onlurking / awesome-infosec

A curated list of awesome infosec courses and training resources.

infosec pentest courses penetration-testing security-professionals lab awesome security

32 commits 2 branches 0 releases 6 contributors

Branch: master New pull request Find file Clone or download

onlurking committed on Jan 16 Merge pull request #11 from PolluxAvenger/master … Latest commit `1b84f0b` on Jan 16

contributing.md	Huge Content Update	3 years ago

readme.md	Add awesome-yara to related lists	7 months ago
readme_cn.md	add Chinese Translation	4 months ago

readme.md

Awesome Infosec

A curated list of awesome information security resources, inspired by the awesome-* trend on GitHub.

Those resources and tools are intended only for cybersecurity professional and educational use in a controlled environment.

Table of Contents

Massive Online Open Courses

Stanford University - Computer Security

In this class you will learn how to design secure systems and write secure code. You will learn how to find vulnerabilities in code and how to design software systems that limit the impact of security vulnerabilities. We will focus on principles for building secure systems and give many real world examples.

- Stanford University - Computer Security

Stanford University - Cryptography I

This course explains the inner workings of cryptographic primitives and how to correctly use them. Students will learn how to reason about the security of cryptographic constructions and how to apply this knowledge to real-world applications. The course begins with a detailed discussion of how two parties who have a shared secret key can communicate securely when a powerful adversary eavesdrops and tampers with traffic. We will examine many deployed protocols and analyze mistakes in existing systems. The second half of the course discusses public-key techniques that let two or more parties generate a shared secret key. We will cover the relevant number theory and discuss public-key encryption and basic key-exchange. Throughout the course students will be exposed to many exciting open problems in the field.

- Stanford University - Cryptography I

Stanford University - Cryptography II

This course is a continuation of Crypto I and explains the inner workings of public-key systems and cryptographic protocols. Students will learn how to reason about the security of cryptographic constructions and how to apply this knowledge to real-world applications. The course begins with constructions for digital signatures and their applications. We will then discuss protocols for user authentication and zero-knowledge protocols. Next we will turn to privacy applications of cryptography supporting anonymous credentials and private database lookup. We will conclude with more advanced topics including multi-party computation and elliptic curve cryptography.

- Stanford University - Cryptography II

University of Maryland - Usable Security

This course focuses on how to design and build secure systems with a human-centric focus. We will look at basic principles of human-computer interaction, and apply these insights to the design of secure systems with the goal of developing security measures that respect human performance and their goals within a system.

- University of Maryland - Usable Security

University of Maryland - Software Security

This course we will explore the foundations of software security. We will consider important software vulnerabilities and attacks that exploit them -- such as buffer overflows, SQL injection, and session hijacking -- and we will consider defenses that prevent or mitigate these attacks, including advanced testing and program analysis techniques. Importantly, we take a "build security in" mentality, considering techniques at each phase of the development cycle that can be used to strengthen the security of software systems.

- University of Maryland - Software Security

University of Maryland - Cryptography

This course will introduce you to the foundations of modern cryptography, with an eye toward practical applications. We will learn the importance of carefully defining security; of relying on a set of well-studied "hardness assumptions" (e.g., the hardness of factoring large numbers); and of the possibility of proving security of complicated constructions based on low-level primitives. We will not only cover these ideas in theory, but will also explore their real-world impact. You will learn about cryptographic primitives in wide use today, and see how these can be combined to develop modern protocols for secure communication.

- University of Maryland - Cryptography

University of Maryland - Hardware Security

This course will introduce you to the foundations of modern cryptography, with an eye toward practical applications. We will learn the importance of carefully defining security; of relying on a set of well-studied “hardness assumptions” (e.g., the hardness of factoring large numbers); and of the possibility of proving security of complicated constructions based on low-level primitives. We will not only cover these ideas in theory, but will also explore their real-world impact. You will learn about cryptographic primitives in wide use today, and see how these can be combined to develop modern protocols for secure communication.

- University of Maryland - Hardware Security

Academic Courses

NYU Tandon School of Engineering - OSIRIS Lab's Hack Night

Developed from the materials of NYU Tandon's old Penetration Testing and Vulnerability Analysis course, Hack Night is a sobering introduction to offensive security. A lot of complex technical content is covered very quickly as students are introduced to a wide variety of complex and immersive topics over thirteen weeks.

- NYU Tandon's OSIRIS Lab's Hack Night

Florida State University's - Offensive Computer Security

The primary incentive for an attacker to exploit a vulnerability, or series of vulnerabilities is to achieve a return on an investment (his/her time usually). This return need not be strictly monetary, an attacker may be interested in obtaining access to data, identities, or some other commodity that is valuable to them. The field of penetration testing involves authorized auditing and exploitation of systems to assess actual system security in order to protect against attackers. This requires thorough knowledge of vulnerabilities and how to exploit them. Thus, this course provides an introductory but comprehensive coverage of the fundamental methodologies, skills, legal issues, and tools used in white hat penetration testing and secure system administration.

- Offensive Computer Security - Spring 2014
- Offensive Computer Security - Spring 2013

Florida State University's - Offensive Network Security

This class allows students to look deep into know protocols (i.e. IP, TCP, UDP) to see how an attacker can utilize these protocols to their advantage and how to spot issues in a network via captured network traffic. The first half of this course focuses on know protocols while the second half of the class focuses on reverse engineering unknown protocols. This class will utilize captured traffic to allow students to reverse the protocol by using known techniques such as incorporating bioinformatics introduced by Marshall Beddoe. This class will also cover fuzzing protocols to see if the server or client have vulnerabilities. Overall, a student finishing this class will have a better understanding of the network layers, protocols, and network communication and their interaction in computer networks.

- Offensive Network Security

Rensselaer Polytechnic Institute - Malware Analysis

This course will introduce students to modern malware analysis techniques through readings and hands-on interactive analysis of real-world samples. After taking this course students will be equipped with the skills to analyze advanced contemporary malware using both static and dynamic analysis.

