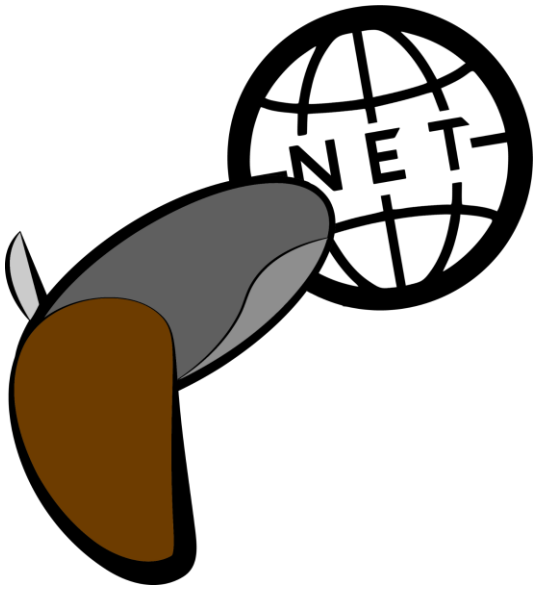


RAD

Requirements Analysis Document

NetGun

Versione	1.1
Data	01/12/2022
Destinatario	Professore Carmine Gravino
Presentato da	Carlo Colizzi, Giulio Incoronato, Antonio Mazzarella

Revision History

Data	Versione	Descrizione	Autori
13/11/2022	0.1	Stesura della sezione Revision History e Sommario	Carlo Colizzi
14/11/2022	0.2	Aggiunta degli Scenari	Tutto il gruppo
17/11/2022	0.3	Aggiunta dei Requisiti Funzionali	Tutto il gruppo
20/11/2022	0.4	Aggiunta degli Use Case, Requisiti Non Funzionali	Tutto il gruppo
21/11/2022	0.5	Aggiunta dei mock-ups	Antonio Mazzarella
23/11/2022	0.6	Aggiunta degli Use Case Diagram, Use Case	Tutto il gruppo
26/11/2022	0.7	Aggiunta dello Statechart, Activity Diagram, Sequence Diagrams	Carlo Colizzi, Giulio incoronato
27/11/2022	0.8	Aggiunta del Class Diagram	Carlo Colizzi
29/11/2022	0.9	Revisione del Class Diagram	Tutto il gruppo
30/11/2022	1.0	Aggiunta Path Navigazionali	Giulio Incoronato
16/12/2022	1,1	Revisione dei contenuti	Tutto il gruppo

Team Members

Nome	Informazioni di contatto
Carlo Colizzi	c.colizzi@studenti.unisa.it
Giulio Incoronato	g.incoronato2@studenti.unisa.it
Antonio Mazzarella	a.mazzarella5@studenti.unisa.it

Sommario

Revision History 2

Team Members 3

1 Introduzione 4

1.1 Obiettivo del Sistema 4

1.2 Ambito del Sistema 4

1.3 Obiettivi e Criteri di Successo 4

1.4 Definizioni, Acronimi e Abbreviazioni 5

1.5 Riferimenti 6

1.6 Organizzazione del Documento 6

2 Sistema Attuale 7

3 Sistema Proposto 9

3.1 Overview 9

3.3 Requisiti Non Funzionali 11

3.4 System Model 12

3.4.1 Scenari 12

3.4.2 Use Case Model 17

3.4.3 Object Model 24

3.4.4 Dynamic Model 30

3.4.5 User Interface – Navigational Paths e Mock-up 34

4 Glossario 40

1 Introduzione

1.1 Obiettivo del Sistema

Il sistema che si intende realizzare ha l'obiettivo di facilitare l'attività di analisi e monitoraggio effettuata sulle infrastrutture di rete dai Penetration Tester. Attraverso un software applicativo, è fornita al Penetration Tester la possibilità di effettuare scansioni di rete su macchine utilizzanti lo standard di comunicazione TCP/IP.

Il sistema ha l'obiettivo di velocizzare processi ripetitivi e macchinosi, facilitando la gestione dell'Attività di Black Box Testing su infrastrutture di rete.

1.2 Ambito del Sistema

Nel dettaglio, le funzionalità del sistema sono:

- Rilevare ed acquisire dati sui servizi offerti dall'infrastruttura di rete
- Rilevare mal configurazioni sui diversi servizi offerti dall'infrastruttura di rete
- Consigliare tools per interagire con i servizi offerti dall'infrastruttura di rete
- Rilevare possibili CVE presenti nei servizi offerti dall'infrastruttura di rete
- Fornire un report sulle analisi effettuate

1.3 Obiettivi e Criteri di Successo

L'obiettivo del progetto è la creazione di un Software Applicativo Linux-Based che sarà di supporto alle Attività di Black Box Testing su infrastrutture di rete.

I criteri di successo stabiliti sono:

- **Facilità di manutenzione e aggiornamento**: Si intente realizzare un sistema software con una buona documentazione e una buona modularità, al fine di poter essere mantenuto e aggiornato con poche difficoltà

- **Astrazione**: Si intende realizzare un sistema software che permetta di svolgere test di rete molto articolati e complessi con una semplice interfaccia grafica
- **Interfaccia Minimale:** Si intende rendere l'interfaccia del software minimale, così da facilitare la comprensione e l'utilizzo del software
- **Rispetto delle scadenze:** Si intende rispettare le scadenze prefissante alla consegna dello Statement of Work

1.4 Definizioni, Acronimi e Abbreviazioni

Di seguito è fornita una lista di definizioni, acronimi e abbreviazioni:

- **ODD:** Object Design Document
- **SDD:** System Design Document
- **UCD**: Use case Diagram
- **CD**: Class Diagram
- **AD**: Activity Diagram
- **SC**: Statechart Diagram
- **RAD**: Requirements Analysis Document
- **SD**: Sequence Diagram
- **NP**: Navigational Path
- **RNF**: Requisito Non Funzionale
- **RF**: Requisito Funzionale

1.5 Riferimenti

Di seguito una lista di riferimenti ad altri documenti utili durante la lettura:

- Requirements Analysis Document: https://github.com/MyCr4ck/NetGun_Classe03/tree/main/Documenti
- System Design Document: https://github.com/MyCr4ck/NetGun_Classe03/tree/main/Documenti
- Progetto Open Source on GitHub: https://github.com/MyCr4ck/NetGun_Classe03
- Test Plane: https://github.com/MyCr4ck/NetGun_Classe03/tree/main/Documenti
- Test Case Specification: https://github.com/MyCr4ck/NetGun_Classe03/tree/main/Documenti
- Il Documento segue le metodologie presentate nel libro: Object-Oriented Software Engineering, di Bernd Bruegge & Allen H. Dutoit

1.6 Organizzazione del Documento

Il presente documento è strutturato nel seguente modo:

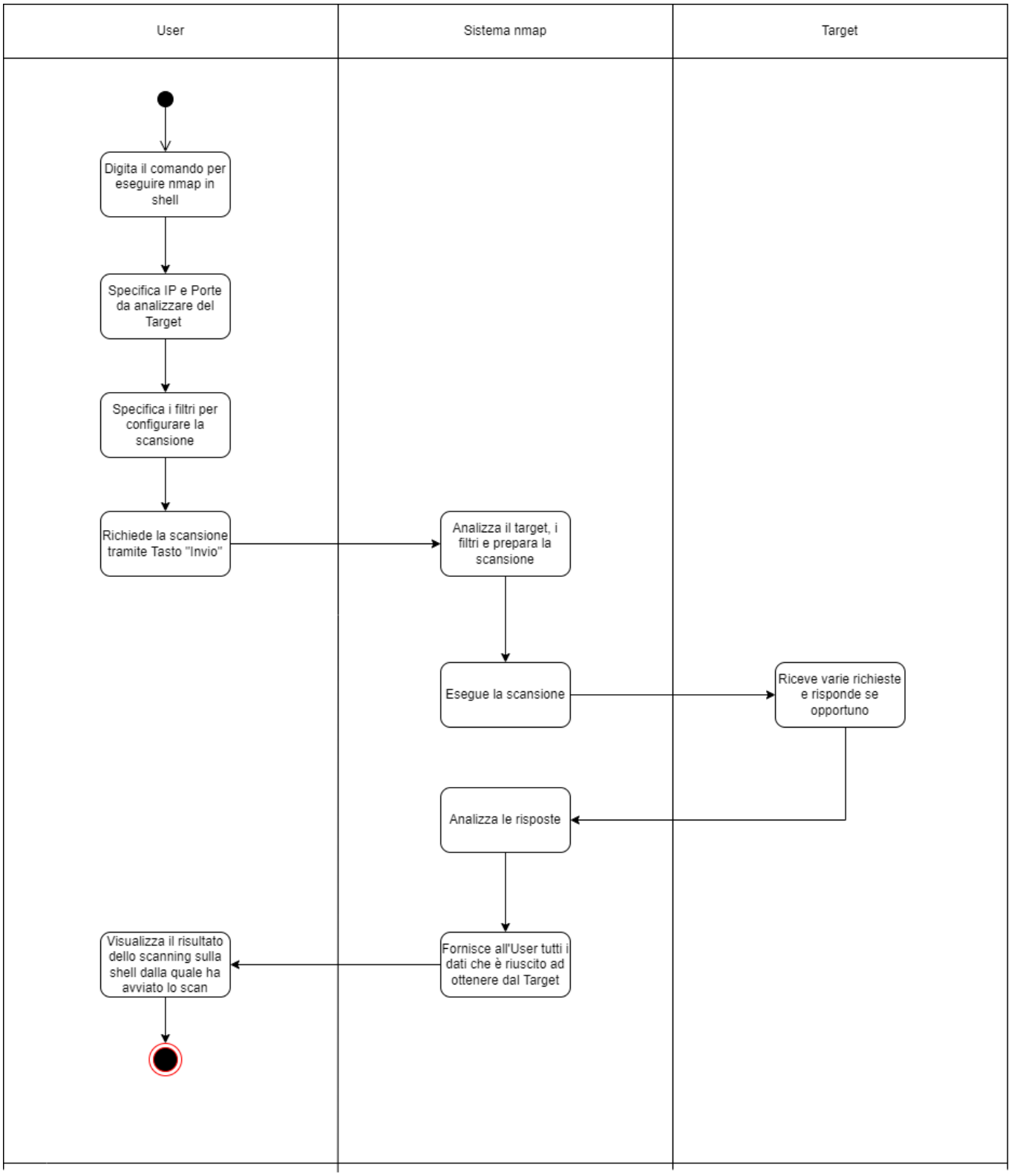
1. **Introduzione**: Contiene l'obiettivo, l'ambito, i criteri di successo del sistema, seguiti da una panoramica sulle definizioni, acronimi e abbreviazioni presenti nel documento.
2. **Sistema attuale**: Descrive verbalmente nmap, un Port Scanner CLI.
3. **Sistema proposto**: Descrive il nuovo sistema, presentandone i requisiti funzionali e non funzionali. Tramite scenari ed use-case vengono descritti gli attori del sistema e come questi ultimi interagiscono con esso. Grazie al Sequence Diagram e al Class Diagram viene mostrata la struttura del sistema. È presente, inoltre, la descrizione dell'interfaccia grafica, mostrata tramite mock-up e Navigational Path.
4. **Glossario**: descrive i termini tecnici presenti nel RAD.

