GUIDEM

Ethical Hacking:
Vulnerability Assessment & Penetration Testing

The best hands-on training course for beginners and professionals who aspire to enter the field of Penetration Testing and Offensive security testing.

Authors: Mark Christian Secretario & Renzon Cruz

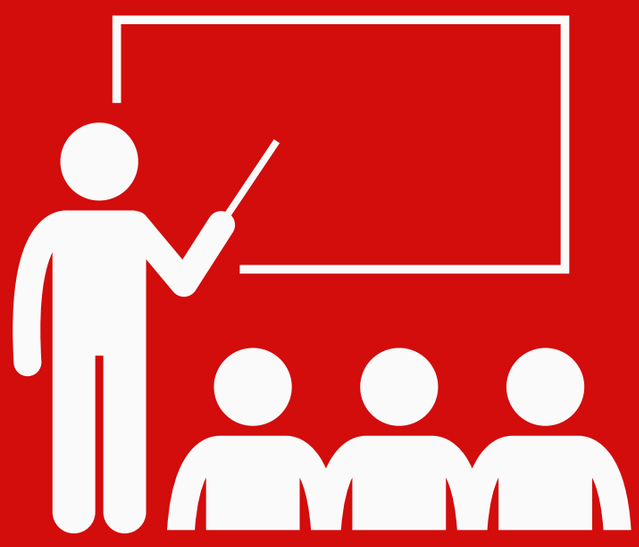
Company Profile

GuideM is a top specialized training and consulting services provider that delivers real-world approaches in both Offensive (Red) and Defensive (Blue) disciplines of Cybersecurity in the Philippines. We provide professional training and services wherein we take pride in producing world-class quality comprehensive, highly technical, and purely hands-on courses.

OUR INSTRUCTORS

- Seasoned Industry Professionals
- Several years of Experience
- Well known in the industry

OUR COURSES



- Hands-on exercises
- Real-world use cases
- Quality discussion
- Final Challenge (CTF)

GuideM Training courses are intensively for security practitioners to gain real-world hands on knowledge which aim to equip useful skills and practical knowledge that is up to date.

GUIDEM

Our Founder

Mark Christian Secretario, also known as Ian, is a highly experienced cybersecurity professional and the esteemed founder of GuideM. Beyond his technical expertise, He plays a pivotal role in leading GuideM's training and consulting services, offering Security Assessments, VAPT, Red Team, Purple Team, and cybersecurity advisory.

Ian is also responsible for the implementation of a cutting-edge learning platform, keeping GuideM at the forefront of technological advancements. He is actively involved in the company and client's growth, personally teaching and developing both offensive and defensive cybersecurity courses, solidifying GuideM's reputation as a trusted authority in the field. He also guides clients in vetting potential employees from the talent pool and oversees immersive learning events, and customized in-house training. Additionally, Ian is working closely mentoring and guiding the next generation of cybersecurity professionals.

GUIDEM

Course Overview

This course is designed to enable those who aspire to enter the Information Security field in understanding the core concepts of network hacking in order to safeguard a network infrastructure. This course provides all the fundamental skills needed to carry out a thorough and professional penetration test against an enterprise network.

This is a purely practical training course where students would spend more time doing the well-prepared hands-on hacking execises while in conjunction to theoretical discussion. This course also provides advice and best practices to solve security issues detected during a penetration test.

At the end of this course, the student will be expected to be familiar on how enterprise system, network and web application security testing hacks are performed and will be fully equipped to test and safeguard a network infrastructure against various real-time attack vectors.

GUIDEM

Course Structure

This training course presents comprehensive ethical hacking concepts. Our topics included on this bootcamp were chosen efficiently based on the current demand of the market when looking for a rockstar penetration tester. The course covers the fundamentals such as basics in Linux and Windows CLI to intermediate topics such as Buffer Overflow.

The objective of this course is to strengthen your ethical hacker mindset and be efficient as a Penetration Tester or VAPT engineer.

Learn Ethical Hacking based on the real world scenarios and use-cases.

