Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA | PNC Piano nazionale per gli investimenti complementari al PNRR Ministero dell'Università e della Ricerca | DARE DIGITAL LIFELONG PREVENTION

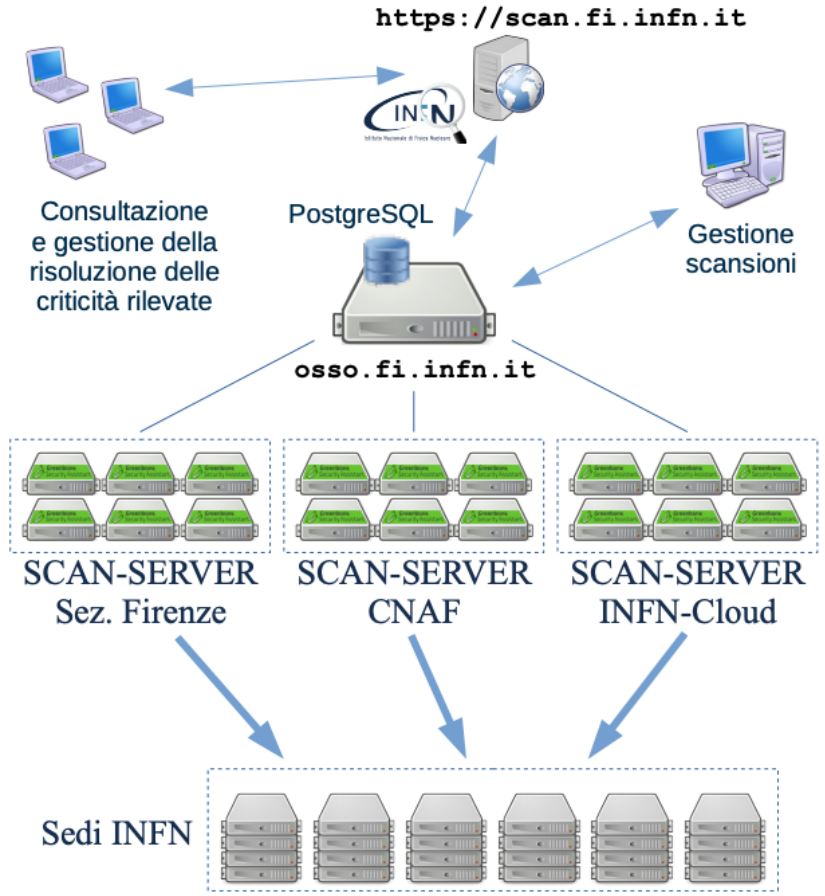
Analisi comparativa e prospettive evolutive degli strumenti di vulnerability assessment adottati dal NUCS dell'INFN

Workshop sul Calcolo nell'INFN – Biodola 2025

Cristian Greco - INFN Roma2
Matteo Sclafani - INFN Laboratori Nazionali del Sud
Stefano Enrico Zotti - INFN CNAF

INFN Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity – NUCS

Cos'è e come funziona il gruppo NUCS



Il gruppo **Scansioni** del NUCS (NUcleo CyberSecurity INFN) si occupa delle scansioni di vulnerabilità sia per le **Sedi INFN** che per la **INFN-CLOUD**.

- Il **NUCS** dispone di **18 SCAN-SERVER** (6 al CNAF, 6 su INFN-Cloud e 6 alla Sezione di Firenze) per compiere scansioni su tutta la rete INFN tramite:
  - **zmap** per la rilevazione di host esposti e relativi servizi attivi (solo TCP);
  - **rustscan** per la rilevazione di host esposti e relativi servizi attivi (solo TCP);
  - **nmap** per la rilevazione e caratterizzazione di host esposti e relativi servizi attivi;
  - **ssh-audit** per la verifica dei server SSH;
  - **testssl.sh** per la verifica dei protocolli di cifratura TLS/SSL;
  - **Greenbone Community Edition (GCE)** per la rilevazione di vulnerabilità di sicurezza sugli host esposti.
- Ulteriore scanserver con **Greenbone Enterprise (DECA).**
- Il nodo **osso.fi.infn.it** gestisce ogni aspetto delle scansioni (configurazione, invio agli SCAN-SERVER, monitoraggio, download ed importazione nel database dei risultati) in modo semiautomatico ed ospita il database.
- Nel nodo **scan.fi.infn.it** è presente l'interfaccia web per la consultazione, gestione e risoluzione delle criticità rilevate.
- Da fine dicembre del 2024 è in produzione **Qualys Vulnerability Management Detection & Response (VMDR)**

