I.S.F.O.A. HOCHSCHULE FÜR SOZIALWISSENSCHAFTEN UND MANAGEMENT

Corso di Laurea Magistrale

Ingegneria Informatica

Tesi di Laurea

Magistrale

Cybersecurity

Strumenti di supporto alla creazione di un inventario delle risorse hardware, software e di rete al fine di garantire un elevato livello di sicurezza delle reti, dei sistemi informativi, dei servizi delle pubbliche amministrazioni e dei privati.

Relatore

Prof. Ing. Gianfranco LIUZZI

Candidato

Vincenzo PERNETTI

Giugno

2022

Non sempre **cambiare** equivale a

migliorare, ma per migliorare bisogna

cambiare

Sommario

1 INTRODUZIONE

La tecnologia dell'informazione (IT) è diventata sempre più importante negli ultimi tempi, poiché influenza sia la vita privata che quella pubblica degli individui in vari modi. Infatti, non solo si utilizzano costantemente dispositivi elettronici per comunicare e creare grandi quantità di dati che vengono costantemente inviati su Internet, ma lo stesso si può dire per diverse aziende in vari campi, che oggigiorno non possono evitare l'uso dell'informatica.

La diffusione di queste nuove tecnologie comporta alcuni inconvenienti, uno su tutti i rischi derivanti dalla possibilità che tali dati vengano rubati o compromessi, e più in generale tutti i problemi legati all'integrità fisica o logica dei beni.

La disciplina preposta ad affrontare queste problematiche è la cybersecurity e gli studi in questo campo sono orientati alla protezione degli asset da possibili attacchi che potrebbero portare ad un danno superiore ad una certa soglia di tolleranza.

La sicurezza informatica è composta da molteplici aspetti, il National Institute of Standards and Technology (NIST) definisce cinque funzioni principali [1]:

- **Identificare:** sviluppare e implementare una comprensione organizzativa per gestire il rischio di sicurezza informatica. Questo nucleo è il fondamento di tutti gli altri;
- **Proteggere:** sviluppare e attuare tutele adeguate al fine di garantire la fornitura dei servizi;
- **Detenere:** sviluppare e implementare attività appropriate per identificare il verificarsi di un evento di cybersecurity;
- **Rispondere:** sviluppare e implementare le attività per rispondere a un rilevato evento di sicurezza informatica;
- **Recuperare:** sviluppare e implementare attività appropriate da mantenere piani per la resilienza e per ripristinare eventuali capacità o servizi danneggiati a causa di un incidente di sicurezza informatica.

Il governo italiano ha deciso di investire risorse nel tema della sicurezza informatica e nella "Legge 18 Novembre 2019, n.133" [11] è stato istituito un nuovo strumento denominato Perimetro di Sicurezza Nazionale Cibernetica (PSNC); il suo scopo è garantire un elevato livello di sicurezza delle reti, dei sistemi informativi, dei servizi delle pubbliche amministrazioni e dei privati che forniscono un servizio essenziale per gli interessi dello Stato.

L'idea alla base del PSNC è che ci sono alcuni beni che devono essere difesi in modo forte e quindi i soggetti inclusi nel PSNC sono tenuti a seguire determinate misure e obblighi definiti nella legge costitutiva. In particolare un soggetto inserito nel PSNC deve:

- Tenere un elenco delle reti, dei sistemi informativi e dei sistemi informatici necessari per fornire il servizio per il quale il soggetto fa parte del PSNC. Inoltre tale elenco deve essere aggiornato almeno una volta all'anno e deve includere la relativa architettura e componenti;
- Segnalare gli incidenti che interessano le reti, i sistemi informativi ei sistemi informatici al Computer Security Incident Response Team (CSIRT) italiano che trasmette tempestivamente tali segnalazioni al Dipartimento delle informazioni per la sicurezza (DIS).

Da questi requisiti emerge che identificare gli asset e gestirli nel modo corretto è fondamentale per assicurarsi che un sistema sia protetto correttamente, poiché questa è la base di tutte le tecniche di sicurezza necessarie per rendere sicuro un sistema.

L'inventario degli asset sta diventando sempre più importante per le aziende e le pubbliche amministrazioni che vogliono mantenere un elevato livello di sicurezza e per questo negli ultimi anni sono stati creati diversi strumenti commerciali, con costi e servizi erogati differenti.

L'obiettivo di questa tesi è esplorare questo vasto mondo di inventario degli asset e trovare le migliori soluzioni con l'obiettivo di soddisfare i requisiti del PSNC.

In particolare l'idea è quella di guardare anche all'aspetto economico e provare a combinare diversi strumenti open-source con lo scopo di creare un nuovo strumento in grado di essere calato all’interno di una pubblica amministrazione con costi minimi ma garantendo un’alta efficienza ed efficacia.

Per raggiungere obiettivo prefissato è stato avviato un notevole studio dell'arte analizzando i diversi strumenti esistenti per capire pro e contro e in generale per capire il funzionamento e cosa si poteva creare sfruttando questi strumenti.

L'attenzione è stata posta nello sviluppo di soluzioni che potessero funzionare in diversi ambienti in modo da non dover legare le tecnologie utilizzate agli strumenti preposti al controllo.

Inoltre si è data molta attenzione alla possibilità di sfruttare il più ampio ventaglio di prodotti open-source, interagendo anche con diverse comunità di sviluppatori.

Il mondo dell'inventario degli asset è strettamente correlato con un altro importante ramo della sicurezza informatica chiamato Vulnerability Assestment and Penetration Testing (VAPT) che è l'unificazione di due pratiche molto importanti per garantire la sicurezza.

Il test di penetrazione e la valutazione della vulnerabilità eseguono due attività diverse, ma vengono eseguiti insieme per fornire un'analisi della vulnerabilità più completa.

In particolare, il Vulnerability Assessment è il processo di identificazione, quantificazione e priorità (o classificazione) delle vulnerabilità in un sistema, mentre un Penetration Test è un attacco informatico simulato autorizzato su un sistema informatico, eseguito per valutarne la sicurezza.

Questo tipo di analisi necessita di diversi strumenti progettati ed implementati per facilitare e rendere più veloce l'esecuzione dei test.

In questa tesi alcuni di essi verranno sfruttati e spiegati nelle loro funzionalità, ma questo mondo è in continua evoluzione, pertanto, in futuro verranno creati strumenti sempre nuovi e con caratteristiche migliorative.

Storicamente, l'inventario delle risorse è stato particolarmente difficile e molto manuale (spesso richiedendo visite fisiche in loco) per i referenti con dispositivi "Grid-edge" (o dispositivi sul campo).

L'atto di eseguire la scoperta degli asset può essere effettuato in due modi principali:

- Attivamente, questo è il metodo più standard e consiste nell'uso di software che sondano i dispositivi attraverso una rete o utilizzano dispositivi di rilevamento che tentano di accedere ai dispositivi per recuperare un inventario completo delle applicazioni connesse. In questo modo la rete potrebbe essere rallentata e questo potrebbe essere un problema per reti sensibili al tempo, motivo per cui il secondo metodo sta diventando più popolare;
- Passivamente, consiste essenzialmente nell'ascoltare il traffico inviato su una rete ed elimina la necessità di consumare larghezza di banda. Al giorno d'oggi, i progressi nel monitoraggio della sicurezza della rete e nell'ispezione approfondita dei pacchetti del protocollo hanno consentito ai proprietari delle risorse di ottenere in modo passivo (non intrusivo) informazioni sull'inventario delle risorse in tempo reale dai dispositivi che comunicano su canali di comunicazione seriali o basati su TCP/IP. Non solo è possibile ottenere la gestione passiva delle risorse in questo modo, ma anche il monitoraggio passivo della sicurezza della rete in grado di rilevare una varietà di anomalie di rete, di sicurezza e operative.

Le soluzioni esplorate in questa tesi prendono in considerazione entrambi questi approcci cercando di sfruttarne i punti di forza, al fine di creare uno strumento che sia proattivo e in

grado di identificare nuovi asset e gestirli nel modo corretto automatizzandolo il più possibile per garantire il minor impiego di lavoro manuale e personale specializzato.

L'inventario delle risorse è necessario per ottenere un quadro completo di tutte le risorse hardware, software e di rete.

Ai fini di questa tesi e dei requisiti specificati nella normativa del PSNC, l'obiettivo finale è quello di raccogliere tutte le informazioni sull'asset attraverso gli strumenti dell'asset discovery e quindi creare un elenco di tutte queste informazioni, in modo che possa essere consultato facilmente e periodicamente aggiornato.

2 ANALISI DEI REQUISITI

Questo capitolo esplora il concetto di gestione degli asset con un focus su un importante protocollo utilizzato in questo campo e offre una panoramica sulla scoperta degli asset e sull'inventario degli asset con il motivo per cui sono importanti. Viene inoltre fornita una breve panoramica sullo strumento di asset discovery utilizzato in questa tesi, con particolare attenzione riservata alle tecniche sfruttate dagli strumenti.

