

CLIENTE: THETA S.P.A.

PROGETTO DI RETE

CRYTECH SRL - VIA BROMBEIS 51, 20124 MILANO

INDICE



DISPOSITIVI NECESSARI	PAGINA 2
STRUTTURA DELLA RETE AZIENDALE	PAGINA 3
ANALISI DEL PRIMO PIANO	PAGINA 4
PREVENTIVO DI SPESA	PAGINA 6
SUBNETTING	PAGINA 7
TEST DI RETE	PAGINA 8
- SCANSIONE PORTE	PAGINA 8
- VERIFICA VERBI HTTP	PAGINA 10
FIREWALL PFSENSE	PAGINA 11

DISPOSITIVI NECESSARI

Al fine di soddisfare la richiesta di preventivo dell'azienda Theta S.p.A. di seguito sono elencati i dispositivi per poter realizzare al meglio il progetto di rete della loro infrastruttura IT.

Switch: dispositivo utilizzato per far comunicare gli host appartenenti alla stessa rete

Router-Gateway: instradatore di pacchetti che consente la comunicazione di host appartenenti a ip network diverse.

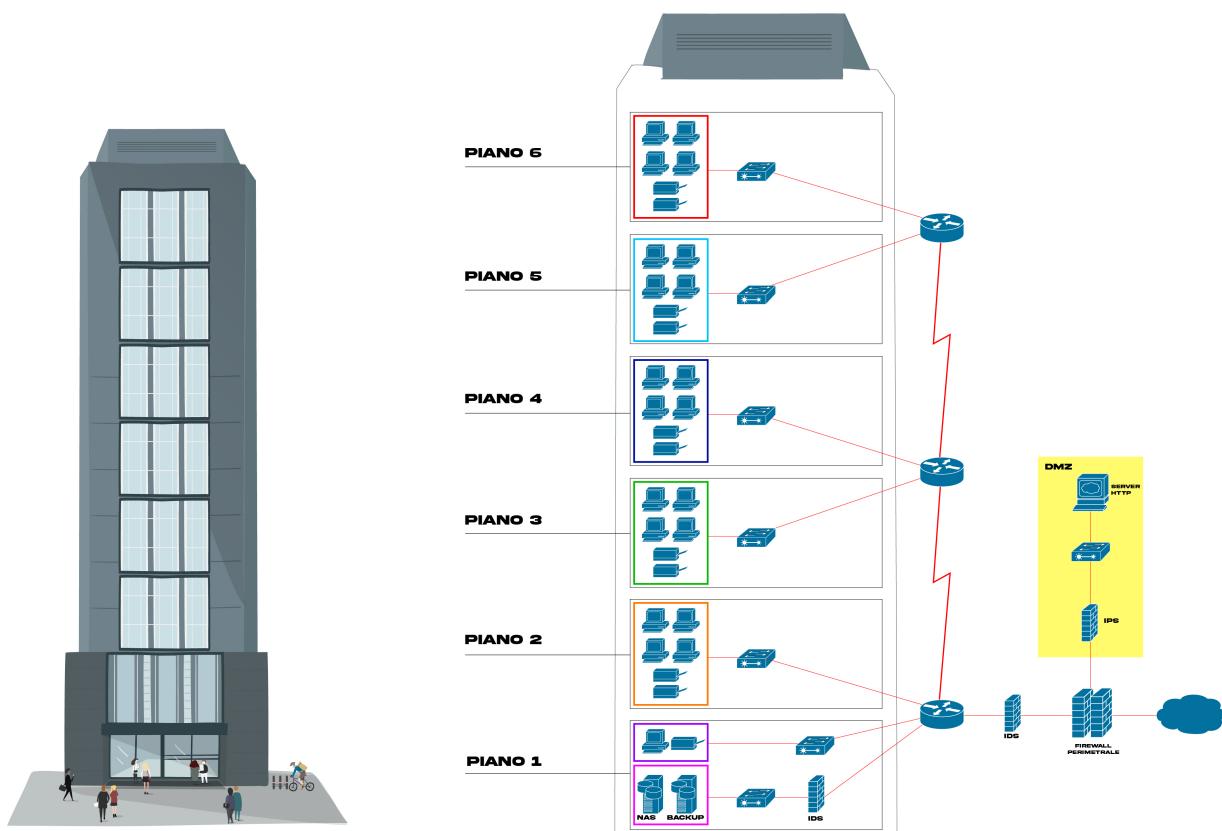
NAS: server contenente diverse unità di memoria per conservare e condividere dati in una rete.

