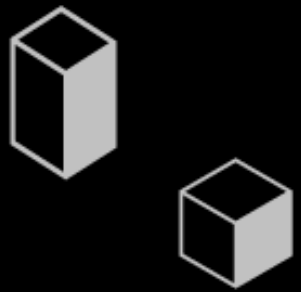
Cyber Security Fundamentals

Learn the Fundamentals of Cybersecurity
"**GOMYCODE MASTERCLASS**"



Presented by: Taher Amine ELHOUARI - CISSP

SUMMARY

- Introduction to Information and Cyber Security
- Privacy and Data Protection
- Introduction to GRC (Governance, Risk, Compliance)
- Introduction to Blue Teams and Defensive Security
- Introduction to Red Teams and Offensive Security
- Cyber Security Certifications
- Networking in the Industry
- Resources and Platforms to Practice
- Project Ideas
- What about CompTIA Security+ | GOMYCODE?
- IT Security Careers & RoadMap
- SURPRISE!!

GOMYCODE

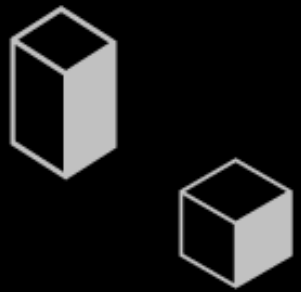
Taher Amine ELHOUARI

Cyber Security Leader & Global Consultant

- Founding President @ OWASP Algiers Chapter
- Global Member @ OWASP Foundation
- Founding Board Member @ ISC2 El Djazair Chapter
- Global Member @ ISC2
- Cyber Security Instructor @ CETIC
- Cyber Security Instructor @ GOMYCODE
- Global CyberSecurity Advisor @ AlphaSights
- Cyber Security Ambassador @ Cyber Cohesion
- Independent Consultant & Instructor
- CISSP, Mini-MBA, CC, eCPPTv2, ISO27001, CEHv12, CCSP/AWS, CNPen, CAP, CNSP, CNSS, CPTAv2, C3SA, ACE/MCNA, QCS/VMDR, CCNA..

GOMYCODE

Introduction to Information and Cyber Security



Presented by: Taher Amine ELHOUARI - CISSP

What is Information Security?

- Information Security refers to the practice of protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction.
- It involves implementing measures to ensure the confidentiality, integrity, and availability of information, whether it is stored in digital or physical form.

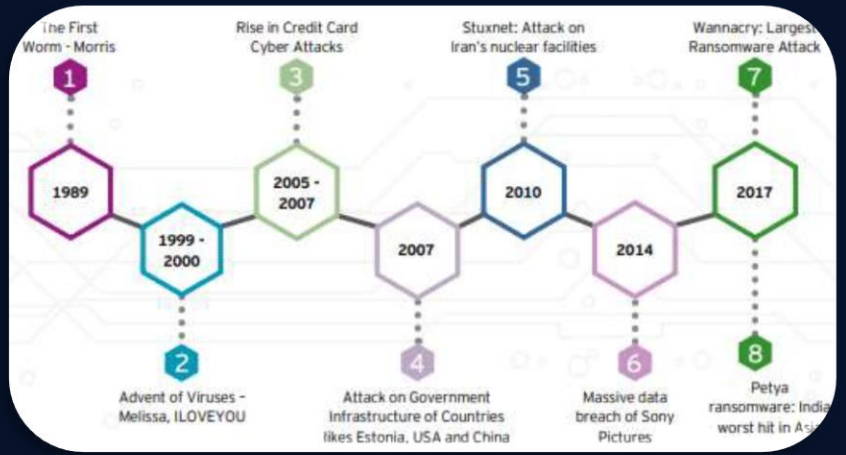
From CIA to CIAAN

- Authenticity
- Non-Repudiation

GOMYCODE
OWASP ALGIERS

What is Cyber Security?

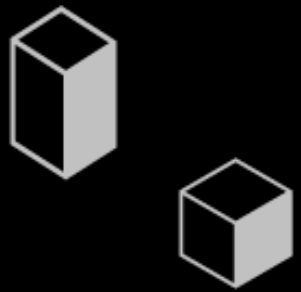
- CyberSecurity refers to the practice of protecting computer systems, networks, and data from digital attacks, unauthorized access, and other cyber threats.
- InfoSec focuses on protecting all forms of information, regardless of the medium, while CyberSec specifically deals with securing digital assets such as computer systems, networks, and data from cyber threats.



GOMYCODE
OWASP ALGIERS

GOMYCODE

Privacy & Data Protection



Presented by: Taher Amine ELHOUARI - CISSP

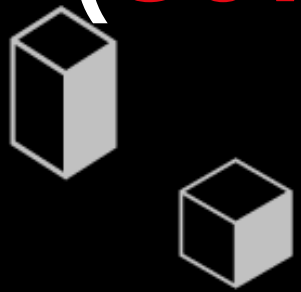
Privacy & Data Protection:

- Privacy and data protection involve safeguarding individuals' personal information from unauthorized access, use, disclosure, alteration, or destruction.

- It includes implementing measures to ensure that personal data is collected, processed, and stored in accordance with applicable laws and regulations, as well as respecting individuals' rights to control their own data.

GOMYCODE

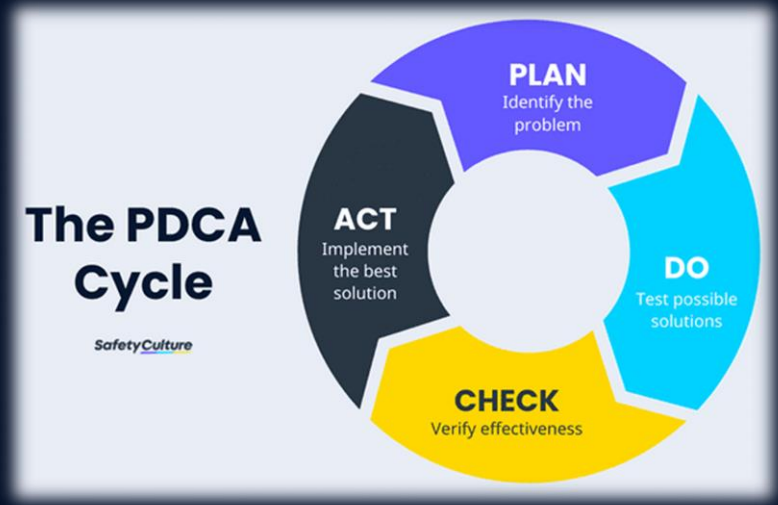
Introduction to GRC (Governance, Risk, Compliance)



Presented by: Taher Amine ELHOUARI - CISSP

What is GRC?

- GRC stands for Governance, Risk, and Compliance. It's a program that organizations use to manage and align their strategies, policies, and regulations to achieve business objectives while addressing risks and ensuring compliance with laws, regulations, and standards.



What is Governance?

- Governance refers to the overall management structure and processes within an organization. It involves defining roles, responsibilities, and decision-making processes to ensure that objectives are achieved efficiently and effectively.
- It focuses on establishing oversight mechanisms and accountability structures to ensure that the organization's activities align with its strategic goals and values.
- Governance frameworks often include elements such as corporate governance, IT governance, and data governance to ensure that resources are managed responsibly and ethically.

What is Risk Management?

- Risk management involves identifying, assessing, and mitigating risks that could impact the achievement of organizational objectives. Risks can arise from various sources, including strategic, operational, financial, and compliance-related factors.

- In the GRC framework, risk management aims to proactively identify and evaluate potential threats and vulnerabilities to the organization's assets, including data, systems, and processes.

- Risk management processes typically involve risk assessment, risk treatment, and risk monitoring to ensure that risks are effectively managed and controlled within acceptable levels.

What is Compliance?

