

ESTGF POLITÉCNICO DO PORTO	Tipo de Prova Trabalho Prático 1	Ano lectivo	Data
	Curso Licenciatura em Segurança Informática em Redes de Computadores	Hora	
	Unidade Curricular Segurança de Redes	Duração 1h30m	

Nome:

N.º:

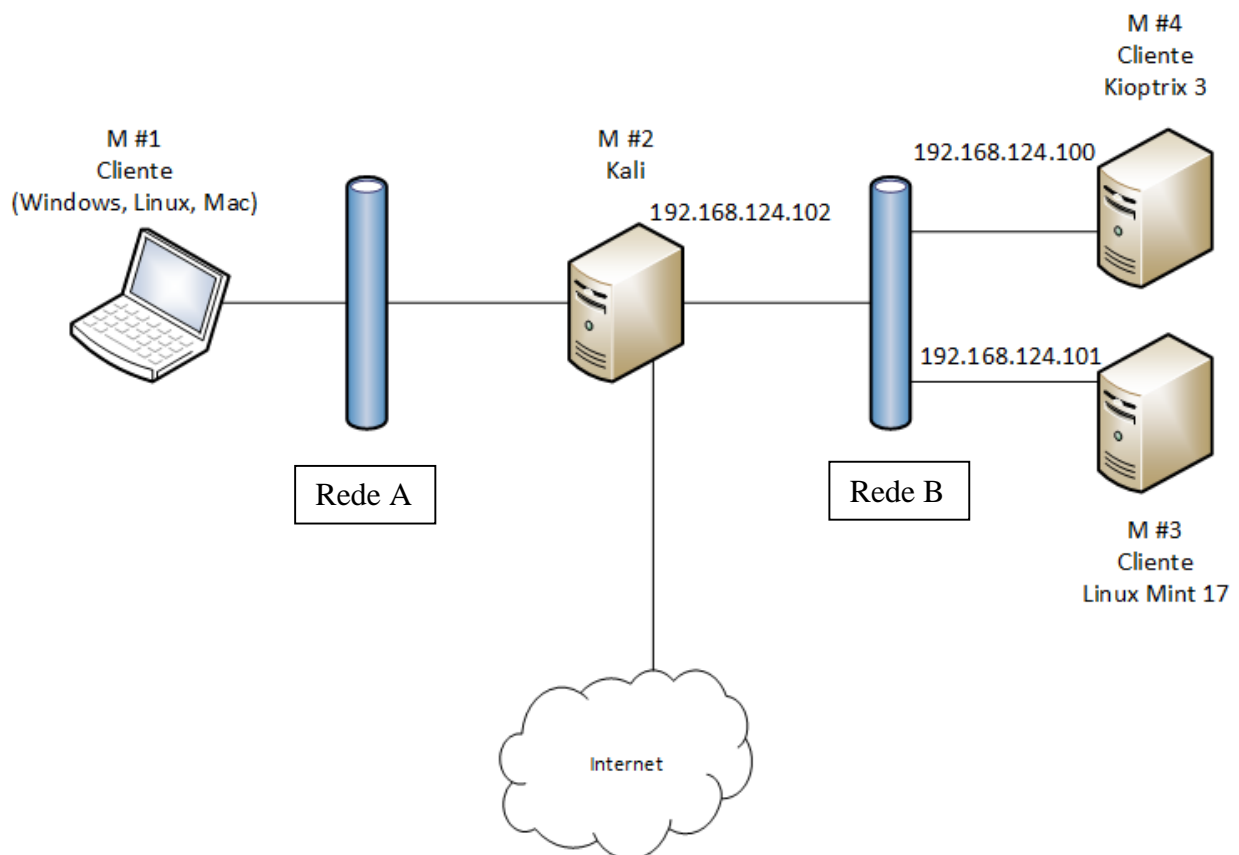
I. Introdução



Uma das tarefas mais importantes de um administrador de sistemas é manter todas as máquinas seguras e disponíveis para suportarem o negócio. Nesse sentido e uma das acções de gestão de segurança de maior importância é a gestão de vulnerabilidades de todas as máquinas que estão conectadas á rede da empresa. É através da exploração destas vulnerabilidades que grande parte dos ataques informáticos é efetuada.

