Istituto Nazionale di Fisica Nucleare
COMMISSIONE DI CALCOLO E RETI

Greenbone ed nmap

Leandro Lanzi

Tutorial days di CCR: Cybersicurezza

Laboratori Nazionali di Frascati, 10-12 ottobre 2022

Introduzione

- Questo intervento si propone di mostrare l'uso di Greenbone ed nmap come strumenti di *Hardening* dei propri sistemi informatici.
- Saranno trattati i seguenti argomenti.

  - **Greenbone Community Edition (GCE)**
    - Breve descrizione del framework GCE.
    - Tutorial
      - Installazione di GCE tramite *docker-compose* su INFN-Cloud.
      - Configurazione dell'interfaccia web di GCE sulla porta 443 (https).
      - Gestione di GCE: accensione e spegnimento dei container, aggiornamento dei feed.
      - Configurazione delle scansioni dall'intefaccia web.
      - Uso della Command Line Inteface (CLI) di GCE.
        - Configurazioni delle scansioni.
        - Salvataggio delle impostazioni.
        - Esportazione dei report.

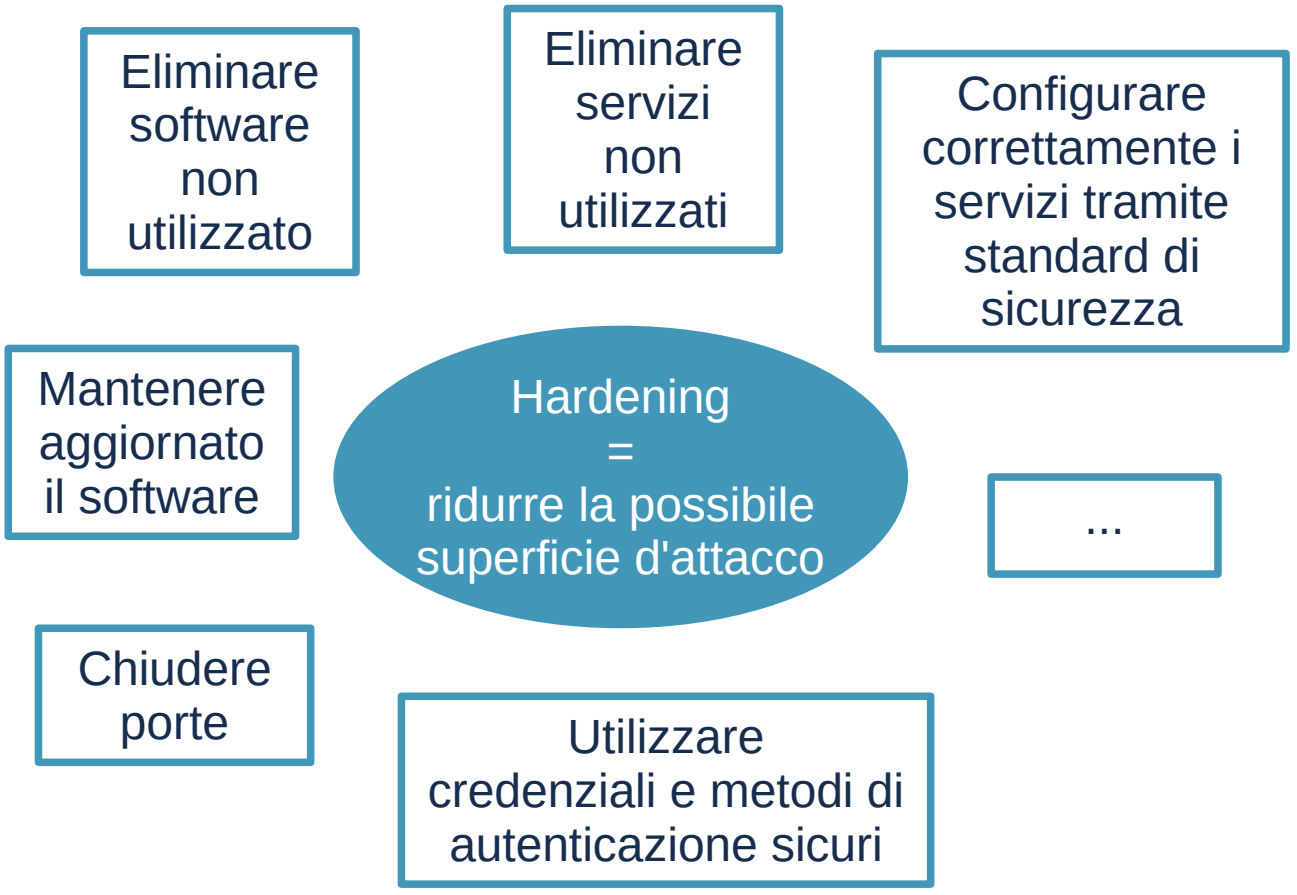
  - **nmap**
    - definizione dei target
    - opzioni di nmap
    - formati dell'output
    - host discovery
    - port scanning
    - service and application version detection
    - OS detection
    - nmap scripting engine (NSE)

