

## Forum:[Hack Forums](#)

Thread: [Comprehensive nMap Guide](#)

**Cyph Jr** - December 14, 2014, 4:20 pm

Do I already have nMap installed?

The first step toward obtaining Nmap is to check whether you already have it. Many free operating system distributions (including most Linux and BSD systems) come with Nmap packages, although they may not be installed by default.

PHP Code

```
<?php
```

```
$ nmap --version
```

Nmap version 4.76 ( <http://nmap.org> )

How do I install nMap?

Nmap.Org is the official source for downloading Nmap source code and binaries for Nmap and Zenmap. Source code is distributed in bzip2 and gzip compressed tar files, and binaries are available for Linux (RPM format), Windows (NSIS executable installer) and Mac OS X (.dmg disk image). Find all of this at <http://nmap.org/download.html>.

What is nMap?

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network.

Discover IP's in a subnet

This is one of the simplest uses of nmap. This command is commonly refereed to as a "ping scan", and tells nmap to send an icmp echo request, TCP SYN to port 443, TCP ACK to port 80 and icmp timestamp request to all hosts in the specified subnet. It can be done by

PHP Code

```
<?php
```

```
$ nmap -sP 192.168.0.0/24
```

Starting Nmap 5.21 ( <http://nmap.org> ) at 2013-02-24 09:37 MST

Nmap scan report for 192.168.0.1

Host is up (0.0010s latency).

Nmap scan report for 192.168.0.95

Host is up (0.0031s latency).

Nmap scan report for 192.168.0.110

Host is up (0.0018s latency).

Discover the Operating System

With the -O option nmap will try to guess the targets operating system. This is accomplished by utilizing information that nmap is already getting through the TCP SYN port scan. This is usually a best guess but can actually be fairly accurate. It can be done by

#### PHP Code

```
<?php
```

```
$ nmap -O 192.168.0.164
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2013-02-24 09:49 MST
```

```
Nmap scan report for 192.168.0.164
```

```
Host is up (0.00032s latency).
```

```
Not shown: 996 closed ports
```

```
PORT STATE SERVICE
```

```
88/tcp open kerberos-sec
```

```
139/tcp open netbios-ssn
```

```
445/tcp open microsoft-ds
```

```
631/tcp open ipp
```

```
MAC Address: 00:00:00:00:00:00 (Unknown)
```

```
Device type: general purpose
```

```
Running: Windows 7
```

```
Network Distance: 1 hop
```

```
Scan for open ports
```

This scan is the default scan for nmap and can take some time to generate. With this scan nmap will attempt a TCP SYN connection to 1000 of the most common ports as well as an icmp echo request to determine if a host is up. It can be done by executing the following command

#### PHP Code

```
<?php
```

```
$ nmap 192.168.0.0/24
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2013-02-24 09:23 MST
```

```
Nmap scan report for 192.168.0.1
```

```
Host is up (0.0043s latency).
```

```
Not shown: 998 closed ports
```

```
PORT STATE SERVICE
```

```
80/tcp open http
```

```
443/tcp open https
```

```
UDP Scan and TCP Syn
```

The TCP SYN and UDP scan will take a while to generate but is fairly unobtrusive and stealthy. This command will check about 2000 common tcp and udp ports to see if they are responding. When you use the -Pn flag this tells nmap to skip the ping scan and assume the host is up.

#### PHP Code

```
<?php
```

```
$ nmap -sS -sU -PN 192.168.0.164
```

```
Starting Nmap 5.21 ( http://nmap.org ) at 2013-02-24 13:25 MST
```

```
Nmap scan report for 192.168.0.164
```

```
Host is up (0.00029s latency).
```

```
Not shown: 1494 closed ports, 496 filtered ports
```

```
PORT STATE SERVICE
```

```
88/tcp open kerberos-sec
```

```
139/tcp open netbios-ssn
```

```
445/tcp open microsoft-ds
```

```
631/tcp open ipp
```

```
88/udp open|filtered kerberos-sec
```

```
123/udp open ntp
```

```
137/udp open netbios-ns
```

138/udp open|filtered netbios-dgm  
631/udp open|filtered ipp  
5353/udp open zeroconf  
Fast scan

This scan limits the scan to the most common 100 ports, if you simply want to know some potential hosts with ports open that shouldn't be this is a quick command to use.