- CSCI 4976 - Fall '15 Malware Analysis

Rensselaer Polytechnic Institute - Modern Binary Exploitation

This course will start off by covering basic x86 reverse engineering, vulnerability analysis, and classical forms of Linux-based userland binary exploitation. It will then transition into protections found on modern systems (Canaries, DEP, ASLR, RELRO, Fortify Source, etc) and the techniques used to defeat them. Time permitting, the course will also cover other subjects in exploitation including kernel-land and Windows based exploitation.

- CSCI 4968 - Spring '15 Modern Binary Exploitation

Rensselaer Polytechnic Institute - Hardware Reverse Engineering

Reverse engineering techniques for semiconductor devices and their applications to competitive analysis, IP litigation, security testing, supply chain verification, and failure analysis. IC packaging technologies and sample preparation techniques for die recovery and live analysis. Deprocessing and staining methods for revealing features bellow top passivation. Memory technologies and appropriate extraction techniques for each. Study contemporary anti-tamper/anti-RE methods and their effectiveness at protecting designs from attackers. Programmable logic microarchitecture and the issues involved with reverse engineering programmable logic.

- CSCI 4974/6974 - Spring '14 Hardware Reverse Engineering

City College of San Francisco - Sam Bowne Class

- CNIT 40: DNS Security
  DNS is crucial for all Internet transactions, but it is subject to numerous security risks, including phishing, hijacking, packet amplification, spoofing, snooping, poisoning, and more. Learn how to configure secure DNS servers, and to detect malicious activity with DNS monitoring. We will also cover DNSSEC principles and deployment. Students will perform hands-on projects deploying secure DNS servers on both Windows and Linux platforms.

- CNIT 120 - Network Security
  Knowledge and skills required for Network Administrators and Information Technology professionals to be aware of

security vulnerabilities, to implement security measures, to analyze an existing network environment in consideration of known security threats or risks, to defend against attacks or viruses, and to ensure data privacy and integrity. Terminology and procedures for implementation and configuration of security, including access control, authorization, encryption, packet filters, firewalls, and Virtual Private Networks (VPNs).

- CNIT 121 - Computer Forensics
  The class covers forensics tools, methods, and procedures used for investigation of computers, techniques of data recovery and evidence collection, protection of evidence, expert witness skills, and computer crime investigation techniques. Includes analysis of various file systems and specialized diagnostic software used to retrieve data. Prepares for part of the industry standard certification exam, Security+, and also maps to the Computer Investigation Specialists exam.

- CNIT 123 - Ethical Hacking and Network Defense
  Students learn how hackers attack computers and networks, and how to protect systems from such attacks, using both Windows and Linux systems. Students will learn legal restrictions and ethical guidelines, and will be required to obey them. Students will perform many hands-on labs, both attacking and defending, using port scans, footprinting, exploiting Windows and Linux vulnerabilities, buffer overflow exploits, SQL injection, privilege escalation, Trojans, and backdoors.

- CNIT 124 - Advanced Ethical Hacking
  Advanced techniques of defeating computer security, and countermeasures to protect Windows and Unix/Linux systems. Hands-on labs include Google hacking, automated footprinting, sophisticated ping and port scans, privilege escalation, attacks against telephone and Voice over Internet Protocol (VoIP) systems, routers, firewalls, wireless devices, Web servers, and Denial of Service attacks.

- CNIT 126 - Practical Malware Analysis
  Learn how to analyze malware, including computer viruses, trojans, and rootkits, using disassemblers, debuggers, static and dynamic analysis, using IDA Pro, OllyDbg and other tools.

- CNIT 127 - Exploit Development
  Learn how to find vulnerabilities and exploit them to gain control of target systems, including Linux, Windows, Mac, and Cisco. This class covers how to write tools, not just how to use them; essential skills for advanced penetration testers and software security professionals.

- CNIT 128 - Hacking Mobile Devices
  Mobile devices such as smartphones and tablets are now used for making purchases, emails, social networking, and many other risky activities. These devices run specialized operating systems have many security problems. This class will cover how mobile operating systems and apps work, how to find and exploit vulnerabilities in them, and how to defend them. Topics will include phone call, voicemail, and SMS intrusion, jailbreaking, rooting, NFC attacks, malware, browser exploitation, and application vulnerabilities. Hands-on projects will include as many of these activities as are practical and legal.

- CNIT 129S: Securing Web Applications
  Techniques used by attackers to breach Web applications, and how to protect them. How to secure authentication, access, databases, and back-end components. How to protect users from each other. How to find common vulnerabilities in compiled code and source code.

- CNIT 140: IT Security Practices
  Training students for cybersecurity competitions, including CTF events and the Collegiate Cyberdefense Competition (CCDC). This training will prepare students for employment as security professionals, and if our team does well in the competitions, the competitors will gain recognition and respect which should lead to more and better job offers.

- Violent Python and Exploit Development
  In the exploit development section, students will take over vulnerable systems with simple Python scripts.

Open Security Training

OpenSecurityTraining.info is dedicated to sharing training material for computer security classes, on any topic, that are at least one day long.

Beginner Classes

- Android Forensics & Security Testing
  This class serves as a foundation for mobile digital forensics, forensics of Android operating systems, and penetration testing of Android applications.

- Certified Information Systems Security Professional (CISSP)®
  Common Body of Knowledge (CBK)® Review
  The CISSP CBK Review course is uniquely designed for federal agency information assurance (IA) professionals in meeting NSTISSI-4011, National Training Standard for Information Systems Security Professionals, as required by DoD 8570.01-M, Information Assurance Workforce Improvement Program.

- Flow Analysis & Network Hunting
  This course focuses on network analysis and hunting of malicious activity from a security operations center perspective. We will dive into the netflow strengths, operational limitations of netflow, recommended sensor placement, netflow tools, visualization of network data, analytic trade craft for network situational awareness and networking hunting scenarios.

