



# Cybersecurity

## Module 4 Challenge Submission File

### Linux Systems Administration

Make a copy of this document to work in, and then for each step, add the solution commands below the prompt. Save and submit this completed file as your Challenge deliverable.

#### Step 1: Ensure/Double Check Permissions on Sensitive Files

1. Permissions on `/etc/shadow` should allow only `root` read and write access.
  - a. Command to inspect permissions:

```
ls -l etc/shadow
```

```
sysadmin@vm-image-ubuntu-dev-1:~/Desktop$ ls -l etc/shadow
ls: cannot access 'etc/shadow': No such file or directory
sysadmin@vm-image-ubuntu-dev-1:~/Desktop$ ls -l /etc/shadow
-rw----- 1 root shadow 3838 Sep 24 10:04 /etc/shadow
```

- b. Command to set permissions (if needed):

```
sudo chmod 600 /etc/shadow
```

```
sysadmin@vm-image-ubuntu-dev-1:~/Desktop$ sudo chmod 600 /etc/shadow
```

2. Permissions on `/etc/gshadow` should allow only `root` read and write access.
  - a. Command to inspect permissions:

```
ls -l /etc/gshadow
```

```
sysadmin@vm-image-ubuntu-dev-1:~/Desktop$ ls -l /etc/gshadow
-rw----- 1 root shadow 1459 Sep 24 10:09 /etc/gshadow
```

- b. Command to set permissions (if needed):

```
sudo chmod 600 /etc/gshadow
```

```
sysadmin@vm-image-ubuntu-dev-1:~/Desktop$ sudo chmod 600 /etc/gshadow
```

3. Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else read access only.

- a. Command to inspect permissions:

```
ls -l /etc/group
```

```
sysadmin@vm-image-ubuntu-dev-1:~/Desktop$ ls -l /etc/group
-rw-r--r-- 1 root root 1755 Sep 24 10:09 /etc/group
```

- b. Command to set permissions (if needed):

```
sudo chmod 644 /etc/group
```

```
sysadmin@vm-image-ubuntu-dev-1:~/Desktop$ sudo chmod 644 /etc/group
sysadmin@vm-image-ubuntu-dev-1:~/Desktop$ ls -l /etc/group
```

4. Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else read access only.

- a. Command to inspect permissions:

```
ls -l /etc/passwd
```

```
sysadmin@vm-image-ubuntu-dev-1:~/Desktop$ ls -l /etc/passwd
-rw-r--r-- 1 root root 4014 Sep 24 10:04 /etc/passwd
```

- b. Command to set permissions (if needed):

```
sudo chmod 644 /etc/passwd
```

```
sysadmin@vm-image-ubuntu-dev-1:~/Desktop$ sudo chmod 644 /etc/passwd
```

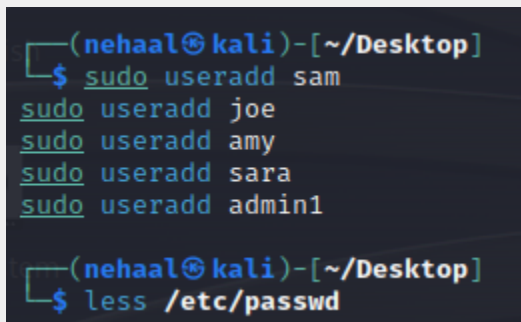
Swapped to VM as virtual vm kept disconnecting me, redid all permissions

## Step 2: Create User Accounts

1. Add user accounts for sam, joe, amy, sara, and admin1 with the useradd command.

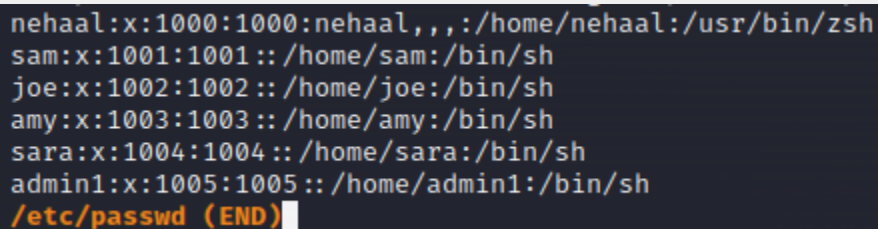
- a. Command to add each user account (include all five users):

```
sudo useradd sam
sudo useradd joe
sudo useradd amy
sudo useradd sara
sudo useradd admin1
```



```
(nehaal@kali)-[~/Desktop]
$ sudo useradd sam
sudo useradd joe
sudo useradd amy
sudo useradd sara
sudo useradd admin1

(nehaal@kali)-[~/Desktop]
$ less /etc/passwd
```

