Rules of Engagement: Penetration Testing and Security Assessment

Information Security Specialist

2025-12-21

Overview

This document defines the Rules of Engagement (RoE) for conducting penetration testing and security assessments of information systems. The document establishes the framework for collaboration between the client and testing team, ensuring security, legality, and effectiveness of the process.

Document Objectives

> **Primary Goal** — Ensure controlled and authorized testing with minimal risks to production systems

The Rules of Engagement guarantee: - **Security** of production systems - **Compliance** with legal requirements - **Transparent communication** between all parties - **Controlled** and authorized testing

.

Contact Information

Client Organization

Role	Contact Details
Primary Contact	
Position	_____
Mobile Phone	_____
Email Address	_____
Secondary Contact	
Position	_____
Mobile Phone	_____
Email Address	_____

Testing Team

Role	Contact Details
Team Lead	
Mobile Phone	_____
Email Address	_____
Backup Contact	
Mobile Phone	_____

Role	Contact Details
Email Address	_____
24/7 Emergency Contact	
Mobile Phone	_____
Email Address	_____

.

Scope of Testing

In-Scope Assets

Network Infrastructure: - Domains: _____ - Subdomains: _____ - IP Ranges: _____ - Cloud Resources: _____

Applications and Services: - Web Applications: _____ - API Interfaces: _____ - Internal Systems: _____

Out-of-Scope Assets

⚠ **Critical Restrictions:**

- Systems not owned by the organization
- Third-party services without written authorization
- Production databases (unless explicitly permitted)
- Social engineering (unless approved)
- Critical infrastructure systems

.

Testing Rules and Procedures

Authorized Activities

Approved Testing Methods:

- Vulnerability scanning
- Manual penetration testing
- Web application testing
- API interface testing
- Cloud configuration analysis
- Network security testing
- Password policy verification

Prohibited Activities

× **Strictly Forbidden Actions:**

- Denial of Service (DoS/DDoS) attacks
- Physical intrusion
- Social engineering without explicit authorization

- Brute-force attacks without rate limiting
- Actions that may cause data corruption
- Unauthorized access to personal data

.

Load Limitations

Technical Constraints for Production Systems

⚡ **Critical Load Limits:**

Parameter	Limitation	Notes
Maximum Requests per Second	_____	To prevent system overload
Concurrent Connections	_____	Parallel connection limit
Payload Size	_____	Maximum data size
Connection Timeout	_____	Response wait time

Time Restrictions

🕐 **Intensive Testing Schedule:**

- **Mass Scanning**: Off-hours only
- **Fuzzing Testing**: _____ (specify time windows)
- **Load Testing**: Prior notification required
- **Automated Scanners**: Rate-limited during business hours

Load Monitoring

📊 **System Impact Control:** - CPU and memory monitoring of target systems - Application response time tracking - Network bandwidth control - Immediate halt if limits exceeded

.

Legal Basis

Legal Foundation for Testing

⚖ **Legal Justification:**

> All penetration testing activities are performed exclusively based on written authorization from an authorized representative of the client organization

Documentary Basis: - Signed service agreement - These Rules of Engagement - Technical specification describing testing scope - Additional agreements (if necessary)

Limitation of Liability

🛡 **Liability Exemption:**

The testing team is exempt from liability for: - Temporary system unavailability resulting from authorized testing - Discovery of vulnerabilities existing prior to testing commencement - Actions performed strictly within the agreed testing scope - Indirect losses related to security issue identification

Legal Compliance

📋 **Regulatory Compliance:** - Adherence to personal data protection legislation - Compliance with industry security standards - Alignment with international penetration testing practices - Documentation of all actions for audit purposes

.

Vulnerability Criticality Matrix

Risk Level Classification

Standardized Assessment System:

Level	Description	Vulnerability Examples	Remediation Time
P0 - Critical	Immediate security threat	RCE, SQL Injection, Authentication Bypass	24-48 hours
P1 - High	Serious security breach	XSS, LFI, Privilege Escalation	1-2 weeks
P2 - Medium	Moderate risk	Security Misconfiguration, CSRF	1 month
P3 - Low	Minimal risk	Information Disclosure, Weak Ciphers	3 months
P4 - Informational	Improvement recommendations	Best Practices, Hardening	As possible

Assessment Criteria

📈 **Criticality Determination Factors:** - **Impact**: Potential damage from exploitation - **Likelihood**: Ease of vulnerability exploitation - **Scope**: Number of affected systems - **Accessibility**: Access requirements for exploitation

Escalation Procedure

⚡ **Emergency Response for Critical Findings:** 1. **P0-P1**: Immediate notification by phone + email 2. **P2**: Notification within business day 3. **P3-P4**: Inclusion in regular reports

.