- Compliance refers to the adherence to laws, regulations, standards, and internal policies relevant to the organization's operations and industry.
- In the GRC context, compliance activities focus on ensuring that the organization complies with applicable legal and regulatory requirements, as well as internal policies and standards.
- Compliance efforts typically involve conducting regular audits, assessments, and reviews to verify adherence to relevant requirements and to identify areas for improvement.
- Compliance with GRC standards helps organizations mitigate legal and regulatory risks, enhance trust and confidence among stakeholders, and promote a culture of integrity and accountability.

Standards, Laws, and Regulations:

- Standards are established guidelines or frameworks developed by recognized authorities or organizations to define best practices or requirements in specific areas. They provide guidance on how organizations can achieve certain objectives or meet specific criteria related to governance, risk management, and compliance.

- Laws are legal statutes enacted by legislative bodies, such as governments or regulatory agencies, that mandate specific behaviors or actions and may impose penalties for non-compliance. They are legally binding and enforceable, and organizations must comply with them to avoid legal consequences.

- Regulations are rules or requirements issued by government agencies or regulatory bodies to implement and enforce laws within specific industries or sectors. They provide detailed guidance on how organizations must comply with legal requirements and may include specific technical standards, reporting obligations, or procedural requirements.

Standards, Laws, and Regulations:

- Government agencies in different nations take different approaches to cybersecurity laws and regulations. The laws of different nations may be structured to result in very dissimilar styles of regulation.

- No country has the perfect solution to the challenge of how best to regulate cybersecurity—this is an area where learning from the variety of approaches around the world can be instructive.

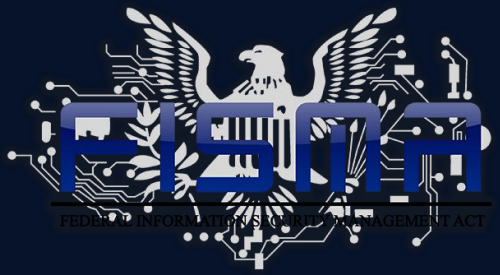
- The word "standards" actually has multiple meanings in the cybersecurity domain. Besides "best practice" standards (such as ISO/IEC 27000), there are "technical standards," such as IEEE 802.11, which defines wireless protocols used on Wi-Fi networks. A third meaning for "standards" refers to the rules that an organization might develop and enforce internally. (e.g., how often employees need to change their passwords.) All meanings are correct, and the intended meaning is usually apparent from the context (Harris and Maymi 2016).

Standards, Laws, and Regulations:

- In summary, standards are voluntary guidelines or frameworks, laws are legal statutes enacted by legislative bodies, and regulations are rules issued by regulatory agencies to implement and enforce laws.
- While organizations may voluntarily adopt standards to improve practices, compliance with laws and regulations is mandatory and carries legal implications for non-compliance.
- GRC programs aim to ensure that organizations effectively navigate and comply with relevant standards, laws, and regulations to manage risks and achieve their objectives.

Most Common Standards & Regulations:

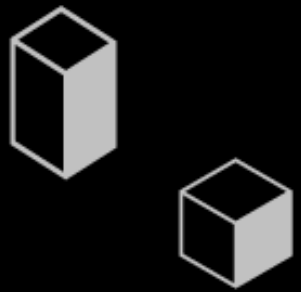
- Several standards, laws, and regulations are prominent in the realm of Governance, Risk, and Compliance (GRC). Here are some of the most famous ones:



GOMYCODE
OWASP ALGIERS

GOMYCODE

Intro to Blue Teams and Defensive Security



Presented by: Taher Amine ELHOUARI - CISSP

Overview of Blue Teams

- Blue Teams are an essential component of cybersecurity defense strategies, working proactively to protect organizations from cyber threats.
- To simplify they are the DEFENDERS!

Role of Blue Teams

- **Cybersecurity Defense:** Blue Teams are responsible for defending an organization's networks, systems, and data against cyber threats.
- **Proactive Security Measures:** Blue Teams focus on implementing proactive security measures to prevent cyber attacks before they occur.
- **Continuous Monitoring:** Blue Teams continuously monitor network traffic, system logs, and security alerts to detect and respond to potential security incidents in real-time.
- **Incident Response:** In the event of a security incident, Blue Teams are responsible for initiating and coordinating incident response efforts.
- **Collaboration with Red Teams:** Blue Teams often collaborate with Red Teams, which simulate cyber attacks to test the organization's defenses.

Function of Blue Teams

- **Threat Detection:** They proactively identify and assess potential security threats and vulnerabilities within the organization's infrastructure.
- **Incident Analysis:** They analyze security incidents to determine the cause, scope, and impact of the breach.
- **Incident Response:** They develop and execute incident response plans to contain and mitigate security incidents effectively. This involves coordinating with internal and external stakeholders.
- **Security Awareness:** They promote cybersecurity awareness and best practices among employees and stakeholders to help prevent security incidents.
- **Continuous Improvement:** Blue Teams continuously evaluate and improve the organization's security posture based on lessons learned from security incidents and emerging threat intelligence.

Security Operations Centers (SOC)

- A Security Operations Center (SOC) is a centralized unit within an organization responsible for monitoring, detecting, and responding to cybersecurity incidents.

Overview of Security Operations Centers (SOCs)

- **Centralized Unit:** A SOC serves as a centralized hub for cybersecurity operations within an organization. It typically consists of a team of security analysts, incident responders, and other professionals.
- **24/7 Monitoring:** SOCs operate around the clock, continuously monitoring the organization's networks, systems, and applications for signs of suspicious or malicious activity. This proactive monitoring approach enables the SOC to detect security incidents in real-time and respond promptly to mitigate the impact.
- **Detection and Analysis:** SOC analysts use a variety of tools and technologies, such as Security Information and Event Management (SIEM) systems, intrusion detection systems (IDS), and endpoint detection and response (EDR) solutions, to collect and analyze security event data from across the organization's infrastructure. They identify potential security threats, investigate alerts, and analyze security incidents to determine the cause, scope, and impact of the breach.

Overview of Security Operations Centers (SOCs)

- **Incident Response:** In the event of a security incident, the SOC is responsible for initiating and coordinating incident response efforts. SOC analysts work to contain the incident, mitigate the damage, and restore normal operations as quickly as possible.

- **Threat Intelligence Integration:** SOCs leverage threat intelligence feeds and information sharing platforms to enhance their threat detection capabilities.

- **Collaboration and Communication:** SOCs collaborate closely with other teams within the organization, including IT teams, network operations teams, and executive leadership, to ensure a coordinated and effective response to security incidents. They also communicate with external entities, such as law enforcement agencies, regulatory bodies, and third-party vendors, as necessary to address security incidents and comply with legal and regulatory requirements.

Computer Emergency Response Team (CERT)

- It is a specialized group within an organization or community/country that is responsible for coordinating and responding to cybersecurity incidents.
- CERTs serve as central hubs for cybersecurity incident management, bringing together a diverse range of experts, tools, and resources to effectively detect, analyze, and mitigate cyber threats.

GOMYCODE
OWASP ALGIERS

Overview of Computer Emergency Response Teams (CERTs)

- **Incident Coordination:** CERTs are tasked with overseeing the organization's response to cybersecurity incidents. This involves identifying and prioritizing incidents, mobilizing response teams, and coordinating efforts to contain and mitigate cyber attacks & breaches.
- **Threat Intelligence Gathering and Analysis:** CERTs collect and analyze threat intelligence from various sources, including internal security systems, external feeds, and industry reports.
- **Incident Response Planning:** CERTs develop and maintain incident response plans and procedures to ensure a coordinated and effective response to security incidents. These plans outline roles and responsibilities, communication protocols, escalation procedures, and mitigation strategies.

Overview of Computer Emergency Response Teams (CERTs)

- **Information Sharing and Collaboration:** CERTs facilitate information sharing and collaboration among internal and external stakeholders, including other CERTs, government agencies, industry partners, and academic institutions.

- **Cybersecurity Awareness and Education:** CERTs promote cybersecurity awareness and education initiatives to raise awareness among employees, stakeholders, and the general public. This includes providing training, developing awareness materials, and participating in community outreach activities.

