Istituto Nazionale di Fisica Nucleare
Laboratori Nazionali del Sud

UN WORKFLOW PER LA SCANSIONE E LA GESTIONE DELLE VULNERABILITÀ DI SICUREZZA

Matteo Sclafani, *E.M. Giorgio, D. Zito, S. Cannizzaro, A. A. Oliva*

WORKSHOP SUL CALCOLO NELL'INFN (PALAU, 20-24 MAGGIO 2024)

INTRODUZIONE

La gestione efficiente delle **vulnerabilità** emerse da periodiche **scansioni** è fondamentale in una rete articolata come quella dei Laboratori Nazionali del Sud.

Questo documento illustra, da una prospettiva prevalentemente **operativa**, la metodologia adottata per la gestione del flusso di lavoro post-scansione. Bisogna evidenziare come l'approccio utilizzi software che la commissione calcolo ha inserito nei servizi nazionali, quindi ampiamente utilizzato in INFN.

INTRODUZIONE

Minaccia:

- Pericolo che può compromettere la sicurezza di un sistema e causare danni

Vulnerabilità:

- Debolezza in un sistema che potrebbe essere sfruttata da un attaccante per guadagnare accessi illegittimi al sistema

Attacco:

- Realizzazione pratica di una minaccia, sfruttando generalmente una vulnerabilità

INTRODUZIONE

Assumed breach scenario

Le scansioni vengono effettuate con l'obiettivo di individuare le vulnerabilità e di effettuare conseguentemente un hardening degli host vulnerabili. Quasi tutti gli host stanno su rete interna, protetti da Firewall perimetrale. Lo scenario che si considera è quello "Assumed Breach", il che prevede che l'attaccante sia già riuscito a penetrare nella rete locale.

Vettori di attacco della categoria del Social Engineering come il **Phishing, Baiting, Man in the middle** (o casi di **Insider treat**) possono condurre all'installazione di Malware attraverso i quali, ad esempio, si possono rubare di credenziali VPN o utilizzare backdoor remote. L'hardening ha lo scopo di limitare il perimetro vulnerabile sul quale l'attaccante può agire una volta effettuato l'accesso.

SOFTWARE UTILIZZATI NEL WORKFLOW

1. Fase preparatoria

FPING ed NTOP

2. Scansioni

GVM (Ossoverde-Lanzi)

3. Documentazione

Alfresco INFN

4. Processing

LNS Sec

LNS Sec tool

5. Follow-up

Jira Service Management (Insight e Service Desk)

1.ATTIVITÀ PREPARATORIA

Rete Target

Intera rete locale 172.16.0.0/16 device Desktop, Server ed attrezzatura scientifica

Distribuzione Ip nella rete

Utilizzo di fping per scansionare host attivi e valutare la densità

Suddivisione in gruppi

Suddividerli in gruppi in base alla densità delle /24 considerate

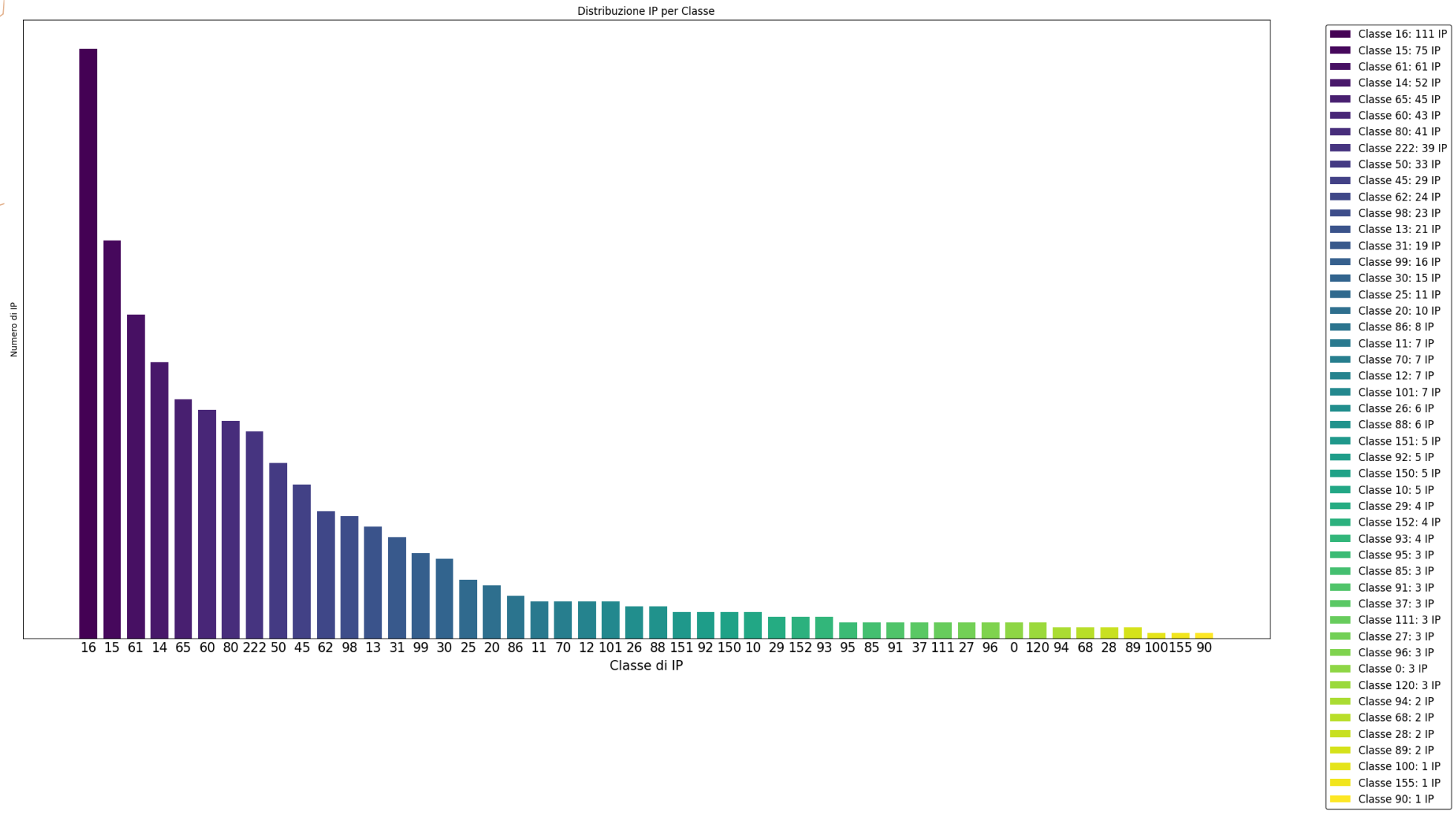
Pianificazione delle scansioni

Le scansioni vengono effettuate su porzioni di rete /24 o /23 in base alla densità di host presenti

