



Contribution ID: 13

Type: **not specified**

SCAN-INFN

Monday, 24 May 2021 14:50 (20 minutes)

Nell'ambito dell'attività delle scansioni di vulnerabilità effettuate regolarmente dal gruppo security/auditing su tutti gli IP pubblici della rete INFN è stato scelto di sostituire il software proprietario per le scansioni di vulnerabilità Tenable Nessus (utilizzato fino a fine 2019) con il software opensource Greenbone Vulnerability Management (GVM) noto spesso come OpenVAS (OpenVAS è solo una parte della piattaforma GVM).

GVM è stato installato su 9 differenti server (scan-server), 4 al CNAF e 5 alla Sezione di Firenze, ma il numero può crescere senza problemi magari coinvolgendo altre Sedi.

L'uso di 9 differenti scan-server dislocati in più sedi permette:

- 1) di bilanciare il carico delle scansioni fra i vari scan-server,
- 2) di ridurre i tempi per compiere scansioni a tappeto su tutti gli IP pubblici della rete INFN,
- 3) di effettuare sempre scansioni dall'esterno della rete a cui appartiene l'IP passato a scansione (Firenze scansiona gli IP della rete del CNAF e viceversa, tutti gli altri IP saranno assegnati in modo casuale ad entrambe le sedi).

Tutto questo si realizza tramite una console centralizzata (vedi talk dal titolo "Greenbone Vulnerability Management + SCANBOT") che bilancia il carico delle scansioni fra i vari server e impedisce che un certo scan-server esegua scansioni su IP appartenenti alla propria rete.

Al completamento delle scansioni i dati sono esportati in formati standard ed importati in un unico database.

I risultati delle scansioni sono consultabili dagli utenti che hanno diritto a visionare tali dati tramite un'interfaccia web.

Questa interfaccia web permette anche di assegnare e gestire in modo molto specifico il diritto di visionare i risultati delle scansioni ai vari utenti che si autenticano tramite INFN-AAI.

E' previsto di assegnare questi diritti di accesso ai dati raggruppando gli utenti sia per Sede di appartenenza che per gruppi di IP e/o reti che possono essere definiti in modo trasversale alle Sedi INFN.

Primary author: LANZI, Leandro (INFN-FI)

Presenter: LANZI, Leandro (INFN-FI)

Session Classification: Servizi ICT

Track Classification: Servizi ICT