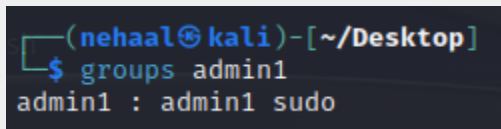


```
nehaal:x:1000:1000:nehaal,,,:/home/nehaal:/usr/bin/zsh
sam:x:1001:1001::/home/sam:/bin/sh
joe:x:1002:1002::/home/joe:/bin/sh
amy:x:1003:1003::/home/amy:/bin/sh
sara:x:1004:1004::/home/sara:/bin/sh
admin1:x:1005:1005::/home/admin1:/bin/sh
/etc/passwd (END)
```

2. Ensure that only the admin1 has general sudo access.

- a. Command to add admin1 to the sudo group:

```
sudo usermod -aG sudo admin1
```



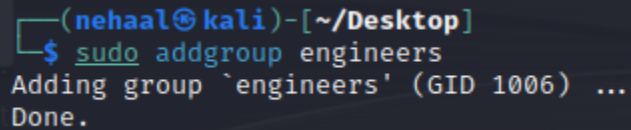
```
(nehaal@kali)-[~/Desktop]
$ groups admin1
admin1 : admin1 sudo
```

### Step 3: Create User Group and Collaborative Folder

1. Add an engineers group to the system.

- a. Command to add group:

```
sudo addgroup engineers
```



```
(nehaal@kali)-[~/Desktop]
$ sudo addgroup engineers
Adding group `engineers' (GID 1006) ...
Done.
```

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.

a. Command to add users to `engineers` group (include all four users):

```
sudo usermod -aG engineers sam
sudo usermod -aG engineers joe
sudo usermod -aG engineers amy
sudo usermod -aG engineers sara
```

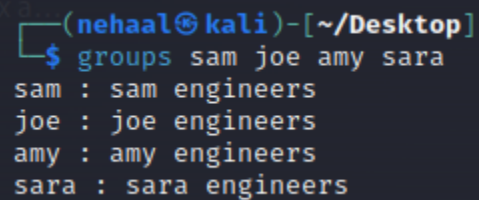


```
(nehaal@kali)-[~/Desktop]
$ sudo usermod -aG engineers sam

(nehaal@kali)-[~/Desktop]
$ sudo usermod -aG engineers joe

(nehaal@kali)-[~/Desktop]
$ sudo usermod -aG engineers amy

(nehaal@kali)-[~/Desktop]
$ sudo usermod -aG engineers sara
```

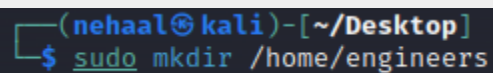


```
(nehaal@kali)-[~/Desktop]
$ groups sam joe amy sara
sam : sam engineers
joe : joe engineers
amy : amy engineers
sara : sara engineers
```

3. Create a shared folder for this group at `/home/engineers`.

a. Command to create the shared folder:

```
sudo mkdir /home/engineers
```



```
(nehaal@kali)-[~/Desktop]
$ sudo mkdir /home/engineers
```

```
(nehaal@kali)-[/home]
$ ls
3-HW-setup-evidence  engineers  movefiles.sh  Roulette_Player_WinLoss_0310
Dealer_Schedules_0310  Lucky_Ducky_Investigations  nehaal
```

