



WOLF ETHICAL HACKER

WOLF  
ETHICAL  
HACKER

# PREVENTIVO **THETA** COMPANY

---

2024

WWW.WOLFEH.COM

# PRIORITY -> SECURITY



WOLF ETHICAL HACKER

**ADVANCE SECURITY**



# INDICE

• Mission	3
• Proposta 1 - Leasing	4 - 7
• Proposta 2 - Acquisto	8 - 10
• Proposta 3 - Pro Advisor	11 - 13
• Proposta 4- Wolf Elite	14 - 17
• Long Support	18
• Hardware	19 - 24
• Analisi Forense - Scansione porte	25 - 29
• Analisi Forense - Scansione verbi HTTP	30 - 33
• Analisi Forense - File Theta Zip	33
• Team	35



# MISSION

---

La scelta dei materiali e delle soluzioni tecnologiche è stata guidata dalla necessità di creare un'infrastruttura IT che sia non solo all'altezza delle attuali esigenze aziendali, ma che possa anche crescere e adattarsi a futuri sviluppi. La scalabilità è garantita dai dispositivi Cisco, che offrono funzionalità avanzate e una facile espansione della rete. La velocità è assicurata dall'uso di tecnologie di cablaggio all'avanguardia e da dispositivi di archiviazione ottimizzati. Infine, la sicurezza è al centro di questa configurazione, con firewall di nuova generazione che proteggono l'azienda da minacce esterne e interne, garantendo così la continuità operativa e la protezione dei dati.



1°

## PROPOSTA - LEASING

---

1

- Struttura dell'edificio è su 6 piani

2

- Dispositivi totali 120 computer in leasing per 60 mesi

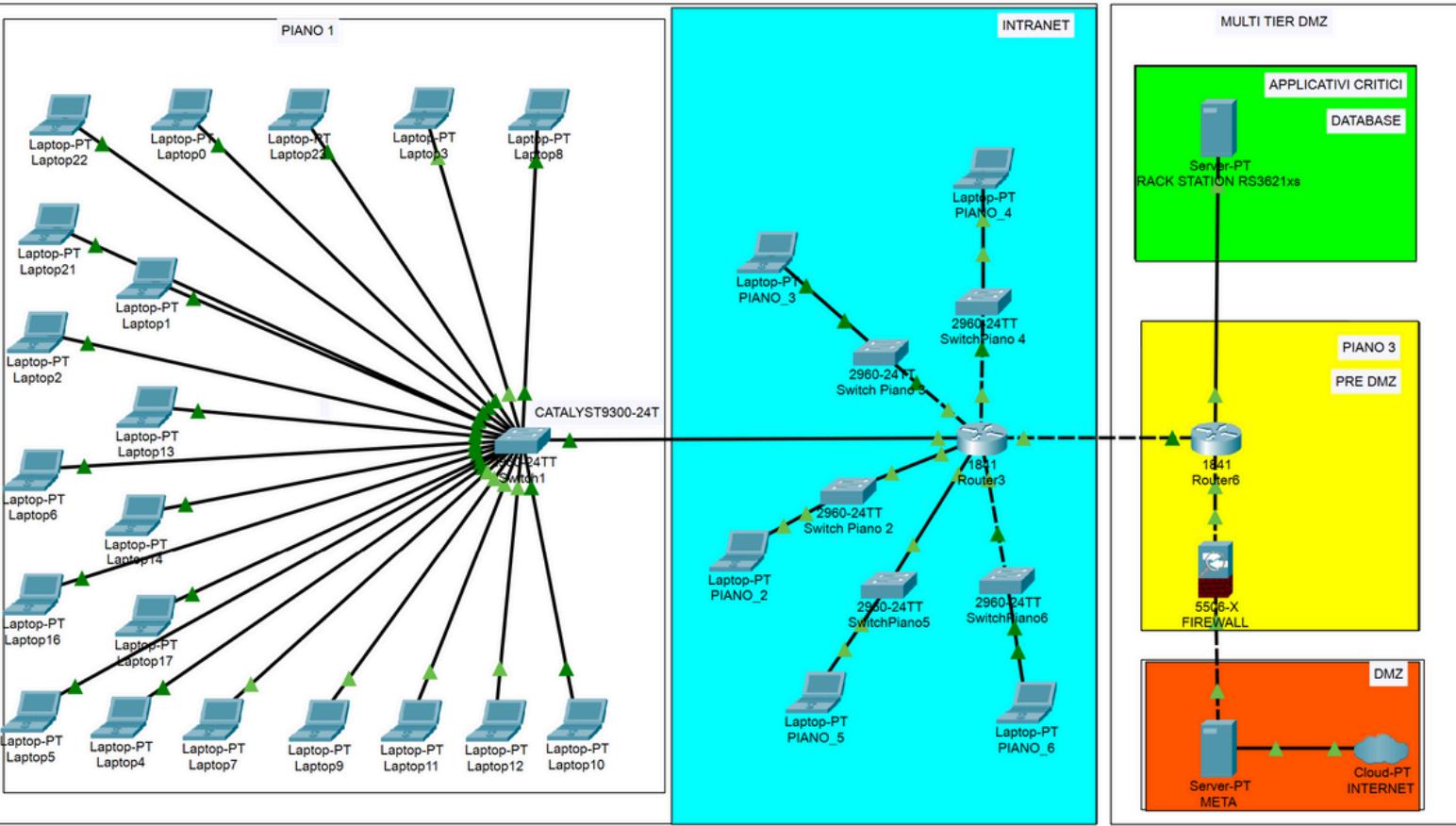
3

Componenti richiesti

- Web server
- Firewall perimetrale
- NAS
- 3 IDS/IPS



# RETE



## RETE

- Tutti i 20 PC del piano sono collegati a uno switch.
- Lo switch indirizza il traffico verso il router centrale che è al 3 piano.

## INTRANET - ROUTER IDS

- Collegato a un altro router/IDS (CISCO ASR 1002-HX) che separa il traffico tra DMZ e Database.
- Questa separazione garantisce maggiore sicurezza, evitando l'esposizione del database al traffico esterno.

## PIANO 3 – SICUREZZA

- Tutto il sistema è protetto da un Firewall fisico/IPS.
- Router/IDS (CISCO ASR 1002-HX) che controlla il traffico interno.
- Il firewall blocca il traffico esterno verso l'Intranet.
- Agisce attivamente contro minacce e intrusioni provenienti dalla rete esterna.

