****

**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 – Preparando o Firefox Para Pen-Test Web’**

O browser Firefox, com sua arquitetura extensível com os plug-ins, serve como o melhor navegador para pen-test em aplicativo web.

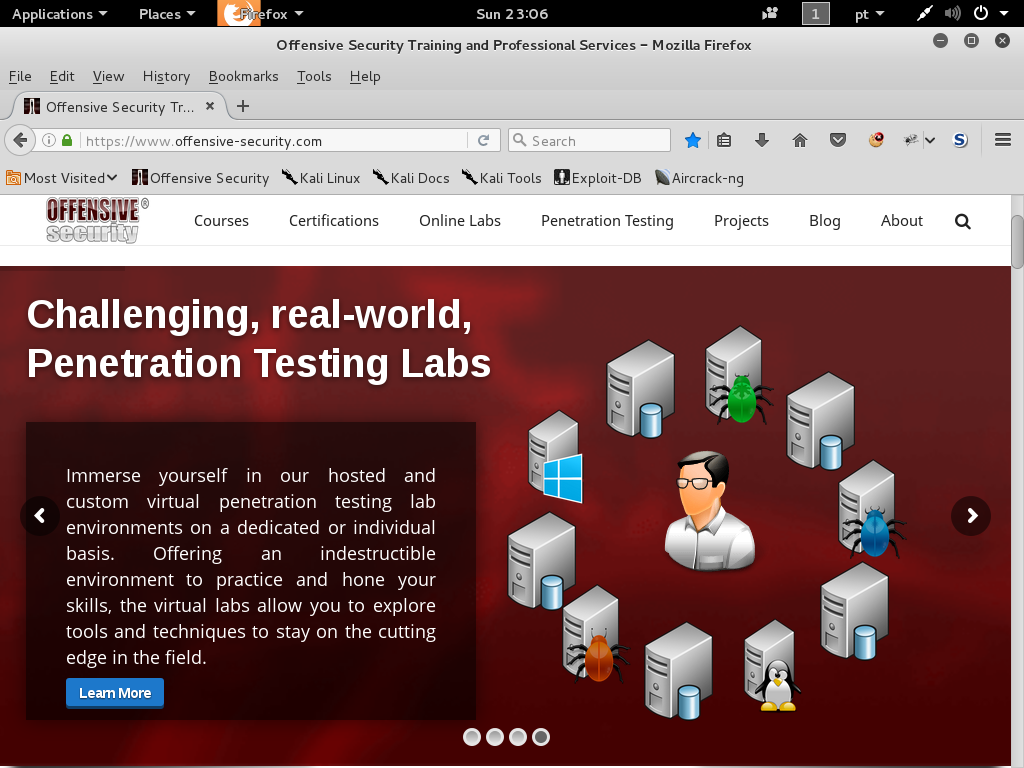


Figura 01 – Browser Firefox

**1 – Instalando as Extensões do Firefox**

As extensões do Firefox oferecem muitas funcionalidades, algumas extensões específicas nos auxiliam em um pen-test web.

Para instalar as extensões, clique no menu na parte superior direita do browser, clique em **Add-ons**.

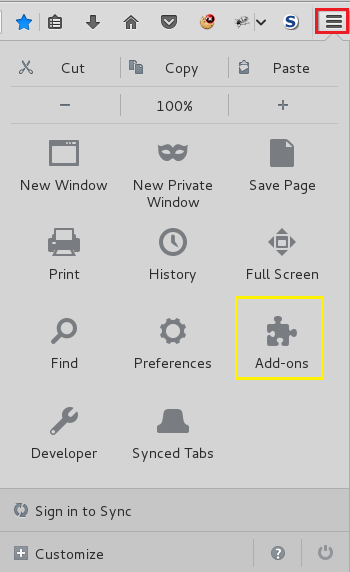


Figura 02 - Menu

Na página web de instalação de extensões clique em **Extensions** do lado direito e em **Search all add-ons**, digite o nome da extensão que desejamos instalar e de **Enter**.

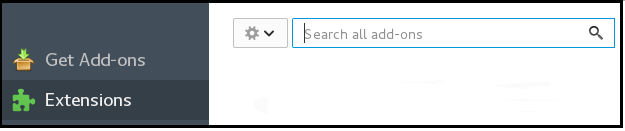


Figura 03 – Página de Instalação de Extensões

Para demostrar uma instalação digite ***“view source chart”*** e de **Enter** que será listado todos as extensões que tem a ver com a frase digitada.

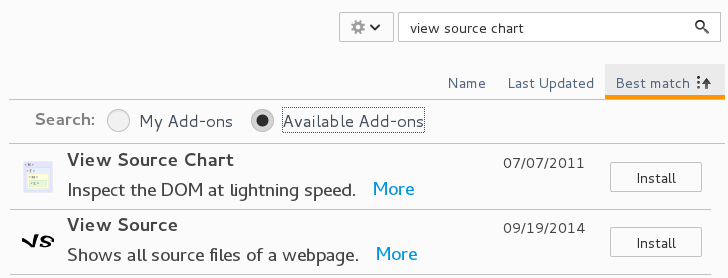


Figura 04 – Extensões Encontradas

Agora basta clicarmos no botão **Install**, que será feito o download e a instalação da extensão, em seguida você será solicitado a reiniciar o Firefox. Não precisa reiniciar imediatamente. Da próxima vez que você fechar todas as janelas do Firefox e iniciar novamente o aplicativo, a extensão estará disponível. Ou clique em **Restart now**, que o Firefox irá reiniciar e a funcionalidade da nova extensão estará disponível.

