****

**Visão**

Com a crescente demanda sobre Tecnologias, percebemos que muitas pessoas apesar de buscarem informações, não possuem fontes que queiram realmente passar o conhecimento da maneira como ela deve ser, livre e com embasamento técnico que permita ser aplicado e utilizado quando necessário, além de serem testados em sua criação, tornando esta informação útil e confiável.

**Missão**

O Laboratório foi criado com a intenção de buscar e disseminar o conhecimento de uma maneira clara e objetiva, de forma gratuita, auxiliando na evolução dos membros e da sociedade na qual estas informações são compartilhadas, buscando o crescimento de todos os envolvidos nesta criação de valores.



Caso você pense que com a leitura dos materiais da How2Security, você irá se tornar um Cracker capaz de invadir sistemas, se você espera encontrar aqui scripts infalíveis para invasão e, a partir deles, sair por aí invadindo computadores, essa não é a leitura indicada. Indicamos, sim a leitura do Código Penal (Lei 2.848/1940), principalmente a Lei Carolina Dickmann (Lei 12.737/2012), nos Artigos 154-A e 154-B.

*154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:*

*Pena – Detenção, de 3 meses a 1 ano, e multa*

Este material é um conjunto de informações compiladas de documentos e ferramentas do Mundo Underground testadas em ambiente de laboratório na nossa intranet. Desta forma, todo conhecimento aqui condensado é tangível, assim como as orientações das contramedidas.

Dessa forma, esperamos ter sido bem claros que, em momento algum, estamos com a pretensão de ensinar a você como se tornar um invasor. Estaremos sim, mostrando muitas das técnicas utilizadas pelos crackers e, em alguns casos, pelos scripts kiddies, para que você, como administrador de redes, seja capaz de identificá-las em tempo hábil para se defender, antes que alguém com desejos menos nobres ô faça por você.

Assim sendo, todo o conteúdo dessa literatura tem apenas o objetivo didático de informar e preparar os administradores de redes dos novos tempos. Em momento algum nos responsabilizamos pelo mau uso desse conhecimento ou por danos causados em seu equipamento ou de terceiros, assim como também não somos responsáveis pelos códigos e ferramentas aqui citados.

Sandro Melo

Adaptado por Wellington Silva aka Well

**0 – Recon Passive - FOCA**

Todas as vezes que criamos documentos, também criamos Metadados? E você sabe o que são os Metadados?

Metadados são dados sobre dados. São informações descritivas sobre um conjunto de dados, objeto ou recurso, incluindo a forma como ele é formatado, quem e quando foi criado, etc.

Os Metadados podem ser uteis para nós, pois eles contêm informações sobre o sistema em que o arquivo foi criado, tais como:

* Nome de usuário logado no sistema;
* Software que criou o documento;
* Sistema Operacional que criou o documento.

O FOCA é uma ferramenta de auditoria que pode nos auxiliar a encontrar metadados em domínios. Ele faz buscas utilizando os principais mecanismos de busca para encontrar arquivos em domínios e baixa-los para que possam ser analisados.

**1 – Usando o FOCA**

Primeiramente devemos baixar a última versão no site https://www.elevenpaths.com/labstools/foca/ e depois descompactar.

Agora podemos criar um novo projeto clicando no menu **Project** 🡪 **New Project**. De um nome para o projeto (AltoroMutual), insira o site alvo (www.altoromutual.com), Selecione um diretório onde serão salvos os documentos encontrado no domínio indicado.

