

---

# Cyber Aces

## Module 3 – System Administration

### Bash Scripting – Practical Uses

---

By Tim Medin and Mark Baggett  
Presented by Tim Medin  
v15Q1

This tutorial is licensed for personal use exclusively for students and teachers to prepare for the Cyber Aces competition. You may not use any part of it in any printed or electronic form for other purposes, nor are you allowed to redistribute it without prior written consent from the SANS Institute.

Cyber Aces Module 3 - ©2015 The SANS Institute. Redistribution Prohibited.

1

Welcome to Cyber Aces, Module 3! This module provides an introduction to Bash Scripting. In this module we'll use the knowledge we've gained in some practical examples.

# Course Roadmap

- Introduction
- Linux Review
- Command Substitution
- Variables & Parameters
- Flow Control
- Parsing
- Searching
- ***Practical Uses***
- Conclusions

- Monitoring SSH Logs
- Iterate through a Network
- Modify Files with SED
- Execute Commands Remotely
- Waiting for Input

Course Roadmap

In this section we will go through some practical scripts.

# Know Thy System

- You should know the processes and files executing on your system
- When an abnormal condition arises, you'll recognize the anomaly
- We'll look at some techniques to do this

## Know Thy System

One of the cardinal rules of information security is to "know thy system". This means that you know the processes and files that are executing or stored on your system in a normal state. Then, when an abnormal condition arises, you will recognize the anomaly. Knowing thy system also means that you monitor the logs on your system. In this section, we will look at useful techniques when processing large numbers of log files.

# Failed SSH Logins

- Say on average you may have 200-300 failed logins on your SSH server
  - One day you may have 5000
  - How do you find and count these events?
  - The command `wc` is used to count lines (-l), words (-w), or bytes (-c)
- ```
# cat /var/log/secure | grep -E "Failed password for [a-z]+" | wc -l
```

Cyber Aces Module 3 - ©2015 The SANS Institute. Redistribution Prohibited.

## Failed SSH Logins

One of the command ways to discover attacks and compromise is to look for things that are out of the ordinary. Looking at SSH logs and seeing an increased number of failed login attempts can show that the system is under attack and could potentially lead you to compromised systems if the login attempts are coming from internal systems.

```
$ cat /var/log/secure | grep -E "Failed password for [a-z]+" | wc -l
```

This command will output the file `/var/log/secure` and pipe it into `grep`. The `grep` command will search for "Failed password for " followed by at least 1 alphabet character. The results are piped into `wc` with the `-l` option to count the number of lines of output.

## Failed SSH Logins (2)

- A script to find the users and number of failures

```
#!/bin/sh
file=/var/log/secure
for failed in `cat $file | grep -oE "Failed password for [a-z]+" | cut
-f 4 -d' ' | sort | uniq`
do
    echo $failed `grep "Failed password for $failed " $file | wc -l`
done
```

- Output

```
root 99
tim 23484
tom 0
yori 42
```

### Failed SSH Logins (2)

The script explained:

```
#!/bin/bash
# Above is the standard first line of a script
# The file we will be working on
file=/var/log/secure
# The for loop will operate on each line of output using the variable $fail.
# The output is from:
# - cat the file
# - search the file using a regex search (-E) for "Failed password for "
# followed by alpha characters and only return the match not the full line
# of text (-o)
# - sort the output and get unique lines
# Each time through the loop the $fail variable will contain something
# similar to "Failed password for root"
for failed in `cat $file | grep -oE "Failed password for [a-z]+" | cut -f4 -d'
' | sort | uniq`
do
    # Output search string, then the output of the next command (in backticks)
    # The grep command will search the file again for lines matching the
    # current failed user and return the number of lines matched (wc -l). The
    # space is added after $failed so that users tim won't match tim and timmy
    echo $failed `grep "Failed password for $failed " $file | wc -l`
# all done with the For loop
```

done

# Iterate through IP Addresses

- School Network is 10.10.0.0 through 10.10.6.255
  - Ping each system to see which are up
- ```
#!/bin/sh
for third in {0..6}
do
  for fourth in {1..254}
  do
    ping -c 2 10.10.$third.$fourth > /dev/null &&
    echo 10.10.$third.$fourth is up
  done
done
```

## Iterate through IP Addresses

This example uses nested loops, or one loop inside another loop. The third octet is a number between 0 and 6 and the fourth is between 1 and 254 (Note: we are intentionally skipping 0 and 255).