FPING

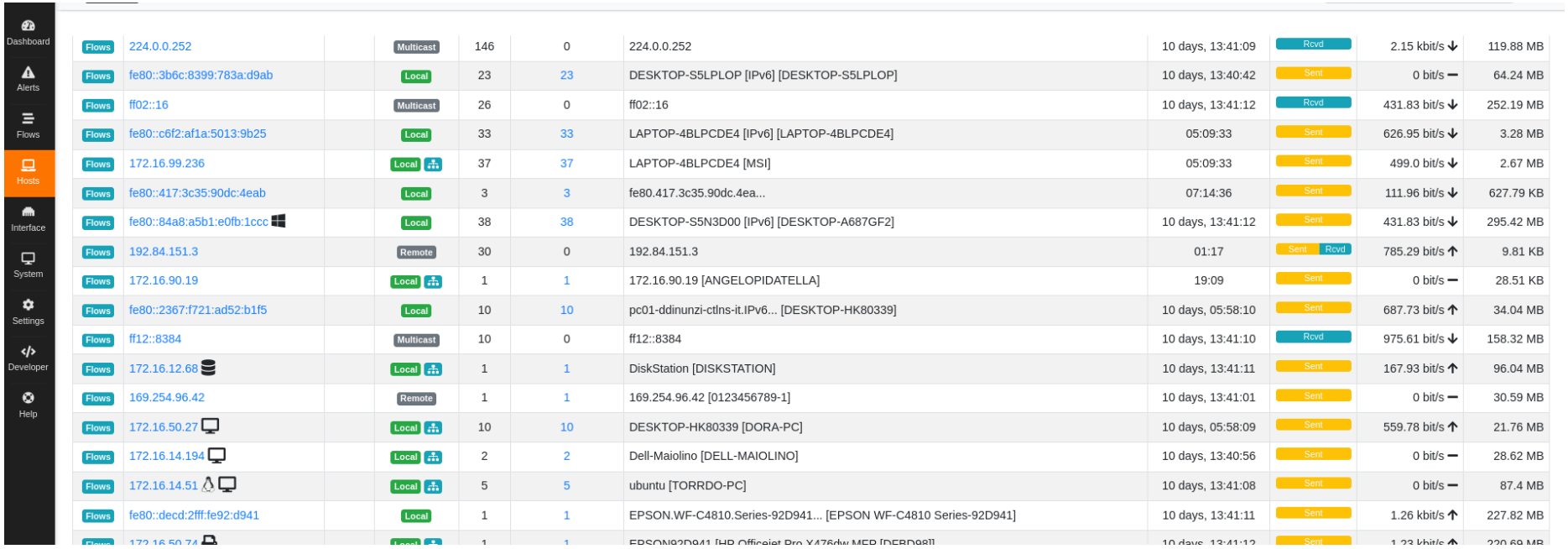
È uno strumento potente(basato su ICMP ping)e versatile utilizzato per eseguire ping in parallelo su più host contemporaneamente. A differenza del tradizionale comando ping, che esegue i ping in sequenza, consente di inviare richieste ICMP contemporaneamente a un gran numero di host, rendendo la scansione delle reti più efficiente e veloce.

ANALISI OUTPUT FPING SULL'INTERA LAN



NTOP-NG

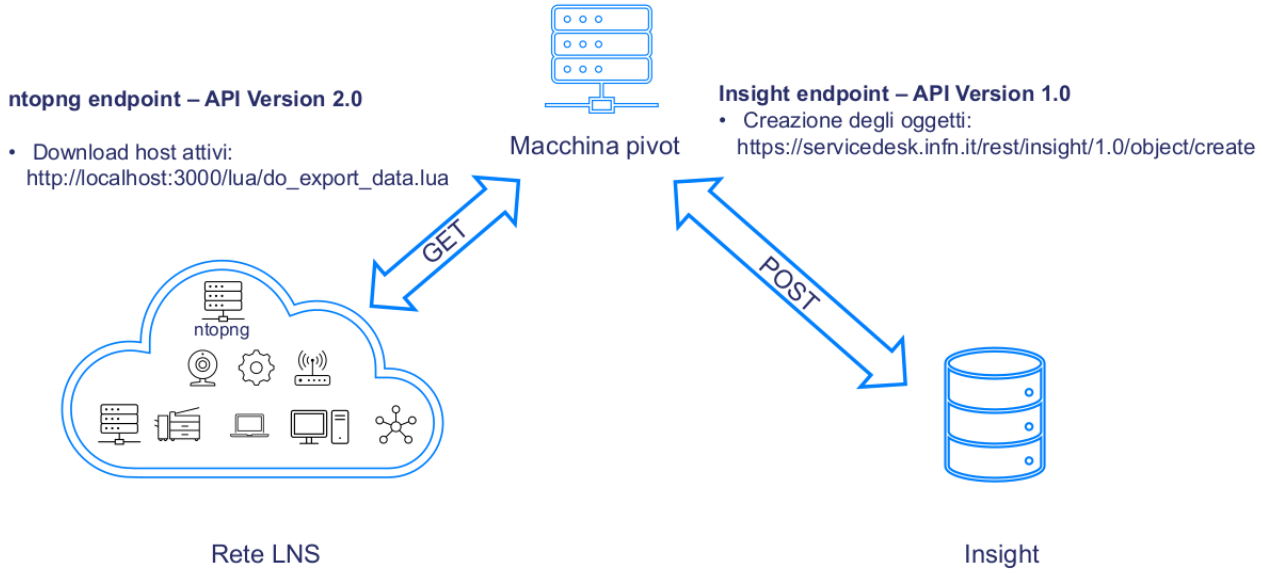
È un tool di discovery in tempo reale (basato su ARP ping ed Nmap) sviluppato dal team NTOP del Prof. Luca Deri (UniPI), la cui versione enterprise gratuita per gli enti di ricerca che ne fanno richiesta. Monitora constantemente la rete fornendo MacAddress, Manufacturer, Device Type, Throughput e tempo di attività degli host attivi.



