

Harcèlement à Nitroba

L'objectif de ce TP est de trouver qui envoie des mails offensif à l'enseignante Lily Tuckrige.

Afin de résoudre ce problème je vais suivre les étapes suivantes:

- 1. Établir la carte du réseau de la chambre des étudiants à Nitroba.
- 2. Trouver qui a envoyer le mail à lilytuckrige@yahoo.com
- 3. Identifier l'autre connexion TCP qui appartient à l'attaquant.
- 4. Trouver des informations dans l'une de ces connexions TCP afin d'identifier l'attaquant.

1. Établir la carte du réseau de la chambre des étudiants à Nitroba

On verifie avec l'IP trouver dans l'en-tête du mail Yahoo dans quels trame elle apparait:

ip.addr == 140.247.62.34					
No.	Time	Source	Destination	Protocol	Length Info
50499	12768.417378	192.168.15.4	140.247.62.34	TCP	82 34526 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734633743 TSecr=0 SACK_PERM
50500	12768.503618	140.247.62.34	192.168.15.4	TCP	78 8000 → 34526 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351651998 TSecr=734633743 WS=128
50501	12768.504990	192.168.15.4	140.247.62.34	TCP	70 34526 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734633744 TSecr=351651998
50512	12797.461488	192.168.15.4	140.247.62.34	TCP	82 34528 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734634033 TSecr=0 SACK_PERM
50513	12797.547524	140.247.62.34	192.168.15.4	TCP	78 8000 → 34528 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351681047 TSecr=734634033 WS=128
50514	12797.548897	192.168.15.4	140.247.62.34	TCP	70 34528 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634034 TSecr=351681047
50515	12799.171175	192.168.15.4	140.247.62.34	TCP	75 34528 → 8000 [PSH, ACK] Seq=1 Ack=1 Win=65612 Len=5 TSval=734634051 TSecr=351681047
50516	12799.258154	140.247.62.34	192.168.15.4	TCP	70 8000 → 34528 [ACK] Seq=1 Ack=0 Win=5888 Len=0 TSval=351682757 TSecr=734634051
50518	12817.474960	192.168.15.4	140.247.62.34	TCP	70 34526 → 8000 [FIN, ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634233 TSecr=351651998
50519	12817.560803	140.247.62.34	192.168.15.4	TCP	70 8000 → 34526 [FIN, ACK] Seq=1 Ack=2 Win=5888 Len=0 TSval=351701063 TSecr=734634233
50524	12828.804459	140.247.62.34	192.168.15.4	TCP	70 34526 → 8000 [ACK] Seq=2 Ack=2 Win=65612 Len=0 TSval=734634297 TSecr=351707308
50555	12823.806086	192.168.15.4	140.247.62.34	TCP	82 34544 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734634330 TSecr=0 SACK_PERM
50556	12827.113703	192.168.15.4	140.247.62.34	TCP	78 8000 → 34544 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351710703 TSecr=734634330 WS=128
50557	12827.198965	140.247.62.34	192.168.15.4	TCP	70 34544 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634331 TSecr=351710703
50558	12827.206313	192.168.15.4	140.247.62.34	TCP	82 34554 → 8000 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=734634599 TSecr=0 SACK_PERM
50872	12853.215233	192.168.15.4	140.247.62.34	TCP	78 8000 → 34554 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1408 SACK_PERM TSval=351736809 TSecr=734634599 WS=128
50873	12853.300279	140.247.62.34	192.168.15.4	TCP	70 34554 → 8000 [ACK] Seq=1 Ack=1 Win=65612 Len=0 TSval=734634591 TSecr=351736809
50874	12853.301590	192.168.15.4	140.247.62.34	TCP	188 Client Hello
50875	12853.302148	192.168.15.4	140.247.62.34	SSLv2	1466 Server Hello
50876	12853.389197	140.247.62.34	192.168.15.4	TCP	70 8000 → 34554 [ACK] Seq=1 Ack=119 Win=5888 Len=0 TSval=351736897 TSecr=734634591
50877	12853.506156	140.247.62.34	192.168.15.4	TLSv1	1460 8000 → 34554 [ACK] Seq=1397 Ack=119 Win=5888 Len=1396 TSval=351737011 TSecr=734634591 [TCP segment of a reassembled PDU]
50878	12853.508100	140.247.62.34	192.168.15.4	TCP	174 8000 → 34554 [PSH, ACK] Seq=2793 Ack=119 Win=5888 Len=104 TSval=351737011 TSecr=734634591 [TCP segment of a reassembled PDU]
50879	12853.508113	140.247.62.34	192.168.15.4	TCP	70 34554 → 8000 [ACK] Seq=119 Ack=2793 Win=64216 Len=0 TSval=734634593 TSecr=351737011
50880	12853.510804	192.168.15.4	140.247.62.34	TCP	70 34554 → 8000 [ACK] Seq=119 Ack=2897 Win=65508 Len=0 TSval=734634593 TSecr=351737011
50881	12853.510397	192.168.15.4	140.247.62.34	TCP	70 34554 → 8000 [ACK] Seq=119 Ack=2897 Win=65508 Len=0 TSval=734634593 TSecr=351737011
50882	12853.596708	140.247.62.34	192.168.15.4	TLSv1	764 Certificate, Server Key Exchange, Server Hello Done
50883	12853.598267	192.168.15.4	140.247.62.34	TCP	70 34554 → 8000 [ACK] Seq=119 Ack=3591 Win=64918 Len=0 TSval=734634594 TSecr=351737104
50884	12853.643734	192.168.15.4	140.247.62.34	TLSv1	268 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
50885	12853.730657	140.247.62.34	192.168.15.4	TCP	70 8000 → 34554 [ACK] Seq=3591 Ack=317 Win=6912 Len=0 TSval=351737239 TSecr=734634595
50886	12853.744678	140.247.62.34	192.168.15.4	TLSv1	129 Change Cipher Spec, Encrypted Handshake Message
50887	12853.745927	192.168.15.4	140.247.62.34	TCP	70 34554 → 8000 [ACK] Seq=317 Ack=3650 Win=65552 Len=0 TSval=734634596 TSecr=351737253
50888	12853.830492	140.247.62.34	192.168.15.4	TLSv1	139 Application Data
50889	12853.831917	192.168.15.4	140.247.62.34	TCP	70 34554 → 8000 [ACK] Seq=317 Ack=3719 Win=65542 Len=0 TSval=734634597 TSecr=351737339