2 Sistema Attuale

Attualmente il software di Port Scanning più utilizzato in ambito Cyber Security è nmap, un software utilizzabile solo a linea di comando, minimale ed efficace per attività di scanning a grana fine.

Nonostante ciò, l'essere a linea di comando lo rende eccessivamente macchinoso durante i test. Va considerato anche che questo software potrebbe essere sfruttato molto meglio se posto in un sistema GUI, con l'ausilio di nuove funzionalità che lo renderebbero più intuitivo, veloce e performante. E per finire questo software è single Thread, il che non gli permette di sfruttare le macchine di ultima generazione.

Per concludere, di seguito è mostrato un AD che illustra il classico utilizzo di nmap:


User
Sistema nmap
Target
Digita il comando per eseguire nmap in shell
Specifica IP e Porte da analizzare del Target
Specifica i filtri per configurare la scansione
Richiede la scansione tramite Tasto "Invio"
Analizza il target, i filtri e prepara la scansione
Esegue la scansione
Riceve varie richieste e risponde se opportuno
Analizza le risposte
Fornisce all'User tutti i dati che è riuscito ad ottenere dal Target
Visualizza il risultato dello scanning sulla shell dalla quale ha avviato lo scan

3 Sistema Proposto

3.1 Overview

La sezione che segue è organizzata in questo modo:

1. **Requisiti funzionali:** descrizione degli attori e dei requisiti funzionali, ovvero descrizione delle interazioni tra il sistema e l'ambiente esterno, quindi gli attori senza tenere in considerazione l'implementazione.
2. **Requisiti non funzionali:** descrizione degli aspetti del sistema che ne indicano la qualità come usabilità, affidabilità, prestazioni, aspetti quindi non legati alle funzionalità del sistema.
3. **Modello del sistema:**
    - **Scenari**: descrizione informale di una singola caratteristica del sistema dal punto di vista dell'utente finale, descrivono cosa gli utenti fanno quando usano il sistema.
    - **Modello dei casi d'uso**: descrizione completa delle interazioni che avvengono quando un attore usa il sistema, specificando anche tutti i possibili scenari per quella determinata azione.
    - **Modello ad oggetti**: descrizione tramite una class Diagram delle classi del sistema, delle loro proprietà e delle loro relazioni.
    - **Modello dinamico**: Rappresenta la struttura dinamica del sistema.
    - **Path navigazionali:** descrivono il percorso tra le pagine che un attore può compiere all'interno del sistema
    - **Mock-ups**: rappresentazioni dell'interfaccia grafica

3.2 Requisiti Funzionali

In questa sezione saranno presenti i requisiti funzionali del sistema proposto.

Identificativo	Nome	Descrizione	Attore	Priorità
RF_1	Shallow Scanning	Il sistema deve permettere di rilevare quali porte sono aperte sulla macchina	Utente	Elevata
RF_2	Deep Scanning	Il sistema deve permettere di ottenere la versione dei servizi in ascolto della macchina	Utente	Elevata
RF_3	Filtering	Il sistema deve permettere di selezionare dei filtri per configurare la scansione	Utente	Elevata
RF_4	Testing Misconfigurations	Il sistema permette di testare le probabili Mal Configurazioni dei servizi	Utente	Media
RF_5	Research CVE	Il sistema ricerca eventuali CVE	Utente	Media
RF_6	Create Report	Il sistema deve creare un report contenete tutte le analisi effettuate	Utente	Elevata
RF_7	Tutorial	Il sistema fornisce dei consigli su come interagire con le varie sezioni	Utente	Elevata
RF_8	Testing Network Performance	Il sistema fornisce delle informazioni sulle prestazioni della rete attuale	Utente	Media
RF_9	Verbose Progress	Il sistema fornisce informazioni sull'avanzamento dello scanner	Utente	Media
RF_10	Tips	Il sistema consiglia dei tools aggiuntivi per contattare e interagire con i servizi	Utente	Media

3.3 Requisiti Non Funzionali

In questa sezione saranno presenti i requisiti non funzionali del sistema proposto.

Identificativo	Nome	Descrizione	Priorità
RNF_1	Usabilità	Il sistema deve garantire all'utente delle chiare e minimali indicazioni di utilizzo in ogni sezione del software tramite un Help, raggiungibile con al massimo 1 click.	Alta
RNF_2	Performance.1	Il sistema deve ottenere un incremento del Throughput proporzionale al numero di Thread messi a disposizione dalla macchina; per i test effettuati in Locale o su VM interne alla macchina.	Alta
RNF_3	Performance.2	Il sistema non può garantire dei tempi di risposta deterministici sugli scan, a causa dell'inaffidabilità della rete.	Alta
RNF_4	Sopportabilità	Il sistema deve essere fortemente modulare per far fronte ad eventuali modifiche relative alla mantenibilità.	Media
RNF_5	Implementazione	Il sistema deve essere sviluppato in linguaggio Python.	Alta
RNF_6	Leggibilità	Il sistema deve avere codice facile da leggere, per favorire lo sviluppo dato dalla community Open Source	Media
RNF_7	Packaging	Il sistema dovrà essere installabile su qualsiasi macchina Linux-Based Debian con interprete Python3.	Media
RNF_8	Legali.1	Il sistema deve essere Open Source.	Alta
RNF_9	Legali.2	Il sistema non può essere utilizzato per scopi illeciti o volti al danneggiamento altrui.	Alta
RNF_10	Performance.3	Il sistema dovrà permettere un tempo di accesso ai dati persistenti minore di un secondo.	Alta
RNF_11	Robustezza	Il sistema deve garantire un elevata robustezza sugli errori causati dalla rete	Media
RNF_12	Costi	Il sistema deve azzerare i costi relativi alla persistenza dei dati	Alta

3.4 System Model

Nella presente sezione sono descritti diversi modelli del sistema che permettono di analizzare il sistema in vari aspetti.

3.4.1 Scenari

Attori del sistema: User

Attori esterni: Target (Server bersaglio dello scan)

NOME SCENARIO	SC1_ShallowScanning	
ATTORI	Mario: Utente, Server: Server Target	
SITUAZIONE INIZIALE	Mario è un Penetration Tester Freelancer, deve effettuare un'analisi sulle porte aperte di un server	
FLUSSO DEGLI EVENTI	Utente	Sistema
	Mario inserisce l'IP del server	
		Il sistema gli permette di scegliere la modalità di scansione fra Shallow e Deep scanning
	Mario seleziona la modalità Shallow e avvia lo scanner	
		Il sistema effettua scanning e restituisce una lista delle porte aperte

NOME SCENARIO	SC2_DeepScanning	
ATTORI	Ugo: Utente, Server: Server Target	
SITUAZIONE INIZIALE	Ugo è un Penetration Tester Freelancer, deve effettuare un'analisi sulle porte aperte di un server	
FLUSSO DEGLI EVENTI	Utente	Sistema
	Ugo inserisce l'IP del server	
		Il sistema gli permette di scegliere la modalità di scansione fra Shallow e Deep scanning
	Ugo seleziona la modalità Deep e avvia lo scanner	
		Il sistema effettua lo scanning, restituendo le porte aperte e i rispettivi servizi in ascolto su queste

NOME SCENARIO	SC3_Filtering	
ATTORI	Claudia: Utente, Server: Server Target	
SITUAZIONE INIZIALE	Claudia è una Web Developer, non riesce ad effettuare il Deploy del suo Web Server, sospetta che le porte da utilizzare siano occupate. Per comprendere quali servizi stiano occupando le porte decide di utilizzare NetGun	
FLUSSO DEGLI EVENTI	Utente	Sistema
	Claudia inserisce l'IP del server	
		Il sistema le permette di scegliere la modalità di scansione fra Shallow e Deep scanning
	Claudia seleziona la modalità	
		Il Sistema le permette di scegliere fra vari tipi di filtri per la scansione
	Claudia seleziona tramite filtri il protocollo di livello Trasposto e le porte da enumerare	
		Il sistema effettua lo scanning basandosi sui filtri inseriti da Claudia e restituisce i dati raccolti

NOME SCENARIO	SC4_TestingBadConfigurations	
ATTORI	Giulio: Utente, Server	
SITUAZIONE INIZIALE	Giulio è un Developer e vuole effettuare dei Test sulle mal configurazioni del suo server FTP	
FLUSSO DEGLI EVENTI	Utente	Sistema
	Giulio ha effettuato un Deep Scan, questo gli ha confermato che il suo server FTP è online	
		Il sistema gli permette di effettuare un test sulle mal configurazioni del servizio
	Giulio richiede al sistema di effettuare il test delle mal configurazioni sul server FTP	
		Il sistema effettua vari Test riportando tutte le mal configurazioni trovate

NOME SCENARIO	SC5_ResearchCVE	
ATTORI	Ginevra: Utente, Sistemi: Server Target	
SITUAZIONE INIZIALE	Ginevra è stata assunta da un'azienda con sistemi informatici molto datati, lei sa che sistemi che non vengono aggiornati da tempo, spesso presentano CVE	
FLUSSO DEGLI EVENTI	Utente	Sistema
	Ginevra avvia uno scanner sulle CVE presenti nel server	
		Il sistema risponde con le probabili CVE riscontrate
	Ginevra prontamente testa se le CVE segnalate sono effettivamente presenti, e aggiorna i servizi vulnerabili	