Flows	224.0.0.252		Multicast	146	0	224.0.0.252	10 days, 13:41:09	Rcvd	2.15 kbit/s ↓	119.88 MB
Flows	fe80::3b6c:8399:783a:d9ab		Local	23	23	DESKTOP-S5LPLOP [IPv6] [DESKTOP-S5LPLOP]	10 days, 13:40:42	Sent	0 bit/s –	64.24 MB
Flows	ff02::16		Multicast	26	0	ff02::16	10 days, 13:41:12	Rcvd	431.83 bit/s ↓	252.19 MB
Flows	fe80::c6f2:af1a:5013:9b25		Local	33	33	LAPTOP-4BLPCDE4 [IPv6] [LAPTOP-4BLPCDE4]	05:09:33	Sent	626.95 bit/s ↓	3.28 MB
Flows	172.16.99.236		Local	37	37	LAPTOP-4BLPCDE4 [MSI]	05:09:33	Sent	499.0 bit/s ↓	2.67 MB
Flows	fe80::417:3c35:90dc:4eab		Local	3	3	fe80.417.3c35.90dc.4ea...	07:14:36	Sent	111.96 bit/s ↓	627.79 KB
Flows	fe80::84a8:a5b1:e0fb:1ccc		Local	38	38	DESKTOP-S5N3D00 [IPv6] [DESKTOP-A687GF2]	10 days, 13:41:12	Sent	431.83 bit/s ↓	295.42 MB
Flows	192.84.151.3		Remote	30	0	192.84.151.3	01:17	Sent Rcvd	785.29 bit/s ↑	9.81 KB
Flows	172.16.90.19		Local	1	1	172.16.90.19 [ANGELOPIDATELLA]	19:09	Sent	0 bit/s –	28.51 KB
Flows	fe80::2367:f721:ad52:b1f5		Local	10	10	pc01-ddinunzi-ctlns-it.IPv6... [DESKTOP-HK80339]	10 days, 05:58:10	Sent	687.73 bit/s ↑	34.04 MB
Flows	ff12::8384		Multicast	10	0	ff12::8384	10 days, 13:41:10	Rcvd	975.61 bit/s ↓	158.32 MB
Flows	172.16.12.68		Local	1	1	DiskStation [DISKSTATION]	10 days, 13:41:11	Sent	167.93 bit/s ↑	96.04 MB
Flows	169.254.96.42		Remote	1	1	169.254.96.42 [0123456789-1]	10 days, 13:41:01	Sent	0 bit/s –	30.59 MB
Flows	172.16.50.27		Local	10	10	DESKTOP-HK80339 [DORA-PC]	10 days, 05:58:09	Sent	559.78 bit/s ↑	21.76 MB
Flows	172.16.14.194		Local	2	2	Dell-Maiolino [DELL-MAIOLINO]	10 days, 13:40:56	Sent	0 bit/s –	28.62 MB
Flows	172.16.14.51		Local	5	5	ubuntu [TORRDO-PC]	10 days, 13:41:08	Sent	0 bit/s –	87.4 MB
Flows	fe80::decd:2fff:fe92:d941		Local	1	1	EPSON.WF-C4810.Series-92D941... [EPSON WF-C4810 Series-92D941]	10 days, 13:41:11	Sent	1.26 kbit/s ↑	227.82 MB
Flows	172.16.50.74		Local	1	1	EPSON92D941 [HP Officejet Pro X476dw MFP [DERD98]]	10 days, 13:41:12	Sent	1.23 kbit/s ↑	220.69 MB

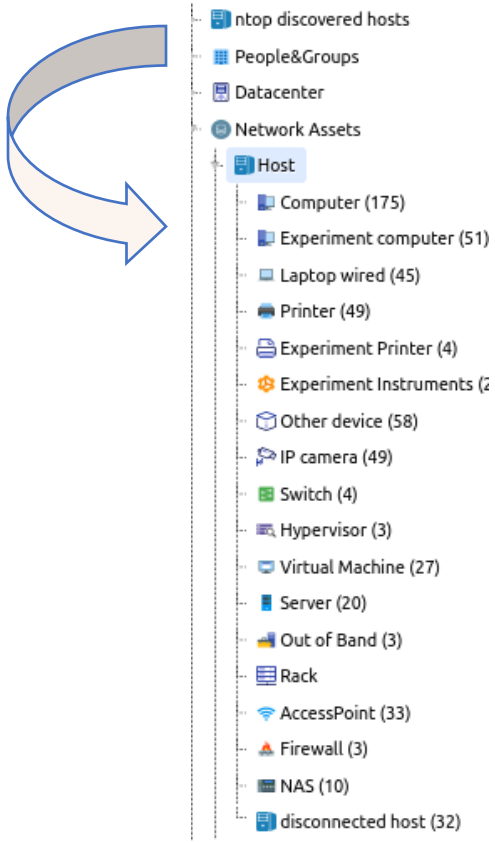
NTOP-NG

Il JSON prodotto da Ntop viene richiesto tramite REST API da una macchina pivot sulla quale girano degli script Python che a loro volta comunicano con le REST API di Insight popolando l'object schema Insight in modo automatico.

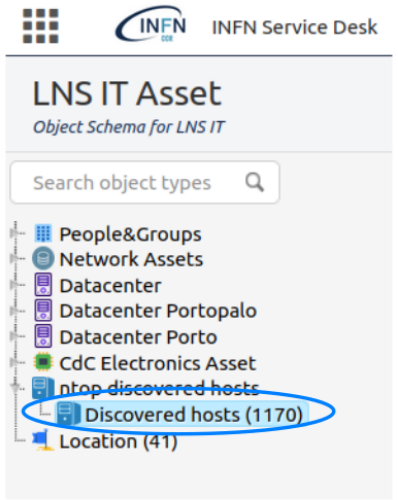


NTOP-NG

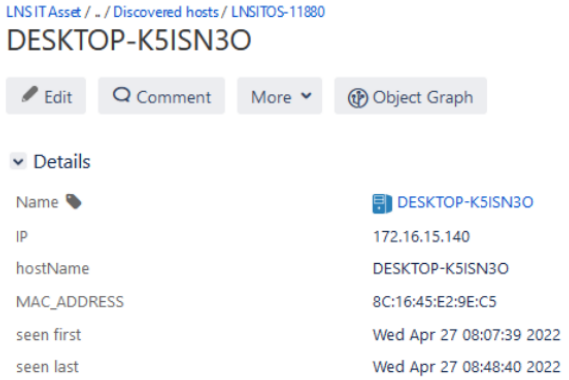
L'object schema viene creato a partire dai template IT predefiniti di Insight, ne è stato definito uno LNS IT ASSET che riflette l'organizzazione logica degli host LNS e gli object sono popolati con gli attributi ritenuti utili. I Discovered host vengono manualmente inseriti negli host group appropriati, il nome del responsabile (owner) dell'host viene inserito in un secondo momento.



Discovered hosts



Attributi del nuovo oggetto



2. SCANSIONI CON GVM

Prima di avviare le scansioni di sicurezza con il Greenbone Vulnerability Manager (GVM), è fondamentale assicurarsi che i feed di OpenVAS siano aggiornati, sono costituiti da una serie di dati utilizzati da GVM per identificare le vulnerabilità e le minacce più recenti.

