Case Name: WK6

[redacted]

Examiner Name: Candace [redacted]

Table of Contents

List of Illustrative Materials

Tables

Figures

Executive Summary

Background

Security staff at the International Chaos Cookie Company recently detected a workstation (192.168.30.105) in their network attempting to make an outbound IRC connection on port 6667. After tracking the location of the workstation to a conference room not meant to have computer activity, security staff need to determine whether activity associated with the workstation was malicious or benign.

Request

The examiner has been asked to analyze the contents of the provided logs. The following should be accomplished:

- Map the suspect IP address back to a MAC address
- Track the MAC address to the physical ports it used.
- Build a timeline of the suspicious system's activities in order to determine if it was a bad actor, and if so, to scope the extent of compromise.

Findings

The IP address 192.168.30.105 was leased to MAC address 00:26:22:cb:10:17. The physical port the device connected to was Ethernet0/6. A timeline was developed: At 16:45:13 on 4/29/11, a previously unseen device with MAC address 00:26:22:cb:10:17 connected to an ethernet port in an empty conference room. After a few seconds, the device tripped IDS alerts and firewall logs when it attempted to make an outbound connection, probably to an IRC, on port 6667. Unsuccessful attempts were made by the device to the firewall at 16:48:51, then to 192.168.1.50 at 16:50:28. At 16:51:33, the device physically disconnected. Based on the attempted connections that were prohibited by policy, it is possible the activity came from a rogue system or a corporate system modified to behave inappropriately. Further access to event logs would enable a deeper understanding of the extent of compromise.

Evidence

Table 1 outlines the evidence items of this case.

Description	Designation	Filename	MD5 Hash
Evidence Provided	Preservation Copy	Ch9-Firewalls.zip	AFE29BD4BC8E34A79DB4EFA0B99E140A
Evidence Created	Working Copy	Ch9-FirewallsXX	AFE29BD4BC8E34A79DB4EFA0B99E140A
Evidence Examined	Working Copy	Ch9-FirewallsXX	AFE29BD4BC8E34A79DB4EFA0B99E140A

Table 1: Case Evidence Items

Analysis

Examiner opened file *Desktop/Week6/Working/Ch9-Firewalls/fw-evidence.txt*. Examiner reviewed the ARP tables and determined the MAC address linked to the suspect system is 00:26:22:cb:10:17 (see figure 1).

```
ant-fw# show clock
16:52:48.927 MDT Fri Apr 29 2011
ant-fw# show arp
    inside 192.168.30.30 0008.742d.2f94 38
    inside 192.168.30.50 0012.3f65.a7e1 51
    inside 192.168.30.105 0026.22cb.1017 138
    inside 192.168.30.102 0012.7964.f718 225
    inside 192.168.30.101 000b.cdc2.e491 226
    inside 192.168.30.90 0008.74a0.2e02 1930
    inside 192.168.30.11 001e.c21d.0c96 2579
    inside 192.168.30.104 0012.3f65.a7e1 4224
    inside 192.168.30.100 0008.74fa.a6cc 5328
    inside 192.168.30.103 0012.3f65.a7e1 5622
    outside 172.30.1.5 0001.031a.d5f6 131
    outside 172.30.1.254 5475.d0ba.522a 347
    outside 172.30.1.77 c80a.a904.c8ca 13170
    dmz 10.30.30.20 0008.74d5.e0c4 51
```

Figure 1: ARP table

Examiner reviewed the CAM table (figure 2) and determined that, based on the expiration of 205 seconds, the entry was updated at 16:51:13. The MAC address was assigned as a member of VLAN 0001 to port Et0/6.

```
   Mac Address   | VLAN |        Type        | Age | Port
-----------------------------------------------------------
0008.742d.2f94 | 0001 |     dynamic        | 287 | Et0/5
0008.74a0.2e02 | 0001 |     dynamic        | 082 | Et0/7
000b.cdc2.e491 | 0001 |     dynamic        | 082 | Et0/3
0012.3f65.a7e1 | 0001 |     dynamic        | 246 | Et0/2
0012.7964.f718 | 0001 |     dynamic        | 082 | Et0/4
0026.22cb.1017 | 0001 |     dynamic        | 205 | Et0/6
d0d0.fdc4.0994 | 0001 |     static         |  -  | In0/1
ffff.ffff.ffff | 0001 | static broadcast   |  -  | In0/1,Et0/0-7
0001.031a.d5f6 | 0002 |     dynamic        | 164 | Et0/0
5475.d0ba.522a | 0002 |     dynamic        | 164 | Et0/0
d0d0.fdc4.0994 | 0002 |     static         |  -  | In0/1
ffff.ffff.ffff | 0002 | static broadcast   |  -  | In0/1,Et0/0-7
0008.74d5.e0c4 | 0003 |     dynamic        | 246 | Et0/1
d0d0.fdc4.0994 | 0003 |     static         |  -  | In0/1
ffff.ffff.ffff | 0003 | static broadcast   |  -  | In0/1,Et0/0-7
```