- Hacking Techniques and Intrusion Detection
  The course is designed to help students gain a detailed insight into the practical and theoretical aspects of advanced topics in hacking techniques and intrusion detection.

- Introductory Intel x86: Architecture, Assembly, Applications, & Alliteration
  This class serves as a foundation for the follow on Intermediate level x86 class. It teaches the basic concepts and describes the hardware that assembly code deals with. It also goes over many of the most common assembly instructions. Although x86 has hundreds of special purpose instructions, students will be shown it is possible to read most programs by knowing only around 20-30 instructions and their variations.

- Introductory Intel x86-64: Architecture, Assembly, Applications, & Alliteration
  This class serves as a foundation for the follow on Intermediate level x86 class. It teaches the basic concepts and describes the hardware that assembly code deals with. It also goes over many of the most common assembly instructions. Although x86 has hundreds of special purpose instructions, students will be shown it is possible to read most programs by knowing only around 20-30 instructions and their variations.

- Introduction to ARM
  This class builds on the Intro to x86 class and tries to provide parallels and differences between the two processor architectures wherever possible while focusing on the ARM instruction set, some of the ARM processor features, and how software works and runs on the ARM processor.

- Introduction to Cellular Security
  This course is intended to demonstrate the core concepts of cellular network security. Although the course discusses GSM, UMTS, and LTE - it is heavily focused on LTE. The course first introduces important cellular concepts and then follows the evolution of GSM to LTE.

- Introduction to Network Forensics
  This is a mainly lecture based class giving an introduction to common network monitoring and forensic techniques.

- Introduction to Secure Coding
  This course provides a look at some of the most prevalent security related coding mistakes made in industry today. Each type of issue is explained in depth including how a malicious user may attack the code, and strategies for avoiding the issues are then reviewed.

- Introduction to Vulnerability Assessment
  This is a lecture and lab based class giving an introduction to vulnerability assessment of some common common computing technologies. Instructor-led lab exercises are used to demonstrate specific tools and technologies.

- Introduction to Trusted Computing
  This course is an introduction to the fundamental technologies behind Trusted Computing. You will learn what Trusted

Platform Modules (TPMs) are and what capabilities they can provide both at an in-depth technical level and in an enterprise context. You will also learn about how other technologies such as the Dynamic Root of Trust for Measurement (DRTM) and virtualization can both take advantage of TPMs and be used to enhance the TPM's capabilities.

- Offensive, Defensive, and Forensic Techniques for Determining Web User Identity
  This course looks at web users from a few different perspectives. First, we look at identifying techniques to determine web user identities from a server perspective. Second, we will look at obfuscating techniques from a user whom seeks to be anonymous. Finally, we look at forensic techniques, which, when given a hard drive or similar media, we identify users who accessed that server.

- Pcap Analysis & Network Hunting
  Introduction to Packet Capture (PCAP) explains the fundamentals of how, where, and why to capture network traffic and what to do with it. This class covers open-source tools like tcpdump, Wireshark, and ChopShop in several lab exercises that reinforce the material. Some of the topics include capturing packets with tcpdump, mining DNS resolutions using only command-line tools, and busting obfuscated protocols. This class will prepare students to tackle common problems and help them begin developing the skills to handle more advanced networking challenges.

- Malware Dynamic Analysis
  This introductory malware dynamic analysis class is dedicated to people who are starting to work on malware analysis or who want to know what kinds of artifacts left by malware can be detected via various tools. The class will be a hands-on class where students can use various tools to look for how malware is: Persisting, Communicating, and Hiding

- Secure Code Review
  The course briefly talks about the development lifecycle and the importance of peer reviews in delivering a quality product. How to perform this review is discussed and how to keep secure coding a priority during the review is stressed. A variety of hands-on exercises will address common coding mistakes, what to focus on during a review, and how to manage limited time.

- Smart Cards
  This course shows how smart cards are different compared to other type of cards. It is explained how smart cards can be used to realize confidentiality and integrity of information.

- The Life of Binaries
  Along the way we discuss the relevance of security at different stages of a binary’s life, from the tricks that can be played by a malicious compiler, to how viruses really work, to the way which malware “packers” duplicate OS process execution functionality, to the benefit of a security-enhanced OS loader which implements address space layout randomization (ASLR).

- Understanding Cryptology: Core Concepts
  This is an introduction to cryptology with a focus on applied cryptology. It was designed to be accessible to a wide audience, and therefore does not include a rigorous mathematical foundation (this will be covered in later classes).

- Understanding Cryptology: Cryptanalysis
  A class for those who want to stop learning about building cryptographic systems and want to attack them. This course is a mixture of lecture designed to introduce students to a variety of code-breaking techniques and python labs to solidify those concepts. Unlike its sister class, Core Concepts, math is necessary for this topic.

Intermediate Classes

- Exploits 1: Introduction to Software Exploits
  Software vulnerabilities are flaws in program logic that can be leveraged by an attacker to execute arbitrary code on a target system. This class will cover both the identification of software vulnerabilities and the techniques attackers use to exploit them. In addition, current techniques that attempt to remediate the threat of software vulnerability exploitation will be discussed.

- Exploits 2: Exploitation in the Windows Environment
  This course covers the exploitation of stack corruption vulnerabilities in the Windows environment. Stack overflows are programming flaws that often times allow an attacker to execute arbitrary code in the context of a vulnerable program.

There are many nuances involved with exploiting these vulnerabilities in Windows. Window's exploit mitigations such as DEP, ASLR, SafeSEH, and SEHOP, makes leveraging these programming bugs more difficult, but not impossible. The course highlights the features and weaknesses of many the exploit mitigation techniques deployed in Windows operating systems. Also covered are labs that describe the process of finding bugs in Windows applications with mutation based fuzzing, and then developing exploits that target those bugs.

- Intermediate Intel x86: Architecture, Assembly, Applications, & Alliteration
  Building upon the Introductory Intel x86 class, this class goes into more depth on topics already learned, and introduces more advanced topics that dive deeper into how Intel-based systems work.

