

THE DEVELOPER'S CONFERENCE

Trilha – SOFTWARE SECURITY

JOAS ANTONIO



THE
DEVELOPER'S
CONFERENCE

Introdução ao Mitre Att&ck e ao Cyber Kill Chain

Joas Antonio

Whoami



THE
DEVELOPER'S
CONFERENCE

Joas Antonio (C0d3Cr4zy)

19 years – Brazil, São Paulo

Apaixonado por tecnologia desde os 7 anos de idade

Asperger/TDAH

PenTester na Inmetrics

Red Team Village, Mitre, Womcy e Hacker Culture Contributor

CEH Master, OSWP, eJPT e eMAPT

Hacking Is Not Crime Advocate

Mitre Contributor

+15 CVE's (XSS, RCE, CSRF, SSRF)

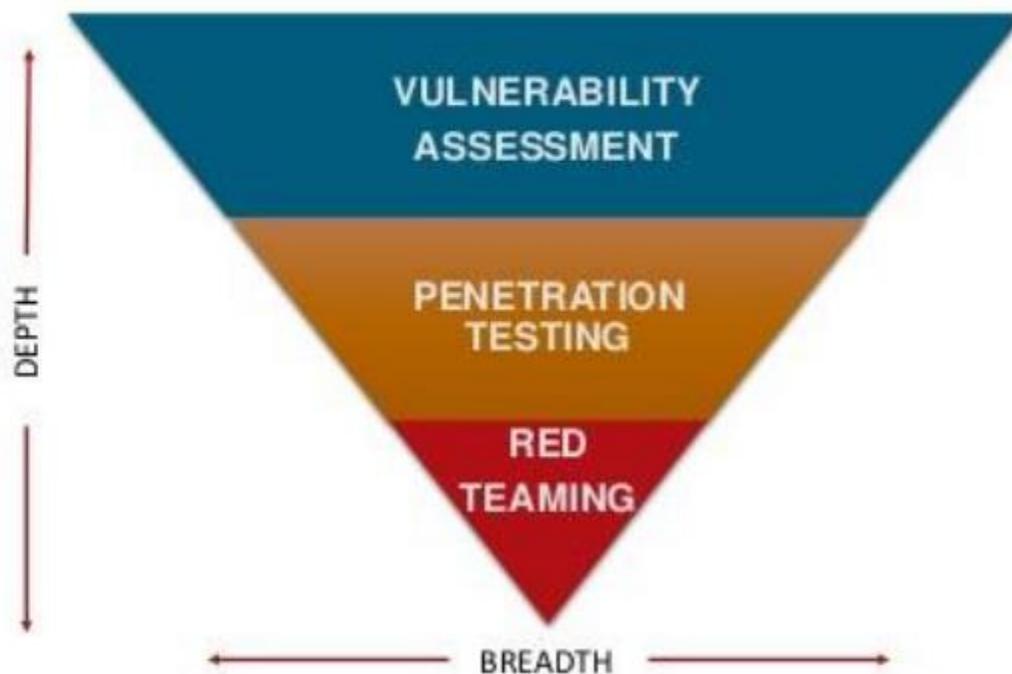


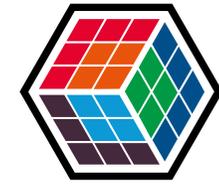
THE
DEVELOPER'S
CONFERENCE

Red Team vs Other Security Tests



Red Teaming VS Other Security Tests





Red Team vs PenTest

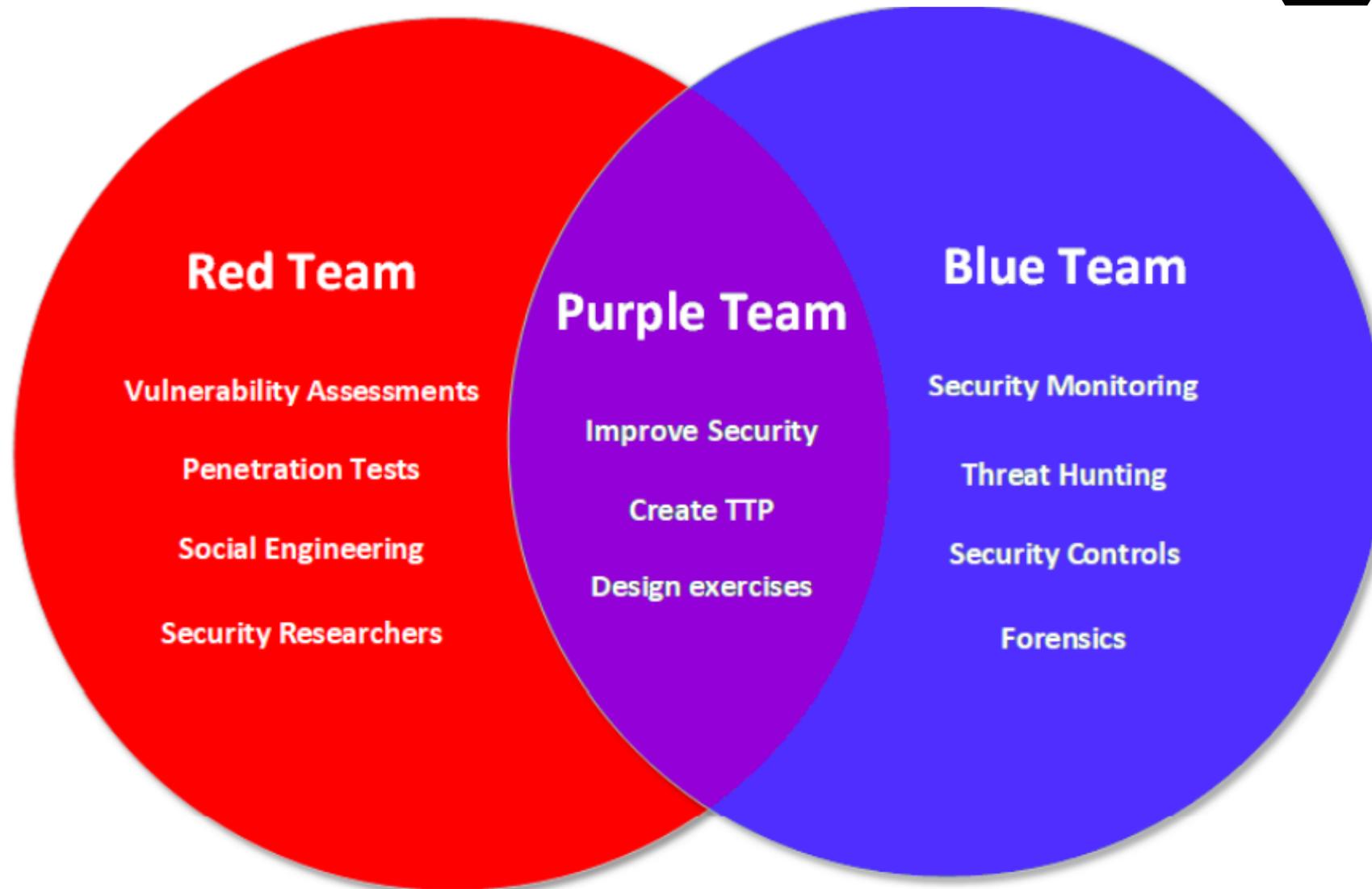
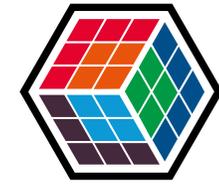
CLASSICAL PENTEST	RED TEAMING
Limited timeframe	Comprehensive timeframe
Static methodology	Flexible methodology
Commercial pentest tools are used	All kinds of resources are used
Employees are aware of the test	Except for a few manager, nobody knows while testing
Testers take advantage of known vulnerabilities	Experts try to discover new vulnerabilities
