

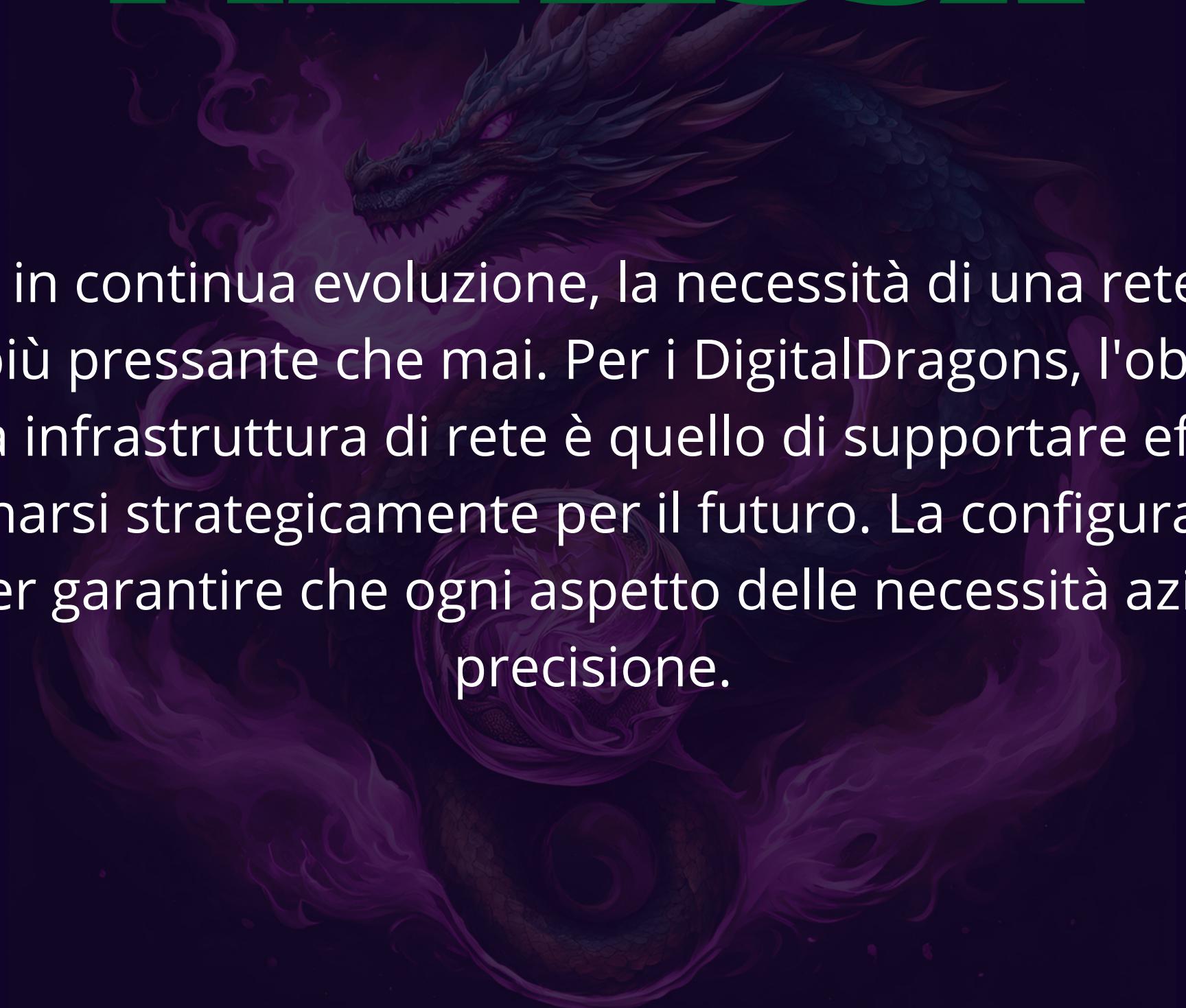


DEFENCE FOR THETA

LA NOSTRA SOLUZIONE!

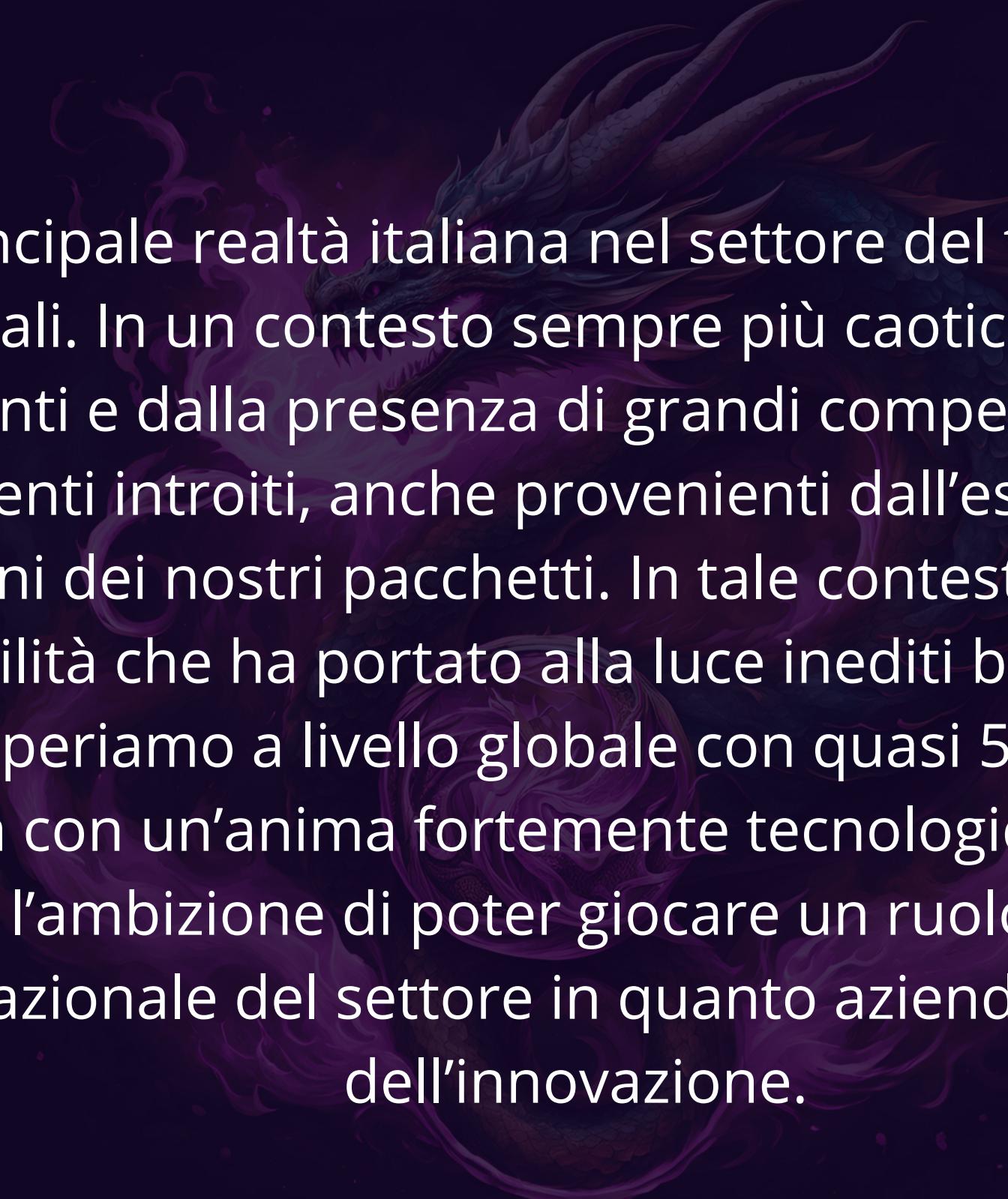


PREMESSA



In un contesto aziendale in continua evoluzione, la necessità di una rete che sia al tempo stesso robusta e flessibile è più pressante che mai. Per i DigitalDragons, l'obiettivo principale nella progettazione della nostra infrastruttura di rete è quello di supportare efficacemente le operazioni quotidiane e di posizionarsi strategicamente per il futuro. La configurazione proposta utilizza tecnologie avanzate per garantire che ogni aspetto delle necessità aziendali sia coperto con precisione.

LA NOSTRA MESSAGGIO



DigitalDragons è la principale realtà italiana nel settore del tech e opera principalmente nell'ambito delle reti aziendali. In un contesto sempre più caotico, caratterizzato da discontinuità tecnologiche senza precedenti e dalla presenza di grandi competitor, in Italia come all'estero, che possono contare su ingenti introiti, anche provenienti dall'estero, che diventano sostegni strutturati dalle esportazioni dei nostri pacchetti. In tale contesto la Build Week rappresenta un evento epocale di instabilità che ha portato alla luce inediti bisogni, dando origine a nuove dinamiche nel settore. Operiamo a livello globale con quasi 50.000 persone, coniugando la componente manifatturiera con un'anima fortemente tecnologica volta all'innovazione continua. Guardiamo al futuro con l'ambizione di poter giocare un ruolo protagonista nel processo di consolidamento internazionale del settore in quanto azienda solida, globale e alla guida dell'innovazione.

