

Auditoria Forense de Redes e Sistemas – Trabalho Prático

Redes e Segurança Informática

Henrique Coutinho, Nº 16984

Novembro, 2019

Índice

Introdução	3
Desenvolvimento	5
Conclusão	11

Índice de Imagens

Figura 1 - Sistema Operativo e Versão	5
Figura 2 - Nome Do Computador	5
Figura 3 - Data De Instalação do SO	5
Figura 4 - Utilizadores do SO	5
Figura 5 - Utilizadores e Grupos	6
Figura 6 - Configurações de Rede	6
Figura 7 - Vírus	8
Figura 8 - Últimos Sites Visitados	8
Figura 9 - Localização e Data de Criação Da Folha de Cálculo	9
Figura 10 - Email Jean	10
Figura 11 - Anexo Email Jean	10

Introdução

Com este relatório pretendo expor a minha abordagem ao trabalho de auditoria que nos foi solicitado pelo professor da disciplina.

Irei abordar os diferentes processos e programas que foram previamente utilizados na sala de aula e fizeram parte da minha “*checklist*” para a realização deste trabalho nomeadamente:

Processos

Verificação do processo de auditoria

- Análise do documento de solicitação com os requisitos da investigação
- Criação do Processo
 - Pasta do processo
- Exportar ficheiros de registo
 - SAM, System, e NTUSER.dat
- *Bypass* ficheiro SAM
 - Exportar a informação do NTUSER.dat
- Definições de Hora
 - Identificar o fuso horário utilizado no dispositivo da vítima
- Criação do caso nas ferramentas forenses
 - Guardar os ficheiros relativos ao processo nas diretorias definidas para o efeito;
 - Utilização de “data carving”.
- Montar a imagem forense recorrendo ao FTK Imager
- Malware e Rootkit Scan
- Análise do registo SAM
 - Documentar todas as contas de utilizador
- Análise e registo de Sistema e Software
 - Documentar o nome do computador
 - Documentar sistema operativo e respetiva data de instalação;
 - Documentar definições de rede
- Registo NTUSER.dat
 - Documentar últimos url’s acedidos

- Criar assinatura das evidências:
 - SHA256
- Análises adicionais
 - Correio eletrónico

Software Utilizado

- RegReport
- Autopsy
- FTK Imager
- HashMyFiles

Desenvolvimento

- Qual é o sistema operativo e respetiva versão do computador da Jean?

De acordo com o RegReport do computador da Jean o Sistema Operativo utilizado era o Windows XP.

```
Operating System
=====

Operating system: Microsoft Windows XP
Version number:   5.1.2600
```

Figura 1 - Sistema Operativo e Versão

- Qual é o nome do computador da Jean?

```
Computer name: JEAN-13FBF038A3
```

Figura 2 - Nome Do Computador

- Qual é a data de instalação do sistema operativo?

Quando criei o RegReport do computador da Jean, este estava com o fuso horário UTC, sabendo esta informação consegui definir com exatidão as horas em que foram efetuados os processos do computador. Foi a partir do RegReport que consegui a maior parte das informações sobre a Jean.

```
Install date: 13/05/2008 21:29:32 UTC
```

Figura 3 - Data De Instalação do SO

- Quantos utilizadores existem no sistema operativo?

```
Users and User Groups
=====

System-ID: S-1-5-21-484763869-796845957-839522115

Accounts / Usernames:
Abijah
Addison
Administrator
Devon
Guest
HelpAssistant
Jean
Kim
```

Figura 5 - Utilizadores e Grupos

Quais eram as configurações de rede do computador?

```
Network connections:
Local Area Connection
  DHCP active: Yes
  DHCP Server IP: 192.168.117.254
  DHCP IP Address: 192.168.117.129
  DHCP Subnet mask: 0.0.0.0
  DHCP Default Gateway: 192.168.117.2
  DHCP active: localdomain
  DHCP active: 192.168.117.2
  IP Auto Configuration: 0.0.0.0
  Last modified: 21/07/2008 01:27:40 UTC (Services\...\Parameters\Tcpip)
  Last modified: 21/07/2008 01:31:12 UTC
(Services\Tcpip\Parameters\Interfaces\...)
```