## APPLICATIVI CRITICI

- Tutto il sistema è protetto da un Firewall fisico/IPS.
- Router/IDS (CISCO ASR 1002-HX) che controlla il traffico interno.
- Il firewall blocca il traffico esterno verso l'Intranet.
- Agisce attivamente contro minacce e intrusioni provenienti dalla rete esterna.



## PROPOSTA – LEASING

Hardware	Quantità	Prezzo Unitario (€)	Totale (€)
<b>Laptop in leasing (DELL XPS – iCore 7)</b>	120	4.245,60	509.472,00 (in 60 mesi)
<b>Synology RackStation RS3621xs+</b>	1	4.600	4.600
<b>HDD Red</b>	5	376	1.880
<b>Cisco Firepower 2120</b>	1	1.998	1.998
<b>Switch Cisco Catalyst 9300- 24T-E</b>	6	1.875	11.250
<b>Cisco ASR 1002-HX</b>	1	29.995	29.995
<b>Cisco 3120 NGFW</b>	1	28.487,30	28.487,30
<b>Totale Hardware Ivato</b>			<b>587.682,30</b>





## PROPOSTA – SERVIZI EXTRA

Elemento	Quantità	Prezzo Unitario (€)	Totale (€)
<b>Cablaggio Cat8 (per 120 computer)</b>	1800 metri	4,50	8100,00
<b>Connettori RJ45</b>	240	0,50	120,00
<b>Pannelli di Patch</b>	6	150,00	900,00
<b>Installazione Firewall</b>	1	200,00	200,00
<b>Installazione Router</b>	1	200,00	200,00
<b>Installazione Switch</b>	6	150,00	900,00
<b>Installazione IPS</b>	3	250,00	750,00
<b>Manodopera per Installazione PC</b>	120 ore	50,00	6.000,00
<b>Manodopera per Configurazione Rete</b>	80 ore	70,00	5.600,00
<b>Totale Manodopera e Cablaggio Ivato</b>			<b>22.770,00</b>

- TOTALE HARDWARE + MANODOPERA:  
610.452,30 €
- ASSISTENZA ANNUALE (10%) COSTO:  
61.045,23 €
- TOTALE CON ASSISTENZA ANNUALE:  
671.497,53 €



2°

## PROPOSTA - ACQUISTO

---

1

- Struttura dell'edificio è su 6 piani

2

- Dispositivi totali 120 computer - Dell Latitude i7

3

Componenti richiesti

- Web server
- Firewall perimetrale
- NAS
- 3 IDS/IPS



2°

# PROPOSTA - ACQUISTO

Hardware	Quantità	Prezzo Unitario (€)	Totale (€)
<b>Laptop in leasing (DELL XPS – iCore 7)</b>	120	1.100,00	132.000,00
<b>Synology RackStation RS3621xs+</b>	1	4.600,00	4.600,00
<b>HDD Red</b>	5	376,00	1.880,00
<b>Cisco Firepower 2120</b>	1	1.998,00	1.998,00
<b>Switch Cisco Catalyst 9300-24T-E</b>	6	1.875,00	11.250,00
<b>Cisco ASR 1002-HX</b>	1	29.995,00	29.995,00
<b>Cisco 3120 NGFW</b>	3	28.487,30	85.461,89
<b>Totale Hardware</b>			<b>266.184,89</b>



## PROPOSTA – SERVIZI EXTRA

Elemento	Quantità	Prezzo Unitario (€)	Totale (€)
<b>Cablaggio Cat8 (per 120 computer)</b>	1800 metri	4,50	8100,00
<b>Connettori RJ45</b>	240	0,50	120,00
<b>Pannelli di Patch</b>	6	150,00	900,00
<b>Installazione Firewall</b>	1	200,00	200,00
<b>Installazione Router</b>	1	200,00	200,00
<b>Installazione Switch</b>	6	150,00	900,00
<b>Installazione IPS</b>	3	250,00	750,00
<b>Manodopera per Installazione PC</b>	120 ore	50,00	6.000,00
<b>Manodopera per Configurazione Rete</b>	80 ore	70,00	5.600,00
<b>Totale Manodopera e Cablaggio Ivato</b>			<b>22.770,00</b>

- TOTALE HARDWARE + MANODOPERA:  
288.954,89 €
- ASSISTENZA ANNUALE (10%) COSTO STIMATO: 28.895,49 €
- TOTALE OPZIONE 1 CON ASSISTENZA ANNUALE: 317.850,38 €



3°

## PROPOSTA – PRO ADVISOR

1

- Struttura dell'edificio è su 6 piani

2

- Dispositivi totali 120 computer – Dell Latitude i7

3

Componenti per ridondanza

- Web server
- 2 Firewall perimetrali
- 2 Router
- NAS
- 5 IDS/IPS



3°

## PROPOSTA – PRO ADVISOR

Elemento	Quantità	Prezzo Unitario (€)	Totale (€)
Laptop (acquisto + licenze + antivirus)	120	1100	132.000,00
Synology RackStation RS3621xs+	1	4.600,00	4.600,00
HDD Red	5	376,00	1.880,00
Firepower 2120	2	1.998,00	3.996,00
Switch Cisco Catalyst 9300-24T-E	6	1.875,00	11.250,00
Cisco ASR 1002-HX (IVA inclusa)	2	29.995,00	59.990,00
Cisco 3120 NGFW	1	28.487,30	28.487,30
<b>Totale Hardware Iva</b>			<b>242.203,30</b>



3°

## PROPOSTA – SERVIZI EXTRA

Elemento	Quantità	Prezzo Unitario (€)	Totale (€)
<b>Cablaggio Cat8 (per 120 computer)</b>	1800 metri	4,50	8100,00
<b>Connettori RJ45</b>	240	0,50	120,00
<b>Pannelli di Patch</b>	6	150,00	900,00
<b>Installazione Firewall</b>	1	200,00	200,00
<b>Installazione Router</b>	1	200,00	200,00
<b>Installazione Switch</b>	6	150,00	900,00
<b>Installazione IPS</b>	3	250,00	750,00
<b>Manodopera per Installazione PC</b>	120 ore	50,00	6.000,00
<b>Manodopera per Configurazione Rete</b>	80 ore	70,00	5.600,00
<b>Totale Manodopera e Cablaggio Ivato</b>			<b>22.770,00</b>