Computer Security Incident Response Team (CSIRT)

- It is a specialized group within an organization, responsible for managing and responding to cybersecurity incidents. CSIRTs are tasked with detecting, analyzing, and mitigating security breaches, as well as coordinating incident response efforts to minimize the impact on organizational assets and operations.
- CSIRTs serve as frontline defenders against cyber threats, employing a combination of expertise, tools, and procedures to effectively manage security incidents.

GOMYCODE
OWASP ALGIERS

Overview of Computer Security Incident Response Team (CSIRTs)

- **Expertise and Specialization:** CSIRTs consist of cybersecurity professionals with specialized knowledge and skills in incident detection, response, forensics, and threat intelligence.
- **Incident Detection and Analysis:** CSIRTs monitor the organization's networks, systems, and applications for signs of security incidents.
- **Incident Response Coordination:** CSIRTs lead and coordinate incident response efforts to contain, mitigate, and remediate security incidents.

Overview of Computer Security Incident Response Team (CSIRTs)

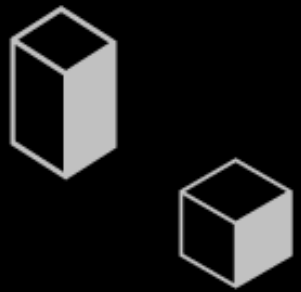
- **Forensic Analysis:** In the event of a security incident, CSIRTs conduct forensic analysis to investigate the cause, scope, and impact of the breach. They collect and analyze digital evidence, such as logs, files, and network traffic, to reconstruct the timeline of events and identify the attacker's tactics, techniques, and procedures (TTPs).

- **Post-Incident Review and Improvement:** After an incident has been resolved, CSIRTs conduct post-incident reviews to evaluate the organization's response effectiveness and identify areas for improvement. They document lessons learned, recommendations, and best practices for enhancing incident response procedures, security controls, and training programs.

- **Knowledge Management and Sharing:** CSIRTs maintain knowledge repositories and incident databases to capture and share information about security incidents, including incident reports, forensic findings, and remediation strategies.

GOMYCODE

Intro to Red Teams and Offensive Security



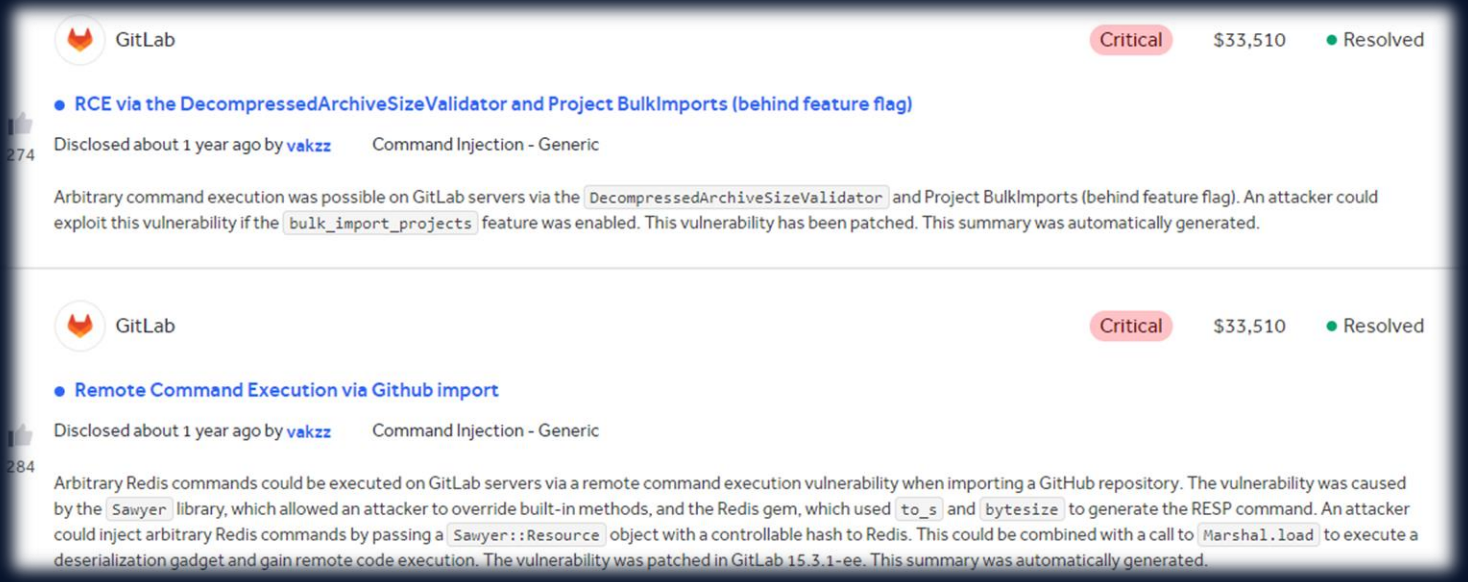
Presented by: Taher Amine ELHOUARI - CISSP

Introduction to Ethical Hacking

Ethical hacking is a proactive approach to cybersecurity, where skilled professionals, known as ethical hackers or white hat hackers, simulate cyberattacks to identify vulnerabilities within an organization's systems, networks, and applications.

Introduction to Bug Bounty Hunting

Bug bounty programs have gained popularity as a crowdsourced method for identifying and remediating security vulnerabilities.



GitLab — Critical — $33,510 — Resolved

- RCE via the DecompressedArchiveSizeValidator and Project BulkImports (behind feature flag)

274

Disclosed about 1 year ago by vakzz — Command Injection - Generic

Arbitrary command execution was possible on GitLab servers via the `DecompressedArchiveSizeValidator` and Project BulkImports (behind feature flag). An attacker could exploit this vulnerability if the `bulk_import_projects` feature was enabled. This vulnerability has been patched. This summary was automatically generated.

GitLab — Critical — $33,510 — Resolved

- Remote Command Execution via Github import

284

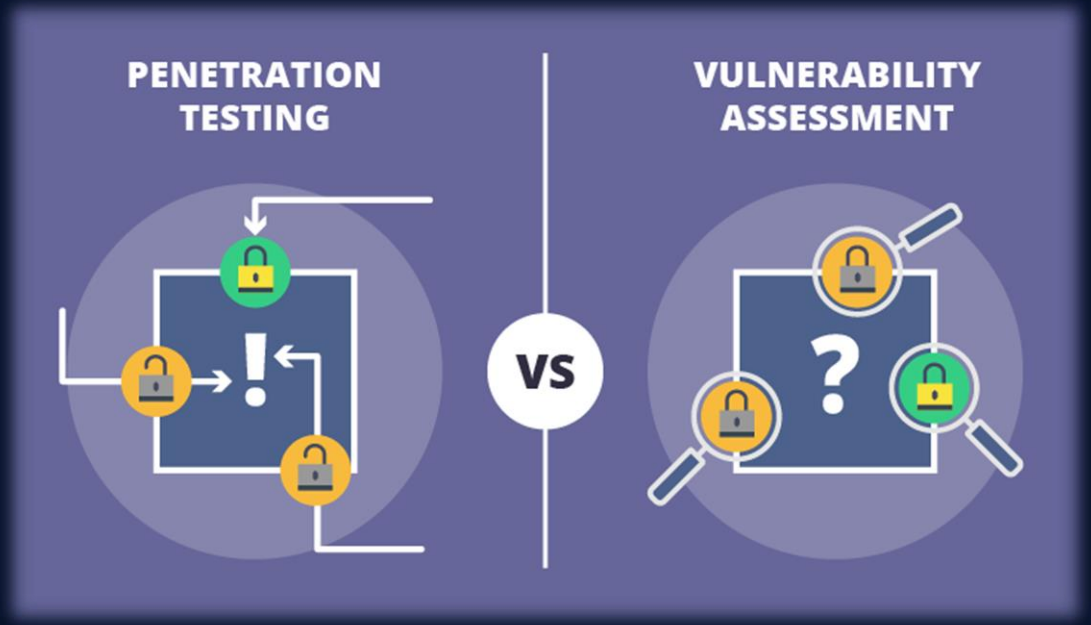
Disclosed about 1 year ago by vakzz — Command Injection - Generic

Arbitrary Redis commands could be executed on GitLab servers via a remote command execution vulnerability when importing a GitHub repository. The vulnerability was caused by the `Sawyer` library, which allowed an attacker to override built-in methods, and the Redis gem, which used `to_s` and `bytesize` to generate the RESP command. An attacker could inject arbitrary Redis commands by passing a `Sawyer::Resource` object with a controllable hash to Redis. This could be combined with a call to `Marshal.load` to execute a deserialization gadget and gain remote code execution. The vulnerability was patched in GitLab 15.3.1-ee. This summary was automatically generated.

