BOA TARDE!
BEM VINDO(A)!

Marcus Augustus Pereira Burghardt
LPIC-1, MCLNA, MCLSA, MCTS
CLA, CCA, ITIL

marcus.apb@gmail.com
http://mapburghardt.blogspot.com

O que veremos?

UltraSurf – Entendendo e Bloqueando

Nível: - Avançado.

Assuntos: - Tunelamento.
- Firewalls.
- Exemplos práticos.
- Alertas.

Pré-requisitos: - TCP/IP e algumas ferramentas Linux.

Tunelamento

Técnica muito preocupante atualmente, pois é muito fácil de ser explorada e traz grandes riscos para a Segurança da Informação.

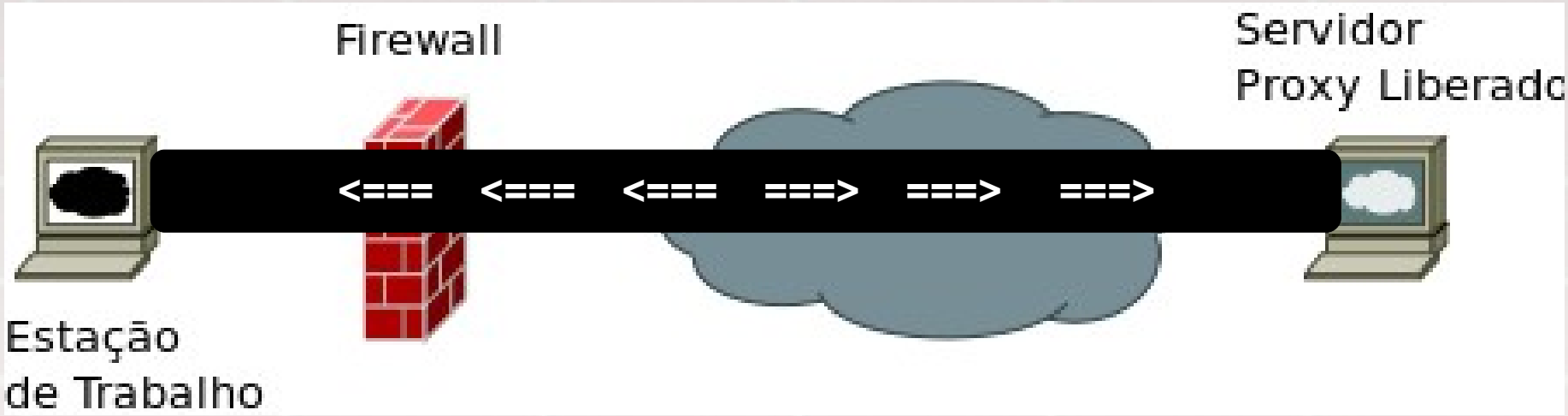
Exemplos: Thor, **UltraSurf** e diversos sites proxies[1].

Entenderemos como essas ferramentas funcionam e como podemos configurar nossos firewalls para bloqueá-las.

Nosso exemplo será didático e com ferramentas comuns, mas os conceitos se aplicam para qualquer ferramenta de tunelamento.

Tunelamento

Mas o que é um tunelamento?



A pergunta clássica: Como bloquear isso?

Políticas de Firewalls

Política Liberal

- Libero tudo e **bloqueio algumas coisas.**
- Jamais poderei afirmar que minha rede está segura.
- Perderei tempo sendo reativo.

Política Restritiva

- **Bloqueio tudo** e libero algumas coisas.
- Poderei afirmar que os acessos são controlados.
- Ganharei tempo sendo proativo.

Políticas de Firewalls

Erros Comuns:

- Liberar acessos com pressa.

- Não monitorar os acessos antes de liberá-los.