2.1 Introduzione

Innanzitutto è importante dare una definizione di asset. La parola asset può avere significati diversi per diversi campi di applicazione. Nell'area della sicurezza informatica una risorsa è qualsiasi dato, dispositivo o altro componente dell'ambiente che supporta attività relative alle informazioni. Ciò può includere hardware, software o qualsiasi tipo di informazione riservata [8]. In generale, un bene deve essere protetto dall'accesso, dall'uso, dalla divulgazione, dall'alterazione, dalla distruzione e/o dal furto illeciti, con conseguenti perdite per l'organizzazione [9].

Una risorsa IT può essere distinta in due componenti principali, che sono entrambe fondamentale per descrivere un sistema:

- **Asset hardware**, in questa categoria sono ricompresi tutti gli aspetti fisici dell'infrastruttura con i suoi componenti e le risorse allocate alle loro esigenze.
- **Asset software**, ovvero tutte le informazioni relative ai programmi in bloccato sui dispositivi che compongono l'infrastruttura.

A queste due definizioni corrispondono rispettivamente i concetti di Hardware Asset Management (**HAM**) e Software Asset Management (**SAM**) che sono entrambi cruciali nel contesto della scoperta degli asset e dell'inventario degli asset per capire quali sono gli asset che devono essere raccolti e quindi protetti.

2.2 Protocollo di gestione della rete semplice

Per svolgere le azioni che riguardano la configurazione, la gestione e la supervisione dei sistemi presenti in una rete è stato definito dall'Internet Engineering Task Force (IETF) un protocollo Internet. Il nome di questo protocollo è Simple Network Management Protocol (SNMP). Le informazioni scoperte attraverso l'uso di questo protocollo sono esposte sotto forma di variabili e sono organizzate in una base di informazioni di gestione (MIB) che viene utilizzata per

descrivere lo stato e la configurazione del sistema. Su queste variabili possono essere applicate query remote utilizzando le applicazioni di gestione. I dispositivi che in genere supportano SNMP includono modem via cavo, router, switch, server, workstation, stampanti e altro [12].

2.2.1 Panoramica e componenti

L'uso tipico di SNMP consiste nell'allestire uno o più computer amministrativi, detti gestori, che hanno il compito di monitorare o gestire un gruppo di altri host o dispositivi che formano una rete di computer. Su questi sistemi gestiti viene installato ed eseguito un componente software, che prende il nome di agente, ed ha il compito di riportare le informazioni via SNMP al gestore.

In una rete gestita da SNMP ci sono tre componenti chiave:

- Dispositivi gestiti, che sono oggetto di analisi le informazioni che vengono raccolte;
- Agent, ovvero il software che gira sui dispositivi gestiti;
- Network Management Station (NMS), ovvero il software in esecuzione sul manager. Ha il compito di eseguire applicazioni che monitorano e controllano i dispositivi gestiti.

Un dispositivo gestito è un nodo di rete che implementa un'interfaccia SNMP che consente l'accesso unidirezionale (sola lettura) o bidirezionale (lettura e scrittura) alle informazioni specifiche del nodo. I dispositivi gestiti si scambiano in base al nodo informazioni con i NMS. Nella figura 2.1 viene mostrato il principio della comunicazione SNMP e viene chiarito il ruolo dei vari attori.

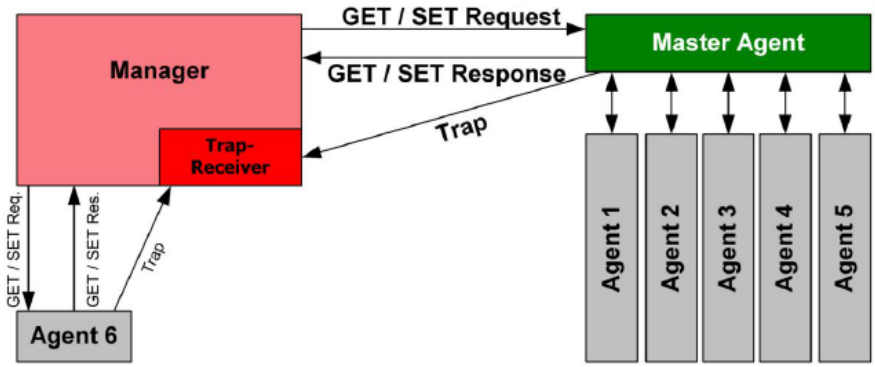

Figura 2.1. Principio della comunicazione SNMP1

Il protocollo SNMP opera sul livello 7 del modello OSI ed è composto da messaggi che vengono trasportati tramite User Datagram Protocol (UDP) [6].

Sono state definite sette unità di dati di protocollo (PDU) principali, cinque da SNMPv1 e le altre sono state specificate più avanti nella versione 2 del protocollo SNMP. La costruzione di una PDU SNMP è mostrata nella figura 2.2 ed è la stessa per tutte le PDU core.

Figura 2.2. Composizione di un'unità di dati del protocollo SNMP

Il campo PDU-type identifica le sette diverse PDU SNMP che sono le seguenti:

- **GetRequest**: una richiesta da manager ad agente inviata per ottenere il valore di una variabile o un elenco di variabili;
- **SetRequest**: una richiesta da manager ad agente inviata per modificare il valore di una variabile o di un elenco di variabili;
- **GetNextRequest**: una richiesta da manager ad agente inviata per scoprire se le variabili sono disponibili ei loro valori;
- **GetBulkRequest**: è una versione ottimizzata di GetNextRequest. In questo caso vengono inviate più iterazioni di GetNextRequest . Questo era uno dei tipi di PDU introdotti nella versione 2 del protocollo SNMP;
- **Response:** è lo strumento con cui le associazioni e le conoscenze variabili vengono restituite da agente a manager in risposta alle varie richieste da manager ad agente;
- **Trap**: è una notifica asincrona dall'agente al manager. La differenza tra Trap e Response è che questo tipo di PDU non è esplicitamente richiesto dal gestore e serve per segnalare eventi significativi;
- **InformRequest**: Originariamente era una comunicazione da manager a manager, ma nella recente implementazione sono possibili anche messaggi da agent a manager. Il compito di questa PDU è riconoscere che è stata ricevuta una notifica asincrona.

2.3 Scoperta delle risorse

Il primo passo per eseguire la gestione degli asset consiste nel rilevare e raccogliere tutte le informazioni sui vari asset presenti in una rete. Questo processo di ricerca ed elenco delle risorse IT e di monitoraggio periodico delle stesse è chiamato Asset Discovery ed è fondamentale per mantenere l'integrità dei dati distribuiti nell'infrastruttura di un'organizzazione.

Lo scenario di base in cui avviene il rilevamento delle **risorse** è tramite un'applicazione installata su una risorsa specifica come un PC, collegato in rete, che è responsabile della scansione dell'intera **infrastruttura** per raccogliere informazioni sulle risorse nella rete.

Questo tipo di asset discovery è sicuramente preferibile ad un elenco manuale di tutti i dati, poiché garantisce, oltre all'eliminazione dell'errore umano, l'aggiornamento costante delle informazioni.

2.3.1 NMAP

Uno dei software più utilizzati nel campo dell'asset discovery è Nmap. L'aspetto più importante che ha contribuito alla popolarità di questo software è sicuramente che è disponibile gratuitamente e opensource tanto da essere usato da, molti altri, software di asset discovery come base per la scansione della rete e il controllo della sicurezza.

Nmap è iniziata come utility Linux, pubblicata come articolo con codice sorgente incluso [3], ma è stata successivamente trasferita su altri sistemi tra cui Windows, macOS e BSD [17].

Figura 2.3. *Logo Nmap*

Nmap offre molte funzionalità diverse [4], tra cui:

- Host discovery - Possibilità di eseguire una scansione della rete per cercare host che rispondono a una richiesta TCP o ICMP o che hanno una particolare porta aperta;
- Scansione delle porte: enumerare ed elencare le porte aperte di un host;

- Version Detection - Interrogazione dei servizi attivi degli host in rete lavorando per determinare il nome dell'applicazione e il numero di versione;
- Impronta digitale dello stack TCP/IP - Determinazione del sistema operativo e delle caratteristiche hardware dei dispositivi di rete sulla base delle osservazioni dell'attività di rete di detti dispositivi;
- Interazione tramite script con il target - nuovissima funzionalità, che grazie a Nmap Script Engine (NSE) [18] permette di utilizzare semplici script per automatizzare un'ampia varietà di attività.

Oltre a questo Nmap può fornire altre informazioni su target come nomi DNS inversi, tipi di dispositivi o indirizzi MAC.

Per eseguire questo tipo di analisi Nmap sfrutta vari metodi, che analizzeremo di seguito spiegando la procedura più importante necessaria per fornire le funzionalità sopra menzionate.

Tecniche di scoperta dell'host di Nmap

Poiché le esigenze di rilevamento degli host sono così diverse e l'ambiente in cui viene utilizzato Nmap potrebbe variare notevolmente a seconda della situazione, questo strumento offre un'ampia varietà di opzioni per personalizzare le tecniche utilizzate.

Solitamente in una rete è comune avere una piccola percentuale di IP attivi (cioè utilizzati da un host o da un dispositivo) in un dato momento, pertanto, il punto di forza di uno strumento come Nmap è la possibilità di eseguire host discovery e trovare le macchine attive in un'area ampia e scarsamente allocata di indirizzi IP in brevissimo tempo [14].

