberCity Hands-on Kinetic Cyber Range Exercise
- SEC573 Automating Information Security with Python | **GPYC**
- SEC575 Mobile Device Security and Ethical Hacking | **GMOB**
- SEC617 Wireless Ethical Hacking, Penetration Testing, and Defenses | **GAWN**
- SEC642 Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques
- SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | **GXPN**
- SEC760 Advanced Exploit Development for Penetration Testers

Digital Forensics and Incident Response

- FOR408 Windows Forensic Analysis | **GCFE**
- FOR518 Mac Forensic Analysis
- FOR526 Memory Forensics In-Depth
- FOR578 Cyber Threat Intelligence
- FOR585 Advanced Smartphone Forensics | **GASF**
- FOR610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques | **GREM**

Software Security

- DEV522 Defending Web Applications Security Essentials **GWEB**
- DEV541 Secure Coding in Java/JEE: Developing Defensible Applications | **GSSP-JAVA**
- DEV544 Secure Coding in .NET: Developing Defensible Applications | **GSSP-.NET**

Management

- MGT514 IT Security Strategic Planning, Policy, and Leadership
- MGT517 Managing Security Operations: Detection, Response, and Intelligence
- MGT525 IT Project Management, Effective Communication, and PMP® Exam Prep | **GCPM**

Audit | Legal

- AUD507 Auditing & Monitoring Networks, Perimeters, and Systems | **GSNA**
- SEC566 Implementing and Auditing the Critical Security Controls – In-Depth | **GCCC**
- LEG523 Law of Data Security and Investigations | **GLEG**