PHP Code

<?php

\$ nmap -T4 -F 192.168.0.164

Starting Nmap 6.01 ( <http://nmap.org> ) at 2013-02-24 12:49 MST

Nmap scan report for 192.168.0.164

Host is up (0.00047s latency).

Not shown: 96 closed ports

PORT STATE SERVICE

88/tcp open kerberos-sec

139/tcp open netbios-ssn

445/tcp open microsoft-ds

631/tcp open ipp

In-depth scan

Unlike some of the earlier commands this command is very aggressive and very obtrusive. It will scan every-port and every service that the host you are scanning is running and executing. To execute the following command enter in this

PHP Code

<?php

\$ nmap -T4 -A 192.168.0.0/24

Nmap scan report for 192.168.0.95

Host is up (0.00060s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1 (protocol 2.0)

| ssh-hostkey: 1024 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:6c (DSA)

|\_ 2048 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:6c (RSA)

80/tcp open http nginx 1.1.19

|\_ http-title: 403 Forbidden

|\_ http-methods: No Allow or Public header in OPTIONS response (status code 405)

111/tcp open rpcbind

| rpcinfo:

| program version port/proto service

| 100000 2,3,4 111/tcp rpcbind

| 100000 2,3,4 111/udp rpcbind

| 100003 2,3,4 2049/tcp nfs

| 100003 2,3,4 2049/udp nfs

| 100005 1,2,3 46448/tcp mountd

| 100005 1,2,3 52408/udp mountd

| 100021 1,3,4 35394/udp nlockmgr

| 100021 1,3,4 57150/tcp nlockmgr

| 100024 1 49363/tcp status

| 100024 1 51515/udp status

| 100227 2,3 2049/tcp nfs\_acl

```
_ 100227 2,3 2049/udp nfs_acl
2049/tcp open nfs (nfs V2-4) 2-4 (rpc #100003)
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
TCP connect scan
```

This command is similar to the TCP SYN scan however rather than sending a SYN packet and reviewing the headers it will ask the OS to establish a TCP connection to the 1000 common ports.

PHP Code

```
<?php
```

```
$ nmap -sT 192.168.0.164
Starting Nmap 5.21 ( http://nmap.org ) at 2013-02-24 12:48 MST
Nmap scan report for 192.168.0.164
Host is up (0.0014s latency).
Not shown: 964 closed ports, 32 filtered ports
PORT STATE SERVICE
88/tcp open  kerberos-sec
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
631/tcp open  ipp
UDP scan and TCP SYN scan for all ports
```

This command will specify the full port range from 1 to 65535 nmap will scan to see if the host is listening on all available ports. You can use the port range specification on any scan that performs a port scan.

PHP Code

```
<?php
```

```
$ nmap -sT 192.168.0.164
Starting Nmap 5.21 ( http://nmap.org ) at 2013-02-24 12:48 MST
Nmap scan report for 192.168.0.164
Host is up (0.0014s latency).
Not shown: 964 closed ports, 32 filtered ports
PORT STATE SERVICE
88/tcp open  kerberos-sec
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
631/tcp open  ipp
Verbose
```

By adding verbose to a majority of the commands above you get a better insight into what nmap is doing; for some scans verbosity will provide additional details that the report does not provide.

