Http Dissector utilizando Python

Guilherme S. Mazzariol
Campinas/SP - Brazil
g138466@g.unicamp.br

Marcelo Machado
Campinas/SP - Brazil
m210402@g.unicamp.br

I. Introdução

Este trabalho tem como objetivo criar um *HTTP Dissector* utilizando a linguagem de programação python. Foi utilizado o python versão 3.4.3, pyshark versão 0.3.7.11, scapy-python3 versão 0.22.

II. Experimento realizado

O programa desenvolvido, recebe como entrada um arquivo de leitura de tráfego de rede (*.pcap), que verifica quais são os pacotes do tipo HTTP existentes. Para cada pacote HTTP encontrado, é verificado a qual stream ele pertence e então eles são separados por streams. Para cada stream HTTP, cada pacote é verificado e apenas o pacote de dados é extraído. Não conseguimos extrair o dado do hexadecimal, entretanto salvamos os binários em arquivos distintos para futura análise.

III. Tipos de Ataques

Utilizando um *HTTP Dissector* é possível monitorar todo o tráfego HTTP de uma rede e extrair os dados que estão sendo transmitidos. Essa análise permite ao atacante realizar vários tipos de ataque, entre eles, podemos citar:

- Roubo de qualquer informação trafegada na rede
- Injeção de código malicioso nas requisições HTTP
- DNS poison caching
- Hijack session
- Ping of Death
- Deny of Service

Essa variedade de ataques só é possível porque com o *HTTP Dissector* o atacante pode descobrir qualquer requisição que está sendo feita pela vítima, qual site ela está acessando e qual dado ela está trafegando.

Referências

[1] Python lib scapy, http://www.secdev.org/projects/scapy/
[2] Python lib pyshark, https://pypi.python.org/pypi/pyshark
[3] Pyshark doc, https://thepacketgeek.com/intro-to-pyshark-for-programmatic-packet-analysis/