	Tipo de Prova Exame Época Recurso	Ano lectivo 2014/2015	Data 15-07-2015
	Curso Mestrado em Engenharia Informática	Hora 19:00	
	Unidade Curricular Informática Forense e Cibercrime	Duração 2 horas	

Grupo I

1) [10 min]

(2,5 valores)

“Um disco formado com FAT32 usa um protective MBR”. Comente a afirmação, indicando também se concorda ou não com a mesma. Use exemplos concretos.

Não concordo com a afirmação visto que não é devido ao facto de um disco estar formatado com FAT32 que define se um disco tem ou não um protective MBR.

Os discos têm um esquema de partição que pode ser MBR ou GPT: O MBR é o mais antigo, projetado para ser utilizado apenas em discos rígidos e com certas limitações como por exemplo na quantidade de partições primárias e na capacidade máxima de armazenamento.

Visto que atualmente existem outros tipos de suporte de armazenamento foi necessário criar um esquema de partição em que não tenha as limitações do anterior, mas para isso é necessário que todos os computadores tenham suporte e o resultado foi o esquema de partição GPT conter um cabeçalho MBR denominado protective MBR em que permite que um computador com BIOS consiga ler as informações necessárias, deixando a única limitação da necessidade do sistema operativo ter suporte para tal.

Resumidamente um disco pode estar formatado com FAT32 independentemente de utilizar o esquema MBR ou GPT mas apenas existe o cabeçalho do protective MBR quando o disco utiliza o esquema GPT.

2) [10 min]

(2,5 valores)

“A segmentação é uma característica intrínseca à análise forense em redes de computadores que facilita a vida do analista forense.”. Comente a afirmação, indicando também se concorda ou não com a mesma. Use exemplos concretos.

Não concordo totalmente com a afirmação visto que a segmentação pode ser benéfica como exatamente o contrário dependendo do contexto.

Se tomarmos o exemplo de computador, de um analista forense investigar os dispositivos de uma empresa, em um cenário em que uma empresa tem milhares de computadores e em um deles ter ocorrido um crime informático, neste caso a “segmentação” apenas complica a vida do analista forense visto ter de avaliar computador por computador mas se tomarmos o exemplo de uma rede de computadores em que cada tipo de dados percorre em uma rede virtual específica, aí já torna a vida mais fácil se por exemplo existir uma VLAN para logs, outra para os dispositivos dos trabalhadores, etc.

Grupo II

3) [10 min]



(2,0 valores)

Distinga a recolha de dados intrusiva da não intrusiva, dando exemplos concretos de duas situações onde se tenha de recorrer a cada uma destas.

Na recolha de dados intrusiva existe algo em que é sempre comprometido, enquanto em uma recolha de dados não intrusiva o mesmo já não acontece.

Não intrusiva por exemplo quando fazemos uma cópia exata do disco não estamos a alterar nenhuma informação do mesmo ou por exemplo a transferir algo remotamente de um servidor em que não estamos a comprometer a integridade do ficheiro.

Intrusiva caso necessitarmos de abrir um dispositivo ou por exemplo para conseguir uma cópia da memória RAM de um computador necessitamos de instalar um programa no computador o que compromete a integridade do sistema

 	Tipo de Prova Exame Época Recurso	Ano lectivo 2014/2015	Data 15-07-2015
	Curso Mestrado em Engenharia Informática	Hora 19:00	
	Unidade Curricular Informática Forense e Cibercrime	Duração 2 horas	

6.d) Qual é a aplicação geradora do pacote?

Uma aplicação de email visto o protocolo IMAP ser utilizado para tal.

6.e) Qual é o propósito deste pacote?

Transferência de um email do servidor para o utilizador porque o src port é mais baixo do que o dst port. Visto estar encriptado não é possível saber ao certo, mas é possível verificar que existe uma troca de informação com o tamanho de 80 bytes.

7) [20 min]

(3,0 valores)

Apresente uma linha de comandos que lhe permita listar **todos os acessos a servidores de email (POP, IMAP, SMTP, cifrados ou não)**, bem como o **todos os pedidos de resolução de nomes efetuados pelo PC com o endereço IP 172.20.20.15** constantes de uma captura de rede guardada no ficheiro **captura.pcap**. Recorra ao **tcpdump** e filtros do tipo **BPF**.