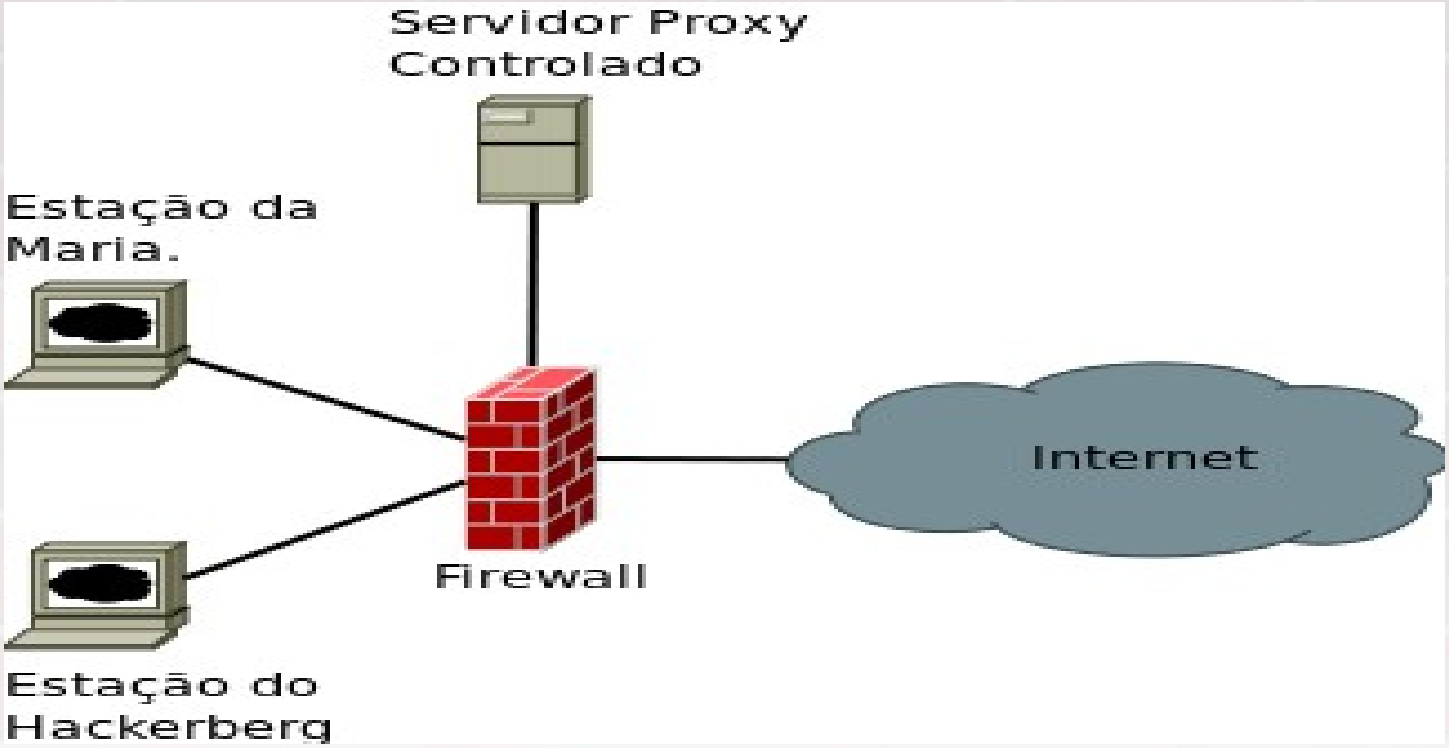
- Não conhecer os acessos que está liberando.

- Não criar regras detalhadas / específicas.

- Pensar como um bobo. Ex.: "*Nenhum usuário da minha rede saberia criar um túnel. Ainda mais nessa porta... hehe*"

Exemplos Práticos

Topologia da Empresa



OBS.: Para navegarem na Internet, os usuários precisam usar o proxy interno.

Exemplos Práticos

Cenário

- Hackerberg é um usuário revoltado com os controles de acesso da empresa em que trabalha.
- Dumbesk administra do firewall dessa empresa.
- Maria, do financeiro, pediu para Dumbesk **liberar** a porta **TCP/5940** para um novo programa de consulta de cheques. (Sim, ela leu isso em um e-mail do fornecedor!).
- Dumbesk, sem monitorar ou questionar, libera o fluxo dessa porta da rede interna para a Internet.
- Maria consegue usar o programa e todos ficam felizes!!

Firewall

Eis a regra criada por Dumbesk:

iptables -A FORWARD -p tcp --dport 5940 -s <REDE INTERNA> -j ACCEPT

Mas qual o problema dessa regra?