Il modo standard per eseguire l'host discovery in Nmap, non considerando quindi l'uso di opzioni specifiche che possono modificare questo comportamento, è l'invio da parte di Nmap di una richiesta echo ICMP, un pacchetto TCP SYN alla porta 443, un pacchetto TCP ACK alla porta 80 e una richiesta di timestamp ICMP. (Per IPv6, la richiesta timestamp ICMP viene omessa perché non fa parte di ICMPv6.)

Esiste un'eccezione per quanto riguarda una rete ethernet locale in cui vengono invece utilizzati ARP (per IPv4) e Neighbor Discovery (per IPv6). Se un utente UNIX non è privilegiato, la scansione predefinita comporterà l'uso di pacchetti SYN sulle porte 80 e 443 utilizzando la chiamata di sistema Connect.

Oltre al metodo standard di esecuzione dell'host discovery menzionato sopra, esistono ancora altre tecniche che possono essere specificate mediante l'uso di opzioni particolari. Questi sono il ping UDP, il ping SCTP INIT (cioè l'invio di un pacchetto SCTP contenente un chunk INIT

minimo, usato per suggerire al sistema remoto che Nmap sta cercando di stabilire un'associazione) ed infine il ping del protocollo IP, che è uno dei opzione di rilevamento host più recente e consiste nell'invio di pacchetti IP con il numero di protocollo specificato impostato nell'intestazione IP.

Tecniche di scansione delle porte Nmap

Nell'arte della scansione delle porte ci sono molte tecniche e trovare quella giusta che può essere adatta a un determinato compito può essere molto difficile, quindi è importante conoscere le differenze tra tutte per capire quale usare in uno specifico contesto. Nmap supporta tutte queste tecniche e quindi in questa sezione viene fornita una breve spiegazione di esse. Quasi tutte le scansioni elencate di seguito richiedono che l'utente disponga dei privilegi di amministratore.

- Scansione TCP SYN: la scansione più rapida e semplice, in grado di sondare migliaia di porte al secondo su una rete veloce non ostacolata da firewall restrittivi. È anche relativamente discreto e nascosto poiché la connessione TCP non è completata;
- Scansione TCP ACK: a differenza delle scansioni sopra citate, questa scansione non determina mai le porte aperte e viene utilizzata principalmente per mappare i set di regole del firewall, determinando se sono stateful o meno e quali porte vengono filtrate;
- Scansione connessione TCP: l'opzione predefinita se la scansione SYN TCP non è disponibile, ad esempio se un utente non dispone dei privilegi per i pacchetti non elaborati. Sfrutta la chiamata di sistema connect ed è meno efficiente e più rilevabile della scansione TCP SYN e quindi quest'ultima è preferibile quando disponibile.
- Scansione TCP Window: molto simile alla scansione ACK ma sfrutta un dettaglio di implementazione che può differenziare le porte aperte da quelle chiuse in alcuni sistemi. Basandosi su un dettaglio di implementazione presente solo in una minoranza dei sistemi, questa scansione non è del tutto affidabile e il sistema che non la supporta di solito restituirà tutte le porte chiuse;
- Scansioni UDP: molti servizi utilizzano UDP invece di TCP (es. DNS, SNMP, DHCP, ecc.) e quindi queste porte possono essere scansionate per rilevare questi servizi. La scansione UDP funziona inviando un pacchetto a ogni porta di destinazione;
- Scansioni TCP NULL, FIN e Xmas: queste tre scansioni sfruttano un difetto nell'RFC TCP che permette di distinguere tra porte aperte e chiuse. Il vantaggio principale di questo

tipo di scansioni è che possono superare alcuni firewall non con stato e router di filtraggio dei pacchetti;

- Scansione SCTP INIT: questa è un'alternativa relativamente nuova a TCP e UDP. La scansione è l'equivalente SCTP di una scansione TCP SYN e mantiene le qualità di rapidità e discrezione;
- Scansione SCTP COOKIE ECHO: questa è una scansione SCTP più avanzata. Ha il vantaggio di essere più invisibile rispetto a una scansione INIT SCTP tradizionale, ma ha lo svantaggio di non essere in grado di distinguere tra porte aperte e filtrate;
- Scansione del protocollo IP: questa non è propriamente una scansione delle porte poiché scorre i numeri del protocollo IP anziché il numero delle porte TCP e UDP. Lo scopo di questa scansione è determinare quali protocolli IP sono supportati dai sistemi di destinazione.

Rilevamento del sistema operativo Nmap

Quando viene eseguita una scansione di una rete, il risultato ideale è la raccolta del maggior numero possibile di informazioni e non solo un elenco di IP e porte attive, infatti il rilevamento del sistema operativo è una caratteristica importante offerta da Nmap [15] in quanto permette di capire, nella maggior parte dei casi, non solo quale tipo di macchina è proprietaria di un determinato indirizzo IP, ma anche l'esatta versione del sistema operativo installato sulla suddetta macchina.

Questo può essere molto utile quando si esegue ogni tipo di valutazione della vulnerabilità ma anche, poiché viene utilizzato ai fini di questa tesi, per eseguire la scoperta e l'inventario degli asset.

Le tecniche alla base del rilevamento di Nmap OS sono varie e sfruttano molte implementazioni diverse aggiunte a caratteristiche specifiche dei sistemi operativi installati sulla macchina di destinazione della scansione. In generale il metodo di rilevamento del sistema operativo fornito da Nmap consiste nell'effettuare vari test al termine dei quali viene prodotta un'impronta digitale con i risultati di questi test. Un tipico esempio di impronta digitale prodotta da una scansione di rilevamento del sistema operativo Nmap può essere visto nella figura 2.4.