The ping command will ping the address twice (-c 2) and all output is discarded (redirected to /dev/null). If the ping is successful (has at least 1 successful response) the Echo command will execute and display the IP address that is up.

# Using SED to Modify Config File

- SED is the Stream Editor
  - Similar to AWK, it has its own scripting language
  - SED can modify files in place or create a backup
    - The `-i` option specifies the backup file extension, if blank there is no backup
  - Syntax is: `sed 's/search/replace/g' filename`
    - The "s" means search
    - The "g" means global, can have multiple replacements per file
  - Example to make a web server listen on port 8080
    - Doesn't require that we know the current listening port if we use a Regular Expression
    - Save a backup of the original with the extension `.bak`.
- ```
sed -i'.bak' -E 's/^Listen [0-9]+/Listen 8080/' httpd.conf
```

Cyber Aces Module 3 - ©2015 The SANS Institute. Redistribution Prohibited.

7

## Using SED to Modify a Config File

SED is a handy command used to modify files or output. It is an extremely powerful tool and even has its own scripting language.

One of the nicest features of SED is its ability to modify a file and create a backup. This is a useful safety tool in case the search and replace is typed incorrectly. If you do not want to create a backup you can use `-i` (that's two single quotes not a single double quote) to specify no backup extension.

If we want to make a webserver listen on another port we can use `sed` to find the "Listen" line in the configuration file and replace it. If we use a regular expression we don't need to know the original listening port.

```
$ sed -i'.bak' -E 's/Listen [0-9]+/Listen 8080/' httpd.conf
```

`-i'.bak'` create a backup file with the extension `.bak`

`-E` is the regular expression to use for our search and replace

`S` perform a search

`/^Listen [0-9]+/` Look for lines starting with the word Listen followed by one or more digits

`/Listen 8080/` Replace with the literal string "Listen 8080"

`httpd.conf` The file to modify



# Executing on Remote Systems

- Commands can be executed remotely via SSH
- SSH keys can be used to allow authentication without putting the password in a clear text file
- Generate the key with `ssh-keygen`
- Copy public key to `.ssh/authorized_keys` in the target system's user home directory (e.g. `/home/tim/.ssh/authorized_keys`)
- Change the listening port on many machines:

```
#!/bin/sh
for third in {0..6}; do
  for fourth in {1..254}; do
    ssh -i timspriv.key tim@10.10.$third.$fourth "sed
-i'.bak' -E 's/Listen [0-9]+/Listen 8080/g'
/etc/httpd.conf"
  done
done
```

Cyber Aces Module 3 - ©2015 The SANS Institute. Redistribution Prohibited.

8

## Executing on Remote Systems

We can execute this remotely on a machine with SSH. If you pass a command to SSH, it will execute that command on the remote host after it logs in. For example:

```
$ ssh username@host 'ls -al'
```

This command will login to 'host' with the username 'username' and will execute the command "ls -la" on the remote host. But what about entering the password? You really don't want to put your password in clear text into a script file. Instead, you would configure SSH private keys so that you can login remotely using the key pairs rather than a password.