Firewall perimetrale (stateful): dispositivo hardware che monitora e filtra il traffico dati in entrata.

Sistema IDS: software che analizza il contenuto del pacchetto e, se rileva una potenziale minaccia, invia una notifica all'admin.

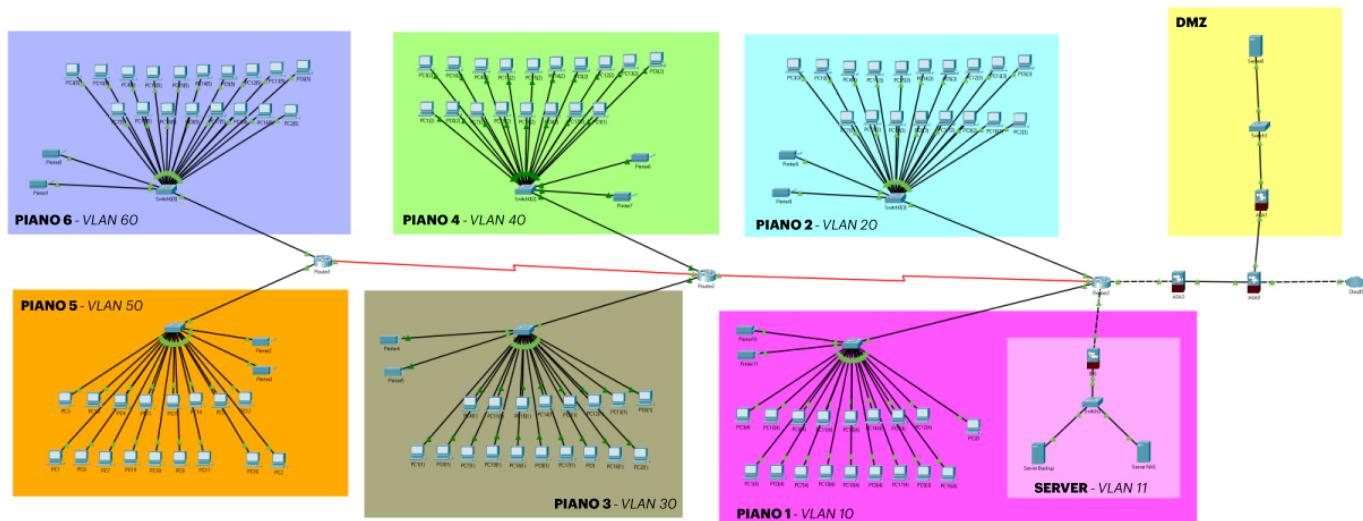
Sistema IPS: a differenza dell'IDS blocca automaticamente il pacchetto sospetto

Server Backup: dispositivo atto alla creazione di una copia di tutti i dati di sistema e file aziendali.



STRUTTURA DELLA RETE AZIENDALE

Nell'immagine sottostante vi è rappresentata a scopo illustrativo l'infrastruttura della rete aziendale. L'edificio è composto da 6 piani e per ogni piano abbiamo 18 workstation e 2 stampanti. Ad eccezione del primo in cui sono presenti, inoltre, un server NAS, un server di Backup, la DMZ con il server HTTP, firewall perimetrale e sistemi IDS/IPS. Avendo così un totale di 120 host.