Hardening

- "*Hardening* indica l'insieme di operazioni specifiche di configurazione di un dato sistema informatico che mirano a minimizzare l'impatto di possibili attacchi informatici che sfruttano vulnerabilità dello stesso, migliorandone pertanto la sicurezza complessiva" [1].
- Nel realizzare procedure atte a "rafforzare" e proteggere i sistemi informatici che permettano di identificare le minacce e di implementare misure adeguate per minimizzare la possibile superficie d'attacco prima che risorse e dati vengano compromessi si distinguono varie metodologie.
  - *One Time Hardening*: viene effettuato solo una volta dopo la prima realizzazione del sistema.
  - *Multiple Time hardening*: viene effettuato più volte durante la vita del sistema, e la sua ripetizione nel tempo dipende da due fattori fondamentali che sono:
    - il rilascio di patch di aggiornamento,
    - la modifica alla configurazione (sia hardware che software).
  - *Continous Vulnerability Assessment*: la verifica periodica e strutturata del sistema.

[1] Wikipedia, definizione di Hardening

GCE ed nmap come strumenti di hardening



Scansioni con nmap e GCE permettono:

- di rilevare la presenza di device e servizi sulla rete configurati dagli utenti e di conoscerne eventuali vulnerabilità,
- verificare se i prori sistemi e servizi sono configurati come previsto.

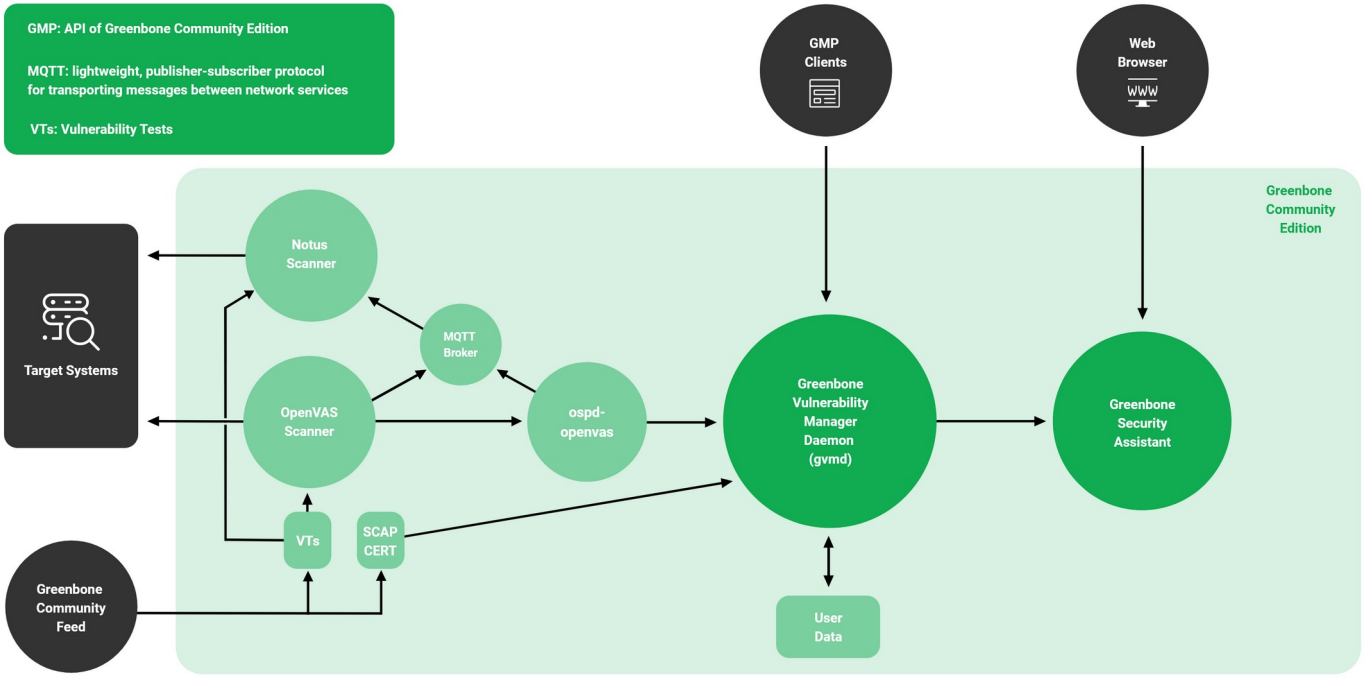
Greenbone Community Edition (GCE) [1/2]

