Curso Superior de Tecnologia em Redes de Computadores

Projeto Integrador II

Seminário de andamento 1

Henrique Rippel
hvrippel@gmail.com

Tema do projeto

Mecanismos de detecção e controle para dispositivos de rede sem fio não autorizados (*Rogue AP's*)

Sumário

1. Introdução

Com a facilidade de uso de dispositivos de rede sem fio para expansão da rede local, informações privadas podem facilmente ser capturadas por terceiros, caso não se tenha uma política de segurança adotada na rede.

Para controlar este tipo de situação é necessário ter mapeado o parque de dispositivos e certificar que todos eles estejam aptos/autorizados a estarem em funcionamento.

2. Objetivo

Estudar mecanismos para detecção e controle de dispositivos de rede sem fio não autorizados na rede local.

2.1. Objetivo geral

Mapear a rede sem fio utilizando ferramentas (NMAP, NET-SNMP, Python e outras) para identificar dispositivos suspeitos, aplicando regras (*ACL's*) adequadas (bloqueio de porta, bloqueio de *MAC ADDRESS* ou permitindo o acesso) nos *switches* gerenciáveis mais próximos à eles.

2.2. Objetivos específicos

- ✓ Realizar pesquisa bibliográfica
- ✓ Montar um cenário para estudo
- ✓ Estudar ferramentas de detecção de dispositivos de rede sem fio
- ✓ Estudar a utilização das ferramentas NET-SNMP e NMAP
- ✓ Desenvolver um *script* automatizado para detectar atividades suspeitas e aplicar regras adequadas nas portas dos *switches*
- ✓ Escrever artigo

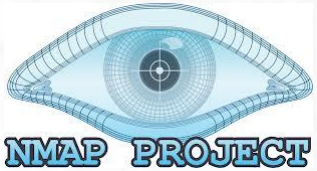
3. Projeto

O presente projeto tem como fundamento a utilização de ferramentas de rede para detecção de dispositivos de rede sem fio, aplicando regras de acordo com a atividade suspeita encontrada.

3. Projeto

As ferramentas adotadas para a construção do projeto, foram:

- NMAP
- NET-SNMP
- Python
- PHP
- MySQL



3. Projeto

Será elaborado um *script*, na linguagem de programação Python, juntamente com as ferramentas NMAP e NET-SNMP, no intuito de executar rotinas de comandos para coletar informações sobre os dispositivos na rede, e aplicar as regras para cada caso. Na Figura 1 temos um exemplo de um *Access Point* não autorizado.