- TOTALE HARDWARE + MANODOPERA:  
264.973,30 €
- ASSISTENZA ANNUALE (10%) COSTO STIMATO: 26.497,33 €
- TOTALE OPZIONE 1 CON ASSISTENZA ANNUALE: 291.470,63 €



4°

## PROPOSTA – WOLF ELITE

---

1

- Struttura dell'edificio è su 6 piani

2

- Dispositivi totali 120 computer – Dell Latitude i7

3

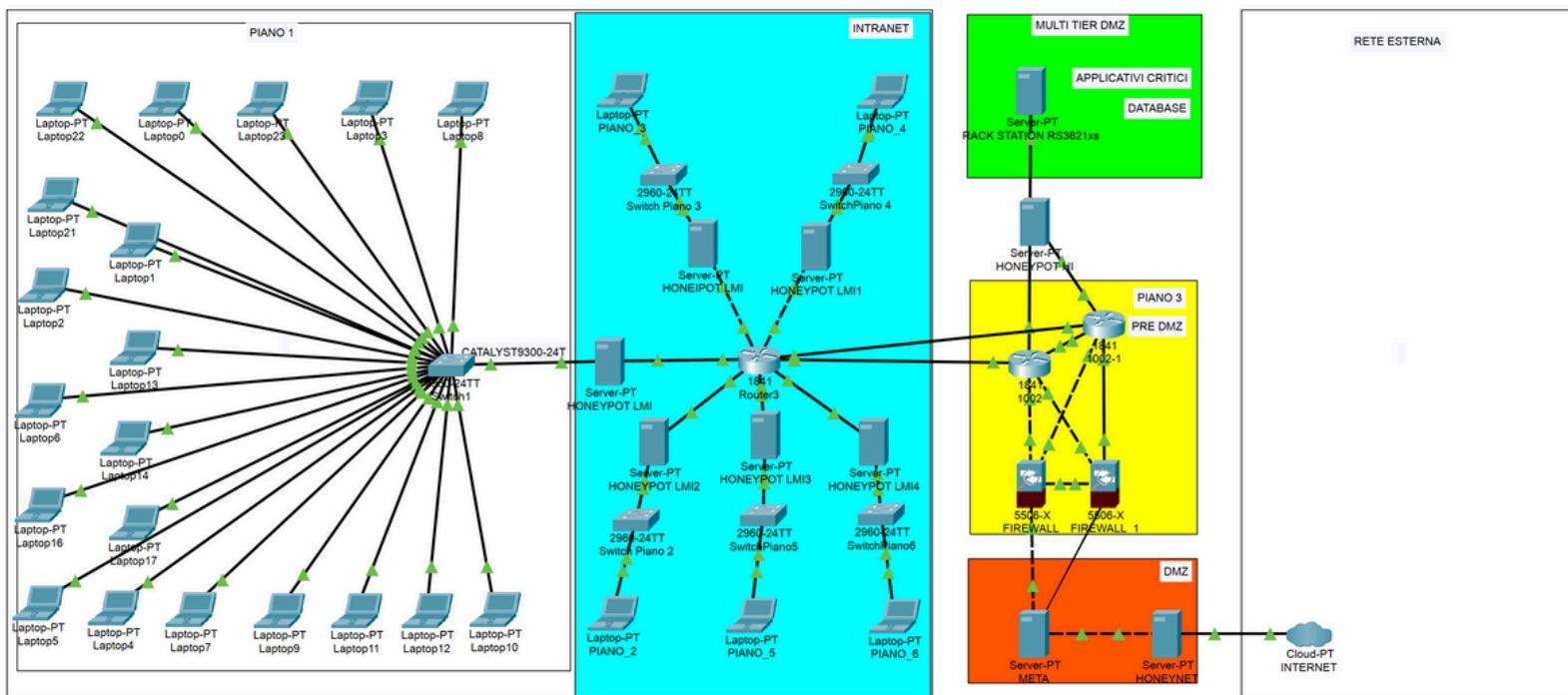
Componenti per ridondanza

- web server
- 2 Firewall perimetrali
- 2 Router
- NAS
- 5 IDS/IPS
- Layered Honeypots
- Honeynet





# RETE



## RETE

- Tutti i 20 PC del piano sono collegati a uno switch.
- Lo switch indirizza il traffico verso il router centrale che è al 3 piano.

## INTRANET – ROUTER IDS

- Collegato a un altro router/IDS (CISCO ASR 1002-HX) che separa il traffico tra DMZ e Database.
- Questa separazione garantisce maggiore sicurezza, evitando l'esposizione del database al traffico esterno.

## PIANO 3 – SICUREZZA

- Tutto il sistema è protetto da un Firewall fisico/IPS.
- Router/IDS (CISCO ASR 1002-HX) che controlla il traffico interno.
- Il firewall blocca il traffico esterno verso l'Intranet.
- Agisce attivamente contro minacce e intrusioni provenienti dalla rete esterna.

## APPLICATIVI CRITICI

- Fornisce servizi e indirizzi IP a tutti i dispositivi interni tramite il protocollo DHCP.
- Configurato per impedire l'eliminazione, il caricamento e la modifica dei dati.
- Il router/IDS notificherà all'amministratore in caso di tentativi di manomissione.



## PROPOSTA – WOLF ELITE

Elemento	Quantità	Prezzo Unitario (€)	Totale (€)
Laptop (acquisto + licenze + antivirus)	120	1100	132.000,00
Synology RackStation RS3621xs+	1	4.600,00	4.600,00
HDD Red	5	376,00	1.880,00
Firepower 2120	2	1.998,00	3.996,00
Switch Cisco Catalyst 9300-24T-E	6	1.875,00	11.250,00
Cisco ASR 1002-HX (IVA inclusa)	2	29.995,00	59.990,00
Cisco 3120 NGFW	1	28.487,30	28.487,30
<b>Totale Hardware Iva</b>			<b>242.203,30</b>



