RSC
Ripple Software Consulting

Pentest +

Engagement Scoping

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

General Scoping Terms

ASV – Approved Security Vendor
ASA – Annual Self Assessment
ROE – Rules of Engagement
Scope creep – When the ROE change during the contract duration
SAQ – Self Assessment Questionnaire
NDA – Non disclosure agreements

Assessment Types

- **Goal-based / objective-based assessment**
  - Testing a new security design
  - Testing changes to IT service infrastructure
  - Application testing
  - Pre-production testing
  - Pre-M&A / Post-M&A corporate valuation assessment
- **Compliance based assessment**
  - Legal requirements
  - Standards requirements
  - May require using a specific testing provider or assessor
- **Red-team assessment**
  - **More targeted** than normal penetration tests
  - Testing team acts like true attacker
  - The organization’s security team is referred to as **Blue-team** and should be active in **defending the network**
  - Targeting sensitive data systems to acquire data
  - **Does not provide complete view** of an organization’s IT security
    - Red-team will **only attempt some vectors** of attack as opposed to white-box testing
    - Red-team does not want to set off alerts / defensive security systems
- **White-box / crystal-box / full knowledge assessments**
  - Assessors can see everything in the environment relevant to scope
    - Network diagrams
    - Lists of systems and services
    - IP network ranges
    - User accounts and privileged accounts

    - Credentials are available in a **credentialed scan**
    - Saves time for assessors to map the network themselves
    - Allows access to resources that assessors may otherwise miss
- **Black-box / zero knowledge assessments**
    - Information about the IT environment is not provided
    - Time consuming
    - May **not provide complete view** of organizational IT security
- **Grey-box assessment**
    - Half way between grey and black-box testing
    - Some information may be provided to assure completeness
- **Adversaries**
    - Script kiddies
    - Hactivists / Hacking groups
    - Professional black hats
    - Organized crime
    - APT Advanced Persistent Threat / Nation State

Rules of Engagement

Purpose Of Engagement Scoping

- **Defines a timeline** for the engagement
- Schedule of **time of day or week** to test
- Defines locations / systems / applications or other targets **in scope** or **excluded from scope**
- Third-party / cloud providers may be in scope or excluded

Data Handling Requirements

- Exposing legally protected data must be prevented
- Destruction of data post-engagement reduces the chances of data loss
- Non-disclosure agreement stipulations can affect communication with organization members

Expected Behaviour

- Target may allow testers to **bypass security controls** such as
    - IT activities such as **active blue-team** responses
    - Whitelist testers **through IPS** to allow more access than would normally be initially possible
    - Whitelist testers **through WAF**
    - Whitelist testers **through NAC**

    - Bypassing **certificate pinning** to allow MiTM attacks
    - Whitelist to VPN
- Target security team may or may not be active during the test
- Setting engagement waypoints to initiate communication with the target contacts

Available Resources

- Resources may be allocated to the pentesting team during white / grey box engagements
    - Workstations
    - Network schematics
    - Software / service versions
    - User accounts / credentials

Legal Concerns

- Regulatory concerns may define some systems **off-limits for testers**
- 3rd party public cloud services need to authorize pentests against their infrastructure
- Some hardware on the target premises may be owned by a 3rd party and may **require explicit permission** to pentest
- Jamming frequency ranges may have FCC restrictions
- Police may be called on the pentester during a physical pentest / dumpster dive
- Pentester may want to carry a copy of contract and contact information
- **Federal law / international laws**
    - May restrict **ROE**
    - Target infrastructure may be located in other international jurisdictions
    - **UK Computer Misuse Act (CMA)** (1990) includes criminal penalties for exploit toolkits (legal grey area)
    - **German Law Section 202c** (2007) forbids possession of password cracking software
    - **USA**
        - The **Export Administration Regulations (EAR) Supplement No. 1 Part 740** limits the exportation of encryption software
        - **Countries** are categorized into groups
            - **B –** Relaxed encryption export rules
            - **D:1 –** Strict export rules
            - **E:1 –** Considered terrorist
            - **740 Supp 1.pdf** can be downloaded with full country list

Communication

- Timeframe for assessors to report findings
- Communication contacts and information channels / escalation path

- Accident reporting in case of breach of ROE
- Critical vulnerability or existing compromise reporting
- Agree on a CVSS level that determines a vulnerability should be reported immediately
- Personnel allowed to engage in assessment and / or request information from inside the company