Figure 2: CAM table

Examiner noted further that the firewall is logging lease assignments to a remote syslog server on inside host 192.168.30.30 (figure 3).

```
140 logging enable
141 logging timestamp
142 logging list notification-dhcp-fw level notifications
143 logging list notification-dhcp-fw message 604101-604104
144 logging list notification-dhcp-fw message 106100
145 logging console alerts
146 logging monitor notifications
147 logging trap notification-dhcp-fw
148 logging asdm informational
149 logging device-id hostname
150 logging host inside 192.168.30.30
```

Figure 3: Firewall config entry related to DHCP assignments

In *Desktop/Week6/Working/Ch9-Firewalls* directory, examiner entered command "grep '192.168.30.105' dhcp.log", as seen in figure 4. The results confirm that the suspicious IP address was assigned to the MAC address identified earlier at 16:47:35.

```
cyberstud@CYB457-12:~/Desktop/Week6/Working/Ch9-Firewalls$ grep '192.168.30.105'
 dhcp.log
2011-04-29T16:47:35-06:00 ant-fw : %ASA-6-604103: DHCP daemon interface inside:
 address granted 0026.22cb.1017 (192.168.30.105)
```

Figure 4: Occurrences of '192.168.30.105' in dhcp.log

Examiner entered command: grep '0026.22cb.1017' dhcp.log in terminal. A lone result, shown in figure 5, indicates that this system was not seen by the server between 16:02:39 and 16:47:35.

```
cyberstud@CYB457-12:~/Desktop/Week6/Working/Ch9-Firewalls$ grep 0026.22cb.1017 d
hcp.log
2011-04-29T16:47:35-06:00 ant-fw : %ASA-6-604103: DHCP daemon interface inside:
 address granted 0026.22cb.1017 (192.168.30.105)
```

Figure 5: Occurrences of MAC address in dhcp.log

The access lists inside the firewall configuration file indicate that the internal hosts of the ICCC are permitted to send ICMP and web traffic anywhere, connect via FTP to external systems, exchange DNS, NTP, SSH traffic with the DMZ server. All permitted actions are logged, so activity by the suspicious system should be available elsewhere for investigation.

In *Desktop/Week6/Working/Ch9-Firewalls* directory, examiner entered command "cat firewall.log | grep \(53\) | grep '192.168.30.105'". The results, truncated in figure 6, reveal that 192.168.30.105 sent traffic on UDP port 53 to the local DNS server 16 times in the space of one minute and 15 seconds (between 16:47:36 and 16:48:51).

```
cyberstud@CYB457-12:~/Desktop/Week6/Working/Ch9-Firewalls$ cat firewall.log | gr
ep \(53\) | grep '192.168.30.105'
2011-04-29T16:47:36-06:00 ant-fw : %ASA-6-106100: access-list inside permitted u
dp inside/192.168.30.105(44724) -> dmz/10.30.30.20(53) hit-cnt 1 first hit [0xb8
20d39, 0x0]
2011-04-29T16:47:36-06:00 ant-fw : %ASA-6-106100: access-list inside permitted u
dp inside/192.168.30.105(42410) -> dmz/10.30.30.20(53) hit-cnt 1 first hit [0xb8
20d39, 0x0]
2011-04-29T16:47:36-06:00 ant-fw : %ASA-6-106100: access-list inside permitted u
dp inside/192.168.30.105(36088) -> dmz/10.30.30.20(53) hit-cnt 1 first hit [0xb8
20d39, 0x0]
2011-04-29T16:47:36-06:00 ant-fw : %ASA-6-106100: access-list inside permitted u
dp inside/192.168.30.105(33475) -> dmz/10.30.30.20(53) hit-cnt 1 first hit [0xb8
20d39, 0x0]
2011-04-29T16:47:48-06:00 ant-fw : %ASA-6-106100: access-list inside permitted u
dp inside/192.168.30.105(48153) -> dmz/10.30.30.20(53) hit-cnt 1 first hit [0xb8
20d39, 0x0]
```

Figure 6: DNS requests by suspicious system (truncated)

Examiner entered "head firewall.log" in terminal. A selection of entries from this query (see figure 7) shows that the suspicious host attempted to send 4 UDP datagrams to 91.189.94.4:123. The host was denied based on the firewall ACLs.

```
2011-04-29T16:47:37-06:00 ant-fw : %ASA-4-106023: Deny udp src inside:192.168.30.10
5/123 dst outside:91.189.94.4/123 by access-group "inside" [0x0, 0x0]
2011-04-29T16:47:48.009774-06:00 ant-fw : last message repeated 3 times
```