## PROPOSTA – SERVIZI EXTRA

Elemento	Quantità	Prezzo Unitario (€)	Totale (€)
<b>Cablaggio Cat8 (per 120 computer)</b>	1800 metri	4,50	8.100,00
<b>Connettori RJ45</b>	240	0,50	120,00
<b>Pannelli di Patch</b>	6	150,00	900,00
<b>Installazione Firewall</b>	1	200,00	200,00
<b>Installazione Router</b>	1	200,00	200,00
<b>Installazione Switch</b>	6	150,00	900,00
<b>Installazione IPS</b>	3	250,00	750,00
<b>Manodopera per Installazione PC</b>	120 ore	50,00	6.000,00
<b>Manodopera per Configurazione Rete</b>	80 ore	70,00	5.600,00
<b>Honeypot a bassa interazione</b>	6	500,00	3.000,00
<b>Honeypot a media interazione</b>	2	1.000,00	2.000,00
<b>Honeypot ad alta interazione</b>	2	2.500,00	5.000,00
<b>Implementazione Honeynet interna</b>	1	8.000,00	8.000,00
<b>Totale Manodopera e Cablaggio Ivato</b>			<b>40.770,00</b>





# LONG SUPPORT



1

- **Totale Hardware + Manodopera:**  
**€ 264.973,30**

2

- **Assistenza Annuale inclusa Formazione Periodica (10%):**  
**€ 26.497,33**

3

- **Totale Complessivo:**  
**€ 291.470,63**

"*Tutto quello di cui hai bisogno per essere al sicuro, oggi e domani.*"

"*Investi nella tranquillità, con un sistema progettato per resistere alle minacce.*"



# CISCO FIREPOWER 2120

## DESCRIZIONE GENERALE

- Firewall di nuova generazione progettato per offrire protezione avanzata contro minacce e intrusi.
- Soluzione integrata di sicurezza che combina:
- Prevenzione delle Intrusioni (IPS)
- Protezione avanzata contro malware
- Filtraggio dei contenuti

## LAYER DI RIFERIMENTO OSI

- Layer 2 (Data Link):
- Supporta bridging e switch per il monitoraggio del traffico sulla rete.
- Layer 3 (Network):
- Include routing, filtraggio IP, NAT e segmentazione della rete.
- Layer 4 (Transport):
- Filtra il traffico basato su protocolli come TCP e UDP.
- Layer 7 (Application):
- Ispezione e controllo del traffico applicativo (HTTP, HTTPS, ecc.).

## FUNZIONALITÀ PRINCIPALI

- Prevenzione delle Intrusioni (IPS):
- Blocca minacce note e sconosciute in tempo reale.
- Advanced Malware Protection (AMP):
- Protezione contro malware avanzato con funzionalità di sandboxing.
- URL Filtering:
- Controllo dell'accesso ai siti web basato su categorie predefinite.
- VPN (Virtual Private Network):
- Supporta connessioni VPN sicure per accesso remoto.

## SCALABILITÀ E PRESTAZIONI

- Progettato per piccole e medie imprese, scalabile con l'aumento delle esigenze di sicurezza.
- Prestazioni firewall fino a 3 Gbps, supporta migliaia di connessioni simultanee.



# CISCO ASR 1002-HX ROUTER

## DESCRIZIONE GENERALE

Il Cisco ASR 1002-HX è un router di fascia alta progettato per gestire grandi volumi di traffico dati e garantire alta disponibilità. È ideale per reti aziendali che richiedono prestazioni elevate e funzionalità avanzate di routing.

## LAYER DI RIFERIMENTO OSI

- Layer 2 (Data Link):
- Supporta tecnologie WAN come Ethernet, MPLS, e Frame Relay.
- Layer 3 (Network):
- Implementa protocolli di routing dinamico come OSPF, BGP, e EIGRP per la gestione avanzata del traffico IP.
- Layer 4 (Transport):
- Gestisce il traffico TCP/UDP con funzionalità avanzate di QoS (Quality of Service) e load balancing.
- Layer 7 (Application):
- Supporta servizi di rete avanzati, come deep packet inspection (DPI) e servizi applicativi integrati.

## FUNZIONALITÀ PRINCIPALI

- Routing Dinamico:
- Supporta protocolli di routing avanzati per gestire il traffico in modo efficiente.
- QoS (Quality of Service):
- Permette di prioritizzare il traffico di rete critico per applicazioni specifiche, garantendo prestazioni ottimali.
- VPN:
- Supporta VPN su larga scala con capacità di cifratura hardware.
- High Availability:
- Include funzionalità di ridondanza e failover per garantire alta disponibilità.

## SCALABILITÀ E PRESTAZIONI

- Supporta fino a 200 Gbps di throughput aggregato.
- Capacità di gestire milioni di pacchetti al secondo, ideale per ambienti ad alta intensità di dati.



# CISCO 3120 NGFW (NEXT GENERATION FIREWALL)

## **CISCO 3120 NGFW (NEXT GENERATION FIREWALL)**

Il Cisco 3120 NGFW è stato selezionato per rafforzare ulteriormente la sicurezza della rete aziendale. Con la sua capacità di ispezione approfondita dei pacchetti (DPI), protezione contro le intrusioni e monitoraggio continuo delle minacce, questo firewall offre una protezione multilivello che è fondamentale per un'azienda che si affida a operazioni sicure e ininterrotte. La sua scalabilità e capacità di gestione del traffico ad alte prestazioni lo rendono ideale per un ambiente in cui la sicurezza non può essere compromessa.



# SWITCH CISCO CATALYST 9300-24T-E



## DESCRIZIONE GENERALE

Il Cisco Catalyst 9300-24T-E è uno switch di rete di fascia enterprise, ottimizzato per la gestione di reti ad alte prestazioni. È particolarmente adatto per ambienti che richiedono alta densità di porte e funzionalità avanzate di switching.

## LAYER DI RIFERIMENTO OSI

- Layer 2 (Data Link): Fornisce switching Layer 2 con supporto per VLAN, spanning tree, e aggregazione di link.
- Layer 3 (Network): Include funzionalità di routing inter-VLAN, routing statico e dinamico.
- Layer 4 (Transport): Supporta QoS e ACL (Access Control Lists) per il controllo avanzato del traffico.

## FUNZIONALITÀ PRINCIPALI

- Stacking: Supporta l'empilamento fisico fino a 8 switch, permettendo la gestione centralizzata e l'espansione della rete.
- Supporto per SD-Access: Integrato con Cisco DNA, consente la gestione automatizzata della rete e la segmentazione basata su policy.
- Security Features: Include Cisco TrustSec per la segmentazione della rete e la protezione delle risorse aziendali.
- Power over Ethernet (PoE): Alimenta dispositivi come telefoni IP e access point wireless direttamente tramite le porte Ethernet.

