GUIDEM

OPT

OFFENSIVE PENETRATION TESTING

LEVEL UP!

- Intermediate course to sharpen penetration testing skills.
- Active Directory Attacks
- Relaying & MSSQL Attacks
- Antivirus Evasion and Obfuscation

Authors: Mark Christian Secretario & Renzon Cruz

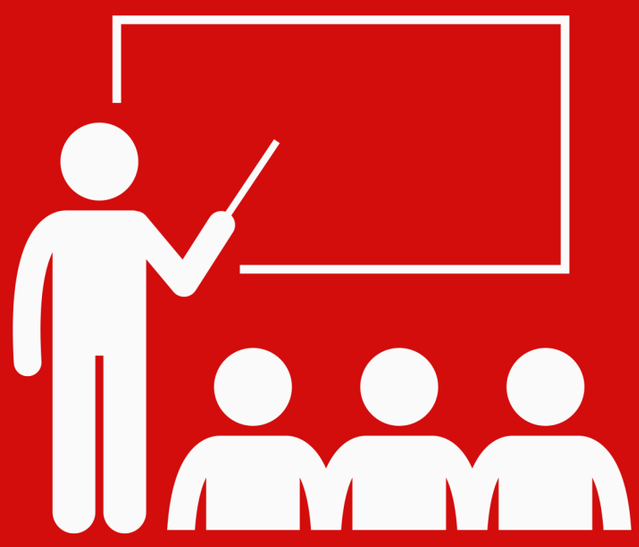
Company Profile

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

Offensive Penetration Testing is an intermediate course is crafted to bridge the skill gap between penetration testers and aspiring red team operators. Providing a detailed and comprehensive approach for gaining the necessary skills to perform penetration tests and moving up deeper understanding of how attacks and misconfigurations work which is an essential skill for senior pentesters and red team operators.

- Provide the next level skillset for penetration testers and security practitioners
- Real-World Scenarios to learn offensive techniques
- Modern approach penetration testing

Why Offensive Penetration Testing

A game changer training course on how to deliver and use the kill chain for penetration testing. Exercises will leverage each phase from Reconnaissance to Data exfiltration.

Prerequisite Knowledge

Students are expected to have practical penetration testing knowledge. The course is a follow up to our EH:VAPT course.

- Knowledge on the basics of Vulnerability Assessment & Penetration Testing
- Ability to conduct extensive research to deeply understand the topics
- Fundamental Penetration testing methodology
- Hands on experience on conducting a penetration test with report

  (if prerequisites are not met consider enrolling on our EH:VAPT course)

Training Highlights

- 70% of the training are focused on laboratory based exercises with over more than 25 Laboratory exercise
- 700 slide presentation slides
- Final CTF Penetration Testing challenge
- Final Capstone Case study
- Included 48 hour hands on based GuideM Certification Exam

System Requirements

The laboratory environment will be a mixed of self hosted machines and an enterprise environment to practice more complex chain of attacks.

- CPU or laptop models released 2019 onwards
- Core i5 11th generation /Ryzen 5 or greater
- 24 GB RAM minimum, 32gb ram or more recommended
- 200GB free storage
- Installed Virtualization software such as VMware Workstation/Fusion

GUIDEM

Course Information

Target Audience

Offensive Penetration testing focuses on attacks and toolsets being used by penetration testers, red teamers and sometimes adversaries, Gaining an understanding about the offensive methodology will be beneficial to any security practitioners.

Red Team

- Learn how to conduct real-world penetration test on an enterprise level
- Gain practical knowledge about assumed breach/internal penetration test
- Obtain foundational knowledge necessary to participate and start a red team career

Blue Team

- Understand how attacks are conducted to improve awareness
- Learn about attacks and toolset being used by adversaries
- Advance your knowledge about offensive tradecraft and strategies

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

GDAT | GNFA | GCFA | GCFE | GCIH | eCIR | eCTHP | eCDFP | eJPT | MCS | MCP | ITIL

Principal Consultant, DFIR at Unit 42 | Co-Founder of GuideM

- 10 yrs. of professional experience
- Part of National Security - GCC
- Course Author & Instructor | Cyber DFIR Consultant

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
- NorthSec Canada 2021
- DEFCON BTV 2021

Certifications:

- GIAC Certified Forensics Analyst
- GIAC Network Forensics Analyst
- GIAC Certified Forensics Examiner
- GIAC Certified Incident Handler
- eLearnSecurity Threat Hunting Professional
- eLearnSecurity Certified Incident Responder
- eLearnSecurity Digital Forensics Professional
- eLearnSecurity Junior Penetration Tester

GUIDEM

Module 1

Modern Penetration Testing

Starting off the training with essential topics on penetration testing such as full surface scoping, attack map surfacing, OSINT, and more. Students will be introduced to how to do "Better Penetration Testing" and provide a high-value penetration test report. We will be leveraging different tools for penetration testing for common vulnerabilities, and adjust them depending on the requirements.