Target is just the technology part	Target is technology, physical and human factors



THE
DEVELOPER'S
CONFERENCE

RED AND BLUE = PURPLE

Joas Antonio





SOBRE PURPLE TEAM

O Purple Team trabalha em sinergia com Red e Blue Teams, com a missão de alcançar um nível ainda maior de segurança dentro da organização, explorando ao máximo rotinas de ataque e defesa, pensando em como reforçar táticas, técnicas e procedimentos (TTP) de defesa.

Essa abordagem ajuda a desenvolver e melhorar as duas equipes. A equipe azul fica mais informada sobre como priorizar, medir e melhorar sua capacidade de detectar e se defender contra ameaças e ataques, e a equipe vermelha obtém uma visão do setor sobre tecnologias e mecanismos usados na defesa.



THE
DEVELOPER'S
CONFERENCE

MITRE ATT&CK

Joas Antonio



Mitre Att&ck

O framework ATT&CK é valioso para uma série de configurações. Qualquer atividade de defesa pode se beneficiar de aplicar as diretrizes do framework. Além de oferecer uma linguagem comum para os profissionais, o ATT&CK também fornece a fundação para atividades de pentest e Red Team. Isso dá a ambas as equipes um padrão comum de comunicação ao se falar sobre os comportamentos adversários.

