TRAINING SERVICES

context

ABOUT CONTEXT

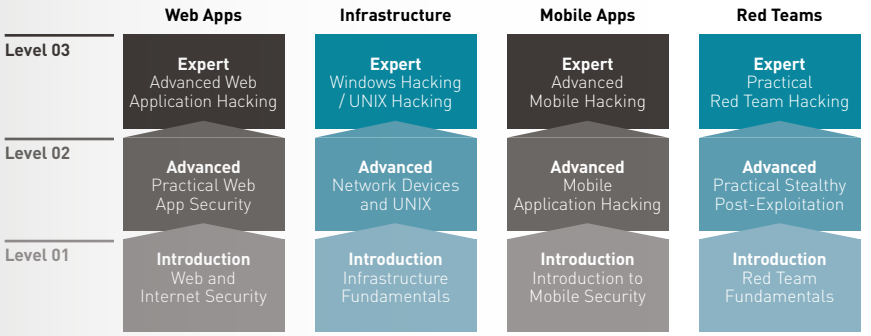
Context is a highly-skilled cyber security consultancy that supports organisations to meet their ever evolving information security challenges. We provide specialist technical consultancy services that include penetration testing, incident response and investigations, and technical security research.

TRAINING COURSES FROM CONTEXT

Effective training programmes provide an organisation and its employees with the knowledge and skills to defend against the ever evolving threats that businesses face today.

Our training programmes are developed from our specialist knowledge and experience in the industry of delivering cutting edge assurance services. Our courses have been designed specifically for IT professionals, managers and CISOs who require a deeper understanding of particular areas of IT security. The courses offered have been developed by Context's experienced tutor consultants to provide a broad selection for organisations to choose from. All courses within a specific topic are connected (see diagram below). Attending one course often naturally leads into the more advanced follow ups but courses are designed to also stand-alone.

If you would like further information or to book one of our training courses, please email info@contextis.co.uk or call +44 (0)20 7537 7515.



WEB APPLICATION HACKING

Almost every organisation now relies on an Internet presence to either present the public face of the company, to provide the core of the business itself or through offering internet services for utilisation by others. As these windows are opened to the outside world, they also serve as a potential risk, broadening the threat landscape of the organisation and presenting would-be attackers with an avenue for compromising the organisation's sensitive data and services.

Our experience in teaching this course has taught us that, in order to properly guard against the ever increasing pool of weaknesses, the defenders must learn to think like their opponents. The course is therefore structured around practical knowledge regarding web application security vulnerabilities, following a step-by-step model; finding the vulnerability, exploiting the vulnerability, understanding the underlying cause and creating a remedy.

Who should attend: Penetration Testers, Web App Developers, Development Leads

Web and Internet Security
Difficulty: Introduction
1 Day

Attendee Level: This is an introductory course and requires no prior experience in this topic.

This course will demonstrate how hackers think when attacking a site and show the common tools of their trade. At the conclusion of the training course attendees will know how to carry out web-app reconnaissance and information gathering and be familiar with well-known attacks.

Topics include:
- Introduction to modern Web Application Security
- Reconnaissance and information gathering
- Intelligent spidering and discovery
- The tools of the trade
- Burp tool in detail
- HTTPS and Transmission Security
- Thinking like an attacker
- Common weaknesses and exploits
- Optional end of the day Capture the Flag

E info@contextis.com
T +44 (0)20 7537 7515

These courses combined align to the syllabus of the CREST Certified Web Application Tester (CCT APP) exam.

Practical Web App Security
Difficulty: Advanced
1–2 Days

Attendee Level: We would recommend this course for those with at least 1–3 years' experience in Web Application development or security.

This course will teach a practical approach to Web Application Security by demonstrating the more advanced techniques used by attackers to steal information from users and databases. At the end of the course the attendees will know and understand practical web app hacking techniques and how to defend against them.