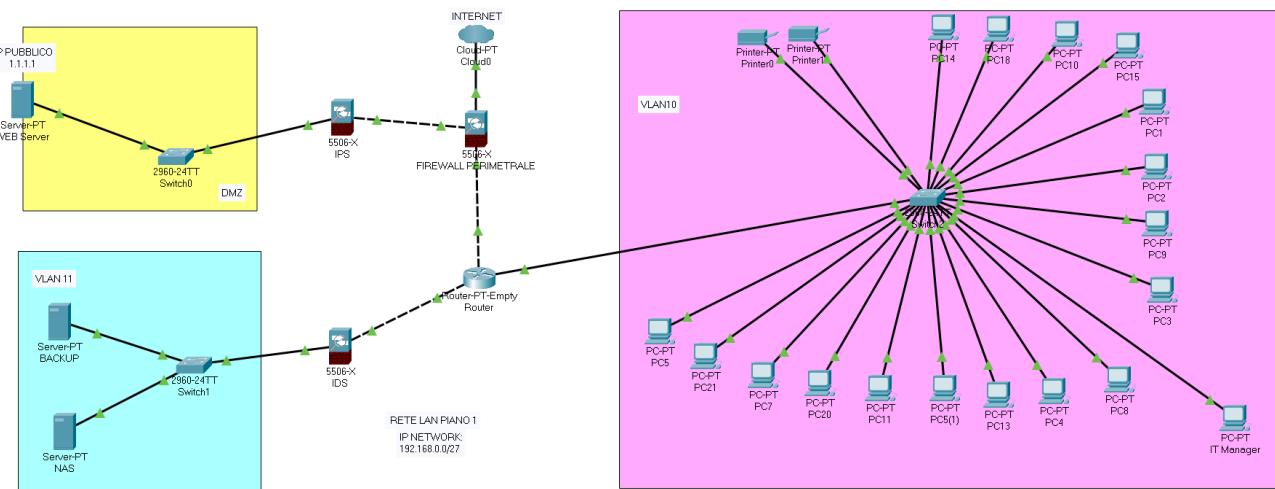


La LAN aziendale è stata segmentata con la tecnica delle VLAN. Rispettivamente vi è una VLAN per ogni piano e una dedicata al server NAS. Questo permette, non solo di migliorare la rete in termini di sicurezza, ma anche per avere una maggiore flessibilità e una migliore gestione del traffico interno.

Ogni piano ha il proprio switch che mette in comunicazione tutti gli host appartenenti alla stessa VLAN. Gli switch di livello 2 sono poi collegati al router gateway che instrada i pacchetti permettendo, così, di far comunicare tra loro tutti i dispositivi appartenenti a VLAN differenti. Inoltre si è deciso di aggiungere altri 2 router alla richiesta dell'azienda, per poter distribuire meglio il traffico di rete, avendo in totale 3 router che gestiscono 2 piani per volta.

ANALISI PRIMO PIANO

Di seguito è raffigurato il primo piano dell'edificio, poiché sono stati inseriti la DMZ (zona demilitarizzata), i sistemi di sicurezza IDS e IPS e soprattutto il server di Backup e il server NAS.



Come si può notare dall'immagine è stato impiegato un firewall perimetrale a protezione della rete e posizionato tra il router e la WAN (wide area network).

Il firewall, attraverso il filtraggio dinamico dei pacchetti, blocca tutte le comunicazioni in arrivo dall'esterno ma permette ai dispositivi interni della LAN di comunicare verso l'esterno. Questo è possibile attraverso la propria tabella ACL, che memorizza l'indirizzo IP pubblico associato all'indirizzo IP privato del dispositivo che vuole connettersi. Una volta terminata la sessione, l'associazione viene eliminata dalla tabella, in quanto memoria volatile (cache).

Sempre al primo piano è stata creata una DMZ, detta zona demilitarizzata, per poter permettere il traffico in entrata e uscita dalla rete consentendo a tutti l'accesso ai servizi offerti dall'azienda. Per questa ragione, al suo interno è stato inserito il web server aziendale. Questa soluzione permette di separare le risorse pubbliche accessibili dall'esterno, dalla rete interna; riducendo così il rischio di attacchi informatici diretti.

Per un'ulteriore misura di sicurezza e monitoraggio del traffico sono stati inseriti 3 sistemi anti-intrusione IDS/IPS. Nel dettaglio sono stati posizionati:

- 2 IDS; il primo posizionato a protezione del server NAS e del server di Backup e l'altro tra il firewall e il router a protezione delle varie VLAN.
-
- 1 IPS, utilizzato per monitorare e bloccare il traffico sospetto verso la DMZ.

