THE MOST TRUSTED NAME FOR INFORMATION AND SOFTWARE SECURITY TRAINING WORLDWIDE

SANS Secure India 2017

20 Feb - 4 Mar | Venue: Le Meridien Bangalore

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling

20-25 Feb | GIAC Cert: GCIH | Steve Armstrong

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.

SEC503
Intrusion Detection In-Depth

27 Feb - 4 Mar | GIAC Cert: GCIA | Jonathan Ham

SEC503 delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. Our goal is to acquaint you with the core knowledge, tools, and techniques to defend your networks. The training will prepare you to put your new skills and knowledge to work immediately upon returning to a live environment.

FOR508
Advanced Threat Hunting and Incident Response

20-25 Feb | GIAC Cert: GCFA | Jake Williams

This in-depth incident response and threat hunting course provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, organized crime syndicates, and hactivism. Constantly updated, FOR508 addresses today's incidents by providing hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to detect, counter, and respond to real-world breach cases.

FOR578
Cyber Threat Intelligence

27 Feb - 3 Mar | Jake Williams

During a targeted attack, an organization needs a top-notch and cutting-edge incident response armed with the critical intelligence necessary to understand how adversaries operate and to combat the threat. FOR578 will train you and your team to detect, scope, and select resilient courses of action in response to such intrusions and data breaches.

GIAC

For further information, contact:

aroy@sans.org | +91-9741900324 (Arindam Roy)

ajohns@sans.org | +91 9717886943 (Andrew Johns)

www.sans.org/secure-india-2017

SANS CURRICULUM ROADMAPS

SECURITY CURRICULUM

Beginners

SEC301 NOTE:
If you have experience in the field, please consider our more advanced course – SEC401.

SEC301 Intro to Information Security **GISF**

Penetration Testing

SEC401 Security Essentials Bootcamp Style **GSEC**

SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling **GCIH**

SEC550 Active Defense, Offensive Countermeasures, and Cyber Deception

NETWORK & EXPLOITS

SEC560 Network Pen Testing and Ethical Hacking **GPEN**

SEC660 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking **GXPN**

SEC760 Advanced Exploit Development for Penetration Testers

WEB

SEC542 Web App Pen Testing and Ethical Hacking **GWAPT**

SEC642 Advanced Web App Pen Testing and Ethical Hacking

MOBILE/WIRELESS

SEC575 Mobile Device Security and Ethical Hacking **GMOB**

SEC617 Wireless Ethical Hacking, Pen Testing, and Defenses **GAWN**

LAB-CENTERED

SEC561 Immersive Hands-On Hacking Techniques

SEC562 CyberCity Hands-on Kinetic Cyber Range Exercise

SPECIALIZATION

SEC567 Social Engineering for Penetration Testers

SEC573 Python for Penetration Testers **GPYC**

SEC580 Metasploit Kung Fu for Enterprise Pen Testing

Network Operations Center, System Admin, Security Architecture

SEC401 Security Essentials Bootcamp Style **GSEC**

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 **GCCC**

SEC579 Virtualization and Private Cloud Security

Security Operations Center/Intrusion Detection

SEC401 Security Essentials Bootcamp Style **GSEC**

SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling **GCIH**

ENDPOINT MONITORING

SEC501 Advanced Security Essentials – Enterprise Defender **GCED**

FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting **GCFA**

THREAT INTELLIGENCE

FOR578 Cyber Threat Intelligence

NETWORK MONITORING

SEC503 Intrusion Detection In-Depth **GCIA**

FOR572 Advanced Network Forensics and Analysis **GNFA**

SEC511 Continuous Monitoring and Security Operations **GMON**

SEC550 Active Defense, Offensive Countermeasures, and Cyber Deception

Industrial Control Systems

ICS410 ICS/SCADA Security Essentials **GICSP**

ICS456 Essentials for NERC Critical Infrastructure Protection

ICS515 ICS Active Defense and Incident Response

FORENSICS CURRICULUM

Incident Response and Threat Hunting

SEC401 Security Essentials Bootcamp Style **GSEC**

SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling **GCIH**

NETWORK ANALYSIS

SEC503 Intrusion Detection In-Depth **GCIA**

FOR572 Advanced Network Forensics and Analysis **GNFA**

ENDPOINT ANALYSIS

FOR408 Windows Forensic Analysis **GCFE**

FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting **GCFA**

MALWARE ANALYSIS

FOR610 Reverse Engineering Malware: Malware Analysis Tools and Techniques **GREM**

FOR578 Cyber Threat Intelligence

SPECIALIZATION

FOR526 Memory Forensics In-Depth

MGT535 Incident Response Team Management

Digital Forensic Investigations

FOR408 Windows Forensic Analysis **GCFE**

SEC504 Hacker Tools, Techniques, Exploits, and Incident Handling **GCIH**

FOR508 Advanced Digital Forensics, Incident Response, and Threat Hunting **GCFA**

FOR585 Advanced Smartphone Forensics **GASF**

FOR518 Mac Forensic Analysis

FOR526 Memory Forensics In-Depth

FOR610 Reverse Engineering Malware: Malware Analysis Tools and Techniques **GREM**

MANAGEMENT CURRICULUM

FOUNDATIONAL

MGT512 SANS Security Leadership Essentials for Managers with Knowledge Compression™ **GSLC**

MGT525 IT Project Management, Effective Communication & PMP® Exam Prep **GCPM**

MGT414 SANS Training Program for CISSP® Certification **GISP**

CORE

MGT514 IT Security Strategic Planning, Policy, and Leadership

LEG523 Law of Data Security and Investigations **GLEG**

MGT535 Incident Response Team Management

SPECIALIZATION

AUD507 Auditing & Monitoring Networks, Perimeters, and Systems **GSNA**

SEC566 Implementing and Auditing the Critical Security Controls – In-Depth **GCCC**

MGT433 Securing The Human: How to Build, Maintain and Measure a High-Impact Awareness Program

PMP is registered mark of the Project Management Institute, Inc.

DEVELOPER CURRICULUM

CORE

Securing The Human for Developers Application Security Awareness Modules

DEV522 Defending Web Applications Security Essentials **GWEB**

DEV531 Defending Mobile Applications Security Essentials

DEV534 Secure DevOps: A Practical Introduction

SECURE CODING

DEV541 Secure Coding in Java/JEE **GSSP-JAVA**

DEV543 Secure Coding in C/C++

DEV544 Secure Coding in .NET **GSSP-.NET**

SPECIALIZATION

SEC542 Web App Pen Testing and Ethical Hacking **GWAPT**

SEC642 Advanced Web App Pen Testing and Ethical Hacking

For information on all of SANS' courses, visit www.sans.org/courses

GIAC

GIAC certification available for courses indicated with GIAC acronyms