



2009 Training Brochure





Why choose ANRC to be your training provider?

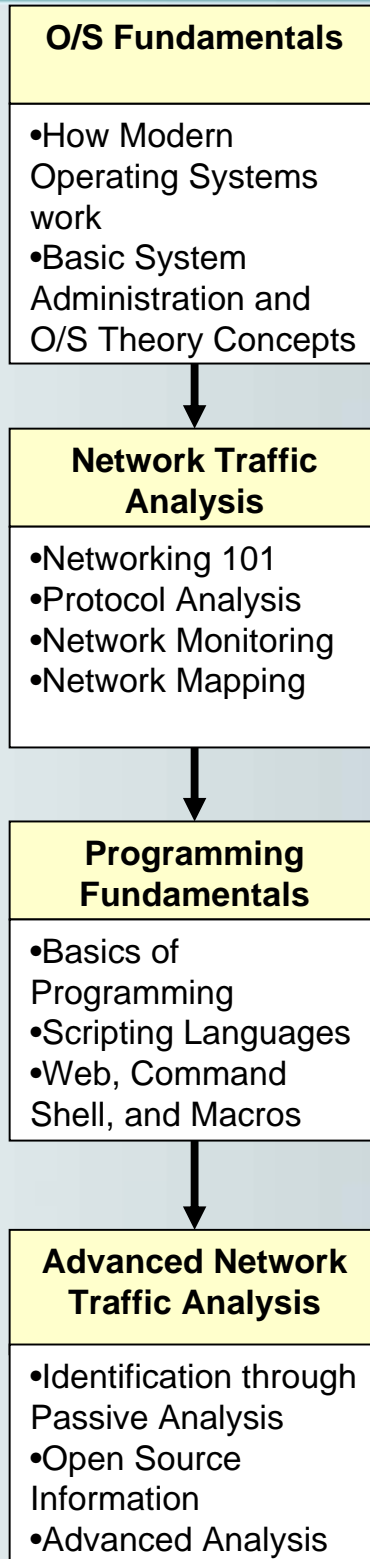
We deliver a complete advanced security training program designed to provide Information Security professionals with the knowledge and skills necessary to defend against today's cyber attacks and tomorrow's emerging threats.

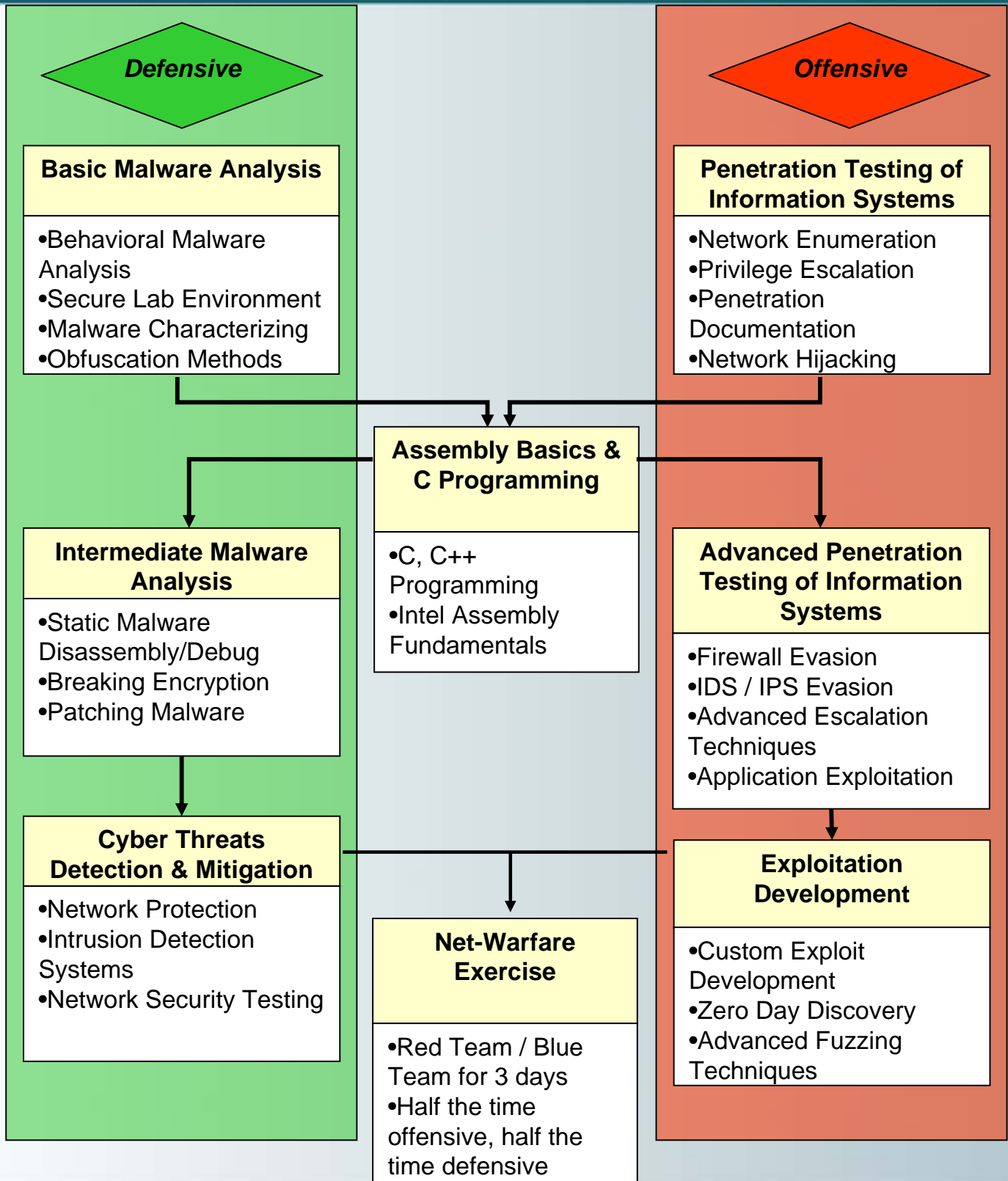
Our instructors are subject matter experts in their respective specializations. Their classroom delivery is derived from “Real Life” computer security field experience. Each instructor utilizes an intensive hands-on laboratory method of training to provide our students with a practical application of classroom presentation.