Advanced Classes

- Advanced x86: Virtualization with Intel VT-x
  The purpose of this course is to provide a hands on introduction to Intel hardware support for virtualization. The first part will motivate the challenges of virtualization in the absence of dedicated hardware. This is followed by a deep dive on the Intel virtualization "API" and labs to begin implementing a blue pill / hyperjacking attack made famous by researchers like Joanna Rutkowska and Dino Dai Zovi et al. Finally a discussion of virtualization detection techniques.
- Advanced x86: Introduction to BIOS & SMM
  We will cover why the BIOS is critical to the security of the platform. This course will also show you what capabilities and opportunities are provided to an attacker when BIOSes are not properly secured. We will also provide you tools for performing vulnerability analysis on firmware, as well as firmware forensics. This class will take people with existing reverse engineering skills and teach them to analyze UEFI firmware. This can be used either for vulnerability hunting, or to analyze suspected implants found in a BIOS, without having to rely on anyone else.
- Introduction to Reverse Engineering Software
  Throughout the history of invention curious minds have sought to understand the inner workings of their gadgets. Whether investigating a broken watch, or improving an engine, these people have broken down their goods into their

elemental parts to understand how they work. This is Reverse Engineering (RE), and it is done every day from recreating outdated and incompatible software, understanding malicious code, or exploiting weaknesses in software.

- Reverse Engineering Malware
  This class picks up where the Introduction to Reverse Engineering Software course left off, exploring how static reverse engineering techniques can be used to understand what a piece of malware does and how it can be removed.

- Rootkits: What they are, and how to find them
  Rootkits are a class of malware which are dedicated to hiding the attacker’s presence on a compromised system. This class will focus on understanding how rootkits work, and what tools can be used to help find them.

- The Adventures of a Keystroke: An in-depth look into keylogging on Windows
  Keyloggers are one of the most widely used components in malware. Keyboard and mouse are the devices nearly all of the PCs are controlled by, this makes them an important target of malware authors. If someone can record your keystrokes then he can control your whole PC without you noticing.

Cybrary - Online Cyber Security Training

- CompTIA A+
  This course covers the fundamentals of computer technology, basic networking, installation and configuration of PCs, laptops and related hardware, as well as configuring common features for mobile operation systems Android and Apple iOS.

- CompTIA Linux+
  Our free, self-paced online Linux+ training prepares students with the knowledge to become a certified Linux+ expert, spanning a curriculum that covers Linux maintenance tasks, user assistance and installation and configuration.

- CompTIA Cloud+
  Our free, online Cloud+ training addresses the essential knowledge for implementing, managing and maintaining cloud

technologies as securely as possible. It covers cloud concepts and models, virtualization, and infrastructure in the cloud.

- CompTIA Network+
  In addition to building one's networking skill set, this course is also designed to prepare an individual for the Network+ certification exam, a distinction that can open a myriad of job opportunities from major companies
- CompTIA Advanced Security Practitioner
  In our free online CompTIA CASP training, you'll learn how to integrate advanced authentication, how to manage risk in the enterprise, how to conduct vulnerability assessments and how to analyze network security concepts and components.
- CompTIA Security+
  Learn about general security concepts, basics of cryptography, communications security and operational and organizational security. With the increase of major security breaches that are occurring, security experts are needed now more than ever.
- ITIL Foundation
  Our online ITIL Foundation training course provides baseline knowledge for IT service management best practices: how to reduce costs, increase enhancements in processes, improve IT productivity and overall customer satisfaction.
- Cryptography
  In this online course we will be examining how cryptography is the cornerstone of security technologies, and how through its use of different encryption methods you can protect private or sensitive information from unauthorized access.
- Cisco CCNA
  Our free, online, self-paced CCNA training teaches students to install, configure, troubleshoot and operate LAN, WAN and dial access services for medium-sized networks. You'll also learn how to describe the operation of data networks.
- Virtualization Management
  Our free, self-paced online Virtualization Management training class focuses on installing, configuring and managing

virtualization software. You'll learn how to work your way around the cloud and how to build the infrastructure for it.

- Penetration Testing and Ethical Hacking
  If the idea of hacking as a career excites you, you'll benefit greatly from completing this training here on Cybrary. You'll learn how to exploit networks in the manner of an attacker, in order to find out how protect the system from them.

- Computer and Hacking Forensics
  Love the idea of digital forensics investigation? That's what computer forensics is all about. You'll learn how to; determine potential online criminal activity at its inception, legally gather evidence, search and investigate wireless attacks.

- Web Application Penetration Testing
  In this course, SME, Raymond Evans, takes you on a wild and fascinating journey into the cyber security discipline of web application pentesting. This is a very hands-on course that will require you to set up your own pentesting environment.

- CISA - Certified Information Systems Auditor
  In order to face the dynamic requirements of meeting enterprise vulnerability management challenges, this course covers the auditing process to ensure that you have the ability to analyze the state of your organization and make changes where needed.

- Secure Coding
  Join industry leader Sunny Wear as she discusses secure coding guidelines and how secure coding is important when it comes to lowering risk and vulnerabilities. Learn about XSS, Direct Object Reference, Data Exposure, Buffer Overflows, & Resource Management.

- NIST 800-171 Controlled Unclassified Information Course
  The Cybrary NIST 800-171 course covers the 14 domains of safeguarding controlled unclassified information in non-federal agencies. Basic and derived requirements are presented for each security domain as defined in the NIST 800-171 special publication.

- Advanced Penetration Testing
  This course covers how to attack from the web using cross-site scripting, SQL injection attacks, remote and local file inclusion and how to understand the defender of the network you're breaking into to. You'll also learn tricks for exploiting a network.

- Intro to Malware Analysis and Reverse Engineering
  In this course you'll learn how to perform dynamic and static analysis on all major files types, how to carve malicious executables from documents and how to recognize common malware tactics and debug and disassemble malicious binaries.

- Social Engineering and Manipulation
  In this online, self-paced Social Engineering and Manipulation training class, you will learn how some of the most elegant social engineering attacks take place. Learn to perform these scenarios and what is done during each step of the attack.

- Post Exploitation Hacking
  In this free self-paced online training course, you'll cover three main topics: Information Gathering, Backdooring and Covering Steps, how to use system specific tools to get general information, listener shells, metasploit and meterpreter scripting.

- Python for Security Professionals
  This course will take you from basic concepts to advanced scripts in just over 10 hours of material, with a focus on networking and security.

- Metasploit
  This free Metasploit training class will teach you to utilize the deep capabilities of Metasploit for penetration testing and help you to prepare to run vulnerability assessments for organizations of any size.

- ISC2 CCSP - Certified Cloud Security Professional
  The reality is that attackers never rest, and along with the traditional threats targeting internal networks and systems, an entirely new variety specifically targeting the cloud has emerged.

Executive

- CISSP - Certified Information Systems Security Professional
  Our free online CISSP (8 domains) training covers topics ranging from operations security, telecommunications, network and internet security, access control systems and methodology and business continuity planning.

- CISM - Certified Information Security Manager
  Cybrary’s Certified Information Security Manager (CISM) course is a great fit for IT professionals looking to move up in their organization and advance their careers and/or current CISMs looking to learn about the latest trends in the IT industry.

- PMP - Project Management Professional
  Our free online PMP training course educates on how to initiate, plan and manage a project, as well as the process behind analyzing risk, monitoring and controlling project contracts and how to develop schedules and budgets.

- CRISC - Certified in Risk and Information Systems Control
  Certified in Risk and Information Systems Control is for IT and business professionals who develop and maintain information system controls, and whose job revolves around security operations and compliance.

- Risk Management Framework
  The National Institute of Standards and Technology (NIST) established the Risk Management Framework (RMF) as a set of operational and procedural standards or guidelines that a US government agency must follow to ensure the compliance of its data systems.

- ISC2 CSSLP - Certified Secure Software Life-cycle Professional
  This course helps professionals in the industry build their credentials to advance within their organization, allowing them to learn valuable managerial skills as well as how to apply the best practices to keep organizations systems running well.

- COBIT - Control Objectives for Information and Related Technologies
  Cybrary’s online COBIT certification program offers an opportunity to learn about all the components of the COBIT 5

framework, covering everything from the business end-to-end to strategies in how effectively managing and governing enterprise IT.

- Corporate Cybersecurity Management
  Cyber risk, legal considerations and insurance are often overlooked by businesses and this sets them up for major financial devastation should an incident occur.

Laboratories

Syracuse University's SEED

Hands-on Labs for Security Education

Started in 2002, funded by a total of 1.3 million dollars from NSF, and now used by hundreds of educational institutes worldwide, the SEED project's objective is to develop hands-on laboratory exercises (called SEED labs) for computer and information security education and help instructors adopt these labs in their curricula.

Software Security Labs

These labs cover some of the most common vulnerabilties in general software. The labs show students how attacks work in exploiting these vulnerabilities.

- Buffer-Overflow Vulnerability Lab
  Launching attack to exploit the buffer-overflow vulnerability using shellcode. Conducting experiments with several countermeasures.

- Return-to-libc Attack Lab
  Using the return-to-libc technique to defeat the "non-executable stack" countermeasure of the buffer-overflow attack.

- Environment Variable and Set-UID Lab
  This is a redesign of the Set-UID lab (see below).

- Set-UID Program Vulnerability Lab
  Launching attacks on privileged Set-UID root program. Risks of environment variables. Side effects of system().

- Race-Condition Vulnerability Lab
  Exploiting the race condition vulnerability in privileged program. Conducting experiments with various countermeasures.

- Format-String Vulnerability Lab
  Exploiting the format string vulnerability to crash a program, steal sensitive information, or modify critical data.

- Shellshock Attack Lab
  Launch attack to exploit the Shellshock vulnerability that is discovered in late 2014.

Network Security Labs

These labs cover topics on network security, ranging from attacks on TCP/IP and DNS to various network security technologies (Firewall, VPN, and IPSec).

- TCP/IP Attack Lab
  Launching attacks to exploit the vulnerabilities of the TCP/IP protocol, including session hijacking, SYN flooding, TCP reset attacks, etc.

- Heartbleed Attack Lab
  Using the heartbleed attack to steal secrets from a remote server.

- Local DNS Attack Lab
  Using several methods to conduct DNS pharming attacks on computers in a LAN environment.

- Remote DNS Attack Lab
  Using the Kaminsky method to launch DNS cache poisoning attacks on remote DNS servers.

- Packet Sniffing and Spoofing Lab
  Writing programs to sniff packets sent over the local network; writing programs to spoof various types of packets.

- Linux Firewall Exploration Lab
  Writing a simple packet-filter firewall; playing with Linux's built-in firewall software and web-proxy firewall; experimenting with ways to evade firewalls.

- Firewall-VPN Lab: Bypassing Firewalls using VPN
  Implement a simple vpn program (client/server), and use it to bypass firewalls.

- Virtual Private Network (VPN) Lab
  Design and implement a transport-layer VPN system for Linux, using the TUN/TAP technologies. This project requires at least a month of time to finish, so it is good for final project.

- Minix IPSec Lab
  Implement the IPSec protocol in the Minix operating system and use it to set up Virtual Private Networks.

- Minix Firewall Lab
  Implementing a simple firewall in Minix operating system.

Web Security Labs

These labs cover some of the most common vulnerabilities in web applications. The labs show students how attacks work in exploiting these vulnerabilities.

Elgg-Based Labs

Elgg is an open-source social-network system. We have modified it for our labs.

- Cross-Site Scripting Attack Lab
  Launching the cross-site scripting attack on a vulnerable web application. Conducting experiments with several countermeasures.