3. Projeto

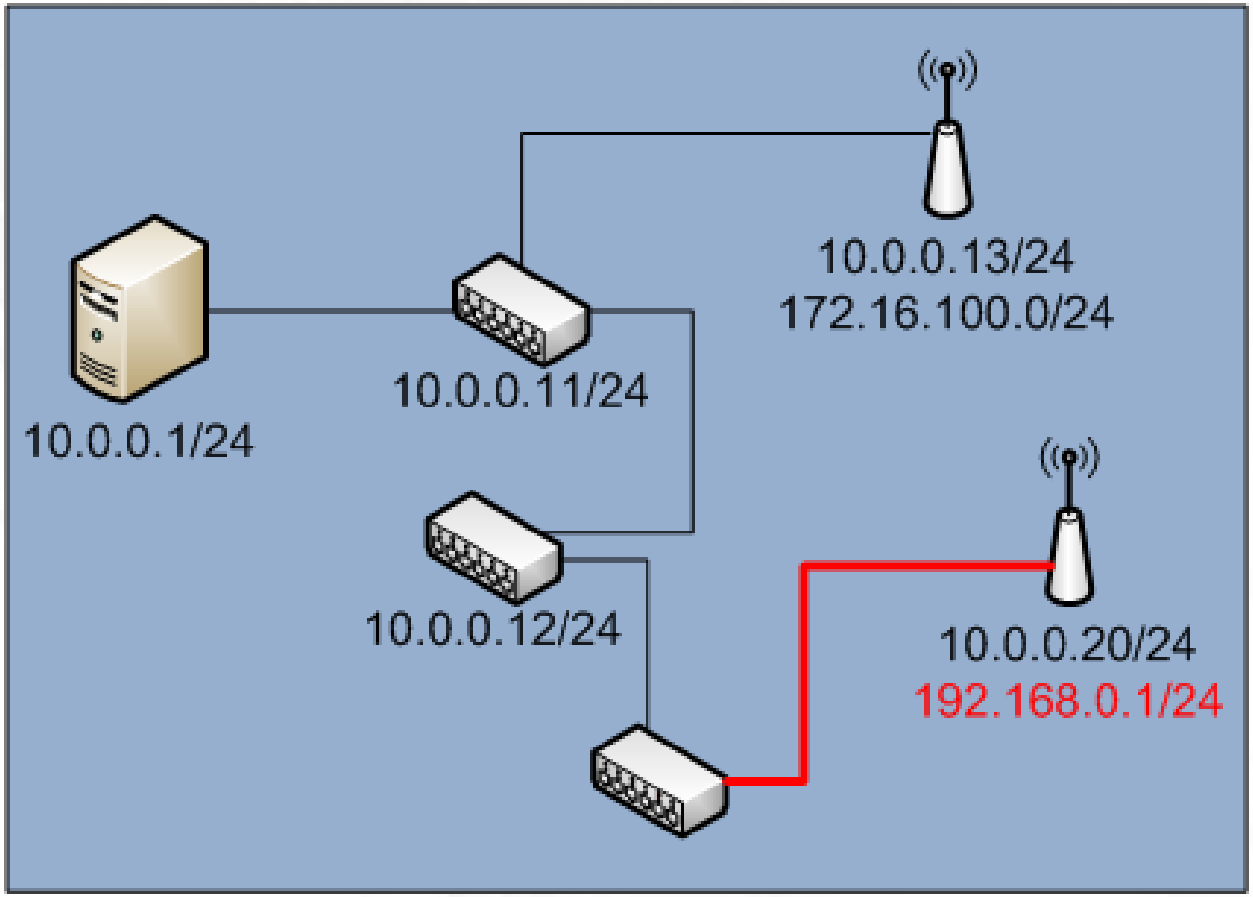