Si è scelto di usare un IDS rispetto ad un IPS per la protezione del NAS. Quest'ultimo, in un'azienda conserva vari tipi di dati, vitali per l'azienda stessa, dai meno confidenziali ai più confidenziali e con accessi a diversi livelli di autorizzazione. Per questo motivo si è scelto di collocarlo in questa posizione.

L' altro IDS in quella posizione, è un ulteriore misura di sicurezza preventiva, nel caso in cui il firewall dovesse permettere il passaggio di pacchetti malevoli.

L'IDS è più veloce dell'IPS, ma soprattutto la differenza sostanziale è che, quando identifica un'anomalia o intrusione, il sistema invia all'amministratore una notifica con i dettagli del motivo del blocco, così facendo si ha un feedback su cosa sta accadendo all'interno della rete.

L'IPS è stato posizionato a protezione della DMZ, in quanto è l'unica zona della rete che permette tutte le comunicazioni in entrata e in uscita. In questo caso l'IPS monitora e blocca automaticamente il traffico sospetto. L' IPS, però, può essere soggetto a falsi positivi.

PREVENTIVO DI SPESA

CryTech S.r.l.
Via Brombeis 51
Milano 20124
amministrazione@crytech.com

Spett.le
Theta S.p.A.
Via Vincenzo Manzoni 14
Roma 00171

Preventivo n.: 235
Data emissione: 22/10/2024
Valido fino al: 05/11/2024

DESCRIZIONE	QTA'	PREZZO(€)	TOTALE
Lenovo all-in-one	108	819,00 €	88.452,00 €
Fotocopiatrice Konica Minolta BH C284	12	894,00 €	10.728,00 €
Win10 Pro Keys	108	2,87 €	309,96 €
Firewall Fortinet FG-401E-BDL-950-60-EU	1	39.610,14 €	39.610,14 €
Synology - SA3200D - NAS server - 12 bays	1	7.124,28 €	7.124,28 €
Synology Enterprise 3.5" SAS HDD - HAS5310 - 20TB	15	878,00 €	13.170,00 €
Switch Arista	8	1.216,98 €	9.735,84 €
Gigabyte Twin Server H262-PC1 - 2U 4-Node – Xeon Scalable - 8x SAS/NVMe - 2-Port 10GbE - 2200W Redundant	1	25.385,56 €	25.385,56 €
Waterfall IDS	2	1.229,51 €	2.459,02 €
Cisco - FPR2110-NGFW-K9 – Firepower 2110 NGFW IPS	1	976,64 €	976,64 €
Router Cisco ISR 4431	3	879,50 €	2.638,50 €
Cavo Ethernet Cat6a (1308 metri)	1308	0,85 €	1.111,80 €
Mano d'opera installazione (Hardware e Software) 170 ore	170	50,00 €	8.500,00 €
Cablaggio rete	100	41,00 €	4.100,00 €
TOTALE PARZIALE			214.301,74 €
IVA 22%			47.146,38 €
TOTALE			261.448,12 €

SUBNETTING

Inizialmente, per la creazione delle 6 sottoreti, si è pensato di utilizzare la tecnica del subnetting. In questo modo, per un eventuale aumento delle macchine per piano in futuro, si è scelto di effettuare la segmentazione con CIDR **/27**, così dagli attuali 20 si può arrivare ad avere 30 host disponibili per ogni piano.

Nella tabella seguente i dettagli del subnetting:

PIANI	IP NETWORK	IP GATEWAY	IP BROADCAST
1 °	192.168.0.0/27	192.168.0.1/27	192.168.0.31/27
2 °	192.168.0.32/27	192.168.0.33/27	192.168.0.63/27
3 °	192.168.0.64/27	192.168.0.65/27	192.168.0.95/27
4 °	192.168.0.96/27	192.168.0.97/27	192.168.0.127/27
5 °	192.168.0.128/27	192.168.0.129/27	192.168.0.159/27
6 °	192.168.0.160/27	192.168.0.161/27	192.168.0.191/27

TEST DI RETE

Al fine di rendere l'intera infrastruttura sicura e ben progettata abbiamo effettuato dei test di rete. Come primo test abbiamo scansionato la rete per verificare sicurezza e accessibilità delle porte, infine abbiamo verificato i verbi HTTP disponibili.

