PantherCrypt

PROGETTO FIREWORKS PER RETE THETA

www.hackme.com

ABOUT US

PantherCrypt è un team di giovani professionisti composto da otto specialisti, dedicati a fornire soluzioni di sicurezza informatica avanzate per aziende leader in diversi settori. La nostra forza risiede nella sinergia tra i nostri team di esperti in reti e software, un approccio collaborativo che ci permette di affrontare le sfide più complesse con efficacia e precisione.

INDICE

PantherCrypt

INDICE

www.hackme.com

VISION AND MISSION

Vision

La nostra visione è quella di costruire un ecosistema digitale robusto e affidabile, dove la sicurezza delle informazioni non è un ideale, ma una realtà concreta. Ci impegniamo a proteggere i dati dei nostri clienti con soluzioni di sicurezza all'avanguardia, anticipando e neutralizzando le minacce informatiche in continua evoluzione

Mission

In un mondo in cui le violazioni dei dati possono causare danni irreparabili, PantherCrypt si pone come un partner affidabile, garantendo la protezione dei patrimoni informativi aziendali. Aspiriamo a diventare un punto di riferimento nel settore della sicurezza informatica, offrendo soluzioni robuste e personalizzate che consentano ai nostri clienti di operare in un ambiente digitale sicuro e protetto.

TEAM DI RETE

Diego Turturo

Lorenzo Piccari

Manuel Pavia

Cristian Pezzella

TEAM DI SOFTWARE

Ettore Njah

Luca Tavani

Salvatore La Pira

Samuele Esposito

PRESENTAZIONE E OBIETTIVI

- La compagnia Theta, leader nel settore sviluppo software, ha incaricato il nostro team di sviluppare un progetto completo per l'aggiornamento e l'ottimizzazione della propria infrastruttura IT. Consapevoli dell'importanza cruciale di una rete efficiente e sicura per le operazioni aziendali, Theta si è rivolta a noi per una soluzione che risponda alle loro specifiche esigenze di crescita e sicurezza.

- Il presente documento ha lo scopo di fornire a Theta un quadro dettagliato del progetto di rete proposto, comprensivo di un preventivo di spesa accurato e di una descrizione tecnica approfondita. L'obiettivo è quello di presentare una soluzione che non solo soddisfi i requisiti attuali, ma che sia anche scalabile e adattabile alle future esigenze dell'azienda.

OBIETTIVI

- Presenza di 121 computer
- Un web server
- NAS (implica un elevato traffico di rete)
- Firewall perimetrale e di sistemi IDS/IPS.
- Server DMZ (isolato dal resto della rete)
- Un router che gestisce le connessioni tra le varie LAN
- DHCP centralizzato
- Crittografia dei dati sensibili.

ANALISI

Presenza di 121 computer, un web server, e un NAS implica un elevato traffico di rete. L'implementazione di un firewall perimetrale e di sistemi IDS/IPS.
Le considerazioni sulla sicurezza includono:

- L'implementazione di politiche di accesso rigorose per il firewall e il NAS.
- La configurazione sicura del web server per prevenire vulnerabilità note.
- L'implementazione di sistemi di autenticazione forte e la crittografia dei dati sensibili. Sarà necessario condurre regolari valutazioni di vulnerabilità e test di penetrazione per identificare e mitigare eventuali debolezze nella rete."

La sicurezza della rete è una priorità assoluta per Theta. È quindi cruciale valutare accuratamente le esigenze di larghezza di banda per garantire prestazioni ottimali. Fattori da considerare includono:

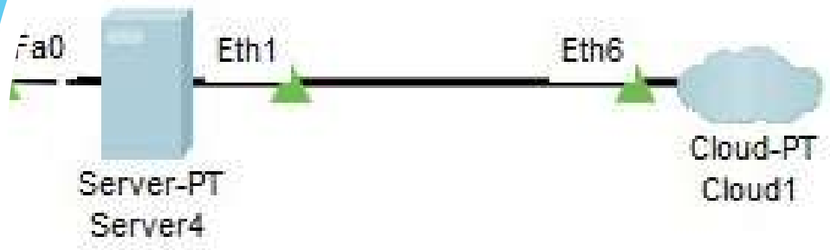
- Il tipo di applicazioni utilizzate dagli utenti (es. applicazioni di grafica, videoconferenze, ecc.).
- Il volume di dati trasferiti verso e dal NAS.
- Il traffico generato dal web server.
- Sulla base di queste valutazioni, sarà necessario dimensionare adeguatamente i dispositivi di rete (switch, router) e le connessioni Internet per evitare colli di bottiglia e garantire una rete reattiva."