NOME SCENARIO	SC6_CreateReport	
ATTORI	Alfredo: Utente, Server	
SITUAZIONE INIZIALE	Alfredo ha completato tutti i test di sicurezza di cui aveva bisogno e vuole esportare un report delle analisi fatte	
FLUSSO DEGLI EVENTI	Utente	Sistema
	Richiede al sistema di esportare un Report contenente tutte le analisi effettuate	
		Fornisce un Report con tutti i dati raccolti

NOME SCENARIO	SC7_Tutorial	
ATTORI	Giorgio: Utente, Server: Server Casalingo	
SITUAZIONE INIZIALE	Giorgio è un Data Analyst, ha notato strane attività nel proprio server casalingo e vorrebbe effettuare un test di sicurezza, ma non essendo pratico in quest'attività ha bisogno di essere guidato, quindi si affida a NetGun	
FLUSSO DEGLI EVENTI	Utente	Sistema
	Giorgio avvia il programma	
		Il sistema mostra una pagina di benvenuto
	Giorgio vuole avviare uno scanning ma non sa come fare	
		Il sistema fornisce un'icona di aiuto affiancata ad ogni funzionalità
	Giorgio clicca sull'icona di aiuto	
		Il programma gli fornisce una finestra con dei consigli su come utilizzare la funzionalità correlata

NOME SCENARIO	SC8_TestingNetworkPerfomance
ATTORI	Lisa: Utente
DESCRIZIONE	Lisa è una Network Analyst, si rende conto che le gli scanner che effettua sono particolarmente lenti

FLUSSO DEGLI EVENTI	Utente	Sistema
	Lisa vuole effettuare un test sulle prestazioni della propria rete	
		Il sistema fornisce una funzionalità per effettuare un test sull' Upload e Download della rete
	Lisa esegue la funzionalità così da effettuare il test	
		Il sistema verifica le performance in Download e Upload della rete attuale e stampa il risultato

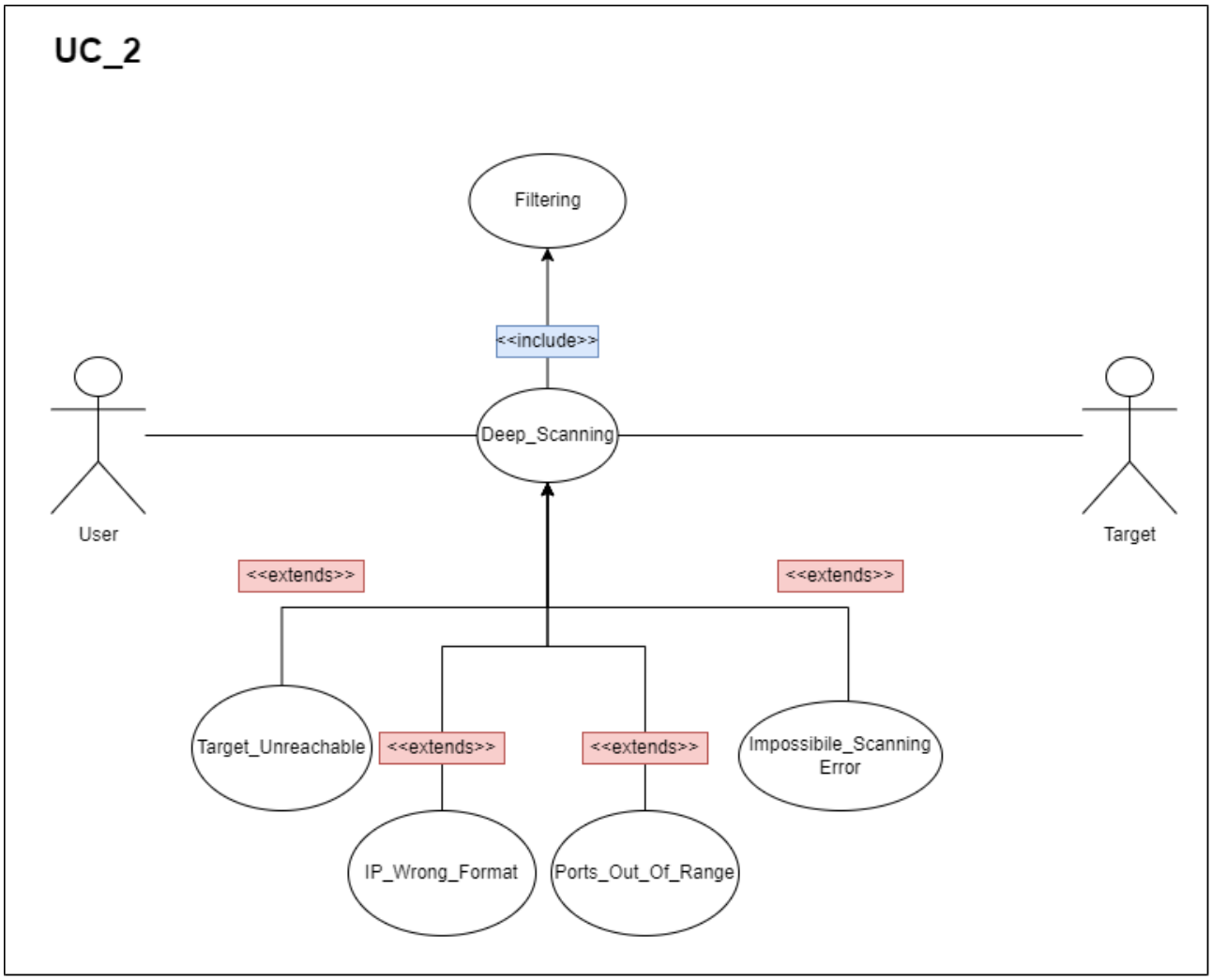
NOME SCENARIO	SC9_VerboseProgress	
ATTORI	Peppe: Security Analyst, Server	
SITUAZIONE INIZIALE	Peppe vuole effettuare uno Scanner di Sicurezza sul Proprio server e vorrebbe avere un feedback istantaneo dell'andamento di questo	
FLUSSO DEGLI EVENTI	Utente	Sistema
	Peppe deve analizzare il server e avvia uno scanning	
		Fa partire uno scanning
	Peppe vuole visualizzare in tempo reale i progressi dell'analisi	
		Mostra una barra di progresso

NOME SCENARIO	SC10_Tips	
ATTORI	Michele: Developer, Server	
SITUAZIONE INIZIALE	Michele vuole contattare uno specifico Servizio ma non sa che software client utilizzare	
FLUSSO DEGLI EVENTI	Utente	Sistema
	Michele ha verificato tramite Deep Scan che il servizio è online	
		Il sistema gli permette di accedere ad una sezione contenente i client consigliati con i quali interagire con il servizio
	Michele richiede di accedere alla sezione Tips	
		Mostra la lista di client consigliati

3.4.2 Use Case Model

In questa sezione sono presentati i diversi casi d'uso del sistema.

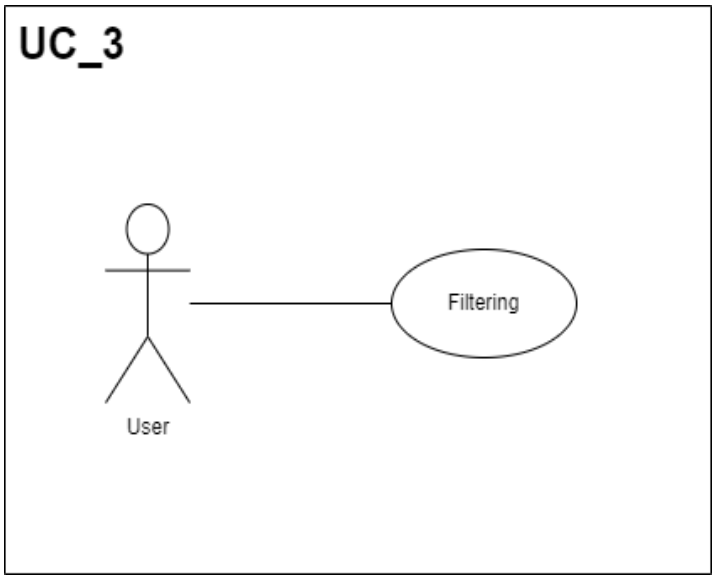
Use Case 2



Identificativo *UC_2*	*L'utente effettua il Deep Scanning*	*Data*	10/11/2022
		Vers.	1.2
		Autore	Utente
Descrizione	L'Utente vuole effettuare uno scanner di rete sulla versione dei servizi in esecuzione sulle porte aperte		
Attore Principale	Utente Interessato ai servizi in esecuzione sulle porte aperte		
Attori secondari	Target: Server		
Entry condition	È visualizzato il comando per effettuare la scansione		
Exit condition On success	È stato possibile interagire con una o più porte AND Visualizzare i protocolli di livello Applicazione utilizzati dalle porte aperte, con la relativa versione del servizio		
Exit condition On failure	Non è stato possibile interagire con le porte		
Rilevanza/User Priority	Elevata		
Frequenza stimata	4/giorno		
FLUSSO DI EVENTI PRINCIPALE/MAIN SCENARIO			
1	Utente:	Include UC_3 (Filtering)	
2	Sistema:	Fornisce all'utente la possibilità di scegliere fra due modalità di scanning: • Shallow • Deep	
3	Utente:	Seleziona la modalità Deep	
	Sistema:	Permette all'utente di avviare lo Scan	
4	Utente:	Avvia lo scan	
5	Sistema:	Verifica che il target inserito sia in un formato corretto AND Verifica se il Target è raggiungibile	
6	Sistema:	Effettua la scansione AND Restituisce una schermata con i dati raccolti. La schermata per ogni porta analizzata contiene: • Numero Porta • Protocollo di livello Trasporto Utilizzato dalla porta • Protocollo di livello Applicazione Utilizzato dalla porta • Versione del Servizio in ascolto sulla porta	
Scenario/Flusso di eventi Alternativo: Le porte inserite non			

rientrano nell'intervallo consentito			
5.1	Sistema:	Notifica che le porte inserite non rientrano nell'intervallo consentito	
5.2	Sistema:	Resta in attesa di un nuovo intervallo	
Scenario/Flusso di eventi Alternativo: L'IP inserito non è in un formato corretto			
5.1	Sistema:	Notifica che L'IP inserito non è in un formato valido	
Scenario/Flusso di eventi Alternativo: Il target non è raggiungibile			
5.1	Sistema:	Visualizza un messaggio di errore, segnala all'utente che il server potrebbe non essere raggiungibile	
5.2	Sistema:	Resta in attesa di un nuovo scan	

