La sicurezza nell'INFN

Stefano Zotti
INFN-CNAF - Software Development (SD)
21/3/2024

Argomenti

1. Cos’è la sicurezza
2. Come ci difendiamo al CNAF
    - monitoraggio
    - prevenzione
    - collaborazione
3. Sicurezza all’interno di INFN

Sicurezza in breve

- Permettere che chi è autorizzato faccia ciò per cui è autorizzato
- Non permettere a chi non è autorizzato di fare ció per cui non è autorizzato

Tutto qui? Sembra facile vero?
Se non fosse per un piccolo dettaglio:

l’attaccante

La sicurezza è un gioco che si fa in due parti

Il difensore protegge un sistema dalle intrusioni

Un attaccante che cerca di entrare

La sicurezza è un gioco che si fa in due parti

1. Il difensore deve essere sempre perfetto
2. Il difensore ha una vita (ed orari di lavoro!)
3. Il difensore deve difendere TUTTO

1. All'attaccante basta essere fortunato una volta
2. L'attaccante ha tutto il tempo del mondo
3. l'attaccante può concentrarsi su un unico host

Dato tempo sufficiente, l’attaccante vincerà sempre

Ma non si può mettere in sicurezza un sistema?

- Non in assoluto, a meno di non fare a pezzettini il computer e tutte le sue memorie

Ma se lo stacco dalla rete?

- Un buon cannocchiale risolve il problema.

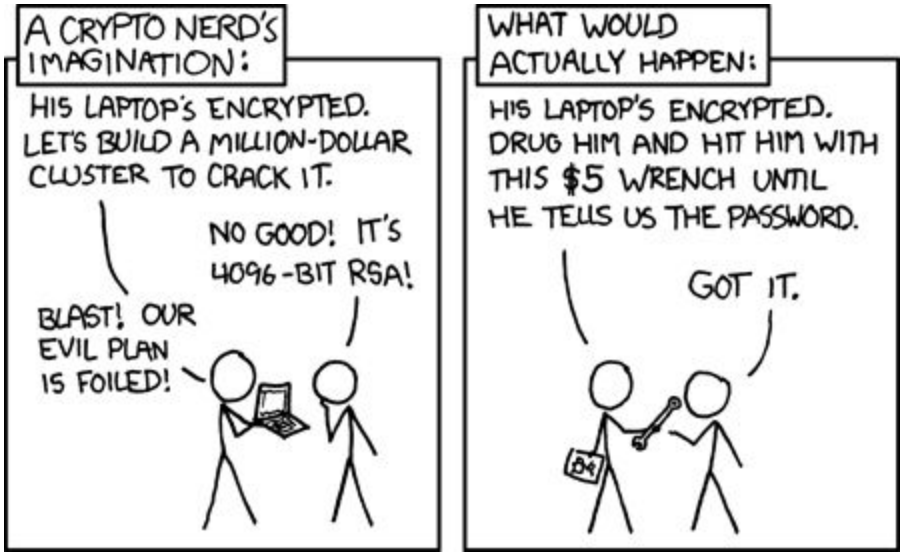
Ma se lo uso solo in una stanza chiusa senza finestre?

- Si può capire cosa viene visualizzato sullo schermo (o digitato sulla tastiera) analizzando il rumore dei tasti o le micro vibrazioni dello schermo (o del tavolo o radio)

Se non porto altri sistemi elettronici nelle vicinanze?

- Si corrompe l'operatore!

[1] Keyboard Acoustic Emanations Revisited
[2] Sniffing Keystrokes With Lasers/Voltmeters
[3] Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel



https://xkcd.com/538

- Se un attaccante vince inevitabilmente cosa si può fare?
  - “Inevitabilmente” non vuol dire “al primo tentativo”
  - Rallentare l’attaccante fino a quando non importa più se penetra nella macchina perché non c’è più nulla di prezioso lì dentro (o non esiste più)

- Come si può rallentare un attaccante?
  - Monitoring
  - Mantenendo il segreto
  - Prevenzione
  - Collaborazione

Cosa si intende con “mantenere il segreto”?

