

11

# FERRAMENTAS DE VARREDURA DE PORTAS ONLINE FÁCEIS DE USAR



# 11 ferramentas de varredura de portas online fáceis de usar

O objetivo deste e-book é ensinar como usar 11 ferramentas de varredura de portas gratuitas e online. Ele complementa o e-book em que também ensinamos a usar ferramentas de varredura. A diferença é que estas são online, não instalam.

Todo hacker ou profissional de segurança da informação precisa saber sobre varredura de portas, uma tarefa necessária em várias operações, como: ethical hacking, pentesting, black hat, CTF (Capture the Flag), Bug Bounty (caçador de recompensas), segurança da informação, prova de conceito, testes de segurança em redes e várias outras.

Não sei como este material (e-book e/ou videoaula) chegou até você, mas se foi por você ter se matriculado na Escola de Hackers ou por ter adquirido algum curso meu na Udemy, então poderá tirar suas dúvidas comigo no WhatsApp:



Prof. Marco Aurélio Thompson

+55 (71) 9-9130-5874

**ATENÇÃO:** Este e-book é o complemento de outro e-book nosso sobre ferramentas de varredura portas. A diferença é que no outro as ferramentas (softwares) são para instalar e as ferramentas que vamos apresentar nesse e-book são para uso online, não instalam.

Sendo online você acessa igual a uma página na internet e de qualquer dispositivo que abra uma página na internet como computador de mesa ou portátil, tablet, smartphone e até SmartTV se você tiver como digitar.

Um conhecimento importante que você precisa ter antes de usar as ferramentas de varredura de portas é justamente o conhecimento a respeito das portas. A informação sobre portas a seguir é a mesma nos dois e-books. Se você já leu e aprendeu sobre portas no e-book anterior, então pode ir direto para a página 16 que é lá que começam as ferramentas de varredura de portas online.



# introdução

Se você teve algum interesse neste e-book podemos supor que você é — ou quer ser — hacker ou profissional de segurança da informação. Não importa, pois, o e-book atende a todos.

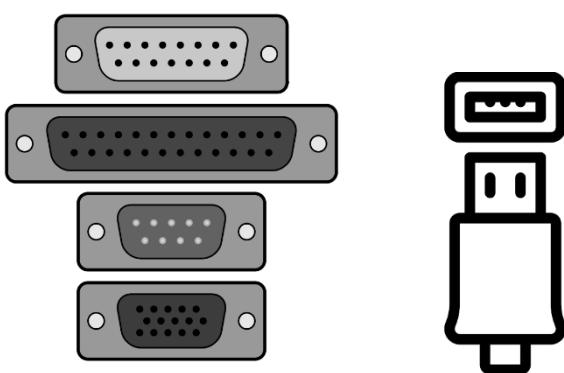
O que é mais importante antes de prosseguirmos é você responder para si mesmo(a) o que você sabe sobre portas do tipo TCP e UDP. Se a resposta for “nada”, então leia esta introdução, mas se você considera que entende o suficiente de portas TCP e UDP, basta seguir para a página em que começamos a apresentar as 10 ferramentas de varredura de portas que prometemos para este e-book.

As páginas a seguir foram escritas apenas para quem precisa saber mais sobre portas antes de usar as ferramentas de varredura.

## O que são portas

As portas são usadas como interfaces ou canais de comunicação. É por onde o computador e demais dispositivos realiza a entrada e saída de dados.

O teclado e o mouse por exemplo, se comunicam com a CPU através da porta USB ou da porta serial nos modelos mais antigos. Da mesma forma os modelos antigos de impressora se comunicam através da porta paralela e os modelos mais recentes usam a porta USB, que, não por acaso, se chama Universal Serial Bus, “Porta Serial Universal” em português:



Portas físicas do PC

A porta física é fácil de entender porque você toca, olha, introduz cabos, já as portas lógicas você não vê e pode não ser fácil aceitar que por ali passam milhares de informações.

## TCP e UDP

As portas podem ser do tipo TCP ou UDP. TCP é a sigla para **T**ransmission **C**ontrol **P**rotocol (protocolo de controle de transmissão) e UDP é a sigla para **U**ser **D**atagram **P**rotocol (protocolo de datagrama do usuário). Ambos são protocolos de comunicação.

A principal diferença é que o TCP é mais confiável e possui bits de controle de fluxo e recebimento. O UDP dispensa esses bits de controle; há apenas o envio direto de dados.

O protocolo TCP equivale a um telefone em que você precisa ter certeza de que o outro lado atendeu antes de começar a falar. O protocolo UDP equivale a um alto-falante de loja, em que você apenas fala sem a preocupação de quantos ou quem vai ouvir você falar.

Para saber mais sobre o assunto, acesse:

- TCP - <https://bit.ly/2BNzjLX>
- UDP - <https://bit.ly/3iGFFNO>
- Diferenças entre TCP e UDP – <https://bit.ly/2Z8hCQ3>

## IP (Internet Protocol)

As redes e a internet são provedores de meios para a comunicação. A comunicação para ser estabelecida precisa de quem transmita (transmissor) e quem receba (receptor), às vezes se revezando nesse papel. Entre as formas usadas para identificá-los está o endereço IP e o URL.

O endereço IP existe em duas versões. A mais antiga e mais usada é a IPv4 (IP versão 4) e a mais recente é a IPv6 (IP versão 6). Neste e-book usaremos a IPv4, um endereço

formado por quatro segmentos de 8 bits (32 bits no total) que vai de 0.0.0.0 a 255.255.255.255, mas você também vai poder usar as ferramentas de varredura com o IPv6, se souber usar.

Com o IPv4, apesar de existir a possibilidade de gerarmos  $2^{32}$  (4.294.967.296) de endereços (mais de 4 bilhões), nem todos estes endereços estão disponíveis ou são usados.

## IP ESTÁTICO x IP DINÂMICO

A função do IP é permitir a localização do dispositivo conectado na rede ou na internet e pode ser do tipo fixo ou estático (não muda) ou dinâmico (muda quando o usuário se desliga da rede ou da internet).

Sites têm IPs fixos. Usuários, em sua maioria, têm IPs dinâmicos. Por este motivo a invasão de usuários não é feita por IP, é feita por invasão reversa, assunto que vamos tratar em outro e-book ou no Curso de Hacker Profissionalizante.

## URL

Outra forma de identificar o dispositivo na rede ou na internet é por URL. URL é a sigla para Uniform Resource Locator, “Localizador Padrão de Recursos” em português.

Os endereços dos sites por exemplo, são URLs:

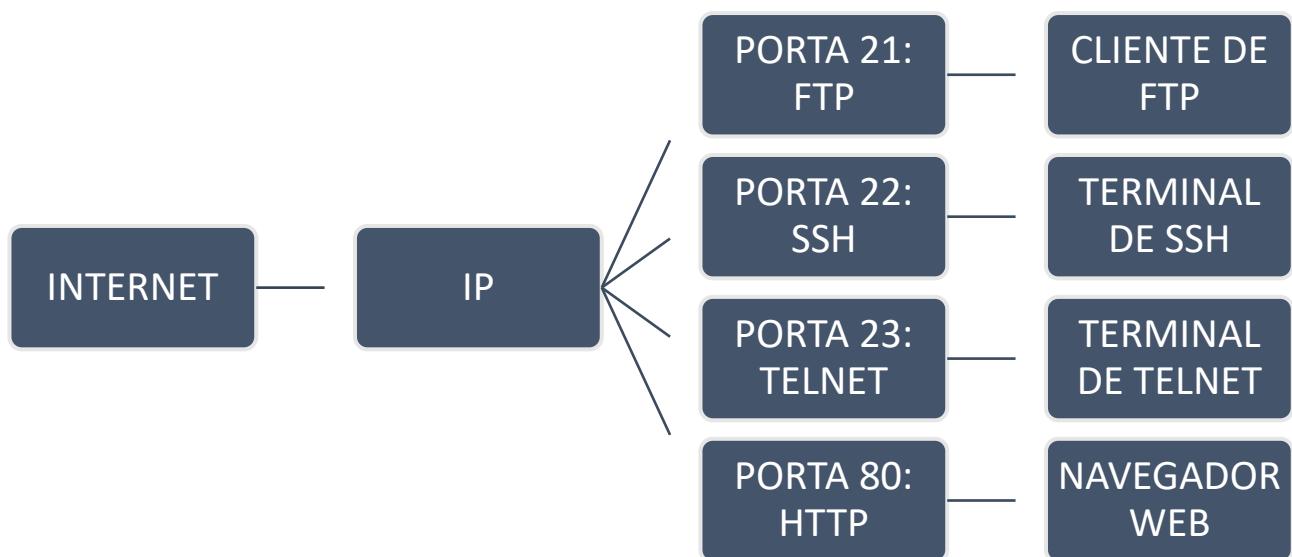
<http://www.escoladehackers.com>

A maioria das ferramentas de varredura aceita tanto endereço IP como Nome de Domínio. Se você quiser testar a segurança de um site investigando quais portas estão ativas e quais serviços estão rodando, poderá informar na ferramenta de varredura tanto o IP do site — se você souber qual é — como o Nome de Domínio, que geralmente é o endereço que a gente digita para acessá-lo.