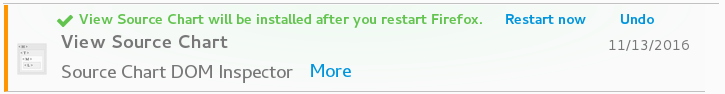


Figura 05 – Instalando uma Extensão

**2 – Extensões Para Pen-Test**

Algumas extensões do Firefox devem estar instaladas em um navegador preparado para pen-test, veja a lista abaixo:

* **Cookie Block**
* **Edit Cookies**
* **Firebug**
* **FoxyProxy Standard**
* **HackBar**
* **Live HTTP headers**
* **NoScript**
* **Redirect Bypasser**
* **Tamper Data**
* **User Agent Switcher**
* **View Source Chart**
* **Passive Recon**

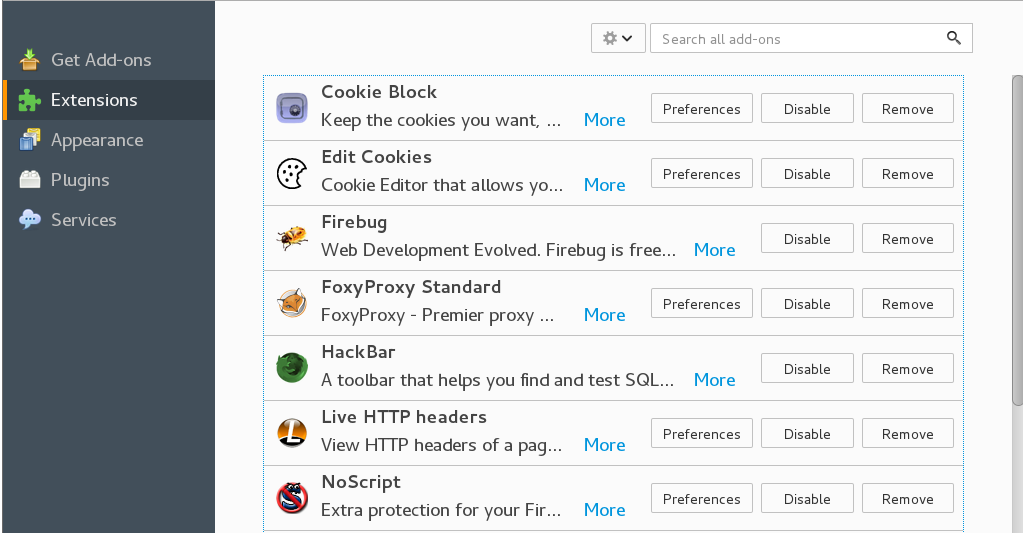


Figura 06 – Extensões Para Pen-Test

Algumas extensões serão vistas na barra de ferramentas do browser outras só podem ser acessadas através do menu **Tools**.

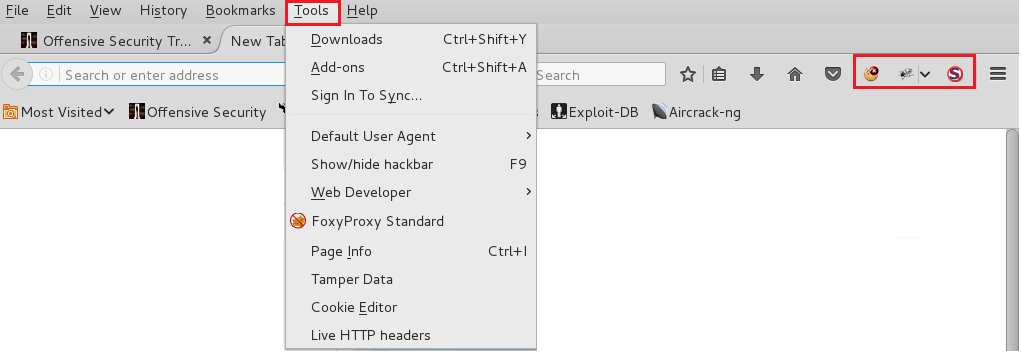


Figura 07 – Menu Tools com as Extensões que Acabamos de Instalar

**3 – Desabilitando o Captive Portal**

O Firefox mantem uma sessão ativa com o portal <http://detectportal.firefox.com/success.txt> para nós que desejamos manipular dados de envio utilizando algum proxy, isso se torna muito chato pelas múltiplas requisições feita pelo browser. Por isso, uma boa ideia é desabilitar essa atividade do browser. Para isso:

* Abra uma nova aba do browser e digite **about:config**, aceite a os riscos na página informando que erros podem deixar seu browser inutilizado;
* Tecle **CTRL+F** para abrir a caixa de **search** e digite **captiv**;
* De um duplo clique quando encontrar a diretiva **network.captive-portal-service.enabled** e altere de **true** para **false**.

Pronto você não será incomodado pelos vários acessos do browser ao portal gerando muito lixo na captura das requisições no seu proxy preferido.

**4 – Referências**

**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.

**[10]** HOPE, Paco; WALTHER, Ben – Web Segura Guia de Testes e Soluções – Rio de Janeiro – 2009, Alta Books.

**[11]** SUPPORT Mozilla. Disponível em <https://support.mozilla.org/en-US/questions/1157121>. Acessado em: 09/03/2018.