Our courses are technically reviewed quarterly to ensure the course information is current and up-to-date. The latest trends and advances in computer security are incorporated into our classes as soon as possible.

Our teaching style is very different than anyone else. At ANRC, we provide truly unique training scenarios that dramatically enhances the transfer of knowledge to our students. We believe that teaching a course should be hands-on with as little boring lectures with MS PowerPoint as possible. We also believe that people who do this stuff in the real world make better instructors teaching it, so all our instructors have resumes full of experiences that make them good at what they do. Finally we only teach in small class sizes. Who wants to feel like cattle in a ballroom? Not us!







Operating Systems Fundamentals

Have you ever wondered what's under the hood of a modern operating system? How does it work? How can I make it better? What components are vulnerable to attacks? All of these questions and more can be answered in our O/S Fundamentals class. This class gives you a firm understanding of the latest Operating Systems used worldwide as well as advanced information that will help you immensely in our Malware and Penetration Testing courses. Starting with the Microsoft O/S we teach registry management, memory management, process management, API usage, dynamically linked libraries and much more. All week long we compare and contrast these components to alternative operating systems such as: Solaris, Unix, Linux, and MacOS. After attending this course students will be fully equipped with the fundamentals of Operating System elements and how they are all interconnected.

The O/S Fundamentals class is where it all starts at ANRC because before we can teach students advanced topics like Malware Analysis, and Penetration Testing they have to understand the central key component of the computer, the Operating System. Other institutions have failed where we have succeeded because they miss this integral concept. You can't teach someone how to hack into computer systems if they barely know how the computer system works. The same holds true for Malware Analysis. You can't teach someone how to defend a computer system or network until they fully understand how it works. We teach the fundamentals required first, then introduce the advanced topics later.

Topics for Microsoft Windows, Solaris, Linux, Mac O/S include:

- User and Group Credentials and Security
- File Management, Memory Management, Process Management
- Networking Management
- Command Shell Tools and Techniques
- Processor Fundamentals and Sharing
- Windows API, Windows Registry, and Dynamically Linked Libraries
- Shared Objects

Class Details:

5 Days M-F, laptops are provided, certificate awarded upon completion of the class.

Network Traffic Analysis

Has some hacker gotten access to your network or is it just normal network traffic? How can you tell when there is thousands or hundreds of thousands of packets to look at? Network monitoring is the least understood aspect of network administration and one of the most important. In this course, a networking expert shows you exactly how to monitor and analyze network traffic in order to maximize performance, reduce congestion, and ensure security. Start by learning the specific details of Ethernet, IP, TCP/IP, 802.11 Wireless, NetBIOS, and SMB protocols so you can monitor and analyze traffic effectively. Then using the Wireshark protocol analyzer you'll learn how to filter, identify, and analyze network traffic activity. After leaving this class you'll have a very strong foundation in modern networking protocols and how to understand all of them. For all network users and administrators seeking a better understanding of the networking world and their own networks.

