****

**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 – Reconnaissance (Reconhecimento)**

*“Dê-me seis horas para cortar uma árvore, e eu gastarei as primeiras quatro horas afiando o machado. ”* **Abraham Lincoln**

Essa é a fase mais importante de um ataque, e de um teste de invasão.

Você deve aprender o máximo possível sobre o ambiente de um alvo e seus colaboradores antes mesmo de lançar um ataque. Quanto mais informações você conseguir sobre seu alvo, maior será as chances de sucesso, achando os caminhos mais fáceis para obter o sucesso nos testes de invasão.

Os testes de invasão Black Box requerem um tempo considerável, pois os dados não são fornecidos.

A fase do reconhecimento envolve uma pesquisa apurada que inclui pesquisas na internet que contenha informações sobre o alvo, tais como, os recursos de monitoramento, pessoas e processos, desenhos de infraestrutura, endereços IP atribuído ao alvo (externo e interno), tipos de sistemas, engenharia social, serviços públicos, helpdesk, portas abertas para o mundo, onde estão hospedados esses serviços, serviços oferecidos para os clientes e fornecedores do alvo, entre outros.

É um serviço de inteligência, onde o maior número de informação irá gerar melhores resultados.

Qualquer informação que seja vinculado ao alvo é considerado de valor nessa primeira fase:

* Concorrentes;
* Nome de funcionários;
* Endereços físicos e lógicos;
* Telefones (principalmente dos departamentos de RH, TI, financeiro, etc.);
* Fornecedores;
* Comunidades sociais;
* Empresas do mesmo grupo;
* Definir aplicativos e uso comercial;
* Identificar tipos de sistemas;
* Identificar portas disponíveis;
* Identificar serviços em execução;
* Informações capturadas de dados com engenharia social passivamente e ativamente;
* Descoberta de documentos.

A fase de reconhecimento é onde coletamos o máximo de informações possíveis sobre o alvo, as quais serão utilizadas para elencarmos possíveis vulnerabilidades, vetores de ataques, etc.

Existem duas formas de fazermos o reconhecimento: de forma Passiva e de forma Ativa.

**0.1 – Reconhecimento Passivo**

A forma passiva de reconhecimento envolve a obtenção de informações sem o conhecimento do alvo, pois todas as informações obtidas são realizadas sem a necessidade de contato com os sistemas alvos.

Normalmente a obtenção das informações são realizadas através de buscas na Internet por pessoas, funcionários da companhia, engenharia social, assim como coleta de informações no lixo (que também são consideradas técnicas passivas de obtenção de informações).

Uma forma furtiva de obter informações passivamente é o sniffing de rede. Muitas informações podem ser obtidas através dos pacotes que trafegam na rede, como endereços IP, nomes de hosts e seus padrões, serviços na rede, etc., porém é necessário que seja feito internamente ou utilizando a técnica do MitM (Man in the Meddle).

Oe reconhecimento passivo também pode ser chamado de Footprint, Data-Mining ou OSINT (Open Source Intelligence).

**0.2 – Reconhecimento Ativo**

O reconhecimento ativo envolve uma sondagem direta a sistemas do alvo, com o objetivo de identificar hosts específicos, endereços IP ou blocos de endereços IP, serviços de rede, aplicações publicadas, entre outras informações.

Embora o reconhecimento ativo possa aumentar as chances do pen-tester ser detectado, diversas informações podem ser obtidas como a identificação da existência de sistemas de segurança, servidores web ativos e suas versões, e até mesmo versões de sistemas operacionais em uso, o que possibilita ao atacante encontrar vulnerabilidades nestes sistemas e explorar tais falhas para obter acesso não autorizados.

A coleta de informações é de suma importância para o sucesso do pen-test, se reunida e usada de forma apropriada. As coletas passivas são muito úteis, pois o alvo nem sequer é acessado, todas as informações são obtidas de fontes de terceiros. Já nas coletas ativas, o alvo é diretamente acessado, podendo causar indícios de ataque ou até mesmo registros e identificação do atacante.