PROGETTAZIONE RETE

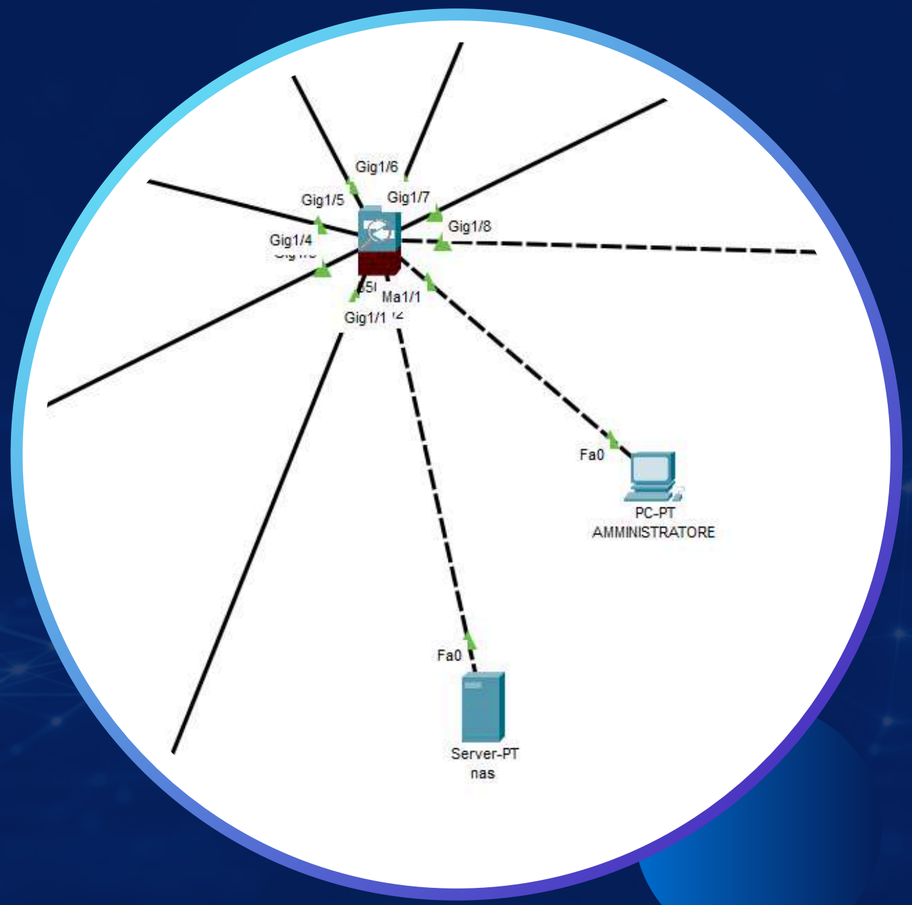
Struttura di rete

- Internet (rappresentato da nuvola): modem che consente la navigazione in Internet

- Server esterno: questo ha la funzione di DMZ e DNS
  - DNS: domain Name server, utile per la ricerca di un IP partendo da un URL esempio www.theta.com, da questo testo avremo la possibilità di risalire all'IP del server
  - DMZ: demilitarized zone, sottorete separata dalla rete interna, questa contiene server e servizi che sono accessibili da Internet fungendo allo stesso tempo da cuscinetto per proteggere la rete interna dalle minacce esterne.