Figura 6 - Configurações de Rede

- **Quais os programas que estão instalados**

Software

=====

```
Adobe Flash Player ActiveX
  Last modified: 10/07/2008 20:09:03 UTC
  Uninstall: C:\WINDOWS\system32\Macromed\Flash\uninstall_activeX.exe

Adobe Flash Player Plugin
  Last modified: 14/05/2008 05:48:01 UTC
  Uninstall: C:\WINDOWS\system32\Macromed\Flash\uninstall_plugin.exe

Aim Plugin for QQ Games
  Last modified: 18/07/2008 04:31:42 UTC
  Uninstall: C:\Program Files\Tencent\QQ Games\Plugin\Uninstall.EXE

AIM Toolbar 5.0
  Last modified: 18/07/2008 04:29:28 UTC
  Uninstall: "C:\Program Files\AOL\AIM Toolbar 5.0\uninstall.exe"

AIM Tunes
  Last modified: 18/07/2008 04:30:49 UTC
  Uninstall: C:\Program Files\AIMTunes\Uninstall.exe
```

AIM 6
Last modified: 18/07/2008 04:29:14 UTC
Uninstall: C:\Program Files\AIM6\uninst.exe

Windows Genuine Advantage Validation Tool (KB892130)
Last modified: 14/05/2008 06:32:13 UTC
Install date: 20080514

Security Update for Windows XP (KB923789)
Last modified: 07/06/2008 05:11:11 UTC
Uninstall: C:\WINDOWS\system32\MacroMed\Flash\genuinst.exe
C:\WINDOWS\system32\MacroMed\Flash\KB923789.inf

Mozilla Firefox (3.0.1)
Last modified: 11/07/2008 05:20:12 UTC
Install path: C:\Program Files\Mozilla Firefox 3 Beta 5
Uninstall: C:\Program Files\Mozilla Firefox 3 Beta 5\uninstall\helper.exe

QQ Bubble Arena
Last modified: 18/07/2008 04:57:53 UTC
Uninstall: C:\Program Files\Tencent\QQ Games\QQ Bubble
Arena\Uninstall.EXE

QQ Games
Last modified: 18/07/2008 04:31:41 UTC
Uninstall: C:\Program Files\Tencent\QQ Games\Uninstall.EXE

Viewpoint Media Player
Last modified: 18/07/2008 04:29:26 UTC
Uninstall: C:\Program Files\Viewpoint\Viewpoint Media
Player\mtsAxInstaller.exe /u

Windows Genuine Advantage Validation Tool (KB892130)
Last modified: 14/05/2008 06:32:13 UTC

Microsoft Office 2000 Premium
Last modified: 06/07/2008 07:38:43 UTC
Install date: 20080706
Uninstall: MsiExec.exe /I{00000409-78E1-11D2-B60F-006097C998E7}

WebFldrs XP
Last modified: 12/07/2008 03:05:46 UTC
Install date: 20080513


VMware Tools
Last modified: 19/07/2008 23:32:23 UTC
Install date: 20080704
Uninstall: MsiExec.exe /I{3B410500-1802-488E-9EF1-4B11992E0440}

Microsoft Visual C++ 2005 Redistributable
Last modified: 19/07/2008 23:31:36 UTC
Install date: 20080704
Uninstall: MsiExec.exe /X{7299052b-02a4-4627-81f2-1818da5d550d}

=====

- **O computador, tem vírus? Se sim, quais?**

Para este teste usei o Windows Defender e o MalwareBytes. O Windows Defender detetou um trojan enquanto que o MalwareBytes não encontrou nenhuma ocorrência. A minha conclusão, após observar o comportamento dos ficheiros em questão, foi que sim, o computador tinha vírus, visto estes ficheiros não pertencerem a nenhum do software fidedigno instalado.



Remediação incompleta
Grave

30/10/2019 22:38

Estado: Falhou
Essa ameaça ou aplicação pode não estar completamente remediada.

Ameaça detetada: TrojanDownloader:Win32/Renos.gen!Z
Nível de alerta: Grave
Data: 30/10/2019 22:39
Categoria: Trojan Downloader
Detalhes: Este programa apresenta mensagens de produto enganadoras.

[Mais informações](#)

Itens afetados:

containerfile: Volume{baccb0e5-eabb-11e9-8d75-80c5f2f2d6dc}\[unallocated space]\0169216\0538576
file: Volume{baccb0e5-eabb-11e9-8d75-80c5f2f2d6dc}\[unallocated space]\0169216\0538576->(EXEEmb)
file: \\?\Volume{baccb0e5-eabb-11e9-8d75-80c5f2f2d6dc}\[unallocated space]\0169216\0538576->(EXEEmb)

Ações

- **Quais são os últimos 5 web sites visitados?**

Utilizei o Autopsy para conseguir ver os últimos 5 websites visitados.