**1 – Footprint**

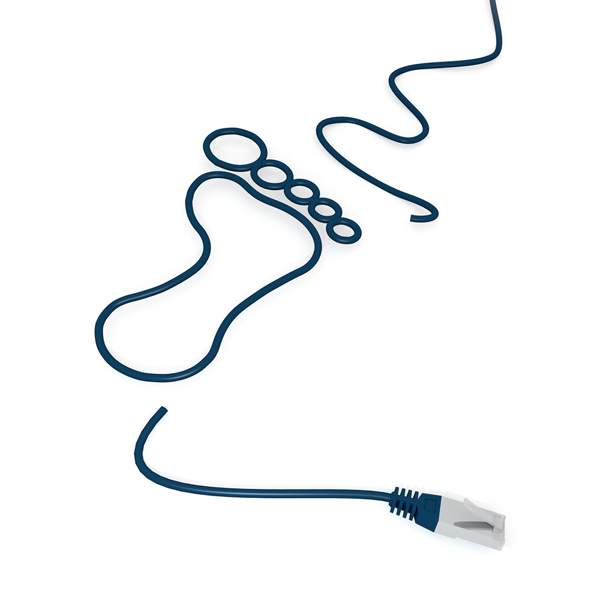


Figura 01 – Footprint Digital

Antes da diversão real do ataque começar, três passos especiais precisam ser executados: Footprint, Fingerprint e Enumeration. O footprint é a fina arte de coletar informações do alvo. Por exemplo, quando um ladrão decide roubar um banco, ele não entra simplesmente no banco e começa a exigir o dinheiro (pelo menos, não os espertos). Em vez disso, eles fazem grandes esforços para obter informações sobre o banco, tais como, as rotas dos carros-fortes e horários de entrega de dinheiro, as câmeras de vídeos, o número de caixas, saídas de emergências e tudo o mais que possa ajuda-los em um roubo bem-sucedido.

O mesmo se aplica a invasores bem-sucedidos. Eles precisam colher grande quantidade de informações para executar um ataque cirúrgico e bem direcionado (um que não seja descoberto imediatamente). Como resultado, um atacante coletará o máximo possível de informações sobre todos os aspectos da segurança de uma organização.

Conhecer o alvo é o objetivo dessa fase. É a partir do footprint que o invasor consegue informações essenciais para o sucesso de uma invasão, como a topologia da rede, nomes de domínios, sistemas operacionais usados (fingerprint). O intuito é criar um perfil do seu host-alvo para tentar descobrir falhas e possíveis brechas que possam ser exploradas a partir de configurações e senhas padrões.

Alguns alvos comuns de footprint são:

* Nomes de domínios;
* Responsáveis pelos domínios;
* Servidores que fazem parte do domínio;
* Identificação de sistemas operacionais do host-alvo (fingerprint);
* Subnets de rede;
* Serviços TCP/UDP disponíveis;
* Topologia de rede;
* Nomes de usuários e de grupos;
* Banners que identificam versões de serviços ou mesmo a versão do sistema operacional;
* Tabelas de roteamento;
* Servidores ocultos por NAT através de análise de TTL dos pacotes;
* Endereços de e-mails;
* Contas de e-mails válidas, contas de FTP e outros serviços;
* Informações de serviços SNMP mal configurados;
* Domínio da organização e os hosts que o compõem;
* Ranges de IP do domínio;
* Estrutura de segurança (Firewalls, IPS/IDS, WAP, DLP, etc.);
* Identificação dos roteadores.

O footprint é a parte mais importante de um teste de invasão, um pen-tester costuma gastar 80% do seu tempo analisando um alvo e levantando informações sobre ele. E apenas 20% do tempo é usado para atacar o alvo.

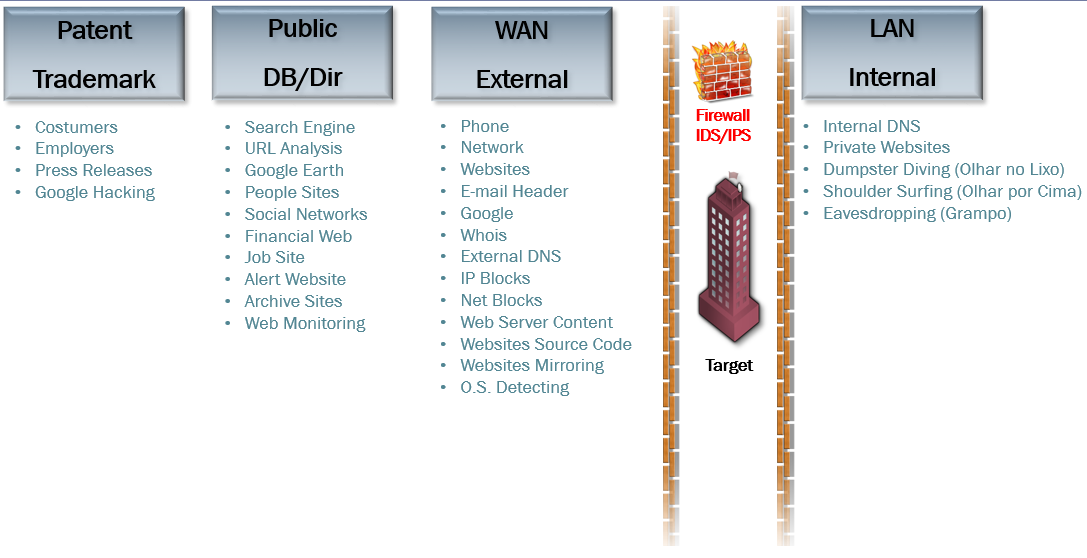


Figura 02 – Objetivos do Footprint

**2 – 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]** 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.