Figure 7: Attempted connections to 91.189.94.4:123

Examiner entered command "dig -x 91.189.94.4" in terminal. It is associated with Ubuntu servers, making it likely the suspicious system was running Ubuntu. NTP requests by internal corporate clients are configured to use the 10.30.30.20 (DMZ) server, another strong indicator that this system should still be considered suspicious.

```
cyberstud@CYB457-12:~/Desktop/Week6/Working/Ch9-Firewalls$ dig -x 91.189.94.4

; <<>> DiG 9.10.3-P4-Ubuntu <<>> -x 91.189.94.4
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29128
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;4.94.189.91.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
4.94.189.91.in-addr.arpa. 2337  IN      PTR     pugot.canonical.com.

;; Query time: 22 msec
;; SERVER: 10.56.1.10#53(10.56.1.10)
;; WHEN: Sun Apr 26 12:08:01 EDT 2020
;; MSG SIZE  rcvd: 86
```

Figure 8: Information on 91.189.94.4

Examiner located another interesting entry, seen in figure 9. The suspicious system tried to make an outbound connection to port 6667 on host 140.211.167.99 at 16:47:48, the same time of the initial IDS alert reported by ICCC staff.

```
cyberstud@CYB457-12:~/Desktop/Week6/Working/Ch9-Firewalls$ cat firewall.log | grep
140.211.167.99
2011-04-29T16:47:48-06:00 ant-fw : %ASA-4-106023: Deny tcp src inside:192.168.30.10
5/50885 dst outside:140.211.167.99/6667 by access-group "inside" [0x0, 0x0]
```

Figure 9: Attempted connection to 140.211.167.99

Examiner queried Whois (figure 10) and Dig for information on destination 140.211.167.99. The Whois indicates the destination in hosted in Oregon. Dig, although unable to be replicated, should have shown a freenode IRC node hosted at that address.

```
NetRange:       140.211.0.0 - 140.211.255.255
CIDR:           140.211.0.0/16
NetName:        NERONET
NetHandle:      NET-140-211-0-0-1
Parent:         NET140 (NET-140-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS3701
Organization:   Network for Education and Research in Oregon (NERO) (UO-12)
RegDate:        1990-06-10
Updated:        2014-08-15
Ref:            https://rdap.arin.net/registry/ip/140.211.0.0


OrgName:        Network for Education and Research in Oregon (NERO)
OrgId:          UO-12
Address:        1225 Kincaid Street
City:           Eugene
StateProv:      OR
PostalCode:     97403
```

Figure 10: Whois results

Starting at 16:48:51, the suspicious system made connection attempts to port 22 of the firewall's internal. However, the ACLs are not set to log internal TCP connections. It also attempted a connection to nonroutable host 192.168.1.50. The Et0/6 port state changed to "down" after a total of 6 and a half minutes.

Conclusion

The examiner was asked to map the suspect IP address back to a MAC address. The IP address 192.168.30.105 was leased to MAC address 00:26:22:cb:10:17. The examiner was asked to track the MAC address to the physical ports it used. The physical port the device connected to was Ethernet0/6. The examiner was asked to build a timeline of the suspicious system's activities in order to determine if it was a bad actor, and if so, to scope the extent of compromise. At 16:45:13 on 4/29/11, a previously unseen device with MAC address 00:26:22:cb:10:17 connected to an ethernet port in an empty conference room. After a few seconds, the device tripped IDS alerts and firewall logs when it attempted to make an outbound connection, probably to an IRC, on port 6667. Unsuccessful attempts were made by the device to the firewall at 16:48:51, then to 192.168.1.50 at 16:50:28. At 16:51:33, the device physically disconnected. Based on the

attempted connections that were prohibited by policy, it is possible the activity came from a rogue system or a corporate system modified to behave inappropriately. Further access to event logs would enable a deeper understanding of the extent of compromise.

Appendix

Appendix A: Examiner Workstation Specifications

- [redacted]
- 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

- Dig v9.10.3
- Whois v5.2.11

Appendix D: Evidence Copies

On 4/26/2020, the examiner created a new *Week6* folder on the *Desktop*, then retrieved archive file *Ch9-Firewalls.zip* via Mozilla Firefox from the CYB457 course shell to the *Week6* 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 *Week6* was created called *Working*. Examiner created a working copy of the *Ch9-Firewalls* archive file in the *Working* folder called *Ch9-FirewallsXX*. 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 *Ch9-Firewalls.*

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	Ch9-Firewalls.zip	AFE29BD4BC8E34A79DB4EFA0B99E140A	Archive file downloaded from Engage
Working Copy	Ch9-FirewallsXX	AFE29BD4BC8E34A79DB4EFA0B99E140A	Working Copy created from preservation copy. This copy was analyzed.
POST-ANALYSIS			
Preservation Copy	Ch9-Firewalls.zip	AFE29BD4BC8E34A79DB4EFA0B99E140A	Archive file downloaded from Engage
Working Copy	Ch9-FirewallsXX	AFE29BD4BC8E34A79DB4EFA0B99E140A	Working Copy created from preservation copy. This copy was analyzed.

Table 2: Evidence Verification Table