



FALCONLOCK
S.P.A.

Home

Video

About Us

Contact



P R E S E N T S

OUR PROJECT FOR THETA



OBIETTIVI:

- Progettazione dell'infrastruttura di rete per la società Theta
- Sviluppo Tools per l'analisi del Web Server
- Mitigazione vulnerabilità Web Server

COMPOSIZIONE TEAM:

- Simeone Cristofaro – **Team Leader**
- Ernesto Mercurio
- Matteo Garau
- Sergio Musto
- Ritish Bantooa
- Andrea Pensierini
- Giuseppe Cevallos
- Alfonso Pio Montalbano

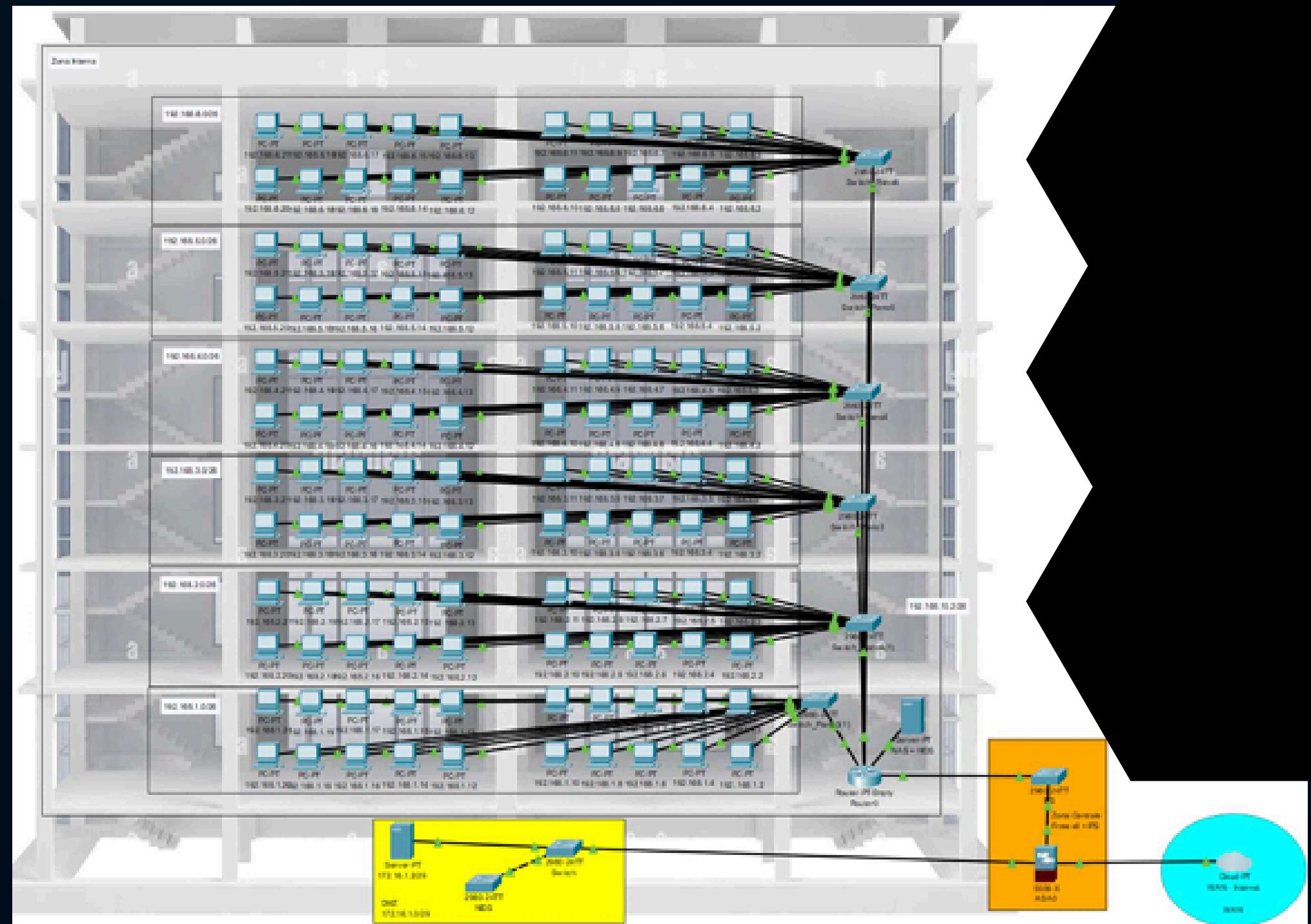
INFRASTRUTTURA

ZONA INTERNA:

