

ПРОВЕДЕНИЕ ТЕСТИРОВАНИЙ НА ПРОНИКНОВЕНИЕ И АНАЛИЗА УЯЗВИМОСТЕЙ

Сергей Леонтьев
Заместитель руководителя отдела консалтинга
АО «ДиалогНаука»



Виды услуг по тестированию

Главная — Услуги — Тестирование на проникновение и анализ защищенности

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ И АНАЛИЗ ЗАЩИЩЕННОСТИ



Тестирование на проникновение в рамках выполнения требования Положений Банка России по защите информации, требований SWIFT CSP, требований PCI DSS



Аудит Интернет-порталов и web-приложений



Анализ безопасности мобильных приложений



Аудит безопасности беспроводных сетей



Внутреннее тестирование на проникновение



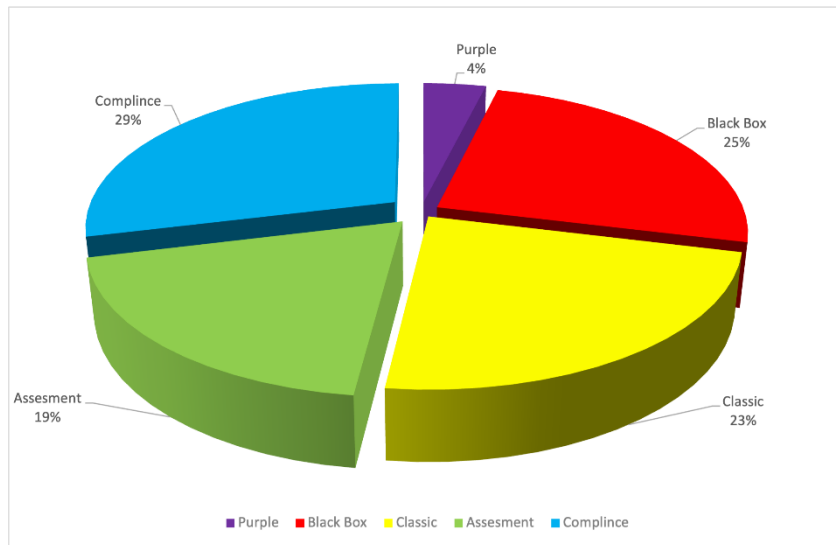
Проведение тестирования на проникновение с целью оценки защищенности от внешних угроз

Виды услуг по тестированию

Услуга	Стандарт	Периодичность
Тестирование на проникновение в рамках выполнения требования Положений Банка России по защите информации, требований SWIFT CSP, требований PCI DSS и т.д.	757-П ГОСТ 57580 PCI DSS SWIFT МинЦифры	ежегодно или чаще
Проведение тестирования на проникновение с целью оценки защищенности от внешних угроз		разово или регулярно (обычно ежегодно)
Внутреннее тестирование на проникновение		разово или регулярно (обычно ежегодно)
Аудит Интернет-порталов и web-приложений		разово или постоянно (например при каждом релизе)
Анализ безопасности мобильных приложений		разово или постоянно (например при каждом релизе)
Аудит безопасности беспроводных сетей	PCI DSS	разово или регулярно
Внешние ежеквартальные сканирования ASV	PCI DSS	ежеквартально
Внутреннее ежеквартальные сканирования	PCI DSS	ежеквартально и после серьезных изменений инфраструктуры

Статистика по проектам

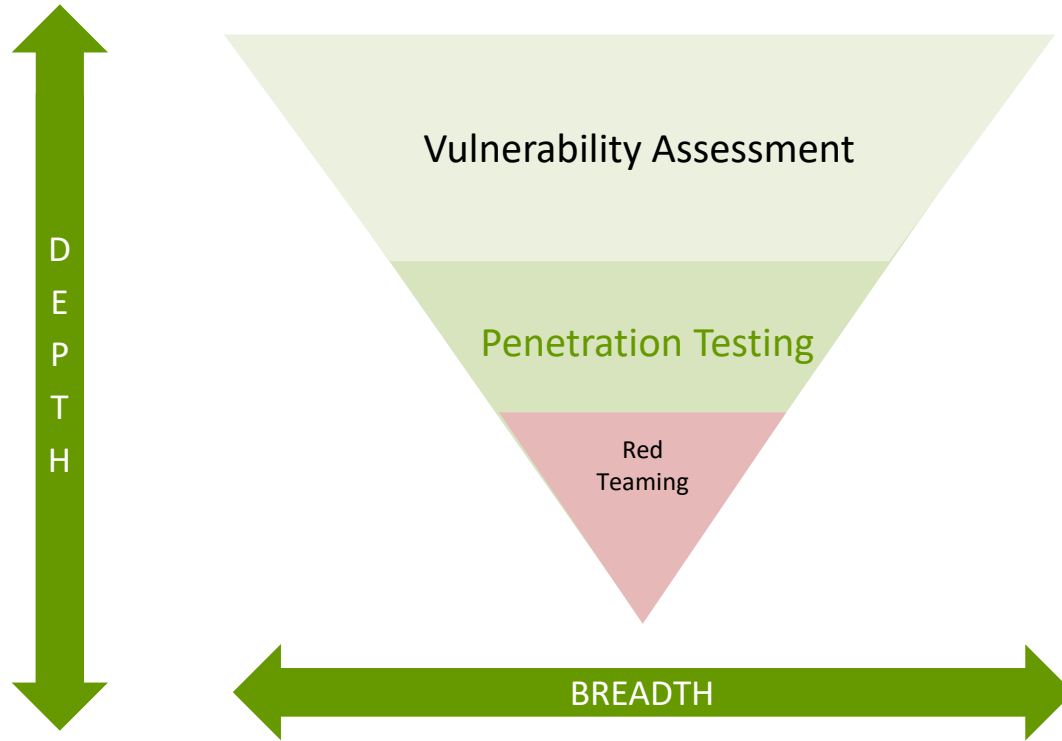
Приблизительная классификация проектов, связанных с тестированием на проникновение и анализом уязвимостей



