****

**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 – Vasculhando o Passado**

O Web Archive é uma organização sem fins lucrativos que foi fundada para construir uma biblioteca da Internet. Seus objetivos incluem oferecer acesso permanente para pesquisadores, historiadores, estudiosos, pessoas portadoras de deficiências e ao público em geral para coleções históricas que existem em formato digital. Fundada em 1996 e localizada em San Francisco, o Web Archive tem recebido doações de dados da Alexa Internet e outros. No final de 1999, a organização começou a crescer para incluir uma coleção maior de informações sobre a Internet. Agora, o Web Archive inclui textos, áudio, imagens em movimento, e software, bem como páginas web arquivadas em suas coleções, e oferece serviços especializados para a leitura e adaptação de acesso à informação para os cegos e outros deficientes **[11]**.

Esse projeto pode nos ajudar a descobrir um pouco do passado da empresa. Descobrir o nome dos ex-funcionários e seus cargos, números de telefones, e-mails, organogramas desatualizados para uma possível Engenharia Social. Fazer uma análise estática do código-fonte a procura de comentários que não deveria estar lá e foi esquecido em uma versão anterior e já nem se preocupam pois não sabem que foi indexado e “cacheado” por empresas como o Google. Arquivos robots.txt antigos, vulnerabilidades corrigidas, entre outras coisas podem ser encontrados nesta análise.

**1 – Web Archive Para Conhecer o Seu Passado**

Para nosso exemplo irei levantar informações do site da Altoro Mutual, um banco fictício utilizado para testar ferramentas de pen-test da IBM.

Vamos acessar o site da Web Archive em http://www.archive.org.

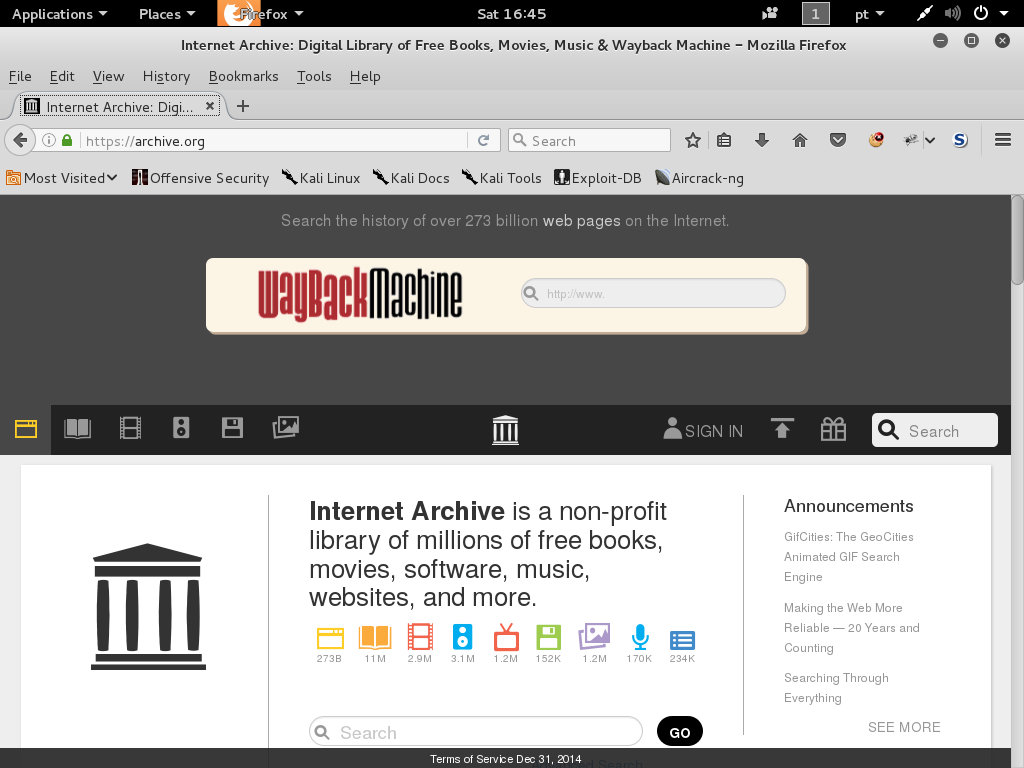


Figura 01 – Site da Web Archive

No campo **WebBack Machine** digite o domínio do site alvo e de **ENTER** (no nosso caso o site da Altoro Mutual)