4. Change ownership on the new engineers' shared folder to the `engineers` group.

- a. Command to change ownership of engineers' shared folder to `engineers` group:

```
sudo chown :engineers /home/engineers/
```

```
(nehaal@kali)-[/home]
$ sudo chown :engineers //home/engineers/

(nehaal@kali)-[/home]
$ ls -l
total 56
-rwxr-xr-x 1 root root 32689 Jun 9 2022 3-HW-setup-evidence
drwxr-xr-x 2 root root 4096 Sep 27 14:10 Dealer_Schedules_0310
drwxr-xr-x 2 root engineers 4096 Sep 27 21:51 engineers
drwxr-xr-x 3 root root 4096 Sep 27 13:57 Lucky_Ducky_Investigations
-rw-r--r-- 1 root root 923 Sep 27 14:10 movefiles.sh
drwx----- 15 nehaal nehaal 4096 Sep 27 21:49 nehaal
drwxr-xr-x 2 root root 4096 Sep 27 14:10 Roulette_Player_WinLoss_0310
```

## Step 4: Lynis Auditing

1. Command to install Lynis:

`apt install lynis` or `sudo apt install lynis` if permission is needed

```
(nehaal@kali)-[/home]
$ apt install lynis
E: Could not open lock file /var/lib/dpkg/lock-frontent - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?

(nehaal@kali)-[/home]
$ sudo apt install lynis
Reading package lists... Done
Building dependency tree... Done
```

2. Command to view documentation and instructions:

```
man lynis
```

```
File Actions Edit View Help
Lynis(8)                               Unix System Administrator's Manual   Lynis(8)

NAME
    Lynis - System and security auditing tool

SYNOPSIS
    lynis [scan mode] [other options]

DESCRIPTION
    Lynis is a security auditing tool for Linux, macOS, and other systems based on UNIX. The tool checks the system and the software configuration, to see if there is any room for improvement the security defenses. All details are stored in a log file. Findings and other discovered data is stored in a report file. This can be used to compare differences between audits. Lynis can run interactively or as a cronjob. Root permissions (e.g. sudo) are not required, however provide more details during the audit.

    The following system areas may be checked:

        - Boot loader files
        - Configuration files
        - Software packages
        - Directories and files related to logging and auditing

FIRST TIME USAGE
    When running Lynis for the first time, run: lynis audit system

COMMANDS
```

3. Command to run an audit:

```
sudo lynis audit system
```

4. Provide a report from the Lynis output with recommendations for hardening the system.

a. Screenshot of report output:

-[ Lynis 3.0.8 Results ]-

**Warnings (3):**

- ! Found one or more vulnerable packages. [PKGS-7392]  
<https://cisofy.com/lynis/controls/PKGS-7392/>
- ! Couldn't find 2 responsive nameservers [NETW-2705]  
<https://cisofy.com/lynis/controls/NETW-2705/>
- ! iptables module(s) loaded, but no rules active [FIRE-4512]  
<https://cisofy.com/lynis/controls/FIRE-4512/>

**Suggestions (50):**

- \* This release is more than 4 months old. Check the website or GitHub to see if there is an update available [LYNIS]  
<https://cisofy.com/lynis/controls/LYNIS/>
- \* Install libpam-tmpdir to set \$TMP and \$TMPDIR for PAM sessions [DEB-0280]  
<https://cisofy.com/lynis/controls/DEB-0280/>
- \* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]  
<https://cisofy.com/lynis/controls/DEB-0810/>
- \* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]  
<https://cisofy.com/lynis/controls/DEB-0811/>
- \* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [DEB-0831]  
<https://cisofy.com/lynis/controls/DEB-0831/>
- \* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]  
<https://cisofy.com/lynis/controls/DEB-0880/>
- \* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]  
<https://cisofy.com/lynis/controls/BOOT-5122/>
- \* Consider hardening system services [BOOT-5264]  
- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service  
<https://cisofy.com/lynis/controls/BOOT-5264/>
- \* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]  
<https://cisofy.com/lynis/controls/KRNL-5820/>
- \* Configure password hashing rounds in /etc/login.defs [AUTH-9230]  
<https://cisofy.com/lynis/controls/AUTH-9230/>
- \* Install a PAM module for password strength testing like pam\_cracklib or pam\_passwdqc [AUTH-9262]  
<https://cisofy.com/lynis/controls/AUTH-9262/>
- \* When possible set expire dates for all password protected accounts [AUTH-9282]  
<https://cisofy.com/lynis/controls/AUTH-9282/>
- \* Look at the locked accounts and consider removing them [AUTH-9284]  
<https://cisofy.com/lynis/controls/AUTH-9284/>
- \* Configure minimum password age in /etc/login.defs [AUTH-9286]  
<https://cisofy.com/lynis/controls/AUTH-9286/>
- \* Configure maximum password age in /etc/login.defs [AUTH-9286]  
<https://cisofy.com/lynis/controls/AUTH-9286/>
- \* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]  
<https://cisofy.com/lynis/controls/AUTH-9328/>
- \* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]  
<https://cisofy.com/lynis/controls/FILE-6310/>
- \* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]  
<https://cisofy.com/lynis/controls/FILE-6310/>
- \* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]  
<https://cisofy.com/lynis/controls/FILE-6310/>
- \* The database required for 'locate' could not be found. Run 'updatedb' or 'locate.updatedb' to create this file. [FILE-6410]  
<https://cisofy.com/lynis/controls/FILE-6410/>
- \* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]  
<https://cisofy.com/lynis/controls/USB-1000/>
- \* Disable drivers like firewire storage when not used, to prevent unauthorized storage or data theft [STRG-1846]  
<https://cisofy.com/lynis/controls/STRG-1846/>
- \* Check DNS configuration for the dns domain name [NAME-4028]  
<https://cisofy.com/lynis/controls/NAME-4028/>
- \* Install debsums utility for the verification of packages with known good database. [PKGS-7370]  
<https://cisofy.com/lynis/controls/PKGS-7370/>
- \* Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or unattended-upgrades [PKGS-7392]  
<https://cisofy.com/lynis/controls/PKGS-7392/>