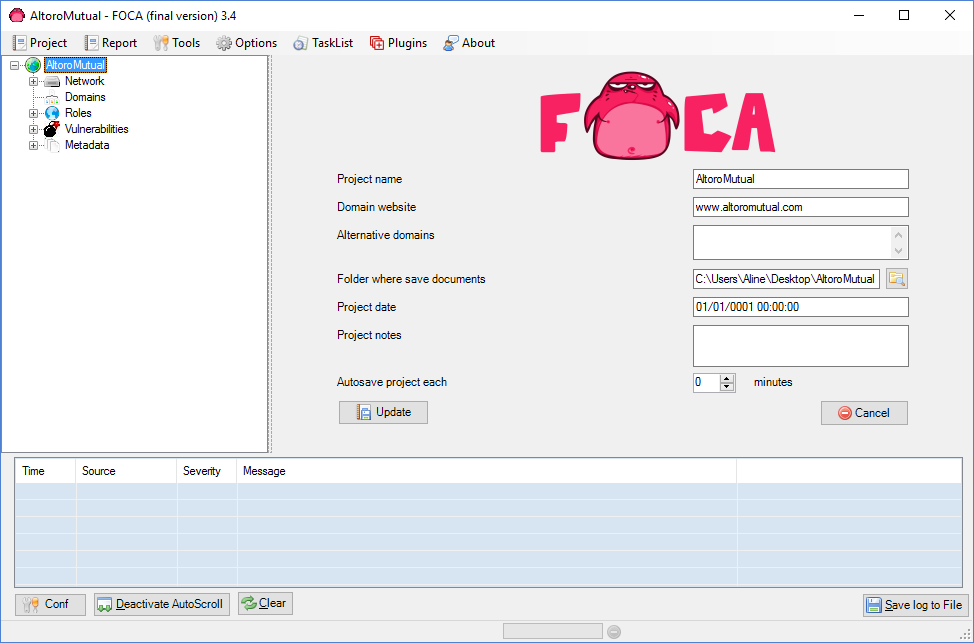


Figura 01 – FOCA Novo Projeto

Depois de preenchido os dados e selecionado onde decidimos armazenar o projeto, bastsa clicarmos no Botão **Create**, Em seguida vamos clicar no botão **Search All** para que o FOCA comece a varrer o domínio atrás de documentos pela Internet.

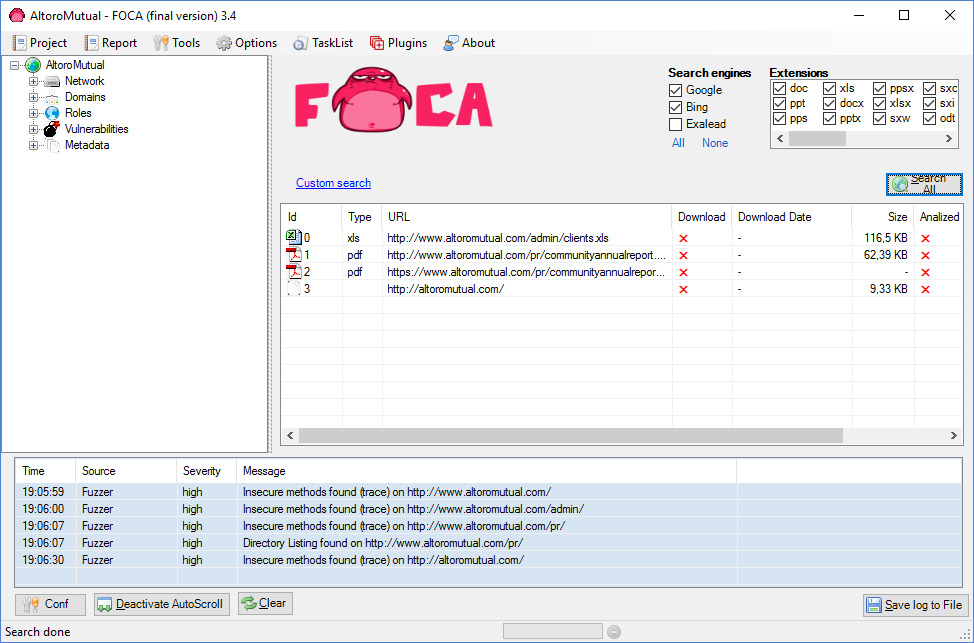


Figura 02 – Arquivos Encontrados

Agora podemos baixar todos os arquivos encontrado clicando com o botão direito do mouse em cima do arquivo e selecionando Download.