Топ выполненных проектов за последний год:

- ✓ Compliance (PCI DSS, SWIFT, ЦБ, МинЦифры etc)
- ✓ Black Box (Red Teaming)
- ✓ Classic (внутренние и/или внешние)
- ✓ Assessment (WEB, Mobile etc)
- ✓ Purple Teaming

Подходы к проведению тестирования



Подходы к проведению тестирования

Vulnerability Assessment:

1. Процесс выявления, классификации и определения приоритетности устранения уязвимостей.
2. В первую очередь позволяет понять какие уязвимости и в каком количестве присутствуют в инфраструктуре, а также определить приоритет их устранения.
3. Результаты возможно использовать для базовой оценки рисков ИБ, при этом необходимо понимать контекст в котором находятся данные уязвимости.
4. Обычно является частью процесса Vulnerability/Patch Management и Compliance в организации.

Подходы к проведению тестирования

Penetration Testing:

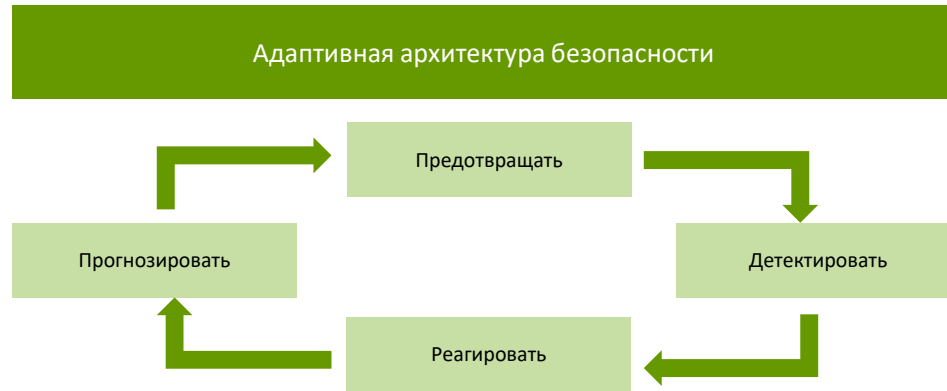
1. Моделирование реальных атак на контролируруемую среду для выявления и эксплуатации уязвимостей.
2. Обычно подразумеваются методы и мотивация реальных злоумышленников.
3. Обычно подразумевается поиск уязвимостей в сетях, системах и приложениях.
4. В некоторых случаях подразумеваются атаки с использованием методов социальной инженерии.

Подходы к проведению тестирования

Red Teaming:

