****

**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 – Scanning (Varredura)**

Nesta fase o pen-tester busca informações mais detalhadas do alvo, que possam revelar os vetores de ataque e enxergar as possibilidades que podem permitir ganhar acesso ao sistema, através da exploração de alguma falha encontrada.

Nesta fase buscamos as vulnerabilidades nas informações que foram colhidas na fase anterior (de reconhecimento). Por exemplo, no reconhecimento você descobre que existe um serviço na porta 80, que executa um serviço web, na fase de varredura você terá que identificar se o servidor web contém uma vulnerabilidade, ainda no exemplo, o alvo utiliza o Apache 1.3, e esta versão tem vulnerabilidades publicadas, porém seu serviço não acaba por aqui, existe outros dispositivos na frente do Servidor Apache vulnerável como IDS/IPS/WAF?

Então nesta fase devemos buscar respostas para algumas perguntas:

* Qual sistema operacional o alvo utiliza?
* Quais os serviços estão sendo executados no alvo?
* Quais serviços estão disponíveis para acesso?
* Quais as versões de cada serviço sendo executado?
* Há IDS/IPS na rede?
* Há honeypots na rede?
* Há firewalls na rede?
* Existe uma rede interna e outra externa, como DMZ?
* Há serviços com acesso público sendo executado em alguma máquina interna?
* Há algum software malicioso sendo executado em alguma máquina?
* Existem fraquezas no que foi encontrado?
* Identificou as vulnerabilidades?
* Descobriu documentos com informações sobre as vulnerabilidades?

A partir dessas informações, o pen-tester pode buscar maiores detalhes na internet ou fóruns especializados em busca de exploit que permitam explorar falhas existentes nas versões dos serviços sendo executados.

**1 – 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.