Case Name: WK5

[redacted]

Examiner Name: Candace [redacted]

Table of Contents

List of Illustrative Materials

Tables

Figures

Executive Summary

Background

Security staff at Bob's Dry Cleaners, having been previously attacked by unhappy customers, have been monitoring activity on their network closely. Recently, they noticed a sudden burst of failed login attempts to their SSH server in the DMZ, beginning at 18:56:50 on April 27, 2011.

Request

The examiner has been asked to analyze the contents of the workstation, server, and firewall logs. The following questions should be addressed:
• Evaluate whether the failed login attempts were indicative of a deliberate attack. If so, identify the source and the target(s).
• Determine whether any systems were compromised. If so, describe the extent of the compromise. Specifically look for potential leakage of credit card data.

Findings

The failed login attempts have the features of a brute-force password guessing attack so were likely the result of a deliberate attack by source 172.30.1.77 on destination 10.30.30.20. The account 'bob' was compromised and used to leverage access from the DMZ to system 192.168.30.101. An FTP connection from 192.168.30.101 to the original source of attack 172.30.1.77 was successfully initiated. As a result, any accounts with credentials stored on 10.30.30.20 (baboon-srv) or 192.168.30.101 (dog-ws) should be treated as compromised. The hard drives of the compromised systems should be analyzed to inventory whether confidential information like credit cards may have been exfiltrated via the FTP server. Flow records should also be inspected for evidence of exfiltrated account data.

Evidence

Table 1 outlines the evidence items of this case.

Description	Designation	Filename	MD5 Hash
Evidence Provided	Preservation Copy	Ch8-EventLogs.zip	35BFDAB6570FFC4A9C7728601BA470D8
Evidence Created	Working Copy	Ch8-EventLogsXX	35BFDAB6570FFC4A9C7728601BA470D8
Evidence Examined	Working Copy	Ch8-EventLogsXX	35BFDAB6570FFC4A9C7728601BA470D8

Table 1: Case Evidence Items

Analysis

Examiner opened the Splunk web interface located at *http://CYB457-12:8000* and clicked **Add Data.** Examiner imported log files *auth.log, firewall.log,* and *workstations.log.* Examiner applied filters to view the events from *auth.log* over a one-minute period from 18:57:59 to 18.57.59 (hour variation is a result of mismatched time zones), as shown in figure 1. Two events occur every 6 seconds, in this case translating to 3 failed logins every six seconds (or 1 failed login every 2 seconds), since one of the two events actually accounts for two. The regularity of each login attempt is indicative of a brute-force password guessing attack.

Figure 1: Auth.log one-minute event pattern

In *Desktop/Week5/Working/Ch8-EventLogs* directory, the commands "grep "authentication failure" auth.log | grep "baboon-srv" | grep "user=root" | grep -c "pam_unix(sshd:auth): authentication failure" and "grep "authentication failure" auth.log | grep "baboon-srv" | grep "user=root" | grep -c "PAM 2 more authentication failures" (see figure 2) were entered in terminal. Cumulatively, these numbers equate to 121 failed login attempts to the 'root' account.

```
cyberstud@CYB457-12:~/Desktop/Week5/Working/Ch8-EventLogs$ grep "authentication
 failure" auth.log | grep "baboon-srv" | grep "user=root" | grep -c "pam_unix(s
shd:auth): authentication failure"
41
cyberstud@CYB457-12:~/Desktop/Week5/Working/Ch8-EventLogs$ ^C
cyberstud@CYB457-12:~/Desktop/Week5/Working/Ch8-EventLogs$ grep "authentication
 failure" auth.log | grep "baboon-srv" | grep "user=root" | grep -c "PAM 2 more
 authentication failures"
40
```

Figure 2: Number of failed 'root' login attempts

Examiner entered similar commands to reveal the number of authentication failures for user 'bob', seen below. There were 85 failed login attempts for account 'bob'.

```
cyberstud@CYB457-12:~/Desktop/Week5/Working/Ch8-EventLogs$ grep "authentication
 failure" auth.log | grep "baboon-srv" | grep "user=bob" | grep -c "pam_unix(ss
hd:auth): authentication failure"
29
cyberstud@CYB457-12:~/Desktop/Week5/Working/Ch8-EventLogs$ grep "authentication
 failure" auth.log | grep "baboon-srv" | grep "user=bob" | grep -c "PAM 2 more
authentication failures"
28
```

Figure 3: Number of failed 'bob' login attempts

Examiner created graphs in Splunk to display the relative timestamps for each user. As can be seen in figures 4 and 5, failed logins for 'root' occurred first and failed logins for 'bob' occurred second.

