

Università degli Studi di Salerno



Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Target Scoping

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Concetti Chiave
- Raccolta dei Requisiti del Cliente
- Preparazione del Test Plan
- Definizione dei Confini del Test
- Definizione degli Obiettivi di Business
- Gestione e Pianificazione di un Progetto

Outline

- **Concetti Chiave**
- Raccolta dei Requisiti del Cliente
- Preparazione del Test Plan
- Definizione dei Confini del Test
- Definizione degli Obiettivi di Business
- Gestione e Pianificazione di un Progetto

Concetti Chiave

- **Scoping**: ambito di valutazione della sicurezza



Concetti Chiave

➤ Il Target Scoping

- Definisce gli obiettivi e l'ambito del processo di penetration testing
- Risponde alle seguenti domande relative a tale processo
 - Cosa sarà valutato?
 - Come avverrà la valutazione?
 - Quali risorse saranno allocate?
 - Quali limitazioni saranno applicate?
 - Quali obiettivi di business saranno garantiti?
 - Come verrà pianificato e schedulato il processo?

Fasi del Target Scoping

1. **Raccolta dei requisiti del cliente:** accumulare quante più informazioni possibili sull'asset da analizzare
 - Attraverso comunicazioni verbali o scritte con il cliente

2. **Preparazione del Test Plan**
 - Modellazione dei requisiti del cliente per farli confluire in un processo di penetration testing strutturato
 - Accordi legali
 - Analisi dei costi
 - Allocazione delle risorse

Fasi del Target Scoping

- 3. Definizione dei confini del test:** determinare le limitazioni a cui deve essere soggetto il processo di penetration testing
- Limitazioni tecnologiche
 - Limitazioni di conoscenza
 - Vincoli formali imposti sull'asset del cliente

Fasi del Target Scoping

4. **Definizione degli obiettivi di business:** allineare la *Business View* del cliente (o dell'organizzazione) con gli obiettivi tecnici del programma di penetration testing

5. **Gestione e pianificazione del progetto:** fornire una tempistica adeguata per ciascuna fase del processo di penetration testing

Outline

- Concetti Chiave
- **Raccolta dei Requisiti del Cliente**
- Preparazione del Test Plan
- Definizione dei Confini del Test
- Definizione degli Obiettivi di Business
- Gestione e Pianificazione di un Progetto

Raccolta dei Requisiti del Cliente

Linee Guida

- Questa fase fornisce generiche linee guida per ricavare dal **cliente** informazioni sull'asset da analizzare
 - Di solito è realizzata attraverso un questionario
 - **Modulo dei Requisiti** (*Maggiori dettagli in seguito...*)
- Un **cliente** può essere un qualsiasi **soggetto legalmente o commercialmente legato all'organizzazione** che ha commissionato l'analisi dell'asset

Raccolta dei Requisiti del Cliente

Linee Guida

- Prima di avviare il processo di penetration testing è fondamentale
 - Identificare tutte le parti interessate
 - Interne ed esterne all'organizzazione (ad es., eventuali terze parti)
 - Analizzare i loro livelli di interesse, aspettativa, importanza ed influenza

Raccolta dei Requisiti del Cliente

Linee Guida

➤ Andrebbero definiti

- Una strategia che tenga in considerazione delle esigenze di tutte le parti coinvolte nel processo di penetration testing
- Un «canale» di comunicazione verso ciascuna parte
 - Per ottenere eventuali informazioni da essa

➤ Obiettivi

- Massimizzare gli effetti positivi del penetration testing
- Mitigare i potenziali impatti negativi del penetration testing

Raccolta dei Requisiti del Cliente

Linee Guida

- Dopo che i requisiti del cliente sono stati identificati e raccolti devono essere validati da quest'ultimo
 - Per rimuovere da essi eventuali informazioni fuorvianti, ambigue o non consone alle richieste del cliente stesso
- Ciò garantirà che il piano di test (**Test Plan**) derivante dai requisiti raccolti sia coerente, completo e consistente con le richieste del cliente

Raccolta dei Requisiti del Cliente

Modulo dei Requisiti

- I requisiti del cliente vengono di solito raccolti tramite un opportuno modulo (o questionario)
 - **Modulo dei Requisiti**
- La creazione del modulo dei requisiti di solito si basa su un elenco di domande
- Questo elenco può essere esteso o abbreviato in base agli obiettivi del cliente



Raccolta dei Requisiti del Cliente

Creazione del Modulo dei Requisiti – Obiettivi

➤ **Raccogliere informazioni di base**

- Nome e indirizzo (fisico) dell'organizzazione
- Sito Web
- Dettagli di contatto
- Indirizzi e-mail
- Numeri di telefono
- Etc

➤ **Determinare i principali obiettivi del progetto di penetration testing**

Raccolta dei Requisiti del Cliente

Creazione del Modulo dei Requisiti – Obiettivi

➤ **Determinare il tipo di penetration testing da condurre**

- Black Box, White Box, etc
- Testing interno o esterno
- Utilizzo o non utilizzo delle seguenti attività
 - *Social Engineering*
 - *Denial of Service (DoS)*
 - *Fake Identity* dei dipendenti
 - Analisi dei sistemi di terze parti
 - Analisi delle informazioni riguardanti i dipendenti
 - Tecniche di post-exploitation (*privilege escalation* ed installazione di *backdoor*)
 - Etc

Raccolta dei Requisiti del Cliente

Creazione del Modulo dei Requisiti – Obiettivi

- **Determinare quanti e quali dispositivi di rete devono essere valutati**
 - Host, firewall, switch, IDS, IPS, etc
- **Determinare quali sistemi operativi, software e tecnologie appartengono all'asset dell'organizzazione**
- **Determinare se sono in atto piani di disaster recovery**
 - Se sì, determinare chi deve essere contattato