Security Through Obscurity is an illusion

- La SOLA segretezza delle informazioni rallenta un attacco ma non ci permette di dormire sonni tranquilli.
  L’obiettivo è rallentare l’attaccante o portarlo a commettere errori:
  - colpire il sistema sbagliato o quello più controllato
  - finire in un vicolo cieco
- Ogni operazione dell’attaccante può portarlo verso la sua scoperta

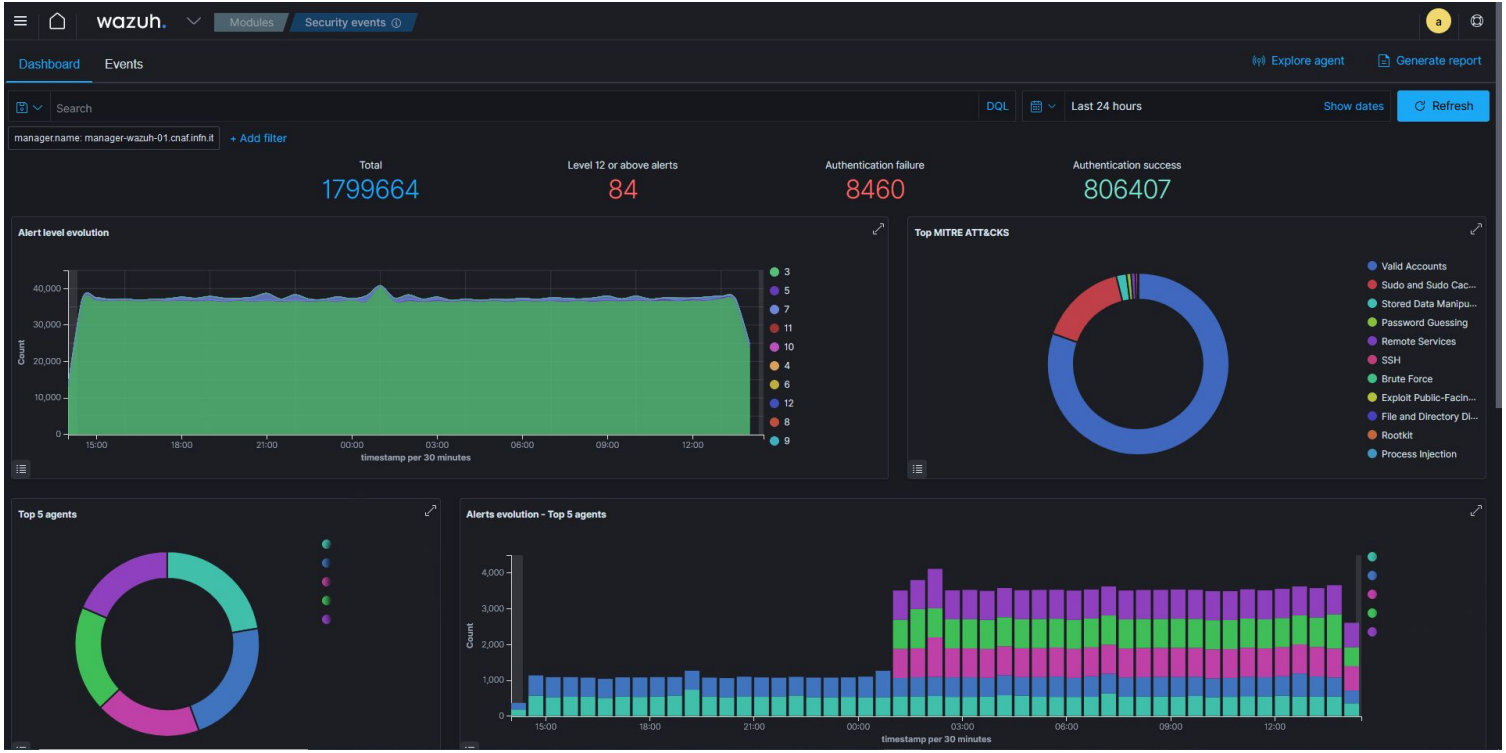
[4] Developing Cyber-Resilient Systems; A Systems Security Engineering Approach

