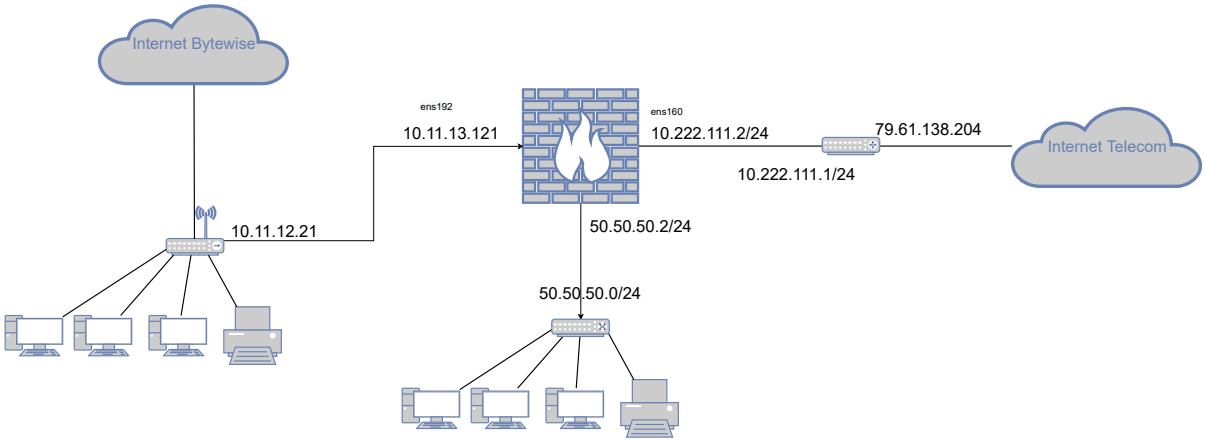
IPS E PENETRATION TEST

Indice

1. INTRODUZIONE

1.1. **COS'È VMWARE E VSPHERE.** VMware è un software che permette di creare macchine virtuali, può essere utilizzato per creare un ambiente per effettuare test di sicurezza. VSphere Client è uno strumento per la gestione dell'intera struttura virtuale tramite browser. Per questa simulazione la versione VMware utilizzata è la 5.5.

1.2. **CONFIGURAZIONE INIZIALE.** La rete ha questa struttura:



Un firewall con tre schede di rete:

- la 10.11.13.121 che si affaccia sulla rete bytewise con default gateway 10.11.12.21.
- la 10.222.111.2 che si affaccia sulla rete telecom con default gateway 10.222.111.1. Questo è il router che viene usato dal firewall quando l'host da raggiungere non è direttamente connesso.
- la 50.50.50.2 sulla lan 50.50.50.0/24
- si osserva che la VMware è visibile dall'esterno tramite l'IP pubblico 79.61.138.204

La macchina virtuale che ospita il **firewall** è stata installata con questa configurazione:
username: root
passwd: mnkjoi09
Le risorse assegnate alla vm sono:

- 8 core
- 32 GB ram
- 250 GB hdd

Il firewall viene configurato manualmente, quindi è stato disabilitato firewalld (systemctl disable firewalld –now) e SELinux.

Il firewall si trova in /root/fwdir.

Algoritmo 1 file di flush in /root/fwdir/flush

```
#!/bin/bash
iptables -F #flush delle catene di forward e input output
iptables -F -t nat #flush delle catene di pre-post routing
iptables -X #delete catene di forward
# politica di accept
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCPT
```

Algoritmo 2 regole iptables in /root/fwdir/fw

```
#!/bin/bash
#---------- FLUSH FIREWALL ----------#
/root/fwdir/flush
echo 1 > /proc/sys/net/ipv4/ip_forward
#---POLICY---#
# politica di drop
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
#---------- FORWARD FILE ----------#
#/root/myfirewalldir/myfirewallForward
#---------- I/O FILE ----------#
#/root/myfirewalldir/myfirewall_IO
service iptables save
```

I servizi attivi sulla macchina sono:

- Un server http apache con vulnerabilità remote code execution.
- MariaDB Version 5.5.68
  - passwd: mnkjoi09
- Samba Version 4.10.16
  - TCP porte 139, 445
  - UDP porta 137
  - utente: josh
  - passwd: johnlennon
  - utente: sadmin
  - passwd: ringostarr