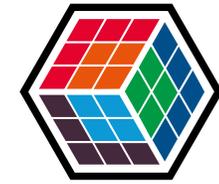
Mitre-Att&ck



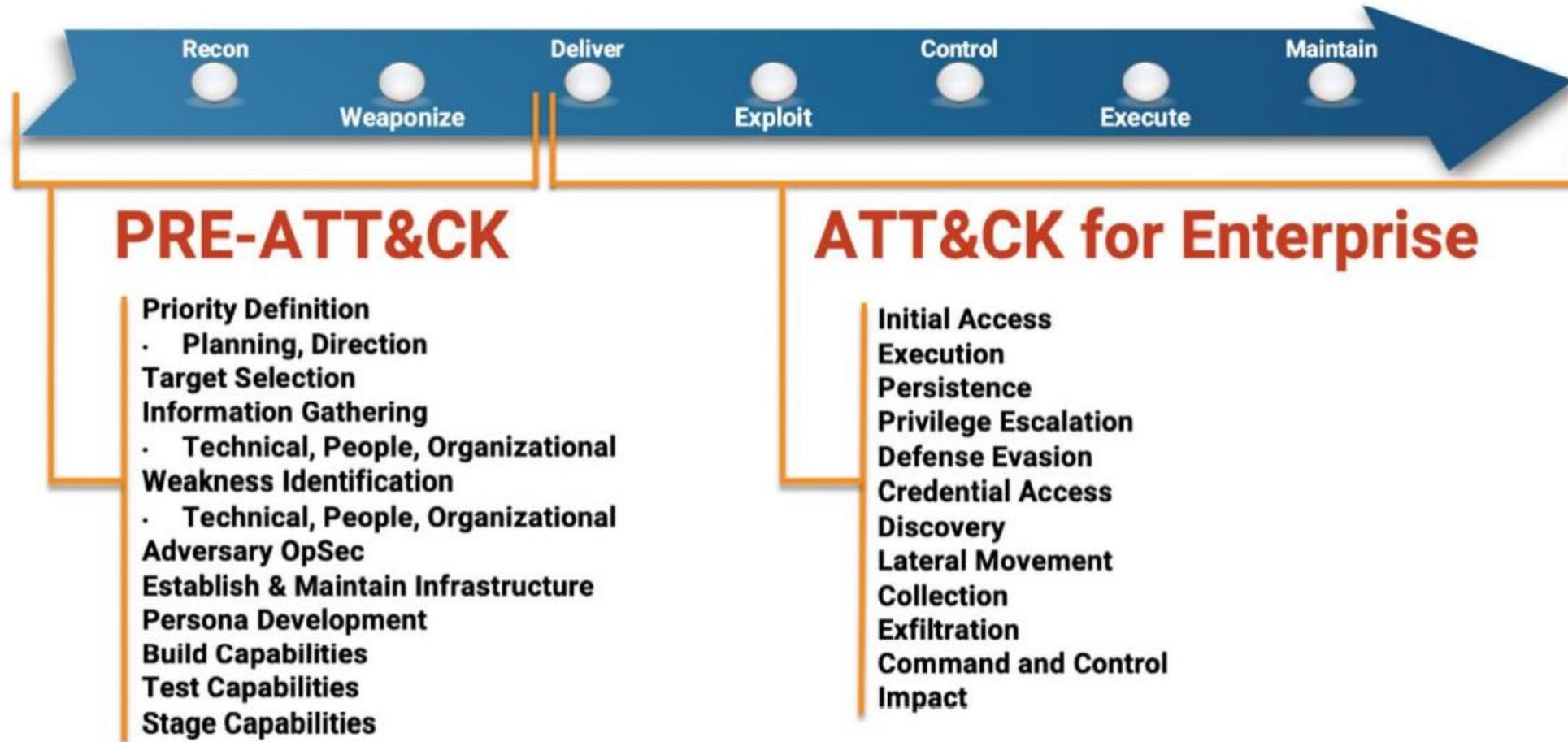
THE
DEVELOPER'S
CONFERENCE

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/5)	Application Window Discovery	Internal Spearphishing
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Dashboard	Remote Services (0/6)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Cloud Service Discovery	Replication Through Removable Media
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/7)	Create Account (0/3)	Domain Policy Modification (0/2)	Direct Volume Access	Man-in-the-Middle (0/2)	Container and Resource Discovery	Software Deployment Tools
Search Open Technical Databases (0/5)		Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Escape to Host	Domain Policy Modification (0/2)	Modify Authentication Process (0/4)	Domain Trust Discovery	Taint Shared Content
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	Software Deployment Tools	Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication
Search Victim-Owned Websites			System Services (0/2)	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	OS Credential Dumping (0/2)	File and Directory Permissions Modification (0/2)	
			User Execution (0/3)		Hijack Execution	File and Directory Permissions Modification (0/2)		Network Service Scanning	
			Windows Management			Hide Artifacts (0/2)		Network Share Discovery	

