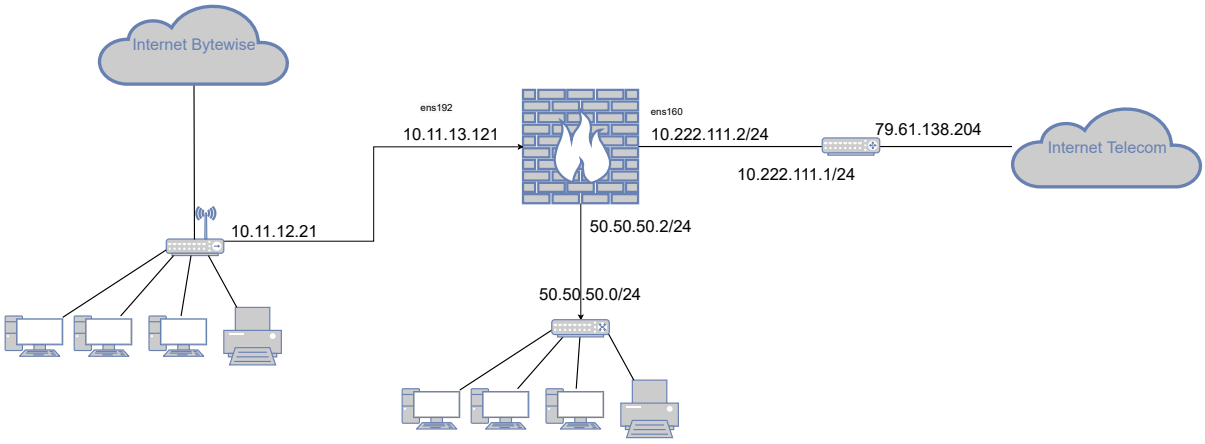
IPS E PENETRATION TEST

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. L'intera struttura virtuale viene gestita tramite browser grazie allo strumento VSphere Client. 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:

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
  - Guida: https://linuxize.com/post/how-to-install-and-configure-samba-on-centos-7/
  - TCP porte 139, 445
  - UDP porta 137
  - utente: josh
  - passwd: johnlennon
  - utente: sadmin
  - passwd: ringostarr

1.3. **COS'È SNORT.** Snort è un software di rilevazione e prevenzione delle intrusioni. I sistemi di rilevazione delle intrusioni (Intrusion Detection Systems, o IDS) individuano pacchetti sospetti, li registrano e ne segnalano la presenza all'amministratore di rete. La loro naturale evoluzione consiste nei sistemi di prevenzione delle intrusioni (Intrusion Prevention Systems, o IPS), che intraprendono azioni attive sui pacchetti sospetti eliminandoli, resettando connessioni e/o bloccando interamente il traffico proveniente da determinati indirizzi IP.

1.4. **INSTALLAZIONE E CONFIGURAZIONE.** Snort è stato installato da sorgente:

- snort-2.9.19.tar.gz
- daq-2.0.7.tar.gz (data acquisition library)

Per configurarlo bisogna modificare il file **/etc/snort/snort.conf.**

La guida è disponibile tramite il link:
https://upcloud.com/community/tutorials/installing-snort-on-centos/

L'indirizzo da proteggere è quello della scheda che si affaccia sulla rete esterna e che corrisponde all'ip 10.222.111.2.

1.5. **TEST PRELIMINARE.** Un test preliminare è stato rilevare tutti i tentativi di connessione sulla porta 22. Bisogna aggiungere una regola nel file **/etc/snort/rules/local.rules**.

La regola è:

- **alert tcp any any -> $HOME_NET 22 (msg:"ssh test"; sid:10000001; rev:001;)**
  - snort manda un alert per i pacchetti che hanno source-ip: **any,** source-port: **any,** destination-ip: **10.222.111.2** (memorizzato nella variabile **$HOME_NET),** destination-port: **22**

Se un host esterno cerca di connettersi tramite la porta 22, il tentativo viene rilevato da snort.

È possibile far partire un'istanza di snort e far stampare a schermo i log digitando il comando:

- **snort -A console -i ens160 -u snort -g snort -c /etc/snort/snort.conf**
  - Nota: ens160 è l'interfaccia che corrisponde all'ip 10.222.111.2

Grazie ai log di snort e ai log di ssh su **/var/log/secure**, è possibile osservare come ogni secondo ci siano tentativi di login su ssh (ovviamente falliti) dovuti a script automatizzati. Per eliminare il problema, ssh è stato reso disponibile sulla porta 65022.