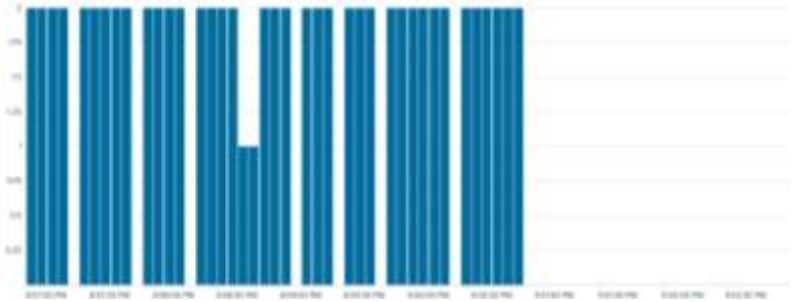

Figure 4: Attacks on 'root'

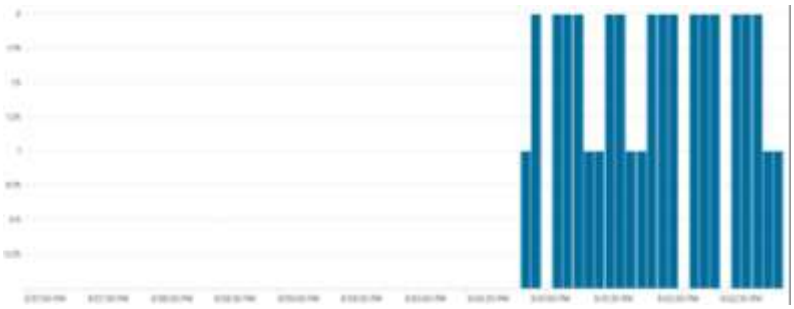

Figure 5: Attacks on 'bob'

Examiner entered command “grep “authentication failure” auth.log | grep “baboon-srv” | grep “sshd” | tail -1” in terminal to identify the last failed login attempt. It occurred at 19:04:05, as shown in figure 6.

```
cyberstud@CYB457-12:~/Desktop/Week5/Working/Ch8-EventLogs$ grep "authentication
 failure" auth.log | grep "baboon-srv" | grep "sshd" | tail -1
2011-04-26T19:04:05-06:00 baboon-srv sshd[6561]: pam_unix(sshd:auth): authentic
ation failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.30.1.77  user=bob
```

Figure 6: Last failed login attempt

Examiner entered command: “grep “Accepted password” auth.log | grep “baboon-srv” | grep “sshd”” in terminal to identify successful login attempts. There were two successful logins from the same remote host as the failed login attempts, as seen in figure 7. Both occurred after the previously unsuccessful attacks, strongly indicating the attacker successfully found the correct password for user ‘bob’.

```
cyberstud@CYB457-12:~/Desktop/Week5/Working/Ch8-EventLogs$ grep "Accepted passw
ord" auth.log | grep "baboon-srv" | grep "sshd"
2011-04-26T19:04:07-06:00 baboon-srv sshd[6561]: Accepted password for bob from
 172.30.1.77 port 49214 ssh2
2011-04-26T19:04:33-06:00 baboon-srv sshd[6632]: Accepted password for bob from
 172.30.1.77 port 49215 ssh2
```

Figure 7: Successful login attempts from 172.30.1.77

Examiner located log entry shown in figure 8. It is probable the attacker used text editor Vim to alter the locally stored authentication records.

```
2011-04-26T19:05:18-06:00 baboon-srv sudo:      bob : TTY=pts/0 ; PWD=/
home/bob ; USER=root ; COMMAND=/usr/bin/vi /var/log/auth.log
```

Figure 8: Command executed by attacker

Examiner located log entry shown in figure 9. The attacker used Tcpdump to send network traffic to the standard output location.

```
2011-04-26T19:05:34-06:00 baboon-srv sudo:      bob : TTY=pts/0 ; PWD=/
home/bob ; USER=root ; COMMAND=/usr/sbin/tcpdump -nni eth0
```

