Avv. Giuseppe Serafini
Law Firm
G. | S.
L. | F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Penetration Testing:

tra consenso dell'avente diritto e profili problematici di responsabilità civile.

ISACA – Roma Chapter
17.05.2016

Avv. Giuseppe Serafini
Law Firm

G. | S.
L. | F.

ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Agenda

- Introduzione.
- Information Security
- Penetration Testing
- Legal Penetration Testing
- Penetration Test Model Clauses
- Q. & A.

About

- Avvocato del Foro di Perugia
- Perf. UNIMI - Cloud, Data Protection, Digital Forensics
- BSI ISO/IEC 27001:2013 Lead Auditor
- Master Privacy Officer
- European Certificate on Cybercrime Evidence

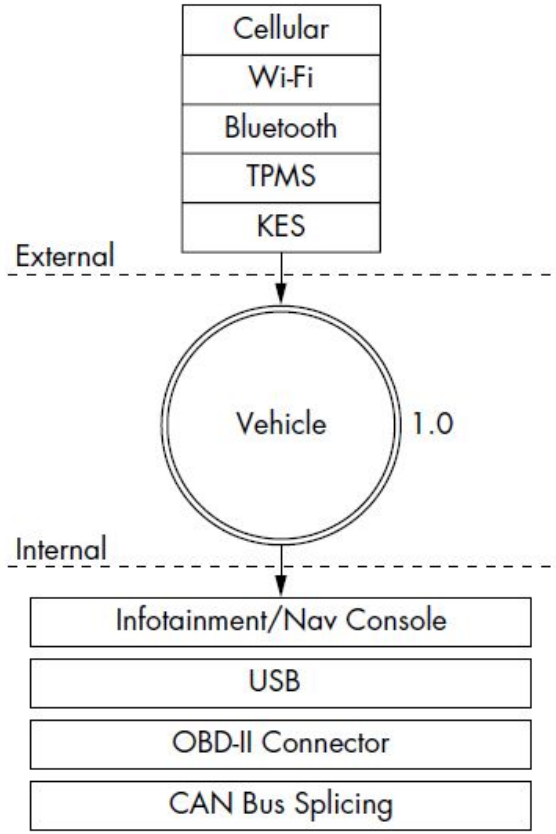
- D.F.A. - Digital Forensics Alumni
- C.S.A. - Cloud Security Alliance
- CLUSIT - Associazione Italiana per la Sicurezza Informatica.
- $(ISC)^2$ - International Information Systems Security Certification Consortium.

Tag

Cyber Crime; Loss; ISACA; Ethical Hacking; IoT; Information Security; ISO 27000; 27001; 27002; 27034,1-2; 27037; PDCA; Penetration Testing; Terms & Conditions May Apply; Vulnerability Assessment; PCI - DSS; RoE; Tipologie di Pen-Test; Black Box; White Box; Grey Box; NIST; Cod. Civ. Obbligazioni di mezzi Vs. Obbligazioni di Risultato; Fasi del Pen-Test; Data Protection; OWASP; Out of Jail; SQL Injection; Kali Linux; Bactrack; BackBox; OSSTM; Diligenza Qualificata;

The Car Hacker's handbook.

A Guide for the Penetration Tester - Copyright © 2016 by C. Smith.

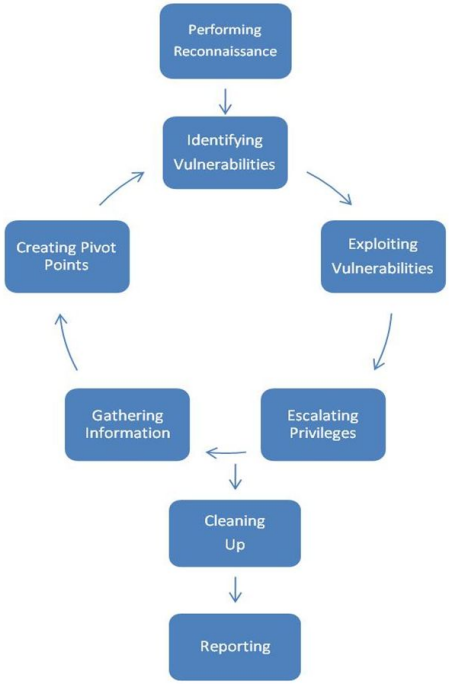


- Shut down;
- Spy occupants;
- Unlock;
- Steal;
- Track;
- Thwart safety systems;
- Install malware;

"Cyber Attack" - Loss

Penetration Test

A **test** methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, ***attempt to circumvent the security features of an information system.***



For determining:

- ❑ How well the system tolerates real world-style attack patterns;
- ❑ The likely level of sophistication an attacker needs to successfully compromise the system;
- ❑ Additional countermeasures that could mitigate threats against the system;
- ❑ Defenders' ability to detect attacks and respond appropriately.