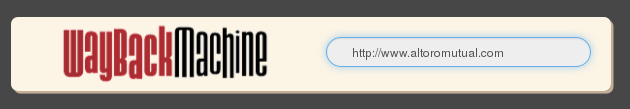


Figura 02 – Pesquisa Pregressa da Altoro Mutual

Em seguida clicamos no primeiro ano em que a página da Altoro Mutual foi indexada. Observe que essa informação está abaixo do campo onde colocamos o domínio a ser pesquisado (que em nosso caso é outubro de 2009). A história da Altoro Mutual pode ser vista aqui, como mostrado na figura abaixo:

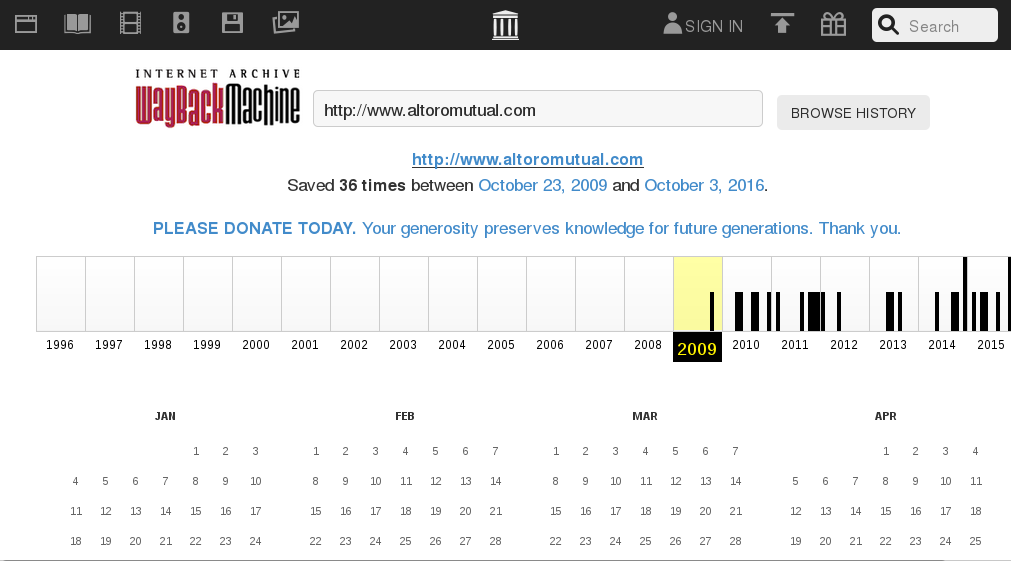


Figura 03 – Período Indexado da Altoro Mutual

Clique na data correspondente a primeira indexação.

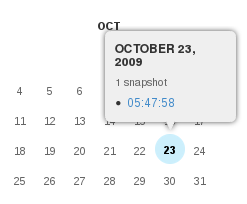


Figura 04 – Primeira Indexação

Na próxima figura podemos ver a página inicial da Altoro Mutual em 2009.