On remarque que cette IP n'apparait que dans des échanges avec l'IP local 192.168.15.4 qui est surement l'IP local de l'attaquant.

On peut vérifier dans l'onglet Statistiques > Point de terminaisons toutes les adresses IP qui apparaissent dans cette capture avec le nombre de paquets qu'elles ont envoyés:

Ethernet · 17		IPv4 · 443	IPv6
Adresse	Paquets	Octets	
192.168.15.1	2154	795 ko	
192.168.15.2	6	536 octets	
192.168.15.4	73197	45 Mo	
192.168.15.5	14	2 ko	
192.168.15.7	3	192 octets	
192.168.15.8	6	600 octets	
192.168.15.255	1	70 octets	

Il y a donc 5 machines connectées sur le réseau (192.168.15.1 est la gateway) mais on remarque que l'IP trouvé précédemment à envoyé beaucoup plus de paquets que les autres (73 197).

2. Trouver qui a envoyer le mail à lilytuckrige@yahoo.com

On vient chercher dans les flux http qui a envoyé un mail à Lily pour ce faire j'utilise le filtre **frame contains "lilytuckrige@yahoo.com"** pour trouver dans les flux http l'email correspondant.

frame contains "lilytuckrige@yahoo.com"						
No.	Time	Source	Destination	Protocol	Length	Info
80614	15110.452871	192.168.15.4	69.80.225.91	HTTP	844	POST /send.php HTTP/1.1 (application/x-www-form-urlencoded)
83601	15197.216422	192.168.15.4	69.25.94.22	HTTP	719	POST /secure/submit HTTP/1.1 (application/x-www-form-urlencoded)