Training Highlights

- 35+ Hands-on Lab Activities
- 400+ Presentation Slides
- 16 Custom VMs that you can hack in different kind of scenarios
- Methodological approach with best practices
- Final Hack The Kingdom challenge (CTF)
- GuideM Certification Exam:
  Guidem Certified Penetration Testerer (GMCPT)

GUIDEM

Course Author

MARK CHRISTIAN SECRETARIO | @iansecretario_

Red Team Consultant / Penetration Tester

11+ years in Information Technology

- Malware Development & Purple Team Practitioner
- Freelance & Independent Consultant

Founder and Lead Instructor

- Cybersecurity Training & Services Provider

Hackstreetboys Member

- All Filipino CTF Team

Specialties & Focus Area:

- Red Team/Offensive Security
- Purple Team/Adversary Simulation
- Security Research & Exploit Development
- Evasion and Malware development

Certifications:

- GIAC Web Application Penetration Tester (GWAPT)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Security Essentials (GSEC)
- GIAC Certified Incident Handler (GCIH)
- GIAC Enterprise Vulnerability Assessor (GEVA)
- GIAC Exploit Researcher & Advanced Penetration Tester (GXPN)
- GIAC Web Application Penetration Tester (GWAPT)
- Offensive Security Certified Expert (OSCE)
- Offensive Security Certified Professional(OSCP)
- Certified Red Team Professional (CRTP)
- Certified Red Team Expert (CRTE)
- Certified Red Team Operator(CRTO)
- Certified Red Team Master(CRTM)
- Certified Red Team Lead(CRTL)
- Certified Azure Red Team Professional (CARTP)
- Red Team Operator Level 1 – Rastalabs (Hackthebox)
- Red Team Operator Level 2 – Cybernetics (Hackthebox)
- Red Team Operator Level 3 – APT Labs(Hackthebox)
- Elearnsecurity Exploit Development Professional(eCXD)
- Elearnsecurity Certified Penetration Testing Extreme(eCPTXv2)
- eLearnSecurity Web Application Penetration Tester Expert (eWPTX)
- eLearnSecurity Web ApplicationPenetration Tester (eWPT)
- Pentester Academy Certified Enterprise Specialist (PACES)
- Certified Red Team Professional (Cyberwarfare)
- Certified Red Team Analyst (CyberWarfare)
- Cisco Certified Network Professional (CCNP)
- Cisco Certified Network Associate (CCNA)
- CCNA Cyber OPS

GUIDEM

Course Author

RENZON CRUZ | @r3nzsec | www.renzoncruz.com

GCFA | GCFE | GCIH | eCTHP | eCDFP | eJPT | MCS | MCP | ITIL

Co-Founder of GuideM | Senior Security Consultant - Digital Forensics & Incident Response

- 8 yrs. of professional experience
- Part of National Security - Middle East
- Course Author & Instructor

Specialties & Focus Area:

- SOC & Threat Hunting
- Incident Response
- Digital Forensics
- Malware Analysis
- Adversary Simulation

Speakership:

- BSides London 2019
- BSides Vancouver 2019
- BSides Doha 2020
- ROOTCON PH 2020

Certifications:

- GIAC Certified Forensics Analyst
- GIAC Certified Forensics Examiner
- GIAC Certified Incident Handler
- eLearnSecurity Threat Hunting Professional
- eLearnSecurity Digital Forensics Professional
- eLearnSecurity Junior Penetration Tester
- Cybersec First Responder
- Microsoft Certified Specialist - Azure
- Microsoft Certified Professional - Virtualization
- Information Technology Infrastructure Library

GUIDEM

Course Information

System Requirements

- Core i5/Ryzen 5 or greater
- 8GB RAM minimum
- 100GB free storage
- Installed Virtualization software such as VMware Workstation or Fusion

Target Audience

Ethical Hacking:VAPT primarily targets students, career-shifters and IT practitioners who wants to gain knowledge in Vulnerability Assessment and Penetration Testing. This is also open to all infosec professionals who wants to improve their workflow in performing the security assessment, vulnerability assessment and penetration testing engagement.

Red Team / Penetration Testers

- Aspiring Penetration Testers, career shifters such as: Software Engineer, HelpDesk, Network Engineer, System Administrator
- IT Professionals with minimum of 1-2 yrs of related experience

Blue Team / IT Security Professionals

- SOC Analyst, IR, Threat Hunters who want to improve their knowledge on how penetration testers and attackers work

GUIDEM

MODULE 1

Information Security, Operating System Commands

The student is initially introduced to the field of Information Security. Here, they will learn the InfoSec culture, terminologies and career opportunities that are waiting for them once succeeded. Day 1 will be a jam-packed start as they will immediately learn common hacking techniques and useful Linux commands, as security professionals love to work on a command line or terminal.

We will also cover what is Kali Linux and why it is a favorite Linux distribution when it comes to penetration testing. We will introduce various tools or we can say “Hacker Tools” within Kali Linux and right after that are the 5 phases in penetration testing.

