Curso Superior de Tecnologia em Redes de Computadores

Projeto Integrador II

Seminário de andamento 2

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

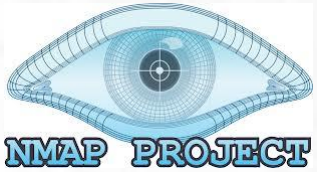
3. Projeto

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

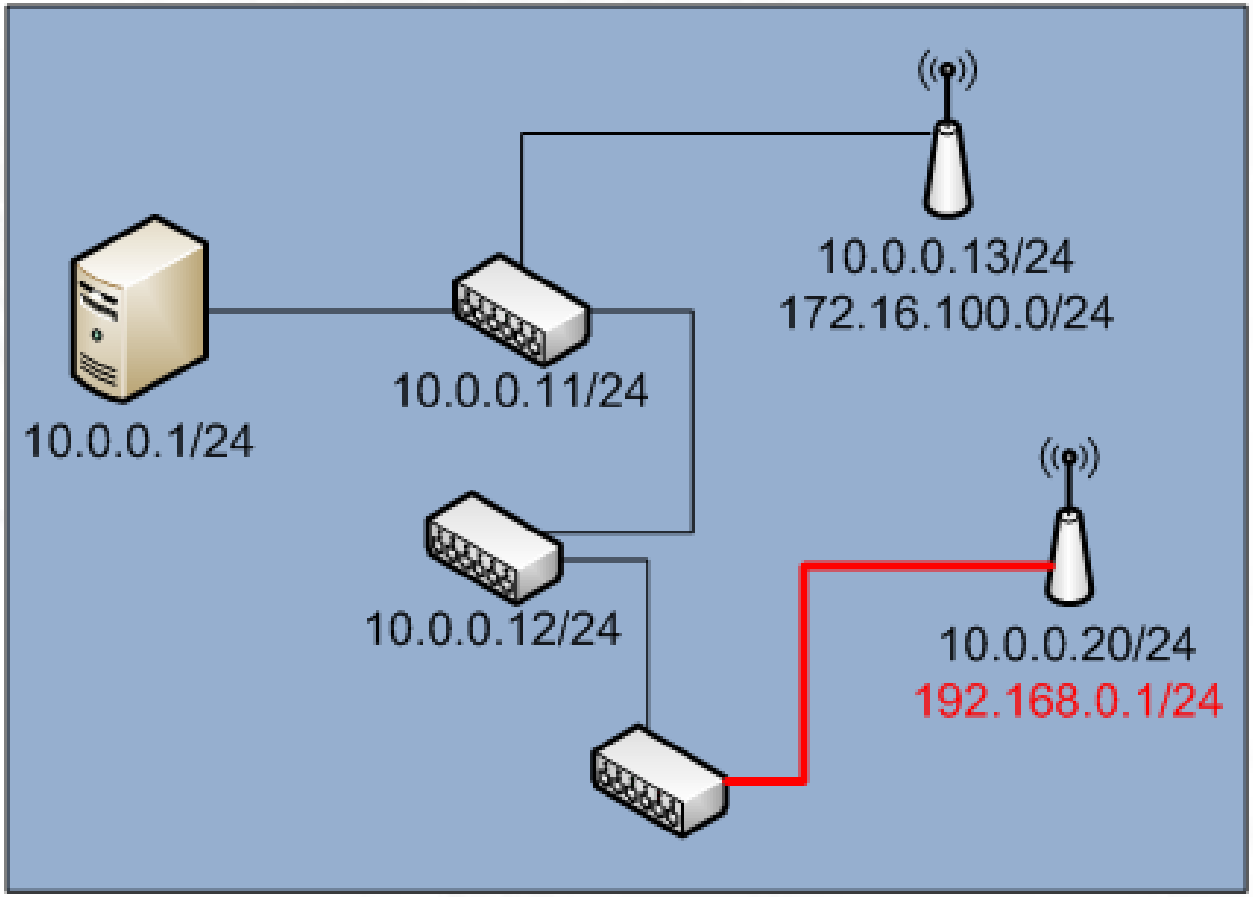
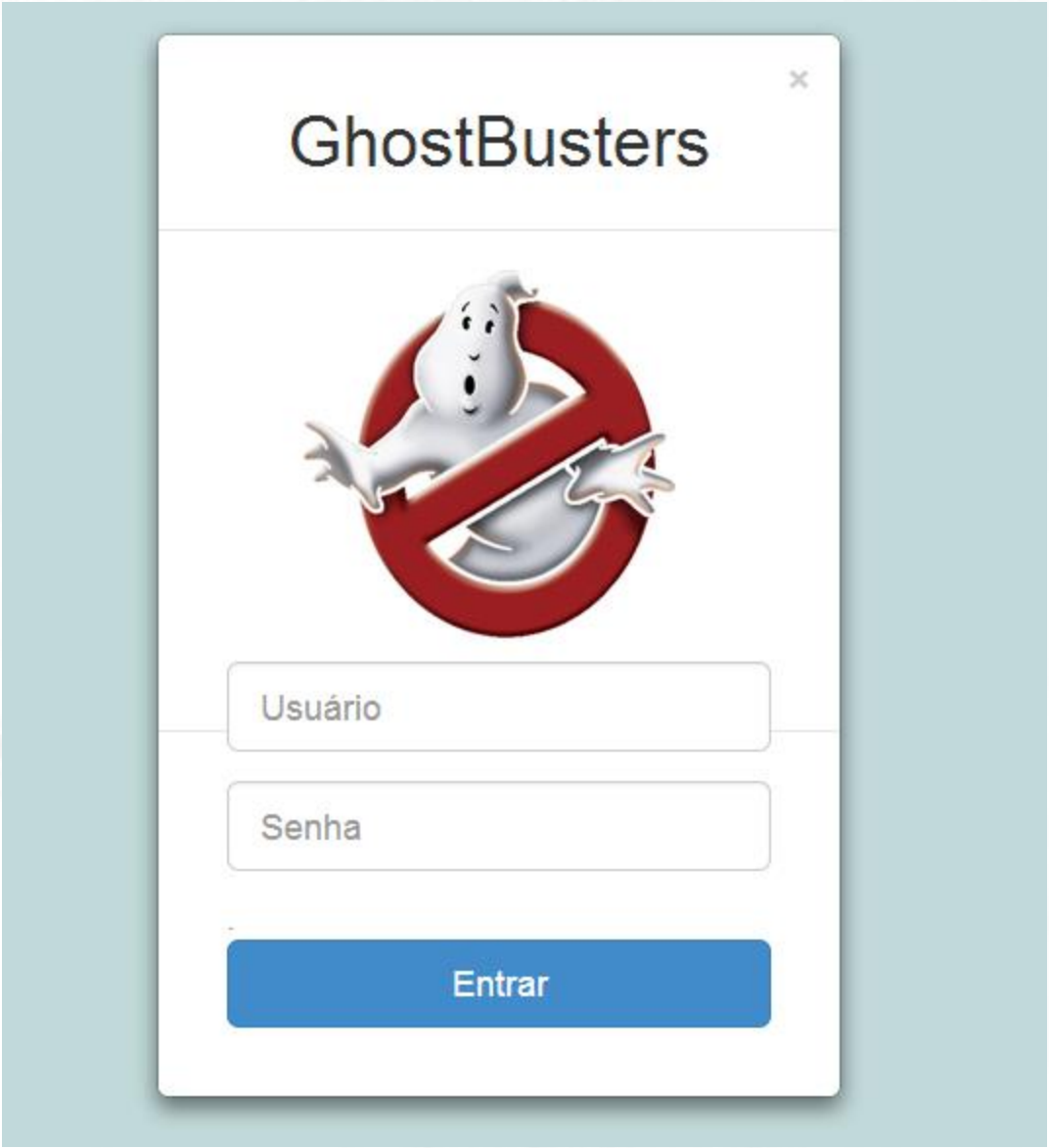


