Greenbone Community Edition

Interfaccia web

Leandro Lanzi

Tutorial days di CCR: Cybersicurezza

Laboratori Nazionali di Frascati, 10-12 ottobre 2022

Indice

1 Interfaccia web di Greenbone Comunity Edition

- L'interfaccia web di Greenbone Comunity Edition (GCE) viene indicata col nome Greenbone Security Assistant e, di solito, vi si accede collegandosi in HTTPS alla porta 443 dell'host su cui è stato installato GCE.
- Dalla pagina di login, dopo aver inserito le proprie credenziali ed aver avuto accesso alla piattaforma, soprattutto al primo accesso subito dopo l'installazione, è opportuno verificare quale sia lo stato di aggiornamento del sistema. Si accede a questa informazione scegliendo nella *Toolbar*:
  - *Administration*
  - *Feed Status*

  Non deve esser presente l'indicazione *"Update in progress..."* in nessun *Status* dei vari *Feed*; se fosse presente tale indicazione, attendere che si siano conclusi gli aggiornamenti dei *Feed* prima di iniziare ad usare l'interfaccia web.

2 Toolbar e comandi dell'interfaccia web

Tutte le operazioni su GCE tramite l'interfaccia web si effettuano:

- andando a selezionare la voce opportuna nella *Toolbar* (figura 1 a pagina 1), Dashboard, Scans, Assets, ...,
- seguendo eventuali link nelle pagine visualizzate,
- operando sui comandi posizionati subito sotto la *Toolbar* in alto a sinistra nella pagina (figura 2 a pagina 2),
  Help..., *New...*, *Import...*,
- eseguendo le *Actions* nella colonna a destra nelle varie tabelle (figura 3 a pagina 2), *Start Tast*, *Resume Task*, *Delete...*, *Edit...*, *Clone...*, *Export...*.

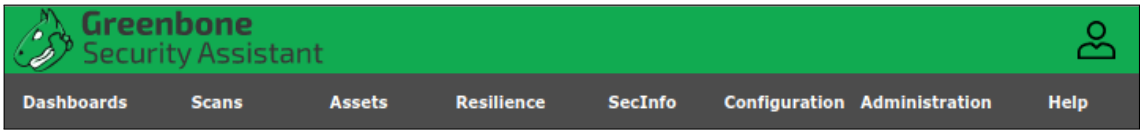

Figura 1: Toolbat di GCE.

3 Configurazione del proprio account

Per modificare le impostazioni del proprio account:

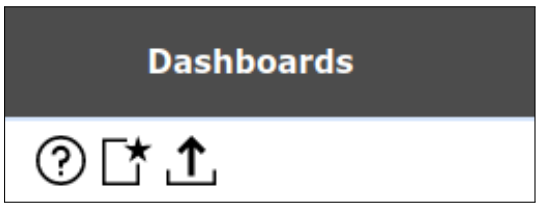

Figura 2: Comandi nelle pagine web: *Help...*, *New...*, *Import...* .

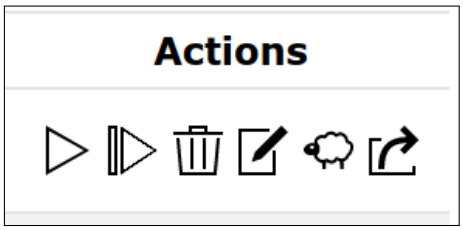

Figura 3: Azioni nelle pagine web: *Start Task*, *Resume Task*, *Delete...*, *Edit...*, *Clone...*, *Export...* .

- Icona dell'utente (in alto a destra)
- *My Settings*
- *General Settings*
- Icona Edit (in alto a sinistra)

Si può, per esempio, modificare:

- la password,
- il numero di righe delle tabelle con cui vengono visualizzati i dati (*Rows Per Page*),
- il fuso orario (*Timezone*) utilizzato per tutte le date e gli orari presenti nelle varie schermate.
- ...