▶ Frame 80614: 844 bytes on wire (6752 bits), 844 bytes captured (6752 bits)

▶ Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)

▶ Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.80.225.91

▶ Transmission Control Protocol, Src Port: 35876, Dst Port: 80, Seq: 1, Ack: 1, Len: 774

▶ Hypertext Transfer Protocol

▶ HTML Form URL Encoded: application/x-www-form-urlencoded

▶ Form item: "email" = "lilytuckrige@yahoo.com"

▶ Form item: "sender" = "the_whole_world_is_watching@nitroba.org"

▶ Form item: "subject" = "Your class stinks"

▶ Form item: "message" = "Why do you persist in teaching a boring class?r\nr\nWe don't like it.r\nr\nWe don't like you.r\nr\nr\n"

▶ Form item: "security_code" = "xkpmkb"

▶ Form item: "submit" = " SEND! "

On trouve bien un mail, provenant de l'IP 192.168.15.4 comme trouvé ci-dessus. On peut voir dans le champ "HTML Form URL Encoded" l'email d'envoi qui est: **the_whole_world_is_watching@nitroba.org**

Cet email ne nous aide pas beaucoup car il ne nous donne pas de réel identité sur l'attaquant.

En revanche, j'ai pu trouver des informations sur l'adresse MAC de l'attaquant dans l'en-tête ethernet.

▼ Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
▶ Destination: HonHaiPrecis_2e:4f:60 (00:1d:d9:2e:4f:60)
▼ Source: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
Address: Apple_e2:c0:ce (00:17:f2:e2:c0:ce)
.....0. = LG bit: Globally unique address (factory default)
.....0. = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Frame check sequence: 0xaf725def [unverified]
[FCS Status: Unverified]

L'adresse MAC de l'attaquant est 00:17:f2:e2:c0:ce, c'est une machine Apple qui est utilisé.