Il report generato da Greenbone (XML, CVS o PDF) è un report unico contenente una overview per il range di host ed una serie di pagine con risultati per host.
Quest'ultimo contiene una vasta gamma di informazioni, alcune delle quali non sono rilevanti per il nostro specifico scopo, che è quello di **comunicare in modo chiaro al proprietario del dispositivo quali vulnerabilità affligono l'host di cui è responsabile e di seguirlo nella fase di hardening** correttiva o preventiva. Pertanto, è necessario elaborare un processo di filtraggio e elaborazione del report per estrarre e presentare solo le informazioni pertinenti e comprensibili agli utenti finali.

Informazioni come il Product Detection Result, le Refences, Quality of Detection, Vulnerability Insight vengono omesse.

3.PROCESSAMENTO DEI REPORT

LNS Sec

Tool per il processing automatico dei report generati da GreenBone (scritto in Python)

Prende in **input:**

- i report dei task greenbone in formato csv.

Genera in **output**:

- **Report generale** contenente tutte le info relativamente a un range di indirizzi (.md e .pdf) (destinato agli expert per individuare la gravità in quel range)
- **Report specifico** per ciascun host scansionato (.md e .pdf) (destinato agli user)
- **Item per lo storico** di tutte le vulnerabilità rilevate per host (destinato agli expert)

3. PROCESSAMENTO DEI REPORT

Il **Report generale** fornisce informazioni su:

- **numero** di vulnerabilità rilevate
- loro **classificazione** CVSS
- **score** generale del range di host
- **dettaglio** del numero di vulnerabilità rilevate per ciascun host
- loro **classificazione** (condotta in accordo al CVSS)

Una **vulnerabilità** può essere classificata come:

- **High** (7 - 10 CVSS - caldamente consigliato)
- **Medium** (4 - 7 CVSS - consigliato)
- **Low** (1- 4 CVSS - scopo informativo)

3.PROCESSAMENTO DEI REPORT

I **report specifici** (uno per ogni host) forniscono informazioni di base sul:

- numero di vulnerabilità rilevate
- rischi potenziali legati a tali vulnerabilità
- possibili workaround per risolvere le vulnerabilità

Esempio di Report Generale

Data la presenza di 233 vulnerabilità classificate come high, l'host range è considerato come **potenzialmente vulnerabile**.

Per tali ragioni, si è proceduto ad attivare il workflow di ripristino di condizioni di normalità:

- Contattando i responsabili degli host vulnerabili (almeno una vulnerabilità high
- Inviando loro un report riguardante i dettagli delle vulnerabilità rilevate
- Chiedendo loro l'attivazione delle procedure di mitigazione del rischio
- Fornendo supporto tecnico per tutte le attività del caso
- Monitorando l'evoluzione della situazione
- Verificando la corretta applicazione delle contromisure

In aggiunta, data la presenza di vulnerabilità classificate come medium, è stata valutata anche la possibilità di agire nei riguardi degli host che hanno mostrato tale profilo di vulnerabilità.

Dopo attento vaglio, si è proceduto attivando il workflow di ripristino di condizioni di normalità in modalità reccomendation:

- Selezionando gli host maggiormente vulnerabili
- Contattando i responsabili dei sistemi identificati
- Inviando loro un report riguardante i dettagli delle vulnerabilità rilevate
- Chiedendo loro l'attivazione delle procedure di mitigazione del rischio
- Fornendo supporto tecnico per tutte le attività del caso

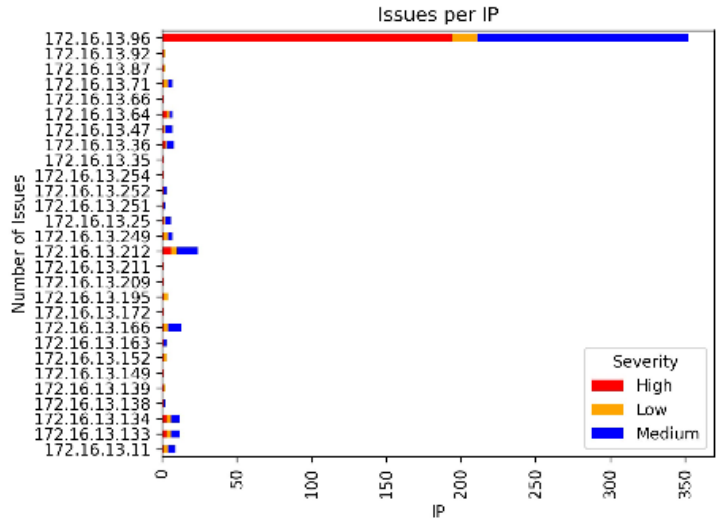
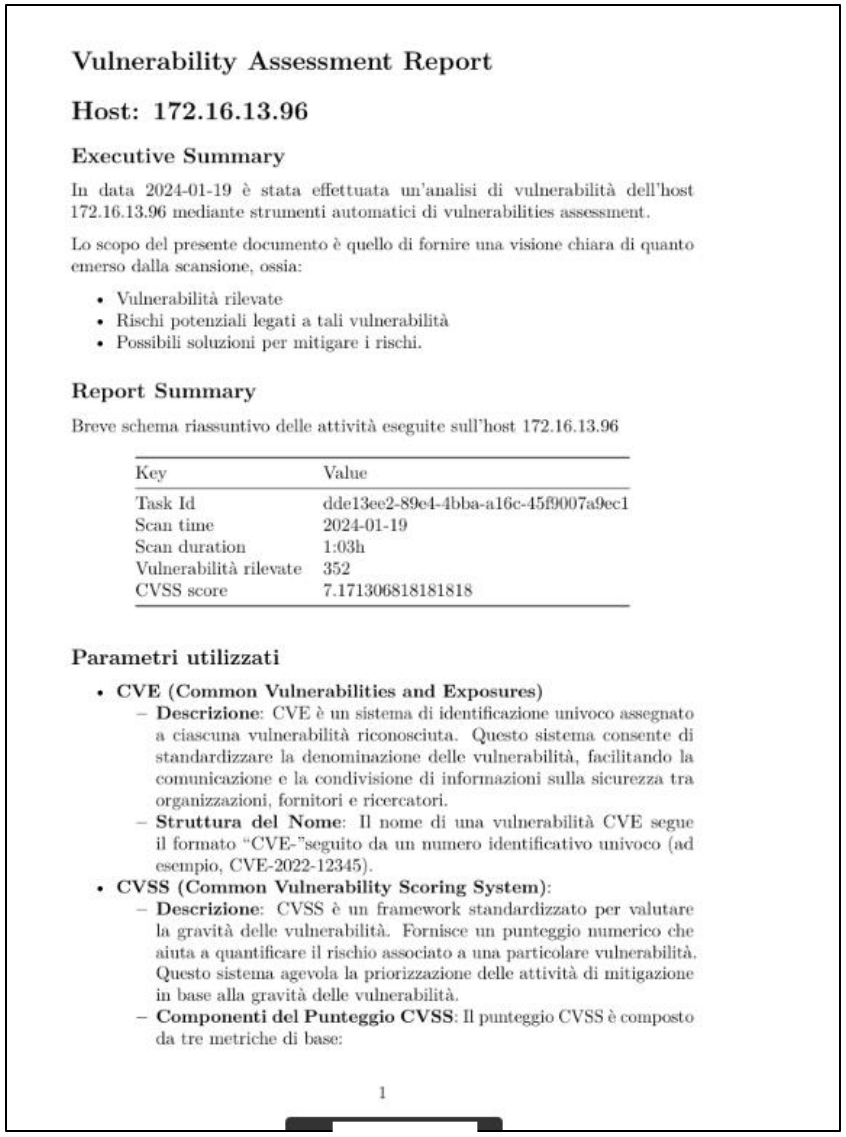


