UNIVERSIDADE DE SÃO PAULO
INSTITUTO DE CIÊNCIAS MATEMÁTICAS E DE COMPUTAÇÃO
Departamento de Ciências de Computação

Lab - NAT e Firewall

Nome: Jônatas Alves Lopes **NUSP:**11796552
Nome: Pedro Henrique Raymundi **NUSP:**11795634
Nome: Wictor Dalbosco Silva **NUSP:**11871027

1) Explique o conteúdo obtido através do tcpdump na máquina EMPRESA2 sendo que ela não foi destino e nem origem de qualquer comunicação. E se fosse uma rede sem fio com proteção fraca?

Por ser uma ferramenta para monitorar a rede, o tcpdump não precisa de que a EMPRESA2 seja a origem ou destino da comunicação. O tcpdump pode ser usado para analisar os cabeçalhos dos pacotes que passam pela interface de rede do roteador.

Um usuário malicioso poderia quebrar a segurança da rede e monitorá-la se fosse sem fio ou com proteção fraca.

2) Quais seriam opções para melhorar a rede interna cabeada? E sem fio?

Um firewall pode ser instalado tanto no SERVIDOR para a INTERNET quanto entre as máquinas internas e o SERVIDOR para melhorar a segurança da rede interna cabeada.

Para o caso de redes sem fio, é recomendável utilizar métodos de criptografia mais atuais, como o WPA2.

3) Como os pacotes são modificados em cada regra do iptables nos comandos executados neste laboratório?

O iptables permite que se altere as portas que estão disponíveis para pacotes que vêm de fontes externas à sua rede. Assim, é possível bloquear o acesso a certos serviços, como o ftp (porta 21) e *ssh* (porta 22), de forma similar à que é feito no laboratório.

4) O que aconteceu com o ftp do SERVIDOR ao criar uma regra bloqueando a porta 20?

O que ocorreu é que todos os pacotes com origem da porta 20 foram bloqueados, entretanto, ao usar o *ftp* nos experimentos do LAB, nada ocorreu.