Introduzione e Obiettivi

Una Rete Sicura, Affidabile e Scalabile

Contesto

L'azienda opera su 6 piani, con un totale di 120 endpoint.

La rete è il cuore operativo, supportando reparti come Amministrazione, Produzione e Vendite, oltre a un server web per l'e-commerce.

Obiettivi del Progetto

Progettare una rete segmentata con VLAN per migliorare sicurezza e gestione.

Implementare ridondanza hardware e software per ridurre i downtime.

Garantire un'infrastruttura pronta per la crescita aziendale.

Approccio

- Struttura Gerarchica: Modello a tre livelli (Access, Distribution, Core).
- Integrazione Completa: Hardware e software scelti per garantire compatibilità e prestazioni.
- Gestione e Monitoraggio: Soluzioni avanzate per semplificare la manutenzione.

Obiettivi Chiave

Sicurezza avanzata:

Segmentazione del traffico tramite VLAN.
Firewall Palo Alto PA-5220 con IDS/IPS integrati.
Controlli di accesso specifici (ACL) per proteggere i dati e le risorse aziendali.

Affidabilità:

Ridondanza in tutti i dispositivi critici:
Switch di distribuzione in StackWise Virtual.
Router WAN configurati con HSRP per failover.
Firewall in modalità Active/Passive per garantire continuità di servizio.
Backup e ripristino dei dati in caso di guasto (piano di disaster recovery con ripristino in 4 ore).

Scalabilità:

Possibilità di aggiungere VLAN e dispositivi senza modifiche strutturali.
Supporto a future espansioni grazie a uplink a 40/100 Gbps.
Rete già pronta per integrare un telefono VoIP per ogni PC.

Architettura e VLAN



Architettura Logica: Una Rete Gerarchica e Modulare

Access Layer

Collegamento degli endpoint tramite 6 switch Cisco Catalyst 9300-48P-A.
Ogni switch supporta PoE+ per alimentare telefoni VoIP e access point.
Segmentazione logica tramite VLAN per ciascun piano e dipartimento.

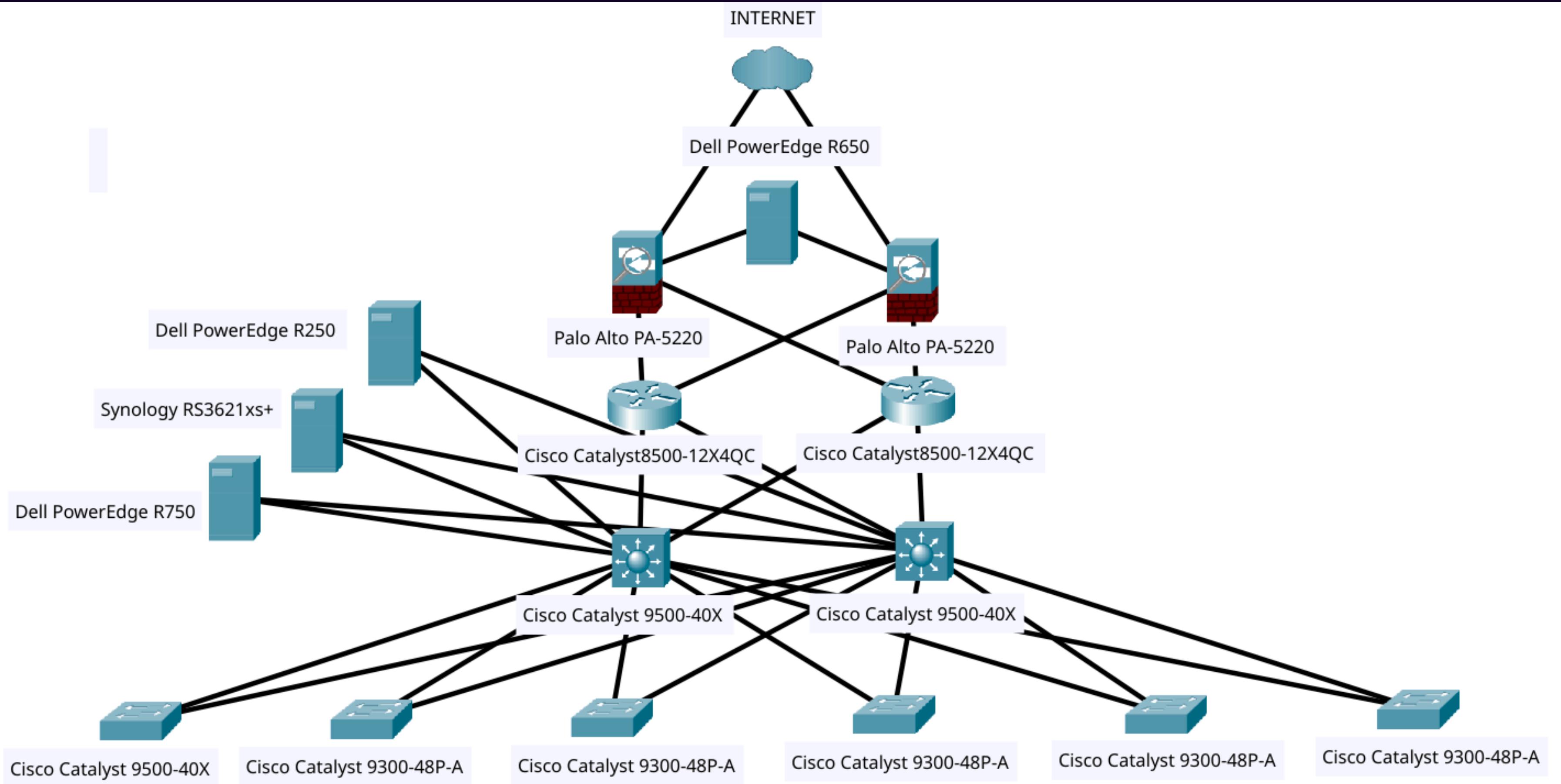
Distribution Layer

2 switch Cisco Catalyst 9500-40X in configurazione StackWise Virtual.
Aggregazione del traffico proveniente dagli switch di accesso.
Routing inter-VLAN e gestione del traffico verso i router WAN e i firewall.

Core Layer

2 router Cisco Catalyst 8500-12X4QC configurati in HSRP per failover.
2 firewall Palo Alto PA-5220 in modalità Active/Passive per sicurezza avanzata e IDS/IPS integrati.

Topologia fisica della rete



Segmentazione VLAN

Definizione

Le VLAN (Virtual Local Area Network) separano logicamente il traffico di rete, migliorando la sicurezza e la gestione.

Ogni VLAN è progettata per un reparto o una funzione specifica, isolando il traffico per evitare interferenze.

Benefici della Segmentazione VLAN

Sicurezza: Isola i reparti per limitare accessi non autorizzati.

Prestazioni: Riduce il traffico broadcast migliorando la velocità di rete.

Gestione: Ogni segmento è configurato per accedere solo alle risorse necessarie.

Routing inter-VLAN:

Routing gestito dagli switch di distribuzione Cisco Catalyst 9500.

Configurazioni coerenti con sicurezza e policy di accesso.

Tabella VLAN

| VLAN ID | Nome | Indirizzo IP | Subnet | Descrizione |
|---------|-----------------|-----------------|--------|---|
| 10 | Amministrazione | 192.168.10.0/24 | /24 | Gestione utenti aziendali. |
| 20 | Produzione | 192.168.20.0/24 | /24 | Operazioni di produzione. |
| 30 | Vendite | 192.168.30.0/24 | /24 | Supporto al reparto vendite. |
| 40 | DMZ | 10.0.40.0/24 | /24 | Server web e-commerce. |
| 50 | NAS | 192.168.50.0/24 | /24 | Archiviazione centralizzata. |
| 70 | VoIP | 192.168.70.0/24 | /24 | Separazione del traffico voce. |
| 80 | Management | 192.168.80.0/24 | /24 | Gestione degli apparati di rete. |
| 90 | Sistemisti | 192.168.90.0/24 | /24 | Accesso sistemisti e autenticazione AD. |

Hardware e Software



Hardware Utilizzato: Prestazioni e Affidabilità



L'hardware selezionato garantisce prestazioni elevate, scalabilità e ridondanza per supportare le operazioni aziendali.

Ogni dispositivo è stato scelto per adattarsi alle necessità specifiche di ogni livello della rete.

Caratteristiche Chiave

Ridondanza: Switch di distribuzione, router WAN e firewall configurati con failover automatico.

Prestazioni elevate: Supporto 10/40 Gbps per uplink e throughput.

Virtualizzazione: Server consolidato per ottimizzare risorse e ridurre i costi.

