

Forum:[Hack Forums](#)

Thread: [Simple Port Scanner -Python-](#)

Goombis - January 24, 2017, 7:57 pm

Hey Everyone Decided to Release a very easy Port Scanner

```
Code from socket import *
import os
```

```
if os.name == 'nt':
    os.system('cls')
else:
    os.system('clear')
```

```
#it is Very Slow So don't Think it doesn't work
print "Simple Port Scanner"
```

```
if __name__ == '__main__':
    targetserver = raw_input('Enter host to scan: ')
    targetIP = gethostbyname(targetserver)
    print 'Ready to scan Host ', targetIP
```

```
#scan reserved ports
for i in range(1, 1025):
    s = socket(AF_INET, SOCK_STREAM)
```

```
    result = s.connect_ex((targetIP, i))
```

```
    if(result == 0) :
        print 'Port %d: OPEN' % (i,)
    s.close()
```

```
print "Scanning Done" Enjoy ? ?
```

captainspalding - January 24, 2017, 8:25 pm

(Jan 24, 2017 08:57 PM)Hentai-Guru Wrote: [\[CITE\]](#) Hey Everyone Decided to Release a very easy Port Scanner

```
Code from socket import *
import os
```

```
if os.name == 'nt':
    os.system('cls')
else:
    os.system('clear')
```

```
#it is Very Slow So don't Think it doesn't work
print "Simple Port Scanner"
```

```

if __name__ == '__main__':
    targetserver = raw_input('Enter host to scan: ')
    targetIP = gethostbyname(targetserver)
    print 'Ready to scan Host ', targetIP

    #scan reserved ports
    for i in range(1, 1025):
        s = socket(AF_INET, SOCK_STREAM)

        result = s.connect_ex((targetIP, i))

        if(result == 0) :
            print 'Port %d: OPEN' % (i,)
            s.close()

print "Scanning Done" Enjoy ? ?
But who wants beginner scanning script when we haz nmap?

```

Goombis - January 24, 2017, 8:29 pm

(Jan 24, 2017 09:25 PM)captainspalding Wrote: [\[CITE\]](#) But who wants beginner scanning script when we haz nmap?
its more directed to people new to python and away from pre made scripts etc.

null™ - January 24, 2017, 10:45 pm

Nice Gesture!

Would be cool if you could do some explaining or so along with what you've done, granted you have the time, etc.
It'd really help out the beginners.

Nevertheless,
Good Contribution :)

Cheers,

Goombis - January 25, 2017, 11:51 am

(Jan 24, 2017 11:45 PM)The Tyrion Lannister Wrote: [\[CITE\]](#) Nice Gesture!

Would be cool if you could do some explaining or so along with what you've done, granted you have the time, etc.
It'd really help out the beginners.

Nevertheless,
Good Contribution :)

Cheers,im pretty new here myself and trying to get better but that'd make sense and i apologize !
will do that from now on
?

Infamia - January 25, 2017, 1:14 pm

Code from socket import *
check_port = lambda ip, port_start, port_max: [[socket(AF_INET, SOCK_STREAM).connect_ex((ip, port)), port] for port in range(port_start, port_max+1)]

Checked on 127.0.0.1 and Python27, apparently SMB was open because it returned a 0 instead of a 10061; regardless most of your code can be just simplified to one line -- but kudos for trying :)

Goombis - January 26, 2017, 1:18 am

(Jan 25, 2017 02:14 PM)Infamia Wrote: [\[CITE\]](#) Code from socket import *
check_port = lambda ip, port_start, port_max: [[socket(AF_INET, SOCK_STREAM).connect_ex((ip, port)), port] for port in range(port_start, port_max+1)]
Checked on 127.0.0.1 and Python27, apparently SMB was open because it returned a 0 instead of a 10061; regardless most of your code can be just simplified to one line -- but kudos for trying :)well like i said this thread is to help newer people to python :)

aetherbit - January 27, 2017, 3:57 am

How about making it scan a list of known ports first?