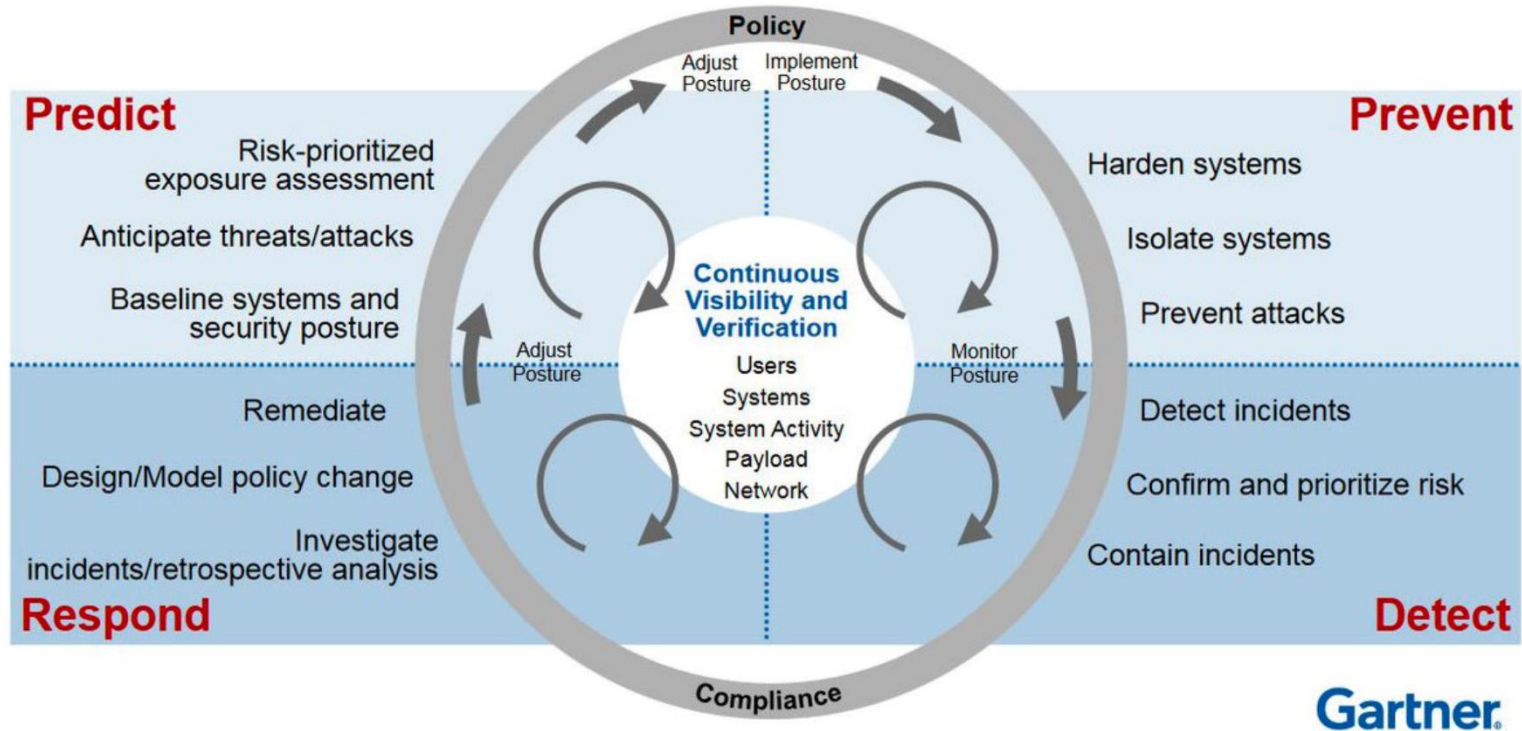
1. Обычно представляет из себя непрерывный процесс симуляции атак с целью оценки всех существующих процессов защиты организации и повышения осведомленности задействованных в этом процессе лиц.
2. При этом имитируется тактика, методы и процедуры (TTP) конкретных субъектов угроз или сценариев.
3. Считается что Red Teaming выходит за рамки классического тестирования на проникновение.
4. Обычно подразумевается использование значительно большей поверхности атаки, чем при Vulnerability Assessment и Penetration Testing.

Концепция адаптивной безопасности



Адаптивная безопасность — подход, который позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на известные риски безопасности а также прогнозировать появления новых.

Концепция адаптивной безопасности



Концепция адаптивной безопасности

OFFENSIVE SECURITY

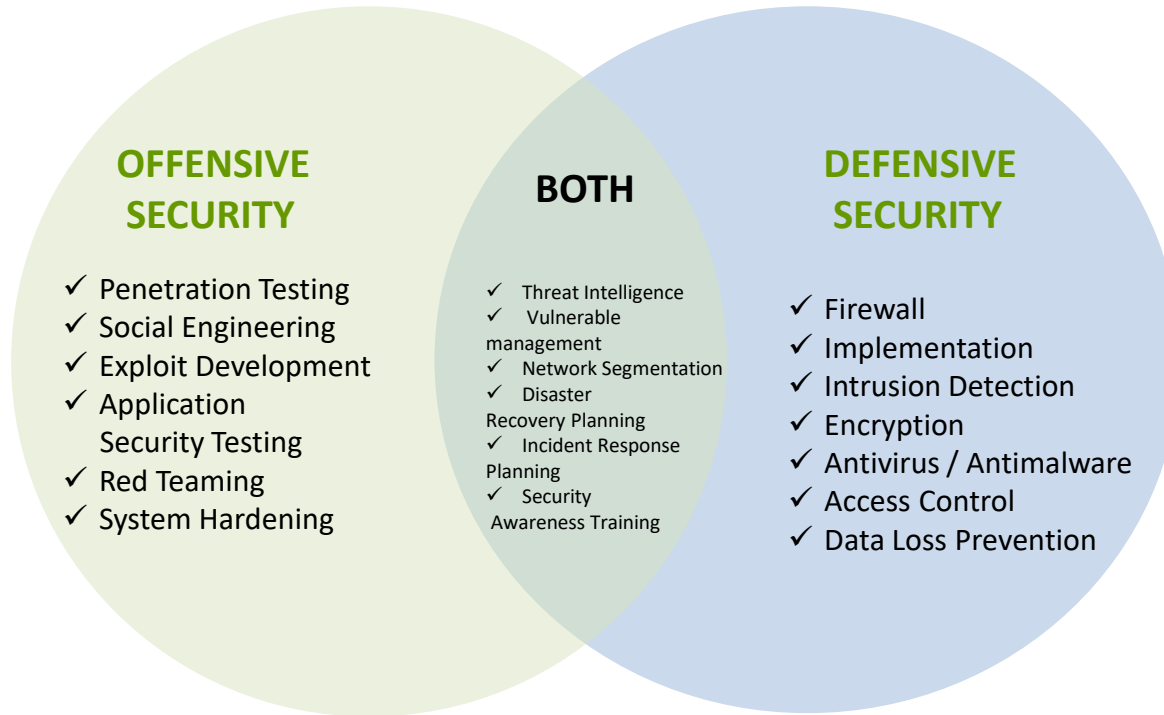
- ✓ Penetration Testing
- ✓ Social Engineering
- ✓ Exploit Development
- ✓ Application Security Testing
- ✓ Red Teaming
- ✓ System Hardening