Attending students will learn:

- Networking Protocols
 - Ethernet, IP, TCP/IP, IPX/SPX, NetBIOS, SONET, HDLC, SLIP, SNMP, VOIP, PPP, PPPOE, SMB, Samba and much more
- Traffic analysis tools and techniques
- Wireshark Protocol Analyzer
 - Display Filters
 - Capture Filters
- 802.11 Wireless Technologies
 - Data Frames
 - Management Frames
 - Control Frames
- Network Security Protocols
 - SSH
 - VPN
 - SSL
 - SFTP

Course Details:

5 Days M-F, laptops are provided, certificate awarded upon completion.

Advanced Network Traffic Analysis

After mastering the basics of the Network Traffic Analysis course you're ready to proceed deeper and gain the title of Advanced Network Analyst by completing this course. Here you will go above and beyond normal LAN based operations and broaden you analyst skills into global networking and large WAN based operations. Protocols used by global routers will be discussed in more detail including Frame Relay, BGP, VOIP, VPN, etc. After a brief review of the common networking protocols used in the networking world today we'll move on to more advanced analysis skills like:

- Mapping Network Structures through Passive Analysis
 - Identifying Firewalls
 - Identifying Routers
 - Identifying DNS Servers
 - Identifying Web Servers
 - Identifying DB's
 - Identifying DMZ's
- Using open source tools for information gathering
 - IANA
 - Whois
 - Ping
 - O/S Identification
- Network Taps / Sensor Fundamentals
- Advanced analysis tools and techniques
- Administration and configuration of enterprise networking equipment
- Identification of infrastructure vulnerabilities from the internet
- Penetration Test planning and weak point identification

Prerequisites:

Completion of Network Traffic Analysis course (required)

Course Details:

5 Days M-F, laptops are provided, certificate awarded upon completion of the class.



Computer Programming Fundamentals

The goal of the Computer Programming Fundamentals course is to give you exposure and a general overview to developing code for modern computer systems. This course teaches PERL programming to assist analysts in their day to day jobs where scripting has become almost essential in today's fast paced and large data repository world.

Automation is the key to providing reliable and fast analysis in a large scale environment. By introducing you to a scripting language like PERL we not only prepare you to go farther into code development but also give you the ability to write scripts that will automate monotonous procedures thereby making you more productive in your job. After a overview of program design, control flows, input / output, and variable usage we'll move into more in-depth topics like module usage, IDE's, and debugging techniques. Specific topics include:

- Portable Scripting Languages
 - PERL
 - PERL CGI Web Scripting
 - Basic HTML
- Programming Skills
 - Variable Usage
 - Repetition (loop) Statements
 - Decision Branches
 - File Input and Output
 - Regular Expressions
 - Report Generation
 - Information Extraction
 - System Automation
- Web Based Scripting
 - Graphical Web Interfaces
 - Form Processing
 - Form Validation
 - Web Reporting

Course Details:

5 Days M-F, laptops are provided, certificate awarded upon completion of the course.

C Programming and Assembly Basics

This course covers the basics of understanding C programming and Assembly. Since the upper levels of our offensive and defensive courses involve the use of programming and complex technical topics, this course was designed to be the stepping stone to prepare our students for these high level, technically dense courses. ANRC has determined that students with a programming background as well as assembly knowledge do much better in the upper level expert classes such as our Intermediate Malware Analysis or Advanced Penetration Testing courses.