## SCALABILITÀ E PRESTAZIONI

- Progettato per supportare fino a 24 porte 10 Gbps, con capacità di aggregazione fino a 480 Gbps.
- Supporta applicazioni ad alta densità di banda, ideale per ambienti aziendali complessi.



# HONEYPOTS

## HONEYPOT A BASSA E MEDIA INTERAZIONE

- Posizione: Distribuiti sui vari piani, in prossimità dei 6 switch Cisco Catalyst 9300-24T-E, vicino ai computer e in punti strategici della rete.
- Obiettivo: Rilevare attacchi comuni e automatizzati, come tentativi di accesso non autorizzato agli switch o attacchi alle interfacce di rete esposte.

## HONEYPOT AD ALTA INTERAZIONE

- Posizione: Prossimo al router Cisco ASR 1002-HX e al NAS Synology RS3621xs+. Questi honeypot saranno più realistici e saranno posizionati per attirare attacchi sofisticati diretti a infrastrutture critiche come il vostro NAS o router aziendale.
- Obiettivo: Monitorare tentativi di compromissione più avanzati e tecniche di persistenza da parte di attaccanti più qualificati.

# HONEYNET

## HONEYNET INTERNA

- Posizione: Simulerà un'intera rete interna, comprensiva di servizi vulnerabili come il server aziendale con DVWA e Metasploit, creando un ambiente che attira attacchi complessi e avanzati.
- Obiettivo: Raccogliere dati su tecniche di movimento laterale e tentativi di sfruttamento all'interno della rete, simulando una compromissione completa dell'infrastruttura.

## MONITORAGGIO CENTRALIZZATO E GESTIONE DEI LOG

Un sistema centralizzato raccoglierà i log di tutte le interazioni sugli honeypot e sulla honeynet. Potrà essere integrato con strumenti come Elastic Stack o Splunk, permettendo una gestione efficiente e in tempo reale dei dati generati.



# SYNOLOGY RACKSTATION RS3621XS E HDD WD RED PRO 10 TB

## SYNOLOGY RACKSTATION RS3621XS+

Il Synology RackStation RS3621xs+ è una soluzione NAS (Network Attached Storage) di fascia alta, progettata per fornire una gestione centralizzata dei dati. Offre prestazioni elevate con una capacità di espansione flessibile, ideale per aziende che necessitano di un'archiviazione sicura e scalabile. Supporta fino a 12 drive, con un'architettura potente per gestire carichi di lavoro intensivi.

## WESTERN DIGITAL RED PRO 10 TB

Il WD Red Pro 10 TB è un hard disk ottimizzato per l'uso in ambienti NAS, progettato per garantire affidabilità e prestazioni elevate. Ideale per carichi di lavoro intensivi, offre una capacità di archiviazione significativa con una velocità di trasferimento dati ottimizzata per le configurazioni multi-drive. Perfetto per le aziende che necessitano di una soluzione di archiviazione robusta e duratura.



# ANALISI FORENSE

## DESCRIZIONE GENERALE SCANSIONE PORTE 1

```
/bin/python  
"/home/sushanto/Documenti/prove/Scansione  
porte.py"  
  [sushanto@parrot]—[~/Documenti/prove]  
      $/bin/python  
"/home/sushanto/Documenti/prove/Scansione  
porte.py"  
Inserisci l'IP o l'hostname da scansionare:  
192.168.50.151
```

Dettagli delle Porte Aperte:

Porta 21: Aperta  
Protocollo: FTP (controllo)  
Livello ISO/OSI: Livello 4 - Trasporto  
Descrizione: Trasferimento di file tra client e server.

Porta 22: Aperta  
Protocollo: SSH  
Livello ISO/OSI: Livello 4 - Trasporto  
Descrizione: Accesso remoto sicuro e crittografato ai sistemi.

Porta 23: Aperta  
Protocollo: Telnet  
Livello ISO/OSI: Livello 4 - Trasporto  
Descrizione: Accesso remoto a dispositivi tramite una connessione TCP.

Porta 25: Aperta  
Protocollo: Sconosciuto  
Livello ISO/OSI: Sconosciuto  
Descrizione: N/D

Porta 53: Aperta  
Protocollo: Sconosciuto  
Livello ISO/OSI: Sconosciuto  
Descrizione: N/D

Porta 80: Aperta  
Protocollo: HTTP  
Livello ISO/OSI: Livello 7 - Applicazione  
Descrizione: Trasmissione di pagine web e dati su Internet.

Porta 111: Aperta  
Protocollo: Sconosciuto  
Livello ISO/OSI: Sconosciuto  
Descrizione: N/D

Porta 139: Aperta  
Protocollo: NetBIOS (Session Service)  
Livello ISO/OSI: Livello 4 - Trasporto  
Descrizione: Servizi di comunicazione tra computer su una rete locale.

Porta 445: Aperta  
Protocollo: SMB  
Livello ISO/OSI: Livello 4 - Trasporto  
Descrizione: Condivisione di file, stampanti e risorse di rete.

Porta 512: Aperta  
Protocollo: Sconosciuto  
Livello ISO/OSI: Sconosciuto  
Descrizione: N/D

Porta 513: Aperta  
Protocollo: Sconosciuto  
Livello ISO/OSI: Sconosciuto  
Descrizione: N/D

Porta 514: Aperta  
Protocollo: Sconosciuto  
Livello ISO/OSI: Sconosciuto  
Descrizione: N/D

Porta 1099: Aperta  
Protocollo: Sconosciuto  
Livello ISO/OSI: Sconosciuto  
Descrizione: N/D

Porta 1524: Aperta  
Protocollo: Sconosciuto  
Livello ISO/OSI: Sconosciuto  
Descrizione: N/D

Porta 2049: Aperta  
Protocollo: Sconosciuto  
Livello ISO/OSI: Sconosciuto  
Descrizione: N/D

Porta 2121: Aperta  
Protocollo: Sconosciuto  
Livello ISO/OSI: Sconosciuto  
Descrizione: N/D

Porta 3306: Aperta  
Protocollo: Sconosciuto  
Livello ISO/OSI: Sconosciuto  
Descrizione: N/D



# ANALISI FORENSE

## DESCRIZIONE GENERALE SCANSIONE PORTE 2

Porta 3632: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porta 5432: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porta 5900: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porta 6000: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porta 6667: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porta 6697: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porta 8009: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porta 8180: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porta 8787: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porta 33542: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porta 39646: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porta 45213: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porta 57526: Aperta

Protocollo: Sconosciuto

Livello ISO/OSI: Sconosciuto

Descrizione: N/D

Porte Chiuse:

1 - 20, 24, 26 - 52, 54 - 79, 81 - 110, 112 - 138, 140 - 444, 446 - 511, 515 - 1098, 1100 - 1523, 1525 - 2048, 2050 - 2120, 2122 - 3305, 3307 - 3631, 3633 - 5431, 5433 - 5899, 5901 - 5999, 6001 - 6666, 6668 - 6696, 6698 - 8008, 8010 - 8179, 8181 - 8786, 8788 - 33541, 33543 - 39645, 39647 - 45212, 45214 - 57525, 57527 - 65535

Porte Aperte:

21 - 23, 25, 53, 80, 111, 139, 445, 512 - 514, 1099, 1524, 2049, 2121, 3306, 3632, 5432, 5900, 6000, 6667, 6697, 8009, 8180, 8787, 33542, 39646, 45213, 57526

Nessun errore riscontrato durante la scansione.