4 Configurazione di un utente per accesso non privilegiato alle macchine da passare a scansione

Per funzionare al meglio e ottenere migliori informazioni dalle scansioni è molto utile (se non necessario) creare un utente non privilegiato sulle macchine da passare a scansione.
Per esempio:

- username: `openvas`
- password: `1-love-CCR-tooo-much!`

Per registrare in GCE le credenziali di accesso di tale utente seguire le seguenti indicazioni.

- Dalla *Toolbar* scegliere: *Configuration* > *Credentials*.
- Sotto la *Toolbar* in alto a sinistra fare click con il puntatore del mouse sull'icona raffigurante un rettangolo con una stella (*New Credential*) per creare una nuova credenziale.
- Compare la maschera per l'inserimento della nuova credenziale. Scegliere un nome (*Name*) per identificare le credenziali, per esempio `INFN_221008`. Riempire i campi impostando i valori di *Username Password* in accordo con quelli creati opportunamente sulla macchina da passare a scansione e premere il pulsante *Create*.

5 Parametri di esecuzione delle scansioni

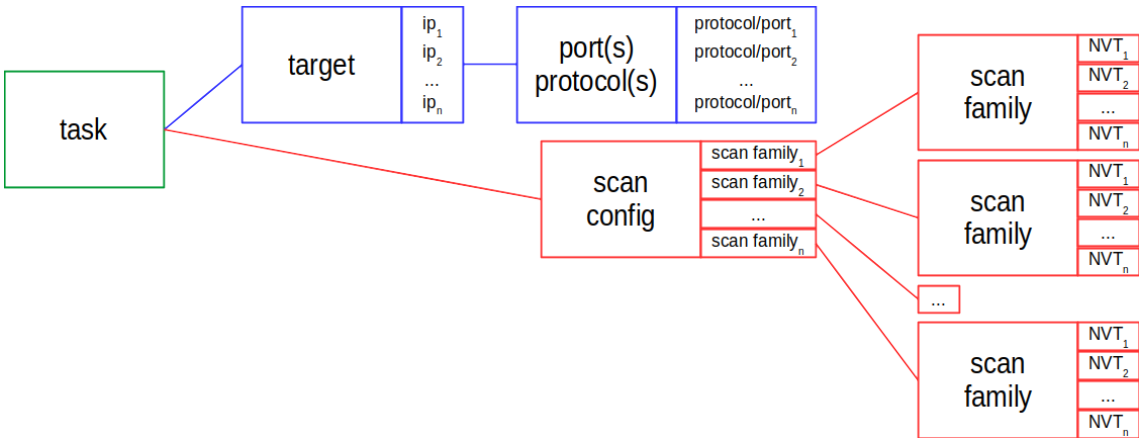

Figura 4: Parametri delle scansioni Greenbone Comunity Edition (GCE).

Le scansioni di Greenbone Comunity Edition (GCE) vengono organizzate per *Task* (figura 4).
Ogni *Task*[1] ha per bersaglio (*Target*[2]) un certo numero di IP e un elenco di coppie porta/-protocollo (TCP/UDP) da passare a scansione.
La modalità con cui le triplette (IP, protocollo, porta) vengono passata a scansione è definita nella configurazione della scansione (*Scan Config*[3]).
Una *Scan Config* è costituita da un insieme di famiglie di scansioni (*"Family"*) e ciascuna *Family* a sua volta è costituita da un insieme di test che nel linguaggio di GCE vengono chiamati *NVT* (Network Vulnerability Test) o semplicemente VT (Network Vulnerability Test).
Per esempio, una delle *scan config* predefinite è la *Full and fast* che richiama[4] 58 *Family* per un totale di 113173 *NVT*. Una delle *scan family* è, per esempio, la *Brute force attacks* che richiama 9 NTV, cioè 9 test differenti.