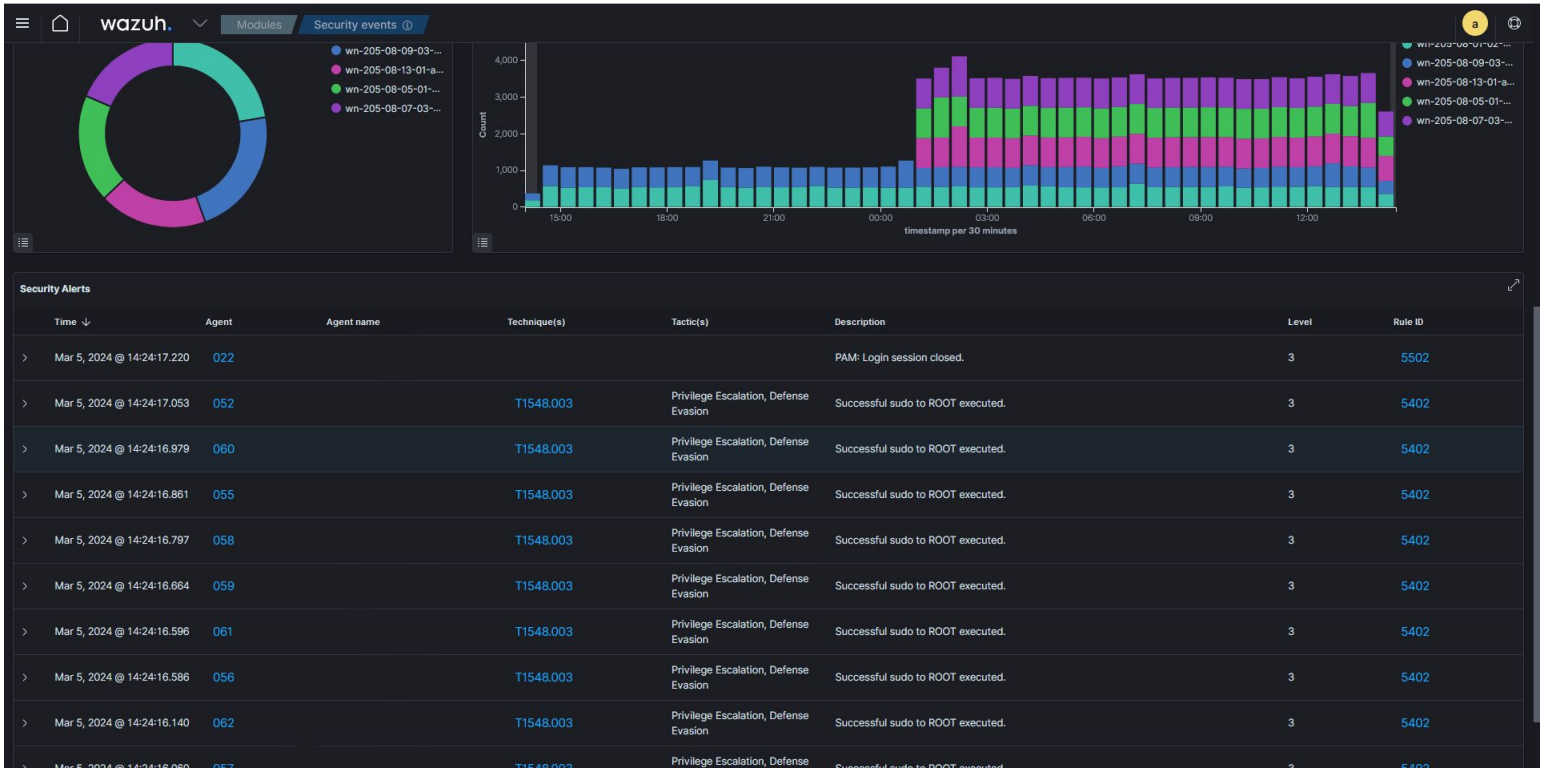
Come opera il CNAF?

