Aula TP - 23/Abr/2018

Cada grupo deve colocar a resposta às perguntas dos seguintes exercícios na área do seu grupo no Github até ao final do dia 23/Abr/2018. Por cada dia de atraso será descontado 0,15 valores à nota desse trabalho.

Note que estes exercícios devem ser feitos na máquina virtual disponibilizada. Caso já tenha a versão da máquina virtual utilizada nas últimas aulas, não precisa de fazer download da nova versão.

Instruções de *update* da máquina virtual, para quem já tem a máquina virtual utilizada nas últimas aulas:

1. Para este ponto necessita de instalar o **gdb** e o **GDB-Peda** na conta do utilizador *user* na máquina virtual. Sugere-se que efetue a seguinte sequência de comandos:

```
sudo apt-get install gdb

cd ~/

git clone https://github.com/longld/peda.git ~/bin/peda

echo 'source ~/bin/peda/peda.py' | sudo tee --append ~/.gdbinit > /dev/null
```

2. Adicionalmente, grave os ficheiros na diretoria Aula 10 para a sua máquina local na diretoria /home/user/Aulas/Aula10 .

Exercícios

1. *Buffer Overflow*

Experiência 1.1 - Organização da memória do programa

Utilize o comando Unix `size` para ver o tamanho, em bytes, do segmento de texto, dados e bss dos programas size1.c, size2.c, size3.c, size4.c e size5.c, seguindo os seguintes passos:

1. Compile os vários ficheiros. Ex.: `gcc -o size1 size1.c`
2. Efetue o comando `size` para cada um dos ficheiros executáveis. Ex.: `size size1`
3. Verifique e explique as diferenças de valores nos vários segmentos de texto, dados e bss.

Experiência 1.2 - Organização da memória do programa

Utilize o programa memoryLayout.c para verificar o layout da memória do programa. Verifique se os resultados são os expectáveis (de notar que as optimizações do compilador e a arquitectura da máquina podem levar a resultados ligeiramente diferentes).

Nota: Terá que compilar e executar o programa.

Experiência 1.3 - Buffer overflow em várias linguagens

Verifique o que ocorre no mesmo programa escrito em Java (LOverflow.java), Python (LOverflow.py) e C++

(LOverflow.cpp), executando-os.

Explique o comportamento dos programas.

Pergunta P1.1 - Buffer overflow em várias linguagens

Verifique o que ocorre no mesmo programa escrito em Java (LOverflow2.java), Python (LOverflow2.py) e C++ (LOverflow2.cpp), executando-os.

Explique o comportamento dos programas.

Pergunta P1.2 - Buffer overflow em várias linguagens

Verifique o que ocorre no mesmo programa escrito em Java (LOverflow3.java), Python (LOverflow3.py) e C++ (LOverflow3.cpp), executando-os.

Explique o comportamento dos programas.

Experiência 1.4 - Buffer overflow em várias linguagens

Verifique o que ocorre no mesmo programa escrito em Java (ReadTemps.java) e Python (ReadTemps.py), executando-os.

- Teste com temps.txt com os valores: 30.0 30.1 30.2 30.3 30.4 30.5 30.6 20.7 30.8 30.9
- Teste com temps.txt com os valores: 30.0 30.1 30.2 30.3 30.4 30.5 30.6 20.7 30.8 30.9 31.0 31.2
- Altere os programas para resolver o problemas SEM alterar o tamanho do array.

Pergunta P1.3 - Buffer overflow

Analise e teste os programs escritos em C RootExploit.c e 0-simple.c .

- Indique qual a vulnerabilidade de *Buffer Overflow* existente e o que tem de fazer (e porquê) para a explorar e (i) obter a confirmação de que lhe foram atribuídas permissões de root/admin, sem utilizar a *password* correta, (ii) obter a mensagem "YOU WIN!!!".

Experiência 1.5 - Formatted I/O

A formatação do I/O, em C, pode fazer toda a diferença.

Analise e teste o programa IOformatado.c e veja qual a diferença entre a função segura() e vulneravel().

Nota: Relembre-se que em C existem diretivas de formatação, tais como %d, %s, …

Pergunta P1.4 - Read overflow

Analise e teste o program escrito em C ReadOverflow.c .