└─[sushanto@parrot]─[~/Documenti/prove]



# REPORT

## SCANSIONE DELLE PORTE SU META

### PORTE COMUNEMENTE UTILIZZATE E POTENZIALI RISCHI

Porta 21: FTP (File Transfer Protocol) – non sicura, usa SFTP sulla porta 22 se possibile.  
Porta 22: SSH (Secure Shell) – sicura, ma deve essere monitorata per evitare accessi non autorizzati.  
Porta 23: Telnet – altamente insicura, da evitare o sostituire con SSH.  
Porta 25: SMTP (Simple Mail Transfer Protocol) – usata per l'invio di email, può essere sfruttata per spam.  
Porta 53: DNS (Domain Name System) – essenziale, ma può essere target di attacchi DDoS o avvelenamento DNS.  
Porta 80: HTTP (HyperText Transfer Protocol) – traffico web non criptato, meglio utilizzare HTTPS sulla porta 443.  
Porta 111: RPC (Remote Procedure Call) – vulnerabile a exploit remoti.  
Porta 135: Microsoft RPC – legata a vulnerabilità di Windows come attacchi DCOM.  
Porta 137-139: NetBIOS – associata a condivisione file su reti Windows, vulnerabile a exploit.  
Porta 443: HTTPS (HyperText Transfer Protocol Secure) – porta per traffico web criptato, da lasciare aperta solo con certificati validi.  
Porta 445: SMB (Server Message Block) – bersaglio di malware come WannaCry.  
Porta 3389: RDP (Remote Desktop Protocol) – vulnerabile a brute force e exploit se non ben protetta

### ALTRÉ PORTE COMUNI A CUI PRESTARE ATTENZIONE

Porta 5900: VNC (Virtual Network Computing) – utilizzata per accessi remoti, da proteggere adeguatamente.  
Porta 3306: MySQL – database, da proteggere con firewall e accessi limitati.  
Porta 5432: PostgreSQL – simile a MySQL, va ben protetta.