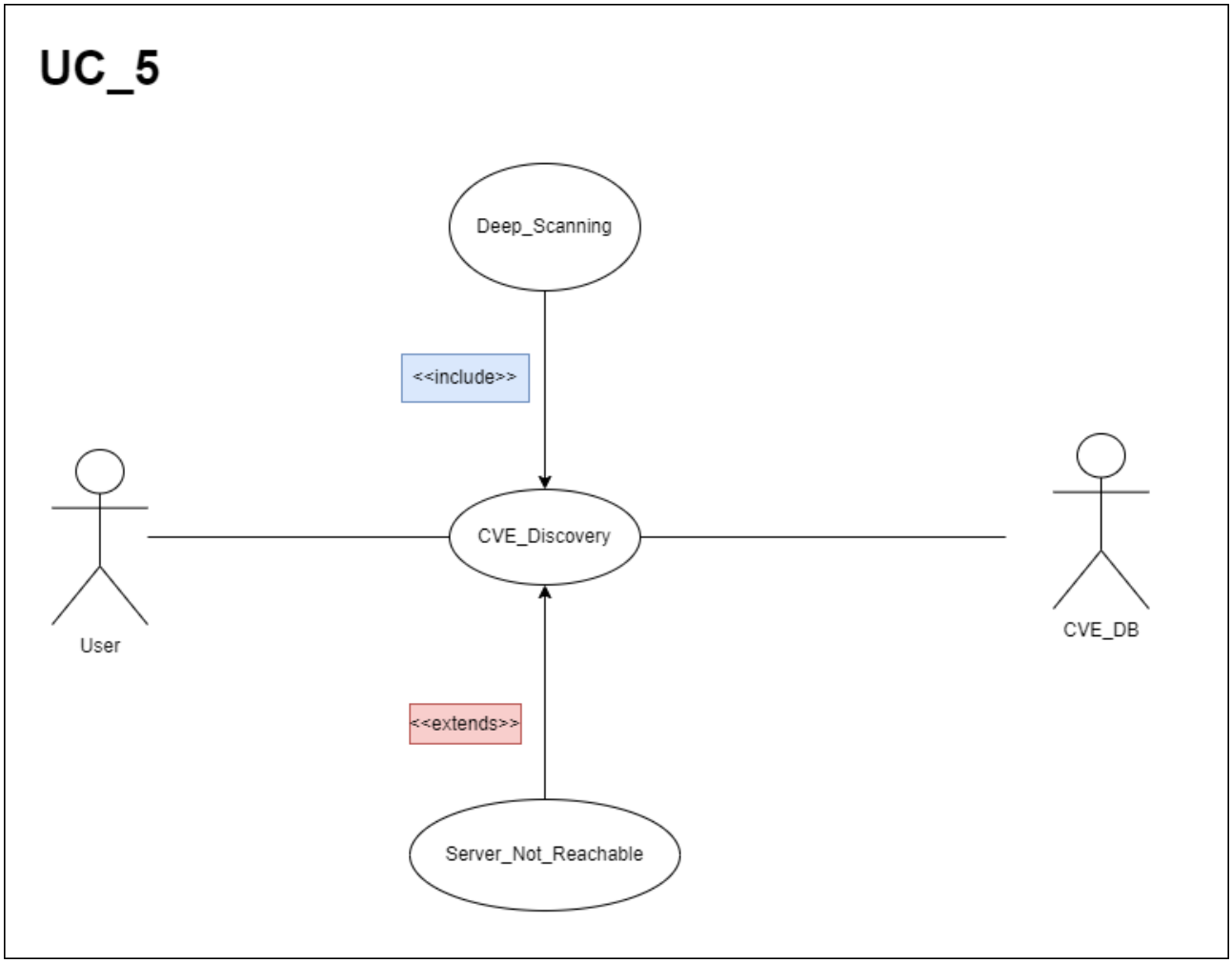
Use Case 3



Identificativo *UC_3*	*L' Utente configura tramite dei filtri il funzionamento dello scanning*	*Data*	13/11/22
		Vers.	0.8
		Autore	Utente
Descrizione	L'Utente vuole aggiungere dei filtri sulla scansione da effettuare		
Attore Principale	Utente Interessato a uno specifico tipo di analisi		
Attori secondari			
Entry Condition	È visualizzato il comando per selezionare i filtri		
Exit condition On success	Lo scanner con filtri è pronto per l'esecuzione		
Exit condition On failure	Non è stato possibile interagire con i filtri		
Rilevanza/User Priority	Elevata		
Frequenza stimata	4/giorno		
FLUSSO DI EVENTI PRINCIPALE/MAIN SCENARIO			
1	Utente:	Inserisce indirizzo IPv4	
2	Sistema:	Fornisce all'utente la possibilità di scegliere fra due protocolli di livello trasporto: • UDP • TCP	
3	Utente:	Seleziona il protocollo di trasporto che vuole utilizzare	
4	Sistema:	Fornisce all'utente la possibilità di scegliere quali porte scannerizzare	
5	Utente:	Inserisce il range di porte che vuole analizzare	
6	Sistema:	Fornisce all'utente la possibilità di selezionare delle modalità di scanning aggiuntive: • Disable Ping	

		• SYN scan • ACK scan • OS detection
7	Utente:	Seleziona le modalità da utilizzare
8	Sistema:	Ha completato la fase di filtering necessaria alla scansione

5 Use Case



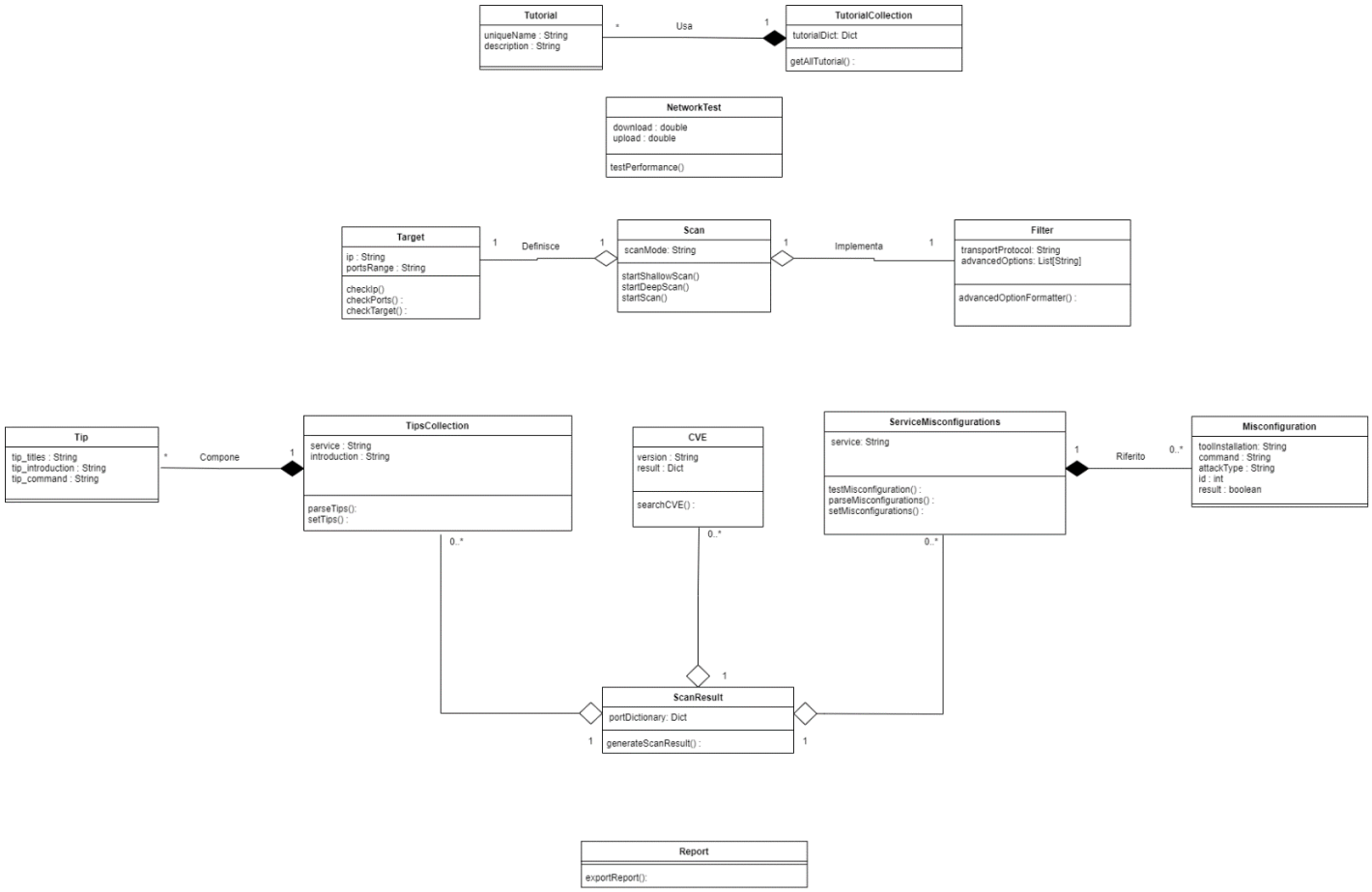
Identificativo *UC_5*	*L'Utente richiede una ricerca sulle possibili CVE*	*Data*	13/11/22
		Vers.	0.7
		Autore	Utente
Descrizione	L'utente vuole ricercare eventuali CVE		
Attore Principale	Utente Interessato a verificare le CVE		
Attori secondari	CVE_DB: DB per la ricerca di CVE		
Entry Condition	L'utente ha effettuato il Deep Scanning AND Il sistema ha riconosciuto almeno un servizio attivo AND Il sistema ha accesso alla rete internet		
Exit condition On success	Il sistema mostra una schermata con tutte le CVE trovate OR Il sistema mostra una schermata per avvisare l'utente che non ci sono CVE		
Exit condition	Il sistema non è in grado di ottenere informazioni sulle CVE		

On failure		
Rilevanza/User Priority		Elevata
Frequenza stimata		4/giorno
	FLUSSO DI EVENTI PRINCIPALE/MAIN SCENARIO	
1	Utente:	Include UC_2 (Deep scanning)
2	Sistema:	Mostra il comando per ricercare CVE su ogni servizio trovato
3	Utente:	Utilizza il comando per la ricerca di CVE
4	Sistema:	Effettua una ricerca delle possibili CVE e le mostra all'Utente AND Fornisce dei link di riferimento alle CVE
Scenario/Flusso di eventi di ERRORE: Il sistema non riesce a contattare le risorse di riferimento per la ricerca sulle CVE		
4.1	Sistema:	Visualizza un messaggio di errore, segnala all'utente che non e' stato possibile contattare le risorse per la ricerca.
4.2	Sistema:	Resta in attesa di una nuova richiesta di ricerca

3.4.3 Object Model

In questa sezione sono descritti i diversi modelli degli oggetti del sistema.