Now, combining this with our script above that goes through all of the computers, we come up with the following:

```
#!/bin/bash
#Simple Counting Loops
for thirdoctet in {0..6}
do
  for lastoctet in {1..254}
  do
    ssh -i timpriv.key tim@192.168.$thirdoctet.$lastoctet "sed -
-i'.bak' -E 's/Listen [0-9]+/Listen 8080/g' /etc/httpd.conf"
  done
done
```

# Restart a Service

- After changing the HTTP listening port, the service needs to be restarted

– We can use SSH again for that too!

```
#!/bin/bash
for third in {0..6}
do
  for fourth in {1..254}
  do
    ssh -i timpriv.key tim@10.10.$third.
    $fourth "/etc/init.d/apache2 restart"
  done
done
```

Cyber Aces Module 3 - ©2015 The SANS Institute. Redistribution Prohibited.

9

## Restart a Service

As a system administrator, you may want to restart a service on multiple computers at one time. Our sample script above can easily be modified to accomplish this. The init.d system is used to start and stop services on many Linux distributions. To restart the HTTPD service on all of the computers in our IP range, we could modify our script as follows:

```
#!/bin/bash
#Simple Counting Loops
for third in {0..6}
do
  for fourth in {1..254}
  do
    ssh -i timpriv.key tim@10.10.$third.$fourth "sed -i'.bak' -E
    's/Listen [0-9]+/Listen 8080/g' httpd.conf && /etc/init.d/
    apache2 restart"
  done
done
```

We could even combine the two commands with an && and have it modify the config file and then restart the service if the modification is successful.

```
#!/bin/bash
#Simple Counting Loops
for third in {0..6}
do
  for fourth in {1..254}
  do
    ssh tim@10.10.$third.$fourth "sed -i'.bak' -E 's/Listen [0-9]+/
    Listen 8080/g' httpd.conf && /etc/init.d/apache2 restart"
  done
done
```

# Killing a Process

- What if you have a script you want to execute on multiple machines?
  - You can copy it over and run it or...
  - Use as input to SSH
- Kill all instances of netcat (nc) on remote machines using a script named kill\_nc.sh

```
#!/bin/bash
for third in {0..6}; do
for fourth in {1..254}; do
ssh -i timpriv.key tim@10.10.$third.$fourth "bash
-s" < kill_nc.sh
done
done
```

Cyber Aces Module 3 - ©2015 The SANS Institute. Redistribution Prohibited.

10

## Killing a Process

Now we will look at how to do something a little more complex. Imagine that we want to run multiple commands and process the results. SSH only allows for the execution of a single command. This time, we want to execute multiple commands on the remote machine. To complicate things even further, this time imagine that we have several different custom installations of Linux with the KILLALL and PS commands in different directories. We will add some code to find "ps", kill our process, and verify that our process was killed. The commands we want to execute on the remote system look like this:

```
#!/bin/bash
PATH_TO_PS=`which ps`; PATH_TO_KILLALL=`which killall`
# we find our ps and killall commands and store their location
if [ $PATH_TO_PS == '' ] || [ $PATH_TO_KILLALL == '' ]; then
# if we didn't find one of them, record an error
echo "One of our commands is missing on $HOSTNAME"
else
# if we did find our programs, we use killall to kill the nc process
$PATH_TO_KILLALL nc
PROCCOUNT=`$PATH_TO_PS a | grep nc | wc -l`
#we count the number of nc processes that are running
if [ $PROCCOUNT -gt 1 ]
#If we have more than 1 (grep will be one) then echo a warning
then
echo "Still running on $HOSTNAME"
fi
fi
```

Save that script on your local computer as "kill\_nc.sh". How would you do this across multiple remote computers? One method is to use "scp" to copy it to the remote computer and execute it. Alternatively, you could use "kill\_nc.sh" as input to the remote BASH prompt as follows:

```
$ ssh user@host 'bash -s' < kill_nc.sh
```

To run it on multiple machines we can wrap it in our earlier script:

# EXPECT

- Sometimes it is necessary to interact with the remote computer, rather than simply sending a single command.
  - Login to a remote computer
  - Wait for a login prompt before transmitting the username
  - After it enters the username, wait until the password prompt appears
  - /usr/bin/expect is the interpreter, not /bin/bash (see 1<sup>st</sup> line of script)
- This script will automate the login to an SSH server

```
#!/usr/bin/expect
set timeout 20
set ip [lindex $argv 0]
set user [lindex $argv 1]
set password [lindex $argv 2]
spawn ssh "$user@$ip"
expect "Password:"
send "$password\r";
interact
```

Cyber Aces Module 3 - ©2015 The SANS Institute. Redistribution Prohibited.