**** NIST - Special Publication 800-53A - Guide for Assessing the Security Controls in Federal Information Systems and Organizations - NIST. Special Publication 800-115 - Technical Guide to Information Security Testing and Assessment.***

IT Laws

- **Codice Penale Italiano;**
  - Art. 50;
  - 615 ter;
  - 635 bis;
- **Codice Civile;**
  - Contratto (Art. 1321);
  - Diligenza (Art. 1176); (Art. 2236)
  - Approvazione espressa di clausole (Artt. 1342 e 1342);
  - Appalto di servizi Vs. Prestazione d'opera intellettuale;
  - Responsabilita' Contrattuale (1218);
  - Responsabilita' extracontrattuale (art. 2043);
- **Codice in materia di protezione dei dati personali;**
  - Art. 29 / Art. 30;
  - Art. 31;
  - Art. 167;
- Allegato B al Codice Privacy;
- Regolamento EU 679/2016;
- D.Lgs 231/2001 - Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica (Art. 24 bis);

Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Quid Juris?

(1). - Vi sono obblighi "normativi o contrattiuali" di procedere ad operazioni di penetration test?
(2). - Che cosa prevede lo standard PCI-DSS a proposito del Penetration Test? Che relazione c'e' tra lo standard ISO/IEC 27001 e lo standard PCI-DSS?
(4). - Il "Penetration Tester" si obbliga a **"riuscire a violare"** le protezioni del committente o a **"tentare di violare"** le protezioni del committente? **-** Se si obbliga a tentare di violare le protezioni di un sistema informativo quale e' la misura dell'adempimento?
(5). - Quali tipologia di prestazioni sono deducibili nell'ambito di obbligazioni relative allo svolgimento di P. T? (hanno tutte la stessa difficolta' intrinseca?) Cosa significa ***"intuitu personae"?***
(6). - Quale e' il livello di diligenza richiesto nell'esecuzione di operazioni di Pen Test?
(7). - Chi risponde dei danni preveduti come **possibili** dal penetation tester?
(8). - A quali fattispecie contrattuale devono ricondursi, dal punto di vista della responsabilita' civile le prestazioni relative all'esecuzione di operazioni di P.T. (Si tratta di obbligazioni di mezzi o di obbligazioni di risultato,?
(9). - Si versa in ipotesi di responsabilita' contrattuale o extracontrattuale in caso di danno ?
(10). - Quali **strumenti** devono essere usati per l'esecuzione di operazioni di P.T.?
(11). - Chi risponde per il danno causato da errori di programmazione dello strumento *software* impiegato per l'esecuzione di operazioni di P.T.?
(12). - Che efficacia hanno le clausole di esonero da responsabilita' stipulate con il destinatario delle operazioni del P.T.? L'accettazione di queste clausole impone specifiche modalita' di sottoscrizione? E' corretto far accettare ai sensi dell'art. 1341 e 1342 cod civ. tutte le clausole di un contratto?
(13). - Qual'e' l'obbligo di Segretezza imposto al Penetration Tester nell'ambito della esecuzione delle operazioni di test?
(**14). -** Dal punto di vista della protezione dei dati personali (Privacy) quale ruolo assume il Penetration Tester nell'esecuzione delle prestazioni contrattualmente dedotte?
(15). - Quali sono i contenuti indispensabili del contratto con il quale si affida ad un soggetto l'incarico di svolgere operazioni di Pen Test?
(16). - Che relazione c'e' tra il contenuto del contratto che conferisce l'incarico di realizzare operazioni di P. T. e l'applicabilita' della scriminante del consenso dell'avente diritto di cui all'art. 50 del Cod. Pen?
(17). - Quale e' il soggetto legittimato ad esprimere la volonta' di applicare la scriminante di cui all'art. 50 per conto di una Societa'?
(18). - Quali sono le norme penalistiche applicabili alle condotte realizzate "out of scope" dal Penetration Tester durante l'incarico?

Art. 50 Cod. Pen.

Consenso dell'avente diritto.

(1). - Non è punibile chi lede o pone in pericolo un diritto, col consenso della persona che può validamente disporne.

** Al fine della sua efficacia scriminante, il consenso, deve essere libero, vale a dire, espresso con volontà libera, non viziata cioè, da errore, violenza o dolo e deve essere perfettamente e compiutamente informato - consapevolezza di ciò cui si acconsente. Deve essere espresso all'esterno, e deve essere attuale, cioè deve esistere al momento del fatto. Si considera legittimato a prestare il consenso il titolare dell'interesse protetto dalla norma, in possesso della capacità di intendere e di volere, da accertarsi caso per caso.*

Bibliografia

- **ISO/IEC 27000 -** Information security management systems Overview and vocabulary;
- **ISO/IEC 27001 -** Information technology - Security Techniques Information security management systems - Requirements;
- **ISO/IEC 27002 -** Code of practice for information security management;
- **ISO/IEC 27034-1** Information technology - Security techniques Application security - Part 1: Overview and concepts;
- **ISO/IEC 27034-2** Information technology - Security techniques Application security - Part 2: Organization normative framework;
- **NIST - SP 800-53A** Guide for Assessing the Security Controls in Federal Information Systems and Organizations;
- **NIST. SP 800-115 -** Technical Guide to Information Security Testing and Assessment.
- **PCI - DSS -** Payment Card Industry Data Security Standard V.3.1;
- **PCI - DSS -** Information Supplement: Requirement 11.3 Penetration Testing;
- **OSSTMM -** The Open Source Security Testing Methodology Manual;
- **(OWASP)** Open Web Application Security Project - Testing Guide;
- **ISACA VENICE** Chapter - Vulnerability Assessment e Penetration Test Linee guida per l'utente di verifiche di terze parti sulla sicurezza ICT;
- Penetration Testing Execution Standard - **www.pentest-standard.org**

Definitions

2.19 - Information security. - Preservation of confidentiality (2.9), integrity (2.25) and availability (2.7) of information..