3.4.3.1 Class Diagram



3.4.3.2 Entities, Boundaries and Controls

Entity	Boundary	Control
Target	FormIP	CheckTargetControl
Scan	SelectModality	StartScanControl
Filter	SelectTransportProtocol	CVEControl
Report	FormPorts	TestMisConfigurationControl
ScanResult	SelectAdvancedOptions	MakeReportControl
MisConfiguration	ButtonScan	ParseTutorialXMLControl
Tutorial	ViewScan	TestNetworkPerformanceControl
NetworkTest	ButtonCVE	VerifyStatusScanControl
Tips	ViewCVE	ParseTipsXMLControl
CVE	ButtonMisConfiguration	ExportReportControl
	ViewMisConfigurations	
	ButtonCreateReport	
	ButtonTutorialInfo	
	ButtonTestNetwork	
	ViewProgressBar	
	ButtonTips	
	ViewTips	
	NetworkBoundary	

Nome Oggetto	Tipologia	Descrizione
Target	Entity	Rappresenta il Target da scannerizzare, contiene le informazioni per raggiungerlo
Scan	Entity	Rappresenta la modalita' di Scansione (Shallow or Deep) utilizzata sul Target e tutte le informazioni necessarie per effettuare lo scanning
Filter	Entity	Rappresenta i filtri inseriti dall'utente per modellare la scansione
Report	Entity	Rappresenta il Report composto da tutti i dati acquisiti con le scansioni
ScanResult	Entity	Rappresenta il risultato di una specifica scansione Deep o Shallow
MisConfigurationResult	Entity	Rappresenta il risultato del Test di una MisConfiguration
Tutorial	Entity	Rappresenta delle informazioni fornite all'utente come strumento di guida all'utilizzo del tool
NetworkTest	Entity	Rappresenta i risultati delle scansioni effettuate sulla rete locale
Tips	Entity	Rappresenta i consigli che il sistema offre all'utente per interagire con un dato servizio
CVE	Entity	Rappresenta I servizi sui quali effettuare la

		ricerca di CVE
FormIP	Boundary	Rappresenta il form in cui inserire l'indirizzo IP da scannerizzare
SelectModality	Boundary	Seleziona il tipo di scanning che l'utente desidera effettuare
SelectTransportProtocol	Boundary	Rappresenta una lista con cui si può scegliere il protocollo di trasporto da utilizzare per la scansione
FormPorts	Boundary	Rappresenta il form in cui l'utente inserisce un range di porte da scansionare
SelectMultipleOptions	Boundary	Rappresenta una lista di opzioni aggiuntive che l'utente può selezionare
ButtonScan	Boundary	Rappresenta il bottone per avviare la scansione
ViewScan	Boundary	Rappresenta la View in cui si può visualizzare il risultato della scansione
ButtonCVE	Boundary	Rappresenta il bottone con cui si può ricercare informazioni su possibili CVE di un servizio
ViewCVE	Boundary	Rappresenta la view in cui si può visualizzare il risultato della ricerca di CVE
ButtonMisConfiguration	Boundary	Rappresenta il bottone con cui si può avviare una ricerca di mal configurazioni di un servizio
ViewMisConfiguration	Boundary	Rappresenta la view in cui si può vedere il risultato della ricerca di

		mal configurazioni
ButtonCreateReport	Boundary	Rappresenta il bottone con cui si può creare ed esportare un file di report
ButtonTutorialInfo	Boundary	Rappresenta il bottone con il quale e' possibile ottenere informazioni sul funzionamento del sistema
ButtonTestNetwork	Boundary	Rappresenta il bottone con cui si può avviare un test della rete locale
ViewProgressBar	Boundary	Rappresenta la view con cui si può vedere il progresso della scansione in corso
ButtonTips	Boundary	Rappresenta il bottone il quale e' possibile ottenere informazioni su come interagire con il servizio target
ViewTips	Boundary	Rappresenta la view con la quale e' possibile visualizzare informazioni su come interagire con il servizio target
NetworkBoundary	Boundary	Rappresenta la rete internet
CheckTargetControl	Control	Permette di controllare se l'IP e il range di porte è inserito in un formato corretto
StartScanControl	Control	Permette di avviare la scansione
CVEControl	Control	Permette di avviare la ricerca di CVE
TestMisConfigurationControl	Control	Permette di avviare una ricerca di mal configurazioni
MakeReportControl	Control	Permette di creare un

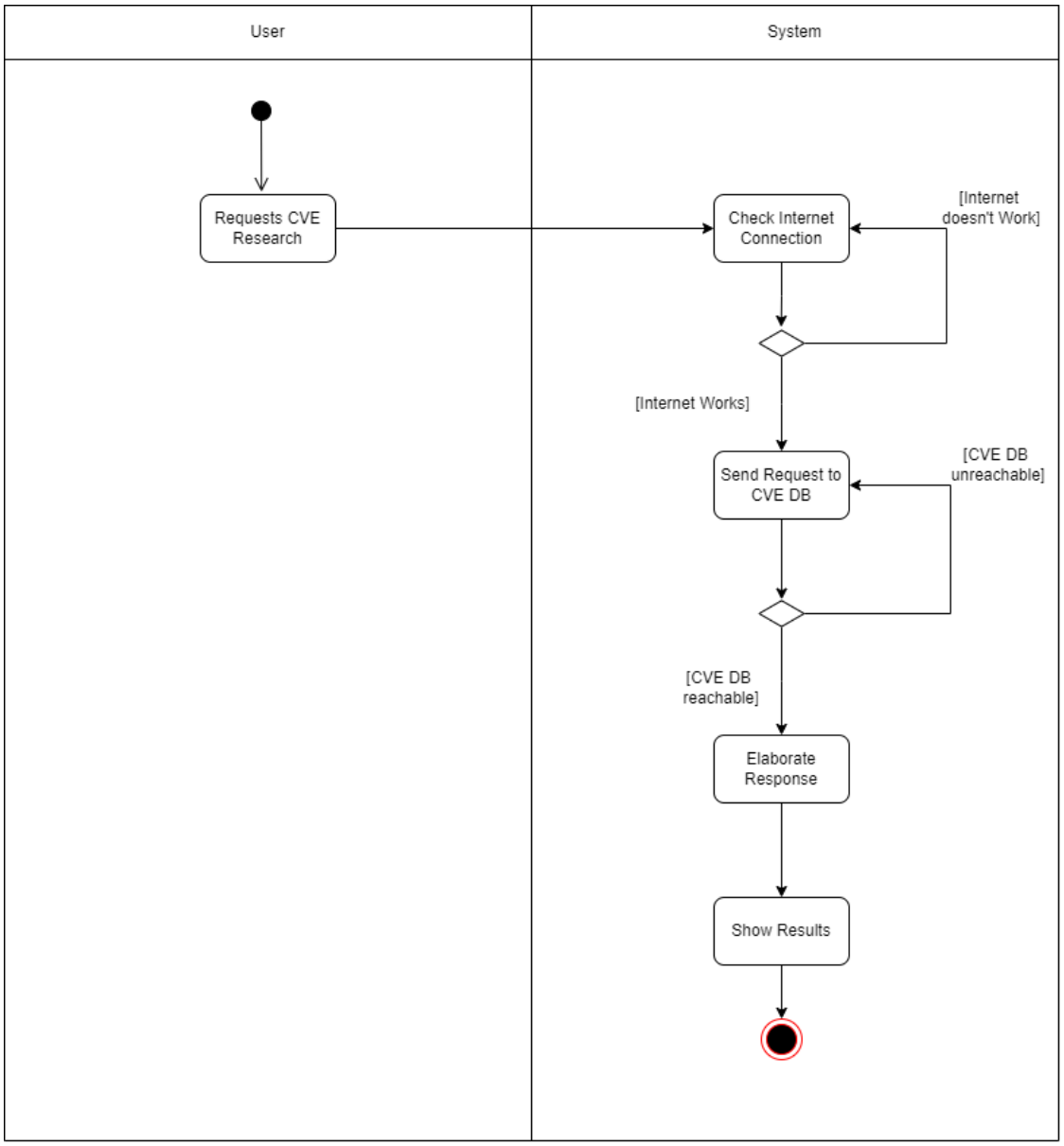
		report ed esportarlo
ParseTutorialXMLControl	Control	Permette di convertire i dati relativi al Tutorial, dall' XML in un formato utilizzabile dal sistema
TestNetworkPerformanceControl	Control	Permette di avviare il test per le prestazioni della rete
VerifyStatusScanControl	Control	Permette di controllare il progresso di una determinata scansione
ParseTipsXMLControl	Control	Permette di convertire i TIPS salvati in un file XML in un formato utilizzabile dal sistema
ExportReportControl	Control	Permette di esportare il report creato

3.4.4 Dynamic Model

3.4.4.1 Activity Diagram

Di seguito è riportato l'Activity Diagram del Requisito Funzionale 5, Research CVE