- Cross-Site Request Forgery Attack Lab
  Launching the cross-site request forgery attack on a vulnerable web application. Conducting experiments with several countermeasures.

- Web Tracking Lab
  Experimenting with the web tracking technology to see how users can be checked when they browse the web.

- SQL Injection Attack Lab
  Launching the SQL-injection attack on a vulnerable web application. Conducting experiments with several countermeasures.

Collabtive-Based Labs

Collabtive is an open-source web-based project management system. We have modified it for our labs.

- Cross-site Scripting Attack Lab
  Launching the cross-site scripting attack on a vulnerable web application. Conducting experiments with several countermeasures.

- Cross-site Request Forgery Attack Lab
  Launching the cross-site request forgery attack on a vulnerable web application. Conducting experiments with several countermeasures.

- SQL Injection Lab
  Launching the SQL-injection attack on a vulnerable web application. Conducting experiments with several countermeasures.

- Web Browser Access Control Lab
  Exploring browser's access control system to understand its security policies.

PhpBB-Based Labs

PhpBB is an open-source web-based message board system, allowing users to post messages. We have modified it for our labs.

- Cross-site Scripting Attack Lab
  Launching the cross-site scripting attack on a vulnerable web application. Conducting experiments with several countermeasures.
- Cross-site Request Forgery Attack Lab
  Launching the cross-site request forgery attack on a vulnerable web application. Conducting experiments with several countermeasures.
- SQL Injection Lab
  Launching the SQL-injection attack on a vulnerable web application. Conducting experiments with several countermeasures.
- ClickJacking Attack Lab
  Launching the ClickJacking attack on a vulnerable web site. Conducting experiments with several countermeasures.

System Security Labs

These labs cover the security mechanisms in operating system, mostly focusing on access control mechanisms in Linux.

- Linux Capability Exploration Lab
  Exploring the POSIX 1.e capability system in Linux to see how privileges can be divided into smaller pieces to ensure the compliance with the Least Privilege principle.

- Role-Based Access Control (RBAC) Lab
  Designing and implementing an integrated access control system for Minix that uses both capability-based and role-based access control mechanisms. Students need to modify the Minix kernel.

- Encrypted File System Lab
  Designing and implementing an encrypted file system for Minix. Students need to modify the Minix kernel.

Cryptography Labs

These labs cover three essential concepts in cryptography, including secrete-key encryption, one-way hash function, and public-key encryption and PKI.

- Secret Key Encryption Lab
  Exploring the secret-key encryption and its applications using OpenSSL.

- One-Way Hash Function Lab
  Exploring one-way hash function and its applications using OpenSSL.

- Public-Key Cryptography and PKI Lab
  Exploring public-key cryptography, digital signature, certificate, and PKI using OpenSSL.

Mobile Security Labs

These labs focus on the smartphone security, covering the most common vulnerabilities and attacks on mobile devices. An Android VM is provided for these labs.

- Android Repackaging Lab
  Insert malicious code inside an existing Android app, and repackage it.

- Android Device Rooting Lab
  Develop an OTA (Over-The-Air) package from scratch to root an Android device.

Pentester Lab

There is only one way to properly learn web penetration testing: by getting your hands dirty. We teach how to manually find and exploit vulnerabilities. You will understand the root cause of the problems and the methods that can be used to exploit them. Our exercises are based on common vulnerabilities found in different systems. The issues are not emulated. We provide you real systems with real vulnerabilities.

- From SQL Injection to Shell
  This exercise explains how you can, from a SQL injection, gain access to the administration console. Then in the administration console, how you can run commands on the system.

- From SQL Injection to Shell II
  This exercise explains how you can, from a blind SQL injection, gain access to the administration console. Then in the administration console, how you can run commands on the system.

- From SQL Injection to Shell: PostgreSQL edition
  This exercise explains how you can from a SQL injection gain access to the administration console. Then in the administration console, how you can run commands on the system.

- Web for Pentester
  This exercise is a set of the most common web vulnerabilities.

- Web for Pentester II
  This exercise is a set of the most common web vulnerabilities.

- PHP Include And Post Exploitation
  This exercice describes the exploitation of a local file include with limited access. Once code execution is gained, you will

see some post exploitation tricks.

- Linux Host Review
  This exercice explains how to perform a Linux host review, what and how you can check the configuration of a Linux server to ensure it is securely configured. The reviewed system is a traditional Linux-Apache-Mysql-PHP (LAMP) server used to host a blog.
- Electronic Code Book
  This exercise explains how you can tamper with an encrypted cookies to access another user's account.
- Rack Cookies and Commands injection
  After a short brute force introduction, this exercice explains the tampering of rack cookie and how you can even manage to modify a signed cookie (if the secret is trivial). Using this issue, you will be able to escalate your privileges and gain commands execution.
- Padding Oracle
  This course details the exploitation of a weakness in the authentication of a PHP website. The website uses Cipher Block Chaining (CBC) to encrypt information provided by users and use this information to ensure authentication. The application also leaks if the padding is valid when decrypting the information. We will see how this behavior can impact the authentication and how it can be exploited.
- XSS and MySQL FILE
  This exercise explains how you can use a Cross-Site Scripting vulnerability to get access to an administrator's cookies. Then how you can use his/her session to gain access to the administration to find a SQL injection and gain code execution using it.
- Axis2 Web service and Tomcat Manager
  This exercice explains the interactions between Tomcat and Apache, then it will show you how to call and attack an Axis2 Web service. Using information retrieved from this attack, you will be able to gain access to the Tomcat Manager and deploy a WebShell to gain commands execution.

- Play Session Injection
  This exercise covers the exploitation of a session injection in the Play framework. This issue can be used to tamper with the content of the session while bypassing the signing mechanism.

- Play XML Entities
  This exercise covers the exploitation of a XML entities in the Play framework.

- CVE-2007-1860: mod_jk double-decoding
  This exercise covers the exploitation of CVE-2007-1860. This vulnerability allows an attacker to gain access to unaccessible pages using crafted requests. This is a common trick that a lot of testers miss.