Tabella Hardware:

| Dispositivo | Modello | Quantità | Funzione |
|-------------------------|----------------------------|----------|------------------------------------|
| Switch di Accesso | Cisco Catalyst 9300-48P-A | 6 | Endpoint e gestione VLAN. |
| Switch di Distribuzione | Cisco Catalyst 9500-40X | 2 | Routing inter-VLAN e aggregazione. |
| Router WAN | Cisco Catalyst 8500-12X4QC | 2 | Routing WAN e failover (HSRP). |
| Firewall | Palo Alto PA-5220 | 2 | Layer 7, IDS/IPS integrato. |
| Server Consolidato | Dell PowerEdge R750 | 1 | Servizi aziendali virtualizzati. |
| Server Web | Dell PowerEdge R650 | 1 | Hosting e-commerce in DMZ. |
| NAS | Synology RS3621xs+ | 1 | Storage RAID 6 centralizzato. |
| Server Monitoraggio | Dell PowerEdge R250 | 1 | PRTG Network Monitor. |

Software Utilizzato: Gestione e Sicurezza

Il software selezionato è stato scelto per garantire una gestione efficiente della rete, la protezione dei dati aziendali e la scalabilità futura.

Ogni applicativo è ottimizzato per lavorare con l'hardware scelto e soddisfare le esigenze specifiche dell'azienda.

Caratteristiche Chiave

Gestione: VMware vSphere consente di virtualizzare i server per migliorare flessibilità e utilizzo delle risorse.

Sicurezza: Windows Server 2019 gestisce l'autenticazione centralizzata tramite Active Directory, oltre a DHCP e DNS.

Protezione: Veeam Backup garantisce il ripristino rapido dei dati aziendali in caso di guasti.

Monitoraggio: PRTG fornisce un monitoraggio continuo per ottimizzare le prestazioni della rete.

Tabella Software

| Software | Funzione | Licenza Necessaria |
|----------------------|----------------------------------|---------------------------|
| VMware vSphere | Virtualizzazione server. | VMware vSphere Standard. |
| Windows Server 2019 | Domain Controller, DHCP, DNS. | 2 licenze per VM. |
| PRTG Network Monitor | Monitoraggio di rete. | Licenza per 500 sensori. |
| Veeam Backup | Backup incrementale. | Licenza Veeam Essentials. |
| PAN-OS | Gestione dei firewall Palo Alto. | Incluso con hardware. |
| Synology DSM | Gestione NAS. | Incluso con hardware. |

Sicurezza e Monitoraggio



Sicurezza della Rete: Protezione Completa e Monitoraggio

La sicurezza è una priorità assoluta per questa rete, progettata per proteggere i dati aziendali da minacce interne ed esterne.

La combinazione di firewall avanzati, IDS/IPS, regole ACL e monitoraggio continuo garantisce un'infrastruttura sicura e resiliente.

Elementi Chiave della Sicurezza

Firewall Palo Alto PA-5220:

Protezione Layer 7 con IDS/IPS integrati.

Rilevamento e blocco di attacchi come DDoS, malware ed exploit.

Policy granulari per la gestione del traffico tra VLAN.

IDS/IPS:

Feed IOC aggiornati per rilevare minacce conosciute e sconosciute.

Analisi del traffico per identificare comportamenti anomali.

ACL (Access Control Lists):

Controllano il traffico tra VLAN per consentire solo accessi autorizzati.

Configurate sugli switch di distribuzione e sui firewall.

Monitoraggio Continuo con PRTG:

Sensori per monitorare stato e traffico dei dispositivi critici.

Log di sicurezza raccolti tramite Syslog dai firewall.

Tabella ACL Configurate:

| Origine | Destinazione | Protocolli | Azione |
|----------------------|-------------------------|-------------|----------|
| VLAN Management | Apparati di rete | HTTPS, SSH | Allow |
| VLAN Amministrazione | NAS | SMB, NFS | Allow |
| VLAN Produzione | NAS | SMB, NFS | Allow |
| VLAN Vendite | NAS | SMB | Allow |
| VLAN DMZ | Internet | HTTP, HTTPS | Allow |
| VLAN Interna | DMZ | - | Deny |
| VLAN Interna | VLAN Interna (tra VLAN) | - | Deny |
| Qualsiasi | Qualsiasi | - | Deny All |

Punti di Forza:

Protezione Proattiva: Blocco delle minacce in tempo reale grazie a IDS/IPS.

Isolamento VLAN: Riduzione del rischio di accessi non autorizzati.

Monitoraggio Completo: Log e analisi per rilevare comportamenti sospetti.

Monitoraggio e Backup



Controllo Continuo e Protezione dei Dati

I monitoraggio proattivo garantisce la continuità operativa e individua rapidamente anomalie o guasti.

Il backup incrementale protegge i dati aziendali, assicurando il ripristino rapido in caso di guasti o attacchi.

Monitoraggio (PRTG Network

Monitor):

Sensori Configurati:

Stato porte degli switch (SNMP).

Traffico aggregato su router WAN (NetFlow).

Log di sicurezza dai firewall (Syslog).

Prestazioni server (CPU, RAM, spazio disco).

Notifiche:

Email/SMS automatiche in caso di anomalie.

Benefici:

Individuazione immediata di guasti o colli di bottiglia.

Monitoraggio continuo delle prestazioni della rete.

Backup (Veeam Backup):

Metodologia:

Backup incrementali per ridurre tempi e consumo di spazio.
Dati salvati su NAS Synology con RAID 6.

Ripristino:

Piano di disaster recovery con ripristino entro 4 ore.

Benefici:

Protezione completa per dati aziendali e macchine virtuali.
Minimizzazione dei tempi di inattività.

Tabella Sensori Monitoraggio:

| Sensore Monitorato | Dispositivo | Protocollo | Descrizione |
|--------------------|-------------------------|---------------|--------------------------------------|
| Stato porte | Switch di Accesso | SNMP | Stato delle porte fisiche e logiche. |
| Uptime e traffico | Switch di Distribuzione | SNMP, NetFlow | Disponibilità e banda aggregata. |
| Log di sicurezza | Firewall Palo Alto | Syslog | Analisi di log per eventi e minacce. |
| Traffico WAN | Router WAN | NetFlow | Monitoraggio HSRP e carico WAN. |
| Prestazioni server | Dell PowerEdge R750 | WMI/Agent | Monitoraggio risorse CPU e RAM. |
| | | | |

Cablaggio, Scalabilità



Cablaggio della Rete: Struttura e Materiali Utilizzati

Il cablaggio è progettato per supportare le prestazioni elevate richieste dalla rete, garantendo ordine, scalabilità e affidabilità.

Utilizzo di materiali di alta qualità per collegamenti backbone e endpoint.

Materiali Utilizzati

Fibra Multimodale OM4:

Backbone per collegamenti tra switch di accesso, distribuzione e core.
Supporta throughput fino a 10 Gbps su distanze di 300 metri.

Cavi Ethernet Cat6a:

Connessioni endpoint per PC, telefoni VoIP e stampanti.
Velocità fino a 10 Gbps su distanze fino a 100 metri.

Rack e Accessori:

Rack 42U, patch panel, prese Ethernet femmina e canaline per una gestione pulita ed efficiente.

Tabella Cablaggio:

| Materiale | Quantità | Note |
|------------------------|-------------------|---------------------------------|
| Fibra multimodale OM4 | ca 36 | da definire in fase sopralluogo |
| Moduli SFP-10G-SR | Ca 36 | da definire in fase sopralluogo |
| Cavi Ethernet Cat6a | ca 120 cavi da 2m | da definire in fase sopralluogo |
| Canaline passa cavi | ca 200m | da definire in fase sopralluogo |
| Patch panel | ca 6 | da definire in fase sopralluogo |
| Rack 42U | 2 | ridondanza datacenter |
| Rack 24U | 6 | uno per piano |
| Prese Ethernet femmina | Ca 120 | da definire in fase sopralluogo |

Scalabilità: Una Rete Pronta per il Futuro

La rete è progettata per crescere insieme alle esigenze aziendali, supportando l'aggiunta di nuovi dispositivi e servizi senza modifiche invasive.

Ogni componente hardware e software è stato scelto con la scalabilità come criterio chiave.

Caratteristiche Scalabili

Switch di Accesso:

Ogni switch Cisco Catalyst 9300 dispone di 48 porte, sufficienti per collegare fino a 48 endpoint per piano (es. PC e telefoni VoIP).

Supporto PoE+ per alimentare nuovi dispositivi come access point o videocamere di sicurezza.

Switch di Distribuzione:

Supporto per uplink a 40 Gbps, con possibilità di espansione fino a 100 Gbps per gestire un carico maggiore di traffico inter-VLAN.

Server:

Capacità di virtualizzazione con VMware vSphere per aggiungere nuovi servizi virtualizzati senza investire in ulteriore hardware.

Cablaggio:

Fibra multimodale OM4 e cavi Cat6a progettati per supportare connessioni ad alta velocità e nuovi dispositivi.