[1] *Toolbar* > *Scans* > *Tasks*
[2] *Toolbar* > *Configuration* > *Targets*
[3] *Toolbar* > *Configuration* > *Scan Configs*
[4] Valori aggiornati al giorno 08/10/2022

Si deve tenere presente che non è possibile modificare le *Scan Config* e le *Port List* di default e quelle che sono già state utilizzate per compiere le scansioni, cioè quelle utilizzate in uno o più *Task*.
Per impostare delle *Scan Config* e delle *Port List* personalizzate si consiglia di clonare (tramite l'icona raffigurante la pecora Dolly nella colonna *Actions*) le *Scan Config* e le *Port List* di default che più si avvicinano alle proprie esigenze e di modificarle prima di configurare i *Task* altrimenti dopo non possono più esser modificate.

6 Configurazione delle scansioni (*Task*)

Prima di configurare una scansione (*Task*) su uno o più IP è necessario aver configurato:

- *Port List*,
- *Scan Config*,
- *Target*.

6.1 Configurazione delle *Port List*

Per impostare una *Port List* personalizzata si consiglia di clonare (tramite l'icona raffigurante la pecora Dolly) una *Port List* di default che più si avvicini alle proprie esigenze e di modificarla prima di configurare i *Task* che la richiamano altrimenti dopo non può più esser modificata.
La procedura consigliata è quindi la seguente.

- *Toolbar* > *Configuration* > *Port Lists*.
- Clonare per esempio la *Port List*: *"All TCP and Nmap top 100 UDP"* .
- Modificare la *Port List* appena creata: *"All TCP and Nmap top 100 UDP Clone 1"*.
  - Modificare il nome (*Name*), per esempio, in `INFN_221008`.
  - Inserire eventualmente un commento (*Comment*).
  - Eliminare eventualmente delle definizioni.
  - Aggiungere eventualmente nuove porte/protocolli o intervalli di porte con i relativi protocolli.
    Si consiglia di aggiungere le porte UDP che, secondo le policy concordate, dovrebbero essere chiuse e/o opportunamente filtrate[5]. Quelle non già presenti in elenco dovrebbero essere solo le porte UDP: 19, 21, 141, 3300 e 6789. Le porte TCP sono già tutte selezionate.
  - Salvare le modifiche con il pulsante *Save*.

[5]Porte UDP da chiudere e/o filtrare: 7, 19, 21, 69, 111, 141, 161, 162, 3300, 6789

6.2 Configurazione delle *Scan Config*

Per impostare una *Scan Config* personalizzata si consiglia di clonare (tramite l'icona raffigurante la pecora Dolly) una *Scan Config* di default che più si avvicini alle proprie esigenze e di modificarla prima di configurare i *Task* che la richiamano altrimenti dopo non può più esser modificata.
La procedura consigliata è quindi la seguente.

- *Toolbar* > *Configuration* > *Scan Configs*.
- Clonare per esempio la *Scan Config*: *"Full and fast"* .
- Modificare la *Scan Config* appena creata: *"Full and fast Clone 1"*.
  - Modificare il nome (*Name*), per esempio, in `INFN_221008`.
  - Inserire eventualmente un commento (*Comment*).
  - Per ogni elemento della sezione *"Edit Network Vulnerability Test Families"* aggiungere o eliminare *Family* di scansioni con la casella di spunta nella colonna *"Select all NVTs"* o tramite il comando *Edit* nella colonna *Actions*.
    Si consiglia di aggiungere tutti gli NVT disponibili.
  - Nella sezione *"Edit Scanner Preferences"* si possono modificare alcuni parametri che influenzano molto la modalità di esecuzione della scansione e la sua durata.
    Si consiglia:
    * **open_sock_max_attempts: 2**
    * **plugins_timeout: 300**
    * **scanner_plugins_timeout: 300**
    * **timeout_retry: 2**

    Una descrizione dettagliata di tutti i parametri delle scansioni è riportata a pagina 10 nella sezione 9.1.
  - La sezione *"Network Vulnerability Test Preferences"* permette di configurare il comportamento di molti dei NVT. Di solito si vanno a modificare i parametri di default solo per correggere la rilevazione di falsi positivi/negativi o se si intende effettuare una scansione particolare. Un esempio è riportato di seguito (sezione 6.2.1 a pagina 5)
  - Salvare le modifiche con il pulsante *Save*.