GOMYCODE
OWASP ALGIERS

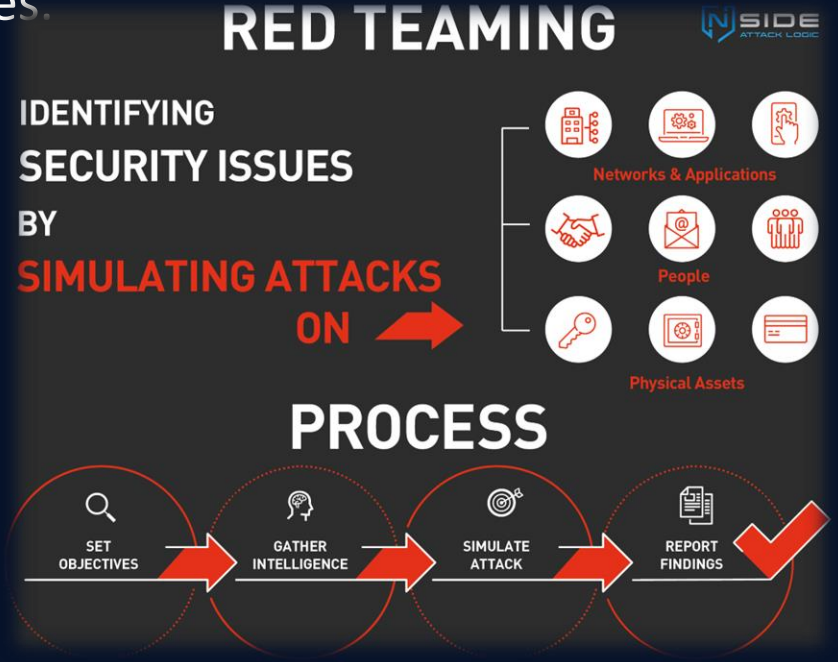
Introduction to Penetration Testing (VAPT)

Vulnerability Assessment and Penetration Testing (VAPT) is a systematic approach to evaluating and fortifying an organization's security posture.



Introduction to Red Teaming

Red teaming goes beyond traditional penetration testing by simulating sophisticated, multi-layered cyberattacks, akin to those launched by skilled adversaries.

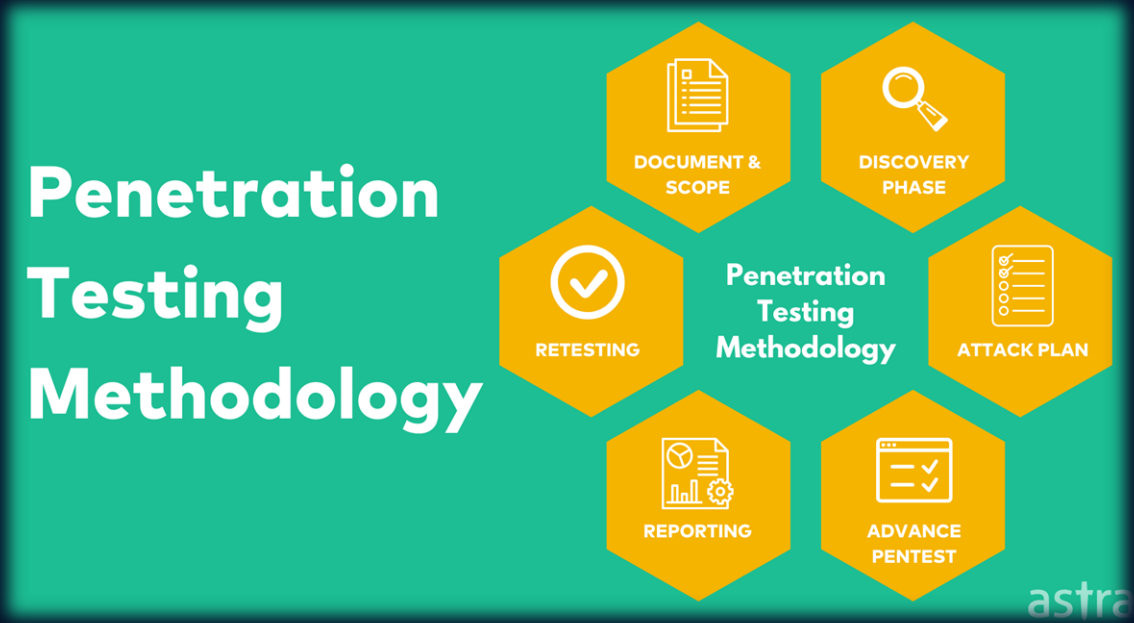


Ethical Hacking Methodology

Ethical hacking follows a structured methodology to maximize the efficiency and effectiveness of testing activities.

Penetration Testing Standards & Frameworks

Standardization is essential for ensuring consistency and repeatability in penetration testing engagements.



GOMYCODE
OWASP ALGIERS

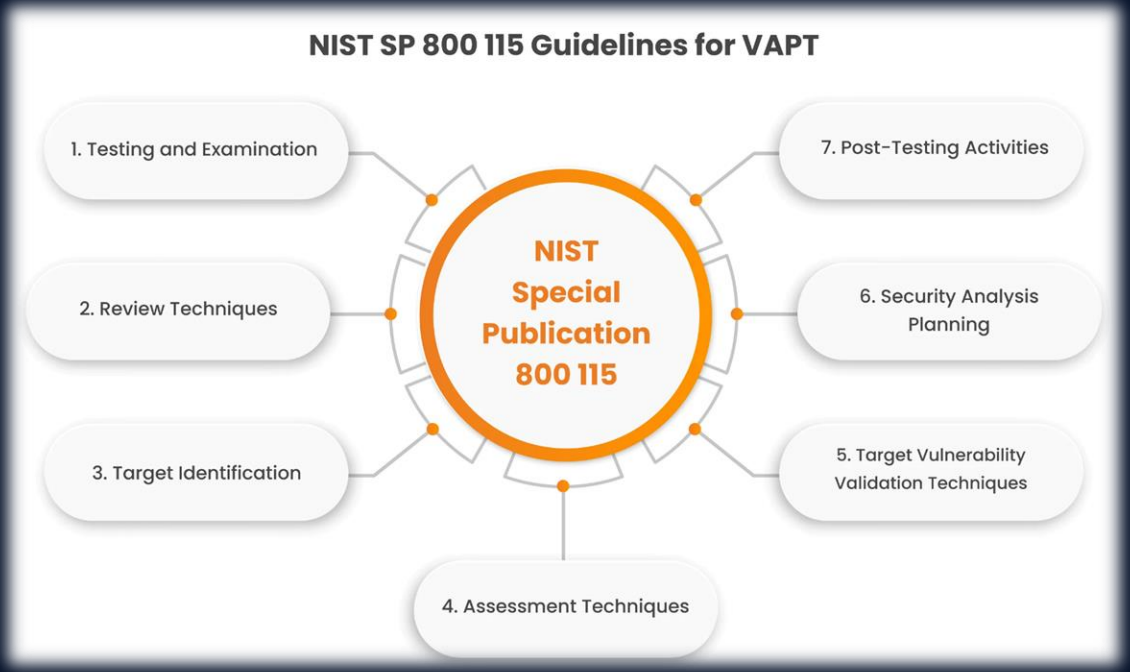
Penetration Testing Standards & Frameworks