L'idea alla base della creazione di un'impronta digitale è che può essere confrontata con quelle create in precedenza e incluse nel database di Nmap per capire quale sistema operativo è in esecuzione sulla macchina.

```
OS:SCAN(V=5.05BETA1%D=8/23%OT=22%CT=1%CU=42341%PV=N%DS=0%DC=L%G=Y%TM=4A91CB
OS:90%P=i686-pc-linux-gnu)SEQ(SP=C9%GCD=1%ISR=CF%TI=Z%CI=Z%II=I%TS=A)OPS(O1
OS:=M400CST11NW5%O2=M400CST11NW5%O3=M400CNNT11NW5%O4=M400CST11NW5%O5=M400CS
OS:T11NW5%O6=M400CST11)WIN(W1=8000%W2=8000%W3=8000%W4=8000%W5=8000%W6=8000)
OS:ECN(R=Y%DF=Y%T=40%W=8018%O=M400CNNSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+
OS:%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=8000%S=O%A=S+%F=AS%O=M400CST11NW
OS:5%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
OS:T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%U
OS:N=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Figura 2.4. Una tipica impronta digitale del soggetto

2.4 Inventario dei beni

Dopo aver raccolto le informazioni sugli asset è importante utilizzare questi dati per costruire un inventario che renda il lavoro performante.

la valutazione della vulnerabilità più è semplice e più in generale permette di avere una visione chiara degli asset che compongono una specifica infrastruttura. Questa pratica è chiamata Asset Inventory ed è ora richiesta da molti standard, testi e regolamenti diversi relativi al governo IT e alla sicurezza delle informazioni, e qui vengono forniti alcuni esempi [5]:

- La norma ISO/IEC 27001 [17] richiede che "qualsiasi risorsa associata alle informazioni e alle strutture di elaborazione delle informazioni deve essere identificata e gestita lungo tutto il ciclo di vita, sempre aggiornata. È necessario creare un registro o un inventario di tali risorse che mostra come sono gestiti e controllati, in base alla loro importanza";
- Il Cobit Framework 4.1 [7] include un inventario dei componenti e dei sistemi critici (DS4), degli elementi hardware e software (DS9), dei supporti archiviati e archiviati (DS11.3), delle strutture fisiche (DS12) che deve anche essere classificati a seguito del processo di gestione del rischio ed infine degli asset informatici sensibili (DS13.4);
- Il NIST oltre al già citato NIST Cybersecurity Frame work[1] menziona l'inventario degli asset anche in un'altra pubblicazione [13] dove è richiesto che l'azienda sviluppi, documenti e mantenga un inventario dei componenti del sistema;
- Lo standard PCI DSS [2] afferma che l'inventario delle risorse è "un elenco completo di risorse che rientrano nell'ambito della valutazione del rischio, ad esempio software, hardware, infrastrutture di rete e di comunicazione e personale".

Per quanto riguarda l'asset discovery, anche per la parte di asset inventory si stanno sviluppando molti nuovi strumenti e questo mondo è in continua evoluzione.

Questo campo può essere molto importante anche per ragioni economiche, poiché il tema è la corretta gestione di asset che potenzialmente hanno un certo valore, e quindi gli strumenti sono spesso piuttosto costosi. In questa tesi come spiegato nell'introduzione lo scopo è cercare di favorire il software open-source.

3 PERIMETRO DI SICUREZZA NAZIONALE CIBERNETICA

In questo capitolo un breve chiarimento del contesto in cui si inserisce questa tesi in parte vengono forniti, con un focus sul Perimetro di Sicurezza Nazionale Cibernetica (PSNC), gli obiettivi che si pongono alla base della sua creazione e una spiegazione della normativa e delle varie terminologie utilizzate nella legge costitutiva e nei successivi Decreti del Presidente del Consiglio dei Ministri (DPCM).

3.1 Storia

Il crescente processo di digitalizzazione della Pubblica Amministrazione fanno si che debbano crescere gli standard di sicurezza necessari a fronteggiare i numerosi attacchi cyber che, sempre più di frequente, mettono a rischio la sicurezza dei dati di milioni di cittadini e di innumerevoli imprese.

Pertanto, già da qualche anno il legislatore ha introdotto numerose norme in materia di Cybersicurezza, tra cui quelle che hanno portato alla nascita e allo sviluppo del Perimetro di sicurezza nazionale cibernetica (PSNC) e della sua disciplina, un iter iniziato con il d.l. 105/2019 e recentemente terminato con il d.lgs. 82/2021, modificato con l. 109 del 4 agosto 2021.

Nonostante il completamento della disciplina sul PSNC, il percorso intrapreso dal legislatore, tra nuovi testi normativi e istituzione di particolari strutture dedicate alla cybersicurezza nazionale, non si è mai arrestato, anzi l'impegno delle istituzioni nazionali ed europee sul tema sta diventando sempre più intenso.

Per mettere finalmente in pratica quanto previsto dalle norme in materia, la sicurezza cibernetica è stata compresa tra i progetti finanziati dal Piano nazionale di ripresa e resilienza (PNRR), trasmesso dal Governo alla Commissione europea il 30 aprile 2021; il PNRR prevede al riguardo un piano di investimenti e riforme finalizzati allo scopo di mettere l'Italia nel gruppo di testa in Europa entro il 2026 (cd. Italia Digitale 2026).

All'investimento, volto alla creazione ed al rafforzamento delle infrastrutture legate alla protezione cibernetica del Paese e alla completa attuazione della disciplina prevista dal PSNC, sono destinati circa 620 milioni di euro di cui: 241 per la creazione di una infrastruttura per la cybersicurezza; 231 per il rafforzamento delle principali strutture operative del perimetro di sicurezza nazionale cibernetica PNSC; 15 per il rafforzamento delle capacità nazionali di difesa informatica presso il ministero dell'Interno, Difesa, Guardia di Finanza, Giustizia e Consiglio di Stato.

Importanti novità riguardano anche le organizzazioni incaricate di attuare la disciplina sulla sicurezza cibernetica e di svolgere le funzioni previste dalla stessa, tra le quali l'Agenzia Nazionale per la Cybersicurezza: dopo l'emanazione del d.l. 82/2021, convertito con L. 109/2021, con cui sono state definite nel dettaglio le sue funzioni e i suoi poteri di controllo, negli ultimi mesi del 2021 sono state messe in atto le operazioni necessarie alla sua messa in opera, tra cui la nomina del direttore generale (prof. Roberto Baldoni) e del vice direttore generale (dott.ssa Nunzia Ciardi), l'emanazione dei regolamenti interni, nonché il recente avvio della collaborazione con l'Autorità Garante per la privacy per lo scambio di informazioni e la promozione di buone pratiche di sicurezza cibernetica.

L'Agenzia Nazionale per la Cybersicurezza svolge inoltre un ruolo fondamentale riguardo il percorso di adozione del cloud da parte delle amministrazioni italiane: lo scorso 18 gennaio 2022, infatti l'Agenzia ha predisposto, in collaborazione con il Dipartimento per la trasformazione digitale, gli atti che definiscono le modalità per la classificazione dei dati e dei servizi pubblici e i requisiti per le tipologie di qualificazione dei servizi cloud della PA.

Infine è previsto l'assorbimento da parte dell'Agenzia Nazionale per la Cybersicurezza delle funzioni già svolte da AgID e dal Ministero per lo Sviluppo Economico.

Tra le più importanti funzioni che verranno trasferite vi sono quelle svolte dal CERT-PA, cioè la struttura responsabile per la conduzione e gestione delle attività operative e per il monitoraggio dello spazio cibernetico delle Pubbliche Amministrazioni.

Le ultime introduzioni normative non potevano non investire le procedure di acquisto di servizi ICT per la PA: in particolare l'art. 53 del d.l. 77/2021 (c.d. "Semplificazioni-bis"), rubricato "semplificazione degli acquisti di beni e servizi informatici strumentali alla realizzazione del PNRR e in materia di procedure di e-procurement e acquisto di beni e servizi informatici", prevede la semplificazione e l'accelerazione dei processi di approvvigionamento attraverso la creazione di una "white list" di fornitori certificati, la creazione di un percorso di "fast track", adottando un approccio semplificato per gli acquisti in ambito PNRR, e la creazione di un servizio che consenta una selezione/comparazione veloce e intuitiva tra i fornitori certificati.

Ci troviamo dunque in un periodo particolarmente ricco di novità in tema di sicurezza cibernetica, in cui è fondamentale approfondire le conoscenze tecniche e normative in materia, in modo da poter seguire "dal vivo" la messa in atto delle stesse, soprattutto in vista delle prossime scadenze previste dal PNRR.

3.2 Obiettivi e organizzazione