- CVE-2008-1930: Wordpress 2.5 Cookie Integrity Protection Vulnerability
  This exercise explains how you can exploit CVE-2008-1930 to gain access to the administration interface of a Wordpress installation.

- CVE-2012-1823: PHP CGI
  This exercise explains how you can exploit CVE-2012-1823 to retrieve the source code of an application and gain code execution.

- CVE-2012-2661: ActiveRecord SQL injection
  This exercise explains how you can exploit CVE-2012-2661 to retrieve information from a database.

- CVE-2012-6081: MoinMoin code execution
  This exercise explains how you can exploit CVE-2012-6081 to gain code execution. This vulnerability was exploited to compromise Debian's wiki and Python documentation website.

- CVE-2014-6271/Shellshock
  This exercise covers the exploitation of a Bash vulnerability through a CGI.

Dr. Thorsten Schneider's Binary Auditing

Learn the fundamentals of Binary Auditing. Know how HLL mapping works, get more inner file understanding than ever. Learn how to find and analyse software vulnerability. Dig inside Buffer Overflows and learn how exploits can be prevented. Start to analyse your first viruses and malware the safe way. Learn about simple tricks and how viruses look like using real life examples.

- Binary Auditing

Damn Vulnerable Web Application (DVWA)

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

- Damn Vulnerable Web Application (DVWA)

Damn Vulnerable Web Services

Damn Vulnerable Web Services is an insecure web application with multiple vulnerable web service components that can be used to learn real world web service vulnerabilities. The aim of this project is to help security professionals learn about Web Application Security through the use of a practical lab environment.

- Damn Vulnerable Web Services

NOWASP (Mutillidae)

OWASP Mutillidae II is a free, open source, deliberately vulnerable web-application providing a target for web-security enthusiest. With dozens of vulns and hints to help the user; this is an easy-to-use web hacking environment designed for labs, security enthusiast, classrooms, CTF, and vulnerability assessment tool targets. Mutillidae has been used in graduate security courses, corporate web sec training courses, and as an "assess the assessor" target for vulnerability assessment software.

- OWASP Mutillidae

OWASP Broken Web Applications Project

Open Web Application Security Project (OWASP) Broken Web Applications Project, a collection of vulnerable web applications that is distributed on a Virtual Machine in VMware format compatible with their no-cost and commercial VMware products.

- OWASP Broken Web Applications Project

OWASP Bricks

Bricks is a web application security learning platform built on PHP and MySQL. The project focuses on variations of commonly seen application security issues. Each 'Brick' has some sort of security issue which can be leveraged manually or using automated software tools. The mission is to 'Break the Bricks' and thus learn the various aspects of web application security.

- OWASP Bricks

OWASP Hackademic Challenges Project

The Hackademic Challenges implement realistic scenarios with known vulnerabilities in a safe and controllable environment. Users can attempt to discover and exploit these vulnerabilities in order to learn important concepts of information security through an attacker's perspective.

- OWASP Hackademic Challenges project

Web Attack and Exploitation Distro (WAED)

The Web Attack and Exploitation Distro (WAED) is a lightweight virtual machine based on Debian Distribution. WAED is pre-configured with various real-world vulnerable web applications in a sandboxed environment. It includes pentesting tools that aid in finding web application vulnerabilities. The main motivation behind this project is to provide a practical environment to learn about web application's vulnerabilities without the hassle of dealing with complex configurations. Currently, there are around 18 vulnerable applications installed in WAED.

- Web Attack and Exploitation Distro (WAED)

Xtreme Vulnerable Web Application (XVWA)

XVWA is a badly coded web application written in PHP/MySQL that helps security enthusiasts to learn application security. It’s not advisable to host this application online as it is designed to be “Xtremely Vulnerable”. We recommend hosting this application in local/controlled environment and sharpening your application security ninja skills with any tools of your own choice. It’s totally legal to break or hack into this. The idea is to evangelize web application security to the community in possibly the easiest and fundamental way. Learn and acquire these skills for good purpose. How you use these skills and knowledge base is not our responsibility.

- Xtreme Vulnerable Web Application (XVWA)

WebGoat: A deliberately insecure Web Application

WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons.

- WebGoat

Audi-1's SQLi-LABS

SQLi-LABS is a comprehensive test bed to Learn and understand nitti gritty of SQL injections and thereby helps professionals understand how to protect.

- SQLi-LABS
- SQLi-LABS Videos

Capture the Flag

Vulnhub

We all learn in different ways: in a group, by yourself, reading books, watching/listening to other people, making notes or things out for yourself. Learning the basics & understanding them is essential; this knowledge can be enforced by then putting it into practice.

Over the years people have been creating these resources and a lot of time has been put into them, creating 'hidden gems' of training material. However, unless you know of them, its hard to discover them.

So VulnHub was born to cover as many as possible, creating a catalogue of 'stuff' that is (legally) 'breakable, hackable & exploitable' - allowing you to learn in a safe environment and practise 'stuff' out. When something is added to VulnHub's database it will be indexed as best as possible, to try and give you the best match possible for what you're wishing to learn or experiment with.

- Vulnhub Repository

CTF Write Ups

- CTF Resources
  A general collection of information, tools, and tips regarding CTFs and similar security competitions.

- CTF write-ups 2016
  Wiki-like CTF write-ups repository, maintained by the community. (2015)

- CTF write-ups 2015
  Wiki-like CTF write-ups repository, maintained by the community. (2015)

- CTF write-ups 2014
  Wiki-like CTF write-ups repository, maintained by the community. (2014)

- CTF write-ups 2013
  Wiki-like CTF write-ups repository, maintained by the community. (2013)

CTF Repos

- captf
  This site is primarily the work of psifertex since he needed a dump site for a variety of CTF material and since many other public sites documenting the art and sport of Hacking Capture the Flag events have come and gone over the years.

