Cibersegurança - Segurança em Software (Módulo 2)

Trabalho Prático - Parte 1

Esta tarefa consiste em explorar a vulnerabilidade shellshock num ambiente controlado. Entrega: ● Documento com evidências e explicações solicitadas em cada questão.

Em 2014 foi identificada uma vulnerabilidade na aplicação *bash* usada para executar comandos nos terminais de sistemas baseados em Linux, a qual ficou conhecida como *ShellShock*. Uma forma de explorar esta vulnerabilidade era o atacante executar remotamente comandos ou programas na máquina vulnerável, através de pedidos HTTP ao servidor vulnerável. As instruções a seguir são baseadas no laboratório *Shellshock* publicado pelo projeto SEED Labs (https://seedsecuritylabs.org/Labs_20.04/Files/Shellshock/Shellshock.pdf).

Apresente um relatório sobre os seguintes pontos:

1. Configure o laboratório executando um contentor Docker[1,2] na sua máquina com a imagem pública disponível no DockerHub: `jsimao/cs-shellshock-amd64` ou `jsimao/cs-shellshock-arm64` em função do seu sistema operativo e arquitetura:

    a) Execute o sistema vulnerável que inclui um servidor Apache à escuta na porta 80 e dois *scripts* que usam a versão vulnerável do *shell* bash. No seu computador o sistema estará disponível na porta 8080.

    Na linha de comandos do sistema operativo:
    `$ docker run -it -p 8080:80 --name shellshock jsimao/cs-shellshock-amd64`

    b) Certifique-se de que o sistema está operacional, chamando os dois programas disponíveis na configuração do Servidor Apache (`/cgi-bin/getenv.cgi` e `/cgi-bin/vul.cgi`). Use um *browser*, ou as ferramentas *curl* ou *Postman* para interagir com os programas referidos. Apresente as evidências que o sistema descrito está operacional.

[1] https://www.docker.com/products/docker-desktop/
[2] https://dockerlabs.collabnix.com/docker/cheatsheet/

2. O objetivo é executar comandos no sistema vulnerável, fazendo pedidos HTTP à aplicação em `/cgi-bin/vul.cgi`.

   O programa `/cgi-bin/vul.cgi` contém:

```
#!/bin/bash_shellshock

echo "Content-type: text/plain"
echo
echo "Hello World"
```

   O ataque não depende do que está no programa CGI, pois tem como alvo a execução do programa bash vulnerável, que é invocado antes das instruções do script de CGI serem executadas. No entanto, se a vulnerabilidade for explorada com sucesso, continua a ser necessário que a resposta ao pedido HTTP siga o protocolo, como é o caso do exemplo acima onde é indicado o *content-type*, uma linha vazia e o corpo (texto) da resposta.

   a) Obtenha o conteúdo do ficheiro /etc/passwd[3] do servidor.

   b) Crie um arquivo dentro da pasta `/tmp` do servidor. Demonstre que o arquivo foi criado entrando no contentor para ver se o arquivo existe, ou use outro ataque Shellshock para listar o arquivo criado.

   c) É possível obter o conteúdo do ficheiro `/etc/shadow` do servidor? Justifique a sua resposta.

   d) Os pedidos HTTP GET podem enviar dados no URL após a marca '?', numa zona designada *query string*. Demonstre que a *query string* aparece também numa variável de ambiente. Podemos usar este método para lançar o ataque Shellshock?

[3] https://en.wikipedia.org/wiki/Passwd