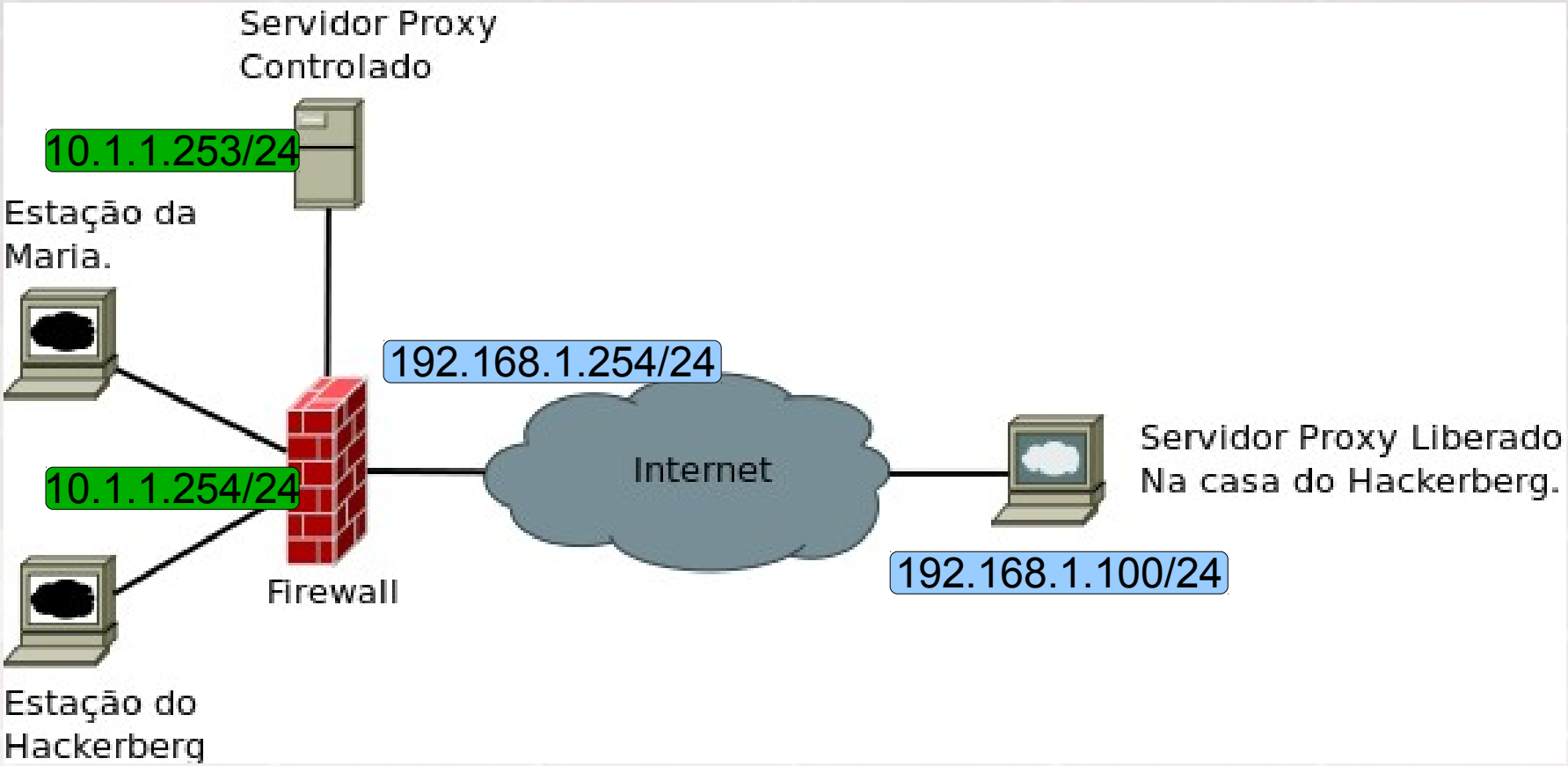
iptables -A FORWARD -p tcp --dport 5940 -s <REDE INTERNA> -d ??? -j ACCEPT

Onde está o real servidor de consulta de cheques? Ele existe? Onde? O que mais roda na porta TCP/5940? etc, etc, etc.

Resultado: Firewall vulnerável ao tunelamento.

Exemplos Práticos

Topologia para o nosso exemplo



Exemplos Práticos

Passo-a-passo para montar um túnel

- Descobrir uma falha no Firewall.
- Preparar uma ferramenta de tunelamento.
- Configurar um proxy externo e liberado.
- Fazer o tunelamento e navegar livremente.
- Manter o anonimato durate o tunelamento.

Exemplos Práticos

Ferramentas para o nosso exemplo

- Squid: Servidor proxy totalmente liberado.
- OpenSSH: Servidor ssh que será usado para fazer o tunelamento criptografado.
- Tcpdump: Sniffer para monitorar o tráfego.
- Iptables: Filtro de Pacotes (Firewall).
- NMAP: Scanner de portas (e muito mais :)).

Exemplos Práticos

Tunelamento com SSH.

Comando para conexão ssh fazendo túnel.

ssh -L 2020:192.168.1.100:3128 root@192.168.1.100 -p 5940

-L: Criar túnel.

Porta_Local:Servidor:Porta_Remota

-p: Porta que o servidor ssh está configurado.

Alertas

Cuidados que devemos ter com túneis

- Você sabe quem está do outro lado do túnel?
- Você sabe por onde a sua informação passa?
- Você sabe o que o cliente de tunelamento pode fazer no seu computador?
- Sua informação é simplesmente repassada ou, quem sabe, armazenada em algum lugar?
- Você digitaria seu dados em um túnel sabendo desses riscos?

Extras

[1] https://www.relakks.com/

[1] https://www.ipredator.se/

[1] http://www.vorratsdatenspeicherung.de

http://filesharefreak.com/2008/10/18/total-anonymity-a-list-of-vpn-service-providers/

http://tecno1.net/excell-bookum-programa-para-voc-acessar-seu-facebook-discretamente/

Obrigado!

DÚVIDAS??

Marcus Augustus Pereira Burghardt

LPIC-1, MCLNA, MCLSA, MCTS

CLA, CCA, ITIL

marcus.apb@gmail.com

http://mapburghardt.blogspot.com