- O que pode concluir?

Experiência 1.6 - Buffer overflow na Heap

O exemplo de *Buffer overflow* na *heap* visto na aula teórica, encontra-se nos ficheiros overflowHeap.1.c e

overflowHeap.2.c.

- Teste e altere o output da variável *readonly*.

Experiência 1.7 - Buffer overflow na Stack

As vulnerabilidades de buffer overflow ocorrem quando é possível escrever e/ou executar código em áreas de memória que normalmente não seria possível, e deriva usualmente da utilização de funções não seguras.

A maioria dos sistemas operativos e compiladores actuais já incorporam algumas características de segurança que previnem esse tipo de ataques, tais como:

- *canaries* (ou canários) - valores colocados na *stack* (pelo compilador) entre um buffer e dados de controlo, de modo a monitorizar *buffer overflows* durante a execução do programa. Se houver um *buffer overflow*, o primeiro dado a ser corrompido/alterado é o canário, e uma verificação falhada dos dados do canário são um alerta para a existência de um *overflow*;
- *Executable space protection* (XP) / *Data Execution Prevention* (DEP) - impede que alguns sectores de memória (por exemplo, a *stack*) possam ser executados (i.e., o programa não consegue executar código que estiver nesses sectores de memória);
- *Address Space Layout Randomisation* (ASLR) - técnica utilizada para impedir que seja executado código injetado no programa, através da colocação randomizada de módulos e estruturas de dados no espaço da memória.

Esta experiência e as próximas perguntas vão necessitar do ASLR desativado, pelo que execute o seguinte comando:

```
echo 0 | sudo tee /proc/sys/kernel/randomize_va_space
```

O exemplo de *Buffer overflow* na *stack* visto na aula teórica, encontra-se nos ficheiros overflowStack.1.c e overflowStack.2.c.

Vamos utilizar o Gnu debugger (GDB) para obtermos a informação necessária para explorar a vulnerabilidade, sem alterar o primeiro programa overflowStack.1.c.

Para isso execute os seguintes comandos:

- compilar overflowStack.1.c com informação de debug, a ser utilizada pelo GDB;

```
gcc overflowStack.1.c -g -o overflowStack.1
```

- iniciar o debug do programa com o gdb

```
gdb overflowStack.1
```

- no gdb, colocar *breakpoint* na função store()

```
b store
```

- no gdb, executar o programa até ao *breakpoint*

```
r
```

- no gdb, obtenha informação sobre a *frame* actual de execução do programa

```
info f
```

- na última linha é-lhe indicado em que endereço de memória está guardado o base pointer (%rbp) e o endereço de retorno (%rip). Como vamos querer reescrever o conteúdo do endereço de retorno, de modo a direcioná-lo para a função debug(), guarde o endereço de memória em que está guardado o %rip (emr).
- o próximo passo é obter o endereço de memória onde está guardada a função debug(). Para isso, no gdb efetue o comando

```
p debug
```

- aponte o endereço que lhe é apresentado, já que é esse endereço que quer reescrever no emr.
- de seguida, para ter a certeza quantos bytes tem de escrever no array buf para reescrever o %rip, veja em que endereço se inicia o array buf (eia)

```
p &buf
```

- O número de bytes a escrever até ao inicio do emr é de emr - eia. Utilize um calculador hexadecimal para obter o resultado (por exemplo, utilize http://www.calculator.net/hex-calculator.html)
- já tem todos os dados que necessita do gdb, pelo que pode sair do gdb com

```
quit
```

- Execute o programa overflowStack.1 com o parâmetro necessário para obter os dados escondidos na função debug().

Pergunta P1.5

Agora que já tem experiência em efetuar o *overflow* a um *buffer* (cf. pergunta P1.3), consegue fazer o mesmo se for necessário um valor exato?

Compile e execute o programa 1-match.c, e obtenha a mensagem de "Congratulations" no ecrã. Notas:

- já ouviu falar de *little-endian* e *big-endian*?

Indique os passos que efetuou para explorar esta vulnerabilidade.

Pergunta P1.6

Compile e execute o programa 2-functions.c, e obtenha a mensagem de "Congratulations" no ecrã. Notas:

- relembre que o nome de uma função em C equivale ao endereço onde esta é escrita em memória;
- poderá fp ser win?

