

Case Name: WK8.1



Examiner Name: Candace 

## Table of Contents

List of Illustrative Materials.....	3
Tables.....	3
Figures.....	3
Executive Summary .....	4
Background.....	4
Request.....	4
Findings.....	4
Evidence.....	4
Analysis.....	5
Conclusion .....	7
Appendix.....	8
Appendix A: Examiner Workstation Specifications.....	8
Appendix B: Virtual Machine (VM) Specifications.....	9
Appendix C: Tools.....	10
Appendix D: Evidence Copies.....	11
Appendix E: Evidence Verification .....	12

# List of Illustrative Materials

## Tables

Table 1: Case Evidence Items.....	4
Table 2: Evidence Verification Table .....	12

## Figures

Figure 1: Protocol hierarchy statistics of packet capture file.....	5
Figure 2: evidence-network-tunneling.pcap capture information.....	5
Figure 3: Protocol hierarchy of traffic originating form 192.168.1.30.....	5
Figure 4: Destination of DNS requests .....	6
Figure 5: Data frame 62 details.....	6
Figure 6: Trimmed contents of data frame 62 .....	7

# Executive Summary

## Background

Security analysts at the Secret Underground Nuclear Missile Facility received an IDS alert for unusual DNS traffic. As one of their servers contain secret missile launch codes, the alert is concerning.

## Request

The examiner has been asked to review a packet capture file containing all traffic relating to IP address 192.168.1.30 in order to:

- Determine if the traffic is truly suspicious.
- Determine the purpose of the unusual DNS traffic.
- If suspicious, recover as much information as possible about the local and remote systems involved.
- Evaluate the risk that data was exfiltrated.

## Findings

The DNS traffic was all of type “NULL”. It also was the only type of traffic besides one ARP request. These characteristics make the capture truly suspicious. The purpose of this DNS traffic is likely for covert tunneling, as “NULL” DNS records can contain any type of data and are often let through organization perimeters. To that end, the examiner successfully carved out a TCP header encapsulated in an IPv4 packet, but the data was encrypted. The remote tunnel endpoint was probably tnlh.slick.evl (172.16.16.220), while the remote endpoint of the tunneled traffic was 10.4.4.2:22 and the local endpoint of the tunneled traffic was 10.4.4.1:43448. Since the TCP flags set on the frame examined indicated it was part of an ongoing TCP conversation, the risk of data exfiltration is significant.

## Evidence

Table 1 outlines the evidence items of this case.

Description	Designation	Filename	MD5 Hash
Evidence Provided	Preservation Copy	Week 8.zip	61667661161E829F11CBD9A5D170E30A
Evidence Created	Working Copy	Week8XX	61667661161E829F11CBD9A5D170E30A
Evidence Examined	Working Copy	Week8XX	61667661161E829F11CBD9A5D170E30A

Table 1: Case Evidence Items

## Analysis

Examiner started Wireshark, opened file *Desktop/Week8/Working/Week8XX\_FILES/Ch11-NetworkTunnels/evidence-network-tunneling.pcap*, then opened **Protocol Hierarchy** from the **Statistics** menu (see figure 1). 99.48% of the traffic within this packet capture is DNS over UDP and .52% is ARP traffic.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	386	100.0	102115	37 k	0	0	0
▼ Ethernet	100.0	386	5.3	5404	1990	0	0	0
▼ Internet Protocol Version 4	99.5	384	7.5	7680	2828	0	0	0
▼ User Datagram Protocol	99.5	384	3.0	3072	1131	0	0	0
Domain Name System	99.5	384	84.1	85885	31 k	384	85885	31 k
Address Resolution Protocol	0.5	2	0.1	56	20	2	56	20

Figure 1: Protocol hierarchy statistics of packet capture file

In directory *Desktop/Week8/Working/Week8XX\_FILES/Ch11-NetworkTunnels*, examiner entered command “capinfos evidence-network-tunneling.pcap” in terminal. Truncated results, shown in figure 2, indicate that the packet capture began on 11/27/2010 at 23:39:45, and ends 22 seconds later at 23:40:07.

```
File name:          evidence-network-tunneling.pcap
File type:         Wireshark/tcpdump/... - pcap
File encapsulation: Ethernet
File timestamp precision: microseconds (6)
Packet size limit: file hdr: 65535 bytes
Number of packets: 386
File size:        108 kB
Data size:       102 kB
Capture duration: 21.722632 seconds
First packet time: 2010-11-28 01:39:45.556364
Last packet time: 2010-11-28 01:40:07.278996
Data byte rate:   4,700 bytes/s
Data bit rate:    37 kbps
Average packet size: 264.55 bytes
Average packet rate: 17 packets/s
SHA256:          da12bb26994715f5798813960f7945ae6f120d2dddd67dbbd203fc8c82f2e81d
RIPEMD160:      4c3b5bed369e666c89d8d4903d511b37410d558f
SHA1:           50562eb60514016520dd50f5744e90cc186baba1
```