II. Objectivo

Pretende-se que seja entregue um relatório detalhado com a resposta às questões indicadas demonstrando todos os passos efetuados.

III. Cenário



 	Tipo de Prova Trabalho Prático 1	Ano lectivo	Data
	Curso Licenciatura em Segurança Informática em Redes de Computadores	Hora	
	Unidade Curricular Segurança de Redes	Duração 1h30m	

1. Detecção de Sistemas Operativos [4 Valores] [5m]

- 1.1. Indicar qual comando/ferramenta a usar para se conseguir detetar, a partir da M #2, os sistemas operativos das M #3 e #4.
- 1.2. Indicar resultado de comando adequado para a identificação indicada em 1.1.

2. Análise e exploração de Vulnerabilidades [4 Valores] [15m]

- 2.1. A partir da M #2, que ferramentas de análise de vulnerabilidades estudadas poderia utilizar para detecção das mesmas nas M #3 e #4?
- 2.2. E se pretende-se explorar essas potenciais vulnerabilidades, que ferramenta utilizaria?
- 2.3. Seria possível explorar essas mesmas potenciais vulnerabilidades sem recorrer a essa ferramenta? Como?
- 2.4. Classifique as diferentes ferramentas apresentadas em 2.1 e 2.2 quanto à “fase” de hacking em que são, usualmente, utilizadas.

3. Firewall [4 Valores] [10m]



- 3.1. Se na M #2 instalássemos no módulo de Firewall uma regra a impedir todo o tráfego da Rede A para a Rede B, qual seria o impacto no acesso à internet da M #3? Porquê?
- 3.2. Imagine agora que pretendíamos adicionar uma nova máquina Servidor web/e-mail ao nosso cenário. Considerando o discutido nas aulas sobre DMZ e Firewall, qual seria uma possível localização do mesmo? Porquê?

4. IPTables [8 Valores] [60m]

Tendo em consideração o cenário de rede apresentado, realize os seguintes exercícios na máquina #2 (todas as regras devem ser *statefull* e o mais granulares possível):

Faça **Flush** a todas as regras existentes:

```
# iptables -F INPUT
# iptables -F FORWARD
# iptables -F OUTPUT
# iptables -t nat -F
```

 	Tipo de Prova Trabalho Prático 1	Ano lectivo	Data
	Curso Licenciatura em Segurança Informática em Redes de Computadores	Hora	
	Unidade Curricular Segurança de Redes	Duração 1h30m	

Faça **DROP** a todo o tráfego:

```
# iptables -P INPUT DROP
# iptables -P FORWARD DROP
# iptables -P OUTPUT DROP
```

- 4.1. Autorize acesso SSH da M #1 à M #2 (tcp / porta 22).
- 4.2. Autorize todo o tráfego ICMP de toda a Rede B à M #2 (e respetivas respostas).
- 4.3. Autorize acessos a pedidos DNS da M #3 à Internet (tcp e udp / porta 53). Valide se o servidor de DNS (172.20.6.100) está devidamente configurado no ficheiro /etc/resolv.conf da M #3 para poder testar convenientemente!
- 4.4. Autorize acesso a pedidos HTTP e HTTPS da M #3 à Internet (tcp / porta 80 e porta 443).
- 4.5. Autorize acesso a pedido SSH da M #1 à M #3 (tcp / porta 22). Se pretender testar, deverá adicionar uma rota na M #1 para a Rede B (route ADD 192.168.124.0 MASK 255.255.255.0 “gateway ip”) e ativar / instalar o serviço SSH na M #3.