Концепция адаптивной безопасности

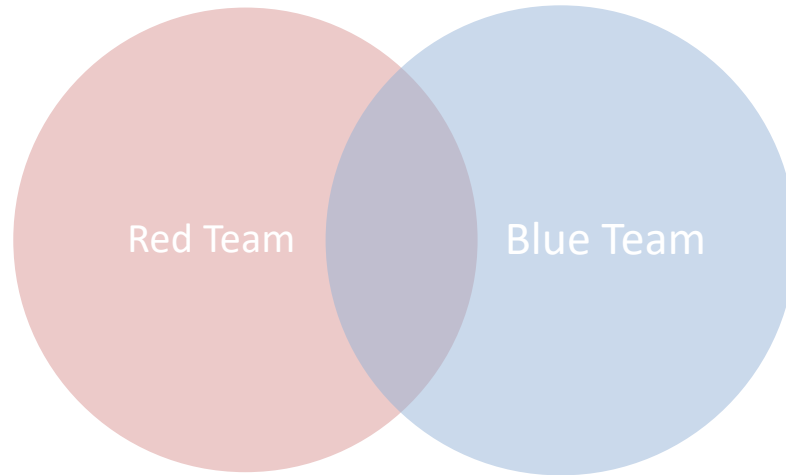
DEFENSIVE SECURITY

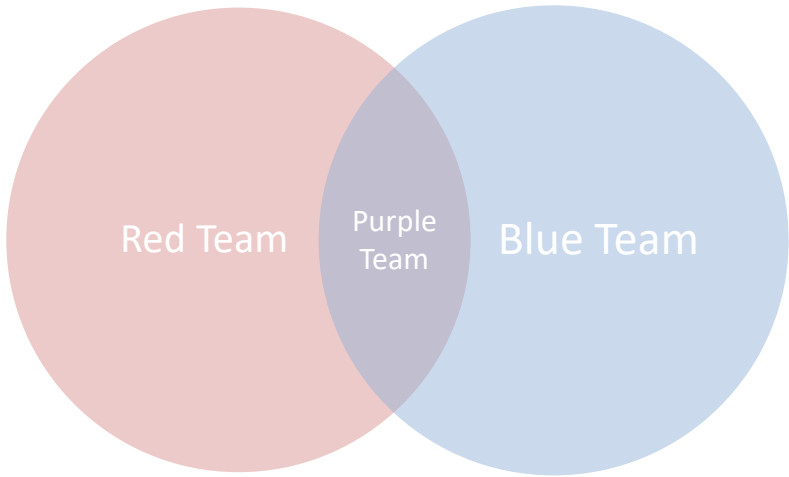
- ✓ Firewall
- ✓ Implementation
- ✓ Intrusion Detection
- ✓ Encryption
- ✓ Antivirus / Antimalware
- ✓ Access Control
- ✓ Data Loss Prevention