Figure 9: Command executed by attacker

Examiner located log entries shown in figure 10. The attacker installed Nmap. Non-privileged commands are not recorded in this log, so it is possible the attacker subsequently ran the Nmap utility on the local network without leaving a trail in the *auth.log* file.

```
2011-04-26T19:07:03-06:00 baboon-srv sudo:      bob : TTY=pts/0 ; PWD=/
home/bob ; USER=root ; COMMAND=/usr/bin/apt-get update
2011-04-26T19:07:15-06:00 baboon-srv sudo:      bob : TTY=pts/0 ; PWD=/
home/bob ; USER=root ; COMMAND=/usr/bin/apt-get install nmap
```

Figure 10: Command executed by attacker

Examiner isolated events from the *firewall.log* file related to 'baboon-srv'. The graph below shows the (abbreviated) number of events originating from 10.30.30.20 over time by destination port number. The visualization suggests that 10.30.30.20 (the compromised 'baboon-srv') engaged in port scanning of different systems.

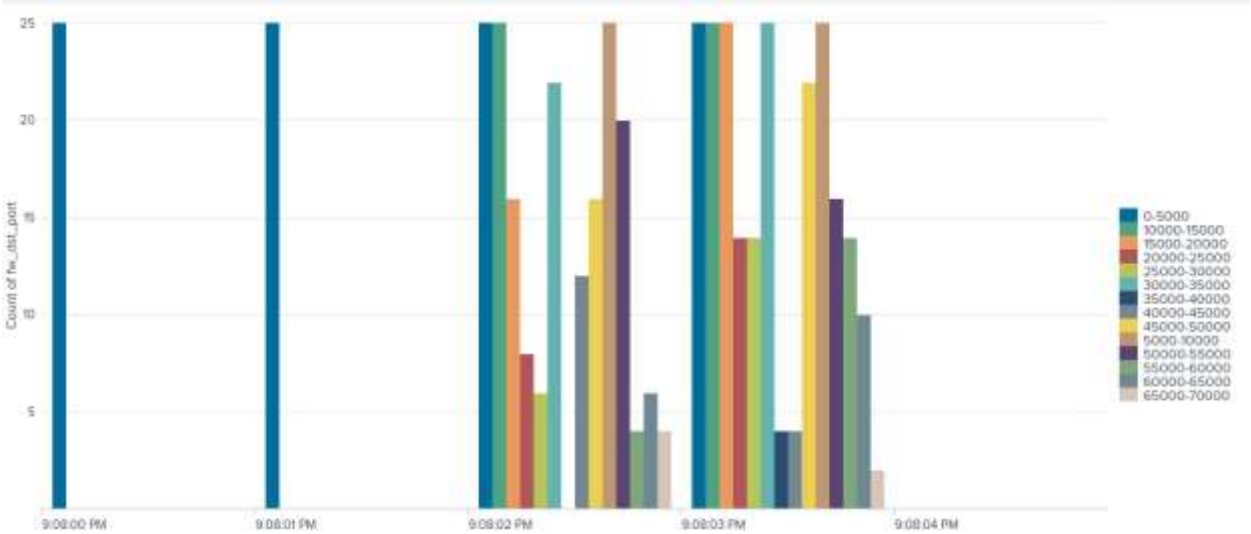

Figure 11: Port numbers targeted by 10.30.30.20

Examiner created a new graph to visualize the time period from 19:08:54 to 19:09:00, shown in figure 12. It shows events originating from 10.30.30.20 to port 3389 only, by IP address- indicating that the compromised server performed a port sweep to try and make a remote connection.