Tabella Scalabilità

| Elemento | Capacità Attuale | Possibilità di Espansione |
|-------------------------|--------------------------|---|
| Switch di Accesso | 48 porte per switch | Possibilità di aggiungere altri switch. |
| Switch di Distribuzione | 40 Gbps uplink | Espansione fino a 100 Gbps. |
| Server Servizi interni | 1 Dell PowerEdge R750 | Aggiunta di nuove VM con VMware. |
| VLAN Configurate | 9 VLAN | Creazione di ulteriori VLAN. |
| Cavi e Cablaggio | 120 connessioni endpoint | Aggiunta di nuove prese Ethernet. |

Benefici della Scalabilità

Supporto a nuovi servizi:

Aggiunta di telefoni VoIP, dispositivi IoT, o VLAN dedicate.

Espansione senza interruzioni:

Nuovi dispositivi o connessioni possono essere aggiunti senza compromettere il funzionamento della rete.

Risparmio a lungo termine:

L'infrastruttura è pronta per adattarsi a futuri cambiamenti senza investimenti significativi.

Conclusioni



In conclusione, questa rete rappresenta una soluzione completa che soddisfa le necessità presenti e future dell'azienda. È sicura, affidabile e scalabile, progettata per garantire protezione, efficienza e una base solida per la crescita aziendale. Siamo pronti a procedere con l'implementazione e assicuriamo il massimo impegno per fornire una rete operativa al 100%, pronta per affrontare le sfide del futuro.

SOFTWARE

Testing della rete

Scanner di Rete e Verifica Verbi HTTP

Introduzione al progetto

I due software sono stati realizzati per affrontare due aspetti critici della sicurezza della rete:

Analisi delle porte di rete

- Le porte di rete sono punti di accesso per la comunicazione tra dispositivi di rete
- La scansione delle porte, identificando lo stato delle stesse e fornisce una panoramica sul livello di sicurezza
- La gestione corretta delle porte è essenziale per prevenire accessi non autorizzati e ottimizzare la configurazione di firewall

I metodi HTTP

- Il protocollo HTTP è essenziale per la comunicazione tra client e server web
- Verificare quali metodi HTTP un server supporta (GET, POST, PUT, DELETE, ecc.) è cruciale per capire se sono presenti metodi pericolosi che potrebbero compromettere la sicurezza del server.
- Assicurarsi che il server rispetti gli standard di conformità ai protocolli HTTP/HTTPS è essenziale per evitare vulnerabilità.

OBIETTIVI DEL PROGETTO

SONO STATI REALIZZATE:

Scanner di Porte

- Identificazione dello stato delle porte
- Supporto alla configurazione di firewall e ottimizzazione delle regole
- Possibilità di scansione di ampi intervalli di porte
- Reportistica dettagliata per la documentazione delle scansioni

Verifica HTTP

- Determinare i metodi HTTP supportati
- Identificazione di metodi insicuri
- Validazione delle configurazioni di server.
- Registrazioni dei test per analisi future

STACK TECNOLOGICO

Linguaggio e librerie usate

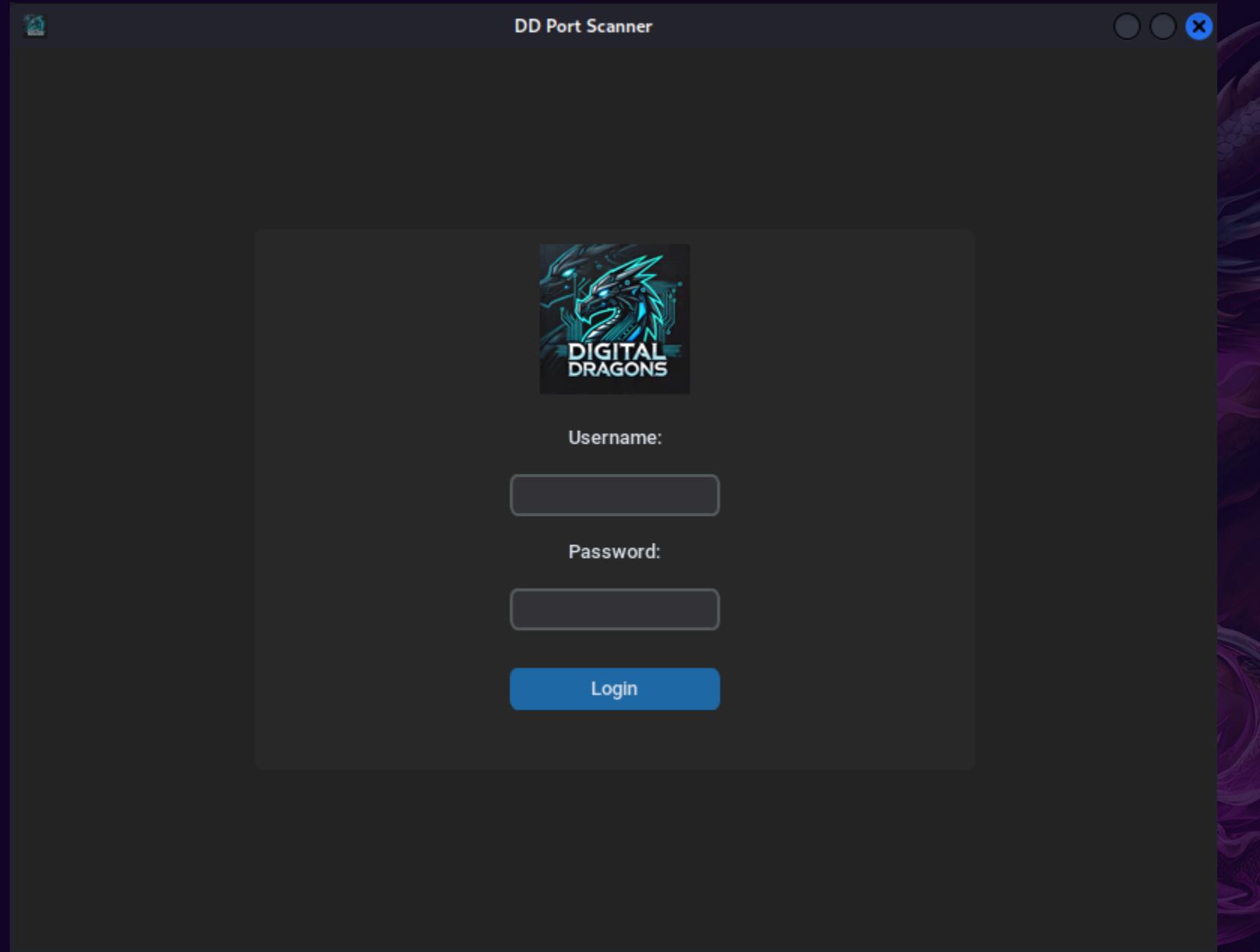
Python:

Usato per entrambi i software grazie alla sua flessibilità, leggibilità e supporto di librerie

Librerie

- **Socket:** Gestione delle connessioni di rete e verifica dello stato delle porte
- **Requests:** Gestione delle richieste HTTP e analisi delle risposte dei server
- **os:** Interazione con il file system
- **datetime:** Aggiunta di timestamp
- **Logging:** Registrazione degli eventi di sistema
- **Openpyxl:** Lettura, scrittura e manipolazione di file Excel
- **Customtkinter:** Libreria per la creazione di interfacce grafiche
- **Threading:** Gestione dell'esecuzione di operazioni parallele
- **Queue:** Sincronizzazione e comunicazione tra thread.
- **Pandas:** Manipolazione e salvataggio dei dati