Topics include:
- Practical attacks
- Heartbleed and Shellshock
- Brute-force enumerating users and directories
- Advanced burp tool techniques
- Automated web app scanners
- Cross site scripting (XSS)
- Logic flaws and bypasses
- File upload vulnerabilities
- SQL injections and database attacks
- End of course Capture the Flag

Advanced Web Application Hacking
Difficulty: Expert
2 Days

Attendee Level: We would recommend this course for those with at least 3 years' experience in Web-Application development or security.

This course will teach advanced web app hacking techniques, covering the tools, methods and scripts to bypass defences and acquire a sustained presence. At the end of the course attendees will know how to find, exploit and protect against these advanced attacks.

Topics include:
- Advanced XSS and stealing from other users
- Advanced SQL injection attacks
- Attacks against modern web frameworks
- Gaining a persistent presence
- Command injection and execution
- Web service attacks
- Full attack walkthroughs
- End of course Capture the Flag

This course uses Context's custom created web applications and services, specifically created to emulate real-world applications and provide a realistic and up-to-date look at the attack surface and vectors available to skilled attackers.

MOBILE HACKING AND SECURITY TESTING

With organisations expanding their presence onto mobile devices, enabling their employees and customers to access business information wherever they are, the threat landscape has never been wider.

Mobile systems offer a whole new set of challenges for security professionals, incident responders and developers to take into account. This includes sensitive data on lost devices, applications leaking access to user accounts, and data exfiltration from corporate devices to name but a few.

This training course is designed to provide attendees with hands-on knowledge on how attackers penetrate the security around mobile applications and security policies. To achieve this it uses custom mobile applications created by Context, crafted to emulate real-world applications and provide a realistic and up-to-date look at the attack surface and vectors available to skilled attackers.

Who should attend: Mobile Developers, Development Managers, Penetration Testers

Introduction to Mobile Security
Difficulty: Introduction
1 Day

Attendee Level: This is an introductory course and requires no prior experience in this topic.

This course will teach attendees the security principles of mobile devices, the vectors attackers take to exploit them and what defensive measures are in place. It covers the current threat landscape, the ongoing changes in security architectures and documents the tools attackers use when hacking mobile applications. At the end of this course attendees will have gained knowledge to help ensure the strong security posture of their own and corporate devices.

Topics include:
- The state of mobile devices
- Mobile Security basics
- Understanding the mobile attack vectors
- Mobile Security architectures
- Jailbreaking and rooting
- iOS specific considerations
- The SWIFT language
- Android specific considerations
- Java, Kotlin and SMALI
- Malware in the wild
- The attackers toolkit
- Certificate Pinning Techniques

Mobile Application Hacking
Difficulty: Advanced
1–2 Days

Attendee Level: We would recommend this course for mobile developers and testers with at least 2 years' experience.

This course will teach attendees how to create a mobile penetration testing environment for iOS and Android, how to acquire and configure the tools needed and how to carry out the initial testing of the applications. Techniques covered include analysing local storage, intercepting and manipulating traffic from the apps and how to deal with and understand middleware layer solutions. At the end of this course attendees will be able to perform a basic security audit of mobile applications.

Topics include:
- Setting up the mobile hacking environment
- Connecting to the Android device
- ADB connections
- Understanding application storage
- Analysing local files and getting access
- Intercepting network traffic
- Web component vulnerabilities
- Middleware layers and weaknesses
- Basic FRIDA injection
- End of course Capture the Flag

Advanced Mobile Hacking
Difficulty: Expert
1–2 Days

Attendee Level: We would recommend this course for mobile security testers and senior developers with at least 3–4 years' experience.

This course will teach attendees how to use advanced attack methods against mobile applications, how to reverse-engineer their code to look for vulnerabilities and use this information for complex attacks. At the end of this course attendees will be able to use advanced mobile penetration testing tools, carry out injection attacks and use reverse engineering methods to deconstruct the advanced defences of modern mobile applications.

Topics include:
- Automating attacks
- Application Logic and bypasses
- Reverse Engineering applications
- Decompiling Android applications
- SMALI and patching
- Decompiling iOS
- Hunting for weaknesses within the decompiled code
- Cryptographic weaknesses
- Manipulating Applications with Injections
- Advanced Runtime Injections
- End of Course Capture the Flag

RED TEAM / SIMULATED TARGETED ATTACK

Building on Context's experience in running large-scale red team and CBEST engagements, this training course aims to teach the methods and approaches taken by real-world attackers when compromising an entire organisation. From initial recognition and phishing, to post-exploitation and acquiring access to every system in an organisation, this course is as close to a real-world hacking attack as it gets.