Monitoraggio

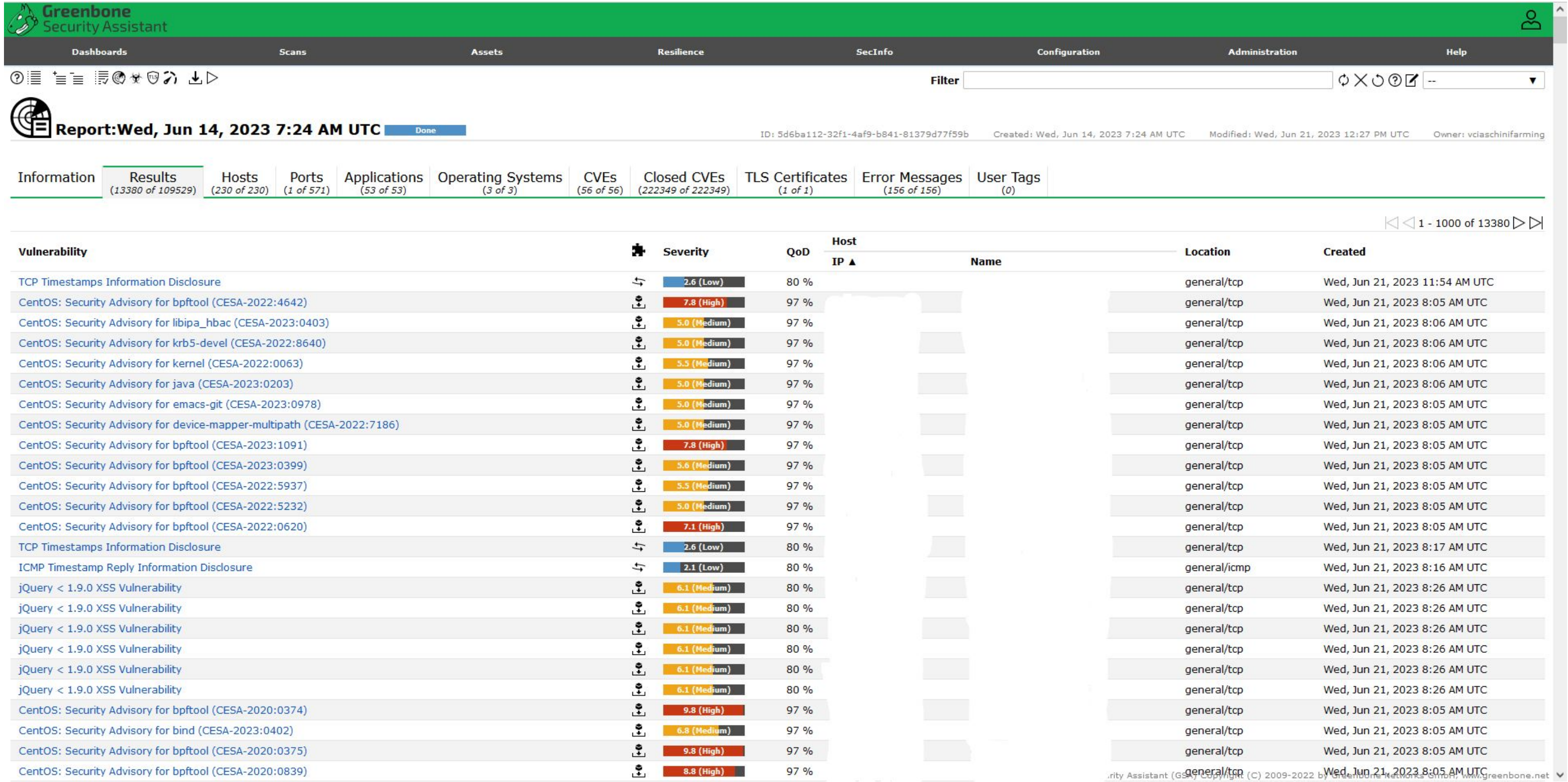
- Attività in continuo progresso, in questo momento si sta mettendo tutto il CNAF sotto il monitoraggio della piattaforma Wazuh
- Piattaforma open-source di monitoraggio e analisi dei log con focus sulla sicurezza informatica