I test sono stati effettuati con dei software proprietari sviluppati in Python.

TEST SCANSIONE PORTE

Il nostro software per la scansione di porte prende in input l'indirizzo IP e il range di porte che si vogliono scansionare, riportando in output un elenco con la lista delle porte e il loro relativo stato e servizio.

Da questa scansione saremo in grado di determinare quali servizi tra le porte note sono a forte rischio di intrusione.

Di seguito il risultato del test:

```

ualbnx-amd64 (Snapshot 2) [Running] - Oracle VM VirtualBox
Input Devices Help
File Edit Search View Document Help
python scanner.py - Mousepad
File Edit Search View Document Help
- /python/scanner.py - Mousepad
4 import socket
5 from datetime import datetime
6
7 #DEFINE OUR TARGET
8
9 if len(sys.argv) == 2:
10     target = socket.gethostbyname(sys.argv[1]) #It translates the host name into IPv4
11 else:
12     print("invalid amout of arguments")
13     print("Syntax: python scanner.py <ip>")
14
15 #argv is the amout of given argument, we need to respect it, in this case is 2
16
17 #ADD A BANNER
18 print("-" * 50) #BANNER
19 print("Scanning target: " + target)
20 print("Time started: " + str(datetime.now()))
21 print("-" * 50)
22
23 try:
24     for port in range(0,1024):
25         s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
26         socket.setdefaulttimeout(1)
27         result = s.connect_ex((target, port))
28         if result == 0:
29             try:
30                 service_name = socket.getservbyport(port, 'tcp')
31             except:
32                 service_name = "Unknown service"
33
34             print(f"port {port} is open ({service_name})")
35
36         s.close()
37
38 except KeyboardInterrupt:
39     print("\nExiting program")
40     sys.exit()
41
42 except socket.gaierror:
43     print("Host name could not be resolved")
44     sys.exit()
45
46 except socket.error:
47     print("Could not connect to server")
48     sys.exit()
49

```

Come si può notare dal risultato abbiamo scansionato le porte note dalla 0 alla 1023, mostrando solo le porte aperte. La porta 23 che ospita il protocollo di rete Telnet

trasmette in chiaro i dati. Questo rende l'azienda soggetta ad attacchi informatici, soprattutto perché il protocollo di rete in questione permette di accedere e leggere dati in remoto e offre anche la possibilità di poter controllare la macchina da remoto.

La porta 80, in questo caso aperta, è utilizzata per il traffico HTTP non protetto può essere soggetta a diversi attacchi web.

La porta **21** che ospita il servizio **FTP** trasmette in chiaro tutti i dati, compresi eventuali user e password. In questo caso consigliamo di disabilitare detto servizio e di utilizzare direttamente l'uso di SFTP sulla porta 22 cifrando così il traffico dei dati.

In questo specifico scenario la porta **23** che utilizza il servizio **TELNET**, ormai in disuso, è opportuno chiuderla per evitare qualsiasi tipo di minaccia a cui è esposto. Per quanto riguarda invece la porta **80 HTTP** nel nostro caso possiamo chiuderla in quanto procederemo a reindirizzare automaticamente il traffico sulla porta **443 HTTPS** evitando così eventuali attacchi Man In The Middle (MITM).

PORTE	PROTOCOLLO	STATO	MOTIVO
21	FTP	chiusa	Trasferimento di file da host a host. Viene chiusa per possibili attacchi man in the middle. Viene sostituita con la porta 22 SFTP che utilizza il protocollo SSH.
23	TELNET	chiusa	Viene chiusa perché obsoleta e trasmette i dati in chiaro, soggetta a possibili attacchi sniffing.
25	SMTP	aperta	Tenuta aperta perché utilizzata per l'invio delle email, si consiglia di utilizzare la 465 SMTPS
53	DNS	aperta	Gestisce l'associazione tra URL e Indirizzo IP del web server
80	HTTP	chiusa	Viene chiusa perché trasmette in chiaro i dati e per possibili attacchi Dos.
143	IMAP	aperta	Viene aperta per permettere la ricezione di email e per favorire l'accessibilità all'azienda
443	HTTPS	aperta	Viene aperta perché la comunicazione è crittografata.
445	SMB	chiusa	Viene chiusa perché è un protocollo obsoleto (si potrebbe usare un cloud) e per la dimensione della rete (ci sono più di 20 host)
161 - 162	SNMP	aperta	Abbiamo installato la versione SNMPv3 perché critta la comunicazione.