- Raggruppa gli uffici dell'azienda Theta che sono disposti su sei piani
- Ogni piano è composto da:
 - 20 personal computer
 - 1 switch 24 porte
- Un router con 8 porte GigabitEthernet
- Un NAS accessibile da tutti i client della zona interna

DMZ:

- Zona a cui è permesso l'accesso dall'esterno della rete aziendale
- I dispositivi presenti non possono contattare la rete interna
- Composta da:
Server Web: DVWA di Metasploitable



ZONA ESTERNA:

- Raffigurata per completezza ma non gestita dalla FalconLock.
- Rete pubblica che permette l'accesso alla WAN.

ZONA CENTRALE:

Assolve i compiti di:

- Collegamento tra le diverse zone che compongono l'infrastruttura
- Filtraggio del traffico tramite la presenza di un Firewall
- Monitoraggio del traffico mediante l'implementazione di:
 - NIDS all'interno della DMZ per ricevere avvisi in caso di attività che richiedano un approfondimento dal SOC
- IPS posto tra il firewall e la rete interna per intervenire prontamente in caso rilevamento di pattern riconosciuti come dannosi



SUBNETS

```
192.168.4.3

Physical Config Desktop Programming Attributes

Command Prompt

C:\> ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.4.1: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\> ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.4.1: Destination host unreachable.

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\> ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127
Reply from 192.168.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

SGUARDO GENERALE:

- Per dividere logicamente i piani degli uffici sono state create 6 subnets.
- Vista la presenza di computer fissi e di numero ben definito si è optato di assegnare staticamente ad ogni client un IP
- Questa scelta permetterà al reparto IT, in caso di necessità, di connettersi da remoto in modo più agevole sapendo a quale IP corrisponde ogni macchina

ESEMPIO DEL PIANO 1:

- IP Network: 192.168.1.0
- Subnetmask: 255.255.255.192
- IP Gateway: 192.168.1.1
- IP Broadcast: 192.168.1.63
- N. Max Hosts: 61 + Gateway

ACL RULES:

- All'interno del Router0 sono state caricate le ACL per bloccare il traffico tra i piani dello stabile consentendo, allo stesso tempo, a tutte le subnets di collegarsi al NAS

```
access-list 110 deny ip 192.168.1.0 0.0.0.63 192.168.2.0 0.0.0.63
```



FIREWALL

Configurazione Porte GigabitEthernet:

- RETEINTERNA: ip 172.16.1.9

Subnet Mask: 255.255.255.248 (CIDR/29)

- DMZ: ip 172.16.1.1

Subnet Mask: 255.255.255.248 (CIDR /29)

- WAN: la configurazione della porta rispecchia i parametri forniti dall'ISP

Rete Interna:

Firewall / Rules / RETEINTERNA

Floating WAN DMZ RETEINTERNA

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	X 0/0 B	IPv4 *	Uffici_Subnets	*	172.16.1.0/29	*	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator

- **Regola1: Impedisce qualsiasi richiesta avanzata dalla zona interna verso la DMZ**

- **Regola2: permette ai client della rete interna di raggiungere internet**

Firewall / Aliases / Edit

Properties

Name: Uffici_Subnets
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description: A description may be entered here for administrative reference (not parsed).

Type: Network(s)

Network(s)

Hint: Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

Network or FQDN	/	26	Port	Delete
192.168.1.0	/	26	Piano 1	
192.168.2.0	/	26	Piano 2	
192.168.3.0	/	26	Piano 3	
192.168.4.0	/	26	Piano 4	
192.168.5.0	/	26	Piano 5	
192.168.6.0	/	26	Piano 6	
192.168.10.0	/	26	NAS	





WAN:

- **Regola 1: impedisce qualsiasi richiesta proveniente da internet destinata alla rete interna**
- **Regola 2 + Regola 3 + Regola 4: permette di raggiungere il server web nella DMZ solo sulla porta 80 o 443**

ESEMPIO DI REGOLA:

- Action: Pass
- Address Family: IPv4
- Protocol: TCP
- Source: Any
- Source Port: Any
- Destination Address or Alias: 172.16.1.2
- Destination Port: 80

DMZ:

- **Regola1: impedisce qualsiasi richiesta avanzata dalla DMZ verso la zona interna**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	IPv4 *	172.16.1.0/29	*	Uffici_Subnets	*	*	*	*	none	

IDS/IPS

La scelta del posizionamento di IDS/IPS e di quali dei due componenti installare nella rete è dovuta a una decisione strategica rappresentata in questo modo:

- IDS, utilizzabile in due modi:
 - HIDS: monitora un singolo dispositivo, analizzando log di sistema, modifiche ai file e attività sospette inviando Alert al SOC. Nel nostro caso il software è installato nel server NAS
 - NIDS: analizza il traffico di rete per identificare attacchi come scansioni, exploit o malware inviando notifiche come l'HIDS. A differenza del precedente lo abbiamo installato all'interno della rete DMZ.
- IPS: utilizzato per implementare la sicurezza delle reti interne. Lo abbiamo posizionato tra il firewall e la rete interna, in modo tale da bloccare immediatamente minacce identificate rivolte all'interno di Theta.

Una delle differenze cruciali tra IDS e IPS è che quest'ultimo rallenta la rete dato che svolge dei processi aggiuntivi più complessi nell'invio dei dati.





SOCKET DI RETE:

ESEMPIO DI BACKDOOR