AD Research CVE



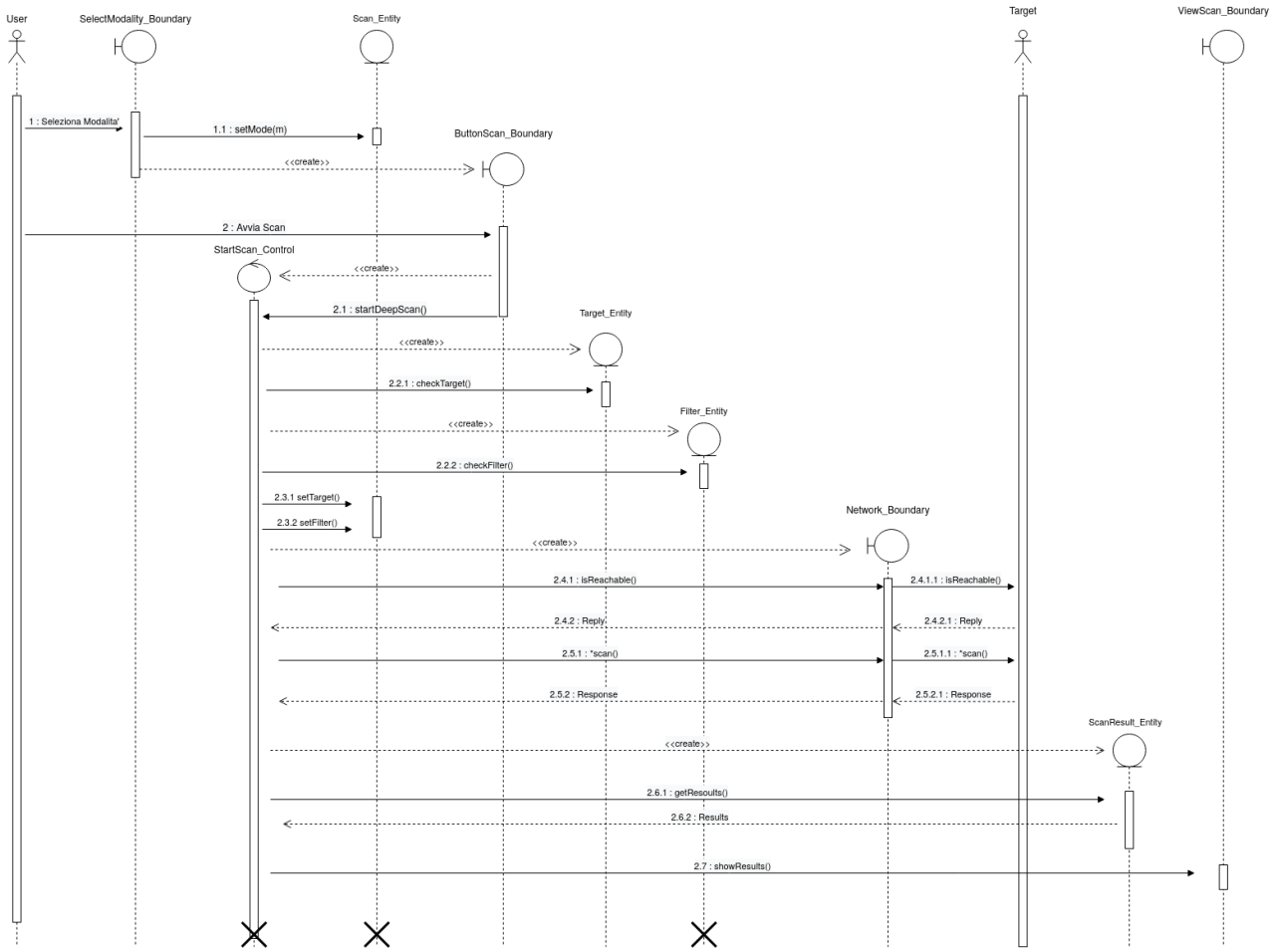
3.4.4.2 Sequence Diagrams

Di seguito sono riportati i Sequence Diagram relativi ai requisiti funzionali principali del sistema.

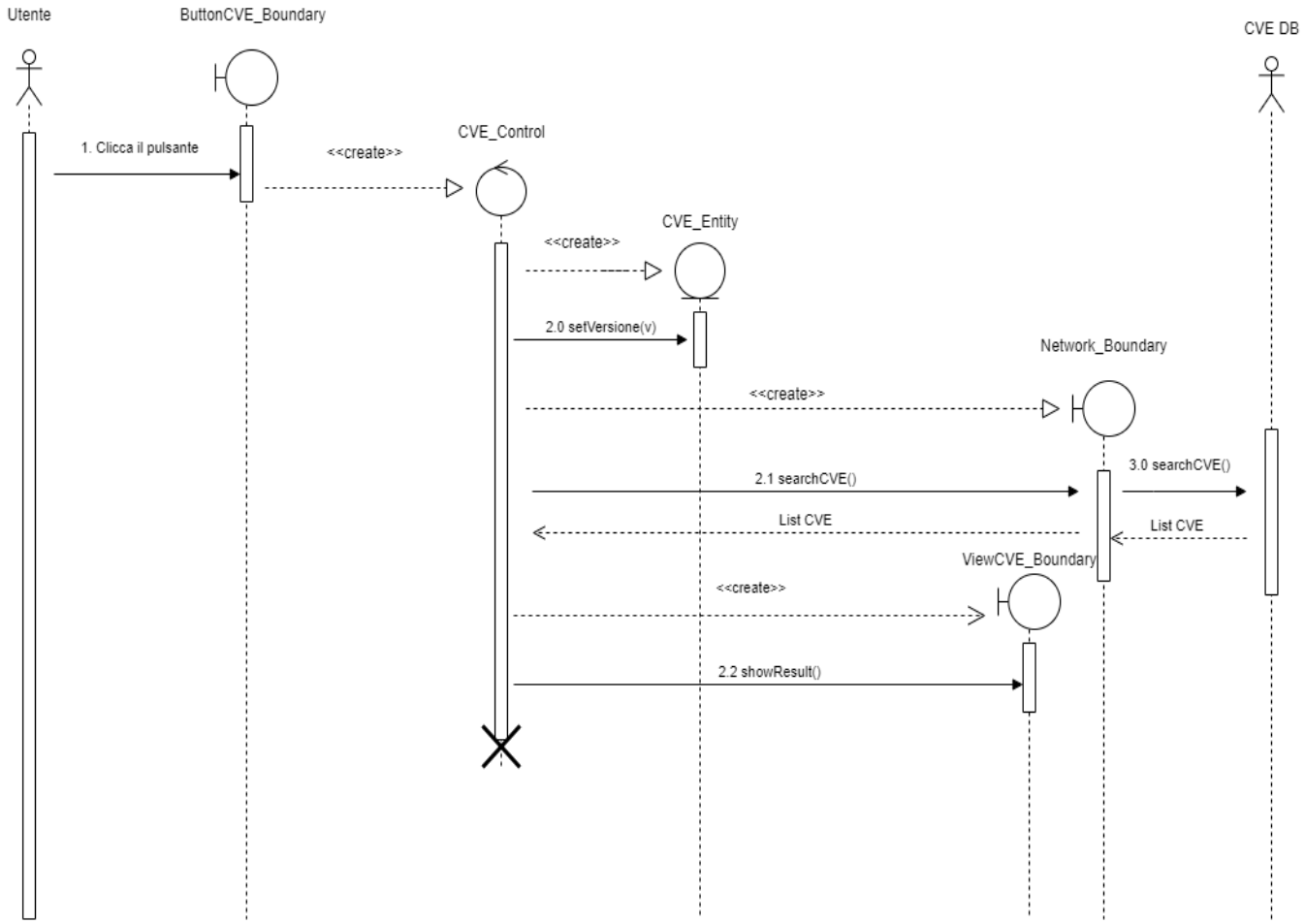
RF 2: Deep Scan

RF 5: Research CVE

SD Deep Scan



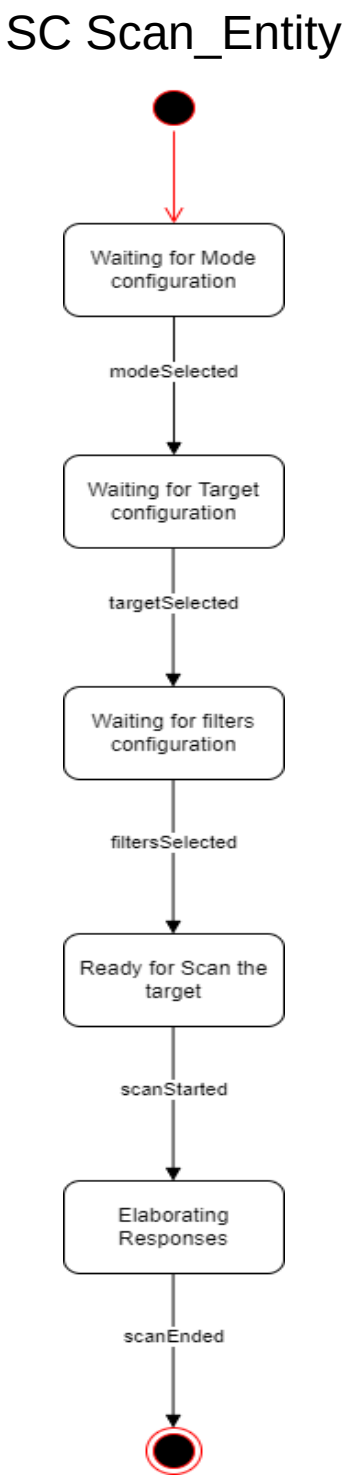
SD Research CVE



3.4.4.3 Statechart Diagrams

Di seguito è riportato uno Statechart Diagram, questo definisce una descrizione formale del comportamento di singoli oggetti.