Listing									
Web History									
Source File	URL	Date Accessed	Referrer URL	Program Name	Domain	Username	Data Source	Tags	
places.sqlite	http://en-us.www.mozilla.com/en-US/firefox/3.0.1/whatsn...	2008-07-21 01:30:44 UTC		Firefox	en-us.www.mozilla.com		nps-2008-jean.E01		
places.sqlite	http://en-us.start2.mozilla.com/firefox?client=firefox-a&rls=...	2008-07-21 01:30:44 UTC		Firefox	en-us.start2.mozilla.com		nps-2008-jean.E01		
places.sqlite	http://www.google.com/firefox?client=firefox-a&rls=org...	2008-07-21 01:30:41 UTC		Firefox	www.google.com		nps-2008-jean.E01		
places.sqlite	http://maps.google.com/	2008-07-21 00:10:56 UTC		Firefox	maps.google.com		nps-2008-jean.E01		
places.sqlite	http://www.tripadvisor.com/ShowUrl-g32199-d604451-a_...	2008-07-20 23:54:36 UTC		Firefox	www.tripadvisor.com		nps-2008-jean.E01		

Figura 8 - Últimos Sites Visitados

- Qual é a localização da folha de cálculo?
- +
- Quando é que a Jean criou a folha de cálculo?

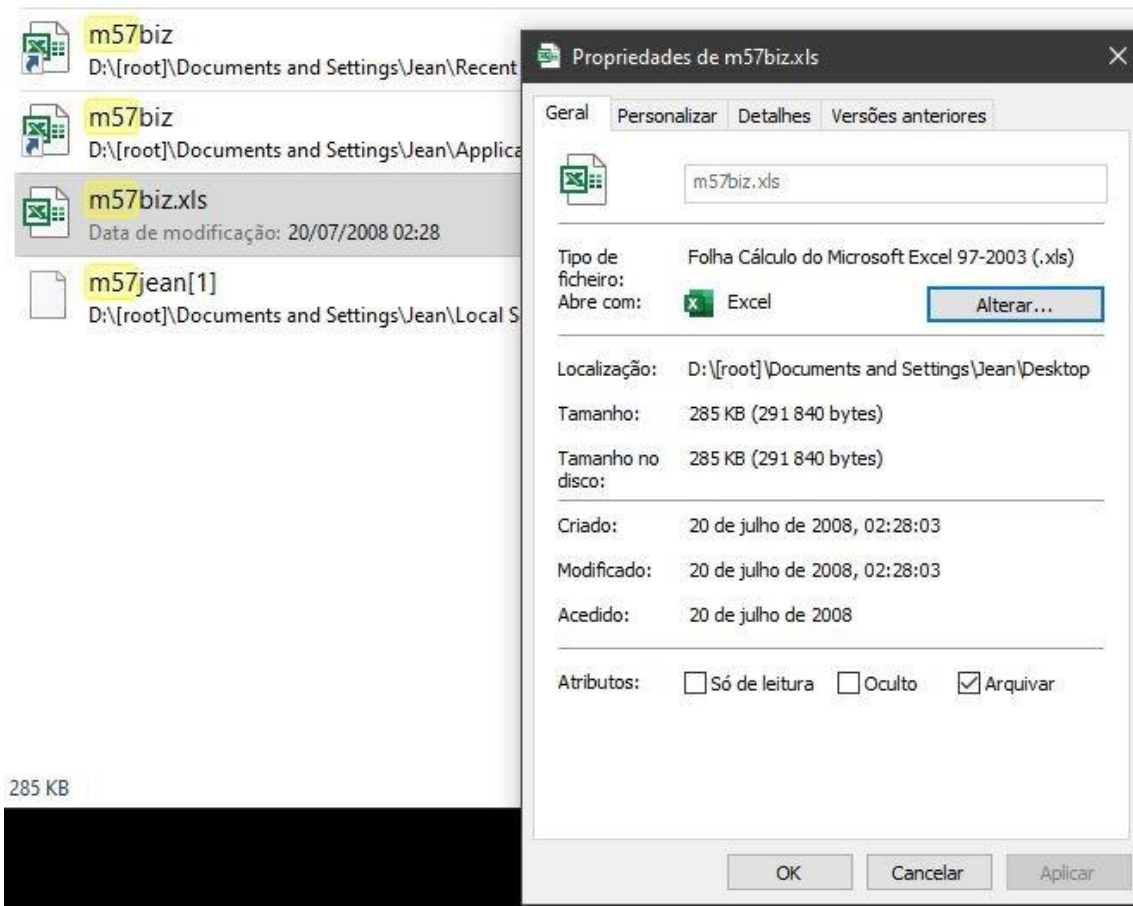


Figura 9 - Localização e Data de Criação Da Folha de Cálculo

Encontrei esta informação ao entrar no disco da Jean. Inicialmente não tinha permissão para aceder às pastas e ficheiros do disco, portanto tive de alterar o modo de acesso para “read only”, visto este permitir listar ficheiros e pastas. Depois disso procurei por ficheiros .xls no disco da Jean para encontrar o ficheiro excel exposto.