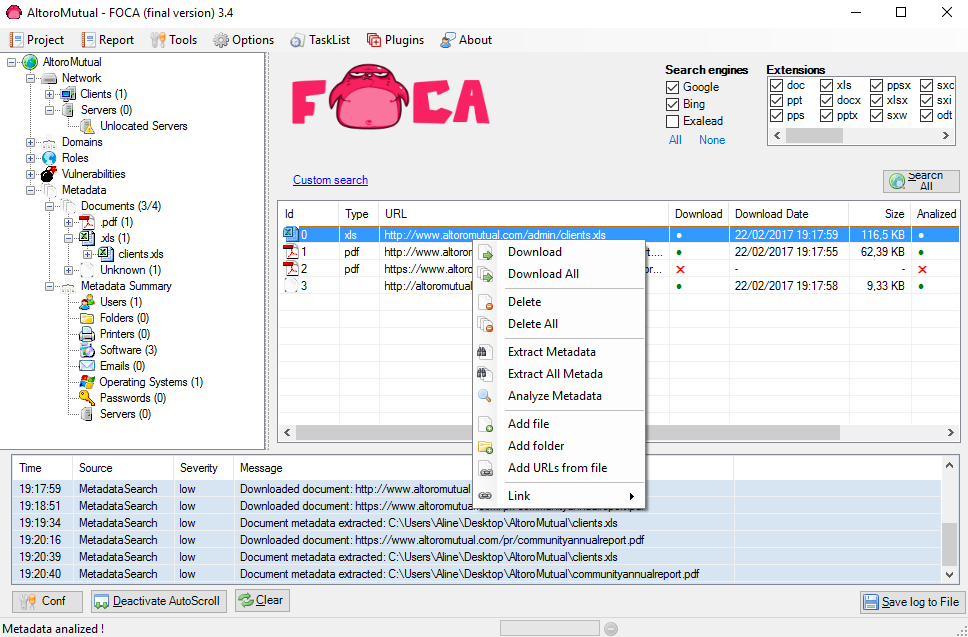


Figura 03 – Download dos Arquivos Encontrado

Vamos fazer o mesmo procedimento anterior, clique com o botão direito do mouse no arquivo e selecione **Extract Metadata**. Também vamos analisar esses metadatas direto no FOCA.

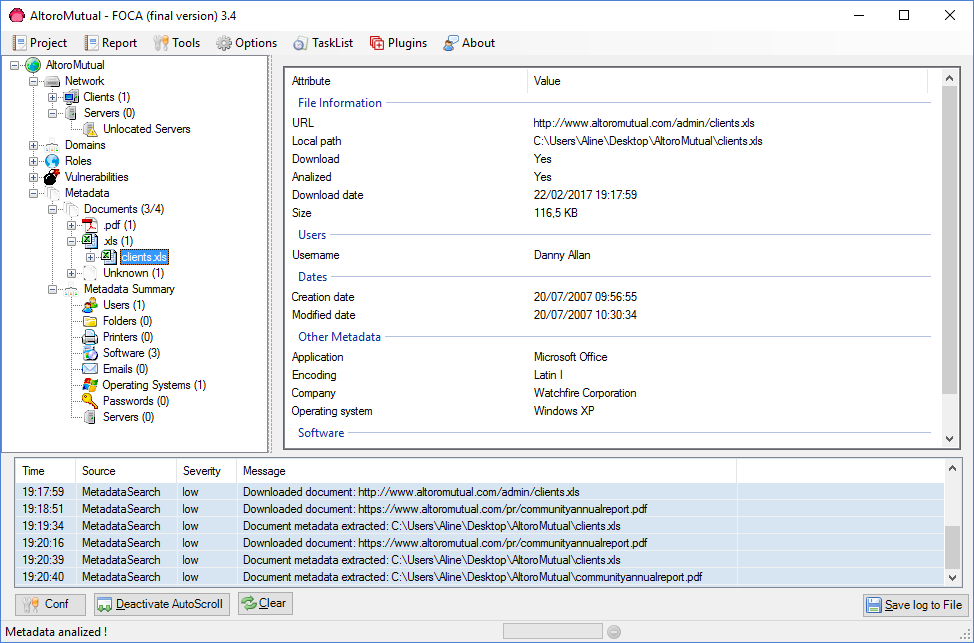


Figura 04 – Analisando os Metadados

Navegue pelos dados extraídos do metadados para ver os usuários, softwares utilizados para criar os documentos, sistema operacional utilizado, etc.