Module Highlights & Key Learning

- Provide high-value on penetration testing engagements
- Conduct OSINT and target interesting users
- Understand the methodologies on External,Internal and Assumed Compromised penetration test
- Better Penetration testing using tools to make life easier
- Metasploit scripting, Data collection and mapping.

Module 2

Network Infrastructure attacks & Credential Abuse

This module is about utilizing network attacks and leveraging credential abuse accross the network infrastructure. Learn about top attack vectors and techniques being used by penetration testers to gain credentials and obtain internal access to the target environment.

Module Highlights & Key Learning

- Learn about external attack surface mapping
- Deeply understand how to conduct internal network attacks
- Poisoning multicast name resolution with Responder
- Launch MiTM attacks like ARP spoofing
- Perform enterprise password attacks such as credential abuse/relay and password spraying

GUIDEM

Module 3

Enterprise Active Directory Attacks

In this module, we'll focus on Enterprise active directory attacks and domain lateral movement techniques. Students will obtain in-depth technical knowledge on how to attack kerberos authentication and learn about typical powershell commands for offensive operations. Students will learn how to enumerate the target organization and map out the internal domain structure in the perspective of identifying feasible attack paths that can be leveraged in order to gain full active directory compromise.

Module Highlights and Key Learning

- Active directory basics
- PowerShell for offensive penetration testing
- Credential dumping and reuse
- Domain Privilege escalation and Token impersonation
- Bloodhound Domain Enumeration and Mapping
- Domain Privilege Escalation & Domain Dominance