## Para que servem as portas TCP e UDP

Quando você se conecta à uma rede ou internet você faz isso para transmitir ou receber algum tipo de informação. Acontece que o IP em geral é único e na mesma comunicação poderá chegar ao computador informações provenientes de diversos protocolos: HTTP, HTTPS, SMTP, SSH, TELNET, etc.

As portas servem para fazer esta separação, enviando para cada programa/serviço/cliente/servidor a mensagem certa para ele trabalhar. Se não houvesse esta separação coisas estranhas poderiam ocorrer, como a mensagem do e-mail ir parar no DNS ou o login no SSH aparecer como página Web.



O IP distribui a informação para as portas

As portas servem para o sistema operacional poder encaminhar cada tipo de comunicação ao software ao qual ele pertence. A porta direciona o tráfego entregando a cada serviço aquilo que ele sabe fazer e que espera receber.

## Quantas portas TCP e UDP existem

Existem 65.536 portas numeradas de 0 a 65.535, mas não pense que todas estão em uso, pois a maioria não, como por exemplo a porta 0 e as portas de números elevados. Além disso, como o mesmo número de porta pode ser do tipo TCP ou UDP, a quantidade de portas é ainda maior.

Exemplo: existe a porta 80 TCP e a porta 80 UDP.

Obs.: A porta 80 é dedicada ao protocolo HTTP, ou seja, é pela porta 80 que você recebe os sites da internet.

## Qual serviço funciona em cada porta

A maioria das portas não tem um serviço (software ou função) associado, mas existem portas reservadas para determinados serviços. Você encontra a lista de portas e serviços associados em:

- <https://bit.ly/3iHD6Uy>

Visite também os sites:

- <https://bit.ly/3iQdU5A>
- <https://bit.ly/2BQHalx>

Para fins de pentest e invasão, as portas e serviços mais comuns são:

PORТА	SERVIÇO
20	FTP
21	FTP
22	SSH
23	TELNET
25	SMTP
53	DNS
80	HTTP
110	POP3

Vejamos um exemplo. Quando a ferramenta de varredura revela que o host (dispositivo da rede ou internet) está com a porta 22 aberta, pela tabela acima sabemos ser o serviço

SSH, um protocolo que permite fazer login remoto criptografado. Essa possível falha de segurança e invasão usando exploit foi mostrada no filme Matrix Reloaded (2003), mas antes de sair por aí invadindo o SSH, você precisa pelo menos saber o que é e como usá-lo.

Ao pesquisar por conta própria ou aprender conosco, descobre que o SSH pode ser acessado via terminal Linux ou usando um programa no Windows, como o Putty ([www.putty.org](http://www.putty.org)) por exemplo.

Aprenderá que para fazer login no SSH você precisa saber o nome do usuário e a senha e que sem saber isso, a única forma de acessar o SSH é fazendo a invasão.

Para invadir o SSH usamos técnicas de invasão, como *password cracking*, *password guessing*, *brute force*, *exploitation*, entre outras. Se você não tem a menor ideia do que são essas técnicas de invasão, baixe este outro e-book:



## Para que serve a varredura de portas

A varredura de portas tem por objetivo revelar ao hacker ou ao profissional de segurança da informação o estado das portas e as **vulnerabilidades implícitas**.

Os estados que a porta pode assumir são três, mas existem outros estados formados pela combinação desses, totalizando seus estados:

- aberto (open)
- fechado (closed)
- filtrado (filtered)

Existem dois tipos de vulnerabilidade: a implícita (oculta) e a explícita (escancarada). A vulnerabilidade implícita é típica da varredura de portas, porque a varredura mostra as portas, serviços, versões dos programas e do sistema operacional, mas quem precisa decidir se o alvo está ou não vulnerável é quem está fazendo a inspeção.

A porta 22 aberta por exemplo, só quem sabe o que é SSH e qual ou quais técnicas de invasão servem para atacá-lo é que vai considerá-la uma vulnerabilidade.

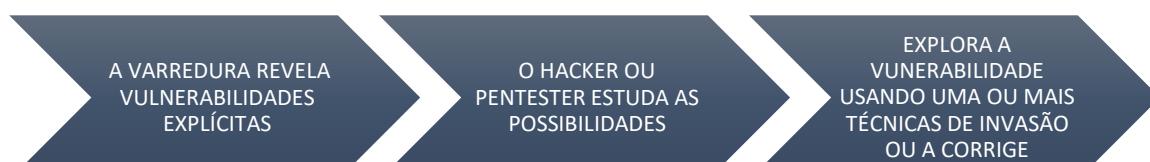
Sem conhecimentos básicos de redes e TCP/IP ou sem nunca ter feito um login autorizado por SSH, esta pessoa vai ver a porta 22 aberta e o SSH rodando e não saberá o que fazer.

A vulnerabilidade explícita é revelada pelas ferramentas de varredura de vulnerabilidades, tema de outro e-book nosso.

Tanto o hacker como o profissional de segurança precisam conhecer as duas formas de varredura, a de portas e a de vulnerabilidades, pois apenas um tipo não revela todas as possíveis falhas de segurança.



Varredura de Portas + Vulnerabilidade Implícita



Varredura de Vulnerabilidades + Vulnerabilidade Explícita

Quando é o invasor que faz a varredura ele explora a falha e invade o sistema ou computador. Se for um profissional de segurança que faz a varredura, ele encontra a falha e corrige. A diferença entre invadir e proteger é quem encontra primeiro a falha de segurança.

A propósito, as varreduras não servem para invasão direta de usuários. A invasão de usuários é feita de forma reversa, de dentro para fora, faça nosso curso de hacker profissionalizante para aprender.

## Como é feita a varredura de portas

A varredura de portas é uma tarefa bem simples que pode ser descrita em 3 passos:

- 1) Informar o IP ou URL a ser inspecionado
- 2) Clicar em Iniciar, Scan ou no botão equivalente
- 3) Aguardar até a exibição do relatório com o resultado

O relatório varia em quantidade e qualidade de acordo com a ferramenta. Opcionalmente podemos fazer a varredura de vários IPs ou faixas de IPs (ranges) e também podemos selecionar portas específicas para varrer.

Usamos o traço para especificar escopo (onde começa e onde termina) e a vírgula para separar valores, exemplo:

- 1-1024 quer dizer: inspeção da porta 1 até 1024.
- 21,23,80 quer dizer: inspeção das portas 21, 23 e 80.
- 192.168.0.1-255 quer dizer: inspeção iniciando no IP 192.168.0.1 até o IP 192.168.0.255.

Para saber mais sobre redes e IPs sugerimos que faça nosso curso profissionalizante de redes.

Quando não informamos as portas que queremos inspecionar o programa de varredura usa as portas configuradas por padrão, geralmente apenas as mais comuns ou as portas baixas, entre 1 e 1.024.

## Por que precisamos conhecer vários programas de varredura de portas

Cada ferramenta de varredura tem um algoritmo que a torna diferente da outra. Algumas ferramentas exibem relatórios muito básicos, outras exibem relatórios mais completos.

O que falta em uma ferramenta às vezes existe na outra. Assim, quando você faz a varredura do mesmo URL ou IP usando diferentes ferramentas de varredura, você consegue mais informações do que uma única ferramenta é capaz de fornecer.

Para testar as ferramentas de varredura usaremos o mesmo IP e URL, ambos autorizados para fins de estudo e testes de invasão. O objetivo é poder comparar os resultados. Use um ou outro, pois o alvo é o mesmo:

IP DOS TESTES	URL DOS TESTES
45.33.32.156	<a href="http://scanme.nmap.org/">http://scanme.nmap.org/</a>

Para testar a máquina que estiver usando, experimente:

IP DA MÁQUINA LOCAL	URL DA MÁQUINA LOCAL
127.0.0.1	localhost

## Programas de varredura de portas gratuitos e online selecionados para este e-book

Essa lista de ferramentas foi selecionada com a ajuda dos participantes do nosso grupo de estudos no WhatsApp :

- 0) TCP Open Port Scanner da Geekflare: <https://gf.dev/port-scanner>
- 1) Port Scanner do site DNS Tools: <http://en.dnstools.ch/port-scan.html>
- 2) Nmap Online Port Scanner: <https://hackertarget.com/nmap-online-port-scanner/>
- 3) IPv6 Online Port Scanner: <http://www.ipv6scanner.com/cgi-bin/main.py>
- 4) Port Forwarding Tester da you get signal: <https://www.yougetsignal.com/tools/open-ports/>
- 5) Online Port Scanner da T1 Shopper: <http://www.t1shopper.com/tools/port-scan/>
- 6) Advanced Port Scanner da Spyse: <https://spyse.com/tools/port-scanner>
- 7) Port Scanner Tool and Associated Codes: <https://www.whatismyip.com/port-scanner/>
- 8) Web Port Scanner: <http://www.webportscanner.com/>
- 9) Nmap Online Port Scanner da NMMapper: <https://www.nmapper.com/st/networkmapper/nmap/online-port-scanning/>
- 10) TCP Port Scanner with Nmap da Pentest-Tools: <https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap>
- 11) Nmap Online: <https://nmap.online/>

A lista está na ordem em que as ferramentas aparecem no e-book. Você percebeu que a lista começa com o número zero e mais adiante vai saber o porquê. Junto da análise de cada ferramenta incluímos o link de acesso para facilitar. Agora é reservar um tempinho porque esse e-book não é para leitura, é para você praticar. Não deixe de assistir também a videoaula.