Концепция адаптивной безопасности

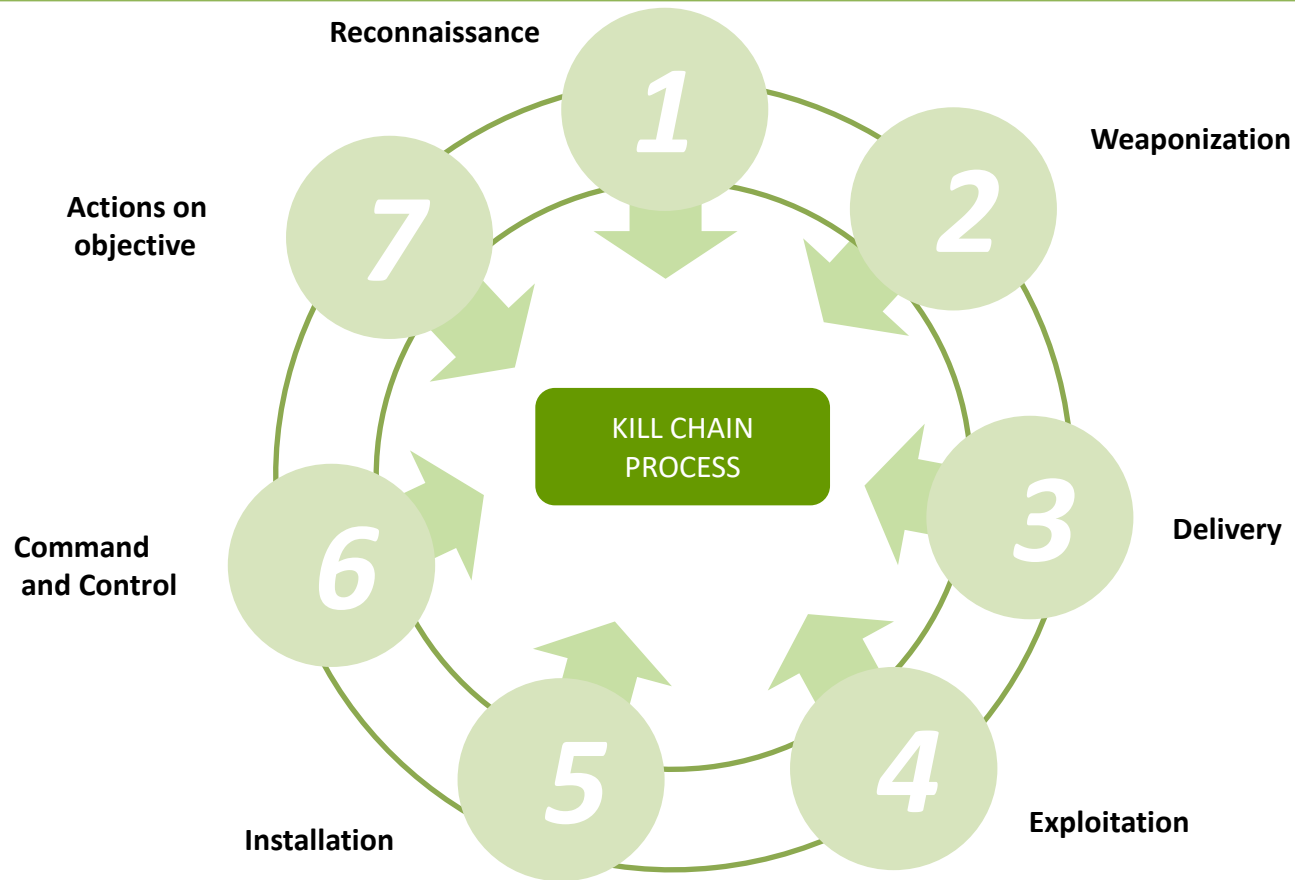


Red Team/Blue Team





Attack/Cyber Kill Chain



KILL CHAIN

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

VS

MITRE ATT&CK

- Initial access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral movement
- Collection
- Exfiltration