PROGETTAZIONE RETE

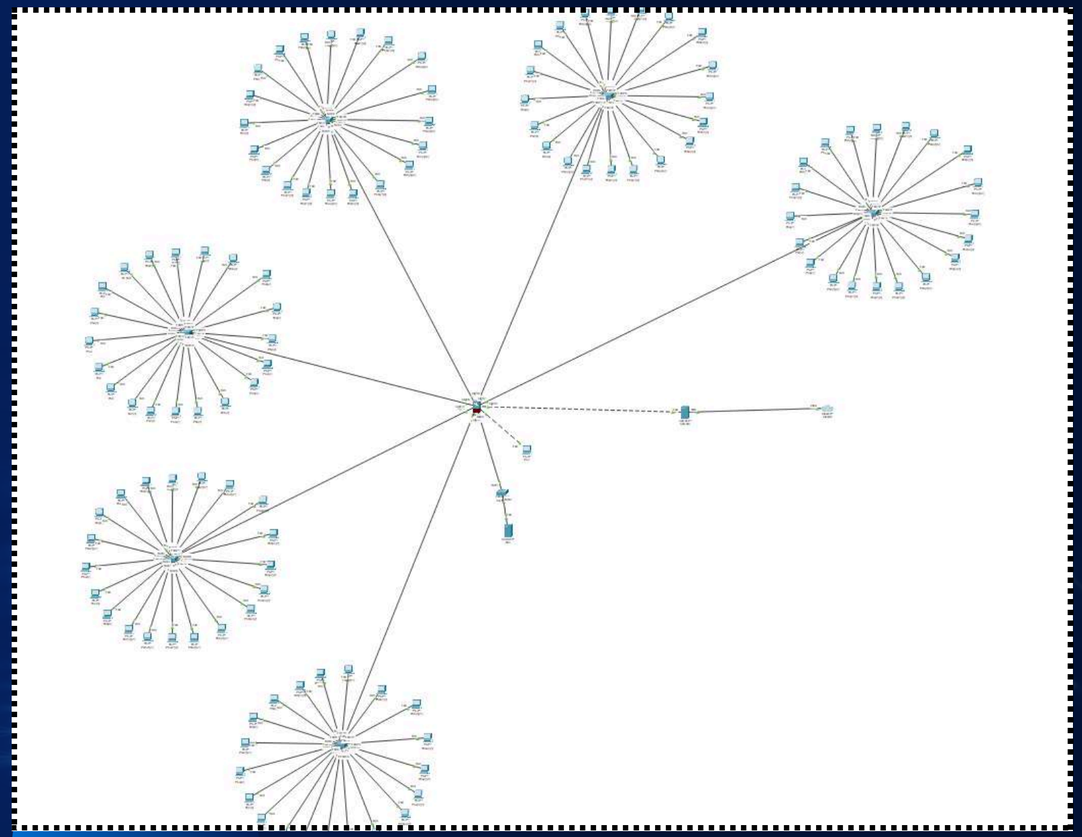


- Firewall centrale: Firewall multifunzione, quest'ultimo possiede diverse funzioni tra cui (router, firewall e DHCP)
  - Router: instradamento del traffico, connessione tra reti
  - Firewall: filtraggio comunicazione dell'azienda tramite delle regole impostate dal team di programmazione (filtro)
  - DHCP: funzione che permette l'assegnazione automatica degli IP di rete. N.B: ogni piano possiede una Pool di indirizzi IP dedicati.

PROGETTAZIONE RETE

- Server NAS: server utilizzato per l’archiviazione condivisa di dati.
- Switch: gli switch hanno la funzione di distribuire fisicamente le LAN.

Pc: utilizzati dagli operatori per svolgere le loro attività lavorative. N.B: i pc sono predisposti per avere poche porte hardware che permettano eventuali installazioni di driver esclusivamente per dispositivi come mouse e tastiera; tutto ciò è fatto per evitare attacchi simulando White box.



PROGETTAZIONE SOFTWARE

La progettazione Software consiste nell'applicare le regole software che permettono o negano l'accesso ad IP conosciuti o sconosciuti, preventivamente può essere aggiunto un registro con IP malevoli noti

REGOLE:

- L'amministratore può comunicare con tutti i piani ma nessuno ha la possibilità di comunicare con lui.
- Le pool di IP sono indirizzate in base al piano in cui si trovano i dispositivi (piano_1 - 192.168.11.0, piano_2 - 192.168.12.0...)
- Tutti i dispositivi comunicano con l'esterno (internet)
- I dati in ricezione vengono filtrati dal FIREWALL per verificare non ci siano dati malevoli (i dispositivi esterni possono soltanto rispondere a richieste effettuate dai dispositivi nella rete interna)

PROGETTAZIONE SOFTWARE

REGOLE:

- I dispositivi di un piano non hanno la possibilità di instradare dati ad altri piani
- Protocolli permessi: DHCP, HTTPS, FTPS, TCP, UDP, ICMP (regolabili in base alle esigenze del cliente)

  - DHCP: è un protocollo che assegna automaticamente indirizzi IP e altre informazioni di rete ai dispositivi, senza richiedere configurazione manuale.
  - HTTPS: è una versione sicura di HTTP che cripta i dati tra il browser e il client per proteggerli.
  - FTPS: è una versione sicura di FTP che utilizza la crittografia tramite SSL/TLS per proteggere i dati durante il trasferimento tra client e server.
  - TCP: è un protocollo che garantisce una trasmissione affidabile dei dati tra due dispositivi, assicurando che arrivino correttamente e nell'ordine giusto.

```
%SYS-5-CONFIG_I: Configured from console by console
show access-list
Extended IP access list 105
    10 permit tcp any any established
    20 permit icmp any any echo-reply
    30 permit udp any any gt 1023
    40 deny ip any any
    50 permit udp any any gt 1
Standard IP access list 10
    10 permit host 192.168.20.30
    20 deny any

Router#
```