- \* Consider using a tool to automatically apply upgrades [PKGS-7420]  
<https://cisofy.com/lynis/controls/PKGS-7420/>
- \* Check your resolv.conf file and fill in a backup nameserver if possible [NETW-2705]  
<https://cisofy.com/lynis/controls/NETW-2705/>
- \* Determine if protocol 'dccp' is really needed on this system [NETW-3200]  
<https://cisofy.com/lynis/controls/NETW-3200/>
- \* Determine if protocol 'sctp' is really needed on this system [NETW-3200]  
<https://cisofy.com/lynis/controls/NETW-3200/>
- \* Determine if protocol 'rds' is really needed on this system [NETW-3200]  
<https://cisofy.com/lynis/controls/NETW-3200/>
- \* Determine if protocol 'tipc' is really needed on this system [NETW-3200]  
<https://cisofy.com/lynis/controls/NETW-3200/>
- \* Install Apache mod\_evasive to guard webserver against DoS/brute force attempts [HTTP-6640]  
<https://cisofy.com/lynis/controls/HTTP-6640/>
- \* Install Apache mod\_security to guard webserver against web application attacks [HTTP-6643]  
<https://cisofy.com/lynis/controls/HTTP-6643/>
- \* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]  
<https://cisofy.com/lynis/controls/LOGG-2154/>
- \* Check what deleted files are still in use and why. [LOGG-2190]  
<https://cisofy.com/lynis/controls/LOGG-2190/>
- \* It is recommended that TFTP be removed, unless there is a specific need for TFTP (such as a boot server) [INSE-8318]  
<https://cisofy.com/lynis/controls/INSE-8318/>
- \* Removing the atftpd package decreases the risk of the accidental (or intentional) activation of tftp services [INSE-8320]  
<https://cisofy.com/lynis/controls/INSE-8320/>
- \* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]  
<https://cisofy.com/lynis/controls/BANN-7126/>
- \* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]  
<https://cisofy.com/lynis/controls/BANN-7130/>
- \* Enable process accounting [ACCT-9622]  
<https://cisofy.com/lynis/controls/ACCT-9622/>
- \* Enable sysstat to collect accounting (disabled) [ACCT-9626]  
<https://cisofy.com/lynis/controls/ACCT-9626/>
- \* Enable auditd to collect audit information [ACCT-9628]  
<https://cisofy.com/lynis/controls/ACCT-9628/>
- \* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]  
<https://cisofy.com/lynis/controls/FINT-4350/>
- \* Determine if automation tools are present for system management [TOOL-5002]  
<https://cisofy.com/lynis/controls/TOOL-5002/>
- \* Consider restricting file permissions [FILE-7524]  
 - Details : See screen output or log file  
 - Solution : Use chmod to change file permissions  
<https://cisofy.com/lynis/controls/FILE-7524/>
- \* Double check the permissions of home directories as some might be not strict enough. [HOME-9304]  
<https://cisofy.com/lynis/controls/HOME-9304/>
- \* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]  
 - Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)  
<https://cisofy.com/lynis/controls/KRNL-6000/>
- \* Harden compilers like restricting access to root user only [HRDN-7222]  
<https://cisofy.com/lynis/controls/HRDN-7222/>
- \* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]  
 - Solution : Install a tool like rkhunter, chkrootkit, OSSEC  
<https://cisofy.com/lynis/controls/HRDN-7230/>