PTES – Penetration Testing Execution Standard

1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post Exploitation
7. Reporting

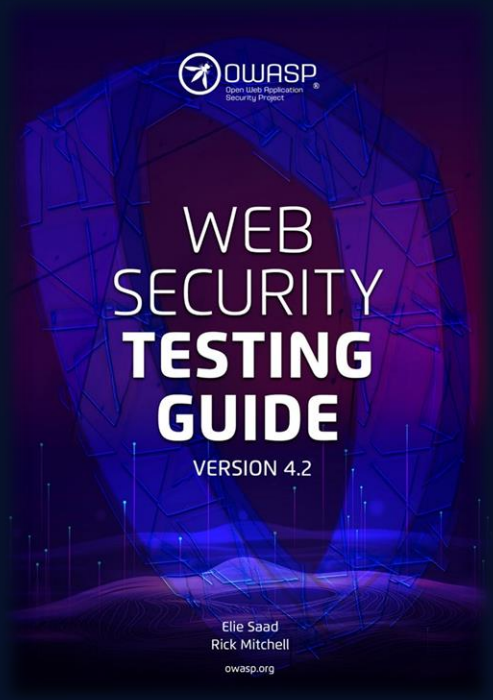
Penetration Testing Standards & Frameworks

NIST Special Publication 800-115



Penetration Testing Standards & Frameworks

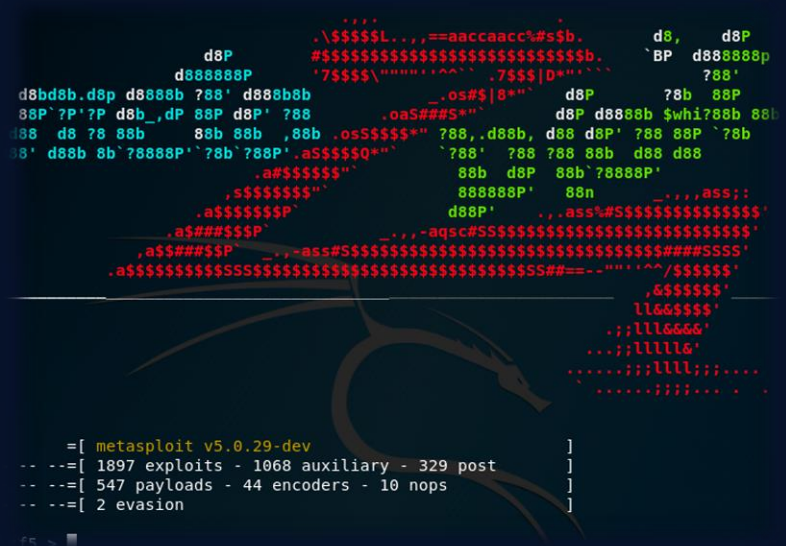
OWASP – Open Worldwide Application Security Project



GOMYCODE
OWASP ALGIERS

Penetration Testing – Most Known Tools

Penetration testers leverage a myriad of specialized tools and utilities to facilitate various stages of the testing process.



OWASP Zed Attack Proxy

GOMYCODE OWASP ALGIERS

Red Teaming Frameworks

Red teaming frameworks serve as strategic blueprints for orchestrating sophisticated cyberattacks that closely mimic real-world threats.

CBEST

Working alongside the UK central Bank, the Bank of England (BoE), CREST has developed a framework to deliver controlled, bespoke, intelligence-led cyber security tests that replicate behaviours of those threat actors, assessed by Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions. CBEST is the first of initiative of its type to be led by any of the world's central banks.

CBEST differs from other security testing currently undertaken by the financial services sector because it is threat intelligence based, is less constrained and focuses on the more sophisticated and persistent attacks against critical systems and essential services. The inclusion of specific cyber threat intelligence will ensure that that the tests replicate as closely as possible the evolving threat landscape and therefore will remain relevant and up to date.

CREST helped to develop the new accreditation standards for CBEST penetration testing, based on the already stringent standards for assessing the capabilities, policies and procedures that CREST member companies have to achieve. CBEST accredited professionals also need to demonstrate extremely high levels of technical knowledge, skill and competency.

iCAST — intelligence-led Cyber Attack Simulation Testing

iCAST is a framework introduced by the Hong Kong Monetary Authority ("HKMA") in response to the changing cybersecurity landscape. Under the **HKMA Cyber Resilience Assessment Framework**, banks which aim to attain the "**intermediate**" or "**advanced**" maturity level are required to conduct iCAST. Not only is it a regulatory requirement, intelligence led simulation testing uses real-world scenarios tailored to the target organisation which can demonstrate an organisation's cyber defence capability to the board, help to measure their maturity and stay ahead of the evolving threat landscape.

What is the driver?

Financial Services is an **increasingly desirable target** for well-funded threat actors. Sophisticated malware and botnets are threatening computer networks across a wide range of sectors, in particular the FS industry.

Skilled individuals are working in **organised groups and sharing their attack techniques**. There is therefore an increased need to gain intelligence on and share these techniques in the white-hat community in order to rapidly develop tests in response to their execution in the wild.

Other regulators have been using threat intelligence-led security testing (e.g. Bank of England CBEST) , recognising the systemic risk cyber presents to industry and their responsibilities to oversee its security and resilience.

What does it involve?

Project Planning Workshops: Conduct workshops with our cyber team to define the scope of the assessment, the targets, and attack scenarios.

Survey: Gather information on the organisation and information from our threat intelligence team which will help to tailor our attack platform to simulate real-world attacks.

Intrusion: Exploit vulnerabilities to gain unauthorised access to systems. Simulate actions of a real-world attacker: pivot to additional systems, maintain persistence, and avoid detection.

Assess Exposures: Analyse weaknesses in controls and clean up affected systems. Deliver interactive workshops to feedback results. Evidence gathered throughout the test will also be used to complete a security operations maturity assessment.

Project planning & scoping → Threat intelligence → APT scenario execution → Testing setup → Analysis and Reporting

What are the outputs?

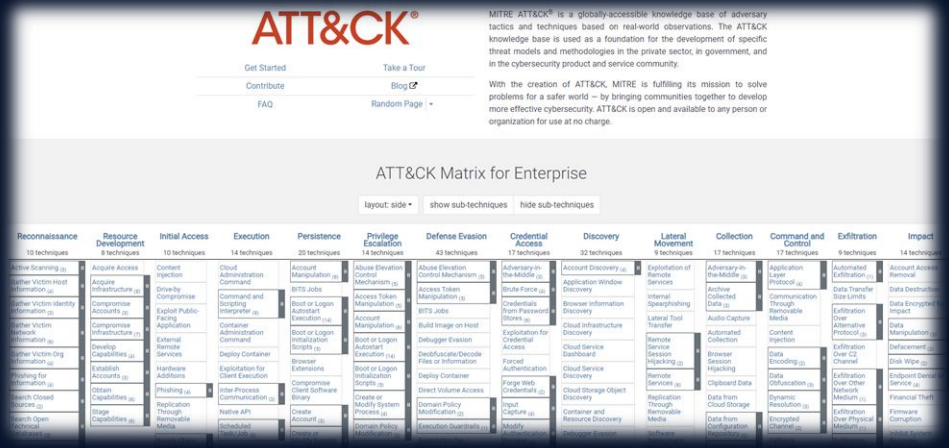
Threat intelligence report: Our threat intelligence report will provide an in-depth overview of the current threat landscape based on our research into the organisation's key lines of services, critical assets and ongoing business relationships. Technical details on specific threat actors and scenarios will also be provided.