Lavoro di analisi di 4 piattaforme

Nell'ambito dell'attività del gruppo Scansioni del NUCS (NUcleo CyberSecurity INFN) è stato scelto, al fine di trovare lo strumento più efficiente per l'attività di scansione, di mettere a confronto le scansioni di vulnerabilità effettuate con:

- Greenbone Enterprise Appliance 22.04.27
- Greenbone Security Assistant 24.6.1
- Tenable Nessus Essentials 10.8.4
- Qualys Enterprise TruRisk Platform 3.20.1.0-7

Informazioni sulle 4 piattaforme

	Greenbone Enterprise DECA	Greenbone Community EDITION	tenable Nessus Essentials	Qualys
Appliance	Appliance virtuale al CNAF	Appliance virtuale su INFN-Cloud	Appliance virtuale a Roma2	SaaS Cloud + N°1 Sonda interna installata a Roma2
Licenza	Commerciale	Free (open source)	Free (limitata a 16 IP)	Commerciale

Target di scansione

Nell'ambito dell'analisi comparativa, è stato definito un target uniforme per valutare le funzionalità e l'efficacia delle piattaforme testate:

Host oggetto di scansione

- **15 host** reali selezionati all'interno della rete INFN, in produzione, rappresentativi di una varietà di sistemi operativi, servizi e configurazioni effettivamente in uso.
- **1 host** vulnerabile in ambiente isolato, basato su immagine Metasploit con vulnerabilità note, utilizzato come benchmark di riferimento per confrontare la capacità di rilevamento dei tool.

Configurazione delle scansioni

- **Profilo di scansione**: è stato utilizzato il profilo predefinito di ciascuna piattaforma, senza modifiche ai parametri o ai plugin attivi, al fine di valutare il comportamento "out-of-the-box".
- **Stato host**: tutti gli host sono stati considerati "alive" a priori, evitando false esclusioni legate alla fase di host discovery.
- **Tipologie di scansione:**
  - **TCP**: tutte le **65535** porte analizzate
  - **UDP**: **100 porte** più comuni secondo classificazione Nmap
  - **Autenticate / Non Autenticate**: entrambe le modalità sono state testate
- **ACL di rete**: configurazioni ad hoc sui **router di frontiera** per **abilitare il traffico di scansione** proveniente dagli IP delle piattaforme verso gli host target

Confronto tra piattaforme

Approccio

Trovare un metodo o uno strumento che possa confrontare le piattaforme di scansione e che ci permetta di avere un benchmark con alcune caratteristiche:

- Simulazione di casi reali
- Nessun pericolo per la rete INFN
- Configurabile e riutilizzabile per ulteriori prove

