Instituto Politécnico do Porto

Escola Superior de Tecnologia e Gestão de Felgueiras

Mestrado em Engenharia Informática

Informática Forense e Cibercrime

Ano Letivo de 2014/2015

Autores:

8090228 - Luís Manuel Magalhães de Sousa

8110253 - Joaquim Cristiano Sampaio Carvalho

Índice de conteúdo

1. Introdução 3
2. Ferramentas Utilizadas 4
3. Funcionalidades 5
4. Modo de Execução 7
5. Conclusão 8
6. Referências de Apoio 9

1. Introdução

O presente documento tem o objetivo de demonstrar o trabalho desenvolvido. Este trabalho consistiu na elaboração de um script, que analisa uma captura de rede, sob a forma de um ficheiro pcap. O script foi desenvolvido em bash scripting e permite extrair informações do ficheiro pcap. Informações como: listagem de ligações, equipamentos, protocolos, ficheiros presentes, portos utilizados, procurar por emails, ou por qualquer string, criar resumos de ficheiros, entre outras funcionalidades. Além disso, é possível gerar ficheiros de texto e reports em html para apresentar os resultados ao utilizador.

2. Ferramentas Utilizadas

De forma a dar consistência ao trabalho desenvolvido foram utilizadas as seguintes ferramentas [1,5]:

tshark – permite analisar e extrair informações de capturas de rede;
md5sum – criar resumos de hash md5;
Sha1sum – criar resumos de hash sha1;
Sha256sum – criar resumos de hash sha256;
Sha512sum – criar resumos de hash sha512;
Chaosreader – extrair informações para ficheiros html;
Tcptrace – criar gráficos de tráfego de rede, obtido na captura;
Tcpdump – permite recolher e analisar capturas de rede;
Foremost – recuperar ficheiros na captura de rede;
capinfos – permite obter informações sobre o ficheiro de captura;

3. Funcionalidades

- **Validação do número de argumentos;**

Permite validar se são introduzidos 2 argumentos válidos.

- **Verificação se o ficheiro de captura é valido;**

Permite verificar se existe o ficheiro de captura passado por argumento

- **Verificação das aplicações necessárias;**

Permite verificar se o script tem todas as aplicações necessárias para executar. Se não tiver informa o utilizador que não tem e automaticamente é instalada [6].

- **Obter informações do ficheiro de captura;**

Indica o número de pacotes da captura, o tamanho da captura, a duração, as hashs entre outras informações relevantes.

- **Obter um lista de hosts no protocolo IPv4 e Ipv6;**

Permite obter todos os ips no protocolo ipv4 e ipv6

- **Obter uma lista de todos os equipamentos (IP´S) na rede;**

Permite obter todos os ips na rede

- **Obter Ligações por protocolo: ethernet, ip, tcp e udp;**

Contém todas as ligações por protocolo.

- **Obter os equipamentos mais usados;**

Contém os equipamentos mais usados, e também os equipamentos mais usados por protocolo : IP, TCP e UDP.

- **Obter uma estatística hierárquica sobre os serviços e protocolos na rede;**

Permite obter informações sobre o protocolo e os serviços a serem usados na rede.

- **Obter os portos usados ;**

Permite obter uma lista sobre as portas que são utilizadas e por quem.

- **Obter Ficheiros presentes na captura ;**

Permite realizar carving, usando a ferramenta Foremost para extrair todos os ficheiros possíveis na captura.

- **Reports em HTML (chaosreader reports);**

Report em HTML com o ip de origem e ip de destino, o protocolo usado, os bytes utilizados em sessões TCP e UDP. Ainda é possivel extrair o conteúdo trocado através dos gets e posts, obter imagens, entre outras informações.

- **Pesquisar e-mails usando uma expressão regular;**

Permite obter todos os e-mails na captura.

- **Pesquisar uma determinada strin**g;

Permite procurar por uma determinada string (ex:pass).

- **Verificar sessões de rede;**

Permite obter nas ligações tcp, o inicio da sessão, o fim da sessão, o ip de origem e destino, a porta usada, o número de bytes transferidos e o número de pacotes transferidos.

- **Criar hashs (md5, sha1, sha256, sha512) ;**

Permite criar resumos md5, sha1, sha256 e sha512 do ficheiro de captura.

- **Todos os comandos são guardados em ficheiros de texto e html;**

Todas as informações podem ser acedidas através de ficheiros de texto e ficheiros html.

4. Modo de Execução

Para uma execução mais fácil devem ser seguidos os seguintes procedimentos:

- Colocar o ficheiro da **captura** e o **script** no mesmo diretório;
- Abrir o terminal e navegar até a localização do ficheiro:
  - ex: cd /home/pcap;
- Na janela de terminal:
  - Dar permissões de leitura/permissões totais ao script (chmod 555 script.sh / chmod 777 script.sh);
  - Executar o script
    - sudo ./ifc_grupo5.sh captura.pcap pasta_de_saida

Ao executar verifica se os argumentos são válidos.

Depois de executado o script, o mesmo verificará se tem todas as aplicações necessárias para executar, senão o utilizador é avisado que falta aquela aplicação e a mesma é instalada automaticamente.

