

Forum:[Hack Forums](#)

Thread: [how to find target customize ssh port](#)

t0x1c0d3r - May 30, 2019, 3:01 pm

hello guys,

i want connet to target server using ssh on port 22, but owner of target server change ssh default port,
any idea for finding new PORT of ssh service ?

thanks to all <3

tt4000 - May 30, 2019, 3:42 pm

you cant use nmap for port scan?!!!

Octogon - May 30, 2019, 3:44 pm

(May 30, 2019 03:42 PM)tt4000 Wrote: [\[CITE\]](#) you cant use nmap for port scan?!!!
He probably been naughty and keeps getting blocked.

t0x1c0d3r - May 30, 2019, 4:52 pm

(May 30, 2019 03:42 PM)tt4000 Wrote: [\[CITE\]](#) you cant use nmap for port scan?!!!

hi brO,

yeah i'm using nmap but don't shown service PORT ;)

nmap -sV -Pn {IP}

output :

Code	PORT	STATE	SERVICE	VERSION
20/tcp	closed	ftp-data		
21/tcp	open	ftp	Pure-FTPd	
25/tcp	open	smtp	Exim smtpd 4.91	
53/tcp	open	domain	ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)	
80/tcp	open	http-proxy	Squid http proxy	
110/tcp	open	pop3	Dovecot DirectAdmin pop3d	
143/tcp	open	imap	Dovecot imapd	
443/tcp	open	ssl/ssl	Apache httpd (SSL-only mode)	
465/tcp	open	ssl/smtp	Exim smtpd 4.91	
587/tcp	open	smtp	Exim smtpd 4.91	
993/tcp	open	ssl/imap3s?		
995/tcp	open	ssl/pop3s?		
2222/tcp	open	ssl/http	DirectAdmin httpd 1.54.1 (Registered to XXX)	
8888/tcp	open	sun-answerbook?		
35500/tcp	closed	unknown		

any idea ?

tt4000 - May 30, 2019, 6:02 pm

(May 30, 2019 04:52 PM)t0x1c0d3r Wrote: [\[CITE\]](#) hi brO,

yeah i'm using nmap but don't shown service PORT ;)

```
nmap -sV -Pn {IP}
```

output :

Code	PORT	STATE	SERVICE	VERSION
20/tcp	closed	ftp-data		
21/tcp	open	ftp	Pure-FTPd	
25/tcp	open	smtp	Exim smtpd 4.91	
53/tcp	open	domain	ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)	
80/tcp	open	http-proxy	Squid http proxy	
110/tcp	open	pop3	Dovecot DirectAdmin pop3d	
143/tcp	open	imap	Dovecot imapd	
443/tcp	open	ssl/ssl	Apache httpd (SSL-only mode)	
465/tcp	open	ssl/smtp	Exim smtpd 4.91	
587/tcp	open	smtp	Exim smtpd 4.91	
993/tcp	open	ssl/imap		
995/tcp	open	ssl/pop3		
2222/tcp	open	ssl/http	DirectAdmin httpd 1.54.1 (Registered to XXX)	
8888/tcp	open	sun-answerbook		
35500/tcp	closed	unknown		

any idea ?

The number of ports is low. Use the Putty or SSH and test everyone

bo0m - May 30, 2019, 10:54 pm

(May 30, 2019 04:52 PM)t0x1c0d3r Wrote: [CITE](#) hi brO,

yeah i'm using nmap but don't shown service PORT ;)

```
nmap -sV -Pn {IP}
```

output :

Code	PORT	STATE	SERVICE	VERSION
20/tcp	closed	ftp-data		
21/tcp	open	ftp	Pure-FTPd	
25/tcp	open	smtp	Exim smtpd 4.91	
53/tcp	open	domain	ISC BIND 9.8.2rc1 (RedHat Enterprise Linux 6)	
80/tcp	open	http-proxy	Squid http proxy	
110/tcp	open	pop3	Dovecot DirectAdmin pop3d	
143/tcp	open	imap	Dovecot imapd	
443/tcp	open	ssl/ssl	Apache httpd (SSL-only mode)	
465/tcp	open	ssl/smtp	Exim smtpd 4.91	
587/tcp	open	smtp	Exim smtpd 4.91	
993/tcp	open	ssl/imap		
995/tcp	open	ssl/pop3		
2222/tcp	open	ssl/http	DirectAdmin httpd 1.54.1 (Registered to XXX)	
8888/tcp	open	sun-answerbook		
35500/tcp	closed	unknown		

any idea ?

the default scan you're using only tests the most common 1,000 ports.....you will need to do a thorough scan of -p1-65535.....or post the IP for help with it

Dimeblade - *June 16, 2019, 7:16 pm*

Set for more ports to be scanned and grep the result.

godjustice555 - *June 16, 2019, 9:04 pm*

hmm. HF seems to block my reply.

was going to share a simple script to help u do that

too bad

blame HF

a simple pseudo code is

for 1-65535

use netcat -v, and then pass in the target ip and the port from the for loop

and save the port number +output to a file

this will help u grab the banner instead of using putty one by one

alternatively, search for ssh banner grabbing