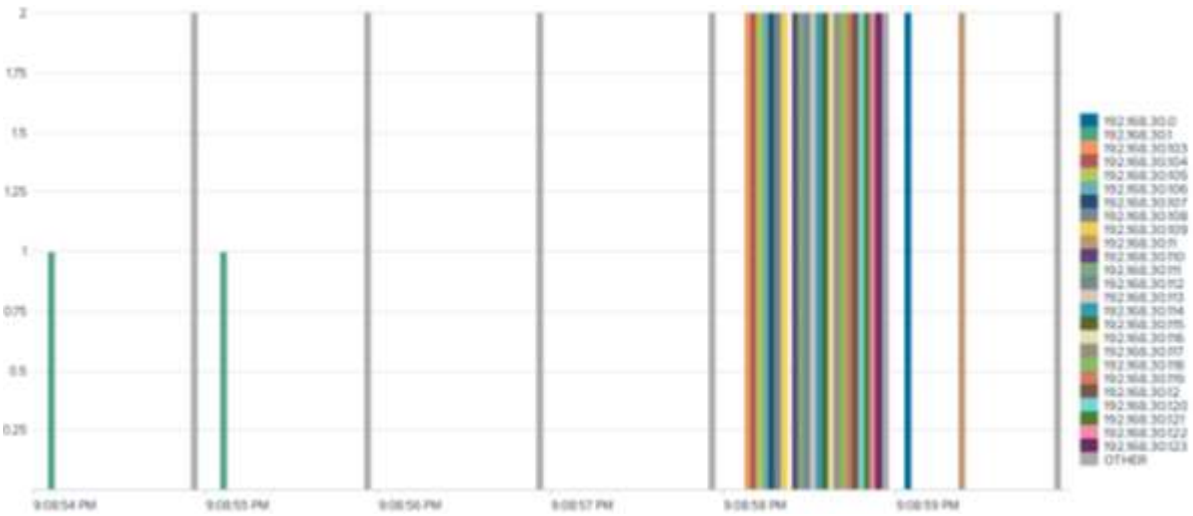

Figure 12: Port 3389 sweep by 10.30.30.20

Although not visible in figure 12, IP address 192.168.30.101 received two more connections (four total) on port 3389 than the other IP addresses. Examiner returned to terminal and entered command "grep '192.168.30.101(3389)' firewall.log". The four connections are displayed in figure 13.

```
cyberstud@CYB457-12:~/Desktop/Week5/Working/Ch8-EventLogs$ grep '192.168.30.101
(3389)' firewall.log
2011-04-26T19:08:58-06:00 ant-fw : %ASA-6-106100: access-list dmz permitted tcp
 dmz/10.30.30.20(49814) -> inside/192.168.30.101(3389) hit-cnt 1 first hit [0xd
a142b8f, 0x0]
2011-04-26T19:09:37-06:00 ant-fw : %ASA-6-106100: access-list dmz permitted tcp
 dmz/10.30.30.20(50215) -> inside/192.168.30.101(3389) hit-cnt 1 first hit [0xd
a142b8f, 0x0]
2011-04-26T19:09:37-06:00 ant-fw : %ASA-6-106100: access-list dmz permitted tcp
 dmz/10.30.30.20(50216) -> inside/192.168.30.101(3389) hit-cnt 1 first hit [0xd
a142b8f, 0x0]
2011-04-26T19:10:47-06:00 ant-fw : %ASA-6-106100: access-list dmz permitted tcp
 dmz/10.30.30.20(50217) -> inside/192.168.30.101(3389) hit-cnt 1 first hit [0xd
a142b8f, 0x0]
```

Figure 13: Four connections allowed from 10.30.30.20 to 192.168.30.101:3389

Examiner entered command "grep 528 workstations.log | grep -i dog-ws" in terminal to isolate successful logins to 192.168.30.101. One event for user 'bob' is shown in figure 14. It is logon type 10, which means a login from a terminal service or remote desktop.

```
cyberstud@CYB457-12:~/Desktop/Week5/Working/Ch8-EventLogs$ grep 528 workstation
s.log | grep -i dog-ws
2011-04-26T19:11:08-06:00 dog-ws MSWinEventLog#0111#011Security#011754#011Tue A
pr 26 19:11:01 2011#011528#011Security#011bob#011User#011Success Audit#011DOG-W
S#011Logon/Logoff#011#011Successful Logon:     User Name: bob     Domain: DOG-W
S     Logon ID: (0x0,0x155A04D)     Logon Type: 10     Logon Process: User32
    Authentication Package: Negotiate     Workstation Name: DOG-WS     Logon GU
ID: {00000000-0000-0000-0000-000000000000}  #011698
```

Figure 14: Successful login to 192.168.30.101

Two further event logs of concern were found by the examiner, shown in figure 15. They show that the account ‘bob’ executed a command shell, then initiated a program used to transfer files between remote systems.