11

## EXPECT

Our last topic in discussing Bash is interacting with a remote computer. Sometimes it is necessary to interact with the remote computer, rather than simply sending a single command. For example, if we are trying to login to a remote computer, you need your script to be able to "spawn" ssh, then have it wait for a login prompt before it transmits the username. After it enters the username, it needs to wait until the password prompt appears before it transmits the passwords. This problem can be solved using "expect".

For additional reading on this subject read this page: <http://www.thegeekstuff.com/2010/10/expect-examples/>

# Exercise

- Install the OpenSSH server on your system with the following commands then answer the questions below.

- This will simulate running the commands on a remote server

```
$ sudo yum -y install openssh-server
```

```
$ sudo service sshd start
```

```
$ passwd
```

```
<enter a new password for yourself>
```

- 1) Write a command that will login to your system via SSH and display the contents of the "/etc" directory.
- 2) Create a script named "remoteclean.sh" in /home/centoslive/ containing the command:

```
echo Clean Complete
```

Then write a command that will execute the local script "/home/centoslive/remoteclean.sh" using SSH.

## Exercise

Install the OpenSSH server on your system with the following commands then answer the questions below.

You will then connect to your own system via SSH to simulate running the commands on a remote server.

```
$ sudo yum -y install openssh-server
```

```
$ sudo service sshd start
```

```
$ passwd
```

```
<enter a new password for yourself>
```

- 1) Write a command that will login to your system via SSH and display the contents of the "/etc" directory.
- 2) Create a script named "remoteclean.sh" in /home/centoslive/ containing the command:

```
echo Clean Complete
```

Then write a command that will execute the local script "/home/centoslive/remoteclean.sh" using SSH.

## Possible Answers

1) Write a command that will login to your system via SSH and display the contents of the "/etc" directory.

- `ssh centosliver@127.0.0.1 'ls /etc'`
- The command is very similar to logging to an SSH server, the only difference is the command, wrapped in quotes, at the end

2) You want to execute the local script "/home/user/remoteclean.sh" on a remote machine. Which of the following ssh commands would you use?

- `ssh centosliver@127.0.0.1 "bash -s" < /home/centosliver/remoteclean.sh`
- Similar to the command above, except the command we want to execute "bash -s". The script will be fed into the shell and executed on the remote system

### Possible Answers

1) Write a command that will login to your system via SSH and display the contents of the "/etc" directory.

**`ssh centosliver@127.0.0.1 'ls /etc'`**

The command is very similar to logging to an SSH server, the only difference is the command, wrapped in quotes, at the end.

2) You want to execute the local script "/home/user/remoteclean.sh" on a remote machine. Which of the following ssh commands would you use?

**`ssh centosliver@127.0.0.1 "bash -s" < /home/centosliver/remoteclean.sh`**

Similar to the command above, except the command we want to execute "bash -s". The script will be fed into the shell and executed on the remote system.

# Course Roadmap

- Introduction
- Linux Review
- Command Substitution
- Variables & Parameters
- Flow Control
- Parsing
- Searching
- Practical Uses
- ***Conclusions***

This is the conclusion of the Bash Scripting Module



## Conclusion for Module 3 - Bash

- This concludes Bash Scripting
  - We've learned about Bash and how to automate tasks in Linux by writing scripts
  - Automation make tasks faster, more accurate, and less mundane
  - Next is PowerShell, the newest shell for Windows

### Bash Scripting Conclusions

This concludes BASH Scripting. We've learned about BASH and how to automate tasks in Linux by writing scripts. Automation make tasks faster, more accurate, and less mundane.

The next module is on PowerShell, the newest shell for Windows.