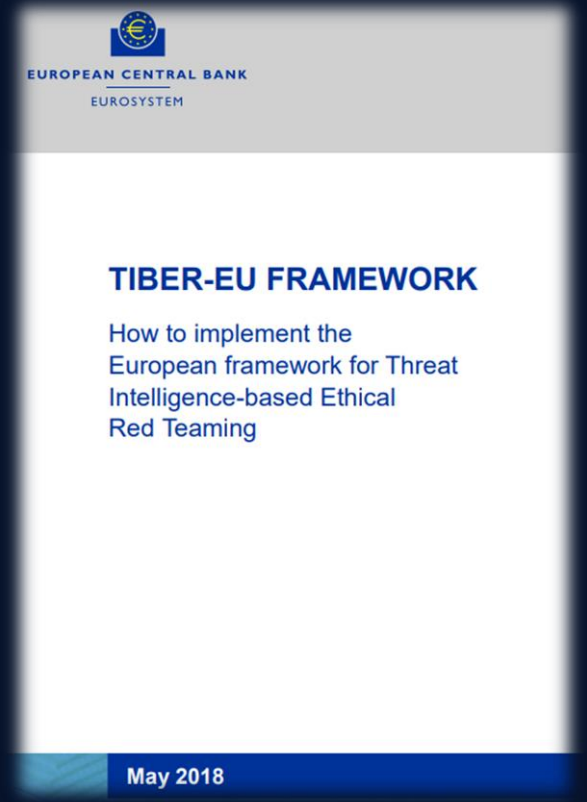
Security testing report: Our assessment report will provide technical descriptions of the issues found and the recommended risk prioritised remediation actions.

Detection and response assessment report: The detection and response assessment report will describe the overall maturity of the organisation's responses relative to the types of attack using our proprietary model. This will include high level commentary of observations made during the assessment.

GOMYCODE
OWASP ALGIERS

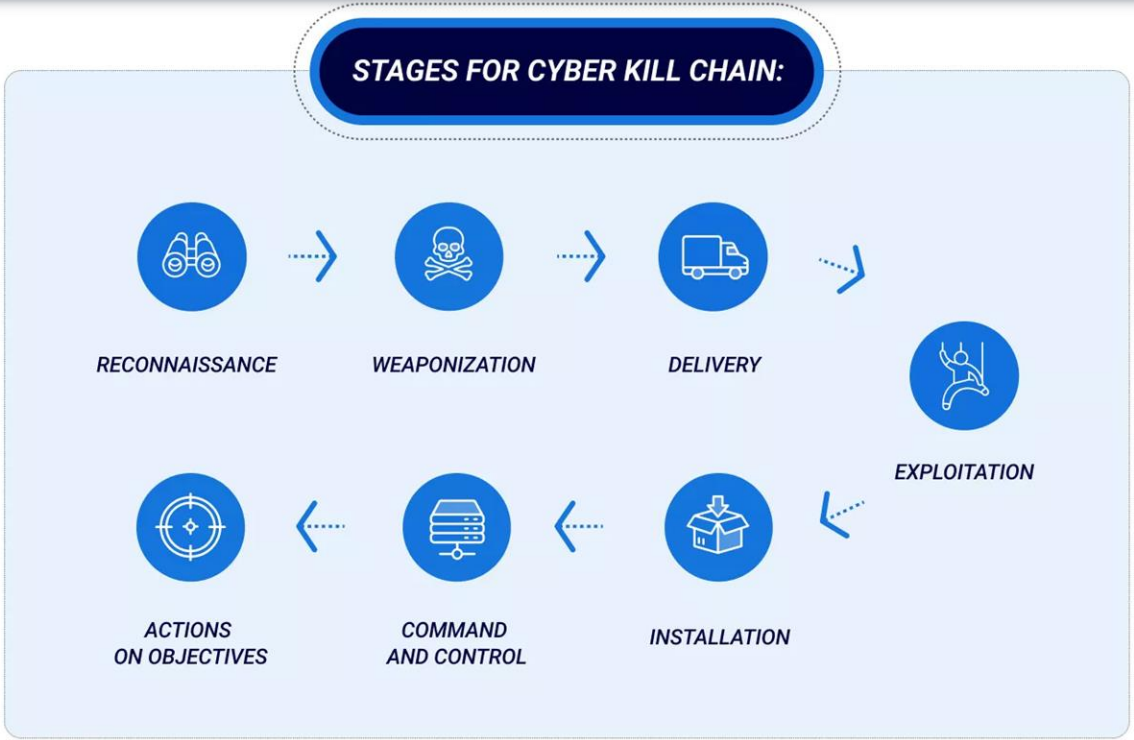
Red Teaming Frameworks





GOMYCODE
OWASP ALGIERS

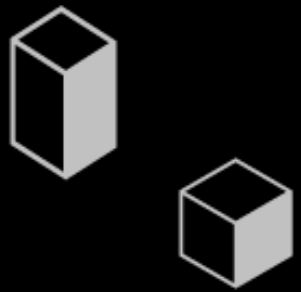
Red Teaming Frameworks



GOMYCODE
OWASP ALGIERS

GOMYCODE

Cyber Security Certifications



Presented by: Taher Amine ELHOUARI - CISSP

Most Common Certifications:

ISC2 - CISSP	• Certified Information Systems Security Professional	
ISACA - CISM	• Certified Information Security Manager	
ISACA - CISA	• Certified Information Systems Auditor	
ECCouncil - CEH	• Certified Ethical Hacker	
OffSec - OSCP	• Offensive Security Certified Professional	
CompTIA – S+	• Security+	

Other Certifications?

TCM SECURITY CERTIFIED
Practical Network Penetration Tester
PNPT

ISC2
CC SM

CCSP
Certified Cloud Security Professional
ISC2 Certification

CGEIT
Certified in the Governance of Enterprise IT
An ISACA® Certification

GIAC PENETRATION TESTER
GPEN

OFFENSIVE security
OSEP

OFFENSIVE security
OSCE3

C|PENT
Certified Penetration Testing Professional

eCPPT V2

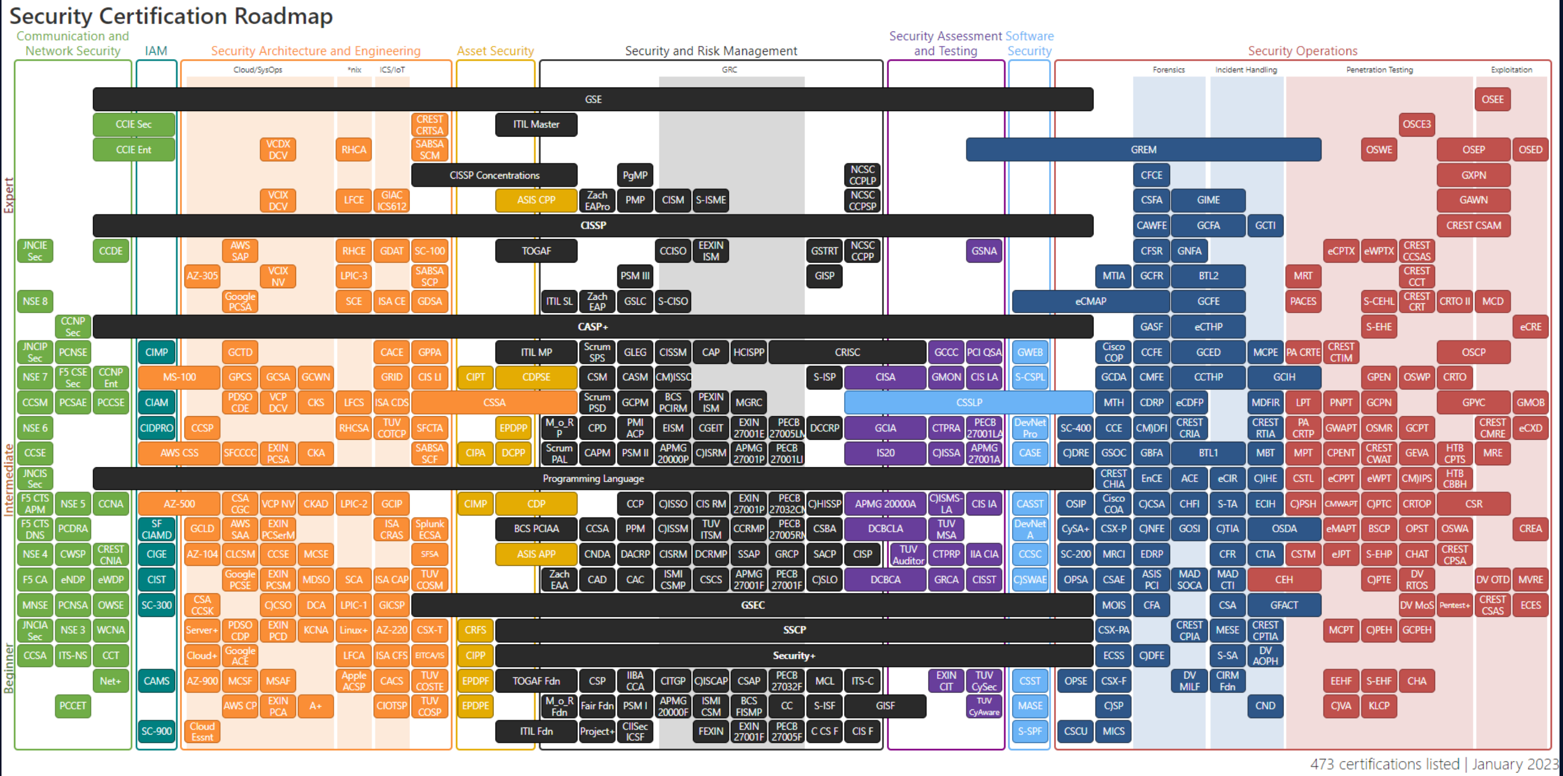
Red Team Specialist V2 [CRTS V2]

CERTIFIED RED TEAM PROFESSIONAL

Certified Red Team Operator
Zero-Point Security
Awarded Jan 14, 2021

GOMYCODE
OWASP ALGIERS

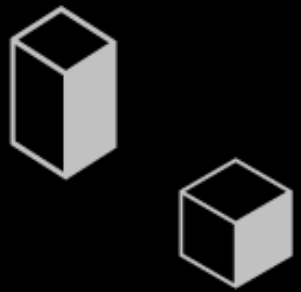
Other Certifications?



https://pauljerimy.com/security-certification-roadmap/

GOMYCODE

Networking in the Industry



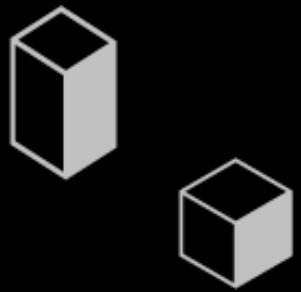
Presented by: Taher Amine ELHOUARI - CISSP

Networking:

- Networking in the cybersecurity industry is crucial for career advancement, staying updated with industry trends, and building professional relationships.
- Here are some tips on how to network effectively in the cybersecurity industry and the benefits it can bring:

GOMYCODE

Resources and Platforms to Practice



Presented by: Taher Amine ELHOUARI - CISSP

Practice:

WEBGOAT

DVWA

GOAD
GAME OF ACTIVE DIRECTORY

OverTheWire
We're hackers, and we are good-looking. We are the

HACKTHEBOX

Try Hack Me

VULNHUB
VULNERABLE BY DESIGN

PentesterLab

RootMe

HACK THIS SITE .ORG

CTF TIME

CyberDefenders
Defend Smarter, Not Harder

LetsDefend

PROXMOX

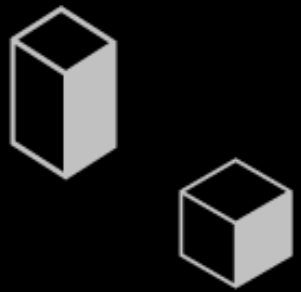
KALI LINUX

PARROT

GOMYCODE
OWASP ALGIERS

GOMYCODE

Project Ideas



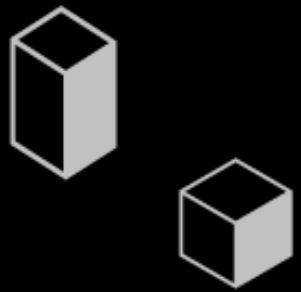
Presented by: Taher Amine ELHOUARI - CISSP

Examples:

- **Open Source Security Tool Development:** Contribute to the development of open-source security tools aimed at improving cybersecurity defenses, such as IDS, vulnerability scanners, CTI platforms, or secure coding frameworks.
- **Bug Bounty Program Participation or CVE Hunting:** Participate in bug bounty programs offered by companies and organizations to identify and responsibly disclose security vulnerabilities in their software, websites, or infrastructure.
- **Security Research Projects:** Conduct original research projects on emerging cybersecurity topics, threat trends, or innovative security solutions, and publish findings in academic journals, industry reports, or online platforms.
- **Community Security Events and Workshops:** Organize and host community security events, workshops, or conferences aimed at fostering collaboration, knowledge sharing, and skills development.

GOMYCODE

What about CompTIA Security+ ?



Presented by: Taher Amine ELHOUARI - CISSP

CompTIA Security+ (AKA: S+)

CompTIA Security+ is a global certification that validates the baseline skills necessary to perform core security functions and pursue an IT security career.

GOMYCODE
OWASP ALGIERS

CompTIA Security+ (AKA: S+)

- **Launch a successful cybersecurity career:** Develop a core foundation of essential skills, paving the way for a fulfilling career. More job roles use Security+ for baseline cybersecurity skills.
- **Assess on-the-job skills:** Security+ is the most widely adopted ISO/ANSI-accredited early career cybersecurity certification on the market with hands-on, performance-based questions on the certification exam.
- **Embrace the latest trends:** Understand and use the most recent advancements in cybersecurity technology, terms, techniques, and tools. By acquiring early career skills in the latest trends such as automation, zero trust, risk analysis, operational technology, and IoT..

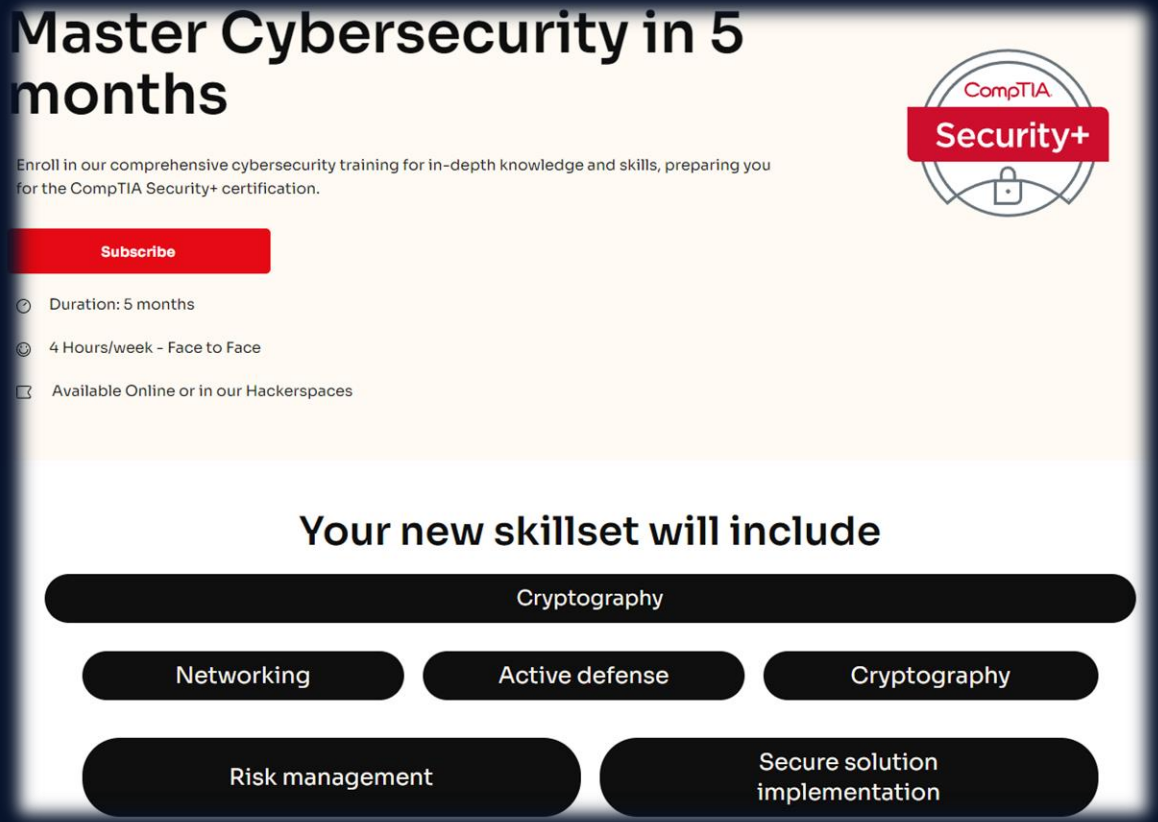
CompTIA Security+ | Skills you will Learn