- shell-storm
  The Jonathan Salwan's little corner.

SecurityTube Playlists

Security Tube hosts a large range of video tutorials on IT security including penetration testing , exploit development and reverse engineering.

- SecurityTube Metasploit Framework Expert (SMFE)
  This video series covers basics of Metasploit Framework. We will look at why to use metasploit then go on to how to exploit vulnerbilities with help of metasploit and post exploitation techniques with meterpreter.
- Wireless LAN Security and Penetration Testing Megaprimer
  This video series will take you through a journey in wireless LAN (in)security and penetration testing. We will start from the very basics of how WLANs work, graduate to packet sniffing and injection attacks, move on to audit infrastructure vulnerabilities, learn to break into WLAN clients and finally look at advanced hybrid attacks involving wireless and applications.
- Exploit Research Megaprimer
  In this video series, we will learn how to program exploits for various vulnerabilities published online. We will also look at how to use various tools and techniques to find Zero Day vulnerabilities in both open and closed source software.
- Buffer Overflow Exploitation Megaprimer for Linux
  In this video series, we will understand the basic of buffer overflows and understand how to exploit them on linux based systems. In later videos, we will also look at how to apply the same principles to Windows and other selected operating systems.

Open Security Books

Crypto 101 - lvh

Comes with everything you need to understand complete systems such as SSL/TLS: block ciphers, stream ciphers, hash functions, message authentication codes, public key encryption, key agreement protocols, and signature algorithms. Learn how to exploit common cryptographic flaws, armed with nothing but a little time and your favorite programming language. Forge administrator cookies, recover passwords, and even backdoor your own random number generator.

- Crypto101
- LaTeX Source

A Graduate Course in Applied Cryptography - Dan Boneh & Victor Shoup

This book is about constructing practical cruptosystems for which we can argue security under plausible assumptions. The book covers many constructions for different tasks in cryptography. For each task we define the required goal. To analyze the constructions, we develop a unified framework for doing cryptographic proofs. A reader who masters this framework will capable of applying it to new constructions that may not be covered in this book. We describe common mistakes to avoid as well as attacks on real-world systems that illustratre the importance of rigor in cryptography. We end every chapter with a fund application that applies the ideas in the chapter in some unexpected way.

- A Graduate Course in Applied Cryptography

Security Engineering, A Guide to Building Dependable Distributed Systems - Ross Anderson

The world has changed radically since the first edition of this book was published in 2001. Spammers, virus writers, phishermen, money launderers, and spies now trade busily with each other in a lively online criminal economy and as they specialize, they get better. In this indispensable, fully updated guide, Ross Anderson reveals how to build systems that stay dependable whether faced with error or malice. Here?s straight talk on critical topics such as technical engineering basics, types of attack, specialized protection mechanisms, security psychology, policy, and more.

- Security Engineering, Second Edition

Reverse Engineering for Beginners - Dennis Yurichev

This book offers a primer on reverse-engineering, delving into disassembly code-level reverse engineering and explaining how to decipher assembly language for those beginners who would like to learn to understand x86 (which accounts for almost all executable software in the world) and ARM code created by C/C++ compilers.

- Reverse Engineering for Beginners
- LaTeX Source

CTF Field Guide - Trail of Bits

The focus areas that CTF competitions tend to measure are vulnerability discovery, exploit creation, toolkit creation, and operational tradecraft.. Whether you want to succeed at CTF, or as a computer security professional, you'll need to become an expert in at least one of these disciplines. Ideally in all of them.

- CTF Field Guide
- Markdown Source

Challenges

- Reverse Engineering Challenges
- Matasano Crypto Challenges

Documentation

OWASP - Open Web Application Security Project

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

- Open Web Application Security Project

Applied Crypto Hardening - bettercrypto.org

This guide arose out of the need for system administrators to have an updated, solid, well re-searched and thought-through guide for configuring SSL, PGP,SSH and other cryptographic tools in the post-Snowdenage. Triggered by the NSA leaks in the summer of 2013, many system administrators and IT security officers saw the need to strengthen their encryption settings.This guide is specifically written for these system administrators.

- Applied Crypto Hardening
- LaTeX Source

PTES - Penetration Testing Execution Standard

The penetration testing execution standard cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.

- Penetration Testing Execution Standard

Related Awesome Lists

- Awesome Pentest
  A collection of awesome penetration testing resources, tools and other shiny things.

- Awesome Appsec
  A curated list of resources for learning about application security.
- Awesome Malware Analysis
  A curated list of awesome malware analysis tools and resources.
- Android Security Awesome
  A collection of android security related resources.
- Awesome CTF
  A curated list of CTF frameworks, libraries, resources and softwares.
- Awesome Security
  A collection of awesome software, libraries, documents, books, resources and cools stuffs about security.
- Awesome Honeypots
  A curated list of awesome honeypots, tools, components and much more.
- Awesome Incident Response
  A curated list of tools and resources for security incident response, aimed to help security analysts and DFIR teams.
- Awesome Threat Intelligence
  A curated list of awesome Threat Intelligence resources.
- Awesome PCAP Tools
  A collection of tools developed by other researchers in the Computer Science area to process network traces.
- Awesome Forensics
  A curated list of awesome forensic analysis tools and resources.

- Awesome Hacking
  A curated list of awesome Hacking tutorials, tools and resources.
- Awesome Industrial Control System Security
  A curated list of resources related to Industrial Control System (ICS) security.
- Awesome Web Hacking
  This list is for anyone wishing to learn about web application security but do not have a starting point.
- Awesome Sec Talks
  A curated list of awesome Security talks.
- Awesome YARA
  A curated list of awesome YARA rules, tools, and people.
- Sec Lists
  SecLists is the security tester's companion. It is a collection of multiple types of lists used during security assessments. List types include usernames, passwords, URLs, sensitive data grep strings, fuzzing payloads, and many more.

Contributing

Pull requests and issues with suggestions are welcome!

License