PROGETTAZIONE SOFTWARE

REGOLE:

- UDP: è un protocollo veloce che invia dati senza garantire affidabilità o ordine.
- ICMP: (Internet Control Message Protocol) è un protocollo utilizzato per inviare messaggi di errore e informazioni diagnostiche sulla rete, come nel caso del comando "ping" per verificare la connessione.

```
%SYS-5-CONFIG_I: Configured from console by console
show access-list
Extended IP access list 105
    10 permit tcp any any established
    20 permit icmp any any echo-reply
    30 permit udp any any gt 1023
    40 deny ip any any
    50 permit udp any any gt 1
Standard IP access list 10
    10 permit host 192.168.20.30
    20 deny any

Router#
```

PREVENTIVO DI SPESA

L'azienda Theta ha richiesto un'infrastruttura IT completa, comprendente dispositivi di rete, computer client, software, installazione, configurazione e manutenzione. Questo documento presenta un preventivo dettagliato suddiviso in tre fasce di prezzo (bassa, media e alta), offrendo soluzioni adatte a diverse esigenze di budget e prestazioni. Le configurazioni proposte includono hardware e software di qualità, garantendo sicurezza, affidabilità e scalabilità nel tempo.

Costi dispositivi di rete

Fascia Bassa
- Switch (7 unità - TP-Link TL-SG1024D): 350 € (50 € ciascuno)
- Firewall (1 unità - Fortinet FortiGate 30E): 600 €
- NAS (1 unità - Synology DS220j): 400 €
- Server (2 unità - Dell PowerEdge T40): 2.500 € (1.250 € ciascuno)
- Modem (1 unità - Mikrotik RB4011iGS+5HacQ2HnD-IN): 250€

Totale dispositivi di rete: 4.100 €

PREVENTIVO DI SPESA

Fascia Media

- Switch (7 unità - Cisco SG350-28P): 700 € (100 € ciascuno)
- Firewall (1 unità - Sophos XG 115): 1.200 €
- NAS (1 unità - QNAP TS-453D): 800 €
- Server (2 unità - HPE ProLiant DL380 Gen10): 5.000 € (2.500 € ciascuno)
- Modem (1 unità - Ubiquiti EdgeRouter Infinity): 1.000€

Totale dispositivi di rete: 8.700 €

Fascia Alta

- Switch (7 unità - Aruba 2930F 24G PoE+ Switch): 1.400 € (200 € ciascuno)
- Firewall (1 unità - Palo Alto Networks PA-220): 2.500 €
- NAS (1 unità - Synology RS820+): 1.500 €
- Server (2 unità - Dell PowerEdge R750): 10.000 € (5.000 € ciascuno)
- Modem (1 unità - Cisco ASR 1001-X): 6.500€

Totale dispositivi di rete: 21.900 €

PREVENTIVO DI SPESA

Costi del computer Client

Fascia Bassa
• PC Client (121 unità - Lenovo ThinkCentre M75s Gen2): 48.400 € (400 € ciascuno)
Fascia Media
• PC Client (121 unità - HP EliteDesk 800 G6 SFF): 72.600 € (600 € ciascuno)
Fascia Alta
• PC Client (121 unità - Dell OptiPlex 7090 Ultra): 121.000 € (1.000 € ciascuno)

Costi del software

Fascia Bassa
• Software e licenze (Windows 10 Pro, Open-source firewall, FreeNAS): 15.000 €
Fascia Media
• Software e licenze (Windows 11 Pro, Sophos Firewall, Synology DSM, Microsoft 365): 27.500 €
Fascia Alta
• Software e licenze (Windows Server 2022, Palo Alto Firewall, QNAP QuTS Hero, Adobe Suite): 50.000 €