Apaga a pasta de output se ela já existir.

Posto isto, é apresentado um menu com as funcionalidades que o utilizador poderá usufruir.

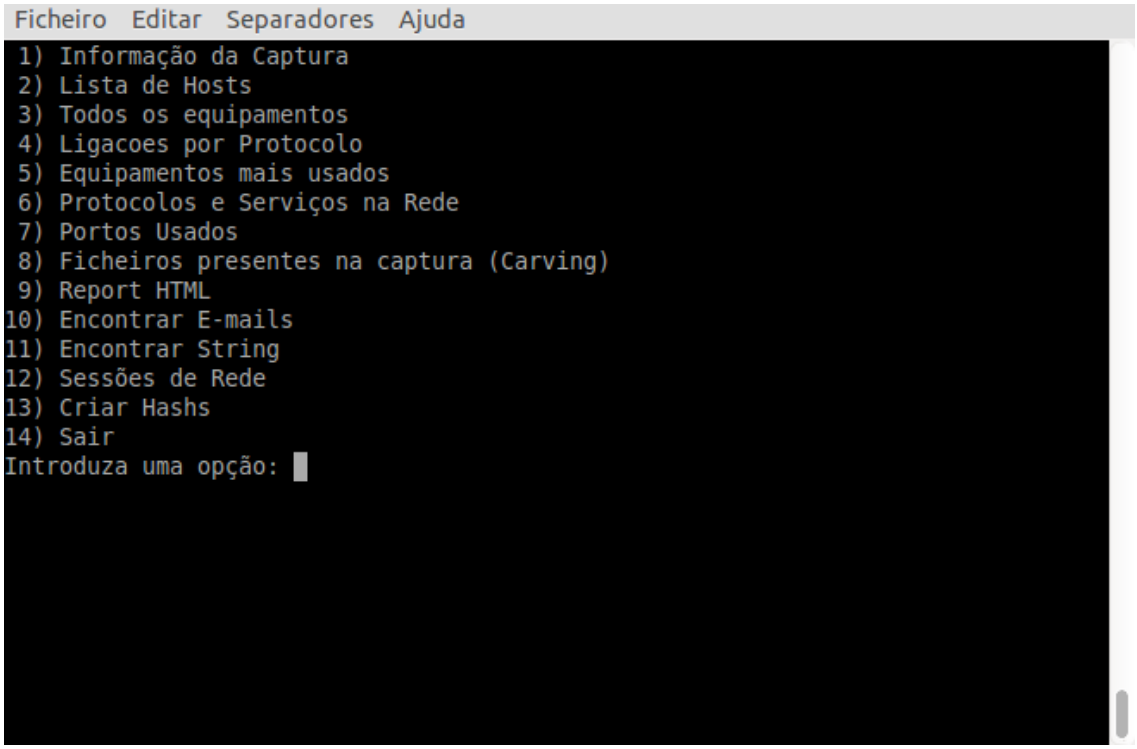

Figura 1: Menu Principal do script

Depois de executar um comando é possível ver o resultado do mesmo em html. Para isso basta executar o ficheiro **index.html** que se encontra na raiz da pasta de saida.

5. Conclusão

Este relatório tem o objetivo de demonstrar todas as funcionalidades implementadas. Ao longo do trabalho surgiram algumas questões, relativamente à utilização dos comandos e estruturas de controlo mais adequadas. Estas dúvidas foram superadas com o decorrer da implementação. O trabalho contribuiu de forma positiva para a nossa aprendizagem. De uma forma geral cumprimos os objetivos estabelecidos, mas temos plena noção que este trabalho poderia ter uma dimensão maior, dado o número de comandos e informações, que podem ser utilizados/extraídas numa captura de rede.

6. Referências de Apoio

[1] InfoSec, “InfoSec Handlers Diary Blog - Tools for extracting files from pcaps.” [Online]. Available: https://isc.sans.edu/diary/Tools+for+extracting+files+from+pcaps/6961. [Accessed: 10-Jun-2015].

[2] Wireshark, “Wireshark · Command Line Manual Pages.” [Online]. Available: https://www.wireshark.org/docs/man-pages/. [Accessed: 10-Jun-2015].

[3] “Network Traffic Analysis With Linux Tools.” [Online]. Available: http://www.slashroot.in/network-traffic-analysis-linux-tools. [Accessed: 10-Jun-2015].

[4] “Packet sniffing - Noah.org.” [Online]. Available: http://www.noah.org/wiki/Packet_sniffing. [Accessed: 10-Jun-2015].

[5] “PCAP Files Are Great Arn’t They” [Online]. Available: https://www.trustwave.com/Resources/SpiderLabs-Blog/PCAP-Files-Are-Great-Arn-t-They--/. [Accessed: 11-Jun-2015].

[6] “bash - Check if a package is installed and then install it if it’s not - Stack Overflow.” [Online]. Available: http://stackoverflow.com/questions/1298066/check-if-a-package-is-installed-and-then-install-it-if-its-not. [Accessed: 11-Jun-2015].