Lo scopo del PSNC è quello di dare una serie di regole a determinati enti che sono considerati parte integrante del sistema-paese in quanto forniscono determinati servizi che sono fondamentali e senza i quali lo Stato sarebbe danneggiato da un carattere civile, sociale o economico punto di vista. Concretamente, come affermato nel capitolo 1, un soggetto che fa parte del perimetro deve tenere un elenco delle risorse informatiche e comunicarlo all'autorità. In aggiunta a questo, ogni organizzazione appartenente al PSNC deve notificare ogni incidente all'autorità CSIRT . L'elenco degli enti aderenti al PSNC è aggiornato periodicamente dal Governo italiano con DPCM, secondo le indicazioni fornite dalle diverse amministrazioni del Comitato interministeriale per la sicurezza della Repubblica (CISR) che operano nel proprio ambito di competenza. L'ente preposto a garantire che gli enti del PSNC seguano le regole scritte nella normativa è il Centro di Valutazione e Certificazione Nazionale (CVCN), che è stato istituito dal ministro dello sviluppo economico e che ha anche il compito di condizionare e test hardware e software da integrare anche in collaborazione con le amministrazioni CISR. Se le varie obbligazioni non vengono adempiute dopo un certo tempo determinato l'ente può incorrere in varie sanzioni pecuniarie previste dalla legge.

4 COME SCEGLIERE LO STRUMENTO PIU ADATTO PER L'INVENTARIO DEGLI ASSET

Il numero di strumenti progettati per eseguire l'inventario degli asset è sempre più elevato e per questo motivo ci sono molte caratteristiche da valutare nella scelta del più adatto al contesto in cui l'inventario deve essere costruito. Per questo motivo in questo capitolo viene fornito un elenco di alcuni aspetti importanti che caratterizzano uno strumento di inventario degli asset.

- Controllo degli asset IT: poiché uno degli aspetti più importanti dell'inventario degli asset è avere una visione chiara degli asset nell'infrastruttura per facilitarne la gestione, è fondamentale che lo strumento scelto per fare l'inventario sia semplice da usare e progettato in modo che tutti gli elementi siano facilmente visibili;
- Configurabilità e personalizzazione: un altro aspetto fondamentale di uno strumento di inventario degli asset è la possibilità di personalizzarlo in base all'ambiente in cui lo strumento verrà utilizzato;
- Buona funzionalità di reportistica: questo punto è molto importante in quanto uno strumento che ha la capacità di riportare informazioni sugli asset raccolti permette di capire rapidamente se tutto funziona correttamente (ad esempio dal punto di vista della cybersecurity uno strumento può segnalare se un software è obsoleto, se un hardware ha avuto un malfunzionamento, ecc.).
- Costo: infine è importante valutare anche il prezzo richiesto per la soluzione, in relazione al contesto. Questo può includere il costo per la licenza dello strumento ma anche il supporto fornito.

In questo capitolo verranno presentate due soluzioni, la prima è open-source e gratuita mentre la seconda ha una versione di prova valida per un certo numero di asset inferiore a 100, mentre c'è un prezzo annuo da pagare che dipende dal numero di asset.

Queste panoramiche sui due strumenti permetteranno di comprendere il motivo alla base della scelta di una soluzione commerciale piuttosto che gratuita o viceversa a seconda dello scenario del caso.

4.1 Snipe-IT

Snipe-IT è un progetto open source gratuito (FOSS) sviluppato da Grokability basato su Laravel e realizzato per la gestione delle risorse IT [19]. È un software basato sul Web, deve essere eseguito su un server Web e accessibile tramite un browser Web. Tutto il codice del progetto è disponibile su Github[29], e il servizio è gratuito se self-hosted mentre ci sono diverse tipologie di abbonamento per quanto riguarda un piano hosted, e in quest'ultimo caso viene fornito anche il supporto tecnico completo.

Snipe-IT ha un'interfaccia grafica molto intuitiva (4.1) e il suo scopo è rendere il lavoro di inventario delle risorse il più semplice possibile. Gli asset che riempiono il database possono essere aggiunti manualmente o importati da un file csv o tramite una specifica API progettata appositamente per questo motivo. L'idea alla base di questo progetto è quella di sostituire i tipici fogli di calcolo che vengono spesso utilizzati anche nel campo dell'inventario delle risorse informatiche con qualcosa di più organizzato e in cui le varie informazioni possono essere facilmente accessibili e modificate al momento del bisogno.

Le funzionalità offerte da Snipe-IT sono numerose e questo è solo un breve elenco di ciò che offre questo strumento:

- Visualizza facilmente quali risorse sono assegnate e la loro posizione fisica
- I modelli di asset consentono di raggruppare caratteristiche comuni;
- Avvisi e-mail per garanzie e licenze in scadenza;
- Controllo delle risorse facile e veloce;
- Aggiungere campi personalizzati per ulteriori attributi delle risorse.

Tutte queste cose sono progettate pensando alla sicurezza. Per questo motivo vengono applicate molte funzionalità di sicurezza per mantenere i dati al sicuro, e in ogni caso poiché Snipe-IT gira su un server web che potrebbe essere self-hostato tutti i passaggi corretti per garantire un elevato livello di sicurezza sono spiegati nel manuale.

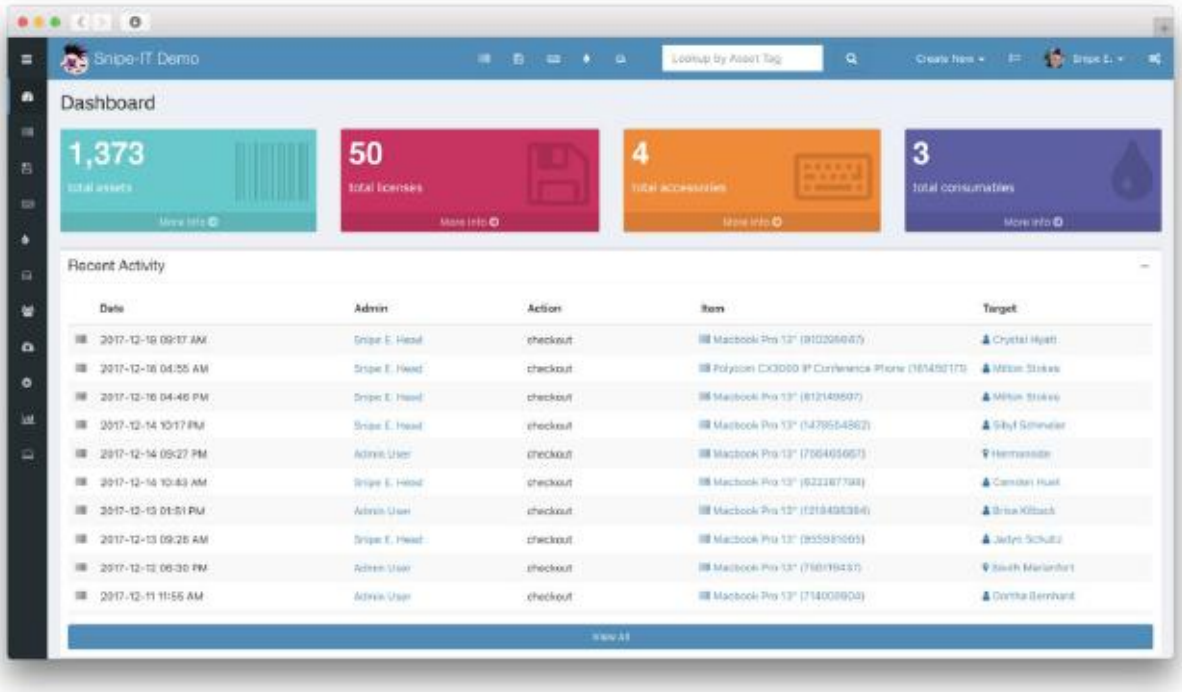

Figura 4.1. Interfaccia grafica Snipe-IT

4.2. Lansweeper

Lansweeper è uno strumento commerciale che consente di eseguire la scoperta e l'inventario degli asset sulla stessa piattaforma, senza la necessità di combinare strumenti diversi [10]. L'idea alla base di questo potente strumento è che tutti i dati delle risorse IT dovrebbero essere raccolti in un unico posto sotto un unico grande inventario delle risorse IT che aiuta l'organizzazione o l'azienda che utilizza questo strumento a tenere traccia di tutte le informazioni.

L'interfaccia è organizzata come in figura 4.2 e tutte le informazioni sull'asset vengono rilevate dagli strumenti, che a differenza di altri strumenti come il suddetto Snipe-IT ha una potente funzionalità integrata di rilevamento degli asset che può anche essere agentless, e quindi non necessita di qualsiasi installazione di software sul dispositivo su cui viene eseguita la scansione. È molto veloce e può rivelare molte informazioni sugli asset IT grazie all'uso di molti protocolli diversi come ad esempio SNMP, di cui si trova una breve descrizione nella sezione 2.2. Un'altra caratteristica interessante è la possibilità di scoprire di più su una risorsa, ad esempio informazioni sull'hardware o sull'archiviazione di una macchina specifica, semplicemente fornendo le credenziali di tale risorsa.

Questa caratteristica è davvero impressionante in quanto può essere sfruttata per eseguire una gestione completa del patrimonio, con tutte le informazioni che possono essere ritenute interessanti, e raccogliere tutto in un database facilmente consultabile e aggiornabile automaticamente con una scansione, anche programmabile da eseguire periodicamente

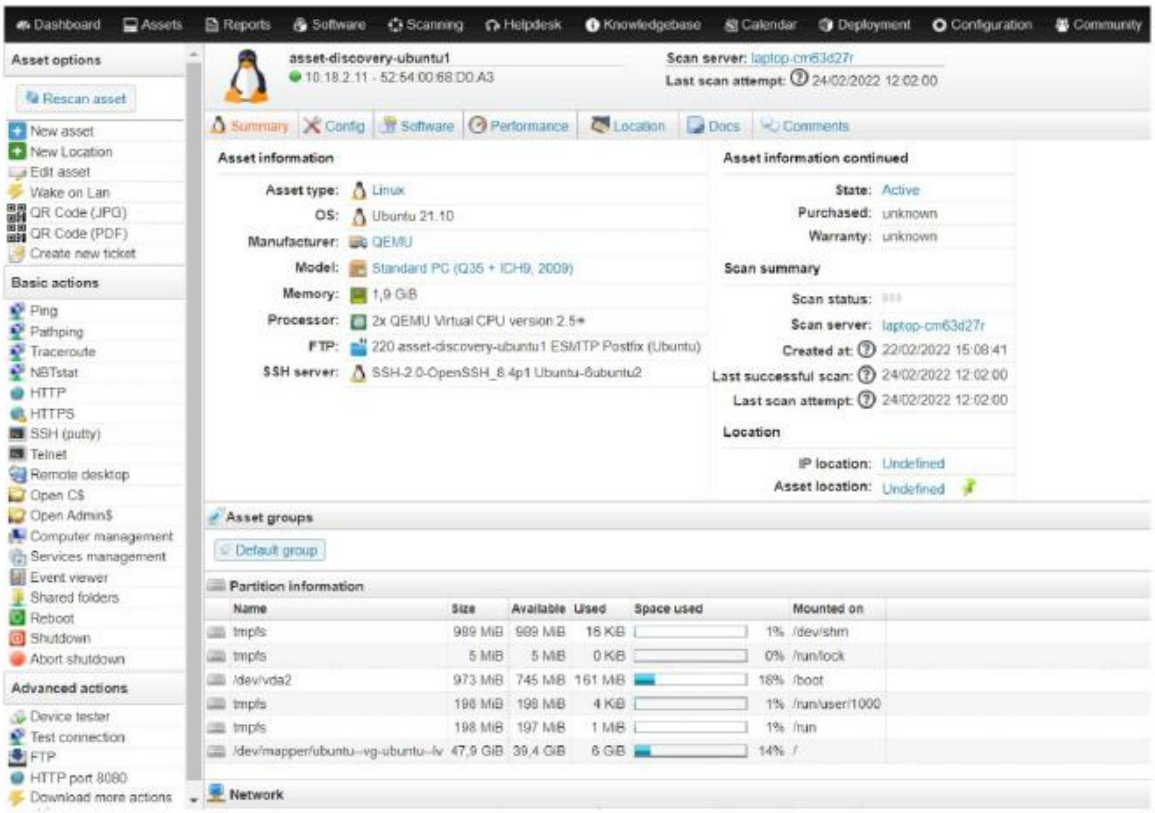

Figura 4.2. Interfaccia grafica di Lansweeper

Le risorse rilevate dallo strumento sono archiviate e organizzate in modo tale da poter essere aggiornate e verificate in qualsiasi momento. Viene data anche la possibilità di eseguire varie azioni sui dispositivi collegati alla rete, caratteristica interessante in quanto può essere sfruttata per controllare e organizzare una rete da un solo endpoint senza la necessità di agire fisicamente sul dispositivo. Inoltre se si vogliono aggiungere qualche informazione in più, oltre a quella scoperta dallo strumento stesso, il processo è semplice e veloce, e questo permette di avere un inventario completo dei dati che l'utente vuole associare ad un determinato bene.

Questa soluzione è potenzialmente molto simile al concetto di ciò che questa tesi si propone di fare, con l'importante inconveniente di non essere open-source e quindi il vero funzionamento viene spiegato solo in superficie e non c'è un'analisi approfondita delle caratteristiche del software. Oltre a questo il costo per l'implementazione di una tale soluzione, come molte altre

nel campo dell'asset management, può essere troppo alto per le aziende che non hanno molte risorse da spendere per mantenere un inventario di asset.

Questo va comunque visto in prospettiva anche del fatto che una soluzione di questo tipo permette di risparmiare ore di lavoro e di questo va tenuto conto quando un'azienda decide se utilizzare o meno questo tipo di strumenti.

5 SVILUPPO DEGLI STRUMENTI

In questo capitolo viene descritto il lavoro svolto per sviluppare lo strumento, spiegando i vari approcci e le ragioni alla base di essi. Prima dell'illustrazione effettiva dei passaggi effettuati nel processo di creazione dello strumento, viene fornita una breve descrizione dell'ambiente di test.

5.1 Ambiente

L'idea alla base della tesi è quella di creare un banco di prova che sia il più completo possibile e che permetta di ricreare uno scenario che eventualmente si può trovare in una pubblica amministrazione o in un'azienda nel processo di gestione degli asset.

Per questo motivo il lavoro svolto nella creazione dell'ambiente è stato quello di allestire un insieme eterogeneo di macchine che simulassero una possibile configurazione di rete presente in una amministrazione o in una azienda. Per fare ciò sono state sfruttate due soluzioni che condividevano lo stesso concetto cardine comune: la virtualizzazione.

