Trabalho Prático N.º 2

Informática Forenses e Cibercrime

António Pinto
apinto@estgf.ipp.pt

ESTGF | POLITÉCNICO DO PORTO

Maio 2015

1 Considerações gerais

O trabalho prático consiste na elaboração de um *script*, que analise uma captura de tráfego de rede (ficheiro pcap), e de um relatório. O trabalho deverá ser desenvolvido em grupo. Serão aceites trabalhos individuais, desde que o aluno manifeste atempadamente a intenção de o fazer.

A deteção de trabalhos fraudulentos invalida a nota de todos os grupos de todos os trabalhos envolvidos. Serão considerados trabalhos fraudulentos, aqueles onde se verifique trabalho desenvolvidos por pessoas que não façam parte do grupo, na totalidade do trabalho ou apenas em parte deste.

1.1 Defesa

Todos os trabalhos práticos estão sujeitos a defesa por parte do grupo que o elaborou. A defesa decorrerá nas aulas práticas seguintes à data de entrega. A não comparência de um aluno à defesa implica a não consideração do trabalho para a nota do aluno em questão.

Uma defesa considerada como não satisfatória por parte do docente da disciplina implica a não consideração do trabalho para a nota do aluno em questão.

1.2 Outras considerações

Quando não seja respeitado o formato de entrega (tipos de ficheiros e nomes), os alunos que compõem o grupo sofrerão uma penalização de 10% na nota final do trabalho.

2 Datas

A data limite para **definição do grupo é 29 de Maio de 2015, pelas 24h00**. A indicação da composição do grupo será efetuada por email para **apinto@estgf.ipp.pt** (até um **máximo de 2 elementos**).

A data limite para a **entrega é 11 de Junho de 2015, pelas 23h55**. Os trabalhos entregues fora de prazo não serão considerados. A entrega deverá ser efetuada por envio pelo *moodle*. Deverá ser entregue o código fonte e o relatório num ficheiro ZIP com o nome: ifc_grupoX.zip (onde X deverá ser substituído pelo numero do grupo).

3 Análise de capturas de rede

O trabalho consiste na elaboração de um *script* ou programa que analise uma captura de rede, sob a forma de um ficheiro pcap, e que gere informação estatística sobre o mesmo. A linguagem a utilizar no desenvolvimento do *script* é da responsabilidade do grupo. Sugere-se *bash scripting* ou PERL. Caso o grupo opte pela elaboração de um programa, i.e. passível de compilação, a linguagem a utilizar poderá ser C, C++ ou Java. O *script*/programa deverá ainda contemplar as seguintes funcionalidades:

- Verificação da existência ou não de eventuais componentes (ou outros programas) que necessite.
- Nome do ficheiro pcap deve ser passado como argumento da linha de comandos.
- Geração dos resultados quer para o ecrã, quer para ficheiro (texto, HTML).
- Calcular diferentes resumos (ex.: SHA256, SHA512, ...) dos ficheiros de captura e de resultados.

A informação de resultado esperada do executar do *script*/programa sobre uma captura deverá ser tão extensa quanto possível. Nomeadamente, deverá ser possível obter-se a seguinte informação estatística:

1. Listagem de ligações (fluxos) existentes.
2. Listagem de equipamentos existentes, bem como o número total de equipamentos.
3. Listagem de protocolos de rede presentes na captura.
4. Identificação dos equipamentos , protocolos, e portos mais usados.
5. Ficheiros presentes na captura e passiveis de extração (*carving*)
6. Outras informações estatísticas consideradas relevantes pelo grupo.

3.1 Funcionalidades avançada

Funcionalidades como a visualização gráfica da informação (eg.: gráficos, grafos de interatividade) ou o estabelecimento de *timelines* são facilitadoras da análise de elevados volumes de dados de que são exemplo as capturas de rede. Tais funcionalidade são particularmente interessantes se permitirem a sua análise interativa.

3.2 Outras considerações

Serão valorizados trabalhos que sejam desenvolvidos maioritariamente pelos elementos do grupo. A criatividade será também fortemente valorizada.

O único formato aceite para o **relatório é o formato ODT!** Recomenda-se a utilização do LibreOffice 4 para a elaboração do relatório.