Figure 1: Tipologia di vulnerabilità per host

Esempio di Report Specifico



Vulnerability Assessment Report

Host: 172.16.13.96

Executive Summary

In data 2024-01-19 è stata effettuata un'analisi di vulnerabilità dell'host 172.16.13.96 mediante strumenti automatici di vulnerabilities assessment.

Lo scopo del presente documento è quello di fornire una visione chiara di quanto emerso dalla scansione, ossia:

- Vulnerabilità rilevate
- Rischi potenziali legati a tali vulnerabilità
- Possibili soluzioni per mitigare i rischi.

Report Summary

Breve schema riassuntivo delle attività eseguite sull'host 172.16.13.96

Key	Value
Task Id	dde13ec2-89e4-4bba-a16c-45f9007a9ec1
Scan time	2024-01-19
Scan duration	1:03h
Vulnerabilità rilevate	352
CVSS score	7.171306818181818

Parametri utilizzati

- **CVE (Common Vulnerabilities and Exposures)**
  - **Descrizione**: CVE è un sistema di identificazione univoco assegnato a ciascuna vulnerabilità riconosciuta. Questo sistema consente di standardizzare la denominazione delle vulnerabilità, facilitando la comunicazione e la condivisione di informazioni sulla sicurezza tra organizzazioni, fornitori e ricercatori.
  - **Struttura del Nome**: Il nome di una vulnerabilità CVE segue il formato "CVE-"seguito da un numero identificativo univoco (ad esempio, CVE-2022-12345).
- **CVSS (Common Vulnerability Scoring System)**:
  - **Descrizione**: CVSS è un framework standardizzato per valutare la gravità delle vulnerabilità. Fornisce un punteggio numerico che aiuta a quantificare il rischio associato a una particolare vulnerabilità. Questo sistema agevola la priorizzazione delle attività di mitigazione in base alla gravità delle vulnerabilità.
  - **Componenti del Punteggio CVSS**: Il punteggio CVSS è composto da tre metriche di base:

1

Annuncia:

- Vulnerabilità
- Minacce legate alle vulnerabilità
- Possibili Soluzioni

- Report Summary

- Parametri utilizzati
  - CVE (specifica vuln)
  - CVSS (punteggio dato da gravità intrinseca e rischio ambiente/specifico)

Esempio di Report Specifico

1. *Base Score*: Valuta la gravità intrinseca di una vulnerabilità.
2. *Temporal Score*: Considera fattori che possono variare nel tempo (ad esempio, la disponibilità di patch).
3. *Environmental Score*: Riflette il rischio specifico legato all'ambiente in cui opera il sistema.

– **Valori del Punteggio**: I punteggi CVSS sono espressi su una scala da 0 a 10, dove 10 rappresenta la gravità massima. Inoltre, il CVSS fornisce vettori di base, temporali ed ambientali che dettagliano i criteri utilizzati per il calcolo del punteggio.

Dettagli delle vulnerabilità

Nell'host preso in esame sono state rilevate 352 vulnerabilità, di cui:

- 194 classificate come *high*
- 141 classificate come *medium*
- 17 classificate come *low*

Data la presenza di 194 vulnerabilità classificate come high, l'host è considerato come **potenzialmente vulnerabile**.

Per tali ragioni, si consiglia **caldamente** di procedere a una revisione dettagliata di tutte le vulnerabilità elencate di seguito e di procedere a mettere in pratica tutte le contromisure del caso.

Allegati

Nel seguito, vengono elencate nel dettaglio tutte le vulnerabilità rilevate, assieme a potenziali soluzioni per mitigarle.

Per qualunque dubbio o chiarimento, contattare il centro di calcolo.

Dettagli vulnerabilità: in base al numero di vuln high si considera il grado di vulnerabilità dell'host (ne basta 1 per valutarlo come potenzialmente vulnerabile)

Esempio di Issue

Issue 0

key	Value
Severity	High
CVSS	10.0
Port	443.0
Protocol	tcp
NVT Name	OpenSSL bn_wexpand() Multiple Vulnerabilities - Windows
NVT OID	1.3.6.1.4.1.25623.1.0.800489
Impact	Has unspecified impact and context-dependent attack vectors.
Solution Type	VendorFix

Summary

OpenSSL is prone to multiple vulnerabilities.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host. Details: OpenSSL 'bn_wexpand()' Multiple Vulnerabilities - Windows (OID: 1.3.6.1.4.1.25623.1.0.800489) Version used: 2021-06-30T11:32:25Z

Solution

Update to version 0.9.8m or later.

Severity
CVSS
Port&Protocol
NVT name & OID
Impact
Solution Type
VulnerabilityDetectionMethod
test ha ritenuto la funzione bn_wexpand() vulnerabile per implementazioni SSL su OS server Windows.
Solution

Esempio di Issue

Issue 2

key	Value
Severity	High
CVSS	7.8
Port	22.0
Protocol	tcp
NVT Name	SSH Brute Force Logins With Default Crede
NVT OID	1.3.6.1.4.1.25623.1.0.103239
Impact	This issue may be exploited by a remote att
access to sensitive information or modify system configuration.	
Solution Type	Mitigation

Summary

It was possible to login into the remote SSH server using default credentials.

Vulnerability Detection Method

Reports default credentials detected by the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013). Details: SSH Brute Force Logins With Default Credentials Reporting (OID: 1.3.6.1.4.1.25623.1.0.103239) Version used: 2023-11-03T05:05:46Z

Solution

Change the password as soon as possible.

