Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Gruppo di lavoro Sicurezza

SIMONA VENUTI

Roma, 29 Maggio 2018

WorkShop GARR 2018

Scansioni vulnerabilita’

Le misure minime di sicurezza chiedono di effettuare delle scansioni di vulnerabilita’ periodiche sulle proprie macchine

- Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
- Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.
- Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio

SCARR

SCA(nsioni)R(emote)R(ipetute)

https://scarr.garr.it

- Servizio di GARR-CERT per effettuare scansioni di vulnerabilita'
- Utilizzo di OpenVAS come backend
- E' necessario essere APM GARR della propria rete (o chiedere ad un APM)
- E' necessario avere un account GARRSSO
- E' necessario essere abilitati alle scansioni su GARRSSO
- Si puo' scansionare qualsiasi IP o rete della propria struttura
- 4 tipi di scansioni possibili: fast o completa, innocua o distruttiva
- Possibilita' di pianificare data e ora della scansione
- Possibilita' di ripetere le scansioni automaticamente 1 volta a settimana o 1 volta al mese senza dover loggarsi ogni volta
- L'APM riceve il report per mail
- L'APM in fase di richiesta scansione puo' chiedere di far spedire il report direttamente all'amministratore del sistema

Gruppo di lavoro sicurezza

- Si occupa di studiare, pensare, immaginare, inventare soluzioni per risolvere questioni inerenti la sicurezza nell'ambito della comunità GARR
  - Universita'
  - Enti di ricerca
  - Istituti vari
  - Scuole!
- Non è un posto dove si apprende qualcosa già fatto ma dove facciamo noi qualcosa che possa essere utile per tutti
  - Guide
  - Best practise
  - Architetture, soluzioni e configurazioni software
- APERTO A TUTTI, NON SOLO APM!!

Contatti

Cerchiamo persone che vogliano partecipare!!!

Sottogruppi

- Contrasto ai DDoS
- Monitoraggio – intrusion detection
- Autenticazione 8021.x su rete cablata
- Best practise (AUP e guide)

Possiamo inventarci nuovi sottogruppi ovviamente

https://wiki-wg-sec.garr.it