Operação Mr. Evil - Trabalho Prático

CET 8493 | UFCD 9196 - Cibersegurança Ativa | Formador: Paulo Vaz
Formando: João Rodrigo Mota da Costa

1. Qual é a hash da imagem? O hash de aquisição e verificação correspondem?

A hash da imagem é `aee4fcd9301c03b3b054623ca261959a`

2. Qual é o sistema operativo usado no computador?

Microsoft Windows XP.

3. Quando foi a data de instalação do sistema operativo?

19 de agosto de 2004.

4. Qual é a configuração do fuso horário?

Europe/London - British Summer Time (BST)

5. Quem é o proprietário registado?

O proprietário registado é o Greg Schardt.

6. Qual é o nome da conta do computador?

O nome da conta do computador é `N-1A9ODN6ZXK4LQ`.

7. Qual é o nome do domínio principal?

Visto que a máquina não está em nenhum domínio, o nome do domínio está como `localhost`.

8. Quando foi a última data/hora do encerramento do computador?

27 de agosto de 2004.

9. Quantas contas estão regsistadas?

8 contas.

10. Qual é o nome do utilizador que mais usa o computador?

```
Mr. Evil
```

11. Qual foi o último utilizador a iniciar sessão?

```
Mr. Evil
```

12. Liste as placas de rede usadas por este computador?

Xircom Cardbus Ethernet 100 + Modem 56.

13. Prova que o Greg Schardt é o Mr. Evil e também o administrator do computador

`irunin.ini` (localizado em `C:\Program Files\Look@LAN\irunin.ini`)

```
%LANUSER%=Mr. Evil; %ISUSERNTADMIN%=TRUE; %REGOWNER%=Greg Schardt
```

14. IP e MAC Address do computador.

```
%LANIP%=192.168.1.111
%LANNIC%=0010a4933e09
```

15. Fornecedor da placa de rede.

XIRCOM.

16. Encontre pelo menos 3 dos 6 programas instalados pelo Mr. Evil.

Powertoys For Windows XP; MPlayer2 ; OutlookExpress

17. Qual o endereço de email utilizador nas configurações do SMTP do Mr. Evil?

```
whoknowsme@sbcglobal.net
```

18. Quais as configurações de NNTP usadas pelo Mr. Evil?

```
NewsServer="news.dallas.sbcglobal.net"; MailServer="smtp.sbcglobal.net"; NNTPPort=119
```

19. Que programa instalado mostra esta informação?

Outlook Express.

20. Cinco grupos de notícias subscritos pelo Mr. Evil.

```
alt.2600.phreaks.dbx
alt.2600.programz.dbx
alt.2600.hacking.beginner.dbx
alt.2600.hacking.computers.dbx
alt.2600.hacking.websites.dbx
```

21. Configurações do utilizador mostradas qunado o mesmo estava online e num canal de chat?

```
[mirc]
user=Mini Me
email=none@of.ya
nick=Mr
anick=mrevilrulez
host=Undernet: US, CA, LosAngeleesSERVER:losangeles.ca.us.undernet.org:6660GROUP:Undernet
```

22. Três canais de acedidos pelo utilizador.

```
#CyberCafe.UnderNet
#evilfork.EFnet
#thedarktower.AfterNET
```

23. Qual é o nome do ficheiro que contém os dados intercetados pelo Ethereal?

`interception` (localizado em `\Documents and Settings\Mr. Evil\interception`)

24. Que model de dispositivo sem fio foi usado pela vítima?

Windows CE (Pocket PC) - Version 4.20

25. A que sites acedeu a vítima?

```
atwola.com
cnn.com
msn.com
yahoo.com
revenue.net
fastclick.net
doubleclick.net
atdmt.com
advertising.com
centrport.net
list.ru
tribalfusion.com
maktoob.com
durdgereport.com
```

26. Ficheio da cópia do email do Yahoo?

`ShowLetter[1].htm`

27. Email do Mr. Evil?

`mrevilrulez@yahoo.com`

28. Quantos ficheiros exercutáveis estão na reciclagem?

4

29. Esses ficheiros estão apagados definitivamente?

Não.

30. Quais os ficheiros marcados para serem apagados definitivamente pelo sistema?

```
Dc1.exe
Dc2.exe
Dc3.exe
Dc4.exe
```