Soluzione

Metasploit

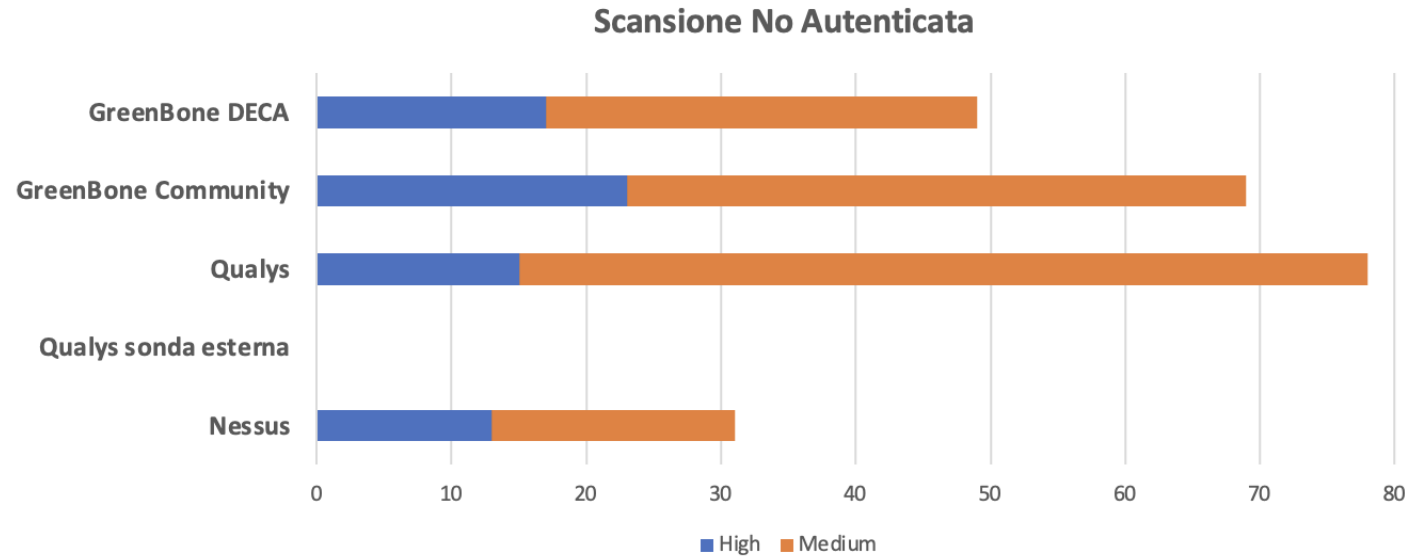
- Vulnerabilità note e documentate
- VM isolata dalla rete esterna e sotto controllo
- File OVA replicabile in ambiente controllato

Configurazione di una VM con Metasploit per Scansioni di Vulnerabilità

Strumento essenziale per fare testing di sicurezza su un ambiente con vulnerabilità note ma che non contiene dati, nel nostro caso si è usata la versione 2 basata su Ubuntu 8.04 (EOL) con diversi servizi attivi come:

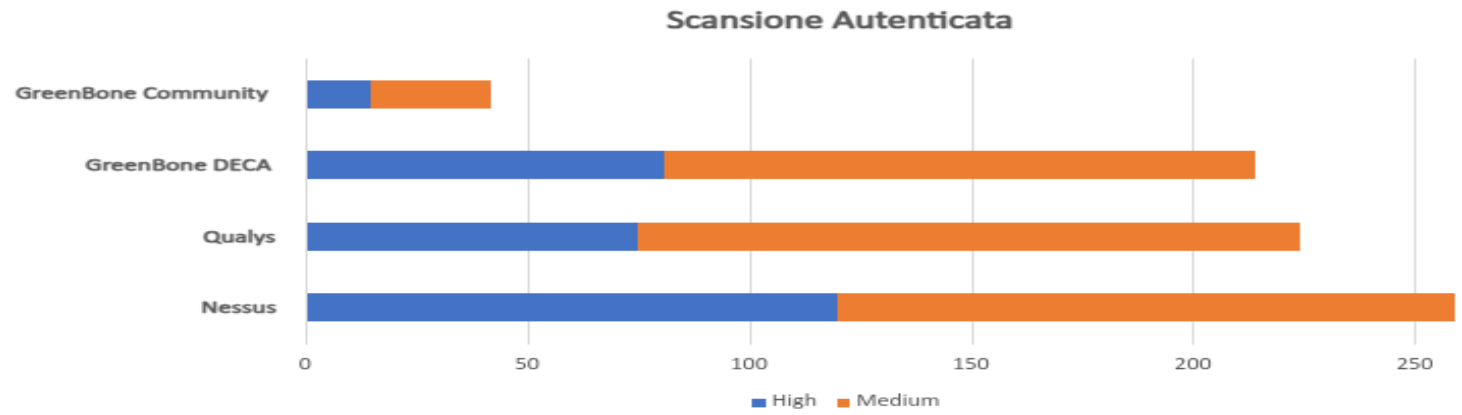
- MySQL sulla porta 3306
- Postgresql porta 5432
- FTP sulla porta 2121
- samba, ecc...