Authorized Testing Tools

Primary Testing Toolkit

Core Toolset:

Category	Tool	Purpose	Version
Vulnerability Scanners	Nessus	Automated scanning	_____
	OpenVAS	Network and application scanning	_____
	Qualys VMDR	Cloud scanning	_____
Web Testing	Burp Suite Professional	Web application testing	_____
	OWASP ZAP	Web application security analysis	_____
	Nikto	Web server scanning	_____
Network Testing	Nmap	Port and service scanning	_____
	Masscan	High-speed scanning	_____
Exploitation	Metasploit Framework	Exploit testing	_____
	Cobalt Strike	Attack simulation (with agreement)	_____

Additional Tools

🛠 **Specialized Software (by agreement):** - **Social Engineering**: SET, Gophish (explicit permission only) - **Wireless Networks**: Aircrack-ng, Kismet - **Mobile Applications**: MobSF, Frida - **Cloud Security**: ScoutSuite, Prowler

Tool Restrictions

⚠ **Prohibited or Restricted Tools:** - DDoS attack tools - Unauthorized scanners with aggressive settings - Password cracking tools without rate limits - Any software not agreed upon with the client

.

Testing Team Identification

Whitelists for Defensive Systems

🔍 **Critical for preventing authorized testing blockage:**

Identification Parameter	Value	Purpose
Source IP Addresses	_____ _____	Static IPs for WAF/IPS whitelisting

Identification Parameter	Value	Purpose
Subnet Ranges	_____ _____	Additional team network segments
User-Agent Strings	_____ _____	Specific identifiers for web scanners
SSH Keys	_____ _____	Public keys for authorized access

Special Identifiers

🏷️ **Markers for logging and monitoring:**

- **Test Request Prefix**: _____
- **Special HTTP Headers**: _____
- **Session Identifiers**: _____
- **Payload Markers**: _____

Blue Team Coordination

Interaction with defense team: - Pre-testing notification of commencement - SOC (Security Operations Center) contact list - Procedure for confirming activity legitimacy - Emergency testing halt protocol

.

High-Risk Test Definition

Risky Operation Classification

⚠ **High-risk tests requiring special attention:**

Test Category	Description	Execution Window	Additional Measures
Brute-force Attacks	Password/PIN guessing	Off-hours only	Rate limiting, lockout monitoring
Application Fuzzing	Invalid data submission	_____	System stability control
Vulnerability Exploitation	Proof-of-concept execution	By agreement	Immediate notification on success
DoS Testing	Load resistance verification	Test environment only	Prior agreement required

Critical Test Service Windows

🕐 **Special time intervals:**

- **Primary risky test window**: _____
- **Backup window**: _____

- **Emergency window (by agreement)**: _____
- **Prohibited periods**: _____

Client-Side Testing

End-user protection:

- **Phishing Simulations**: Written HR consent only
- **Browser Testing**: Isolated test machines
- **Social Engineering**: Strictly limited scope
- **Personal Data Protection**: Avoid access to personal information

.

Technical Methodology

Standards and Classifications

📊 **International standards used:**

Standard	Version	Application
CVSS	v3.1/4.0	Vulnerability criticality assessment
OWASP Top 10	2021	Web applications
NIST Cybersecurity Framework	v1.1	General methodology
OSSTMM	v3	Testing methodology
PTES	v1.0	Penetration testing standard

Testing Model

🔍 **Information access level:**

- ☐ **Black Box** - No prior system knowledge
- ☐ **Gray Box** - Partial access to documentation/architecture
- ☐ **White Box** - Full access to code and architecture

Selected Model: _____

CVSS Assessment

📈 **Vulnerability assessment criteria:**

- **Base Metrics**: Attack vector, complexity, privileges, user interaction
- **Temporal Metrics**: Exploit availability, remediation level
- **Environmental Metrics**: Impact on client's specific environment
- **Threshold Values**: P0 (9.0-10.0), P1 (7.0-8.9), P2 (4.0-6.9), P3 (0.1-3.9)

.

Additional Legal Aspects

Cross-Border Data Transfer

🌍 **International compliance:**

> When working with international testing teams, compliance with GDPR, CCPA, and other applicable data protection regulations is ensured

Jurisdictional Requirements: - **Team base country**: _____ - **Applicable legislation**: _____ - **Data transfer mechanisms**: Standard Contractual Clauses (SCC) / Adequacy Decision - **Data localization**: _____

International Standards Compliance

🏷️ **Regulatory compliance:**

Standard/Regulation	Compliance Status	Notes
GDPR (EU)	_____	Personal data protection
ISO 27001	_____	Information security management system
SOC 2 Type II	_____	Security controls
PCI DSS	_____	Payment systems

Audit Rights

🔍 **Data processing control:**

The client has the right to: - Verify data deletion procedures after project completion - Request confirmation of confidential information destruction - Audit testing team security measures - Obtain compliance certificates for applicable standards

.