Topics

- Information Security Domains
- Information Security Jobs and Career Path
- Basic Security Terminologies
- CIA Triad, Threats, Risk and Vulnerabilities
- Operating System Fundamentals
- Identifying and Classifying Vulnerabilities
- Best Practices in Vulnerability Assessment
- Validating Vulnerability Scans
- Vulnerability Reporting Guideline

Hands-on Exercises

- Linux Fundamentals
- Windows CLI Fundamentals
- Vulnerability Scanning
- Vulnerability Assessment Validation
- Vulnerability Reporting Guideline

MODULE 2

Penetration Testing and Real-World Use Cases

This module will start off by introducing the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. As one of the most important part of the penetration test is reporting, this Module will teach best practices on current enterprise reporting standard. The student will be hacking throughout the use of Metasploit Framework and utilize theory with practice.

We will also be optimizing real-world scenarios wherein how much of these vulnerabilities are still being exploited on enterprise environments.

Topics

- Ethical Hacking & Penetration Testing
- Types of Penetration Tests
- Penetration Testing Process
- Scanning & Enumeration
- Identify & Exploit Most Common Infrastructure Vulnerabilities
- Exploiting Vulnerabilities with Metasploit
- Exploits, Payloads, Server-Side & Client Side Attacks
- Penetration test Data Collection and Organization
- Penetration Test Reporting

Hands-on Exercises

- Attacking a Windows Host
- Attacking a Linux Host
- Bind Shell
- Reverse Shell
- File transfer using Netcat
- Metasploit and MSFVenom
- Data Management using Metasploit

MODULE 3

Establishing Foothold and Moving Deeper into the Infrastructure

Shell is only the beginning. This Module will thoroughly discuss privilege escalation in Linux and Windows operating systems, varying from basics such as file permissions, running processes and weak services to in-depth coverage and demonstrations of actual privilege escalation techniques.

Students will also gain essential skills that will reinforce real-world mindset on utilizing obtained sensitive information that can be used on a penetration testing engagement.

Topics

- Windows Privilege Escalation
- Tools for Finding Local Privilege Escalation Vulnerabilities on Windows
- Linux Privilege Escalation
- Tools for Finding Local Privilege Escalation Vulnerabilities on Linux
- Pivoting and Lateral Movement
- Password Cracking Techniques
- Password Dumping & Credential Reuse

Hands-on Exercises

- Windows Privilege Escalation Labs
  - Kernel Exploitations
  - Unquoted Service Path
  - Weak Binary Permission & More
- Linux Privilege Escalation Labs
  - Kernel Exploits
  - Abusing Sudo Permission
  - Cron Jobs
  - Exploiting SUID Binaries & More
- Pivoting and Lateral Movement Lab
- Password Attacks
- Password Dumping Attacks
- Capstone 1 : Pentest Report

MODULE 4

Fundamentals in Web and Web Application Technologies

One of the biggest demand in the market today is Web Application Security, where you can earn tons of money by joining bug bounty programs. This module contains an introduction to Web Application Security. It also dissects and explains the most widespread web application vulnerabilities and types of attack that are commonly used when exploiting vulnerable web apps such as SQL Injection, Cross Site Scripting, etc.

The primary topics within this course cover both manual and automated methods of detection and exploitation of web application vulnerabilities. Students will be getting actual hands-on exposure to industry standard tools such as Burpsuite, Nmap, Nikto, Sqlmap and many more.

Topics

- Web Application Security Fundamentals
- Web Application Testing Methodology
- OWASP Top 10 Web Application Attacks
- Tools, Process and Best Practices
- Identify and Exploit Web Application Vulnerabilities

Hands-on Exercises

- Manual SQL Injection
- SQLi using SQLmap
- Credential Bruteforcing using Burp
- XXE injection
- Local File Inclusion
- Remote File Inclusion

MODULE 5

Exploit Development Basics & PowerShell Fundamentals

In the world of cybersecurity, vulnerabilities are unintended flaws found in software programs or operating systems. The term “zero-day” refers to a newly discovered software vulnerability. Because the developer has just learned about the flaw this would also mean an official patch or update to fix the issue hasn’t been developed or released yet.

PowerShell is now the most abused, such as requiring scripts that can almost do anything. This Module covers the Living off the Land technique of being a penetration tester. PowerShell fundamentals teaches the student the very essentials of PowerShell from utilizing command line interface to various useful commands and components as they relate to PowerShell and its use in Penetration Testing.

Topics

- Assembly x86 Bit Fundamentals
- Exploit Development Process
- Fuzzing and Vulnerability Discovery
- Buffer Overflow Attacks
- Creating Your Own Exploit using Python
- PowerShell fundamentals
- PowerShell for Post Exploitation

Hands-on Exercises

- Exploit Development Lab 1
- Exploit Development Lab 2
- Powershell Empire
- Hack The Kingdom
- Final Capstone : CTF pentest report

Contact Us

training@guidem.ph

facebook.com/guidemtraining

linkedin.com/company/guidemtraining

twitter.com/guidemtraining

instagram.com/guidemtraining

GUIDEM