```
import socket

SRV_ADDR = "127.0.0.1"
SRV_PORT = 44444

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.bind((SRV_ADDR, SRV_PORT))
s.listen(1)
print("Server started! Waiting for connections...")
connection, address = s.accept()
print("Client connected with address", address)

while 1:
    data = connection.recv(1024)
    if not data : break
    connection.sendall(b"-- Message Received -- \n")
    print(data.decode('utf-8'))
connection.close()
```

The image shows two terminal windows from a Kali Linux environment. The top window, titled 'kali@kali: ~/Documents/python', contains a Python script named 'conessione_socket.py'. It creates a TCP server on port 44444, waits for a connection, and then prints the client's address and a message received from the client. The bottom window, also titled 'kali@kali: ~', runs the command '\$ netcat 127.0.0.1 44444' to connect to the server. The output shows the server's greeting and two messages received from the client, which are identical to the ones sent by the server.

```
kali@kali: ~/Documents/python
File Actions Edit View Help
(kali㉿kali)-[~/Documents/python]
$ python conessione_socket.py
Server Started! Waiting for connections...
Client connected with address: ('127.0.0.1', 51748)
>>> FalkonLock <<<

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ netcat 127.0.0.1 44444
>>> FalkonLock <<<
-- Message Received --
-- Message Received --
```

ANALISI DVWA: PORT

WELL KNOWN PORTS:

File Transfer (FTP) 21: NOT SECURE

- La porta in questione consente la condivisione, upload e download tra il client e il server

FTPS : RACCOMANDED

TELNET 23: NOT SECURE

- Telnet fa sì che ci sia una comunicazione bidirezionale tra due macchine su rete TCP/IP, permette anche di accedere in remoto su un computer e di eseguire comandi come se si fosse collegati localmente

UTILIZZO DI SSH : RACCOMANDED

Simple Mail Transfer 25 (SMTP): NOT SECURE

- SMTP è un protocollo standard per l'invio di email attraverso le reti IP dal client al server di posta notificando eventuali errori nel processo

UTILIZZO DI SSL/TLS : RACCOMANDED

ENUMERAZIONE PORTE APERTE:

```
Enter the IP address to scan (default: 192.168.100.110):  
Enter the port range to scan (default: 1-1024): 1-65365  
Scanning host 192.168.100.110 from port 1 to port 65365  
>>> Port 21 File Transfer [Control] - OPEN  
>>> Port 22 SSH Remote Login Protocol - OPEN  
>>> Port 23 Telnet - OPEN  
>>> Port 25 Simple Mail Transfer - OPEN  
>>> Port 53 Domain Name Server - OPEN  
>>> Port 80 World Wide Web HTTP - OPEN  
>>> Port 111 SUN Remote Procedure Call - OPEN  
>>> Port 139 NETBIOS Session Service - OPEN  
>>> Port 445 Microsoft-DS - OPEN  
>>> Port 512 Remote process execution - OPEN  
>>> Port 513 Remote Login - OPEN  
>>> Port 514 Remote Shell - OPEN  
>>> Port 1099 RMI Registry - OPEN  
>>> Port 1524 dtspcd / ingres - OPEN  
>>> Port 2049 Network File System - Sun Microsystems - OPEN  
>>> Port 2121 CCPProxy FTP / SCIENTIA-SSDB - OPEN  
>>> Port 3306 MySQL - OPEN  
>>> Port 5432 postgres database server - OPEN  
>>> Port 5900 VNC Virtual Network Computing - OPEN  
>>> Port 6000 X-Windows / W32.LoveGate.ak virus - OPEN  
>>> Port 6667 IRC - OPEN  
>>> Port 8009 Apache JServ Protocol - OPEN
```

PORT SCANNER

Il programma permette di scansionare un range di porte date in input e di visualizzare quelle aperte associandone il relativo servizio in esecuzione.

```
1 ~ import socket
2  import csv
3
4  target = input('Enter the IP address to scan (default: 192.168.100.110): ')
5  portrange = input('Enter the port range to scan (default: 1-1024): ')
6
7 ~ if target == "":
8     target = "192.168.100.110"
9
10 ~ if portrange == "":
11    portrange = "1-1024"
12
13  tcp_port_aray = []
14
15 ~ with open("tcp.csv") as csvfile:
16     reader = csv.reader(csvfile, quoting=csv.QUOTE_NONNUMERIC)
17 ~     for row in reader:
18         tcp_port_aray.append(row)
19     csvfile.close()
20
21  lowport = int(portrange.split('-')[0])
22  highport = int(portrange.split('-')[1])
23
24  print('Scansono host ', target, ' dalla porta ', lowport, ' alla porta ', highport)
25
26 ~ for port in range(lowport, highport):
27     s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
28     status = s.connect_ex((target, port))
29 ~     if(status == 0):
30 ~         for i in range(len(tcp_port_aray)):
31 ~             if tcp_port_aray[i][1] == port:
32 ~                 print('>>> Port ', port, tcp_port_aray[i][2], ' - OPEN')
33 ~                 break
34     s.close()
```



ANALISI DVWA: METODI HTTP

Analisi Metodi http:

Il programma sottostante permette di visualizzare i codici di stato che il server comunica alle nostre interrogazioni http:

```
1 import http.client
2
3 http_methods = ['GET', 'POST', 'DELETE', 'PATCH', 'OPTIONS', 'PUT', 'HEAD', 'CONNECT', 'TRACE']
4
5 host = input('Inserire URL completa del sistema target (default:192.168.100.110/phpMyAdmin/index.php):')
6
7 if host == "":
8     host = "192.168.100.110/phpMyAdmin/index.php"
9
10 host = host.split('/')
11 url_domain = host[0]
12
13 url_path = ""
14 for i in range(1, len(host)):
15     url_path = url_path + "/" + host[i]
16
17 port = input('Inserire la porta del sistema target (default:80): ')
18
19 if(port == ""):
20     port = 80
21
22 for i in range(len(http_methods)):
23     try:
24         connection = http.client.HTTPConnection(url_domain,port)
25         connection.request(http_methods[i], url_path)
26         response = connection.getresponse()
27         print(http_methods[i] + " : ", response.status, " - ", response.reason)
28         connection.close()
29     except ConnectionRefusedError:
30         print("Connessione fallita")
31
```

