****

**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 – Enumerando DNS Server**

Mapear a infraestrutura de DNS do alvo mostrará quais as estações/servidores estão ativos e são acessíveis.

Em um pen-test, mesmo que o servidor alvo não apresente qualquer falha que possa comprometê-lo, ao mapear os domínios e subdomínios, talvez algum ativo apresente algum tipo de vulnerabilidade. Assim, a vulnerabilidade exposta por ativo mapeado pode permitir acesso ao servidor alvo. Por exemplo, um ataque de força bruta em um serviço web pode revelar uma senha que pode ser utilizado em outro serviço como o SSH para acesso remoto.

**1 – Usando a Tool DNSEnum**

Enumerar o DNS, na tentativa de realizar uma transferência de zona, fornecerá ao pen-tester a topologia de todos os computadores que estão na rede. Comprometer uma única estação poderá dar acesso a todo ambiente. Caso a transferência de zona não seja possível, uma lista de palavras poderá ser usada para enumeração de nomes de subdomínio.

root@kali-well:~tools# dnsenum how2security.com.br

Smartmatch is experimental at /usr/bin/dnsenum line 698.

Smartmatch is experimental at /usr/bin/dnsenum line 698.

dnsenum VERSION:1.2.4

----- how2security.com.br -----

Host's addresses:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

how2security.com.br. 3600 IN A 167.114.4.170

Name Servers:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_

a.sec.dns.br. 168443 IN A 200.160.0.11

b.sec.dns.br. 168245 IN A 200.192.232.11

Mail (MX) Servers:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

aspmx.l.google.com. 145 IN A 64.233.186.26

aspmx3.googlemail.com. 80 IN A 108.177.119.27

aspmx2.googlemail.com. 293 IN A 74.125.206.27

alt2.aspmx.l.google.com. 31 IN A 108.177.119.26

alt1.aspmx.l.google.com. 105 IN A 74.125.206.26

Trying Zone Transfers and getting Bind Versions:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Trying Zone Transfer for how2security.com.br on a.sec.dns.br ...

AXFR record query failed: REFUSED

Trying Zone Transfer for how2security.com.br on b.sec.dns.br ...

AXFR record query failed: REFUSED

brute force file not specified, bay.

root@kali-2k17-x64:~/tools#

root@kali-well:~tools#

Utilizando a força bruta com o DNSEnum.

root@kali-well:~tools# dnsenum how2security.com.br –f wordlist\_dns.txt

--==[ Resumido ]]==--

Brute forcing with wordlist\_dns.xt:

\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

webmail.how2security.com.br. 3600 IN CNAME ghs.googlehosted.com.

ghs.googlehosted.com. 289 IN A 216.58.222.83

www.how2security.com.br. 1742 IN CNAME how2security.com.br.

how2security.com.br. 1742 IN A 167.114.4.170

how2security.com.br class C netranges:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

167.114.4.0/24

Performing reverse lookup on 256 ip addresses:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

0 results out of 256 IP addresses.

how2security.com.br ip blocks:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

done.

root@kali-well:~tools#

Como podemos ver ele resolveu outros domínios e subdomínios para nós.

**2 – Referências Bibliográficas**

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