Benchmark scansione non autenticata su Metalsploitable



Piattaforma	High	Medium	Low	Total
GreenBone DECA	17	32	4	53
GreenBone Community	23	46	6	75
Qualys	15	63	157	235
Qualys sonda esterna	0	0	11	11
Nessus	13	18	7	38

Benchmark scansione autenticata su Metalsploitable



Piattaforma	High	Medium	Low	Total
GreenBone Community	15	27	5	47
GreenBone DECA	81	133	13	227
Qualys	75	149	162	386
Nessus	120	139	17	276

Scansione esterna

La scansione di **15 Host** è un processo fondamentale per valutare la sicurezza e la vulnerabilità di una rete. Una scansione esterna, in particolare, viene **eseguita dall'esterno del perimetro di rete**, simulando l'approccio di un potenziale attaccante. Durante tale processo, il firewall gioca un ruolo cruciale, bloccando la maggior parte dei tentativi di accesso non autorizzati e permettendo solo le connessioni agli endpoint pubblici designati.

Piattaforma	Durata	Tot. Vulnerabilità	High	Medium
Qualys VMDR con Sonda esterna	1:18:00	104	47	57
Greenbone Enterprise Appliance 22.04.27	1:50:00	32	2	30
Greenbone Security Assistant 24.6.1	0:55:00	1	1	0
Nessus Essentias 10.8.4	0:27:00	90	9	81

Scansione interna non autenticata

Una scansione interna non autenticata è un tipo di scansione in cui si valuta la rete dall'interno, senza utilizzare credenziali di accesso, per identificare vulnerabilità e punti di ingresso potenziali per attacchi. Questo approccio simula il comportamento di un aggressore interno o di un malware che ha già bypassato le difese perimetrali.

Piattaforma	Durata	Tot. Vulnerabilità	High	Medium
Qualys VMDR con Scanner Interno	2:56:00	92	47	45
Greenbone Enterprise Appliance 22.04.27	3:39:00	103	30	73
Greenbone Security Assistant 24.6.1	1:45:00	115	26	89
Nessus Essentias 10.8.4	0:27:00	99	10	89

