JAMK University of Applied Sciences

Data Security Testing

Laboratory 1 Network audit File

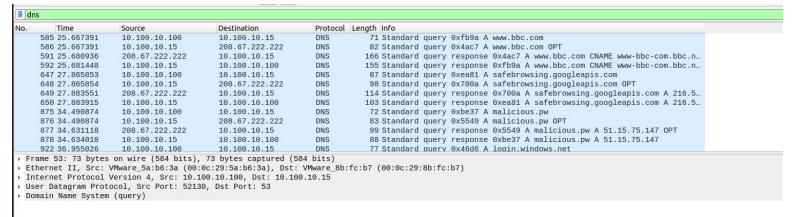
Teacher: Markku Vajaranta

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.



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	Lengl	th Info
	DNS		72 Standard query 0xbe37 A malicious.pw
	DNS	1	B3 Standard query 0x5549 A malicious.pw OPT
	DNS		99 Standard query response 0x5549 A malicious.pw A 51.15.75.147 OPT
	DNS	1	B8 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	1	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	4	78 GET /invite_to_ski_trip.docx HTTP/1.1
	TCP		54 80 → 49213 [ACK] Seq=1 Ack=425 Win=64240 Len=0
	20.20		rear train found tone a lab to the break a lab to be the break and the b

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 rkgenpg guvf qbphzrag naq sbhaq gur synt. Abj svaq bhg jung gur qbphzrag qbrf. Urer yf gur synt gung lbh ner ybbxvat sbe:

AVKH {jul_qbrf_cuvfuvat_jbex_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.

No.	Time	Source	Destination	Protocol	Length Info
	1108 56.048480	51.15.75.147	10.100.10.100	SSL	60 Continuation Data
1	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.

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
```