### PORTE SPECIFICHE

Porta 23 (Telnet): Insicura e da evitare a favore di SSH.  
Porta 512-514: Rlogin/Rsh – protocolli vecchi e insicuri, da evitare.  
Porta 6667: IRC (Internet Relay Chat) – può essere usata per canali di comando e controllo dei bot.  
Porta 8080, 8180: HTTP alternativo o applicazioni di sviluppo.



```
import socket Python

# Mappatura delle porte ai protocolli, livelli ISO/OSI e descrizioni
protocolli_iso_osi = {
    20: {'protocollo': 'FTP (dati)', 'livello': 'Livello 4 - Trasporto', 'descrizione': 'Trasferimento di file tra client e server.'},
    21: {'protocollo': 'FTP (controllo)', 'livello': 'Livello 4 - Trasporto', 'descrizione': 'Trasferimento di file tra client e server.'},
    22: {'protocollo': 'SSH', 'livello': 'Livello 4 - Trasporto', 'descrizione': 'Accesso remoto sicuro e crittografato ai sistemi.'},
    23: {'protocollo': 'Telnet', 'livello': 'Livello 4 - Trasporto', 'descrizione': 'Accesso remoto a dispositivi tramite una connessione TCP.'},
    67: {'protocollo': 'DHCP (server)', 'livello': 'Livello 4 - Trasporto', 'descrizione': 'Assegna automaticamente indirizzi IP e parametri di rete.'},
    68: {'protocollo': 'DHCP (client)', 'livello': 'Livello 4 - Trasporto', 'descrizione': 'Assegna automaticamente indirizzi IP e parametri di rete.'},
    80: {'protocollo': 'HTTP', 'livello': 'Livello 7 - Applicazione', 'descrizione': 'Trasmissione di pagine web e dati su Internet.'},
    137: {'protocollo': 'NetBIOS (Name Service)', 'livello': 'Livello 4 - Trasporto', 'descrizione': 'Servizi di comunicazione tra computer su una rete locale.'},
    138: {'protocollo': 'NetBIOS (Datagram Service)', 'livello': 'Livello 4 - Trasporto', 'descrizione': 'Servizi di comunicazione tra computer su una rete locale.'},
    139: {'protocollo': 'NetBIOS (Session Service)', 'livello': 'Livello 4 - Trasporto', 'descrizione': 'Servizi di comunicazione tra computer su una rete locale.'},
    143: {'protocollo': 'IMAP (standard)', 'livello': 'Livello 7 - Applicazione', 'descrizione': 'Accesso e sincronizzazione di email sui server.'},
    443: {'protocollo': 'HTTPS', 'livello': 'Livello 7 - Applicazione', 'descrizione': 'Versione sicura di HTTP che utilizza SSL/TLS per criptare i dati.'},
    445: {'protocollo': 'SMB', 'livello': 'Livello 4 - Trasporto', 'descrizione': 'Condivisione di file, stampanti e risorse di rete.'},
    465: {'protocollo': 'SMTP (over SSL)', 'livello': 'Livello 7 - Applicazione', 'descrizione': 'Invio di email tra server di posta.'},
    587: {'protocollo': 'SMTP (sicuro con STARTTLS)', 'livello': 'Livello 7 - Applicazione', 'descrizione': 'Invio di email tra server di posta.'},
    993: {'protocollo': 'IMAP (sicuro con SSL/TLS)', 'livello': 'Livello 7 - Applicazione', 'descrizione': 'Accesso e sincronizzazione di email sui server.'},
    995: {'protocollo': 'POP (sicuro con SSL/TLS)', 'livello': 'Livello 7 - Applicazione', 'descrizione': 'Scaricamento di email dai server.'},
    110: {'protocollo': 'POP (standard)', 'livello': 'Livello 7 - Applicazione', 'descrizione': 'Scaricamento di email dai server.'},
    161: {'protocollo': 'SNMP', 'livello': 'Livello 7 - Applicazione', 'descrizione': 'Monitoraggio e gestione dei dispositivi di rete.'},
    162: {'protocollo': 'SNMPTRAP', 'livello': 'Livello 7 - Applicazione', 'descrizione': 'Monitoraggio e gestione dei dispositivi di rete.'},
    989: {'protocollo': 'FTPS (dati espliciti)', 'livello': 'Livello 4 - Trasporto', 'descrizione': 'Variante sicura di FTP che utilizza SSL/TLS per cifrare i dati.'},
    990: {'protocollo': 'FTPS (dati impliciti)', 'livello': 'Livello 4 - Trasporto', 'descrizione': 'Variante sicura di FTP che utilizza SSL/TLS per cifrare i dati.'},
    8880: {'protocollo': 'HTTP', 'livello': 'Livello 7 - Applicazione', 'descrizione': 'Trasmissione di pagine web e dati su Internet.'}
}

def scansione_porte(host, porte):
    aperte = []
    dettagli_aperte = {}
    chiuse = []
    errori = []

    for porta in porte:
        try:
            s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
            s.settimeout(1)
            risultato = s.connect_ex((host, porta))
            if risultato == 0:
                aperte.append(porta)
                stato_porta = 'Aperta'
                if porta in protocolli_iso_osi:
                    info_protocolli = protocolli_iso_osi[porta]
                    dettagli_aperte[porta] = [
                        'stato': stato_porta,
                        'protocollo': info_protocolli['protocollo'],
                        'livello': info_protocolli['livello'],
                        'descrizione': info_protocolli['descrizione']
                    ]
            else:
                chiuse.append(porta)
        except:
            errori.append(porta)

    return aperte, dettagli_aperte, chiuse, errori
```



```
        else:
            chiuse.append(porta)
    except Exception as e:
        errori.append(f"Errore sulla porta {porta}: {str(e)}")
    finally:
        s.close()

    return aperte, dettagli_aperte, chiuse, errori

def formatta_porte(porte):
    if not porte:
        return "Nessuna porta trovata."

    porte.sort()
    range_porte = []
    inizio = porte[0]
    fine = porte[0]

    for i in range(1, len(porte)):
        if porte[i] == fine + 1:
            fine = porte[i]
        else:
            if inizio == fine:
                range_porte.append(f"{inizio}")
            else:
                range_porte.append(f"{inizio} - {fine}")
            inizio = porte[i]
            fine = porte[i]

    if inizio == fine:
        range_porte.append(f"{inizio}")
    else:
        range_porte.append(f"{inizio} - {fine}")

    return ", ".join(range_porte)

# Chiedi all'utente di inserire l'host
host = input("Inserisci l'IP o l'hostname da scansionare: ")
porte = range(1, 65536) # Scansione di tutte le porte da 1 a 65535
aperte, dettagli_aperte, chiuse, errori = scansione_porte(host, porte)

# Stampa i dettagli delle porte aperte
if aperte:
    print("\nDettagli delle Porte Aperte:")
    for porta in aperte:
        info = dettagli_aperte[porta]
        print(f"Porta {porta}: {info['stato']}")
        print(f"Protocollo: {info['protocollo']}")
        print(f"Livello ISO/OSI: {info['livello']}")
        print(f"Descrizione: {info['descrizione']}\n")

# Stampa l'array delle porte chiuse in un formato compatto
print("\nPorte Chiuse:")
print(formatta_porte(chiuse))

# Stampa l'array delle porte aperte in un formato compatto
if aperte:
    print("\nPorte Aperte:")
    print(formatta_porte(aperte))
else:
    print("\nNessuna porta aperta trovata.")

# Stampa eventuali errori
if errori:
    print("\nErrori riscontrati durante la scansione:")
    for errore in errori:
        print(errore)
else:
    print("\nNessun errore riscontrato durante la scansione.")
```



# ANALISI FORENSE

## DESCRIZIONE GENERALE SCANSIONE VERBI HTTP

```
— [sushanto@parrot] — [~/Documenti/prove]
  — $ /bin/python "/home/sushanto/Documenti/prove/Scansione verbi HTTP.py"
Inserisci l'URL da verificare: http://192.168.50.151/phpMyAdmin/
```

--- GET ---

Status Code: 200 – OK: La richiesta è stata eseguita con successo.  
Content: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"  
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="ltr">  
<head>  
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />  
 <link rel="icon" href="./favicon.ico" type="image/x-icon" />  
 <link rel="shortcut icon" href="./favicon.ico" type="image/x-icon" />  
 <title>phpMyAdmin </title>  
 <link rel="stylesheet" type="text/css" hr...>

--- POST ---

Status Code: 200 – OK: La richiesta è stata eseguita con successo.  
Content: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"  
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="ltr">  
<head>  
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />  
 <link rel="icon" href="./favicon.ico" type="image/x-icon" />  
 <link rel="shortcut icon" href="./favicon.ico" type="image/x-icon" />  
 <title>phpMyAdmin </title>  
 <link rel="stylesheet" type="text/css" hr...>

--- PUT ---

Status Code: 200 – OK: La richiesta è stata eseguita con successo.  
Content: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"  
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="ltr">  
<head>  
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />  
 <link rel="icon" href="./favicon.ico" type="image/x-icon" />  
 <link rel="shortcut icon" href="./favicon.ico" type="image/x-icon" />  
 <title>phpMyAdmin </title>  
 <link rel="stylesheet" type="text/css" hr...>

--- DELETE ---

Status Code: 200 – OK: La richiesta è stata eseguita con successo.  
Content: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"  
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">  
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en" dir="ltr">  
<head>  
 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />  
 <link rel="icon" href="./favicon.ico" type="image/x-icon" />  
 <link rel="shortcut icon" href="./favicon.ico" type="image/x-icon" />  
 <title>phpMyAdmin </title>  
 <link rel="stylesheet" type="text/css" hr...>

Nessun errore riscontrato.

```
— [sushanto@parrot] — [~/Documenti/prove]
  — $
```



# REPORT

## SCANSIONE DEI VERBI HTTP

### PROBLEMATICHE CON PUT E DELETE

- PUT (200): Questo può essere un segnale di allarme. Il metodo PUT è spesso utilizzato per aggiornare risorse sul server. Se è abilitato senza limitazioni adeguate, un utente malintenzionato potrebbe potenzialmente modificare dati sensibili o caricare file dannosi.
- DELETE (200): Anche questo è preoccupante. Il metodo DELETE dovrebbe essere molto ben controllato. Se un attaccante riesce a inviare richieste DELETE senza restrizioni, potrebbe potenzialmente eliminare dati importanti.