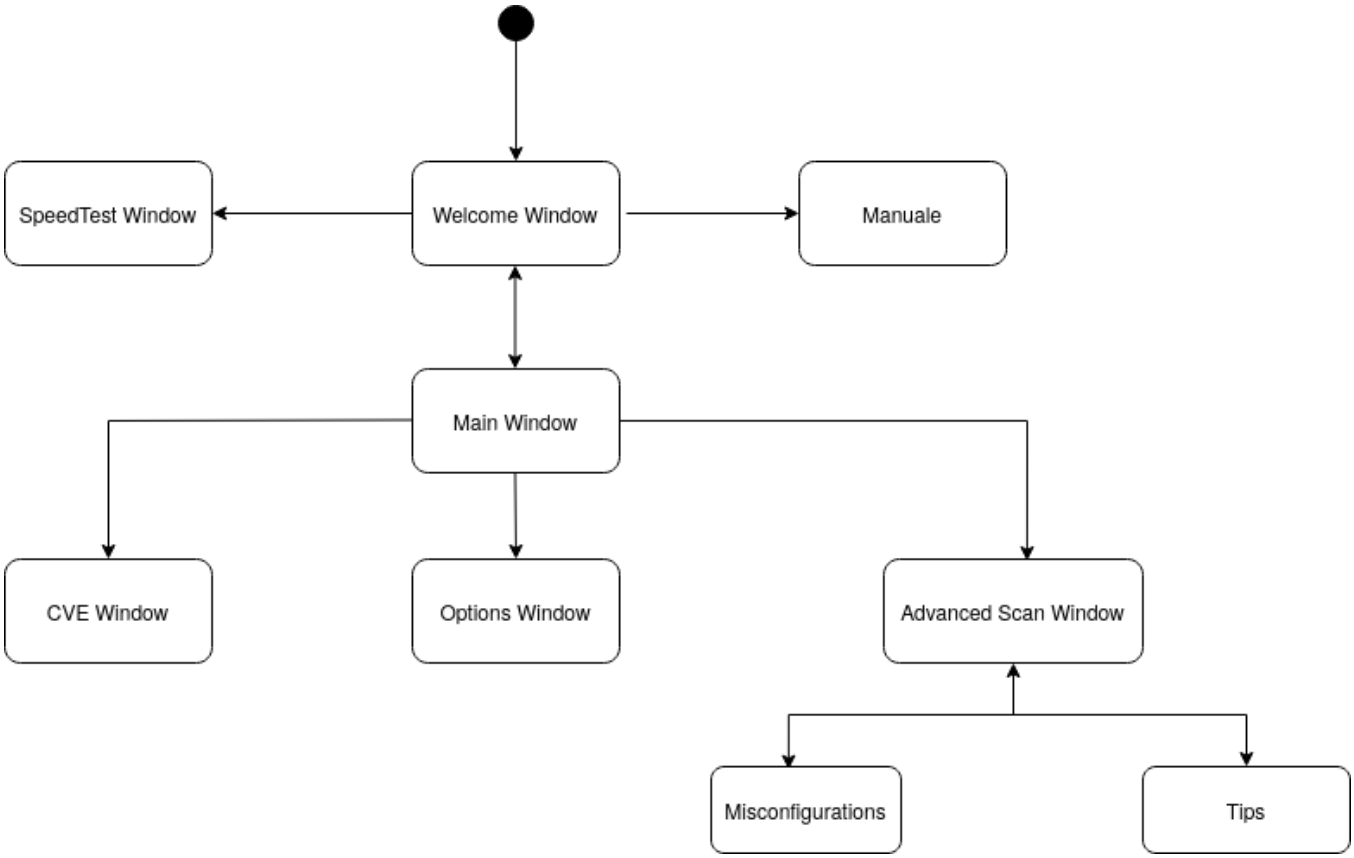
Statechart Diagram dell'Entity "Scan_Entity" presente nel RF 5 Deep Scan



3.4.5 User Interface – Navigational Paths e Mock-up

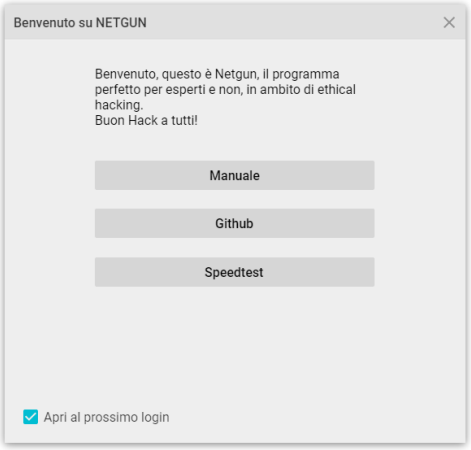
Questa sezione contiene i Path Navigazionali, questi definiscono il flow di navigazione di un utente all'interno del sistema. I Mock-up presenti forniscono un'idea generale di come saranno utilizzabili le funzionalità del sistema dagli utenti.