Scanner di Rete



Schermata di login

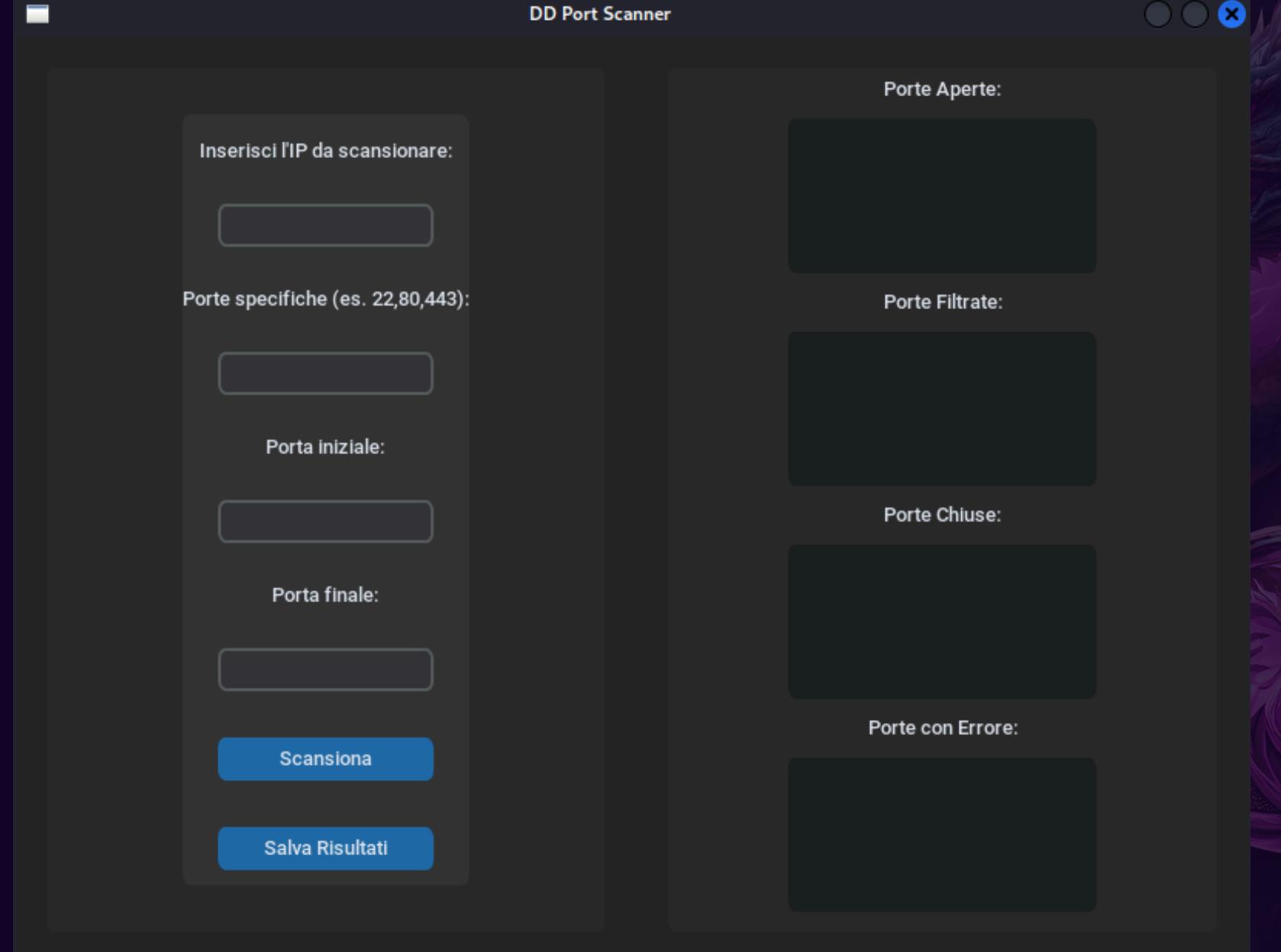
Obiettivo

Analizzare le porte di rete sui dispositivi per verificare la loro sicurezza e accessibilità

Funzionalità

- Scansione di porte TCP/UDP
- Identificazione delle porte aperte, chiuse e filtrate o con errori di connessione
- Supporto multi-threading per scansioni parallele veloci.
- Generazione di report log per documentare i risultati.
- Accesso protetto

Scanner di Rete

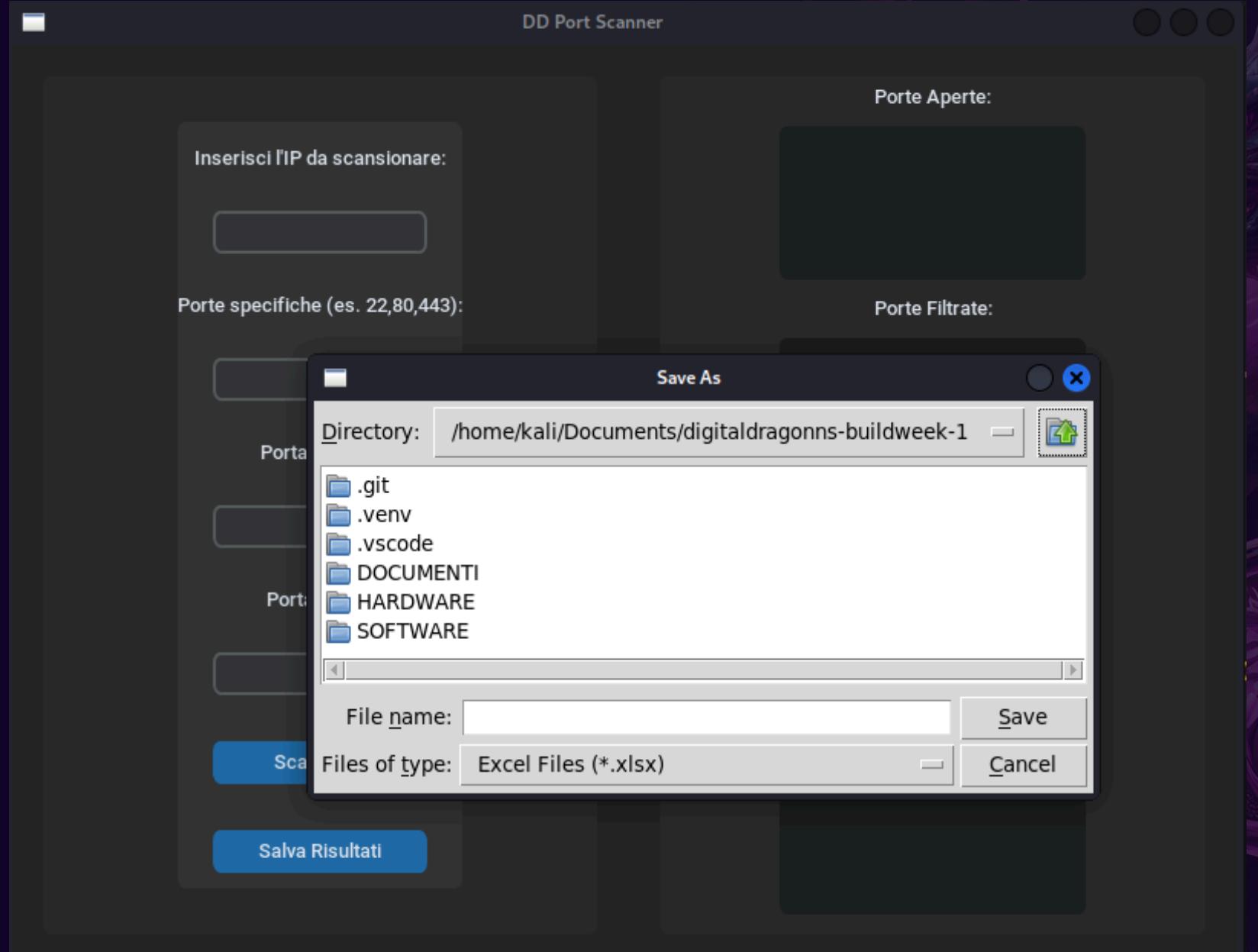


MainPage programma

Come si presenta

- Input IP da scansionare
- Input di Porte Specifiche
- Range di Porte
- Tasto “Scansiona”
- Tasto Salva
- Box Output Porte aperte
- Box Output Porte filtrate
- Box Output Porte chiuse
- Box Output Porte con errore