2.24 - Information security risk. - Potential that a threat (2.45) will exploit a vulnerability (2.46) of an asset (2.3) or group of assets and thereby cause harm to the **organization.**

A12.6 - Technical Vulnerability Management - Objective: To prevent exploitation of technical vulnerabilities.

A.12.6.1 - Management of technical vulnerabilities - Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

A.14.2.3 - Technical review of applications after operating platform changes Control - When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

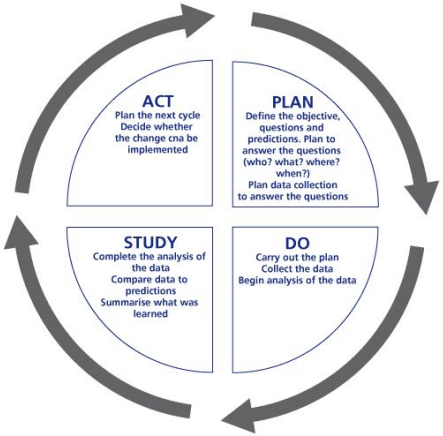
A.14.2.8 - System security testing - Control Testing of security functionality shall be carried out during development.

3.3 - Application - IT solution, including application software, application data and procedures, designed to help an organization's users perform particular tasks or handle particular types of IT problems by automating a business process or function

3.8 - Application Security Control - ASC - Data structure containing a precise enumeration and description of a security activity and its associated verification measurement to be performed at a specific point in an application's life cycle.

I.S.M.S.

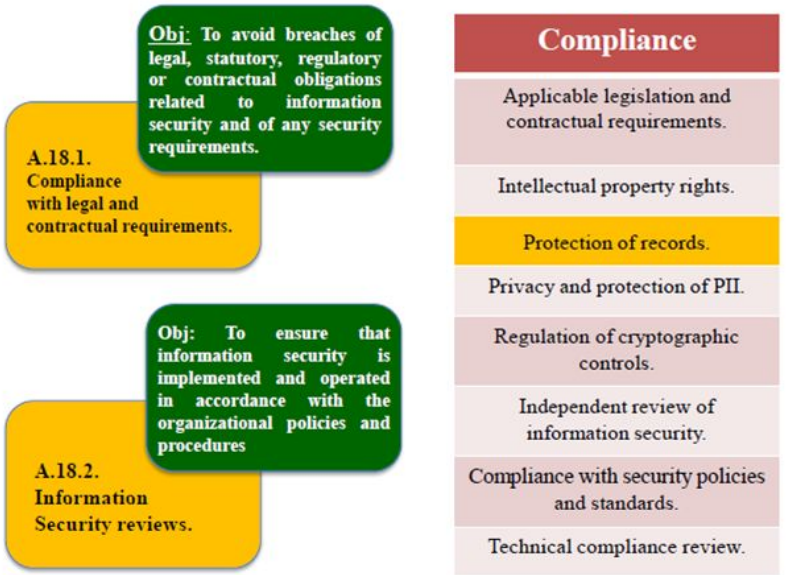
Audit: systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.



ISO/IEC - 27001- 27002

ISO/IEC - 27002

Compliance reviews also cover, for example, penetration testing and vulnerability assessments, which might be carried out by independent experts **specifically contracted** for this purpose.



Penetration testing and vulnerability assessments provide a snapshot of a system in a specific state at a specific time.

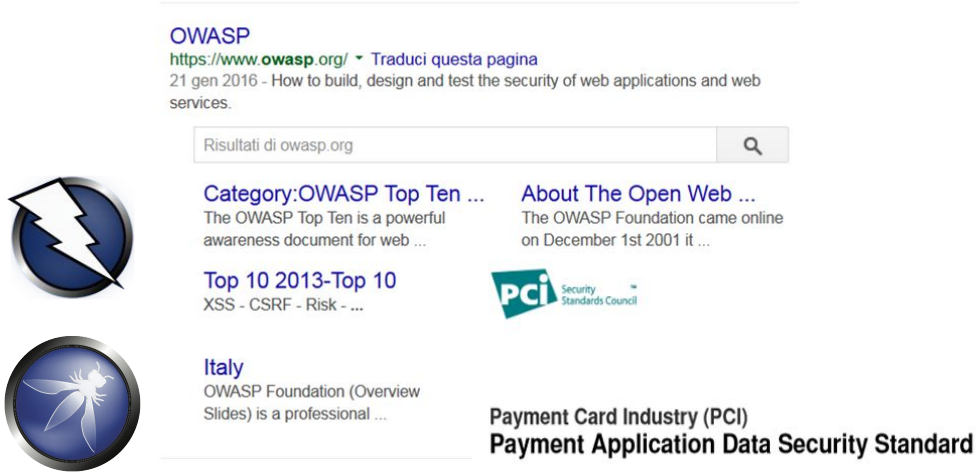
The snapshot is limited to those portions of the system actually tested during the penetration attempt(s).