In the first half of the course we teach the generic rules of writing C programming code. Then in the later half of the week we demonstrate how the C code gets compiled into the Assembly code which ultimately gets processed through the Operating System. Once you have the ability to read both C Programming Language and Assembly code then statically reverse engineering malware is much easier. Likewise being able to write and understand exploitation code in our Advanced Penetration Testing course comes much more naturally after attending this course. Topics covered are:

- C Programming Skills
 - Variable Usage
 - Repetition (loop) Statements
 - Decision Branches
 - File Input and Output
 - Windows API Usage and Standard Libraries
- Assembly Programming Skills
 - Understanding Computational Expressions
 - Identifying Repetition Statements
 - Identifying Decision Statements
 - Jumps and Calls
 - Intel Register and CPU Flags
 - Identifying Function Calls and Procedures
 - Windows API Usage and Standard Libraries

Course Details:

5 Days M-F, laptops are provided, certificate awarded upon completion of the course.

Introduction to Java

Introduction to Java teaches the fundamentals required for developing Object Oriented portable Java applications. Starting out with simple console applications this course gives beginning programmers a nice leg up on how to program in a modern and powerful programming language. During the week the course increases in difficulty adding more and more programming exercises to facilitate rapid absorption of the material. By the end of the week students will be coding advanced graphical user interfaces and web applets with confidence and assurance. Specific topics covered are:

- **Basic Programming Skills**
 - Program Flow
 - Data Structures
 - Repetition Statements
 - Selection Statements
 - File Input and Output
- **Advanced Programming Skills**
 - Creating Custom Methods
 - System Interaction
 - Error Handling
 - Advanced String Manipulation
 - Creating Custom Classes
 - Graphical User Interface Design
 - GUI Development Tools
 - Event Handling
- **Web Application Development**
 - Web applets
 - Form Processing
 - Form Validation
 - Web Reporting

Course Details:

5 Days M-F, laptops are provided, certificate awarded upon completion of the course.



Basic Malware Analysis

Basic Malware Analysis teaches you all the fundamental requirements necessary to analyze malicious software from a behavioral perspective. Using system monitoring tools this course teaches how to observe malware in a controlled environment to quickly analyze its malicious affects to the system. From simple keyloggers to massive botnets this class covers a wide variety of current threats used on the Internet today with actual samples being analyzed in the training environment. With the majority of the class being hands-on each student will be issued a laptop with a secure environment to learn the skills and essential methodology required to be an effective malware analyst.

Attending students will learn:

- How to identify malware and discover it's capabilities
- How to setup a secure lab environment to analyze malicious software
- How to use open source tools to characterize malware samples quickly
- Obfuscation methods used by attackers to escape detection

Course Details:

5 Days M-F, laptops are provided, certificate awarded upon completion of the course. A class CD is also provided to the student with all the tools used and taught during the class.

Intermediate Malware Analysis

Equipped with the behavioral Malware Analysis knowledge from the Basic Malware Analysis course you're ready to adventure into more advanced malware topics by attending the Intermediate Malware Analysis course. During this five day course we'll show you how to do Static Malware Analysis through a debugger. Since looking at assembly code in a debugger can be frustrating and almost impossible without a previous understanding of programming fundamentals and compiler operations we require that the students who attend this course have Assembly language knowledge or have completed our C Programming and Assembly Basics course. During the week of instruction we introduce you to the OllyDbg Debugger. Through controlled evaluation using the debugger we'll teach you how to identify exactly what the malware specimen does and how it's doing it. After you've mastered the evaluation portion of the class we'll teach you how to patch the specimen to make it inactive or crack the program to allow full access to areas that have been hidden or encrypted by the malware developer. Students who attend this class will graduate with the following intermediate malware analysis skills:

- Assembly language debugging fundamentals including:
 - Conversion methodology from source code to assembly code
 - Intel CPU memory management and structures
 - CPU control flows and order of operations
- Olly Debugger including:
 - Tool Features
 - Stepping, Stepping Over and Running code
 - Useful Plug-ins and Add-ons
 - Breakpoint fundamentals and usage
 - Patching and assembling executables
 - Decrypting and decoding packed executables

Prerequisites:

C Programming and Assembly knowledge is required.

Course Details:

5 Days M-F, laptops are provided, certificate awarded upon completion of the course. A class CD is also provided to the student with all the tools used and taught in the course.

Cyber Threats Detection & Mitigation

Cyber threats are increasing at an alarming rate every year and the ability for organizations to defend against full-scaled distributed attacks quickly and effectively is becoming more and more difficult. In order to be safe and secure on today's Internet organizations must learn to become more automated. This means being capable of characterizing attacks across hundreds or even thousands of IP sessions and improving their ability to recognize attack commonalities. With Intrusion Detection Systems and trained network security auditors organizations have a reliable means to prioritize, and isolate only the most critical threats in real time. Taught by leaders in network defense who work in the computer security industry, this course demonstrates how to defend large scale network infrastructure by building and maintaining intrusion detection systems, network security auditing, and incident response techniques.

The student will learn:

- How to identify the best defensive measures to effectively protect a network
- How to setup and maintain an intrusion detection system
- How to analyze and respond to intrusion attempts
- How to recover from a successful intrusion

Course Details:

5 Days M-F, laptops are provided, certificate awarded upon completion of the course. A class CD is also provided to the student with all the tools used and taught during the course.



Penetration Testing

The ability of an organization to proactively test its own defenses is quickly becoming more of a requirement than a luxury. Penetration testing (Pentesting) is a method of evaluating the security of a computer system or network by simulating an attack by a malicious user. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, and known and/or unknown hardware or software flaws. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered.

Attendants of this class will learn:

- How to analyze their organization's network as a potential intruder would
- How to scan and launch attacks against encountered vulnerabilities
- How to gain access and escalate privileges without being detected
- How to recover from a successful intrusion
- How to use ANRC's Linux Security Auditor Distro to audit their networks

Course Details:

5 Days M-F, laptops are provided, certificate awarded upon completion of the course. A class CD is also provided to the student with all the tools used and taught during the course.

Advanced Penetration Testing

To become an elite Penetration Tester you must broaden the exposure you received from the Penetration Testing course. Advanced Penetration Testing builds on your knowledge and expands on the basics you've already learned by introducing advanced techniques and current exploits recently uncovered. We'll teach you advanced hacking techniques used by the bad guys so that you can use them ethically against your systems to ensure you know what they know. Custom attacks, advanced penetration tools, perimeter defense evasion and cyber warfare techniques are just some of the advanced topics you'll receive from this course.

Physical security is also taught in this course to cover all the arenas involved in doing a full Penetration Test of an organization. In the advanced course we teach the student physical topics such as lock picking, information gathering, and social engineering. Each student receives their own lock picks and will practice lock picking our locked practice door. This example demonstrates how easily physical security can be breached and what makes a good and secure lock. After the social engineering lesson our students also place a call to our fake helpdesk to see if they can get access by using social engineering, afterward we grade their performance with the other classmates.

Technical Topics include:

- DNS Poisoning
- Cross Site Scripting
- Malicious Email Generation
- IDS/IPS Evasion
- ARP Poisoning
- Wireless Access Point Hijacking
- Exploit Generation

Prerequisites:

Penetration Testing, C Programming and Assembly Basics (or programming skills)

Course Details:

5 Days M-F, laptops are provided, certificate awarded upon course completion.



Security+ / CISSP Certification Two In One



Why pay for 2 separate classes (and miss two weeks of work attending them) to prepare for your Security+ and CISSP certifications? You could simply take one comprehensive course from us. It's true. We teach you all domains of both certifications and provide you with the best books, test review questions, and preparation materials available on the market today – all geared to ensure you can pass these certification exams after attending a single 5-day course from ANRC. How can we do it? It's actually simple!

We took a hard look at the domains of each certification and found a large amount of overlap between them. In fact, there is so much overlapping information that when you study for one of these certifications, you are really studying for both. This allows us to consolidate the two courses into a single, comprehensive 5-day course that is still entirely effective in preparing for either of these certifications. One exam or both exams, you choose your path.

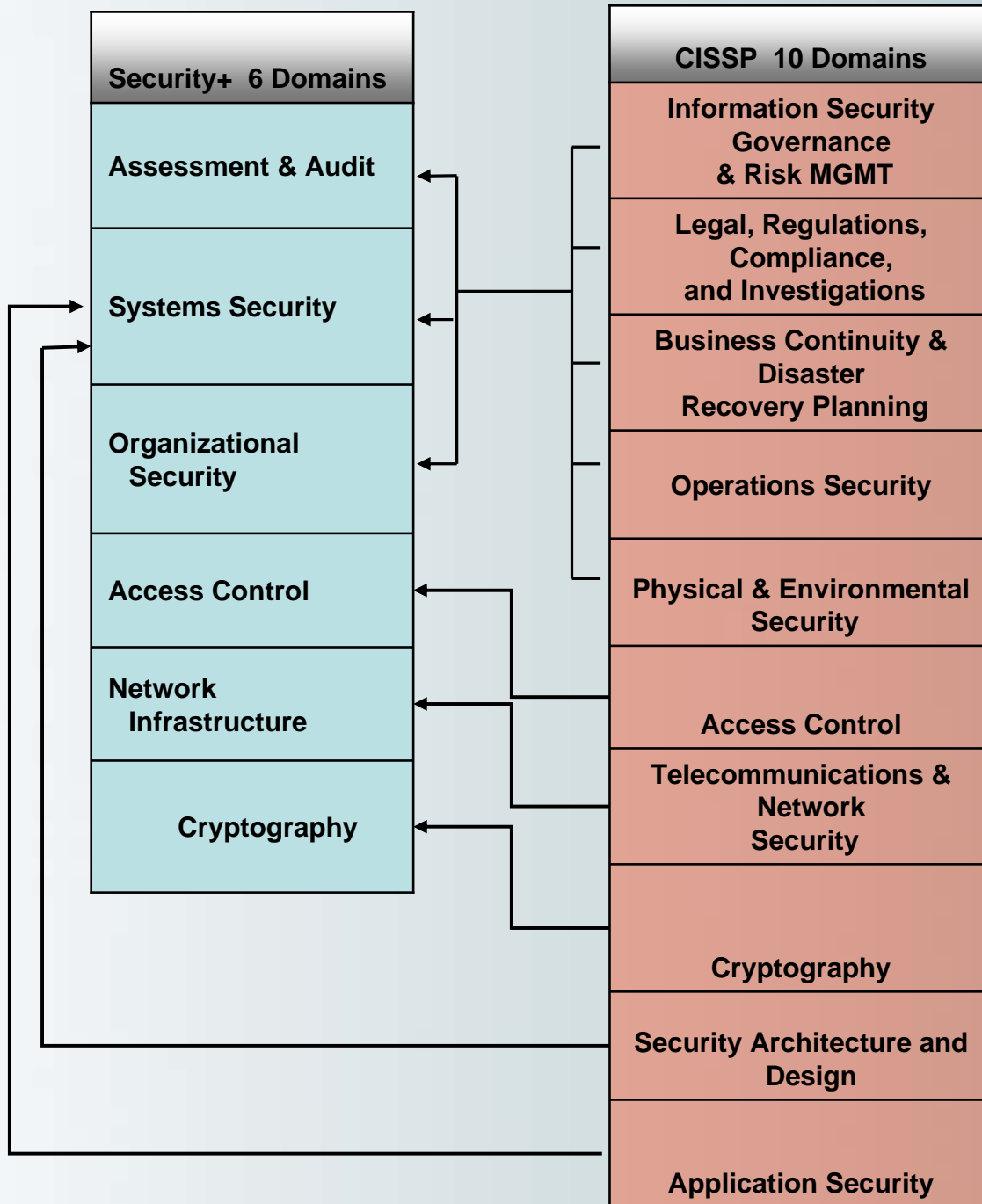
When you couple the experience of our certified instructors, the large amount of test review questions, and test prep material we provide, you'll see why we're confident our students will be fully prepared for one or both of the exams at whatever point they choose to get certified.

Each student will receive:

- Hard copies of all the slides (slides are cross-referenced to specific page numbers in the supplemental materials below)
- The CISSP All-In-One 4th edition by Shon Harris
- The Security+ All-In-One 2nd edition by Greg White & WM. Arthur Conklin
- An ANRC developed CD with additional practice questions, review videos, and other invaluable preparation information.
- A voucher for the Security+ test (a \$258 value)

See the next page for an illustration of how we've mapped the courses together!





Sample timeline for a student from the Security+ / CISSP Two-In-One Course

Begin timeline	→	2 to 3 weeks	→	6 to 8 weeks
End of the class		Security+ Certified!		CISSP Certified!





Custom Course Development

Don't see a class in our brochure that you would like to see? Don't worry because we do custom course development as well! Our customers enjoy our hands-on approach so much that some of them have asked us to build a course just for them to meet their specific needs with our proven learning style blended in. The results have been spectacular! In fact our latest custom development course for the U.S. Navy was so successful they've asked us to do more classes for them. Let us design and develop a custom course for you today.



Contact us for pricing information

ANRC Corporate Office

Exchange Parkway Plaza

5309 Wurzbach Rd.

Suite 101

San Antonio, Texas 78238

Phone: 1-800-742-7931 (toll free)

Fax: 1-866-611-7047 (toll free)

Email: training@anrc-services.com

Web: <http://www.anrc-services.com>

Our classroom courses are completely mobile so on-site training is available in almost any location. Please call for more information and pricing.

Proudly serving those who serve us in the U.S Military as well as Federal Agencies that are dedicated in the same fight to making America Safe and Secure.

Computer security shouldn't be an afterthought...