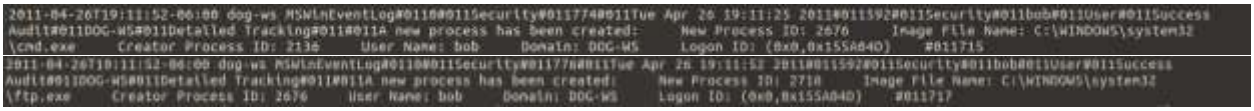

Figure 15: Commands executed via remote login

To confirm if any FTP connections initiated were successful, examiner entered command “grep ‘192.168.30.101’ firewall.log”. One result, as seen in figure 16, indicates that the firewall did permit an FTP connection from 192.160.30.101 to 172.30.1.77.

Conclusion

The examiner was asked to Evaluate whether the failed login attempts were indicative of a deliberate attack. The examiner determined the failed login attempts had the features of a brute-force password guessing attack so were likely the result of a deliberate attack by source 172.30.1.77 on the DMZ 10.30.30.20. The examiner was asked to determine whether any systems were compromised, and to what extent. Examiner found that the account ‘bob’ was compromised and used to leverage access from the DMZ to system 192.168.30.101. An FTP connection from 192.168.30.101 to the original source of attack 172.30.1.77 was successfully initiated. As a result, any accounts with credentials stored on 10.30.30.20 (baboon-srv) or 192.168.30.101 (dog-ws) should be treated as compromised. The hard drives of the compromised systems should be analyzed to inventory whether confidential information like credit cards may have been exfiltrated via the FTP server.

Appendix

Appendix A: Examiner Workstation Specifications

- 
- System date/time is consistent with the time zone listed above, as verified by: http://nist.time.gov/.

Appendix B: Virtual Machine (VM) Specifications

- Virtual Machine Name: CYB457-12
- Operating System Name: Ubuntu
- System Make/Model: VMware, Inc. VMware Virtual Platform
- Virtual Machine Serial Number: VMware-42 1b 8a 7d d6 56 cd 16-8c 9a 80 0e 79 fb c8 f9
- VM's Time Zone: Eastern Daylight Time
- System date and time are consistent with the time zone listed above, as verified by: http://nist.time.gov/.

Appendix C: Tools

- Splunk 8.0.3

Appendix D: Evidence Copies

On 4/18/2020, the location of the week 5 lab files was made known to the examiner. The examiner created a new *Week5* folder on the *Desktop*, then retrieved archive file *Ch8-EventLogs.zip* via Mozilla Firefox from the CYB457 course shell to the *Week5* folder.

Examiner used the online utility located at onlinemd5.com to obtain the md5 hash value of the downloaded archive file. No checksum for comparison was provided, so the examiner was unable to determine the purity of the preservation copy.

A new folder in *Week5* was created called *Working*. Examiner created a working copy of the *Ch8-EventLogs* archive file in the *Working* folder called *Ch8-EventLogs*. Onlinemd5.com was used to determine the hash value of the evidence created, which matched the preservation copy, confirming the integrity of the working copy.

Examiner unzipped the working copy archive, revealing file folder *Ch8-EventLogs*.

Appendix E: Evidence Verification

Table 2 outlines the hashes obtained throughout the evidence verification process. Onlinemd5.com was used to calculate MD5 hashes.

Designation	Filename	MD5 Hash	Description
PRE-ANALYSIS			
Preservation Copy	Ch8-EventLogs.zip	35BFDAB6570FFC4A9C7728601BA470D8	Archive file downloaded from Engage
Working Copy	Ch8-EventLogsXX	35BFDAB6570FFC4A9C7728601BA470D8	Working Copy created from preservation copy. This copy was analyzed.
POST-ANALYSIS			
Preservation Copy	Ch8-EventLogs.zip	35BFDAB6570FFC4A9C7728601BA470D8	Archive file downloaded from Engage
Working Copy	Ch8-EventLogsXX	35BFDAB6570FFC4A9C7728601BA470D8	Working Copy created from preservation copy. This copy was analyzed.

Table 2: Evidence Verification Table