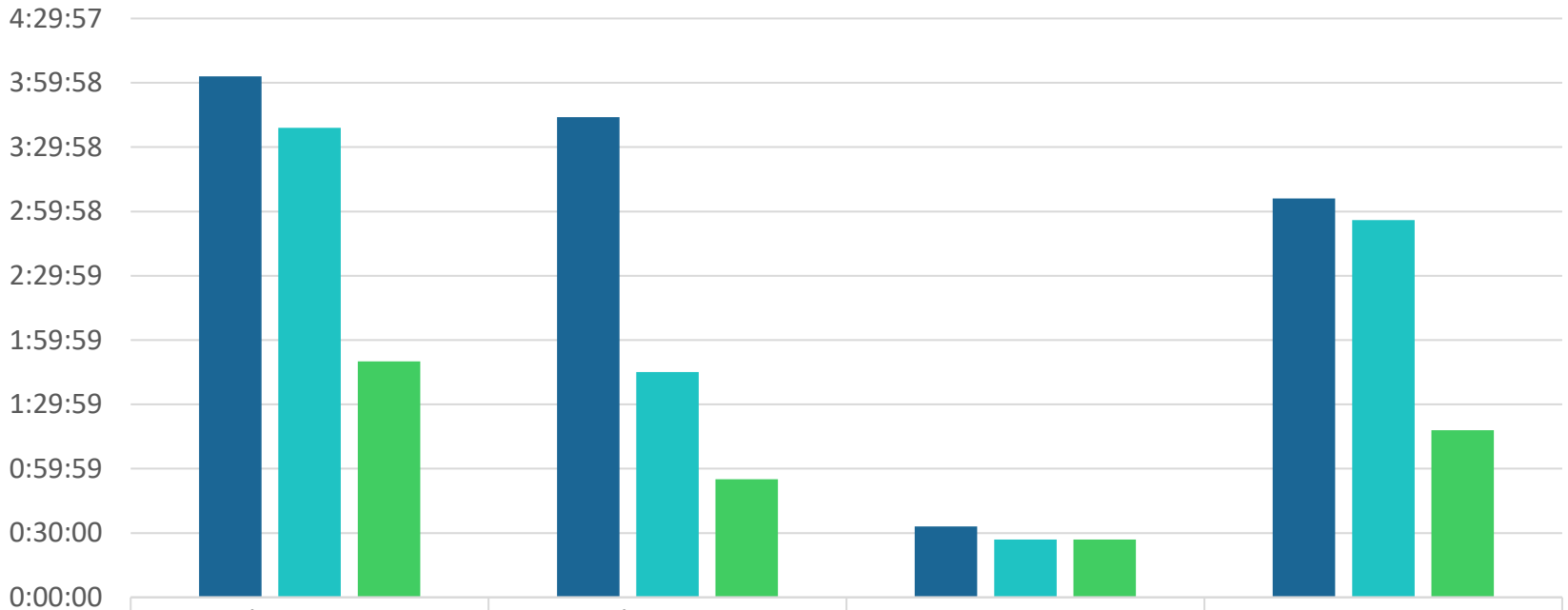
Scansione interna autenticata

Una scansione interna autenticata viene eseguita con **credenziali valide**, permettendo un'analisi approfondita delle risorse di rete. Questo tipo di scansione offre una visione dettagliata delle potenziali minacce, consentendo di valutare la sicurezza da una prospettiva privilegiata e di identificare punti deboli che potrebbero essere sfruttati da utenti malintenzionati con accesso alla rete.

Piattaforma	Durata	Tot. Vulnerabilità	High	Medium
Qualys VMDR con Sonda interna	3:06:00	2115	1359	756
Greenbone Enterprise Appliance 22.04.27	4:03:00	1049	585	464
Greenbone Security Assistant 24.6.1	3:44:00	573	258	315
Nessus Essentias 10.8.4	0:33:00	1093	648	445

Confronto delle Durate di Scansione

La tabella e il grafico mostrano la durata delle scansioni di vulnerabilità effettuate su un totale di **15 Host**



	Greenbone Enterprise Appliance 22.04.27	Greenbone Security Assistant 24.6.1	Nessus Essentias 10.8.4	Qualys VMDR
Scansione Autenticata	04:03:00	03:44:00	00:33:00	03:06:00
Scansione Non Autenticata	03:39:00	01:45:00	00:27:00	02:56:00
Scansione No ACL	01:50:00	00:55:00	00:27:00	01:18:00

Analisi vulnerabilità

Questa slide presenta i risultati di una **scansione autenticata** eseguita su un singolo host.

Il confronto evidenzia il numero totale di vulnerabilità rilevate da ciascun tool.

Piattaforma	Durata	Tot. Vulnerabilità	High	Medium	Low
Qualys VMDR con Sonda interna	3:05:00	40	19	10	11
Greenbone Enterprise Appliance 22.04.27	1:40:00	30	8	19	3
Greenbone Security Assistant 24.6.1	1:30:00	33	8	22	3
Nessus Essentias 10.8.4	0:18:00	10	1	9	0

Durante la scansione dell'host, che ospita anche un sito **WordPress**, è emersa una differenza significativa.

Piattaforma	Vulnerabilità WordPress
Qualys VMDR	✅
Greenbone Enterprise Appliance 22.04.27	✅
Greenbone Security Assistant 24.6.1	✅
Nessus Essentias 10.8.4	❌

Nonostante **Nessus Essentials** abbia a disposizione i plugin Wordpress già scaricati e disponibili, nelle impostazioni di default di scansione i **plugin specifici per WordPress** risultano **disattivati**

Analisi vulnerabilità

Qualys è l'unico tools che ha rilevato nel plugin **Ultimate Member** per **WordPress** la vulnerabilità «**WordPress Plugin Ultimate Member Unauthenticated SQL Injection Vulnerability**» identificata come **CVE-2024-1071**

Questa vulnerabilità, pubblicata il 13/03/2024 consente ad utenti non autenticati di aggiungere query SQL aggiuntive a query già esistenti, che possono essere utilizzate per estrarre informazioni sensibili dal database.