6.2.1 Esempio di modifica dei valori di default dei Network Vulnerability Test (NVT)

Nel definire una nuova *Scan Config* o nel modificarne una esistente di solito non si modificano i parametri di default dei *"Network Vulnerability Test* utilizzati.

Talvolta può essere utile modificare il loro parametri per correggere la rilevazione sistematica di falsi positivi o la non rilevazione di falsi negativi.
In altri casi può essere utile modificare tali parametri se si compiono scansioni particolari. Per esempio può essere utile rilevare la versione di un protocollo di cifratura utilizzato da un certo servizio ed impostare una policy che segnala l'uso di un protocollo obsoleto con la seguente procedura.

- Nel momento in cui si definisce/modifica la *Scan Config*, scendere nei *"Network Vulnerability Test Preferences"* fino a quelli riportati in figura 5 a pagina 6.
- Modificare le impostazioni di default del NVT `SSL/TLS: Policy Check` con l'opportuno pulsante di modifica (figura 5 a pagina 6).
- Si apre la form per la modifica dei parametri di default del NVT (figura 6 a pagina 7).
- Impostare i valori opportuni dei vari parametri e salvare con il pulsante *Save* (figura 6 a pagina 7).

In questo modo, durante la scansione vengono controllate le versioni SSL/TLS impostate e in caso di violazione della policy viene indicata una vulnerabilità.

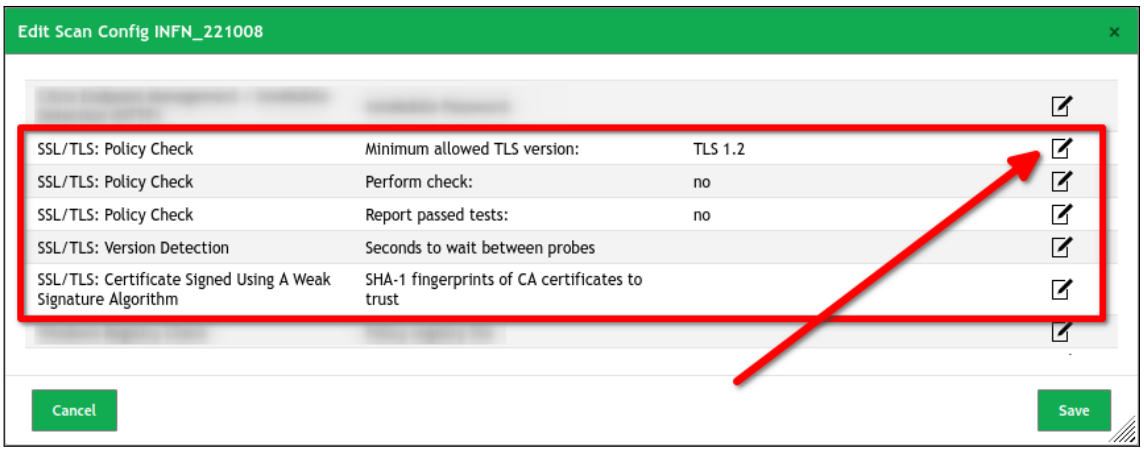

Figura 5: Parametri del NVT `SSL/TLS: Policy Check`.

6.3 Configurazione dei *Target*

L'impostazione di un *Target* consiste nella definizione degli IP e/o delle reti che si vogliono passare a scansione specificando quali *Port List* e quali *Credentials* utilizzare.
La procedura per configurare un *Target* è la seguente.

- *Toolbar* > *Configuration* > *Target*.
- Eseguire il comando *New Target* (rettangolo con stella in alto a sinistra della pagina).
- Nella form che compare riempire i seguenti campi.

