Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:
http://vmzsolutions.com.br

Localizando arquivos com o Panoptic

Nessa aula, vamos trabalhar com o File Inclusion com o uso da ferramenta do Panoptic.

https://github.com/lightos/Panoptic

O **File Inclusion**, faz a inclusão de um código através de um novo arquivo ou de um arquivo já existente. Podemos também dizer que é uma inclusão **NO** arquivo. Uma prática comum é usar os servidores FTP de modo anônimo e fazer um *upload* de um script em PHP de modo remoto em uma pasta e a partir daí podemos tentar rodar um meterpreter nesse servidor.

Já o **Local File Inclusion**, é quando atravessa de diretório saindo servidor Web e acessando outros arquivos do Sistema. Logo no DVWA é justamente isso que acontece. Vamos abrir ele e entrar no campo File Inclusion e fazer uns pequenos testes antes. Ao ver a sua URL, vamos alterar de:

page=include.php

para:

/etc/passwd

Localizando arquivos com o Panoptic

Verá que conseguimos ver algumas informações. Mas para agente agilizar esse processo, temos o auxilio da ferramenta do Panoptic para ele achar todos os arquivos disponíveis. Ao entrar no DVWA e entrar nessa seção do File Inclusion, vamos pegar o PHPSESSID dessa seção pelo BurpSuite e depois vamos baixar o programa do Panoptic.

Localizando arquivos com o Panoptic

```
# git clone https://github.com/lightos/Panoptic.git

# python panoptic.py --cookie="security=low;

PHPSESSID=ss5j4kprma6ntprkvdvf75ine7" -u

http://192.168.1.163/dvwa/vulnerabilities/fi/?page=include.php
```

Localizando arquivos com o Panoptic

Se você não encontrou o arquivo '/var/log/apache2/access.log' Vá em sua máquina da OWASP e deixe ele em modo de leitura para agente pode dar continuaidade de nossas aulas, pois é nele que vamos trabalhar. Dê o comando:

```
# chmod 777 -R /var/log/apache2/
```