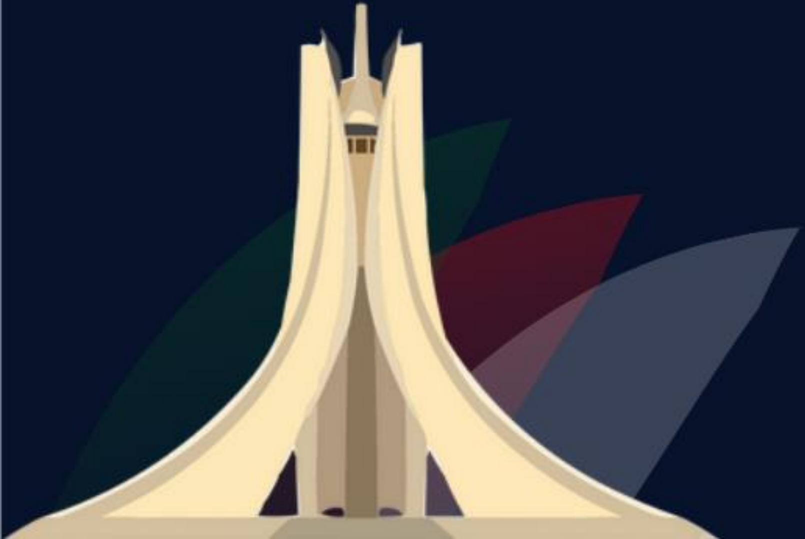
OWASP ALGiERS



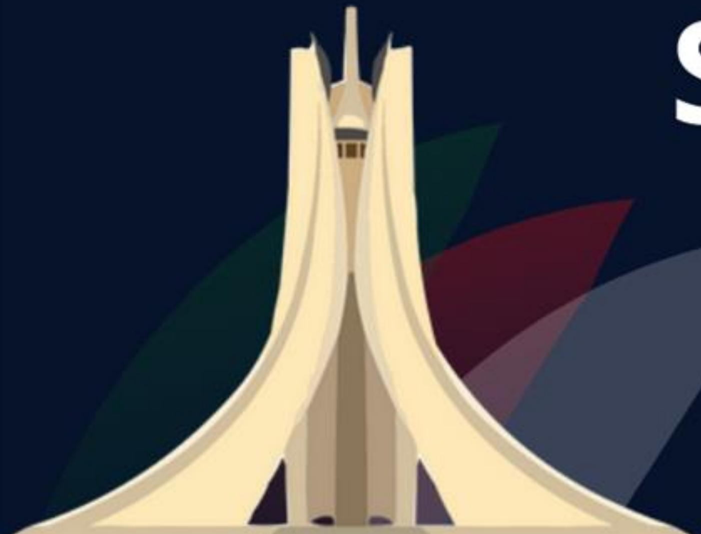
Ethical Hacking

Navigating the World of White Hat Security Testing

SUMMARY

- Introduction to Ethical Hacking
- Introduction to Bug Bounty Hunting
- Introduction to Penetration Testing (VAPT)
- Introduction to Red Teaming
- Penetration Testing Standards
- Ethical Hacking Methodology
- Penetration Testing Most Known Tools
- Red Teaming Frameworks
- Reporting
- SURPRISE!!

OWASP ALGiERS



SPEAKER

Taher Amine ELHOUARI

CyberSecurity Leader & Global Consultant

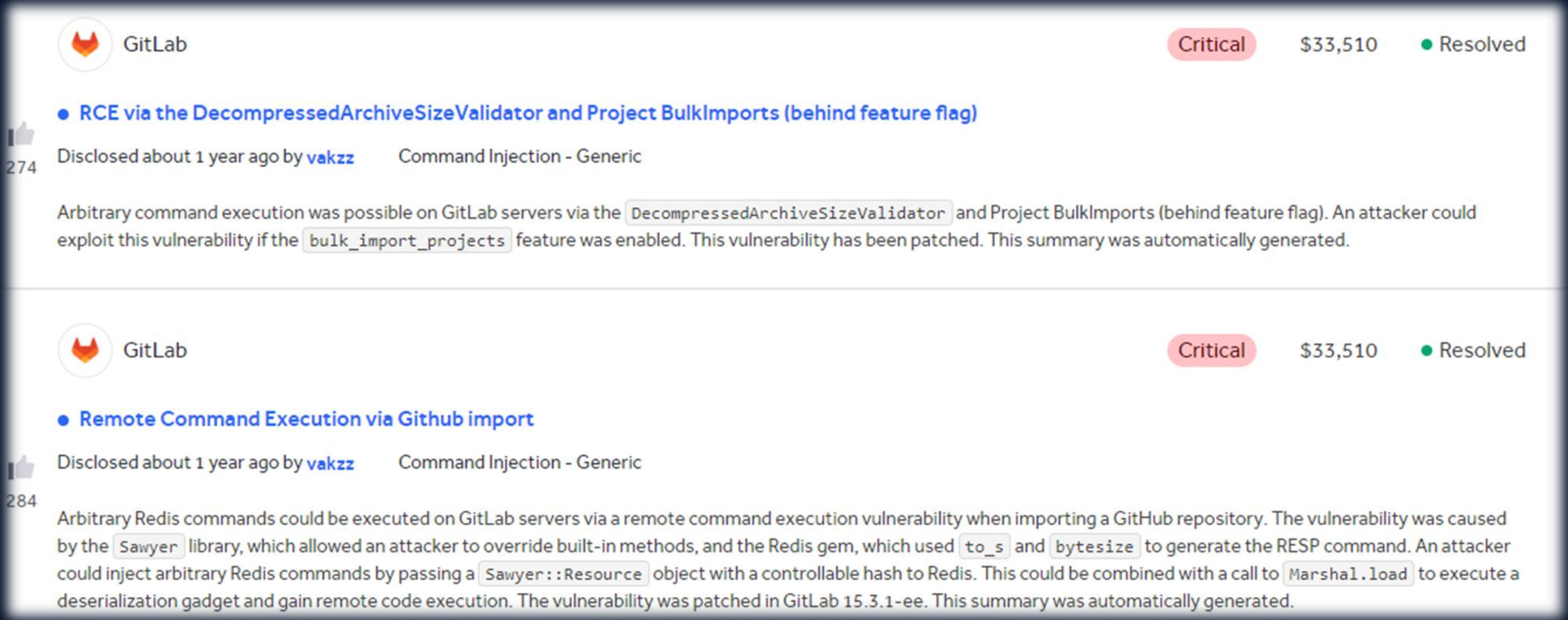
- Founder & President @ OWASP Algiers Chapter
- Global Member @ OWASP Foundation
- Founding Board Member @ ISC2 ElDjazair Chapter
- Global Member @ ISC2
- CyberSecurity Instructor @ GoMyCode
- Global CyberSecurity Advisor @ AlphaSights
- CyberSecurity Ambassador @ Cyber Cohesion
- Independent Consultant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