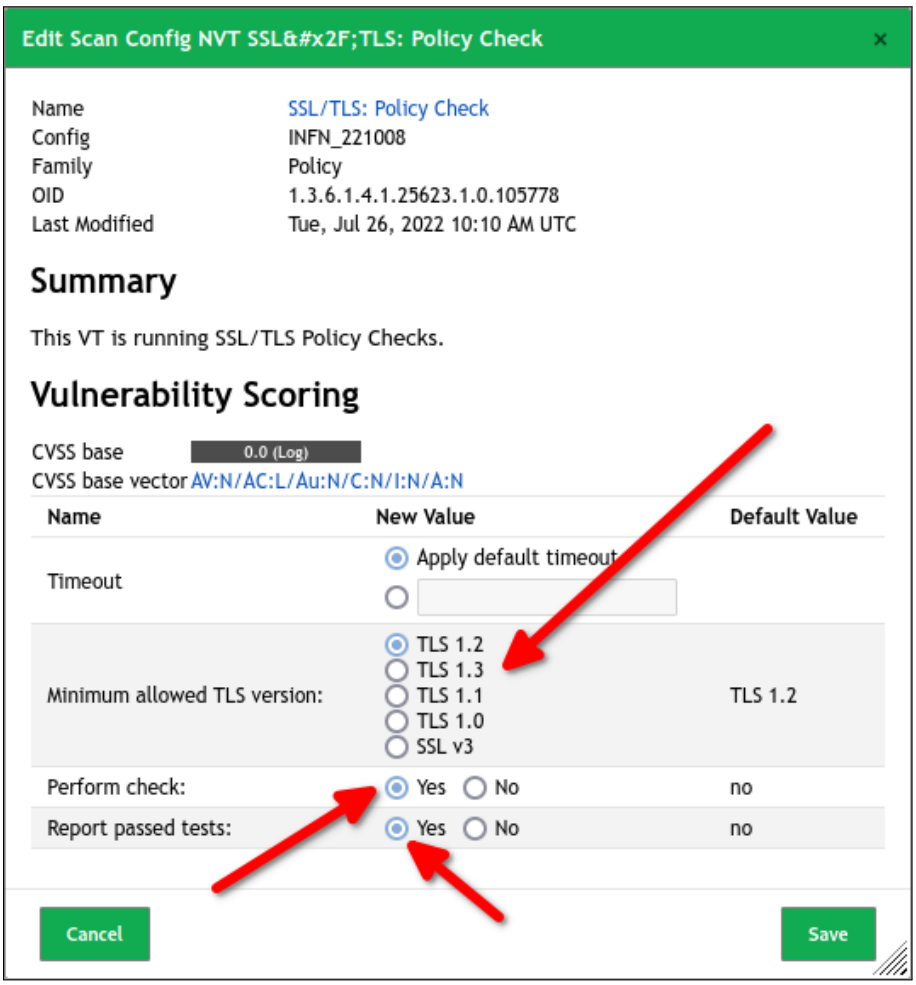

Figura 6: Modifica dei parametri di default del NVT `SSL/TLS: Policy Check`.

- *Name* è il nome con cui identificare il *Target*.
- Si può aggiungere una descrizione nel campo *Comment*.
- I singoli IP o le reti su cui effettuare la scansione si possono inserire nella sezione *Hosts* nel campo *Manual* separati da virgole o caricati da un file.
- Eventuali IP o reti da escludere dalla scansione si possono inserire nella sezione *Exclude Hosts* nel campo *Manual* separati da virgole o caricati nel campo *Manual* separati da virgole o caricati da un file.e.
- Nel campo *Port List* scegliere una *Port List* fra quelle di default oppure creata in precedenza. Per esempio scegliere la *Port List* creata in precedenza `INFN_221008`.
- Nel campo *Alive Test* scegliere il meccanismo che si vuole usare per verificare se l'host è acceso. Se la scansione viene eseguita su host sicuramente accesi si può scegliere l'opzione `Consider Alive`, mentre in generale si può scegliere `ICMP, TCP-ACK Service & ARP Ping`
- Nel campo *SSH* scegliere la *Credential* creata in precedenza (`INFN_221008`).
- Impostati tutti i parametri, premere il pulsante *Create*.