The knowledge gained can permit network architects, incident response managers and senior security personnel to take their defensive strategies to the next level by understanding the methodologies and mindset of the attackers.

Who should attend: Senior Security Personnel, Senior Penetration Testers, CISOs, Security Incident Responders

Red Teams Fundamentals

Difficulty: Introduction
1 Day

Attendee Level: We would recommend this course for senior security personnel and company decision makers looking to understand the impact of red teams / real attacks.

This course teaches the fundamentals of red team testing; how they operate to achieve the real-world experience of a genuine cyber-attack, the open-source research sources, the social engineering, the attacks and the targets within. At the end of this course attendees will understand how red teams operate, the benefits of them to organisations and how the lessons learned can be applied to defensive strategies.

Topics include:
- Red teams explained
- The security landscape
- The Kill Chain
- Attackers and agendas
- Threat intelligence
- Open source intelligence sources
- Social engineering
- Planting malware
- Evasion and exfiltration
- Prime targets

Practical Stealthy Post-Exploitation

Difficulty: Advanced / Expert
2–3 Days

Attendee Level: We would recommend this course for experienced testers with at least 3 years' experience in Windows security.

This course aims to detail how attackers create custom code to bypass security controls to abuse native windows processes, inject shell-code and create stagers for additional malware downloads, through practical examples and coding workshops. At the end of the course attendees will be able to create custom executables to evade anti-virus and other security technologies and bypass Windows security features such as AppLocker, SRP and Firewalls using custom created executables.

Topics include:
- Introduction to native Windows defenses
- Writing and compiling code with Visual Studio and GCC
- Bypassing Windows security controls
- Injecting into running processes
- Avoiding anti-virus with custom code
- Bypassing Firewalls with multi-staged exploits
- Combining techniques for full exploitation

Red Team Tactics

Difficulty: Advanced / Expert
3–4 Days

Attendee Level: We would recommend this course for experienced security practitioners, defensive or offensive, with at least 4 years' experience.

This course will teach attendees how to carry out a red team from start to finish; setting up the attack environment, carrying out intelligence gathering, creating and running phishing campaigns, deploying implants, doing internal network reconnaissance, finding sensitive files and escalating access all the way to Domain Administrator. At the end of this course the attendees will be able to carry out a complete red team test.

Topics include:
- Red teams explained
- Organisation research and target analysis
- OSINT
- Phishing for access
- Command and control
- Deploying malicious implants
- Network reconnaissance
- Staying hidden
- Hunting for sensitive files and data
- Windows command-line techniques
- Powershell and scripts
- Pivoting and escalating
- Stealing accounts and access
- Becoming the Domain Admin

E info@contextis.com
T +44 (0)20 7537 7515

HACKING NETWORK INFRASTRUCTURE

For most organisations, the internal and externally facing Linux and Windows servers form the backbone of their ability to operate. Running everything from domains and databases, to legacy applications and source-code repositories, network requirements are getting evermore complex.

This course details the steps attackers take in compromising a server; from discovery to full control, the reconnaissance, access and escalation techniques used in real-world attacks are demonstrated and analysed throughout.

Who should attend: Domain Administrators, Network Architects, Penetration Testers, Server / Network Administrators

Infrastructure Fundamentals
Difficulty Level: Introduction
2 Days

Attendee Level: This is an introductory course and requires no prior experience in this topic.

This course will teach the fundamentals of network security, including scanning hosts, enumerating attack surfaces to find vulnerabilities and exploiting weaknesses to gain access to the system. At the end of this course attendees will be able to use industry standard tools to perform reconnaissance and exploitation of Linux and Windows systems.

