Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Atacando com Beef

BeEF é abreviação de The Browser Exploitation Framework. É uma ferramenta de teste de penetração que se concentra nos navegadores web.

Atacando com Beef

O BeEF permite que o profissional na área avalie a postura real de segurança de um ambiente-alvo usando vetores de ataque do lado do cliente. Ao contrário de outros *frameworks* de segurança, o BeEF olha além do perímetro de rede e do sistema cliente, e ele examina a exploração dentro do contexto de uma porta obrigatoriamente aberta: o navegador da web.

Atacando com Beef

O BeEF vai atacar um ou mais navegadores da web e usá-los como porta de entrada para o lançamento de módulos de comando direcionado e assim permitir mais ataques contra o sistema a partir do navegador.

Atacando com Beef

Inicie o serviço BeEF em um terminal e digite o seguinte

comando:

```
# cd /usr/share/beef-xss/

# ./beef
```

Atacando com Beef

Usaremos a página de demonstração avançada do BeEF para ligar o nosso cliente. Na VM cliente do Windows, abra o Firefox e navegue pelo link

http://192.168.1.128:3000/demos/butcher/index.html

Agora, faça login no painel do BeEF (

http://192.168.1.128:3000/ui/panel). Nós devemos ver o novo

navegador capturado lá.

Atacando com Beef

Uma vez que o cliente está ligado ao Beef, é possível enviar ordens de comandos (através do hook.js) para o navegador de nossa vítima. Podemos fazer diversas coisas com ele, como enviar sites falsos, capturar senhas e logins, enviar programas para serem baixados, etc.