6.4 Configurazione dei *Task*

L'impostazione di un *Task* consiste nell'associare ad un *Target* una *Scan Config*.
La procedura per configurare un *Task* è la seguente.

- *Toolbar* > *Scans* > *Task*.
- Nella form che compare riempire i seguenti campi.
  - *Name* è il nome con cui identificare il *Task*.
  - Si può aggiungere una descrizione nel campo *Comment*.
  - Nel campo *Scan Targets* scegliere un *Target* creato in precedenza.
  - Di solito si lasciare impostato il valore di default nel campo *Min QoD* [6] .
  - Impostando il valore `Yes` nel campo *Alterable Task*, in futuro si può modificare i parametri del *Task*.
  - Nel campo *Scan Config* scegliere il tipo di scansione che si vuole effettuare, per esempio quella definita in precedenza `INFN_221008`.
  - Impostati tutti i parametri, premere il pulsante "Create".

7 Avvio delle scansioni (*Task*)

Per visualizzare tutte le scansioni (*Task*) impostate: *Toolbar* > *Scans* > *Task*.
Per avviare una scansione premere il pulsante *Start* nella colonna *Actions* della scansione che si vuole effettuare.

8 Consultazione dei risultati delle scansioni

Una volta che una certa scansione si è conclusa si possono consultare i risultati in vari modi.

8.1 *Reports*

Per accedere al riepilogo di tutti i *Report* di tutti i *Task* effettuati: *Toolbar* > *Scans* > *Reports*.

[6] **Quality of Detection (QoD)**
The QoD is a value between 0% and 100% describing the reliability of the executed vulnerability detection or product detection. One of the main reasons to introduce this concept was to handle the challenge of potential vulnerabilities properly. The goal was to keep such in the results database but only visible on demand. While the QoD range allows to express the quality pretty refined, in fact most of the test routines use a standard methodology. Therefore the QoD Types were introduced of which each is associated with a QoD value. The Feed content is updated over time to add a QoD for all NVTs. Any NVT not explicitly assigned will apply 75% and therefore visible by default in order to not change the default behavior compared to OpenVAS-7. However, meanwhile any NVTs formerly requiring the "paranoid" setting in the scan configuration is now reporting always but stay invisible in the database until the user decides to view results with a lower quality of detection.

Si ottiene una tabella che riporta il numero di vulnerabilità per ogni *Task* effettuato oltre ad altre informazioni.
Per visualizzare i risultati di un singolo *Report* si segue il link nella colonna *Date* del *Report* di interesse.
Si ottiene una pagina da cui è possibile accedere a tutti i i risultati della scansione organizzati per *Results*, *Hosts*, *Ports*, ...
Sempre da questa pagina è possibile esportare il *Report* in vari formati come PDF, CVS, TXT, HTML (figura 7 a pagina 9).

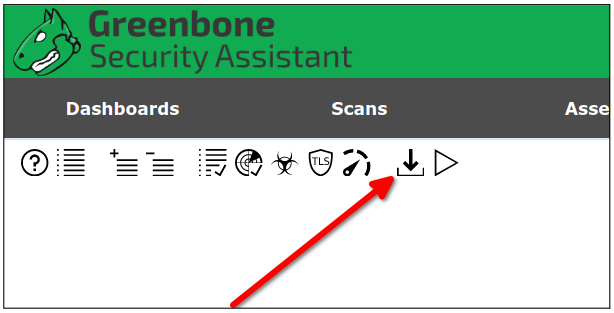

Figura 7: Esportazione dei *Report*.

8.2 *Results*

Per visualizzare tutte le vulnerabilità di tutti i singoli IP oggetto di scansioni: *Toolbar* > *Scans* > *Results*.
Si ottiene una tabella in cui in ciascuna riga è riportata la singola vulnerabilità rilevata per un particolare IP con il suo grado do criticità oltre ad altre informazioni.