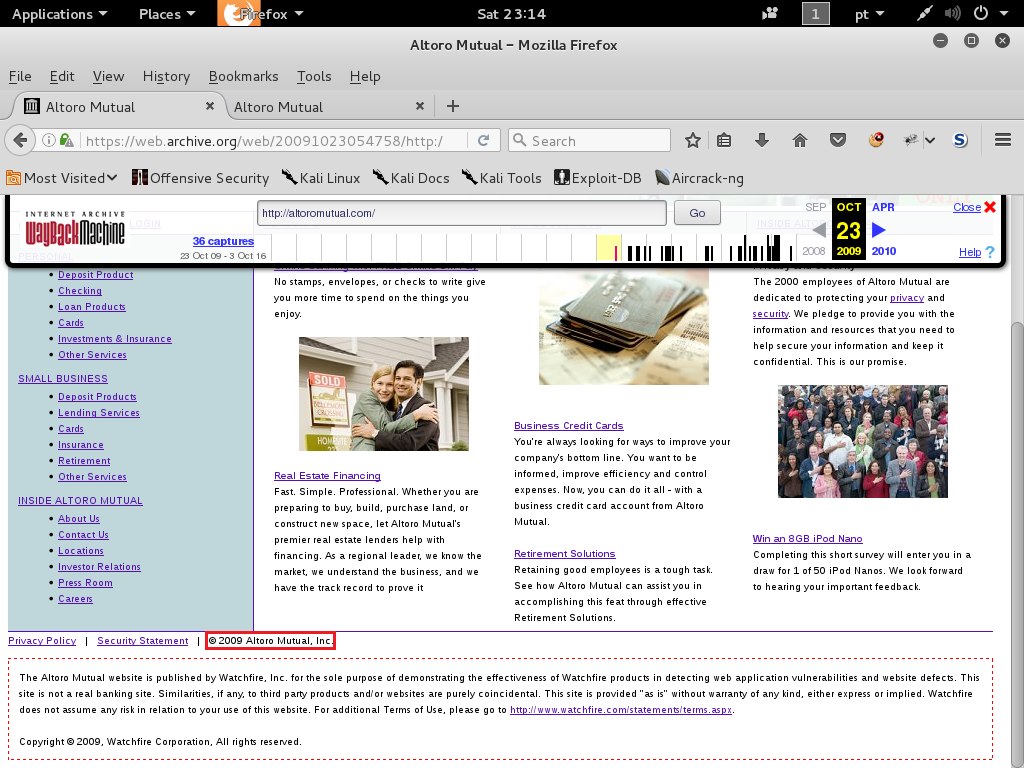


Figura 05 – Página Principal da Altoro Mutual em outubro de 2009

Agora vejamos a página principal da Altoro Mutual atualmente.

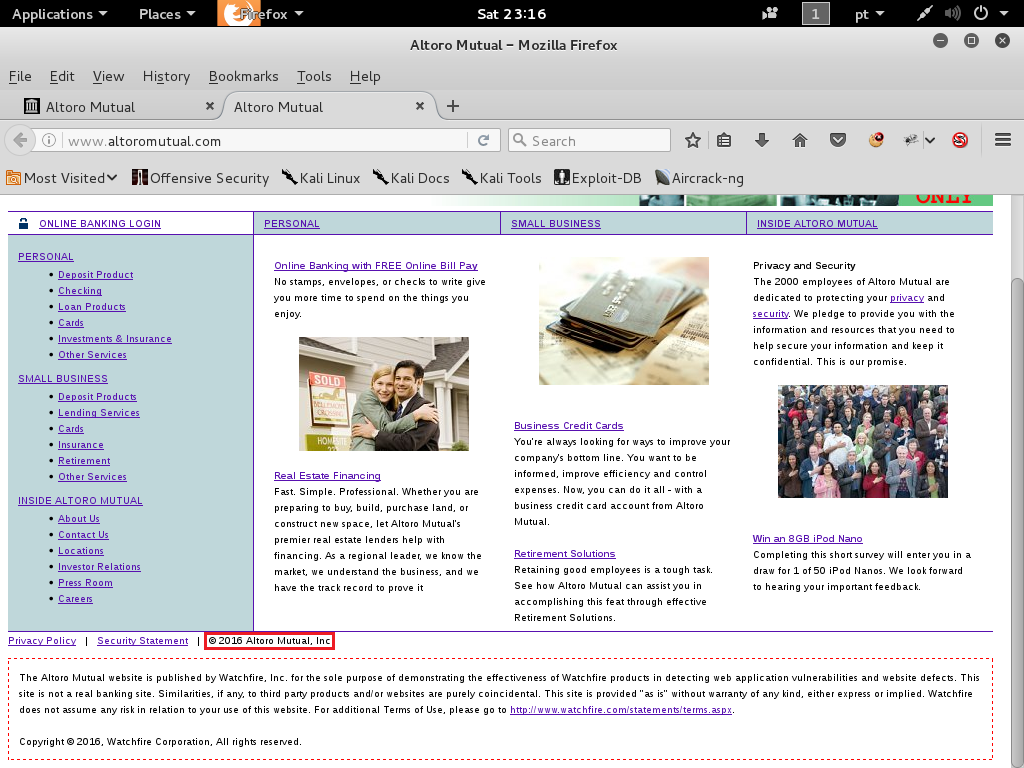


Figura 06 – Página Principal da Altoro Mutual Nos Dias de Hoje

Conseguimos navegar normalmente pelos links. Passe o mouse pelos links quebrados e observe na barra inferior para onde ele aponta. Dessa forma podemos clicar no link que aponta para o login.