- Greenbone Community Edition è il nuovo nome utilizzato da Greenbone per identificare la versione “community” dei prodotti commerciali Greenbone Enterprise per le scansioni di vulnerabilità.
- Fino al 2021 veniva utilizzato il termine Greenbone Vulnerability Management (GVM).
- Questo nuovo nome è stato introdotto quando è stata resa disponibile la versione sotto forma di docker container del software.
- Inizialmente il framework di scansioni di Greenbone è stato sviluppato con il nome di OpenVAS e prima ancora col nome GNessUs, come fork del software Nessus dopo che i suoi sviluppatori (Tenable Network Security) avevano trasformato in software proprietario il codice iniziale open source nell’ottobre del 2005.
- Quando il progetto OpenVAS è stato lanciato, consisteva solo in un motore per la scansione delle vulnerabilità.
- Poco dopo è stata fondata Greenbone Networks col fine di sviluppare e offrire supporto professionale al prodotto. Greenbone Networks ha iniziato a guidare lo sviluppo di OpenVAS, ha aggiunto diversi componenti e lo ha trasformato in un software completo e articolato di gestione delle vulnerabilità mantenendo i valori del software libero.
- Dopo il rilascio della versione 9 di OpenVAS, il progetto open source è stato rinominato Greenbone Vulnerability Management (GVM). A partire da GVM 10, il termine OpenVAS viene utilizzato solo per la componente scanner come era all’inizio del progetto.
- GVM veniva rilasciato sotto forma di sorgenti open source completamente liberi col nome di Greenbone Source Edition (GSE) e attualmente, sia come sorgenti che come docke container, con il nome di Greenbone Community Edition (GCE).
- Parallelamente a GCE viene mantenuta una versione Enterprise, Greenbone Professional Edition (GPE), e una versione Cloud, Greenbone Cloud Services (GCS), entrambe con licenze a pagamento.

Greenbone Community Edition (GCE) [2/2]

GCE è formato di tre parti principali:

- due applicazione di scansione (OpenVAS e Notus Scanner) che eseguono i test di vulnerabilità (VT, vulnerability tests o NVT, network vulnerability tests),
- il demone Greenbone Vulnerability Manager Daemone (gvmd),
- l'applicazione Greenbone Security Assistant (GSA) con il demone Greenbone Security Assistant Daemon (gsad).



nmap

- Nmap è uno scanner di rete creato da Gordon Lyon nel 1997 (25 anni fa), rilasciato con licenza GPL e tuttora mantenuto costanemente aggiornato; l'ultima versione stabile è del primo settembre 2022 (circa un mese fa).
- Nmap viene comunemente utilizzato per:
  - host discovery,
  - audit dei servizi di rete,
  - troubleshoot dei servizi di rete.

Tutorial

- **Si consiglia l'installazione di GGE e di nmap su una macchina situata nella rete della propria Sede per compiere scansioni interne e su una macchina su INFN-Cloud per compiere scansioni dall'esterno della propria rete.**
- Link ai tutorial Greenbone:
  - macchia virtuale su INFN-Cloud
  - installazione e configurazione
  - interfaccia web
  - Command Line Inteface (CLI)
- Link al tutorial nmap.

Link e riferimenti

- Greenbone Community Edition Documentation:
  - https://greenbone.github.io/docs/latest/index.html
- INFN-Cloud
  - https://www.cloud.infn.it
- Greenbone Networks GmbH su dockerhub (Docker Verified Publisher)
  - https://hub.docker.com/u/greenbone
- Greenbone Community Portal
  - https://community.greenbone.net/
- Glossario dei termini usati in GCE
  - https://greenbone.github.io/docs/latest/glossary.html
- XML Scripting
  - https://greenbone.github.io/gvm-tools/scripting.html
- API Documentation for GCE 22.04 (riferimento per tutti i comandi utilizzabili nella CLI)
  - https://docs.greenbone.net/API/GMP/gmp-22.04.html
- Installazione, configurazione e manutenzione di un server per scansioni di vulnerabilità non invasive (Nota di CCR, INFN-58/2021/P, 6 dicembre 2021)
  - https://www.lnf.infn.it/sis/preprint/pdf/getfile.php?filename=INFN-22-02-CCR.pdf
- Nmap
  - https://nmap.org
- The Official Nmap Project Guide to Network Discovery and Security Scanning
  - https://nmap.org/book/toc.html