### RISCHI

- phpMyAdmin esposto: Se phpMyAdmin è accessibile pubblicamente con questi verbi HTTP abilitati, è necessario assicurarsi che l'accesso sia adeguatamente protetto con autenticazione e restrizioni IP.
- Test PUT e DELETE: Questi metodi dovrebbero essere bloccati se non strettamente necessari, soprattutto su endpoint critici.

### AZIONI CONSIGLIATE

- Assicurarsi che l'accesso a phpMyAdmin sia protetto da autenticazione e che sia visibile solo a chi ne ha bisogno (ad esempio, limitando l'accesso tramite firewall o VPN).
- Disabilita i metodi PUT e DELETE a meno che non siano necessari e configura le opportune regole di autenticazione e autorizzazione per l'uso di questi metodi.
- Verifica la corretta validazione e filtraggio delle richieste POST, PUT e DELETE per prevenire attacchi come SQL injection, file upload malevolo o cancellazione non autorizzata di dati.



```
def completa_url(url):
    """ Completa l'URL solo se necessario. """
    if not url.startswith(('http://', 'https://')):
        if not url.startswith('www.'):
            url = 'http://www.' + url
        else:
            url = 'http://' + url
    return url

def verifica_http(url):
    """ Verifica i principali metodi HTTP e raccoglie i risultati. """
    metodi = ['GET', 'POST', 'PUT', 'DELETE']
    risultati = {'GET': [], 'POST': [], 'PUT': [], 'DELETE': []}
    errori = []

    for metodo in metodi:
        try:
            risposta = requests.request(metodo, url, timeout=10)
            risposta.raise_for_status() # Solleva un HTTPError per risposte 4xx/5xx
            risultato = {
                'status_code': risposta.status_code,
                'content': risposta.content.decode('utf-8', errors='replace') if risposta.content else ''
            }
            risultati[metodo].append(risultato)
        except requests.exceptions.SSLError as e:
            errori.append({
                'metodo': metodo,
                'error': 'SSLError',
                'descrizione': "Errore SSL, possibile problema con il certificato del server.",
                'dettagli': str(e)
            })
        except requests.exceptions.ConnectionError as e:
            errori.append({
                'metodo': metodo,
                'error': 'ConnectionError',
                'descrizione': "Impossibile stabilire una connessione con il server. Il server potrebbe essere offline, l'IP sbagliato, o la porta non aperta.",
                'dettagli': str(e)
            })
        except requests.exceptions.Timeout as e:
            errori.append({
                'metodo': metodo,
                'error': 'Timeout',
                'descrizione': "Il tempo di attesa per la risposta è scaduto. Il server potrebbe essere lento o ci sono problemi di rete.",
                'dettagli': str(e)
            })
        except requests.exceptions.HTTPError as e:
            errori.append({
                'metodo': metodo,
                'error': 'HTTPError',
                'descrizione': "Errore HTTP ricevuto, indica problemi lato client (4xx) o lato server (5xx).",
                'dettagli': str(e)
            })
        except requests.exceptions.TooManyRedirects as e:
            errori.append({
                'metodo': metodo,
                'error': 'TooManyRedirects',
                'descrizione': "Troppe redirezioni. Potrebbe esserci un loop di redirezioni.",
                'dettagli': str(e)
            })
        except requests.exceptions.RequestException as e:
            errori.append({
                'metodo': metodo,
                'error': 'RequestException',
                'descrizione': "Errore generale relativo alla richiesta HTTP.",
                'dettagli': str(e)
            })

    return risultati, errori
```



```
# Chiede all'utente di inserire l'URL e lo completa automaticamente
url = input("Inserisci l'URL da verificare: ")
url = completa_url(url.strip())

# Esegue la verifica HTTP
risposte, errori = verifica_http(url)

# Stampa le risposte HTTP
for metodo, risultati_metodo in risposte.items():
    if risultati_metodo:
        print(f"\n--- {metodo} ---")
        for risultato in risultati_metodo:
            print(f"Status Code: {risultato.get('status_code', 'N/A')}")
            print(f"Content: {risultato['content'][:500]}...") # Stampa solo i primi 500 caratteri del contenuto
            print()

# Stampa eventuali errori ed eccezioni alla fine
if errori:
    print("\nErrori riscontrati durante la verifica:")
    for errore in errori:
        print(f"--- {errore['metodo']} ---")
        print(f"Errore: {errore['error']}")
        print(f"Descrizione: {errore['descrizione']}")
        print(f"Dettagli: {errore['dettagli']}\n")
else:
    print("\nNessun errore riscontrato.")
```

# ANALISI FORENSE FILE THETA.ZIP

## REPORT SCANSIONE FILE THETA.ZIP

L'amministratore delegato ci ha consegnato un file zip chiamato 'THETA'. A una prima verifica, tutto sembrava normale.

Tuttavia, il team di Wolf Ethical Hackers ha notato qualcosa di strano nelle dimensioni dei file jpg all'interno.

Utilizzando il tool Steghide, hanno scoperto che questi file erano cifrati con l'uso di linguaggi esoterici, come Brainfuck e Cow language.

Inoltre, i file decodificati in base64 rivelavano un altro file che conteneva un messaggio criptato.

All'interno del file 'text.txt' si leggeva: 'Abbiamo svuotato i conti, grazie azienda Theta!'.



“Non sprecate il vostro tempo.  
La vostra sicurezza è la nostra  
sicurezza”

WOLF ETHICAL HACKERS



# MEET OUR TEAM



SUSHANTO ROMA



ANGELO LOMBARDI



NICOLO' BIASIO

MICHELE GUIDO



FRANCESCO LETO



MATTIA DELEU



ANDREA BRANDI



GET  
IN TOUCH

[WWW.WOLFEH.COM](http://WWW.WOLFEH.COM)