SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DO PIAUÍ
CAMPUS FLORIANO
EIXO TECNOLÓGICO: INFORMAÇÃO E COMUNICAÇÃO
CURSO: ESPECIALIZAÇÃO EM DESENVOLVIMENTO WEB
DISCIPLINA: SEGURANÇA WEB
PROFESSOR: MARCONY M. MAXIMO

Atividade: Relatório de Invasão

COMPONENTES:
Laiton Garcia dos Santos
Rubens dos Santos Lopes
Felipe Mateus M Mendes
Justino Duarte Santos
Antônio Carlos M Barros
Thiago Rafael P de Carvalho
Manoel da G N da Cruz
Sérgio Willames Oliveira Costa
Luiz Filipe Ibiapino Oliveira
Robert Ferraz de Sousa

Floriano – PI, 20 de fevereiro de 2017.

I. INTRODUÇÃO

O objetivo deste relatório e apresentar os primeiros passos utilizados para sondagem de hosts na internet com a utilização da ferramenta **nmap** para escanear computadores a procura por portas tcp ou udp abertas e os possíveis serviços e ou sistemas operacionais que as utilizam e através de suas vulnerabilidades ataca-los. Tudo disponível para pesquisa na internet.

Não houve a preocupação de se ater a um site especifico, o trabalhar foi realizado como os *Newbies* (novatos) e *Lammers* o fazem. Foi utilizado o Zenmap que é uma interface gráfica do nmap o que pode torna mais simples o uso da ferramenta sem a necessidade de aprendizado de comandos.

II. FERRAMENTA NMAP

O Nmap é um dos mais utilizados e completos programas para se fazer uma análise/rastreio de uma rede, host, servidor, ou sub net. Ele possui várias facetas, utilidades e uma lista enorme de comandos e opções. Ele é um *portscan* de uso geral, principalmente para verificar portas abertas em determinado host ou um grupo deles.

Foi desenvolvido por Gordon Lyon, e com este programa tentou resolver questões em relação aos testes que fazia, como:

- Identificar os computadores que estão ligados na rede local;
- Quais ips se encontram na rede;
- Qual o sistema operacional;
- Quais portas estão abertas;
- Os serviços que utilizam essas portas;
- Descobrir se o sistema está infectado com vírus ou malwares;
- Pesquisar por computadores ou serviços não autorizados na rede.

III. UTILIZANDO NMAP

O programa **Zenmap** torna o escaneamento uma tarefa simples de ser executada. O primeiro passo para executar um escaneamento é escolher o seu alvo. Você pode inserir um domínio (exemplo.com.br), um endereço IP (127.0.0.1), uma rede (192.168.1.0/24) ou uma combinação destes.

Os perfis são pré-definidos em grupos de modificadores que alteram o que é lido. Os perfis admitem escolher diferentes tipos de escaneamentos sem ter de digitar os modificadores ou parâmetros na linha de comando. Escolha o perfil que melhor se adapta às suas necessidades:

- Escaneamento intenso (*Intense Scan*) Um escaneamento completo. Contém detecção de Sistema Operacional (SO), detecção de versão, escaneamento de scripts, rastreio de rota (*traceroute*) e possui também um tempo de escaneamento ou varredura agressivo. Este é considerado um escaneamento intrusivo. Escaneamento de *Ping* (*Ping Scan*) Este escaneamento simplesmente detecta se o alvo está online, não escaneando qualquer porta.
- Escaneamento Rápido (*Quick scan*) Este é mais rápido do que um escaneamento regular e apenas escaneia portas selecionadas.
- Escaneamento Regular (*Regular scan*) Este é o escaneamento padrão do Nmap sem quaisquer modificadores ou parâmetros. Ele retornará um *ping* e as portas abertas no alvo.

Os resultados ativos do escaneamento serão apresentados na aba de saída do Nmap. O tempo necessário para o escaneamento dependerá do perfil de escaneamento selecionado, da distância física até o alvo e das configurações de rede alvo.