Figura 1

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

Dispositivos encontrados

ID	MAC	IP	Portas	S.O.	Tipo	Switch	Porta	Data/Hora	Observações	Ação
287										
288	326	00:04:96:35:A4:4C	200.132.102.232		23/tcp open ,161/udp open	(Extreme Networks)	Extreme24t	24	2014-05-20 17:19	
289	327	00:15:77:F2:00:DE	200.132.102.236		21/tcp filtered,22/tcp filtered,23/tcp filtered,80/tcp filtered,443/tcp filtered,8080/tcp filtered,53/udp open|filtered,161/udp open|filtered,1900/udp open|filtered,5353/udp open|filtered	(Allied Telesyn)	Extreme24t	13	2014-05-20 17:19	
325										
326										
327	328	A0:F3:C1:11:E9:71	200.132.102.239		21/tcp filtered,22/tcp filtered,23/tcp filtered,80/tcp filtered,443/tcp filtered,8080/tcp filtered,53/udp open|filtered,161/udp open|filtered,1900/udp open|filtered,5353/udp open|filtered	(Unknown)	Extreme24t	5	2014-05-20 17:19	
328										

```
root@rippel:/var/www/projeto# ./ghostbusters.py
```

ID	MAC	IP	Switch	Porta	Tipo	Data/Hora
287	00:04:96:35:97:F2	200.132.102.132	teste		(Extreme Networks)	2014-05-20 16:55
288	2C:27:D7:A1:5D:DC	200.132.102.148	teste	48	(Unknown)	2014-05-20 16:55
289	00:1F:D0:E5:EA:31	200.132.102.150	teste	48	(Giga-byte Technology Co.)	2014-05-20 16:55
291	2C:27:D7:A1:1D:9B	200.132.102.155	teste	48	(Unknown)	2014-05-20 16:55
292	00:1F:D0:E5:15:1F	200.132.102.158	teste	48	(Giga-byte Technology Co.)	2014-05-20 16:55
293	00:1D:7D:FA:27:9F	200.132.102.160	teste	48	(Giga-byte Technology Co.)	2014-05-20 16:55
294	40:01:C6:09:73:C0	200.132.102.165	teste	48	(3com Europe)	2014-05-20 16:55
295	00:19:D1:FA:47:F9	200.132.102.176	teste	48	(Intel)	2014-05-20 16:55
296	00:1F:D0:E4:D5:96	200.132.102.181	teste	48	(Giga-byte Technology Co.)	2014-05-20 16:55
297	D4:AE:52:FC:D6:DD	200.132.102.183	teste	48	(Unknown)	2014-05-20 16:55
298	B0:48:7A:E4:EF:80	200.132.102.186	teste	48	(Unknown)	2014-05-20 16:55
299	E0:69:95:A3:22:1A	200.132.102.190	teste	48	(Unknown)	2014-05-20 16:55
300	00:1F:D0:E6:27:27	200.132.102.191	teste	48	(Giga-byte Technology Co.)	2014-05-20 16:55
301	00:1F:D0:FF:CE:96	200.132.102.207	teste	48	(Giga-byte Technology Co.)	2014-05-20 16:55
302	00:1F:D0:FF:D2:91	200.132.102.217	teste	48	(Giga-byte Technology Co.)	2014-05-20 16:55
303	78:2B:CB:C2:B0:74	200.132.102.220	teste	48	(Unknown)	2014-05-20 16:55
304	D4:AE:52:FC:D6:DB	200.132.102.229	teste	48	(Unknown)	2014-05-20 16:55
305	00:1F:D0:E5:E8:E9	200.132.102.245	teste	48	(Giga-byte Technology Co.)	2014-05-20 16:55

```
                    Detalhes
-------------------------------------------------
                ID:  327
       MAC Address:  00:15:77:F2:00:DE
                IP:  200.132.102.236
            Switch:  Extreme24t
         Porta SW:  13
              Tipo:  (Allied Telesyn)
              S.O.:
      Portas descobertas:  21/tcp   filtered,22/tcp   filtered,23/tcp   filtered,80/tcp   filtered,443/tcp  filtered,8080/tcp filtered,53/udp   open|filtered,1
61/udp  open|filtered,1900/udp open|filtered,5353/udp open|filtered
            Data/Hora:  2014-05-20 17:19
       Observações:
-------------------------------------------------
```


```
                Data/Hora:  2014-05-20 17:19
           Observações:
-------------------------------------------------
```

5. Próximos passos

- ✓ Continuar escrevendo o artigo

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?