Topics include:
- Network security fundamentals
- Scanning techniques
- TCP vs UDP
- Tools of the trade
- Nmap and Nessus introductions
- Advanced Nmap scripts and tricks
- Understanding packets
- Planning the attack
- Thinking like an attacker
- Enumerating the attack surface
- Finding local vulnerabilities
- Using exploits
- Cracking passwords
- End of day Capture the Flag

E info@contextis.com
T +44 (0)20 7537 7515

These courses combined align to the syllabus of the CREST Certified Infrastructure Tester (CCT INF) exam.

Network Devices
Difficulty: Advanced
1 Day

Attendee Level: We would recommend this course for anyone with at least 1 years' experience of networks and UNIX systems.

This course will teach attendees how to understand and exploit the lower layer traffic flowing from the routers and switches on a network. At the end of the course the attendees will be able to exploit vulnerabilities and evaluate the security of routing devices and the networks they reside on.

Topics include:
- The OSI layers
- SNMP information gathering
- Virtual networks
- Network devices basics
- Attacking a device
- Layer 2 attacks
- Cain, Wireshark and other Tools
- Compromising routers
- Switch configurations and vulnerabilities
- IPv6 Fundamentals
- Using tools with IPv6
- End of course Capture the Flag

Advanced Infrastructure
Difficulty: Advanced / Expert
2 Days

Attendee Level: We recommend this course for those with 3 or more years' experience in UNIX systems.

This course will teach attendees how to carry out an end-to-end attack against UNIX systems, including Solaris and popular flavours of Linux, covering the entire process from initial recon and access, to breakouts and privilege escalation. At the end of the course attendees will be able to use advanced attacks and perform privilege escalation against a variety of Linux systems.

Topics include:
- Scanning and planning attacks
- Remotely attacking Linux systems
- Service information disclosure
- UNIX fundamentals
- Crafting packets
- Solaris systems
- Server configuration application and weaknesses
- Database service attacks
- Shell breakouts
- Privilege escalation basics
- Advanced privilege escalation
- Compiling and running exploits
- End of course Capture the Flag

Windows Breakout
Difficulty: Advanced / Expert
2 Days

Attendee Level: We recommend this course for those with 3 or more years' experience in Windows and Windows Domains.

This course will teach attendees how to hack Windows Domains and break out of locked-down systems. From initial access to a single machine to owning the entire network, this course takes a practical approach to escalating access out of lockdown all the way to system. At the end of this course the attendees will be able to enumerate Windows security controls and bypass or secure them effectively.

Topics include:
- Windows built-in protection
- AppLocker and SRP
- Windows 10 Specifics
- Enumerating defenses
- Understanding and bypassing locked-down powershell
- Breaking out of locked-down Windows Systems
- Modifying custom code for bypasses
- Gather local information
- Owning the system with privilege escalation

All practical systems are custom built by Context for this course. The course is very practical and features many exercises to give hands-on experience in bypassing (or preventing a bypass) of Windows Security controls.

E info@contextis.com
T +44 (0)20 7537 7515

"Context was one of several companies that I used to train development staff in secure coding concepts several years ago. When it came time to train a new group of developers, I immediately sought out Context because of their expertise, lab-based approach toward the training, ability to customize curriculum to meet our requirements, and very positive feedback that I received from attendees."

Mike Badeaux
Vice President – Information Security, American Equity Investment Life Insurance Company®

OTHER INFORMATION

Location:
We can host training at our London office premises. Alternatively, our training Consultants are able to come to your offices on a date and time to suit your schedule.

Prices:
Each course is provided on a per delegate basis. Depending on your requirements we can discuss each course with you to decipher your needs, from which we can then define the cost of the course for your organisation and may offer discounts for large volume purchases.

Bespoke Courses:
If looking for a pre-defined course, please consider the pre-requisites of the particular course you are interested in, if you require something slightly different we are able to offer bespoke courses for your particular needs.

Each delegate is required to have their own laptop for use during the training course. Material to be pre-installed will be provided by Context before the training course commences.

Certification:
At the end of each course you will receive a certificate to confirm that you have completed the course together with the date and an overview of what you learnt.

E info@contextis.com
T +44 (0)20 7537 7515

contextis.com
info@contextis.com
@CTXIS