PREVENTIVO DI SPESA

Costi di installazione e configurazione

Fascia Bassa
- Installazione e configurazione: 12.000 €

Fascia Media
- Installazione e configurazione: 21.000 €

Fascia Alta
- Installazione e configurazione: 35.000 €

Costi di manutenzione e supporto

Fascia Bassa
- Manutenzione e supporto: 12.000 €

Fascia Media
- Manutenzione e supporto: 21.000 €

Fascia Alta
- Manutenzione e supporto: 35.000 €

PREVENTIVO DI SPESA

Tabella riassuntiva costi

- Dispositivi di rete: Fascia Bassa 4.100€, Fascia Media 8.700€, Fascia Alta 21.900€
- PC Client: Fascia Bassa 48.400€, Fascia Media 72.600€, Fascia Alta 121.000€
- Software: Fascia Bassa 15.000€, Fascia Media 27.500€, Fascia Alta 50.000€
- Installazione e configurazione: Fascia Bassa 12.000€, Fascia Media 21.000€, Fascia Alta 35.000€
- Manutenzione e supporto: Fascia Bassa 12.000€, Fascia Media 21.000€, Fascia Alta 35.000€
- Totale generale: Fascia Bassa 91.500€, Fascia Media 150.800€, Fascia Alta 262.900€
- ***Nota: I prezzi sono indicativi e possono variare in base ai fornitori e alle necessità specifiche del cliente.***

IMPLEMENTAZIONE E PIANO LAVORO

Il progetto di implementazione della rete per la compagnia Theta è stato realizzato in un arco di cinque giorni da un team di otto specialisti di PantherCrypt. Al fine di ottimizzare i tempi e garantire un'esecuzione efficiente, il team è stato suddiviso in due gruppi distinti: un team dedicato all'infrastruttura di rete, responsabile della configurazione hardware e della connettività, e un team specializzato nella parte software, incaricato della configurazione dei sistemi di sicurezza, del web server e del NAS. Questa divisione del lavoro ha permesso di affrontare simultaneamente le diverse sfide del progetto, assicurando un risultato finale di alta qualità.

- Fase 1: Pianificazione dettagliata:Definizione precisa dei requisiti specifici di ogni piano e dei reparti.
- Scelta definitiva dell'hardware e del software, con specifiche tecniche dettagliate.
- Creazione di schemi di rete dettagliati, sia logici che fisici.
- Pianificazione dell'indirizzamento IP.

IMPLEMENTAZIONE E PIANO LAVORO

- Fase 2: Preparazione dell'ambiente:Verifica delle infrastrutture esistenti (cablaggi, spazi per i dispositivi).
- Acquisto e preparazione dell'hardware (switch, router, firewall, NAS, IDS/IPS, server, PC).
- Configurazione iniziale dei dispositivi in un ambiente di test.

- Fase 3: Implementazione della rete fisica:Installazione e cablaggio dei dispositivi di rete nei vari piani.
- Collegamento dei dispositivi al firewall perimetrale.
- Installazione e configurazione del NAS.

- Fase 4: Configurazione della rete logica
- Collegamento delle postazioni di lavoro alla rete.
- Migrazione dei dati sul NAS.
- Integrazione del web server nella rete aziendale.

IMPLEMENTAZIONE E PIANO LAVORO

- Fase 5: Test e ottimizzazione: Test di connettività, prestazioni e sicurezza della rete.
- Ottimizzazione delle configurazioni per garantire prestazioni ottimali.
- Test di sicurezza approfonditi, inclusi test di penetrazione.

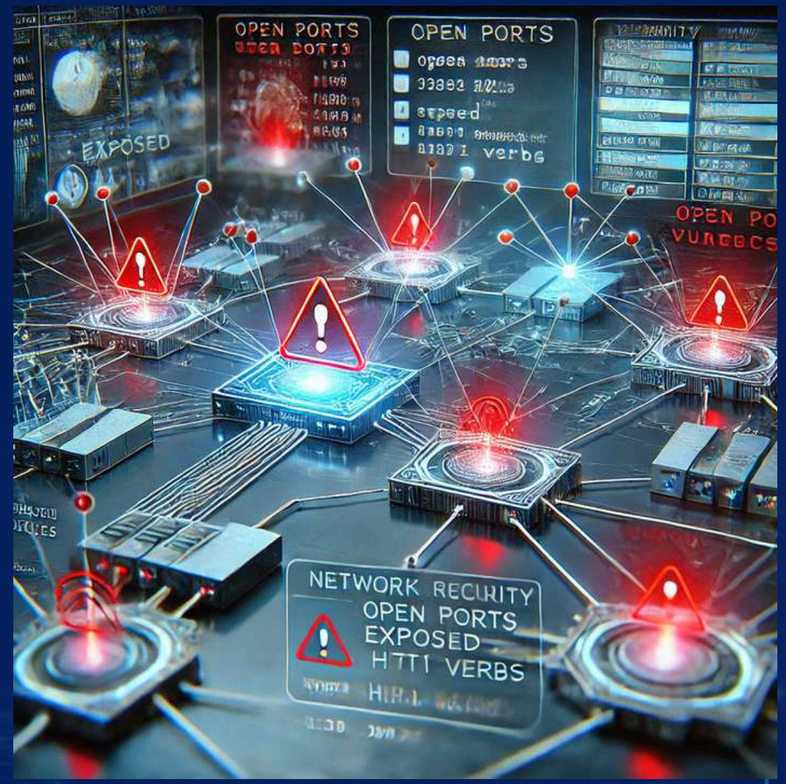
- Fase 6: Formazione e consegna: Formazione del personale IT di Theta sull'utilizzo e la gestione della nuova rete.
- Consegna della documentazione completa del progetto.