PHP Code

```
<?php
```

```
$ nmap -T4 -A -v 192.168.0.164
Starting Nmap 6.01 ( http://nmap.org ) at 2013-02-24 12:50 MST
NSE: Loaded 93 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 12:50
Scanning 192.168.0.164 [2 ports]
Completed Ping Scan at 12:50, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:50
```

Completed Parallel DNS resolution of 1 host. at 12:50, 0.01s elapsed  
Initiating Connect Scan at 12:50  
Scanning 192.168.0.164 [1000 ports]  
Discovered open port 139/tcp on 192.168.0.164  
Discovered open port 445/tcp on 192.168.0.164  
Discovered open port 88/tcp on 192.168.0.164  
Discovered open port 631/tcp on 192.168.0.164  
Completed Connect Scan at 12:50, 5.22s elapsed (1000 total ports)  
Initiating Service scan at 12:50  
Scanning 4 services on 192.168.0.164  
Completed Service scan at 12:51, 11.00s elapsed (4 services on 1 host)  
NSE: Script scanning 192.168.0.164.  
Initiating NSE at 12:51  
Completed NSE at 12:51, 12.11s elapsed  
Nmap scan report for 192.168.0.164  
Host is up (0.00026s latency).  
Not shown: 996 closed ports  
PORT STATE SERVICE VERSION  
88/tcp open kerberos-sec Mac OS X kerberos-sec  
139/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)  
445/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)  
631/tcp open ipp CUPS 1.4  
| http-methods: GET HEAD OPTIONS POST PUT  
| Potentially risky methods: PUT  
|\_ See <http://nmap.org/nsedoc/scripts/http-methods.html>  
| http-robots.txt: 1 disallowed entry  
|\_  
Service Info:  
Ening

So that's how you download, install, and use nMap. This is not all the commands nMap is limited to, but the ones I find most useful for you guys to use. If you wish to learn more about nMap, check out nMaps wiki where they have every command possibly executable on their wiki page. If you have any questions or concerns regarding this tutorial, please feel free to leave them below or PM me regarding it.

**Tirus** - December 14, 2014, 5:50 pm

Nice thread Cyph, keep up the good work man.

**Raz3r** - December 14, 2014, 6:08 pm

Very nice guide, explains it well.

~ViagraFalls

**Cyph Jr** - December 14, 2014, 6:17 pm

(Dec 14, 2014 07:08 PM)ViagraFalls Wrote: [\[CITE\]](#) Very nice guide, explains it well.

~ViagraFalls

Thanks for your feedback, is there anything I can add / improve on.

**Raz3r** - December 14, 2014, 6:29 pm

I would keep it like this, the problem with other tuts is that their to long and confusing.  
You made this a 10/10 in my opinion.

~ViagraFalls

**Orchid** - December 14, 2014, 7:10 pm

This was Tirus's guide, why would you post it for him, reputation I suppose.

**Cyph Jr** - December 14, 2014, 7:41 pm

(Dec 14, 2014 08:10 PM)Orchid Wrote: [\[CITE\]](#) This was Tirus's guide, why would you post it for him, reputation I suppose.

Actually this is my guide so I don't know why you're here making up bullshit.

**Cyph Jr** - December 16, 2014, 10:12 pm

Thanks for your feedback everyone, looking for ideas on a next guide.

**Schweppes** - December 16, 2014, 11:30 pm

lol not sure what the point of writing a guide is when NMap has a free guide on their website, and there are already hundreds of books on it and stuff...

**Cyph Jr** - December 17, 2014, 3:59 am

(Dec 17, 2014 12:30 AM)Schweppes Wrote: [\[CITE\]](#) lol not sure what the point of writing a guide is when NMap has a free guide on their website, and there are already hundreds of books on it and stuff...

Not everyone has to the time to be searching up guides and if I feel like giving back to the community I can so if you don't have any thing positive or constructive to say buzz off.

**Im gone brah** - December 18, 2014, 5:38 am

(Dec 17, 2014 04:59 AM)Cyph Jr Wrote: [\[CITE\]](#) Not everyone has to the time to be searching up guides and if I feel like giving back to the community I can so if you don't have any thing positive or constructive to say buzz off.

Quote:Not everyone has to the time to be searching up The NMAP documention is straight forward and 100 times better than this. Not to mention, why would you write something that has been covered a thousand times already?

**Cyph Jr** - December 24, 2014, 7:09 am

Upping this thread so people can see it.

**Opak3** - December 24, 2014, 9:30 am

Good work! Sure is going to help a lot of people over here.