TEST VERIFICA VERBI HTTP

Il nostro software per la verifica dei verbi HTTP, dato in input un URL, richiede quali verbi si vogliono verificare inviando così le rispettive richieste al server web, riportando poi in output quali sono i metodi disponibili per quel determinato URL.

Di seguito il risultato del nostro test:

```
(kali㉿kali) [-/python] python verbscanner.py
Insertare l'url da esaminare: https://www.phpmyadmin.net
Quale verbo HTTP vuoi conoscere? all
GET request:
Status Code: 200
POST Request:
Status Code: 403
PUT Request:
Status Code: 403
PATCH Request:
Status Code: 403
DELETE Request:
Status Code: 200
OPTIONS Request:
Status Code: 200
Allowed Methods: GET, HEAD, OPTIONS
```

Da questo risultato possiamo determinare che per il path /phpmyadmin/ sono disponibili all'utente i seguenti metodi: GET, HEAD e OPTIONS.

Tra questi quello più vulnerabile è il metodo GET solo se si utilizza una connessione HTTP (non cifrata).

Abbiamo inoltre deciso di disabilitare il metodo DELETE modificando il patch e rendendolo disponibile solo agli autorizzati.

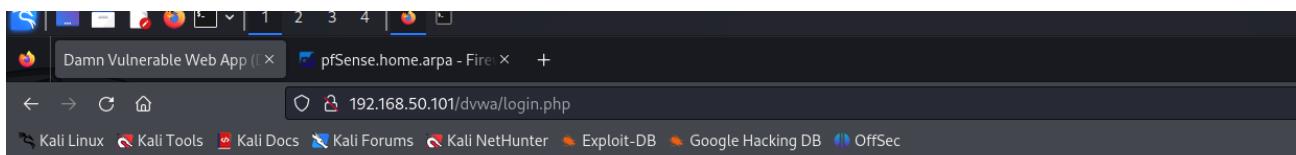
FIREWALL PFSENSE

Di seguito viene illustrato un esempio di funzionamento di un firewall, in questo caso utilizziamo PFSense.

In primo luogo vediamo la regola disattivata e quindi le due macchine che dialogano.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/195 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/2 KiB	IPv4 TCP	192.168.1.101	*	192.168.50.101	80 (HTTP)	*		none		
<input type="checkbox"/>	0/88 KiB	IPv4 *	LAN subnets	*	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	*	none	Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator



Username

Password

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

In questo caso invece attivando la regola possiamo vedere come il firewall PFSENSE blocca la comunicazione sulla porta 80, infatti non si può accedere alla pagina ma

Rules (Drag to Change Order)											
□	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/1.35 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
✗	0/3 KiB	IPv4 TCP	192.168.1.101	*	192.168.50.101	80 (HTTP)	*	none			🔗 📝 📋 🗑️
✗	0/647 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	🔗 📝 📋 🗑️ ✗
✗	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 📝 📋 🗑️ ✗

```

kali㉿kali: ~
File Actions Edit View Help
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.863/0.982/1.122/0.106 ms
[(kali㉿kali)-~] $ ifconfigig
The connection has timed out
Command 'ifconfigig' not found, did you mean:
  command 'ifconfig' from deb net-tools
Try: sudo apt install <deb name>
Ver at 192.168.50.101 is taking too long to respond.

[(kali㉿kali)-~] $ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=63 time=5.82 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=63 time=1.02 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=63 time=1.53 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=63 time=0.940 ms
^C
--- 192.168.50.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.940/2.328/5.824/2.030 ms
[(kali㉿kali)-~] $ 

```

comunque i due host possono comunicare tramite altre porte.

**TEAM: PAOLO TAVIAN, SAMUEL GRILLO, SARA LARIZZA, SIMONE
MORETTI, STEFANO FIORI, DANIELE PAOLONE, GHASSAN HAOUEM**



RINGRAZIAMO PER L'ATTENZIONE

CRYTECH TEAM