- **General Security Concepts:** Includes key cybersecurity terminology and concepts up front to provide a foundation for security controls.
- **Threats, Vulnerabilities & Mitigations:** Focuses on responding to common threats, cyberattacks, vulnerabilities, and security incidents.
- **Security Architecture:** Includes security implications of different architecture models, principles of securing enterprise infrastructure.
- **Security Operations:** Includes applying and enhancing security and vulnerability management techniques.
- **Security Program Management & Oversight:** Updated to better reflect the reporting and communication skills required for Security+ job roles relating to governance, risk management, compliance, assessment, and security awareness.

CompTIA Security+ | Exam

- **Version:** SY0-701 (Launch Date: 7 November 2023).
- **Description:** It will verify the successful candidate has the knowledge and skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents.
- **Number of Questions:** Maximum of 90 Questions.
- **Type of Questions:** MCQ & Performance Based.
- **Exam Time:** 90 Minutes.
- **Passing Score:** 750 (on a scale of 100-900).
- **Exam Location:** Online Test or Onsite (PearsonVUE Centers).

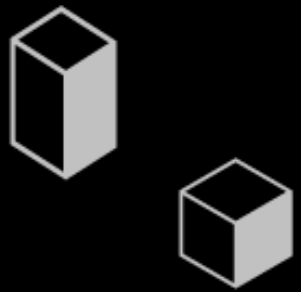
CompTIA Security+ | GOMYCODE



GOMYCODE
OWASP ALGIERS

GOMYCODE

IT Security
Careers & RoadMap

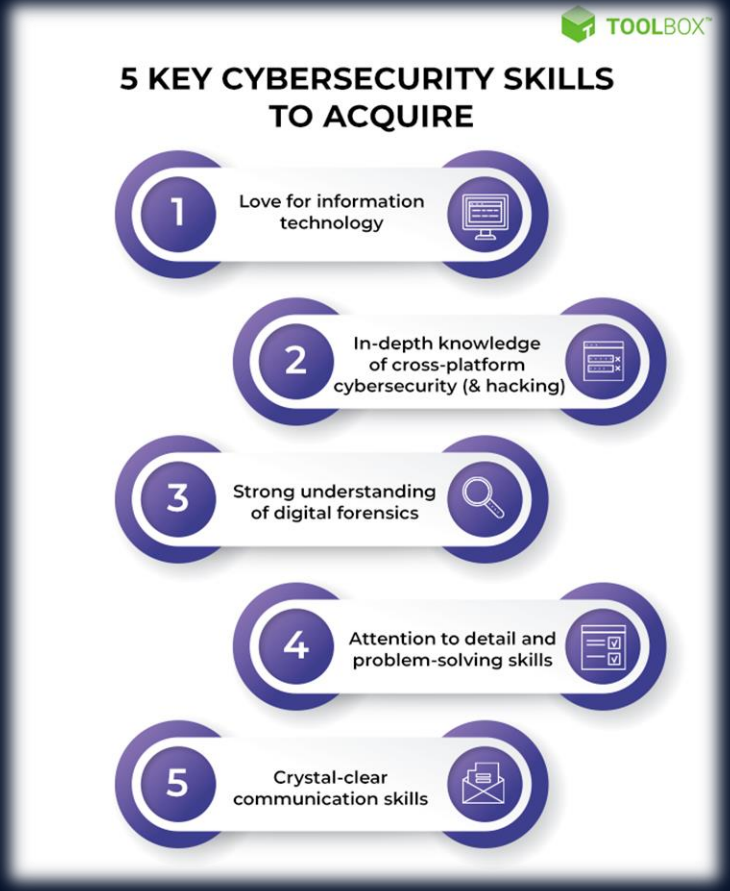


Presented by: Taher Amine ELHOUARI - CISSP

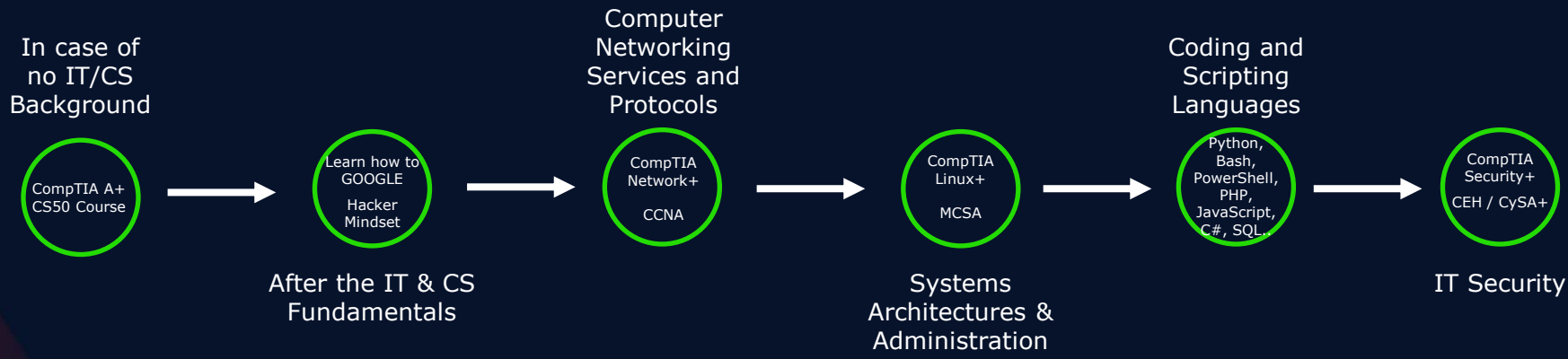
Career Options in IT Security:

Offensive Security	Defensive Security	GRC & Management
Red Team Operator	Threat Hunter	CISO / VP of Security
Offensive Sec Specialist	DFIR Specialist	IT Security Director
Penetration Tester	CERT/CSIRT Operator	IT Security Manager
Vulnerability Assessor	SOC Analyst	IT Security Auditor
Ethical Hacker	IT Security Engineer	IT Security Risk Analyst

Extra:

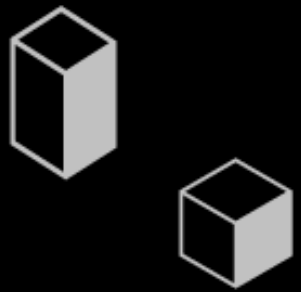


IT Security: Zero to Hero



GOMYCODE

SURPRISE!!



Presented by: Taher Amine ELHOUARI - CISSP

ISC2 CC – OWASP Algiers

Free Training + Free Exam Voucher

GOMYCODE

Thank you