Жизненный цикл атаки



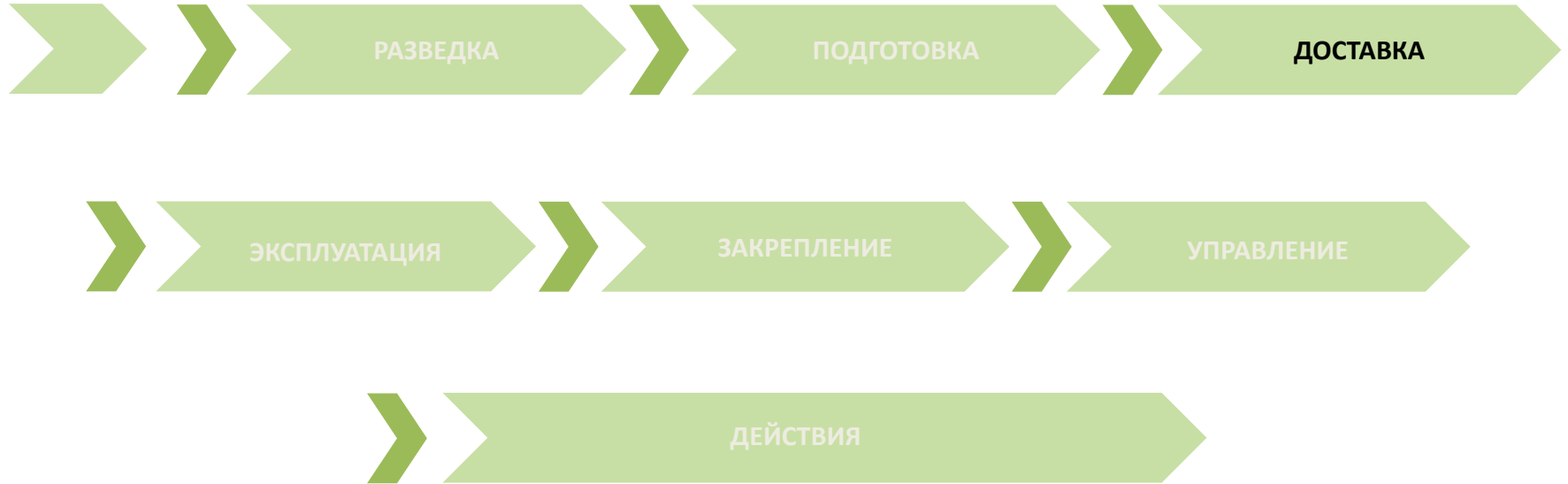
Жизненный цикл атаки



Жизненный цикл атаки



Жизненный цикл атаки



Жизненный цикл атаки



Жизненный цикл атаки



Жизненный цикл атаки



Жизненный цикл атаки



ATT&CK Matrix for Enterprise

ATT&CK Matrix for Enterprise

layout: side - show sub-techniques - hide sub-techniques

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 43 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (2)	Acquire Access (2)	Content Injection (1)	Cloud Administration Command (1)	Account Manipulation (2)	Abuse Elevation Control Mechanism (2)	Abuse Elevation Control Mechanism (2)	Adversary in the Middle (2)	Account Discovery (2)	Exploitation of Remote Services (1)	Adversary in the Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal (1)
Gather Victim Host Information (4)	Acquire Infrastructure (2)	Drive-by Compromise (1)	Command and Scripting Interpreter (1)	BITS Jobs (1)	Access Token Manipulation (2)	Access Token Manipulation (2)	Brute Force (2)	Application Window Discovery (1)	Archive Collected Data (2)	Archive Collected Data (2)	Communication Through Removable Media (1)	Data Transfer Size Limits (1)	Data Destruction (1)
Gather Victim Identity Information (2)	Compromise Accounts (3)	Exploit Public-Facing Application (1)	Container Administration Command (1)	Boot or Logon Autostart Execution (1)	Account Manipulation (4)	Account Manipulation (4)	Credentials from Password Stores (2)	Browser Information Discovery (1)	Audio Capture (1)	Automated Collection (1)	Content Injection (1)	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact (1)
Gather Victim Network Information (4)	Compromise Infrastructure (2)	External Remote Services (1)	Deploy Container (1)	Boot or Logon Initialization Scripts (2)	Build Image on Host (1)	Build Image on Host (1)	Exploitation for Credential Access (1)	Cloud Infrastructure Discovery (1)	Automated Hijacking (1)	Browser Session Hijacking (1)	Data Encoding (2)	Exfiltration Over C2 Channel (1)	Data Manipulation (2)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions (1)	Exploitation for Client Execution (1)	Browser Extensions (1)	Debugger Evasion (1)	Debugger Evasion (1)	Exploitation for Local Access (1)	Cloud Service Dashboard (1)	Clipboard Data (1)	Remote Service Session Hijacking (1)	Clipboard Data (1)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (2)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (2)	Compromise Host Software Binary (1)	Boot or Logon Autostart Execution (1)	Boot or Logon Initialization Scripts (2)	Exploitation for Remote Access (1)	Cloud Service Dashboard (1)	Remote Services (2)	Replication Through Removable Media (1)	Data from Cloud Storage (1)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (1)	Replication Through Removable Media (1)	Native API (1)	Create Account (2)	Create or Modify System Process (2)	Create or Modify System Process (2)	Input Capture (2)	Cloud Storage Object Discovery (1)	Remote Services (2)	Software Deployment Tools (1)	Data from Configuration Repository (1)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (2)	Stage Capabilities (2)	Supply Chain Compromise (2)	Scheduled Task/Job (2)	Create or Modify System Process (2)	Domain or Tenant Policy Modification (2)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception (1)	Container and Resource Discovery (1)	Debugger Evasion (1)	Software Deployment Tools (1)	Data from Information Repositories (2)	Exfiltration Over Web Service (4)	Financial Theft (1)
Search Open Websites/Domains (2)	Trusted Relationship (1)	Trusted Relationship (1)	Serverless Execution (1)	Event Triggered Execution (1)	Domain or Tenant Policy Modification (2)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception (1)	Device Driver Discovery (1)	Device Driver Discovery (1)	Taint Shared Content (1)	Data from Local System (1)	Ingress Tool Transfer (1)	Firmware Corruption (1)
Search Victim Owned Websites (1)	Valid Accounts (2)	Valid Accounts (2)	Shared Modules (1)	External Remote Services (1)	Event Triggered Execution (1)	Event Triggered Execution (1)	Multi-Factor Authentication Interception (1)	File and Directory Discovery (1)	Use Alternate Authentication Material (2)	Use Alternate Authentication Material (2)	Data from Network Shared Drive (1)	Scheduled Transfer (1)	Inhibit System Recovery (1)