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

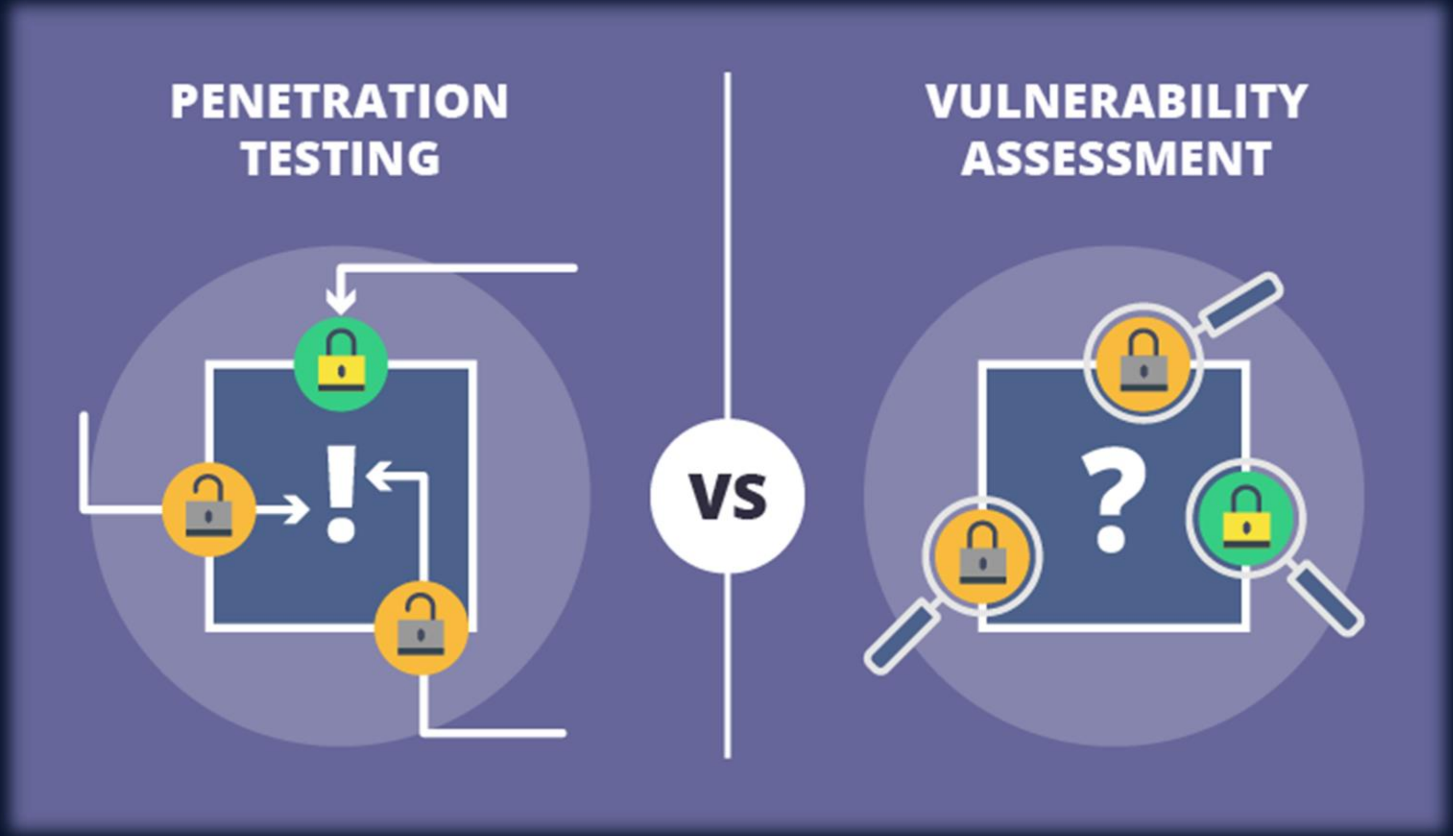
284

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.