Navegue pelo domínio no FOCA para ver os dados extraído do domínio.

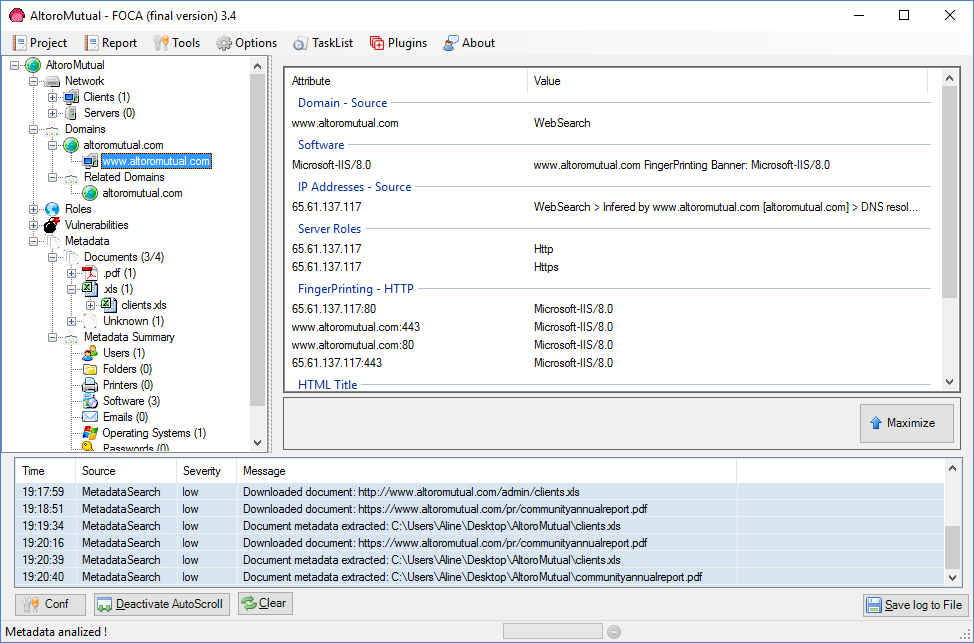


Figura 05 – Dados do Domínio

Em muitos casos, os atacantes serão capazes de ver muito mais informações e reunir dados de inteligência sobre um alvo.

**2 – Referências Bibliográficas**

**[1]** MUNIZ, JOSEPH and LAKHANI, AAMIR – Web Penetration Testing with Kali Linux, 2013, Birmingham – Mumbai, Packet Publishing

**[2]** GRAVES, KIMBERLY – CEH – Official Ethical Hacker Review Guide, Indianapolis - Indiana, 2007, Wiley Publishing Inc.

**[3]** STUTTARD, DAFYDD and PINTO, MARCUS – The Web Application Hacker’s Handbook, Indianapolis - Indiana, 2º Edition, Wiley Publishing Inc.

**[4]** SCAMBRAY, JOEL, McCLURE, STUART and KURTZ, GEORGE – Hackers Expostos Segredos e Soluções para a Segurança de Redes, São Paulo, 2001, MAKRON Books Ltda.

**[5]** LONG, JOHNNY - GOOGLE HACKING - Para Teste de Invasão [tradução Sérgio Pereira Couto] 2005, DIGERATI (BOOKS)

**[6]** MELO, Sandro – Estudo de Técnicas para Exploração de Vulnerabilidades em Redes TCP/IP, 2º Ed, Rio de Janeiro, 2006, Editora Alta Books Ltda.

**[7]** AHARONI, Mati; Offensive Security Lab Exercises - Curso de Pen-Test oferecido pela Offensive Security, 2007

**[8]** SCAMBRAY, Joel; LIU, Vicent; SIMA, Caleb - Hacking Exposed Web Application: Web Application Security Secrets And Solutions – 3ª Edition, New York – 2011, McGraw-Hill

**[9]** DHANJANI, Nitesh; RIOS, Billy; HARDIN, Brett - Hacking A Próxima Geração – Rio de Janeiro – 2011, Alta Books