Scanner di Rete

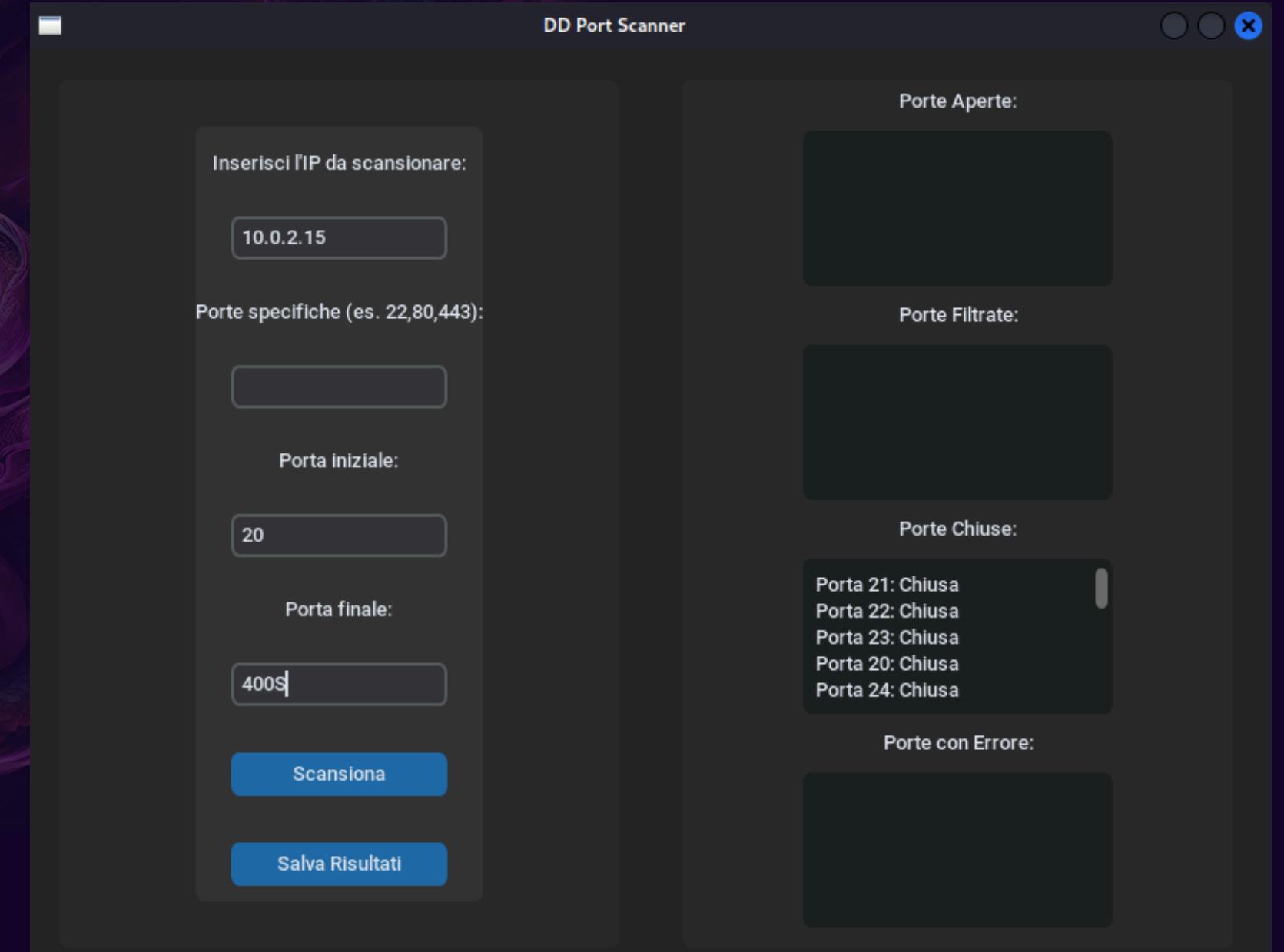


Schermata di salvataggio

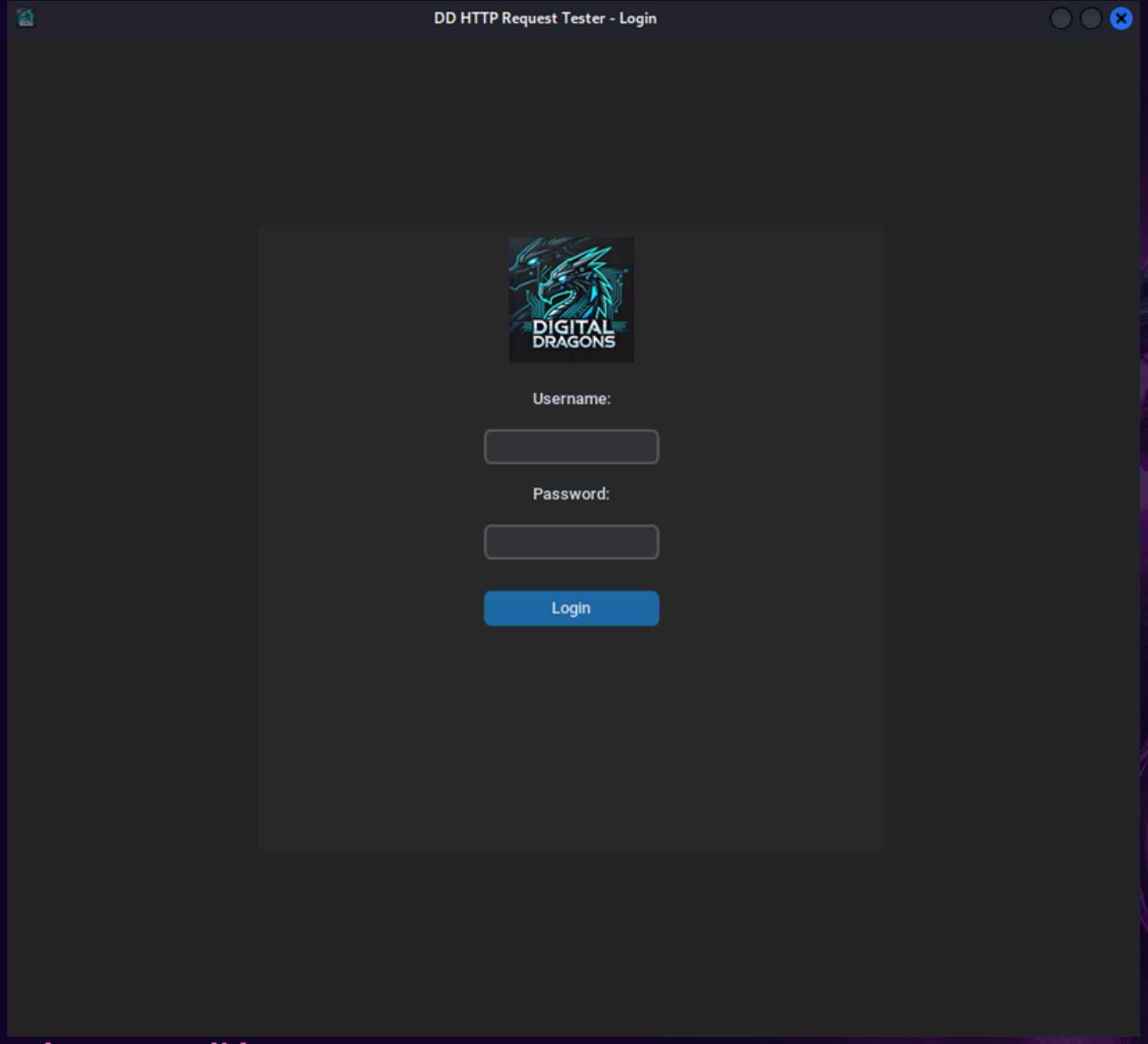
Se si vuole salvare la scansione, basta cliccare su "Salva Risultato" e scegliere poi il percorso dove si preferisce salvare il file

Come funziona

Dopo aver inserito l'indirizzo IP da scansionare e aver scelto le porte o il range di porte, premere "Scansiona"



Verifica HTTP



Schermata di logIn

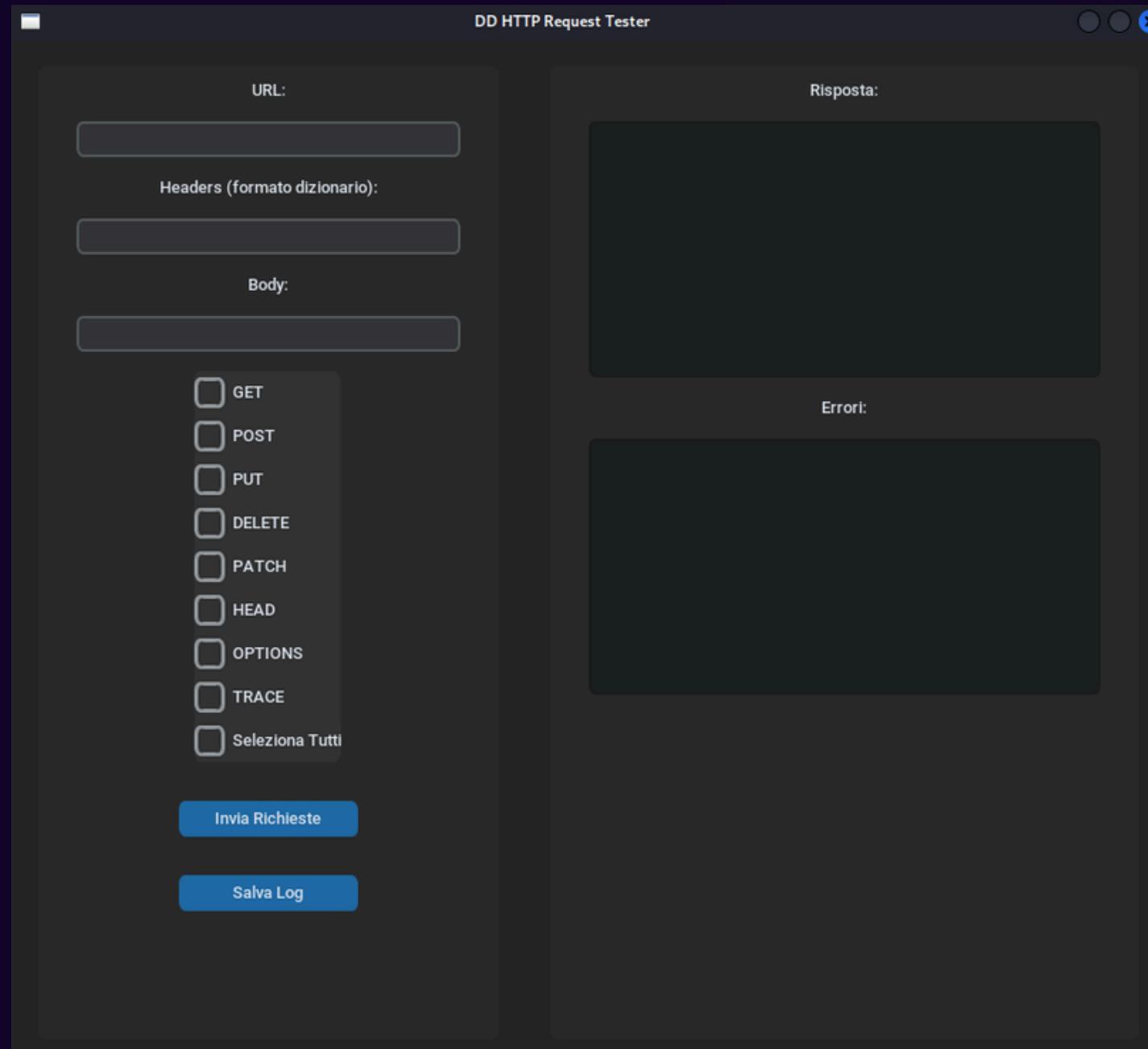
Obiettivo

Analizzare le porte di rete sui dispositivi per verificare la loro sicurezza e accessibilità