Uma vez que o escaneamento tenha finalizado, você verá a mensagem "*Nmap done*" (Nmap finalizado) na parte inferior da aba de saída ou retorno do Nmap. Você poderá agora checar seus resultados, dependendo do tipo de escaneamento que você executou. Todos os resultados serão listados na aba principal de saída ou retorno do Nmap, mas você pode utilizar as outras abas para conseguir uma melhor visualização de algum dado em específico:

- Portas/Hosts (*Ports*/*Hosts*) Esta aba lhe apresentará os resultados de seu escaneamento de portas, incluindo os serviços para estas portas.
- Topologia (*Topology*) Isto apresentará um rastreamento de rotas para o escaneamento realizado. Você poderá ver quantos saltos seus dados dão até atingir o alvo.
- Detalhes de Host (*Host Details*) Isto lhe mostra um sumário aprendido de seu alvo durante o escaneamento, tais como o número de portas, endereços IP, nomes de máquinas, sistemas operacionais e outras informações.
- Escaneamentos (*Scans*) Esta aba armazena os comandos que você digitou anteriormente para escaneamentos. Isto permite-lhe reescanear rapidamente com um conjunto específico de parâmetros.

Apesar de existirem os *frontends* gráficos disponíveis, os comandos passados em modo texto permitem uma enorme flexibilidade e, ao contrário do que possa parecer, o uso não é difícil. A sintaxe básica do comando sempre será:

nmap <variável> <parâmetros> <alvo> p <portas>

Onde o alvo é o endereço IP do host ou rede que se deseja escanear. Caso exista uma forma de resolver nomes, como um DNS configurado, você pode usar o nome do host ao invés do IP. Com a opção -p podemos especificar portas ou faixas de portas para análise.

Pode-se utilizar variáveis na linha de comando para alterar os parâmetros do escaneamento, resultando em um retorno mais ou menos detalhado. Alterando as variáveis do escaneamento você estará também alterando o grau de intrusão do escaneamento. Você pode adicionar múltiplas variáveis ou parâmetros inserindo um espaço entre cada uma delas. Os parâmetros são ajustados de acordo com o que se deseja obter, os principais são:

- **-sS**: Este é um escaneamento furtivo SYN. Ele é menos detectável que o escaneamento padrão, mas pode levar mais tempo. Muitos firewalls modernos podem detectar um escaneamento -sS.

- **-sn**: Este é um escaneamento com *ping*. Isto irá desabilitar o escaneamento de portas e irá checar apenas se o host ou alvo está online.
- **-O**: Este é um escaneamento de Sistema Operacional. O escaneamento tentará determinar o sistema operacional do alvo.
- **-A**: Esta variável habilita diversos dos mais utilizados escaneamentos: detecção de SO, detecção de versão, escaneamento de scripts e rotas.
- **-F**: Este habilita o modo rápido e irá reduzir o número de portas escaneadas.

- **-v**: Este mostrará mais informações em seu resultado, tornando-as mais fáceis de ler.

IV. COMEÇANDO O RASTREAMENTO

Lammers não são verdadeiramente experientes mas dão muita dor de cabeça aos proprietários, pois fazem suas invasões de forma aleatória, não querem saber a quem fizeram o mal mas o fazem e gabam-se de que o fizeram.

O primeiro passo foi identificar o IP da máquina local, numa máquina virtual Debian, como pode ser visto na figura 1, com o comando ifconfig no CMD, ou pelo site meuip.com.br. Pega-se o IP mantém-se os identificadores da rede e altera apenas o quarto octeto para **1/24** para utilizar no próximo passo.

Esta varredura foi realizada em uma rede Wifi simples criada para este fim, no Laboratório I de Informática no campus Floriano. A rede foi composta por duas maquinas virtuais e três físicas. Após identificar a rede descrita no passo anterior, o primeiro comando usado no Nmap foi para determinar quantos e quais *hosts* estão na rede, utilizando o comando **nmap -sN 192.168.0.1/24*.*** Foram encontrados as 5 *hosts,* listados por ordem de IP, alguns com seu domínio, inclusive todos eles estavam online, como pode ser visto em parte desse relatório na figura 2.