Issue (**SSH brute force vuln!**)

4. DOCUMENTAZIONE

L'output prodotto dal processamento dei report GVM, organizzato in directory, per classi di Ip ed hosts, viene conservato nel document repository ufficiale dell'INFN, Alfresco.
Lo storico dei follow-up viene conservato per tenere traccia delle azioni intraprese.

5. FOLLOW-UP

Fase di **follow-up manuale:**

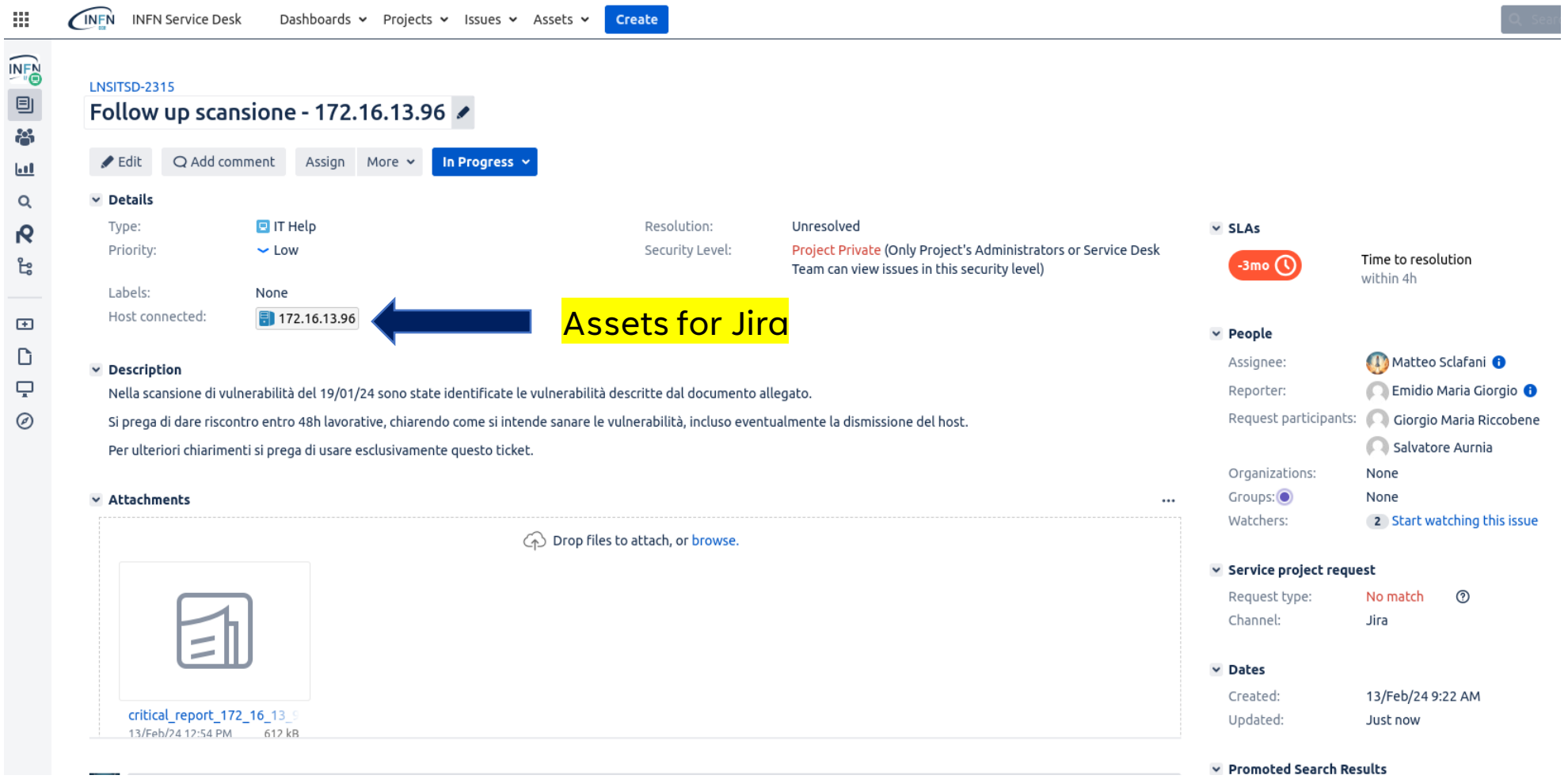
- Importante il follow-up, una vulnerabilità con CVSS alto potrebbe, contestualizzandola ad una rete interna non essere considerata come grave**:**
  - **CVE-2020-25695** - PostgreSQL Privilege Escalation via Extension Installation.
  - **CVE-2021-29447** (WordPress Authenticated SQL Injection)

- possibile utilizzo API di **Jira** SM o semplicemente invio e-mail predefinita per l'apertura automatica di ticket inviata direttamente da LNS sec script in base alla gravità della vulnerabilità