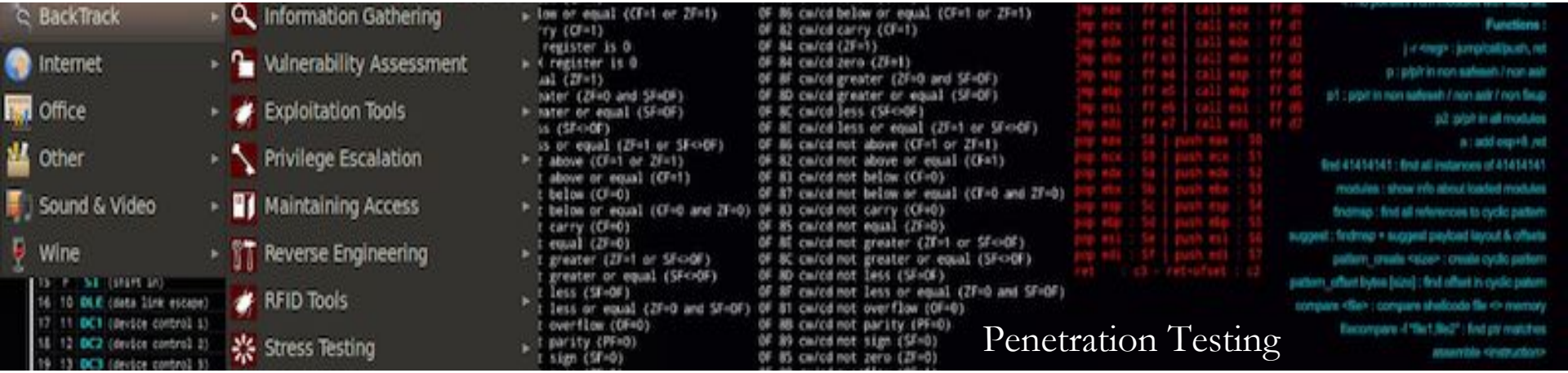
Steps

1). - Spear-Phishing Attack Vectors
2). - Website Attack Vectors
3). - Infectious Media Generator
4). - Create a Payload and Listener
5). - Mass Mailer Attack
6). - Arduino-Based Attack Vector
7). - SMS Spoofing Attack Vector
8). - Wireless Access Point Attack Vector
9). - QRCode Generator Attack Vector

Pre-engagement
Intelligence Gathering
Threat Modeling
Vulnerability Analysis
Exploitation
Post Exploitation
Reporting

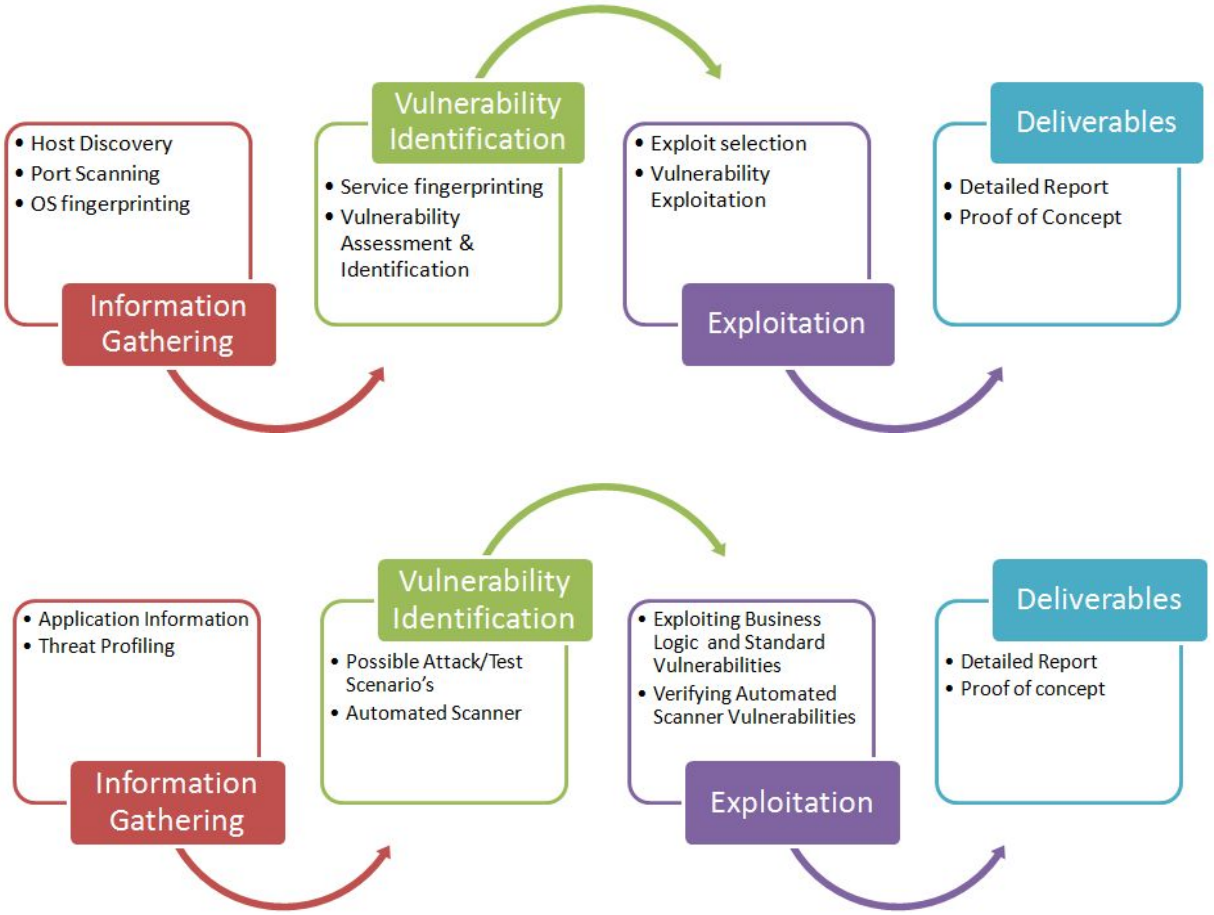
Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security





Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Penetration Test / App



Tipologie di Pen-Test

BLIND: quando l'attaccante non conosce minimamente il sistema da analizzare. E' conosciuto solamente il target (Indirizzi IP o URL)

DOUBLE BLIND: simile a quello precedente con la differenza che alcune persone del committente sono al corrente del test. Viene tipicamente usato per verificare se il personale interno dedicato alla sicurezza è "vigile" e svolge con diligenza il proprio lavoro.

GRAY BOX: sia l'attaccante che l'attacco sono pienamente a conoscenza sia del sistema informatico da analizzare che delle modalità di attacco. Viene utilizzato quando si analizza il proprio sistema interno.

DOUBLE GRAY BOX: è un gray box che prevede la conoscenza delle credenziali di accesso. Viene usato per testare l'accesso ad informazioni più riservate rispetto al suo livello da parte di un utente.

TANDEM: analisi del codice. Chi verifica e chi crea il codice collaborano

REVERSAL: test a uso interno. Il tester ha una grande quantità di informazione il committente non sa i tempi e le metodologie con cui verrà attaccato.

Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Tools.

Back Track
Back Box
KALI Linux
Etc.

PCI - Methodology

- 4 **Methodology**
- **4.1 Pre-Engagement**
- 4.1.1 Scoping
- 4.1.2 Documentation
- 4.1.3 Rules of Engagement
- 4.1.4 Third-Party/Cloud Environments
- 4.1.5 Success Criteria
- 4.1.6 Review of Threats and Vulnerabilities
- 4.1.7 Avoid scan interference on security appliances.
- **4.2 Engagement: Penetration Testing**
- 4.2.1 Application Layer
- 4.2.2 Network Layer
- 4.2.3 Segmentation
- 4.2.4 What to do when cardholder data is encountered
- 4.2.5 Post-Exploitation
- **4.3 Post-Engagement**
- 4.3.1 Remediation Best Practices
- 4.3.2 Retesting Identified Vulnerabilities
- 4.3.3 Cleaning up the Environment
- 4.4 Additional Resources
- **5 Reporting and Documentation**
- 5.1 Identified Vulnerability Reporting
- 5.1.1 Assigning a Severity Score
- 5.1.2 Industry Standard References
- 5.2 Reporting Guidelines
- 5.2.1 Penetration Test Report Outline
- 5.2.2 Retesting and Report Outline
- **5.3 Evidence retention**
- 5.3.1 What is considered evidence?
- 5.3.2 Retention
- 5.4 Penetration Test Report Evaluation Tool

PCI-DSS - R.o.E.

Prior to the commencement of any testing, it is important to document and agree upon the conditions in which testing is to be performed and the degree of exploitation, if any, that is permitted.

• During what time window will testing need to be performed?
• Are there any legacy systems that have known issues with automated scanning? If so, how should testing be performed against these systems?
• Is there a preferred method of communicating about scope and issues encountered during the engagement?
• Does the entity want updates regarding ongoing exploitation of systems during the test? If so, the entity will need to determine whether they will or will not act upon such information or make changes to the environment. The entity may also want to implement its incident response plan in response to an exploit.
• Are there security controls that would detect or prevent testing? Consider whether these should be disabled or configured to not interfere during testing.
• If passwords or other sensitive data are compromised during the testing, does the tester need to disclose a list of all passwords and/or sensitive data accessed?
• If equipment owned by the tester is to be connected to the organization's network, what steps must be taken to ensure the equipment does not pose a threat to the environment?
• Does the tester need to provide all IP addresses from which testing will originate?
• Will sensitive data shown to be accessible during the test be retained by the tester during and after the penetration test?
• What steps will be taken if the tester detects a previous or active compromise to systems being tested?

OSSTM - R.o.E.

• **Contracts** must clearly explain the limits and dangers of the security test as part of the statement of work; in the case of remote testing, the contract must include the origin of the Analysts by address, telephone number or IP address.
• The client must provide a signed statement which provides testing permission exempting the Analysts from trespass within the scope, and damages liability to the cost of the audit service with the exception where malicious activity has been proven.
• The contract must include clear, specific permissions for tests involving survivability failures, denial of service, process testing, and social engineering.
• The scope must be clearly defined contractually before verifying vulnerable services.
• Performing security tests against any scope without explicit written permission from the target owner or appropriate authority is strictly forbidden.
• Contracts should limit liability to the cost of the job, unless malicious acivity has been proven.
• The Analysts are required to know their tools, where the tools came from, how the tools work, and have them tested in a restricted test area before using the tools on the client organization.
• Verified limitations, such as discovered breaches, vulnerabilities with known or high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may immediately ***endanger lives, discovered during testing must be reported to the customer with a practical solution as soon as they are found.***
• Client notifications are required whenever the Analyst changes the testing plan, changes the source test venue, has low trust findings, or any testing problems have occurred. Notifications must be provided previous to running new, dangerous, or high traffic tests, and regular progress updates are required.