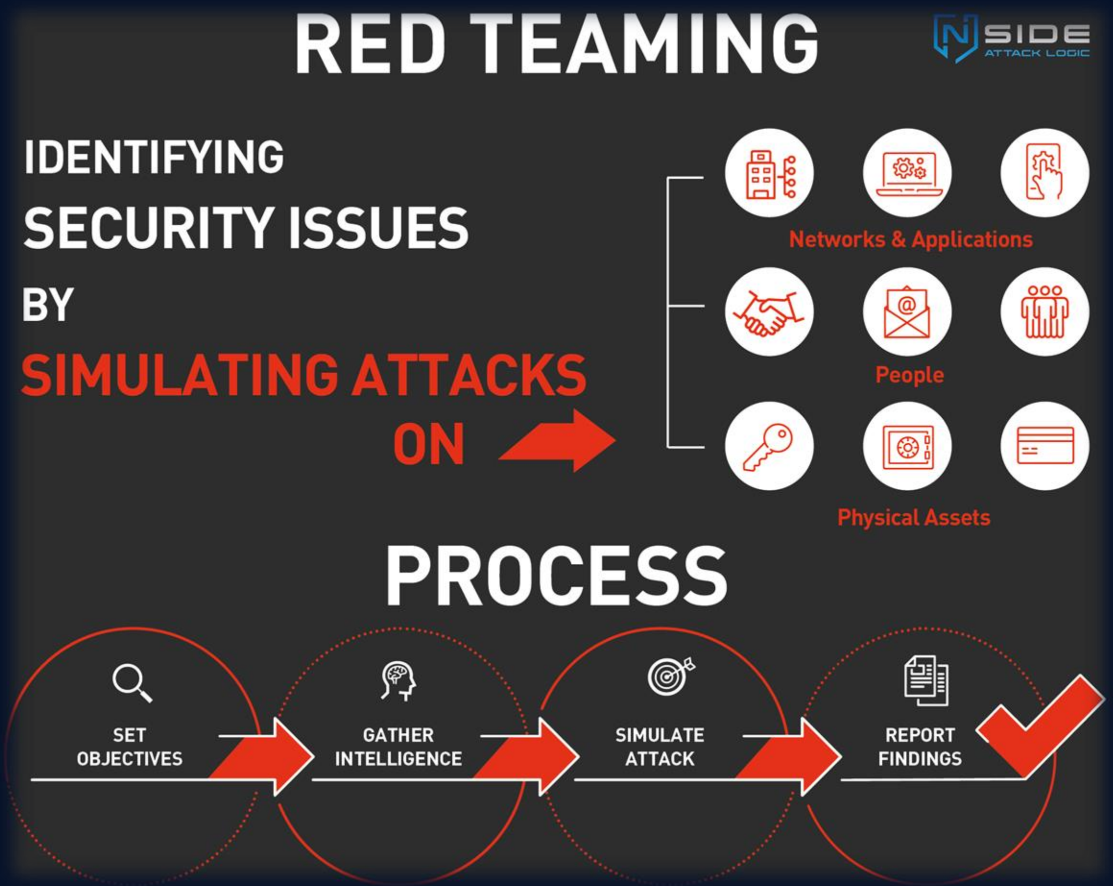
Introduction to Penetration Testing (VAPT)

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



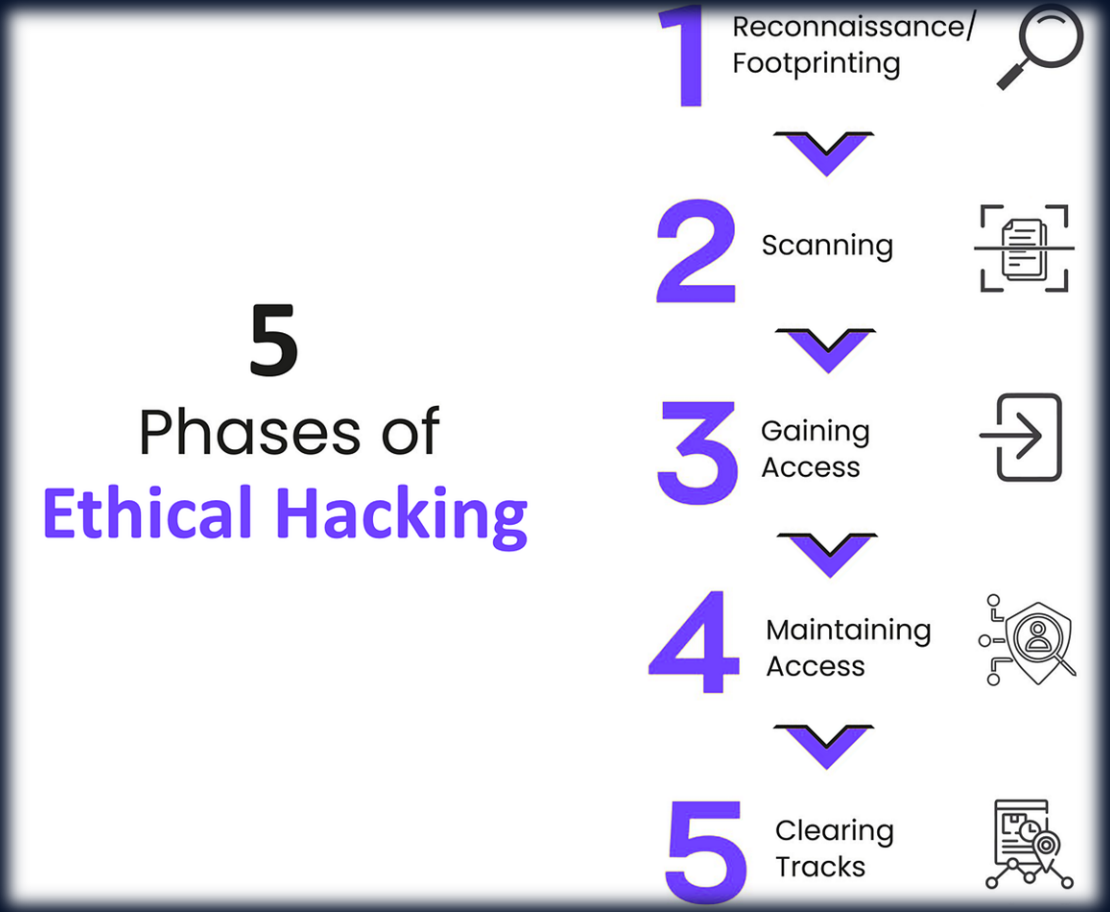
Introduction to Red Teaming

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.



