Practical Assignment #1

João Neto – 2023234004

Vasco Alves – 2022228207

22 de março de 2026

Conteúdo

1 Introduction

O objetivo principal deste trabalho era aprender IPTables e como configurar um com o Suricata um sistema de filtração e deteção de ataques. Para esse fim, foi simulado um sistema dividido em três redes e um router para conectar-las. As três redes são a DMZ (23.214.219.128/25, enp0s8), Internal network (192.168.10.0/24, enp0s9) e Internet (87.248.214.0/24, enp0s10). As três redes tem varios serviços, o DMZ tem dns(23.214.219.130), mail(23.214.219.134), vpn-gw(23.214.219.133), www(23.214.219.132) e smpt(23.214.219.131). A Internal network tem ftp(192.168.10.2), datastore(192.168.10.3) e clientes (nos testes os clientes tem ip 192.168.10.4, mas está configurado para dar para qualquer edereço). Por fim a rede Internet tem dns2 (87.248.214.99) e eden (87.248.214.100), existe também outros serviços (87.248.214.98).

2 Firewall

2.1 Packet fileter without NAT

O policy que foi escolhido foi: iptables -P INPUT DROP iptables -P FORWARD DROP iptables -P OUTPUT ACCEPT Foi escolhido porque é mais facil dar DROP a todos os pacotes que não foi criado regras do que criar uma regra de DROP para todos os protocolos e possibilidades, o OUTPUT ficou para ACCEPT porque não existe razão para dar DROP dos pacotes que estamos a enviar neste trabalho. Para o router conseguir resolver DNS requests e para aceitar coneções SSH da rede interna ou da VPN gateway foi utilizado estes comandos: sudo iptables -A INPUT -o enp0s10 -p udp –dport 53 -j ACCEPT sudo iptables -A INPUT -i enp0s9 -p tcp –dport 22 -j ACCEPT sudo iptables -A INPUT -i enp0s8 -s 23.214.219.133 -p tcp –dport 22 -j ACCEPT Para conseguirmos a confirguração pedida entre redes foi utilizado estes commandos: sudo iptables -A FORWARD -i enp0s8 -o enp0s10 -s 23.214.219.130 -p udp –dport 53 -j ACCEPT sudo iptables -A FORWARD -i enp0s9 -o enp0s8 -d 23.214.219.130 -p udp –dport 53 -j ACCEPT sudo iptables -A FORWARD -i enp0s8 -o enp0s10 -s 23.214.219.130 -p tcp –dport 53 -j ACCEPT sudo iptables -A FORWARD -i enp0s9 -o enp0s8 -d 23.214.219.131 -p tcp –dport 587 -j ACCEPT sudo iptables -A FORWARD -i enp0s9 -o enp0s8 -d 23.214.219.134 -p tcp –dport 143 -j ACCEPT sudo iptables -A FORWARD -i enp0s9 -o enp0s8 -d 23.214.219.134 -p tcp –dport 110 -j ACCEPT sudo iptables -A FORWARD -i enp0s9 -o enp0s8 -d 23.214.219.132 -p tcp –dport 80 -j ACCEPT sudo iptables -A FORWARD -i enp0s9 -o enp0s8 -d 23.214.219.132 -p tcp –dport 443 -j ACCEPT sudo iptables -A FORWARD -i enp0s9 -o enp0s8 -d 23.214.219.133 -p udp –dport 1194 -j ACCEPT sudo iptables -A FORWARD -i enp0s8 -o enp0s9 -s 23.214.219.133 -d 192.168.10.2 -j ACCEPT sudo iptables -A FORWARD -i enp0s8 -o enp0s9 -s 23.214.219.133 -d 192.168.10.3 -j ACCEPT

2.2 Packet filtering with NAT

Para conecções com origem/destino na internet foi utilizado DNAT/SNAT e iptables para ”esconder”o ip para a internet que quer aceder a rede interna e iproutes para bloquear certos pacotes de entrar, para conseguir a configuração utilizamos estes comandos: sudo iptables -A FORWARD -i enp0s10 -o enp0s9 -d 192.168.10.2 -p tcp –dport 21 -j ACCEPT sudo iptables -A FORWARD -i enp0s9 -o enp0s10 -p tcp –sport 20 -j ACCEPT sudo iptables -t nat -A PREROUTING -s $dns2 - ptcp - -dport22 - jDNAT--to-destination192.168.10.3sudoiptables-tnat-APREROUTING-s$eden -p tcp –dport 22 -j DNAT –to-destination 192.168.10.3 sudo iptables -t nat -A PREROUTING -i enp0s10 -p tcp –dport 21 -j DNAT –to-destination 192.168.10.2 sudo iptables -A FORWARD -i enp0s10 -o enp0s9 -d 192.168.10.3 -s $dns2 - ptcp - -dport22-jACCEPTsudoiptables-AFORWARD-ienp0s10-oenp0s9-d192.168.10.3 - s$eden -p tcp –dport 22 -j ACCEPT

2.3 External Network

2.4 Internal Network

3 Intrusion Detection

Suricata rules: drop tcp (dollar)EXTERNAL-NET any -¿ (dollar)HOME-NET any (msg:”ET”; flags:S; threshold:type both, track by-src, count 5, seconds 60; classtype:attempted-recon; sid:1000001; rev:1;) drop tcp any any -¿ any 80 (msg:”SQL injection”; content:”union”; nocase; content:”select”; nocase; classtype:web-application-attack; sid:1000002; rev:1;) drop tcp any any -¿ any 80 (msg:”SQl injection”; content:”’or 1=1”; nocase; classtype:web-application-attack; sid:1000003; rev:1;) drop tcp any any -¿ any 80 (msg:”XSS”; content:≪script”; nocase; classtype:web-application-attack; sid:1000004; rev:1;)

4 Conclusion

Fuck we learned alot