5.1.1 Soluzione Oracle VM VirtualBox

La prima soluzione era basata sull'utilizzo di una macchina host Windows 10 con Oracle VM VirtualBox1 installato e una raccolta di varie macchine virtuali con diversi sistemi operativi.

Oracle VM VirtualBox[1] è un prodotto di virtualizzazione gratuito che offre molte funzionalità e possibilità quando si tratta di costruire e supportare l'esecuzione di macchine virtuali. Con questo software è possibile costruire un'intera rete tra le macchine virtuali in esecuzione grazie all'utilizzo di un adattatore di rete virtualizzato e alla funzionalità data da VirtualBox di creare una rete NAT virtuale, con indirizzi IP privati assegnati alle macchine virtuali ad essa collegate, che è completamente indipendente dal reti esterne ma ha accesso a Internet come mostrato nella figura 5.1.

[1] https://www.virtualbox.org/

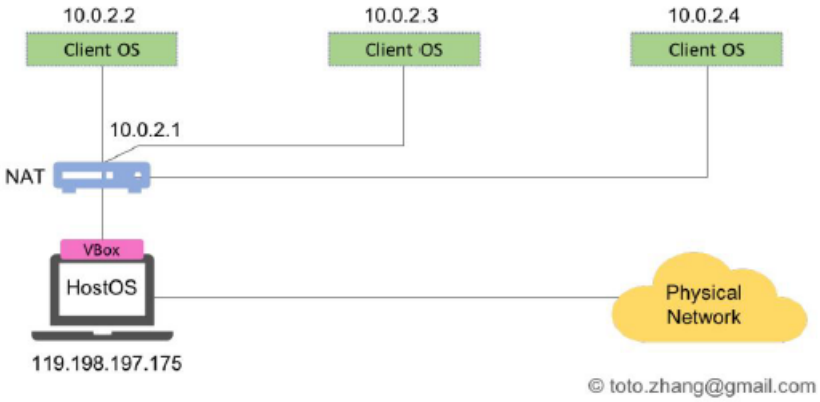

Figura 5.1. Rappresentazione dell'opzione di rete Virtual Box NAT

L'ambiente di lavoro era composto da una macchina virtuale principale con Kali Linux2[2] installato, che aveva più risorse allocate ed era la fonte di tutti i processi di test e di individuazione delle risorse di rete. Kali Linux è stato scelto perché è un sistema operativo pensato per attività di sicurezza come il network discovery o più in generale il penetration testing di ogni tipo.

Le funzionalità offerte da un sistema operativo come Kali Linux sono molte e la scelta è ricaduta su di esso anche perché viene offerto un ottimo manuale e le funzioni di network asset discovery sono ben documentate. Il resto dell'ambiente di test era formato da altre sei macchine virtuali con diversi sistemi operativi scelti in quanto ragionevolmente leggeri in termini di utilizzo delle risorse, e questo era importante per garantire che le prestazioni dell'intero sistema non venissero sminuite, e aveva diversi sistemi operativi e configurazioni in esecuzione (ad es. porte aperte, applicazioni installate, ecc.) e questo ha portato a un ambiente di test più completo.

5.1.2 Virtualizzazione del server remoto

L'idea alla base dell'introduzione di questa seconda soluzione è stata quella di creare un ambiente ancora più rappresentativo di una possibile infrastruttura di rete di un'azienda che deve svolgere attività di asset management. In questo caso le macchine virtuali utilizzate sono state allestite su un server e vi si accedeva tramite un tunnel VPN realizzato con Wireguard[3]. Il vantaggio di questo tipo di soluzione era che c'erano più risorse allocate per la creazione

[2] https://www.kali.org/
[3] https://www.wireguard.com

dell'ambiente, fatto che permetteva di lavorare con meno problemi di stabilità, e in generale questo tipo di allestimento era più adatto al contesto di lavoro che questa tesi intendeva.
La rete virtuale era composta da sei istanze di Ubuntu Server[4] in particolare nella sua versione 21.10, basata su Linux Kernel 5.13. Come nella soluzione precedente, è stata inclusa una macchina virtuale con più risorse allocate con l'idea di utilizzare questa macchina principale per eseguire lo strumento sviluppato ed eseguire il rilevamento delle risorse di rete sull'altra macchina virtuale della rete.
Tutte le operazioni sono state eseguite tramite SSH e sulle varie macchine un lavoro preliminare di installazione di servizi e applicazioni in modo che queste macchine potessero simulare in modo realistico il lavoro di un server.

5.2 Ragioni e panoramica

Per comprendere meglio le scelte attuative è importante rimarcare l'obiettivo alla base del lavoro svolto in questa tesi. L'obiettivo è la creazione di uno strumento che possa facilitare il processo di gestione degli asset, standardizzandolo e cercando di automatizzare la maggior parte dei passaggi in modo che nell'utilizzo dello strumento sia richiesto poco lavoro e nessuna conoscenza particolare. Tutte le procedure descritte in questa sezione sono progettate tenendo presente questo concetto. Il risultato finale del lavoro è uno script automatizzato scritto in bash che sfrutta la funzionalità di Nmap e chiama internamente un altro programma scritto in Python. I risultati dello script vengono quindi raccolti e rappresentati attraverso l'uso di Neo4J, un programma che verrà presentato e descritto più avanti in questo capitolo.

5.3 Scoperta delle risorse

Il primo passo fatto nelle ricerche per questa tesi è stato quello di utilizzare uno strumento di rilevamento per raccogliere la maggior parte delle informazioni sull'asset attraverso una scansione della rete. Lo strumento scelto per eseguire questa scansione, come accennato in precedenza, è Nmap. La scelta è stata dettata da molteplici ragioni, tra queste sicuramente figurano:

- Semplicità dei comandi, insieme alle varie opzioni che consentono di essere più veloci, più furtivi o di effettuare analisi più approfondite a seconda del contesto in cui viene utilizzato lo strumento;

[4] https://ubuntu.com/server

- Buona leggibilità dell'output e facile manipolazione. Infatti Nmap offre diversi formati di output incluso XML, che è molto utile quando si tratta di eseguire l'analisi del software. Un esempio di un tipico output di Nmap è fornito nella figura 5.2;
- Leggerezza e portabilità. Nmap è disponibile su tutti i principali sistemi operativi e richiede pochissime risorse per funzionare, e questo lo rende un ottimo strumento per l'obiettivo perseguito in questa tesi.

Una volta scelto lo strumento per eseguire il rilevamento delle risorse, il passaggio successivo è stato decidere quale opzione utilizzare per eseguire la scansione della rete.

Poiché l'obiettivo del progetto è quello di trovare tutte le informazioni possibili, la scelta è ricaduta su una scansione aggressiva che includeva tutte le funzionalità più preziose offerte da Nmap scan, ovvero rilevamento del sistema operativo, rilevamento della versione, scansione degli script e tracer out. L'idea alla base di questa scelta è che la persona che utilizza uno strumento come quello proposto da questa tesi stia lavorando in modo specifico per ottenere informazioni dalle varie macchine che compongono la rete e non ha alcun interesse a essere eventualmente scoperto, e quindi non ha bisogno di eseguire un'operazione più furtiva ma anche scansione meno efficace.

A questo punto si deciso lo strumento di individuazione della rete, la fase successiva è stata la creazione dello script responsabile dell'esecuzione della scansione. Il codice è molto semplice e infatti gli unici compiti che vengono eseguiti dallo script sono:

- Eseguire una scansione Nmap della rete con l'opzione summenzionata sull'IP di destinazione specificato come argomento durante l'esecuzione dello script

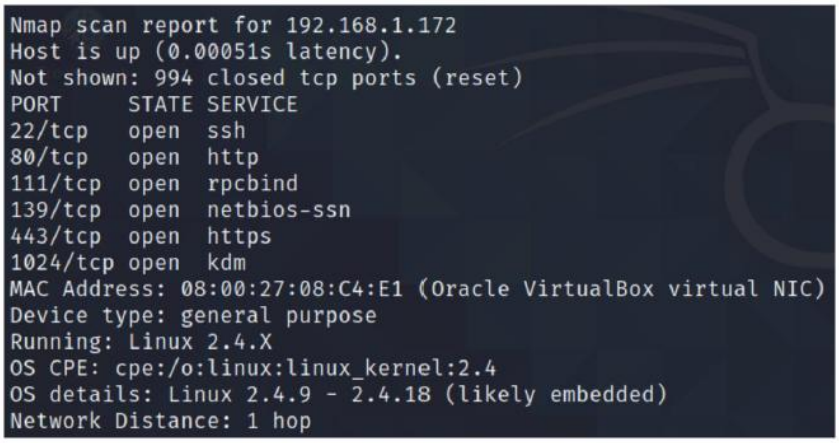

Figura 5.2. Una tipica scansione Nmap

Un esempio dell'uso dello script e dell'output prima della scansione effettiva può essere visto in figura 5.3;

- Memorizzare i risultati della scansione in un file XML;
- Passare il file ottenuto al programma scritto in Python che è responsabile dell'analisi dell'output in un file CSV che sarà necessario nella fase successiva dello sviluppo.

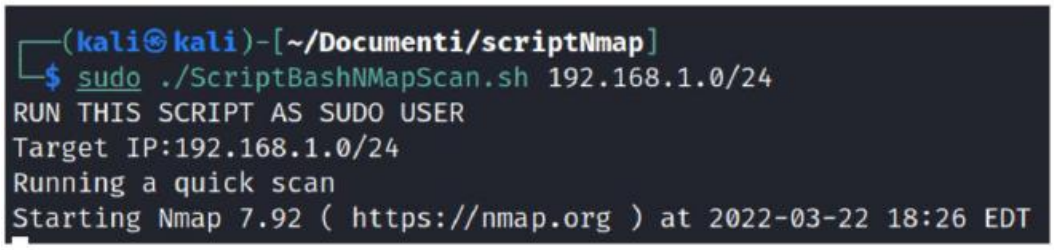

Figura 5.3. Uso dello script sviluppato

Dopo aver eseguito lo script si ottengono tre nuovi file:

1. L'output della scansione in formato XML prodotto da Nmap, è abbastanza dettagliato e contiene molte informazioni non rilevanti per lo scopo di questa tesi;
2. Un secondo file XML contenente i dati salienti estratti dal file Nmap. Queste informazioni sono: IP (versione 4 e versione 6 se presente) e indirizzi MAC, porte aperte e servizi che sfruttano tali porte e la versione del sistema operativo se Nmap è riuscita a indovinarla correttamente. Queste informazioni sono divise per host e un esempio dell'output può essere visto nella figura 5.4;
3. Il file CSV contenente le stesse informazioni del suddetto file che sarà utilizzato nella fase di inventario dei beni.

Al termine di questa fase tutto il lavoro relativo alla scoperta degli asset di rete è completato e l'output prodotto può quindi essere utilizzato nella fase di inventario degli asset che verrà descritta nella sezione successiva.

5.4 Inventario dei beni

La seconda parte del progetto sviluppato in questa tesi consiste nel manipolare i dati ottenuti durante la fase di scoperta degli asset e ottenerne una rappresentazione grafica. Per eseguire questa attività ci sono molte opzioni praticabili. Nella progettazione di questo progetto la scelta è ricaduta sull'utilizzo di un software che permettesse di ottenere una bella rappresentazione grafica anche se dal punto di vista pratico avrebbero potuto essere interessanti anche altre possibilità da esplorare.

5.4.1 Neo4J

Il software che è stato scelto come il più adatto nell'ambito della tesi per raccogliere e gestire le informazioni sull'asset è Neo4J5[5]. Questo software non è propriamente uno strumento di inventario delle risorse. In effetti, il Neo4J è primario