5 Phases of **Ethical Hacking**

1 Reconnaissance/ Footprinting

2 Scanning

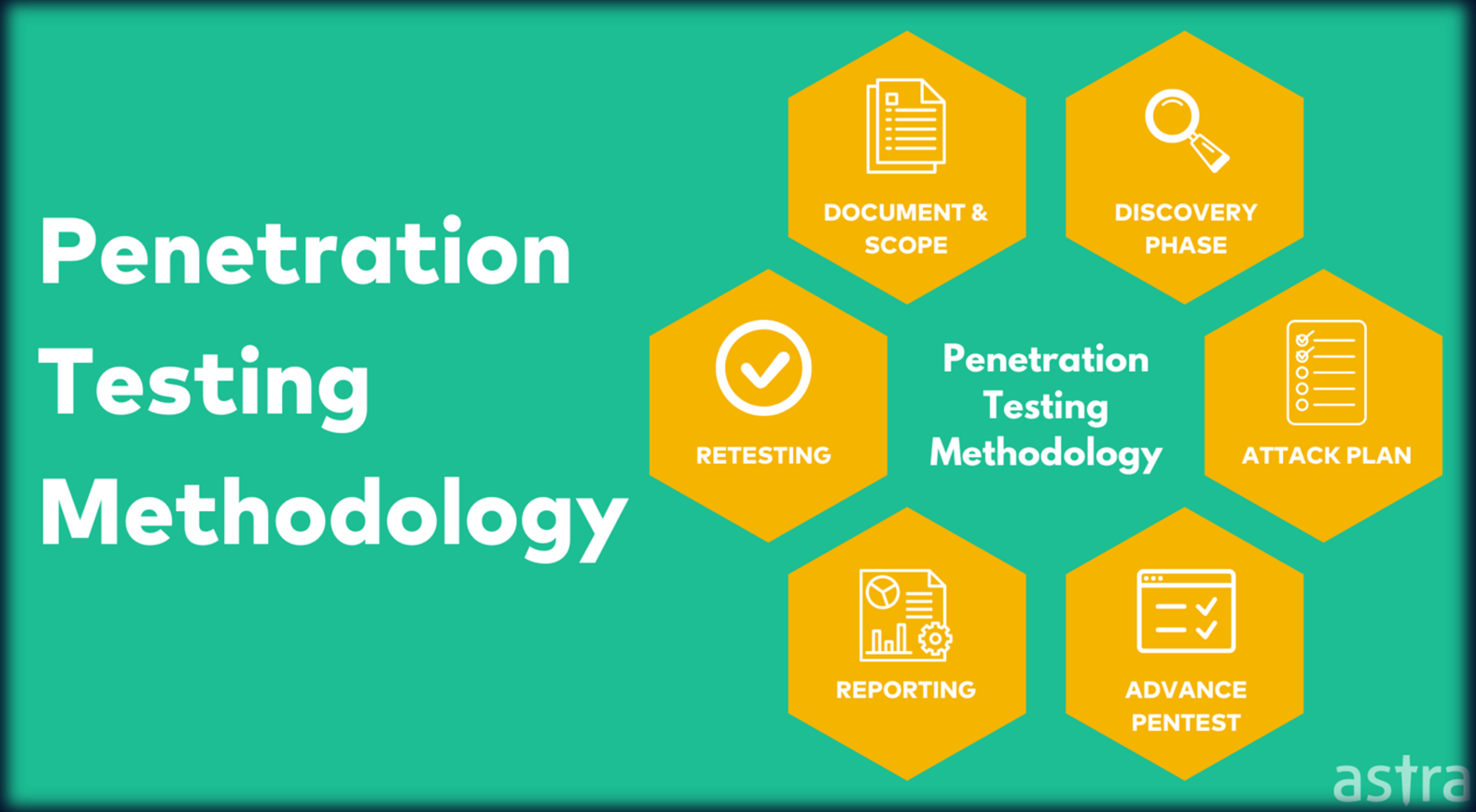
3 Gaining Access

4 Maintaining Access

5 Clearing Tracks

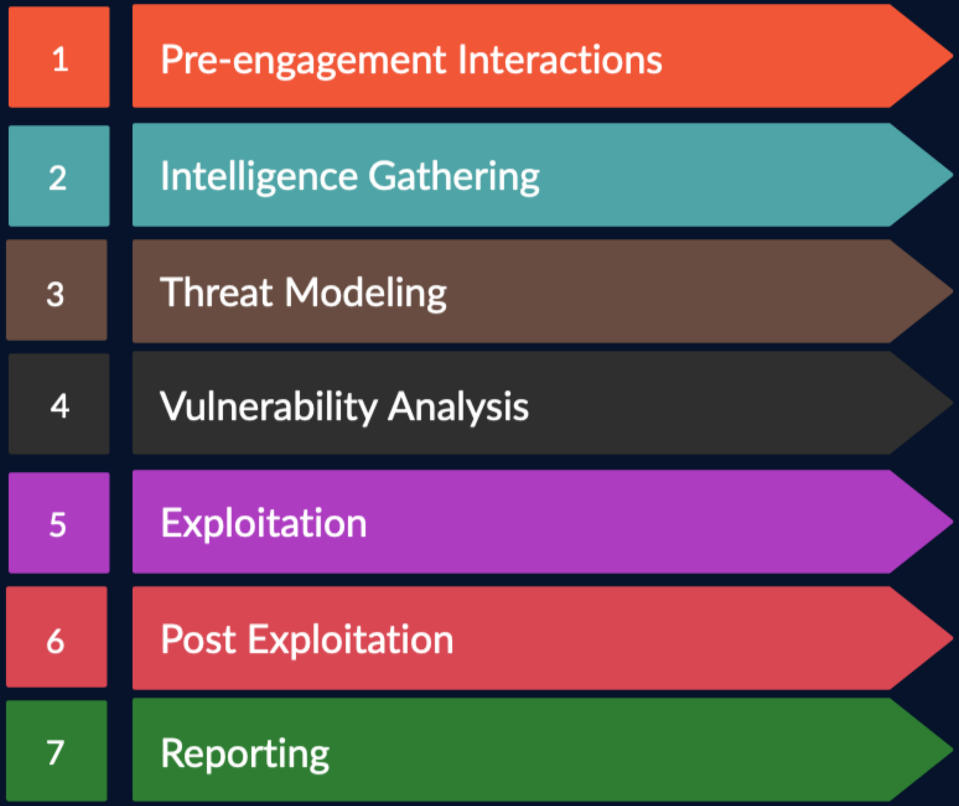
Penetration Testing Standards & Frameworks