#### Follow-up:

- Show details of a test (lynis show details TEST-ID)
- Check the logfile for all details (less /var/log/lynis.log)
- Read security controls texts (<https://cisofy.com>)
- Use --upload to upload data to central system (Lynis Enterprise users)

---

#### Lynis security scan details:

```
Hardening index : 60 [#####]
Tests performed : 259
Plugins enabled : 1
```



```
Components:
- Firewall [V]
- Malware scanner [X]

Scan mode:
Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

Lynis modules:
- Compliance status [?]
- Security audit [V]
- Vulnerability scan [V]

Files:
- Test and debug information : /var/log/lynis.log
- Report data : /var/log/lynis-report.dat
```

---

**Lynis 3.0.8**

Auditing, system hardening, and compliance for UNIX-based systems  
(Linux, macOS, BSD, and others)

2007-2021, CISOfy - <https://cisofy.com/lynis/>

**Enterprise support available (compliance, plugins, interface and tools)**

## Optional Additional Challenge

1. Command to install chkrootkit:

```
sudo apt install chkrootkit
```

```
(nehaal@kali)-[/home]
$ sudo apt install chkrootkit
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  exim4-base exim4-config exim4-daemon-light gnutls-bin
  libgnutls30 libgsasl18 libgssglue1 libmailutils9 libntlm
  libpython3.11-stdlib libunistring5 mailutils mailutils-common
Suggested packages:
  exim4-doc-html | exim4-doc-info eximon4 spf-tools-perl
  python3.11-doc binfmt-support
The following NEW packages will be installed:
  chkrootkit exim4-base exim4-config exim4-daemon-light
  libunistring5 mailutils mailutils-common
The following packages will be upgraded:
```

```

update-alternatives: using /usr/bin/mail.mailutils to provi
Setting up python3.11-dev (3.11.5-3) ...
Processing triggers for systemd (252.5-2) ...
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for mailcap (3.70+nmu1) ...
Processing triggers for kali-menu (2023.1.7) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for doc-base (0.11.1) ...
Processing 3 added doc-base files ...
Processing triggers for libc-bin (2.36-8) ...

```

2. Command to view documentation and instructions:

man chkrootkit

```

(nehaal@kali)-[/home]
$ man chkrootkit

```

```

chkrootkit(8)                                System Manager's Manual                                chkrootkit(8)
NAME
  chkrootkit - Scan the system for signs of rootkits
SYNOPSIS
  chkrootkit [OPTION]... [TESTNAME]...
DESCRIPTION
  chkrootkit examines the target system for signs that it has been tampered with. Some tools which chkrootkit uses can be found in
  /usr/lib/chkrootkit.
OPTIONS
  Unlike usual programmes, options cannot be 'combined', so you cannot need to write '-q -n' instead of '-qn'
  -q      Enter quiet mode. This suppresses output of tests that find nothing suspicious.
  -x      Enter expert mode. This makes many tests produces additional output showing what they have found.
  -d      Enter debug mode. This shows exactly what chkrootkit is doing at every step (it includes running chkrootkit with 'set -x').
  -e "FILE1[ FILE2 ...]"
          Exclude listed files from the results of some tests. The list should be pace-separated (which will generally require quot-
          ing when run from a shell. You can also specify -e several times). Use this to remove false positives from the result of
          many tests - see /usr/share/doc/chkrootkit/README.FALSE-POSITIVES.
  -s REGEXP
          Similar to -e but only applies to the result of the sniffer test. This test will flag standard network managers like sys-

```

3. Command to run expert mode:

sudo chkrootkit -x

```

-x      Enter expert mode. This makes many tests produces additional output showing what they have found.