Indique os passos que efetuou para explorar a vulnerabilidade.

Pergunta P1.7

Compile e execute o programa 3-return.c, e obtenha a mensagem de "Congratulations" no ecrã. Notas:

Indique os passos que efetuou para explorar a vulnerabilidade.

Nota final: Para voltar a ativar o ASLR que desativou na Experiência 1.7, execute o seguinte comando:

```
sudo /sbin/sysctl -w kernel.randomize_va_space=2
```

Projeto de desenvolvimento de software

Os alunos deverão utilizar o resto desta aula TP para continuarem o projeto de desenvolvimento de software.

O projeto 1 (Leilões online) será efetuado, em conjunto, pelos grupos 1, 6, 10, 11, 12.

O projeto 2 (Gestor de passwords com base em QrCodes) será efetuado, em conjunto, pelos grupos 2, 3, 4, 5, 7, 8, 9.

- Projeto 1 – Leilões online
  - Leilões online, com entrega de propostas em "carta fechada";
  - Pode ser uma extensão para software open source de leilões online.
- Projeto 2 – Gestor de passwords com base em QrCodes
  - Gestor de passwords, em que com base em QrCode apresentado pelo site, o telemóvel lê o QrCode e envia o user + password para desbloquear o acesso;
  - Pode ser uma extensão para software open source de gestão de passwords.

Nesta primeira fase, os dois grupos de projeto devem definir em traços gerais o projeto e as suas funcionalidades, e pensarem de que modo serão utilizado as técnicas criptográficas no projeto.

Como output desta fase, deverão ter um primeiro draft de:

- definição do projeto e suas funcionalidades,
- etapas e fluxos de comunicação / mensagens, podendo utilizar como exemplo o formato visto no segundo exemplo do voto eletrónico, na aula teórica. Esta componente deve conter um diagrama e uma parte textual de explicação do diagrama,
- identificar os passos efetuados para a concepção e desenvolvimento do projeto, de forma a seguir os princípios

de "*privacy by design*" e "*data minimization*" do RGPD (Regulamento Geral de Proteção de Dados);
- identificar de que modo o software garante os direitos do titular dos dados, de acordo com o RGPD.

Estes pontos deverão fazer parte do relatório final do projeto.

SAMM (*Software Assurance Maturity Model*)

Nesta fase do projeto é-lhe pedido para, utilizando o ciclo de melhoria contínua do SAMM,

1. Avaliar a maturidade das práticas de segurança utilizadas no desenvolvimento de software deste projeto (Fase *Assess*);
2. Estabelecer o objetivo para cada uma das 12 práticas de segurança (Fase *Set the Target*), i.e., o nível de maturidade pretendido;
3. Desenvolver o plano para atingir o nível de maturidade pretendido, em quatro fases (Fase *Define the Plan*).

Para isso deverá utilizar a Toolbox (ficheiro excel) fornecida na diretoria Aula9, onde também encontrará mais informação relativa ao SAMM.

Note que:

- Para a Fase *Assess* deverá preencher a *sheet* "*Interview*";
- Para a Fase *Set the Target*, o grupo deverá discutir qual o *score* objetivo para cada uma das 12 práticas de segurança, que sirva de guia para atuar sobre as atividades mais importantes. Pode partir do princípio que a sua organização é uma startup que vai efectuar desenvolvimento de software na área de i) sistemas web seguros online (caso do projeto 1) e ii) sistemas de identificação eletrónica (caso do projeto 2). Se necessitar de outros pressupostos, indique-os na justificação à decisão tomada;
- Para a Fase *Define the Plan* deverá preencher a *sheet* "*Roadmap*", supondo que cada uma das fases tem 3 meses de duração. Tenha em conta o esforço necessário e a eventual dependência entre atividades em cada uma das fases.

A Toolbox (ficheiro excel) deverá fazer parte do relatório final do projeto, fornecendo o ficheiro excel como anexo ao relatório. Adicionalmente, no documento do relatório deverá incorporar um anexo em que indique a decisão da Fase *Set the Target* e a justifique.

Note que não há respostas certas nem erradas.