```
kali@kali: ~/Documents/python
File Actions Edit View Help
(kali㉿kali)-[~/Documents/python]
$ python HTTP_Methods_Scanner.py
Inserire URL completa del sistema target (default:192.168.100.110/phpMyAdmin/index.php):
Inserire la porta del sistema target (default:80):
GET : 200 - OK
POST : 200 - OK
DELETE : 200 - OK
PATCH : 200 - OK
OPTIONS : 200 - OK
PUT : 200 - OK
HEAD : 200 - OK
CONNECT : 400 - Bad Request
TRACE : 200 - OK
(kali㉿kali)-[~/Documents/python]
$
```





ANALISI DVWA: METODI HTTP

Analisi risposte:

- GET: 200 - OK => Risposta corretta
- POST: 200 - OK => Risposta non corretta. Dovrebbe restituire 400 - Bad Request in quanto non sono stati forniti dati da processare
- DELETE: 200 - OK => Risposta non corretta. Il server non esegue la DELETE della risorsa. Dovrebbe restituire 401 - Unauthorized in quanto è stata inviata una richiesta per una cancellazione di una risorsa senza fornire nessun metodo di autenticazione.
- PATCH: 200 - OK => Risposta non corretta. Il server non esegue la PATCH. Dovrebbe restituire 401 - Unauthorized in quanto è stata inviata una richiesta per una modifica di una risorsa senza fornire nessun metodo di autenticazione.
- OPTION: 200 - OK => Risposta corretta. A seguito di ulteriori analisi si riscontra che il server non invia in risposta i metodi ammessi.
- PUT: 200 - OK => Risposta non corretta. Il server non esegue la PUT. Dovrebbe restituire 401 - Unauthorized in quanto è stata inviata una richiesta per un inserimento di una nuova risorsa senza fornire nessun metodo di autenticazione.
- HEAD: 200 - OK => Risposta corretta
- CONNECT: 400 - Bad Request => Risposta corretta.
- TRACE: 200 - OK => Risposta corretta.



Mitigazione:

- Implementare una corretta gestione delle richieste dapprima settando adeguatamente i file di configurazione del servizio web impostando i metodi ammessi.



CONTRATTO

Sezioni del contratto

1. Oggetto del contratto
2. Durata del contratto
3. Servizi offerti
4. Costi del servizio
5. Obblighi del fornitore
6. Obblighi del cliente
7. Risoluzione del contratto



CONTRATTO SERVIZI OFFERTI

Supporto tecnico:

- Assistenza tecnica, sia da remoto che on-site, per problematiche hardware e software
- Tempo di risposta garantito entro 2 ore dalla segnalazione

Gestione Licenze Software:

- Monitoraggio, aggiornamento e gestione delle licenze software in uso
- Controllo delle scadenze e rinnovo delle licenze

Protezione Antivirus per PC e Server:

- Fornitura e gestione di soluzioni antivirus avanzate
- Aggiornamento e monitoraggio continuo per la protezione da minacce informatiche



CONTRATTO

SERVIZI OFFERTI

Sistema di Backup:

- Implementazione di soluzioni di backup automatiche e periodiche
- Verifica dell'integrità dei dati e ripristino in caso di necessità

Formazione del Personale:

- Sessioni formative di base per la sicurezza informatica e prevenzione delle minacce
- Fornitura di materiali didattici e guide operative

Manutenzione della Rete:

- Monitoraggio e manutenzione della rete aziendale
- Ottimizzazione delle configurazioni per garantire prestazioni ottimali

Interventi di Risoluzione Problemi:

- Diagnosi e riparazione di guasti hardware e software
- Ripristino d'emergenza in caso di guasti critici



CONTRATTO

COSTI DEL SERVIZIO:

Servizio	Costo (€)
Supporto tecnico	40.000
Licenze software	3.600
Antivirus PC + server	4.200
Sistema di backup	5.000
Formazione del personale	18.000
Manutenzione rete	11.200
Interventi di risoluzione problemi	10.000
Totale annuo	90.000



OBBLIGHI DEL FORNITORE

OBBLIGHI DEL CLIENTE

RISOLUZIONE DEL CONTRATTO

CONCLUSIONE

Una corretta progettazione della rete è fondamentale per garantire la sicurezza.

- Strumenti come IPS, HIDS e NIDS devono essere posizionati strategicamente per assicurare alta qualità dei servizi senza interruzioni.
- La configurazione del firewall protegge le aree sensibili aziendali
- L'identificazione delle vulnerabilità sui sistemi applicativi è cruciale per evitare compromissioni.

In particolare, il Web Server, esposto a internet, presenta molte vulnerabilità che potrebbero compromettere la sicurezza dell'azienda, nonostante le misure di protezione adottate.



THANK YOU!