Funzionalità

- Invio di richieste HTTP
- Verifica di metodi insicuri
- Monitoraggio delle risposte dei server per garantire la corretta gestione dei protocolli HTTP/HTTPS.
- Accesso protetto

Verifica HTTP



MainPage programma

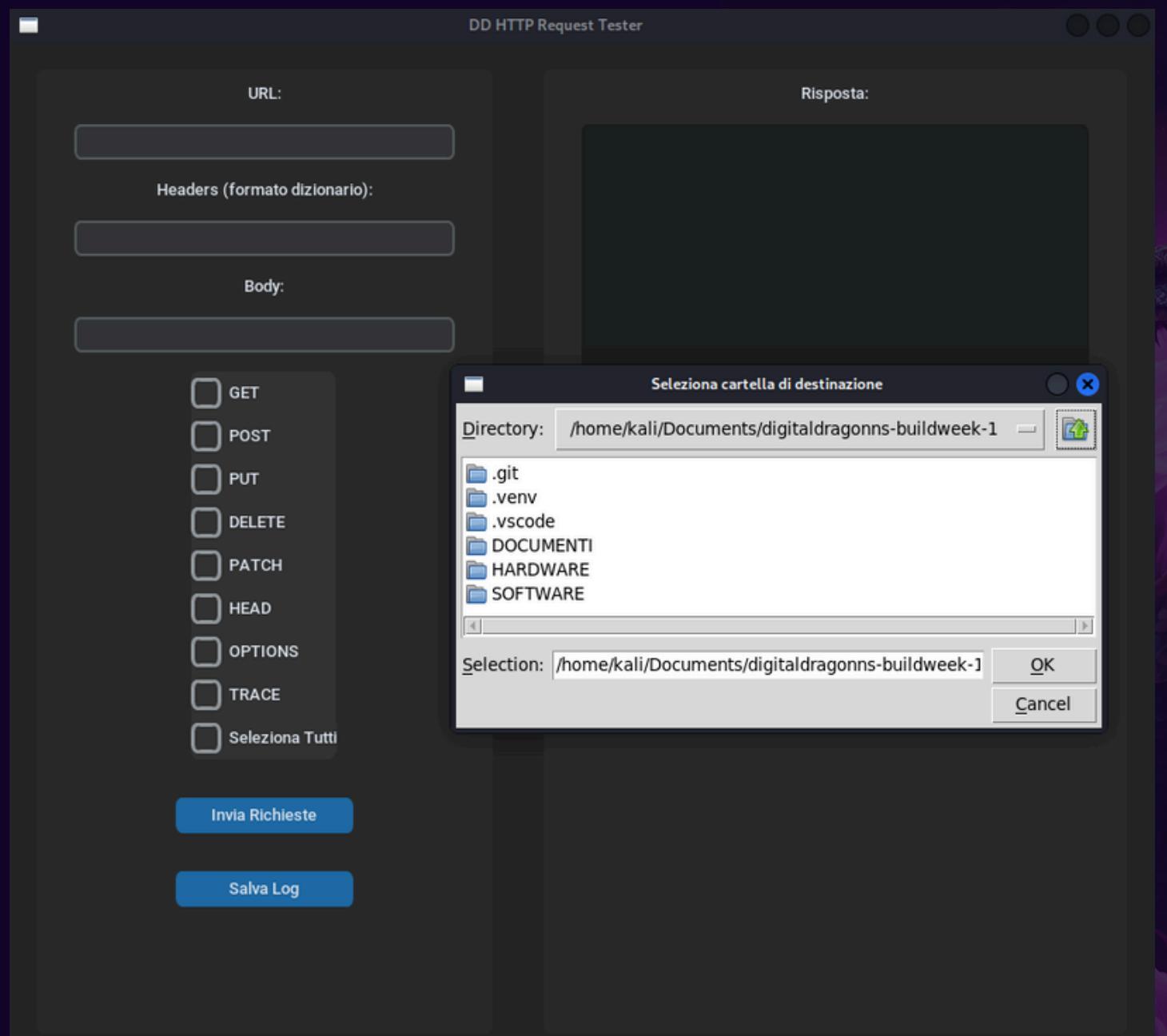
Come si presenta

- Input URL da interrogare
- Box Output Risposta
- Input eventuale header
- Box Output Errori
- Input eventuale body
- Checkbox selezione richieste
- Tasto “Invia Richiesta”
- Tasto Salva

Verifica HTTP

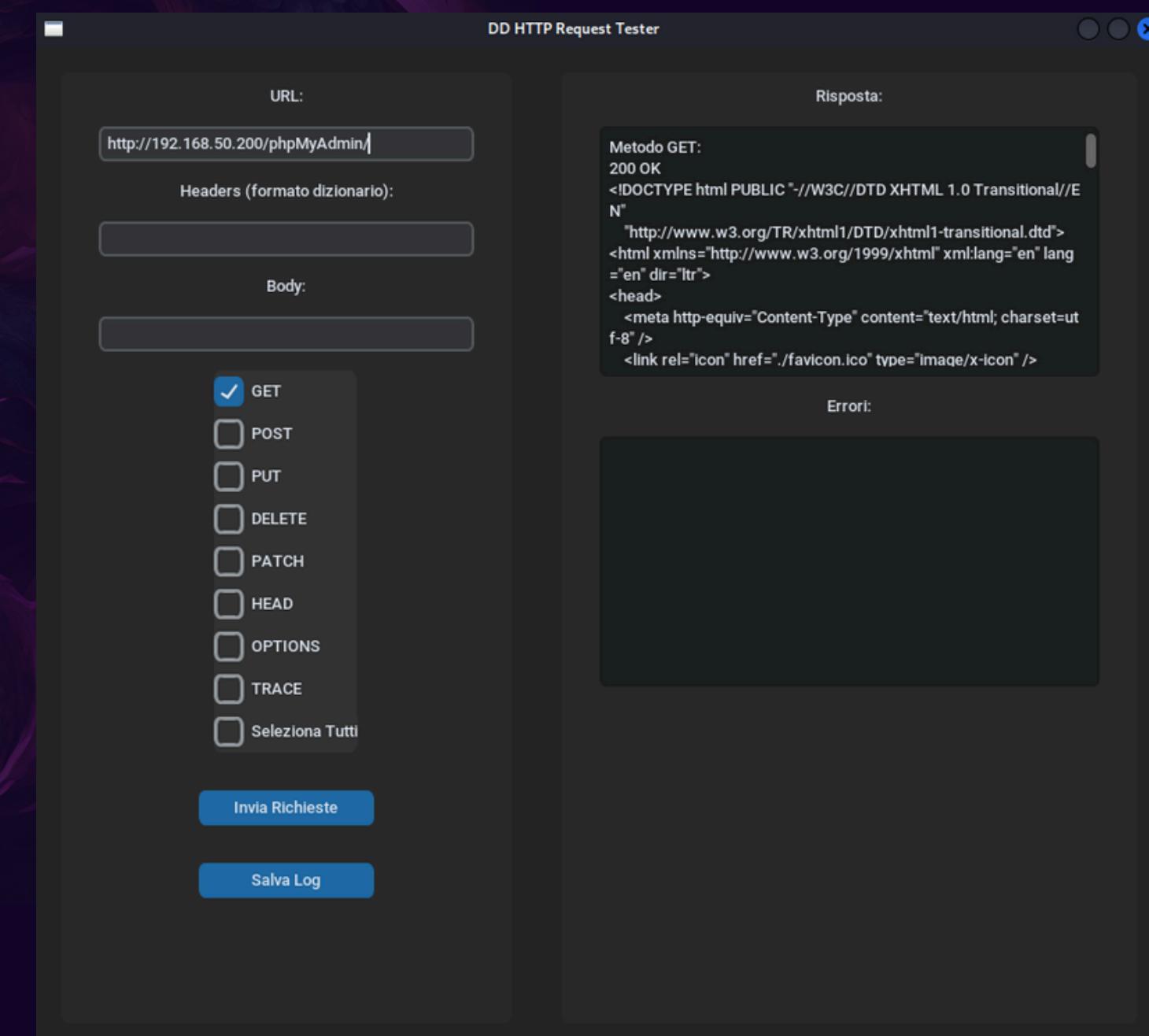
Come funziona

Dopo aver scelto l'URL da interrogare, l'header e/o il body spuntare le checkbox per selezionare il metodo preferito e premere poi "Invia Richiesta"