# 00 - TCP Open Port Scanner da Geekflare



<https://gf.dev/port-scanner>

A ferramenta **TCP Open Port Scanner** da Geekflare é fácil de usar:

- 1) Informe o **IP ou Nome de Domínio** do alvo,
- 2) Marque a caixa de seleção **I am authorized to scan this target and I agree with the Terms of Service** (**Estou autorizado a verificar este alvo e concordo com os Termos de Serviço**) e
- 3) Clique no botão cor de laranja **Check TCP Ports**.

Em segundos você verá o relatório, muito fraco por sinal, apenas o número da porta e o serviço. A decepção com essa ferramenta virá

quando você comparar o relatório dela com o de outras e verá que além de mais completos, incluem a descoberta de mais portas e revelam mais informações.

The screenshot shows a network scanning interface. At the top left is a gear icon. Next to it is the IP address **45.33.32.156**. To the right is a timestamp: **Tested from United States on Aug 15, 2020 3:54 AM**. On the far right is a red **Feedback** button with a speech bubble icon. Below this header is a table with two columns: **Port** and **Service**. The table contains two rows: one for port **22** which is associated with the service **ssh**, and another for port **80** which is associated with the service **http**.

Port	Service
22	ssh
80	http

Não foi sem motivo que atribuímos o número zero a **TCP Open Port Scanner**; ela sequer será contada nesta seleção. Prometemos onze ferramentas no e-book e daremos onze ferramentas boas. A **TCP Open Port Scanner** começa nossa jornada para você entender que existem ferramentas de varredura ruins.

A propósito, em todas as varreduras usaremos o mesmo IP padrão:

**45.33.32.156**

É um IP cuja varredura é autorizada e retorna um bom número de portas e serviços vulneráveis. Ele é ótimo para praticar sem a preocupação de estar se metendo em alguma coisa errada.

Existem alguns critérios que definem uma boa ferramenta de varredura de portas. Na lista a seguir explicamos quais são eles e você pode usá-la como referência para analisar outras ferramentas de varredura além destas dos e-books que venha a conhecer:

- Ter a opção de fazer a varredura de múltiplos IPs e incluir a possibilidade de uso do caractere curinga (wildcard).
- Ter a opção de fazer a varredura selecionando entre porta individual e lista de portas, sequenciais (range), intercaladas e mistas: sequenciais e intercaladas na mesma varredura.
- Ter a opção de selecionar qualquer número de porta, desde a 0 até a 65.535.
- Vir com perfis de varredura pré-configurados.

Em relação aos relatórios das ferramentas, os melhores relatórios apresentam as seguintes características:

- Exibem o número da porta, o estado da porta, se é TCP ou UDP, qual serviço está associado a cada porta e qual a versão de cada serviço.
- Incluem uma breve descrição do serviço identificado em cada porta.
- São exportáveis em vários formatos, como doc/docx, txt, html, pdf, etc.
- Usam um código de cores para identificar portas abertas, fechadas e filtradas.

Estas são as qualidades desejadas nas ferramentas de varredura de portas (valem também para as ferramentas de varredura de vulnerabilidades), mas você vai perceber que nenhuma das ferramentas apresentadas vem com todos esses recursos, mas juntando os resultados de algumas delas você os conseguirá sim.

A propósito, o desenvolvedor da **TCP Open Port Scanner** oferece no mesmo site, no endereço <https://gf.dev/toolbox>, várias ferramentas classificadas por categoria que podem ser úteis em diversas ocasiões. As categorias e ferramentas são as seguintes e inclui ferramentas de varredura de vulnerabilidades:

#### ❖ SEO

- Broken Link Checker
  - Check if your web page contains internal or external broken links

#### ❖ DNS

- DNS Record Lookup
  - DNS lookup for A, TXT, MX, SPF and NS records
- IPv6 Test
  - Check if your site or IP is accessible over IPV6
- CAA Record Lookup
  - Check CAA record of the domain
- Ping Test
  - Check if your site or IP can respond to ping globally
- Traceroute Test
  - Traceroute your IP or site to find network related issue
- TCP Port Scanner
  - Quickly find out what ports are open on public Internet-facing IP or website
- IP Location
  - Find out where the IP address is located

- What's My IP
  - Quickly find out public Internet IP

## ❖ HOSTING

- Whois Hosting
  - Find out the hosting provider of any site, quickly

## ❖ SECURITY

- HTTP Headers Checker
  - Test the headers are being advertised by your web server or network edge device
- Secure Headers Test
  - Check if your site has secure headers to restrict browsers running from avoidable vulnerabilities
- HSTS Test
  - Check if your site is defending from cookie hijacking & protocol downgrade attack
- HPKP Test
  - Check if your site is using HPKP header to defend fraudulent certificate attack
- X-Frame-Options Test
  - Test if your website is defending from Clickjacking attack
- X-XSS-Protection Test
  - Verify if cross-site scripting vulnerability protection is enabled in your site's HTTP response headers
- MIME Sniffing Test

- Verify if cross-site scripting vulnerability protection is enabled in your site's HTTP response headers
- CSP Test
  - Check if your site is defending from code injection, XSS, clickjacking by using CSP header
- Cross-Domain-Policy Test
  - Check if a cross-domain policy is implemented on the website
- Referrer-Policy Test
  - Check what referrer information is being advertised in the HTTP response headers
- Expect-CT Test
  - Instruct browser to validate Certificate Transparency compliance
- Feature-Policy Test
  - Verify if Feature-Policy is enabled on the site
- Secure Cookie Test
  - Test HTTPOnly and Secure flag in Cookie response headers
- Server Signature Test
  - Check if the site is leaking version information through Server or X-Powered-By header
- SPF Record Lookup
  - SPF Record Check
- TLS 1.3 Test
  - Test supported TLS version on the site
- TLS Scanner

- Check the supported protocol, server preferences, certificate details, common vulnerabilities and more
- DNSSEC Test
  - Check if DNS Security Extensions is enabled on your domain
- Blacklist Lookup
  - Getting Google Blacklist warning? Verify if your site is in unsafe resources database
- WordPress Security Scanner
  - Check if your WordPress site has known vulnerabilities
- Mixed Content Checker
  - Check if a web page tries to load resources over HTTP

## ❖ PERFORMANCE

- HTTP/2 Test
  - Check if HTTP/2 is enabled on your website
- HTTP/3 Test
  - Check if H3/QUIC is enabled on your website
- TTFB Test
  - Check how quickly your server responds to the requests made by the browser
- Website Performance Audit
  - Find out how does your site perform against more than 40 essential metrics
- Capture Screenshot

- Test how does your site render globally

## ❖ OTHER

- Sprint Name Generator
  - Generate sprint name for your development, product management and support work

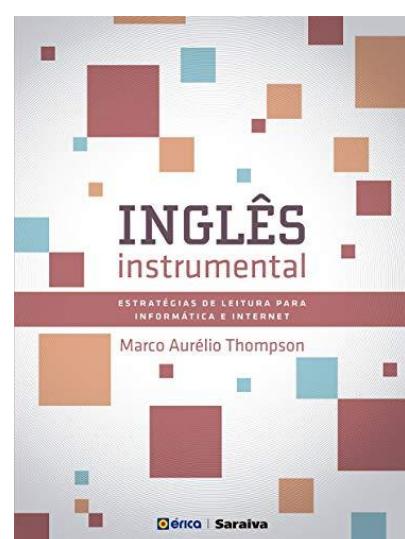
Não fez parte desse e-book testar as outras ferramentas da Geekflare e esperamos que o resultado medíocre da ferramenta de varredura de portas não se repita nas outras.

De qualquer forma vale a pena conhece-las e testá-las também. Se você fizer isso compartilhe conosco os resultados, OK?

Memorize o relatório da **TCP Open Port Scanner** e compare com o relatório da próxima ferramenta online que vamos apresentar, agora sim a número um, de um total de onze até o final do e-book.

Sua jornada está só começando. ☺

As ferramentas hacker e de segurança exibem seus relatórios no idioma inglês. Se você realmente quer levar a sério essa história de ser hacker use parte do seu tempo para aprender inglês nem que seja apenas para leitura. Esse livro que aparece aí do lado é de minha autoria e pode ser uma boa ajuda.



# 01 - Port Scanner do site DNS Tools



<http://en.dnstools.ch/port-scan.html>

A ferramenta **Port Scanner** disponibilizada pelo site DNS Tools segue a simplicidade desse tipo de ferramenta online, bastando informar o IP ou Nome de Domínio, marcar a caixa de seleção do reCAPTCHA para informar ao sistema que você não é um robô e dar início a varredura clicando em Scan.

Comparando o relatório do **Port Scanner** com o anterior é nítida a diferença entre eles, pois dessa vez temos a apresentação do

número da porta, a sinalização do estado por cor, além da descrição do serviço identificado:

Port status on host 45.33.32.156.

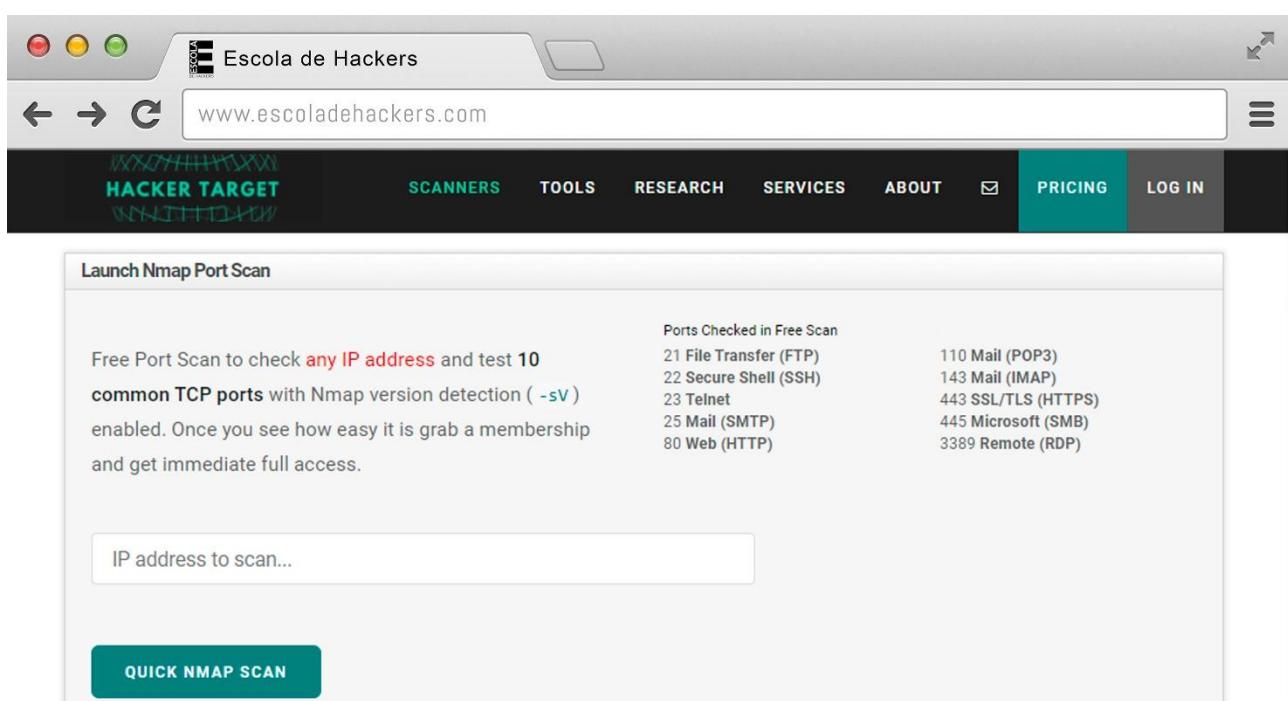
21	"FTP"-Port is closed. <i>Will be used to transfer data through ftp.</i>
22	"SSH"-Port is open. <i>Will be used to connect a Secure Shell.</i>
23	"Telnet"-Port is closed. <i>Will be used for terminal emulation.</i>
25	"SMTP"-Port is closed. <i>Will be used for email delivery (see also port 465).</i>
53	"DNS"-Port is closed. <i>Will be used to resolve domain names into ip addresses.</i>
79	"Finger"-Port is closed. <i>Will be used to show informations about a user.</i>
80	"HTTP"-Port is open. <i>Will be used to communicate with the webserver.</i>
110	"POP3"-Port is closed. <i>Will be used by clients to connect to an email server.</i>

Não esqueça de usar o mesmo IP em todas as ferramentas durante esse processo de imersão que é para você identificar as diferenças que existem nos relatórios entre elas. Depois você usa os IPs e/ou Nomes de Domínio dos alvos que pretende testar a segurança.

Além da varredura de portas experimente também, se já souber como usar, as ferramentas da barra lateral esquerda:

- My IP
- Traceroute
- Ping
- DNS Query
- Reverse IP e
- Dropped Domains.

# 02 - Nmap Online Port Scanner



<https://hackertarget.com/nmap-online-port-scanner/>

A ferramenta **Nmap Online Port Scan** do site Hacker Target é uma versão limitada da poderosa ferramenta de varredura Nmap. Se você ler a descrição verá que a varredura na versão gratuita usa o Nmap com a chave **-sV** (portas abertas e informações de serviço) limitando a varredura nas portas 21, 22, 23, 25, 80, 110, 143, 443, 445 e 3389, cuja descrição dos serviços associados também aparece na tela inicial do site.

O uso é simples. Basta informar IP ou Nome de Domínio e clicar em Quick Nmap Scan para ver o relatório com porta, estado e serviço.

# Escola de Hackers

Desde 2004 formando hackers éticos.

[Todos os cursos](#)



Aulas em vídeo



Suporte a dúvidas



Certificado



Exercícios práticos



Assista onde quiser



COPYRIGHT 2004-2020 ESCOLA DE HACKERS

## FORMAÇÃO COMPLETA EM 12 MESES: DO BÁSICO AO AVANÇADO

Três cursos em um, todos com certificado: dois cursos profissionalizantes e mais a certificação CEH da Escola de Hackers:

- **Curso de Hacker Profissionalizante** (20 cursos em videoaulas, 2 cursos liberados por mês)
- **Certificação Ethical Hacking (CEH)** (20 laboratórios práticos: e-books + videoaulas, 2 laboratórios por mês)
- **Curso Profissionalizante de Redes Locais com e sem Fio** (6 módulos, 1 a cada 2 meses)

**SÃO APENAS 100 VAGAS POR MÊS - GARANTA A SUA EM: [www.escoladehackers.com](http://www.escoladehackers.com)**

Não cobramos mensalidade. Você estuda com APENAS UMA ANUIDADE que pode ser parcelada em até 12x no cartão.

**GRÁTIS:** Acesso aos **12 Volumes da Bíblia Hacker** 2a ed. na Biblioteca Virtual (liberamos 1 volume por mês de permanência no curso).

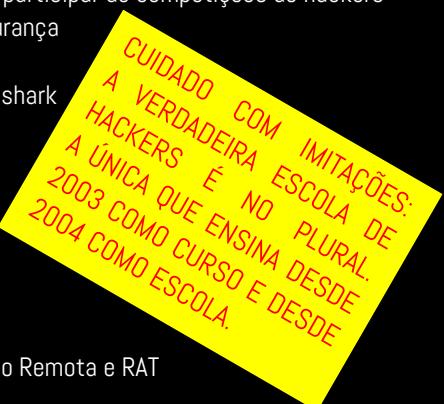
Pare de procurar cursos que prometem e não ensinam o que você quer aprender. A formação da Escola de Hackers tem **GARANTIA DE RESULTADO**. Experimente gratuitamente **ESTUDANDO DE GRAÇA** durante uma semana. Após realizar a matrícula, se você se arrepender, terá mais 7 dias a contar da data do pagamento da anuidade para CANCELAR A MATRÍCULA e RECEBER O DINHEIRO DE VOLTA. Sem burocracia, direto com o **Pag Seguro**.

## Só aqui você encontra:

- **TUDO** o que precisa saber para ser um hacker de verdade, do básico ao avançado.
- **TRÊS CURSOS** em um:
  - ✓ **Curso de Hacker Profissionalizante**
  - ✓ **Curso Profissional de Redes**
  - ✓ **Certificação Ethical Hacker (CEH) da Escola de Hackers**
- Você receberá **dois certificados e uma certificação** (após ser aprovado nas três avaliações).
- Poderá tirar suas dúvidas em qualquer dia ou horário, diretamente com o professor pelo WhatsApp. Ele sempre está à disposição dos alunos, experimente fale com ele agora no **+55 (71) 9-9130-5874** ☎.
- **Aprende com quem mais entende de hacking no Brasil** e um dos mais antigos também, desde 1987.
- Terá acesso aos 12 Volumes d'**A Bíblia Hacker** 2<sup>a</sup> ed. online na plataforma, em nossa Biblioteca Virtual.
- **As aulas são online**, acesse quando e de onde quiser.
- Dá para fazer o curso usando **Windows, Linux ou macOS**. Hackers não podem depender de plataforma.
- Pode procurar: **ninguém ensina tão bem, com tanta qualidade e por tão pouco**.
- Todos os cursos são em videoaula e **os laboratórios são em videoaula** e tem e-book também.

## Estes são alguns assuntos que você vai aprender:

A Técnica de Invasão em 3 Passos  
Bug Bounty: Como iniciar como caçador de recompensas  
Criptografia e Criptoanálise  
CTF (Capture the flag): Como participar de competições de hackers para encontrar falhas de segurança  
CygWin  
Captura de pacotes com Wireshark  
Cracking  
Defacement  
Deep Web  
Exploits e Payloads  
Esganografia  
Estudo de Casos  
Ferramentas Hacker  
Ferramentas de Administração Remota e RAT (Remote Access Trojan)  
Fundamentos da Eletrônica para IoT  
Fundamentos de Banco de dados, SQL e SQL Injection  
Fundamentos de Redes e Internet para Hackers  
Firewall  
Google Hacking Avançado  
Hacker Games  
Hardware Hacking e IoT  
Invasão de Redes sem Fio



*CUIDADO COM IMITAÇÕES,  
A VERDADEIRA ESCOLA DE  
HACKERS É NO PLURAL.  
A ÚNICA QUE ENSINA DESDE  
2003 COMO CURSO E DESDE  
2004 COMO ESCOLA.*

Invasão sem Ferramentas  
Invisibilidade na Web  
Invasão de e-Mail e Redes Sociais  
Iniciação Hacker  
Laboratório Hacker com Appliances  
Linux para Invasão  
Metasploit  
O Mínimo que um Hacker precisa saber sobre Direito e Crimes de Informática  
Proteção e Segurança na Internet  
Programação para Hackers com Python  
Programação Web para Hackers com HTML, CSS e JavaScript  
Servidor Linux  
Segurança na Internet  
Segurança da Informação para Hackers  
Scraping (captura de dados em páginas Web)  
Servidor Windows  
TCP/IP, IPv4 e IPv6  
Técnicas de Invasão  
Treinamento das Habilidades Hacker  
Treinamento em Seleção de Alvos  
VPN  
Virtualização com VirtualBox

**TEM AULA NOVA TODA SEMANA DURANTE 1 ANO**

## FORMAÇÃO COMPLETA EM 12 MESES: DO BÁSICO AO AVANÇADO

\* SÃO APENAS 100 VAGAS POR MÊS \* GARANTA A SUA EM: [www.escoladehackers.com](http://www.escoladehackers.com)

Não cobramos mensalidade. Você estuda com **APENAS UMA ANUIDADE** que pode ser parcelada em até 12x no cartão.

# 03 - IPv6 Online Port Scanner

IPv6 Scanner Beta Contact

IPv6 Online Port Scanner

IPv6Scanner is a port scanner that allows you to probe a server for open, closed or filtered ports. You can specify a host name, IPv4 or IPv6 address. The purpose of this tool is to enable the administrators to verify security. Use with the intent to compromise third-party hosts is not allowed. For this reason the number of systems that can be scanned in a period is limited.

Your IP address is 2804:d47:5630:1400:a802

Enter a Host Name, IPv4 or IPv6 Address

Ports: Common server ports

I am authorized to initiate this port scan.

IPv6 Scanner is a personal project of Javier Yáñez

<http://www.ipv6scanner.com/cgi-bin/main.py>

A ferramenta **IPv6 Online Port Scanner** tem uma aparência simples, mas o resultado da varredura é muito bom. Apesar do título, você pode fazer varreduras tanto do IP versão 4 como do IP versão 6. Basta informar o IP ou Nome de Domínio no campo de buscas, marcar a caixa de seleção **I am authorized to initiate this port scan** (**Estou autorizado a iniciar esta varredura de porta**) e clicar em Scan.

O relatório informa porta, estado e o serviço associado. A sinalização por cor ajuda a identificar o estado das portas:

TCP Port	IPV4 State	Service
21	CLOSED	ftp
22	OPEN	ssh

# 04 – Port Forwarding Tester

The screenshot shows a web browser window with the title 'Escola de Hackers' and the URL 'www.escoladehackers.com'. The main content is a tool titled 'Port Forwarding Tester' from 'you get signal'. The interface includes a sidebar with icons for port forwarding, external address, and open port finder. The main area shows the IP address '191.214.16.16' entered into a field. To the right, there's a list of 'common ports' with their respective service names:

common ports
21 FTP
22 SSH
23 TELNET
25 SMTP
53 DNS
80 HTTP
110 POP3
115 SFTP
135 RPC
139 NetBIOS
143 IMAP
194 IRC
443 SSL
445 SMB
1433 MSSQL
3306 MySQL
3389 Remote Desktop
5632 PCAnywhere
5900 VNC
6112 Warcraft III
Scan All Common Ports

At the bottom of the page, the URL 'https://www.yougetsignal.com/tools/open-ports/' is displayed.

A ferramenta **Port Forwarding Tester** da empresa you get signal também sinaliza por cor o estado da porta. O serviço associado a cada porta não aparece no relatório, mas está em uma coluna do lado direito na página inicial do site.

Para usá-la corretamente você informa o IP ou Nome de Domínio no campo de texto e em vez de clicar em **Check** clique em **Scan All Common Ports**. Essa opção aparece no canto direito, no final da lista de portas comuns com seus respectivos serviços.

# 05 - Online Port Scanner

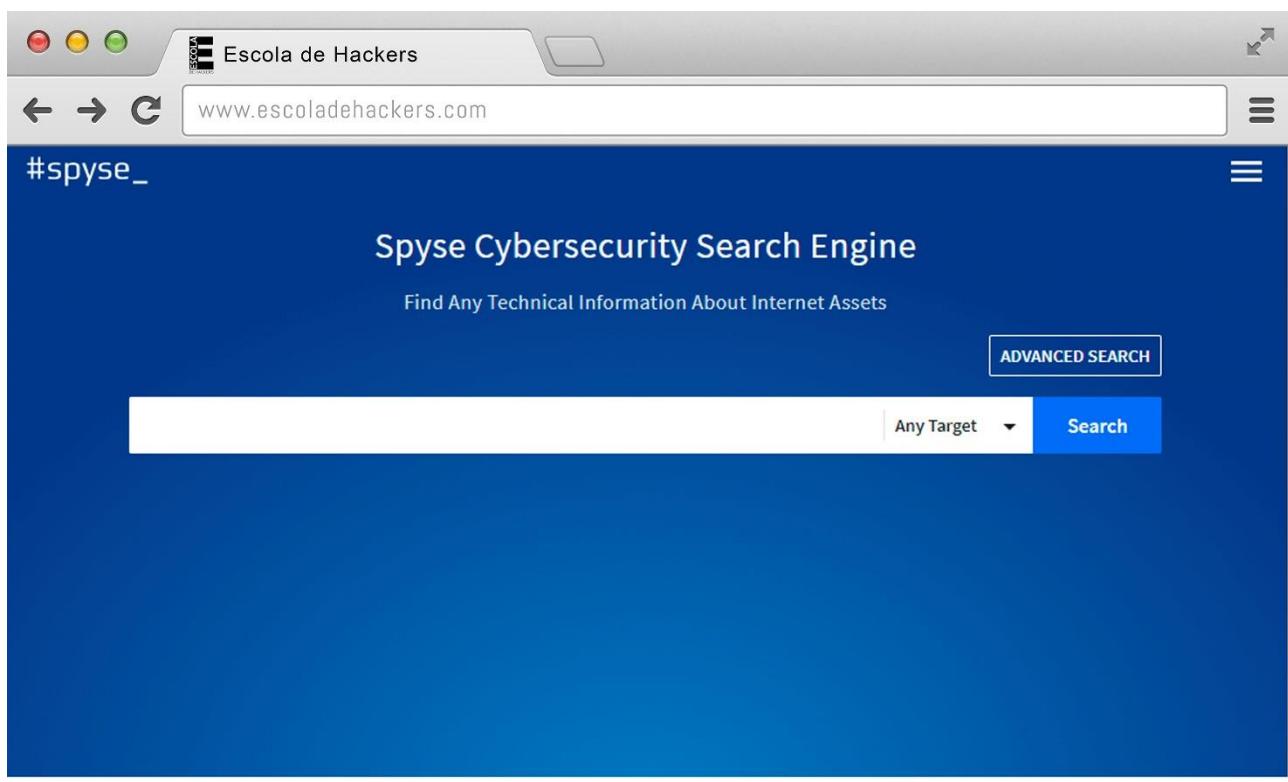
The screenshot shows a web browser window with the following details:

- Title Bar:** Escola de Hackers
- Address Bar:** www.escoladehackers.com
- Page Content:**
  - Header:** TI Shopper, the complete telecom source, Home | Internet Phone Service | T1 Line | T3 Line Pricing | Speed Test | Contact Us | Customers | Tools
  - Section:** BROADBAND SERVICE SEARCH, ZIP code for service > Get Providers
  - Form:** Online Port Scan
    - Text: Use this tool to scan individual ports to determine if the device is listening on that port. Scanning TCP ports only (UDP scanning available soon by free registration). Over 12,791,239,816 ports scanned for our guests.
    - Input: Host name or IPv4 address: 191.214.16.205
    - Input: Scan this list of port numbers: [ ] Scan [?]
    - Input: Scan a range of ports: (less than 500 ports please) Beginning port number [ ] Ending port number [ ]
    - Checkboxes (multiple options selected):
      - FTP/file server open/vulnerable ([port 21](#))
      - SMTP relay vulnerable ([port 25](#))
      - HTTP/web server vulnerable ([port 80](#))
      - Scan for [NETBIOS](#) susceptibility ([port 139](#))
      - Microsoft Remote Desktop vulnerable ([port 3389](#))
      - VPN (PPTP) service open/vulnerable ([port 1723](#))
      - Oracle database service open/vulnerable ([port 1521](#))
      - TELNET service open/vulnerable([port 23](#))
      - POP3/mail server vulnerable ([port 110](#))
      - Scan for Windows file sharing susceptibility ([port 445](#))
      - Scan for firewall remote login ([port 8080](#))
      - VNC Remote Desktop vulnerable ([port 5900](#))
      - Microsoft SQL Server open/vulnerable ([port 1433](#))
      - MySQL database open/vulnerable ([port 3306](#))
    - Buttons: Check All, Uncheck All
- Sidebar:** Creative Cloud, Crie com a Creative Cloud. Aplicativos para fotografia, design, vídeo e Web por R\$ 43,00/mês. Associe-se já

<http://www.t1shopper.com/tools/port-scan>

A Online Port Scan tem como diferencial oferecer uma série de varreduras personalizadas, como por exemplo verificar se o alvo está com o serviço Microsoft Remote Desktop vulnerável. Um detalhe importante é que a(a) porta(s) a ser(em) inspecionada(s) precisa(m) ser informada(s). Para informar uma lista de portas em sequência separe-as por traço e para informar portas intercaladas separe-as por vírgula ou espaço.

# 06 - Advanced Port Scanner da Spyse

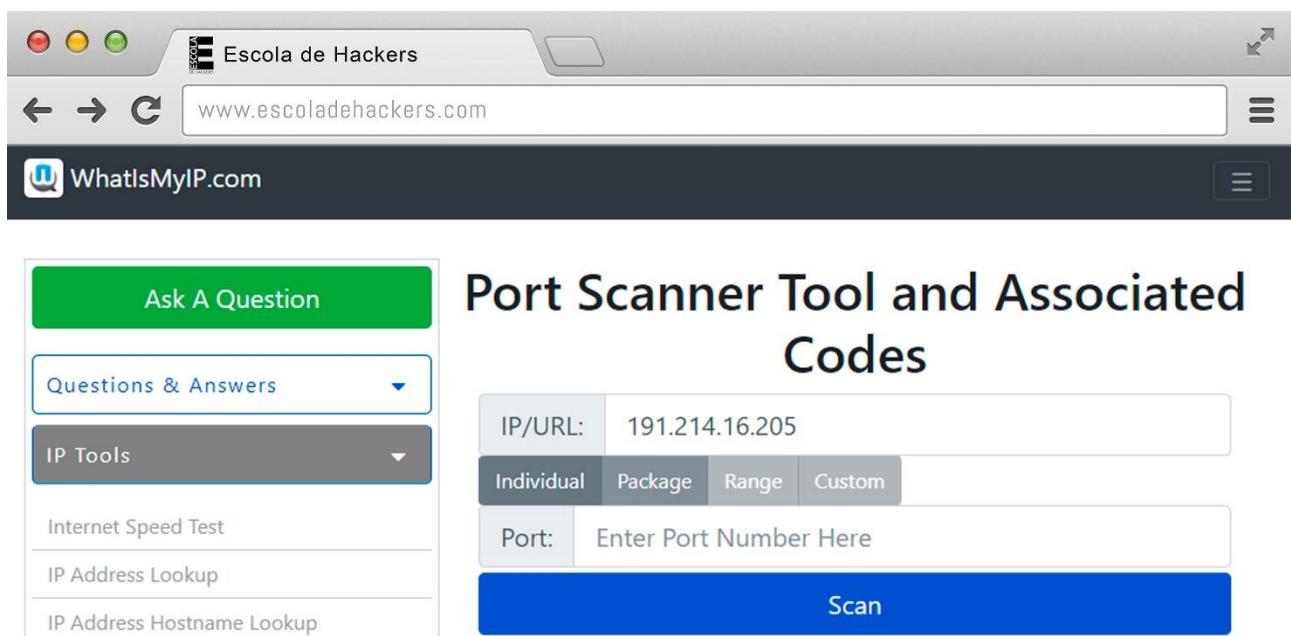


<https://spyse.com>

A ferramenta Advanced Port Scan da Spyse possui uma das interfaces mais simples da nossa coleção, porém ela é um misto de ferramenta de varredura de portas e de vulnerabilidades, ou seja, além do estado das portas o relatório vai informar também se há vulnerabilidades.

Outro diferencial é a exibição no formato dashboard (painel), algo que é mais comum nas ferramentas de varredura de vulnerabilidades, mas como essa é mista está valendo.

# 07 - Port Scanner Tool and Associated Codes



The screenshot shows a web browser window with the title bar "Escola de Hackers" and the URL "www.escoladehackers.com". Below the browser is a dark navigation bar with the "WhatIsMyIP.com" logo. The main content area displays a form titled "Port Scanner Tool and Associated Codes". On the left, there's a sidebar with a green button "Ask A Question" and dropdown menus for "Questions & Answers" and "IP Tools" (which includes "Internet Speed Test", "IP Address Lookup", and "IP Address Hostname Lookup"). The main form has fields for "IP/URL" (containing "191.214.16.205") and "Port" (with placeholder "Enter Port Number Here"). Below these are tabs for "Individual", "Package", "Range", and "Custom", with "Package" being the active tab. A large blue "Scan" button is at the bottom.

<https://www.whatismyip.com/port-scanner>

O Port Scanner Tool da What Is My IP tem como diferencial as opções de varredura por porta única (Individual), pacote (Package), faixa de portas (Range) e personalizada (Custom), sendo estas duas últimas disponíveis apenas na versão paga.

Apesar da aparente limitação, seu ponto forte está na opção Package que permite selecionar um conjunto de portas mais comuns por uso, com as seguintes opções:

- 1) Varredura usando as portas básicas mais comuns (Basic)
- 2) Varredura usando as portas Web mais comuns (Web)

- 3) Varredura usando as portas de jogos mais comuns (Games)
- 4) Varredura usando as portas mais comuns usadas por códigos maliciosos (Malicious)

A seguir listamos que portas são estas para que você também possa usar as mesmas portas em outras ferramentas de varredura:

#### ❖ Basic

- 21 - File Transfer Protocol (FTP)
- 22 - Secure File Transfer Protocol (SFTP)
- 25 - Simple Mail Transfer Protocol (SMTP)
- 26 - [threat] W32.Netsky
- 80 - Hypertext Transfer Protocol (HTTP)
- 110 - Post Office Protocol v3 (POP3)
- 143 - Internet Message Access Protocol (IMAP)
- 443 - Hypertext Transfer Protocol over TLS/SSL (HTTPS)
- 587 - Simple Mail Transfer Protocol (Often more secure than port 25)
- 993 - Internet Message Access Protocol over TLS/SSL (IMAPS)
- 995 - Post Office Protocol 3 over TLS/SSL (POP3S)
- 2525 - Remote Access Trojans
- 3306 - MySQL database system

#### ❖ Web

- 23 - Telnet protocol - unencrypted text communications
- 43 - WHOIS protocol
- 53 - Domain Name System (DNS)
- 67 - Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) server
- 68 - Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) client

- 69 - Trivial File Transfer Protocol (TFTP)
- 123 - Network Time Protocol (NTP) - time synchronization
- 137 - NetBIOS Name Service
- 138 - NetBIOS Datagram Service
- 139 - NetBIOS Session Service
- 161 - Simple Network Management Protocol (SNMP)
- 162 - Simple Network Management Protocol Trap (SNMPTRAP)
- 389 - Lightweight Directory Access Protocol (LDAP)
- 636 - Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
- 989 - FTPS Protocol (data), FTP over TLS/SSL
- 990 - FTPS Protocol (control), FTP over TLS/SSL
- 2077 - TrelliSoft Agent
- 2078 - TrelliSoft Server
- 2082 - cPanel default
- 2083 - Secure RADIUS Service (radsec)
- 2086 - WebHost Manager default
- 2087 - WebHost Manager default SSL
- 2095 - cPanel web mail default
- 2096 - cPanel SSL web mail default

## ❖ Games

- 1725 - Valve Steam Client
- 2302 - ArmA and Halo: Combat Evolved
- 3074 - Xbox Live and/or Games for Windows Live
- 3724 - World of Warcraft
- 6112 - Blizzard's Battle.net Gaming Service
- 6500 - Gamespy Arcade, Unreal, Tony Hawk, Warhammer, Starwars, Civilization III and IV, BoKS Master, Command & Conquer

- 12035 - Linden Lab viewer to sim on SecondLife
- 12036 - Second Life
- 14567 - Battlefield 1942
- 25565 - Minecraft Dedicated Server
- 27015 - GoldSrc and Source engine dedicated server port
- 28960 - Call of Duty

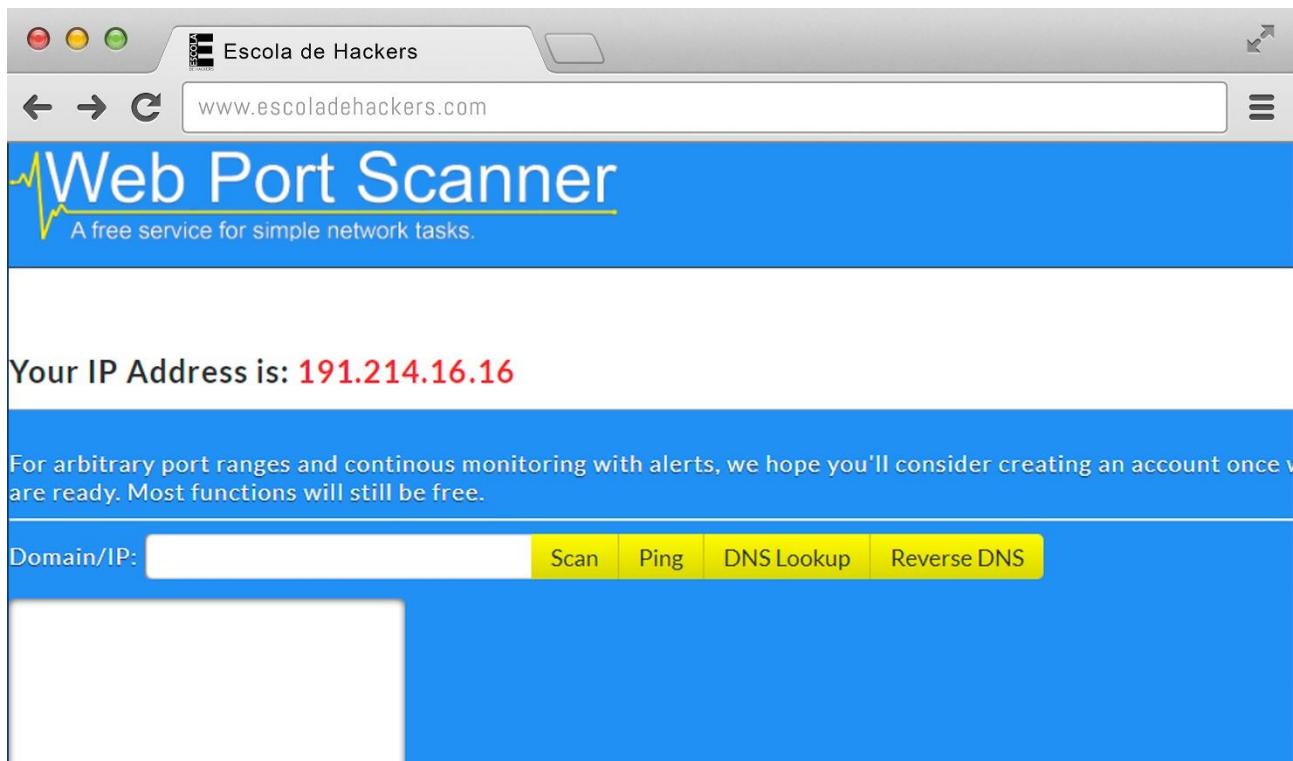
### ❖ Malicious

- 1080 - W32.Beagle, WinHole, W32.HLLW.Deadhat, and several others like keyloggers, remote peekers, etc.
- 2745 - Bagle Virus Backdoor
- 3127 - W32.Mockbot, W32.Solame, and others
- 4444 - Metasploit's default listener port
- 5554 - W32.Dabber and W32.Sasser
- 8866 - W32.Beagle
- 9898 - CrashCool and W32.Dabber
- 9988 - Used by many trojans and worms
- 12345 - Used by many trojans and worms
- 27374 - Used by many trojans, remote access hacks, worms, etc.
- 31337 - Used by many trojans and worms

Além do Port Scanner o site oferece outras ferramentas úteis, como: Internet Speed Test, IP Address Lookup, IP Address Hostname Lookup, IP WHOIS Lookup, Server Headers Check, Email Header Analyzer, Blacklist Check, User Agent Info, DNS Lookup, Reverse DNS Lookup e Proxy Check, disponíveis no menu do lado direito no site.

Se você não souber do que se trata vale a pena usar um pouco do seu tempo para estudar e aumentar ainda mais o seu potencial de invasão.

# 08 - Web Port Scanner



<http://www.webportscanner.com>

A ferramenta Web Port Scan é simples, porém eficiente. A partir do mesmo IP ou Nome de Domínio informado no campo de texto você poderá optar entre Scan, Ping, DNS Lookup e Reverse DNS.

O relatório aparece em uma coluna do lado esquerdo, identificando com cores o estado das portas. O que não nos agradou foi a falta de ordenação do resultado da varredura, fazendo com que a porta 5.060 por exemplo, apareça antes da porta 22.

Fora isso o relatório é decente e conciso, informando o número da porta, o serviço associado entre parênteses e o estado da porta identificado também por cor.



Marco Aurélio Thompson

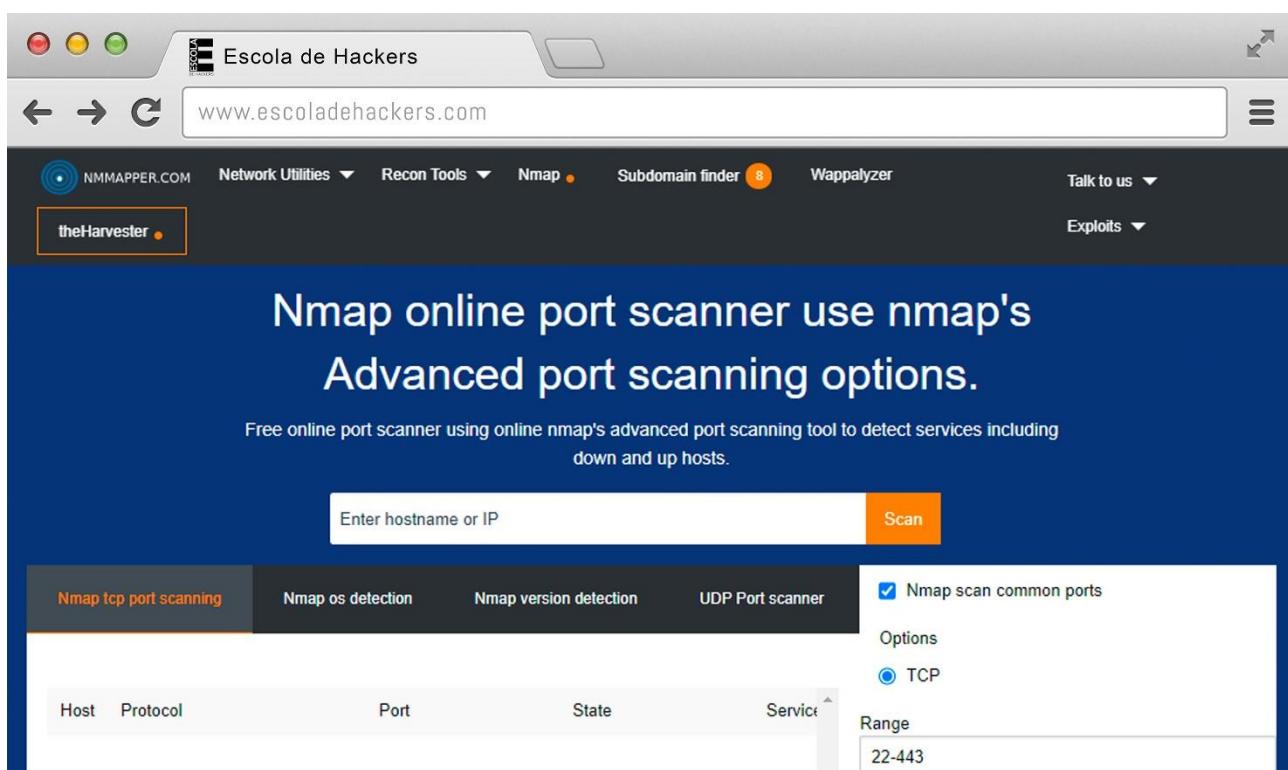
GRÁTIS: Acesso aos 12 Volumes da Bíblia Hacker online para todos os estudantes matriculados na Escola de Hackers. Você terá acesso a um volume para cada mês que permanecer na plataforma.

# A Bíblia **HACKER**



[www.abibliahacker.com](http://www.abibliahacker.com)

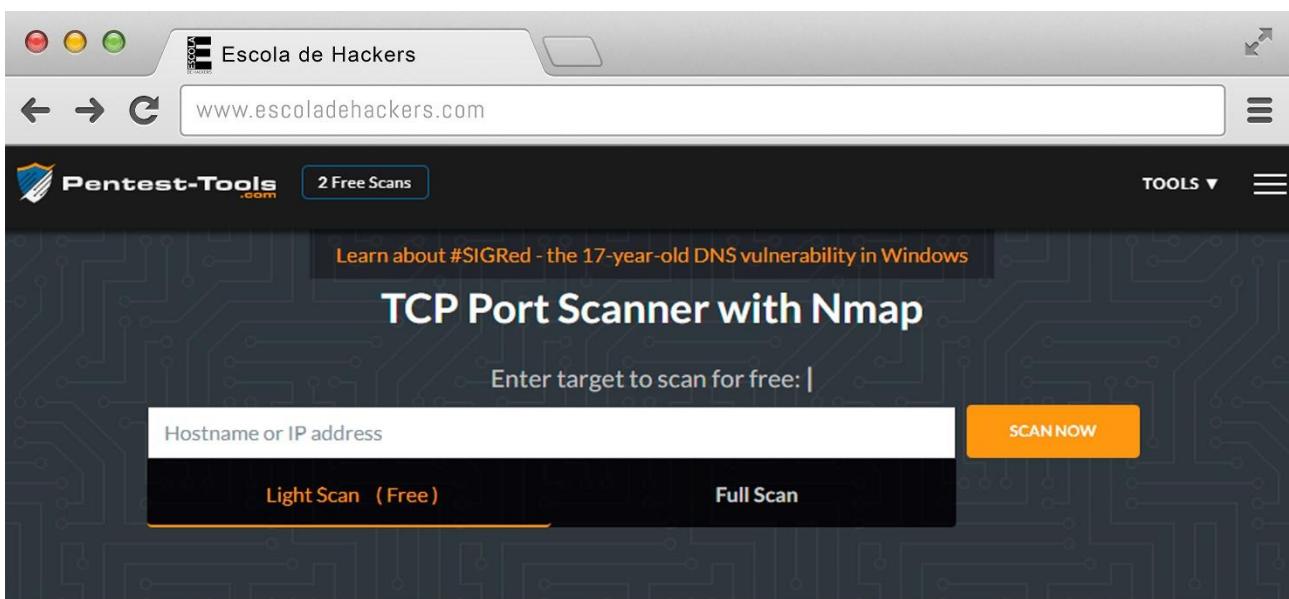
# 09 - Nmap Online Port Scanner da NMMapper



<https://www.nmmapper.com/st/networkmapper/nmap/online-port-scanning>

Mais uma ferramenta que se propõe a ser um Nmap online, algo que só nos beneficia, mas sem ignorar o fato de que o Nmap com todo o seu potencial você só encontra em seu computador ou acessado diretamente de forma remota. A ferramenta da NMMapper permite com o mesmo IP fazer varredura TCP e UDP, identificação do sistema operacional (OS Detection) e da versão dos serviços do alvo (Nmap version detection). Se não quiser usar as portas mais comuns, informe outras em Range.

# 10 - TCP Port Scanner with Nmap da Pentest-Tools (TCP e UDP)



## About this Online Port Scanner

Detects open TCP ports, running services (including their versions) and does OS fingerprinting on a target IP address or hostname



<https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap>

A ferramenta **TCP Port Scanner with Nmap** da Pentest-Tools é outra que se propõe a oferecer o Nmap online e desde já você precisa saber que ela só permite a realização de duas varreduras gratuitas (2 Free Scan). Outra informação importante é que ela disponibiliza dois tipos de varredura, a Light Scan (Free) e a Full Scan, que é paga.

As duas varreduras incluem:

- As 100 portas mais comuns
- A detecção da versão do serviço que estiver em uso no alvo

A varredura do tipo Full Scan inclui:

- A varredura de todas as 65.535 portas
- A detecção do sistema operacional do alvo e
- Traceroute

Não vemos uma real vantagem no uso da opção Full Scan, porque fazer a varredura de 65.535 portas, detectar o sistema operacional do alvo e o Traceroute, são recursos encontrados em outras ferramentas. E apesar de o relatório desse desenvolvedor incluir informações importantes, como a versão do serviço identificado no alvo, a quantidade de portas encontradas decepciona quando comparamos com o relatório de outras ferramentas.

Como é costume acontecer o site não tem só o port scan. No link abaixo você encontra várias outras ferramentas de varredura:

<https://pentest-tools.com/alltools>

Em sua maioria são de varredura de vulnerabilidade como a SQL Injection Scanner, Website Scanner, XSS Scanner, WordPress Scanner, além de HTTP Request Logger, ICMP Ping, entre outras.

Infelizmente devido a limitação de apenas duas varreduras grátis talvez seja melhor pensar em outras ferramentas para a mesma finalidade ou encontrar um *hack* que permita usar o serviço mais de duas vezes ☺.

# 11 - Nmap Online

The screenshot shows a web browser window for 'Escola de Hackers' at [www.escoladehackers.com](http://www.escoladehackers.com). The page features a dark header with the 'NMAP' logo and links for ABOUT, NMAP COMMANDS, PRICING, CONTACTS, LOGIN, and SIGN IN. Below the header, there's a message to 'Authenticate your profile to see activity'. The main content area is titled 'Nmap Online' and contains a form with fields for 'Target' (dropdown), 'Domain or IP' (text input), and 'Scan Method' (dropdown set to 'Fast Scan (nmap -F ...)'). A large green button labeled 'SCAN HOST' is on the right. A note below the form says 'Some firewalls blocks Nmap scans. For get true positive results add nmap.online IP addresses (208.76.253.234-208.76.253.237) to the whitelist'. On the left, there's a section about the 'Fast Scan' method and an 'nmap command' example:

```

Starting Nmap 7.80 ( https://nmap.org ) at year-mo-day hh:mm
Nmap scan report for site.domain (xx.xx.xx.xx)
Host is up (0.01s latency).
Not shown: 80 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3

```

<https://nmap.online>

Deixamos para o final a versão do Nmap online que mais recursos oferece e, como já era de se esperar, alguns recursos só estão disponíveis apenas na versão paga, mas isso não será um problema para você que está lendo este e-book. Aguarde e confirme.

Na primeira caixa de seleção você tem as opções Target (alvo) e \$ IP Range, sendo que este cifrão indica que a varredura de listas de IPs é um serviço pago. Essa limitação não é importante porque se houver necessidade de fazer a varredura usando listas de IPs podemos fazer isso com o Nmap instalado ou acessado remotamente em sua versão completa.

O campo seguinte é para você informar o IP ou Nome de Domínio, mas o que torna essa ferramenta especial são os perfis de varredura disponíveis no terceiro campo. Um total de dez, sendo quatro gratuitos e seis pagos identificados pelo cifrão inicial:

- 1) Fast Scan (nmap -F ...)
- 2) Port scan (nmap -sV -p 21,22,25,80,110,143,443,445 ...)
- 3) Scan OS information and Traceroute (nmap -A ...)
- 4) OS Detection (nmap -O ...)
- 5) **\$** Firewall Detection (nmap -sA ...)
- 6) **\$** Scan the top 5 ports (nmap --top-ports 5 ...)
- 7) **\$** Scan the top 20 ports (nmap --top-ports 20 ...)
- 8) **\$** Scan top TCP ports (nmap --top-ports 20 -sT ...)
- 9) **\$** Scan top UDP ports (nmap --top-ports 20 -sU ...)
- 10) **\$** Detecting malware infections (nmap --top-ports 3 -sV --script=http-malware-host ...)

Acontece que a empresa disponibilizou a linha de comandos usada em cada perfil de teste e você pode copiar e usar a mesma linha no Nmap instalado em seu computador.

Por exemplo, na opção 5 em que o Nmap faz uma varredura de detecção de firewall, basta digitar **nmap -sA** e mais o IP ou Nome de Domínio do alvo no Nmap ou no Zenmap.

Só não esqueça de ignorar os pontinhos após o comando, pois eles representam o IP ou o Nome de Domínio que virá depois.

O relatório apresentado é exatamente o relatório do Nmap, até porque você estará realmente usando o Nmap online, embora não tenha a liberdade para selecionar todo tipo de configuração.

# conclusão

Neste e-book você teve uma introdução às portas TCP e UDP, noções de como se planeja uma invasão a partir da varredura de portas e a apresentação de 11 ferramentas de varredura de portas gratuitas e online para você começar a praticar.

Por falar em praticar, junto a este e-book você encontra videoaulas para ver as ferramentas em funcionamento e receber dicas adicionais.

Apesar de ser um “simples e-book” como dirão alguns, conseguimos reunir bastante informação útil sobre varredura de portas online de forma a permitir que até alguém com pouca ou nenhuma experiência em varredura consiga resultados.

Como você pôde observar, boa parte das ferramentas apresentadas são versões da Nmap com limitações, o que só reforça a importância de saber usar o Nmap de forma profissional.

Se você quiser saber mais sobre o assunto e se profissionalizar sugerimos que faça o **Curso de Hacker Profissionalizante da Escola de Hackers**.

Agora eu fico por aqui, mas nos vemos no próximo e-book ou videoaula. Até lá!



Prof. Marco Aurélio Thompson

+55 (71) 9-9130-5874

**10**

FERRAMENTAS  
DE VARREDURA DE PORTAS  
PORT SCANNING  
FÁCEIS DE USAR



**11**

FERRAMENTAS  
DE VARREDURA DE PORTAS  
ONLINE  
FÁCEIS DE USAR



**3**

FORMAS  
DE INVASÃO  
QUE QUALQUER PESSOA  
CONSEGUE FAZER



**9**

PRINCIPAIS  
COMANDOS  
DO NMAP



**21**

MANEIRAS  
DE USAR AS  
MÁQUINAS  
VIRTUAIS



**13**

COMANDOS  
DE TERMINAL  
DO WINDOWS



**5**

DISTRIBUIÇÕES  
LINUX PARA  
HACKERS



**14**

COMANDOS  
DE TERMINAL  
DO LINUX



**31**

SITES QUE TODO  
**HACKER**  
PRECISA CONHECER



**17**

DICAS PARA NÃO  
SER VÍTIMA  
DE HACKERS



**6**

SITES QUE VOCÊ  
PODE INVADIR  
PARA PRATICAR



**3**

MELHORES FERRAMENTAS  
DE VARREDURA  
DE VULNERABILIDADES



**7**

TÉCNICAS DO  
**MR. ROBOT**  
EXPLICADAS



**18**

FERRAMENTAS  
**HACKER**  
QUE FUNCIONAM  
ONLINE



**5**

LIVROS  
**HACKER**  
RESUMIDOS



**4**

JOGOS HACKER  
PARA VOCÊ  
APRENDER  
INVASÃO