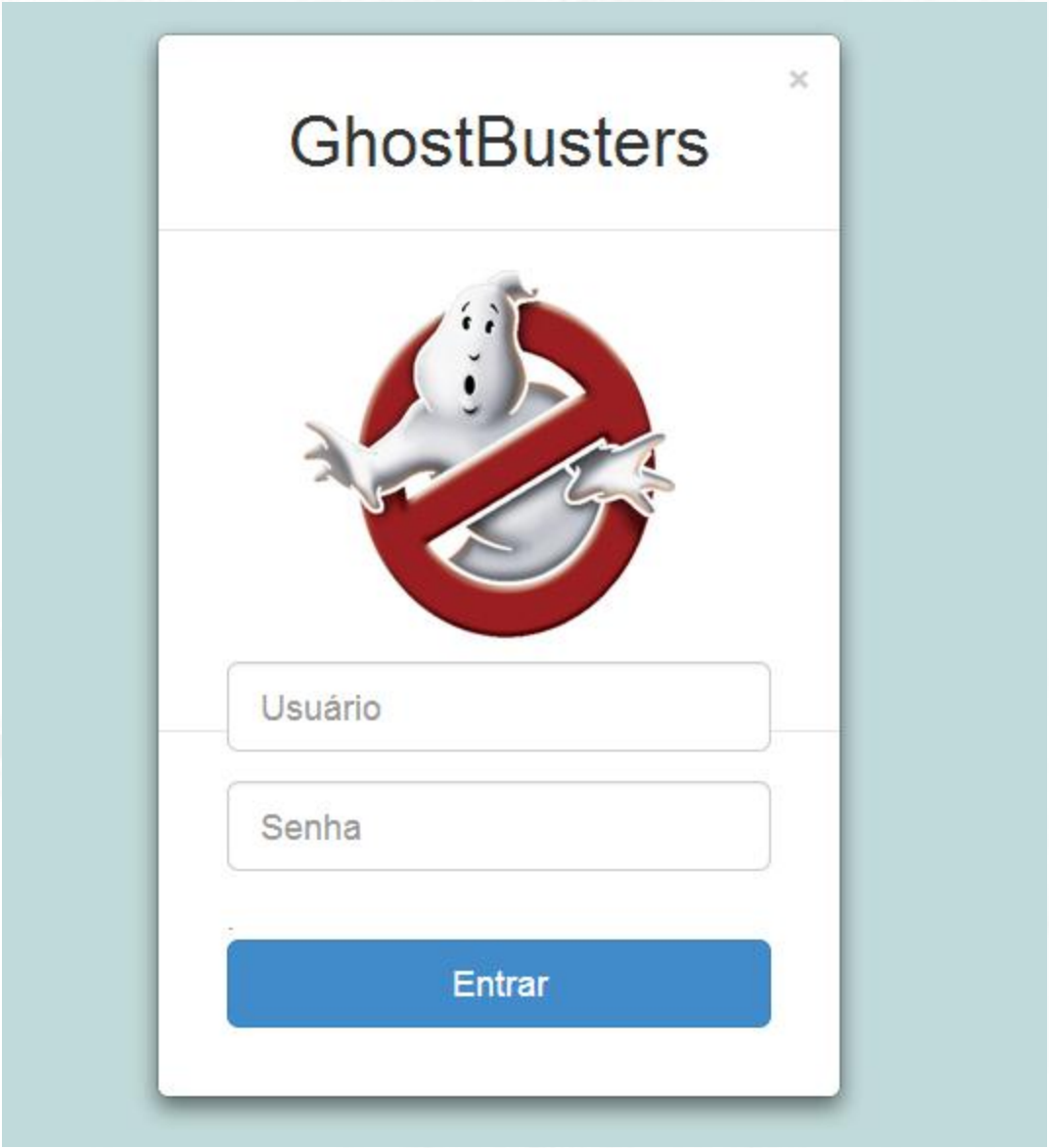
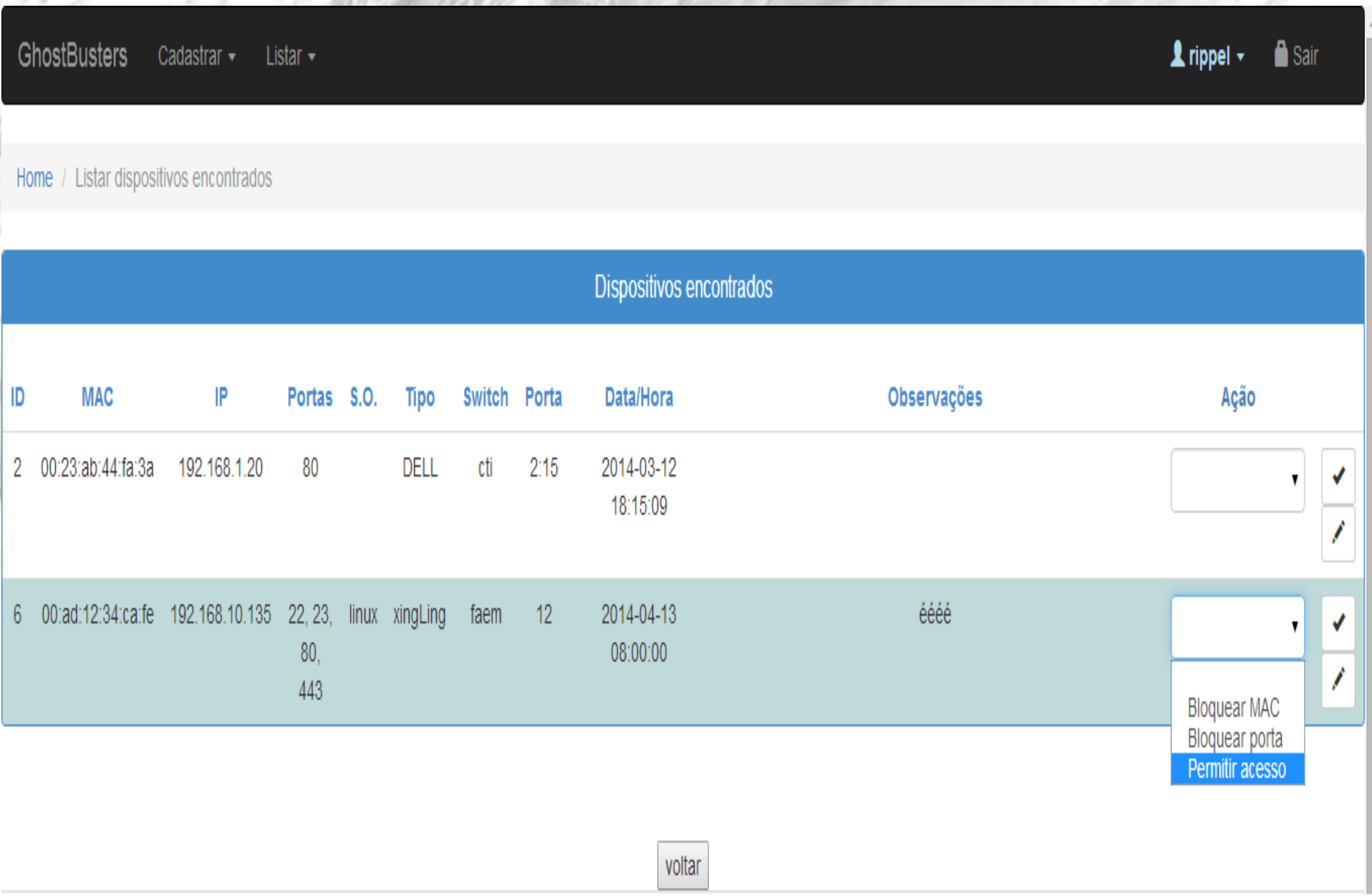