*** - The Open Source Security Testing Methodology Manual (Pag. 40)**

Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Legal Penetration Testing

Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Quid Juris?

(1). - Vi sono obblighi "normativi o contrattiuali" di procedere ad operazioni di penetration test?
(2). - Che cosa prevede lo standard PCI-DSS a proposito del Penetration Test? Che relazione c'e' tra lo standard ISO/IEC 27001 e lo standard PCI-DSS?
(4). - Il "Penetration Tester" si obbliga a **"riuscire a violare"** le protezioni del committente o a **"tentare di violare"** le protezioni del committente? **-** Se si obbliga a tentare di violare le protezioni di un sistema informativo quale e' la misura dell'adempimento?
(5). - Quali tipologia di prestazioni sono deducibili nell'ambito di obbligazioni relative allo svolgimento di P. T? (hanno tutte la stessa difficolta' intrinseca?) Cosa significa ***"intuitu personae"?***
(6). - Quale e' il livello di diligenza richiesto nell'esecuzione di operazioni di Pen Test?
(7). - Chi risponde dei danni preveduti come **possibili** dal penetation tester?
(8). - A quali fattispecie contrattuale devono ricondursi, dal punto di vista della responsabilita' civile le prestazioni relative all'esecuzione di operazioni di P.T. (Si tratta di obbligazioni di mezzi o di obbligazioni di risultato,?
(9). - Si versa in ipotesi di responsabilita' contrattuale o extracontrattuale in caso di danno ?
(10). - Quali **strumenti** devono essere usati per l'esecuzione di operazioni di P.T.?
(11). - Chi risponde per il danno causato da errori di programmazione dello strumento *software* impiegato per l'esecuzione di operazioni di P.T.?
(12). - Che efficacia hanno le clausole di esonero da responsabilita' stipulate con il destinatario delle operazioni del P.T.? L'accettazione di queste clausole impone specifiche modalita' di sottoscrizione? E' corretto far accettare ai sensi dell'art. 1341 e 1342 cod civ. tutte le clausole di un contratto?
(13). - Qual'e' l'obbligo di Segretezza imposto al Penetration Tester nell'ambito della esecuzione delle operazioni di test?
(**14). -** Dal punto di vista della protezione dei dati personali (Privacy) quale ruolo assume il penetration tester nell'esecuzione delle prestazioni contrattualmente dedotte?
(15). - Quali sono i contenuti indispensabili del contratto con il quale si affida ad un soggetto l'incarico di svolgere operazioni di Pen Test?
(16). - Che relazione c'e' tra il contenuto del contratto che conferisce l'incarico di realizzare operazioni di P. T. e l'applicabilita' della scriminante del consenso dell'avente diritto di cui all'art. 50 del Cod. Pen?
(17). - Quale e' il soggetto legittimato ad esprimere la volonta' di applicare la scriminante di cui all'art. 50 per conto di una Societa'?
(18). - Quali sono le norme penalistiche applicabili alle condotte realizzate "out of scope" dal penetration tester durante l'incarico?

Reg. E.U. *27.04.2016* Nr. 679.

Art. 32 - Sicurezza del Trattamento.

(1). - Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

(a). - la pseudonimizzazione e la cifratura dei dati personali;
(b). - la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
(c). - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
(d). - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento

Reg. E.U. *27.04.2016* Nr. 679. C (81)

Il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino *garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento*.

L'esecuzione dei trattamenti da parte di un responsabile del trattamento dovrebbe essere disciplinata da **un contratto o da altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri che vincoli il responsabile del trattamento al titolare del trattamento.

Intuitu Personae

The following are some examples of common ***penetration testing certifications:***

- ❑ Offensive Security Certified Professional (OSCP);
- ❑ Certified Ethical Hacker (CEH);
- ❑ Global Information Assurance Certification (GIAC) Certifications (e.g., GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), or GIAC Exploit Researcher and Advanced Penetration Tester (GXPN);
- ❑ CREST Penetration Testing Certifications;
- ❑ Communication Electronic Security Group (CESG) IT Health Check Service (CHECK) certification.

Payment Card Industry

Requisito 11 - Eseguire regolarmente test dei sistemi e processi di protezione. 11.3 Implementare una metodologia per il test di penetrazione che preveda quanto segue:

• Sia basata sugli approcci ai test di penetrazione accettati dal settore (ad esempio, NIST SP800-115);
• Includa la copertura dell'intero perimetro dell'ambiente dei dati dei titolari di carta e i dei sistemi critici;
• Includa i test dall'interno e dall'esterno della rete;
• Comprenda i test per convalidare eventuali controlli di segmentazione e riduzione della portata;
• Definisca i test di penetrazione a livello di applicazione affinché includano almeno le vulnerabilità elencate nel requisito 6.5;
• Definisca i test di penetrazione a livello di rete affinché includano componenti che supportano le funzioni di rete nonché i sistemi operativi;
• Includa la revisione e la valutazione delle minacce e delle vulnerabilità verificatesi negli ultimi 12 mesi;
• Specifichi la conservazione dei risultati dei test di penetrazione e dei risultati delle attività di correzione.