Raccolta dei Requisiti del Cliente

Creazione del Modulo dei Requisiti – Obiettivi

- **Determinare chi gli sono amministratori dell'asset**
- **Determinare se bisogna attenersi a requisiti specifici, per essere conformi a standard o metodologie del settore**
 - Se sì, elencare quali
- **Determinare chi sarà il punto di contatto durante il processo di penetration testing**
- **Determinare qual è la timeline per condurre il processo di penetration testing**
- **Determinare qual è il budget per condurre il processo di penetration testing**
- **Definire, se necessario, eventuali altri requisiti**

Raccolta dei Requisiti del Cliente

Creazione del Modulo dei Requisiti – Obiettivi

- **Determinare quali tipi di report sono previsti**
 - *Executive Report*
 - *Technical Assessment Report*
 - *Developer Report*

- **Determinare in quale formato si preferisce che i report vengano consegnati**
 - *PDF, HTML, DOCX, etc*

- **Determinare come dovrebbero essere consegnati i report**
 - *E-mail, e-mail cifrate, documenti stampati, etc*

Raccolta dei Requisiti del Cliente

Creazione del Modulo dei Requisiti – Obiettivi

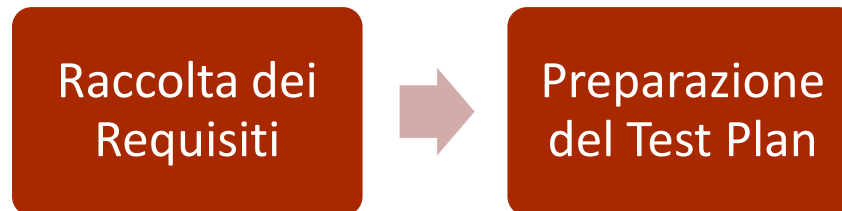
➤ **Determinare chi è il responsabile della ricezione e della gestione dei report**

- Azionista
- Manager
- Dipendente
- Valutatore appartenente a terze parti
- Autorità governative
- Etc

Raccolta dei Requisiti del Cliente

Considerazioni Finali

- La lista degli elementi da considerare durante la fase di raccolta dei requisiti può variare
 - Gli elementi dovrebbero essere aggiunti o rimossi in base alle aspettative ed alle esigenze specifiche dei clienti
- Utilizzando tale modulo è possibile
 - Ricavare in maniera chiara, completa e non ambigua le esigenze del cliente
 - Far confluire tali esigenze nel *Test Plan*



Outline

- Concetti Chiave
- Raccolta dei Requisiti del Cliente
- **Preparazione del Test Plan**
- Definizione dei Confini del Test
- Definizione degli Obiettivi di Business
- Gestione e Pianificazione di un Progetto

Preparazione del Test Plan

- Quando i requisiti sono stati raccolti e verificati dalle parti coinvolte, essi confluiscono in un piano formale di testing
 - **Test Plan**
- Nel Test Plan confluiscono anche altre informazioni
 - Necessarie per fini legali e/o commerciali del processo di penetration testing

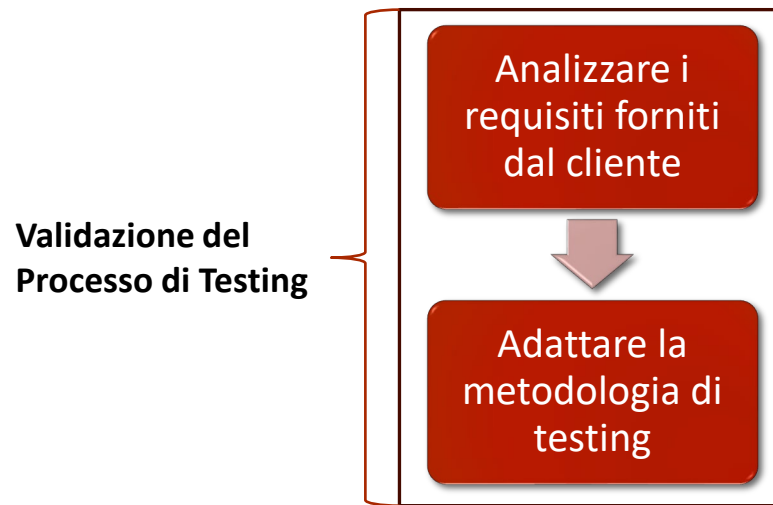
Preparazione del Test Plan

- Gli elementi più importanti di un tipico Test Plan sono
 - Struttura del Processo di Penetration Testing
 - Allocazione delle Risorse
 - Analisi dei Costi
 - *Rules Of Engagement (ROE)*
 - *Non-Disclosure Agreement (NDA)*
 - Contratto di Penetration Testing
 - Checklist del Piano di Testing

Preparazione del Test Plan

Struttura del Processo di Penetration Testing

- Dopo aver analizzato i requisiti raccolti dal cliente potrebbe essere necessario adattare la metodologia di penetration testing
 - Operazione nota come **Validazione del Processo di Testing**



Preparazione del Test Plan

Struttura del Processo di Penetration Testing

- Il Test Plan deve essere sempre aggiornato ad ogni cambiamento nei requisiti del cliente
 - L'esecuzione durante il processo di penetration testing di azioni non previste potrebbe causare violazioni e gravi sanzioni
- Potrebbero esserci modifiche al processo di penetration testing in base al tipo di testing che si intende effettuare
 - Ad es., il testing White Box potrebbe non richiedere le fasi di Information Gathering e Target Discovery, poiché il pentester è già a conoscenza dell'infrastruttura di rete da analizzare



