

# JAMK University of Applied Sciences

## Data Security Testing

### Laboratory 1 Network audit File

Teacher: Markku Vajaranta

Autor of Assignment: Adam Pawełek

Group: TTKS0700-3001

Jamk number: AA4917

# Assignment 1

I started my search in Wireshark with a dns filter. This was what Wireshark returned as a result.

dns						
No.	Time	Source	Destination	Protocol	Length	Info
585	25.667391	10.100.10.100	10.100.10.15	DNS	71	Standard query 0xfb9a A www.bbc.com
586	25.667391	10.100.10.15	208.67.222.222	DNS	82	Standard query 0x4ac7 A www.bbc.com OPT
591	25.680936	208.67.222.222	10.100.10.15	DNS	166	Standard query response 0x4ac7 A www.bbc.com CNAME www-bbc-com.bbc.n...
592	25.681448	10.100.10.15	10.100.10.100	DNS	155	Standard query response 0xfb9a A www.bbc.com CNAME www-bbc-com.bbc.n...
647	27.865853	10.100.10.100	10.100.10.15	DNS	87	Standard query 0xea81 A safebrowsing.googleapis.com
648	27.865854	10.100.10.15	208.67.222.222	DNS	98	Standard query 0x700a A safebrowsing.googleapis.com OPT
649	27.883551	208.67.222.222	10.100.10.15	DNS	114	Standard query response 0x700a A safebrowsing.googleapis.com A 216.5...
650	27.883915	10.100.10.15	10.100.10.100	DNS	103	Standard query response 0xea81 A safebrowsing.googleapis.com A 216.5...
875	34.490874	10.100.10.100	10.100.10.15	DNS	72	Standard query 0xbe37 A malicious.pw
876	34.490874	10.100.10.15	208.67.222.222	DNS	83	Standard query 0x5549 A malicious.pw OPT
877	34.631118	208.67.222.222	10.100.10.15	DNS	99	Standard query response 0x5549 A malicious.pw A 51.15.75.147 OPT
878	34.634010	10.100.10.15	10.100.10.100	DNS	88	Standard query response 0xbe37 A malicious.pw A 51.15.75.147
922	36.955026	10.100.10.100	10.100.10.15	DNS	77	Standard query 0x46d6 A login.windows.net

▶ Frame 53: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)  
▶ Ethernet II, Src: VMware\_5a:b6:3a (00:0c:29:5a:b6:3a), Dst: VMware\_8b:fc:b7 (00:0c:29:8b:fc:b7)  
▶ Internet Protocol Version 4, Src: 10.100.10.100, Dst: 10.100.10.15  
▶ User Datagram Protocol, Src Port: 52130, Dst Port: 53  
▶ Domain Name System (query)

I found out that some of dns protocols come from malicious sites.

After I used filter with word “malicious” I saw that the first GET HTTP request was file invite\_to\_ski\_trip.docx

String				malicious
	Protocol	Length	Info	
	DNS	72	Standard query 0xbe37 A malicious.pw	
	DNS	83	Standard query 0x5549 A malicious.pw OPT	
	DNS	99	Standard query response 0x5549 A malicious.pw A 51.15.75.147 OPT	
	DNS	88	Standard query response 0xbe37 A malicious.pw A 51.15.75.147	
	TCP	66	49213 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
	TCP	66	49214 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1	
	TCP	58	80 → 49213 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460	
	TCP	54	49213 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0	
	HTTP	478	GET /invite_to_ski_trip.docx HTTP/1.1	
	TCP	54	80 → 49213 [ACK] Seq=1 Ack=425 Win=64240 Len=0	

Then I opened the invite\_to\_ski\_trip.docx and saw the text with the similar format to the nixu flag after decrypt it with Caesar cipher (ROT 13) I found the flag which was:

NIXU{why\_does\_phishing\_work\_so\_well}

Unable to display images

Tbbq! Lbh unir znantrq gb rkgennp guvf qbphzrag naq sbhaq gur synt. Abj syaq  
bhg jung gur qbphzrag qbrf. Urer vf gur synt gung lbh ner ybbxvat sbe:  
AVKH{jul\_qbrf\_cuvfuvat\_ibex\_fb\_jryy}

Good! You have managed to extract this document and found the flag. Now find out what the document does. Here is the flag that you are looking for:  
NIXU{why\_does\_phishing\_work\_so\_well}

## Assignment 2

First I tried to find tls connection between 51.15.75.147 (malicious source) and infected computer.

ip.src == 51.15.75.147 and tls						
No.	Time	Source	Destination	Protocol	Length	Info
1108	56.048480	51.15.75.147	10.100.10.100	SSL	60	Continuation Data
1225	61.387322	51.15.75.147	10.100.10.100	SSL	65	Continuation Data
1242	64.422396	51.15.75.147	10.100.10.100	SSL	60	Continuation Data

After Follow TCP stream showed the data how the infected program works.

```
whoami
acme\octavio.gardner
PS C:\Users\octavio.gardner\Downloads> dir

Directory: C:\Users\octavio.gardner\Downloads

Mode                LastWriteTime         Length Name
----                -
-a---             15.2.2018      15:53         23771 invite_to_ski_trip.docx
```

Then when I was scrolling down through the data I found that program type cleartext.txt (the same name as in the HINT) and displayed data looks like a NIXU flag. I decrypted it with ROT (1). The second flag is : NIXU{wh4t\_1s\_th1s\_cl34rt3xt\_tr1ck3ry}

```
PS C:\> type cleartext.txt
MHWT{vg4s_1r_sg1r_bk34qs3ws_sq1bj3qx}
PS C:\> get-childitem -path env:computername
```