Figure 2: evidence-network-tunneling.pcap capture information

Examiner opened the **Protocol Hierarchy** with display filter “ip.src==192.168.1.30” applied, as shown in figure 3. 192 DNS packets were sent in the span of the capture. No other traffic types were captured, which is unusual since DNS queries are typically followed by other application-layer traffic.

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	192	100.0	43873	16 k	0	0	0
▼ Ethernet	100.0	192	6.1	2688	991	0	0	0
▼ Internet Protocol Version 4	100.0	192	8.8	3840	1416	0	0	0
▼ User Datagram Protocol	100.0	192	3.5	1536	566	0	0	0
Domain Name System	100.0	192	81.6	35809	13 k	192	35809	13 k

Figure 3: Protocol hierarchy of traffic originating from 192.168.1.30

The main window in Wireshark shows the outbound traffic from 192.168.1.30 was directed to 10.1.1.20, the internal DNS server (see figure 4). By closer inspection of packet details, examiner discovered that the DNS query type of all packets was “NULL”, which is very uncommon. Examiner also discovered in frame 17 an unusual name being queried: Paaqrabj.tnl.slick.evl. The response to this packet reveals the authoritative name server for tnl.slick.evl is tnlh.slick.evl. It corresponds with IP address 172.16.16.220.

Time	Source	Destination	Protocol	Length	Info
1	2018-11-27 23:39:45.556364	192.168.1.30	10.1.1.20	DNS	93 Standard query 0x0998 NULL Paaiaq5r.tnl.slick.evl OPT
3	2018-11-27 23:39:46.583988	192.168.1.30	10.1.1.20	DNS	93 Standard query 0x0999 NULL Paaiaq55.tnl.slick.evl OPT
5	2018-11-27 23:39:47.614829	192.168.1.30	10.1.1.20	DNS	93 Standard query 0x099a NULL Paaiarah.tnl.slick.evl OPT
7	2018-11-27 23:39:48.643985	192.168.1.30	10.1.1.20	DNS	93 Standard query 0x099b NULL Paaiarap.tnl.slick.evl OPT
9	2018-11-27 23:39:49.678752	192.168.1.30	10.1.1.20	DNS	93 Standard query 0x099c NULL Paaiarax.tnl.slick.evl OPT
11	2018-11-27 23:39:50.780881	192.168.1.30	10.1.1.20	DNS	93 Standard query 0x099d NULL Paaiaara5.tnl.slick.evl OPT
13	2018-11-27 23:39:51.733865	192.168.1.30	10.1.1.20	DNS	93 Standard query 0x099e NULL Paaiaarb.tnl.slick.evl OPT

Figure 4: Destination of DNS requests

To find evidence of tunneled IP packets, examiner entered the following command in terminal: “ngrep -I evidence-network-tunneling.pcap -X “4500” -t -x ‘udp’”. Three matches were found, the first was sent at 23:39:54.283012, which corresponds to frame 62 in Wireshark. The data length of the frame is 117 bytes (see figure 5) and does contain the hexadecimal value “4500” in its payload. Examiner exported frame data as *evidence-network-tunneling-62.raw*.

```

> Frame 62: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits)
> Ethernet II, Src: Vmware_38:63:95 (00:0c:29:38:63:95), Dst: Vmware_63:c9:a8 (00:0c:29:63:c9:a8)
> Internet Protocol Version 4, Src: 10.1.1.20, Dst: 192.168.1.30
> User Datagram Protocol, Src Port: 53, Dst Port: 33777
v Domain Name System (response)
  Transaction ID: 0x09b6
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 1
  Additional RRs: 2
  > Queries
v Answers
  v Pabaardr.tnl.slick.evl: type NULL, class IN
    Name: Pabaardr.tnl.slick.evl
    Type: NULL RR (10)
    Class: IN (0x0001)
    Time to live: 0
    Data length: 117
    Null (data): e0a178da01680097ff000008004500006442f440004006db...
  > Authoritative nameservers
  > Additional records
  [Request In: 61]
  [Time: 0.016830000 seconds]