Preparazione del Test Plan

Allocazione delle Risorse

- Affinché il testing abbia successo è fondamentale individuare i migliori specialisti che possano condurlo
 - Sempre in relazione ai vincoli di budget
- Attribuire l'incarico a pentester adeguatamente qualificati per condurre un determinato compito di solito comporta una migliore valutazione della sicurezza
 - Ad es., per il penetration testing di una Web App sarebbe necessario un pentester esperto nella sicurezza delle Web App



Preparazione del Test Plan

Analisi dei Costi

- I costi relativi ad un processo di penetration testing possono variare e dipendere da diversi fattori
 - Numero di giorni necessari per raggiungere gli obiettivi stabiliti
 - Numero di persone necessarie per raggiungere gli obiettivi stabiliti
 - Eventuali requisiti aggiuntivi, quali social engineering e valutazione della sicurezza fisica
 - Eventuali conoscenze o strumenti specifici, richiesti per la valutazione di determinati software o tecnologie



Preparazione del Test Plan

Rules Of Engagement (ROE)

- Il **processo di penetration** testing può essere **invasivo** e richiede
 - Chiara comprensione
 - Delle richieste di valutazione da parte del cliente
 - Del potenziale impatto o effetto che ogni tecnica e strumento di valutazione può avere sull'asset
 - Piena conoscenza degli strumenti utilizzati
 - Supporto fornito dal cliente



Preparazione del Test Plan

Rules Of Engagement (ROE)

- Le regole di ingaggio definiscono tutti i criteri procedurali e tecnici che dovrebbero essere seguiti durante l'intero processo di penetration testing
- Non si dovrebbero mai oltrepassare i limiti stabiliti dalle regole d'ingaggio concordate



Preparazione del Test Plan

Non-Disclosure Agreement (NDA)

- Tipicamente è necessario firmare un **accordo di non divulgazione (NDA)**, che rifletta gli interessi di tutte le parti coinvolte nel processo di penetration testing
 - Cliente, pentester ed eventuali terze parti coinvolte



Preparazione del Test Plan

Non-Disclosure Agreement (NDA)

- Un Non-Disclosure Agreement (NDA), o Accordo di Riservatezza, è un contratto legale tra due o più parti che stabilisce l'obbligo di non divulgare informazioni riservate o sensibili scambiate tra di loro
- L'obiettivo principale di un NDA è proteggere informazioni riservate e impedire che vengano condivise o utilizzate senza autorizzazione



Preparazione del Test Plan

Non-Disclosure Agreement (NDA)

- Un NDA può essere di vari tipi
 - **Unilaterale:** quando solo una parte si impegna a mantenere la riservatezza
 - **Bilaterale (o reciproco):** quando entrambe le parti hanno obblighi di non divulgazione
 - **Multilaterale:** quando più soggetti condividono informazioni e devono rispettare la segretezza



Preparazione del Test Plan

Non-Disclosure Agreement (NDA)

- Un NDA di solito contiene
 - Definizione delle informazioni riservate
 - Obblighi e doveri delle parti
 - Durata della riservatezza
 - Eccezioni (es. informazioni già pubbliche)
 - Conseguenze in caso di violazione



Preparazione del Test Plan

Non-Disclosure Agreement (NDA)

- Un accordo di non divulgazione reciproca permette di chiarire i termini e le condizioni secondo cui il processo di penetration testing deve essere svolto
 - Il pentester deve rispettare questi termini durante tutto il processo di penetration testing
 - La violazione anche di un singolo termine di accordo potrebbe comportare gravi sanzioni (ad es., multe o richieste di risarcimento danni), oltre all'esonero permanente dall'attività di penetration testing commissionata



Preparazione del Test Plan

Contratto di Penetration Testing

- Accordo legale che regola le questioni tecniche, amministrative e commerciali tra cliente e pentester
 - Oltre che, eventualmente, tra le altre parti coinvolte
- Data la sua importanza, il contratto di penetration testing dovrebbe essere stipulato servendosi del supporto di un avvocato o comunque di un consulente legale



Preparazione del Test Plan

Contratto di Penetration Testing

- Tale contratto dovrebbe esplicitare
 - Quali servizi (attività) di testing devono essere svolti
 - I loro obiettivi principali
 - Come e quando saranno condotti i servizi di testing
 - Dichiarazione di pagamento
 - Come mantenere la riservatezza dell'intero progetto



Preparazione del Test Plan

Checklist del Piano di Testing

- Preparare un Test Plan permette di
 - Avere una visione coerente del processo di penetration testing
 - Fornire al pentester dettagli specifici di valutazione, elaborati in base alle esigenze del cliente
- È buona prassi preparare una **checklist del piano di testing (Test Plan)**
 - Utilizzata per verificare con il contraente (cliente) i criteri di valutazione e le relative condizioni

Preparazione del Test Plan

Checklist del Piano di Testing

- Per preparare una checklist del piano di testing è importante considerare i seguenti aspetti
 - Sono stati soddisfatti tutti i requisiti dichiarati durante la *Request For Proposal (RFP)*?
 - L'ambito del processo di penetration testing è stato definito in modo chiaro?
 - Sono state identificate tutte le componenti da valutare?
 - Sono state identificate tutte le parti coinvolte nel processo di penetration testing?