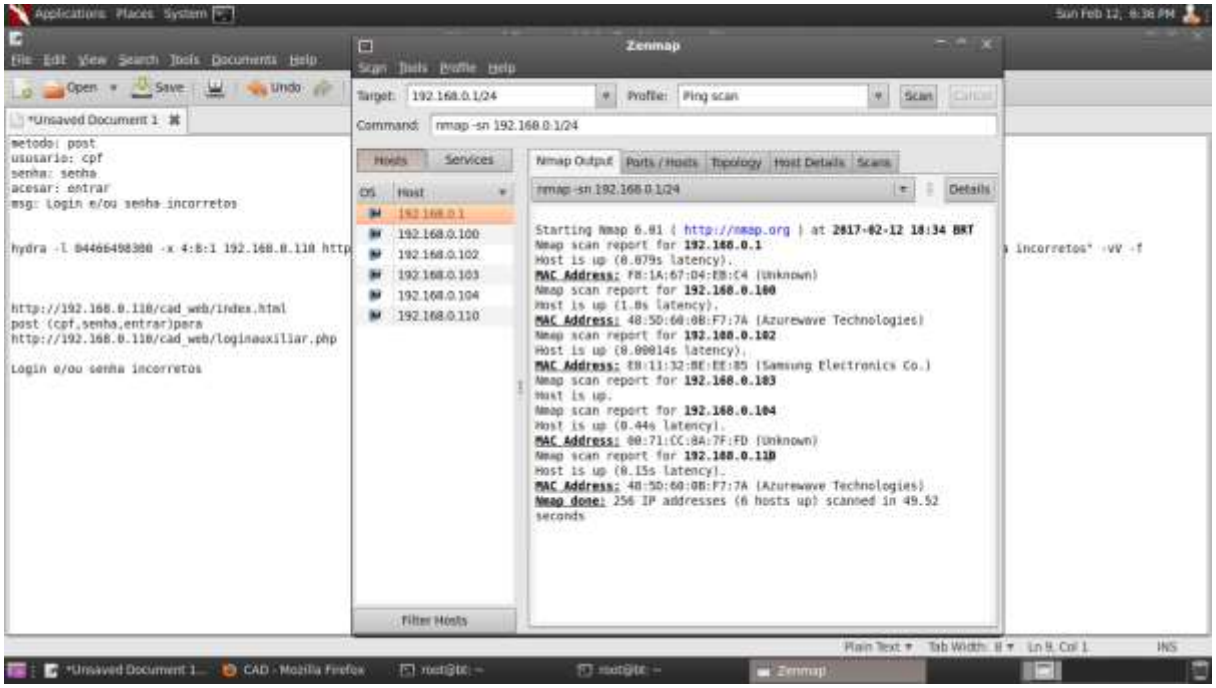

Figura 2: Varredura identificas todos os hosts na rede

Agora o Lammer pode analisar se existe algum alvo especifico para ele focar ou fazer novas varreduras:

- Fazer uma verificação e identificar quais *hosts* possuem portas abertas com o comando **nmap --open 192.168.0.1/24**, mas uma porta aberta não quer dizer uma vulnerabilidade, vulnerável pode ser o serviço que utiliza aquela porta.
- Fazer uma verificação e identificar as portas abertas e os possíveis programas/serviços que utilizam aquela porta com o comando **nmap –sV 192.168.0.1/24.**
- Fazer uma verificação de quais portas não estão protegidas por um firewall, **nmap –sA 192.168.0.1/24.**

São várias as opções possíveis de varredura, a escolhida foi a de verificar detecção de SO, detecção de versão, escaneamento de scripts e rotas: **nmap –A 192.168.0.1**. Dentre os resultados estão:

Neste *host,* figura 3, o Nmap não conseguiu identificar se as portas são filtradas ou não, mas pudemos identificar uma porta 80/tcp com um Servidor Apache com um serviço http.