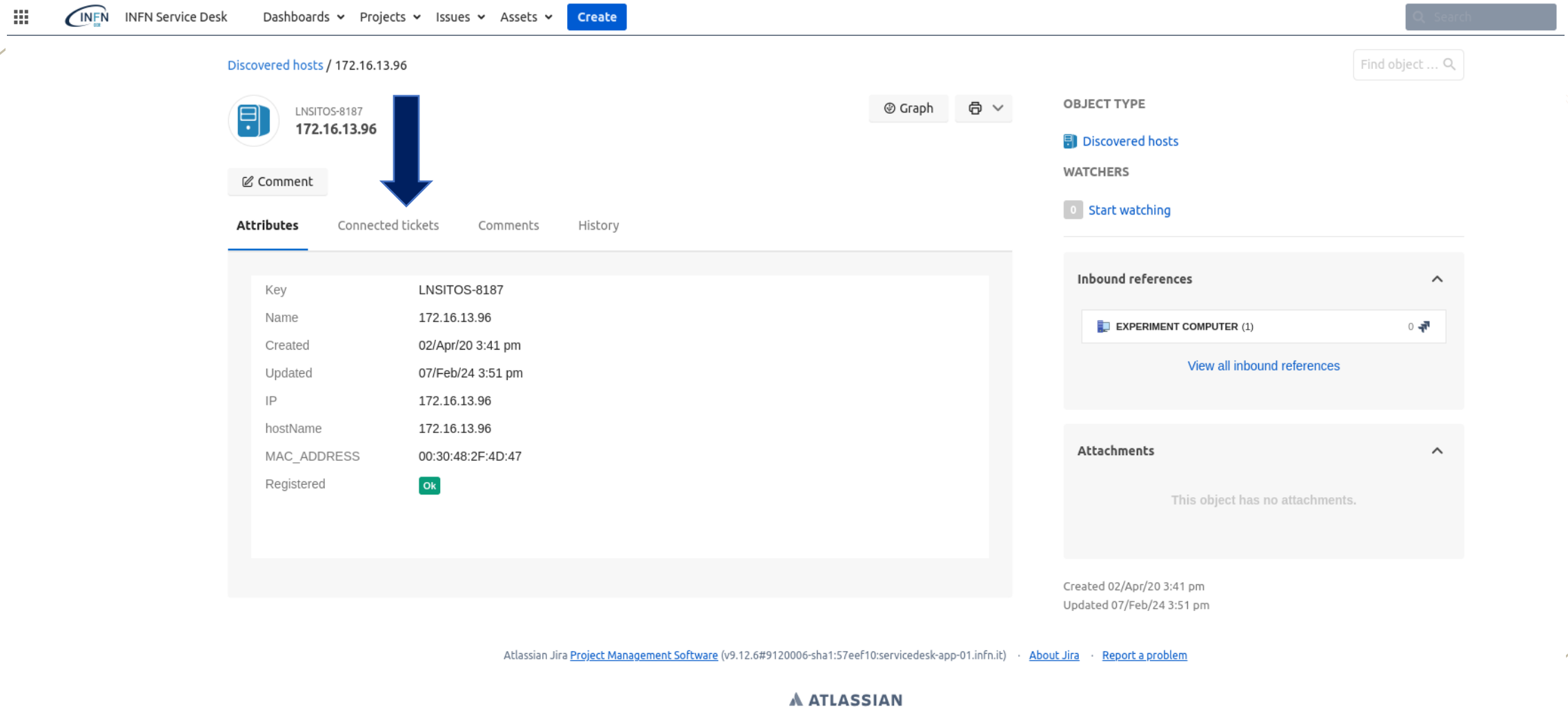
- Il ticket viene associato all'host presente in inventario

- In questo modo guardando la scheda dell'host è possibile consultare lo storico dei ticket associati all'host, compresi quelli sulla vulnerabilità.

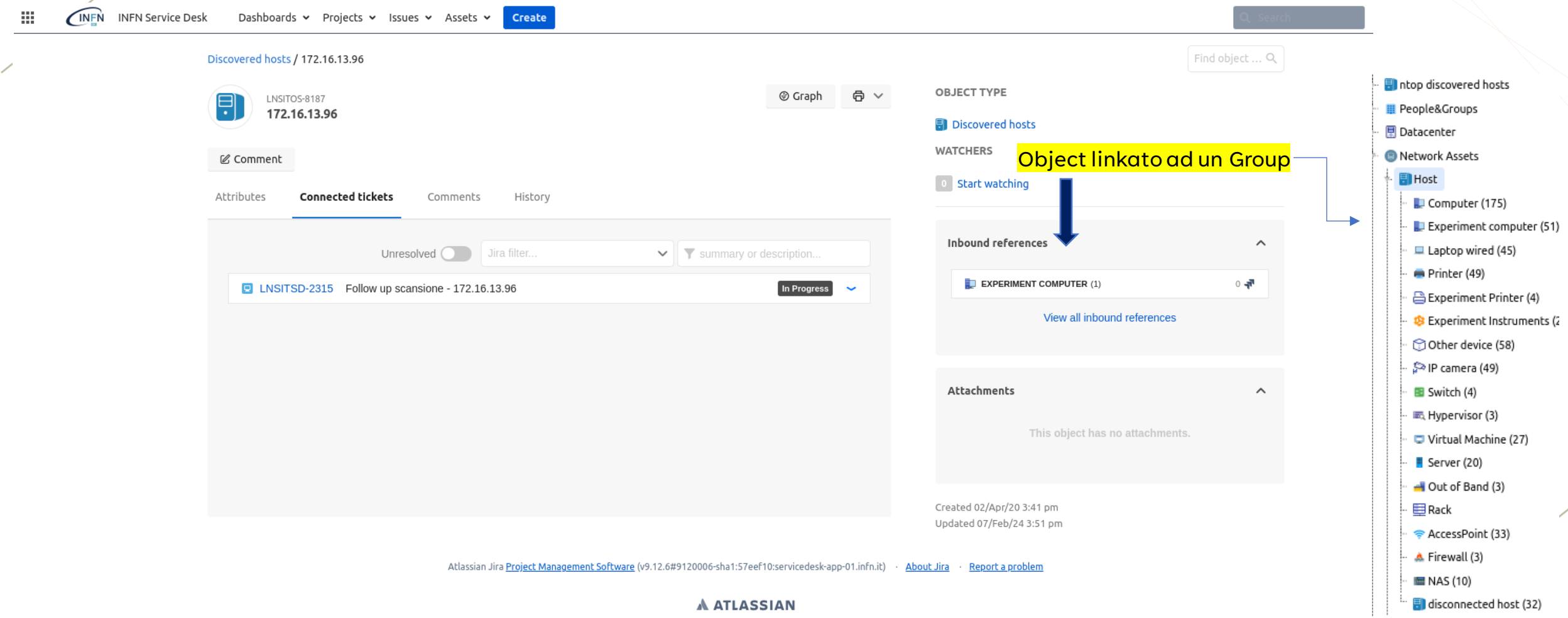
5. FOLLOW-UP


INFN Service Desk
Dashboards
Projects
Issues
Assets
Create
LNSITSD-2315
Follow up scansione - 172.16.13.96
Edit
Add comment
Assign
More
In Progress
Details
Type: IT Help
Priority: Low
Resolution: Unresolved
Security Level: Project Private (Only Project's Administrators or Service Desk Team can view issues in this security level)
Labels: None
Host connected: 172.16.13.96
Assets for Jira
Description
Nella scansione di vulnerabilità del 19/01/24 sono state identificate le vulnerabilità descritte dal documento allegato.
Si prega di dare riscontro entro 48h lavorative, chiarendo come si intende sanare le vulnerabilità, incluso eventualmente la dismissione del host.
Per ulteriori chiarimenti si prega di usare esclusivamente questo ticket.
Attachments
Drop files to attach, or browse.
critical_report_172_16_13_
13/Feb/24 12:54 PM 612 kB
SLAs
-3mo
Time to resolution
within 4h
People
Assignee: Matteo Sclafani
Reporter: Emidio Maria Giorgio
Request participants: Giorgio Maria Riccobene
Salvatore Aurnia
Organizations: None
Groups: None
Watchers: 2 Start watching this issue
Service project request
Request type: No match
Channel: Jira
Dates
Created: 13/Feb/24 9:22 AM
Updated: Just now
Promoted Search Results