8.3 *Vulnerabilities*

Per visualizzare tutte le vulnerabilità rilevate nelle scansioni: *Toolbar* > *Scans* > *Results*.
Si ottiene una tabella simile a quella descritta nella sezione precedente ma in cui i risultati sono raggruppati per vulnerabilità e viene riportato, oltre al grado do criticità della vulnerabilità, il numero di IP interessati dalla vulnerabilità (colonna *Hosts*) e il numero di volte che è stata rilevata (colonna *Results*).

9 Appendici

9.1 Scanner Preferences

- auto_enable_dependencies
  OpenVAS plugins use the result of each other to execute their job. For instance, a plugin which logs into the remote SMB reg- istry will need the results of the plugin which finds the SMB name of the remote host and the results of the plugin which at- tempts to log into the remote host. If you want to only select a subset of the plugins available, tracking the dependencies can quickly become tiresome. If you set this option to 'yes', open- vas will automatically enable the plugins that are depended on.

- cgi_path
  By default, openvas looks for default CGIs in /cgi-bin and /scripts. You may change these to something else to reflect the policy of your site. The syntax of this option is the same as the shell $PATH variable: path1:path2:...

- checks_read_timeout
  Number of seconds that the security checks will wait for when doing a recv(). You should increase this value if you are run- ning openvas across a slow network slink (testing a host via a dialup connection for instance)

- expand_vhosts
  Whether to expand the target host's list of vhosts with values gathered from sources such as reverse-lookup queries and VT checks for SSL/TLS certificates.

- non_simult_ports
  Some services (in particular SMB) do not appreciate multiple connections at the same time coming from the same host. This op- tion allows you to prevent openvas to make two connections on the same given ports at the same time. The syntax of this option is "port1[, port2....]". Note that you can use the KB notation of openvas to designate a service formally. Ex: "139, Ser- vices/www", will prevent openvas from making two connections at the same time on port 139 and on every port which hosts a web server.

- open_sock_max_attempts
  When a port is found as opened at the beginning of the scan, and for some reason the status changes to filtered/closed, it will not be possible to open a socket. This is the number of un- successful retries to open the socket before to set the port as closed. This avoids to launch plugins which need the opened port as a mandatory key, therefore it avoids an overlong scan dura- tion. If the set value is 0 or a negative value, this option is disabled. It should be take in account that one unsuccessful at- tempt needs the number of retries set in "timeout_retry".

- optimize_test
  By default, optimize_test is enabled which means openvas does trust the remote host banners and is only launching plugins against the services they have been designed to check. For exam- ple it will check a web server claiming to be IIS only for IIS related flaws but will skip plugins testing for Apache flaws, and so on. This default behavior is used to optimize the scan- ning performance and to avoid false positives. If you are not sure that the banners of the remote host have been tampered with, you can disable this option.

- plugins_timeout
  This is the maximum lifetime, in seconds of a plugin. It may happen that some plugins are slow because of the way they are written or the way the remote server behaves. This option allows you to make sure your scan is never caught in an endless loop because of a non-finishing plugin. Doesn't affect ACT_SCANNER plugins.

- safe_checks
  Most of the time, openvas attempts to reproduce an exceptional condition to determine if the remote services are vulnerable to certain flaws. This includes the reproduction of buffer over- flows or format strings, which may make the remote server crash. If you set this option to 'yes', openvas will disable the plug- ins which have the potential to crash the remote services, and will at the same time make several checks rely on the banner of the service tested instead of its behavior towards a certain in- put. This reduces false positives and makes openvas nicer to- wards your network, however this may make you miss important vulnerabilities (as a vulnerability affecting a given service may also affect another one).

- scanner_plugins_timeout
  Like plugins_timeout, but for ACT_SCANNER plugins.

- test_empty_vhost
  If set to yes, the scanner will also test the target by using empty vhost value in addition to the target's associated vhost values.

- time_between_request
  Some devices do not appreciate quick connection establishment and termination neither quick request. This option allows you to set a wait time between two actions like to open a tcp socket, to send a request through the open tcp socket, and to close the tcp socket. This value should be given in milliseconds. If the set value is 0 (default value), this option is disabled and there is no wait time between requests.

- timeout_retry
  Number of retries when a socket connection attempt timesout.