Wireless

- **SSIDs** that are in scope
- **MAC addresses** that are in scope

Legal Aspects of Pentest Contracting

Types Of Agreements

- **SOW –** Statement of work
- **SOO –** Statement of objectives
- **PWS –** Performance work statements
- **MSA –** Master service agreement
  - Common for long-term contracts / support contracts between parties
- **NDA –** Non-disclosure agreements
- **Non-complete agreements**
  - Asks you not to engage with other competitors
  - May have duration of effect
  - Contract between the assessor and client organization
    - Disclaimers for the **duration of validity** of the assessment

Purposes For Agreements

- **Limiting the liability** of assessors
  - Indemnification language releases the tester from liability
- **Authorization**
  - 3rd party authorization maybe required for cloud resources or other internal infrastructure
- **Legal concerns**

Compliance Based Assessments

Overview Of Compliance Based Assessments

- Compliance regulations for organizations in **specific industries**
  - Finance, health, education, payment processing, public entities

- Sometimes easier to perform since the **criteria is clearly stated**
- Sometimes the **legal terminology is vague** and therefore more difficult to determine if compliance is attained
- **Data isolation is important** due to the protected nature of data under federal laws

HIPPA – Health Insurance Privacy Protection Act

- Does not directly require penetration testing
- Does require risk assessment which drives testing
- **NIST SP 800-66** An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

FERPA – Family Education And Privacy Act

- Regulates how **institutions structure and manage their IT**
- Requires vulnerability scan and remediation of cloud-based databases
- FERPA demands that **information cannot be disclosed without student consent**
- https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

SOX – Sarbanes Oxley Act

- US Federal law that sets standards for US public company boards, management and accounting firms
- Requirement of **annual security control testing**
  - Authentication
  - Network security

GLBA – Gramm-Leach-Bliley Act

- Regulates how **financial institutions** handle **use of personal data**
- Requires **written Information Security plans** that describe processes and efforts intended to protect information
- Requires **testing and documentation**
- Requires **continuous monitoring**

PCI-DSS Payment Card Industry Data Security Standard

- **CDE –** Cardholder Data Environments
- Requires organizations to **implement pentest annually or after changes to the system**
- Based on industry pentest approaches in **NIST SP 800-115**
- Requires testing from **internal and external network**
- Requires testing to **validate any network segmentation and scope** reduction controls

- Requires **application layer tests** to include vulnerabilities listed in section 6.5
  - SQL Injection
  - Buffer overflow
  - Insecure cryptographic storage
  - Insecure communications
  - Improper error handling
  - Cross-site scripting
  - Cross site request forgery
  - Broken authentication
  - Improper access controls
- Requires competent **appliance testing** and **OS testing**
- Requires review of **threats and vulnerabilities experienced in past 12 months**
- Requires **retention of pentest results** and **documentation of remediation activities**
- See **PCI-DSS Version 3.2**

FIPS Federal Information Processing Standard

- **FIPS 140-2** Security Requirements for Cryptographic Modules
- Key management software
- **Pre-certified environments** can provide compliance documentation

Scoping Using Frameworks & Standards

Scoping should start with a full knowledge of the most rigorous IT security standards, and contain approaches and methods for checking all aspects of the target that have been approved by the organization.

Penetration Testing Frameworks

- **PTES – Penetration Testing Execution Standards**
  - http://www.pentest-standard.org/index.php/Main_Page
- **OSSTMM – Open Source Security Testing Methodology Manual**
  - https://www.isecom.org/research.html
- **NIST – SP 800-115**
  - https://www.nist.gov/publications/technical-guide-information-security-testing-and-assessment
- **OWASP – The OWASP Testing Framework**
  - https://owasp.org/www-project-web-security-testing-guide/
  - https://owasp.org/www-project-mobile-security-testing-guide/
- **ISSAF – Information System Security Assessment Framework**
  - https://untrustednetwork.net/files/issaf0.2.1.pdf

Scoping Guidelines

- **Crest –** A guide for running an effective Penetration Testing programme
    - https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf
- **SANS –** Guidelines for Developing Penetration Rules of Behavior
    - https://www.sans.org/reading-room/whitepapers/testing/paper/259
- **PCI Security Standards Council –** Penetration Testing Guidance
    - https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf