SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DO PIAUÍ
CAMPUS FLORIANO
EIXO TECNOLÓGICO: INFORMAÇÃO E COMUNICAÇÃO
CURSO: TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS
PERÍODO LETIVO: 2º SEMESTRE **BLOCO:** VI
DISCIPLINA: SEGURANÇA E AUDITORIA DE SISTEMAS
PROFESSOR: SILVINO MARQUES DA SILVA JUNIOR
ALUNO (A): LAITON GARCIA DOS SANTOS

Atividade: Relatório de Invasão

Floriano – PI, 28 de Abril de 2016.

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 com o comando ipconfig 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 na rede do IFPI, campus Floriano, 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 200.137.xxx.1/24*.*** Foram encontrados 29 *hosts,* listados por ordem de IP, alguns com seu domínio, inclusive todos eles online, como pode ser visto no **apêndice A**, e apresentados ordenados por IP como na figura 1.

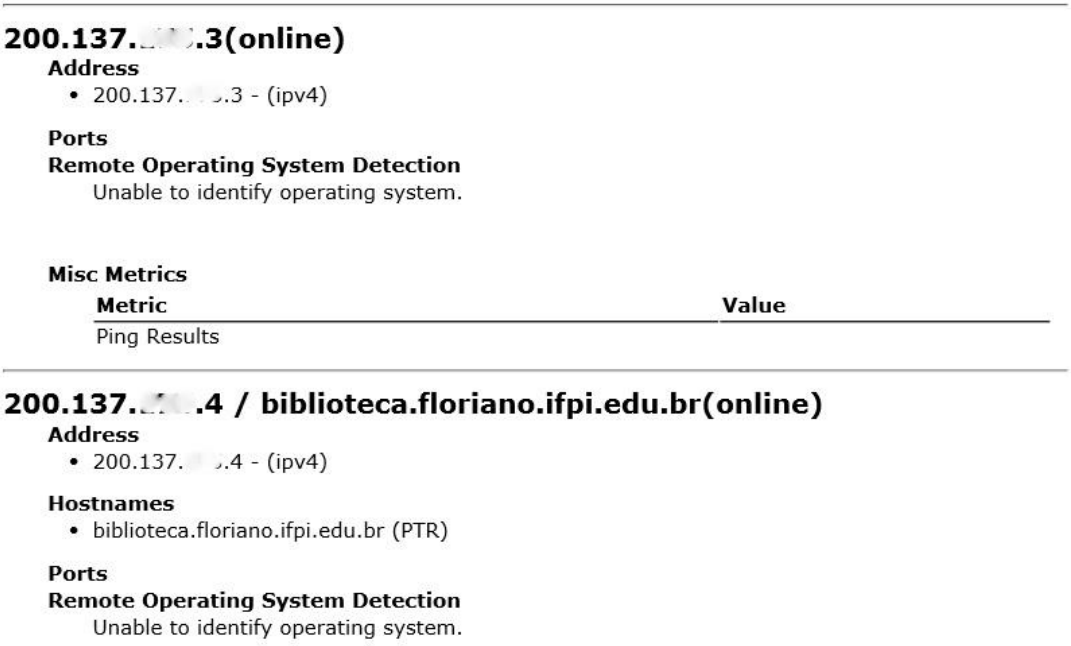


Figura 1: Varredura identificas todos os hosts na rede

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 200.137.xxx.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 200.137.xxx.1/24.**
- Fazer uma verificação de quais portas não estão protegidas por um firewall, **nmap –sA 200.137.xxx.1/24.**

São várias as opções possíveis de varredura, a escolhida foi a de verificar as portas que não são filtradas por um firewall **nmap –sA 200.137.xxx.1/24**. Dentre os resultados estão:

Neste *host,* figura 2, o Nmap não conseguiu identificar se as portas são filtradas ou não, então teria que recorrer a outros comandos ou a outros tipos de scan, como scan Window, scan Syn e outros.

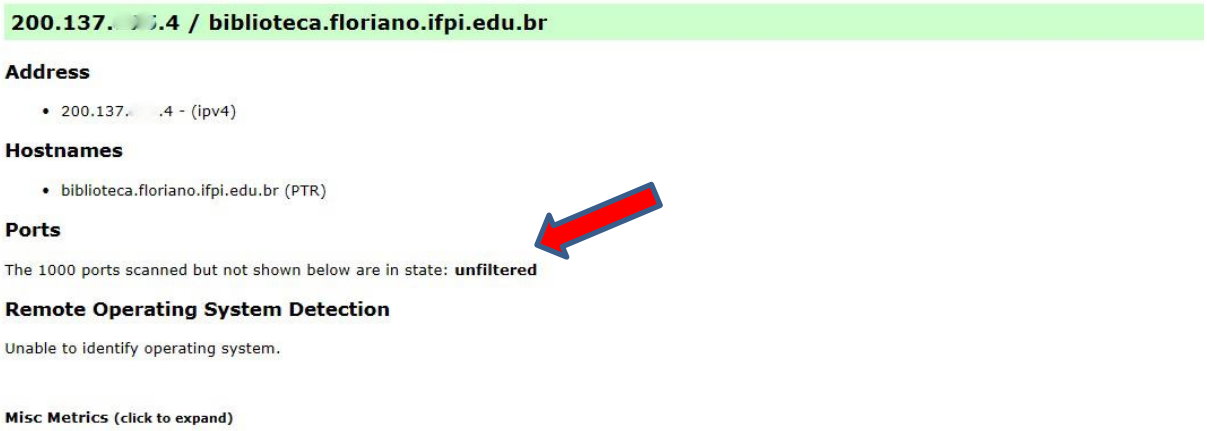


Figura 2: Varredura identifica portas com firewall

Neste outro *host,* figura 3, o Nmap identificou que 997 portas estão sendo filtradas e, na primeira coluna da tabela, as portas 22, 80 e 443 não estão sendo filtradas, também os tipos de serviços por elas usadas respectivamente ssh, http e https.

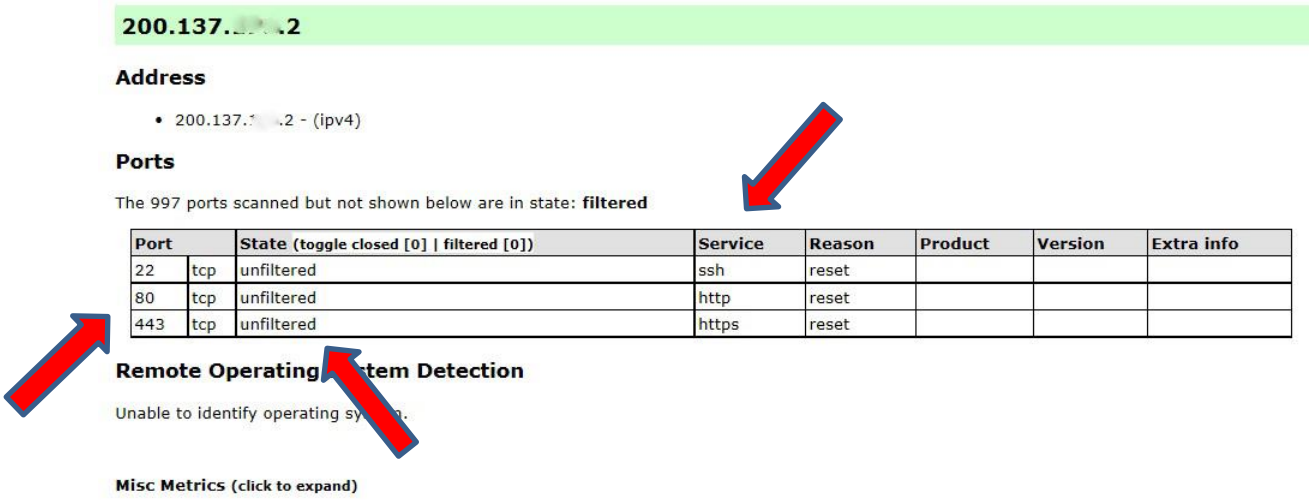
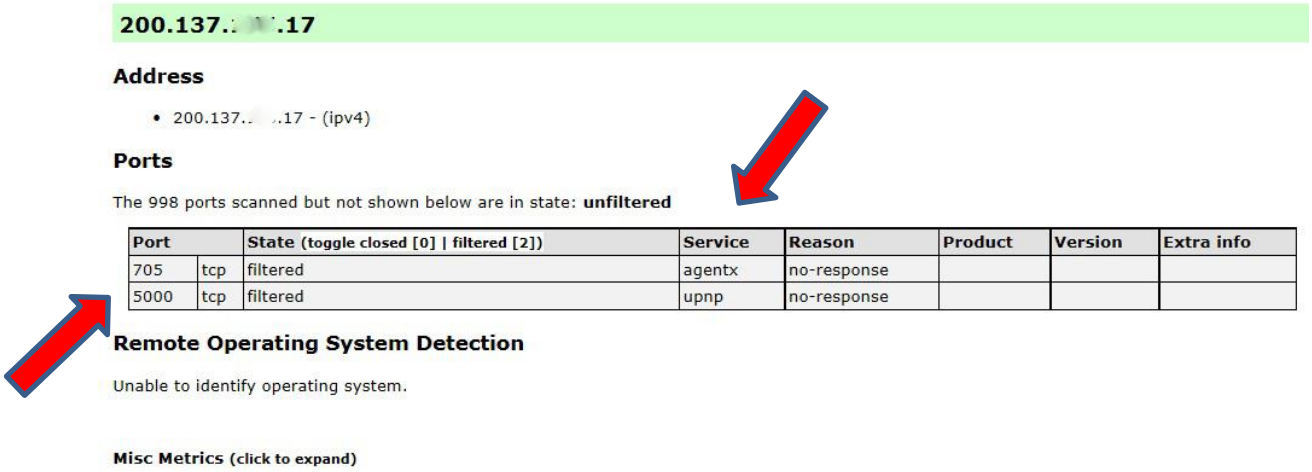


Figura 3: Varredura identifica portas não filtradas firewall

Este *host*, figura 4, apresenta duas portas, 705 e 5000, que não estão sendo filtradas por um firewall mas pelos serviços agentx e upnp respectivamente.



200.137.[illegible].17

Address

- 200.137.[illegible].17 - (ipv4)

Ports

The 998 ports scanned but not shown below are in state: **unfiltered**

Port		State (toggle closed [0] | filtered [2])	Service	Reason	Product	Version	Extra info
705	tcp	filtered	agentx	no-response			
5000	tcp	filtered	upnp	no-response			

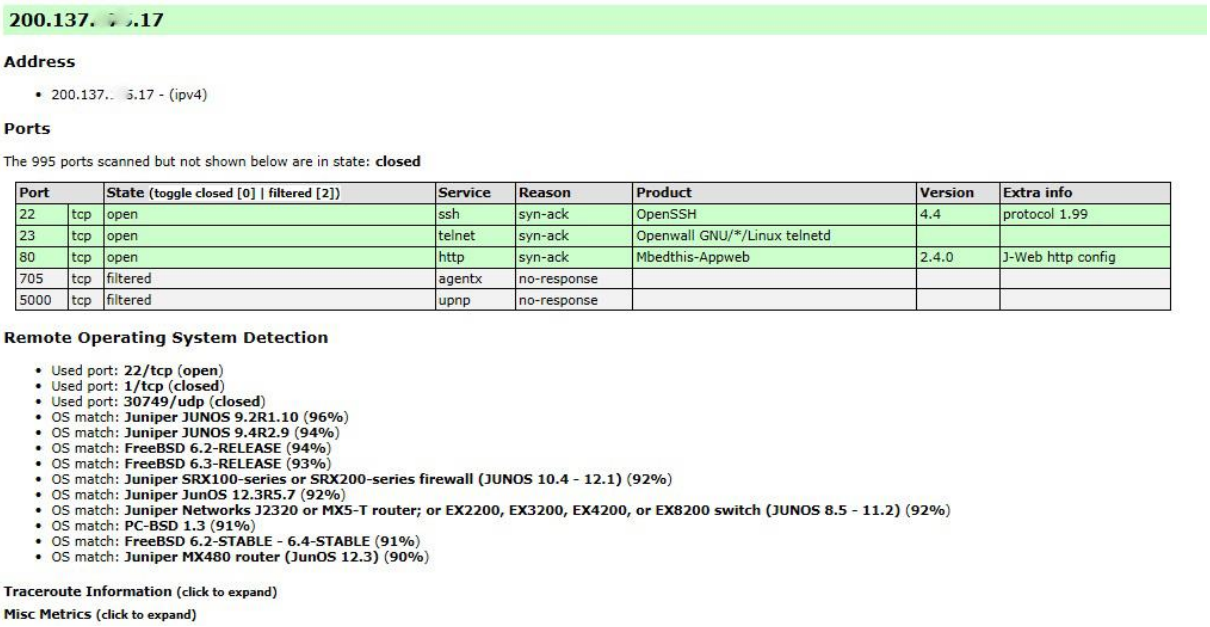
Remote Operating System Detection

Unable to identify operating system.

Misc Metrics (click to expand)

Figura 4: Varredura identifica portas sem filtros

O host 200.137.xxx.17 apresentam os serviços agentx e upnp, agora aplica-se uma varredura, com o seguinte comendo **nmap –A 200.137.xxx.17**, neste computador para verificar suas portas abertas e os serviços executados nelas e também seu SO. O resultado pode ser visto na figura 5.



200.137.[illegible].17

Address

- 200.137.[illegible].17 - (ipv4)

Ports

The 995 ports scanned but not shown below are in state: **closed**

Port		State (toggle closed [0] | filtered [2])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	4.4	protocol 1.99
23	tcp	open	telnet	syn-ack	Openwall GNU/*/Linux telnetd		
80	tcp	open	http	syn-ack	Mbedthis-Appweb	2.4.0	J-Web http config
705	tcp	filtered	agentx	no-response			
5000	tcp	filtered	upnp	no-response			

Remote Operating System Detection

- Used port: **22/tcp (open)**
- Used port: **1/tcp (closed)**
- Used port: **30749/udp (closed)**
- OS match: **Juniper JUNOS 9.2R1.10 (96%)**
- OS match: **Juniper JUNOS 9.4R2.9 (94%)**
- OS match: **FreeBSD 6.2-RELEASE (94%)**
- OS match: **FreeBSD 6.3-RELEASE (93%)**
- OS match: **Juniper SRX100-series or SRX200-series firewall (JUNOS 10.4 - 12.1) (92%)**
- OS match: **Juniper JunOS 12.3R5.7 (92%)**
- OS match: **Juniper Networks J2320 or MX5-T router; or EX2200, EX3200, EX4200, or EX8200 switch (JUNOS 8.5 - 11.2) (92%)**
- OS match: **PC-BSD 1.3 (91%)**
- OS match: **FreeBSD 6.2-STABLE - 6.4-STABLE (91%)**
- OS match: **Juniper MX480 router (JunOS 12.3) (90%)**

Traceroute Information (click to expand)

Misc Metrics (click to expand)

Figura 5: Varredura identifica portas abertas e serviços

A partir daqui o Lammer ou cracker começa a ter mais interesse na invasão, pois conseguiu identificar alguns serviços e suas versões. Agora é pesquisar quais destes serviços apresentam vulnerabilidades e quais são mais fáceis de serem penetradas. Aqui poderíamos citar como exemplo:

- **Serviço upnp: (porta 5000)** ou *Universal Plug in Play* é um protocolo que permite que produtos em rede se encontrem e automaticamente criem uma conexão para compartilhar dados, streaming ou reproduzir mídia. Ele normalmente é utilizado dentro de redes fechadas, porém a pesquisa encontrou mais de 80 milhões de ips públicos que respondiam a chamadas uPnP na internet. Desses 80 milhões, 20% deles deixaram exposto o UPnP SOAP (*Simple Object Access Protocol*□ na internet. Isto permite que hackers tenham acesso a redes que estejam bloqueadas por Firewall e obtenham dados confidenciais deles. De acordo com a Rapid7, boa parte destes aparelhos utilizavam uma biblioteca chamada *Portable UPnP SDK*. Dentro dela, foram encontradas oito vulnerabilidades, sendo que duas delas permitem a execução de códigos maliciosos remotamente.
- **Serviço OpenSSH: (porta 22)** De acordo com várias notícias publicadas nas últimas horas, o interpretador de comandos *Bash* tem um grave problema de segurança. Stephane Chazelas, o autor de tal descoberta, refere que a vulnerabilidade está presente até a versão 4.4 do *Bash* e coloca em risco máquinas Linux e Macs. A vulnerabilidade pode ser explorada remotamente através de serviços como é o caso do Apache ou OpenSSH. Quem tem máquinas Linux ou Macs com OSX é muito importante que verifique se a *shell Bash* tem uma versão inferior ou igual a 4.4. No caso do seu sistema ser afetado por tal vulnerabilidade é importante que saiba que o mesmo pode ser atacado remotamente por atacantes não autenticados.

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.

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.

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