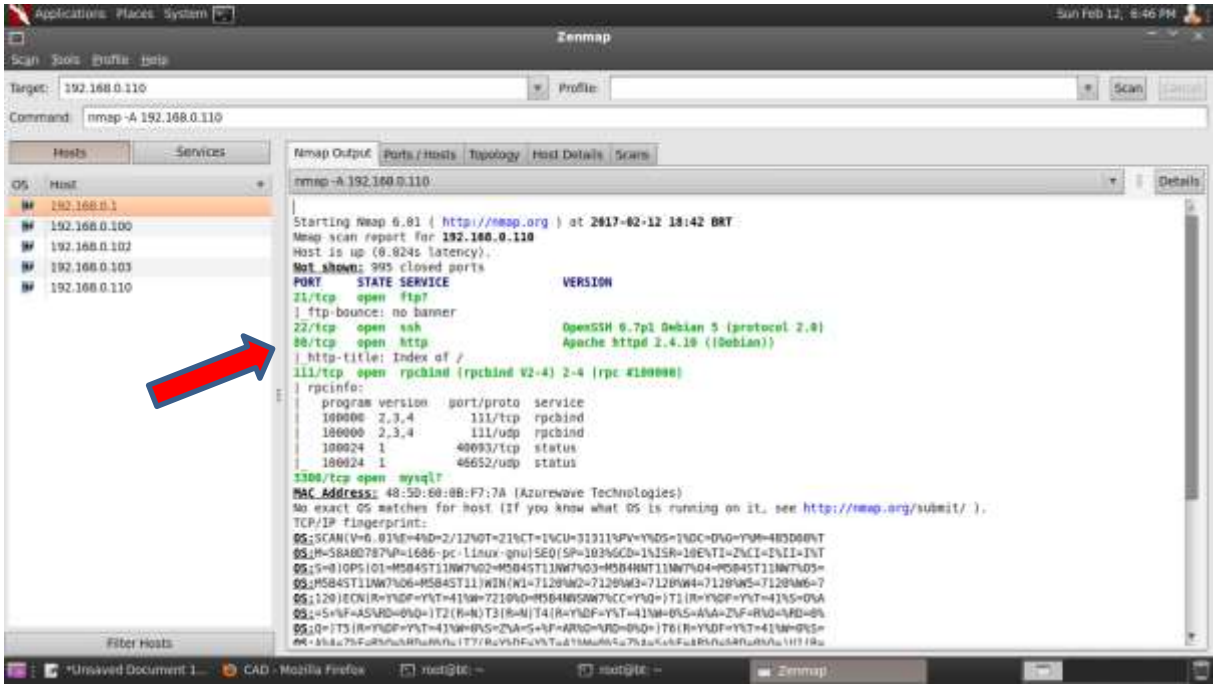

Figura 3: Varredura identifica portas e SO

Utilizando o seu ip 192.168.0.110, figura 4, fomos até a página e verificamos o conteúdo da primeira pasta CAD_WEB e vimos se tratar de um site com um formulário de login. Por se tratar de um ataque simulado, sabemos que o site utiliza uma senha de 4 dígitos e CPF para login, conforme figura 5.

