4.1 - Firewall - Atividade Prática

prof. Fábio Engel

fabioe@utfpr.edu.br

Firewall - Atividade Prática

- **Avaliação e prática do netfilter iptables (STATELESS)**.

1. Configure os serviços TELNET e SSH em sua máquina, certifique-se que os serviços estão operacionais e que não existem filtros de pacotes aplicados.
2. Configure as políticas do iptables para DROP nas chains INPUT, OUTPUT e FORWAD. Faça testes de ICMP e de conexão com os serviços configurados, analisando o tráfego com o analisador de protocolos.
3. Crie uma regra para registrar logs das (target LOG) do tráfego no servidor para as chains INPUT, OUTPUT e FORWARD. Exemplo:

```
1        iptables -A INPUT -p ALL -j LOG --log-prefix ‘‘INPUT’’
```

Firewall - Atividade Prática

4. Inclua a regra abaixo. Verifique quais serviços foram afetados com essa regra. Analise o log e procure entender o que aconteceu.

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

5. Inclua a regra a seguir. Verifique quais serviços foram afetados com essa regra.

```
iptables -I INPUT 1 -p tcp -j ACCEPT
```

6. Exclua as regras adicionadas no item 4 e configure as políticas padrão para ACCEPT.

Firewall - Atividade Prática

- **Avaliação e prática do netfilter iptables (STATEFUL)**

1. Utilizando dois computadores, simule o "ping of death".
2. Crie uma regra, via iptables, para bloquear esse tipo de ataque.