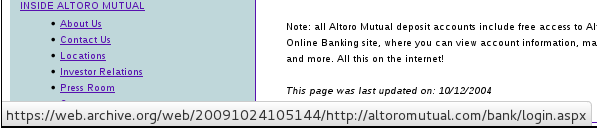


Figura 07 – Link Apontando para o Site Indexado

Como Ppen-tester, esta é uma ferramenta valiosa, pois não deixa rastros de reconhecimento nos sistemas alvo. Na verdade, você nem tocou nos sistemas do alvo toda informação manipulada aqui está arquivada no WebBack Machine.

Veja a importância da ferramenta, fomos observar o arquivo robots.txt na versão indexada e demos de cara com uma mensagem de erro padrão do IIS de 404 File Not Found.

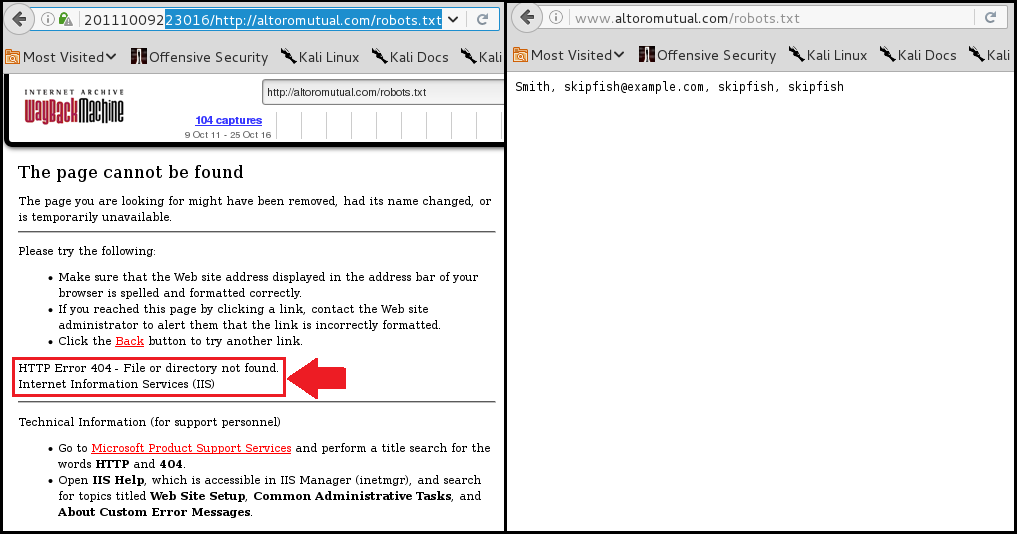


Figura 08 – Arquivo Robots.txt Nas Duas Versões do Site Alvo

**2 – Caches e a Indexação**

O cache dos mecanismos de buscas são algo maravilhoso. O fato é que ele registra uma página ou documento e você pode sempre contar em conseguir uma cópia, mesmo se a fonte original tiver secado e desaparecido. É claro que o lado ruim é que outros podem conseguir uma cópia de dados sensíveis mesmo que você desligue o plug que conecta o servidor. O cache pode registrar seu site inteiro, incluindo as áreas que você esqueceu, e isso pode ser recuperado sem nem mesmo enviar um único pacote para seu servidor. E se ele não recebeu nenhum pacote não tem muito a ser registrado em seu log, você pode não saber que seus dados sensíveis foram levados.

Entender como podemos realizar consultas anônimas a seus dados via cache é de suma importância.

Na figura abaixo podemos ver os principais sistemas de busca (Bing, Yahoo e Google) nos dando a opção de navegar na aplicação web da Altoro Mutual em cache.