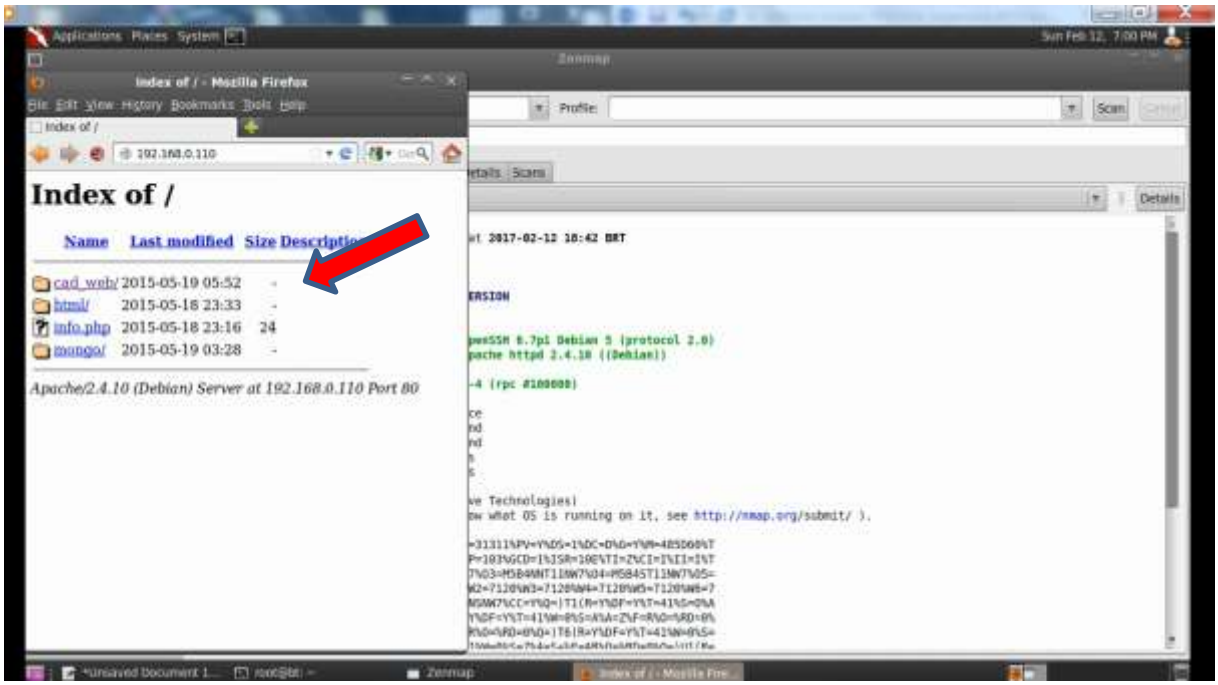

Figura 4: Varredura no ip 192.168.0.110

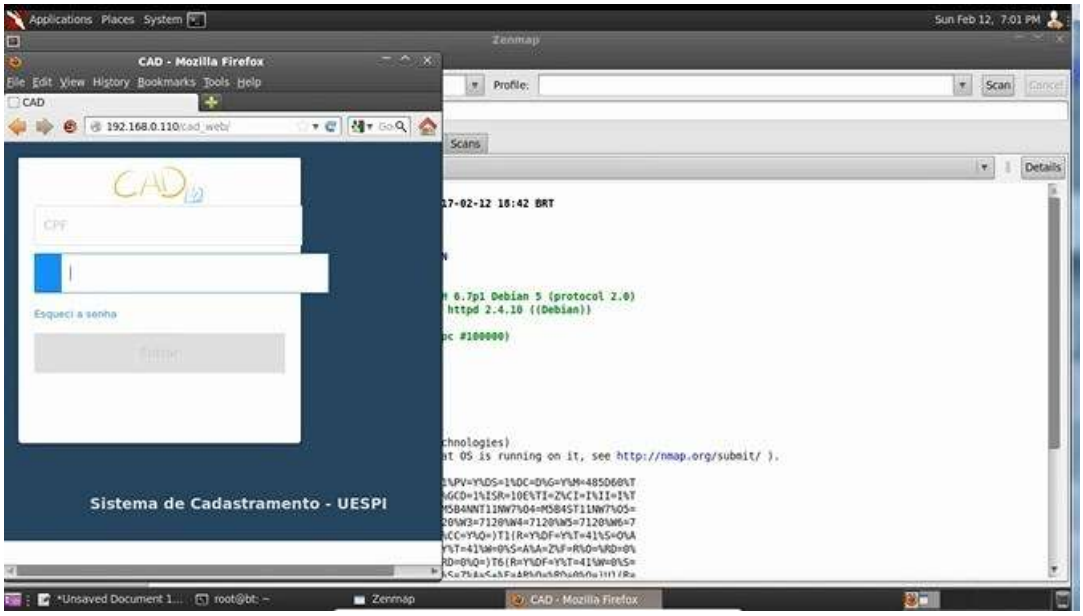

Figura 5: Serviço CAD_WEB o alvo

A partir daqui o Lammer ou cracker começa a ter mais interesse na invasão, pois conseguiu identificar alguns serviços e suas versões. Primeiramente verificamos o código fonte da página identificando os componentes, campos e direcionamentos, do formulário html. Para o ataque utilizamos a ferramenta Hydra, constante no pacote Backtrack 5, que é um ataque de força bruta. Para isso o Hydra precisa ser configurado com os dados do formulário que pegamos ao analisar o código fonte da página como pode ser visto na figura 6. A seguir listamos os dados e o comando para o ataque da ferramenta:

- Método: post
- Usuário: cpf
- Senha: senha
- Acessar: entrar
- Mensagem de erro: Login e/ou senha incorretos

Comando no Hydra:

hydra -l 04466498300 -x 4:8:1 192.168.0.110 http-post-form "/cad_web/loginauxiliar.php:cpf=^USER^&senha=^PASS^&entrar=Entrar:Login e/ou senha incorretos" -vV -f