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



Penetration Testing Standards & Frameworks

PTES – Penetration Testing Execution Standard



1 Pre-engagement Interactions

2 Intelligence Gathering

3 Threat Modeling

4 Vulnerability Analysis

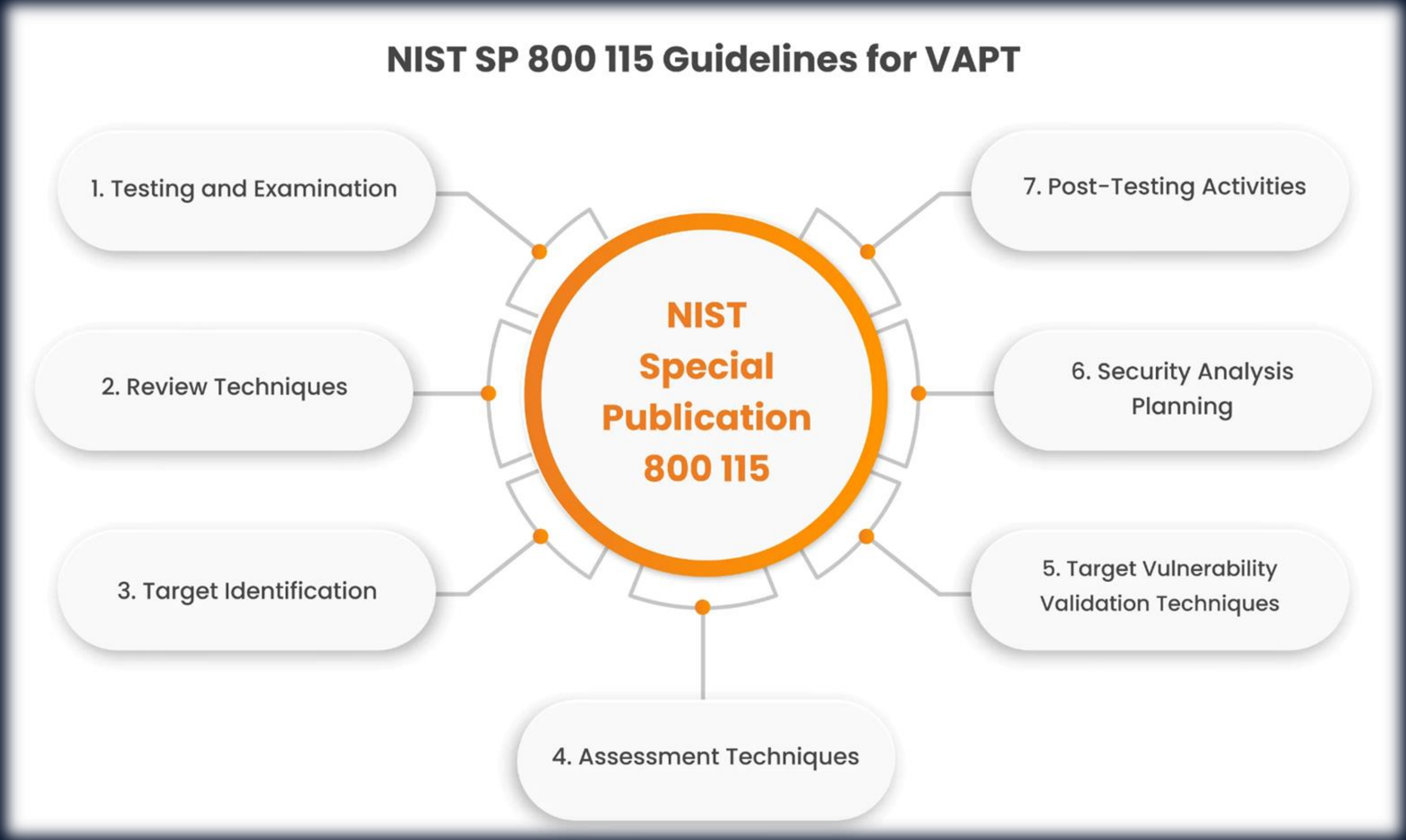
5 Exploitation

6 Post Exploitation

7 Reporting

Penetration Testing Standards & Frameworks

NIST Special Publication 800-115



NIST SP 800 115 Guidelines for VAPT

NIST Special Publication 800 115
1. Testing and Examination
2. Review Techniques
3. Target Identification
4. Assessment Techniques
5. Target Vulnerability Validation Techniques
6. Security Analysis Planning
7. Post-Testing Activities

Penetration Testing Standards & Frameworks

OWASP – Open Worldwide Application Security Project

MASTG

Mobile Application Security Testing Guide

Sven Schleier
Bernhard Mueller

Carlos Holguera
Jeroen Willemsen

OWASP

ISTG

IoT Security Testing Guide

Luca Pascal Rotsch
Aaron Guzman

OWASP

OWASP
Open Web Application Security Project

WEB SECURITY **TESTING GUIDE**

VERSION 4.2

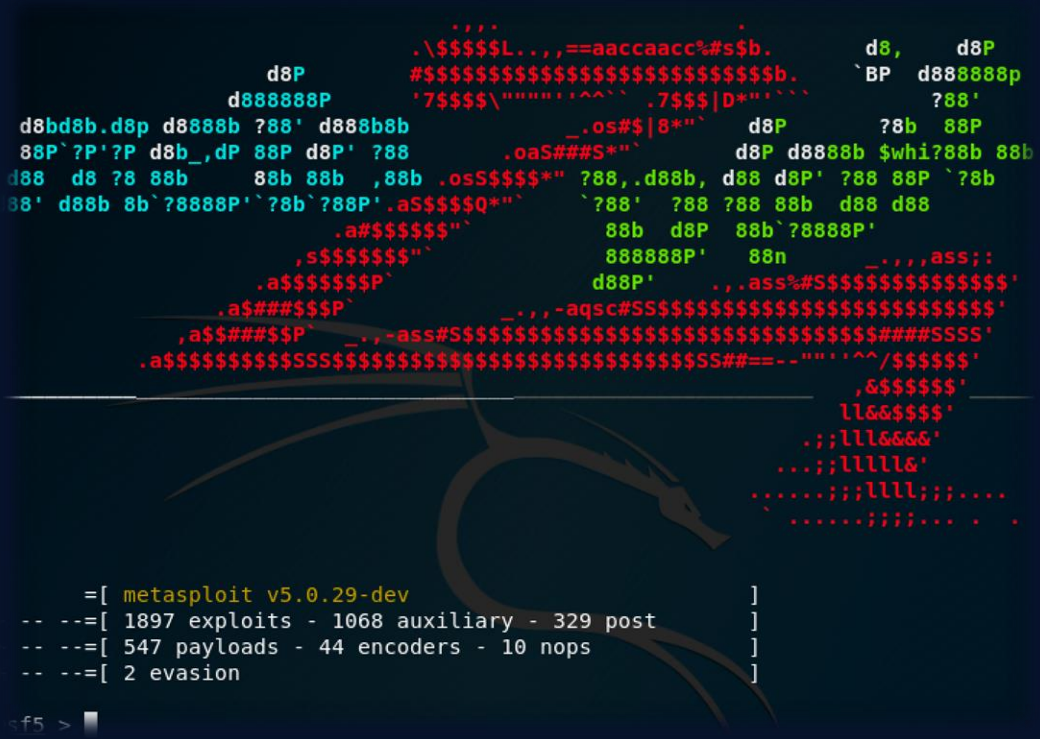
Elie Saad
Rick Mitchell

owasp.org

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.