Preparazione del Test Plan

Checklist del Piano di Testing

- Per preparare una checklist del piano di testing è importante considerare i seguenti aspetti
 - Verrà seguito uno specifico processo/metodologia di penetration testing?
 - Quando il processo di testing sarà terminato, verranno prodotti deliverable? Se sì, quali?
 - L'obiettivo della valutazione (*asset*) è stato mai analizzato e documentato in precedenza?

Preparazione del Test Plan

Checklist del Piano di Testing

- Per preparare una checklist del piano di testing è importante considerare i seguenti aspetti
 - Sono stati assegnati tutti i ruoli e le responsabilità per le attività di penetration testing?
 - Sono previste figure (professionisti) di terze parti per effettuare specifiche valutazioni (metodologiche, tecnologiche o strumentali)?
 - Etc

Outline

- Concetti Chiave
- Raccolta dei Requisiti del Cliente
- Preparazione del Test Plan
- **Definizione dei Confini del Test**
- Definizione degli Obiettivi di Business
- Gestione e Pianificazione di un Progetto

Definizione dei Confini del Test

- Necessario comprendere i «**limiti**» ed i «**confini**» dell'asset da valutare
- Le **limitazioni** possono riguardare **aspetti tecnologici**, di **conoscenza** o qualsiasi **altra restrizione formale** (ad es., divieti) imposta dal cliente sull'asset
 - Ciascuna restrizione potrebbe causare interruzioni al processo di testing e dovrebbe (se possibile) essere superata utilizzando metodi alternativi
- Alcune limitazioni potrebbero non essere superate/modificate
 - Vengono utilizzate dal cliente per controllare o limitare il processo di penetration testing

Definizione dei Confini del Test

Limitazioni Tecnologiche

- L'ambito del processo di penetration testing è stato definito correttamente, ma nell'asset è presente una **tecnologia che non può essere analizzata dal pentester**
 - Il pentester non possiede le competenze, le licenze o gli strumenti necessari per la valutazione di tale tecnologia
- La valutazione delle tecnologie proprietarie o di nuove tecnologie è uno degli aspetti più critici in un processo di penetration testing

Definizione dei Confini del Test

Limitazioni Tecnologiche

➤ **Esempio**

- Utilizzo di tecnologie proprietarie all'interno di un firewall
- Ciò impedisce il corretto funzionamento di eventuali strumenti per la valutazione del firewall

Definizione dei Confini del Test

Limitazioni di Conoscenza

➤ Possibili Limitazioni

- Insufficiente preparazione o esperienza del pentester
- Poca conoscenza di determinate tecnologie da valutare
- Conoscenza verticale solo di alcuni aspetti specifici del penetration testing
 - Fasi, strumenti, etc
- Etc

Definizione dei Confini del Test

Limitazioni di Conoscenza

➤ **Esempio**

- Un pentester esperto solo di database sarebbe in grado di valutare la sicurezza fisica di un'infrastruttura di rete?
- Per raggiungere l'obiettivo richiesto è bene dividere ruoli e responsabilità in base alle capacità ed alle competenze del (o dei) pentester

Definizione dei Confini del Test

Limitazioni Infrastrutturali

- Alcune restrizioni sul testing possono essere applicate dal cliente per controllare il processo di valutazione
 - **Esempio:** limitare la «vista» di un asset solo a specifici dispositivi e segmenti di rete che necessitano di una valutazione
- Generalmente, questo tipo di restrizione viene introdotto durante la fase di raccolta dei requisiti
 - **Esempio:** valutare tutti i dispositivi di rete che si trovano all'interno di un determinato segmento di rete, tranne un determinato server

Definizione dei Confini del Test

Limitazioni Infrastrutturali

- È importante **riflettere bene prima di applicare** tali **restrizioni** al processo di penetration testing
- La mancata analisi di alcuni dispositivi o di alcuni segmenti di rete potrebbe compromettere la sicurezza dell'intero asset



Definizione dei Confini del Test

Accordarsi sulle Limitazioni

- La valutazione delle restrizioni è importante
 - Può essere fatta durante la fase di raccolta dei requisiti del cliente
- Un pentester dovrebbe analizzare ogni requisito e discutere con il cliente per eliminare (o modificare) eventuali restrizioni che potrebbero causare
 - Interruzioni al processo di penetration testing
 - Future violazioni di sicurezza

Definizione dei Confini del Test

Superare le Limitazioni

- Alcune limitazioni potrebbero essere superate (o mitigate)
 - Assumendo pentester altamente qualificati
 - Utilizzando strumenti e tecniche avanzate di valutazione
- Altre limitazioni potrebbero non essere superate
 - Ad es., potrebbe essere necessario più tempo per sviluppare soluzioni ad hoc che permettano il testing di determinate tecnologie

Outline

- Concetti Chiave
- Raccolta dei Requisiti del Cliente
- Preparazione del Test Plan
- Definizione dei Confini del Test
- **Definizione degli Obiettivi di Business**
- Gestione e Pianificazione di un Progetto

Definizione degli Obiettivi di Business

- Gli obiettivi di business sono «il punto di incontro» tra la parte tecnica e gestionale di un'organizzazione
 - Per supportare e garantire la sicurezza dei sistemi informativi dell'organizzazione stessa
- Gli obiettivi di business possono essere molteplici e variano in base a numerosi fattori
 - Dimensione ed settore dell'organizzazione
 - Disponibilità di risorse
 - Etc