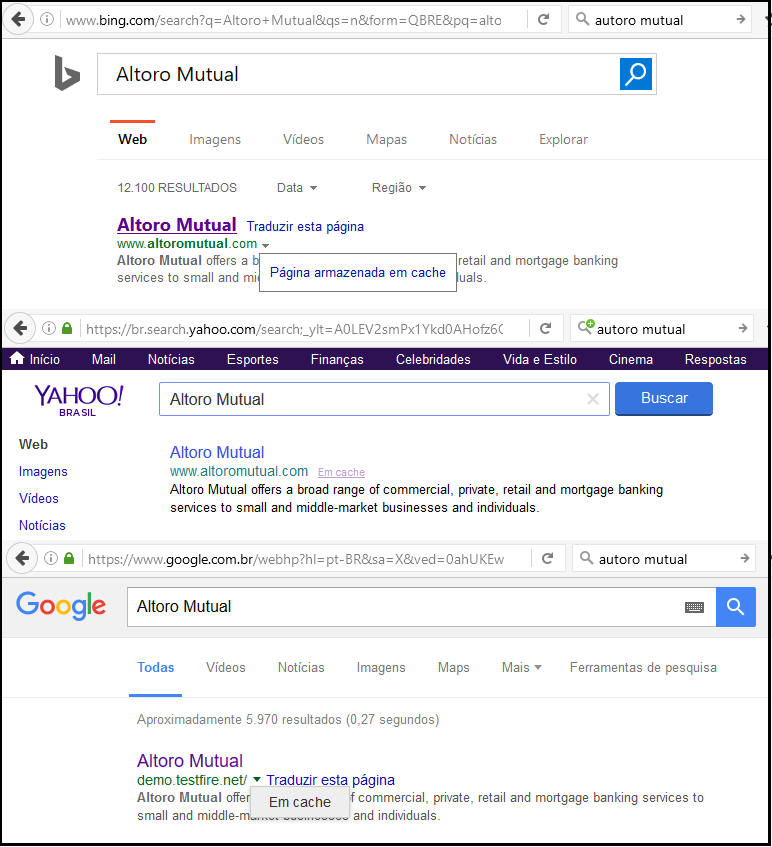


Figura 09 – Bing, Yahoo e Google Com a Opção de Acessar A Página em Cache

Agora podemos ver as páginas “cacheadas” e as mensagens exibidas pelos mecanismos de busca.