POP3 não encriptado: tcp 110

POP3 encriptado: tcp 995

SMTP ambos (existem outras portas): tcp 25

IMAP não encriptado: tcp 143

IMAP encriptado: tcp 993

DNS: udp 53

`tcpdump -r captura.pcap \"(src host 172.20.20.15 and dst port 53) or \"(tcp port 110 or tcp port 143 or tcp port 25 or tcp port 993 or tcp port 995 or udp port 53)\"`

ESTGF POLITÉCNICO DO PORTO	Tipo de Prova Exame Época Recurso	Ano lectivo 2014/2015	Data 15-07-2015
	Curso Mestrado em Engenharia Informática	Hora 19:00	
	Unidade Curricular Informática Forense e Cibercrime	Duração 2 horas	

8) [25 min]

(3,0 valores)

Analise a seguinte sessão de terminal de um analista forense digital. Note que o comando utilizado suprime sequências de linhas iguais, apresentando apenas um asterisco (*) no início da linha. As linhas foram ainda numeradas recorrendo ao comando nl.

```
[aap@eb-aap ~] $ hexdump -C -n 1536 hdd.img | nl
 1 00000000 eb 3c 90 6d 6b 66 73 2e 66 61 74 00 02 08 01 00 |.<.mkfs.fat.....|
 2 00000010 02 00 02 00 00 f8 00 01 20 00 40 00 00 00 00 00 |.....|. @.....|
 3 00000020 00 00 08 00 80 00 29 80 32 ea 33 42 41 44 4d 42 |.....).2.3BADMB|
 4 00000030 52 20 20 20 20 20 46 41 54 31 36 20 20 20 0e 1f |R FAT16 ..|
 5 00000040 be 5b 7c ac 22 c0 74 0b 56 b4 0e bb 07 00 cd 10 |. [| | ".t.V.....|
 6 00000050 5e eb f0 32 e4 cd 16 cd 19 eb fe 54 68 69 73 20 |^..2.....This |
 7 00000060 69 73 20 6e 6f 74 20 61 20 62 6f 6f 74 61 62 6c |is not a bootabl|
 8 00000070 65 20 64 69 73 6b 2e 20 20 50 6c 65 61 73 65 20 |e disk. Please |
 9 00000080 69 6e 73 65 72 74 20 61 20 62 6f 6f 74 61 62 6c |insert a bootabl|
10 00000090 65 20 66 6c 6f 70 70 79 20 61 6e 64 0d 0a 70 72 |e floppy and..pr|
11 000000a0 65 73 73 20 61 6e 79 20 6b 65 79 20 74 6f 20 74 |less any key to t|
12 000000b0 72 79 20 61 67 61 69 6e 20 2e 2e 2e 20 0d 0a 00 |ry again.....|
13 000000c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
14 *
15 000001f0 00 00 00 00 00 00 00 00 00 00 00 00 00 55 aa |.....U.|
16 00000200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
17 *
18 00000400 00 00 01 00 00 00 04 00 33 33 00 00 3a b6 03 00 |.....33.....|
19 00000410 ef ff 00 00 01 00 00 00 00 00 00 00 00 00 00 00 |.....|
20 00000420 00 20 00 00 00 20 00 00 00 08 00 00 69 b1 9a 55 |. . . . .i..U|
21 00000430 b8 b1 9a 55 02 00 ff ff 53 ef 01 00 01 00 00 00 |...U....S.....|
22 00000440 a0 af 9a 55 00 00 00 00 00 00 00 00 01 00 00 00 |...U.....|
23 00000450 00 00 00 00 0b 00 00 00 80 00 00 00 3c 00 00 00 |.....<.....|
24 00000460 02 00 00 00 01 00 00 00 39 aa 5b 8a 5e ce 45 55 |. .... 9. [ ^ .EU|
25 00000470 bb 9f b4 67 46 ec e2 f9 00 00 00 00 00 00 00 00 |...gF.....|
26 00000480 00 00 00 00 00 00 00 00 2f 74 6d 70 2f 65 6e 65 |. .... /tmp/ene|
27 00000490 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |r.....|
28 000004a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
29 *
30 000004c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 |. ....|
31 000004d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |. ....|
32 000004e0 08 00 00 00 00 00 00 00 00 00 00 00 06 8d 89 81 |. ....|
33 000004f0 73 a9 4b ae 81 36 11 5a b3 3d 3d 06 01 01 00 00 |s.K..6.Z.==.....|
34 00000500 0c 00 00 00 00 00 00 00 a0 af 9a 55 03 c1 01 00 |. ....U. ....|
35 00000510 04 c1 01 00 05 c1 01 00 06 c1 01 00 07 c1 01 00 |. ....|
36 00000520 08 c1 01 00 09 c1 01 00 0a c1 01 00 0b c1 01 00 |. ....|
37 00000530 0c c1 01 00 0d c1 01 00 0e c1 01 00 0f c1 01 00 |. ....|
38 00000540 10 c2 01 00 00 00 00 00 00 00 00 00 00 00 80 00 |. ....|
39 00000550 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |. ....|
40 00000560 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |. ....|
41 00000570 00 00 00 00 00 00 00 00 8e 01 00 00 00 00 00 00 |. ....|
42 00000580 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |. ....|
43 *
44 00000600
```

Que informação consegue extrair do ficheiro **hdd.img**? Na sua resposta, seja tão exaustivo quanto possível.

Partição FAT16

Nome da partição: BADMBR

Cerca de 12 itens identificáveis