Definizione degli Obiettivi di Business

➤ **Garantire**

- **Reputazione:** ampia visibilità ed accettazione per l'organizzazione

 - Mantenendo regolari controlli di sicurezza

- **Conformità** rispetto a standard e regolamentazioni

 - **GDPR, NIS 2, ISO/IEC 27001**, etc

➤ **Proteggere** i sistemi informativi che memorizzano dati riservati

- Riguardanti ad esempio clienti, dipendenti ed altre entità dell'organizzazione

➤ **Elencare vulnerabilità e minacce** presenti nell'asset dell'organizzazione

- Contribuendo a creare politiche e procedure di sicurezza per contrastare rischi noti ed ignoti (*0-day*)

Definizione degli Obiettivi di Business

- **Minimizzare i costi** per la **gestione** della **sicurezza** dell'asset
 - Eliminando i potenziali rischi che potrebbero causare danni economici e di reputazione se sfruttati da malintenzionati
 - Descrivendo le procedure tecniche da applicare per risolvere eventuali problematiche di sicurezza
- **Seguire le migliori pratiche** del settore
- **Utilizzare le migliori tecniche** ed i **migliori strumenti** per valutare la sicurezza dell'asset
- **Fornire soluzioni di sicurezza** per proteggere l'asset

Outline

- Concetti Chiave
- Raccolta dei Requisiti del Cliente
- Preparazione del Test Plan
- Definizione dei Confini del Test
- Definizione degli Obiettivi di Business
- **Gestione e Pianificazione di un Progetto**

Gestione e Pianificazione di un Progetto

- Per valutare la sicurezza di un determinato asset potrebbero essere necessari più pentester (*team*)
 - Coordinati da un *Project Manager*

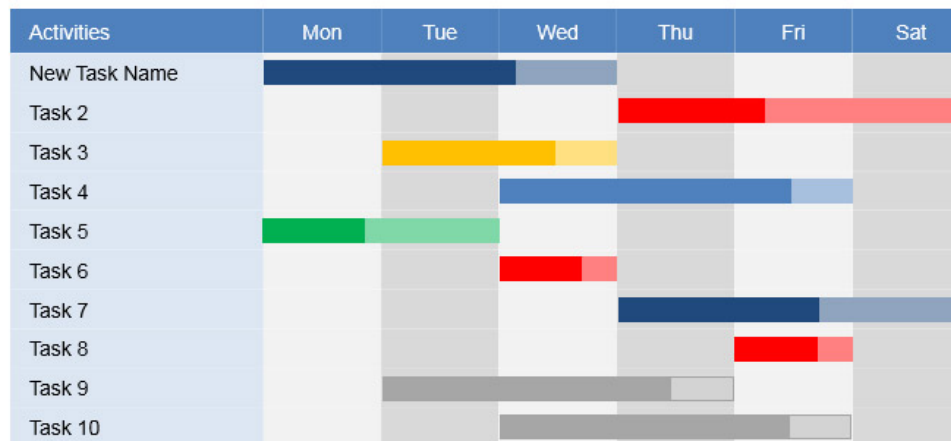


Gestione e Pianificazione di un Progetto

- Il processo di penetration testing richiede un'**attenta ripartizione del tempo** in base alle risorse disponibili
 - Tale processo non deve superare la scadenza dichiarata / preventivata
- Una **risorsa** potrebbe essere un **pentester**, ma anche uno **strumento** utilizzato per condurre un'**attività** di penetration testing
 - Un'**attività** è definita come il lavoro svolto dal pentester

Gestione e Pianificazione di un Progetto

- Dopo aver **identificato** ed **assegnato** le **risorse** per eseguire determinate attività è necessario definire una **timeline** che mostri l'utilizzo di tali risorse durante il processo di penetration testing
- Esistono numerosi **strumenti** che permettono di **gestire** in maniera efficiente **risorse** ed **attività** durante il processo di penetration testing
 - Molti fanno uso di **Diagrammi di Gantt**



Gestione e Pianificazione di un Progetto

- Utilizzando questi strumenti il lavoro del pentester può essere monitorato e gestito in base alle attività ed alle scadenze prestabilite
- Questi strumenti forniscono anche funzionalità più avanzate
 - Ad es., generazione di alert per il Project Manager se l'attività è stata completata o la scadenza per una determinata attività è stata superata

Gestione e Pianificazione di un Progetto

- Altri vantaggi derivanti dall'utilizzo di tali strumenti
 - Efficienza nella fornitura dei servizi nei tempi concordati
 - Migliore produttività del processo di testing
 - Maggiore soddisfazione del cliente
 - Maggiore qualità e quantità di lavoro svolto nel processo di testing
 - Etc

Gestione e Pianificazione di un Progetto

- Per gestire tutte le fasi del processo di penetration testing in modo efficiente ed economico sono disponibili numerosi Strumenti di Project Management, tra i quali
 - *OpenProject*
 - *OrangeScrum*
 - *Project Open*
 - *Taiga*
 - *Redmine*
 - *Etc*

Gestione e Pianificazione di un Progetto – OpenProject

➤ <https://www.openproject.org/download-and-installation/>

The image shows the OpenProject website and a screenshot of the OpenProject web interface. The website features the OpenProject logo, navigation links (Features, Hosting, Enterprise Edition, Pricing), and a prominent green button labeled "Get started for FREE". The main heading is "Collaborative Project Management" with the tagline "Open source project management software. Powerful. Easy-to-use. Free." Below this is a form to "Enter organization name" and another "Get started for FREE" button. A navigation bar includes links for "GANTT CHARTS", "WORK PACKAGES", "AGILE AND SCRUM", "TIME AND COSTS", and "WIKI". The screenshot of the web interface shows a "Project plan" view for a project named "Website Relaunch". It includes a sidebar with "Work packages" and "FAVORITE VIEWS" (Gantt chart, Meilensteinplan, Product Timeline, Project plan, Resource overview). The main area displays a table of work packages with columns for "SUBJECT" and "STATUS".