Schermata di salvataggio

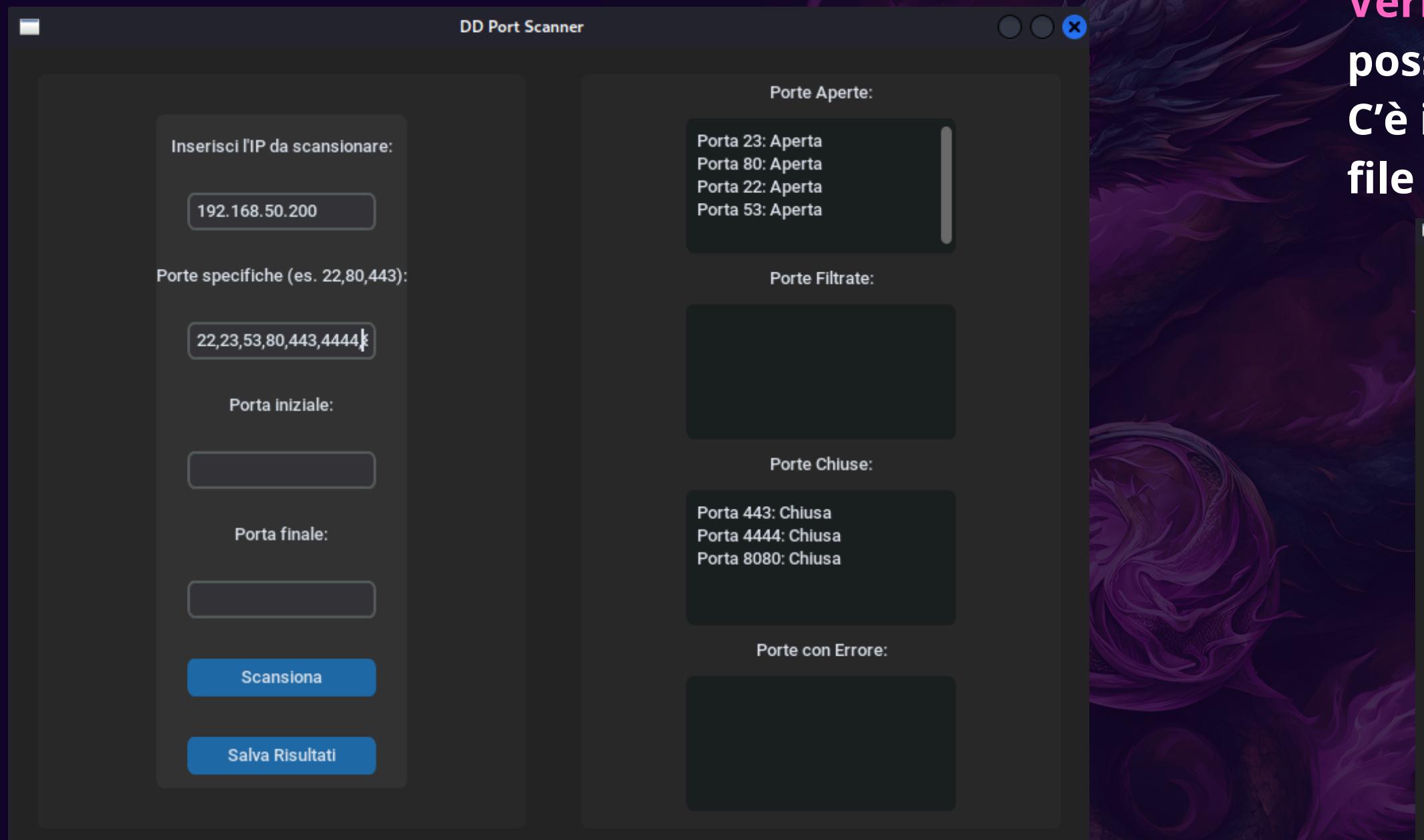
Se si vuole salvare la scansione, basta cliccare su "Salva Risultato" e scegliere poi il percorso dove si preferisce salvare il file



Result

Risultati

Risultati simulati con Metasploitable

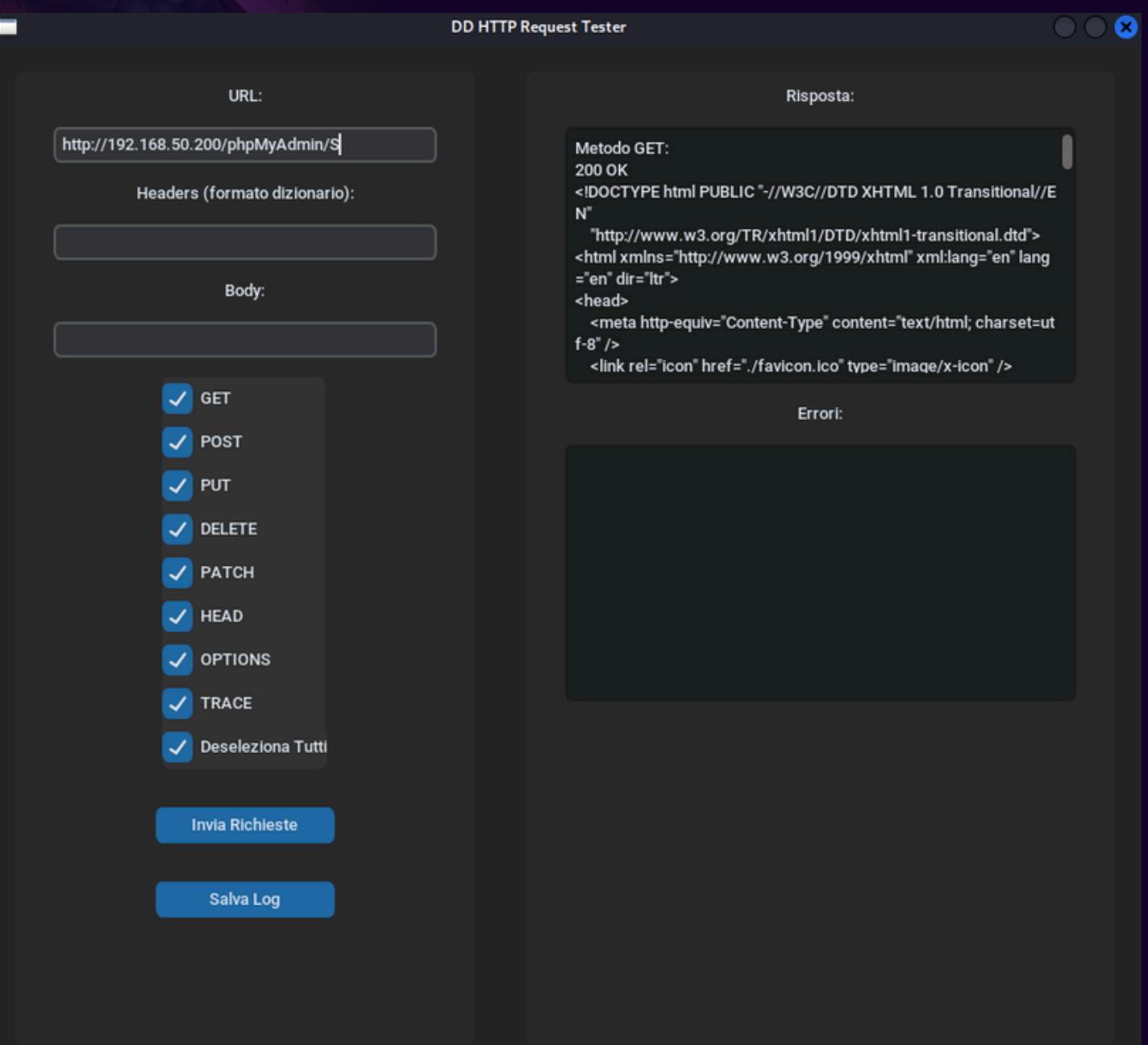


Risultati

Scanner di rete: Come è possibile notare se si prova a scansionare il codice è possibile vedere nel lato destro della finestra lo stato delle porte selezionate.

Tuttavia è possibile salvare il risultato su un file Excel.

Verifica HTTP: Come evidenzia l'immagine è possibile vedere la risposta a destra della finestra. C'è inoltre la possibilità di salvare le risposte su un file di testo.



Risultati

Conclusione

Riflessioni finali

Entrambi i software offrono un approccio modulare.

L'uso di Python e librerie specifiche consente di eseguire test complessi in modo efficiente.

I risultati possono essere utilizzati per migliorare la configurazione della rete e dei server, contribuendo ad un sistema più sicuro.

Best Practices

**Anche se le nostre decisioni potranno aiutarvi
contro le minacce esterne, non dimenticate:**

- Gestione delle password
- Autenticazione a Due Fattori (2FA)
- Crittografia e Protezione dei Dati
- Aggiornamenti Software
- Consapevolezza sulle Minacce
- Navigazione Sicura
- Segnalazione di Incidenti

MADE WITH LOVE :

ANDREA NASTRUZZO

CARMINE INSERRATO

DANIELE VEGLIA

ANGELO MIELE

FABIO PILU

FRANCESCO DE BARTOLOMEO

FEDERICO SELLA

RACHELE MARTANO