Cod. Civ. Art. 1337.
Trattative e responsabilità precontrattuale.

(1). - Le parti, nello svolgimento delle trattative e nella formazione del contratto, devono comportarsi secondo buona fede.

Cod. Civ. Art. 1325
Indicazione dei Requisiti

(1). - I requisiti del contratto sono: 1) l'accordo delle parti [1326]; 2) la causa [1343]; 3) l'oggetto [1346]; 4) la forma, quando risulta che è prescritta dalla legge sotto pena di nullità [1350, 1352].

Cod. Civ. - Art. 1176.
Diligenza nell'adempimento.

(1). - Nell'adempiere l'obbligazione il debitore deve usare la diligenza del buon padre di famiglia.

(2). - Nell'adempimento delle obbligazioni inerenti all'esercizio di **un'attività professionale**, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata.

Cod. Civ. - Art. 2236
Responsabilità del prestatore d'opera

(1). - Se la prestazione implica la soluzione di problemi tecnici di speciale difficoltà, il prestatore d'opera non risponde dei danni, se non in caso di dolo o di colpa grave

Cass. n. 8546/2005

In tema di responsabilità del prestatore di opera intellettuale, poichè l'art. 1176 c.c. fa obbligo al professionista di usare, nell'adempimento delle obbligazioni inerenti la sua attività professionale, la diligenza del buon padre di famiglia, il medesimo risponde normalmente per colpa lieve; nella sola ipotesi che la prestazione implichi la soluzione di problemi tecnici di particolare difficoltà, l'art. 2236 c.c. prevede un'attenuazione di responsabilità, nel senso che il professionista è tenuto al risarcimento del danno unicamente per dolo o colpa grave.

Pertanto, la prova dell'esistenza di tale presupposto, derogando alle norme generali sulla responsabilità per colpa, incombe al professionista; peraltro, la domanda di risarcimento del danno, basata sulla colpa grave, contiene quella per colpa lieve, senza che, pertanto, la pronuncia di condanna fondata su colpa lieve del professionista possa dar luogo a vizio di ultrapetizione.

Cod. Civ. Art. 1341.
Condizioni generali di contratto.

(1). - Le condizioni generali di contratto predisposte da uno dei contraenti sono efficaci nei confronti dell'altro, se al momento della conclusione del contratto questi le ha conosciute o avrebbe dovuto conoscerle usando l'ordinaria diligenza.
(2). - In ogni caso non hanno effetto, se non sono specificamente approvate per iscritto, le condizioni che stabiliscono, a favore di colui che le ha predisposte, limitazioni di responsabilità , facoltà di recedere dal contratto o di sospenderne l'esecuzione, ovvero sanciscono a carico dell'altro contraente decadenze , limitazioni alla facoltà di opporre eccezioni, restrizioni alla libertà contrattuale nei rapporti coi terzi , tacita proroga o rinnovazione del contratto, clausole compromissorie o deroghe alla competenza dell'autorità giudiziaria.

Cod. Civ. Art. 1342
Contratto concluso mediante moduli o formulari

(1). - Nei contratti conclusi mediante la sottoscrizione di moduli o formulari, predisposti per disciplinare in maniera uniforme determinati rapporti contrattuali, le clausole aggiunte al modulo o al formulario prevalgono su quelle del modulo o del formulario qualora siano incompatibili con esse anche se queste ultime non sono state cancellate.
(2). - Si osserva inoltre la disposizione del secondo comma dell'articolo precedente.

Cod. Civ. Art. 1218.
Responsabilita' del debitore.

(1). - Il debitore che non esegue esattamente la prestazione dovuta [1176, 1181] è tenuto al risarcimento del danno [1223 ss.], se non prova che l'inadempimento o il ritardo è stato determinato da impossibilità della prestazione derivante da causa a lui non imputabile [1221, 1229, 1257, 1307, 1557, 1558, 1673, 1693, 1821, 2740; 160 disp. trans.].

Cod. Civ. Art. 2043
Risarcimento per fatto illecito

(1). - Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno [2058].

La qualificazione come contrattuale della responsabilità del Penetration tster determina, in particolare:

(a). - l'applicabilità della regola di cui all'art. 1218 c.c. in tema d'inadempimento, essendo quindi il debitore inadempiente a dover dimostrare che l'inadempimento, o il ritardo, è stato determinato dall' impossibilità della prestazione derivante da causa a lui non imputabile;
(b). - l'operatività del termine di prescrizione decennale;
(c). - la risarcibilità del danno circoscritta, ai sensi dell'art. 1225 c.c., a quello prevedibile al tempo in cui è sorta l'obbligazione, in assenza di dolo in capo al debitore inadempiente;
(d). - l'operatività non solo del limite di responsabilità previsto all'art. 2236 c.c., nei casi, quindi, di dolo e colpa grave nell'ipotesi di risoluzione di problemi tecnici di particolare difficoltà, ma anche del limite di cui all'art. 1176, II comma c.c., essendo il Penetration Tester assimilabile ad un debitore qualificato e, pertanto, onerato di un dovere di diligenza qualificata e superiore a quella del buon padre di famiglia, con la conseguente responsabilità anche per colpa lieve se, nell'esecuzione delle sue prestazioni, abbia provocato un danno per omissione di diligenza.

Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Penetration Testing Contractual Clauses

doc. all.1

(Pre) Requisiti di sicurezza.

Il sottoscritto, K. Mitnick in qualità di Legale Rapp.te. p.t. dell'Impresa BLUE TEAM Ltd., dichiara quanto segue:

• gli elementi dell'Impresa che svolgono attività in forza del contratto di **"Prestazione d'opera intellettuale"** con ALFA si impegnano ad osservare le previsioni dello standard internazionale ISO/IEC 27001
• tutti i suddetti elementi hanno sottoscritto e consegnato all'Impresa la "**Dichiarazione di presa d'atto degli obblighi di segreto** (doc. all. 2)";
• l'Impresa si impegna a far sottoscrivere e a farsi consegnare la menzionata dichiarazione anche dagli elementi che verranno incaricati di svolgere attività presso la Banca d'Italia nel prosieguo del rapporto contrattuale;
• l'Impresa si impegna a custodire le menzionate dichiarazioni e a esibirle prontamente alla Banca d'Italia su sua semplice richiesta.

In fede.
data SOCIETÀ
(indicazione in chiaro della qualifica e del nome del firmatario).

doc. all.2

Dichiarazione di presa d'atto degli obblighi di segreto professionale nell' ambito dei progetti di ALFA

Il sottoscritto Thomas A. Anderson, addetto all'Impresa Blue Team Ltd., per incarico della quale svolge attività in forza del contratto di "Prestazione d'opera intellettuale" stipulato dalla predetta Società con ALFA, dichiara di essere pienamente a conoscenza che, nell'espletamento di detta attività è vincolato/a al segreto professionale concernente:

- l'obbligo di riservatezza su tutte le informazioni comunque acquisite in occasione dell'esercizio della propria attività;
- il divieto di divulgazione, a qualsiasi titolo e nei confronti di chiunque, di informazioni o documentazione comunque ottenute in occasione dell'esercizio della propria attività.

Gli obblighi e i divieti sopra menzionati permangono anche dopo la cessazione dell'attività in favore di ALFA.

In fede.
(data) (firma)

Avv. Giuseppe Serafini
Law Firm
G. S.
L. F.
ISO/IEC 27001 Lead Auditor - IT Laws, Forensics, Privacy & Security

Quid Juris?

(1). - Vi sono obblighi "normativi o contrattiuali" di procedere ad operazioni di penetration test?
(2). - Che cosa prevede lo standard PCI-DSS a proposito del Penetration Test? Che relazione c'e' tra lo standard ISO/IEC 27001 e lo standard PCI-DSS?
(4). - Il "Penetration Tester" si obbliga a **"riuscire a violare"** le protezioni del committente o a **"tentare di violare"** le protezioni del committente? **-** Se si obbliga a tentare di violare le protezioni di un sistema informativo quale e' la misura dell'adempimento?
(5). - Quali tipologia di prestazioni sono deducibili nell'ambito di obbligazioni relative allo svolgimento di P. T? (hanno tutte la stessa difficolta' intrinseca?) Cosa significa ***"intuitu personae"?***
(6). - Quale e' il livello di diligenza richiesto nell'esecuzione di operazioni di Pen Test?
(7). - Chi risponde dei danni preveduti come **possibili** dal penetation tester?
(8). - A quali fattispecie contrattuale devono ricondursi, dal punto di vista della responsabilita' civile le prestazioni relative all'esecuzione di operazioni di P.T. (Si tratta di obbligazioni di mezzi o di obbligazioni di risultato,?
(9). - Si versa in ipotesi di responsabilita' contrattuale o extracontrattuale in caso di danno ?
(10). - Quali **strumenti** devono essere usati per l'esecuzione di operazioni di P.T.?
(11). - Chi risponde per il danno causato da errori di programmazione dello strumento *software* impiegato per l'esecuzione di operazioni di P.T.?
(12). - Che efficacia hanno le clausole di esonero da responsabilita' stipulate con il destinatario delle operazioni del P.T.? L'accettazione di queste clausole impone specifiche modalita' di sottoscrizione? E' corretto far accettare ai sensi dell'art. 1341 e 1342 cod civ. tutte le clausole di un contratto?
(13). - Qual'e' l'obbligo di Segretezza imposto al Penetration Tester nell'ambito della esecuzione delle operazioni di test?
(**14). -** Dal punto di vista della protezione dei dati personali (Privacy) quale ruolo assume il Penetration Tester nell'esecuzione delle prestazioni contrattualmente dedotte?
(15). - Quali sono i contenuti indispensabili del contratto con il quale si affida ad un soggetto l'incarico di svolgere operazioni di Pen Test?
(16). - Che relazione c'e' tra il contenuto del contratto che conferisce l'incarico di realizzare operazioni di P. T. e l'applicabilita' della scriminante del consenso dell'avente diritto di cui all'art. 50 del Cod. Pen?
(17). - Quale e' il soggetto legittimato ad esprimere la volonta' di applicare la scriminante di cui all'art. 50 per conto di una Societa'?
(18). - Quali sono le norme penalistiche applicabili alle condotte realizzate "out of scope" dal Penetration Tester durante l'incarico?

Conclusioni

Grazie per l'attenzione.

Avv. Giuseppe Serafini
www.giuseppeserafini.legal
giuseppe.serafini@ordineavvocati.perugia.it