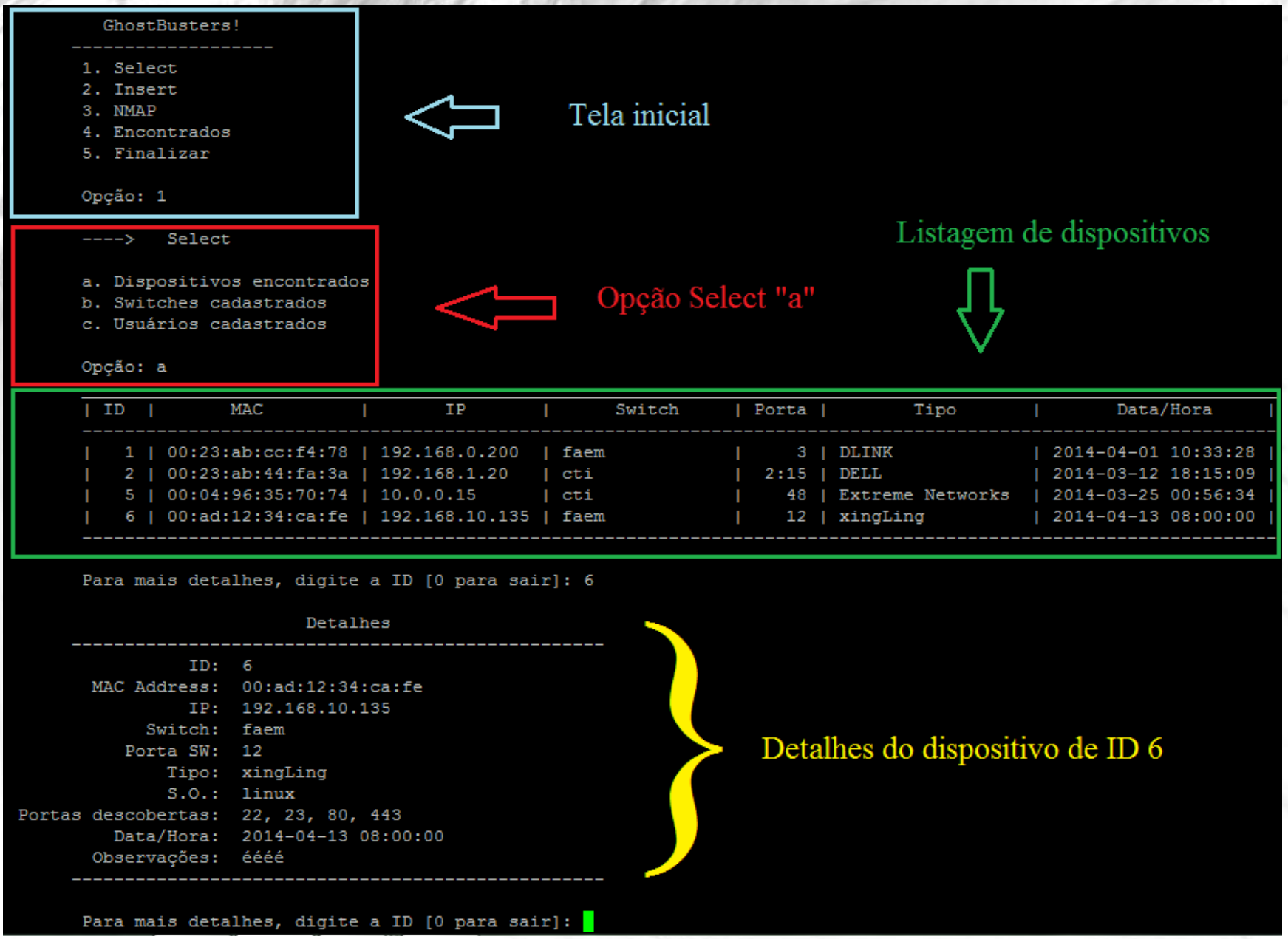
Figura 1

4. Andamento

- ✓ Esboço do projeto
- ✓ Estudo de usabilidade das ferramentas
- ✓ Cenário para testes
- ✓ Painel administrativo via web
- ✓ Desenvolvimento do *script* em Python