Critical Situation Response Process

Emergency Response Algorithm

Step-by-step procedure for critical incidents:

1. CRITICAL SITUATION DETECTION
   ↓
2. IMMEDIATE TESTING HALT
   ↓
3. CLIENT NOTIFICATION (within 15 minutes)

↓
4. IMPACT AND DAMAGE ASSESSMENT
↓
5. CONTINUATION DECISION
↓
6. INCIDENT DOCUMENTATION
↓
7. ROOT CAUSE ANALYSIS AND CORRECTIVE MEASURES

Escalation Matrix

Contacts by criticality levels:

Level	Response Time	Communication Method	Responsible
P0 - Critical	15 minutes	Phone + SMS + Email	_____
P1 - High	1 hour	Phone + Email	_____
P2 - Medium	4 hours	Email + Slack/Teams	_____
P3 - Low	24 hours	Email	_____

Testing Halt Criteria

Automatic work cessation triggers:

- Critical service unavailability for more than 5 minutes
- Discovery of active vulnerability exploitation by third parties
- Exceeding agreed load limits
- Halt request from any authorized representative

Evidence Handling and Cleanup

Evidence Handling Protocol

Evidence Handling - strict security requirements:

Stage	Requirements	Responsible
Collection	Encryption, hashing, timestamps	Tester
Storage	Isolated storage, access control	Project Manager
Transfer	Secure channels, receipt confirmation	Both parties
Destruction	Irreversible deletion, destruction certificate	Testing team

Post-Test Cleanup Plan

Post-test Cleanup - mandatory procedures:

Created Object Removal: - [ ] Test user accounts - [ ] Uploaded files and scripts - [ ] Temporary configurations - [ ] Test databases and tables

Original State Restoration: - [ ] Configuration change rollback - [ ] Test certificate removal - [ ] Testing log cleanup (by agreement) - [ ] Backup restoration (if necessary)

Data Destruction Certification

Documentary confirmation:

Upon project completion, the testing team provides: - Certificate of irreversible deletion of all client data - Report on performed cleanup procedures - Confirmation of compliance with data destruction standards (DoD 5220.22-M or equivalent)

.

Testing Schedule

Time Framework

Parameter	Value
Start Date	_____
End Date	_____
Testing Window	_____
Time Zone	_____
Daily Briefing	_____

Communication Protocol

Regular Updates: - Daily status reports - Weekly progress summaries - Emergency notifications for critical findings

.

Incident Handling

Incident Response Procedure

In case of system instability during testing:

1. **Immediate halt** of testing by team
2. **Notification** of client organization
3. **Decision making** by emergency contact regarding continuation
4. **Incident documentation**

Testing Halt Criteria

🔍 **Conditions for work cessation:** - Discovery of critical vulnerabilities - Production system instability - Exceeding agreed testing scope - Client request

.

Data Handling and Confidentiality

Data Handling Principles

Confidentiality — priority number one when processing any information

Testing Team Obligations: - Sensitive data not stored unless necessary - All collected data encrypted - Data deleted after report delivery - Avoidance of personal data access

Non-Disclosure Agreement

All testing participants commit to: - Maintain confidentiality of obtained information - Not disclose results to third parties - Use data exclusively for testing purposes

.

Reporting Requirements

Report Structure

Interim Reports: - Daily or weekly updates - Task completion status - Preliminary findings

Final Reporting: - **Technical Report** — detailed vulnerability description - **Management Report** — recommendations for leadership - **Executive Summary** — brief overview for top management

Results Presentation Format

📊 **Standardized structure:** - Vulnerability classification by criticality - Remediation recommendations - Remediation timeframes - Security metrics

.

Risk Acceptance

Client Organization Confirmation

The client organization confirms understanding that:

- Testing may reveal critical vulnerabilities
- Some tests may cause temporary performance degradation
- All actions are authorized and agreed upon
- Results will be used to improve security

.

Testing Readiness Checklist

Preparatory Activities

- ☐ Testing scope defined
- ☐ Responsible contacts assigned
- ☐ Work schedule agreed
- ☐ All necessary documents signed
- ☐ Communication channels established
- ☐ Test environment prepared (if necessary)
- ☐ Testing team briefing conducted

Control Points During Testing

- ☐ Daily status meetings
- ☐ Production system monitoring
- ☐ All actions documented
- ☐ Timeline compliance
- ☐ Regular client communication

.

Signatures and Approvals

Client Organization Representative

Field	Value
Name and Position	_____
Signature	_____
Date	_____

Testing Team Lead

Field	Value
Name and Position	_____
Signature	_____
Date	_____

.

Emergency Contact Form

Rapid Response Information

Parameter	Contact Details
Primary Client Contact	_____
Secondary Client Contact	_____
Testing Lead	_____
24/7 Emergency Line	_____

Emergency Contact Procedure

1. **Primary contact** — main client representative
2. **If unavailable** — secondary contact
3. **Critical situations** — 24/7 emergency line
4. **Documentation** of all communications

.

This document is a legally binding agreement between the parties and must be signed by all participants in the penetration testing process.