3. Identifier l'autre connexion TCP qui appartient à l'attaquant

eth.src == 00:17:f2:e2:c0:ce and tcp						
No.	Time	Source	Destination	Protocol	Length	Info
18820	9526.633433	192.168.15.4	72.21.210.11	TCP	82	32814 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=643973886 TSecr=0 SACK_PERM
18822	9526.716841	192.168.15.4	72.21.210.11	TCP	64	32814 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
18823	9526.717575	192.168.15.4	72.21.210.11	HTTP	763	GET / HTTP/1.1
18829	9527.582784	192.168.15.4	72.21.210.11	TCP	64	32814 → 80 [ACK] Seq=706 Ack=2817 Win=65535 Len=0
18830	9527.624982	192.168.15.4	72.21.210.11	TCP	64	32814 → 80 [ACK] Seq=706 Ack=4225 Win=65535 Len=0
18833	9527.670916	192.168.15.4	72.21.210.11	TCP	64	32814 → 80 [ACK] Seq=706 Ack=7041 Win=65535 Len=0
18838	9527.710852	192.168.15.4	72.21.210.11	TCP	64	32814 → 80 [ACK] Seq=706 Ack=9857 Win=65535 Len=0
18840	9527.732434	192.168.15.4	69.22.167.225	TCP	82	32816 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=643973897 TSecr=0 SACK_PERM
18841	9527.732853	192.168.15.4	69.22.167.225	TCP	82	32816 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=643973897 TSecr=0 SACK_PERM
18844	9527.744287	192.168.15.4	69.22.167.225	TCP	70	32816 → 80 [ACK] Seq=1 Ack=1 Win=524288 Len=0 TSval=643973897 TSecr=2616953456
18845	9527.744644	192.168.15.4	69.22.167.225	HTTP	471	GET /images/G/01/nav2/gamma/n2CoreLibs/n2CoreLibs-n2v1-43122_V252271770_css HTTP/1.1
18846	9527.745448	192.168.15.4	69.22.167.225	TCP	70	32818 → 80 [ACK] Seq=1 Ack=1 Win=524288 Len=0 TSval=643973897 TSecr=2616953457
18847	9527.746070	192.168.15.4	69.22.167.225	HTTP	460	GET /images/G/01/nav2/gamma/n2CoreLibs/n2CoreLibs-utilities-38260_V252271771_js HTTP/1.1
18856	9527.772198	192.168.15.4	69.22.167.225	HTTP	70	32816 → 80 [ACK] Seq=482 Ack=2123 Win=524168 Len=0 TSval=643973897 TSecr=2616953480
18859	9527.776791	192.168.15.4	69.22.167.225	TCP	70	32818 → 80 [ACK] Seq=391 Ack=2793 Win=523496 Len=0 TSval=643973897 TSecr=2616953482
18861	9527.781322	192.168.15.4	69.22.167.225	TCP	70	32818 → 80 [ACK] Seq=391 Ack=5585 Win=523496 Len=0 TSval=643973897 TSecr=2616953482
18865	9527.791875	192.168.15.4	69.22.167.225	TCP	70	32818 → 80 [ACK] Seq=391 Ack=8377 Win=523496 Len=0 TSval=643973897 TSecr=2616953489
18868	9527.796733	192.168.15.4	69.22.167.225	TCP	70	32818 → 80 [ACK] Seq=391 Ack=11169 Win=524288 Len=0 TSval=643973897 TSecr=2616953499
18869	9527.797216	192.168.15.4	69.22.167.225	TCP	70	32818 → 80 [ACK] Seq=391 Ack=12036 Win=524024 Len=0 TSval=643973897 TSecr=2616953504
18873	9527.825275	192.168.15.4	72.21.210.11	TCP	64	32814 → 80 [ACK] Seq=706 Ack=19713 Win=65535 Len=0
18874	9527.853853	192.168.15.4	69.22.167.225	HTTP	463	GET /images/G/01/nav2/gamma/n2CoreLibs/n2CoreLibs-staticPopover-64246_V15093810_js HTTP/1.1
18878	9527.874797	192.168.15.4	69.22.167.225	TCP	70	32816 → 80 [ACK] Seq=795 Ack=4915 Win=524288 Len=0 TSval=643973898 TSecr=2616953581
18880	9527.877082	192.168.15.4	69.22.167.225	TCP	70	32816 → 80 [ACK] Seq=795 Ack=6311 Win=523496 Len=0 TSval=643973898 TSecr=2616953581
18881	9527.878995	192.168.15.4	69.22.167.225	TCP	70	32816 → 80 [ACK] Seq=795 Ack=7690 Win=523512 Len=0 TSval=643973898 TSecr=2616953581
18882	9527.887796	192.168.15.4	69.22.167.225	HTTP	461	GET /images/G/01/nav2/gamma/n2CoreLibs/n2CoreLibs-popoverPane-29787_V15093773_js HTTP/1.1
18886	9527.908624	192.168.15.4	69.22.167.225	TCP	70	32816 → 80 [ACK] Seq=1186 Ack=18482 Win=524288 Len=0 TSval=643973898 TSecr=2616953615