Score	Severity	Version	Vector String
9.8	CRITICAL	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Fonte: cve.org

5 WordPress Plugin Ultimate Member Unauthenticated SQL Injection Vulnerability — port 443/tcp

QID:	731205		
Category:	CGI	**CVSS Base:**	7.5[1]
Associated CVEs:	CVE-2024-1071	**CVSS Temporal:**	5.9
Vendor Reference	Ultimate Member Plugin Release Notes	**CVSS3.1 Base:**	9.8
Bugtraq ID:	-	**CVSS3.1 Temporal:**	8.8
Service Modified:	11/25/2024		
User Modified:	-		
Edited:	No		
PCI Vuln:	Yes		

Fonte: Report Qualys – scansione 16/05/2025

Analisi vulnerabilità

Altre Vulnerabilità WordPress rilevate solo da Qualys:

#	CVE	Titolo vulnerabilità	Componente	CVSS v3.1
1	CVE-2024-31210	WordPress Core Multiple Vulnerabilities	WordPress Core	7.6
2	CVE-2024-31211	WordPress Core Security Updates – Arbitrary Option Update	WordPress Core	6.4
3	CVE-2024-6307	WordPress Core < 6.5.5 – Multiple Vulnerabilities	WordPress Core	6.4

Dettagli tecnici (esempi)

- **CVE-2024-31210**: vulnerabilità multiple nel core WordPress risolte nella versione 6.4.3.
- **CVE-2024-31211**: vulnerabilità che permetteva modifiche non autorizzate ad opzioni tramite script.
- **CVE-2024-6307**: ultima serie di vulnerabilità prima della 6.5.5, collegate a gestione permessi e informazioni.

Conclusione

Piattaforma	✅ Pro	❌ Contro
Greenbone Enterprise Appliance	✅ Ampia copertura delle vulnerabilità, grazie al Greenbone Enterprise Feed ✅ Gestione centralizzata ✅ Reportistica dettagliata in più formati	❌ Versione Deca limita a 2 sonde ❌ Nessun rilevamento su vulnerabilità del Core ❌ Gestione locale
Qualys Enterprise TruRisk Platform	✅ Aggregazione da oltre 25 feed di threat intelligence ✅ Copertura completa e continua tramite agenti e sonde ✅ Nessun limite di sonde installabili ✅ Integrazione con Jira ✅ Prioritizzazione basata su rischio reale (TruRisk) ✅ Integrazione con AAI INFN	❌ Interfaccia complessa ❌ Scansioni interne più lente rispetto a sonde cloud ❌ Limite attuale: 3000 IP
Greenbone Security Assistant	✅ Interfaccia intuitiva ✅ Report completi (PDF, CSV, XML) ✅ Buona documentazione anche se free	❌ 28% in meno di NVT ❌ Assenza totale di NVT per AlmaLinux/Rocky ❌ Aggiornamenti feed solo via CLI
Tenable Nessus Essentials	✅ Feed CVE aggiornato come nella versione Pro ✅ Scansioni rapide ✅ Interfaccia semplice e user-friendly ✅ VM facilmente installabile	❌ Limite 16 IP ❌ Plugin molto limitati nella configurazione standard ❌ Richiede personalizzazione delle scansioni per affidabilità

Prospettive future

- Proseguire l'analisi comparativa per individuare la piattaforma più idonea a garantire la conformità ai requisiti della direttiva **NIS2**, in un'ottica di adozione coordinata a livello nazionale.
- Approfondire il confronto tra le **due piattaforme** commerciali attualmente in uso (**Greenbone Enterprise Appliance e Qualys VMDR**), estendendo la base dei target analizzati e sfruttando i dati storici di scansione per valutazioni più complete.
- Eseguire ulteriori **scansioni mirate** su host in produzione, utilizzando profili di scansione personalizzati in funzione degli obiettivi specifici.
- Raccogliere e analizzare sistematicamente i feedback delle sezioni che stanno utilizzando **Qualys**, al fine di individuare criticità, raccogliere suggerimenti e valorizzare le potenzialità operative. In base agli esiti, confermare l'adozione definitiva della piattaforma e pianificare eventuali corsi di formazione aggiuntivi.
- **Coinvolgere attivamente** le sezioni nella mitigazione delle vulnerabilità rilevate dalle scansioni, promuovendo un approccio proattivo alla sicurezza.