Wazuh dashboard




wazuh.
Modules
Security events
wn-205-08-09-03-...
wn-205-08-13-01-a...
wn-205-08-05-01-...
wn-205-08-07-03-...
Count
4,000
3,000
2,000
1,000
0
15:00
18:00
21:00
00:00
03:00
06:00
09:00
12:00
timestamp per 30 minutes
Security Alerts
Time
Agent
Agent name
Technique(s)
Tactic(s)
Description
Level
Rule ID
Mar 5, 2024 @ 14:24:17.220 022 PAM: Login session closed. 3 5502
Mar 5, 2024 @ 14:24:17.053 052 T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402
Mar 5, 2024 @ 14:24:16.979 060 T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402
Mar 5, 2024 @ 14:24:16.861 055 T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402
Mar 5, 2024 @ 14:24:16.797 058 T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402
Mar 5, 2024 @ 14:24:16.664 059 T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402
Mar 5, 2024 @ 14:24:16.596 061 T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402
Mar 5, 2024 @ 14:24:16.586 056 T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402
Mar 5, 2024 @ 14:24:16.140 062 T1548.003 Privilege Escalation, Defense Evasion Successful sudo to ROOT executed. 3 5402

Prevenzione con Greenbone



Greenbone è un'applicazione open-source per la scansione e gestione delle vulnerabilità

Prevenzione

1. Assessment del software
   Analisi del software alla ricerca di vulnerabilità e chiusura delle falle prima che un attaccante la scopra

2. Analisi prove
   Nel caso l'attaccante sia arrivato prima di noi, la ricerca e lo studio delle tracce lasciate ci aiuta a capire e a migliorare.
   Le domande a cui è importante rispondere sono:

   - come e quando è entrato
   - se e cosa è riuscito a fare

   Per comprendere al meglio bisogna per prima cosa analizzare i file di LOG e gli eseguibili usati dall'attaccante con tecniche di disassembly e decompilazione

3. Formazione degli utenti
   La formazione e la consapevolezza da parte degli utenti è un fattore determinante per la sicurezza

INFN

Collaborazione

Il CNAF è membro/partner attivo del progetto internazionale Worldwide LHC Computing Grid **WLCG** (source https://wlcg.web.cern.ch) che prevede la collaborazione tra data center dedicati alla fisica delle alte energie. Tra gli obiettivi del progetto è presente anche la condivisione di informazioni di sicurezza:

- da dove è stato lanciato l'attacco
- chi ha lanciato l'attacco
- chi è il bersaglio dell'attacco

Computer Security Incident Response Team (CSIRT)

All’interno di INFN è presente un un gruppo CSIRT, il cui scopo è quello di fornire informazioni e assistenza ai propri utenti (sezioni e laboratori di INFN) nell’attuare misure proattive volte a ridurre i rischi di incidenti di sicurezza informatica e nella risposta in caso questi eventi si verifichino.

Il CNAF è fortemente coinvolto all’interno di questo gruppo con 3 membri su 7

Security Operation Center (SOC)

Gruppo responsabile del piano operativo in caso di incidenti di sicurezza.
Attività di cui si occupa il SOC:

- Monitora un subset delle macchine esposte all'interno della rete INFN
- Automatizza il processo di analisi degli eventi
- Centralizza le risposte

Esempi di attacchi noti

1. Keyboard acoustic emanations revisited
2. Sniffing Keystrokes With Lasers/Voltmeters
3. Screen Gleaning: A Screen Reading TEMPEST Attack on Mobile Devices Exploiting an Electromagnetic Side Channel

Link utile

Developing Cyber-Resilient Systems; A Systems Security Engineering Approach