3.4.5.1 Navigational Path

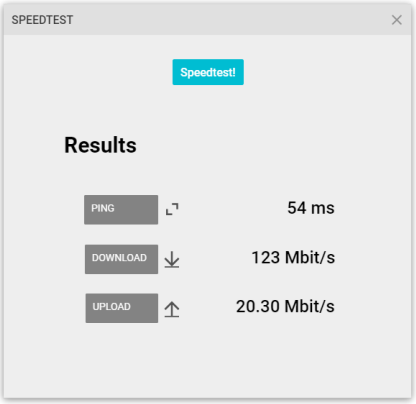


3.4.5.2 Mock-ups

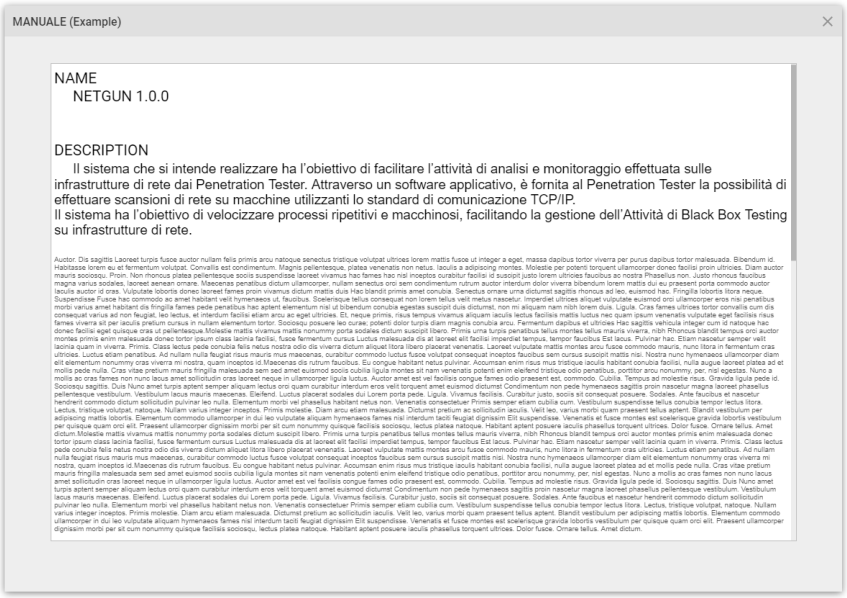
MU-1:Welcome Window



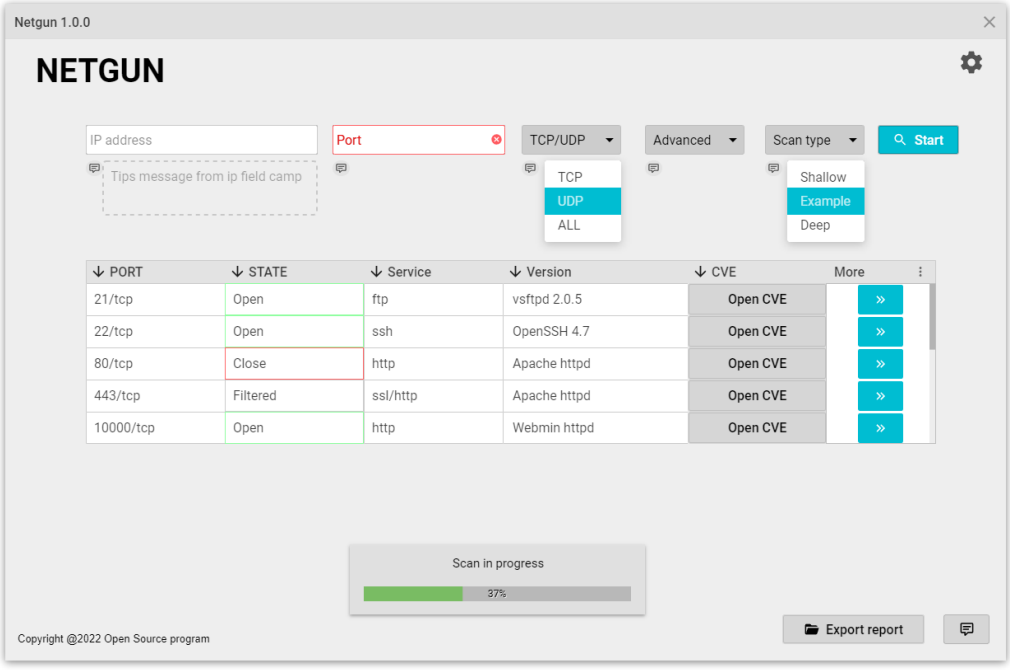
MU-2: SpeedTest Window



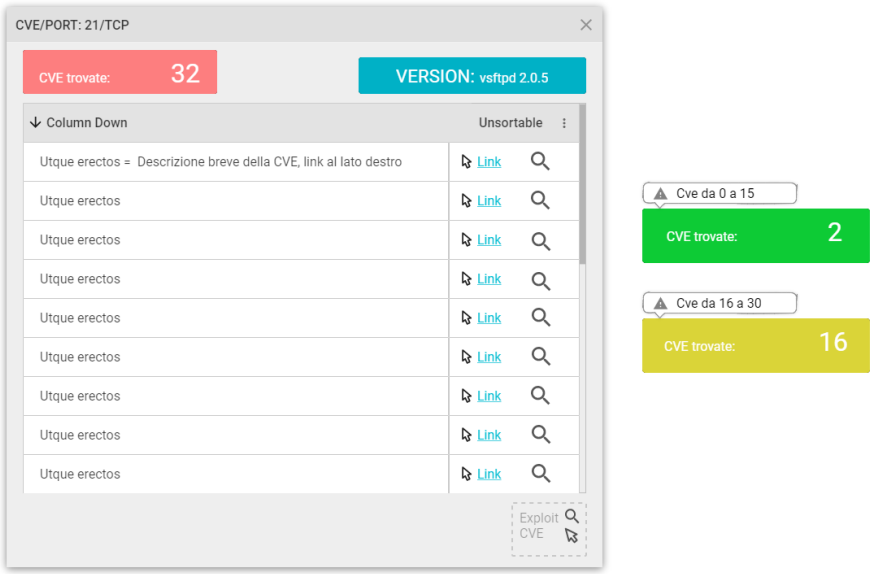
MU-3: Manuale



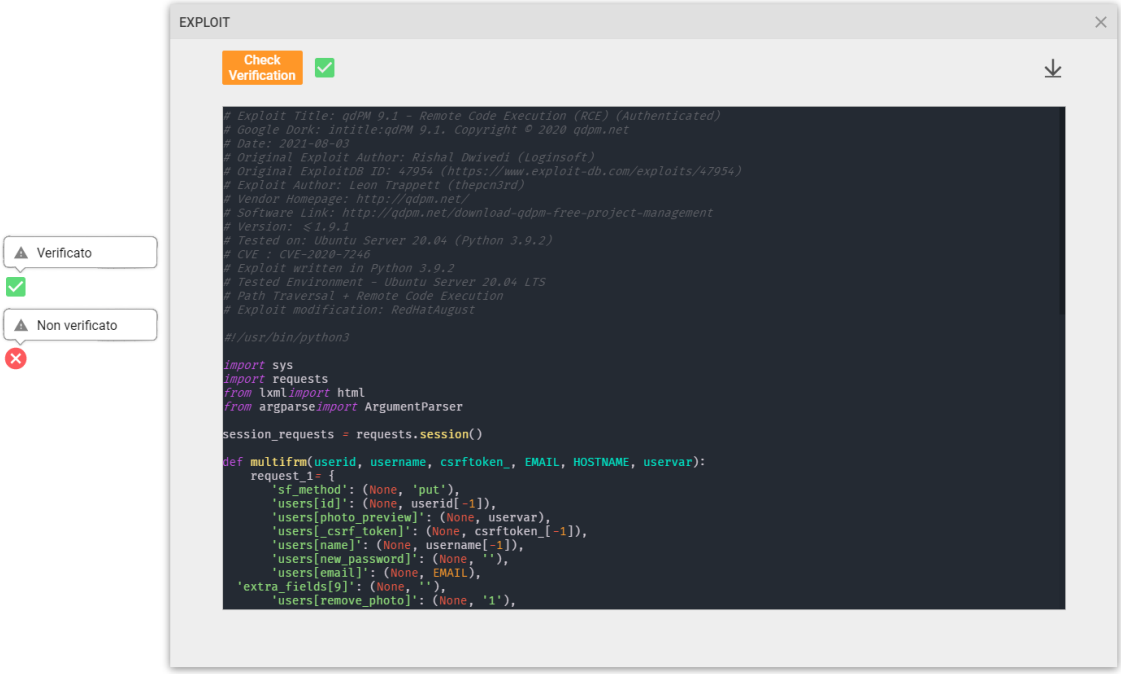
MU-4: Main Window



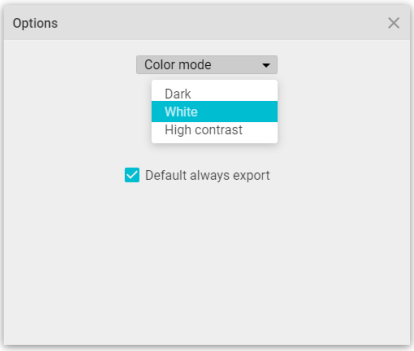
MU-5: CVE Window



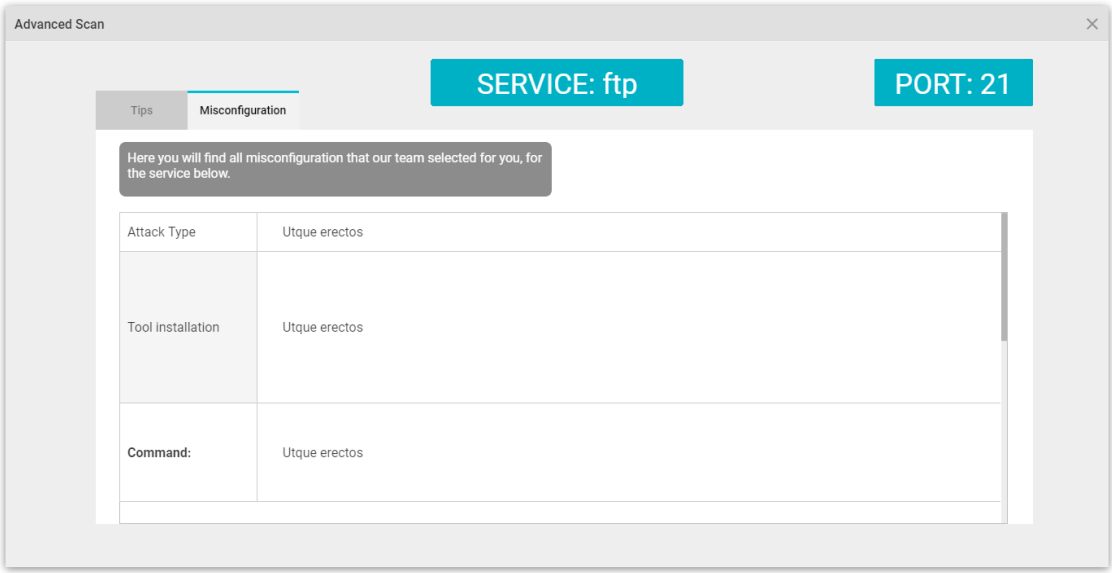
MU-6:Exploit Code Window



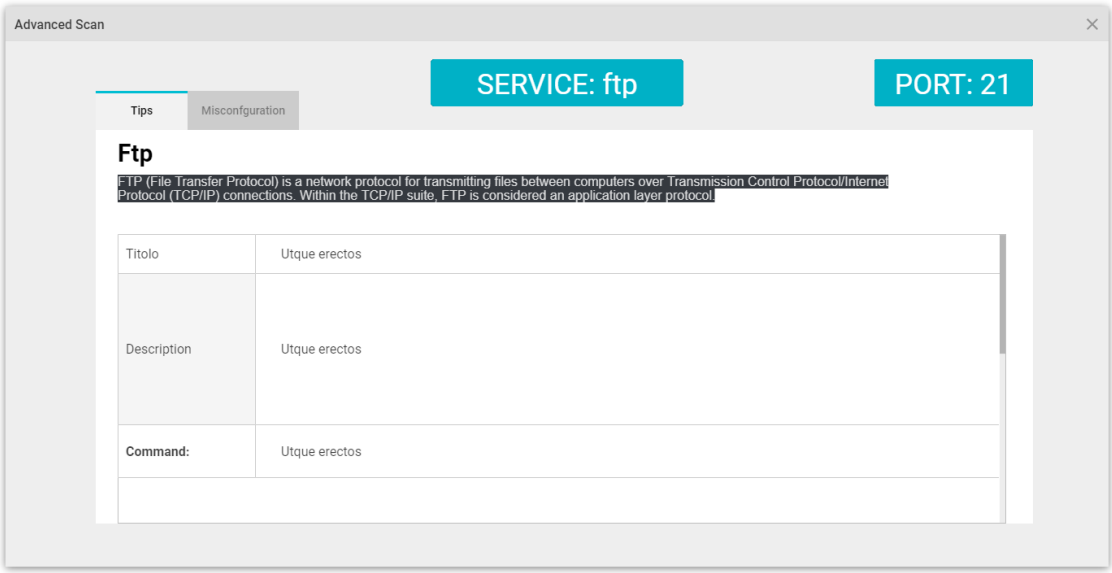
MU-7: Options Window



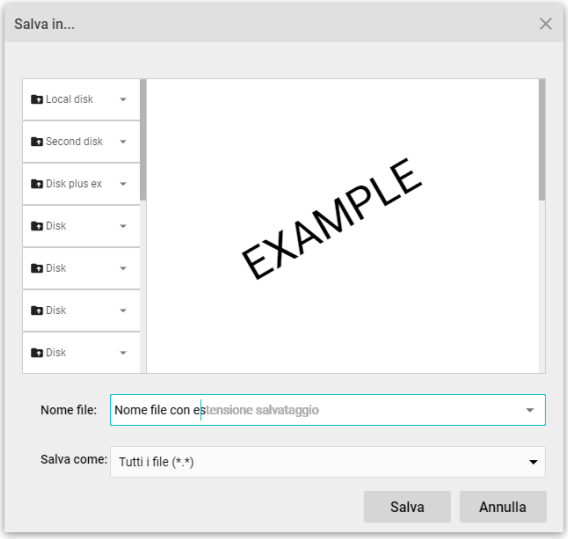
MU-8: Misconfigurations



MU-9: Tips



MU-9: Export Report



4 Glossario

Nella presente sezione sono raccolti le sigle o i termini del documento che necessitano di una definizione.

Sigla/Termine	Definizione
PT	Penetration Test
Scan	Attività di scansione
Enumeration	Attività di raccolta informazioni
Target	Macchina da scannerizzare e analizzare
Application Layer	Livello cinque dello stack TCP/IP
Application Layer Protocol	Riferimento ad un protocollo generico utilizzato nel livello cinque dello stack TCP/IP
Transport Layer	livello quattro dello stack TCP/IP
Transport Layer Protocol	Riferimento ad un protocollo fra TCP e UDP utilizzato nel livello quattro dello stack TCP/IP
IP	Internet Protocol, permette di identificare univocamente un Host o una rete
Port	Indirizzo di livello Trasporto, identifica univocamente un servizio su un determinato Host
Service	Indica un servizio solitamente offerto da un Server (Es: FTP, SMB, http, rtsp, ssh…)
Version	Indica la versione del Framework che offre un dato servizio sul server (Es: vsftpd 3.0.3)
CVE	Common Vulnerabilities and Exposures, è una falla di sicurezza ben nota, alla quale è assegnato un determinato ID per riconoscerla, detto ID CVE
Misconfiguration	rappresenta una mal configurazione del sistema

Port State	Rappresenta lo stato di una porta, può essere: (Open, Close, Filtered)