ODU Portal | Writing Assignment Two: Pers | Cybersecurity Clinic Paper | Lab #12 - Log Analysis | Log Analysis | Infosec Learnin

lab.infoseclearning.com/course/THHEVIKBNL/lab/QSZZJKORLW?check_logged_in=1

MyOdu | Main view | Gmail | APA Style Introduc... | Fundamentals of I... | Cybercrime and Di... | New Tab

Old Dominion University - CYSE 300 – Introduction to Cybersecurity

Log Analysis

38 To **switch** to the log directory, **type** the following command. **Press** Enter.

root@kali2: `# cd /var/log`

```
root@kali2:~# cd  /var/log
root@kali2:/var/log#
```

39 To **view** auth.log for forensicuser, **type** the following command and **press** Enter.

root@kali2:/var/log# `cat auth.log | grep forensicuser`

```
root@kali2:/var/log# cat auth.log | grep forensicuser
Oct 30 18:03:13 kali2 useradd[2449]: new group: name=forensicuser, GID=1003
Oct 30 18:03:13 kali2 useradd[2449]: new user: name=forensicuser, UID=1000, GID=1003, home=/home/forensicuser, shell=/bin/sh
Oct 30 18:04:17 kali2 passwd[2455]: pam_unix(passwd:chauthtok): password changed for forensicuser
Oct 30 18:07:57 kali2 sshd[2462]: Accepted password for forensicuser from 192.168.1.175 port 48310 ssh2
Oct 30 18:07:57 kali2 sshd[2462]: pam_unix(sshd:session): session opened for user forensicuser by (uid=0)
Oct 30 18:07:57 kali2 systemd-logind[858]: New session 11 of user forensicuser.
Oct 30 18:07:57 kali2 systemd: pam_unix(systemd-user:session): session opened for user forensicuser by (uid=0)
```

40 To view auth.log for flag6, **type** the following command and **press** Enter.

root@kali2:/var/log# `cat auth.log* | grep flag6`

→ CHALLENGE #5

Get flag6 from the grep output of cat. Type the Flag number displayed.

Submit Skip

← PREVIOUS NEXT →

Topology

Console | Infosec Learning

lab.infoseclearning.com/console/4938755/35

MyOdu | Main view | Gmail | APA Style Introduc... | Fundamentals of I...

NET_SEC_INT-... | Enforce US Keyboard Layout | View Fullscreen | Send Ctrl+Alt+Delete | Reboot

Applicati... | Places | Termi... | Sun 14:41

root@kali2: /var/log

File Edit View Search Terminal Help

```
root@kali2:~# cd /var/log
root@kali2:/var/log# cat auth.log | grep forensicuser
Nov 17 14:15:28 kali2 useradd[2044]: new group: name=forensicuser, GID=1003
Nov 17 14:15:28 kali2 useradd[2044]: new user: name=forensicuser, UID=1000, GID=1003, home=/home/forensicuser, shell=/bin/sh
Nov 17 14:18:17 kali2 useradd[2078]: failed adding user 'forensicuser', data deleted
Nov 17 14:18:50 kali2 passwd[2079]: pam_unix(passwd:chauthtok): password changed for forensicuser
Nov 17 14:21:38 kali2 sshd[2084]: Accepted password for forensicuser from 192.168.1.175 port 37328 ssh2
Nov 17 14:21:38 kali2 sshd[2084]: pam_unix(sshd:session): session opened for user forensicuser by (uid=0)
Nov 17 14:21:38 kali2 systemd: pam_unix(systemd-user:session): session opened for user forensicuser by (uid=0)
Nov 17 14:21:38 kali2 systemd-logind[822]: New session 4 of user forensicuser.
root@kali2:/var/log# cat auth.log* | grep flag6
root@kali2:/var/log# cat auth.log* | flag6
bash: flag6: command not found
root@kali2:/var/log# cat auth.log* |grep flag6
root@kali2:/var/log#
```

Windows Attack Machine