-GUIDE-

Olá, boa tarde.

Venho apresentar o meu trabalho de estágio. O projecto que até agora nem nome tinha, mas como tudo necessita de um nome chamei-lhe Security Hawk. Porque o Falcão-Americano é uma das Aves com melhor visão que o permite localizar potenciais alvos com extrema precisão e é isso que pretendemos no nosso projecto.

-

Esta apresentação vai decorrer da seguinte forma:

Vou fazer uma introdução do projecto. Especificar os objectivos, o que atingimos e o que não. A arquitectura e como é constituído. Os scripts, tanto os que funcionaram e estão implementados como os que não. A base de dados em MySQL. Os resultados obtidos. E o trabalho que deixamos para depois. E a Conclusão.

-

Este projecto faz uma analise ao espectro wifi de 2.5GHz e faz uma leitura e recolha dos dispositivos e dos APs guardando num ficheiro netxml que é exportado para uma base de dados MySQL.

O projecto iniciou-se com a inicativa da criação de uma ferramenta de wIDS e eu inicialmente optei por um abeirumento de uso do Python para a criação da mesma. No entanto algumas dificuldades foram surgindo, logo decidi optar por usar scripts em bash com calls ao Aircrack-ng e MySQL-Client.

É desta forma e com estes chamados que conseguimos fazer a captura e armazenar a informação obtida.

-

Com o objectivo e eu aprender e entender mais sobre o wifi que este projecto foi-me proposto. A criação de uma ferramenta que analise o espectro wifi capture e recolha informação e armazene o output obtido numa base de dados MySQL local e/ou externa. Como já tinha referido.

-

A funciona da seguinte forma: Existe um Script Bash que é iniciado juntamente com o sistema linux, esse script coloca a placa de wireless em modo monitor e começa a fazer analises, no intervalo de cada analise ele muda o nome do output da analise, transfere-o para a base de dados e elimina-o recorrendo ao chamado de um outro segundo script bash.

O output de cada analise vem em formato ‘ \*.kismet.netxml ’ logo podemos enviar a informação diretamente para a base de dados, apenas tivemos de criar as tabelas.

-

Aqui encaixamos os scripts feitos por mim. Tentativas falhadas e os dois scripts que estão a ser usados. Mas devo dizer que infelizmente perdi os scripts em python, embora possa dizer-vos de que consistiam.

Abordagem Python

>reorganizecsv.py

Este script organiza o csv-output do aircrack. Vai de linha e de virgula a virgula de modo a orientar um ficheiro de texto com essa mesma informação mas disposta de forma vertical sendo mais facil para leitura humana. Este script foi criado com bases de um outro projecto parecido que encontrei na Internet.

>csvtosql.py

Este script por sua vez iria reorganizar o output do reorganizecsv.py para uma tabela SQLite mas por sua vez tinha montes de erros e nem sempre resultava. Foi logo descartado.

>processcsv.py

Este foi um script em python também mas feito por mim para me relembrar de python, poderia ter até um proposito util para o projecto pois de um csv ele separava as duas tabelas e da de cima (dispositivos e não os APs) mostrava todos os macs.

>spawnkilldump.py

Este foi a ideia principal por detrás dos bash, era o que iria fazer exactamente o mesmo que o collector.sh porem tornar-se ia mais lento pois tinha muitas libs e demoraria mais tempo a processar.

Abordagem Bash

>collector.sh

O que este script (em Bash) faz é basicamente tudo. É um script que foi inserido na crontab, inicia automaticamente com o kali, coloca a placa de wireless em modo monitor e faz uma análise primaria. De seguida entra num loop onde guarda e exporta a informação obtida para um ficheiro .netxml e volta a fazer análises.

>insert.sh

Este por sua vez é bastante curto mas importante na mesma. É chamado pelo collector.sh quando este cria o ficheiro .netxml. Ele que exporta o output da análise para uma base de dados em MySQL.

-

A base de dados do MySQL está dividida em 3 tabelas a ‘ssid’, a ‘wirelessclient’ e a ‘wirelessnetwork’. As duas ultimas contêm os registos dos Dispositivos e os APs respectivamente. A ‘ssid’ guarda os registos dos SSIDs.

-

Os resultados obtidos nem sempre foram os melhores, porem, os resultados obtidos no projecto final têm sido bons. A colecta de informação corre suavemente, o airodump-ng funciona, e o armazenamento digamos.. armazena.

Apenas posso afirmar que não houve tempo para fazer uma dashboard.

-

E isso é o que nos leva a crer que é um trabalho que pode ser feito posteriormente para enriquecer esta ferramenta para que um dia possa talvez ser comercializada.

-

Concluindo. Este projecto é quase um “backbone” de um wIDS, ele verifica o espectro wifi e faz uma análise dos dispositivos e dos APs e regista num ficheiro que é exportado para uma base de dados local e/ou externa. Ele é constituído por 2 scripts em bash feitos por mim e usam programas que existem no kali linux, dos quais o MySQL (Server e Client) e o Aircrack-ng.

-

Obrigado pela vossa atenção. Caso queiram perguntar alguma coisa não hesitem.