			Software Deployment Tools (1)	Hijack Execution Flow (1)	Exploitation for Privilege Escalation (1)	Exploitation for Defense Evasion (1)	Multi-Factor Authentication Request Generation (1)	File and Directory Discovery (1)	File and Directory Discovery (1)	Group Policy Discovery (1)	Data from Removable Media (1)	Transfer Data to Cloud Account (1)	Network Denial of Service (2)
			System Services (2)	Implement Internal Image (1)	Hijack Execution Flow (2)	Hide Artifacts (2)	Group Policy Discovery (1)	Log Enumeration (1)	Log Enumeration (1)	Non-Application Layer Protocol (1)	Non-Standard Port (1)	Resource Hijacking (1)	Service Stop (1)
			User Execution (2)	Hide Artifacts (2)	Hijack Execution Flow (2)	Hijack Execution Flow (2)	Log Enumeration (1)	Network Service Discovery (1)	Network Service Discovery (1)	Non-Application Layer Protocol (1)	Non-Standard Port (1)	System Shutdown/Reboot (1)	
			Windows Management Instrumentation (1)	Process Injection (1)	Process Injection (1)	Hijack Execution Flow (2)	Network Sniffing (1)	Network Share Discovery (1)	Network Share Discovery (1)	Protocol Tunneling (1)	Non-Standard Port (1)		
				Office Application Startup (1)	Scheduled Task/Job (2)	Scheduled Task/Job (2)	Network Sniffing (1)	Network Sniffing (1)	Network Sniffing (1)	Data Staged (2)	Protocol Tunneling (1)		
				Power Settings (1)	Valid Accounts (4)	Valid Accounts (4)	Network Sniffing (1)	Network Sniffing (1)	Network Sniffing (1)	Email Collection (2)	Protocol Tunneling (1)		
				Pre-OS Boot (2)	Indicator Removal (2)	Indicator Removal (2)	OS Credential Dumping (2)	Network Service Discovery (1)	Network Service Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
				Scheduled Task/Job (2)	Indirect Command Execution (1)	Indirect Command Execution (1)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
				Server Software Component (2)	Masquerading (2)	Masquerading (2)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
				Traffic Signaling (2)	Modify Authentication Process (2)	Modify Authentication Process (2)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
				Valid Accounts (4)	Modify Cloud Compute Infrastructure (2)	Modify Cloud Compute Infrastructure (2)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Modify Registry (1)	Modify Registry (1)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Modify System Image (2)	Modify System Image (2)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Network Boundary Bridging (1)	Network Boundary Bridging (1)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Obfuscated Files or Information (1)	Obfuscated Files or Information (1)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Pre-OS Boot (2)	Pre-OS Boot (2)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Process Injection (2)	Process Injection (2)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Reflective Code Loading (1)	Reflective Code Loading (1)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Rogue Domain Controller (1)	Rogue Domain Controller (1)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Rootkit (1)	Rootkit (1)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Subvert Trust Controls (2)	Subvert Trust Controls (2)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					System Binary Proxy Execution (1)	System Binary Proxy Execution (1)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					System Script Proxy Execution (2)	System Script Proxy Execution (2)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Template Injection (1)	Template Injection (1)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Traffic Signaling (2)	Traffic Signaling (2)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Trusted Developer Utilities Proxy Execution (1)	Trusted Developer Utilities Proxy Execution (1)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Unusual/Unsupported Cloud Regions (1)	Unusual/Unsupported Cloud Regions (1)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Use Alternate Authentication Material (2)	Use Alternate Authentication Material (2)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Valid Accounts (4)	Valid Accounts (4)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Virtualization/Sandbox Evasion (2)	Virtualization/Sandbox Evasion (2)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					Weaken Encryption (2)	Weaken Encryption (2)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		
					XSL Script Processing (1)	XSL Script Processing (1)	OS Credential Dumping (2)	Network Share Discovery (1)	Network Share Discovery (1)	Input Capture (2)	Protocol Tunneling (1)		