```

Figure 5: Data frame 62 details

In Bless, examiner deleted the preamble and located the source IP address: 10.4.4.2 (as converted from the hexadecimal highlighted in red in figure 6) and the destination IP address: 10.4.4.1 (as converted from the hexadecimal highlighted in blue in figure 6). The number “06”, highlighted in green, indicates the layer 4 protocol embedded inside the IP packet is TCP. The number “16”, highlighted in yellow, are the first two bytes of the actual TCP segment. The number 16 corresponds to 22 in decimal, indicating the source port from which the data was sent is port 22. Unfortunately, this corresponds with Secure Shell Protocol, which means the data is likely

encrypted. “A9 B8”, highlighted in purple, are the second two bytes of the TCP segment- they represent the destination port. In this case, the hexadecimal value corresponds to decimal value 43448. This port is unassigned according to IANA. “18”, highlighted in orange, is a flag that indicates this extracted segment is part of a successfully established TCP conversation.

```

00000000 | 45 00 00 64 42 F4 40 00 40 06 DB 95 0A 04 04 02 0A 04 | E...dB.@.@.....
00000012 | 04 01 00 16 A9 B8 E3 E6 1A CB E5 62 7F 93 80 18 07 94 | .....b.....
00000024 | F8 C8 00 00 01 01 08 0A 00 03 57 5D 00 03 D0 97 9B 96 | .....W].....
00000036 | 62 E2 CA B6 E8 85 35 6B 7D 2B 17 61 51 3E 24 A7 8C 36 | b.....5k}+.aQ>$..6
00000048 | 1C 67 92 A0 F2 B8 5A E6 71 B1 2E AB 31 37 7A CA 79 33 | .g....Z.q...17z.y3
0000005a | AD 19 3B 6D 88 8F 42 3C 31 57 BF 27 25 66 | ..;m..B<1W.'%f

```









Figure 6: Trimmed contents of data frame 62

## Conclusion

The examiner was asked to determine if the traffic was truly suspicious. Based on the almost exclusively DNS traffic being solely of type “NULL”, the examiner did determine the traffic was genuinely suspicious. The examiner was asked to determine the purpose of the unusual DNS traffic. It is likely for covert tunneling, as “NULL” DNS records can contain any type of data and are often let through organization perimeters. To that end, the examiner successfully carved out a TCP header encapsulated in an IPv4 packet, but the data was encrypted. The examiner was asked to recover as much information as possible about the local and remote systems involved. . The remote tunnel endpoint was probably tnlh.slick.evl (172.16.16.220), while the remote endpoint of the tunneled traffic was 10.4.4.2:22 and the local endpoint of the tunneled traffic was 10.4.4.1:43448. The examiner was asked to evaluate the risk that data was exfiltrated. Since the TCP flags set on the frame examined indicated it was part of an ongoing TCP conversation, the risk of data exfiltration is significant.

# 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

- Wireshark v3.0.6

## Appendix D: Evidence Copies

On 5/4/2020, the examiner created a new *Week8* folder on the *Desktop*, then retrieved archive file *Week 8.zip* via Mozilla Firefox from the CYB457 course shell to the *Week8* folder.

Examiner used the online utility located at [onlinemd5.com](http://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 *Week8* was created called *Working*. Examiner created a working copy of the *Week 8.zip* archive file in the *Working* folder called *Week8XX*. [Onlinemd5.com](http://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 *Week8XX\_FILES* and subfolders *Ch11-NetworkTunnels* and *Ch12-Malware*.

## 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
<b>PRE-ANALYSIS</b>			
Preservation Copy	Week 8.zip	61667661161E829F11CBD9A5D170E30A	Archive file downloaded from Engage
Working Copy	Week8XX	61667661161E829F11CBD9A5D170E30A	Working Copy created from preservation copy. This copy was analyzed.
<b>POST-ANALYSIS</b>			
Preservation Copy	Week 8.zip	61667661161E829F11CBD9A5D170E30A	Archive file downloaded from Engage
Working Copy	Week8XX	61667661161E829F11CBD9A5D170E30A	Working Copy created from preservation copy. This copy was analyzed.

Table 2: Evidence Verification Table