GhostBusters
Usuário
Senha
Entrar


GhostBusters
Cadastrar
Listar
rippel
Sair
Home / Listar dispositivos encontrados
Dispositivos encontrados
ID MAC IP Portas S.O. Tipo Switch Porta Data/Hora Observações Ação
2 00:23:ab:44:fa:3a 192.168.1.20 80 DELL cti 2:15 2014-03-12 18:15:09
6 00:ad:12:34:ca:fe 192.168.10.135 22, 23, 80, 443 linux xingLing faem 12 2014-04-13 08:00:00 éééé
Bloquear MAC
Bloquear porta
Permitir acesso
voltar


GhostBusters!
1. Select
2. Insert
3. NMAP
4. Encontrados
5. Finalizar
Opção: 1
Tela inicial
----> Select
a. Dispositivos encontrados
b. Switches cadastrados
c. Usuários cadastrados
Opção: a
Opção Select "a"
Listagem de dispositivos
ID	MAC	IP	Switch	Porta	Tipo	Data/Hora
1	00:23:ab:cc:f4:78	192.168.0.200	faem	3	DLINK	2014-04-01 10:33:28
2	00:23:ab:44:fa:3a	192.168.1.20	cti	2:15	DELL	2014-03-12 18:15:09
5	00:04:96:35:70:74	10.0.0.15	cti	48	Extreme Networks	2014-03-25 00:56:34
6	00:ad:12:34:ca:fe	192.168.10.135	faem	12	xingLing	2014-04-13 08:00:00
Para mais detalhes, digite a ID [0 para sair]: 6
Detalhes
ID: 6
MAC Address: 00:ad:12:34:ca:fe
IP: 192.168.10.135
Switch: faem
Porta SW: 12
Tipo: xingLing
S.O.: linux
Portas descobertas: 22, 23, 80, 443
Data/Hora: 2014-04-13 08:00:00
Observações: éééé
Detalhes do dispositivo de ID 6
Para mais detalhes, digite a ID [0 para sair]:

5. Próximos passos

- ✓ Coletar, com o *script*, as informações necessárias, de forma automática
- ✓ Executar a ação adequada para cada caso encontrado
- ✓ Realizar testes e documentar projeto

6. Conclusões

- ✓ A ferramenta desenvolvida será capaz de centralizar e controlar informações sobre o parque de *switches* gerenciáveis, permitindo executar ações manuais ou automáticas, de acordo com a política adotada

- ✓ O administrador de rede terá capacidade de coletar informações destes dispositivos por meio de um painel web e/ou via linha de comando

7. Cronograma

	Fev	Mar	Abr	Mai	Jun
Realizar pesquisa bibliográfica	X	X	X		
Montar um cenário para estudo		X	X		
Estudar ferramentas de detecção de dispositivos de rede sem fio		X	X		
Estudar a utilização das ferramentas NET-SNMP e NMAP		X	X		
Desenvolver um *script* automatizado para detectar atividades suspeitas e aplicar regras adequadas nas portas dos *switches*		X	X	X	
Escrever artigo			X	X	X

8. Referências bibliográficas

Segurança Informática – Rogue APs (2012). Disponível em: <http://pplware.sapo.pt/informacao/segurana-informtica-rogue-aps-wifi-sabe-o-que-so/>. Acesso em 22/02/2014.

Eliminate Rogue APs (2009). Disponível em: <http://www.rogueap.com/>. Acesso em 22/02/2014.

Net-SNMP (2013). Disponível em: <http://www.net-snmp.org/>. Acesso em 22/02/2014.

NMAP (2014). Disponível em: <http://nmap.org/>. Acesso em 10/03/2014.

Discovering Rogue Access Points With Nmap (2008). Disponível em: <http://securityweekly.com/2008/11/discovering-rogue-access-point.html>. Acesso em 10/03/2014.

Wiki

Henrique Rippel

Wiki – Projeto 8

http://187.7.106.14/wiki2014_1/doku.php?id=projeto08:seminario1

Perguntas?