ATT&CK Matrix for Enterprise

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (0/10)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/6)	BITS Jobs	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/8)	Compromise Infrastructure (0/8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Autostart Execution (0/14)	Deobfuscate/Decode Files or Information	Forged Authentication	Cloud Service Dashboard	Remote Services (0/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Defacement (0/2)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Host Software Binary (0/3)	Boot or Logon Initialization Scripts (0/5)	Deploy Container	Forge Web Credentials (0/2)	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Exfiltration Over Other Network Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (0/7)	Replication Through Removable Media	Native API	Create Account (0/3)	Create or Modify System Process (0/5)	Direct Volume Access	Input Capture (0/4)	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage (0/2)	Encrypted Channel	Exfiltration Over Physical Medium (0/1)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create or Modify System Process (0/5)	Domain or Tenant Policy Modification (0/2)	Domain or Tenant Policy Modification (0/2)	Modify Authentication Process (0/9)	Debugger Evasion	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Exfiltration Over Physical Medium (0/1)	Financial Theft
Search Open Websites/Domains (0/3)	Trusted Relationship (0/4)	Serverless Execution	Shared Modules	Event Triggered Execution (0/16)	Escape to Host (0/2)	File and Directory Permissions Modification (0/2)	Multi-Factor Authentication Interception	Device Driver Discovery	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Hide Infrastructure	Exfiltration Over Web Service (0/4)	Firmware Corruption
Search Victim-Owned Websites	Valid Accounts (0/4)	Software Deployment Tools	System Services (0/2)	Event Triggered Execution (0/16)	Hijack Execution Flow (0/13)	Hide Artifacts (0/12)	Multi-Factor Authentication Request Generation	File and Directory Discovery		Data from Local System	Ingress Tool Transfer	Exfiltration Over Web Service (0/4)	Inhibit System Recovery
		User Execution (0/3)	Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (0/13)	Impair Defenses (0/11)	Network Sniffing	Group Policy Discovery		Data from Network Shared Drive	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (0/2)
				Hijack Execution Flow (0/13)	Process Injection (0/12)	Hijack Execution Flow (0/13)	OS Credential Dumping (0/8)	Log Enumeration		Data from Removable Media	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking
				Process Injection (0/12)	Indicator Removal (0/9)	Impersonation	Network Service Discovery	Network Service Discovery		Data Staged (0/2)	Proxy (0/4)		Service Stop
				Scheduled Task/Job (0/5)	Indirect Command Execution	Indicator Removal (0/9)	Network Share Discovery	Network Sniffing		Email Collection (0/3)	Remote Access Software		System Shutdown/Reboot
				Valid Accounts (0/4)	Masquerading (0/9)	Indirect Command Execution	Network Service Discovery	Password Policy Discovery		Input Capture (0/4)	Traffic Signaling (0/2)		
					Masquerading (0/9)	Masquerading (0/9)	OS Credential Dumping (0/8)	Peripheral Device Discovery		Screen Capture	Web Service (0/3)		
					Modify Authentication Process (0/9)	Masquerading (0/9)	Steal or Forge Kerberos Tickets (0/4)	Permission Groups Discovery (0/3)		Video Capture			
					Modify Cloud Compute Infrastructure (0/5)	Masquerading (0/9)	Steal Web Session Cookie (0/4)	Process Discovery					
					Modify Registry (0/5)	Modify Authentication Process (0/9)	Unsecured Credentials (0/8)	Query Registry					
					Modify System Image (0/2)	Modify Cloud Compute Infrastructure (0/5)		Remote System Discovery					
					Network Boundary Bridging (0/1)	Modify Registry (0/5)		Software Discovery (0/1)					
						Network Boundary Bridging (0/1)		System Information Discovery					
								System Location					



Open Source Security Testing Methodology Manual (OSSTMM) – пожалуй, единственная методика, которая акцентирует внимание не только на технических тестах, но и на атаках, связанных с социальной инженерией и направленных на пользователей корпоративной сети.



NIST SP800-115 – данный документ хотя и не является методикой, но описывает общие аспекты проведения тестов на проникновение.



The Information Systems Security Assessment Framework (ISSAF) – фреймворк (framework), ориентированный на инструментальный поиск уязвимостей.



PCI DSS (раздел 11.3 стандарта) – согласно разделу 11.3 стандарта PCI DSS в организациях, соответствующих стандарту, не реже раза в год должен проводиться тест на проникновение. Для разъяснения данного раздела PCI DSS был выпущен документ Information Supplement Requirement 11.3 Penetration Testing, в очень общих чертах описывающий последовательность проведения инструментальной проверки внешнего периметра сетевой инфраструктуры тестируемой компании (по сути, данная инструментальная проверка не является тестом на проникновение).



The Open Web Application Security Project (OWASP) – руководство по тестированию веб-безопасности, которое является основной методологией тестирования безопасности для разработчиков веб-приложений и специалистов по информационной безопасности и разрабатывается международным консорциумом OWASP.



The Penetration Testing Execution Standard (PTES) – Стандарт по тестированию на проникновение. Стандарт проведения тестирования на проникновение состоит из семи (7) основных разделов. Они охватывают всё, что связано с тестом на проникновение – от первоначального общения и обоснования пентеста до этапов сбора разведанных и моделирования угроз. Тестировщики работают за кулисами, чтобы лучше понять тестируемую организацию, через исследование уязвимостей, эксплуатации и постэксплуатации, когда технический опыт тестировщиков в области безопасности сочетается с пониманием бизнеса. И, наконец, с отчетностью, которая охватывает весь процесс таким образом, который обеспечивает наибольшую ценность.



PWK – Методология курса «Тестирование на проникновение с Kali Linux». Является основным материалом для получения сертификата по тестированию на проникновение – OSCP и практическим руководством.

Спасибо за внимание