```

4. Provide a report from the chrootkit output with recommendations for hardening the system.

a. Screenshot of end of sample output:

WARNING: The following suspicious files and directories were found:

- /usr/lib/ruby/vendor\_ruby/rubygems/optparse/.document
- /usr/lib/ruby/vendor\_ruby/rubygems/ssl\_certs/.document
- /usr/lib/ruby/vendor\_ruby/rubygems/tsort/.document
- /usr/lib/ruby/gems/3.1.0/gems/typeprof-0.21.2/vscode/.vscodeignore
- /usr/lib/ruby/gems/3.1.0/gems/typeprof-0.21.2/vscode/.gitignore
- /usr/lib/ruby/gems/3.1.0/gems/typeprof-0.21.2/vscode/.vscode
- /usr/lib/hashcat/modules/.lock
- /usr/lib/jvm/.java-1.17.0-openjdk-amd64.jinfo
- /usr/lib/llvm-14/build/utils/lit/tests/.coveragerc
- /usr/lib/llvm-14/build/utils/lit/tests/Inputs/reorder/.lit\_test\_times.txt
- /usr/lib/python3/dist-packages/lsassy/resources/.gitkeep
- /usr/lib/python3/dist-packages/numpy/f2py/tests/src/assumed\_shape/.f2py\_f2cmap
- /usr/lib/python3/dist-packages/numpy/f2py/tests/src/f2cmap/.f2py\_f2cmap
- /usr/lib/python3/dist-packages/numpy/core/include/numpy/.doxyfile
- /usr/lib/python3/dist-packages/matplotlib/tests/tinypages/\_static/.gitignore
- /usr/lib/python3/dist-packages/matplotlib/tests/tinypages/.gitignore
- /usr/lib/python3/dist-packages/matplotlib/tests/baseline\_images/.keep
- /usr/lib/python3/dist-packages/matplotlib/backends/web\_backend/.prettierrc
- /usr/lib/python3/dist-packages/matplotlib/backends/web\_backend/.eslintrc.js
- /usr/lib/python3/dist-packages/matplotlib/backends/web\_backend/.prettierignore

Searching for LPD Worm...	not found
Searching for Ramen Worm rootkit...	not found
Searching for Maniac rootkit...	not found
Searching for RK17 rootkit...	not found
Searching for Ducoci rootkit...	not found
Searching for Adore Worm...	not found
Searching for ShitC Worm...	not found
Searching for Omega Worm...	not found
Searching for Sadmin/IIS Worm...	not found
Searching for MonKit...	not found
Searching for Showtee rootkit...	not found
Searching for OpticKit...	not found
Searching for T.R.K...	not found
Searching for Mithra rootkit...	not found
Searching for OBSD rootkit v1...	not tested
Searching for LOC rootkit...	not found
Searching for Romanian rootkit...	not found
Searching for HKRK rootkit...	not found
Searching for Suckit rootkit...	not found
Searching for Volc rootkit...	not found
Searching for Gold2 rootkit...	not found
Searching for TC2 rootkit...	not found
Searching for Anonoying rootkit...	not found
Searching for ZK rootkit...	not found
Searching for ShKit rootkit...	not found
Searching for AjaKit rootkit...	not found
Searching for zaRwT rootkit...	not found
Searching for Madalin rootkit...	not found
Searching for Fu rootkit...	not found
Searching for Kenga3 rootkit...	not found
Searching for ESRK rootkit...	not found
Searching for rootedoor...	not found
Searching for ENYELKM rootkit...	not found
Searching for common ssh-scanners...	not found
Searching for Linux/Ebury 1.4 - Operation Windigo...	not tested
Searching for Linux/Ebury 1.6...	not found
Searching for 64-bit Linux Rootkit...	not found
Searching for 64-bit Linux Rootkit modules...	not found
Searching for Mumblehard...	not found
Searching for Backdoor.Linux.Mokes.a...	not found
Searching for Malicious TinyDNS...	not found
Searching for Linux.Xor.DDoS...	not found
Searching for Linux.Proxy.1.0...	not found
Searching for CrossRAT...	not found
Searching for Hidden Sabre...	not found