SUBJECT	STATUS
Develop v2.0	In development
Identify website scope	In development
Legal notes	On hold
Bug fixing v2.0	Tested

The screenshot also shows a Gantt chart for the "Sep 2018" period, with tasks like "Develop v2.0", "Identify website scope", "Legal notes", and "Bug fixing v2.0" represented by colored bars.

Target Scoping

Gestione e Pianificazione di un Progetto – OrangeScrum

➤ <https://www.orangescrum.com/>

OrangeScrum Product > Solutions > Features > Resources > Self-Hosted Pricing Sign in Try Free >>

Project Management Made Better

Organize Project, Task, Time, Resource & Budget, at one place!

Chroma FORD OTOSAN HONDA FAREWAY

Get started now >> No Credit Card Required

Capterra

OrangeScrum Dashboard

Projects: 850 / 1100 Tasks: 100 / 110 Resources: 85 / 90 Time Spent: 752 / 885 hours

Project Summary

Project Name	Project Manager	Due Date	Status	Progress
Agile Project	Marilisa Streich	June 6, 2022	Completed	100%
Android Development	Cathrine Marvin	July 10, 2022	On Track	80%
iOS App Development	Vladimir Hintz	Nov 5, 2022	Delayed	60%
Media Channel	Dustin Rippin	Nov 20, 2022	At Risk	40%

Milestone Progress

Project Name	Milestone	Due Date	Status	Progress
Agile Project	Social Media Marke	June 6, 2022	Completed	100%
Android Development	HR Activities	July 10, 2022	On Track	80%
iOS App Development	Software Architects	Nov 5, 2022	Delayed	60%
Media Channel	Media Channel	Nov 20, 2022	At Risk	40%

Overall Progress

70% Completed

24 Total Projects 15 Projects Completed 9 Projects In Progress 4 Projects Delayed

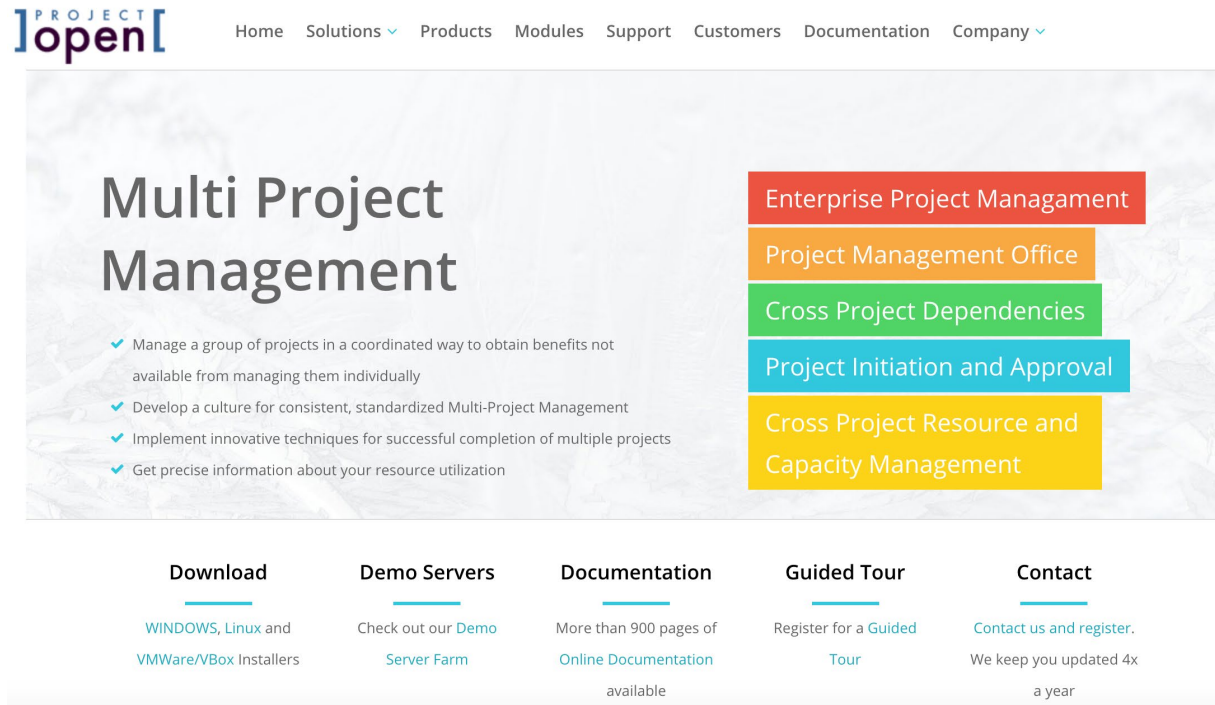
70% Completed

15 Milestones Achieved 12 Milestones In Progress 4 On Track

Target Scoping

Gestione e Pianificazione di un Progetto – Project Open

➤ <http://www.project-open.com/en/list-installers>



PROJECT
open

Home Solutions ▾ Products Modules Support Customers Documentation Company ▾

Multi Project Management

- ✓ Manage a group of projects in a coordinated way to obtain benefits not available from managing them individually
- ✓ Develop a culture for consistent, standardized Multi-Project Management
- ✓ Implement innovative techniques for successful completion of multiple projects
- ✓ Get precise information about your resource utilization

- Enterprise Project Management
- Project Management Office
- Cross Project Dependencies
- Project Initiation and Approval
- Cross Project Resource and Capacity Management