CONSIDERAZIONI SULLA SICUREZZA

Durante la progettazione dell'ambiente di rete l'azienda Theta ha subito un attacco di cui ci siamo occupati personalmente.
Analizzando i file corrotti con un dovuto programma realizzato ad hoc dai nostri programmatori e dopo aver decrittografato tutti i messaggi nascosti all'interno delle foto tramite steganografia siamo risaliti ai colpevoli e ci siamo accertati che i movimenti bancari sospetti fossero, a tutti gli effetti, dei furti da parte di hacker esterni alla rete.
A questo punto abbiamo ritenuto necessario che il nostro team di programmazione si occupasse della creazione di uno scanner che potesse analizzare le vulnerabilità dell'azienda e, in particolare, le possibili porte accessibili da utenti esterni.

CONSIDERAZIONI SULLA SICUREZZA

I test condotti hanno evidenziato aree di potenziale rischio nella configurazione della rete
della Compagnia Theta. È stata rilevata l'esposizione di verbi HTTP non necessari, suggerendo la limitazione a quelli essenziali, inoltre La scansione delle porte ha mostrato la presenza di servizi non protetti su porte aperte.
Suggeriamo di limitare i verbi HTTP disponibili, chiudere o filtrare le porte non necessarie e infine Implementare un sistema di monitoraggio continuo. Nelle slide successive illustreremo graficamente quanto appena spiegato.



CONSIDERAZIONI SULLA SICUREZZA

```
File  Actions  Edit  View  Help
  GNU nano 8.3
import socket
import ipaddress

def scan_ports(ip, start_port, end_port):
    print(f"Scanning {ip} from port {start_port} to {end_port}...")
    for port in range(start_port, end_port + 1):
        with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as sock:
            sock.settimeout(0.5)
            result = sock.connect_ex((ip, port))
            if result == 0:
                print(f"[OPEN] Port {port}")

def find_hosts(subnet, start_port, end_port):
    print(f"Scanning subnet {subnet} for active hosts...")
    for ip in ipaddress.IPv4Network(subnet, strict=False):
        try:
            with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as sock:
                sock.settimeout(0.3)
                if sock.connect_ex((str(ip), 80)) == 0:
                    print(f"[ACTIVE] Host found: {ip}")
                    scan_ports(str(ip), start_port, end_port)
        except Exception:
            continue

find_hosts('192.168.40.101/24', 1, 100)
```

```
┌──(kali㉿kali)-[~]
└─$ python3 scanner_metaspoitable.py
Scanning subnet 192.168.40.101 for active hosts...
[ACTIVE] Host found: 192.168.40.101
Scanning 192.168.40.101 from port 1 to 1023...
[OPEN] Port 21
[OPEN] Port 22
[OPEN] Port 23
[OPEN] Port 25
[OPEN] Port 53
[OPEN] Port 80
[OPEN] Port 111
[OPEN] Port 139
[OPEN] Port 445
[OPEN] Port 512
[OPEN] Port 513
[OPEN] Port 514
```

CONCLUSIONI

Cybersecurity

Il progetto per la Compagnia Theta è stato completato con successo. L'implementazione di una rete robusta, sicura e scalabile fornirà a Theta una solida base per le sue attività future, supportandone la crescita.

Security Operations

PantherCrypt è fiduciosa che la nuova infrastruttura di rete fornirà a Theta un vantaggio competitivo significativo. Siamo a disposizione per qualsiasi supporto o ulteriore sviluppo futuro.

Development

PantherCrypt è impegnata a supportare Theta nell'adozione di nuove tecnologie e nell'innovazione continua.

THANK YOU FOR YOUR ATTENTION