Grazie a tutti i membri del gruppo NUCS

- Leandro Lanzi
- Luca Giovanni Carbone
- Vincenzo Ciaschini
- Stefano Stalio
- Alessandro Tirel
- Vincenzo Rega

Thank you

This research was co-funded by the Italian Complementary National Plan PNC-I.1 "Research initiatives for innovative technologies and pathways in the health and welfare sector" D.D. 931 of 06/06/2022, "DARE - DigitAI lifelong pRevEntion" initiative, code PNC0000002, CUP: B53C22006450001

Ministero dell'Università e della Ricerca | Italiadomani | PNC Piano nazionale per gli investimenti complementari al PNRR | DARE DIGITAL LIFELONG PREVENTION

Slide Bonus

Greenbone Enterprise Appliance - DECA

Tipo: Appliance in versione virtuale installata presso il CNAF
Licenza: Commerciale con sottoscrizione annuale
Funzionalità principali:

- **Ampia Copertura delle Vulnerabilità:** Grazie al Greenbone Enterprise Feed aggiornato automaticamente e quotidianamente, offre un'elevata capacità di rilevamento delle vulnerabilità, inclusi i zero-day.
- **Gestione Centralizzata ed Efficiente:** La piattaforma unica per la scansione, l'analisi e la gestione delle vulnerabilità semplifica il flusso di lavoro e migliora l'efficienza delle operazioni di sicurezza.
- **Reportistica Dettagliata:** I report sono molto dettagliati e disponibili in diversi formati (PDF, XML, HTML, CSV, TXT)
- **Architettura Flessibile:** supporta la scansione distribuita tramite configurazione master-sensor, la versione Deca può controllare fino a due sensori

Greenbone Security Assistant

Tipo: Appliance in versione virtuale
Licenza: Open Source - Gratuito
Funzionalità principali:

- **Interfaccia Utente Intuitiva e Moderna:** Il GSA presenta un'interfaccia web ben progettata e facile da navigare, dove l'utente può gestire le scansioni e analizzare i risultati
- **Reportistica Dettagliata:** I report sono molto dettagliati ma sono disponibili meno formati rispetto a Greenbone Enterprise Appliance (PDF, CSV, XML)
- **Integrazione Completa con il Framework GVM:** L'aggiornamento dei feed deve essere avviato manualmente e sono disposizione meno NVT rispetto a Greenbone Enterprise Appliance (circa il 28% in meno)

Qualys Enterprise TruRisk Platform

Tipo: Piattaforma in cloud
Licenza: Commerciale con sottoscrizione annuale (Limite a 3000 il numero massimo di IP scansionabili)
Funzionalità principali:

- **Visibilità unificata:** Offre una visione centralizzata di tutti gli asset IT, vulnerabilità, configurazioni e indicatori di minaccia, fornendo un contesto completo per la gestione del rischio.
- Si possono effettuare **scansioni autenticate** (**e non**) sia dalla **cloud Qualys** sia da **virtual scanner dedicati** dispiegati in rete locale.
- Possibilità di implementare un controllo continuo tramite **agent installati sui nodi** e realizzare un sistema di asset management
- **Gestione Utenti**: possibilità di impostare i permessi di un utente per limitare l'accesso al proprio asset group
- L'autenticazione è stata agganciata ad **INFN-AAI**
- La piattaforma offre strumenti avanzati per la gestione delle **Remediation**, integrati direttamente nel suo flusso di **Vulnerability Management**
- Integrazione con strumenti ITSM come ad esempio **Jira Service Management**

Tenable Nessus Essentials 10.8.4

Tipo: Appliance in versione virtuale installata presso Roma2
Licenza: Free Edition (max 16 IP)
Funzionalità principali:

- Scanner CVE con feed aggiornato come nella versione a pagamento Nessus Professional
- Supporto scansioni autenticate
- Scansioni estremamente veloci
- L'interfaccia utente è intuitiva e semplice da navigare, rendendo il processo di scansione e analisi dei risultati accessibile anche ai meno esperti