Mitre Att&ck



THE
DEVELOPER'S
CONFERENCE



Mitre Att&ck



THE
DEVELOPER'S
CONFERENCE

Enterprise ATT&CK
PRE-ATT&CK

} It's just
ATT&CK



THE
DEVELOPER'S
CONFERENCE

Cyber Kill Chain

Joas Antonio



CYBER KILL CHAIN vs. MITRE ATT&CK

CYBER KILL CHAIN

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objectives



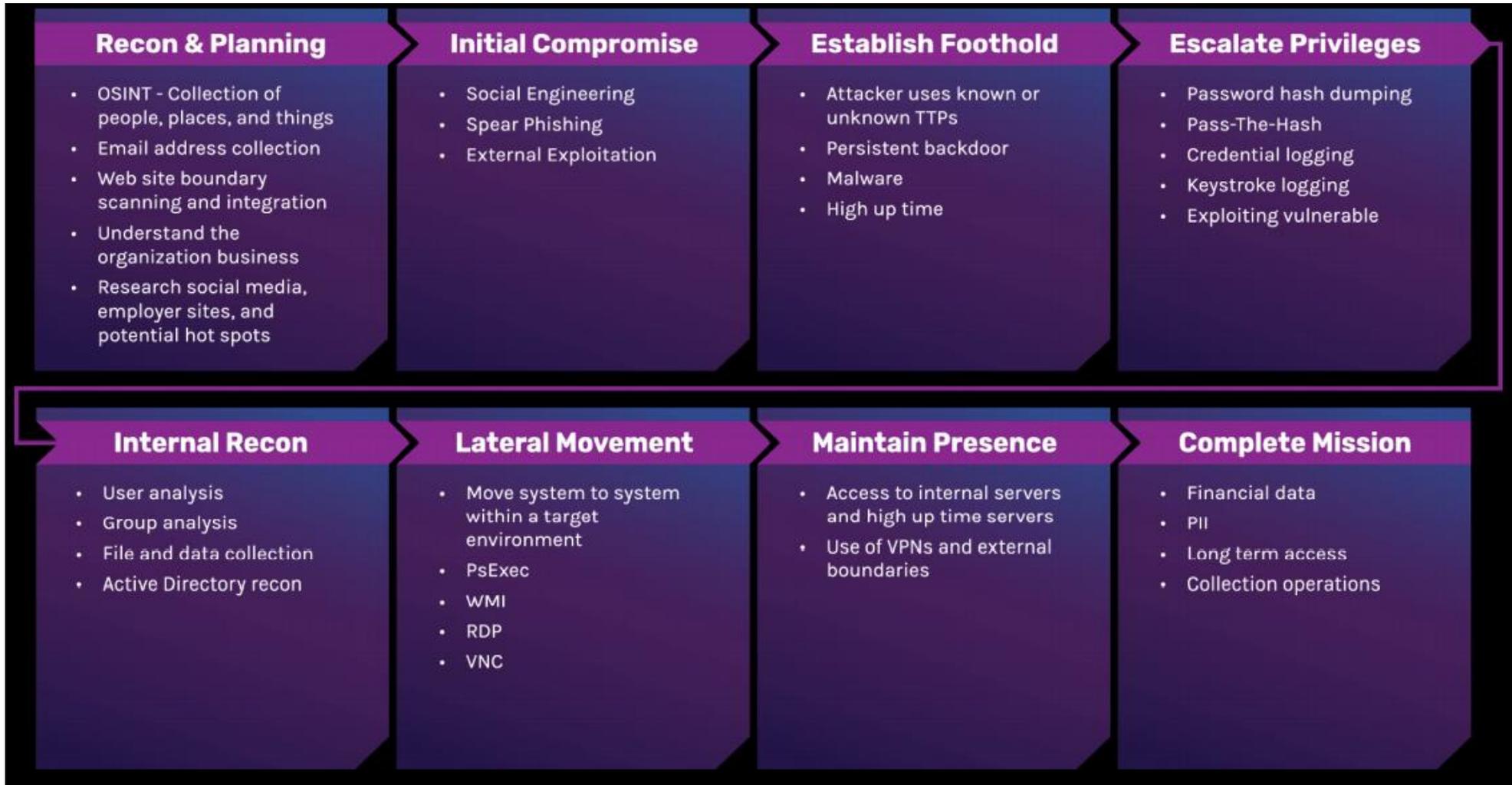
MITRE ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control
- Impact

Adversary Emulation



THE
DEVELOPER'S
CONFERENCE





THE
DEVELOPER'S
CONFERENCE



Muito obrigado pela oportunidade

Joas Antonio (C0d3Cr4zy)

Credits: Filipi Pires, João Paulo de Andrade
and Information Security Community Brazilian