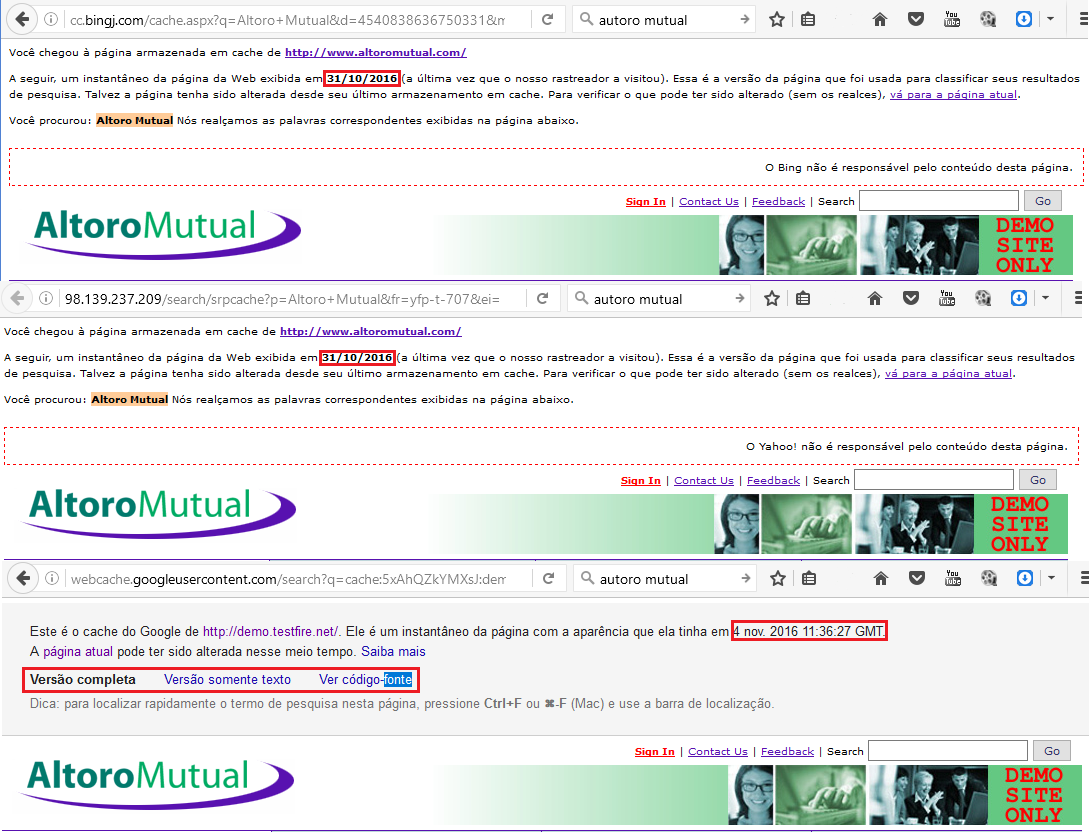


Figura 10 – Site da Altoro Mutual em Cache nos Mecanismos de Buscas

Observe que o Bing e o Yahoo utilizam o mesmo sistema de cache e tem uma cópia do dia 31/10/2016 e o Google que tem seu próprio sistema de cache e a cópia é do dia 04/11/2016. Com isso, podemos analisar pelo menos duas versões em cache atrás de informações relevantes e arquivos esquecidos nos servidores web.

Outra funcionalidade bastante interessante é que estamos sendo “proxiado” pelos sistemas de busca nesta navegação. Veja o endereço que aparece quando acesso ao site do http://meuip.com.br através de cache.



Figura 11 – IP de Acesso Via Cache

**3 – NetCraft Para Entender o Alvo**

Com o NetCraft podemos colher informações importante sobre as tecnologias utilizadas no passado e no presente do nosso alvo.

Para nosso exemplo irei levantar informações do site da Altoro Mutual, como anteriormente.

Vamos acessar o site da NetCraft em https://www.netcraft.com.

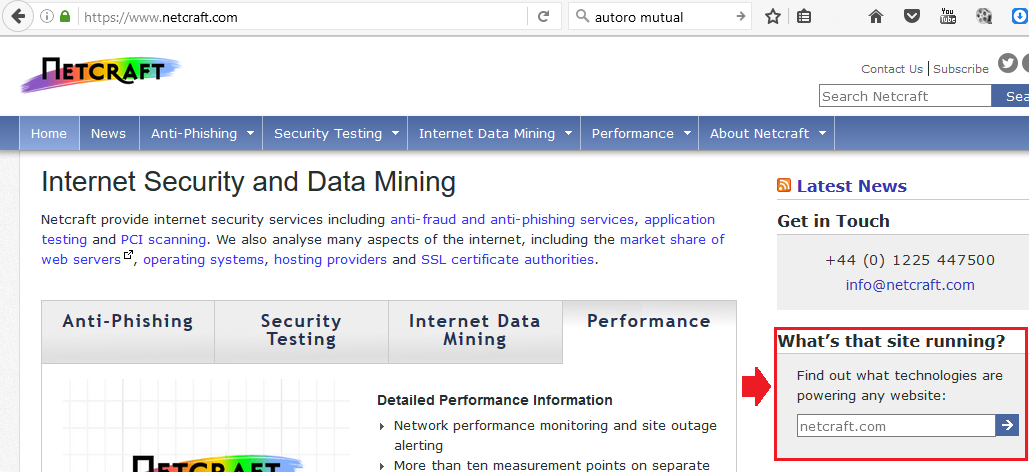


Figura 12 – Site da NetCraft

No campo **What’s that site running?** digite o domínio do site alvo e de **ENTER** (no nosso caso o site da Altoro Mutual)



Figura 13 – Pesquisa no Site da Altoro Mutual

Em seguida nos é fornecido diversas informações sobre o alvo tais como:

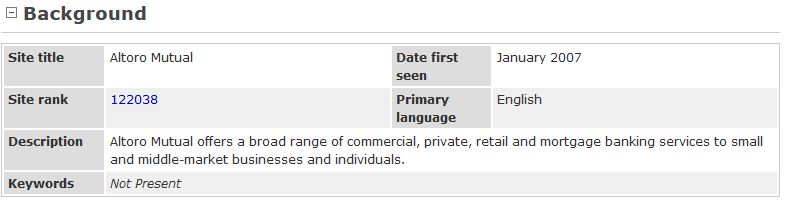


Figura 14 – Background da Altoro Mutual

Temos informações como: a data da primeira visualização do site, seu rank e uma breve descrição.