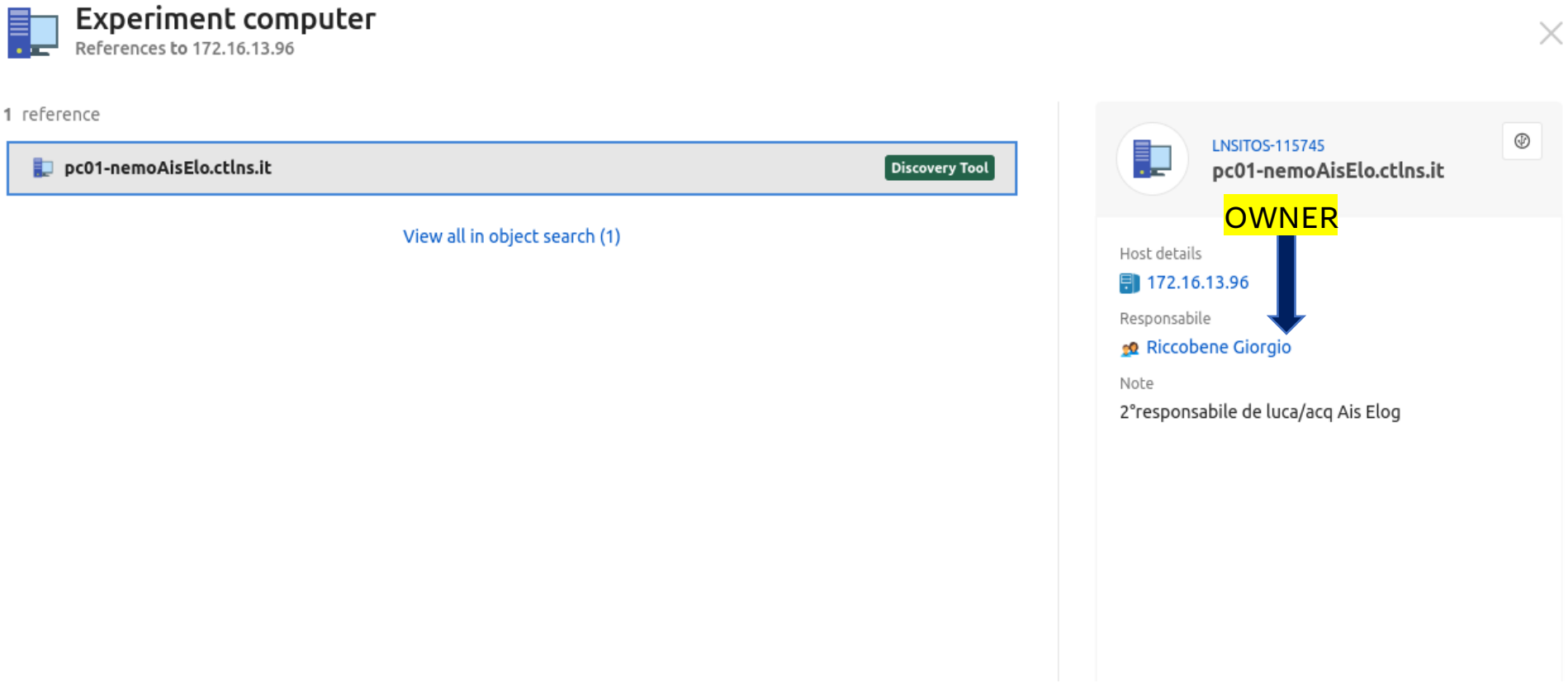
5. FOLLOW-UP


INFN Service Desk
Dashboards
Projects
Issues
Assets
Create
Search
Discovered hosts / 172.16.13.96
Find object ...
LNSITOS-8187
172.16.13.96
Graph
Comment
Attributes
Connected tickets
Comments
History
Key LNSITOS-8187
Name 172.16.13.96
Created 02/Apr/20 3:41 pm
Updated 07/Feb/24 3:51 pm
IP 172.16.13.96
hostName 172.16.13.96
MAC_ADDRESS 00:30:48:2F:4D:47
Registered Ok
OBJECT TYPE
Discovered hosts
WATCHERS
0 Start watching
Inbound references
EXPERIMENT COMPUTER (1) 0
View all inbound references
Attachments
This object has no attachments.
Created 02/Apr/20 3:41 pm
Updated 07/Feb/24 3:51 pm
Atlassian Jira Project Management Software (v9.12.6#9120006-sha1:57eef10:servicedesk-app-01.infn.it) · About Jira · Report a problem
ATLASSIAN

5. FOLLOW-UP


INFN Service Desk
Dashboards
Projects
Issues
Assets
Create
Search
Discovered hosts / 172.16.13.96
Find object ...
LNSITOS-8187
172.16.13.96
Graph
OBJECT TYPE
Discovered hosts
WATCHERS
Object linkato ad un Group
0 Start watching
Comment
Attributes
Connected tickets
Comments
History
Unresolved
Jira filter...
summary or description...
LNSITSD-2315 Follow up scansione - 172.16.13.96
In Progress
Inbound references
EXPERIMENT COMPUTER (1)
0
View all inbound references
Attachments
This object has no attachments.
Created 02/Apr/20 3:41 pm
Updated 07/Feb/24 3:51 pm
Atlassian Jira Project Management Software (v9.12.6#9120006-sha1:57eef10:servicedesk-app-01.infn.it) · About Jira · Report a problem
ATLASSIAN
ntop discovered hosts
People&Groups
Datacenter
Network Assets
Host
Computer (175)
Experiment computer (51)
Laptop wired (45)
Printer (49)
Experiment Printer (4)
Experiment Instruments (2
Other device (58)
IP camera (49)
Switch (4)
Hypervisor (3)
Virtual Machine (27)
Server (20)
Out of Band (3)
Rack
AccessPoint (33)
Firewall (3)
NAS (10)
disconnected host (32)

5. FOLLOW-UP


Experiment computer
References to 172.16.13.96
1 reference
pc01-nemoAisElo.ctlns.it
Discovery Tool
View all in object search (1)
LNSITOS-115745
pc01-nemoAisElo.ctlns.it
OWNER
Host details
172.16.13.96
Responsabile
Riccobene Giorgio
Note
2°responsabile de luca/acq Ais Elog

CONCLUSIONI

Questo approccio operativo dunque facilita la **comprensione** delle **minacce** e, grazie a JSM, degli **interventi** sull'host. **Educa** (sperabilmente) l'utente a mantenere il proprio host aggiornato e sicuro ed **utilizza strumenti** già ampiamente **diffusi** e testati in INFN.

INFN
LNS
Istituto Nazionale di Fisica Nucleare
Laboratori Nazionali del Sud

GRAZIE!