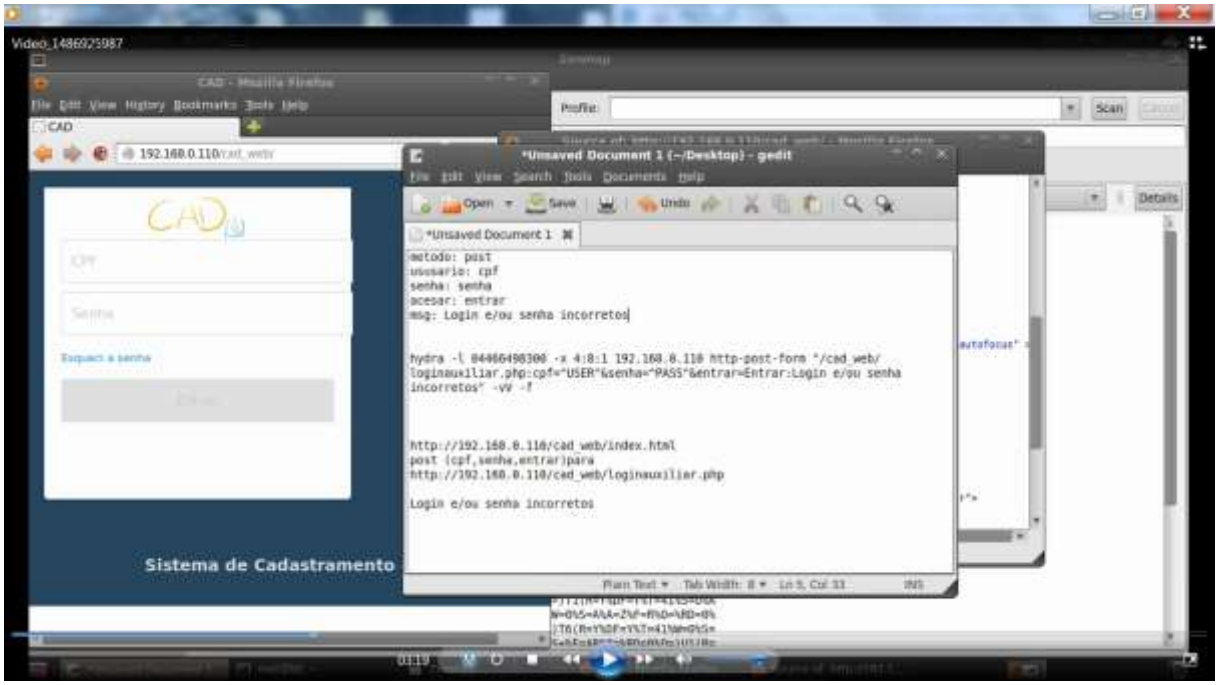

Figura 6: Configurando ataque com Hydra

V. CONCLUSÃO

A máxima é de que nenhum sistema é ou está seguro. É um desafio constante e que todos os envolvidos através de tentativas, acertos e erros conseguem lograr resultados tanto no sentido de assegurar a integridade dos dados como no sentido de corromper e adulterá-los. Novos tipos de ataques e intrusões acontecem principalmente quando novos sistemas aparecem, devemos estar constantemente atualizados as vulnerabilidades dos sistemas, conhecer as ferramentas de proteção e preocupar principalmente em ter um bom Plano de Contingência.

Para maiores detalhes desse trabalho acompanha CD-ROM com vídeo em anexo.

Referências:

André07. **Usando o Nmap**. Coluna Andre07, www.invasão.com.br. Acessado aos: 26 de abril de 2016.

Hacks. **Nmap – 30 exemplos de comandos para analises de redes e portas**. Coluna Feramentas, em www.hacks.pt. Acessado aos 27 de abril de 2016.

Lucas Mura. **Pesquisa encontra falhas no UPNP de programas.** Categoria Segurança, www.baboo.com.br. Acessado aos: 27 de abril de 2016.

Ppiware. **Vulnerabilidade na shell bash poe em risco máquinas Linux**. Disponivel em: <http://pplware.sapo.pt/linux/vulnerabilidade-na-shell-bash-poe-em-risco-maquinas-linux/>, acessada aos: 25 de abril de 2016.

Back|track-linux.org. **Quebrando senhas via HTTP com (Hydra).** Disponível em: <http://www.backtrack-linux.org/forums/showthread.php?t=27322>, acessada aos 12 de fevereiro de 2017.

Wikihow. **Como Executar um Simples Escaneamento com o Nmap**. Disponível em: <http://pt.wikihow.com/ExecutarumSimplesEscaneamentocomoNmap>, acessada aos: 26 de abril de 2016.