```
<host5>
  <addresses>
    <address name="192.168.1.172" addrtype="ipv4" />
    <address name="08:00:27:08:C4:E1" addrtype="mac" />
  </addresses>
  <ports>
    <port name="22" state="open" service="ssh" />
    <port name="80" state="open" service="http" />
    <port name="111" state="open" service="rpcbind" />
    <port name="139" state="open" service="netbios-ssn" />
    <port name="443" state="open" service="https" />
    <port name="1024" state="open" service="status" />
  </ports>
  <os>
    <osmatch name="Linux 2.4.9 - 2.4.18 (likely embedded)" />
  </os>
</host5>
```

Figura 5.4. Esempio del file XML prodotto dopo l'analisi

Figura 5.5. *Logo Neo4J*

una piattaforma di dati grafici e offre molte funzionalità relative alla memorizzazione e alla gestione dei dati.

Al centro della piattaforma grafica Neo4J c'è un database che è fatto in modo tale che i dati siano collegati mentre vengono archiviati, consentendo query molto potenti.

Questo database deve essere ospitato e la piattaforma Neo4J offre un servizio cloud che consente di utilizzare liberamente un database per piccoli progetti. In aggiunta a questo viene fornito uno strumento chiamato Neo4J Desktop che permette di creare, lavorare e gestire database locali. Una caratteristica interessante di questo software è la possibilità di interagire con il contenuto del database tramite query scritte in un linguaggio chiamato Cypher e ottenere una rappresentazione grafica dei dati recuperati con la query. Quest'ultima caratteristica è

[5] https://neo4j.com

quella che è stata sfruttata nello sviluppo del progetto per questa tesi e nella sezione successiva viene fornita una breve spiegazione del lavoro svolto.

5.4.2 Attuazione

In questa fase finale di sviluppo dello strumento il punto di partenza sono le informazioni raccolte nella fase di scoperta degli asset. Con questi dati l'obiettivo è creare una mappa della rete e per ogni endpoint aggiungere le proprietà che sono state scoperte nella prima fase. Per fare ciò è stata scritta una query Cypher molto semplice, come si può vedere in figura 5.6 che ha il compito di associare un id ad ogni nodo e quindi impostare le varie proprietà se presenti. Il risultato finale sarà mostrato come risultato nel prossimo capitolo di questa tesi.