18888	9527.911866	192.168.15.4	69.22.167.225	TCP	70	32816 → 80 [ACK] Seq=1186 Ack=19010 Win=523760 Len=0 TSval=643973898 TSecr=2616953615
18894	9527.919142	192.168.15.4	69.22.167.225	HTTP	459	GET /images/G/01/nav2/gamma/n2CoreLibs/n2CoreLibs-dynUpdate-18629_V15093772_js HTTP/1.1
18901	9527.940620	192.168.15.4	69.22.167.225	TCP	70	32816 → 80 [ACK] Seq=1575 Ack=15802 Win=524288 Len=0 TSval=643973899 TSecr=2616953646
18903	9527.943553	192.168.15.4	69.22.167.225	TCP	70	32816 → 80 [ACK] Seq=1575 Ack=18594 Win=524288 Len=0 TSval=643973899 TSecr=2616953646
18908	9527.953470	192.168.15.4	69.22.167.225	TCP	70	32816 → 80 [ACK] Seq=1575 Ack=21386 Win=524288 Len=0 TSval=643973899 TSecr=2616953646
18909	9527.956447	192.168.15.4	69.22.167.225	TCP	70	32816 → 80 [ACK] Seq=1575 Ack=22817 Win=524288 Len=0 TSval=643973899 TSecr=2616953663
18910	9527.970784	192.168.15.4	69.22.167.225	HTTP	465	GET /images/G/01/nav2/gamma/n2CoreLibs/n2CoreLibs-multiPanePopover-33447_V6309567_js HTTP/1.1
18914	9527.991261	192.168.15.4	69.22.167.225	TCP	70	32816 → 80 [ACK] Seq=1970 Ack=25609 Win=524288 Len=0 TSval=643973899 TSecr=2616953698
18915	9527.991770	192.168.15.4	69.22.167.225	TCP	70	32816 → 80 [ACK] Seq=1970 Ack=26310 Win=524192 Len=0 TSval=643973899 TSecr=2616953698
18916	9528.025264	192.168.15.4	72.21.210.11	TCP	64	32814 → 80 [ACK] Seq=706 Ack=29569 Win=65535 Len=0
18922	9528.122608	192.168.15.4	72.21.210.11	TCP	64	32814 → 80 [ACK] Seq=706 Ack=36231 Win=65535 Len=0
18925	9528.216127	192.168.15.4	216.73.86.52	TCP	82	32820 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=643973902 TSecr=0 SACK_PERM
18928	9528.286259	192.168.15.4	8.12.217.125	TCP	82	32822 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=643973902 TSecr=0 SACK_PERM
18929	9528.286809	192.168.15.4	8.12.217.125	TCP	82	32824 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=0 TSval=643973902 TSecr=0 SACK_PERM
18932	9528.290374	192.168.15.4	8.12.217.125	TCP	70	32822 → 80 [ACK] Seq=1 Ack=1 Win=524288 Len=0 TSval=643973902 TSecr=452580104
18933	9528.299959	192.168.15.4	8.12.217.125	HTTP	442	GET /images/G/01/advertising/pin/visa/visa-pin_V251923494_gif HTTP/1.1
18934	9528.300559	192.168.15.4	8.12.217.125	TCP	70	32824 → 80 [ACK] Seq=1 Ack=1 Win=524288 Len=0 TSval=643973902 TSecr=452579084
18935	9528.301129	192.168.15.4	8.12.217.125	HTTP	451	GET /images/G/01/gno/images/orangeBlue/navLeftBrowseBottom_V510842_gif HTTP/1.1
18940	9528.321527	192.168.15.4	8.12.217.125	TCP	70	32822 → 80 [ACK] Seq=373 Ack=2793 Win=523496 Len=0 TSval=643973902 TSecr=452580106
18942	9528.324918	192.168.15.4	8.12.217.125	TCP	70	32824 → 80 [ACK] Seq=382 Ack=572 Win=524288 Len=0 TSval=643973902 TSecr=452579087
18944	9528.334296	192.168.15.4	8.12.217.125	TCP	70	32822 → 80 [ACK] Seq=373 Ack=2908 Win=524288 Len=0 TSval=643973903 TSecr=452580108
18946	9528.350168	192.168.15.4	216.73.86.52	TCP	70	32820 → 443 [ACK] Seq=1 Ack=1 Win=524288 Len=0 TSval=643973902 TSecr=172566468

L'attaquant a de nombreuses connexions TCP qui lui appartiennent cependant on peut rechercher uniquement celles qui sont relatives à des mails avec le filtre suivant: **frame contains "mail"**

L'adresse email est: jcoachj@gmail.com

On regardant la liste des élèves fournie, un élève semble correspondre à cet email.

Chemistry 109 class list:

Teacher: Lily Tuckrige

Students:

Amy Smith

Burt Greedom

Tuck Gorge

Ava Book

Johnny Coach

Jeremy Ledvkin

Nancy Colburne

Tamara Perkins

Esther Pringle

Asar Misrad

Jenny Kant

L'étudiant qui a envoyé tout ces mails à Lily Tuckrige est **Johnny Coach** dont l'email est jcoachj@gmail.com.