****

**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 – Shodan**



Figura 01 – Shodan

O Shodan diferentemente do Google, o Shodan realiza captura de banners de serviços.

Desta forma, em vez de procurar websites, ele busca serviço (FTP, SSH, etc.). Acesse o serviço em <http://shodan.oi> (será necessário criar uma conta para utilização de filtros).

**1 – Filtros de Buscas do Shodan**

Os comandos do Shodan são:

* **after/before** 🡪 Antes (after) e depois (before) de uma determinada data. Deve seguir o formato dd/mm/yyyy (dia e mês com dois dígitos e ano com quatro dígitos) ou dd-mm-yy. Por exemplo, a consulta after:01/01/2010 busca dispositivos inseridos na base de dados do Shodanapós o dia primeiro de janeiro de 2010;
* **city** 🡪 Filtra por cidades. Exemplo: city:”São Paulo”;
* **country** 🡪 Filtra por país. Exemplo: country:BR;
* **geo** 🡪 Filtra por geolocalização (em radianos). Exemplo: geo:-11.111,-22.222;
* **title** 🡪 Filtra por palavras no título da página do aplicativo web. Exemplo: title:WebOS;
* **hostname** 🡪 Filtra por nome dehost. Exemplo: hostname:.com.br;
* **net** 🡪 Filtra por range de endereços IP. Exemplo: net:200.2.1.0/24;
* **os** 🡪 Filtra por sistema operacional. Exemplo: os:”Windows xp”;
* **port** 🡪 Filtra por portas. Exemplo: port:80.

Suponha que seja necessário buscar por servidores Microsoft IIS pelo Brasil. Deste modo, digitamos iis country:BR no campo de busca e esse termo será destacado em vermelho no lugar em que foi capturado no banner.

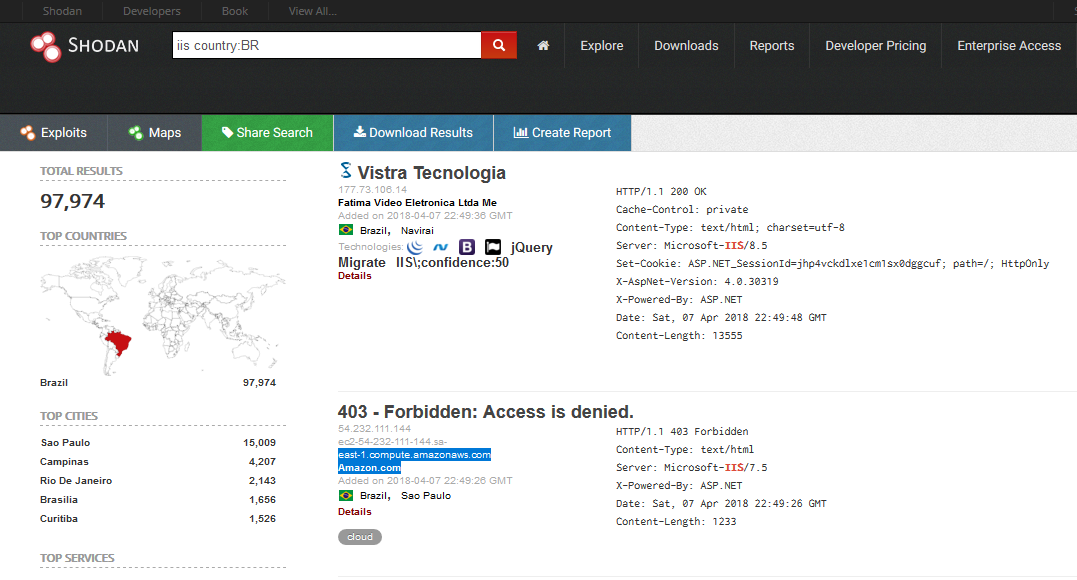


Figura 02 – Pesquisa por Web Server MS-IIS no Brasil

As aspas duplas devem ser utilizadas em nomes que necessitam de espaço. Assim a consulta city:“São Paulo”, por exemplo, retornam equipamentos localizados na cidade de São Paulo – Brasil. Agora a consulta city:São Paulo retorna cidades que começam com São em seu nome, tais como, São Paulo, São João, São Gonçalo, etc. e que tenha em seu banner palavra Paulo.

**2 – Exemplos de Buscas**

Alguns exemplos de buscas:

* **bigfoolcat ftp server** 🡪 Servidores EasyFTP potencialmente vulneráveis a Stack Buffer Overflow (https://exploit-db.com/exploits/16737);
* **os:”Windows xp” remote desktop protocol** 🡪 Servidores Windows XP/2003 com RDP habilitado potencialmente vulneráveis a ataques de negação de serviço (<https://technet.microsoft.com/pt-br/library/security/ms12-020.aspx>);
* **hfs 2.3** 🡪 Servidores HTTP File Server (HFS) potencialmente vulneráveis a ataques de RCE (<https://exploit-db.com/exploits/34668>);
* **title:”IP CAMERA Viewer”** 🡪 Câmeras conectadas na internet;
* **Linux upnp avtech country:BR** 🡪 Câmeras do modelo AVTECH.

**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]** 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]** MORENO, Daniel – Penest em Aplicações Web – São Paulo – 2017, Novatec