Contribution ID: **69** Type: **Presentazione orale**

Un Workflow per la scansione e la gestione delle vulnerabilità di sicurezza

Friday, 24 May 2024 09:25 (25 minutes)

Questo documento illustra la procedura operativa utilizzata per gestire il flusso di attività derivante dalle scansioni di sicurezza all'interno della LAN dei Laboratori Nazionali del Sud.
Le scansioni vengono svolte periodicamente, con una frequenza semestrale. Questa cadenza è stata definita da un'attività preparatoria volta all'identificazione di tutti gli indirizzi IP da sottoporre a scansione, ed una opportuna suddivisione in gruppi. Per ogni campagna di scansioni viene effettuata una ricognizione dell' intera LAN (una classe B) inviando pacchetti ICMP in parallelo, allo scopo di individuare in modo veloce ed affidabile tutti gli host raggiungibili [1] e di valutare la distribuzione degli stessi nelle varie subnet. Questa suddivisione permette di pianificare le scansioni in modo efficace, evitando che ciascuna scansione generi report riguardanti un numero eccessivo di host, poi difficili da gestire. Le scansioni di vulnerabilità (note e potenziali) sono eseguite utilizzando Greenbone Vulnerability Manager (GVM)[2] su Debian GNU/Linux, i cui Community Feed sono mantenuti aggiornati per garantire affidabilità alla procedura. Se necessario, con alcuni host, è previsto utilizzare anche le funzionalità di scripting di Nmap [3] per effettuare ulteriori analisi e assessment.
Dopo l'esecuzione delle scansioni, si procede con il trattamento dei report XML generati da ogni scansione di Greenbone. A tale scopo è stata predisposta una app dedicata sviluppata in Python che: i) processa i dati; ii) li filtra opportunamente; iii) applica diverse strategie di ranking; iv) produce in output dei documenti riepilogativi in pdf e markdown. Questi documenti sono allegati alla comunicazione inviata ai responsabili degli host interessati, per rendere più trasparente le informazioni relative alle vulnerabilità individuate e le contromisure proposte. Per integrare efficacemente questa attività con i workflow già in produzione, si fa uso di Jira Service Management (JSM), suite ampiamente utilizzato ai LNS sia per le interazioni con gli utenti sia per la gestione dell'inventario delle risorse informatiche [4]. Il security incident in questione viene comunicato attraverso un ticket dove il responsabile dell'host viene incluso come partecipante. L'aggiunta del campo "Host connected" consente di associare le vulnerabilità rilevate e di avere una history delle attività svolte su di esso. Segue una fase di follow-up, tracciata via ticket, durante la quale si collabora con il responsabile dell'host per attuare le misure correttive necessarie per la mitigation o remediation delle vulnerabilità riscontrate.
Per garantire una gestione completa della documentazione a supporto dell'attività viene utilizzato Alfresco come repository per tenere traccia di tutti i report generati e delle azioni intraprese per ogni host. In sintesi, questo approccio fornisce una metodologia completa per la gestione del flusso di lavoro successivo a ciascuna scansione di sicurezza. L'integrazione di Ntop, Greenbone Vulnerability Manager, Jiira ed Alfresco consente un'identificazione, una gestione e una documentazione efficienti delle vulnerabilità, valutandone i progressi nel tempo e migliorando complessivamente la sicurezza della rete nel lungo termine.
[1]GitHub di fping: https://github.com/schweikert/fping
[2]https://greenbone.github.io/docs/latest/
[3]https://nmap.org/book/nse.html
[4]https://agenda.infn.it/event/30202/contributions/168469/

Primary authors: SCLAFANI, Matteo (Istituto Nazionale di Fisica Nucleare); GIORGIO, Emidio Maria (Istituto Nazionale di Fisica Nucleare); ZITO, Daniele (Istituto Nazionale di Fisica Nucleare)

Co-authors: CANNIZZARO, Stefano (Istituto Nazionale di Fisica Nucleare); OLIVA, Alessandro Alberto (INFN-LNS)

Presenter: SCLAFANI, Matteo (Istituto Nazionale di Fisica Nucleare)

Session Classification: Sessione ”Servizi ICT”

Track Classification: Servizi ICT