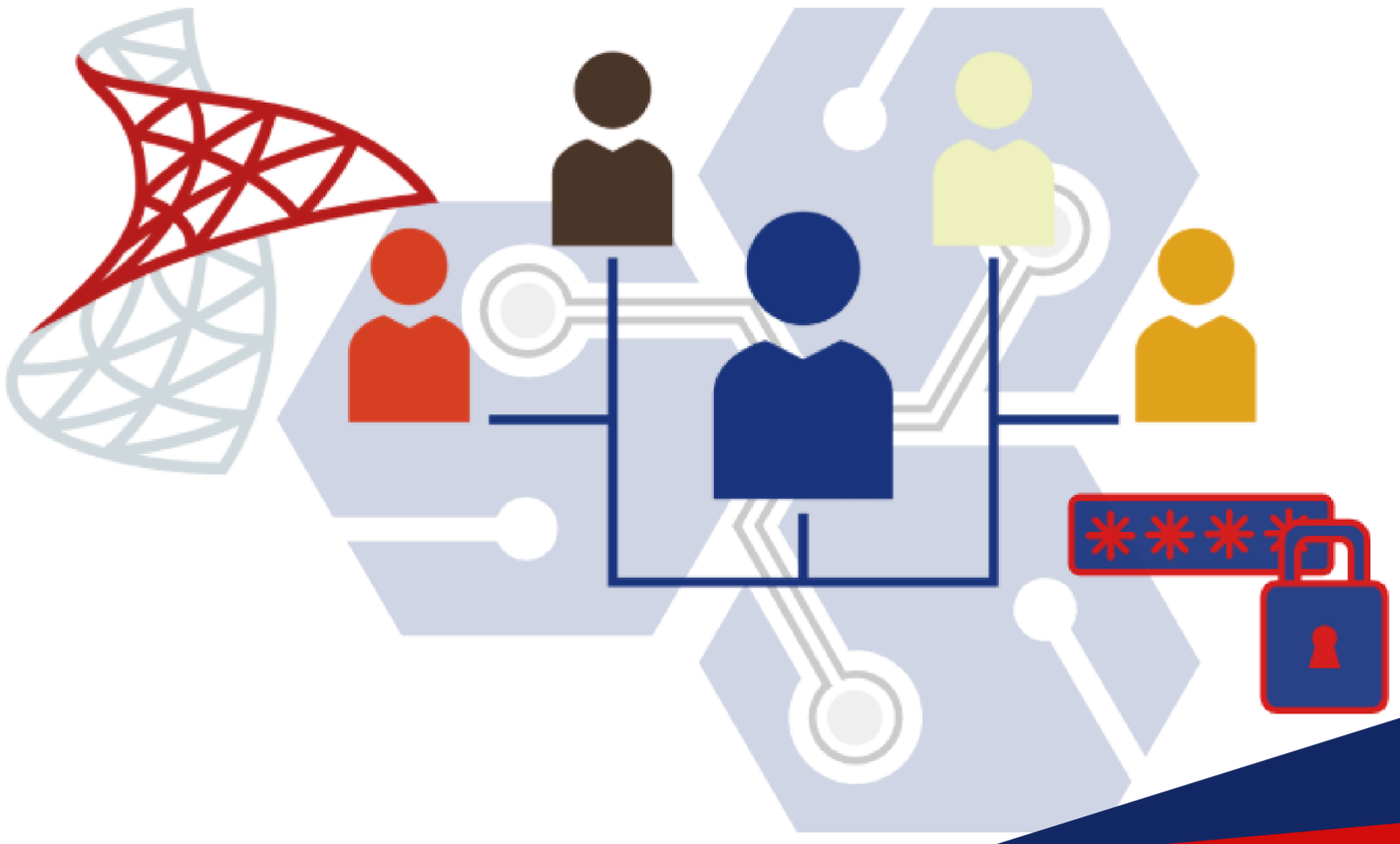
Module 4

System & Web Infrastructure Pillaging

This part of the module will go in depth on how to move laterally and break into different parts of an enterprise. Starting out from an assume breach standpoint. Students will be learning about how to attack internal web applications, employee portals and perform privilege escalation. This module will also tackle on how to move from one system to another with the goal of accessing confidential information about the target organization.

Module Highlights and Key Learning

- Elevate and escalate privileges
- Perform attack against internal web application
- Attack and exploit MSSQL servers
- Adapt and Enumerate systems within scope
- Perform pivoting and lateral movement
- Analyze users in the systems and perform post-exploitation



GUIDEM

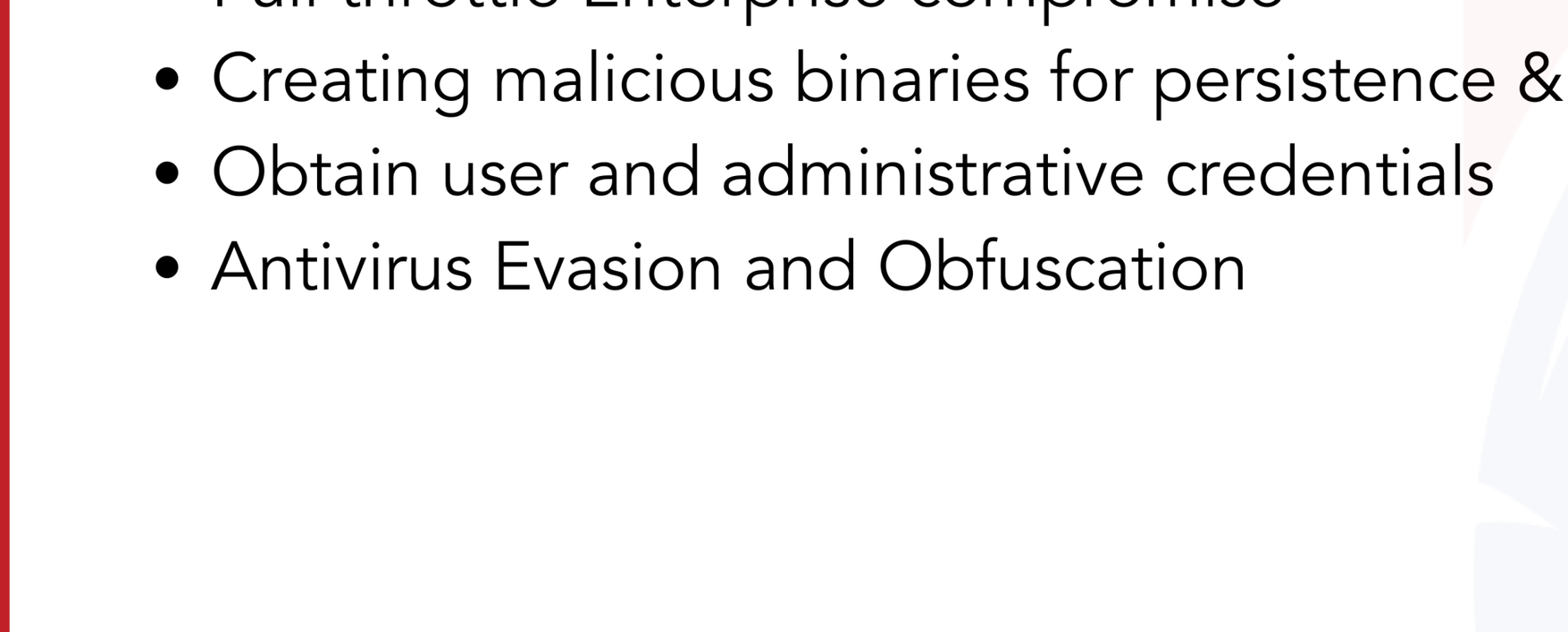
Module 5

Full Throttle Offensive Penetration Testing

The last module will summarize the overall objective of this training. All the laboratories will be putting together all the lessons and methodology in order to fully compromise and obtain full control of an enterprise organization using active directory attacks.

Module Highlights and Key Learning

- Full throttle Enterprise compromise
- Creating malicious binaries for persistence & maintaining access
- Obtain user and administrative credentials
- Antivirus Evasion and Obfuscation



GUIDEM

Contact Us

training@guidem.ph

facebook.com/guidemtraining

linkedin.com/company/guidemtraining

twitter.com/guidemtraining

instagram.com/guidemtraining

GUIDEM