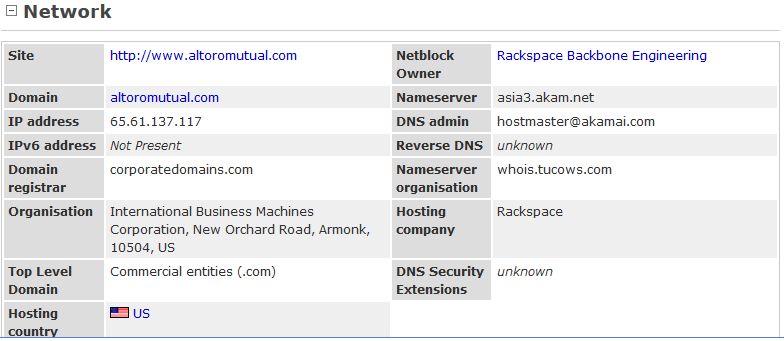


Figura 15 – Network da Altoro Mutual

Aqui temos informações preciosas como: dono do bloco IP, endereço IP, organização mantenedora IBM (International Business Machine), o país em que está hospedado, entre outras.



Figura 16 – Histórico de Hosting da Altoro Mutual

Aqui temos o histórico da plataforma utilizada pela Altoro Mutual, e começamos parte do nosso fingerprint do sistema operacional (Microsoft Windows Server), plataforma de hospedagem (Microsoft IIS) e a data da última consulta pelo NetCraft.

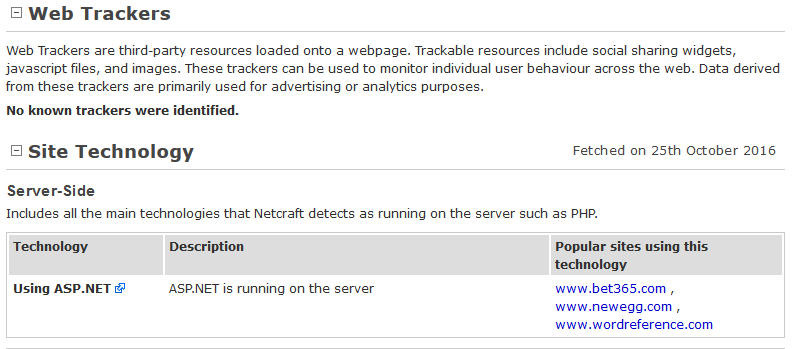


Figura 17 – Tecnologia Web da Altoro Mutual

Começamos a fazer o tracking da linguagem utilizada pela Altoro Mutual, no caso ASP.NET.

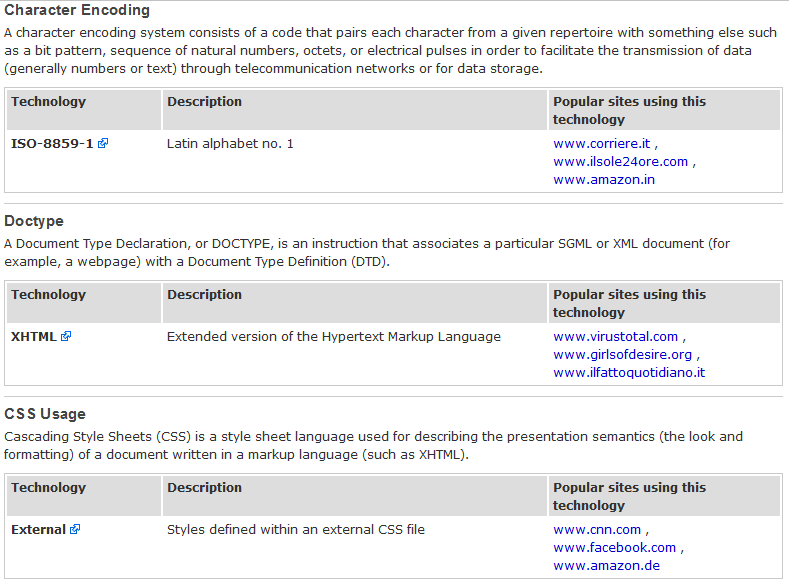


Figura 18 – Outras Tecnologias Web Utilizada Pela Altoro Mutual

Como podemos ver reunir diversas informações do passado de uma organização que resolve nascer no meio digital com suas aplicações e portais web.

**3 – 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]** TANENBAUM, Andrew S. – Redes de Computadores, 4º Ed, São Paulo, 2003, Editora Campus.

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

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

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

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

**[11]** WebBack Machine. Disponível em: <http://www.archive.org/about/about.php>. Acessado em: 05/05/2013.