Download
WINDOWS, Linux and
VMWare/VBox Installers

Demo Servers
Check out our [Demo](#)
[Server Farm](#)

Documentation
More than 900 pages of
[Online Documentation](#)
available

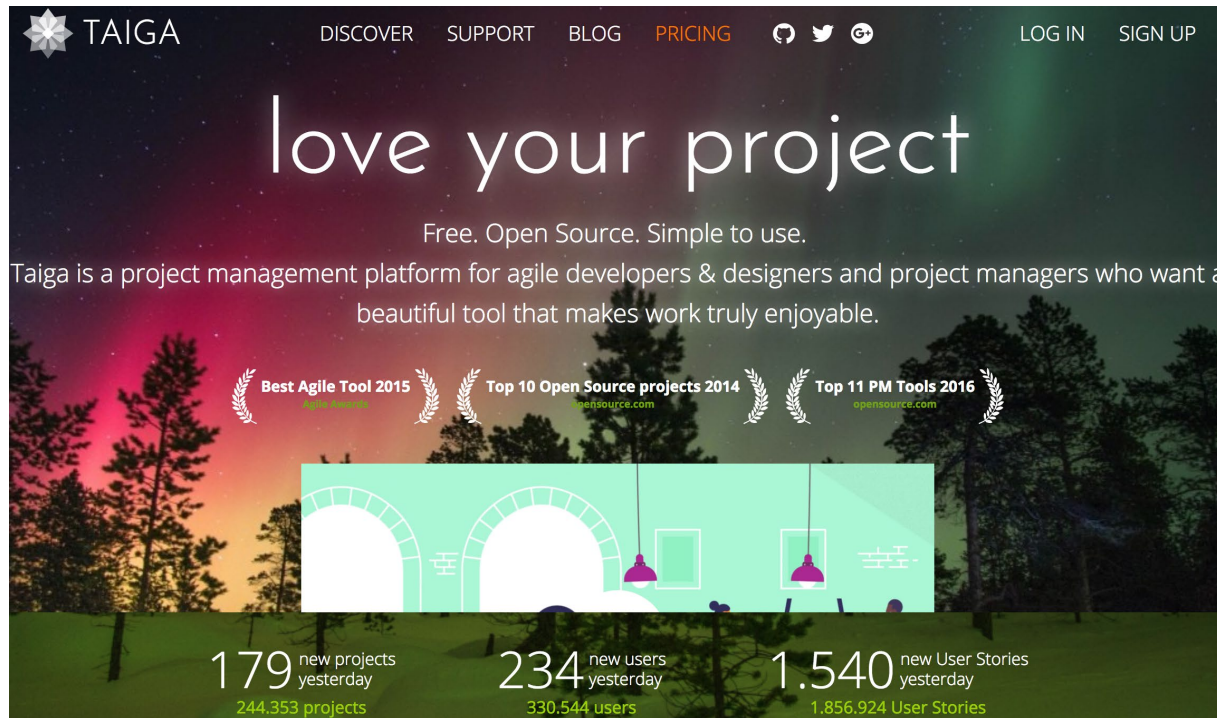
Guided Tour
Register for a [Guided](#)
[Tour](#)

Contact
[Contact us and register.](#)
We keep you updated 4x
a year

Target Scoping

Gestione e Pianificazione di un Progetto – Taiga

➤ <https://taiga.io/>



The image shows the homepage of the Taiga project management platform. The background is a dark, starry night sky with a forest silhouette. The Taiga logo is in the top left. Navigation links include DISCOVER, SUPPORT, BLOG, PRICING, and social media icons. The main headline is 'love your project' with the tagline 'Free. Open Source. Simple to use.' Below this, a description states: 'Taiga is a project management platform for agile developers & designers and project managers who want a beautiful tool that makes work truly enjoyable.' Three award laurels are displayed: 'Best Agile Tool 2015' from agile-alliance.org, 'Top 10 Open Source projects 2014' from opensource.com, and 'Top 11 PM Tools 2016' from opensource.com. A central illustration shows a stylized room with arches and hanging lamps. At the bottom, three statistics are shown: 179 new projects yesterday (244,353 projects total), 234 new users yesterday (330,544 users total), and 1,540 new User Stories yesterday (1,856,924 User Stories total).

TAIGA

DISCOVER SUPPORT BLOG PRICING

LOG IN SIGN UP

love your project

Free. Open Source. Simple to use.

Taiga is a project management platform for agile developers & designers and project managers who want a beautiful tool that makes work truly enjoyable.