- Qual é o valor SHA256 da folha de cálculo?

Sha256 - 34456b5f714dc9d8dd23c742d54c3f5f582ecb042bc1c4d3042b88203863779f

- Como é que a folha de cálculo saiu do computador da Jean para ir parar ao site da empresa concorrente?

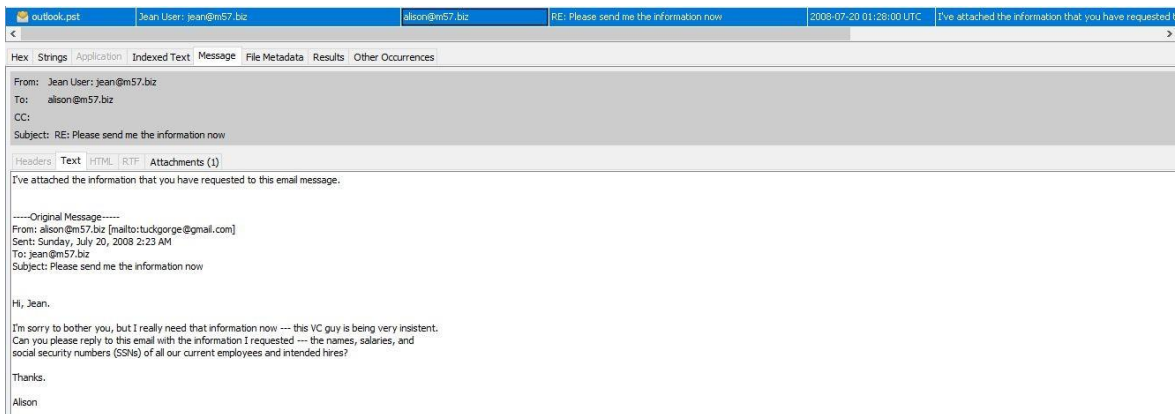


Figura 10 - Email Jean

+

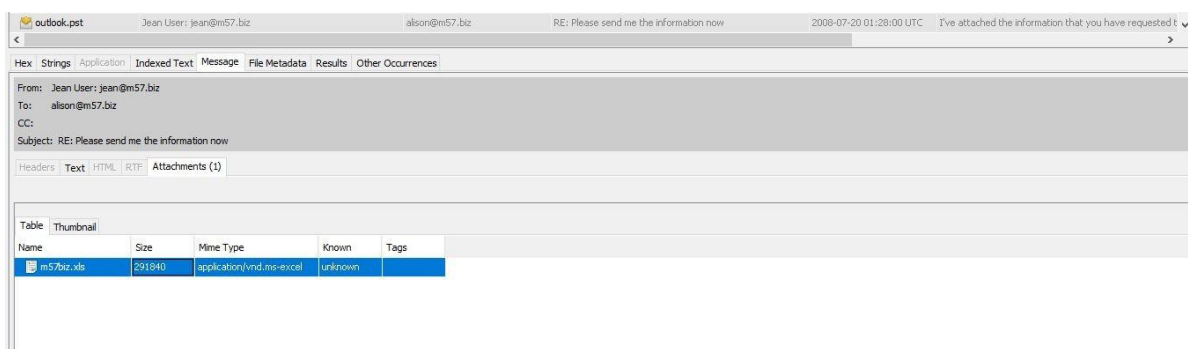


Figura 11 - Anexo Email Jean

Para encontrar esta informação tive que investigar os emails da Jean um a um até encontrar o email onde foi feito o vazamento das informações da empresa. Acabei por o conseguir encontrar e é possível ver que o email que a Jean pensou ter sido enviado pelo Alisson na verdade tinha sido enviado por um utilizador não pertencente à empresa com o email "tuckgorge@gmail.com", que receberia a resposta da Jean e consequentemente o ficheiro da empresa.

Conclusão

Com este trabalho ganhei algumas noções básicas sobre como deve ser feita a auditoria forense de um computador e aprendi que é possível recuperar inúmeras informações de um sistema que anteriormente pensei serem inacessíveis.

Com o decorrer do trabalho fiquei mais interessado pelo assunto e acabei por achar que é uma tarefa extremamente importante na área da informática da o qual não tinha conhecimento e por essa razão gostei de realizar este trabalho e assim explorar outros temas.