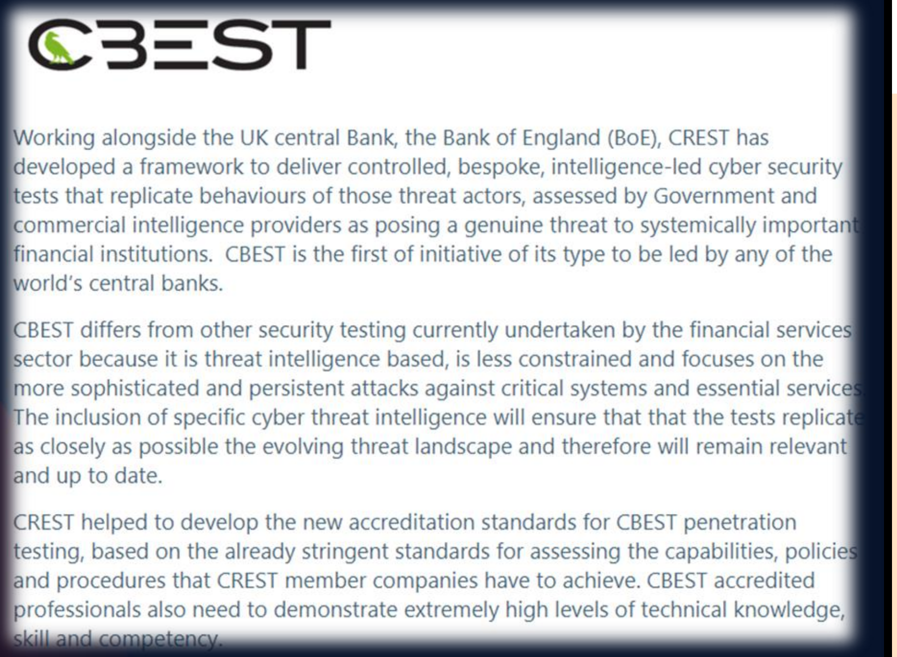


```
       =[ metasploit v5.0.29-dev                          ]
+ -- --=[ 1897 exploits - 1068 auxiliary - 329 post       ]
+ -- --=[ 547 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 > 
```