Best Agile Tool 2015
agile-alliance.org

Top 10 Open Source projects 2014
opensource.com

Top 11 PM Tools 2016
opensource.com

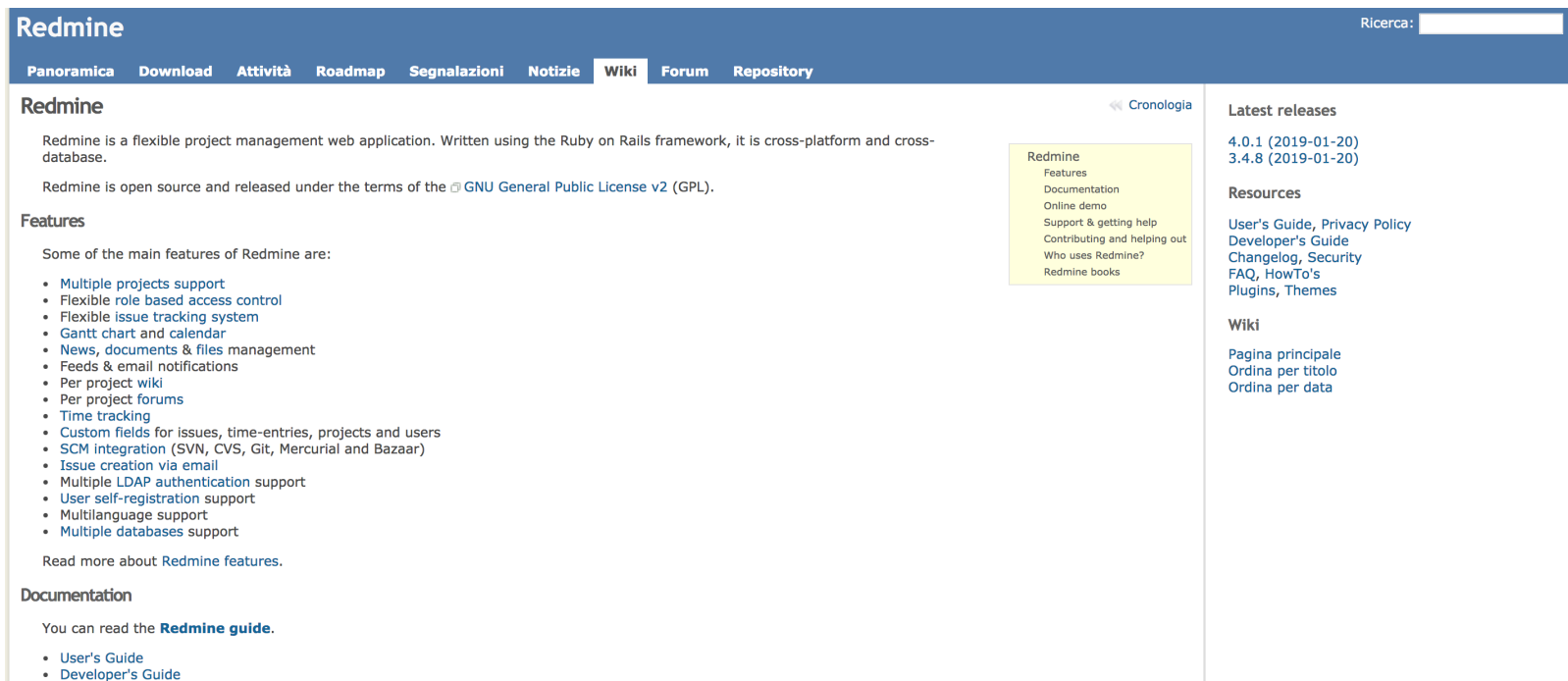
179 new projects yesterday
244,353 projects

234 new users yesterday
330,544 users

1,540 new User Stories yesterday
1,856,924 User Stories

Gestione e Pianificazione di un Progetto – Redmine

➤ <https://www.redmine.org/>



The screenshot shows the Redmine website homepage. The header is dark blue with the 'Redmine' logo on the left and a search bar on the right. Below the header is a navigation menu with links: Panoramica, Download, Attività, Roadmap, Segnalazioni, Notizie, Wiki, Forum, and Repository. The main content area is white and divided into three columns. The left column contains the 'Redmine' title, a description of the application, its open-source status under the GNU GPL v2 license, and a 'Features' section listing various capabilities like multiple project support, flexible access control, and issue tracking. The middle column has a 'Cronologia' link and a yellow box listing links to Redmine features, documentation, online demo, support, and books. The right column contains 'Latest releases' (4.0.1 and 3.4.8), 'Resources' (User's Guide, Privacy Policy, etc.), and a 'Wiki' section with links to the main page, title, and data.

Redmine

Ricerca:

[Panoramica](#) [Download](#) [Attività](#) [Roadmap](#) [Segnalazioni](#) [Notizie](#) [Wiki](#) [Forum](#) [Repository](#)

Redmine

Redmine is a flexible project management web application. Written using the Ruby on Rails framework, it is cross-platform and cross-database.

Redmine is open source and released under the terms of the [GNU General Public License v2 \(GPL\)](#).

Features

Some of the main features of Redmine are:

- [Multiple projects support](#)
- [Flexible role based access control](#)
- [Flexible issue tracking system](#)
- [Gantt chart and calendar](#)
- [News, documents & files management](#)
- [Feeds & email notifications](#)
- [Per project wiki](#)
- [Per project forums](#)
- [Time tracking](#)
- [Custom fields for issues, time-entries, projects and users](#)
- [SCM integration \(SVN, CVS, Git, Mercurial and Bazaar\)](#)
- [Issue creation via email](#)
- [Multiple LDAP authentication support](#)
- [User self-registration support](#)
- [Multilanguage support](#)
- [Multiple databases support](#)

Read more about [Redmine features](#).

Documentation

You can read the [Redmine guide](#).

- [User's Guide](#)
- [Developer's Guide](#)

[Cronologia](#)

Redmine

- [Features](#)
- [Documentation](#)
- [Online demo](#)
- [Support & getting help](#)
- [Contributing and helping out](#)
- [Who uses Redmine?](#)
- [Redmine books](#)

Latest releases

[4.0.1 \(2019-01-20\)](#)
[3.4.8 \(2019-01-20\)](#)

Resources

[User's Guide, Privacy Policy](#)
[Developer's Guide](#)
[Changelog, Security](#)
[FAQ, HowTo's](#)
[Plugins, Themes](#)

Wiki

[Pagina principale](#)
[Ordina per titolo](#)
[Ordina per data](#)

Bibliografia

- **Kali Linux 2 - Assuring Security by Penetration Testing. Third Edition.** Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016

- Capitolo 3