```
//Load with everything as property
LOAD CSV WITH HEADERS FROM 'file:///csvParsedOutput.csv' AS row
MERGE (e:Endpoint {endpointId: row.id, ipv4: coalesce(row.ipv4,NULL)})
SET e.ipv6 = CASE trim(row.ipv6) WHEN "" THEN null ELSE row.ipv6 END
SET e.mac = CASE trim(row.mac) WHEN "" THEN null ELSE row.mac END
SET e.ports = CASE trim(row.ports) WHEN "" THEN null ELSE row.ports END
SET e.services = CASE trim(row.services) WHEN "" THEN null ELSE row.services END
SET e.os = CASE trim(row.os) WHEN "" THEN null ELSE row.os END
WITH e
UNWIND split(row.network, ':') AS endpoint
MATCH (e1:Endpoint {endpointId: endpoint})
MERGE (e)-[r:IS_IN_THE_NETWORK_WITH]-(e1)
```

Figura 5.6. La query *Cypher* che carica l'asset

Nella soluzione finale vengono caricate come proprietà le caratteristiche associate ai vari asset, e questo significa che per ogni nodo del grafico saranno presenti varie etichette che lo descrivono. Inoltre le connessioni sono rappresentate nel grafico come frecce unidirezionali poiché questo è un limite di un'implementazione fatta in un software come Neo4J che non è propriamente destinato a creare una mappa di rete. Comunque l'importante aspetto positivo di tale soluzione è la sua rapidità e immediatezza, che consentono all'utente che ha appena eseguito una scansione e poi inserito le informazioni ottenute nel database di vedere una rappresentazione grafica della rete e della connessione tra i dispositivi.

6 RISULTATI E DISCUSSIONE

Questo capitolo si concentra sui risultati ottenuti con lo sviluppo di questa tesi, insieme alle caratteristiche principali della soluzione implementata.

6.1 Risultati ottenuti

La soluzione implementata in questa tesi ha l'obiettivo di migliorare e rendere più agevole il processo di asset management sfruttando l'utilizzo di strumenti già esistenti. I risultati raggiunti vanno in quella direzione e qui sono elencate alcune delle caratteristiche che lo strumento sviluppato ha e può aiutare nel contesto in cui questa tesi si è inserita:

- Semplicità di funzionamento. Il codice sviluppato in questa tesi è pensato per essere utilizzato in contesto con molte macchine e dispositivi collegati nella stessa rete, ma l'utilizzo dello strumento è semplice e non richiede la lettura di troppa documentazione;
- Automazione del processo. Un punto che è stato sempre presente durante lo sviluppo di questa tesi è stato quello di cercare di realizzare uno strumento che fosse il più possibile autonomo e questo si riflette nella soluzione finale che non necessita di particolare lavoro da parte dell'utilizzatore dello strumento;
- Rappresentazione grafica. L'utilizzo dello script sviluppato in combinazione con l'applicazione Neo4J Desktop e la query Cypher fornita nella sezione 5.4.2 consente di avere un prodotto finale facilmente leggibile e personalizzabile. Un esempio può essere visto nella figura 6.1.

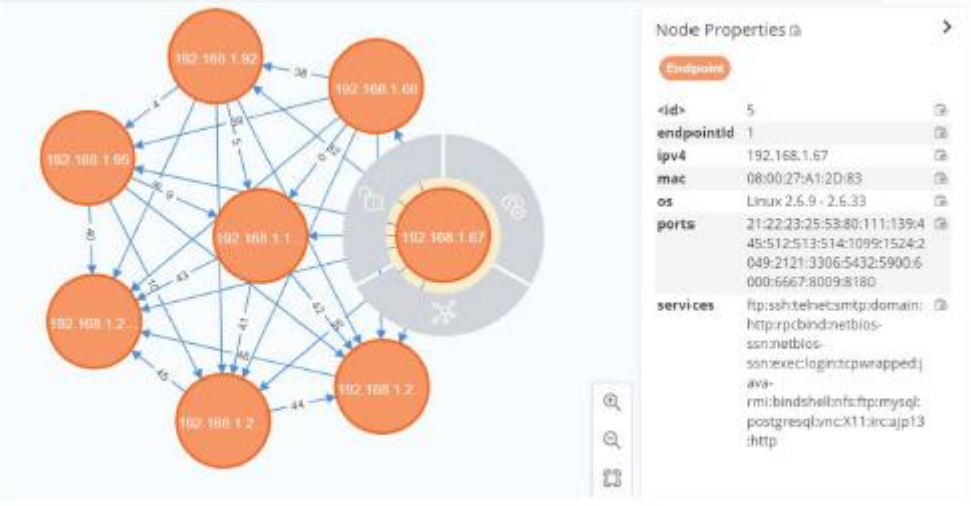

Figura 6.1. La rappresentazione grafica ottenuta in Neo4J

Il risultato finale è uno strumento molto semplice che dà all'utente la possibilità di vedere alcune delle caratteristiche dell'asset nella rete in modo molto semplice senza la necessità di conservare fogli di calcolo o altro tipo di documentazione per elencare gli asset, che può necessitano di lavoro extra e soprattutto la procedura è pericolosa poiché è difficile ottenere informazioni in tempo reale su un bene in determinati contesti.

6.2 Ragioni alla base delle scelte progettuali

Questo tipo di soluzione è difficile da testare e descrivere con un parametro misurabile, perché ci sono più variabili che possono influenzare l'esecuzione dello script e lo strumento nel suo insieme. Un parametro che può essere preso in considerazione per una misurazione quantitativa delle prestazioni è il tempo necessario per eseguire la scansione Nmap, che è sicuramente la fase più dispendiosa in termini di tempo nell'implementazione dello strumento proposto in questa tesi.

Più che una vera e propria valutazione della performance, che come spiegato prima è difficile da ottenere anche con un certo grado di approssimazione, in questa sezione viene fornita una considerazione sul tipo di scansione in relazione al tempo necessario per eseguirla.

La scansione Nmap che viene eseguita, come descritto nella sezione 5.3, è una scansione di rete aggressiva e completa. Ciò significa che anche per una piccola rete può eventualmente richiedere molto tempo. Nell'ambito di questa tesi, comunque, questo non è mai stato un problema poiché il numero di macchine da scoprire e analizzare nella rete era piuttosto ridotto rispetto a quello che potrebbe richiedere un contesto reale. Ma questo potrebbe rivelarsi uno svantaggio in determinati ambienti, quindi una possibile soluzione è utilizzare un tipo di scansione più leggero che potrebbe essere meno preciso ma più veloce.

In ogni caso la soluzione adeguata deve basarsi sul contesto reale, ma per questo è importante sapere che è possibile continuare a utilizzare lo strumento e basta applicare alcune piccole modifiche per arrivare a un compromesso tra prestazioni e affidabilità.

7 CONCLUSIONI

In sintesi, in questa tesi è stato affrontato il problema dell'utilizzo di strumenti di asset discovery a supporto di un inventario di cybersecurity e gran parte del contributo è stato orientato allo studio delle varie tecniche e strumenti disponibili in questo campo. Il lavoro svolto ha mostrato come questo mondo sia vasto e ci siano molte soluzioni commerciali che cercano di rispondere a questo problema, ma non c'è qualcosa che possa essere considerato standard e che possa essere universalmente utilizzato. Infatti nella maggior parte dei casi ogni azienda sviluppa o utilizza software o strumenti che possono differire in molti modi l'uno dall'altro. Per questo motivo è molto difficile immaginare un modo standard di effettuare l'inventario degli asset e questo diventa un problema in un contesto come quello del PSNC, in cui viene richiesto all'ente di raccogliere e inviare periodicamente l'elenco degli asset nel proprio possesso.

Il lavoro svolto in questa tesi cerca di colmare questa lacuna con una soluzione che aspira ad essere un esempio di ciò su cui la ricerca potrebbe cercare di concentrarsi. Lo strumento sviluppato è molto semplice e non è pronto per essere utilizzato in un contesto più complesso, ma la parte cruciale di questo lavoro è che pone le basi per uno studio più complesso che deve essere svolto in questo campo che ha ancora molto da fare offrire e da scoprire. In ogni caso la soluzione che questa tesi propone è utile per comprendere il flusso di lavoro da seguire nello sviluppo di uno strumento di asset management e quali sono i vantaggi di costruire un inventario di cybersecurity forte e sicuro.

In conclusione, l'obiettivo iniziale del lavoro può considerarsi solo parzialmente risolto in quanto la ricerca ei risultati che questo documento offre possono essere la base per più progetti orientati in questo vasto campo. È interessante notare che un primo impiego di risorse finalizzato a trovare una buona soluzione a questo problema si tradurrebbe poi in un'importante riduzione dei costi futuri e soprattutto un risultato finale più sicuro. Per questo motivo nella sezione successiva viene presentato un elenco di miglioramenti futuri e possibili nuove soluzioni.

BIBLIOGRAFIA

[1] Matthew P Barrett et al. «Quadro per il miglioramento della sicurezza informatica delle infrastrutture critiche versione 1.1». In: (2018).

[2] Consiglio per gli standard di sicurezza PCI. *Linee guida per la valutazione del rischio PCI DSS 1.0a* *https://www.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf* 2012.

[3] The Art of Port Scanning - by Fyodor https://nmap.org/nmap_doc.html. 1997.

[4] Gordon Fëdor Lione. *Scansione di rete Nmap: https://nmap.org/book/man.html* .

[5] Guarnaccia. *Il valore aggiunto dell'asset inventory come elemento cen trale di un'azienda.* https://www.ettoreguarnaccia.com/archives/ 3796. 2016.

[6] Hardaker. Transport Layer Security (TLS) Transport Model for the Sim-ple Network Management Protocol (SNMP). RFC 6353. RFC Editor, July 2011. url: https://www.rfc-editor.org/rfc/rfc6353.txt.

[7] IT Governance Insitute. Cobit 4.1 Framework.. https://www.bauer.uh.edu/parks/cobit_4.1.pdf. 2007.

[8] ISO/IEC. ISO/IEC 27001:2013 Information technology — Security tech-niques — Information security management systems — Requirements. https://www.iso.org/isoiec-27001-information-security.html 2013.

[9] Jones. An Introduction to Factor Analysis of Information Risk (FAIR). *https://www.yumpu.com/en/document/view/7271140/an-introduction-to-factor-analysis-of-information-risk-fair* . 2006.

[10] *Sito web di Lansweeper.* https://www.lansweeper.com.

[11] *Legge 18 novembre 2019, n.133 "Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica"* https://www.gazzettaufficiale.it/eli/id/2019/11/20/19G00140/sg 2019.

[12] Schmidt Mauro. Essential SNMP 1st edition. O'Reilly, 2001.

[13] NIST. Security and Privacy Controls for Information Systems and Or-ganizations. https://nvlpubs.nist.gov/. 2020.

[14] *Nmap Host Discovery.* https://nmap.org/book/man-host-discovery.html

[15] *Nmap OS Discovery..* https://nmap.org/book/osdetect.html.

[16] *Nmap Altre piattaforme.* https://nmap.org/book/inst-other-platforms.html.

[17] *Scansione porta Nmap.* https://nmap.org/book/man-port-scanningTechniques.html.

[18] *Motore di script Nmap.* https://nmap.org/book/nse.html.

[19] *Documentazione Snipe-IT.* https://snipe-it.readme.io/docs.

[20] *Github Snipe-IT.* https://github.com/snipe/snipe-it.