Red Teaming Frameworks

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

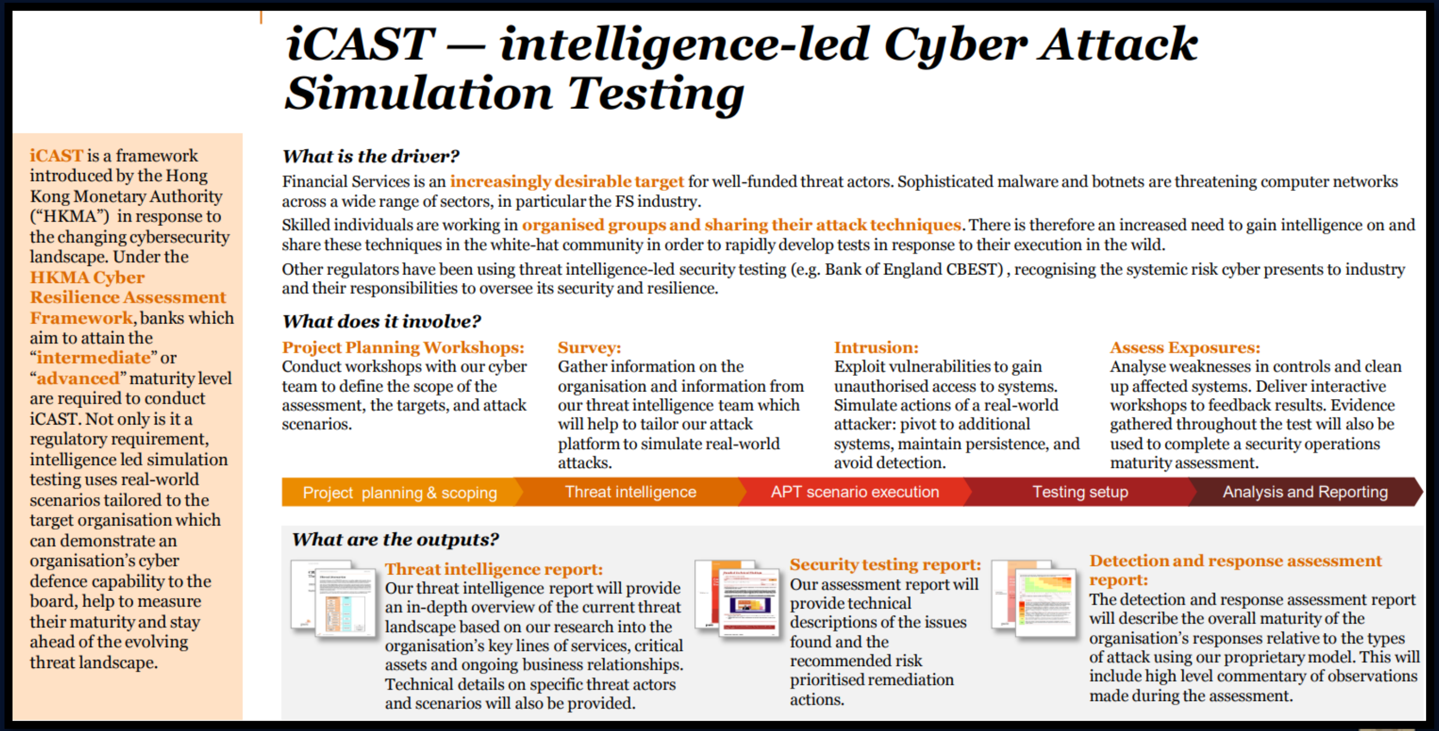


CBEST

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

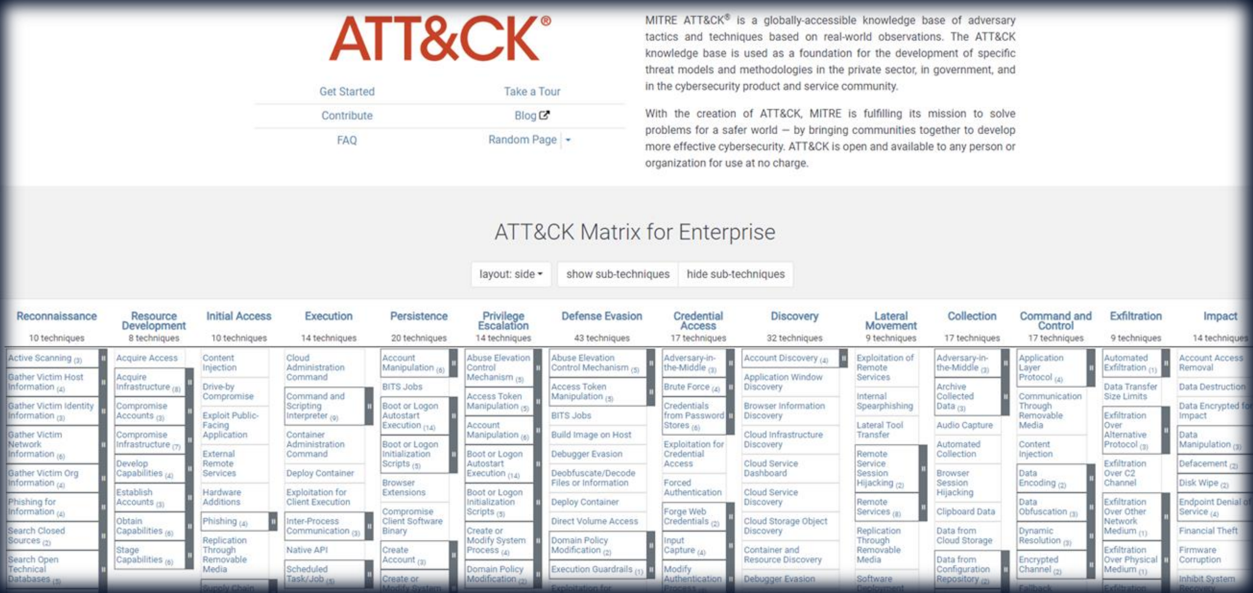
What are the outputs?

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.

Red Teaming Frameworks



ATT&CK®

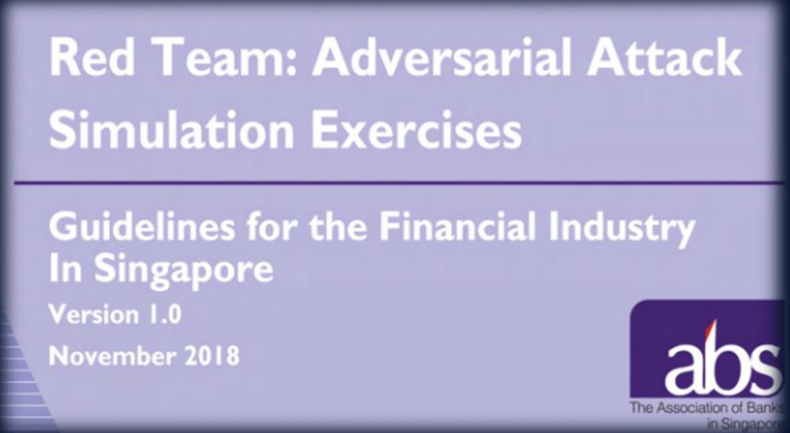
MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (5)	Abuse Elevation Control Mechanism (5)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Client Software Binary	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain	Scheduled Task/Job (5)	Create or Modify System		Direct Volume Access
						Domain Policy Modification (2)
						Execution Guardrails (1)
						Exploitation for

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Input Capture (4)	Cloud Storage Object Discovery	Software Deployment	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration	Endpoint Denial of Service (4)
Modify Authentication Process	Container and Resource Discovery		Data from Configuration Repository (2)	Fallback		Financial Theft
	Debugger Evasion					Firmware Corruption
						Inhibit System Recovery



Red Team: Adversarial Attack Simulation Exercises

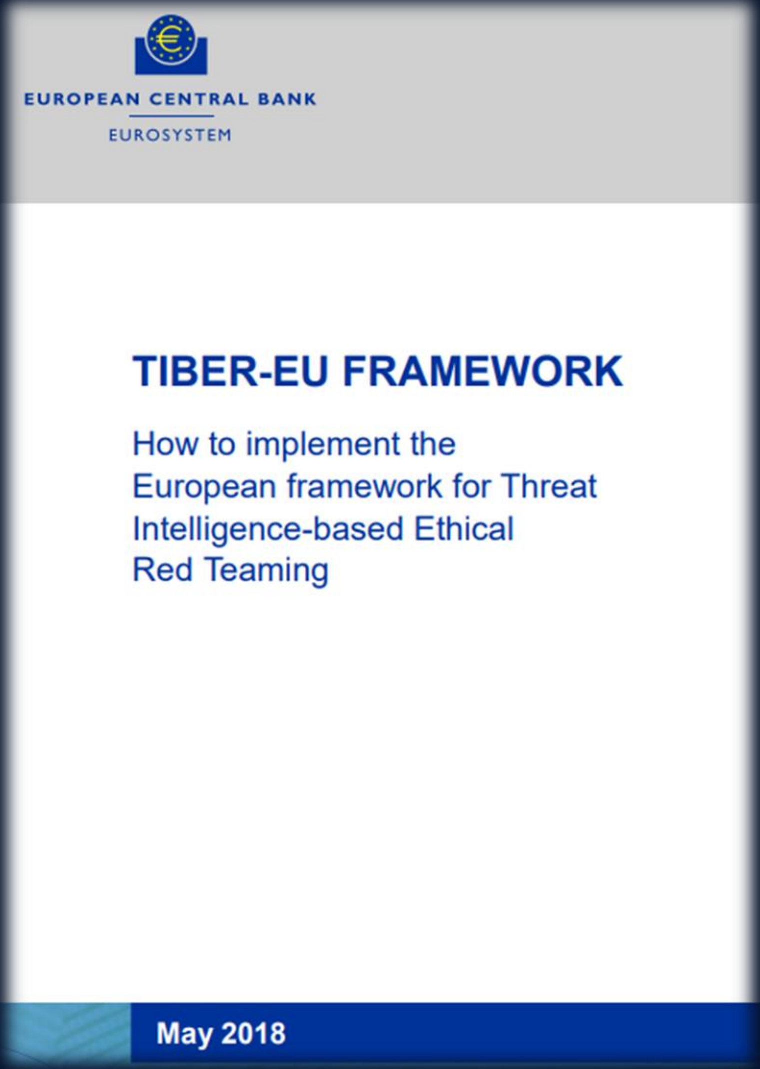
Guidelines for the Financial Industry In Singapore

