

Ivo Machado

Especialista em Segurança da Informação, Gestão de Riscos e Planos de Continuidade de Negócios, tendo já trabalhado no Brasil e exterior. Hoje atua como diretor de serviços da e-Horus Security & Audit. ivo.machado@e-horus.com.br

Segurança

Metagoofil - Google Hacking automatizado

Metagoofil é uma ferramenta para enumeração, desenhada para extrair informações a partir do header de metadata de documentos públicos (.pdf, .doc, .xls, .ppt, .odp, .ods) disponíveis no site da rede-alvo.

Após varrer o Google à procura dos documentos especificados na command line, ele irá gerar um HTML de saída com os resultados do metadata extraído, listando **potenciais usernames** que serão muito úteis para preparar um Brute-Force attack em serviços disponibilizados, como, por exemplo, POP3, FTP, web applications, VPN etc. Além disso, ele irá extrair também uma lista de **PATHs** que foram armazenados no metadata. Com essa informação, é possível acessar o FingerPrint do sistema operacional alvo, nomes de redes, Shared Resources etc.

Esta nova versão do Metagoofil extrai também o MAC Address de documentos Microsoft Office. Agora você pode ter uma ideia do tipo de hardware que o sistema operacional alvo está utilizando.

Todas essas informações não deveriam estar disponíveis na internet, porém a grande maioria das empresas não tem políticas para Information Leaking (Vazamento de Informações). Isso sem falar que, dessa grande maioria, 90% nem sabem que este tipo de informação realmente existe. Com isto, você pode mostrar a elas quanta informação um atacante pode obter com uma técnica muito simples.

Como funciona?

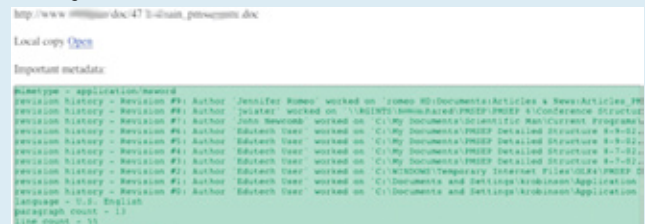
1 - Em primeiro lugar, o Metagoofil irá procurar no Google por documentos públicos sobre determinada empresa. Exemplo: arquivos .PDF (abaixo segue a query para Google Hacking).



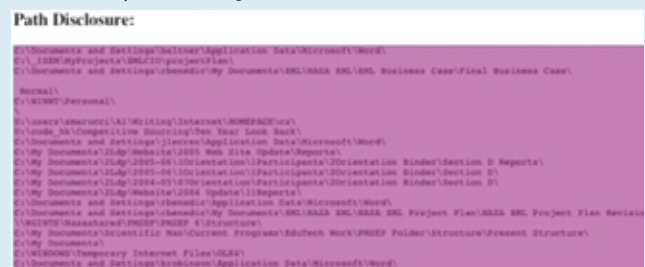
2 - Ele faz download de todos os documentos encontrados e extrai os metadata de todos eles, aplicando um filtro para capturar somente as informações realmente interessantes.



3 - Exemplo de resultados extraídos por uma sessão de Metagoofil:



4 - Exemplo de lista de paths disponíveis, extraídos do metadata pelo Metagoofil:



Portanto, tenha cuidado com os documentos que você posta na internet. Eles podem revelar muitas informações que podem ser utilizadas por atacantes e facilitar a vida deles, fornecendo usuários de sua rede e informações sobre os hosts que podem ser vítimas de ataque. É possível, ainda, durante o início de um ataque, colher dados que podem ser utilizados para engenharia social.