Version 1.0

November 2018

abs

The Association of Banks in Singapore



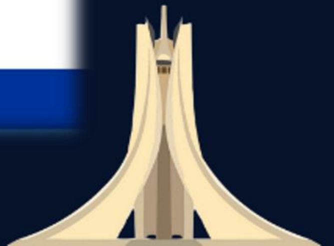
EUROPEAN CENTRAL BANK

EUROSYSTEM

TIBER-EU FRAMEWORK

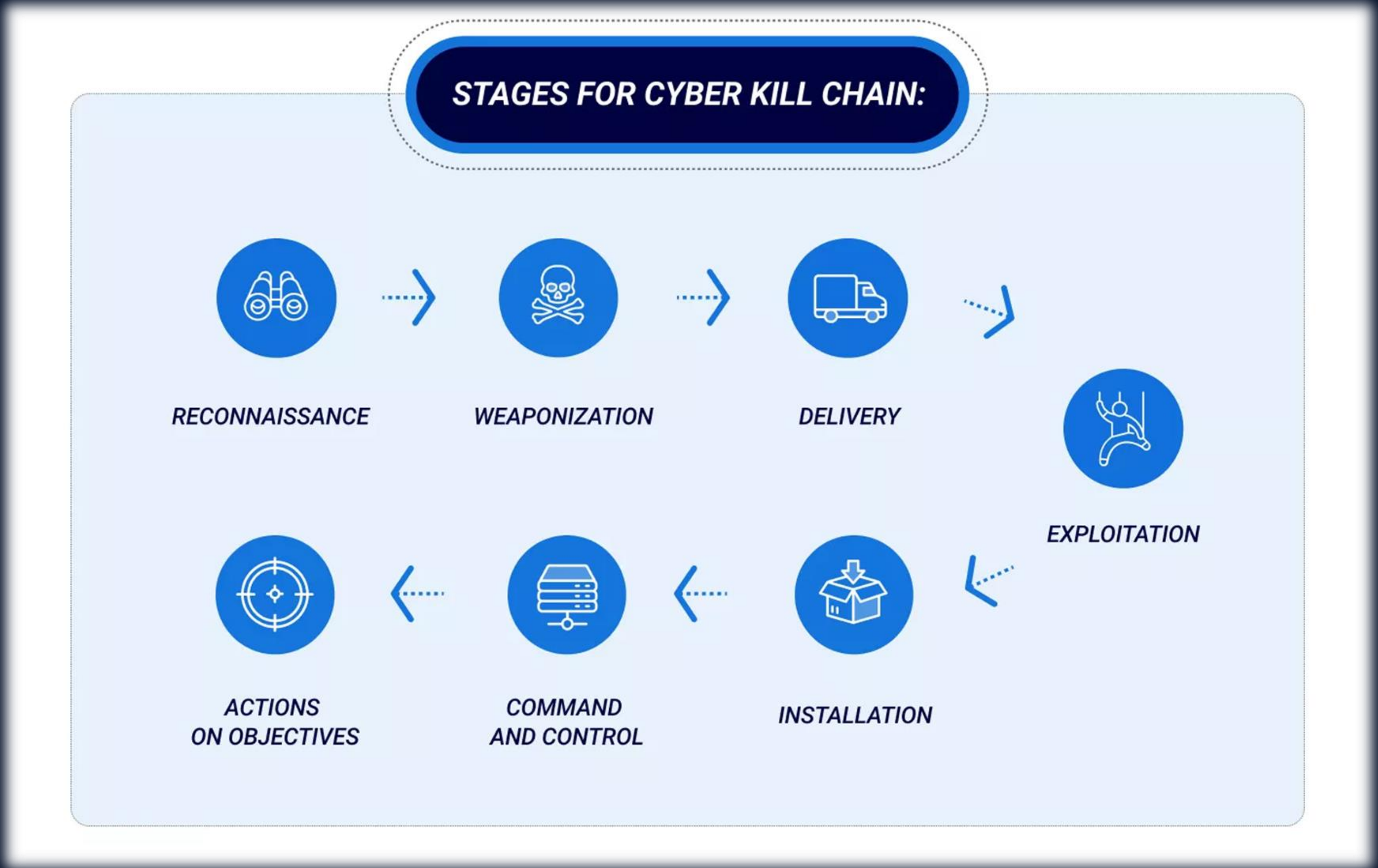
How to implement the European framework for Threat Intelligence-based Ethical Red Teaming

May 2018



OWASP ALGIERS

Red Teaming Frameworks



STAGES FOR CYBER KILL CHAIN:

RECONNAISSANCE

WEAPONIZATION

DELIVERY

EXPLOITATION

INSTALLATION

COMMAND AND CONTROL

ACTIONS ON OBJECTIVES

Reporting

Effective reporting is the cornerstone of any ethical hacking or penetration testing engagement.

SURPRISE!!

OWASP ALGIERS

Contact us

ALGIERS-LEADERS@OWASP.ORG

https://owasp.org/www-chapter-algiers/